ユーザマニュアル

Private Cloud 11.0

MDaemon Private Cloud
ユーザマニュアル

MDPC 11.0.0 - 7月 2023

目次

セクション 1

1 MDaemon Private Cloud 11.0

はじめに

MDaemon Technologies社のMDaemon Messaging Serverは、標準プロトコルのSMTP/POP3/IMAPに準拠したメールサーバーで、Windows 7, Server 2008 R2及びそれ以降のOSに対応しており、幅広い機能を搭載しています。MDaemonはあらゆる規模のユーザーニーズに答えるために設計され、メールアカウントやメッセージフォーマットの管理を統合的に行なえるよう設計されています。MDaemonは、LDAPやActive Directory連携も行えるSMTP、POP3、IMAP4のメールサーバー機能と、Webメール機能、コンテンツフィルタリング、スパムフィルタ、セキュリティといった数々の機能を搭載しています。

MDaemonの機能

MDaemonはSMTP, POP3, IMAP4のメール処理に加えて、様々な機能を搭載しています。その一部を下記の通りご紹介します。

- ウィルスチェックに対応しており、MDaemonやMDaemon Provate Cloudエディションへのアドオンとして利用できます。この機能により、Outbreak Protection 583や MDaemon AntiVirus 609によるメールのスキャンや隔離、削除が、宛先アドレスへ到達する前にリアルタイムで行われます。更に、ウィルス発見時、管理者や送信者、宛先に対して通知するようMDaemonで設定する事もできます。
- MDaemonにはメーリングリストやグループ管理機能が搭載されており、社内・社外のメンバーを無制限に所有できる配布リスト機能も搭載されています。リストについては購読要求を許可または拒否の設定、公開又は非公開の設定、メール返信をメーリングリストに行うか送信者に行うか、ダイジェストフォーマットの利用、他の機能の有効化などを設定する事ができます。
- MDaemonの統合機能として Webmail 291 があります。これを使う事で、パソコンに上のメーラーの代わりに、お好きなウェブブラウザを使ってメールにアクセスできるようになります。これは、モバイルユーザーやメール受信用に専用パソコンを持っていないユーザーにとって非常に便利な機能です。
- MDaemon Webmail 一般的なメーラーが持つ機能を全て搭載しています。例えば、メールの送受信、スペルチェック、複数の個人フォルダの管理、18カ国語での画面表示、会議や打ち合わせのスケジュール、他のユーザーとの予定や仕事情報の共有、(Remote Administration 321と併用した場合)MDaemonアカウントの設定、連絡先の管理、といった機能が用意されています。また、WebmailにはMDaemon Instant Messenger (MDIM) 292も搭載されており、エンドユーザーのパソコンから簡単にダウンロードしインストールする事ができま

す。このユーティリティにより、ウェブブラウザを開くことなく、新着メールの確認や既存メール/フォルダへのアクセスが容易に行えます。さらに、MIDMや他のXMPP[340]を使用し、MDaemonユーザー間で手軽に"チャット"ができるインスタントメッセンジャー機能も備えています。

- MDaemonには、メールシステムを安全性を高めるための機能も数多く搭載しています。スパマーがドメイン宛に送信するスパムメールのほとんどは、スパムフィルタとDNSブロックリストでブロックされます。IPスクリーニングとホストスクリーニングおよびアドレスブロックリストは、特定のアドレスやドメインから、自社のメールサーバー経由で外部へのメール送信を行う、いわゆる踏み台にされるリスクから、システムを保護するための機能です。逆に、特定のIPアドレス以外からのメールは受け付けないように制限する事などもできます。
- MDaemonは、Lightweight Directory Access Protocol (LDAP)連携も行えるため、LDAPサーバーで管理しているアカウント情報を最新の状態に保つ事ができます。これにより、LDAPの連絡先情報も最新の情報で保持する事ができるため、LDAP対応のメーラーで、エンドユーザーも情報を有効活用できます。また、MDaemon自身が管理するユーザー情報についても、ODBC互換のデータベースやローカルのUSERLIST.DATではなく、Active DirectoryやLDAPサーバーをお使い頂けます。このため、異なる場所に設置した複数のMDaemonで同じアカウントデータベースを使用したい、といった要件にも、簡単に対応する事ができます。
- MDaemonの詳細な帯域制御機能により、ダイアルアップ接続でISPのPOP3メールボックスを受信するのと同等の負荷で、LAN全体にメールの一斉配信が行えます。通常ネットワークにかかるコストのほんの少しで、ネットワーク全体のメールシステムとしてもご利用頂く事ができます。
- アドレスエイリアス機能では、"架空の"メールボックスに届くメールを実在するアカウントやメーリングリストへ転送することができます。これにより、個々のアカウントやメーリングリストが複数のメールアドレスもしくはドメインのアドレスを持つことができます。
- ドメインゲートウェイ機能は、各部門やグループに対して個別に割り振られたドメインが、ローカルネットワークあるいはインターネット上にあるかに関わらずご利用頂ける機能です。この機能を利用すると、各ドメインのメールボックスを持つサーバ群を代表して、それらのドメインすべてのメールを受信し、その後各サーバへ配信されます。この機能は他のドメインのメールサーバのバックアップ受信サーバとして使用することもできます。
- ウェブからご利用頂けるリモート管理機能が搭載されています。MDaemonの Remote Administration[321] はMDaemonやWebmailと統合されており、ユーザーがブラウザからアカウントの設定を確認したり変更したりできるようになります。ユーザーが編集できる設定内容は事前に選択でき、アカウント毎にアクセス権を割り当てる事もできます。Remote Administrationは、管理者(もしくは、その権限が与えられたユーザー)が使う事もでき、MDaemonサーバーや関連する設定ファイルの編集など、事前に許可した範囲で管理を行う事ができるようになります。
- RAWメールとして知られている内部的なメール配信システムにより、シンプルなメールの配信やメールソフトウェア開発を実現しています。RAWを使用する事で、シンプルなテキストエディタと数個のバッチファイルだけで、完全なメールシステムを構築できるようになっています。
- 多目的に使えるコンテンツフィルタリングシステムにより、送受信されるメールの内容によってサーバの振る舞いを調整することができます。メッセージヘッダやフッダへの文字列の挿入や削除、添付ファイルの削除、他のユーザへメールコピーの送信、インスタントメッセージでの通知、任意のプログラムを実行、といった、環境に応じたカスタマイズが行えます。

MDaemon Private Cloud

MDaemon Private Cloud (MDPC) はMDaemon Messaging Serverの特別なエディションで、MDaemonを使ってホスティングサービスを行うリセラーやITサービスプロバイダ向けに開発されました。オンプレミスのMDaemonと違い、MDPCはホスティング環境での使用を想定したライセンスシステムやコード

で構成されています。MDaemon Private Cloudは、MDaemonの全機能に加え、次のような機能を搭載しています:

- 新しいライセンスと課金システム（ユーザー別/月別）
- Outlook対応
- 拡張した複数ドメイン管理
- ドメイン毎のブランディング（ホワイトラベル）
- ドメイン毎のレポート
- 課金対象外のテスト用アカウント（アカウントは課金対象のカウントに含まれません）
- Outbreak Protection、MDaemon Antivirus、ClamAVアンチウィルスエンジン（別料金でのオプション）
- ActiveSync for MDaemon（別料金でのオプション）

システム要件

MDaemonシステム要件や推奨要件につきましては、 www.mdaemon.comからSystem Requirementsページをご覧ください。

商標

参照:

MDaemon Private Cloud 11.0の新機能 14
MDaemon Private Cloud 11.0.0へのアップグレード 55
MDaemonの管理画面 64
製品サポート 60

1.3 MDaemon Private Cloud 11.0の新機能

MDaemon Private Cloud 11.0.0の新機能

- MDaemon Private Cloud 11.0にはMDaemon 23.0.2とMDaemon Connector 7.0.7が含まれています。
- MDaemonは、バージョン7.0.6以前のバージョンのMDaemon Connectorの自動更新に不具合があったため、自動更新を無効化しました。

MDaemonの変更点全てを確認するには MDaemon 23.0.2 リリースノート.を参照して下さい。

MDaemon Connectorの変更点全てを確認するには MDaemon Connector 7.0.7 リリースノート.を参照して下さい。

変更点と新機能

MDaemon Server

- （23.0.2） 設定 | サーバ設定 | MultiPOP[130] 画面に、MultiPOPアカウントの複数のメール受信に失敗した際の通知メールを送信するオプションを追加しました。一時的な受信失敗は、あり得ることなので通知までの間、どのくらいの失敗が続いた時に通知するオプションとなります。通知メールが多すぎることを避けるため、通知の間隔日数を指定するオプションもあります。通信メールの内容と受信者は、¥MDaemon¥App¥MPOPFailure Notice.datで調整することもできます。デフォルトでは、5回の受信失敗が続いた後、1週間ごとに1度MultiPOPアカウントユーザーに送信されます。

- サーバー設定の中に、新しくMultiPOP[130]ページができました。このページから、MDaemonのMultiPOPサーバーの、有効化/無効化が行え、（従来 MultiPOP収集[350]ページで使用していた）「*MultiPOP収集後…*」オプションを使用し、全てのユーザーの、*POPサーバーへメールのコピーを残す*[673]オプションを上書きする事ができます。また、新しいページはOAuth 2.0にも対応しており、GmailやOffice 365からのMultiPOPメール収集を行うためのオプションも追加しました。

  GmailとOffice365からのMultiPOPメール収集がOAuth 2.0に対応[131] — OAuth 2.0は**先進認証と呼ばれ、**GmailやMicrosoft（Office）365が、従来のレガシー/基本認証のサポートを無効化すると同時に必須とした認証方式です。MDaemonのMultiPOPで、ユーザーに代わってGmailやOffice 365から先進認証でメールの収集を行うには、MDaemonを、Googleであればの Google APIコンソール、Microsoftであれば Microsoft Azure Active Directoryから、OAuth 2.0アプリケーションとして作成する必要があります。手順はWebmailユーザー用のDropbox統合[309]に似ています。OAuth 2.0に対応した設定手順についてはMultiPOP[131]を参照してください。

- MDaemonの IMAPサーバーがキーワードフラグに対応しました。Mozilla Thunderbirdなどのメーラーからサーバーへ、メール本文のキーワードをもとにしたタグを保存する事で、別のクライアント側でもタグの表示ができるようになります。

- サイズの大きいメールフォルダを開く際のIMAPサーバーのパフォーマンスを改善しました。

セキュリティ

- （23.0.2） Spamhaus Data Query サービス（DQS）を、セキュリティマネージャ | スパムフィルタ[616]に追加しました。Spamhaus DQSの詳細につきましては、https://info.spamhaus.com/getting-started-with-dqsをご参照下さい。

- ダイナミックスクリーニング[556]に*ブロックログインポリシー侵害*という名前の新しいオプションを追加し、ログインにメールアドレスを使用しなかったIPアドレスをブロックできるようになりました。このオプションはデフォルトで無効に設定されています。関連するオプション「*サーバの認証に完全なメールアドレスが必要*」についての詳細は システム[450]ページを参照してください。

- 認証失敗トラッキング[559]ページの、*毎回同じパスワードが使われた場合は除く*オプションを拡張し、*存在するアカウントにだけ適用する*追加オプションを搭載しました。サインインしようとしているユーザーが正しい場合のみ、同じパスワードが使われた場合に認証失敗から除外したい

場合には、このオプションを有効にして下さい。これにより、クライアントがパスワード変更を行った際、別のクライアントが古いパスワードを使用していても、正しいログオン名をしようしているため、重複パスワードだけを無視が有効になります。ボットは通常ランダムなログインIDと類似パスワードでログインを試しますが、こうした接続は認証失敗ですぐに拒否されます。これによりボット対策が早急に行えるようになります。XML APIダイナミックスクリーンの処理も、こうした新機能を反映したものへアップデートしました。

- コンテンツフィルタ ≫ 添付ファイル[599] へ、*禁止された添付ファイルが削除された場合、メール本文の上部へ警告を追加する*オプションを追加しました。例えばウィルスを検出した場合など、MDaemonがメールから添付ファイルを削除した際、メール本文の上に警告を追加する事ができます。メッセージのテンプレートの確認や編集用に、**警告メッセージ**ボタンも追加しました。このオプションはデフォルトで有効です。
- *信用するIPsをウィルスチェック対象から除外する*[609]オプションを追加しました。
- MDaemon[525], Webmail[528], Remote Administration[532] のSSL証明書[523]の有効期限が近づいた際、MDaemonから管理者へ警告メールを送るようになりました。
- MTA-STS[538] が除外リストを持つようになり、問題があるドメインが配送に影響を与えた際、MTA-STSを停止するのではなく、対象ドメインを除外する事ができるようになりました。
- ClamAV AntiVirusコンポネントを0.105.2へアップデートしました。

Webmail

- Google Drive統合[311] — WebmailがGoogleアカウントとリンクし、各ユーザーがメールの添付ファイルをGoogle Driveへ直接保存し、保管されたデータの編集や管理を行う事ができるようになりました。これを有効にするには、**APIキー**, **クライアントID**, **クライアントシークレット** が必要です。これらの情報はGoogle APIコンソールでアプリを作成し、MDaemonをサービスとして登録した際Googleから直接提供されます。OAuth 2.0 認証コンポネントはアプリの一部で、Webmailユーザーが Webmailへサインインし、Goolgle Driveへアクセスするための認証を行うのに使用されます。認証されると、ユーザーはGoogle Drive内のフォルダやファイルを閲覧できます。また、ファイルのアップロード、ダウンロード、移動、コピー、名称変更、削除に加え、ローカルのドキュメントフォルダのコピーや移動も行えます。ユーザーが編集を行う際には、Google Driveでファイルを表示するオプションをクリックする事で、ユーザーのGoogle Driveでの権限に基づき、編集を行う事ができるようになります。Google Driveの設定はMDaemonのDropbox統合[309] や MultiPOP OAuth統合[130]に似ています。詳細については、Google Drive統合[311]を参照してください。
- Liteを除く全てのテーマへ、「*フォルダのドラッグアンドドロップを有効化する*」オプションを追加しました。この新しいオプションは、Webmailの**オプション**内の**フォルダ**ページからアクセスでき、設定はデフォルトで有効です。
- HTTPSを介したセッションクッキーがセキュアになりました。
- MDaemonへカテゴリの変更通知が送信されるようになりました。
- WorldClientの起動時にrobots.txtファイルの編集を行わないようになりました。
- 内蔵ウェブサーバーではHTMLから.dllファイルの直接のダウンロードを禁止するようになりました。
- 新しいパスワードの入力時に最大数を追加し、「最長15文字」を満たしていない事を表示するようになりました。
- ダイナミックスクリーニングのログインポリシー侵害をブロック[556]に対応した、完全なメールアドレスを使わずに行ったサインインのレポートを追加しました。

- （23.0.2）スヌーズ解除オプションをオレンジ色で強調することで、可視性を高めました。

Proテーマ

- 開封確認に対応しました。
- HTMLエディタのコンテキストメニューを無効化するオプションを追加しました。
- フォルダー覧のリサイズ機能を追加しました。

Remote Administration (MDRA)

- **23.0.2**
- "AntiVirus[609]スキャンから信用するIPアドレスを除外する"チェックボックスを追加しました。
- [26434] SMTP[476]認証画面に、"SMTPポートに対する認証を認めない"オプションを追加しました。
- [26430] 設定 | パブリックフォルダ | パブリックフォルダマネージャ[283] | 編集 の画面に、ActiveSync表示名の項目を追加しました。
- Added four more filter options to the Account Manager[648]: Admins Only, Non-Admins Only, Global Admins Only, and Domain Admins Only
- [26433] スパムフィルタ[616]の設定画面に、Data Queryサービスの設定画面を追加しました。Spamhaus DQSの詳細につきましては、https://info.spamhaus.com/getting-started-with-dqsをご参照下さい。

23.0.0

- ドメインマネージャの Webmail設定[316] へ、「*ユーザーがメールで2段階認証用の承認コードを受け取る事を許可*」のオプションを追加し、ユーザーがGoogle認証アプリではなく関連するメールアドレスで認証コードを受け取る事ができるようになりました。この設定はデフォルトで有効です。
- LookupとReadへ新しいACLエントリを追加した際使用するデフォルトの権限を変更しました。
- スパムフィルタ ≫ DNS-BL ≫ ホスト[639] と 設定 ≫ Active Directory ≫ 認証[749] のテストボタンを、処理中は無効化するよう変更しました。
- スパムフィルタ | DNS-BL | ホストと設定 | Active Directory | 認証 で処理を行っている間はテストボタンを無効化するようになりました。
- 内蔵ウェブサーバーでTemplateディレクトリの.dllファイルを直接実行したりダウンロードしたりする事を禁止するようになりました。
- ウィンドウの右上にあるユーザー名（例．frank.thomas）をクリックし、Remote Administrationウェブインターフェイスの見た目をカスタマイズできるようになりました。インターフェイスは、ダークモードへの切替やフォントサイズの変更、言語の変更が行えます。
- カウントの削除確認でカスタマイズされた確認機能を使用するよう変更しました。
- 完全なメールアドレスを使わずに行ったサインインを、ダイナミックスクリーニングのレポートへ追加しました。

ActiveSync

- クライアント設定へ *Junk-Emailフォルダへ移動したメールの送信者をブロックする*[384] オプションを追加しました。有効にすると、クライアントが特定のメールを自分のJunk Emailフォルダへ移

動した際、このメールの送信者やFromアドレスが、ブロックした送信者の連絡先フォルダへ追加されます。

- 必要に応じて、ActiveSyncクライアントの フルワイプボタン[422] を無効化できるようになりました。これにより、新しく追加した工場出荷状態へワイプする機能を無効化する[384]オプションを無効化していないと、ActiveSync端末のフルワイプが行えなくなりました。
- BodyPreferencesデータを人が読み取れるように変換し、同期に関する問題発生時のトラブルシュートを簡単に行えるようにアップデートしました。
- クライアントが大きなサイズのメールボックスを同期していた場合の、シャットダウン時のパフォーマンスを改善しました。
- メールボックスとパブリックフォルダの表示名を変更できるようになりました。
- シャットダウン時のパフォーマンスを改善しました。
- ActiveSyncクライアントで連絡先フォルダへ個人配布リストを送信できるようになりました。
- クライアント設定ダイアログのレイアウトを変更し、新しい設定用のスペースを追加しました。

その他

- (23.0.2) コンテンツフィルタにおいて、ルールの処理に$LIST_ATTACHMENTS_REMOVED$[604]マクロを使用できるようになりました。(例:"send note", "add warning...")
- MDaemon GUIで、LookupとRead用の新しいACLエントリを追加した際使用するデフォルトの権限を変更しました。
- MDaemon GUIで、Webmail, Remote Administration, XMPP BOSHサーバーのポートが競合した際、警告用のポップアップを表示するようになりました。
- XMLAPI – MDaemonの各種INIファイルの編集用のエディタ操作を追加しました。
- 複数のプラグインで新しいバージョンの利用を許可するよう変更し、お客様がhotfix/patchバージョンをテストしやすくなりました。

MDaemonサーバーリリースノート

MDaemonの\Docs\サブフォルダにあるRelNotes.htmlでは、MDaemon 23.0.1で追加された機能や変更点、修正点の詳細をご覧頂けます。

MDaemon Private Cloud 10.0.2の新機能

- MDaemon Private Cloud 10.0にはMDaemon 22.0.5とMDaemon Connector 7.0.7が含まれています。

特記事項

- Outbreak Protectionが復元されました。Outbreak Protection[583] の設定がデフォルト値にリセットされている可能性があるため、設定を確認してください。

MDaemonの変更点全てを確認するには MDaemon 22.0.5 リリースノート.を参照して下さい。

MDaemon Private Cloud 10.0.1の新機能

- MDaemon Private Cloud 10.0にはMDaemon 22.0.4とMDaemon Connector 7.0.7が含まれています。

特記事項

- [26765] これまで使用していたCyren社のアンチウィルス機能から、IKARUS社のアンチウィルス機能へと変更しました。Cyren社が突然の事業停止となり、それに代わるウィルス対策パートナーを慎重かつ確実な検討を行ない、IKARUS社の検出率と反映率が優れていたので変わって採用しました。IKARUS社のアンチウィルス機能では、10分毎にウィルス定義ファイルの自動更新を行います。AntiVirusライセンスの有効期限がきれますと、IKARUSを使ったウィルススキャンは無効化されます。
- [26802] Cyren Outbreak Protection が削除されます。OEMとして使用していたCyren社が事前の話しもほとんどなく、事業の停止計画を発表したためです。そのため、同社と似た仕組みを持つ代わるスパム対策技術を現在積極的に調査と検討を行なっております。

MDaemonの変更点全てを確認するには MDaemon 22.0.4 リリースノート.を参照して下さい。

MDaemon Private Cloud 10.0.0の新機能

- MDaemon Private Cloud 10.0にはMDaemon 22.0.3とMDaemon Connector 7.0.7が含まれています。

MDaemonの変更点全てを確認するには MDaemon 22.0.3 リリースノート.を参照して下さい。

MDaemon Connectorの変更点全てを確認するには MDaemon Connector 7.0.7 リリースノート.を参照して下さい。

MDaemon 22.0の新機能

変更点と新機能

Webmail

Proテーマ

- メールを表示した際、送信者名にカーソルを合わせるとポップアップが起動し、送信者を連絡先や許可リスト、ブロックリストへ追加できるようになりました。
- メール作成、メール一覧、予定表、連絡先、仕事、メモの表示で新しくウィンドウを開くようになりました。
- メールのプレビュー画面や表示画面で、次の未読メールを開く事ができるようになりました。
- 複数行の場合、メール一覧へメールスニペットを追加しました。
- Proテーマの 設定 | 作成 画面に、エイリアスの表示名を編集できるオプションを追加しました。この機能は、デフォルトで無効ですが、Webmail設定 316の"エイリアス表示名の編集をユ

ーザーに許可する"を有効することで使用することができます。注意点：このオプションは MDaemon Remote Administration (MDRA)[321] からのみ利用できます。

- "ホワイトリスト"と"ブラックリスト"と呼んでいたオプションやリンクを、"許可リスト"と"ブロックリスト"へ変更しました。また、ホワイトリスト、ブラックリストフォルダについても、"許可送信者"と"ブロック送信者"へと変更しました。
- メールリストのソートオプションに、フラグでソートする選択肢を追加しました。
- 仕事リストで、期限を過ぎたタスクを赤く表示するようになりました。
- XMPPのバージョンが 4.4.0に更新されました。

その他

- "強固なパスワードを求める"設定を行なった際、パスワード要件がリスト表示されるようになり、要件を満たしたパスワードは緑色で確認できます。またパスワードに問題があった際には、その理由をエラーメッセージとして表示されるようになりました。
- メールの送信や返信、転送の際に使用するデフォルトのFromアドレスを指定するためのオプションを、作成オプションへ追加しました。
- 受信トレイの一覧の再表示時間で、"1分毎"とするオプションを追加しました。
- サインインのページでCSRFトークンを使用できるようになりました。Webmail設定 ≫ Webサーバー[295]で、"Cross-Site-Request-Forgeryトークンを使用する"を有効にすることで使用できます。もし、Webmailへのカスタムテンプレートを使用する場合、次のログインフォームを指定して下さい。`<input type="hidden" name="LOGINTOKEN" value=<$LOGINTOKEN$> />`
- パブリック予定表において、今日から次の30日までのリスト表示が行えるようになりました。
- メッセージ表示において、URL記述をハイパーリンクへ自動的に変換するようになりました。
- Webmailにユーザーログイン時の選択言語にあわせて、デフォルトのフォルダ名（下書き、送信済みアイテムなど）を変換できるようになりました。これは従来英語版MDaemonにのみ搭載されていた機能です。
- 二段階認証の認証コードを指定のメールアドレスに送信するオプションを追加しました。
- LookOut と WorldClientにおいて、すべてのリストカテゴリーが一致するようになりました。
- Webmailにおいて"許可した送信者"と"ブロックした送信者"へアイコンを追加し、特殊なフォルダである事が認識しやすくなりました。

Remote Administration (MDRA)

- MDRAのメインメニューへ 2段階認証を除外するIP設定 ページを追加しました。ここへ記載されたアドレスからRemote AdminやWebmailへ接続すると、2FAを求められる事はありません。
- MDRAのWebmail設定[316] へ、新たに*ユーザーのエイリアス表示名の編集を許可*オプションを追加しました。 WebmailのProテーマでは、設定 >> 作成 の中のエイリアス表示名の編集を使用して表示名が編集できます。
- パスワードフィールドのautocomplete="off"をautocomplete="new-password"へと変更し、FireFoxがログインページでパスワードを自動補完できないようにしました。
- コンテンツフィルタ の 通知[601] 画面に、通知メッセージを編集できるエディタ機能が追加されました。

- サインインのページで、CSRFトークンに対応しました。MDRAの Remote Administration設定ページで、"Cross-Site-Request-Forgeryトークンを使用する"を有効にすることで使用できます。
- MDRAの メールとキュー セクション内で、作成した全てのローカル及びリモートカスタムキュー[798]が管理できるようになりました。

セキュリティ

- MDaemonは、新しいWindowsバージョンで、TLS 1.3を使用できるようになりました。Windows 2022やWindows 11では、デフォルトでTLS 1.3を使用することができます。Windows 10 バージョン2004（OS Build 19041）以降では、実験的なTLS 1.3が使用でき、次のレジストリを入れることで、インバウンド接続において有効にすることができます。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi
    ders\SCHANNEL\Protocols\TLS 1.3\Server

DisabledByDefault (DWORD) = 0

Enabled (DWORD) = 1
```

- MDaemonは、SSL/TLSコネクションで使用する暗号化方式（例、TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384）をログに記録するようになりました。
- パスワード[778]画面の強固なパスワードの条件として、記号文字(!"#$% &'()*+,-./:;<=>?@[¥]^_`{|}~)を含めることを必須とするオプションが追加されました。このオプションは新規インストールされた際にはデフォルトで有効になりますが、既存環境では無効となっております。
- AVメールボックススキャナ - メールボックス内にウィルス感染したメッセージを検出した際、MDaemonのウィルス感染カウンターがカウントアップされるようになりました。
- AntiVirus - ClamAVのバージョンが 0.104.3に更新されました。

ActiveSync

- フォルダ同期のパフォーマンスが向上しました。
- ActiveSync接続モニタリングダイアログ画面において、マウスの右クリックで、セッションの切断やクライアントのブロックを行なうメニューが追加されました。
- クライアント設定[422]ダイアログへ Outlookからエイリアスを使ったメール送信を行うオプションを追加しました。もし、送信者アカウントのReply-Toにエイリアスが指定されたら、メッセージはエイリアスアドレスからの送信となります。
- EAS 16.1のFindコマンドに対応しました。iOSで、EAS 16.1の使用を妨げるプロトコル制限[395]を削除しました。

その他

- コンテンツフィルタ - "会社署名を追加する[590]" 処理で$CONTACT...$マクロが使用できるようになりました。これらのマクロは、パブリック連絡先フォルダ内の送信者連絡先情報を使って、署名を個人用にカスタマイズできます。 参照: 署名マクロ[121]で使用可能なマクロの全リストをご確認頂けます。
- コンテンツフィルタ - 添付ファイルの取り出し[590]と 添付ファイルリンクを追加する[333]処理を追加しました。

- holdingキュー、隔離キュー、Badキューについてのサマリーメール796 に、その中にあるメールを解放、再度キューに入れる、削除を実施できるリンクを追加しました。このオプションは、デフォルトで有効です。注意点： リンクの生成には、Remote Administration URL322 の設定が必要です。
- LetsEncrypt541 - PS 7のスクリプトで動作するように更新されました。
- メッセージリコール109 画面の遅延配信欄に、"メッセージを配信する際、'Date'ヘッダの値を配信時の時間に置き換える" のオプションを追加しました。このオプションはデフォルトで無効です。
- MDaemon Connector353 のバージョンが、7.0.7に更新されました。
- XMLAPI – 予定の転送に対応しました。

MDaemonサーバーリリースノート

MDaemonの¥Docs¥サブフォルダにあるRelNotes.htmlで、MDaemon 22 で追加された機能や変更点や修正点の全てをご覧頂けます。

MDaemon Private Cloud 9.5.0の新機能

- MDaemon Private Cloud 9.5には MDaemon 21.5.2 と MDaemon Connector 7.0.6が含まれています。

MDaemonの変更点全てを確認するには MDaemon 21.5.2 リリースノートを参照して下さい。

MDaemon Connectorの変更点全てを確認するには MDaemon Connector 7.0.6 リリースノートを参照して下さい。

MDaemon 21.5の新機能

Major New Features

Appパスワード683

Appパスワードとは、メーラーやアプリで使用する、非常に強力なランダム生成されたパスワードで、メールアプリケーションのような2段階認証656（2FA）を使用できない場合であっても、これをより安全に利用するためのものです。 2FAを使用するとWebmailや MDaemon Remote Administration（MDRA）へ安全にサインインする事ができますが、メーラーは認証アプリを入力しなかった場合であってもバックグラウンドでメールへアクセスする必要がある事から、2FAを利用できません。Appパスワード機能を使う事で、アカウントパスワードを2FAに保護されている場合であっても、アプリで使用する強力で安全なパスワードを作成する事ができます。Appパスワードはメーラーでのみ使用でき、WebmailやMDRAへのログインには使用できません。つまり、Appパスワードが何らかの方法で不正に盗まれた場合であっても、認証されていないユーザーがアカウントのパスワードや他の設定を変更する事はできず、ユーザー本人は、アカウントへパスワードと2FAでログインし、盗まれたAppパスワードを削除し、新しいAppパスワードを必要に応じて作成する事ができます。

Appパスワードの要件と推奨設定

- Appパスワードを生成するには、アカウントの2FAが有効になっている必要があります。(ただし必要に応じてこの要件を無効化[778]する事もできます。)
- Appパスワードはメーラーでのみ使用できます - WebmailやMDRAへのサインインへは使用できません。
- Appパスワードは作成時に一度だけ表示されます。後から再取得は行えず、作成時にアプリケーションへ入力する必要があります。
- メーラー毎にAppパスワードは異なるものを使用する事をお勧めします。また、アプリケーションの利用を終了する際や端末を紛失したり盗難にあったりした際にはAppパスワードの削除をお勧めします。
- 各Appパスワードは、作成日、最終利用日時、アカウントのメールから最終アクセスした際のIPアドレスが併せて表示されます。最終利用日やIPアドレスのデータが疑わしい場合には、Appパスワードを削除し、再度作成する事をお勧めします。
- アカウントパスワードを変更すると、全てのAppパスワードは自動削除されます。ユーザーは古いAppパスワードを継続して利用する事はできません。

SMTP, IMAP, ActiveSync等へのログインにAppパスワードを必須とする

アカウントエディタの設定[693]ページへ「*SMTP, IMAP, ActiveSync等へのログインにAppパスワードを必須とする*」ためのオプションがあります。

Appパスワードを必須にする事で、アカウントのパスワードを、SMTPやIMAP等での辞書攻撃やブルートフォース攻撃から保護する事ができます。Appパスワードは、例えばパスワードが漏えいしてしまった場合でも、本来のパスワードではなく、MDaemonは正しいAppパスワードのみを受け付けるため、パスワードを取得した攻撃者はこれが本来のパスワードでない事を確認できません。更に、MDaemonアカウントがActive Directory[747]認証を使用しており、Active Directoryがパスワードの連続失敗によりアカウントをロックしたとしても、このオプションを使う事でMDaemonからロックされる事がなくなります。MDaemonはAppパスワードのみで認証を行い、ActiveDirectoryへの問合せを行う事がないためです。

その他変更点と新機能

Proテーマ

- Mobileテーマは、Proテーマへと名称が変わりました。このテーマは異なる種類の端末や異なるサイズの画面にて、機能性を損なわずにシームレスに操作する事を目的に開発されました。
- より安全な処理のためにCross-Site-Request-Forgeryトークンを追加しました。この機能はデフォルトで無効に設定されています。有効化するには、MDRAでメイン | Webmail設定 | Webサーバー[295]で「Cross-Site-Request-Forgeryトークンを使用する」をチェックします。
- 設定 | 初期設定 へダークモードを有効化するためのオプションを追加しました。
- メールの表示画面へ「荷物を追跡」リンクを追加しました。
  - デフォルトで監視する追跡番号は、USPS, UPS, OnTrac, FedEx, DHLの番号です。
  - デフォルトの設定ファイルは、¥MDaemon¥WorldClient¥package_tracking.jsonです。
  - 管理者は`package_tracking.json`と同じ形式で`\MDaemon\WorldClient\package_tracking.custom.json`を、運送業者追加用

に作成する事ができます。1つ以上のサービス名、追跡URL、1つ以上の有効な正規表現の記載が必要です。メールへサービス名が表示されていると、誤った追跡を避けやすくできます。

- メール一覧レイアウト用ダイアログが小さいブラウザサイズ用に追加されました。メール一覧のサイズ設定のみが表示されます。
- パスワード強度メーターを追加しました。
- メール表示用に画像スライドショー機能を追加しました。
- 連絡先一覧へカード表示を追加しました。
- デスクトップサイズの画面では、ツールバーにあった「新しいアイテム」ボタンがフォルダー一覧の上部のスペースへ移動します。
- カレンダー表示で新しいカレンダーの作成時、「個人」の隣にプラスアイコンを追加しました。
- イベントツールチップを追加し、出席者宛のメールを編集し、送信できるオプションを追加しました。
- 1200px又はそれ以上のブラウザサイズだった場合には、検索バーが常に表示されるようになりました。
- ユーザーがホワイトリストへ連絡先を追加した際、自動的にブラックリストから削除したり、その逆の操作をするためのダイアログを追加しました。
- フォルダの作成や名称変更時にエラーが発生した場合、エラーメッセージが表示されるようになりました。
- イベント、連絡先、仕事、メモをHTMLで登録できるようになりました。
- 現在のHTMLエディタ(CKEditor) をJoditへ変更しました。
- ベースヘッダでFromメールアドレスを表示するように変更しました。
- ボイスレコーダーを追加しました。

その他のWebmail変更点

- メールへList-Unsubscribeヘッダが存在する場合に、Fromアドレスの隣へUnsubscribeのリンクを追加するようになりました。これは、設定 | 初期設定で無効化する事もできます。
- 現在のメッセージ一覧へメールをインポートする機能を追加しました。
- Dropbox連携をアップデートし、Dropboxが提供しているrefresh_tokenでOAuthダイアログを介さずにユーザーが再接続できるようになりました。access_tokenの期限が切れると、Webmailは新しいaccess_tokenを取得するのにrefresh_tokenを使用します。クラウドアプリケーションで不要になった設定を削除しました。管理者はDropbox.comで設定変更を行う必要はありません。
- 全てのフォルダ/サブフォルダの検索で、未購読のフォルダが非表示の場合、未購読フォルダを検索対象に含まないよう変更しました。
- 全てのフォルダ/サブフォルダの検索で、特定のフォルダを除外する「検索をスキップ」というチェックボックスを追加しました。
- Remote Adminで2段階認証と認証情報を記憶のチェックボックスを非表示にできるようボタンを追加しました。
- ユーザーセッションが終了した際、背景がぼやける効果を追加しました。

- 設定 | 作成 へ自動CCとBCCを追加しました。
- WorldClient\Domains.ini [Default:Settings] PreventComposeWithAlias,のオプションを追加しました。これはエイリアスでメール作成を行わないようにするための設定です。設定はデフォルトで無効に設定されています。
- Liteテーマ - 作成画面へ下書きの自動保存を追加しました。
- オプション | フォルダ 画面でユーザーがオートコンプリート検索から連絡先フォルダをスキップする機能を追加しました。右クリックメニューへもこのオプションを追加しました。
- ユーザーがログインした際のユーザーエージェントをログに記録するようにしました。
- ローカル受信者が自動応答を有効にしていた場合、メール作成画面で通知するようになりました。
- WorldClientテーマ - 添付ファイル付きのイベントに、クリップアイコンを表示するようになりました。
- 新規インストールでは、添付ファイルの最大サイズが25MBとなります。
- 「空のフォルダ」用に「全てのフォルダを削除」アクションを追加しました。
- WorldClientテーマ - セキュリティページへ「パスワードの変更」と「リカバリーメールアドレスの変更」ボタンを追加しました。

Remote Administration (MDRA)

- コンテントフィルタルールをドラッグ＆ドラッグで設定できるようにしました。コピー、編集、削除ボタンをそれぞれのルールへ追加しました。
- より安全な処理のためにCross-Site-Request-Forgeryトークンを追加しました。この機能はデフォルトで有効です。無効化するには、メイン | Remote Admin 設定 | 設定 で「Cross-Site-Request-Forgeryトークンを使用する」を無効にしてください。
- パスワードのフィールドへ、パスワード強度メーターを追加しました。
- WebmailとRemote Adminで、ドメイン毎の 設定 | ドメインマネージャ | 編集 | Webmail設定 176 と、全体設定の メイン | Webmail設定 | 設定 316 へ、「2段階認証と認証情報を記憶を有効にする」オプションを追加しました。
- ダイナミックスクリーニング用のブロックされたIPと拒否されたIPレポートを追加しました。
- ActiveSyncへグループ 431 とクライアントタイプ 438 を表示する画面を追加しました。
- ActiveSync診断 393 と チューニング 381 ページをアップデートしました。
- レポート | トラフィック | Webmailログイン統計へOS毎のブラウザ使用率を示すチャートとテーブルを追加しました。
- メイン | メーリングリスト | 編集 | 新規 251 へ、ユーザーとグループを一覧からメンバーへ追加するポップアップ表示のためのボタンを追加しました。ドメイン管理者かグローバル管理者 690 だけがこのボタンを使用できます。
- メイン | アカウント | ActiveSyncクライアント と ActiveSync | クライアント管理 422 へ、アカウントだけをワイプするオプションを追加しました。

- 変更ログを追加しました。ここへはRemote Administrationで行った変更が全て記録されます。
- メッセージリコール109の設定をMDaemon GUIと同じになるようアップデートしました。
- セキュリティ | コンテンツフィルタ | 圧縮607へ「winmail.datから添付ファイルを展開」オプションを追加しました。
- MDRA - MDaemon Remote Administrationへスロベニア語を追加しました。

その他のMDaemonの変更点

- SMTP Command Pipelining（RFC 2920）に対応しました。MDaemonは個々にではなく、バッチ処理でMAIL, RCPT, DATAコマンドを送信し、負荷の高いネットワークにおけるパフォーマンスを改善する事ができるようになりました。SMTP pipeliningはインバウンドの接続では常に有効です。アウトバウンドの接続においても、デフォルトで有効ですが、設定 | サーバー設定 | サーバー & 配信 | サーバー82で無効化する事もできます。
- SMTP CHUNKING（RFC 3030）に対応しました。CHUNKINGは行で構成されていないメッセージの配信を許可します。これはインバウンド接続ではデフォルトで有効化されていますが、アウトバウンド接続に対しては無効化されています。受信メールの中の通信データはデフォルトでキャリッジ・リターン通信へ変換されます。このデフォルト値は ¥MDaemon¥App¥MDaemon.iniの[Special] SMTPChunkingInbound=Yes/No, SMTPChunkingOutbound=Yes/No, SMTPChunkingAllowBareLF=Yes/No を設定する事で変更できます。
- コンテンツフィルタ - デフォルトの禁止添付拡張子599の一覧をアップデートしました。
- コンテンツフィルタ - メールへ添付ファイルを追加590するアクションを追加しました。
- ActiveSyncサーバーの開始と終了をMDaemonのシステムログへ記録するようになりました。
- クラスタリング - セカンダリーノードからリマインダの同期が行えるようになりました。
- ダイナミックスクリーニング - ロケーションデータを名称ではなくISOコードでログへ記録556するためのオプションを追加しました。
- XMLAPI - ActiveSyncのAlwaysSendMeetingUpdates 設定に対応しました。
- XMLAPI - セマフォファイルの作成に対応しました。
- XMLAPI - 設定/サーバー設定/ロギングから、レポートと設定変更が行えるようアップデートしました。
- MDaemonインスタントメッセンジャー - グループチャット機能へ、グループチャットを行う複数ユーザー選択機能を追加しました。また、チャットルールのリクエストを自動で許可するオプションを追加しました。
- 国別スクリーニング520で、'X-MDOrigin-Country'ヘッダをメールへ付与するかどうかを選択するオプションを追加しました。これはデフォルトで有効です。
- アカウント | アカウント設定 | エイリアス | 設定759 へエイリアスでのログオンを許可するかどうか選択するオプションを追加しました。これはデフォルトで有効に設定されています。
- MDaemon Connectorのバージョンを7.5.0へアップデートしました。

- デフォルトの送信確認メッセージテキスト（¥MDaemon¥App¥Receipt.dat で定義）を、実際のメールアドレスがエイリアスのアドレスと競合するのを防ぐため、$RECIPIENT$マクロではなく$HEADER:X-RCPT-TO$マクロを使うよう変更しました。

MDaemonサーバーリリースノート

MDaemonの¥Docs¥サブフォルダにあるRelNotes.htmlで、MDaemon 21.5で追加された機能や変更点や修正点の全てをご覧頂けます。

MDaemon Private Cloud 9.0.0の新機能

- MDaemon Private Cloud 8.0にはMDaemon 21.0.2とMDaemon Connector 7.0.4が含まれています。

MDaemonの変更点全てを確認するには MDaemon 21.0.2 リリースノート.を参照して下さい。

MDaemon Connectorの変更点全てを確認するには MDaemon Connector 7.0.4 リリースノート.を参照して下さい。

MDaemon 21.0の新機能

主な新機能

継続チャットルーム342

MDaemonのXMPPサーバーは継続的なチャットルームに対応しました。これにより、全ユーザーがチャットルームから退出する度に、新しいチャットルームを再生成する必要がなくなります。設定は 設定 | Web & IMサービス | XMPPから行えます。

ウィルス/スパム誤判定レポート

MDaemon GUIの隔離、Bad、Spam Trapキュー画面で右クリックすると、ポップアップメニューから誤検知や検出漏れをMDaemon.com へレポートとして送信できるようになりました。関連したオプションがMDaemon Remote Administrationへも追加されました。メッセージは解析され、外部ベンダーへ正常な検出用に提出されます。

ActiveSyncマイグレーションクライアント（ASMC）GUI

稼働中のASMC（MDaemonの¥app¥フォルダにあるASMCUI.exe）の設定を行うための管理画面が追加されました。ここでは設定の保存と、読み込みが行えます。ASMCはメール、仕事、メモ、連絡先をプロトコルバージョン14.1に対応したActiveSyncサーバーから移行するための機能です。詳細はMDaemonのDocsフォルダの\MDaemon\Docs\ActiveSync Migration Client.htmlを参照してください。

Webmail Mobileテーマのアップデート

Webmailユーザー用のMobileテーマが大幅にアップデートしました。MDaemonの \Docs\ フォルダにあるRel Notes.html で追加した機能の全てをご確認頂けます。

クラスタリングのアップデート 373

MDaemonのクラスターサーバー機能を大きく改善しました:

- マルチノードメールルーティング 375 オプションを追加し、メールキューをクラスターノード間で共有できるようになりました。複数マシンのプロセスの所持とメール配信で処理は均等に分散され、ダウンしているマシンのキューへ留まる事がなくなります。
- SSL証明書がプライマリからセカンダリノードへレプリケーションされるようになりました。
- セカンダリノードのキューが、初回のデータレプリケーションの間は凍結されるようになり、起動時の処理が向上しました。
- MDaemonの停止処理が開始されるとクラスタ関連の終了処理が遅延しないよう、レプリケーションを一時停止するようにしました。
- クラスタリング - クラスタリングサービスを有効にした際、自動アップデートが無効になっている事を管理者へ通知するようになりました。
- ClusterノードがIPアドレスやDNS名を使って追加できるようになりました。
- 共有ネットワークパスが新しい共有ネットワークパス画面から簡単に管理できるようになりました。
- ロギングと分析ツールが、新しい「分析」画面で使用できるようになりました。

その他の新機能と変更点

Remote Administration (MDRA)

MDaemonのRemote Administrationの管理画面へ、多数のオプションを追加しました。MDaemonの \Docs\ フォルダにあるRel Notes.html で、MDRAへ追加した機能や変更点の全てをご確認頂けます。

コンテンツフィルタ

7-Zipで圧縮されたファイルの 禁止されたファイルの検索 599 が行えるようになりました。

自動応答 761

自動応答がUnicode (UTF-8)に対応し、全ての言語を利用できるようになりました。

IMAPフィルタ 670

IMAPフィルタリングルールでメール本文の特定の文字列を検索できるようになりました。

Webmail

- LookOutとWorldClientテーマの右クリックメニュー、モバイルテーマのイベントプレビューから新しいメールへイベントを追加する機能を追加しました。
- 全ての新規アカウント作成機能が削除されました。
- カレンダーのリンクを共有した公開が行えるようになりました。デフォルトカレンダー表示(例. 月/週/日)を設定するオプションを追加しました。

- ユーザー毎にIP継続チェックをスキップするオプションを追加しました。MDRAのユーザーアカウント編集から、ウェブサービスの「Webmailセッションの IP継続チェックをスキップ」オプションをチェックしてください。
- 詳細検索からCCフィールドの検索が行えるようになりました。
- 通常のカレンダーリンクに加え、空き状況カレンダーリンクを公開するためのオプションを追加しました。
- 表示されているクォータで一日に送信できる最大メール数 666 が表示されるようになりました。

ユーザーインターフェイス

- 設定 | モバイルデバイス管理が削除され、設定 | ActiveSyncのActiveSync管理へ変更されました。
- ActiveSyncクライアント設定画面が削除されました。チューニング、ドメイン、グループ、アカウント、クライアント画面でクライアント設定をカスタマイズできます。
- ActiveSyncクライアント種類の画面へ除外リストとブロックリストのクライアント種類に関するメニューコマンドを追加しました。
- 設定 | メッセージインデックスを追加し、Webmail、ActiveSync、Remote Administrationで使用される検索インデックスのリアルタイムと夜間メンテナンス中の設定が行えるようになりました。
- 診断画面を複数のプラグインで共有するようになりました。
- MDRAとWebmailのブラウザベースのヘルプシステムをレスポンシブテーマへアップデートし、異なるデバイスからも利用しやすくしました。

XML API

- XMLAPIドキュメントポータルの表示が全体又はドメイン単位でカスタマイズできるようになりました。 ヘルプポータル(例. http[s]://ServerName[:MDRAPort]/MdMgmtWS)の中の「Changes and development notes」かディスクの¥MDaemon¥Docs¥API¥XML API¥Help_Readme.xmlをInternet Expolorerで表示し、詳細な情報を確認できます。¥MDaemon¥Docs¥API¥XML API¥Samples¥Brandingへ、サンプルのcompany.mailディレクトリが用意されています。
- エイリアス管理を単純にするため、エイリアスのリゾルブとレポートの操作を追加しました。
- メール検索を行うのに、フォルダ操作検索を追加しました。
- クラスタサービスがQueryServiceStateとControlServiceStateに対応しました。

アーカイブ 116

- メールがローカルアカウント間で送信された際、「受信メールをアーカイブ」と「送信メールをアーカイブ」が有効になっていれば、「イン」と「アウト」両方のアーカイブコピーが生成されるようになりました。
- バージョン20.0で削除した、スパムメールをアーカイブするオプションが復活しました。
- Spam Trapから解放されたスパムメールがアーカイブされるようになりました。

コンポネントのアップデート

- MDaemon Connectorがバージョン7.0.0へアップデートされました。

- スパムフィルタ: SpamAssassin 3.4.4へアップデートし、local.cfの古い設定を削除しました。
- AntiVirus: ClamAVをバージョン0.103.0へアップデートし、Cyren AVエンジンをバージョン6.3.0.2へアップデートしました。
- XMPP Server: データベースバックエンドをSQLiteバージョン3.33.0へアップデートしました。

MDaemonサーバーリリースノート

MDaemonの¥Docs¥サブフォルダにあるRelNotes.htmlで、MDaemon 21で追加された機能や変更点や修正点の全てをご覧頂けます。

MDaemon Private Cloud 8.0.0の新機能

- MDaemon Private Cloud 8.0にはMDaemon 20.0.2とMDaemon Connector 6.5.2が含まれています。

MDaemonの変更点全てを確認するには MDaemon 20.0.2 リリースノート.を参照して下さい。

MDaemon Connectorの変更点全てを確認するには MDaemon Connector 6.5.2 リリースノート.を参照して下さい。

MDaemon 20.0の新機能

MDaemonクラスタサービス 373

MDaemonのクラスタサービスはネットワーク上の2台以上のMDaemon間での設定を共有するために設計されました。これによりMDaemonサーバー間でメール処理に対しハードウェアやソフトウェアのロードバランスが行えるようになり、ネットワークの負荷を減らすことによる速度向上や効率化が期待できます。また、1台でハードウェアやソフトウェアの障害が発生した際の冗長化としても役立ちます。MDaemonサーバークラスタの詳細情報や設定はクラスタサービス 373を参照してください。

新しいSMTP拡張

RequireTLS (RFC 8689) 538
IETFへのRequireTLSの取り組みがついに完了し、この機能へ正式対応しました。RequireTLSはメールの送信時TLSを必須とするようフラグ付けできるSMTP拡張です。TLSが不可能（またはTLS証明書の交換が不可能）の場合、メールは暗号化されずに送信するのではなく、エラーとして戻されます。RequireTLSはデフォルトで有効ですが、RequireTLSの処理対象となるメッセージは新しいコンテンツフィルタアクション 590である「REQUIRETLS…のフラグを追加」でコンテンツフィルタによるフラグ付けされたものか、<local-part>+requiretls@ domain.tld（例えば arvel+requiretls@ mdaemon.com）宛のメールだけです。他のメールは全て、サービスが無効であるかのように処理されます。メールをRequireTLSを使って送信するにはいくつかの条件があります。条件を満たせない場合メールは送られずにエラーとして戻されます。要件の詳細やRequireTLSの設定については、SMTP拡張 538を参照してください。RequireTLSの詳細な説明は: RFC 8689: SMTP Require TLS Optionを参照してください。

SMTP MTA-STS (RFC 8461) - Strict Transport Security 539
IETFへのMTA-STSの取り組みがついに完了し、この機能へ正式対応しました。SMTP MTA Strict Transport Security（MTA-STS）は は、メールサービスプロバイダー（SPs）側でメールを受信するにあたり、セキュアなSMTP接続が行えるトランスポート層レベルのセキュリティTransport Layer Security（TLS）に対応していることを宣言し、信頼のできるサーバ証明書を使用していない場合にメール送信側でメールを送信するかしないかを指定できる仕組みです。MTA-STSはデフォルトで有効化されています。設定についての詳細は、SMTP拡張 538を参照してください。MTA-STSの詳細な説明はRFC 8461: SMTP MTA Strict Transport Security (MTA-STS)を参照してください。

SMTP TLS Reporting (RFC 8460) 539
TLS Reportingは、MTA-STSポリシーの取得やSTARTTLSを使ったセキュアな接続のネゴシエーションに失敗した通知を、MTA-STSを使用するドメインに行ないます。有効にすると、MDaemonは各MTA-STSを使用するドメインへその日の送信した（もしくは送信を試みた）メールのレポートを日次で送ります。レポートに含む情報について、設定できる幾つかのオプションがあります。TLS Reportingはデフォルトで無効に設定されており、RFC 8460: SMTP TLS Reportingで議論されています。

1つのキーによるドメイン/企業レベルのMDPGP暗号化

MDPGP 574 で1つの暗号化キーを使ってドメイン間の全てのユーザーメールを暗号化できるようになりました。例えば「Domain-a」と「Domain-b」の間でやり取りする全てのメールを暗号化するのに、全ユーザーアカウント向けのキーの設定は行いたくない場合などに使用できます。これは今後次のように実現できます：

「Domain-a」と「Domain-b」はそれぞれ任意の方法で生成した公開鍵を提供します。例えば、互いに既存の公開鍵をMGPGP UI内で右クリックし、「メールのエクスポートとメール送信」をクリックします。この暗号化のために、専用の鍵を生成する場合は「特定のユーザー向けに鍵を生成」ボタンを押し、「_Domain Key（domain.tld）_ <anybody@domain.tld>」を（実際にはどの鍵も使用できますが）専用の鍵として選択します。双方の鍵を交換した後は、MDPGP UIで「ドメインの鍵をインポート」をクリックし鍵を使って暗号化するドメイン名を入力します。

一方が既に公開鍵を持っていて、キーリングへ存在する場合は、MDPGP UIで右クリックし「ドメインの鍵として設定」をクリックします。ただし、関連する秘密鍵は使用しないで下さい。これを行ってしまうと、MDPGPはメールを暗号化すると同時に復元用のキーを使って同じメールを復元してしまいます。

この時点でMDPGPは「<domain>宛の全てのメールを暗号化」というコンテンツフィルタルールを生成し、対象ドメイン宛の全てのメールが暗号化されます。このコンテンツフィルタを使用する事でコンテンツフィルタルールの有効化や無効化で暗号化処理をコントロールできるようになります。また、暗号化を行う前に、ルールを調整する事もできます。（例えば、2つのドメイン内に存在する特定のユーザーを対象にする、など）コンテンツフィルタはこれを実現するための柔軟性を提供してくれます。

宛先IPを元に送信メールを暗号化

MDPGP 574 へ特定のIPアドレス宛てのメール全てを、特定の鍵で暗号化するための新しいオプションを追加しました。ここで指定されたIP宛の外部SMTPセッションは対応する鍵を使って全てのメールを暗号化します。メールが既に暗号化されていた場合はこの処理はスキップされます。この機能は例えば特定のパートナーや業者とのメール全てを暗号化したい、といった場合に便利です。

メーリングリスト用のマクロ

メーリングリスト エディタ » ルーティング 269 メーリングリスト宛のメール本文でマクロの使用を許可するための新しいオプションが追加されました。メーリングリスト宛のメール本文でマクロが使用できるようになりま

した。これにより(例えば)それぞれのメーリングリスト用メールを個人用に設定する事ができるようになりました。マクロは従来もメーリングリスト用のメールヘッダやフッタでは利用できていましたが、メール本文では使用できませんでした。このマクロが個別のメーリングリストメンバーに関連している事から、このオプションは「リストメールを個々の宛先メンバーへ配信する」オプションが有効化されているメーリングリストでのみ使用できます。セキュリティの目的で、メーリングリスト用のパスワードを入力しないとマクロが展開されないようにするチェックボックスも追加されました。パスワードを使用しない場合には、書き込み権限を持つ全てのメンバーがマクロを使用できます。詳細についてはメーリングリスト ルーティング 269を参照してください。

ハイジャック検出機能の向上

ハイジャック検出 516 で盗まれたパスワードを使ってアカウントがスパム送信してしまうのを防ぐためのオプションが追加されました。スパムメールの一般的な特徴として、不正な宛先に短時間で大量のメールを送信しようとする、というものがあります。これはスパム送信者が古いメールアドレスや考えられる新しいメールアドレスの全てに対しメール配信を試みるためです。このため、MDaemonアカウントが不正な宛先へ大量のメールを送信した場合、アカウントがスパム送信のためにハイジャックされている可能性があります。これを防ぐため、MDaemonは認証ユーザーが配信に失敗した回数を監視し、必要に応じてアカウントを凍結できるようになりました。凍結されたアカウントはpostmasterへ通知され、この通知メールを使ってアカウントの凍結解除を行う事ができます。注意点:この機能の搭載過程で、Fromヘッダ編集オプションはFromヘッダスクリーニング 522へと移動させ、ハイジャック検出の新しいオプションを追加しました。

保留メールキューとメッセージリコールのアップデート 109

MDaemonに保留メール専用のキューが新しく追加されました。メールはメッセージリコールとDeferred-Deliveryヘッダ対応の一部として保留される事になります。従来、インバウンドキューを保留メールにも使用していた事で、保留されていないメールの配信を行うためのシステムに遅延が生じていました。今後はツールウィンドウの中でDeferredキューを確認することができ、キューのルートタブ内の保留用のサブタブでDeferredキューの内容の詳細を確認できます。Deferredキューに配置されたメールは日付毎に並べられエンコードされたファイル名が使用されます。MDaemonは一分おきにDeferredキューを確認し、通常配信が可能なメールをインバウンドキューへ、通常処理を行えるよう移動します。

MDaemonは認証されたローカルユーザーから送信された最近のメールのMessage-IDを記録するようになりました。これによりRECALLを件名とし、mdaemon@ のシステムアカウントへメールを送るだけで、最後に送信したメールをユーザーがリコールできるようになりました。(ただし、最後に送信したメールのみが対象です) 最後に送信したメールをリコールする場合は、対象メールを探してMessge-IDをコピーする手間は不要です。最後のメール以外をリコールする場合には従来通り件名へMessage-IDを入力し送信済アイテムにある元のメールを添付する必要があります。

認証ユーザーが最後に送信したメールを記憶しておく事に加え、MDaemonは全ての認証済ユーザーが送った最新の1000通のメールのMessage-IDを記憶します。これによりメールフォルダ内のコンテンツを把握する必要が生じ、パフォーマンスの低下を招く可能性があります。リコール対象であるメール総数だった1000通の値を増やす事ができるようになりました。リコールは送信メールが直近の1000通(又は指定した値)より古い場合には失敗します。この機能でユーザーが送信済のメールであってもリコールできるようになります。メールはリコールされると、ユーザーのメールクライアントや電話から削除されます。注意点:これはもちろん対象メールがローカルユーザー宛の場合に限ります。一度MDaemonが別サーバーへ配信したメールについては、MDaemonの管理下にはないため、リコールする事はできません。

認証失敗ログ

「認証失敗」の、新しいログファイルが追加され、SMTP、IMAP、POPログインに失敗した場合、その詳細が記録されるようになりました。情報には、仕様したプロトコル、セッションIDが含まれ、この情報を元

に、他のログファイルを検索し、IPや、ログオンに使用されたアカウント（適合するアカウントがない場合は「none」と表示されます）が確認できます。

転送/ルーティングメールの認証

複数の場所で、転送メールに対して認証を追加できるようになりました。つまり、APPフォルダ内のforward.dat、MDaemon.ini, メーリングリストの.grpファイルといった複数のファイルでログオン情報を追加できるようになりました。暗号化は一時的な処置としては充分強力ではありますが、ハッカーから守るのに充分な強度とは言えません。常に警告している通り、OSのツールや他の方法でMDaemon端末とディレクトリ構成を、不正アクセスから保護しておいてください。 認証オプションは次の画面へ追加されました: 不明なメール[92], メーリングリスト ルーティング[269], ゲート ウェイエディタ ≫ 転送[238], ゲート ウェイエディタ ≫ デキュー[240], アカウント エディタ ≫ 転送[663]

ホスト認証[112]

ホスト認証用の新しい画面が追加され、全てのホストで使用するポート、ログオン、パスワードを設定できるようになりました。MDaemonがSMTPメールを対象ホストへ送信する際、ここで指定した認証情報が使用されます。指定する認証情報を使用は代替案であり、他の認証情報が使用できない場合にのみ使われる点に注意してください。例えば、アカウント エディタ ≫ 転送[663] や ゲート ウェイマネージャ ≫ デキュー[240] 等でログオンとパスワードを使用した場合、 そちらの設定が優先されます。この機能は（IPではなく）ホスト名でのみ有効です。

カスタムキューとメールルーティング機能のアップデート[798]

ホスト、ログオン、パスワード、SMTP return-path、ポートを全てのリモートキューで指定できるようになりました。指定された場合、キュー内の全てのメールは新しい設定値を使って配信されます。ただし、環境によっては個々のメールが既に独自の配送用データを保持している場合があり、このデータの優先度によっては、メニュー内で指定したデータよりも優先されます。また、作成したいリモートキューの無制限な作成、キュー毎にコンテンツフィルタルールの定義と適用、キュー毎の配信スケジュール、完全に異なるルーティングの実行が行えるようになりました。

ドメイン共有のアップデート[103]

ドメイン共有では必要に応じてSMTP MAIL送信者のルックアップを実行してきましたが、メールは「認証が必要です」というエラーで拒否される事が多くあり、異なるサーバーにおいては送信者認証が実行できないでいました。 この点についてMDaemonは他のサーバーに存在するアカウントを認証なしで受け付ける事ができるようになりました。送信者認証 ≫ SMTP認証[476]でこの設定を無効にできます。現在SMTP MAIL送信者に対しドメイン共有でのルックアップを全く行っていない場合には、ドメイン共有オプションで、 デフォルトで有効化されている設定値を、完全に無効化する事もできます。

メーリングリストでもドメイン共有が使用できるようになりました。 メールがメーリングリスト宛に届くと、ドメイン共有のホスト分のコピーが生成され、リストのバージョンも保持されるようになります。ホストでコピーを受け取ると、全メンバーに対して対象のメールを配信します。この方法で、メールはその機能性を損なう事なく複数サーバーに跨るメーリングリストメンバーへメールを配信できるようになります。 この機能を利用するには、ドメイン共有のホストが、信頼するIP[473] へ、他のホストを指定する必要があります。

最後に、ドメイン共有へ詳細ボタンが追加され、ドメイン共有の利用を許可するドメイン名を指定するファイルを開く事ができるようになりました。（デフォルトの状態で）何もファイル内にない場合は全てのドメインがドメイン共有を利用できます。ファイルの上部にある説明を参照してください。

転送メールのコントロール機能のアップデート

初期設定 ≫ その他[459] へ新しいチェックボックスが追加され、管理者が外部のドメインからのメール転送を防ぐ事ができるようになりました。 ユーザーがアカウントで外部ドメインへのメール転送を設定する

と、転送メールはBadキューへ移動します。この設定はアカウントの メール転送オプションを使った転送メールに対してのみ適用されます。

アカウント エディタ ≫ 転送 663 へ新たに「スケジュール」ボタンが追加され、アカウントのメール転送の開始時間と終了時間を指定できるようになりました。また、この設定はアカウント テンプレート 736 にも追加されました。この設定では転送の開始日時と停止日時を指定できますが、転送されるのは指定した曜日のみとなります。

新規アカウント テンプレート 722 の転送アドレスのフィールドがアカウント用マクロで動作するようになりました。新規アカウントの作成時のみこのマクロは機能しますが、今後は関連するアカウントの姓名、ドメイン、メールボックス、パスワードの値でも使用できるようになります。このため、(例えば)アカウントの転送を同じユーザー名で異なるドメインに対して行いたい場合は、これを転送アドレスフィールドへ次のように指定できます: `$MAILBOX$@example.com` マクロはまた、差出人の指定, AUTH ログオン, AUTHパスワードのフィールド(新しいフィールドです)でも使用できます。

メール転送で転送アカウントの最後のアクセス日時を更新するようになりました。これによりアカウントがメール転送を行った場合は何の操作もなかったアカウントとして自動削除されなくなります。転送は実際に行われている必要があり、他の設定による制限を受けて動作していなかった場合は除く点に注意してください。転送アドレスを指定しただけでアカウントがアクティブになるわけではなく、実際に転送が行われている必要があります。

SMTP認証のアップデート

送信者認証 ≫ SMTP認証 476 へ2つの新しいオプションが追加されました。「SMTPポートでの認証を許可しない」は完全にSMTPポートでのAUTH対応を無効化します。AUTHはEHLOレスポンスでも提供されず、SMTPクライアントがコマンドを送っても、不明なコマンドとして処理されます。また、AUTHは「認証を試みたIPをダイナミックスクリーンへ追加」で、AUTHが無効化されていた場合にAUTHを実行しようとしたクライアントのIPアドレスをダイナミックスクリーン 571 へ追加するようになりました。接続はすぐに終了します。正規なアカウントが認証済メールの配信にMSAポートを使っている場合には非常に便利な設定です。このような設定の場合、SMTPポートを使って認証を行ってくるIPアドレスは攻撃しようとしているIPといえるからです。

アカウント管理のアップデート

アカウント マネージャをアップデートしました。有効なアカウント、MultiPOPを使用しているアカウント、クオータに近い(70%)のアカウント、クオータに近い(90%)のアカウント、転送していないアカウントを選択できるようになりました。また、アカウントの説明フィールドを検索し、その検索結果を元に任意のアカウントを選択できるようになりました。アカウント マネージャの右クリックメニューへ選択したアカウントをメーリングリストやグループから削除できるようになりました。新しいアカウント作成に、既存のアカウントをコピーできるようになりました。既存のアカウントは、フルネーム、メールボックス、パスワード、メールフォルダ設定を除いて、全て新しいアカウントにコピーされます。最後に、アカウント エディタの IMAPフィルタ 670 へ「公開」という新しいボタンを追加し、新しいルールを編集中のアカウントへ追加したり、ドメイン内の他のアカウント全てに追加できるようになりました。これはルールが全員に必要な場合に便利にお使い頂けます。

ドメイン全体用の終業時間設定 167

ドメインマネージャの ホスト名とIP 167 へ新しいオプションを追加し、終業時間設定をドメイン全体で有効化できるようにしました。アクティブにすると、ドメインは全てのユーザーからの接続を拒否しますが、外部からのメールは受け付けます。「終業時間」の開始と終了はスケジュールする事ができます。例えば2020年の5月1日から2020の6月30日を指定し、5:00pmから7:00am、月曜から土曜と指定した場合、メールサービスは対象の期間の指定の曜日、5:00pm以降はメールの受信が行えず、7:01amから再度行えるようになります。スケジュールの開始と終了日を削除すると予定は無効化され、ドメインが永久に「終業時間」という扱いになります。

アーカイブのアップデート 116

MDaemonのシンプルメールアーカイブシステムがより効果的で安定するシステムへアップデートしました。アーカイブは次のように機能するようになりました: メールがローカルキューからユーザーメールフォルダへ配信される際、アーカイブ用のコピーが生成されます(宛先の受信フォルダへ保存されます)。メールがリモートキューで処理対象となった際(送信が成功したかどうかにかかわらず)アーカイブ用のコピーが生成されます(送信者の送信フォルダへ保存されます)。ローカル・リモートキューが処理される度、ルーティングログへは "ARCHIVE message: pgp5001000000172.msg"といった行や、"ARCHIVE message: pgp5001000000172.msg"といった行が追加されます。「ToArchive」というキューがシステムキューとして追加されます(UIでは確認できません。)このキューは定期的に確認され、(手動、プラグイン、またはその他の方法で)削除されます。 確認されたメールでアーカイブ対象でないものはすぐに削除されます。キューの名前は、 ¥MDaemon¥queue¥ToArchive¥となります。ルーティング画面/ログはメールがアーカイブに成功したかどうかと、その詳細が確認できます。 暗号化されたメールのアーカイブはより確実に行われるようになりました。デフォルトで暗号化メールの暗号化されていないコピーはアーカイブ対象として保持されていました。メールが復元できない場合は、暗号化されたメールが今後はアーカイブされます。また、パブリック投稿アドレス宛てのメールをアーカイブするオプションが追加されました。最後に、次の種類のメールはアーカイブされません: メーリングリスト通信、スパム、ウィルス付きメール、システム生成メール、自動応答メール。

より効果的なロギング 159

MDaemonでは空のログファイルを生成する事はなくなりました。設定画面でこのアイテムが無効化されていた場合、これに関連したログファイルが起動時に生成される事はありません。既にファイルが存在している場合で対象アイテムが無効の場合は元の場所に残ります(削除されません)。存在していないログファイルに関連したアイテムが有効化された場合、対象のファイルが生成されます。この変更はMDaemonのコアエンジンが管理する全てのログファイルへ適用されます。ダイナミックスクリーニング, インスタントメッセージ, XMPP, WDaemon, WebMail のログはMDaemonとは別に稼働しておりアップデートの対象ではありません。他のログ関連の変更には次のようなものがあります: ATRNセッションログの精度向上、全てのログの色分け表示、セッションとChild ID、MultiPOPサーバーのログがセッション内で分かれて記録されてしまう点を改善し、無駄なログを記録しないよう改善しました。RouterログでINBOUNDとLOCALキューメール処理のみを記録するようになりました。REMOTEキューの処理は、配信が行われた際ログへ記録するようになりました。これにより、RouterログとSMTP(out)ログの両方をメールが処理された際検索する必要がなくなります。

ACTIVE DIRECTORY連携のアップデート

Active Direcotry グループへユーザーを追加するとMDaemonへ追加し、グループからユーザーを削除した場合は、MDaemon上で対象アカウントを(削除ではなく)無効化できるようになりました。この機能を使用するには、Active Directoryの検索フィルタを正しく設定しておく必要があります。詳細は、Active Directory ≫ 認証 749を参照してください。

Active Directoryの 認証 749 へ、独立した「連絡先検索フィルタ」オプションを追加しました。連絡先検索用に個別の(異なる)検索フィルタを指定できるようになりました。従来、連絡先検索はユーザー検索フィルタを使ってテストボタンで動作が確認できるようになっていました。AD検索は最適化され、検索フィルタが同一だと判断した場合には単一のクエリで全データを更新できます。フィルタが異なる場合は2つのクエリがそれぞれ必要となります。

次のフィールドがActiveDS.datファイルテンプレートへ追加され、Active Directoryモニタリングで連絡先を作成したり更新したりした際、連絡先レコードへ含まれるようになりました: `abTitle=%personalTitle%`, `abMiddleName=%middleName%`, `abSuffix=%generationQualifier%`, `abBusPager=%pager%`, `abBusIPPhone=%ipPhone%`, `abBusFax=%FacsimileTelephoneNumber%`.

Active Directoryからアカウントが削除された際、対応する連絡先がパブリックフォルダ連絡先からも削除されるようになりました。 連絡先が削除されるのは、対象の連絡先がActive Directory連携機能で作成された場合のみです。この設定はActive Directoryモニタリング[752]で調整することができます。

Active Directoryモニタリングシステムがアカウントの作成や更新を行った際、メールボックス値がMDaemonの制限されたメールボックス値に対して長すぎると分かった場合、メールボックスの値は従来通り省略されますが、同時にフルサイズのメールボックス値でエイリアスを生成するようになりました。また、アカウントやエイリアスが生成された際、監視の目的で、管理者権限の割り当て[690]のメモが更新されます。

メーリングリストマネージャのActive Directory[274]ではメーリングリストメンバーのフルネーム用にActive Directory属性を入力できるようになりました。

Active Directoryでアカウントプロパティを変更した際、アカウントが以前MDaemonで削除されていたものでも、MDaemonで再生成できるようになりました。アカウントをこのように再生成するため、新しいオプションが、Active Directoryモニタリング[752]へ追加されました。デフォルトで、MDaemonで手動で削除したアカウントは再生成されません。

FROMヘッダスクリーニング のアップデート[522]

'Fromヘッダ変換'が、ハイジャック検出画面から、個別のFromヘッダスクリーニング[522]となり、新しい機能がいくつか追加されました。 例えば、Fromヘッダスクリーニングで、表示名の中からメールアドレスに見える「From」ヘッダをチェックできるようになりました。もしも表示名のメールアドレスが実際のアドレスと異なる場合は実際のメールアドレスへ書き換えられます。例えば、From: ヘッダがFrom: "Frank Thomas <friend@ friend.com>" で<enemy@ enemy.com>が実際のアドレスの場合、次のように変換されます: From: "Frank Thomas <enemy@ enemy.com>"

脆弱なパスワードの確認[778]

MDaemonはサードパーティーサービスが提供する脆弱なパスワード一覧を使ってユーザーパスワードチェックを行う事ができます。この確認はパスワードをサービスへ配信する事なく行う事ができ、ユーザーのパスワードが一覧に存在していた場合であっても、パスワードがハッキングされたという事ではありません。これは、どこかの誰かが同じ文字列をパスワードに使用していた事があり、悪用された事がある事を示唆しています。公開されているパスワードは辞書攻撃でハッカーが使用している場合もあり、使用された事のないパスワードの利用はより安全です。Pwned Passwordsにて詳細をご覧頂けます。

セキュリティ設定のパスワード[778]では、MDaemonが脆弱なパスワード一覧と同じ文字列の使用を禁止するためのオプションが追加されました。 ログインの度に定期的にパスワードチェックを行い、警告メールをユーザーとpostmasterへ送信する設定も行えるようになりました。警告メールは¥MDaemon¥Appフォルダのテンプレートファイルを編集する事でカスタマイズできます。MDaemonへ保持しているか、ActiveDirectory認証を使っているかにより、パスワード変更方法の手順は異なるため、テンプレートファイルはCompromisedPasswordMD.datとCompromisedPasswordAD.datの2つが用意されています。 マクロはメールの個別設定や件名、あて先の変更などに使用する事ができます。

追加の機能と変更点

MDaemon 23には250を超える新機能や変更点があり、ここへ記載されていないものも数多く存在します。MDaemonの¥Docs¥サブフォルダにあるRelNotes.htmlで全ての新機能や変更点、修正点をご確認頂けます。

MDaemon Private Cloud 7.5.0の新機能

- MDaemon Private Cloud 7.5にはMDaemon 19.5.3とMDaemon Connector 6.5.1が含まれています。

MDaemonの変更点全てを確認するには MDaemon 19.5.3 Release Notes.を参照して下さい。

MDaemon Connectorの変更点全てを確認するには MDaemon Connector 6.5.1 Release Notes.を参照して下さい。

MDaemon 19.5の新機能

新しいWebmailモバイルテーマ

モバイルテーマが、従来よりも流行りのGUIとなり、新機能が搭載されたものへとアップデートされました。メール一覧機能には個別のカテゴリ設定が行えるようになった他、メールのスヌーズ、フラグ付き/未読/スヌーズ済メールでのソート、カラムのソート、メッセージリコールが行えるようになりました。予定表機能には予定をcsvやicsファイルとでインポート・エクスポートできる機能が新たに追加され、外部の予定表を追加したり、プライベート用のアクセスリンク設定、公開、同時に複数予定表の閲覧が行えるようになりました。編集機能には配信遅延、複数署名、text/htmlメール、メール雛形の機能が搭載されました。他にも、メールフィルターのドラッグ＆ドロップ、複数署名用エディタ、フォルダ管理オプション、通知、カラムのドラッグ＆ドロップ、カテゴリのドラッグ＆ドロップ管理、その他の機能が搭載されました。WebmailをIIS上で稼働している場合、追加の設定が必要です。詳細については、Knowledge Base article 1236を参照してください。

クライアント署名の管理 125

署名をWebmailとMDaemon Connectorへプッシュ配信する機能を追加しました。デフォルトクライアント署名 125 をドメイン毎に作成したり、ドメインマネージャのクライアント署名 188 より作成を許可できるようになりました。 $CONTACTFULLNAME$, $CONTACTEMAILADDRESS$ といった署名マクロ 126 で、ドメインのパブリック連絡先フォルダのユーザー別情報から引用したデータで、署名の個別設定を行ってください。$ATTACH_INLINE:filename$ マクロを使用し、HTML署名へインライン画像を使う事もできます。署名用のテキストを入力すると、Webmailでは「システム」署名として表示され、ユーザーのデフォルト署名となります。これは Webmail設定 316 又はドメイン毎であれば ドメインマネージャ 176 から有効化や無効化が行えます。MDaemon Connector用に、署名や関連設定が MCクライアント設定の署名 371 より行えるようになりました。この機能にはMDaemon Connector 6.5.0かそれ以降が必要です。

カテゴリページ 315

MDaemonのRemote Administration（MDRA）内のWebmailオプションへ カテゴリ 315 ページを追加しました。ここではドメインカテゴリやデフォルトの個人カテゴリの管理が行えます。

追加のMDRAの新機能

従来MDaemonのアプリケーションで行えていた設定の多くをMDRAでも行えるよう追加しました。全ての機能についてはリリースノートを参照してください。

追加の機能と変更点

MDaemon 23.0 には他にも多くの新機能や変更点があります。MDaemonの¥Docs¥サブフォルダにあるRelNotes.htmlで全ての新機能や変更点、修正点をご確認頂けます。

MDaemon Private Cloud 7.0の新機能

- MDaemon Private Cloud 7.0にはMDaemon 19.0.2とMDaemon Connector 6.0.1が含まれています。

MDaemonの変更点全てを確認するには MDaemon 19.0.2リリースノートを参照して下さい。

MDaemon Connectorの変更点全てを確認するには MDaemon Connector 6.0.1 リリースノートを参照して下さい。

MDaemon 19.0の新機能

TLS Server Name Indication（SNI）に対応 525

MDaemonがTLSプロトコルのServer Name Indication（SNI）へ対応し、サーバのホスト名毎にそれぞれの異なる証明書を使用きるようになりました。MDaemonは、有効な証明書を参照し、SubjectAlternative Names（サーバ別名）フィールド内から要求されたホスト名を持つ証明書を選択し使用します。クライアントがホスト名を指定しなかったり、一致する証明書が無かった場合には、デフォルトの証明書を使用します。

XML-API によるフォルダ、アイテム管理

XML-APIを拡張して、メールボックスフォルダやフォルダ内のメールアイテムの管理が行えるようになりました。フォルダに関しては、APIからのフォルダの作成、削除、名前変更、移動を行うことができます。アイテムに関しては、メール,予定表,連絡先,仕事,メモが対象で、APIから作成、削除、移動を行うことができます。MDaemon¥Docs¥API¥XML-API ディレクトリーに、ドキュメントがありますのでご参照下さい。

Remote Administrationのアップデート

MDaemonの Remote Administration（MDRA）のウェブインターフェイスが更にアップデートし、従来MDaemonの管理画面でのみ行えた多くの設定がMDRAからも行えるようになった他、MDRAからのみ行えるオプションも追加されました。新規インストールを行った際、スタートメニューにある"MDaemonを開始"ショートカットから、これまでのMDaemon管理画面ではなく、MDaemon Remote Administrationを開くブラウザが起動するようになりました。このデフォルトの動作を変更するには、¥MDaemon¥App¥MDaemon.iniファイル内の［MDLaunch］セクション内のパラメータ、OpenConfigSession=Yes/No と OpenRemoteAdmin=Yes/No にてご調整頂くか、スタートメニューの"MDaemon"から"MDaemon Configuration Sessionを開く"もしくは"MDaemon Remote Administrationを開く"を選んでご選択ください。もし、自動生成されたURLで起動できない場合や、外部Webサーバを使ってRemote Administrationをご使用の場合、管理画面から 設定≫WebとIMサービス≫Remote Administration ≫Webサーバ 322から、"Remote Administration URL"の設定を行なって下さい。最後に、Windowsのスタートメニューの MDaemonプログラムグループへ、MDaemon管理画面を起動とMDaemon Remote Administrationを起動が追加されました。

Webmailのアップデート

- Webmailにおいて、(Webmailのオプション >> フォルダにある)"保存済み検索条件"へ"全ての未読メール"と"全てのフラグ付きメール"を追加できるオプションを追加しました。初回ログイン時のみ、ユーザーには"保存済み検索条件"へ追加するかを確認する画面が表示されます。もし、"いいえ"を選択しても、後でオプション | フォルダの画面で追加することもできます。管理者は MDaemon\WorldClient\Domains.ini の[Default:UserDefaults] へ DefaultSavedSearchesCheck=Yesを追加する事で、ユーザーへの確認を行わないようにする事もできます。
- *WorldClient* テーマのアイコンを見やすく作り変えました。
- セッションが期限切れになった際、ブラウザのタブタイトルへ"(EXPIRED)"と表示されるようにし、ユーザーがセッションの期限が切れている事を確認しやすくしました。
- 自動保管リストから連絡先を削除するための削除アイコンを追加しました。

MDaemon Private Cloud 6.5の新機能

- MDaemon Private Cloud 6.5にはMDaemon 18.5.1とOutlook Connector 5.6.0が含まれています。

MDaemonの変更点全てを確認するにはMDaemon 18.5.1のリリースノートを参照して下さい。

MDaemon Connectorの変更点全てを確認するには MDaemon Connector 5.6.0のリリースノート を参照して下さい。

MDaemon 18.5の新機能

署名マクロ

MDaemonの署名にて、ドメイン内のパブリックフォルダにある連絡先フォルダから、送信者の連絡先情報を差し込めるマクロを使用できるようになりました。これにより、デフォルト署名もしくはドメイン署名を送信者情報を使って設定できるようになりました。例えば、送信者の名前には、$CONTACTFULLNAME$を使い、送信者メールアドレスには、$CONTACTEMAILADDRESS$ と指定することができます。パブリックフォルダ内の情報はWebmail, MDaemon Connector, そしてActiveSyncから編集でき、送信者に関する連絡先が無い場合にはブランクになります。使用できるマクロのすべてのリストを参照するにはデフォルト署名ページをご参照下さい。

MDaemon署名をどこへ配置するかについては、送信者が$SYSTEMSIGNATURE$ を用いてメッセージの下部以外にも指定することができます。アカウントの署名を使用するには、$ACCOUNTSIGNATURE$ を指定します。

Webmail内で使用できるMDaemon Instant Messaging

WorldClientとLookOutテーマにおいて、ブラウザベースのXMPPクライアント機能が搭載されました。これにより、ユーザーは MDaemon Instant Messengerデスクトップアプリケーションや XMPPクライアントをインストールすることなく、インスタントメッセージをご使用頂けます。ユーザーは、Webmailの オプション | 初期設定 画面にある、"ブラウザ上で、MDaemon's Instant Messager機能を有効にする"でインスタントメッセージを有効化できます。管理者は、インスタントメッセージ機能を、ドメインマネージャからドメ

イン毎に、アカウントエディタから個人毎に、グループマネージャからグループ毎に、使用できる/できないを設定できます。

MDaemonへ新しくBOSHサーバーが搭載され、Webmailでのインスタントメッセージの利用に対応しました。この設定はXMPP画面 340より行う事ができます。(18.5.1の新機能)

Webmailを国別スクリーニングから除外

Webmailにて、2段階認証を行っているユーザーを国別スクリーニングから除外するユーザーオプションを追加しました。User.iniファイルの[User] セクションでBypassLocationScreeningTFA=Yesを設定されているユーザーで、2段階認証を有効化されているユーザーは、ロケーションスクリーニングが除外されます。これによりユーザーは国別スクリーニングでブロックされている国からもWebmailへ接続する事ができるようになります。

AD連携機能を強化

ActiveDirectory連携を行なっているユーザーが、Webmailからパスワードを変更すると、ActiveDirectory上のパスワードも変更できるようになりました。この機能を使用するには、¥MDaemon¥WorldClient¥Domains.iniファイル内の "AllowADPasswordChange"パラメータを有効にして下さい。デフォルトは、無効化されています。

MDRAの拡張

MDaemonのRemote Administration (MDRA) ウェブインターフェイスをアップデートし、従来MDaemonの管理画面でのみ行えた多くの設定がMDRAからも行えるようになりました。

MDaemon Private Cloud 6.0の新機能

- MDaemon Private Cloud 6.0にはMDaemon 18.0.2とOutlook Connector 5.5.2が含まれています。

MDaemonの変更点全てを確認するにはMDaemon 18.0.2のリリースノートを参照して下さい。

MDaemon Connectorの変更点全てを確認するにはMDaemon Connector 5.5.2のリリースノートを参照して下さい。

MDaemon 18.0の新機能

DNSSEC 540

新しいDNSSECEC (DNS Security Extensions)オプションで、MDaemonがRFCの 4033 と4035 にて「DNSクエリの送信やDNS応答の受信、スタブリゾルバのサービスを提供できるDNSSEC対応ネームサーバーとの安全な通信の確立を行うエンティティ」と定義された、署名を検証しないDNSSEC対応スタブリゾルバとして動作できるようになります。 これはMDaemonがDNSへの問合せを行う際DNSSECサービスをDNSサーバーへ要求し、AD (Authentic Data)ビットを使った問合せを行い、応答を確認できるようになるという事です。DNSSECは現在全てのDNSサーバーが全てのトップレベルドメイン向けに対応しているものではありませんが、これによりDNS処理中に追加レベルのセキュリティを実装する事ができるようになります。

有効化すると、DNSSECサービスは選択条件にマッチしたメールに対してのみ適用されます。DNSSECサービスはメール毎に「要求」したり「必須」としたりできます。DNSSEC画面で「ヘッダ値」の組み合わせを選択するだけで、MDaemonはDNSの問合せの際条件にマッチしたメールにのみDNSSECサービスを要求します。「必須」としている場合で認証データを含むDNSの応答に失敗すると、メールは送信者へ返されます。「要求」している場合はDNSSECサービスで失敗した場合でも何も起こりません。ただし、特定のメールに対してDNSSECを必須とする場合は、ヘッダ値の組み合わせへ「SECURE」を追加してください。(例. `To *@example.net SECURE`)これらのメッセージで認証データを含むDNSの応答に失敗すると、メールは送信者へ返されます。**注意点**: DNSSECルックアップには従来よりも時間やリソースが必要となり、また、DNSSECは全てのサーバーで対応しているわけではないため、MDaemonは全てのメール配信へDNSSECを適用するデフォルト設定にはなっていません。ただし、必要に応じ、設定ファイルの中に「To *」などの行を一行追加する事で、全ての送信メールでDNSSECの利用を必須とする事ができます。

AntiVirusメールボックススキャン

セキュリティ ≫ AntiVirus[609]へ全てのメッセージをn日毎にスキャンする新しいオプションが追加され、保存されているメールを定期的にスキャンし、ウィルス定義ファイルがアップデートされる前に通過した感染メールを検出する事ができるようになりました。感染メールは隔離フォルダへ移動され、X-MDBadQueue-Reasonヘッダが追加され、MDaemon上で隔離された理由を確認できるようになります。スキャンできないメッセージは隔離されません。また、メールボックススキャンオプションの設定ではどの頻度でメッセージをスキャンするのかや何日前のメールまでをスキャン対象とするのかを指定する事ができます。また、ここからメールボックススキャンを手動ですぐに実行する事もできます。

既知のActiveSync端末を国別スクリーニングから除外

ActiveSyncクライアント設定画面に追加された、新しい国別スクリーニングから除外[422]オプションを使うと、国別スクリーニング[520]から端末を除外する事ができるようになります。これにより、正規のユーザーは例えば認証がブロックされている場所へ旅行している場合でも、ActiveSync経由でのアクセスを継続できるようになります。端末を除外するためには、チューニング画面の中で指定したこの日数を超える非アクティブクライアントを削除[381]の範囲内で、ActiveSyncで接続と認証を行う必要があります。デバイスをスクリーニングの対象外とする方法として、接続しているリモートIPアドレスを除外リストへ追加する事もできます。これは同じIPアドレスを使って接続している他のクライアントも併せて許可する際に便利です。

WebmailとMDRAの新機能

認証情報を記憶

Webmail設定画面[316]とMDRAウェブサーバー画面[322]のオプションから、MDaemon WebmailとMDaemon Remote Administration (MDRA)のログインページへ「認証情報を記憶」のチェックボックスを追加できるようになりました。このオプションを有効化すると、httpsポートで接続したユーザーには、ログインページへチェックボックスが表示されるようになります。これをチェックすると、認証情報が端末へ保存されます。その後はWebmailやMDRAへ接続する際、ユーザーは手動でサインアウトするか認証情報の保存期間が終了するまで、自動ログインができるようになります。認証情報を記憶オプションはデフォルトで無効化されており、全てのドメインに適用されています。特定のWebmailドメイン用の設定を上書きするには、MDaemonの管理画面にあるドメインマネージャのWebmail画面[176]にて認証情報を記憶オプションを使用します。

デフォルトで、ユーザーが再ログインしなくてはならなくなるまでの有効期間は30日間で、(MDRAの中の)次の日数まで認証情報を記憶、のオプションで異なる日数を指定する事ができます。設定できる最大有効期間は365日間です。**注意点**:2段階認証[656](2FA)には¥MDaemon¥WorldClient¥内のDomains.iniの[Default:Settings]セクションへ、独自の認

証情報の記憶用キー(TwoFactorAuthRememberUserExpiration=30)を所持しています。そのため、認証情報を記憶する期間内であった場合にも、2FAのトークンの期限が切れた場合は従来通り認証を要求されます。

MDRAには、認証情報を初期化ボタンも追加され、アカウントがセキュリティ上の問題があると思った際に使用できるようになりました。これを使うと全てのユーザーの認証情報の記憶が初期化され、全てのユーザーは再度ログインが必要になります。

メールのスヌーズ

MDaemon Webmailで、ユーザーが一覧の中のメールをスヌーズできるようにしました。メールがスヌーズされると、指定した時間、メールを非表示にできます。メールをスヌーズ設定するには、対象のメールを右クリックし「次の時間スヌーズする」を選択します。日時の入力が行えるブラウザを使っている場合のみ、「日時を選択」オプションが表示されます。非表示になったメールはLookOutテーマであればツールバーのドロップダウンメニューから「スヌーズ状態のメールを表示」を選択する事で閲覧できます。この機能はデフォルトで有効です。これを無効にするにはオプション| 初期設定へ進み、受信設定の「メールのスヌーズを有効化」のチェックを外します。スヌーズ機能の操作はLiteやMobileテーマからは行えませんが、スヌーズ状態のメールはこれらのテーマでアクセスした場合でも非表示になります。

パブリックカレンダー

MDaemon Webmailユーザーがカレンダーをアクセス用リンク付きで公開できるようになりました。ユーザーはカレンダーをパスワードで保護するかどうかをオプションで指定できます。カレンダーを公開するには、LookOutかWorldClientテーマの場合は、オプション | フォルダで、公開したいカレンダーの隣に表示されている「フォルダ共有」ボタンをクリックします。 ダイアログの中でパブリックアクセスタブを開き、表示名とパスワードを要求するかどうかを選択し、「カレンダーを公開」ボタンをクリックします。その後の動作について確認用のダイアログが表示されます。 OKをクリックするとカレンダー用の新しいURLがアラートとして表示されます。カレンダーが公開されると、表示されている画面内へもリンクが表示されます。カレンダーを非公開にするには、「カレンダーを非公開」ボタンをクリックします。パスワードや表示名を変更する場合は、「更新」ボタンをクリックします。

この機能を全体で無効化するにはDomains.iniの中の [Default:Settings] EnablePublicCalendarsをNoへ変更してください。ユーザー毎にこれを無効化する場合は、各ユーザーのUser.iniファイルでCanPublishCalendars=Noを追加してください。ユーザー毎にこの機能を無効化するには、User.iniファイルの中へCanPublishCalendars=Noを追加してください。

MDaemon Private Cloud 5.5の新機能

- MDaemon Private Cloud 5.5にはMDaemon 17.5.2とOutlook Connector 5.0.1が含まれています。

MDaemonの変更点全てを確認するにはMDaemon 17.5のリリースノートを参照して下さい。

Outlook Connectorの変更点全てを確認するにはOutlook Connector 5.0.1のリリースノートを参照して下さい。

MDaemon 17.5の新機能

国別スクリーニング 520

場所を元にブロックするシステムを開発し、受信するSMTP, POP, IMAP, Webmail, ActiveSync, AutoDiscovery, XML API, Remote Administration, CalDAV/CardDAV, XMPP, Minger接続が承認していない地域からのものだった場合、これをブロックできるようになりました。SMTPについては、ロケーションスクリーニングでAUTHを使った接続のみをブロックする事もできます。これは、例えばユーザーは特定の国にいるわけではないもの、その場所からメールの送受信を行いたいユーザーがいる場合などに便利です。これを使った場合、サーバーへログインしようとした接続のみをブロックできます。

\MDaemon\Geo\ フォルダには、IPに関するマスターデータベースが格納されています。このファイルはMaxMind (www.maxmind.com)が提供しているものであり、必要に応じてそちらのサイトから最新版をダウンロードできます。

全プロトコル/サービス用ダイナミックスクリーニング 556

MDaemonのダイナミックスクリーニングを、SMTP, POP, IMAP, WorldClient, ActiveSync, AutoDiscovery, XML API, Remote Administration, CalDAV/CardDAV, XMPP, Mingerの処理が行えるよう拡張しました。これらのサービス全ての認証失敗は記録され、IPアドレスはこれら全てでブロックされます。セキュリティメニュー以下のダイナミックスクリーニングのUIからこれらの設定が行えます

PIM用添付ファイル

PIM (予定表、連絡先、仕事、メモ)用アイテムが、添付ファイルに対応しました。添付ファイルはWebmail、Outlook Connector, CalDAV/CardDAV経由で追加できます。会議の予定を追加すると、添付ファイルは会議の出席予定者へ送信されます。

SMTP処理中のPGP鍵交換 574

MDPGPダイアログへSMTPメッセージ処理の1つとして公開鍵の自動交換を行う新しいオプションを追加しました。これを実装するため、MDaemonのSMTPサーバーがRKEYと呼ばれるSMTPコマンドに対応しました。RKEYに対応しているメールサーバーへメールを送信すると、MDaemonは送信者の最新又は優先する公開鍵の転送を行うかどうか確認します。対象ホストはキーの有無を確認し、それ以上の処理が不要("250 2.7.0 Key already known")かキーが必要がどうかを返します。キーが必要な場合はキーはすぐにASCIIフォーマット("354 Enter key, end with CRLF.CRLF")でメッセージと同様に転送されます。期限切れになったキーや無効化されたキーは転送されません。MDaemonが送信元のキーを複数持っている場合は常に優先度の高いキーを送信します。優先キーがない場合は、最初に確認したキーを送信します。有効なキーがない場合は処理が行われません。ローカルユーザーに紐づけられた公開鍵だけが提供されます。

公開鍵の転送はメールを配信するSMTPメールセッションの1部として実行されます。公開鍵を許可するため、公開鍵は、キーの所有者によってi= のパラメーターを使ったDKIM署名 484付きのメールと合わせて送信される必要があります。このDKIM署名はFrom: ヘッダのアドレスと完全に一致する必要があります。「キーの所有者」はキー自体から判別されます。また、メールは送信者のSPFパス 479から届いたものである必要があります。最後に、キーの所有者(又はワイルドカードの使用によるドメイン全体)はRKEYにより検証済である必要があります。検証のためには、MDPGPルールファイル(ルールファイルの中に説明が記載されています。)でドメインが公開鍵の交換を行える機関である事を示しておく必要があります。これらの検証は全て自動で行われrますが、DKIM 481とSPF検証 479が有効化されていないと、処理が実行されない点にご注意下さい。

MDPGPログには結果とインポートまたは削除された全てのキーの詳細情報が記録され、この処理はSMTPセッションログへも記録されます。正しく動作しているとSMTPセッションログにキーの処理の詳細が記録され、MDPGPログファイルにも詳細が記録されます。

Outlook ConnectorユーザーのOutlook Add-inの管理 372

OCクライアント設定ダイアログへAdd-insという新しい画面を追加し、Outlook Connectorユーザーが使っているOutlook Add-inの状態を管理できるようにしました。普段使用するアドインの許可や選択したアドインの無効化を行う事ができます。この機能は特定のアドインがOutlook Connectorクライアントと競合している事を把握していて、競合によって発生する問題を避けたいと考えている時に、これを無効化できる便利な機能です。Add-insはOutlook Connector 5.0以上に対応しています。

Webmailの変更点

グループ/配布先情報のインポート/エクスポート
LookOutとWorldClientテーマにおいて、グループ/配布先情報を連絡先からインポートしたり、連絡先へエクスポートするためのオプションを追加しました。Outlookではグループのインポートやエクスポートが行えない事から、フォーマットはMDaemon Webmail独自のフォーマットです。具体的なフォーマットは次の通りです:

カラム - グループのGUID, グループ名, GUI, Full Name, Email

各行はグループ名又はグループのGUIDから始まり、これを新しいグループとして処理します。GUID、Full Name、Emailはグループや配布先の最初の連絡先として処理されます。

Excel用の例は次の通りです:

グループGUID	グループ名	GUID	Full Name	Email
	The Jedis		Anakin Skywalker	ani@jedi.mail
			Leia Organa	leia.organa@jedi.mail
			Luke Skywalker	luke.skywalker@jedi.mail
			Yoda	yoda@jedi.mail
	The Siths		Darth Maul	darth.maul@sith.mail
			Darth Vader	darth.vader@sith.mail
			Emperor Palpatine	emperor.palpatine@sith.mail

インポートの際、グループのGUIDは新規に生成されたGUIDへ置き換えられます。グループ名が含まれていない場合、名前は"ImportedFromCSV_%GUID%"の変換なしで表示されます。%GUID%はGUIDの最初の5文字と変換されます。グループ名の隣のセルを空白にすると次の行がグループ/配布先の最初のメンバーとなります。Emailフィールドはメンバーの追加に必須の項目です。

ボイスレコーティング
LookOutとWorldClientテーマにおいて、ボイスレコーディング機能を追加しました。この機能には特定のブラウザに対応しているマイクロフォンが必要です。この機能は管理者又はユーザー毎にEnableVoiceRecorder=NoをUser.iniに追加する事で無効化できます。ユーザーは5分間の5トラック

までを使用できます。5トラックを超える録音を行おうとすると、選択済のトラックか最初のトラックが新しいトラックへ置き換えられます(ユーザーへ確認画面が表示されます)。録音が(自動又はユーザーにより手動で)停止すると、トラックはmp3形式へ変換され、サーバーへアップロードされます。各トラックには次の4つのユーザーオプションがあります:

- デスクトップへ保存
- デフォルトのWorldClientドキュメントフォルダへ保存
- To, CC, BCC, 件名, plain/textでのメール本文のみが含まれるクイックダイアログを使ったメールでの送信

Toだけが必須フィールドです。件名や本文を入力していない場合は定型文が代わりに使用されます。

- トラックが添付された状態で新しいメール作成画面が起動します。

ここでは、1回で1つのトラックの処理のみ行う事ができます。例えば、1つのトラックだけを1通に添付できます。ユーザーがメールへ複数トラックを添付する場合は、各トラックをドキュメントフォルダへ保存し、そこから新しいメール作成画面へトラックを添付する必要があります。

新しいフォルダ管理機能
LookOutとWorldClientテーマの オプション ≫ フォルダ 画面とメインのフォルダー覧画面へフォルダ管理機能を追加しました。

フォルダー覧画面 (左側のペイン):

- ドラッグ&ドロップでフォルダを1つの上位フォルダから別の上位フォルダへ移動させる事ができます。
- (フォルダの選択後)ダブルクリックでフォルダの名称変更やニックネームの追加が行えます。
- LookOutテーマにて種類別フォルダ表示を行えるようになりました。
- (お気に入りフォルダは1つ以上追加されるまでは非表示のため)最低1つのお気に入りフォルダがある場合は、フォルダをドラッグ&ドロップでお気に入りフォルダへ追加する事ができます。(お気に入り以外の場所へドラッグ&ドロップした場合は何も起こりません。)
- 新しいフォルダとフォルダ名変更ダイアログをLookOutテーマへ追加しました。

オプション ≫ フォルダー覧で、フォルダツリーが折りたたまれた状態で表示されるようになりました。新しいフォルダダイアログをWorldClientテーマのように別ウィンドウへ移動しました。

MDaemon Private Cloud 5.0の新機能

- MDaemon Private Cloud 5.0にはMDaemon 17.0.2とOutlook Connector 4.5が含まれています。
- Updated to a newer version of the Cyren AV engine.
- Domain Administrators may now manage the Web Services in Remote Administration for MDPC.

MDaemonの変更点全てを確認するにはMDaemon 17.0.2のリリースノートを参照して下さい。

Outlook Connectorの変更点全てを確認するにはOutlook Connector 4.5.0のリリースノートを参照して下さい。

MDaemon 17.0の新機能

WorldClient Instant Messenger(292)(WCIM)のXMPP(340)対応

WCIMがWorldClient独自のプロトコルではなくXMPPプロトコルに対応しました。これによりWCIMデスクトップクライアントは他のWCIMクライアントはもちろん、(モバイルクライアントを含む)MDaemonのXMPPサーバーへ接続しているサードパーティー製のXMPPクライアントとも通信できるようになりました。WCIMには、WorldClientへ接続し新着メール通知とメール数をカウントする「WCMailCheck」と、XMPPサーバーへ接続しインスタントメッセージを行う「WCIMXPP」という2種類の通信があります。WCMailCheckはWorldClientへ新着メール通知とメール数のカウント用に通信を行います。WCIMXMPPはXMPPサーバーへインスタントメッセージ用の通信を行います。これに伴い、WCIMユーザーはクライアントの接続画面で接続の種類別の通信一覧が確認できるようになります。(例. "Example.com Mail" や "Example.com)バージョン17へアップデートすると、WCIMはWCIMXMPP通信を自動生成し、WCMailCheck通信と連携します。その後、IMの連絡先を古いシステムから自動的にXMPP用に変換します。新しいWCIMクライアントのデザインや操作性は基本的に同じですが、連絡先やチャットの管理方法等で、異なる点がいくつかあります。WCIMクライアントのヘルプにて、変更点の詳細を確認して下さい。

WorldClient Dropbox連携(309)

WorldClientに新しくDropboxとの連携機能が搭載されました。これにより、ユーザーは添付ファイルをDropboxアカウントへ保存したり、Dropbox内のファイルに対するリンクを送信メールへ挿入できるようになります。WorldClientでこの機能を利用するには、Dropboxプラットフォームにて、WorldClientをDropbox appとして設定する必要があります。これは、Dropboxアカウントでログインし、app用に固有の名前を作成し、Dropboxへフルアクセス権限を与え、WorldClientへのリダイレクト用URIを指定し、デフォルト設定の1つを変更するという単純な処理です。その後、Dropbox App KeyとApp SecretをMDaemonのDropboxオプションへ入力します。その後、ユーザーがWorldClientへログインすると、WorldClientの画面上にDropboxアカウントへのリンクが表示されます。Dropbox appの作成とWorldClientへのリンク方法についての詳しい手順は、Dropbox Appの作成とリンク(311)を参照して下さい。

Dropbox appを作成すると、初期段階でのステータスは「Development」となります。これはWorldClientユーザーの内500ユーザーまでがDropboxアカウントからappへリンクできるというステータスです。ただし、Dropboxによれば、「appが50のDropboxユーザーとリンクした場合、ステータスをProductionとして申請し、承認を受けるのに2週間待つ必要が生じます。その間、500ユーザー中何ユーザーがリンクしているのかに関わらず、Dropboxユーザーの追加を行う事はできません。」つまり、ステータスがproductionになるまで、Dropbox連携は機能し続けますが、ユーザーの追加を行う事はできません。productionの承認手続きについてはDropboxのガイドラインやサービス要項を確認して下さい。詳細についてはDropbox Platform開発者ガイドを参照して下さい。

WorldClient appが正しく作成し設定すると、各WorldClientユーザーへ、アカウントをDropboxアカウントへ接続するためのオプション画面が追加されます。ユーザーはDropboxへログインしDropboxアカウントへ接続するのに必要な権限をappへ与える必要があります。ユーザーは認証処理中にDropboxへ渡したWorldClient URIを使用して元の画面へ戻されます。セキュリティ目的でURIはDropbox.comのapp情報ページで指定したRedirect URIと同じものである必要があります。最後に、WorldClient とDropboxはアクセスコードとアクセストークンを交換し、WorldClientがユーザーの

Dropboxアカウントへ接続し、添付ファイルを保存できるようになります。交換されたアクセストークンは7日間毎に期限切れとなり定期的にユーザーはDropboxと認証を行う必要があります。ユーザーは手動でDropboxから接続を解除したり、必要に応じて再認証を行ったりする事ができ、その際にはWorldClientのCloud Appオプションページを使用します。

PowerShellスクリプトを使ったLet's Encryptとの連携

MDaemon[525], WorldClient[528], Remote Administration[532]で SSL/TLS と HTTPS[523]に対応するには、SSL/TLS証明書が必要です。証明書は小さなファイルで認証局(CA)によって発行され、対象サーバーへ接続したクライアントやブラウザで、SSL/TLS/HTTPSによる安全な接続を行おうとしているものに対して、通信元が偽装されているものではない事を証明しています。Let's Encryptとは証明書を無償で提供する認証局です。従来、安全なウェブサイトを実現するためには、証明書の手動生成や検証、署名、インストール、更新が必要でしたが、Let's Encryptはこうした複雑なプロセスを軽減するため、自動処理を行えるよう設計されています。

LetsEncrypt対応として、MDaemonではPowerShellスクリプトをMDaemon¥LetsEncryptディレクトリへ格納しています。このスクリプトが依存しているACMESharpモジュールは PowerShell 3.0が必要です。つまり、このスクリプトはWindows 2003では動作しません。WorldClientは80番ポートを待ち受けポートにする必要があり、それ以外の場合スクリプトは動作しません。このスクリプトを実行する前にはPowerShellの実行用ポリシーを正しく設定する必要があります。このスクリプトを実行すると、http-01チャレンジを実行するのに必要なファイルをWorldClientのHTTPディレクトリへ配置するなどの必要な処理を行います。MDaemon, WorldClient, RemoteAdministrationで証明を行うため、デフォルトドメイン[165]のSMTPホスト名[167]を使用し、証明書を取得し、Windowsへインポートした後で、MDaemonで証明書を使用できるようにするための設定を行います。

デフォルトドメインとしてMDaemonサーバー以外を指しているFQDN[167]を使っている場合は、このスクリプトは機能しません。証明書で使っているホスト名を使用する事もできます。その場合はコマンドラインで対象のホスト名を渡す必要があります。

使用例:

```
..\LetsEncrypt.ps1 -AlternateHostNames mail.domain.com,wc.domain.com -
   IISSiteName MySite -To "admin@yourdomain.com"
```

AlternateHostNamesの一覧でデフォルトドメインのFQDNを使用する必要はありません。例えば、デフォルトドメインがexample.comでFQDNがmail.example.comの場合、ここでは代わりにimap.example.comを使用する事ができます。スクリプト実行時には、imap.example.comを代わりのホスト名として引き渡します。また、代わりのホスト名を送信すると、HTTPチャレンジがそれらの情報を処理する必要が生じます。名前解決が完了しない場合、全体の処理は正しく完了されません。代わりのホスト名を渡す必要がない場合、-AlternateHostNamesパラメータはコマンドラインで使用する必要はありません。

WorldClientをIISで稼働させている場合、このスクリプトを-IISSiteNameパラメーターでサイト名を指定した上で実行して下さい。IISで証明書の自動設定を行うにはMicrosoftのWebスクリプティングツールがインストールされている必要があります。

最後に、スクリプトではMDaemon¥Logs¥フォルダへLetsEncrypt.logというログファイルを生成します。ログファイルはスクリプト実行の度に削除され再生成されます。ログにはスクリプトの開始日時は記録されますが、実行毎の日時は記録されません。また、通知メールがエラー発生毎に送信されます。これはPowerShellスクリプトで自動生成された$error変数を使って行われます。エラー発生時にメール通知を行わない場合は、-Toパラメータはコマンドラインへ含まないで下さい。

メールボックスパスワードを復元できない暗号化方式で保管するオプション

新しい パスワードオプション[778] が追加され、メールボックスのパスワードを復元できない暗号化方式で暗号化し保管できるようになりました。Ctrl+U| その他 | パスワード へチェックボックスを追加し、メールボックスのパスワードを復元できない暗号化方式で暗号化し保管できるようになりました。これにより、パスワードはMDaemon、管理者、攻撃者の誰からも復元できなくなります。これを有効にすると、MDaemonはbcryptパスワードハッシュを使用します。これは今までよりも長いパスワード(72文字まで)を許可しており、アカウントのエクスポートやインポートの際には、パスワードを除く事もなくなり、パスワードが記載されていても、暗号化されているため情報が洩れる心配がありません。MDaemonのバージョンによって、APOP & CRAM-MD5認証や弱いパスワード検出などMDaemonによって復元する機能がある場合もあり、この機能との互換性はありません。復元できないパスワードはデフォルトで有効化されています。

ActiveSyncクライアント承認

新しいActiveSync設定で、アカウントに「新しいクライアントは同期を行うのに管理者による承認が必要」とする事ができるようになりました。承認待ちのクライアント[422] は一覧で確認でき、管理者は同じ画面から承認を行う事ができます。このオプションは全体設定[384]かアカウント別[697]クライアント設定画面から行う事ができます。全体設定はデフォルトで無効化されており、アカウントオプションは設定を引き継ぐようにデフォルト値が設定されています。

ActiveSync通知

ActiveSyncへ管理用の2つの通知が追加されました: 同期のロールバック通知とエラー通知です。

同期のロールバック通知

ActiveSyncサービスで、クライアントが繰り返し/頻繁に期限切れの同期用のキーを同期処理用に送信している場合に管理者へ通知を送るようになりました。

クライアントが期限切れの同期用キーで同期要求を行っている事から、こうした処理はデータのロールバックを意味する事がよくあります。件名は「期限切れの同期用キーを使用しているActiveSyncクライアント」です。これは、過去にクライアントへ送られたコンテンツがネットワークの問題等で同期できていなかった問題を表す場合があります。場合によっては、過去の同期データが送信されたかどうかによって、IDだけが送信されていた場合もあります。

ロールバックの警告は、クライアントが同期できていないという意味ではなく、クライアントが同期対象外になる可能性がある事や、それをシステムで検知した事を示しています。データのロールバック警告は24時間に一度だけ通知されます。

- [System] SendRollbackNotifications=[0|1|Yes|No|True|False]
- [System] RollbackNotificationThreshhold=[1-254]: ロールバックの数字は管理者へ通知される前に実行される必要のある回数です。ここでは、ネットワークの問題も関係する事から、最小5回を推奨します
- [System] RollbackNotificationCCUser=[0|1|Yes|No|True|False]: 期限切れの同期用キーを送ったクライアントをCCへ含むかどうかを指定します。

ActiveSyncエラーメール通知

ActiveSyncサービスで管理者へ処理されなかった特定のメッセージを通知するようになりました。これらのメッセージは対象のアイテムが処理できず、それによってその後のアクションが実行できない旨をリアルタイムで管理者へ通知します。件名は「エラーメッセージ通知」です。従来、これらのアイテムによってクラッシュの可能性がありました。多くの場合、msgファイルの内容はMIMEデータではありませんでしたが、これがMIMEデータの場合、エラーの場合がほとんどでした。これらの通知で関連す

るユーザーをCCに入れるかどうかを選択でき、ユーザーへの通知はCMNCCUserキーを付与するため、メールボックスに届いたメールが読み取りできない場合でもそれを知る事ができます。こうした場合に行うべき対応は対象のmsgファイルをユーザーのメールボックスから移動し、これを解析して処理できなかった原因とどのような解決策があるのかを検討する事です。

[System] CMNCCUser==[0|1|Yes|No|True|False]

MDaemon Private Cloud 4.5の新機能

- MDaemon Private Cloud 4.5にはMDaemon 16.5.2とOutlook Connector 4.0.1が含まれています。
- ClamAVプラグインへスキャンできなかったファイルを隔離するオプションを追加しました。また、スキャンできなかったパスワード付ファイルを許可するオプションも追加しました。スキャンされる事なく許可されたファイルには「X-CAV-Result:」ヘッダが付与され、これには次のような結果が含まれます：″encrypted″（パスワード保護されたファイル），″non-scan″（スキャンできなかったファイル），″scanning error″（スキャン中にエラーが発生したファイル）。

MDaemonの変更点全てを確認するにはMDaemon 16.5のリリースノートを参照して下さい。

Outlook Connectorの変更点全てを確認するにはOutlook Connector 4.0.1のリリースノートを参照して下さい。

MDaemon 16.5の新機能

MDPGPのアップデート 574

キーサーバに対応

WorldClient

WorldClientが基本的な公開鍵サーバーとして動作します。MDPGPの「HTTP（WorldClient）経由で公開鍵を送信」オプションを有効化すると、WorldClinetでユーザーの公開鍵リクエストを受け付けるようになります。要求するためのURL形式は次の通りです：`http://<WorldClient-URL>/WorldClient.dll?View=MDPGP&k=<Key-ID>`。 <WorldClient-URL>にはWorldClientサーバーのパス（例えば、http://wc.altn.com といった形です）を入力し、<Key-ID>には16桁のkey-id（例，″0A1B3C4D5E6F7G8H″）を入力します。key-idはフィンガープリントの最後の8バイトで構成され、全部で16文字となります。

DNS (PKA1)

新しいMDPGPオプションである「DNS（pka1）から公開鍵を収集し[xx]時間キャッシュする」を有効化すると、MDPGPがPKA1を使ってDNS経由で宛先の公開鍵の確認できるようになりました。この機能により、宛先の公開鍵の取得の処理が自動化でき、暗号化メール送信時の、手動でのキーの取得が不要になります。PKA1クエリが生成されると、キーURIがすぐに収集され、検証された上でキーリングへ追加されます。正しくキーリングへインポートされたキーはオプションで指定した値かPKI1レコードのTTL値のうち大きい値を元に、指定時間が経過すると自動で期限切れとなります。

キー処理

トラッキングキー

MDPGPで、key-idやsub-key-idではなく、プライマリkey-idでのトラッキングを常時行うようになりました。併せて、MDPGPのキー一覧ダイアログで、不必要な2つの列を削除しました。また、MDPGPのエクスポート用フォルダの操作がより厳密に行われるようになりました。結果としてエクスポートされたローカルユーザーのキーは常に対象フォルダへ格納されるようになりました。キー自体は暗号化されているものの、ユーザーの秘密鍵がこのフォルダへ保管されているため、このフォルダ(と可能であればPEMフォルダ構造全体)への不正アクセスが行われないよう、OS側で保護するようにして下さい。

優先キー

従来、同じメールアドレス用の異なる複数のキーが、キーリング上に存在した場合、MDPGPは複数あるキーの中で最初に発見したキーを使うという単純な仕様になっていました。今後は、対象のキーを右クリックし、優先キーとして設定する事ができます。優先キーが見つかった場合、キーは複数存在する場合でも、常に優先して使用されます。優先キーとして設定されているものがない場合は、最初に見つかったキーが使用されます。メールの復号化の際には、それぞれのキーが使用されます。

無効なキー

無効なキーや削除されたキーは、新しい oldkeys.txt へトラッキングされるようになりました。従来のバージョンでは、対象のkey-idをplugins.datファイルへ記録していました。

MDPGP署名検証

MDPGPはメール内に組み込まれた署名で暗号化されていないものを検出できるようになりました。従来、署名の検証を行うには、メールへ署名と暗号化の両方が行われている必要がありました。WorldClientで検証済の署名を持つメールを表示すると、新しいアイコンが検証済である事を示すのに表示されます。署名検証はローカル以外のユーザーに対してはデフォルトで有効ですが、このサービスを使用するユーザー、使用しないユーザーのメールアドレスを直接指定する事もできます。(MDaemonのMDPGPダイアログ[574]).

XMPPインスタントメッセージングサーバー[340]

Extensible Messaging and Presence Protocol (XMPP) サーバーがパッケージされ、MDaemonでPidgin, Gajim, Swiftいった、サードパーティーのXMPPクライアントを使ったインスタントメッセージが行えるようになりました。クライアントはほとんどのOSやモバイル端末用に提供されています。XMPPインスタントメッセージはMDaemonの従来のチャットシステム(WorldClient Instant Messenger)とは完全に別のシステムで、2つのシステムがコミュニケーションを行ったり、知り合いリストを共有する事はできません。

XMPPサーバーはWindowsサービスとしてインストールされ、設定画面はMDaemon UIでCtrl+W | XMPPからアクセスできます。XMPPサーバーではデフォルトで5222番ポート(STARTTLSを使ったSSL)と5223番ポート(SSL専用)を使用します。XMPPサーバーはMDaemonで有効化されているSSL設定情報を使って通信を行います。また、XMPPクライアントによってはホスト名の自動検出にDNS SRVを使用するものもあります。詳細はhttp://wiki.xmpp.org/web/SRV_Recordsを参照して下さい。

ユーザーは選択したXMPPクライアントへメールアドレスとパスワードでログインします。クライアントによっては、メールアドレスとログインIDを異なるコンポネントとして扱う場合もあります。例えば、frank@example.com ではなくログイン/パスワードにはfrankを使用し、ドメイン名としてexample.comを指定するといった形式です。

複数のユーザーチャットは、通常「rooms」や「conference」として表示されます。グループチャットのセッションを開始するには、roomやconference(名前をつけて下さい)を作成し、他のユーザーを招待しま

す。多くのクライアントではサーバーの場所を指定する必要はなく、名前だけで招待が行えます。チャットの場所を指定する必要がある場合は、名前と場所を次のように記載して下さい: "room@conference.<your domain>"(例. Room01@conference.example.com).

(Pidginなど)ユーザー検索に対応しているクライアントもあり、サーバー上のユーザーを名前やメールアドレスで検索し、簡単に連絡先として追加する事ができます。ユーザー検索サービスは、デフォルトで「search.(ドメイン名)」で指定します。% シンボルはワイルドカードとして使用できます。例えばメールアドレス欄に「% @ example.com」と入力する事で、@ example.comで終わる全てのメールアドレスを一覧表示する事ができます。

OCクライアント設定の一元管理 356

OCクライアント設定ダイアログでOutlook Connectorユーザーのクライアント設定を一元管理できるようになりました。画面毎にクライアント設定を行うと、Outlook Connectorユーザーからの接続があった際、MDaemonは対象クライアントへプッシュ配信します。OCクライアント設定は前回クライアントが接続し設定を受け取ってから、設定に変更があった場合にのみ送信されます。これを有効にする場合は「OCユーザーによるプッシュ配信された設定の上書きを許可する」オプションを有効にしておくと、個々のクライアント設定をユーザーが上書きできるようになります。このオプションを無効にしておくと、クライアント設定全てがグレーアウトされ、Outlook Connectorユーザーが設定を変更する事はできません。

ユーザー毎、ドメイン毎に異なる値が必要な項目を設定するのに、OCクライアント設定へは$USERNAME$, $EMAIL$, $DOMAIN$といったマクロを使用できます。このフィールドへは「Frank Thomas」といった、ハードコードされた値を使わないよう注意して下さい。全般 358 画面にはマクロ参照ボタンがあり、対応マクロが一覧表示されます。

MDaemon Private Cloud (MDPC)の場合は、ドメインマネージャー 165 へOCクライアント設定ダイアログがあり、ドメイン毎にOutlook Connectorクライアント設定が行えます。

この機能はデフォルトで無効になっており、Outlook Connector v4.0.0か、それ以上のバージョンを使っている場合にのみ使用できます。

FROMヘッダの保護/変更 516

新しいセキュリティ機能として受信メールのFrom: ヘッダを名前とメールアドレス両方を含んだものへ変更する機能が搭載されました。この機能はFromヘッダを偽装した攻撃を防ぐための機能で、Fromヘッダの偽装は、メールクライアントの多くが、メールアドレスを表示せず名前だけを表示している事が起因しています。メールアドレスを確認するには、メールを開いた上で対象アドレスを右クリックする、といった操作が必要になります。そのため、攻撃者は、目に入る部分のみに、会社名などを入力しておきます。例えば、メールの実際のFromヘッダが「Honest Bank and Trust" <lightfingers.klepto@example.com>」だったとしても、クライアントでは「Honest Bank and Trust」のみが表示されます。Fromヘッダの変更機能は、送信者のヘッダを「lightfingers.klepto@example.com -- Honest Bank and Trust」という表示へ変更し、送信元を判断しやすくします。この機能はローカルユーザー宛のメールに対してのみ適用され、デフォルトで無効に設定されています。

IPスクリーンのアップデート 510

IPスクリーンにインポートボタンを追加し、APFや.htaccessからIPアドレスデータをインポートできるようにしました。これらのファイルへの対応は、現時点では次のように限定されます。

- 「deny from」と「allow from」は認識します
- (ドメインではなく)IPで指定された値のみがインポート対象となります。

- CIDR notationを使用できますが、部分的なIPは使用できません。
- 各行は空白（又はカンマ）で分けられたIPアドレスが含まれます。例えば、「deny from 1.1.1.1 2.2.2.2/16」はOKで、「3.3.3.3, 4.4.4.4, 5.5.5.5」も使用できます。
- # から始まる行は無視されます。

製品の最新バージョン自動インストール

自動アップデート機能を使って、MDaemonがpostmasterへ最新版の無人インストールを行うかどうか、行うとすればいつ行うか、を指定する事ができます。MDaemonそのものと、（使用中の場合は）SecurityPlusとOutlook Connectorの自動アップデートが行えます。最新バージョンの自動インストールは製品毎にそれぞれ処理されており、サーバーの再起動が必要です。MDaemonが製品の新バージョンを検出すると、プログラムをダウンロードし指定した時刻にインストールを実行するためキューへ保管します。システムログにはインストール処理の全てが記録され、postmasterへの通知も行われます。アップデート ダイアログで詳細を確認して下さい。

WORLDCLIENTのアップデート

カテゴリ

WorldClientのLookOutとWorldClientテーマで、メールをカテゴリ別に分類できるようになりました。ユーザーはオプション | カラムの中の、メール一覧のセクションで、「カテゴリ」をチェックし、カテゴリのカラムをメール一覧へ追加できます。1通または複数のメールに対してカテゴリを選択するには、対象のメールを選択し、右クリックして下さい。

- WorldClientの管理者も、独自のカテゴリを作成できます。独自カテゴリ用に、DomainCategories.jsonと PersonalCategories.jsonの2つのファイルが存在しています。
- ドメインカテゴリはデフォルトで全体に対し有効化されています。これを無効にするには、MDaemon¥WorldClient¥Domains.ini [Default: Settings] でDomainCategoriesEnabledの値をNoへ変更して下さい。
- ユーザーは個々のカテゴリの追加や編集が行えるようデフォルトで設定されています。これを無効化するには、ユーザー毎（ユーザーのUser.iniの[User]以下）か全体（MDaemon¥WorldClient¥Domains.iniの[Default: UserDefaults]以下）で、CanEditPersonalCategoriesの値をNoへ変更して下さい。カテゴリ
- ドメインカテゴリが有効で、ユーザーが個々のカテゴリ編集を行えないようにすると、ユーザーはDomainCategories.jsonへ記載されているカテゴリー覧の表示のみが行えるようになります。
- ドメインカテゴリが無効化されており、ユーザーも個々のカテゴリの編集が行えない場合、ユーザーへはPersonalCategories.json内のカテゴリー覧が表示されます。
- CustomCategoriesTranslations.json で複数言語でのカスタムカテゴリを使用する事ができます。必要なカテゴリの翻訳分を必要に応じてこのファイルへ追加して下さい。WorldCientでは予定やメモ、仕事に使用するカテゴリ名をこのファイルから認識する事ができます。

より詳細な情報は、MDaemon\WorldClient\CustomCategories.txtファイルを参照して下さい。

除外リストとブロックリスト

管理者がWorldClientユーザーの除外リストやブロックリストフォルダを隠す事ができるようになりました。この設定を行う場合は、MDaemon¥WorldClient¥Domains.iniの [Default: UserDefaults]で、HideWhiteListFolder= YesとHideBlackListFolder= Yesを設定して下さい。ユーザー毎のUser.ini内

の[User]セクションで、HideWhiteListFolder=NoやHideBlackListFolder=Noが設定されているユーザーは、個別の除外リストやブロックリストを引き続き表示できます。

添付ファイルの確認

LookOutとWorldClientテーマにおいて、メール作成画面で、件名や本文に添付という記載があった際、送信前に添付ファイルの確認を行うオプションを追加しました。

2段階認証 656

2段階認証（2FA）システムの利用を必須とするかどうか、2段階認証システムの利用を許可するかどうか、を設定するための新しいチェックボックスが2つ追加されました。新規アカウント 728 テンプレートで新規に追加するアカウントのデフォルト値をコントロールできます。ユーザー毎の2FA管理を行うのに、ウェブサービス 656 画面から対応したオプションを使用できます。

MDaemon Private Cloud 4.0の新機能

- MDaemon Private Cloud 4.0にはMDaemon 16.0.3とOutlook Connector 3.5.2が含まれています。
- Outbreak Protectionエンジンをバージョンアップしました。
- ClamAVエンジンを0.99.2へバージョンアップしました。

MDaemonの変更点全てを確認するにはMDaemon 16.0リリースノートを参照して下さい。

Outlook Connectorの変更点全てを確認するにはOutlook Connector 3.5.2リリースノートを参照して下さい。

MDaemon 16.0の新機能

MDaemon Remote Administration（MDRA）GUIのアップデート

MDRAのGUIはフレームを廃止しモバイル対応のレスポンシブデザインへアップデートしました。対応ブラウザはIE10+、Chromeの最新バージョン，Firefoxの最新バージョン、MacとiOS用Safariの最新バージョンへ制限されます。Androidの標準ブラウザはスクロールに既知の問題がありますが、Androidに搭載のChromeであれば正常に動作します。

スパムボット検出 518（MDaemon PROが必要です）

スパムボット検出という新機能では、全てのSMTP MAIL（return-path）の値で使用されたIPアドレスを一定期間記録します。短時間の間に複数のIPアドレスで同じreturn-pathを使っていた場合、スパムボットネットワークである場合があります。もちろん、メールシステム全体として正当な場合もあります（この機能に対するルールは現時点ではありません。）それでも、検証した結果、同じreturn-pathが使われるスパムボットネットワークの検出に、効果的である事が確認されています。スパムボットが検出されると、その時点での接続はすぐに遮断され、return-pathの値はオプションとして、指定した時間ブロックリストとして登録されます。ユーザーが定義した期間全てのスパムボットIPをブロックリストへ登録する事もできます。

CardDAV (MDaemon PROが必要です)

MDaemon がCardDAVプロトコルを使った連絡先の同期に対応しました。MDaemonのCardDAVサーバーで、認証したCardDAVクライアントからMDaemonで保持している連絡先情報へアクセスできるようになります。有名なCardDAVクライアントには (Mac OS Xに含まれている) Appleアドレス帳、Apple iOS (iPhone)、SOGoプラグイン経由でのMozilla Thunderbirdがあります。CardDAVやCardDAVの設定に関する詳細は、CalDAV & CardDAVをご参照下さい。

WORLDCLIENTとREMOTE ADMINISTRATION用の2段階認証

MDaemonがWorldClient や MDaemonの Remote Administrationのウェブインターフェイスへのログイン時、Two Factor Authentication (2段階認証)に対応しました。

WorldClientへHTTPSでサインインできるユーザーは **オプション >> セキュリティ** より、2段階認証を有効化する事ができます。設定後、ユーザーはWorldClientやRemote Administrationへサインインする際、認証コードを入力する必要があります。コードはユーザーのモバイル端末やタブレットへインストールした認証アプリから取得できます。この機能はGoogle認証システムに対応している全てのクライアントで利用できます。

ACTIVESYNCプロトコルマイグレーションクライアント

MDaemonにActiveSyncプロトコルをベースにしたマイグレーションクラインと(ASMC.exe)がパッケージされました。この機能を使い、プロトコルバージョン14.1に対応しているActiveSyncサーバーから、メールや予定表、仕事、メモ、連絡先情報を移行する事ができます。¥MDaemon¥Docsからこの文書をご参照下さい。

管理用のXML API

MDaemonはhttp(s)用XMLをベースにしたAPIを同梱する事になりました。これにより、MDaemon管理クライアントが、http(s)://のpostリクエストの送信が行える全てのプラットフォーム上で、全ての言語で記述できるようになりました。MDaemonでは、これは認証された全体管理者でのみ利用でき、MDaemon Private Cloudでは、認証されたドメイン管理者がアクセス権を持つ機能に対し、これらのAPIを利用する事ができます。APIはAPIの仕様に関する文書を掲載したウェブサイトも生成します。インストール後のデフォルト設定では、https://servername/MdMgmtWS/でアクセスできますが、こちらはセキュリティの強化を目的とし、任意のURLへ設定変更する事ができます。

利用可能な操作には次のものが含まれています。

- Help
- CreateDomain
- DeleteDomain
- GetDomainInfo
- UpdateDomain
- CreateUser
- DeleteUser
- GetUserInfo
- UpdateUser
- CreateList

- DeleteList
- GetListInfo
- UpdateList
- AddDomainAdministrator
- DeleteDomainUsers
- GetDomainList
- GetVersionInfo
- GetQueueState
- GetServiceState
- SetAddressRestriction
- GetAddressRestriction

現時点で、コマンドラインのクライアントとして、Javascript, Powershell, VBScript, C, C++, Visual Basicで記述したものについては動作確認済です。一般的なブラウザ内で操作できるウェブベースの管理コンソール、というコンセプトを証明する目的で、シンプルなHTMLとJavascriptを使ったテスト用サイトが使用されていました。テストしたわけではありませんが、APIはPHP、Perl、その他開発用プラットフォーム上でも正常動作するものと予想されます。

参照:

初めに 12
MDaemon Private Cloud 11.0.0へのアップグレード 55
MDaemonの管理画面 64

1.4 MDaemon Private Cloud 11.0.0へのアップグレード

以前のバージョンからMDaemon 23.0.2 へアップデートする際の特記事項と注意事項は下記の通りです。MDaemon 23.0.20で追加された機能や変更点、修正点の詳細は、MDaemonの \Docs\ サブフォルダにあるRelNotes.htmlを参照してください。

Version 23.0.2

- Outbreak Protection機能が再び使用できるようになりました。Outbreak Protection 583の設定がデフォルト値に戻っていないかをご確認ください。

Version 23.0.1

- これまで使用していたCyren社のアンチウィルス機能から、IKARUS社のアンチウィルス機能へと変更しました。Cyren社が突然の事業停止となり、それに代わるウィルス対策パートナーを慎重かつ確実な検討を行ない、IKARUS社の検出率と反映率が優れていたので変わって採用しました。IKARUS社のアンチウィルス機能では、10分毎にウィルス定義ファイルの自動更新を行います。AntiVirusライセンスの有効期限がきれますと、IKARUSを使ったウィルススキャンは無効化されます。
- Cyren Outbreak Protection が削除されます。OEMとして使用していたCyren社が事前の話しもほとんどなく、事業の停止計画を発表したためです。そのため、同社と似た仕組みを持つ代わるスパム対策技術を現在積極的に調査と検討を行なっております。
- ¥MDaemon¥App¥MDaemon.iniにある[Special]セクション内のパラメータ IMAPKeywordFlags=Yes/No にてIMAPキーワードフラグの有効/無効を切り替えるようになりました。Thunderbirdメールクライアントでメッセージのタグが無くなってしまうことを考慮し、Ver.23より前のMDaemonからのバージョンアップを行なった際には、このオプションは無効になっています。ThunderbirdのIMAPキーワードでは接続すると読み取ったIMAPメッセージのタグをブランク(空白)にします。IMAPキーワードフラグは、新規インストールやVer.23.0.0以降でのバージョンアップ時にはデフォルトで有効になっています。

Version 22.0.0

- 32bit版MDaemonのご提供が終了しました。MDaemon 22.0以降は、64bit版だけのご提供となります。もし、64bit版のWindows OS上で32bit版のMDaemonをご使用の場合、64bit版のMDaemonを上書きインストールするだけで切り替えることができます。
- 強固なパスワードの最少文字数[778]が8文字以上となりました。MDaemon 22へバージョンアップする前に、8文字よりも少ない文字数でご使用頂いていても、バージョンアップ後は8文字に変更されます。新規インストールをされた場合のデフォルトの最少文字数は、10文字となります。
- MDaemonは、"ホワイトリスト"と"ブラックリスト"という用語を変更し、"許可リスト"と"ブロックリスト"としました。IPや、メールアドレスなどで除外するために使用していた"ホワイトリスト"表記も"除外リスト"と変更しました。各ユーザーのスパムフィルタ連絡先フォルダも、"許可送信者"と"ブロック送信者"と変更します。すべてのアカウントのフォルダは、MDaemon 22が最初に起動する時にフォルダ名が変更されます。

Version 21.5.0

- ロケーションスクリーニング[520]でメールへ追加する、'X-MDOrigin-Country'ヘッダが、国の大陸名全部ではなく、2文字の国と大陸コードを使用するようになりました。このヘッダで特定の値をフィルタリングしている場合は、この値を更新してください。
- WebmailのMobileテーマをProテーマと名称変更した事で、Mobileテーマで認証情報を記憶しているユーザーへ影響がある可能性があります。ユーザーは添付ファイルが開けない場合があります。この場合、ユーザーは一旦ログアウトし、再度ログインを行ってください。

Version 21.0.2

- 設定 ≫ 初期設定 ≫ その他 の画面にある、"システムが生成するpostmaster宛ての通知のコピーをグローバル管理者やドメイン管理者に送信する"で送信されるメールの内容が増え、アカウントの凍結や無効化、'No such user'応答、ディスクエラー、空き容量不足やベータ版と

AV有効期限などが含まれます。もし、管理者がこれらの通知を不要とする場合、設定を無効にする必要があります。

Version 20.0.3

- "Heuristics.Limits.Exceeded"によるAVスキャンの失敗が多発したため、MDaemonがClamAVの clamd.conf にある"AlertExceedsMax yes"の行をコメントアウトするようになりました。

Version 20.0.1

- これまでMDaemonサービス(及び、Remote AdministrationとXMPPサーバサービス)は、SYSTEMアカウントとして稼働しておりましたが、ネットワークリソースへアクセスできるよう管理画面の設定 | 初期設定 | Windowsサービスから設定するアカウントの権限でプロセスやスレッドを実行するようになります。このバージョンへのインストールやバージョンアップを行なうと、そのアカウント権限でサービスが起動するように設定が更新されます。
- clamd.conf内の多くの設定項目の廃止や変更があったため、インストーラは既存のclamd.confを新しいファイルとして上書きします。もし、clamd.confファイルをカスタマイズされていた場合、インストール後に内容を確認して編集して下さい。

Version 20.0.0

- リリースノートの[8930]のラベルの項目ではActive Directory連携システムの変更について説明していますので、注意してお読みください。この変更により、過去の設定が無効となり、再設定が必要になる場合があります。変更箇所について記載されているセクションを注意してご確認下さい。
- MDaemon 20.0 の動作には Windows 7, Server 2008 R2, 又はそれ以降のシステムが必要です。
- 初期設定 ≫ その他 459 に新しく2つのチェックボックスが追加されました。システムが生成し、定期的に送信するPostmasterエイリアス宛の通知メールを、全体又はドメイン毎の管理者へも送信するかどうかを選択できます。デフォルトで、このオプションはどちらも有効です。ドメイン管理者はドメイン宛の通知とリリースノートのみを受信します。全体管理者はキューサマリーレポート、統計レポート、リリースノート、(全ドメインの)「存在しないユーザー」レポート、ディスクエラー通知、全ドメインのアカウントの凍結や無効通知(ドメイン管理者のように、アカウントの凍結解除や有効化が行えます)、ライセンスの警告、ベータバージョンの通知、スパムサマリーレポート、その他の全ての通知を受信します。管理者へ全ての通知を送らないようにするには、この設定を無効化する必要があります。
- 自動応答の保管方法が変更されました。アカウントの自動応答用のテキストはOOF.MRKとしてアカウントのルートメールフォルダ内に新たに作成されるDATAフォルダ内に保存されます。自動応答スクリプトはAPPフォルダへは今後保管されず、アカウント間で共有される事はありません。MDaemonの初回起動時、既存の自動応答用ファイルは全て新しい形式へ変換され、正しい場所へ再配置されます。AUTORESP.DATファイルは今後使用されないため全てのアカウント毎の.RSPファイルと同様に削除されます。(OutOfOffice.RSPとアカウント以外の特別なファイルは参照やサンプルの目的のために残されます。)もしもすぐに1つの自動応答設定を複数アカウントへ適用させたい場合は、アカウント設定 ≫ 自動応答 660 に新しく追加された公開ボタンを使用してください。このボタンは既存の自動応答スクリプト用テキストと自動応答設定を、現在のアカウントや選択した対象アカウントへコピーします。 自動応答ファイルの編集 660 ボタンでも、デフォルトの自動応答スクリプト(OutOfOffice.rsp)の編集が行えます。

このデフォルト値はアカウントのOOF.MRKが存在していなかったり、空だった場合にコピーされます。

- アカウント署名ファイルの保管方法が変更されました。アカウントの署名ファイルはSIGNATURE.MRKとしてアカウントのルートメールフォルダ内に新たに作成されるDATAフォルダ内に保存されます。MDaemonの初回起動時、既存の署名ファイルは全て新しい形式へ変換され、正しい場所へ再配置されます。ルートのMDaemon Signaturesフォルダには今後アカウント毎の署名ファイルは保持しませんが、元のファイルはWebAdminやコンテンツフィルタで必要な場合のみそのまま保持されます。元のSignaturesフォルダは変換の際¥Backup¥20.0.0a¥Signatures¥へバックアップされます。最後に、全てのアカウント用のADMINNOTES.MRKは、アカウントのルートメールフォルダから、新しいDATAサブフォルダへ移動されます。
- スパムフィルタ ≫ 除外リスト（自動）627 の中の「‥DKIMで認証された除外リストのアドレスのみ」オプションのデフォルト値が無効へ変更されました。この値を有効化すると制限がかかり、MultiPOPやDomainPOPで使用するアドレス帳を除外リストへ追加する事ができなくなります。設定が希望する値でない場合は、このオプションを再度有効化してください。
- 初期設定 ≫ UI447 の「全てのUIダイアログをセンタリング」は全ユーザーに対して「有効」となるよう初期化されます。希望の設定でない場合はこれを無効化してください。この設定により、画面が部分的にフレームからはみだしたり、複数の画面が重なる事で選択しにくくなる事を防ぎます。
- セキュリティマネージャ ≫ スクリーニング ≫ 国別スクリーニング520 – デフォルト値が無効から有効へ変更されました。国別スクリーニングを有効化すると、ブロックされていない国や地域であっても、接続元の国や地域が（把握できる範囲で）ログに記録されます。そのため、（ブロックする対象の国を選択せず）どの国もブロックしない場合においても、国別スクリーニングを有効化しておくことで、国や地域を表示し、ログへ記録する事ができます。デフォルト設定値が変更となったため、国別スクリーニング設定画面の確認と修正をアップグレードの際に行ってください。MDaemonではコンテンツフィルタや他の目的のため'X-MDOrigin-Country'ヘッダにて国や地域の情報を挿入します。
- スパムフィルタでスキャンできるハードコードの最大値であった2MBが削除されました。スキャンできるスパムのサイズ制限がなくなりました。制限が必要な場合はこれを指定する事もできますが、0を設定すると、今後は制限なしとして扱われます。あわせて、サイズ制限はKBからMBへ変更され、既存の設定値は自動で0へ変更されます。スパムフィルタ ≫ 設定636 にて、設定値が想定している値となっているかどうかを確認してください。
- メインUIのキュー画面へ'送信者ドメイン'と'宛先ドメイン'の列を追加しました。これにより保存されている列の幅が初期化されます。列の幅を自分で設定していた場合は設定した値が保存されます。
- デフォルトでホストスクリーンがMSA接続へ適用されます。必要に応じて、セキュリティマネージャ ≫ スクリーニング ≫ ホストスクリーン512にて設定変更を行ってください。
- デフォルトで MDaemon IMAP, Webmail, ActiveSyncサーバーは無効化されたアカウントの共有フォルダに対するアクセスを許可しないようになりました。この設定は、サーバ設定 ≫ パブリック & 共有フォルダ107から変更できます。

Version 19.5.2

- サーバ設定 ≫ サーバー82 にある「*許可するRSETコマンドの最大値*」オプションはSMTPスクリーン514にある機能と重複しており、柔軟性を低下させる事から削除しました。SMTPスクリーンはダイナミックスクリーニングの一部で、アカウントの判定基準を広げる事ができます。（除外リストの有無、認証状態の配慮等）古い設定値はSMTPスクリーンへ移動するため、想定してい

る設定値と同じ設定になっているかどうかを確認してください。デフォルト値（且つ推奨値）はRSET最大値が**20**であり「ブロックされたIPのSMTPセッションを閉じる」が**チェックされ、有効になっている**状態です。

Version 19.5.1

- LetsEncrypt[541]機能が、ACME v2を使用するようにアップデートされました。このアップデートにより、LetsEncryptのご使用にあたりまして、ACME v1,PowerShell 5.1, Net Framework 4.7.2の使用ができる環境が必要となりました。

Version 19.5.0

- ¥MDaemon¥App¥MDaemon.iniファイルにあった、ライセンスキーなどの情報が、¥MDaemon¥LocalData¥LocalData.ini へと保存場所が変更されます。もし、以前のバージョンへ戻す必要が発生した際には、新しい場所へ移動したパラメータ値を認識できないため、ライセンスキーの再入力が求められることになります。このような手順を避けるため、MDaemon.iniの設定を新しいファイルへ移行するといった調整をお願いします。

Version 19.0.0

- MDaemonの Remote Administration（MDRA）のウェブインターフェイスが更にアップデートし、従来MDaemonの管理画面でのみ行えた多くの設定がMDRAからも行えるようになった他、MDRAからのみ行えるオプションも追加されました。新規インストールを行った際、スタートメニューにある"MDaemonを開始"ショートカットから、これまでのMDaemon管理画面ではなく、MDaemon Remote Administrationを開くブラウザが起動するようになりました。このデフォルトの動作を変更するには、¥MDaemon¥App¥MDaemon.iniファイル内の［MDLaunch］セクション内のパラメータ、OpenConfigSession=Yes/No と OpenRemoteAdmin=Yes/No にてご調整頂くか、スタートメニューの"MDaemon"から"MDaemon Configuration Sessionを開く"もしくは"MDaemon Remote Administrationを開く"を選んでご選択ください。もし、自動生成されたURLで起動できない場合や、外部Webサーバを使ってRemote Administrationをご使用の場合、管理画面から 設定≫WebとIMサービス≫Remote Administration≫Webサーバ[322]から、"Remote Administration URL"の設定を行なって下さい。最後に、Windowsのスタートメニューの MDaemonプログラムグループへ、MDaemon管理画面を起動とMDaemon Remote Administrationを起動が追加されました。
- SyncML対応を終了し、管理画面からも削除しました。
- MDaemonのディスク容量の計算方法が、いくつかの場所で一貫性がなかった（1K byteの計算で、ある場所では 1000、ある場所では 1024 byteでの計算という具合に）ため、1024 byte計算に統一しました。その結果、以前のバージョンとユーザーの使用ディスク容量の計算結果が変わることになります。設定値と照らし合わせて、必要に応じて設定をご調整下さい。
- "失敗時のみアンチウィルスのアップデート通知を行う[606]" オプションがデフォルト値になりました。MDaemon 19へアップデートした際、最初にMDaemonを起動したタイミングでこのオプションが有効化されます。

参照:

はじめに[12]

MDaemon Private Cloud 11.0の新機能[14]

MDaemonの管理画面[64]

1.5 サポート

サポートオプション

製品サポートはMDaemon Technologiesのお客様満足度における大きな役割の1つです。製品は最初の購入からサポートが付属しており、不具合修正なども順次行われています。日本語での製品サポートを受けるには、以下のMDaemon Technologiesのチャネルパートナーへお問い合わせをお願いします。詳しくは、www.mdaemon.com/support/ をご覧ください。

MDaemonベータテスト

MDaemon Technologiesは製品用のベータテスティングチームを保有しています。MDaemonベータチームへの参加方法については、 MDaemonBeta@mdaemon.comへお問合せ下さい。

ベータチームは、製品の一般公開前に、最新バージョンをテストする目的のものであり、テクニカルサポートはありません。MDaemonに対するテクニカルサポートは、下記のURLへ記載されている方法でのみ提供されます：
www.mdaemon.com/support/

連絡先窓口

営業時間
M-F 8:30 am - 5:30 pm Central Standard Time
Excludes weekends and U.S. holidays
Customer Service or Sales
U.S. Toll Free: 866-601-ALTN (2586)
International: 817-601-3222
sales@helpdesk.mdaemon.com

技術的なお問合せ
www.mdaemon.com/support/

教育に関するお問合せ
training@mdaemon.com

パートナーに関するお問合せ
alliance@mdaemon.com

メディア関連のお問合せ
press@mdaemon.com

リセラーの情報
チャネルパートナー ページをご覧ください。

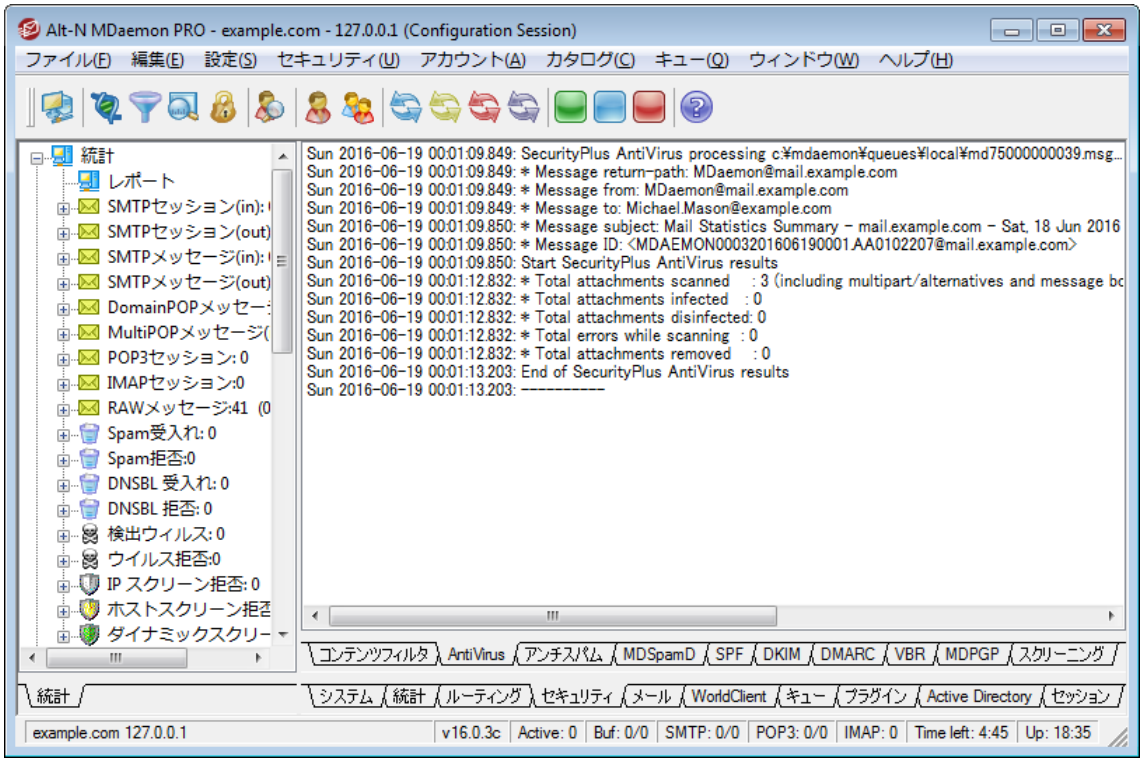
本社所在地

MDaemon Technologies, Ltd.
4550 State Highway 360, Suite 100
Grapevine, Texas 76051
U.S. Toll Free: 866-601-ALTN (2586)
International: 817-601-3222
Fax: 817-601-3223

商標

セクション 2

2 MDaemonの管理画面



MDaemonのメイングラフィカル管理画面(GUI)では、MDaemonのリソース、統計情報、アクティブなセッション、キューにある処理待ちのメール状況などに関する重要な情報が確認できます。また、この画面から、MDaemonに搭載されたサーバー機能の多くを有効化・無効化する事ができます。GUIのタブで分割された画面には、サーバ毎に、最新の送受信メールや接続状況が表示されています。

統計

統計画面のペインが、デフォルトでMDaemonのメイン画面の左側にあります。このペインは統計、キュー、アカウント、サーバの4つのセクションで構成されています。

*統計*セクションには、MDaemonが開始してから送受信されたメッセージの数やPOP3やIMAPセッション数などの統計情報が含まれています。受信や拒否したスパムやウィルスの数なども確認できます。メールカウンター統計アイテムには、カウントをリセットするための右クリックでのショートカットメニューが含まれています。

"ルートノードのカウンタをリセットする"オプションをクリックすると、右クリックで選択したカウンタだけでなく、全てのカウンタがリセットされます。なお、[設定 >> 初期設定 >> GUI]では[*再起動時にルートノードメールカウンタを保持する*]機能を使用することができます。この機能が有効でない場合は、サーバが再起動する度に、カウンタがリセットされます。

アカウント セクションにはMDaemon, MDaemon Connector, ActiveSync用のエントリが表示されています。それぞれのエントリには使用したアカウント数と残りのアカウント数が、お持ちのライセンス数に合わせて表示されています。

キューセクションでは、メッセージキュー毎のエントリと、各キューに含まれるメールの数が確認できます。各キューを右クリックすると、キューの種類によって、次の中から選択できる1つ又はそれ以上のショートカットメニューが表示されます。

キューを表示
このオプションは、メイン画面を選択したキューの画面に切り替え、キューの中のメッセージ一覧が表示されます。表示されるメッセージを右クリックすると、コピー、移動、編集、といった、キュー/統計マネージャで利用できるオプションに似たショートカットメニューが表示されます。

キュー/統計マネージャ
メイン画面を[キューおよび統計マネージャ]の画面に切り替え、キューの中のメッセージ一覧が表示されます。

すぐに処理
このオプションは、キューに含まれるすべてのメッセージを再度キューに入れ、通常の配信を試みます。Holding,Badのようなキューに含まれるメッセージを処理する場合、同じエラーにより、元のキューに戻される可能性があります。

キューを凍結/解除
対象キューの処理を一時的に停止したり、停止中の処理を再開します。

解放
Holdingキューからメッセージを解放します。MDaemonは、前回発生したエラーに関係なくメールの配信を試みます。メッセージがHoldingキューに入るきっかけになったエラーと同様のエラーが発生しても、このメッセージはHoldingキューには戻されません。

再度キューに入れる
これはHoldingキューで選択できるオプションで、上記の*すぐに処理*と同じ機能を持ちます。

キューを有効/無効にする
Holdingキューを有効または無効にします。無効の場合、メッセージはエラーの種類に関わらず、Holdingキューにいれられることはありません。

*サーバ*セクションにはMDaemon内の各サーバについてのエントリがあり、各エントリは「アクティブ」「非アクティブ」といった、サーバの現在の状態を表示しています。サーバエントリの下には、ドメイン毎のサーバーのエントリが、使用中のポートとIPアドレスと併せて表示されます。ショートカットメニューでは、各サーバのアクティブと非アクティブの切り替えが行えます。サーバがアクティブでない時、アイコンは赤に変わります。

イベント監視とログ

デフォルトで、管理画面の右側には、MDaemonの各サーバおよびリソースの、現在の動作および状態を表示するグループ毎のタブがあり、現在のサーバ状況を反映するために絶えず更新されています。各動作が完了する度に、アクティブなセッションとサーバ動作は該当する画面へ記録されます。アクティビティをログへ記録するよう設定した場合、これらの画面で表示される情報はLOGディレクトリのログファイルに反映されます。

MDaemonのメイン画面には、次のタブが含まれています。

システム
プログラムの起動の際、システムタブは初期化処理のログを表示し、MDaemonの構成または

状況に関して、問題となる可能性があるかどうかの判断に役立ちます。さらにMDaemonの各種サーバの有効/無効といったアクティビティを表示します。

統計
この画面では、統計とツールのペインにある、統計画面の中の、様々なルートノードカウンタに含まれる情報に関連したサーバに関する統計レポートが表示されます。このレポートのフォントや文字のサイズを変更する場合は、MDaemon.iniファイルで以下のキーを編集してください。

```
[ReportWindow]
DefFontFace=Courier New
DefFontHeigh=15
DefFontWidth=7
```

さらに、Postmasterとコンテンツフィルタで指定された受信者[606]アドレスに対して、毎日深夜に、メールでレポートが送信されます。このレポートは[一般的なメール管理[819]]で説明している[Status]コマンドで生成されるレポートと同じものです。このレポートが不要な場合は、初期設定画面の「その他[459]」にある*"深夜にpostmasterへレポートを送信する"*オプションを無効にして下さい。

ルーティング — MDaemonによって解析された各メッセージの宛先、送信者、メッセージIDなどのルーティング情報を表示します。

セキュリティ — このタブをクリックすると、セキュリティに関連するタブが上部に表示されます。

コンテンツフィルタ — MDaemonのコンテンツフィルタ[588]の実行内容が、この画面に表示されます。コンテンツフィルタのメッセージルールの条件に一致すると、対象メールに関連する情報と行ったアクションが、この画面に記録されます。

AntiVirus — AntiVirusアクティビティが、この画面に表示されます。 メッセージでウィルスが検知されると、関連情報とウィルス検知時のアクションについて、この画面に記録されます。

アンチスパム — MDaemonのスパムフィルタリング[616]と保護アクティビティを表示します。

MDSpamD — MDaemon Spam Daemon[625]の全アクティビティを表示します。

SPF — Sender Policy Framework[479]の全アクティビティを表示します。

DKIM — DomainKeys Identified Mail[481]の全アクティビティを表示します。

DMARC —DMARC[488]の全アクティビティを表示します。

VBR — VBRメッセージ証明書[501]の全アクティビティを表示します。

MDPGP — MDPGP[574]の全アクティビティを表示します。

スクリーニング — ターピット[548]とダイナミックスクリーニング[514]の全アクティビティを表示します。

認証失敗 — このタブ(と関連するログファイル)には全てのSMTP、IMAP、POPログオンの失敗が記録されます。情報には使用したプロトコル、セッションID(これで他のログファイルを検索できます)、接続元IP、ログオンで使用した値(エイリアスの場合もあります)、ログオンに紐づいたアカウント(又は'none')が含まれます。タブの中の対象行を右クリックし、IPアドレスをブロックリストへ登録できます。

MTA-STS — 全てのSMTP MTA Strict Transport Security (MTA-STS) 関連アクティビティを表示します。

メール — このタブをクリックすると、メール関連タブが上部に表示されます。

SMTP (in) — SMTPプロトコルを使用したすべての受信セッションが表示されます。

SMTP (out) — SMTPプロトコルを使用したすべての送信セッションが表示されます。

IMAP — IMAPプロトコルを使用したメールセッションが表示されます。

POP3 — POP3プロトコルでMDaemonからメールを受信した場合、そのアクティビティが表示されます。

MultiPOP — MDaemonのMultiPOPでのメール受信に関するアクティビティが表示されます。

DomainPOP — MDaemonのDomainPOPアクティビティが表示されます。

LDAP — LDAPサーバのアクティビティが表示されます。

Minger — Minger[785]サーバのアクティビティが表示されます。

RAW — RAWあるいはシステムが生成したメッセージアクティビティが表示されます。

MDaemon Connector — すべてのMDaemon Connectorのアクティビティが表示されます。

Webmail

Webmail — すべてのWebmailのアクティビティが表示されます。

ActiveSync — ActiveSyncのアクティビティが表示されます。

キュー — このタブをクリックすると、Local、Remote、Holding、Quarantine、Bayesian、スパムなどの、各メッセージキューに対応したタブが表示されます。

プラグイン — MDaemonのプラグインに関するすべてのアクティビティが表示されます。

Active Directory — Active Directoryの動作に関連したログが表示されます。

セッション — このタブをクリックすると、MDaemonへの接続方法毎のタブが上部に表示されます。接続がSMTPでの送受信、IMAP、Webmail、ActiveSyncのどれかに該当すれば、それぞれのアクティブなセッションがここで表示されます。アクティブセッションをダブルクリックすると、セッションウィンドウ[77]が起動しSMTPセッションで行われている処理内容をリアルタイムで確認できます。

これらのタブに表示される情報は、ログファイルに実際に格納されるデータ量へ影響を及ぼすことはありません。ただし、MDaemonは、ファイルに記録されるログの種類や量に対して、高い柔軟性も持っています。ログに関する詳細情報はロギング[150]ダイアログを参照してください。

イベント監視ウィンドウのショートカットメニュー

イベント追跡ウィンドウを右クリックすると、ショートカットメニューが表示されます。ここでは、選択、コピー、削除、印刷といった様々なオプションを使用できます。**印刷/コピー**では、選択されている画面をメモ帳で開くことができ、そのデータを印刷、ファイルに保存することができます。**削除**では選択したテキストを削除することができます。**検索**では、ログファイルを検索するための単語やフレーズを入力するウィンドウを開き、その文字列が含まれるすべてのログファイルを検索と、その文字列が含まれるセッションの記録を検索し、notepadを使った確認が行えるよう、検索結果を1ファイルへ出力します。この機能の利用例としては、全てのセッション情報を含むログから特定のメッセージIDを検索する、といったものです。タブの中に、誤検知や検出漏れをMDaemon.comへレポートとして送信するオプションを追加しました。レポートとして送られたメッセージは解析され、外部ベンダーへ正常な検出用に提出されます。

MDaemon GUIのレイアウトは、上記のデフォルトのレイアウト以外の配置も行えます。メニューバーから[**ウィンドウ>> ペインを切り替え**]で、ペインの位置を切り替えることができます。

コンポジットログの表示

MDaemonのメニューバーの[**ウィンドウ**]メニューに、[**コンポジットログ表示**]オプションがあります。このオプションをクリックすると、メイン画面のタブ毎に表示された情報を1つに統合したウィンドウが、メイン画面に追加されます。このウィンドウへ表示される情報は、ロギングの中のコンポジットログ[152]画面のオプションから設定が行えます。

パフォーマンスカウンタ

MDaemonはWindowsパフォーマンスカウンタに対応しており、MDaemonのステータスをリアルタイムで監視する事ができます。プロトコル毎のアクティブセッション数、キューの中のメール数、サーバーのアクティブ・インアクティブステータス、MDaemonの稼働時間、セッションとメールの統計を表示するカウンタがあります。

パフォーマンスカウンタを使用するには、コントロールパネル | 管理ツール | パフォーマンスのシステムモニタを開始するか、"perfmon"を実行します。32-bitカウンターを使用する場合は、"mmc /32 perfmon.msc"を実行します。 カウンタの追加をクリックし、MDaemonのパフォーマンスオブジェクトを選択し、確認したいカウンタを選択して追加をクリックします。他のマシンで稼働しているMDaemonのパフォーマンスカウンタを表示するには「リモートレジストリ」サービスを起動し、ファイアウォールの設定を行う必要があります。

参照:

セッションウィンドウ[77]
トレーアイコン[75]
ショートカットメニュー[76]
コンポジットログ[152]

2. .1 AutoDiscoveryサービス

MDaemonは、メールサーバー名やポートといった詳細情報の代わりに、メールアドレスとパスワードだけでメーラーがアカウントに接続できるようになる、AutoDiscoveryサービスに対応してます。ほとんどのクライアントはこのサービスに対応していますが、中には限定的に対応しているものもあります。AutoDiscoveryサービスはデフォルトで有効ですが、MDaemonのメイン管理画面から手動で有効化や無効化を行う事もできます。統計画面の**サーバー**の下の**AutoDiscoveryサービス**を右クリックし、**AutoDiscoveryサービスの有効化/無効化**が行えます。

Clients in which the AutoDiscoveryサービスに完全対応しているクライアントはユーザーのメールアドレスのドメイン名を DNSサービス(SRV)レコードで、_autodiscover._tcpサービスタイプのルックアップとサーバーから追加の情報取得を行うのに使用します。そのため、AutoDiscovery対応には、AutoDiscoveryとこれに対応するサービス用のDNS SRVレコードを作成する必要があります。

MDaemonのAutoDiscoveryサービスは次の機能に実装されています: ActiveSync 379 (airsync), IMAP, POP, SMTP, DAV, XMPP

```
_autodiscover._tcp  SRV 0 0 443 adsc.example.com.
_airsync._tcp       SRV 0 0 443 eas.example.com.
_imap._tcp          SRV 0 0 0   imap4.example.com.
_pop._tcp           SRV 0 0 0   pop3.example.com.
_smtp._tcp          SRV 0 0 0   msa.example.com.
_caldav._tcp        SRV 0 0 0   dav.example.com.
_carddav._tcp       SRV 0 0 0   dav.example.com.
_xmpp-client._tcp   SRV 0 0 0   chat.example.com.
```

注意点: クライアントの中には、必ず最初に`autodiscover.{domain}.{tld}` を確認するものもあります。そのため、AutoDiscoveryサービスレポートが autodiscover.{domain}.{tld} という名前のサーバーに関連付けられている事が役に立つ場合もあります。次の例では、AutoDiscoveryサーバーを adsc.example.comとしています。

例:

ドメイン名: example.com

管理者は サービスタイプ_autodiscover用に、_tcp serviceレコードを設定します。

```
_autodiscover._tcp SRV 0 0 443 adsc.example.com.
```

この場合、レコードは adsc.example.comを指しており、Aレコードとして 192.168.0.101を指しています。

クライアントはサーバーへ接続し、 ActiveSync, IMAP, XMPP, SMTP, DAVといった特定のプロトコル用に、接続先へ情報の問合せを行います。

AutoDiscoveryサービスはリクエストされたプロトコルのルックアップを行い、プロトコル用の正しいサーバー名を応答として返します。例:ActiveSyncは サービスレコード_airsyncの_tcpで定義されているサーバー名を返し、この例では、 eas.{domain}.{tld} となります。

OutlookがAutoDiscoveryを呼び出すと、_imap や _msaの_tcpサービスレコードを指している、IMAPやSMTP サーバーを返します。これは例えば、imap4.example.com や msa.example.com といった応答になります。

これは Auto Discoveryサービスの正しい設定例となります。 この例では各プロトコルにそれぞれ固有の名前を割り当てると仮定していますが、mail.example.comといった、共通の名前を使用する方が簡単に設定が行えます。

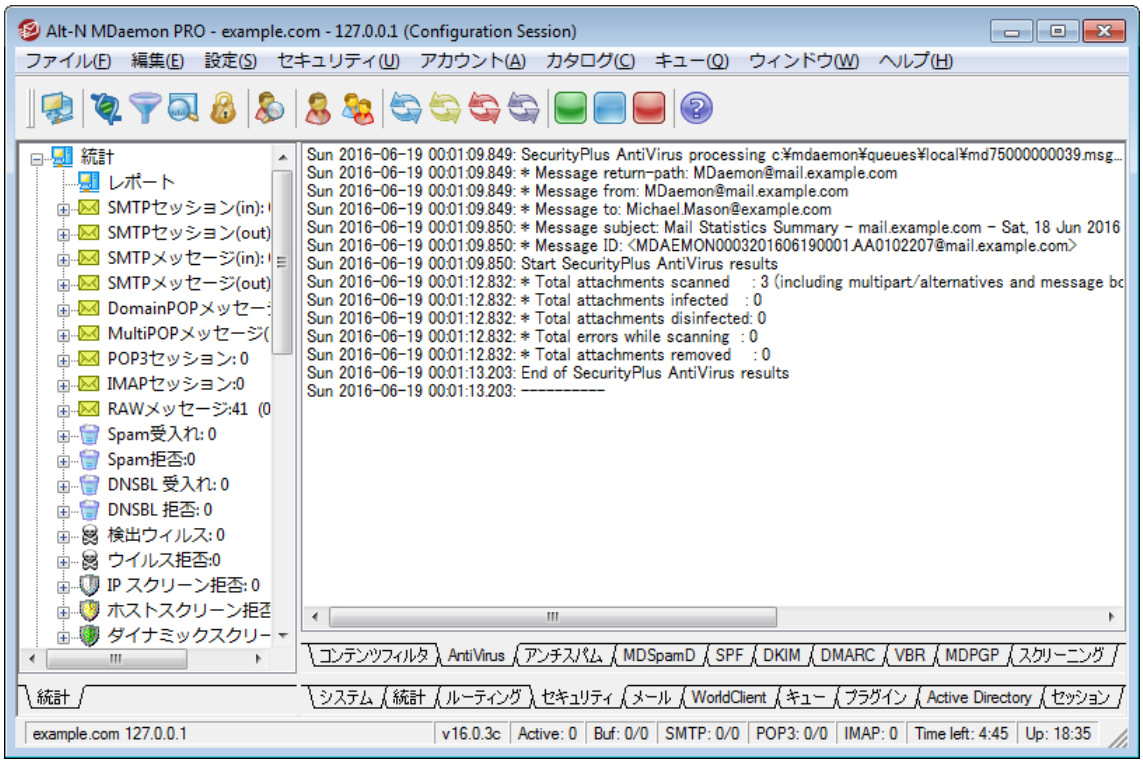
```
;
;  Database file example.com.dns for example.com zone.
;

@ IN  SOA dns.mydnsprovider.org. hostmaster.mydnsprovider.org. (
        4            ; serial number
        900          ; refresh
        600          ; retry
        86400        ; expire
        3600       ) ; default TTL
```

```
;
;  Zone NS records
;

@       NS dns.mydnsprovider.org

;
;  Zone records
;

@             A 192.168.0.100
adsc                A 192.168.0.101
www                 A 192.168.0.102
imap4               A 192.168.0.103
pop3                A 192.168.0.104
msa                 A 192.168.0.105
eas                 A 192.168.0.106
api                 A 192.168.0.107
autodiscover        A 192.168.0.108
dav                 A 192.168.0.109
chat                A 192.168.0.110
inbound       A 192.168.0.111

              MX 10 inbound.example.com.
;
;  Service records
;

_autodiscover._tcp  SRV 0 0 443 adsc.example.com.
_airsync._tcp       SRV 0 0 443 eas.example.com.
_imap._tcp          SRV 0 0 0   imap4.example.com.
_pop._tcp           SRV 0 0 0   pop3.example.com.
_smtp._tcp          SRV 0 0 0   msa.example.com.
_caldav._tcp        SRV 0 0 0   dav.example.com.
_carddav._tcp       SRV 0 0 0   dav.example.com.
_xmpp-client._tcp   SRV 0 0 0   chat.example.com.
```

参照:

AutoDiscoverについての一般的な情報は、次のMicrosoftのページをご覧下さい: Autodiscover for Exchange.

2.2 イベント監視とログ



MDaemonのメイングラフィカル管理画面(GUI)では、MDaemonのリソース、統計情報、アクティブなセッション、キューにある処理待ちのメール状況などに関する重要な情報が確認できます。また、この画面から、MDaemonに搭載されたサーバー機能の多くを有効化・無効化する事ができます。GUIのタブで分割された画面には、サーバ毎に、最新の送受信メールや接続状況が表示されています。

統計

統計画面のペインが、デフォルトでMDaemonのメイン画面の左側にあります。このペインは統計、キュー、アカウント、サーバの4つのセクションで構成されています。

*統計*セクションには、MDaemonが開始してから送受信されたメッセージの数やPOP3やIMAPセッション数などの統計情報が含まれています。受信や拒否したスパムやウィルスの数なども確認できます。メールカウンター統計アイテムには、カウントをリセットするための右クリックでのショートカットメニューが含まれています。

"ルートノードのカウンタをリセットする"オプションをクリックすると、右クリックで選択したカウンタだけでなく、全てのカウンタがリセットされます。なお、[設定 >> 初期設定 >> GUI]では[*再起動時にルートノードメールカウンタを保持する*]機能を使用することができます。この機能が有効でない場合は、サーバが再起動する度に、カウンタがリセットされます。

アカウント セクションにはMDaemon, MDaemon Connector, ActiveSync用のエントリが表示されています。それぞれのエントリには使用したアカウント数と残りのアカウント数が、お持ちのライセンス数に合わせて表示されています。

キューセクションでは、メッセージキュー毎のエントリと、各キューに含まれるメールの数が確認できます。各キューを右クリックすると、キューの種類によって、次の中から選択できる1つ又はそれ以上のショートカットメニューが表示されます。

キューを表示
このオプションは、メイン画面を選択したキューの画面に切り替え、キューの中のメッセージ一覧が表示されます。表示されるメッセージを右クリックすると、コピー、移動、編集、といった、キュー/統計マネージャで利用できるオプションに似たショートカットメニューが表示されます。

キュー/統計マネージャ
メイン画面を[キューおよび統計マネージャ]の画面に切り替え、キューの中のメッセージ一覧が表示されます。

すぐに処理
このオプションは、キューに含まれるすべてのメッセージを再度キューに入れ、通常の配信を試みます。Holding,Badのようなキューに含まれるメッセージを処理する場合、同じエラーにより、元のキューに戻される可能性があります。

キューを凍結/解除
対象キューの処理を一時的に停止したり、停止中の処理を再開します。

解放
Holdingキューからメッセージを解放します。MDaemonは、前回発生したエラーに関係なくメールの配信を試みます。メッセージがHoldingキューに入るきっかけになったエラーと同様のエラーが発生しても、このメッセージはHoldingキューには戻されません。

再度キューに入れる
これはHoldingキューで選択できるオプションで、上記の*すぐに処理*と同じ機能を持ちます。

キューを有効/無効にする
Holdingキューを有効または無効にします。無効の場合、メッセージはエラーの種類に関わらず、Holdingキューにいれられることはありません。

*サーバ*セクションにはMDaemon内の各サーバについてのエントリがあり、各エントリは「アクティブ」「非アクティブ」といった、サーバの現在の状態を表示しています。サーバエントリの下には、ドメイン毎のサーバーのエントリが、使用中のポートとIPアドレスと併せて表示されます。ショートカットメニューでは、各サーバのアクティブと非アクティブの切り替えが行えます。サーバがアクティブでない時、アイコンは赤に変わります。

イベント監視とログ

デフォルトで、管理画面の右側には、MDaemonの各サーバおよびリソースの、現在の動作および状態を表示するグループ毎のタブがあり、現在のサーバ状況を反映するために絶えず更新されています。各動作が完了する度に、アクティブなセッションとサーバ動作は該当する画面へ記録されます。アクティビティをログへ記録するよう設定した場合、これらの画面で表示される情報はLOGディレクトリのログファイルに反映されます。

MDaemonのメイン画面には、次のタブが含まれています。

システム
プログラムの起動の際、システムタブは初期化処理のログを表示し、MDaemonの構成または

状況に関して、問題となる可能性があるかどうかの判断に役立ちます。さらにMDaemonの各種サーバの有効/無効といったアクティビティを表示します。

統計

この画面では、統計とツールのペインにある、統計画面の中の、様々なルートノードカウンタに含まれる情報に関連したサーバに関する統計レポートが表示されます。このレポートのフォントや文字のサイズを変更する場合は、MDaemon.iniファイルで以下のキーを編集してください。

```
[ReportWindow]
DefFontFace=Courier New
DefFontHeigh=15
DefFontWidth=7
```

さらに、Postmasterとコンテンツフィルタで指定された受信者[606]アドレスに対して、毎日深夜に、メールでレポートが送信されます。このレポートは[一般的なメール管理[819]]で説明している[Status]コマンドで生成されるレポートと同じものです。このレポートが不要な場合は、初期設定画面の「その他[459]」にある*"深夜にpostmasterへレポートを送信する"*オプションを無効にして下さい。

ルーティング — MDaemonによって解析された各メッセージの宛先、送信者、メッセージIDなどのルーティング情報を表示します。

セキュリティ — このタブをクリックすると、セキュリティに関連するタブが上部に表示されます。

コンテンツフィルタ — MDaemonのコンテンツフィルタ[588]の実行内容が、この画面に表示されます。コンテンツフィルタのメッセージルールの条件に一致すると、対象メールに関連する情報と行ったアクションが、この画面に記録されます。

AntiVirus — AntiVirusアクティビティが、この画面に表示されます。 メッセージでウィルスが検知されると、関連情報とウィルス検知時のアクションについて、この画面に記録されます。

アンチスパム — MDaemonのスパムフィルタリング[616]と保護アクティビティを表示します。

MDSpamD — MDaemon Spam Daemon[625]の全アクティビティを表示します。

SPF — Sender Policy Framework[479]の全アクティビティを表示します。

DKIM — DomainKeys Identified Mail[481]の全アクティビティを表示します。

DMARC —DMARC[488]の全アクティビティを表示します。

VBR — VBRメッセージ証明書[501]の全アクティビティを表示します。

MDPGP — MDPGP[574]の全アクティビティを表示します。

スクリーニング — ターピット[548]とダイナミックスクリーニング[514]の全アクティビティを表示します。

認証失敗 — このタブ（と関連するログファイル）には全てのSMTP、IMAP、POPログオンの失敗が記録されます。情報には使用したプロトコル、セッションID（これで他のログファイルを検索できます）、接続元IP、ログオンで使用した値（エイリアスの場合もあります）、ログオンに紐づいたアカウント（又は'none'）が含まれます。タブの中の対象行を右クリックし、IPアドレスをブロックリストへ登録できます。

MTA-STS — 全てのSMTP MTA Strict Transport Security（MTA-STS）関連アクティビティを表示します。

メール — このタブをクリックすると、メール関連タブが上部に表示されます。

SMTP (in) — SMTPプロトコルを使用したすべての受信セッションが表示されます。

SMTP (out) — SMTPプロトコルを使用したすべての送信セッションが表示されます。

IMAP — IMAPプロトコルを使用したメールセッションが表示されます。

POP3 — POP3プロトコルでMDaemonからメールを受信した場合、そのアクティビティが表示されます。

MultiPOP — MDaemonのMultiPOPでのメール受信に関するアクティビティが表示されます。

DomainPOP — MDaemonのDomainPOPアクティビティが表示されます。

LDAP — LDAPサーバのアクティビティが表示されます。

Minger — Minger[785]サーバのアクティビティが表示されます。

RAW — RAWあるいはシステムが生成したメッセージアクティビティが表示されます。

MDaemon Connector — すべてのMDaemon Connectorのアクティビティが表示されます。

Webmail

Webmail — すべてのWebmailのアクティビティが表示されます。

ActiveSync — ActiveSyncのアクティビティが表示されます。

キュー — このタブをクリックすると、Local、Remote、Holding、Quarantine、Bayesian、スパムなどの、各メッセージキューに対応したタブが表示されます。

プラグイン — MDaemonのプラグインに関するすべてのアクティビティが表示されます。

Active Directory — Active Directoryの動作に関連したログが表示されます。

セッション — このタブをクリックすると、MDaemonへの接続方法毎のタブが上部に表示されます。接続がSMTPでの送受信、IMAP、Webmail、ActiveSyncのどれかに該当すれば、それぞれのアクティブなセッションがここで表示されます。アクティブセッションをダブルクリックすると、セッションウィンドウ[77]が起動しSMTPセッションで行われている処理内容をリアルタイムで確認できます。

これらのタブに表示される情報は、ログファイルに実際に格納されるデータ量へ影響を及ぼすことはありません。ただし、MDaemonは、ファイルに記録されるログの種類や量に対して、高い柔軟性も持っています。ログに関する詳細情報はロギング[150]ダイアログを参照してください。

イベント監視ウィンドウのショートカットメニュー

イベント追跡ウィンドウを右クリックすると、ショートカットメニューが表示されます。ここでは、選択、コピー、削除、印刷といった様々なオプションを使用できます。**印刷/コピー**では、選択されている画面をメモ帳で開くことができ、そのデータを印刷、ファイルに保存することができます。**削除**では選択したテキストを削除することができます。**検索**では、ログファイルを検索するための単語やフレーズを入力するウィンドウを開き、その文字列が含まれるすべてのログファイルを検索と、その文字列が含まれるセッションの記録を検索し、notepadを使った確認が行えるよう、検索結果を1ファイルへ出力します。この機能の利用例としては、全てのセッション情報を含むログから特定のメッセージIDを検索する、といったものです。タブの中に、誤検知や検出漏れをMDaemon.comへレポートとして送信するオプションを追加しました。レポートとして送られたメッセージは解析され、外部ベンダーへ正常な検出用に提出されます。

MDaemon GUIのレイアウトは、上記のデフォルトのレイアウト以外の配置も行えます。メニューバーから[**ウィンドウ > > ペインを切り替え**]で、ペインの位置を切り替えることができます。

コンポジットログの表示

MDaemonのメニューバーの[**ウィンドウ**]メニューに、[**コンポジットログ表示**]オプションがあります。このオプションをクリックすると、メイン画面のタブ毎に表示された情報を1つに統合したウィンドウが、メイン画面に追加されます。このウィンドウへ表示される情報は、ロギングの中のコンポジットログ[152]画面のオプションから設定が行えます。

パフォーマンスカウンタ

MDaemonはWindowsパフォーマンスカウンタに対応しており、MDaemonのステータスをリアルタイムで監視する事ができます。プロトコル毎のアクティブセッション数、キューの中のメール数、サーバーのアクティブ・インアクティブステータス、MDaemonの稼働時間、セッションとメールの統計を表示するカウンタがあります。

パフォーマンスカウンタを使用するには、コントロールパネル | 管理ツール | パフォーマンスのシステムモニタを開始するか、"perfmon"を実行します。32-bitカウンターを使用する場合は、"mmc /32 perfmon.msc"を実行します。 カウンタの追加をクリックし、MDaemonのパフォーマンスオブジェクトを選択し、確認したいカウンタを選択して追加をクリックします。他のマシンで稼働しているMDaemonのパフォーマンスカウンタを表示するには「リモートレジストリ」サービスを起動し、ファイアウォールの設定を行う必要があります。

参照:

セッションウィンドウ[77]
トレーアイコン[75]
ショートカットメニュー[76]
コンポジットログ[152]

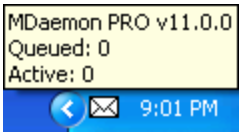
2.4 トレイアイコン

MDaemonサーバが実行されている時は、常にシステムトレイにアイコンが表示されます。このアイコンは、単にサーバが実行されているかどうかを知らせるだけではなく、現在のサーバの状態をその色によってリアルタイムに表示します。色の変化についての詳細は次の通りです。

✉	正常に稼動中です。リモートあるいはローカルキューにメールはありません。

	正常に稼動中です。リモートあるいはローカルキューにメールがあります。
	利用可能なディスクの空きが設定値よりも少なくなっている。(参照: 設定 >> 初期設定 >> ディスク452)
	ネットワークのダウン、ダイアルアップの失敗またはディスクの空きがない。
アイコンの点滅	MDaemonの新規バージョンが利用可能。

アイコンのツールヒントによって、追加情報が利用可能なサーバについてあります。マウスポインタをアイコンに重ねるとツールヒントが現れます。現在、キューにあるメッセージおよびアクティブなセッション数を表示します。



ショートカットメニュー

タスクトレイにあるMDaemonのアイコンを右クリックすると、ショートカットメニューが現れます。このメニューから、MDaemonのメイン画面を開くことなく、ほとんどのメニューと機能にアクセスすることができます。

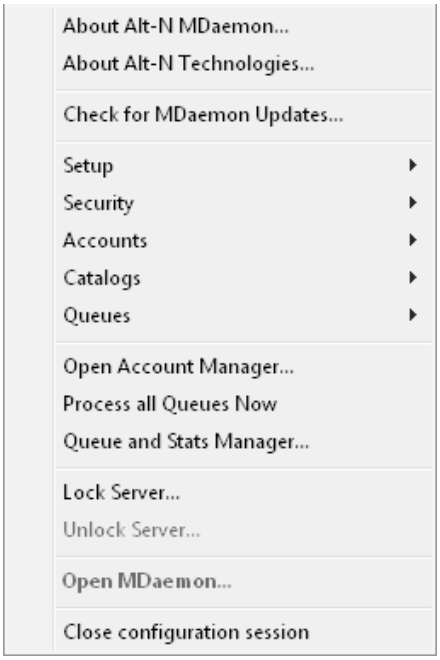
メニューの一番上にある[About MDaemon…]をクリックすると、MDaemonとMDaemon Technologies社に関する情報が表示されます。

次のセクションには、"MDaemonのアップデートをチェック…"があります。新しいバージョンが利用可能な場合にはダウンロードを行うことができます。

3番目のセクションでは、MDaemonメニューにもある、設定、セキュリティ、アカウント、キューにアクセスできます。これらのメニューは、メイン画面のメニューバーにある各項目と同じものです。

4番目のセクションには、アカウントマネージャ、キューの処理、すべてのキューを処理するキュー/統計マネージャを開くオプションがあります。

次のセクションには、MDaemonのインターフェイスをロックあるいはアンロックするためのコマンド(次の"MDaemonのメイン画面のロックとアンロック"を参



照）があり、さらに次のセクションには、"MDaemonを開く..."があり、システムトレイに最小化されているMDaemonを復元します。

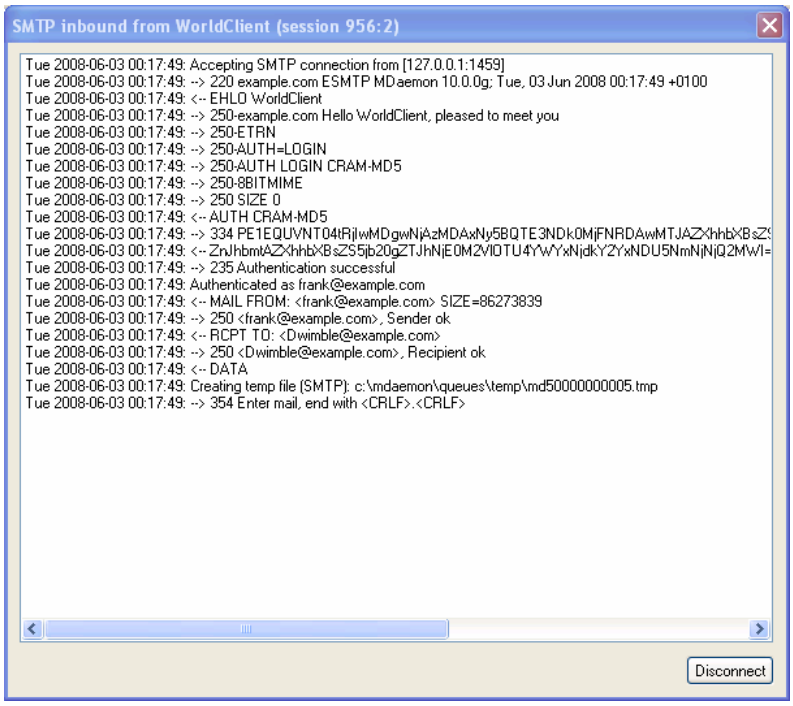
最後は、"Configuration Sessionを終了"で、MDaemonの管理画面を終了します。Configuration Sessionを終了してもMDaemonサービスを終了する訳ではありません。

MDaemon管理画面のロックとアンロック

MDaemonを最小化して、ユーザインターフェイスをロックするには、"**サーバをロック**..."をクリックし、開いたダイアログにパスワードを入力してください。パスワードを確認するために2回入力すると、ユーザインターフェイスはロックされ、MDaemonは通常通りに稼動を続けます。しかし、同じメニューにある[すべてのキューを処理する…]オプションはこの状態においても使用可能で、このコントロールによって、キューにあるメールを手動で処理することができます。MDaemonをアンロックするには、トレイアイコンをダブルクリックして[MDaemonをアンロックする]ダイアログを開くか、またはトレイアイコンを右クリックして"サーバを解除.."を選択し、ロック時に入力したパスワードを入力するとロックが解除されます。

2.5 セッションウィンドウ

メインGUIのセッション画面 65の中で、アクティブなセッションをダブルクリックすると、そのエントリに対応するセッションウィンドウを開きます。セッションウィンドウは、進行中のセッションのSMTP処理を表示します。切断ボタンをクリックすると、進行中のセッションを中断する事ができます。



2.6 MDaemonのSMTPワークフロー

SMTPからの通信を受け付けると、MDaemonは、メール配信を許可するかどうかを判断と、その後の実際の配送のために、複雑な処理を行います。以下のチャートはSMTPでメールを受け付けた際のワークフローを示したものです。

ステップの実行範囲はそれぞれの設定により異なります。設定が無効になっている場合、1つ以上のステップがスキップされる事があります。

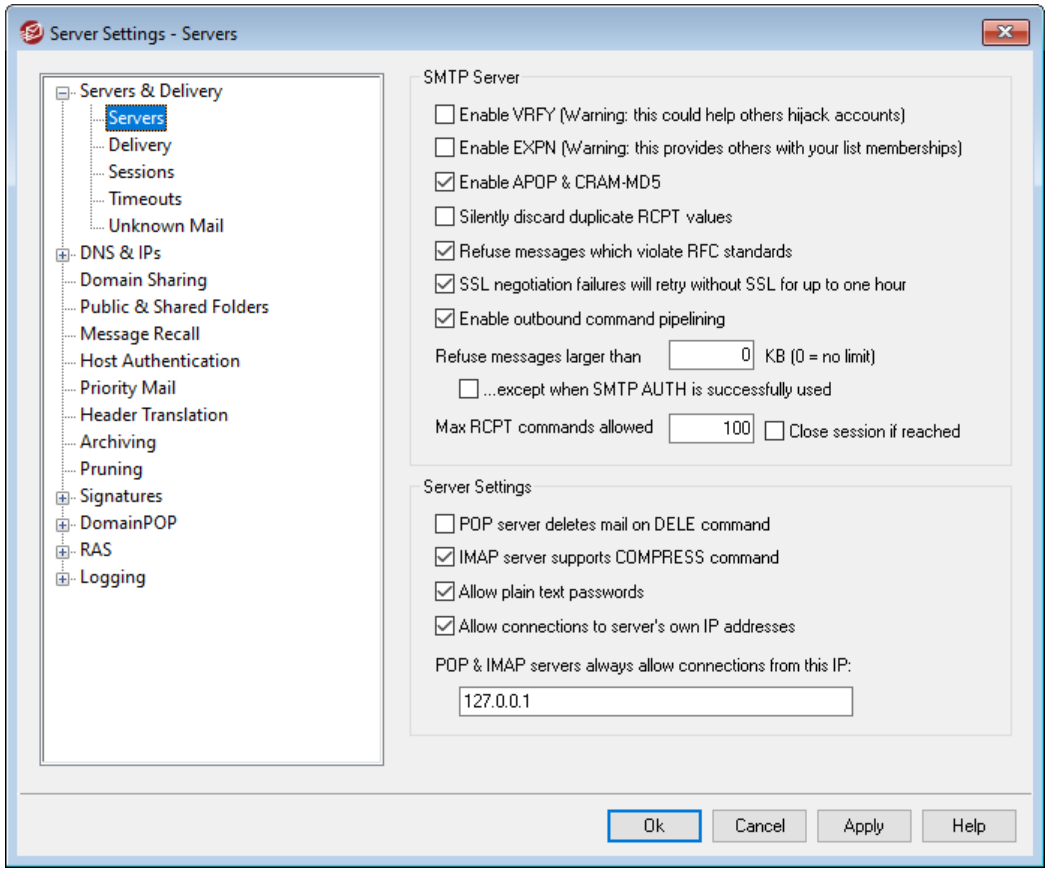
セクション 3

3 設定メニュー

3.1 サーバ設定

3.1.1 サーバ & 配信

3.1.1.1 サーバ



SMTPサーバ

VRFYを許可
このスイッチをクリックするとSMTP VRFYコマンドに応答します。このコマンドは、SMTPの着信転送(Call forward)やコールバック(Call back)機能をもつサーバーが、メールアドレスの存在を確認するのに使用される場合があります。この機能は、デフォルトで無効になっています。

EXPNを許可
MDaemonでEXPNコマンドを許可する場合に、このチェックボックスを選択します。

APOP と CRAM-MD5を受け入れる

デフォルトで(POP、IMAPなどの)MDaemonサーバは、APOPやCRAM-MD5の方式によるユーザー認証を許可していません。こうした認証方式は復元可能な暗号方式でパスワードを保存しなくてはならず、これはセキュリティ上、MDaemonや管理者、攻撃者によってパスワードが復元されてしまう可能性があることからおすすめしていません。また、このオプションは、パスワードオプション[778]の「メールボックスパスワードを復元きない暗号化方式で保持する」やActive Directory認証とも互換性がありません。しかしながら、SSL/TLSを使っていない場合は、APOPやCRAM-MD5を使って、クリアテキストでパスワード送信を行う事なく、追加のセキュリティを付与することができます。

重複したRCPT値があった場合、重複分を無視する

同一のSMTPセッションで重複した宛先があった場合、これをSMTPサーバーが無視するにはこのオプションを有効にします。MDaemonはこうしたメールを許可し、重複した宛先を無視するようになります。このオプションはデフォルトで無効になっています。

RFCに準拠していないメッセージを拒否する

RFCインターネット標準に準拠していないメールをSMTPプロセス中に拒否する場合はこのオプションを有効にします。メッセージがコンプライアンステストを通過するには次の条件を満たしている必要があります。

1. サイズが32バイトを超える(これはすべての必要なパーツを含むのに必要な最低サイズです)。
2. 1つのFROM: またはSENDER: ヘッダを持つ。
3. 1つ以上のFROM: ヘッダを持たない。
4. (必ずしもSUBJECTヘッダは必須ではないが)、1つ以上のSUBJECT: ヘッダを持たない。

認証を通過したものや、信頼するドメインやIPからのメールについては、この条件から除外されます。

SSLのネゴシエーションに失敗した場合最大1時間SSLを使わずにリトライする

送信SMTPセッション中にSSLエラーが発生した際、一時的にSSLを使わずにリトライを行う場合はこのオプションを使用します。

送信コマンドパイプラインを有効にする

デフォルトでMDaemonは SMTP Service Extension for Command Pipelining (RFC 2920)に対応しており、MAIL, RCPT, DATAコマンドを個別ではなくバッチで送信する事で、負荷の高いサイトのパフォーマンスを改善できます。SMTPパイプラインは受信接続では常に使われていて、送信接続用にもデフォルトで有効です。送信接続にパイプラインを使用しない場合は、このオプションを無効にしてください。

指定サイズ以上のメッセージを拒否する(0=無制限)

MDaemonで指定サイズを超えるメッセージの受付や処理を禁止する場合は、ここでサイズを指定します。この機能が有効な場合、MDaemonは、RFC-1870で指定されるESMTP SIZEコマンドを使用します。送信エージェントがこのSMTP拡張機能をサポートする場合、MDaemonは、実際に配信する前にメッセージサイズを調べ、即座にメッセージを遮断します。送信エージェントが、このSMTP拡張をサポートしない場合、MDaemonはメッセージの受け入れを開始する必要があり、転送中に定期的にサイズを調査して、一度処理が完了すると、最終的にメッセージを配信することを拒否します。サイズ制限を設定しない場合、このオプションを0にします。認証されたセッションをSIZEチェックから除外するには、後述の「ただし認証されたSMTPセッションは除く」をチェックします。

...SMTPセッションが正常に通った場合は除く

このオプションを有効にするとSMTPセッションが認証された場合にメッセージサイズのチェックから除外されます。

RCPTコマンドの最大数

メール毎のRCPTコマンドの数を制限する場合は、このオプションを使用します。0で無制限になります。

上限に達した際、セッションを閉じる
RCPTコマンドの最大数が最大数に到達した時に、直ちにセッションを閉じる場合、このチェックボックスを選択します。

サーバ設定

POPサーバにおいて、DELEコマンドでメールを直ちに削除する
POPセッションが適切に終了してしない場合であっても、MDaemonが直ちにユーザが取り出したメッセージを削除する場合、このオプションをクリックします。

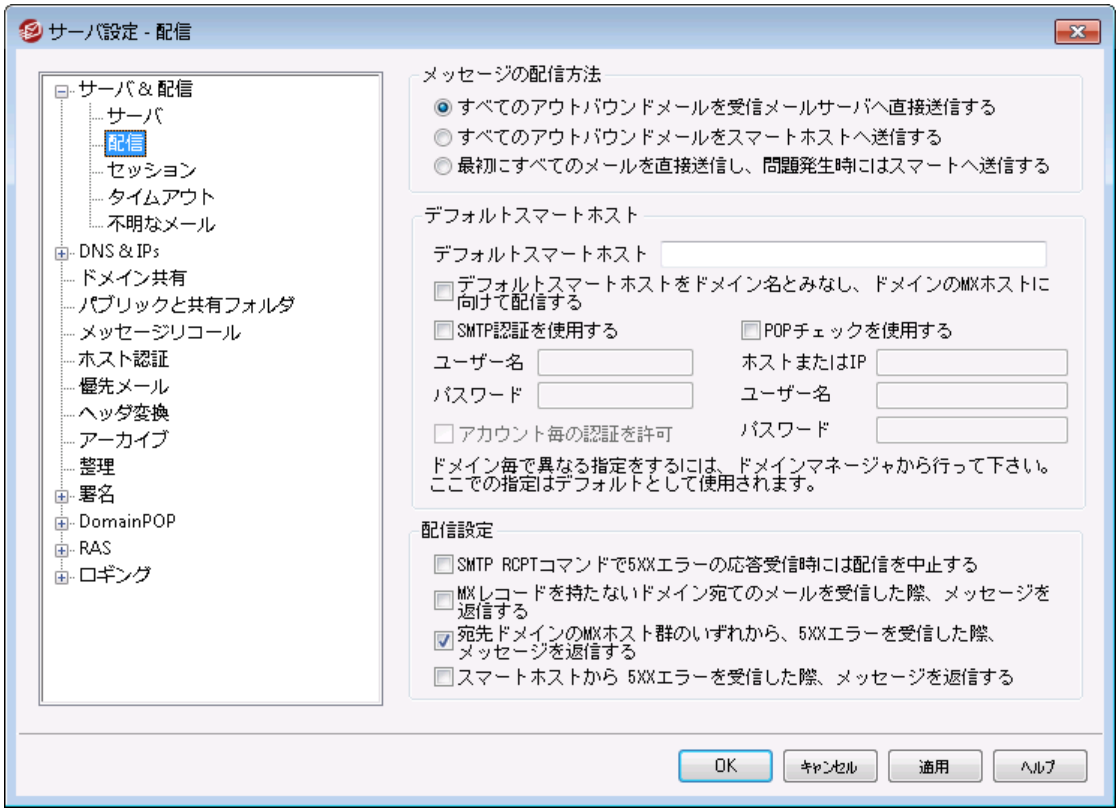
IMAPサーバにおいて、COMPRESSコマンドを有効にする
IMAP COMPRESS拡張（RFC4978)を有効にする場合はこのチェックをクリックします。クライアントで処理されるデータは全て圧縮され、IMAPセッション毎のCPUやメモリ使用量が改善します。

プレーンテキストパスワードを許可
このオプションでMDaemonがSMTP, IMAP, POP3サーバーでプレーンテキストのパスワードを許可するかどうかを指定します。無効にしていた場合、POP3 USER, POP3 PASS, IMAP LOGIN, IMAP AUTH LOGIN, SMTP AUTH LOGIN コマンドはSSLを使わない限りエラーとなります。

サーバーが持つ自身のIPアドレスへの接続を許可
このオプションが有効な場合、MDaemonは自身のIPアドレスに接続できます。

POP & IMAPサーバはこのIPからの接続を常に許可する
スクリーン設定やシールド設定に依らず、ここで指定したIPアドレスからの接続はPOPサーバやIMAPサーバで常に許可します。

3.1.1.2 配信



メッセージの配信方法

すべてのアウトバウンドメールを受信メールサーバへ直接送信する

このオプションを選択すると、MDaemonは別のホストに渡す代わりに、直接すべてのメール配信を試みます。MDaemonは、配達不能メッセージをリトライシステムに格納し、メールキューダイアログのRetryキュー[794]画面で設定するパラメータおよび時間間隔にしたがって再配信を継続します。MDaemonのメニューバーから、この画面を表示するには、[キュー ≫メールキュー ≫Retryキュー]をクリックします。

すべてのアウトバウンドメールをスマートホストへ送信する

宛先ドメインに関係なく、すべての送信メールを配信用の別のサーバへスプールする場合には、このオプションを選択します。このオプションを選択すると、すべての送信メールは、*デフォルトスマートホスト*として指定されたサーバーへ送信されます。この機能は通常、メールが大量にあり、直接のメール配信がサーバリソースの過度な負荷を招く場合がある時に便利です。メッセージを指定されたサーバに配信することができない場合、リトライキューへ移動し、メールキューダイアログのRetryキュー[794]画面で設定するパラメータおよび時間間隔に従って再配信を継続します。

最初にすべてのメールを直接送信し、問題発生時にはスマートホストへ送信する

このオプションは、上記2つのオプションを組み合わせたものです。まずMDaemonは送信メールを宛先サーバーへ直接配信しますが、配信が行えない場合は、*デフォルトスマートホスト*へ送信します。配信不能なメールとは、実際のIPアドレスに解決することのできないホスト宛のメール(例えばリモートネットワークへの未登録のゲートウェイ)や正しく解決できるが直接接続できない、あるいは直接の接続を遮断されたホストへのメールを指します。このオプションをMDaemonで設定すると、これらのメールを送信者へ返さずに、より強力なMTAにメッセージを渡すことができます。ISPによって運用され

ているメールシステムは、ローカルサーバで直接アクセスのできないメール配信のルーティング方法を持つ場合があります。メッセージを指定したサーバに配信できなかった場合は、そのメールはリトライシステムに送られ、メールキューダイアログのRetryキュー[794]で設定された間隔およびパラメータにしたがって再配信が試行されます。それぞれの再配信は、まずは直接配信し、次に指定されたスマートホストに対して行われます。

デフォルト スマート ホスト

デフォルト スマート ホスト
ISPやメールホスト名あるいはIPアドレスをここで指定してください。通常はISPのSMTPサーバを入力します。.

MDaemon自身のドメイン名やIPアドレスを入力しないように注意して下さい。ここで入力するのは、メールを中継する別サーバーやISPです。

デフォルト スマート ホストをドメイン名とみなし、ドメインのMXホストに向けて配信する
MDaemonがデフォルト スマート ホストをドメイン名とみなし、DNSレコードを問い合わせた上でMXホストへメール配信を行う場合は、このオプションを有効にして下さい。

SMTP認証を使用する

デフォルト スマート ホスト で認証が必要な場合はこれを有効にし、認証情報を入力します。認証情報はスマート ホストへ送信されるSMTPメッセージ全てで使用されます。ただし、下部にある[**アカウントごとの認証を許可**]オプションを選択した場合、アカウント エディタのメールサービス[654]画面で指定されるスマート ホスト用のログイン情報を使用して、メール毎にスマート ホスト用の認証を行います。

ユーザ名
ユーザ名またはログイン名を指定します。

パスワード
スマート ホストのログインパスワードを指定します

POPチェックを使用する

スマート ホストがメッセージ受信にPOP3チェックを要求している場合は、チェックボックスを有効にして、次のログオン情報を入力します。

ホストまたはIP
接続先のホスト名あるいはIPアドレスを入力します。

ユーザ名
POPアカウントのログイン名又はアカウント名です。

パスワード
POPアカウントのパスワードです。

アカウントごとの認証を許可
指定した*デフォルト スマート ホスト*への送信SMTPメッセージで、アカウントごとに認証を行う場合は、この設定を有効にしてください。この画面で入力した認証情報ではなく、各ユーザーのメールサービ

スマート ホスト画面で設定する、スマート ホスト用認証情報が使用されます。スマート ホスト用のログイン情報が指定されていないアカウントについては、上記の認証情報が使用されます。

アカウントごとの認証に、*スマート ホスト*用ではなく、通常のメールパスワードを使わせたい場合は、MDaemon.ini の以下の行を編集して下さい。

[AUTH]
ISPAUTHUsePasswords=Yes (デフォルトはNo)

ISPAUTHUsePasswords=Yesオプションを有効にすると、すべてのアカウントのローカルメールパスワードを使って、スマート ホストと一定時間効率よく通信します。これは、機密情報を別のサーバに提供する事から、メールシステムに対してセキュリティのリスクをもたらす可能性があります。この機能が必要で、且つ、スマート ホストが信頼できるホストである場合である場合のみ、このオプションを使用して下さい。さらに、このオプションを有効にしており、且つ、Webmail等で各ユーザーにメールパスワードを変更する許可を与えている場合、メールパスワードの変更が、スマート ホスト パスワードも事実上変更することに注意してください。メールパスワードがローカルで変更され、対応するスマート ホスト パスワードがスマート ホスト上で変更されていない場合、アカウントがスマート ホストでのログインに失敗する可能性があります。

SMTP RCPTコマンドで5xxエラーの応答受信時には配信を中止する
SMTP RCPTコマンドのレスポンスとして5xxの致命的エラーが返された場合、MDaemonからのメッセージ配信を中止する場合は、このオプションを有効にします。このオプションは、デフォルトで無効に設定されています。

MXレコードを持たないドメイン宛てのメールを受信した際、メッセージを返信する
以前MDaemonではDNSルックアップを行い、MXレコードが見つからない場合には、MXとAレコードを検索し、その両方が見つからない場合に、送信元へメッセージを戻していました。MXが見つからない場合に、Aレコードを検索するのではなく、すぐにメッセージを戻す場合はこのオプションを選択します。このオプションは、デフォルトで無効に設定されています。

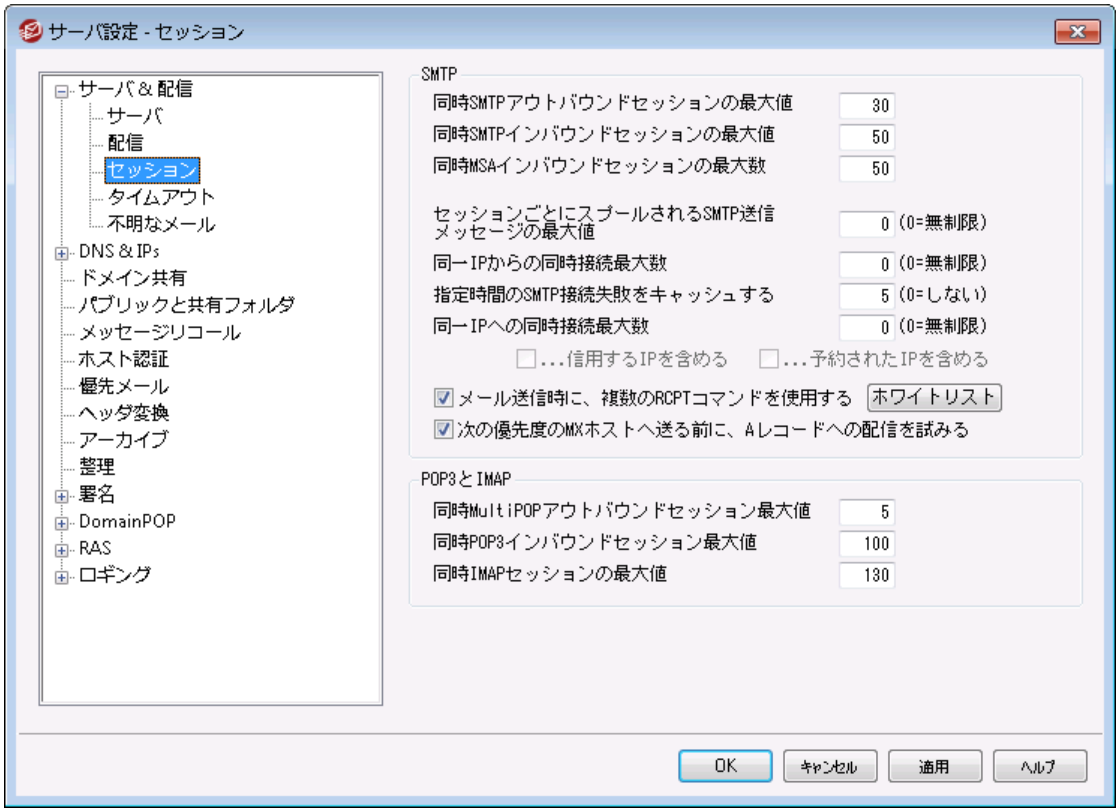
宛先ドメインのMXホスト群のいずれかから、5XXエラーを受信した際、メッセージを返信する
このチェックボックスを有効にすると、MDaemonは、MXホストから5xxの致命的なエラーレスポンスを受信すると、すぐにメッセージを戻し、結果的に、宛先ドメインのMXホストへのメッセージ配信を中止します。このオプションが無効の場合、最低1つのMXホストが、4xxの致命的なエラーレスポンスを返さない限り、MDaemonがメッセージを戻すことはありません。このオプションはデフォルトで有効です。

スマート ホストから、5XXエラーを受信した際、メッセージを返信する
このチェックボックスを有効にすると、MDaemonは、スマート ホストから5xxの致命的なエラーレスポンスを受信すると、メッセージを戻します。

参照:

Retryキュー
メールサービス

3.1.1.3 セッション



SMTP

同時SMTPアウトバウンドセッションの最大値
外部向けメールを送信する時に作成される送信SMTPセッションの最大数をここに入力します。各セッションは、キューが空になるか、または[**セッションごとにスプールされるSMTPアウトバウンドメッセージの最大値**]での設定値に達するまで、外部向けメッセージを送信します。例えば、メールを送信時、外部キューに送信待ちの20個のメッセージがあり、この設定値を5にした場合、5つのセッションが作成され、各セッションで4つのメッセージを配信します。

このオプションはデフォルトで30に設定されていますが、いくつかの設定を試し、帯域幅に対して最適なパフォーマンスとなるセッション数を確認してください。セッション数が多すぎると、帯域幅の過負荷やマシンのリソース消費で、配信効率が悪くなる場合があります。MDaemonで作成される各SMTPセッションは順番にメッセージを配信しますので、1つのメッセージを8つのスレッドで配信するより、それぞれが2つのメッセージを配信する4スレッドの方が効率良く速いかもしれません。28.8K/56Kモデムでは5-10スレッド、ISDN環境では10-15スレッド、ブロードバンド環境では20-30スレッドから始めると良いでしょう。

同時SMTPインバウンドセッションの最大値
この値は同時に発生する内部向け同時SMTPセッションの数をコントロールします。セッション数がこの値に達するとサーバは"Server Too Busy"メッセージを返します。デフォルトは50です。

同時MSAインバウンドセッションの最大数
同時並行のメールサブミッションエージェント（MSA）Inboundセッションの最大数を指定するために、このオプションを使用します。

セッション毎にスプールされるSMTP送信メッセージの最大値
ここでは、セッション毎に処理するメッセージの最大値を制限します。最大値に到達すると、システム上のメモリを解放するため、メールの配信は一旦停止します。通常はこのフィールドには0に設定し、キューが空になるまで各セッションで配信を続けるようにします。

指定時間SMTP接続失敗をキャッシュする(0 =しない)
特定のホストに対するSMTP接続が失敗した際、このオプションで指定された時間（分単位）、そのホストへの接続は行いません。これにより、問題のあるホストへの不必要な接続がなくなります。例えば、同じドメイン宛の複数のメールがあった場合、最初のメール送信時に対象ドメインのサーバーがダウンしていると、MDaemonはデフォルトで5分間、対象サーバーへの接続を行いません。SMTP失敗をキャッシュしない場合、0を使用してください。

同一IPからの同時接続最大数（0 = 無制限）
同一IPからの同時接続を最大いくつまで許可するのかをここで指定します。制限しない場合には0を指定してください。

同一IPへの同時接続最大数(0 = 無制限)

メール配信の間、シングルIPアドレスへ許可される同時接続の数を制限するために、このオプションを使用してください。同時接続を制限しない場合、0を使用してください。

このオプションは、1回の同時接続数が多すぎる場合、これを押さえるのに便利です。ここで指定した以上の接続が必要になると、接続中のIPとの通信は使わずに、次のMXホスト（あるいはスマートホスト）が使用されます。追加のホストがない場合、メッセージは次の配信サイクルのために待ち状態になります。デフォルトで、このオプションは無効で既存の動作を維持します。

> **...信用するIPを含める**
> デフォルトで、信頼されたIPアドレスへの接続は、同一IPへの同時接続最大数から除外されています。信用するIPへも同様のオプションを適用するにはこのボックスを有効にします。
>
> **...予約されたIPを含める**
> デフォルトで、予約されたIPアドレスへの接続は、この機能から除外されています。これらは、127.0.0.*、192.168.*.*、10.*.*.*および172.16.0.0/12です。しかし、予約IPアドレスへも同様のオプションを適用するにはこのボックスを有効にします。

メール送信時に複数のRCPTコマンドを使用する
デフォルトでMDaemonはスマートスプーリングを使用します。これはメール送信時に複数のRCPTコマンドを1つのセッション内で使用するというものです。このオプションはセッション毎に使用するRCPTコマンドを1つに制限したい場合に無効化して下さい。

除外リスト
このボタンはスマートスプーリング除外リストを起動します。MDaemonがこのリストにあるドメインへメールを送信する際には、スマートスプーリングを使用しません。セッション毎に1つのRCPTコマンドのみが使用されます。

次の優先度のMXホストへ送る前に全てのAレコードへの配信を試みる
配信エラーや失敗で、デフォルトではMDaemonは次のMXホストへ移動する前にMXホストの全てのAレコードへ配信を行います。MDaemonでエラー発生時全てのAレコードを試すのではなく、次のMXホストへ移動する場合はこのオプションを無効化してください。

POP3とIMAP

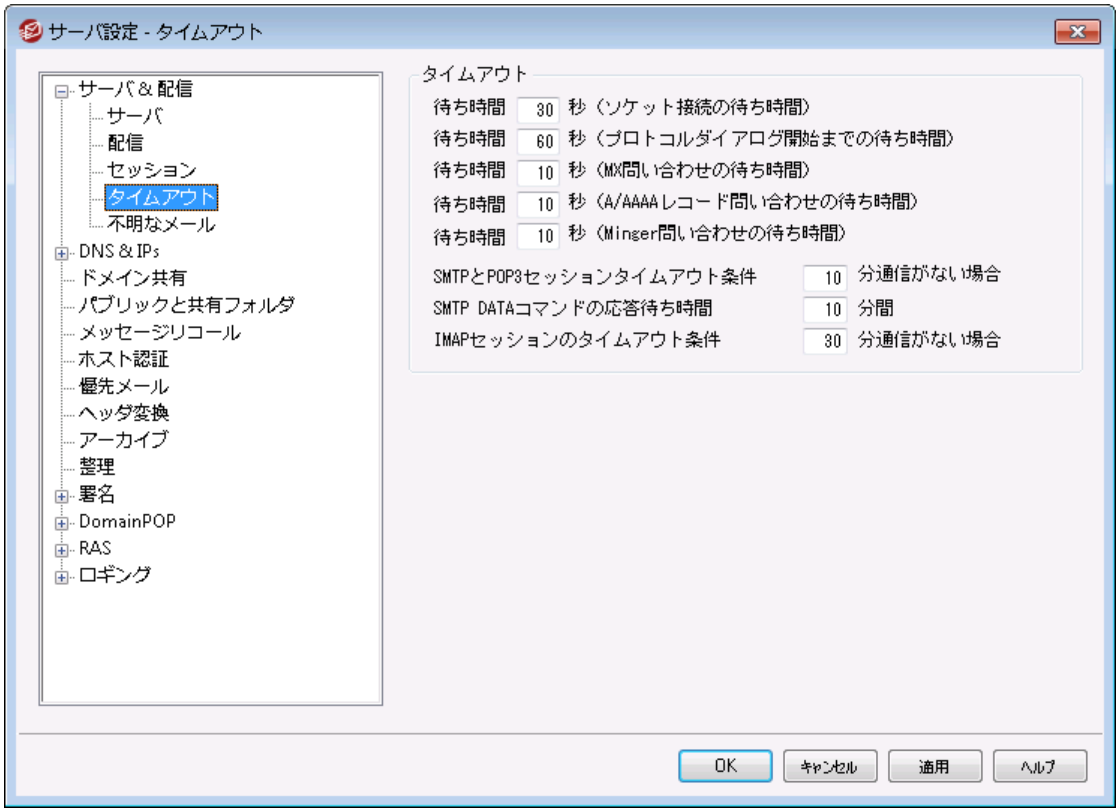
同時MultiPOPアウトバウンドセッション最大値
ここで入力される値は、MultiPOPメールを収集する時に作成される、アウトバウンドPOPセッションの最大数です。各セッションは、すべてのMultiPOPサーバが処理され、すべてのメールが収集されるまで、このタイプのメールを収集します。例えば、すべてのユーザ間で合計15のMultiPOPセッションがある場合に、この設定値を3にセットすると、それぞれのセッションは5つのMultiPOPソース(サーバ)に接続しメールを収集します。

いくつかの設定を試して、帯域幅に最適なパフォーマンスとなるセッション数を確認してください。セッション数が多すぎると、帯域幅に負荷がかかり過ぎマシンのリソースを消費し尽くし配信効率が悪くなる場合があります。MDaemonによって作成される各POPセッションは、すべてのソース(サーバ)が処理されるまでメールを収集することに注意してください。すなわち、1つのソースからメールを集める20のセッションよりも、20のソースからメールを集める4つのセッションの方が効率良く速いかもしれません。

同時POP3インバウンドセッション最大値
この値は、サーバが受け付ける同時POPInboundセッションの最大数をコントロールします。セッション数がこの値に達するとサーバは"Server Too Busy"メッセージを返します。

同時IMAPセッションの最大値
この値は、サーバが受け付ける同時IMAPセッションの最大数をコントロールします。セッション数がこの値に達するとサーバは"Server Too Busy"メッセージを返します。

3.1.1.4 タイムアウト



タイムアウト

待ち時間 xx 秒（ソケット接続の待ち時間）
接続リクエストを開始した後、リモートシステムからの接続を最大何秒待つのかをここで指定します。リモートシステムが、この時間内に応答しなければ、サーバー設定の 配信 85 で行った設定を元に、*スマートホスト* へ配信するか、またはリトライシステムへメッセージを送信します。

待ち時間 xx 秒（プロトコルダイアログ開始までの待ち時間）
リモートホストとの接続を確立すると、リモートホストがSMTPまたはPOP3プロトコルのセッション開始を、ここで指定した秒数待ちます。リモートホストがこの時間内にプロトコルセッションを開始しなければ、サーバー設定の 配信 85 で行った設定を元に、*スマートホスト* へ配信するか、またはリトライシステムへメッセージを送信します。

待ち時間 XX 秒（MX問合せの待ち時間）
リモートドメインのMXホスト解決のためにDNSサービスを利用している場合、MDaemonは、ここで指定した秒数だけMXへの問い合わせの応答を待ちます。この時間内にDNSサーバが応答しなければ、リモートホストのDNSのAレコードで指定されているIPアドレスへメッセージを送信しようとします。それが失敗する場合には、サーバー設定の 配信 85 で行った設定を元に、*スマートホスト* へ配信するか、またはリトライシステムへメッセージを送信します。

待ち時間 XX 秒（A/AAAAレコード問合せの待ち時間）
MDaemon がリモートホストのIPアドレスを解決しようとする際の待ち時間を指定します。試行が失敗した場合、サーバー設定の 配信 85 で行った設定を元に、*スマートホスト* へ配信するか、またはリトライシステムへメッセージを送信します。

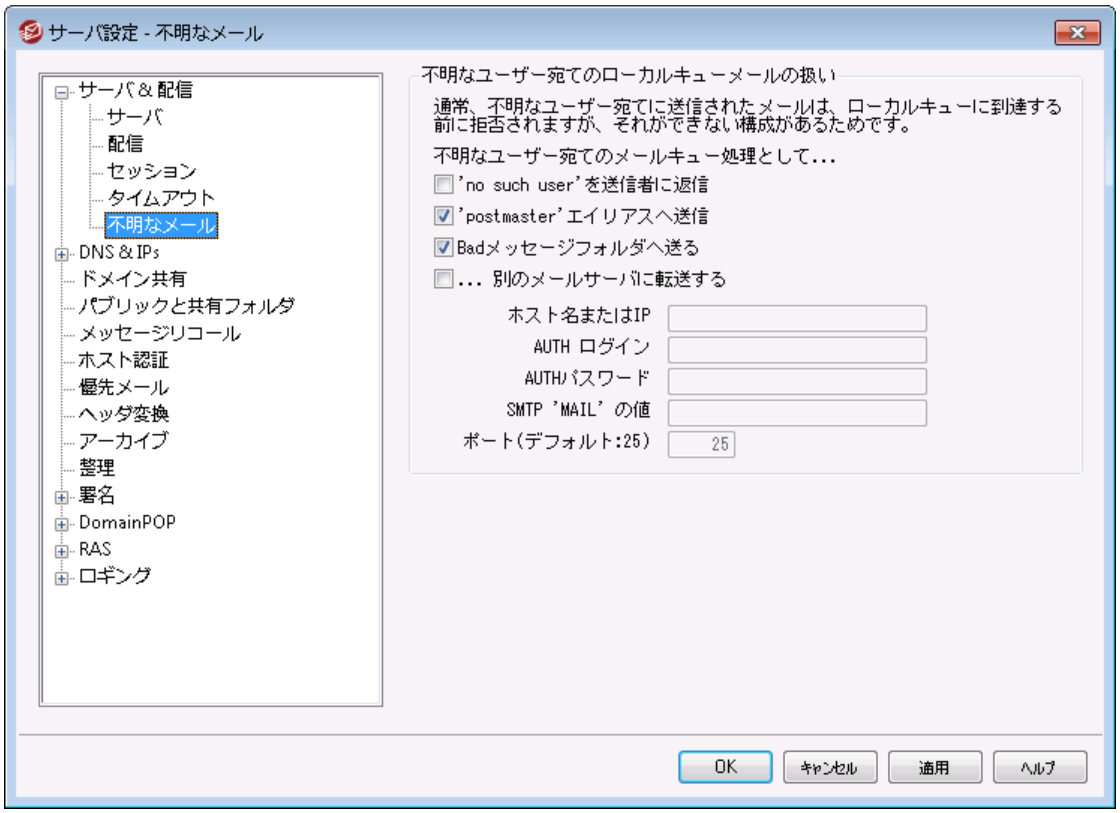
待ち時間 XX 秒(Minger問合せの待ち時間)
MDaemonがMinger[785]サーバから応答を待つ秒数です。

SMTPとPOP3セッションタイムアウト条件 XX 分通信がない場合
接続に成功して、処理中のセッションがここで指定した時間、無通信(入出力なし)の状態が継続した場合、MDaemonは処理を中止します。そして、次回の処理予定時に再び接続を試みます。

SMTP DATAコマンドの応答待ち時間 XX 分間
SMTPの処理中にDATAコマンドの[250 OK]という応答までに待つ時間を、ここに指定することができます。受信サーバの中には、アンチスパムやウィルスチェックあるいはその他の必要なオペレーションに時間がかかる場合があり、それらのタスクの完了に猶予を与えるために、ここでその時間を指定することができます。デフォルトは10分です。

IMAPセッションのタイムアウト条件 xx 分通信がない場合
IMAP セッションがここで指定した時間(分)、無通信の状態になった場合、MDaemon はセッションを閉じます。

3.1.1.5 不明なメール



不明なユーザー宛のローカルキューメールの扱い...

'no such user' を送信者へ返信
このオプションを有効にすると、宛先が不明なローカルユーザ宛てのメールは送信元へ戻されます。警告メールの本文をカスタマイズするには、MDaemon¥App¥フォルダへNoShUser.datというテキストファイルを作成し、ファイルの中にメールの本文を入力します。

"postmaster"エイリアスへ送信
デフォルトでは、宛先が不明なローカルユーザ宛てのメールは[Postmaster]としてエイリアスが設定されたユーザへ転送されます。これらのメッセージをpostmasterへ送信しない場合は、このオプションを解除します。

Badメッセージフォルダへ送る
デフォルトでは、宛先が不明なローカルユーザ宛てのメールは、Badメッセージキューに移動されます。これらのメッセージをBadキューへ移動しないようにするには、チェックボックスを解除します。

...別のメールサーバーへ転送
不明なローカルユーザー宛のメールを別のメールサーバーへ転送するにはこのオプションを使用します。

ホスト名又はIP
メールを転送する先のホスト名かIPアドレスを指定します。

下記については、MDaemonがメールの転送、コピー、送信を許可するホスト全体に対して適用されます。かぎ括弧[]内にホスト名を指定すると(例えば[example.com])、MDaemonは、そのホストへの配信時MXレコードのルックアップを省略します。例えばここでの指定がexample.comの場合は、MXレコードのルックアップは通常通り実行されますが、ここでの指定が[example.com]のようにかぎ括弧で括られている場合は、Aレコードのルックアップのみが実行されます。

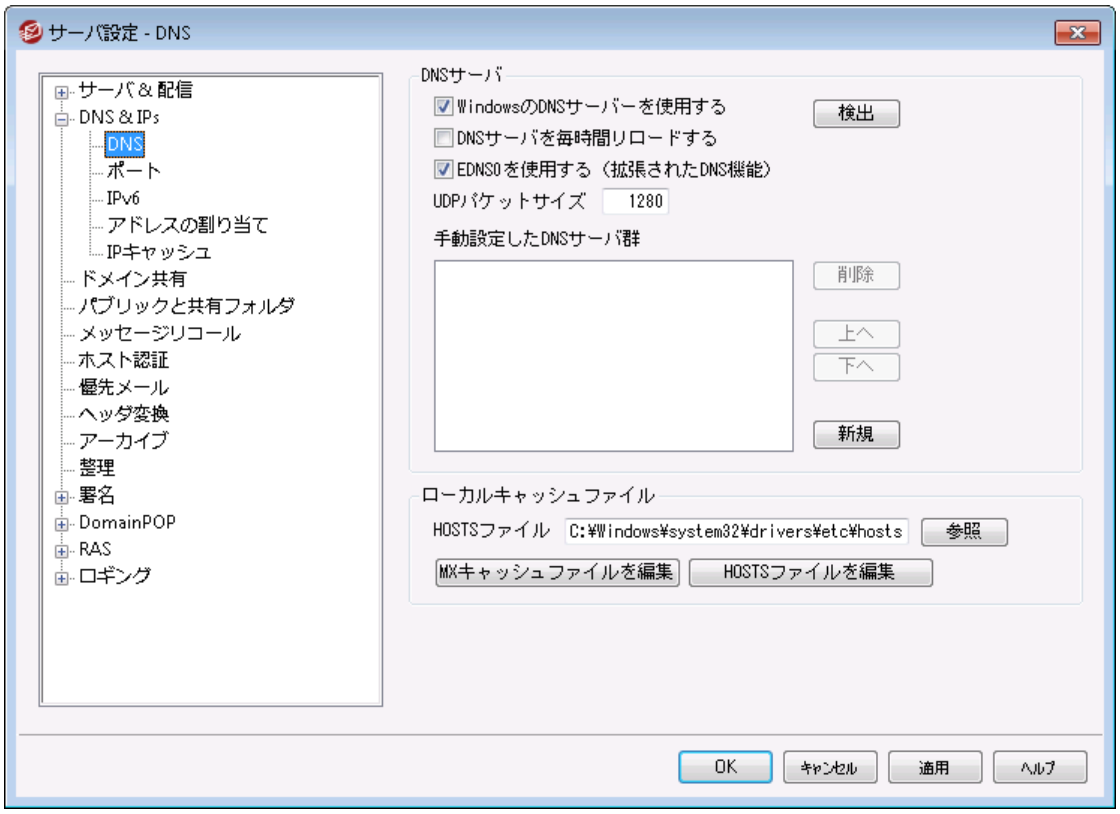
AUTHログイン/パスワード
不明なユーザー宛のメールを転送するメールサーバーで必要な認証用のログイン/パスワード情報を入力します。

SMTP 'MAIL' の値
このアドレスは、通信先ホストを許可するためのセッション内のハンドシェイク内で、"Mail From:"ステートメントとして使用されます。SMTPエンベロープのこの部分は、通常メッセージの送信者として使用されます。[MAIL FROM <>]のような空のコマンドが必要な場合、このフィールドに"[trash]"と入力してください。

ポート(デフォルト:25)
MDaemonがメッセージの送信に使用するポートを指定します。デフォルトでは25番ポートです。

3.1.2 DNS & IPs

3.1.2.1 DNS



DNSサーバ

Windows のDNSサーバを使用する
このオプションが選択されていると、MDaemonはWindowsのTCP/IP設定の中の全てのDNSサーバーを使用します。MDaemonはルックアップを各DNSサーバーへ一回づつ行い、全てのサーバーへ問合せを行い、最初の応答が戻ってくるまでその動作を繰り返します。DNSサーバの手動登録オプションへDNSサーバーを追加登録した場合は、それらのサーバーに対してもルックアップを実行します。最後に、起動時のシステムログには、各DNSサーバーと、それぞれの参照元（手動で追加したものか、Windowsを参照したものか）が表示されます。

一時間毎にDNSサーバーをリロード
1時間毎にDNSサーバーをリロードする場合はこのボックスを有効にします。これはデフォルトで無効です。

EDNS0 (DNS用拡張メカニズム)を使用
デフォルトで、MDaemonはDNS用拡張メカニズム(RFC 26712参照)に対応しています。対応を望まない場合はこのチェックボックスを無効化してください。

UDP packet size
このオプションでUDPパケットサイズを管理します。デフォルトサイズは1280バイトです。

DNSサーバの手動設定

MDaemonはDNSルックアップに、ここで指定された全てのDNSサーバーを利用します。MDaemonはルックアップを各DNSサーバーへ一回づつ行い、全てのサーバーへ問合せを行うか、最初の応答が戻ってくるまでその動作を繰り返します。Windows DNSサーバを使用するオプションを有効にしていた場合は、WindowsのTCP/IP設定で指定されたDNSサーバーに対してもルックアップを実行します。最後に、起動時のシステムログには、各DNSサーバーと、それぞれの参照元(手動で追加したものか、Windowsを参照したものか)が表示されます。

ローカルキャッシュファイル

HOSTSファイル...
DNSサーバに問い合わせる前に、最初にWindows HOSTSファイルを処理してアドレス解決を試みます。このファイルに、問い合わせるドメインのIPアドレスが含まれている場合、MDaemonはDNSサーバに問い合わせしません。

ファイル名でなく、ファイルの完全なパスを入力する必要があります。MDaemonは、このファイルのデフォルトの場所として次の値を使用します。

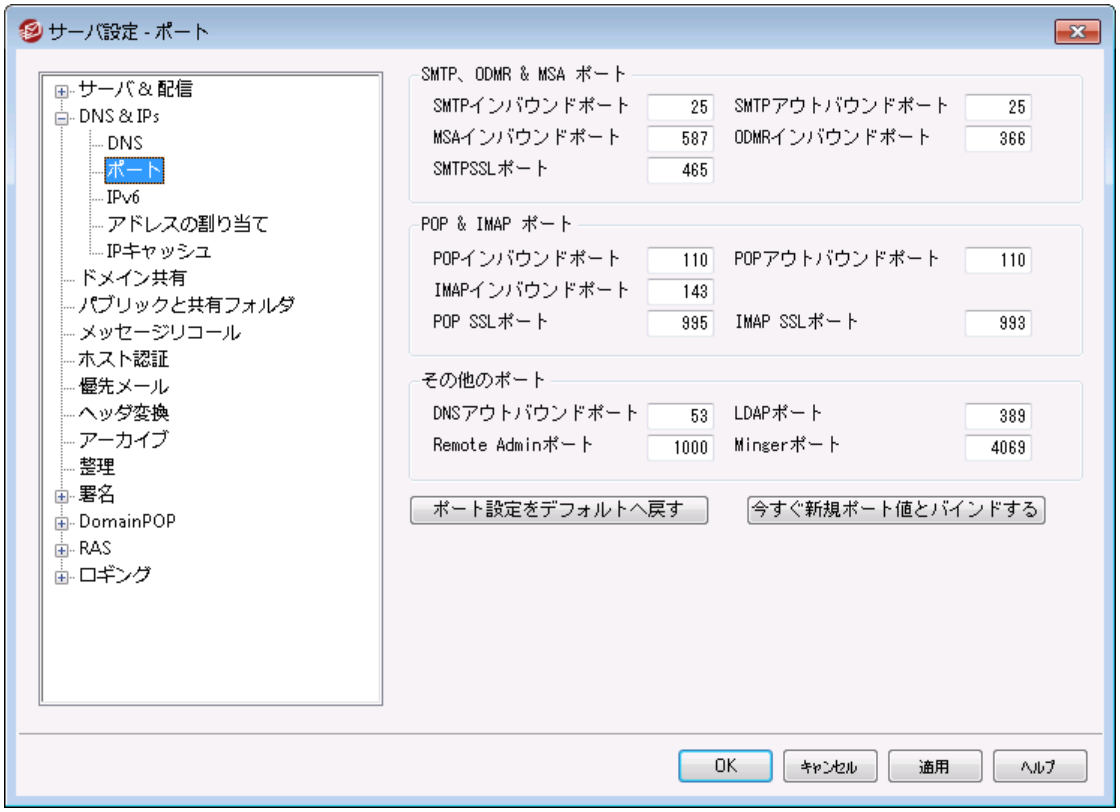
[drive]:\windows\system32\drivers\etc\hosts

HOSTSファイルは、ドメイン名に対してAレコードまたはプライマリIPアドレスを含むWindowsファイルです。MDaemonも、MXCACHE.DAT.と呼ばれているファイル内にMXレコードIPアドレスを指定することができます。このファイルは、MDaemon¥APP¥フォルダにあります。MXCACHE.DATファイルをテキストエディタで開き、詳細はファイルの最上位のコメントを参照してください。

MXキャッシュファイルを編集
MXCACHE.DATファイルを表示または編集する場合は、このボタンをクリックしてください。

HOSTSファイルを編集
HOSTSファイルを表示または編集する場合は、このボタンをクリックしてください。

3.1.2.2 ポート



SMTP / ODMR / MSAポート

SMTPインバウンド ポート
SMTPクライアント から、このTCPポート の受 信 接 続 をモニタします。これはメインSMTPポート で、通 常 は25番 ポート のデフォルト 設 定 です。

SMTPアウト バウンド ポート
このポート は、別 のSMTPサーバへメールを送 信 する場 合 に使 用 します。

MSAインバウンド ポート
これは、上 記 のSMTPインバウンド ポート 指 定 の代 わりに使 うことができるMessage Submission Agent(MSA)ポート です。このポート の通 信 にはAUTHが要 求 されるため、ユーザは、このポート でメールを送 る際 には、その接 続 が認 証 されるようにメールクライアント を構 成 する必 要 があります。一 部 のISPはポート 25をブロックしていますが、MSAポート を使 用 することにより、その制 限 を回 避 することができます。MSAポート を使 用 しない場 合 は、0(ゼロ)を入 力 することでMSAポート は無 効 になります。

MSAポート への接 続 は、PTR、リバースルックアップ、ホスト とIPスクリーニング、IPシールド 、ターピット から除 外 されます。またMSAポート 接 続 は、辞 書 攻 撃 に対 する接 続 を制 限 し続 けます。

ODMRインバウンドポート
このポート番号でドメインゲートウェイからのATRNなどのODMR(On-Demand Mail Relay)受信接続をモニタします。

SMTP SSLポート
このポートはSSL(Secure Sockets Layer)を使用するPOP3メールクライアントのために使われます。SSLと証明書[523]をご覧ください。

POP3 & IMAP ポート

POP3インバウンドポート
このポート番号でリモートPOPクライアントからの受信接続をモニタします。

POP3アウトバウンドポート
POP3サーバからメールが取り出される時に、このポート番号が使用されます。

IMAPインバウンドポート
このポート番号でIMAPリクエストの受信接続をモニタします。

POP3 SSLポート
このポートはSSL(Secure Sockets Layer)を使用するPOP3メールクライアントのために使われます。SSLと証明書[523]をご覧ください。

IMAP SSL ポート
このポートはSSL(Secure Sockets Layer)を使用するIMAPメールクライアントのために使われます。SSLと証明書[523]をご覧ください。

その他のポート

DNSアウトバウンドポート
DNS サーバとのデータ送受信用ポート番号を入力します。

LDAPポート
MDaemonはこのポートを使用して、LDAPサーバのデータベースやアドレス帳へ情報を投稿します。

参照: LDAPアドレス帳対応[754]

Remote Admin port
このポート番号でRemote Administration[321]接続を監視します。

Mingerポート
Minger[785]サーバが接続を監視するポートです。

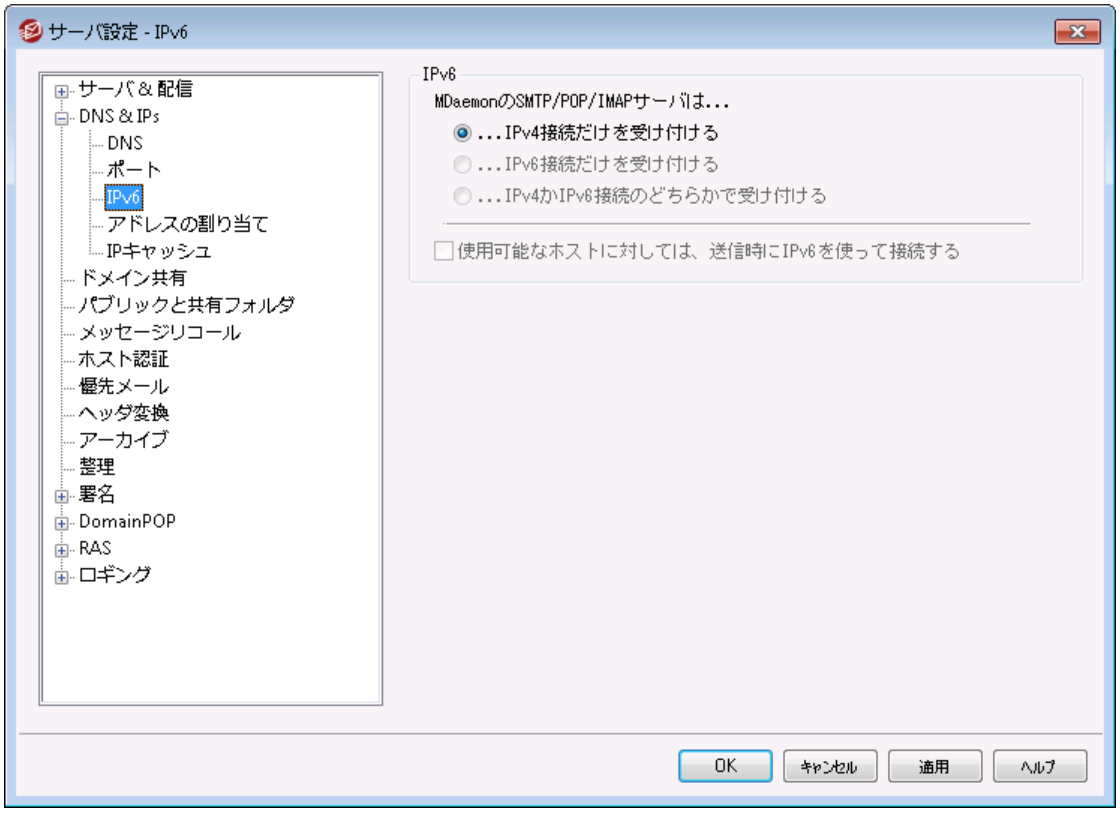
ポート設定をデフォルトへ戻す
このボタンはすべてのポート設定をデフォルト値に戻します。

今すぐ新規ポートにバインドする
ポート設定を変更した際、値をすぐに反映するには、このボタンをクリックします。それ以外は、サーバを再起動するまで反映しません。

ポート番号の設定はサーバの正常動作のために非常に重要です。この値は本当に必要でない限りは変更しないでください。MDaemonのポート設定を行う事で、特定のポート番号を要求するプロキシシステムやその他のソフトウェアサービスと共存できるよう構成する事ができます。

一つのIPアドレス(クライアント)は、サービス毎に1つのポートを使用できます。あるプログラムが既に他の製品で使っているポートへアクセスしようとすると、リクエストしたアドレス(IP:PORT)がすでに使用中であるというエラーメッセージが、ユーザへ通知されます。

3.1.2.3 IPv6



MDaemonはデフォルトでOSが対応しているIPv6のレベルと可能であればデュアルスタックを自動検出します。自動検出できなかった場合は、MDaemonがIPv4とIPv6をそれぞれ監視します。

IPv6

MDaemonのSMTP/POP3/IMAPサーバは...

...IPv4接続だけを受け付ける
IPv4接続だけを受け付ける場合はこのオプションを選択します。

...IPv6接続だけを受け付ける
IPv6接続だけを受け付ける場合はこのオプションを選択します。

...IPv4とIPv6の両方を受け付ける
IPv4とIPv6の両方を受け付ける場合はこのオプションを選択します。これはデフォルト設定で、MDaemonは可能な限りIPv6の接続を優先します。

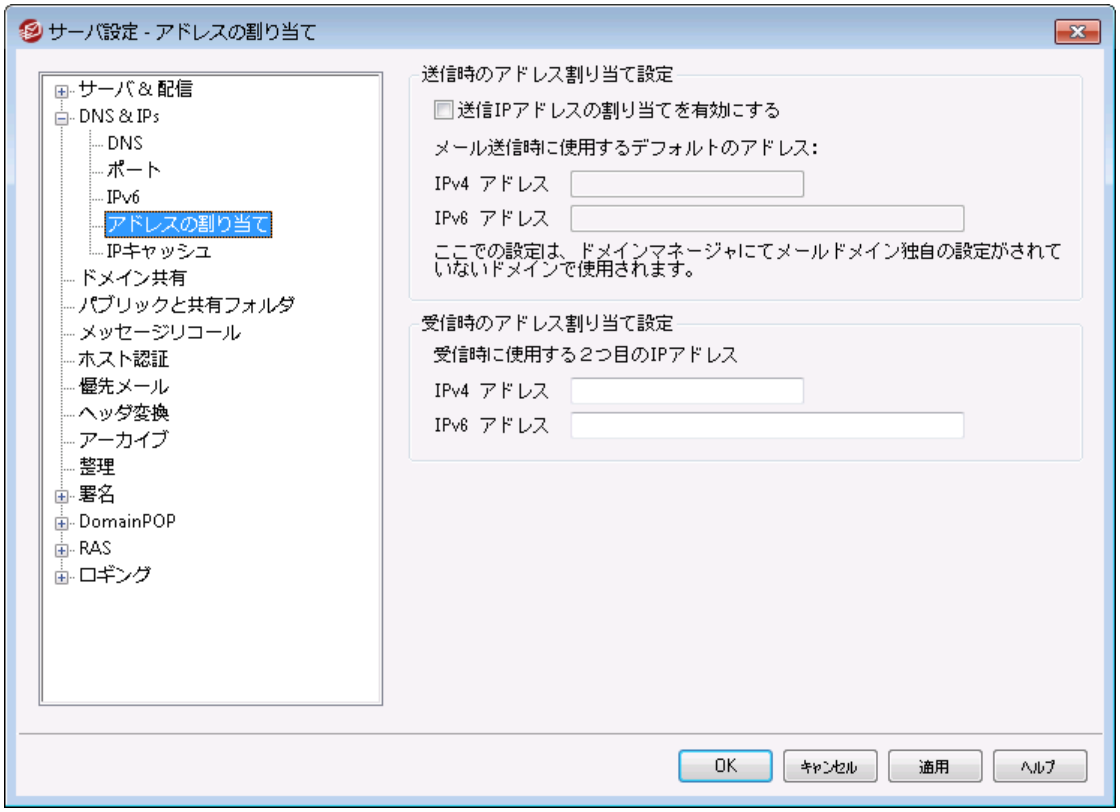
使用可能なホストに対しては、送信時にIPv6を使って接続する
MDaemonが、可能な限りIPv6を使って送信を行うようにするには、このオプションを有効にして下さい。

MDaemonがIPv6ホストへ接続を行う際には、自分自身もIPv6アドレスを使用する必要があります。IPv6アドレスはドメインマネージャ ≫ ホスト名 & IP 167で設定します。必要に応じてアドレスの割り当て 100画面で送信ソケットに使用するポートを指定します。

参照:

アドレスの割り当て 100
ドメインマネージャ ≫ ホスト名 & IP 167

3.1.2.4 アドレスの割り当て



送信時のアドレス割り当て設定

送信IPアドレスの割り当てを有効にする
このオプションを有効にすると、MDaemonは送信ソケットを常に割り当てるようになります。ホスト名 & IP[167]画面で*ドメインはこのIP宛の接続のみを使用する*[167]オプションを使っているドメインに対しては、MDaemonはドメイン用に設定したIPを使用します。それ以外の場合は、下記の*デフォルトで使用する送信IPアドレス*を使用します。

デフォルトで使用する送信IPアドレス: IPv4/IPv6アドレス
ドメインマネージャのホスト名 & IP[167]で特定のIPアドレスを指定されていないホストが送信時に使用するIPアドレスです。

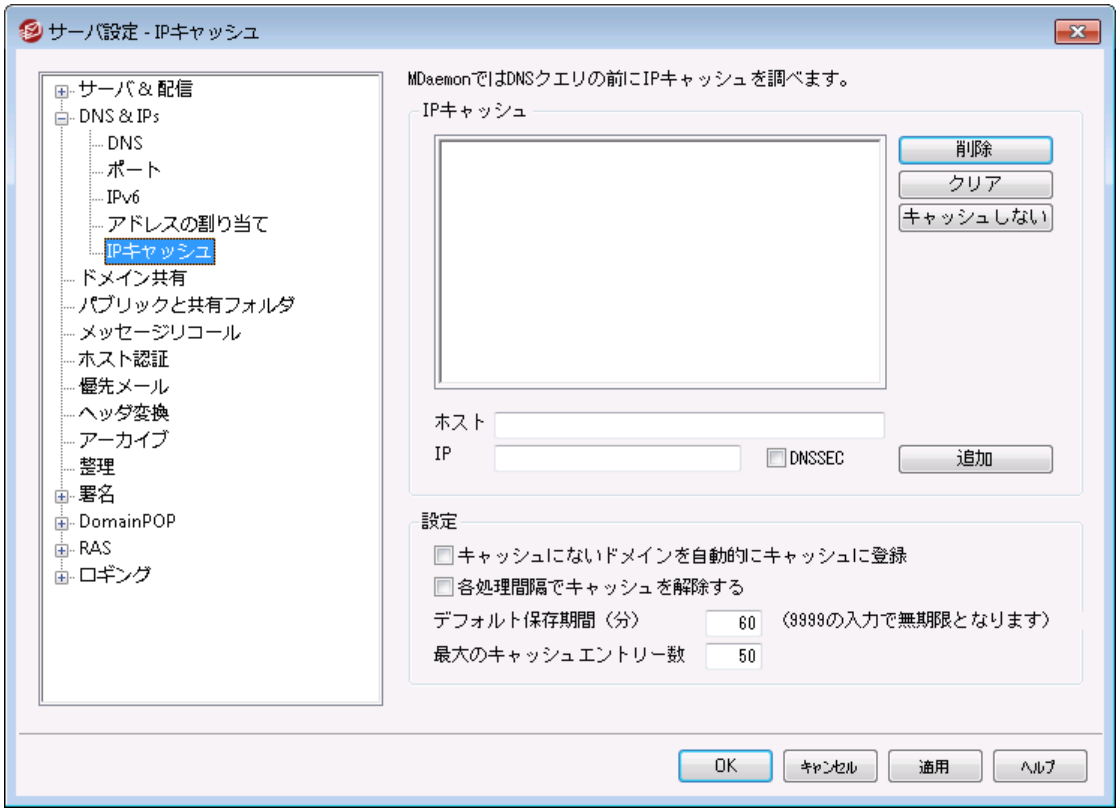
受信時のアドレス割り当て設定

受信時に使用する2番目のIPアドレス: IPv4/IPv6アドレス
2番目に使用する受信時のアドレス[167]を指定する場合はこのオプションを使用します。

参照:

ドメインマネージャ » ホスト名 & IP[167]
IPv6[98]

3.1.2.5 IPキャッシュ



メッセージ配信の速度を上げ、メールの処理時間を短くするために、MDaemonでは、接続をするホストすべてのIPアドレスをキャッシュします。これらのIPは保存（キャッシュ）され、MDaemonがドメイン名に対してDNS解決を要求するたびに、保存されたキャッシュがチェックされます。解決を必要とするドメイン名がIPキャッシュで見つかった場合、DNSルックアップ（検索）はスキップされます。これにより驚異的な量の処理時間を節約することができます。この画面での設定は、キャッシュが機能するパラメータを操作することができます。また、エントリを手動で追加と削除ができ、DNSSECを使用するかどうかの設定、キャッシュの最大サイズ、キャッシュを残す時間を設定することもできます。IPキャッシュは**設定 ≫ サーバ設定 ≫ IPキャッシュ**メニューから選択することができます。

IPキャッシュ

ホスト
IPキャッシュに追加するドメイン名またはホストを指定します。

IPアドレス
IPキャッシュに追加するIPアドレスを指定します。

DNSSEC
DNSSECをチェックします。

追加

ホスト名とIPアドレスの入力後、このボタンをクリックしてIPキャッシュに追加します。

削除
現在キャッシュされているIPリストでエントリを選択し、このボタンをクリックすると、リストからエントリが削除されます。

クリア
このボタンでキャッシュのエントリすべてを削除します。

キャッシュしない
IPキャッシュに追加したくないドメイン名やIPアドレスを選択し、このボタンをクリックします。

設定

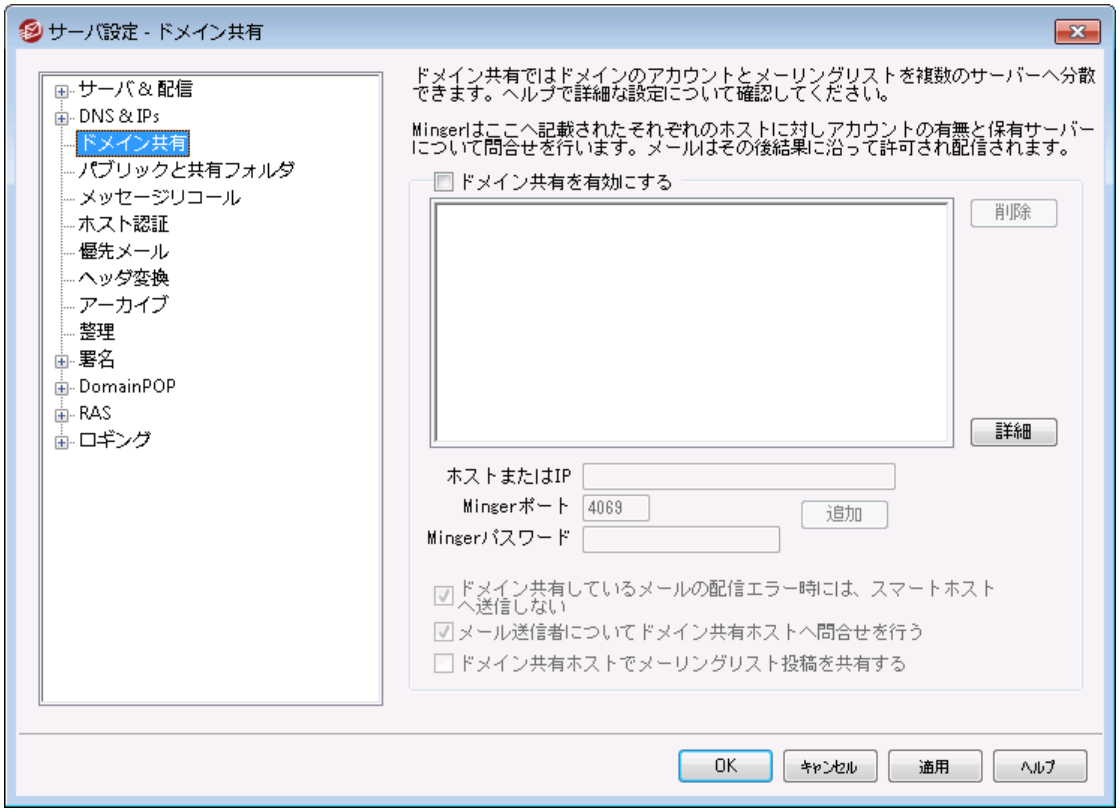
キャッシュにないドメインを自動的にキャッシュに登録
このオプションでは、MDaemonの内部的な自動キャッシュエンジンを使用します。MDaemonが自動でドメインをキャッシュできるようにするには、このオプションを有効にしてください。IPキャッシュを自分で構築する場合は、このチェックボックスを解除してください。

各処理間隔でキャッシュを解除する
このチェックボックスが選択されると、キャッシュ全体の内容は各メールセッションの最初にクリアされます。これにより、それぞれの処理毎に、キャッシュをリフレッシュすることができます。

デフォルト保存時間(分)
これは、IPキャッシュのエントリが残存することができる時間(分)のデフォルト値です。指定された時間を超えると、IPキャッシュに残っているエントリがMDaemonによって削除されます。IPキャッシュのエントリを永久的に残す場合は、ここに9999を指定してください。

最大キャッシュエントリー数
ここでは、キャッシュに含まれるエントリの最大数を指定します。エントリがここで設定した数に達すると、次のエントリは一番目のエントリを削除します。

3.1.3 ドメイン共有



ドメイン共有は、複数サーバで、1つのドメインのユーザを分割することができる機能です。これは、異なる場所にあるMDaemonサーバーが、同じドメインを使って、それぞれのアカウント管理を行う際に使用します。ドメインのユーザアカウントの1部分は1台のサーバでホスティングされ、他の部分は1つ以上の他のサーバでホスティングされます。ドメイン共有ダイアログは、これらの別々のサーバが、どこに位置するか特定するために利用します。受信メッセージが、メールボックスを持たないローカルユーザ宛てだった場合、ドメイン共有は、対象ユーザのアカウントが存在するかどうかを、Mingerを使って他のサーバーへ問合せます。アドレスが有効である場合、MDaemonはメッセージを受信し、対象ユーザーが所属するサーバーへメールを配信します。

例えば、異なる場所にある複数のオフィスで、全従業員に@example.comで終わるメールアドレスを付与したい場合に、この機能を使用できます。各オフィスのMDaemonは、自分のオフィスにいる従業員分のアカウントだけを管理し、全てのオフィスがドメイン共有を使う事で、全従業員のメールは正しいオフィスに対して配信されるようになります。

ドメイン共有ではアドレスの検証にMinger[785]を使用するので、各サーバーが正しく問合せを行えるよう、Mingerが有効で、且つ正しく機能するように構成済である必要があります。ただし、例えばサーバーのうちの1台が一時的に利用できないなど、Mingerの問合せでエラーが発生した場合、送信サーバが後でメールを再送できるよう、MDaemonは[451]の一時的なエラーコードで応答します。さらに、アドレスが確認できると、MDaemonはその情報を5日間キャッシュとして保管するため、同じアドレスからのメールはその間すぐに受信され、対象のサーバーへ配信されます。

最後に、複数サーバーでアカウントが重複するという潜在的なリスクを回避するため、MDaemonは新しいアカウントを作成する前に、ドメイン共有を行っている全てのサーバに対してユーザーの検証を行います。

ゲートウェイエディタの ゲートウェイ全体設定 244 画面には、 *"Minger検証ルックアップを、ドメイン共有ルックアップのトリガーにします。"* というオプションがあります。 このオプションは、ゲートウェイで Minger検証 235 を行う際、ドメイン共有ホストの問い合わせも行うためのオプションです。

ドメイン共有を有効にする
このチェックボックスを選択すると、ドメイン共有を有効にします。ドメイン共有を有効にし、この一覧にドメイン共有するホストまたはIPアドレスを追加します。Minger 785 を利用可能にし、ローカルアドレスを検証する場合に、それらのホストからの問い合わせに応答するように構成をしてください。

削除
ドメイン共有のエントリを削除するには、一覧から削除をするエントリを選んで、このボタンをクリックします。

詳細
このボタンでドメイン共有で使用できるドメイン名の設定を行うためのファイルが開きます。何も記載されていない場合（デフォルトの状態です）は、全てのドメインでドメイン共有が使用できます。ファイルの上部へ記載されている説明文で詳細を確認できます。

ホストまたはIP

このフィールドに、共有するホストまたはIPアドレスを入力し登録します。デフォルトではないポートを使用する場合、コロンの後にポート番号を指定します。（例えばmail.example.com:2525）。これは、下記のMingerポートと同じポートではありません。

Mingerポート
Mingerが、このホストに問い合わせする時に使用するポートです。デフォルトでは4069番です。

Mingerパスワード（オプション）
追加したホストでMingerパスワードを要求する場合は、ここでパスワードを設定します。Mingerでのパスワード要求は必須ではなくオプションですが、パスワードの設定を推奨します。

追加
ホストまたはIP、パスワード、ポートを指定し、このボタンをクリックして登録を完了します。

ドメイン共有しているメールの配信エラー時に、スマートホストへ送信しない
このオプションが有効な場合、MDaemonがドメイン共有メールの配信に（例えばドメイン共有しているホストがオフラインの場合などの原因で）失敗すると、メールはスマートホスト 85 へ送信されるのではなくキュー 794 で保持されます。これらのメールをスマートホストへ配信する事で、メールループが発生する場合があります。このオプションは、デフォルトで有効です。

メッセージ送信者用にドメイン共有ホストをクエリ
デフォルトで MDaemonは他のドメイン共有ホストへ存在するアカウントからのメールを受け付けます。SMTP MAILの送信者でドメイン共有のルックアップを行わないようにするにはこのオプションを無効にしてください。

メーリングリストの投稿をドメイン共有ホストと共有する
ドメイン共有ホストとメーリングリストを共有する場合はこのオプションを有効にします。メールがメーリングリスト宛に到着すると、コピーがそれぞれのドメイン共有ホストへ配信され、メーリングリストのバージョン管理も行われます（そのためのクエリが生成されます）。ホストがコピーを受け取ると、対象のメ

ーリングリスト メンバーへメールを配 信します。このようにメーリングリスト は機 能 を落 とす事 なく複 数 サーバー間 で分 散させる事 ができます。正 しく動 作 するためには各 ドメイン共 有 ホスト がそれぞれの信頼 するIP 473 設 定 の中 で他 のホスト のIPを指 定 しておく必 要 があります。この設 定 を行 っていないと、メーリングリスト メールは「送 信 者 はメーリングリスト のメンバーではなありません」というエラーで拒否 される場 合 があります。

参照:

Minger 785
ドメインマネージャ 165

3.1.4 パブリックフォルダ

MDaemonはパブリックフォルダやユーザーIMAPフォルダに対 応しています。(パブリックフォルダマネージャ 283 で管 理 できる) パブリックフォルダは特 定 のアカウント に属さない特 別 のフォルダですが、複 数 のIMAPユーザ用 として使 用 する事 もできます。ユーザフォルダは、個 々 のMDaemonアカウント に属 するIMAPフォルダです。パブリックフォルダかユーザーフォルダかによらず、共 有 されているフォルダには、それぞれがMDaemonユーザーの一 覧 と関 連 付 けされており、この一 覧 に属 したユーザーだけが、MDaemon WebmailやIMAP対 応 のメールクライアント 経 由 で対 象 フォルダへアクセスする事 ができます。

IMAPユーザが個 人 用 フォルダの一 覧 へアクセスすると、アクセス権 を持 っているパブリックフォルダや共 有 フォルダも、一 覧 へ表 示 されます。このようにして、特 定 のフォルダは複 数 ユーザー間 で共 有 する事 ができ、また、アクセスするためには、個 々 の認 証 情 報 が必 要 になります。更 に、フォルダへのアクセス権 は、必 ずしもフォルダへの読 み書 きができる管 理 者 権 限 である必 要 はありません。アクセス権 は、ユーザー毎 に細 かく設 定 する事 ができ、例 えば、あるユーザにメッセージを削 除 する権 限 を与 えて、他 のユーザにはその権 限 を与 えないといった設 定 が行 えます。

パブリックあるいはIMAPユーザフォルダが作 成 されると、コンテンツフィルタを使 用 して、あるメッセージをそのフォルダに移 動 させるための条 件 を設 定 することができます。例 えば、宛 先 にsupport@example.comを含 むメッセージを、サポート パブリックフォルダに移 動 させるルールを作 成 できます。コンテンツフィルタ処理 590 の[Move Message to a パブリックフォルダ…]と[Copy Message to a public folder…]という動 作 が可 能 にします。パーソナルIMAPフィルタ 670 のルールを使 用 して、特 定 のメッセージを共 有 ユーザフォルダへ送 ることもできます。コンテンツフィルタとIMAPフィルタの使 用 に加 えて、特 定 のアカウント を共 有 フォルダに関 連 付 けることにより、"Submission Address"宛 てのメッセージを、自 動 的 に共 有 フォルダに送 ることができます。しかし、フォルダへの[投 稿]の許 可 が与 えられたユーザだけが、そのアドレスに送 信 することができます。

更 に、メーリングリスト エディタのパブリックフォルダ 273 の画 面 でも、特 定 のメーリングリスト 用 パブリックフォルダを設 定 する事 ができます。この機 能 を有 効 にすると、それぞれのリスト メッセージのコピーは指 定 されたパブリックフォルダに保 存 されます。すべてのパブリックフォルダは、MDaemonインスト ールフォルダにある¥PublicFolders¥ディレクト リに格 納 されます。

Webmailドキュメント フォルダ

Webmailはドキュメント フォルダを使 ったファイル共 有 に対 応しています。ドキュメント フォルダは他 の共 有 フォルダと同 様 にアクセスコント ロールリスト (ACL) 285 に対 応しており、共 有 時 のアクセス権 限 や共 有 で

きるファイル形式を設定する事ができます。Webmailユーザーは内蔵機能を使ってドキュメントフォルダへファイルをアップロードできます。LookOutテーマをお使いの場合、ChromeやFirefoxなど、HTML5のドラッグ＆ドロップAPIに対応しているブラウザであれば、ファイルをドラッグしてデスクトップからブラウザへ直接アップロードする事もできます。ファイル名は変更や検索はもちろん、メール作成時にドキュメントフォルダから直接添付する事もできます。

ドキュメントフォルダ(及び他の共有フォルダ)は、ドメイン単位であれば ¥WorldClient¥Domains.iniファイルやユーザー個別であれば¥Users¥..¥WC¥user.iniを編集する事で、有効化/無効化ができます。ここではデフォルト設定や、個別設定も行え、個別設定はデフォルト設定を上書きします。設定例は次の通りです。

```
[Default:UserDefaults]
DocumentsFolderName=Documents
EnableDocuments=Yes

[example.com:UserDefaults]
DocumentsFolderName=Example Documents
EnableDocuments=Yes

[superControllingDomain.gov:UserDefaults]
EnableDocuments=No
EnableCalendar=No
EnableNotes=No
EnableTasks=No
```

ファイルサイズの制限

ドキュメントフォルダへアップロードする個々のファイルサイズを制限する場合は、Domains.ini ファイルへ次の値を変更します: MaxAttachmentSize=<value in KB> デフォルトは0で、無制限に設定されています。

ファイル形式の禁止と許可

ドキュメントフォルダへアップロードするファイルで、特定のファイル形式を禁止するにはDomains.iniへBlockFileTypes=の後にファイル形式を追加します。複数のファイル形式はスペースかカンマで区切ります。例: BlockFileTypes=exe dll js

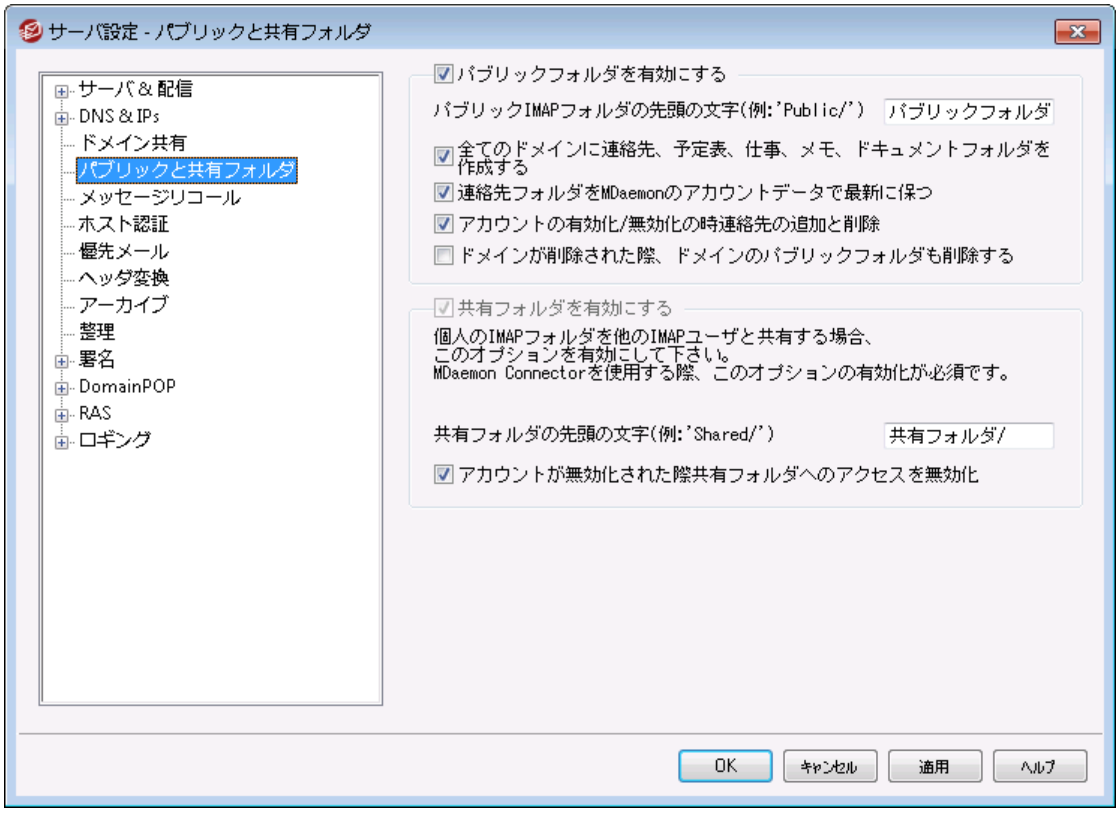
ドキュメントフォルダへアップロードするファイルで、特定のファイル形式のみを許可するにはDomains.iniへAllowFileTypes=の後にファイル形式を追加します。複数のファイル形式はスペースかカンマで区切ります。例: AllowFileTypes=jpg png doc docx xls xlsx

禁止と許可の設定両方が行われると、設定が矛盾した際、禁止設定が優先されます。例えば、同じ拡張子が禁止と許可の両方で記載されていた場合、その拡張子は禁止されます。この行に実際の値(拡張子)が記載されていない場合、この行は使用されません。ファイル形式の指定の際には.(例えば.exeや.dll)を使う事もできますが、必須ではありません。

参照:

パブリックと共有フォルダ 107
パブリックフォルダマネージャ 283
アクセスコントロールリスト 285
アカウントエディタ » 共有フォルダ 676
メーリングリスト » パブリックフォルダ 273

3.1.4.1 パブリックと共有フォルダ



パブリックと共有フォルダの設定を行うには、設定 » サーバ設定 » パブリックと共有フォルダ をクリックします。

パブリックフォルダを有効にする

IMAPユーザにパブリックフォルダへのアクセスを許可する場合は、このオプションを有効にしてください。アクセスできるユーザと、与えられるアクセスのレベルは、パブリックフォルダマネージャ 283 で設定できます。全ユーザからパブリックフォルダを隠す場合は、このチェックボックスを解除してください。

パブリックIMAPフォルダの先頭の文字（例：'Public/'）
パブリックフォルダは、# やPublicFolders/等、最大20文字の名前を持つフォルダを最上位に指定します。これにより、ユーザーはメーラーなどで、個人用のフォルダとパブリックフォルダを簡単に区別できるようになります。テキストボックスにはこの最上位のパブリックフォルダ名を入力して下さい。

全ドメイン用の連絡先、カレンダー仕事、履歴およびメモフォルダを作成する

これらのフォルダを全ドメイン用に作成する場合は、このチェックボックスを有効にしてください。MDaemonにドメイン[165]が追加されると、これらのフォルダは自動的に作成されます。

連絡先フォルダをMDaemonユーザ情報で最新に保つ
このオプションを有効にすると、アカウントリストが連絡先フォルダと同期されます。

アカウントの有効化/無効化の時連絡先の追加と削除
デフォルトで、アカウントを無効化すると、ドメインのパブリック連絡先からも対象アカウントは削除されます。再度アカウントを有効化した場合、連絡先にも再度追加されます。このオプションはデフォルトで有効で無効化されたアカウントがWebmailの自動保管機能で表示される事を防いでいます。

ドメインが削除された際、ドメインのパブリックフォルダも削除する
ドメインが削除された場合にドメイン用のパブリックフォルダも削除する場合は、この設定を有効にします。

共有フォルダを有効にする

IMAPユーザに、IMAPフォルダへのアクセスを共有させる場合は、このオプションを有効にしてください。フォルダにアクセスできるユーザと、与えられるアクセスのレベルは、アカウントエディタの共有フォルダ[676]（アカウント ≫ アカウントマネージャ≫ [User Account] ≫ 共有フォルダ）で指定します。ユーザにフォルダ共有をさせない場合は、このチェックボックスを解除してください。この場合、アカウントエディタに前述の共有フォルダの画面は表示されなくなります。

MDaemon Connector[353]を使用する場合は、このオプションは利用できません。フォルダ共有はMDaemon Connectorには必須の機能で、これを解除することはできないからです。

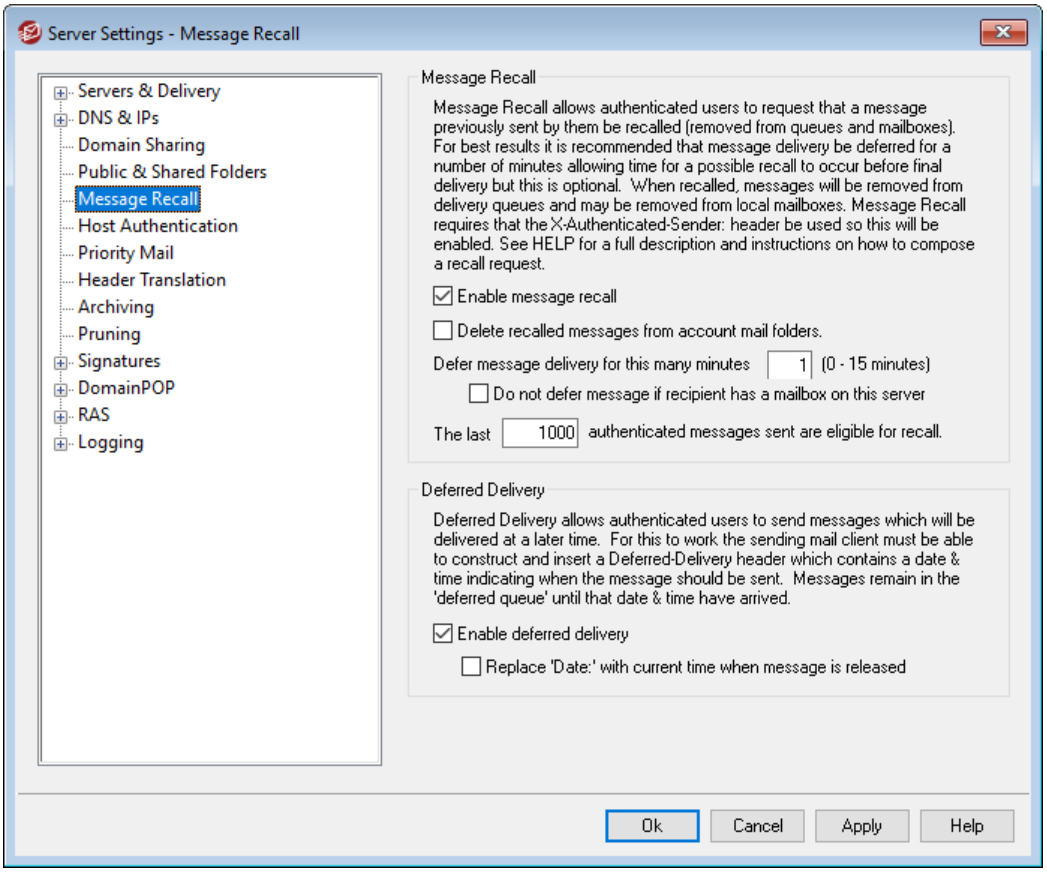
共有IMAPフォルダの接頭辞（例：'Shared/'）
ユーザ共有フォルダは、PublicFolders/等、最大20文字の名前を持つフォルダを最上位に指定します。これにより、ユーザーはメーラーなどで、個人用のフォルダとパブリックフォルダを簡単に区別できるようになります。テキストボックスにはこの最上位のユーザー共有フォルダ名を入力して下さい。

アカウントが無効化された際共有フォルダへのアクセスも無効化
デフォルトで、MDaemonのIMAP, Webmail, ActiveSyncサーバーは無効化されたアカウントによる共有フォルダへのアクセスを許可しません。無効化されたアカウントであっても共有フォルダへのアクセスを許可する場合はこのオプションを無効化します。

参照:

パブリックフォルダについて 105
パブリックフォルダマネージャ 283
アクセスコントロールリスト 285
アカウントエディタ » 共有フォルダ 676
メーリングリスト » パブリックフォルダ 273

3.1.5 メッセージリコール



メッセージリコールシステム

MDaemonにはメッセージリコール機能が搭載されており、認証済のローカルユーザーからのメール配信を1から15分の間遅らせる事ができます。ユーザーはこの間でメールの送信を取り消す事ができます。配信を遅延している間メールはIncomingではなく専用の配信キューへ配置されます。配信キューの中のメールはキューからなくなる時間がファイル名としてエンコードされています。MDaemonは1分おきにキューを

確認しメールがキューからなくなる時間になると、これをInboundキューへ移動させ、通常の配信処理を行います。アクティビティはルーティングタブとログファイルへ記録されます。

希望に応じて遅延時間は0にも設定できますが、これにより、送信を取り消したいメールが配信されてしまう可能性は高くなります。そのため、取り消したいメールに気が付いてからMDaemonへリクエストを送信し、MDaemonが配信リコールを実行するまでの間、最低1から2分程度遅延時間を設定しておくことをお勧めします。ただし、MDaemonは配信取消されたメールをRemoteキューから削除する事もできるため、遅延配信のタイマーが不要だと思う管理者もいるかと思います。

メッセージリコール

メールの送信は複数の方法で取消する事ができます。

1. MDaemon Webmailにて、送信済アイテムの中で取消できるメールを選択し、画面上に表示されるリコールボタンをクリックします。リコールできる時間内であれば、WebmailはRECALLという通知をMDaemonへ送信します。
2. mdaemon@example.comのシステムアカウント宛に、RECALLという件名のメールを送信します。最後に送信したメールだけが取消されます。
3. メールクライアントの送信済アイテムから、対象のメールを「添付ファイルとして転送」し、これをmdaemon@example.comのシステムアカウント宛に、RECALLという件名で送る事もできます。
4. メールのヘッダを確認し、「Message-ID: <message-ID value>」ヘッダをコピーし、新しく作成したメールの件名を、RECALL Message-ID: <message-ID value>として送信します。

リコールの方法に依らず、MDaemonは送信元に対して、リコールが成功したかどうかを通知します。メール配信の取消に成功すると、MDaemonはキューからメールを削除します。追加で、取消されたメールをアカウントのメールフォルダからも削除、のオプションが有効になっていた場合、MDaemonはローカルユーザーのメールフォルダからもメールの削除を試みます。複数の宛先へ配信されたメールも、一つのリクエストのみでリコールが行えます。最後に、メッセージリコールシステムはX-Authenticated-Senderを必須としていて、これにより、メール作成者以外のユーザーがメールの配信を取り消してしまう事を防いでいます。このため、メッセージリコールを有効化すると、ヘッダの無効化オプション455が上書きされます。

メッセージリコール

メッセージリコールを有効にする
このチェックボックスをクリックし、メッセージリコールを有効にします。この機能はデフォルトで無効になっています。

アカウントのメールフォルダからリコールしたメッセージを削除する
リコールしたメッセージの配信が取り消される前に配送されていた場合、ローカルアカウントのメールボックスから削除するにはこのオプションを有効化します。これはローカルユーザーのメールクライアントや電話からメッセージがなくなってしまう可能性があります。このオプションはデフォルトで無効に設定されています。

指定の間メッセージを滞留させる(1-15分)
ここで指定した時間(分)、MDaemonは認証済のローカルユーザーからのメールの処理を保留します。RECALLというメッセージをこの時間内に受け取った場合、MDaemonは対象のメールを削除します。このオプションは1から15の間で設定できます。1分間がデフォルト値になっています。

受信者がこのサーバー上へメールボックスを持っている場合はメールを遅延させることなく配信する
宛先メールボックスが送信者と同じMDaemon上にある場合にメールを遅延させないようにするにはこのチェックを有効にします。注意点:アカウントのメールフォルダからリコールしたメッセージを削除、のオプションが有効の場合、メールが配信されているにも関わらずメールボックスから削除されてしまう場合があります。

直近[xx]通の認証済メールがリコール対象となる
MDaemonは認証済ユーザーからの直近のメールについて、そのメッセージIDとロケーションを記憶しています。メールグループがリコールされなかった場合にリコール処理は失敗し、アカウントのメールフォルダからリコールしたメッセージを削除、が使われていた場合、配信済のメールがユーザーのメールボックスからすぐにリコールされてしまう可能性があります。デフォルトでこのオプションは1000通と設定されています。

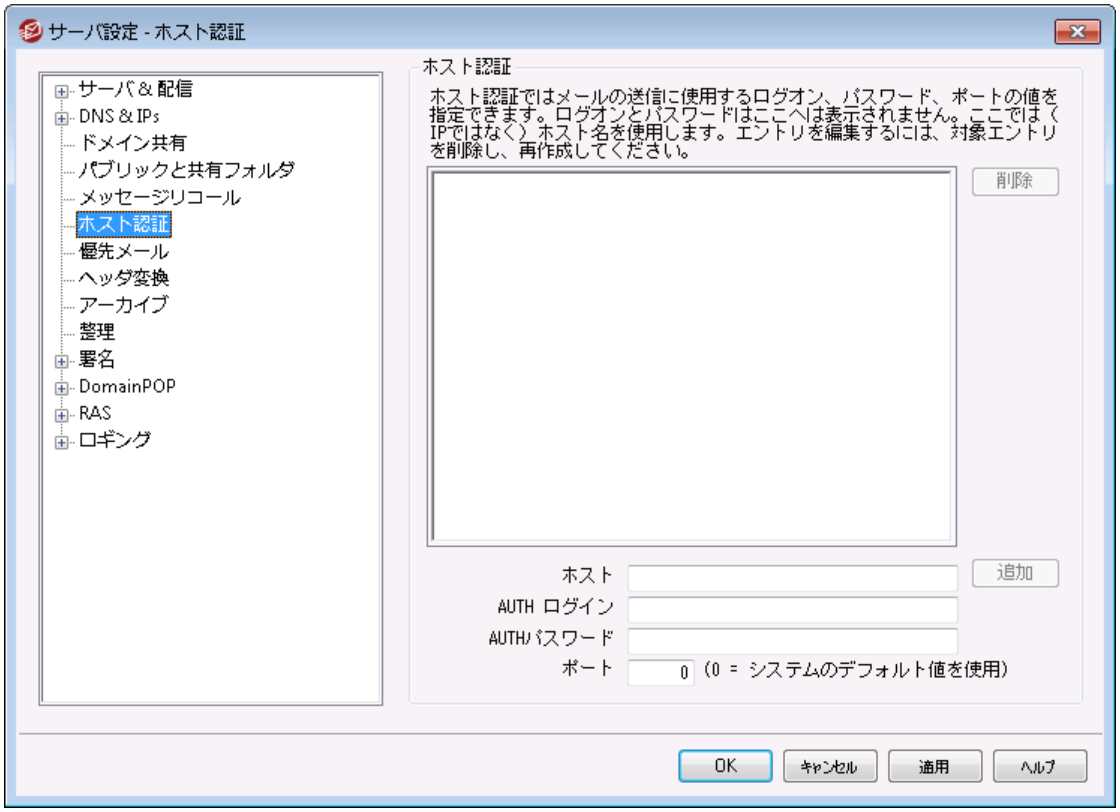
遅延配信

遅延配信オプションで認証されたクライアントは指定日時にメール送信できるようになります。Webmailにはこのオプションが含まれており、ユーザーは「後ほど送信」ボタンをクリックし、メール送信日時を指定する事ができます。メールには送信日時が含まれた `Deferred-Delivery` メールヘッダが追加されます。メッセージリコールオプションが有効でリコール要求が遅延配信メールに対して送信されると、MDaemonは対象メールを削除します。

遅延配信を有効化
認証済クライアントが`Deferred-Delivery` ヘッダを使って遅延配信を行えるようにするにはこのオプションを有効化します。このオプションが有効の場合、Webmailユーザーは、WorldClientやLookOutテーマで、後ほど送信オプションを使用できるようになります。このオプションはデフォルトで無効化されています。

メール解放時'Date:'を現在時刻へ置換
メールを保留キューから開放した際Date:ヘッダを現在時刻へ置換する場合はこのオプションを有効化します。これはデフォルトで無効に設定されています。

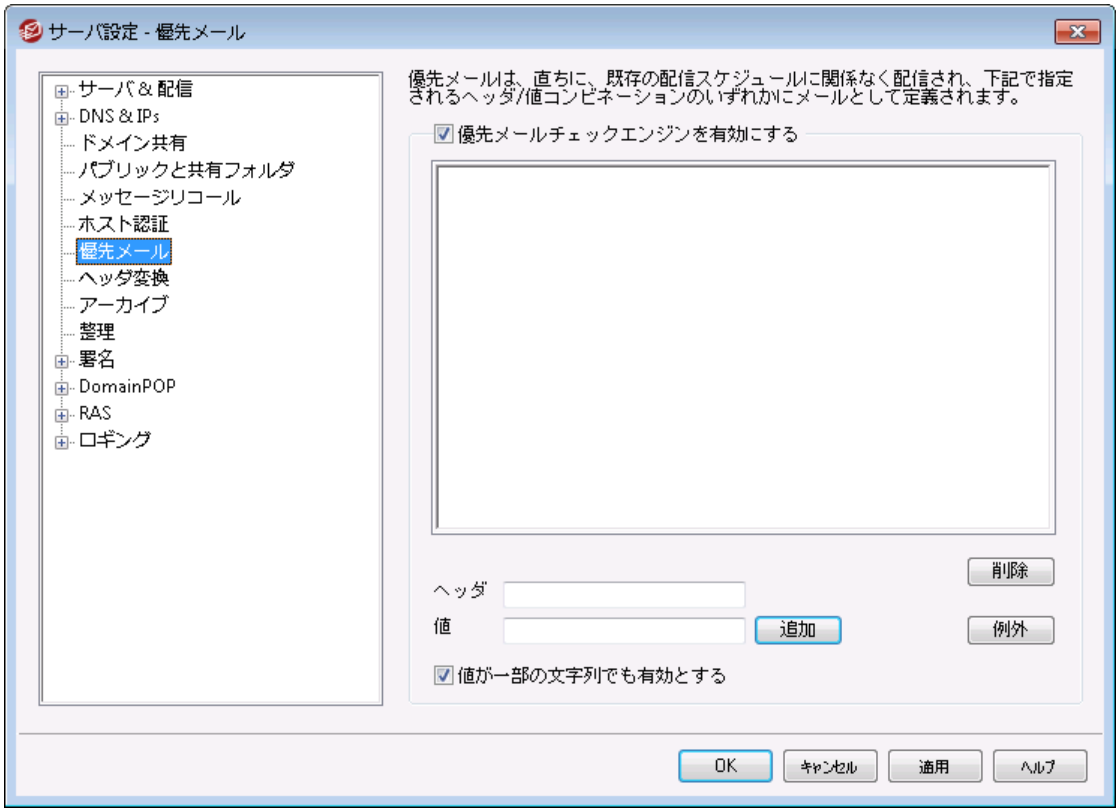
3.1.6 ホスト認証



ホスト認証

この画面では、全てのホストに対するログオン、パスワード、ポートの設定が行えます。MDaemonがホストへのSMTPによるメール送信時、ここで指定した認証情報を使用します。ここでの認証情報は代替手段であり、個別の認証情報が使用できない場合にのみ使われるという点にご注意下さい。例えば、アカウントエディタの転送オプションやゲートウェイマネージャのデキューオプションといった機能でログオン情報を設定していた場合、認証情報はそちらが優先して使用されます。この機能は（IPアドレスではなく）ホスト名でのみ機能します。

3.1.7 優先メール



[設定 >> サーバ設定 >> 優先メール]を選択すると、優先メールダイアログが開きます。ここで、システムで優先メールの構成を定義することができます。優先メールはスケジュールされたメール処理間隔に関わらず、MDaemonによって即座に配信されます。新規メッセージが届くと、MDaemonでは、このダイアログで指定したヘッダと値の組み合わせを調べます。指定したセットを検出すると、そのメッセージを最優先のものと判断して即座に配信します。

優先メールエンジン

優先メールチェックエンジンを有効にする
このチェックボックスを有効にすると、優先メールの機能が有効になります。MDaemonでは、優先状態を着信メッセージについて調べます。

ヘッダ
このフィールドにメッセージのヘッダを入力します。最後にコロンは使えません。

値
優先メッセージとするためのヘッダを指定します。

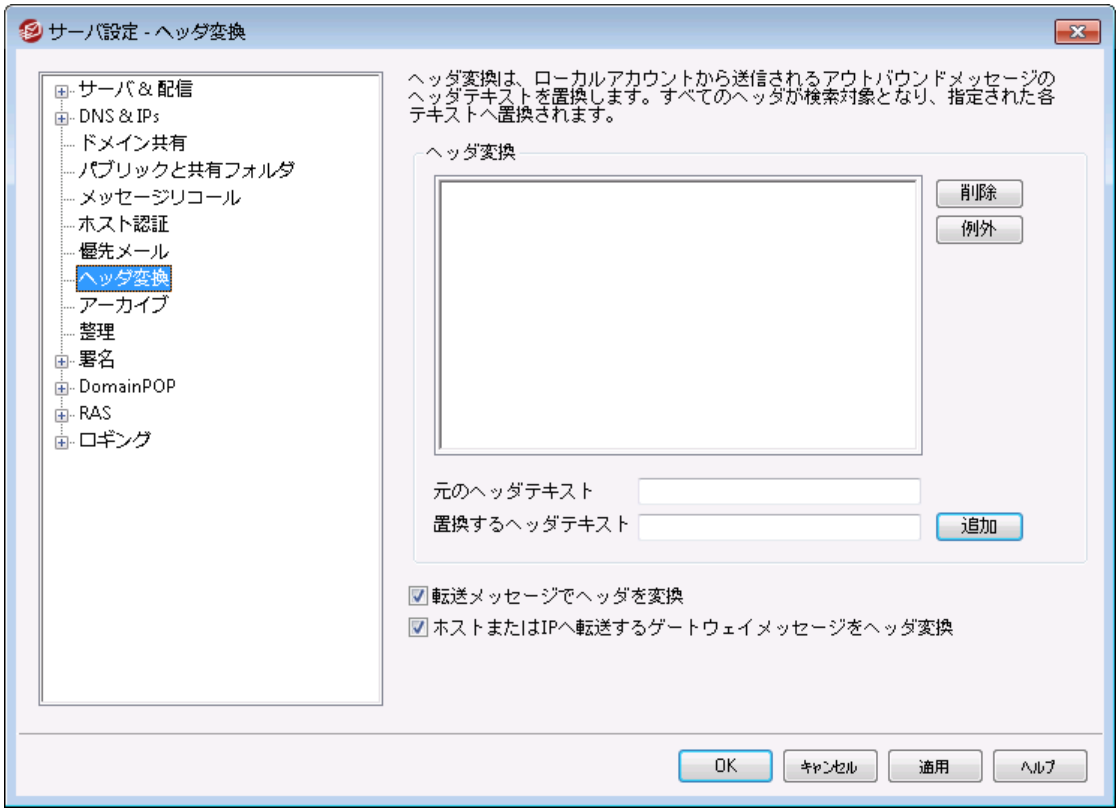
値が部分文字列でも有効とする
新しい優先メールの設定を入力する場合に、この機能を選択してヘッダ値の一部(または文字列の一部)で優先する条件を有効にすることができます。例えば、Toヘッダに値Bossを設定して優先メールを作成します。すると、ヘッダにBoss@ anythingを含むすべてのメールは優先メールと見なされます。このオプションを使わずにエントリを作成した場合は、ヘッダの値はそのエントリと完全一致しなければなりません。部分一致の値は有効になりません。

追加
指定されたテキストボックスにヘッダと値の情報を入力し、このエントリが文字列の一部に適用されるかどうかを指定した後に、その新規の優先メールのエントリを作成するために[追加]ボタンをクリックしてください。

削除
[現在の優先メール ヘッダ/値の組み合わせ]ウィンドウから選択されたエントリを削除するには、このボタンをクリックしてください。

除外
優先メール設定から除外するフィールドと値の組み合わせを定義することができます。除外設定が行える事で、より柔軟なコントロールが行えます。

3.1.8 ヘッダ変換



ヘッダ変換機能は、ドメインから外部宛てにメールが送信される度に、ヘッダの中のテキストの一部を別の値に変換する機能です。検索するテキストを変換する値をここで指定します。MDaemonは、メッセージのヘッダを検索し、対象のテキストを変換します。また、このダイアログの[例外]ボタンをクリックすると、MDaemonに変換させないヘッダ(Subjectヘッダ、Receivedヘッダなど)を指定することができます。

これは、MDaemonのローカルドメイン名が、架空あるいは外部向けに表示されるドメイン名とは異なる場合に必要な機能です。ヘッダ変換機能は、例えば@local domainというドメインを、@RemoteDomainといったドメインへ変換するのに使用します。

ヘッダ変換

このリストは、MDaemonが外向けメッセージヘッダで検索するテキスト部分と、これを置換するテキストです。

削除
定義済みのヘッダ変換リスト中のエントリを選択し、このボタンをクリックすると、リストからそのエントリが削除されます。

例外
このボタンをクリックして、ヘッダ変換の除外 115ダイアログを開いてください。このダイアログでは、ヘッダ変換プロセスから除外するヘッダを指定することができます。

既存のヘッダテキスト
このリストに、MDaemonが送信メッセージヘッダでスキャンするテキストの部分と、それが一致した時に置き換えられるテキストが含まれています。

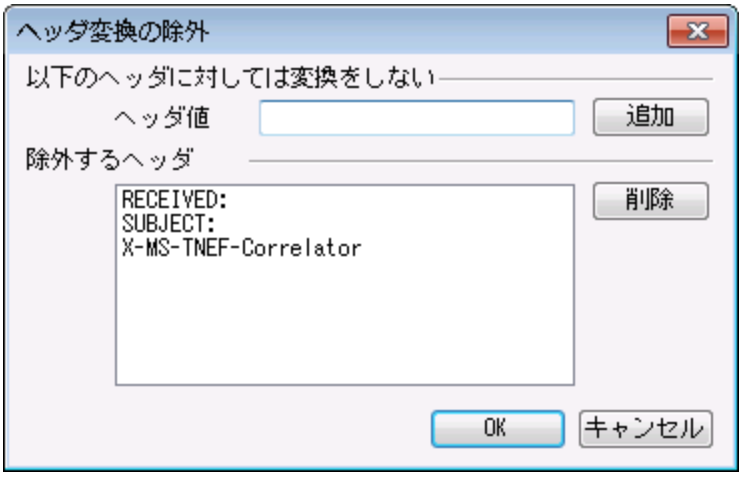
新規ヘッダテキスト
上記の[既存のヘッダテキスト]で入力したテキストから置き換えたいテキストを入力してください。

追加
このボタンをクリックして、上記のテキストを[既存のヘッダテキスト]のリストに加えてください。

転送メッセージでヘッダを変換
このヘッダ変換機能を、ローカルドメインからローカルではないドメインへ自動的に転送されるメッセージにヘッダ変換機能を適用する場合は、このチェックボックスをクリックしてください。

ホストまたはIPへ転送するゲートウェイメッセージをヘッダ変換
ドメインゲートウェイへ転送するメールのヘッダを変換する場合は、このチェックボックスをクリックしてください。詳しい情報に関しては、ゲートウェイエディタの転送 238画面をご覧ください。

3.1.8.1 ヘッダ変換の除外



以下のヘッダに対しては変換をしない

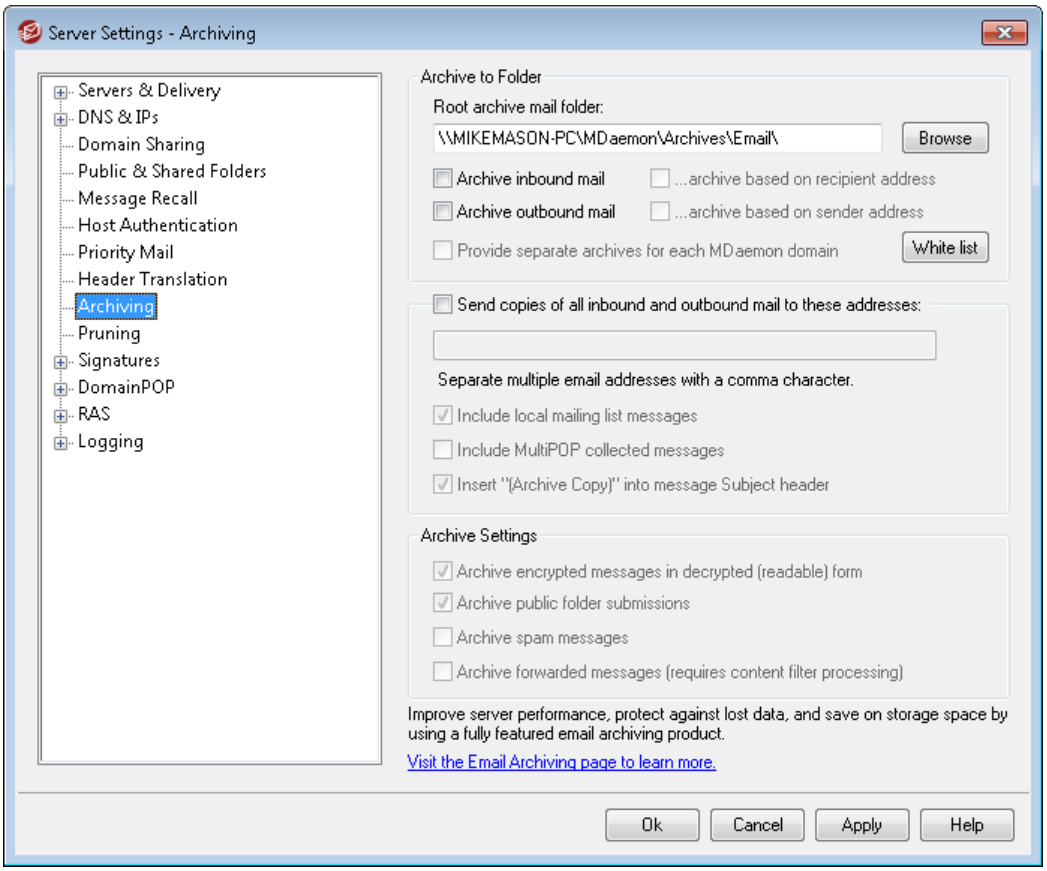
ヘッダ値
ヘッダ変換 114 処理から除外するヘッダを入力します。

追加
このボタンをクリックして、新しいヘッダをリストに追加してください。

除外するヘッダ
MDaemonはこれらのヘッダに対して変換を行いません。

削除
リストの中のヘッダを選択し、このボタンをクリックすると、リストからそのエントリが削除されます。

3.1.9 アーカイブ



全ての送受信メールをフォルダへアーカイブする時には、この機能を使用してください。デフォルトのアーカイブフォルダは C:\MDaemon\Archives\Email\ フォルダですが、これは任意のフォルダへ変更できます。ローカルユーザー「宛て」の受信メールのアーカイブ、ローカルユーザー「から」の送信メールのアーカイブ、又はその両方をアーカイブするかを選択できます。メーリングリストのメール、転送メール、システムレベルのメール、自動応答はアーカイブされず、スパムやウィルス感染したメールもアーカイブされません。

受信メールと送信メールは、それぞれ「In」と「Out」サブフォルダへアーカイブされます。このフォルダは更に、*宛先アドレスを元にアーカイブ*や*送信者アドレスを元にアーカイブ*のオプションで細分化する事ができます。また、MDaemonの*ドメイン毎にそれぞれアーカイブを行う*のオプションで、ドメイン毎にアーカイブを管理する事もできます。

アーカイブされたメールは、ローカルユーザーのメールフォルダか、送信準備完了状態の送信メールとして保存されます。例えば、コンテンツフィルタでヘッダを追加するルールなどがあれば、アーカイブ済のメールにもこのフィルタリングを適用できるようになります。

アーカイブフォルダを参照するには管理しているアカウントの1つを使用し(又は新たにアカウントを作成し)アーカイブ用フォルダ(デフォルトではC:¥MDaemon¥Archives¥Email¥)をこのアカウントのメールフォルダ[653]として指定します。複数のユーザーがアーカイブへアクセスできるようにするには、アーカイブ用のログインIDとパスワードを共有しログインするか、Access Control List[285]を使ってメールボックスを他のユーザーと共有[676]して下さい。

非表示のシステムキューが次の場所へ格納されています: \MDaemon\Queues\ToArchive\。このキューは定期的に手動やプラグイン等によって格納されたメールの有無をチェックされます。メールが格納されていた場合は、すぐにアーカイブされ削除されます。メールがアーカイブ対象でない場合は、単純に削除されます。ルーティング画面/ログでメールが正しくアーカイブされたかどうかを確認できます。

フォルダへアーカイブ

アーカイブ用のメールフォルダをここで指定します。デフォルト値はC:\MDaemon\Archives\Email\ですが、必要に応じて任意のフォルダへ変更できます。

インバウンドメールをアーカイブ

このチェックボックスを有効にすると、ローカルユーザー宛の全てのメールのコピーが保存されます。メーリングリストメールやウィルスを含んだメールはアーカイブされません。

...受信者アドレスによるアーカイブ

このオプションを有効にすると、受信メールのアーカイブが宛先メールアドレス毎に分類されるようになります。

アウトバウンドメールをアーカイブ

このチェックボックスを有効にすると、ローカルユーザーからの全てのメールのコピーが保存されます。メーリングリストメールやウィルスを含んだメールはアーカイブされません。

...送信者アドレスによるアーカイブ

このオプションを有効にすると、送信メールのアーカイブが送信元メールアドレス毎に分類されるようになります。

MDaemonの持つ各ドメイン毎に区別したアーカイブを用意する

このオプションを有効にすると、ドメインごとにアーカイブを管理することができます。

除外リスト
このボタンをクリックするとアーカイブ用除外リストが起動します。ここではアーカイブから除外したい宛先と送信元のメールアドレスの一覧を作成できます。

このアドレスへ全ての送受信メールのコピーを送信する
アーカイブメッセージを送信するアドレスを1つ以上指定します。カンマで区切ることで複数のアドレスを指定できます。ローカル、リモート及びエイリアスアドレスを指定できます。

ローカルメーリングリストメッセージを含む
このオプションを有効にすると、ローカルメーリングリストのメッセージも指定したアドレスへ送信されます。

MultiPOP収集メッセージを含む
このオプションを有効にすると、MDaemonの MultiPOP[673]機能で収集したメッセージもメール送信されます。

Subjectヘッダに"(Archive Copy)"を挿入する
このオプションを有効にすると、送信メールのSubject:(件名)のヘッダへ"(Archive Copy)"という文字を付けます。

アーカイブ設定

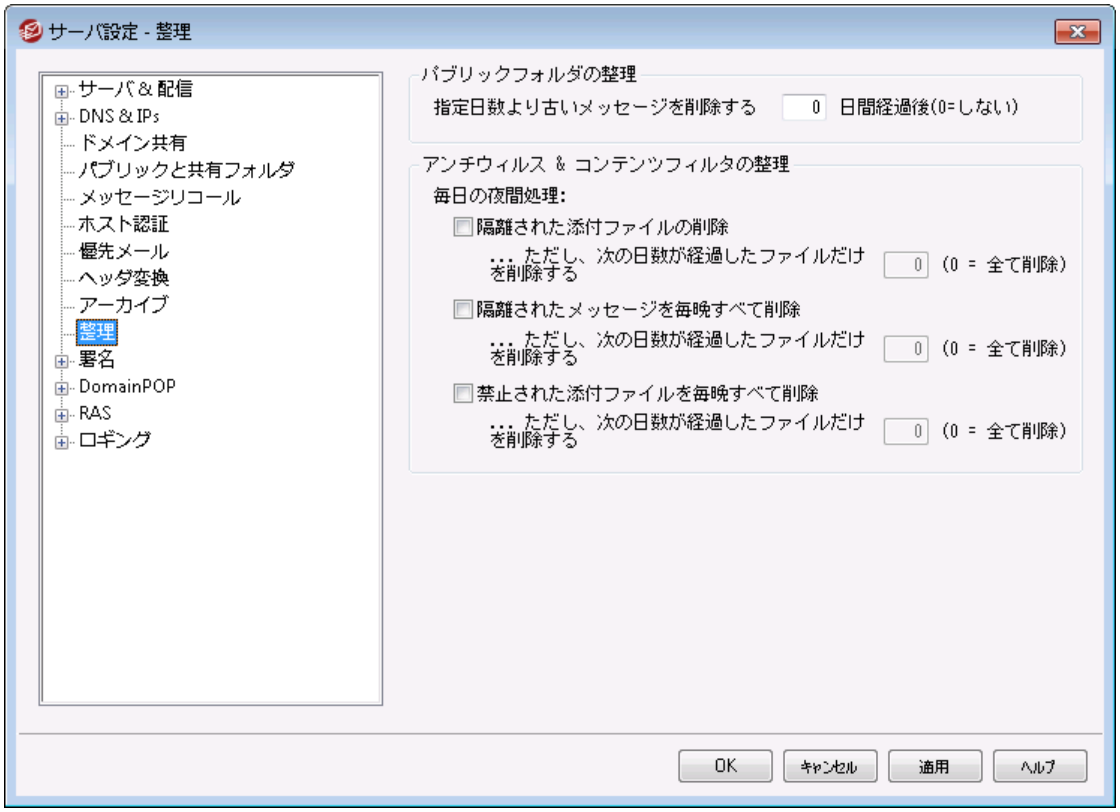
暗号化されたメールを複合化(読める形にして)アーカイブする
デフォルトで、復元された暗号化メールのコピーがアーカイブとして保管されます。ただし、複合化できないメールは暗号化された状態で保管されます。複合化できる場合であっても暗号化されたままの状態でアーカイブしたい場合はこのオプションを無効化してください。

パブリックフォルダ配下へアーカイブする
デフォルトで、パブリックフォルダの投稿アドレス宛てのメールもアーカイブされます。これらのメールをアーカイブ対象外にするにはこのオプションを無効化してください。

スパムメールをアーカイブする
スパムとしてマークされたメールをアーカイブ対象としてコピー送信する場合はこのオプションを有効にしてください。

転送されたメッセージもアーカイブする(コンテンツフィルタ処理が必要です)
このオプションを有効にすると、転送メールもアーカイブやメール送信の対象となります。デフォルトでは、転送メールはアーカイブされません。

3.1.10 整理



パブリックフォルダの整理

古いメッセージを削除(経過日数 XX 日)(0=しない)
一定の日数を経過したメッセージを[パブリックフォルダ](105)から削除する場合は、ここにその日数を入力してください。

アンチウイルス & コンテンツフィルタの整理

隔離された添付ファイルを毎晩全て削除
すべての隔離された添付ファイルを毎晩削除する場合は、ここにチェックを入れてください。

...ただしこの日数より古い場合のみ [xx](0 = 全てのファイル)
デフォルトで全ての隔離ファイルは削除されます。このオプションで日数を指定すると、指定した値よりも古いファイルだけが削除されます。

隔離されたメッセージを毎晩全て削除
すべての隔離されたメッセージを毎晩削除する場合は、ここにチェックを入れてください。

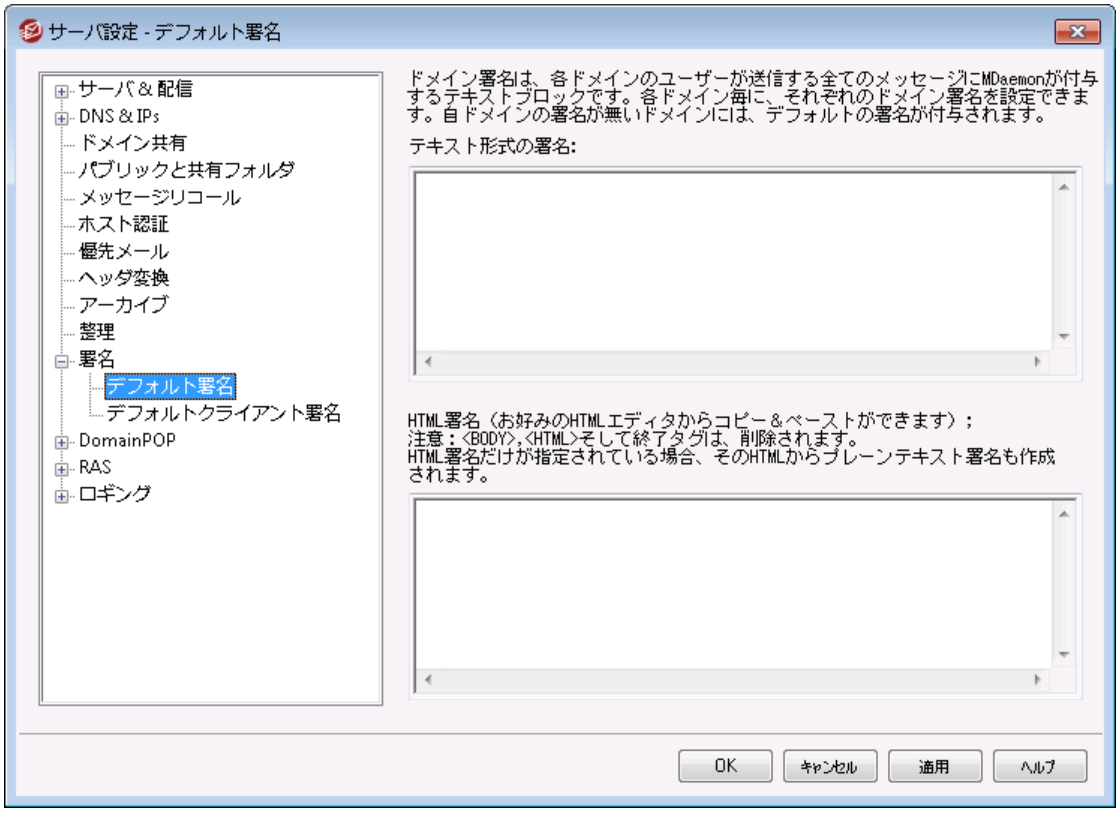
...ただしこの日数より古い場合のみ [xx](0 = 全てのファイル)
デフォルトで全ての隔離メッセージは削除されます。このオプションで日数を指定すると、指定した値よりも古い隔離メッセージだけが削除されます。

禁止された添付ファイルを毎晩全て削除
すべての禁止された添付ファイルを毎晩削除する場合は、ここにチェックを入れてください。

...ただしこの日数より古い場合のみ [xx] (0 = 全てのファイル)
デフォルトで全ての禁止ファイルは削除されます。このオプションで日数を指定すると、指定した値よりも古い禁止ファイルだけが削除されます。

3.1.11 署名

3.1.11.1 デフォルト署名



この画面では全ユーザーから送信されるメッセージへ追加する署名の設定を行います。ドメイン毎に署名を変更したい場合はドメインマネージャの署名 184 から設定ができます。署名は通常メッセージの下へ追加され、フッタ 271 を使っているメーリングリストのメールについては、フッタが署名の下に追加されます。また、アカウントエディタの 署名 686 から各アカウントの署名設定が行えます。アカウント署名はデフォルト署名やドメイン署名の直前に追加されます。

テキスト形式の署名

ここではテキスト形式の署名を指定します。もしもtext/html形式の署名を使いたい場合は、次の*HTML署名*を使って下さい。署名が両方に設定されていた場合、MDaemonはメッセージのフォーマットに応じて適した方の署名を使用します。HTML署名が指定されていない場合は形式を問わずテキスト形式の署名が追加されます。

HTML形式の署名（ご使用のHTMLエディタからコピーして貼りつけて下さい）

ここではtext/html形式のメッセージで使うHTML署名を指定します。署名 がこことテキスト形式の署名の両方で設定されている場合は、MDaemonはメッセージのフォーマットに応じて適した方の署名を使用します。Plain text署名が指定されていない場合はhtml形式の署名が追加されます。

HTML署名はHTMLコードを手動で入力するか、HTMLエディタからコピーしたものを貼り付けて下さい。HTML署名の中に画像ファイルを含む場合は、$ATTACH_INLINE:path_to_image_file$マクロを使用して下さい。

例:

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \images\mr_t_and_arnold.jpg$">
```

MDaemonのRemote Administration 321でも、複数の方法で署名へ画像を追加できます。

- Remote Administrationのデフォルト署名画面で、HTMLエディタの「画像」ツールバーをクリックし、アップロードタブを選択します。
- Remote Administrationのデフォルト署名画面で、HTMLエディタのツールバーにある「画像の追加」ボタンをクリックします。
- Chrome, FireFox, Safari, MSIE 10+では、HTMLエディタのデフォルト署名画面へ画像をドラッグ＆ドロップできます。
- Chrome, FireFox, MSIE 11+ではHTMLエディタのデフォルト署名画面へクリップボードの画像をコピーして貼り付けできます。

<body></body> と <html></html> タグは許可されておらず、使用した場合は削除されます。

署名マクロ

MDaemonの署名機能はマクロに対応しており、送信者の連絡先情報や、パブリック連絡先に登録してある送信者連絡先情報を、署名へ追加する事ができます。これにより、デフォルトやドメイン毎の署名も、送信者情報を個別に指定できるようになります。 例えば、 $CONTACTFULLNAME$ は送信者の氏名を挿入し、$CONTACTEMAILADDRESS$ は送信者のメールアドレスを挿入します。パブリック連絡先は、Webmail, MDaemon Connector, ActiveSyncから編集できます。空の値は送信者の連絡先情報が存在しない場合に使用されます。利用できるマクロは次の通りです。

ユーザーはMDaemon署名を、 $SYSTEMSIGNATURE$ マクロでデフォルト/ドメイン署名へ、$ACCOUNTSIGNATURE$ マクロでアカウント署名へ変換できます。

Signature Selector	
$SYSTEMSIGNATURE$	デフォルト署名 120またはドメイン署名をメッセージに配置する。両方が存在する場合は、ドメイン署名 184が使用される。
$CLIENTSIGNATURE$	メッセージにデフォルトクライアント署名 125またはドメインクライアント署名 188を入れる。両方が存在する場合は、ドメインクライアント署名を使用する。
$ACCOUNTSIGNATURE$	アカウント署名 686をメッセージに配置する。
名前とID	
Full name	**$CONTACTFULLNAME$**
First name	**$CONTACTFIRSTNAME$**
Middle name	**$CONTACTMIDDLENAME$,**
Last name	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
Suffix	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Yomi First Name	**$CONTACTYOMIFIRSTNAME$**
Yomi Last Name	**$CONTACTYOMILASTNAME$**
Account name	**$CONTACTACCOUNTNAME$**
Customer ID	**$CONTACTCUSTOMERID$**
Government ID	**$CONTACTGOVERNMENTID$**
File as	**$CONTACTFILEAS$**
メールアドレス	
Email address	**$CONTACTEMAILADDRESS$**
Email address 2	**$CONTACTEMAILADDRESS2$**
Email address 3	**$CONTACTEMAILADDRESS3$**
電話とFAX番号	
Mobile phone	**$CONTACTHOMEMOBILE$**
Mobile phone 2	**$CONTACTMOBILE2$**
Car phone	**$CONTACTCARPHONENUMBER$**
Home phone	**$CONTACTHOMEPHONE$**
Home phone 2	**$CONTACTHOMEPHONE2$**

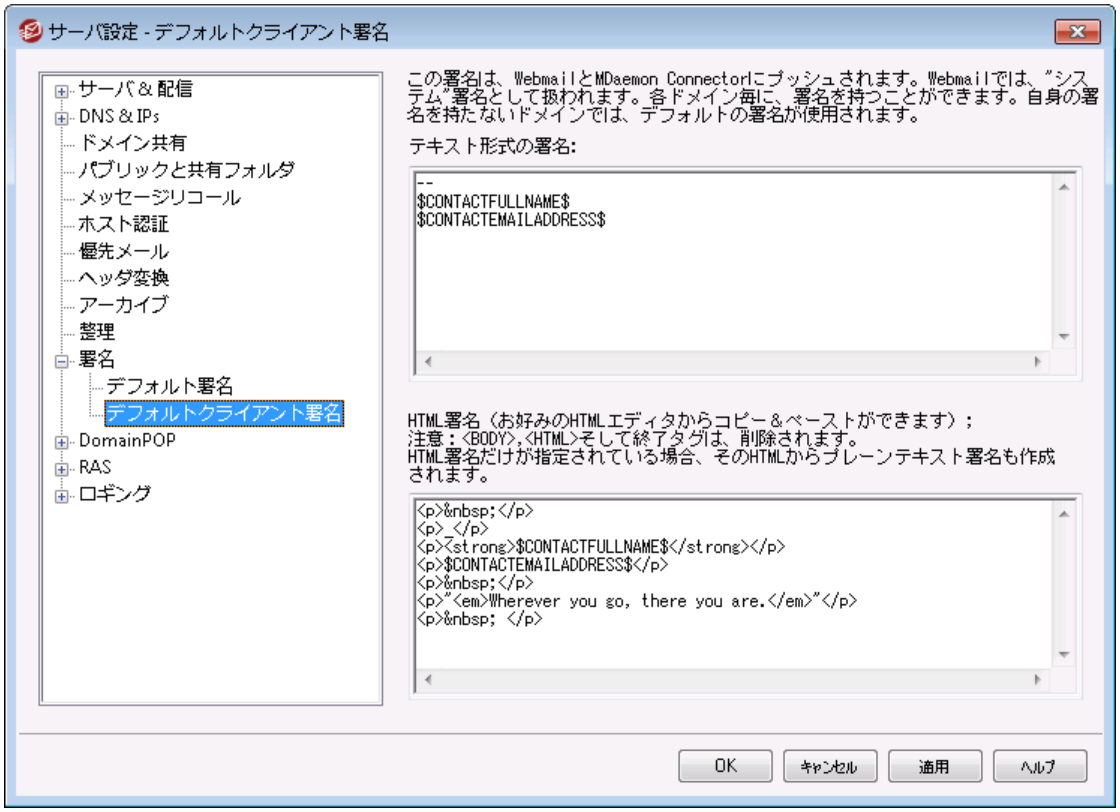
Home fax	**$CONTACTHOMEFAX$**
Other phone	**$CONTACTOTHERPHONE$**
インスタント メッセージとウェブ	
IM Address	**$CONTACTIMADDRESS$**
IM Address 2	**$CONTACTIMADDRESS2$**
IM Address 3	**$CONTACTIMADDRESS3$**
MMS Address	**$CONTACTMMSADDRESS$**
Home web address	**$CONTACTHOMEWEBADDRESS$**
住所	
Home address	**$CONTACTHOMEADDRESS$**
Home city	**$CONTACTHOMECITY$**
Home state	**$CONTACTHOMESTATE$**
Home zip code	**$CONTACTHOMEZIPCODE$**
Home country	**$CONTACTHOMECOUNTRY$**
Other address	**$CONTACTOTHERADDRESS$**
Other city	**$CONTACTOTHERCITY$**
Other state	**$CONTACTOTHERSTATE$**
Other zip code	**$CONTACTOTHERZIPCODE$**
Other country	**$CONTACTOTHERCOUNTRY$**
仕事関連	
Business Name	**$CONTACTBUSINESSCOMPANY$**
Yomi Business Name	**$CONTACTYOMICOMPANYNAME$**
Business title	**$CONTACTBUSINESSTITLE$**
Business office	**$CONTACTBUSINESSOFFICE$**
Business department	**$CONTACTBUSINESSDEPARTMENT$**
Business manager	**$CONTACTBUSINESSMANAGER$**
Business assistant	**$CONTACTBUSINESSASSISTANT$**
Business assistant phone	**$CONTACTBUSINESSASSISTANTPHONE$**
Business main phone	**$CONTACTBUSINESSMAINPHONE$**
Business phone	**$CONTACTBUSINESSPHONE$**

Business phone 2	**$CONTACTBUSINESSPHONE2$**
Business IP phone	**$CONTACTBUSINESSIPPHONE$**
Business fax	**$CONTACTBUSINESSFAX$**
Business pager	**$CONTACTBUSINESSPAGER$**
Business radio	**$CONTACTBUSINESSRADIO$**
Business address	**$CONTACTBUSINESSADDRESS$**
Business city	**$CONTACTBUSINESSCITY$**
Business state	**$CONTACTBUSINESSSTATE$**
Business zip code	**$CONTACTBUSINESSZIPCODE$**
Business country	**$CONTACTBUSINESSCOUNTRY$**
Business web address	**$CONTACTBUSINESSWEBADDRESS$**
その他	
Spouse	**$CONTACTSPOUSE$**
Children	**$CONTACTCHILDREN$**
Categories	**$CONTACTCATEGORIES$**
Comment	**$CONTACTCOMMENT$**

参照:

ドメインマネージャ ≫ 署名 184
アカウントエディタ ≫ 署名 686

3.1.11.2 デフォルトクライアント署名



この画面ではメール作成時に自動挿入されるデフォルトクライアント署名を作成でき、この署名は MDaemon Webmail 176 や MDaemon Connector 371 へプッシュ配信できます。下記のマクロは署名を個人用に設定するために使用でき、名前やメールアドレス、電話番号といった、ユーザー個々の情報へ書き換えられます。ドメイン用の署名は、ドメインマネージャの クライアント署名 188 で作成する事ができます。ドメイン用の署名が作成されている場合は、ドメイン用の署名がデフォルトクライアント署名の代わりに使用されます。*クライアント署名のプッシュ配信* 176 オプションでクライアント署名をWebmailへプッシュ配信でき、 *Outlook用クライアント署名をプッシュ配信* 371 オプションでMDaemon Connectorへプッシュ配信が行えます。Webmailの作成オプションで、プッシュ配信されたクライアント署名は「システム」と呼ばれています。MDaemon Connector用にはOutlookで表示される名称を指定する事ができます。

テキスト形式の署名

ここではテキスト形式の署名を指定します。もしもHTML形式の署名を使いたい場合は、次の*HTML形式の署名*を使って下さい。署名が両方に設定されていた場合、MDaemonはメッセージのフォーマットに応じて適した方の署名を使用します。html形式の署名が指定されていない場合は形式を問わずテキスト形式の署名が追加されます。

HTML形式の署名（ご使用のHTMLエディタからコピーして貼りつけて下さい）

ここではtext/html形式のメッセージで使うHTML署名を指定します。署名 がこことテキスト形式の署名の両方で設定されている場合は、MDaemonはメッセージのフォーマットに応じて適した方の署名を使用します。テキスト形式の署名が指定されていない場合はhtml形式の署名が追加されます。

html 署名はhtmlコードを手動で入力するか、HTMLエディタからコピーしたものを貼り付けて下さい。HTML署名の中に画像ファイルを含む場合は、$ATTACH_INLINE:path_to_image_file$マクロを使用して下さい。

例:

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \images\mr_t_and_arnold.jpg$">
```

MDaemonのRemote Administration[321]でも、複数の方法で署名へ画像を追加できます。

- Remote Administrationの署名/フッタ画面で、HTMLエディタの「画像」ツールバーをクリックし、アップロードタブを選択します。
- Remote Administrationの署名/フッタ画面で、HTMLエディタのツールバーにある「画像の追加」ボタンをクリックします。
- Chrome, FireFox, Safari, MSIE 10+では、HTMLエディタの署名/フッタ画面へ画像をドラッグ&ドロップできます。
- Chrome, FireFox, MSIE 11+ではHTMLエディタの署名/フッタ画面へクリップボードの画像をコピーして貼り付けできます。

<body></body> と <html></html> タグは許可されておらず、使用した場合は削除されます。

署名マクロ

MDaemonの署名機能はマクロに対応しており、送信者の連絡先情報や、パブリック連絡先に登録してある送信者連絡先情報を、署名へ追加する事ができます。これにより、デフォルトやドメイン毎の署名も、送信者情報を個別に指定できるようになります。例えば、$CONTACTFULLNAME$ は送信者の氏名を挿入し、$CONTACTEMAILADDRESS$ は送信者のメールアドレスを挿入します。パブリック連絡先は、Webmail, MDaemon Connector, ActiveSyncから編集できます。空の値は送信者の連絡先情報が存在しない場合に使用されます。利用できるマクロは次の通りです。

ユーザーはMDaemon署名を、$SYSTEMSIGNATURE$ マクロでデフォルト/ドメイン署名へ、$ACCOUNTSIGNATURE$ マクロでアカウント署名へ変換できます。

Signature Selector	
$SYSTEMSIGNATURE$	デフォルト署名[120]またはドメイン署名をメッセージに配置する。両方が存在する場合は、ドメイン署名[184]が使用される。
$CLIENTSIGNATURE$	メッセージにデフォルトクライアント署名[125]またはドメインクライアント署名[188]を入れる。両方が存在する場合は、ドメインクライアント署名を使用する。
$ACCOUNTSIGNATURE$	アカウント署名[686]をメッセージに配置する。
名前とID	

Full name	**$CONTACTFULLNAME$**
First name	**$CONTACTFIRSTNAME$**
Middle name	**$CONTACTMIDDLENAME$,**
Last name	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
Suffix	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Yomi First Name	**$CONTACTYOMIFIRSTNAME$**
Yomi Last Name	**$CONTACTYOMILASTNAME$**
Account name	**$CONTACTACCOUNTNAME$**
Customer ID	**$CONTACTCUSTOMERID$**
Government ID	**$CONTACTGOVERNMENTID$**
File as	**$CONTACTFILEAS$**
メールアドレス	
Email address	**$CONTACTEMAILADDRESS$**
Email address 2	**$CONTACTEMAILADDRESS2$**
Email address 3	**$CONTACTEMAILADDRESS3$**
電話とFAX番号	
Mobile phone	**$CONTACTHOMEMOBILE$**
Mobile phone 2	**$CONTACTMOBILE2$**
Car phone	**$CONTACTCARPHONENUMBER$**
Home phone	**$CONTACTHOMEPHONE$**
Home phone 2	**$CONTACTHOMEPHONE2$**
Home fax	**$CONTACTHOMEFAX$**
Other phone	**$CONTACTOTHERPHONE$**
インスタントメッセージとウェブ	
IM Address	**$CONTACTIMADDRESS$**
IM Address 2	**$CONTACTIMADDRESS2$**
IM Address 3	**$CONTACTIMADDRESS3$**
MMS Address	**$CONTACTMMSADDRESS$**

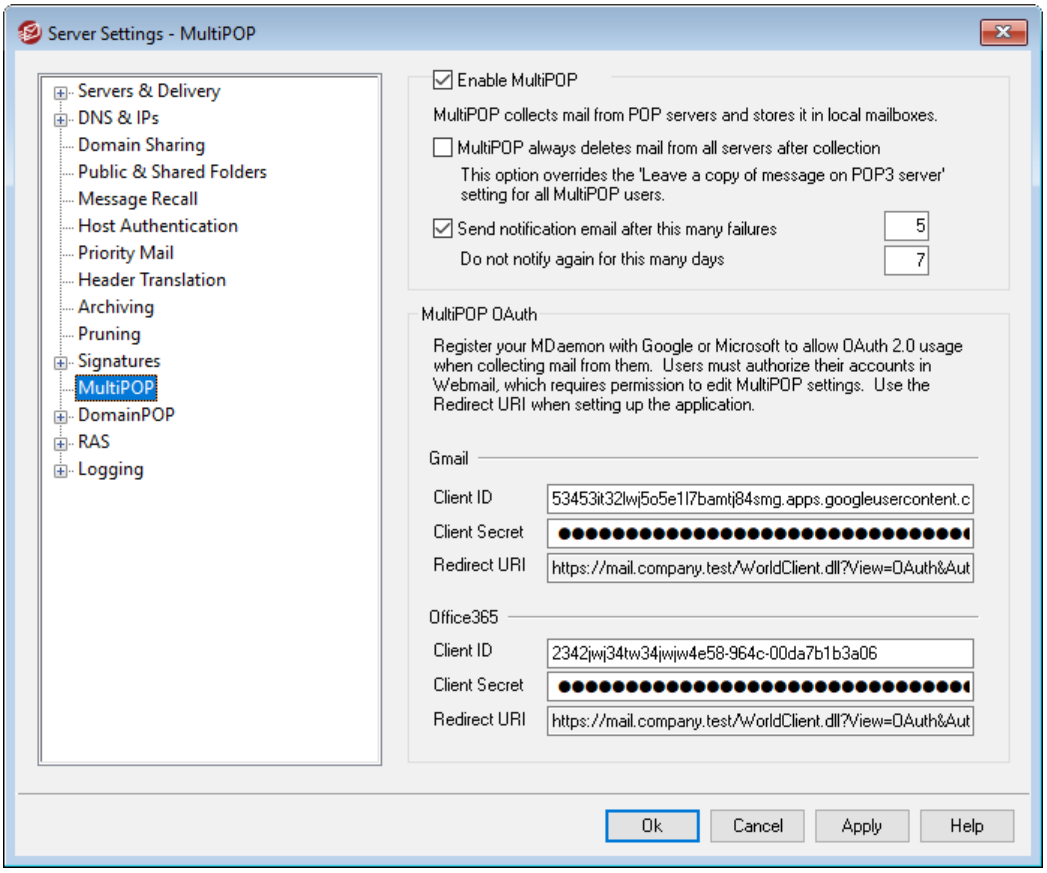
Home web address	**$CONTACTHOMEWEBADDRESS$**
住所	
Home address	**$CONTACTHOMEADDRESS$**
Home city	**$CONTACTHOMECITY$**
Home state	**$CONTACTHOMESTATE$**
Home zip code	**$CONTACTHOMEZIPCODE$**
Home country	**$CONTACTHOMECOUNTRY$**
Other address	**$CONTACTOTHERADDRESS$**
Other city	**$CONTACTOTHERCITY$**
Other state	**$CONTACTOTHERSTATE$**
Other zip code	**$CONTACTOTHERZIPCODE$**
Other country	**$CONTACTOTHERCOUNTRY$**
仕事関連	
Business Name	**$CONTACTBUSINESSCOMPANY$**
Yomi Business Name	**$CONTACTYOMICOMPANYNAME$**
Business title	**$CONTACTBUSINESSTITLE$**
Business office	**$CONTACTBUSINESSOFFICE$**
Business department	**$CONTACTBUSINESSDEPARTMENT$**
Business manager	**$CONTACTBUSINESSMANAGER$**
Business assistant	**$CONTACTBUSINESSASSISTANT$**
Business assistant phone	**$CONTACTBUSINESSASSISTANTPHONE$**
Business main phone	**$CONTACTBUSINESSMAINPHONE$**
Business phone	**$CONTACTBUSINESSPHONE$**
Business phone 2	**$CONTACTBUSINESSPHONE2$**
Business IP phone	**$CONTACTBUSINESSIPPHONE$**
Business fax	**$CONTACTBUSINESSFAX$**
Business pager	**$CONTACTBUSINESSPAGER$**
Business radio	**$CONTACTBUSINESSRADIO$**
Business address	**$CONTACTBUSINESSADDRESS$**
Business city	**$CONTACTBUSINESSCITY$**

Business state	**$CONTACTBUSINESSSTATE$**
Business zip code	**$CONTACTBUSINESSZIPCODE$**
Business country	**$CONTACTBUSINESSCOUNTRY$**
Business web address	**$CONTACTBUSINESSWEBADDRESS$**
その他	
Spouse	**$CONTACTSPOUSE$**
Children	**$CONTACTCHILDREN$**
Categories	**$CONTACTCATEGORIES$**
Comment	**$CONTACTCOMMENT$**

参照:

デフォルト署名 120
ドメインマネージャ » 署名 184
ドメインマネージャ » クライアント署名 188
アカウントエディタ » 署名 686
Webmail設定 316
MCクライアント設定 » 署名 371

3.1.12 MultiPOP



Enable MultiPOP

MultiPOPサーバーを有効にするにはこのオプションを有効化します。MultiPOPとは、ユーザーの代わりにPOPサーバーからメールを収集し、ローカルのメールボックスへ保管する機能です。POP3のホスト/ユーザ/パスワードの組み合わせで、複数のソースからのメール収集を行うことができます。これはメールアドレスを複数持っているユーザーが、一カ所でメールを管理したい場合に役立つ機能です。MultiPOPで収集されたメールは、ユーザのメールボックスへ配信される前に、ローカルキューに配置されるため、他のメールと同様に、自動応答やコンテンツフィルタを適用する事ができます。MultiPOPのスケジュールオプションは、設定 ≫ イベントスケジューリング ≫ メールスケジュールオプション ≫ MultiPOP収集 350からアクセスできます。

MultiPOP収集後サーバから全てのメールを削除する
すべてのユーザに対してPOP3サーバにメッセージのコピーを残す（アカウントエディタのMultiPOP 673画面）の設定をこの設定で上書きするには、このチェックボックスを選択します。メールの収集後、各MultiPOPサーバから全てのメッセージが削除されます。

この数の失敗の後に通知電子メールを送信する
デフォルトでは、MultiPOPアカウントをチェックするとき、MDaemonは複数の失敗の後に通知電子メールを送信します。一時的な失敗は一般的であるため、このオプションは、通知をトリガするために必要な連続した失敗を指定することができます。通知メールの内容と受信者は、□MDaemon□App□MPOPFailureNotice.datを編集してカスタマイズできます。デフォルトでは、通知は5回失敗したらMultiPOPアカウント所有者に送信されます。

この日数の間、再通知しない
デフォルトでは、MultiPOPの障害通知は7日ごとに1回以上送信されません。この間隔を調整したい場合は、このオプションを使用します。

MultiPOP OAuth

OAuth 2.0はGmailやMicrosoft（Office）365が、従来のレガシー/基本認証のサポートを無効化すると同時に必須とした、先進認証です。MDaemonのMultiPOPで、ユーザーに代わってGmailやOffice 365から先進認証でメールの収集を行うには、MDaemonを、Googleであれば Google APIコンソール、Microsoftであれば Microsoft Azure Active Directoryから、OAuth 2.0アプリケーションとして作成する必要があります。手順はWebmailユーザー用の Dropbox統合 309 に似ています。

Gmail やMicrosoft（Office）365からユーザーのメールをMultiPOPで収集するには:

1. 先ほどのMultiPOPを有効にする オプションを選択します。
2. 後述の手順に沿って、GmailやOffice 365用に MultiPOP OAuthアプリの作成とリンク 132 を行います。
3. アカウントエディタのMultiPOPページ 673 で、GmailやOffice 365からMultiPOPでメールを受信するユーザー毎に、MultiPOPを有効にする オプションを選択します。
4. 各ユーザー用に、Gmail（pop.gmail.com:995）又は Office 365（outlook.office365.com:995）アカウントを入力し、OAuthを使用オプションを有効にします。この設定はユーザー自身がWebmail 291 にて行う事もできます。 **注意点**：Gmailアカウント用には、それぞれのGmailアカウントをGmail OAuthアプリのテストユーザーとして追加する必要があります。（下記の*MultiPOP OAuthアプリの作成とリンク* 132 に記載の**公開ステータス**の注意点を参照してください。）
5. アカウントエディタのWebサービス 656 ページで、ユーザー毎に"...MultiPOP設定の編集"オプションを有効化します。
6. 各ユーザーはWebmailへサインインし、オプションの中の**メールボックス**ページで、（管理者側で設定を行っていない場合は）GmailやOffice 365アカウントの設定を行い、**認証**をクリックし、GmailやOffice 365アカウントへサインインし、MDaemonからメール収集を行うために設定を行う必要があります。

Gmail/Office 365

クライアント ID
Google APIコンソールやMicrosoft Azure Active Directory上でMultiPOP OAuth 2.0アプリの作成時、割り当てられる固有のクライアントIDです。アプリ作成後、クライアントIDをコピーし、ここへペーストしてください。

クライアント シークレット
Google APIコンソールやMicrosoft Azure Active DirectoryポータルでMultiPOP OAuth 2.0アプリの作成時、割り当てられる固有のクライアント シークレットです。アプリ作成後、クライアント シークレットをコピーし、ここへペーストしてください。**注意点**： Azureアプリ用のクライアント シークレットは、後から確認する事ができないため、作成時にコピーしておく必要があります。コピーできなかった場合は、シークレットを削除し、新しいものを再作成してください。

リダイレクト URI
GmailやOffice 365用にOAuth 2.0アプリを作成するには、リダイレクトURIを指定する必要があります。MultiPOP画面に表示されているリダイレクトURIは、Webmailへサインインするのに使用する

ドメインのユーザー用のデフォルトドメインのSMTPホスト名を元にした例です。追加のMDaemonドメイン用にリダイレクトURIも追加します。例えば、"https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=Office365" は mail.example.com へログインするユーザー全てに適用できます。後述のMultiPOP OAuthアプリの作成とリンクを参照してください。

リダイレクトURIの例:

```
https://mail.example.com/WorldClient.dll?
    View=OAuth&AuthRequest=Gmail

https://mail.example.com/WorldClient.dll?
    View=OAuth&AuthRequest=Office365
```

MultiPOP OAuthアプリの作成とリンク

MultiPOP OAuth 2.0アプリを作成する手順は次の通りです。

Google Gmail用

MultiPOPでOAuth 2.0を使ってGmailへアクセスし、メール収集を行うには、次の手順に沿って設定を行って下さい:

1. ブラウザで、Google APIコンソールへアクセスします。
2. プロジェクトの一覧からは、**新しいプロジェクト**をクリックし、リソース管理ページからは(+)**プロジェクトを作成**をクリックします。
3. **プロジェクト名**を入力し、プロジェクトIDを編集する場合は**編集**をクリックするか、デフォルト値を使う場合はそのままにします。**注意点**:プロジェクトIDはプロジェクト作成後は変更する事ができません。
4. 左側の画面の**APIとサービス**でOAuth**同意画面**へアクセスします。
5. **外部**を選択し、**作成**をクリックします。
6. **アプリケーション名**(例. MultiPOP OAuth 2.0 for Gmail)を入力し、ユーザー連絡先用の**サポートメールアドレス**とプロジェクト変更に関するGoogleへの連絡先用の**開発者メールアドレス**を入力します。このページでの設定はこれで全部ですが、組織や検証要件によっては、企業ロゴの指定や利用規約や個人情報保護方針へのリンクの設定が必要な場合もあります。**認証済ドメイン**のフィールドは後にリダイレクトURIを入力すると自動で入力されます。**注意点**;ここでの情報はユーザーがMultiPOPでGmailからのメール収集用に認証した際表示されます。
7. **保存して続行**をクリックします。
8. **スコープの追加と削除**で、「スコープを手動で追加」の下へ、**https://mail.google.com/**を入力します。その後、**テーブルへ追加**をクリックし、**更新**をクリックします。
9. **保存して続行**をクリックします。
10. テストユーザーで、**ユーザーを追加**をクリックし、メール収集を行う各Gmailアカウントを入力した後、**追加**をクリックします。(アプリの公開ステータスについては後述の注意点を参照してください。)
11. **保存して続行**をクリックします。

12. サマリページ下部にある、**ダッシュボードへ戻る**をクリックします。
13. 左側の画面の**認証情報**で、(+) **認証情報を作成**をクリックし、OAuthクライアントIDを選択します。
14. 「アプリケーションタイプ」のドロップダウンボックスで、「認証済リダイレクトURI」の下の、**Webアプリケーション**を選択し、**+ URIを追加**をクリックします。リダイレクトURIを入力します。MultiPOP画面へ表示されているリダイレクトURIは、Webmailへサインインするのドメインのユーザー用にデフォルトドメインのSMTPホスト名を元に生成した例です。追加のMDaemonドメイン用にリダイレクトURIも追加します。例えば、"https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=Gmail"はWebmailへサインインする際、mail.example.comへログインするユーザー全てに適用できます。
15. 作成をクリックします。
16. MultiPOPページで**GmailクライアントID**と**Gmailクライアントシークレット**の値を**クライアントID**と**クライアントシークレット**のボックスへコピーします。

> **公開ステータス** – ここでの手順は、Googleアプリで公開ステータスを「テスト中」として作成する事を前提としています。設定はアプリを使ってGmailからメール収集を行うGoogleアカウント毎に行う必要があり、ユーザー数の上限は100ユーザーです。また、Webmailでユーザーが Googleからメール収集するために認証を求められた際、「ユーザーはプロジェクトに対しテストアクセスを行っているものの、未検証のアプリケーション上のデータへのアクセス許可に伴うリスクについても考慮して下さい」といった警告メッセージが表示されます。また、認証は7日間で期限切れとなり、各ユーザーは週に1度Googleアクセス用の再認証を実行する必要があります。
>
> こうした要件や制限を削除するには、ステータスを「稼働中」へ変更する必要があります。この時、環境によってはユーザータイプの外部から内部への変更が必要となる場合があります。アプリケーションの検証や公開ステータスについては、Googleの次のページを参照して下さい: Setting up your OAuth consent screen 及び OAuth API verification FAQs

Microsoft (Office) 365用

MultiPOPでOAuth 2.0を使って認証し、Office 365からメール収集を行うためのMicrosoft Azureアプリは、次の手順で作成します。

1. Azureポータルの Microsoft Azure Active Directory で、画面左側の**アプリ登録**をクリックします。(Azureアカウントを持っていない場合は、フリー又は有料のAzureアカウントを用意する必要があります。)
2. **+ 新しく登録**をクリックします。
3. **名称**フィールドへアプリケーション名を入力します。(例. Mailbox OAuth for Office 365)
4. 「サポートされるアカウントの種類」で**任意の組織用ディレクトリ(任意のAzure ADディレクトリ – マルチテナント)**を選択します。
5. 「リダイレクトURI」用に、**web**を選択し、Office 365用の**リダイレクトURI**を入力します。MultiPOP画面へ表示されているリダイレクトURIは、Webmailへサインインするのドメインのユー

ザー用にデフォルトドメインのSMTPホスト名を元に生成した例です。追加のMDaemonドメイン用にリダイレクトURIも追加します。例えば、"https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=Office365"はWebmailへサインインする際、mail.example.comへログインするユーザー全てに適用できます。

6. **登録**をクリックします。
7. **アプリケーション（クライアント）ID**（隣にクリップボードへコピーするためのアイコンが表示されています）をメモしておきます。このIDは画面左の概要をクリックして確認する事もできます。
8. リダイレクトURIを追加する場合は、**リダイレクトURI：1 web**を右クリックします。**URIを追加**をクリックし、URIを入力し、これを必要な回数行います。入力後、**保存**をクリックします。
9. 左側の画面の**API権限**をクリックします。
10. **+ 権限を追加**をクリックします。
11. **Microsoft Graph**をクリックします。
12. **代理権限**をクリックします。
13. **POP**へスクロールし、**POP.AccessAsUser.All**をクリックし、**ユーザー**で**User.Read**（User.Readはデフォルトで選択されています）が選択されている事を確認します。
14. **権限を追加**をクリックします。
15. 左側の画面の**証明書とシークレット**をクリックします。
16. **+ 新しいクライアントシークレット**をクリックします。
17. 説明を入力します（例 "Office 365 MultiPOP OAuthアプリ用クライアントシークレット"）
18. クライアントシークレットの有効期間を設定します。
19. **追加**をクリックします。
20. 生成されたクライアントシークレット用のノートを**値**フィールドへ入力します（隣にクリップボードへコピー用のボタンが表示されています）。**注意点：**クライアントシークレットは再度表示する事はできません。エントリの隣にある削除アイコンから必要に応じて削除し、新しいクライアントシークレットを再作成してください。
21. MDaemonのサーバー設定の中のMultiPOPページで、Office 365セクションへアプリケーション（クライアント）IDとクライアントシークレットを**クライアントID**と**クライアントシークレット**フィールドへ入力します。

参照:

アカウントエディタ | MultiPOP 673
メールスケジュール | MultiPOP収集 350

3.1.13 DomainPOP

DomainPOPメール収集（設定 » サーバ設定 » DomainPOP）を使うと、MDaemonはリモートのPOPメールボックスをダウンロードし、ユーザーへ再配信できるようになります。MDaemonは指定された認証情報でISPのPOPメールボックスからPOP3プロトコルを使って全メールを収集します。収集後、メールはダイ

アログの設定に基づいて解析され、メールが通常のSMTP処理でメールサーバーへ届いた時と同じように、ユーザーへ再配信されたり、remoteキューへ配送されたりします。

POP3プロトコルを使って保存されたり取得されたりするメールからは、通常SMTPプロトコルで配信されたメールには付与されている、重要なルーティング情報（これはメールの「envelope」とも呼ばれています）がなくなってしまう点に注意して下さい。ルーティング情報が無い場合、MDaemonは、元の宛先情報を判断するために、メッセージのヘッダ情報を強制的に読み取り、解析を行いますが、これは理にかなった方法ではありません。メッセージヘッダでは、宛先を判断する十分な情報が欠けている場合が時々あります。メールの宛先といった、必要な情報が欠けてしまうという事に、驚かれるかも知れませんが、元々POPプロトコルはメールの配信用のプロトコルではありません。SMTPの場合は、セッション中にプロトコル自身が、メールの宛先を明示するので、メールの内容に影響を受ける事はあまりありません。

POPの収集と配信を確実に安定して行えるよう、MDaemonには強力なヘッダ処理オプションが搭載されています。MDaemonは、メッセージをリモートPOPソースからダウンロードする時に、そのメッセージ内のすべての適切なヘッダを即座に解析し、可能性のある受信者情報を集めます。MDaemonが検査するヘッダに含まれている全てのメールアドレスが、この中に含まれます。

この処理が完了すると、MDaemonの受信者の集合は、ローカルとリモートのセットに分けられます。さらに、ローカルとリモートへ分ける前には、エイリアス[757]変換機能によって全てのメールアドレスが解析され処理されます。（MDaemonで管理しているドメインとメールアドレスのドメインが一致する）ローカルセットのメンバーは、メッセージのコピーを受け取ります。リモートセットに何が起こるかは、このダイアログ内の設定に依存します。これらのアドレスを単純に無視する、Postmasterへサマリリストを転送する、あるいはMDaemonがリモート受信者のメールボックスへメッセージのコピーを実際に配信するように受け付ける、などを選択することができます。リモート受信者へメッセージを配信する事はあまりありません。

重複メッセージや無限ループメールの配信をしないように注意してください。SMTPエンベロープの欠如に起因する一般的な問題は、メーリングリストのメールで現れます。メーリングリストによって配信されたメッセージは、メッセージ本文に宛先アドレスに関する情報を持ちません。それどころか、リストエンジンは単純にTO: フィールドへメーリングリストの名前を挿入します。これは直ちに問題を起こします。TO: フィールドがメーリングリストの名前だった場合、MDaemonでは、このメッセージをダウンロードしTO: フィールドを解析し、同じメーリングリスト宛てにメールを配信します。結果、MDaemonが最初のメッセージをダウンロードしたPOPメールボックスに、同じメッセージのコピーが配信され、再度それをダウンロードするというように、永遠に繰り返すサイクルを開始してしまいます。このような問題に対処するために、メール管理者は、メーリングリストメールを削除するか、メールが正しく配信されるようエイリアスを設定するなどの注意が必要です。また、正しい受信者にメッセージを配信するために、ルーティングルールあるいはコンテンツフィルタを使用することもできます。

このようなメール収集方法の採用時、もう一つの懸念は、主にメッセージの重複の問題です。SMTPを使用してISPのPOPメールボックスに配信されるメールは、いったんDomainPOPを使用して収集されると重複を生成してしまいます。例えば、ドメイン内のユーザへメッセージを送信するとし、同じユーザがCC:（カーボンコピー）をドメイン内の他のユーザへ送信するとします。この場合、SMTPは、同じ内容の2つのコピーをISPのメールボックスへ各受信者宛てに配信します。2つのメッセージファイルは、両方の受信者への参照を含みます。1つはTO: フィールドにあり、もう1つはCC: フィールドにあります。MDaemonでは、これらの同じ2つのメッセージファイルを収集し、それぞれから両方のアドレスを解析します。これは両方の受信者が1通の不要な重複メッセージを受信する結果となります。
このような重複を防ぐために、MDaemonには、重複チェックを行うためのヘッダを指定する機能が搭載されています。通常は、[Message-ID]フィールドの利用が理想的です。
上記の例では両方の2つのメッセージはまったく同じもので、同じ[Message-ID]を使っています。
MDaemonはこの値を識別しアドレス情報を参照する前に2通目のメールを削除します。

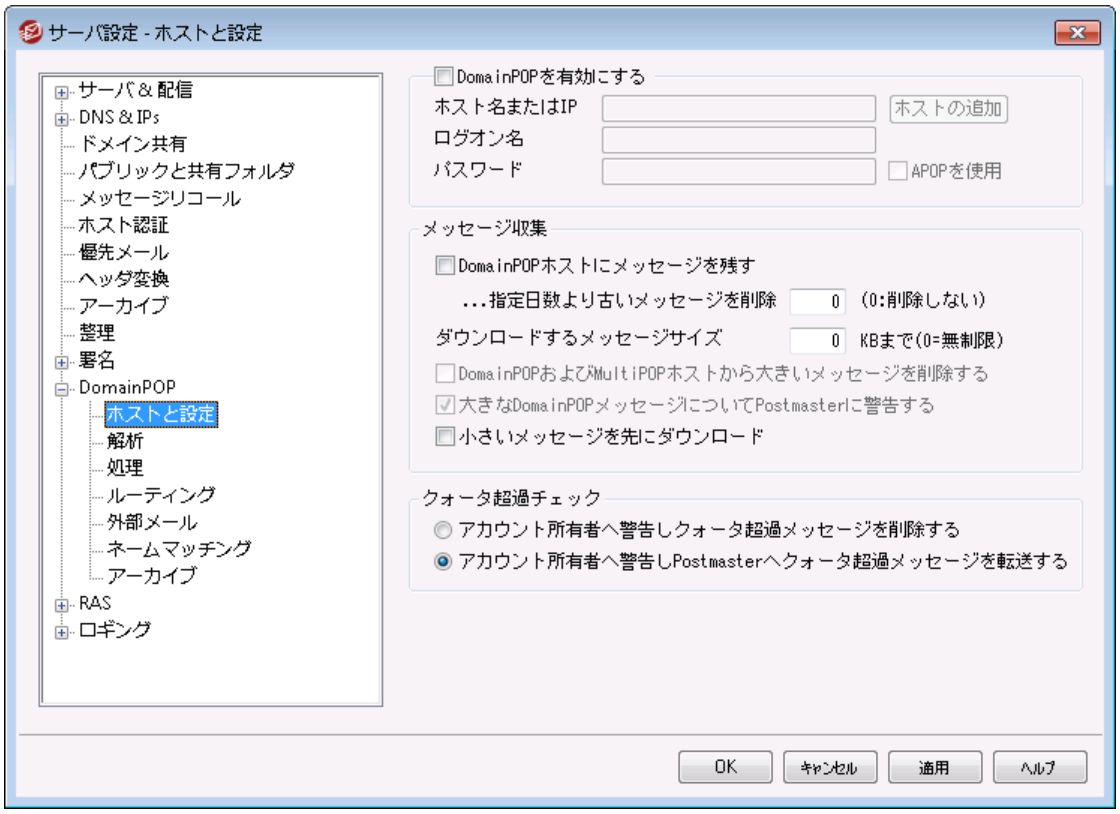
重複メッセージと無限ループするメッセージを防ぐ最後の方法として、MDaemonにはメールがセッション中に何回往復したか、あるいは[ホップ数]が何回なのか、検出する機能が搭載されています。SMTPメールサーバは、メールの処理毎に、そのメッセージに[Received]ヘッダと併せて「スタンプ」を付与します。MDaemonはそのヘッダをカウントし、指定回数を超えるものについては、これを配信ループとみなし、メ

ールストリームからBadキューへと配信されます。この値はRetryキュー[794]画面で設定することができます。

参照:

コンテンツフィルタ[587]
メーリングリスト[245]

3.1.13.1 ホストと設定



DomainPOPホストプロパティ

DomainPOPメール収集エンジンを有効にする
このチェックボックスを選択すると、MDaemonは、この画面上で提供される設定を使って、ローカル再配信のためにDomainPOPメールホストからメールを収集します。

ホスト名またはIP
ここにDomainPOPホストのドメイン名を入力してください。

ログオン名
DomainPOPによって使用されるPOPアカウントのログオン名を入力してください。

パスワード
POPまたはAPOPアカウントのパスワードを入力してください。

APOPを使用
メールを検索する際に、APOPコマンドとCRAM-MD5認証を使用する場合は、このチェックボックスをクリックしてください。これにより、テキストのパスワードを送らずに認証を行うことができるようになります。

メッセージ収集

DomainPOPホストにメッセージを残す
このチェックボックスを選択すると、MDaemonは、DomainPOPメールホストから収集したメッセージを削除しません。

...指定日数より古いメッセージを削除(0=しない)
ここには、メッセージが自動的に削除される前に、そのメールボックスの中に存在できる日数を指定してください。ここに0(ゼロ)を指定すると、そのメッセージは削除されることがありません。

一部のホストでは、メールボックスに保存できるメッセージの量を制限している場合があります。

ダウンロードするメッセージのサイズ [XX] KB (0 = 制限なし)
このサイズ(バイト単位)以上のメッセージは、DomainPOPメールホストからダウンロードされずにサーバ上に残ります。サイズに関係なくMDaemonにメッセージをダウンロードする場合は0(ゼロ)を入力してください。

DomainPOPおよびMultiPOPホストから大きなメッセージを削除する
このオプションをクリックすると、MDaemonは、設定されている最大サイズを超えるメッセージを削除します。メッセージはDomain POPおよびMultiPOPメールホストから削除され、ダウンロードはされません。

大きなDomainPOPメッセージについてPostmasterに警告する
このオプションをクリックすると、MDaemonは、Domain POPメールボックスに大きなサイズのメッセージを発見した際に、Postmasterへ警告を発信します。

小さいメッセージを先にダウンロード
メッセージのダウンロードを、小さなサイズから大きなサイズの順で行う場合、このチェックボックスを有効にしてください。

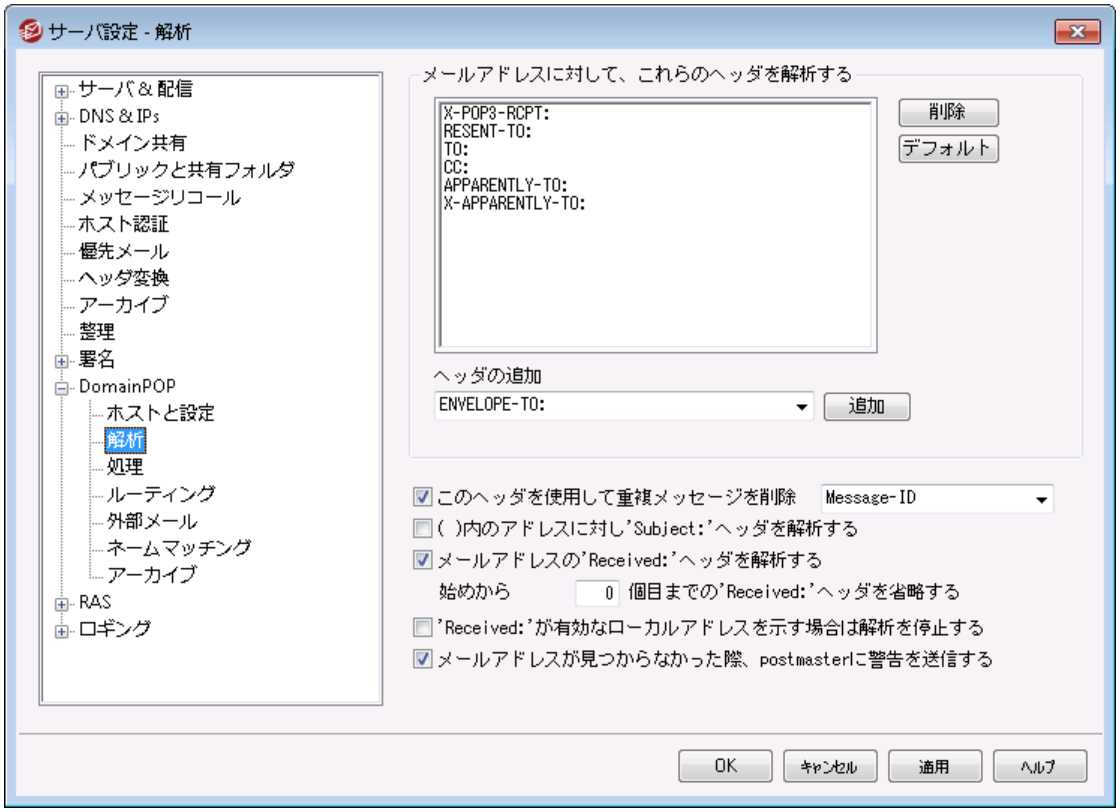
このオプションは、サイズが小さいメッセージは迅速に処理しますが、大きなものは内部的に大量のソーティングと処理を必要とします。

クォータ超過チェック

アカウント所有者へ警告しクォータ超過メッセージを削除する
このオプションが選択され、メッセージがアカウントの割り当て量(アカウントエディタのクォータ666)を超えて収集される場合、MDaemonは、そのメッセージを削除して、そのアカウントのユーザに上限を超えているという警告を送ります。

アカウント所有者へ警告し、Postmasterへクォータ超過メッセージを転送する
このオプションが選択されて、メッセージがアカウントの割り当て量(アカウントエディタの[クォータ]画面で指定される)を超えて収集される場合、MDaemonはメッセージをPostmasterに転送して、アカウントのユーザに上限を超えているという警告を送ります。

3.1.13.2 解析



メールアドレスに関して解析するヘッダ

ここで、MDaemonがアドレスを取り出す際に解析するヘッダのリストです。ここにリストされたすべてのヘッダには、アドレスのチェックが行われます。

削除
このボタンは、ヘッダリストから選択されたエントリを削除します。

デフォルト
このボタンは、現在のヘッダリストの内容をクリアし、MDaemonのヘッダのデフォルトリストを追加します。一般的に、デフォルトのヘッダは、メッセージからすべてのアドレスを取り出すのに十分な情報を持っています。

新規ヘッダ
ここに、ヘッダリストに追加するヘッダを入力してください。

追加
新規ヘッダのフィールドにリストされたヘッダを、ヘッダリストに追加します。

このヘッダを使用して重複メッセージを検出
このオプションが選択されると、MDaemonは、指定されたヘッダの値を記憶し、同じ処理の中で同じ値を含んだメールは処理しません。[Message-ID]ヘッダは、このオプションで使用されるデフォルトヘッダです。

( ) 内のアドレスに対し'Subject:'ヘッダを解析する
このチェックボックスが選択された状態で、MDaemonがメッセージの[Subject:]ヘッダ内の ( ) に囲まれるアドレスを見つけると、そのアドレスは他の解析されたアドレスと一緒に、メッセージの受信者のリストに加えられます。

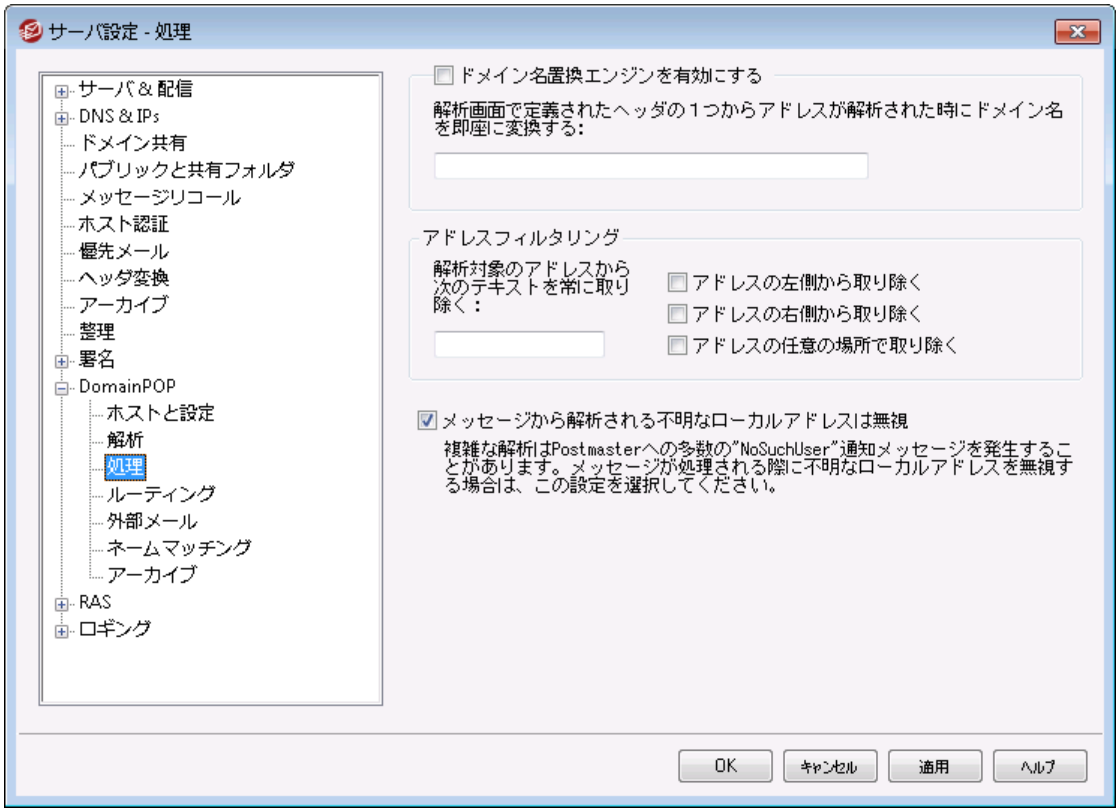
メールアドレスの"Received:"ヘッダを解析する
通常は"Received"メッセージのエンベロープでのみで検出される受信者情報を、メッセージヘッダに保存することが可能です。その結果、メールメッセージの解析処理において、単にヘッダを検査するだけで実際の受信者アドレスを収集することができるようになります。メールメッセージ内で検出される"received"ヘッダの全部の有効なアドレスを解析する場合、このチェックボックスをクリックしてください。

始めから xx 個目までの"Received:" ヘッダを省略する
サーバ構成によって、Receivedヘッダを解析はするものの、最初のいくつかを省略したい場合には、ここで省略するヘッダの数を指定します。

"Received:"ヘッダが有効なローカルアドレスを示す場合は解析を停止する
MDaemonが[Received]ヘッダの解析中に有効なローカルアドレスを発見した場合は、後のすべての解析を中止し、MDaemonは可能性のある配信先検索を行いません。

メールアドレスが見つからなかった際postmasterへ警告を送信する
解析処理の中でメールアドレスが見つからなかった際、デフォルトでMDaemonはpostmasterへ警告メールを送信します。警告を送信しないようにするにはこのオプションを無効化してください。

3.1.13.3 処理



ドメイン名置換

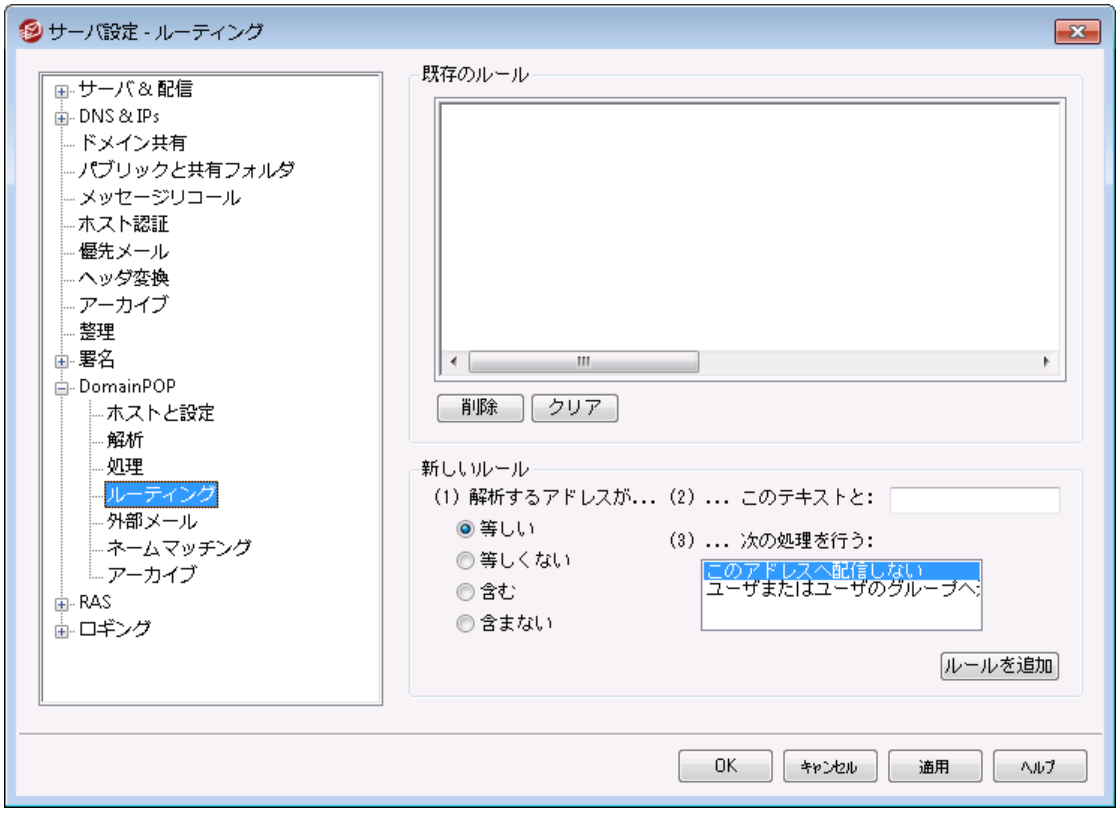
ドメイン名置換エンジンを有効にする
このオプションはサイトが要求するドメインエイリアスの数を減らすことができます。メッセージがダウンロードされると、メッセージから解析されるすべてのアドレス中の全ドメイン名は、ここで指定されるドメイン名に変換されます。

アドレスフィルタリング

解析されるすべてのアドレスから次のテキストを常に取り除く
一部のホストは、左または右側のどちらかにアドレスに付加するわずかなルーティング情報とともに、メッセージの受信者が、だれであるかについて示すラインで、各メッセージにスタンプします。このスタンプは、付加されたルーティング情報が、多くのアカウントエイリアスのない受信者を不可能にすることを除いて、受信者アドレスを解析するための利用に最適です。すべてを実行するのではなく、この機能と関連するエディットコントロールで、この追加されたテキストを指定することができます。そして、MDaemonは解析するすべてのアドレスから、このテキストの発生を取り除きます。

メッセージから解析される不明なローカルアドレスは無視
上の項目にあるように、ドメイン名置換機能は、メッセージから解析される全メールアドレスのドメイン名を、この画面で指定するものに変更します。これにより、ローカルサイトのメールボックスアカウントと一致しない、いくつかのアドレスを作成する可能性があります。ドメイン名はプライマリドメイン名と一致するので、MDaemonは、そのようなアドレスをローカルと考えますが、それらは定義されていません。一般にそのようなメールは、Postmaster宛ての[No Such User]メッセージを生成します。このスイッチはドメイン名置換エンジンが[No Such User]メッセージを生成することを防止します。

3.1.13.4 ルーティング



既存のルール

このリストはすでに作成されて、メッセージに適用されるルールを表示します。

削除
このボタンを押すと既存のルールから選択されたルールが削除されます。

クリア
このボタンはすべての既存のルールを削除します。

新しいルール

(1) 解析されたアドレスが...

等しい, 等しくない, 含む, 含まない
これらは、アドレスがこのルーティングルールと比較される時に作成される比較のタイプです。MDaemonは、各アドレスの[このテキスト]フィールドに含まれるテキストを検索し、このコントロールの設定にしたがって処理します。完全なテキストが正確に一致しているか、いないか、テキストが含まれるか、含まれないか、などの項目で検索します。

(2) ...このテキスト:
ここに、処理されるアドレスをテストする時に使用するテキスト文字列を入力してください。

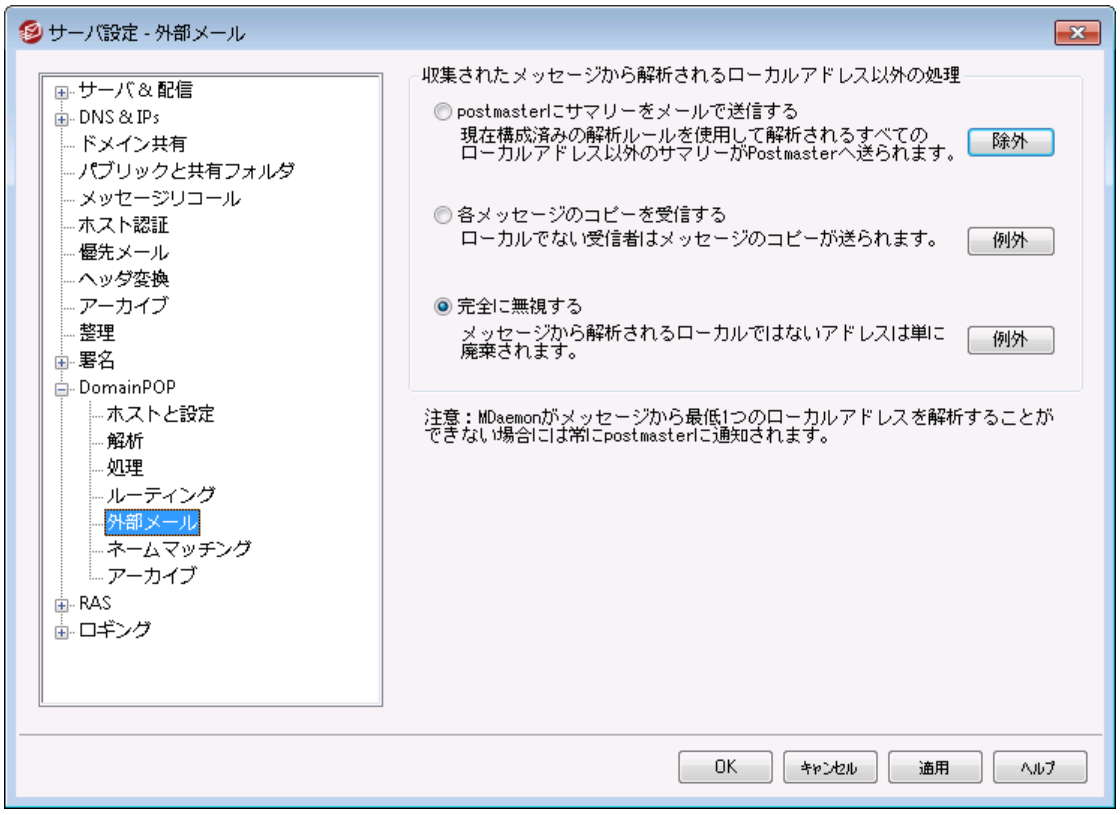
(3) ...次の処理を行う:
ここには、そのルールの結果が真(true)の場合に利用可能なアクションがリストされます。以下はそのアクションの一覧とその内容です。

このアドレスへ配信しない - このルールを選択すると、指定されるアドレスへそのメッセージが配信されるのを防ぎます。

ユーザまたはユーザのグループへ送信 - このルールを選択すると、処理されたメッセージのコピーを受信するメールアドレスのリストが作成できるダイアログが表示されます。

ルール追加
新規ルールのパラメータを設定後、ルールのリストへ登録する場合に、このボタンをクリックします。

3.1.13.5 外部メール



収集されたメッセージから解析されるローカルアドレス以外の処理...

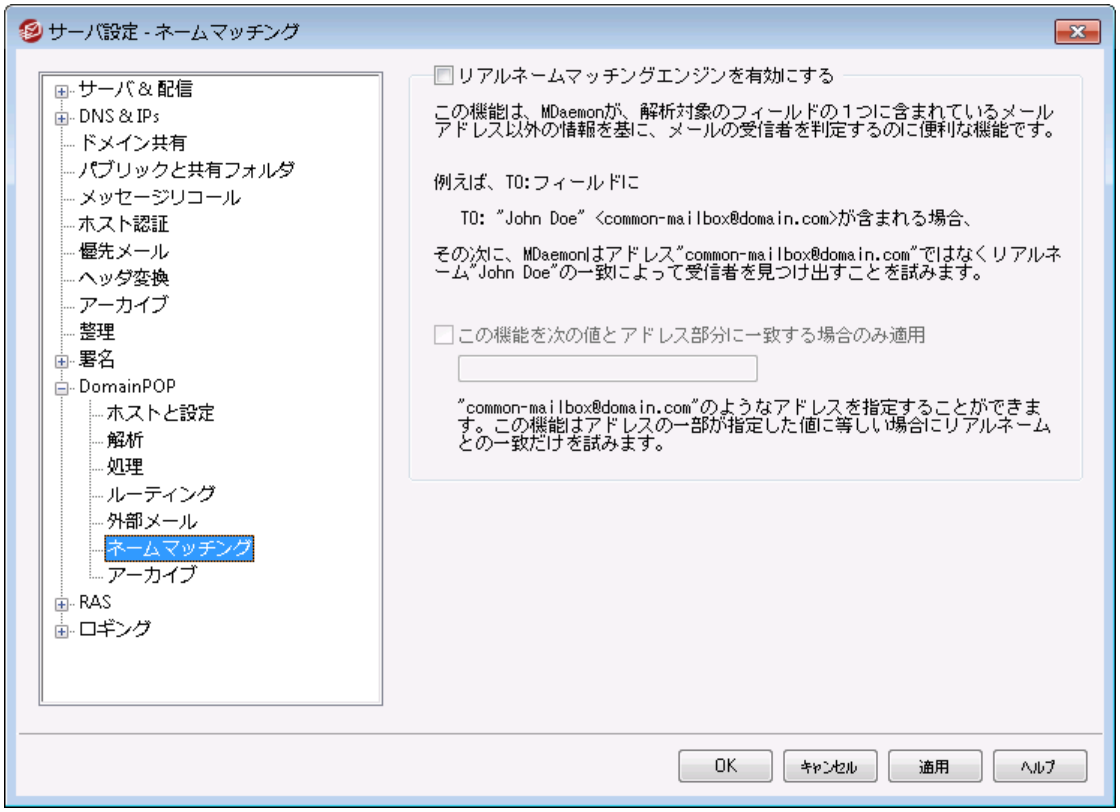
...postmasterへサマリーをメールで送信する
このオプションを選択すると、Postmasterへ、対象のヘッダと解析ルールを元に取りだした、ローカルユーザー以外のアドレスのサマリー情報のコピーを送ります。

...各メッセージのコピーを受信する
このオプションを選択すると、対象のヘッダで検出されたローカルアドレス以外の宛先へ、メッセージのコピーが配信されます。

...完全に無視する
このオプションを選択すると、ローカルアドレス以外のアドレスが受信者リストから削除されます。MDaemonは、元のダウンロードされたメッセージからのリモートアドレスを、解析しないようになります。

除外と例外ボタンでルールの例外となるアドレスを定義することができます。

3.1.13.6 ネームマッチング



ネームマッチング機能は、DomainPOPメール収集エンジンと組み合わせた場合のみ動作します。この機能を使用する場合は、DomainPOPを有効にする必要があります。DomainPOPは 設定 ≫ サーバ設定 ≫ DomainPOP"で設定できます。

リアルネームマッチング エンジン

リアルネームマッチングエンジンを有効にする
この機能により、MDaemonは、解析されたメールアドレスではなく、アドレスで含まれるテキスト部分によって、DomainPOP収集されるメッセージの受信者を決定することができます。これは一般的には宛先のリアルネームです。

例えば、メッセージの[TO:]ヘッダは以下のようになります:

TO: "Michael Mason" <user01@example.com>

または

TO: Michael Mason <user01@example.com>

ネームマッチングは、アドレスの "user01@example.com"の部分は無視します。その代わり、[Michael Mason]の部分を取り出し、これがMDaemon ユーザあるか検索します。アカウントのリアルネームフィールドに一致した名前を見つけると、そのアカウントのローカルのメールアドレスが配信のために使われます。見つからない場合は、MDaemonはデータから解析したメールアドレス(この例では user01@example.com)へメッセージの配信を行います。

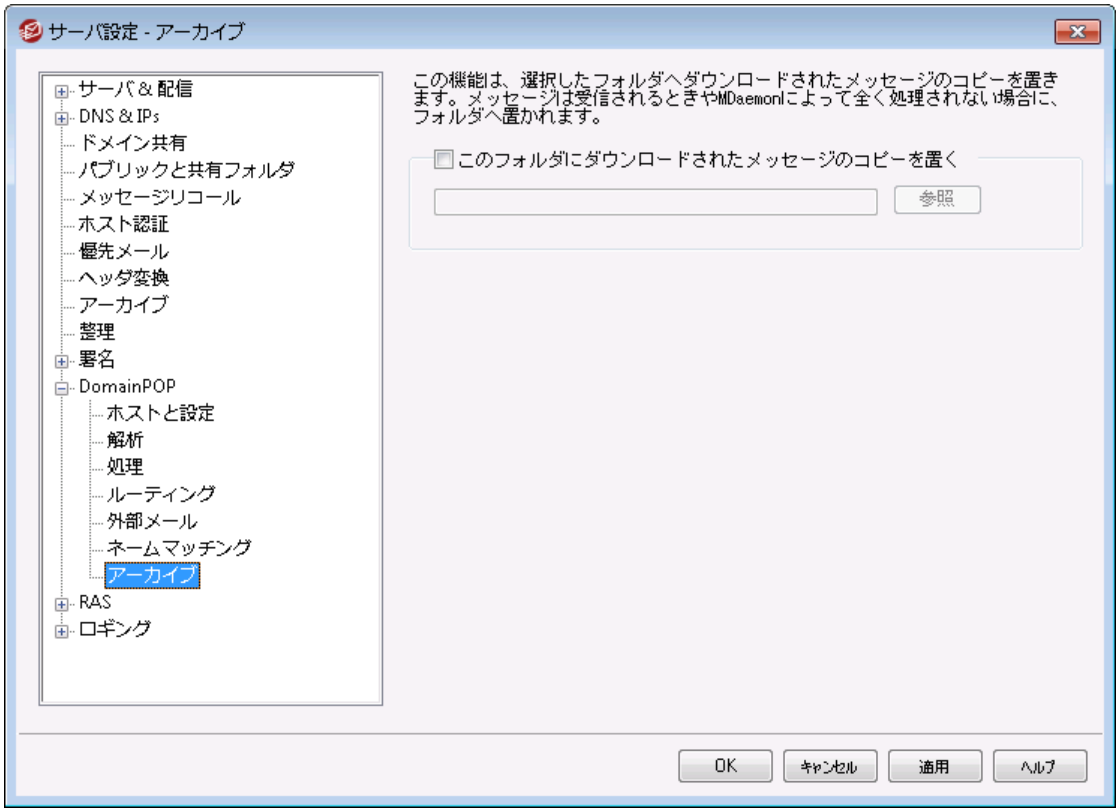
アドレスのリアルネームの部分はカンマ、セミコロン、コロンを含むことはできません。

この機能をアドレス部分が以下の値にマッチする場合のみ適用
このオプションでは、リアルネームマッチング処理を行うために取り出されるデータに必要なメールアドレスを指定することができます。これはネームマッチング機能が採用された場合のコントロール手段となります。例えば、アドレスとして"user01@example.com" のように指定すると、この値に一致するアドレスのみがネームマッチングの候補となります。

このオプションで "user01@example.com"と指定すると 、これは、次のような意味になります。

"TO: 'Michael Mason' <user01@example.com>" はネームマッチングの候補になりますが、 TO: 'Michael Mason' <user02@example.com> はなりません。

3.1.13.7 アーカイブ

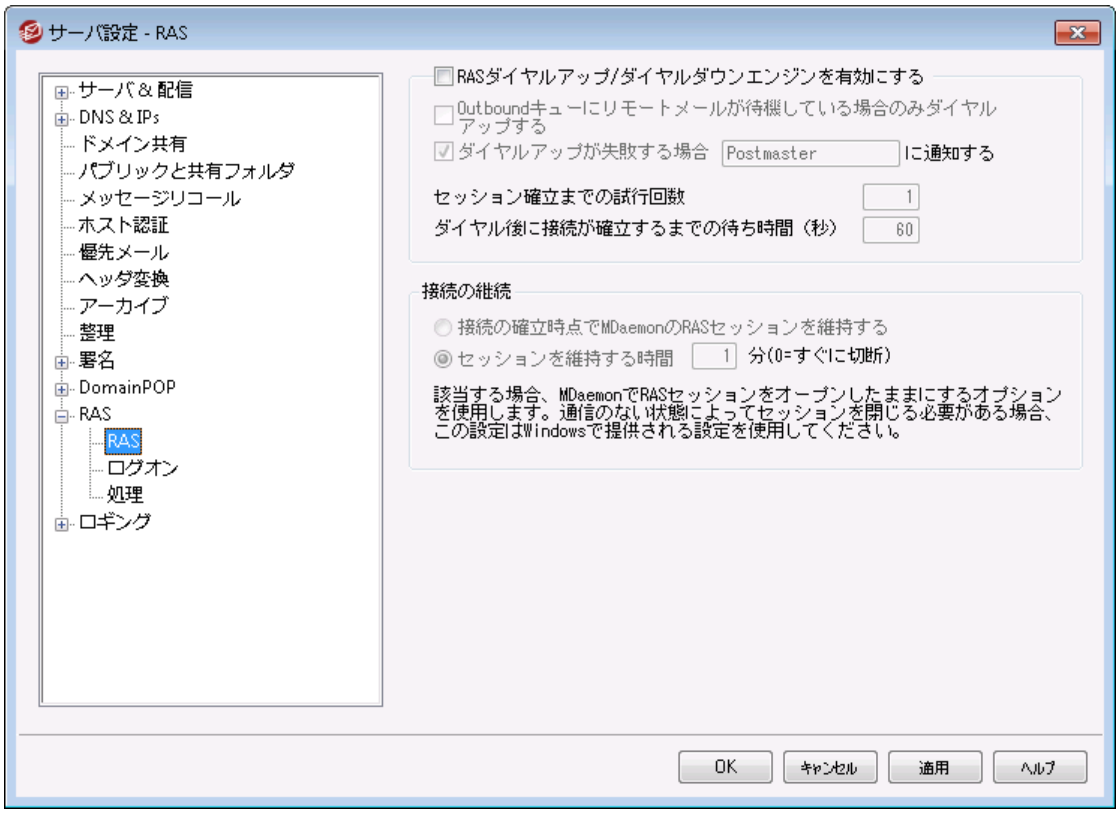


アーカイブ

このフォルダにダウンロードされたメッセージのコピーを置く
これは、多量にメールをダウンロードする時は、出現する可能性がある思いがけない構文解析または他のエラーによるメールを失わないための機能です。ダウンロードしたメッセージのコピーを指定したフォルダへ保存する場合は、このチェックボックスを選択してください。これは、正しく受信しMDaemonによって処理をされていないコピーがフォルダに置かれます。

3.1.14 RAS

3.1.14.1 RAS



"設定 ≫ サーバ設定 ≫ RAS" メニューではRASダイアルアップの設定が行えます。ダイアログはシステム上にリモートアクセスサービスがインストールされている場合にのみ使用できます。MDaemonはリモートメール処理イベントでISPへダイアルアップする時だけ、このサービスを使用します。

RASダイアルアップ/ダイアルダウンエンジンを有効にする
このオプションを選択すると、リモートホストメールを送信または受信する前にリモートホストへ接続するために、ここで指定した設定を使います。

送信キューでリモートメールが待機している場合のみダイアルアップする
このチェックボックスを選択すると、リモートメールがリモートキューで送信待ちしていない場合、ISPへダイアルアップしません。これは、いくつかの環境では有効ですが、ダイアルアップをしないとメールの収集もできない（ローカルLAN内の配信以外）ことに注意してください。

通知 [アドレス]（ダイアルアップに失敗したとき）
このチェックボックスを選択すると、何かのエラーでダイアルアップ予定が失敗した場合、指定したアドレスへメッセージを送信します。

セッションを確立するために試行する回数
接続を切断する前に、ここで指定した回数だけリモートホストへ接続します。

ダイアル後 正 しく接 続 するために待 機 する時 間
この値 は、リモートコンピュータが応 答 してRAS接 続 を完 了 するのを、MDaemonで待 つ時 間 を設 定 します。

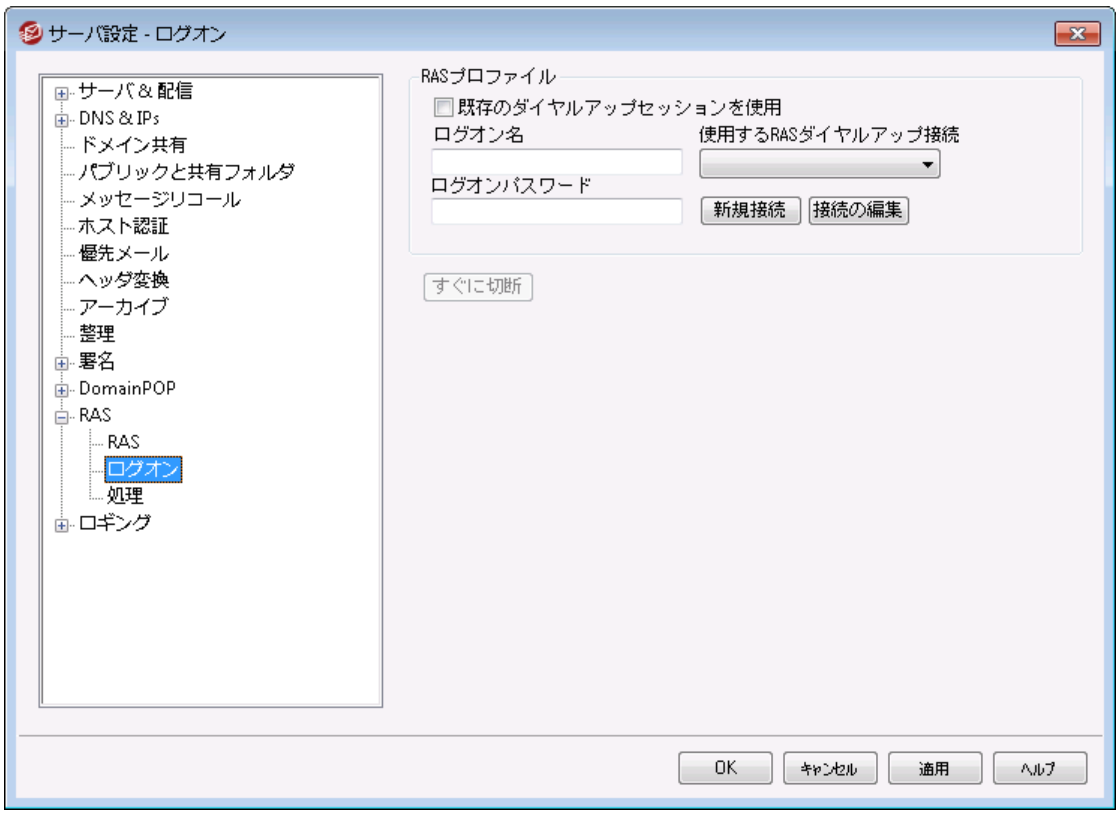
接 続 を継 続

接 続 が確 立 したらMDaemonはRASセッションをクローズしない
デフォルトでは、MDaemonはすべてのメール処 理 が完 了 した後 、すぐに確 立 した接 続 をシャットダウンし、そのセッションは使 用 できなくなります。このオプションを選 択 することにより、すべての処 理 が完 了 した後 でも、接 続 は続きます。

> MDaemonは確 立 していない接 続 をクローズすることはありません。

セッションを維 持 する時 間　最 低 xx　分
このオプションを有 効 にすると、MDaemonが作 成 したRASセッションを、指 定 した時 間（分）だけ、あるいはすべてのメール処 理 が完 了 するまで、どちらか長 い時 間 開 き続 けます。

3.1.14.2　ログオン



RASプロファイル

既存のダイアルアップセッションを使用
このチェックボックスをクリックすると、他のアクティブな接続プロファイルをMDaemonが検知した際に、そのセッションを使用できるようになります。MDaemonは、ダイアルアップする時に、初めに、ダイアルアップの代わりとして利用可能なアクティブな接続があるかどうかを確認します。

ログオン名
ここの指定した値は、認証処理で必要なユーザ識別あるいはリモートホストへ渡すログオン名です。

ログオンパスワード
ここの指定した値は、認証処理に必要なリモートホストへ渡すパスワードです。

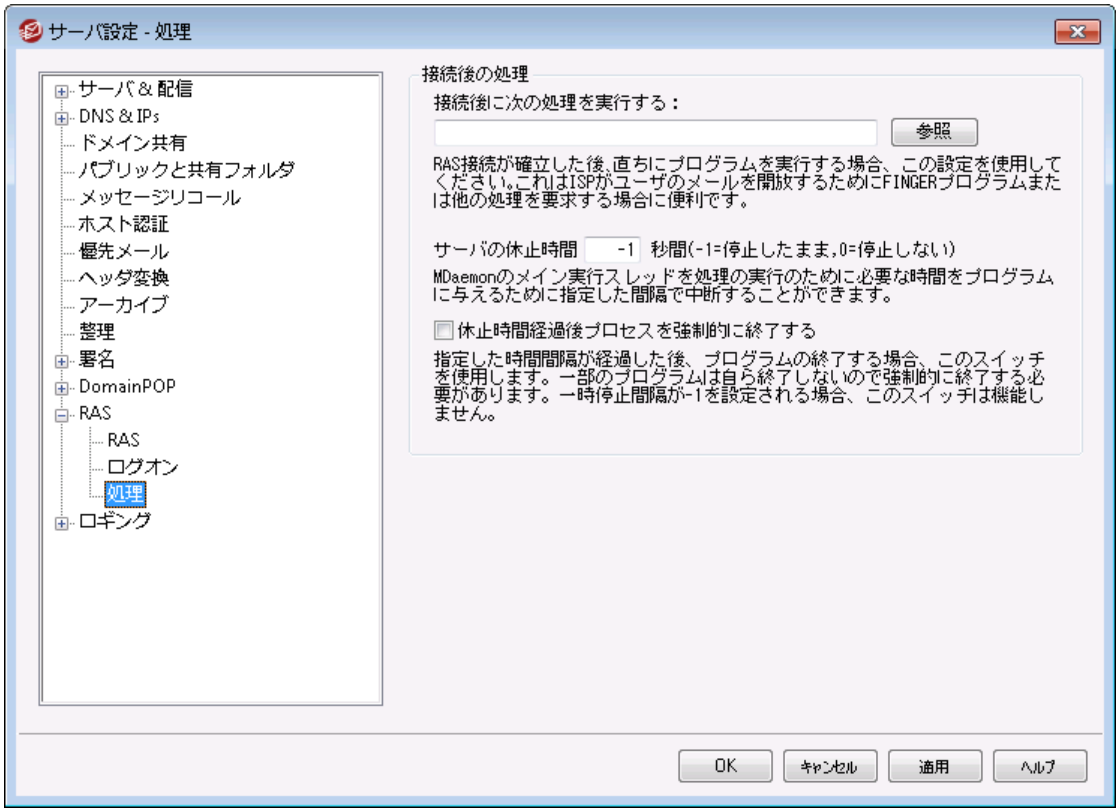
使用するRASダイアルアップ接続
このドロップダウンリストから、Windowsダイアルアップネットワークまたはリモートアクセスサービスの設定によって、前もって定義されたセッションプロファイルを選ぶことができます。

新規接続
このボタンをクリックして、ダイアルアップネットワークまたはリモートアクセスサービスの新しいプロファイルを作成してください。

接続編集
このボタンをクリックして、現在選択されているダイアルアップネットワーク、またはリモートアクセスサービスのプロファイルを編集してください。

すぐに切断
このボタンはISPへの接続を切断します。このボタンは、MDaemonがRASセッションを開始した場合にのみ動作します。

3.1.14.3 処理



接続後の処理

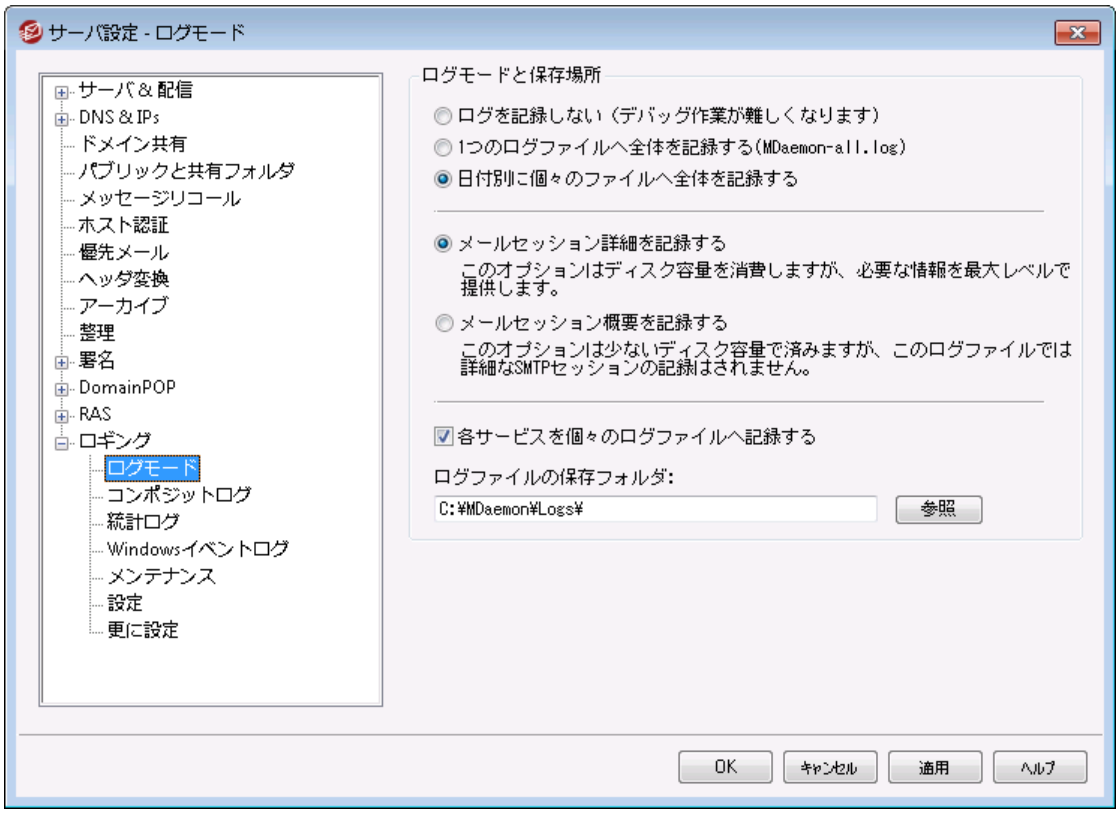
接続されたら、以下の処理を実行する
ここにプログラムが指定されると、MDaemonはスレッドを作成し処理を実行します。これは、ISPのメールボックスをアンロックするためにFinger、または他のプログラムが必要な場合にとても便利です。

サーバの休止時間 (-1 = 停止したまま, 0=停止しない)
[接続されたら以下の処理を実行する]のフィールドが有効なエントリを含む場合、サーバは実行している処理が戻るまで待つ一方で、ここで指定した時間(秒)だけ作業を一時停止させます。-1を入力すると、サーバは処理が戻るまで無制限に待ち続けます。

休止時間経過後、プロセスを強制的に終了する
実行する必要のあるプログラムは、実行しはじめると終了しない場合があります。いくつかのプログラムは終了するためにユーザによる処理が必要です。これはソフトウェアが単独で動作する場合には受け入れられません。このスイッチが選択されると、MDaemonは、[**サーバの休止時間 XX秒間**]で指定した時間(秒)が経過すると、処理スレッドを強制終了させます。この機能は、処理に戻るのを無制限に待ち続けるようにサーバを構成している場合は動作しません。

3.1.15 ロギング

3.1.15.1 ログモード



設定 ≫ サーバ設定 ≫ ロギング メニューをクリックし、ログの設定が行えます。ログは問題を分析し、管理者がいない間にサーバーに何が起こったのかを特定するのに役立ちます。

> 初期設定ダイアログには、MDaemonの管理画面でイベントトラッキング画面に表示されるログデータの量、といった幾つかのオプションがあります。詳細な情報については、初期設定 ≫ UI 447をご参照下さい。

ログモードと保存場所

ログを記録しない
このオプションを選択すると、すべての記録が無効になります。ログファイルは作成されますが、データの記録はされません。

> このオプションの使用を推奨しません。メールに関連する問題が生じた場合に、ログが残っていない場合には、問題の解決は非常に難しくなります。

1つのログファイルへ全体を記録する(MDaemon-all.log)
全体のアクティビティを`MDaemon-all.log`という名称の1つのファイルに記録する場合は、このオプションを有効にしてください。

日付別に個々のファイルへ全体を記録する
このオプションを選択すると、日毎に別々のログファイルが生成されます。ファイル名は作成された日付を元に作成されます。

メールセッション詳細を記録する
このオプションを有効にすると、セッション毎に最大レベルのログ情報が記録されます。

メールセッション概要を記録する
このオプションを有効にすると、セッション毎のサマリーがログファイルに記録されます。

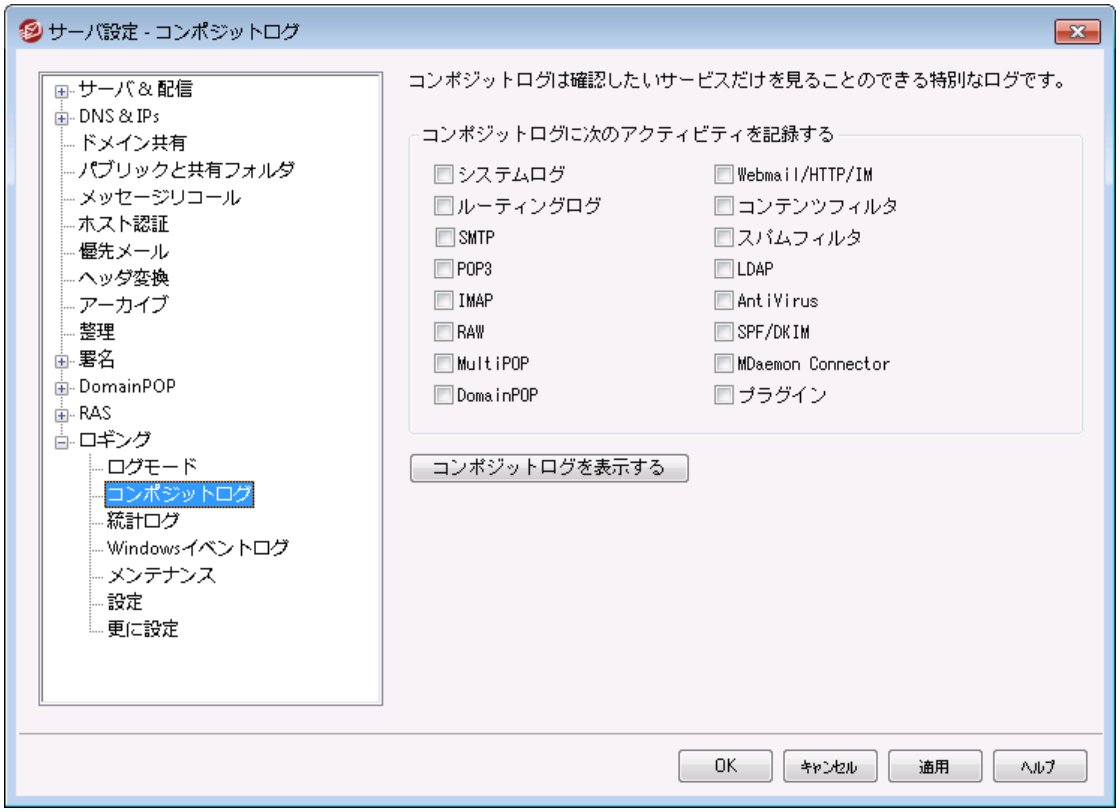
各サービスを個々のログファイルへ記録する
このチェックボックスをクリックすると、1つのファイルではなく、サービス毎に個々のログファイルを管理できます。例えば、このスイッチにより、MDaemonはSMTPアクティビティをMDaemon-SMTP.logへ、IMAPアクティビティをMDaemon-IMAP.logへ記録します。MDaemonインターフェイスでConfigurationSessionやターミナルサービスのインスタンスを実行する場合は、ログ情報を表示するタブ用に、このオプションを選択する必要があります。

このフォルダへログファイルを置く:
ログファイルの格納場所として特定のフォルダを指定する場合は、このオプションを使用します。

BadAddress.txtファイル

ログファイルに加え、MDaemonはログフォルダへBadAddress.txtを保持しています。送信メールで5xxエラーが発生した場合、アドレスはこのファイルへ追記されます。これは、例えばメーリングリストへ機能していないアドレスがあった場合に対象アドレスを特定するのに、SMTPログを確認するよりも簡単に確認が行えます。このファイルはサイズが大きくなりすぎないよう、日別の夜間処理内で自動的に削除されます。

3.1.15.2 コンポジットログ



コンポジット ログ

コンポジット ログに次 のアクティビティを記 録 する
MDaemonメニューバーのWindowsメニューにはコンポジット ログ表 示 オプションがあります。このオプションをクリックすると、1つ以 上 のイベント 追 跡 タブの情 報 を表 示 するための画 面 がMDaemonの管 理 画 面 へ追 加 されます。ここではどの画 面 の情 報 をウィンドウ内 で表 示 するかを指 定 することができます。以 下 から表 示 する情 報 を選 択 してください。

システム
サービスの初 期 化 やMDaemonにサーバの有 効 /無 効 のようなMDaemonのシステムアクティビティを表 示 します。

ルーティング
MDaemonによって分 析 された各 メッセージのルーティング情 報（To、From、Message IDなど）を表 示 します。

SMTP
SMTPプロトコルを使 用 したすべての送 信 /受 信 セッションアクティビティが表 示 されます。

POP3
ユーザが、POP3プロトコルを使 用 してMDaemonからメールを収 集 する際 のアクティビティが表 示 されます。

IMAP
IMAPプロトコルを使 用 したメールセッションが表 示 されます。

RAW
RAW あるいはシステムが生 成したメッセージアクティビティが表 示されます。

MultiPOP
MDaemonのMultiPOPメール収 集 アクティビティを表 示します。

DomainPOP
MDaemonのDomainPOPアクティビティを表 示します。

Webmail/HTTP/IM
すべてのWebmailとインスタント メッセージのアクティビティを表 示します。

コンテンツフィルタ
MDaemonのコンテンツフィルタのアクティビティが表 示されます。

Spam Filter
すべてのスパムフィルタリングアクティビティが表 示されます。

LDAP
LDAPアクティビティが表 示されます。

AntiVirus
AntiVirusの動 作 が表 示されます。

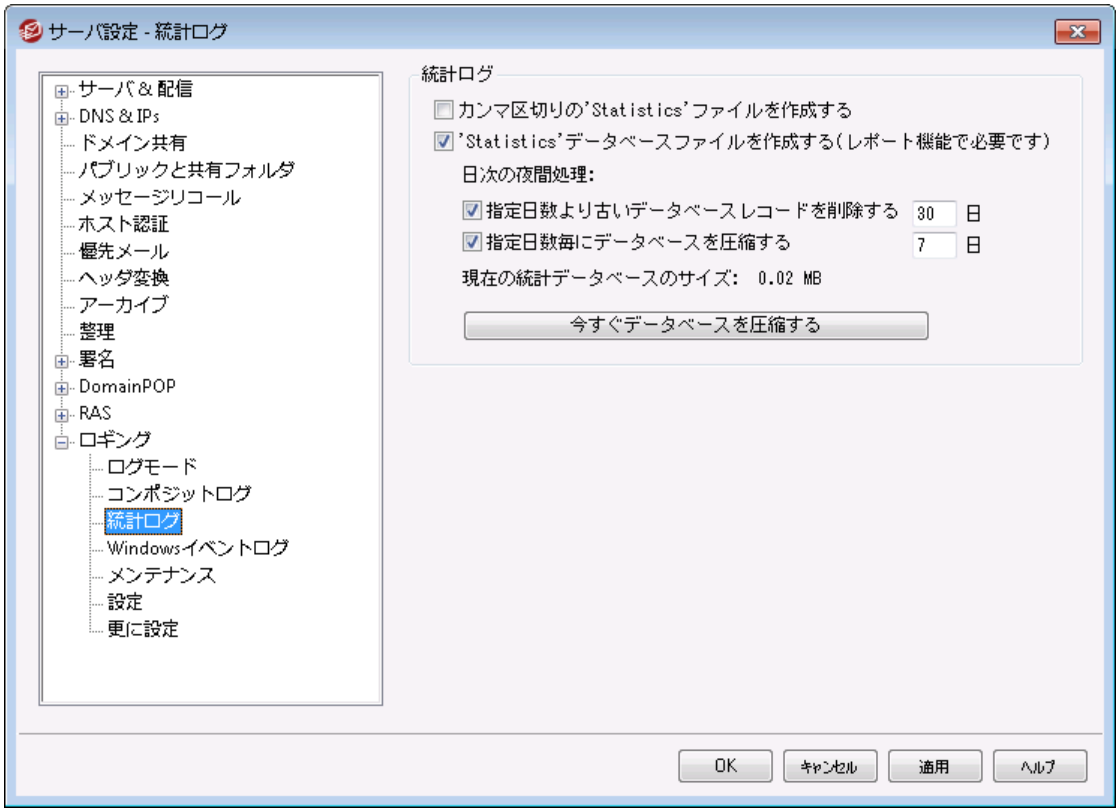
SPF/DKIM
すべてのSPFとDKIMのアクティビティが表 示されます。

MDaemon Connector
すべてのMDaemon Connectorのアクティビティが表 示されます。

プラグイン
コンポジット ログへMDaemonプラグインのアクティビティが表 示されます。

コンポジット ログを表 示 する
このボタンをクリックするとMDaemonのメイン画 面 にコンポジット ログウィンド ウが追 加されます。これは MDaemonツールバーのウィンド ウメニューからも表 示 できます。

3.1.15.3 統計ログ



統計ログ

カンマ区切りの'統計'ファイルを作成する
カンマ区切りの統計ログを管理する場合はこのオプションを使用します。統計ログには送受信メール数、スパム統計、アンチウィルス統計などの情報が含まれています。このオプションはデフォルトで無効になっています。

'統計'データベースファイルを作成する(レポート機能で必要です)
ログの統計情報をSQLiteデータベースファイルへ記録する場合はこのチェックボックスをクリックします。データベースにはMDaemonの使用帯域、送受信メールの数、スパム統計などの情報が含まれています。デフォルトでこのデータベースは"MDaemon¥StatsDB"フォルダへ30日間保存されますが、保存期間は30日から任意の期間へ変更できます。指定日数よりも古いデータは深夜のメンテナンス処理の1つとして削除されます。MDaemonが空き容量を確保するためデータベースの圧縮を行う頻度もここから設定できます。

MDaemonのRemote Administration用レポートページでも、全体管理者向けに様々なレポートが生成されています。各レポート用に、データはそれぞれの期間で生成されており、管理者は任意の期間を指定する事もできます。管理者は次のレポートを選択できます。

- 拡張帯域レポート
- 受信 vs. 送信メッセージ
- 適正 vs. ジャンクメッセージ(スパムやウィルスメールのパーセンテージ)
- 処理した受信メール数

- メッセージ数での上位受信者
- メッセージサイズの上位受信者
- 処理した送信メール数
- スパム送信者の上位（ドメイン）
- スパム受信者の上位
- 時間別にブロックされたウィルス
- 名前別にブロックされたウィルス

日時の夜間処理:
次のオプションは夜間のメンテナンス処理として実行できるデータベース関連タスクです。

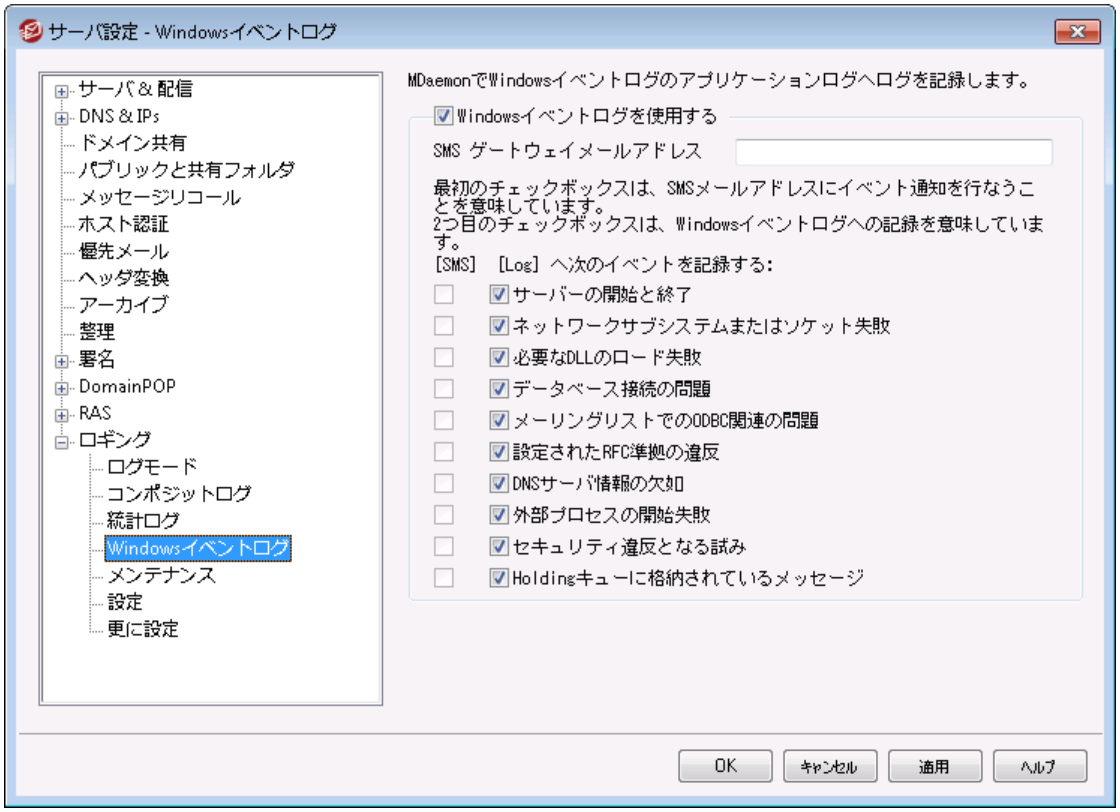
指定日数より古いデータベースレコードを削除する
統計データベース情報を保持する最大日数を指定します。このオプションはデフォルトで有効で、30日間です。

指定日数毎にデータベースを圧縮する
空き容量を確保するため定期的にデータベースの圧縮を行う場合はオプションで指定します。デフォルトでこのオプションは有効で、圧縮は7日間毎に行われます。

現在の統計データベースのサイズ:
現在の統計データベースのサイズが表示されます。

今すぐデータベースを圧縮する
すぐにデータベースの圧縮を行う場合はこのボタンをクリックします。

3.1.15.4 Windowsイベントログ



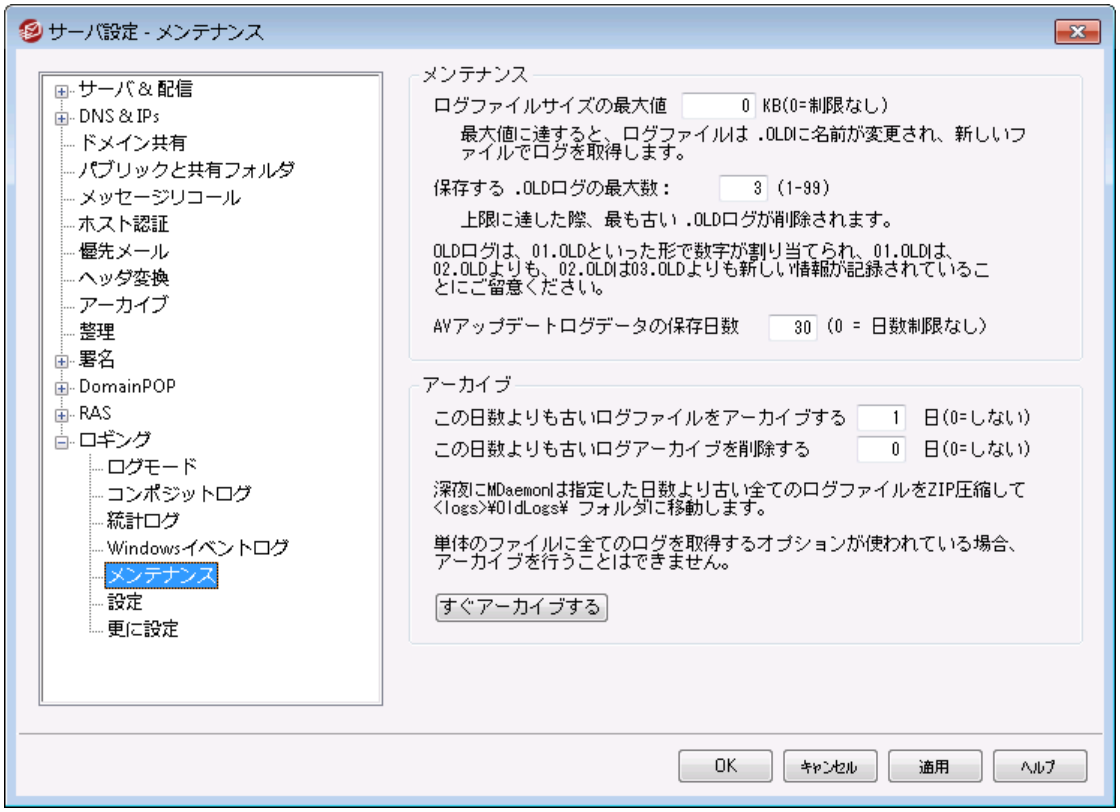
Windowsイベントログを使用する
重要なシステムエラーや警告などのログをWindowsイベントログのアプリケーションセクションへ記録する場合は、このチェックボックスを有効にしてください。

SMSゲートウェイメールアドレス
イベントデータをSMS（テキスト）メールとして特定の端末へ送信する場合はこのオプションを使用して下さい。このオプションでは、例えばVerizonであれば`PhoneNumber@vtext.com`（例. `8175551212@vtext.com`）といった、電話キャリアの提供するメールをSMSとして送信する事ができるメールアドレスを記入して下さい。その後端末に送信したいイベントをSMSカラムのチェックボックスで指定して下さい。

SMS | 次のイベントを記録:
端末にテキストメッセージでイベントを記録するのにSMSオプションを使用できます。Windowsイベントログのアプリケーションセッションへイベントのログを記録する場合は、ログオプションを使用して下さい。SMSメッセージを送信するには、上記の電話キャリアのメールをSMSゲートウェイへ変換する事ができるメールアドレスオプションを使用して下さい。また、通知メールをSMSゲートウェイへ送信するイベントによって、リモートキューが処理されます。通知は「緊急」メールとして処理されます。

サーバーの開始と終了イベント用のSMSオプションでは、開始イベントメールをSMSとして通知しますが、終了イベントは通知しません。

3.1.15.5 メンテナンス



メンテナンス

ログファイルサイズの最大値 [xx] KB

ログファイルの最大サイズをキロバイト単位で指定します。ファイルサイズが指定したサイズに到達するとログファイルはLOGFILENAME.01.OLDにコピーされ、新しいログを開始します。
LOGFILENAME.01.OLDが存在している場合は、下記の「保管する.OLDログの最大数」の値に沿って、古いログファイルは削除されるか、LOGFILENAME.02.OLDにコピーされます。ファイルサイズで制限をかけたくない場合は、この値を「0」へ設定して下さい。このオプションはデフォルトで「0」が設定されています。

保存する.OLDログの最大数 (1-99)
上記のログファイルサイズを制限するオプションを使用している場合、このオプションで保管する.OLDログファイルの数を指定します。バックアップファイルは「LOGFILENAME.01.OLD」「LOGFILENAME.02.OLD」といったファイル名になり、最も新しいものが少ない数字となります。例えば、SMTP(out).log.01.old は`SMTP(out).log.02.old`よりも新しいファイルとなります。最大数に到達すると、新しいファイルが生成されたタイミングで、一番古いログを削除します。

AVアップデートログデータの保存日数 (0=日数制限なし)
このオプションではAntivirusアップデートログ（例. avupdate.log）を何日間保管するかを指定します。日時の夜間処理やMDaemonのアップグレード後の起動のタイミングで、古いデータがファイルから削除されます。日数制限を設けない場合は0を指定して下さい。デフォルトでは、30日間分のデータが保存されます。

AVアップデートログはデフォルトでサイズの上限として5120 KBが設定されています。サイズ制限を変更したり制限をなくしたい場合は、**セキュリティ ≫ AntiVirus ≫ AVアップデータ ≫ AVアップデータ構成 ≫ 初期設定**にある AVアップデータ設定 615 ダイアログから設定変更して下さい。

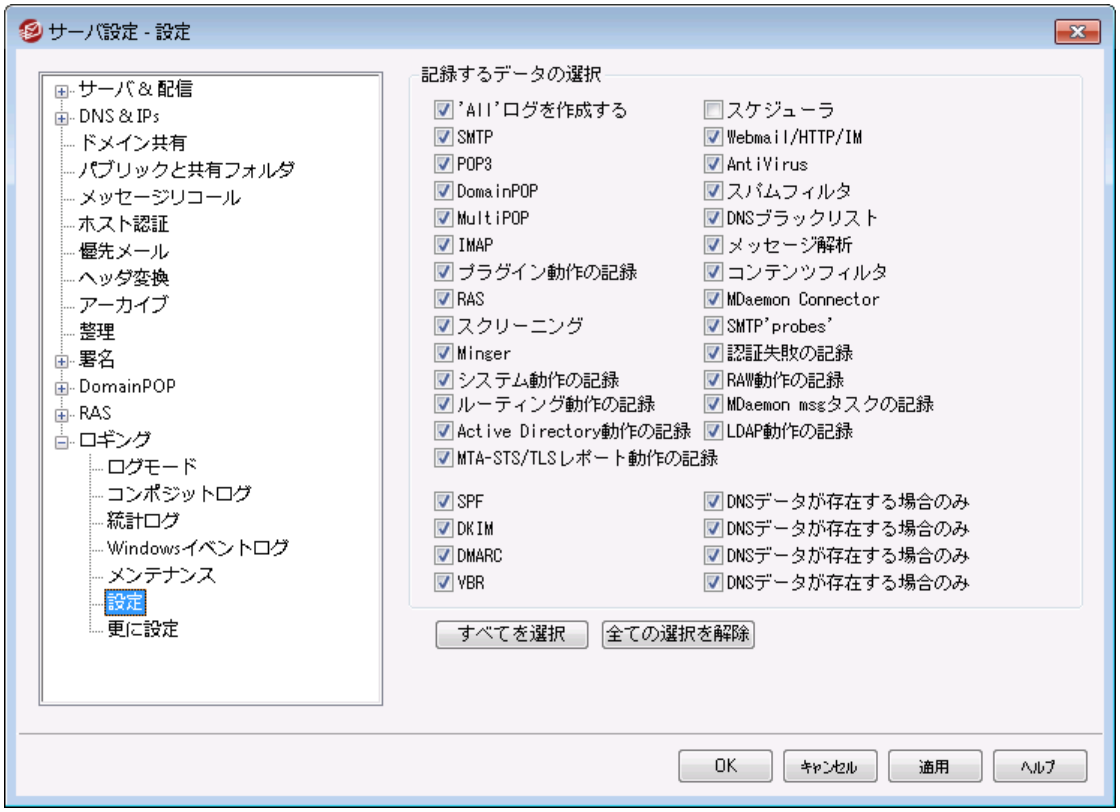
アーカイブ

この日数よりも古いログファイルをアーカイブする (0=しない)
ここで指定した日数よりも古いログファイルをアーカイブする場合は、このオプションを有効にしてください。毎日深夜、MDaemonは古い*.logファイルと*.oldファイルをZIP化し、(オリジナルファイルを削除して) ¥Logs¥OldLogs¥サブフォルダに移動します。この処理では使用中のファイルはアーカイブや削除はされません。ただしログモード 150 画面で*単体のファイルに全てのログを取得する (MDaemon-all.log)*が有効な場合はアーカイブされます。

この日数よりも古いログファイルを削除する (0=しない)
ここで指定した日数よりも古いアーカイブされたログファイルを自動削除する場合はこのオプションを使用します。0で自動削除を行わなくなります。削除処理は、毎日深夜に実行されます。

すぐアーカイブする
MDaemonの自動アーカイブ処理を待たずに、古いログファイルを即座にアーカイブする場合は、このボタンをクリックしてください。

3.1.15.6 ログ設定



記録するデータの選択

'All' ログを作成する
すべての活動を記録する "*-all.log"ファイルを作成する場合は、このオプションを有効にしてください。

SMTP
MDaemonのSMTP送受信ログを記録する場合は、このオプションを有効にしてください。

POP3
すべてのPOPに関するログを記録する場合はこのチェックボックスを有効にしてください。このオプションはユーザのPOP収集セッションを記録します。

DomainPOP
すべてのDomainPOPメールを記録する場合はこのチェックボックスを有効にしてください。

MultiPOP
すべてのユーザのMultiPOP収集を記録する場合はこのチェックボックスを有効にしてください。

IMAP
このオプションを有効にすると、MDaemonのログファイルに全ユーザのIMAPセッションを記録します。

プラグイン動作の記録
このオプションを有効にすると、プラグイン関連動作を記録します。

RAS
ログファイルにRASダイアルアップ/ダイアルダウンの動作を記録する場合は、このオプションを有効にしてください。この情報はダイアルアップに問題が発生した場合の解決に役立ちます。

スクリーニング
このオプションを有効にすると、MDaemonのスクリーニングに関するログが記録されます。

Minger

このオプションを有効にするとMingerサーバアクティビティのログを記録します。

システム動作の記録
このオプションを有効にすると、システム関連動作を記録します。

ルーティング動作の記録
このオプションを有効にすると、Inbound、Local、Remoteキュー全部の処理動作を記録します。

Active Directoryの記録
このオプションを有効にすると、MDaemonに関連したActive Directory動作を記録します。

MTA-STS/TLSレポート動作の記録
全てのSMTP MTA Strict Transport Security（MTA-STS）関連動作を記録します。

スケジューラ
イベントスケジューラ[347]に関する全てのログを記録する場合は、このチェックボックスを有効にします。

Webmail/HTTP/IM
すべてのWebmail、HTTP、MDaemon Instant Messengerのアクティビティを記録する場合は、このオプションを有効にしてください。このオプションを無効にしても、Webmailの起動と終了時間を記録したWebmailとHTTPログファイルは生成されますが、その他のWebmailとHTTP、インスタントメッセージの動作は記録されません。

AntiVirus
AntiVirus の動作をログへ記録するオプションです。

スパムフィルタ
このオプションを有効にするとすべてのスパムフィルタの動作を記録します。

DNSブロックリストの処理
このオプションを有効にすると、DNSブロックリストの動作を記録します。これによりブロックリストされているサイトを簡単に参照することができます。

メッセージ解析
MDaemonはメッセージの配信先を決定する際に、定期的に大量のメッセージを分析します。このオプションを有効にすると、この分析情報がログファイルに記録されます。

コンテンツフィルタ
このチェックボックスを有効にすると、コンテンツフィルタの動作がログファイルに記録されます。

MDaemon Connector
このオプションを有効にすると、MDaemon Connectorの動作が記録されます。

SMTP 'probes'
送信サーバーから(DATAコマンドを使わなかった場合など)メッセージデータを受け取らなかったSMTPセッションについてのログを記録する場合は、このオプションを有効にして下さい。

認証失敗を記録
認証失敗を記録するにはこのオプションを使用します。

RAW動作の記録
MDaemonのRAWメール動作を記録します。

MDaemon msgタスクを記録
メッセージタスクを記録します。

LDAP動作の記録
全てのLDAP動作を記録します。

SPF
すべてのSPF(Sender Policy Framework)のルックアップに関するログを記録する場合は、このオプションを有効にしてください。

...DNSデータが存在する場合のみ
SPFの動作を記録する際に、すべてのSPFルックアップではなく、DNSルックアップでSPFデータが存在した場合のみログを記録する場合は、このオプションを有効にしてください。

DKIM
全てのDomainKey Identified Mail(DKIM)の動作を記録する場合は、このオプションを有効にしてください。

...DNSデータが存在する場合のみ
すべてのアクティビティではなく、DNSルックアップでDKIMデータが存在した場合のみログを記録する場合は、このオプションを有効にしてください。

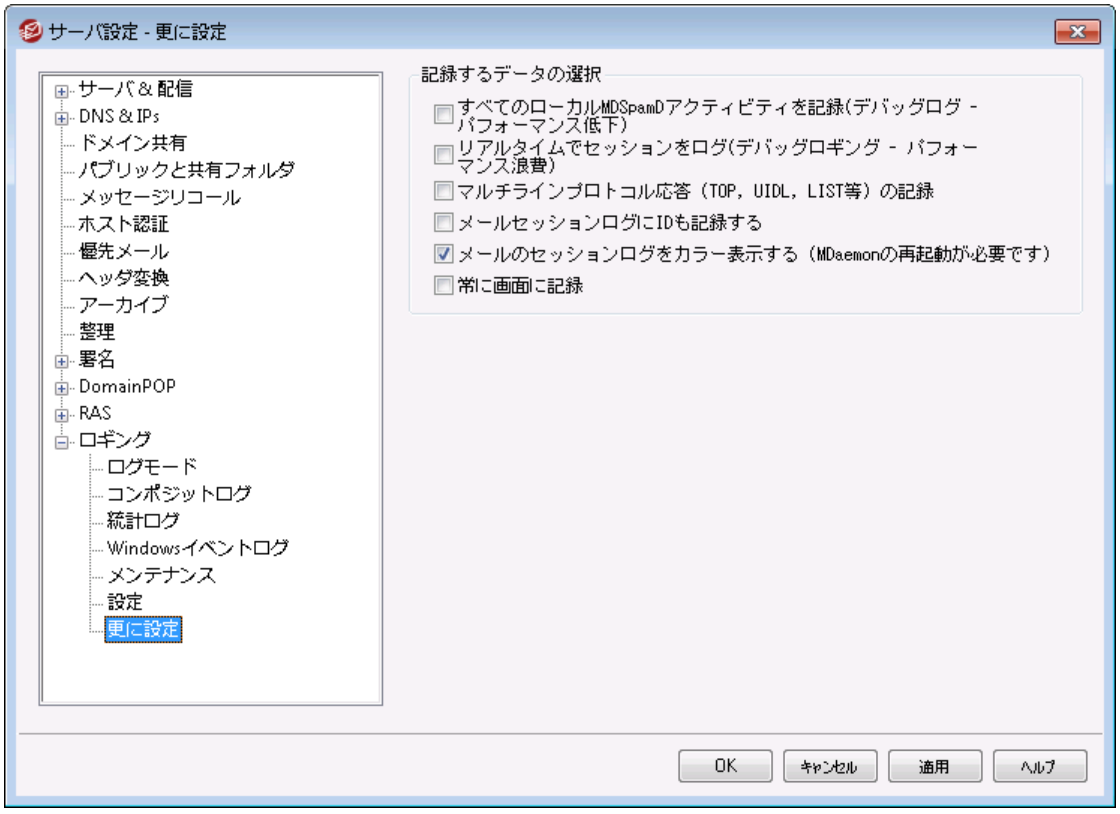
DMARC
DMARCの全ての動作を記録する場合は、このオプションを有効にしてください。

...DNSデータが存在する場合のみ
すべてのアクティビティではなく、DNSデータが存在した場合のみログを記録する場合は、このオプションを有効にしてください。

VBR
メッセージ証明書 501をログに記録する場合はこのオプションを有効にしてください。

...DNSデータが存在する場合のみ
DNSルックアップで証明書データが存在した場合のみログを記録する場合は、このオプションを有効にしてください。

3.1.15.7 詳細ログ設定



記録するデータの選択

全てのローカル MDSpamDアクティビティを記録（デバッグログ –パフォーマンス低下）
全てのローカル MDSpamDアクティビティをログへ残すにはこのオプションをクリックします。（後述の注意点をご覧ください。）

リアルタイムでのセッションを記録（デバッグログ– パフォーマンス低下）
通常、リソースを節約するためにセッション情報はセッションが完了した時点で記録されます。このオプションを有効にすると、セッションログがリアルタイムで記録されます。

> 上記2つのオプションのどちらか又は両方を使用する場合、システムの構成や活動の状況によって、メールシステムのパフォーマンスが低下する可能性があります。これらのオプションはデバッグ目的のみに使用することをお勧めします。

マルチラインプロトコル応答（UIDLやLISTなど）
プロトコルリクエストへの応答が1行を超える場合があります。追加の行のログも記録しておく場合はこのチェックボックスを有効にします。

> このオプションを有効にすると、ログ情報が膨大になる可能性があります。応答が何行になるかは事前には把握できないので、POPやTOPなどメッセージの実際の内容まで含まれる不必要な情報が、ログ情報を一杯にしてしまう可能性があります。もしログファイルのサイズが重要な場合は、この機能を使用することはお勧めしません。

マルチセッションログにログIDも記録する
セッションログに[%d:%d]という固有ID文字列を含める場合は、このオプションを有効にしてください。

メールセッションログをカラー表示（MDaemonの再起動が必要です）
MDaemonの管理画面にあるイベント監視とログ[65]タブのテキスト表示を色分けする場合はこのオプションを使用します。このオプションはデフォルトで無効になっており、有効/無効の切り替えにはMDaemonの再起動が必要です。下記の「セッションログのカラー表示」で詳細をご確認下さい。

常に画面にログを行う
MDaemonが最小化されている時やトレイで動作している時にも、ログデータをMDaemon GUIへコピーしておきたい場合は、このオプションを選択します。

このコントロールが解除されると、MDaemonがシステムトレイで動作している間は、ログがイベント追跡用の画面へコピーされません。同様に、MDaemonを起動した際、最近のアクティビティが表示されなくなり、開いた時点からのログだけが表示されます。

セッションログのカラー表示

MDaemonのユーザ画面[65]にある、ルーティング, SMTP-in, SMTP-out, IMAP, POP, MultiPOP, DomainPOP の状態を表示するタブは、セッション毎に異なるイベントを判別できるようカラー表示できます。この機能はデフォルトでは無効になっていますが、ログ設定 ≫ 更に設定[162]や初期設定 ≫ UI[447]にある*"メールのセッションログをカラー表示する"* オプションを使って有効化できます。デフォルトのテキスト

色はLogColors.datの[Colors]セクションを編集して変更する事ができます。デフォルト色の一覧は下記のチャートを参照して下さい。

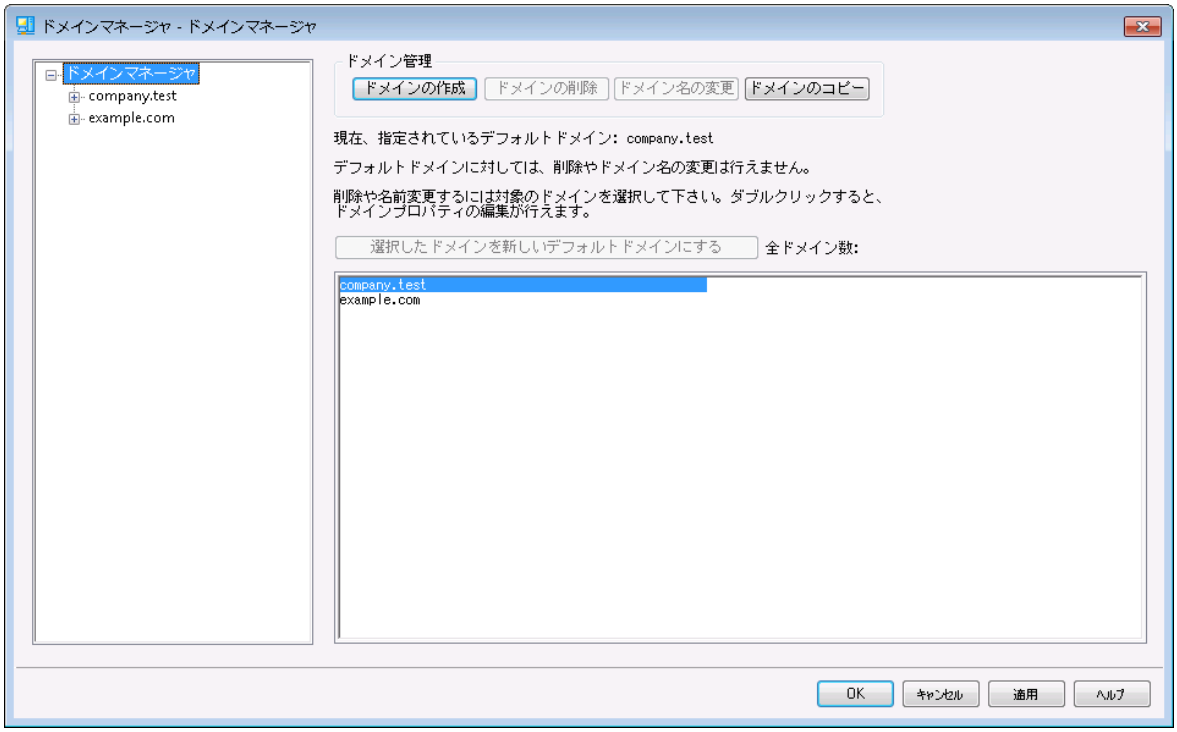
カラー表示を使用はしたいものの、一覧の中のいくつかはカラー表示を行わずに使いたい場合は、対象のカラー要素を0（例えばSpamFilter=0）に設定します。0と指定された要素は、デフォルトの色を使用します。ただし、背景や選択した背景については、色の指定が必要です。色の値は16進数の"0xbbggrr"の形式で指定する必要があります。"0xbbggrr"の"bb"はブルー、"gg"はグリーン、"rr"はレッドを示しています。例えば、"Error=0x0000ff"と指定すると、エラーテキストがレッドで表示されます。**注意点**：これは一般的に知られている"rrggbb"といったカラーコードの反対です。色の変更を行ったら、MDaemonを再起動するか、COLORS.SEMファイルを作成し、MDaemonの¥APP¥フォルダへ置いておく必要があります。

デフォルトのログカラー

Background=0x000000	背景色；ブラック
SelectedBackground=0xff0000	選択済背景色；ブルー
Default=0xffffff	デフォルトテキスト色；ホワイト
Processing=0x00ffff	内部処理と遅延アクティビティ: デフォルトはイエロー
DataIn=0x008040	他のサーバーから受信したデータ: デフォルトはダークグリーン
DataOut=0x00ff00	別サーバー宛の送信データ: デフォルトは明るいグリーン
Error=0x0000ff	エラーメッセージ；デフォルトはレッド
TCPIP=0xff8000	TCP/UDP/DNS/PTR関連アクティビティ；デフォルトはライトブルー
SpamFilter=0x0080ff	スパムフィルタリング；デフォルトはオレンジ
AntiVirus=0xdda0dd	アンチウィルス処理；デフォルトはプラム
DKIM=0xff00ff	DKIM；デフォルトは赤紫
VBR=0x40c0ff	Vouch by Reference処理；デフォルトはライトオレンジ
SPF=0x808080	Sender Policy Framework処理；デフォルトはグレー
Plugins=0x0080c0	プラグインからのメッセージ；デフォルトはブラウン
Localq=0x00ffff	ローカルキューの処理；デフォルトは黄色
Spam=0x0080ff	スパムメッセージ処理；デフォルトはオレンジ
Restricted=0x40c0ff	制限されたメッセージ処理：デフォルトは明るいオレンジ
BlackList=0x808080	ブロックリストメッセージ処理：デフォルトはグレー
Gateway=0x00ff00	ゲートウェイメッセージ処理；デフォルトは明るいグリーン

Inboundq=0xff8000	受信メッセージ処理；デフォルトは明るいブルー
PublicFolder=0xdda0dd	パブリックフォルダのメッセージ処理；デフォルトはプラム

3.2 ドメインマネージャ



MDaemonは複数ドメインに対応しており、ドメインマネージャからドメイン毎の管理を行う事ができます。ドメインマネージャを使うことで、ドメイン名やIPアドレス、アカウントとメッセージの自動削除設定、Webmail設定などドメイン毎に個別の設定を行えます。

MDaemon は、単一のIPアドレスで使用することも、複数のIPアドレスを割り当てて使用することできるため、ドメイン毎に個別のIPアドレスを割り当てたり、1つのIPアドレスを複数のドメインで共有することができます。さらに、アカウントやメーリングリスト、いくつかのセキュリティ設定は、ドメインを基本としています。例えば、アカウントを作成するには、その新しいアカウントが属するドメインを指定する必要がありますし、メーリングリストも同様です。IPスクリーン[510]やIPシールド[474]といった機能も、ドメイン固有の設定としてドメインを指定します。

DomainPOP[134]内にあるネームマッチング[143]のように、いくつかの設定はデフォルトドメインにだけ適用されます。デフォルトドメインは、アカウントやメーリングリストを作成する時のようなドメイン選択を行う際に、デフォルトとしても表示されます。さらに、MDaemonがシステムメッセージを送信するために、デフォルトで用意されている次のエイリアス[757]はMDaemon内のデフォルトドメインにあるメールボックスへ割り当てられています。

```
MDaemon@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
listserv@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
listserver@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
list-serv@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
```

最後に、複数のメールドメインに対応するため、MDaemonはデフォルトでログイン時に使用するユーザー名をメールボックス名（例："user01"）ではなく、完全なメールアドレス（例："user01@example.com"）で指定する必要があります。しかしながら、一部のとても古いメールクライアントにおいては、ログイン名に'@'が使えないものがあります。このようなメールクライアントに対応するため、初期設定のシステム[450]画面で代替文字を指定することができます。メールボックス名とドメイン名の間の区切り文字に、'$'といった代替の一文字を指定することもできますし、最大10文字まで指定することもできます。例えば、'.at.'を指定した場合、"user02.at.example.com"をログイン名として使用できます。ログイン名として、完全なメールアドレス形式を使わないで、メールボックス名だけにすることもできますが、もし今後1つ以上のメールドメインを使用することになる可能性を考えますと、お勧めいたしません。

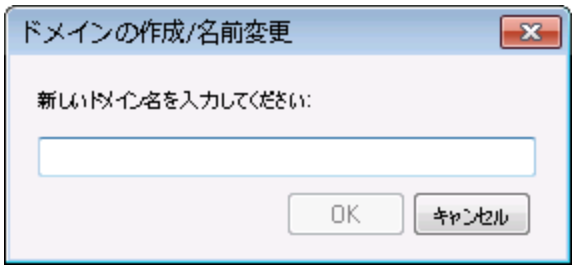
ドメインリスト

この画面の左側には、現在お持ちのドメインがリスト表示され、各ドメイン固有の設定をここから行うことができます。デフォルトドメインは、一番上に表示され、それ以外のドメインはアルファベット順に並びます。画面の右側にあるドメインリストから、ドメインの削除や名前変更、デフォルトドメインの選択が行えます。リストにあるドメインを選択しダブルクリックすると、そのドメインの設定画面となります。

ドメイン管理

ドメインの作成

新しいドメインを作成する: *ドメインの作成* ボタンをクリックし、ドメインの作成/更新 画面にドメイン名を入力し、*OK*ボタンを押します。



一般的に、ここへ入力するドメイン名は、インターネットからこのマシンのIPアドレスへアクセスできるようにDNSサーバに登録されたドメイン名、もしくは別名ホスト名を入力します。この場合には、正しくメール配信を行うために、ヘッダ変換[114]機能やドメイン名置換エンジン[140]も使う必要がある場合もあります。

ドメインの削除

ドメインの削除: 下にあるリストから対象のドメインを選択し、*ドメインの削除*ボタンをクリックし、ドメイン削除の確認表示がされましたら、*はい*ボタンを押します。

> デフォルトドメインに対しては、削除や名前の変更が行えません。もし、削除や名前の変更を行いたい場合には、最初にデフォルトドメインとして別のドメインを選択してから行ってください。

ドメイン名の変更

ドメイン名の変更: 下にあるリストから対象のドメインを選択し、*ドメイン名の変更*ボタンをクリックし、ドメインの作成/更新 画面へ新しいドメイン名を入力し、*OK*ボタンを押します。

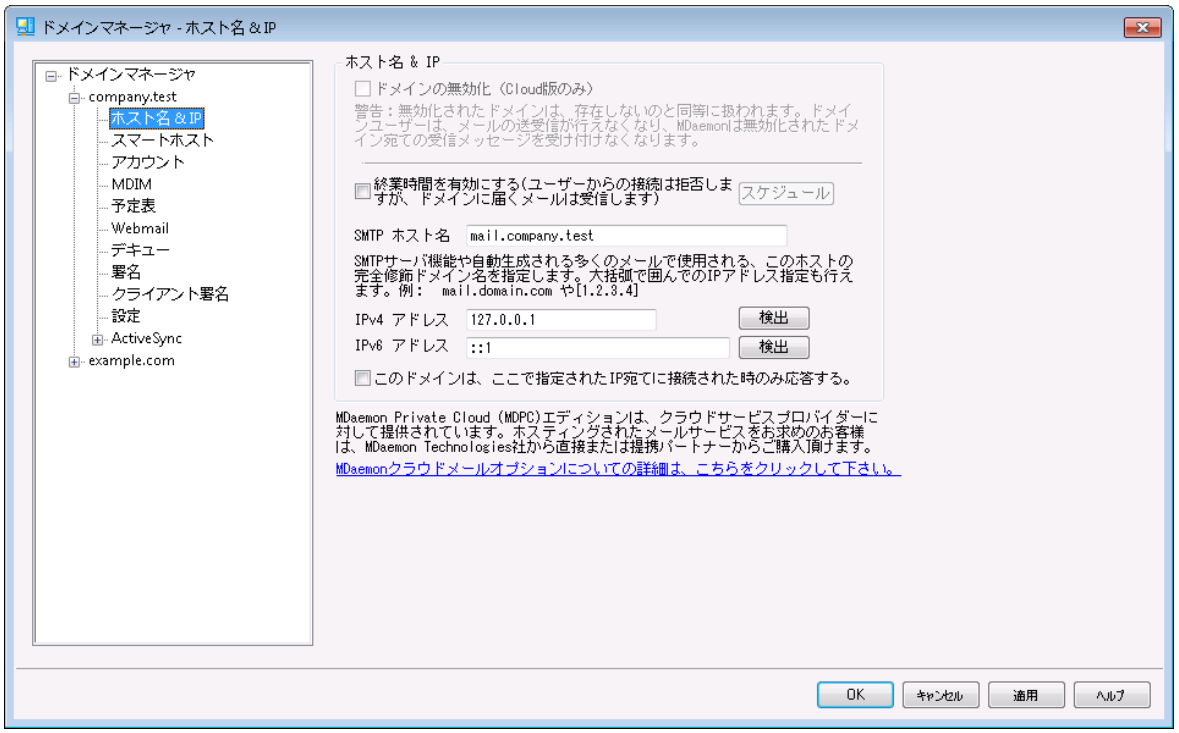
ドメインのコピー
新しいドメインを別のドメインと同じ設定で作成するには、対象ドメインを一覧から選択し、このボタンをクリックした後、新しいドメイン名を指定します。アカウント、メーリングリストなどは新しいドメインへコピーされません。

選択したドメインを新しいデフォルトドメインにする
MDaemonのデフォルトドメインを変更するには、対象ドメインを一覧から選択し、このボタンを押します。

参照:

初期設定 ≫ システム 450

3.2.1 ホスト名 & IP



ホスト名 & IP

ドメインを無効にする (クラウドのみ)
ドメインを無効にするにはこのチェックボックスを使用して下さい。無効化されたドメインはMDaemonに存在しないものとして処理されます。ドメインユーザーはメールの送受信が行えず、MDaemonは

対象ドメイン宛のメールを受け付けません。このオプションはMDaemon Private Cloudでのみ利用できます。

終業時間を有効にする
ドメインの終業時間設定を有効にするにはこのオプションを使用します。有効化されていると、対象時間、ドメインはユーザーやサービスからの接続を拒否しますが、外部からのメールは受け付けます。

スケジュール
終業時間の開始と終了をスケジュールするにはこのボタンをクリックします。例えば、2020年5月1日から6月30日の5:00pmから7:00am、月曜から金曜、と設定した場合、対象期間の間、5:00pmからメールサービスは利用できず、7:01amから再度利用できるようになります。スケジュールを削除するとスケジュールが無効化され、ドメインが永久に終業時間という設定になってしまいます。

SMTP ホスト名
ここには、完全修飾ドメイン名（FQDN）を指定します。この値は、メール受信時のSMTP HELO/EHLOコマンドへの応答に使用されます。受信用の接続において、「このドメインは上記のホストIPアドレスへの接続にだけ応答する」オプションが使用されていると、正しくIPアドレスと関連付けされたドメインと正しいFQDNが、対象ドメイン用の接続に使用されます。ただ、このオプションは厳密に動作する必要がありません。2つ又はそれ以上のドメインを同じIPアドレスで使用している場合はFQDNとアルファベット順で先頭のドメインから順番に関連付けられます。

ほとんどの場合、FQDNはドメイン名又は（例えば、“mail.example.com”のような）サブドメインですが、“[192.0.2.0]”のようなIPアドレスが使われる場合もあります。FQDNが指定されていない場合は、MDaemonはデフォルトドメインのFQDNを使用します。

IPv4/IPv6アドレス
このドメイン用のIPv4とIPv6 アドレスを入力します。IPアドレスが入力されていない場合、MDaemonが自動で利用可能なアドレス検出を実行します。

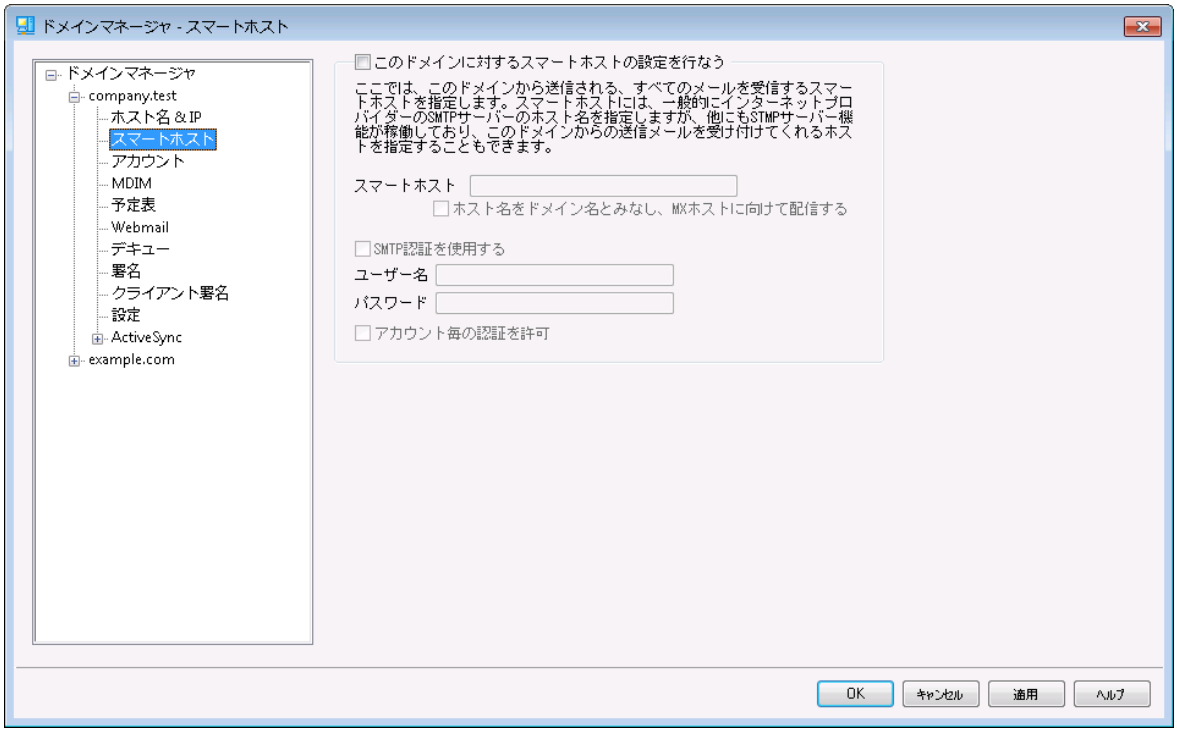
検出
このボタンで利用可能なIPアドレスを検出します。一覧から使用するIPアドレスを選択して下さい。

このドメインは、ここで指定されたIP宛に接続された場合のみ応答する
このドメインをホストIPアドレスに対する接続のみに限定する場合は、このオプションをクリックします。デフォルトで、この設定はInbound接続にのみ適用されます。アウトバウンドソケットの割り当てはサーバ設定 ≫ アドレスの割り当て100にあるオプションで設定して下さい。

参照:

ドメインマネージャ 165
初期設定 ≫ システム 450
アドレスの割り当て 100
IPv6 98

3.2.2 スマートホスト



このドメインに対するスマートホストの設定を行う

対象ドメインのメール配信に、デフォルトの 配信 85 オプションではなく、スマートホストを使用するにはこのチェックボックスを有効にし、スマートホストを指定します。対象ドメインの送信メールは、全てこのホストへ配信されます。

スマートホスト
ISPやメールホスト名、IPアドレスを指定します。一般的にはISPのSMTPサーバーを入力します。

ここへはMDaemonのデフォルトドメインやIPアドレスは入力しないで下さい。ここではメール転送を行うISPや外部のメールサーバーを指定します。

ホストをドメイン名としMXホストへ配送を行う
ホストを特定のサーバー名ではなくドメイン名として扱い、ドメインに対応したMXホストを転送先とする場合はこの設定を有効にします。

SMTP認証を使用する

スマートホスト で認証が必要な場合はこれを有効にし、認証情報を入力します。認証情報はスマートホスト宛ての送信SMTPメッセージ全てで使用されます。ただし、下部にある[**アカウントごとの認証を許可**]オプションを選択した場合、アカウントエディタのメールサービス654画面で指定するアカウントのスマートホスト ユーザ/パスワードを使用してSMTP認証を行います。

ユーザ名
ユーザ名またはログイン名を指定します。

パスワード
スマートホストのログインパスワードを指定します

アカウントごとの認証を許可
指定した*スマートホスト*へのSMTPメールに対しユーザー毎の認証情報を使用する場合は、この設定を有効にしてください。スマートホストで指定したユーザ名およびパスワードを使用する代わりに、メールサービス654画面で設定する、スマートホストユーザ/パスワードで設定したログイン情報が使用されます。スマートホストユーザ/パスワード設定が行われていないアカウントについては、上記の認証情報が使用されます。

アカウントごとの認証に、*スマートホスト*用ではなく、通常のメールパスワードを使わせたい場合は、MDaemon.ini の以下の行を変更してください。

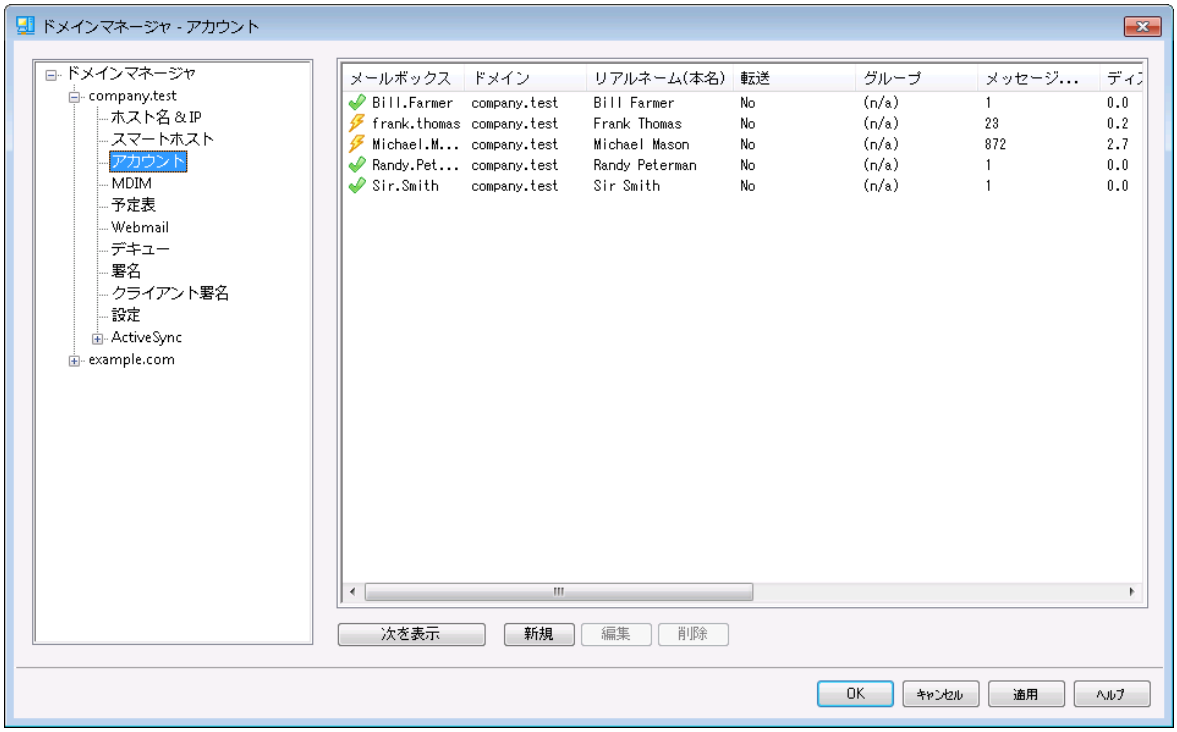
[AUTH]
ISPAUTHUsePasswords=Yes (デフォルトはNo)

ISPAUTHUsePasswords=Yesオプションを有効にすると、全アカウントがローカルのメールパスワードを使ってスマートホストとの通信を行うようになります。これは、機密情報を別のサーバに送っている点で、メールセキュリティにおけるリスクとなる可能性があります。この機能が必要で、且つ、スマートホストが信頼できるホストである場合である場合のみ、このオプションを使用して下さい。さらに、このオプションを有効にしており、且つ、Webmailまたは他の手段で、各ユーザーにメールパスワードを変更する許可を与えている場合、メールパスワードの変更が、スマートホストパスワードも事実上変更することに注意してください。これは、メールパスワードがローカルで変更され、対応するスマートホストパスワードがスマートホスト上で変更されていない場合、アカウントのスマートホスト認証で失敗する可能性があるためです。

参照:

ドメインマネージャ165
サーバ設定 ≫ 配信85
アカウントエディタ ≫ メールサービス654

3.2.3 アカウント



アカウント ページでは、管 理しているMDaemonアカウント が一 覧 表 示されます。 リスト の各 エントリは、アカウント のステータスアイコン（後 述 を参 照 ）、メールボックス、それぞれが属 するドメイン、アカウント 保 有 者 の[リアルネーム]、所 属 するグループ、メッセージ数 、使 用しているディスク容 量（MB）、最 後 のアクセス時 間 、メールの保 存 先 フォルダです。このリスト は、カラムを選 択 する事 で、昇 順 または降 順 でソートすることができます。いずれかのカラムの見 出しをクリックすると、リスト は昇 順 でソート されます。同じカラムの見 出しを再 度 クリックすると、次 にリスト は降 順 でソート されます。

アカウント ステータスアイコン

アカウント はグローバルまたはドメイン管 理 者

フルアクセスアカウント 。POPおよびIMAPアクセスが可 能 。

制 限 アカウント 。POPやIMAP、又 はその両 方 が無 効 。

凍 結 アカウント 。MDaemonは対 象 アカウント 宛 のメールを受 け付 けるが、ユーザーによるメール確 認 やメール送 信 不 可 。

無効なアカウント。このアカウントへのすべてのアクセスが無効。

新規
このボタンをクリックすると、新しいアカウントを作成するための[アカウントエディタ](#)650を開きます。

編集
リストからアカウントを選択し、このボタンをクリックして[アカウントエディタ](#)650を開きます。

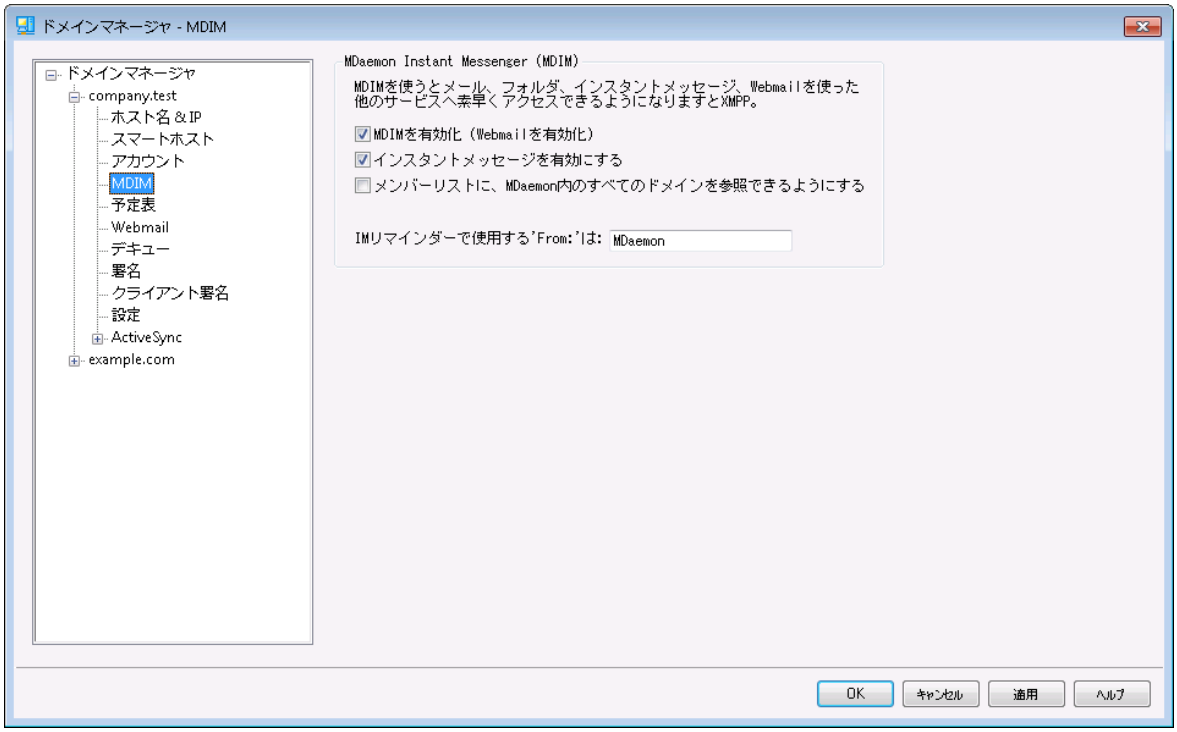
削除
アカウントを削除するには、リストからアカウントを選択してこのボタンをクリックしてください。削除処理を進める前に、本当に削除するかどうかの確認メッセージが表示されます。

次を表示
リストには一度に500アカウントしか表示されません。500以上のアカウントが存在する環境でこのボタンを押すと、次の500アカウントが表示されます。一度に500以上のアカウントを表示させたい場合は、上記の注意事項の内容をご確認の上、表示する最大アカウント数の設定を変更して下さい。

参照:

[アカウントマネージャ](#)648
[アカウントエディタ](#)650
[アカウントの作成テンプレート](#)722

3.2.4 MDIM



この画面ではドメイン向けの MDaemon Instant Messenger (MDIM)292 に関する各種設定が行えます。この画面の初期設定はWeb & IMサービスダイアログにあるデフォルトのMDaemon Instant Messenger304 設定を元にしています。MCIMサービスは ウェブサービス656 や グループプロパティ714 画面から、特定のアカウントやグループ毎に有効化・無効化が行えます。

MDaemon Instant Messenger (MDIM)

MDIMを有効化（Webmailを有効化）
ドメインユーザーがデフォルトでWebmailから MDaemon Instant Messengerをダウンロードし、利用できるようにする場合はこのオプションを有効化して下さい。ダウンロードは *オプション ≫ MDaemon Instant Messenger* ページから行えます。ダウンロードされたインストール用ファイルは自動でユーザーアカウント毎に、インストールと設定が簡単に行えるよう設定されています。このオプションではMDIMを私のメールフォルダ機能用に使用する事もでき、ユーザーは新着メールをMDIMのショートカットメニューをクリックし、Webmailを起動する事で簡単に行えるようになります。MDIMはデフォルトで有効です。

インスタントメッセージを有効化
デフォルトで、ユーザーはドメイン内の他のユーザーとの間でMDIMやサードパーティーのXMPP340 クライアントを使ったインスタントメッセージが行えます。ドメインユーザーのインスタントメッセージを許可しない場合はこのチェックボックスを無効化して下さい。

IMユーザーが、MDaemonの全 ユーザーを参 照 できるようにする

ドメインに関 係なくMDaemonユーザの全 てを、連 絡 先 に追 加 するにはこのオプションを選 択します。このオプションを無 効 化 すると、連 絡 先 に追 加 されるのは同じドメインのユーザだけになります。例 えばMDaemonがexample.comとexample.orgのドメインを使 用していた場 合 、このオプションが有 効であれば、example.comユーザーは両 方 のドメインのユーザーをメンバーへ追 加 できます。これを無 効 にすると、example.comドメインのユーザーのみを追 加 できます。このオプションはデフォルト で無 効になっています。

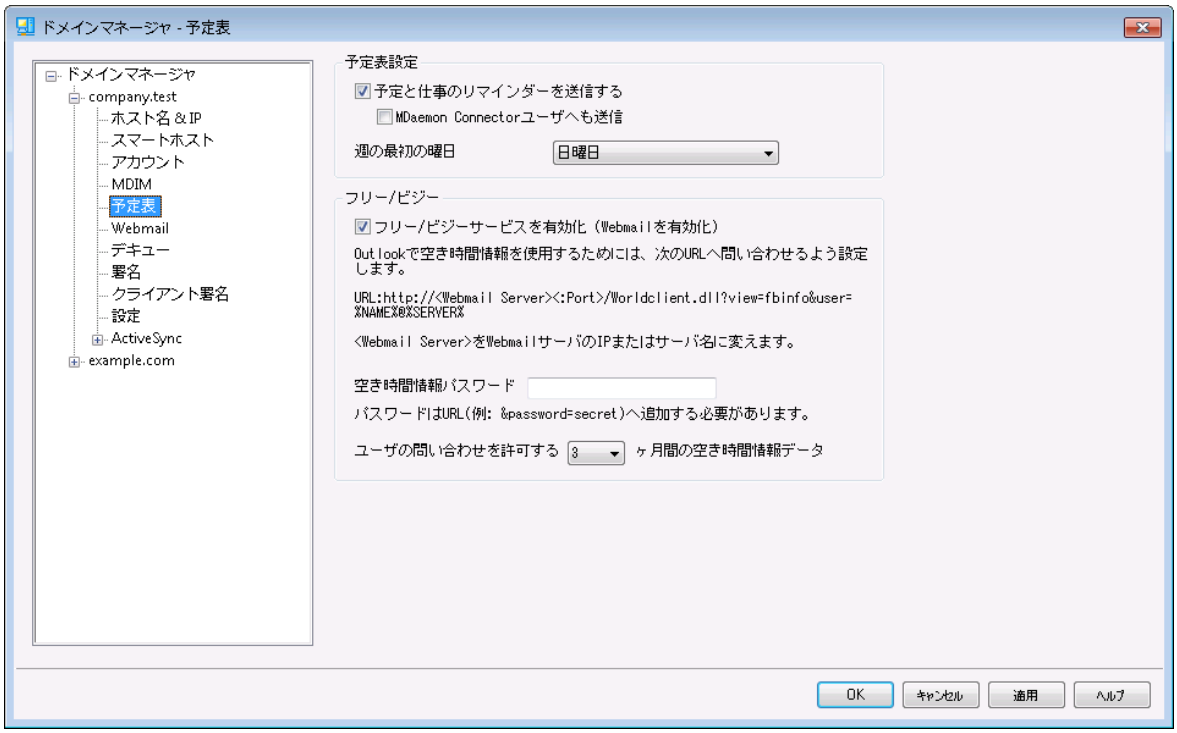
IMリマインダーで使 用 するFrom は: [*text*]

Webmail予 定 表 へ予 定 が追 加 されると、イベント のリマインダーが指 定した時 間 にユーザーへ送 信 されます。所 属ドメインのIMシステムが有 効 の場 合 、リマインダーがインスタント メッセージで対 象 ユーザーへ送 信 されます。このテキスト ボックスで、メッセージのFrom: として表 示 させたい名 前 を指 定します。

参照:

ドメインマネージャ 165
Webmail » MDIM 304
アカウント エディタ » ウェブサービス 656
グループプロパティ 714

3.2.5 予定表



ここではドメイン用のMDaemon予定表設定が行えます。ここでの初期設定は、WebとIMサービスの中の、予定表[306]を元にしています。

予定表設定

予定と仕事のリマインダーを送信する
このチェックボックスをクリックするとWebmailへ登録された予定と仕事のリマインダーがメールやMDaemon Instant Messengerで送信されます。

MDaemon Connectorユーザーへも送信
上記の"予定と仕事のリマインダーを送信する"オプションを有効にしている場合、このオプションをクリックするとMDaemon Connector[353]ユーザへもリマインダーが送信されます。

週の最初の曜日
ドロップダウンリストから曜日を選択してください。選択された曜日は、週の最初の曜日として予定表に表示されます。

Free/Busy

フリー/ビジー

MDaemonにはFree/Busyサーバ機能が含まれています。これにより会議を計画している人が、出席可能なメンバーを事前に確認することができます。
この機能にアクセスするためには、Webmailで新しいアポイントメントを作成する際に[予定表]をクリックしてください。するとスケジューリング ウィンドウが開き、参加者のリストや色分けされたカレンダーが表示されます。それぞれの参加者の行は色分けされており、彼らが会議に参加可能な時間が表示されます。色の区分には[取り込み中][離席中][外出中][情報なし]があります。また[次の回を自動的に選ぶ]ボタンがあり、すべての参加者が次に同時に参加可能になる時間を、サーバに問い合わせることができます。アポイントメントの作成が完了すると、すべての参加予定者に招待状が送られ、参加予定者は参加/不参加の返事をします。

WebmailのFree/Busyサーバ機能は、Microsoft Outlookとの互換性があります。これを使用するには、OutlookにFree/Busyサーバのデータを問合せできるよう設定を行ってください。例えば、Outlook 2002のFree/Busyオプションは、"ツール ≫ オプション ≫ 予定表オプション... ≫ 空き時間情報オプション..."にあります。

Outlookで使用するFree/BusyオプションのURLは以下のとおりです。

```
http://<Webmail><:Port>/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

上記のURLの<Webmail>は、使用しているWebmailサーバのIPアドレスまたはドメインに置き換えてください。また、デフォルトのポートを使用していない場合は、<:Port>をポート番号に置き換えてください。例えば、以下のようなURLとなります。

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

WebmailのFree/Busy機能で予定を登録する方法に関する詳細は、Webmail内のオンラインヘルプをご覧ください。

Free/Busyサービスの有効化（Webmailを有効）
ユーザーがFree/Busyサーバー機能へアクセスできるようにするにはこのオプションを有効化します。

Free/Busyパスワード
ドメインユーザがOutlook経由で空き時間情報サーバにアクセスする際に、パスワードの入力を求める場合は、ここにそのパスワードを入力してください。このパスワードは、ユーザがOutlookでの空き時間情報機能のURL設定をする際に、そのURLに("&password=FBServerPass"の部分で)含まれていなければなりません。例えば以下のようなURLとなります。

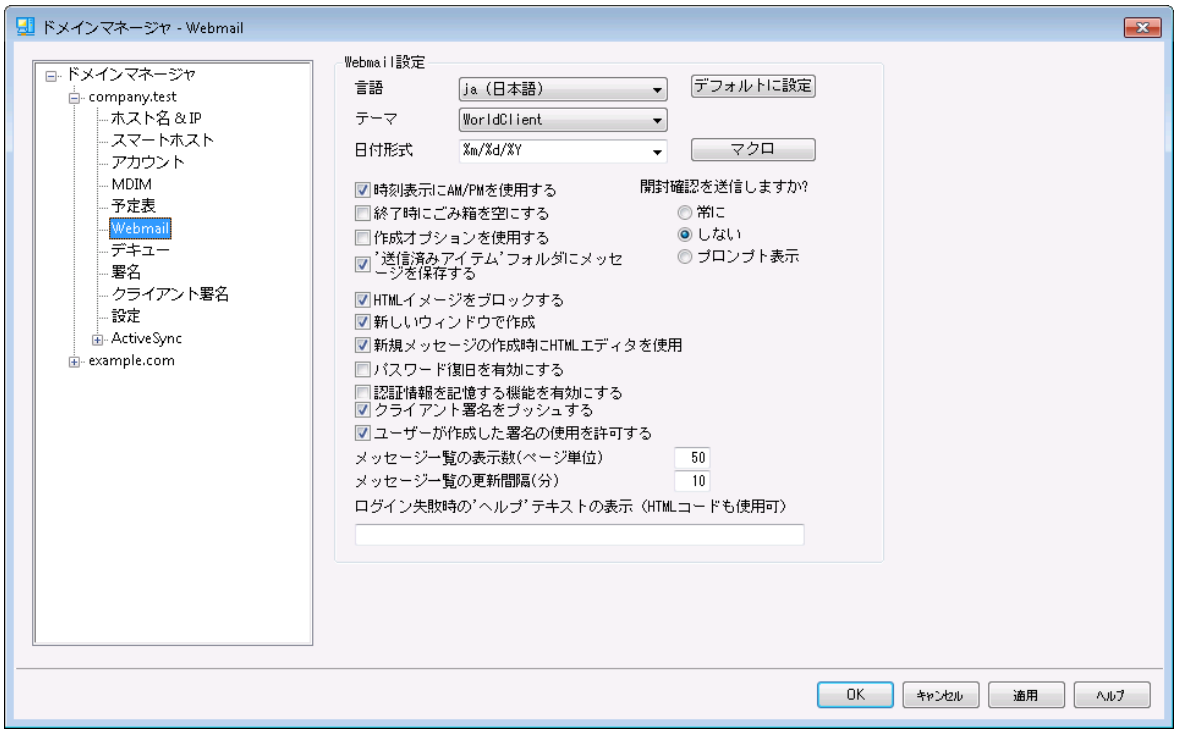
```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%SERVER%
&password=MyFBServerPassword
```

ユーザの問合わせを許可するXヶ月間の空き時間情報データ
ユーザが問合せを行える空き時間情報の保有月数を指定します。

参照:

Webmail ≫ 予定表 306

3.2.6 Webmail



この画面では、ドメイン毎に、様々なクライアントレベルのWebmail設定が行えます。Webmailへサインインすると、ここで設定したオプションが機能します。この設定は、Webmailのオプションページでユーザー毎にカスタマイズできます。ここでのデフォルト値はWeb & IMサービスのWebmail ≫ 設定 316を元に設定されています。

Webmail設定

デフォルトに設定
このボタンでドメイン設定をデフォルトのWebmail設定 316で初期化します。

言語
ユーザが最初にログオンする時に、Webmailの画面表示に使用するデフォルト言語を、ドロップダウンから選択します。ユーザはWebmailのオプション ≫ 初期設定やWebmailのサインインページから、使用する言語を変更することができます。

テーマ
ユーザが最初にログオンする時に、画面表示に使用するWebmailのデフォルトテーマを、ドロップダウンから選択します。ユーザはWebmailのオプション ≫ 初期設定から、使用するテーマを変更することができます。

日付形式
このテキストボックスを使用して、デフォルトの日付形式を設定してください。[マクロ]ボタンをクリックすると、このテキストボックスで使用することができるマクロコードのリストが表示されます。ここでは、以下のマクロを使用することができます。

%A - 曜日

%B - 月

%d - 日("01-31")

%m - 月("01-12")

%y - 年2桁

%Y - 年4桁

例えば、"%m/%d/%Y"の場合、Webmailでは"12/25/2011"と表示されます。

マクロ
このボタンをクリックすると、日付形式として使用することができるマクロコードのリストが表示されます。

開封確認を送信しますか?
このオプションは、開封確認要求が受信メッセージに含まれていた場合の応答方法を指定します。

常に
このオプションが選択される場合、MDaemonはメッセージが読まれたことを送信者に通知を送信します。メッセージを受信したWebmailユーザは、開封確認がリクエストまたは応答された表示をしません。

しない
Webmailで開封確認リクエストを無視する場合、このオプションを選択します。

プロンプトを表示
Webmailユーザに、開封確認の送信の有無を確認するには、このオプションを選択します。

時刻表示にAM/PMを使用する
Webmailの時刻表示に、AM/PMを付けた12時間表示を使用する場合は、このオプションを有効にしてください。24時間表示の場合は、チェックボックスを解除してください。各ユーザは、Webmailのオプション ≫ 予定表にある、「時刻表示にAM/PMを使用する」オプションを使って、設定を変更することができます。

終了時にゴミ箱を空にする
このオプションは、ユーザがWebmailからログオフする時に、そのユーザのごみ箱を空にします。各ユーザは、Webmailの オプション ≫ 初期設定で、この設定を変更することができます。

高度な設定を使用する
このオプションをクリックすると、ユーザのデフォルト画面として、通常の構成画面ではなく、詳細な構成画面が開かれます。各ユーザは、Webmailの オプション ≫ 作成で、この設定を変更することができます。

'Sent'フォルダにメッセージを保存する
メールボックスの送信済みフォルダに送信済みメッセージのコピーを保存する場合は、このオプションを選択してください。各ユーザは、Webmailの オプション ≫ 作成で、この設定を変更することができます。

HTMLイメージをブロックする
WebmailでHTMLメールメッセージを表示する場合、自動的にリモートイメージ表示を禁止する場合、このチェックのボックスを選択します。イメージを表示するには、ユーザはブラウザウィンドウでメッセージ上部に現れるバーをクリックする必要があります。多くのスパムメールには画像を表示したユーザーのメールアドレスを抜き出す特別なURL付きの画像が含まれており、こうした画像を表示すると、現在利用していて有効なメールアドレスを、スパムメールの送信元へ通知する事になります。これは、そういった脅威を防ぐための機能で、デフォルトで有効です。

新しいウィンドウで編集
メッセージの作成時にメインウィンドウとメッセージの構成画面を切り換えるのではなく、別々のブラウザウィンドウを開いて作業する場合は、このオプションを選択してください。別々のウィンドウを開きたくない場合は、チェックボックスをクリアしてください。 個々のユーザは、Webmailの オプション ≫ 作成で、この設定を変更することができます。

新規メッセージの作成時HTMLエディタを使用
ユーザがHTML形式でメッセージを編集できるようにする場合は、このチェックボックスを選択してください。ユーザはWebmailのオプション ≫ 作成で、この設定を変更することができます。

パスワードリカバリを有効にする
自分のパスワード編集 656 という権限を持っているユーザーが、Webmailで代理アドレスを入力し、パスワードの紛失時にパスワードを初期化するためのリンクを送る事ができるようになります。この機能を設定する際、ユーザーはオプション >> セキュリティページで、パスワードリカバリー用のメールアドレスと現在使用しているパスワードの両方を入力する必要があります。設定後、ユーザーが間違ったパスワードでログインしようとすると、「パスワードをお忘れですか？」というリンクが表示されます。このリンクをクリックすると、パスワードリカバリー用の代理メールアドレスを確認するためのページへ移動します。正しいアドレスを入力すると、パスワード変更用ページのURLが対象メールアドレスに送信されます。この機能はデフォルトで無効に設定されています。

このオプションはWebmailユーザー用の`user.ini`(例: `\Users\example.com\frank\WC\user.ini`)で以下を変更する事で、ユーザー毎に有効化・無効化できます。

```
[User]
EnablePasswordRecovery=Yes （=Noで無効化します）
```

2段階認証情報の記憶を許可（Remote Adminへも適用）
WebmailやRemoteAdminへサインインする際、2段階認証（2FA）を使用していた場合、2段階認証ページへも認証情報を記憶するオプションを表示し、指定日数の間は2段階認証を要求しないようにするにはこのオプションを使用します。2段階認証を記憶するオプションを表示しない場合はこのオプションを無効にしてください。無効にした場合、2FAを有効にしているユーザーは毎回サインインする毎に2FAコードの入力を求められます。注意点： このオプションは MDaemon Remote Administration (MDRA) 321ウェブインターフェイスでのみ有効です。

認証情報を記憶

https 300 ポートを使ってMDaemon Webmailのログオンページへアクセスすると、認証情報を記憶、のオプションをクリックする事で認証情報を記憶できます。ユーザーはログオンページの「認証情報を記憶」オプションをチェックする事で、認証情報は対象デバイスへ記録されます。その後、対象デバイスからWebmailへアクセスすると、手動でサインアウトした時か認証情報の記憶用トークンが期限切れとなるまで、サインインは自動的に行われます。

デフォルトで、認証情報は再ログインが必要になるまで最大30日間記憶されます。認証を記憶する期間を増やすには、 MDaemon Remote Administration (MDRA) 321 ウェブインターフェイスの、この日数を越えた認証情報は期限切れとしますの値を増やしてください。また、同様の設定が、\MDaemon\WorldClient\ フォルダの中の、Domains.iniにある、RememberUserExpiration=30の値を編集する事でも行えます。ここで指定できる最大値は365日です。注意点： 2段階認証 656（2FA）では、\MDaemon\WorldClient\ フォルダの中の、Domains.iniにある、[Default: Settings]にて、独自の有効期限(TwoFactorAuthRememberUserExpiration=30)が設定されています。そのため、2FAの有効期限が切れると、通常の有効期限内であった場合でも、再度認証を求められる事になりますので、ご注意下さい。

認証情報を記憶するオプションはデフォルトで無効に設定されており、対象ドメインにのみ適用されます。全体設定はWebmailの設定 316画面にて行えます。

> 認証情報を記憶する事で、ユーザーは複数のデバイスから継続的にログインできるようになるため、パブリックネットワークでは使用しないようにしてください。また、アカウントにセキュリティの問題が疑われる場合は、MDRAの「認証情報をリセット」ボタンで認証情報の記憶用トークンをリセットできます。この場合は、全てのユーザーが再度認証を行う必要があります。

クライアント署名をプッシュ配信
クライアント署名 188 をこのドメインのWebmailユーザーへプッシュ配信するにはこのボックスを有効にします。Webmailでは、これによりオプション >> 作成内の署名オプション内の「システム」へ署名が生成されます。ユーザーはこの署名を選択し、メールの新規作成時に自動挿入できるようになります。このオプションが有効で、ドメインマネージャのクライアント署名画面で署名を作成していなかった場合、デフォルトクライアント署名 125オプションが代わりに使用されます。デフォルトクライアント署名も設定されていなかった場合、Webmailのシステム署名オプションは使用できません。

ユーザーの署名作成を許可する
ドメインのユーザーが自分自身の署名をWebmailで作成できるようにする場合はこのボックスを有効にします。これにより、ユーザーは自分で作成した署名を選択し、メールの新規作成時に自動挿入できるようになります。ユーザーの署名作成を許可しておらず、クライアント署名をプッシュ配信するオ

プションが有効だった場合、（例えばWebmailのシステム署名といった） クライアント署名 125 だけが自動挿入されます。Webmailでは署名オプションは **オプション ≫ 作成** からアクセスできます。

メッセージ一覧として1ページ毎に表示するメール数
この値は、各メールフォルダで表示するメッセージの一覧で、ページ毎に表示するメールの数です。フォルダがこの数以上のメッセージを含む場合、リストの上と下に、ページ移動のコントロールが現れます。個々のユーザは、Webmailのオプション ≫ 初期設定 で、この設定を変更することができます。

メッセージ一覧の更新間隔(分)
これはWebmailが、自動的にメッセージリストを更新する前に待つ時間(分)です。個々のユーザは、Webmailの オプション ≫ 初期設定で、この設定を変更することができます。

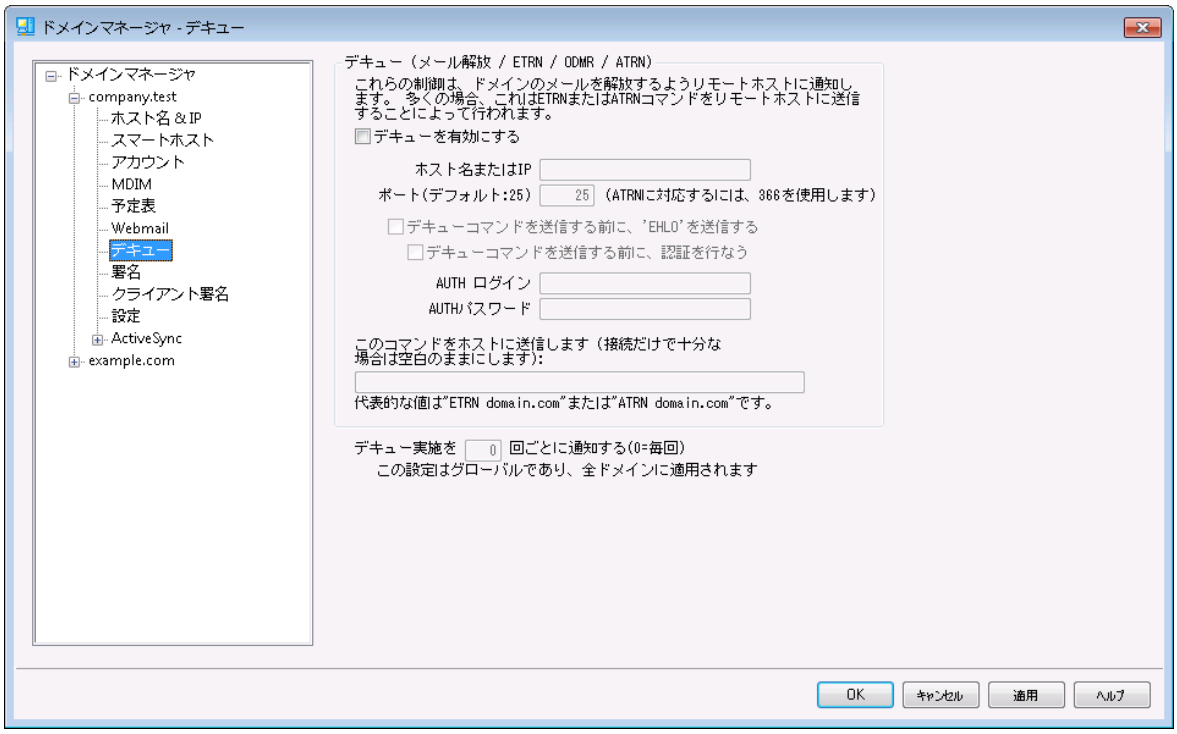
ログイン失敗時の'ヘルプ'テキストの表示（HTMLコード利用可）
ユーザがログオンでトラブルに遭遇した時、Webmailログオンページで表示する一文を、プレーンテキストかHTMLで指定できます。テキストは、次のデフォルトテキストが表示されます：″ログインが正しくありません。ヘルプが必要な場合は、メール管理者に問い合わせてください。このテキストは、Webmailのログオンに関する連絡先窓口の通知として使用する事ができます。

この機能を複数ドメインで正しく使用するためには、正しい SMTPホスト名 167 の設定がドメイン毎に必要です。正しい設定でない場合、デフォルトドメイン 165 用のテキストが使用されます。そのため、例えば複数ドメインが存在し、全てのWebmailユーザーがサインイン用に1つのホスト名を使用しているような場合、正しい、ドメイン専用のログイン失敗時の「ヘルプ」テキストは表示されない可能性があります。

参照:

Webmail ≫ 設定 316

3.2.7 デキュー



デキュー（メールリリース/ ETRN/ODMR/ATRN）

デキューを有効にする

MDaemonはリモートメールを処理する時に、任意のポートで任意のサーバに接続ができ、任意の文字列を送信することができます。この機能は、リモートサーバに例えば、ATRN、ETRN、QSNDなどの文字列を送ることによって、メールを開放するように指示する場合に役立ちます。また、この機能はオンラインであることをリモートホストまたはISPから確認するためのFINGERかTELNETセッションをリクエストされている場合にも使用できます。

ホスト名またはIP

メールを解放するためのシグナルを送信するホスト名とIPです。

ポート

接続するポートを登録します。デフォルトは25（SMTPポート）で、ETRNまたはQSNDの通信用に推奨されているポートです。366番ポートは通常ATRNで使用されており、79番はFINGERに使用されています。

文字列を送信する前に"EHLO"を送信

このチェックボックスを有効にした場合、メールの開放を通知するためにSMTPサーバに接続しなければなりません。このスイッチは指定されたホストとのSMTPセッションを開始した際、セッションがアンロックの文字列を送信する前に実行する、SMTPの[EHLO]処理を省略して手続きができるようになります。

文字列を送信する前に認証する(ATRNが必要です)

セキュリティ対策として、一部のホストまたはサーバは、メール開放の前に、クライアントによるESMTP AUTHでの認証を求める場合があります。ご利用のメールホストがこうした動作に一致する場合は、チェックボックスをクリックし必要な認証情報を入力して下さい。

ATRNコマンドを使ってメールを解放する際には、認証が必要です。

AUTHログオン
ホストから要求されるAUTHログオンパラメータをここへ入力します。

AUTHパスワード
AUTHパスワードをここへ入力します。

この文字列をホストへ送信する(接続に問題がない場合にはブランク)
このコントロールは、メールを解放するのにホストへ送信する文字列を定義するために使用します。例えば、ETRNメソッドは、キューに入れられているサイトのドメイン名が続くテキスト「ETRN」を必要とします。他の方法では異なったテキストを送信するように要求されます。メールキューを開放するために何を送信するかについてのさらに詳しい情報はISPへお問い合わせください。方法を選択できる場合は、可能な限り On-Demand Mail Relay (ODMR) 183 をお勧めします。ODMRにはATRNコマンドが必要です。

デキュー実施を[xx]回ごとに通知する(0=毎回)
デフォルトでは、リモートメールが処理されるたびにメール解放(デキュー)の信号が送信されます。ここで数字を入力する事により、デキュー信号が毎回送信される事がなくなります。信号はここで指定した時間毎に送信されるようになります。例えば、3をセットした場合には、リモートメールが3回処理される毎に一回信号が送信されます。

これは全体設定で全てのドメインへ適用されます。

On-Demand Mail Relay (ODMR)

ホスティングのキュー/デキューメソッドとメールの解放が必要な時に、使用可能な場合はいつでも、オンデマンドのメールリレー(ODMR)を使用することを勧めます。このメソッドは、ETRNおよび他のメソッドより優れていますがメールを開放する前に認証が必要です。さらに、ODMRは、静的なIPアドレスを持つことをクライアント(顧客)に要求しない、ATRNと呼ばれるESMTPコマンドを使用します。ATRNは、クライアントおよびサーバ)間のデータのフローを直ちに逆転し、(ETRNとは異なり)新しい接続を行う必要なしに、メッセージを解放します。

MDaemonは、クライアント側では、ATRNコマンドおよびメールの解放 180 の認証コントロールを使用して、またサーバ側では、ゲートウェイエディタのデキュー 240 でドメインゲートウェイ機能を使用することによって、全面的にODMRをサポートします。

一部のメールサーバはODMRをサポートしていないことがありますので、この機能を利用する前にご利用のプロバイダに確認してください。

参照:

メールの解放 180
ゲートウェイエディタ » デキュー 240

3.2.7.1 On-Demand Mail Relay (ODMR)

ホスティングのキュー/デキューメソッドとメールの解放が必要な時に、使用可能な場合はいつでも、オンデマンドのメールリレー(ODMR)を使用することを勧めます。このメソッドは、ETRNおよび他のメソッドより優れていますがメールを開放する前に認証が必要です。さらに、ODMRは、静的なIPアドレスを持つことをクライアント(顧客)に要求しない、ATRNと呼ばれるESMTPコマンドを使用します。ATRNは、クライアントおよびサーバ)間のデータのフローを直ちに逆転し、(ETRNとは異なり)新しい接続を行う必要なしに、メッセージを解放します。

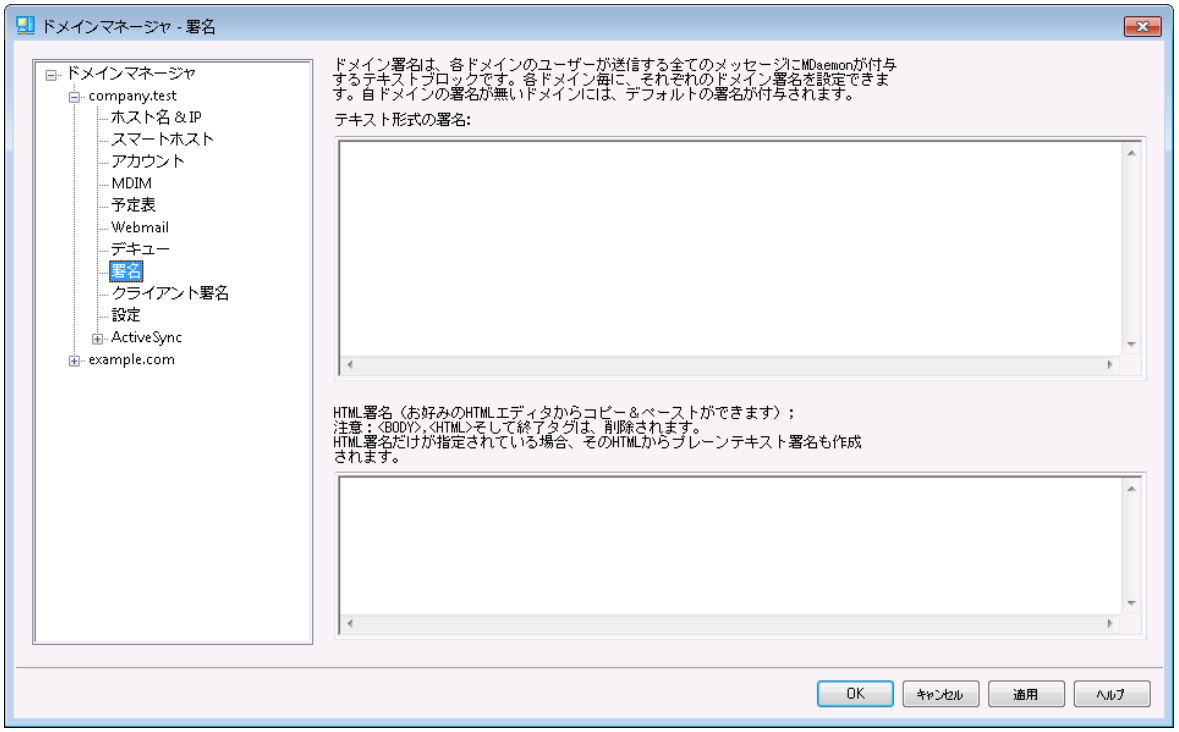
MDaemonは、クライアント側では、ATRNコマンドおよびメールの解放 180の認証コントロールを使用して、またサーバ側では、ゲートウェイエディタのデキュー 240でドメインゲートウェイ機能を使用することによって、全面的にODMRをサポートします。

一部のメールサーバはODMRをサポートしていないことがありますので、この機能を利用する前にご利用のプロバイダに確認してください。

参照:

メールの解放 180
ゲートウェイエディタ » デキュー 240

3.2.8 署名



この画面ではドメインのユーザーから送信される全てのメッセージへ追加される署名を設定します。署名が指定されていない場合は代わりにデフォルト署名[120]が追加されます。署名はフッタ[271]を使っているメーリングリスト以外のメッセージには一番下へ追加され、使っている場合にはフッタが署名の下に追加されます。また、各アカウントの署名についてはアカウントエディタの署名[686]から設定が行えます。アカウント署名はデフォルト署名やドメイン署名の直前に追加されます。

テキスト形式の署名

ここではテキスト形式の署名を指定します。もしもHTML形式の署名を使いたい場合は、次の*HTML形式の署名*を使って下さい。署名が両方に設定されていた場合、MDaemonはメッセージのフォーマットに応じて適した方の署名を使用します。html形式の署名が指定されていない場合は形式を問わずテキスト形式の署名が追加されます。

HTML形式の署名（ご使用のHTMLエディタからコピーして貼りつけて下さい）

ここではtext/html形式のメッセージで使うHTML署名を指定します。署名 がこことテキスト形式の署名の両方で設定されている場合は、MDaemonはメッセージのフォーマットに応じて適した方の署名を使用します。テキスト形式の署名が指定されていない場合はhtml形式の署名が追加されます。

html署名はhtmlコードを手動で入力するか、HTMLエディタからコピーしたものを貼り付けて下さい。HTML署名の中に画像ファイルを含む場合は、$ATTACH_INLINE:path_to_image_file$マクロを使用して下さい。

例:

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \images\mr_t_and_arnold.jpg$">
```

MDaemonのRemote Administration[321]でも、複数の方法で署名へ画像を追加できます。

- Remote Administrationの署名/フッタ画面で、HTMLエディタの「画像」ツールバーをクリックし、アップロードタブを選択します。
- Remote Administrationの署名/フッタ画面で、HTMLエディタのツールバーにある「画像の追加」ボタンをクリックします。
- Chrome, FireFox, Safari, MSIE 10+では、HTMLエディタの署名/フッタ画面へ画像をドラッグ&ドロップできます。
- Chrome, FireFox, MSIE 11+ではHTMLエディタの署名/フッタ画面へクリップボードの画像をコピーして貼り付けできます。

<body></body> と <html></html> タグは許可されておらず、使用した場合は削除されます。

署名マクロ

MDaemonの署名機能はマクロに対応しており、送信者の連絡先情報や、パブリック連絡先に登録してある送信者連絡先情報を、署名へ追加する事ができます。これにより、デフォルトやドメイン毎の署名も、送信者情報を個別に指定できるようになります。例えば、$CONTACTFULLNAME$ は送信者の氏名を挿入し、$CONTACTEMAI LADDRESS$ は送信者のメールアドレスを挿入します。パブリック連絡先は、Webmail, MDaemon Connector, ActiveSyncから編集できます。空の値は送信者の連絡先情報が存在しない場合に使用されます。利用できるマクロは次の通りです。

ユーザーはMDaemon署名を、$SYSTEMSIGNATURE$ マクロでデフォルト/ドメイン署名へ、$ACCOUNTSIGNATURE$ マクロでアカウント署名へ変換できます。

Signature Selector	
$SYSTEMSIGNATURE$	デフォルト署名 120またはドメイン署名をメッセージに配置する。両方が存在する場合は、ドメイン署名 184が使用される。
$CLIENTSIGNATURE$	メッセージにデフォルトクライアント署名 125またはドメインクライアント署名 188を入れる。両方が存在する場合は、ドメインクライアント署名を使用する。
$ACCOUNTSIGNATURE$	アカウント署名 686をメッセージに配置する。
名前とID	
Full name	**$CONTACTFULLNAME$**
First name	**$CONTACTFIRSTNAME$**
Middle name	**$CONTACTMIDDLENAME$,**
Last name	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**

Suffix	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Yomi First Name	**$CONTACTYOMIFIRSTNAME$**
Yomi Last Name	**$CONTACTYOMILASTNAME$**
Account name	**$CONTACTACCOUNTNAME$**
Customer ID	**$CONTACTCUSTOMERID$**
Government ID	**$CONTACTGOVERNMENTID$**
File as	**$CONTACTFILEAS$**
メールアドレス	
Email address	**$CONTACTEMAILADDRESS$**
Email address 2	**$CONTACTEMAILADDRESS2$**
Email address 3	**$CONTACTEMAILADDRESS3$**
電話とFAX番号	
Mobile phone	**$CONTACTHOMEMOBILE$**
Mobile phone 2	**$CONTACTMOBILE2$**
Car phone	**$CONTACTCARPHONENUMBER$**
Home phone	**$CONTACTHOMEPHONE$**
Home phone 2	**$CONTACTHOMEPHONE2$**
Home fax	**$CONTACTHOMEFAX$**
Other phone	**$CONTACTOTHERPHONE$**
インスタントメッセージとウェブ	
IM Address	**$CONTACTIMADDRESS$**
IM Address 2	**$CONTACTIMADDRESS2$**
IM Address 3	**$CONTACTIMADDRESS3$**
MMS Address	**$CONTACTMMSADDRESS$**
Home web address	**$CONTACTHOMEWEBADDRESS$**
住所	
Home address	**$CONTACTHOMEADDRESS$**
Home city	**$CONTACTHOMECITY$**
Home state	**$CONTACTHOMESTATE$**

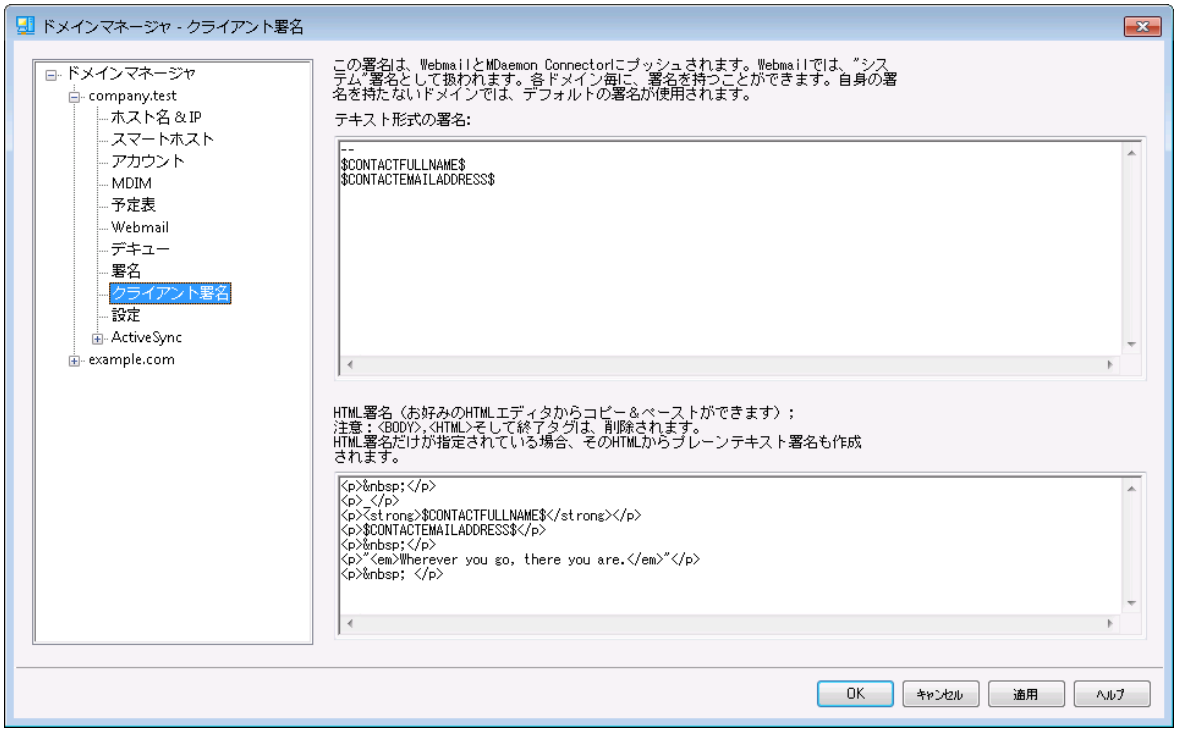
Home zip code	**$CONTACTHOMEZIPCODE$**
Home country	**$CONTACTHOMECOUNTRY$**
Other address	**$CONTACTOTHERADDRESS$**
Other city	**$CONTACTOTHERCITY$**
Other state	**$CONTACTOTHERSTATE$**
Other zip code	**$CONTACTOTHERZIPCODE$**
Other country	**$CONTACTOTHERCOUNTRY$**
仕事関連	
Business Name	**$CONTACTBUSINESSCOMPANY$**
Yomi Business Name	**$CONTACTYOMICOMPANYNAME$**
Business title	**$CONTACTBUSINESSTITLE$**
Business office	**$CONTACTBUSINESSOFFICE$**
Business department	**$CONTACTBUSINESSDEPARTMENT$**
Business manager	**$CONTACTBUSINESSMANAGER$**
Business assistant	**$CONTACTBUSINESSASSISTANT$**
Business assistant phone	**$CONTACTBUSINESSASSISTANTPHONE$**
Business main phone	**$CONTACTBUSINESSMAINPHONE$**
Business phone	**$CONTACTBUSINESSPHONE$**
Business phone 2	**$CONTACTBUSINESSPHONE2$**
Business IP phone	**$CONTACTBUSINESSIPPHONE$**
Business fax	**$CONTACTBUSINESSFAX$**
Business pager	**$CONTACTBUSINESSPAGER$**
Business radio	**$CONTACTBUSINESSRADIO$**
Business address	**$CONTACTBUSINESSADDRESS$**
Business city	**$CONTACTBUSINESSCITY$**
Business state	**$CONTACTBUSINESSSTATE$**
Business zip code	**$CONTACTBUSINESSZIPCODE$**
Business country	**$CONTACTBUSINESSCOUNTRY$**
Business web address	**$CONTACTBUSINESSWEBADDRESS$**
その他	

Spouse	**$CONTACTSPOUSE$**
Children	**$CONTACTCHILDREN$**
Categories	**$CONTACTCATEGORIES$**
Comment	**$CONTACTCOMMENT$**

参照:

デフォルト署名 120
アカウントエディタ ≫ 署名 686

3.2.9 クライアント署名



この画面ではメール作成時に自動挿入されるドメイン用のクライアント署名を作成でき、この署名は MDaemon Webmail 176 や MDaemon Connector 371 へプッシュ配信できます。下記のマクロは署名を個人用に設定するために使用でき、名前やメールアドレス、電話番号といった、ユーザー個々の情報へ書き換えられます。デフォルトクライアント署名 125 画面ではドメイン用ではないクライアント署名を作成する事ができます。ドメイン用の署名が作成されている場合は、ドメイン用の署名がデフォルトクライアント署名の代わりに使用されます。*クライアント署名のプッシュ配信* 176 オプションでクライアント署名をWebmailへプッシュ配信でき、 *Outlook用クライアント署名をプッシュ配信* 371 オプションでMDaemon Connectorへプッシュ配信が行えます。Webmailの作成オプションで、プッシュ配信されたクライアント署名は「システム」と呼ばれています。MDaemon Connector用にはOutlookで表示される名称を指定する事ができます。

テキスト形式の署名

ここではテキスト形式の署名を指定します。もしもHTML形式の署名を使いたい場合は、次の*HTML形式の署名*を使って下さい。署名が両方に設定されていた場合、MDaemonはメッセージのフォーマットに応じて適した方の署名を使用します。html形式の署名が指定されていない場合は形式を問わずテキスト形式の署名が追加されます。

HTML形式の署名（ご使用のHTMLエディタからコピーして貼りつけて下さい）

ここではtext/html形式のメッセージで使うHTML署名を指定します。署名 がこことテキスト形式の署名の両方で設定されている場合は、MDaemonはメッセージのフォーマットに応じて適した方の署名を使用します。テキスト形式の署名が指定されていない場合はhtml形式の署名が追加されます。

html署名はhtmlコードを手動で入力するか、HTMLエディタからコピーしたものを貼り付けて下さい。HTML署名の中に画像ファイルを含む場合は、$ATTACH_INLINE: path_to_image_file$マクロを使用して下さい。

例:

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \images\mr_t_and_arnold.jpg$">
```

MDaemonのRemote Administration 321でも、複数の方法で署名へ画像を追加できます。

- Remote Administrationの署名/フッタ画面で、HTMLエディタの「画像」ツールバーをクリックし、アップロードタブを選択します。
- Remote Administrationの署名/フッタ画面で、HTMLエディタのツールバーにある「画像の追加」ボタンをクリックします。
- Chrome, FireFox, Safari, MSIE 10+では、HTMLエディタの署名/フッタ画面へ画像をドラッグ＆ドロップできます。
- Chrome, FireFox, MSIE 11+ではHTMLエディタの署名/フッタ画面へクリップボードの画像をコピーして貼り付けできます。

<body></body> と <html></html> タグは許可されておらず、使用した場合は削除されます。

署名マクロ

MDaemonの署名機能はマクロに対応しており、送信者の連絡先情報や、パブリック連絡先に登録してある送信者連絡先情報を、署名へ追加する事ができます。これにより、デフォルトやドメイン毎の署名も、送信者情報を個別に指定できるようになります。 例えば、 $CONTACTFULLNAME$ は送信者の氏名を挿入し、$CONTACTEMAILADDRESS$ は送信者のメールアドレスを挿入します。パブリック連絡先は、Webmail, MDaemon Connector, ActiveSyncから編集できます。空の値は送信者の連絡先情報が存在しない場合に使用されます。利用できるマクロは次の通りです。

ユーザーはMDaemon署名を、 $SYSTEMSIGNATURE$ マクロでデフォルト/ドメイン署名へ、$ACCOUNTSIGNATURE$ マクロでアカウント署名へ変換できます。

Signature Selector	
$SYSTEMSIGNATURE$	デフォルト署名 120またはドメイン署名をメッセージに配置する。両方が存在する場合は、ドメイン署名 184が使用される。
$CLIENTSIGNATURE$	メッセージにデフォルトクライアント署名 125またはドメインクライアント署名 188を入れる。両方が存在する場合は、ドメインクライアント署名を使用する。
$ACCOUNTSIGNATURE$	アカウント署名 686をメッセージに配置する。
名前とID	
Full name	**$CONTACTFULLNAME$**
First name	**$CONTACTFIRSTNAME$**
Middle name	**$CONTACTMIDDLENAME$,**
Last name	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
Suffix	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Yomi First Name	**$CONTACTYOMIFIRSTNAME$**
Yomi Last Name	**$CONTACTYOMILASTNAME$**
Account name	**$CONTACTACCOUNTNAME$**
Customer ID	**$CONTACTCUSTOMERID$**
Government ID	**$CONTACTGOVERNMENTID$**
File as	**$CONTACTFILEAS$**
メールアドレス	
Email address	**$CONTACTEMAILADDRESS$**
Email address 2	**$CONTACTEMAILADDRESS2$**
Email address 3	**$CONTACTEMAILADDRESS3$**
電話とFAX番号	
Mobile phone	**$CONTACTHOMEMOBILE$**
Mobile phone 2	**$CONTACTMOBILE2$**
Car phone	**$CONTACTCARPHONENUMBER$**
Home phone	**$CONTACTHOMEPHONE$**
Home phone 2	**$CONTACTHOMEPHONE2$**

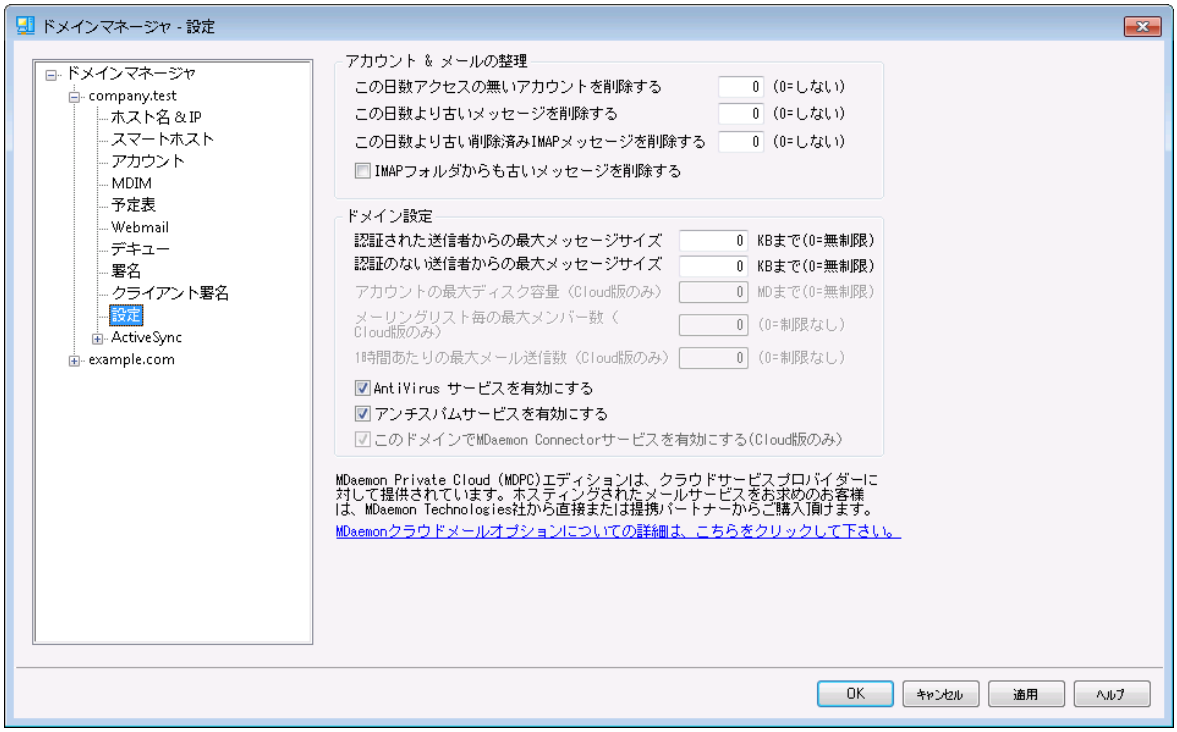
Home fax	**$CONTACTHOMEFAX$**
Other phone	**$CONTACTOTHERPHONE$**
インスタント メッセージとウェブ	
IM Address	**$CONTACTIMADDRESS$**
IM Address 2	**$CONTACTIMADDRESS2$**
IM Address 3	**$CONTACTIMADDRESS3$**
MMS Address	**$CONTACTMMSADDRESS$**
Home web address	**$CONTACTHOMEWEBADDRESS$**
住所	
Home address	**$CONTACTHOMEADDRESS$**
Home city	**$CONTACTHOMECITY$**
Home state	**$CONTACTHOMESTATE$**
Home zip code	**$CONTACTHOMEZIPCODE$**
Home country	**$CONTACTHOMECOUNTRY$**
Other address	**$CONTACTOTHERADDRESS$**
Other city	**$CONTACTOTHERCITY$**
Other state	**$CONTACTOTHERSTATE$**
Other zip code	**$CONTACTOTHERZIPCODE$**
Other country	**$CONTACTOTHERCOUNTRY$**
仕事関連	
Business Name	**$CONTACTBUSINESSCOMPANY$**
Yomi Business Name	**$CONTACTYOMICOMPANYNAME$**
Business title	**$CONTACTBUSINESSTITLE$**
Business office	**$CONTACTBUSINESSOFFICE$**
Business department	**$CONTACTBUSINESSDEPARTMENT$**
Business manager	**$CONTACTBUSINESSMANAGER$**
Business assistant	**$CONTACTBUSINESSASSISTANT$**
Business assistant phone	**$CONTACTBUSINESSASSISTANTPHONE$**
Business main phone	**$CONTACTBUSINESSMAINPHONE$**
Business phone	**$CONTACTBUSINESSPHONE$**

Business phone 2	**$CONTACTBUSINESSPHONE2$**
Business IP phone	**$CONTACTBUSINESSIPPHONE$**
Business fax	**$CONTACTBUSINESSFAX$**
Business pager	**$CONTACTBUSINESSPAGER$**
Business radio	**$CONTACTBUSINESSRADIO$**
Business address	**$CONTACTBUSINESSADDRESS$**
Business city	**$CONTACTBUSINESSCITY$**
Business state	**$CONTACTBUSINESSSTATE$**
Business zip code	**$CONTACTBUSINESSZIPCODE$**
Business country	**$CONTACTBUSINESSCOUNTRY$**
Business web address	**$CONTACTBUSINESSWEBADDRESS$**
その他	
Spouse	**$CONTACTSPOUSE$**
Children	**$CONTACTCHILDREN$**
Categories	**$CONTACTCATEGORIES$**
Comment	**$CONTACTCOMMENT$**

参照:

デフォルトクライアント署名 125
デフォルト署名 120
ドメインマネージャ » 署名 184
アカウントエディタ » 署名 686
ドメインマネージャ » Webmail設定 176
MCクライアント設定 » 署名 371

3.2.10 設定



アカウント & メールの整理

このダイアログでは、未使用のアカウントや古いメッセージを、いつ、MDaemonが削除するのかを設定します。MDaemonは毎晩深夜に、この設定で指定された期間を過ぎたすべてのメッセージとアカウントを削除します。アカウントエディタのクォータ666でも、これと似たオプションが設定でき、アカウント毎の設定は、ここでの設定を上書きします。

より詳しい情報とコマンドラインオプションに関しては、"…MDaemon¥App¥"フォルダにあるAccountPrune.txtを参照してください。

アカウントを自動削除(非アクティブな日数 XX 日)(0 = しない)

このドメインに属するアカウントが、ここで指定した日数の間未使用だった場合、これを削除します。0(ゼロ)の値を指定すると、アカウントが使用されていなくても、削除しません。

古いメッセージを削除(経過日数 XX 日)(0 = しない)

メールがMDaemonで自動削除するまでの日数を指定できます。0(ゼロ)の値を指定すると、メッセージの経過日数に関係なく、メッセージは削除されないことを意味します。**注意点:** このオプション設定は、後述の「古いメッセージをIMAPフォルダからも削除する」オプションを有効にしていなければ、IMAPフォルダのメールへは適用されません。

削除済みIMAPメッセージの削除(XX 日)(0 = しない)

ユーザのフォルダ内で削除フラグのあるIMAPメッセージを何日後にMDaemonが自動削除するのかをここで指定します。ここで指定された日数よりも長い期間フラグのあるメッセージは、メールボックスから削除されます。0(ゼロ)の値を指定すると、削除フラグのあるIMAPメッセージは古さに関係なく削除されないことを意味します。

古いメッセージをIMAPフォルダからも削除する

上記の[古いメッセージを削除]オプションを、IMAPフォルダ内のメッセージにも適用する場合は、このチェックボックスをクリックしてください。このコントロールが無効の場合は、IMAPフォルダ内のメッセージは、古さに関係なく削除されません。

ドメイン設定

認証済ユーザーからの最大メッセージサイズ [xx] KB (0=無制限)
認証済ユーザーからのドメイン宛のメールで許可する最大サイズを設定します。メッセージサイズを制限したくない場合は0を指定します。

その他ユーザーからの最大メッセージサイズ [xx] KB (0=無制限)
認証していないユーザーからのドメイン宛に届くメールの最大サイズを設定します。メッセージサイズを制限したくない場合は0を指定します。 認証済ユーザーからのメールサイズを制限する場合は、前述のオプションを使用します。

アカウントの最大ディスクサイズ [xx] MB (0=無制限)(クラウドのみ)
ドメインで使用できるディスク容量を制限するにはこのオプションを使用します。

メーリングリスト毎の最大メンバー数 [xx](0=無制限)(クラウドのみ)
このドメインで、メーリングリスト毎に登録できるメンバー数を制限するにはこのオプションを使用します。メーリングリストマネージャの設定[248]画面にもこれに似た全体オプションがあります。

一時間毎に送信できる最大メール数 [xx](0=無制限)(クラウドのみ)
ドメインが一時間毎に送信できる最大メール数を指定するにはこのオプションを使用します。指定した上限に到達すると、その後のメールはカウントが初期化されるまでキューへ残されます。メッセージカウントは一時間毎かサーバー再起動のタイミングで初期化されます。このオプションはMDaemon Private Cloudでのみ利用できます。

このドメインでAntiVirusサービスを有効にする
このオプションで、対象ドメインに対するAntiVirus[587]を有効化します。

このドメインでアンチスパムサービスを有効にする

MDaemonのスパムフィルタ設定をこのドメインにも適用する場合はこのチェックボックスをクリックします。

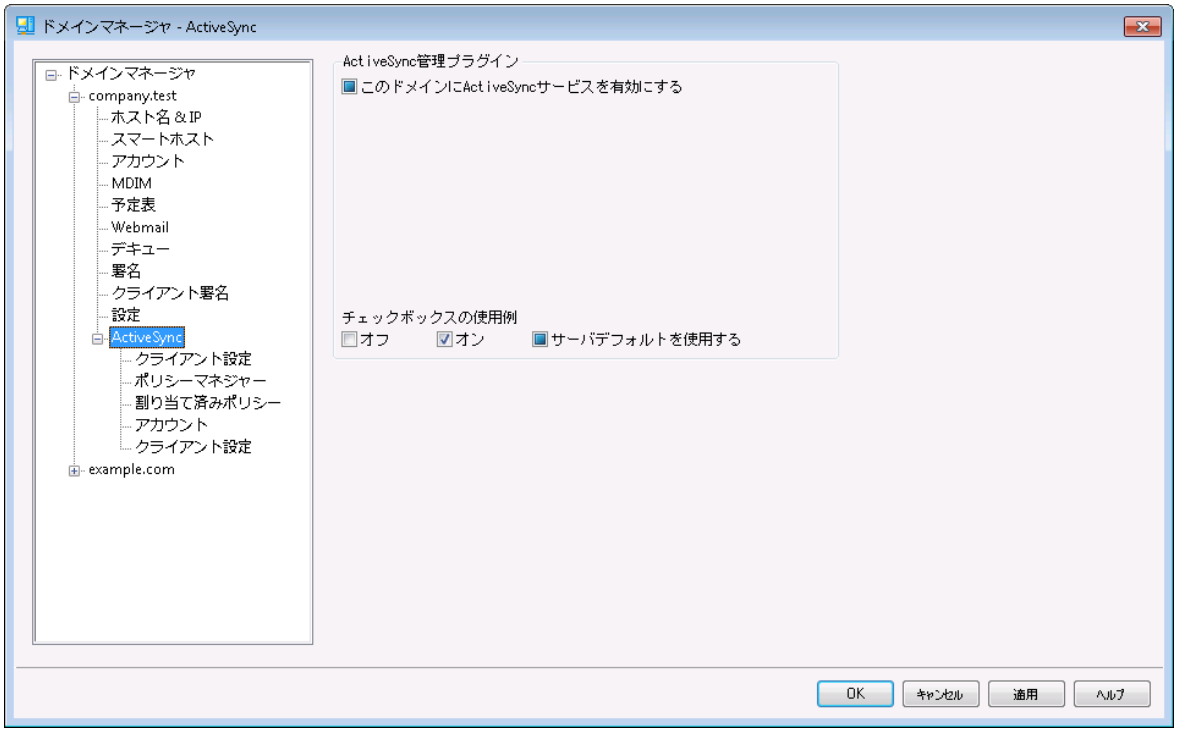
このドメインでMDaemon Connectorサービスを有効にする（クラウドのみ）

このドメインでMDaemon Connectorサービスを有効にする場合はこのオプションを有効化します。

参照:

アカウントエディタ ≫ クォータ 666

3.2.11 ActiveSync



ドメインマネージャのこの画面からは、ドメイン毎のActiveSync 379設定が行えます。ActiveSyncの設定やのデフォルト値の管理はActiveSyncマネージャの、ドメイン 397 から行えます。

ActiveSync for MDaemon管理プラグイン

このドメインでActiveSyncサービスを有効にする

このオプションでドメインのユーザーが、デフォルトで、ActiveSyncクライアントのメールとPIMデータへアクセスできるようにするかどうかを指定します。デフォルト値はデフォルトのActiveSync状態 397を引き継ぎますが、このチェックボックスの有効化・無効化で、デフォルト値を上書きできます。ここでの設定はアカウント 413 やクライアント 422 の設定によっても上書きされます。 **注意点：** このドメインでActiveSyncを無効化すると、ドメインユーザー全体のActiveSync接続を終了するかどうかの確認画面が表示されます。ドメインユーザーでActiveSyncを利用しているユーザーが継続して

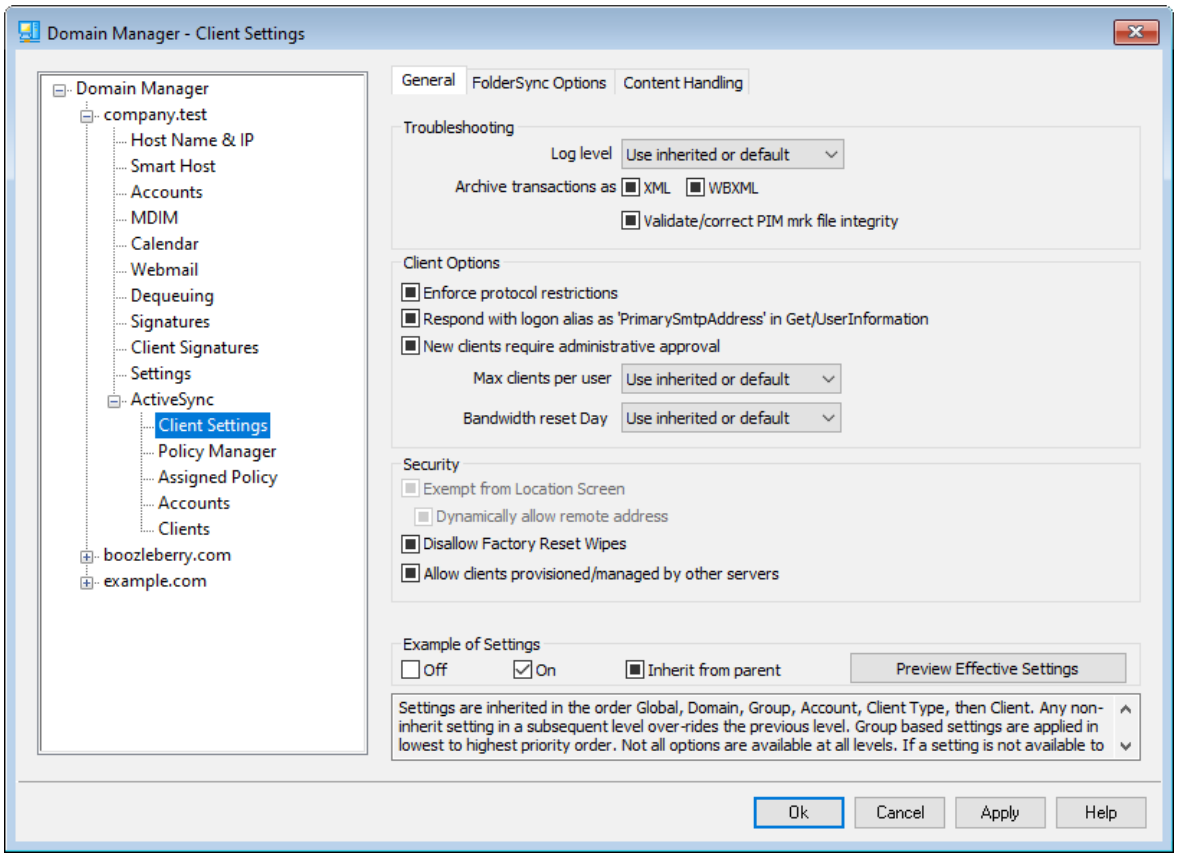
ActiveSyncを利用できるようにするには、いいえを選択してください。はいを選択すると、ドメインユーザー全体でActiveSyncが無効化されます。

この設定は、ActiveSyncが稼働しているとき、デフォルトでドメインユーザーがこの機能を利用できるようにするかどうかを決定するためだけのものです。ActiveSyncへ、許可されたドメインやユーザーが実際にアクセスできるようにするには、全体オプションの ActiveSyncプロトコルを有効にする 379 が有効になっている必要があります。

参照:

ActiveSync ≫ ドメイン 397
ActiveSync ≫ アカウント 413
ActiveSync ≫ クライアント 422

3.2.11.1 クライアント設定



この画面では、ドメインに対応したアカウントとクライアントのデフォルト設定を行う事ができます。

デフォルトで画面上の全てのオプションは、「継承またはデフォルト」という設定になっており、全体クライアント設定[384]を元に設定されています。同様に、ドメインのアカウント[171]は、上位の設定であるこの画面の設定値を引き継ぎます。この画面で行った変更は全てアカウント設定へも反映されます。更に、個々のクライアント[220]の設定画面では、その設定をアカウント設定から引き継ぎます。この画面で変更を行う事で、ドメインのアカウントやクライアント全てに対して設定変更が行えます。アカウントやクライアントの設定を行う事で、ここでの設定値を上書きする事もできます。

全般

トラブルシューティング

ログレベル

ActiveSync for MDaemonはログデータ量に応じた、6つのレベルのログに対応しています。

デバッグ 最も詳細なログで、記録できる全ての情報が含まれており、問題の診断にのみ使用されます。

情報 通常のログで、一般的な操作が詳細なしで記録されます。これはデフォルトのログレベルです。

警告 警告、エラー、クリティカルエラー、起動と終了がログに記録されます。

エラー エラー、クリティカルエラー、起動と終了がログに記録されます。

クリティカル クリティカルエラー、起動と終了がログに記録されます。

なし 起動と終了だけがログに記録されます。

継承 デフォルトで、ログレベルの設定はクライアント設定の階層から継承されます。そのため、クライアントは設定をクライアントタイプから引継ぎ、クライアントタイプはアカウントから引継ぎ、アカウントはグループから引継ぎます。全体のクライアント設定は診断[393]ダイアログのログレベル設定を元にしています。

トランスアクションを [XML | WBXML]としてアーカイブ

XMLやWBXMLデータをアーカイブするには、*XMLと WBXMLをアーカイブ...* のオプションを使用します。これはデバッグの際役立ちます。全体オプションはデフォルトで無効になっています。

PIM mrkファイルの整合性を確認する

クライアントのPIMデータの整合性テストを実施し、iCal UIDの重複や空の要求フィールドといった、同期を妨げているものがないかどうかを確認します。この全体設定はデフォルトで無効になっています。

クライアントオプション

プロトコル制限を強制する

クライアントで許可されているプロトコルバージョン以外のアクセスを拒否する場合はこのオプションを

有効にします。デフォルトでこのオプションは無効になっており、プロトコル制限は異なるプロトコルのクライアントを拒否していません。プロトコル制限は単純に、クライアントに対して使用するべきプロトコルを伝えるのみの機能を提供しています。クライアントがそれでも制限されているプロトコルを使った場合、MDaemonはその接続を受け入れます。詳細は次のページをご覧下さい: プロトコル制限 395

Get/UserInformationへの応答でログオンエイリアスを'PrimarySmtpAddress'として使用する
サービスがSettings/Get/UserInformationリクエストに対する応答としてエイリアスやセカンダリアドレスをプライマリアドレスとして利用できるようにします。これはiOS 9.xへアップデートした際エイリアスからメールを送信できなくなった事に対する対処です。このオプションによって使用に反した応答を受け取る場合があります。

新しいクライアントは管理者の承認が必要
新しいクライアントがアカウントとの同期を開始する前に、管理者による承認を必要とする場合はこのオプションを有効にします。 クライアント 422 一覧で認証待ちのクライアントが確認でき、管理者は同じ画面から承認が行えます。この設定はデフォルトで無効になっています。

ユーザー毎の最大クライアント
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域リセット日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

セキュリティ

ロケーションスクリーンから除外する
ActiveSyncクライアント設定で端末をロケーションスクリーニング 520 から除外する場合はこのオプションを有効化します。これにより認証済ユーザーは、例えば認証がブロックされている場所へ出張しているような場合であっても、ActiveSync経由でアカウントへアクセスする事ができるようになります。端末を除外するためには、チューニング画面にあるこの日数を超えて認証されなかった端末を自動削除 381 設定の時間内に、ActiveSyncを使った接続と認証を行っておく必要があります。

リモートアドレスを動的に除外
接続元のリモートIPアドレスをロケーションスクリーニングの除外リストへ追加する事ができます。このオプションは、同じIPアドレスを使って接続する他のクライアントがある場合に便利です。

ユーザー毎の最大クライアント数
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域の統計情報をリセットする日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。

リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

他のサーバーで管理されているクライアントへの接続を許可する
デフォルトで、ActiveSyncサーバーが特定のクライアントへデータやポリシーを送信する際、対象クライアントが他のActiveSyncサーバーからも管理されている事が分かった場合も、クライアントはMDaemonへアクセスする事ができます。しかし、このような環境の場合、適用するポリシーが他のActiveSyncサーバーと競合する可能性があります。一般的に、クライアントはポリシーが競合した場合、厳しい方へ合わせる傾向があります。こうしたクライアントからの接続を制限する場合は、このオプションを無効化して下さい。

工場出荷時への完全ワイプを無効化
オン/はい、を設定すると、ActiveSyncクライアントの完全ワイプが行えなくなります。クライアントでリモートからの完全ワイプを許可する場合、最初にこのオプションを無効化して下さい。このオプションはデフォルトで無効に設定されています。クライアントページの次の項目を参照して下さい:
ActiveSyncクライアントの完全ワイプ 422

フォルダ同期オプション

フォルダ同期オプション

除外

ユーザの [許可リスト/ブロックリスト] フォルダ
デフォルトでユーザーの許可リストとブロックリストの連絡先フォルダは端末と同期を行いません。これらはMDaemonがスパムからシステムを自動的に保護するのを支援する目的で使用されます。そのため、許可リストやブロックリストは端末上に連絡先として表示する必要性はありません。

デフォルト以外のメールフォルダ
デフォルトで、ユーザーが作成したメールフォルダとデフォルトメールフォルダは全て端末と同期します。同期するのを受信箱や送信箱、削除済アイテム、下書き、といった、デフォルトのメールフォルダのみにしたい場合はこのオプションを有効にして下さい。ユーザーが作成したフォルダは同期対象に含まれません。 このオプションはデフォルトで無効になっています。

デフォルト以外のPIMフォルダ
デフォルトで、（連絡先、予定表、仕事などの）PIMフォルダは全て端末と同期します。同期するのをデフォルトのPIMフォルダのみにしたい場合はこのオプションを有効にして下さい。このオプションが有効な場合で、ユーザーが複数の予定表を保有してる場合デフォルトの予定表のみが同期対象となります。 このオプションはデフォルトで無効になっています。

含む

パブリックフォルダの階層
ユーザーがアクセス権を持っている パブリックフォルダ 283 をユーザーのActiveSync用端末のフォルダー覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
パブリックフォルダ[283]をユーザーが検索できるようになります。これはデフォルトで許可されています。

パブリックフォルダの横断（フォルダ名の公開）
デフォルトで、クライアントがパブリックのサブフォルダへのアクセスや同期を行うには、サブフォルダと上位のパブリックフォルダ[283]全てに対してルックアップ権限[285]が必要です。上位のフォルダに対するアクセス権がない場合、その中のサブフォルダに対しては、例え設定上は許可されていても、アクセスする事はできません。クライアントからこうしたサブフォルダへアクセスできるようにする場合は、このオプションを有効にします。注意点：このオプションを有効化すると、上位のフォルダもクライアントへ許可する事となり、セキュリティのリスクを招く恐れがあります。このオプションはデフォルトで無効になっています。

許可するパブリックフォルダの最大数
端末で処理するパブリックフォルダ数を制限する場合はこのオプションを使用します。制限が設定されると、サーバーは最大数に到達するまでフォルダー覧を処理し、これを超えるとその後のデータを送りません。処理するフォルダの順番を決める事はできません。デフォルトで、全体での最大数は設定されていません。

共有フォルダも含める

ユーザーがアクセス権を持っている共有フォルダ[107]をユーザーのActiveSync用端末のフォルダー覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
共有フォルダ[676]をユーザーが検索できるようになります。これはデフォルトで許可されています。

コンテンツ処理

コンテンツ処理オプション

クライアントにフラグ付けされたメール用にタスク・リマインダーを作成
このオプションでMDaemonはフラグが付いたアイテムごとに仕事を作成し、リマインダーをユーザーへ送信できるようになります。この設定の全体値はデフォルトで有効です。

予定を編集した際、常にミーティングのアップデートを送信
クライアントの中には、ミーティングを編集した際、更新情報を適切に送信しないものもあります。このオプションを使うとActiveSyncサービスへ、ミーティングが開催者によって更新された際、更新情報を送信するよう促す事ができるようになります。これはミーティングの更新情報の送信に失敗しているクライアント[422]やクライアントタイプ[438]に限定して使用するべきで、更新情報が重複して送られてしまう可能性があります。また、このオプションはクライアントとクライアントタイプの設定ページでのみ利用できます。

全ての送信メールで開封確認を要求
クライアントから送信される全てのメールで開封確認要求を行うにはこのオプションを有効にして下さい。これはデフォルトで無効になっています。

送信者からリクエストされた際送信済メールについて開封確認を送信
サーバー側で開封確認要求を検出し、既読フラグがついたメールの開封通知を送信するにはこのオプションを使用します。これはデフォルトで無効になっています。

ReplyToアドレスに指定したエイリアスとして送る
クライアントによっては、エイリアスを使ったメール送信を許可していません。この機能は Exchange ActiveSync（EAS）プロトコル 395 16.xで追加されたものですが、クライアントの中には16.xに対応していないものもあります。例えば、Windows用OutlookはEAS 14.0だけを使用しており、ユーザーが関連するアドレスを指定して送信する事のみ許可しており、生成されたメールはユーザーの選択を正しく反映していません。このオプションでは、ReplyToのアドレスがユーザー用の正しいエイリアス 757 であれば、これを使ってメール送信を行います。この設定の全体値はデフォルトで有効です。

デフォルトの連絡先にパブリック連絡先を仮想的に統合する
パブリック連絡先をユーザーの端末上でデフォルトの連絡先と統合したい場合はこのオプションを有効にします。これは仮想的な統合で、実際には連絡先フォルダへデータのコピーは行っていません。これはグローバルアドレス帳（GAL）の検索機能に対応していないクライアントにとって便利な機能です。これはデフォルトで無効になっています。

Junk-Emailフォルダへ移動したメールの送信者をブロックする
有効にすると、クライアントが特定のメールを自分のJunk Emailフォルダへ移動した際、対象のメール送信者がブロックされた送信者連絡先フォルダへ追加されます。

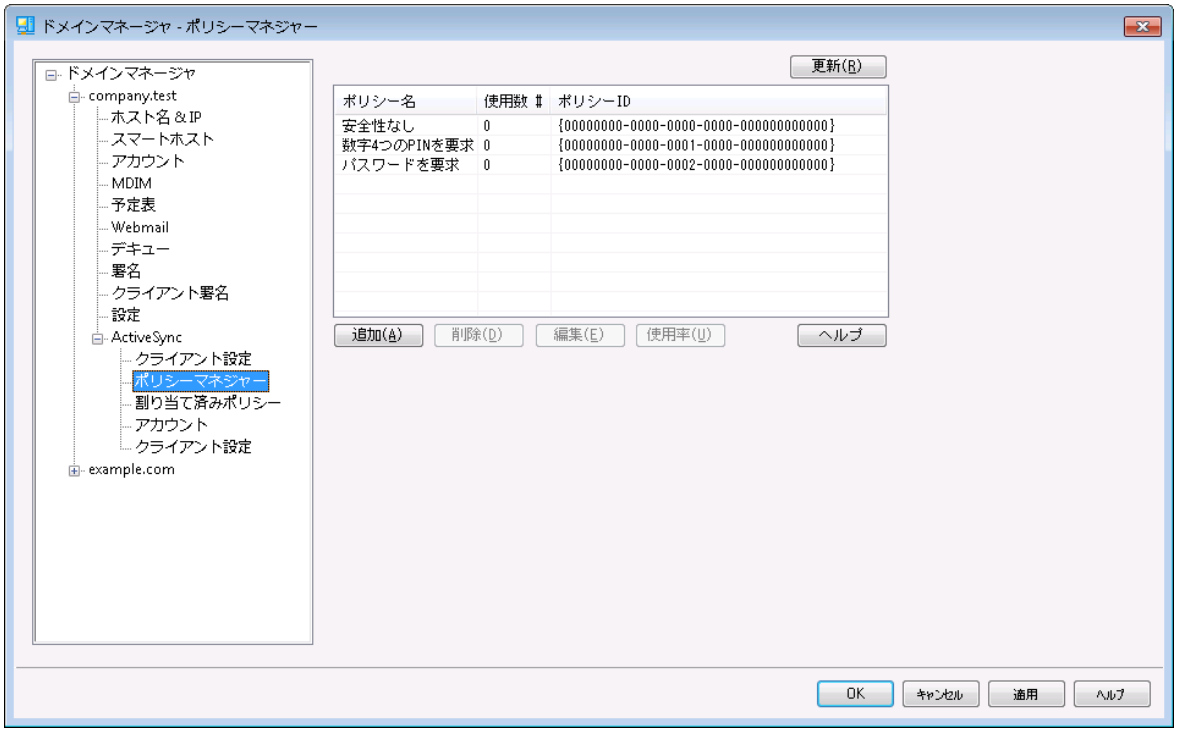
ミーティング要求が許可/拒否された際、ミーティング要求に対する応答の送信を強制的に行う
このオプションを使用すると、クライアントがミーティング要求に対して、許可や拒否、その他のアクションを選択した際、ミーティング要求に対する応答を開催者へ送信します。これは、こうした更新情報を自動送信する事ができない特定のクライアント用の機能です。

有効な設定をプレビュー
このボタンは全てのクライアント設定（ドメイン 397, アカウント 413, クライアント 422）に対して使用できます。画面のオプションはデフォルト値をその上位の画面から引き継いでいるため、この機能は表示されている画面の現在の設定確認を行う際にもご利用頂けます。

参照:

ActiveSync » クライアント設定 384
ActiveSync » アカウント 413
ActiveSync » クライアント 422

3.2.11.2 ポリシーマネージャ



ここではユーザーのデバイスに適用するActivSyncポリシーに関する様々な設定を行います。定義済ポリシーが提供されており、独自のポリシーの作成や編集、削除もここで行えます。ドメインのデフォルトポリシーはアカウント 413 やクライアント 422 へ適用された割り当て済ポリシーで上書きされます。

全てのActiveSyncデバイスがポリシーを常に認識したり適用したりできるわけではありません。ポリシー又は同時に適用された特定のポリシーを無視する場合や、変更を適用するのにデバイスの再起動が必要となる場合があります。また、新しいポリシーをデバイスに適用しても、デバイスへ実際にポリシーが適用されるのは次にActiveSyncサーバーへ接続したタイミングとなります。ポリシーはデバイス側から接続するまで、「プッシュ」配信は行われません。

ActiveSyncポリシー

一覧を右クリックすると次のオプションへのショートカットメニューが表示されます。

ポリシーの作成
このボタンでActiveSyncポリシーエディタを起動し、ポリシーの作成や編集が行えます。

削除
ポリシーの削除を行うには、カスタマイズしたポリシーを一覧から右クリックし、削除をクリックします。確認画面ではいをクリックします。用意されているポリシーは削除できません。

ポリシーの編集
ポリシーを編集するには、カスタマイズしたポリシーを一覧から右クリックし、編集ボタンをクリックします。変更を行ったら、OKボタンをクリックします。用意されているポリシーは編集できません。

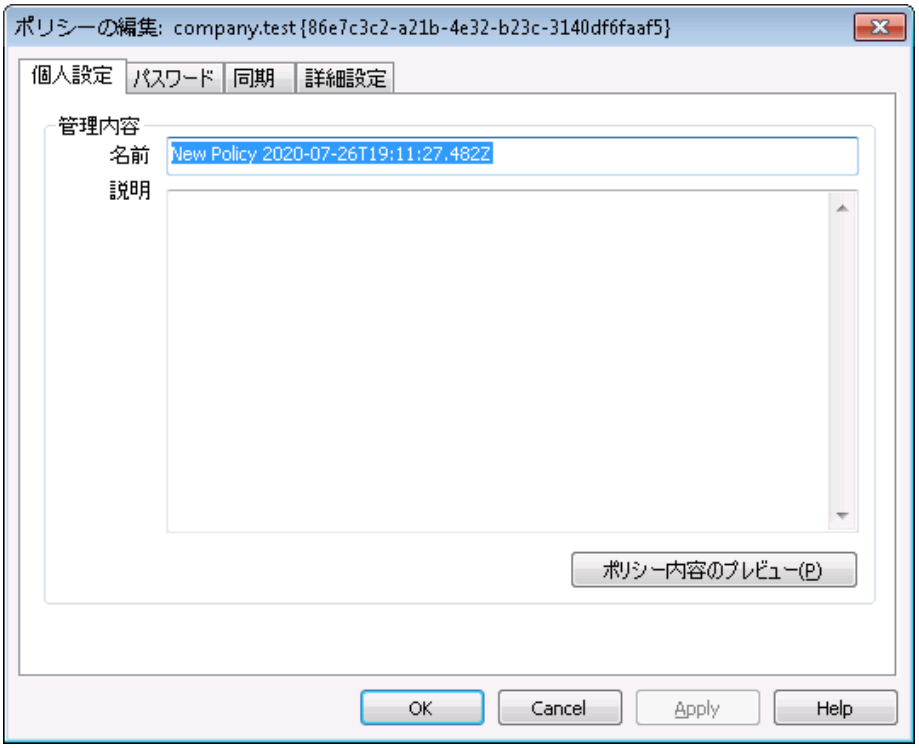
ポリシー使用状況の表示
ポリシーを右クリックしこのボタンをクリックすると、このポリシーを適用しているドメイン、アカウント、クライアントの一覧を表示できます。I

ActiveSyncポリシーエディタ

ActiveSyncポリシーエディタには個人設定、パスワード、同期、詳細設定の4つのタブがあります。この詳細設定タブはActiveSyncシステム場面の*詳細ポリシーオプションの変更を有効にする*[379]をアクティブにするまで非表示になっています。

個人設定

ポリシーの名称と説明を設定します。XMLポリシー文書のプレビューも行えます。



管理内容

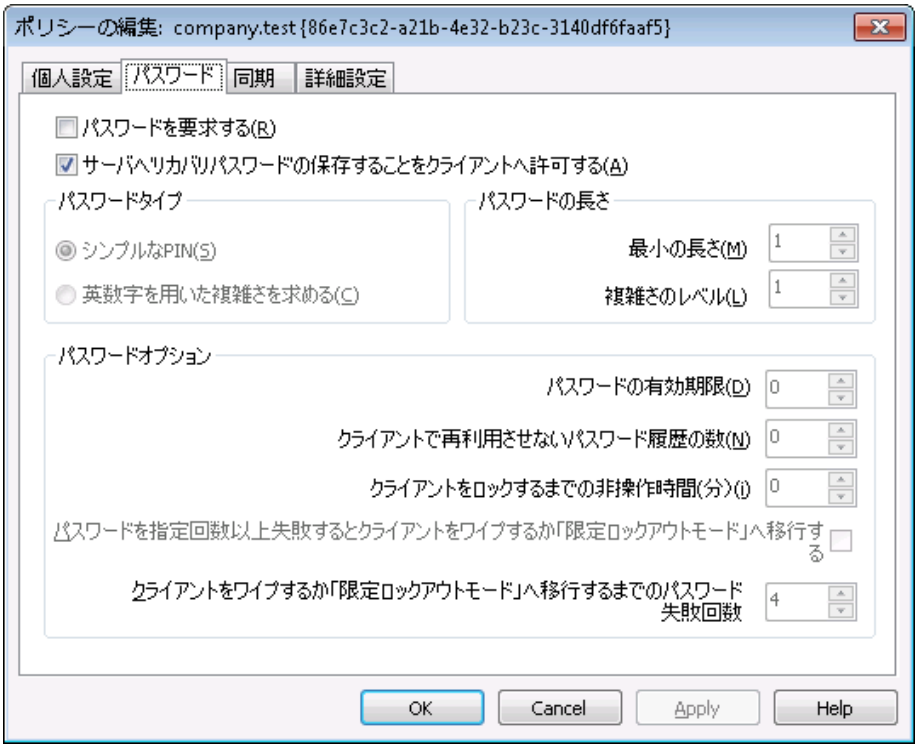
名前
カスタムポリシー名称を指定します。

説明
カスタムポリシーの説明を入力します。ここでの説明はドメイン、アカウント、クライアントへ適用するポリシーの選択の際使用します。

ポリシー内容のプレビュー
ポリシー用のXMLドキュメントのプレビューにこのボタンを使用します。

パスワード

ポリシー用のパスワードオプションと要求設定にこのタブを使用します。



パスワードを要求する
端末でパスワードを要求するにはこのボックスを有効にします。これはデフォルトで無効に設定されています。

サーバで「リカバリーパスワード」の保存を許可するデバイス

クライアントがActiveSyncのリカバリーパスワードオプションを利用できるようにするにはこのオプションを有効にします。端末は一時的なリカバリーパスワードをサーバーへ保存しておく事ができ、パスワードを忘れた場合にこれを使って解除できます。管理者はクライアントの詳細設定[422]でこのパスワードを確認できます。多くの端末ではこの機能に未対応です。

パスワードタイプ

シンプルなPIN
このオプションの実装方法は端末により異なりますが、シンプルなPINをパスワードタイプとして選択した場合、一般的には最少の長さ以外の規定や複雑さのレベルを求められる事はありません。次のようなシンプルなパスワードが利用できます:"111", "aaa", "1234", "ABCD"

英数字を用いた複雑さを求める
シンプルなPINよりも複雑で安全なパスワードを要求する場合はこのポリシーオプションを使用します。複雑さのレベルでは具体的にパスワードの複雑さのレベルを指定します。これはポリシーでパスワードを要求した場合のデフォルト設定です。

パスワードの長さ

最少の長さ
デバイスパスワードの最少文字数を1-16の間で設定するのに使用します。デフォルトでは1に設定されています。

複雑さのレベル
英数字を用いた複雑さの内、複雑さのレベルを指定します。レベルはパスワードに含む必要のある文字列の種類の数で、大文字、小文字、数字、(記号など)英数字以外の文字、の1-4で指定します。例えば、オプションが2と設定されている場合、パスワードには、大文字と小文字、数字と記号、といった、最低2種類の文字列が必要です。このオプションはデフォルトで1に設定されています。

パスワードオプション

パスワードの有効期限
デバイスパスワードを変更するまでの日数を指定します。これはデフォルトで無効(0を指定)に設定されています。

デバイスで再利用させないパスワードの数
古いパスワードの再利用を禁止する履歴の数を指定します。例えば、このオプションが2と設定されていた場合、デバイスのパスワードを変更する際、過去に使った2回前のパスワードまでは再利用できません。これはデフォルトで無効(0を指定)に設定されています。

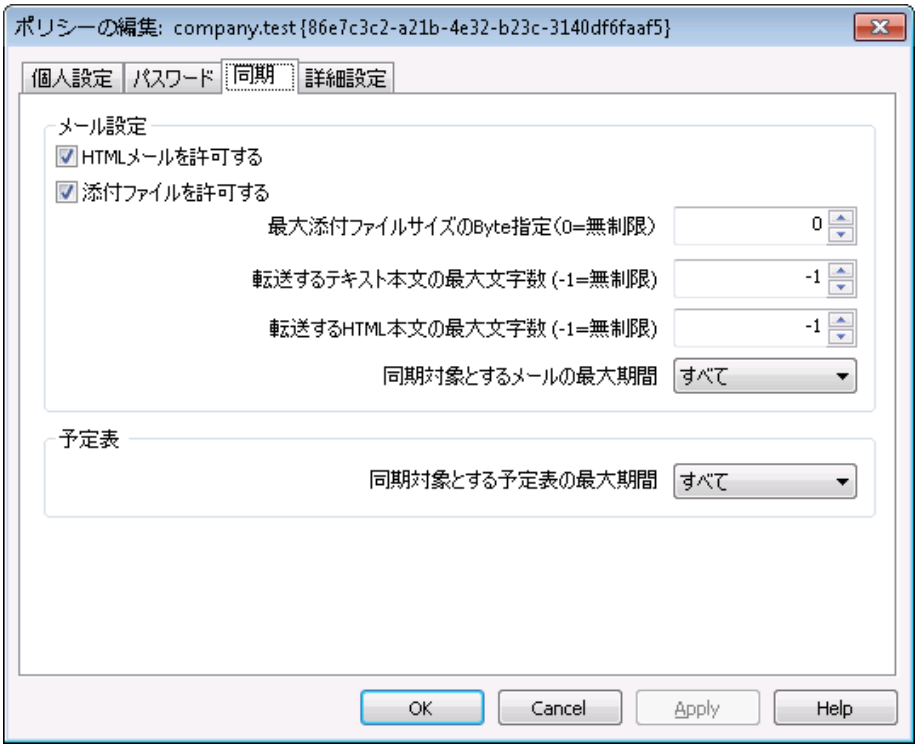
デバイスをロックするまでの非操作期間(分)
端末がロックされるまでの非操作時間を分で指定します。このオプションはデフォルトで無効(0を指定)に設定されています。

連続した認証失敗時端末初期化又はロックアウトモードへの移行
このオプションが有効で、指定した回数パスワード認証に失敗した場合、端末はロックされるか全てのデータが初期化されます。このオプションはデフォルトで無効になっています。

端末初期化又はロックアウトモードへ移行するまでのパスワード入力失敗回数
「デバイスを初期化」が有効で、指定した回数ユーザーがパスワード認証へ失敗した場合、端末の設定によって、端末は初期化されるか、「ロックアウトモード」を開始します。

同期

この画面ではHTMLメールの設定や、添付ファイルの許可、転送する文字数の制限、予定表の同期対象期間の設定が行えます。



メール設定

HTMLメールを許可する

デフォルトでHTML形式のメールはActiveSyncクライアントと同期したり、ActiveSyncクライアントへ送信されます。このチェックをオフにすると、プレインテキスト形式のメールのみが送信されます。

添付ファイルを許可する

デバイスが添付ファイルをダウンロードできるようになります。このオプションはデフォルトで有効です。

最大添付ファイルサイズbytes指定(0=無制限)

デバイスで自動ダウンロードできる添付ファイルの最大サイズを指定します。デフォルトでサイズの制限はありません(0に設定されています)。

転送するテキスト本文の最大文字数(-1=無制限)

クライアントに送信されるプレインテキストメールの本文の最大文字数を指定します。本文に指定した数を超える文字数が使用された場合、本文は最大文字数で短縮されます。デフォルトでこの値は無制限(-1に設定)されています。この値を0にすると、メッセージヘッダのみが送信されます。

転送するHTML本文の最大文字数(-1=無制限)

クライアントに送信されるHTMLメールの本文の最大文字数を指定します。本文に指定した数を超える文字数が使用された場合、本文は最大文字数で短縮されます。デフォルトでこの値は無制限(-1に設定)されています。この値を0にすると、メッセージヘッダのみが送信されます。

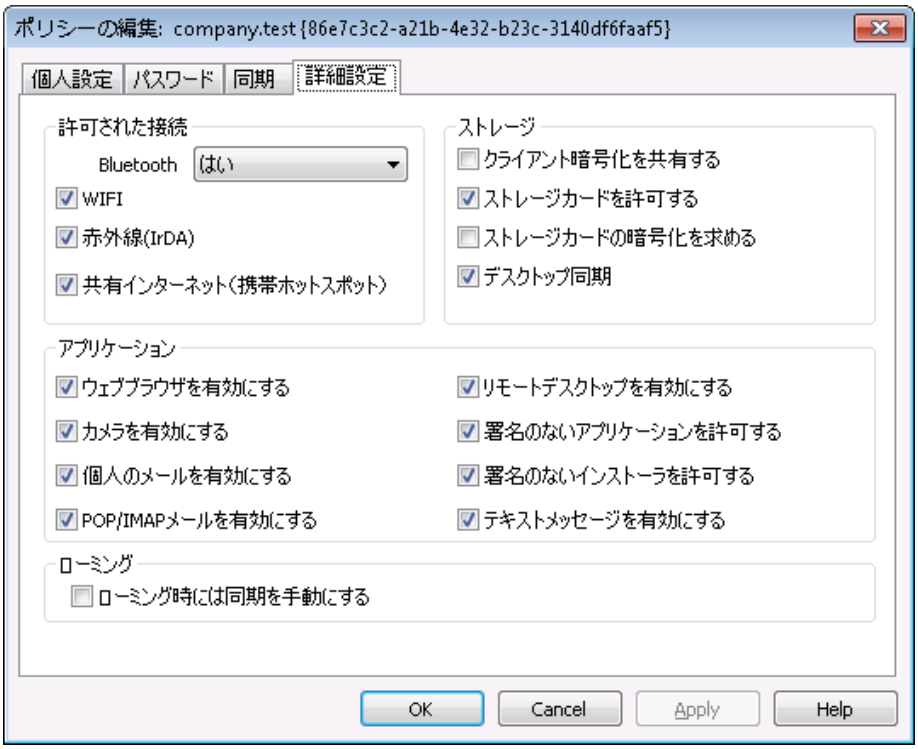
同期対象とするメールの最大期間
最大日数分前の日付から今日までのメールが、デバイスとの同期対象となります。デフォルトでは「全て」に設定されており、メールは配信日時に関わらず全て同期対象となります。

予定表

同期対象となる予定表の最大期間
今日から何日前までの予定表をデバイスとの同期対象とするかをここで指定します。デフォルトでは「全て」に設定されており、予定は日時に関わらず全て同期対象となります。

詳細設定

詳細設定タブでは許可する接続の種類、特定のアプリケーションの許可、ストレージと暗号化、ローミングの設定が行えます。



この詳細設定タブはActiveSyncfor MDaemon 場面の*詳細ポリシーオプションの変更を有効にする*[379]をアクティブにするまで非表示になっています。

許可された接続

Bluetooth
端末へのBluetooth接続を許可するかどうかを指定します。はい、でBluetooth接続を許可し、いいえ、で拒否、ハンズフリーでBluetoothをハンズフリーの場合のみに制限します。このオプションはデフォルトで、はい、に設定されています。

WIFI
WIFI接続を許可します。デフォルトで有効です。

赤外線（IrDA）
赤外線（IrDA）接続を許可します。デフォルトで有効です。

共有インターネット（携帯ホットスポット）
デバイスによる共有インターネット（ホットスポット）の利用を許可します。これはデフォルトで有効です。

ストレージ

デバイスの暗号化を要求する
デバイスの暗号化を要求する場合はこのオプションを有効にします。全てのデバイスが暗号化の要求に対応しているわけではありません。これはデフォルトで無効になっています。

ストレージカードを許可する
デバイスでのストレージカードの利用を許可します。これはデフォルトで有効です。

ストレージカードの暗号化を求める
ストレージカードの暗号化を要求する場合にこのオプションを使用します。これはデフォルトで無効になっています。

デスクトップ同期
デバイスでデスクトップActiveSyncを許可します。デフォルトで有効です。

アプリケーション

ウェブブラウザを有効にする
デバイスでブラウザの利用を許可します。このオプションはデバイスによって未対応の場合があり、3rdパーティー製のブラウザには適用できない場合があります。デフォルトで有効です。

カメラを有効にする
デバイスでのカメラの利用を許可します。デフォルトで有効です。

個人のメールを有効にする
デバイスで個人用メールアカウントの設定を許可します。無効になっている場合、ActiveSync端末毎にメールアカウントやサービスが接続不可となります。これはデフォルトで有効です。

POP/IMAPメールを有効にする
POPやIMAPメールへのアクセスを許可します。デフォルトで有効です。

リモートデスクトップを有効にする

リモートデスクトップの利用を許可します。デフォルトで有効です。

署名のないアプリケーションを許可する
デバイスで未署名のアプリケーションの利用を許可します。これはデフォルトで有効です。

署名のないインストーラを許可する
デバイスで未署名のインストーラの実行を許可します。これはデフォルトで有効です。

テキストメッセージを有効にする
デバイスでテキストメッセージを許可します。これはデフォルトで有効です。

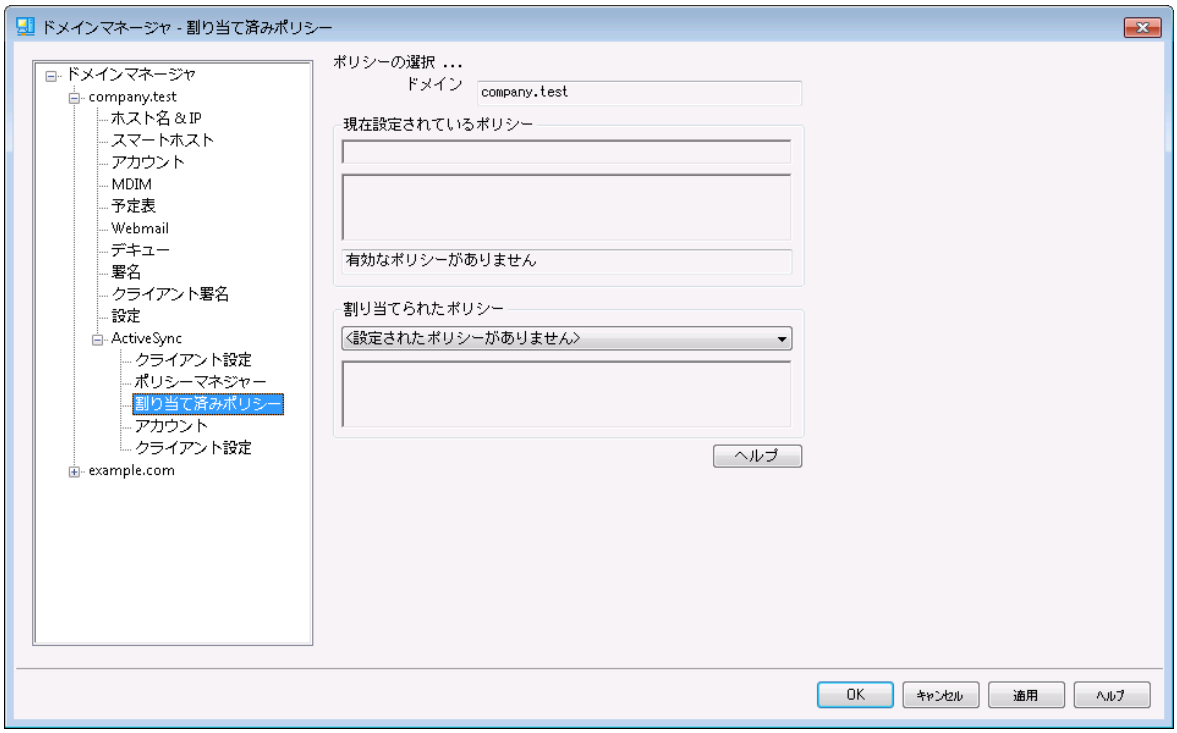
ローミング

ローミング中には同期を手動にする
ローミング中にはデバイスとの同期を手動で行わせるようにする場合はこのポリシーオプションを使用します。ローミング中の自動同期を行うと、キャリアや契約内容によって、データの転送コストが上がってしまう場合があります。このオプションはデフォルトで無効になっています。

参照:

ドメインマネージャ ≫ 割り当て済ポリシー 210
ActiveSync ≫ アカウント 413
ActiveSync ≫ クライアント 422

3.2.11.3 割り当て済みポリシー



ここではドメインへデフォルトのActiveSyncポリシー202割り当てを行います。ActiveSyncクライアントがこのドメインに属するアカウントを使って接続してきた場合、アカウントに特化した代わりのポリシーがなければ、デフォルトのポリシーがクライアントに割り当てられます。

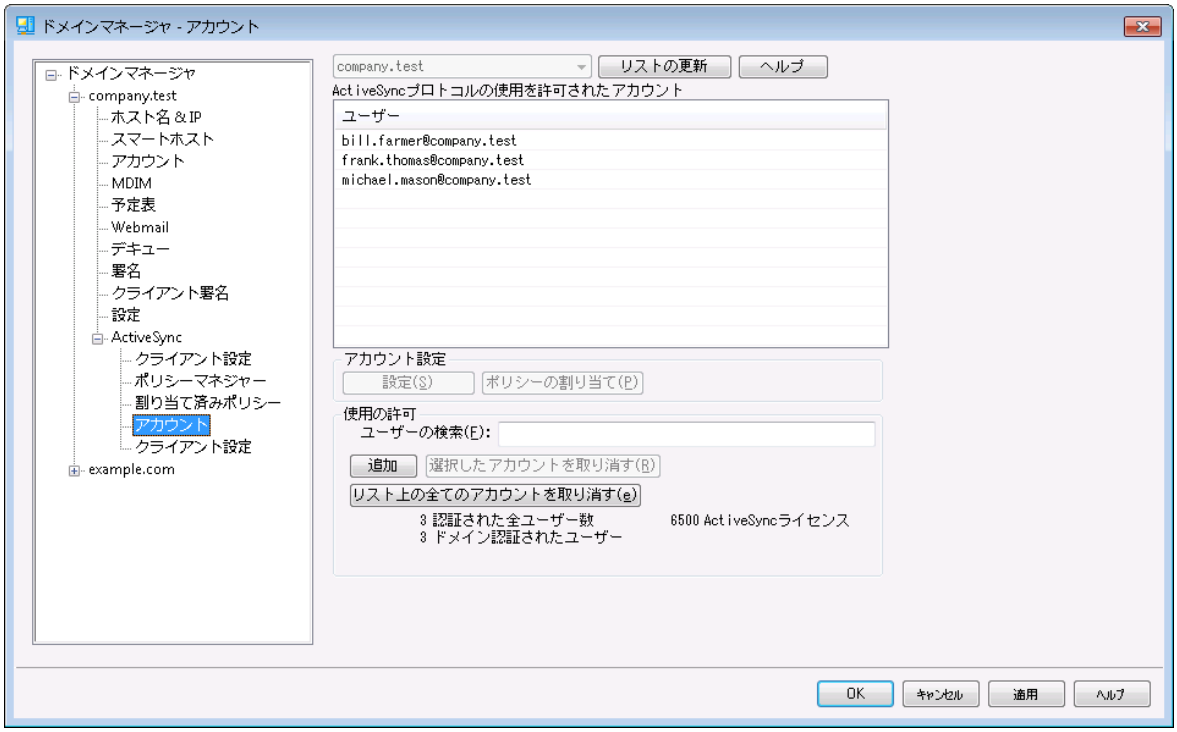
デフォルトのActiveSyncポリシーを割り当てる

デフォルトのActiveSyncポリシーをドメインに割り当てる場合は、ポリシーの割り当て、のドロップダウンメニューをクリックし、対象ポリシーを選択し、OKをクリックします。

参照:

ドメインマネージャ ≫ ポリシーマネージャ202
ActiveSync ≫ アカウント413
ActiveSync ≫ クライアント422

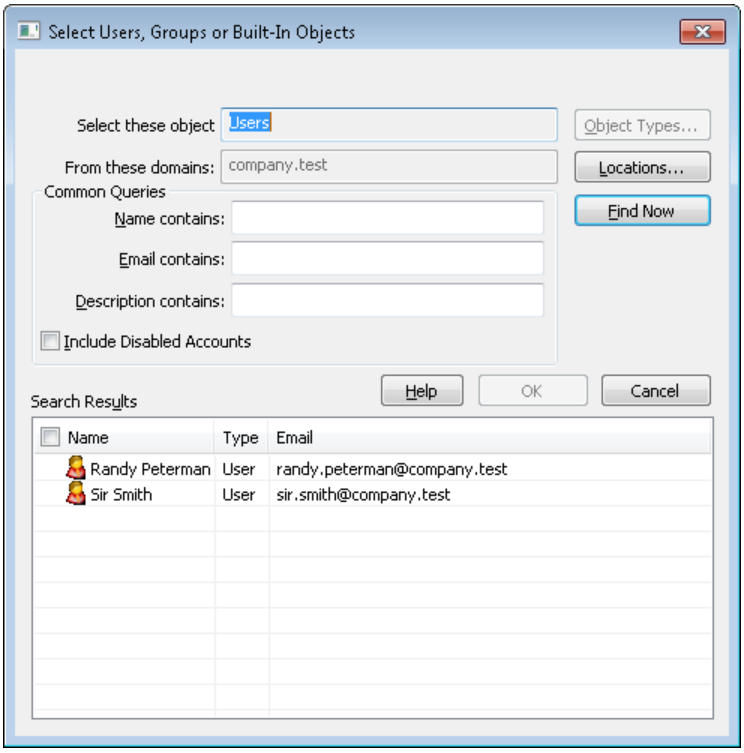
3.2.11.4 アカウント



この画面では、ActiveSyncの利用を許可するドメインユーザーを指定したり、各ユーザーのクライアント設定を編集したり、ActiveSyncポリシーの割り当てを行う事ができます。

アカウントを許可する

追加 をクリックし、ドメインアカウントのActiveSync利用を手動で許可する事ができます。アカウントの検索や選択のためのユーザー選択ダイアログが起動します。



共通クエリ
このオプションでユーザー名、メールアドレス、アカウントの説明[650]の中の一部を使って検索範囲を絞り込む事ができます。検索範囲に一致した全ユーザーを検索結果に表示するには、このフィールドは空白のままにしてください。

無効化されたアカウントも含む
無効化されたアカウント[650]を検索対象に含むにはこのオプションをクリックします。

今すぐ検索
検索条件を指定したら、今すぐ検索をクリックして検索を実行します。

検索結果
検索後、検索結果からユーザーを選択し、OKをクリックすると、許可されたユーザー一覧に対象ユーザーが追加されます。

アカウントを取り消す

アカウントのActiveSyncの利用権限を取り消すには、一覧から選択し、選択アカウントを取り消すをクリックします。全てのアカウントを取り消すには、リスト上の全アカウントを取り消すボタンをクリックします。

> *ActiveSyncプロトコルを使った最初のアクセス時にアカウントへ許可する*[413]のオプションを有効にしていた場合、アカウントの取り消しによりアカウントの持つアクセス権は一覧から削除されますが、次に端末がアカウントへ接続した際、再度認証が行われます。

ActiveSyncポリシーの割り当て

ポリシー[405]をアカウントへ割り当てるには:

1. 一覧からアカウントを選択します。
2. **ポリシーを適用**をクリックします。ポリシー適用ダイアログが起動します。
3. 適用するポリシーのドロップダウンリストから、適用するポリシーを選択します。
4. **OK**をクリックします。

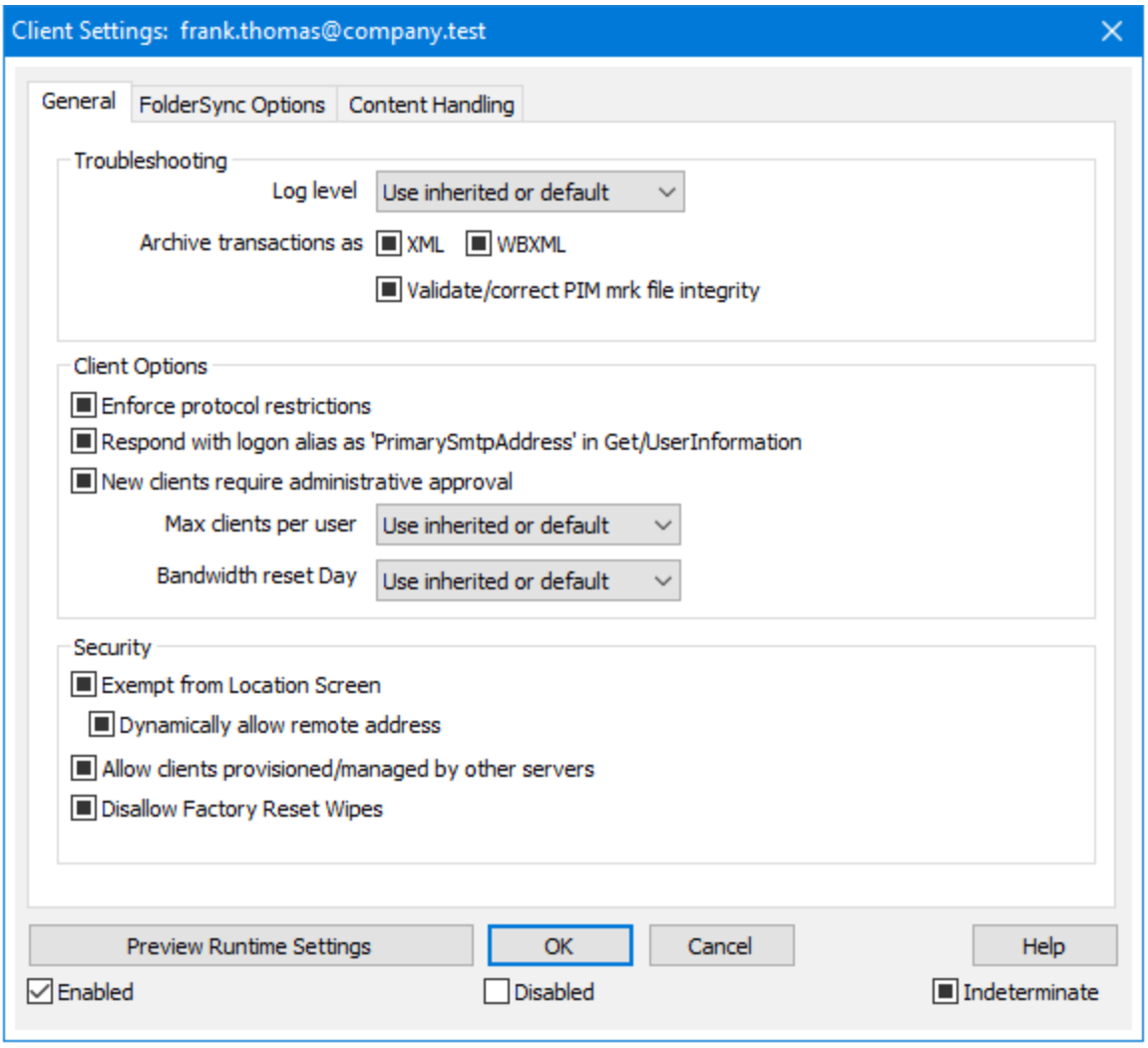
ポリシーはこのアカウントへ接続する新規デバイスに対して適用されます。

許可されたアカウント一覧の検索

ActiveSyncの利用を許可しているアカウント数が多い場合は、特定のアカウント一覧を検索するのに、ユーザー検索ボックスを使用できます。アカウントのメールアドレスの先頭文字をいくつかタイプしてください。

設定

アカウントを選択し、設定をクリックすると、対象アカウントのクライアント設定が行えます。ここでの設定は対象アカウントへ接続しているActiveSyncクライアントに対して適用されます。



デフォルトでこの画面の全てのオプションは「継承又はデフォルト」となり、ドメインのクライアント設定[196]画面の該当オプションから、設定内容を引き継ぐ事になっています。ドメインのクライアント設定で行った変更はこの画面へも反映されます。反対に、この画面で行った設定変更はアカウントのドメインレベル設定を上書きします。

全般

トラブルシューティング

ログレベル

ActiveSync for MDaemonはログデータ量に応じた、6つのレベルのログに対応しています。

デバッグ 最も詳細なログで、記録できる全ての情報が含まれており、問題の診断にのみ使用されます。

情報 通常のログで、一般的な操作が詳細なしで記録されます。これはデフォルトのログレベルです。

警告	警告、エラー、クリティカルエラー、起動と終了がログに記録されます。
エラー	エラー、クリティカルエラー、起動と終了がログに記録されます。
クリティカル	クリティカルエラー、起動と終了がログに記録されます。
なし	起動と終了だけがログに記録されます。
継承	デフォルトで、ログレベルの設定はクライアント設定の階層から継承されます。そのため、クライアントは設定をクライアントタイプから引継ぎ、クライアントタイプはアカウントから引継ぎ、アカウントはグループから引継ぎます。全体のクライアント設定は 診断 393 ダイアログのログレベル設定を元にしています。

トランスアクションを [XML | WBXML]としてアーカイブ
XMLやWBXMLデータをアーカイブするには、*XMLと WBXMLをアーカイブ...* のオプションを使用します。これはデバッグの際役立ちます。全体オプションはデフォルトで無効になっています。

PIM mrkファイルの整合性を確認する
クライアントのPIMデータの整合性テストを実施し、iCal UIDの重複や空の要求フィールドといった、同期を妨げているものがないかどうかを確認します。この全体設定はデフォルトで無効になっています。

クライアントオプション

プロトコル制限を強制する
クライアントで許可されているプロトコルバージョン以外のアクセスを拒否する場合はこのオプションを有効にします。デフォルトでこのオプションは無効になっており、プロトコル制限は異なるプロトコルのクライアントを拒否していません。プロトコル制限は単純に、クライアントに対して使用するべきプロトコルを伝えるのみの機能を提供しています。クライアントがそれでも制限されているプロトコルを使った場合、MDaemonはその接続を受け入れます。詳細は次のページをご覧下さい: プロトコル制限 395

Get/UserInformationへの応答でログオンエイリアスを'PrimarySmtpAddress' として使用する
サービスがSettings/Get/UserInformationリクエストに対する応答としてエイリアスやセカンダリアドレスをプライマリアドレスとして利用できるようにします。これはiOS 9.xへアップデートした際エイリアスからメールを送信できなくなった事に対する対処です。このオプションによって使用に反した応答を受け取る場合があります。

新しいクライアントは管理者の承認が必要
新しいクライアントがアカウントとの同期を開始する前に、管理者による承認を必要とする場合はこのオプションを有効にします。 クライアント 422 一覧で認証待ちのクライアントが確認でき、管理者は同じ画面から承認が行えます。この設定はデフォルトで無効になっています。

ユーザー毎の最大クライアント
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用

できません。

帯域リセット日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

セキュリティ

ロケーションスクリーンから除外する
ActiveSyncクライアント設定で端末をロケーションスクリーニング[520]から除外する場合はこのオプションを有効化します。これにより認証済ユーザーは、例えば認証がブロックされている場所へ出張しているような場合であっても、ActiveSync経由でアカウントへアクセスする事ができるようになります。端末を除外するためには、チューニング画面にあるこの日数を超えて認証されなかった端末を自動削除[381]設定の時間内に、ActiveSyncを使った接続と認証を行っておく必要があります。

リモートアドレスを動的に除外
接続元のリモートIPアドレスをロケーションスクリーニングの除外リストへ追加する事ができます。このオプションは、同じIPアドレスを使って接続する他のクライアントがある場合に便利です。

ユーザー毎の最大クライアント数
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域の統計情報をリセットする日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

他のサーバーで管理されているクライアントへの接続を許可する
デフォルトで、ActiveSyncサーバーが特定のクライアントへデータやポリシーを送信する際、対象クライアントが他のActiveSyncサーバーからも管理されている事が分かった場合も、クライアントはMDaemonへアクセスする事ができます。しかし、このような環境の場合、適用するポリシーが他のActiveSyncサーバーと競合する可能性があります。一般的に、クライアントはポリシーが競合した場合、厳しい方へ合わせる傾向があります。こうしたクライアントからの接続を制限する場合は、このオプションを無効化して下さい。

工場出荷時への完全ワイプを無効化
オン/はい、を設定すると、ActiveSyncクライアントの完全ワイプが行えなくなります。クライアントでリモートからの完全ワイプを許可する場合、最初にこのオプションを無効化して下さい。このオプションはデフォルトで無効に設定されています。クライアントページの次の項目を参照して下さい:
ActiveSyncクライアントの完全ワイプ[422]

フォルダ同期オプション

フォルダ同 期 オプション

除 外

ユーザの [許 可 リスト /ブロックリスト] フォルダ
デフォルト でユーザーの許 可 リスト とブロックリスト の連 絡 先 フォルダは端 末 と同 期 を行 いません。これらはMDaemonがスパムからシステムを自 動 的 に保 護 するのを支 援 する目 的 で使 用 されます。そのため、許 可 リスト やブロックリスト は端 末 上 に連 絡 先 として表 示 する必 要 性 はありません。

デフォルト 以 外 のメールフォルダ
デフォルト で、ユーザーが作 成 したメールフォルダとデフォルト メールフォルダは全 て端 末 と同 期 します。同 期 するのを受 信 箱 や送 信 箱 、削 除 済 アイテム、下 書 き、といった、デフォルト のメールフォルダのみにしたい場 合 はこのオプションを有 効 にして下 さい。ユーザーが作 成 したフォルダは同 期 対 象 に含 まれません。 このオプションはデフォルト で無 効 になっています。

デフォルト 以 外 のPIMフォルダ
デフォルト で、(連 絡 先 、予 定 表 、仕 事 などの) PIMフォルダは全 て端 末 と同 期 します。同 期 するのをデフォルト のPIMフォルダのみにしたい場 合 はこのオプションを有 効 にして下 さい。このオプションが有 効 な場 合 で、ユーザーが複 数 の予 定 表 を保 有 してる場 合 デフォルト の予 定 表 のみが同 期 対 象 となります。 このオプションはデフォルト で無 効 になっています。

含 む

パブリックフォルダの階 層
ユーザーがアクセス権 を持 っている パブリックフォルダ 283 をユーザーのActiveSync用 端 末 のフォルダー 覧 へ含 むにはこのオプションを有 効 にします。これはデフォルト で有 効 です。

検 索 を許 可 する
パブリックフォルダ 283 をユーザーが検 索 できるようになります。 これはデフォルト で許 可 されています。

パブリックフォルダの横 断 (フォルダ名 の公 開)
デフォルト で、クライアント がパブリックのサブフォルダへのアクセスや同 期 を行 うには、サブフォルダと上 位 のパブリックフォルダ 283 全 てに対 してルックアップ権 限 285 が必 要 です。上 位 のフォルダに対 するアクセス権 がない場 合 、その中 のサブフォルダに対 しては、例 え設 定 上 は許 可 されていても、アクセスする事 はできません。クライアント からこうしたサブフォルダへアクセスできるようにする場 合 は、このオプションを有 効 にします。注 意 点 : このオプションを有 効 化 すると、上 位 のフォルダもクライアント へ許 可 する事 となり、セキュリティのリスクを招 く恐 れがあります。 このオプションはデフォルト で無 効 になっています。

許 可 するパブリックフォルダの最 大 数
端 末 で処 理 するパブリックフォルダ数 を制 限 する場 合 はこのオプションを使 用 します。制 限 が設 定 されると、サーバーは最 大 数 に到 達 するまでフォルダー 覧 を処 理 し、これを超 えるとその後 のデータを送 りません。処 理 するフォルダの順 番 を決 める事 はできません。デフォルト で、全 体 での最 大 数 は設 定 されていません。

共 有 フォルダも含 める

ユーザーがアクセス権を持っている 共有フォルダ[107] をユーザーのActiveSync用端末のフォルダー一覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
共有フォルダ[676] をユーザーが検索できるようになります。これはデフォルトで許可されています。

コンテンツ処理

コンテンツ処理オプション

クライアントにフラグ付けされたメール用にタスク・リマインダーを作成
このオプションでMDaemonはフラグが付いたアイテムごとに仕事を作成し、リマインダーをユーザーへ送信できるようになります。この設定の全体値はデフォルトで有効です。

予定を編集した際、常にミーティングのアップデートを送信
クライアントの中には、ミーティングを編集した際、更新情報を適切に送信しないものもあります。このオプションを使うとActiveSyncサービスへ、ミーティングが開催者によって更新された際、更新情報を送信するよう促す事ができるようになります。これはミーティングの更新情報の送信に失敗しているクライアント[422]やクライアントタイプ[438]に限定して使用するべきで、更新情報が重複して送られてしまう可能性があります。また、このオプションはクライアントとクライアントタイプの設定ページでのみ利用できます。

全ての送信メールで開封確認を要求
クライアントから送信される全てのメールで開封確認要求を行うにはこのオプションを有効にして下さい。これはデフォルトで無効になっています。

送信者からリクエストされた際送信済メールについて開封確認を送信
サーバー側で開封確認要求を検出し、既読フラグがついたメールの開封通知を送信するにはこのオプションを使用します。これはデフォルトで無効になっています。

ReplyToアドレスに指定したエイリアスとして送る
クライアントによっては、エイリアスを使ったメール送信を許可していません。この機能は Exchange ActiveSync（EAS）プロトコル[395] 16.xで追加されたものですが、クライアントの中には16.xに対応していないものもあります。例えば、Windows用OutlookはEAS 14.0だけを使用しており、ユーザーが関連するアドレスを指定して送信する事のみ許可しており、生成されたメールはユーザーの選択を正しく反映していません。このオプションでは、ReplyToのアドレスがユーザー用の正しいエイリアス[757]であれば、これを使ってメール送信を行います。この設定の全体値はデフォルトで有効です。

デフォルトの連絡先にパブリック連絡先を仮想的に統合する
パブリック連絡先をユーザーの端末上でデフォルトの連絡先と統合したい場合はこのオプションを有効にします。これは仮想的な統合で、実際には連絡先フォルダへデータのコピーは行っていません。これはグローバルアドレス帳（GAL）の検索機能に対応していないクライアントにとって便利な機能です。これはデフォルトで無効になっています。

Junk-Emailフォルダへ移動したメールの送信者をブロックする
有効にすると、クライアントが特定のメールを自分のJunk Emailフォルダへ移動した際、対象のメー

ル送信者がブロックされた送信者連絡先フォルダへ追加されます。

ミーティング要求が許可/拒否された際、ミーティング要求に対する応答の送信を強制的に行う
このオプションを使用すると、クライアントがミーティング要求に対して、許可や拒否、その他のアクションを選択した際、ミーティング要求に対する応答を開催者へ送信します。これは、こうした更新情報を自動送信する事ができない特定のクライアント用の機能です。

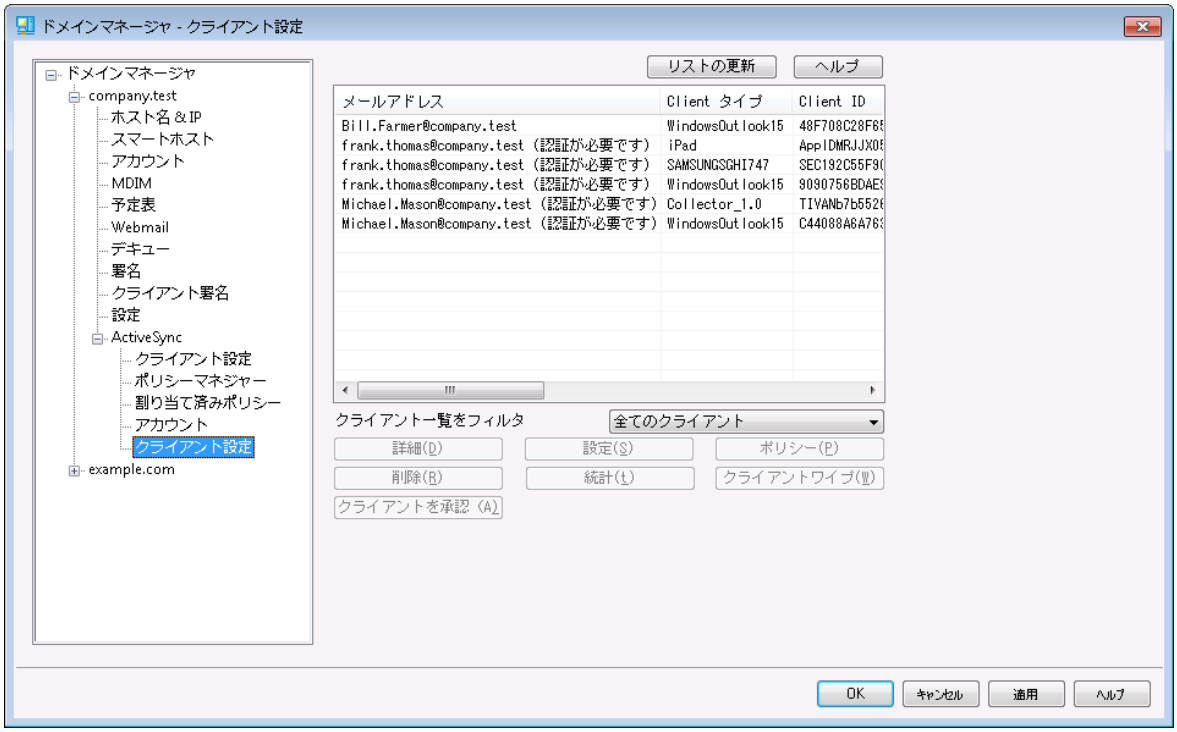
有効な設定をプレビュー

このボタンは全てのクライアント設定（ドメイン397, アカウント413, クライアント422）に対して使用できます。画面のオプションはデフォルト値をその上位の画面から引き継いでいるため、この機能は表示されている画面の現在の設定確認を行う際にもご利用頂けます。

参照:

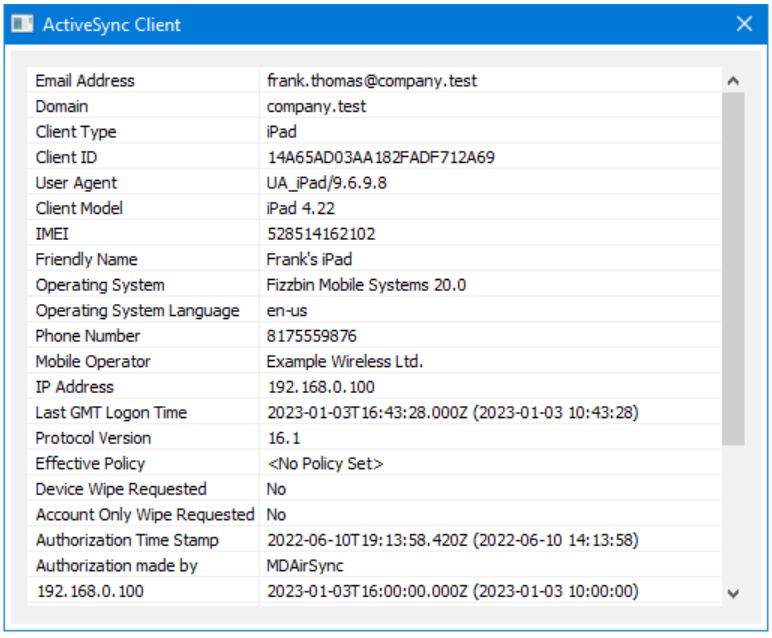
ActiveSync ≫ クライアント設定384
ActiveSync ≫ ドメイン397
ActiveSync ≫ クライアント422

3.2.11.5 クライアント



ここではドメインに関連付けされたActiveSyncデバイス毎のエントリが確認できます。

ActiveSync Client Details



エントリを選択し**詳細**をクリック(またはエントリをダブルクリック)すると、クライアント詳細ダイアログが起動します。この画面では、Clientタイプ、Client ID、最終ログイン時間、といった、クライアントの情報を確認できます。

クライアント設定

クライアントを右クリックし **クライアント設定のカスタマイズ** をクリックするとクライアント設定の管理画面が起動します。デフォルト設定はClientタイプの設定を継承していますが、この値は任意のものへ変更する事ができます。デバイスのクライアント設定の管理を参照してください。

ActiveSyncポリシーの適用

ポリシー[405]は次のように端末へ適用します:

1. 一覧から端末を右クリックします。.
2. **ポリシーの適用**をクリックすると、ポリシーの割り当てダイアログが起動します。
3. **割り当てポリシー**のドロップダウンリストからポリシーを選択します。
4. **OK**をクリックします。

統計

エントリを右クリックし、**統計を表示**をクリックすると、クライアント統計ダイアログが起動し、クライアント様々な統計情報を確認できます。

統計のリセット

クライアントの統計情報を初期化するには、統計、統計のリセットをクリックし、確認メッセージでOKをクリックします。

ActiveSyncクライアントの削除

ActiveSyncクライアントを削除するには、 クライアントを右クリックし 削除 をクリックし、はい、をクリックします。これにより、クライアントとMDaemonに関連した全ての同期情報が削除されます。今後ユーザーが同じActiveSyncクライアントで同期を行った場合、MDaemonは対象クライアントを初めて同期を行うクライアントとして取扱います。全てのデータはMDaemonと再同期されます。

ActiveSyncクライアントの完全初期化

選択したActiveSyncクライアントへ ポリシー[405]が適用されると、クライアントはポリシーを適用し、応答した後に完全初期化を利用できます。ActiveSyncクライアントを完全に初期化するには、クライアントを一覧から選択し完全初期化をクリックします。次回クライアントが接続すると、MDaemonは全てのデータを削除するか、工場出荷時の設定をリストアします。クライアントによっては、ダウンロード済アプリなど、全てのデータを削除してしまう場合があります。また、クライアントのActiveSyncエントリがMDaemonに残っている間は、クライアントがMDaemonへ接続する度に再度初期化が実行されます。クライアントを削除する際には、これをブロックリスト[391]へ追加し、今後の接続を行わないようにします。最後に、初期化済のデバイスを再度接続する場合は、デバイスを右クリックし、ワイプアクションを中止、をクリックします。同時にブロックリストからも削除して下さい。

アカウントのActiveSyncクライアントのワイプ

クライアントから、メール、予定表、連絡先といった、アカウントのデータのみを削除する場合は、右クリックし、**クライアントからメールとPIMのアカウントワイプ**をクリックします。 アカウントワイプオプションは完全初期化ににていますが、全てのデータを初期化するのではなく、メールや予定表、連絡先といったアカウント関連データのみを対象にします。その他の、アプリや写真、音楽などは端末上に残ります。

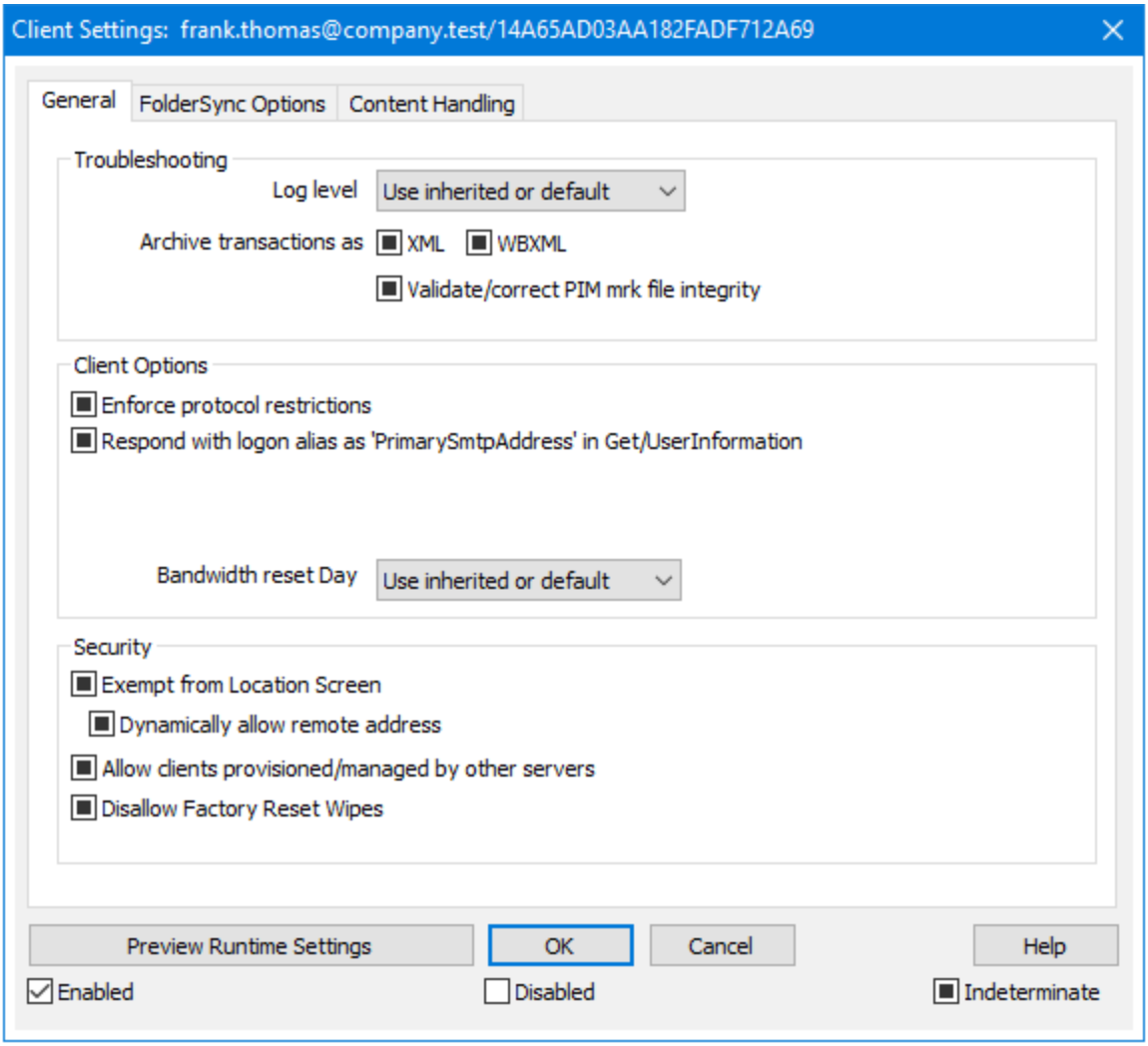
クライアントの承認

ActiveSyncクライアント設定[384]の*"新規クライアントは管理者の承認が必要"*オプションが承認が必要と設定されていた場合、クライアントを選択し クライアントの同期を許可、 をクリックすることでクライア

ントのサーバーとの同期を承認します。

デバイスのクライアント設定の管理

デバイスレベルのクライアント設定画面では端末毎の設定が管理できます。



デフォルトでこの画面の全てのオプションは「継承又はデフォルト」と設定されており、各オプションがClientタイプクライアント設定[438]の関連オプションの設定を継承します。同様に、この画面で行った設定変更はデバイスのクライアントレベル設定を上書きします。

全般

トラブルシューティング

ログレベル

ActiveSync for MDaemonはログデータ量に応じた、6つのレベルのログに対応しています。

デバッグ	最も詳細なログで、記録できる全ての情報が含まれており、問題の診断にのみ使用されます。
情報	通常のログで、一般的な操作が詳細なしで記録されます。これはデフォルトのログレベルです。
警告	警告、エラー、クリティカルエラー、起動と終了がログに記録されます。
エラー	エラー、クリティカルエラー、起動と終了がログに記録されます。
クリティカル	クリティカルエラー、起動と終了がログに記録されます。
なし	起動と終了だけがログに記録されます。
継承	デフォルトで、ログレベルの設定はクライアント設定の階層から継承されます。そのため、クライアントは設定をクライアントタイプから引継ぎ、クライアントタイプはアカウントから引継ぎ、アカウントはグループから引継ぎます。全体のクライアント設定は 診断 393 ダイアログのログレベル設定を元にしています。

トランスアクションを [XML | WBXML]としてアーカイブ
XMLやWBXMLデータをアーカイブするには、*XMLと WBXMLをアーカイブ...* のオプションを使用します。これはデバッグの際役立ちます。全体オプションはデフォルトで無効になっています。

PIM mrkファイルの整合性を確認する
クライアントのPIMデータの整合性テストを実施し、iCal UIDの重複や空の要求フィールドといった、同期を妨げているものがないかどうかを確認します。この全体設定はデフォルトで無効になっています。

クライアントオプション

プロトコル制限を強制する
クライアントで許可されているプロトコルバージョン以外のアクセスを拒否する場合はこのオプションを有効にします。デフォルトでこのオプションは無効になっており、プロトコル制限は異なるプロトコルのクライアントを拒否していません。プロトコル制限は単純に、クライアントに対して使用するべきプロトコルを伝えるのみの機能を提供しています。クライアントがそれでも制限されているプロトコルを使った場合、MDaemonはその接続を受け入れます。詳細は次のページをご覧下さい: プロトコル制限 395

Get/UserInformationへの応答でログオンエイリアスを'PrimarySmtpAddress' として使用する
サービスがSettings/Get/UserInformationリクエストに対する応答としてエイリアスやセカンダリアドレスをプライマリアドレスとして利用できるようにします。これはiOS 9.xへアップデートした際エイリアスからメールを送信できなくなった事に対する対処です。このオプションによって使用に反した応答を受け取る場合があります。

新しいクライアントは管理者の承認が必要
新しいクライアントがアカウントとの同期を開始する前に、管理者による承認を必要とする場合はこのオプションを有効にします。 クライアント 422 一覧で認証待ちのクライアントが確認でき、管理者

は同じ画面から承認が行えます。この設定はデフォルトで無効になっています。

ユーザー毎の最大クライアント
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域リセット日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

セキュリティ

ロケーションスクリーンから除外する
ActiveSyncクライアント設定で端末をロケーションスクリーニング[520]から除外する場合はこのオプションを有効化します。これにより認証済ユーザーは、例えば認証がブロックされている場所へ出張しているような場合であっても、ActiveSync経由でアカウントへアクセスする事ができるようになります。端末を除外するためには、チューニング画面にあるこの日数を超えて認証されなかった端末を自動削除[381]設定の時間内に、ActiveSyncを使った接続と認証を行っておく必要があります。

リモートアドレスを動的に除外
接続元のリモートIPアドレスをロケーションスクリーニングの除外リストへ追加する事ができます。このオプションは、同じIPアドレスを使って接続する他のクライアントがある場合に便利です。

ユーザー毎の最大クライアント数
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域の統計情報をリセットする日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

他のサーバーで管理されているクライアントへの接続を許可する
デフォルトで、ActiveSyncサーバーが特定のクライアントへデータやポリシーを送信する際、対象クライアントが他のActiveSyncサーバーからも管理されている事が分かった場合も、クライアントはMDaemonへアクセスする事ができます。しかし、このような環境の場合、適用するポリシーが他のActiveSyncサーバーと競合する可能性があります。一般的に、クライアントはポリシーが競合した場合、厳しい方へ合わせる傾向があります。こうしたクライアントからの接続を制限する場合は、このオプションを無効化して下さい。

工場出荷時への完全ワイプを無効化
オン/はい、を設定すると、ActiveSyncクライアントの完全ワイプが行えなくなります。クライアントでリモートからの完全ワイプを許可する場合、最初にこのオプションを無効化して下さい。このオプションはデフォルトで無効に設定されています。クライアントページの次の項目を参照して下さい:
ActiveSyncクライアントの完全ワイプ 422

フォルダ同期オプション

フォルダ同期オプション

除外

ユーザの [許可リスト/ブロックリスト] フォルダ
デフォルトでユーザーの許可リストとブロックリストの連絡先フォルダは端末と同期を行いません。これらはMDaemonがスパムからシステムを自動的に保護するのを支援する目的で使用されます。そのため、許可リストやブロックリストは端末上に連絡先として表示する必要性はありません。

デフォルト以外のメールフォルダ
デフォルトで、ユーザーが作成したメールフォルダとデフォルトメールフォルダは全て端末と同期します。同期するのを受信箱や送信箱、削除済アイテム、下書き、といった、デフォルトのメールフォルダのみにしたい場合はこのオプションを有効にして下さい。ユーザーが作成したフォルダは同期対象に含まれません。 このオプションはデフォルトで無効になっています。

デフォルト以外のPIMフォルダ
デフォルトで、(連絡先、予定表、仕事などの) PIMフォルダは全て端末と同期します。同期するのをデフォルトのPIMフォルダのみにしたい場合はこのオプションを有効にして下さい。このオプションが有効な場合で、ユーザーが複数の予定表を保有してる場合デフォルトの予定表のみが同期対象となります。 このオプションはデフォルトで無効になっています。

含む

パブリックフォルダの階層
ユーザーがアクセス権を持っている パブリックフォルダ 283 をユーザーのActiveSync用端末のフォルダ一覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
パブリックフォルダ 283 をユーザーが検索できるようになります。 これはデフォルトで許可されています。

パブリックフォルダの横断 (フォルダ名の公開)
デフォルトで、クライアントがパブリックのサブフォルダへのアクセスや同期を行うには、サブフォルダと上位のパブリックフォルダ 283 全てに対してルックアップ権限 285 が必要です。上位のフォルダに対するアクセス権がない場合、その中のサブフォルダに対しては、例え設定上は許可されていても、アクセスする事はできません。クライアントからこうしたサブフォルダへアクセスできるようにする場合は、このオプションを有効にします。注意点: このオプションを有効化すると、上位のフォルダもクライアントへ許可する事となり、セキュリティのリスクを招く恐れがあります。 このオプションはデフォルトで無効になっています。

許可するパブリックフォルダの最大数
端末で処理するパブリックフォルダ数を制限する場合はこのオプションを使用します。制限が設定されると、サーバーは最大数に到達するまでフォルダー一覧を処理し、これを超えるとその後のデータを送りません。処理するフォルダの順番を決める事はできません。デフォルトで、全体での最大数は設定されていません。

共有フォルダも含める

ユーザーがアクセス権を持っている 共有フォルダ[107] をユーザーのActiveSync用端末のフォルダー一覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
共有フォルダ[676] をユーザーが検索できるようになります。これはデフォルトで許可されています。

コンテンツ処理

コンテンツ処理オプション

クライアントにフラグ付けされたメール用にタスク・リマインダーを作成
このオプションでMDaemonはフラグが付いたアイテムごとに仕事を作成し、リマインダーをユーザーへ送信できるようになります。この設定の全体値はデフォルトで有効です。

予定を編集した際、常にミーティングのアップデートを送信
クライアントの中には、ミーティングを編集した際、更新情報を適切に送信しないものもあります。このオプションを使うとActiveSyncサービスへ、ミーティングが開催者によって更新された際、更新情報を送信するよう促す事ができるようになります。これはミーティングの更新情報の送信に失敗しているクライアント[422]やクライアントタイプ[438]に限定して使用するべきで、更新情報が重複して送られてしまう可能性があります。また、このオプションはクライアントとクライアントタイプの設定ページでのみ利用できます。

全ての送信メールで開封確認を要求
クライアントから送信される全てのメールで開封確認要求を行うにはこのオプションを有効にして下さい。これはデフォルトで無効になっています。

送信者からリクエストされた際送信済メールについて開封確認を送信
サーバー側で開封確認要求を検出し、既読フラグがついたメールの開封通知を送信するにはこのオプションを使用します。これはデフォルトで無効になっています。

ReplyToアドレスに指定したエイリアスとして送る
クライアントによっては、エイリアスを使ったメール送信を許可していません。この機能は Exchange ActiveSync（EAS）プロトコル[395] 16.xで追加されたものですが、クライアントの中には16.xに対応していないものもあります。例えば、Windows用OutlookはEAS 14.0だけを使用しており、ユーザーが関連するアドレスを指定して送信する事のみ許可しており、生成されたメールはユーザーの選択を正しく反映していません。このオプションでは、ReplyToのアドレスがユーザー用の正しいエイリアス[757]であれば、これを使ってメール送信を行います。この設定の全体値はデフォルトで有効です。

デフォルトの連絡先にパブリック連絡先を仮想的に統合する
パブリック連絡先をユーザーの端末上でデフォルトの連絡先と統合したい場合はこのオプションを有効にします。これは仮想的な統合で、実際には連絡先フォルダへデータのコピーは行っていません。これはグローバルアドレス帳（GAL）の検索機能に対応していないクライアントにとって便利な機能です。これはデフォルトで無効になっています。

Junk-Emailフォルダへ移動したメールの送信者をブロックする
有効にすると、クライアントが特定のメールを自分のJunk Emailフォルダへ移動した際、対象のメール送信者がブロックされた送信者連絡先フォルダへ追加されます。

ミーティング要求が許可/拒否された際、ミーティング要求に対する応答の送信を強制的に行う
このオプションを使用すると、クライアントがミーティング要求に対して、許可や拒否、その他のアクションを選択した際、ミーティング要求に対する応答を開催者へ送信します。これは、こうした更新情報を自動送信する事ができない特定のクライアント用の機能です。

有効な設定をプレビュー
このボタンは全てのクライアント設定（ドメイン397, アカウント413, クライアント422）に対して使用できます。画面のオプションはデフォルト値をその上位の画面から引き継いでいるため、この機能は表示されている画面の現在の設定確認を行う際にもご利用頂けます。

参照:

ActiveSync ≫ アカウント413
ActiveSync ≫ セキュリティ391

3.3 ゲートウェイマネージャ

ゲートウェイマネージャは 設定 ≫ ゲートウェイマネージャメニューからアクセスできます。 多少の制限はありますが、セカンダリレベルでの複数ドメインのホスティングに対応したり、バックアップメールサーバとして動作させる場合に便利です。

例えば:

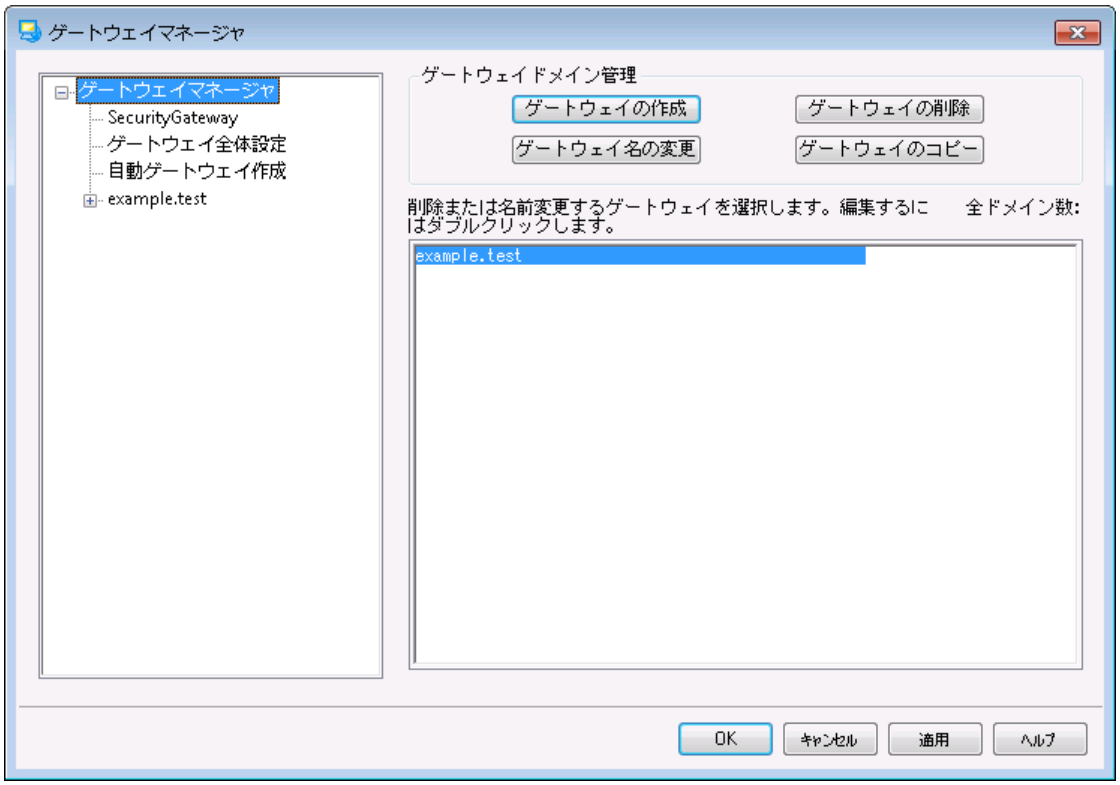
サードパーティー製品のバックアップサーバーや、受信メールの保存は行うものの、ドメイン全体の管理や、個々のユーザーアカウントは持たないメールドロップとして動作すると仮定します。"example.com"を使用します。

最初に行うことは、ゲートウェイマネージャの新しいゲートウェイをクリックし、"example.com"と入力することでゲートウェイを作成する事です。これで対象ドメイン宛のメールはメインのメールストリームから切り離され、メールの個々の宛先に依らず、ゲートウェイのドメイン234で指定されたフォルダへ保管されます。

次に、実際のユーザーアカウントを管理しているドメインのメールサーバーへ、ドメイン宛のメールをどのように収集したり配送したりするかを決定します。これには2通りの方法があります。1つはドメイン画面[234]のリモートメールを処理するたびに、保存メッセージを配信するオプションを使用する方法、もう1つはデキュー[240]オプションを使う方法です。また、MDaemonアカウントを作成し、アカウント毎のメールフォルダ[653]をゲートウェイと同じストレージフォルダ[234]へ変更する方法もあります。これで、MDaemonを経由して、メーラーからMDeamonへメールを収集しに行くことができます。

最後に、MDaemonサーバが、ドメインのMXホストとなるよう、example.comのDNSを設定しておく必要があります。

他にも様々なオプションや機能がありますが、上記の例は一般的なゲートウェイを実装する際の基本的なものです。ただ、例えば「company.mail」のような実在しないドメイン名を使う場合など、上記とは異なる構成となる場合、必要な設定も上記とは異なります。無効なドメイン名でのメール受信は可能ではありますが、ドメイン名はデフォルトドメイン[165]アドレスに「隠れた」状態である必要があります。この方法であれば、デフォルトドメインから受け取ったメールをゲートウェイへ配送する事ができます。例えば、デフォルトドメインがexample.comで、ゲートウェイがcompany.mailだった場合、bob{company.mail}@example.comを使ってbob@company.mailへメールを送る事ができます。example.comがMDaemonが管理する登録済ドメインであれば、このメールは正しく配送されますが、MDaemonが先ほどのフォーマットでメールを受け取ると、アドレスをbob@company.mailへ変換した上でゲートウェイ用のフォルダへ配送を行います。もちろん、最も簡単な方法は正しいドメイン名をゲートウェイへ割り当て、example.comのDNSやMXレコードを設定する事です。



ゲートウェイ一覧

ダイアログの左側にあるナビゲーションでは、ゲートウェイの一覧が確認でき、ここからゲートウェイ毎の様々な設定画面へアクセスできます。ここからは、ゲートウェイ全体設定[230]や自動ゲートウェイ作

成 232へもアクセスできます。右側の一覧はドメインの削除や名称変更に使用します。一覧からゲートウェイをダブルクリックし、それぞれの設定画面へ切り替える事ができます。

ゲートウェイドメイン管理

ゲートウェイの作成
ゲートウェイを作成するには **ゲートウェイの作成** をクリックし、ゲートウェイの名称（例えばexample.mail）を入力し、OKをクリックします。

ここで入力する値はDNSでサーバーが稼働しているマシンとIPアドレスの名前解決ができる登録済のドメイン名が一般的ですが、（例えばcompany.mailといった）社内でのみ使用しているドメインや非公開のドメインを、ゲートウェイの名称として使用する事もできます。ただし、その場合は、上記の例のように、ドメインに関連付いたメールが正しく配信されるよう、各種設定変更が必要となる場合があります。

ゲートウェイの削除
ゲートウェイを削除するには、一覧から対象のゲートウェイを選択し **ゲートウェイの削除** をクリックし、確認画面で「はい」を選択します。

ゲートウェイ名の変更
ゲートウェイの名前を変更するには、一覧から対象のゲートウェイを選択し **ゲートウェイ名の変更** で、ドメインの作成/編集ダイアログへ新しい名前を入力し、OKをクリックします。

ゲートウェイのコピー
ゲートウェイを他のゲートウェイと同じ設定で作成するには、対象のゲートウェイを選択しこのボタンをクリックし、ゲートウェイ名を指定します。

ゲートウェイエディタ
ゲートウェイエディタでは各ゲートウェイの設定編集が行え、次の設定画面が含まれています。

ドメイン 234
ゲートウェイの有効化や無効化、ドメインメールを保存するフォルダの指定、その他の配信や添付ファイルの処理に関する設定が行えます。

検証 235
外部のドメイン用サーバーがLDAPやActive Directoryサーバーでメールボックスやエイリアス、メーリングリストの情報を最新の状態にしていた場合や、Mingerサーバーで外部のアドレス認証を行っていた場合、このダイアログでサーバーを指定し、受信メールの宛先アドレスの検証を行う事ができます。宛先アドレスが無効なものだった場合、メールはその場で拒否されます。この方法で、ドメインに配信するメールの宛先が正しいかどうかに依らず、全て受信してしまう状況を避ける事ができます。

転送 238
ドメイン宛のメールを転送する先となるホストやアドレスを指定します。メールのコピーをローカルに残すかどうかや転送するメールの送信先ポートの設定もここで行えます。

デキュー 240
ここではMDaemonのドメインのメールをすぐに配送するために送られるETRNやATRN要求に対する応答の設定が行えます。デキューに関連したその他オプションもここから設定が行えます。

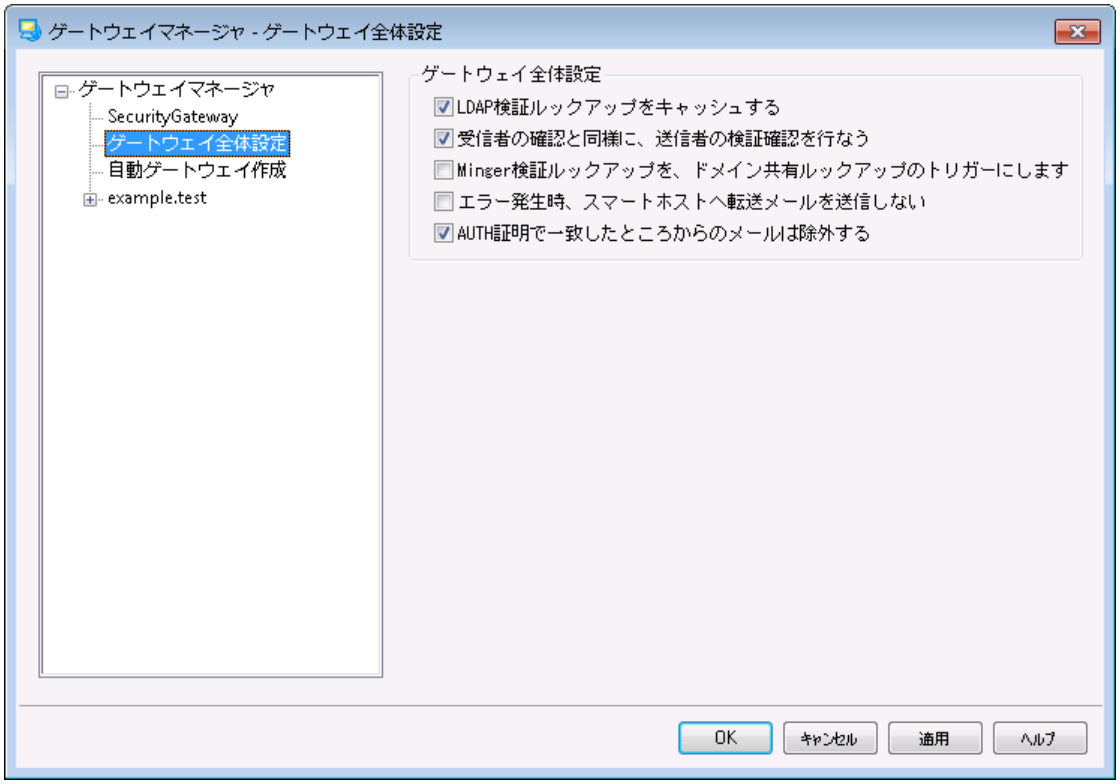
クォータ 243
ドメインに割り当てる最大ディスク容量や最大メール本数の制限が行えます。

設定 244
対象のドメインゲートウェイに適用する各種設定が行えます。例えば、アンチウィルスやアンチスパムの有効化や無効化、メールをキューから取り出す際に認証を要求するかどうか、認証パスワード、その他の設定がここで行えます。

参照:

ゲートウェイ全体設定 230
自動ゲートウェイ作成 232
ドメインマネージャ 165

3.3.1 ゲートウェイ全体設定



ゲートウェイ全体設定

以下は全体オプションで、特定のゲートウェイに限定した設定ではありません。

LDAP検証ルックアップをキャッシュする
LDAP検証 235 の結果をドメインゲートウェイ用にキャッシュするにはこのオプションを有効にします。

受信者の確認と同様に、送信者の検証確認を行う
デフォルトで、アドレス検証オプション[235]はゲートウェイが有効になっていると、MDaemonはゲートウェイメッセージの受信者と送信者を検証します。受信者のみを検証するにはこのオプションを無効化して下さい。

Minger検証ルックアップをドメイン共有ルックアップのトリガーにします
このオプションが有効で Minger[785] がゲートウェイでアドレス検証に使用されていた場合、Mingerで検証[235]を行うタイミングで、ドメイン共有[103]用にも問合せを行います。このオプションはMingerを使用している全てのゲートウェイに対して適用されます。

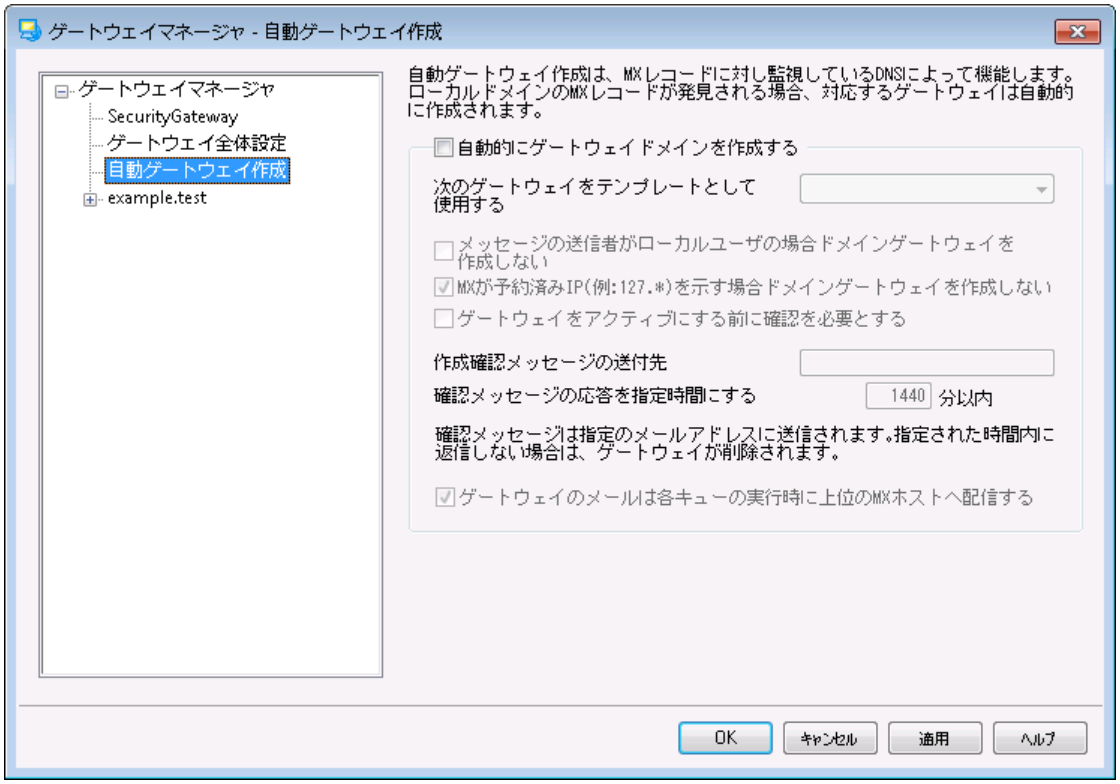
エラー発生時スマートホストへ転送メールを送信しない
配信エラーが発生した際転送メールの送信を禁止するにはこのオプションを有効化します。このオプションはデフォルトで無効になっています。

AUTH証明で一致したところからのメールは除外する
デフォルトでゲートウェイメールはSMTP認証[476]画面の「認証情報はreturn-pathアドレスとの一致が必要」「認証情報はFrom:ヘッダアドレスとの一致が必要」の2つのオプションからは除外されます。ゲートウェイメールをこれらの要件から除外しない場合はこのオプションを無効化して下さい。ただし、これを無効化する事でゲートウェイメールのストレージや転送に問題が生じる可能性があります。

参照:

ゲートウェイマネージャ[227]
ゲートウェイエディタ » 検証[235]
Minger[785]
ドメイン共有[103]

3.3.2 自動ゲートウェイ作成



自動ゲートウェイ作成

この機能は、他のソースからドメイン宛のメールがMDaemonに配送されて来た場合に、MDaemonからのDNSサーバーへの問合せで、自身が正しいMXレコードとして認識できた際、登録のないドメインのゲートウェイを自動作成するための機能です。

例えば、

自動ゲートウェイ作成機能が有効で、MDaemonのデフォルトドメインのIPアドレスが[192.0.2.0]の時、登録のないexample.comドメイン宛のメールがSMTPで配送されてきたとします。この時MDaemonは[example.com]のMXレコードとAレコードを参照し、[192.0.2.0]が、リレーホストとして認識されているのかどうかを確認します。DNSを参照した結果、MDaemonのIPアドレスが[example.com]用の正しいMXホストである事が確認できると、MDaemonは自動的に新しいドメインゲートウェイを作成し、対象ドメイン宛のメールを受け付けるようになります。[example.com]宛てのメールは特別なフォルダに格納され、設定によっては、リモートメールの処理毎に、上位のMXホストへ配信を行います。この機能を使うと、DNSへMDaemonのIPアドレスを代替MXホストとして登録するだけで、効率的にMDaemonを他のドメインのバックアップサーバーとして利用できるようになります。

この機能の安全性を高めるため、MDaemonは任意のメールアドレスに確認リクエストを送るよう設定する事もできます。確認リクエストの応答を待っている間、対象ドメイン宛てのメールの受付と格納は行いますが、配信は行いません。確認リクエストは指定時間内に返信しなくてはならず、返信がない場合、自動作成したゲートウェイは削除され、格納済のメールも全て削除されます。確認リクエストに対する返信を受信した場合は、格納済メールは通常通り配信されます。

悪意のあるユーザやスパマーが、DNSサーバーへMDaemonのIPアドレスをMXホストの1つとして登録し、この機能を悪用する可能性があります。そのため、自動ゲートウェイ作成を使用する際には注意が必要です。不正利用の防ぐ方法の1つとして**作成確認メッセージの送付先...**機能を、できるだけ利用することを推奨します。

自動的にゲートウェイドメインを作成する
DNSクエリの結果に基づいて、ドメインゲートウェイを自動的に作成する場合は、このチェックボックスを選択してください。

次のゲートウェイをテンプレートとして使用する
ドロップダウンリストからドメインゲートウェイを選択すると、今後自動作成するすべてのゲートウェイは、このドメインゲートウェイの設定をテンプレートとして使用します。

メッセージの送信者がローカルユーザーの場合はドメインゲートウェイを作成しない
ローカルユーザからのメールによって、ゲートウェイが自動作成されるのを防ぐには、この設定を有効にしてください。

MXが予約されたIPを示す場合ドメインゲートウェイを作成しない
MXレコードが[127.*]や[192.*]などの予約済IPに関連付けされていた場合に、ゲートウェイが自動作成されるのを防ぐには、この設定を有効にしてください。

ゲートウェイをアクティブにする前に確認を必要とする
この設定が有効な場合、MDaemonは、自動的に作成されたゲートウェイが有効であるかどうかを確認するためのメールを選択されたアドレスに送信します。MDaemonは確認中もメールを受け入れ続けますが、確認が取れるまではそのメールを配信しません。

作成確認メッセージの送付先
このテキストボックスには、確認メッセージを送信するアドレスを入力してください。

確認メッセージの応答を指定時間にする
MDaemonが確認メッセージの応答を待つ時間(分)を指定してください。この制限時間が経過するとドメインゲートウェイは削除されます。

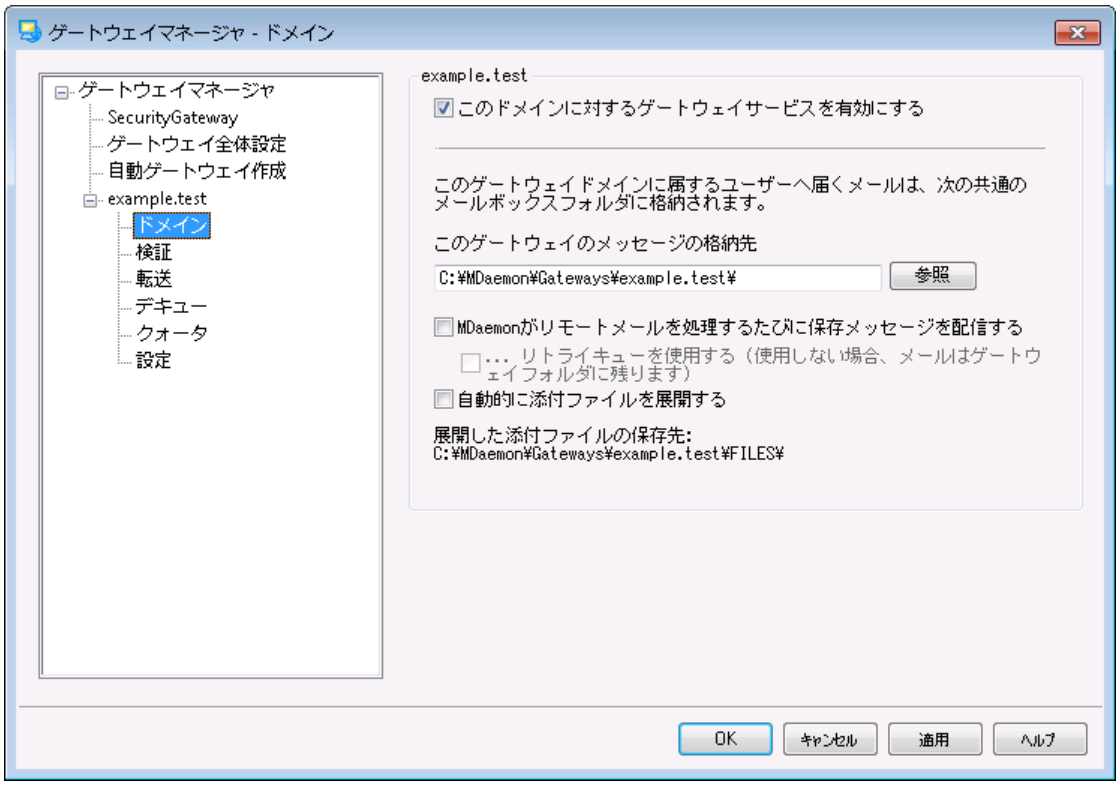
ゲートウェイのメールは各キューの実行時に上位のMXのホストへ配信する
リモートキューが処理されるたびに、このゲートウェイのメールを上位のMXホストへ送信する場合は、この設定を有効にしてください。

参照:

ゲートウェイマネージャ 227

3.3.3 ゲートウェイエディタ

3.3.3.1 ドメイン



ゲート ウェイド メイン

ゲート ウェイサービスを有 効 にする
ドメインゲート ウェイを有 効 化 します。

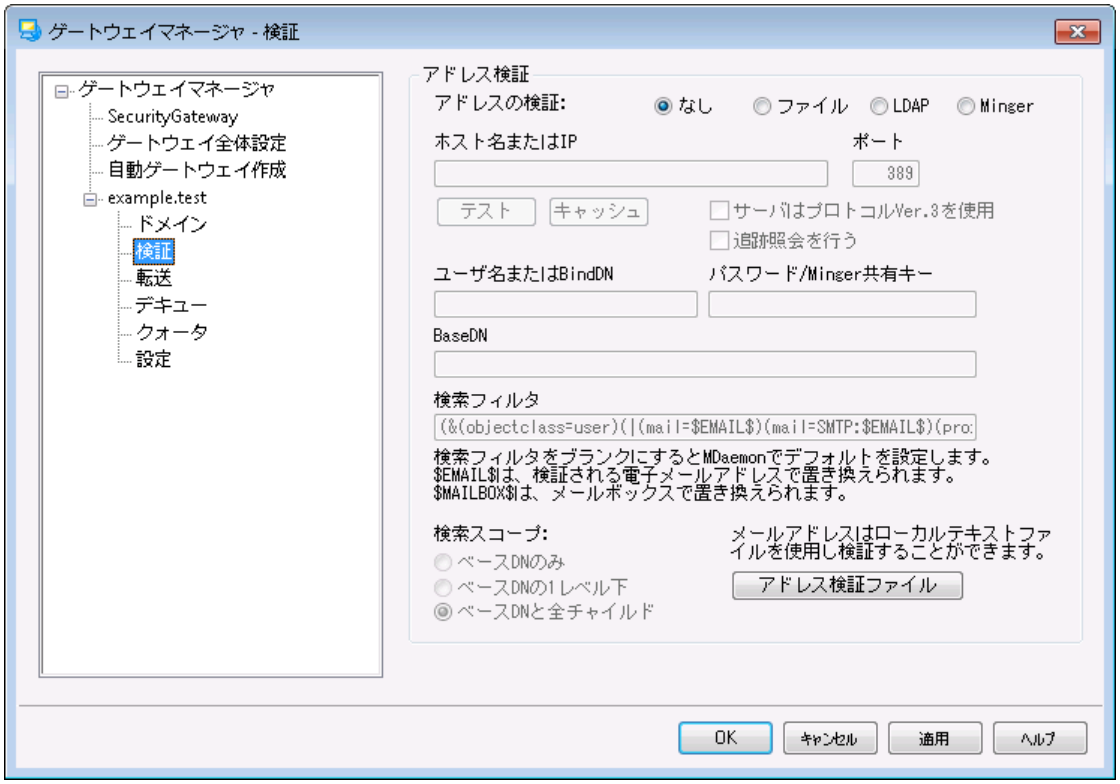
ゲート ウェイド メイン用 メールの格 納 先 :
ドメイン用 の受 信 メールを格 納 するディレクト リを入 力 します。全 てのメールは各 メールが個 人 宛 かどうかに関 わらず、このフォルダへ格 納 されます。

MDaemonがリモート メールを処 理 するたびに保 存 メッセージを配 信 する
通 常 、MDaemonがゲート ウェイとして対 象 となるメールを受 信 すると、ドメインのメールシステムがMDaemonからメールを収 集 するまでの間 、メールはMDaemonが保 持 します。環 境 によっては、メールの収 集 を待 つよりもSMTPでメールを直 接 配 信 させたい場 合 があります。このオプションを有 効 にすると、リモート メールの処 理 を行 う度 に、MDaemonがドメインのメール配 信 を行 います。ゲート ウェイのメールボックスは一 時 的 にリモート キューとして配 信 処 理 されます。配 信 できないメールは、メールが収 集 されるか、正 常 に配 信 されるまでゲート ウェイのメールボックスに残 り、リモート キューやリト ライシステムへは移 動 しません。ただし、ドメインのDNSが正 しく設 定 されていなかったり、全 ての送 信 メールを他 のホスト へ配 信 するよう設 定 を行 っていた場 合 、こうしたメールがループに陥 る場 合 があり、結果 、これらのメールは配 信 できないメールとして扱 われます。

リトライキューを使用する（又はメールをゲートウェイフォルダへ保持）
メール配信に リトライキュー[794] のメカニズムを使用するにはこのオプションを使用します。これはデフォルトで無効になっており、ゲートウェイメールは配信できないものであってもゲートウェイフォルダへ永久に保持されます。

添付ファイルを自動的に取り出す
メールシステムによっては、メール配信の前に添付ファイルの展開を求める場合があります。これに対応するため、MDaemonには受信したMIMEメールの添付ファイルを自動展開し、それをドメイン用メールフォルダのサブディレクトリである¥Files¥ディレクトリに保存する機能を搭載しています。自動的に添付ファイルを展開するにはこのチェックボックスをクリックします。

3.3.3.2 検証



一般的に、ドメインゲートウェイやメールドロップの抱える問題の1つは、メール受信者のアドレス検証を行う方法がないという点です。例えば、example.comのゲートウェイとして稼働しているシステムに対して、user01@example.com宛のメッセージが届いた場合に、example.comのメールサーバ上に、実際にそのアドレス、エイリアスまたはメーリングリストが存在するかどうかを知る事はできません。したがって、アドレスが有効であると仮定してメッセージを受け入れるほかありません。さらに、通常スパマーは無効なアドレスに大量のメールを送信してきますので、結果的に、ゲートウェイ側で大量のスパムメールを受信してしまうという状態になります。

MDaemonは、こうした問題を防ぐために、受信メールのアドレスを検証する事ができます。外部のドメイン用サーバーがLDAPやActive Directoryサーバーでメールボックスやエイリアス、メーリングリストの情報を最新の状態にしていた場合や、Mingerサーバーで外部のアドレス認証を行っていた場合、MDaemonでもLDAPやAD、Mingerサーバーを指定し、今後example.com宛てのメールが到着した際、宛先アドレスの問合せを指定したサーバーに対して行う事ができます。

アドレス検証

アドレスの検証:

なし
ドメインゲートウェイに対してアドレス検証を使用しない場合は、このオプションを選択します。MDaemonは、ドメインのアドレスが実在するかどうかを判定できないため、アドレスは有効なものという前提で、全ての受信メールを処理します。

ファイル
受信メールの宛先が有効かどうかを検証するのに、GatewayUsers.datファイルのリストを使用する場合は、このオプションを選択します。これは、全アドレスの一覧で、全てのドメインゲートウェイで使用でき、他の検証方法を選択した場合であっても、追加の検証用ソースとして利用する事ができます。ただし、ファイルオプションを選択した場合、これが唯一の検証用オプションとなります。下記の[**アドレス検証ファイル**]ボタンをクリックすることによって、有効なアドレスリストを開き編集することができます。

LDAP
LDAPやActive Directoryサーバー経由でリモートでのアドレス検証を行う場合は、このオプションを選択します。メールが届くたびに、LDAPやActive Directoryサーバが宛先アドレスが有効かどうかの問合せを行い、有効でないアドレス宛のメールは拒否されます。MDaemonがLDAP/ADサーバに接続することができない場合は、アドレスは有効であるものとして処理します。

Minger
宛先アドレスの検証にMingerサーバを使用するにはこのオプションを選択します。MDaemonがサーバに接続することができない場合は、アドレスは有効であるものとして処理します。ドメイン共有 103ホストに対する問合せも同時に行うためのオプションも、ゲートウェイ全体設定 230画面で選択できます。

ホスト名またはIP
ドメインのLDAP/Active DirectoryまたはMingerサーバのホスト名またはIPアドレスを入力します。これは、MDaemonが受信メールの宛先アドレスの検証を行うために接続するLDAP/AD又はMingerサーバーです。

ポート
ドメインのLDAP/ADまたはMingerサーバが使用しているポートを指定します。LDAP、Active DirectoryまたはMingerへアドレス検証を行う際、MDaemonがこのポートを使用します。

テスト
アドレス検証の設定が正しく行われているかどうかをテストするのに、このボタンをクリックします。MDaemonは指定されたLDAP/ADへ接続し、特定の情報に対する応答内容を検証します。

キャッシュ
LDAP/Mingerキャッシュを開くために、このボタンをクリックします。ゲートウェイ全体設定 230でキャッシュを有効/無効にすることができます。

サーバーはプロトコルバージョン3を使用
ゲートウェイ検証でLDAPプロトコルバージョン3を使用する場合はこのチェックボックスをクリックして下さい。

追跡照会を行う
LDAPサーバーが必要なオブジェクトを所有してはいないものの、クライアントからロケーションを参照する事ができる場合があります。ゲートウェイ検証でこうした照会情報を追跡するにはこのオプションを有効化して下さい。このオプションはデフォルトで無効に設定されています。

ユーザ名またはBindDN
ドメインのLDAP/ADサーバに対して管理者権限を持つアカウントのユーザー名又はDNを入力することで、受信メールの宛先アドレス検証を行うことができます。これは、バインド操作で認証のために使用されるDNです。

パスワード/Minger共有キー
LDAPもしくはActive Directoryへ、認証用のBind DNとあわせて送信されるパスワードを設定します。Mingerの場合は、共有キー又はパスワードを指定します。

BaseDN
識別名(DN)や、MDaemonがアドレス検証をLDAP/ADサーバに行う際使用するディレクトリ情報ツリー(DIT)のルートポイントを指定します。

検索フィルタ
アドレス検証に用いられるLDAP/AD検索フィルタです。MDaemonには、ほとんどの環境で使用できるデフォルトの検索フィルタが設定されています。

検索スコープ:

LDAP/ADの検索範囲は次の通りです。

ベースDNのみ
検索を上記で指定されるベースDNだけに制限する場合、このオプションを選択します。検索は、ツリー(DIT)をその位置より下に続行しません。

ベースDNの1レベル下
DITで提供されたDNより1レベル下にLDAP/AD検索を与える場合、このオプションを使用します。

ベースDNとすべてのチャイルド
このオプションは、DITで最も小さいチャイルドエントリまで、提供されたDNからチルドレンの全部まで検索の範囲を拡大します。

アドレス検証ファイル
ゲートウェイ有効メールアドレスリスト(GatewayUsers.dat)を開くのに、このボタンをクリックします。受信メールのアドレス検証を行う際、MDaemonはここで指定されているアドレスを有効なアドレスとして取り扱います。上記のどの検証方法を選択した場合であっても、このファイルは追加の検証用ソースとして利用する事ができます。ただし、ファイルオプションを選択した場合、これが唯一の検証用オプションとなります。

LDAP検証用クエリに複数の設定を使用する

ゲートウェイドメインに対して、複数のLDAP設定を指定することができます。LDAPパラメータとして特別な設定を行う場合は、まずはLDAP設定を通常通りに行い、それからエディタを使ってGATEWAYS.DATファイルを手動で編集します。

パラメータのセットは、次のフォーマットで作成します:

LDAPHost1=<host name>
LDAPPort1=<port>
LDAPBaseEntry1=<base entry DN>
LDAPRootDN1=<root DN>
LDAPObjectClass1=USER
LDAPRootPass1=<password>
LDAPMailAttribute1=mail

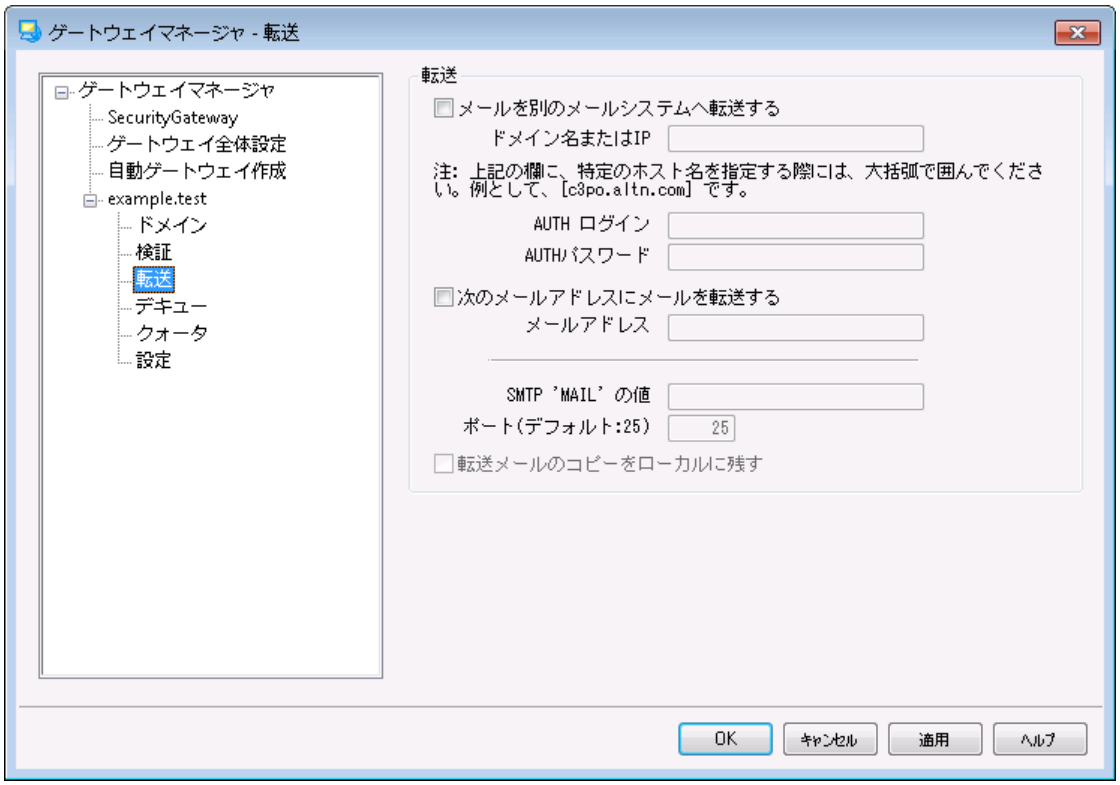
パラメータセット毎に、上記の数字を1から順に増やしていきます。例えば上記のサンプルで、各パラメータ名は1で終わっています。追加でパラメーターセットを指定する場合は数字の1を2に変更し、更に追加する場合はこれを3にします。

LDAPが検証を行う際、MDaemonは複数のLDAPサーバーへ同時に検証を行います。途中でエラーの発生や検索結果にマッチした場合には、その後の検証は行いません。

参照:

LDAP/アドレス帳オプション 754
Minger 785

3.3.3.3 転送



転送

別のメールシステムへメールを転送する
ドメインへ到着したすべてのメールのコピーを転送するのが都合の良い場合があります。この転送を行うようにMDaemonを構成するには、この受信メールのコピーを送信するドメインの名前またはIPアドレスを入力してください。メールを特定のホストに転送する場合は、カギカッコでホスト名を指定してください(例:[host1.example.net])。メールの転送に必要な認証情報をAUTHログイン/パスワードオプションにて指定してください。

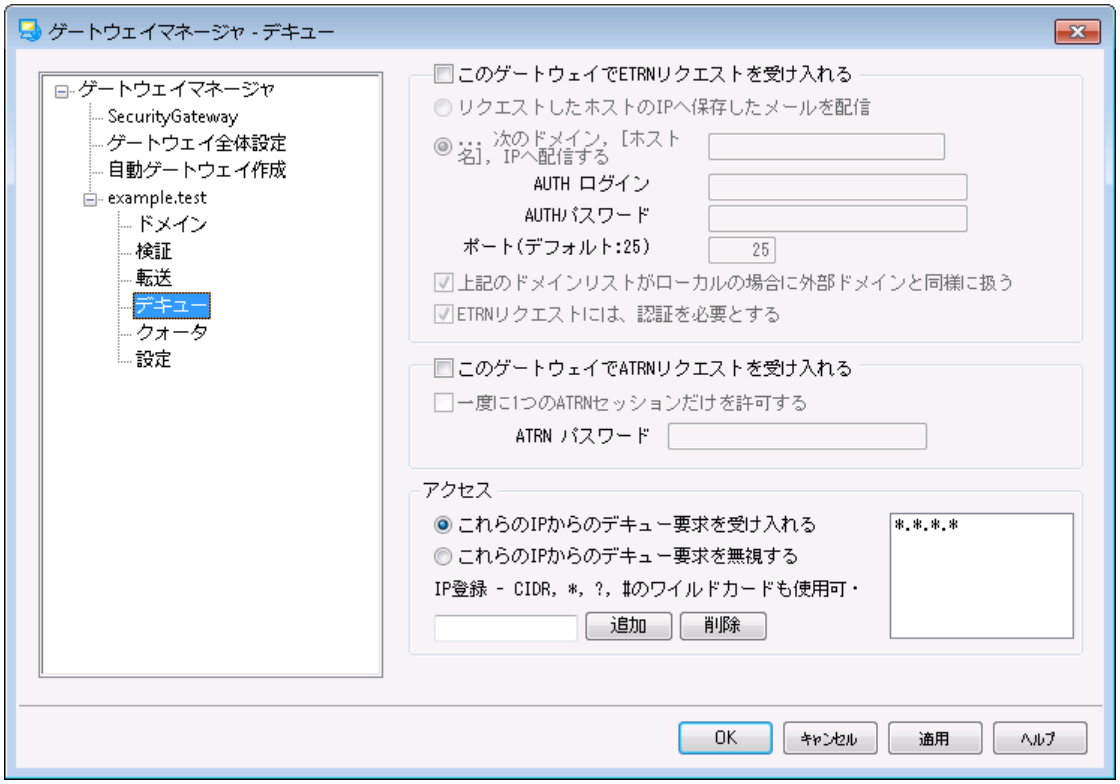
メールアドレスへメールを転送する
このクライアントドメイン宛てのすべてのメールを特定のメールアドレスへ転送する場合に、この機能を使用してください。

SMTP 'MAIL'の値
MDaemon はメール転送の際、SMTPの "Mail From" としてこの値を使用します。

使用するTCPポート (デフォルト = 25)
MDaemon はメール転送の際、このポートを使用します。

転送メールのコピーをローカルに残す
デフォルトで、転送されたメール毎のコピーは、ローカルユーザのメールボックスに通常配信されます。このチェックボックスを選択しないと、ローカルコピーは保持されません。

3.3.3.4 デキュー



ETRN

このゲートウェイでETRNリクエストを受け入れる
このスイッチを有効にする場合、MDaemonはメールゲートウェイとして実行しているドメインに代わり、特定のホストからのETRNリクエストに応答します。
ETRNコマンドは、ドメインのメールを保留するサーバへ、そのメールのスプールを開始する時が来たことを通知するSMTPの拡張命令です。MDaemonがドメインのETRNリクエストを受信すると、直ちに以降のSMTP処理を使用して配信のために格納されたメールをスプールし始めます。ETRNリクエストを発行するSMTPセッションが格納されたメールを受信するものでないない点に注意をしてください。MDaemonは、後に続く独立したSMTP処理を使用して、そのドメインに保留していたメールを送信します。これはメッセージエンベロープを保護するので、より安全な方法です。またMDaemonが格納されたメールをスプールするホストで、これらのメッセージの受信を直ちに開始しない点に注意をします。ETRNは保留されたメールが配信のためにスプールされることのみを保証します。実際の配信処理は他の管理者が設定した制限に従い、次回に予定されているリモートメール処理が行われるまで、送信メールキューで待機しなければならない場合があります。これらの制限があるので、ETRNよりもOn-Demand Mail Relay (ODMR) 183とそのATRNコマンドを使用することをお勧めします。しかしながら、この方法はすべてのクライアントとサーバによってサポートされるわけではなく、上記の方法を使用するサーバのクライアントドメインのみで利用可能になります。MDaemonは、クライアントとサーバの両方でODMRを完全にサポートしています。

デフォルトで、MDaemonは接続するホストがETRN要求を発行した場合、最初にドメイン名 234とゲートウェイAUTHパスワード 244を使用して、接続ホストのESMTP認証を行います。認証を行わない場合、設定 244で

> *ATRN*デキューは認証が必要を解除することで無効にすることができます。

リクエストしたホストのIPへ保存したメールを配信
このオプションを選択すると、ETRNリクエストを行ったマシンのIPアドレスに格納されたメールを送信します。リクエストを行っているマシンでは、これらのメールを受け取るためにSMTPサーバが実行されている必要があります。

このドメイン、[ホスト]又はIPへ保存したメールを配信
これは、ETRNリクエストが受け入れられた時に、格納されていたメールが送信されるホスト名、ドメイン名またはIPアドレスです。このマシンでは、これらのメールを受け取るためにSMTPサーバが実行されている必要があります。注意:このオプションでドメイン名が指定されている場合、配信中のDNS検索の結果によりAレコードとMXレコードが使用されます。メールを特定のホストに配信する場合は、カギカッコでホスト名を指定するか(例:[host1.example.net])、ドメイン名ではなくIPアドレスを指定してください。必要なAUTHログインとパスワードを入力してください。

ポート(デフォルト=25)
このボックスを使用して、ドメインのメールがスプールされるポートを指定してください。

上記のドメインリストがローカルの場合に外部ドメインと同様に扱う
ローカルのドメインに、それがリモートであるかのようにメールをスプールさせたい場合は、このコントロールを有効にしてください。

ETRNキュー解除は認証が必要
デキュー画面でESMTP ETRNリクエストを受け付けるよう設定していた場合、このオプションを使って接続ホストに対し、ESMTP AUTHコマンドを使った最初の認証を必須とするかどうかを指定します。このオプションを有効にしていた場合、「ATRNパスワード」で認証用パスワードの設定が必要です。

ETRNリクエストで認証を必須としない場合は、このオプションを無効にしてください。

ATRN

このゲートウェイでATRNリクエストを受け入れる
ゲートウェイドメインからのATRNコマンドに応答するにはこのオプションを有効にしてください。ATRNはOn-Demand Mail Relay (ODMR)[183]で使用されるESMTPコマンドで、現時点ではメールホスティングのための最良のリレー方法です。この方法がETRNやその他の方法より優れている点は、メールがデキューされる前に認証を必要とし、静的なIPアドレスを必要としない点にあります。静的IPが必要とされない理由は、MDaemonとクライアントドメインとの間のデータフローが即座にリバースされ、メールが新しい接続なしにスプールアウトされるからです。これはETRNのように、ETRNコマンドを送出した後に個別の接続を使用する方法よりも優れています。この方法では、オリジナルのSMTPエンベロープが保護されるので、動的IPを使ったクライアントドメインが、POP3またはDomainPOPを使用する事なくメールを収集できるようになります。

> ATRNではAUTHコマンドを使用したセッションが必要です。認証情報はゲートウェイエディタの設定[244]画面で指定する事ができます。

一度に1つのATRNセッションだけを許可する
一度にATRNセッションを一つだけ受け付ける場合は、このチェックボックスを有効にしてください。

ATRNパスワード
ATRNを使って対象ゲートウェイのメールをデキューする場合やETRNデキューには認証が必要オプションで認証が要求された場合、ゲートウェイのATRNパスワードをここで指定します。

The domain for which MDaemonがメールゲートウェイとして稼働しているドメインでは、ログオン名としてドメイン名を使用する必要があります。例えば、ドメインゲートウェイがexample.comでATRNによるデキューを行う場合、認証には、ログオンIDとしてexample.com、パスワードはここで指定したパスワードを使用する必要があります。

アクセス

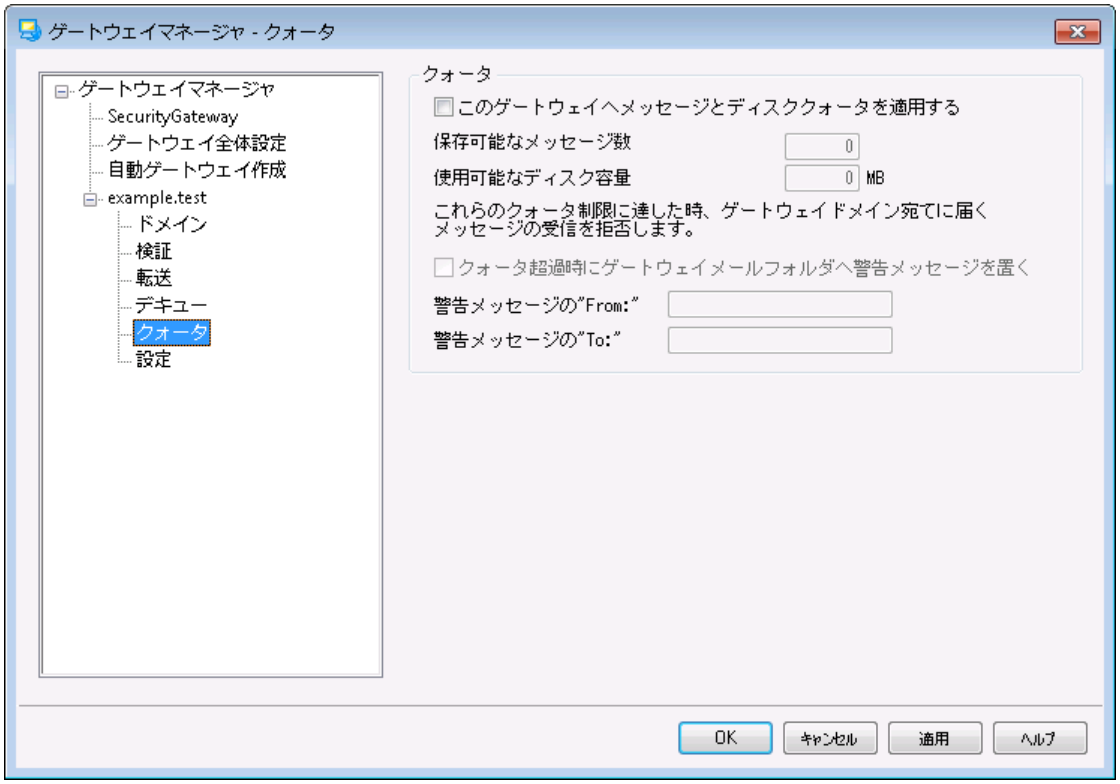
これらのIPからのデキュー要求を受け入れる
この設定でMDaemonは関連アドレス一覧にあるIPからのETRN/ATRNリクエストを受け付けます。

これらのIPからのデキュー要求を無視する
この設定でMDaemonは関連アドレス一覧にあるIPからのETRN/ATRNリクエストを無視します。

追加
現在の一覧にIPを追加するにはテキストボックスへIPを追加し、追加ボタンをクリックします。

削除
選択したエントリを一覧から削除する場合はこのボタンをクリックします。

3.3.3.5 クォータ



クォータ

このドメインへのメッセージとディスク容量クォータを適用する
このオプションを有効にすると、ドメインで保存できるメッセージの最大数または使用することが可能なディスク容量の上限を(キロバイトで)指定することができます。これにはファイルディレクトリにデコードされた添付ファイルのサイズも含まれます。クォータが上限に達すると、そのドメイン宛のそれ以降の受信メールはすべて拒否されます。

一度に保存できる最大メッセージ数
このゲートウェイドメインに対して保存することができるメッセージの最大数を指定するために、このオプションを使用します。オプションで0(ゼロ)をすると、メッセージ数の制限はありません。

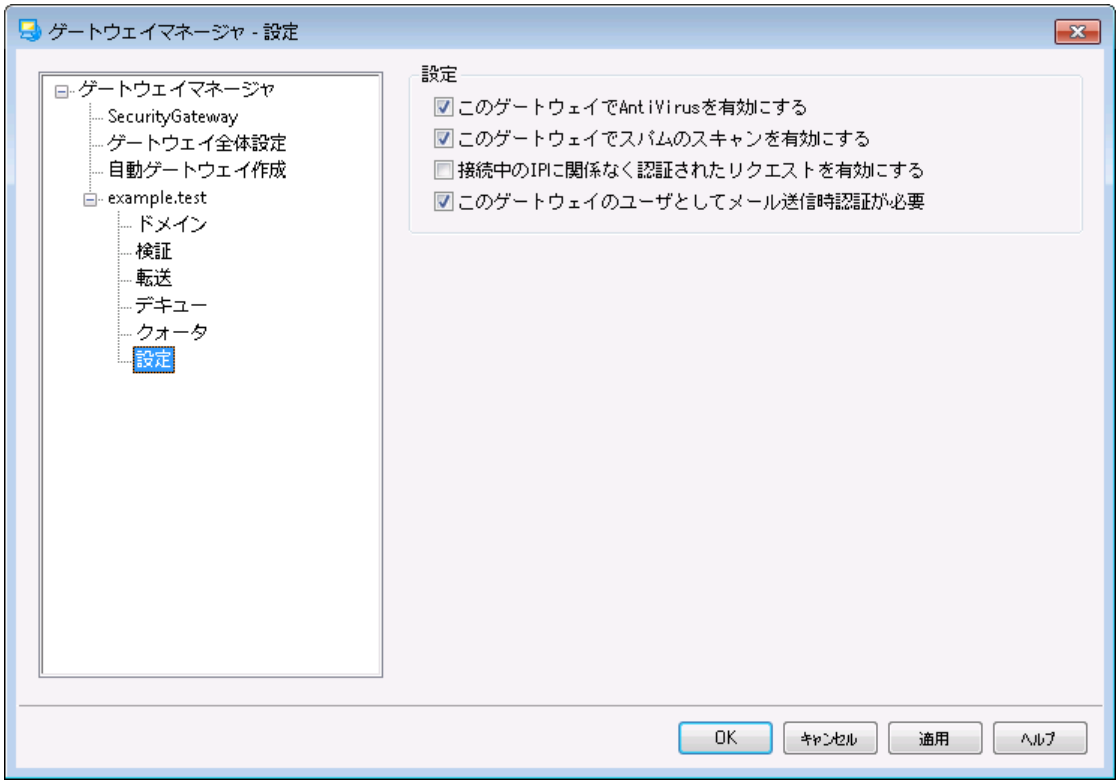
許可する最大ディスク容量
使用できるディクス容量の最大数をメガバイト単位で指定してください。メッセージやファイルの総容量がこの値に達すると、それ以降の受信メールはすべて遮断されます。オプションで0(ゼロ)をすると、メッセージ数の制限はありません。

クォータ超過時にゲートウェイメールフォルダへ警告メッセージを置く
このオプションが有効で、ドメインへ配信しようとしたメールが、割り当てられた最大メッセージ数または最大ディスク容量を超えた場合、しかるべき警告メッセージがドメインゲートウェイのメールフォルダに送られます。警告メッセージの"From"と"To"は、以下の説明のように指定することができます。

警告メッセージ "From:"
クォータ超過時の警告メッセージで使用される"From: "アドレスを指定するために、このオプションを使用します。

警告メッセージ "To:"
クォータ超過時の警告メッセージで使用される"To: "アドレスを指定するために、このオプションを使用します。

3.3.3.6 設定



設定

このゲートウェイでアンチウィルススキャンを有効にする
MDaemon AntiVirus 587を使っていて、このドメインゲートウェイのメッセージをスキャンする場合は、このオプションを有効にしてください。このオプションを無効にするとAntiVirusはこのゲートウェイのメッセージをスキャンしません。

このゲートウェイにアンチスパムスキャンを有効にする
このドメインゲートウェイのメッセージにスパムフィルタの設定を適用する場合は、このオプションを有効にしてください。このオプションを無効にするとそれらはスパムフィルタリングから除外されます。

認証されたリクエストは接続中のIPを問わず有効
どのIPアドレスからの認証リクエストでも受け入れるようにする場合は、このチェックボックスを有効にしてください。このコントロールが有効でない場合は、IPアドレスの項目で指定されるIPアドレスからのリクエストのみが受け入れられます。

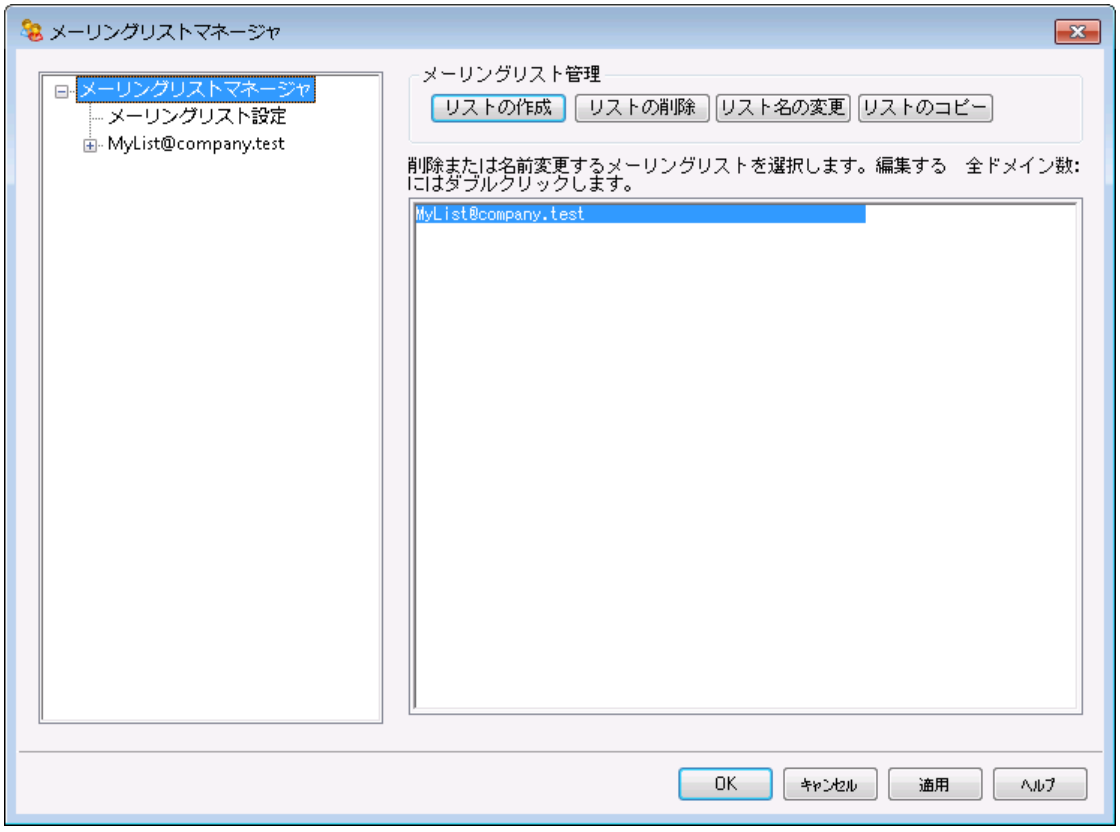
このゲートウェイのユーザとしてメール送信認証が必要
このドメインからのすべてのメールに対して認証を求める場合は、このオプションを有効にしてください。メールがこのドメインから送信されることが予想される場合、認証接続の使用か、信頼されたIPアドレスからの接続が必要となります。それ以外の場合はメールが遮断されます。このオプションはデフォルトで有効になっています。

新しいドメインゲートウェイが作成される際には、このオプションは自動的に有効になっています。このオプションを使用したくない場合は、MDaemon.iniファイルの以下のキーを編集して、デフォルト設定を変更してください。

[Special]
GatewaySendersMustAuth=No (デフォルトは Yes)

3.4 メーリングリストマネージャ

メーリングリストとは、メールグループや配布リストとも呼ばれ、あたかも1つのメールボックスを共有しているかのように動作する、複数のユーザで構成されるグループです。メーリングリストへ送信されるメールのコピーは、各メンバーに配布されます。メーリングリストには、ローカルやリモートのアドレスを含むことができ、公開または非公開、ダイジェスト 264 または普通のフォーマットのメールの送信など、様々な設定が行えます。



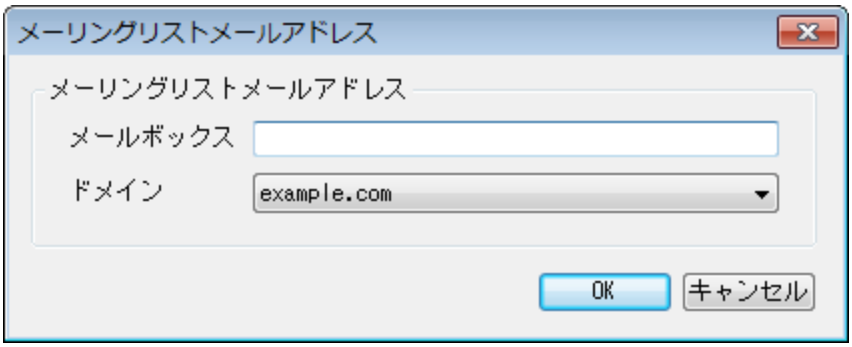
設定 ≫ メーリングリスト マネージャ... メニューを選 択 すると、メーリングリストを管 理 するためのメーリングリ スト マネージャ が利 用 できるようになります。

メーリングリストの管 理

ダイアログの左 側 にあるダイアログにはメーリングリスト 毎 のエントリが一 覧 表 示 されており、メーリングリス ト 毎 の詳 細 設 定 ページへのリンクになっています。ここから メーリングリスト 設 定 248 へもアクセスする事 が でき、ここではメーリングリスト に関 連 する全 体 設 定 が行 えます。ダイアログの右 側 はメーリングリスト の作 成 や削 除 、名 称 変 更 を行うのに使 用 できます。メーリングリスト 名 をダブルクリックすると、メーリングリスト の設 定 を行うための、メーリングリスト エディタが起 動 します。

リスト の作 成

新 しくメーリングリストを作 成 するには, リスト の作 成 をクリックし、メーリングリスト アドレスダイアログを 起 動 します。"MyList"といったメールボックス名 を作 成 し、"example.com"のようなドメインを選 択 し ます。 これはメーリングリスト のメールアドレス(例: MyList@ example.com)となります。このアドレス 宛 のメールは、設 定 に基 づきメーリングリスト のメンバーに配 布 されます。OKをクリックしてメーリングリ スト を作 成 します。作 成 した後 にエントリをダブルクリックすると、メーリングリスト の設 定 やメンバーの 追 加 が行 えます。注 意 点: メーリングリスト 名 には"! " や "| "は使 用 できません。



リスト の削 除

メーリングリストを削 除 するには、メーリングリストを選 択 し、**リスト の削 除** をクリックし、確 認 画 面 で **はい**をクリックします。

リスト 名 の変 更

メーリングリスト 名 を変 更 するには、メーリングリストを選 択 し、**リスト 名 の変 更** をクリックし、メーリング リスト アドレス画 面 で必 要 な変 更 を行った後 、OKをクリックします。

リスト のコピー

メーリングリストを他 のメーリングリスト と同 じ設 定 とメンバーで作 成 するには、対 象 のメーリングリスト を選 択 しこのボタンをクリックし、メーリングリスト 用 のメールボックス名 とドメイン名 を指 定 します。

メーリングリスト の設 定

メーリングリスト の設 定 を行うには、メーリングリスト マネージャでメーリングリスト をダブルクリックします。左 側 のナビゲーション部 分 から、設 定 したいメニューをクリックして下 さい。

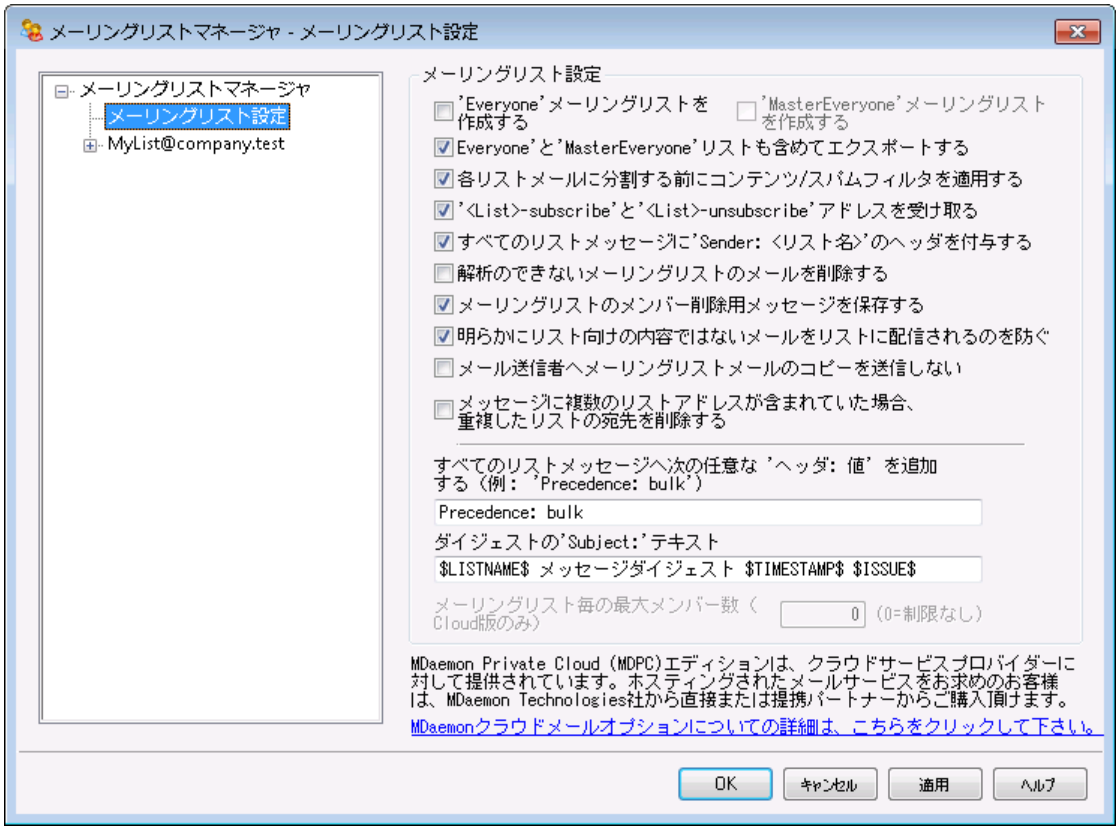
メーリングリスト設定

メーリングリスト マネージャ 248 画面の左側にあるメーリングリスト設定 をクリックすると、メーリングリストに関連した全体設定が行えます。

参照:

メーリングリスト設定 248

3.4.1 メーリングリスト設定



メーリングリスト設定

'Everyone'メーリングリストを作成する
ドメイン全員用に、（例えば everyone@example.comといった）"Everyone" メーリングリストを作成するにはこれをクリックします。このメーリングリストはドメイン毎に作成でき、"everyone@<domain>"宛てにメールを送信するだけで、ドメイン全員に対してメールを送る事ができるようになります。"Everyone" メーリングリストではプライベートアカウント 693 は非表示になっています。 このオプションはデフォルトで無効になっています。

'MasterEveryone'メーリングリストを作成する
"MasterEveryone" メーリングリストを作成するにはこのチェックボックスを有効にします。"everyone"メーリングリストを有効にしている全てのドメインのメンバーがこのメーリングリストへ含まれます。このオプションはデフォルトで無効になっています。

エクスポート時システム生成の'Everyone'と'MasterEveryone'メーリングリストを含む

デフォルトで、「アカウント >> エクスポート」オプションからメーリングリストをエクスポートした際、'Everyone'と'MasterEveryone'メーリングリストも含まれます。メーリングリストをエクスポートする際、これを含まないようにするには、このオプションを無効にして下さい。

各リストメールに分割する前にコンテンツ/スパムフィルタを適用する

メーリングリストエディタの[ルーティング](269)*でリストメールを各メンバーへ配信する*オプションが有効な場合この設定を有効にするとコンテンツフィルタルールやスパムフィルタがメールがコピーされメンバーへ配信される前に適用されるようになります。

<List>-subscribe' と '<List>-unsubscribe' を受けとる

MDaemonにメーリングリストの購読や購読解除を受け取るためのメールアドレスを(メーリングリストが実在する限り)認識できるようにするには、このオプションをクリックします。例えば、MyList@ example.comというメーリングリストを管理しているとします。MyList-Subscribe@ example.comやMyList-Unsubscribe@ example.comへメールを送信することで、メーリングリストの購読や購読解除が行えます。メールの件名や本文は何でも構いません。この機能が有効な場合、MDaemonは全てのメーリングリストメールへ次のヘッダを挿入します:

```
List-Unsubscribe: <mailto:<List>-Unsubscribe@example.com>
```

メーラーによってはこれを認識し、自動的にUNSUBSCRIBEボタンを生成します。

> メーリングリストエディタの[モデレーション](267)にあるメーリングリストURLオプションでList-SubscribeやList-Unsubscribeヘッダの値を指定する事により、メーリングリスト毎に、この設定を上書きする事ができます。

全てのリストメッセージに 'Sender: <List>' ヘッダを付与する

メーリングリストメールへSenderヘッダを挿入するにはこのオプションを有効にして下さい。

解析のできないメーリングリストのメールを削除する

このオプションを有効にすると、解析できるアドレスを含まないメーリングリストメールを削除します。

メーリングリスト用のメンバー削除メールを保存する

MDaemonはメーリングリスト宛てのメールで、一部のメンバーから戻ってきた場合、リストメンバーから削除する対象のアドレスとして保存します。詳細な情報については[設定](254)オプションの*到達できないアドレスの削除...* を参照して下さい。

明らかにメーリングリスト向けではないメールのリストへの配信を防ぐ

メーリングリスト宛てのメールで、本来はシステムアカウントへ送信するべきメールであると判断した場合に、そのメールを削除するにはこの設定を有効にします。例えば、ユーザーがメーリングリストの購読や購読解除のコマンド行うには、SubscribeやUnsubscribeコマンドをメールの最初に入力し、(mdaemon@ example.com)などのシステムアドレスへ送信しますが、ユーザーがこうしたメールをメーリングリスト自体へ誤って送信する事はよくあります。このオプションはこうしたメールがメーリングリストへ届いてしまう事を防ぎます。

メール送信者へメーリングリストメールのコピーを送信しない
このオプションが有効で、メーリングリストのメンバーがメーリングリスト宛てにメールを送信した場合、メール送信者は自分が送信したメールを受け取りません。このオプションはデフォルトで無効になっています。

メッセージに複数のリストアドレスが含まれていた場合重複したリストのアドレスを削除する
メールが複数のメーリングリスト宛てに送信された際、MDaemonが複数メーリングリストに所属しているメンバーに1通だけメールの送信を行うようにするには、このオプションを有効にします。例えば、frank@example.net がList-A@example.com とList-B@example.com 両方に属しており、両方のメーリングリスト宛てにメールが送信された場合、Frankは2通ではなく1通のみメールを受信するようになります。このオプションはメーリングリストにのみ適用できます。つまり、もしもこのメールがFrank宛で直接送られた場合には、Frankは合計で3通ではなく2通のメールを受け取る事になります。このオプションはデフォルトで無効になっています。

> このオプションの有効化は一般的に推奨されません。ユーザーによってメーリングリストは様々な使われ方をしており、この方法で重複を制限した場合、どのメーリングリストでメールを受信できたのか判断する事ができなくなるためです。そのため、メッセージスレッドの初期設定や、IMAPフィルタ 670 でメールを特定のフォルダに振り分ける際など、ユーザーによってはこのオプションが不要な混乱を招く場合があります。

全てのリストメッセージへ次の任意な'ヘッダ: value'値を追加する
(Precedence: bulk といった)固定のヘッダ/値の組み合わせを全てのメーリングリストへ挿入する場合は、そのヘッダと値の組み合わせをここで入力します。

ダイジェストの'Subject:'テキスト:
メーリングリストダイジェスト 264 へ送るメールの件名をカスタマイズする場合はこのオプションを使用します。デフォルトでは"$LISTNAME$ message digest $TIMESTAMP$ $ISSUE$."です。マクロはメーリングリスト名、ダイジェストメールの生成時刻、登録番号へ展開されます。

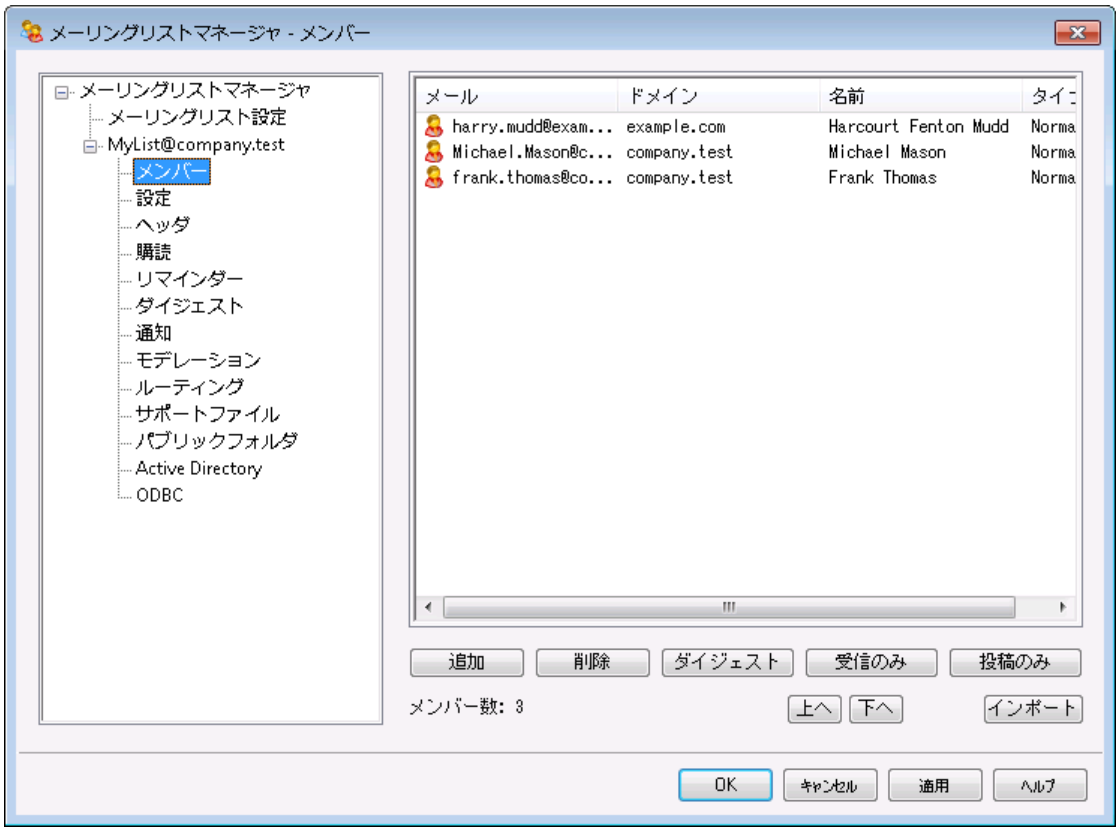
メーリングリスト毎の最大メンバー数 [xx] (0=無制限)
メーリングリスト毎に設定できる最大メンバー数を設定するにはこのオプションを使用します。ドメイン毎の最大メンバー数は、ドメインマネージャの設定 193 画面で設定できます。このオプションはMDaemon Private Cloudでのみ使用できます。

参照:

メーリングリストマネージャ 245

3.4.2 メーリングリストエディタ

3.4.2.1 メンバー



このボックスは、リストを現在購読しているメンバーのメールアドレスおよび名前をと、**通常**、**ダイジェスト**、**受信専用**、**投函のみ**をいった「タイプ」を表示しています。メンバーの設定を編集するには、メンバーのエントリをダブルクリックします。

追加
このボタンをクリックすると新しいメンバーを設定するための新しいメンバーの追加 252 が起動します。

削除
リストからメンバーを削除するには、エントリを選択し削除ボタンをクリックします。

ダイジェスト
メンバーを選択し、ダイジェスト 264 に変更する場合には、このボタンをクリックします。ボタンをもう一度クリックすると「ノーマル」へ戻ります。

受信のみ
メンバーのエントリを選択し、[**受信(読み取り)のみ**]に切り替えるとき、このボタンをクリックします。受信だけのメンバーは、メッセージを受信だけで送信することはできません。ボタンをもう一度クリックすると「ノーマル」へ戻ります。

投稿のみ
メンバーを選択した後、このボタンをクリックすると、メンバーを[投稿のみ]に設定できます。[投稿のみ]では、メンバーは、メッセージを送信できますが受信することはできません。ボタンをもう一度クリックすると「ノーマル」へ戻ります。

上へ/下へ
メンバーを選択し、このボタンをクリックすると、リスト内で上下へ移動できます。カラムのヘッダをクリックすつろソートする事もできます。注意点：カラムのヘッダでソートした場合、上へ/下へのボタンで手動でソートした一覧を上書きします。

インポート
このボタンをクリックすると、カンマで区切られたテキストファイルからメンバーリストをインポートします。メンバーはそれぞれ1行となっており、全フィールドがカンマによって区切られていなければなりません。さらに、1行目（ベースライン）は、フィールド名を入力する必要があります。メールアドレス用の"Email"フィールドが1つ必要です。更に2つのオプションとして "FullName"と"Type"があります。"FullName"にはメーリングリストメンバーの名前を含み、Typeは"通常", " 投稿のみ", "ダイジェスト", "受信のみ"のどれかが入ります。その他のフィールドはインポートの際には無視されます。

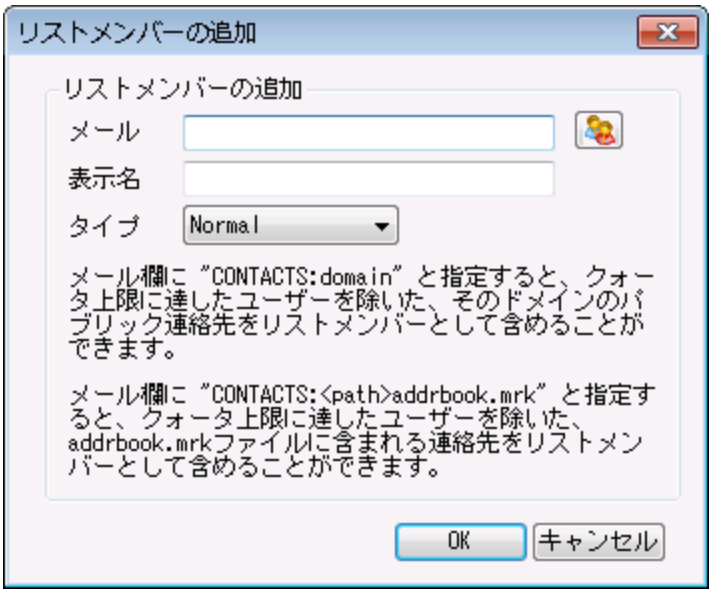
例：

```
"Email", "FullName", "Type", "Address", "telephone"
"user01@altn.com", "Michael Mason", "Digest", "123 Street St", "519.555.0100"
```

インポートされたメンバーにはウェルカムメールは送信されません。またインポートの際にメンバーの重複はチェックされません。

メンバー数：
現在のメーリングリストメンバーの合計数が画面の下部へ表示されます。

新しいメンバーの追加



新規メンバーの追加

新規メンバーのアドレス
メーリングリストへ追加するメールアドレスを入力して下さい。アカウントアイコンをクリックし、MDaemonアカウントやグループをリストメンバーとして選択する事もできます。リストメンバーのアドレスには !や | は使用できません。

特定のグループに、ドメインの全ユーザーや特定のグループに属した全ユーザーを追加する場合は、メールアドレスを個々に入力するのではなく、**ALL_USERS:<domain>** や **GROUP:<group-name>** を使用できます。例えば、ALL_USERS:example.comを新規メンバーとして追加すると、example.comドメイン内のユーザーアカウント全てを1つづつ入力した場合と同様に追加できます。

また、**CONTACTS:<domain>** でドメインの公開連絡先[107]へリストメンバーとして登録する事もできます。例 `CONTACTS:example.com`

リアルネーム
このフィールドへメンバーの名前を入力します。この名前は、ヘッダ[257]画面の*"TO"ヘッダの"表示名"を"メンバー名"へ置き換える*が選択されている場合、メーリングリストメールのTO:ヘッダへ表示されます。

タイプ
ドロップダウンボックスからユーザーのメンバータイプを選択します。

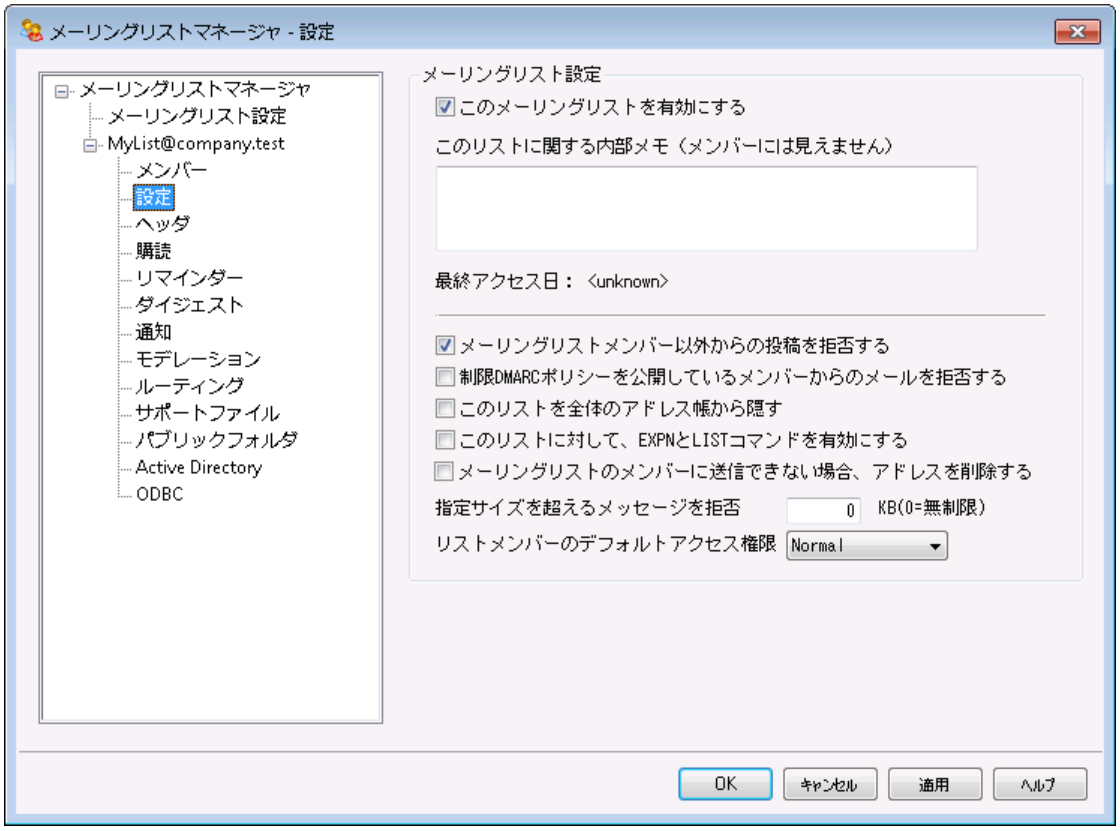
Normal– メンバーはメーングリストメールを通常通り送受信できます。

Digest– メンバーはメーリングリストの送受信が行えますが、受信したメールはダイジェストフォーマットとなります。

Read only– メンバーはメールを受信できますが、メールの送信は行えません。

Post only– メンバーはメーリングリスト宛てのメールは送信できますが、受信する事はできません。

3.4.2.2 設定



メーリングリストの設定

このメーリングリストを有効にする
メーリングリストを一時的に無効にするにはこの設定を外してください。メーリングリストが無効になっている間、SMTP経由で届いたメールやメーリングリストによって生成されたメールは451の一時的なエラーで拒否されます。

このリストに関する内部メモ（メンバーには見えません）
メーリングリストに関する非公開メモ用のフィールドです。ここで記入した内容はメーリングリストのメンバーにも非公開です。

最終アクセス日
メーリングリストへ誰かが最終的にアクセスした日時が表示されます。これによって、メーリングリストがあまり使われていなかったり、全く使われていなかったりした場合に、それを判定できるようになります。

メーリングリストメンバー以外からの投稿を拒否する
このコントロールを有効にすると、メーリングリストは[プライベート]と見なし、リストのメンバーのみがメッセージを送信することができます。メンバー以外のメッセージは拒否されます。

制限DMARCポリシーを公開しているメンバーからのメールを拒否する
制限 DMARC[488] ポリシー（例：p=quarantine or p=reject）を公開しているドメインに所属しているユーザーからメーリングリストへ送られてきたメールを拒否する場合はこのオプションを有効にします。このオプションは ヘッダ[257]で*"次の場合リストの 'From:' アドレスを変換する"*オプションを有効にしている場合は、指定する必要はありません。

このオプションと*"次の場合リストの 'From:' アドレスを変換する"*[257]オプションの両方が無効の場合、メーリングリストメールは受信側のサーバーで拒否される場合があり、設定によっては受信者がリスト宛先メールアドレスがメーリングリストメンバーから自動的に削除[256]されることがあります。このため、オプションの中の最低1つは有効にするようにして下さい。

このリストを全体のアドレス帳から非表示にする
WebmailおよびLDAPパブリックアドレス帳からメーリングリストを非表示にするには、このオプションをクリックします。

このリストでEXPNおよびLISTコマンドを有効にする
デフォルトで、メンバー情報をプライベートな情報として保持するため、MDaemonはEXPNやLISTコマンドを受け付けません。このオプションを有効にすると、メーリングリストのメンバー情報が、EXPNやLISTコマンドの要求に対する応答として返されます。

リストメンバーシップから配信不能な電子メールアドレスを削除する
この機能が有効になっていると，MDaemonは、メール配信時に回復不能なfatalエラーが発生した場合、自動的にメンバーリストからメールアドレスを削除します。この機能が有効の場合、MDaemonは、メール配信時に回復不能なfatalエラーが発生したメールアドレスをメーリングリストのメンバーから自動削除します。メールアドレスはRetry[794]システムの中のメールからも期限切れになると削除されます。

配信不能なメールアドレスを削除する..オプションはリモートメールサーバーがメールの受け入れを拒否する状況に対応するためだけの機能です。これは、ルーティング画面で[269]「各メンバーに個別にリストメールを配信する」が選択されている場合にのみ機能します。リストメッセージをスマートホストにルーティングする場合は、以下の「リスト整理の拡張[256]」を参照してください。

指定サイズを超えるメッセージを拒否 [xx] KB
このコントロールでは、このメーリングリストで許容されるメッセージのサイズの上限を設定します。この制限を超えるメッセージは拒否されます。

リストメンバーのデフォルトアクセスタイプ
このオプションで新しいメンバーのデフォルトでのアクセスモードを選択します。既存メンバーのアクセスモードはメンバー[251]からいつでも変更できます。4種類のメンバーシップモードがあります。

Normal– メンバーはメーングリストメールを通常通り送受信できます。

Digest– メンバーはメーリングリストの送受信が行えますが、受信したメールはダイジェストフォーマットとなります。

Read only– メンバーはメールを受信できますが、メールの送信は行えません。

Post only– メンバーはメーリングリスト宛てのメールは送信できますが、受信する事はできません。

リスト整理の拡張

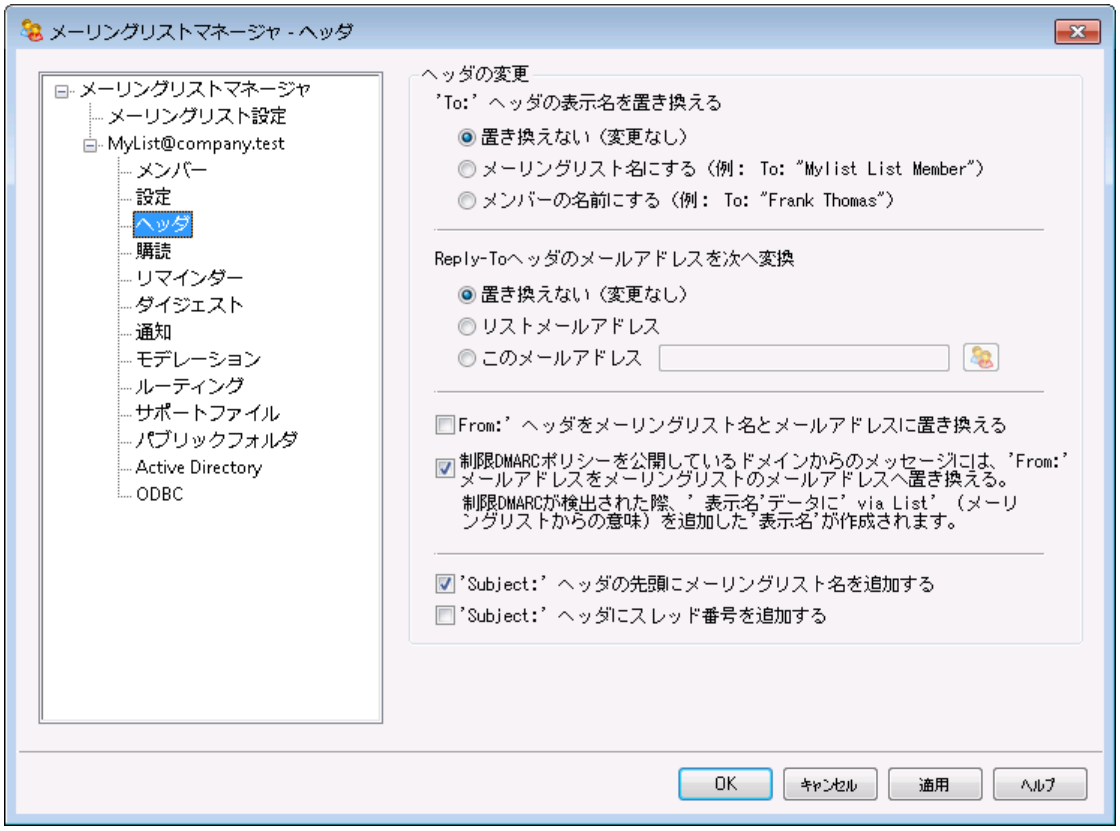
*配信不能なアドレスをリストメンバーから削除する*オプションが有効でメーリングリフトメールのリターンパス（通知265にある、リストのSMTP 'Bounce' アドレスオプションをご覧ください）が指定されている場合、MDaemonは夜間にエラーで返信されたメールを解析し、配信できないメンバーを削除します。この機能は、特にメーリングリストのメールを直接配信ではなくスマートホスト経由で配信している場合に、メーリングリストから効率よく無効なメールアドレスを削除するのに役立ちます。

メーリングリスト設定248には、この機能に関連する2つのオプションがあります。メーリングリスト解析できないメッセージを削除すると、解析可能なアドレスを含まない返されたメッセージが削除され、*メーリングリスト のメンバー削除用メッセージを保存する*オプションはリストメンバーの削除される結果となるすべてのメッセージが保存されます。

*リストのSMTP 'Bounce' アドレス*265 へローカルユーザーアドレスを使用すると、メーリングリスト設定248のリスト整理の設定に基づき、ユーザーのメールが削除されてしまう場合があります。

送信メールが5xxエラーになった場合、対象アドレスはBadAddress.txtファイルへ追加されます。これにより、例えば無効なアドレスがメーリングリストへ含まれていた場合、SMTPログを確認するよりも素早く簡単に、対象アドレスを把握できます。このファイルはサイズが大きくなりすぎないよう、日別の夜間処理で自動削除されます。

3.4.2.3 ヘッダ



ヘッダの変更

'TO:'ヘッダの表示名を置き換える
MDaemonがメーリングリスト宛てのメールを受信する際の、TO: ヘッダの表示名を指定します。

なし（そのまま）
このオプションが選択されると、表示アドレスの変更はありません。TO: フィールドのアドレスは、メッセージの送信者が入力したのと同じものが表示されます。

リスト名
このオプションが選択されるとTO: ヘッダにはメーリングリストのアドレスが表示されます。

メンバーのフルネーム
このオプションが選択されると、TO: ヘッダには、（確認できる場合は）メールの宛先となるリストメンバーの名前とアドレスが表示されます。

> ルーティング画面 269 で*リストメールを各メンバーへ配信する*が選択されている場合は、**メンバーのフルネーム**以外は選択できません。**各メンバーにRCPTコマンドを使用しリストメールを配信する**が選択されている場合は、MDaemonは、リスト名をデフォルトとして設定します。

Reply-Toヘッダのメールアドレスを置き換える
このオプションは各メーリングリストメールのReply-To: ヘッダへ表示される値を指定するのに使用します。

なし（そのまま）
このオプションが選択されると、Reply-To: ヘッダの変更はありません。メーリングリストへ投稿したメールに対して、メーリングリスト全体ではなく、送信者に直接返信してほしい場合、一般的にはこのオプションが選択されます。

リストメールアドレス
特定の個人やアドレスではなくメーリングリストへ返信が欲しい場合はこのオプションを選択します。メーリングリストをグループ間での会話に使用するなど、全員に対してメール送信を行いたい場合は、一般的にこのオプションを選択します。

このメールアドレス
特定のアドレスへ返信を行いたい場合はここで対象のメールアドレスを指定するか、特定のMDaemonアカウントのアカウントアイコンをクリックします。例えば返信を特定のユーザーに対して送ってほしいメールマガジンの配信などで、このオプションを選択します。

'From:'をメーリングリスト名とメールアドレスへ書き換える
From: ヘッダの内容をメーリングリスト名とメールアドレスへ置き換えるにはこのボックスをチェックします。

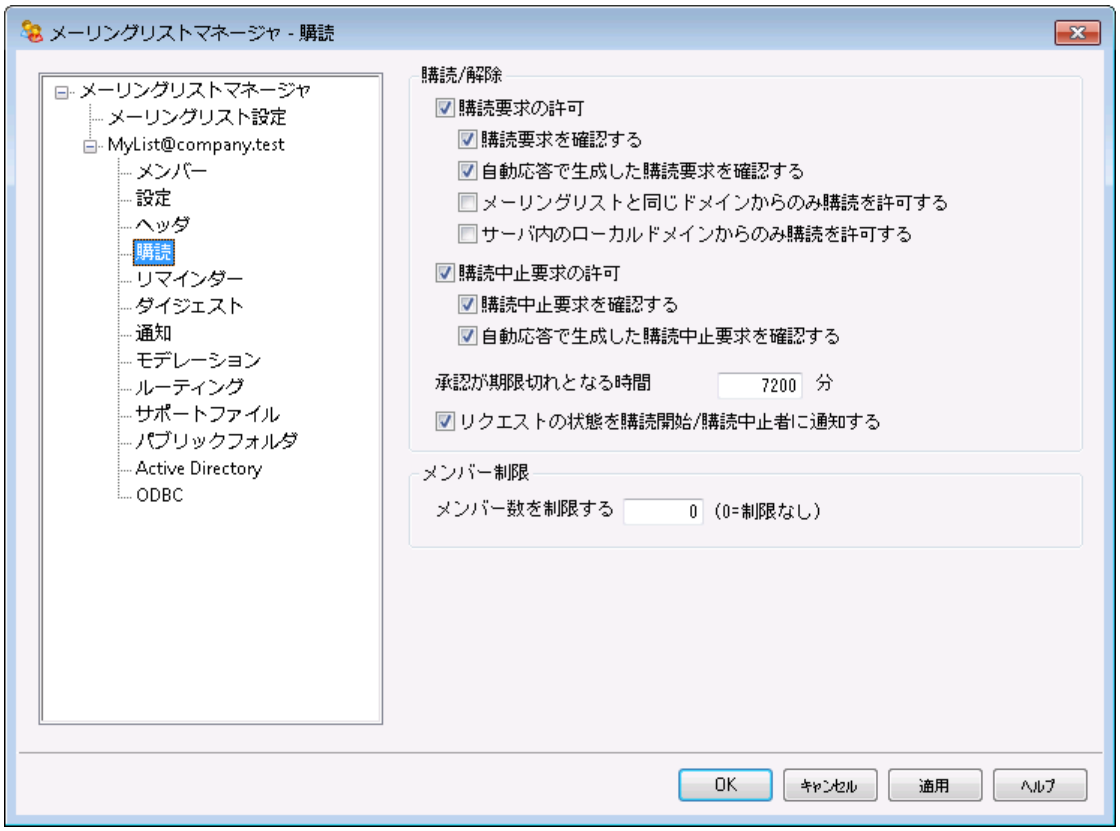
制限DMARCポリシーを公開しているドメインからのメッセージは 'From:' メールアドレスをメーリングリストのアドレスへ置き換える
制限 DMARC[488] ポリシー（例: p=quarantine or p=reject）を公開しているドメインに所属しているユーザーからメーリングリストへメールが送られてきた場合、デフォルトでMDaemonは、メーリングリストへメールを送信する前にFrom: ヘッダのメールアドレスをメーリングリストアドレスへ置き換えます。これは、制限DMARCポリシーからのメールをサーバーが拒否してしまうのを防ぐために必要な設定です。From: ヘッダのアドレス変更に加え、表示名は「～による」を追加し、メーリングリストに所属した特定のユーザーからのメールである事を意味します。更に、From: ヘッダが書き換えられた場合、元のFrom: ヘッダ情報は、Reply-To: ヘッダが存在せず、メーリングリストでカスタマイズしたReply-To: ヘッダの表示を行っていない場合に限り、Reply-To: ヘッダへ移動します。

このオプションは、この機能の意味と必要性を把握していない限り、無効にするべきではありません。このオプションを無効にすると、メーリングリストメールは受信側のサーバーで拒否される場合があり、設定によっては宛先メールアドレスが*メーリングリストメンバーから自動削除*[256]されます。その代わりに、制限DMACポリシーに所属するドメインから受信したメールに対しては、*制限DMARCポリシーからのメッセージを拒否する*[254]オプションを使用できます。

"Subject:'ヘッダの先頭にリスト名を追加する
この設定により、MDaemon はこのメーリングリストに送信される全メールの Subject: の前にブラケット（[ ]）で囲んだメーリングリストの名前（例えば [ListName]）を追加します。この機能はデフォルトで有効です。

"Subject:'ヘッダにスレッド番号を追加する
このスイッチにより、スレッド番号をメールのSubject:ヘッダに表示するかどうかを切り換えることができます。そのスレッド番号は仮想スレッド番号として、Subject:フィールドの最後に追加されます。Subject:内のスレッドを利用して、メーリングリストのメールを並び替えることが可能になります。 このオプションはデフォルトで無効になっています。

3.4.2.4 購読



購読/購読解除

購読要求を許可する
このオプションで特定形式のメールや自動応答機能で購読要求を許可するかどうかを指定します。詳細についてはメーリングリストの購読 261を参照して下さい。

購読要求を確認する
このオプションを有効にすると、MDaemonは固有に生成したコードを購読要求を行ったアドレスに対して送信します。この確認用メールに返信があった場合はMDaemonは対象ユーザーをメーリングリストのメンバーとして追加します。確認メールは時間に依存します。言い換えると、ユーザーはここで指定した時間(分)の間に返信を行う必要があります。 **注意点:** 確認メッセージの内容はMDaemon¥app¥フォルダ内のSubConf.datファイルへ記載されています。

自動応答で生成した購読要求を確認する
このオプションを有効にすると、MDaemonは自動応答 660オプションの*"送信者をメーリングリストへ追加"*オプションを使い、自動で購読確認メールを生成します。上記のオプションと同様、

MDaemonは固有に生成したコードを購読要求を行ったアドレスに対して送信し、確認メールに返信があった場合はMDaemonは対象ユーザーをメーリングリストのメンバーとして追加します。確認メールは時間に依存し、ユーザーはここで指定した時間(分)の間に返信を行う必要があります。

メーリングリストと同じドメインからのみ購読を許可する
メーリングリストのドメインに所属したユーザーからの購読要求のみを許可する場合はこのオプションを選択します。例えば、MyList@example.comの購読は、@example.comドメインのユーザーのみが許可されます。

サーバ内のローカルドメインからのみ購読を許可する
MDaemonサーバーのローカルドメインに所属しているユーザーからの購読要求のみを許可する場合はこのオプションを選択します。

購読解除

購読解除要求を許可する
このオプションで特定形式のメールや自動応答機能で購読解除要求を許可するかどうかを指定します。詳細についてはメーリングリストの購読 261を参照して下さい。

購読解除要求を確認する
このオプションを有効にすると、MDaemonは固有に生成したコードを購読解除要求を行ったアドレスに対して送信します。この確認用メールに返信があった場合はMDaemonは対象ユーザーをメーリングリストのメンバーから削除します。確認メールは時間に依存します。言い換えると、ユーザーはここで指定した時間(分)の間に返信を行う必要があります。 **注意点**: 確認メッセージの内容はMDaemon¥app¥フォルダ内のUnSubConf.datファイルへ記載されています。

自動応答で生成した購読中止要求を確認する
このオプションを有効にすると、MDaemonは自動応答 660 オプションの*"送信者をメーリングリストから削除"*オプションを使い、自動で購読解除確認メールを生成します。上記のオプションと同様、MDaemonは固有に生成したコードを購読解除要求を行ったアドレスに対して送信し、確認メールに返信があった場合はMDaemonは対象ユーザーをメーリングリストのメンバーから削除します。確認メールは時間に依存し、ユーザーはここで指定した時間(分)の間に返信を行う必要があります。

承認が期限切れとなる時間 [XX] 分
これは、受信者が購読または購読解除確認メッセージに返信しなければならない時間(分単位)で、この時間に到達するとメールは期限切れとなり、アドレスはリストへ追加されたり、リストから削除されたりする事はありません。アドレスは、リストに参加または解除の新規リクエストを送信する必要があります。このオプションのデフォルト設定は、7200分(5日)です。

これは、グローバル設定で、特定のリストだけではなく、全てのメーリングリストに適用されます。

リクエストの状態を購読開始/購読中止者に通知する
この設定を有効にすると、MDaemonは、メーリングリストの購読開始や購読解除の処理が完了した事をユーザーへ通知します。

メンバー制限

メンバー数を制限する(0=制限なし)
この機能で、メーリングリストで購読メンバー数の上限を指定できます。0(ゼロ)を指定すると制限はありません。

この制限は、メーリングリストの購読[261]で説明したメールを使った購読者アドレスに対してのみ適用されます。リストパスワード[267]を含んだメールを使った購読開始者や、メンバー[251]画面から手動で登録したメンバーに対しては適用されません。

参照:

メーリングリストの購読[261]
自動応答[660]

3.4.2.4.1 メーリングリストの購読

メールコマンドによる購読と購読解除

メーリングリストの購読や購読解除には、メーリングリストを管理するドメインのMDaemon(またはそのエイリアス)に、本文の一行目をSubscribeまたはUnsubscribeと記載したメールを送信します。例えば、mdaemon.comにMD-Supportというメーリングリストがあるとします。これを購読するには、mdaemon@mdaemon.comにメールを送信し、本文の一行目をSUBSCRIBE MD-Support@mdaemon.com と記載します。メールの件名は何でも構いませんし、空白であっても構いません。

メールを使ったコマンドに関する詳細は、メールによるリモートサーバコントロール[816]を参照してください。

ユーザーがメーリングリストの購読や購読解除のコマンドを、MDaemonシステムアカウントではなくメーリングリスト自体へ誤って送信する事はよくあります。こうしたメールがメーリングリストへ届いてしまう事を防ぐには、(設定 ≫ 初期設定 ≫ システム[450])の*明らかにメーリングリスト向けではないメールのリストへの配信を防ぐ*オプションを有効にします。これはデフォルトで有効です。

メールアドレスによる購読と購読解除

設定 ≫ メーリングリストマネージャ ≫ メーリングリスト設定[248]にある「<List>-subscribe'と'<List>-unsubscribe'アドレスを受け取る」オプションを使うと、上記のSubscribe/Unsubscribeのようなコマンドを送るのではなく、特別な電子メールアドレスにメッセージを送る事でメーリングリストの購読や購読解除が行えるようになります。この方法で購読や購読解除を行う場合は、指定したメーリングリストアドレスの、メールボックス名の最後に-subscribeや-unsubscribeを追加して、メールを送信する必要があります。例えば、リストの名前がfranks-list@ example.comである場合、"franks-list-subscribe@ example.com"へメールを送信することでユーザーはメーリングリストの購読が開始できます。購読を解除するためは、"franks-list-unsubscribe@ example.com"にメールを送信します。いずれの場合においても、サブジェクトおよびメッセージ本文の内容は無関係です。また、この機能がアクティブな時に、MDaemonはすべてのリストメッセージに次のヘッダを挿入します:

```
List-Unsubscribe: <mailto:<List>-Unsubscribe@example.com>
```

メーラーによってはこれを認識し、自動的にUNSUBSCRIBEボタンを生成してくれるものもあります。

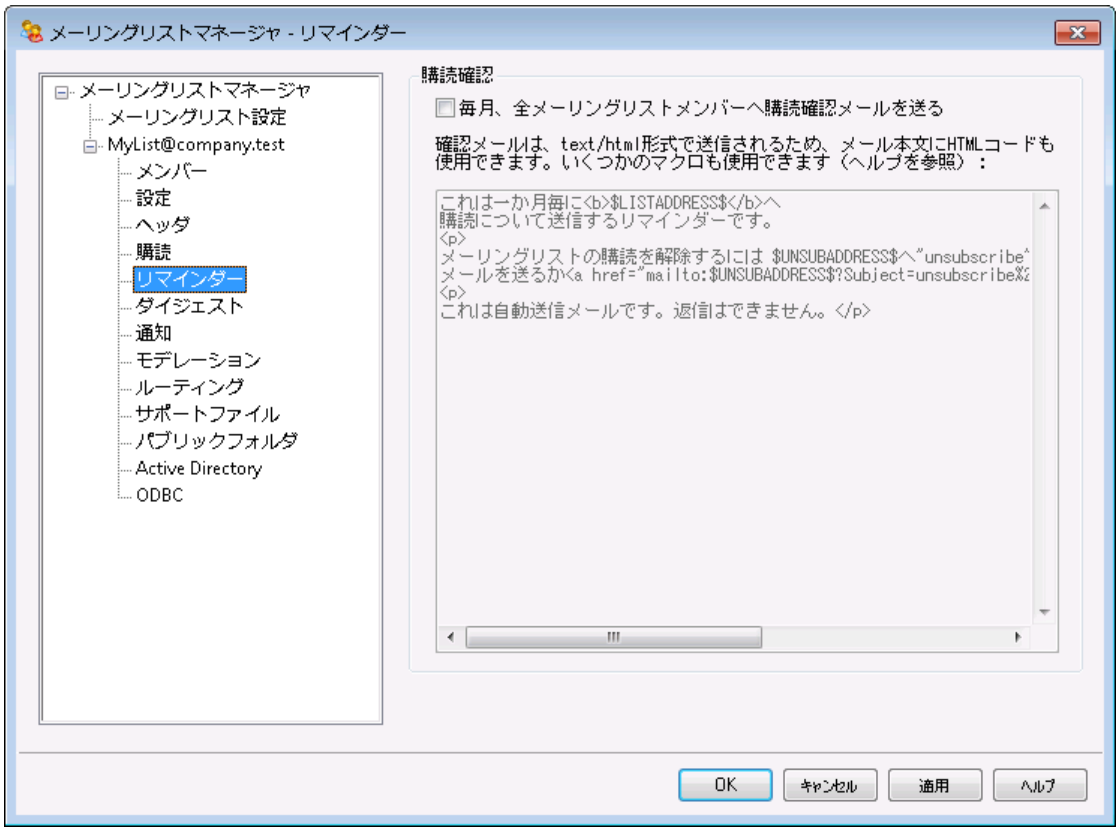
自動応答による購読と購読解除

自動的にリストメンバーを追加または削除するために、自動応答[660]を利用することもできます。これを行うためには、アカウント毎の自動応答機能によって、アドレスの追加や削除を行うためだけのMDaemonアカウントを作成します。例えば、"franks-list@example.com"と呼ばれるメーリングリストがある場合、"join-franks-list@example.com"というMDaemonアカウントを作成します。続いて、メーリングリストの購読を行うのに"franks-list@example.com"へメールを送信します。これは、上記のメールコマンドの方法を通して購読/購読解除によって必要とされる特別なメールコマンドを覚える必要がなく、ユーザにとって非常にシンプルな方法です。

参照:

購読[259]
メールによるリモートサーバコントロール[816]
自動応答[660]
初期設定 ≫ システム[450]
初期設定 ≫ その他[459]

3.4.2.5 リマインダー



購読確認

毎月全メーリングリストメンバーへ購読確認メールを送る
このオプションを有効にすると、毎月1日にメーリングリストメンバーに購読確認メールを送ります。メールの内容はテキストボックスで指定したものをtext/html形式で送ります。必要に応じて、ここではHTMLコードも使用できます。下記のマクロが購読確認メールの中で利用できます:

$LISTADDRESS$ - メーリングリストのメールアドレスに置き換わります（例. MyList@example.com)

$LISTNAME$ - メーリングリストのメールアドレスのローカル部分に置き換わります（例. MyList).

$UNSUBADDRESS$ - メーリングリストの購読解除アドレスに置き換わります（MDaemonシステムメールアドレスです。例. mdaemon@example.com）

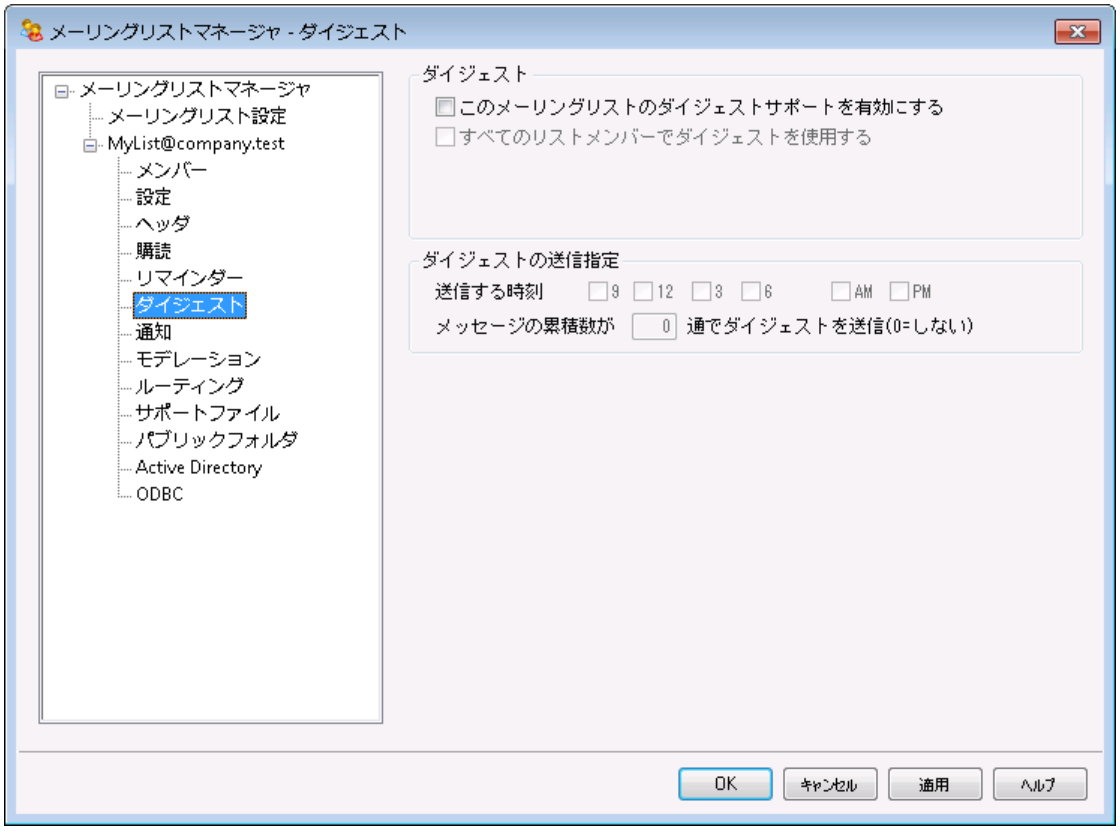
$MEMBERADDRESS$ - 購読確認メールを受け取るメーリングリストメンバーのアドレスに置き換わります（例. frank.thomas@example.com）

購読確認を毎月別の日に送信する場合は、MDaemon.iniファイルの次の値を使って変更できます:

```
[Special]
ListReminderDay=X
```

Xは1から28までの数字で置き換えて下さい。この数字は、確認メールを送りたい日付を表しています。

3.4.2.6 ダイジェスト



ダイジェスト

このメーリングリストでダイジェストのサポートを有効にする
このメーリングリストのダイジェストサポートを有効にするにはこのオプションをチェックします。ダイジェストサポートが有効な場合、メーリングリストに送信するメールのアーカイブが保管され、メンバータイプ[251]がダイジェストとして設定されているメンバーに対しては、定期的にこれらメールのアーカイブがコンパクトにインデックスされたダイジェストとして送信されるようになります。

すべてのリストメンバーにダイジェストを使用させる
デフォルトでは、リストメンバーはメッセージを通常の形式かダイジェスト形式で受け取るかを選択することができます。このオプションによって、選択したモードに関わらず、メンバー全員にダイジェストモードを使用させるようにすることができます。

ダイジェストの送信時間

ここでは、ダイジェスト形式のメールを受信するよう設定されているユーザーが、どの位の頻度で、又は、どういった条件の下でダイジェストメールを受け取るのかを設定します。オプションのすべては、互いに独立して動作します。つまり、一つの設定を行うだけで、ダイジェストメールの送信が行えるようになります。

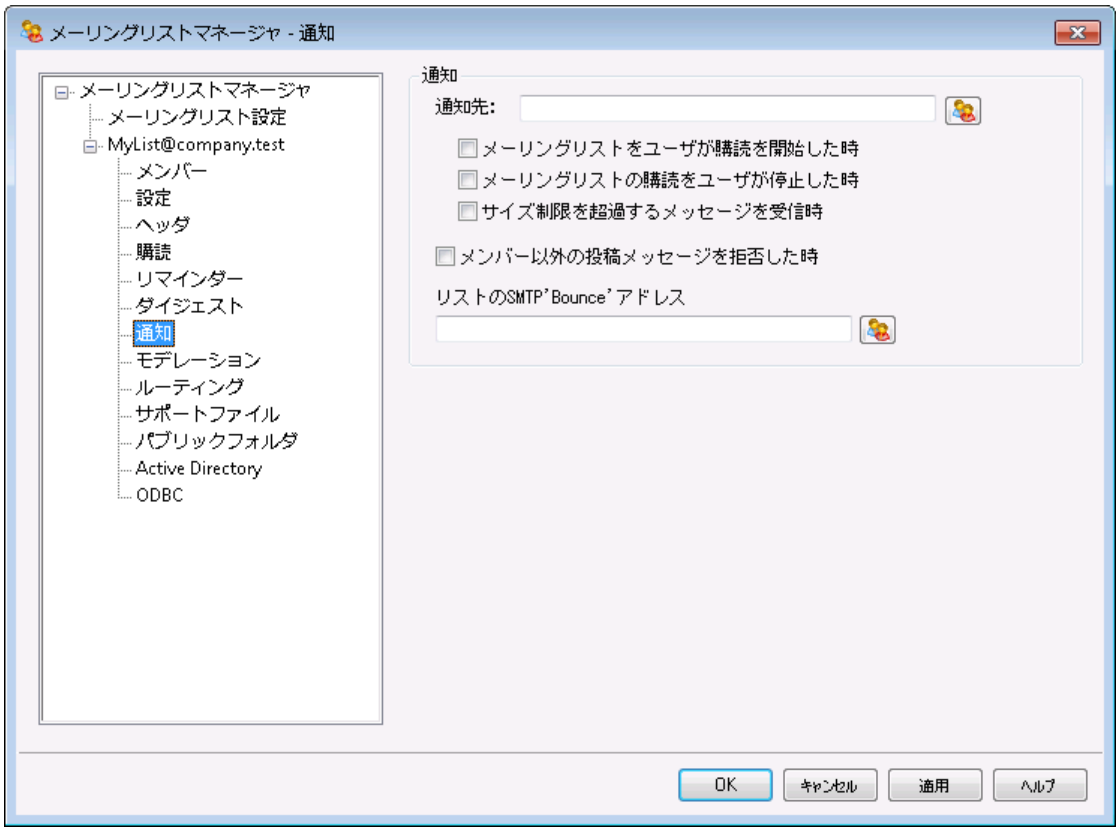
送信する時刻 9, 12, 3, 6 AM/PM
ダイジェスト送信の頻度を指定します。全てのオプションを選択すると、ダイジェストは、この後のオプションで設定したタイミングに加え、3時間毎に送信されることになります。

蓄積メッセージ数が [xx] 通になったらダイジェストを送信 (0 = しない)
蓄積したメールの本数が指定した数になったらダイジェストを送信する場合、このフィールドに数を指定します。このオプションを使用しない場合、0を使用します。0はデフォルト設定です。

参照:

メンバー
電子メールによるリモートサーバーコントロール 816

3.4.2.7 通知



通知

イベント発生時に通知先となるアドレスを指定して下さい。

...このメーリングリストにユーザが購読した時
このチェックボックスを選択すると、メーリングリストの購読を開始すると、上部のフィールドで指定したアドレスへ通知が送信されます。

...このメーリングリストをユーザが購読停止した時
このチェックボックスを選択すると、メーリングリストの購読解除がされると、上部のフィールドで指定したアドレスへ通知が送信されます。

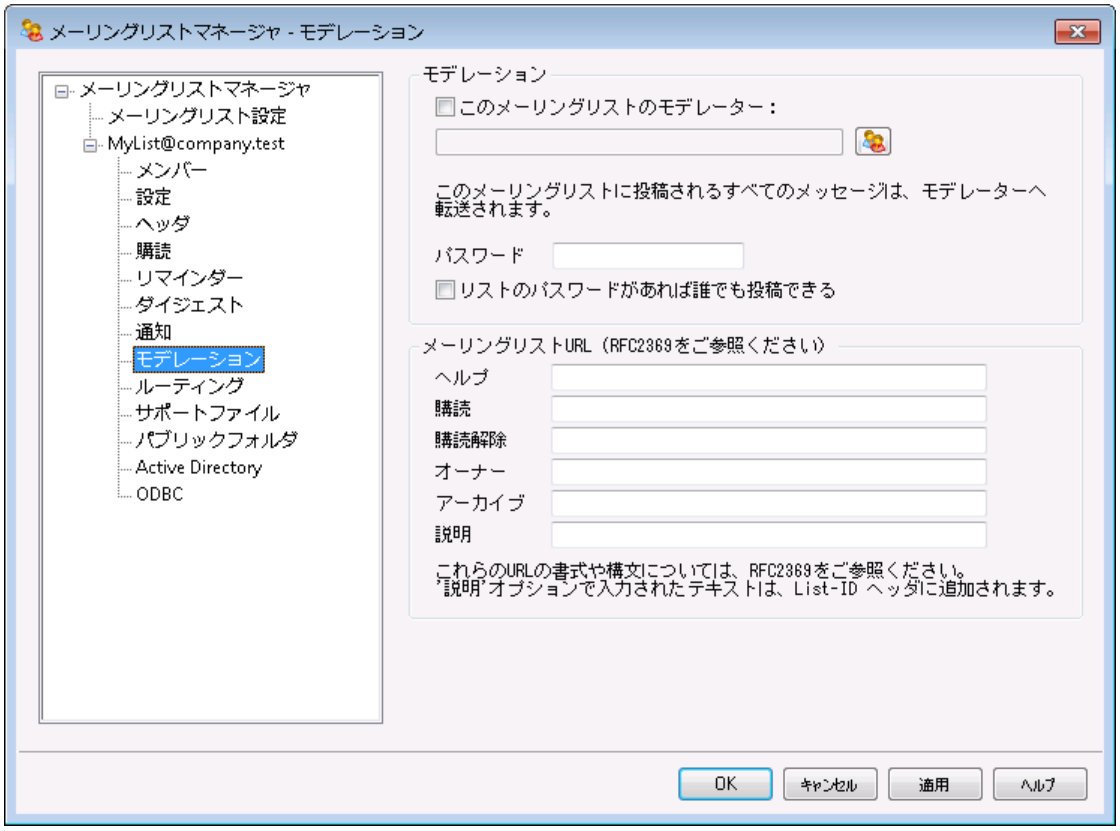
...サイズ制限を超過するメッセージの受信時
このチェックボックスを選択すると、設定 254 画面で指定サイズを超えるメッセージを拒否 で指定したサイズを超えるメッセージがメーリングリストへ送信されると、上部で指定したアドレスへ通知が送信されます。

メンバー以外の投稿メッセージを拒否した時
プライベートのメーリングリストへ非メンバーがメールを送信したとき、リストがプライベート(非公開)であることを送信者へ通知します。同時に、メーリングリストへの加入方法も通知します。設定 254 画面にあるこのリストへはメンバーだけが投稿可能オプションを用いてプライベートとしてリストを指定します。

リストのSMTP 'Bounce'アドレス
バウンスメールの受信またはリストトラフィックから生成されるステータス通知メッセージを配信するアドレスを、このオプションで指定します。例えば、100人の受信者をもつメーリングリストにメッセージを送信され、アドレスの変更、サーバのダウンなどにより10通の配信不能アドレスを持つ可能性があります。SMTPシステムは、これらの配達不能の条件に関係ある通知メッセージをメッセージの送信者に生成し戻します。このオプションを使用して、メーリングリストに対し、これらのメッセージを受信するアドレスを指定することができます。さらに、誰もメールを受信しない選択をすることができ、その場合には、リターンメールが使用できないという方法で、MDaemonはメールストリームにリストメールを配置します。このアドレスは、メーリングリストのアドレスにしないでください。

リストのSMTP 'Bounce' アドレス としてローカルユーザーのアドレスを指定すると、メーリングリスト設定 248 で指定するメーリングリスト整理の結果として、そのユーザー宛のメールが削除される場合があります。ローカルユーザーのアドレスを使う場合はご注意ください。詳しい情報はリスト整理の拡張 256 を参照して下さい。

3.4.2.8 モデレーション



モデレーション

リストの管理者
指定されたユーザがメーリングリストを管理するには、このチェックボックスを選択します。管理対象のリストは、モデレータにすべての投稿メールを転送します。モデレータはリストにメッセージを送信または転送できます。

パスワード
このリストへパスワードを割り当てる場合、ここに入力します。下記のリストのパスワードオプションを知っているユーザは投稿することができ、メンバーシップを無効にするために、購読画面 259 にあるオプションを制限します。メールによるリモートサーバのコントロール 816 で記述のある機能も使用できます。

リストのパスワードがあれば誰でも投稿できる
メーリングリストにパスワードが指定され、このオプションが有効な場合、議論を管理されたリストで送信者がモデレータでなくても、リストのパスワードが件名の最初にあるメッセージは、リストへ投函することができます。

メーリングリストURL（RFC 2369を参照）

MDaemonはメーリングリストのメールへRFC2369「*メーリングリストコマンドにおけるMeta-SyntaxとしてのURL利用とメールのヘッダフィールドの処理*」で定義された、**List-Help**, **List-Subscribe**, **List-Unsubscribe**, **List-Post**, **List-Owner**, **List-Archive** の6つのヘッダを付与する事ができます。メーリングリストのメールにこのヘッダを使うには、フィールドの中にヘッダ値を入力して下さ

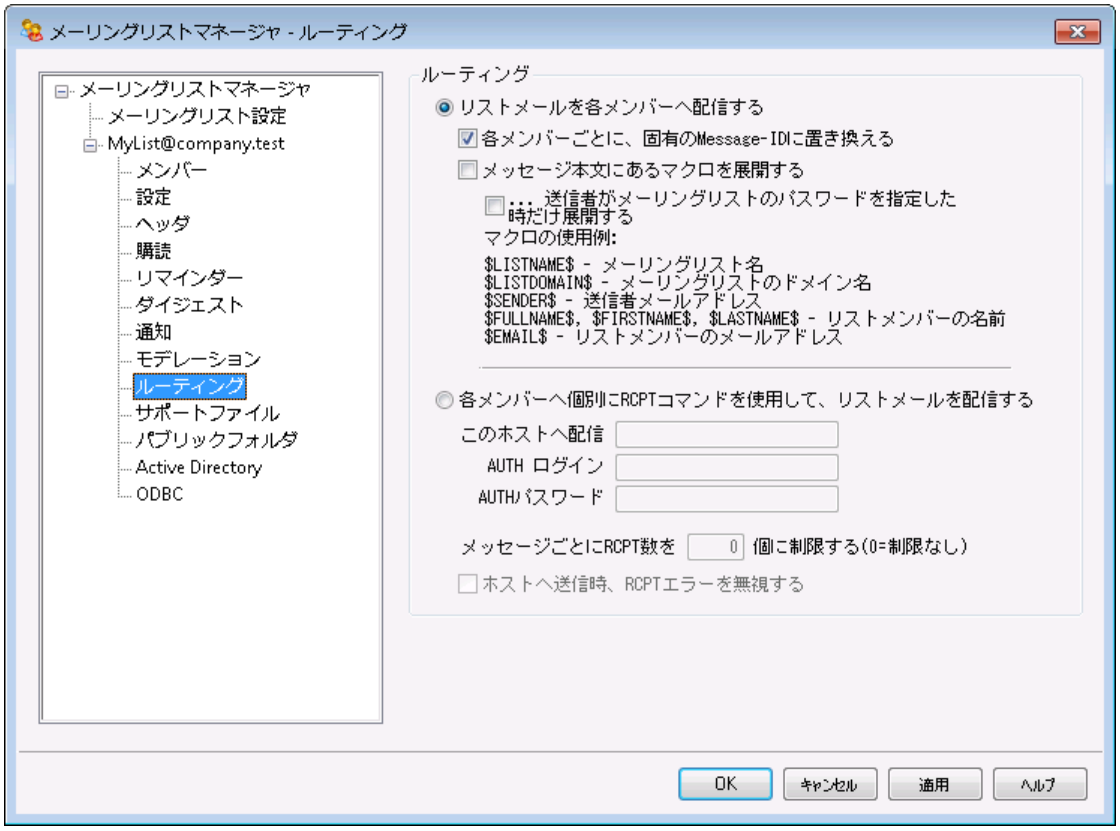
い。ヘッダ値はRFC 2369に準拠した値（例: <mailto:list@example.com?subject=help>）である必要があります。各ヘッダのサンプルはリンクされたドキュメントを参照して下さい。MDaemonはこのデータを変更する事はありません、そのため、データが正しいフォーマットでなかった場合、指定したヘッダは機能しません。

説明（List-ID:ヘッダで使用）
説明（List-ID: ヘッダで使用します）

メーリングリスト宛てのメールのList-ID: ヘッダへ含む短い説明文をここへ入力します。ここで入力した内容とメーリングリストの識別名がヘッダへ含まれます。（例: List-ID: "Frankの個人メーリングリスト" <MyList.example.com>）メーリングリストの識別名が、メーリングリストのアドレスで"@ "を"."に置き換えた形式となっている点に注意して下さい。これはList-ID specification に基づいたものとなっています。この説明オプションを空白にすると、List-ID: ヘッダにはメーリングリストの識別名（例: List-ID: <MyList.example.com>）のみが表示されます。もしもメーリングリスト宛ての受信メールで、既にList-ID: ヘッダを定義してあった場合、MDaemonはこれを適切なものへ入れ替えます。

初期設定 ≫ その他 459 の*'<List>-subscribe'と'<List>-unsubscribe'アドレスを受け取る*オプションが有効になっていると、全てのメーリングリストメールにはデフォルトでList-SubscribeとList-Unsubscribeヘッダが挿入されます。このメーリングリストに対しては自動で挿入されるこれらのヘッダではなく、別の値を挿入したい場合は、ここで挿入する値を指定します。オプションが無効になっている場合は、ここで指定した場合を除いて、List-SubscribeやList-Unsubscribeヘッダが挿入されることはありません。

3.4.2.9 ルーティング



ルーティング

リストメールを各メンバーへ配信する
このオプションが有効の場合、メーリングリスト宛てのメールを受け取ると、リストメンバー毎に個別のメールが生成され、配信されるようになります。これは、非常に多いメッセージが作成される結果となるので、リストサイズおよびサーバの負荷により、パフォーマンスに影響する可能性があります。

各メンバーごとに固有のMessage-IDに置き換える
MDaemonが各メンバーに対して個別のメールを生成する際、メールに固有のMessage-IDを割り当てるにはこのオプションを選択します。このオプションはデフォルトで無効に設定されており、特別に必要な場合を除いて有効化しない事をお勧めします。

メール本文内のマクロを置き換える
メーリングリストメッセージ用の特別なマクロの使用を許可する場合はこのオプションを有効化します。マクロがあると、MDaemonは各メーリングリストメンバーへ配信を行う前に、定義済の値とマクロを置き換えます。

...送信者がメーリングリストパスワードを使用した場合に限る
メール本文のマクロを許可する際、マクロの利用に メーリングリストパスワード 267 を必須とする場合はこのオプションを有効化します。このオプションが無効の場合、誰でもメーリングリスト宛のメールでマクロを使用できるようになります。

マクロ:

$LISTNAME$	メーリングリストの名前か、メーリングリストアドレスの「メールボックス」の部分（例：MyList@example.comのMyListの部分）
$LISTDOMAIN$	メーリングリストのドメイン（例：MyList@example.comのexample.com部分）
$SENDER$	メール送信者のメールアドレス
$FULLNAME$ $FIRSTNAME$ $LASTNAME$	メーリングリストメンバーの姓名、名、姓（利用可能な場合）
$EMAIL$	メーリングリストメンバーのメールアドレス

各メンバーに個別のRCPTコマンドを使用してリストメールを配信する
このオプションが有効にすると、MDaemonは指定されたスマートホストに対し、メンバー毎のメールコピーを送信します。この方法は、対象ホストとのSMTPセッション内で、複数ののRCPT TOコマンドを使用します。

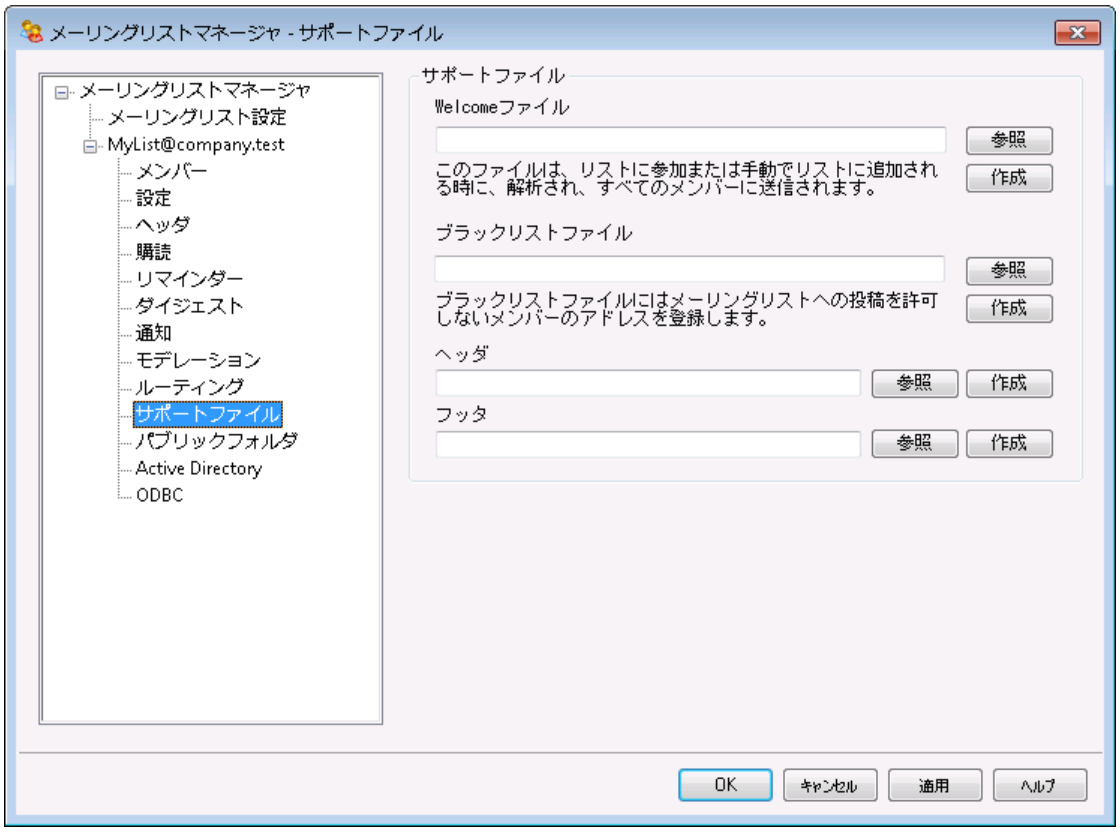
このホストへ配信
このオプションを選択すると、各メンバーに対しRCPT TOステートメントを使用して、すべてのリストメッセージの配信を渡すスマートホストを指定します。

AUTHログオン/パスワード
ホストが要求する認証情報です。

メッセージ毎にRCPTを [xx] 個までに制限する(0=制限なし)
いくつかのスマートホストは、メールをルーティングしようとすると、それを受け入れるRCPT TOステートメントの数を制限する場合があります。このコントロールで制限を指定する場合、MDaemonはメッセージの追加されたコピーを作成して、リストをより小さいグループに分けることによって機能します。そして制限を越えないように、その分割したグループにメールを配信します。これは前述であるリストメールを各メンバーへ配信するオプションと類似していますが、より少ないコピーを生成し各メンバーのために別々のコピーを生成しないでアドレスのグループに各コピーを送信します。

ホストへ送信時RCPTエラーを無視する
いくつかのスマートホストは、特定のドメインのメールキューあるいはメールスプールを拒否する場合があるので、メーリングリスト配信でのルーティングの使用は問題になる場合があります。この拒否の結果、スマートホストから返されるエラーコードによって、配信が中断されます。このオプションをチェックすると、MDaemonはルーティングされるメーリングリストの配信中にスマートホストからのエラーコードを無視します。それにより、メーリングリストのメンバーはメールを受け取ることができるようになります。

3.4.2.10 サポートファイル



サポート ファイル

W e l c o m e ファイル
ここで指 定 された内 容 はメーリングリスト の購 読 を開 始 したメンバーへのメール本 文 として送 信 されます。w e l c o m e ファイルの中 では、次 のマクロが使 用 できます:

$PRIMARYDOMAIN$	ドメインマネージャ 165 で指 定 しているMDaemonのデフォルトドメイン名 に置 き換 えられます。
$PRIMARYIP$	MDaemonの デフォルトドメイン 165 に紐 づいたIPv4アドレスへ置 き換 えられます。
$PRIMARYIP6$	MDaemonの デフォルトドメイン 165 に紐 づいたIPv6アドレスへ置 き換 えられます。
$DOMAINIP$	ドメインに紐 づいたIPv4アドレスへ置 き換 えられます。

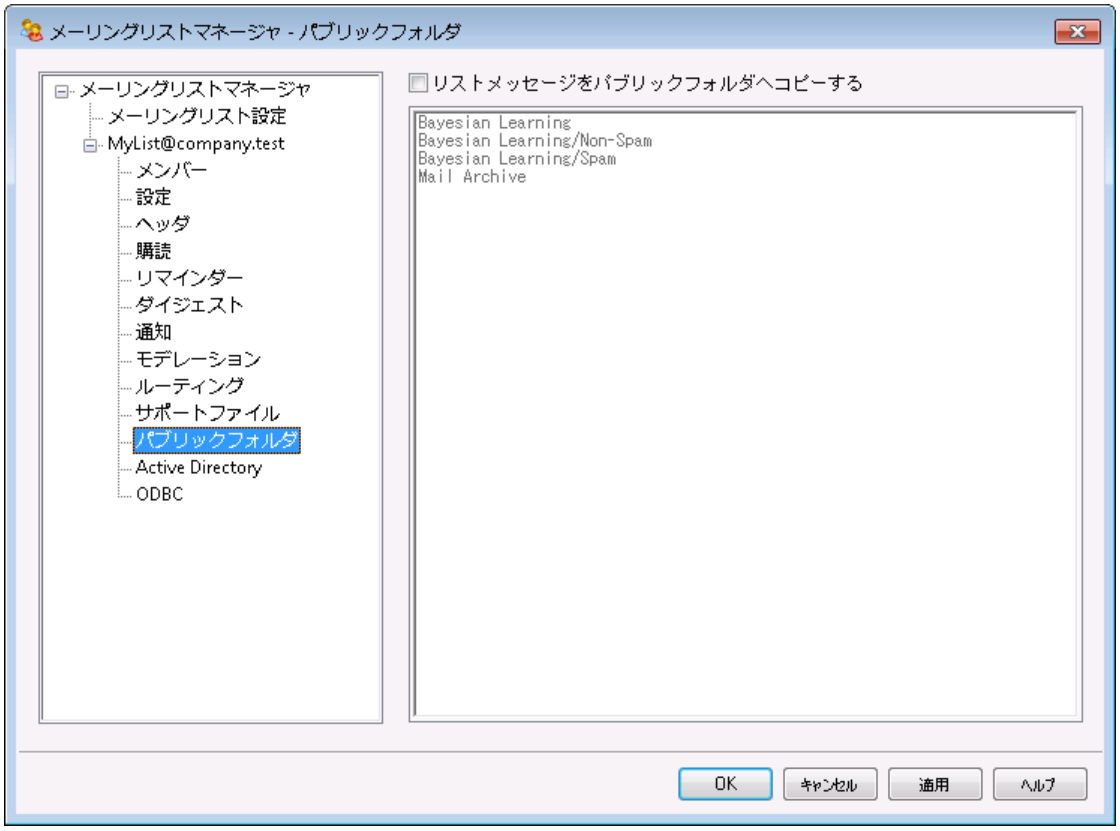
$DOMAINIP6$	ドメインに紐づいたIPv6アドレスへ置き換えられます。
$MACHINENAME$	ドメイン画面で指定したFQDNに置き換えられます。
$LISTEMAIL$	リストのメールアドレスを表示します。例: MyList@example.com
$LISTNAME$	メーリングリストの名前を表示します。例: MyList
$LISTDOMAIN$	メーリングリストのドメインを表示します。例: example.com
%SETSUBJECT%	Welcomeメッセージの件名に使用するマクロです。件名とするテキストには、$LI STEMAI L$といった、他のマクロも使用できます。例: %SetSubject%=Welcome to the $LISTNAME$ list.

ブロックリストファイル
ここで指定されたファイルは、特定ユーザから送信されるメッセージを隠すために使用されます。

ヘッダ/フッタファイル
ここに指定される内容をメーリングリストのヘッダまたはフッタとして使用します。

作成
新規のファイルを作成するには、作成するファイルに対応する**作成**ボタンをクリックし、ファイル名を指定して、**開く**をクリックします。ノートパッドで最近作ったファイルが表示されます。

3.4.2.11 パブリックフォルダ

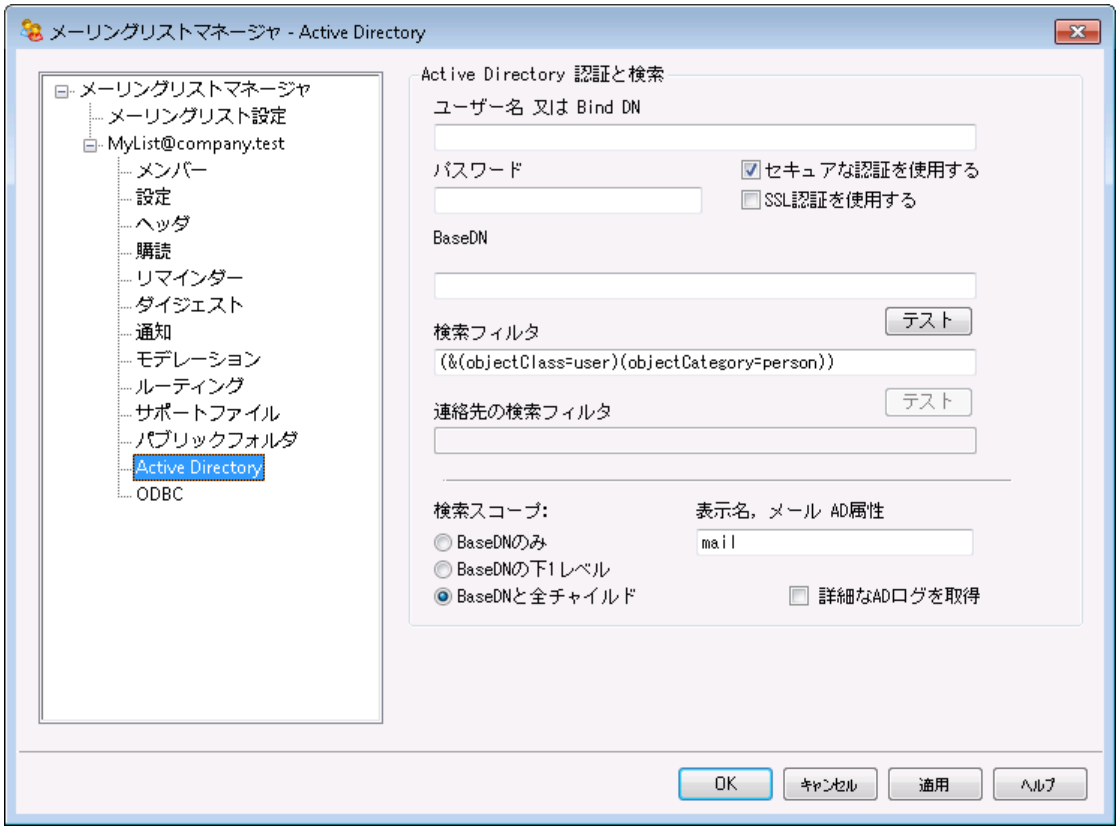


MDaemonは、メーリングリストでパブリックIMAPフォルダ[105]を使用をサポートします。1ユーザーのみがアクセスできる個人用IMAPフォルダと違い、パブリックフォルダは、複数のIMAPユーザが利用できる追加のフォルダです。この画面の上のオプションは、メーリングリスト宛てのすべてのメッセージを、指定されたパブリックフォルダへ自動的にコピーするために使用されます。

リストメッセージをパブリックフォルダへコピー
このメーリングリストのメッセージを配信とともに指定したパブリックフォルダにコピーする場合は、このコントロールを有効にしてください。

パブリックフォルダの選択
メッセージをコピーするパブリックフォルダを選択してください。

3.4.2.12 Active Directory



Active Directoryからメーリングリストメンバーのアドレスを取得するにはこのオプションを使用します。

Active Directory認証と検索

ユーザー名又はBind DN
Windowsアカウントのログオン名又は、LDAPを使用してActive Directoryにバインドする際に使用するDN(識別名)です。Active Directoryではバインドの際にWindowsアカウントやUPNの利用を許可しています。

このオプションでWindowsログオンではなくDN(識別名)を使用する場合は、以下の**セキュアな認証を使用**オプションを無効にしてください。

パスワード
上記の**Bind DN**オプションで使用するDNやWindowsログオンに対応するパスワードを入力してください。

セキュアな認証を使用する
Active Directory検索でセキュアな認証を使用するにはこのチェックボックスを有効にして下さい。上記のBind DNオプションでWindowsログインではなくDNを使用している場合、このオプションは利用できません。

SSL認証を使用する
Active Directory検索でSSL認証を使用するにはこのチェックボックスをクリックします。

このオプションを使用するにはSSLサーバーとWindowsネットワーク及びActive Directory用のインフラが必要です。ネットワーク構成が不明な場合はIT部門へ確認の上、このオプションを有効化するかどうかを判断して下さい。

BaseエントリDN
MDaemonがActive Directoryでアドレスを検索する際のディレクトリインフォメーションツリー(Directory Information Tree =DIT)の開始点、あるいは識別名(Distinguished Name =DN)を指定します。ここに"LDAP://rootDSE"を入力すると、MDaemonはRoot DSE(Active Directory階層の最上位)から検索を開始します。検索対象のユーザアカウントやグループに、より近い階層を指定する事で、検索時間を短縮する事ができます。Active Directoryからはアドレス検索を行わない場合は、ここを空白にしてください。

検索フィルタ
Active Directoryを検索する際に使用されるLDAP検索フィルタです。このフィルタを使用することにより、リストメンバーとするユーザアカウントやアドレスを、より正確な場所に配置することができます。

テスト
このボタンをクリックすると、Active Directoryの設定をテストすることができます。

表示名, mail AD属性
このリストで使用するメールアドレスを含む属性をここで指定する必要があります。例えば、このフィールドに"Mail"を入力すると、Active Directoryでリストメンバーとして扱う各アカウントは、メールアドレスを含む"Mail"属性を持たなくてはなりません。追加で、メーリングリストメンバーのメールアドレス属性の前に、カンマ区切りでフルネームのフィールドを入力する事ができます。例えば、"mail"ではなく"displayName, mail"と入力する事ができます。最初のActive Directory属性は、フルネームであり、2つ目の属性はメール属性となります。

検索スコープ:

ここではActive Directory検索の範囲を指定します。

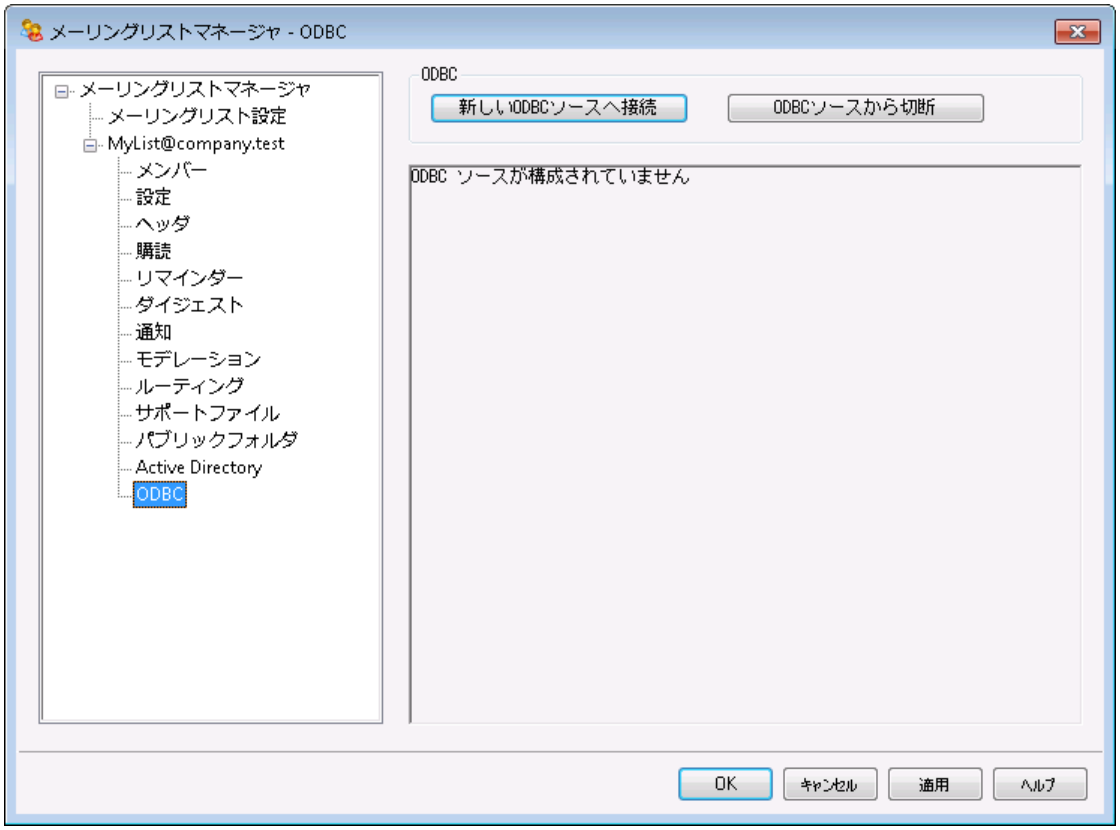
Base DN only
検索範囲を上記で指定したベースDNのみにする場合は、このオプションを選択してください。検索は、ツリー(DIT)でそのポイントより下に進みません。

BaseDNの下1レベル
DIT内の指定されたDNの1レベル下までActive Directory検索を広げる場合、このオプションを使用します。

BaseDNと全 チャイルド
DITで最も下 のチャイルドエントリまで、このオプションは提 供されたDNからチルドレンすべてまで検 索範 囲を拡 大します。これは、選 択されるデフォルト オプションで、上 記 のデフォルト Root DSE設 定と結 合 される時 に、Root DSE以 下 の全 てのDITが検 索されることを意 味します。

詳 細 なADログを取 得
デフォルト では MDaemonはActive Directory用 に詳 細 ログを使 用します。このチェックボックスを外すと、ログの詳 細 度 は低くなります。

3.4.2.13 ODBC



ーリングリスト エディタのODBC画 面 は、リスト にリンクするMDaemon用 のデータソース、テーブルおよびフィールド マッピングを選 択 するのに使 用します。ために用 います。メールが到 着 する度 に、SQLクエリが自 動 的 に実 行 され、その結 果 、メールアドレスが、リスト のメンバーの1つとなります。

ODBC対 応 データベースアプリケーションのデータベースであれば、これでリスト のメンバーを追 加 、削 除 、変 更 することができます。

ODBC

このセクションは、メーリングリスト に設 定 した現 在 のODBCプロパティを表 示します。各 メンバーのメンバーシップ状 況 (標 準 、投 函 のみ、受 信 のみまたはダイジェスト モード)を指 定 するために構 成 したデータベースのフィールド マッピングおよびSQLクエリを示します。

新しいODBCソースへ接続
このボタンをクリックし、メーリングリストを選択するためのODBC選択ウィザードを開きます。

ODBCソースから切断
上記で記載されるODBCデータソースからリストの接続を解除するためには、このボタンをクリックします。

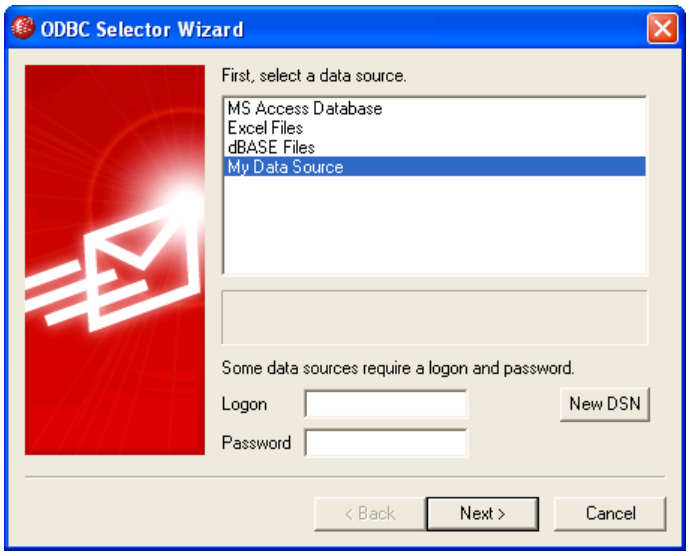
参照:

メーリングリスト用のＯＤＢＣシステムデータソースを構成する 277
新規システムデータソースを作成 279

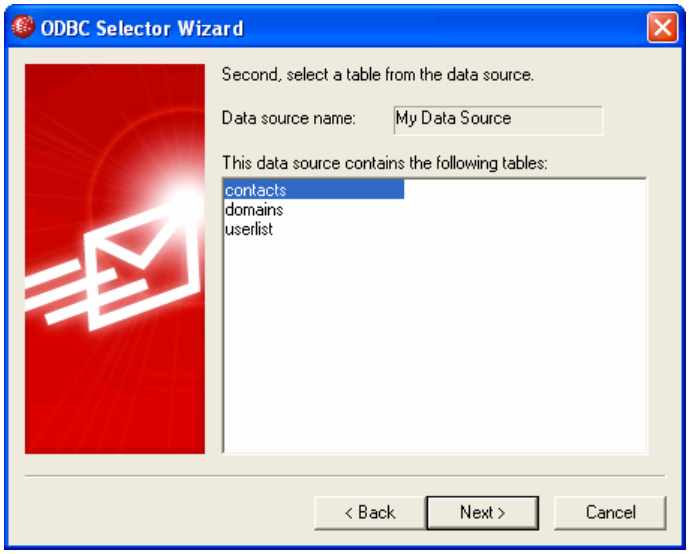
3.4.2.13.1 メーリング用ODBCデータソースの設定

メーリングリスト用のODBCアクセシブルデータベースを使用するには:

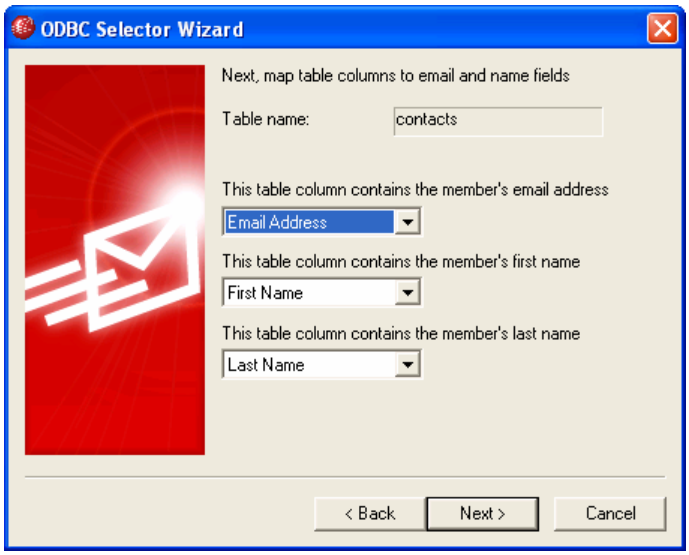
1. メーリングリストエディタのODBC画面 276 を選びます。ODBC選択ウィザードを開くために、**新しいＯＤＢＣソースへ接続** ボタンをクリックします。



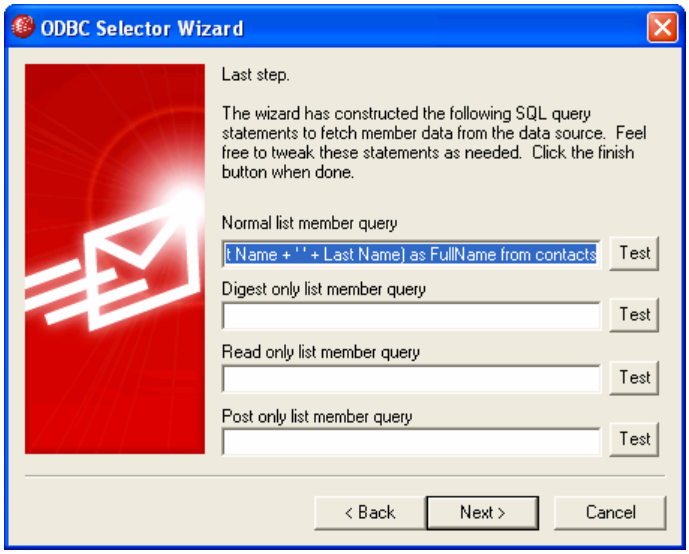
2. リストで使用するデータソースを選択します。データソースがない場合は、新しいDSNをクリックし新規ODBCデータソースの作成 279 指示に従いデータソースを作成します。
3. **ログオン名**と**パスワード**が必要な場合は、これらのフィールドに入力します。
4. **次へ**をクリックします。
5. データソースは、メールアドレスと名前のフィールドを持つテーブルが少なくとも1つなければなりません。この条件を満たす1つ以上のテーブルがある場合、使用するテーブルを選択して**次へ**をクリックしてください。それ以外の場合は、**キャンセル**をクリックしてウィザードを終了し、次の手順に進む前にデータベースアプリケーションを使用して、関連データベースにテーブルを追加してください。



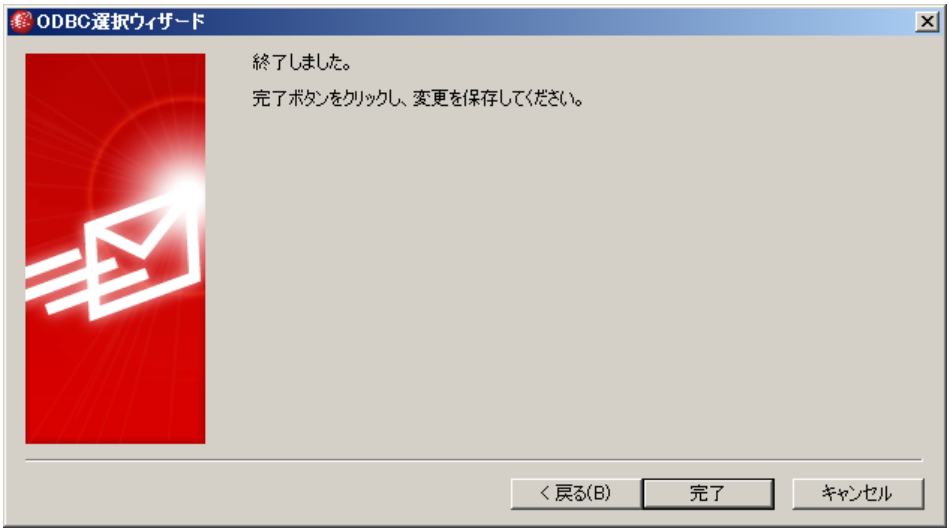
6. ドロップダウンリストを使用して、メールアドレス、苗字および名前に対応するテーブルフィールドを指定して**次へ**をクリックします。



7. ODBC選択ウィザードは、手順 6 で選択した内容に基づいてSQLステートメントを構成します。MDaemonは、それを使用してデータベースから標準メーリングリストメンバーのデータを検索します。メンバーにダイジェストモードでメールの受信またメンバーを受信専用あるいは投稿専用として指定するためにこのステートメントを編集、残りのコントロールで他のクエリステートメントを指定ことができます。各コントロールの横にあるテスト ボタンで、クエリステートメントが適切なデータを検索するかどうかを確認することができます。クエリのステートメントの構成が完了したら**次へ**ボタンをクリックします。



8. 完了をクリックします。



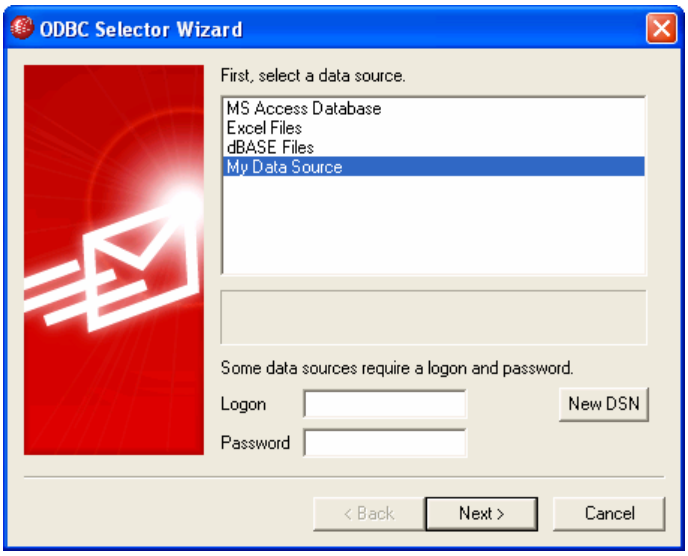
参照:

メーリングリストエディタ » ODBC 276
新規ODBCデータソースの作成 279

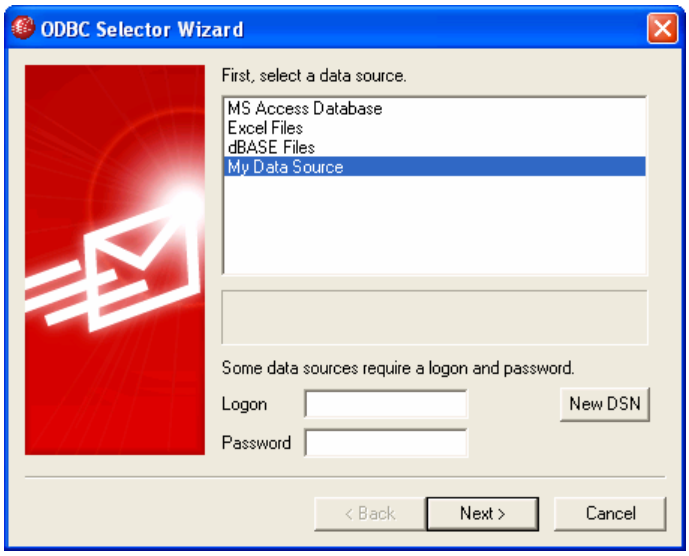
3.4.2.13.2 新規ODBCデータソースの作成

メーリングリストで使用するために、新しいODBCシステムデータソースを作成するには、

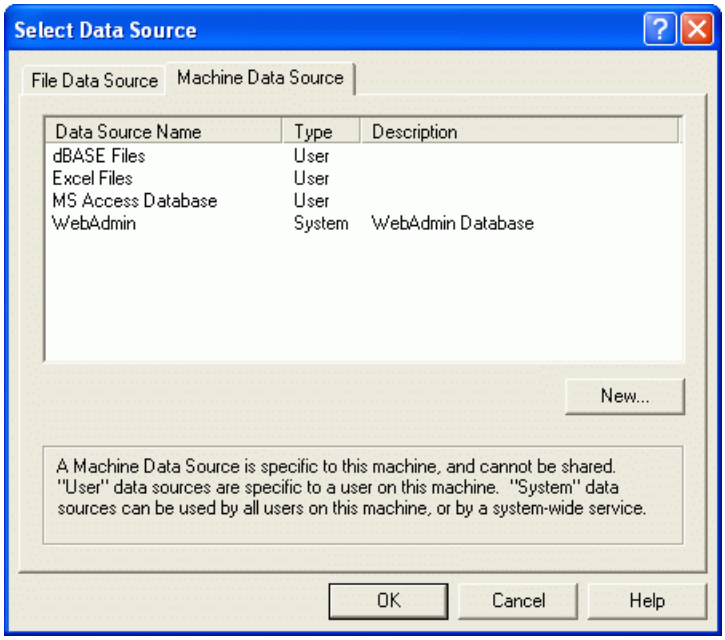
1. メーリングリストエディタのODBC画面 276を選びます。ODBC選択ウィザードを開くために、新しいODBCソースへ接続 ボタンをクリックします。



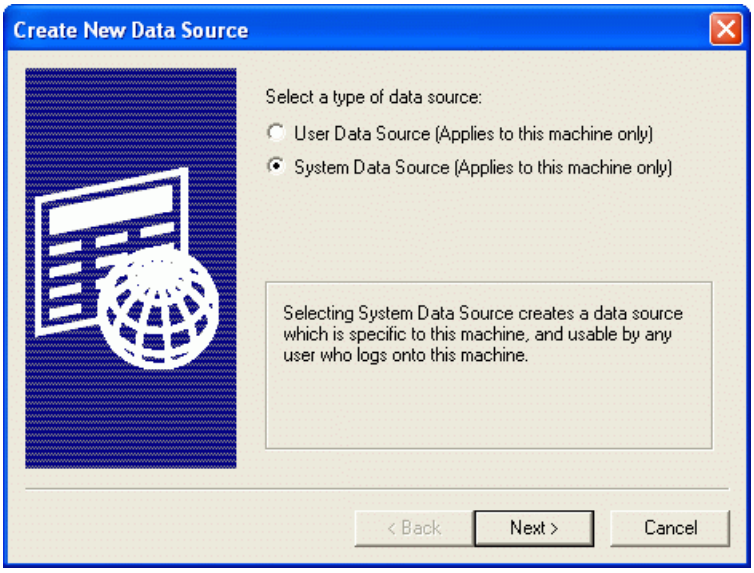
2. 新しいＤＳＮ ボタンをクリックし、データソースの選択画面を表示します。



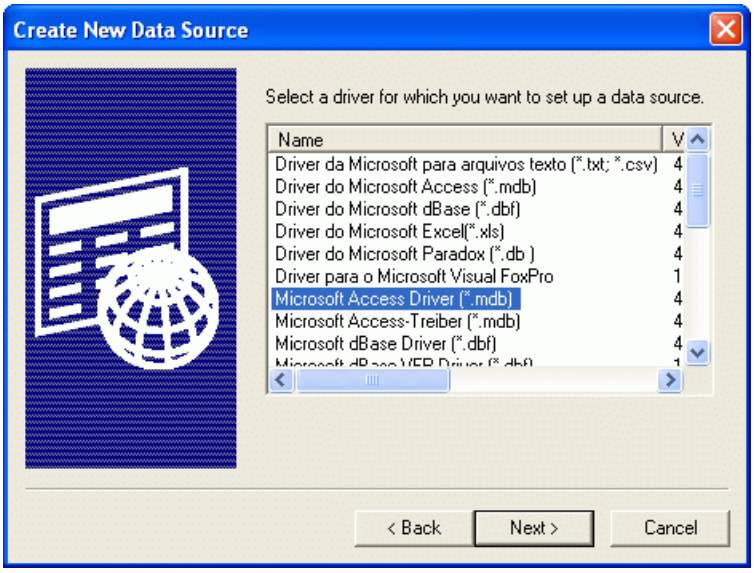
3. コンピュータデータソース 画面をクリックします。**新規作成...** ボタンをクリックしてデータソースの**新規作成**ダイアログを表示します。



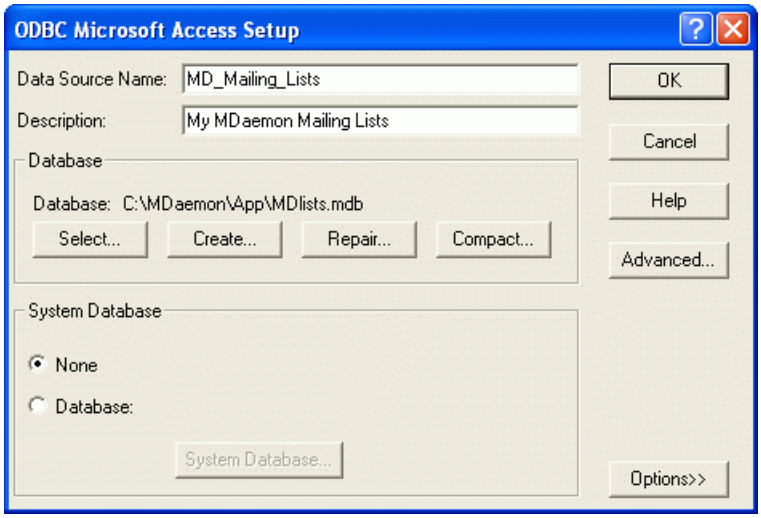
4. システムデータソースを選択して次へをクリックします。



5. データソースを設定するデータベースドライバを選択して次へをクリックします。



6. 完了をクリックして、ドライバ固有の設定ダイアログを表示します。このダイアログは選択したドライバによって表示が異なります(次の例はMicrosoft Accessの設定ダイアログです)



7. データソース名を指定し、ドライバ固有のダイアログ(データベースの指定や作成、ディレクトリやサーバの選択など)が必要とするその他の情報を指定してください。

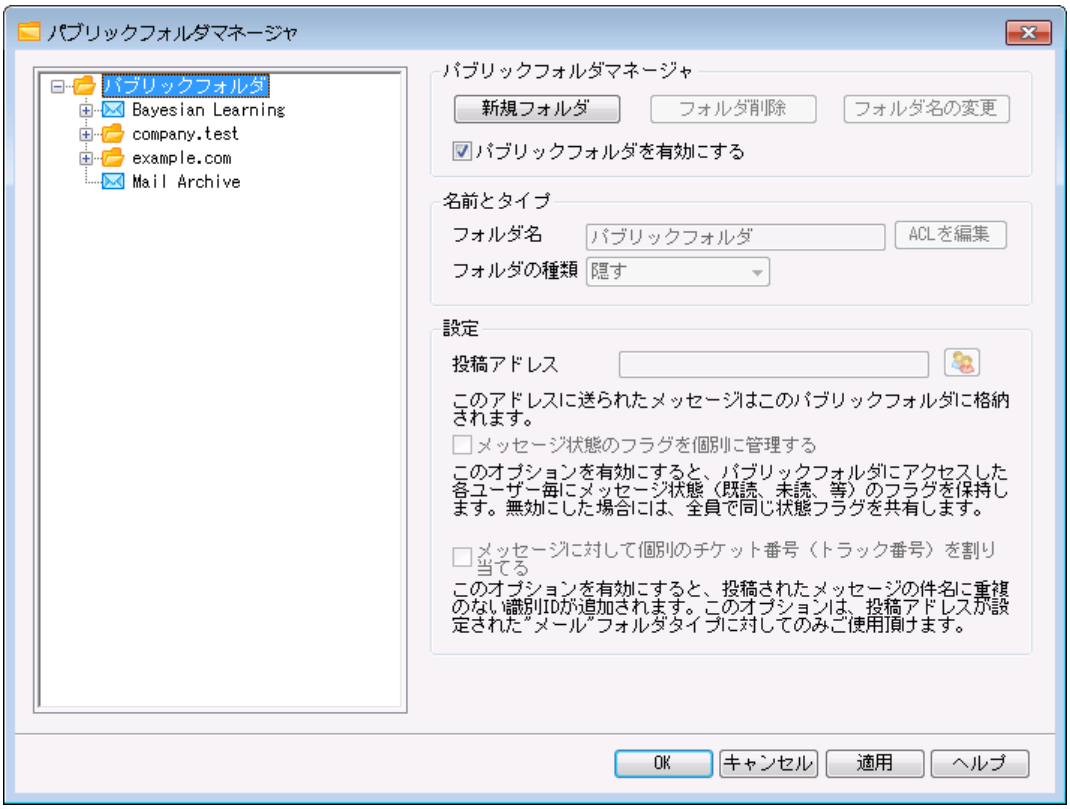
8. OKをクリックして、ドライバ固有のダイアログを閉じてください。

9. OKをクリックしてデータソースの選択ダイアログを閉じます。

参照:

ＯＤＢＣ － メーリングリスト 276
メーリングリスト用のＯＤＢＣシステムデータソースの設定 277

3.5 パブリックフォルダマネージャ

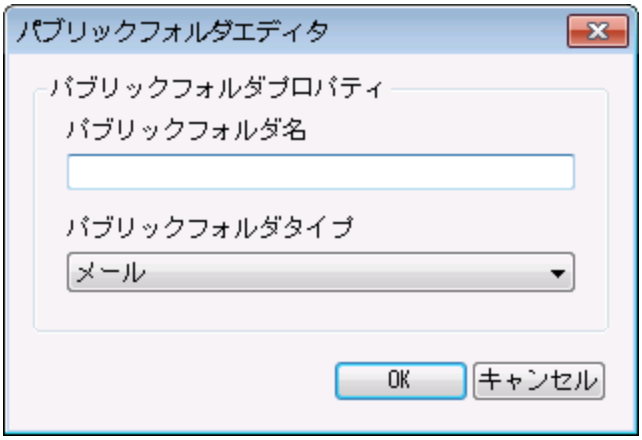


ここでは[パブリックフォルダ](#)105の管理が行えます。設定 » パブリックフォルダマネージャをクリックします。

パブリックフォルダの管理

新しいフォルダ

新しいパブリックフォルダを作成するには、親フォルダを選択し、「新規フォルダ」をクリックします。フォルダ名を入力し、種類を選択した後、OKボタンをクリックします。



フォルダの削除
パブリックフォルダを一覧から削除するには、対象フォルダを選択し、フォルダの削除をクリックします。

フォルダ名の変更
パブリックフォルダ名を変更するには、対象フォルダを選択し、フォルダ名の変更をクリックした後、フォルダ名を入力し、OKボタンを押します。

パブリックフォルダを有効にする
ユーザにパブリックフォルダへのアクセスを許可するには、このオプションを有効にしてください。アクセスできるユーザと、与えられるアクセスのレベルは、フォルダを選択して、「ACLを編集」をクリックした後設定する事ができます。

名前とタイプ

フォルダ名
フォルダ名をが表示されています。残りのオプションはこのフォルダに対して設定されたオプションです。

フォルダの種類
ドロップダウンからフォルダの種類を選択します。選択できるのは次のような種類です: メール、連絡先、予定表等

ACLを編集
フォルダを選択してこのボタンを押すとアクセスコントロールリスト 285ダイアログが起動します。ユーザーやグループ用のアクセスコントロールリストを使って各ユーザーやグループがフォルダへアクセスできるように設定して下さい。

設定

投稿アドレス
共有フォルダに関連付けるローカルメールアドレスを入力するか、MDaemonアカウントを選択すると、投稿アドレス宛てのメールは自動的に共有フォルダへルーティングされます。ただし、このアドレスへ投稿を行えるのは、「投稿」権限を持っているユーザーのみです。

メッセージ状態のフラグを個別に管理する
フォルダのメッセージフラグ(既読、未読、返信済み、転送済みなど)をユーザごとに設定する場合は、このチェックボックスを有効にしてください。各ユーザは、共有フォルダ内のメッセージに対する個人的な状態を見ることができます。例えば、メッセージを読んでいないユーザには[未読]フラグが表示され、読んだユーザには[既読]フラグが表示されます。このコントロールが無効の場合は、すべてのユーザに同じ状態が表示されます。つまり、1人のユーザがメッセージを読むと、すべてのユーザのメッセージが[既読]とマークされます。

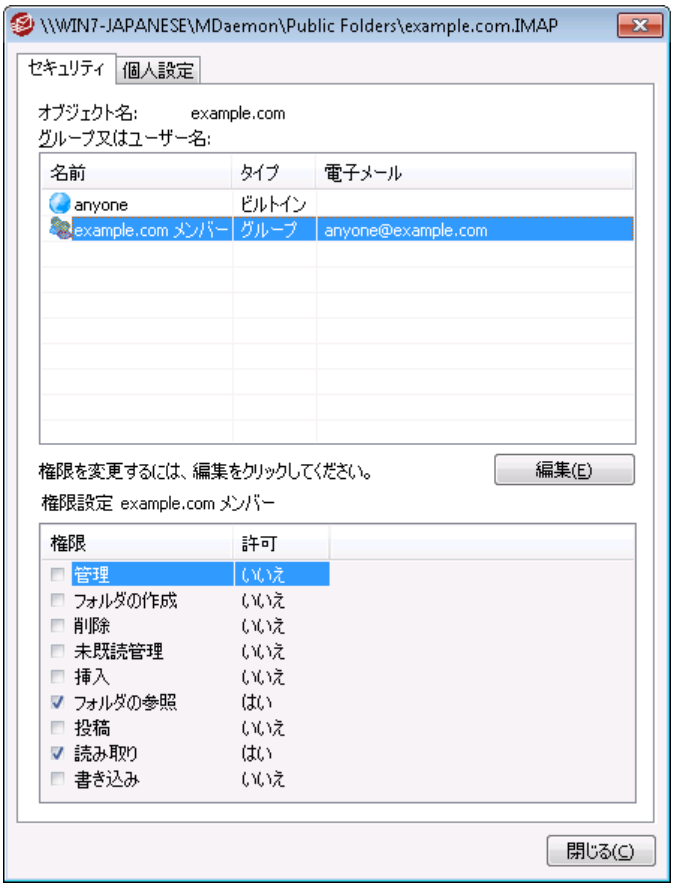
メッセージに対して個別のチケット番号(又はトラック番号)を割り当てる
パブリックフォルダをチケッティングパブリックフォルダとして設定する場合はこのオプションを使用します。MDaemonはフォルダ名と一意のIDを、投稿アドレスへ送信された全メッセージの件名に付与します。特殊なフォーマットの件名を持つ送信メッセージは「Reply To」というサブフォルダへ配送されます。さらに、特殊なフォーマットの件名を持つ受信メールは、宛先を問わず、自動的に対象パブリックフォルダへ配送されます。

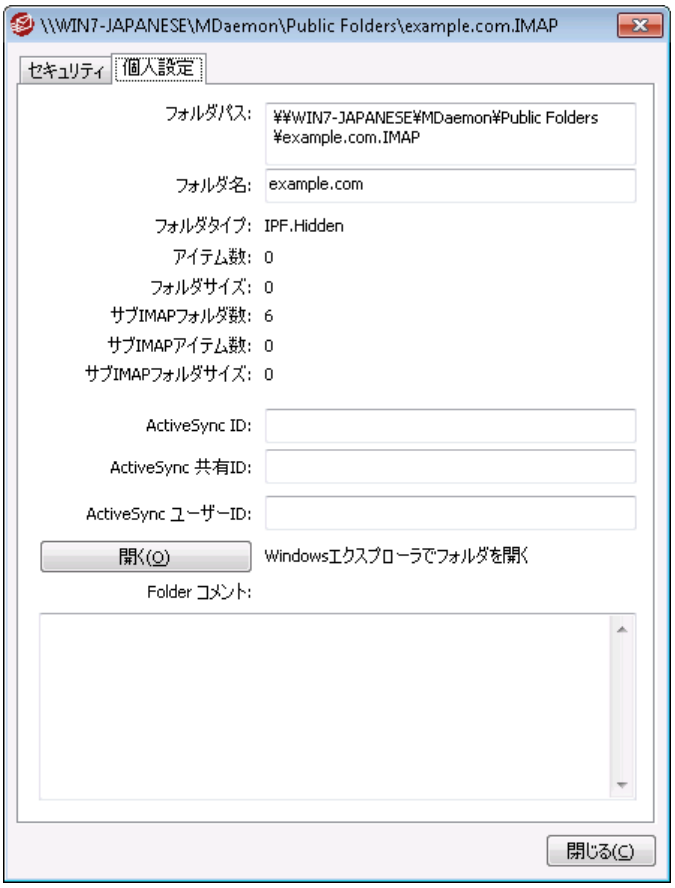
参照:

アクセスコントロールリスト 285
パブリックフォルダ Overview 105
パブリックと共有フォルダ 107
アカウントエディタ » 共有フォルダ 676
メーリングリスト » パブリックフォルダ 273

3.5.1 アクセスコントロールリスト

アクセスコントロールリスト（ACL）は、ユーザーやグループのパブリック及び共有フォルダ 105 に対するアクセス権を設定するのに使用します。パブリックフォルダマネージャ 283 のACLを編集ボタンか、アカウントエディタの 共有フォルダ 676 にある*アクセスコントロールリストの編集*ボタンをクリックし、この機能にアクセスできます。





セキュリティ

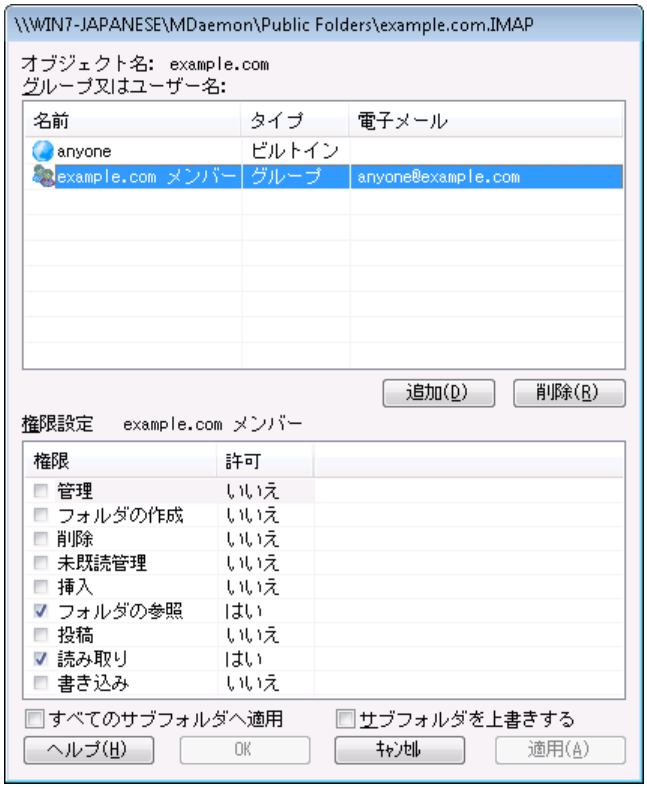
このタブにはフォルダに関連付けられたグループやユーザーの一覧と、詳細なアクセス権が表示されます。グループやユーザーを選択すると、下にあるアクセス権ウィンドウからそれぞれのアクセス権 288 が確認できます。アクセス権を編集するには編集 287 をクリックします。

個人設定

このタブにはフォルダのパスや名前、種類、サイズといった、プロパティが表示されます。

ACLエディタ

ACLのセキュリティタブで編集をクリックすると、ACLエディタが起動し、アクセス権の編集が行えます。



オブジェクト名
ACLアクセス権が適用されるオブジェクトやフォルダ名です。

グループ又はユーザー名
何らかのアクセス権限を持つグループやユーザーです。グループやユーザーを選択すると、権限設定ウィンドウにアクセス権が表示されます。アクセス権に並んで表示されているボックスをクリックする事で、対象のアクセス権限を割り当てる事ができます。

追加
一覧に表示されていないグループやユーザーを追加するには、追加 289をクリックします。

削除
グループやユーザーを削除するには対象のエントリを選択し、削除をクリックします。

<グループやユーザー>の権限設定
アクセス権限の隣にあるボックスをクリックする事で、上部で選択したグループやユーザーに対象のアクセス権限を割り当てる事ができます。

次のアクセス権限を選択できます。

管理者 – ユーザは、このフォルダのACL(アクセスコントロールリスト)を管理することができます。

作成 – ユーザは、このフォルダ中でサブフォルダを作成することができます。

削除 – ユーザは、このフォルダからメッセージを削除することができます。

未既読管理 – ユーザは、このフォルダのメッセージの既読/未読の状態を変更することができます。

挿入 – ユーザは、このフォルダにメッセージを追加したりコピーすることができます。

ルックアップ – ユーザは、IMAPフォルダの個人的なリストの中で、このフォルダを見ることができます。

投稿 – ユーザは、このフォルダに直接メールを送ることができます(フォルダが許可されている場合)。

読み込み – ユーザは、このフォルダを開いて、その内容を見ることができます。

書き込み – ユーザは、このフォルダのメッセージのフラグを変更することができます。

全てのサブフォルダへ適用
このフォルダのアクセス権を作成済のサブフォルダ全てに適用する場合はこのオプションを有効にします。フォルダのユーザー及びグループアクセス権がサブフォルダへ適用され、競合するアクセス権は上書きされます。しかし、現在既に設定されているアクセス権が削除される事はありません。

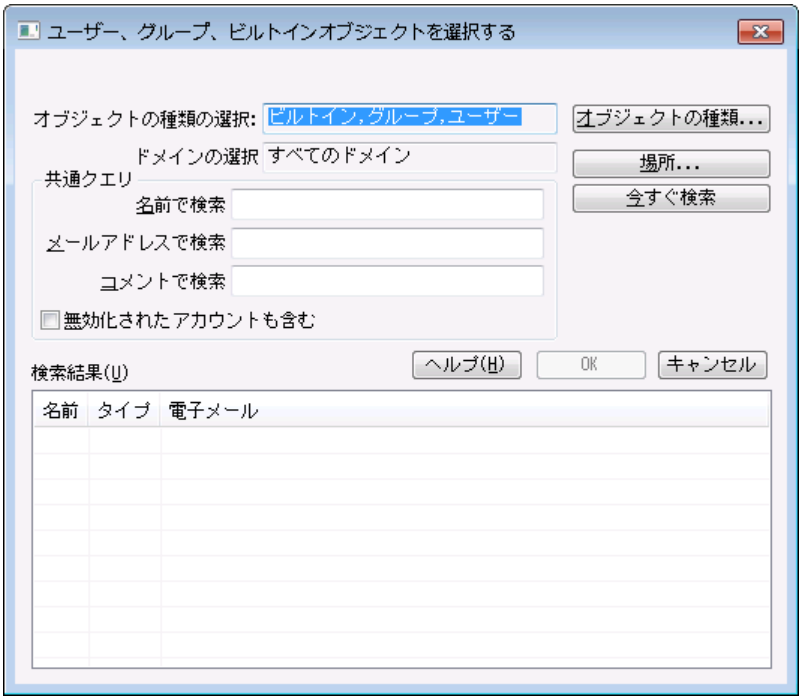
例えば

上位のフォルダがユーザーAとユーザーBに特定のアクセス権を割り当てており、サブフォルダはユーザーBとユーザーCにアクセス権を割り当てていたとします。このオプションではユーザーAのアクセス権をサブフォルダにも適用し、ユーザーBのサブフォルダに対する既存のアクセス権を上書きし、ユーザーCに対しては何の処理も行いません。そのため、サブフォルダはユーザーAとユーザーB、ユーザーCに対するアクセス権を持つことになります。

サブフォルダを上書きする
この設定を有効にすると、サブフォルダの全てのアクセス権が上位フォルダのアクセス権で上書きされます。サブフォルダのアクセス権は上位フォルダと同じものに設定されます。

グループやユーザーの追加

ACLエディタで追加をクリックし、グループやユーザーの追加用画面から検索や追加を行う事で、アクセスコントロールリストへグループやユーザーを追加できます。



オブジェクトの種類の選択
オブジェクトの種類をクリックし、追加したいグループやユーザーの種類を、ビルトイン、グループ、ユーザーの中から選択します。

場所の指定
場所をクリックし検索対象のドメインを選択します。ここでは全てのMDaemonドメインや特定のドメインを選択できます。

共通クエリ
このオプションを使用し、ユーザー名やメールアドレス、アカウントの説明[650]の一部を指定する事で、検索範囲を狭くする事ができます。オブジェクトの種類や場所に一致する全てのグループやユーザーを対象に検索を行う場合は、この項目を空白にして下さい。

無効化されたアカウントも含む
検索対象に無効化されたアカウント[650]も含む場合はこれをチェックします。

今すぐ検索
検索条件を指定した後、今すぐ検索をクリックし検索を行います。

検索結果
検索実行後、検索結果からグループやユーザーを選択し、OKをクリックする事で、対象グループやユーザーをACLへ追加できます。

アクセス権はMDaemonのACL(アクセスコントロールリスト)サポートによってコントロールされます。ACLは、IMAP4(インターネットメッセージアクセスプロ

トコル)の拡張機能で、IMAPメールボックスにアクセス権限を割り当てるためのもので、これを使って他ユーザーにもフォルダに対するアクセス権限を与える事ができるようになっています。メールクライアントがACLに対応していない場合であっても、このダイアログからアクセス権限の設定が行えます。

ACLはRFC 2086で定義されており、次のサイトからご覧頂けます: http://www.rfc-editor.org/rfc/rfc2086.txt.

参照:

パブリックフォルダマネージャ 283
パブリックフォルダについて 105
パブリックと共有フォルダ 107
アカウントエディタ » 共有フォルダ 676
メーリングリスト » パブリックフォルダ 273

3.6 WebとIM サービス

3.6.1 Webmail

3.6.1.1 概要

MDaemon Webmailは、ウェブブラウザからメールクライアントの機能を利用するために開発された、MDaemonに標準パッケージされているウェブメールソリューションです。Webmailは従来のメールクライアントと同等な機能はもちろん追加機能も標準搭載されており、ユーザーはインターネット接続できる環境さえあれば、こうした機能をどこからでも利用する事ができます。さらに、全てのメールフォルダ、連絡先、カレンダーが、ローカルコンピュータではなくサーバで管理されるため、ユーザーはデスクにいる時と同様に、全ての情報にアクセスする事ができます。

管理者にとって、Webmailは様々なメリットがあります。まず、Webmailは、多くのクライアントアプリケーションとは異なり、クライアントの環境に依存する事なく、サーバーで全て管理する事ができます。インターフェイスの画像やHTMLをカスタマイズすることによって、社内や顧客のニーズに沿った環境を構築する事ができます。さらに、ユーザ自身でも個人のアカウント設定が行え、設定できる範囲については環境に応じて決定できるため、管理負荷を軽減する事ができます。

最後に、ウェブメールとしての便利さに加えて、Webmailでは、拡張メール機能、30カ国語言語対応、個人・全体アドレス帳、メールフォルダとフィルタリング、添付ファイルの送受信、複数の視覚的に異なるテーマ、モバイル対応、予定表、グループウェア、メッセンジャー等、ユーザーに役立つ多くの追加機能を搭載しています。

カレンダーとスケジュールシステム

MDaemonには、統合連携システムが搭載されており、簡単に、会議や打合せ予定を作成したり、アドレス帳を管理することができます。繰り返し予定にも完全対応しており、個々の予定の登録には、詳細な情報を記述するための多くのフィールドが用意されています。更に、連絡先、予定表、仕事などのデータは、各ユーザのメールのルートディレクトリにあるIMAPフォルダに保存されます。各ユーザはWebmailを経由して、これらのパーソナルなフォルダにアクセスすることができ、また他のユーザからのアクセ

スをコントロールすることもできます。すべてのテーマ(特にLookOutテーマ)には、連絡先や予定表、仕事、メモフォルダがテンプレート化されています。

予定表システムがMDaemonと一体型である事で、スケジュール管理で行うメール通知においても、追加のメリットがあります。自分以外の第3者が打合せの予定を追加した際、打合せに関する通知メールが送られます。打合せの出席予定者は、打合せの日時や場所、内容、その他出席者等の詳細情報が記載された通知メールを受け取る事ができます。更に、打合せの時間帯に既に別の予定が入っている出席者は、打合せの予定と、指定の時間に別の予定と競合している旨が通知されます。打合せの予定を追加した人は、打合せの詳細と、出席予定者に他の予定が入っているかどうかの通知を受け取ります。

また、カレンダーシステムは、Microsoft Outlookやその他のiCalendar互換のメールプログラムが使用するインターネットカレンダー(iCal)にも対応しています。カレンダーシステムは、ユーザに送られたiCalendar情報を検知し、その情報に基づいてカレンダーを更新します。ユーザが、Webmail内からiCalendarの添付ファイルを開くと、添付ファイルに含まれていた情報は、ユーザのWebmailカレンダーに反映されます。また、ユーザが新しい打合せを追加する際、iCalenderメールを送信するメールアドレスを指定する事もできます。この機能はWebmailオプションでユーザーが個別に設定できます。

MDaemon Instant Messenger

MDaemon Instant Messenger(MDIM)は、MDaemonのセキュアなインスタントメッセージングクライアントで、Webmail機能へ素早くアクセスするためのアプレットも搭載しています。MDIMは、Webmailユーザ毎にダウンロードし、インストールできます。ダウンロードの時点で事前設定が行われるため、手動で設定を行う必要はほとんどありません。

MDIMは、バックグラウンドで、新規メールのチェックを直接Webmailサーバに対して行います。これにより、新規メールをチェックするために、ブラウザを開くこと、あるいは開いたままにしておく必要がなくなります。サウンドまたは視覚的なアラートによって、新規メールの到着を知らせます。また、メールフォルダのリスト、メッセージの数、未既読情報を表示します。更に、ブラウザを起動し、特定のメールフォルダへ素早くアクセスする事ができます。

また、MDIMはインスタントメッセージシステムも搭載しており、[仲間]リストの表示、それぞれのオンライン状態(オンライン離席中オフライン)、その中の一人あるいはグループ全体での会話の開始、自分のオンライン状態の設定、historyフォルダで過去の会話の確認なども行えます。

MDaemon Instant Messengerの使用方法についてはオンラインヘルプをご覧ください。

MDaemon Instant Messengerのインスタントメッセージ

MDIMにはMDaemonのXMPP 340 サーバーで利用できるインスタントメッセージ(IM)クライアントが搭載されています。これを使う事で、ドメイン(及びオプションとしてMDaemonサーバーで管理している別ドメイン)を共有している他のユーザーをMDIM連絡先一覧へ追加し、いつでも簡単にコミュニケーションを図る事ができます。オンラインステータスの設定や、連絡先のステータス確認、エモーションの利用、テキストカラーの設定、ファイル送信、通知音の設定、その他初期設定の管理が行えます。また、複数の連絡先と一度に行うグループチャットも利用できます。IM機能はトレイアイコンのショートカットメニューやMDIMウィンドウからも実行する事ができます。

MDIMのインスタントメッセージはスクリプトにも対応しており、独自のプログラムとも連携させる事ができます。¥MDaemon¥WorldClient¥フォルダでセマフォ(SEM)ファイルを作成することによって、外部アプリケーションは、MDIMユーザにインスタントメッセージを送信することができます。SEMファイルのフォーマットは次の通りです:

To: user1@example.com　　MDIM ユーザのメールアドレス

From: user2@example.com	インスタントメッセージ送信者のメールアドレス
<blank line>	
Text of instant message.	インスタントメッセージで送信されたテキスト

SEMファイルの名前は、"IM-"という文字に続いて重複のない数字が続きます。例えば、"IM-0001.SEM"となります。また、アプリケーション側でSEMファイルをロックするため、それぞれに対応した"IM-0001.LCK"というファイルを作成します。SEMファイルが完了すると、LCKファイルは削除されSEMファイルが処理されます。MDaemonは、今後の予定についてインスタントメッセージ経由のリマインダーを送る際に、このスクリプティング方式を使用しています。

インスタントメッセージの送信用のスクリプティング方式は、アクションとしてコンテンツフィルタの中に搭載されています。また、このアクションを使っているルールではIMのコンテンツフィルタマクロを使用する事ができます。例えば、インスタントメッセージを送るためのルールとして、次のような指定を行う事ができます。

```
$SENDER$からのメールを受信しました。
件名:  $SUBJECT$
```

このルールは、MDIM経由で新しいメール通知を行うのに効果的な方法です。

従来、IMシステムの社内利用は、一元管理の難しさやトラフィックの監視機能の不足が原因で、その利用が敬遠されてきました。こうした問題を最小限にするようMDIMは設計されています。最初に、MDIMのシステムは、クライアントが直接ピアツーピアで接続しません。すべてのIMがサーバを経由するので、各メッセージはMDaemonの管理者がアクセスしやすい場所に記録されます。全ての会話を記録する事で、会社や従業員、ユーザーのセキュリティを守る事ができます。IMに関する記録は、MDaemon¥LOGS¥ディレクトリにあるXMPPServer-<date>.logと呼ばれるファイルに記録されます。

インスタントメッセージはドメインごとに提供されます。インスタントメッセージの全体設定はWebmailのMDIM画面[304]（設定 ≫ ウェブとIMサービス ≫ MDIM）から行う事ができます。ドメインマネージャ[173]にも同様の設定画面があり、ここからドメイン毎に設定の有効化や無効化が行えます。

MDaemon Instant Messengerスキン

MDIMのインターフェイスは、インターネットで入手できるmsstyle のスキンと互換性を持っています。様々なスタイルが含まれてはいますが、新しいスタイルをインストールするには、`*.msstyles` を、MDIMの ¥Styles¥ フォルダ以下に、ファイル名と同じ名前のサブフォルダを作成し、その中にダウンロードします。例えば Red.msstyles の場合、フォルダは `\.\Styles\Red\Red.msstyles` となります。

Dropbox連携

Ctrl+W | Webmail| Dropboxへ新しい設定画面が追加されました。ここではDropboxの「app key」や「app secret」、プライバシーポリシーの文言を追加する事ができます。 ここでの情報は連携のために必要な情報で、Dropboxのウェブサイトでwebmailをdropboxのアプリとして登録するのに使われます。これは管理者が自分で行う必要のある設定ですが、一度設定を行えば、その後の設定は必要ありません。DropboxでWebmailをアプリとして登録する手順についてはナレッジベース1166を参照して下さい。

app keyとapp secretが設定されると、Webmailから各アカウントがDropboxアカウントへ接続できるようになります。ユーザーがWorldClientやLookOutテーマで最初にログインした際、ページの上部へドロップダウンメニューが表示されます。ここへは「次回ログイン時にドロップダウンメニューを表示」「今後このオプションを表示しない」「新しいオプション | クラウドAppへ移動する」という3つのオプションがあり、Dropbox設定ボタンを押す事ができます。このボタンを押すとOAuth 2.0ポップアップが表示されます。

ポップアップではユーザーの接続先やWebmailで必要な認証情報の詳細が表示されます。また、ここへはプライバシーポリシーと「Dropboxへ接続」ボタンが表示されます。ユーザーが「Dropboxへ接続」ボタンをクリックすると、Dropboxへ移動します。ユーザーがDropboxへログインしていない場合、Dropboxはログイン又はアカウント作成の画面へ移動します。このステップが完了すると、ユーザーはWebmailへアカウントに対するフルアクセス権を与えるかどうかの確認ページへ移動します。「許可」をクリックすると、ユーザーは元の画面へ戻り、認証が成功したかどうかを示すメッセージが表示されます。認証情報は1週間使用する事ができ、次の1週間用には、もう一度同じアクセストークンで認証を行う必要があります。認証が行われると、ユーザーの受信メール画面にて、添付ファイルの隣にDropboxのアイコンが表示されます。アイコンをクリックすると、添付ファイルがユーザーのDropboxアカウントの/Webmail_Attachmentsフォルダへ保管されます。

WorldClientとLookOutのメール作成画面では、ユーザーは、HTMLエディタのツールバーにある(左上の)アイコンをクリックし、Dropboxアカウントのファイルを選択する事ができるようになります。この機能を使うのに、ユーザーはオプション | Cloud Appからアカウントや OAuth 2.0の設定を行う必要はありません。app keyとapp secretのみが必要です。

Dropbox対応はデフォルトで無効に設定されていますが、MDaemonのDropbox[309]画面で有効化できます。ユーザー毎にDropboxの有効化や無効化を行うには、User.iniへDropboxAccessEnabled=Yesを追加して下さい。

Webmailの利用

Webmailの開始

Webmailサーバーの開始と終了を行うには、3つの方法があります:

1. MDaemon GUIの左側にあるStats画面で、Webmailを右クリックし、「有効/無効を切り替える」を選択します。
2. "ファイル » Webmailを有効化" をクリックします。
3. "設定 » Web & IMサービス" をクリックし、ウェブサーバー画面で、Webmailを内蔵ウェブサーバーで実行をクリックします。

Webmailへのログイン

1. ブラウザで、http://example.com:Webmailポート番号を入力します。ポート番号の設定はWebサーバー[295]で行います。Webmailでデフォルトのウェブ用ポート(ポート80)を使用するよう設定していた場合は、URLにポート番号の指定を行う必要はありません。(例えば、www.example.com:3000ではなく、www.example.com と指定します)
2. MDaemonアカウントのユーザー名とパスワードを入力します。
3. ログインをクリックします。

Webmailの通信ポートの設定

1. メニューバーの "設定 » Web & IMサービス" をクリックします。
2. *Webmail サーバーをこの TCPポートで使用する.*へ、任意のポート番号を入力します。
3. OKをクリックします。

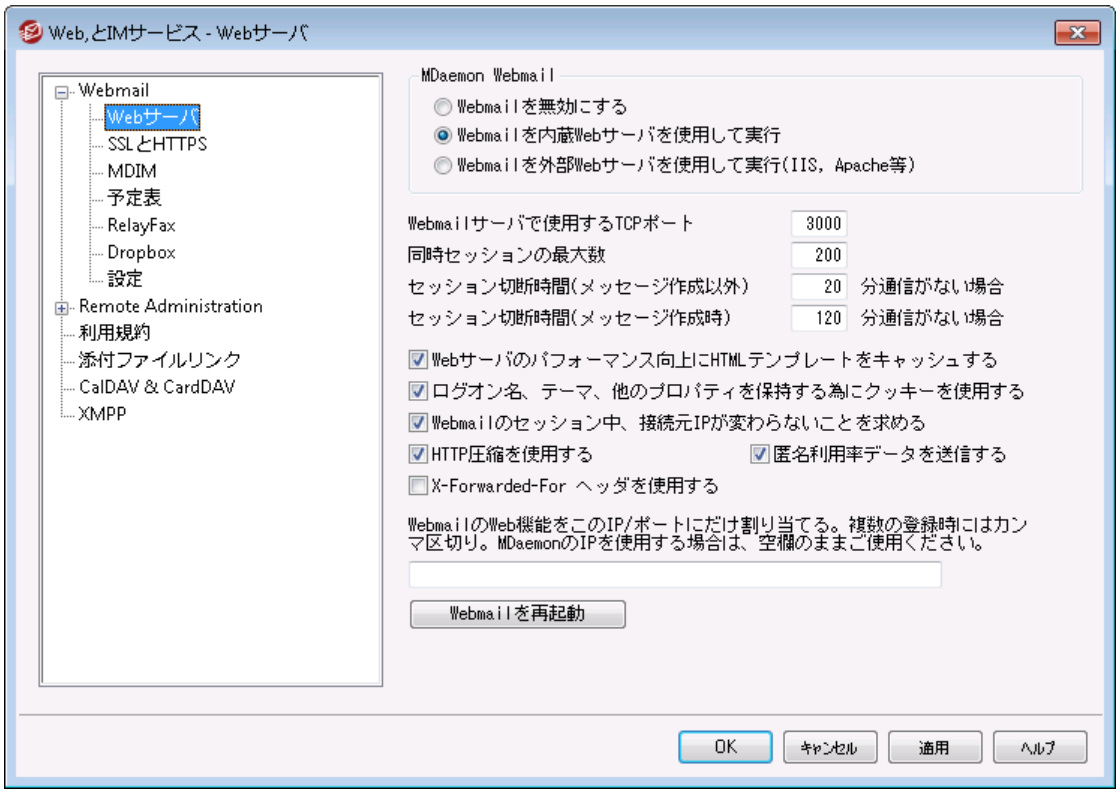
クライアント向けのヘルプ情報

Webmailにはユーザー向けのヘルプファイルが搭載されています。クライアント向けの機能については、Webmailからアクセスできるヘルプファイルを参照して下さい。

アドレス帳オプションに関する詳細は下記を参照して下さい:

Webmail » MDIM 304
LDAP 754

3.6.1.2 Webサーバー



この画面では、Webmailについて、ユーザーやドメインに依存しない全体設定を行えます。

MDaemon Webmail

Webmailを無効にする
Webmailを無効にするには、このオプションを選択してください。Webmailの有効化/無効化は、MDaemon管理画面のメインにある統計情報フレームやファイルメニューからも切り替えることができます。

添付ファイルリンク[333]機能を使用するには、Webmailが有効になっている必要があります。

Webmailは内蔵Webサーバを使用して実行
MDaemonが内蔵しているWebサーバを使って、Webmailを有効にする際、このオプションを使用します。Webmailの有効化/無効化は、MDaemon管理画面のメインにある統計情報フレームやファイルメニューからも切り替えることができます。

Webmailは外部Webサーバを使用して実行(IIS, Apache等)
MDaemonが内蔵しているWebサーバの代わりに、Internet Information Server (IIS)やその他のWebサーバを使って、Webmailを実行する際、このオプションを選択してください。これにより、他のWebサーバとGUI画面表示において、衝突が発生することを防ぎます。

詳細は、IIS6でWebmailを実行する[297]をご覧ください。

WebmailサーバでTCPポート
Webmailが、ユーザのウェブブラウザからの接続を受け付けるポート番号を指定します。

同時セッション数の最大値
Webmailへ同時に接続できるセッション数の最大値を指定します。

セッション切断時間(メッセージ作成以外)
Webmailへログインした後、自動的にWebmailセッションを終了させるまでに、ユーザーが操作を何もしない時間を指定します。ただし、メッセージを作成中の場合は除きます。ここで指定した時間の間、ユーザーが操作を行なわない場合、自動的にWebmailセッションは終了します。

セッション切断時間(メッセージ作成時)
ここで指定する時間は、Webmailへログインした後、ユーザーがメッセージを作成中でありながらも、かつ無操作であった場合に、どれくらい待ってからWebmailセッションを終了させるかを指定します。通常は、ユーザがメッセージを作成する際、非アクティブの方が長いため、*[セッション切断時間(メッセージ作成時以外)]*よりも長くなるように設定すると良いでしょう。なぜならば、メッセージの作成中は、そのメッセージが送信されるまでサーバとの通信が発生せず、無操作とみなされてしまうためです。

Webサーバのパフォーマンス向上にHTMLテンプレートをキャッシュする
このチェックボックスを有効にすると、Webmailはメモリ上にテンプレートをキャッシュするため、アクセスされる都度読み込むのに比べ、パフォーマンスが飛躍的に向上します。ただし、テンプレートファイルを変更した場合には、Webmailを再起動する必要があります。

ログオン名、テーマ、他のプロパティを残すためにクッキーを使用する
このチェックボックスを有効にすると、Webmailは各ユーザのログオン名、テーマ、その他のプロパティ情報を格納したCookieをそのユーザのローカルコンピュータに格納させることができます。この機能を使うことで、前回のログイン時の情報を引き継ぐことができるため便利ですが、ブラウザ側でCookieのサポートが有効になっている必要があります。

Webmailセッションを通してIPパーシステンスを使用する
セキュリティ対策の追加機能として、このチェックボックスを有効にすると、Webmailは各ユーザーのセッション開始時に接続されたIPアドレスとだけ通信を行なうようにできます。これにより、IPアドレスを継続的に要求するため、他人がそのセッションを"盗む"ことができなくなります。この設定は、より確実

なセキュリティを確保することができますが、プロキシーサーバを使っている環境やIPアドレスが動的に変わる環境では、逆に接続できなくなる可能性があることにご注意ください。

X-Forwarded-Forヘッダを使用する
X-Forwarded-Forヘッダを使用するにはこのオプションをクリックします。このヘッダはプロキシーサーバーによって追加される事もあります。このオプションはデフォルトで無効になっています。プロキシーサーバーがこのヘッダを追加する場合のみこのオプションを有効にしてください。

HTTP圧縮を使用
このチェックボックスを有効にすると、Webmailセッションにおいて、HTTP圧縮を使用することができます。

匿名利用率データを送信する
デフォルトでWebmailは匿名で、使用OSやブラウザバージョン、言語、といった情報を送信します。このデータはMDaemon TechnologiesでWebmailの機能向上を目的に使用されます。匿名使用率データを送信したくない場合はこのオプションを無効にして下さい。

WebmailのWeb機能をこれらのIP/ポート番号にだけ割り当てる
Webmailtサーバ機能を特定のIPアドレスとポート番号だけに制限をしたい場合、ここでIPアドレスとカンマで区切ったポート番号を指定します。"IP_address:Port"の書式(例:192.0.2.0:80)で指定します。ポート番号の指定しなかった場合は、SSL & HTTPS[300]画面で指定したデフォルトのtcpポートとHTTPSポートが使用されます。全てのポートを使用するには、"*"を使って下さい。例えば "*,*:80" を指定するとWebmailは、全てのIPアドレスのデフォルトポート(3000と443)を使用し、且つ、全てのIPアドレスの80番ポートを使用します。このフィールドを空欄にすると、Webmailはドメイン[165]で指定した全てのIPアドレスを使用します。

Webmailを再起動(Port番号やIISの設定値を変更した場合に必要)
このボタンをクリックすると、Webmail サーバが再起動されます。注意:Webmailのポート設定を変更した時は、変更を反映するためにWebmailを再起動する必要があります。

3.6.1.2.1 IIS6でWebmailを実行する

Webmailは、内蔵のウェブサーバで稼動しますので、必ずしもIIS(Internet Information Server)を必要としません。しかし、WebmailはIISに対応しており、ISAPI DLLとして稼動させることができます。WebmailをIIS6で実行するように設定するには以下の手順にしたがってください。この情報は、www.mdaemon.comにあるMDaemonナレッジベースの文書 #01465に収録されています。

1. IISマネジメントコンソールを開きます。
2. アプリケーションプールを右クリックします。
3. アプリケーションプールの追加 を選択します。
4. 名前に Alt-N と入力し OK ボタンをクリックします。
5. Alt-Nを右クリックします。

6.プロパティをクリックします。

7.パフォーマンスタブをクリックします。

8.アイドルなワーカープロセスのシャットダウンまでの待ち時間　と　カーネル内要求キューを制限するのオプションをはずします。

9.識別タブをクリックします。

10.ドロップダウンリストからLocal Systemを選択します。

11.OKボタンをクリックします。

12.Webサイトを右クリックします。

13.新規を選択します。

14.Webサイトをクリックします(ウィザードが立ち上がります)。

15.次へ ボタンをクリックします。

16.サイト名を入力します(例:Webmail)。

17.次へ ボタンをクリックします。

18.再度 次へボタンをクリックします。

19.ホームディレクトリを表示します。デフォルトでは、 C:¥MDaemon¥WorldClient¥HTML です。

20.次へ ボタンをクリックします。

21.Read, Run ScriptsおよびExecute のオプションが有効になっていることを確認します。

22.次へ ボタンをクリックします。

23.完了 ボタンをクリックします。

24.作成したウェブサイト (Webmail).を右クリックします。

25.プロパティを選択します。

26.ドキュメント 画面をクリックします。

27.表示されたドキュメントをすべて削除します。

28.WorldClient.dllを追加します。

29.Home Directory 画面を選択します。

30.ドロップダウンリストからAlt-N を選択します。

31.K ボタンをクリックします。

32.Web Service Extensions.ボタンをクリックします。

33.All Unknown ISAPI Extension を有効にするか、新しいWorldClient.DLLを作成します。

インターネット ゲスト アカウント のIUSER_<SERVER_NAME>にはMDaemonのサブディレクト リを含 むすべてのMDaemonディレクト リへのNTFSFull Access 権限 が必 要 です。

1. MDaemonディレクト リ(C:¥MDaemon)を右 クリックします。

2. プロパティを選 択します。

3. セキュリティ画 面 を選 択します。

4. 追 加 ボタンをクリックします。

5. Advancedボタンをクリックします。

6. Find Now ボタンをクリックします。

7. IUSER_ <SERVER_ NAME>(ローカルPCの名 前)]を選 択します。

8. OKボタンをクリックします。

9. 再 度 OKボタンをクリックします。

10. Full Controlオプションを有 効 にします。

11. OKボタンをクリックします。

同 様 の手 順 を、MDaemonで使 用 している全 てのフォルダへ適 用 する必 要 があります。

Webを設 定 した後 、MDaemonをアップグレードした場 合:

1) IISマネジメント コンソールを開きます。

2) アプリケーションプールリスト を開きます。

3) Alt-N.を右 クリックします。

4) 停 止 を選 択します。

5) MDaemonを終 了 します。

6) アップグレード のインスト ールを行 います。

7) インスト ールの完 了 後 、MDaemonを再 起 動します。

8) IISマネジメント コンソールで、再 度 Alt-Nを右 クリックします。

9) 開 始 をクリックします。

上 記 の手 順 の後 は、以 下 のような手 順 が表 示 されます。

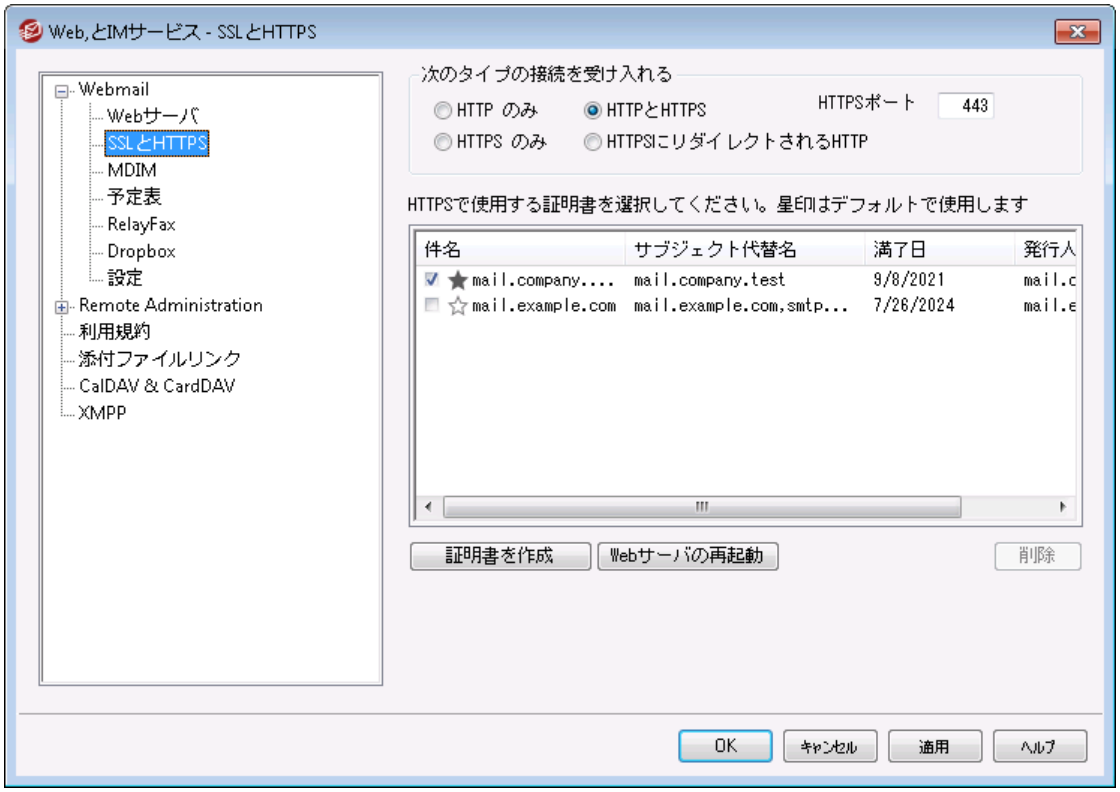
1) アプリケーションプール停 止 後 に、Service Unavailableというメールが配 信 されます。

2) これらの手順を踏めば、MDaemonのアップグレードに際して、コンピュータの再起動を最小限にすることができます。

IISの下でこのプログラムをセットアップすることは、テクニカルサポートによるサポートの対象となりません。また、IISの下でWebmailを実行する場合は、いかなるアプリケーションの起動や、セキュリティに関しても、充分な注意を払う必要があります。WebmailをISAPIエクステンションとしてインストールする前に、IISに対するすべてのパッチと更新を終了しておいてください。

IISでWebmailを実行している場合、MDaemonのインターフェイスからは、Webmailのコントロールを行うことはできません。IISからのコントロールのために提供されるツールを使用しなければなりません。

3.6.1.3 SSL & HTTPS



MDaemonに搭載されているウェブサーバーはSecure Sockets Layer (SSL)プロトコルに対応しています。SSLとは、サーバー/クライアント間のウェブコミュニケーションを安全に行うための標準規格であり、サーバー認証、データ暗号化、TCP/IP接続用に追加のクライアント認証などの機能を提供しています。ほとんどのブラウザでは(HTTP over SSLのような)HTTPSに対応しているため、サーバー側に正しい証明書をインストールするだけで、クライアントはSSL機能を利用できるようになります。

Webmail でHTTPSを使用するには、設定 ≫ Web & IM サービス ≫ Webmail の中のSSL & HTTPS 画面へアクセスして下さい。利便性向上のため、この設定項目は、セキュリティ ≫ セキュリティ設定 ≫ SSL & TLS » Webmail からも使用できます。

SSLプロトコルと証明書についての詳細は、次のページを参照して下さい: SSL & 証明書 523

MDaemonの内蔵ウェブサーバーを使用している場合、ここでの設定はWebmailにのみ適用されます。WebmailがIISなどの他のウェブサーバーを使用していた場合このオプションは使用できません。SSL/HTTPSは他のウェブサーバーで提供されているツールを使って設定を行う必要があります。

次の接続タイプを許可

HTTPのみ
Webmailへの接続にHTTPSの利用を許可しない場合はこのオプションを選択します。HTTP接続のみが使用できるようになります。

HTTPとHTTPS
WebmailでSSL対応は有効にするものの、ユーザーにHTTPSの利用を強制しない場合には、このオプションを選択します。Webmailは指定されたHTTPSポートでのみ接続を受け付けますが、WebmailのWebサーバー 295で指定したWebmail用TCPポートへのhttp接続に対しても応答を行います。

HTTPSのみ
WebmailでHTTPS接続だけに応答するにはこのオプションを選択します。このオプションが有効の場合、WebmailはHTTPS接続のみ応答し、HTTPリクエストに対しては応答しません。

HTTPをHTTPSへリダイレクトする
全てのHTTP接続をHTTPSポートへリダイレクトするには、このオプションを使用します。

HTTPSポート
SSL通信でWebmailが使用するTCPポートを指定します。デフォルトのSSLポートは443番です。デフォルトのSSLポートを使う場合は、WebmailのURLに、ポート番号を含む必要はありません。(例えば、"https://example.com" は "https://example.com:443"と同じURLを示します)

このポートはWebmailの Webサーバー 295 で指定したWebmailポートとは異なります。WebmailでHTTP接続を許可するのであれば、Webmailでは正しく接続できるよう異なるポートを使用する必要があります。HTTPS接続はHTTPSポートを使用する必要があります。

HTTPS/SSL用証明書の選択

ここにはお使いのSSL証明書が表示されます。Webmailで使用する証明書をクリックして選択します。デフォルトとして使用したい証明書の隣にある星印をクリックします。 MDaemonはTLSプロトコルの拡張であるServer Name Indication (SNI)に対応しており、サーバーのホスト名毎に、異なる証明書を使用する事ができます。MDaemonはアクティブな証明書を確認し、Subject Althernative Namesフィールドから、要求されたホスト名を選択します。(証明書の生成時、別名を指定する事もできま

す。)クライアントがホスト名を要求していなかった場合や、対象の証明書が存在していなかった場合、デフォルトの証明書が使用されます。Windowsの証明書ダイアログを起動し、証明書のレビューを行うには、対象の証明書をダブルクリックしてください。(これはブラウザベースのリモート管理画面ではなく、アプリケーション画面からのみ利用できます。)

削除
一覧から証明書を選択し削除をクリックします。確認画面で証明書を削除するかどうかを質問されます。

証明書の作成

このボタンをクリックしSSL証明書の作成ダイアログを起動します。

証明書詳細

ホスト名
証明書作成時、ユーザーが接続する際のホスト名を入力します。(例: wc.example.com)。

組織/会社名
証明書を所有する組織名や会社名を入力します。

ホスト名の別名 (カンマで複数設定)
ユーザーが接続する際などに使用するWebmailの別ホスト名がある場合は、カンマで区切ったドメイン名をここへ入力します。ワイルドカードにも対応しており、例えば"*.example.com"は(例えば"wc.example.com", "mail.example.com"といった)example.comのサブドメインに対しても適用できます。

MDaemonはTLSプロトコルの拡張であるServer Name Indication (SNI)に対応しており、サーバーのホスト名毎に、異なる証明書を使用する事ができます。MDaemonはアクティブな証明書を確認し、Subject Althernative Namesフィールドから、要求されたホスト名を選択します。クライアントがホスト名を要求していなかった場合や、対象の証明書が存

在していなかった場合、デフォルトの証明書が使用されます。

暗号キーの長さ
この証明書で使用する暗号化キーのビットの長さを選択します。長い暗号化キーを使うとより安全な通信が行えますが、全てのアプリケーションで512を超える長さのキーに対応しているわけではありあせん。

国
サーバーが設置している国や地域を選択します。

ハッシュアルゴリズム
使用するハッシュアルゴリズムをSHA1かSHA2から選択します。デフォルトはSHA2です。

webサーバーの再起動
ボタンをクリックしウェブサーバーを再起動します。新しい証明書を使用するにはウェブサーバーの再起動が必要です。

証明書の管理にLet's Encryptを使用する

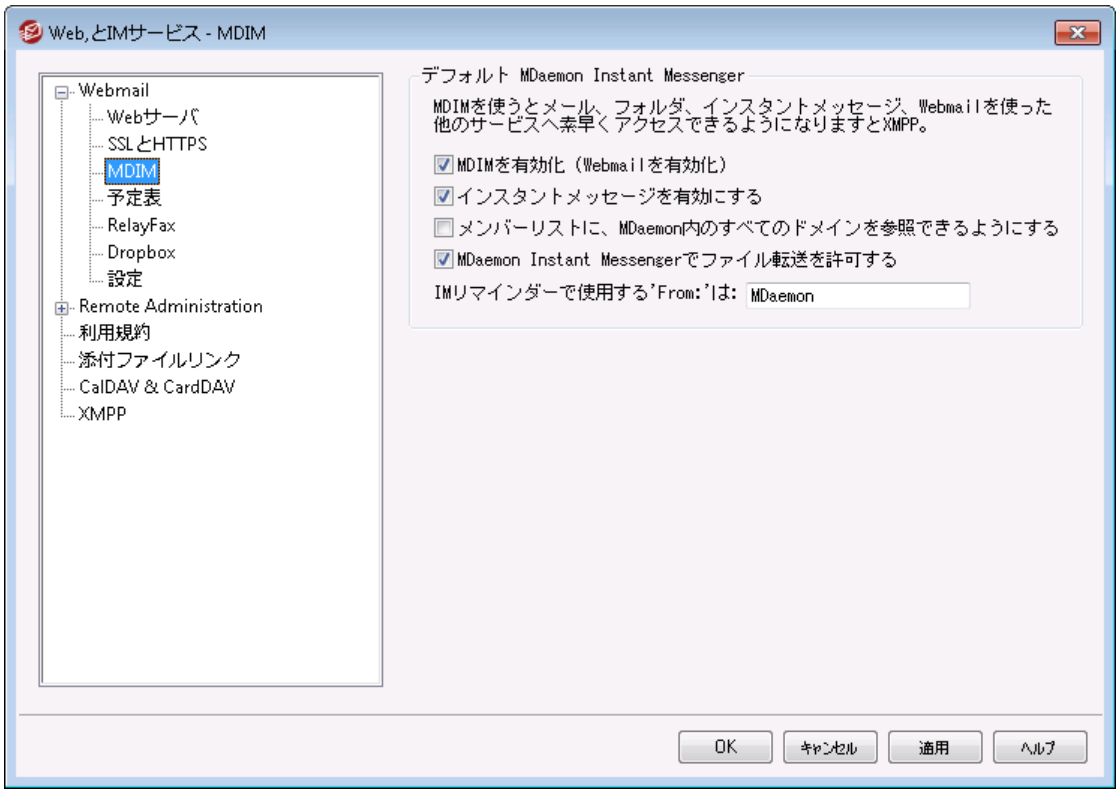
Let's Encryptとは、セキュアなウェブサイト向けに、従来手動で行っていた証明書の生成、検証、署名、インストール、更新といった複雑な処理を自動化し、無償の証明書を発行している認証局（CA）です。

Let's Encryptの自動処理で証明書を管理するのに、Let's Encrypt 541 画面にてMDaemon¥LetsEncryptフォルダに格納されたPower Shellスクリプトを簡単に実行するためのオプションを用意しています。スクリプトを実行するとLet's Encrypt用に、Webmail HTTPフォルダへhttp-01チャレンジに必要なファイルの配置を含む、全ての設定が行われます。ここでは、証明書用のドメインとしてデフォルトドメイン 165 のSMTPホスト名 167 が関連するホスト名と併せて使用され、証明書の取得と受信、Windowsへのインポート、MDaemon, Webmail, Remote Administrationでこれらの証明書を使用するためのMDaemon設定が行われます。更に、スクリプトはMDaemon¥Logs¥フォルダへLetsEncrypt.logというログも生成します。このログはスクリプト実行の度に削除され再生成され、スクリプトの開始時間が記録されます。通知用の管理者アドレスへは、エラー発生時にはメールでの通知も行われます。詳細についてはLet's Encrypt 541 を参照してください。

参照:

SSL & 証明書 523
SSL証明書の作成と使用 830

3.6.1.4 MDIM



この画面では新しいドメイン向けの MDaemon Instant Messenger (MDIM) 292 に関するデフォルト設定が行えます。ドメイン毎の設定はドメインマネージャのドメインマネージャのMDIM画面 173 から行います。MDaemon Instant Messengerサービスは、ウェブサービス 656 や グループプロパティ 714 画面から、特定のアカウントやグループ毎に有効化・無効化が行えます。

デフォルト MDaemon Instant Messenger

MDIMを有効化（Webmailを有効化）
デフォルトでWebmailからMDaemon Instant Messengerをダウンロードし、利用できるようにする場合はこのオプションを有効化して下さい。ダウンロードは *オプション ≫ MDaemon Instant Messenger* ページから行えます。ダウンロードされたインストール用ファイルは自動でユーザーアカウント毎に、インストールと設定が簡単に行えるよう設定されています。このオプションではMDIMを私のメールフォルダ機能用に使用する事もでき、ユーザーは新着メールをMDIMのショートカットメニューをクリックし、Webmailを起動する事で簡単に行えるようになります。MDIMはデフォルトで有効です。

インスタントメッセージを有効にする
デフォルトで、ユーザーはMDIMやサードパーティーのXMPP 340 クライアントでドメインの他のユーザーとでインスタントメッセージが行えます。デフォルトでインスタントメッセージを許可しない場合はこのチェックボックスを無効化して下さい。

メンバーリストに、MDaemon内のすべてのドメインを参照できるようにする
ドメインに関係なくMDaemonユーザの全てを、連絡先に追加するにはこのオプションを選択します。同じドメインのユーザだけメンバーに追加する場合、このチェックボックスを解除します。例えばMDaemonがexample.comとexample.orgを管理している時、このオプションを有効にすると、example.comユーザーは両方のドメインのユーザーをメンバーへ追加できます。これを無効にすると、example.comドメインのユーザーのみを追加できます。このオプションはデフォルトで無効になっています。ドメイン用の同様のオプションがドメインマネージャ[173]から有効化・無効化できます。

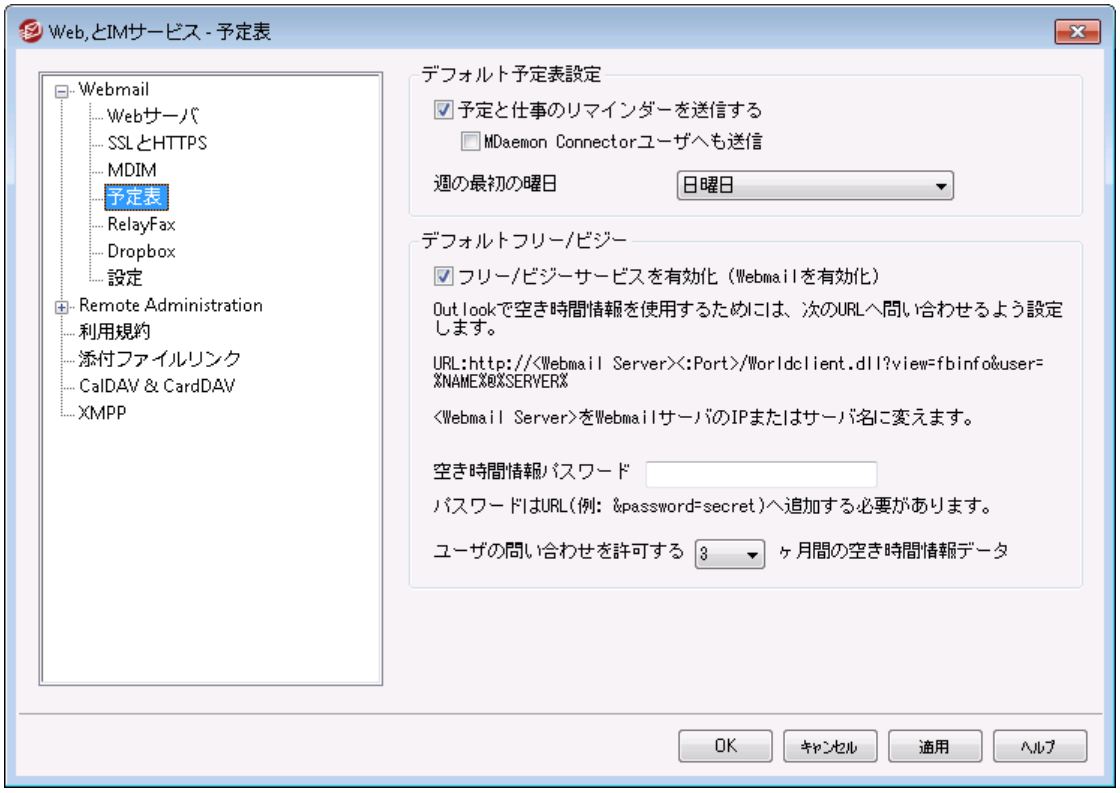
MDaemon Instant Messengerでファイル転送を許可
デフォルトで MDIMユーザーは連絡先との間でファイルの転送が行えます。MDIMでファイル転送を許可しない場合はこのオプションを無効化します。

IMリマインダーで使用するFromは: [*text*]
Webmail予定表へ予定が追加されると、イベントのリマインダーが指定した時間にユーザーへ送信されます。所属ドメインのIMシステムが有効の場合、インスタントメッセージが対象ユーザーへ送信されます。このテキストボックスで、メッセージのFrom:として表示させたい名前を指定します。これは新しいドメインのデフォルト設定です。特定のドメイン設定については、ドメインマネージャの MDaemon Instant Messenger[173] 画面から変更できます。

参照:

ドメインマネージャ ≫ MDaemon Instant Messenger[173]
アカウントエディタ ≫ ウェブサービス[656]
グループプロパティ[714]

3.6.1.5 予定表



ここではデフォルトのMDaemon予定表の設定が行えます。特定のドメインに対する設定はドメインマネージャの 予定表 174 画面から行えます。

デフォルト予定表設定

予定と仕事のリマインダーを送信する
このチェックボックスをクリックするとWorldClientへ登録された予定と仕事のリマインダーがメールやMDaemon Instant Messengerで送信されます。

MDaemon Connectorユーザーへも送信
上記の"予定と仕事のリマインダーを送信する"オプションを有効にしている場合、このオプションをクリックするとMDaemon Connectorユーザへもリマインダーが送信されます。

週の最初の曜日
ドロップダウンリストから曜日を選択してください。選択された曜日は、週の最初の曜日として予定表に表示されます。

デフォルトフリー/ビジー

MDaemonにはFree/Busyサーバ機能が含まれています。これにより会議を計画している人が、出席可能なメンバーを事前に確認することができます。
この機能にアクセスするためには、Webmailで新しいアポイントメントを作成する際に[予定表]をクリックしてください。するとスケジューリング ウィンドウが開き、参加者のリストや色分けされたカレンダーが表示されます。それぞれの参加者の行は色分けされており、彼らが会議に参加可能な時間が表示されます。色の区分には[取り込み中][離席中][外出中][情報なし]があります。また[次の回を

自動的に選ぶ]ボタンがあり、すべての参加者が次に同時に参加可能になる時間を、サーバに問い合わせることができます。アポイントメントの作成が完了すると、すべての参加予定者に招待状が送られ、参加予定者は参加/不参加の返事をします。

WebmailのFree/Busyサーバ機能は、Microsoft Outlookとの互換性があります。OutlookにFree/Busyサーバの URLへのクエリを設定するだけで使用することができます。例えばOutlook 2002のFree/Busyオプションは、"ツール ≫ オプション ≫ 予定表オプション... ≫ 空き時間情報オプション..."にあります。

Outlookで使用するFree/Busyオプションの URLは以下のとおりです。

http://<Webmail><:Port>
/Worldclient.dll?view=fbinfo&user=%NAME%@%SERVER%

上記のURLの<Webmail>は、使用しているWebmailサーバのIPアドレスまたはドメインに置き換えてください。また、デフォルトのポートを使用していない場合は、<:Port>をポート番号に置き換えてください。例えば、以下のようなURLとなります。

http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%SERVER%

Webmailのフリー/ビジーサーバーの詳細については、Webmailからアクセスできるヘルプファイルも参照してください。

Free/Busyサービスを有効にする
ユーザに対してFree/Busy機能を有効にするには、このオプションをクリックしてください。

空き時間情報パスワード
ユーザがOutlook経由で空き時間情報サーバにアクセスする際に、パスワードの入力を求める場合は、ここにそのパスワードを入力してください。このパスワードは、ユーザがOutlookでの空き時間情報機能のURL設定をする際に、そのURLに("&password=FBServerPass"の部分で)含まれていなければなりません。例えば以下のようなURLとなります。

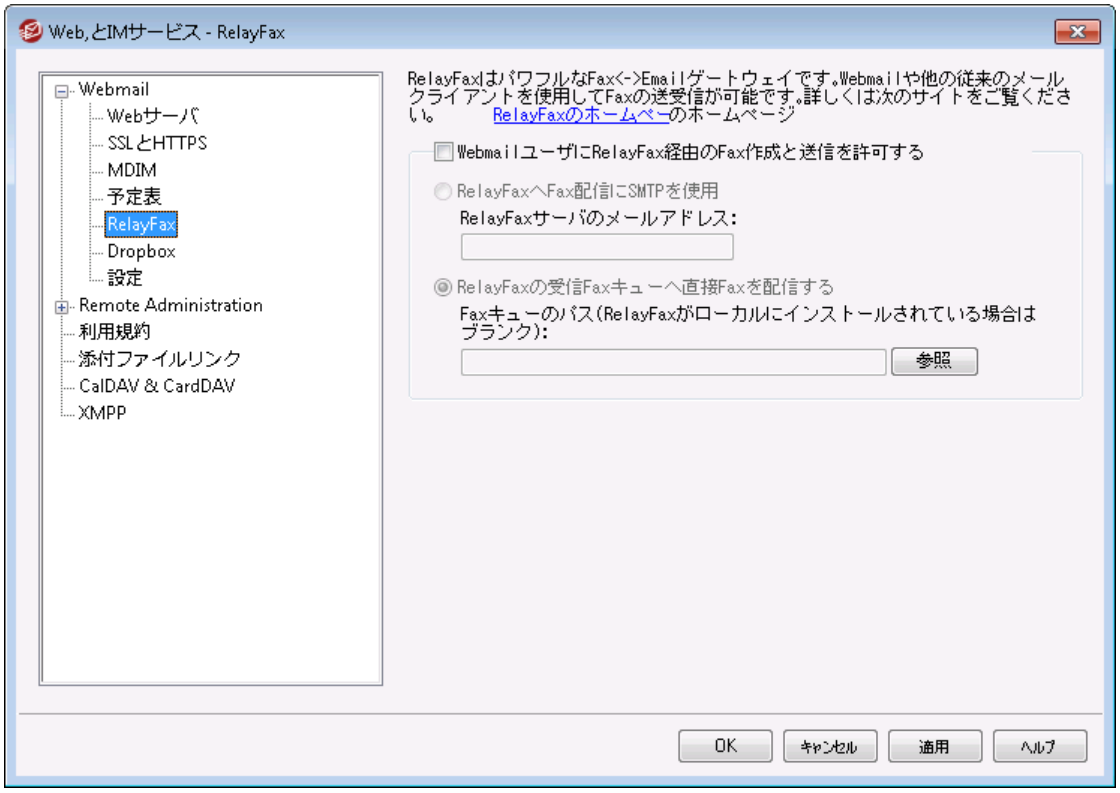
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%SERVER%
&password=MyFBServerPassword

ユーザの問合わせを許可するXヶ月間の空き時間情報データ
ユーザが空き時間の問合せを行える対象期間を月単位で指定します。

参照:

ドメインマネージャ ≫ 予定表 174

3.6.1.6 RelayFax



MDaemon Technologies社のRelayFaxサーバは、Webmailとの連携も行える、メールからファックス、ファックスからメールへのシームレスな変換を行うためのゲートウェイ製品です。この機能を有効にする事で、WebmailユーザはRelayFaxのもつ様々な機能へのアクセスが可能になり、Webmailのクライアントページからファックスの作成ができるようになります。RelayFaxに関する詳しい情報は、www.mdaemon.comのRelayFax sectionをご覧ください。

RelayFax統合オプション

WebmailユーザにRelayFax経由のFax作成と送信を許可
このオプションをクリックして、RelayFaxとWebmailが連携します。Webmailのページにファックスの作成などファックスに関連した機能が表示されるようになります。

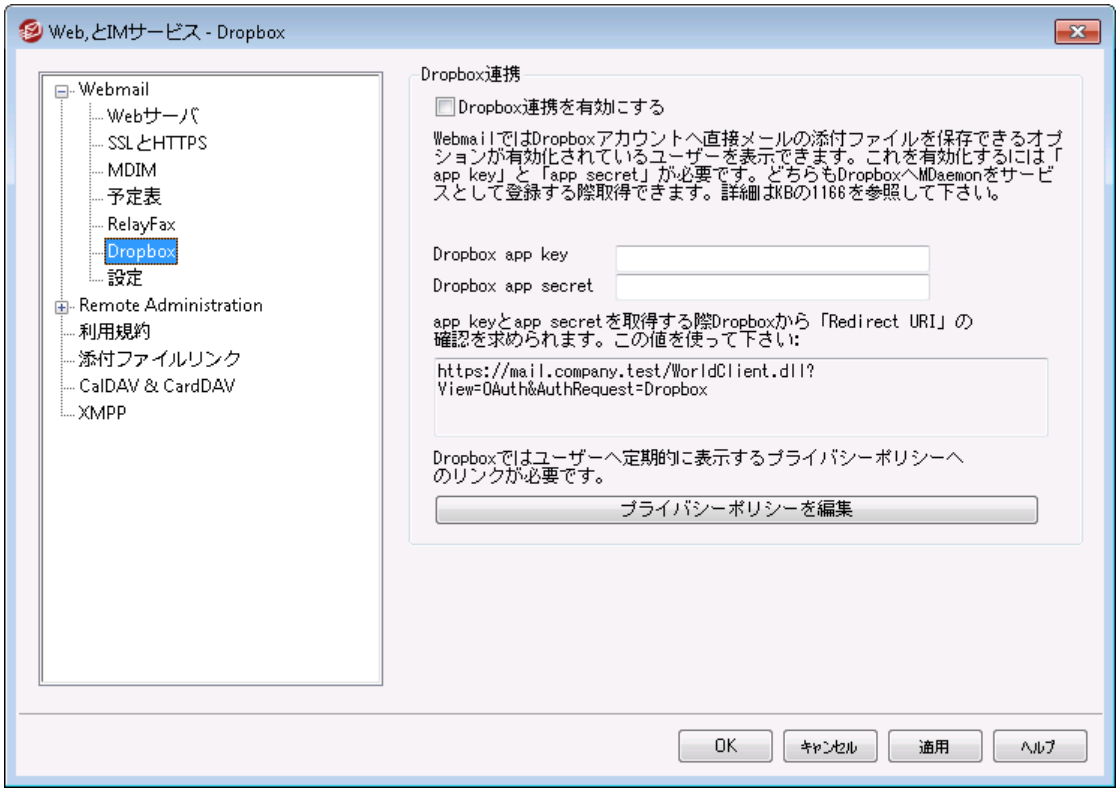
RelayFaxへのFax配信にSMTPを使用
RelayFaxはファックスで送られる受信メッセージ用の特定のメールボックスをモニタします。このオプションをクリックすると、MDaemonは、通常のSMTPメール配信プロセスを使用して、これらのメッセージをその特定のメールボックスのアドレスへ送信します。このオプションは、RelayFaxがLAN以外の位置するメールボックスをモニタするのに役立ちます。RelayFaxがLANの中にある場合は、MDaemonにメッセージを直接RelayFaxのメッセージキューに送信させ、SMTP配信プロセス全体を回避させることができます。この方法に関する詳しい記述は、以下の**RelayFaxの受信FAXキューへ直接FAXを配信する**を参照してください。

RelayFaxサーバのメールアドレス
ファックスとして送信するメッセージを送信するメールボックスのアドレスを指定してください。このアドレスは、これらのメッセージ用のメールボックスをモニタするようにRelayFaxを構成した時のアドレスと一致していなければなりません。

RelayFaxの受信FAXキューへ直接FAXを配信する
RelayFaxがLANの中にある場合は、ファックス用のメッセージの配信にSMTPを使うよりも、この方法を使用した方が良いかもしれません。この方法を使用すると、MDaemonがRelayFax用のメッセージを受け取った場合、それをSMTPで配信するのではなく、RelayFaxのincomingキューに直接そのメッセージを渡します。

Faxキューのパス
RelayFaxがMDaemonが動作しているマシン上で稼働している場合、ここでのファイルパスは空白のままで構いません。それ以外の場合は、RelayFaxの¥app¥フォルダのネットワークパスを、ここで指定する必要があります。

3.6.1.7 Dropbox



WebmailにはDropboxとの連携機能が搭載されており、ユーザーは添付ファイルをDropboxアカウントへ保存したり、Dropbox内のファイルに対するリンクを送信メールへ挿入できるようになります。Webmailでこの機能を利用するには、Dropboxプラットフォームにて、WebmailをDropbox appとして設定する必要があります。これは、Dropboxアカウントでログインし、app用に固有の名前を作成し、Dropboxへフルアクセス権限を与え、Webmailへのリダイレクト用URIを指定し、デフォルト設定の1つを変更するという単純な処理です。その後、Dropbox App KeyとApp SecretをMDaemonのDropboxオプションへ入力します。その後、ユーザーがWebmailへログインすると、Webmailの画面上にDropboxアカウントへのリンクが表示されます。Dropbox appの作成とWebmailへのリンク方法についての詳しい手順は、Dropbox Appの作成とリンク 311を参照して下さい。

Dropbox appを作成すると、初期段階でのステータスは「Development」となります。これはWebmailユーザーの内500ユーザーまでがDropboxアカウントからappへリンクできるというステータスです。ただし、Dropboxによれば、「appが50のDropboxユーザーとリンクした場合、ステータスをProductionとして申請

し、承認を受けるのに2週間待つ必要が生じます。その間、500ユーザー中何ユーザーがリンクしているのかに関わらず、Dropboxユーザーの追加を行う事はできません。」つまり、ステータスがproductionになるまで、Dropbox連携は機能し続けますが、ユーザーの追加を行う事はできません。productionの承認手続きについてはDropboxのガイドラインやサービス要項を確認して下さい。詳細については Dropbox Platform開発者ガイドを参照して下さい。

Webmail appが正しく作成・設定されると、各Webmailユーザーへ、アカウントをDropboxアカウントへ接続するためのオプション画面が追加されます。ユーザーはDropboxへログインしDropboxアカウントへ接続するのに必要な権限をappへ与える必要があります。ユーザーは認証処理中にDropboxへ渡したWebmail URIを使用して元の画面へ戻されます。セキュリティ目的でURIはDropbox.comのapp情報ページで指定したRedirect URIと同じものである必要があります。最後に、WebmailとDropboxはアクセスコードとアクセストークンを交換し、Webmailがユーザーのdropboxアカウントへ接続し、添付ファイルを保存できるようになります。交換されたアクセストークンは7日間毎に期限切れとなり定期的にユーザーはDropboxと認証を行う必要があります。ユーザーは手動でDropboxから接続を解除したり、必要に応じて再認証を行ったりする事ができ、その際にはWebmailのCloud Appオプションページを使用します。

Dropbox連携

Dropbox連携を有効にする

Dropbox appを作成し、Webmailへリンクさせるには、このチェックボックスをクリックしWebmailユーザーがそれぞれのDropboxアカウントへリンクできるようにして下さい。ユーザー毎にDropboxの有効化・無効化を行うには、User.iniで`DropboxAccessEnabled=Yes`（または `No`）を指定して下さい。

Dropbox app keyとapp secret

App keyとApp secretがDropbox.comのapp情報ページで確認できます。これを入力する事でWebmailがDropbox appへリンクできるようになります。

Redirect URI

Redirect URIはDropbox.comのapp情報ページで指定する必要があります。MDaemonは入力するURIを自動で表示します。ただ、ここでは複数のRedirect URIを指定できるため、サーバー機からWebmailへログインする際などに使用するlocalhostを含む複数ドメイン毎にURIを指定する事もできます。

例:

```
https://mail.company.test/WorldClient.dll?
    View=OAuth&AuthRequest=Dropbox

https://example.com/WorldClient.dll?
    View=OAuth&AuthRequest=Dropbox

https://localhost/WorldClient.dll?View=OAuth&AuthRequest=Dropbox
```

DropboxのRedirect URIはセキュアな通信である必要があり、HTTPS 300をWebmailで有効にしておく必要があります。

プライバシーポリシーを編集

このボタンをクリックし、Webmail Appのプライバシーポリシーを編集します。Dropboxでは定期的に、**Dropboxへ接続のページ**にて「プライバシーポリシー」へのリンクからプライバシーポリシーを表示させる必要があります。リンクから、テキストとダウンロードボタンを含むウィンドウが起動し、ボタンをクリックする事でダウンロードが行えます。ファイルにはHTMLコードを使用する事ができ、リンクなどを含む事もできます。

Dropbox Appの作成とリンク

Dropbox appの作成とWebmailへのリンクは次のように行います。

1. ブラウザから Dropboxプラットフォームへ接続します。
2. Dropboxアカウントへサインインします。
3. **Dropbox API**を選択します。
4. **Full Dropbox**を選択します。
5. appへ重複のない名前をつけます。
6. **Create App**をクリックします。
7. **Enable additional users**をクリックし**Okay**をクリックします。
8. **Allow implicit grant**を**Disallow**へ変更します。
9. 1つまたはそれ以上のRedirect URIを、**Add** をクリックして追加します。セキュアなURLでWebmailへ接続する必要があります。（WebmailでHTTPSを有効にする必要があります。）

   例:

   https://mail.company.test/WorldClient.dll?View=OAuth&AuthRequest=Dropbox

   https://localhost/WorldClient.dll?View=OAuth&AuthRequest=Dropbox
10. ブラウザでapp情報ページを開いたまま、MDaemon GUIを起動します。
11. **設定**をクリックします。
12. **Web & IMサービス**をクリックします。
13. **Webmail**の中の**Dropbox**をクリックします。
14. **App key**と**App secret** をブラウザからコピーし、貼り付けます。
15. **適用**をクリックします。
16. **OK**をクリックします。

Webmailユーザーからそれぞれのdropboxアカウントへリンクする方法は、Webmailのヘルプか Knowledge Base article 1166をご覧ください。

3.6.1.8 Google Drive

このページはMDaemon Remote Administration 321（MDRA）ウェブインターフェイスでのみ利用できます。

Google Driveとの統合

MDaemon Webmailではユーザー向けにGoogle Driveアカウントへ添付ファイルを直接保存するオプションを提供しており、Google Driveへ保管されたデータの編集や管理を行う事もできます。これを有

効にするには、**API Key**, **Client ID**, **Client Secret** が必要です。これらの情報はGoogle APIコンソールでアプリを作成し、MDaemonをサービスとして登録した際Googleから直接提供されます。OAuth 2.0 認証コンポネントはアプリの一部で、Webmailユーザーが Webmailへサインインし、Goolgle Driveへアクセスするための認証を行うのに使用されます。認証されると、ユーザーはGoogle Drive内のフォルダやファイルを閲覧できます。また、ファイルのアップロード、ダウンロード、移動、コピー、名称変更、削除に加え、ローカルのドキュメントフォルダのコピーや移動も行えます。ユーザーが編集を行う際には、Google Driveでファイルを表示するオプションをクリックする事で、ユーザーのGoogle Driveでの権限に基づき、編集を行う事ができるようになります。Google Driveの設定はMDaemonのDropbox統合 309や MultiPOP OAuth統合 130に似ています。

Google Drive統合を有効にする
このオプションを有効にし、Google Drive統合を有効化します。後述の、**Google Drive統合の設定**を参照してください。

Google Drive API Key:
個別のAPIキーで、アプリの作成時、Google Driveコンソールで生成されます。API Keyをここでコピー＆ペーストしてください。

クライアントドライブ　クライアントID
アプリの作成時、Google Driveアプリへ割り当てられる固有のクライアントIDです。アプリ作成後、クライアントIDをコピーし、ここへペーストしてください。

Google Drive クライアントシークレット
Google APIコンソールでGoogle Driveアプリを作成した際割り当てられる固有のクライアントシークレットです。アプリの作成後、クライアントシークレットをコピーし、ここへペーストします。

リダイレクトURI
Google Driveアプリ作成では、1つ以上のリダイレクトURIを指定する必要があります。リダイレクトURIの例としては、Webmailへサインインするのに使用するドメインのユーザー用のデフォルトドメインのS 165MTPホスト名 167を元にしたものです。 追加のMDaemonドメイン用にリダイレクトURIも追加します。例えば、"`https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive`" は `mail.example.com` へログインするユーザー全てに適用できます。後述の**Google Drive統合の設定**を参照してください。

個人情報保護方針の編集
Google Drive統合では正しい個人情報保護方針へのリンクが存在するかどうかを定期的に調査するよう定義しています。このボタンをクリックし、個人情報保護方針を編集します。

Google Driveアプリの作成とリンク

Google Driveアプリを作成する手順は次の通りです。

次の手順でGoogleアプリケーションを作成し、ユーザーがWebmailのドキュメントページからGoogle Driveへアクセスできるようにします。

1. MDaemon Remote Administration 321へサインインし、Google Driveページ（メイン ≫ Webmail設定の下）へ進み、**Google Drive統合を有効にする**オプションを有効にします。
2. 別のブラウザのタブで、Googleアカウントでサインインし、Google APIコンソールへ進みます。
3. プロジェクトの一覧からは、**新しいプロジェクト**をクリックし、リソース管理ページからは（＋）**プロジェクトを作成**をクリックします。

4. 「Google Drive for MDaemon」といった、**プロジェクト名**を入力し、プロジェクトIDを編集する場合は**編集**をクリックするか、デフォルト値を使う場合はそのままにします。**注意点**：プロジェクトIDはプロジェクト作成後は変更する事ができません。
5. 組織リソースがある場合は、ロケーションから選択します。なければ、「組織なし」の設定のままにしておきます。
6. ロードされたら、+ **APIとサービスの有効化** をクリックします。
7. 検索フィールドで「Google Drive」と入力し、**Google Drive API**をクリックして、**有効**をクリックします。
8. 左側の画面で、**APIとサービス**の**認証情報**をクリックします。
9. ページ上部の + **認証情報を作成** をクリックし、ドロップダウンメニューから **APIキー** を選択します。
10. **APIキー** をコピーします（クリップボードへコピーするためのアイコンが隣に表示されています）。
11. ブラウザのMDaemonタブへ戻り **Google Drive APIキー** フィールドをコピーして、MDaemonのGoogle Driveページへペーストします。（後ほど設定する場合は別の場所へペーストしておきます。）
12. 左側の画面の**APIとサービス**で**OAuth同意画面**をクリックします。
13. ユーザータイプで **外部** を選択し、作成をクリックします。注意点： 組織リソース を持っている場合やアプリの公開ステータスが依存している場合、内部を選択した方がいい場合もあります。後述の公開ステータス 314 で詳細を確認してください。
14. **アプリケーション名**（例. Google Drive for Webmail)を入力し、ユーザー連絡先用の**サポートメールアドレス**とプロジェクト変更に関するGoogleへの連絡先用の開発者メールアドレスを入力します。このページでの設定はこれで全部ですが、組織や検証要件によっては、企業ロゴの指定や 利用規約 332 や個人情報保護方針（先述をご覧下さい。）へのリンクの設定が必要な場合もあります。**認証済ドメイン**のフィールドは後にリダイレクトURIを入力すると自動で入力されます。**注意点**；ここでの情報はユーザーがWebmailからGoogle Driveへアクセスする際表示される同意画面にて表示されます。
15. **保存して続行**をクリックします。
16. **スコープの追加と削除**で、「スコープを手動で追加」の下へ、以下のURIをコピー＆ペーストします。（全てを一度にコピー＆ペーストする事もできます。その後、**テーブルへ追加**をクリックします。
```
https://www.googleapis.com/auth/userinfo.email
https://www.googleapis.com/auth/drive.file
https://www.googleapis.com/auth/documents
https://www.googleapis.com/auth/drive
https://www.googleapis.com/auth/drive.readonly
https://www.googleapis.com/auth/drive.metadata
https://www.googleapis.com/auth/drive.photos.readonly
https://www.googleapis.com/auth/drive.activity.readonly
https://www.googleapis.com/auth/spreadsheets
```
17. **保存して続行**をクリックします。
18. テストユーザーで、**ユーザーを追加** をクリックし、Google Drive MDaemonへこのアプリからアクセスするGoogleアカウントを入力し、追加をクリックします。（アプリの公開ステータス 314 については後述の注意点を参照してください。）
19. **保存して続行**をクリックします。

20. サマリページのページ下部にある、**ダッシュボードへ戻る**をクリックします。
21. 左側の画面の**認証情報**で、(+) **認証情報を作成**をクリックし、**OAuthクライアントID**を選択します。
22. 「アプリケーションタイプ」のドロップダウンボックスで、「認証済リダイレクトURI」の下の、**Webアプリケーション**を選択し、**+ URIを追加**をクリックします。リダイレクトURIを入力します。MDaemonのGoogle Driveページへ表示されているリダイレクトURIは、Webmailへサインインするのドメインのユーザー用にデフォルトドメインのSMTPホスト名を元に生成した例です。追加のMDaemonドメイン用にリダイレクトURIも追加します。例えば、"https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive" は mail.example.com へログインするユーザー全てに適用できます。もしも、例えば、"mail.company.test"というホストを使用していた場合は、このドメイン用にもリダイレクトURIを入力します。例. "https://mail.company.test/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive".
23. 作成をクリックします。
24. MDaemonのGoogle Driveページにて、**Google Driveクライアント ID**と**Google Driveクライアントシークレット**の値を**クライアントID**と**クライアントシークレット**のボックスへコピーします。Google Drive APIキーの入力を行っていない場合は、APIキーもここで入力します。

> **公開ステータス** – ここでの手順は、Googleアプリで公開ステータスを「テスト中」として作成する事を前提としています。設定はGoogle Driveへアプリを使ってアクセスするユーザー毎に行う必要があり、ユーザー数の上限は100ユーザーです。また、WebmailでユーザーがGoogleへアクセスするためのMDaemon認証を求められた際、「ユーザーはプロジェクトに対しテストアクセスを行っているものの、未検証のアプリケーション上のデータへのアクセス許可に伴うリスクについても考慮して下さい」といった警告メッセージが表示されます。また、認証は7日間で期限切れとなり、各ユーザーは週に1度Googleアクセス用の再認証を実行する必要があります。
>
> こうした要件や制限を削除するには、ステータスを「稼働中」へ変更する必要があります。この時、環境によってはユーザータイプの外部から内部への変更が必要となる場合があります。アプリケーションの検証や公開ステータスについては、Googleの次のページを参照して下さい: Setting up your OAuth consent screen 及び OAuth API verification FAQs

WebmailでのGoogle Drive認証

Google Driveアプリを作成し、MDaemonのGoogle Driveページの設定を行ったら、WebmailからGoogle Driveへアクセスするユーザーは、最初に認証を行う必要があります。各ユーザーは、次の手順で認証を行います:

1. Webmailへサインインします。
2. 右上の**オプション**アイコンをクリックし、**クラウドアプリ**をクリックします。
3. **Google Drive設定**をクリックします。(**OAuth 2.0** ページが起動します)
4. **Google Driveへ接続**をクリックします。

5. サインインしていない場合は、Google Driveがサインイン情報またはアカウントの選択を求めます。
6. 「Googleはこのアプリを検証していません。テスト中のアプリへ接続しようとしています。招待を送った開発者を知っている場合のみ処理を続行してください」といった警告メッセージが表示される場合があります。**継続**をクリックします。
7. Webmailがアクセスできる Google Drive機能を選択し、**続行**をクリックします。
8. MDaemonがGoogle Driveへ接続した事を示す、最終ページが表示されます。ユーザーはここでウィンドウを閉じる事ができます。
9. Webmailの**ドキュメント**ページからユーザーがGoogle Driveへアクセスできるようになりました。

参照:

MultiPOP OAuth 130
Dropbox統合 309

3.6.1.9 カテゴリ

MDaemonの Remote Administrationでは **メイン ≫ Webmail設定 ≫ カテゴリ**でカテゴリオプションへアクセスできます。

WebmailのLookOutとWorldClientテーマはメール、イベント、メモ、仕事のカテゴリに対応しています。ユーザーはメール一覧セクションの、"**オプション ≫ 列**" で "**カテゴリ**" をクリックする事で、カテゴリの列をメール一覧へ追加できます。

メール一覧の中のメールへカテゴリの設定を行うには、対象メールを選択し、右クリックします。コンテキストメニューからカテゴリを指定できます。また、メールを開いてツールバーのオプションからもカテゴリ設定が行えます。

カテゴリ

MDaemonの Remote Administrationのカテゴリページでは、ドメインカテゴリを設定できます。これはWebmailで使用できるカテゴリの一覧ですが、編集や削除は行えません。個人用のカテゴリのデフォルトの一覧を新しいユーザー用にも作成できます。

ドメインカテゴリ

ドメインカテゴリは並べ替えや編集、削除がユーザー個人では行えないカテゴリです。ドメインカテゴリを有効にするオプションを有効化していると、Webmail内でユーザーのカテゴリー覧の上部へ表示されるようになります。提供されているオプションを使って、ドメインカテゴリの並べ替えや編集、削除や作成が行えます。

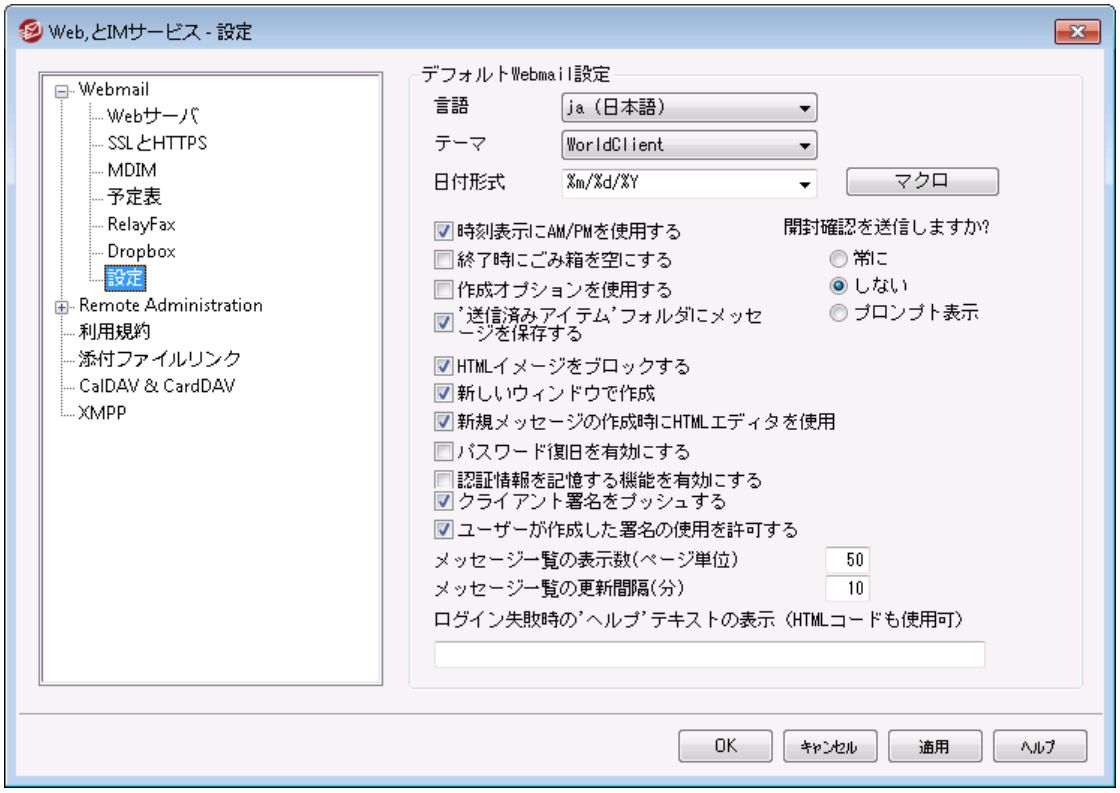
個人カテゴリ

これは新しいWebmailユーザーのアカウントへコピーされるデフォルトのカテゴリー覧です。個人カテゴリの一覧はユーザーが完全にコントロールできます。並べ替え、編集、削除、新規作成が行えます。しかしながら、ドメインカテゴリも使用している場合はドメインカテゴリの一覧は各ユーザーのカテゴリー覧の上部へ表示され、編集や重複するカテゴリ作成はできません。個人カテゴリの名前でドメインカテゴリと同じものがあった場合は非表示となります。個人カテゴリの使用を許可しない場合は、ユーザーの個人カ

テゴリの編集を許可するオプションを無効化します。この場合ドメインカテゴリだけが表示されます。ドメインカテゴリオプションも無効だった場合、カテゴリオプションをユーザーが利用する事はできません。

カテゴリやカテゴリ翻訳を管理しているMDaemonファイルの詳細は、こちらを参照してください:
MDaemon\WorldClient\CustomCategories.txt

3.6.1.10 設定



この画面では、ドメインマネージャのWebmail設定 176 のデフォルト値を設定します。ユーザーがWebmailへサインインすると、ここで設定したオプションが機能します。設定の中の多くは、Webmailのオプションページでユーザー毎にカスタマイズできます。

Default Webmail Settings

言語

ユーザが最初にログオンする時に、Webmailの画面表示に使用するデフォルト言語を、ドロップダウンから選択します。ユーザはWebmailのオプション ≫ 初期設定やWebmailのサインインページから、使用する言語を変更することができます。

テーマ
ユーザが最初にログオンする時に、画面表示に使用するWebmailのデフォルトテーマを、ドロップダウンから選択します。ユーザはWebmailのオプション ≫ 初期設定から、使用するテーマを変更することができます。

日付形式
このテキストボックスを使用して、デフォルトの日付形式を設定してください。[マクロ]ボタンをクリックすると、このテキストボックスで使用することができるマクロコードのリストが表示されます。ここでは、以下のマクロを使用することができます。

%A - 曜日

%B - 月

%d - 日("01-31")

%m - 月("01-12")

%y - 年2桁

%Y - 年4桁

例えば、 "%m/%d/%Y"の場合、Webmailでは "12/25/2011"と表示されます。

マクロ
このボタンをクリックすると、日付形式として使用することができるマクロコードのリストが表示されます。

開封確認を送信しますか?
このオプションは、開封確認要求が受信メッセージに含まれていた場合の応答方法を指定します。

常に
このオプションが選択される場合、MDaemonはメッセージが読まれたことを送信者に通知を送信します。メッセージを受信したWebmailユーザは、開封確認がリクエストまたは応答された表示をしません。

しない
Webmailで開封確認リクエストを無視する場合、このオプションを選択します。

プロンプトを表示
Webmailユーザに、開封確認の送信の有無を確認するには、このオプションを選択します。

時刻表示にAM/PMを使用する

Webmailの時刻表示に、AM/PMを付けた12時間表示を使用する場合は、このオプションを有効にしてください。24時間表示の場合は、チェックボックスを解除してください。各ユーザは、Webmailのオプション ≫ 予定表にある、「時刻表示にAM/PMを使用する」オプションを使って、設定を変更することができます。

終了時にゴミ箱を空にする
このオプションは、ユーザがWebmailからログオフする時に、そのユーザのごみ箱を空にします。各ユーザは、Webmailの オプション ≫ 初期設定で、この設定を変更することができます。

高度な設定を使用する
このオプションをクリックすると、ユーザのデフォルト画面として、通常の構成画面ではなく、詳細な構成画面が開かれます。各ユーザは、Webmailの オプション ≫ 作成で、この設定を変更することができます。

'Sent'フォルダにメッセージを保存する
メールボックスの送信済みフォルダに送信済みメッセージのコピーを保存する場合は、このオプションを選択してください。各ユーザは、Webmailの オプション ≫ 作成で、この設定を変更することができます。

HTMLイメージをブロックする
WebmailでHTMLメールメッセージを表示する場合、自動的にリモートイメージ表示を禁止する場合、このチェックのボックスを選択します。イメージを表示するには、ユーザはブラウザウィンドウでメッセージ上部に現れるバーをクリックする必要があります。多くのスパムメールには画像を表示したユーザーのメールアドレスを抜き出す特別なURL付きの画像が含まれており、こうした画像を表示すると、現在利用していて有効なメールアドレスを、スパムメールの送信元へ通知する事になります。これは、そういった脅威を防ぐための機能で、デフォルトで有効です。

新しいウィンドウで編集
メッセージの作成時にメインウィンドウとメッセージの構成画面を切り換えるのではなく、別々のブラウザウィンドウを開いて作業する場合は、このオプションを選択してください。別々のウィンドウを開きたくない場合は、チェックボックスをクリアしてください。 個々のユーザは、Webmailの オプション ≫ 作成で、この設定を変更することができます。

新規メッセージの作成時HTMLエディタを使用
ユーザがHTML形式でメッセージを編集できるようにする場合は、このチェックボックスを選択してください。ユーザはWebmailのオプション ≫ 作成で、この設定を変更することができます。

パスワードリカバリを有効にする
自分のパスワード編集 656 という権限を持っているユーザーが、Webmailで代理アドレスを入力し、パスワードの紛失時にパスワードを初期化するためのリンクを送る事ができるようになります。この機能を設定する際、ユーザーはオプション >> セキュリティ ページで、パスワードリカバリー用のメールアドレスと現在使用しているパスワードの両方を入力する必要があります。設定後、ユーザーが間違ったパスワードでログインしようとすると、「パスワードをお忘れですか？」というリンクが表示されます。このリンクをクリックすると、パスワードリカバリー用の代理メールアドレスを確認するためのページへ移動します。正しいアドレスを入力すると、パスワード変更用ページのURLが対象メールアドレスに送信されます。この機能はデフォルトで無効に設定されています。

このオプションはWebmailユーザー用のuser.ini(例: \Users\example.com\frank\WC\user.ini)へ次の値を追加して頂く事で、ユーザー毎に有効化・無効化できます。

```
[User]
EnablePasswordRecovery=Yes （=Noで無効化します）
```

2段階認証情報の記憶を許可（Remote Adminへも適用）
WebmailやRemoteAdminへサインインする際、2段階認証（2FA)を使用していた場合、2段階認証ページへも認証情報を記憶するオプションを表示し、指定日数の間は2段階認証を要求しないようにする場合はこのオプションを使用します。2段階認証を記憶するオプションを表示しない場合はこのオプションを無効にしてください。無効にした場合、2FAを有効にしているユーザーは毎

回サインインする毎に2FAコードの入力を求められます。注意点： このオプションは MDaemon Remote Administration (MDRA) 321 ウェブインターフェイスでのみ有効です。

認証情報を記憶する機能を有効にする
https 300 ポートで接続した際、MDaemon Webmailのサインインページへ認証情報を記憶するチェックボックスを追加する場合は、このオプションを有効化します。この機能を使うと、同じ端末からWebmailへ再接続した際、認証情報用のトークンが期限切れになるか、ユーザーが手動でサインアウトするまでの間、サインインが自動的に行われるようになります。

認証情報を記憶オプションはデフォルトで無効化されており、全てのドメインに適用されています。特定のWebmailドメイン用の設定を上書きするには、MDaemonの管理画面にあるドメインマネージャのWebmail画面 176 にて認証情報を記憶オプションを使用します。

デフォルトで、ユーザーが再ログインしなくてはならなくなるまでの有効期間は30日間で、MDaemon Remote Administration (MDRA) 321 の次の日数まで認証情報を記憶、のオプションで異なる日数を指定する事ができます。ここでの設定は、¥MDaemon¥WorldClient¥内のDomains.iniの[Default:Settings]セクションにある、RememberUserExpiration=30 からも変更が行えます。設定できる最大有効期間は365日間です。**注意点**：2段階認証 656 (2FA) には¥MDaemon¥WorldClient¥内のDomains.iniの[Default:Settings]セクションへ、独自の認証情報の記憶用キー(TwoFactorAuthRememberUserExpiration=30)を所持しています。そのため、認証情報を記憶する期間内であった場合にも、2FAのトークンの期限が切れた場合は従来通り認証を要求されます。

認証情報を記憶オプションはデフォルトで無効化されており、全てのドメインに適用されています。特定のWebmailドメイン用の設定を上書きするには、MDaemonの管理画面にあるドメインマネージャのWebmail 176 画面にて認証情報を記憶オプションを使用します。

認証情報を記憶する機能により、ユーザーは複数のデバイスから継続的なログインが行えるようになる事から、公共ネットワークでは極力この機能を使用しないようにしてください。アカウントがセキュリティ上の問題があると思った際にはMDRAのセキュリティ設定の画面から認証情報を初期化ボタンをクリックします。これを使うと全てのユーザーの認証情報の記憶が初期化され、全てのユーザーは再度ログインが必要になります。

クライアント署名をプッシュ配信
デフォルトクライアント署名 125 をWebmailユーザーへプッシュ配信するにはこのボックスを有効にします。Webmailでは、これによりオプション >> 作成内の署名オプション内の「システム」へ署名が生成されます。ユーザーはこの署名を選択し、メールの新規作成時に自動挿入できるようになります。ドメイン用の署名を個別に用意する場合は、ドメインマネージャの クライアント署名 188 や Webmail 176 オプションを使用します。

ユーザーの署名作成を許可する
ドメインのユーザーが自分自身の署名をWebmailで作成できるようにする場合はこのボックスを有効にします。これにより、ユーザーは自分で作成した署名を選択し、メールの新規作成時に自動挿入できるようになります。ユーザーの署名作成を許可しておらず、クライアント署名をプッシュ配信するオプションが有効だった場合、(例えばWebmailのシステム署名といった) クライアント署名 125 だけが自動挿入されます。Webmailでは署名オプションは **オプション ≫ 作成** からアクセスできます。

ユーザーのエイリアス表示名の編集を許可
ユーザーがアカウントに対応した表示名の編集を行えるようにするにはこのオプションを有効にします。WebmailのProテーマでは、設定 >> 作成 の中のエイリアス表示名の編集を使用して表示名が編集できます。このオプションはデフォルトで無効に設定されています。注意点： このオプションは MDaemon Remote Administration (MDRA) 321 ウェブインターフェイスでのみ有効です。

メッセージ一覧として1ページ毎に表示するメール数
この値は、各メールフォルダで表示するメッセージの一覧で、ページ毎に表示するメールの数です。フォルダがこの数以上のメッセージを含む場合、リストの上と下に、ページ移動のコントロールが現れます。個々のユーザは、Webmailのオプション ≫ 初期設定 で、この設定を変更することができます。

メッセージ一覧の更新間隔(分)
これはWebmailが、自動的にメッセージリストを更新する前に待つ時間(分)です。個々のユーザは、Webmailの オプション ≫ 初期設定で、この設定を変更することができます。

ログイン失敗時の'ヘルプ'テキストの表示 (HTMLコード利用可)
ユーザがログオンでトラブルに遭遇した時、Webmailログオンページで表示する一文を、プレーンテキストかHTMLで指定できます。テキストは、次のデフォルトテキストが表示されます:"ログインが正しくありません。ヘルプが必要な場合は、メール管理者に問い合わせてください。このテキストは、Webmailのログオンに関する連絡先窓口の通知として使用する事ができます。

この機能を複数ドメインで正しく使用するためには、正しい SMTPホスト名 167 の設定がドメイン毎に必要です。正しい設定でない場合、デフォルトドメイン 165 用のテキストが使用されます。そのため、例えば複数ドメインが存在し、全てのWebmailユーザーがサインイン用に1つのホスト名を使用しているような場合、正しい、ドメイン専用のログイン失敗時の「ヘルプ」テキストは表示されない可能性があります。

除外リストとブロックリストのカスタマイズ

MDaemon\WorldClient\ フォルダ内の特定のファイルを編集し、Webmailの様々な機能をカスタマイズできます。

管理者はWebmailユーザーの除外リストやブロックリストフォルダをデフォルトで隠す事ができます。この設定を行う場合は、MDaemon¥WorldClient¥Domains.iniの中の [Default:UserDefaults]にある、HideWhiteListFolder= とHideBlackListFolder= の値をNoからYesへ設定して下さい。User.ini内の [User]セクションで、同様のキーを設定する事で、特定のユーザーに対してフォルダの表示・非表示を行う事ができます。

参照:

ドメインマネージャ ≫ Webmail設定 176

3.6.1.11 ブランディング

ログインページやナビゲーション用サイドバーに表示されるWebmailのバナー画像は、Remote Administration[321]のブランディングページから変更する事ができます。

画像を変更するには:

1. カスタマイズの**カスタムイメージへ変更する**をクリックします。
2. ログインページ画像で、(お使いのブラウザによって)ファイルを選択、又は、開くオプションで、アップロードするファイルを選択します。このセクションではログインページ画像のデフォルトサイズの一覧も認できます。
3. **カスタムイメージのアップロード**をクリックします。
4. ステップ2と3をサイドバーイメージとナビゲーションサイドバーイメージ用に繰り返します。

アップロードしたイメージはWebmailデフォルトイメージに代わって、それぞれの場所で使用されます。

3.6.2 Remote Administration

MDaemonのRemote Administration(MDRA)は、ブラウザを使ってリモートからMDaemonを管理するためのサーバーアプリケーションで、MDaemonと同じサーバー上で、バックグラウンドで稼働します。Remote Administrationにアクセスするには、ブラウザを開き、remote administrationサーバーのURLとポート番号(例. www.example.com:1000)を指定します。ログオン情報を入力した後は、MDaemonサーバーに対して、様々な操作や管理が行えるようになります。設定できる種類や数は、ログインユーザーに与えられているアクセス権により異なります。Remote administrationには、グローバル管理者、ドメイン管理者、ユーザーという3種類のアクセス権レベルがあります。

グローバル管理者 – グローバル管理者はMDaemonのアカウント設定でグローバル管理者権限を与えられたユーザーです。グローバルアクセスとはRemote Administration経由でアクセスできる全ての設定やコントロールに対するアクセス権を意味しています。グローバル管理者は、ユーザー、ドメイン、メーリングリストの追加や編集、削除が行えます。また、製品のINIファイルの編集、他のユーザーをドメイン管理者として指定、パスワード管理、その他にも多くの操作が行え、完全な管理権限を持っています。

ドメイン管理者 – グローバル管理者と同様に、ドメイン管理者もRemote Administration経由でアクセスできるユーザーや設定をコントロールする権限を保有していますが、その範囲は、グローバル管理者や、アクセス権を持つ他のドメイン管理者によってウェブサービス[656]からアクセス権を与えられた1つ又はそれ以上のドメインに限定されます。

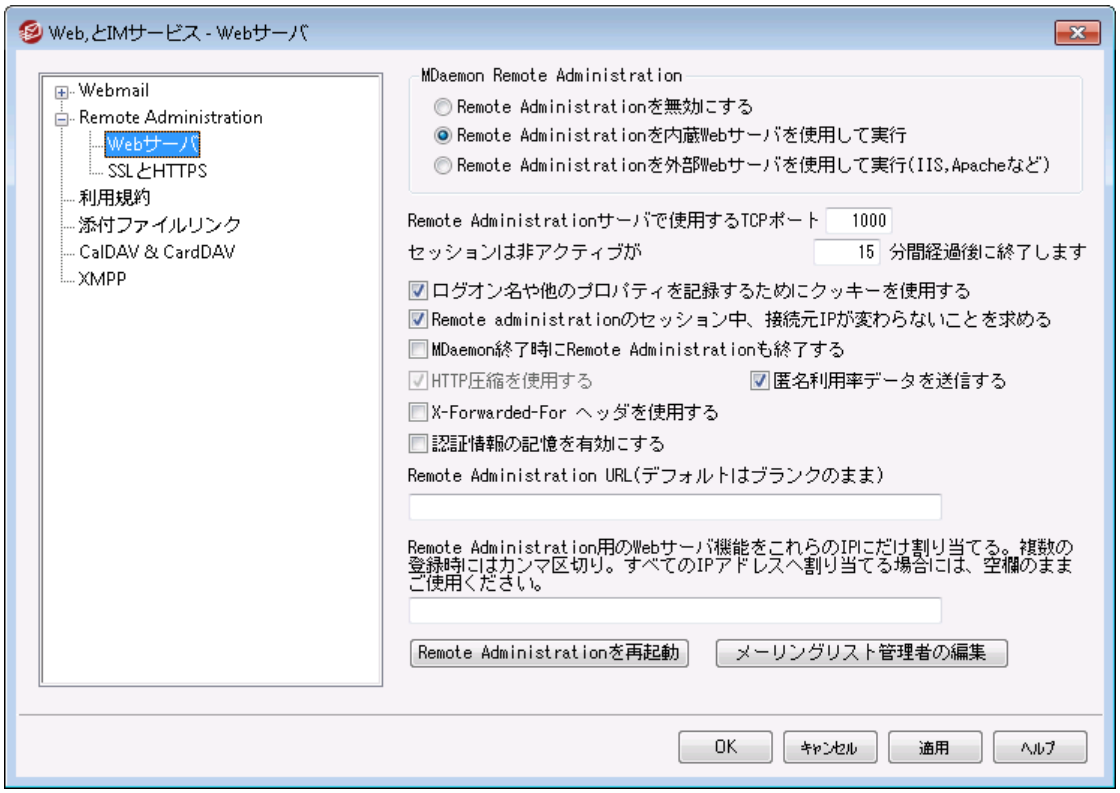
一般ユーザ – Remote Administrationへのアクセスにおいて最も低いアクセス権レベルが一般ユーザーです。MDaemonユーザはremote administrationにログオンし、自分自身の、例えば、MultiPOPエントリ、メールフィルタ、自動応答といった設定にアクセスできます。編集できる設定の種類や数は与えられた権限により異なります。

Webmailとの両方にアクセス権を持っている全てのユーザーは、それぞれにログインするのではなく、Webmail内からRemote Administrationへアクセスできます。Remote Administrationはオプションの中の詳細設定をクリックすると、新しいウィンドウで表示されます。

参照:

Remote Administration ≫ Webサーバ 322
Remote Administration » HTTPS 325
テンプレートマネージャ ≫ ウェブサービス 728
アカウントエディタ ≫ ウェブサービス 656
Remote AdministrationをIISで実行する 329

3.6.2.1 Webサーバ



MDaemon Remote Administration

Remote Administration を無効にする
Remote Administrationを無効にするには、このオプションを選択してください。Remote Administrationの有効化/無効化は、MDaemon管理画面のメインにある統計情報フレームやファイルメニューからも切り替えることができます。

Remote Administrationは内蔵Webサーバを使用して実行
MDaemonが内蔵しているWebサーバを使って、Remote Administrationを実行するには、このオプションを使用します。Remote Administrationの有効化/無効化は、MDaemon管理画面のメインにある統計情報フレームやファイルメニューからも切り替えることができます。

Remote Administrationは外部Webサーバを使用して実行(IIS, Apacheなど)
Remote AdministrationをMDaemon内蔵のウェブサーバではなくIIS(Internet Information Server)などの外部のウェブサーバで実行する場合は、このチェックボックスを選択してください。これで、複数サーバーの起動による競合などの可能性を防止することができます。

詳細については IISでRemote Administrationを起動する 329を参照して下さい。

このTCPポートでRemote Administrationサーバを実行する
Remote Administrationが使用するTCPポート番号を入力してください。デフォルトは1000番ポートです。

セッションは次の時間経過後無効にするxx分通信がない場合
Remote Administrationにログイン後、Remote Administrationがセッションを閉じるまでの無操作時間の最大値を指定します。デフォルトは15分です。

初期設定

ログオン名やその他のプロパティを記録するためクッキーを使用する
デフォルトでRemote Administrationはログオン名やその他のプロパティ情報を保存するのにクッキーを使用しています。クッキーを使用させたくない場合はこのオプションを無効にして下さい。この機能によりカスタマイズされたログオンが可能になりますが、利用するブラウザでのクッキー機能が有効になっている必要があります。

remote administrationセッションを通してIPパーシステンスを必要とする
セキュリティを向上させるために、各セッションの接続開始時のIPアドレスをセッション終了まで持続するようにRemote Administrationを設定することができます。これにより、IPパーシステンスが必要となるので、他者がセッションを盗むことはできなくなります。この機能によりセキュリティは向上しますが、プロキシサーバの使用、IPアドレスが動的に変化するインターネット接続を使用する場合には問題を引き起こす可能性があります。

MDaemon終了時にRemote Administrationも終了
MDaemonの終了と同時にRemote Administrationを終了させる場合はこのオプションを選択してください。このオプションを選択していない場合は、Remote Administrationはバックグラウンドで稼動し続けます。

HTTP圧縮を使用
Remote AdministrationセッションでHTTP圧縮を使用するにはこのチェックボックスをクリックします。

匿名利用率データを送信する
デフォルトでMDaemonのRemote Administrationは、匿名の、使用OSやブラウザバージョン、言語、といった情報を送信します。このデータは MDaemon TechnologiesでRemote Administrationの機能向上を目的に使用されます。匿名使用率データを送信したくない場合はこのオプションを無効にして下さい。

X-Forwarded-Forヘッダ
プロキシーサーバーが付与する場合のある、 `X-Forwarded-For` ヘッダを有効にするにはこのオプションを使用してください。このオプションはデフォルトで無効に設定されています。プロキシーサーバーがこのヘッダを挿入する場合にのみ使用してください。

Remote Administration URL
ユーザが、Remote Administrationでアカウント設定を編集するのに、詳細設定をクリックした際、Webmailが内部的に使用するURLです。Remote Administrationを内蔵のウェブサーバで使用する場合は、このフィールドは空白にしてください。Remote AdministrationをIISなどの外部のウェブサーバで使用するよう設定している場合は、ここにURLを入力してください。

Remote AdministrationのWebサーバをこれらのIPのみバインドする
Remote Administrationサーバを特定のIPアドレスに対してのみに制限する場合は、ここにアドレスをカンマで区切って入力してください。このフィールドが空白の場合は、Remote Administrationはドメイン 165 に指定されたすべてのIPアドレスをモニタします。

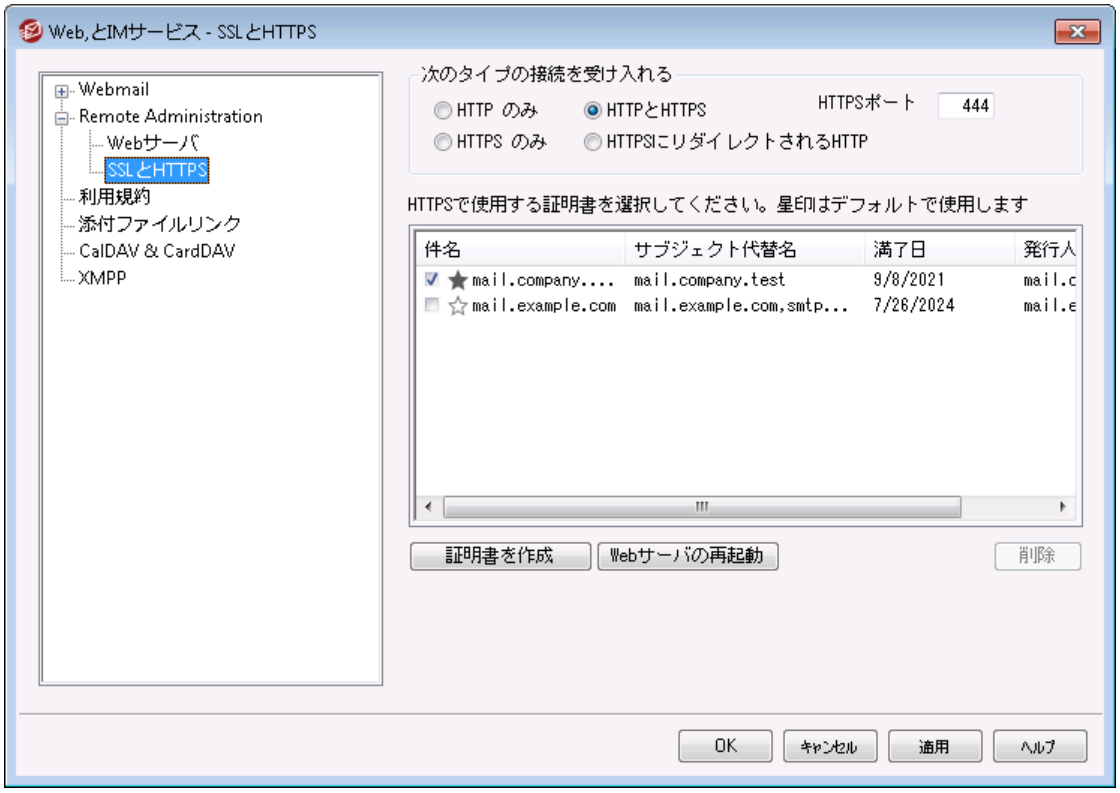
Remote Administrationの再起動（ポートやIISの値変更時に必要）
remote administrationサーバーを再起動する際はこのボタンをクリックします。注意点：ポート設定を変更した際には新しい設定を適用するためRemote Administrationの再起動が必要です。

メーリングリスト管理者を編集
メーリングリスト管理者ファイルを開いて、確認や編集を行うにはこのボタンをクリックします。

参照:

Remote Administration 321
Remote Administration » HTTPS 325
IISでRemote Administrationを実行する 329
テンプレートマネージャ » ウェブサービス 728
アカウントエディタ » ウェブサービス 656

3.6.2.2 SSLとHTTPS



MDaemonに搭載されているウェブサーバーはSecure Sockets Layer (SSL)プロトコルに対応しています。SSLとは、サーバー/クライアント間のウェブコミュニケーションを安全に行うための標準規格であり、サーバー認証、データ暗号化、TCP/IP接続用に追加のクライアント認証などの機能を提供しています。ほとんどのブラウザでは(HTTP over SSLのような)HTTPSに対応しているため、サーバー側に正しい証明書をインストールするだけで、クライアントはSSL機能を利用できるようになります。

Remote Administration でSSLを使用するには、設定 ≫ Web & IM サービス ≫ Remote Administrationの中のSSL & HTTPS画面へアクセスして下さい。利便性向上のため、この設定項目は、セキュリティ ≫ セキュリティ設定 ≫ SSL & TLS ≫ Remote Administration からも使用できます。

SSLプロトコルと証明書についての詳細は、次のページを参照して下さい: SSL & 証明書 523

この画面の設定は、Remote AdministrationがMDaemonの内蔵ウェブサーバーを使用している場合のみ適用されます。Remote AdministrationがIISなどの他のウェブサーバーを使用していた場合このオプションは使用できません。SSL/HTTPSは他のウェブサーバーで提供されているツールを使って設定を行う必要があります。

次の接続タイプを許可

HTTPのみ
Remote Administrationへの接続にHTTPSの利用を許可しない場合はこのオプションを選択します。HTTP接続のみが使用できるようになります。

HTTPとHTTPS
Remote AdministrationでSSL対応は有効にするものの、ユーザーにHTTPSの利用を強制しない場合には、このオプションを選択します。Remote Administrationは指定されたHTTPSポートでのみ接続を受け付けますが、Web Server 322で指定したRemote Administration用TCPポートへのhttp接続に対しても応答を行います。

HTTPSのみ
Remote AdministrationでHTTPS接続だけに応答するにはこのオプションを選択します。このオプションが有効の場合、Remote AdministrationはHTTPS接続のみ応答し、HTTPリクエストに対しては応答しません。

HTTPをHTTPSへリダイレクトする
全てのHTTP接続をHTTPSポートへリダイレクトするには、このオプションを使用します。

HTTPSポート
SSL通信でRemote Administrationが使用するTCPポートを指定します。デフォルトのSSLポートは444番です。デフォルトのSSLポートを使う場合は、Remote AdministrationのURLに、ポート番号を含む必要はありません。(例えば、"https://example.com" は "https://example.com:444"と同じURLを示します)

> このポートはWeb Server 322で指定したRemote Administrationポートとは異なります。Remote AdministrationでHTTP接続を許可するのであれば、Remote Administrationでは正しく接続できるよう異なるポートを使用する必要があります。HTTPS接続はHTTPSポートを使用する必要があります。

HTTPS/SSL用証明書の選択

ここにはお使いのSSL証明書が表示されます。Webmailで使用する証明書をクリックして選択します。デフォルトとして使用したい証明書の隣にある星印をクリックします。 MDaemonはTLSプロトコルの拡張であるServer Name Indication (SNI)に対応しており、サーバーのホスト名毎に、異なる証明書を使用する事ができます。MDaemonはアクティブな証明書を確認し、Subject Althernative Namesフィールドから、要求されたホスト名を選択します。(証明書の生成時、別名を指定する事もできます。)クライアントがホスト名を要求していなかった場合や、対象の証明書が存在していなかった場合、デフォルトの証明書が使用されます。Windowsの証明書ダイアログを起動し、証明書のレビューを行うには、対象の証明書をダブルクリックしてください。(これはブラウザベースのリモート管理画面ではなく、アプリケーション画面からのみ利用できます。)

削除
一覧から証明書を選択し削除をクリックします。確認画面で証明書を削除するかどうかを質問されます。

証明書の作成
このボタンをクリックしSSL証明書の作成ダイアログが起動します。

証明書詳細

ホスト名
証明書作成時、ユーザーが接続する際のホスト名を入力します。（例: wc.example.com）。

組織/会社名
証明書を所有する組織名や会社名を入力します。

ホスト名の別名（カンマで複数設定）
ユーザーが接続する際などに使用するWebmailの別ホスト名がある場合は、カンマで区切ったドメイン名をここへ入力します。ワイルドカードにも対応しており、例えば"*.example.com"は(例えば "wc.example.com", "mail.example.com"といった)example.comのサブドメインに対しても適用できます。

> MDaemonはTLSプロトコルの拡張であるServer Name Indication (SNI)に対応しており、サーバーのホスト名毎に、異なる証明書を使用する事ができます。MDaemonはアクティブな証明書を確認し、Subject Althernative Namesフィールドから、要求されたホスト名を選択します。クライアントがホスト名を要求していなかった場合や、対象の証明書が存在していなかった場合、デフォルトの証明書が使用されます。

暗号キーの長さ
この証明書で使用する暗号化キーのビットの長さを選択します。長い暗号化キーを使うとより安全な通信が行えますが、全てのアプリケーションで512を超える長さのキーに対応しているわけではありあせん。

国
サーバーが設置している国や地域を選択します。

ハッシュアルゴリズム
使用するハッシュアルゴリズムをSHA1かSHA2から選択します。デフォルトはSHA2です。

webサーバーの再起動

ボタンをクリックしウェブサーバーを再起動します。新しい証明書を使用するにはウェブサーバーの再起動が必要です。

証明書の管理にLet's Encryptを使用する

Let's Encryptとは、セキュアなウェブサイト向けに、従来手動で行っていた証明書の生成、検証、署名、インストール、更新といった複雑な処理を自動化し、無償の証明書を発行している認証局（CA）です。

Let's Encryptの自動処理で証明書を管理するのに、Let's Encrypt[541]画面にてMDaemon¥LetsEncryptフォルダに格納されたPower Shellスクリプトを簡単に実行するためのオプションを用意しています。スクリプトを実行するとLet's Encrypt用に、Webmail HTTPフォルダへhttp-01チャレンジに必要なファイルの配置を含む、全ての設定が行われます。ここでは、証明書用のドメインとしてデフォルトドメイン[165]のSMTPホスト名[167]が関連するホスト名と併せて使用され、証明書の取得と受信、Windowsへのインポート、MDaemon, Webmail, Remote Administrationでこれらの証明書を使用するためのMDaemon設定が行われます。更に、スクリプトはMDaemon¥Logs¥フォルダへLetsEncrypt.logというログも生成します。このログはスクリプト実行の度に削除され再生成され、スクリプトの開始時間が記録されます。通知用の管理者アドレスへは、エラー発生時にはメールでの通知も行われます。詳細についてはLet's Encrypt[541]を参照してください。

SSLと証明書についての詳細はこちらを参照して下さい:

IISでRemote Administrationを使用する[329]
SSLと証明書[523]
SSL証明書の作成と利用[830]

Remote Administrationについての詳細はこちらを参照して下さい:

Remote Configuration[321]
Remote Administration ≫ Webサーバ[322]
Webアクセスのデフォルト[728]
アカウントエディタ ≫ Web[656]

3.6.2.3 Remote AdministrationをIISで実行する

MDaemonには内蔵ウェブサーバが搭載されており、Remote Administrationは必ずしもIIS(Internet Information Server)を必要としません。しかし、Remote AdministrationはIISに対応しており、ISAPI DLLとして動作します。

IIS 5で動作させるように設定するには:

1.Remote Administrationを停止します。MDaemon管理画面の画面左側のRemote Administrationエントリを右クリックし、有効/無効を切り替えるをクリックする事でもRemote Administrationを停止する事ができます。

2.IIS管理プログラム(Start -> 設定 -> コントロールパネル -> 管理ツール -> インターネットサービスマネジャ)を起動します。

3.既定のWebサイトを右クリックして新規作成→仮想ディレクトリを選択します。

4.ウィザードにしたがって仮想ディレクトリを作成します。以下はウィザードで使用する名前とロケーションの例ですが、Remote Administrationのロケーションによって必ずしもこの例が適しているとは限りません。

a. エイリアス: “WebAdmin”。[次へ]をクリックします。

b. ディレクトリ: “c:¥mdaemon¥webadmin¥templates”。[次へ]をクリックします。

c. [次へ]をクリックします。

d. [完了]をクリックします。

5.実行アクセス権を[スクリプトのみ]に設定します。

6.アプリケーション保護を「低」に設定します。

7.仮想ディレクトリ画面のアプリケーションの設定で[構成]ボタンをクリックします。

8.[マッピング]タブで[追加]をクリックします。

9.実行ファイルフィールドで[c:¥mdaemon¥webadmin¥templates¥WebAdmin.dll]を入力します。このフィールドには空白を含むことはできません。ファイルパスに空白が含まれる場合は、8.3形式(8文字以内の英数字.3文字以内の英数字)に変換する必要があります。[dir /x]コマンドによって、そのファイルまたはディレクトリの8.3形式が表示されます。

10.拡張子フィールドに[.wdm]と入力し動詞欄で[すべての動詞]を選択します。

11.[スクリプトエンジン]チェックボックスを有効にします。

12.[OK]をクリックします。

13.その他のすべてのマッピングを削除することも可能です。次に[OK]をクリックします。

14.ドキュメント画面のデフォルトドキュメントに[login.wdm]を追加して、その他のすべてのエントリをリストから削除します。

15.MDaemonに移動して、設定→**Web**と**IM**サービス→**Remote Administration**と進み、[Remote Administrationサーバを有効にする]と[Remote AdministrationをIISで実行する]の両方のチェックボックスを有効にします。

16.Remote Administration URLの欄に[¥WebAdmin¥login.wdm]と入力します。

17.[OK]をクリックします。

IIS 6で動作させるように設定するには:

Remote Administration用の新しいアプリケーションプールを作成します:

1. Remote Administrationが稼働していた場合はこれを停止します。MDaemonの設定画面からサーバーの中のRemote Administrationを右クリックし、有効/無効を切り替えるをクリックして下さい。
2. IISマネージャを起動します。(Start -> 設定 -> コントロールパネル -> 管理ツール -> IISマネージャ)
3. アプリケーションプールを右クリックします。
4. 新規作成→アプリケーションプールをクリックします。
5. アプリケーションプールIDフィールドへ「Alt-N」と入力し、OKをクリックします。
6. **Alt-N**を右クリックします。
7. プロパティをクリックします。
8. パフォーマンスタブをクリックします。
9. 「アイドルなワーカープロセスの解放までの待ち時間」と「カーネル内要求キューを制限する」を無効にします。
10. 識別タブをクリックします。
11. ドロップダウンメニューから、ローカルシステムを選択します。
12. [OK]をクリックします。

Remote Administration用の仮想ディレクトリを作成する:

1.IISマネージャを起動します。(Start -> 設定 -> コントロールパネル -> 管理ツール -> IISマネージャ)

2.ウェブサイトを右クリックして、新規作成(仮想ディレクトリ)を選択します。

3.仮想ディレクトリのエイリアスを指定します。(例:WebAdmin)

4.パスの入力欄でRemote Administrationのテンプレートディレクトリのパスを入力します。(例:C:\Program Files\Alt-N Technologies\WebAdmin\Templates)

5.[Read]と[Run Script]はチェックされたままにしておきます。

6.ウィザードを終了して作成された仮想ディレクトリを右クリックします。

7.[プロパティ]を選択します。

8.ホームディレクトリ 画 面 でアプリケーションプールを[Alt-N]に変 更します。

9.[構 成]ボタンをクリックします。

10.[追 加]をクリックしてISAPI拡 張 マッピングを追 加します。

11.実 行 ファイルフィールドに[WebAdmin.dll]ファイルへのパスを入 力します。(例: C:¥Program Files\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll)

12.拡 張 子 フィールドに[.wdm]と入 力します。

13.[スクリプト エンジン]と[ファイルの存 在 を確 認 する]のチェックボックスを有 効 にします。

14.[OK]をクリックします。

15.その他 のすべてのマッピングを削 除 することも可 能 です。次 に[OK]をクリックします。

16.ドキュメント タブを開きます。

17.[Enable default content page]チェックボックスがチェックされていることを確 認します。

18.リストに[login.wdm]のみがあることを確 認します。

19.[OK]をクリックして仮 想 ディレクトリのプロパティを終 了します。

許 可 されたウェブ拡 張 子 のリストに.wdm を追 加 する:

1.[Webサービスの拡 張 子]フォルダをクリックします。

2.[新しいWebサービスの拡 張 子 の追 加]をクリックします。

3.拡 張 子 の名 前 フィールドに[WebAdmin]と入 力します

4.[追 加]をクリックしてWebAdmin ISAPI拡 張 子 を参 照します。(例: C:¥Program Files¥Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll)

5.[Set extension status to allowed]チェックボックスを有 効 にします。

6.[OK]をクリックします。

7.MDaemonから[設 定→**Web**と **IM**サービス→**Remote Administration**] をクリックし、**Remote Administration**を外 部 **Web**サーバで実 行 を選 択します。

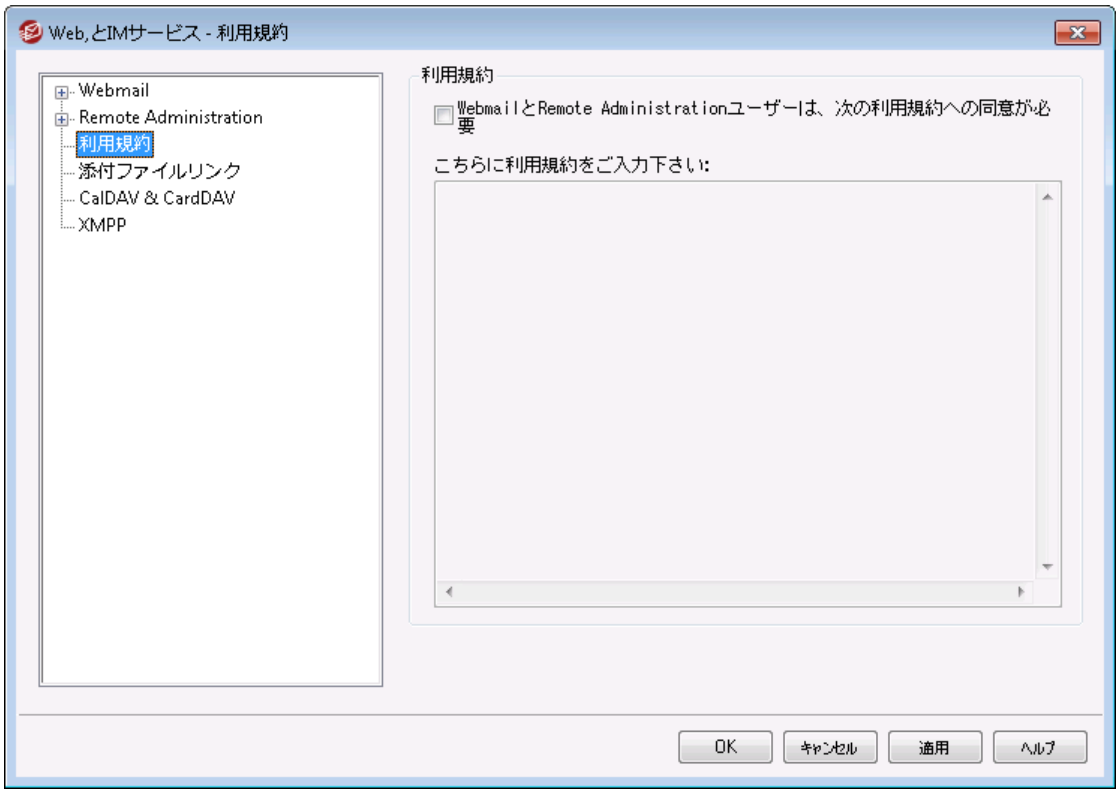
8.**Remote Administration URL**の欄 に "/WebAdmin/login.wdm"と入 力します。

9.OKをクリックします。

Remote Administrationに関する詳細情報は次を参照して下さい:

Remote Administration 321
Remote Administration ≫ Webサーバ 322
Remote Administration » SSL & HTTPS 325
Template Manager ≫ ウェブサービス 728
アカウントエディタ ≫ ウェブサービス 656

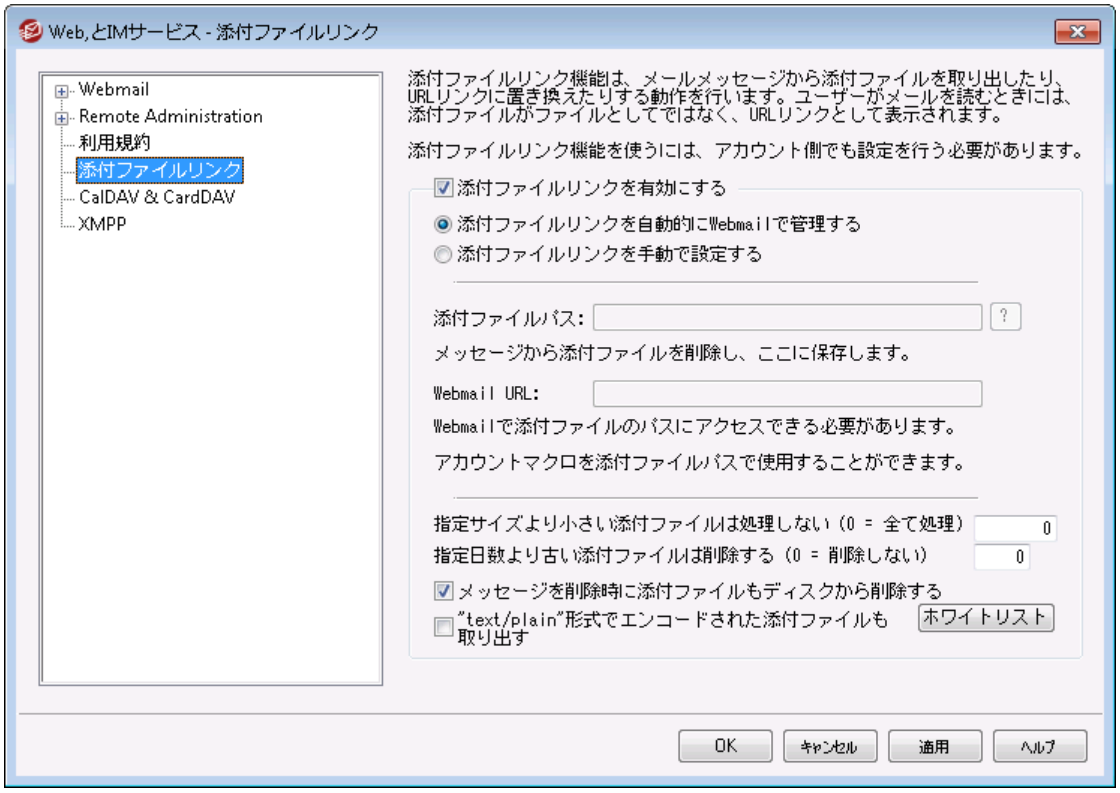
3.6.3 利用規約



WebmailとRemote Administrationsユーザーは、次の利用規約への同意が必要

WebmailとRemote Administrationユーザーがサインインする度に利用規約に同意させる場合はこのオプションを有効化し、利用規約を入力してください。

3.6.4 添付ファイルリンク



添付ファイルリンク(設定 ≫WebとIMサービス ≫添付ファイルリンク)は、MDaemonで受信メールメッセージから添付ファイルを取り除き、指定された位置に保存し、対象ファイルを各メールでURLに置き換える機能です。受信者側は、メールの中のリンクをクリックする事で、添付されていたファイルをダウンロードできます。この機能により、大きなサイズの添付ファイルが付いたメールをユーザーが受信する際や、そういったメールを含むメールフォルダを同期する際の処理速度を大きく向上させる事ができます。

添付ファイルリンクは、添付ファイルが中央で一元管理され、ユーザーが自由にダウンロードできない事で、セキュリティや保護レベルの向上を図る事もできます。さらに、"添付ファイルを自動的にWebmailで管理する"オプションを選択すると、ファイルの場所やWebmail URLは自動的に処理されます。添付ファイルリンクの管理を手動で行うよう選択した場合、ファイルを保存場所を指定する事ができ、保存場所をダイナミックに指定するための特別なマクロを使用する事もできます。添付ファイルリンクを使用するには、この画面のオプションを使って、添付ファイルリンク機能を全体として有効化し、アカウント毎の設定を、アカウントエディタの添付ファイル669で個々に行う必要があります。同じ画面の中で、送信メールに対しても添付ファイルを有効にでき、これによって添付ファイルが展開され、リンクへ置き換えられます。最後に、MDaemonがメール本文に挿入する添付ファイルへのリンクは、ファイルのパスを直接含むものではなく、固有の識別子であるGUIDを使って、内部的にファイルの実際の保存場所を示しています。GUIDマップはAttachmentLinking.datファイルへ保管されています。

添付ファイルリンクは(存在する場合は) MIMEヘッダのファイル名を使用します。ファイル名が50文字を超える場合は最後の50文字のみが使用されます。拡張子がない場合は、".att"が使用されます。

デフォルトで、添付ファイルリンク機能は"MDaemonは次のファイルをこのリンクへ置き換えました"というテキストを特定のメールに挿入します。このテキストを変更するには、¥app¥フォルダの中のMDaemon.iniファイルへ次のキーを追加し、MDaemonを再起動します。

```
[AttachmentLinking]
Header Text=テキストを入力
```

添付ファイルリンクを有効にする
アカウントエディタの添付ファイル[669]で、添付ファイルリンクを使用するよう設定した全てのアカウントで、添付ファイルリンク機能を有効にするには、このチェックボックスを使用します。この全体オプションを有効にすると、全てのMDaemonアカウントに対してアカウント毎の設定を有効化するかどうかを確認されます。「はい」を選択すると、全てのアカウント向けに添付ファイルリンクが有効になり、アカウントの作成[740]テンプレートの関連オプションも有効化されます。「いいえ」を選択すると、添付ファイルリンク機能は有効になりますが、アカウント毎の設定は有効にはならず、使用するアカウント毎に手動で有効化する必要があります。添付ファイルリンクを有効にしている間は、Webmailサーバもアクティブである必要があります。

添付ファイルリンクを自動的にWebmailで管理する
これは、添付ファイルリンクが有効な場合のデフォルトオプションです。Webmailで自動的に添付ファイルリンクを処理させたい場合、このオプションを使用します。抽出されたファイルは "...\MDaemon\Attachments\$DOMAIN$\$MAILBOX$\"に保存されます。

添付ファイルリンクを手動で設定する
抽出された添付ファイルを保存するフォルダを指定する場合、このオプションを選択します。このオプションを選択する時、添付ファイルのパスおよびWebmail URLを指定する必要があります。

添付ファイルパス
展開した添付ファイルの保存先フォルダをここで指定します。静的なファイルパスを設定するか、テンプレート[724]やスクリプト[766]マクロでダイナミックパスを指定します。例えば、"$ROOTDIR$¥Attachments¥$DOMAIN$¥"と指定する事で、MDaemonのルートフォルダ(通常C:¥MDaemon¥)の中の"Attachments"サブフォルダに、ドメイン名毎のサブフォルダが生成され、グループ分けされます。この例に当てはめると、"user1@example.com"の添付ファイルは"C:¥MDaemon¥Attachments¥example.com¥"へ保管されます。添付ファイルの保存先は"$MAILBOX$"テンプレートマクロを使う事で更に細分化できます。この場合は、user1の添付ファイルは、"\example.com\"のuser1フォルダへ保管されます。これにより、新しいファイルパスは、"C:\MDaemon\Attachments\example.com\user1\"となります。

Webmail URL
WebmailのURLをここへ入力します(例えば、http://mail.example.com:3000/WorldClient.dll)。MDaemonは、メールへ挿入する添付ファイルへのリンクに、このURLを使用します。

このサイズ(KB)を下回る添付ファイルを無視する(0 = 無制限)
添付ファイルがメールから展開される最小サイズを指定します。このオプションはサイズが小さい添付ファイルを展開したくない場合に使用します。0を指定すると、添付ファイルリンクは、ファイルサイズに依らず全ての添付ファイルに対して行われます。

この日数を経過した添付ファイルを削除する(0 = 削除しない)
指定した日数を超えた添付ファイルを削除する場合はこのオプションを使用します。日時クリーンアップイベントの一つとしてMDaemonは、指定した添付ファイルフォルダ又はそのサブフォルダ内にある、指定した日数よりも古いファイルを削除します。デフォルトフォルダは、"<MDaemonRoot>\Attachments\..."です。添付ファイルフォルダを他の場所へ変更している場合は添付ファイルは削除されません。このオプションはデフォルトで無効(0に設定)になっています。

メッセージが削除時に添付ファイルもディスクから削除する
メッセージが削除されると同時にそのメッセージにリンクされている添付ファイルを削除する場合は、このオプションを有効にしてください。

オプションが有効で、ユーザがPOP3でメールの受信を行っており、サーバー上にメッセージを残さない設定になっていた場合、抽出された添付ファイルは全て削除されます。このオプションが無効であれば、添付ファイルも失われませんが、一方で、不必要なファイルでハードディスク容量を消費してしまう結果になります。一般的に、すべてのPOPクライアントはサーバ上にメッセージを残す機能を搭載しています。

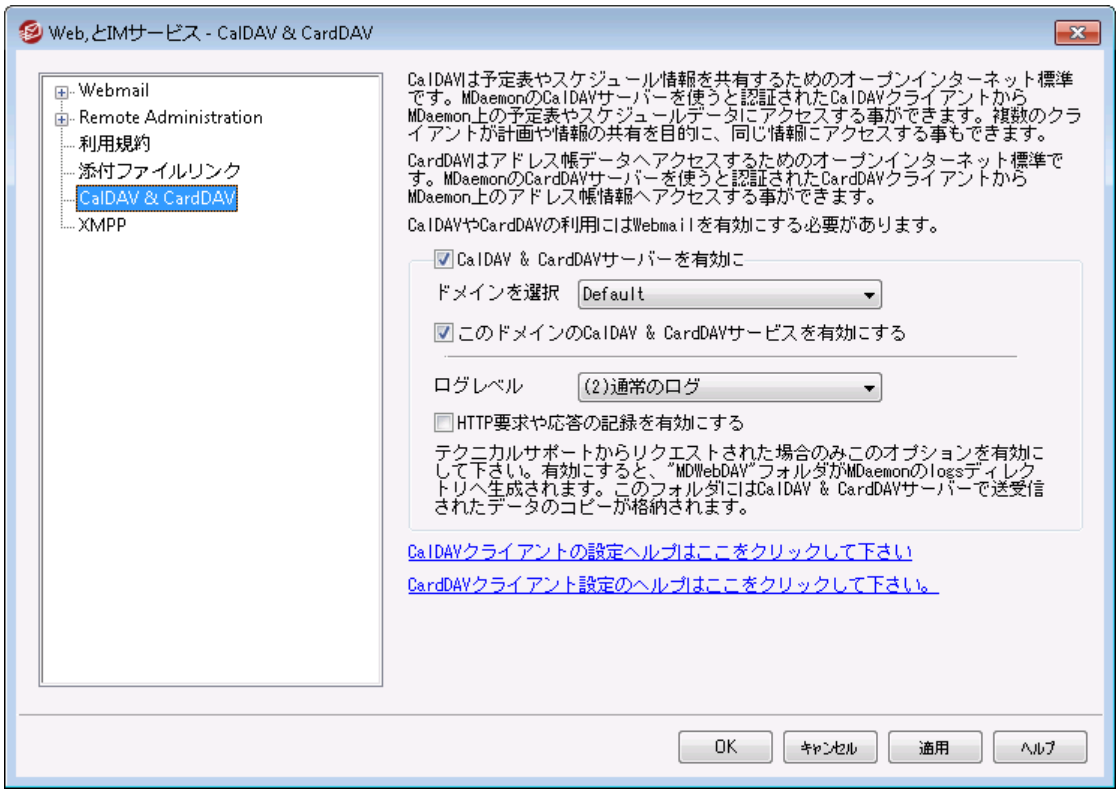
"text/plain"でエンコードされた添付ファイルも取り出す
デフォルトではtext/plain形式の添付ファイルは展開されません。自動展開したい場合はこのチェックボックスをクリックします。

除外リスト
添付ファイルリンクの除外リストを開くにはこのボタンをクリックします。メールから展開させたくないファイル名を記載します。Winmail.datはデフォルトで含まれています。

参照:

アカウントの作成テンプレート 723
アカウントエディタ » 添付ファイル 669
テンプレートマクロ 724
スクリプトマクロ 766

3.6.5 CalDAV & CardDAV



CalDAVはカレンダーや予定表の情報を管理・共有するためのインターネット標準プロトコルです。MDaemonのCalDAVサポートにより、CalDAVに対応したクライアントを使っているユーザーは個人の予定表やタスクにクライアントからアクセスしたり管理したりできるようになります。また、アクセス権[285]に基づき、パブリック[283]や共有[676]の予定表や仕事データへもアクセスできるようになります。CardDAVは連絡先やアドレス帳データへアクセスするための標準規格です。MDaemonのCardDAVサーバーにより、認証済のCardDAVクライアントはMDaemon上で管理している連絡先情報へアクセスする事ができるようになります。

CalDAV & CardDAVサーバーを有効にする

CalDAV/CardDAVサポートはデフォルトで有効です。ただし、これにはWebmailが必須で、利用するためにはWebmailを有効にする必要があります[295]。CalDAVやCardDAVを使用しない場合はこの機能を無効にします。ドメイン毎に有効/無効の設定を行うには、後述のオプションを使用して下さい。

ドメインのデフォルトCalDAV/CardDAV設定を変更する

初期設定では、全てのMDaemonドメインでCalDAV/CardDAVはドメインの選択のドロップダウンリストのデフォルトを元に有効化又は無効化されています。デフォルト設定は次の手順で変更できます。

1. *ドメインを選択*のドロップダウンリストで、デフォルトを選択します。
1. **このドメインでCalDAVサーバーを有効にする**のチェックボックスを有効にして、全てのドメインでCalDAVを有効化するか、デフォルト設定を無効化する場合はこのチェックボックスを無効にします。
2. **Ok**をクリックします。

このドメインでCalDAVサーバーを有効/無効にする
個々のドメインのデフォルトCalDAV/CardDAV設定は、次のように上書き設定します:

1. *ドメインを選択*のドロップダウンリストで、**デフォルト**を選択します。
2. **このドメインでCalDAV & CardDAVサーバーを有効にする**のチェックボックスを有効にして、このドメインでCalDAVやCardDAVを有効化するか、チェックボックスを外してこれらを無効化します。
3. **Ok**をクリックします。

ロギング

ログレベル
ドロップダウンリストを使ってどのようなCalDAV/CardDAV処理をログに残すのかを指定できます。ログのレベルは 1-デバッグログ 2-通常のログ（デフォルト）, 3-警告とエラーのみ 4-エラーのみ 5-クリティカルエラーのみ 6-ログを残さない の6種類から選択できます。これは全体設定で、特定のドメインにのみ適用する事はできません。

HTTP要求や応答のログを有効にする
有効にすると、MDaemonのlogsフォルダの中に`MDWebDAV`フォルダが生成されます。CalDAV/CardDAVサーバーが送受信した全てのデータはこのフォルダへ記録されます。このオプションはサポート窓口で有効化するよう言われた場合を除いては使用する機会はほとんどなく、有効にする必要はありません。

CalDAV クライアントの設定

RFC 6764 (Locating Services for Calendaring Extensions to WebDAV (CalDAV) and vCard Extensions to WebDAV (CardDAV)) に対応しているクライアントは、サーバー、ユーザー名、パスワードのみで設定が行えます。正しいURLへクライアントがアクセスできるようDNSレコードを設定する事ができます。DNSレコードが設定されていない場合、ユーザーは "hostname/.well-known/caldav"という、特別な「well-known URL」を使う事ができます。例: `http://example.com:3000/.well-known/caldav` 。Webmailの内蔵ウェブサーバーはwell-known URLに対応しています。.

Lightningプラグイン経由のMozilla Thunderbirdのような、CalDAVサービスの自動設定に未対応のクライアントは、それぞれの予定表や仕事の一覧用に、URLをフルで入力する必要があります。MDaemonのCalDAV URLは次のように構成されています:

予定表と仕事
ユーザーのデフォルト予定表や仕事のリストの場合:

`http://[host]/webdav/calendar`
(e.g. `http://example.com:3000/webdav/calendar`)

`http://[host]/webdav/tasklist`
(e.g. `http://example.com/webdav/tasklist`)

ユーザーのカスタマイズされた予定表や仕事のリストの場合:

`http://[host]/webdav/calendar/[calendar-name]`
(e.g. `http://example.com/webdav/calendar/personal`)

http://[host]/webdav/tasklist/[tasklist-name]
(e.g. http://example.com/webdav/tasklist/todo)

ユーザーのサブフォルダ内にあるカスタマイズされた予定表や仕事のリストの場合:

http://[host]/webdav/calendar/[folder]/[calendar-name]
(e.g. http://example.com/webdav/calendar/my-stuff/personal)

http://[host]/webdav/tasklist/[folder]/[tasklist-name]
(e.g. http://example.com/webdav/tasklist/my-stuff/todo)

共有予定表と仕事
他のユーザーのデフォルト予定表や仕事のリストの場合:

http://[host]/webdav/calendars/[domain]/[user]
(e.g. http://example.com/webdav/calendars/example.net/frank)

http://[host]/webdav/tasks/[domain]/[user]
(e.g. http://example.com/webdav/tasks/example.net/frank)

他のユーザーのカスタマイズされた予定表や仕事のリストの場合:

http://[host]/webdav/calendars/[domain]/[user]/[calendar-name]
(e.g. http://example.com/webdav/calendars/example.net/frank/personal)

http://[host]/webdav/tasks/[domain]/[user]/[tasklist-name]
(e.g. http://example.com/webdav/tasks/example.net/frank/todo)

パブリック予定表と仕事
ドメインのデフォルト予定表や仕事のリストの場合:

http://[host]/webdav/public-calendars/[domain]
(e.g. http://example.com/webdav/public-calendars/example.com)

http://[host]/webdav/public-tasks/[domain]
(e.g. http://example.com/webdav/public-tasks/example.com)

パブリックフォルダの最上位にある予定表や仕事リストの場合:

http://[host]/webdav/public-calendars/[calendar-name]
(e.g. http://example.com/webdav/public-calendars/holidays)

http://[host]/webdav/public-tasks/[tasklist-name]
(e.g. http://example.com/webdav/public-tasks/projects)

OutlookDAVクライアントのテストには十分な注意が必要です。過去に、複数のMAPIプロファイルが存在している環境で、サーバーの応答により全ての予定表データが消えてしまうというクライアント側の問題が確認されています。OutlookDAVはデフォルトのMAPIプロファイルのみに対応しています。

CalDAVクライアントの設定に関する詳細は、MDaemon Knowledge BaseでCalDavと検索して下さい。

CardDAVクライアントの設定

RFC 6764 (Locating Services for Calendaring Extensions to WebDAV (CalDAV) and vCard Extensions to WebDAV (CardDAV))に対応しているクライアントは、サーバー、ユーザー名、パスワードのみで設定が行えます。Appleアドレス帳やiOSはこの規格に準拠しています。正しいURLへクライアントがアクセスできるようDNSレコードを設定して下さい。DNSレコードが設定されていない場合、ユーザーは "/.well-known/carddav"という、特別な「well-known URL」を使う事ができます。Webmailの内蔵ウェブサーバーはwell-known URLに対応しています。CardDAVサービスへの自動接続に未対応のクライアントは、フルURLを入力する必要があります。

広く使われているCardDAVクライアントにはApple Contacts（Mac OS Xに搭載されています）、Apple iOS (iPhone)、SOGOプラグインを使ったMozilla Thunderbirdなどがあります。

OS X 10.11（EL Capitan）の現時点では、Apple Contactsアプリケーションが1つのコレクション/フォルダのみに対応しています。CardDAVサーバーがApple Contactsアプリケーションを検出すると、認証済ユーザーのデフォルト連絡先フォルダのみが返されます。更に、OS X 10.11（EL Capitan）にはダイアログの「詳細」表示を使ってCardDAVアカウントを追加する際に発生する既知の問題が確認されています。

アドレス帳へのアクセス

「addressbook」へのパスはデフォルトアドレス帳へのショートカットです。

`http://[host]/webdav/addressbook` - デフォルトの連絡先フォルダ

`http://[host]/webdav/addressbook/friends` -「friends」連絡先フォルダ

`http://[host]/webdav/addressbook/myfolder/personal` - 「myfolder」のサブフォルダである「personal」連絡先フォルダ

アクセス権のある他のユーザーの共有フォルダへのアクセス

「contacts」へのパスはデフォルト共有連絡先へのショートカットです。

`http://[host]/webdav/contacts/example.com/user2` - user2@example.comのデフォルト連絡先フォルダ

`http://[host]/webdav/contacts/example.com/user2/myfolder` - user2@ example.comの「myfolder」連絡先フォルダ

アクセス権を持つパブリックフォルダへのアクセス

「public-contacts」へのパスはデフォルトパブリック連絡先へのショートカットです。

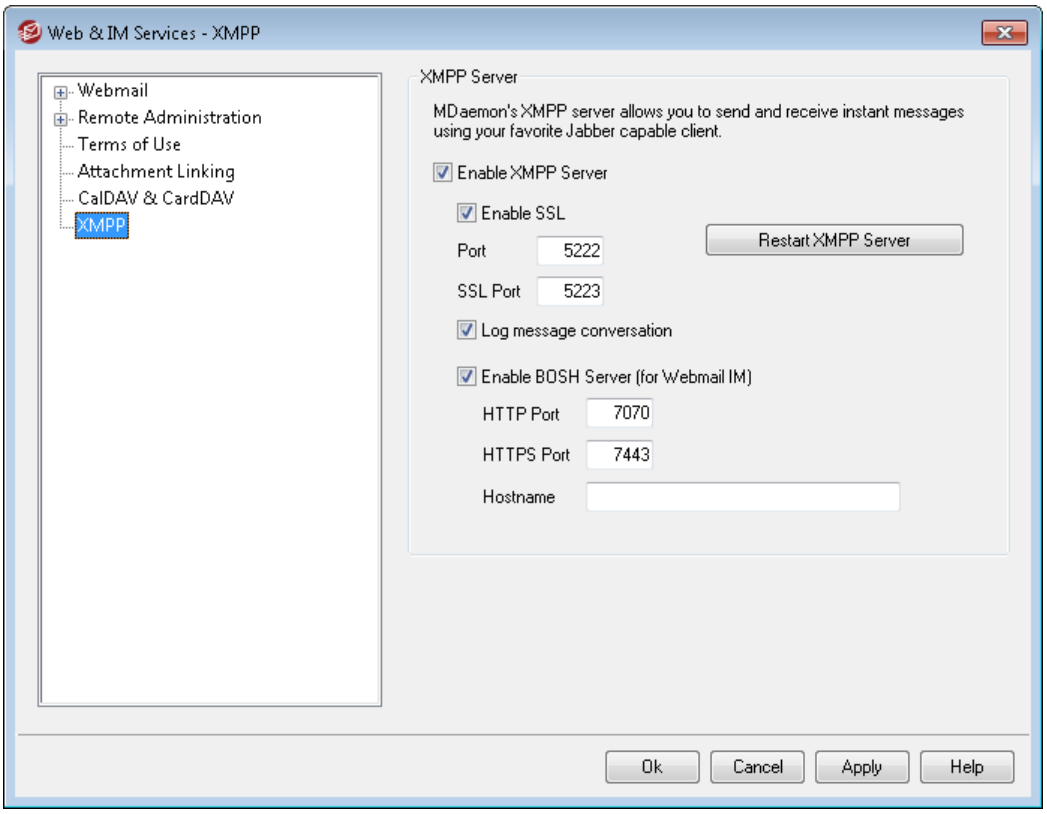
`http://[host]/webdav/public-contacts/example.com` - example.comのデフォルト連絡先フォルダ

`http://[host]/webdav/public-contacts/foldername` - パブリックフォルダの最上位にある「foldername」連絡先フォルダ

OutlookDAVクライアントのテストには十分な注意が必要です。OutlookDAVはデフォルトMAPIプロファイルにのみ対応しています。複数のMAPIプロファイルが存在している場合、サーバーからの応答に含まれている全てのデータに対して削除コマンドを発行してしまう可能性があります。

CardDAVクライアントの設定についての詳細は MDaemon Knowledge Base でCardDavと検索して下さい。

3.6.6 XMPP



MDaemonにはExtensible Messaging and Presence Protocol (XMPP)サーバーがパッケージされており、これはJabberサーバとの呼ばれています。これにより、MDaemon Instant Messenger 292やPidgin, Gajim, Swiftいった、サードパーティーのXMPPクライアントを使って、インスタントメッセージの送受信が行えます。クライアントはほとんどのOSやモバイル端末用に提供されています。

XMPPサーバーはWindowsサービスとしてインストールされ、デフォルトで5222番ポート(STARTTLSを使ったSSL)と5223番ポート(専用SSL)を使用します。XMPPサーバーはMDaemonで有効化されているSSL設定情報を使って通信を行います。また、XMPPクライアントによってはホスト名の自動検出に

DNS SRVを使用するものもあります。詳細はhttp://wiki.xmpp.org/web/SRV_Recordsを参照して下さい。

ユーザーは選択したXMPPクライアントへメールアドレスとパスワードでログインします。クライアントによっては、メールアドレスとログインIDを異なるコンポネントとして扱う場合もあります。例えば、frank@example.com ではなくログイン/パスワードにはfrankを使用し、ドメイン名としてexample.comを指定するといった形式です。

複数のユーザーチャットは、通常「rooms」や「conference」として表示されます。グループチャットのセッションを開始するには、roomやconference(名前をつけて下さい)を作成し、他のユーザーを招待します。多くのクライアントではサーバーの場所を指定する必要はなく、名前だけで招待が行えます。チャットの場所を指定する必要がある場合は、名前と場所を次のように記載して下さい: "room@conference.<your domain>"(例. Room01@conference.example.com).

(Pidginなど)ユーザー検索に対応しているクライアントもあり、サーバー上のユーザーを名前やメールアドレスで検索し、簡単に連絡先として追加する事ができます。ユーザー検索サービスは、デフォルトで「search.(ドメイン名)」で指定します。% シンボルはワイルドカードとして使用できます。例えばメールアドレス欄に「% @ example.com」と入力する事で、@ example.comで終わる全てのメールアドレスを一覧表示する事ができます。

XMPPサーバー

XMPPサーバーを有効にする
このオプションをクリックしてXMPPサーバーを有効化します。インスタントメッセージを使用するには、MDIM 304 画面で**インスタントメッセージを有効**にする必要がある点にご注意下さい。

ポート
XMPPのデフォルトポートは5222番でSTARTTLSを使ったSSLに対応しています。

SSLポート
XMPPの専用SSLポートは5223番です。

XMPPサーバーの再起動
XMPPサーバーを再起動する際にはこのボタンをクリックして下さい。

メッセージを記録する
デフォルトで全ての会話はMDaemon\Logs\にあるXMPPServer-<date>.logへ記録されます。ログを残したくない場合はこのチェックボックスを無効にして下さい。

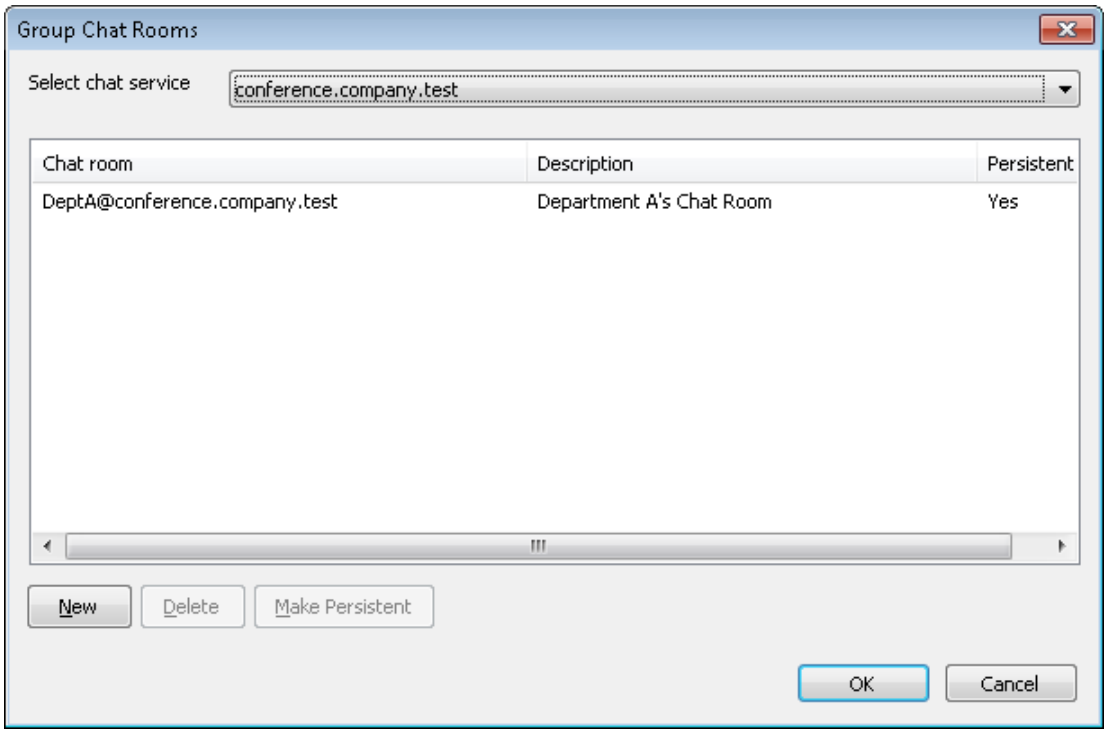
BOSHサーバーを有効にする(Webmail IM用)
BOSHサーバーを有効にするにはこのボタンをクリックすると、MDaemon Webmail内でインスタントメッセージを使用できるようになります。

HTTPポート
デフォルトでBOSHサーバーはHTTPポートの7070を使用します。

HTTPS Port
SSLを有効にする、を有効化していると、BOSHサーバーはこのHTTPSポートを使用します。デフォルトポートは7443です。

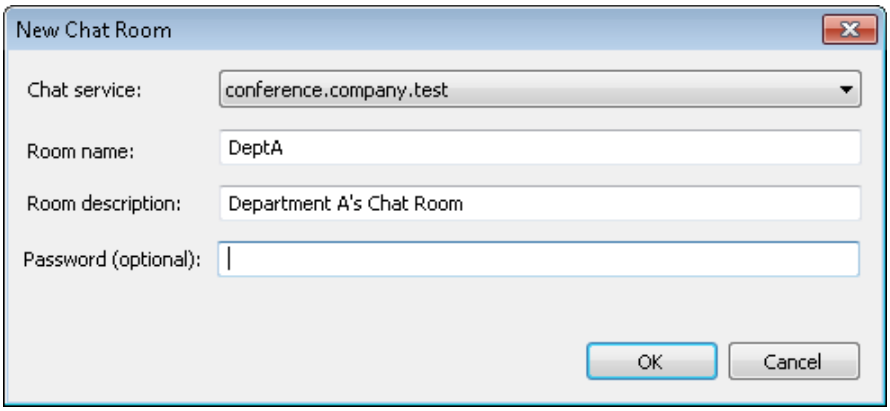
ホスト名
必要に応じてホスト名を指定します。

継続チャットルームの設定
このボタンをクリックしグループチャットルームのダイアログを起動します。従来、ユーザーが作成したチャットルームは、最後の方がチャットルームを退出すると削除されていましたが、このオプションを使用して、空室でも存在するチャットルームを作成できるようになりました。また、チャットルームを削除したり、一時的なチャットルームを継続チャットルームへ変換する事もできます。



チャットサービスの選択
ドメインのチャットルームを選択します。

新規
このボタンをクリックし、継続チャットルームを作成します。



チャット サービスの選 択
チャット ルーム用 のサービスを選 択します。

ルーム名
チャット ルームの名 称を空 白なしで記 入します。

ルームの説 明
チャット ルームの説 明を入 力します。ユーザーは参 加 するチャット ルームを選 択 する際 この説 明を閲 覧 できます。

パスワード（オプション）
チャット への参 加 にパスワードを要 求 する場 合 は、ここでパスワードを入 力します。

削 除
ルームを削 除 する場 合 は、これを選 択しこのボタンをクリックします。

継 続 する
一 時 的なチャット ルームが一 覧 にある場 合 は、対 象 のルームを選 択しこのボタンをクリックすると継 続 チャット ルームへ変 換されます。

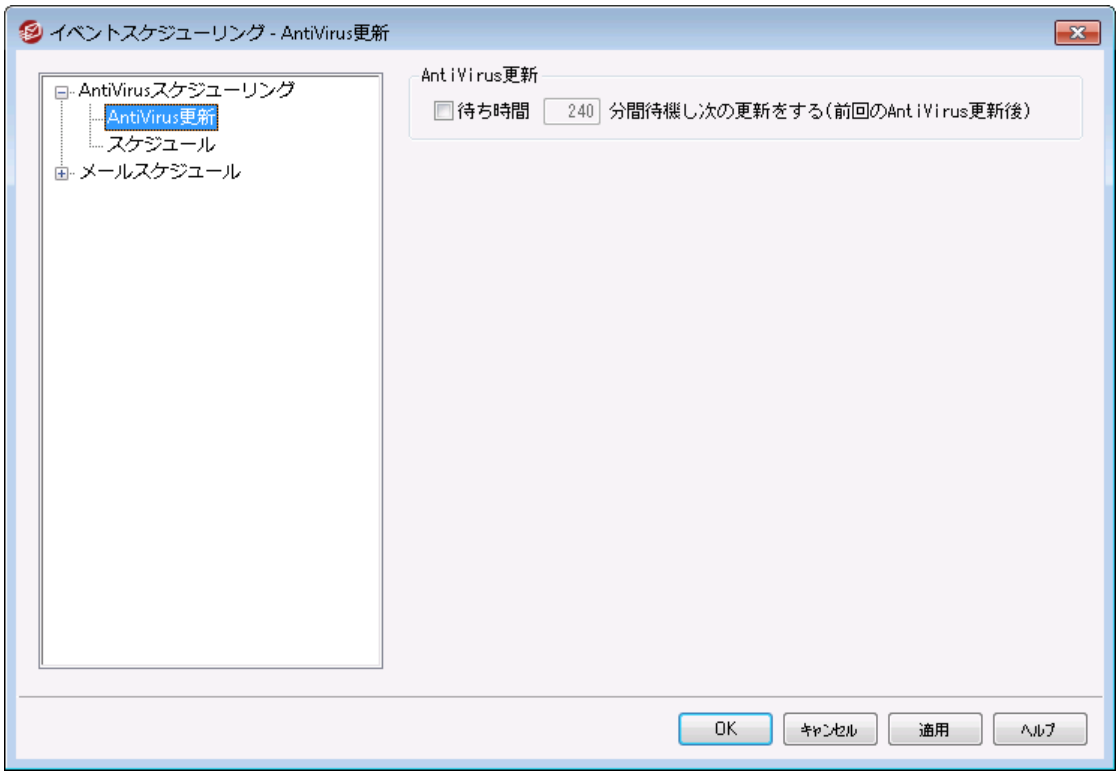
参照:

Webmail » MDIM 304

3.7 イベントスケジューリング

3.7.1 AntiVirusスケジュール

3.7.1.1 AntiVirus更新



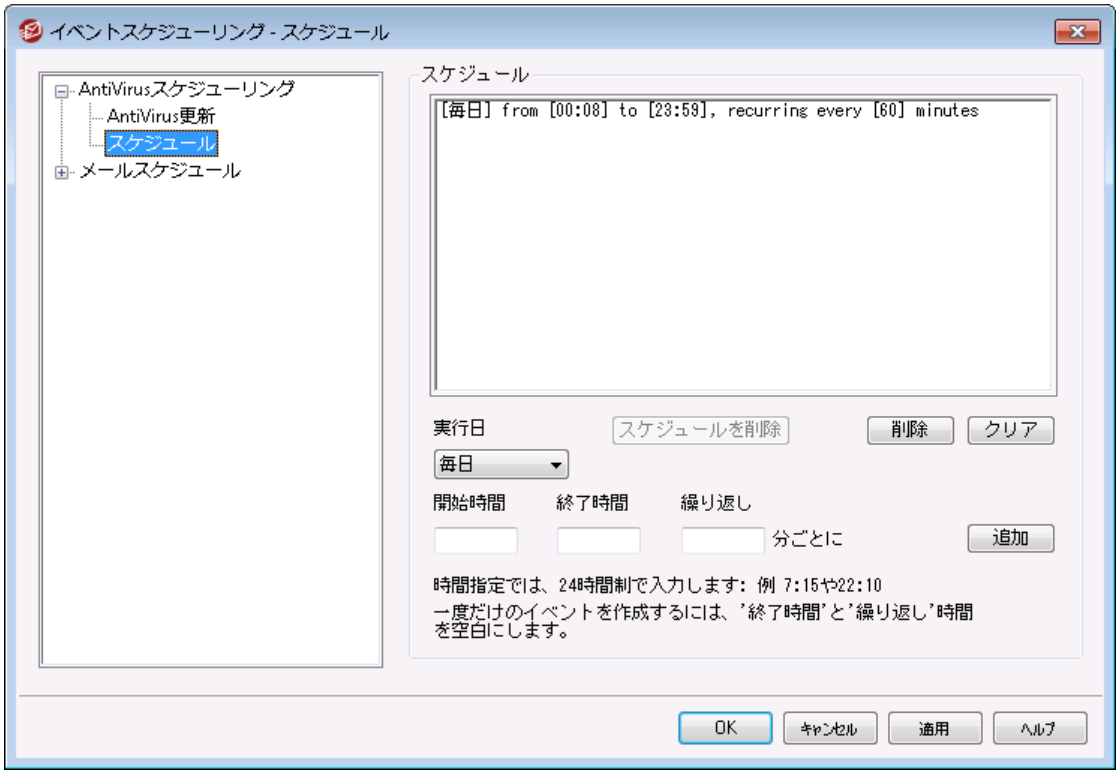
AntiVirusアップデート

待ち時間XX分間待機し次の更新をする(前回のAntiVirus更新時)
このチェックボックスをクリックして、ウイルス定義の新しい更新を確認するまでにAntiVirusが待機する時間を分単位で指定します。これは、実際には、自動か手動かを問わず、更新を最後に確認した後、AntiVirusが待機を試みる時間(分)です。スケジュールされたアップデートチェックや手動でのチェックは、この設定よりも高い優先度となっており、AntiVirusアップデートチェックが、それらの方法で行われた場合、このカウンタはリセットされます。したがって、たとえば、240分ごとに更新をチェックするようにこのオプションを設定し、100分後に手動で更新をチェックすると、このカウンタは再び240分にリセットされます。

参照:

AntiVirusスケジュール 345
AntiVirus 609
AntiVirus更新 613

3.7.1.2 スケジュール



AntiVirusアップデート スケジュールでは、特定の時間にAntiVirusのアップデートの有無をチェックできます。スケジュールは 設定» イベント スケジュール»AntiVirus更新»スケジュール からアクセスできます。

スケジュール

削除
リストからイベントを削除するには、対象のエントリを選択してからこのボタンをクリックします。

クリア
このボタンは、スケジュールからすべてのエントリを削除します。

スケジュールイベントの作成

実行日
スケジュールの新しいイベントを作成するときは、まずこのスケジュールされた更新チェックイベントが行うタイミングの日を選択します。毎日、平日(月曜日～金曜日)、週末(土曜日と日曜日)、または特定の曜日を選択できます。

開始時間
予定を開始する時間を入力します。00:00から23:59まで時間値が24時間制の形式である必要があります。これが繰り返されている予定でなく1つの予定の場合は、これは、入力は1つの時間値です(終了 と繰り返し [xx] 分ごとをブランクにします)

終了時間..
終了予定時間を入力します。00:00から23:59まで時間値が24時間制の形式である必要があります。また開始時間以降でなければなりません。例えば、開始が10:00である場合、この値は10:01から23:59までにできます。繰り返しの予定ではなく単独の場合は、このオプションをブランクにします。

[xx]分ごとに繰り返し
これは、AntiVirusが指定されたアップデートチェック開始時間から終了時間までの間の更新をチェックする時間間隔です. 繰り返されるイベントではなく、アップデートチェックを手動で行う場合、このオプションを空白のままにします。

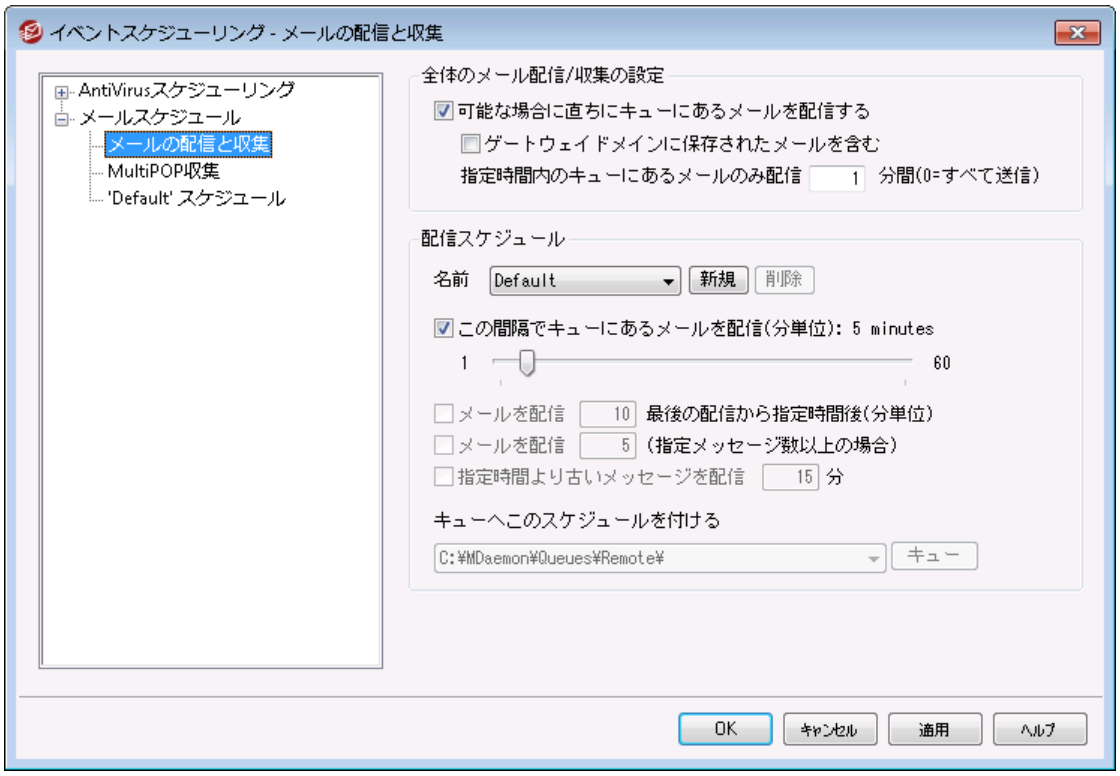
追加
実行日と開始時間、終了時間、繰り返し、を設定したら、イベントに予定を追加するには、このボタンをクリックします。

参照:

AntiVirus更新
AntiVirus 609
AntiVirusアップデータ 613

3.7.2 メールスケジュール

3.7.2.1 メールの配信と収集



設定 ≫ イベントスケジューリングから、MDaemonのイベントスケジューラを開きます。このダイアログから、MDaemonのリモートメール処理イベントを、詳細にも、シンプルにも、お好きな方法でスケジュールすることができます。メールスケジュール[351]で、メールの配信と収集の時間を、正確にスケジュールすることができ、一定の間隔でメールを処理するためにカウンタを使用することができます。また、スケジュールではなく、例えば一定の数のメールが溜まった場合や、配信待ち時間が指定した時間に到達した場合、といったトリガーで、メールの処理を行わせる事もできます。さらに、カスタムリモートメールキューへカスタムスケジュールを割り振る事もできます。カスタムスケジュールによって、様々なタイプのメッセージに対して異なるスケジュールを設定することができます。例えば、サイズの大きなメッセージやメーリングリストのメッセージ、特定のドメインなどに対してそれぞれのスケジュールを作成することができます。

イベントスケジューラのAntiVirus更新[343]でMDaemonのAntiVirus[587]アップデート確認頻度を設定します。

メール配信/収集の全体設定

可能な場合に直ちにキューにあるメールを配信する
このオプションが有効で、到着したメッセージがリモートキューへ入ると、MDaemonは次の指定時間やトリガーイベントを待つのではなく、すぐに*指定時間内のキューにあるメールのみ配信［xx］*で指定した時間内のメール全ての処理を行います。

...ゲートウェイドメインに保存されたメールを含む
このオプションを選択すると、ドメインゲートウェイへのメールもすぐに配信されます。ただし、このオプションは ゲートウェイエディタのゲートウェイ[234]設定画面で、[MDaemonがリモートメールを処理するたびに、保存メッセージを配信する]オプションが有効な場合のみ適用されます。

指定時間内のキューにあるメールのみ配信 [xx] 分間 (0=すべて送信)
このオプションは、上記の*可能な場合に直ちにキューにあるメールを配信する*オプションが配信に対してスプールする前に、どれほど頻度でキューに入れるか制限します。キューですべてを配達する代わりに、このオプションがリモートメール処理を起こす場合、MDaemonは、指定された時間内(分)で待ち行列にあるメッセージを処理します。
しかしながら、[キューを処理]キューツールバーボタンが押される、あるいは他の標準スケジューリング予定がリモートメール処理を開始する場合、全体のキューは、今まで通り処理されます。デフォルトで、このオプションは、1分にセットされます。リモートメール処理が発生するたびに、全体のキューを処理する場合、0に設定できますが、それほど効果がないのでお勧めしません。

上記のオプションはデフォルトスケジュールに適用されます。カスタムスケジュールは適用されません。(次の*名前...* オプションを参照)

配信スケジュール

名前...
ドロップダウンリストで編集するスケジュールを選択します。デフォルトのスケジュールは常にリモートメールキューとDomainPOPとMultiPOPで収集されるメールに使用されます。ダイアルアップサービスを使用した設定では、デフォルトスケジュールはLANドメインに使用されます。LANドメインは、ローカルエリアネットワークに指定したリモートドメインで、RASダイアルアップを必要としません。その他のスケジュールは、カスタムリモートメールキューに割り当てることができ、メールはコンテンツフィルタ[588]によって自動的にカスタムキュー[798]に転送することができます。スケジュールの編集が完了したら、[OK]ボタンをクリックしてください。スケジュールを変更し他のスケジュールを選択すると、他のスケジュールに移行する前に変更を保存するか破棄するかを確認するダイアログボックスが開きます。

新規
新しいスケジュールを作成するには、このボタンをクリックしてください。カスタムスケジュールの時間や設定を行う前に名前を指定するダイアログボックスが開きます。スケジュールの名前を指定すると、対応するメールスケジュール[351]画面が左側にメニューを作成し、スケジュールに時間を指定する画面を使用します。

削除
カスタムスケジュールを削除するには、[名前]のドロップダウンリストで目的のスケジュールを選択し、[削除]ボタンをクリックします。削除を確認するダイアログボックスが開きます。カスタムスケジュールを削除した場合でも、カスタムリモートキューや関連するコンテンツフィルタルールは削除されません。しかし、カスタムキューを削除した後に、関連するスケジュールを削除すると、キューと共に関連するコンテンツフィルタルールも削除されてしまいます。

この間隔でキューにあるメールを配信(分単位)
このチェックボックスを選択しスライドバーを左右にスライドして、メール処理セッション間隔の時間を設定してください。1分から60分の間隔で設定することができます。設定された時間を経過するとリモートメールを処理します。このチェックボックスが無効の場合、他のスケジュールオプションの設定によって処理間隔が決定します。

メールを配信 [xx]最後の配信から指定時間後(分単位)
セッションを始動した要因に関係なく、リモートメール処理セッションで発生する最後のセッション後、一定の時間間隔で発生する必要とする場合、このオプションを使用します。特定の時間を設定する場合、または、**この間隔でキューにあるメールを配信**スライドバーで使用する場合、使用する厳密に一定の間隔とは異なり、このオプションの時間間隔はメールが処理される各時間をリセットします。

メールを配信 [xx](指定メッセージ数以上の場合)
リモートキューのメッセージ数が、ここで指定した値以上の場合、MDaemonは、メールセッションを開始します。これらのメールセッションは、スケジュールされているその他のセッションに追加されます。

指定時間より古いメッセージを配信 [xx]分
このコントロールが有効な場合、リモートキューに配信待ちしているメッセージが、ここで指定した時間以上を経過した場合、メールセッションが開始されます。これらのセッションは、スケジュールされているその他のセッションに追加されます。

キュー

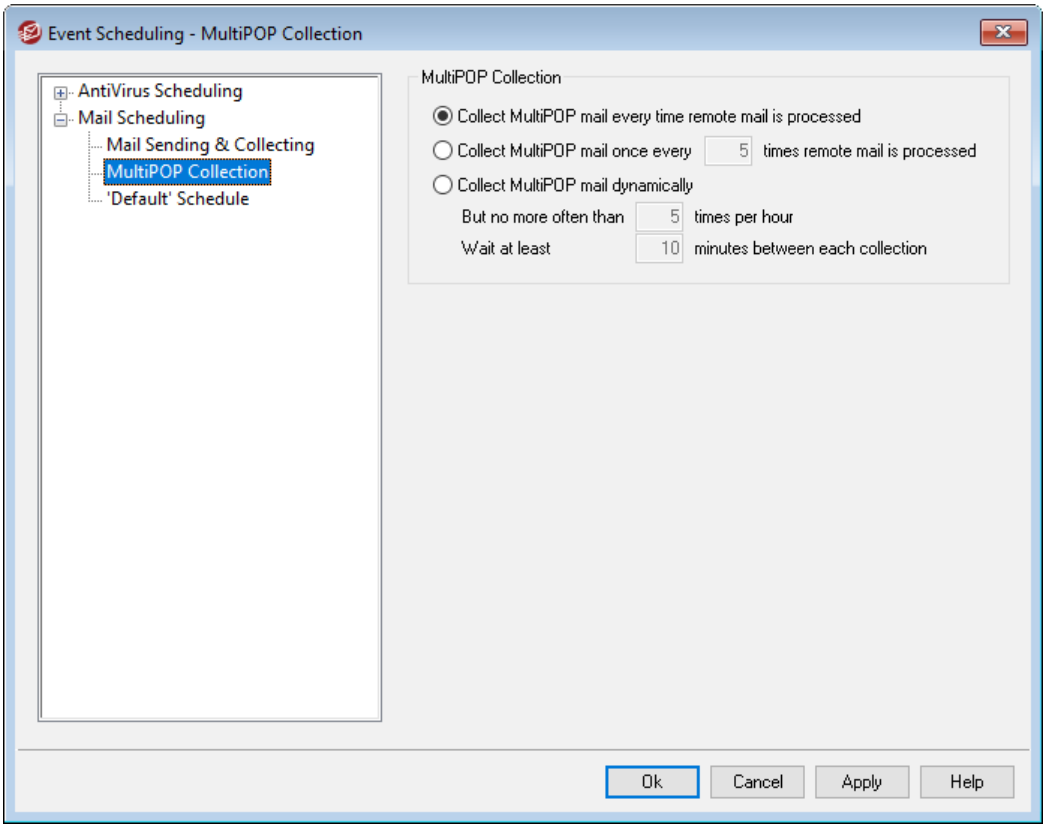
キューへこのスケジュールを付ける
選択されたスケジュールと特定のカスタムリモートメールキューと関連付けするために、このオプションを使用します。特定のメッセージをキューに送るルールを作成するために、コンテンツフィルタを使用することができます。例えば、特定の時間で配信するリモートアドレスについて予定したメーリングリストメッセージを必要とする場合、そのメッセージに対してカスタムキューを作成、その全部をカスタムキュー入れるルールの作成、カスタマイズしたスケジュールとキューの指定をすることができます。

キュー
カスタムキュー 798 を開くためにはこのボタンをクリックしてください。ここでは予定スケジューラで使用するカスタムリモートキューを作成することができます。

参照:

メールスケジュール 351
AntiVirus更新 343

3.7.2.2 MultiPOP収集



MultiPOP収集

リモートメールが処理される度にMultiPOPメールを収集する
リモートメールが処理されるたびに、MDaemonで、すべてのMultiPOP[673]メールを収集する場合は、このオプションを選択してください。

リモートメールが処理されるXX回に一回MultiPOPメールを収集する
リモートメールが処理される頻度よりも少ない頻度でMultiPOPメールを収集する場合は、このオプションを選択して、ボックスに回数を入力してください。この回数は、MultiPOPメールが1回収集されるのに、何回リモートメールの処理を行うかを指定するためのものです。

MultiPOPを動的に収集する
MultiPOPメッセージを動的に収集する場合は、このチェックボックスを選択してください。通常MultiPOPメールは、各リモートメールの処理ごとに、あるいは何回か間隔をおいて収集されます。動的に収集すると、すべてのユーザのメールを一度に収集するのではなく、ユーザがPOP、IMAP、またはWebmailを通して自分のローカルのメールをチェックする時に、個別にMultiPOPメッセージを収集できます。しかし、MultiPOPメールの収集は、ユーザのメールチェックによって始動するので、MultiPOPで受信した新着メールは、そのユーザが再び自分のメールをチェックするまでは表示されません。したがって、ユーザが新しいMultiPOPメールを見るためには、メールを2回チェックする必要があります。一度目はMultiPOPメールを始動し、二度目でその収集されたメールを参照するということです。

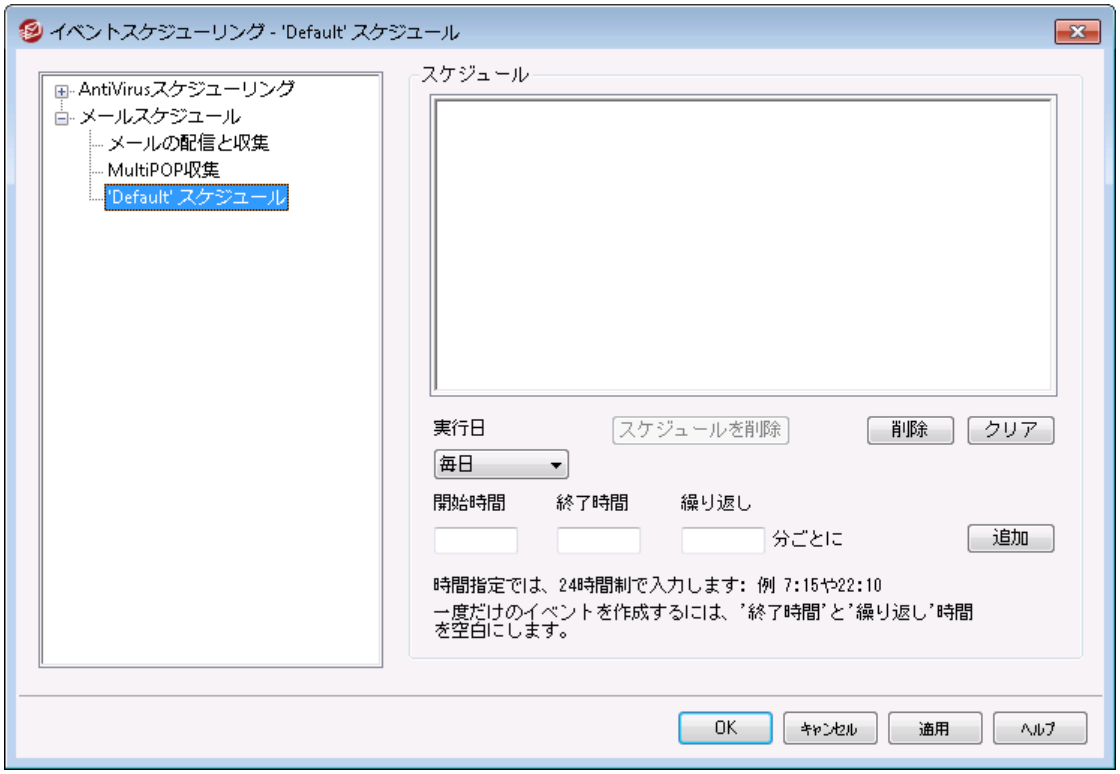
1時間にXX回まで
MDaemonでの過度なMultiPOPの使用によるパフォーマンスの低下を避けるために、各ユーザが1時間ごとにMultiPOPでメールを収集できる回数の最大値を指定することができます。

前回の収集後XX分間後に収集する
このオプションは、各ユーザーがMultiPOPメールを収集する頻度を制限する事で、メールサーバーに対する負荷を軽減するためのオプションです。この設定は、ユーザーが一度に何度もMultiPOP収集を行おうとした際、それを制限できます。ユーザーがMultiPOPメール収集後、次の収集までに待たなくてはならない時間を分で指定します。

参照:

MultiPOP 130
アカウントエディタ | MultiPOP 673

3.7.2.3 メールスケジュール



各メールスケジュールは、メールの配信と収集 347画面のドロップダウンリストで表示される名前が、同じ名前のスケジュールに対応しています。メールスケジュールは特定の時間にリモートメール処理を行う場

合に使用します。メールスケジュールは、次の場所からアクセスします: 設定 ≫ イベントスケジュール ≫ メールスケジュール ≫ 'スケジュール名' スケジュール

スケジュール

スケジュールを削除
このボタンは、カスタマイズしたメールスケジュールを削除します。スケジュールは削除され、その登録は[メールの配信と収集](#) 347画面のドロップダウンリストから削除されます。このボタンをクリックすると、スケジュールの削除を確認するダイアログが現れます。このオプションはカスタマイズしたスケジュールに利用できるだけで、デフォルトスケジュールは削除されることができません。

削除

エントリを削除する場合は、リストからエントリを選択して、このボタンをクリックします。

クリア
このボタンはスケジュールからすべてのエントリを削除します。

スケジュールの作成

期間
スケジュールに対して新しい予定を作成する時に、最初に、日またはこのスケジューリング予定が発生する期日選択します。以下を選択することができます: 毎日、週日(月曜日から金曜日)、週末(土曜日および日曜日)または特定の曜日。

開始
予定を開始する時間を入力します。00:00から23:59までの24時間制の形式である必要があります。これが繰り返されている予定でなく1つの予定の場合は、これは、入力は1つの時間値です(終了 と繰り返し [xx] 分ごとをブランクにします)

終了
終了予定時間を入力します。00:00から23:59まで時間値が24時間制の形式である必要があります。また**開始**時間以降でなければなりません。例えば、開始が10:00である場合、この値は10:01から23:59までにできます。繰り返しの予定ではなく単独の場合は、このオプションをブランクにします。

繰り返し [xx] 分ごと
これは、メールが指定された**開始**と**終了**時間の間で処理される時間間隔です。繰り返されている予定ではなく単独にする場合、このオプションを空白のままにします。

追加
期間および**開始**時間を指定し任意の**終了**.時間および**繰り返し**をスケジュールに予定を追加するには、このボタンをクリックします。

要件により、メールの処理間隔は[メールの配信と収集](#) 347でシンプルに行う事をお勧めします。例えば、1分間隔でメール収集を行うようメールスケジュールオプションで指定するのと、この画面で毎日分刻みでスケジュールを作成するのは、結果として同じ動作になり、スケジュールを作成する意味がありません。一方で、処理間隔が1時間以上経過する、または特定

の期日だけである場合、スケジュールオプションと処理間隔オプションを組み合わせて使用する事ができます。

参照:

メールの配信と収集 347
AntiVirusアップデート 343
AntiSpamアップデート 634

3.8 MDaemon Connector

MDaemon Private CloudのMDaemon Connector（MC）機能でMicrosoft Outlookを標準のメールクライアントとして使用しているユーザーはMDaemon Connector for MDaemonを利用できます。MDaemon Connectorを使うと、Outlookのメールや空き状況付きカレンダー、アドレス帳、配布先リスト、仕事、メモをOutlookとMDaemon間で通信する事で、グループウェアや共有機能として使用する事ができます。

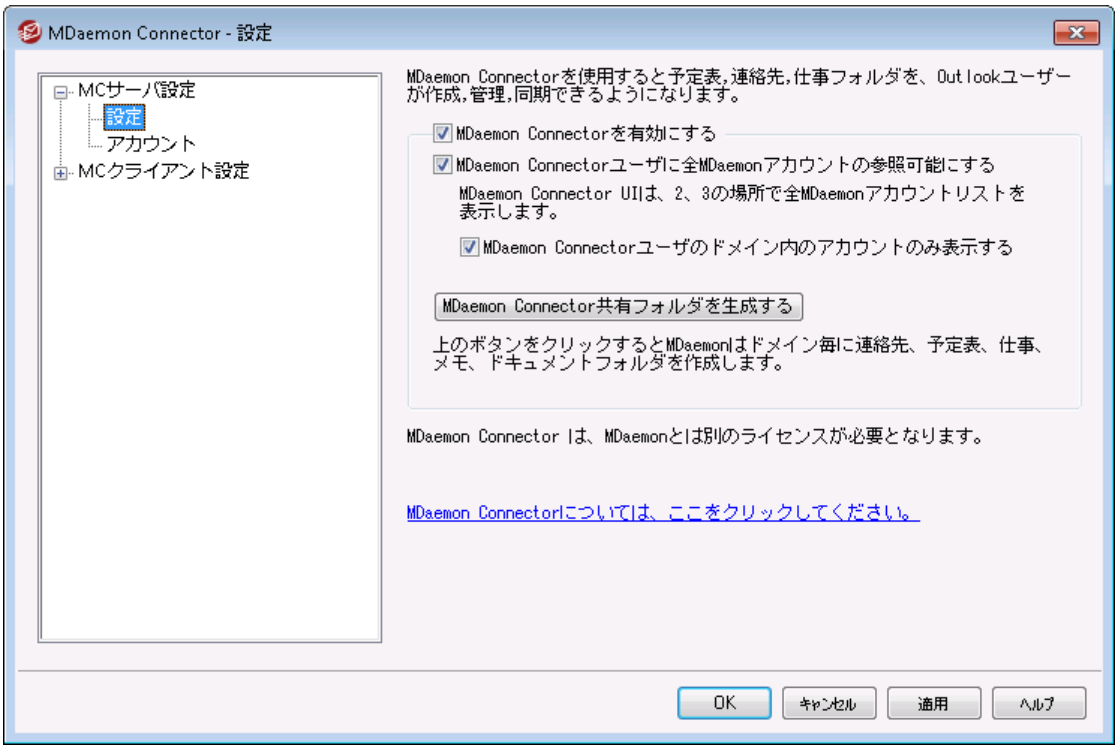
MDaemon Connectorダイアログは、設定 » MDaemon Connectorから起動でき、ここではMCの有効化や設定、MDaemon Connectorを使用するアカウントの認証を行うことができます。

参照:

MCサーバー設定 » 設定
MC 354 サーバー設定 » アカウント 355
MC 354 クライアント設定 356

3.8.1 MCサーバー設定

3.8.1.1 設定



MDaemon Connector

MDaemon Connectorを有効にする
MDaemon Connector(MC)を有効にするには、このチェックボックスをクリックします。このオプションが有効になっていない限り、ユーザはMCの機能を利用できません。

MDaemon Connectorユーザへ全てのMDaemonアカウントの参照を許可
ユーザーのクライアント上のMDaemon Connectorへ表示される「許可」一覧にMCを使った接続が行える全てのMDaemonアカウントを表示する場合はこのオプションを有効にしてください。Outlookの項目を共有する場合、MCユーザは、このリストから許可するアカウントを選択することになります。この機能が無効な場合、MDaemon Connectorの[許可]リストは空欄になり、ユーザは直接メールアドレスを手入力しなければなりません。この場合、MCによる接続を許可されたアカウントのみがOutlookの項目の共有が可能です。有効なMDaemon Connectorアカウントではないメールアドレスを入力した場合、そのメールアドレスではMCによって承認されるまでアイテムを共有することができません。

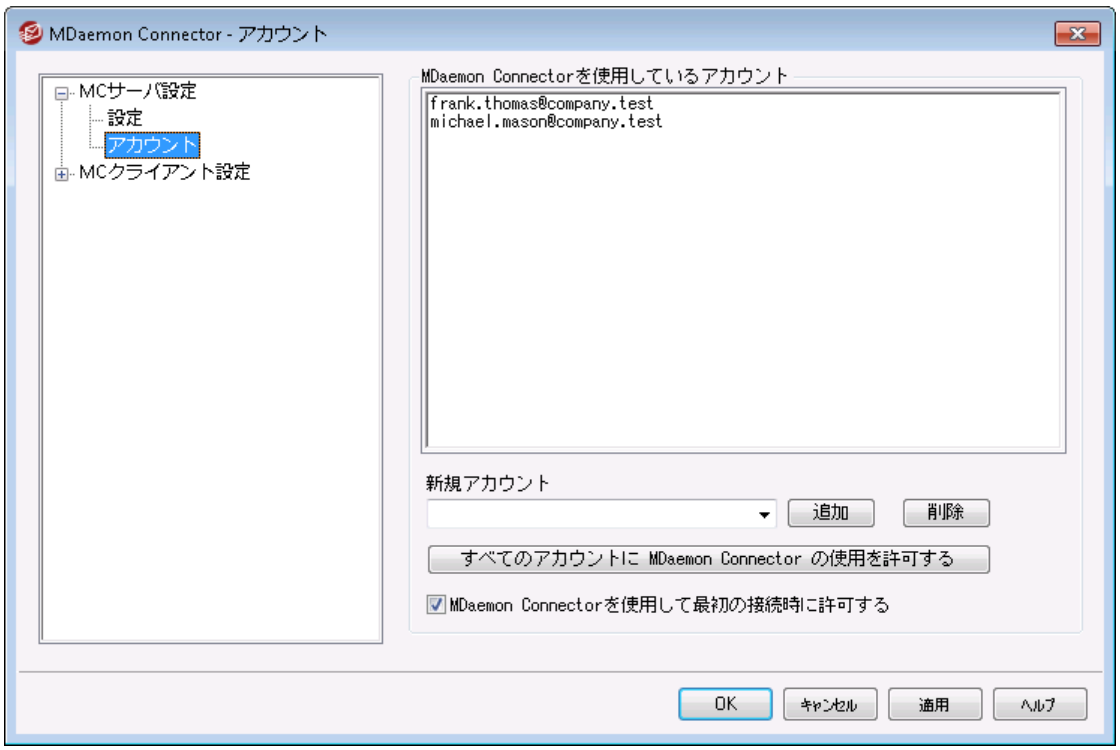
...MDaemon Connectorユーザドメイン内のアカウントのみ表示する
この機能は上記のMDaemon ConnectorユーザにMDaemonアカウントすべて参照可能にするオプションが有効な場合のみ機能します。MDaemon Connectorによる接続を許可されたユーザでMCの[許可]リスト上に表示されるユーザと同じドメインに属するアカウントのみに情報の共有を制限する場合は、このチェックボックスを選択してください。その他のドメインに属するアカウントは、有効なMDaemon Connectorアカウントがあっても一覧に表示されません。

MDaemon Connector共有フォルダを生成する
各ドメインにMCフォルダのセットを作成するにはこのボタンをクリックしてください。この作業により連絡先、予定、ジャーナル、仕事、メモというフォルダが作成されます。

参照:

MCサーバー設定 ≫ アカウント 355
MCクライアント設定 356

3.8.1.2 アカウント



MDaemon Connectorアカウント

これは、MDaemon Connector経由でOutlookフォルダ、カレンダー、連絡先、メモなどを共有できるMDaemonアカウントの一覧です。下記のオプションを使用して、リストにアカウントを追加できます。

新規アカウント
MDaemonユーザをMDaemon Connectorユーザとして追加するには、このドロップダウンリストから目的のユーザを選び**追加**ボタンを押してください。ユーザを削除する場合は、リストから目的のユーザを選択して[削除]ボタンをクリックしてください。

すべてのアカウントにMDaemon Connectorの使用を許可する
すべてのMDaemonユーザをMDaemon Connectorによる接続の認証ユーザとして即座に承認する場合は、このボタンをクリックしてください。このボタンをクリックすると、ユーザリストへMDaemonアカウントが追加されます。

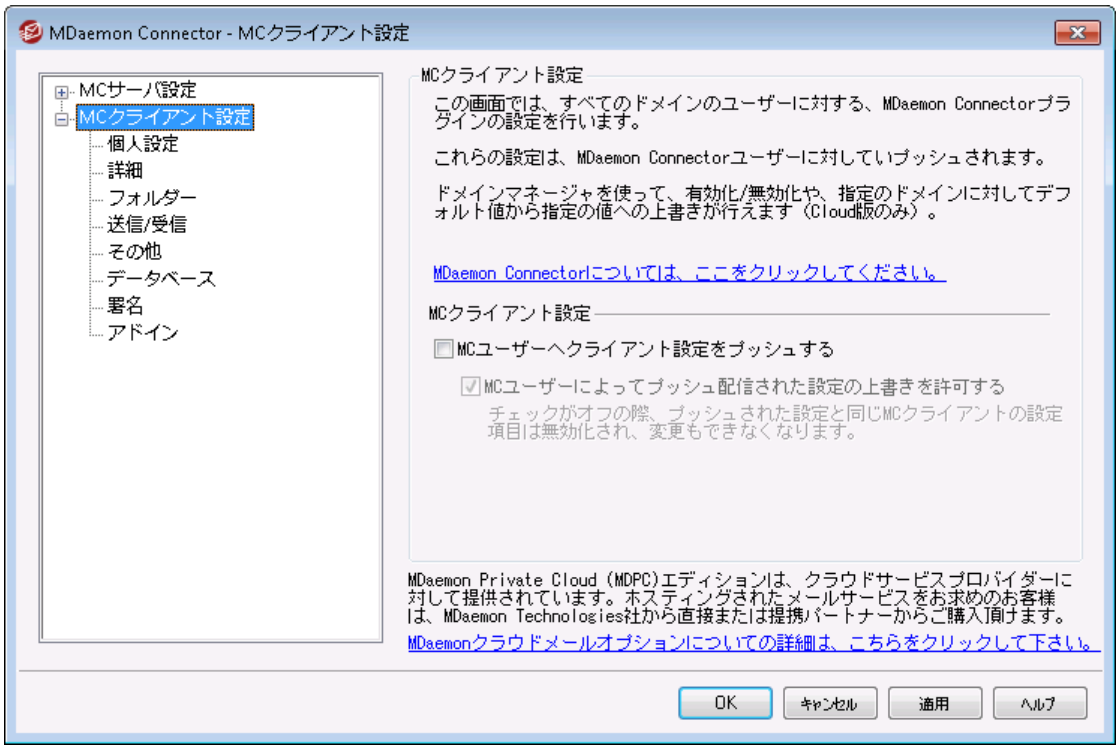
MDaemon Connectorへの最初の接続時に利用を許可する
ユーザが最初にMDaemon Connectorに接続した際、MDaemon Connectorアカウントの一覧に対象ユーザーを追加するには、このチェックボックスをオンにしてください。注意：このオプションを有効にした場合、実質的にすべてのMDaemonアカウントにMDaemon Connentorの使用を承認することになります。最初に使用するまではリストにアカウントは追加されません。

MDaemon Connectorを使用して最初の接続時に許可する
MDaemon Connectorを使用して初めて接続するときに、個々のアカウントをMDaemon Connectorアカウントリストに追加する場合は、このチェックボックスをクリックします。注意：このオプションを有効にすると、MDaemon Connectorを使用するすべてのMDaemonアカウントが有効になります。アカウントは、初めて使用するまでリストに追加されません。

参照:

MCサーバー設定 ≫ 設定 354
MCクライアント設定 356

3.8.2 MCクライアント設定



MCクライアント設定ダイアログでは、MDaemon Connector（MC）ユーザーのクライアント設定を一元管理できます。各設定画面にて必要なクライアント設定を行うと、MDaemonは、MDaemon Connectorユーザーがサーバーへ接続する度に、必要に応じて設定値をプッシュ配信します。MCクライアント設定は最後にクライアントが接続した際に受信した設定値から変更があった場合にのみ送信されます。後述の「MCユーザーの配信された設定値の上書きを許可する」オプションが有効の場合、ユーザーはクライアントへ個別に配信された設定値を上書きする事ができます。オプションが無効の場合、全てのクライアント画面はロックされ、MDaemon Connectorユーザーが変更を行う事はできなくなります。

ユーザー毎、ドメイン毎に異なる値が必要な項目を設定するのに、MCクライアント設定へは$USERNAME$, $EMAIL$, $DOMAIN$といったマクロを使用できます。これらのマクロは設定をクライアントへプッシュ配信した際、ユーザー又はドメイン固有のデータへ変換されます。このフィールドへは「Frank Thomas」といった、ハードコードされた値を使わないよう注意して下さい。この操作で、全てのMDaemon Connectorユーザーの名前が、「Frank Thomas」に設定されてしまいます。全般 358 画面にはマクロ参照ボタンがあり、対応マクロが一覧表示されます。

MDaemon Private Cloud（MDPC）の場合は、ドメインマネージャー 165 へMCクライアント設定ダイアログがあり、ドメイン毎にMDaemon Connectorクライアント設定が行えます。

この機能はデフォルトで無効になっており、MDaemon Connector v4.0.0以上のバージョンを使っている場合にのみ使用できます。

MCクライアント設定

MCユーザーへクライアント設定をプッシュする
MDaemon Connectorユーザーが接続する度に事前設定したMCクライアント設定をプッシュ配信する場合は、このオプションを有効にして下さい。MCクライアント設定は、クライアントが最後に接続してから設定内容に変更があった場合のみ送信されます。このオプションはデフォルトで無効になっています。

MCユーザーによるプッシュ配信された設定の上書きを許可する
そのオプションを有効にすると、ユーザーはプッシュ配信された設定を個々に上書きできるようになります。無効の場合、すべてのクライアントの画面はロックされ、MCユーザーは変更を加えることができなくなります。

プッシュ配信された設定をユーザーが上書きできるようにする事は、サーバーがクライアントへプッシュ配信する事を禁止する事にはなりません。例えば、ユーザーがMDaemon Connectorの設定の一つを変更し、管理者がMCクライアント設定で変更を加えた場合、次にユーザーのクライアントがサーバーへ接続した際、全てのMCクライアント設定はユーザーのクライアント設定を上書きします。つまり、ユーザーが事前に上書きした設定はサーバー側で行った設定と同じものに変更されます。

MC設定の自動検出

最初にMDaemon Connectorプラグインをクライアントにて設定する時、ユーザーは個人設定画面でユーザー名とパスワードを入力後「*テストとアカウント設定の取得*」ボタンをクリックできます。これによって、MDaemon Connectorは資格情報を検証し、対象アカウントのサーバー情報を自動取得します。

サーバーに接続するには、クライアントは最初に一般的なFQDN値を試します。IMAPの場合、専用SSLポート、次にTLSの非SSLポートを使って、mail.<domain>（例. mail.example.com)を試みます。これでサーバーへ接続できなかった場合、同じ処理をimap.<domain>、次に<domai>、最後に、imap.mail.<domain>を試みます。全てで失敗した場合、暗号化されていないサインインを同様に実行します。

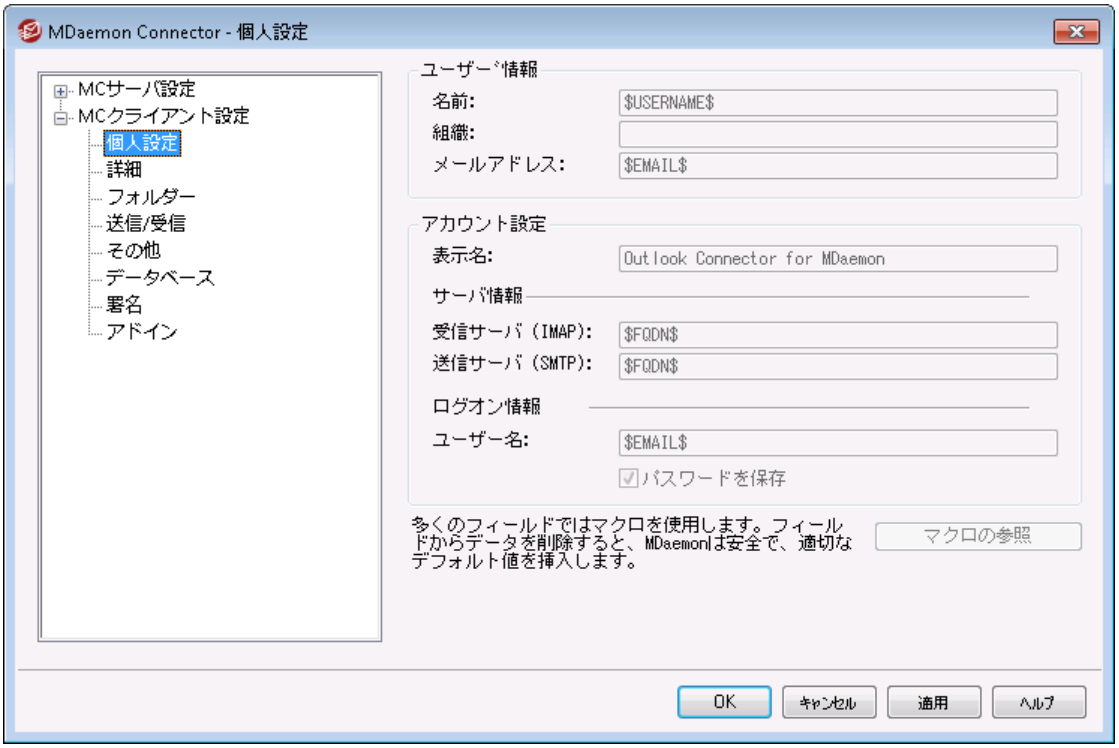
SMTPの場合は、587、25、465番ポートを使って、まずはSSL、次にTSLを使用し、mail.<domain>を試行します。これはsmtp.<domain>, <domain>, smtp.mail.<domain>で繰り返されます。全てが失敗した場合、非暗号化サインインが同様に試行されます。

MDaemon Connectorの認証が正しく行われると、SSL/TLS情報と共に、受信サーバーと送信サーバーの情報が自動設定されます。

参照:

MCサーバー設定 ≫ 設定 354
MCサーバー設定 ≫ アカウント 355
MCクライアント設定 ≫ 全体設定 358

3.8.2.1 個人設定



MC クライアント設定 356 画面で「MCユーザーへクライアント設定をプッシュ配信する」オプションを有効化していた場合、MDaemon Connectorが次回サーバーへ接続した際、この画面の設定が対象のMDaemon Connectorクライアント画面の設定を上書きします。MCクライアント設定は最後にクライアントが接続した際に受信した設定値から変更があった場合にのみ更新されます。この画面のほとんどの項目は、固定値ではなくマクロを含んでいます。後述の マクロの参照 359 をご覧ください。

ユーザー情報

名前
デフォルトでこのオプションには$USERNAME$マクロを使用し、ユーザーの姓と名に置き換えられます。この値はユーザーのメールのFrom: ヘッダへ表示されます。

組織
ここへは追加で企業名や組織名を入力します。

メールアドレス
デフォルトでこのオプションには$EMAIL$マクロを使用し、ユーザーのメールアドレスに置き換えられます。この値はユーザーのメールのFrom: ヘッダへ表示されます。

アカウント設定

表示名
ここでの名前はOutlookで表示され、どのアカウントが使われているのかを把握する事ができます。この機能は、プロファイルで複数アカウントを所有しているユーザーにとって便利です。ユーザーのみがこの情報を確認できます。デフォルトではMDaemon Connector」と設定されています。

サーバー情報

受信サーバ (IMAP)
MDaemon Connectorクライアントがメールの取得や管理を行うサーバーを指定します。デフォルトでは$FQDN$が設定されています。

送信サーバ (SMTP)
MDaemon Connectorクライアントがメール送信を行うサーバーを指定します。通常は上記の受信メール (IMAP) サーバーと同じです。デフォルトでは$FQDN$が設定されています。

ログオン情報

ユーザー名
ユーザーのMDaemon Connectorメールアカウントへ接続する際のユーザー名です。一般的には上記のメールアドレスと同じです。デフォルトでは$EMAIL$が指定されています。

パスワードを保存
デフォルトでMDaemon Connectorクライアントはパスワードを保存しており、Outlookが起動するとパスワードを確認する事なく自動的にメールアカウントへサインインします。Outlook起動時にユーザーにパスワード入力を行わせるにはこのオプションを無効化します。

マクロの参照

ユーザー毎、ドメイン毎に異なる値が必要な項目用に、MCクライアント設定では$USERNAME$, $EMAIL$, $DOMAIN$といったマクロを使用できます。クライアントへ設定をプッシュ配信する際、マクロが

特定のユーザーやドメインに書き換えられます。例えばYOURNAMEフィールドへ「Frank Thomas」といった固定値を指定しないよう注意してください。これを行ってしまうと、MDaemonへ接続する全MCユーザー名が「Frank Thomas」になってしまいます。 マクロ参照ボタンを押すと対応マクロが一覧表示されます。

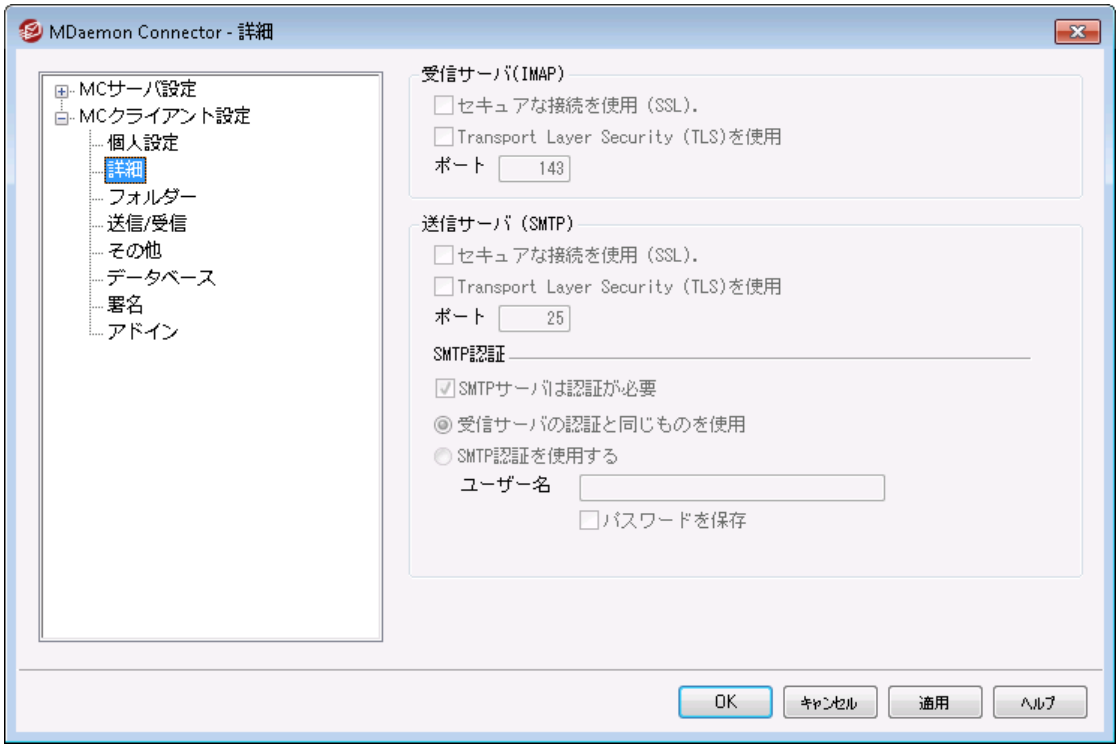
$USERNAME$	このマクロはユーザーの アカウント詳細 650 画面の「名前」を挿入します。次のマクロと同じ意味です: "$USERFIRSTNAME$ $USERLASTNAME$"
$EMAIL$	ユーザーのメールアドレスを挿入します。次のマクロと同じ意味です: $MAILBOX$@ $DOMAIN$.
$MAILBOX$	このマクロはアカウントの メールボックス名 650 を挿入します。
$USERFIRSTNAME$	このマクロはアカウント所有者の名に置き換えられます。
$USERFIRSTNAMELC$	このマクロはアカウント所有者の名に小文字で置き換えられます。
$USERLASTNAME$	このマクロはアカウント所有者の姓に置き換えられます。
$USERLASTNAMELC$	このマクロはアカウント所有者の姓に小文字で置き換えられます。
$USERFIRSTINITIAL$	このマクロはアカウント所有者の名のイニシャルに置き換えられます。
$USERFIRSTINITIALLC$	このマクロはアカウント所有者の名のイニシャルに小文字で置き換えられます。
$USERLASTINITIAL$	このマクロはアカウント所有者の姓のイニシャルに置き換えられます。
$USERLASTINITIALLC$	このマクロはアカウント所有者の名のイニシャルに小文字で置き換えられます。
$MAILBOXFIRSTCHARSn$	「n」の部分には1から10までの数字が入ります。これはメールボックス名の最初の「n」文字と書き換えられます。
$DOMAIN$	アカウントの メールボックスドメイン 650 を挿入します。
$DOMAINIP$	このマクロはアカウントが属しているドメインに関連付けられた IPv4アドレス 167 へ置き換えられます。

$DOMAINIP6$	このマクロはアカウントが属しているドメインに関連付けられたIPv6アドレス[167]へ置き換えられます。
$FQDN$	アカウントが属しているドメインのFQDNやSMTPホスト名[167]を挿入します。
$PRIMARYDOMAIN$	このマクロはMDaemonのデフォルトドメイン[165]名へ置き換えられます。
$PRIMARYIP$	このマクロはMDaemonのデフォルトドメイン[165]に関連付けられたIPv4アドレス[167]へ置き換えられます。
$PRIMARYIP6$	このマクロはMDaemonのデフォルトドメイン[165]に関連付けられたIPv6アドレス[167]へ置き換えられます。

参照:

MC クライアント設定[356]
MCサーバー設定 ≫ 設定[354]
MCサーバー設定 ≫ アカウント[355]

3.8.2.2 詳細



MC クライアント設定 356 画面で「MCユーザーへクライアント設定をプッシュ配信する」オプションを有効化していた場合、MDaemon Connectorが次回サーバーへ接続した際、この画面の設定が対象のMDaemon Connectorクライアント画面の設定を上書きします。MCクライアント設定は最後にクライアントが接続した際に受信した設定値から変更があった場合にのみ送信されます。この画面のほとんどの項目は固定値ではなくマクロを含んでいます。

受信サーバ(IMAP)

セキュアな接続を使用 (SSL)
クライアントが受信メール(IMAP)サーバーへの接続にセキュアなSSL接続を使用できるようにするにはこのボックスをチェックして下さい。このオプションを有効化すると自動的にポート設定がデフォルトSSLポートである「993」となります。

Transport Layer Security (TLS)を使用
受信メール(IMAP)サーバーへの接続にセキュアなTLS接続を使用できるようにするにはこのボックスをチェックして下さい。

ポート
MDaemon Connectorクライアントが受信メール(IMAP)サーバーへの接続に使用するポートです。デフォルトではIMAP用に143、SSL暗号化されたIMAP接続用に993が設定されています。

送信サーバ（SMTP）

セキュアな接続を使用（SSL）
MCクライアントが送信メール（SMTP）サーバーへの接続にセキュアなSSL接続を使用できるようにするにはこのボックスをチェックして下さい。このオプションを有効化すると自動的にポート設定がデフォルトSSLポートである「465」となります。

Transport Layer Security（TLS）を使用
MCクライアントが送信メール（SMTP）サーバーへの接続にセキュアなTLS接続を使用できるようにするにはこのボックスをチェックして下さい。

ポート
MDaemon Connectorクライアントが送信メール（SMTP）サーバーへの接続に使用するポートです。デフォルトではSMTP用に25、SSL暗号化されたSMTP接続用に465が設定されています。

SMTP認証

SMTPサーバは認証が必要
デフォルトで、メール送信時、ユーザーは正しいログイン情報を使い送信サーバー（SMTP）で認証を通過する必要があります。

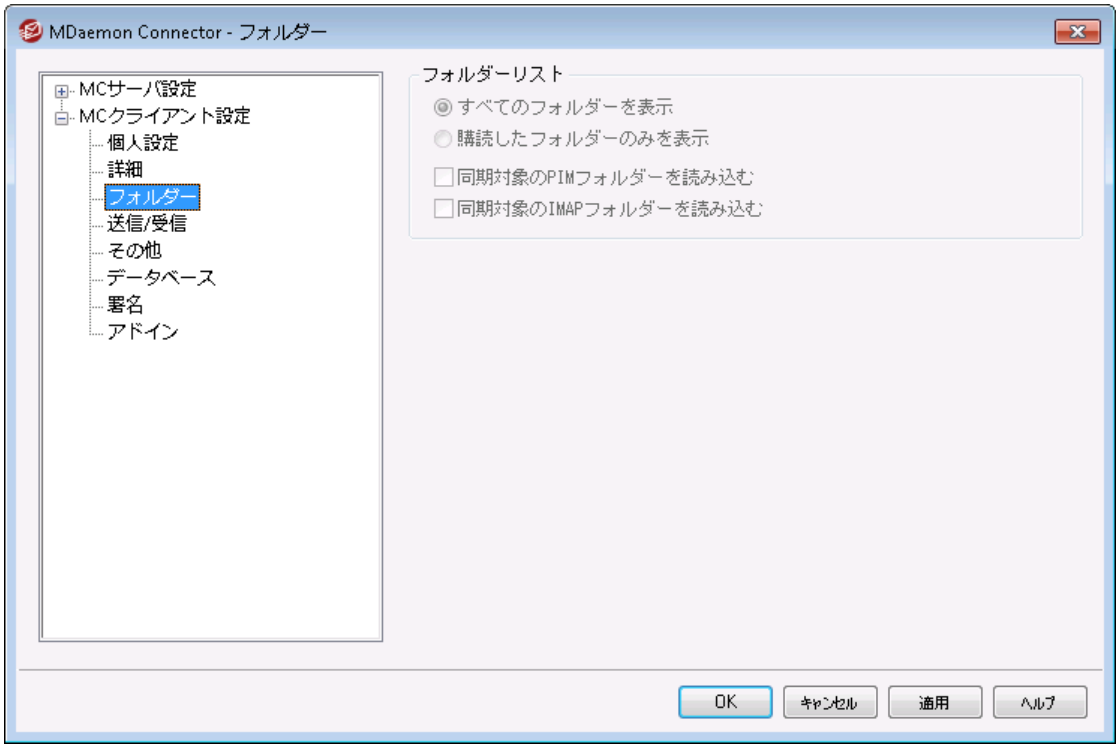
受信サーバの認証と同じものを使用
デフォルトで、MDaemon Connectorクライアントは送信（SMTP）認証に受信（IMAP）サーバーで使用する認証情報と同じ情報を使用します。

SMTP認証を使用する
異なるメールサーバーで送信を行う場合など、MDaemon Connectorユーザーがメール送信時に異なる認証情報を使用する場合はこのオプションを選択します。

参照:

MCクライアント設定 356
MCサーバー設定 ≫ 設定 354
MCサーバー設定 ≫ アカウント 355

3.8.2.3 フォルダ



MCクライアント設定 356 画面で「MCユーザーへクライアント設定をプッシュ配信する」オプションを有効化していた場合、MDaemon Connectorが次回サーバーへ接続した際、この画面の設定が対象のMDaemon Connectorクライアント画面の設定を上書きします。MCクライアント設定は最後にクライアントが接続した際に受信した設定値から変更があった場合にのみ送信されます。この画面のほとんどの項目は固定値ではなくマクロを含んでいます。

フォルダーリスト

全てのフォルダーを表示
デフォルトでOutlookのフォルダー一覧画面ではMDaemon Connectorユーザーがアクセスできるメールサーバー上の全フォルダを表示します。

購読したフォルダーのみを表示
Outlookのフォルダー一覧画面で、ユーザーが購読しているフォルダのみを表示するにはこのオプションを選択します。

同期対象のPIMフォルダを読み込む
多くの場合このオプションは変更せず、MDaemon ConnectorユーザーはMDaemon Connectorが(メール以外の連絡先、予定表、仕事などの)PIMフォルダをロードしている間も、継続してOutlookを使用できます。このオプションを有効化すると、Outlookはデータがロードされるまで Outlookの利用をブロックします。一般的に、この設定はユーザーがPIMフォルダへアクセスするサードパーティー製品を使用している場合などにのみ必要です。

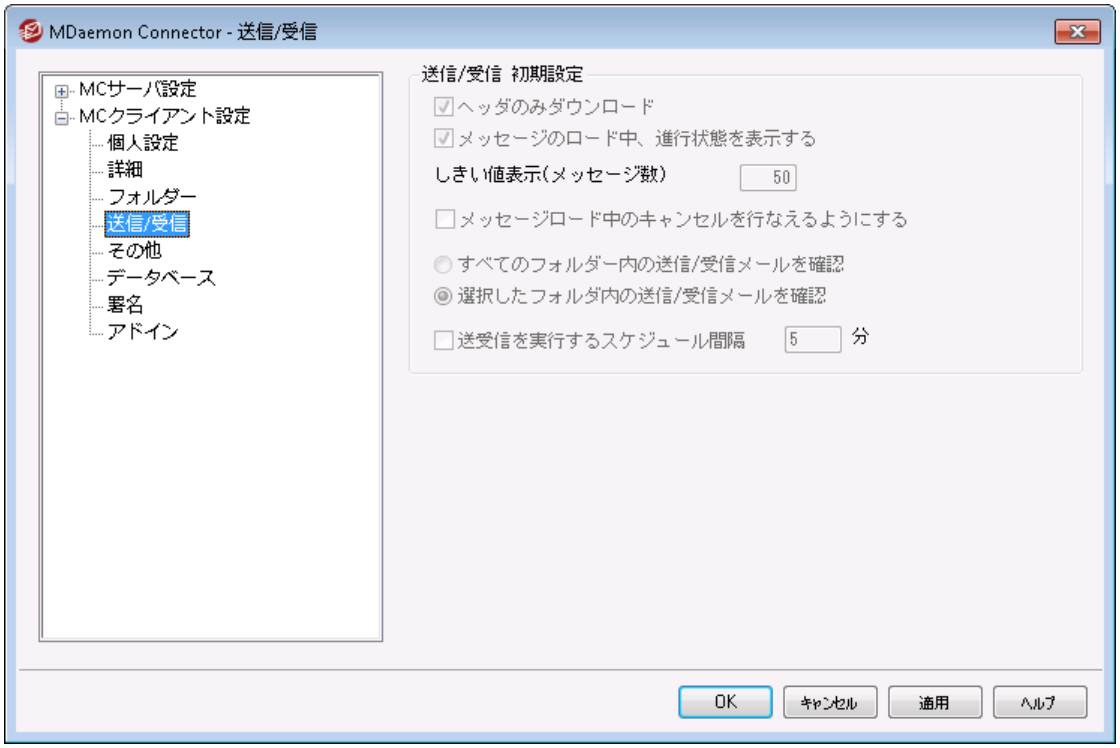
同期対象のIMAPフォルダを読み込む
多くの場合このオプションは変更せず、MDaemon ConnectorユーザーはMDaemon Connectorが IMAPメールフォルダをロードしている間も、継続してOutlookを使用できます。このオプションを有効

化すると、Outlookはデータがロードされるまで Outlookの利用をブロックします。一般的に、この設定はユーザーがメールフォルダへアクセスするサードパーティー製品を使用している場合などにのみ必要です。

参照:

MCクライアント設定 356
MCサーバー設定 ≫ 設定 354
MCサーバー設定 ≫ アカウント 355

3.8.2.4 送信/受信



MCクライアント設定 356 画面にある、「*クライアント設定をMCユーザーへプッシュ配信する*」オプションを有効化していると、MDaemon Connectorユーザーがサーバーへ接続する際、画面上の設定がMDaemon Connectorクライアントの関連する画面へプッシュ配信されます。MCクライアント設定は最後にクライアントが接続しデータを受け取ってから変更があった場合にのみ送信されます。

送信/受信初期設定

ヘッダのみダウンロード
デフォルトでMDaemon Connectorが送信/受信を行い新着メールを見つけると、(To、From、Subjectなどの)メッセージヘッダのみをダウンロードし、メールを一覧表示します。メール全体は表示するまでダウンロードしません。

メッセージのロード中、進行状況を表示する
MDaemon Connectorは大量のメールをダウンロードする際、進捗状況を表示します。進捗状況の表示を行わない場合はこのチェックボックスを無効にして下さい。

しきい値表示（メッセージ数）
進行状況を表示する‥オプションを有効化していると、ここで指定した数以上のメールをダウンロードしている場合に進捗状況を表示します。

メッセージロード中のキャンセルを行えるようにする
MDaemon Connectorユーザーが大きなサイズのメールのダウンロードを行っている途中でキャンセルできるようにするにはこのボックスをチェックします。

全てのフォルダ内の送信/受信メールを確認
MDaemon Connectorで送信/受信を行った際、ユーザーアカウントの全てのメールフォルダで新着メールを確認するにはこのオプションをクリックします。

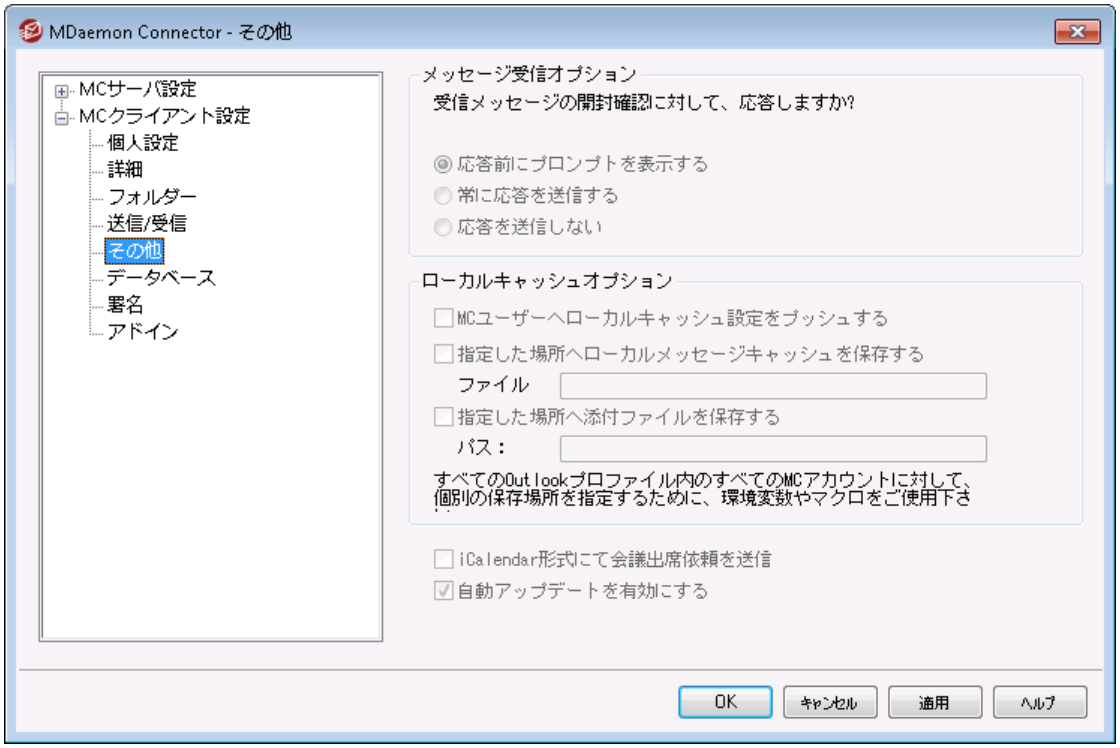
選択したフォルダ内の送信/受信メールを確認
MDaemon Connectorで送信/受信を行った際、ユーザーが指定したフォルダの新着メールを確認するにはこのオプションをクリックします。

送受信を実行するスケジュール間隔 [xx] 分
特定の間隔で送受信を行うにはこのオプションを使用します。

参照:

MC クライアント設定 356
MCサーバー設定 ≫ 設定 354
MCサーバー設定 ≫ アカウント 355

3.8.2.5 その他



MCクライアント設定 356 画面で「MCユーザーへクライアント設定をプッシュ配信する」オプションを有効化していた場合、MDaemon Connectorが次回サーバーへ接続した際、この画面の設定が対象のMDaemon Connectorクライアント画面の設定を上書きします。MCクライアント設定は最後にクライアントが接続した際に受信した設定値から変更があった場合にのみ送信されます。この画面のほとんどの項目は固定値ではなくマクロを含んでいます。

メッセージ受信オプション

受信メールの中には開封確認を求める特殊なヘッダが付与されているものがあります。ここではMDaemon Connectorが開封確認に対してどのように対処するのかを指定する事ができます。

応答前にプロンプトを表示する
開封確認を要求しているメールを開いた際、開封確認を送信するかどうかを都度選択する場合は、このオプションを選択して下さい。

常に応答を送信する
開封確認を要求しているメールを開いた際、常に開封確認通知を送信する場合は、このオプションを選択して下さい。

応答を送信しない
MDaemon Connectorから開封確認通知を送信しない場合はこのオプションを選択して下さい。

ローカルキャッシュオプション

このセクションにはMDaemon Connectorユーザーのローカルメッセージキャッシュの場所や添付ファイルの保存先を指定するオプションがあります。

これらのオプションにはユーザーのMDaemon Connectorプラグインのバージョン4.5.0又はそれ以降のものが必要です。

MCユーザーへローカルキャッシュ設定をプッシュ
デフォルトでMDaemonはここでの設定をMDaemon Connectorクライアントへプッシュ配信しません。プッシュ配信する場合はこの設定を有効にして下さい。MDaemon Connectorクライアントはローカルファイルを現在の場所からデフォルトの場所、又は下記の保存先を指定した場合には指定した場所へキャッシュを移動させます。

指定した場所へローカルメッセージキャッシュを保存する | ファイル名
MDaemon Connectorクライアントのローカルファイルを指定の場所へ移動するにはここでキャッシュのローカルパスとファイル名を指定します。ユーザー毎に固有の場所を指定する場合は、環境変数やマクロを使用する事ができます。例えば次の通りです:

```
%APPDATA%\Alt-N\Outlook Connector 2.0\Accounts\%OUTLOOKPROFILE%\%
  OUTLOOKEMAIL%\LocalCache.db
```

指定した場所へ添付ファイルを保存する | パス
MDaemon Connectorクライアントの添付ファイルを指定の場所へ保存するにはここでパスを指定します。ユーザー毎に固有の場所を指定する場合は、環境変数やマクロを使用する事ができます。

---

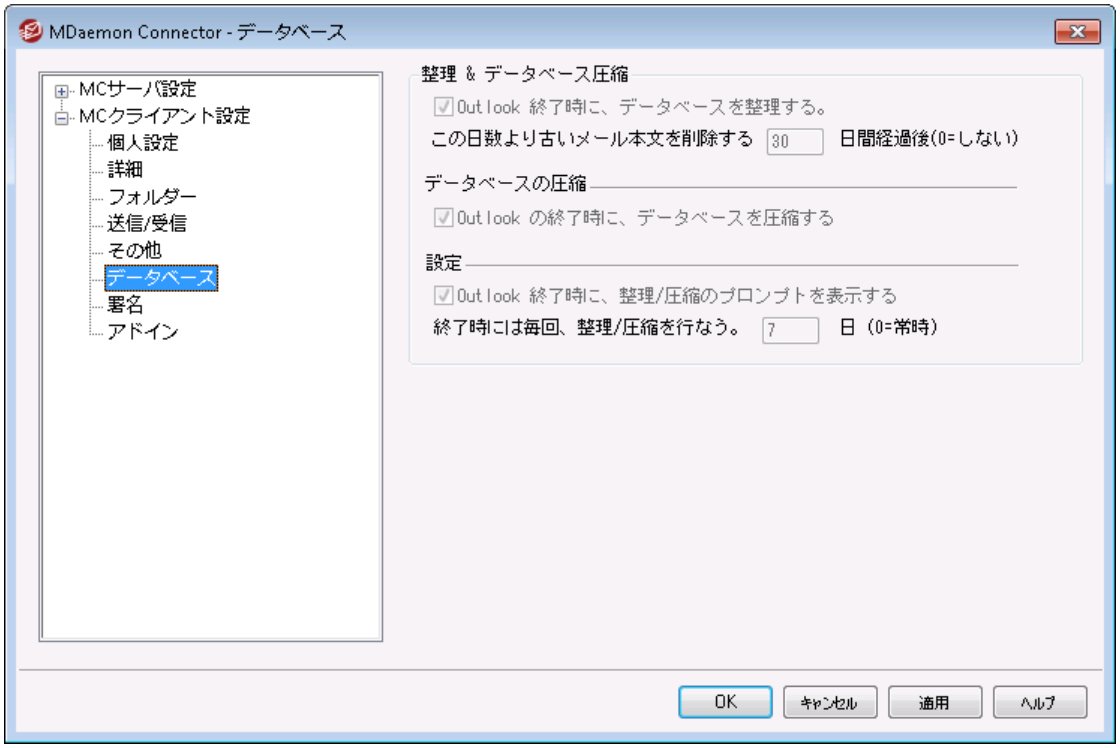
iCalendar形式にて会議出席依頼を送信
MDaemon ConnectorがiCalendar（iCal）形式で会議出席依頼を送信するようにするには、このチェックボックスを有効にして下さい。

自動アップデートを有効にする
MDaemon Connectorはデフォルトで新バージョンが利用可能になると自動アップデートされます。自動アップデートを行わないようにするには、このチェックボックスを無効化して下さい。

参照:

MC クライアント設定 356
MCサーバー設定 ≫ 設定 354
MCサーバー設定 ≫ アカウント 355

3.8.2.6 データベース



MC クライアント設定 356 画面で「MCユーザーへクライアント設定をプッシュ配信する」オプションを有効化していた場合、MDaemon Connectorが次回サーバーへ接続した際、この画面の設定が対象のMDaemon Connectorクライアント画面の設定を上書きします。MCクライアント設定は最後にクライアントが接続した際に受信した設定値から変更があった場合にのみ送信されます。この画面のほとんどの項目は固定値ではなくマクロを含んでいます。

整理 & データベース圧縮

Outlook終了時にデータベースを整理する
ディスク容量を節約しパフォーマンスを向上させるのに、デフォルトでMDaemon Connectorは Outlook終了時に古いメール本文の圧縮や整理を行います。これはメールヘッダを削除したり、サーバー上に保管されているメールへ影響を与えたりするものではなく、単純にローカルへキャッシュされた古いメール本文のみを削除します。既に整理された古いメールを後から開くと、メール本文はパソコンへ自動的に再ダウンロードされます。また、整理されるのはメールのみで、連絡先、予定表、仕事、ジャーナル、メモへ影響する事はありません。シャットダウン時のデータベース整理を無効化する場合は、このオプションのチェックを外して下さい。

この日数より古いメール本文を削除するXX日間経過後(0=しない)
Outlook終了時にメール本文を整理するのに、どの位古いメールを対象とするのかを指定します。デフォルトで、整理対象となるメールは30日よりも古いものです。日数はメールの更新日時を元にカウントされます。整理を行いたくない場合は、0を指定して下さい。

データベースの圧縮

Outlook終了時にデータベースを圧縮する
ディスク容量を節約しパフォーマンスを向上させるのに、デフォルトでMDaemon Connectorは Outlook終了時にローカルへキャッシュされたメールデータベースファイルの圧縮とデフラグを実行します。Outlookは圧縮処理を行う前提として、正常終了しなくてはなりませんが、Outlookがクラッシュしたり、タスクマネージャから「タスクの終了」を選んで終了した場合などには、圧縮処理が行われません。下記の設定セクションでは圧縮処理の頻度や、圧縮前に確認プロンプトを表示するかどうかが設定できます。

設定

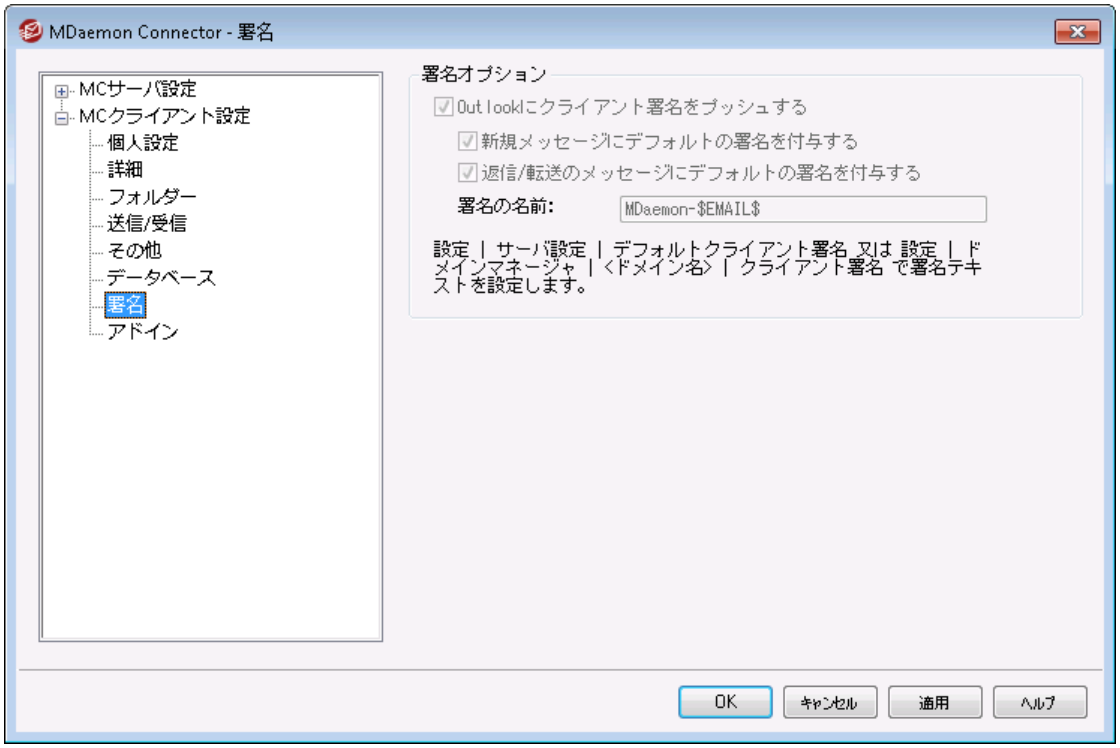
Outlook終了時に整理/圧縮のプロンプトを表示する
MDaemon Connectorが整理や圧縮の実行前に確認用プロンプトを表示するにはこのオプションを有効化します。ユーザーが「はい」を選択すると、整理や圧縮処理が行われ、進捗状況が表示されます。確認プロンプトの表示を行われない場合は、このオプションを無効化して下さい。この場合、MDaemon Connectorはシャットダウン時整理や圧縮を自動実行し、進捗状況のみを表示します。

終了時には毎回整理/圧縮を行うXX日間経過後(0=常時)
このオプションではどのくらいの頻度でMDaemon Connectorがデータベースの整理や圧縮を実行するのかをコントロールします。デフォルトで、このオプションは7日間と設定されており、整理や圧縮が7日間に1度行われます。ユーザーがOutlookを終了する度にデータベースの整理や圧縮を行うようにするには、この値を0へ変更して下さい。

参照:

MC クライアント設定 356
MCサーバー設定 ≫ 設定 354
MCサーバー設定 ≫ アカウント 355

3.8.2.7 署名



MCクライアント設定 356 の「MCユーザーへクライアント設定をプッシュ配信」オプションを有効にすると、ここで選択した設定が署名（Outlookのファイル ≫ オプション ≫ メール ≫ 署名）画面へMDaemon Connectorユーザーがサーバーへ接続した際プッシュ配信されます。この機能はMDaemon Connector 6.5.0以上が必要です。

署名オプション

Outlookへクライアント署名をプッシュ配信
デフォルトクライアント署名 125（作成している場合は、ドメイン用の クライアント署名 188 ）をMDaemon Connectorユーザーへプッシュ配信するにはこのオプションを使用します。署名の名称オプションで署名に使用する名称を指定できます。

新しいメッセージ用のデフォルト署名を作成
新しいメッセージでデフォルト署名として使用するクライアント署名を作成する場合はこのオプションを有効化します。

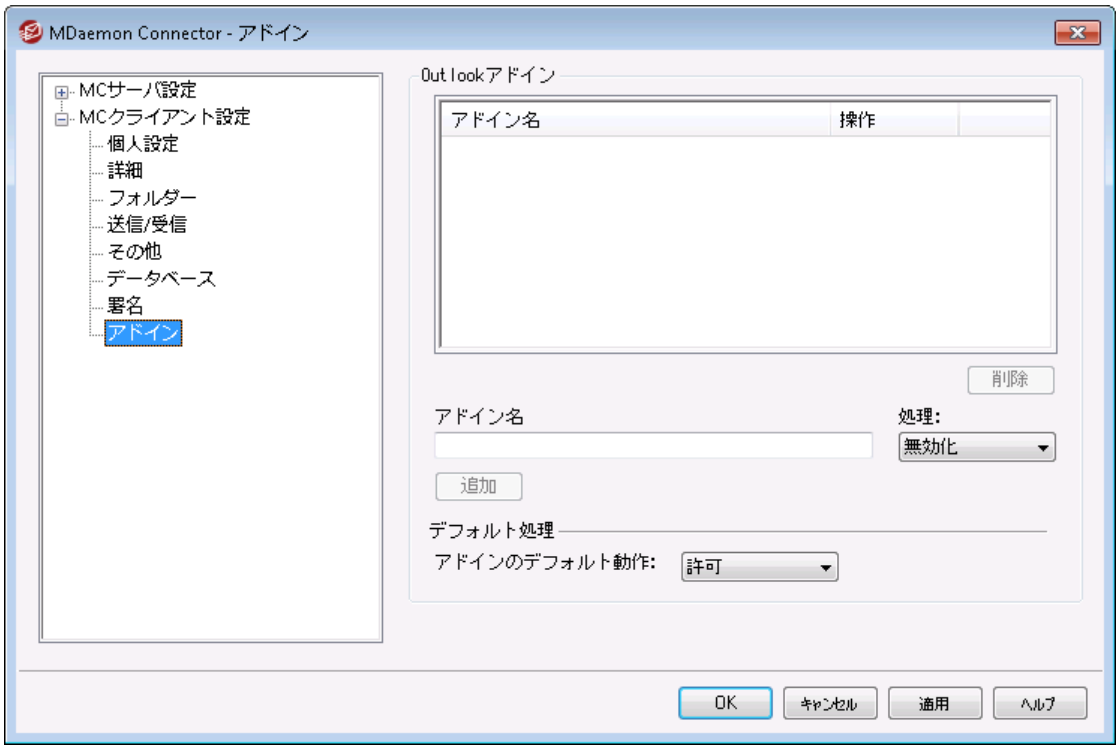
返信/転送メールのデフォルト署名にする
クライアント署名を返信メールや転送メールのデフォルトにする場合はこのボックスを有効化します。

署名の名称:
MDaemon ConnectorユーザーのOutlook用メールアカウントへプッシュ配信する署名の名称を指定します。デフォルトの名称は "MDaemon-$EMAIL$"と指定されています。$EMAIL$ マクロはユーザーのメールアドレスへ書き換えられます。例えば、"MDaemon-Frank.Thomas@company.test"といった名称になります。

参照:

MCクライアント設定 356
MCサーバー設定 ≫ 設定 354
MCサーバー設定 ≫ アカウント 355
デフォルトクライアント署名 125
ドメインマネージャ ≫ クライアント署名 188

3.8.2.8 アドイン



アドイン画面では、MDaemon Connectorユーザーが使っているOutlookアドインの状態を管理する事ができます。普段使用するアドインの許可や選択したアドインの無効化を行う事ができます。この機能は特定のアドインがMDaemon Connectorクライアントと競合している事を把握していて、競合によって発生する問題を避けたいと考えている時に便利な機能です。アドイン機能は、MDaemon Connector 5.0以上に対応しています。

Outlookアドイン

このボックスにはユーザーのOutlookアドインとそれぞれに割り当てられた「無効」「許可」「デフォルト」の中の何れかのアクションが一覧表示されています。MDaemonユーザーがOutlookを開始すると、MCクライアントはユーザーのアドインの一覧をMDaemonへ送信し、無効とされているアドインを無効化します。許可と設定されている場合は変更を行いません。デフォルトと設定されている場合は下記のデフォルト処理が適用されます。

MDaemon ConnectorではMicrosoft Outlookのデフォルト アカウントをMDaemon Connectorへ設定しているユーザーのOutlookアドインのみを管理できます。

アドインの追加、削除、変更

アドインの追加

アドインを一覧へ追加するには、Outlookで表示されるアドイン名を入力し、追加をクリックします。このオプションは管理したいアドインが分かっていて、ユーザーがアドインのインストールをおこなう前には便利なオプションです。

アドインの削除

一覧からアドインを削除する場合は、対象のadd-inを選択し、削除をクリックします。

アドインのアクション設定

アドインを変更するには、選択した後、ドロップダウンリストでアクションを選択し、追加をクリックします。

デフォルト アクション

アドインのデフォルト アクション

このオプションを許可または無効と設定します。許可と設定していた場合、デフォルトで MDaemon Connector は「無効」と設定されているadd-inの無効化のみを行うため、特に設定変更は行われません。無効と設定していた場合、MDaemon Connectorは許可されているもの以外のadd-in全てを無効化します。このオプションはデフォルトで許可されています。

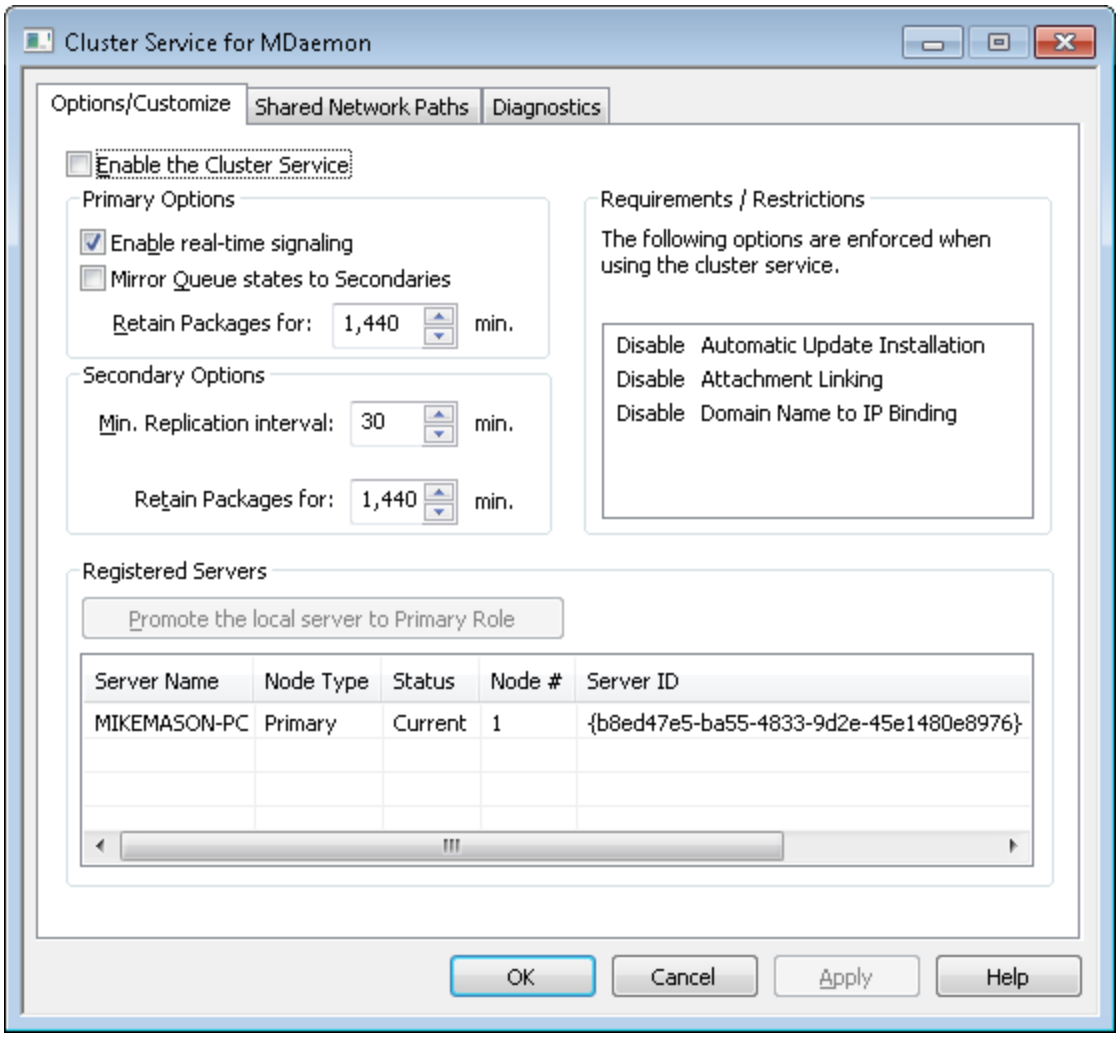
参照:

MCクライアント設定 356
MCサーバー設定 ≫ 設定 354
MCサーバー設定 ≫ アカウント 355

3.9 クラスタサービス

3.9.1 オプション/カスタマイズ

オプション/カスタマイズ



クラスターサービスの有効化
チェックしてクラスタサービスを有効化します。

プライマリオプション

リアルタイム更新を有効にする
デフォルトで、プライマリノードで変更があった場合、セカンダリノードへレプリケーション信号が送信され、ノード間で設定同期を行うためのレプリケーションリクエストを生成します。

プライマリのキューの状態をセカンダリへミラーする
プライマリノードのキューの状態(凍結や無効化)に変更があった際、セカンダリノードでも状態を変更する場合はこの設定を有効化します。

セカンダリオプション

レプリケーション間隔 [xx] 分
セカンダリノードがプライマリノードからのレプリケーション信号を待つ間隔で、到達するとレプリケーションを実行します。デフォルトでは30分です。

登録済サーバー

MDaemonサーバークラスタ内の全てのノードを表示します。

ローカルサーバーをプライマリへ昇格
セカンダリをプライマリとする場合は、昇格したいセカンダリを選択し、昇格をクリックします。新しいプライマリが元のプライマリへクラスタへセカンダリとして参加するよう通知します。複数のセカンダリノードの環境では、2台目以降のセカンダリノードは削除し再度クラスタへ追加する必要があります。

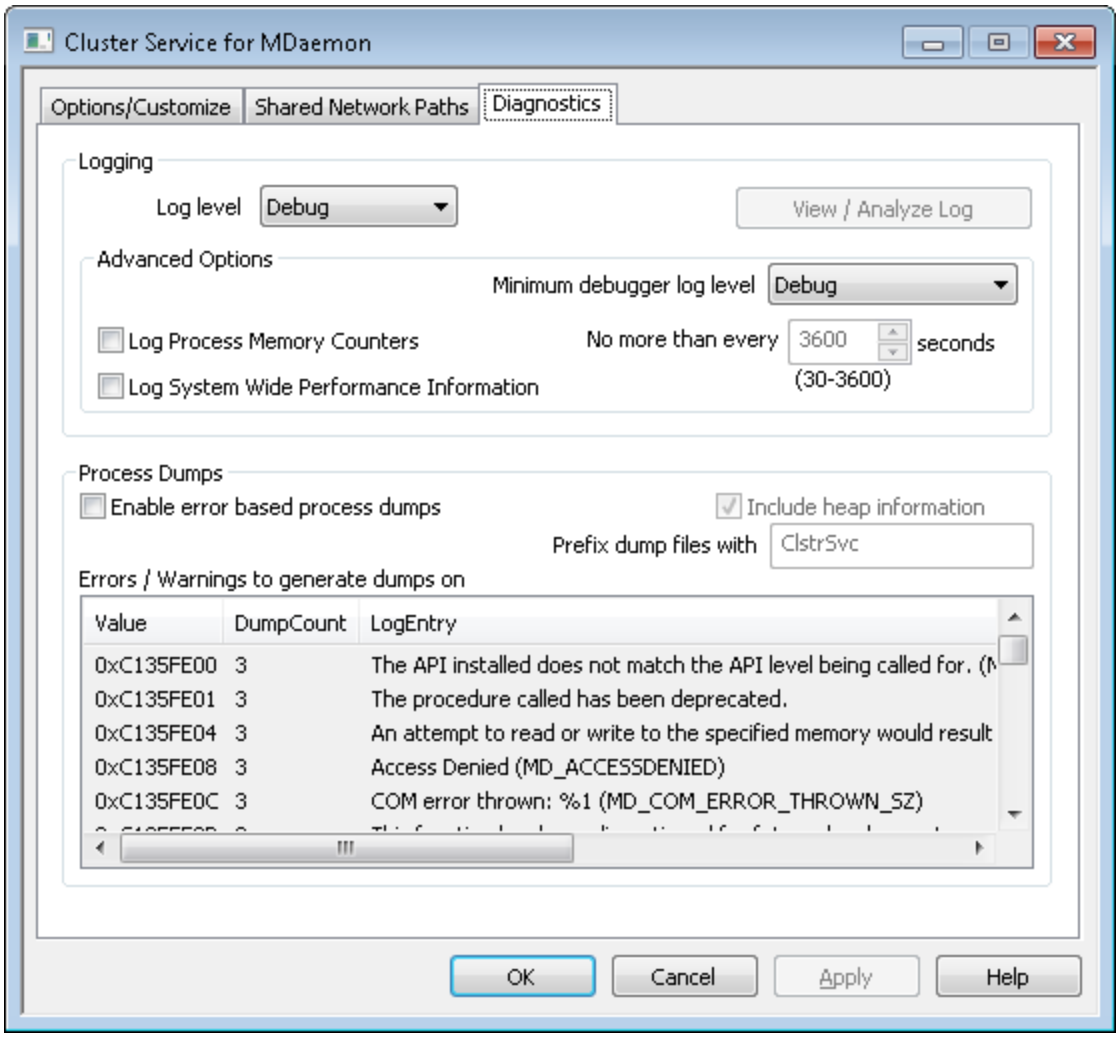
新たなMDaemonサーバーをクラスターへ追加
新しいMDaemonサーバーをクラスタへ追加するには、登録済サーバーの一覧を右クリックし、**新たなMDaemonサーバーをクラスターへ追加** をクリックします。MDaemonがインストールされたセカンダリノードのNETBIOS名、IPアドレス、DNS名のどれかを入力するか、ドロップダウンからサーバーを選択します。ネットワーク内で使用できるサーバーを検索するため時間がかかる場合があります。

参照:

クラスターサービス 373
クラスターサービス | 共有ネットワークパス 375
クラスターサービス | 診断 377

3.9.2 共有ネットワークパス

共有ネットワークパス



共有ネットワークパスの編集を有効化（クラスタの最初のノードで必要）

この画面のオプションを使ってMDaemonクラスターが使用する共有ネットワークパスの設定を行う事ができます。これはクラスタの最初のノードで必要で、共有ネットワークパスが他のノードへレプリケーションされます。

コモンMDaemonネットワーク共有で全ネットワークパスを設定
全ての共有ネットワークパスを一つのコモンネットワーク共有へ配置するにはこのオプションを選択します。このオプションは全てのパスをデフォルト値として設定し、全てのパスは読み取り専用となります。

全ネットワークパスを個々に設定
各共有ネットワークパスを個別に設定するにはこのオプションを選択します。例えばメールフォルダとメールアーカイブを異なるネットワークの場所へ格納する場合には、このオプションを選択します。

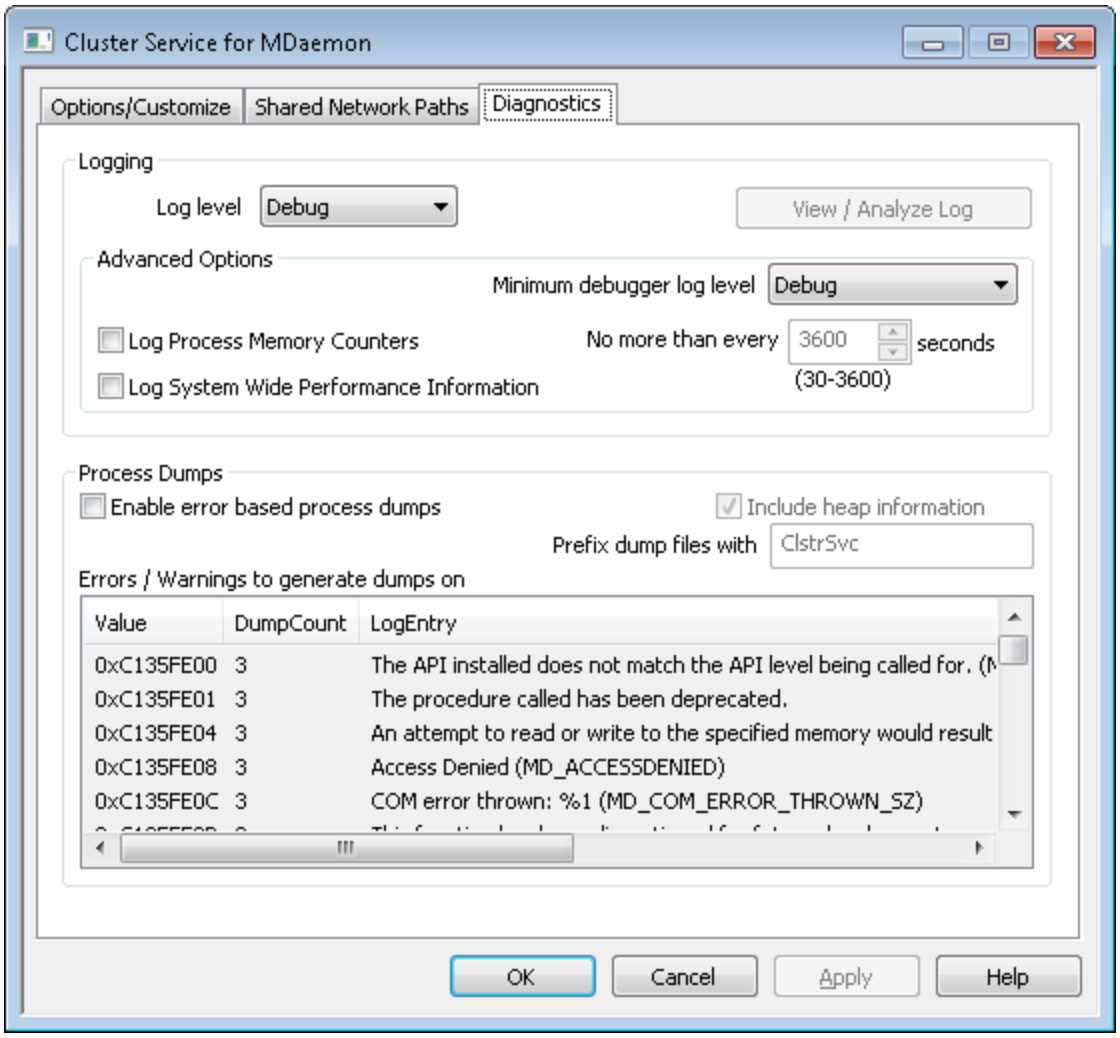
マルチノードでのメールルーティングを有効化
メールキューをクラスタノード間で共有する場合はマルチノードメールルーティングを使用します。複数サーバー処理でのメール配信によって、均等な負荷分散が行えるようになり、サーバーがダウンした際キューへメールが溜まってしまう事も防ぐ事ができるようになります。

参照:

クラスターサービス 373
クラスターサービス | オプション/カスタマイズ 373
クラスターサービス | 診断 377

3.9.3 診断

診断



ロギング

ログレベル

ログデータ量に応じた、6つのレベルのログに対応しています。

デバッグ　最も詳細なログで、記録できる全ての情報が含まれており、問題の診断にのみ

使用されます。

情報 通常のログで、一般的な操作が詳細なしで記録されます。これはデフォルトのログレベルです。

警告 警告、エラー、クリティカルエラー、起動と終了がログに記録されます。

エラー エラー、クリティカルエラー、起動と終了がログに記録されます。

クリティカル クリティカルエラー、起動と終了がログに記録されます。

なし 起動と終了だけがログに記録されます。

ログの表示/分析
このボタンをクリックすると、MDaemon詳細システムログビューアが起動します。デフォルトでログは"..\MDaemon\Logs\"へ格納されます。

詳細オプション

最小デバッガーログレベル
デバッガー向けの最小ログレベルを指定します。使用できるログレベルは下記の通りです。

プロセスメモリカウンターをログへ残す
プロセス毎のメモリ、ハンドラ、スレッド情報をログへ残す場合はこのオプションを有効化します。潜在的なリードやアロケーション問題を特定するのに役立ちます。ログエントリは前回のログから変更があって初めて生成されます。

システム単位でのパフォーマンス情報をログへ残す
システムレベルのパフォーマンス情報をログへ残す場合にはこのオプションを有効化します。潜在的なリードやアロケーション問題を特定するのに役立ちます。ログエントリは前回のログから変更があって初めて生成されます。

[xx]秒毎にログを記録する
プロセスやパフォーマンス情報がログへ記録される頻度をこのオプションで指定します。

プロセスダンプ

エラーを元にしたプロセスダンプを有効化
下記で指定した特定の警告やエラー発生時プロセスダンプを生成するにはこのオプションを有効化します。

ダンプファイルへヒープ情報を含む
デフォルトで、ヒープ情報はプロセスダンプへ含まれます。含まない場合はチェックボックスをクリアしてください。

ダンプファイルの頭文字
プロセスダンプのファイル名はここで指定した文字から始まります。

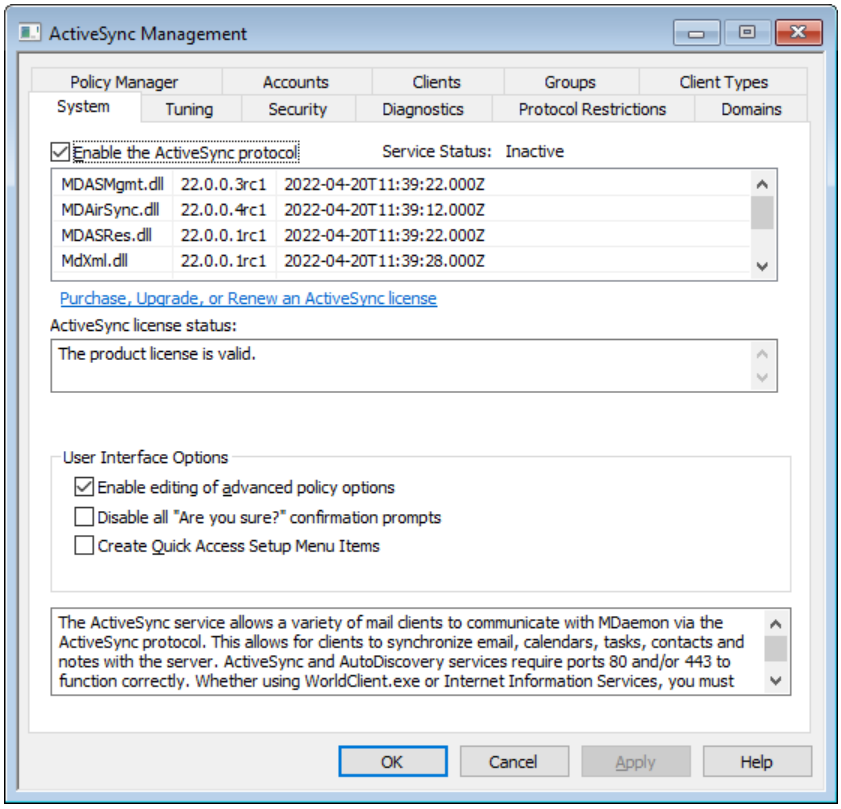
ダンプファイルを生成するエラー/警告
右クリックして、エントリを追加/編集/削除...オプションをクリックし、プロセスダンプの生成のトリガーとするエラーや警告の管理を行います。各エントリではディアクティベートまでのプロセスダンプの数を指定する事ができます。

参照:

クラスターサービス 373
クラスターサービス | オプション/カスタマイズ 373
クラスターサービス | 共有ネットワークパス 375

3.10 ActiveSync

3.10.1 システム



MDaemon はMDaemon Private Cloudのアドオンであるover-the-air（OTA）ActiveSyncサーバー"ActiveSync for MDaemon"に対応しています。このサーバーは、ユーザーのメール、デフォルトの連絡先、デフォルトの予定表、仕事の情報をMDaemon/Webmailのアカウントと ActiveSync対応デバイスとの間で同期する事ができます。

ActiveSyncはウェブサービスの拡張で、**80**（http用）と**443**（https）番ポートのみ使用できます。これはActiveSyncの動作要件です。ActiveSyncが有効でWebmailの内蔵ウェブサーバーを80又は443番ポート以外で使用している場合はWebサーバー295やSSL & HTTPS300で設定しているポートを80番へ変更してください。もしもWebmailでIISなどの他のサーバーを使っている場合は、80番や443番ポートを使用するよう、手動で設定を行って下さい。

ActiveSyncをIISで稼働させる場合は、"/Microsoft-Server-ActiveSync"が要求された際、ActiveSync DLL（MDAirSync.dll）を呼び出す必要があります。これは全てのActiveSyncクライアントで必要です。IISのバージョンによっては、この機能に対応しておらず、そのためのソフトウェアを、別途ダウンロード、インストール、設定する必要が生じる場合があります。

> ActiveSyncと最初の同期を行う際にはサーバーからデバイスに対して一方向の同期が行われます。ActiveSyncでの最初の同期時、デバイス内のデータが消去されます。これはActiveSyncの動作要件です。そのため、デバイス内のデータは、ActiveSyncとの初回同期を行う前にバックアップして下さい。ActiveSync対応のデバイスのほとんどは、**"データが消去されます"**といった警告文を表示しますが、機種によって警告が表示されない場合もあります。ActiveSyncの操作は慎重に行って下さい。

ActiveSyncの有効化／無効化

ActiveSyncプロトコルを有効化 をクリックする事で、ActiveSync for MDaemonが有効になります。その後、ドメイン397のオプションで、全てのドメインや個々のドメインに対してActiveSyncを有効化できます。

ユーザー管理オプション

詳細ポリシーオプションの編集の有効化
ActiveSyncポリシーエディタ406で詳細タブを表示するにはこのオプションを有効にします。多くの場合は変更する必要のない、詳細なポリシー設定がこの画面に含まれています。このオプションはデフォルトで無効になっています。

"実行してよろしいでしょうか？"とする確認全てを無効化する
デフォルトでは、ActiveSyncの設定変更を行うと、「実行してもよろしいでしょうか」という確認用のプロンプトが表示されます。これを無効化する場合には、このオプションを有効化します。

クイックアクセス設定メニューアイテムを生成
このオプションを有効にすると、MDaemonの管理画面の 設定 ≫ ActiveSync メニューが変更され、ActiveSync接続モニターとログビューア/アナライザへのリンクが表示されます。 **注意点：** このオプションを無効化しても、これらのツールには管理画面のサーバーの下のActiveSyncを右クリックしてアクセスする事ができます。

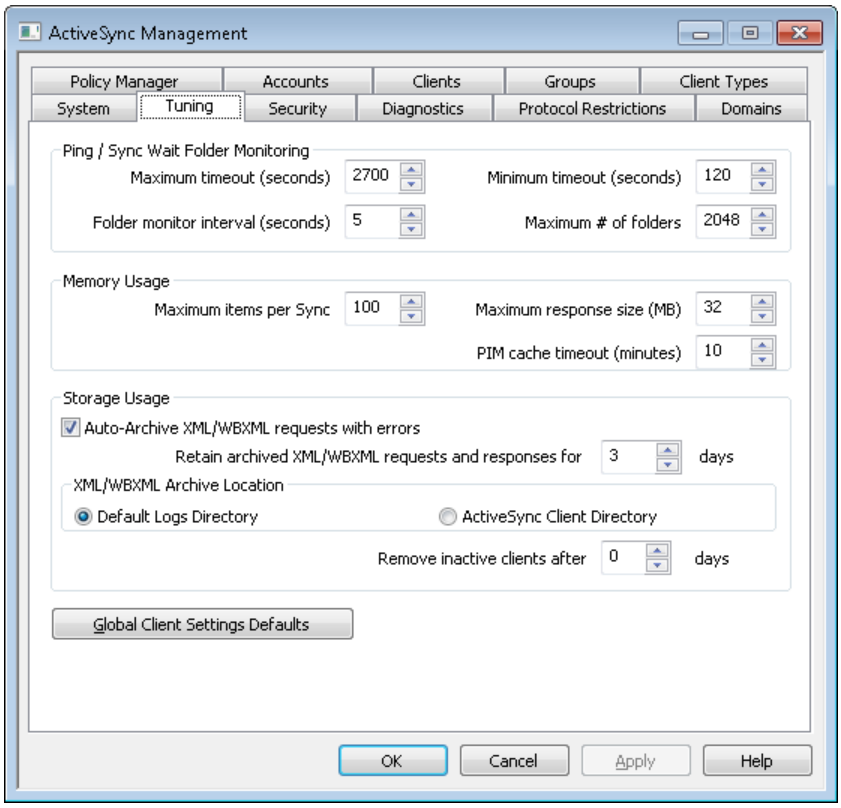
ActiveSync自動検出サービス

MDaemonのActiveSync自動検出サービスにより、ユーザーはActiveSyncサーバーのホスト名を知らなくとも、メールアドレスとパスワードだけでActiveSync用アカウントを設定できるようになります。自動検出を行うにはHTTPS300を有効化する必要があります。また、多くのシステムでは、ActiveSyncが稼働しているサーバへ"autodiscover.yourdomainname.com"（例，autodiscover.example.com）という名前解決ができるようDNSサーバ上に新たにCNAMEまたはAレコードの登録も必要です。

参照:

アカウントエディタ ≫ ActiveSync 696
ActiveSync ≫ ドメイン 397
SSL & HTTPS 300
Webサーバー 295

3.10.2 チューニング



ここでは、ほとんど調整の必要がない詳細設定を行う事ができ、グローバルクライアント設定のデフォルト 384 ボタンから、ActiveSyncクライアントのデフォルト値の調整も行えます。

Ping / 同期応答フォルダの監視

最大タイムアウト（1200-7200秒）
MDaemon ActiveSync Service（MDAS）がフォルダ監視において、クライアントからの応答を待ち、タイムアウトになるまでの最大時間を指定します。デフォルト値は2700秒（45分）です。

最小タイムアウト（120-480秒）
MDaemon ActiveSync Service（MDAS）がフォルダ監視において、クライアントからの応答を待ち、タイムアウトになるまでの最小時間を指定します。デフォルト値は120秒です。必要に応じてこの

値を上げ、クライアントからの接続頻度を下げる事で、サーバーに対する接続数を下げる事ができます。

フォルダ監視の間隔（3-50秒）
ActiveSyncでフォルダ監視を行う際、次の監視を実行するまでに何秒間待つのかをここで指定します。デフォルトは5秒です。

フォルダの最大数
ActiveSyncデバイス毎に変更を監視できるフォルダの最大数です。デフォルト値は2048です。

メモリ使用

同期毎の最大アイテム数
ActiveSyncサービスが同期リクエストに対する応答でクライアントから受け取るアイテムの最大数を指定します。このオプションで低い値を設定すると、使用率の高いサーバーにおけるメモリ使用率は下げる事ができますが、より多くの接続と通信帯域が必要になります。また、デバイスが同期の際、全ての変更を受け取るためにより多くのリクエストを送るため、バッテリー寿命を早める可能性があります。ここで大きい値を指定するとメモリ使用率は大きくなるものの、通信エラーが発生する可能性が高くなります。デフォルト値である100を推奨しています。特に意味はありませんが、クライアントに合わせた値を指定することで、クライアントによっては効率よく使用するリソースを減らす事ができる場合があります。クライアントのリクエスト値が最大値より大きい場合は、最大値が使用されます。

XML応答の最大サイズ（MB）
クライアントからの同期リクエストに対して許可する応答の最大サイズです。サーバーからクライアントへの同期を処理する前に、現在の応答サイズをチェックし、この値と同じかそれ以上だった場合は、まだ変更がある事を示すフラグを追加し、応答用アイテムとします。これは大きなサイズの添付ファイルをメールで定常的にやり取りしている環境において便利な機能です。

PIMデータのキャッシュの保存期間（5-60分）
連絡先、ドキュメント、予定などのPIMデータは静的で、クライアントから時々アップデートがあるだけ、という場合はよくあります。MDASはこのデータをキャッシュとして保存し、ディスクの負荷を軽減します。ただ、このキャッシュはディスクに書き込んだデータに変更があった場合は自動でリロードされます。この値はユーザーのデータを最後のアクセスから最大どのくらいの時間キャッシュするかを指定するものです。

ストレージ利用

エラーの発生したXML/WBXMLを自動保存
クライアント設定 384 画面の*[XML / WBXML]リクエストと応答をアーカイブする*オプションを無効にした際、このオプションで問題のあるXMLやWBXML応答のみをアーカイブできます。このオプションはデフォルトで有効です。

アーカイブしたXML/WBXMLリクエストと応答を[xx]日間保管する
自動アーカイブされた応答を保存する日数を指定します。デフォルト値は3日間です。

XML/WBXMLアーカイブの保存先

デフォルトのログディレクトリ
自動アーカイブされるXML/WBXMLリクエストとエラーのファイルは、デフォルトでMDaemonのログディレクトリへ保存されます。

ActiveSyncクライアント ディレクトリ
ユーザーのActiveSyncクライアント デバッグディレクトリへファイルを保存する場合はこのオプションを選択します。

使用のないクライアントを削除するまでの期間 [xx] 日
ActiveSyncデバイス[422]がMDASに接続しなくてもよい最大日数で、この日数に到達すると管理対象からこの端末が削除されます。端末が削除されると、設定が全てなくなり、端末が再接続した際には、MDaemonはこれを管理した事のない新しい端末として扱います。ドメイン[397]やアカウント[413]用ポリシーが用意されていればこれを適用し、対象フォルダを全て再同期します。このオプションによりサーバーは古い端末や未使用端末の情報をメンテナンスする必要がなくなります。このオプションはデフォルトで31日と設定されています。

グローバルクライアント設定のデフォルト
このボタンをクリックするとグローバルActiveSyncクライアント設定[384]ダイアログが起動し、ActiveSyncクライアント用のデフォルト値の設定が行えます。

ActiveSync通知

ActiveSyncへ管理用の2つの通知が追加されました: 同期のロールバック通知とエラー通知です。

同期のロールバック通知

ActiveSyncサービスで、クライアントが繰り返し/頻繁に期限切れの同期用のキーを同期処理用に送信している場合に管理者へ通知を送るようになりました。

クライアントが期限切れの同期用キーで同期要求を行っている事から、こうした処理はデータのロールバックを意味する事がよくあります。件名は「期限切れの同期用キーを使用しているActiveSyncクライアント」です。これは、過去にクライアントへ送られたコンテンツがネットワークの問題等で同期できていなかった問題を表す場合があります。場合によっては、過去の同期データが送信されたかどうかによって、IDだけが送信されていた場合もあります。

ロールバックの警告は、クライアントが同期できていないという意味ではなく、クライアントが同期対象外になる可能性がある事や、それをシステムで検知した事を示しています。データのロールバック警告は24時間に一度だけ通知されます。

- [System] SendRollbackNotifications=[0|1|Yes|No|True|False](デフォルトは無効化)
- [System] RollbackNotificationThreshhold=[1-254]: ロールバックの数字は管理者へ通知される前に実行される必要のある回数です。ここでは、ネットワークの問題も関係する事から、最小5回を推奨します(デフォルトは10)
- [System] RollbackNotificationCCUser=[0|1|Yes|No|True|False]: 期限切れの同期用キーを送ったクライアントをCCへ含むかどうかを指定します。(デフォルトは無効化)

ActiveSyncエラーメール通知

ActiveSyncサービスで管理者へ処理されなかった特定のメッセージを通知するようになりました。これらのメッセージは対象のアイテムが処理できず、それによってその後のアクションが実行できない旨をリアルタイムで管理者へ通知します。件名は「エラーメッセージ通知」です。従来、これらのアイテムによってクラッシュの可能性がありました。多くの場合、msgファイルの内容はMIMEデータではありませんでしたが、これがMIMEデータの場合、エラーの場合がほとんどでした。これらの通知で関連す

るユーザーをCCに入れるかどうかを選択でき、ユーザーへの通知はCMNCCUserキーを付与するため、メールボックスに届いたメールが読み取りできない場合でもそれを知る事ができます。こうした場合に行うべき対応は対象のmsgファイルをユーザーのメールボックスから移動し、これを解析して処理できなかった原因とどのような解決策があるのかを検討する事です。
\MDaemon\Data\AirSync.ini の[System]ヘッダ以下で、次のキーを編集できます。

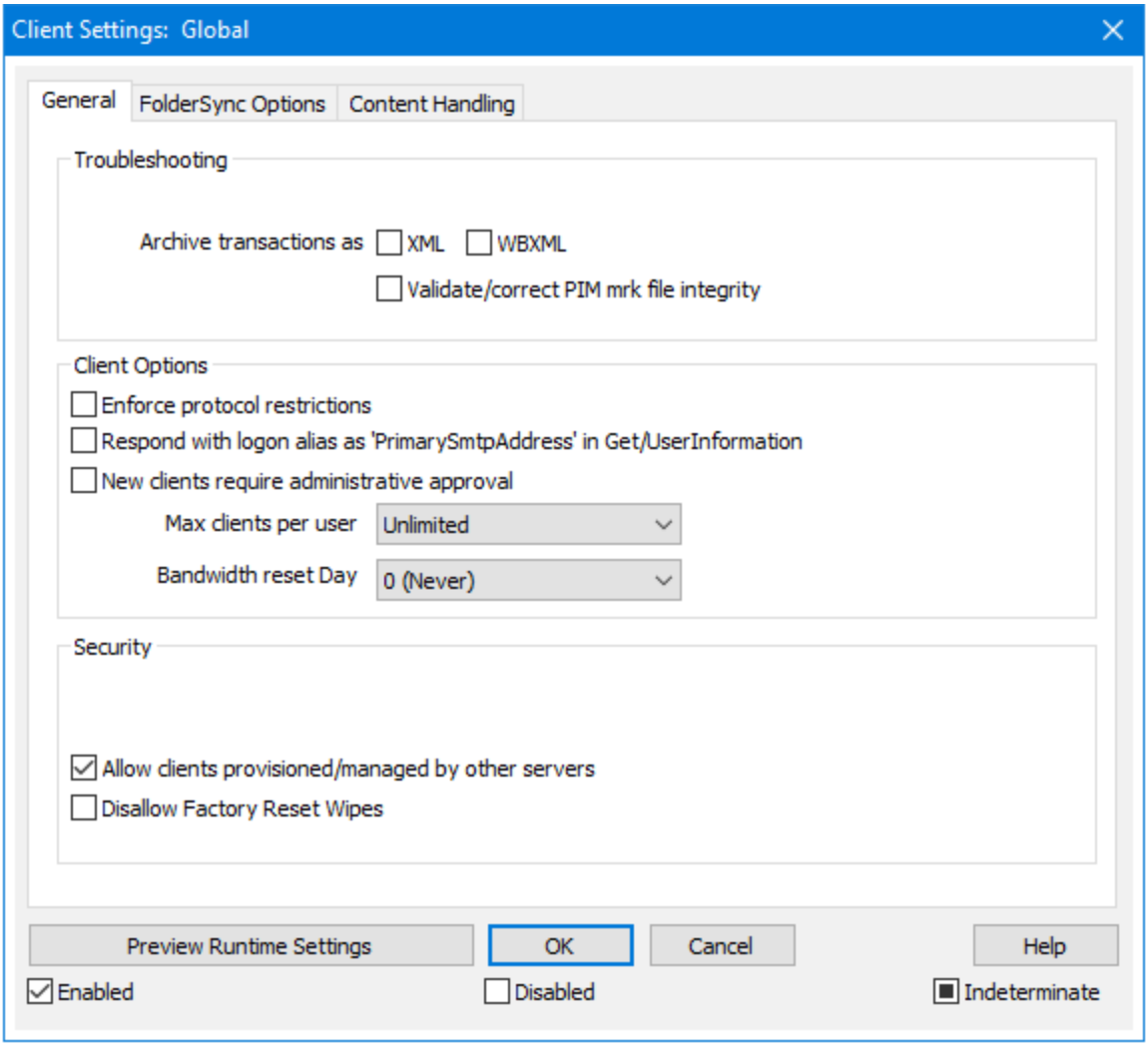
- [System] SendCorruptMessageNotifications=[Yes|No|1|0|True|False]（デフォルトは有効）
- [System] CMNCCUser==[0|1|Yes|No|True|False]（デフォルトは有効）

参照:

ActiveSync ≫ 診断 393

3.10.2.1 クライアント設定

クライアント設定画面には、ActiveSync用に設定されたデフォルトのActiveSync設定プロファイルの一覧が表示されています。次のクライアント設定プロファイルを作成・編集する事ができます： 全体設定, ドメイン 188, グループ 431, アカウント 413, クライアントタイプ 438, クライアント 422（例．端末）



この画面ではActiveSyncクライアントを管理するための全体設定が行えます。これに対応したクライアント設定が、ActiveSyncの、ドメイン[397], アカウント[413]、クライアント[422]、といった他のページにも存在します。全体設定で特定の値を設定すると、ドメイン、アカウント、クライアントのデフォルト値は上位のオプションを引き継ぎます。そのため、この画面で行った設定は、他の設定にも影響を与える事になります。この画面で設定を行う事により、下位のクライアント全ての設定を効率よく管理できます。また、ドメインやアカウント、それ以外の下位の設定は上位の設定値を上書きし、必要に応じてドメイン、アカウント、その他のレベルで設定変更が行えます。

デバイスへ適用され、デバイスの挙動を決定するポリシー[405]同様、クライアント設定はクライアントに関連したオプションを元に、アカウントが利用できるActiveSyncクライアントの最大数、パブリックフォルダがアカウントフォルダと同様同期を行うのかどうか、ユーザーの許可リストを含むかどうか、といった、サーバーの挙動を決定します。

全般

トラブルシューティング

ログレベル

ActiveSync for MDaemonはログデータ量に応じた、6つのレベルのログに対応しています。

デバッグ 最も詳細なログで、記録できる全ての情報が含まれており、問題の診断にのみ使用されます。

情報 通常のログで、一般的な操作が詳細なしで記録されます。これはデフォルトのログレベルです。

警告 警告、エラー、クリティカルエラー、起動と終了がログに記録されます。

エラー エラー、クリティカルエラー、起動と終了がログに記録されます。

クリティカル クリティカルエラー、起動と終了がログに記録されます。

なし 起動と終了だけがログに記録されます。

継承 デフォルトで、ログレベルの設定はクライアント設定の階層から継承されます。そのため、クライアントは設定をクライアントタイプから引継ぎ、クライアントタイプはアカウントから引継ぎ、アカウントはグループから引継ぎます。全体のクライアント設定は 診断 393 ダイアログのログレベル設定を元にしています。

トランスアクションを [XML | WBXML]としてアーカイブ
XMLやWBXMLデータをアーカイブするには、*XMLと WBXMLをアーカイブ...* のオプションを使用します。これはデバッグの際役立ちます。全体オプションはデフォルトで無効になっています。

PIM mrkファイルの整合性を確認する
クライアントのPIMデータの整合性テストを実施し、iCal UIDの重複や空の要求フィールドといった、同期を妨げているものがないかどうかを確認します。この全体設定はデフォルトで無効になっています。

クライアントオプション

プロトコル制限を強制する
クライアントで許可されているプロトコルバージョン以外のアクセスを拒否する場合はこのオプションを有効にします。デフォルトでこのオプションは無効になっており、プロトコル制限は異なるプロトコルのクライアントを拒否していません。プロトコル制限は単純に、クライアントに対して使用するべきプロトコルを伝えるのみの機能を提供しています。クライアントがそれでも制限されているプロトコルを使った場合、MDaemonはその接続を受け入れます。詳細は次のページをご覧下さい: プロトコル制限 395

Get/UserInformationへの応答でログオンエイリアスを'PrimarySmtpAddress' として使用する
サービスがSettings/Get/UserInformationリクエストに対する応答としてエイリアスやセカンダリアドレスをプライマリアドレスとして利用できるようにします。これはiOS 9.xへアップデートした際エイリアスか

らメールを送信できなくなった事に対する対処です。このオプションによって使用に反した応答を受け取る場合があります。

新しいクライアントは管理者の承認が必要
新しいクライアントがアカウントとの同期を開始する前に、管理者による承認を必要とする場合はこのオプションを有効にします。クライアント[422]一覧で認証待ちのクライアントが確認でき、管理者は同じ画面から承認が行えます。この設定はデフォルトで無効になっています。

ユーザー毎の最大クライアント
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域リセット日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

セキュリティ

ロケーションスクリーンから除外する
ActiveSyncクライアント設定で端末をロケーションスクリーニング[520]から除外する場合はこのオプションを有効化します。これにより認証済ユーザーは、例えば認証がブロックされている場所へ出張しているような場合であっても、ActiveSync経由でアカウントへアクセスする事ができるようになります。端末を除外するためには、チューニング画面にあるこの日数を超えて認証されなかった端末を自動削除[381]設定の時間内に、ActiveSyncを使った接続と認証を行っておく必要があります。

リモートアドレスを動的に除外
接続元のリモートIPアドレスをロケーションスクリーニングの除外リストへ追加する事ができます。このオプションは、同じIPアドレスを使って接続する他のクライアントがある場合に便利です。

ユーザー毎の最大クライアント数
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域の統計情報をリセットする日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

他のサーバーで管理されているクライアントへの接続を許可する
デフォルトで、ActiveSyncサーバーが特定のクライアントへデータやポリシーを送信する際、対象クライアントが他のActiveSyncサーバーからも管理されている事が分かった場合も、クライアントは

MDaemonへアクセスする事ができます。しかし、このような環境の場合、適用するポリシーが他のActiveSyncサーバーと競合する可能性があります。一般的に、クライアントはポリシーが競合した場合、厳しい方へ合わせる傾向があります。こうしたクライアントからの接続を制限する場合は、このオプションを無効化して下さい。

工場出荷時への完全ワイプを無効化
オン/はい、を設定すると、ActiveSyncクライアントの完全ワイプが行えなくなります。クライアントでリモートからの完全ワイプを許可する場合、最初にこのオプションを無効化して下さい。このオプションはデフォルトで無効に設定されています。クライアントページの次の項目を参照して下さい: ActiveSyncクライアントの完全ワイプ 422

フォルダ同期オプション

フォルダ同期オプション

除外

ユーザの [許可リスト/ブロックリスト] フォルダ
デフォルトでユーザーの許可リストとブロックリストの連絡先フォルダは端末と同期を行いません。これらはMDaemonがスパムからシステムを自動的に保護するのを支援する目的で使用されます。そのため、許可リストやブロックリストは端末上に連絡先として表示する必要性はありません。

デフォルト以外のメールフォルダ
デフォルトで、ユーザーが作成したメールフォルダとデフォルトメールフォルダは全て端末と同期します。同期するのを受信箱や送信箱、削除済アイテム、下書き、といった、デフォルトのメールフォルダのみにしたい場合はこのオプションを有効にして下さい。ユーザーが作成したフォルダは同期対象に含まれません。 このオプションはデフォルトで無効になっています。

デフォルト以外のPIMフォルダ
デフォルトで、(連絡先、予定表、仕事などの) PIMフォルダは全て端末と同期します。同期するのをデフォルトのPIMフォルダのみにしたい場合はこのオプションを有効にして下さい。このオプションが有効な場合で、ユーザーが複数の予定表を保有してる場合デフォルトの予定表のみが同期対象となります。 このオプションはデフォルトで無効になっています。

含む

パブリックフォルダの階層
ユーザーがアクセス権を持っている パブリックフォルダ 283 をユーザーのActiveSync用端末のフォルダ一覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
パブリックフォルダ 283 をユーザーが検索できるようになります。 これはデフォルトで許可されています。

パブリックフォルダの横断 (フォルダ名の公開)
デフォルトで、クライアントがパブリックのサブフォルダへのアクセスや同期を行うには、サブフォルダと上位のパブリックフォルダ 283 全てに対してルックアップ権限 285 が必要です。上位のフォルダに対するアクセス権がない場合、その中のサブフォルダに対しては、例え設定上は許可されていて

も、アクセスする事はできません。クライアントからこうしたサブフォルダへアクセスできるようにする場合は、このオプションを有効にします。注意点: このオプションを有効化すると、上位のフォルダもクライアントへ許可する事となり、セキュリティのリスクを招く恐れがあります。 このオプションはデフォルトで無効になっています。

許可するパブリックフォルダの最大数
端末で処理するパブリックフォルダ数を制限する場合はこのオプションを使用します。制限が設定されると、サーバーは最大数に到達するまでフォルダー覧を処理し、これを超えるとその後のデータを送りません。処理するフォルダの順番を決める事はできません。デフォルトで、全体での最大数は設定されていません。

共有フォルダも含める

ユーザーがアクセス権を持っている 共有フォルダ[107] をユーザーのActiveSync用端末のフォルダー覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
共有フォルダ[676] をユーザーが検索できるようになります。 これはデフォルトで許可されています。

コンテンツ処理

コンテンツ処理オプション

クライアントにフラグ付けされたメール用にタスク・リマインダーを作成
このオプションでMDaemonはフラグが付いたアイテムごとに仕事を作成し、リマインダーをユーザーへ送信できるようになります。この設定の全体値はデフォルトで有効です。

予定を編集した際、常にミーティングのアップデートを送信
クライアントの中には、ミーティングを編集した際、更新情報を適切に送信しないものもあります。このオプションを使うとActiveSyncサービスへ、ミーティングが開催者によって更新された際、更新情報を送信するよう促す事ができるようになります。これはミーティングの更新情報の送信に失敗しているクライアント[422]やクライアントタイプ[438]に限定して使用するべきで、更新情報が重複して送られてしまう可能性があります。また、このオプションはクライアントとクライアントタイプの設定ページでのみ利用できます。

全ての送信メールで開封確認を要求
クライアントから送信される全てのメールで開封確認要求を行うにはこのオプションを有効にして下さい。これはデフォルトで無効になっています。

送信者からリクエストされた際送信済メールについて開封確認を送信
サーバー側で開封確認要求を検出し、既読フラグがついたメールの開封通知を送信するにはこのオプションを使用します。 これはデフォルトで無効になっています。

ReplyToアドレスに指定したエイリアスとして送る
クライアントによっては、エイリアスを使ったメール送信を許可していません。この機能は Exchange ActiveSync（EAS）プロトコル[395] 16.xで追加されたものですが、クライアントの中には16.xに対応していないものもあります。例えば、Windows用OutlookはEAS 14.0だけを使用しており、ユーザー

が関連するアドレスを指定して送信する事のみ許可しており、生成されたメールはユーザーの選択を正しく反映していません。このオプションでは、ReplyToのアドレスがユーザー用の正しいエイリアス[757]であれば、これを使ってメール送信を行います。この設定の全体値はデフォルトで有効です。

デフォルトの連絡先にパブリック連絡先を仮想的に統合する
パブリック連絡先をユーザーの端末上でデフォルトの連絡先と統合したい場合はこのオプションを有効にします。これは仮想的な統合で、実際には連絡先フォルダへデータのコピーは行っていません。これはグローバルアドレス帳（GAL）の検索機能に対応していないクライアントにとって便利な機能です。これはデフォルトで無効になっています。

Junk-Emailフォルダへ移動したメールの送信者をブロックする
有効にすると、クライアントが特定のメールを自分のJunk Emailフォルダへ移動した際、対象のメール送信者がブロックされた送信者連絡先フォルダへ追加されます。

ミーティング要求が許可/拒否された際、ミーティング要求に対する応答の送信を強制的に行う
このオプションを使用すると、クライアントがミーティング要求に対して、許可や拒否、その他のアクションを選択した際、ミーティング要求に対する応答を開催者へ送信します。これは、こうした更新情報を自動送信する事ができない特定のクライアント用の機能です。

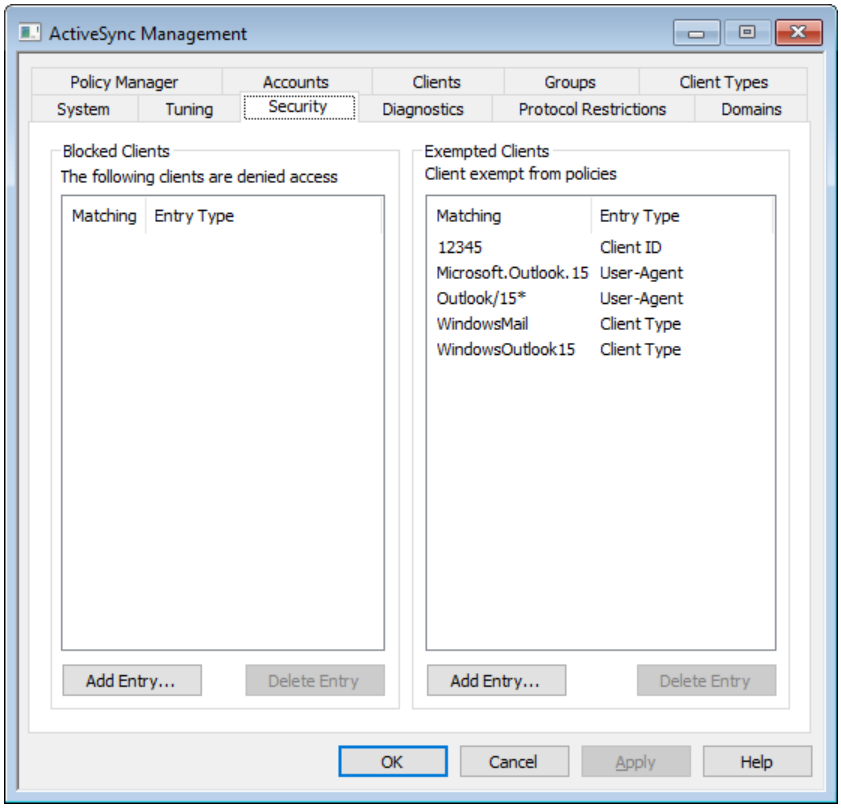
有効な設定をプレビュー

このボタンは全てのクライアント設定（ドメイン[397], アカウント[413], クライアント[422]）に対して使用できます。画面のオプションはデフォルト値をその上位の画面から引き継いでいるため、この機能は表示されている画面の現在の設定確認を行う際にもご利用頂けます。

参照:

ActiveSync » ドメイン[397]
ActiveSync » アカウント[413]
ActiveSync » クライアント[422]

3.10.3 セキュリティ

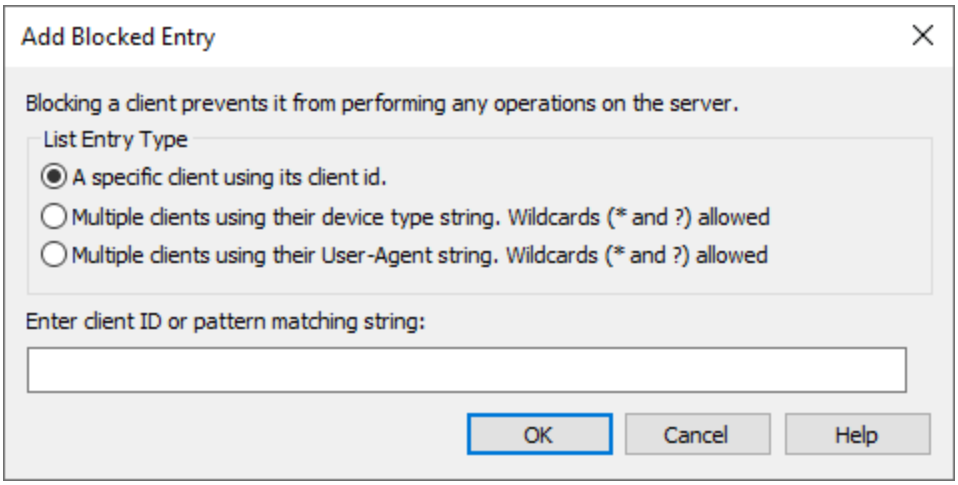


ブロック対象のクライアント

特定のデバイスタイプ、クライアントID、ユーザーエージェントがMDaemonのActiveSyncサーバーへ接続するのを防ぐにはこのオプションを使用します。

ブロックエントリーの登録

一覧へエントリを追加するには、**エントリの登録**をクリックし、デバイス情報を指定した後**Ok**をクリックします。デバイスがMDaemonのActiveSyncサーバーへ接続した事があれば、デバイスの情報はActiveSyncログファイルでも確認する事ができます。



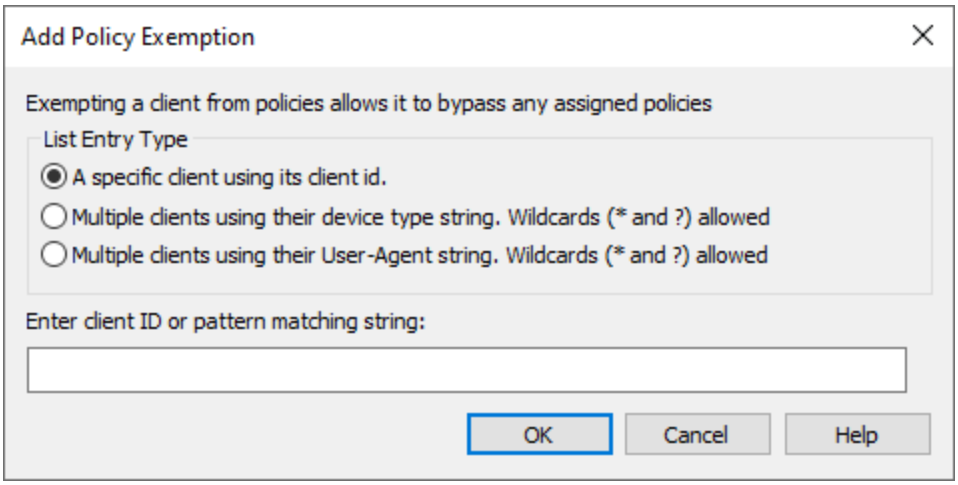
クライアント[422]ダイアログでもデバイスを簡単にブロックできます。クライアントを右クリックした後、**クライアントをブロック**をクリックします。

ブロックエントリーの削除
エントリを削除するには一覧からエントリを選択し、エントリーの削除をクリックします。削除前に、確認画面が表示されます。

除外対象のクライアント

特定のデバイスタイプ、クライアントID、ユーザーエージェントを[ポリシー][405]制限などから除外するにはこのオプションを使用します。

除外対象クライアントの登録
一覧へエントリを追加するには、**エントリの登録**をクリックし、デバイス情報を指定した後**Ok**をクリックします。デバイスがMDaemonのActiveSyncサーバーへ接続した事があれば、デバイスの情報はActiveSyncログファイルでも確認する事ができます。



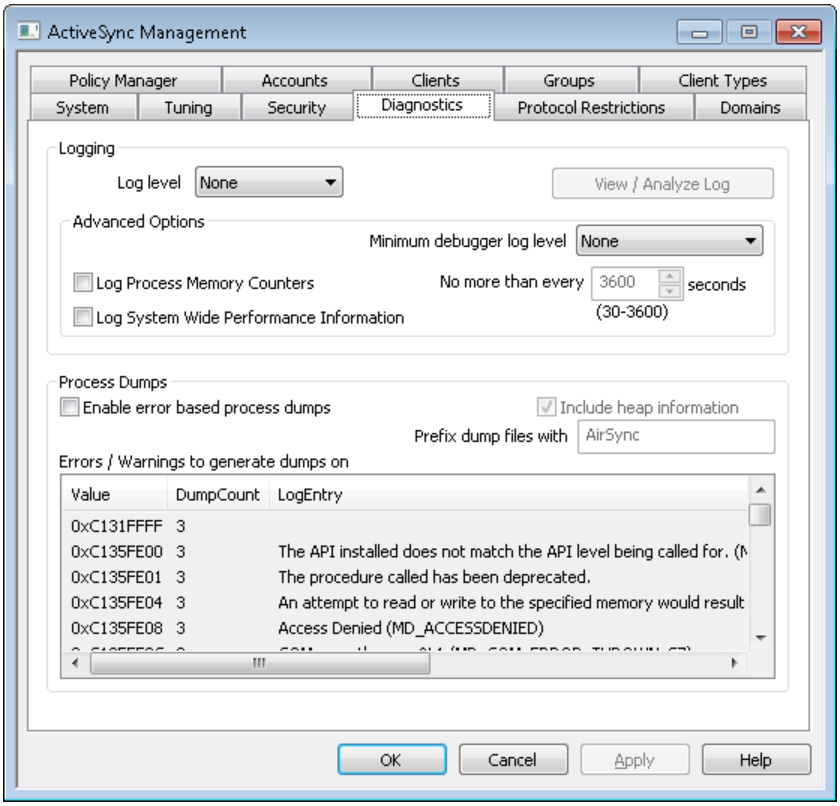
クライアント 422 ダイアログでもデバイスを簡単に除外できます。クライアントを右クリックした後、**クライアントをポリシーから除外**をクリックします。

エントリーの削除
エントリを削除するには一覧からエントリを選択し、エントリーの削除をクリックします。削除前に、確認画面が表示されます。

参照:

ActiveSync » クライアント 220

3.10.4 診断



ここでは、技術サポート等で依頼された場合などを除き、ほとんど調整の必要がない詳細設定を行えます。

ログとアーカイブ

このセクションはActiveSyncのグローバルログレベルの設定用の画面です。ドメインクライアント設定 196 でログレベルの設定が「継承またはデフォルト」になっていると、設定はこの画面から引継ぎます。

ログレベル

ログデータ量に応じた、6つのレベルのログに対応しています。

デバッグ 最も詳細なログで、記録できる全ての情報が含まれており、問題の診断にのみ使用されます。

情報 通常のログで、一般的な操作が詳細なしで記録されます。これはデフォルトのログレベルです。

警告 警告、エラー、クリティカルエラー、起動と終了がログに記録されます。

エラー エラー、クリティカルエラー、起動と終了がログに記録されます。

クリティカル クリティカルエラー、起動と終了がログに記録されます。

なし 起動と終了だけがログに記録されます。

ログの表示/分析
このボタンをクリックすると、MDaemon詳細システムログビューアが起動します。デフォルトでログは"..\MDaemon\Logs\"へ格納されます。

詳細オプション

最小デバッガーログレベル
デバッガー向けの最小ログレベルを指定します。使用できるログレベルは下記の通りです。

プロセスメモリカウンターをログへ残す
プロセス毎のメモリ、ハンドラ、スレッド情報をログへ残す場合はこのオプションを有効化します。潜在的なリードやアロケーション問題を特定するのに役立ちます。ログエントリは前回のログから変更があって初めて生成されます。

システム単位でのパフォーマンス情報をログへ残す
システムレベルのパフォーマンス情報をログへ残す場合にはこのオプションを有効化します。潜在的なリードやアロケーション問題を特定するのに役立ちます。ログエントリは前回のログから変更があって初めて生成されます。

[xx]秒毎にログを記録する
プロセスやパフォーマンス情報がログへ記録される頻度をこのオプションで指定します。

プロセスダンプ

エラーを元にしたプロセスダンプを有効化
下記で指定した特定の警告やエラー発生時プロセスダンプを生成するにはこのオプションを有効化します。

ダンプファイルへヒープ情報を含む
デフォルトで、ヒープ情報はプロセスダンプへ含まれます。含まない場合はチェックボックスをクリアしてください。

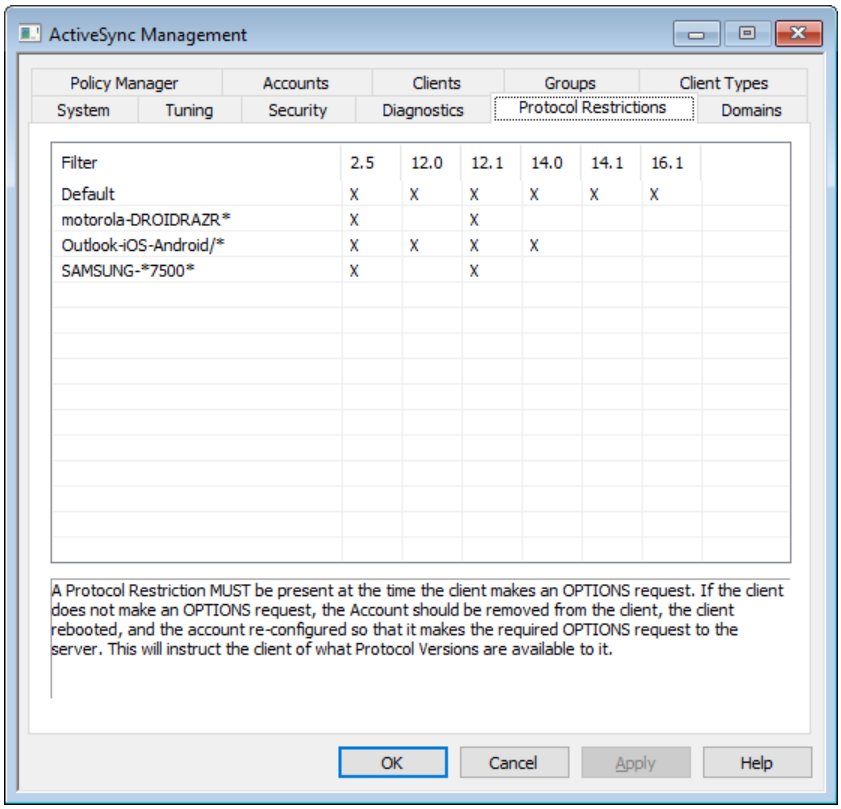
ダンプファイルの頭文字
プロセスダンプのファイル名はここで指定した文字から始まります。

ダンプファイルを生成するエラー/警告
右クリックして、エントリを追加/編集/削除...オプションをクリックし、プロセスダンプの生成のトリガーとするエラーや警告の管理を行います。各エントリではディアクティベートまでのプロセスダンプの数を指定する事ができます。

参照:

ActiveSync ≫ チューニング 381

3.10.5 プロトコル制限



デバイスプロトコル制限

"ActiveSync ≫ プロトコル制限"から特定のクライアントや端末に対してActiveSyncプロトコルを制限できます。これは例えば特定の種類のデバイスが、特定のプロコルには対応しておらず、別のプロトコルには対応しているといった場合に便利です。プロトコル制限の作成/編集 396 ダイアログでは、ユーザーエージェントやデバイスの種類を元に、ActiveSyncプロトコル2.5, 12.0, 12.1, 14.0, 14.1, 16.1 の使用に限定することができます。

デフォルトで、プロトコル制限はクライアントが異なるプロトコルを使用しようとする動きを制限するものではなく、クライアントに使用するプロトコルを伝えるものとなっています。それでもクライアントが制限されているプロトコルを使用しようとした場合は、MDaemonはその通信を許可します。制限されたプロトコルでの通信を拒否したい場合は、クライアント設定[384]の、*全てのプロトコル制限を強制する*オプションを使用します。

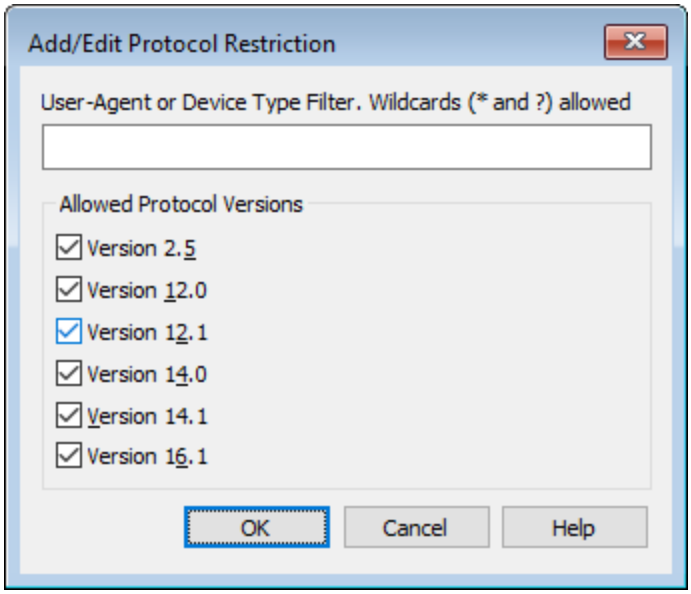
一覧からエントリを右クリックすると、以下のショートカットメニューが表示されます。:

プロトコル制限の追加
このボタンをクリックするとプロトコル制限の追加/編集[396]ダイアログが起動します。ここでプロトコル制限の作成や編集が行えます。

プロトコル制限の編集
プロトコルの制限を編集するには、対象のエントリをダブルクリックするか、右クリックで、*制限を編集する*をクリックします。 変更後、OKをクリックします。

プロトコル制限の削除
制限を削除する場合は、対象のエントリをダブルクリックするか、右クリックで*制限の削除*をクリックします。制限の削除の確認画面で、はい、をクリックして下さい。

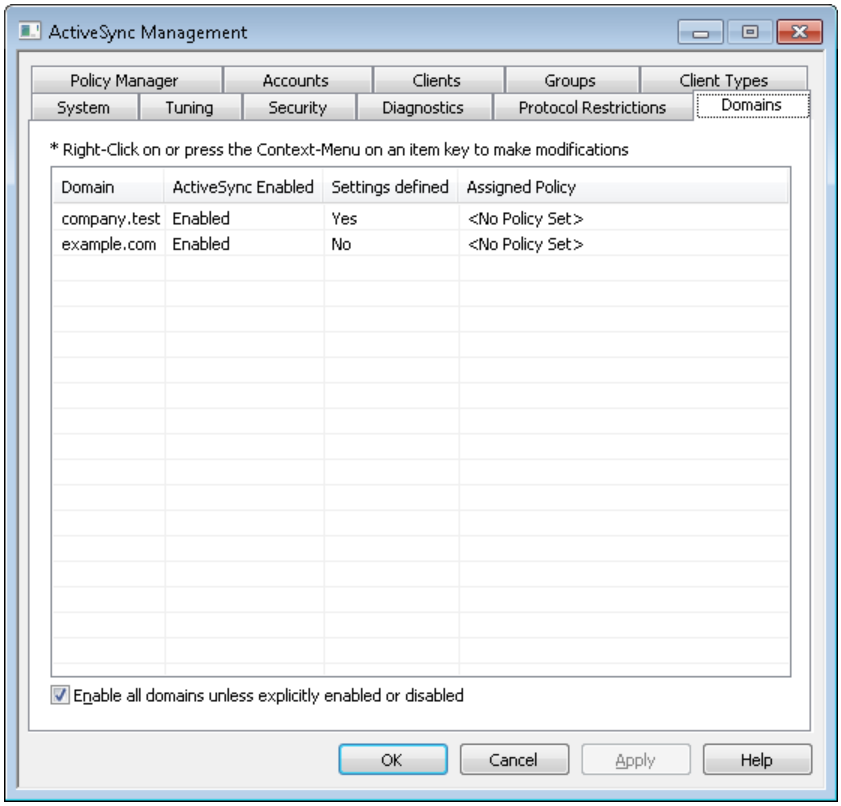
プロトコル制限の作成と編集



ユーザーエージェント又は端末種別でフィルタ
制限を行いたいユーザーエージェンやデバイスタイプを入力します。エージェントの判定にMDaemonは値の最初の"/"文字列も使用します。もしも存在しない場合は、値全てが使用されます。ユーザーエージェントやデバイスタイプの正式名称が分からない場合は、クライアントが一度MDaemon ActiveSync（MDAS）に接続した後で、クライアント[384]画面へアクセスし、対象クライアントを選択してから、詳細をクリックして下さい。MDASログファイルを直接確認する事で正式名称を把握する事もできます。

許可するプロトコルバージョン
対象デバイスやエージェントで利用できるプロトコルをチェックして下さい。対象クライアントがMDaemonに接続すると、MDaemonは選択したプロトコルを使用するようクライアントに命令を送ります。

3.10.6 ドメイン



ドメイン[165]毎のActiveSync設定を行います。ドメイン毎に、ActiveSyncの有効化/無効化、デフォルトのActiveSyncポリシー[405]適用、デフォルトのクライアント設定、ドメインに関連付けられた端末の管理が行えます。

特定のドメインでActiveSyncの有効化/無効化を行う
ドメイン毎にActiveSyncの状態を設定するには:

1. 一覧から対象ドメインを右クリックします。
2. **有効**, **無効**, **デフォルト** のどれかをクリックします。「デフォルト」を選択した場合は、以下の*明示的に有効化/無効化を設定されていない限り全てのドメインを有効化する*でActiveSyncが有効かどうかが確認されます。

ActiveSyncを有効にするにはユーザー端末のActiveSyncクライアントを正しく設定する必要があります。設定方法については、ActiveSync for MDaemonの設定 379 にある、*ActiveSync for MDaemonの購入、アップブレード購入はこちらから* のリンクをクリックし、端末の設定手順までスクロールして下さい。

ActiveSyncのデフォルトの状態を設定する

明示的に有効化/無効化を設定されていない限り全てのドメインを有効化する の設定を行う事で、ActiveSyncのデフォルト状態を設定できます。このオプションが有効の場合、全ドメインで、ActiveSyncはデフォルトで有効になります。これが無効の場合、ActiveSyncはデフォルトで無効です。ドメイン毎に有効か無効を設定すると、デフォルトの設定値を上書きします。

ドメインの*ActiveSyncを有効化* 設定を無効と変更すると、対象ドメインのユーザーによるActiveSyncアクセスを禁止するかどうかの確認画面が起動します。ActiveSyncの利用を継続しているドメインユーザーに、継続利用を許可する場合はいいえを選択してください。はいを選択すると、ActiveSyncは対象ドメインユーザー全員に対して無効化されます。

ドメインのクライアント設定の変更

ドメインを右クリックすると、ドメイン用のクライアント設定を管理できます。デフォルトでこの設定は全体クライアント設定 384 を引き継ぎます。詳細はドメインのクライアント設定を管理する 398 を参照して下さい。

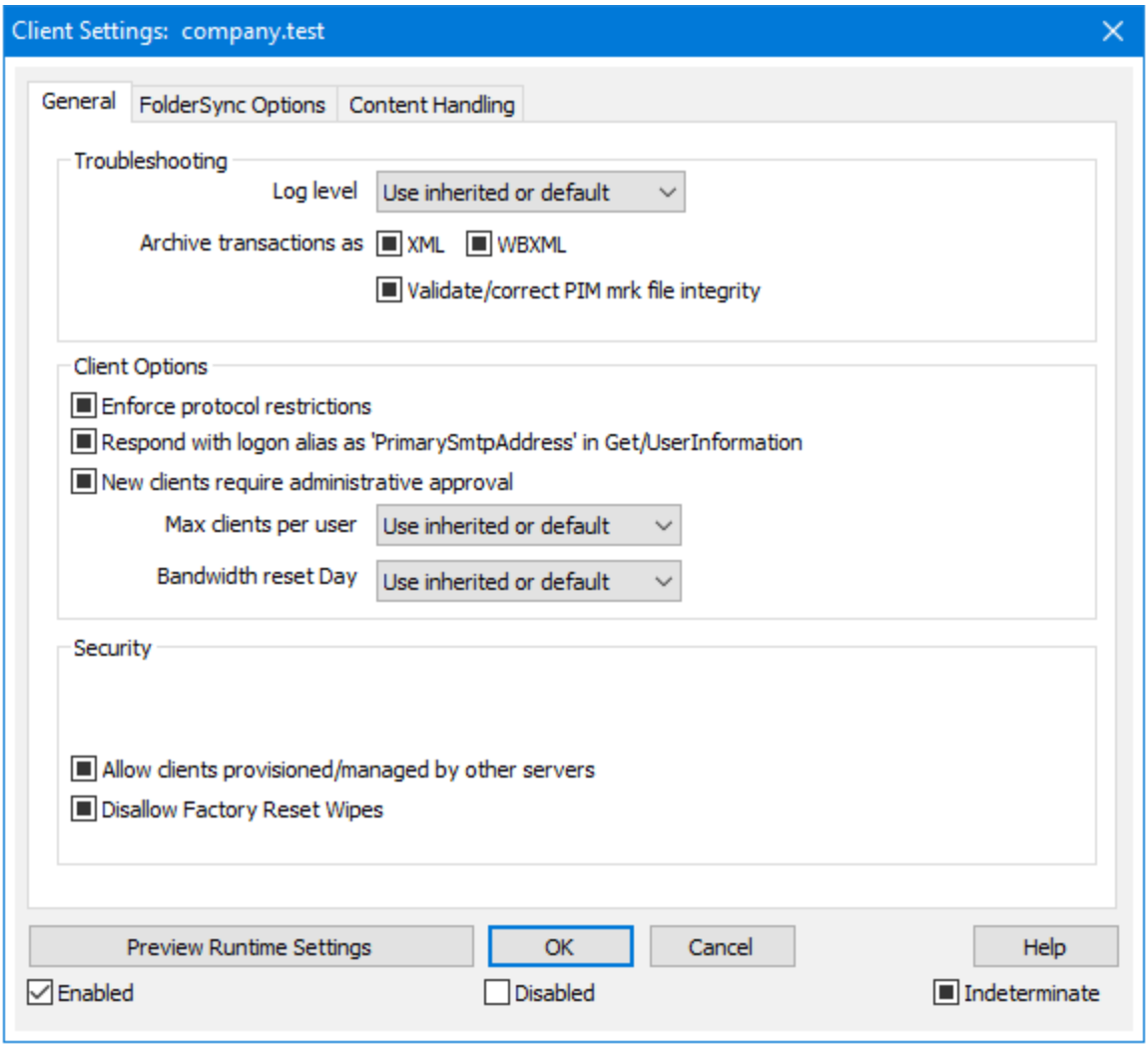
デフォルトActiveSyncポリシーの適用

ドメインへデフォルトのActiveSyncポリシーを適用するには:

1. ドメインを右クリックします。
2. **ポリシーの割り当て**をクリックします。
3. **割り当てられたポリシー**のドロップダウンリストから対象ポリシーを選択します。(利用できるポリシーの管理はポリシーマネージャ 405 で行います。)
4. **OK**をクリックします。

ドメインのクライアント設定管理

ドメインのクライアント設定画面ではドメインに関連付けられたアカウントやクライアントのデフォルト設定を管理する事ができます。



デフォルトでこの画面の全てのオプションは「継承又はデフォルト」と設定されており、各オプションがアカウントのクライアント設定[413]の関連オプションの設定を継承し、設定変更した場合はこの画面へ反映されます。同様に、ドメインのアカウント[413]設定は、この画面で行った設定を継承します。その後も、クライアントタイプは設定をアカウントレベルの設定から継承し、最終的には個々のクライアント[422]が自身の設定値を保持する事になります。この設定でドメインのアカウントとクライアント全体の設定を、この画面から設定を行うだけで変更する事ができるようになり、必要に応じて全てのアカウントやクライアント設定を上書きできるようになります。

全般

トラブルシューティング

ログレベル

ActiveSync for MDaemonはログデータ量に応じた、6つのレベルのログに対応しています。

デバッグ 最も詳細なログで、記録できる全ての情報が含まれており、問題の診断にのみ使用されます。

情報 通常のログで、一般的な操作が詳細なしで記録されます。これはデフォルトのログレベルです。

警告 警告、エラー、クリティカルエラー、起動と終了がログに記録されます。

エラー エラー、クリティカルエラー、起動と終了がログに記録されます。

クリティカル クリティカルエラー、起動と終了がログに記録されます。

なし 起動と終了だけがログに記録されます。

継承 デフォルトで、ログレベルの設定はクライアント設定の階層から継承されます。そのため、クライアントは設定をクライアントタイプから引継ぎ、クライアントタイプはアカウントから引継ぎ、アカウントはグループから引継ぎます。全体のクライアント設定は 診断 393 ダイアログのログレベル設定を元にしています。

トランスアクションを [XML | WBXML]としてアーカイブ
XMLやWBXMLデータをアーカイブするには、*XMLと WBXMLをアーカイブ...* のオプションを使用します。これはデバッグの際役立ちます。全体オプションはデフォルトで無効になっています。

PIM mrkファイルの整合性を確認する
クライアントのPIMデータの整合性テストを実施し、iCal UIDの重複や空の要求フィールドといった、同期を妨げているものがないかどうかを確認します。この全体設定はデフォルトで無効になっています。

クライアントオプション

プロトコル制限を強制する
クライアントで許可されているプロトコルバージョン以外のアクセスを拒否する場合はこのオプションを有効にします。デフォルトでこのオプションは無効になっており、プロトコル制限は異なるプロトコルのクライアントを拒否していません。プロトコル制限は単純に、クライアントに対して使用するべきプロトコルを伝えるのみの機能を提供しています。クライアントがそれでも制限されているプロトコルを使った場合、MDaemonはその接続を受け入れます。詳細は次のページをご覧下さい: プロトコル制限 395

Get/UserInformationへの応答でログオンエイリアスを'PrimarySmtpAddress' として使用する
サービスがSettings/Get/UserInformationリクエストに対する応答としてエイリアスやセカンダリアドレスをプライマリアドレスとして利用できるようにします。これはiOS 9.xへアップデートした際エイリアスからメールを送信できなくなった事に対する対処です。このオプションによって使用に反した応答を受け取る場合があります。

新しいクライアントは管理者の承認が必要
新しいクライアントがアカウントとの同期を開始する前に、管理者による承認を必要とする場合はこのオプションを有効にします。 クライアント 422 一覧で認証待ちのクライアントが確認でき、管理者は同じ画面から承認が行えます。この設定はデフォルトで無効になっています。

ユーザー毎の最大クライアント
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域リセット日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

セキュリティ

ロケーションスクリーンから除外する
ActiveSyncクライアント設定で端末をロケーションスクリーニング[520]から除外する場合はこのオプションを有効化します。これにより認証済ユーザーは、例えば認証がブロックされている場所へ出張しているような場合であっても、ActiveSync経由でアカウントへアクセスする事ができるようになります。端末を除外するためには、チューニング画面にあるこの日数を超えて認証されなかった端末を自動削除[381]設定の時間内に、ActiveSyncを使った接続と認証を行っておく必要があります。

リモートアドレスを動的に除外
接続元のリモートIPアドレスをロケーションスクリーニングの除外リストへ追加する事ができます。このオプションは、同じIPアドレスを使って接続する他のクライアントがある場合に便利です。

ユーザー毎の最大クライアント数
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域の統計情報をリセットする日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

他のサーバーで管理されているクライアントへの接続を許可する
デフォルトで、ActiveSyncサーバーが特定のクライアントへデータやポリシーを送信する際、対象クライアントが他のActiveSyncサーバーからも管理されている事が分かった場合も、クライアントはMDaemonへアクセスする事ができます。しかし、このような環境の場合、適用するポリシーが他のActiveSyncサーバーと競合する可能性があります。一般的に、クライアントはポリシーが競合した場合、厳しい方へ合わせる傾向があります。こうしたクライアントからの接続を制限する場合は、このオプションを無効化して下さい。

工場出荷時への完全ワイプを無効化
オン/はい、を設定すると、ActiveSyncクライアントの完全ワイプが行えなくなります。クライアントでリ

モートからの完全ワイプを許可する場合、最初にこのオプションを無効化して下さい。このオプションはデフォルトで無効に設定されています。クライアントページの次の項目を参照して下さい: ActiveSyncクライアントの完全ワイプ 422

フォルダ同期オプション

フォルダ同期オプション

除外

ユーザの [許可リスト/ブロックリスト] フォルダ
デフォルトでユーザーの許可リストとブロックリストの連絡先フォルダは端末と同期を行いません。これらはMDaemonがスパムからシステムを自動的に保護するのを支援する目的で使用されます。そのため、許可リストやブロックリストは端末上に連絡先として表示する必要性はありません。

デフォルト以外のメールフォルダ
デフォルトで、ユーザーが作成したメールフォルダとデフォルトメールフォルダは全て端末と同期します。同期するのを受信箱や送信箱、削除済アイテム、下書き、といった、デフォルトのメールフォルダのみにしたい場合はこのオプションを有効にして下さい。ユーザーが作成したフォルダは同期対象に含まれません。 このオプションはデフォルトで無効になっています。

デフォルト以外のPIMフォルダ
デフォルトで、(連絡先、予定表、仕事などの) PIMフォルダは全て端末と同期します。同期するのをデフォルトのPIMフォルダのみにしたい場合はこのオプションを有効にして下さい。このオプションが有効な場合で、ユーザーが複数の予定表を保有してる場合デフォルトの予定表のみが同期対象となります。 このオプションはデフォルトで無効になっています。

含む

パブリックフォルダの階層
ユーザーがアクセス権を持っている パブリックフォルダ 283 をユーザーのActiveSync用端末のフォルダー覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
パブリックフォルダ 283 をユーザーが検索できるようになります。 これはデフォルトで許可されています。

パブリックフォルダの横断 (フォルダ名の公開)
デフォルトで、クライアントがパブリックのサブフォルダへのアクセスや同期を行うには、サブフォルダと上位のパブリックフォルダ 283 全てに対してルックアップ権限 285 が必要です。上位のフォルダに対するアクセス権がない場合、その中のサブフォルダに対しては、例え設定上は許可されていても、アクセスする事はできません。クライアントからこうしたサブフォルダへアクセスできるようにする場合は、このオプションを有効にします。注意点: このオプションを有効化すると、上位のフォルダもクライアントへ許可する事となり、セキュリティのリスクを招く恐れがあります。 このオプションはデフォルトで無効になっています。

許可するパブリックフォルダの最大数
端末で処理するパブリックフォルダ数を制限する場合はこのオプションを使用します。制限が設

定されると、サーバーは最大数に到達するまでフォルダー一覧を処理し、これを超えるとその後のデータを送りません。処理するフォルダの順番を決める事はできません。デフォルトで、全体での最大数は設定されていません。

共有フォルダも含める

ユーザーがアクセス権を持っている共有フォルダ[107]をユーザーのActiveSync用端末のフォルダー一覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
共有フォルダ[676]をユーザーが検索できるようになります。これはデフォルトで許可されています。

コンテンツ処理

コンテンツ処理オプション

クライアントにフラグ付けされたメール用にタスク・リマインダーを作成
このオプションでMDaemonはフラグが付いたアイテムごとに仕事を作成し、リマインダーをユーザーへ送信できるようになります。この設定の全体値はデフォルトで有効です。

予定を編集した際、常にミーティングのアップデートを送信
クライアントの中には、ミーティングを編集した際、更新情報を適切に送信しないものもあります。このオプションを使うとActiveSyncサービスへ、ミーティングが開催者によって更新された際、更新情報を送信するよう促す事ができるようになります。これはミーティングの更新情報の送信に失敗しているクライアント[422]やクライアントタイプ[438]に限定して使用するべきで、更新情報が重複して送られてしまう可能性があります。また、このオプションはクライアントとクライアントタイプの設定ページでのみ利用できます。

全ての送信メールで開封確認を要求
クライアントから送信される全てのメールで開封確認要求を行うにはこのオプションを有効にして下さい。これはデフォルトで無効になっています。

送信者からリクエストされた際送信済メールについて開封確認を送信
サーバー側で開封確認要求を検出し、既読フラグがついたメールの開封通知を送信するにはこのオプションを使用します。これはデフォルトで無効になっています。

ReplyToアドレスに指定したエイリアスとして送る
クライアントによっては、エイリアスを使ったメール送信を許可していません。この機能はExchange ActiveSync（EAS）プロトコル[395]16.xで追加されたものですが、クライアントの中には16.xに対応していないものもあります。例えば、Windows用OutlookはEAS 14.0だけを使用しており、ユーザーが関連するアドレスを指定して送信する事のみ許可しており、生成されたメールはユーザーの選択を正しく反映していません。このオプションでは、ReplyToのアドレスがユーザー用の正しいエイリアス[757]であれば、これを使ってメール送信を行います。この設定の全体値はデフォルトで有効です。

デフォルトの連絡先にパブリック連絡先を仮想的に統合する
パブリック連絡先をユーザーの端末上でデフォルトの連絡先と統合したい場合はこのオプションを有効にします。これは仮想的な統合で、実際には連絡先フォルダへデータのコピーは行っていません。

これはグローバルアドレス帳（GAL）の検索機能に対応していないクライアントにとって便利な機能です。これはデフォルトで無効になっています。

Junk-Emailフォルダへ移動したメールの送信者をブロックする
有効にすると、クライアントが特定のメールを自分のJunk Emailフォルダへ移動した際、対象のメール送信者がブロックされた送信者連絡先フォルダへ追加されます。

ミーティング要求が許可/拒否された際、ミーティング要求に対する応答の送信を強制的に行う
このオプションを使用すると、クライアントがミーティング要求に対して、許可や拒否、その他のアクションを選択した際、ミーティング要求に対する応答を開催者へ送信します。これは、こうした更新情報を自動送信する事ができない特定のクライアント用の機能です。

有効な設定をプレビュー

このボタンは全てのクライアント設定（ドメイン397, アカウント413, クライアント422）に対して使用できます。画面のオプションはデフォルト値をその上位の画面から引き継いでいるため、この機能は表示されている画面の現在の設定確認を行う際にもご利用頂けます。

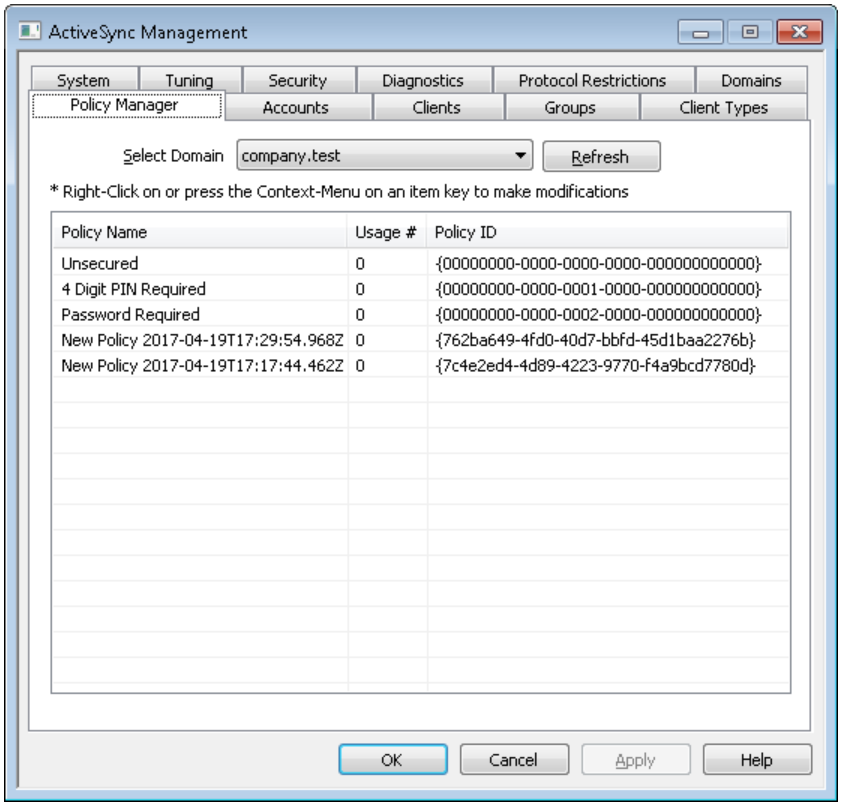
参照:

ドメインマネージャ ≫ ActiveSync クライアント設定196
ドメインマネージャ ≫ ActiveSyncクライアント220
ActiveSync ≫ ポリシーマネージャ405

参照:

ドメインマネージャ ≫ ActiveSync クライアント設定196
ドメインマネージャ ≫ ActiveSyncクライアント220
ActiveSync ≫ ポリシーマネージャ405
ActiveSync ≫ クライアント422

3.10.7 ポリシーマネージャ



ここではユーザーのデバイスに適用するActivSyncポリシーに関する様々な設定を行います。定義済ポリシーが提供されており、独自のポリシーの作成や編集、削除もここで行えます。デフォルトポリシーはドメイン毎 397 や アカウント毎 413 に適用され、特定のクライアント 220 へも適用できます。

全てのActiveSyncデバイスがポリシーを常に認識したり適用したりできるわけではありません。ポリシー又は同時に適用された特定のポリシーを無視する場合や、変更を適用するのにデバイスの再起動が必要となる場合があります。また、新しいポリシーをデバイスに適用しても、デバイスへ実際にポリシーが適用されるのは次にActiveSyncサーバーへ接続したタイミングとなります。ポリシーはデバイス側から接続するまで、「プッシュ」配信は行われません。

ActiveSyncポリシー

一覧を右クリックすると次のオプションへのショートカットメニューが表示されます。

ポリシーの作成
このボタンでActiveSyncポリシーエディタを起動し、ポリシーの作成や編集が行えます。

削除
ポリシーの削除を行うには、カスタマイズしたポリシーを一覧から右クリックし、削除をクリックします。確認画面ではいをクリックします。用意されているポリシーは削除できません。

ポリシーの編集
ポリシーを編集するには、カスタマイズしたポリシーを一覧から右クリックし、編集ボタンをクリックします。変更を行ったら、OKボタンをクリックします。用意されているポリシーは編集できません。

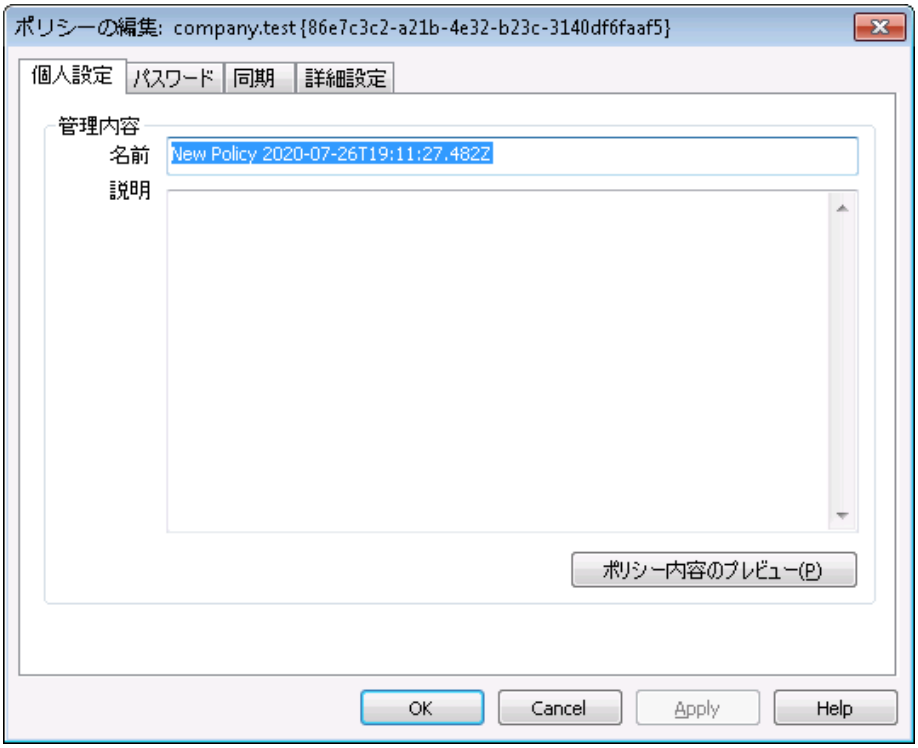
ポリシー使用状況の表示
ポリシーを右クリックしこのボタンをクリックすると、このポリシーを適用しているドメイン、アカウント、クライアントの一覧を表示できます。I

ActiveSyncポリシーエディタ

ActiveSyncポリシーエディタには個人設定、パスワード、同期、詳細設定の4つのタブがあります。この詳細設定タブはActiveSyncシステム場面の*詳細ポリシーオプションの変更を有効にする*379をアクティブにするまで非表示になっています。

個人設定

ポリシーの名称と説明を設定します。XMLポリシー文書のプレビューも行えます。



管理内容

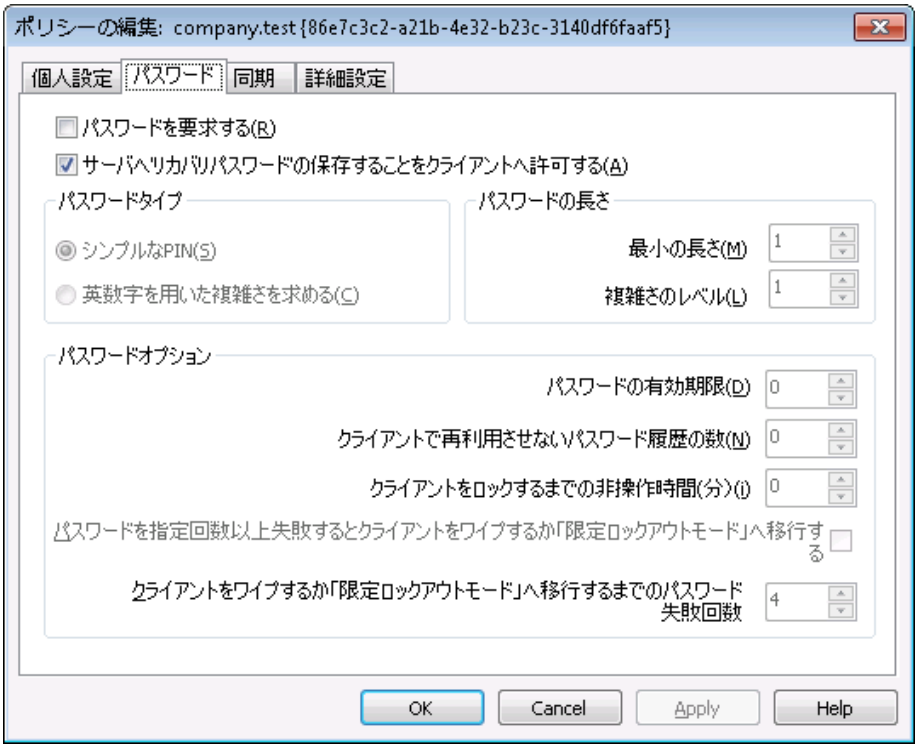
名前
カスタムポリシー名称を指定します。

説明
カスタムポリシーの説明を入力します。ここでの説明はドメイン、アカウント、クライアントへ適用するポリシーの選択の際使用します。

ポリシー内容のプレビュー
ポリシー用のXMLドキュメントのプレビューにこのボタンを使用します。

パスワード

ポリシー用のパスワードオプションと要求設定にこのタブを使用します。



パスワードを要求する
端末でパスワードを要求するにはこのボックスを有効にします。これはデフォルトで無効に設定されています。

サーバで「リカバリーパスワード」の保存を許可するデバイス

クライアントがActiveSyncのリカバリーパスワードオプションを利用できるようにするにはこのオプションを有効にします。端末は一時的なリカバリーパスワードをサーバーへ保存しておく事ができ、パスワードを忘れた場合にこれを使って解除できます。管理者はクライアントの詳細設定 422でこのパスワードを確認できます。多くの端末ではこの機能に未対応です。

パスワードタイプ

シンプルなPIN
このオプションの実装方法は端末により異なりますが、シンプルなPINをパスワードタイプとして選択した場合、一般的には最少の長さ以外の規定や複雑さのレベルを求められる事はありません。次のようなシンプルなパスワードが利用できます: "111", "aaa", "1234", "ABCD"

英数字を用いた複雑さを求める
シンプルなPINよりも複雑で安全なパスワードを要求する場合はこのポリシーオプションを使用します。複雑さのレベルでは具体的にパスワードの複雑さのレベルを指定します。これはポリシーでパスワードを要求した場合のデフォルト設定です。

パスワードの長さ

最少の長さ
デバイスパスワードの最少文字数を1-16の間で設定するのに使用します。デフォルトでは1に設定されています。

複雑さのレベル
英数字を用いた複雑さの内、複雑さのレベルを指定します。レベルはパスワードに含む必要のある文字列の種類の数で、大文字、小文字、数字、(記号など)英数字以外の文字、の1-4で指定します。例えば、オプションが2と設定されている場合、パスワードには、大文字と小文字、数字と記号、といった、最低2種類の文字列が必要です。このオプションはデフォルトで1に設定されています。

パスワードオプション

パスワードの有効期限
デバイスパスワードを変更するまでの日数を指定します。これはデフォルトで無効(0を指定)に設定されています。

デバイスで再利用させないパスワードの数
古いパスワードの再利用を禁止する履歴の数を指定します。例えば、このオプションが2と設定されていた場合、デバイスのパスワードを変更する際、過去に使った2回前のパスワードまでは再利用できません。これはデフォルトで無効(0を指定)に設定されています。

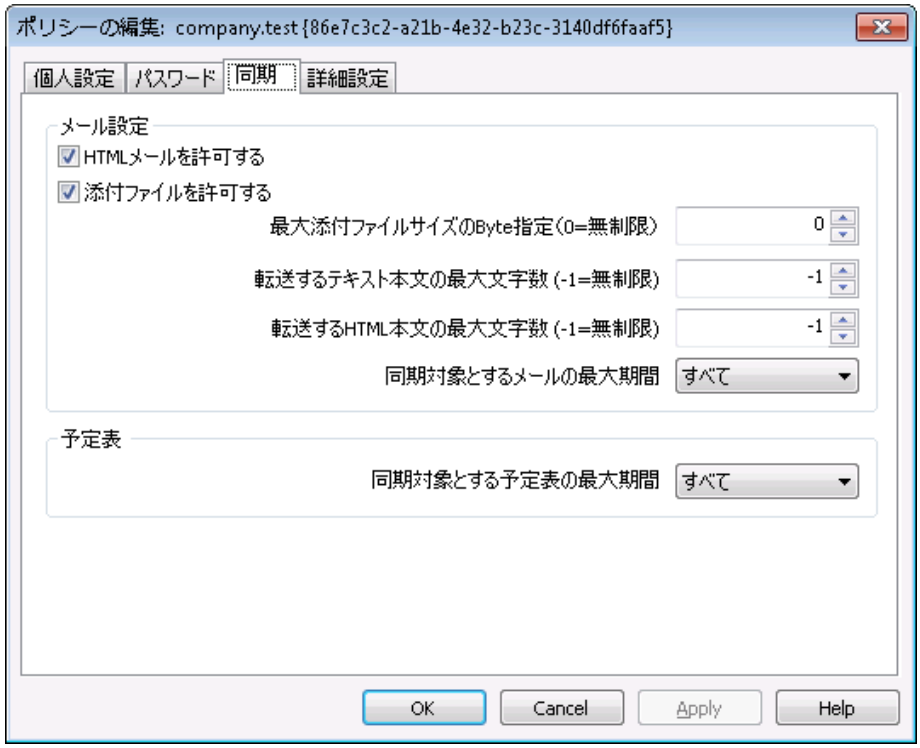
デバイスをロックするまでの非操作期間(分)
端末がロックされるまでの非操作時間を分で指定します。このオプションはデフォルトで無効(0を指定)に設定されています。

連続した認証失敗時端末初期化又はロックアウトモードへの移行
このオプションが有効で、指定した回数パスワード認証に失敗した場合、端末はロックされるか全てのデータが初期化されます。このオプションはデフォルトで無効になっています。

端末初期化又はロックアウトモードへ移行するまでのパスワード入力失敗回数
「デバイスを初期化」が有効で、指定した回数ユーザーがパスワード認証へ失敗した場合、端末の設定によって、端末は初期化されるか、「ロックアウトモード」を開始します。

同期

この画面ではHTMLメールの設定や、添付ファイルの許可、転送する文字数の制限、予定表の同期対象期間の設定が行えます。



メール設定

HTMLメールを許可する

デフォルトでHTML形式のメールはActiveSyncクライアントと同期したり、ActiveSyncクライアントへ送信されます。このチェックをオフにすると、プレインテキスト形式のメールのみが送信されます。

添付ファイルを許可する

デバイスが添付ファイルをダウンロードできるようになります。このオプションはデフォルトで有効です。

最大添付ファイルサイズbytes指定(0=無制限)

デバイスで自動ダウンロードできる添付ファイルの最大サイズを指定します。デフォルトでサイズの制限はありません(0に設定されています)。

転送するテキスト本文の最大文字数(-1=無制限)

クライアントに送信されるプレインテキストメールの本文の最大文字数を指定します。本文に指定した数を超える文字数が使用された場合、本文は最大文字数で短縮されます。デフォルトでこの値は無制限(-1に設定)されています。この値を0にすると、メッセージヘッダのみが送信されます。

転送するHTML本文の最大文字数(-1=無制限)

クライアントに送信されるHTMLメールの本文の最大文字数を指定します。本文に指定した数を超える文字数が使用された場合、本文は最大文字数で短縮されます。デフォルトでこの値は無制限(-1に設定)されています。この値を0にすると、メッセージヘッダのみが送信されます。

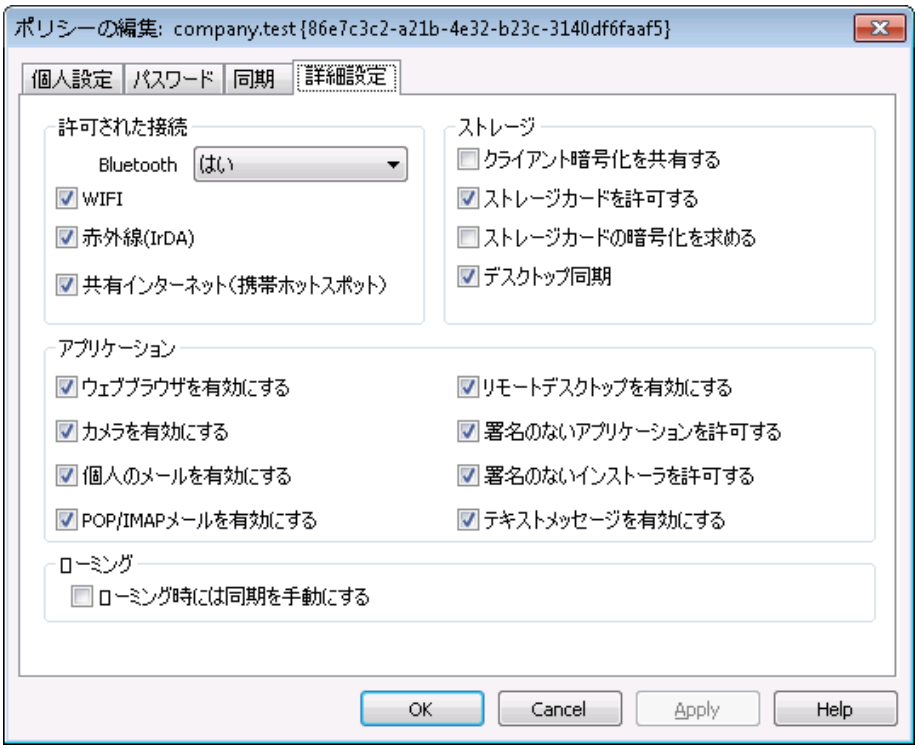
同期対象とするメールの最大期間
最大日数分前の日付から今日までのメールが、デバイスとの同期対象となります。デフォルトでは「全て」に設定されており、メールは配信日時に関わらず全て同期対象となります。

予定表

同期対象となる予定表の最大期間
今日から何日前までの予定表をデバイスとの同期対象とするかをここで指定します。デフォルトでは「全て」に設定されており、予定は日時に関わらず全て同期対象となります。

詳細設定

詳細設定タブでは許可する接続の種類、特定のアプリケーションの許可、ストレージと暗号化、ローミングの設定が行えます。



この詳細設定タブはActiveSyncfor MDaemon 場面の*詳細ポリシーオプションの変更を有効にする*[379]をアクティブにするまで非表示になっています。

許可された接続

Bluetooth
端末へのBluetooth接続を許可するかどうかを指定します。はい、でBluetooth接続を許可し、いいえ、で拒否、ハンズフリーでBluetoothをハンズフリーの場合のみに制限します。このオプションはデフォルトで、はい、に設定されています。

WIFI
WIFI接続を許可します。デフォルトで有効です。

赤外線（IrDA）
赤外線（IrDA）接続を許可します。デフォルトで有効です。

共有インターネット（携帯ホットスポット）
デバイスによる共有インターネット（ホットスポット）の利用を許可します。これはデフォルトで有効です。

ストレージ

デバイスの暗号化を要求する
デバイスの暗号化を要求する場合はこのオプションを有効にします。全てのデバイスが暗号化の要求に対応しているわけではありません。これはデフォルトで無効になっています。

ストレージカードを許可する
デバイスでのストレージカードの利用を許可します。これはデフォルトで有効です。

ストレージカードの暗号化を求める
ストレージカードの暗号化を要求する場合にこのオプションを使用します。これはデフォルトで無効になっています。

デスクトップ同期
デバイスでデスクトップActiveSyncを許可します。デフォルトで有効です。

アプリケーション

ウェブブラウザを有効にする
デバイスでブラウザの利用を許可します。このオプションはデバイスによって未対応の場合があり、3rdパーティー製のブラウザには適用できない場合があります。デフォルトで有効です。

カメラを有効にする
デバイスでのカメラの利用を許可します。デフォルトで有効です。

個人のメールを有効にする
デバイスで個人用メールアカウントの設定を許可します。無効になっている場合、ActiveSync端末毎にメールアカウントやサービスが接続不可となります。これはデフォルトで有効です。

POP/IMAPメールを有効にする
POPやIMAPメールへのアクセスを許可します。デフォルトで有効です。

リモートデスクトップを有効にする

リモートデスクトップの利用を許可します。デフォルトで有効です。

署名のないアプリケーションを許可する
デバイスで未署名のアプリケーションの利用を許可します。これはデフォルトで有効です。

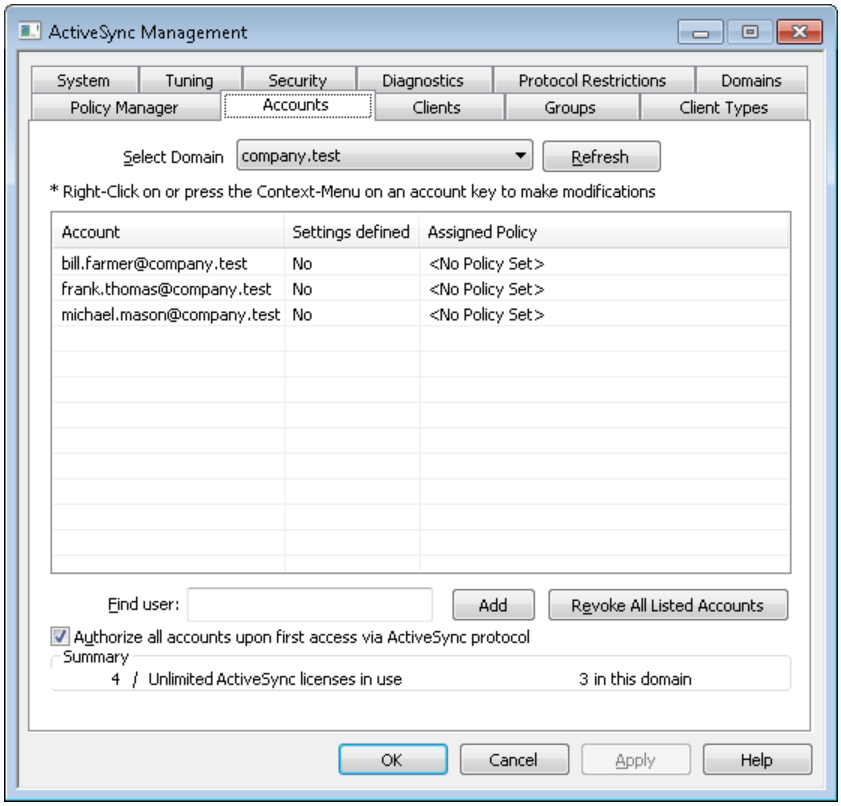
署名のないインストーラを許可する
デバイスで未署名のインストーラの実行を許可します。これはデフォルトで有効です。

テキストメッセージを有効にする
デバイスでテキストメッセージを許可します。これはデフォルトで有効です。

ローミング

ローミング中には同期を手動にする
ローミング中にはデバイスとの同期を手動で行わせるようにする場合はこのポリシーオプションを使用します。ローミング中の自動同期を行うと、キャリアや契約内容によって、データの転送コストが上がってしまう場合があります。このオプションはデフォルトで無効になっています。

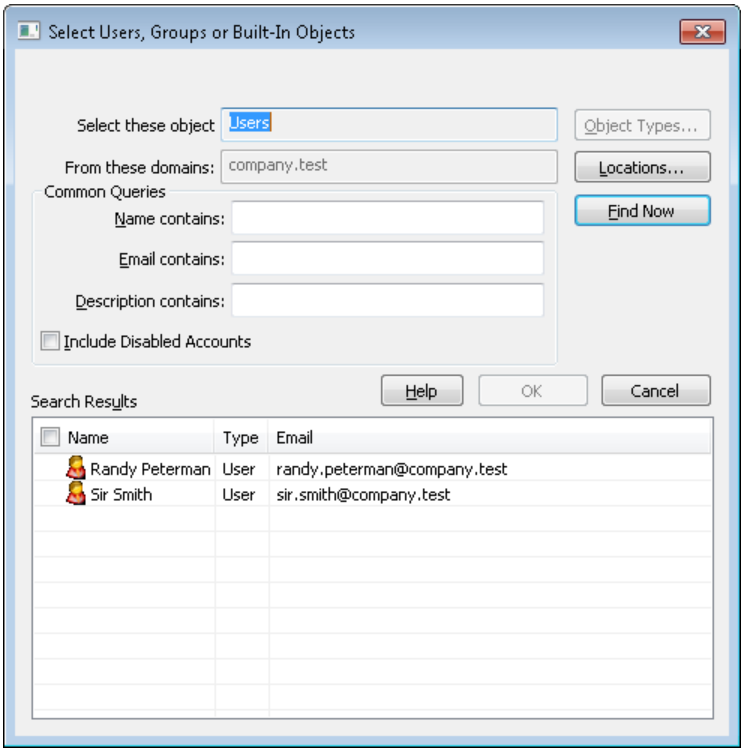
3.10.8 アカウント



この画面ではActiveSyncを利用するアカウントの指定を行います。手動でアカウントの追加や削除を行ったり、アカウントがActiveSyncで接続してきたタイミングで、自動で利用を許可するようMDaemonへ設定する事ができます。

手動でのアカウント承認

アカウント画面で、ドメインを選択のドロップダウンリストから対象ドメインを選択し、追加をクリックする事で、手動でアカウントのActiveSync利用を許可できます。この操作でユーザー選択ダイアログが起動し、アカウントの検索と選択が行えます。



ドメイン
アカウント画面のドメイン選択で選択したドメインの一覧です。ドメイン内のユーザーを検索できます。

共通クエリ
このセクションにあるオプションで検索結果をユーザー名やメールアドレス、アカウントのコメント 650 で絞り込む事ができます。ドメインユーザー全員を表示させるには、ここでのオプション欄はブランクにして下さい。

無効化されたアカウントも含む
無効化されたアカウント 650 を検索対象にする場合はこのオプションを有効にします。

今すぐ検索
検索条件の設定を行ったら、今すぐ検索で検索を実行します。

検索結果
検索実行後、対象ユーザーを検索結果から選択し、OKをクリックすると、対象アカウントが追加されます。

アカウントの利用権限を取り消す

アカウントの利用権限を取り消すには、アカウントを右クリックし、ActiveSync利用権限を取り消す、をクリックします。全てのアカウントの利用権限を取り消すには、全てのアカウントの利用権限を取り消す、のボタンをクリックします。

*ActiveSyncプロトコルを使った最初のアクセス時にアカウントを許可する*のオプションを有効にしていた場合、アカウントを取り消す、のオプションで一覧から削除されたアカウントは、次回の接続で再度利用権限が与えられます。

ActiveSyncプロトコルを使った最初のアクセス時にアカウントを許可する

このチェックを有効にすると、アカウントがActiveSyncを使ってMDaemonに接続した際、自動的に利用許可が与えられます。

ActiveSyncポリシーの適用

アカウントにポリシー[405]を適用するには:

1. アカウントを一覧から右クリックします。
2. **ポリシーの割り当て**をクリックします。
3. **割り当てられたポリシー**のドロップダウンリストから対象ポリシーを選択します。(利用できるポリシーの管理はポリシーマネージャ[405]で行います。)
4. **OK**をクリックします。

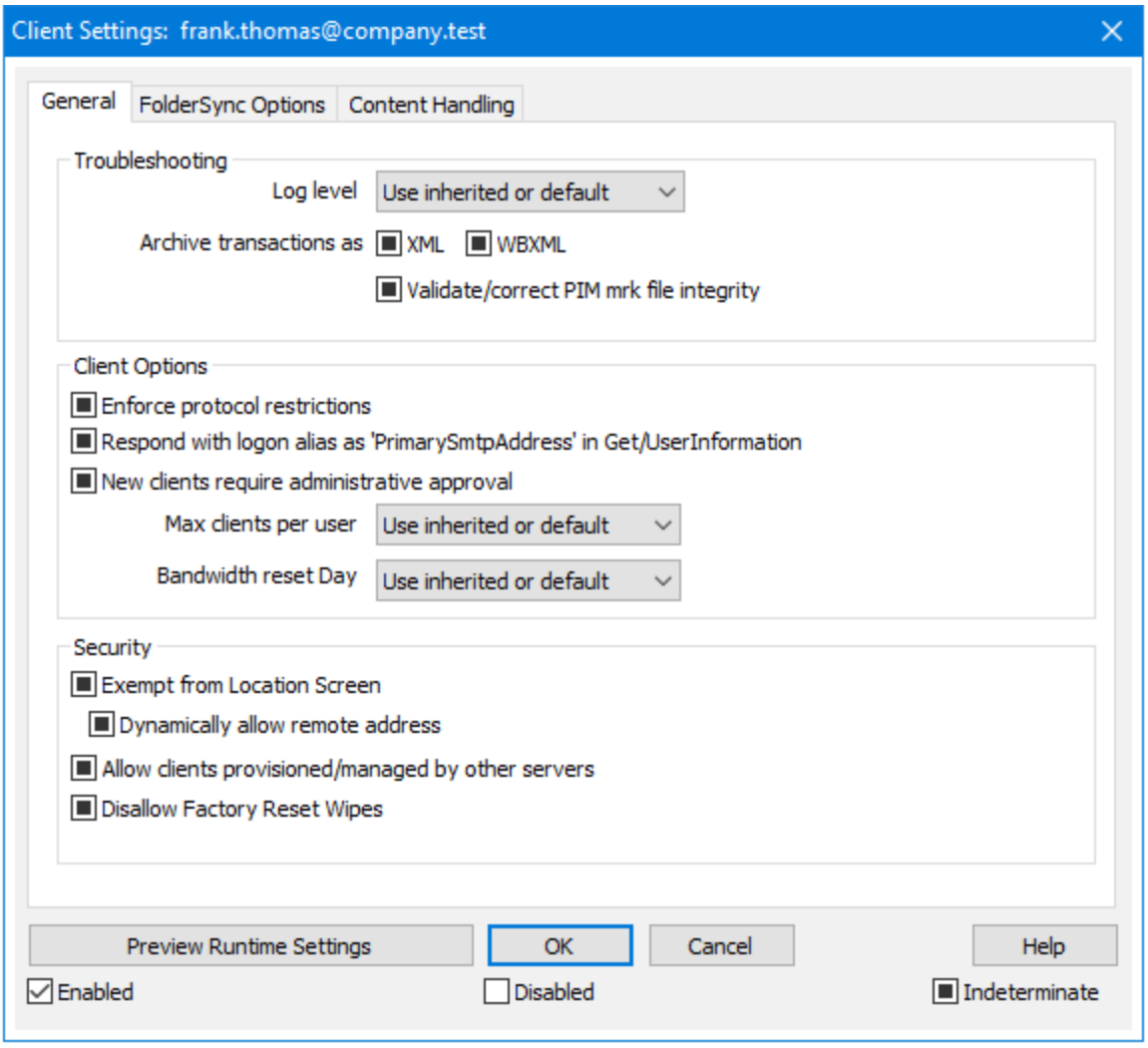
このポリシーはアカウント用の新しい端末全てに適用されます。

使用を許可されたアカウントの一覧検索

ActiveSyncの利用を大勢のアカウントに許可している場合は、ユーザー検索を使って、一覧からユーザー検索を行う事ができます。アカウントのメールアドレスの内、先頭の数文字を入力するだけで、ユーザーの絞り込みが行えます。

アカウントクライアント設定

アカウントを右クリックしてクライアント設定のカスタマイズをクリックし アカウントのクライアント設定が行えます。設定はアカウントへ接続するActiveSyncクライアントへ適用されます。



デフォルトでこの画面の全てのオプションは「継承又はデフォルト」となります。つまり、アカウントがグループ[384]に所属していた場合、オプション設定はグループのクライアント設定の値を引き継ぎます。アカウントがグループメンバーでない場合は、グループ用のクライアント設定が存在しない場合、各オプションの値はドメインのクライアント設定[196]の値を継承します。ドメインのクライアント設定画面で行った変更は、この画面の値へ反映されます。同様に、この画面で行った設定は、アカウントのグループレベル又はドメインレベルの設定を上書きします。

全般

トラブルシューティング

ログレベル

ActiveSync for MDaemonはログデータ量に応じた、6つのレベルのログに対応しています。

デバッグ 最も詳細なログで、記録できる全ての情報が含まれており、問題の診断にのみ使用されます。

情報 通常のログで、一般的な操作が詳細なしで記録されます。これはデフォルトのログレベルです。

警告 警告、エラー、クリティカルエラー、起動と終了がログに記録されます。

エラー エラー、クリティカルエラー、起動と終了がログに記録されます。

クリティカル クリティカルエラー、起動と終了がログに記録されます。

なし 起動と終了だけがログに記録されます。

継承 デフォルトで、ログレベルの設定はクライアント設定の階層から継承されます。そのため、クライアントは設定をクライアントタイプから引継ぎ、クライアントタイプはアカウントから引継ぎ、アカウントはグループから引継ぎます。全体のクライアント設定は 診断 393 ダイアログのログレベル設定を元にしています。

トランスアクションを [XML | WBXML]としてアーカイブ
XMLやWBXMLデータをアーカイブするには、*XMLと WBXMLをアーカイブ...* のオプションを使用します。これはデバッグの際役立ちます。全体オプションはデフォルトで無効になっています。

PIM mrkファイルの整合性を確認する
クライアントのPIMデータの整合性テストを実施し、iCal UIDの重複や空の要求フィールドといった、同期を妨げているものがないかどうかを確認します。この全体設定はデフォルトで無効になっています。

クライアントオプション

プロトコル制限を強制する
クライアントで許可されているプロトコルバージョン以外のアクセスを拒否する場合はこのオプションを有効にします。デフォルトでこのオプションは無効になっており、プロトコル制限は異なるプロトコルのクライアントを拒否していません。プロトコル制限は単純に、クライアントに対して使用するべきプロトコルを伝えるのみの機能を提供しています。クライアントがそれでも制限されているプロトコルを使った場合、MDaemonはその接続を受け入れます。詳細は次のページをご覧下さい: プロトコル制限 395

Get/UserInformationへの応答でログオンエイリアスを'PrimarySmtpAddress' として使用する
サービスがSettings/Get/UserInformationリクエストに対する応答としてエイリアスやセカンダリアドレスをプライマリアドレスとして利用できるようにします。これはiOS 9.xへアップデートした際エイリアスからメールを送信できなくなった事に対する対処です。このオプションによって使用に反した応答を受け取る場合があります。

新しいクライアントは管理者の承認が必要
新しいクライアントがアカウントとの同期を開始する前に、管理者による承認を必要とする場合はこのオプションを有効にします。 クライアント 422 一覧で認証待ちのクライアントが確認でき、管理者は同じ画面から承認が行えます。この設定はデフォルトで無効になっています。

ユーザー毎の最大クライアント
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域リセット日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

セキュリティ

ロケーションスクリーンから除外する
ActiveSyncクライアント設定で端末をロケーションスクリーニング[520]から除外する場合はこのオプションを有効化します。これにより認証済ユーザーは、例えば認証がブロックされている場所へ出張しているような場合であっても、ActiveSync経由でアカウントへアクセスする事ができるようになります。端末を除外するためには、チューニング画面にあるこの日数を超えて認証されなかった端末を自動削除[381]設定の時間内に、ActiveSyncを使った接続と認証を行っておく必要があります。

リモートアドレスを動的に除外
接続元のリモートIPアドレスをロケーションスクリーニングの除外リストへ追加する事ができます。このオプションは、同じIPアドレスを使って接続する他のクライアントがある場合に便利です。

ユーザー毎の最大クライアント数
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域の統計情報をリセットする日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

他のサーバーで管理されているクライアントへの接続を許可する
デフォルトで、ActiveSyncサーバーが特定のクライアントへデータやポリシーを送信する際、対象クライアントが他のActiveSyncサーバーからも管理されている事が分かった場合も、クライアントはMDaemonへアクセスする事ができます。しかし、このような環境の場合、適用するポリシーが他のActiveSyncサーバーと競合する可能性があります。一般的に、クライアントはポリシーが競合した場合、厳しい方へ合わせる傾向があります。こうしたクライアントからの接続を制限する場合は、このオプションを無効化して下さい。

工場出荷時への完全ワイプを無効化
オン/はい、を設定すると、ActiveSyncクライアントの完全ワイプが行えなくなります。クライアントでリ

モートからの完全ワイプを許可する場合、最初にこのオプションを無効化して下さい。このオプションはデフォルトで無効に設定されています。クライアントページの次の項目を参照して下さい: ActiveSyncクライアントの完全ワイプ 422

フォルダ同期オプション

フォルダ同期オプション

除外

ユーザの [許可リスト/ブロックリスト] フォルダ
デフォルトでユーザーの許可リストとブロックリストの連絡先フォルダは端末と同期を行いません。これらはMDaemonがスパムからシステムを自動的に保護するのを支援する目的で使用されます。そのため、許可リストやブロックリストは端末上に連絡先として表示する必要性はありません。

デフォルト以外のメールフォルダ
デフォルトで、ユーザーが作成したメールフォルダとデフォルトメールフォルダは全て端末と同期します。同期するのを受信箱や送信箱、削除済アイテム、下書き、といった、デフォルトのメールフォルダのみにしたい場合はこのオプションを有効にして下さい。ユーザーが作成したフォルダは同期対象に含まれません。 このオプションはデフォルトで無効になっています。

デフォルト以外のPIMフォルダ
デフォルトで、(連絡先、予定表、仕事などの) PIMフォルダは全て端末と同期します。同期するのをデフォルトのPIMフォルダのみにしたい場合はこのオプションを有効にして下さい。このオプションが有効な場合で、ユーザーが複数の予定表を保有してる場合デフォルトの予定表のみが同期対象となります。 このオプションはデフォルトで無効になっています。

含む

パブリックフォルダの階層
ユーザーがアクセス権を持っている パブリックフォルダ 283 をユーザーのActiveSync用端末のフォルダー覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
パブリックフォルダ 283 をユーザーが検索できるようになります。 これはデフォルトで許可されています。

パブリックフォルダの横断 (フォルダ名の公開)
デフォルトで、クライアントがパブリックのサブフォルダへのアクセスや同期を行うには、サブフォルダと上位のパブリックフォルダ 283 全てに対してルックアップ権限 285 が必要です。上位のフォルダに対するアクセス権がない場合、その中のサブフォルダに対しては、例え設定上は許可されていても、アクセスする事はできません。クライアントからこうしたサブフォルダへアクセスできるようにする場合は、このオプションを有効にします。注意点: このオプションを有効化すると、上位のフォルダもクライアントへ許可する事となり、セキュリティのリスクを招く恐れがあります。 このオプションはデフォルトで無効になっています。

許可するパブリックフォルダの最大数
端末で処理するパブリックフォルダ数を制限する場合はこのオプションを使用します。制限が設

定されると、サーバーは最大数に到達するまでフォルダー一覧を処理し、これを超えるとその後のデータを送りません。処理するフォルダの順番を決める事はできません。デフォルトで、全体での最大数は設定されていません。

共有フォルダも含める

ユーザーがアクセス権を持っている共有フォルダ[107]をユーザーのActiveSync用端末のフォルダー一覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
共有フォルダ[676]をユーザーが検索できるようになります。これはデフォルトで許可されています。

コンテンツ処理

コンテンツ処理オプション

クライアントにフラグ付けされたメール用にタスク・リマインダーを作成
このオプションでMDaemonはフラグが付いたアイテムごとに仕事を作成し、リマインダーをユーザーへ送信できるようになります。この設定の全体値はデフォルトで有効です。

予定を編集した際、常にミーティングのアップデートを送信
クライアントの中には、ミーティングを編集した際、更新情報を適切に送信しないものもあります。このオプションを使うとActiveSyncサービスへ、ミーティングが開催者によって更新された際、更新情報を送信するよう促す事ができるようになります。これはミーティングの更新情報の送信に失敗しているクライアント[422]やクライアントタイプ[438]に限定して使用するべきで、更新情報が重複して送られてしまう可能性があります。また、このオプションはクライアントとクライアントタイプの設定ページでのみ利用できます。

全ての送信メールで開封確認を要求
クライアントから送信される全てのメールで開封確認要求を行うにはこのオプションを有効にして下さい。これはデフォルトで無効になっています。

送信者からリクエストされた際送信済メールについて開封確認を送信
サーバー側で開封確認要求を検出し、既読フラグがついたメールの開封通知を送信するにはこのオプションを使用します。これはデフォルトで無効になっています。

ReplyToアドレスに指定したエイリアスとして送る
クライアントによっては、エイリアスを使ったメール送信を許可していません。この機能はExchange ActiveSync（EAS）プロトコル[395]16.xで追加されたものですが、クライアントの中には16.xに対応していないものもあります。例えば、Windows用OutlookはEAS 14.0だけを使用しており、ユーザーが関連するアドレスを指定して送信する事のみ許可しており、生成されたメールはユーザーの選択を正しく反映していません。このオプションでは、ReplyToのアドレスがユーザー用の正しいエイリアス[757]であれば、これを使ってメール送信を行います。この設定の全体値はデフォルトで有効です。

デフォルトの連絡先にパブリック連絡先を仮想的に統合する
パブリック連絡先をユーザーの端末上でデフォルトの連絡先と統合したい場合はこのオプションを有効にします。これは仮想的な統合で、実際には連絡先フォルダへデータのコピーは行っていません。

これはグローバルアドレス帳（GAL）の検索機能に対応していないクライアントにとって便利な機能です。これはデフォルトで無効になっています。

Junk-Emailフォルダへ移動したメールの送信者をブロックする
有効にすると、クライアントが特定のメールを自分のJunk Emailフォルダへ移動した際、対象のメール送信者がブロックされた送信者連絡先フォルダへ追加されます。

ミーティング要求が許可/拒否された際、ミーティング要求に対する応答の送信を強制的に行う
このオプションを使用すると、クライアントがミーティング要求に対して、許可や拒否、その他のアクションを選択した際、ミーティング要求に対する応答を開催者へ送信します。これは、こうした更新情報を自動送信する事ができない特定のクライアント用の機能です。

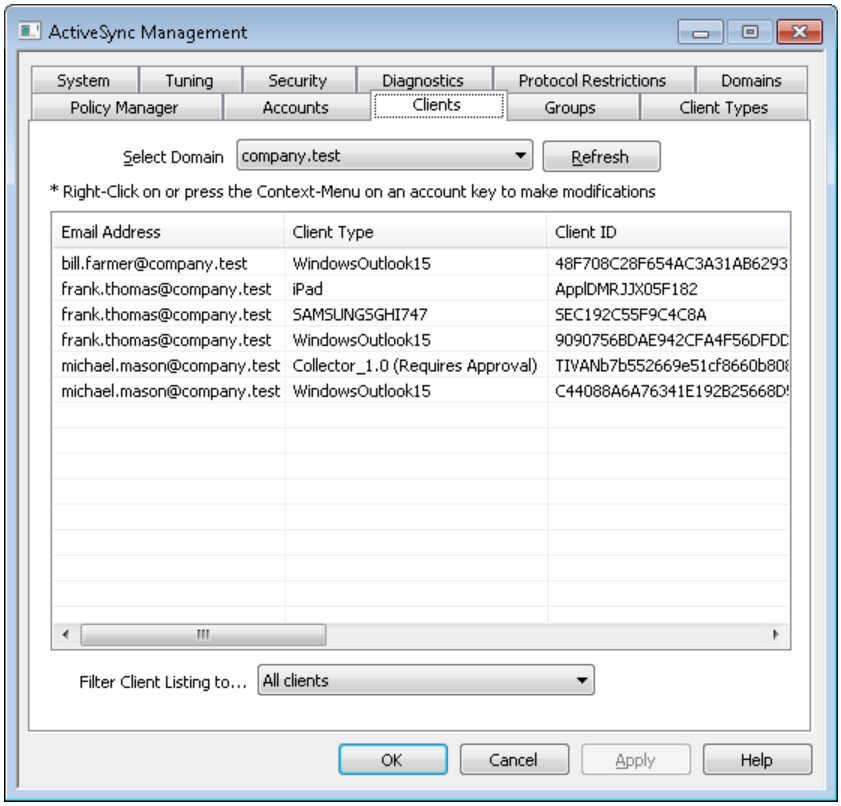
有効な設定をプレビュー

このボタンは全てのクライアント設定（ドメイン397, アカウント413, クライアント422）に対して使用できます。画面のオプションはデフォルト値をその上位の画面から引き継いでいるため、この機能は表示されている画面の現在の設定確認を行う際にもご利用頂けます。

参照:

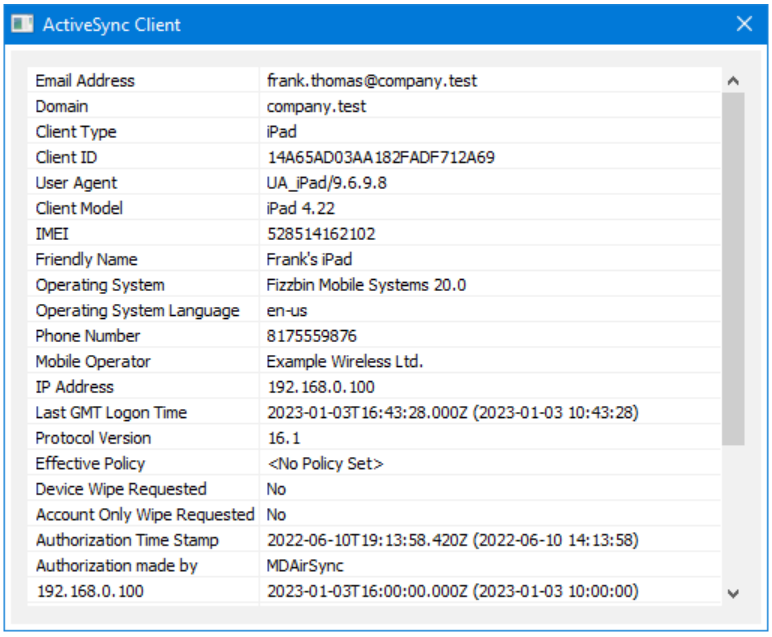
ActiveSync ≫ クライアント設定384
ActiveSync ≫ ドメイン397
ActiveSync ≫ クライアント384
アカウント ≫ ActiveSyncクライアント設定697
アカウント ≫ ActiveSyncクライアント703

3.10.9 クライアント



ここへはドメインと関連付けされたActiveSyncクライアントが一覧表示されます。詳細を確認するには対象のエントリをダブルクリックして下さい。右クリックするとショートカットメニューが表示され、クライアント設定のカスタマイズや統計情報の表示、その他機能を使用できます。

ActiveSync Client Details



エントリを選択し**詳細**をクリック(またはエントリをダブルクリック)すると、クライアント詳細ダイアログが起動します。この画面では、Clientタイプ、Client ID、最終ログイン時間、といった、クライアントの情報を確認できます。

クライアント設定

クライアントを右クリックし**クライアント設定のカスタマイズ**をクリックするとクライアント設定の管理画面が起動します。デフォルト設定はClientタイプの設定を継承していますが、この値は任意のものへ変更する事ができます。デバイスのクライアント設定の管理を参照してください。

ActiveSyncポリシーの適用

ポリシー405は次のように端末へ適用します:

1. 一覧から端末を右クリックします。.
2. **ポリシーの適用**をクリックすると、ポリシーの割り当てダイアログが起動します。
3. **割り当てポリシー**のドロップダウンリストからポリシーを選択します。
4. **OK**をクリックします。

統計

エントリを右クリックし、**統計を表示**をクリックすると、クライアント統計ダイアログが起動し、クライアント様々な統計情報を確認できます。

統計のリセット

クライアントの統計情報を初期化するには、**統計**、**統計のリセット**をクリックし、確認メッセージでOKをクリックします。

ActiveSyncクライアントの削除

ActiveSyncクライアントを削除するには、クライアントを右クリックし**削除**をクリックし、はい、をクリック

します。これにより、クライアントとMDaemonに関連した全ての同期情報が削除されます。今後ユーザーが同じActiveSyncクライアントで同期を行った場合、MDaemonは対象クライアントを初めて同期を行うクライアントとして取扱います。全てのデータはMDaemonと再同期されます。

ActiveSyncクライアントの完全初期化

選択したActiveSyncクライアントへ ポリシー[405] が適用されると、クライアントはポリシーを適用し、応答した後に完全初期化を利用できます。ActiveSyncクライアントを完全に初期化するには、クライアントを一覧から選択し完全初期化をクリックします。次回クライアントが接続すると、MDaemonは全てのデータを削除するか、工場出荷時の設定をリストアします。クライアントによっては、ダウンロード済アプリなど、全てのデータを削除してしまう場合があります。また、クライアントのActiveSyncエントリがMDaemonに残っている間は、クライアントがMDaemonへ接続する度に再度初期化が実行されます。クライアントを削除する際には、これをブロックリスト[391]へ追加し、今後の接続を行わないようにします。最後に、初期化済のデバイスを再度接続する場合は、デバイスを右クリックし、ワイプアクションを中止、をクリックします。同時にブロックリストからも削除して下さい。

アカウントのActiveSyncクライアントのワイプ

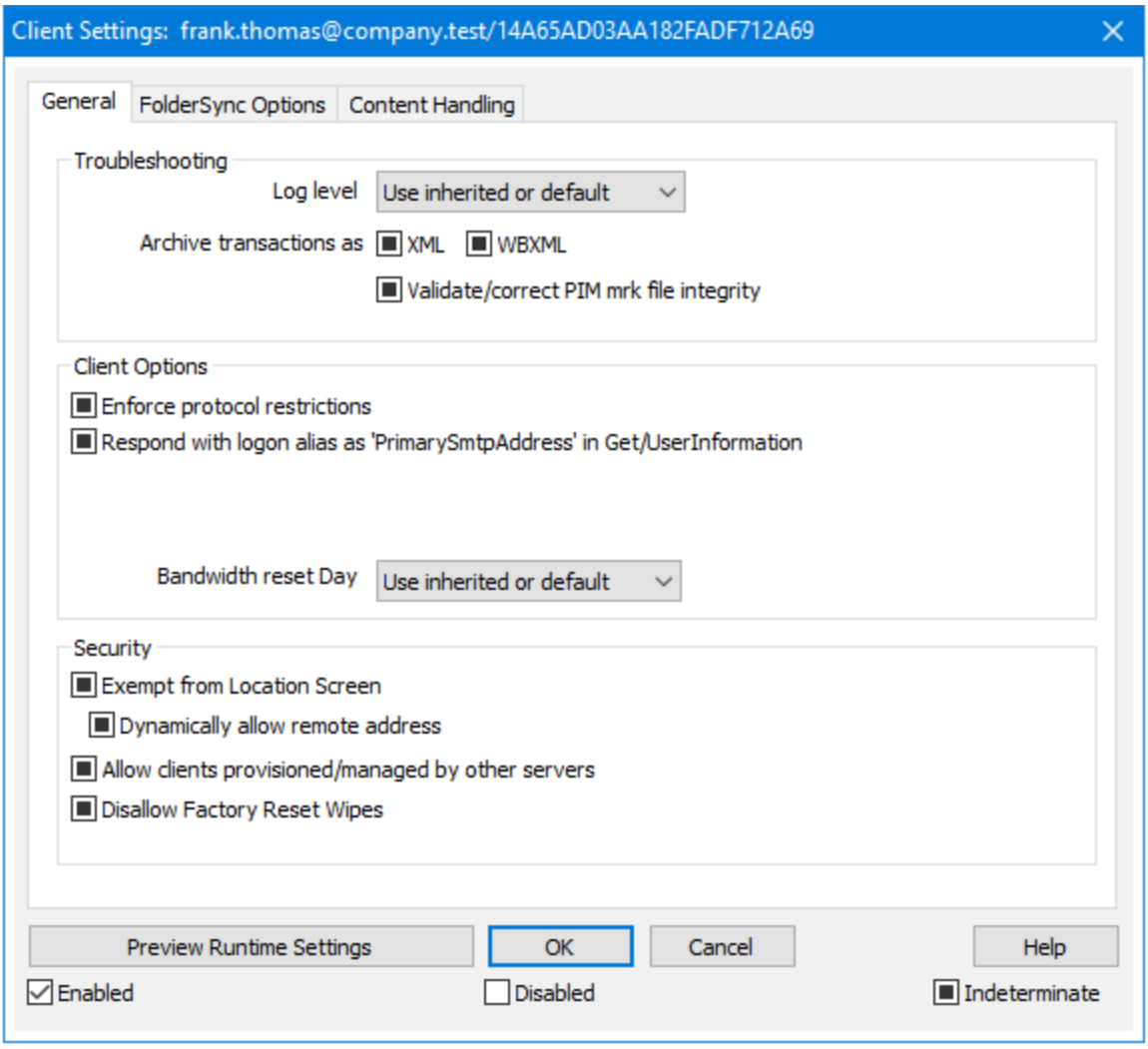
クライアントから、メール、予定表、連絡先といった、アカウントのデータのみを削除する場合は、右クリックし、**クライアントからメールとPIMのアカウントワイプ**をクリックします。 アカウントワイプオプションは完全初期化ににていますが、全てのデータを初期化するのではなく、メールや予定表、連絡先といったアカウント関連データのみを対象にします。その他の、アプリや写真、音楽などは端末上に残ります。

クライアントの承認

ActiveSyncクライアント設定[384] の*"新規クライアントは管理者の承認が必要"*オプションが承認が必要と設定されていた場合、クライアントを選択し クライアントの同期を許可、 をクリックすることでクライアントのサーバーとの同期を承認します。

デバイスのクライアント設定の管理

デバイスレベルのクライアント設定画面では端末毎の設定が管理できます。



デフォルトでこの画面の全てのオプションは「継承又はデフォルト」と設定されており、各オプションがClientタイプクライアント設定 438の関連オプションの設定を継承します。同様に、この画面で行った設定変更はデバイスのクライアントレベル設定を上書きします。

全般

トラブルシューティング

ログレベル

ActiveSync for MDaemonはログデータ量に応じた、6つのレベルのログに対応しています。

デバッグ 最も詳細なログで、記録できる全ての情報が含まれており、問題の診断にのみ使用されます。

情報 通常のログで、一般的な操作が詳細なしで記録されます。これはデフォルトのログレベルです。

警告	警告、エラー、クリティカルエラー、起動と終了がログに記録されます。
エラー	エラー、クリティカルエラー、起動と終了がログに記録されます。
クリティカル	クリティカルエラー、起動と終了がログに記録されます。
なし	起動と終了だけがログに記録されます。
継承	デフォルトで、ログレベルの設定はクライアント設定の階層から継承されます。そのため、クライアントは設定をクライアントタイプから引継ぎ、クライアントタイプはアカウントから引継ぎ、アカウントはグループから引継ぎます。全体のクライアント設定は 診断 393 ダイアログのログレベル設定を元にしています。

トランスアクションを [XML | WBXML]としてアーカイブ
XMLやWBXMLデータをアーカイブするには、*XMLと WBXMLをアーカイブ...* のオプションを使用します。これはデバッグの際役立ちます。全体オプションはデフォルトで無効になっています。

PIM mrkファイルの整合性を確認する
クライアントのPIMデータの整合性テストを実施し、iCal UIDの重複や空の要求フィールドといった、同期を妨げているものがないかどうかを確認します。この全体設定はデフォルトで無効になっています。

クライアントオプション

プロトコル制限を強制する
クライアントで許可されているプロトコルバージョン以外のアクセスを拒否する場合はこのオプションを有効にします。デフォルトでこのオプションは無効になっており、プロトコル制限は異なるプロトコルのクライアントを拒否していません。プロトコル制限は単純に、クライアントに対して使用するべきプロトコルを伝えるのみの機能を提供しています。クライアントがそれでも制限されているプロトコルを使った場合、MDaemonはその接続を受け入れます。詳細は次のページをご覧下さい: プロトコル制限 395

Get/UserInformationへの応答でログオンエイリアスを'PrimarySmtpAddress' として使用する
サービスがSettings/Get/UserInformationリクエストに対する応答としてエイリアスやセカンダリアドレスをプライマリアドレスとして利用できるようにします。これはiOS 9.xへアップデートした際エイリアスからメールを送信できなくなった事に対する対処です。このオプションによって使用に反した応答を受け取る場合があります。

新しいクライアントは管理者の承認が必要
新しいクライアントがアカウントとの同期を開始する前に、管理者による承認を必要とする場合はこのオプションを有効にします。 クライアント 422 一覧で認証待ちのクライアントが確認でき、管理者は同じ画面から承認が行えます。この設定はデフォルトで無効になっています。

ユーザー毎の最大クライアント
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用

できません。

帯域リセット日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

セキュリティ

ロケーションスクリーンから除外する
ActiveSyncクライアント設定で端末をロケーションスクリーニング[520]から除外する場合はこのオプションを有効化します。これにより認証済ユーザーは、例えば認証がブロックされている場所へ出張しているような場合であっても、ActiveSync経由でアカウントへアクセスする事ができるようになります。端末を除外するためには、チューニング画面にあるこの日数を超えて認証されなかった端末を自動削除[381]設定の時間内に、ActiveSyncを使った接続と認証を行っておく必要があります。

リモートアドレスを動的に除外
接続元のリモートIPアドレスをロケーションスクリーニングの除外リストへ追加する事ができます。このオプションは、同じIPアドレスを使って接続する他のクライアントがある場合に便利です。

ユーザー毎の最大クライアント数
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域の統計情報をリセットする日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

他のサーバーで管理されているクライアントへの接続を許可する
デフォルトで、ActiveSyncサーバーが特定のクライアントへデータやポリシーを送信する際、対象クライアントが他のActiveSyncサーバーからも管理されている事が分かった場合も、クライアントはMDaemonへアクセスする事ができます。しかし、このような環境の場合、適用するポリシーが他のActiveSyncサーバーと競合する可能性があります。一般的に、クライアントはポリシーが競合した場合、厳しい方へ合わせる傾向があります。こうしたクライアントからの接続を制限する場合は、このオプションを無効化して下さい。

工場出荷時への完全ワイプを無効化
オン/はい、を設定すると、ActiveSyncクライアントの完全ワイプが行えなくなります。クライアントでリモートからの完全ワイプを許可する場合、最初にこのオプションを無効化して下さい。このオプションはデフォルトで無効に設定されています。クライアントページの次の項目を参照して下さい:
ActiveSyncクライアントの完全ワイプ[422]

フォルダ同期オプション

フォルダ同 期 オプション

除 外

ユーザの [許 可 リスト /ブロックリスト] フォルダ
デフォルト でユーザーの許 可 リスト とブロックリスト の連 絡 先 フォルダは端 末 と同 期 を行 いません。これらはMDaemonがスパムからシステムを自 動 的 に保 護 するのを支 援 する目 的 で使 用 されます。そのため、許 可 リスト やブロックリスト は端 末 上 に連 絡 先 として表 示 する必 要 性 はありません。

デフォルト 以 外 のメールフォルダ
デフォルト で、ユーザーが作 成 したメールフォルダとデフォルト メールフォルダは全 て端 末 と同 期 します。同 期 するのを受 信 箱 や送 信 箱 、削 除 済 アイテム、下 書 き、といった、デフォルト のメールフォルダのみにしたい場 合 はこのオプションを有 効 にして下 さい。ユーザーが作 成 したフォルダは同 期 対 象 に含 まれません。 このオプションはデフォルト で無 効 になっています。

デフォルト 以 外 のPIMフォルダ
デフォルト で、(連 絡 先 、予 定 表 、仕 事 などの) PIMフォルダは全 て端 末 と同 期 します。同 期 するのをデフォルト のPIMフォルダのみにしたい場 合 はこのオプションを有 効 にして下 さい。このオプションが有 効 な場 合 で、ユーザーが複 数 の予 定 表 を保 有 してる場 合 デフォルト の予 定 表 のみが同 期 対 象 となります。 このオプションはデフォルト で無 効 になっています。

含 む

パブリックフォルダの階 層
ユーザーがアクセス権 を持 っている パブリックフォルダ 283 をユーザーのActiveSync用 端 末 のフォルダ一 覧 へ含 むにはこのオプションを有 効 にします。これはデフォルト で有 効 です。

検 索 を許 可 する
パブリックフォルダ 283 をユーザーが検 索 できるようになります。 これはデフォルト で許 可 されています。

パブリックフォルダの横 断 (フォルダ名 の公 開)
デフォルト で、クライアント がパブリックのサブフォルダへのアクセスや同 期 を行 うには、サブフォルダと上 位 のパブリックフォルダ 283 全 てに対 してルックアップ権 限 285 が必 要 です。上 位 のフォルダに対 するアクセス権 がない場 合 、その中 のサブフォルダに対 しては、例 え設 定 上 は許 可 されていても、アクセスする事 はできません。クライアント からこうしたサブフォルダへアクセスできるようにする場 合 は、このオプションを有 効 にします。注 意 点 : このオプションを有 効 化 すると、上 位 のフォルダもクライアント へ許 可 する事 となり、セキュリティのリスクを招 く恐 れがあります。 このオプションはデフォルト で無 効 になっています。

許 可 するパブリックフォルダの最 大 数
端 末 で処 理 するパブリックフォルダ数 を制 限 する場 合 はこのオプションを使 用 します。制 限 が設 定 されると、サーバーは最 大 数 に到 達 するまでフォルダー 覧 を処 理 し、これを超 えるとその後 のデータを送 りません。処 理 するフォルダの順 番 を決 める事 はできません。デフォルト で、全 体 での最 大 数 は設 定 されていません。

共 有 フォルダも含 める

ユーザーがアクセス権を持っている 共有フォルダ[107] をユーザーのActiveSync用端末のフォルダー一覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
共有フォルダ[676] をユーザーが検索できるようになります。これはデフォルトで許可されています。

コンテンツ処理

コンテンツ処理オプション

クライアントにフラグ付けされたメール用にタスク・リマインダーを作成
このオプションでMDaemonはフラグが付いたアイテムごとに仕事を作成し、リマインダーをユーザーへ送信できるようになります。この設定の全体値はデフォルトで有効です。

予定を編集した際、常にミーティングのアップデートを送信
クライアントの中には、ミーティングを編集した際、更新情報を適切に送信しないものもあります。このオプションを使うとActiveSyncサービスへ、ミーティングが開催者によって更新された際、更新情報を送信するよう促す事ができるようになります。これはミーティングの更新情報の送信に失敗しているクライアント[422]やクライアントタイプ[438]に限定して使用するべきで、更新情報が重複して送られてしまう可能性があります。また、このオプションはクライアントとクライアントタイプの設定ページでのみ利用できます。

全ての送信メールで開封確認を要求
クライアントから送信される全てのメールで開封確認要求を行うにはこのオプションを有効にして下さい。これはデフォルトで無効になっています。

送信者からリクエストされた際送信済メールについて開封確認を送信
サーバー側で開封確認要求を検出し、既読フラグがついたメールの開封通知を送信するにはこのオプションを使用します。これはデフォルトで無効になっています。

ReplyToアドレスに指定したエイリアスとして送る
クライアントによっては、エイリアスを使ったメール送信を許可していません。この機能は Exchange ActiveSync（EAS）プロトコル[395] 16.xで追加されたものですが、クライアントの中には16.xに対応していないものもあります。例えば、Windows用OutlookはEAS 14.0だけを使用しており、ユーザーが関連するアドレスを指定して送信する事のみ許可しており、生成されたメールはユーザーの選択を正しく反映していません。このオプションでは、ReplyToのアドレスがユーザー用の正しいエイリアス[757]であれば、これを使ってメール送信を行います。この設定の全体値はデフォルトで有効です。

デフォルトの連絡先にパブリック連絡先を仮想的に統合する
パブリック連絡先をユーザーの端末上でデフォルトの連絡先と統合したい場合はこのオプションを有効にします。これは仮想的な統合で、実際には連絡先フォルダへデータのコピーは行っていません。これはグローバルアドレス帳（GAL）の検索機能に対応していないクライアントにとって便利な機能です。これはデフォルトで無効になっています。

Junk-Emailフォルダへ移動したメールの送信者をブロックする
有効にすると、クライアントが特定のメールを自分のJunk Emailフォルダへ移動した際、対象のメー

ル送信者がブロックされた送信者連絡先フォルダへ追加されます。

ミーティング要求が許可/拒否された際、ミーティング要求に対する応答の送信を強制的に行う
このオプションを使用すると、クライアントがミーティング要求に対して、許可や拒否、その他のアクションを選択した際、ミーティング要求に対する応答を開催者へ送信します。これは、こうした更新情報を自動送信する事ができない特定のクライアント用の機能です。

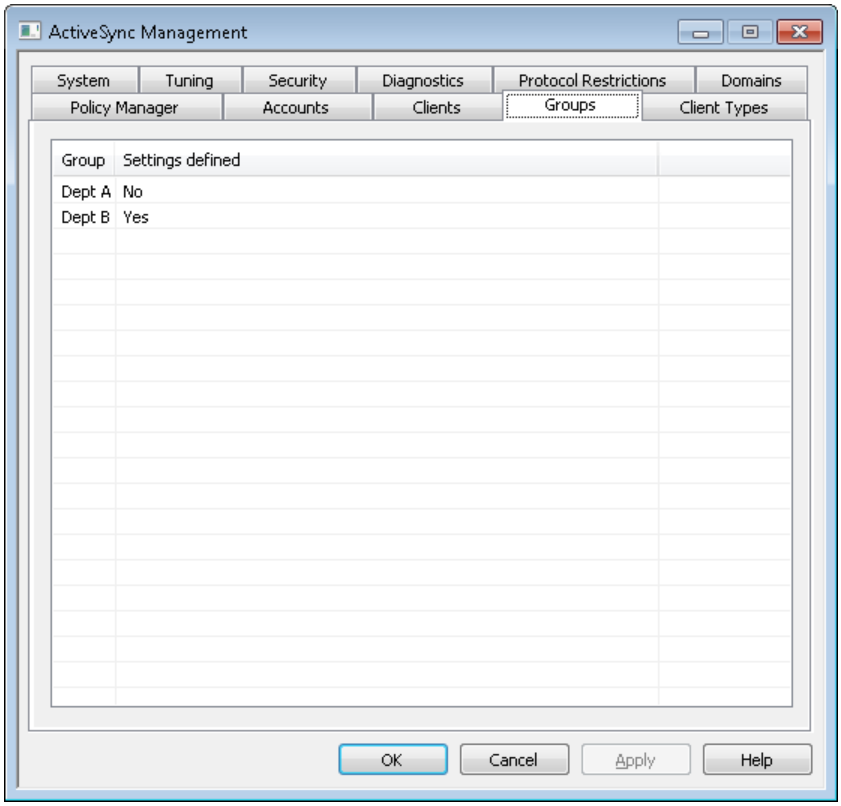
有効な設定をプレビュー

このボタンは全てのクライアント設定（ドメイン397, アカウント413, クライアント422）に対して使用できます。画面のオプションはデフォルト値をその上位の画面から引き継いでいるため、この機能は表示されている画面の現在の設定確認を行う際にもご利用頂けます。

参照:

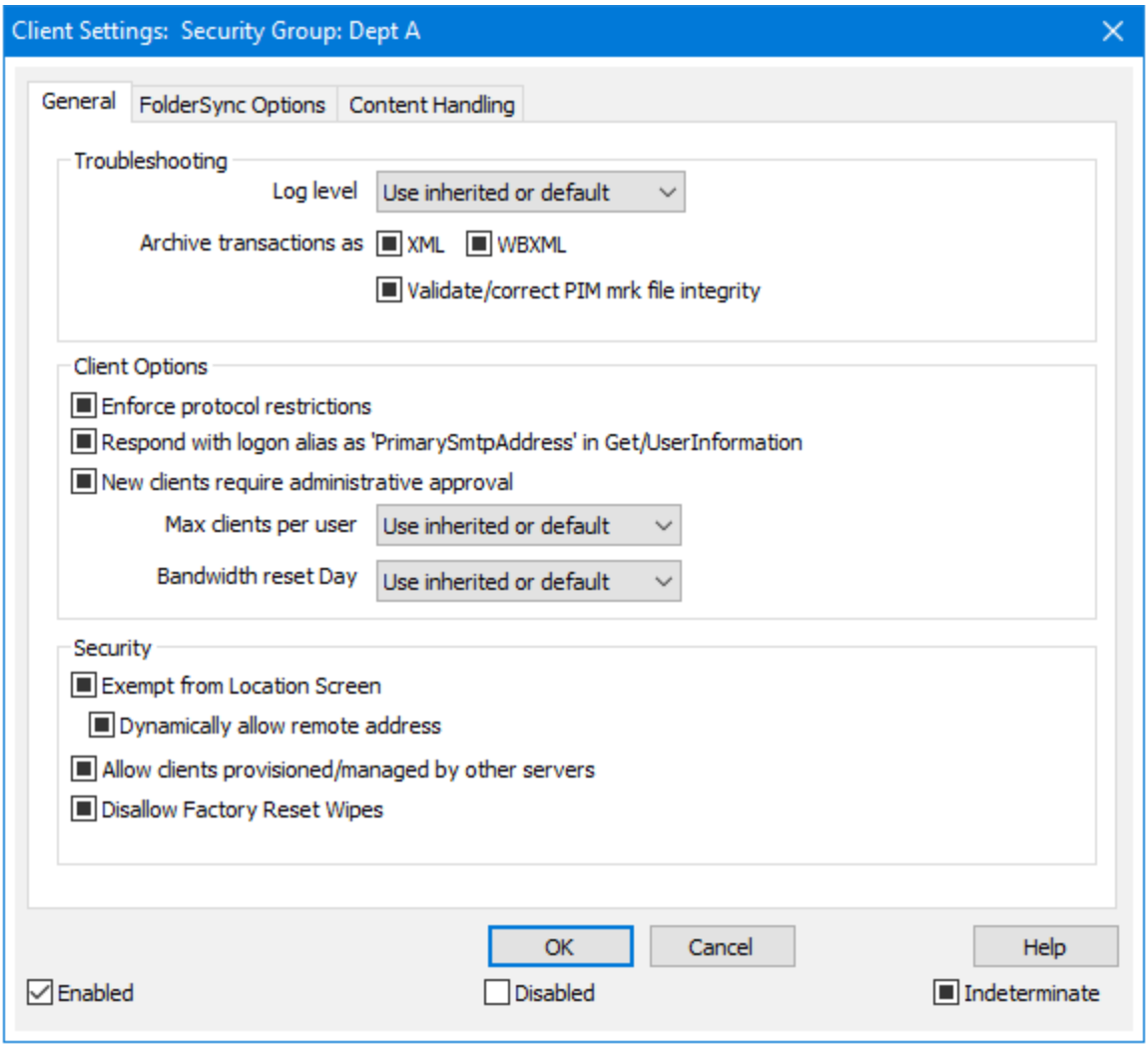
ActiveSync ≫ クライアント設定384
ActiveSync ≫ ドメイン397
ActiveSync ≫ アカウント413

3.10.10 グループ



カスタマイズしたActiveSyncクライアント設定をアカウントグループへ割り当てるには、この画面で設定を管理する事ができます。全てのグループはここへ一覧表示され、各グループのエントリがカスタマイズされたものかどうかを確認できます。グループのクライアント設定を変更する場合は、グループをダブルクリックするか、グループを右クリックしクライアント設定のカスタマイズをクリックします。

グループクライアント設定



デフォルトで各グループのクライアント設定はユーザーのドメインクライアント設定[196]を継承して設定されます。グループ設定を変更すると、変更箇所はアカウントが属したグループのドメイン設定を上書きします。グループクライアント設定を特定のグループメンバーやデバイスへ適用しない場合は、アカウント[413]、クライアントタイプ[438]、クライアント[422]向けのクライアント設定を変更する事で、グループ設定を上書きしてください。

全般

トラブルシューティング

ログレベル

ActiveSync for MDaemonはログデータ量に応じた、6つのレベルのログに対応しています。

デバッグ 最も詳細なログで、記録できる全ての情報が含まれており、問題の診断にのみ使用されます。

情報 通常のログで、一般的な操作が詳細なしで記録されます。これはデフォルトの

ログレベルです。

警告 警告、エラー、クリティカルエラー、起動と終了がログに記録されます。

エラー エラー、クリティカルエラー、起動と終了がログに記録されます。

クリティカル クリティカルエラー、起動と終了がログに記録されます。

なし 起動と終了だけがログに記録されます。

継承 デフォルトで、ログレベルの設定はクライアント設定の階層から継承されます。そのため、クライアントは設定をクライアントタイプから引継ぎ、クライアントタイプはアカウントから引継ぎ、アカウントはグループから引継ぎます。全体のクライアント設定は 診断 393 ダイアログのログレベル設定を元にしています。

トランスアクションを [XML | WBXML]としてアーカイブ
XMLやWBXMLデータをアーカイブするには、*XMLと WBXMLをアーカイブ...* のオプションを使用します。これはデバッグの際役立ちます。全体オプションはデフォルトで無効になっています。

PIM mrkファイルの整合性を確認する
クライアントのPIMデータの整合性テストを実施し、iCal UIDの重複や空の要求フィールドといった、同期を妨げているものがないかどうかを確認します。この全体設定はデフォルトで無効になっています。

クライアントオプション

プロトコル制限を強制する
クライアントで許可されているプロトコルバージョン以外のアクセスを拒否する場合はこのオプションを有効にします。デフォルトでこのオプションは無効になっており、プロトコル制限は異なるプロトコルのクライアントを拒否していません。プロトコル制限は単純に、クライアントに対して使用するべきプロトコルを伝えるのみの機能を提供しています。クライアントがそれでも制限されているプロトコルを使った場合、MDaemonはその接続を受け入れます。詳細は次のページをご覧下さい: プロトコル制限 395

Get/UserInformationへの応答でログオンエイリアスを'PrimarySmtpAddress' として使用する
サービスがSettings/Get/UserInformationリクエストに対する応答としてエイリアスやセカンダリアドレスをプライマリアドレスとして利用できるようにします。これはiOS 9.xへアップデートした際エイリアスからメールを送信できなくなった事に対する対処です。このオプションによって使用に反した応答を受け取る場合があります。

新しいクライアントは管理者の承認が必要
新しいクライアントがアカウントとの同期を開始する前に、管理者による承認を必要とする場合はこのオプションを有効にします。 クライアント 422 一覧で認証待ちのクライアントが確認でき、管理者は同じ画面から承認が行えます。この設定はデフォルトで無効になっています。

ユーザー毎の最大クライアント
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、

ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域リセット日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

セキュリティ

ロケーションスクリーンから除外する
ActiveSyncクライアント設定で端末をロケーションスクリーニング[520]から除外する場合はこのオプションを有効化します。これにより認証済ユーザーは、例えば認証がブロックされている場所へ出張しているような場合であっても、ActiveSync経由でアカウントへアクセスする事ができるようになります。端末を除外するためには、チューニング画面にあるこの日数を超えて認証されなかった端末を自動削除[381]設定の時間内に、ActiveSyncを使った接続と認証を行っておく必要があります。

リモートアドレスを動的に除外
接続元のリモートIPアドレスをロケーションスクリーニングの除外リストへ追加する事ができます。このオプションは、同じIPアドレスを使って接続する他のクライアントがある場合に便利です。

ユーザー毎の最大クライアント数
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域の統計情報をリセットする日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

他のサーバーで管理されているクライアントへの接続を許可する
デフォルトで、ActiveSyncサーバーが特定のクライアントへデータやポリシーを送信する際、対象クライアントが他のActiveSyncサーバーからも管理されている事が分かった場合も、クライアントはMDaemonへアクセスする事ができます。しかし、このような環境の場合、適用するポリシーが他のActiveSyncサーバーと競合する可能性があります。一般的に、クライアントはポリシーが競合した場合、厳しい方へ合わせる傾向があります。こうしたクライアントからの接続を制限する場合は、このオプションを無効化して下さい。

工場出荷時への完全ワイプを無効化
オン/はい、を設定すると、ActiveSyncクライアントの完全ワイプが行えなくなります。クライアントでリモートからの完全ワイプを許可する場合、最初にこのオプションを無効化して下さい。このオプションはデフォルトで無効に設定されています。クライアントページの次の項目を参照して下さい：
ActiveSyncクライアントの完全ワイプ[422]

フォルダ同期オプション

フォルダ同 期 オプション

除 外

ユーザの [許 可 リスト /ブロックリスト] フォルダ
デフォルト でユーザーの許 可 リスト とブロックリスト の連 絡 先 フォルダは端 末 と同 期 を行 いません。これらはMDaemonがスパムからシステムを自 動 的 に保 護 するのを支 援 する目 的 で使 用 されます。そのため、許 可 リスト やブロックリスト は端 末 上 に連 絡 先 として表 示 する必 要 性 はありません。

デフォルト 以 外 のメールフォルダ
デフォルト で、ユーザーが作 成 したメールフォルダとデフォルト メールフォルダは全 て端 末 と同 期 します。同 期 するのを受 信 箱 や送 信 箱 、削 除 済 アイテム、下 書 き、といった、デフォルト のメールフォルダのみにしたい場 合 はこのオプションを有 効 にして下 さい。ユーザーが作 成 したフォルダは同 期 対 象 に含 まれません。 このオプションはデフォルト で無 効 になっています。

デフォルト 以 外 のPIMフォルダ
デフォルト で、(連 絡 先 、予 定 表 、仕 事 などの) PIMフォルダは全 て端 末 と同 期 します。同 期 するのをデフォルト のPIMフォルダのみにしたい場 合 はこのオプションを有 効 にして下 さい。このオプションが有 効 な場 合 で、ユーザーが複 数 の予 定 表 を保 有 してる場 合 デフォルト の予 定 表 のみが同 期 対 象 となります。 このオプションはデフォルト で無 効 になっています。

含 む

パブリックフォルダの階 層
ユーザーがアクセス権 を持 っている パブリックフォルダ[283] をユーザーのActiveSync用 端 末 のフォルダー 覧 へ含 むにはこのオプションを有 効 にします。これはデフォルト で有 効 です。

検 索 を許 可 する
パブリックフォルダ[283] をユーザーが検 索 できるようになります。 これはデフォルト で許 可 されています。

パブリックフォルダの横 断 (フォルダ名 の公 開)
デフォルト で、クライアント がパブリックのサブフォルダへのアクセスや同 期 を行 うには、サブフォルダと上 位 のパブリックフォルダ[283]全 てに対 してルックアップ権 限 [285]が必 要 です。上 位 のフォルダに対 するアクセス権 がない場 合 、その中 のサブフォルダに対 しては、例 え設 定 上 は許 可 されていても、アクセスする事 はできません。クライアント からこうしたサブフォルダへアクセスできるようにする場 合 は、このオプションを有 効 にします。注 意 点 : このオプションを有 効 化 すると、上 位 のフォルダもクライアント へ許 可 する事 となり、セキュリティのリスクを招 く恐 れがあります。 このオプションはデフォルト で無 効 になっています。

許 可 するパブリックフォルダの最 大 数
端 末 で処 理 するパブリックフォルダ数 を制 限 する場 合 はこのオプションを使 用 します。制 限 が設 定 されると、サーバーは最 大 数 に到 達 するまでフォルダー 覧 を処 理 し、これを超 えるとその後 のデータを送 りません。処 理 するフォルダの順 番 を決 める事 はできません。デフォルト で、全 体 での最 大 数 は設 定 されていません。

共有フォルダも含める

ユーザーがアクセス権を持っている 共有フォルダ[107] をユーザーのActiveSync用端末のフォルダー一覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
共有フォルダ[676] をユーザーが検索できるようになります。 これはデフォルトで許可されています。

コンテンツ処理

コンテンツ処理オプション

クライアントにフラグ付けされたメール用にタスク・リマインダーを作成
このオプションでMDaemonはフラグが付いたアイテムごとに仕事を作成し、リマインダーをユーザーへ送信できるようになります。この設定の全体値はデフォルトで有効です。

予定を編集した際、常にミーティングのアップデートを送信
クライアントの中には、ミーティングを編集した際、更新情報を適切に送信しないものもあります。このオプションを使うとActiveSyncサービスへ、ミーティングが開催者によって更新された際、更新情報を送信するよう促す事ができるようになります。これはミーティングの更新情報の送信に失敗しているクライアント[422]やクライアントタイプ[438]に限定して使用するべきで、更新情報が重複して送られてしまう可能性があります。また、このオプションはクライアントとクライアントタイプの設定ページでのみ利用できます。

全ての送信メールで開封確認を要求
クライアントから送信される全てのメールで開封確認要求を行うにはこのオプションを有効にして下さい。これはデフォルトで無効になっています。

送信者からリクエストされた際送信済メールについて開封確認を送信
サーバー側で開封確認要求を検出し、既読フラグがついたメールの開封通知を送信するにはこのオプションを使用します。 これはデフォルトで無効になっています。

ReplyToアドレスに指定したエイリアスとして送る
クライアントによっては、エイリアスを使ったメール送信を許可していません。この機能は Exchange ActiveSync（EAS）プロトコル[395] 16.xで追加されたものですが、クライアントの中には16.xに対応していないものもあります。例えば、Windows用OutlookはEAS 14.0だけを使用しており、ユーザーが関連するアドレスを指定して送信する事のみ許可しており、生成されたメールはユーザーの選択を正しく反映していません。このオプションでは、ReplyToのアドレスがユーザー用の正しいエイリアス[757]であれば、これを使ってメール送信を行います。この設定の全体値はデフォルトで有効です。

デフォルトの連絡先にパブリック連絡先を仮想的に統合する
パブリック連絡先をユーザーの端末上でデフォルトの連絡先と統合したい場合はこのオプションを有効にします。これは仮想的な統合で、実際には連絡先フォルダへデータのコピーは行っていません。これはグローバルアドレス帳（GAL）の検索機能に対応していないクライアントにとって便利な機能です。これはデフォルトで無効になっています。

Junk-Emailフォルダへ移動したメールの送信者をブロックする
有効にすると、クライアントが特定のメールを自分のJunk Emailフォルダへ移動した際、対象のメール送信者がブロックされた送信者連絡先フォルダへ追加されます。

ミーティング要求が許可/拒否された際、ミーティング要求に対する応答の送信を強制的に行う
このオプションを使用すると、クライアントがミーティング要求に対して、許可や拒否、その他のアクションを選択した際、ミーティング要求に対する応答を開催者へ送信します。これは、こうした更新情報を自動送信する事ができない特定のクライアント用の機能です。

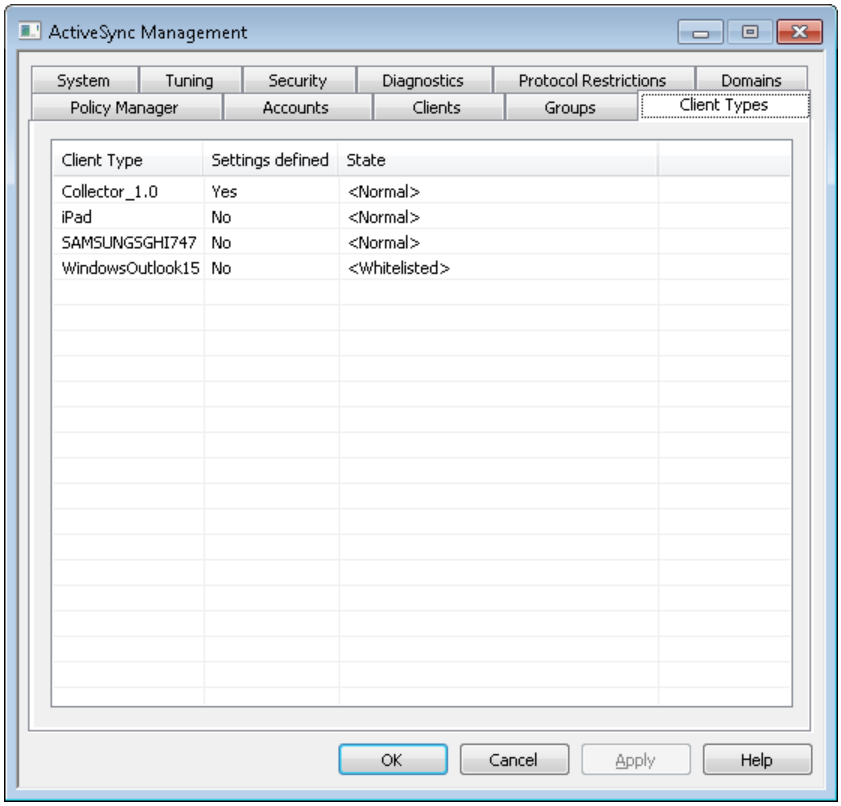
有効な設定をプレビュー

このボタンは全てのクライアント設定（ドメイン397, アカウント413, クライアント422）に対して使用できます。画面のオプションはデフォルト値をその上位の画面から引き継いでいるため、この機能は表示されている画面の現在の設定確認を行う際にもご利用頂けます。

参照:

ActiveSync ≫ ドメイン397
ActiveSync ≫ アカウント413
ActiveSync ≫ クライアント422

3.10.11 クライアントタイプ



カスタマイズしたActiveSyncクライアント設定を特定の種類のActiveSyncクライアントへ適用するには、この画面で設定を行います。ActiveSyncを利用できる全ての現在認証済のクライアント[422]はここへ一覧表示され、各クライアントタイプが指定されたものかどうかを確認できます。クライアント設定のクライアントタイプを編集するには、エントリをダブルクリックするか、右クリックし**クライアント設定のカスタマイズ**をクリックします。カスタマイズした設定は右クリックで削除したり、ActiveSyncの許可リストや除外リスト[391]へクライアントタイプの追加や削除を行う事もできます。

デフォルトでクライアント設定の各クライアントタイプはアカウントクライアント設定[697]を継承して設定されます。クライアントタイプを変更すると、変更箇所は対象のクライアントタイプを使用しているアカウントの設定を上書きします。クライアントタイプ設定を特定のクライアントへ適用しない場合は、クライアントのクライアント設定[422]を変更する事で、クライアントタイプ設定を上書きしてください。

全般

トラブルシューティング

ログレベル

ActiveSync for MDaemonはログデータ量に応じた、6つのレベルのログに対応しています。

デバッグ　最も詳細なログで、記録できる全ての情報が含まれており、問題の診断にのみ使用されます。

情報 通常のログで、一般的な操作が詳細なしで記録されます。これはデフォルトのログレベルです。

警告 警告、エラー、クリティカルエラー、起動と終了がログに記録されます。

エラー エラー、クリティカルエラー、起動と終了がログに記録されます。

クリティカル クリティカルエラー、起動と終了がログに記録されます。

なし 起動と終了だけがログに記録されます。

継承 デフォルトで、ログレベルの設定はクライアント設定の階層から継承されます。そのため、クライアントは設定をクライアントタイプから引継ぎ、クライアントタイプはアカウントから引継ぎ、アカウントはグループから引継ぎます。全体のクライアント設定は 診断 393 ダイアログのログレベル設定を元にしています。

トランスアクションを [XML | WBXML]としてアーカイブ
XMLやWBXMLデータをアーカイブするには、*XMLと WBXMLをアーカイブ...* のオプションを使用します。これはデバッグの際役立ちます。全体オプションはデフォルトで無効になっています。

PIM mrkファイルの整合性を確認する
クライアントのPIMデータの整合性テストを実施し、iCal UIDの重複や空の要求フィールドといった、同期を妨げているものがないかどうかを確認します。この全体設定はデフォルトで無効になっています。

クライアントオプション

プロトコル制限を強制する
クライアントで許可されているプロトコルバージョン以外のアクセスを拒否する場合はこのオプションを有効にします。デフォルトでこのオプションは無効になっており、プロトコル制限は異なるプロトコルのクライアントを拒否していません。プロトコル制限は単純に、クライアントに対して使用するべきプロトコルを伝えるのみの機能を提供しています。クライアントがそれでも制限されているプロトコルを使った場合、MDaemonはその接続を受け入れます。詳細は次のページをご覧下さい: プロトコル制限 395

Get/UserInformationへの応答でログオンエイリアスを'PrimarySmtpAddress' として使用する
サービスがSettings/Get/UserInformationリクエストに対する応答としてエイリアスやセカンダリアドレスをプライマリアドレスとして利用できるようにします。これはiOS 9.xへアップデートした際エイリアスからメールを送信できなくなった事に対する対処です。このオプションによって使用に反した応答を受け取る場合があります。

新しいクライアントは管理者の承認が必要
新しいクライアントがアカウントとの同期を開始する前に、管理者による承認を必要とする場合はこのオプションを有効にします。 クライアント 422 一覧で認証待ちのクライアントが確認でき、管理者は同じ画面から承認が行えます。この設定はデフォルトで無効になっています。

ユーザー毎の最大クライアント
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クラ

イアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域リセット日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

セキュリティ

ロケーションスクリーンから除外する
ActiveSyncクライアント設定で端末をロケーションスクリーニング[520]から除外する場合はこのオプションを有効化します。これにより認証済ユーザーは、例えば認証がブロックされている場所へ出張しているような場合であっても、ActiveSync経由でアカウントへアクセスする事ができるようになります。端末を除外するためには、チューニング画面にあるこの日数を超えて認証されなかった端末を自動削除[381]設定の時間内に、ActiveSyncを使った接続と認証を行っておく必要があります。

リモートアドレスを動的に除外
接続元のリモートIPアドレスをロケーションスクリーニングの除外リストへ追加する事ができます。このオプションは、同じIPアドレスを使って接続する他のクライアントがある場合に便利です。

ユーザー毎の最大クライアント数
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域の統計情報をリセットする日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

他のサーバーで管理されているクライアントへの接続を許可する
デフォルトで、ActiveSyncサーバーが特定のクライアントへデータやポリシーを送信する際、対象クライアントが他のActiveSyncサーバーからも管理されている事が分かった場合も、クライアントはMDaemonへアクセスする事ができます。しかし、このような環境の場合、適用するポリシーが他のActiveSyncサーバーと競合する可能性があります。一般的に、クライアントはポリシーが競合した場合、厳しい方へ合わせる傾向があります。こうしたクライアントからの接続を制限する場合は、このオプションを無効化して下さい。

工場出荷時への完全ワイプを無効化
オン/はい、を設定すると、ActiveSyncクライアントの完全ワイプが行えなくなります。クライアントでリモートからの完全ワイプを許可する場合、最初にこのオプションを無効化して下さい。このオプションはデフォルトで無効に設定されています。クライアントページの次の項目を参照して下さい:
ActiveSyncクライアントの完全ワイプ[422]

フォルダ同期オプション

フォルダ同 期 オプション

除 外

ユーザの [許 可 リスト /ブロックリスト] フォルダ
デフォルト でユーザーの許 可 リスト とブロックリスト の連 絡 先 フォルダは端 末 と同 期 を行 いません。これらはMDaemonがスパムからシステムを自 動 的 に保 護 するのを支 援 する目 的 で使 用 されます。そのため、許 可 リスト やブロックリスト は端 末 上 に連 絡 先 として表 示 する必 要 性 はありません。

デフォルト 以 外 のメールフォルダ
デフォルト で、ユーザーが作 成 したメールフォルダとデフォルト メールフォルダは全 て端 末 と同 期 します。同 期 するのを受 信 箱 や送 信 箱 、削 除 済 アイテム、下 書 き、といった、デフォルト のメールフォルダのみにしたい場 合 はこのオプションを有 効 にして下 さい。ユーザーが作 成 したフォルダは同 期 対 象 に含 まれません。 このオプションはデフォルト で無 効 になっています。

デフォルト 以 外 のPIMフォルダ
デフォルト で、(連 絡 先 、予 定 表 、仕 事 などの) PIMフォルダは全 て端 末 と同 期 します。同 期 するのをデフォルト のPIMフォルダのみにしたい場 合 はこのオプションを有 効 にして下 さい。このオプションが有 効 な場 合 で、ユーザーが複 数 の予 定 表 を保 有 してる場 合 デフォルト の予 定 表 のみが同 期 対 象 となります。 このオプションはデフォルト で無 効 になっています。

含 む

パブリックフォルダの階 層
ユーザーがアクセス権 を持 っている パブリックフォルダ 283 をユーザーのActiveSync用 端 末 のフォルダー 覧 へ含 むにはこのオプションを有 効 にします。これはデフォルト で有 効 です。

検 索 を許 可 する
パブリックフォルダ 283 をユーザーが検 索 できるようになります。 これはデフォルト で許 可 されています。

パブリックフォルダの横 断 (フォルダ名 の公 開)
デフォルト で、クライアント がパブリックのサブフォルダへのアクセスや同 期 を行 うには、サブフォルダと上 位 のパブリックフォルダ 283 全 てに対 してルックアップ権 限 285 が必 要 です。上 位 のフォルダに対 するアクセス権 がない場 合 、その中 のサブフォルダに対 しては、例 え設 定 上 は許 可 されていても、アクセスする事 はできません。クライアント からこうしたサブフォルダへアクセスできるようにする場 合 は、このオプションを有 効 にします。注 意 点 : このオプションを有 効 化 すると、上 位 のフォルダもクライアント へ許 可 する事 となり、セキュリティのリスクを招 く恐 れがあります。 このオプションはデフォルト で無 効 になっています。

許 可 するパブリックフォルダの最 大 数
端 末 で処 理 するパブリックフォルダ数 を制 限 する場 合 はこのオプションを使 用 します。制 限 が設 定 されると、サーバーは最 大 数 に到 達 するまでフォルダー 覧 を処 理 し、これを超 えるとその後 のデータを送 りません。処 理 するフォルダの順 番 を決 める事 はできません。デフォルト で、全 体 での最 大 数 は設 定 されていません。

共有フォルダも含める

ユーザーがアクセス権を持っている 共有フォルダ[107] をユーザーのActiveSync用端末のフォルダー一覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
共有フォルダ[676] をユーザーが検索できるようになります。 これはデフォルトで許可されています。

コンテンツ処理

コンテンツ処理オプション

クライアントにフラグ付けされたメール用にタスク・リマインダーを作成
このオプションでMDaemonはフラグが付いたアイテムごとに仕事を作成し、リマインダーをユーザーへ送信できるようになります。この設定の全体値はデフォルトで有効です。

予定を編集した際、常にミーティングのアップデートを送信
クライアントの中には、ミーティングを編集した際、更新情報を適切に送信しないものもあります。このオプションを使うとActiveSyncサービスへ、ミーティングが開催者によって更新された際、更新情報を送信するよう促す事ができるようになります。これはミーティングの更新情報の送信に失敗しているクライアント[422]やクライアントタイプ[438]に限定して使用するべきで、更新情報が重複して送られてしまう可能性があります。また、このオプションはクライアントとクライアントタイプの設定ページでのみ利用できます。

全ての送信メールで開封確認を要求
クライアントから送信される全てのメールで開封確認要求を行うにはこのオプションを有効にして下さい。これはデフォルトで無効になっています。

送信者からリクエストされた際送信済メールについて開封確認を送信
サーバー側で開封確認要求を検出し、既読フラグがついたメールの開封通知を送信するにはこのオプションを使用します。 これはデフォルトで無効になっています。

ReplyToアドレスに指定したエイリアスとして送る
クライアントによっては、エイリアスを使ったメール送信を許可していません。この機能は Exchange ActiveSync（EAS）プロトコル[395] 16.xで追加されたものですが、クライアントの中には16.xに対応していないものもあります。例えば、Windows用OutlookはEAS 14.0だけを使用しており、ユーザーが関連するアドレスを指定して送信する事のみ許可しており、生成されたメールはユーザーの選択を正しく反映していません。このオプションでは、ReplyToのアドレスがユーザー用の正しいエイリアス[757]であれば、これを使ってメール送信を行います。この設定の全体値はデフォルトで有効です。

デフォルトの連絡先にパブリック連絡先を仮想的に統合する
パブリック連絡先をユーザーの端末上でデフォルトの連絡先と統合したい場合はこのオプションを有効にします。これは仮想的な統合で、実際には連絡先フォルダへデータのコピーは行っていません。これはグローバルアドレス帳（GAL）の検索機能に対応していないクライアントにとって便利な機能です。これはデフォルトで無効になっています。

Junk-Emailフォルダへ移動したメールの送信者をブロックする
有効にすると、クライアントが特定のメールを自分のJunk Emailフォルダへ移動した際、対象のメール送信者がブロックされた送信者連絡先フォルダへ追加されます。

ミーティング要求が許可/拒否された際、ミーティング要求に対する応答の送信を強制的に行う
このオプションを使用すると、クライアントがミーティング要求に対して、許可や拒否、その他のアクションを選択した際、ミーティング要求に対する応答を開催者へ送信します。これは、こうした更新情報を自動送信する事ができない特定のクライアント用の機能です。

有効な設定をプレビュー

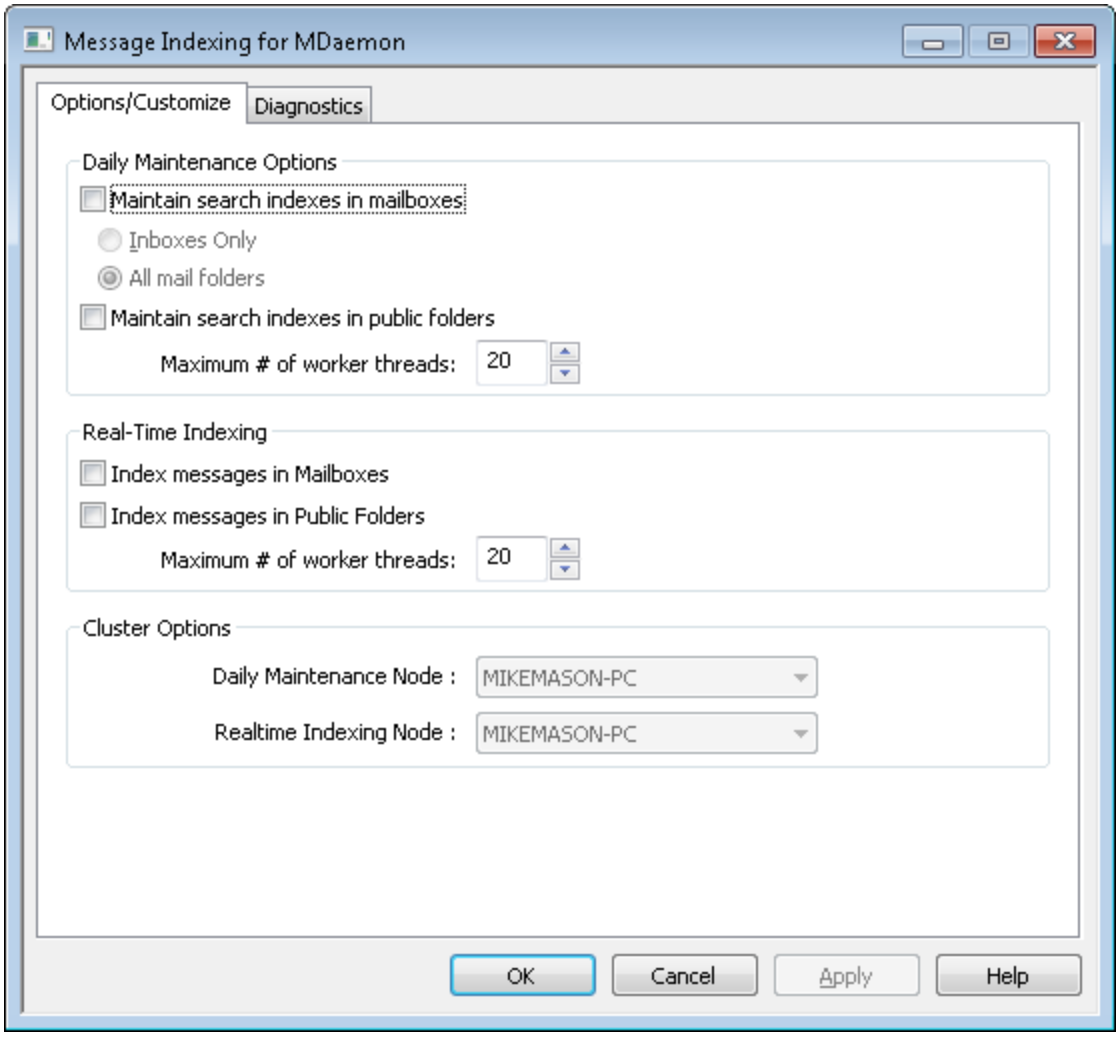
このボタンは全てのクライアント設定（ドメイン397, アカウント413, クライアント422）に対して使用できます。画面のオプションはデフォルト値をその上位の画面から引き継いでいるため、この機能は表示されている画面の現在の設定確認を行う際にもご利用頂けます。

See:

ActiveSync » Accounts413
ActiveSync » Clients422
ActiveSync » Security391

3.11 メッセージインデックス

3.11.1 オプション/カスタイズ



メッセージインデックスダイアログはWebmail、ActiveSync、Remote Administrationで使用する検索インデックスのリアルタイム又は夜間処理を管理するのに使用します。

日次メンテナンスオプション

このセクションのオプションは夜間の検索インデックスの設定に使用します。

メールボックスの検索インデックスの調整

メールボックスフォルダの検索インデックスを調整する場合はこのチェックボックスを有効にします。これは1つのインボックスか全てのメールフォルダを選択できます。

パブリックフォルダの検索インデックスの調整

パブリックフォルダ 283 の検索インデックスを調整する場合はこのチェックボックスを有効にします。ここでは同時処理を許可する最大数の指定も行えます。

リアルタイムインデックス

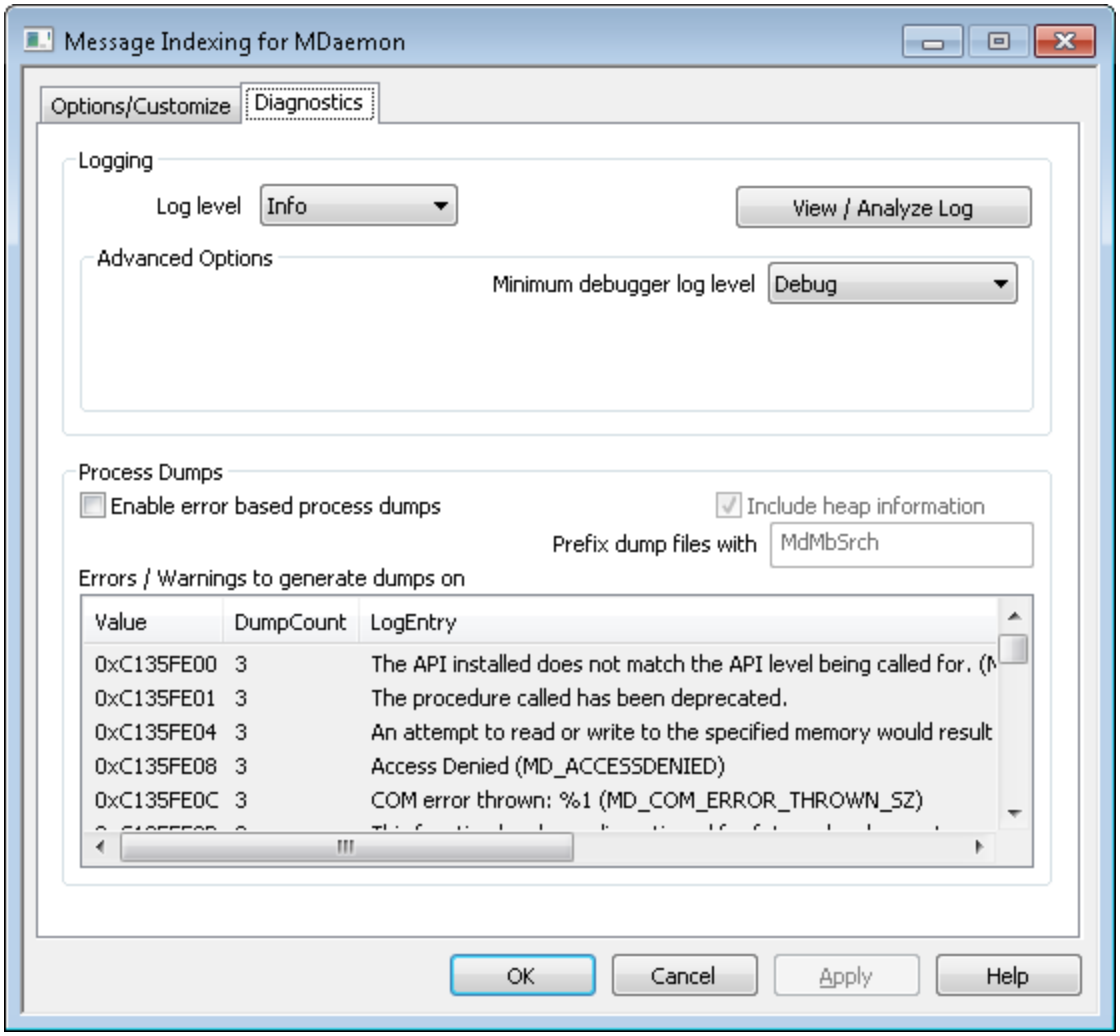
メールボックスのメッセージをインデックス
メールボックスのリアルタイムの検索インデックスを実施する場合はこのオプションを有効にし、検索インデックスを常に最新の状態にします。

パブリックフォルダのメッセージをインデックス
パブリックフォルダ[283]のリアルタイムの検索インデックスを実施する場合はこのオプションを有効にします。

クラスターオプション

クラスターを使用している場合は、このオプションを使い日次インデックス調整やリアルタイムインデックスを行うクラスターノードを指定する事ができます。

3.11.2 診断



ここでは、メッセージインデックスの問題分析や技術サポート等で依頼された場合などを除き、ほとんど調整の必要がない詳細設定を行えます。

ロギング

ログレベル

ログデータ量に応じた、6つのレベルのログに対応しています。

デバッグ 最も詳細なログで、記録できる全ての情報が含まれており、問題の診断にのみ使用されます。

情報 通常のログで、一般的な操作が詳細なしで記録されます。これはデフォルトのログレベルです。

警告 警告、エラー、クリティカルエラー、起動と終了がログに記録されます。

エラー エラー、クリティカルエラー、起動と終了がログに記録されます。

クリティカル クリティカルエラー、起動と終了がログに記録されます。

なし 起動と終了だけがログに記録されます。

ログの表示/分析

このボタンをクリックすると、MDaemon詳細システムログビューアが起動します。デフォルトでログは"..\MDaemon\Logs\"へ格納されます。

詳細ログオプション

最小デバッガーログレベル

デバッガー向けの最小ログレベルを指定します。使用できるログレベルは上記と同じです。

プロセスダンプ

エラーを元にしたプロセスダンプを有効化
下記で指定した特定の警告やエラー発生時プロセスダンプを生成するにはこのオプションを有効化します。

ダンプファイルへヒープ情報を含む
デフォルトで、ヒープ情報はプロセスダンプへ含まれます。含まない場合はチェックボックスをクリアしてください。

ダンプファイルの頭文字
プロセスダンプのファイル名はここで指定した文字から始まります。

ダンプファイルを生成するエラー/警告
右クリックして、エントリを追加/編集/削除...オプションをクリックし、プロセスダンプの生成のトリガーとするエラーや警告の管理を行います。各エントリではディアクティベートまでのプロセスダンプ

の数を指定する事ができます。

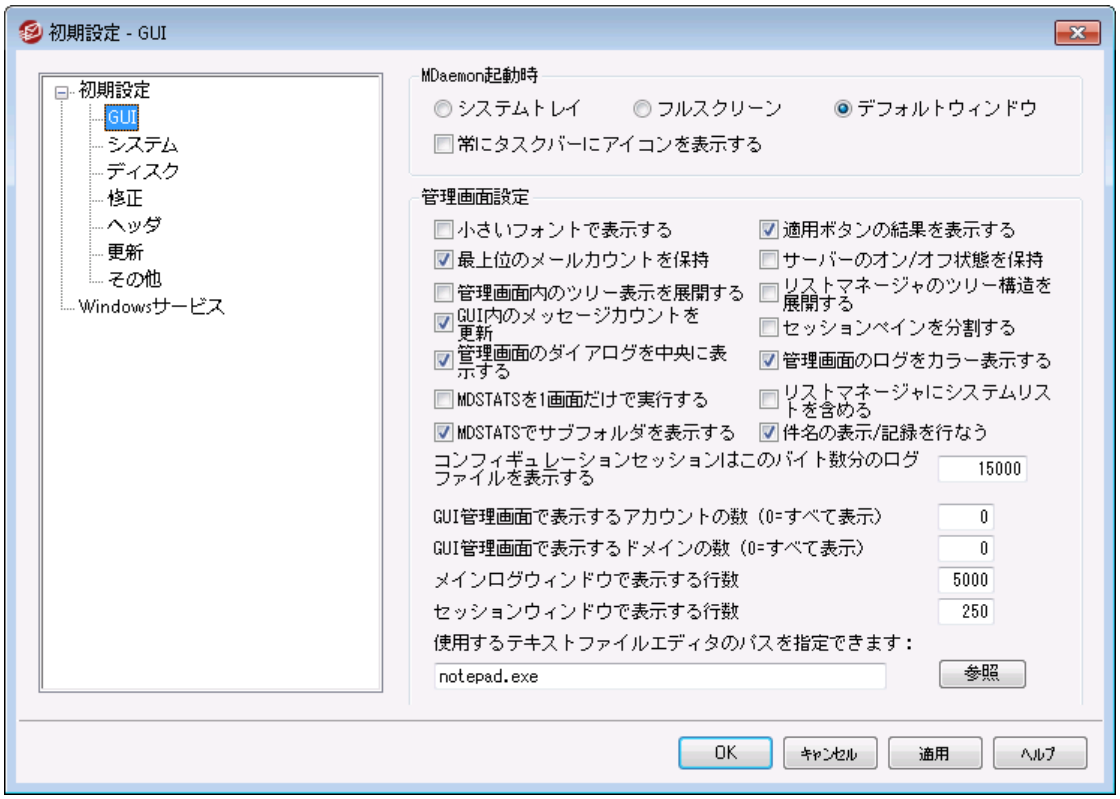
参照:

ダイナミックスクリーニング ≫ オプション/カスタマイズ 556

3.12 初期設定

3.12.1 初期設定

3.12.1.1 GUI



MDaemon起動時

...システムトレイ
MDaemonを最小化の状態で起動する場合は、このオプションを選択してください。MDaemonアイコンはシステムトレイに現れます。

...フルスクリーン
MDaemonを最大化の状態で起動する場合は、このオプションを選択してください。

...デフォルトウィンドウ
MDaemonの画面をデフォルトのウィンドウとして起動する場合は、このオプションを選択してください。

常にタスクバーへアイコンを表示
このオプションが有効な場合、MDaemonは最小化の状態で起動され、タスクバーとシステムトレイにアイコンが表示されます。最小化した時にWindowsのタスクバーにMDaemonのアイコンを表示しない場合は、このチェックボックスを解除してください。トレイアイコンのみが表示されるようになります。

管理画面設定

小さいフォントで表示する
イベントトラッキングとセッションのウィンドウで、スモールディスプレイフォントを使用します。

適用ボタンの結果を表示する
デフォルトで、ダイアログの適用ボタンをクリックするとき、ダイアログの設定の保存を確認するメッセージボックスを表示します。このメッセージボックスの表示をしないで変更を適用する場合は、チェックボックスを解除します。

最上位でのメールカウントを保持
サーバを再起動後にルートノードのカウンタの値を保持する場合は、このオプションを有効にしてください。ルートノードのカウンタはMDaemonのメイン画面の[統計]画面にある[統計]セクションに表示されます。

サーバのオン/オフ状態を保持

サーバを再起動後にサーバーの状態(オン又はオフ)を保持する場合は、このオプションを有効にしてください。

管理画面内のツリー表示を展開する
様々なダイアログで使っている画面左側のナビゲーションツリーを自動で展開したい場合はこの設定を使用します。この設定はメーリングリストマネージャ[245]には適用されません。メーリングリストのツリーを自動展開するには、後述の*リストマネージャのツリー状態を展開する*を使用します。

リストマネージャのツリー状態を展開する

メーリングリストマネージャ[245]の左側にあるナビゲーションの階層を自動で展開するにはこのチェックボックスを有効にします。

GUI内のメッセージカウントを更新
このオプションはMDaemonがディスクのメールキューにあるメールをカウントするかどうかを指定するためのものです。

セッションペインを展開
MDaemonの管理画面GUIのセッションタブを他のタブとは別で表示したい場合はこのオプションを有効にして下さい。この設定変更にはMDaemon管理画面の再起動が必要で、画面を切り替えるためのWindowsメニューは使用できなくなります。

管理画面のGUIを中央に表示する
デフォルトで全てのダイアログは互いに重なるのではなく画面の中央に表示されています。ダイアログを重ねて表示するにはこのオプションを無効にしますが、これにより部分的に画面やフレームからGUIがはみ出す場合があります。

管理画面のログをカラー表示する
MDaemon GUIのイベントトラッキングとロギング[65]タブのテキストをカラー表示するにはこのオプションを使用します。これはデフォルトで有効になており、設定の変更を適用するにはMDaemon設定画面の再起動が必要です。セッションログのカラー表示[163]で詳細を確認して下さい。

リストマネージャにシステムリストを含む
メーリングリストマネージャ[245]へMDaemonのシステムで自動生成されたメーリングリスト(例:Everyone@ やMasterEveryone@)を含むにはこのオプションを有効にします。このオプションが無効の場合は、システムアカウントは非表示になりますが、このアカウントの使用は行えます。このオプションはデフォルトで無効になっています。

MDSTATSを一画面のみで実行する
一度に起動できるMDaemonのキューと統計マネージャ[804]のコピーを1つのみにしたい場合はこのチェックボックスを有効にします。マネージャを稼働中に起動させると、現在稼働しているインスタンスがアクティブウィンドウとして表示されるようになります。

MDSTATSでサブフォルダを表示する
キューと統計マネージャ[804]で様々なキューやユーザーのメールキューを含むサブフォルダを表示させるにはこのチェックボックスを有効にします。

件名の表示/ログ
デフォルトでSubject: 行のデータはMDaemon UIへ表示され、ログファイルへ書き込まれます。ただし、Subject:行にはメール送信者にとって表示されたりログへ残したくないものである事もあり、また、メーリングリストの場合はSubject:行にパスワードを入力する場合もあります。そのため、このオプションは無効化する事をお勧めします。

コンフィギュレーションセッションにはこのバイト数分のログファイルを表示する
コンフィギュレーションセッション実行時、イベントトラッキングとロギング[65]タブに表示すうr最大ログデータをここで指定します。デフォルト設定は15000バイトです。

GUI管理画面で表示するアカウントの最大数(0=すべて表示)
これは、様々なダイアログのドロップダウンリストに表示されるアカウントの最大数です。さらに、このコントロールの値が0(ゼロ)(=すべてを表示)以外に設定されている場合、[**アカウントの編集**]と[**アカウントの削除**]オプションはアカウントメニューに表示されません。これらの機能は、アカウントマネージャ[648]から利用できるだけです。このコントロールへの変更を反映させるには、MDaemonを再起動する必要があります。デフォルトはゼロで表示するすべてのカウントに影響します。

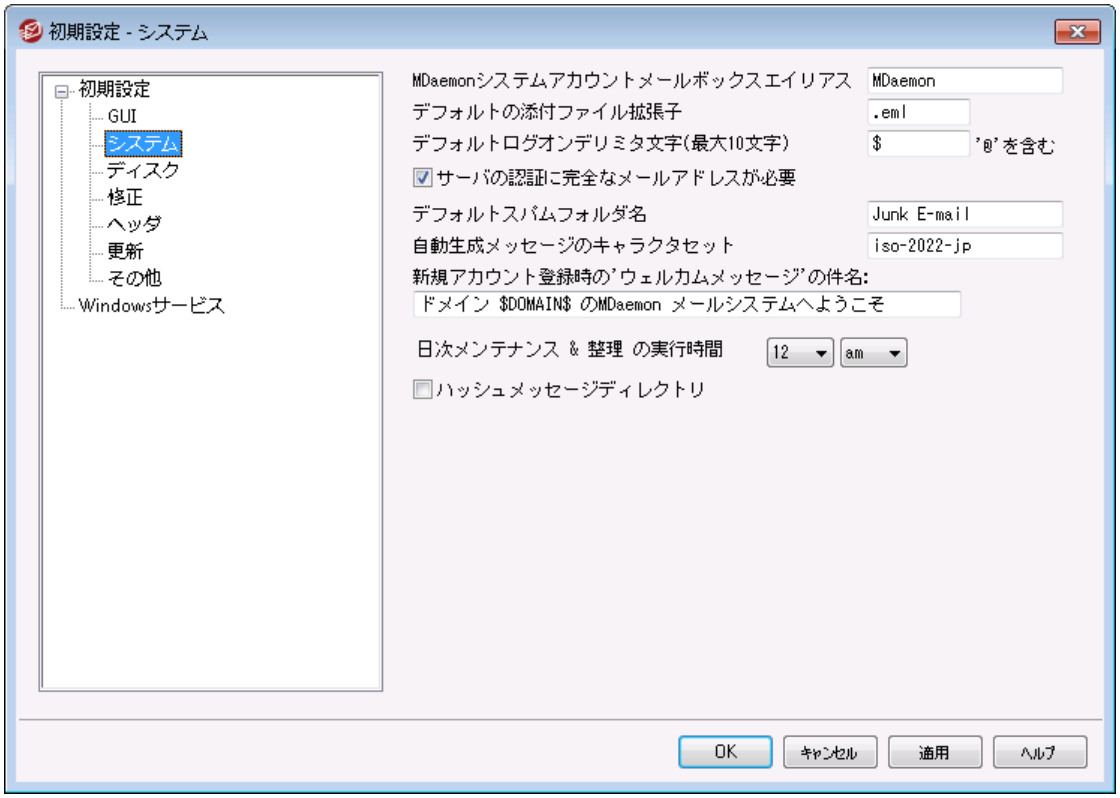
GUI管理画面で表示するドメインの数(0=すべて表示)
これは、実際に使用しているドメインの数に関わらず、メイン画面のツールウィンドウに表示されるドメインの最大数です。この値を変更した後、反映させるには、MDaemonを再起動しなければなりません。デフォルトはゼロで、すべてのドメインを表示します。

メインログウィンドウで表示する行数
これはメイン画面のログウィンドウに表示される行数の最大値です。行数がこの値に達すると、ウィンドウはクリアされます。これはログファイルには影響せず、表示のみがクリアされます。

セッションウィンドウで表示する行数
これは、セッションウィンドウ[77]に表示される行数の最大値です。これはログファイルには影響しません。

使用するテキストエディタのパスを指定できます
Notepad.exeは必要に応じてMDaemonがデフォルトで使用するテキストエディタです。他のテキストエディタを使用するにはここで実行ファイル名のパスを指定します。

3.12.1.2 システム



MDaemonシステムアカウントメールボックスエイリアス[アドレス]
これはシステムメッセージが届くメールアドレスです。購読の確認メッセージ、[配送できなかった(DSN)]というメッセージ、様々な通知メッセージはシステムメッセージです。

デフォルトの添付ファイル拡張子
システムメッセージは、この拡張子を使用して作成されます。また、これはシステムメッセージに含まれる添付ファイルに使用される拡張子でもあります。例えば、MDaemonが特定のメッセージついて警告メッセージをPostmasterに送信すると、警告メッセージは、その特定のメッセージを指定した拡張子で添付します。

デフォルトログオンデリミタ文字(最大10文字)
アカウントログオンパラメータとしてメールアドレスを使用するとき、@に代わる文字あるいは文字列を使用することができます。これは、ログオンフィールドで@をサポートしないメールクライアントを使用しているユーザにとって必要な機能です。例えば、このフィールドで$を指定した場合、ユーザは"user$example.com"あるいは"user@example.comのどちらかを使用してログオンすることができます。

サーバの認証に完全なメールアドレスが必要
デフォルトで、MDaemonのPOPやIMAPサーバ認証には、ログオン名としてメールアドレスが必要です。メールボックス名だけのログイン(例えば、user1@example.comの"user1")を使用する場合はこのオプションを無効にして下さい。ただし、MDaemonで複数ドメインを使用している場合は、メールボックス名でのログインは紛らわしいので推奨していません。

デフォルトスパムフォルダ名
このテキストボックスにはMDaemonユーザ用のスパムフォルダを自動作成する際のデフォルト名を指定します。デフォルトの設定は[Junk E-mail]であり、広く使用される製品でのデフォルト設定値と同じです。

自動生成メッセージのキャラクタセット
自動生成されるメッセージに使用するキャラクタセットを指定してください。デフォルト設定は日本語版ではISO-2022-jpです。

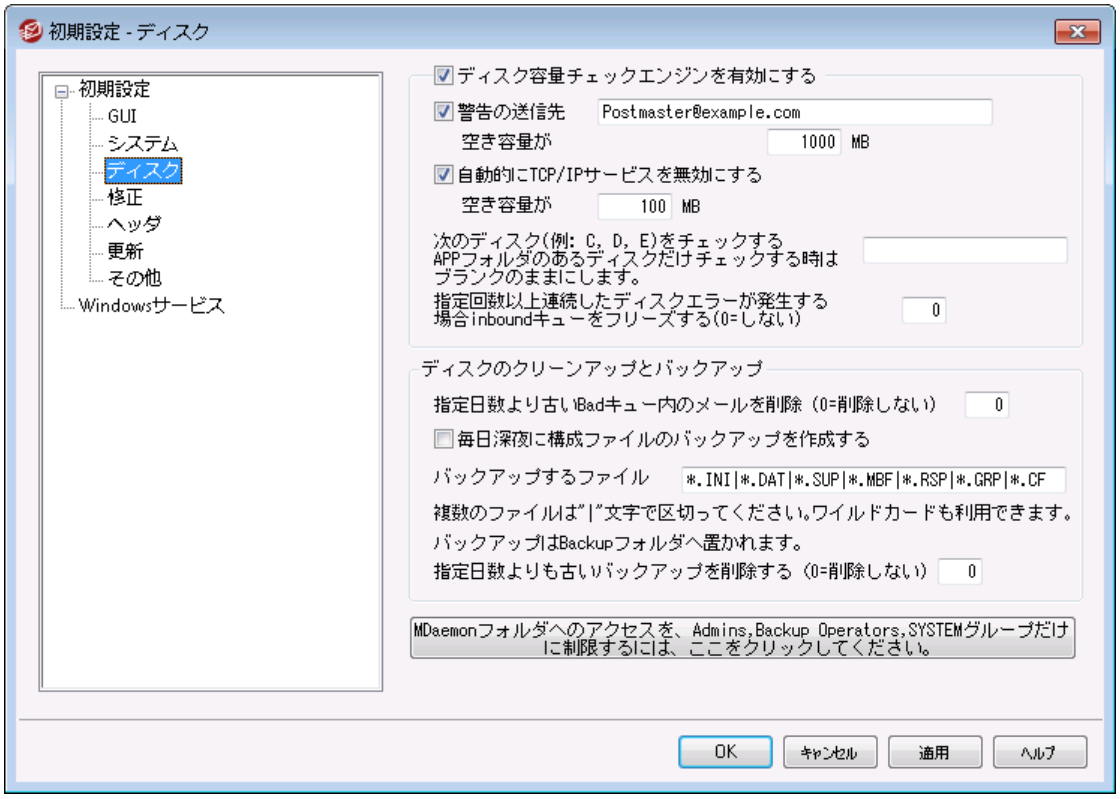
新規アカウント登録時のウェルカムメッセージの件名:
MDaemonは、通常は新規のアカウントに"ようこそメッセージ"を送信します。ここへ指定されるテキストは、メッセージの"Subject"ヘッダに現れます。このメッセージは…/MDaemon/app/フォルダで含まれるNEW USERHELP.DATファイルから作成されます。このSubjectヘッダには自動応答スクリプト 766で許可されているマクロも使用できます。

日次メンテナンス&整理の実行時間 [1-12] [am/pm]
日次メンテナンスと整理を行う時間を選択します。デフォルトであり推奨設定は12pmです。

設定した時間に拠らず、ログファイルのメンテナンスやmidnight.datの実行といった処理は常に深夜に行われます。

ハッシュメッセージディレクトリ
ディレクトリのハッシュ値を有効にする場合は、このチェックボックスを有効にしてください。MDaemonでは、最大65のサブディレクトリのハッシュ処理を行います。このハッシュは、特定の大規模サイトでパフォーマンス向上を望めますが、逆に典型的なMDaemonサイトでは、多少パフォーマンスが落ちることがあります。このオプションはデフォルトでは無効になっています。

3.12.1.3 ディスク



ディスク容量チェックエンジンを有効にする
このチェックボックスを有効にすると、MDaemon.exeが置かれたドライブのディスク容量の監視を行ないます。

空き容量が [xx] MB以下になったら [ユーザーまたはメールアドレス] へ通知する
このオプションでは、ディスクの空き容量として確保したいサイズの指定と、それを下回った際の警告メッセージの送信先をユーザー名かメールアドレスで指定することができます。デフォルト値は1000MBです。

空き容量が [xx] MB以下になったら自動的に TCP/IPサービスを無効にする
空き容量がここでの値を下回るとMDaemonはTCP/IPサービスを自動的に無効にします。TCP/IPサービスの停止は、空き容量不足によるシステム全体が不安定になることを防ぐために行ないます。デフォルトは100MBです。

次のディスク(例:C,D,E)をチェックする
このオプションを使用することで、ここで指定した複数のドライブ上の使用可能容量の監視を行えます。もし、ブランクの場合には、MDaemonの¥app¥フォルダが格納されたドライブだけがチェック対象となります。

指定回数以上連続したディスクエラーが発生する場合、inboudキューをフリーズする(0=しない)
ここで指定した回数ディスクエラーが発生する場合、MDaemonはその状況が解消されるまでinbound キューを停止させます。これは信頼できない状態のディスクでメールを受信して、メールが紛

失することを防ぐためです。この状態が発生した際には、postmasterのメールボックスへエラーが発生した旨のメールを配置します。

ディスクのクリーンアップとバックアップ

毎日深夜にBADメッセージキューのメッセージすべてを削除する
このチェックボックスを有効にすると、MDaemonは毎日深夜にBADメッセージキューのすべてのファイルを削除し、ディスク容量の節約を行ないます。

毎日深夜に構成ファイルのバックアップを作成する
このチェックボックスを有効にすると、毎日深夜にMDaemonの構成ファイルを Backup ディレクトリーへ保存します。

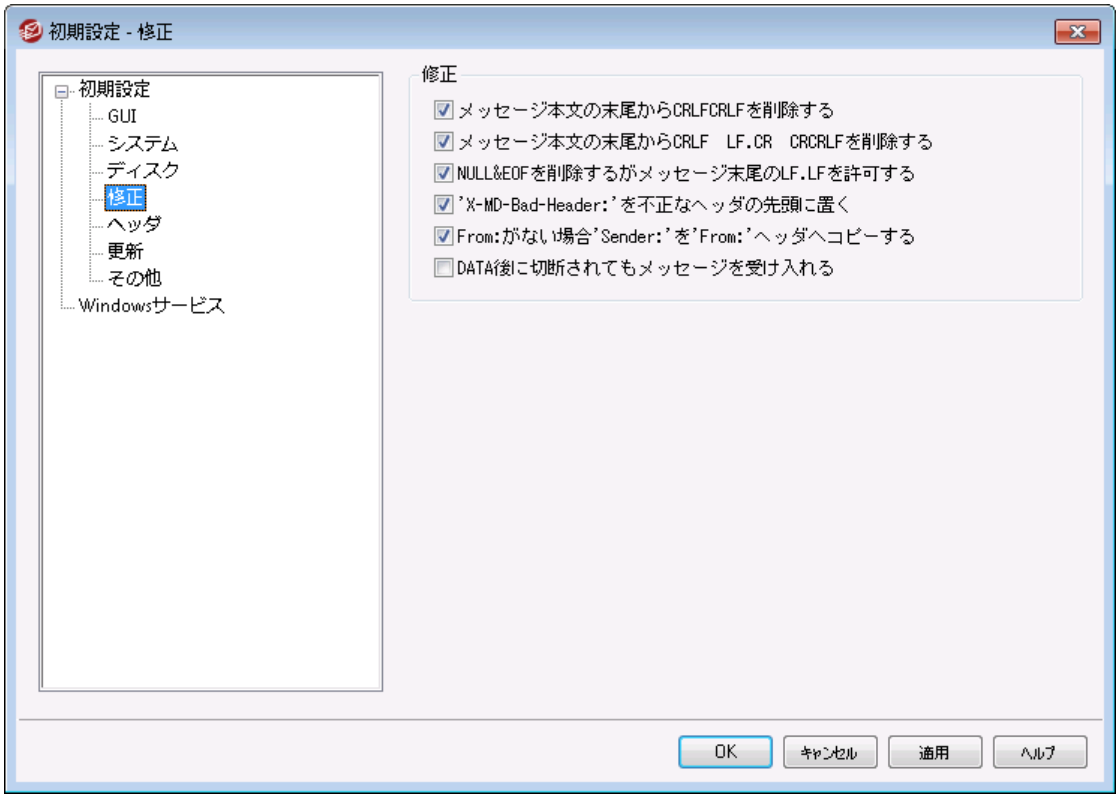
バックアップするファイル
このテキストボックスでは、バックアップ対象となるファイルの拡張子を指定します。ワイルドカードの使用も可能で、ファイル名や拡張子は"|"で区切り指定します。

この日数より古いファイルを削除 (0=削除しない)
古いバックアップファイルを自動削除するのにこのオプションを使用します。この日数より古いファイルは深夜のクリーンアップ処理で自動削除されます。デフォルト値は0で古いバックアップファイルは削除されません。

MDaemonフォルダへのアクセスを Admins, Backup Operators, SYSTEM グループだけに制限する

このボタンをクリックすると、¥MDaemon¥ ルートフォルダとそのサブフォルダへのアクセスを次の Windowsのアカウント/グループ(Administrators, Backup Operators, and SYSTEM)だけに制限することができます。

3.12.1.4 修正



メッセージ本文の最後からCRLFCRLFを削除する
inboundキューを処理するとき、指定回数のディスクエラーが発生する場合、状態を解決するまでMDaemonでキューの処理を停止します。このシャットダウンが発生する時に、メールはpostmasterのメールボックスに配置されます。

メッセージ本文の最後からCRLF LF.CR CRCRLFを削除する
一部のメールクライアントに問題を引き起こす可能性があるので、デフォルトで、メッセージの終わりからこのシーケンスを除去します。メッセージから、このシーケンスを取り除かない場合、このチェックボックスの選択を解除します。

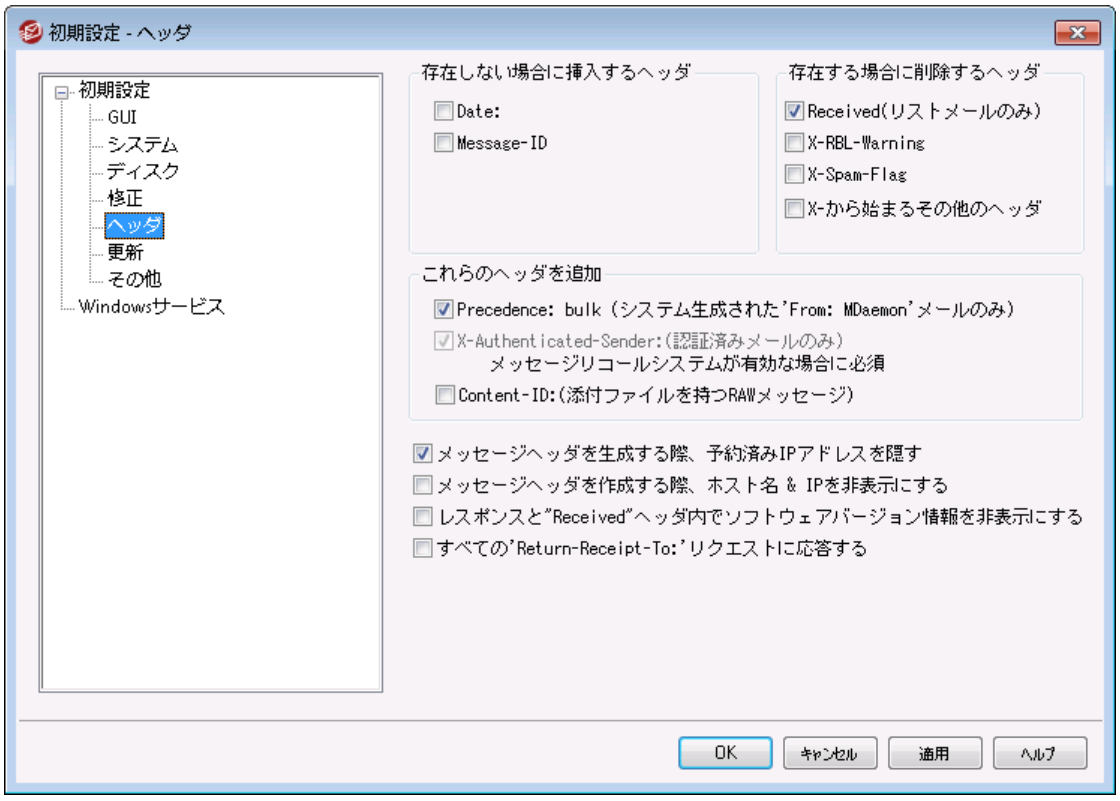
NULL & EOFを削除しメッセージの最後にLF.LFを許可する
このチェックボックスを選択する時に、メッセージ本文の終わりからNullおよびEOF文字を削除しますが、メッセージがLFで.LFメッセージの終わりを意味する通常のCRLF .CRLFシーケンスによるメッセージ終了と同様に終わるのを許可します。このオプションは、デフォルトで有効です。

"X-MD-Bad-Header:" ヘッダを違法なヘッダの先頭につける
このオプションが有効な場合に不正なメッセージヘッダを受信すると、MDaemonは"X-MD-Bad-Header:"をプレフィックスとして配置します。このオプションはデフォルトで有効です。

'From:'が存在しない場合'Sender:'を'From:'へコピーする
一部のメールクライアントでは、メッセージを構成する際にFROM:ヘッダの作成に失敗する場合があります。代わりに、FROM:フィールドの情報が、Sender:ヘッダに置かれます。これはメールサーバおよびメッセージの受信者を混乱させます。このスイッチを選択すると、MDaemonはSender:ヘッダのアドレスを使用して、欠けているFROM:ヘッダを作成します。このオプションはデフォルトで有効です。

DATA後に切断されてもメッセージを受け入れる
セッションがSMTPプロセス中DATAコマンド実行中または直後に中止される場合でも、MDaemonはメッセージを受け入れ配信します。これは、通常は使用する必要のないオプションで、有効にすることで受信メッセージの重複が発生する可能性があります。

3.12.1.5 ヘッダ



存在しない場合、これらのヘッダを挿入

日付
このオプションが有効な場合、Date: ヘッダを持たないメッセージを受信すると、MDaemonでは"Date: "ヘッダを作成し、そのメッセージファイルに追加します。追加される日付はMDaemonが最初にそのメッセージを受信した日であり、メッセージが送信者によって作成された日ではありません。このヘッダを作成しないメールクライアントがいくつか存在し、そのようなメッセージの受付を拒否するメールサーバも存在するので、この機能によって配信が可能になります。

Message-ID
"Message-ID"ヘッダを持たないメッセージに遭遇すると、MDaemonはランダムに"Message-ID"ヘッダを作成し、それをメッセージに挿入します。

存在する場合、ヘッダを削除

Received (リストメールのみ)
すべての既存の"Received: "ヘッダをメーリングリストメッセージから取り除く場合、このボックスを選択します。

X-RBL-Warning
メッセージに存在する、すべての"X-RBL-Warning:"ヘッダを取り除く場合は、このチェックボックスを選択します。デフォルトでは、この機能は有効ではありません。

X-Spam-Flag
メッセージから古い"X-Spam-Flag:"ヘッダを取り除く場合は、このオプションを有効にしてください。

X-で始まる全てのヘッダ
MDaemonと他のメールサーバは、メールの経路設定、他の機能を実行するためにX-Typeヘッダと呼ばれている多くのサーバ特定のヘッダを使用します。このオプションを有効にすると、MDaemonはメッセージからこれらのヘッダを取り除きます。注意:この機能は X-RBL-Warning ヘッダは削除しません。このヘッダを削除するには、上記のX-RBL-Warningを使用して下さい。

これらのヘッダを追加

Precedence: bulk (システムで生成した「From: MDaemon」のメールのみ)
システムが生成したすべてのメッセージ(挨拶文、警告、[配信できませんでした]メッセージなど)にPrecedence: bulkヘッダを挿入する場合は、このオプションをクリックしてください。

X-Authenticated-Sender: (認証したメールのみ)
デフォルトで、AUTHコマンドを使用して認証されたセッションで受信されたメッセージに、"X-Authenticated-Sender:"ヘッダを追加する場合は、このオプションをクリックしてください。このヘッダを追加しない場合は、選択を解除します。

Content-ID: (添付ファイルを持つRAWメッセージ)
添付ファイルを含むRAWメッセージに、一意のMIME Content-IDヘッダを追加する場合、このオプションを選択してください。

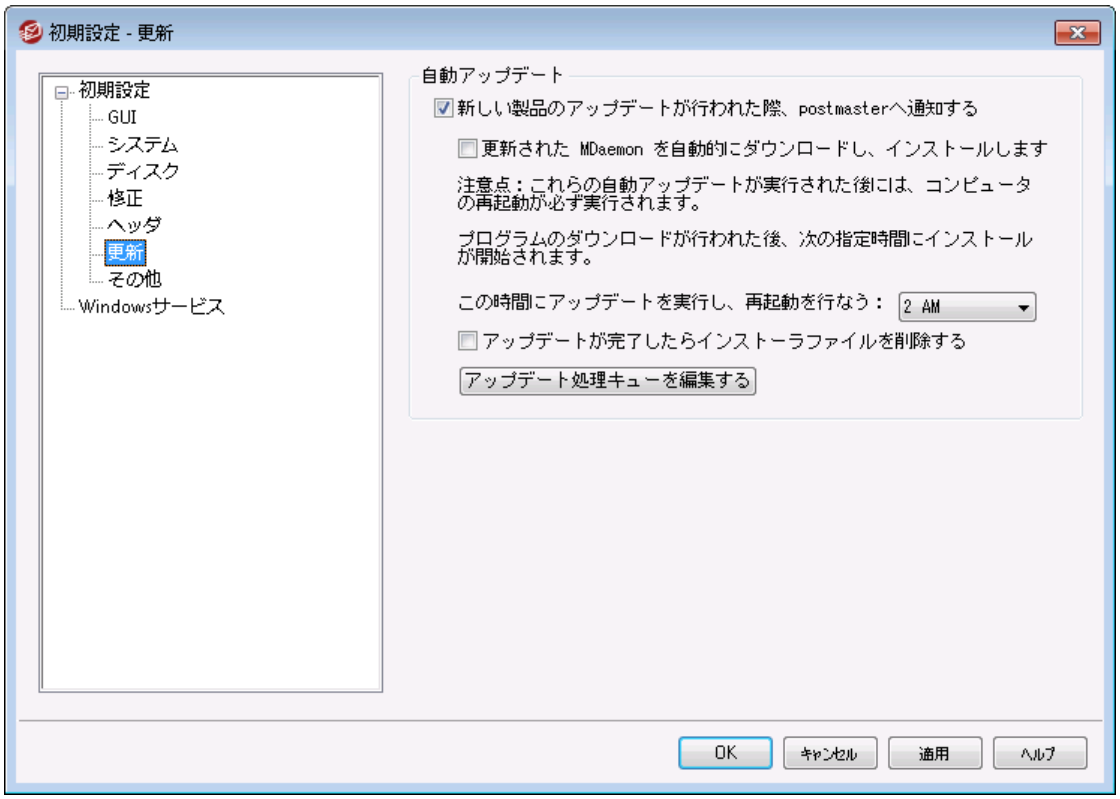
メッセージヘッダ作成時予約済IPを隠す
このオプションはデフォルトで有効となっており、MDaemonがメールヘッダを作成した際予約済IPアドレスが表示されないように設定されています。予約済IPには次のようなIPが含まれます:
127.0.0.*, 192.168.*.*, 10.*.*.*, 172.16.0.0/12。(LANドメインを含む)ドメインIPをヘッダに表示されないようにするにはMDaemonのapp¥MDaemon.iniの次のスイッチを手動で設定して下さい: [Special] HideMyIPs=Yes (デフォルトはNoです)

メッセージヘッダ作成時ホスト名とIPを隠す
メール作成時Received:ヘッダからホスト名やIPアドレスを隠す場合はこのオプションをクリックします。このオプションはデフォルトで無効になっています。

'Received:'ヘッダの応答でソフトウェアバージョンの識別情報を隠す
MDaemonがReceivedヘッダの応答生成時や他の様々なプロトコルへの応答でソフトウェアバージョンを隠すようにするにはこのオプションを使用します。このオプションはデフォルトで無効になっています。

すべての'Return-Receipt-To:'リクエストに応答する
このオプションを有効にすると、受信メッセージから配信確認を要求された場合、確認メッセージを送信者に送ります。このオプションはデフォルトでは無効です。

3.12.1.6 更新



自動更新

自動更新機能を使用すると、MDaemonの更新プログラムが利用できるようになった際postmasterへ通知し、自動的に更新プログラムをダウンロードしてインストールするよう設定が行えます。更新プログラムが自動的にインストールされるたびにサーバーは常に再起動されます。アップデートが検出されるとファイルがダウンロードされますが、インストールと再起動は、次回指定した時間で実行されます。すべてのインストールアクティビティがMDaemonシステムログに記録され、更新が行われた後にpostmasterに通知されます。

新しい製品のアップデートが行われた際、postmasterへ通知する
このオプションを使うと、MDaemonの最新バージョンが利用できる事をpostmasterへ通知します。このオプションはデフォルトで有効です。

MDaemonの自動アップデートを行うよう設定していると、通知は送信されません。代わりに、最新バージョンがインストールされた事と、最新バージョンの特記事項についてpostmasterへ通知されます。

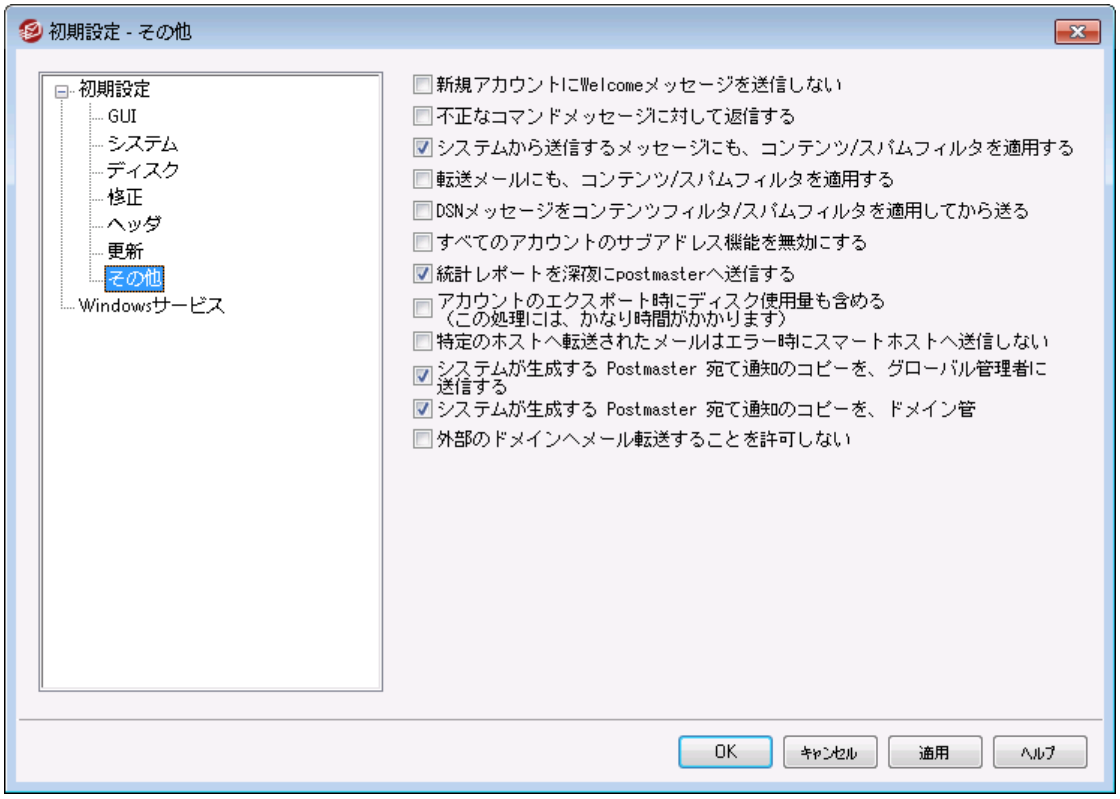
更新されたMDaemonを自動的にダウンロードし、インストールします
MDaemonの最新バージョンの自動インストールを行う場合はこのオプションを有効にします。最新バージョンを見つけると、インストーラーが自動的にダウンロードされますが、インストールと再起動は、指定した時間に実行されます。このオプションはデフォルトで無効に設定されています。

この時間にアップデートを実行し、再起動を行う:
自動アップデートは最新バージョンを見つけるとすぐにダウンロードされ、\MDaemon\Updatesフォルダへ格納されますが、インストールはここで指定した時間まで実行されません。MDaemonがインストールされたサーバーはアップデートを実行する度に再起動されます。このオプションはデフォルトで2 AMに設定されています。

アップデートが完了したらインストーラファイルを削除する
アップデートが完了したらインストーラーファイルを削除するには、このオプションをチェックして下さい。

アップデート処理キューを編集する
アップデートがダウンロードされると、後に実行するインストール用にキューへ配置されます。処理待ちのアップデートはQueuedUpdates.datへ書き込まれます。このボタンをクリックすると、一覧の確認や処理待ちのアップデートの削除が行えます。

3.12.1.7 その他



新規アカウントへWelcomeメッセージを送信しない
デフォルトでは、新規ユーザアカウントが作成されると、MDaemonはNEWUSERHELP.DATの内容を新規ユーザアカウントへ配信します。このメッセージの送信をしない場合は、このチェックボックスを選択してください。

無効なコマンドに対するメッセージを送信
デフォルトでは、システムアカウント宛に有効なコマンドが含まれていないメッセージが送信されても、有効なコマンドが含まれていなかった事を、MDaemonが通知する事はありません。こうしたメールを送信したい場合には、このオプションを有効にして下さい。

システム生成メッセージにも、コンテンツ/スパムフィルタを適用する
デフォルトでは、システムの自動作成されたメールはコンテンツフィルタやスパムフィルタ経由で送信されます。コンテンツフィルタやスパムフィルタから除外する場合は、チェックボックスを解除します。

転送メールにも、コンテンツ/スパムフィルタを適用する

転送メールをコンテンツフィルタやスパムフィルタ経由で送信するにはこの設定を有効にします。これはデフォルトで無効になっています。

DSNメッセージはコンテンツフィルタやスパムフィルタを通して送信
DSNメッセージ[801]をコンテンツフィルタやスパムフィルタ経由で送信するにはこのオプションを有効にします。このオプションはデフォルトで無効になっています。

すべてのアカウントのサブアドレス機能を無効にする
全体にわたりサブアドレス機能を無効にする場合は、このオプションを選択してください。各アカウント設定に関係なく、サブアドレス機能は利用できません。詳細は、アカウントエディタのIMAPフィルタ[670]を参照してください。

統計レポートを深夜にpostmasterへ送信する
デフォルトで、毎日夜間処理の中で統計レポートがpostmasterへ送信されます。レポート送信を必要としない場合、このチェックボックスを解除します。 このオプションは、MDaemonのメイン画面にある統計[64]タブに対応します。

アカウントのエクスポート時にディスク使用量を含める(この処理にはかなり時間がかかります)
デフォルトでは、アカウントのエクスポート時、ファイル数やディスク使用量は含まれません。これらの情報を含みたい場合はこのオプションを有効にして下さい。ただし、この処理にはかなりの時間がかかる場合があります。

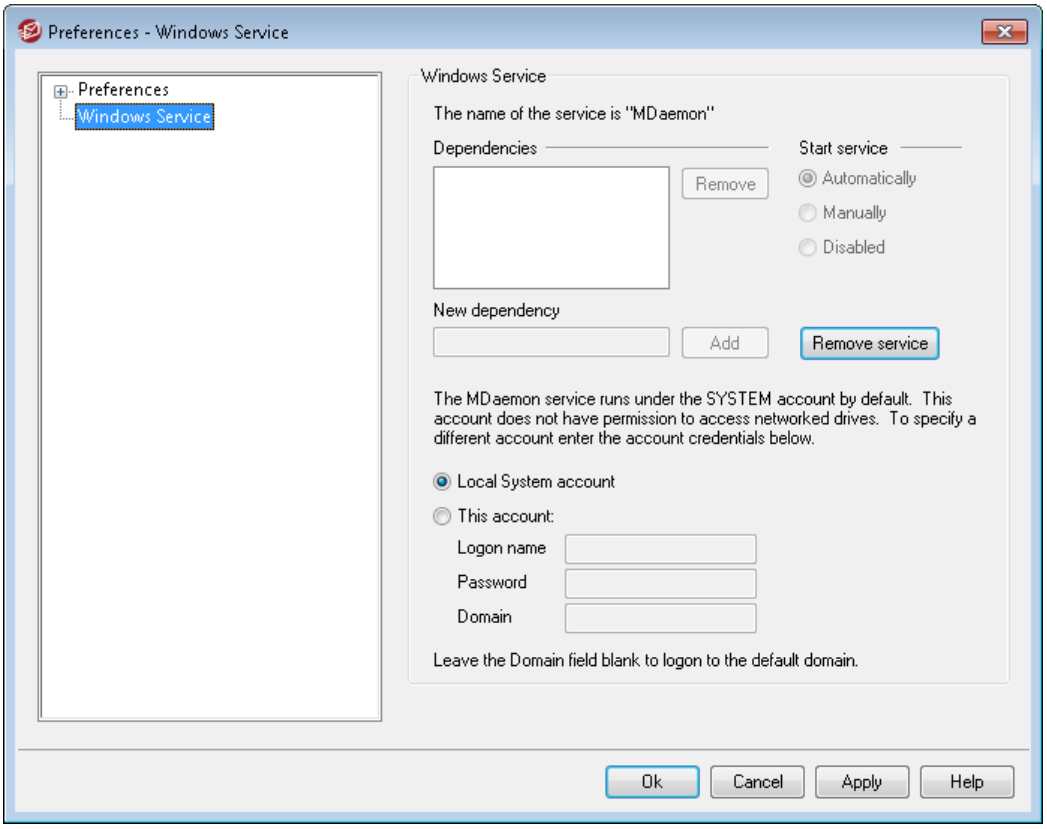
特定のホストへ転送されたメールはエラー発生時にはスマートホストへ送信しない
アカウントエディタの転送[663]画面にある「詳細転送設定」を使用し、アカウントはMDaemonの標準配送処理で使用するスマートホストではなく特定のホストに対してメール転送を行うよう設定できるようになります。デフォルトでは、MDaemonで配信エラーが発生すると、メールはbadキューへ配送されます。このオプションを使用するとMDaemonは通常の配信処理を使用してメールを配送するよう、badキューではなくRetryキュー[794]へメールを配送します。

システムが生成するPostmaster宛の通知のコピーをグローバル管理者へ送信
デフォルトで、Postmaster宛にシステムが生成する通知メールはグローバル管理者[690]へも送信されます。 グローバル管理者は、キューサマリレポート、統計レポート、リリースノート、(全ドメインの)No Such User、ディスクエラー通知、全てのドメインのアカウントの凍結や無効化通知(ドメイン管理者と同様、アカウントの凍結解除や再有効化に使用できます)、ライセンスの警告やテストバージョンの有効期限、スパムサマリレポート、等を受信します。グローバル管理者がこうした通知を受け取らないようにするには、この設定を無効にしてください。

システムが生成するPostmaster宛の通知のコピーをドメイン管理者へ送信
デフォルトで、Postmaster宛にシステムが生成する通知メールはドメイン管理者[690]へも送信されます。 ただし、ドメイン管理者の受信する通知は管理しているドメインのものに限定されます。ドメイン管理者がこうした通知を受け取らないようにするには、この設定を無効にしてください。

外部のドメインへメール転送する事を許可しない
アカウントの外部ドメインへのメール転送を許可しない場合はこの設定を有効にしてください。ユーザーが外部ドメインへのメール転送を設定した場合、転送先アドレスは無視されます。この設定はアカウントのメール転送オプション[663]を使った転送メールに対してのみ適用されます。

3.12.2 Windowsサービス



Windowsサービス

MDaemonをサービスとして実行している場合、サービス名は "MDaemon"となります。

依存関係

MDaemonサービスの開始よりも前に実行させたいサービスがある場合は、このオプションを使用します。

サービス開始

これは、サービスの初期状態で、自動、手動、停止の中から選択します。

サービスのインストール/削除

このボタンをクリックするとMDaemonのサービスがインストールまたは削除されます。

ネットワークリソースアクセス

MDaemonをシステムサービスとして実行している場合、デフォルトでは、システムアカウントで実行されます。このアカウントは、ネットワークデバイスへアクセスすることができないため、MDaemonは別のコンピュータにメールを保存する場合などに、データへアクセスすることができません。ネットワークを共有するマシンへアクセスするためには、MDaemonサービス用アカウントがネットワークへのログオン権限を持っている必要があります。こうした場合は、MDaemonの実行用に、Windowsのユーザアカウントを作成し、所属しているネットワークリソースへアクセスできるよう適切な権限を割り当てて下さい。なお、MDaemonアカウントによって起動する全てのアプリケーションは、同じ認証情報を使用します。

ログオン名
MDaemonサービスを実行するWindowsアカウントのログオン名です。

パスワード
Windowsアカウントのパスワードです。

ドメイン
アカウントが属するWindowsドメインです。デフォルトのドメインにログオンする場合は、このフィールドはブランクにしてください。

セクション 4

4 セキュリティメニュー

MDaemonは、セキュリティを管理するための機能を多数搭載しています。メニューバーのセキュリティから、以下の機能へアクセスできます。

- **AntiVirus** 587 － MDaemon Private CloudのAntiVirus機能を使うと、最新の統合セキュリティ機能によって、メール経由のウィルスからシステムを保護する事ができます。ウィルスを検知すると、これを捕獲し、隔離や修復、削除などの処理を行います。Outbreak Protection 583によって、従来のシグニチャを元にしたウィルスチェックでは対応できなかったスパムメールやフィッシングメール、未知のウィルスからもシステムを保護する事ができます。
- コンテンツフィルタ 588 － 柔軟性が高くマルチスレッドに完全対応したコンテンツフィルタをご利用頂く事で、送受信メールの内容に基づいて、サーバの動作をカスタマイズすることができます。メッセージヘッダの挿入や削除、フッタの追加、添付ファイルの削除、他ユーザへのコピーの配布、インスタントメッセージの送信、他のプログラムの実行を始め、様々な処理を行う事ができます。
- スパムフィルタ 616 － メールの「スコア」を継続的に検証するスパムフィルタリング技術を使用しています。このスコアはメールがスパムかどうかを判定するために使用され、このスコアに基づいてサーバーはメールの拒否やフラグの追加といった特定のアクションを実行する事ができます。参照: スパムトラップ 644
- DNSブロックリスト 638 メッセージをサーバに送信する場合、ブロックリストをチェックするDNSを指定することができます。接続IPが、このリストへ一致した場合、メッセージは拒否されます。
- リレー設定 466 － fromやtoにローカルアドレスを含んでいないメールが到着した際のMDaemonの動きをコントロールできます。
- IPシールド 474 － 一覧で指定されたドメイン名からの接続時、IPアドレスが割り当て済のものと同じかどうかを判断します。
- リバースルックアップ 468 － MDaemonは、メッセージが到着する間に報告されるドメイン名とアドレスの正当性を、DNSサーバに問い合わせることができます。この画面のコントロールは、怪しいメッセージを拒否、あるいはそのようなメッセージに特別なヘッダを挿入するために使用することができます。リバースルックアップのデータもMDaemonのログで報告されます。
- **POP Before SMTP** 471 － この画面のコントロールを使用することにより、各ユーザはMDaemonを通してメールを送信する前に、まず対象となるサーバにアクセスすることを要求されます。アクセスしたユーザは、有効なアカウントのユーザでありメールシステムを利用することが許されます。
- 信頼するホスト 472 － リレーコントロールで指定されたルールから除外するドメイン名とIPアドレスの一覧です。
- SMTP認証 476 － MDaemonに最初に認証する場合やそうでない場合に、どのように処理するかを設定する事ができます。
- **SPF** 479 － 多くのドメインはメールサーバーマシンのMXレコードを公開していますが、送信できる場所の識別を行う事はできません。Sender Policy Framework（SPF）は、MXの逆引きレコードの公開情報でメールの送信を許可するという手法です。
- **DomainKeys Identified Mail** 481 － DomainKeys Identified Mail（DKIM）はメールの認証システムで成り済ましを防ぐための手法の1つです。また、DKIMは受信メールのメールサーバーへ署名の照合を行う事で、メールの正当性を確認するためにも使用されています。この署名には公開鍵と秘密鍵による公開鍵認証が使われています。送信メールは秘密鍵を使った署名を付与され、受信メールは送信元のDNSサーバーが公開している公開鍵を使って、メール署名を検証します。
- 証明書 501 ー メッセージ証明は、正当なメールを第3者機関によって証明するのに使用されます。証明書は、メールが保証されないスパムフィルタ分析により、誤ってまたは不必要に影響を受けなくな

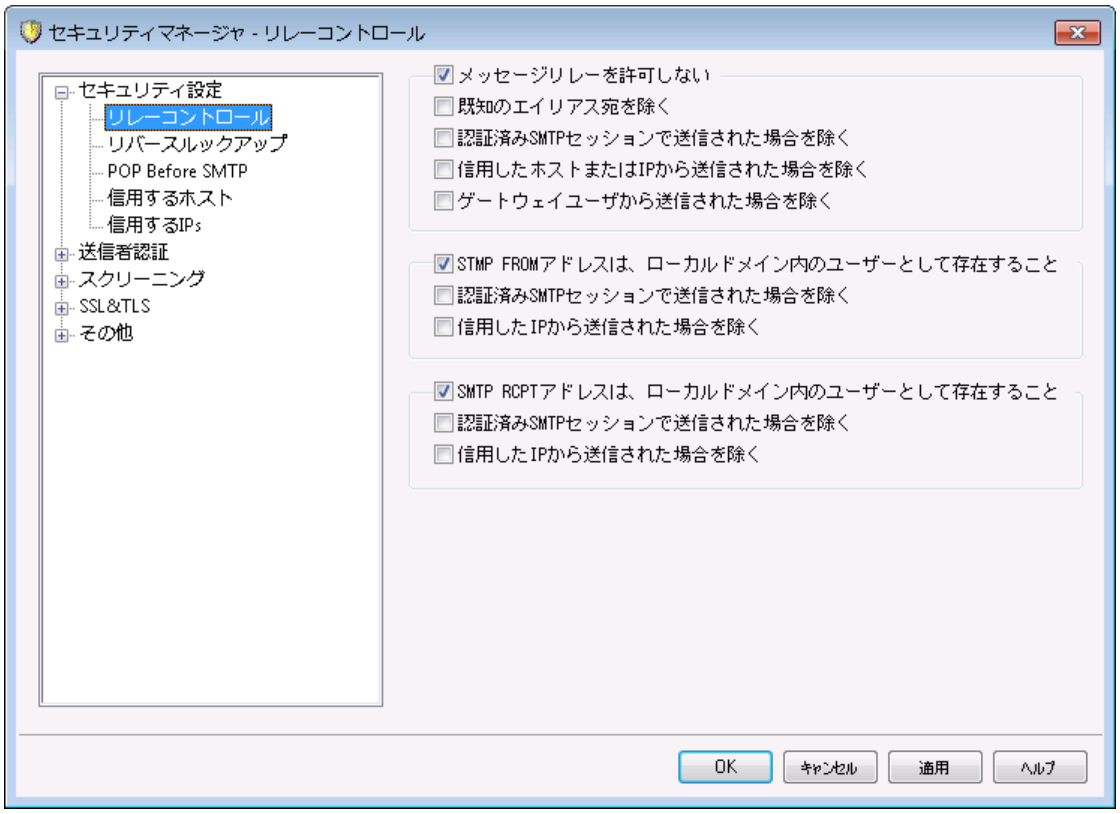
るため便利な機能です。また、各メッセージを処理するために必要とされるリソースを軽減するために便利です。

- 送信者ブロックリスト[507] ー サーバーからのメール送信を禁止しているアドレスの一覧です。
- IPスクリーン[510] ー サーバへの接続を許可または拒否するIPアドレスを指定します。
- ホストスクリーン[512] ー サーバへの接続を許可又は拒否するホスト(ドメイン名)を指定できます。
- **Dynamic Screening**[556] ー ダイナミックスクリーニング機能を使用して、MDaemonは送信サーバーによる疑わしい挙動を記録し、その状態によって動的に応答を返す事ができます。例えば、指定された時間内に認証失敗回数が最大数に到達した場合、(IPアドレス範囲か)IPアドレスをブロック[559]できます。また、認証回数が多すぎるアカウントに対してアカウントの凍結[559]も行えます。
- **SSL & TLS**[523] ー MDaemonはSMTP、POP、IMAP、そしてWebmailのSSL(Secure Sockets Layer)プロトコルに対応しています。SSLはサーバ/クライアント間のインターネット通信を安全に行うための標準プロトコルです。
- バックスキャッタ保護[543] ー 「バックスキャッタ」とは、送信した事のないメールに返信される、不達メッセージの事を意味します。これは、スパムやウィルスが偽造アドレスをReturn-Pathに含む事により発生します。バックスキャッタ保護は、ユーザーの送信メールのReturn-Pathへ、生成した秘密キーハッシュを有効期限付きで埋め込む事により、アカウントに対し、届くべき不達メッセージや自動応答メールのみを届ける機能です。
- 帯域幅調整[546] ー MDaemonによって使用される帯域幅の消費を監視することができ、進行中のセッションあるいはサービスの割合をコントロールすることができます。これによりMDaemonの主なサービスにおいてドメインやドメインゲートウェイも含むドメイン毎の設定が行えます。
- ターピット[548] ー 指定された数のRCPTコマンドをメッセージの送信者から受け取ると、意図的に接続速度を減速させることを可能にします。これは、スパムの送信者がサーバを利用して、大量のスパムメールを送信することを思いとどまらせる効果があります。このテクニックでは、スパムメールの送信者に対して、個々のメールの送信に関わる時間を長くかけさせることにより、彼らの意欲を減退させ、将来的にサーバを送信ターゲットから除外する目的があります。
- グレーリスト[550] ー グレーリストはSMTPサーバが一時的なエラーコード(例えば[再試行])を受けたメッセージの再配信を試みるという機能を悪用するスパムメールに対応するための技術です。この技術を使用すると、許可リストにない送信者や、未知の送信者からのメールについては、送信者、受信者、送信サーバのIPアドレスが記録され、SMTPセッション内で、一時的なエラーコードと共にグレーリストによって拒否されます。その後、正しく機能しているサーバから、数分後にメールが再送された場合、このメールは受信されます。スパマーは一般的に、メールの再送を行わないため、グレーリストはユーザが受信するスパムの量を減らすのに大変便利な機能です。
- **LAN IP**[554] ー LAN(ローカルエリアネットワーク)にあるIPアドレスをここで指定します。帯域幅調整においてはローカル接続として扱われます。さらに、様々なセキュリティの制限やスパムブロックからも除外されます。
- サイトポリシー[555] ー すべてのSMTPメールセッションの始めにサーバに送信されるサイトセキュリティポリシーの作成のために使用されます。一般的なサイトポリシーの例は[このサーバは中継しません(This server does not relay)]です。

4.1 セキュリティマネージャ

4.1.1 セキュリティ設定

4.1.1.1 リレーコントロール



セキュリティ ≫ セキュリティ設定 ≫ リレーコントロールメニューを選択して、メールリレーをどのように処理するかを設定する事ができます。ローカルアドレスからでもなく、ローカルアドレス宛でもないメールがサーバーに届くと、に関連しないメッセージがメールサーバに届いた際、そのサーバは、メッセージをリレー(配信)するように依頼されます。サーバに未知のユーザへメールをリレーしない場合は、ここに用意された設定を使用することができます。

> 他のサーバに無差別にメールをリレーするこは、結果として1つ以上のDNS-BLサービス[638]でドメインがブロックリストとして登録されてしまう可能性があります。スパマーが追跡を隠すためにオープンサーバを活用するので、オープンリレーはお勧めできません。

メールのリレー

メッセージリレーを許可しない
このオプションが有効な場合には、ローカルユーザの送受信メールの配信を拒否します。

...既知のエイリアス宛の場合を除く
リレーコントロール設定にかかわらず、エイリアス[757]向けにメールをリレーさせたい場合は、このチェックボックスをクリックしてください。

...認証されたSMTPセッションで送信された場合を除く
このチェックボックスが有効の場合、認証されたSMTPセッションからのメールが送られると、MDaemonは常にそのメールをリレーします。

...信頼されたホストまたはIPから送信された場合を除く
信頼されたホストやIPからのメールをリレーする場合は、このオプションを有効にしてください。

...ゲートウェイユーザから送信された場合以外を除く
リレー設定にかかわらず、ドメインゲートウェイを経由したメールのリレーを許可する場合は、このチェックボックスを有効にしてください。この機能はデフォルトでは無効になっており、この機能の使用は推奨しません。

アカウント検証

ローカルドメインを使用する場合SMTP MAILアドレスの存在が必要
ローカルドメインあるいはゲートウェイから、実在するアドレスに送られるメールのSMTP処理中に渡されるMAIL値を確認する場合は、このチェックボックスを有効にしてください。

...認証されたSMTPセッションで送信された場合を除く
このチェックボックスが有効の場合、認証されたSMTPメールセッションからのメールが送信され、[ローカルドメインを使用する場合SMTP MAILアドレスの存在が必要]オプションからメッセージを除外する場合、このチェックボックスを選択してください。

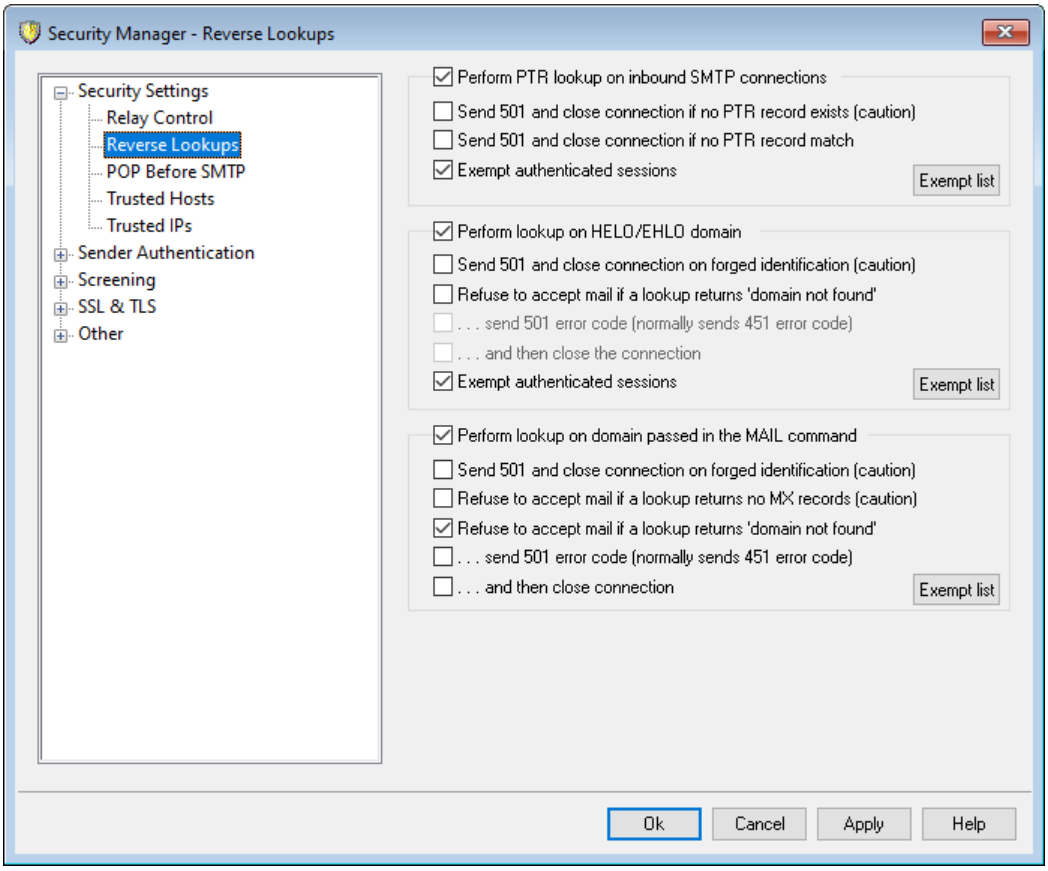
...信頼されたIPから送信された場合を除く
信頼されたIPから送信されたとき、[ローカルドメインを使用する場合SMTP MAILアドレスの存在が必要]オプションからメッセージを除外する場合は、このチェックボックスを選択してください。

ローカルドメインを使用する場合SMTP RCPTアドレスの存在が必要
ローカルドメインから実在するアドレスに送られるメールのSMTP処理中に渡されるRCPT値を確認する場合はこのチェックボックスを有効にしてください。

...認証されたSMTPセッションで送信された場合を除く
このチェックボックスが有効の場合、認証されたSMTPメールセッションからのメールが送信され、[ローカルドメインを使用する場合SMTP RCPTアドレスの存在が必要]オプションからメッセージを除外する場合、このチェックボックスを選択してください。

...信頼されたホストまたはIPから送信された場合を除く
信頼されたIPから送信されたとき、[ローカルドメインを使用する場合SMTP RCPTアドレスの存在が必要]オプションからメッセージを除外する場合は、このチェックボックスを選択してください。

4.1.1.2 リバースルックアップ



この画面のオプションを使用することにより、HELO/EHLOやMAILコマンドで渡されるドメインのリバースルックアップを行う事ができます。ルックアップの方法として、MDaemonはまずドメインのMXレコードとAレコードで指定されている全てのIPアドレスを取得します。その後、接続中のサーバーIPアドレスと先ほど取得したIPアドレスとを比較して、ドメイン情報を偽っていないかどうかの判定を行います。

また、受信されるIPアドレスのPTRレコードに対して、リバースルックアップを実行することができます。このオプションを使用すると、受信されるIPアドレスがどのPTRレコードとも一致しない場合、メッセージに警告ヘッダの挿入あるいは接続を中止することができます。

さらに、存在しないドメインを使用して自身を識別するようなソースからのメールを受け入れることは任意であるべき、というのが一般的な理解です。したがって、DNSサーバからの"domain not found"というメッセージを、リバースルックアップ処理が返すことを遮断することができるスイッチがあります。このような場合、MDaemonは、451エラーコードを返して、メッセージを拒否し、SMTPセッションの進行を許可します。しかし、501エラーコードを返すか、ソケット接続を終了するか、またはその両方を行うかを求める場合、そのような目的のための他のスイッチがあります。

信頼するIPアドレスとローカルホスト(127.0.0.1)は、常にリバースルックアップから除外されます。

インバウンドSMTP接続についてPTRルックアップを実行する
MDaemonで、インバウンドSMTP接続すべてにPTRレコードのルックアップを実行させたい場合は、このオプションを有効にしてください。

...PTRが存在しない場合501を送信し接続を閉じる(警告)
このチェックボックスが有効な場合、ドメインのPTRレコードが存在しない場合、MDaemonは501エラーコード(パラメータの構文または引数のエラー)を送信して接続を終了します。

...PTRレコードが一致しない場合501を送信し接続を閉じる
このチェックボックスが有効な場合、PTRレコードのルックアップの結果が一致しない場合、MDaemonは、501エラーコード(パラメータの構文または引数のエラー)を送信して接続を終了します。

認証済セッションを除外する
接続が認証されたものであるかどうかを確認するために、受信時のSMTP接続でのPTRルックアップを、SMTP MAILコマンドまで遅らせたい場合は、このチェックボックスを有効にします。

除外リスト
PTRルックアップ除外リストを開いて、PTRリバースルックアップから除外するIPを指定するにはこのボタンをクリックします。

HELO/EHLOドメインに関してルックアップを実行する
セッションのHELO/EHLO処理中に報告されるドメイン名にルックアップを実行する場合は、このチェックボックスを選択してください。HELO/EHLOコマンドは、クライアント(送信マシン)が自身をサーバに特定させるために使用されます。このコマンドでクライアントから渡されたドメイン名は、[Received]ヘッダの[FROM]部分に挿入するために、サーバで使用されます。

...偽造の認証に501を送信して接続を閉じる(警告)
ルックアップの結果が偽造された認証と思われる場合に501エラーコードを送信し接続を閉じるにはこの設定を有効化します。

サーバーが使用しているリバースルックアップで偽造の認証と判断しているとき、結果が誤っている場合がよくあります。メールサーバーの逆引きIPアドレスがホスト名と紐づけされていない場合はよくあります。これはISPの制限だったり他の環境が原因です。そのため、このオプションの有効化には細心の注意を払ってください。このオプションを有効化する事で、サーバーが正規のメールを拒否してしまう場合があります。

ルックアップが 'domain not found'を戻す場合メールの受け入れを拒否
ルックアップの結果が "domain not found"だった場合、このオプションを有効化する事でメールを451エラーコード(Requested action aborted: local error in processing) で戻し、残りのセッションの通常処理を受け付けます。

...501エラーコードを送信(通常451エラーコードを送信)
"domain not found" の結果として返すエラーコードとして、451ではなく501(パラメーターや引数のシンタックスエラー)を使用するにはこのオプションを有効化します。

...接続を閉じる
リバースルックアップの結果が"domain not found"だった場合に、残りの処理を許可するのではなくすぐに接続を終了するにはこのオプションを有効にしてください。

認証済セッションを除外する
接続が認証されたものであるかどうかを確認するために、ルックアップを、SMTP MAILコマンドまで遅らせたい場合は、このチェックボックスを有効にします。

除外リスト
HELO/EHLOルックアップ除外リストを開いて、HELO/EHLOリバースルックアップから除外するIPやドメイン/ホスト名を指定するにはこのボタンをクリックします。

MAILコマンドで渡された値でルックアップを実行
このチェックボックスを選択すると、メール処理のMAILコマンド部分で渡されるドメイン名にルックアップを実行させることができます。MAILコマンドで渡されるアドレスは、メッセージのリバースパスであり、通常はメッセージを送出するメールボックスです。しかしながら、このアドレスは、エラーメッセージが導かれるべきアドレスである場合もあります。

...偽造の認証(警告)に対し501コマンドを送信して接続を閉じる
このチェックボックスを選択する場合、ルックアップで偽装されたIDが見つかると、MDaemonは、501エラーコードを送信して接続を終了します。

偽造の認証をリバースルックアップの結果で判断すると、正常な結果が得られない事がよくあります。これは、メールシステムをISPで運用している場合などに、メールサーバーが逆引き情報を持たない事が多くあるためです。そのため、このオプションを有効にする前には十分に注意を払ってください。このオプションの使用によりサーバが正当なメッセージを排除してしまうという結果をもたらす可能性があります。

MXレコードを持たないメールを拒否する(注意)
MXレコードを持たないドメインからのメールを拒否する場合はこれを有効にして下さい。このオプションはデフォルトで無効になっており、ドメインは必ずしもメール送受信にMXレコードを持たない場合もあることから、使用には十分ご注意ください。

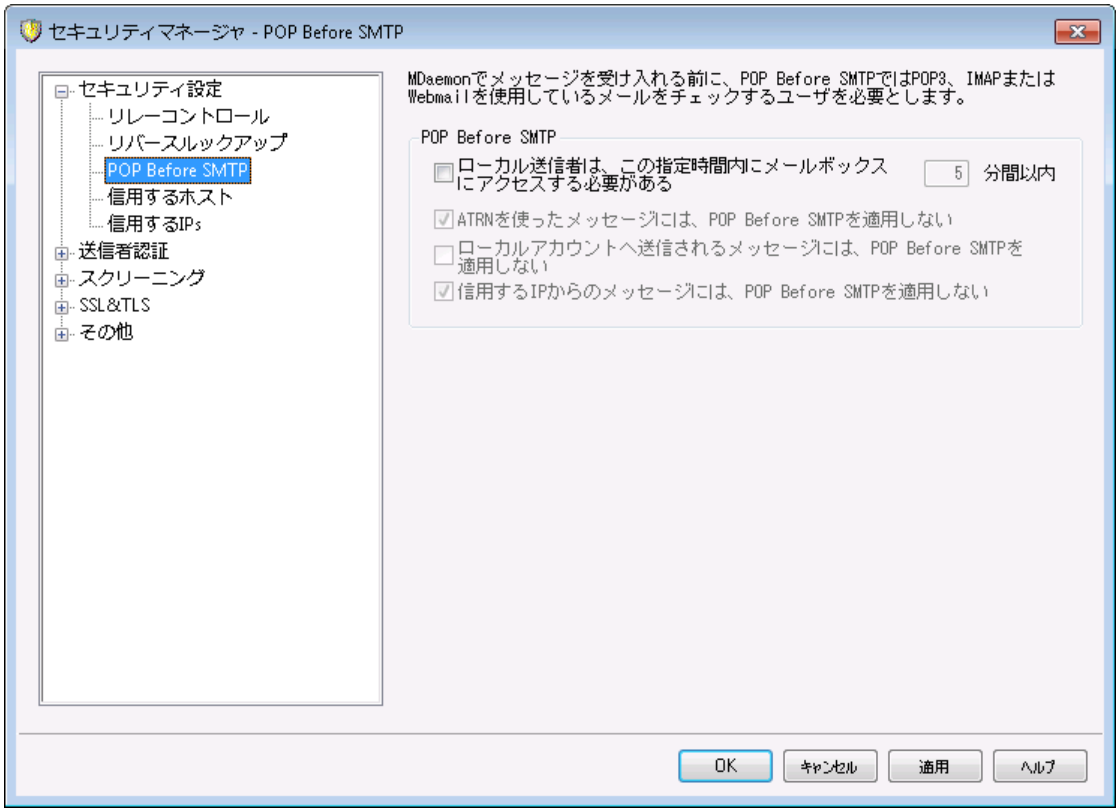
ルックアップが'domain not found'を戻す場合メールの受け入れを拒否
このオプションを有効にすると、検索の結果が"domain not found"(ドメインが見つかりません)という場合、451エラーコード(要求された処理の中止:処理中にローカルエラーが発生)と共に、メッセージは拒否されます。そして、セッションは、通常どおり最後まで処理を続けます。

...501エラーコードを送信(通常451エラーコードを送信)
[ドメインが存在しません]という結果に対応して送られるエラーコードを、451ではなく501(パラメータの構文または引数のエラー)にする場合は、このチェックボックスを選択してください。

...エラー送信後切断する
リバースルックアップの結果が"domain not found"である時、セッションの進行を許可せずに、即座に接続を切断する場合は、このチェックボックスを選択してください。

除外リスト
このボタンをクリックすると、MAILルックアップの除外リスト ダイアログが開きます。MAILルックアップ処理から除外するIPアドレス、ホスト名、ドメイン名をここから指定できます。

4.1.1.3 POP Before SMTP



POP Before SMTP

ローカルの送信者はメールボックスにアクセスしておく必要がある [XX] 分間
この機能が有効な場合、ローカルユーザは、メールの送信が許可される前にログオンを行い、指定された時間(分)以内にローカルのメールボックスを確認しなければなりません。

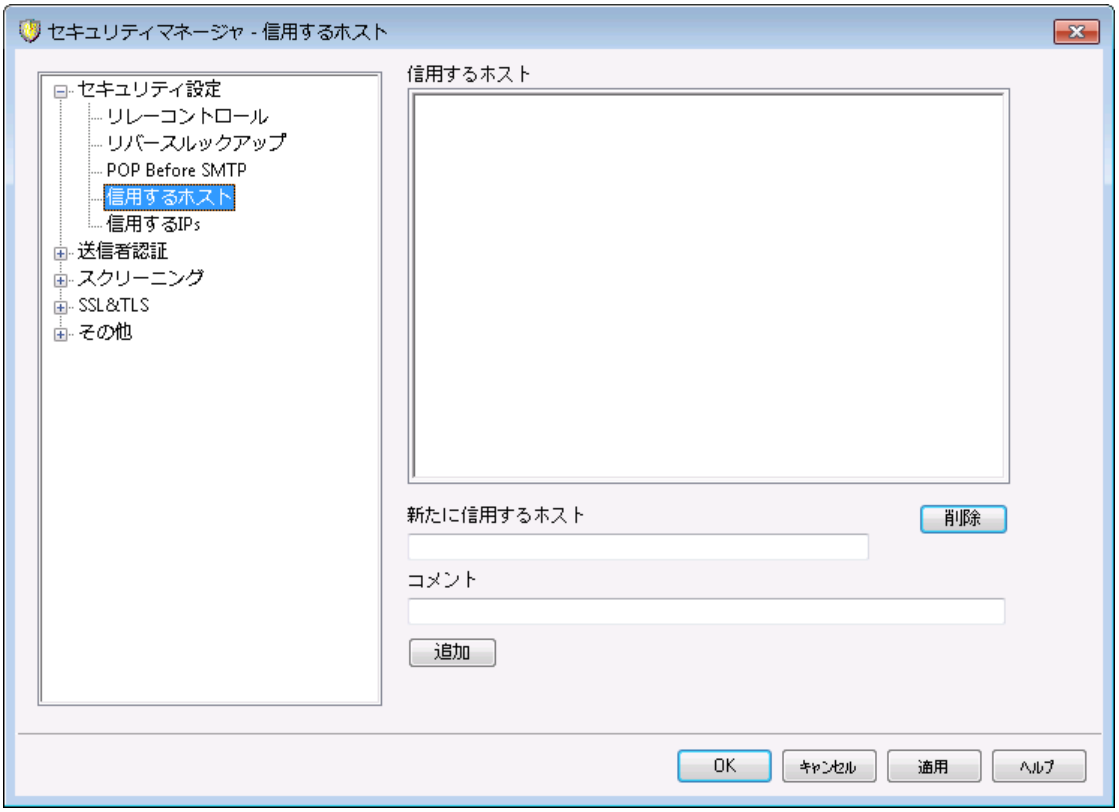
ATRNで収集したメッセージにPOP Before SMTPを適用しない
ATRN[240]によって収集されるメッセージに対して、POP Before SMTPの制限から除外する場合は、このチェックボックスを選択してください。

ローカルアカウントへ送信されるメッセージにPOP Before SMTPを適用
メッセージがローカルユーザから他のローカルユーザへ送られる時に、そのメッセージをPOP Before SMTP制限から除外する場合は、このチェックボックスを選択してください。通常、送信者が既知にされるとすぐに、MDaemonは要求を実施します。しかし、このコントロールが使用可能にされると、メッセージの受信者が必要かどうか確定する前に明らかにされるまで、MDaemonは待機します。

信頼したIPからのメッセージにPOP Before SMTPを適用しない
このチェックボックスが有効な場合、信頼したホスト 472にあるIPアドレスリストからのメッセージはPOP Before SMTPから除外します。

SMTP認証 476画面上にオプションにより認証されたセッションをPOP Before SMTP規制から免除することができます。

4.1.1.4 信用するホスト



MDaemonの全体にわたる各種ダイアログおよびセキュリティ機能には、"信頼するホスト"、"信頼するドメイン"または"信頼するIP"を、例外や除外の対象とするかどうかを選択するオプションがあります。この画面のリストもこうしたオプションの1つです。

信用するホスト
これは、特定の指定されたセキュリティオプションから免除されているホストの一覧です。

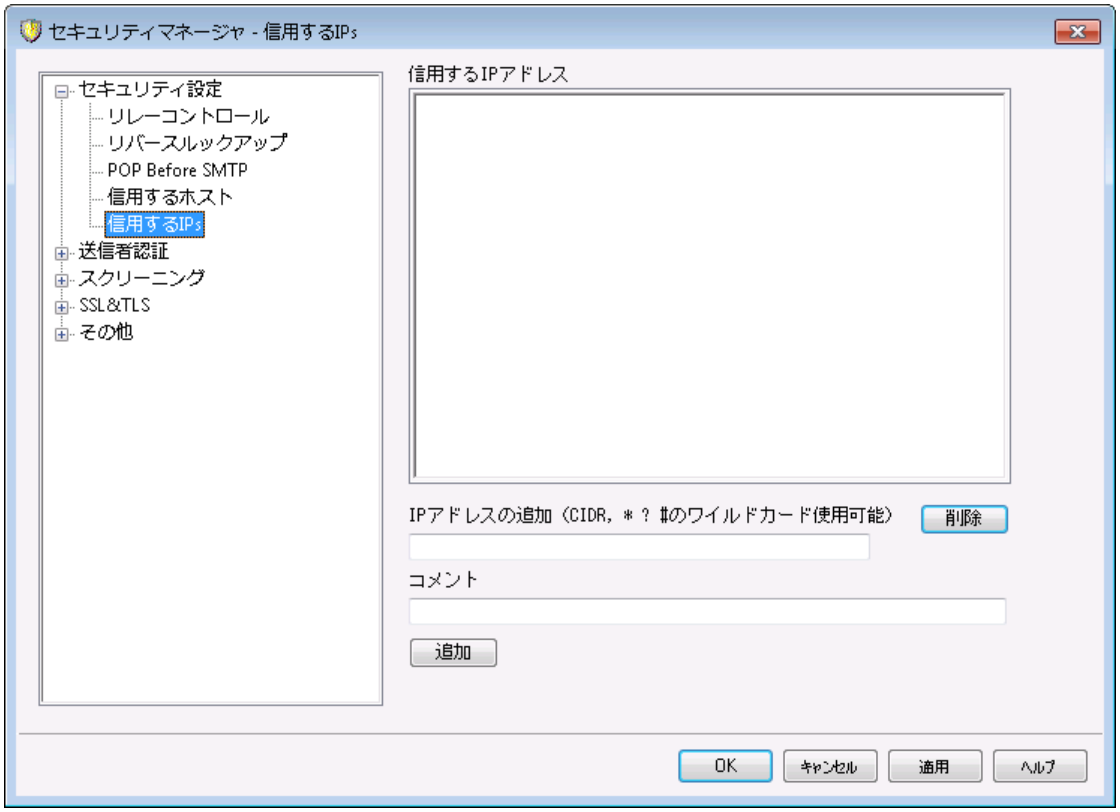
新たな信用するホスト
信用するホストへ追加する新しいドメインを入力します。

コメント
エントリに関する任意のコメントを入力します。

追 加
信 用 するホスト へ新しくドメインを追 加 するには、このボタンをクリックします。

削 除
このボタンをクリックすると信 用 するホスト から選 択したエントリを削 除します。

4.1.1.5 信頼するIP



MDaemonの全 体 にわたる各 種 ダイアログおよびセキュリティ機 能 には、"信 頼 するホスト"、"信 頼 するドメイン"または"信 頼 するIP"を、例 外 や除 外 の対 象 とするかどうかを選 択 するオプションがあります。この画 面 のリスト もこうしたオプションの1 つです。

信 用 するIPアドレス
これは、特 定 の指 定 されたセキュリティオプションから免 除 されているIPアドレスのリスト です。

新 たに信 用 するIP
信 用 するIPアドレスリスト へ追 加 する新 規 のIPアドレスを入 力します。

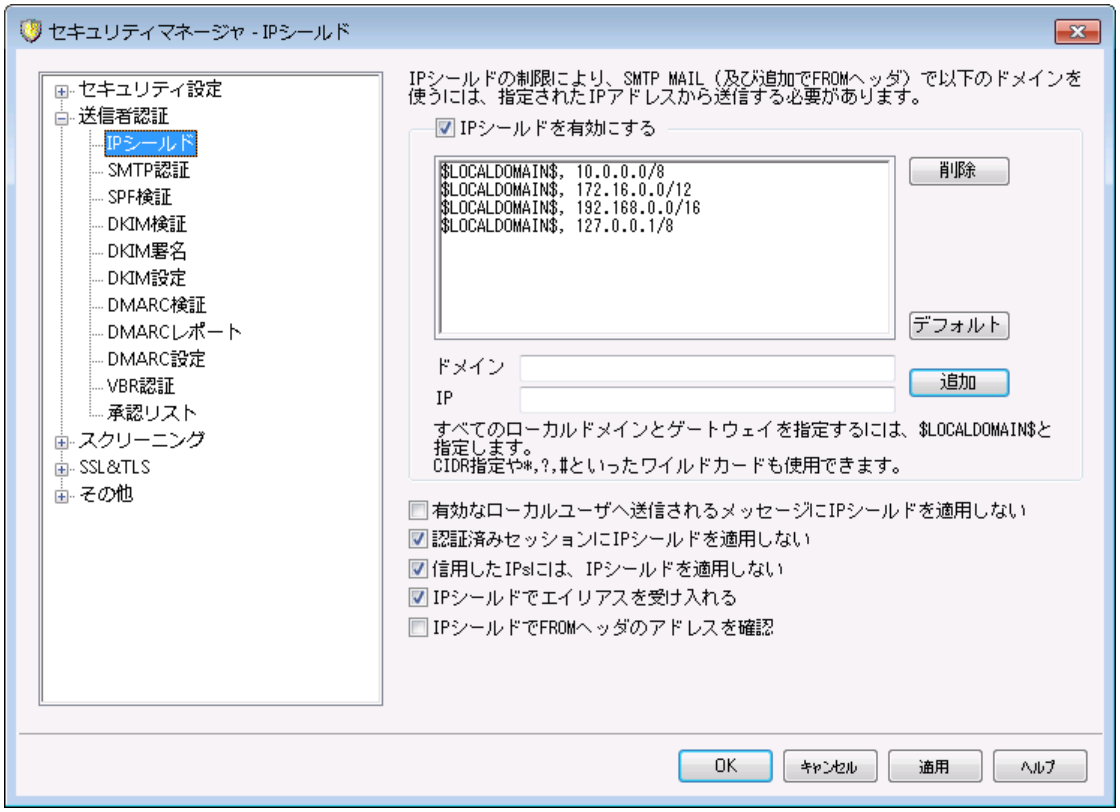
コメント
エントリに関 する任 意 のコメント を入 力します。

追加
信用するIPアドレスへ新しいIPアドレスを追加するには、このボタンをクリックします。

削除
信用するIPアドレスから選択したエントリを削除するには、このボタンをクリックします。

4.1.2 送信者認証

4.1.2.1 IPシールド



セキュリティ ≫ セキュリティ設定 ≫ 送信者認証の中にあるIPシールドとは、SMTPセッション中に、MAIL Fromコマンドで渡されるドメインとそれに紐づいたIPアドレスの一覧です。対象ドメインからのSMTPセッションは、正しく関連付けられたIPアドレスからの接続である場合のみ有効とされます。例えば、ドメイン名が[example.com]で、ローカルLANで使用されているIPが[192.168.0.0]から[192.168.0.255]の範囲とします。このような場合、IPシールディングに設定するドメイン名は[example.com]で、そのドメインに関連付けするIPアドレス範囲として[192.168.0.*]を指定することができます(ワイルドカードが可能です)。その結果、コンピュータがSMTPサーバに接続し、"MAIL FROM <someone@example.com>"を要求する場合、SMTPセッションでは接続を要求しているコンピュータが指定したIPアドレス範囲(この場合は[192.168.0.0]から[192.168.0.255]まで)を持つ場合のみ継続されます。

IPシールドを有効にする

これは、ドメイン名のリストで、ある人がそれらのうちの1つからMDaemonに接続することを試みる時に、比較される対応するIPアドレス。

ドメイン名

特定のIPアドレスの範囲に関連付けするドメイン名を入力してください。ここでは `$LOCALDOMAIN$` マクロで、(ゲートウェイを含む)全てのドメインを指定することもできます。このマクロを使用すると、ローカルドメインやゲートウェイの変更時、IPシールドの設定を更新する必要がなくなります。デフォルトでは、$LOCALDOMAIN$に関連付けられた全てのドメイン範囲がエントリとして設定されています。

IPアドレス

ドメイン名に関連付けするIPアドレスを入力してください。このアドレスは、ドットのある10進数の形式で入力しなければなりません。

追加

[追加]ボタンをクリックすると、入力したドメインとIPアドレスの範囲がリストに追加されます。

削除

このボタンをクリックすると、選択したエントリをリストから削除できます。

有効なローカルユーザへ送信されるメールにIPシールドを適用しない

ローカルユーザではない宛先、または無効なユーザに届いたメールのみドメイン/IPのチェックを行う場合は、このオプションをクリックしてください。これは、サーバを通してのメールリレーするために、ローカルユーザの1人としてメールの送信を防止しますが、ユーザに対するアドレスであるメッセージをチェックしないので、リソースを節約します。このオプションと以下で説明されている**IPシールドはエイリアスを受け入れる**の両方を有効にすると、有効なエイリアスへのメッセージも同じように受け入れられます。

認証済セッションにIPシールドを使用しない

IPシールドを認証済のユーザーへ適用しない場合はこれを有効にして下さい。IPアドレスに関わらず、認証されたユーザーからのメールは受信できるようになります。更に、認証されておらず、接続が拒否された場合、ユーザーがメール送信前に認証を行う事で問題が回避できると分かるよう、SMTPクライアントには「認証が必要です」というメッセージを含んだメッセージを送信します。

信用したIPにはIPシールドを使用しない

この機能が有効な場合、信頼するIP 472 からの接続にIPシールドは適用されません。このオプションはデフォルトで有効です。

IPシールドはエイリアスを受け入れる

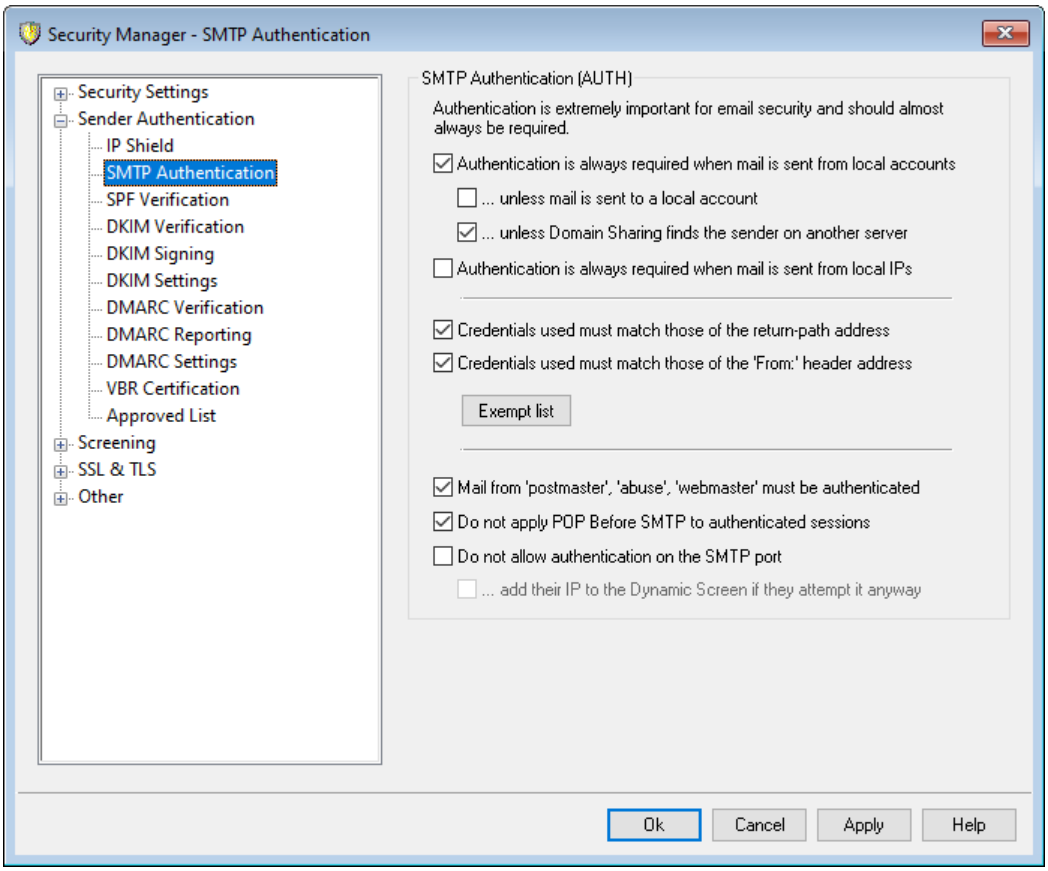
ドメイン/IPアドレスシールドでチェックを行う際に、アドレスエイリアスを有効にする場合は、このオプションをクリックしてください。このオプションが有効な場合、IPシールディングはエイリアスを実際のアカウントに変換するので、シールドを通過させることができます。このオプションを無効にすると、IPシールディングはアドレスエイリアスをそのままのアカウントのアドレスとして認識してしまいます。したがって、エイリアスのIPアドレスはIPシールディングを侵害することとなり、そのメッセージは拒否されてしまいます。このオプションは、エイリアスの設定画面 759 でも設定ができます。ここでの設定変更は、エイリアスエディタにも反映されます。

有効なアドレスエイリアスへの内部向けメッセージを、IPシールディングのチェックから除外する場合は、このオプションと有効なローカルユーザへ送信されたメッセージにIPシールドを適用しないの両方を有効にしてください。

IPシールドで FROMヘッダのアドレスを確認
IPシールドで、SMTP MAILの値に加えてFROMヘッダの確認も行いたい場合は、このオプションを有効にして下さい。このオプションはデフォルトで無効になっています。

このオプションはメーリングリストからのメールといった、特定の種類のメッセージにおいて、問題を起こす場合があります。このため、必要な場合のみ、このオプションを有効にして下さい。

4.1.2.2 SMTP認証



SMTP認証（AUTH）

ローカルアカウントからのメールの場合は常に認証を必要とする
このオプションが有効で、受信メールがMDaemonのドメインの1つである場合は、そのアカウントは最初に認証されなければなりません。その認証がない場合は、MDaemonはメッセージの配信を拒否します。 このオプションはデフォルトで有効です。

…ローカルアカウントへのメールは除外
ローカル送信者からメッセージの場合に認証を必要としている場合でも、そのメールの宛先がローカルアカウントであれば、このオプションを有効にすることによって、認証を省略することができます。このオプションは、ユーザに対して送信用と受信用で異なるメールサーバを使用させる場合などに必要となる場合があります。

…ドメイン共有で別サーバーに送信者が存在する場合は除外
デフォルトで ドメイン共有 103 で送信者が他のサーバーに存在した場合、前述の送信者は認証は常に必要…のオプションから除外されます。こうした送信者に対しても認証を必須とする場合はこのオプションを無効化してください。

ローカルIPからのメールの場合は常に認証を必要とする
受信メールがローカルIPアドレスから届いた場合に認証を要求するにはこのオプションを有効化して下さい。認証情報が正しくないと、メッセージは拒否されます。信頼するIP 473 は除外され、このオプションは新規インストールではデフォルトで有効です。

使用される認証アカウントはreturn-pathのアドレスと一致すること
デフォルトで、SMTP認証で使用する認証情報はメールのreturn-pathのアドレスと一致している必要があります。これを要求しないようにするには、オプションを無効化して下さい。ゲートウェイメールストレージと転送のため、 グローバルゲートウェイ設定 230 画面にもデフォルト設定として「ゲートウェイメールをAUTH認証情報のマッチング要件から除外」するオプションがあります。

使用される認証アカウントはFrom:ヘッダのアドレスと一致すること
デフォルトで、SMTP認証で使用する認証情報はメールのFrom:アドレスと一致している必要があります。これを必須としない場合は、オプションを無効化して下さい。ゲートウェイメールストレージと転送のため、 グローバルゲートウェイ設定 230 画面にも、これに関連する設定として「ゲートウェイメールをAUTH認証情報のマッチング要件から除外」するオプションがあります。

除外リスト
認証情報のマッチング除外リストは、上記の「認証アカウントは…と一致する」のオプションから除外するアドレスの登録に使用します。上記オプションから除外するには、アドレスはメールのReturn-Pathのアドレスと一致する必要があります。「使用される認証アカウントはFrom:ヘッダのアドレスと一致すること」のオプションから除外する場合は、アドレスはメールのFrom:ヘッダのアドレスと一致する必要があります。

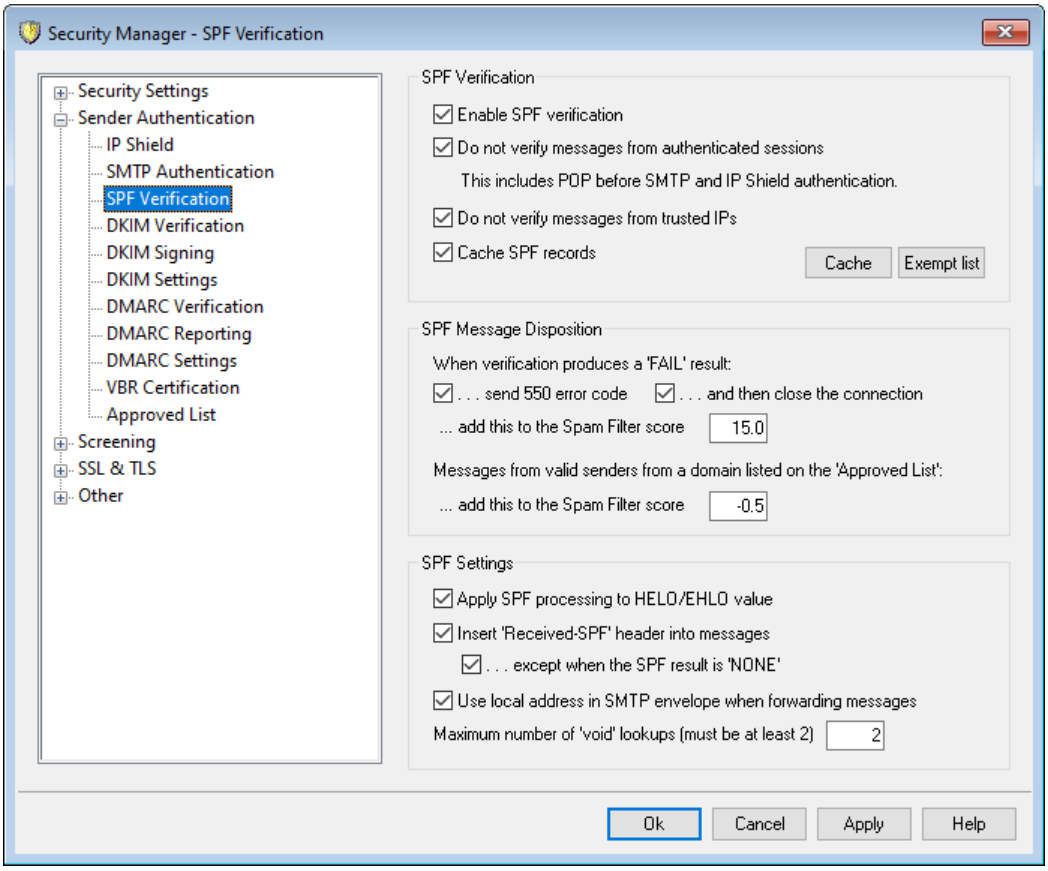
'Postmaster', 'abuse', 'webmaster'からのメールには認証が必要
MDaemonが"postmaster@...", "abuse@..." または"webmaster@..."のエイリアス又は実アドレスからのメールに対し、常に認証を求める場合はこのチェックボックスを有効にします。スパムの送信者やハッカーは、サーバにPostmasterアカウントが存在し、そのアカウントからシステムへメールが送信されることを知っています。このオプションを有効にすることによって、そのような権限のないユーザからのアクセスを拒否することができます。また、このオプションは、エイリアスの設定画面[759]からでも設定が可能です。ここでの設定変更は、エイリアスエディタにも反映されます。

認証されたセッションにPOP Before SMTPを適用しない
セキュリティ機能としてPOP Before SMTP[471]を使用している場合は、このチェックボックスを選択することにより、認証されたユーザを、この制限から除外することができます。これにより、認証されたユーザは、メールの送信前に自分のメールをチェックする必要がなくなります。

SMTPポートを使った認証を許可しない
このオプションはSMTPポートでの認証を無効化します。認証はEHLOレスポンスの後には使用されず、SMTPクライアントから送信された不明なコマンドとして処理されます。この設定と、後述の「…ダイナミックスクリーンにIPを登録する」設定は認証されたメールをMSAや他のポートで送信している環境においては便利な設定です。こうした環境の場合、SMTPポートを使った認証は攻撃者からの場合がほとんどだからです。

...このポートでの認証が続く場合ダイナミックスクリーンにIPを登録する
上記のSMTPポートを使った認証を許可しないオプションを使っていた場合、SMTPポートを使った認証が続いた場合にダイナミックスクリーンへIPを登録するにはこのオプションを使用します。この時のSMTP接続もすぐに終了されます。

4.1.2.3 SPF 検証



MDaemonは、スプーフィング(なりすまし)やフィッシュングを防ぐために、センターポリシーフレームワーク(Sender Policy Framework (SPF))に対応しています。スプーフィング(なりすまし)やフィッシュングは、メールの送信者が送信元を他人からであるように偽造する典型的な手段です。

多くのドメインは、メールの受信が許されるロケーションを特定するために、Domain Name System(DNS)でMXレコードを発行しますが、これはメールの送信元を特定できるものではありません。SPFは、ドメインが送信記録を発行することにより、メールの送信を許可されたロケーションを特定するためのシステムです。受信メールにSPFを適用することにより、MDaemonは送信サーバが意図しているドメインに対してメールの配信が許可されているかや送信者のアドレスが偽造されているかどうかを判断することができます。

この画面のオプションを使用して、サーバーのSPF設定を構成します。

SPFに関する詳細は、下記をご覧ください:

http://www.open-spf.org

SPF検証

SPF検証を有効にする
このオプションを有効にすると、MDaemonは受信メールの送信者毎に、対象送信サーバーによるメール配信を許可するかどうか、DNSへSPFレコードの問合せを行います，送信側サーバーがそのためにメッセージを送信することを許可されていることを確認します。 MDaemonはSMTPセッション中のMAILで返される値から検証を行います。 SPF検証はデフォルトで有効になっています。

認証されたセッションからのメッセージを確認しない
デフォルトでは、認証された接続はSPF検証から除外されます 認証されたセッションにはSMTP認証[476]、POP before SMTP[471]、IPシールド[474]で認証されたものが含まれます。認証されたセッションをSPF検証から除外しない場合には、このオプションを無効にして下さい。

信頼できるIPからのメッセージを検証しない
デフォルトでは、信頼されたIPアドレス[473]からのメッセージはSPF検証から免除されます。

検証結果をキャッシュする
MDaemonはデフォルトでドメインのDNSでの問合せで把握したSPFポリシーレコードを一時的にキャッシュとして保存します。SPFポリシーをキャッシュとして保存しない場合はこのチェックボックスをクリアして下さい。

キャッシュ
このボタンでSPFキャッシュが起動し、現在キャッシュへ保管されているSPFレコードの一覧が確認できます。

除外リスト
このボタンをクリックすると、SPFの除外リストが開き、SPF検証から除外するIPアドレス、メールアドレス、ドメインを指定することができます。メールアドレスはメールのFromヘッダではなくSMTPエンベロープと比較されます。ドメインはドメイン名の最初を"spf"と変換して除外リストとして登録されます。MDaemonはMDaemon専用の"w linclude:<domain>"タグを使ってドメインのSPF全てを検証します。この方法であれば、バックアップ用MXプロバイダーを全ての送信者の正しいSPFソースとして利用する事ができます。

SPFメッセージの処理

検証処理がFAILの場合:

...550エラーを送信
SPFクエリの結果が失敗だった場合、550エラーコードを送信するにはこのチェックボックスを選択します。

...エラー送信後切断する
550エラーコードを返した直後に接続を閉じるにはこのオプションを有効にします。

...この値をスパムフィルタスコアに加算
SPF検証に失敗した場合メールのスパムスコアに加算する値を指定します。.

承認リストドメインからの正規の送信者からのメール

...この値をスパムフィルタスコアに加算
SPF検証によってメールが承認リスト[506]のドメインからのメールであると確認できた場合、スパムフィルタスコアに加算する値をここで指定します。

承認リストのメールからスパムスコアを減算するため、通常ここでは負の値が指定されます。

SPFの設定

SPF処理をHELO/EHLO値に適用する
このオプションは、SMTPプロセスの開始時にHELOまたはEHLOコマンドで渡された値にSPF検証を適用します。これはデフォルトで有効になっています。

メッセージに'Received-SPF'ヘッダを挿入する
Received-SPFヘッダーを各メッセージに挿入する場合は、このオプションをクリックします。

....SPF結果が'なし'の場合は除外する
SPFの結果が[なし]であった際に、"Received-SPF"ヘッダを挿入しない場合は、このオプションを有効にしてください。

メッセージを転送するときにSMTPエンベロープのローカルアドレスを使用する
MDaemonが転送するすべてのメールでSMTPエンベロープのローカルアドレスを使用する場合は、このオプションを有効にします。通常、転送されたメッセージは、実際に転送を行っている電子メールアドレスではなく、元の送信者の電子メールアドレスを使用して送信されます。状況によっては、受信サーバが転送されたメッセージを「偽装された」アドレスを有すると誤って識別しないようにするために、ローカルアドレスを使用することが必要な場合があります。このオプションは、デフォルトで有効になっています。

'Void'ルックアップの最大数（最小値は2）
MDaemonがpermanentエラーを生成するまでに実行するSPFクエリの最大"void"ルックアップ数です。「ドメインが存在しない」または「応答が存在しない」という結果はVoidルックアップの1つです。この値は最少でも2である必要があります。

4.1.2.4 DomainKeys Identified Mail

DomainKeys Identified Mail（DKIM）は、メールアドレスの詐称を防止するための電子メール暗号署名システムです。また、多くのスパムメールは偽のアドレスを含むため、DKIMによって、スパム防止ツールを使用していなくてもスパムの受信を大幅に減らすことができます。
さらに、DKIMは受信メールの整合性を高め、メールがサーバからクライアントに受信するまでの間に改ざんされないことを保証します。言い替えれば、DKIM暗号署名によって、受信サーバは受信メールが確かにそれを署名したサーバからのものであることと、そのメールが改ざんされていないことを確認することができます。

電子メールの正当性と整合性を確実にするために、DKIMはパブリックとプライベートのキーシステムの組み合わせを使用します。暗号化された公開鍵は、送信サーバのDNS情報を送信し、それぞれの送信メールはそれに対応する暗号化された秘密鍵を使用するサーバによって認証されます。受信サーバは受信メールが送信サーバのDNS情報からの公開鍵を持つことを確認して、メールの暗号署名と比較してその正当性を判断します。受信メールが認証されない場合は、受信サーバはそのメールに偽のアドレスが使われているかどうかや、メールが改ざんされているかどうかを判断します。検証に失敗したメールは遮断されるか、受信されつつもスパムスコアを調整されます。

暗号署名された受信メールをMDaemonで検証するには、DKIM検証 482 画面のオプションを使用します。送信メールに署名するように設定するには、DKIM署名 484 画面のオプションを使用します。どちらもセキュリティ ≫ セキュリティ設定 ≫ 送信者認証からアクセスできます。MDaemonのメイン画面インターフェイス 64 には、（セキュリティタブの下に）"DKIM"タブがあり、DKIM活動状況をリアルタイムでモニタすることができます。また、DKIMの活動は、設定 ≫ サーバ設定 ≫ ロギング ≫ 設定を使用して、ログに記録することもでき

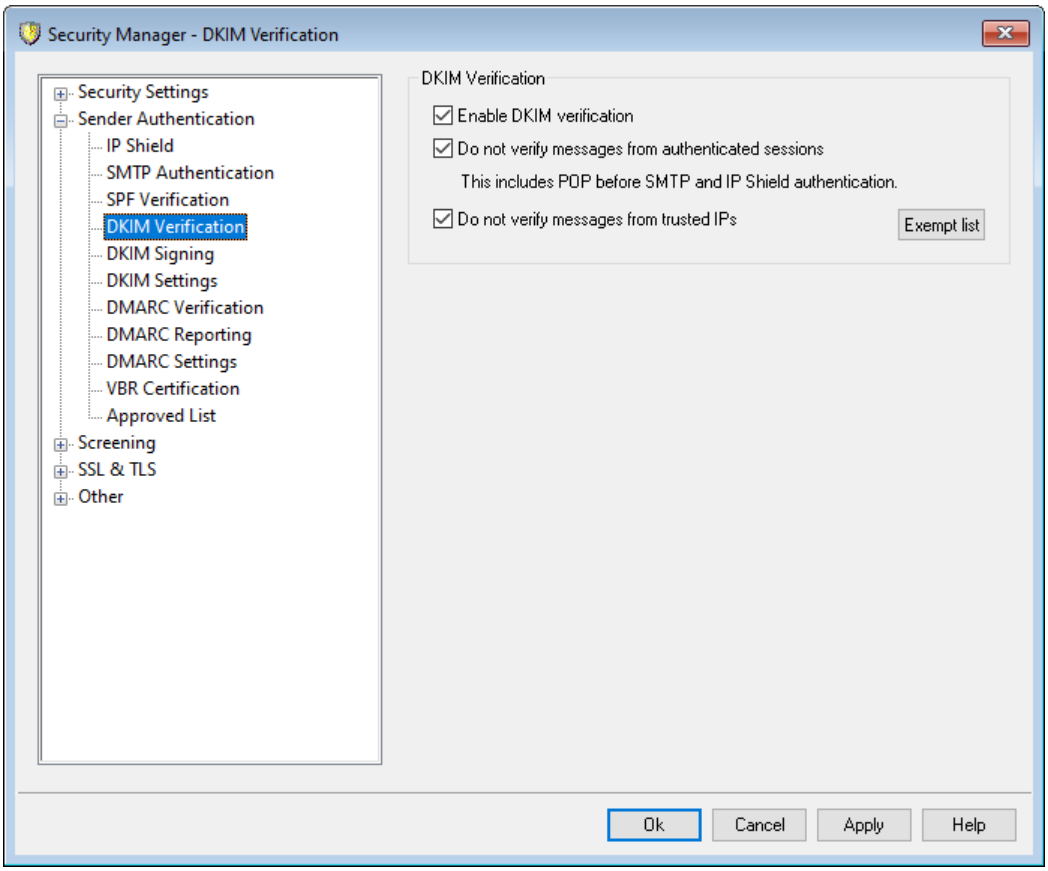
ます。

参照:

DKIM検証 482
DKIM署名 484
DKIMオプション 486

DomainKey Identified Mailの詳細はこちらを参照して下さい: http://www.dkim.org/

4.1.2.4.1 DKIM検証



この画面では、受信メールのDomainKey Identified Mail(DKIM)の検証設定が行えます。この機能が有効で、受信メッセージが暗号署名されている場合、MDaemonは署名サーバのDNSレコードから公開鍵を取得し、そのキーを使用してメールのDKIM署名の正当性のテストを行います。

DKIM署名が検証テストを通過すると、メールは通常の配信処理における次のステップへ進みます。さらに、署名から取得したドメインが承認リスト 506のドメインと一致した場合、メッセージのスパムフィルタスコアは適宜調節されます。

DKIMについてはこちらを参照して下さい: http://www.dkim.org/

DKIM検証

DKIM検証を有効にする
受信するメールのDomainKey Identified Mail検証を有効にするには、このオプションを選択してください。

認証されたセッションからのメッセージを検証しない
認証されたセッションを検証から除外するにはこのオプションを使用して下さい。認証されたセッションにはSMTP認証[476]、POP before SMTP[471]、IPシールド[474]が含まれます。

信頼されたIPからの接続はDKIM検証から除外する
信頼するIPアドレス[472]からのメールをDKIM検証から除外するにはこのオプションを使用して下さい。

除外リスト
このボタンをクリックすると除外リストが開きます。このリストに含まれるIPアドレスから発信されたメッセージは検証の対象となりません。

Authentication-Resultsヘッダ

メールがSMTP認証、SPF、DomainKeys Identified Mail、DMARCでの検証を通過すると、MDaemonは認証処理の結果を、Authentication-Resultsヘッダとして対象メール挿入します。MDaemonが認証に失敗した場合でもメールを受け付けるよう設定されていた場合は、Authentication-Resultsヘッダから失敗の理由を判断する事ができます。failure.

このヘッダやこのセクションで説明している認証プロトコルについては、現在もInternet Engineering Task Force (IETF)で協議されています。本件についての詳細は、次のIETFのウェブサイトを参照して下さい: http://www.ietf.org/.

メーリングリストメールのDKIMヘッダ

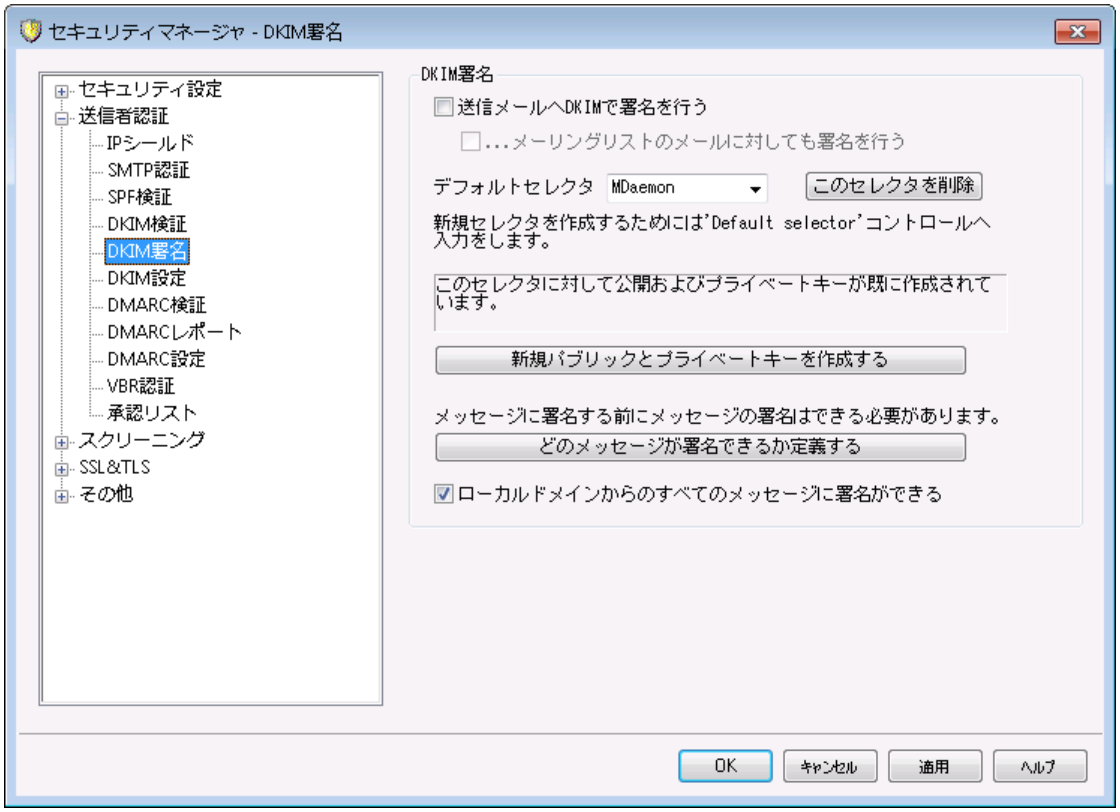
デフォルトで、MDaewmonはメーリングリストからのメールに付与されたDKIM署名を取り除きます。これらの署名はメーリングリストのメールヘッダや本文処理の中で破損したり変更されたりする場合が多いためです。メーリングリストメールの署名をそのまま残す場合は、MDaemon.iniファイルへ次のオプションを追加し、設定を行う事ができます:

```
[DomainKeys]
StripSigsFromListMail=No (デフォルトは"Yes")
```

参照:

DomainKeys Identified Mail[481]
DKIM署名[484]
DKIM設定[486]

4.1.2.4.2 DKIM署名



DKIM署名の画面では、MDaemonが送信メールへDKIMで署名を付与する設定を行ったり、どのメッセージに署名するかを選択したりできます。またセレクタを指定し、DKIMの仕様に沿った公開鍵および秘密鍵を生成することができます。デフォルトのセレクタ(MDaemon)とデフォルトの公開鍵や秘密鍵はスタートアップ時に自動的に作成されます。すべてのキーは一意であり、セレクタの指定に関係なく、決して同じものが生成されることはありません。またデフォルトではキーは安全な2048ビットで生成されます。

DKIM署名

送信メールへDKIMで署名する
送信メッセージにDomainKey Identified Mailを使用した暗号署名を行いたい場合は、このオプションを有効にしてください。
メッセージに署名するためには、**どのメッセージが署名できるか定義する**ボタンで指定された判定基準を満たさなければならず、認証されたセッションで配信されMDaemonによって受信されなければなりません。またコンテンツフィルタの*"Sign with DKIM selector..."*という機能で署名することもできます。

...メーリングリストのメールに対しても署名を行う
送信されるすべてのメーリングリストメッセージに暗号署名を行いたい場合は、このチェックボックスを選択してください。MDaemonではリストのすべてのメールに署名されるので、暗号署名に関して**どのメッセージが署名できるか定義する**オプションを使用する必要はありません。

メーリングリストのメールへの署名を行うには、リストを解読後にそれぞれのメッセージに対してコンテンツフィルタ処理が必要です。この処理は大規模

で使用頻度の高いメーリングリストを処理する際、サーバのパフォーマンスに影響する可能性があります。

デフォルト セレクタ
ドロップダウンリストから、MDaemonがメッセージに署名する際に使用するパブリックとプライベートのキーの組み合わせに対応するセレクタを選択してください。異なるセレクタで新しいキーの組み合わせを使用する場合は、ここに必要なセレクタ名を入力し、下記の**新規パブリックもしくは秘密鍵を作成する**をクリックします。代替セレクタを使用してメッセージに署名する場合は、**どのメッセージが署名できるか定義する**でセレクタを指定するか、コンテンツフィルタの*"Sign with DKIM selector..."* を使用してルールを作成してください。

このセレクタを削除
セレクタを削除する場合、このボタンをクリックしてください。画面表示にしたがってください。

新規パブリックとプライベート キーを作成する
上記のセレクタについてパブリック/プライベート・キーペアを生成するために、このボタンを選択します。パブリック/プライベート・キーペアはセレクタについて生成され、ファイルdns_readme.txtが生成され自動的に開きます。このファイルには、ドメインのDNSレコードを発行するために必要なDKIMデータと、指定されたセレクタに対する公開鍵のサンプルデータが含まれています。このファイルにはテストおよび未テスト状態のサンプル、ドメインからのすべてのメッセージあるいはいくつかのメッセージだけに署名する場合などのサンプルなどが記載されています。現在、DKIMまたはこのセレクタをテストしている場合、テストの対象に応じて、ポリシーかセレクタのテスト内容を含む情報を使う必要があります。テストしている状態でなければ、未テスト エントリが必要です。

すべてのキーはPEM形式で保存され、すべてのセレクタとキーの情報は¥MDaemon¥Pem以下のフォルダに保存されます。

```
\MDaemon\Pem\<Selector>\rsa.public - public key for this selector
\MDaemon\Pem\<Selector>\rsa.private - private key for this selector
```

これらのフォルダに含まれているファイルは、暗号化された状態や非表示になっていませんが、許可されていない第3者がアクセスするべきでないRSAプライベート キーが含まれています。OSの機能を利用してこのフォルダやサブフォルダにセキュリティをかけることをお勧めします。

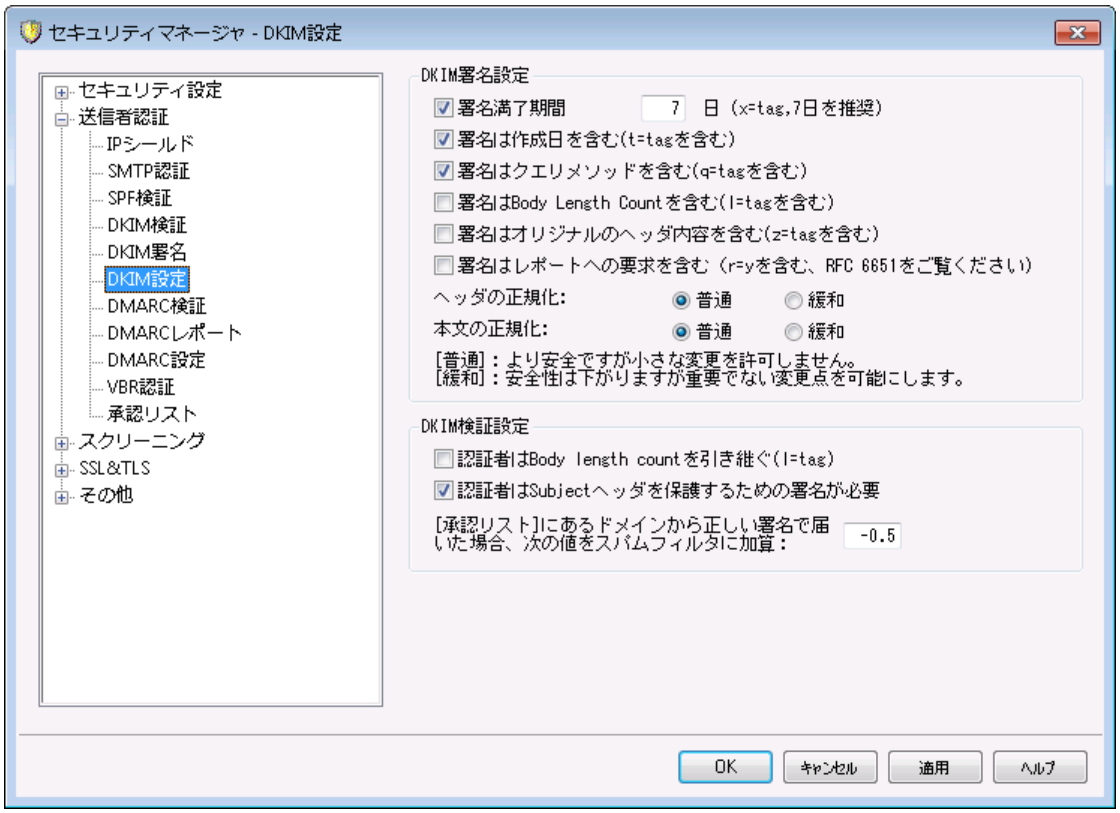
どのメッセージが署名できるか定義する
上記の[**送信メールに署名する**]オプションの一部あるいは両方を有効にした場合、このボタンをクリックするとDKSign.datファイルを編集することができます。DKSign.datファイルにはMDaemonがメッセージに署名すべきかどうかを判断をするドメインとアドレスのリストが含まれています。署名を行うにはToやFromにこのアドレスが必要かどうかを指定し、[Reply-To]や[Sender]ヘッダを追加するといった指定も行えます。マッチした各エントリに対して任意のセレクタを指定し、署名を追加する事もできます。最後に、署名ヘッダ内の[d=]タグで署名に使用するドメインを指定することができます。この機能は複数のサブドメインによる署名メッセージがある場合などに便利です。このような場合、[d=]を使用することによりシングルドメインのDNSレコードでDKIMキーを探すように受信サーバに命令することができます。これにより、個々のサブドメインの個々のレコードを管理するのではなく、1つのレコードですべてのキーを管理することが可能となります。ドメインとアドレスの両方でワイルドカードが使用できます。

ローカルドメインからのすべてのメッセージに対して署名ができる
ローカルドメインからのメール全てを署名対象とする場合はこのオプションを使用してください。このオプションを使用すると、特定のセレクタあるいは"d="タグを指定する場合を除き(DKSign.datファイルで)ローカルドメインの追加を行う必要はありません。このオプションは、デフォルトで有効です。

参照:

DomainKeys Identified Mail 481
DKIM設定 486
DKIM検証 482

4.1.2.4.3 DKIM設定



DKIM署名設定

署名満了期間 [XX] 日 ("x=" タグ, 7 日を推奨)
DKIM署名の有効日数を制限する必要ある場合、このオプションを選択し日数を指定します。期限切れの署名が付与されたメールは、検証に失敗します。このオプションは、署名の"x="タグに対応します。このオプションは、デフォルトで有効で7日が設定されています。

署名は作成日を入れる ("t=" タグを含む)
このオプションを有効にすると、署名作成時間スタンプ("t="タグ)が署名に含まれます。これは、デフォルトで有効です。

署名はクエリメソッドを含む("q="タグを含む)
デフォルトで有効です。DKIMの署名にクエリ要素のタグ(例えば、q=dnq)を含みます。

署名はBody length countを含む("l="タグを含む)
Body length countをDKIM署名に含む必要がある場合、このオプションを有効にします。

署名はオリジナルのヘッダ内容を含む("z="タグを含む)
DKIMの署名に[z=]タグを含む場合はこのオプションを有効にしてください。このタグにはメッセージのオリジナルヘッダのコピーが含まれます。そのため署名のサイズが非常に大きくなる可能性があります。

署名はレポートへの要求を含む(r=yタグを含む)
署名されたメールへr=yタグを含むにはこのオプションを有効にします。このタグは、自分がメールを送信した後、対象サーバーから、DKIM検証の失敗が原因で拒否された場合、AFRFレポートを受け取れるよう指示するためのものです。ただし、このレポートを受け取るためには、自分のDNSへDKIMレポート用のTXTレコードを指定する必要があります。構文や設定方法についての詳細はRFC-6651、: *Extensions to DomainKeys Identified Mail (DKIM) for Failure Reporting*を参照して下さい。このオプションにはDNSの変更が必要となるため、デフォルトで無効になっています。

正規化

正規化とは、DKIM署名の作成前に、メールのヘッダと本文を正規の規格に変換し、[標準化される]プロセスです。メールサーバや転送システムシステムによっては、メールの処理中に様々な小さな変更を行うため、メールの署名を行う前に正規化しなかった場合、署名が壊れてしまう可能性があります。現在、DKIM署名と検証に使われている正規化の方法には、SimpleとRelaxedという2つの方法があります。Simpleは最も厳しい方式でメールへの変更はほとんど認められません。Relaxedはより緩い方式で、多少の変更を許可しています。

ヘッダの正規化方式:Simple, Relaxed
これはメッセージに署名する際に、メッセージヘッダに使用される正規化メソッドです。[Simple]はヘッダの変更を一切認めず、[Relaxed]はヘッダ名(ヘッダ値ではありません)を小文字に変換、複数の連続したスペースを1つに変換、その他当たり障りのない変換を許可しています。デフォルトは[Simple]です。

本文の正規化方式:Simple, Relaxed
これはメッセージに署名する際に、メッセージ本体に使用される正規化メソッドです。[Simple]はメッセージの最後の空白行を無視し、その他の変更を一切認めません。[Relaxed]はメッセージの最後の空白行を許可し、行の最後の空白を無視し、一行内の連続した空白を1つにまとめ、その他の軽微な変換を許可しています。デフォルトの方式は[Simple]です。

DKIM検証設定

認証者はbody length countを引き継ぐ("l=" tag)
このオプションが有効な場合、body length countタグが受信メッセージのDKIM署名に含まれていると、MDaemonがそのタグを引き継ぎます。実際のbody lengthがタグに含まれている数値より大きい場合、MDaemonでは、タグで指定された数値までしか検証を行わず、残りの部分はそのままになります。これは何かがメッセージに追加され、その結果として、未確認の部分が疑わしい可能性がある事を示しています。一方、実際のボディ長がこのタグに含まれている数値より小さい場合は、署名は認証されません("FAIL"を受信)。これは、メッセージのある部分が削除され、その結果として、body lengthのカウントがタグで指定された数値以下になってしまったことを示しています。

認証者はSubjectヘッダを保護するために署名が必要
受信メールへSubject ヘッダを保護するためのDKIM署名を必要とするには、このオプションを有効にしてください。

「承認リスト」ドメインからの有効な署名に次のスパムフィルタスコアを追加:
承認リスト[506]にあるドメインから、DKIM検証に成功したメールが届いた場合、ここで指定したスコアをスパムフィルタスコアへ追加します。メールの署名検証に成功しても承認リストにドメインが含まれていない場合は、スパムフィルタスコアの調整は行われません。検証された署名はスコアに影響する事はありません。ただし、通常のスパムフィルタ処理とスコア処理が対象メッセージに対して行われます。

通常ここで指定する値はネガティブな数で、そのためスパムスコアは、承認リスト[506]ドメインからの正しい暗号化署名付きのメールから減算されます。MDaemonのこのオプションのデフォルト値は-0.5です。

参照:

DomainKeys Identified Mail[481]
DKIM検証[482]
DKIM署名[484]

4.1.2.5 DMARC

Domain-based Message Authentication, Reporting & Conformance (DMARC)とは、メールのFrom: ヘッダを偽装したスパムやフィッシングメールを減らす目的で設計された標準規格です。DMARCを使う事で、ドメイン所有者はDNSを通して、宛先サーバーに対し自分のドメインを名乗ってはいるものの、実際の情報とは異なっているメールをどのように扱うか、といった情報を、ポリシーとして通達できるようになります。このポリシーは、宛先のDNSサーバーが受信メールの処理中に行うDNSクエリに応じて、隔離・削除・何もしない(通常通り処理する)といった処理が行われます。ポリシーに加え、ドメインのDMARC用DNSレコードには、サーバーに対して自社ドメインの名乗る偽装メールの数や失敗した認証の回数や、それぞれの詳細情報をDMARCレポートとして送信するようリクエストも含まれています。DMARCのレポート機能はメールの認証処理の効果やドメインがどの位の頻度で偽装されているのかを検証するのに大変役立つ機能です。

セキュリティ設定画面の中の送信者認証へ、DMARC検証とレポート設定用に、DMARC検証、DMARCレポート、DMARC設定の3つの画面があります。

DMARC検証[494]

DMARC検証処理の1つとして、MDaemonは受信メールのFrom: ヘッダに含まれるドメインに対して、DMARCのDNSクエリを行います。ここではドメインがDMARCを使用しているかどうかを確認し、使用している場合は、ポリシーやその他DMARC関連情報を含んだDMARC DNSレコード[490]を取得します。更に、DMARCはSPF[479]やDKIM[482]を使ってメールの検証を行い、最低でもどちらかの検証で成功しないと、DMARC検証を通過できません。メールの検証に成功すると、MDaemonは残りの配送処理やフィ

ルタリング処理を通常通り行います。DMARC検証に失敗した場合は、ドメインのDMARCポリシーとMDaemonのDMARC検証失敗メールの処理設定の組み合わせに応じて、メールの処理が行われます。

DMARC検証に失敗し、DMARCドメインが"p=none"ポリシーを使っていた場合、特別な処理は行われず、メールは通常通り処理されます。一方で、DMARCドメインが、"p=quarantine"や"p=reject"といった制限ポリシーを使っていると、MDaemonはオプションでメールを自動的にユーザーのスパム(Junk E-mail)フォルダへ振り分ける事もできます。また、ドメインが"p=reject"ポリシーを使っていた場合に、MDaemonにメールを拒否するよう設定する事もできます。制限ポリシーで検証に失敗したメールについては、更にMDaemonの設定によって、"X-MDDMARC-Fail-policy: quarantine"ヘッダを挿入する事ができます。このヘッダを使う事で、コンテンツフィルタで、メールを指定したフォルダへ移動するといった、何らかの処理を行う事ができます。

DMARC検証はデフォルトで有効で、ほとんどのMDaemon設定で推奨しています。

DMARCレポート 496

MDaemonがDNSへDMARCレコードの問合せを行った際、DMARCレコードに、対象ドメインを名乗るメールでDMARC検証に失敗したものを、ドメイン所有者にレポートとして提供するように求めるタグが含まれている場合があります。DMARCレポートのオプションでは、要求されている種類のレポートの送信を行うかどうかの指定や、レポートに追加するメタ情報の指定を行う事ができます。統計レポートはUTCの深夜に送信され、失敗レポートは、検証に失敗する毎に送信されます。レポートは常にXMLファイルをzip圧縮した上でメールへ添付し送信され、このレポートを簡単に閲覧するための様々なツールがオンラインで提供されています。

デフォルトでMDaemonは統計レポートや失敗レポートを送信しません。レポートを送信するには、DMARCレポート画面で関連するオプションを有効にして下さい。

DMARC設定 499

DMARC設定ではDKIMの特定の情報をレポートに含むかどうか、DMARCのDNSレコードをログへ残すかどうか、MDaemonがDMARCで使用するPublic Suffixファイルを更新するかどうか、といった様々な設定が行えます。

DMARC検証とメーリングリスト

DMARCの目的が、メールのFrom: ヘッダのドメインが偽装されていない事を確認するためのものであるため送信サーバーは当然対象ドメインとしてメール送信する事を許可されていなくてはなりません。これはメーリングリストに対して独自の問題を引き起こす場合があります。これは、異なるドメインのメーリングリストメンバーがメーリングリストのアドレスでメール送信を行い、From: ヘッダの変換は行われていない、という状況がよくあるためです。つまり、受信サーバーがメーリングリストのメールに対してDMARC検証を行った場合、メールがFrom: ヘッダのドメインとして公式に認定されて場所から届いたものとして判断されるという事です。DMARCドメインが制限DMARCポリシーを使っていた場合、これによりメールは受信サーバーで隔離されたり拒否される事になります。環境によっては、宛先メールアドレスがメーリングリストのメンバーから削除されてしまう場合もあります。こうした問題を回避するため、MDaemonは制限DMARCポリシーを使っているドメインからのメーリングリストメールを受信すると、メールのFrom: ヘッダをメーリングリストのアドレスへ書き換えます。また、制限ポリシーを使っているドメインからのメーリングリストメールを受け付けないようMDaemonを設定する事もできます。このオプションで、制限ポリシーを使っているドメインのユーザーからのメーリングリストに対する投稿を効率よく止める事ができます。From: ヘッダを書き換えるオプションは、メーリングリストエディタのヘッダ 257画面からアクセスできます。メールを拒否するためのオプションへは、設定 254画面からアクセスできます。

MDaemonドメインでDMARCを利用

自分のドメインでDMARCを使用する、つまり、先方のDMARC対応メールサーバーにメールが自分のドメインからのものである事をDMARCを使って検証させるには、まず、DNS用に、SPFとDKIMレコードを作成します。最低限その中の1つは正常に動作させておく必要があります。もしもDKIMを使用する場合は、更にMDaemon側のDKIM署名 484オプションを設定します。追加で、DMARC用のDNSレコードを作成します。DNSへこの特殊な形式のTXTレコードの問合せを行うと、受信側のサーバーは送信元ドメインのDMARCポリシーと、使用している認証モード、レポートの要求有無、レポートの送信先メールアドレス、といった、追加パラメータを確認します。

DMARCを正しく設定し、DMARC XMLレポートの受信が始まったら、レポートの表示や潜在的な問題の分析を行う様々なオンラインツールが利用できます。利便性向上のため、¥MDaemon¥App¥フォルダの中にも、DMARCレポーターというツールがパッケージされています。DMARCReporterReadMe.txtで使用方法を確認して下さい。

DMARC TXTリソースレコードの定義

以下は最も基本的な、広く使われているDMARCレコードです。詳細な情報や、設定方法については、こちらを参照して下さい: www.dmarc.org.

Ownerフィールド

DMARCリソースレコードのOwner（又は「Name」や「left-hand」）フィールドは **_dmarc** で指定するか、レコードを適用するドメインやサブドメインを指定するための **_dmarc.domain.name** を使用します。

例:

example.comのDMARCレコード

```
_dmarc IN TXT "v=DMARC1;p=none"
```

このレコードは user@example.com や、user@support.example.com, user@mail.support.example.comといった、example.comのサブドメインからのメール全てに適用されます。

```
_dmarc.support.example.com IN TXT "v=DMARC1;p=none"
```

このレコードはuser@support.example.comには適用されますが、user@example.comには適用されません。

```
_dmarc.support IN TXT "v=DMARC1;p=none"
```

このレコードは user@support.example.com, user@a.support.example.com, user@a.b.support.example.comなどからのメール全てに適用されます。

DMARCレコードのタグと値

必須タグ

タグ	値	説明
v=	**DMARC1**	これはバージョンタグで、DMARC用レコードのテキストの最初のタグとなります。他のDMARCタグは大文字小文字の区別はありませんが、**v=**タグの値は全て大文字である必要があります: **DMARC1**.

		例: `_dmarc IN TXT "v=DMARC1;p=none"`
p=	**none** **quarantine** **reject**	これはPolicyタグで、DMARCレコードのv=タグに続き2つ目のタグとなります。 **p=none** は宛先サーバーがDMARCクエリの結果に対して何も行いません。DMARCチェックに失敗したメールも、それが原因で隔離されたり失敗したりする事はありませんが、DMARCとは関係のないスパムフィルタテストや他の原因での隔離や拒否の可能性はあります。 **p=none** は「監視」や「監視モード」と呼ばれる事もあり、これは **rua=** タグと同時に使用する事で、メールに関するレポートを宛先ドメインから受け取る事ができるようになるため、DMARCチェックに失敗した原因を把握するという目的で使用できるためです。このポリシーはDMARCのテスト完了まで使用する事ができ、より制限をかけるための**p=quarantine** ポリシーへ移行するための準備が行えます。 **p=quarantine** は他のメールサーバーが、From: ヘッダで自分のドメインを名乗っていて、DMARCチェックに失敗したメールを疑わしいメールとして扱うよう求めるポリシーです。サーバーのローカルポリシーによって、こうしたメールは追加の確認が行われたり、宛先ユーザーのスパムフォルダへ配信されたり、他のサーバーへ転送されたり、その他の処理が行われます。 **p=reject** は宛先メールサーバーに、DMARC検証に失敗したメールを拒否するよう求めるポリシーです。サーバーによっては、こうしたメールを拒否せずに受信し、隔離フォルダへ格納したり、件名に追加の文字列を挿入したりする場合もあります。これは最も厳しいポリシーで一般的にはお使いのメールポリシーやメールの利用者が確実に分かっている場合以外では使用しません。例えば、ユーザーがサードパーティーのメーリングリストに所属する事を許可している場合、 **p=reject** によって正しいメールが配信拒否されてしまう事がよくあります。更に、特定のメーリングリストから、自動的にユーザーが購読解除されてしまう可能性もあります。 例: `_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:dmarc-report@example.net"`

オプションタグ
下記のタグはオプションです。タグが使われていない場合は、それぞれのデフォルト値が代わりに使用されます。

タグ	値	説明

sp=	**none** **quarantine** **reject** — デフォルト値: **sp=** がない場合は **p=** タグがドメインとサブドメインの両方に適用されます。	このタグはDMARCレコードを適用するドメインのサブドメインで使われるポリシーを指定するものです。例えば、このタグがexample.comの管理下のレコードで使われる場合、p=タグはexample.comからのメールへ使用し、sp=タグは、例えばmail.example.comなど、example.com内のサブドメインからのメールに使用されます。このタグがレコードに使われていない場合は、p=タグがドメインとサブドメインの両方へ適用されます。 例: `_dmarc IN TXT "v=DMARC1;p=quarantine;sp=reject"`

rua=	DMARC統計レポートの送信先となるメールアドレスをカンマで区切ります。メールアドレスはURIとして入力する必要があります: **mailto:user@example.com**
	—
	デフォルト値: **none**
	このタグがない場合、統計レポートは送信されません。
		このタグはFrom:の送信ドメインが自社のドメインだったものに関するDMARC統計レポートを受信サーバーへ要求するのに使われています。この中ではURIとして1つ又は複数のメールアドレスを(複数の場合はカンマで区切ったURIとして)指定します: **mailto:user@example.com**
		例:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:user01@example.com,mailto:user02@example.com"`
		一般的にここで指定するアドレスは対象レコードが管理しているドメインに所属するアドレスです。もしも他のドメインへレポートを送信する場合は、レポート送信先ドメインのDNSゾーンファイルにも、DMARCレポートを受け付けるための特別なDMARCレコードが必要です。
		example.comのレコード例:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:non-local-user@example.net"`
		example.netで必要なレコード:
		`example.com._report._dmarc TXT "v=DMARC1"`

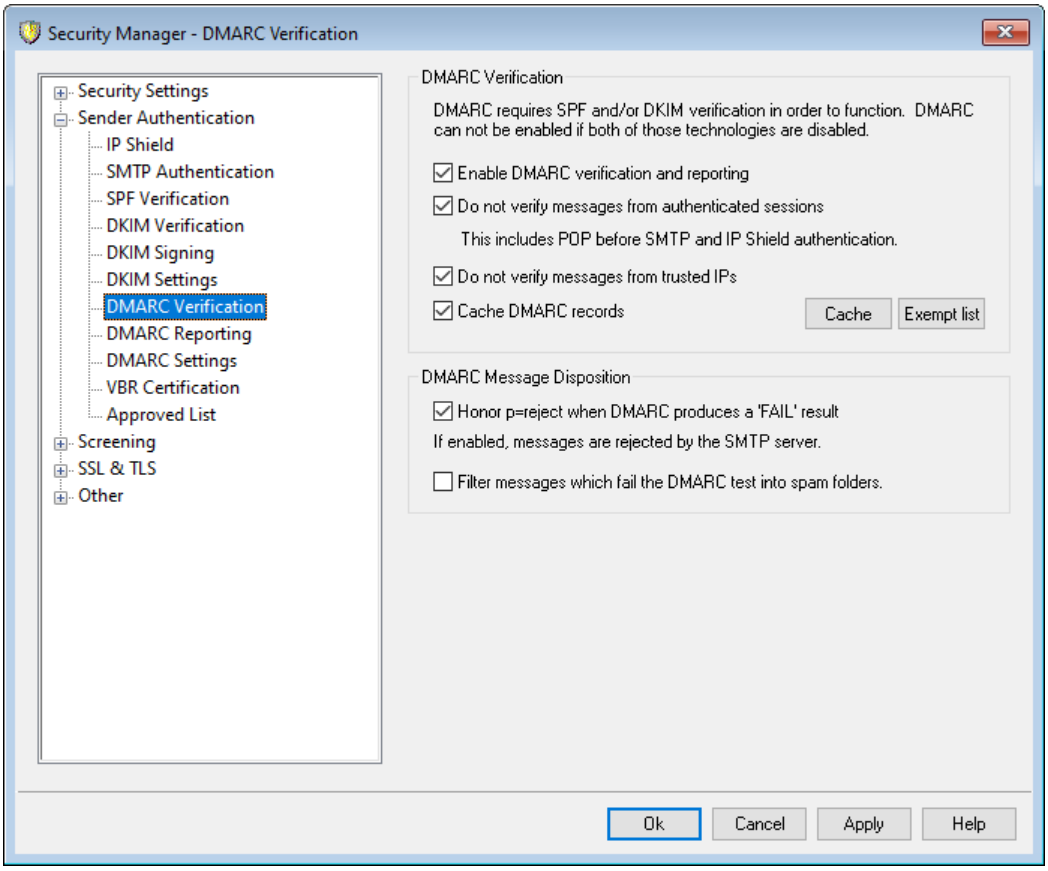
ruf=	DMARC失敗レポートの送信先となるメールアドレスをカンマで区切ります。メールアドレスはURIとして入力する必要があります: **mailto:user@example.com**
	
	—
	
	デフォルト値: **none**
	
	このタグがない場合、統計レポートは送信されません。
		このタグはFrom:の送信ドメインが自社のドメインだった場合で、受信メールがfo=タグの条件に一致した場合、DMARC失敗レポートを受信サーバーへ要求するのに使われています。デフォルトで、fo=タグがない場合、失敗レポートはメールが(例えばSPFとDKIMの両方に失敗した場合など)全てのDMARC検証に失敗した場合にのみ送信されます。この中ではURIとして1つ又は複数のメールアドレスを(複数の場合はカンマで区切ったURIとして)指定します: **mailto:user@example.com**
		
		例:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:dmarc-failures@example.com"`
		
		一般的にここで指定するアドレスは対象レコードが管理しているドメインに所属するアドレスです。もしも他のドメインへレポートを送信する場合は、レポート送信先ドメインのDNSゾーンファイルにも、DMARCレポートを受け付けるための特別なDMARCレコードが必要です。
		
		example.comのレコード例:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:non-local-user@example.net"`
		
		example.netで必要なレコード:
		`example.com._report._dmarc TXT "v=DMARC1"`

DMARCの仕様に関する詳細な情報は、次を参照して下さい: www.dmarc.org.

参照:

DMARC検証 494
DMARCレポート 496
DMARC設定 499
メーリングリスト » 設定 254
メーリングリスト » ヘッダ 257

4.1.2.5.1 DMARC検証



DMARC検証

DMARC検証とレポートを有効にする
このオプションを有効にすると、MDaemonは受信メールのFrom:に含まれているドメインについて、DMARC DNS問合せを行い、DMARCレポート[496]画面で設定されていれば、統計レポートや失敗レポートの送信を行います。DMARCはメールの検証にSPF[479]やDKIM[482]を使っているため、DMARCを使う前に最低どちらか1つの機能は有効化されている必要があります。DMARC検証とレポートはデフォルトで有効になっており、ほとんどのMDaemon設定で使用されています。

> DMARC対応を無効化する事で、スパム、フィッシング、その他の不正なメールが増加する可能性があります。また、メーリングリストのメールが他のサーバーで拒否されたり、リストメンバーが自動削除されてしまう可能性があります。DMARCは、確実にその意味を把握している場合を除いて、無効化はお勧めしていません。

認証済セッションからのメッセージを検証しない
デフォルトでMDaemonは認証済セッションから届いたメールに対してはDMARC検証を行いません。認証方式にはSMTP認証[476], POP before SMTP[471], IPシールド[474]が含まれます。

信頼するIPからのメッセージを検証しない
デフォルトでMDaemonは信頼するIP[473]からのメールに対してはDMARC検証を行いません。

DMARCレコードをキャッシュする

デフォルトでMDaemonはDNSルックアップで確認したDMARCレコードをキャッシュします。一時的にこの情報をキャッシュとして保持する事で、同じドメインから続けて到着するメール受信を効率化できます。

キャッシュ

このボタンでDMARCキャッシュを起動します。ここへは現在キャッシュされているDMARCレコードが一覧表示されています。

除外リスト

このボタンをクリックすると、DMARCから除外するリストが起動します。ここで指定されたIPからのメールはDMARC検証の対象にはなりません。

DMARC検証ではVBR証明書 503 や 承認リスト 506 も使用する事ができ、除外リストはDKIM認証やSPFパスを元に作成されています。例えばメールがDMARC検証に失敗した場合でありながら、承認リストのドメインから送られたものであり、正しいDKIM署名も付与されている場合、メールはDMARCポリシーの制限を受ける事はありません（メールはポリシーが"p=none"だった場合と同様に扱われます）。SPF検証において、対象ドメインが承認リストのドメインと一致した場合においても、これと同じ状態となります。

DMARCメッセージ処理

DMARC処理にて'FAIL'の結果があった場合p=rejectとして扱う

デフォルトでこのオプションは有効となっており、メールのFrom:ドメインがDMARCレコードポリシーを公開していて対象メールがDMARC検証に失敗した場合、MDaemonはp=rejectのDMARCポリシーを受け入れます。DMARC検証に失敗したメールはSMTPセッション中に拒否されます。

このオプションが無効の場合にDMARC検証に失敗すると、MDaemonはメールを拒否する代わりに、"X-MDDMARC-Fail-policy: reject"をヘッダへ挿入します。この場合はコンテンツフィルタでヘッダの存在を元に、メールを特定のフォルダへ移動するなどの処理を行う事ができます。更に「DMARC検証に失敗したメールをスパムフォルダへ振り分ける」オプションを使って、メールを宛先ユーザーのスパムフォルダへ振り分ける事もできます。

このオプションを無効にしていた場合でも、メールはDMARCに関連しない、例えばスパムフィルタスコア 617 がしきい値を超えていた場合など、他の理由で拒否される可能性があります。

DMARCテストで失敗したメールをスパムフォルダへ振り分ける

メールがDMARC検証で失敗した場合、宛先アカウントのスパム(Junk E-mail)フォルダへ振り分ける場合は、このオプションを有効にします。フォルダが存在していない場合、必要に応じてMDaemonがフォルダを自動生成します。

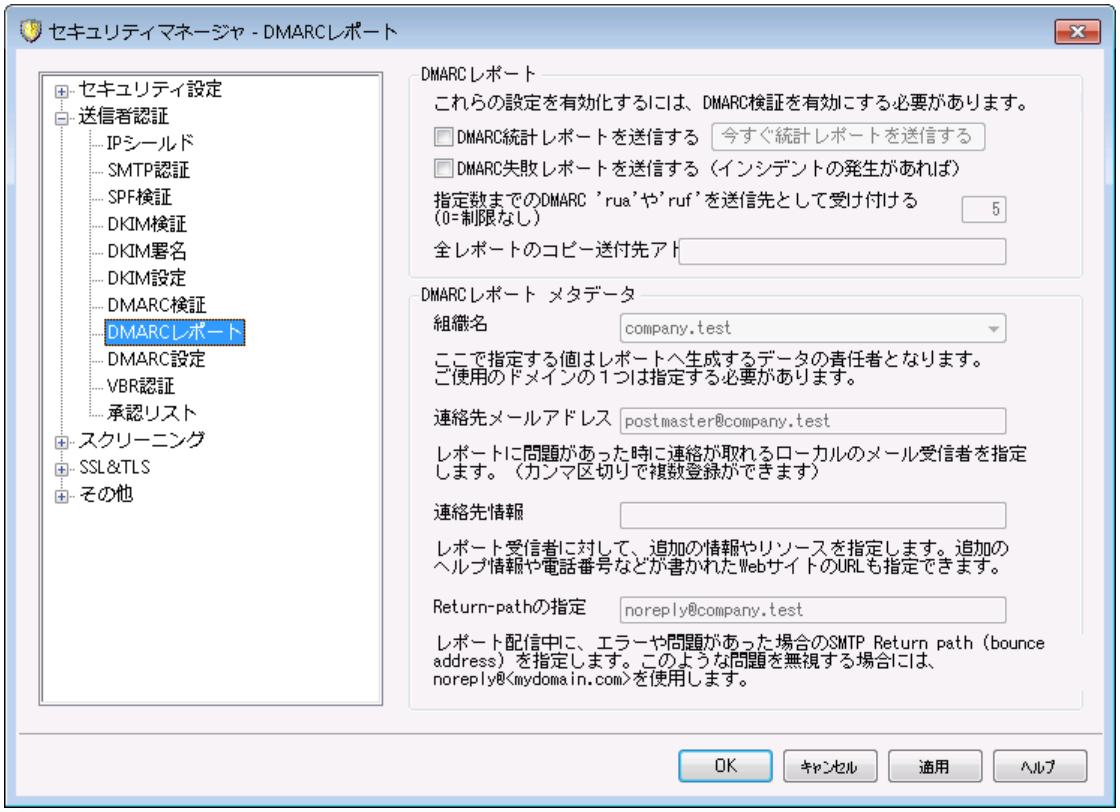
有効化すると、このオプションはFrom:ドメインが制限DMARCポリシー(例:p=quarantine or p=reject)の場合にのみ適用されます。ドメインの公

> 開ポリシーがp=noneだった場合、DMARCはドメインを監視しているだけで、それを規制する処理は行わないという事を示しています。

参照:

DMARC 488
DMARCレポート 496
DMARC設定 499
メーリングリスト » 設定 254
メーリングリスト » ヘッダ 257
承認リスト 506

4.1.2.5.2 DMARCレポート



MDaemonがDNSへDMARCレコードの問合せを行った際、DMARCレコードに、対象ドメイン所有者が、そのドメインを名乗ったメールをレポートとして提供するように求めるタグが含まれている場合があります。DMARCレポートのオプションでは、要求されている統計又は失敗レポートを送信するかどうかや、レポートに追加するメタ情報の指定を行う事ができます。この画面にあるオプションは、DMARC検証 494 でDMARC検証とレポートを有効にする オプションが有効化されている場合にのみ利用できます。また、DMARCの仕様によると、レポートの宛先サーバーが対応していれば、レポート送信にはSTARTTLS 525 を使用する必要があります。STARTTLSを可能な限り有効化して下さい。

DMARCレポート

DMARC統計レポートを送信する

DMARC統計レポートを要求しているドメイン宛に、統計レポートを送信するにはこのオプションを有効にします。メールのFrom:ドメインに対しDMARC DNSクエリを行った際、DMARCレコードに"rua="タグ（例．rua=mailto:dmarc-reports@example.com）が入っていたら、それはドメイン所有者がDMARCの統計レポートを希望していることを意味しています。MDaemonは受信したメールの中から対象ドメインを名乗っていたものについて、DMARC関連情報を保存しておきます。統計レポートの送信先メールアドレス、各メッセージの検証方式（SPF，DKIM，両方）、メールが検証に成功したかどうか、送信元サーバー、IPアドレス、適用したDMARCポリシー、その他の情報が含まれます。この情報を元に作成したレポートが、毎日UTCの深夜、対象ドメインに送られます。レポート送信後は、保存されていたDMARCデータがクリアされ、MDaemonは全てのプロセスを最初からやり直します。

MDaemon はDMARCレポートで、統計レポートのインターバルタグ（例．"ri="）に対応していません。MDaemonは統計レポートを毎日UTCの深夜にDMARCデータを所有しているドメイン宛に、前回レポート送信後に保持されたデータを元にしたレポートを送信します。

今すぐ統計レポートを送信する

現在保存されているDMARCデータを使って、次回のUTC深夜にレポートを自動送信するのではなく、すぐに統計レポートの生成と送信を行うにはこのボタンをクリックします。これによりレポートはすぐに送信され、UTC深夜に実行される場合と同様、保存されているDMARCデータはクリアされます。MDaemonは次の深夜UTCイベントか、再度このボタンをクリックするまでの、どちらか早い方までの間、再度DMARCデータの蓄積を開始します。

MDaemonは統計レポート送信やDMARCデータのクリアを行うため、UTCの深夜に稼働している必要があります。MDaemonが該当の時間帯に停止していた場合、レポートは生成されず、DMARCデータもクリアされません。このデータはMDaemonが再度稼働した際引き続き蓄積されますが、レポートは次回のUTC深夜のイベントか、今すぐ統計レポートを送信するボタンを押すまで生成されません。

DMARC失敗レポートを送信する（インシデントの発生があれば）

DMARC失敗レポートを要求しているドメイン宛に、失敗レポートを送信するにはこのオプションを有効にします。メールのFrom:ドメインに対しDMARC DNSクエリを行った際、DMARCレコードに"ruf="タグ（例．ruf=mailto:dmarc-failure@example.com）が入っていたら、それはドメイン所有者がDMARCの失敗レポートを希望していることを意味しています。統計レポートと違い、このレポートはインシデントが発生すると生成され、失敗を引き起こした事象やエラーの詳細が含まれています。レポートはドメイン管理者がメールシステムの設定やフィッシング攻撃といった他の問題によって起こった事象を解析するために使用する事ができます。

失敗レポートを生成するきっかけとなる失敗の種類はドメインのDMARCレコードにある"fo="タグの値によって異なります。デフォルトの失敗レポートは実施されたDMARCチェック全てで失敗（例． SPFとDKIMの両方で失敗）した場合に生成されますが、ドメインは様々な"fo="タグを使用する事ができ、例えばSPFに失敗した場合や、DKIMに失敗した場合、どちらかに失敗した場合、その他の組み合わせなど、要望に応じて失敗レポートの生成を行う事ができます。また、失敗レポートは、DMARCレコードの"ruf="タグを公開している宛先数、"fo="タグの値、メールの処理中発生した認

証失敗の数に応じて複数生成されます。MDaemonが送信するレポートの宛先数を制限するには、次の、指定数までのDMARC ruaやrufを宛先として受け付ける オプションを使用します。

レポートのフォーマットについて、MDaemonはrf=afrf タグ（Authentication Failure Reporting Using the Abuse Reporting Format）のみを許可しており、これはDMARCのデフォルトです。全てのレポートはDMARCレコードにrf=iodef が含まれていた場合であっても、このフォーマットで送信されます。

DMARC失敗レポートに対応するため、MDaemonでは次の機能に完全対応しています: RFC 5965: An Extensible Format for Email Feedback Reports, RFC 6591: Authentication Failure Reporting Using the Abuse Reporting Format, RFC 6652: Sender Policy Framework (SPF) Authentication Failure Reporting Using the Abuse Reporting Format, RFC 6651: Extensions to DomainKeys Identified Mail (DKIM) for Failure Reporting, RFC 6692: Source Ports in Abuse Reporting Format (ARF) Reports.

DMARCの "fo="タグでSPF関連の失敗レポートを要求された場合、MDaemonはSPF失敗レポートをRFC 6522に基づいて生成します。そのため、仕様の拡張がドメインのSPFレコードに含まれている必要があります。SPF失敗レポートはDMARC処理とは独立して送信されたり、RFC6522拡張なしで生成される事はありません。

DMARCの "fo="タグでDKIM関連の失敗レポートを要求された場合、MDaemonはDKIM失敗レポートをRFC 6651に基づいて生成します。そのため、仕様の拡張がドメインのDKIM署名のヘッダフィールドに含まれており、ドメインのDNSでは正しいDKIMレポート用TXTレコードを公開している必要があります。DKIM失敗レポートはDMARC処理と独立して送信されたり、RFC6651拡張なしで生成される事はありません。

指定数までのDMARC 'rua'や'ruf'を宛先として受け付ける（0 = 制限なし）
MDaemonが送信するDMARC統計レポートやDMARC失敗レポートの宛先の数を制限する場合は、ここで最大数を指定します。DMARCレコードのrua=やruf=タグに指定した最大数以上のアドレスが含まれていた場合は、記載されていたアドレスの順番に、最大数に到達するまでMDaemonはレポートを送信します。デフォルトではこの数に制限はありません。

全レポートのコピー送付先アドレス:
1つ又はカンマで区切った複数アドレスを入力します。ここで入力したアドレスへはDMARCの全統計レポート及び失敗レポート（fo=0又はfo=1のみ）のコピーが送信されます。

DMARCレポートメタデータ

次のオプションは組織のメタデータを指定するのに使用し、DMARCレポートの中に含まれます。

組織名
DMARCレポートの責任者となる組織名です。これはMDaemonドメインである必要があります。使用するドメインをドロップダウンリストから選択します。

連絡先メールアドレス
レポートに関する問題等を連絡する相手のメールアドレスを指定します。複数アドレスはカンマで区切ります。

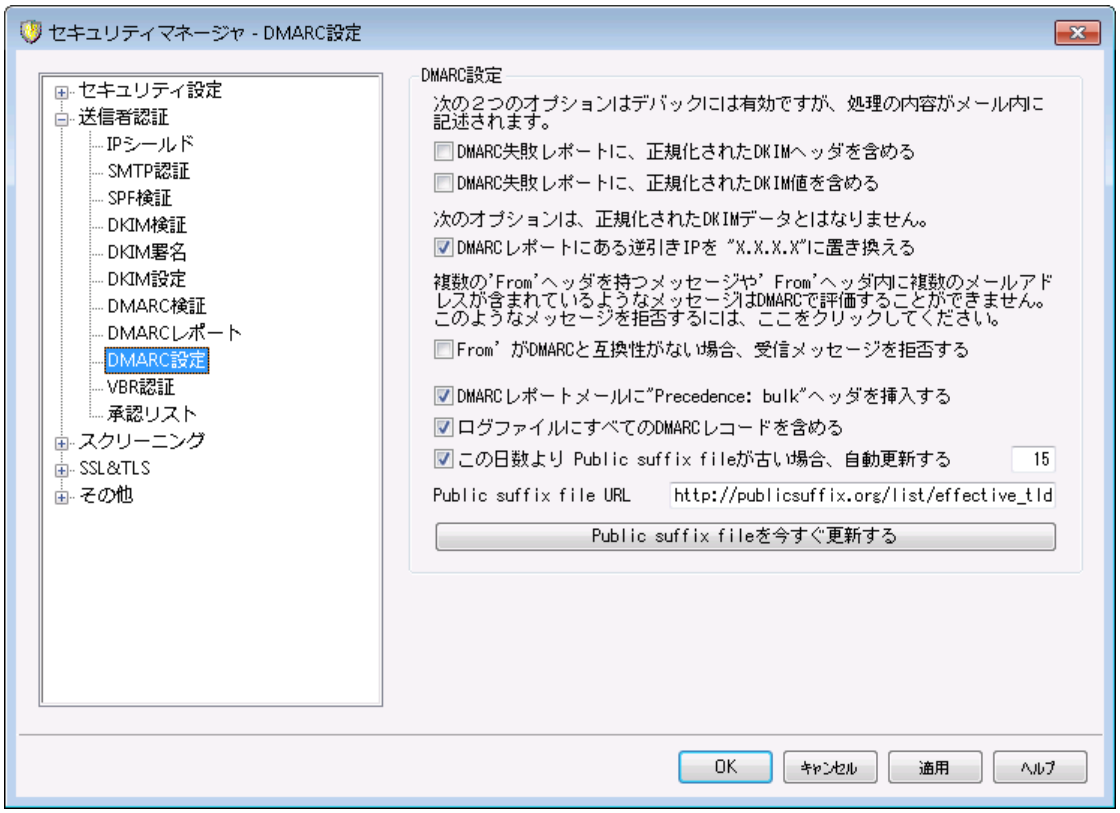
連絡先情報
レポートの宛先ユーザー向けに追加の連絡先情報を入力します。これには、ウェブサイト、電話番号などが含まれます。

return-pathの指定
MDaemonが送るレポートメール用のSMTP return path（メラーメールの戻り先アドレス）で、配信エラーが発生した場合に使用します。こうした問題を無視するには`noreply@<mydomain.com>`を使用します。

参照:

DMARC 488
DMARC検証 494
DMARC設定 499

4.1.2.5.3 DMARC設定



DMARC設定

DMARC失敗レポートに正規化されたDKIMヘッダを含む
DMARC失敗レポート[496]へDKIMの正規化ヘッダ[486]を含むにはこのオプションを有効にします。これはデフォルトで無効になっています。

DMARC失敗レポートに正規化されたDKIM本文を含む
DMARC失敗レポート[496]へDKIMの正規化本文[486]を含むにはこのオプションを有効にします。これはデフォルトで無効になっています。

DMARCレポートにある逆引きIPを"X.X.X.X"に置き換える
デフォルトでMDaemonはDMARCレポートの逆引きIPを"X.X.X.X"に置き換えます。DMARCレポートで逆引きIPも確認できるようにする場合はこのオプションを無効化して下さい。このオプションはDKIMの正規化データには適用されません。

'From'がDMARCと互換性がない場合受信メッセージを拒否する
Fromヘッダの構成がDMARCの要件に対応していないメールを拒否する場合はこのオプションを有効にして下さい。複数のFromヘッダを持つメールや1つのFromヘッダに複数メールアドレスが含まれているメールがありますが、このようなメールは現時点ではDMARC処理から除外されています。複数のアドレスを1つのFromヘッダで指定する事は、技術的にプロトコルに反しているわけではないため、この設定はデフォルトで無効になっています。ただし、この設定を有効にすることで、DMARCで最大限に保護する事もできます。この設定はDMARC検証[494]が有効になっている場合のみ適用できます。

DMARCレポートメールに"Precedence: bulk"ヘッダを挿入する
デフォルトでMDaemonはDMARCレポートメールへbulkメールヘッダを挿入します。このヘッダを挿入しないようにするには、このチェックボックスをオフにしてください。

ログファイルに全てのDMARCレコードを含める
デフォルトでMDaemonはDMARC DNSクエリで取得したDMARC DNSレコード全てをログに記録します。DMARC DNSレコード全てをログに残さないようにするには、このチェックボックスをオフにしてください。

この日数よりpublic suffix fileが古い時自動更新する
DMARCではDNSレコードの問合せ先ドメインの信頼性を確認するため、public suffix fileを要求します。デフォルトでMDaemonは保持している15日経過したpublic suffix fileを自動更新します。この日数を変更したい場合は値を任意のものへ変更して下さい。自動アップデートを行わない場合はこのオプションを無効にします。

Public suffix file URL
MDaemonがDMARC用にダウンロードするpublic suffix fileのURLです。デフォルトでMDaemonはhttp://publicsuffix.org/list/effective_tld_names.datを使用します。

Public suffix fileを今すぐ更新する
Publix suffix file URL からpublic suffix fileをすぐに更新するには、このボタンをクリックします。

参照:

DMARC 488
DMARC検証 494
DMARCレポート 496
DKIM設定 486

4.1.2.6 メッセージ証明書

メッセージ証明書は、第3者機関が、正規のメールであることを[証明]するためのプロセスで使用されます。そのため、証明書つきメールの受信者は、送信者のメールアドレスドメインに対して安心感をもち、メールを受け取る事ができるようになります。このサーバからの受信メールは、証明されたものであり、スパムメールなどの問題を送ることはない、という判断につながります。証明書を使うと、送信する側の組織にとってもメリットがあります。証明書は誤りなどにより不用意にスパムフィルタに適合する可能性を防ぐことができるため、それぞれのメッセージ配送に必要なリソースを軽減する手助けにもなります。

MDaemon は、"Vouch-By-Reference"(VBR)と呼ばれている新しいインターネットメールプロトコルを使ったメッセージ証明書に対応しており、世界で最初の商用での実装を実現しています。メッセージ証明をサポートし、MDaemon Technologiesは、Domain Assurance Council(DAC)へのその参加を通して、拡張の支援にために作業しています。VBRはCertification Service Providers(CSP)か、特定のドメインからの、正規メールの[認証局]を利用したメカニズムを提供しています。

受信メールの証明

メッセージ証明書機能を使って、MDaemonでは簡単に受信メールをチェックするよう構成を行えます。VBR証明書ダイアログ(**セキュリティ » セキュリティ設定 » 送信者認証 » VBR証明書**)で、**受信メッセージの証明書を有効にする**を選択し、受信メール(例えばvbr.emailcertification.org)について保証する信用する一つ以上の証明提供者を指定するだけです。さらにスパムフィルタリングから証明されたメッセージを免除あるいは有益な調整をスパムフィルタスコアに与えるか選択をすることができます。

送信メールの証明

MDaemonで外向けメッセージに証明書を挿入する構成が可能です。その前に、最初にCPSがメールを証明するように準備する必要があります。MDaemon Technologiesは、証明書サービスをMDaemonユーザに提供しています。詳細はこちらを参照して下さい: www.mdaemon.com

CSPに名前を登録した後で、アウトバウンドメッセージでメッセージ証明書を使用するよう、MDaemonサーバを構成します:

1. VBR証明書ダイアログを開きます。
   (セキュリティ » セキュリティ設定 » 送信者認証 » VBR証明書
2. **送信メッセージへ証明書データを挿入する**を選択します。
3. **メッセージ証明書のドメインを編集する** を選択します。[証明書設定]ダイアログが開きます。
4. 証明書データを持つ外向けメッセージのドメイン名を入力してください。
5. [メールタイプ]ドロップダウンリストからCSPが、このドメインに対して証明することに適するメールタイプを選ぶか、タイプが記載されない場合、新規のタイプを入力してください。

6. ドメインのアウトバウンドメッセージを証明するCSPを入力してください。複数のCSPを所有している場合、半角スペースを使用し区切ります。
7. OKをクリックします。
8. DKIM[481]でドメインの送信メッセージに署名したり、SPF[479]承認されたサーバから送信するよう、サーバを設定します。これは、適切にメッセージが創造したという保証に必要です。受信サーバでメッセージが確実であると最初に確定することができない限り、メッセージを証明することができません。

VBRは、証明書付のメールやCSPへの配信を要求するものではありません。CSPはメールの署名や検証を行うためのものではなく、ドメインのメール基準を満たしているかどうかを確認するためのものです。

MDaemon Technologiesが提供している電子メール証明書について:
http://www.mdaemon.com/email-certification/

VBRの仕様 - RFC 5518:

http://tools.ietf.org/html/rfc5518

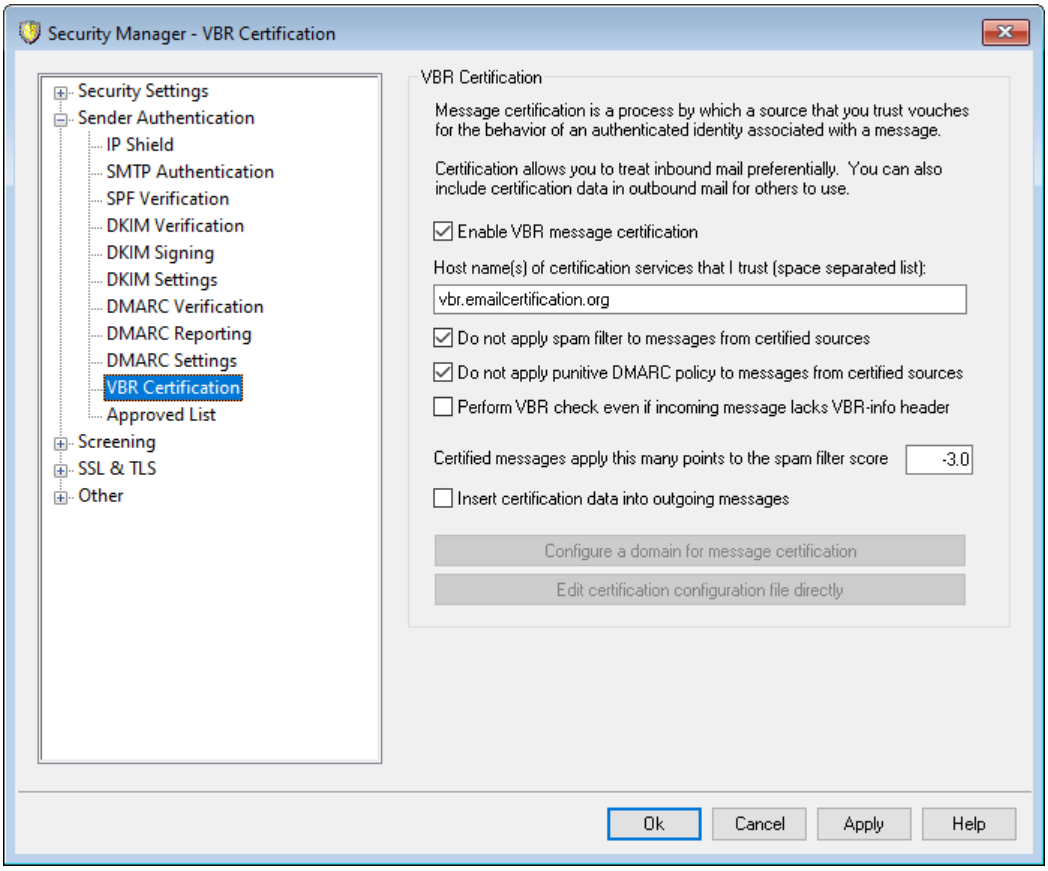
DKIMについて:

http://www.dkim.org/

参照:

VBR証明書[503]

4.1.2.6.1 VBR証明書



VBR証明書ダイアログは、セキュリティ ≫ セキュリティ設定 ≫ 送信者認証 ≫ VBR証明書で表示できます。

VBR証明書

VBRメッセージ証明書を有効にする
受信メッセージに証明書を使用するには、このチェックボックスを選択します。MDaemonが証明書を必要としているInboundメッセージを受信する場合、メッセージが実際のところ、[証明された]かどうか確認する信頼されたCSPを問い合わせます。その場合、下記の選択したオプションにしたがって、メッセージはスパムフィルタ[616]から免除されるか、スパムフィルタスコアが調節されます。

信頼する証明書サービスのホスト名(スペース区切りのリスト):
このボックスを使用して、信頼する証明書サービスのホスト名を入力します。複数のサービスを信頼する場合にはスペースで区切って入力します。

証明されたソースからのメールにはスパムフィルタを適用しない
このオプションはスパムフィルタリングから証明されたメッセージを除外する場合に選択します。

証明されたソースからのメールには罰則DMARCポリシーを適用しない
このオプションは罰則DMARCポリシー[494](例. p=quarantine や p=reject)から証明されたドメインからのメールでDMARCチェックに失敗したメールを除外する場合に選択します。このオプションはデフォルトで有効です。

VBR-infoヘッダのない受信メッセージに対してもVBRチェックを実施する
受信メールにVBR-Infoがないメールでも VBRチェックを行うにはこのオプションを有効にします。通常このヘッダは必要ですが、VBRはそれがなくとも動作します。ヘッダがなかった場合、MDaemonは信頼するCSPへ"all"メールタイプを使って問合せを行います。このオプションはデフォルトで無効になっています。

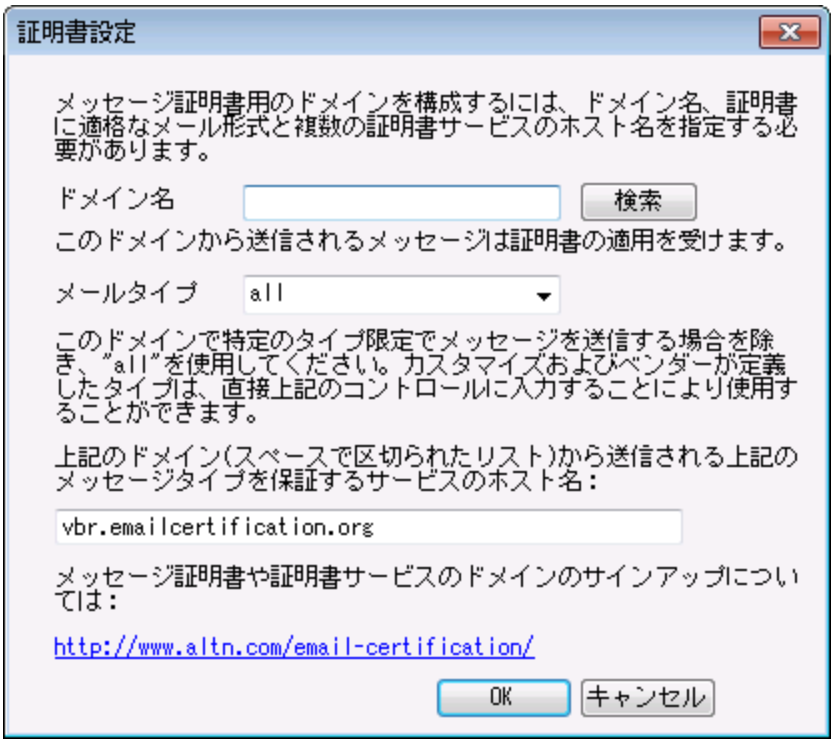
証明されたメッセージは、スパムフィルタスコアへこのポイントを追加する
証明されたメッセージをスパムフィルタリングから除外しない場合は、このオプションでメールのスパムフィルタスコアを調節できます。通常、証明されたメールは、その値を有利にするため、スパムスコアは減算用に負の値が指定されます。デフォルト設定は、-3.0です。

送信メッセージへ証明書データを挿入する
外向けメッセージへ証明書データを挿入する場合、このチェックボックスを選択します。さらに[**メッセージへ証明書のドメインを編集する**]ボタンをクリックして[**証明書設定**]ダイアログを表示します。証明されている特定のドメインおよび関連しているCSPを指定してください。

メッセージ証明書のドメインを編集する
上記の[**送信メッセージへ証明書データを挿入する**]オプションを可能にした後に、証明書セットアップダイアログを開くために、このボタンをクリックしてください。このダイアログでアウトバウンドメッセージが証明されるドメイン、証明されるメールのタイプ、ならびにドメインと関連しているCSPを指定します。

証明書構成ファイルを直接編集する
上記の[**送信メッセージへ証明書データを挿入する**]オプションを有効にした後、このボタンをクリックすると、Vouch-by-Reference (VBR)構成ファイルが開きます。関連するVBRデータに加えVBRを使用するために証明書設定ダイアログで構成した任意のドメインを、このファイルに記載します。このファイルを使用してエントリを編集、あるいは新規エントリを編集できます。

証明書設定



証明書ダイアログで[送信メッセージへ証明書データを挿入する]を有効にした後、[証明書設定]ダイアログを開くには[メッセージ証明書のドメインを編集する]ボタンをクリックします。このダイアログは、アウトバウンドメッセージが証明されるドメイン、証明されるメールおよびドメインと関連しているCSPのタイプを指定するために使用します。

証明書設定

ドメイン名
アウトバウンドメッセージが証明されるドメインを入力するために、このオプションを使用してください。

検索
以前に特定のドメインのためにメッセージ証明書設定を構成した場合、ドメイン名を入力し、このボタンをクリックし、ドメインの設定が証明書設定ダイアログのオプションで一覧にされます。

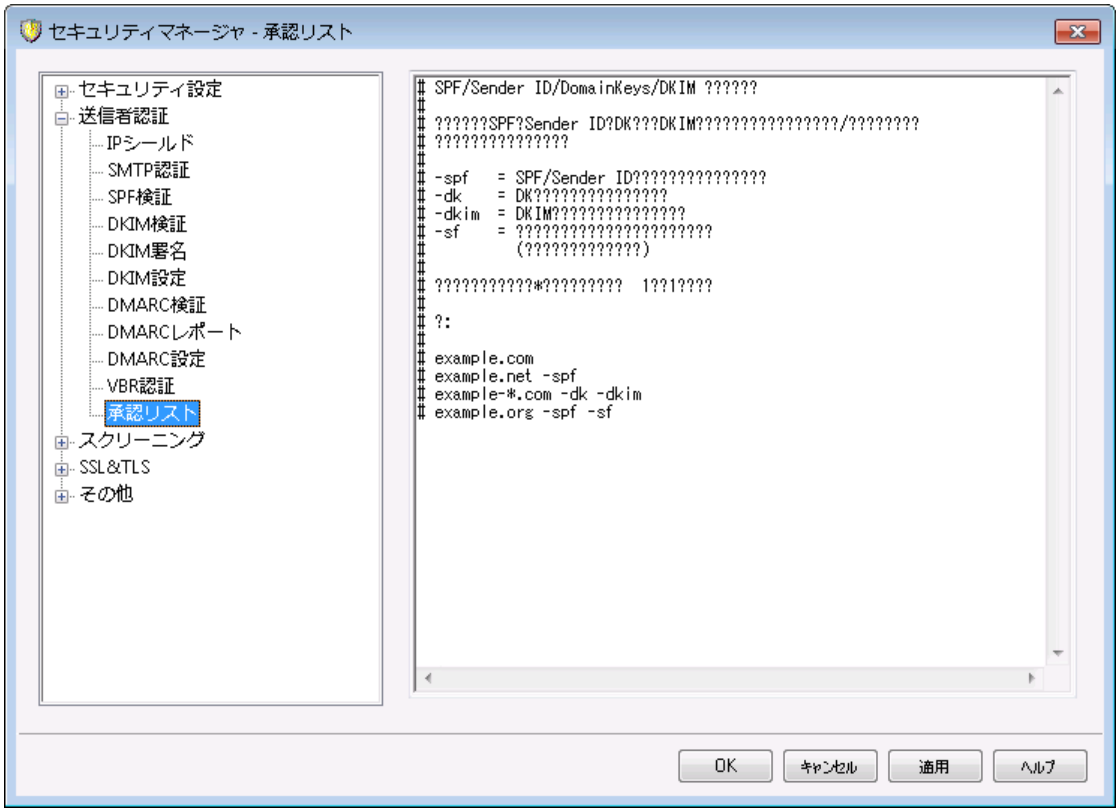
メールタイプ
関連するCSPが、このドメインに対して証明に受諾するメールタイプをドロップダウンリストから選んでください。タイプがリストにない場合、手動で入力することができます。

サービスのホスト名 …
ドメインのアウトバウンドメッセージを証明することに同意したCSPのホスト名を入力してください(例えばvbr.emailcertification.org)。複数のCSPを入力する場合、スペースでそれぞれを区切ってください。

参照:

メッセージ証明書 501

4.1.2.7 承認リスト



スパム送信者がSPFを使用し始めたり、有効なDKIMでメッセージに署名し始めたりしているので、メッセージが署名され認証されていて、有効なソースから発信されているものであっても、必ずしもそのメッセージがスパムではないという保証はありません。そのため、署名を引き継ぐドメインが認証リストにない限りは、SPFやDKIM検証の結果として、メッセージのスパムスコアが下げられることはありません。この許可リストは受信メッセージが検証された際、そのメッセージのスパムスコアを下げることを許可したドメインを指定するために必要です。

これらのドメインで署名されたメッセージが、SPFまたはDKIMで検証された場合、そのスパムスコアはSPF 479やDKIM検証 482画面での設定に基づいて減算されます。
しかし、以下にあるフラグ(やその組み合わせ)を追加することにより、これらの要素によりスコアが減算されるのを防ぐことができます。また、これらのフラグを使用することにより、検証されたメッセージがスパムフィルタを通過してしまうことを防ぐこともできます。

-spf このドメインから送信されたメッセージに対して、SPFによるスパムスコアの減算を行わない。

-dkim　このドメインから送信されたメッセージに対して、DKIM認証によるスパムスコアの減算を行わない。

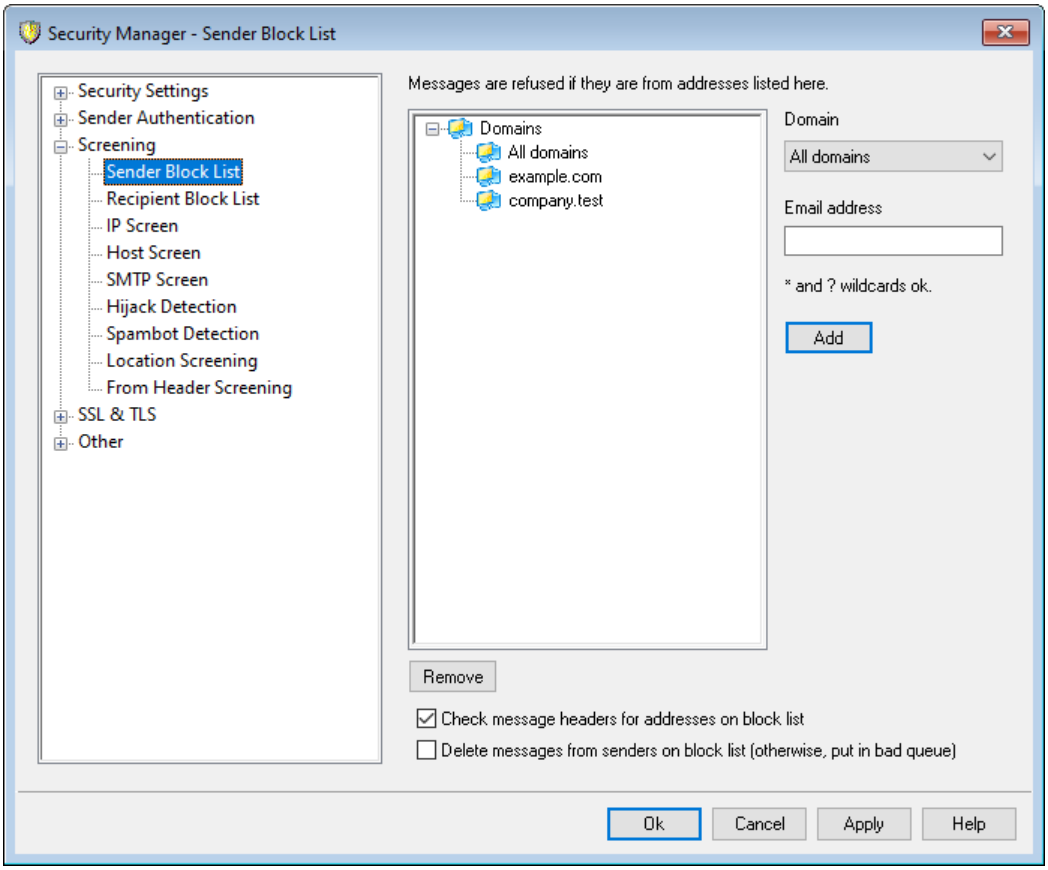
-sf　このドメインから送信されたメッセージに対して、スパムフィルタによる検証を行わない。

DMARCと承認リスト

DMARC検証 494 も、正規のDKIM署名や信頼するソースからのSPFのパスを元に作られた承認リストを使用しています。そのため、例えば、DMARCの検証に失敗したメールが、承認リストに一致するドメインからのもので、且つ正しいDKIM署名を使っていた場合、罰則DMARCポリシーは適用されません。(メッセージは、ポリシーをp=noneと設定していた時と同様に処理されます)。SPFパス検証が承認リストのドメインに一致した場合にもこれと同じ事が起こります。

4.1.3 スクリーニング

4.1.3.1 送信ブロックリスト



送信ブロックリストは、セキュリティ ≫ セキュリティ設定 ≫ スクリーニングで表示できます。ここにはサーバーでのメール送信が行えないアドレスを一覧で設定します。この一覧から届いたメッセージはSMTPセッション中に拒否されます。ユーザーの問題を操作するのに便利です。アドレスはドメイン毎か全体に対してブロックリスト化できます。

ここへ記載されているドメインからのメッセージを拒否する
ここには現在ブロックリストとして拒否しているアドレスが、ドメイン毎にリスト表示されています。

ドメイン
ブロックリストのアドレスに関連付けるドメインを選択します。特定のアドレスからのメール受信を拒否するドメインを選択します。Allドメインで全体で受信を拒否する事もできます。

メールアドレス
ブロックリストへ追加するアドレスを入力します。ワイルドカードが使用できるため、"*@example.net"は"example.net"からの全てのメールを意味し、"user1@*"は、ドメインに関わらず、user1@から始まるメールアドレス全てを意味します。

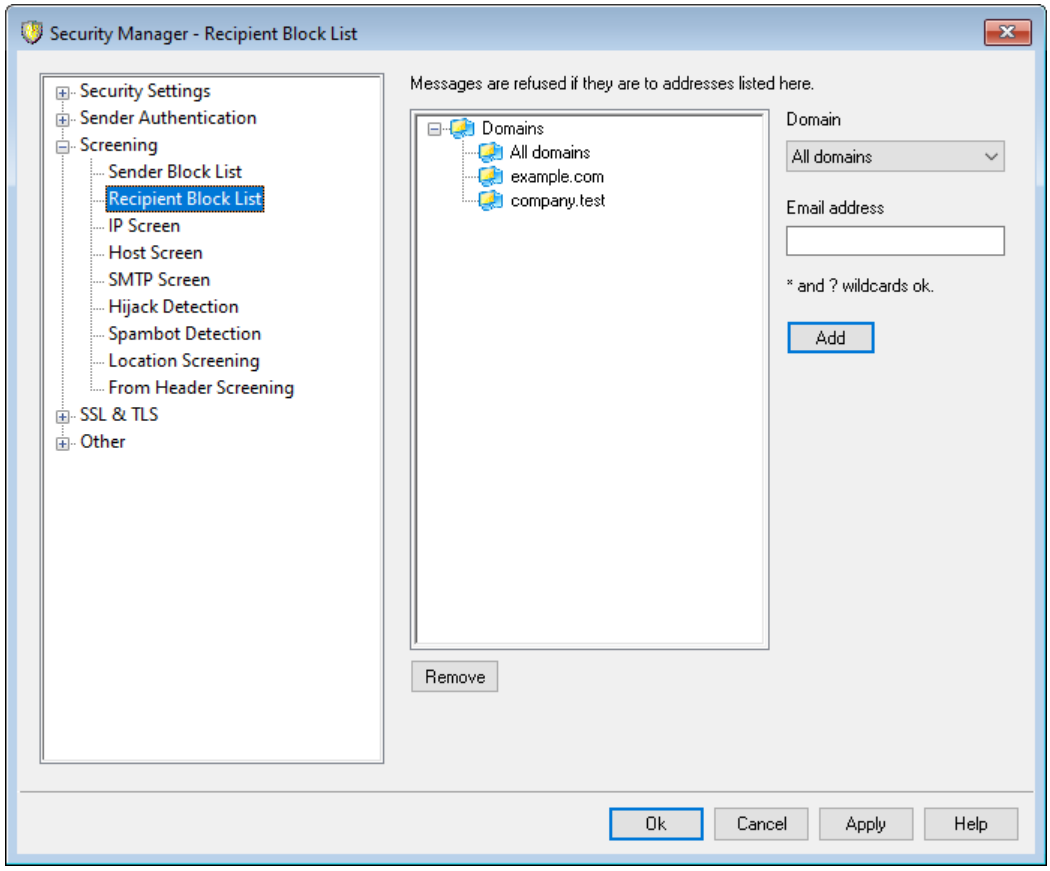
追加
ブロックリストへアドレスを追加するのにこのボタンを使用します。.

削除
ブロックリストへアドレスを追加するのにこのボタンを使用します。.

ブロックリストアドレスでメッセージヘッダを確認
デフォルトで、MDaemonはSMTPセッション中にFrom/Senderヘッダを確認します。これにより、メッセージがMTAによって後で検出され、badキューへ移動されるのを防ぐ事ができます。

ブロックリストに登録された送信者からのメールを削除する（又はbadキューへ配信する）
このオプションを有効にするとMDaemonは宛先ユーザーの個人用ラックリストに登録された送信元からのメールを削除します。通常のメールに加え、このオプションはMultiPOPやDomainPOP経由のメールへも適用されます。このオプションが無効の場合、メールはBadキューへ配信されます。このオプションはデフォルトで無効になっています。

4.1.3.2 宛先ブロックリスト



宛先ブロックリストは、セキュリティ ≫ セキュリティ設定 ≫ スクリーニングで表示できます。ここにはサーバーを通じてメール受信を許可していないアドレスを一覧で設定します。この一覧へ届いたメッセージは拒否されます。アドレスはドメイン毎か全体に対してブロックリスト化できます。宛先ブロックリストは(メッセージヘッダではなく)SMTP envelopeのRCPTデータのみを処理します。

ここへ記載されているアドレスへのメッセージを拒否する
ここには現在ブロックリストとして拒否しているアドレスが、ドメイン毎にリスト表示されています。

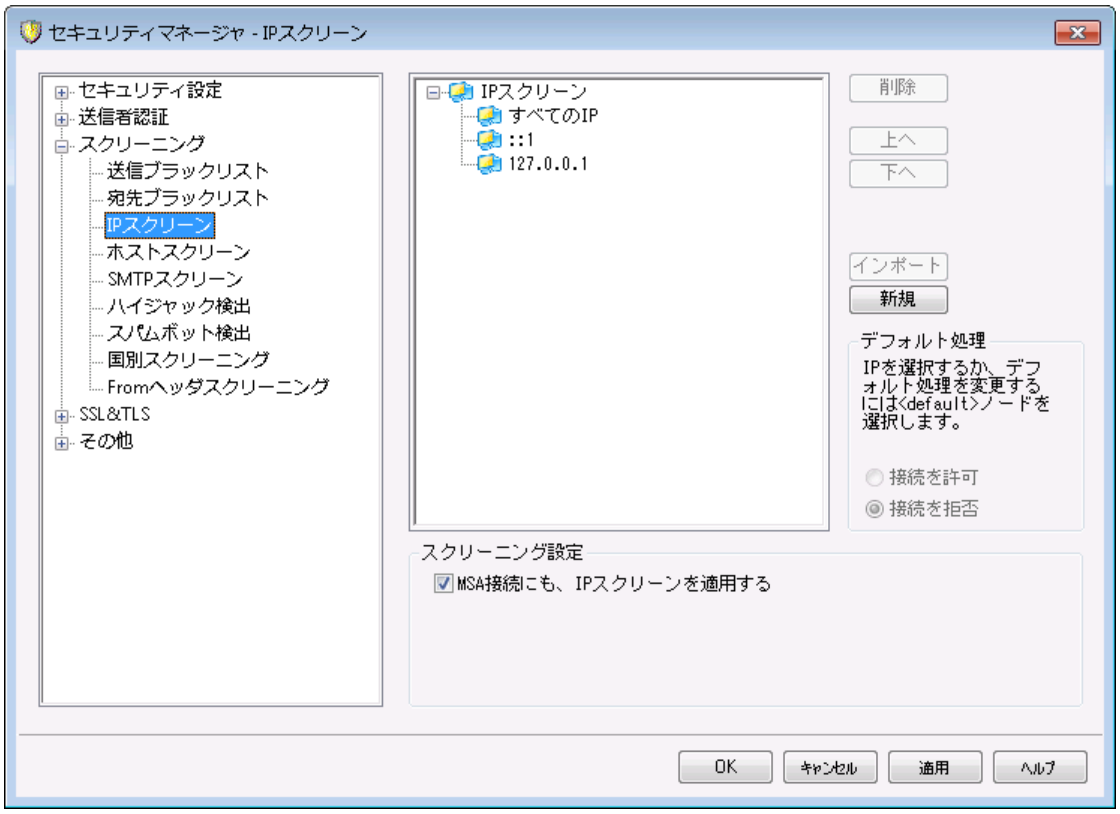
ドメイン
ブロックリストのアドレスに関連付けるドメインを選択します。特定のアドレスからのメール受信を拒否するドメインを選択します。Allドメインで全体で受信を拒否する事もできます。

メールアドレス
ブロックリストへ追加するアドレスを入力します。ワイルドカードが使用できるため、"*@example.net"は"example.net"からの全てのメールを意味し、"user1@*"は、ドメインに関わらず、user1@から始まるメールアドレス全てを意味します。

追加
ブロックリストへアドレスを追加するのにこのボタンを使用します。

削除
ブロックリストへアドレスを追加するのにこのボタンを使用します。

4.1.3.3 IPスクリーン



IPスクリーンは、セキュリティ ≫ セキュリティ設定 ≫ スクリーニングで表示できます。IPスクリーンは、ローカルIPアドレスに対して接続を許可するIPと接続を許可しないIPを指定するのに使用します。IPスクリーンで指定するIPアドレスは、ローカルアドレス全てを指定する事も、個々のIPを指定する事もできます。CIDR表記法およびワイルドカード*, #, and ?が使用できます。

例:

..*.*	すべてのIPアドレスと一致します。
#.#.#.#	すべてのIPアドレスと一致します。
192.*.*.*	192で始まるすべてのIPアドレスと一致します。
192.168.*.239	192.168.0.239から192.168.255.239までのIPアドレスと一致します。
192.168.0.1??	192.168.0.100から192.168.0.199までのIPアドレスと一致します。

新規IPスクリーンの登録

新しいIPスクリーンのエントリを作成するには、新規をクリックします。新規IPスクリーンの登録ダイアログが起動し、新しいIPスクリーンを登録できます。

ローカルIP
ドロップダウンリストから、適用する特定のIPか、[すべてのIP]のどちらかを選択してください。

リモートIP (CIDR、*?、#ワイルドカードが使用できます)
追加する上記のローカルIPに対応するリモートIPアドレスを入力します。

接続を許可
このオプションを選択すると指定したリモートIPアドレスが対応するローカルIPへ接続できるようになります。

接続を拒否
このオプションを選択と、指定したリモートIPアドレスから対象のローカルIPアドレスに対する接続が許可されません。接続は拒否または破棄されます。

インポート

IPアドレスを選択しこのボタンを押すとAPFや.htaccessファイルからIPアドレスデータをインポートします。MDaemonは、現時点で次の情報にのみ対応しています。

- 「deny from」と「allow from」は認識します
- (ドメインではなく)IPで指定された値のみがインポート対象となります。
- CIDR notationを使用できますが、部分的なIPは使用できません。
- 各行は空白(又はカンマ)で分けられたIPアドレスが含まれます。例えば、「deny from 1.1.1.1 2.2.2.2/16」はOKで、「3.3.3.3, 4.4.4.4, 5.5.5.5」も使用できます。
- #から始まる行は無視されます。

削除
エントリを選択して、このボタンをクリックすると、一覧から削除されます。

デフォルトの処理

定義されていないリモートIPからの接続に関するデフォルトの処理を指定するには、IPアドレスを一覧から選択し、許可又は拒否をクリックします。デフォルト処理が指定された後でも、IPアドレスの"<default>"を選択し、新しいデフォルト設定を選択する事で設定変更が行えます。

許可
このオプションを選択すると、IPスクリーンで定義していないIPアドレスからの接続を許可します。

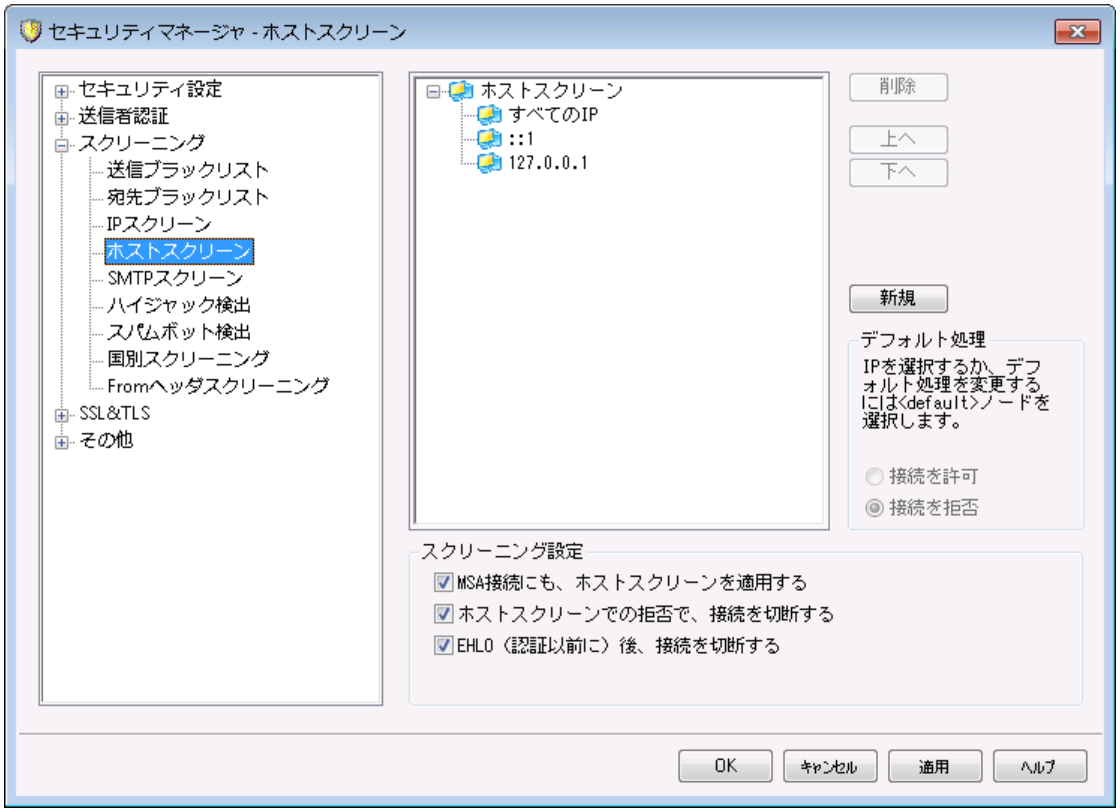
拒否
このオプションを選択すると、IPスクリーンで定義していないIPアドレスからの接続を拒否します。

IPスクリーニングでは信頼したIP[472]とローカルIPをブロックする事はありません。

スクリーニング設定

MSA接続にもIPスクリーンを適用する
サーバーのMSAポート[96]に対してもIPスクリーンを適用するにはこのオプションを使用します。通常これは必須ではありません。この設定はデフォルトで有効になっています。

4.1.3.4 ホストスクリーン



ホストスクリーン設定画面は、セキュリティ ≫ セキュリティ設定 ≫ スクリーニングから接続できます。ホストスクリーンは、ご使用になられているローカルIPアドレスに接続できるリモートホストを定義するのに使われます。この機能により、特定のホストからだけ接続を許可する、もしくは特定のホストからの接続を拒否するといった設定が可能になります。ホストスクリーンでは、SMTPセッション内で使用される EHLOとPTRでの値とここで指定したリスト内の値を比較します。

新規ホストスクリーンの登録

新しいホストスクリーンのエントリを作成するには、新規をクリックします。新規ホストスクリーンの登録ダイアログが起動し、新しいホストスクリーンを登録できます。

ローカルIP
ドロップダウンリストからホストスクリーンを適用するIPアドレスを選択します。「全てのIP」で全てのローカルIPへホストスクリーンを適用します。

リモートホスト（*と#のワイルドカードが使用できます。）
上のローカルIPと関連付けるリモートホストを入力します。

接続を許可
このオプションを選択すると指定したリモートIPアドレスが対応するローカルIPへ接続できるようになります。

接続を拒否
このオプションを選択することは、指定されたリモートIPアドレスが関連したローカルIPアドレスに接続許可しないことを意味します。

削除
エントリを選択して、このボタンをクリックすると、一覧から削除されます。

デフォルトの処理

定義されていないリモートIPからの接続に関するデフォルトの処理を指定するには、IPアドレスを一覧から選択し、許可又は拒否をクリックします。デフォルト処理が指定された後でも、IPアドレスの"<default>"を選択し、新しいデフォルト設定を選択する事で設定変更が行えます。

許可
このオプションを選択すると、ホストスクリーンで定義していないホストからの接続を許可します。

拒否
このオプションを選択すると、ホストスクリーンで定義していないホストからの接続を拒否します。

ホストスクリーンでは 信頼した[472]ホストやローカルホストからの接続を拒否する事はありません。

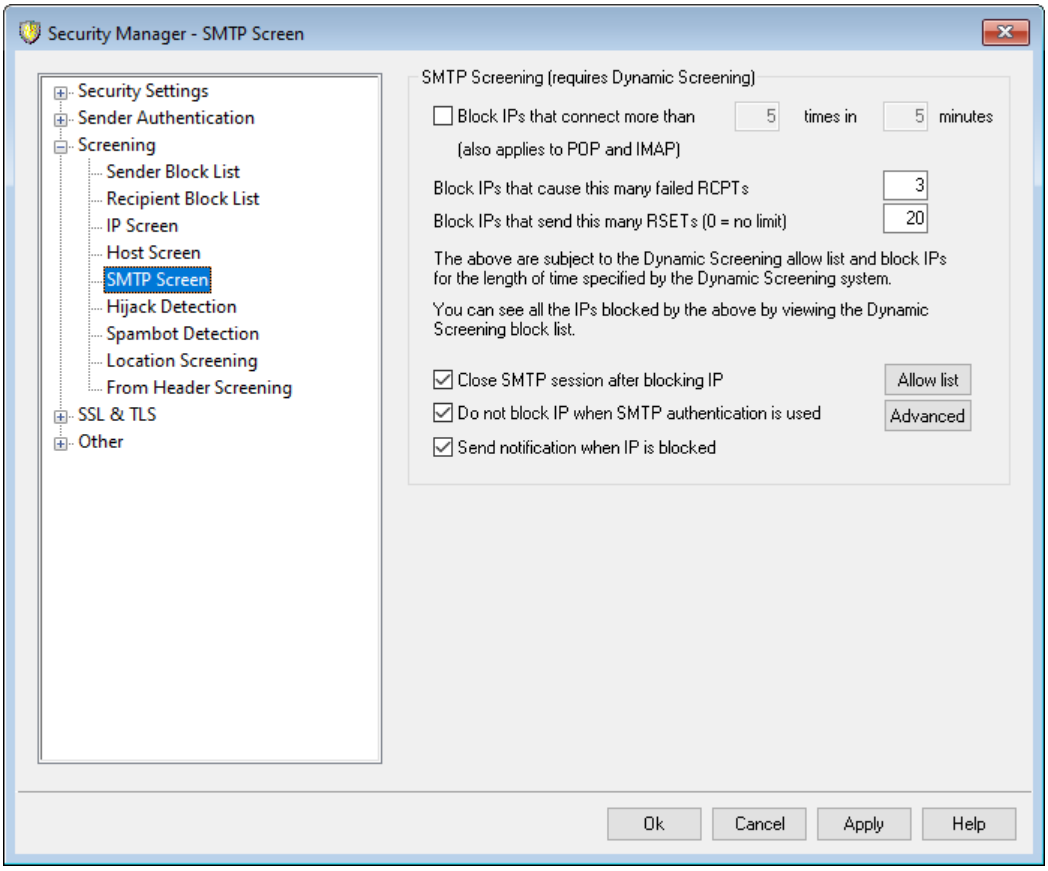
スクリーン設定

MSA接続にもホストスクリーンを適用する
サーバーのMSAポート[96]に対してもホストスクリーンを適用するにはこのオプションを使用します。この設定はデフォルトで有効になっています。

ホストスクリーンでの拒否で、接続を切断する
このオプションを有効にすると、ホストスクリーンで拒否されるとすぐに接続が切断されます。

EHLOの後（認証を待たずに)切断する
このオプションを有効にするとEHLO/HELOの直後に接続を切断します。通常は認証を待って切断します。この設定はデフォルトで有効になっています。

4.1.3.5 SMTPスクリーン



SMTPスクリーンを使うと、指定した分数の間で指定回数以上の認証失敗があったIPアドレスをブロックできるようになります。また、指定回数以上失敗したRCPTや、指定数以上のRSETコマンドの送信元もブロックできます。 SMTPスクリーンにはダイナミックスクリーニングが必要で、ダイナミックブロックリスト[571]とダイナミック許可リスト[569]を使用します。

指定回数以上の接続をするIPをブロックする [X] 回 [X] 分
限られた時間内に、指定回数以上サーバーへ接続したIPアドレスを一時的にブロックするにはこのオプションを有効にします。接続できる回数と時間（分）を指定します。アドレスは認証失敗トラッキング[559]で指定した時間ブロックされます。このオプションはPOPとIMAP接続へも適用できます。

RCPTコマンドが指定回数以上失敗したIPをブロックする
メールセッション内で指定回数の「宛先不明」エラーを発生させたIPアドレスを認証失敗トラッキング[559]で指定した時間ブロックするにはこのオプションを使用します。頻繁な「宛先不明」エラーは送信者がスパムメールを利用していないアドレスや誤ったアドレスへ一括送信しようとしている場合によく発生します。

指定数のRSETコマンドを発行したIPをブロックする (0 = 制限なし)
メールセッション内で指定回数のRSETコマンドを送ったIPアドレスをブロックするにはこのオプションを使用します。制限しない場合には「0」を指定します。サーバー設定のサーバー[82]にもこれと似たオプションがあり、RSETコマンドの最大数を指定できます。IPアドレスは認証失敗トラッキング[559]で指定した時間ブロックされます。

IPをブロックした後 SMTPセッションを閉じる
このオプションを有効にすると、IPをブロックした後MDaemonがSMTPセッションを閉じます。これはデフォルトで有効です。

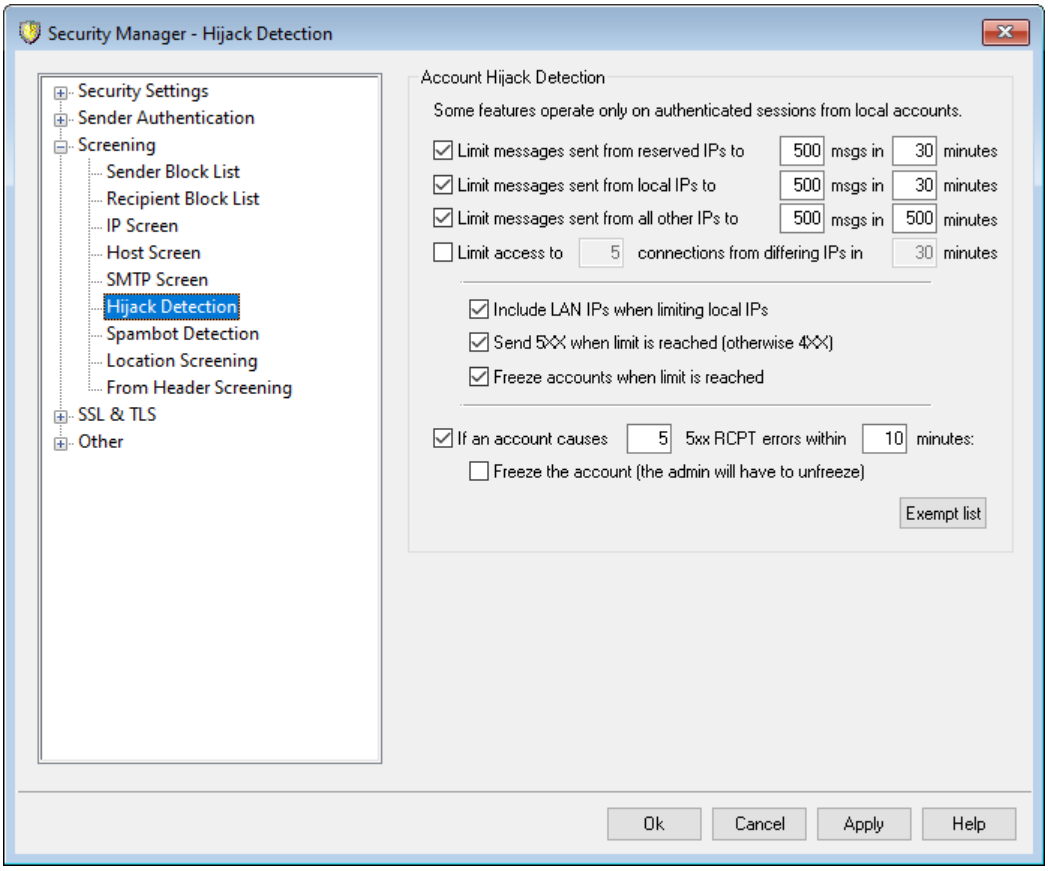
SMTP認証の使用時にはIPをブロックしない
認証したユーザーのセッションをダイナミックスクリーンから除外するにはこのオプションを有効にします。これはデフォルトで有効です。

IPがブロックされた際通知
デフォルトで、IPアドレスはダイナミックスクリーニングシステムで自動ブロックされ、ダイナミックスクリーニングの *IP アドレスブロックレポート* 564 オプションを使うと対象のアクションを通知することができます。IPアドレスがSMTPスクリーニング機能でブロックされた場合も通知を受け取らないようにするには、このオプションをクリアしてください。

許可リスト
クリックするとダイナミック許可リスト 569 が起動します。ここへ記載されたIPアドレスはSMTPスクリーンから除外されます。

詳細
クリックするとダイナミックスクリーニング 556 ダイアログが起動します。

4.1.3.6 ハイジャック検出



アカウント ハイジャック検 出

この画 面 では、MDaemonアカウント でハイジャックされた可 能 性 のあるアカウント を検 出し、自 動 でメー ル送 信 を防 止 する機 能 を有 効 化 できます。例 えば、何 らかの方 法 でスパム送 信 者 がアカウント のメール アドレスとパスワードを入 手 した場 合 、この機 能 を使 う事 でスパム送 信 者 が対 象 アカウント を使 って MDaemonサーバーからメール送 信 するのを防 ぐことができます。接 続 しているIPアドレスを元 に、1分 間 で 送 信 できる最 大 メール数 を指 定 する事 ができ、この制 限 に到 達 したアカウント を無 効 化 する事 もできま す。ここでは除 外 リスト を使 用 する事 もでき、こうした制 限 から除 外 することもできます。アカウント のハイ ジャック検 出 はデフォルト で有 効 です。

アカウント のハイジャック検 出 は認 証 済 セッションのローカルアカウント に対 してのみ適 用 され、Postmasterは自 動 で除 外 されます。

予 約 されたIPからの最 大 メッセージ送 信 の上 限 [xx]通 [xx]分
予 約 されたIPから接 続 したMDaemonアカウント が、指 定 した分 数 の間 で最 大 何 通 のメールを送 信 できるか、このオプションで指 定 します。予 約 されたIPアドレスはRFCで定 義 されています。(例 : 127.0.0.*, 192.168.*.*, 10.*.*.*, 172.16.0.0/12, ::1, FD00::/8, FEC0::/10, and FE80::/64)

ローカルIPからの最大メッセージ送信の上限 [xx] 通 [xx]分
ローカルIPから接続したMDaemonアカウントが、指定した分数の間で最大何通のメールを送信できるか、このオプションで指定します。ローカルIPとはMDaemonドメイン用に設定された全てのIPアドレスを意味します。

その他のIPからの最大メッセージ送信の上限 [xx] 通 [xx]分
その他IPから接続したMDaemonアカウントが、指定した分数の間で最大何通のメールを送信できるか、このオプションで指定します。

異なるIPからの最大接続数 [xx] 回 [xx] 分
異なるIPアドレスからの接続回数を、指定した時間内に最大何回とするか、制限するにはこのオプションを使用します。例えば、通常、アカウントが様々な異なるIPアドレスから短時間で接続した場合、対象アカウントはハイジャックされている可能性が高いものとみなします。このオプションはデフォルトで無効になっています。

ローカルIPの制限時LAN IPを含む
ローカルIPからの最大メッセージ送信の上限を使用している時、デフォルトでLAN IP[554]が含まれます。ローカルIPを制限するのにLAN IPを含めたくない場合はこのオプションを無効化して下さい。

最大値に到達した際5XXを送信する(又は4XX)
デフォルトで、最大値に到達するとMDaemonはハイジャックされたアカウント用に5XXの応答を返します。このオプションを無効化すると、5XXではなく4XXの応答を返します。

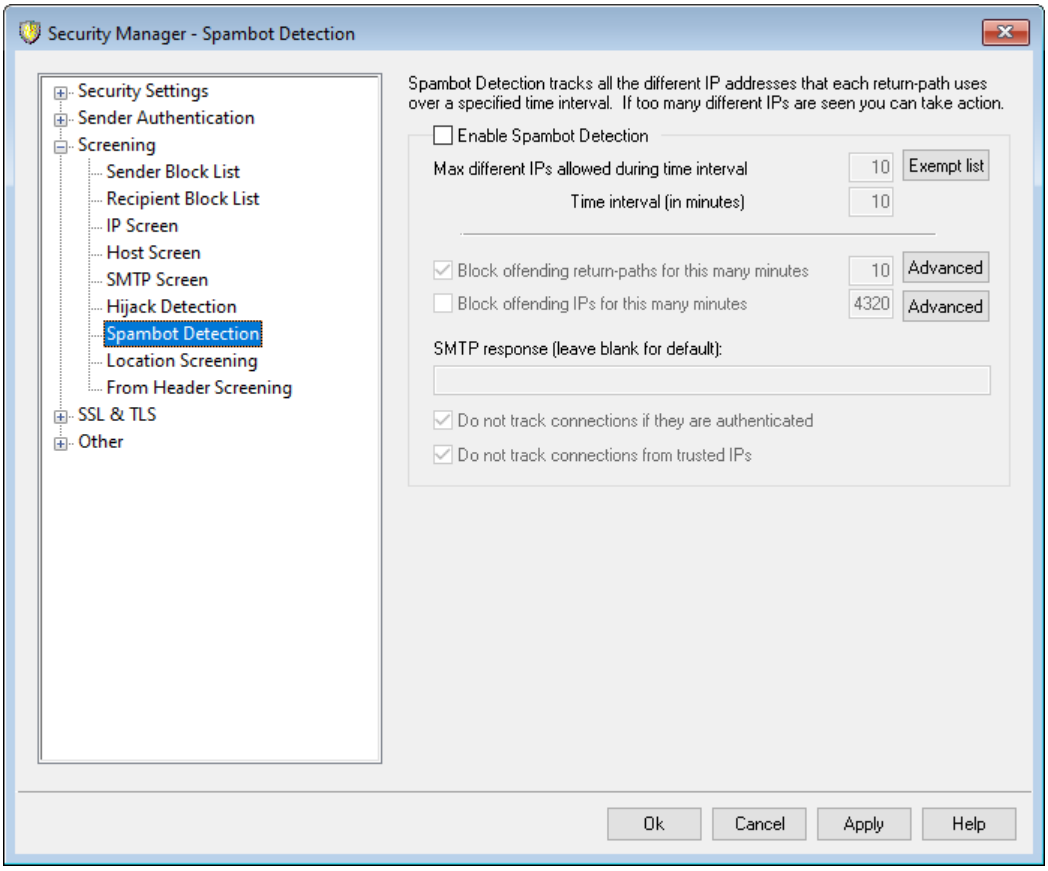
指定回数に到達したアカウントを凍結
最大値として指定した数を超えるメッセージを送信したアカウントを無効にするにはこのボックスをチェックします。この場合は、サーバーは552エラーを返し、接続が閉じられ、アカウントはすぐに無効化されます。このアカウントはその後メール送信や受信確認を行えなくなりますが、メール受信だけは受け付けます。最後に、アカウントが無効化された時には、postmasterへその旨のメールが送られ、そのメールへ返信するとアカウントは再度有効化されます。

アカウントが次の回数 [xx] 5xx RCPTエラー [xx] 分
このオプションはアカウントが不明な宛先に指定間隔の中で何回メール配信を試みたかを監視します。スパムメールの一般的な特徴として、不正な宛先に短時間で大量のメールを送信しようとする、というものがあります。これはスパム送信者が古いメールアドレスや考えられる新しいメールアドレスの全てに対しメール配信を試みるためです。このため、MDaemonアカウントが不正な宛先へ大量のメールを送信した場合、アカウントがスパム送信のためにハイジャックされている可能性があります。下記の「アカウントを凍結…」とこのオプションを使用する事で、ハイジャックされたアカウントによる大きなダメージを防ぐ事ができます。注意点:このオプションでは、メール配信時にRCPTコマンドで5xxエラーコードが返された宛先を不正な宛先とみなします。

アカウントを凍結(管理者による凍結解除が必要)
"*アカウントが次の回数 [xx] 5xx ...*"の閾値に到達した際、アカウントを凍結するにはこのオプションを使用します。この場合、管理者へメール通知が行われ、管理者がアカウントの凍結解除を行う事ができます。

除外リスト
ハイジャックされたアカウントの検出から特定のアドレスを除外する場合は除外リストを使用します。ワイルドカードが使用できます。例えば"newsletters@example.com"はexample.comドメインのnewslettersアカウントを除外し、"*@newsletters.example.com"は、newsletters.example.comドメインの中の全てのアカウントを除外します。Postmasterアカウントは自動的にハイジャックされたアカウントの検出から除外されます。

4.1.3.7 スパムボット検出



スパムボット検出は、一定期間の間に使われた、全てのSMTP MAIL (return-path)の値を記録する機能です。短時間の間に複数のIPアドレス(端末の切り替えで複数になる事はあります)で同じreturn-pathを使っていた場合、スパムボットネットワークである場合があります。スパムボットが検出されると、その時点での接続はすぐに遮断され、必要に応じてreturn-pathの値を指定した時間ブロックリストとして登録する事もできます。また、ユーザーが定義した期間、全てのスパムボットIPをブロックリストへ登録する事もできます。

スパムボット検出を有効にする
このオプションをクリックしスパムボット検出を有効化します。これはデフォルトで無効に設定されています。

この時間内に許可する異なるIPアドレスの最大数
指定した時間内に1つのreturn-pathが使用可能な異なるIPアドレス数を指定します。

時間間隔（分）
スパムボットネットワークを検出する際に使用する時間間隔（分）を指定します。

除外リスト
このボタンをクリックすると、スパムボット検出の除外リスト画面が起動します。ここではスパムボット検出から除外するIPアドレス、送信者、宛先を指定できます。

この時間内（分）はブロックリスト登録されたreturn-pathを拒否します
スパムボットとして検出されたreturn-pathをブロックリスト登録するにはこのオプションを使用します。MDaemonは指定した時間（分）はブロックリスト登録されたreturn-pathからのメールを受け付けません。このオプションはデフォルトで有効です。

詳細
このボタンをクリックすると、スパムボット送信者のファイルが起動します。ここへは現在ブロックリストへ登録されたreturn-pathとブロックリストから削除されるまでの時間（分）が表示されます。

この時間内（分）はブロックリスト登録されたIPを拒否します
スパムボットとして検出されたIPをブロックリスト登録するにはこのオプションを使用します。MDaemonは指定した時間（分）はブロックリスト登録されたIPからのメールを受け付けません。このオプションはデフォルトで無効になっています。

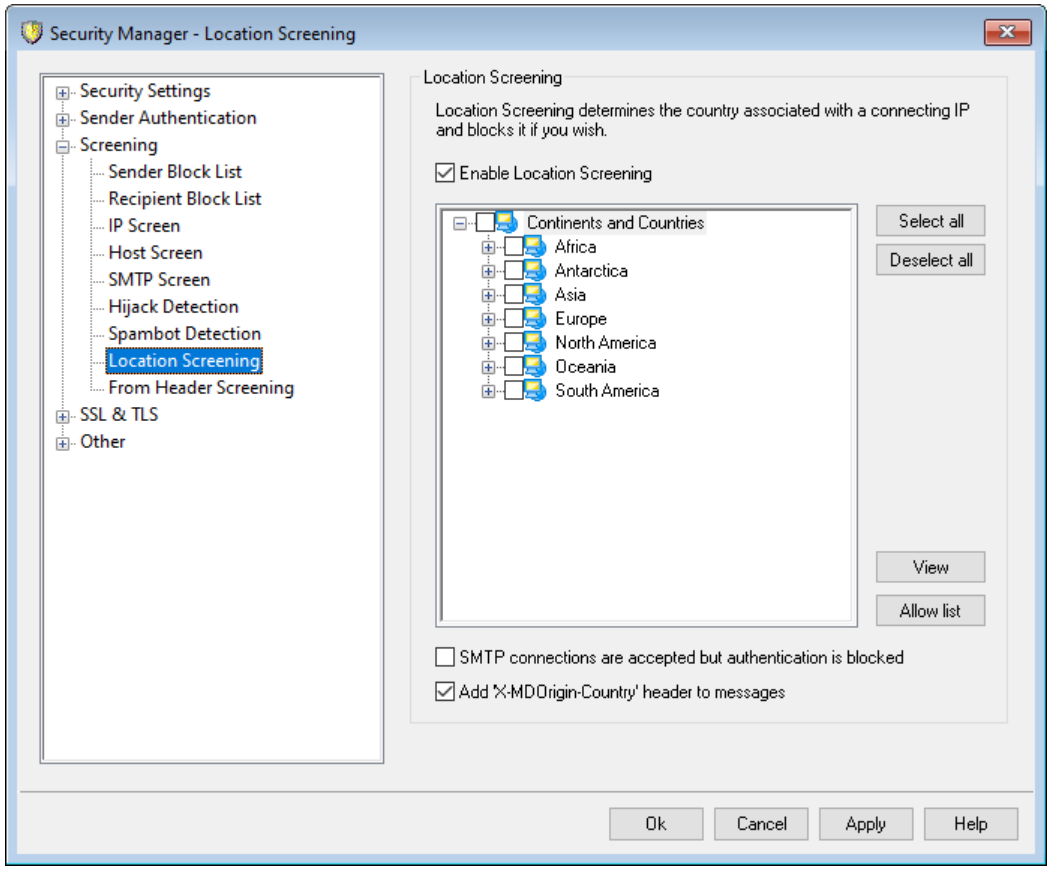
詳細
このボタンをクリックすると、スパムボットIPのファイルが起動します。ここへは現在ブロックリストへ登録されたIPとブロックリストから削除されるまでの時間（分）が表示されます。

SMTP応答（デフォルトはブランク）
ここではブロックリスト登録されたreturn-pathやIPアドレスからのスパムボットに対して返すSMTPレスポンスコードをカスタマイズできます。MDaemonはSMTPレスポンスとして、デフォルトのものではなく「551 5.5.1 <your custom text>」を返します。MDaemonのデフォルト値を使用する場合はこの欄を空白のままにして下さい。

認証済の接続は記録しない
デフォルトでMDaemonは認証済[476]セッションからの接続をスパムボット検出へは記録しません。認証済接続を除外しない場合は、このオプションを無効にして下さい。

信頼するIPからの接続は記録しない
デフォルトでスパムボット検出は信頼するIP[473]アドレスからの接続を記録しません。信頼するIPを除外しない場合は、このオプションを無効にして下さい。

4.1.3.8 国別スクリーニング



国別スクリーニング

国別スクリーニングは、場所を元にブロックするシステムで、SMTP, POP, IMAP、Webmail, ActiveSync, 自動検出 68, XML API, Remote Administration, CalDAV/CardDAV, XMPP, Minger接続で使用できます。MDaemonは接続元IPアドレスが属する国を判別し、制限対象の国からの接続だった場合はこれをブロックし、Screeningログへ記録します。SMTPについては、国別スクリーニングでAUTHの接続のみをブロックする事もできます。これは、例えばユーザーは特定の国にいるわけではないもの、その場所からメールの送受信を行いたいユーザーがいる場合などに便利です。これを使った場合、サーバーへログインしようとした接続のみをブロックできます。

\MDaemon\Geo\ フォルダには、IPと所属する国に関するマスターデータベースが格納されています。このファイルはMaxMind（www.maxmind.com）が提供しているものであり、必要に応じてそちらのサイトから最新版をダウンロードできます。

国別スクリーニングの有効化

国別スクリーニングはデフォルトで有効ですが、地域や国はブロックする対象として設定されていません。MDaemonは接続元の国や地域をブロックはせず、ログへの記録のみ行います。 国別スクリーニングを使用する場合は、ブロック対象の地域や国にチェックを入れ、OK又は適用をクリックします。国別スクリーニングが有効な時、ブロックされているかどうかに寄らず、MDaemonはメールへ "X-

MDOrigin-Country" ヘッダを付与し、このヘッダはコンテンツフィルタや他の目的で使用されます。このヘッダには2文字のISO 3166 の国及び地域コードが実際の国名の代わりに含まれています。

全てを選択/選択解除
一覧を全て選択したり選択解除する場合はこのボタンを使用します。

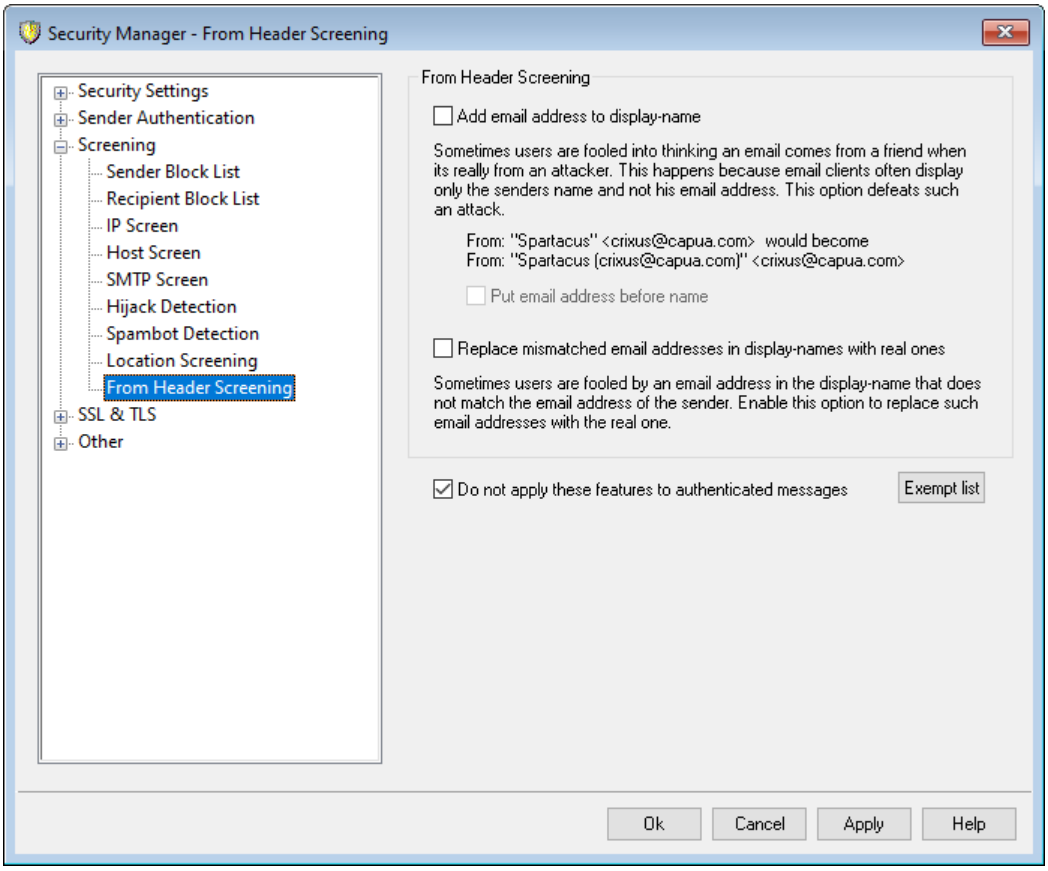
表示
このボタンをクリックすると、現在国別スクリーニングでブロックしている全ての場所が一覧表示されます。一覧でボックスの選択や選択解除を行ったら、適用ボタンをクリックするまで表示ボタンは使用できません。

許可リスト
このボタンをクリックすると国別スクリーニングでも使用している ダイナミックスクリーニング許可リスト 569 が起動します。国別スクリーニングから除外したIPアドレスがある場合は、このボタンをクリックし、IPアドレスと期限を指定してください。

SMTP接続は受けつけましたが認証はブロックしました
このオプションを有効化すると、SMTP接続のうち、認証用の接続のみがブロックされます。

メールへ'X-MDOrigin-Country'ヘッダを付与
デフォルトで、国別スクリーニングが有効な場合、MDaemonはメールへ "X-MDOrigin-Country" ヘッダを付与し、このヘッダはコンテンツフィルタや他の目的で使用されます。このヘッダには2文字のISO 3166 の国及び地域コードが実際の国名の代わりに含まれています。このヘッダをメールへ追加しない場合はオプションを無効にして下さい。

4.1.3.9 Fromヘッダスクリーニング



From ヘッダスクリーニング

このセキュリティ機能を使うと、受信メールの「From:」ヘッダの名前の部分に、名前とメールアドレス両方を含むようになります。この機能はFromヘッダを偽装した攻撃を防ぐための機能で、Fromヘッダの偽装は、メールクライアントの多くが、メールアドレスを表示せず名前だけを表示している事が起因しています。メールアドレスを確認するには、メールを開いた上で対象アドレスを右クリックする、といった操作が必要になります。そのため、攻撃者は、目に入る部分のみに、会社名などを入力しておきます。例えば、メールの実際のFromヘッダが「Honest Bank and Trust" <lightfingers.klepto@example.com>」だったとしても、クライアントでは「Honest Bank and Trust」のみが表示されます。Fromヘッダの変更機能は、送信者のヘッダを"Honest Bank and Trust (lightfingers.klepto@example.com)" <lightfingers.klepto@example.com>という表示へ変更し、送信元を判断しやすくします。

表示名へメールアドレスを追加
クライアント側で表示される「From:」ヘッダの値に、名前とメールアドレスの両方が含まれるようにするには、このオプションを有効化して下さい。新しいヘッダは、従来の"送信者名" <mailbox@example.com>という形式を、"送信者名 (mailbox@example.com)" <mailbox@example.com>"の形式へ書き換えます。この機能はローカルユーザー宛のメールに対してのみ適用され、デフォルトで無効に設定されています。ユーザーによっては、例え偽装であっても、From: ヘッダの書き換えを望まない場合もあるため、このオプションの有効化は慎重に行って下さい。

名前の前にメールアドレスを付ける
表示名へメールアドレスを追加、のオプションを使用していて、Fromヘッダでメールアドレスを最初に挿入する場合はこのオプションを有効にしてください。上記の例の場合、"送信者名" <mailbox@example.com> という形式は次のように書き換えられます。:
"mailbox@example.com(送信者名)" <mailbox@example.com>

表示名の中のメールアドレスが異なっていた場合実際のメールアドレスへ置き換える
スパムで使用されるもう一つの手法は、From: ヘッダの表示名とメールアドレスを実際に使っているものとは別のものへ書き換えるというものです。このオプションを使用すると、表示されているメールアドレスが実際のものと異なる場合、表示されているアドレスを実際のアドレスに書き換える事ができます。

認証済メールにこの機能を使用しない
Fromヘッダスクリーニングオプションを、MDaemonで認証済の受信メールへは適用しない場合には、このオプションを有効にしてください。

除外リスト
Fromヘッダスクリーニングの除外リストへアドレスを追加するにはこのオプションを使用します。リストのアドレスへのメールについては、From: ヘッダの書き換えを行いません。

4.1.4 SSL & TLS

MDaemonは、SMTP, POP, IMAP[525]、及びMDaemon Remote Administration[532]やWebmail[528]ウェブサーバーで使用する、SSL(Secure Socket Layer)プロトコルとTLS(Transport Layer Security)プロトコルに対応しています。ネットスケープコミュニケーション社によって開発されたSSLプロトコルは、サーバとクライアント間のインターネット接続を安全に行うための標準プロトコルです。SSLは、サーバ認証、データ暗号化、TCP/IP接続用のクライアント認証などを提供します。さらに、SSLはメジャーなブラウザ全てに組み込まれているので、有効なデジタル証明書をサーバにインストールするだけで、MDRAやWebmailへの接続でSSL機能を利用する事ができるようになります。

Webmailではなくメーラーで標準のメールポートに接続している場合、MDaemonはSMTPとIMAPに対してはTLSのSTARTTLS拡張機能を、POP3に対してはSTLS拡張機能をサポートしています。しかし、すべてのメールクライアントがこの機能をサポートしているわけではないので、最初にクライアントがこれらのSSLを使用できるよう設定しなければなりません。STARTTLSホワイトリスト[536]とSTARTTLSリスト[537]ページにて、STARTTLSを使用しない、または必須とするホストやアドレスを指定できます。

SSL & TLSダイアログには、DNSSEC[540](DNSセキュリティ拡張)を有効にするページや、RequireTLS, MTA-STA, TLS Reportingを有効にするSMTP拡張[538]ページ、Let's Encrypt Certificate Authority(CA)を使用するためのLet's Encrypt[541]ページも含まれています。

SSLは、セキュリティ ≫ セキュリティマネージャ » SSL & TLS ダイアログのSSL&TLSセクションから有効化や設定が行えます。SMTP、POP3およびIMAP用のSSLポート設定は、設定 ≫ サーバ設定 ≫ DNS &

IPのポート 96 画面から行えます。 Webmail 528 や Remote Administration 532 からも同様にSSL設定が行えます。

SSL証明書の作成や利用に関する詳細は、以下を参照して下さい:

SSL証明書の作成と利用 830

—

RFC-4346で定義されている、TLS/SSLプロトコルに関してはこちらを参照してください: The Transport Layer Security (TLS) Protocol Version 1.1

RFC-3207で定義されている、SMTPにおけるSTARTTLS拡張に関してはこちらを参照してください: SMTP Service Extension for Secure SMTP over Transport Layer Security

RFC-2595で定義されている、IMAPおよびPOP3におけるTLSの使用に関してはこちらを参照してください: Using TLS with IMAP, POP3 and ACAP

DNSSEC (DNS Security Extensions) はこちらで定義されています: RFC-4033: DNS Security Introduction and Requirements and RFC-4035: Protocol Modifications for the DNS Security Extensions as

RequireTLSの定義の全文はこちらをご覧下さい: RFC 8689: SMTP Require TLS Option.

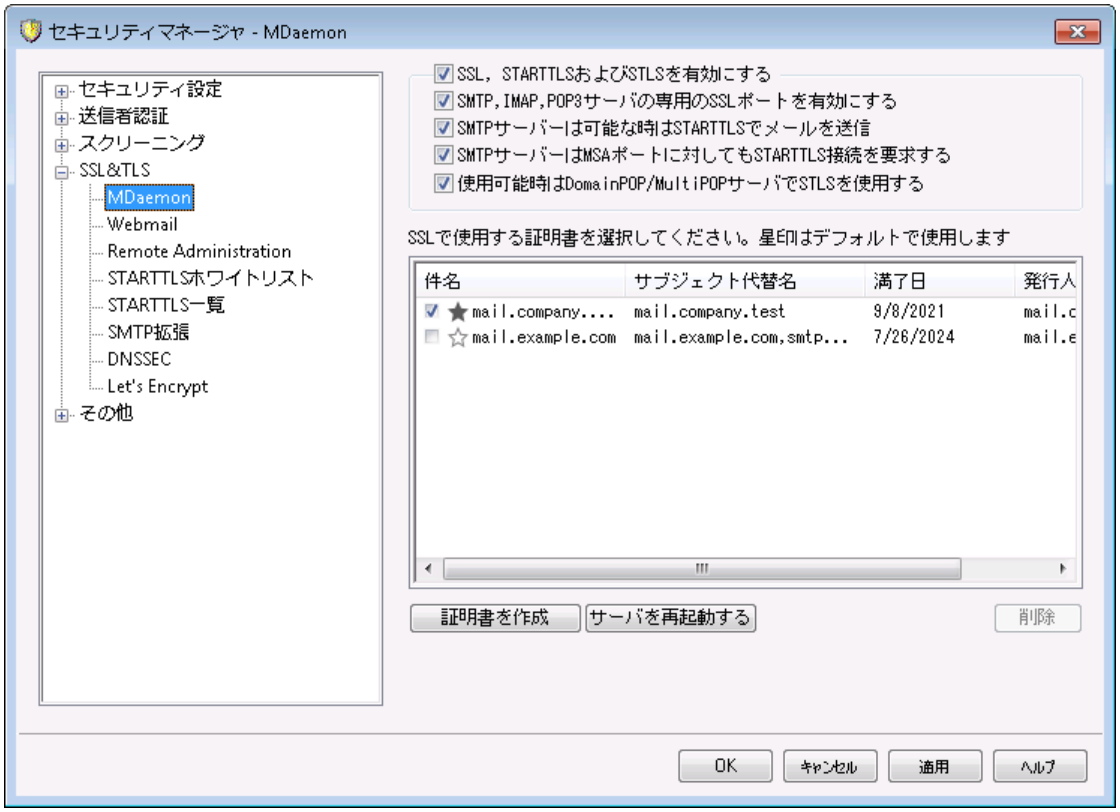
MTA-STS対応はこちらで定義されています: RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

TLS Reportingはこちらで定義されています RFC 8460: SMTP TLS Reporting.

参照:

SSL & TLS » MDaemon 525
SSL & TLS » Webmail 528
SSL & TLS » Remote Administration 532

4.1.4.1 MDaemon



SSL, STARTTLSおよびSTLSを有効にする
SSL/TLSプロトコルおよびSTARTTLSとSTLS拡張のサポートを開始するには、このオプションを選択し、以下の一覧から使用する証明書を選択してください。

SMTP, IMAP, POP3サーバの専用SSLポートを有効にする
サーバ設定のポート 96 で指定した専用SSLポートを有効にする場合は、このオプションを選択してください。これはデフォルトのメールポートでSTARTTLSおよびSTLSを使用しているクライアントには影響せずに、単にSSLサポートへの補足レベルを提供するだけです。

SMTPサーバーは使用可能な時はSTARTTLSを使用する
MDaemonが送信するすべてのSMTPメッセージにSTARTTLS拡張を使用する必要がある場合、このオプションを選択してください。MDaemonが接続しているサーバがSTARTTLSをサポートしない場合、メッセージはSSLを使用することなく通常配信されます。特定のドメインに対してSTARTTLSから除外する場合には、このセクションにある STARTTLS非使用リスト 536 を使用します。

SMTPサーバーはMSAポートにおいてもSTARTTLSを要求する
MSAポート 96 に対する接続に対してもSTARTTLSを要求するにはこのオプションを有効にして下さい。

使用可能時はDomainPOP/MultiPOPサーバでSTLSを使用する
使用可能な場合はいつでもDomainPOPおよびMultiPOPサーバでSTLS拡張を使用するにはこのチェックボックスを選択します。

HTTPS/SSL用の証明書を選択

このボックスにはSSL証明書が表示されます。アクティブにする証明書の隣のボックスをチェックします。デフォルト証明書として使用する証明書は、隣に表示されている星マークをクリックします。MDaemonはTLSプロトコルのServer Name Indication（SNI）拡張に対応しており、サーバーのホスト名毎に異なる証明書を使用する事ができます。MDaemonはアクティブな証明書から要求されたホスト名がSubject Alternative Namesフィールドへ含まれているものを選択します。クライアントがホスト名を要求していなかったり、マッチする証明書が存在しなかった場合は、代わりにデフォルトの証明書が使用されます。ダブルクリックすると証明書ダイアログが起動し、証明書のレビューをここから行う事ができます。（この操作はブラウザベースのRemote administrationからではなく、アプリケーションから行う必要があります。）

削除

リストから証明書を選択してこのボタンをクリックすると、その証明書が削除されます。実際に削除される前に確認ダイアログがポップアップされます。

証明書の作成

このボタンをクリックしSSL証明書の作成ダイアログが起動します。

証明書詳細

ホスト名

証明書作成時、ユーザーが接続する際のホスト名を入力します。（例: wc.example.com）。

組織/会社名

証明書を所有する組織名や会社名を入力します。

ホスト名の別名（カンマで複数設定）

接続する際に使用するドメインが複数あり、証明書をそれぞれのホストへ適用する場合は、ドメイン名をカンマで区切って指定します。ワイルドカードが使用でき、「*.example.com」はexample.comのサブドメイン（例えばwc.example.com、mail.example.comなど）すべてに対して適用されます。

MDaemonはTLSプロトコルのServer Name Indication（SNI）拡張に対応しており、サーバーのホスト名毎に異なる証明書を使用する事ができます。MDaemonはアクティブな証明書から要求されたホスト名がSubject Alternative Namesフィールドへ含まれているものを選択します。クライアントがホスト名を要求していなかったり、マッチする証明書が存在しなかった場合は、代わりにデフォルトの証明書が使用されます。

暗号キーの長さ
この証明書で使用する暗号化キーのビットの長さを選択します。長い暗号化キーを使うとより安全な通信が行えますが、全てのアプリケーションで512を超える長さのキーに対応しているわけではありあせん。

国
サーバーが設置している国や地域を選択します。

ハッシュアルゴリズム
使用するハッシュアルゴリズムを、SHA1又はSHA2の中から選択します。デフォルト設定はSHA2です。

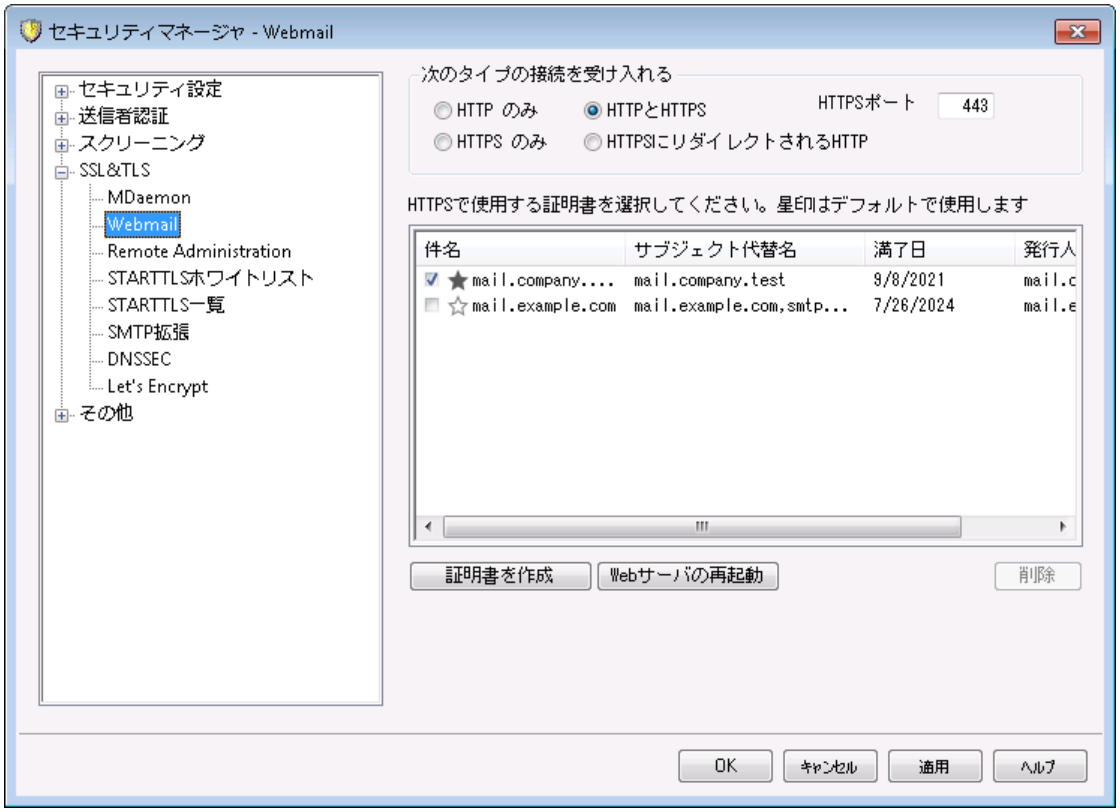
サーバーの再起動

SMTP/IMAP/POPサーバーを再起動する際にクリックします。証明書を変更した際にはサーバーの再起動が必要です。

参照:

SSL & TLS 523
SSL証明書の作成と利用 830

4.1.4.2 Webmail



MDaemonに搭載されているウェブサーバーはSecure Sockets Layer (SSL)プロトコルに対応しています。SSLとは、サーバー/クライアント間のウェブコミュニケーションを安全に行うための標準規格であり、サーバー認証、データ暗号化、TCP/IP接続用に追加のクライアント認証などの機能を提供しています。ほとんどのブラウザでは(HTTP over SSLのような)HTTPSに対応しているため、サーバー側に正しい証明書をインストールするだけで、クライアントはSSL機能を利用できるようになります。

Webmailでは、設定 ≫ Web & IM サービス ≫ Webmail の中のSSL & HTTPS 画面へアクセスして下さい。利便性向上のため、この設定項目は、セキュリティ ≫ セキュリティ設定 ≫ SSL & TLS » Webmail からも使用できます。

SSLプロトコルと証明書についての詳細は、次のページを参照して下さい: SSL & 証明書 523

> MDaemonの内蔵ウェブサーバーを使用している場合、ここでの設定はWebmailにのみ適用されます。WebmailがIISなどの他のウェブサーバーを使用していた場合このオプションは使用できません。SSL/HTTPSは他のウェブサーバーで提供されているツールを使って設定を行う必要があります。

次の接続タイプを許可

HTTPのみ
Webmailへの接続にHTTPSの利用を許可しない場合はこのオプションを選択します。HTTP接続のみが使用できるようになります。

HTTPとHTTPS
WebmailでSSL対応は有効にするものの、ユーザーにHTTPSの利用を強制しない場合には、このオプションを選択します。Webmailは指定されたHTTPSポートでのみ接続を受け付けますが、WebmailのWebサーバー[295]で指定したWebmail用TCPポートへのhttp接続に対しても応答を行います。

HTTPSのみ
WebmailでHTTPS接続だけに応答するにはこのオプションを選択します。このオプションが有効の場合、WebmailはHTTPS接続のみ応答し、HTTPリクエストに対しては応答しません。

HTTPをHTTPSへリダイレクトする
全てのHTTP接続をHTTPSポートへリダイレクトするには、このオプションを使用します。

HTTPSポート
SSL通信でWebmailが使用するTCPポートを指定します。デフォルトのSSLポートは443番です。デフォルトのSSLポートを使う場合は、WebmailのURLに、ポート番号を含む必要はありません。(例えば、"https://example.com" は "https://example.com:443"と同じURLを示します)

> このポートはWebmailのWebサーバー[295]で指定したWebmailポートとは異なります。WebmailでHTTP接続を許可するのであれば、Webmailでは正しく接続できるよう異なるポートを使用する必要があります。HTTPS接続はHTTPSポートを使用する必要があります。

HTTPS/SSL用証明書の選択

ここにはお使いのSSL証明書が表示されます。Webmailで使用する証明書をクリックして選択します。デフォルトとして使用したい証明書の隣にある星印をクリックします。 MDaemonはTLSプロトコルの拡張であるServer Name Indication (SNI)に対応しており、サーバーのホスト名毎に、異なる証明書を使用する事ができます。MDaemonはアクティブな証明書を確認し、Subject Althernative Namesフィールドから、要求されたホスト名を選択します。(証明書の生成時、別名を指定する事もできます。)クライアントがホスト名を要求していなかった場合や、対象の証明書が存在していなかった場合、デフォルトの証明書が使用されます。Windowsの証明書ダイアログを起動し、証明書のレビューを行うには、対象の証明書をダブルクリックしてください。(これはブラウザベースのリモート管理画面ではなく、アプリケーション画面からのみ利用できます。)

削除
一覧から証明書を選択し削除をクリックします。確認画面で証明書を削除するかどうかを質問されます。

証明書の作成
このボタンをクリックしSSL証明書の作成ダイアログを起動します。

証明書詳細

ホスト名
証明書作成時、ユーザーが接続する際のホスト名を入力します。（例: wc.example.com）。

組織/会社名
証明書を所有する組織名や会社名を入力します。

ホスト名の別名（カンマで複数設定）
ユーザーが接続する際などに使用するWebmailの別ホスト名がある場合は、カンマで区切ったドメイン名をここへ入力します。ワイルドカードにも対応しており、例えば"*.example.com"は(例えば "wc.example.com", "mail.example.com"といった)example.comのサブドメインに対しても適用できます。

> MDaemonはTLSプロトコルの拡張であるServer Name Indication (SNI)に対応しており、サーバーのホスト名毎に、異なる証明書を使用する事ができます。MDaemonはアクティブな証明書を確認し、Subject Althernative Namesフィールドから、要求されたホスト名を選択します。クライアントがホスト名を要求していなかった場合や、対象の証明書が存在していなかった場合、デフォルトの証明書が使用されます。

暗号キーの長さ
この証明書で使用する暗号化キーのビットの長さを選択します。長い暗号化キーを使うとより安全な通信が行えますが、全てのアプリケーションで512を超える長さのキーに対応しているわけではありあせん。

国
サーバーが設置している国や地域を選択します。

ハッシュアルゴリズム
使用するハッシュアルゴリズムをSHA1かSHA2から選択します。デフォルトはSHA2です。

webサーバーの再起動

ボタンをクリックしウェブサーバーを再起動します。新しい証明書を使用するにはウェブサーバーの再起動が必要です。

証明書の管理にLet's Encryptを使用する

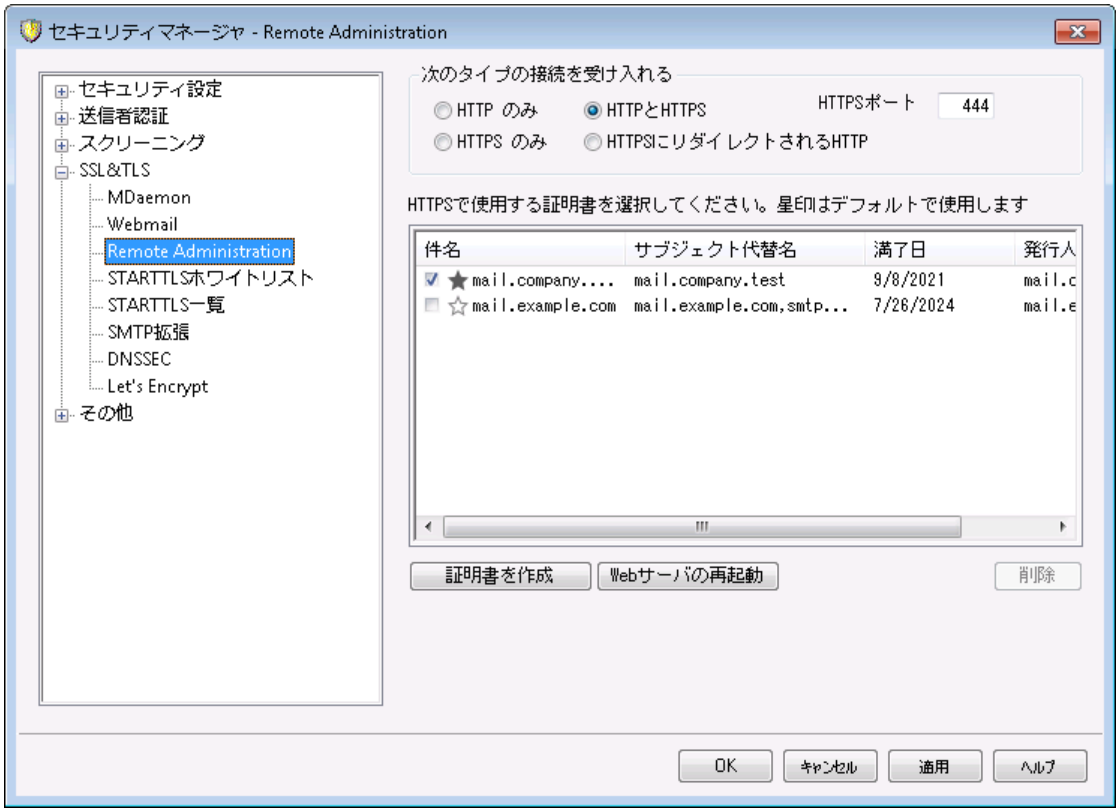
Let's Encryptとは、セキュアなウェブサイト向けに、従来手動で行っていた証明書の生成、検証、署名、インストール、更新といった複雑な処理を自動化し、無償の証明書を発行している認証局（CA）です。

Let's Encryptの自動処理で証明書を管理するのに、Let's Encrypt[541]画面にてMDaemon¥LetsEncryptフォルダに格納されたPower Shellスクリプトを簡単に実行するためのオプションを用意しています。スクリプトを実行するとLet's Encrypt用に、Webmail HTTPフォルダへhttp-01チャレンジに必要なファイルの配置を含む、全ての設定が行われます。ここでは、証明書用のドメインとしてデフォルトドメイン[165]のSMTPホスト名[167]が関連するホスト名と併せて使用され、証明書の取得と受信、Windowsへのインポート、MDaemon, Webmail, Remote Administrationでこれらの証明書を使用するためのMDaemon設定が行われます。更に、スクリプトはMDaemon¥Logs¥フォルダへLetsEncrypt.logというログも生成します。このログはスクリプト実行の度に削除され再生成され、スクリプトの開始時間が記録されます。通知用の管理者アドレスへは、エラー発生時にはメールでの通知も行われます。詳細についてはLet's Encrypt[541]を参照してください。

参照:

SSL & 証明書[523]
SSL証明書の作成と使用[830]

4.1.4.3 Remote Administration



MDaemonに搭載されているウェブサーバーはSecure Sockets Layer (SSL)プロトコルに対応しています。SSLとは、サーバー/クライアント間のウェブコミュニケーションを安全に行うための標準規格であり、サーバー認証、データ暗号化、TCP/IP接続用に追加のクライアント認証などの機能を提供しています。ほとんどのブラウザでは(HTTP over SSLのような)HTTPSに対応しているため、サーバー側に正しい証明書をインストールするだけで、クライアントはSSL機能を利用できるようになります。

Remote Administration でSSLを使用するには、設定 ≫ Web & IM サービス ≫ Remote Administrationの中のSSL & HTTPS画面へアクセスして下さい。利便性向上のため、この設定項目は、セキュリティ ≫ セキュリティ設定 ≫ SSL & TLS ≫ Remote Administration からも使用できます。

SSLプロトコルと証明書についての詳細は、次のページを参照して下さい: SSL & 証明書 523

この画面の設定は、Remote AdministrationがMDaemonの内蔵ウェブサーバーを使用している場合のみ適用されます。Remote AdministrationがIISなどの他のウェブサーバーを使用していた場合このオプションは使用できません。SSL/HTTPSは他のウェブサーバーで提供されているツールを使って設定を行う必要があります。

次の接続タイプを許可

HTTPのみ
Remote Administrationへの接続にHTTPSの利用を許可しない場合はこのオプションを選択します。HTTP接続のみが使用できるようになります。

HTTPとHTTPS
Remote AdministrationでSSL対応は有効にするものの、ユーザーにHTTPSの利用を強制しない場合には、このオプションを選択します。Remote Administrationは指定されたHTTPSポートでのみ接続を受け付けますが、Web Server 322で指定したRemote Administration用TCPポートへのhttp接続に対しても応答を行います。

HTTPSのみ
Remote AdministrationでHTTPS接続だけに応答するにはこのオプションを選択します。このオプションが有効の場合、Remote AdministrationはHTTPS接続のみ応答し、HTTPリクエストに対しては応答しません。

HTTPをHTTPSへリダイレクトする
全てのHTTP接続をHTTPSポートへリダイレクトするには、このオプションを使用します。

HTTPSポート
SSL通信でRemote Administrationが使用するTCPポートを指定します。デフォルトのSSLポートは444番です。デフォルトのSSLポートを使う場合は、Remote AdministrationのURLに、ポート番号を含む必要はありません。(例えば、"https://example.com" は "https://example.com:444"と同じURLを示します)

このポートはWeb Server 322で指定したRemote Administrationポートとは異なります。Remote AdministrationでHTTP接続を許可するのであれば、Remote Administrationでは正しく接続できるよう異なるポートを使用する必要があります。HTTPS接続はHTTPSポートを使用する必要があります。

HTTPS/SSL用証明書の選択

ここにはお使いのSSL証明書が表示されます。Webmailで使用する証明書をクリックして選択します。デフォルトとして使用したい証明書の隣にある星印をクリックします。 MDaemonはTLSプロトコルの拡張であるServer Name Indication (SNI)に対応しており、サーバーのホスト名毎に、異なる証明書を使用する事ができます。MDaemonはアクティブな証明書を確認し、Subject Althernative Namesフィールドから、要求されたホスト名を選択します。(証明書の生成時、別名を指定する事もできます。)クライアントがホスト名を要求していなかった場合や、対象の証明書が存在していなかった場合、デフォルトの証明書が使用されます。Windowsの証明書ダイアログを起動し、証明書のレビューを行うには、対象の証明書をダブルクリックしてください。(これはブラウザベースのリモート管理画面ではなく、アプリケーション画面からのみ利用できます。)

削除
一覧から証明書を選択し削除をクリックします。確認画面で証明書を削除するかどうかを質問されます。

証明書の作成
このボタンをクリックしSSL証明書の作成ダイアログが起動します。

証明書詳細

ホスト名
証明書作成時、ユーザーが接続する際のホスト名を入力します。（例: wc.example.com）。

組織/会社名
証明書を所有する組織名や会社名を入力します。

ホスト名の別名（カンマで複数設定）
ユーザーが接続する際などに使用するWebmailの別ホスト名がある場合は、カンマで区切ったドメイン名をここへ入力します。ワイルドカードにも対応しており、例えば"*.example.com"は(例えば "wc.example.com", "mail.example.com"といった)example.comのサブドメインに対しても適用できます。

> MDaemonはTLSプロトコルの拡張であるServer Name Indication (SNI)に対応しており、サーバーのホスト名毎に、異なる証明書を使用する事ができます。MDaemonはアクティブな証明書を確認し、Subject Althernative Namesフィールドから、要求されたホスト名を選択します。クライアントがホスト名を要求していなかった場合や、対象の証明書が存在していなかった場合、デフォルトの証明書が使用されます。

暗号キーの長さ
この証明書で使用する暗号化キーのビットの長さを選択します。長い暗号化キーを使うとより安全な通信が行えますが、全てのアプリケーションで512を超える長さのキーに対応しているわけではありあせん。

国
サーバーが設置している国や地域を選択します。

ハッシュアルゴリズム
使用するハッシュアルゴリズムをSHA1かSHA2から選択します。デフォルトはSHA2です。

webサーバーの再起動

ボタンをクリックしウェブサーバーを再起動します。新しい証明書を使用するにはウェブサーバーの再起動が必要です。

証明書の管理にLet's Encryptを使用する

Let's Encryptとは、セキュアなウェブサイト向けに、従来手動で行っていた証明書の生成、検証、署名、インストール、更新といった複雑な処理を自動化し、無償の証明書を発行している認証局（CA）です。

Let's Encryptの自動処理で証明書を管理するのに、Let's Encrypt[541]画面にてMDaemon¥LetsEncryptフォルダに格納されたPower Shellスクリプトを簡単に実行するためのオプションを用意しています。スクリプトを実行するとLet's Encrypt用に、Webmail HTTPフォルダへhttp-01チャレンジに必要なファイルの配置を含む、全ての設定が行われます。ここでは、証明書用のドメインとしてデフォルトドメイン[165]のSMTPホスト名[167]が関連するホスト名と併せて使用され、証明書の取得と受信、Windowsへのインポート、MDaemon, Webmail, Remote Administrationでこれらの証明書を使用するためのMDaemon設定が行われます。更に、スクリプトはMDaemon¥Logs¥フォルダへLetsEncrypt.logというログも生成します。このログはスクリプト実行の度に削除され再生成され、スクリプトの開始時間が記録されます。通知用の管理者アドレスへは、エラー発生時にはメールでの通知も行われます。詳細についてはLet's Encrypt[541]を参照してください。

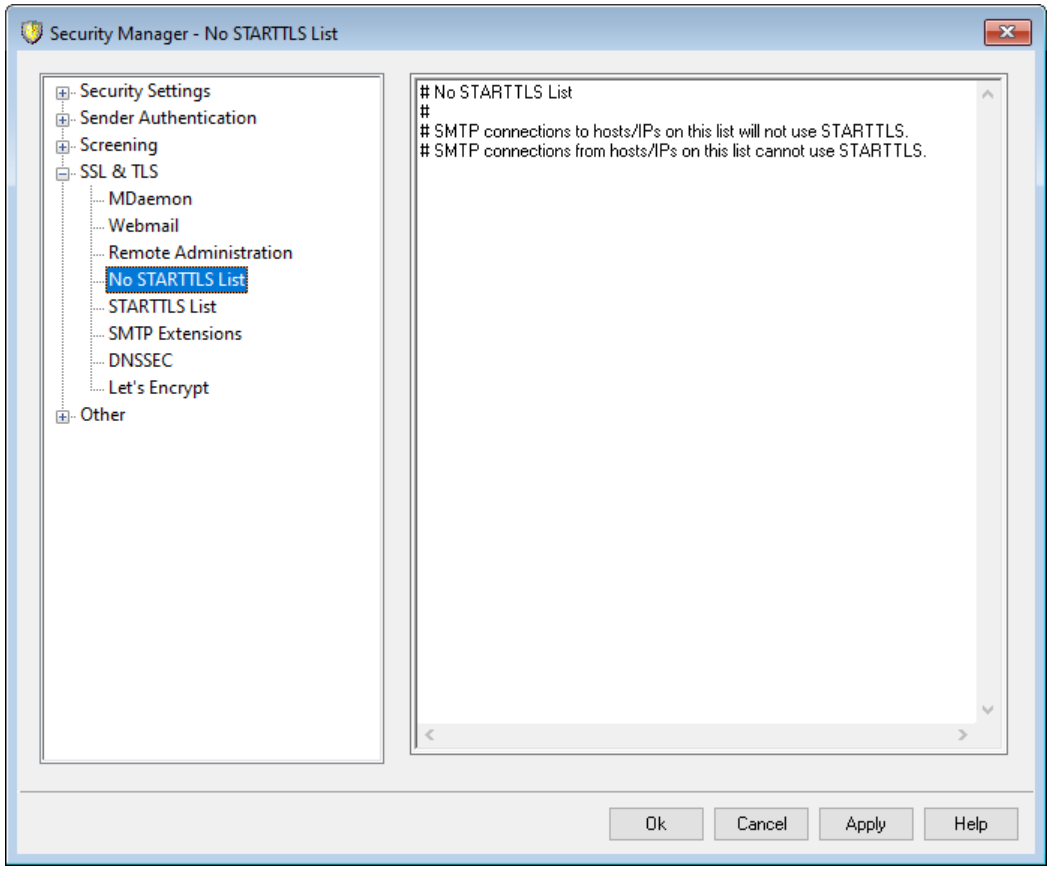
SSLと証明書についての詳細はこちらを参照して下さい:

IISでRemote Administrationを使用する[329]
SSLと証明書[523]
SSL証明書の作成と利用[830]

Remote Administrationについての詳細はこちらを参照して下さい:

Remote Configuration[321]
Remote Administration ≫ Webサーバ[322]
Webアクセスのデフォルト[728]
アカウントエディタ ≫ Web[656]

4.1.4.4 STARTTLS非使用リスト



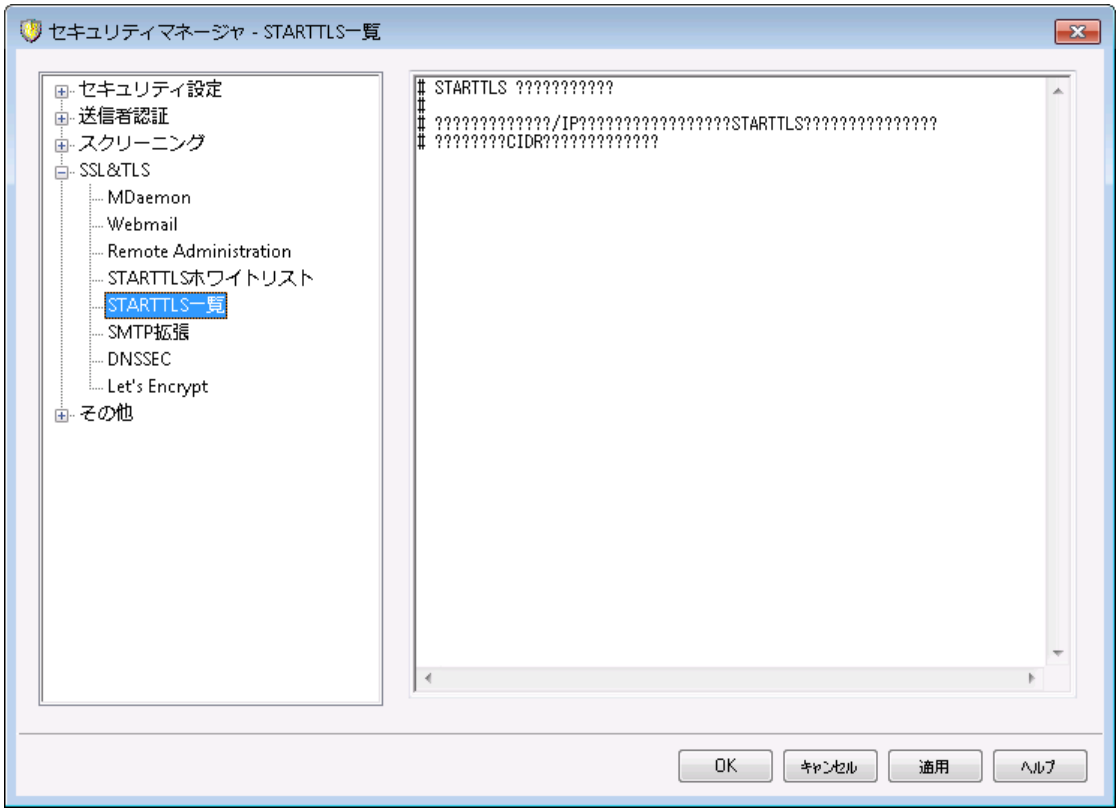
特定のホストやIPアドレスとのメール送受信時、STARTTLSの使用を行わないようにするには、このリストを使用します。

STARTTLS非使用リストは STARTTLS要求リスト 537 や *SMTPサーバーはMSAポートのSTARTTLSを必須とする* 525 オプションよりも優先されます。

RFC-3207で定義されているSMTPのSTARTTLS拡張については、下記を参照してください:

http://www.rfc-editor.org/rfc/rfc3207.txt

4.1.4.5 STARTTLS一覧

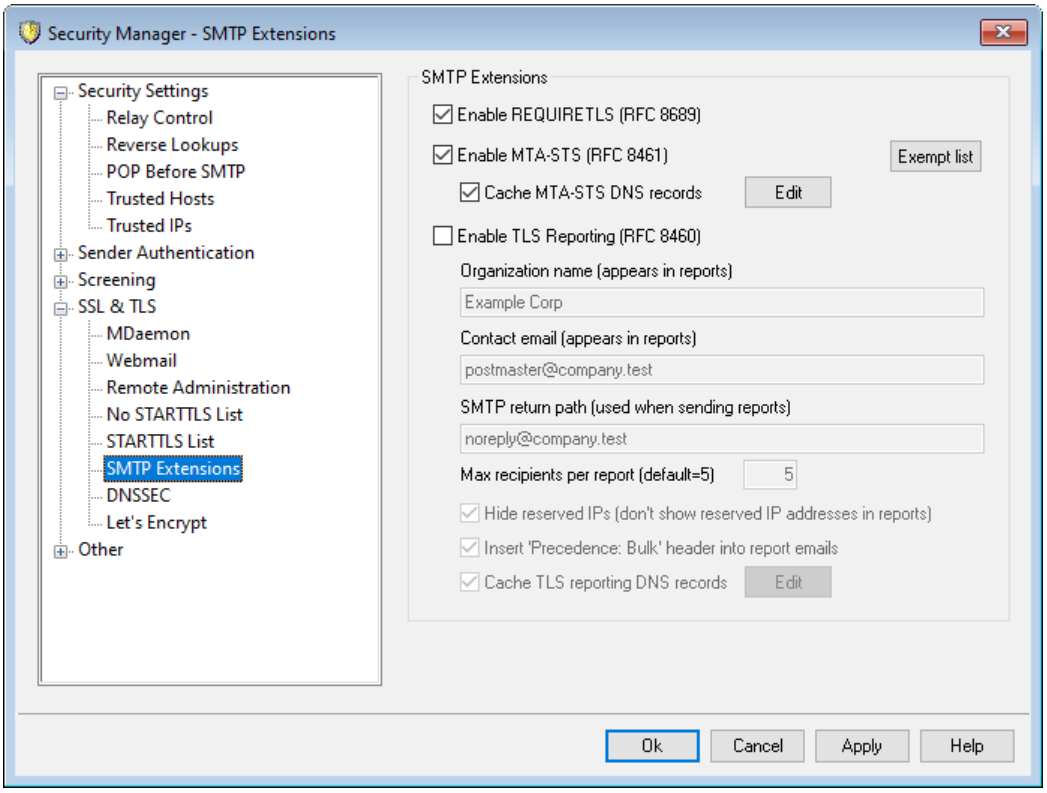


ここでは、サーバーとでメールの送受信を行うのにSTARTTLS拡張を必須とするホストやIP、MAIL FROMアドレスを指定します。

RFC-3207で定義されているSMTPのSTARTTLS拡張については、下記を参照してください:

http://www.rfc-editor.org/rfc/rfc3207.txt

4.1.4.6 SMTP拡張



SMTP拡張

REQUIRETLSを有効化（RFC 8689）
RequireTLSはメールの送信時TLSを必須とするようフラグ付けできるSMTP拡張です。TLSが不可能（またはTLS証明書の交換が不可能）の場合、メールは暗号化されずに送信するのではなく、エラーとして戻されます。RequireTLSの詳細な説明は: RFC 8689: SMTP Require TLS Optionを参照してください。

RequireTLSはデフォルトで有効ですが、RequireTLSの処理対象となるメッセージは新しいコンテンツフィルタアクション[590]である「REQUIRETLS…のフラグを追加」でコンテンツフィルタによるフラグ付けされたものか、<local-part>+requiretls@domain.tld（例えばarvel+requiretls@mdaemon.com）宛のメールだけです。他のメールは全て、サービスが無効であるかのように処理されます。メールをRequireTLSを使って送信するにはいくつかの条件があります。条件を満たせない場合メールは送られずにエラーとして戻されます。要件は次の通りです。

- RequireTLSが有効化されていること
- コンテンツフィルタアクションや"<localpart>+requiretls@..."アドレスで、メールへRequireTLS処理が必要というフラグ付けがされていること
- 宛先MXホストへのDNSルックアップでDNSSEC[540]を使用している（下記を参照）か、MXがMTA-STSで検証済である事
- 受取側のホストへの接続にSSL（STARTTLS）が使用されていること
- 受取側のホストのSSL証明書がMXホスト名と一致しており、信頼するCAへ紐づけられていること

- 受信メールサーバーがREQUIRETLSに対応しておりEHLOレスポンスを返す事ができること

RequireTLSにはMXレコードホストのDNSSECによるルックアップか、MXがMTA-STSによる検証が必要です。DNSSECで、DNSSECサービスのルックアップ用パラメータを指定する事でDNSSECの設定[540]が行えます。MDaemonのIPキャッシュ[101]にはDNSSEC処理を許可するオプションがあり、DNSSEC関連の説明がMX Hostsファイル[94]の最初にも記載されています。最後に、DNSSECは正しく設定されたDNSサーバーが必要ですが、これはこのヘルプファイルの説明の対象外となります。

MTA-STSを有効化（RFC 8461）

MTA-STS対応はデフォルトで有効化されており、RFC 8461: SMTP MTA Strict Transport Security (MTA-STS)にて詳細をご確認頂けます。

SMTP MTA Strict Transport Security（MTA-STS）は は、メールサービスプロバイダー（SPs）側でメールを受信するにあたり、セキュアなSMTP接続が行えるトランスポート層レベルのセキュリティTransport Layer Security（TLS）に対応していることを宣言し、信頼のできるサーバ証明書を使用していない場合にメール送信側でメールを送信するかしないかを指定できる仕組みです。管理しているドメインに対してMTA-STSを設定するには、HTTPSを使った通信でURL https://mta-sts.domain.tld/.well-known/mta-sts.txt（"domain.tld"部分は、実際のドメイン名に置き換えてください）からMTA-STSポリシーファイルをダウンロードできるようにする必要があります。ポリシーファイルは、次のフォーマットで記載してください:

```
version: STSv1
mode: testing
mx: mail.domain.tld
max_age: 86400
```

modeパラメータには、"none"、"testing"、"enforce"の指定が可能です。mxパラメータには、MXホスト名を指定して下さい。サブドメインに対しては、"*.domain.tld"といったワイルドカードの使用もできます。max_ageの単位は秒で、一般的な値は86400（1日）か604800（1週間）です。

また、DNSサーバには、TXTレコードに、_mta-sts.domain.tld（"domain.tld"は実際のドメイン名に置き換えてください）という登録が必要で、次のフォーマットで値を記述して下さい。

```
v=STSv1; id=20200206T010101;
```

"id"の値は、ポリシーファイルの編集を行った際、その反映のため都度値を変更してください。一般的にidには、タイムスタンプを使用します。

除外リスト

特定のドメインをMTA-STSから除外するにはこのリストを使用します。

MTA-STS DNSレコードをキャッシュ

デフォルトで MDaemonは MTA-STS DNS レコードをキャッシュとして保持します。編集をクリックし、現在のキャッシュファイルの表示や編集が行えます。

TLS Reportingを有効化（RFC 8460）

TLS Reportingはデフォルトで無効に設定されており、RFC 8460: SMTP TLS Reportingで議論されています。

TLS Reportingは、MTA-STSポリシーの取得やSTARTTLSを使ったセキュアな接続のネゴシエーションに失敗した通知を、MTA-STSを使用するドメインに行ないます。有効にすると、MDaemonは

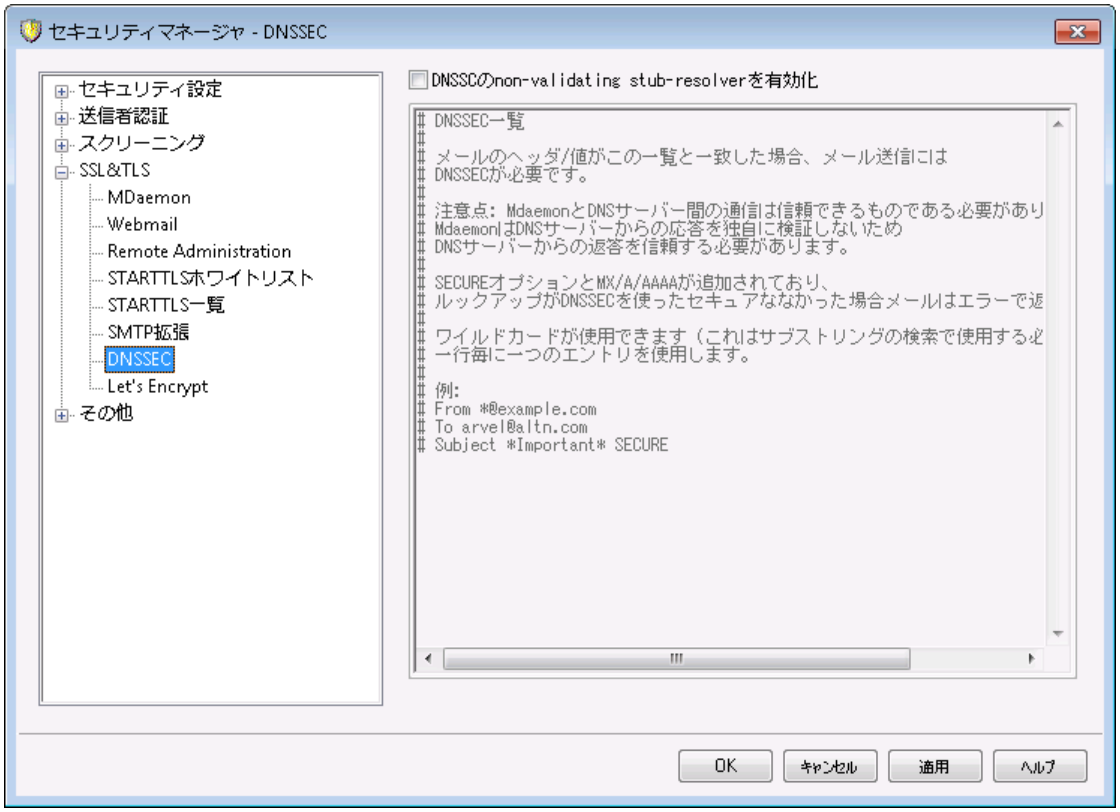
各MTA-STSを使用するドメインへその日の送信した(もしくは送信を試みた)メールのレポートを日次で送ります。レポートに含む情報について、設定できる幾つかのオプションがあります。

ドメインのTLS Reportingを設定するには、DKIM署名[484]を有効にし、DNS TXTレコードを_smtp._tls.domain.tldといった形式で作成します。"domain.tld"は実際のドメイン名に置き換えてください:

```
v=TLSRPTv1; rua=mailto:mailbox@domain.tld
```

mailbox@domain.tldの部分には、レポートメールを受信するメールアドレスをご指定下さい。

4.1.4.7 DNSSEC



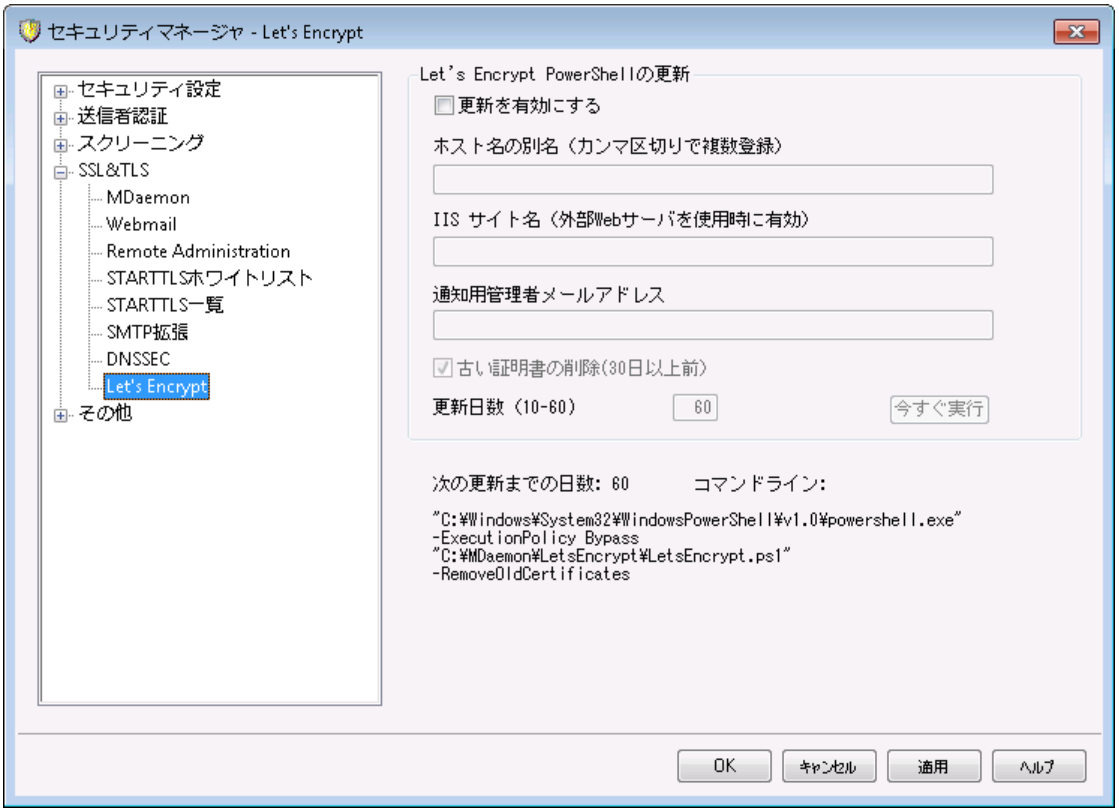
新しいDNSSECEC (DNS Security Extensions)オプションで、MDaemonがRFCの 4033 と4035 にて「DNSクエリの送信やDNS応答の受信、スタブリゾルバのサービスを提供できるDNSSEC対応ネームサーバーとの安全な通信の確立を行うエンティティ」と定義された、署名を検証しないDNSSEC対応スタブリゾルバとして動作できるようになります。これはMDaemonがDNSへの問合せを行う際DNSSECサービスをDNSサーバーへ要求し、AD (Authentic Data)ビットを使った問合せを行い、応答を確認できるようになるという事です。DNSSECは現在全てのDNSサーバーが全てのトップレベルドメイン向けに対応しているものではありませんが、これによりDNS処理中に追加レベルのセキュリティを実装する事ができるようになります。

有効化すると、DNSSECサービスは選択条件にマッチしたメールに対してのみ適用されます。DNSSECサービスはメール毎に「要求」したり「必須」としたりできます。DNSSEC画面で「ヘッダ値」の組み合わせを選択するだけで、MDaemonはDNSの問合せの際条件にマッチしたメールにのみDNSSECサービスを要求します。「必須」としている場合で認証データを含むDNSの応答に失敗すると、メールは送信者へ返されます。「要求」している場合はDNSSECサービスで失敗した場合でも何も起こりません。ただし、特定のメールに対してDNSSECを必須とする場合は、ヘッダ値の組み合わせへ「SECURE」を追加してください。(例. `To *@example.net SECURE`)これらのメッセージで認証データを含むDNSの応答に失敗すると、メールは送信者へ返されます。**注意点**: DNSSECルックアップには従来よりも時間やリソースが必要となり、また、DNSSECは全てのサーバーで対応しているわけではないため、MDaemonは全てのメール配信へDNSSECを適用するデフォルト設定にはなっていません。ただし、必要に応じ、設定ファイルの中に「To *」などの行を一行追加する事で、全ての送信メールでDNSSECの利用を必須とする事ができます。

メールのセッションログの最初にはDNSSECが使われたかどうかが、ログのセキュアデータの隣にDNSSECとして記録されます。

MDaemonは非公式のスタブリゾルバーです。つまり、MDaemonはDNSサーバーへ認証データをリクエストしますが、単独でデータがセキュアかどうかを確認する事ができません。ただし、(例えばLAN内のサーバー間の場合など)DNSサーバーへの接続が既知のものだったり信頼できるものだったりする場合は、これをセキュリティ強化の目的で活用する事ができます。

4.1.4.8 Let's Encrypt



証明書の管理にLet's Encryptを使用する

MDaemon 525, Webmail 528, Remote Administration 532, でSSL/TLSやHTTPS 523を使用するには、SSL/TLSの証明書が必要です。証明書は小さなファイルで認証局（CA）によって発行され、対象サーバーへ接続したクライアントやブラウザで、SSL/TLS/HTTPSによる安全な接続を行おうとしているものに対して、通信元が偽装されているものではない事を証明しています。Let's Encryptとは、セキュアなウェブサイト向けに、従来手動で行っていた証明書の生成、検証、署名、インストール、更新といった複雑な処理を自動化し、無償の証明書を発行している認証局（CA）です。

LetsEncrypt対応として、MDaemonではPowerShellスクリプトをMDaemon¥LetsEncryptディレクトリへ格納しています。スクリプトを実行するとLet's Encrypt用に、Webmail HTTPフォルダへhttp-01チャレンジに必要なファイルの配置を含む、全ての設定が行われます。ここでは、証明書用のドメインとしてデフォルトドメイン 165のSMTPホスト名 167が関連するホスト名と併せて使用され、証明書の取得と受信、Windowsへのインポート、MDaemon, Webmail, Remote Administrationでこれらの証明書を使用するためのMDaemon設定が行われます。更に、スクリプトはMDaemon¥Logs¥フォルダへLetsEncrypt.logというログも生成します。このログはスクリプト実行の度に削除され再生成され、スクリプトの開始時間が記録されます。通知用の管理者アドレスへは、エラー発生時にはメールでの通知も行われます。

> Let's Encrypt は PowerShell 5.1 と.Net Framework 4.7.2が必要であり、Windows 2003では動作しません。 Webmail 295は80番ポートを待ち受けポートにする必要があり、デフォルトドメインSMTPホスト名 167としてMDaemonサーバー以外を指している場合は、このスクリプトは機能しません。

Let's Encrypt PowerShellの更新

更新を有効にする
Let's EncryptスクリプトでSSL/TLSの証明書の自動生成や更新を行うにはこのチェックボックスをクリックします。証明書は更新日数により10～60日毎に更新されます。

ホスト名の別名（カンマ区切りで複数登録）
証明書でホスト名の別名を使用する場合はここで、カンマ区切りで指定します。ここへはデフォルトドメインのSMTPホスト名を含む必要はありません。例えば、デフォルトドメインがexample.com、FQDNがmail.example.comの場合で、imap.example.comを使用したい場合、別名としてimap.example.comのみを指定します。別名が不要の場合は、ここは空白のままにしておきます。注意点：ここで別名を指定した場合、対応するHTTPチャレンジをLet's Encryptで用意する必要があります。チャレンジを全てパスしないと、プロセスは失敗として終了します。

IISサイト名（外部Webサーバーを使用している場合に有効）
WebmailをIISで稼働させている場合、IISサイト名をここで指定します。IISで証明書の自動設定を行うにはMicrosoftのWebスクリプティングツールがインストールされている必要があります。

通知用管理者アドレス
Let's Encryptの更新でエラーが発生した際、通知メールを送るにはここで管理者用のメールアドレスを指定します。

(期限切れから30日以上の)古い証明書を削除
デフォルトで MDaemon は30日以上経過した古い証明書を削除します。証明書を自動で削除したくない場合はこのボックスをクリアしてください。

更新日数 (10-60)

証明書の更新頻度を日数で指定します。10から60の間の数値を指定でき、デフォルトは60日です。

今すぐ実行
スクリプトをすぐに実行する場合はこのボタンを押してください。

4.1.5 その他

4.1.5.1 バックスキャッタ保護 - 概要

バックスキャッタ(後方散乱)

バックスキャッタとは、ユーザーが実際には送っていなかったメールに対する応答メールを意味しています。これはスパムメールやウィルスによって送られたメールに含まれる、偽装されたReturn-Pathが原因で起こります。結果として、こうしたメールが受信者側で拒否されたり、自動応答機能などで返信されたりすると、応答メールは偽装された側のアドレスへ送信されてしまいます。これにより、大量の配信失敗通知や応答通知がユーザーのメールボックスを一杯にします。スパム送信者やウィルス開発者がこの方法を用いる事は珍しくなく、時には世界中から届く通知メールを氾濫させる事により、DoS攻撃を行う場合もあります。

MDaemonのソリューション

バックスキャッタを防止するために、MDaemon はバックスキャッタ保護(BP)と呼ばれる機能を持ちます。BPは、プライベートなハッシュキーを生成して送信メールのReturn-Pathアドレスへ埋め込む事で、正しい配信失敗通知や自動応答メールだけが届いている事を確認する機能です。メールが配信エラーになり戻ってきた場合や、自動応答が"mailer-daemon@ ..."やNULLリバースパスで送られてきた場合、MDaemonは生成したハッシュキーを確認し、このメールがMDaemonが管理しているアカウントが元になっているのかどうかを判断します。アドレスに特別なコードが含まれていなかった場合や、7日間以上経過していた場合、MDaemonのログへ記録され、メールは拒否されます。

バックスキャッタ保護 544 はMDaemonのセキュリティメニューの、セキュリティ ≫ セキュリティ設定 ≫ その他 ≫ Backscatter保護からアクセスできます。

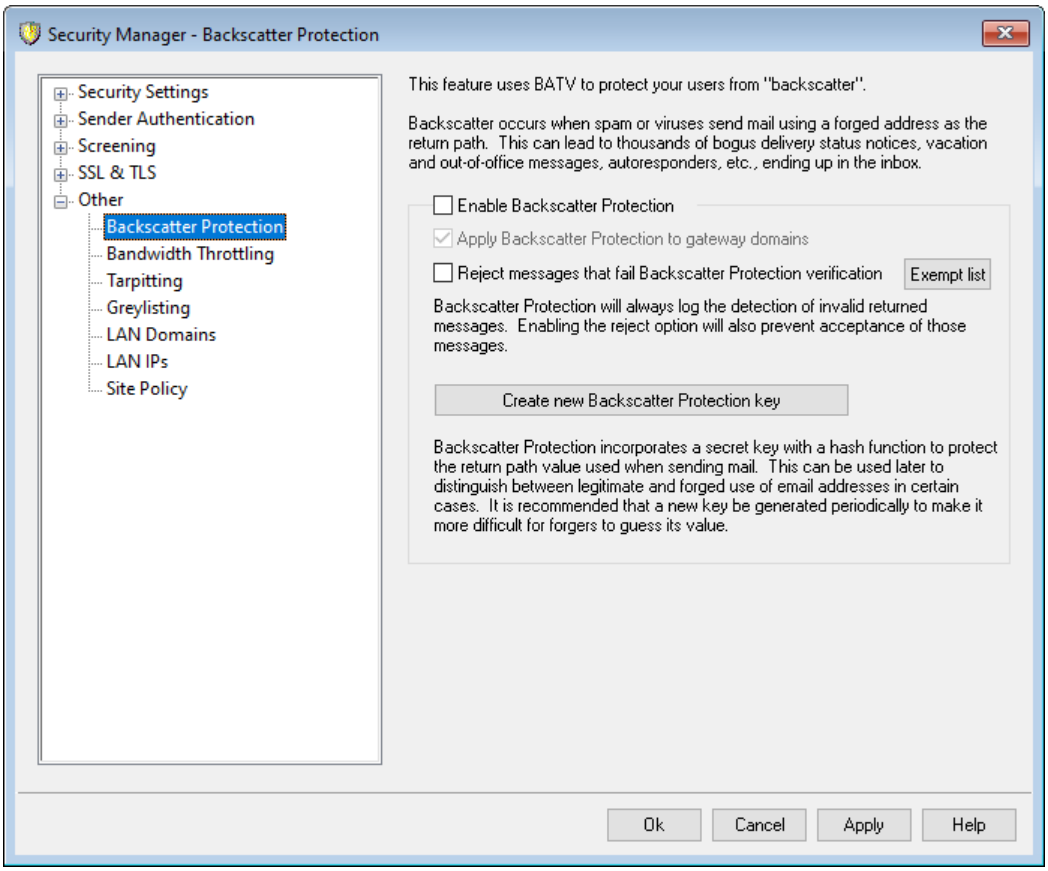
バックスキャッタ保護は Bounce Address Tag Validation (BATV)により開発されました。BATVについては以下のURLを参照してください。

http://www.mipassoc.org/batv/

参照:

バックスキャッタ保護 544

4.1.5.1.1 バックスキャッタ保護



バックスキャッタ保護

バックスキャッター保護を有効にする
特別なバックスキャッタ保護(BP)用コードを送信メールの`Return-Path`へ挿入する場合には、このオプションを選択してください。有効にすると、MDaemonは PEM_batv フォルダ内のrsa.privateファイルで指定された秘密鍵を使用して、7日間有効な特別なコードを生成します。受信する配信失敗通知や(`"mailer-daemon@ ..."`やNULLリバースパスからの)その他の自動応答メールには、正しい有効期間内のBPコードが必要で、このコードが確認できないメールはBP検証に失敗します。

このオプションが無効の場合、MDaemonは送信メッセージに特別なBPコードを挿入しません。ただし有効なコードによる任意の受信メッセージが誤って拒否されないことを保証する受信DSNおよび自動応答メッセージをチェックし続けます。

ゲートウェイドメインに適用する
バックスキャッタ保護が有効であり、MDaemonがゲートウェイまたはバックアップサーバとして実行しているドメインに適用する場合、このオプションをクリックします。(ゲートウェイマネージャ 227参照)

バックスキャッター保護の検証に失敗したメッセージを拒否する
BP検証に失敗するDSNまたは他の自動応答メッセージを拒否する場合、このチェックボックスを選択します。"mailer-daemon@ ..."やNULLリバースパスが含まれるメールで、特別なコードがないものや7日間のライフサイクルを超えてしまっていたものは検証に失敗します。Backscatter Protectionの堅牢な信頼性で、誤検出またはメッセージが有効/無効という「グレーゾーン」がありません。この理由のために、アカウントの送信メッセージのすべてが特別なBPコードを持つことを保証する限り、無効なメッセージを拒否するためにMDaemonを構成するのは安全です。ただし、検証に失敗したメールを拒否しない場合や、いかなる場合であっても、BP検証の結果はSMTP-inログファイルに記録されます。上記の**ゲートウェイドメインに適用する**オプションを選択しない限り、ゲートウェイ用の受信メールが拒否される事はありません。

バックスキャッタ保護を有効にする場合は、BPを有効にする前に送ったメールに対してDSNや自動応答を受信する可能性が高いという理由から、無効な自動応答メールを拒否する設定を行う前に約1週間待つ事をお勧めします。BPがその期間中に無効なメッセージを拒否する構成がされる場合、正当な応答メッセージは誤って拒否されます。1週後に、無効なメッセージを拒否し始めるのは確実です。新規のBPキーを作成し、別の7日間機能を継続することを許可する代わりに、直ちに旧式キーを削除を選ぶ場合、この同じ警告は適用されます。（**新しくバックスキャッター保護用キーを作成する** を参照）

除外リスト
このボタンをクリックすると、バックスキャッタ保護の除外リストが開きます。バックスキャッタ保護から除外する任意のIPアドレスまたはドメインを指定するために、このリストを使用します。

新しくバックスキャッター保護用キーを作成する
新規のBackscatter Protectionキーを生成するには、このボタンをクリックしてください。このキーを使ってMDaemonは、メールに挿入する特別なBPコードを作成し、これを検証します。キーは、MDaemonのPEM/_batv/フォルダにrsa.privateと呼ばれるファイルとして生成されます。新規のキーが生成されると、削除しない限り古いキーが7日間継続して機能する事を通知するダイアログが表示されます。ほとんどの場合、古いキーを7日間使えるよう、"いいえ"を選ぶ事をお勧めします。すぐにキーを削除してしまうと、古いキーで生成された特別なコードを含むメールへのレスポンスを受信した場合に、受信メールがBP検証で失敗してしまう場合があります。

複数サーバでメールトラフィックを分散させている場合、キーファイルを他の全てのサーバやMail Transfer Agents(MTA)と共有する必要があります。

参照:

バックスキャッタ保護 - 概要 543

4.1.5.2 帯域幅調整 - 概要

帯域幅を調節する機能により、MDaemonによって使用される帯域幅の消費を監視することができ、進行中のセッションあるいはサービスの割合をコントロールすることができます。これによりMDaemonの主なサービスにおいてドメインゲートウェイや各ドメイン単位で異なる割合を設定することができます。またドロップダウンリストで[ローカル通信]を選択することにより、ローカル接続の帯域幅の範囲を設定することも可能です。これにより、ローカルIPアドレスまたはドメイン名からの(あるいはそこへの)接続に対して、特定の帯域幅の設定を行うことができます。これらの設定を行うためのローカルIPアドレスおよびドメイン名のリストを構成する新しい画面が用意されています。

帯域幅の調節はセッションごとあるいはサービスごとに行うことができます。セッションごとのモードの場合、各セッションはそれぞれ独立して調節することができます。このように、同時に発生している同じサービスタイプの複数のセッションは、サービスの設定された値を超えることができます。サービスごとのモードの場合、MDaemonは同じサービスタイプのすべてのセッションの合計をモニタし、各々に対して帯域幅の合計を等しく分配します。これにより、すべてのサービスをひとまとめにした限界値を設定することが可能になります。

帯域幅の調節をドメインゲートウェイに拡張する場合、ドメインゲートウェイは特定のIPアドレスを持たないので、通常のドメインとは多少異なる設定方法が必要です。MDaemonはRCPTコマンドで渡された値を使用して、受信したSMTPセッションがゲートウェイ宛てかどうかを判断しなければなりません。それがゲートウェイ宛てであるならば、そのセッションにはSMTP受信帯域幅の調節が適用されます。SMTPの制限により、あるメッセージの複数の受信者のうちの一人のみがドメインゲートウェイに向けられている場合でも、すべてのセッションが調節の対象となります。

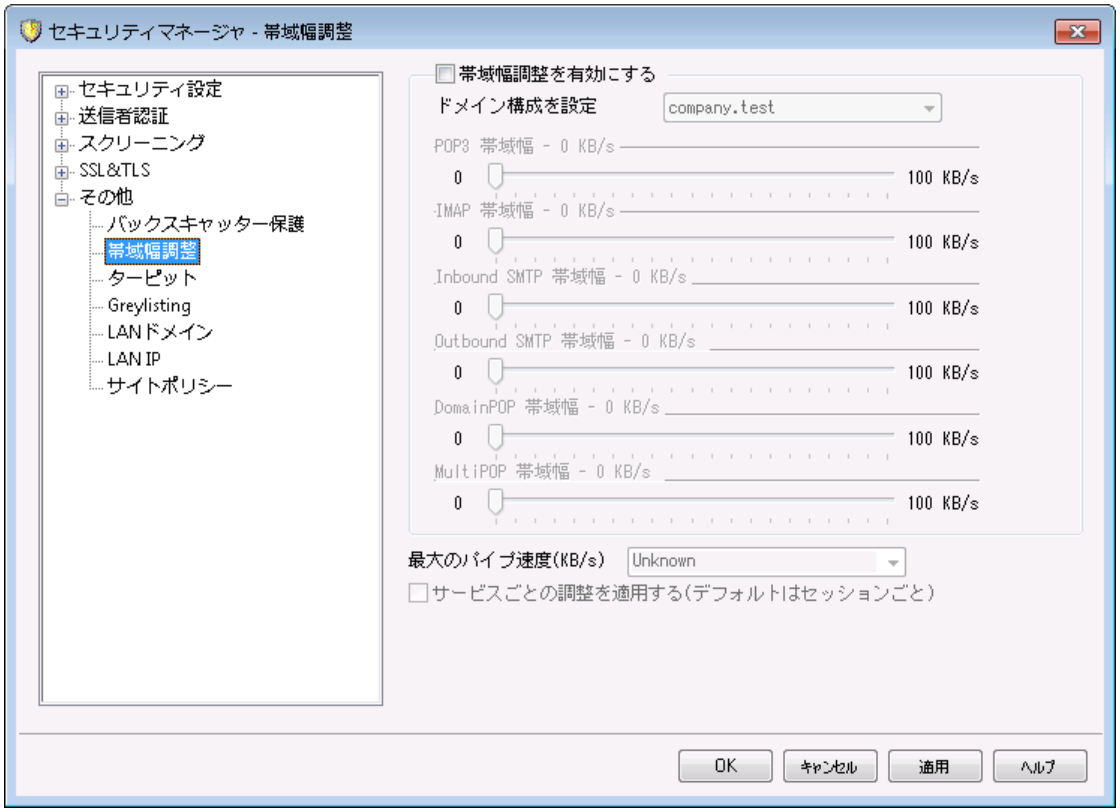
帯域幅調整システムはキロバイト/秒で表されます。ここでの0(ゼロ)は進行中のセッションまたはサービスのスピードに制限がなく、利用できる帯域幅の最大量を使用することを表します。例えば、この数字が[10]の場合は、MDaemonによる接続スピードを10キロバイト/秒前後に制限するように強制します。

セッションの開始直後に突発的に発生するアクティビティにより、帯域幅が設定値を超えてしまう場合がありますが、セッションの進行に伴い適正な値に調節されます。

参照:

帯域幅調整 547
LAN IPs 554

4.1.5.2.1 帯域幅調整



帯域幅調整を有効にする
帯域幅調整の機能を開始する場合、このチェックボックスを選択します。

ドメインの構成を設定
ドロップダウンリストからドメインを選択して、そのドメインに対する帯域幅調整を設定するための様々なオプションを調整してください。どのコントロールにおいても0(ゼロ)は帯域幅の制限をなくすことを意味します。ドロップダウンリストの一番下には"Local traffic"というエントリがあります。このオプションの帯域幅調整の設定は、ローカルトラフィック(すなわち、外部でなくローカルLANの上で発生しているセッションおよびサービス)に配置される制限を決めます。LAN IP[554]画面は、ローカルもので処理されるIPアドレスを一覧にするために使用することができます。

サービス

[サービスのタイプ] 帯域幅 - XX KB/s
ドロップダウンリストからドメインを選択したら、これらのコントロールを調節して、そのドメインに関する帯域幅制限を設定してください。ここでの0(ゼロ)は帯域幅の制限をなくすことを意味します。スライダーを0(ゼロ)以外に設定した場合は、その設定した数字が帯域幅の最大値(キロバイト/秒)となります。

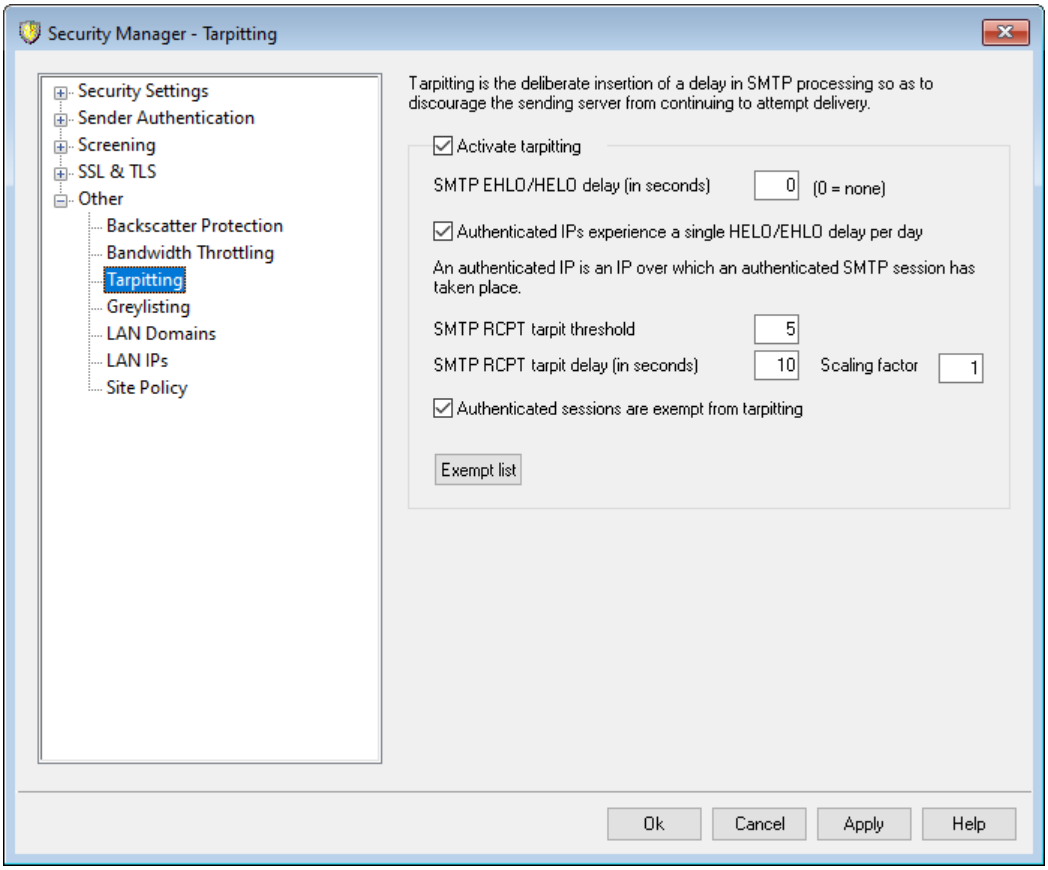
最大のパイプ速度(KB/s)
ドロップダウンリストボックスから、接続の最大速度(毎秒キロバイト単位)を選択します。

サービスごとの調整を適用する(デフォルトはセッションごと)
デフォルトであるセッションごとの帯域幅調整ではなく、サービスごとの調整に変更する場合は、このチェックボックスを選択してください。サービスごとの調整の場合、サービスに指定される帯域幅は同じサービスタイプのすべてのセッションの合計をモニタし、各々に対して帯域幅の合計を等しく分配します。例えば、同時に接続している複数のIMAPクライアントが使用する帯域幅の合計は、接続しているクライアントの数に関わらず、指定された帯域幅を超えることは決してありません。しかし、セッションごとの調整の場合は、1つのIMAPセッションは指定された帯域幅を超えることはありませんが、セッションの合計の帯域幅は指定された値を超えることができます。

参照:

帯域幅調整 - 概要 546

4.1.5.3 ターピット



ターピッティングは、セキュリティメニューのセキュリティ ≫ セキュリティ設定 ≫ その他 ≫ ターピットにあります。

ターピットでは、メール送信者から受け取ったRCPTコマンドが指定した回数に到達すると、意図的に接続間隔を遅らせる事ができます。これは、スパム送信者がサーバを利用して、大量のバルクメール(スパム)を送信することを思いとどまらせる効果があります。ターピッティングを開始するのに必要なRCPTコマンドの回数と接続を遅延させる場合の接続間隔を秒数で指定する事ができます。このテクニックでは、スパムメールの送信者に対して、個々のメールの送信に関わる時間を長くかけさせることにより、彼らの意欲を減退させ、将来的にサーバを送信ターゲットからはずすという目的があります。

ターピットを有効にする
このチェックボックスを選択するとMDaemonのターピット機能を開始します。

SMTP EHLO/HELO遅延(秒単位)
EHLO/HELO SMTPコマンドに対するサーバ応答の遅延時間を設定します。わずか10秒の遅延でも、スパムを受信する量が減りますので、処理時間の大幅な短縮ができます。スパマーにとっては短時間でメールをばらまくことが重要なので、EHLO/HELOコマンドの応答を待ち続けることを嫌います。そのため、わずかな遅延であっても、スパム送信ツールは送信を諦めて次のターゲットへの送信へ移ります。(サーバ設定のポート 96 画面で設定できる)MSAポートへの接続はこの遅延から除外されます。このオプションのデフォルト設定は0(ゼロ)で、EHLO/HELO遅延を行いません。

認証されたIPで1日に1度のEHLO/HELO遅延を発生する
特定のIPアドレスからの認証済み接続のEHLO / HELO遅延を1日1回に制限する場合は、このチェックボックスを有効にします。 そのIPアドレスからの最初のメッセージは遅延されますが、同じIPアドレスから送信される後続のメッセージは送信されません。

SMTP RCPTターピットしきい値
MDaemonが、そのホストにターピットを開始する前に、メールセッション中で許可するSMTP RCPTコマンドの数を指定してください。例えば、この数が10に設定されて、サーバがメッセージを20のアドレス(すなわち、20のRCPTコマンド)への送信を試みている場合、MDaemonは最初の10件の送信を許可して、その後の10件に対しては、コマンドを受け取るごとに、以下の[SMTP RCPTターピット遅延]コントロールで設定した時間だけ接続を停止します。

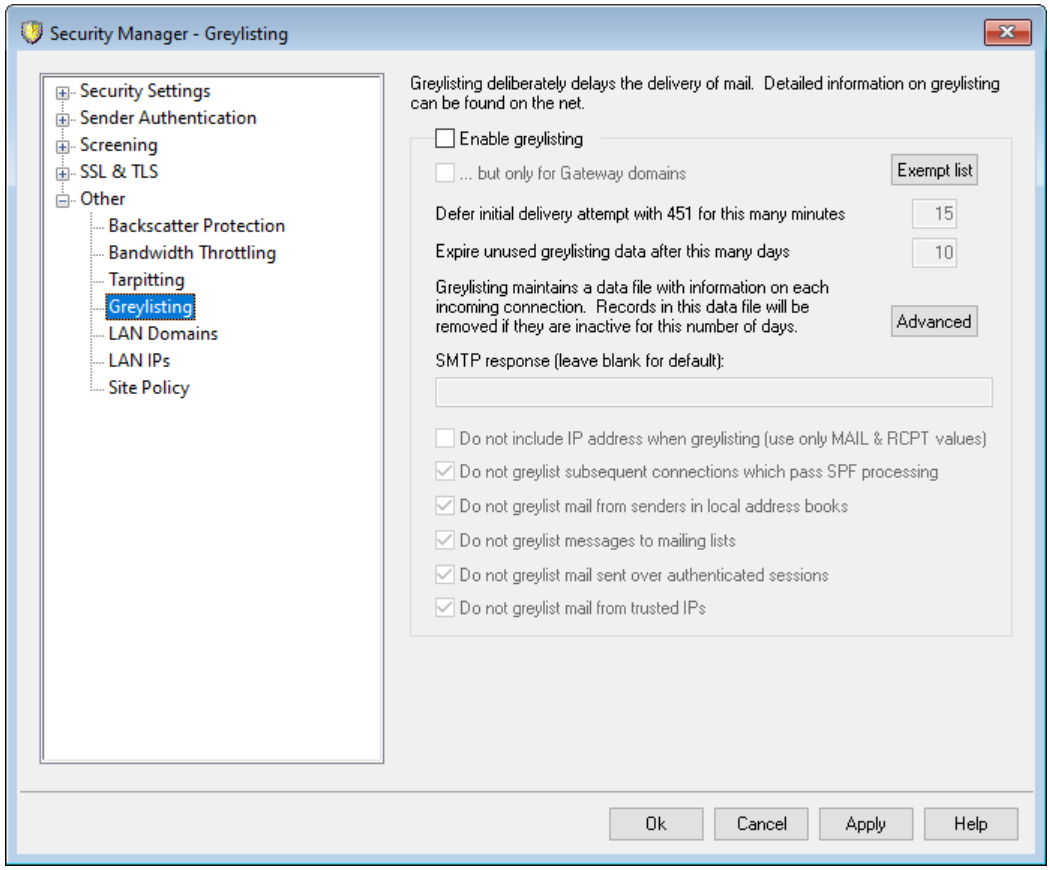
SMTP RCPTターピット遅延(秒)
この数値は、1つのメールセッション中のRCPTコマンドの数が上記の[SMTP RCPTターピットしきい値]の数値に達した時に、その後各RCPTコマンドを受け取るごとに、MDaemonが停止する時間(秒)です。

スケーリング係数
これはベースターピット遅延が時間と共に増大される乗数です。ターピットしきい値に達し、ターピット遅延がセッションに適用される場合、この値を乗じた秒数が次の遅延の長さになります。例えばターピット遅延が10でスケール係数が1.5の場合、最初の遅延は10秒、2番目の遅延は15秒、3番目は22.5秒、次は33.75(例えば10 ×1.5=15、15 ×1.5=22.5といった具合)となります。デフォルトのスケール係数は1ですので遅延の増大はありません。

認証されたセッションをターピットから除外する
これはベースターピット遅延が時間と共に増大される乗数です。ターピットしきい値が到達され、ターピット遅延がセッションに適用される場合、この値を乗じた秒数が次の遅延の長さになります。例えばターピット遅延が10でスケール係数が1.5の場合、最初の遅延は10秒、2番目の遅延は15秒、3番目は22.5秒、次は33.75(例えば10 ×1.5=15、15 ×1.5=22.5といった具合)となります。デフォルトのスケール係数は1ですので遅延の増大はありません。

除外リスト
タービットでも使用されるダイナミック許可リスト[569]を開くには、このボタンをクリックします。タービットから除外するIPアドレスを指定できます。

4.1.5.4 グレーリスト



グレーリストはセキュリティ ≫ セキュリティ設定 ≫ その他 ≫ グレーリストにあり、SMTPサーバが("try again later"などの)メールの再配信を試みるという機能を悪用するスパムメールに対応するための技術です。この技術を使用すると、メッセージが許可リストへ登録されていなかったり未知の送信者から送られた場合、その送信者、受信者、送信サーバのIPアドレスが記録され、そのメッセージはSMTPセッション内で、一時的なエラーコードと共にグレーリストによって拒否されます。さらに指定した期間(例えば15分間)は、同一サーバからの配信は同様に拒否されます。通常スパム送信者は、メールが拒否された際、再配信は行わないため、グレーリストによってユーザが受け取るスパムメッセージの数を大幅に減少させることができます。仮にスパム送信者が一定の時間の後に再び配信を試みた場合でも、その時までにスパム送信者を特定することは可能であり、DNSブロックリスト[638]などの他のスパムメール対策オプションによってブロックすることも可能です。しかし、この方法により[良い]メールが[悪い]メールと共に配信の遅延を起こしてしまう可能性があることに注意してください。その場合は、グレーリストの有効期間が切れた後に、正規のメールが通常どおりに配信されることになります。また送信サーバが次の送信試行までどのくらいの間隔をあけるかを知る方法が無い点についても注意をしておいてください。一時的なエラーコードによってメッセージを拒否すると、短い場合は数分で、長い場合は終日にわたって遅延が発生する可能性があります。

グレーリストには、従来からのいくつかの問題と否定的な副作用があります。そしてグレーリスト画面には、それらの問題に対処するように設計された多くのオプションが含まれています。

最初は、アウトバウンドメールを送る際に、いくつかの送信ドメインはメールサーバのプールを使用します。この方法はそれぞれの配信に、異なるメールサーバを使用することができるので、それぞれのメール配信の試行はグレーリストエンジンとの新しい接続として扱われます。これは、それぞれの試行が前のメッセージの再試行ではなく個別メッセージであるかのようにグレーリスト化されるので、通常より大幅に時間がかかる場合があります。SPFルックアップオプションを利用することによって、SPFデータを発行する送信ドメインにおけるこの問題を解決することができます。さらに、送信メールサーバのIPを完全に無視するオプションもあります。 このオプションを使用すると、グレーリストする効率は下がりますが、サーバプール問題を完全に解決することができます。

二番目に、グレーリストはそれぞれの接続要求を追跡しなければならないので、伝統的に大容量データベースを必要とします。MDaemonは、グレーリスト機能をSMTP処理の最後の段階で行うことにより、接続の追跡の必要性を最小限に押さえます。これにより、グレーリストの処理が行われる前に、MDaemonの他のすべてのオプションがメッセージを拒否することができます。その結果、グレーリストデータファイルのサイズは大きく減少し、またその機能はメモリに常駐するので、実用上の影響がほとんどありません。

最後に、[良い]メッセージへのグレーリストの影響を最小限にするために利用可能ないくつかのオプションがあります。最初に、メーリングリストに送られたメッセージは除外することができます。 次に、グレーリストは自身の除外リストファイルを持ち、グレーリストから除外するIPアドレス、送信者、および受信者を指定することがでます。最後に、グレーリストは各アカウントのプライベートアドレス帳を除外リストとしての使用するためのオプションを含んでいます。 したがって、そのユーザのアドレス帳に含まれるユーザへのメールはグレーリストから除外することができます。

グレーリストに関する一般的な情報は、以下のEven Harrisのサイトを参照してください。

http://projects.puremagic.com/greylisting/

グレーリスト

グレーリストを有効にする

MDaemonでグレーリスト機能を有効にするためには、このオプションを選択してください。

...ゲートウェイドメインに対してのみ
ゲートウェイドメインに対して送られるメッセージをグレーリストにする場合、このチェックボックスを選択してください。

除外リスト
このボタンをクリックすると、グレーリストで除外する送信者、受信者およびIPアドレスを指定するためのグレーリスト除外リストが開きます。

この時間の間に451によって初期の配信試みを延期する
配信の試みが、最初の試みの後にグレーリストにされる時間(分)を指定してください。その間に、同じサーバ/送信者/受信者の組み合わせ(グレーリストトリプレット)による配信の試みは、一時的な別のエラーコードで拒否されます。グレーリストの期間が経過すると、そのgreylistingデータベースレコードが期限切れにならない限り、そのトリプレットに対するグレーリスト遅延の動作は実行されません。

この期間以後未使用のグレーリストデータベースレコードを失効する
あるグレーリストトリプレットに対する最初のグレーリスト期間が経過した後は、そのトリプレットに関するそれ以降のメッセージの一致に対してGreylistingによる遅延は発生しません。しかし、このオプションで指定された期間(日数)、このトリプレットがメッセージの一致を受信しない場合、そのGreylistingデータベースレコードは期限切れになります。それ以降の同じトリプレットによる試みに対しては、新しいGreylistingレコードが作成され、再び最初のグレーリスト期間を経なければなりません。

詳細
Greylistingデータベースを開くにはこのボタンを選択してください。グレーリスト トリプレットのチェックあるいは編集を行うことができます。

SMTP応答(デフォルトはブランク)
テキストのカスタマイズした文字列を、このテキスト入力ボックスに準備する場合、MDaemonはSMTPレスポンス(デフォルト451 Greylisting enabled, try again in X minutes.でなく"451 <your custom text>")を戻します。例えば、グレーリストの説明にURLを含む文字列を準備する場合、これは便利です。

グレーリスト(MAIL & RCPT値のみ使用)の場合IPアドレスを含まない
グレーリストパラメータの1つとして送信サーバのIPアドレスを使用する場合は、このチェックボックスを選択してください。これはサーバプールによって引き起こされる潜在的な問題を解決しますが、Greylistingの効率を落とします。

SPF処理を渡す以後の接続をグレーリストにしない
このオプションを有効にすると、受信メッセージがトリプレットの送信者および受信者と一致するが送信サーバと一致しない場合でも、SPF処理によって送信サーバがトリプレットにリストされているものに対して有効な代替サーバであると確定されれば、そのメッセージは新しいGreylistingレコードが必要な接続としてではなく、そのトリプレットに一致しているものとしてその後の配信が行われます。

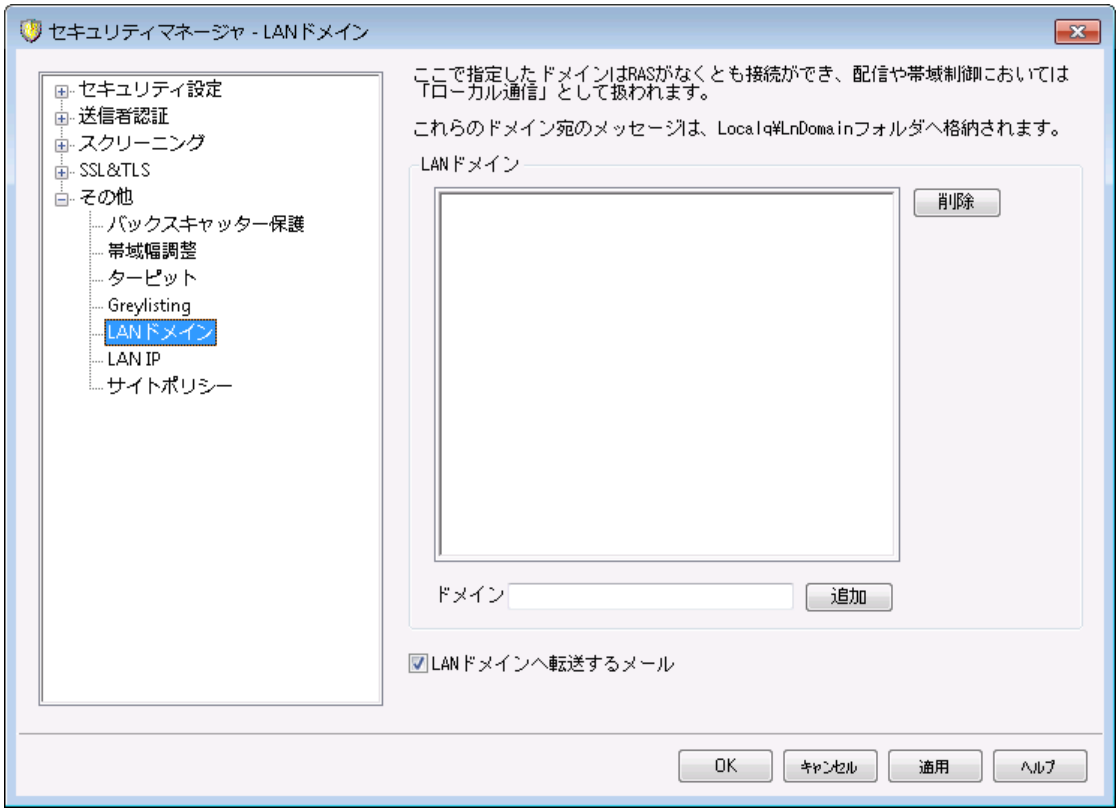
ローカルアドレス帳の送信者からのメールをグレーリストにしない
受信者のアドレス帳に含まれているアドレスからのメールをグレーリストから除外する場合は、このオプションを選択してください。

メーリングリストへメッセージをグレーリストにしない
メーリングリストからのメッセージをグレーリストから除外する場合は、このチェックボックスをクリックしてください。

認証セッションで送信されたメールをグレーリストにしない
認証セッション経由で受信されたすべてのメッセージをグレーリストから除外する場合はこのオプションを使用してください。

信頼されたIPからのメールをグレーリストにしない
信頼されたIPからのすべてのメッセージをグレーリストから除外する場合はこのオプションを使用してください。

4.1.5.5 LANドメイン



LAN ドメイン

ここで指定されたドメインはLAN(local area network)の一部であるとみなされます。これらに対するメッセージ配信にはダイアルアップやインターネット接続は必要ありません。

ドメイン
ドメイン名を入力し、追加ボタンを押すと、ドメイン名を追加します。

追加
ドメインオプションでドメインを追加した後、このボタンを押して追加します。

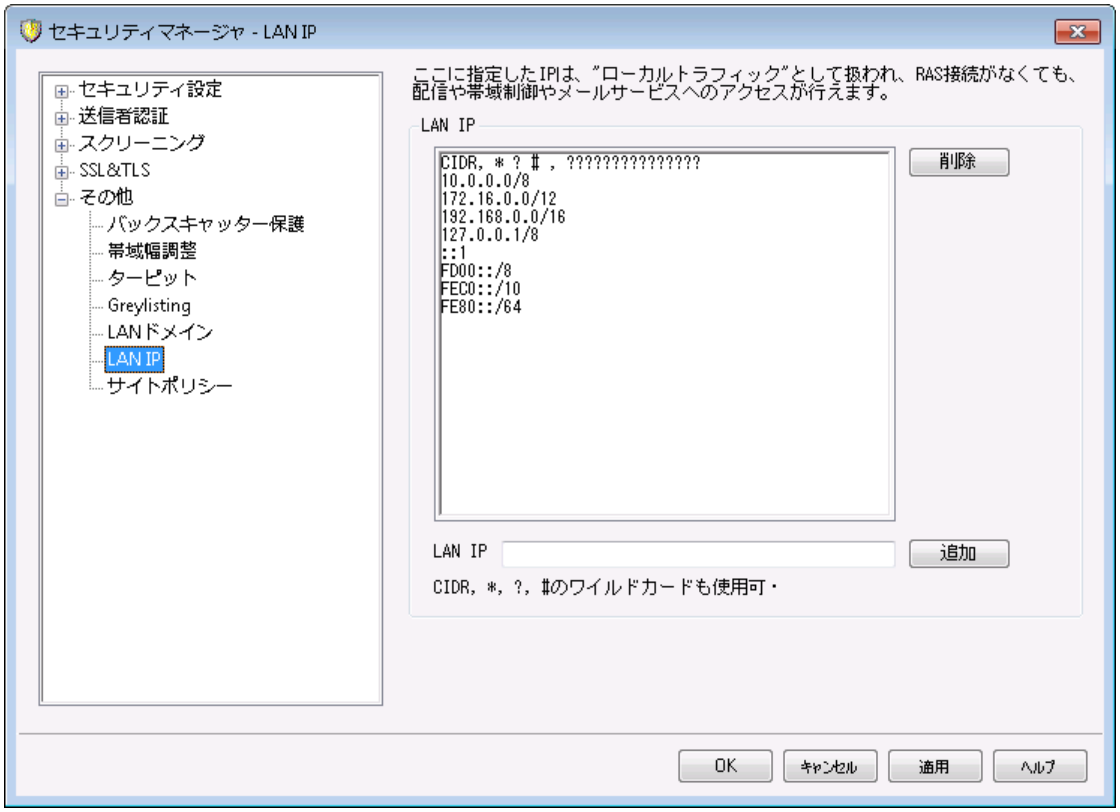
削除
ドメインを選択し、このボタンを押すと削除します。

LANドメインへメールを転送
このチェックを有効にすると、MDaemonがそれらのドメイン宛のメールを転送します。これにより、ドメインとのメール送受信のトラフィックをコントロールできます。

参照:

LAN IP 554

4.1.5.6 LAN IP



LAN IP

この画面はLANドメイン[553]と似て、LAN（Local area network）のIPアドレスの一覧を指定するのに使用します。これらのIPアドレスへの接続にはインターネット接続は必要なく、帯域幅調整においてはローカル接続として扱われます。さらに、様々なセキュリティの制限やスパムブロックからも除外されます。

削除
リストからIPアドレスを選択し、このボタンをクリックしてそのエントリを削除してください。

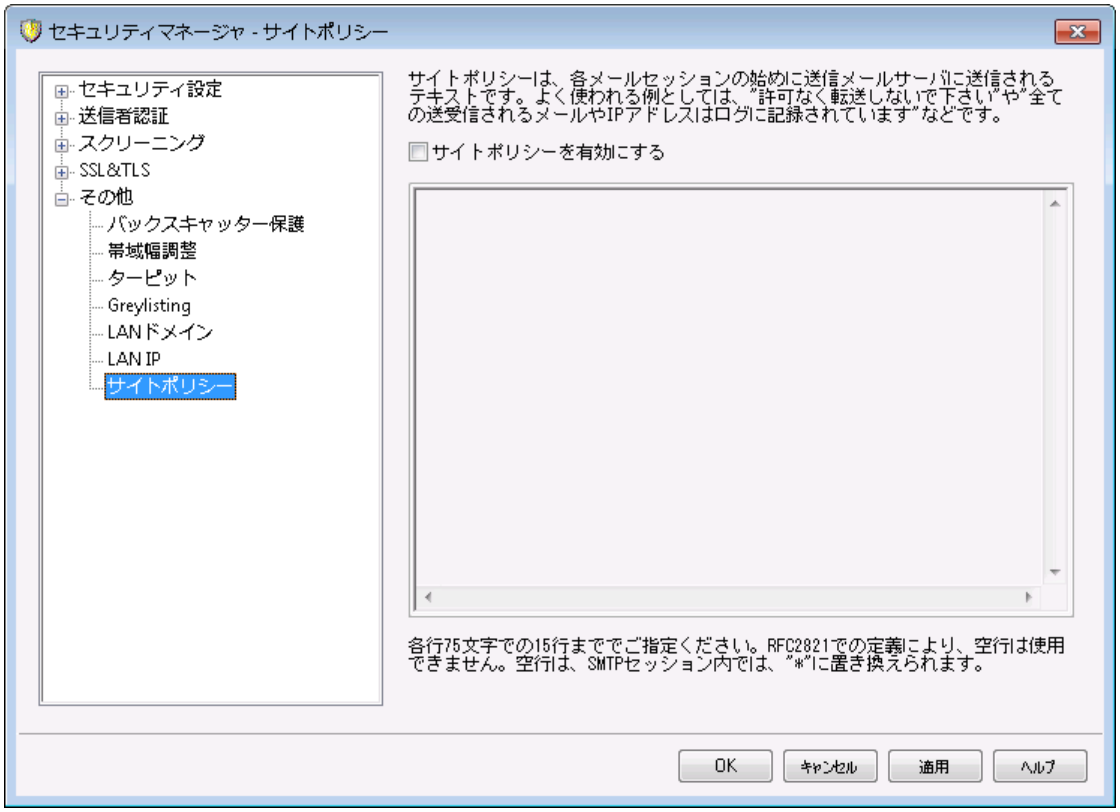
LAN IP
ローカルIPリストにIPアドレスを入力して、[追加]ボタンをクリックしてください。[127.0.*.*]のようなワイルドカードが使用できます。

追加
[LAN IP]フィールドに、IPアドレスを入力した後に、このボタンをクリックしてリストに追加してください。

参照:

LANドメイン[553]

4.1.5.7 サイトポリシー



SMTPサイト ポリシーステート メント の作 成
このダイアログを使 用して、サイト のセキュリティポリシーを作 成してください。このテキスト はMDaemon の¥appサブディレクト リにあるPOLICY.DATというファイルに保 存され、各 SMTPメールセッションの最 初にサーバへ送 信されます。一 般 的なサイト ポリシーの例 は"This server does not relay."または"Unauthorized use prohibited."です。各 ラインの先 頭に[220]あるいは[220-]などのプリペンドコードを追 加する必 要 はありません。MDaemonはそれらのプリペンドコード の有 無 にかかわらず処 理を行います。

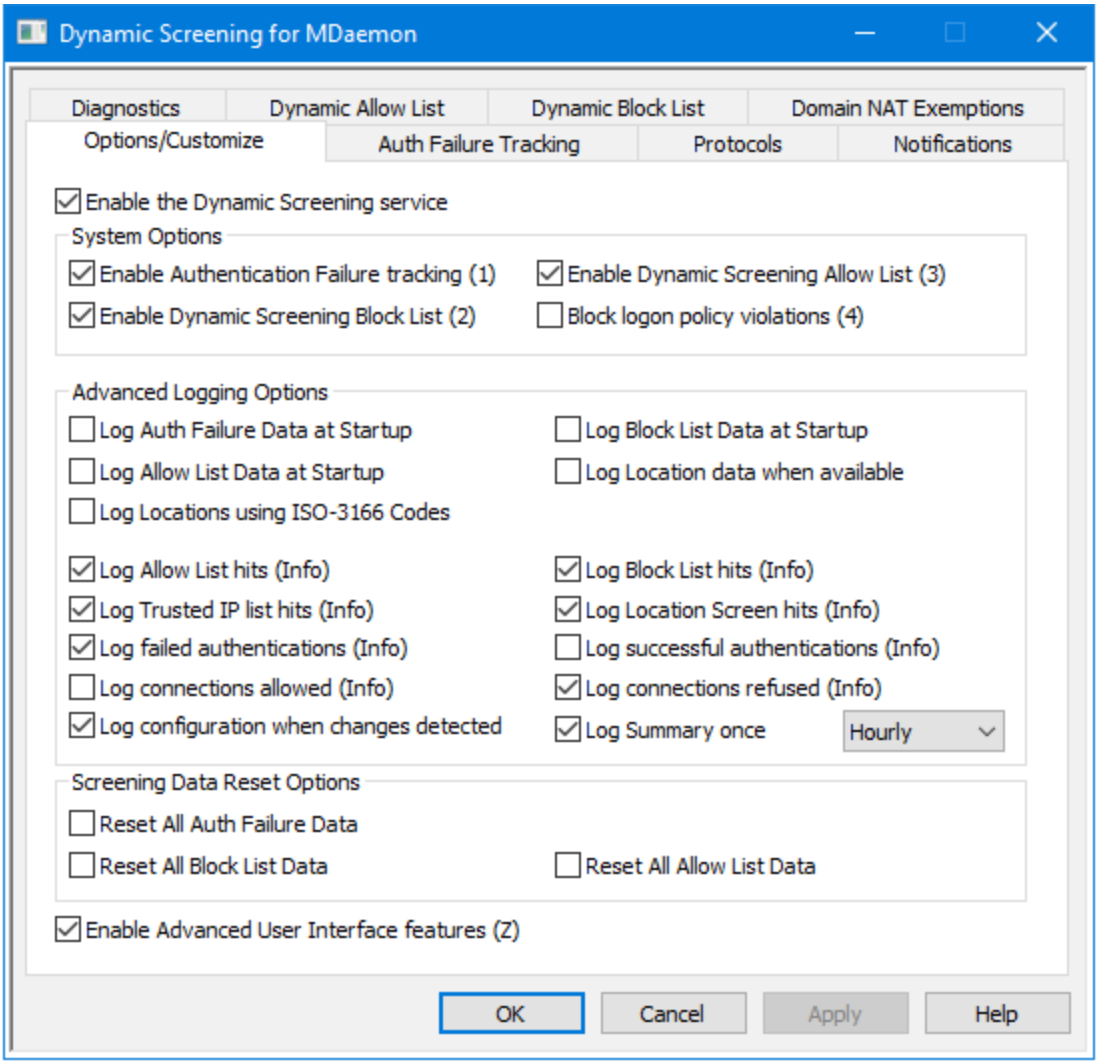
例えば、メールのリレーに関 する命 令を備えたPOLICY.DATファイルは、SMTP処 理の間 、次 のようになります。

```
220-Alt-N Technologies ESMTP MDaemon
220-This site does relay unauthorized email.
220-If you are not an authorized user of our server
220-then you must not relay mail through this site.
220
HELO example.com...
```

POLICY.DATファイルは、印刷可能なASCIIテキストのみで構成され、1行に512文字以内でなければなりません; ただし、1行 に75文 字 以 下 を使 用 することを強くお勧 めします。 このファイルの最 大 サイズは 5000バイト です。 MDaemonは5000バイト を超 えるファイルを表 示しません。

4.2 ダイナミックスクリーニング

4.2.1 オプション/カスタマイズ



ダイナミックスクリーニングを使用すると、MDaemonで受信接続から疑わしい動きを検出し必要な対応を行えるようになります。指定した時間内に指定回数を超える認証失敗があった際、IPアドレスのブロック559（またはIPアドレス範囲のブロック）が行えます。また、短時間で認証失敗回数が多かったアカウントについてはアカウントの凍結559が行えます。IPアドレスがブロックされたりアカウントが凍結される時間は無期限ではありません。IPアドレスのブロックは指定した分、時間、日数の間で行われます。凍結されたアカウントは指定した時間を経過した後か、管理者の操作によって再開できます。

ダイナミックスクリーニングサービスを有効にする
ダイナミックスクリーニングサービスを有効にするにはこのボックスをクリックします。MDaemonの管理画面のナビゲーションにあるサーバーセクションからも、このサービスの有効化・無効化が行えます。

システムオプション

認証失敗トラッキングを有効にする
このオプションを有効にすると、ダイナミックスクリーニングでプロトコル[562]タブで指定したプロトコルでの認証失敗と認証失敗トラッキング[559]タブのオプションに沿って実施された処理をログへ記録するようになります。このオプションはデフォルトで有効です。

ダイナミックスクリーニングブロックリスト
このオプションで ダイナミックスクリーニングのIPアドレスや範囲のブロックリスト機能が有効化されます。ブロックリストはダイナミックブロックリスト[571]タブで管理できます。ブロックリストオプションはデフォルトで有効です。

ダイナミックスクリーニング許可リスト
このオプションで ダイナミックスクリーニングの機能の1つである、IPアドレスや範囲を許可リストへ追加し ダイナミックスクリーニングから除外する ダイナミック許可リスト[569] 機能が有効化されます。許可リストオプションはデフォルトで有効です。

ログオンポリシーに違反している場合にブロック
デフォルトでMDaemonはアカウントがアドレスのメールボックス部分ではなくメールアドレスをログインに使用するよう設定されています。(例:「user1」ではなく「user1@example.com」を使用する必要があります) これはシステム[450]ページの「サービスは完全なメールアドレスでの認証を必要とする」オプションによって管理されています。このオプションが有効になっていて、且つ、「ログオンポリシーに違反している場合にブロック」を有効にする事で、メールアドレスを使用せずにログオンしてきたIPアドレスをブロックできます。このオプションはデフォルトで無効に設定されています。

詳細ログオプション

開始時に認証失敗データを記録
このオプションを有効化すると、起動時にダイナミックスクリーニングによる全ての 認証失敗データ[559]を記録します。これはデフォルトで無効になっています。

開始時にブロックリストデータを記録
このオプションを有効化すると、起動時にダイナミックスクリーニングによる全ての ダイナミックブロックリスト[571]を記録します。これはデフォルトで無効になっています。

開始時に許可リストデータを記録
このオプションを有効化すると、起動時にダイナミックスクリーニングによる全ての ダイナミック許可リスト[569]を記録します。これはデフォルトで無効になっています。

ロケーション情報が利用できる場合に記録
接続毎のロケーション情報が使用できる場合にログへ記録する場合はこのオプションを有効にします。

ISO-3166コードでロケーションを記録
名称の代わりにISO-3166の2文字の国コードを使用する場合はこのオプションを有効にします。

許可リストとの一致を全て記録
このオプションを有効化すると、ダイナミック許可リスト[569]へ登録されているアドレスからの受信接続が発生する毎にダイナミックスクリーニングへエントリを追加します。

ブロックリストとの一致を全て記録
このオプションを有効化すると、ダイナミックブロックリスト[571]へ登録されているアドレスからの受信接続が発生する毎にダイナミックスクリーニングへエントリを追加します。

信頼するIPとの一致を全て記録
このオプションを有効化すると、信頼するIP[473]からの受信接続を、都度ダイナミックスクリーニングログへ記録します。

国別スクリーンとの一致を全て記録
このオプションを有効化すると、国別スクリーニング[520]によって拒否された受信接続を、都度ダイナミックスクリーニングログへ記録します。

認証失敗を全て記録
このオプションを有効化すると、認証に失敗した受信接続を、都度ダイナミックスクリーニングログへ記録します。

認証成功を全て記録
このオプションを有効化すると、認証に成功した受信接続を、都度ダイナミックスクリーニングログへ記録します。 これはデフォルトで無効になっています。

許可された接続を全て記録
このオプションを有効化すると、ダイナミックスクリーニングを通過してその後の処理を許可した接続全てをログへ記録します。 これはデフォルトで無効になっています。

拒否した接続を全て記録
このオプションを有効化すると、ダイナミックスクリーニングで拒否した受信接続全てをログへ記録します。

変更点が検出された際設定を記録
このオプションを有効化すると、(手動でINIファイルを編集した際など)外部ソースでの設定変更が検出された際、ダイナミックスクリーニング設定をログへ記録します。通常の変更は情報ログレベルで記録されます。

サマリ記録間隔[日別|時間別|分別]
ダイナミックスクリーニング統計へ、ダイナミックスクリーニングログサマリを追加します。日毎、時間毎、分毎に記録できます。デフォルトではサマリが時間毎に記録されます。

スクリーニングデータリセットオプション

全ての認証データをリセット
ダイナミックスクリーニングの認証データ全てをクリアするにはこのチェックボックスをクリックします。**適用**又は**OK**をクリックすると初期化が行われます。

全てのブロックリストデータをリセット
ダイナミックスクリーニングのブロックリストデータ全てをクリアするにはこのチェックボックスをクリックします。**適用**又は**OK**をクリックすると初期化が行われます。

全ての許可リストデータをリセット
ダイナミックスクリーニングの許可リストデータ全てをクリアするにはこのチェックボックスをクリックします。**適用**又は**OK**をクリックすると初期化が行われます。

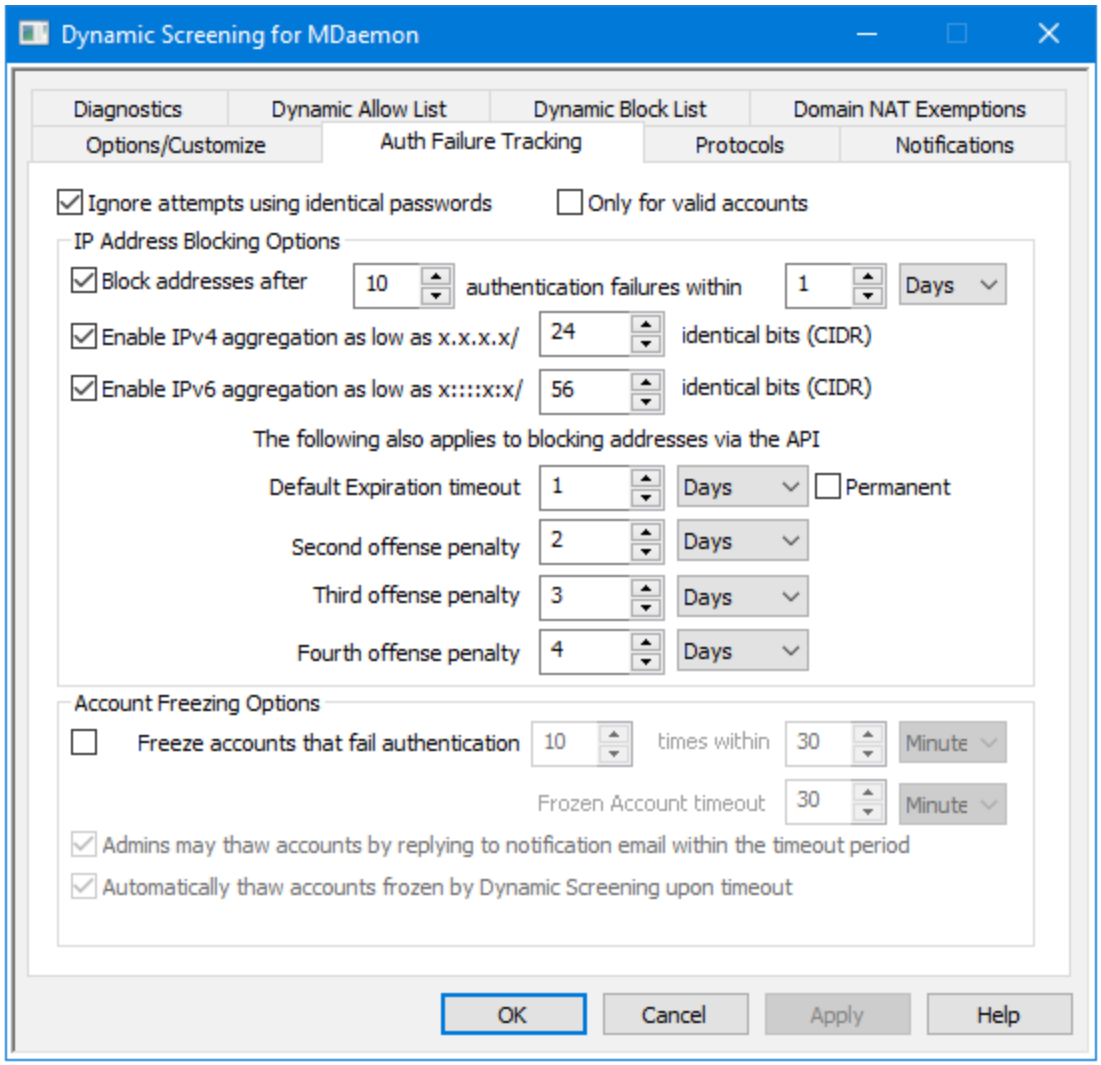
詳細な管理画面を有効にする

このボックスをチェックして画面を閉じるか再起動すると、MDaemonの設定画面へ詳細ダイナミックスクリーニング機能を追加する事ができます。このボックスをチェックしてMDaemonの管理画面を再度開くと、ダイナミックスクリーニング機能へ詳細な管理画面が複数追加されます。除外ドメインNAT[573]画面がダイナミックスクリーニングダイアログへ追加され、対象IPアドレスでパスワード認証に失敗したユーザーをダイナミックスクリーニングから除外する事ができます。また、ツールバーのダイナミックスクリーニングセクションにもショートカットが追加され、管理画面のサーバーセクションからは、ダイナミックスクリーニングサービスを無効にするのではなく一時停止し、設定中にクライアントがサービスへアクセスする事のないよう設定する事ができます。

参照:

認証失敗トラッキング[559]
ダイナミック許可リスト[569]
ダイナミックブロックリスト[571]
除外ドメインNAT[573]
プロトコル[562]
国別スクリーニング[520]
SMTPスクリーン[514]

4.2.2 認証失敗トラッキング



毎回同じパスワードが使われた場合は除く

このオプションは以下のIPアドレスブロックオプションとアカウント凍結オプションに対して適用されます。デフォルトで、認証失敗は、同じパスワードを使用している場合は無視されます。IPアドレスのブロックやアカウントの凍結が行われるまでの認証失敗回数にはカウントされません。複数回同じIPアドレスからの認証失敗は、例えばユーザーのメールパスワードが変更されたり有効期限が切れたりした際などに、古いパスワードで認証を行おうとして発生する場合があります。

存在するアカウントにだけ適用する
このオプションを使用すると、正しいアカウントへサインインしようとした場合のみ、重複したパスワード認証を除外できるようになります。つまり、例えば、ユーザーが自分のパスワードをメーラーで変更し、別のパソコンで古いパスワードを使ったままメーラーが起動していた場合、ユーザー名が正規のものであるため、古いクライアントのサインインは無視されます。ボットは通常類似したパスワードとランダムのユーザー名でアクセスを試みますが、この場合、同様の恩恵は受けられず、認証失敗検出後すぐに接続がブロックされます。

IPアドレスブロックオプション

アドレスのブロック [xx] 回の認証失敗が、この期間で [xx] [分 | 時 | 日]
指定した時間内に上限を超える回数の認証失敗があった場合、対象IPアドレスを一時的にブロックするにはこのチェックボックスをクリックします。分、時間、日数と期間内に許可する認証失敗回数を指定します。

x.x.x.x/といったIPv4の集約の有効化 [xx] これらのビット数単位 (CIDR)
これは認証失敗時に1つのIPアドレスではなく互いに近いIPアドレスからの通信だった場合、IPv4アドレスの範囲をブロックするためのオプションです。

x::::x:x/といったIPv6の集約の有効化 [xx] これらのビット数単位 (CIDR)
これは認証失敗時に1つのIPアドレスではなく互いに近いIPアドレスからの通信だった場合、IPv6アドレスの範囲をブロックするためのオプションです。

複数攻撃のペナルティ

認証で指定した回数の失敗があった場合にダイナミックスクリーニングにブロックされるIPやIPアドレス範囲の総数です。デフォルトでIPアドレスがブロックされる時間はブロックされる回数が増える毎に増加します。デフォルトで、認証失敗数が上限を超えると、IPアドレスは一日ブロックされます。更に次の日また上限を超えると、次は2回目の攻撃のペナルティがデフォルトの有効期限へ追加され、次は3回目の攻撃のペナルティが追加されます。ペナルティの長さは4回目の攻撃へのペナルティが最大です。

デフォルトの有効期限までの時間
上記で指定した時間の間に認証失敗回数の上限に達した場合、対象IPやIP範囲からMDaemonへの接続をブロックする時間をここで指定します。デフォルトでは一日です。

2回目の攻撃へのペナルティ
ダイナミックスクリーニングでIPアドレスやIP範囲が2回目にブロックされた際、ここで指定した時間がデフォルトの時間へ加算されます。

3回目の攻撃へのペナルティ
ダイナミックスクリーニングでIPアドレスやIP範囲が3回目にブロックされた際、ここで指定した時間がデフォルトの時間へ加算されます。

4回目の攻撃へのペナルティ
ダイナミックスクリーニングでIPアドレスやIP範囲が4回目にブロックされた際、ここで指定した時間がデフォルトの時間へ加算されます。

無制限
認証失敗を指定回数以上繰り返したIPアドレスを、一時的ではなくずっとブロックする場合はこのオプションを有効化します。

アカウント凍結オプション

認証の失敗が続くアカウントを凍結 [xx] 回、期間は [xx] [分 | 時 | 日]
指定時間内に指定した回数の認証失敗があった場合にアカウントの状態 650 を凍結にする場合はこのオプションを使用します。MDaemonは凍結アカウント宛のメールは受信するものの、アカウントがサインインしたりメールの送受信を行う事は(アカウントの状態を有効にするといった)凍結解除が行われるまでできません。このオプションはデフォルトで有効です。

凍結アカウントのタイムアウト
下記の、タイムアウトの時間経過したら自動的にダイナミックスクリーンでのアカウント凍結を解除する、を有効にしていた場合、アカウントを凍結しておく時間をここで指定します。

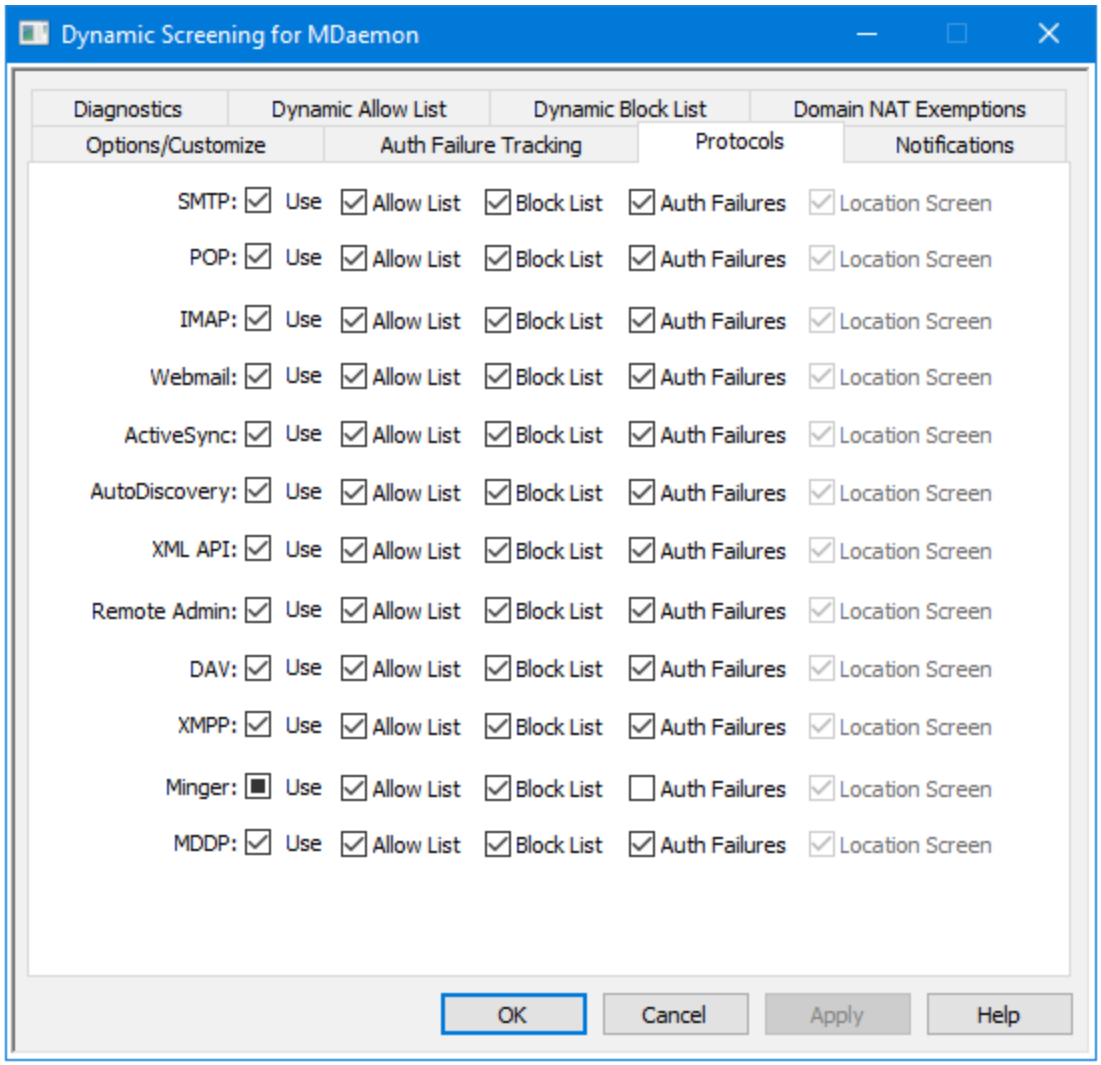
管理者はタイムアウトまでに通知メールへ返信する事で凍結解除が行えます。
アカウントがダイナミックスクリーニングで凍結されると、デフォルトで管理者は通知メールを受信します。このオプションを有効化していると、管理者はこのメールへ返信する事で、アカウントの凍結を解除できるようになります。このオプションはデフォルトで有効で、通知 564タブの凍結アカウントレポートを有効にしておく必要があります。

タイムアウトの時間経過したら自動的にダイナミックスクリーンでのアカウント凍結を解除する
このオプションを有効化すると、凍結されたアカウントが指定時間経過後に自動的に凍結解除されます。このオプションはデフォルトで無効です。

参照:

オプション/設定 556
ダイナミック許可リスト 569
ダイナミックブロックリスト 571
通知 564

4.2.3 プロトコル

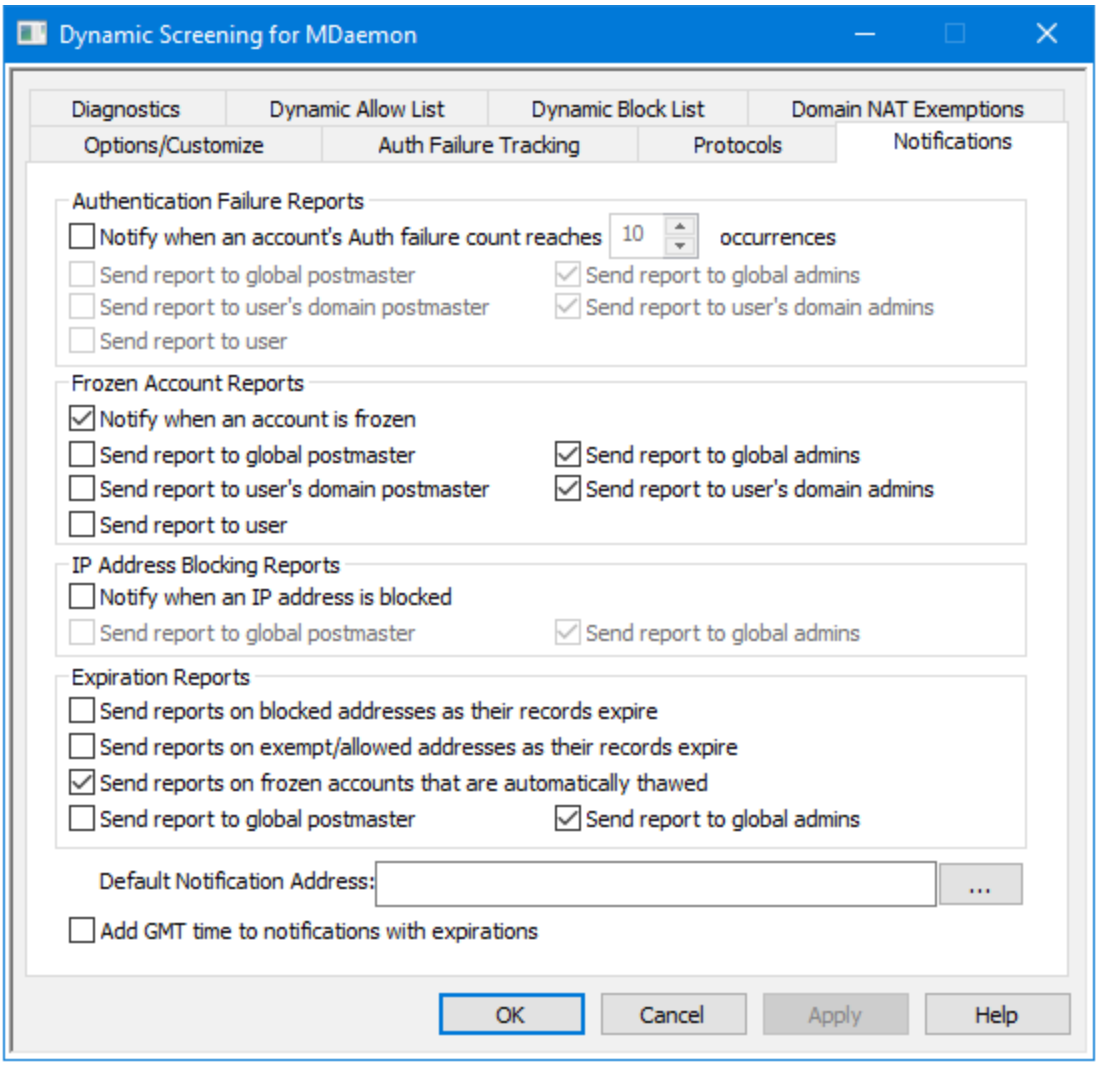


デフォルトでは、ダイナミックスクリーニングサービスはSMTP、POP、IMAP、Webmail、ActiveSync、AutoDiscovery[68]、管理API、MDaemonリモート管理。WebDAVとCalDAV、XMPP、およびMingerプロトコルに適用されます。プロトコルタブでは、インバウンドセッションにおけるダイナミック除外リスト[569]やダイナミックブロックリスト[571]のチェックや国別スクリーニング[520]が適用された認証失敗のログ[559]の対象とするプロトコルを選択できます。デフォルトでは、このダイアログのすべてのオプションはMinger認証失敗を除いて有効になっています。

参照:

認証失敗のログ[559]
ダイナミック許可リスト[569]
ダイナミックブロックリスト[571]

4.2.4 通知



認証失敗レポート

アカウントに認証失敗回数が次に達したら通知 [xx]回
このオプションを有効にすると、MDaemonは指定回数以上認証に失敗したアカウントについて、postmaster又は選択した宛先に通知を送ります。選択したアドレスが見つからない場合は、後述のデフォルト通知アドレスへ通知を送ります。アドレスが指定されていない場合は、通知は送信されません。このオプションはデフォルトで有効で、10回がデフォルト値となっています。

グローバルpostmasterへレポート送付
レポートをグローバルpostmaster[757]へ送信するにはこのオプションを有効にします。これはデフォルトで有効です。

グローバル管理者へレポート送付
レポートをグローバル管理者[690]へ送信するにはこのオプションを有効にします。

ドメインのpostmasterへレポート送付
認証に失敗したアカウントに関するレポートを[ドメインpostmaster](757)へ送信するにはこのオプションを有効にします。

ドメイン管理者へレポート送付
認証に失敗したアカウントに関するレポートを[ドメイン管理者](690)へ送信するにはこのオプションを有効にします。

ユーザーへレポート送付
認証に失敗したアカウントにのみレポートを送付するにはこのオプションを有効にします。

凍結アカウントレポート

アカウントが凍結された時に通知
このオプションを有効にすると、MDaemonは、[指定回数以上の認証失敗](559)によって凍結されたアカウントについて、postmaster又は選択した宛先に通知を送ります。選択したアドレスが見つからない場合は、後述のデフォルト通知アドレスへ通知を送ります。アドレスが指定されていない場合は、通知は送信されません。このオプションはデフォルトで有効です。

グローバルpostmasterへレポート送付
レポートを[グローバルpostmaster](757)へ送信するにはこのオプションを有効にします。これはデフォルトで有効です。

グローバル管理者へレポート送付
レポートを[グローバル管理者](690)へ送信するにはこのオプションを有効にします。

ドメインのpostmasterへレポート送付
凍結アカウントに関するレポートを[ドメインpostmaster](757)へ送信するにはこのオプションを有効にします。

ドメイン管理者へレポート送付
凍結アカウントに関するレポートを[ドメイン管理者](690)へ送信するにはこのオプションを有効にします。

ユーザーへレポート送付
凍結されたアカウントにのみレポートを送付するにはこのオプションを有効にします。

IPアドレスブロックレポート

IPアドレスをブロックした時に通知
このオプションを有効にすると、MDaemonは、ダイナミックスクリーンによってブロックされたアカウントについて、postmaster又は選択した宛先に通知を送ります。選択したアドレスが見つからない場合は、後述のデフォルト通知アドレスへ通知を送ります。アドレスが指定されていない場合は、通知は送信されません。このオプションはデフォルトで有効です。

グローバルpostmasterへレポート送付
レポートを[グローバルpostmaster](757)へ送信するにはこのオプションを有効にします。これはデフォルトで有効です。

グローバル管理者へレポート送付
レポートを グローバル管理者 690 へ送信するにはこのオプションを有効にします。

有効期限切れレポート

レコードが期限切れとなり、ブロックしたアドレスのレポート送付
このオプションを使うと、ブロックされていたIPアドレスが期限を迎え ダイナミックブロックリスト 571 の対象外になった際、指定したアドレスへレポートを送信します。これはデフォルトで有効です。

レコードが期限切れになった、除外/許可リストアドレスのレポート送付
このオプションを使うと、許可リストのIPアドレスが期限を迎え ダイナミック許可リスト 569 の対象外になった際、指定したアドレスへレポートを送信します。これはデフォルトで有効です。

自動的に凍結が解除されたアカウントのレポート送付
このオプションを使うと、凍結アカウントが、凍結アカウントのタイムアウトで指定した時間を経過し、自動での凍結解除 559 となった際、指定したアドレスへレポートを送信します。これはデフォルトで有効です。

グローバルpostmasterへレポート送付
レポートを グローバルpostmaster 757 へ送信するにはこのオプションを有効にします。これはデフォルトで有効です。

グローバル管理者へレポート送付
レポートを グローバル管理者 690 へ送信するにはこのオプションを有効にします。

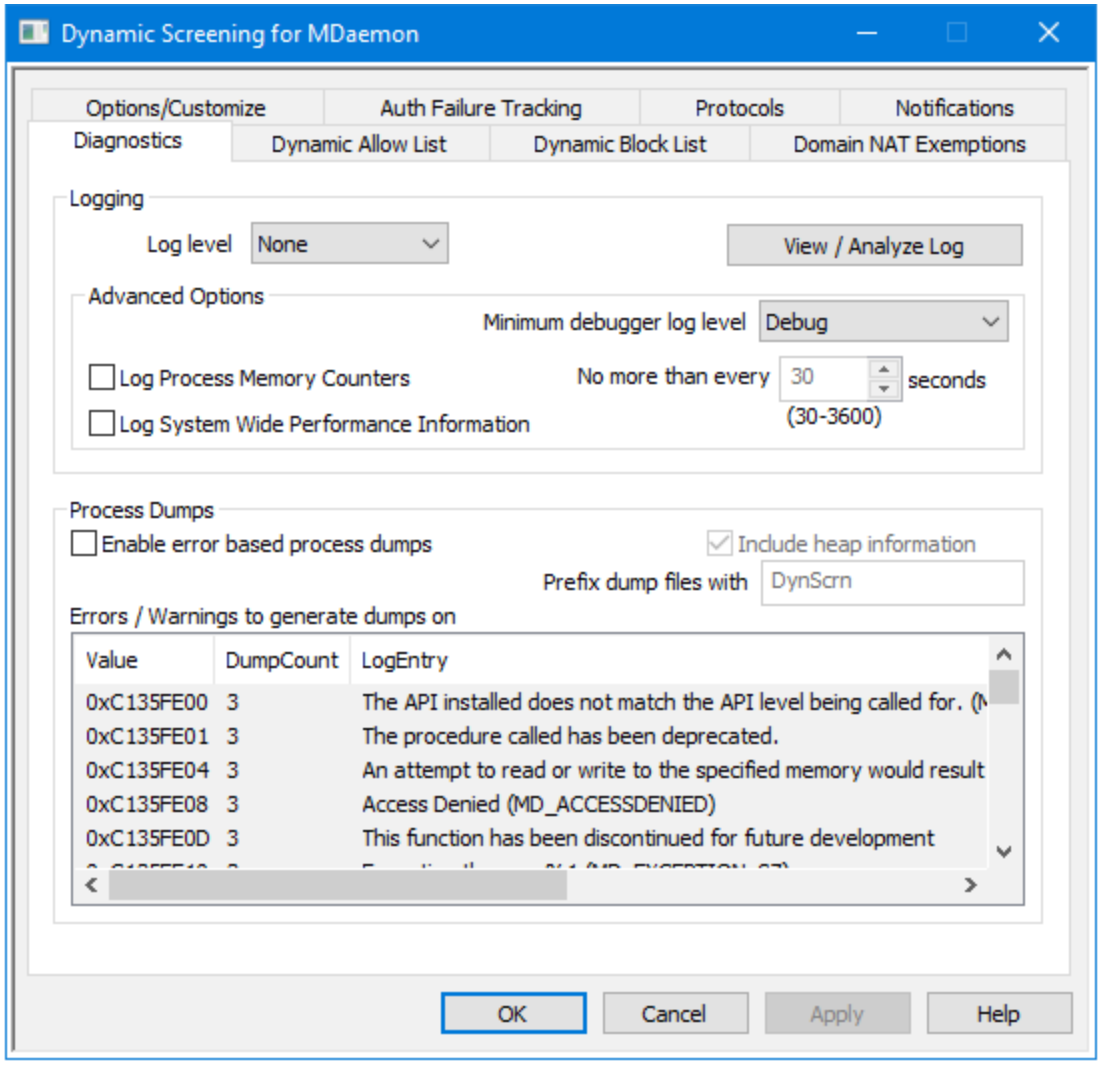
デフォルトの通知先
このアドレスは、通知レポートの送付先アドレスが指定されていなかったり、指定したアドレスが存在しなかった場合などに通知レポートが送信されるアドレスです。指定アドレスが見つからず、デフォルト通知先アドレスが指定されていなかった場合、レポートは送信されません。

期限切れに伴う通知にGMT標準時間を追加する
デフォルトで通知レポートにはサーバーのローカル時間を元にした有効期限が記載されています。このオプションを有効にすると、GMT時間を記載するようになります。これは管理者が異なるタイムゾーンの地域にいる場合に便利です。

参照:

オプション/設定 556
認証失敗トラッキング 559

4.2.5 診断



ここでは、ダイナミックスクリーニングの問題分析や技術サポート等で依頼された場合などを除き、ほとんど調整の必要がない詳細設定を行えます。

ロギング

ログレベル

ログデータ量に応じた、6つのレベルのログに対応しています。

デバッグ 最も詳細なログで、記録できる全ての情報が含まれており、問題の診断にのみ使用されます。

情報 通常のログで、一般的な操作が詳細なしで記録されます。これはデフォルトのログレベルです。

警告 警告、エラー、クリティカルエラー、起動と終了がログに記録されます。

エラー　エラー、クリティカルエラー、起動と終了がログに記録されます。

クリティカル　クリティカルエラー、起動と終了がログに記録されます。

なし　起動と終了だけがログに記録されます。

ログの表示/分析
このボタンをクリックすると、MDaemon詳細システムログビューアが起動します。デフォルトでログは"..\MDaemon\Logs\"へ格納されます。

詳細オプション

最小デバッガーログレベル
デバッガー向けの最小ログレベルを指定します。使用できるログレベルは下記の通りです。

プロセスメモリカウンターをログへ残す
プロセス毎のメモリ、ハンドラ、スレッド情報をログへ残す場合はこのオプションを有効化します。潜在的なリードやアロケーション問題を特定するのに役立ちます。ログエントリは前回のログから変更があって初めて生成されます。

システム単位でのパフォーマンス情報をログへ残す
システムレベルのパフォーマンス情報をログへ残す場合にはこのオプションを有効化します。潜在的なリードやアロケーション問題を特定するのに役立ちます。ログエントリは前回のログから変更があって初めて生成されます。

[xx]秒毎にログを記録する
プロセスやパフォーマンス情報がログへ記録される頻度をこのオプションで指定します。

プロセスダンプ

エラーを元にしたプロセスダンプを有効化
下記で指定した特定の警告やエラー発生時プロセスダンプを生成するにはこのオプションを有効化します。

ダンプファイルへヒープ情報を含む
デフォルトで、ヒープ情報はプロセスダンプへ含まれます。含まない場合はチェックボックスをクリアしてください。

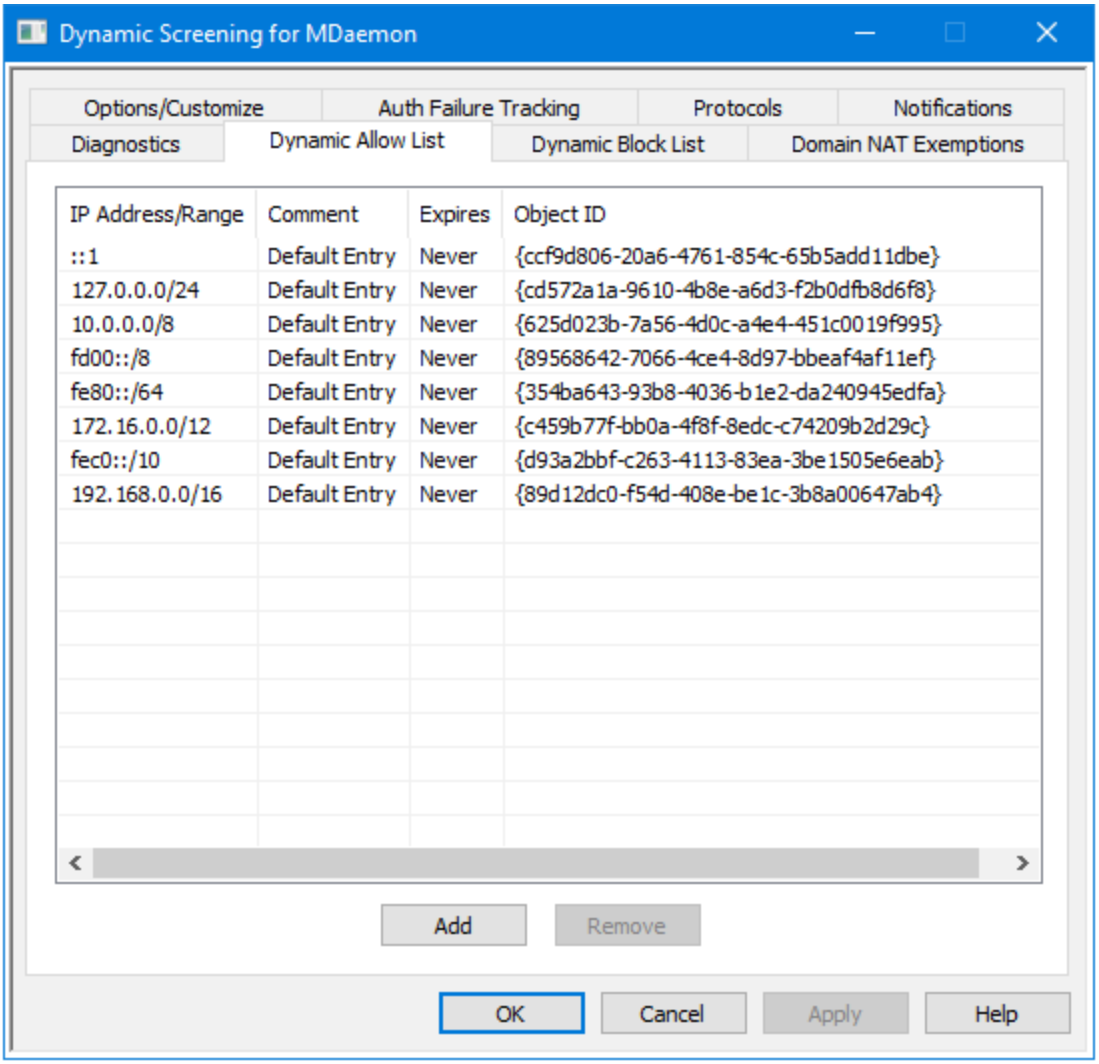
ダンプファイルの頭文字
プロセスダンプのファイル名はここで指定した文字から始まります。

ダンプファイルを生成するエラー/警告
右クリックして、エントリを追加/編集/削除...オプションをクリックし、プロセスダンプの生成のトリガーとするエラーや警告の管理を行います。各エントリではディアクティベートまでのプロセスダンプの数を指定する事ができます。

参照:

ダイナミックスクリーニング » オプション/カスタマイズ 556

4.2.6 ダイナミック許可リスト

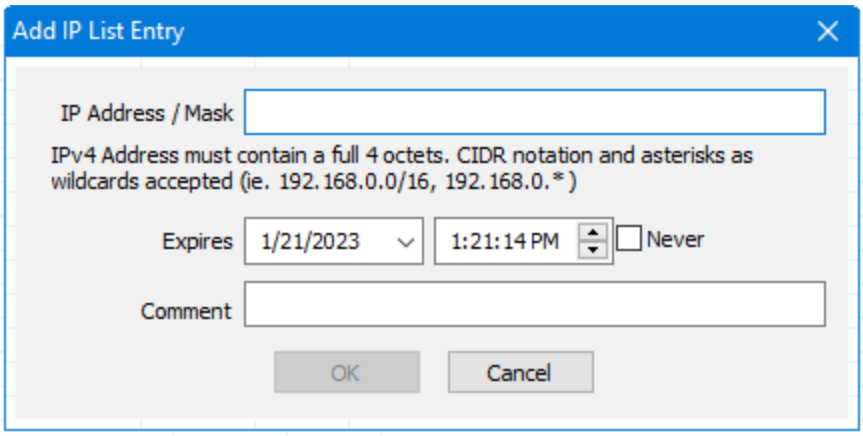


ダイナミック許可リストはMDaemonへ接続しようとした際ダイナミックスクリーニングサービスのブロック対象から除外するIPアドレスやアドレス範囲の一覧です。アドレスは追加ボタンから手動で追加する事ができます。各エントリはIPアドレス又は範囲とエントリの期限日時(「なし」を設定すると無期限となります)、エントリに追加するコメント、オブジェクトIDから構成されています。ダイナミック除外リストはSMTPスクリーン 514, ロケーションスクリーニング 520, ターピッティング 548でも使用されます。

ダイナミック許可リストへエントリを追加

一覧へエントリを追加するには:

1. 追加をクリックします。IPリストのエントリ用ダイアログが起動します。



2. IPアドレスかIPアドレス範囲を入力します。
3. エントリの有効期限日時を選択するか、「なし」をクリックします。
4. エントリ用のコメントを入力します。（オプションです）。
5. **OK**をクリックします。

一覧からエントリを削除

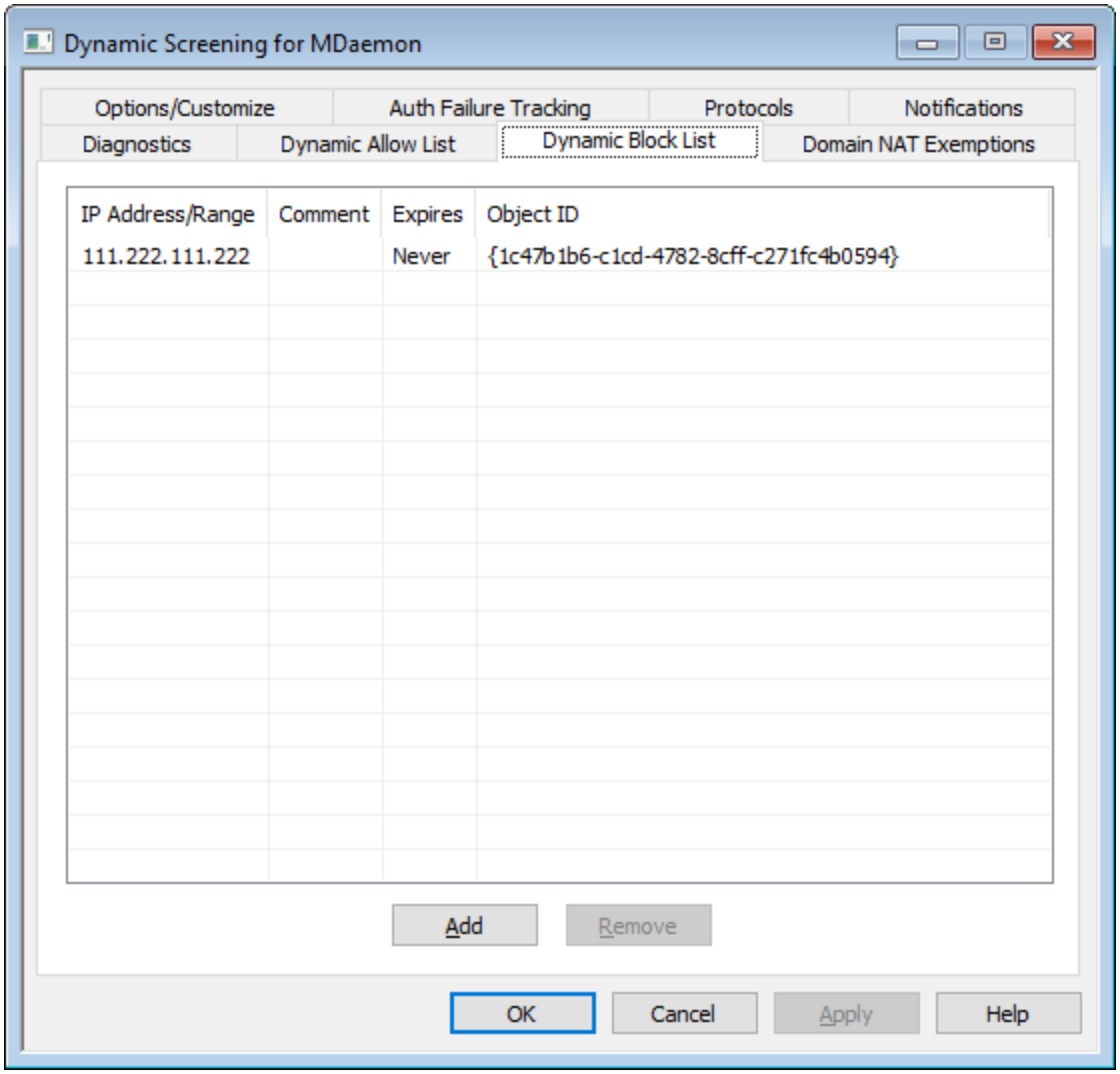
一覧からエントリを削除するには:

1. 削除したいエントリを一覧から選択します（Ctrl+クリックで複数エントリを選択できます。）
2. **削除**をクリックします。

参照:

オプション/設定 556
認証失敗トラッキング 559
ダイナミックブロックリスト 571
プロトコル 562

4.2.7 ダイナミックブロックリスト

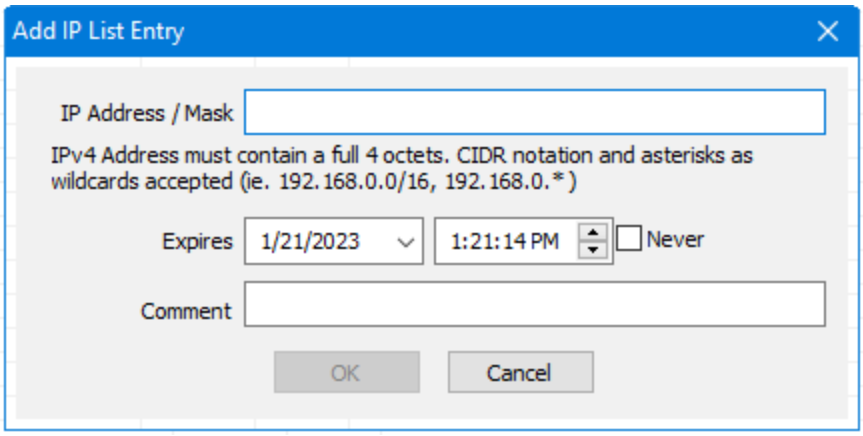


ダイナミックブロックリストではMDaemonへ接続しようとした際ダイナミックスクリーニングサービスでブロックされたIPアドレスやアドレス範囲の一覧を確認できます。アドレスは認証失敗トラッキング[559]やSMTPスクリーン[514]オプションで自動追加したり、追加ボタンから手動で追加する事ができます。各エントリはIPアドレス又は範囲とエントリの期限日時(「なし」を設定すると無期限となります)、エントリに追加するコメント、オブジェクトIDから構成されています。

一覧へエントリを追加

一覧へエントリを追加するには:

1. 追加をクリックします。IPリストのエントリ用ダイアログが起動します。



2. IPアドレスかIPアドレス範囲を入力します。
3. エントリの有効期限日時を選択するか、「なし」をクリックします。
4. エントリ用のコメントを入力します。（オプションです）。
5. **OK**をクリックします。

一覧からエントリを削除

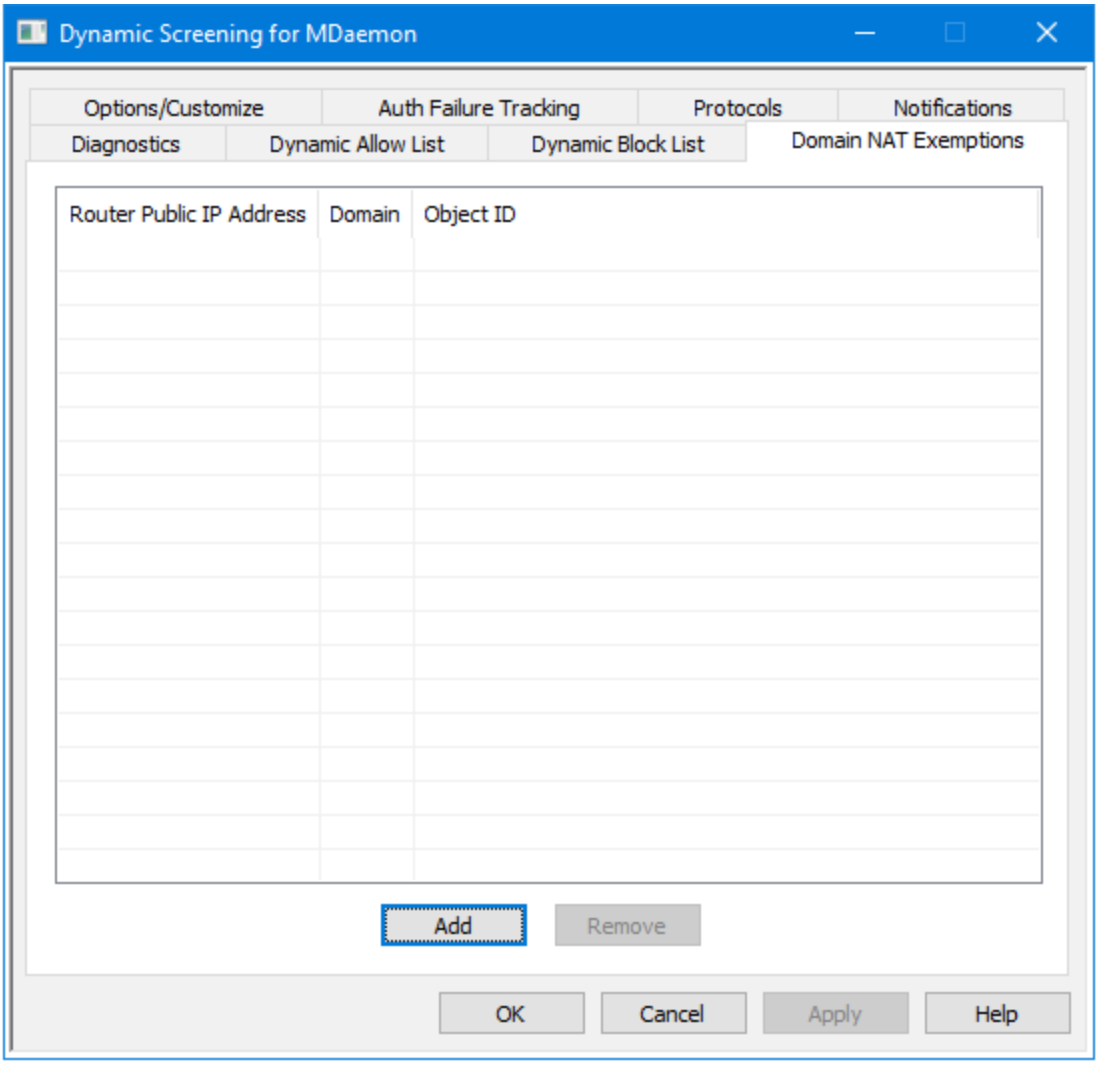
一覧からエントリを削除するには:

1. 削除したいエントリを一覧から選択します（Ctrl+クリックで複数エントリを選択できます。）
2. **削除**をクリックします。

参照:

オプション/設定 556
認証失敗トラッキング 559
ダイナミック許可リスト 569
プロトコル 562

4.2.8 除外ドメインNAT



この画面はダイナミックスクリーニングの[オプション/設定](#) 556で、*詳細な管理画面を有効にする*、を有効化すると利用できるようになります。

この機能はローカルエリアネットワーク(LAN)でネットワークアドレス変換(NAT)を使い、単一のパブリックIPアドレスを使用しているユーザーのグループに対して適用できます。LANのパブリックIPアドレスとMDaemonドメインを追加する事で、特定のユーザーがパスワードの入力ミスで認証に失敗した際、ダイナミックスクリーニングによりIPアドレスがブロックされてしまう事を防ぎます。この機能を使用しなかった場合、正規のユーザーがメーラーの設定を正しく行っていなかった場合等に、LAN IPがブロックされ、全ユーザーがメールへアクセスできなくなる可能性があります。例えば、ユーザーのパスワード変更を行った際、ユーザーがメールクライアントの設定を更新し忘れた場合などにも、同様の可能性があります。

この一覧にあるIPアドレスは、正規ではないアカウントでログインしようとしたり、MDaemonドメインではないアドレスでログインしようとした、といった、他の理由でブロックされる可能性があります。対象のIPアドレスを完全に除外する場合は、[ダイナミック許可リスト](#) 569を使用してください。

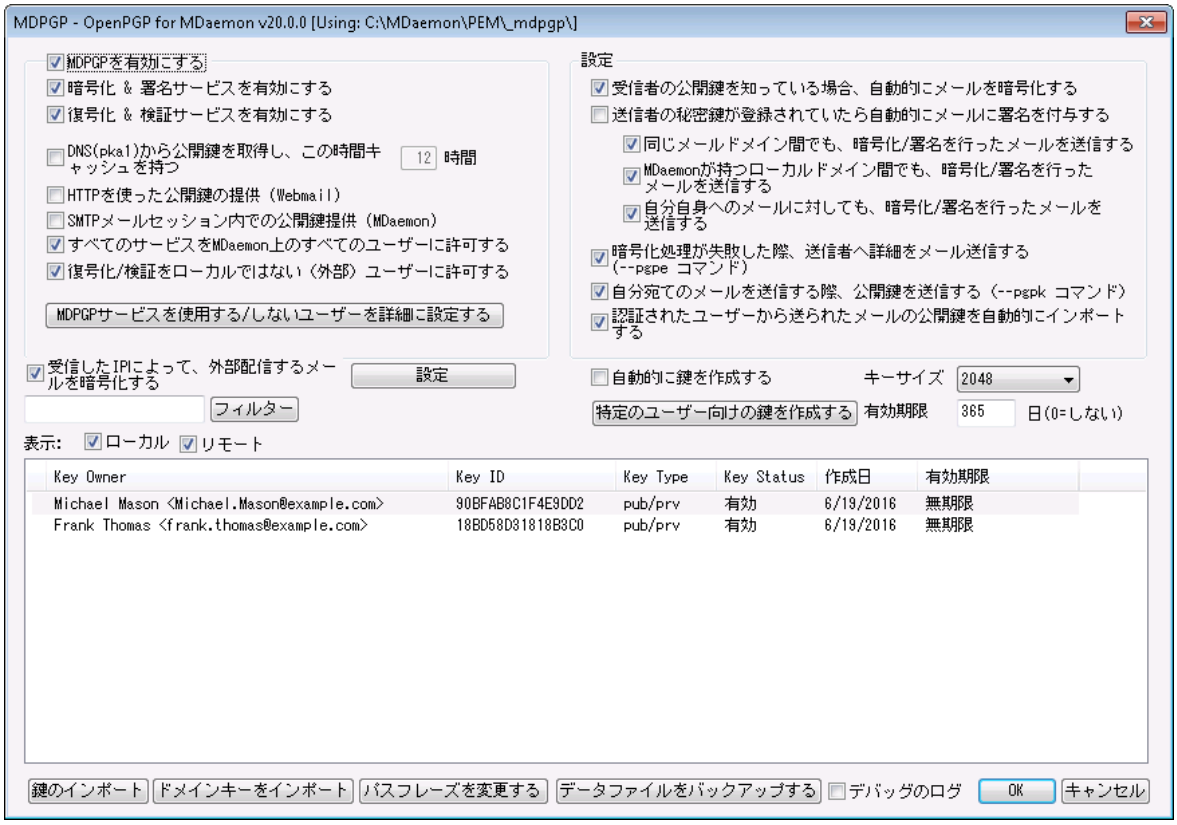
除外ドメインNATの追加

追加をクリックし、LANのルーターパブリックIPアドレスを入力し、対象IPからログインするユーザーが所属しているMDaemonドメインを選択します。OKをクリックしてください。

参照:

オプション/設定 556

4.3 MDPGP



OpenPGPは暗号化されたデータをやり取りするための業界標準プロトコルで、ユーザーが暗号化メールを送受信できるよう、数々のメールクライアント用OpenPGPプラグインが存在しています。MDPGPはMDaemonに搭載されたOpenPGPコンポネントで、ユーザーはメールクライアント用プラグインを使っていなくとも、暗号化、復元、簡単な鍵管理が行えます。

MDPGPは公開鍵認証システムを使ったメールの暗号化と復元を行います。MDPGPでメールを暗号化すると、MDPGPは送信先から以前取得したキー(送信先の「公開鍵」)を使ってメールの暗号化を行い、MDPGPへインポートします。反対に先方から暗号化されたメールが到着する場合、送信者はあなたのキーを使ってメールを暗号化します。送信者がメールの暗号化を行うのに、公開鍵を送っておく事は当然必要です。メールの暗号化には、自分専用の公開鍵を使う必要があり、そうする事で、自分が所持している秘密鍵を使ったメールの復元が行えます。

署名や暗号化、復元をMDPGPで行うためには、まずは公開鍵と秘密鍵の2つの鍵をペアとする鍵束（キーリング）を管理します。MDPGPはユーザー専用の鍵を必要に応じて自動・手動で生成する機能を搭載しています。他で作成した鍵をインポートする事もできます。また、MDaemonは社内のユーザーから送られた暗号化メールを監視し、使われている鍵を自動でインポートする事もできますので、まずユーザーがメールの送信先となる人物から受け取った鍵を使ってメールを暗号化し、その後MDPGPはそれを社内で共有している鍵束（キーリング）へインポートする事ができます。最後に、メールが鍵束として管理している鍵と紐づいたアドレスから到着した場合、MDPDGPは設定を元に、必要に応じてメールへの署名や、暗号化・復元を行います。アドレスで複数のキーを使用していた場合、MDPGPは優先キーとして指定されているキーを使ってメッセージを暗号化します。優先キーが設定されていない場合は、MDPGPは最初のキーを使用します。メッセージを復元する際には、MDaemonは両方のキーを使用します。

MDPGPの署名と暗号化は自動で行うよう設定する事もできますし、手動で行う事もできます。自動でこうした操作を行う際、MDPGPは可能な限り自動でメールへの署名と暗号化を行います。手動で行うよう設定を行った場合、対象アカウントがMDPGPの使用を許可されているアカウントであれば、MDPGPはメールへの署名又は暗号化（または復元）のみを行います。

OpenPGPの仕様はRFCの 4880 と 3156で定義されています。

MDPGPの有効化

MDPGPを有効にする
MDPGPはデフォルトで有効ですが、キー作成とキーリングへのインポートを行うか、後述するMGPGPによるキーの自動生成を行うよう設定するまでは、実際のメールの署名や暗号化、復元を行う事はできません。

暗号化&署名サービスを有効にする
デフォルトでは要求されたキーがキーリングに存在する場合、メールへの署名が追加され暗号化が行われます。MDPGPでメールへの署名追加や暗号化を行わない場合はこのオプションを無効化します。

メールは暗号化なしで署名されますが、MDPGPで暗号化されたメールには必ず署名が付与されます。

復号化&検証サービスを有効にする
デフォルトでは受信した暗号化メールは、宛先の秘密鍵が分かっていれば復元されます。またMDPGPは組み込まれた署名の検証も行います。ただし、このサーバー上の全てのユーザーにMDPGPを使用させる、や、MDPGPを使用するユーザーを設定する、のオプションを使用している場合、復号化/検証サービスには、宛先と送信元の両方が認証されている必要がありますのでご注意下さい。（デフォルトでは全員が認証されます。）例えばユーザーにメールクライアントプラグインで個々に復元処理を行わせる場合など、MDPGPにメールの復号を行わせない場合はこのオプションを無効にして下さい。無効化すると、受信した暗号化メールは通常のメールと同様に処理され、宛先メールボックスへ配信されます。

DNS (pka1)から公開鍵を取得しこの時間キャッシュを持つ [xx] 時間
MDPGPがメールの宛先の公開鍵をPKA1を使ってDNSサーバーから取得できるようにするにはこのオプションを有効化します。これは宛先用の公開鍵を取得するプロセスを部分的に自動化でき、暗

号化メールを送信するのに従来必要だった手動での処理を簡略化できるという点で便利です。PKA1で問合せを行うと、見つかったキーURIがすぐに収集され、検証後、キーリングへ追加されます。正しく取得されキーリングへインポートされたキーは、その情報がfetchedkeys.txtへ記録され、このオプションで指定した時間が経過した際、又はPKA1のTTL値の、どちらか大きい方の値に基づき期限切れとなります。そのため、ここで指定した値はキーがキャッシュされるべき最少時間を指定します。デフォルト値は12時間で最少単位は1時間です。

所有している公開鍵をDNSへ公開するには特別なTXTレコードを生成する必要があります。例えば、frank@example.comが、キーid: 0A2B3C4D5E6F7G8H を所有している場合、"example.com"ドメインのDNSへ"frank._pka.example.com"(._pkaの値はメールアドレスの@と読み替えて下さい)というTXTレコードを追加します。. TXTレコードのデータは次のようになります。: "v=pka1; fpr=<key's full fingerprint>; uri=<Webmail-URL>/WorldClient.dll?view=mdpgp&k=0A2B3C4D5E6F7G8H" この中の<key's full fingerprint>はキーのフィンガープリントです(20バイトのフィンガープリント値を表現する40文字から生成されます。)MDPGPの管理画面でキーをダブルクリックすると、フィンガープリント全体の値を確認する事ができます。

HTTP(Webmail)で公開鍵を送信

Webmailを簡易公開鍵サーバーとして使用するにはこのオプションを選択します。Webmailが公開鍵のリクエストを受け付けるようになります。リクエストを送る場合のURLの形式は次の通りです: "http://<Webmail-URL>/WorldClient.dll?View=MDPGP&k=<Key-ID>"。<Webmail-URL>はWebmailサーバーのパスと差し替えて下さい(例:"http://wc.example.com")。また、<Key-ID>は任意の16文字から成るキーidです。(例: "0A1B3C4D5E6F7G8H") キーidは最後の8byteがキーフィンガープリントとなっており、合計16文字から成り立っています。

SMTPメールセッション内での公開鍵提供(MDaemon)

SMTPメール配信処理の1つとして公開鍵の自動交換を行うには、このオプションを有効にします。これで、MDaemonのSMTPサーバーがRKEYと呼ばれるSMTPコマンドに対応します。RKEYに対応しているメールサーバーへメールを送信すると、MDaemonは送信者の最新又は優先する公開鍵の転送を行うかどうか確認します。対象ホストはキーの有無を確認し、それ以上の処理が不要("250 2.7.0 Key already known")かキーが必要がどうかを返します。キーが必要な場合はキーはすぐにASCIIフォーマット("354 Enter key, end with CRLF.CRLF")でメッセージと同様に転送されます。期限切れになったキーや無効化されたキーは転送されません。MDaemonが送信元のキーを複数持っている場合は常に優先度の高いキーを送信します。優先キーがない場合は、最初に確認したキーを送信します。有効なキーがない場合は処理が行われません。ローカルユーザーに紐づけられた公開鍵だけが提供されます。

公開鍵の転送はメールを配信するSMTPメールセッションの1部として実行されます。公開鍵を許可するため、公開鍵は、キーの所有者によってi=のパラメーターを使ったDKIM署名 484付きのメールと合わせて送信される必要があります。このDKIM署名はFrom:ヘッダのアドレスと完全に一致する必要があります。「キーの所有者」はキー自体から判別されます。また、メールは送信者のSPFパス 479から届いたものである必要があります。最後に、キーの所有者(又はワイルドカードの使用によるドメイン全体)はRKEYにより検証済である必要があります。検証のためには、MDPGPルールファイル(ルールファイルの中に説明が記載されています。)でドメインが公開鍵の交換を行える機関である事を示しておく必要があります。これらの検証は全て自動で行われrますが、DKIM 481とSPF検証 479が有効化されていないと、処理が実行されない点にご注意下さい。

MDPGPログには結果とインポートまたは削除された全てのキーの詳細情報が記録され、この処理はSMTPセッションログへも記録されます。正しく動作しているとSMTPセッションログにキーの処理の詳細が記録され、MDPGPログファイルにも詳細が記録されます。

全てのサービスをMDaemon上のすべてのユーザーに許可する
MDaemonユーザー全員が、上記で設定したオプションに応じて、MDPGPでメールへの署名、暗号化、復号化を行えるようにするにはこのオプションを有効にします。サービス毎、ユーザー毎に利用の許可や禁止を行うには、後述の「MDPGPを使用する/しないユーザーを詳細に設定する」を使用して下さい。特別なローカルユーザーのみを認証する場合にのみ、このオプションを無効化して下さい。この場合「MDPGPを使用する/しないユーザーを詳細に設定する」で権限を与えるユーザーの設定を行って下さい。

復号化/検証をローカルではなく(外部)ユーザーに許可する
デフォルトで、MDPGPがローカルの宛先ユーザーの秘密鍵を把握している場合は、ローカル以外から届いた暗号化されたメールは復号化されます。これと同様に、MDPGPは外部から届いたメールの署名の検証も行います。特定のローカル以外から届いたメールを検証や復号化の対象から外したい場合は、後述の「MDPGPを使用する/しないユーザーを詳細に設定する」を使用して下さい。送信元がローカルアドレスでない場合に、メールの復号化や署名検証を行わないようにする場合はこのオプションを無効化して下さい。この場合であっても、後述の「MDPGPを使用する/しないユーザーを詳細に設定する」でユーザー個別の設定が行えます。

MDPGPを使用する/しないユーザーを詳細に設定する
このボタンをクリックするとrules.txtが開き、MDPGP用のユーザーパーミッションを設定できます。このファイルではメールへの署名、メールの暗号化、メールの復元を許可するユーザーをそれぞれ指定する事ができます。また、制限するユーザーも指定する事ができます。例えば、ここで"+*@example.com"というルールを使い、example.comがメールを暗号化できるようにし、"-frank@example.com"というルールを更に追加する事で、frank@example.comを除外する事ができます。rules.txtの先頭部分に、ルールの説明と例が記載されています。

Rules.txtの注意点とSyntax

- MDaemonサーバー内の、SMTP認証を通過したユーザーのメールのみが暗号化サービスを利用できます。ただし、暗号化サービスを制限するローカル以外のアドレスを指定すると、MDPGPは公開鍵が分かっている場合であってもメールの暗号化を行いません。
- rules.txtの設定と、全体の「*すべてのサービスをMDaemon上のすべてのユーザーに許可する*」オプションが競合した場合、rules.txt設定が使用されます。
- rules.txtの設定と、全体の「*復号化/検証をローカルではない(外部)ユーザーに許可する*」オプションが競合した場合、rules.txt設定が使用されます。
- #の後のテキストは無視されます。
- 一行で複数アドレスを指定する場合は空白で区切ります。
- メールアドレスにはワイルドカード(* と?)が使用できます。
- MDPGPで暗号化したメールは常に署名されますが、暗号化の許可と、暗号化していないメールに対する署名の許可は異なります。暗号化されていないメールへ署名を付与するには、アカウントは署名を行うためのパーミッションを付与されている必要があります。
- 各アドレスは次のタグの中のどれかを先頭に付けた上で指定します:

+(プラス) - アドレスはMDPGP暗号化サービスを使用できます。

-(マイナス) - アドレスはMDPGP暗号化サービスを使用できません。

!（エクスクラメーション）- アドレスはMDPGP復元サービスを使用できます。

~（チルド）- アドレスはMDPGP復元サービスを使用できません。

^（キャレット）- アドレスはMDPGP署名サービスを使用できます。

=（イコール）- アドレスはMDPGP署名サービスを使用できません。

$（ダラー）- アドレスはMDPGP検証サービスを使用できます。

&（アンド）- アドレスはMDPGP検証サービスを使用できません。

例:

+*@* ー 全ドメインの全ユーザーが暗号化できます。

!*@* ー 全ドメインの全ユーザーが復号できます。

^*@* ー 全ドメインの全ユーザーが署名できます。

^*@example.com ー example.comの全ユーザーが署名できます。

+frank@example.com ~frank@example.com ー ユーザーは暗号化できますが復元できません。

+GROUP:EncryptingUsers ー MDaemonの EncryptingUsers グループメンバーは暗号化できます。

^GROUP:Signers ー MDaemonの Signers グループメンバーは署名できます。

暗号化/署名モード

自動モード

設定オプションで、許可されているアカウントに対しては、MDPGPがメールの署名や暗号化を自動で行うよう設定できます。アカウントが認証済メールを送信しMDPGPが必要な鍵を把握している時、メールには下記の設定に基づいて署名を付与し暗号化されます。

下記の手動モードで定義されている特別な件名コードは自動モードオプションよりも優先されます。そのため、これらのオプションが無効になっていても、署名や暗号化が許可されているユーザーであれば、以下のコードを使用して、手動でメールへ署名を追加したり暗号化したりすることができます。

設定

受信者の公開鍵を知っている場合、自動的にメールを暗号化する
デフォルトで、アカウントがメール暗号化を許可されている場合、MDPGPは宛先の公開鍵が分かっている場合はメールを自動で暗号化します。もしも自動で暗号化を行わない場合はこのオプションを無効化して下さい。メールは、以下で説明している手動モードの特別なコードを使う事で手動で暗号化する事ができます。

送信者の秘密鍵が登録されていたら自動的に署名を付与する
メールへの署名が許可されているアカウントは、MDPGPが送信アカウントの秘密鍵が分かっている場合には署名を付与するようになります。署名を自動で行わない場合はこのオプションを無効化して

下さい。メールには、以下で説明している手動モードの特別なコードを使う事で、署名を追加する事ができます。

同じドメイン間でも暗号化/署名を行ったメールを送信する
MDPGPがメールを自動で暗号化したり署名を付与するよう設定されていた場合、これはメールが同一ドメイン間でのやり取りだった場合であっても、必要な鍵を把握していれば自動でメール暗号化や署名付与を行うためのオプションです。このオプションはデフォルトで有効です。

MDaemonが持つローカルドメイン間のメールも暗号化/署名を行う
MDPGPがメールを自動で暗号化したり署名を付与するよう設定されていた場合、これはメールがMDaemonのローカルドメイン間でのやり取りだった場合であっても、必要な鍵を把握していれば自動でメール暗号化や署名付与を行うためのオプションです。例えば、MDaemonドメインに「example.com」と「example.net」が含まれていた場合、このドメイン間でやり取りされたメールは自動で暗号化され、署名が付与されます。このオプションはデフォルトで有効です。

自分へのメールも、暗号化/署名を行う
MDPGPがメールを自動で暗号化したり署名を付与するよう設定されていた場合、このオプションを使用すると、ユーザーが自分自身へ送ったメール(frank@example.comがfrank@example.comへ送ったメール)であっても、同様にメールの自動暗号化や署名付与が行われます。つまり、(デフォルト設定として)アカウントが暗号化と復号化の両方を使用する権限を持っている場合、メールはMDPGPにより暗号化され、すぐに復号化されてユーザーのメールボックスへ配信されます。しかしながら、アカウントが復号のパーミッションを与えられていないと、メールが暗号化されたままユーザーのメールボックスへ配信され、配信後も暗号化されたままになってしまう場合があります。このオプションはデフォルトで有効です。

手動モード

メールへ署名を自動追加するが無効になっている場合、MDPGPは手動モードで使われています。MDPGPはメールが認証済で且つ、メールの件名に次のコードのどれかが含まれている場合でないとメールへの署名追加や暗号化は行いません:

--pgps 可能な場合メールへ署名を追加します。コードは件名の最初か最後に配置されます。

--pgpe 可能な場合メールを暗号化します。コードは件名の最初か最後に配置されます。

--pgpx メールは暗号化される必要があります。(宛先の鍵が不明な場合など)暗号化が行えなかった場合は配信を行わないようにして下さい。メールは配信に失敗し、送信者へ戻されます。コードは件名の最初か最後に配置されます。

--pgpk 自身の公開鍵の送信依頼を行います。コードは件名の最初か最後に配置され、ユーザーは自分自身にこのメールを送ります。MDPGPはその後ユーザーへユーザー自身の公開鍵情報をメール送信します。

--pgpk<Email> 対象メールアドレスの公開鍵の送信を依頼します。コードは件名の最初か最後に配置され、ユーザーは自分自身にこのメールを送ります。MDPGPはその後ユーザーへ対象ユーザーの公開鍵情報をメール送信します。

例:

```
Subject: --pgpk<frank@example.com>
```

鍵の管理

公開鍵と秘密鍵はMDPGPダイアログの下の方にあるオプションで管理されています。キー毎にエントリが一あり、このエントリを右クリックすると、キーのエクスポートや削除、有効化/無効化を行う事ができます。鍵のエクスポートを選択すると、鍵は \MDaemon\Pem_mdpgp\exports\ フォルダへ保管され、必要に応じてこの公開鍵をメールで送信する事ができます。"ローカル/リモートを表示"や"フィルタ"オプションを使用して、特定のアドレスやグループを指定する事ができます。

ドメインキーの使用

追加で、送信者に関わらず、特定のドメイン宛の全てのメールを暗号化するためのドメインキーを使用する事ができます。これは、例えば、ドメインの1つと別の場所へホスティングされている別ドメイン間でやり取りされている全てのメールを暗号化する場合などで、ドメイン内の全アカウント用の暗号化キーを個別に管理したくない、といった場合などに便利です。ドメインキーの実装には複数の方法があります:

- 別ドメイン用に既にパブリックキーを持っていて、このキーを送信メールの暗号化に使用したい場合は、対象のキーを右クリックし、**ドメインキーとして設定**をクリックします。ドメイン名を入力し、OKをクリックします。これにより、コンテンツフィルタルールが自動生成され、To:に対象ドメインが含まれる全てのメールが指定されたキーを使って全て暗号化されるようになります。
- ドメインのパブリックキーは提供されているものの、まだ一覧にはない場合、**ドメインキーをインポート**をクリックし、ドメイン名を入力し、OKをクリックします。ドメインのpublic.ascファイルを選択し、開くをクリックします。これによりコンテンツフィルタルールが生成され、ドメイン宛のメールが暗号化されるようになります。
- 暗号化対象のメールなどの要件に合うよう、コンテンツフィルタルールを必要に応じて編集します。
- 別ドメインから自分のドメイン宛に届くメールを暗号化するのに新しいキーを作成するには、「特定のユーザー用のキー生成」の手順に沿って、一覧から"_Domain Key (domain.tld)_ <anybody@domain.tld>"を選択します。

対応するプライベートキーを持っているメールの送信時暗号化用のキーを使用しないでください。使用すると、MDPGPはメールを暗号化し、その直後に自身が管理している復元キーを使ってメールを復元してしまいます。

送信者へ暗号化失敗の詳細をメール送信する(--pgpeコマンド)
ユーザーが--pgpeコマンドで暗号化メールを送信し、(例えば暗号化を行うための鍵が見つからないなどの理由で)対象メールが暗号化に失敗すると、このオプションは送信者へ暗号化の失敗通知を送信します。このオプションはデフォルトで無効になっており、失敗の通知は送信されません。

自分へのメールで公開鍵をメール送信する(--pgpkコマンド)
"--pgpk<email address>"という件名(例 --pgpk<frank@example.com>)で自分宛てにメールを送信します。メールアドレス用のパブリックキーがあると、これを送信者へ返信します。

認証されたユーザーから送られたメールの公開鍵を自動でインポートする
デフォルトで、認証ユーザーが公開鍵をASCII形式で付与したメールを送った場合MDPGPはキーリングへこの公開鍵をインポートします。連絡先の公開鍵を自分自身へメール送信しMDPGPへ取り込ませる事で、簡単に連絡先の公開鍵をMDPGPに読み込ませる事ができます。公開鍵の自動インポートを行わない場合にはこのオプションを無効化します。

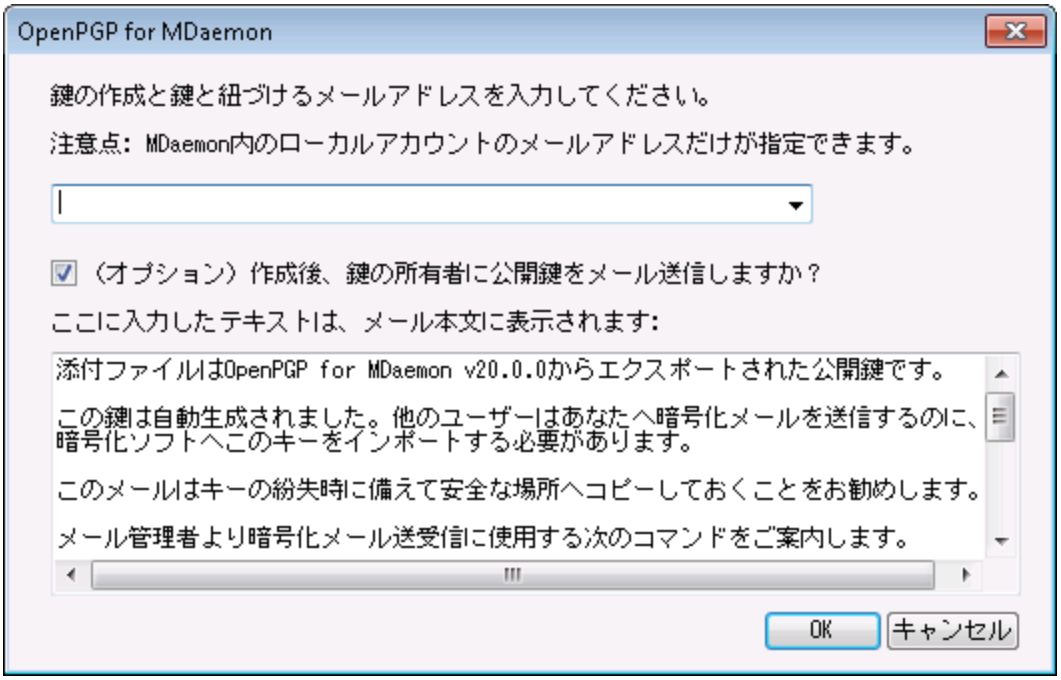
自動的に鍵を作成する
MDPGPがMDaemonユーザー毎に、自動で公開鍵/秘密鍵を生成できるようにするにはこのオプションを有効化します。全ての鍵を一度に作成するよりも、MDPGPは、各ユーザーが次回のメール送信時に鍵のペアを使う事ができるよう、時間をかけて鍵の作成を行います。このオプションは負荷を抑え、MDPGPを使う事がないようなアカウント向けに不要な鍵を作成するのを防ぐため、デフォルトで無効に設定されています。

鍵サイズ
MDPGPが生成する鍵のサイズを指定します。サイズとして指定できるのは、1024, 2048, 4096です。デフォルト設定は2048です。

[xx]日間の有効期間 (0=無制限)
このオプションはMDPGPが生成する鍵の有効期限を日数で指定するオプションです。0を設定すると鍵の有効期限はなくなります。デフォルト値は0です。

特定のユーザー向けの鍵を作成する
アカウントに手動で鍵のペアを作成するには

1. 特定のユーザー向けに鍵を作成するをクリックします。
2. 対象アカウントをドロップダウンリストから選択します。ドメインの全アカウントで1つのキーを使う場合は、一覧から "_Domain Key (domain.tld)_ <anybody@domain.tld>"オプションを選択します。
3. **追加**: メールの添付ファイルとしてユーザーに鍵を送る場合は、公開鍵を鍵の所有者へメールで送る...をクリックします。
4. **Ok**をクリックします。



宛先IPを元に送信メールを暗号化
特定のIPアドレス宛てのメール全てを、特定の鍵で暗号化するには、このオプションを有効にし、設定をクリックし、MDaemon Message Transport Encryptionファイルを開いて、IPアドレスと対応するKey IDを指定します。ここで指定されたIP宛の外部SMTPセッションは対応する鍵を使って全てのメールを暗号化します。メールが既に暗号化されていた場合はこの処理はスキップされます。

鍵のインポート
MDPGPへ手動で鍵をインポートするには、このボタンをクリックし、鍵ファイルを指定し、開くをクリックします。秘密鍵ファイルをインポートする際、公開鍵をインポートする必要はなく、公開鍵は秘密鍵の中に含まれています。パスフレーズで保護された秘密鍵をインポートすると、MDPGPはパスフレーズの入力を求めてきます。パスフレーズを入力していないと、秘密鍵のインポートは行えません。秘密鍵をインポートすると、MDameonはMDPGPが使用している鍵のパスフレーズを変更します。

ドメインキーをインポート
特定のドメインへのメールを全て暗号化するためのパブリックキーが提供されている場合、このボタンをクリックし、ドメイン名を入力し、OKをクリックします。ドメインのpublic.ascファイルを選択し、開くをクリックします。これによりコンテンツフィルタルールが生成され、ドメイン宛のメールが暗号化されるようになります。

パスフレーズの変更
秘密鍵はパスフレーズによって常に保護されています。秘密鍵をインポートする際にはパスフレーズのインポートが必要です。秘密鍵をエクスポートする際でも、対象の鍵はパスフレーズで保護されており、パスフレーズがなければエクスポートする事ができません。MDPGPのデフォルトパスフレーズは**MDaemon**です。MDPGPで鍵を作成したり、鍵をインポートしたりすると、このパスフレーズは全てデフォルトパスフレーズへと設定（又は変更）されます。セキュリティのため、MDPGPの利用を開始したら、このパスフレーズを変更して下さい。MDPGPのパスフレーズの変更をクリックする事で、いつでもパスフレーズの変更が行えます。パスフレーズを変更したら、キーリングの全ての秘密鍵は新しいパスフレーズへアップデートされます。

データファイルをバックアップする
このボタンをクリックするとKeyring.private と Keyring.public のキーリングファイルがバックアップされます。デフォルトでバックアップファイルは\MDaemon\Pem_mdpgp\backups へコピーされ、日付と.bak拡張子がファイル名へ追加されます。

- 転送メールは暗号化されません。
- 自動応答メールは暗号化されません。
- 「DNS（pka1）から公開鍵を取得しこの時間キャッシュを持つ」や「HTTP(*Webmail*)で公開鍵を送信」以外の、鍵サーバー機能や鍵の取消機能には対応していません。
- コンテンツフィルタの暗号化処理は既に暗号化されているメールの処理は行わず、暗号化や復元処理はMDPGP設定を行う際の要件に基づいて処理されます。
- MDaemonアカウントを表示するドロップダウンリストはデフォルトで最初の500ユーザーまでを表示します。全てのアカウントを表示するには plugins.dat で MaxUsersShown=0 を設定して下さい。ユーザー数が多いと、この設定によってロードに時間を要する場合があります。
- MDPGPUtil.exeはコマンドラインから暗号化や復号を行うためのツールです。MDPGPUtilを引数なしで実行するとヘルプ情報を閲覧できます。

4.4 Outbreak Protection

Outbreak Protectionは、オプションである MDaemon AntiVirus 609 機能の一部です。MDaemon AntiVirusを有効化すると、最初の30日は評価期間として動作します。この機能を購入するには、MDaemonの認定リセラーへ連絡するか、次のサイトを参照してください。: www.mdaemon.com

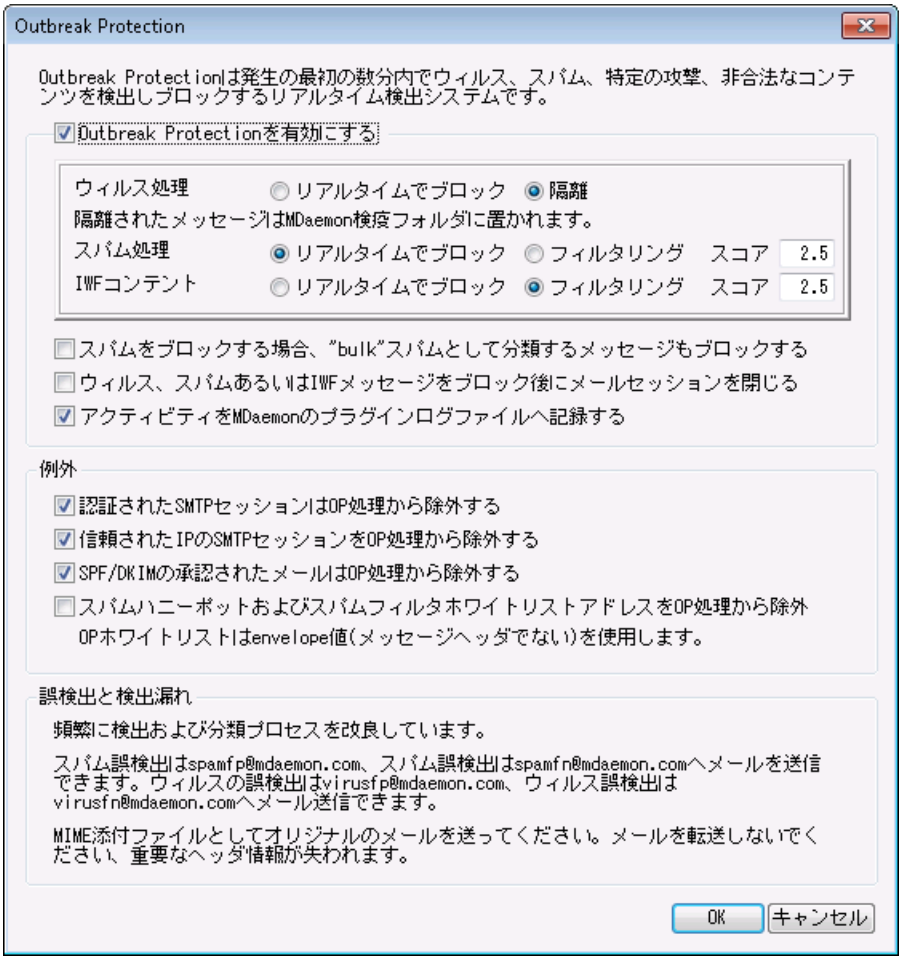
Outbreak Protection（OP)は、MDaemonのセキュリティメニュー（セキュリティ ≫ Outbreak protection..., または Ctrl+Shift+1）から接続できます。これは、MDaemonのメール環境に影響を及ぼすスパム、ウィルス、フィッシングを、発生から数分の間に自動でリアルタイムに防御する事ができる革新的な機能です。

Outbreak Protectionはコンテンツに依存しない、つまりメッセージに含まれる語句に限定された解析に依存せずに機能します。そのためヒューリスティックルールやコンテンツフィルタ、定義ファイルの更新などの必要がありません。その代わり、OPはRecurrent Pattern DetectionとZero-hourテクノロジーを基にしています。これは、メール構造やSMTPのメール配信パターンを数学的に分析し、その結果を世界

中の数百万に上る電子メールからリアルタイムに収集されたパターンと比較します。注意点：OPは実際のメールデータを送信したり、メール内容を読み解くことはありません。

メッセージをリアルタイムで世界中の電子メールのパターンと比較できるため、新しい脅威に対する保護機能を数分で(早い場合は数秒で)提供することができます。ウィルスの場合は、アンチウィルスベンダーが新しいウィルスに対する定義ファイルを更新するまでに時間がかかるため、しばしばウィルスが広範囲に感染した後に定義ファイルの更新が提供されることがあります。この間、Outbreak Protectionが導入されていないコンピュータはこれらの新しい脅威に対して全くの無力となります。これと同様にスパムに関しても、現状のヒューリスティックやコンテンツをベースとしたシステムでは、新しいスパムを分析しフィルタリングルールを作成するまでに時間がかかります。Outbreak Protectionはこれらの危険な期間を解消するために開発された技術です。

しかしながら、Outbreak Protectionの機能は、従来のアンチウィルスやアンチスパム、アンチフィッシングの代替となるものではありません。実際に、OPはMDaemonの持つ既存のヒューリスティック、署名、コンテンツフィルタリングに別の保護レイヤーを追加提供しています。具体的には、OPは従来の、対象を絞ったウィルスではなく、大規模感染を防ぐという目的で設計されています。



Outbreak Protection

Outbreak Protectionを有効にする

Outbreak Protectionを有効にするには、このチェックボックスに選択します。受信メッセージは、進行中のウィルス、スパムまたはフィッシングの発生の一部であるか確認するために分析されます。この

ダイアログの他のオプションは、メッセージに問題が含まれていた場合の動作の指定、送信者をOutbreak Protectionの処理から除外するために使用されます。

ウィルス処理...

リアルタイムでブロック
ウィルス発生と判断される場合、SMTP処理中にメッセージをブロックする場合、このオプションを選択します。これらのメッセージは、隔離あるいは予定受信者に配信されません。サーバによって拒否されます。

隔離
OPがウィルス発生と判定するメッセージを受け入れる場合、このオプションを選択します。これらのメッセージはサーバによって拒否されず、目的の受信者に配信されず隔離されます。隔離されたメッセージは、quarantineフォルダに置かれます。

スパム処理...

リアルタイムでブロック
OPがスパム発生の一部であると確認する場合、SMTP処理中にメッセージをブロックする場合、このオプションを選択します。これらのメッセージはスパムとしてフラグを付けず、目的とされた受信者に配信されません。サーバによって拒否されます。"バルク"メールとしてOPによって分類されたメッセージは、[スパムをブロックする場合、"bulk"として分類するメッセージをブロックする]オプションを、下記でアクティブにしない限りこのオプションによってブロックされません。
OPによる「バルク」と分類されるメッセージは単に特定の非常に多数のメーリングリストの一部または他の類似した広く配布されたコンテンツである可能性があるので、それらのタイプのメッセージがスパムであると見なすか不明です。そのために、それらのタイプのメッセージは、一般に負の値に記録されない、あるいはOPによってブロックされません。

フィルタリング
スパムフィルタリングならびにコンテンツフィルタ処理を行うために、スパム発生の一部とOPが認識するメッセージを受け入れる場合は、このオプションを選択します。これらのメッセージはOPによってブロックされますが、スコアオプションによってスパムフィルタスコアが調整されます。

フィルタリングオプションを使用する場合、OutbreakProtectionが直接スパムメールをブロックすることはありませんが、スパムフィルタの中のスパムフィルタ[617]画面にて、[SMTPは次の数以上のスコアを所有するメッセージを拒否する]を有効にすると、スパムはMDaemonによってSMTP処理中にブロックされます。

例えばスコアオプションが、対象メッセージを15.0と判断した場合、[SMTPは次の数以上のスコアを所有するメッセージを拒否する]で対象スコアを15.0以上と設定していると、メッセージはスパムとした該当メッセージを破棄します。

スコア
上記のフィルタオプションを使用する場合、OPがメッセージでスパム発生の一部であることを判断する場合、この値はメッセージのスパムフィルタスコアに追加されます。この値はメッセージのスパムフィルタスコアに

IWFコンテント
Internet Watch Foundation（IWF）が幼児虐待に関連した内容が記載されていると定義したコンテンツに対して適用されるオプションです。OutbreakProtectionはIWFが提供しているリストを統合し、このコンテンツが含まれているタグを検知することが可能です。IWFは、世界中の幼児虐待コンテンツをもつ違法性のあるオンラインサイト、潜在的に違法なオンラインコンテンツを報告するために、独立したインターネット“ホットライン”を運営します。彼らは、違法なオンラインコンテンツの利用可能性を防止するために、警察、政府、より広いオンライン業界および一般市民と協力して作業します。財団のURLリストは、児童虐待画像のホストしている新しいサイトを毎日更新します。

特に不愉快または違法なマテリアルに関して、多くの組織の従業員によって送信または受信されるメールのコンテンツを調整している内部コンプライアンスルールがあります。加えて、多くの国は、送信または当該コンテンツの受取りを違法としました。この機能は、コンプライアンスを保証するために、効果を促進することができます。

IWFの詳細情報は次のURLを参照してください

http://www.iwf.org.uk/

IWFコンテント...

リアルタイムでブロック
SMTP処理中にIWFの制限されたコンテンツを持つ受信メッセージを拒否する場合、このオプションを選択します。

フィルタリング
IWF制限されたコンテンツを持つ場合、拒否するのではなく、メッセージのスパムフィルタスコアを加算する場合は、このオプションを選択します。スパムフィルタスコアは、下のスコアオプションで指定される値を加算します。

スコア
上記のフィルタオプションの受け入れを選択する場合、これは、IWF制限コンテンツを含む場合、メッセージのスパムフィルタスコアに追加される値です。

スパムをブロックする場合、“bulk”スパムとして分類するメッセージをブロックする
OPはスパムとみなす特定のメッセージを識別しますが、時々、合法的なバルクメールやニュースレターの場合、既知のスパマーあるいはボットネットから送信されていません。OPは、これらのメッセージタイプを"Spam（confirmed）"でなく"Spam（bulk）"で分類します。同様にOPのスパムブロック機能を"Spam（bulk）"メールに適用する場合、このチェックボックスを選択してください。このオプションが無効にされる場合、"Spam（confirmed）"だけがOPのスパムブロック機能に影響します。その後の処理で、このタイプのスパムの受け入れは、バルクメールの受信が必要でありながら、送信者を何かしらの理由でソースまたは宛先を除外できないサイトにおいて必要になる場合があります。

アクティビティをMDaemonのプラグインログファイルへ記録する
OutbreakProtectionのアクティビティをMDaemonのプラグインログへ記録する際にはこのチェックボックスを有効にします。

例外

認証されたSMTPセッションはOP処理から除外する
認証されたSMTPセッションをOP処理から除外するにはこのオプションを選択します。これにより、対象メッセージに対してはOutbreakProtectionのチェックが実施されなくなります。

信頼されたIPからのSMTPセッションはOP処理から除外する
信頼されたIPアドレスをOutbreakProtectionの検査対象外とする場合には、このオプションを選択してください。

SPF/DKIMに承認されたメールはOP処理から除外
SPFやDKIMで承認された一覧である承認リスト[506]へ送信ドメインが含まれていた場合に、OutbreakProtectionの検査対象外とする場合には、このオプションを選択してください。

スパムトラップおよびスパムフィルタ許可アドレスをOP処理から除外
Outbreak Protectionからスパムハニーポット[644]およびスパムフィルタ許可アドレスを除外する場合、このオプションを選択します。"許可リスト"は受信者、または、SMTPセッション中に与えられるRCPT値に適用されます。"許可リスト(送信者)"は送信者、またはSMTPセッション中に与えられるMAIL値に適用されます。これらの操作は、メッセージヘッダ値に基づきません。

誤検出および検出漏れ

まれに正規のメッセージが、伝搬中のスパムあるいはフィッシングとして分類される誤検出(非スパムメールの遮断)が生じることがあります。このような場合、そのメッセージがスパムやフィッシングに関するものであれば spamfp@mdaemon.com 、ウィルスに関するものであればvirusfp@mdaemon.comへ報告してください。我々の検知機能と分類機能の向上のために役立たせていただきます。

スパムメールの通過(検出漏れ)は、非スパムメールの遮断(誤検出)よりも頻繁に起こりえます。これはOutbreak Protectionがすべてのスパムやウィルスをタイムリーかつ的確に捕らえることが難しく、伝搬中のそれらの脅威から守るための1つの方法でしかないためです。しかし、そのような場合でも、AntiVurusやMDaemonの機能によって捕捉することが可能です。もしこのような状況が発生しましたら、そのメッセージがスパムやフィッシングに関するものであればspamfn@mdaemon.com、ウィルスに関するものであればvirusfn@mdaemon.comへ報告してください。我々の検知機能と分類機能の向上のために役立たせていただきます。

このような報告をいただく場合、オリジナルのメールを転送するのではなく、MIME形式の添付ファイルとして送信してください。メールの転送では重要なヘッダ情報などが失われてしまうからです。

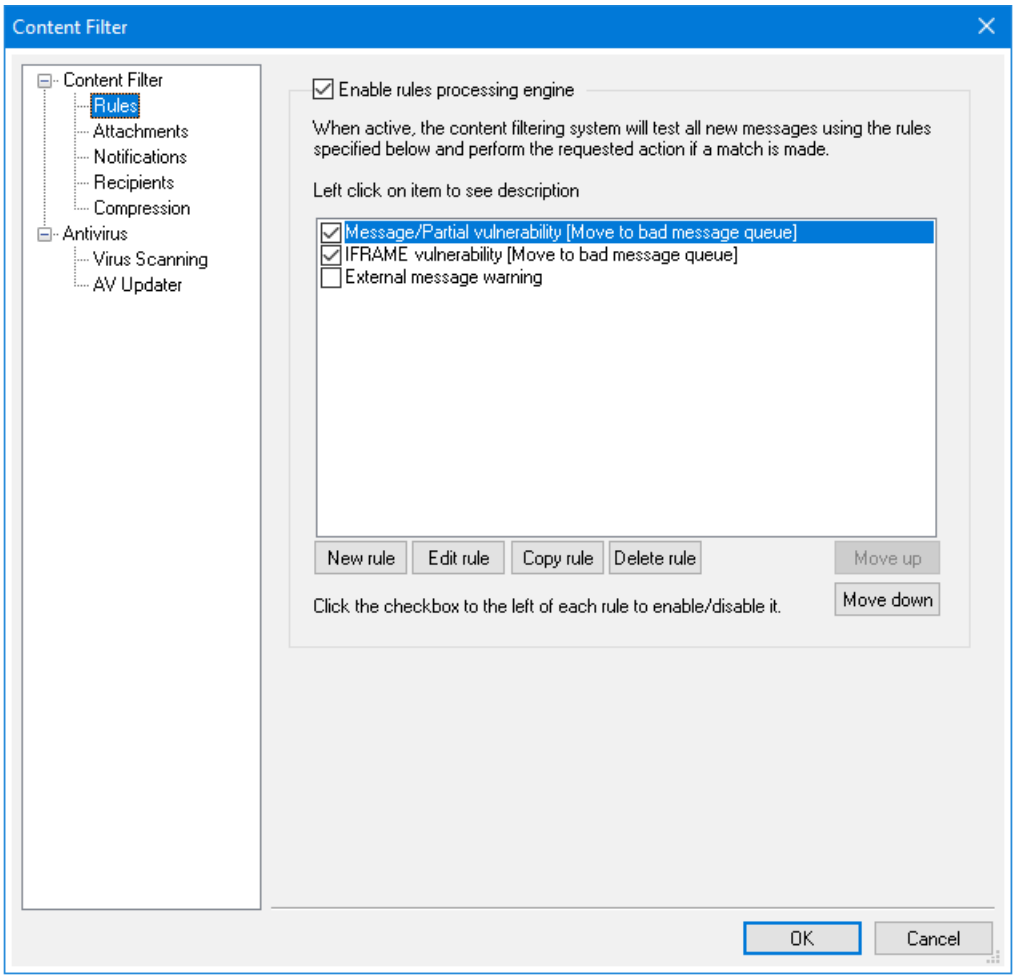
4.5 コンテンツフィルタとアンチウィルス

コンテンツフィルタ

コンテンツフィルタ[588] (セキュリティ ≫ コンテンツフィルタ) は、スパムメールの防止、ウィルスを含むメッセージの遮断、特定ユーザーへメールのコピーを送信、メッセージの下部へメモまたは免責事項を追加、ヘッダの削除、メールの添付ファイルの削除、メッセージの削除など多くの目的で使用できます。非常に高い柔軟性を持っており、ご利用の環境に合わせて管理や運用が行えます。大掛かりな設計は不要で、簡単な検証を行うだけで、大変便利にご利用頂けます。

4.5.1 コンテンツフィルタエディタ

4.5.1.1 ルール



MDaemonによって処理されるすべてのメッセージは、一時的にメッセージキューに置かれます。コンテンツフィルタを有効にすると、キューからメッセージが送り出される前に、まずコンテンツフィルタの処理がされます。この処理によりメッセージをどのように扱うかを決めることができます。

文字"P"から開始されているファイル名があるメッセージは、コンテンツフィルタリングプロセスによって無視されます。その他のメッセージは、コンテンツフィルタシステムによって処理されます。処理されると、MDaemonはファイル名の先頭文字を"P"に変えます。このようにして、メッセージはコンテンツフィルタリングシステムによって処理されます。

コンテンツフィルタルール

ルール処理エンジンを有効
コンテンツフィルタを有効にするには、このチェックボックスを選択してください。MDaemonで処理されるメッセージすべては、配信前にコンテンツフィルタのルールによりフィルタされます。

既存のコンテンツフィルタルール

このボックスはコンテンツフィルタルールすべてを一覧表示し、各チェックボックスで有効/無効の指定ができます。内部のスクリプトフォーマットでルールの説明を参照するには、ルールをクリックし、マウスカーソルをルール上で停止してください(マウスを移動させると説明が消失します)。
メッセージがコンテンツフィルタで処理される時は、一覧の表示順ので、ルールは適用されます。MDaemonで処理されるメッセージすべては、配信前にコンテンツフィルタのルールによってフィルタされます。

例えば、[これはスパムです!]という語句を含むメッセージを削除するルールと、メッセージをPostmaster宛てに送るという2つのルールがあるとします。この2つのルールを正しい順番で設定することにより、両方のルールをメッセージに適用することができます。また、[Stop Processing Rules]というルールが、上記2つのルールよりも下のレベルにある必要があります。そうするためには、[上へ][下へ]ボタンを使って、[ルールの処理を停止する]というルールを他のルールより下に移動します。これにより[これはスパムです!]という語句を含むメールはPostmaster宛てに送信された後に削除されます。

MDaemonは、複数のタスクを実行でき、AND/ORのロジックが利用可能なルールを作成することができます。したがって、上記の例のように、複数のルールを使用するより、これらすべてのタスクを実行可能な1つのルールを作成することが可能です。

新規
このボタンをクリックすると、新規のコンテンツフィルタルールを作成することができます。これにより、新規ルール作成 590ダイアログが開きます。

編集
このボタンをクリックすると、選択されたルールをルール変更エディタ 595で開くことができます。

コピー
このボタンをクリックすると、選択されたコンテンツフィルタルールをコピーすることができます。まったく同じルールが作成され、リストに追加されます。コピーされるルールは、[Copy of "元のルール名"]というデフォルトの名前が付けられます。この機能は、複数の類似したルールを作成する際に便利です。ルールを1つ作成して、それを何回かコピーし、必要に応じてそのコピーを編集することができます。

削除
このボタンをクリックすると、選択されたコンテンツフィルタルールを削除することができます。

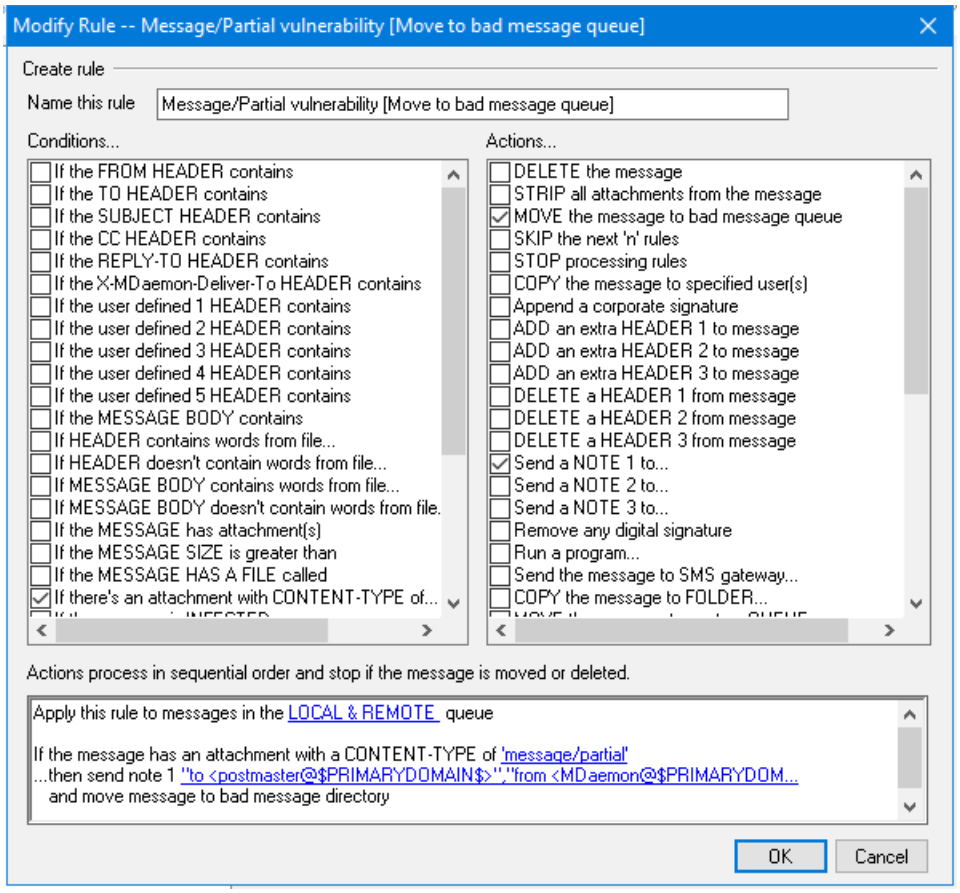
上へ
選択されたルールを上へ移動するには、このボタンをクリックしてください。

下へ
選択されたルールを下へ移動するには、このボタンをクリックしてください。

参照:

新規コンテンツフィルタルールの作成 590
既存のコンテンツフィルタルールの変更 595
フィルタルールで正規表現を利用 595

4.5.1.1.1 新しいコンテンツフィルタルールの作成



このダイアログでは、新しいコンテンツフィルタルールを作成できます。コンテンツフィルタ ダイアログの[新規]ボタンをクリックしてください。

ルールの作成

このルールの名前
新規ルール名を入力してください。デフォルトの新規ルールの名前は[New Rule #n]となります。

条件...

このフィールドには、新規ルールに適用できる条件の一覧が表示されます。新規ルールに適用する条件に該当するチェックボックスをクリックしてください。有効にされた条件は、一番下のルールの説明フィールドに表示されます。多くの条件は、ルールの説明フィールドでハイパーリンクをクリックして、条件に情報を指定する必要があります。

If the [HEADER] contains—
これらのヘッダオプションをクリックして、特定のメッセージヘッダの内容をルールの条件にします。ここでは、検索するテキストを指定する必要があります。この条件では正規表現を利用できます。参照: フィルタルールで正規表現を利用 595

If the user defined [# HEADER] contains—
これらのオプションをクリックして、ユーザ定義のメッセージヘッダをルールの条件にします。新規ヘッダ、および検索するテキストを指定する必要があります。この条件では正規表現を利用できます。参照: フィルタルールで正規表現を利用 595

If the MESSAGE BODY contains—
このオプションは、メッセージ本文から1つの条件を作成します。この条件は、検索するテキスト文字列を指定する必要があります。この条件で正規表現を利用できます。参照: フィルタルールで正規表現を利用 595

If the MESSAGE has Attachment(s)—
このオプションを選択する場合、ルールで1つ以上の添付ファイルの存在が条件となります。この条件には追加情報は必要ありません。

If the MESSAGE SIZE is greater than—
このオプションは、メッセージサイズがを条件とします。サイズはKB単位で指定してください。デフォルトは10KBです。

If the MESSAGE HAS A FILE called—
このオプションは、特定の名前の添付ファイルをスキャンします。ファイル名の指定が必要です。*.exeやfile*.*などのワイルドカードが使用できます。

If message is INFECTED... MDaemonでメッセージがウィルスに感染していると判定した場合、真(TRUE)となります。

If the EXIT CODE from a previous run process is equal to
ルール一覧で前のルールが"Run Process"を利用する場合、この条件を使用して、そのプロセスからExit Codeを探すことができます。

If the MESSAGE IS DIGITALLY SIGNED
この条件はデジタル署名されたメッセージに適用されます。この条件には追加情報は必要ありません。

If SENDER is a member of GROUP...
ルールで示されるアカウントグループのメンバーであるアカウントによって送信される時に、この条件はメッセージに適用されます。

If RECIPIENT is a member of GROUP...
ルールで示されるアカウントグループのメンバーのアカウントで受信される時に、この条件はメッセージに適用されます。

If ALL MESSAGES
ルールをすべてのメッセージに適用させたい場合は、このオプションをクリックします。追加情報は必要ありません。このルールは、Stop Processing RulesあるいはDelete Messageというアクションが前のルールによって適用されている場合以外、すべてのメッセージに影響します。

処理...

メッセージがルールの条件と一致した場合に、MDaemonは次のアクションをとります。いくつかのアクションはルールの説明フィールドでアクションのハイパーリンクをクリックして、情報を指定する必要があります。

Delete Message
このアクションを選択すると、メッセージが削除されます。

Strip All Attachments From Message
このアクションを選択すると、メッセージから添付ファイルが取り除かれます。

Move Message To Bad Message Directory
このアクションを選択すると、メッセージを不正(BAD)メッセージディレクトリに移動します。

Append a corporate signature— このアクションにより、メッセージのフッタに短いテキストを追加することができます。また、テキストファイルのコンテンツを加えることもできます。HTMLを使用 のチェックボックスを使用する事で、署名のテキストの中にHTMLコードを使用する事もできます。 この処理は $CONTACT...$ signature macros[121]にも対応しています。

> 例:[このメールはOOより発信されております。お問い合わせまたは苦情に関しましては user01@example.com までお願い申し上げます]という文章をメッセージのフッタに追加することができます。

Skip n Rules
このアクションを選択すると、指定した数だけルールをスキップします。これは、特定の状況のメッセージ限定でルールを適用し、他のメッセージには適用しない時に便利な機能です。

例えば:"Spam"という語句を含むメッセージは削除し、"Good Spam"という語句を含むメッセージは削除しないとします。
この条件は、まず"Spam"という語句を含むメッセージを削除するルールを作成し、その上に[メッセージに" Good Spam" が含まれる場合はルールを1つスキップする]という別のルールを置くことで実現できます。

Stop Processing Rules
このアクションを選択すると、残りのすべてのルールをスキップします。

Copy Message To Specified User(s)
このアクションにより、メッセージのコピーを指定の受信者に送信されます。ここでは、メッセージの受信者を指定する必要があります。

Add Extra Header Item To Message
このアクションはメッセージにヘッダを追加します。ここでは、新しいヘッダとその内容を指定する必要があります。

Delete A Header Item From Message
このアクションはメッセージからヘッダを削除します。ここでは、削除するヘッダを指定する必要があります。

Send note To...
このアクションは、特定のアドレスにメールを送信します。受信者、送信者、件名およびテキストを指定することができます。本来のメッセージにメモに添付するために、このアクションを構成することができます。特定のアドレスに対してメール通知を行います。宛先、送信元、件名、数行のテキストデータを指定する事ができます。併せて、元のメールを添付するよう設定が行えます。注意点: return-pathのないメールは全てこのアクションの対象外となります。そのため、例えばDelivery Status Notification (DSN)メールを使う事はできません。

例:「これはスパムです」という文字列を含むメール全てをbadメールキューへ移動するためのルールを作成する場合、このルールが実行された旨を通知するためのルールも同時に必要になります。

Remove Digital Signature
このアクションを選択すると、デジタル署名をメッセージから削除します。

Run Process...
このアクションは、メッセージがルールの条件と一致した時に特定のプログラムを実行させることができます。実行させたいプログラムへのパスを指定してください。メッセージ名を処理に渡すには$MESSAGEFILENAME$マクロを使用することができ、MDaemonが処理の終了を待つ際に、その動作を一時的にまたは無期限にサスペンドさせるかどうかも指定することができます。さらに、処理を強制的に終了、バックグラウンドで実行することもできます。

Send Message Through SMS Gateway Server...
このオプションを選択すると、メッセージはSMSゲートウェイサーバを通して送信されます。ホストまたはIPアドレス、およびSMSの電話番号を指定してください。

Copy Message to Folder...
このオプションを選択すると、メッセージのコピーを特定のフォルダに置くことができます。

MOVE the messages to custom QUEUE...
このオプションではメッセージを、作成したカスタムリモートメールキューに移動することができます。その際には、予定スケジューラでカスタムスケジュールオプションを使用して処理のタイミングを管理することができます。

Add Line To Text File
このオプションは、特定のテキストファイルにテキストを追加します。このアクションを選択する場合、ファイルのパスと追加するテキストを指定する必要があります。テキスト内で、いくつかのMDaemonマクロを使用することにより、メッセージの送信者、受信者、メッセージID、などの動的な情報をコンテンツフィルタに含ませることができます。[行をテキストファイルへ追加]ダイアログの[マクロ]ボタンをクリックすると、使用できるマクロのリストが表示されます。

このオプションを使用すると、特定のヘッダ内の特定の語句を検索して、それを削除または置換することができます。このルールを作成する場合、ルールの説明フィールドの[specify information]リンクをク

リックして、[ヘッダ - 検索および置換]ダイアログを開き、削除または置換するヘッダと語句を指定してください。この処理では正規表現を利用できます。参照: フィルタルールで正規表現を利用 595

[Copy|Move] Message to Public Folders...メールをパブリックフォルダへコピー又は移動するのにこのアクションを使用します。

Search and Replace Words in the Message Body
このオプションを使用すると、メッセージの本文を検索して、それを任意のテキストに置換することができます。この処理では正規表現を利用できます。参照: フィルタルールで正規表現を利用 595

Jump to Rule...
このアクションを選択すると、2つのルール間のすべてのルールをスキップして、リストの下の方のルールへ即座にジャンプすることができます。

Send an instant message
このアクションを選択すると、メールが条件に一致した場合にインスタントメッセージを送信する事ができます。宛先メールアドレスと送信元メールアドレス、メール本文を指定します。

Add to Windows Event Log...- テキスト文字列をWindowsイベントログへ書き込みます。文字列にはマクロが使用でき、使用できるマクロを表示するボタンも用意されています。

Extract attachments to folder...- メールの添付ファイルを解凍します。添付ファイルをコピーするフォルダを指定する事もでき、解凍後、メールから添付ファイルを削除する事もできます。また、解凍する添付ファイルを、ファイル名、種類、添付ファイルのサイズを元に選択するよう設定も行えます。

Change message processing priority...- メッセージの処理に関する優先度設定が行えます。"10 (緊急)" から "90 (リトライ)"の範囲を選択でき、デフォルト設定は"50 (通常)"です。

Sign with DKIM selector...
ルールによりメッセージにDKIM署名 484を行います。DKIMダイアログで指定された署名ではなく、セレクタを使用して署名する場合にも使用できます。

Flag message for REQUIRETLS...メールへ REQUIRETLS 538を使用するようフラグ付けします。

[Sign|Encrypt|Decrypt] message with the user's [Private|Public] key...- プライベート又はパブリックキーを使って署名、暗号化、復元を行います。詳細はMDPGP 574をご参照下さい。注意点:このアクションはMDPGPが無効な場合でも実行されます。

Add a warning to the top of the message...- メールの最初に警告文を追加します。プレインテキストか「HTMLを使用」をチェックした後HTMLコードで文字列の入力が行えます。ファイルから文字列を読み込む事もできます。

Add an attachment
条件に一致したメールにファイルを添付する場合は、このアクションを使用します。添付ファイルは ./MDaemon/CFilter/Attachments/フォルダへ格納する必要があります。

Extract attachment and add link...
条件に一致したメールの添付ファイルを解凍し、リンクを追加する場合はこのアクションを使用します。参照: 添付ファイルリンク 333

Rule description
このフィールドには、新規ルールの内部スクリプト形式が表示されます。ルールの条件かアクション(ハイパーリンクとして表示される)のどれかをクリックしてください。そうすると、必要な情報を指定するためのエディタが開かれます。

参照:

コンテンツフィルタエディタ 588
既存のコンテンツフィルタルールの編集 595
フィルタルールで正規表現を使用 595

4.5.1.1.2 既存コンテンツフィルタの編集

既存のコンテンツフィルタルールを編集するには、ルールを選択し、コンテンツフィルタダイアログの[編集]ボタンをクリックしてください。[ルールの編集]エディタでルールが開かれ編集可能になります。このエディタ上のコントロールは、ルール作成ダイアログ 590と同じものです。

参照:

コンテンツフィルタエディタ 588
新規コンテンツフィルタルールの作成 590
フィルタルールで正規表現を使用 595

4.5.1.1.3 フィルタルールで正規表現を使用

コンテンツフィルタリングシステムは、特定の値はもちろんテキストパターンも検索できる、[正規表現]検索に対応しています。正規表現は、一致する条件を表す文字列と記号の事で、これによりコンテンツフィルタルールをより強力に、柔軟に作成する事ができるようになっています。

正規表現とは?
正規表現(regexp)とは、メタキャラクタとして知られている特殊文字、アルファベット、数字との組み合わせ、"abc ,"123"などのリテラル文字列から構成されるテキストパターンです。文字列はこれらのパターンと一致しているかどうかを比較され、主にテキストへのマッチング、検索、置換などに使用されます。

メタキャラクタは特定の機能を持つ特殊な文字で、正規表現の中で使用されます。MDaemonのコンテンツフィルタで使用できるメタキャラクタは以下のとおりです。

```
\ | () [] ^ $ * + ? . <>
```

メタキャラクタ	解説
\	メタキャラクタを文字列として処理するよう、メタキャラクタの前に追加します。メタキャラクタとして使用される記号が含まれている文字列検索

に正規表現を使用する場合は必須となります。例えば、"+"を検索ための正規表現では、"¥+"を使う必要があります。

| オルタネーション文字("or"または"bar")は、対象文字列に文字側の表現式のどちらかにマッチする必要がるときに使用します。正規表現"abc|xyz"は、テキスト文字列を検索している"abc"あるいは"xyz"のどちらかにマッチします。

[...] かぎカッコ[ ]に挟まれた文字のセットは、そのセットの任意の文字にマッチします。また半角ダッシュ'-'を始めの文字と終わりの文字で挟むことで範囲を指定することができます。例えば、[a-z]という正規表現で[abc]という文字列の検索は"a","b","c"にマッチします。[az]という正規表現では"a"のみにマッチします。

^ 文字列の先頭を表します。"abc ab a"というターゲット文字列に対して"^a"は最初の1文字だけマッチします。"^ab"は最初から2文字にマッチします。

[^...] 左かぎカッコ[のすぐ後のキャレット("^")には別の意味があります。これはカッコ内の残りの文字の否定を表します。例えば"[^0-9]"という表現は、ターゲット文字が数字ではないことを表します。

(...) カッコはパターンの順序に影響し、検索と置換の表現に使用するためのグループ化の役割を果たします。

正規表現による検索結果は一時的に保存され、新しい表現のための置換表現に使用することができます。置換表現では、"$0"を含むことができ、正規表現の検索でマッチしたサブストリングに置き換えられます。例えば、"a(bcd)e"という検索表現がサブストリングにマッチした場合、"123-$0-123"という置換表現は"123-abcde-123"にマッチします。

同様に、"$1","$2","$3"などの特殊文字を置換表現で使用することができます。これらも文字はサブストリング全体のマッチの代わりにグループ化の結果により置換されます。後の数字はどのグループ表現を参照するかを示します。例えば、検索表現が"(123)(456)"であり、置換表現が"a-$2-b-$1"である場合、マッチするサブストリングは"a-456-b-123"に置き換えられ、置換表現が"a-$0-b"である場合、は"a-123456-b"に置き換えられます。

$ 文字列の最後の文字を表します。"13 321 123"という文字列に対して、"3$"という表現は文字列の最後の文字にマッチします。"123$"という表現は最後から3文字にマッチします。

* ("*")は直前の文字の0回以上の繰り返しを表します。例えば、"1*abc"は"111abc"および"abc"にマッチします。

+ 上記のアスタリスクに似ていますが、"+"は直前の文字の1回以上の繰り返しを表します。例えば、"1+abc"は"111abc"にマッチしますが"abc"にはマッチしません。

?	？は、記号の左側の文字と0又は1回マッチするする事を表します。つまり、"1?abc" は"abc"にマッチし、"111abc"の中の"1abcの部分にマッチします。
.	任意の1文字にマッチします。例えば、".+abc"は"123456abc"にマッチし、"a.c"は"aac","abc","acc"などにマッチします。

適格な条件とアクション
正規表現はフィルタルールの条件の任意のヘッダに使用することができます。例えば、[if the FROM HEADER contains]というルールの条件に使用できます。また、[if the MESSAGE BODY contains]という条件にも使用することができます。

正規表現は、2つのコンテンツフィルタルール処置を使用されることができます: "Search and Replace Words in a Header"および"Search and Replace Words in the Message Body"。

コンテンツフィルタルール条件で使用される正規表現は、大文字と小文字の区別をしません。コンテンツフィルタルール処置で使用される正規表現の大文字／小文字の区別は任意です。

ルールの処置の中で正規表現を作成する場合、大文字／小文字の区別をするオプションがあります。

ルールの条件に正規表現を設定する

ヘッダまたはメッセージ本文の条件に正規表現を使用するように設定するには、

1. ルールの作成ダイアログで、ルールに適用するヘッダまたはメッセージ本文の条件に対応するチェックボックスをクリックします。
2. ルールの作成ダイアログの一番下にあるルールの説明で、上記のステップ1で選択した条件に対応する"**contains specific strings**"リンクをクリックしてください。これにより検索テキストの指定ダイアログが開かれます。
3. "Currently specified strings..."で"**contains**"リンクをクリックします。
4. ドロップダウンリストから"Matches Regular Expression"を選択して[OK]をクリックします。
5. 正規表現の作成にヘルプが必要な場合、またはそれをテストする場合は、ボタンをクリックします。"**Test regular expression**.ダイアログが必要ない場合は、用意されているテキストボックスに正規表現を入力し、[追加]をクリックしてステップ8へ進んでください。
6. [Search expression]テキストボックスに正規表現を入力します。作業をシンプルにするために、正規表現に目的のメタキャラクタを簡単に挿入するためのショートカットメニューが用意されています。このメニューには[＞]ボタンをクリックしてアクセスしてください。このメニューからオプションを選択した場合、それに対応するメタキャラクタが表現に挿入され、テキストの挿入ポイントがキャラクタによって要求される適宜の場所に移動されます。

7. 用意されたテキストエリアに表現をテストするために使用するテキストを入力し[テスト]ボタンをクリックします。表現のテストが終了したら[OK]をクリックします。

8. [OK]をクリックします。

9. その後、通常の方法でルールの作成を続けてください。

ルールのアクションに正規表現を設定する

[Search and Replace Words in…]アクションに正規表現を使用するように設定するには、

1. ルールの作成ダイアログで、ルールに挿入する[Search and Replace Words in…]アクションに対応するチェックボックスを有効にします。

2. ルールの作成ダイアログの一番下にあるサマリで、上記のステップ1で選択したアクションに対応する[specify information]をクリックしてください。これによりSpecify Search and Rplaceダイアログが開かれます。

3. ステップ1で[Search‥header]アクションを選択した場合、ドロップダウンリストから検索するヘッダを選択するか、あるいはもしリストに目的のヘッダがない場合はボックスにヘッダを入力してください。ステップ1で[Search‥header]アクションを選択していない場合はこの手順を省略してください。

4. このアクションで使用する検索表現を入力してください。作業をシンプルにするために、正規表現に目的のメタキャラクタを簡単に挿入するためのショートカットメニューが用意されています。このメニューには[＞]ボタンをクリックしてアクセスしてください。このメニューからオプションを選択した場合、それに対応するメタキャラクタが表現に挿入され、テキストの挿入ポイントがキャラクタによって要求される適宜の場所に移動されます。

5. このアクションで使用する置換表現を入力してください。検索表現と同様にこのオプションにもショートカットメニューが用意されています。マッチしたサブストリングをテキストで置換するのではなく削除する場合は、このテキストボックスを空白として残してください。

6. 表現で大文字と小文字の区別をする場合は[Match case]をクリックしてください。

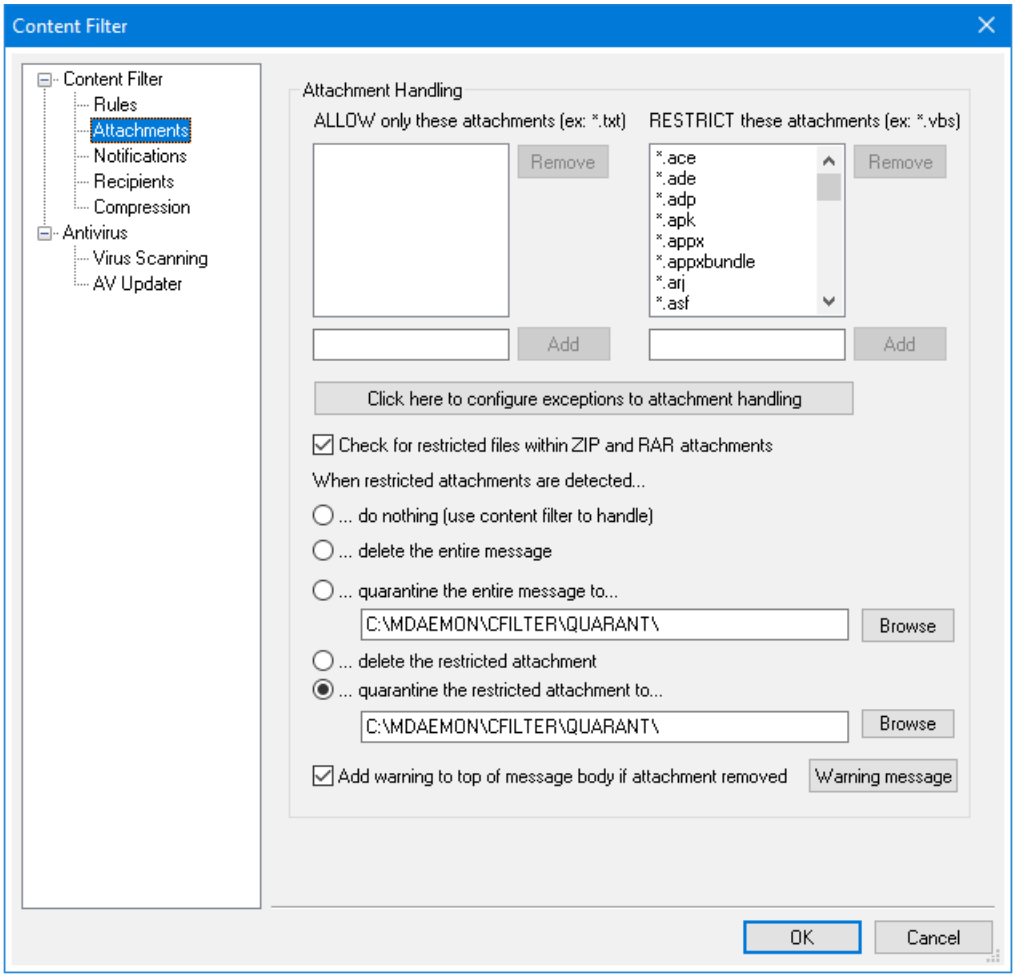
7. 検索および置換のストリングを正規表現とする場合は[Regular expression]をクリックします。さもないとそれぞれのストリングは、サブストリングの検索と置換として扱われ、正規表現の処理を行う代わりにテキストの完全なリテラルのマッチングを検索することになります。

8. 表現をテストする必要がない場合は、このステップを省略してください。テストが必要な場合は[Run Test]をクリックします。Search and Replace Testerダイアログで、テストする検索と置換表現を入力し[Test]をクリックします。テストが終了したら[OK]をクリックしてください。

9. [OK]をクリックします。

10. その後、通常の方法でルールの作成を続けてください。

4.5.1.2 添付ファイル



この画面から、許可したり拒否したりする添付ファイルを指定します。禁止対象の添付ファイルは、メッセージから自動的に削除されます。

添付の処理

[**これらの添付ファイルを禁止**]リストで指定するファイル名は、MDaemonで検知すると、自動的に取り除かれます。[**これらの添付ファイルのみを許可**]リストにファイルを追加した場合は、これらのファイルのみが添付を許可されて、それ以外のファイルはメッセージから取り除かれます。添付ファイルを取り除かれたメッセージは、通常通りに配信されます。**通知**タブのオプションを使用すると、対象の添付ファイルが検知された時、指定の宛先に通知メールを送信できます。

このエントリには、ワイルドカードを使用することができます。例えば、[*.exe]というエントリは、EXEファイル拡張子を持つすべての添付ファイルを許可または禁止することができます。リストのどちらかにエントリを追加するには、[追加]ボタンの横のフィールドにファイル名を入力して、[**追加**]ボタンをクリックしてください。

添付ファイル処理の例外を設定するには、ここをクリック
このボタンをクリックして、添付ファイル制限の監視から除外するアドレスを指定してください。メッセージがこれらのアドレスの1つに配信されると、制限される添付ファイルを含んでいても、MDaemonはそのメッセージの配信を許可します。

ZIPとRARファイル内の禁止ファイルをチェック
ZIP、7-Zip、RARで圧縮されたファイルの内容をスキャンする場合は、このオプションを有効にしてください。また、このオプションを有効にすると、特定のファイル名を検索するように設定されたコンテンツフィルタルールでもZIPファイルの中身をチェックすることができるようになります。

禁止ファイルを検出したら...
メールに禁止している添付ファイルが含まれていた場合のアクションを選択します。

...何もしない(コンテンツフィルタを使用)
添付ファイル処理では特に何も行わず、コンテンツフィルタルール 588 で処理を行う場合はこのオプションを選択します。

...メッセージ全体を削除
禁止ファイルを含んでいたメッセージ全体を削除する場合はこのオプションを選択します。

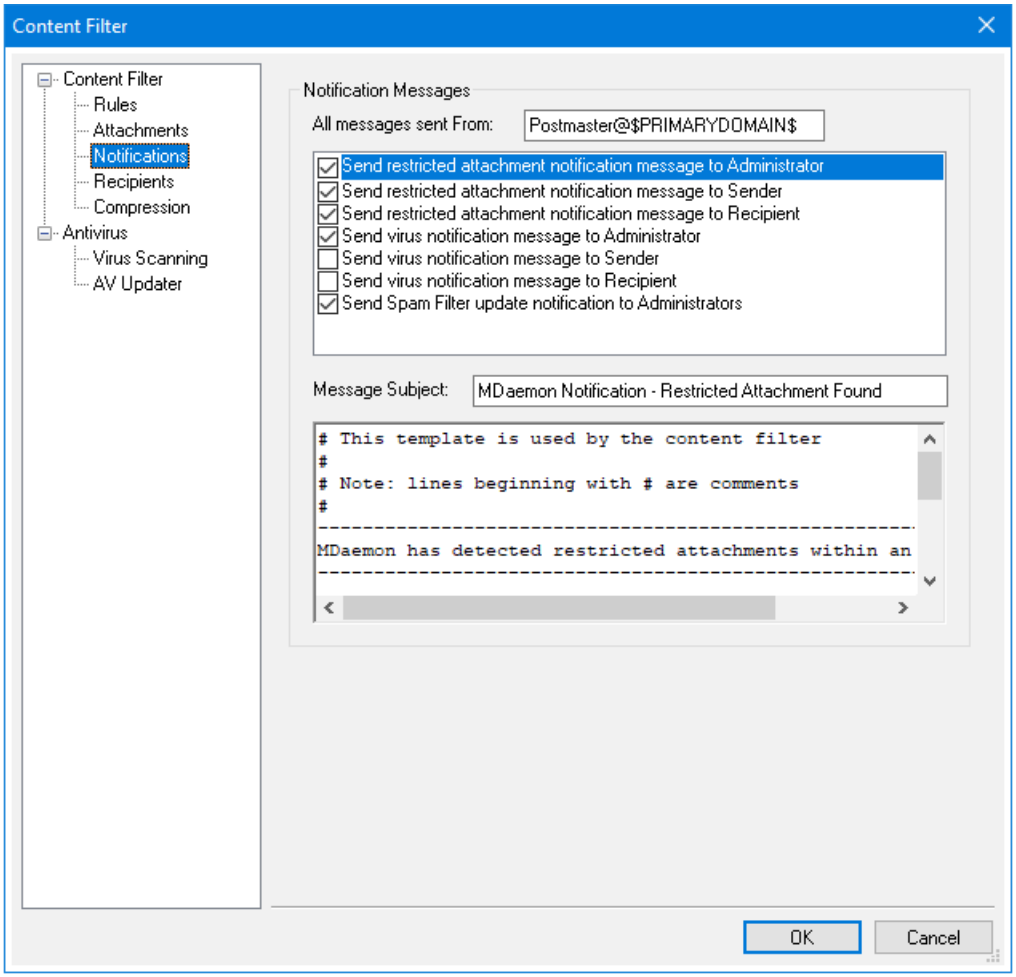
...メッセージ全体を隔離する...
禁止ファイル付きのメッセージ全体を指定の場所へ隔離する場合はこのオプションを選択します。

...禁止ファイルを削除する
メッセージ全体ではなく、禁止ファイルのみを削除する場合はこのオプションを選択します。

...禁止ファイルを次の場所へ隔離する...
削除ではなく特定の場所に禁止した添付ファイルを隔離する場合、このオプションをクリックし場所を指定します。これはデフォルト設定です。

添付ファイルを削除した際、メッセージ本文の上部に警告を追加する
例えばウィルスを検出した場合など、MDaemonがメールから添付ファイルを削除した際、メール本文の上に警告を追加する事ができます。**警告メッセージ**ボタンをクリックし、メッセージのテンプレートを確認したり編集したりできます。このオプションはデフォルトで有効です。

4.5.1.3 通知



この画面では、ウィルスや禁止されている拡張子の添付ファイルの発見時や、アンチウィルスやスパムフィルタのアップデート時に送信される通知メールの設定が行えます。

通知メッセージ

すべてのメッセージをFrom:へ
このボックスを指定して、通知メッセージの送信者となるアドレスを指定してください。

ウィルス通知メッセージを送る...
添付ファイルにウィルスを含むメッセージが到着すると、このセクションで指定した各ユーザ宛に警告メッセージを送信します。カスタマイズされた警告メッセージは、送信者、受信者、[受信者]画面で指定した管理者に送ることができます。これらの3つのエントリのメッセージをカスタマイズするには、リストからそのエントリを選択します。さらに、この画面の下に現れるフィールドでメッセージを編集します。各エントリ用のメッセージがありますが、デフォルトでは3つすべてが同じメッセージなので、その違いが分かりません。

禁止添付ファイルの通知メッセージを送る...
禁止された添付ファイルのエントリ([添付ファイル]画面に表示される)と一致するファイルが添付されたメールが到着すると、このセクションで指定された各ユーザに警告メッセージが送信されます。カスタ

マイズされた警告メッセージは、送信者、受信者、そして[受信者]画面で指定した管理者に送ることができます。これらの3つのエントリのメッセージをカスタマイズするには、リストからそのエントリを選択します。さらに、この画面の下に現れるフィールドでメッセージを編集します。各エントリ用のメッセージがありますが、デフォルトでは3つすべてが同じメッセージなので、その違いが分かりません。

スパムフィルタのアップデート通知を管理者へ送る
管理者へスパムフィルタがアップデートした際通知を送るかどうかを指定します。このオプションはスパムフィルタ ≫ アップデート にある「アップデートの結果を含んだ通知を送信」と同じものです。

メッセージの件名:
このテキストは、送信されるメッセージの[Subject]ヘッダに表示されます。

メッセージ
上のリストで選択したエントリに対応するチェックボックスが有効の場合に、そのエントリに対して送信されるメッセージです。このメッセージは表示されているフィールド内で直接編集することができます。

このテキストを含む実際のファイルは、MDaemon¥app¥ ディレクトリ以下に格納されています:

cfattrem[adm].dat - 制限された添付ファイル- 管理者
cfattrem[rec].dat - 制限された添付ファイル- 受信者
cfattrem[snd].dat - 制限された添付ファイル- 送信者
cfvirfnd[adm].dat - ウィルスが見つかったメッセージ- 管理者
cfvirfnd[rec].dat - ウィルスが見つかったメッセージ- 受信者
cfvirfnd[snd].dat - ウィルスが見つかったメッセージ- 送信者

これらのメッセージをオリジナルに戻す場合は、対象ファイルを削除して下さい。MDaemonがデフォルトの内容でメッセージを再作成します。

メールマクロ

利便性の向上のため、コンテンツフィルタで生成する通知やその他のメールにて、マクロを使用する事ができます。次のマクロを使用できます。

$ACTUALTO$	一部のメッセージは、書式換えまたはエイリアス文字変換の前にオリジナルユーザで入力されたように、通常、転送先のメールボックスとホストを示す"ActualTo"フィールドを含みます。このマクロは、その値で置き換えられます。
$AV_VERSION$	使用している AntiVirus のバージョン情報が表示されます。
$CURRENTTIME$	メールを処理した時間に置き換えられます。
$ACTUALFROM$	一部のメッセージは、書式換えまたはエイリアス文字変換の前にオリジナルユーザで入力されたように、通常、転送先のメールボックスとホストを示す"ActualFrom"フィールドを含みます。このマクロは、その値で置き換えられます。

$FILTERRULENAME$	メッセージが一致した条件のルール名に置き換えられます。
$FROM$	メールのFrom:へ含まれる全メールアドレスへ置き換えられます。
$FROMDOMAIN$	このマクロはメールのFrom:ヘッダにあるメールアドレスのドメイン名を挿入します。(メールアドレスの@の右側の部分です)
$FROMMAILBOX$	このマクロはメールのFrom:ヘッダにあるメールアドレスのメールボックス名を挿入します。(メールアドレスの@の左側の部分です)
GEN_GUID	11桁の英数字で構成されるユニークなIDを意味します。例: 0XVBASADTZC
$HEADER:XX$	このマクロはメールの再フォーマット時にヘッダの特定ーに展開する値をxxとして指定します。例えば:元のメールで "TO: user01@example.com" が含まれていた場合、$HEADER:TO$ マクロは"user01@example.com"となります。元のメールに"Subject: This is the subject"が含まれていた場合、$HEADER:SUBJECT$ マクロは"This is the subject"という値に置き換えられます。
$HEADER:MESSAGE-ID$	上記の$HEADER: XX$と同様に、Message-IDヘッダの値を置き換えます。
$LIST_ATTACHMENTS_REMOVED$	添付ファイルをメールから削除した際、削除された添付ファイルを一覧表示します。
$LIST_VIRUSES_FOUND$	ウィルスがメッセージに発見された時、それらをリストします。
$MESSAGEFILENAME$	現在処理されているメッセージのファイル名と置き換わります。
$MESSAGEID$	メッセージIDの値から"<>"を取り除く以外は、上記の$HEADER:MESSAGE-ID$と同じです。
$PRIMARYDOMAIN$	ドメインマネージャ[165]で指定されているMDaemonのデフォルトドメイン名に置き換わります。
$PRIMARYIP$	ドメインマネージャ[165]で指定されているIPv4アドレス[167]に展開します。
$PRIMARYIP6$	ドメインマネージャ[165]で指定されているIPv6 address[167]に展開します。
$RECIPIENT$	メッセージ受信者の完全なアドレスとなります。
$RECIPIENTDOMAIN$	メッセージ受信者のドメイン名を挿入します。
$RECIPIENTMAILBOX$	受信者のメールボックスをリストします(メールアドレスの@マークの左側の値です)。
$REPLYTO$	メッセージの[Reply-to]ヘッダの値と置き換わります。

$SENDER$	メッセージの送信先の完全なアドレスに置き換わります。
$SENDERDOMAIN$	メッセージの送信者のドメイン名を挿入します(メールアドレスの@ マークの右側の値です)。
$SENDERMAILBOX$	送信者のメールボックスをリストします(メールアドレスの@ マークの左側の値です)。
$SUBJECT$	メッセージの件名に含まれたテキストを表示します。

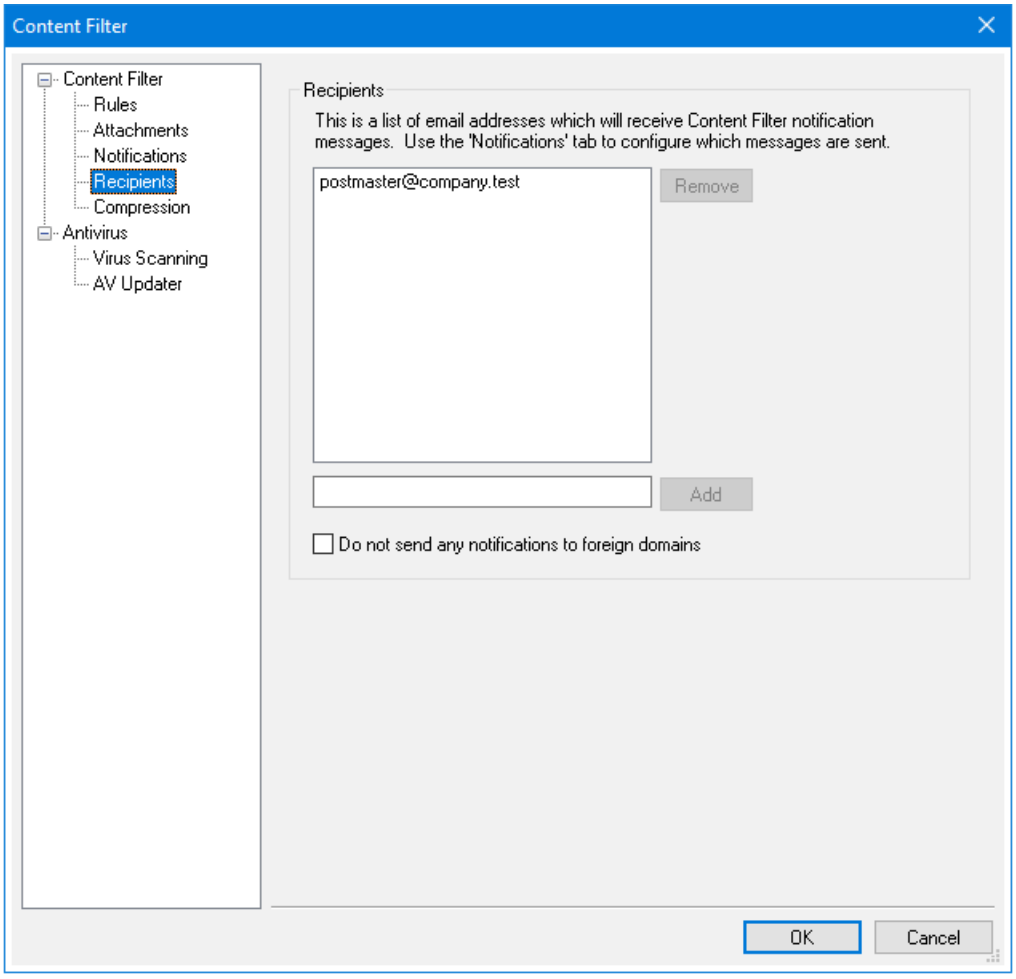
4.5.1.3.1 メッセージマクロ

利便性の向上のため、コンテンツフィルタで生成する通知やその他のメールにて、マクロを使用する事ができます。次のマクロを使用できます。

$ACTUALTO$	一部のメッセージは、書式換えまたはエイリアス文字変換の前にオリジナルユーザで入力されたように、通常、転送先のメールボックスとホストを示す"ActualTo"フィールドを含みます。このマクロは、その値で置き換えられます。
$AV_VERSION$	使用している AntiVirus のバージョン情報が表示されます。
$CURRENTTIME$	メールを処理した時間に置き換えられます。
$ACTUALFROM$	一部のメッセージは、書式換えまたはエイリアス文字変換の前にオリジナルユーザで入力されたように、通常、転送先のメールボックスとホストを示す"ActualFrom"フィールドを含みます。このマクロは、その値で置き換えられます。
$FILTERRULENAME$	メッセージが一致した条件のルール名に置き換えられます。
$FROM$	メールのFrom: へ含まれる全メールアドレスへ置き換えられます。
$FROMDOMAIN$	このマクロはメールのFrom: ヘッダにあるメールアドレスのドメイン名を挿入します。(メールアドレスの@ の右側の部分です)
$FROMMAILBOX$	このマクロはメールのFrom: ヘッダにあるメールアドレスのメールボックス名を挿入します。(メールアドレスの@ の左側の部分です)

GEN_GUID	11桁の英数字で構成されるユニークなIDを意味します。例: 0XVBASADTZC
$HEADER:XX$	このマクロはメールの再フォーマット時にヘッダの特定一に展開する値をxxとして指定します。例えば:元のメールで "TO: user01@example.com" が含まれていた場合、$HEADER:TO$ マクロは"user01@example.com"となります。元のメールに"Subject: This is the subject"が含まれていた場合、$HEADER:SUBJECT$ マクロは"This is the subject"という値に置き換えられます。
$HEADER:MESSAGE-ID$	上記の$HEADER: XX$と同様に、Message-IDヘッダの値を置き換えます。
$LIST_ATTACHMENTS_REMOVED$	添付ファイルをメールから削除した際、削除された添付ファイルを一覧表示します。
$LIST_VIRUSES_FOUND$	ウィルスがメッセージに発見された時、それらをリストします。
$MESSAGEFILENAME$	現在処理されているメッセージのファイル名と置き換わります。
$MESSAGEID$	メッセージIDの値から"<>"を取り除く以外は、上記の$HEADER: MESSAGE-ID$と同じです。
$PRIMARYDOMAIN$	ドメインマネージャ[165]で指定されているMDaemonのデフォルトドメイン名に置き換わります。
$PRIMARYIP$	ドメインマネージャ[165]で指定されているIPv4アドレス[167]に展開します。
$PRIMARYIP6$	ドメインマネージャ[165]で指定されているIPv6 address[167]に展開します。
$RECIPIENT$	メッセージ受信者の完全なアドレスとなります。
$RECIPIENTDOMAIN$	メッセージ受信者のドメイン名を挿入します。
$RECIPIENTMAILBOX$	受信者のメールボックスをリストします(メールアドレスの@マークの左側の値です)。
$REPLYTO$	メッセージの[Reply-to]ヘッダの値と置き換わります。
$SENDER$	メッセージの送信先の完全なアドレスに置き換わります。
$SENDERDOMAIN$	メッセージの送信者のドメイン名を挿入します(メールアドレスの@マークの右側の値です)。
$SENDERMAILBOX$	送信者のメールボックスをリストします(メールアドレスの@マークの左側の値です)。
$SUBJECT$	メッセージの件名に含まれたテキストを表示します。

4.5.1.4 宛先

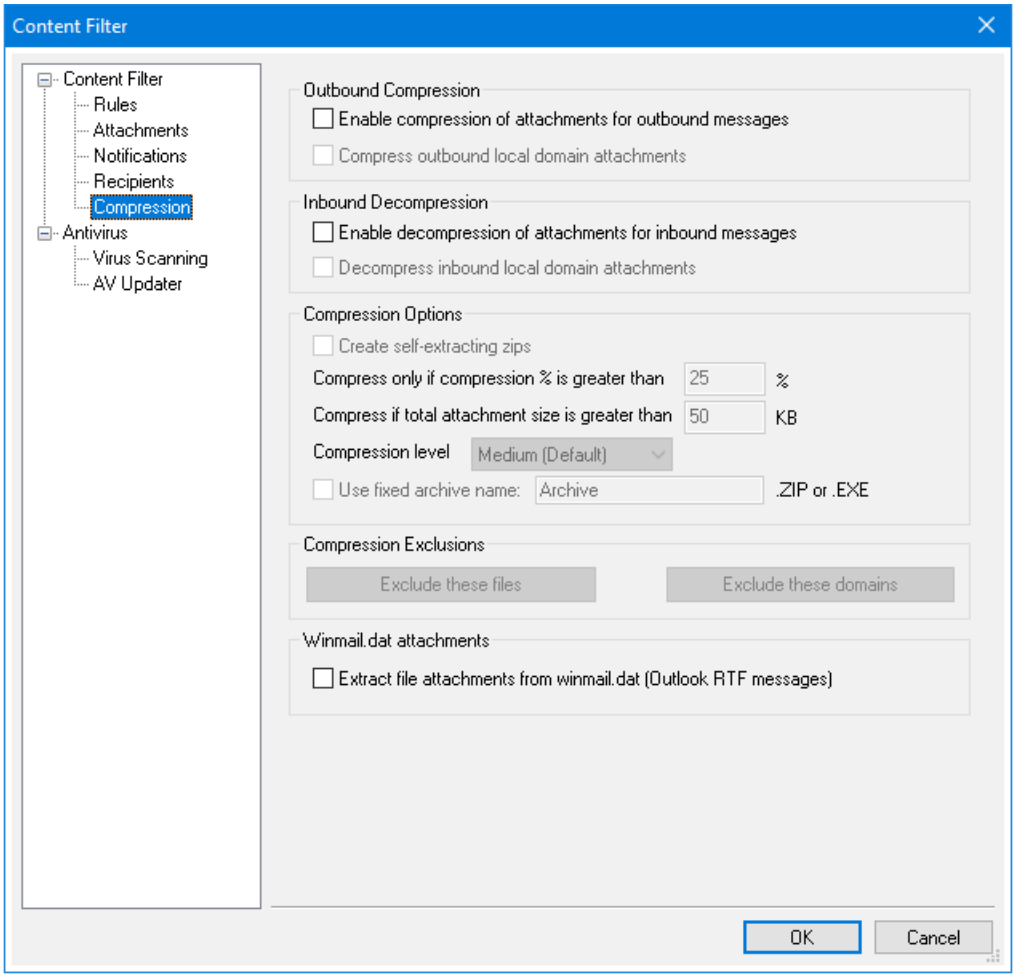


宛先

[通知]画面で設定した[**ウィルス通知メッセージを送る…**]オプションで指定した内容と同じものが表示されます。通知画面で管理者オプションが選択されると、これらのアドレスに通知メッセージが送られます。このセクションでアドレスを追加するには、フィールドにアドレスを入力して[**追加**]ボタンをクリックしてください。アドレスを削除する場合は、リストからアドレスを選択して[**削除**]ボタンをクリックしてください。

外部ドメインへは通知を送信しない
コンテンツフィルタ通知メールをローカルドメインの宛先のみに送信するにはこのチェックボックスを選択します。このオプションはデフォルトで無効です。

4.5.1.5 圧縮



このタブのコントロールを使用すると、メッセージが配信される前に、添付ファイルの自動圧縮や解凍を行うことができます。他のいくつかのパラメータや例外だけでなく圧縮のレベルをコントロールすることができます。この機能は、外部向けメールの送信に必要な帯域幅やスループットを大幅に減少させることができます。

送信時の圧縮

アウトバウンドメッセージの添付ファイルの圧縮を有効にする
アウトバウンドリモートメールメッセージの添付ファイルに対する自動圧縮機能を有効にする場合は、このチェックボックスを選択してください。このコントロールを有効にしても、すべての添付ファイルを圧縮するわけではありません。単に、この機能が有効になるだけです。アウトバウンドメッセージの添付ファイルが圧縮されるかどうかは、この画面の残りの設定によって決まります。

アウトバウンドローカルドメイン添付ファイルの圧縮
このコントロールを有効にすると、たとえ送信先が別のローカルアドレスであっても、すべてのアウトバウンドメールにファイル圧縮の設定が適用されます。

受信時の解凍

Inboundメッセージの添付ファイルの解凍を有効にする
Inboundリモートメールメッセージの添付ファイルの自動解凍機能を有効にする場合は、このチェックボックスを選択してください。メッセージがZIP形式の添付ファイルと共に受信された場合、その添付ファイルはローカルユーザのメールボックスへ配信する前に解凍されます。

Inboundローカルドメイン添付ファイルの解凍
ローカルメールに自動解凍を適用する場合は、このコントロールを有効にしてください。

圧縮オプション

自己解凍ZIPを作成
MDaemonが作成する圧縮ファイルを、.EXEファイル拡張子を持つ自己解凍のZIPファイルにする場合は、このチェックボックスを選択してください。この機能は、メッセージの受信者が解凍ユーティリティを持っているか不明な場合に便利な機能です。自己解凍ZIPファイルは、そのファイルをダブルクリックするだけで、解凍することができます。

指定%以上の場合だけ圧縮
このコントロールで指定される値より大きい比率で圧縮できる場合、MDaemonでは送信する前に、メッセージの添付ファイルを圧縮します。例えば、ここで20を指定し特定の添付ファイルが、少くとも21% までに圧縮することができない場合、MDaemonはメッセージを送信する前に、圧縮しません。

MDaemonは、どんな割合で圧縮することができるか判定するために、ファイルを最初に圧縮する必要があります。したがって、この機能は、ファイル圧縮を防止しません。指定された値以上にファイルを圧縮することができない時、圧縮形式の添付ファイルをしません。つまり、この値より更に圧縮することができないと検出すると、圧縮は無視され、メッセージは、そのまま添付ファイルで配信されます。

添付ファイルの総計が指定サイズ以上の場合圧縮する XX KB
添付ファイルの自動圧縮が有効な場合、合計サイズが、ここで指定された値を超える時のみ圧縮を行います。添付ファイルの圧縮合計サイズが、この値に到達しない場合は、メッセージは通常通り添付ファイルを変更しない状態で送信します。

圧縮レベル
添付ファイルの自動圧縮が有効な場合、合計サイズが、ここで指定された値を超える時のみ、圧縮を行います。添付ファイルの圧縮合計サイズが、この値に届かない場合は、そのメッセージは通常通り、添付ファイルを変更しない状態で送信します。

固定アーカイブを使用: [アーカイブ名]
自動圧縮された添付ファイルに、特定のファイル名を付ける場合は、このチェックボックスを選択して、名前を選択してください。

圧縮の除外

これらのファイルを除外...
自動圧縮機能から除外するファイルを指定するには、このボタンを選択します。圧縮設定に関係なく、メッセージ添付ファイルがこれらのファイル名の1つに合致する場合、圧縮されません。ワイルドカー

ドが、これらのエントリで使用できます。例えば、"*.exe"を指定すると、すべての". exe"を最後にもつファイルは圧縮されません。

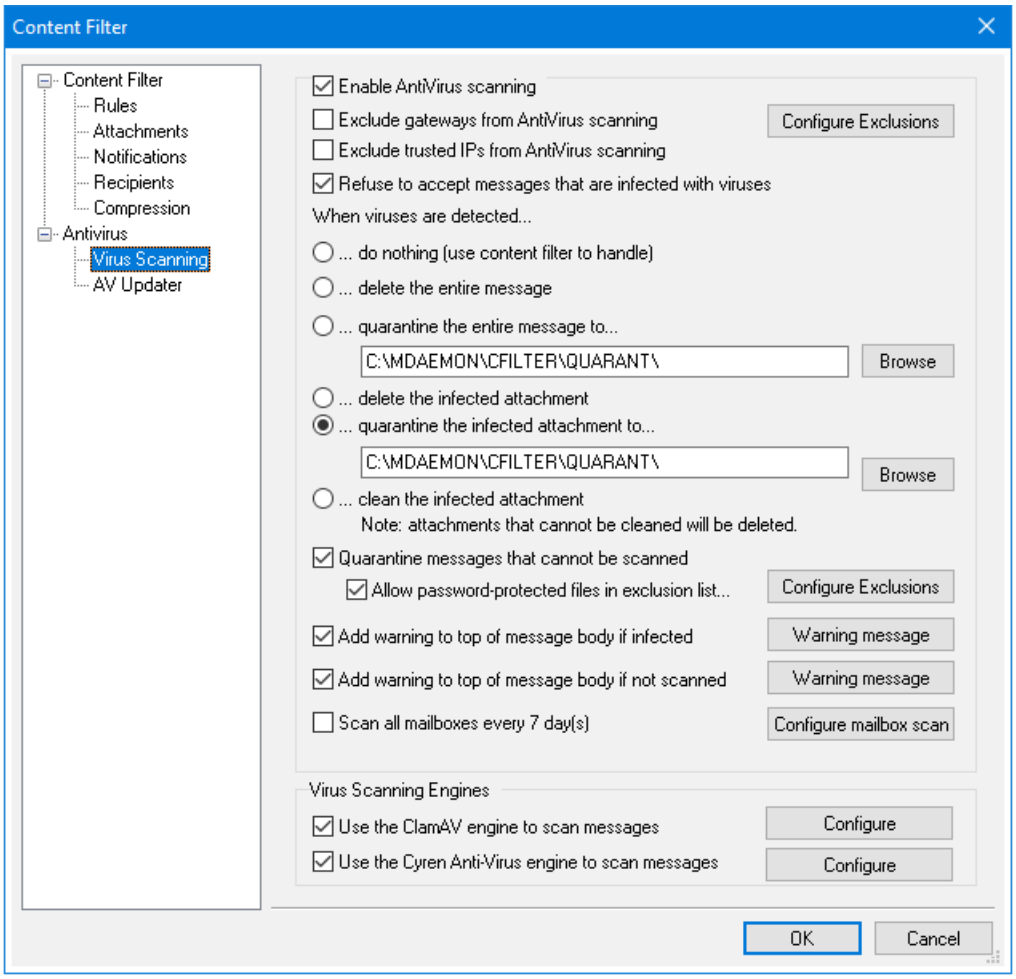
これらのドメインを除外...
このボタンをクリックすると、自動圧縮機能から除外するメッセージの受信ドメインを指定することができます。これらのドメイン宛てのメッセージの添付ファイルは、圧縮の設定にかかわらず圧縮されません。

Winmail.dat 添付ファイル

winmail.dat(Outlook RTF形式のメッセージ)から添付ファイルを取り出す
winmail.datから添付ファイルを取り出しMIME形式の添付ファイルへ変換するにはこのオプションを有効化します。

4.5.2 AntiVirus

4.5.2.1 ウィルススキャン



この画面のオプションはオプションの MDaemon AntiVirus 609 機能をご利用の場合のみ使用できます。MDaemon AntiVirusを初めて有効にすると、30日間の評価版として動作します。この機能を購入するには、MDaemon認定リセラーにご連絡するか、次のURLを参照してください: www.mdaemon.com

AntiVirusスキャンを有効

このチェックボックスを選択すると、メッセージのアンチウィルススキャンが有効になります。 MDaemonが添付ファイル付メールを受信すると、メールが宛先に到着する前にウィルスチェックを実行します。

AntiVirusスキャンからゲートウェイを除外

MDaemonのドメインゲートウェイ宛のメッセージをウィルススキャンから除外する場合、このチェックボックスを選択します。これは、ドメインで所有しているメールサーバ宛てのメールを除外した場合に便利です。ドメインゲートウェイに関する詳しい情報は、ゲートウェイマネージャ 227 をご覧ください。

除外設定

ウィルススキャンから除外する受信者のアドレスを指定する場合は、[除外設定]ボタンをクリックしてください。 対象アドレス宛てのメッセージはウィルススキャンされません。 このアドレスには、ワイルドカードを使用することができます。このため、この機能を、すべてのドメインまたはドメイン内の特定のメールボックスを除外するために使用することができます。例えば、*@example.comやVirusArchive@*などです。

信頼するIPをAntiVirusスキャンから除外

信頼するIPアドレス 473 からのメールをAntiVirusスキャンから除外する場合はこのオプションを有効にしてください。

ウィルスに感染したメッセージの受け入れを拒否

セッションが終了した後ではなくSMTPセッション中に、ウィルススキャンを受信メッセージで行い、ウィルスを含むメッセージを拒否する場合は、このオプションを選択します。MDaemonで正式にメッセージを受け入れる前に、各受信メッセージをスキャンしてセッションが終了するので、送信サーバは、今まで通り役割を果たします。したがって、ウィルスを検出する場合、メッセージを完全に拒否することができます。さらに、メッセージが拒否されたので、もうこれ以上、このダイアログで一覧にされるアンチウィルス関連の処置をしません。隔離または駆除を行わず通知メッセージも送信されません。これは、受信する感染メッセージおよびウィルス通知メッセージの数を劇的に減らすことができます。

SMTP-(受信)ログには、AntiVirus処理の結果が表示されます。次のような結果を確認できます。

- the message was scanned and found infected with a virus
  メールがスキャンされ、ウィルス感染が見つかりました。

- the message was scanned and no virus was found
  メールがスキャンされ、ウィルスは見つかりませんでした。

- the message could not be scanned (usually because a ZIP or other type or attachment could not be opened/accessed)
  メールをスキャンすることができませんでした。(通常はZIPなどの開くことができない添付ファイルのためです)

- the message could not be scanned (it exceeds the max size limit)
  メールをスキャンすることができませんでした。(許容サイズを超えています)

- an error occurred during the scan
  メールのスキャン中にエラーが発生しました。

ウィルスを検出した時...
このセクションのオプションボタンの1つをクリックすることにより、MDaemonがウィルスを検出した際の動作を指定することができます。

...何もしない(コンテンツフィルタを使用)
上記のすべてのアクションを行わずに、コンテンツフィルタのルールによって処理を行う場合は、このオプションを有効にしてください。

...メッセージ全体を削除
このオプションは、ウィルスが発見された場合、添付ファイルではなくメッセージ全体を削除します。これはメッセージ全体を削除するので、[**感染していたら警告メッセージをメッセージ本文の先頭に追加する**]というオプションは適用されません。しかし、[通知]画面のコントロールを使用することによって、受信者に通知メッセージを送ることは可能です。

...メッセージ全体を隔離する...
このオプションは[**メッセージ全体を削除**]という上記のオプションに似ていますが、メッセージは削除されるのではなく、指定された場所に隔離されます。

...感染ファイルを削除する
このオプションは感染した添付ファイルを削除します。メッセージは、感染した添付ファイルを持たずに配信されます。感染した添付ファイルが削除されたことをユーザに通知するテキストをメッセージに追加するには、このダイアログの一番下の[**感染していたら警告メッセージをメッセージ本文の先頭に追加する**]を使用してください。

...感染ファイルを隔離する...
このオプションを選択し、感染した添付ファイルを削除または消去するのではなく隔離する場合、隔離するフォルダを指定してください。[**感染添付ファイルを削除**]オプションと同様に、メッセージは、感染した添付ファイル無しで配信されます。

...感染ファイルを駆除する
このオプションを選択すると、AntiVirusは感染した添付ファイルの駆除を試みます。添付ファイルから駆除できない場合、添付ファイルを削除します。

スキャンできないメッセージを隔離
このオプションが有効の場合、MDaemonはパスワード保護されているファイルなどのスキャンできないメッセージを隔離します。

除外リストにあるパスワードファイルは除く
ファイル名や種類が除外設定に含まれており、且つ、パスワード保護のためスキャンできなかったファイルがAntiVirusスキャナーを通過できるようにするにはこのオプションを使用します。

感染していたら警告メッセージをメール本文の先頭に追加する
上記の[感染添付ファイルを…]というオプションが選択されている場合、このオプションをクリックすると、感染したメールの上部に警告メッセージを追加することができます。メッセージの受信者に、添付ファイルが取り除かれている事実とその理由を知らせることができます。

警告メッセージ…
このボタンで感染していたメールの上部へ追加する警告メッセージが表示されます。必要な変更を行った後、**OK**をクリックするとダイアログが閉じ、変更が保存されます。

スキャンできない場合には、メッセージ本文の上部に警告メッセージを追加する
このオプションが有効の場合、MDaemonはスキャンできないメールの上部に警告メッセージを追加できます。

警告メッセージ…
このボタンでスキャンできないメールの上部へ追加する警告メッセージが表示されます。必要な変更を行った後、 **OK**をクリックするとダイアログが閉じ、変更が保存されます。

全てのメールボックスをn日毎にスキャン
このオプションを有効化すると、保存されているメールボックスを定期的にスキャンし、ウィルス定義ファイルがアップデートされる前に通過した感染メールを検出する事ができます。感染メールは隔離フォルダへ移動され、 X-MDBadQueue-Reasonヘッダが追加され、MDaemon上で隔離された理由を確認できるようになります。スキャンできないメッセージは隔離されません。

メールボックスのスキャン設定
このボタンをクリックし、どの頻度でメッセージをスキャンするのかや何日前のメールまでをスキャン対象とするのかを指定する事ができます。また、ここからメールボックススキャンを手動ですぐに実行する事もできます。

ウィルススキャンエンジン

MDaemon AntiVirusにはClamAVとIKARUS Anti-Virusの2つのエンジンが搭載されています。両方が有効の場合、メールは最初にIKARUS Anti-Virus、次にClamAVの、両エンジンでスキャンされます。これにより、ウィルス対策用のレイヤーが追加される事となり、1つのエンジンのシグニチャが更新される前にウィルスが発生する場合がある、という潜在的なリスクに対応する事ができます。

ClamAVエンジンをメールのスキャンに使用する
ClamAVエンジンをメールのウィルスチェックに使用する場合はこのチェックボックスをクリックします。

設定
このボタンをクリックすると、ClamAVのデバッグログのアクティベーションを行えます。 ログファイルはMDaemonのlogsフォルダへ生成されます。

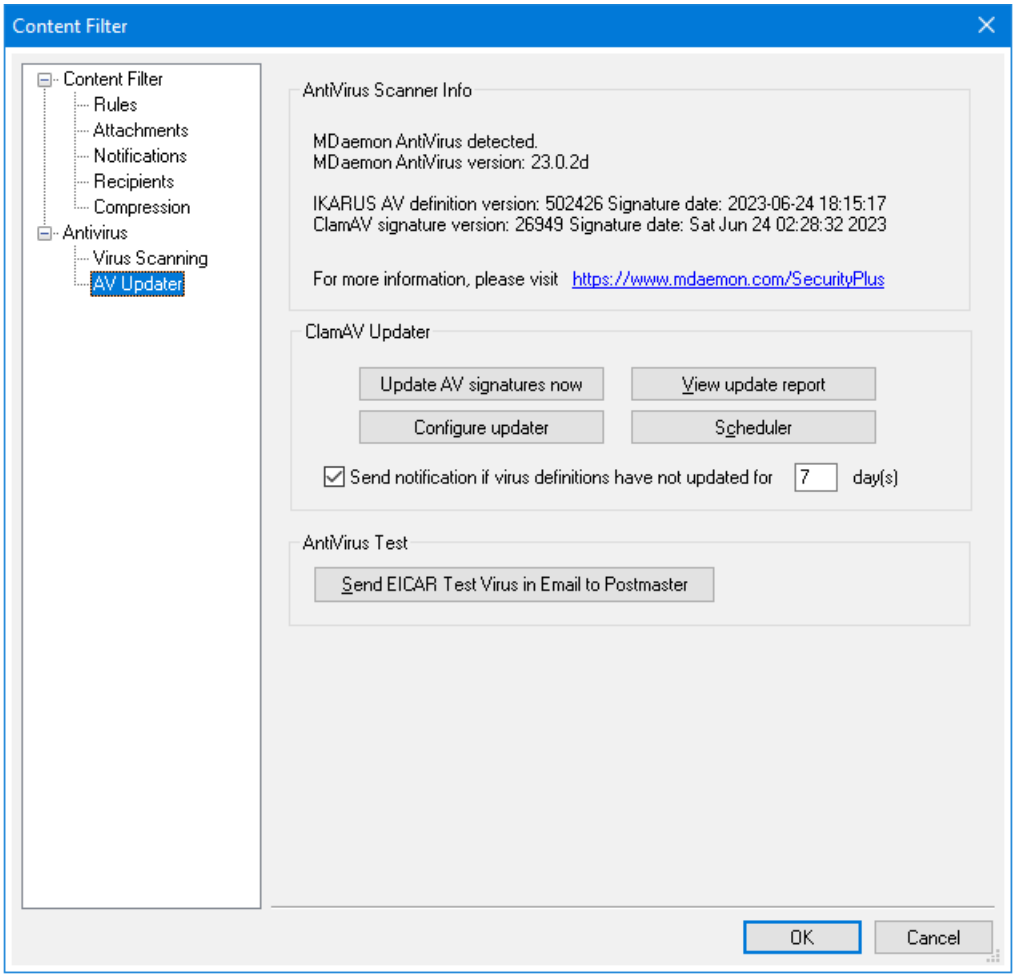
IKARUS Anti-Virusエンジンをメールのスキャンに使 用 する
IKARUS Anti-virusエンジンをメールのウィルスチェックに使 用 する場 合 はこのチェックボックスをクリックします。

設 定
マクロを含 む添 付 ファイルをウィルスとみなす場 合 このオプションを使 用します。ヒューリスティックレベルを-1から5の間 で指 定 できます。-1は自 動 で、0は無 効 の意 味 となり、1-5が低 い方 から高 い方 へのヒューリスティックレベルを意 味します。

参照:

AVアップデータ 613
コンテンツフィルタとAntiVirus 587

4.5.2.2 AVアップデータ



この画面のオプションはオプションの MDaemon AntiVirus 609 機能をご利用の場合のみ使用できます。MDaemon AntiVirusを初めて有効にすると、30日間の評価版として動作します。この機能を購入するには、MDaemon認定リセラーにご連絡するか、次のURLを参照してください: www.mdaemon.com

手動または自動でAntiVirusのウィルス定義のアップデートをするには、このタブを使用します。自動更新のスケジューラ、いつ、どのアップデートがダウンロードされたかレビューすることができるレポートビューア、ウィルススキャンが適切に稼働しているか確認するために使用するテスト機能があります。

アンチウィルススキャン情報

このセクションには、インストールされているAntiVirusのバージョンや最後の更新日などが表示されます。

ClamAVアンチウィルスアップデータ

AV署名をすぐにアップデートする

このボタンをクリックし、ウィルスの定義ファイルを手動でアップデートします。アップデータはすぐに接続を行います。

アップデータの構成

このボタンをクリックすると、アップデータ構成 615 が開きます。アップデータには、アップデートURL、接続、プロキシ、その他画面があります。

更新レポートの表示

[更新レポートの表示]ボタンをクリックし、アンチウィルスログビューアを起動します。このビューアには、各アップデートに関する回数、取られたアクション、その他の情報が表示されます。

スケジューラ

このボタンをクリックすると、MDaemonのAntiVirus更新 345 が開きます。ここでは特定の日時か指定間隔でウィルスの定義ファイルのアップデートを確認するスケジュールを設定します。

ウィルス定義ファイルがxx日間更新されなかった際、通知メールを送信する

デフォルトで管理者はClamAVウィルス定義ファイルがここで指定した日数の間で更新がなかった場合は通知メールを受信します。

AntiVirusのテスト

PostmasterへメールでEICAR Test Virusを送る

このボタンをクリックすると、EICARウィルスファイルが添付されたテストメッセージを、Postmasterへ送信することができます。この添付ファイルは無害で、AntiVirusテストのためのみに使用されます。MDaemonのメイン画面のコンテンツフィルタログウィンドウを見ることによって、MDaemonがこのメッセージを受け取った時にどのような動作をするかを確認することができます。例えば、設定にもよりますが、以下のようなログの抜粋が表示されます:

```
Mon 2008-02-25 18:14:49: Processing C:\MDAEMON\LOCALQ\md75000001128.msg
Mon 2008-02-25 18:14:49: > eicar.com (C:
\MDaemon\CFilter\TEMP\cf1772420862.att)
Mon 2008-02-25 18:14:49: > Message from: postmaster@example.com
Mon 2008-02-25 18:14:49: > Message to: postmaster@example.com
```

```
Mon 2008-02-25 18:14:49: > Message subject: EICAR Test Message
Mon 2008-02-25 18:14:49: > Message ID:
<MDAEMON10001200202251814.AA1447619@example.com>
Mon 2008-02-25 18:14:49: Performing viral scan...
Mon 2008-02-25 18:14:50: > eicar.com is infected by EICAR-Test-File
Mon 2008-02-25 18:14:50: > eicar.com was removed from message
Mon 2008-02-25 18:14:50: > eicar.com quarantined to C:
\MDAEMON\CFILTER\QUARANT\
Mon 2008-02-25 18:14:50: > Total attachments scanned    : 1 (including
multipart/alternatives)
Mon 2008-02-25 18:14:50: > Total attachments infected   : 1
Mon 2008-02-25 18:14:50: > Total attachments disinfected: 0
Mon 2008-02-25 18:14:50: > Total attachments removed    : 1
Mon 2008-02-25 18:14:50: > Total errors while scanning  : 0
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (sender)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (recipient)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (admin)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (admin)
Mon 2002-02-25 18:14:50: Processing complete (matched 0 of 12 active
rules)
```

参照:

アップデータ構成ダイアログ 615
AntiVirus 609
コンテンツフィルタとAntiVirus 587

4.5.2.2.1 アップデータ構成ダイアログ

AVアップデータ 613 画面でアップデータの構成ボタンをクリックすると、AVアップデータ設定ダイアログが現れます。このダイアログには4つの画面があります。

URLの更新
アップデートURLタブは、AntiVirusがアップデートでチェックするサーバを指定するために使用されます。AntiVirusでアップデートサーバーを順番にチェックするか、ランダムにチェックするかを選択する事ができます。

接続
接続タブは AntiVirusが、アップデートサイトに接続する時に使用する、インターネット接続のプロファイルを指定できます。[コントロールパネルのインターネット接続を使用]というオプションはデフォルトのインターネット接続の設定を使用します。接続プロファイルの選択や、ユーザ名とパスワードの設定を手動で行う場合は、[手動でインターネット接続を設定]というオプションと、それに付随するコントロールを使用してください。

プロキシ
プロキシ画面には、現在のネットワーク構成がアップデートサイトに接続するために必要とする、HTTPやFTPプロキシの設定のオプションがあります。

その他
その他画面には、アップデータのロギング状態を管理するオプションが含まれます。アップデータの動作をログファイルに記録することができ、そのファイルの最大サイズを指定することができます。

参照:

AVアップデータ 613
AntiVirus 609
コンテンツフィルタとAntiVirus 587

4.6 スパムフィルタ

4.6.1 スパムフィルタ

機能性の高いスパム防止ツールであるスパムフィルタがさらに強化されました。スパムフィルタは、着信メールを検査するために複雑なルールの[スコア]を計算する新しい技術を提供します。この[スコア]はスパムの可能性があるメールを判断するために使用され、それに対して受信を拒否する、フラグ付けなどの必要な処置を行うことができます。

アドレスは、許可や拒否、あるいはスパムフィルタの検査から完全に除外することもできます。また、メッセージにスパムのスコアやそのスコアがどのようにして計算されたかを示すスパムレポートを挿入することも可能です。あるいは個別のメールとしてレポートを生成し、そこに含まれるオリジナルのスパムメールを添付することも可能です。さらに、スパムフィルタがスパムを継続的にチェックする事で検出精度を向上させる事ができるベイジアン学習 620(Bayesian learning)を使用することができます。

また、フィルタのルールは数千種類もの既知のスパムメッセージを検証することにより最適化されていますので、スパムの検知に関しては非常に信頼できるものになっています。しかし、特別な設定を必要とする場合は、スパムフィルタの設定ファイルを編集することにより、新しいルールを追加やルールをカスタマイズが可能です。

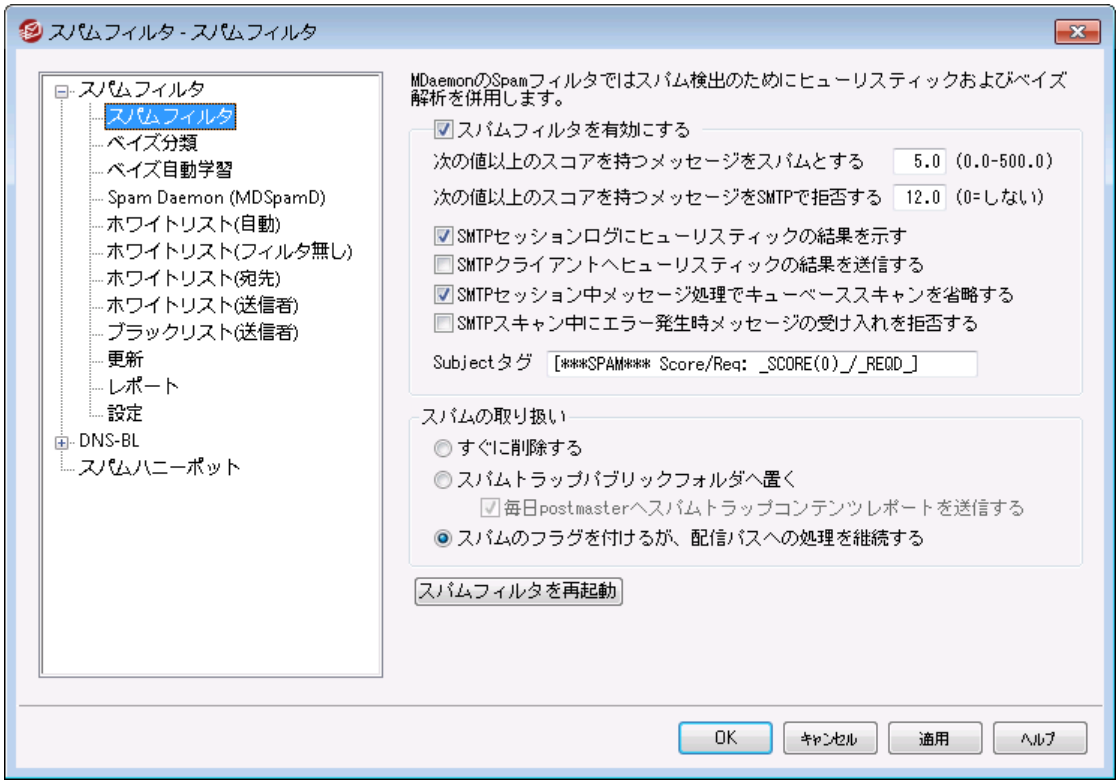
MDaemonのスパムフィルタは、ポピュラーな統合されたオープンソースのヒューリスティック(経験則に基づいた)技術を使用します。オープンソースプロジェクトのURLは以下の通りです。

http://www.spamassassin.org

参照:

スパムフィルタ 617
DNSブロックリスト 638

4.6.1.1 スパムフィルタ



スパムフィルタを有効にする

ヒューリスティックメッセージをスコアリング、スパムフィルタリングシステムを起動するには、このチェックボックスを選択します。このオプションが有効にするまで、この画面の他のスパムフィルタオプションのいずれも利用できません。

メッセージスコアが次の値以上ならばスパムとする [XX] (0.0-500.0)
ここへ指定する値は、MDaemonが各メッセージのスパムスコアに比較する必要とするスパムしきい値です。この合計以上のスパムスコアをもつメッセージはスパムと見なされ、適切な処置が他のスパムフィルタの設定に基づいて行われます。

次の数以上のスコアを持つメッセージをSMTPで拒否する XX (0=なし)
スパムスコア拒否しきい値を指定するために、このオプションを使用します。メッセージのスパムスコアが、このスコア以上の場合、残りのオプションで続行し配信するのではなく完全に拒否されます。このオプションの値は、上記の[メッセージスコアが次の値以上ならばスパムとする"オプションの値より常に大きいです。一方、メッセージはスパムと見なされず、残りのスパムフィルタのオプションが適用されません。単に配信中に、拒否されます。このオプションで、SMTPプロセス中に、スキャンすることを無効にする、、スコアに関係なくMDaemonが任意のメッセージを拒否しない場合、"0"を使用します。SMTPスキャンが無効にされる場合、受け入れられた後で、キューベースのスキャンはメッセージに関して今まで通り実行されます。このオプションのデフォルト設定は、12.0です。

例：

5.0に設定されるスパムスコアしきい値と10.0に設定される拒否しきい値を持つ場合、5.0以上であるが10.0未満であるスパムスコアによるメッセージは、スパムと見なされ、残りのスパムフィルタの設定に

したがって処理されます。10.0以上のスパムスコアによるメッセージは、配信プロセス中に、MDaemonによって拒否されます。

時間とともにスパムフィルタのパフォーマンスをモニタして、必要性に適している両方のスパムおよび拒否しきい値を調整します。比較的少ない検出漏れ(認識できないものを通り抜けたスパム)およびまれに誤検出(非スパムをスパムのフラグを付ける)で、5.0のスパムスコアしきい値は、多くのスパムを捕えます。10-15の拒否しきい値によって、拒否されるスパムであるメッセージを確実に捕らえます。正当なメッセージが、高いスコアを持つことは非常にまれです。デフォルト拒否しきい値は12です。

SMTPセッションログにヒューリスティックの結果を示す
SMTPセッションログ[159]にSMTPセッションの間、ヒューリスティック処理の結果を記録するために、このオプションを選択します。

SMTPクライアントへヒューリスティックの結果を送信する
SMTPセッションコピーでヒューリスティック処理結果インラインを表示するために、このオプションを選択します。"0"(スパムがそのスコアのために拒否されない)に設定されるスパムスコア拒否しきい値を持つ時に、このオプションは利用可能でありません。詳細は、上記の「次の数以上のスコアを持つメッセージをSMTPで拒否するXX(0=なし)」を参照。

SMTPセッション中メッセージ処理でキューベーススキャンを省略する
MDaemonのデフォルトでは、SMTPセッション中のすべてのメッセージに対して、上記のスパムスコアが拒否のしきい値を越えているかスキャンを行います。MDaemonにより受け入れられたメッセージには、その後他のキューベースのスキャンが行われ、そのスコアとスパムフィルタの構成に従う処理がされます。このオプションを有効にすると、キューベースのスキャンを省略し、最終的なものとして最初のスパムフィルタスキャンの結果を処理します。これによりCPUの負荷を大幅に軽減でき、アンチスパムのシステム効率を上げることができます。しかし、キューベースのスキャンが省略される場合は、デフォルトのSpamAssassinヘッダのみがメッセージに追加されます。local.cfファイルでデフォルトのSpamAssassinヘッダや特定のカスタムヘッダに任意の変更を行った場合、これらの変更や追加は無視されます。

SMTPスキャン中にエラー発生時メッセージの受け入れを拒否する
SMTP処理中のスキャンにエラーが発生した場合、メッセージを拒否する時は、このオプションを選択します。

Subjectタグ
このタグは、設定されたしきい値以上のスパムスコアを持つメッセージのSubjectヘッダの最初に挿入されます。スパムスコアに関する情報を持つことができ、メッセージを検索するためにIMAPメッセージフィルタを使用し、それに応じたフィルタリング(スパムメッセージの配信を継続するスパムフィルタを持つとみなす)をすることができます。これは、指定された"spam"フォルダに自動的にスパムメッセージを割り振るためのシンプルな方法です。動的にメッセージのスパムスコアおよび必要とされたスパムしきい値の値を挿入する場合、メッセージのスコアにタグ"_HITS_"および必要とするしきい値には"_REQD_"を使用してください。
これ以外に、"_HITS_"の代わりに"_SCORE(0)_"を使用することができます。これはより低いスコアに前置ゼロを挿入しこれはより低いスコアに前置ゼロを挿入します。そして、一部のメールクライアントで件名によってメッセージをソートする時に、該当するソート順を確保するために便利です。あるいは[_HITS_]の代わりに[_SCORE(0)_]を使用することもできます。これは前置きゼロを下のスコアに挿入するので、メールクライアントでSubjectを使用してメッセージをソートする場合、正確にソートすることができます。

例えば

subject タグを
SPAM Score/Req: _HITS_/_REQD
に設定すると、スパムメッセージのスコアが6.2で、そのsubjectは
SPAM Score/Req: 6.2/5.0 – Hey, here's some spam!
となります。

"_HITS_"の部分に"_SCORE(0)_"と置き換えると、
"***SPAM*** Score/Req: 06.2/5.0 – Hey, here's some spam!"
となります。

subjectヘッダによる変更を使用したくない場合は、ここをブランクにしてください。Subjectタグは挿入されません。

スパムフィルタ処理について別のサーバのMDaemonスパムデーモン（MDSpamD）を使用するMDaemonを構成する場合、このオプションは利用できません。Subjectタグ設定は、他のサーバの設定で決定されます。詳しくはSpam Daemon[625]を参照してください。

スパムの取扱い

メッセージのスパムスコアが、上記で指定されたスコア以上である場合、スパムフィルタは、下記で選択される機能を実行します。

...すぐ削除する
スパムスコアが指定された値を超えた場合、メッセージを削除する場合は、このオプションを選択してください。

...スパムトラップパブリックフォルダへ置く
スコアを超えたメッセージを配信するのではなく、スパムとしてメッセージをにフラグを付け、スパムパブリックフォルダへ移動するには、このオプションを選択します。

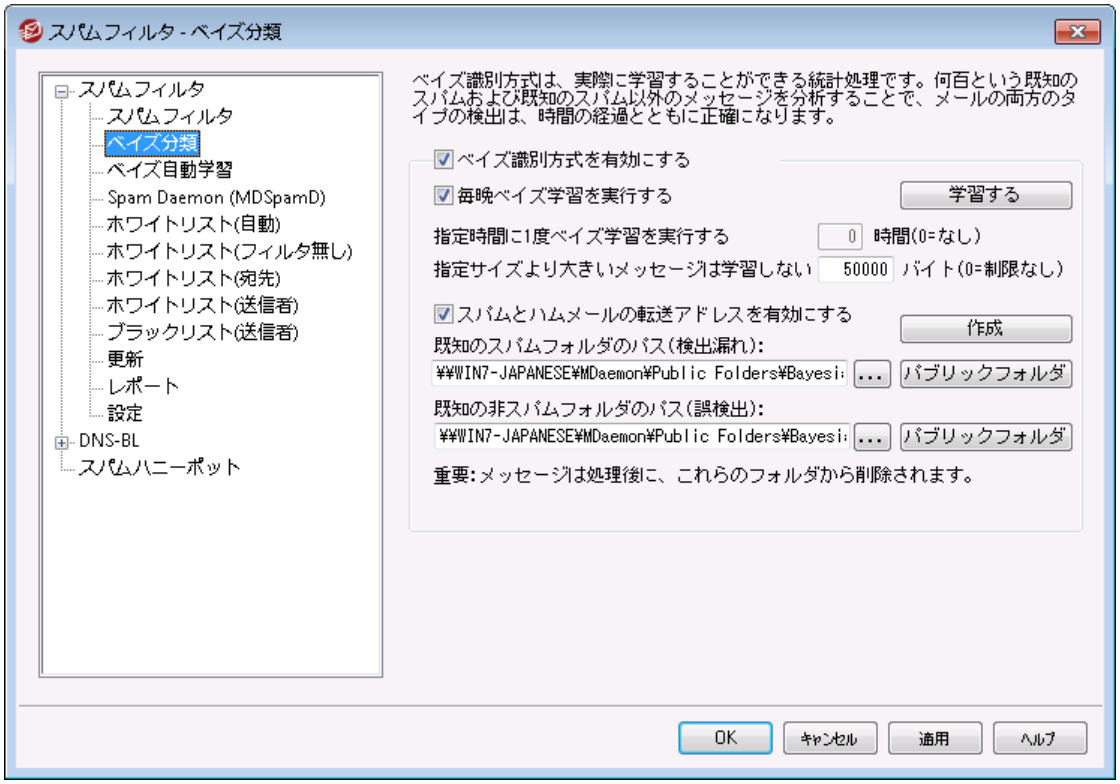
毎日postmasterへスパムトラップコンテントレポートを送信する
上記の[スパムトラップパブリックフォルダへ置く]オプションを選択した場合に、このチェックボックスをクリックすると、Postmaster宛にフォルダ内容のサマリを送信します。

...スパムにフラグを付けるが配信パスへの処理を継続する
受信者への各スパムメッセージの配信を継続するが、各スパムヘッダを挿入すること、あるいは上記で指定したタグおよびレポート[635]画面でスパムとしてフラグを付ける場合、このオプションを選択します。これはデフォルトオプションで、例えば、レビューのためにスパムフォルダにメールをフィルタするよう、ユーザがオプションの利用でき、誤ってスパム（すなわち誤検出）ラベル付けされる可能性があるメッセージを見失うことを回避します。

スパムフィルタを再起動

ボタンをクリックしてスパムフィルタエンジンを再起動します。

4.6.1.2 ベイジアン分類



MDaemonのスパムフィルタ処理に、別サーバーで稼働しているMDaemon Spam Daemon(MDSpamD)を使うよう設定した場合、ベイジアン分類は利用できません。ベイジアン学習は、他のサーバで実行されます。詳しくは Spam Daemon 625 画面を参照してください。

スパムフィルタはベイジアン学習をサポートしています。これは、スパム認識の信頼度を増加させるために、スパムおよび非スパムメッセージを分析するために自由に使用することができる、統計的なプロセスです。スパムメッセージと非スパムメッセージ用にフォルダを指定して、一定の間隔で手動または自動的にスキャンすることができます。そのフォルダ内のすべてのメッセージは、分析されインデックス化されるので、スパムに類似したものを判断するために新しいメッセージをそれらと比較することが可能です。そして、そのベイジアンによる比較の結果によって、スパムフィルタのスパムスコアの増減が可能です。

ベイジアン分析が、自動学習 623 画面で指定されたスパムおよび非スパムメッセージ数で実行されるまで、スパムフィルタはメッセージにベイジアン分類を適用しません。これはベイジアン比較を行う場合に、スパムフィルタが十分な数の引数を持つために必要な行程です。指定された数のメッセージ分析が実行されれば、個々に受信されるメッセージのスパムスコアにベイジアン比較の結果を適用するのに十分となります。さらに多くのメッセージを分析し続けることにより、ベイジアン分類は徐々に正確になります。

ベイジアンによる分類

Bayesian classificationを有効にする
各メッセージのスパムスコアに、現在既知のベイズ統計との比較に基づいて調整する場合、このチェックボックスを選択してください。

毎晩ベイズ学習を実行する
このオプションが有効な場合、一日に一度深夜にベイジアン学習が行われ、以下に指定するスパムあるいは非スパムフォルダ内のすべてのメッセージが削除されます。これ以外の間隔でベイジアン学習を行う場合は、このオプションを無効にして、以下の[**指定時間に一度ベイジアン学習を実行する**]オプションを使用します。ベイジアン学習を自動的に行わない場合は、このオプションを無効にし、以下のオプションに0(ゼロ)を入力してください。

指定時間に1度ベイズ学習を実行するXX時間(0=なし)
一日に一度深夜以外に、ある一定の間隔でベイジアン学習を行う場合は、上記の[**毎晩深夜にベイジアン学習を行うようにスケジュールする**]オプションを無効にし、このオプションに時間を指定します。ここに入力した時間が経過すると、ベイジアン学習が行われ、以下に指定するスパムあるいは非スパムフォルダ内のすべてのメッセージが削除されます。ベイジアン学習を自動的に行いたくない場合は、このオプションを無効にして以下のオプションに0(ゼロ)を入力してください。

> 一部の理由により、分析後にメッセージの削除をしない場合、¥MDaemon¥App¥サブフォルダでLEARN.BATをMYLEARN.BATへコピー、そのファイルの最下付近の"if exist"で始まる2行を削除して防ぐことができます。MYLEARN.BATファイルが、¥MDaemon¥Appフォルダに存在する時、MDaemonはMYLEARN.BATを使用します。詳細は¥MDaemon¥SpamAssassin¥サブフォルダでSA-Learn.txtを参照のこと。 ヒューリスティック スパム フィルタリング技術と、ベイジアン学習に関するより詳しい情報に関しては、以下のウェブサイトを参照してください。
>
> http://www.spamassassin.org/doc/sa-learn.html.

指定サイズより大きいメッセージは学習しないXXバイト(0=制限なし)
ベイジアン分析を行うメッセージの最大サイズをキロバイトで入力します。ここで指定した値より大きなサイズのメッセージは分析されません。ここに0(ゼロ)を入力すると、そのサイズに関わらずすべてのメッセージが分析されます。

学習する
指定したフォルダに対して自動的に行われるベイジアン分析を待たずに、手動で分析を行う場合は、このボタンをクリックしてください。

SpamHam転送アドレスを有効にする
ユーザがスパムメールおよび非スパム(Ham)メールを指定したアドレスに転送して、ベイジアンシステムに学習させることを許可する場合は、このオプションを有効にしてください。
MDaemonで使用するデフォルトアドレスはSpamLearn@<domain>とHamLearn@<domain>です。このアドレスに送信されるメールは、SMTP AUTHで認証されたSMTPセッションを経由して受信される必要があります。と同時にこれらのメールは、[message/rfc822]タイプの添付として扱われます。これ以外の形式でこのアドレスに送信されるメールは処理されません。

以下の[CFILTER.INI]ファイル内のキーを追加することにより、MDaemonで使用するアドレスを変更することができます。

```
[SpamFilter]
SpamLearnAddress=MySpamLearnAddress@
HamLearnAddress=MyNonSpamLearnAddress@
```

注意： ここで使用するアドレスは@ で終わるようにしてください。

作成
自動的にSpamと非スパムのパブリックIMAPフォルダ105を作成し、設定するためにはこのボタンをクリックしてください。以下のフォルダが作成されます。

\Bayesian Learning.IMAP\	IMAPのルートフォルダ
\Bayesian Learning.IMAP\Spam.IMAP\	検出漏れ用（スパムメールの通過）= フラグされるまでのスコアにいたらなかったスパムメール
\Bayesian Learning.IMAP\Non-Spam.IMAP\	誤検出用（非スパムメールの遮断）= スパムではないのにスコアの誤りによってスパムとしてフラグされたメール

デフォルトでは、このフォルダへのアクセス権はローカルドメインのローカルユーザのみにあり検索と挿入の権限があります。Postmasterのデフォルト権限は検索、閲覧、挿入および削除です。

既知のスパムフォルダのパス（検出漏れ）:
これは既知のスパムメッセージをベイジアン分析で使用するフォルダへのパスです。このフォルダにはスパムと思われるメッセージのみコピーしてください。自動学習623またはスパムハニーポット644オプションで、スパムと思われるメッセージのみコピーを実行しない限り、メッセージをこのフォルダへコピーするプロセスを自動化するべきでありません。この自動処理を行うと、非スパムメッセージがスパムとして分析され、ベイジアン統計の信頼性を低下させる可能性があります。

既知の非スパムフォルダのパス（誤検出）:
これは、明確にスパムでないメッセージのベイジアン分析を使用するフォルダのパスです。スパムとみなさないメッセージのみ、このフォルダへコピーされます。自動学習623で、スパムとみなさないメッセージのコピーを実行しない限り、メッセージをこのフォルダへコピーするプロセスを自動化するべきでありません。この自動処理を行うと、非スパムメッセージがスパムとして分析され、ベイジアン統計の信頼性を低下させる可能性があります。

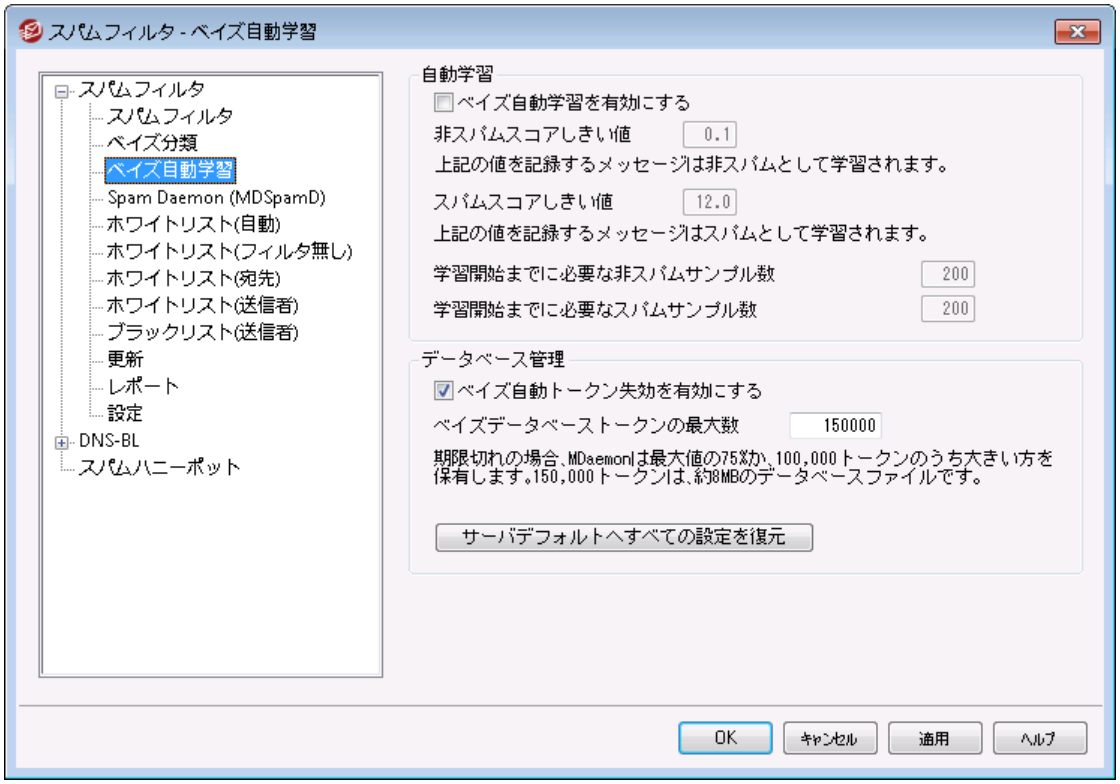
パブリックフォルダ
これらのボタンのどちらかをクリックすると、パブリックフォルダの1つをベイジアンディレクトリとして指定することができます。これはユーザが彼らのメッセージを、スパムあるいは非スパムとして不正確な分類のままにベイジアン分析用のディレクトリに移動する簡単な方法です。しかしこの方法により、より多くのユーザがメッセージを間違ったフォルダへ移動してしまい、分析の信頼性を低下させる可能性があるという点にご注意ください。

メールクライアント、Windowsのエクスプローラなどによりパブリックフォルダの名前を変更した場合、その新しいフォルダへのパスを手動で変更する必要があります。フォルダの名前を変更したにもかかわらず、ここでそのフォルダへのパスを変更しなかった場合は、スパムフィルタは古いフォルダへのパスをベイジアンフォルダへのパスとして使い続けます。

参照:

自動学習 623
スパムハニーポット 644

4.6.1.3 ベイジアン自動学習



MDaemonのスパムフィルタ処理に、別サーバーで稼働しているMDaemon Spam Daemon(MDSpamD)を使うよう設定した場合、ベイジアン自動学習は利用できません。ベイジアン学習は、他のサーバで実行されます。詳しくはSpam Daemon 625 画面を参照してください。

自動学習

ベイジアン自動学習を有効にする
ベイジアン自動学習によって、スパムと非スパムのしきい値を指定することができます。スパムおよび非スパムフォルダにおいて、手動でメッセージを配置するのではなく、自動的にメッセージから学習するためのベイジアン学習システム用に許可します。非スパムしきい値は以下のスコアは自動学習機能により非スパムとして扱われます。スパムしきい値が上のメッセージスコアでは、スパムとして扱われます。自動学習で、データベース(データベース管理: 下記で参照)から取り除かれる古い期限切れのトー

クンは、自動的に置き換えることができます。これは、期限切れのトークンのリカバリするために手動の再学習が必要ありません。しきい値をセットする際に慎重である場合、自動学習は、フォルダで不適切に分類されたメッセージを配置することを回避するために役立ちます。

非スパムのしきい値
この値以下のスパムスコアを持つメッセージは、ベイジアン分類システムにより非スパムとして扱われます。

スパムスコアしきい値
この値以上のスパムスコアを持つメッセージは、ベイジアン分類システムによりスパムとして扱われます。

学習前に必要な非スパムサンプル
スパムフィルタは、非スパムメッセージ(そして、次のオプションで指定されるスパムメッセージ)の数がベイジアンシステムによって分析されるまで、ベイジアン分類をメッセージに適用しません。これは、ベイジアン比較をするときに、寄り集まる統計量に充分なプールをスパムフィルタが有するために必要です。システムに分析するメッセージを与えるならば、ベイジアン比較の結果を各受信メッセージのスパムスコアに適用し始めるために十分に備えられます。より多くのメッセージも分析し続けることで、ベイジアン分類は、時間とともにより正確になります。

学習前に必要なスパムサンプル
前のオプションが非スパムメッセージに適用する通りで、このオプションはスパムフィルタがベイジアン分類をメッセージに適用し始める前に、分析される必要があるスパムメッセージの数を指定します。

データベース管理

ベイジアン自動トークンを有効にする
ここに指定されたトークンの数に到達したら、ベイジアンシステムがデータベーストークンを自動的に期限切れにするようにする場合は、このオプションを有効にしてください。トークンの上限を設定すれば、ベイジアンのデータベースが過度に大きくなるのを防ぐことができます。

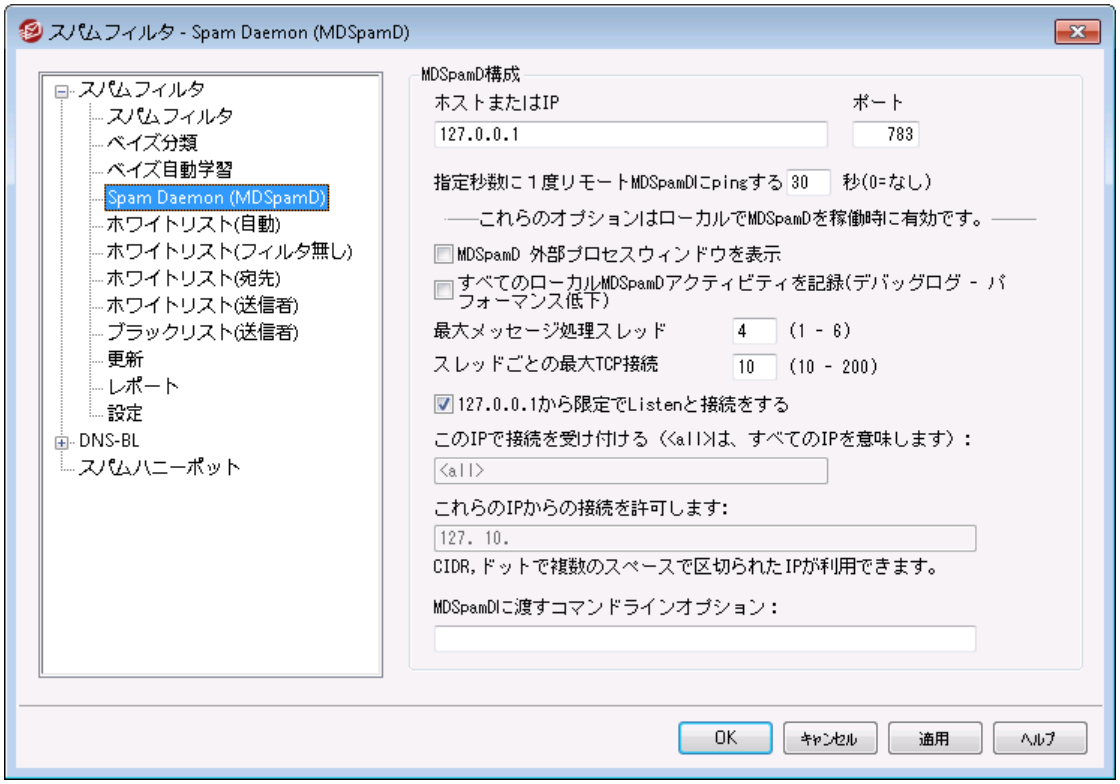
ベイジアンデータベーストークンの最大値
ここにはベイジアンデータベーストークンの許容最大値を入力してください。ここに入力された数値に達した場合、ベイジアンシステムは一番古いデータから削除を始め、全体の75% あるいは100,000トークンのどちらか高い方の数値まで削除しますが、期限切れのトークンの数にかかわらず、そのどちらかの大きい方の数字以下になることはありません。注意:150,000トークンは約8MBになります。

サーバデフォルトへすべての設定を復元
すべてのベイジアンの詳細オプションをデフォルト値に戻す場合はこのボタンをクリックしてください。

参照:

Bayesian分類 620
スパムハニーポット 644

4.6.1.4 Spam Daemon (MDSpamD)



MDaemonのスパムフィルタリングシステムは、独立したデーモンであるMDaemon Spam Daemon(MDSpamD)として動作し、TCP/IPでメールをスキャンします。これによりスパムフィルタの性能が大幅に増強され、別々のローカルコンピュータでMDSpamDの実行や、他の場所で実行されているもう1つのMDSpamD(あるいはSpamDが有効な製品)を、MDaemonで使用することが可能となります。MDSpamDはデフォルトで、ローカルで動作し、127.0.0.1のポート783でメッセージを受信します。このIPとポート番号を変更し、他のロケーションや他のポートで実行されているSpam Daemonへメッセージを送信する事もできます。

MDSpamD設定

ホストまたはIP
これは、MDaemonがMDSpamDによってスキャンされるメッセージを送信するホストまたはIPアドレスです。MDSpamDがローカルで動作している場合、127.0.0.1を使用します。

ポート
メッセージが送信されるポートです。MDSpamDのデフォルトポートは783です。

指定秒数に1度リモートMDSpamDにpingする XX 秒(0=なし)
遠隔地で動作しているspam daemonに対して定期的にpingを送信するにはこのオプションを使用できます。対象のロケーションに対してpingを送る必要が無い場合は、ここに0(ゼロ)を入力します。

ローカルMDSpamDを実行中利用できるオプション

MDSpamD外部プロセスウィンドウを表示
MDSpamDがローカルで実行中の時、外部のプロセスウインドウを起動するにはこのオプションを有効にします。このオプションは、MDaemonの内部UIまたはロギングシステムではなく外部のプロセスウインドウにMDSpamDのアウトプットをパイプで送ります。このオプションを使用すると、MDSpamDのデータをMDaemonに対してパイプで送ったり記録したりする必要がなくなるため、パフォーマンスの向上を図る事ができます。しかし、ログファイルは作成されず、下記のロギングオプションは使用できません。また、MDSpamDデータはMDaemonの管理画面でも[Security≫MDSpamD]タブに表示されなくなります。

すべてのローカルMDSpamDアクティビティを記録(デバッグログ-パフォーマンス浪費)
MDSpamDのすべてのアクティビティを記録する場合は、このオプションを有効にしてください。このオプションは上記の[MDSpamDの外部プロセスウィンドウを表示する]オプションが有効な場合は使用できません。さらに、SYSTEMアカウントのMDaemonではなくWindowsサービス[461]ダイアログによる認証情報を利用している場合も、MDSpamDアクティビティを記録することはできません。

> このログオプションを使用する場合、システムの構成や実行環境によっては、メールシステムのパフォーマンスが低下する場合があります。通常、このオプションはデバッグ目的にのみ使用されることをお勧めします。

最大メッセージ処理スレッド(1-6)
MDaemonが内部処理で使用するスレッド数の最大値を入力します。1から6まで指定ができます。

スレッドごとの最大TCP接続(10-200)
ここにはMDSpamDスレッドが他のスレッドに分岐する前に受け入れるTCP接続数の最大値を入力します。10から200まで設定できます。

127.0.0.1からのみリスンと接続をする
ローカルのMDSpamDに外部ソースからの接続を受け入れさせないようにするには、このオプションを有効にします。この場合、同じマシンからの接続のみを受け入れます。

このIP接続を監視する
前のオプションが無効にされる場合、接続を特定のIPアドレスにバインドするかまたは制限するために、このオプションを使用することができます。指定されたIPアドレスだけの接続が可能になります。MDSpamDを任意の特定のIPアドレスに制限しない場合、"<all>"を使用します。

これらのIPから接続を許可する
ここで指定するすべてのIPからの接続を受け入れます。その他のIPからの接続は遮断されます。この機能は、スパムフィルタ処理を共有する他のサーバからの接続がある場合に便利な機能です。

MDSpamDに渡す任意のコマンドラインオプション:

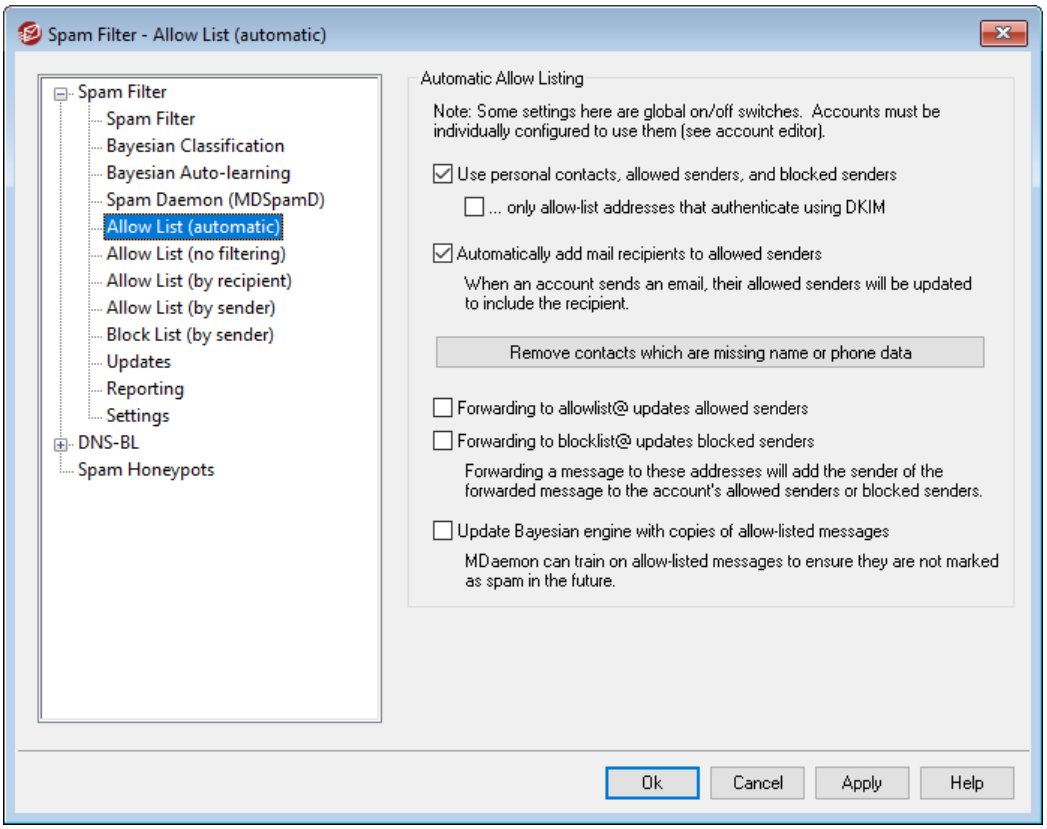
MDSpamDでは多くのコマンドラインオプションが使用可能です。詳細は以下のサイトをご覧ください。

http://spamassassin.apache.org/

これらのオプションを使用する際には、目的のオプションが含まれる文字列を作成しここに入力します。

オプションの一部は、このダイアログで設定することができ、コマンドのラインオプションを使用して手動で設定する必要はありません。

4.6.1.5 ホワイトリスト(自動)



許可リストの自動生成

個人の連絡先、許可リスト、ブロックリストを使用する
個人の連絡先情報、許可リスト、ブロックリストを、個人用スパムフィルタとして使用するにはこのオプションを有効にします。受信メール毎に、MDaemonは連絡先と許可リスト、ブロックリストに、メール送信者が一致するかどうかを検索します。一致した場合、対象の送信者をブロックリストや許可リストへ自動的に追加します。許可リストやブロックリストへの自動登録をMDaemonユーザ単位で無効化する場合は、アカウントエディタの許可リスト[691]画面にある*個人の連絡先*、*許可リスト*、*ブロックリストを使用する*というオプションを無効にします。

..DKIMで認証された許可リストアドレスのみ使用する
このオプションが有効にすると、メッセージがDomainKeys Identified Mail[481](DKIM)を通して認証される場合にのみ、送信者を許可リストへ登録します。このオプションはデフォルトで無効に設定されています。

メール宛先を自動的に許可リストへ追加
このオプションを有効にすると、ユーザーがローカル以外のメールアドレスへメールを送信した際、MDaemonは宛先をユーザーの許可リストへ自動登録します。上記の「個人の連絡先、許可リスト、ブロックリストを使用する」と併用すると、スパムフィルタの誤検知は飛躍的に減少します。

このオプションを全てのMDaemonユーザーへ適用しない場合は、アカウントエディタの許可リスト[691]画面で[**スパムフィルタ用の個人用連絡先、個人用許可リスト、ブロックリストを使用する**]チェックボックスを無効にしてください。

> このオプションは自動応答を使用しているアカウントでは利用できません。

名前または電話のない連絡先を削除する
各ユーザのデフォルト連絡先フォルダからメールアドレスだけの連絡先を削除する場合、このボタンを選択します。最低でも名前または電話番号を持たない連絡先は削除されます。このオプションは、許可リストの機能として追加された連絡先削除機能で、主にバージョン11より以前にMDaemonの自動的な許可リストオプションを使用していた人々を手助けするものです。MDaemonの以前のバージョンでは、メールアドレスを専用許可リストフォルダではなく、メインの連絡先情報へ追加していました。これにより、実際には使用していない連絡先情報が数多く登録されてしまっていたユーザーもありました。

> メールアドレスだけだったとしても適切な連絡先である場合もあるので、このオプションの使用に慎重な考慮が必要です。

allowlist@へ転送し許可リスト情報を更新
このオプションを有効にすると、アカウントエディタの設定画面で[**スパムフィルタ用の個人用連絡先、個人用許可リスト、ブロックリストを使用する**]を使用しているアカウントは、allowlist@<domain>へメールを転送する事で、アカウントの許可リストへ送信者を追加する事ができるようになります。許可アドレスは転送されたメールのFromヘッダを参照します。

allowlist@<domain>に転送されるメールはmessage/rfc822形式の添付ファイルとして転送される必要があり、認証済のSMTPセッションにてMDaemonが受信する必要があります。これらの条件を満たしていない転送メールは処理されません。

CFILTER.INIファイルで次のキーを編集することによってMDaemonが使用するアドレスを変更することができます。

```
[SpamFilter]
WhiteListAddress=MyAllowListAddress@
```

注意: 最後の文字は"@"でなければなりません。

blocklist@へ転送しブロックリスト情報を更新
このオプションを有効にすると、アカウントエディタの設定画面で[**スパムフィルタ用の個人用連絡先、個人用許可リスト、ブロックリストを使用する**]を使用しているアカウントは、blocklist@<domain>へメールを転送する事で、アカウントのブロックリストへ送信者を追加する事ができるようになります。ブロックされるアドレスは転送されたメールのFromヘッダを参照します。

blocklist@<domain> に転送されるメールはmessage/rfc822形式の添付ファイルとして転送される必要があり、認証済のSMTPセッションにてMDaemonが受信する必要があります。これらの条件を満たしていない転送メールは処理されません。

許可リストメッセージのコピーでベイジアンエンジンを更新する
(ベイジアン620画面で設定できる)非スパムメールの学習用フォルダへ、対象となるメールのコピーを自動的に保存するにはこの設定を有効にしてください。これはベイジアンエンジンに非スパムメールのサンプルを自動的に提供する役割を果たします。非スパムメールのサンプルでベイジアンエンジンをアップデートする事で、運用が進む毎にスパムの検出精度が向上し、正常なメールの誤検知を減らしていくことができます。

この機能を有効に活用するためには、受信メールの宛先がローカルユーザで、送信者はそのユーザのアドレス帳又は送信者許可リストに含まれている必要があります。送信メールの場合も、宛先は送信者のアドレス帳か送信者許可リストに含まれている必要があります。送信メールに対してこの機能を適用しない場合は、テキストエディタを使用してCFILTER.INIの以下の部分を編集してください。

```
[SpamFilter]
UpdateHamFolderOutbound=No (default = Yes)
```

受信メールが非スパムメールと判定されると、そのメールは、ベイジアン画面の学習スケジュール機能が無効の場合でも、ベイジアンの非スパム学習フォルダにコピーされます。そのため、その後学習スケジュールが有効になった時、手動学習を実行した際、一定の量の非スパムメッセージが用意されていることになります。しかしながら、判定されたすべてのメールが学習フォルダにコピーされるわけではありません。この機能が有効になると、指定された数に達するまで、MDaemonは適格のメッセージをコピーします。その後、指定された間隔で一回のメッセージをコピーします。デフォルトでは最初の200個の判定メールがすべてコピーされ、その後は10個ごとのメールのみがコピーされます。最初にコピーされるメールの数は、ベイジアン自動学習623の[学習前に必要な非スパムメールのサンプル数]で指定される値と同じものとなります。この設定を変更すると両方の値に影響します。メール数に応じたコピー間隔を変更するには、テキストエディタを使用してMDaemon.iniファイルの以下の部分を編集してください。

```
[SpamFilter]
HamSkipCount=10 (default = 10)
```

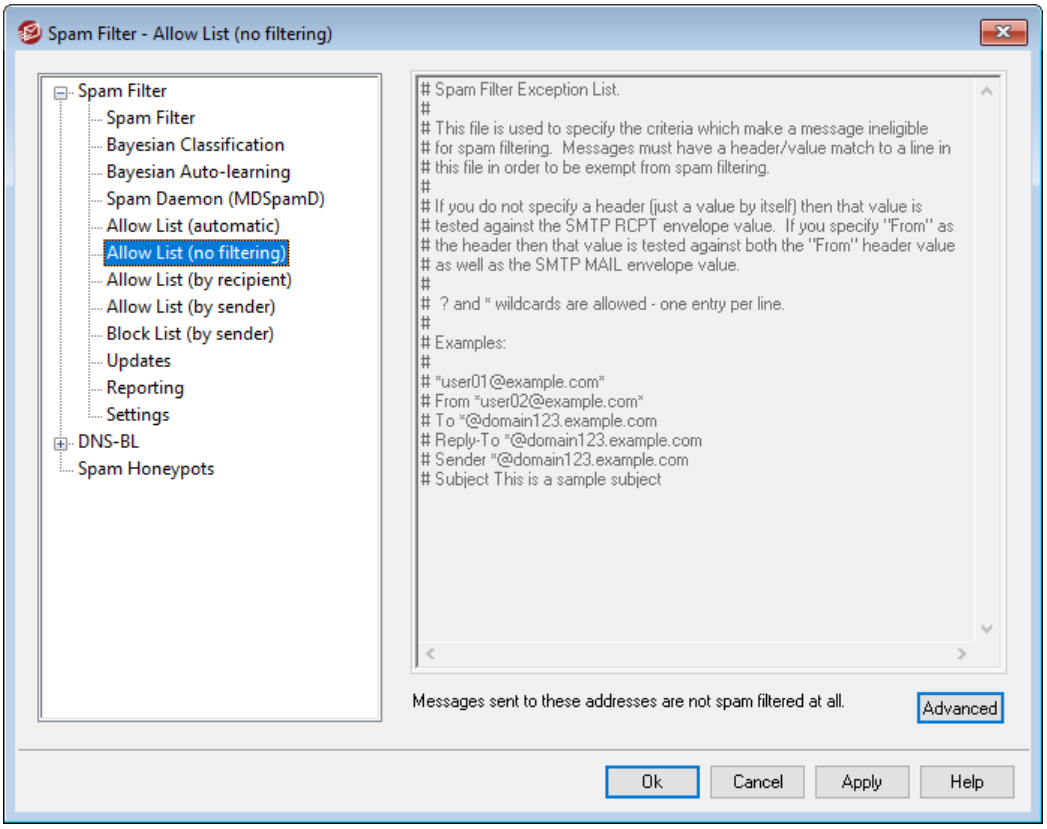
最後に、コピーされたメールの合計数が指定された値に達した場合、すべてのプロセスが最初から繰り返されます。合計数は、200又は指定した値です。デフォルトでは500個のメールがコピーされると、処理が最初から繰り返されます。この合計数を変更する場合は、テキストエディタを使用してMDaemon.iniファイルの以下の部分を編集してください。

```
[SpamFilter]
HamMaxCount=500 (default = 500)
```

MDaemonのスパムフィルタ処理に、別サーバーで稼働しているMDaemon Spam Daemon(MDSpamD)を使うよう設定した場合、このオプションは利用できません。ベイジアン学習は、他のサーバで行われた設定に従って処理されます。詳しくはSpam Daemon625画面を参照してください。

-

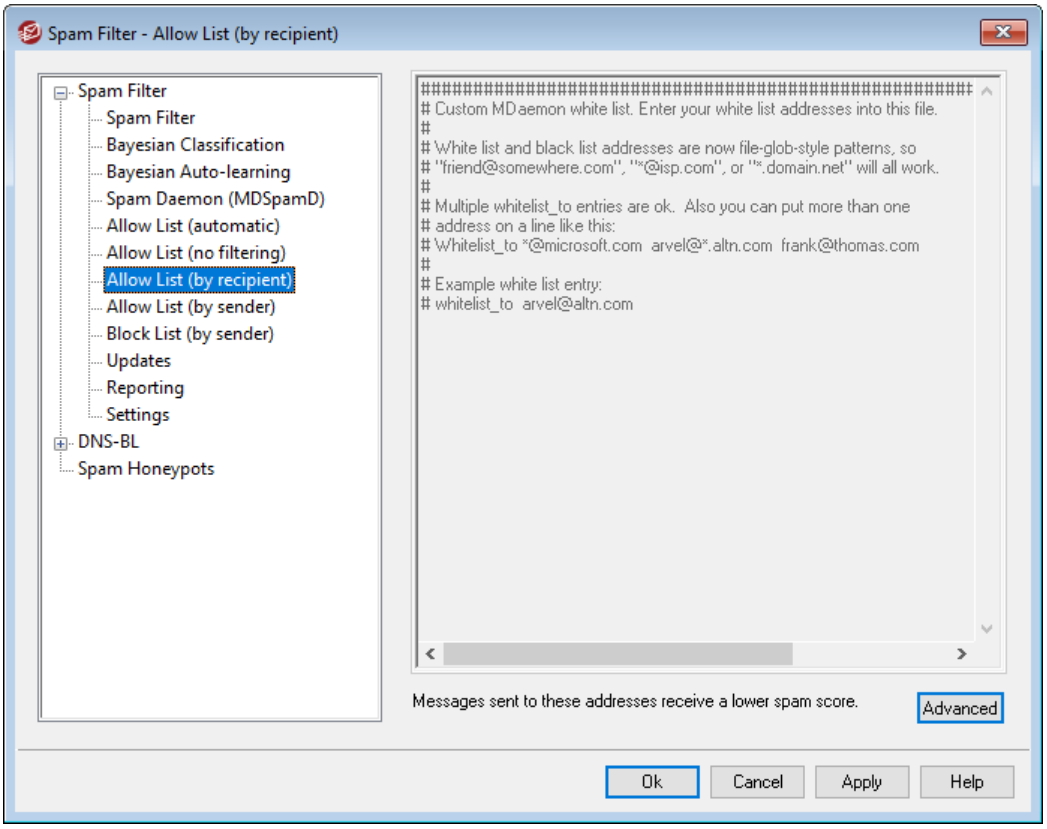
4.6.1.6 許可リスト（フィルタなし）



これらのアドレスへのメッセージはスパムフィルタ無しで送信します
詳細をクリックし、宛先アドレスを指定できます。これらのアドレス宛のメッセージは、スパムフィルタによって処理されません。

スパムフィルタの処理において、他のサーバのMDaemon Spam Daemon(MDSpamD)を使用するようにMDaemonを設定した場合、このオプションは使用できなくなります。スパムフィルタリストは、別のサーバで維持されます。詳しくはSpam Daemon 625画面を参照してください。

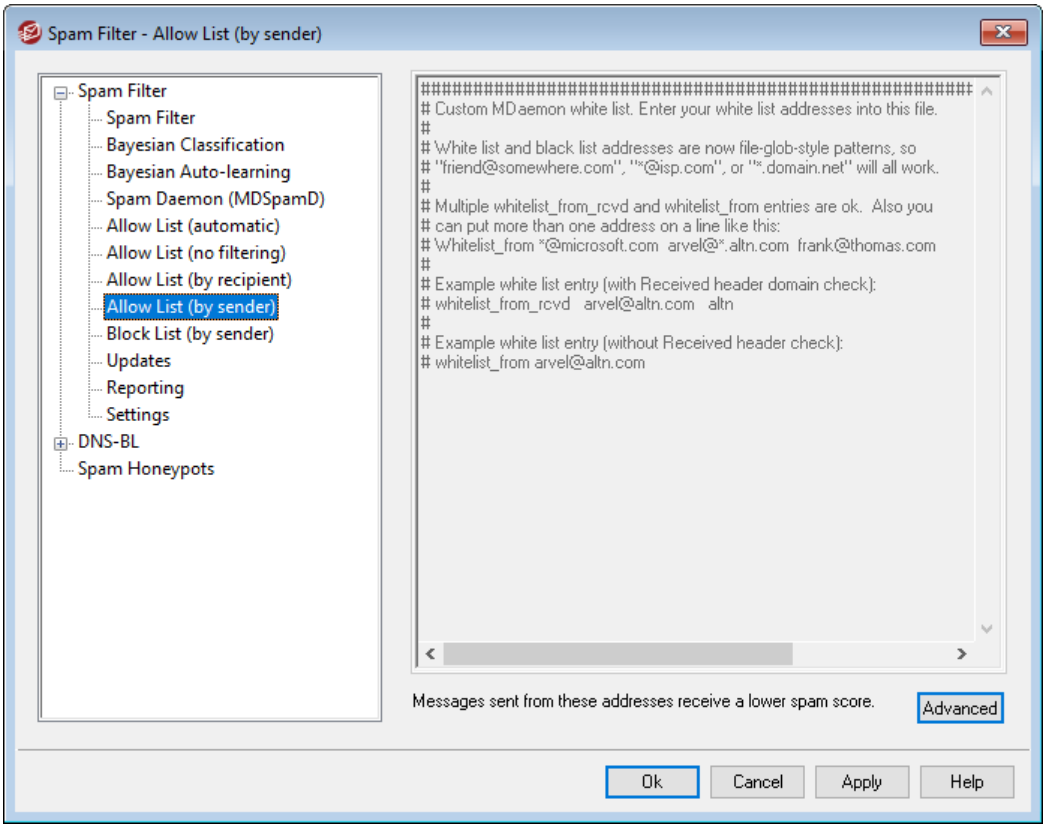
4.6.1.7 許可リスト（宛先）



これらのアドレスへのメッセージは、スパムスコアを低くして受信します
詳細 をクリックしてアドレスをこのリストへ追加します。この一覧は *許可リスト（フィルタなし）*[630] に似ていますが、宛先に応じてスパムフィルタ処理からメールを除外するのではなく、スパムフィルタ処理は行いスパムフィルタ設定[636]で指定したスコアから、スパムフィルタスコア[617]を減算するようになります。例えば、スパムスコアのしきい値を5.0、許可リストの値を100と設定した場合、スパムと思われるメールがスパムスコア105.0以上になった場合は、許可リストの値を減算した場合であっても、最終的には5.0以上のスコアとなり、対象のメールはスパムとして処理されます。このような高いスコアがカウントされる事は、送信者がブロックリストへ登録されていた場合など、他の要因がない限りほとんどありません。

スパムフィルタの処理において、他のサーバのMDaemon Spam Daemon(MDSpamD)を使用するようにMDaemonを設定した場合、このオプションは使用できません。スパムフィルタリストは、別のサーバで維持されます。詳しくはSpam Daemon[625]画面を参照してください。

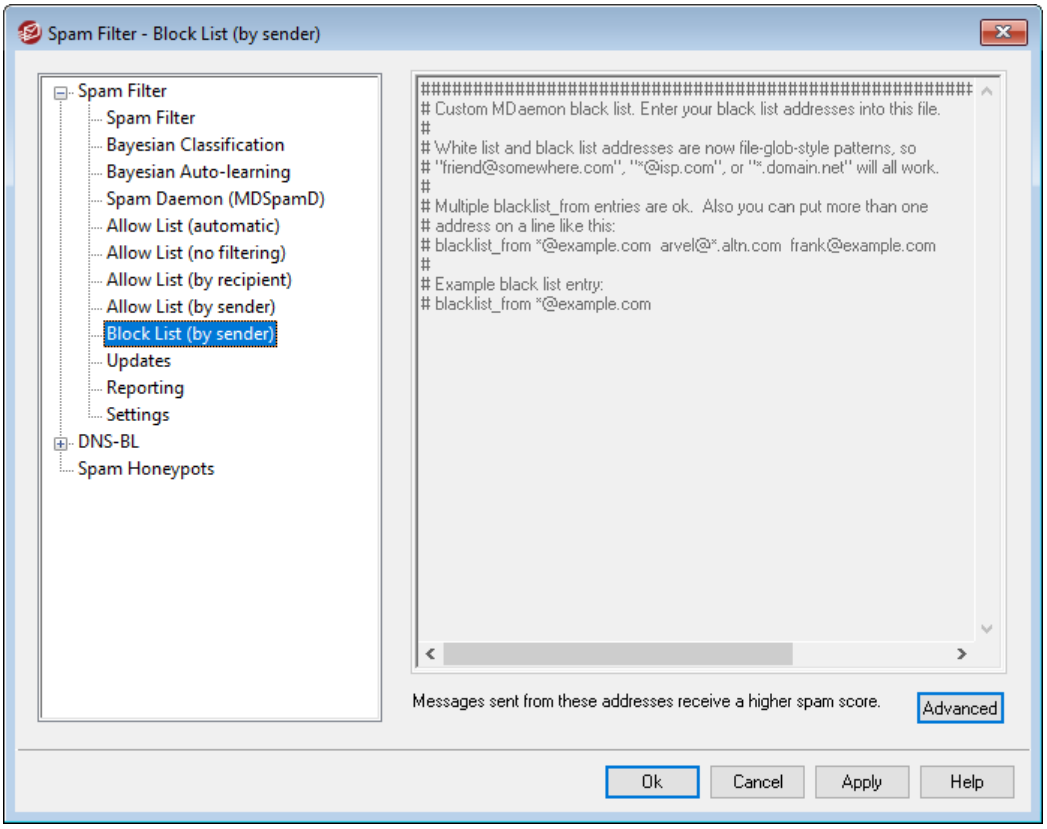
4.6.1.8 許可リスト（送信者）



これらのアドレスからのメッセージは、スコアを低くして受信します
詳細 をクリックしてアドレスをこのリストへ追加します。この許可リストは*許可リスト（宛先）*[631]に似ていますが、宛先に応じてスパムフィルタ処理からメールを除外するのではなく、スパムフィルタ処理は行いスパムフィルタ設定[636]で指定したスコアから、スパムフィルタスコア[617]を減算するようになります。例えば、スパムスコアのしきい値を5.0、許可リストの値を100と設定した場合、スパムと思われるメールがスパムスコア105.0以上になった場合は、許可リストの値を減算した場合であっても、最終的には5.0以上のスコアとなり、対象のメールはスパムとして処理されます。このような高いスコアがカウントされる事は、送信者がブロックリストへ登録されていた場合など、他の要因がない限りほとんどありません。

スパムフィルタの処理において、他のサーバのMDaemon Spam Daemon(MDSpamD)を使用するようにMDaemonを設定した場合、このオプションは使用できません。スパムフィルタリストは、別のサーバで維持されます。詳しくはSpam Daemon[625]画面を参照してください。

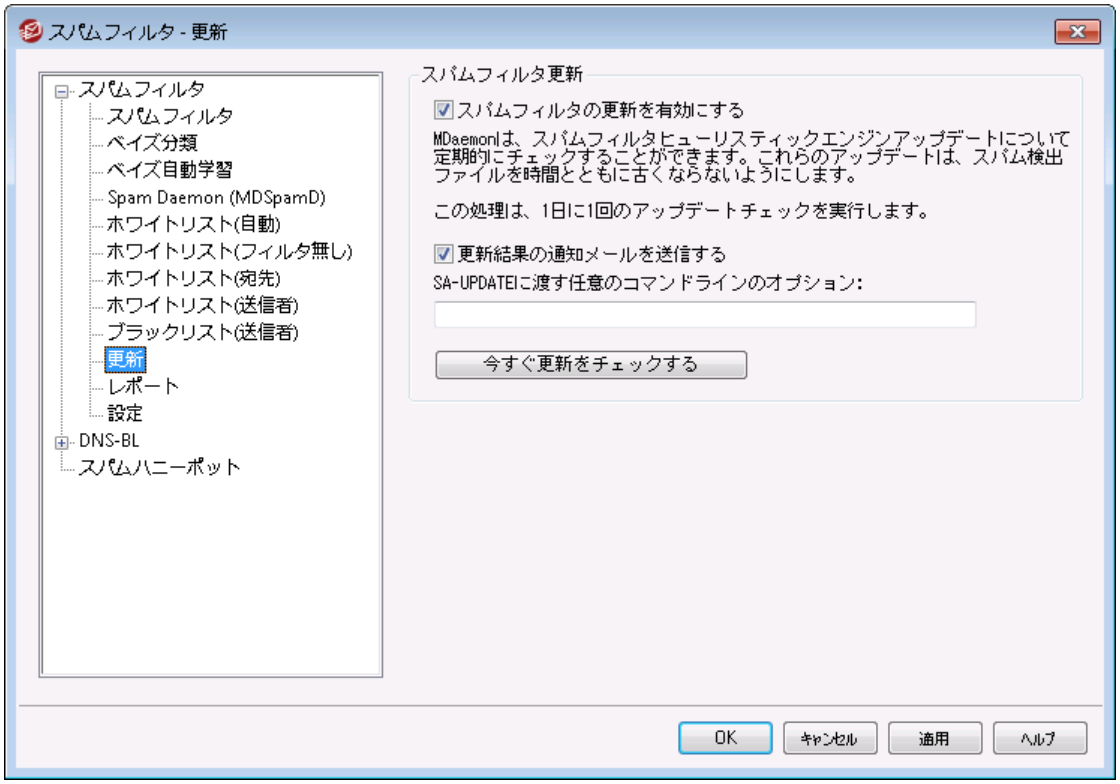
4.6.1.9 ブロックリスト（送信者）



これらのアドレスからのメッセージは、受信時にスパムスコアを高めます
詳細 をクリックしてアドレスをこのリストへ追加します。このブロックリストにあるアドレスからのメールは、スパムフィルタ設定 636で指定したスコアへ、スパムフィルタスコア 617を加算するようになります。一般的にはこれでスパムとしてマークされるようになりますが、このアドレスが自動でスパムとして認識されるようになるわけではありません。例えば、送信者がブロックリストへ含まれていても、受信者が許可リストに含まれていた場合、スコアはそれぞれのスコアを相殺して、最終的にしきい値を下回っていた場合は、メールは送信者へ配信されます。これはブロックリストのスコアを小さい値で設定していた場合などに起こります。

スパムフィルタの処理において、他のサーバのMDaemon Spam Daemon（MDSpamD）を使用するようにMDaemonを設定した場合、このオプションは使用できなくなります。スパムフィルタリストは、別のサーバで維持されます。詳しくはSpam Daemon 625画面を参照してください。

4.6.1.10 更新



スパムフィルタ更新

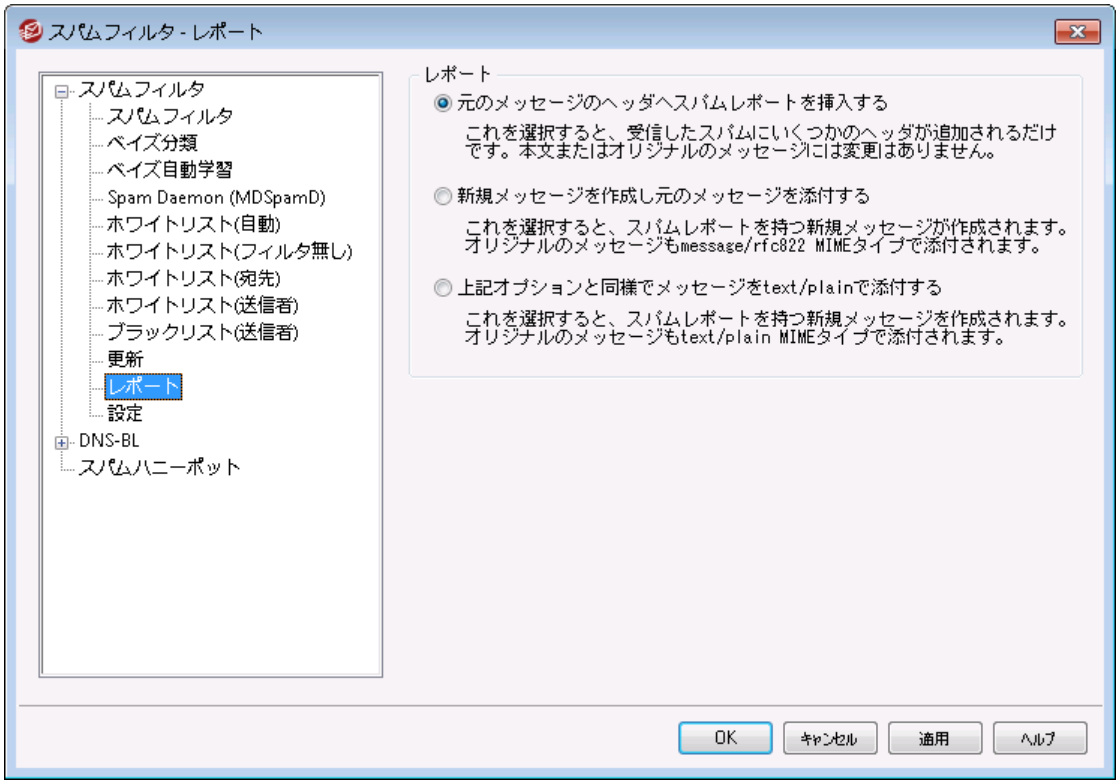
スパムフィルタ更新を有効にする
スパムフィルタルールを自動的に更新する場合はこのチェックボックスを有効にしてください。一日毎に、スパムフィルタはスケジュールされた間隔でAlt-N Technologiesに接続して新しいルールをチェックし、新しいルールがあれば自動的にダウンロードしインストールを行います。

更新の結果を通知メールで送信する
更新の結果を含む迷惑メールフィルタが更新されるたびに管理者に電子メールを送信する場合は、このオプションを使用します。このオプションは、「コンテンツフィルタ≫通知」にある「管理者へのスパムフィルタ更新通知の送信」オプションと同じです。

SA-UPDATEに渡す任意のコマンドラインオプション
SA-UPDATEにコマンドラインオプションを渡す場合は、この特別なオプションを使用します。

今すぐ更新をチェックする
このボタンをクリックすると、すぐに迷惑メールフィルタのルールの更新を確認できます。

4.6.1.11 レポート



MDaemonのスパムフィルタ処理に、別サーバーで稼働しているMDaemon Spam Daemon(MDSpamD)を使うよう設定した場合、スパムフィルタレポートは利用できません。スパムフィルタレポートは、他のサーバで管理されます。詳しくはSpam Daemon 625 画面を参照してください。

レポート

元のメッセージのヘッダへスパムのレポートを挿入する
これはデフォルトのオプションです。スパムフィルタにより、スパムメールのヘッダにスパムレポートを挿入させたい場合は、このオプションを有効にしてください。以下はシンプルなスパムレポートの例です。

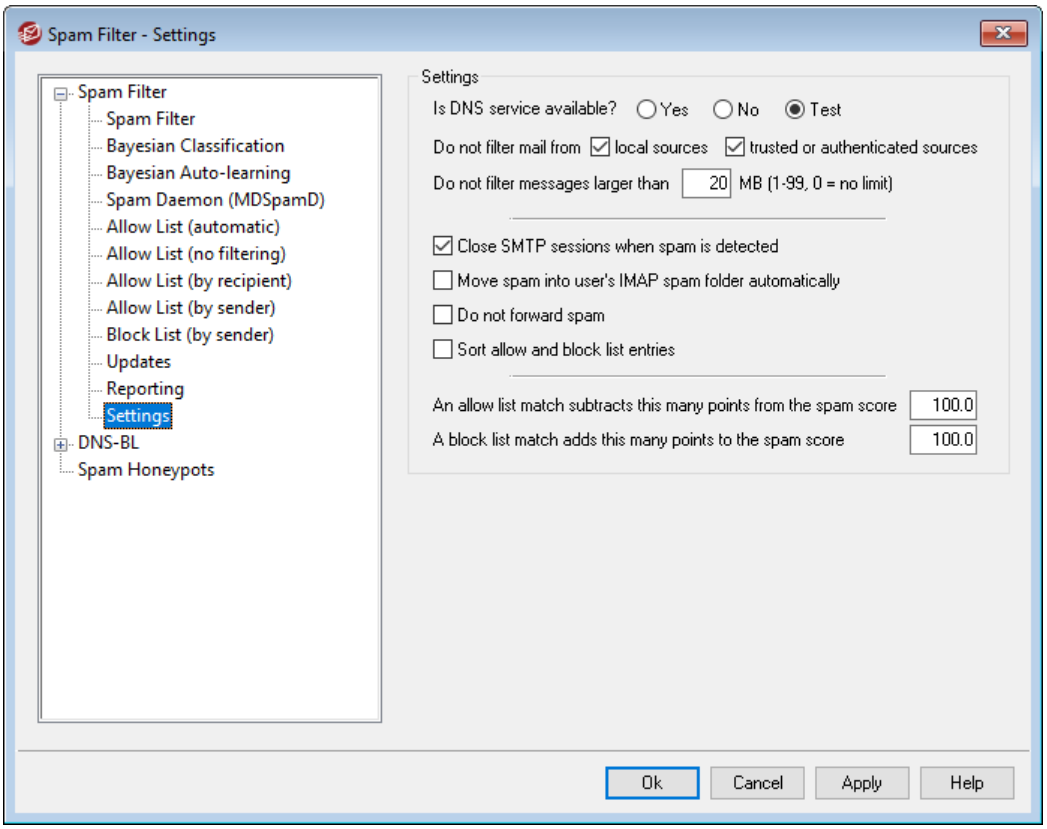
```
X-Spam-Report: ---- Start Spam Filter results
  5.30 points, 5 required;
  * -5.7 -- Message-Id indicates the message was sent from MS Exchange
  *  2.0 -- Subject contains lots of white space
  * -3.3 -- Has a In-Reply-To header
  *  3.0 -- Message has been marked by MDaemon's DNS-BL
  *  2.9 -- BODY: Impotence cure
  *  2.2 -- BODY: Talks about exercise with an exclamation!
  *  0.5 -- BODY: Message is 80% to 90% HTML
  *  0.1 -- BODY: HTML included in message
  *  1.6 -- BODY: HTML message is a saved web page
  *  2.0 -- Date: is 96 hours or more before Received: date
```

```
---- End of Spam Filter results
```

新規メッセージを作成し元のメッセージを添付する
スパムレポートを持つ新規のメッセージを作成する場合は、このオプションを選択してください。オリジナルのスパムメッセージはファイルとして添付されます。

上記オプションと同様で元のメッセージをtext/plain形式で添付する
前のレポートオプションのように、このオプションは、オリジナルのスパムメッセージを添付した新規メッセージとしてスパムレポートを生成します。この違いは、オリジナルメッセージがtext/plain MIMEタイプで添付されます。スパムは時々各メッセージに対してユニークなHTMLコードを含み、スパマーに潜在的に、どの電子メールおよびIPアドレスが開いているか明らかにすることができるので、このメソッドは、HTMLコードをプレーンテキストに変えることを禁止します。

4.6.1.12 設定



設定

DNSサービスは利用可能ですか?
これらのオプションによって、メッセージを処理する時に、DNSがスパムフィルタを利用できるかどうか選択することができます。以下のオプションのうちの1つを選択することができます:

はい
DNSを使用します。DNS接続が必要なSURBL/RBLやその他のルールが適用可能になります。

いいえ
DNSを使用しません。DNS接続を必要とするスパムフィルタルールは適用できません。

テスト
利用可能なDNSがテストされ、存在すれば使用されます。これはデフォルト設定です。

指定送信元からのメールをフィルタしない

ローカルソース
ローカルユーザとドメインからのメッセージをスパムフィルタから除外する場合は、このオプションを選択してください。

信頼/認証されたソース
信頼されたドメインあるいは認証された送信者からのメッセージをスパムフィルタから除外する場合は、このオプションを選択してください。

指定サイズ以上のメッセージはフィルタしない [XX] MB (1-99, 0 = 無制限)
スパマーの通例の目的が最も短い期間にできるだけ、多くのメッセージを配信することになっているという理由から実際にスパムメッセージは小さいのが特徴です。一定のサイズ以上のメッセージをスパムフィルタから除外する場合 はそのサイズ(MB)をここで指定してください。スパムフィルタを行うのにサイズ制限を行いたくない場合は、ここで0(ゼロ)を指定してください。

スパム検出時にSMTPセッションを閉じる
このオプションはデフォルトで有効で、インラインスキャンがスパムメッセージを検出した場合にSMTPセッションを閉じます。

自動的にスパムをユーザのIMAPスパムフォルダへ移動する
このオプションを有効にすると、MDaemonはスパムフィルタがスパムであると判断したメッセージを自動的にユーザのスパムフォルダに移動します。また、新しいユーザアカウントが追加された時に、スパムフォルダを自動的に作成します。

さらにこのオプションを有効にすると、すでに存在するユーザアカウントに対してもフォルダを作成するかどうかをMDaemonが尋ねてきます。[はい]を選択すると、すべてのユーザに対してフォルダが作成されます。[いいえ]を選択すると、新しく追加されたユーザのみにフォルダが作成されます。すでに存在するフォルダに対しては、修正が加えられたり影響が及ぶことはありません。

スパムを転送しない
スパムメッセージを転送しない場合は、このチェックボックスを選択してください。

許可リストとブロックリストのエントリをソート
スパムフィルタの許可リストとブロックリストをソートした状態で管理する場合はこのオプションを選択します。**注意点:** ファイルへ独自のコメントを追加していると(#から始まる行です)このオプションを有効にすることで、こうしたコメントはファイルの上部へソートされます。これはデフォルトで無効になっています。有効にした後、ソートは次回許可リストやブロックリストへ変更が加わったタイミングで実行されます。

MDaemonのスパムフィルタ処理に、別サーバーで稼働しているMDaemon Spam Daemon(MDSpamD)を使うよう設定した場合、この後のオプション

は利用できません。詳しくはSpam Daemon[625]画面を参照してください。

スパムスコアから減算(許可リストに適合)
スパムフィルタの許可リスト(宛先)[631]や許可リスト(送信者)[632]へ追加したアドレスであっても、このアドレスと送受信したメールが、必ずしもスパムとして処理されない訳ではなく、このアドレスとのやり取りにおいては、既存のスパムスコアから、指定した値を減算する事ができます。例えば、スパムスコアのしきい値が5.0である場合、この値を100に設定すると、許可リストによる差し引かれる前のスパムスコアが105.0以上のスパムメッセージの最終的なスパムスコアは最低でも5.0となり、このメッセージはスパムとして処理されます。しかしながら、そのメッセージがブロックリストにあるアドレスのような例外的にスパムスコアを高くするような要素を含んでいない限り、それほど高い値であることはあまりないので、このような現象はめったに起こりません。もちろん、許可リストによる差し引きの値をもっと低く設定した場合は、この現象が生じる可能性は高くなります。

特定の宛先に対するメールに対して、スコアの調整ではなくスパムフィルタを回避させたい場合には、宛先アドレスを許可リスト(フィルタなし)[630]へ追加して下さい。許可リスト(自動)[627]画面のオプションを使用し、送信者に応じてメールをスパムフィルタスコアから除外することもできます。

スパムスコアに加算(ブロックリストに適合時)
ここでの値は、メールの送信者アドレスがブロックリスト(送信者)[633]のアドレスと一致した場合に、スパムスコアに加算されます。上記の許可リストオプションと同様、スパムフィルタのブロックリストへ登録されているアドレスが、必ずしもスパムメールとして判定される訳ではありません。代わりに、このオプションで指定した値がメールのスパムスコアに加算され、その合計値を元に、メールがスパムかどうかを判定されます。

4.6.2 DNSブロックリスト(DNS-BL)

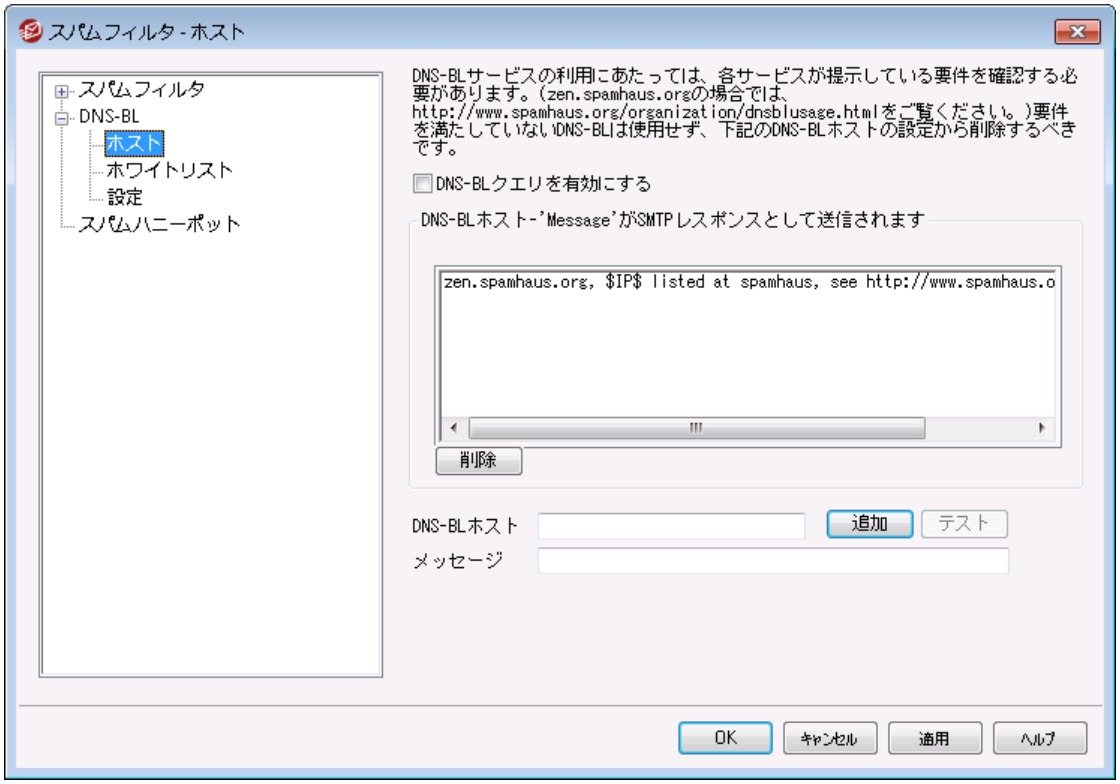
DNSブロックリスト(DNS-BL)を使用することにより、スパムメールからの保護ができるようになります。このセキュリティ機能は、(スパムメール中継サーバーとして認知されているホストの一覧を管理している)DNSブロックリストサービスを指定する事により、受信メールを受け取る度に、対象メールをチェックできるようになるというものです。接続IPが登録しているサービスの内の1つに登録されていた場合、設定[641]画面内の設定内容に基づき、対象のメールは拒否されるか、フラグが追加され処理されます。

DNSブロックリストは、DNS-BLの参照から除外するIPアドレスを指定する[許可リスト]データベースも搭載しています。この機能を有効にする前に、ローカルIPアドレス範囲を許可リストへ追加しておき、スパムメール参照から除外するようにしてください。127.0.0.1は例外として設定済のため、改めて登録する必要はありません。

参照:

DNS-BLホスト 639
DNS-BL設定 641
DNS-BL許可リスト 640

4.6.2.1 ホスト



DNS-BLホスト

DNS-BLクエリを有効
受信メールをDNSブロックリストと照合する場合、このオプションを有効にしてください。MDaemonは送信IPアドレスのDNS-BLに対するルックアップを実行します。ホストがクエリに陽性の結果で応答する場合、MDaemonでは、DNS-BL設定 641 画面で有効にしたオプションにしたがって、メッセージのフラグ付け、または受け入れの拒否ができます。

削除
DNS-BLサービスリストからエントリを選択し、ボタンをクリックしてリストから削除します。

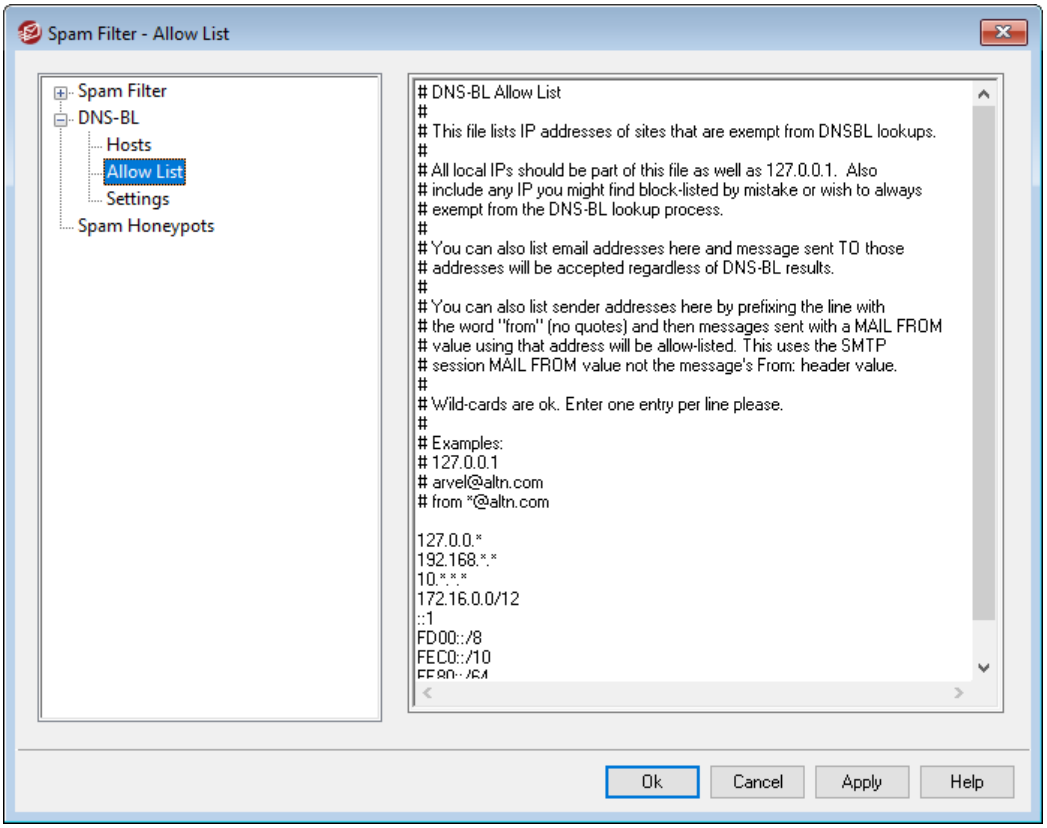
DNS-BLホスト
ブロックリストIPアドレスへ新しいホストの問合せを行う場合、ここに入力します。

テスト
DNS-BLホスト へホスト 情 報 を入 力 し、このボタンを押 すと、127.0.0.2のルックアップをテストします。

メッセージ
これは、IPアドレスが上 記 のDNS-BLホスト に掲 載 されていた場 合 、SMTPセッション中 に表 示 される メッセージです。このメッセージは、DNS-BL設 定 641 画 面 の[...'user unknown'でなく'Message'で 応 答 する] オプションに対 応 します。

追 加
ホスト および返 答 メッセージを入 力 した後 に、DNS-BLホスト に追 加 するために、このボタンをクリックして ください。

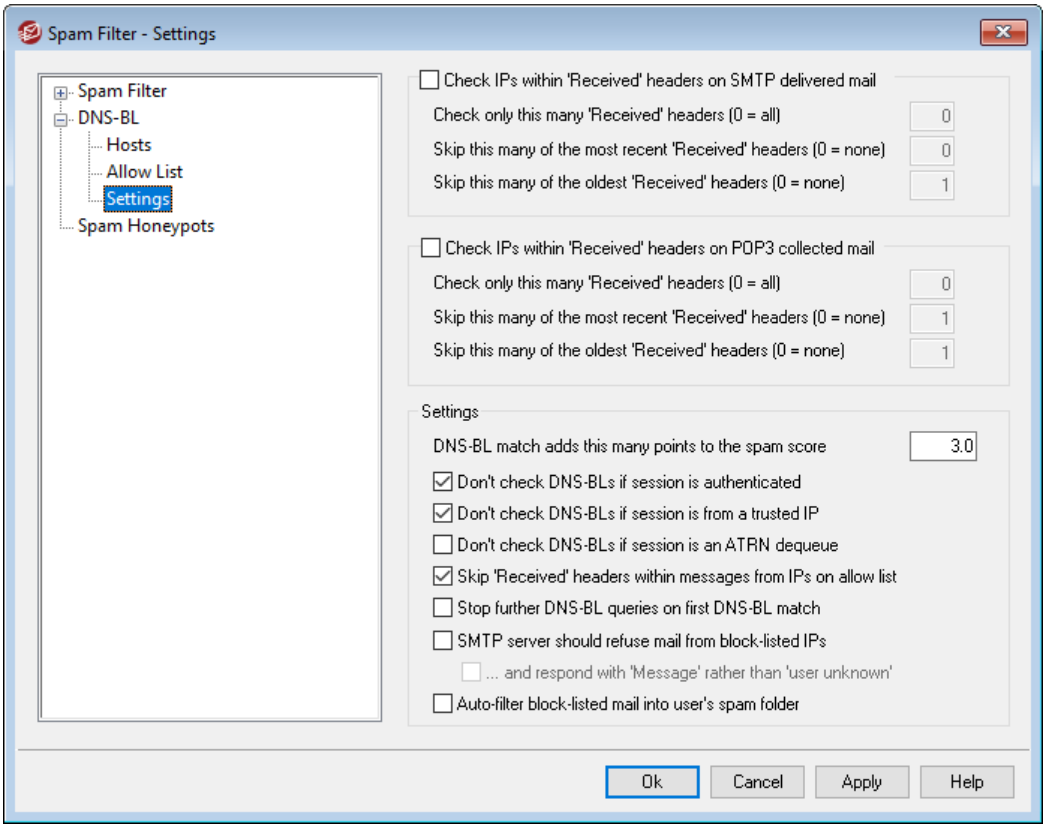
4.6.2.2 許可リスト



この画 面 では、DNSブロックリスト 検 索 から除 外 するIPアドレスを指 定 できます。DNS-BLがローカルユー ザーからのメールを拒 否 しないよう、(例 えば127.0.0.*、192.168.*.* などの)ローカルIP範 囲 やドメ インを入 力 して下 さい。ここではメールアドレスを指 定 する事 もできます。このリスト に対 して送 信 したメー ルはDNS-BLルックアップ結 果 によらず受 信 する事 ができます。最 後 に、「from sender@ example.com」を一 覧 に追 加 入 力 する事 で、特 定 の送 信 者 をDNS-BL結 果 から除 外 する 事 もできます。アドレスはメールの「From: 」ヘッダではなくSMTPセッションの「MAIL FROM」の値 に一 致 している必 要 があります。

1行 には1つのエントリのみ入 力 できます。ワイルドカードも使 用 できます。

4.6.2.3 設定



SMTP配信されたメールの'Received'ヘッダ内のIPをチェックする
SMTP経由で受信したメッセージのReceivedヘッダへ記載されているIPがDNSブロックリストへ登録されているものかどうかをチェックするにはこの設定を有効にします。

'Received'ヘッダをチェックする最大数(0 = すべて)
DNS-BLでチェックする"Received"ヘッダの最大数を指定します。ゼロを指定すると、すべての"Received" ヘッダがチェックされます。

直近から指定した数の'Received'ヘッダを省略する(0 =なし)
SMTPをチェックする時、1つ以上の直近のReceivedヘッダを省略する場合には、このオプションを有効にします。

指定より古い'Received'ヘッダを省略する(0 =なし)
SMTPメッセージをチェックする場合、最も古いReceivedヘッダのチェックを指定した数分DNS-BLで省略する場合、このオプションを使用してください。

POP3収集されたメールの'Received'ヘッダ内のIPをチェックする
有効な場合、DNS-BLはDomainPOPとMultiPOPで受信されたメールのReceivedヘッダに挿入されたIPアドレスをチェックします。

'Received'ヘッダをチェックする最大数(0 = すべて)
DNS-BLでチェックする"Received"ヘッダの数を指定します。ゼロを指定すると、すべての"Received" ヘッダがチェックされます。

直近から指定した数の'Received'ヘッダを省略する(0 =なし)
DomainPOPとMultiPOPメッセージをチェックする場合、1つ以上の最新のReceivedヘッダを省略させたい場合、このオプションを使用してください。DomainPOPなどのPOP3で収集されたメールの直近のReceivedヘッダのチェックを省略する必要は頻繁に生じるので、このオプションはデフォルトで1に設定されています。

指定より古い'Received'ヘッダを省略する(0 =なし)
DomainPOPとMultiPOPメッセージをチェックする時に指定よりも以前のReceivedヘッダを省略させたい場合、DNS-BLが必要な場合、このオプションを使用してください。

設定

DNS-BLの一致で指定値をスパムスコアに加算
DNS-BLと一致したメールに対して、加算するスパムスコア[617]を指定します。スパムフィルタのヒューリスティック検査では、DNS-BLの結果について加算されるスコアが、スパムと判定するには十分でない場合があります。ここでスパムスコアを追加すると、スパムメールの検出率を向上させる事ができます。デフォルトでDNS-BLに一致した場合にはスパムスコアへ3.0ポイントが加算されます。

次のセッションの場合はDNS-BLをスキップ:

認証済
AUTHコマンドで認証したセッションからのメールをDNS-BL問合せの対象外とする場合はこのオプションをクリックして下さい。

信頼するIPからのセッション
信頼するホスト[472]からのメールをDNS-BL問合せの対象外とする場合はこのオプションをクリックして下さい。

ATRNデキュー
ATRNデキューセッションで収集したメールをDNS-BL問合せの対象外とする場合はこのオプションをクリックして下さい。この設定はデフォルトで無効に設定されていますが、スマートホストでメールのDNS-BLチェックを既に行っている場合などは有効にして頂く事もできます。

許可リストからのメールの 'Received' ヘッダをスキップ
このオプションを有効にすると、DNS-BL 許可リスト[640]に含まれているIPアドレスからのメールについては「Received」ヘッダのチェックを行いません。

最初のDNS-BLの一致で以降のDNS-BL問合せを中止
メールヘッダに複数のホストが含まれていて、DNS-BL処理が複数回行れる事は頻繁にあります。デフォルトで、DNS-BLは一致した数によらず、全ての問合せ処理を行います。DNS-BLに一致した時点で、対象メールのそれ以降の問合せを中止する場合は、このオプションを有効にして下さい。

ブロックリストのIPからのメールをSMTPサーバで拒否する
デフォルトでは、このオプションは無効で、SMTPセッション中ブロックリストにあるIPアドレスからメッセージを拒否するのではなく、X-MDDNSBL-Resultヘッダを挿入します。コンテンツフィルタ機能を使って、このヘッダを検索し、要件に応じた処理を行う事ができます。また、後述のユーザのスパムフォルダ

ヘブロックリスト のメールを自 動 的 にフィルタオプションを使 って、各 ユーザのスパムフォルダへ自 動 的 にメッセージを振 り分 けることもできます。フラグ付 けでなく、ブロックリスト に登 録 されたIP からのメールを拒 否 する場 合 は、このオプションを有 効 にして下 さい。

一 部 のIPアドレスが誤 ってブロックリスト に記 載 される可 能 性 があるので、フラグを付 けるのではなく、メッセージの拒 否 を選 択 する前 に注 意 をしなければなりません。メッセージへフラグを付 けに加 えて、 スパムフィルタ[617]の *DNS-BLの一 致 で指 定 値 をスパムスコアに加 算* でスパムスコアを調 整 することもできます。

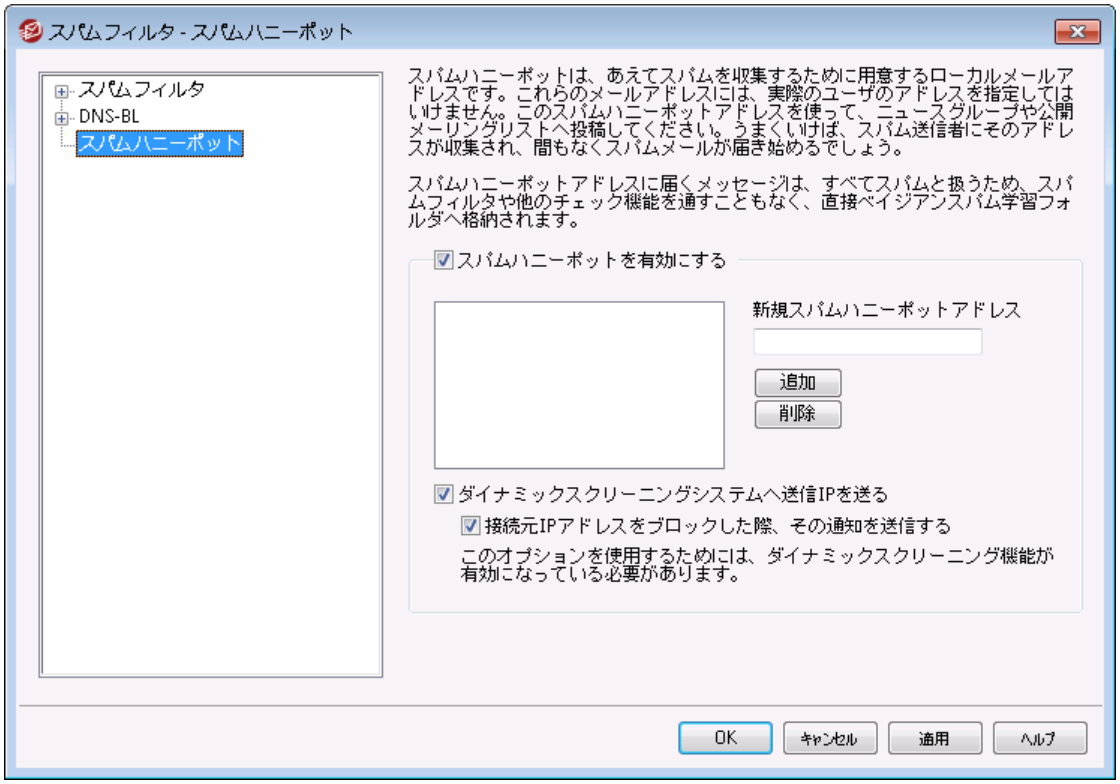
...'user unknown'でなく'Message'で応 答 する
IPアドレスがリスト に含 まれているかどうかをSMTPセッション中 に特 定 の形 式 でDNS-BLホスト[639]へ渡 す場 合 はこのオプションを使 用 します。
それ以 外 は、"user unknown"メッセージが代 わりに渡 されます。上 記 の**ブロックリスト のIPからのメールをSMTPサーバで拒 否 する**オプションの使 用 を選 択 した場 合 に、このオプションは、利 用 可 能 です。

ユーザのスパムフォルダへブロックリスト のメールを自 動 的 にフィルタ
このオプションをクリックすると、この後 に追 加 する全 てのアカウント で、アカウント 用 の"Junk E-mail" IMAPフォルダが作 成 されます。またMDaemonはユーザ毎 にX-MDDNSBL-Resultヘッダを検 索 するメールフィルタを作 成 し、このヘッダを含 むメッセージをユーザのスパムフォルダに移 動 します。また、このオプションをクリックすると、MDaemonの既 存 のユーザアカウント に対 しても、同 じようにこれらのフォルダを作 成 しフィルタを適 用 するかどうかを尋 ねられます。下 記 の[アカウント 別 スパムフォルダとフィルタの自 動 生 成]をご覧 ください。

アカウント 別 スパムフォルダとフィルタの自 動 生 成

MDaemonは自 動 的 にアカウント 毎 の"Junk E-mail" IMAPメールフォルダを作 成 し、X-MDDNSBL-Resultヘッダを発 見 するとそのフォルダへメッセージを振 り分 けるルールを作 成 します。上 記 の**ユーザのスパムフォルダへブロックリスト のメールを自 動 的 にフィルタ**オプションをクリックすると、すべてのアカウント に対 してフォルダと対 応 するルールを作 成 するかどうかを確 認 されます。フォルダとフィルタを作 成 するには[はい]を選 択 してください。この方 法 で、簡 単 且 つ敏 速 に、全 てのユーザーで、スパムメールが正 規 のメールと混 同 してしまうのを避 ける事 ができます。ユーザーが行 わなくてはならない事 は唯 一 、定 期 的 にスパムフォルダをチェックして、重 要 なメールが誤 ってスパムフォルダに送 られていないか(時 には発 生 する可 能 性 があります)を確 認 する事 のみです。アカウント にフォルダとフィルタを作 成 する際 、すでにX-MDDNSBL-Resultヘッダをチェックするフィルタを持 つアカウント が存 在 すると、MDaemonは何 もアクションを起 こさず、ルールも作 成 しません。IMAPフォルダの名 前 を"Junk E-mail"以 外 にする場 合 は、設 定 ≫ 初 期 設 定 の システム[450] 画 面 の**デフォルト スパムフォルダ名** を変 更 します。

4.6.3 スパムハニーポット



スパムハニーポット（ セキュリティ ≫ スパムフィルタ ≫ スパムハニーポット）は、スパムの収集を目的としたローカルメールアドレスです。これらスパムハニーポットは、MDaemonの正規のメール送受信用のメールやメールエイリアスを使うべきではありません。このスパムハニーポットアドレスをニュースグループや公開メーリングリストなど、スパム送信者がアドレス収集に使用するソースに置くことにより、スパムメッセージの送信元アドレスを収集することができます。また、他の実在しないアドレス宛てに届いたスパムメールについても、その送信元アドレスを抜き出して使用する事ができます。スパムハニーポットでは正規のメールを受信することはなく、このアドレスへのメールはすべてスパムと認識され、ベイジアンスパム学習フォルダ[620]へダイレクトに送られ、処理されます。さらに、送信サーバのIPアドレスをダイナミックスクリーン[514]システムに追加することも可能で、これにより、そのサーバからの接続を一定期間、拒否することができます。このようなシステムにより、スパムの送信元を特定し、受信するスパム数を減らしていくことができます。

スパムハニーポット

スパムハニーポットとして利用しているメールアドレスがここに表示されます。

スパムハニーポットを有効にする

このオプションはデフォルトで有効になっています。スパムハニーポットを無効にする場合は、このチェックを外して下さい。

新規スパムハニーポットアドレス

スパムハニーポットに新しいアドレスを追加するときは、ここにアドレスを入力して[追加]ボタンをクリックします。

削除
スパムハニーポット用のアドレスを削除する場合は、リストから目的のアドレスを選択して[削除]ボタンをクリックします。

ダイナミックスクリーニングシステムへ送信IPを送る
スパムハニーポットメッセージで収集したIPアドレス全てをダイナミックスクリーン 514 システムに送信する場合は、このチェックボックスを選択します。この機能を使用するには、ダイナミックスクリーニング(セキュリティ ≫ セキュリティ設定 ≫ スクリーニング ≫ ダイナミックスクリーニング)を有効にする必要があります。

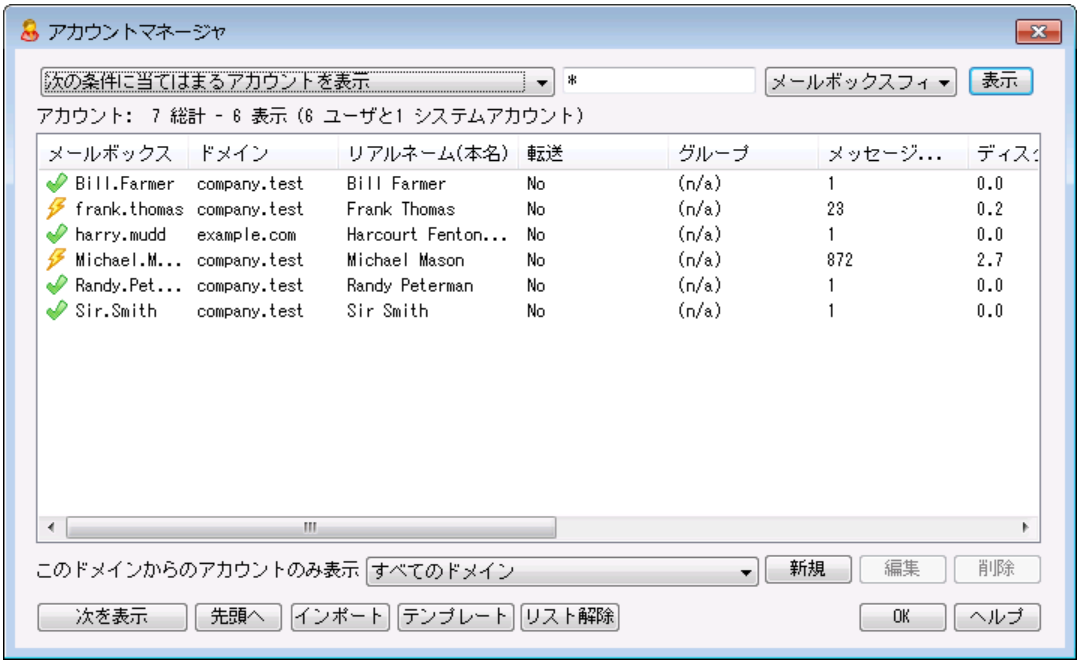
IPがブロックされたら通知する
デフォルトで、対象IPアドレスがダイナミックスクリーニングでブロックされると、ダイナミックスクリーニング *IPアドレスブロックレポート* 564 オプションにてアクションに関する通知が送られます。IPアドレスがブロックされた時通知を送らないようにするには、このオプションをクリアしてください。

セクション 5

5 アカウントメニュー

5.1 アカウントマネージャ

アカウントの選択、追加、削除または変更を効率的に管理するために、MDaemonにはアカウントマネージャ機能が搭載されています。ダイアログからは、アカウント情報へアクセスしたり、メールボックス、ドメイン、リアルネーム、メールフォルダでの並べ替えを行う事ができます。アカウントマネージャは、アカウントメニューの中の、アカウント ≫ アカウントマネージャ...で表示できます。



アカウントの管理

アカウントリストの上部には、リストに関する2つの統計情報が表示されます。最初の数字は、現在システム上に存在するMDaemonのユーザアカウントの合計数です。2番目の数字は、現在アカウントリストに表示されているアカウント数です。どのアカウントが表示されるかは、**このドメインからのアカウントのみ表示**というオプションによって異なります。**すべてのドメイン**が選択されている場合は、すべてのMDaemonアカウントがリストに表示されます。検索オプションが、このダイアログの最上部にあります。どのドメインに属する以外に、表示するアカウントを定義することができます。

一覧では、エントリ毎に、アカウントのステータスアイコン(後述を参照)、メールボックス、それぞれが属するドメイン、アカウント保有者の[リアルネーム]、所属するグループ、メッセージ数、使用しているディスク容量(MB)、最後のアクセス時間、メールの保存先フォルダが表示されます。この一覧は、カラムをクリックする事で、昇順または降順でソートすることができます。いずれかのカラムの見出しをクリックすると、リストは昇順でソートされます。同じカラムの見出しを再度クリックすると、次にリストは降順でソートされます。

デフォルトでは、リストには一度に500アカウントしか表示されません。現在選択しているドメイン(または[**すべてのドメイン**]を選択している場合は、すべてのアカウント)の続きを表示する場合は、**次を表示**ボタンをクリックすると、次の500アカウントを表示します。一度に500以上のアカウントを表

> 示させたい場合は、MDaemon.iniファイルを開き、MaxAccountManagerEntries=500というキーを必要な値に変更してください。

アカウント ステータスアイコン

 アカウントはグローバルまたはドメイン管理者

 フルアクセスアカウント。POPおよびIMAPアクセスが可能。

 制限アカウント。POPやIMAP、又はその両方が無効。

 凍結アカウント。MDaemonは対象アカウント宛のメールを受け付けるが、ユーザーによるメール確認やメール送信不可。

 無効なアカウント。このアカウントへのすべてのアクセスが無効。

新規
このボタンをクリックすると、新規アカウントを作成するための[アカウント エディタ](#)を開きます。

編集
リストからアカウントを選択し、このボタンをクリックして[アカウント エディタ](#)を開きます。アカウントを選択し、ダブルクリックしても、同様の画面を起動できます。

削除
アカウントを削除するには、リストからアカウントを選択してこのボタンをクリックしてください。削除処理を進める前に、本当に削除するかどうかの確認メッセージが表示されます。

このドメインからのアカウントのみ表示
このドロップダウンリストから**すべてのドメイン**を選択すると、すべてのMDaemonアカウントが表示されます。特定のドメインのアカウントのみを表示させる場合は、対象ドメインを選択します。

次を表示
リストには一度に500アカウントしか表示されません。500以上のアカウントが存在する環境でこのボタンを押すと、次の500アカウントが表示されます。一度に500以上のアカウントを表示させたい場合は、上記の注意事項の内容をご確認の上、表示する最大アカウント数の設定を変更して下さい。

先頭へ
アカウント一覧の最初へ素早く戻るにはこのボタンをクリックします。

インポート
カンマ区切りのテキストファイルからアカウントをインポートする場合は、このボタンをクリックします。これは、アカウント ≫ インポート ≫ カンマ区切りテキストファイルからアカウントをインポート、と同じです。

テンプレート
このボタンをクリックし、グループとテンプレート 712 ダイアログを開きます。新しいアカウント 722 のデフォルト設定やアカウントグループのメンバー設定の管理が行えます。

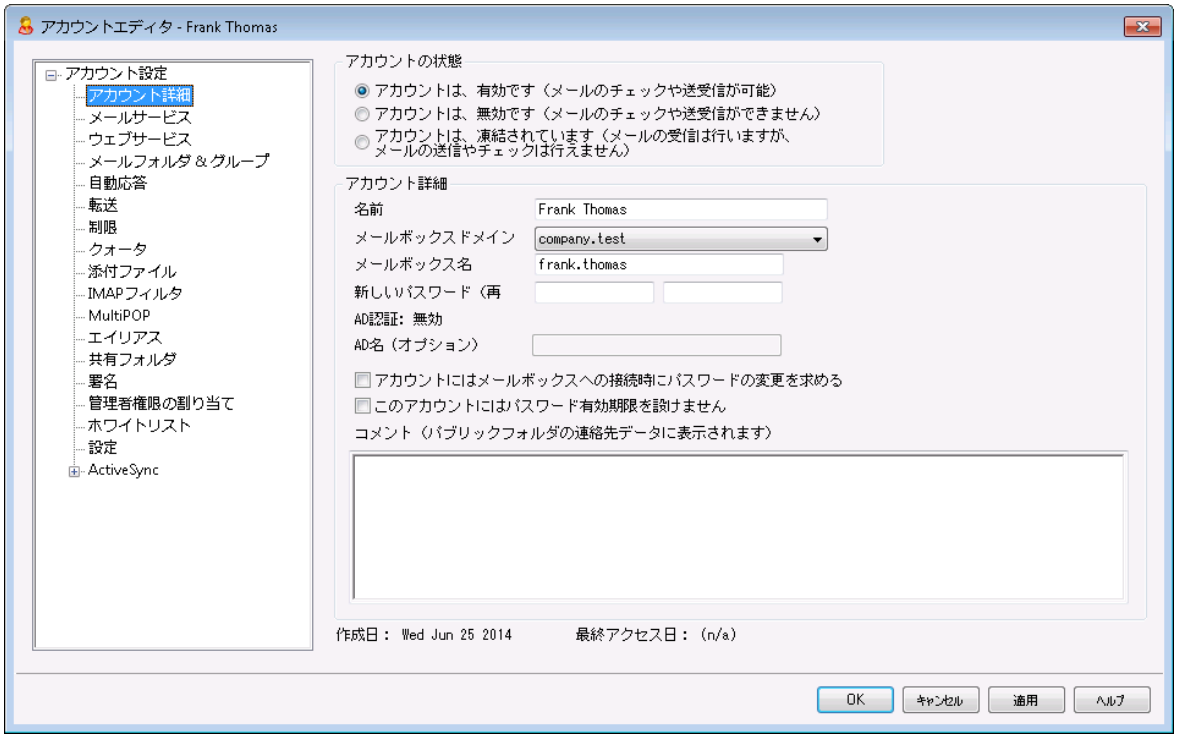
De-list
管理しているメーリングリスト 251 の購読を中止する場合、アカウントを選択し、このボタンをクリックします。ダイアログが現れ削除の確認を行います。

参照:

アカウントエディタ 650
新規アカウントの作成テンプレート 722

5.1.1 アカウントエディタ

5.1.1.1 アカウント詳細



アカウントの状態

アカウントは、有効です（メールのチェックや送受信が可能）
これはデフォルトオプションで、アカウントはメールのチェックや送受信が行えます。

アカウントは、無効です（メールのチェックや送受信ができません）
アカウントに対する全てのアクセスを無効にする場合はこのオプションを選択します。ユーザーはどういった目的あであっても、メールボックスへアクセスしたりメールの送受信を行う事はできません。アカウ

ントは無効にしても、削除される訳ではなく、MDaemonのライセンス数としてはカウントされます。無効化されたアカウントが他のユーザーとフォルダ共有していた場合、他のユーザーはフォルダのACL権限[285]に基づきアクセスする事ができますが、この1つの例外を除き、MDaemonの動作としては、アカウントが存在しない場合と同様の挙動となります。

アカウントは、凍結されています（メールの受信は行いますが、メールの送信やチェックはできません）
アカウントが、メール受信はでき、メールの確認や送信は行えないようにする場合はこのオプションを選択します。これは、例えばアカウントがハイジャックされている可能性がある場合などに便利です。アカウントの凍結は悪意のあるユーザーによるメッセージ送信を防ぐ事はできますが、受信メールに対してはアクセスできてしまうため注意が必要です。

アカウント詳細

名前
ユーザの名前をここに登録します。新規のアカウント作成時、ユーザの名前を入力し、メールボックスドメインを選択すると、アカウントエディタの各種の画面で（メールボックス名やフォルダ名など）幾つかのフィールドの値は、自動的に入力されます。名前フィールドには、!や| を使用することができません。

メールボックスドメイン
このドロップダウンリストでアカウントが所属するドメインを選択します。デフォルトではMDaemonのデフォルトドメイン[165]が表示されます。

メールボックス名
ここでの値はドメイン内の他のアカウントと重複しない、一意のものである必要があります。完全なメールアドレス（例．[*メールボックス名*]@[メールボックスドメイン]）がアカウントの識別やPOP3、IMAP、Webmailのログインに使用されます。メールアドレスには空白や!や| を使用することはできません。また、ここでは@を使う事はできません。例えば、"frank.thomas@ "といった指定はせずに、"frank.thomas"と指定して下さい。

新しいパスワード（再入力）
パスワード変更を行う場合は、新しいパスワードをそれぞれのボックスへ2回入力します。このパスワードはアカウントがMDaemonのPOP3やIMAPでメールの送受信を行う時、SMTPで認証を行う時、WebmailやRemote Administration, MDaemon Connectorを使用する時に使用します。どちらのボックスもパスワードが一致しない場合やパスワード制限[778]に抵触した場合は赤でハイライトされます。それ以外の場合は緑でハイライトされます。

このアカウントで Active Directory認証[788] を使用している場合は、2つのバックスラッシュと、ユーザーが所属しているWindowsドメインをパスワードの代わりに入力する必要があります。（例：123Passwordではなく¥¥ALTN）その下のパスワードフィールドには、対象アカウントのAD認証が有効か無効かを示す短いステートメントが入ります。

メールアカウントがPOP3/IMAPを利用しないものだったとしても、パスワードは必ず設定して下さい。メールセッションの認証に加え、メールアドレスとメールボックスパスワードは、リモートアカウント設定やリモートファイルの取得を許可するために使用されます。POP/IMAPアクセスを無効にする場合、メールサービス[654]画面のオプションを使用します。すべてのサービスへのアクセスを禁止する場合は、**アカウントは無効です**や**アカウントは凍結されています**のオプションを選択してください。

AD名（オプション）
アカウントへアクセスするActive Directoryのアカウント名をオプションで指定する場合はこちらから行って下さい。

アカウントはメールボックスへの接続前にパスワードの変更が必要
POP, IMAP, SMTP, Webmail, Remote Administrationへ接続する前に、ユーザーにメールボックスパスワードの変更を要求する場合は、このオプションを有効にします。ユーザーはWebmailやRemote Administrationへの接続は行えますが、処理を行う前にパスワード変更を求められます。ただし、パスワード変更を行うためには、ウェブサービス[656]画面のアクセス権の設定箇所で、ユーザーに対する「パスワードの変更」権限を与えておかなくてはならないので、ご注意下さい。パスワードが変更されると、このオプションは無効になります。

> パスワードの変更は一部のユーザーにとっては簡単な事ではなかったり、環境によっては不可能な場合がありますので、このオプションを有効にする際には注意して下さい。

パスワードは有効期限なし
アカウントをパスワード[778]ダイアログで設定したパスワード有効期限オプションから除外する場合はこの設定を有効にします。

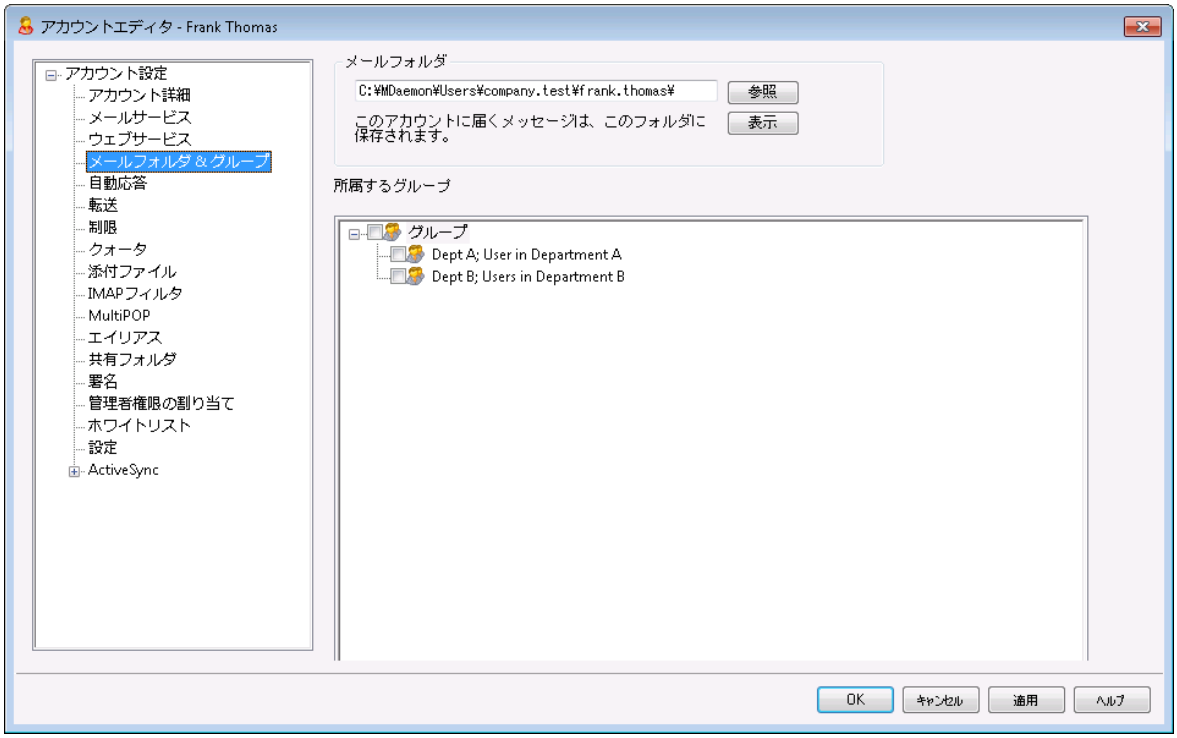
コメント
アカウントの公開メモを追加します。

> ここでの説明は、対象アカウントのパブリック連絡先情報にも含まれるものであり、他のユーザーからも閲覧できます。ここへはプライベートな情報は入力しないよう注意してください。対象アカウントに関するプライベートなメモやコメントは、管理者権限[690]の画面から入力して下さい。

参照:

AD認証[788]
パスワード[778]
アカウントエディタ ≫ ウェブサービス[656]

5.1.1.2 メールフォルダ & グループ



メールフォルダ

アカウントのメールを保存するフォルダを入力します。アカウントを新たに作成すると、このフォルダのデフォルトは、アカウントの作成テンプレート[723]で指定したメールフォルダ設定を元に決定します。

表示
このボタンを押すと、ユーザーのメールフォルダ情報をキュー/統計マネージャ[805]で確認することができます。

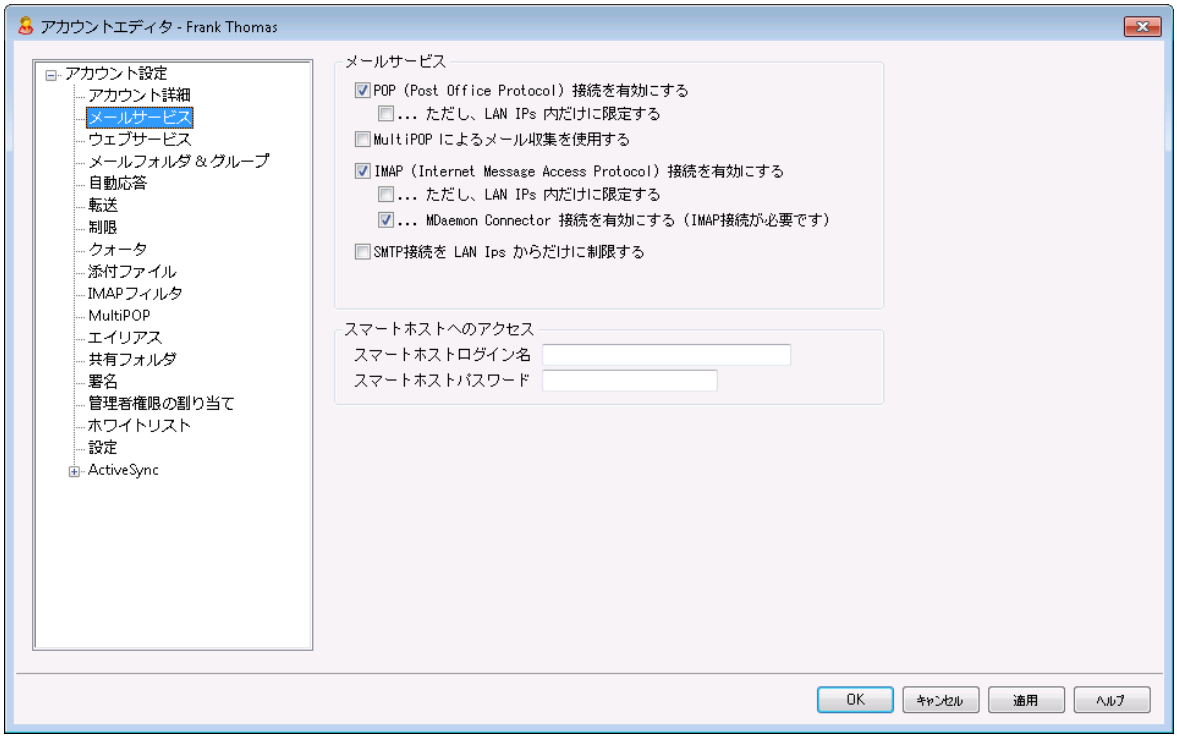
所属するグループ

アカウントを1つまたは複数のグループ[712]へ追加するにはこのボックスを使用します。各グループの隣にあるチェックボックスを選択し、アカウントをグループへ追加してください。

参照:

アカウントの作成テンプレート[723]
グループ[712]

5.1.1.3 メールサービス



この画面では、POP, IMAP, MultiPOP, MDaemon Connectorの中で、アカウントが使用できるメールサービスを設定します。Webmail経由でのメールへのアクセスは、ウェブサービス[656]画面で設定できます。ここには追加でアカウント用のスマートホスト用認証情報も設定できます。

メールサービス

POP (Post Office Protocol)を使用する
この設定が有効の場合、アカウントはPost Office Protocol (POP)を使ってメールへアクセスできるようになります。このプロトコルは、全てのメールクライアントが対応しているプロトコルです。

...ただし、LAN IP 内だけに限定する
ユーザーがLAN IPアドレス[554]からの接続の場合のみPOPアクセスを許可する場合は、このオプションを有効にして下さい。

MultiPOPによるメールを収集を有効にする
アカウントが MultiPOP[673] を使用できるようにするには、このオプションを有効にします。MultiPOPを使うと、ユーザーは他のメールサーバーで管理している、別のメールアドレスのメールを同時に収集できるようになります。

IMAP (Internet Message Access Protocol)を使用する
この設定が有効の場合、アカウントは Internet Message Access Protocol (IMAP)を使ってメールへアクセスできるようになります。IMAPはPOP3よりも広い目的に対応したプロトコルで、サーバー側でメールを管理し、複数のクライアントから接続することができます。多くのメールクライアントソフトウェアが、このプロトコルに対応しています。

...ただし、LAN IP 内だけに限定する
ユーザーがLAN IPアドレス[554]からの接続の場合のみIMAP経由でのアクセスを許可する場合は、このオプションを有効にして下さい。

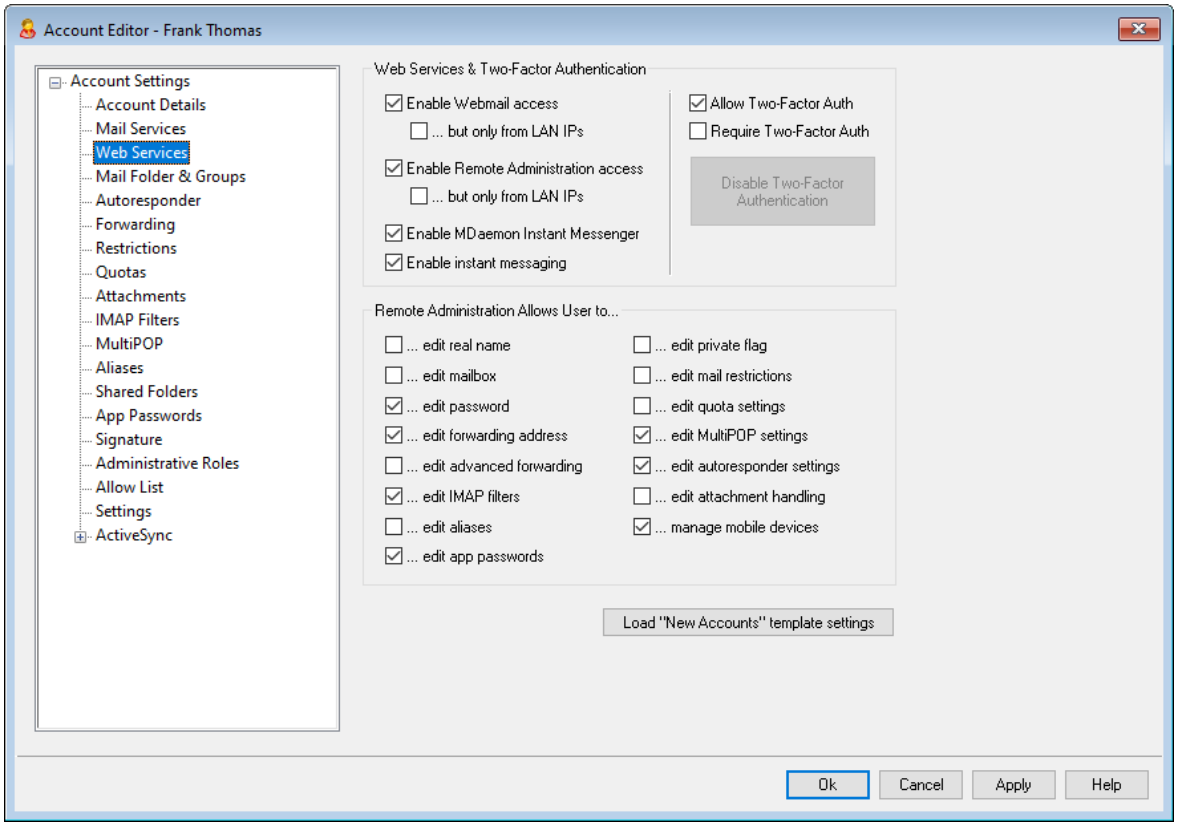
...MDaemon Connectorを有効にする（IMAPが必要です）
MDaemon Connector[353]を使って、新規に作成したアカウントがMicrosoft Outlookでデータ共有できるようにするには、このオプションを有効にします。**注意：** このオプションはMDaemon Connectorがインストールされている場合のみ有効です。

SMTP接続をLAN IPからだけに制限する
SMTP接続をLAN IPのみに制限する場合はこのボックスを有効にします。これによりネットワークに接続していないアカウントのメール送信を防ぐ事ができます。アカウントが外部のIPからメール送信を行うと、接続が拒否され送信を中止します。

スマートホストへのアクセス

スマートホストログイン/パスワード
設定 ≫ サーバ設定の 配信[85] 画面で、アカウント毎の認証を許可のオプションが有効の場合で、アカウント毎の認証をこのアカウントでも使いたい場合は、アカウントのスマートホスト用の認証情報をここで入力します。ユーザー毎の認証を使わない場合はここを空白のままにしておきます。

5.1.1.4 ウェブサービス



ウェブサービス

Webmailへのアクセスを有効にする
ユーザがWebブラウザを使用して、メールの確認やその他操作をWebmail[291]で行えるようにするには、このチェックボックスを選択します。

...ただし、LAN IP内だけに限定する
ユーザーがLAN IPアドレス[554]からの接続の場合のみWebmailへのアクセスを許可する場合は、このオプションを有効にして下さい。

Remote Administrationへのアクセスを有効にする
MDaemonのユーザに、Remote Administration[321]経由でのアカウント設定の変更を許可する場合は、この機能を有効にしてください。ユーザは以下の項目で有効にした設定のみを編集することが可能です。

この機能が有効で、Remote Administrationサーバーが稼働していると、ユーザーはMDaemon用のドメインとRemote Administration用ポート[321](例. http://example.com:1000)をブラウザで指定する事によりRemote Administrationにログインすることができます。まずログオン画面が表示され、次にユーザが編集の許可を与えられている設定画面が表示されます。ユーザに必要な作業は、選択した設定を変更して、[変更を保存]ボタンをクリックするだけです。そして、ブラウザからログアウトしてブラウザを閉じます。 ユーザーがWebmailに対するアクセス権も与えられている場合、Webmailの詳細オプションメニューからもRemote Administrationへアクセスする事ができます。

（アカウントエディタの管理者権限の割り当て690画面で指定する）全体あるいはドメイン管理者としてのアクセス権限が与えられているユーザの場合、Remote Administrationにログオンしたあとに表示される画面が異なります。

...ただし、LAN IP内だけに限定する
ユーザーがLAN IPアドレス554からの接続の場合のみWebmail経由でのアクセスを許可する場合は、このオプションを有効にして下さい。

MDaemon Instant Messengerを有効にする
アカウントがWCIM292を使用できるようにするにはこの設定を有効にします。

インスタントメッセージを有効にする
アカウントのMDIM利用を有効にしている場合で、MDIMのインスタントメッセージも利用できるようにする場合は、このオプションをクリックします。このチェックボックスがクリアされている場合、WCIMの他の機能は利用できますが、インスタントメッセージは利用できません。

ユーザーのカテゴリ編集を許可
Webmailユーザーのカテゴリ編集を許可する場合はこのオプションを使用します。これはデフォルトで有効です。

WebmailセッションのIPパーシステンスチェックをスキップ
Webmailウェブサーバー295オプションの"Webmailセッションを通してIPパーシステンスを使用する"が有効な時、ユーザーをIPパーシステンスの要件から除外するにはこのオプションを有効にします。

2段階認証

MDaemonは、各ユーザーがWebmailやMDaemonのRemote Administrationのウェブインターフェイスへのログインに使用する、2段階認証（2FA）に対応しています。HTTPSでWebmailへサインインできるユーザーは、オプション≫セキュリティ画面上で、アカウントの2段階認証を有効にすることができます。2段階認証を設定すると、ユーザーはWebmailやRemote Administrationへログインする際、認証コードの入力が必要になります。サインインに必要な認証コードは、ユーザーのモバイルデバイスやタブレット用の認証アプリから取得できます。この機能はGoogle認証に対応しているクライアント全てで利用できます。アカウント毎の2FA設定の詳細は、Webmailのヘルプファイルを参照して下さい。

2段階認証を許可する
デフォルトで、新規アカウント728はWebmailにおける2段階認証の設定や利用を許可されています。新規アカウントの2段階認証利用を許可しない場合には、このチェックボックスをクリアして下さい。

2段階認証を必須とする
ユーザーがWebmailにサインインする際、2段階認証（2FA）を強制的に使用させる場合は、このオプションを有効にします。2FAが構成されていないアカウントは、Webmailへの次回サインイン時に設定画面にリダイレクトされます。アカウントの2FAの設定の詳細については、Webmailのヘルプファイルを参照してください。

2段階認証を無効化する
アカウントの2段階認証を無効にするにはこのボタンをクリックします。例えば、ユーザーが端末を紛失し、認証情報へアクセスできない場合などに、このボタンを使用します。

Remote Administrationで行える設定

リアルネーム
この機能を有効にすると、ユーザは*姓名* 650を変更することが許可されます。

メールボックス
この機能を有効にすると、ユーザは*メールボックス名* 650を変更することが許可されます。

メールボックスはアカウントのメールアドレス(アカウント用の固有識別子およびログイン値)の一部であるので、これを変更するという事は、ユーザが自分の実際のメールアドレスを変更していることを意味します。これは、拒否あるいは削除されたような古いアドレスとなる可能性があります。

パスワード
ユーザがアカウントのメールパスワードの変更できるようにする場合、このチェックボックスを選択します。パスワード要件については パスワード 778を参照してください。

転送アドレス
この機能を有効にすると、ユーザは転送 663アドレスの設定を変更することが可能になります。

転送先詳細設定
この機能を有効にすると、ユーザが*転送先詳細設定* 663を変更できるようになります。

IMAPフィルタ
このコントロールを使用すると、ユーザは自身のIMAPフィルタ 670を作成、管理できます。

エイリアスを編集
Remote Administrationからアカウントに関連した エイリアス 675 を編集できるかどうかを指定します。

Appパスワードを編集
デフォルトで、ユーザーはそれぞれ Appパスワード 683 を編集できます。ユーザーに編集させないようにするにはこのチェックボックスを無効にしてください。

プライベートフラグ
このオプションは、ユーザがRemote Administrationから、アカウントエディタの設定 693画面にある *"Everyone"メーリングリスト*、*共有予定表*、*VRFYからアカウントを隠します"*オプションを編集できるかどうかを指定します。

メール制限
制限 664 画面の送信/受信メール制限を編集できるかどうかコントロールします。

クォータ設定
アカウントにクォータ 666設定の変更を許可する場合は、このチェックボックスを選択してください。

MultiPOP設定
MDRA 321で、新規のMultiPOP 673エントリを追加したり、それらのエントリに対してMultiPOP収集の有効化/無効化を行えるよう、アカウントに権限を与える場合はこの設定を有効にします。このオプ

ションとアカウントの*MultiPOPを有効*673設定のどちらも有効の場合、Webmail291のメールボックスページが有効化され、ユーザーが自分のMultiPOPメールボックス設定を行えるようになります。MultiPOPサーバーの有効化/無効化の全体設定は、設定 » サーバー設定 » MultiPOP130から行えます。

自動応答の設定
ユーザにアカウントの自動応答660の追加、編集、または削除を許可する場合は、このチェックボックスを選択してください。

添付ファイル処理の編集
ユーザが、添付ファイル669画面の中の添付ファイル処理オプションを編集できるようにする場合、このチェックボックスを選択します。

モバイルデバイスの管理
アカウント所有者が、Remote Administrationを使って、BlackBerryやActiveSyncデバイスといった、端末毎の設定を行えるようにするにはこのオプションをチェックします。

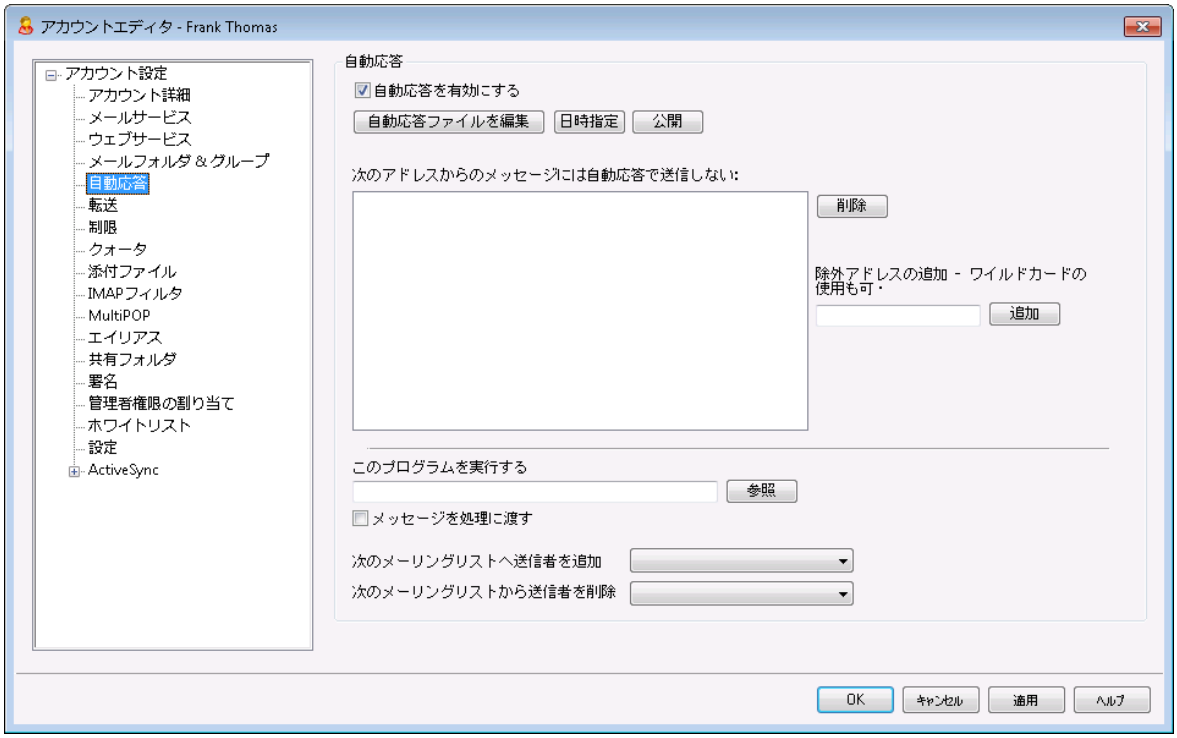
新規アカウントテンプレート設定を読み込む

この画面の設定を*アカウントの作成*テンプレートのウェブサービス728で指定しているデフォルト値へ戻すにはこのボタンをクリックします。

参照:

Webmail291
Remote Administration321
テンプレートマネージャ » ウェブサービス728

5.1.1.5 自動応答



自動応答は、例えば、プログラムの実行、メーリングリストに送信者を追加、自動的に生成されたメッセージでの応答など、受信メールによって特定のイベントを発生するのに便利な機能です。自動応答で最も一般的な使用方法は、メールの受信者が休暇中ですぐに対応できず、できるだけ早く返信する、といった内容の返信を自動で送信するというものです。Webmail[291]またはRemote Administration[321]へのWebアクセス[656]を使って、MDaemonユーザは、自動応答メッセージの作成や自動応答の利用期間のスケジュール設定が行えます。最後に、自動応答はユーザーのルート¥data¥フォルダにあるOOF.mrkファイルの内容を元にしています。このファイルは多数のマクロに対応しており、その結果として、自動応答機能へ高い柔軟性を搭載しています。

メッセージがリモートソースからの場合、自動応答は常に引き継がれます。ただし、ユーザーが属するドメインから送信されるメッセージについては、自動応答 » 設定[765]画面の、メールに自動応答するオプションが有効な場合のみ実行されます。自動応答メールは、送信者毎に1日1回までと制限する事もできます。

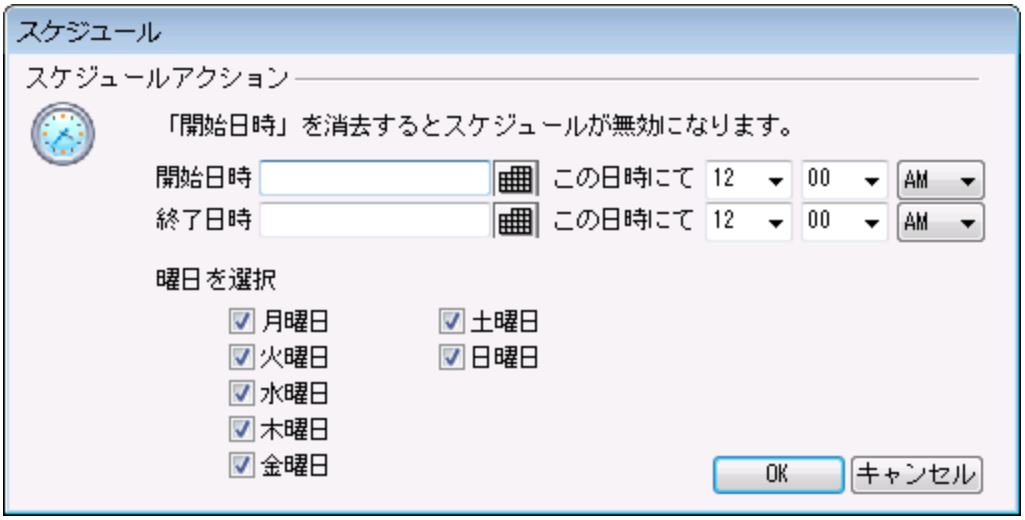
自動応答

自動応答を有効にする
このコントロールを有効にすると自動応答機能が開始されます。詳細は自動応答[761]を参照してください。

自動応答ファイルの編集
自動応答スクリプトを開いて編集する場合はこのボタンをクリックします。このファイルはユーザーの¥data¥フォルダにあるOOF.mrkファイルです。

スケジュール

このボタンをクリックするとスケジュールダイアログが開き、自動応答の開始と終了の日時やアクティブにしておく曜日をここで設定できます。自動応答を継続的に起動させたい場合は、スケジュールを空欄にしてください。



公開

アカウントの自動応答ファイルを他のアカウントへコピーするにはこのボタンをクリックします。自動応答をコピーしたいアカウントを選択し、OKをクリックします。

次のアドレスからのメッセージには自動応答で返信しない
ここには、自動応答から除外するアドレスを入力してください。

> 場合によって、自動応答メッセージを送ったメールアドレスで、更に自動応答メールが返信される場合があります。これは、「ピンポン」のように、2台のサーバ間でメールが絶えず行ったり来たりする状態を生み出してしまう可能性があります。こうしたアドレスを確認した場合は、送受信し合ってしまう先程のような状態を避けるため、ここで対象アドレスを登録しておきます。同様なオプションは自動応答 ≫ 設定[765]画面にもあり、自動応答メールは、送信者毎に1日1回までと制限する事もできます。

削除
このボタンをクリックすると、除外リストで選択したエントリを削除することができます。

除外アドレスの追加 -ワイルドカード使用可
[除外アドレスの追加]テキストボックスにアドレスを入力してこのボタンをクリックすると、除外リストにそのアドレスが追加されます。

実行するプログラム

このプログラムを実行する

新規のメールが、このアカウントに届く時、実行するプログラムのパスおよびファイル名を指定するために、このフィールドを使用します。注意は、このプログラムが適切に終了し無人で実行することができる必要があります。任意のコマンドラインパラメータは、必要に応じて実行可能なパスの後に登録することができます。

メッセージを処理に渡す

このオプションを選択すると、[実行するプログラム]フィールドで指定した処理は、最初に利用できるコマンドラインパラメータとして、実行されるメッセージの名前を渡されます。自動応答が、メールを他の場所へ転送しているアカウントに設定され、そして自分のメールボックスにローカルのコピーを保持していない時は(転送 663 参照)、この機能は無効になります。

デフォルトでは、MDaemonはコマンドラインの最後のパラメータとしてメッセージファイル名を渡します。$MESSAGE$マクロを使って、この動作を変更することができます。例えば、メッセージファイル名が置かれるべき場所にこのマクロを使うとします。すると、logmail /e /j /message=$MESSAGE$ /qのような複雑なコマンドラインの使用が可能になり、より柔軟な設定ができるようになります。

メーリングリスト

次のメーリングリストへ送信者を追加

このフィールドにメーリングリストのアドレスを入力すると、メールの送信者は自動的にメーリングリストのメンバーに追加されます。これは、自動的にメーリングリストを作成する場合に非常に便利な機能です。

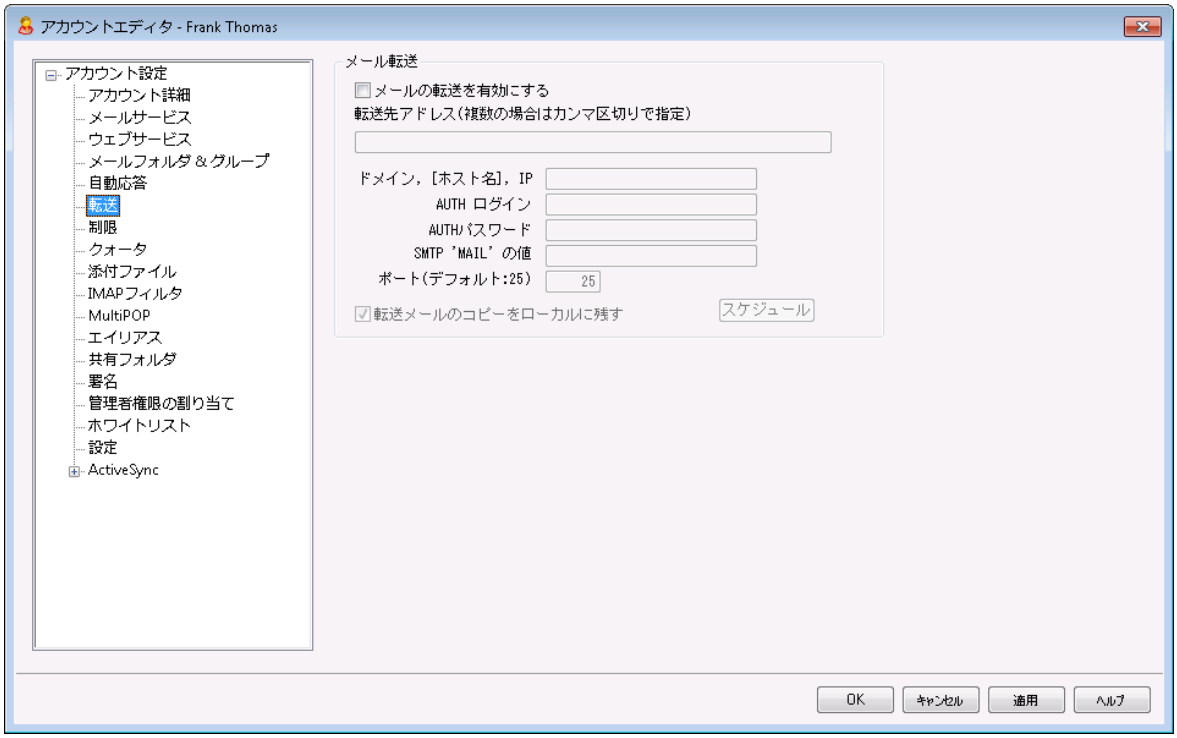
次のメーリングリストから送信者を削除

このフィールドにメーリングリストのアドレスを入力すると、メールの送信者は自動的にメーリングリストから削除されます。

参照:

自動応答 ≫ アカウント 761
自動応答 ≫ 許可リスト 764
自動応答 ≫ 設定 765
自動応答スクリプトの作成 766

5.1.1.6 転送



メール転送

メールの転送を有効にする
次の転送先アドレスで指定したアドレスに、メッセージを転送する場合、このチェックボックスを選択します。Webmail[291]またはRemote Administration[321]に対するWebアクセス権限[656]をもつMDaemonユーザは、管理者に設定変更を依頼するのではなく、自分自身で転送設定を行う事ができます。

転送先アドレス(複数の場合はカンマ区切りで指定)
このアカウントの受信メッセージのコピーを転送する必要あるアドレスで指定するために、このフィールドを使用します。上記のメール転送を有効にするオプションが有効の場合、受信メールのコピーが自動生成され、ここで指定されているアドレスへ転送されます。複数アドレスへの転送は、カンマ区切りで指定します。

ドメイン, [ホスト名], IP
転送メールを特定のドメインのMXサーバといった他のサーバを経由させるには、このオプションを有効にし、ここにそのドメインを入力してください。転送メールの送信に特定のホストを経由させる場合は、カギかっこでその値を入力してください。(例: [host1.example.com])

AUTHログイン/パスワード
転送に必要なログイン/パスワード認証情報を入力します。

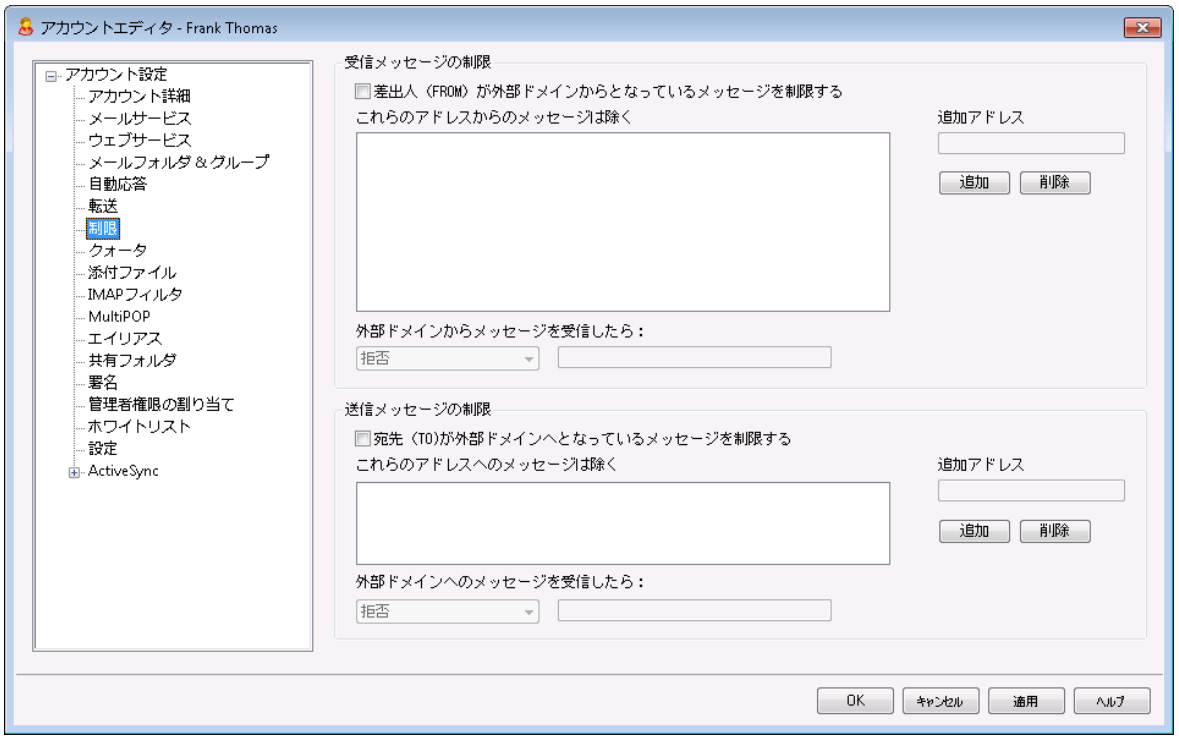
SMTP 'MAIL'の値
アドレスをここで指定すると、受付ホストとのSMTPセッション中に、"MAIL From"ステートメントとして、実際の送信者の代わりにここで指定した値が使用されます。空のSMTP"MAIL From"ステートメント(すなわち"MAIL FROM <>")を必要とする場合、このオプションに"[trash]"を入力します。

使用するTCPポート
MDaemonは、ここで指定されるTCPポートを使用して転送されたメッセージを送信します。デフォルトSMTPポートは25です。

転送メールのコピーをローカルに残す
デフォルトで、転送されたメール毎のコピーは、ローカルユーザのメールボックスに通常配信されます。このチェックボックスを選択しないと、ローカルコピーは保持されません。

スケジュール
このボタンでメールの転送スケジュールを作成します。開始日時と終了日時、曜日の指定が行えます。

5.1.1.7 制限



この画面では、アカウントがローカルではないドメインとのメッセージ送受信を制限するオプションの設定を行います。

受信メッセージの制限

差出人（FROM)が外部ドメインからとなっているメッセージを制限する
ローカルドメイン以外からのメッセージを、このアカウントで受け取らない場合は、このチェックボックスを選択してください。

...これらのアドレスからのメッセージは除く
このフィールドで指定されるアドレスは、内部向けメール制限の例外となります。ここでの設定には、ワイルドカードが使えます。したがって、例外として"*@altn.com"を指定した場合、altn.comからのメールすべて受信され、目的のアカウントへ配信されます。

追加アドレス
新しいアドレスを内部向けメール制限の例外として追加する場合は、このフィールドにそのアドレスを入力し、[追加]ボタンをクリックしてください。

追加
[追加アドレス]オプションにアドレスを入力した後、このボタンをクリックすると、そのアドレスが例外リストに追加されます。

削除
制限リストからアドレスを削除する場合は、目的のアドレスを選択して、この[削除]ボタンをクリックしてください。

外部ドメインからメッセージを受信したら
このドロップダウンリストで選択できるオプションでは、ローカルではない、あるいは認証されていないドメインからのメールが到着した時、そのメールをどのように処理するかを指定することができます。以下のオプションから選択してください。

拒否 - 制限されたメールは、MDaemonによって受信を拒否されます。

送信者に戻す - 制限されたアドレスからのメールは、送信者に返送されます。

postmasterに送信 - 制限されたメールは受信されますが、目的のアカウントではなくPostmasterに転送されます。

指定アドレスへ送信 - 制限されたメールは、MDaemonに受け入られますが、テキストボックスで指定したアドレスへ配信されます。

送信メッセージの制限

宛先(TO)が外部ドメインへとなっているメッセージを制限する
ローカルドメイン以外にメッセージを送信しない場合は、このチェックボックスを選択してください。

...これらのアドレス宛のメッセージは除く
このフィールドで指定されるアドレスは、送信メール制限の例外となります。ここでの設定には、ワイルドカードが使えます。したがって、例外として"*@altn.com"を指定した場合、altn.comへの送信メールはすべて許可され、通常どおり配信されます。

追加アドレス
新しいアドレスを送信メール制限の例外として追加する場合は、このフィールドにそのアドレスを入力し、[追加]ボタンをクリックしてください。

追加
[追加アドレス]オプションにアドレスを入力した後、このボタンをクリックすると、そのアドレスが例外リストに追加されます。

削除
制限リストからアドレスを削除する場合は、目的のアドレスを選択して、この[削除]ボタンをクリックしてください。

外部ドメインへのメールを受信したら...
このドロップダウンリストで選択できるオプションでは、ローカルではない、あるいは認証されていないドメインへのメールが発信された時、そのメールをどのように処理するかを指定することができます。以下のオプションから選択してください。

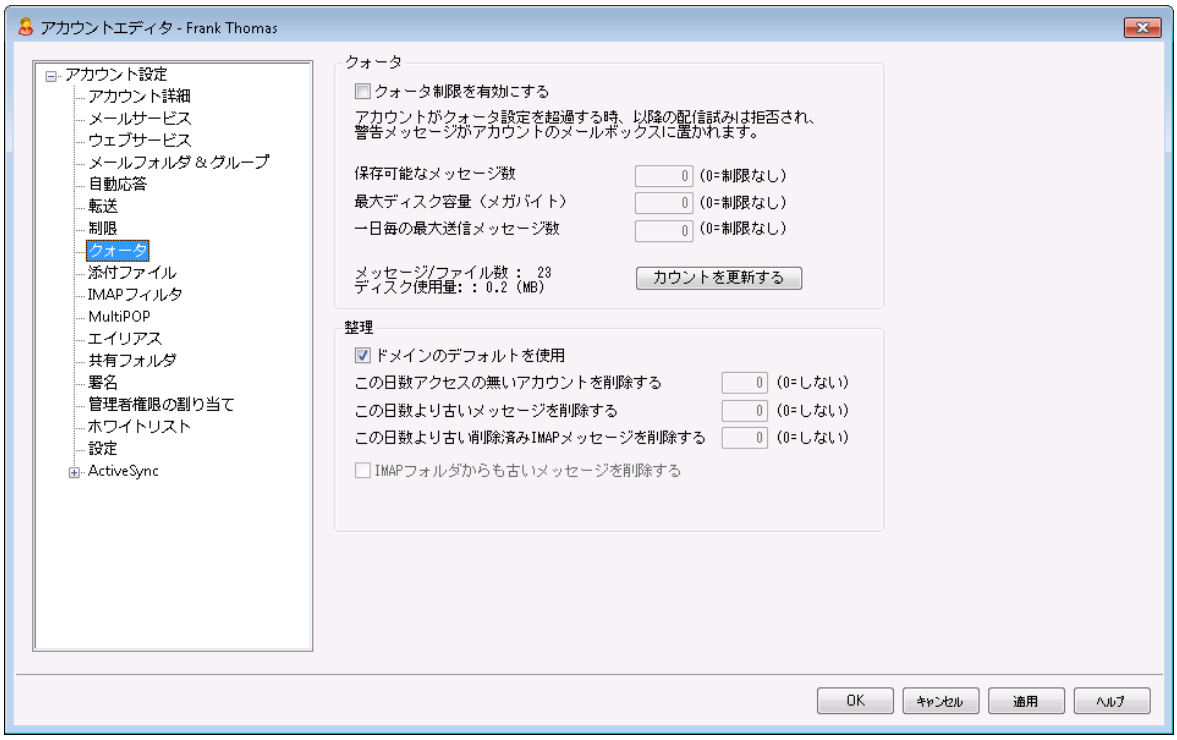
拒否
メッセージはMDaemonによって送信を拒否されます。

送信者に戻す
制限されたドメイン宛てのメールは、送信者に返送されます。

postmasterに送信
制限されたメールは、MDaemonに受け入れられますが、目的のアカウントではなくPostmasterに転送されます。

指定アドレスへ送信
制限されたメールは、MDaemonに受け入られますが、テキストボックスで指定したアドレスへ配信されます。

5.1.1.8 クォータ



クォータ

クォータ制限を有効にする
アカウントで保存ができるメッセージの最大数、あるいは(アカウントのドキュメントフォルダ内の添付ファイルを含む)アカウントが使用できるディスクの最大容量を制限するには、このチェックボックスを選択します。アカウントへのメール配信時、最大メッセージ数またはディスク容量制限を超えると、メッセージは拒否され、警告メッセージがユーザのメールボックスに設定されます。MultiPOP[673]収集がアカウントの最大を超える場合、類似した警告は発行され、アカウントのMultiPOPエントリは、自動的に無効へ切り替えられます(ただし、データベースから削除されることはありません)。

"アカウント ≫ アカウント設定 ≫ クォータ[738]" で*上限に近付いたアカウントへクォータ警告メールを送信する*オプションを使用するとクォータ制限に近づいたアカウントへメールが送信されます。アカウントが指定した保存する最大メール数や最大ディスク容量の制限値に対して、指定したパーセンテージを超えると、深夜に対象アカウントに対する警告メールが送信されます。メールはアカウントのメール数、メールボックスのサイズ、使用済のパーセンテージと残りのパーセンテージを情報として含みます。さらに、既存の警告メールがアカウントのメールボックスに残っていた場合は、その後更新された警告メールで、既存のメールが上書きされます。

保存可能なメッセージ数
アカウントに対して保存することができるメッセージの最大数を指定するために、このオプションを使用します。オプションで0(ゼロ)をすると、メッセージ数の制限はありません。

最大ディスク容量(メガバイト)
アカウントのドキュメントフォルダで保存している添付ファイルを含むディスク容量の最大量を指定するために、このオプションを使用します。オプションで0(ゼロ)をすると、メッセージ数の制限はありません。

一日毎の最大送信メッセージ数
アカウントが一日にSMTPを使って送信できる最大メッセージ数を指定する場合はこのオプションを使用します。この値に到達すると、深夜にカウンターがリセットされるまで、メッセージを送信する事ができなくなります。0を指定すると、アカウントが送信できるメッセージ数は無制限になります。

カウントの更新
このボタンをクリックすると左側に表示されているメール/ファイルカウントと使用済ディスク容量の統計がアップデートされます。

整理
このセクションのオプションは、アカウントが非アクティブになってからMDaemonによって削除されるまでの時間を指定するために用います。アカウントに関係ある古いメッセージが一定量の時間の後、削除されるかどうか、指定することもできます。MDaemonは毎晩深夜に、この設定で指定された期間を過ぎたすべてのメッセージを削除したり、または休止状態の日数制限に到達したアカウントの完全削除を行います。

ドメインデフォルトを使用
デフォルトの整理設定はドメイン毎に行い、ドメインマネージャの設定[193]画面からアクセスできます。テンプレートで管理しているアカウントに対する設定をドメインのデフォルト設定値で上書きするにはこのチェックボックスをクリアし、次のオプションで任意の値を設定してください。

次の日数非アクティブのアカウントを削除（0 = 削除しない）
このドメインに属するアカウントが指定日数の間、未使用のままである場合、このアカウントは削除されます。0（ゼロ）の値を指定すると、アカウントが使用されていなくても削除しません。

この日数より古いメールを削除（0 = 削除しない）
この値は、メッセージがMDaemonによって自動的に削除される前に、ユーザのメールボックスに残す日数を指定できます。0（ゼロ）の値を指定すると、メッセージの経過日数に関係なく削除されないことを意味します。 **注意点：** このオプションは「IMAPフォルダからも古いメッセージを削除する」オプションが有効になっていない限り、IMAPフォルダへは適用されません。

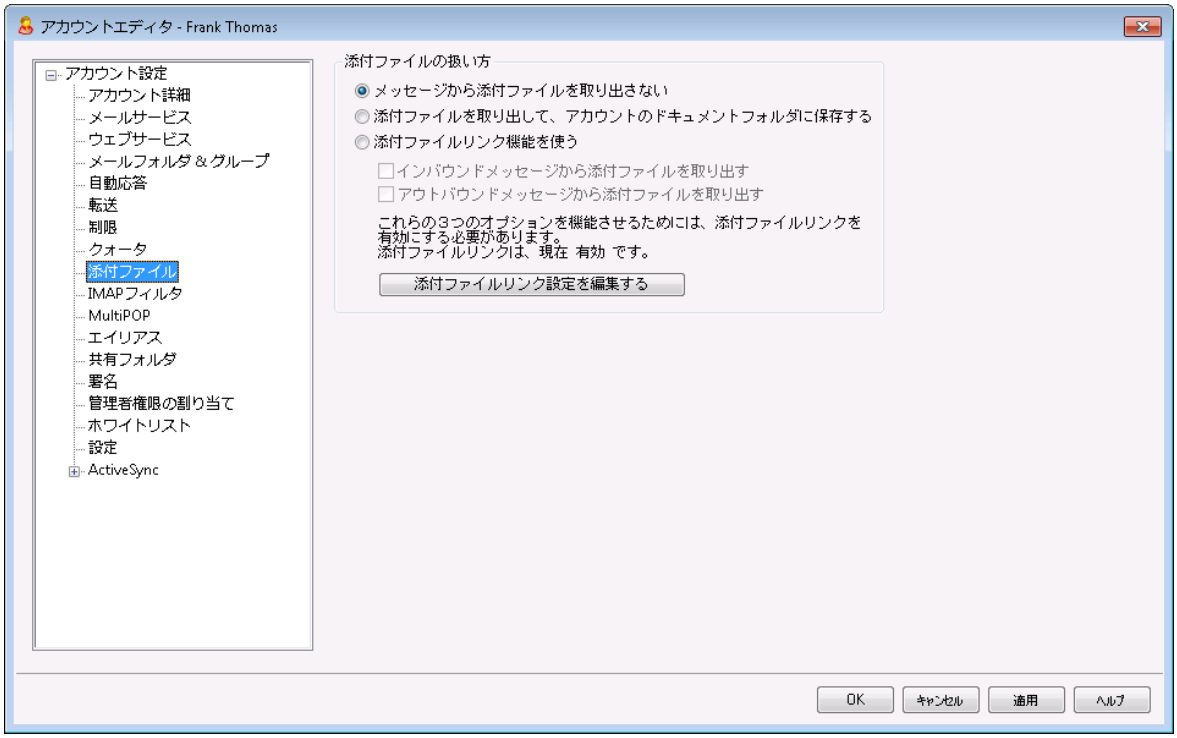
この日数よりも古いIMAPメールを削除（0 = 削除しない）
このコントロールを使用し、指定日数を超えたIMAPフォルダ内のメールへ削除フラグを追加します。ここで指定された日数よりを超えると、削除フラグが追加され、対象メールがメールボックスから削除されます。0（ゼロ）の値を指定すると、IMAPメッセージは古さにかかわらず、決して削除されないことを意味します。

IMAPフォルダからも古いメッセージを削除する
この日数よりも古いメールを削除を、IMAPフォルダ内のメッセージにも適用する場合は、このチェックボックスをクリックしてください。このコントロールが無効の場合は、IMAPフォルダ内のメッセージは、古いものであっても削除される事はありません。

参照：

テンプレートマネージャ » クォータ 738
アカウント設定 » クォータ 782

5.1.1.9 添付ファイル



添付ファイル処理

この画面ではMDaemonがアカウントのメッセージの添付ファイルを展開するかどうかを指定します。このオプションに対するデフォルト値はテンプレートマネージャ[740]から設定できます。

メッセージから添付ファイルを取り出さない
このオプションが有効の場合、添付ファイルはアカウントのメッセージから取り出されません。添付ファイル付のメッセージは通常のメールと同様に処理され、添付ファイルはメッセージに組み込まれたままの状態となります。

添付ファイルを取り出してアカウントのドキュメントフォルダへ保存する
設定されている場合、MDaemonはアカウント宛の受信メールへBase64 MIMEフォーマットの添付ファイルがあった場合、これを自動的に取り出します。取り出されたファイルは受信メールからは削除され、アカウントのドキュメントフォルダへ保存されます。メッセージ本文の中に、取り出されたファイル名が追加されます。このオプションでは保存された添付ファイルへのリンクを提供する事はありませんが、ユーザーはWebmail[291]からドキュメントフォルダへアクセスする事ができます。

添付ファイルリンク機能を使う
添付ファイルが付いている送受信メールに対して添付ファイルリンク機能を使用するにはこのオプションを選択します。

> このオプションが有効でも添付ファイルリンク[333]ダイアログで添付ファイルリンク機能が無効になっていた場合、添付ファイルは取り出される事はありません。

インバウンドメッセージの添付ファイルを展開する
このオプションが有効の場合、添付ファイルは受信メールから取り出され、添付ファイルリンク333で指定された場所へ保存されます。メッセージ本文の中に、URLリンクが追加され、これをクリックするとファイルをダウンロードできます。セキュリティのため、URLリンクはダイレクトアクセスURLではありません。代わりにリンクには一意の識別子（GUID）が含まれていて、サーバー側で実際のファイルとリンクしています。GUIDマップは`AttachmentLinking.dat`ファイルで管理されています。このオプションはデフォルトで有効です。

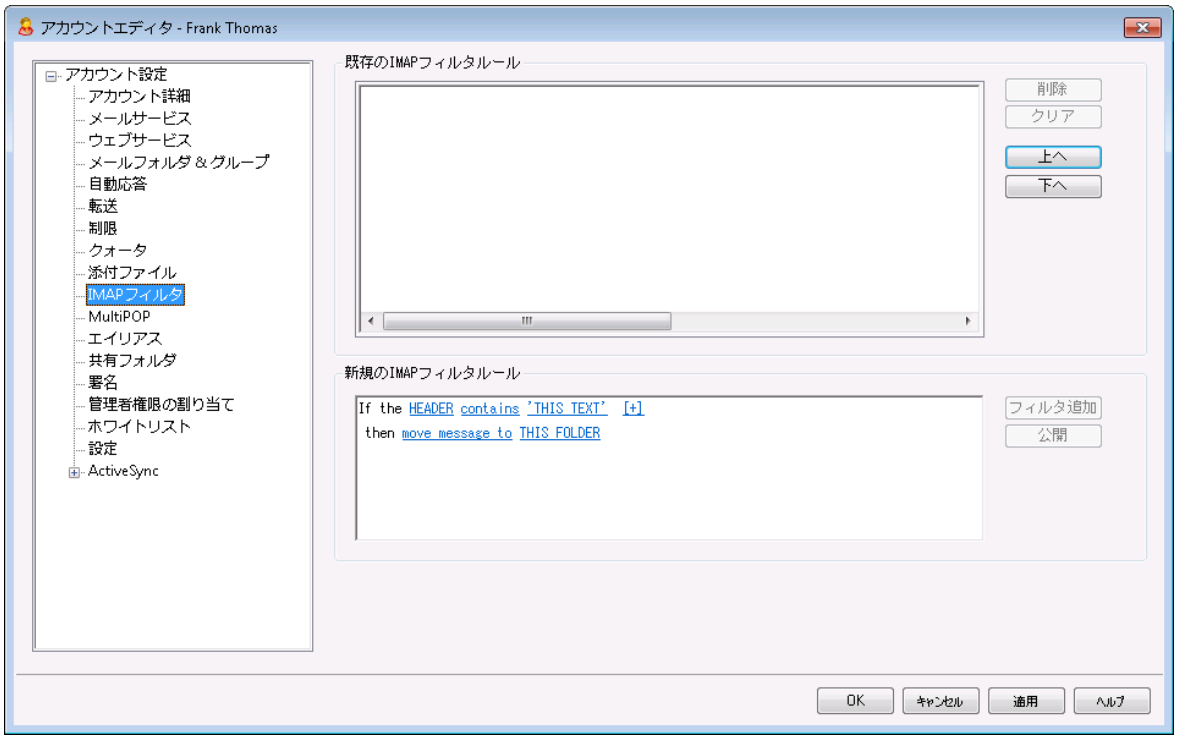
アウトバウンドメッセージの添付ファイルを展開する
このオプションを有効にすると、添付ファイルリンク機能で送信メールから添付ファイルを取り出す事ができます。アカウントがメールを送信すると、添付ファイルは取り出され、ファイルをダウンロードするためのURLが代わりに追加されます。

添付ファイルリンク設定を編集する
このボタンをクリックすると添付ファイルリンク333ダイアログが起動します。

参照:

添付ファイルリンク653
テンプレートマネージャ » 添付ファイル740

5.1.1.10 IMAPフィルタ



IMAPやWebmail[291]ユーザは、フィルタを使って特定のメールを自動振り分けすることができます。コンテンツフィルタ[588]と同様に、MDaemonは受信メールのヘッダに記載されたドメインを、フィルタルールと比較します。アカウントへのメールが、それらの規則の1つと一致すると、その規則で指定されるフォルダに振り分けられます。この方法は、クライアント側でメッセージをフィルタにかけるよりも(クライアントとサーバの両方にとって)はるかに効率的です。IMAPメールの中にはローカルメール規則やフィルタリング機能さえないものがある中で、MDaemonではこのような機能も提供が可能なのです。

管理者は、アカウントエディタのIMAPフィルタ画面や、Remote Administration[321]を使ってフィルタを作成することができます。しかし、ユーザにWebmailまたはRemote Administration内から彼ら自身でフィルタを作成して管理する許可を与えることもできます。これらの許可は、ウェブサービス[656]画面で設定できます。

既存のIMAPフィルタルール

この画面へは、アカウントに対して作成されたすべてのフィルタのリストを表示します。フィルタは、一致が起こるまで、リストに示される順位で処理されます。そのために、メッセージフィルタのうち1つと一致すると、そのフィルタで指定されているフォルダへ移動し、そのメッセージのためのフィルタ処理は終わります。リストでフィルタを別の位置へ動かすために、**上へ**および**下へ**ボタンを使用します。

削除

リストの中の目的のエントリを選択し[削除]ボタンをクリックすると、そのフィルタを削除することができます。

クリア

このボタンをクリックするとフィルタ全体を削除します。

上へ

リストの中のフィルタを選択し、このボタンをクリックすると、そのフィルタの順番を上に移動することができます。

下へ

リストの中のフィルタを選択し、このボタンをクリックすると、そのフィルタの順番を下に移動することができます。

新規のIMAPフィルタルール

画面にあるリンクから、新しくIMAPフィルタルールを作成できます。ルールが完成したら、**フィルタを追加**で既存のIMAPフィルタルールへ作成したルールを追加できます。

フィルタ条件

フィルタリングルールの最初のセクションにあるリンクをクリックすると、フィルタ条件の設定が行えます。フィルタ条件に一致したメッセージに対して、フィルタアクションが適用されます。

HEADER

HEADERを押して、フィルタルールで検索対象とするヘッダやその他のメッセージコンポネントを選択して下さい。**TO**, **CC**, **FROM**, **SUBJECT**, **SENDER**, **LIST-ID**, **X-MDMAILING-LIST**, **X-MDRCPT-TO**, **X-MDDNSBL-RESULT**, **X-SPAM-FLAG**, **MESSAGE SIZE**, **MESSAGE BODY**, **Other...** の中から選択できます。「Other...」を選択すると、フィルタ条件の設定用ウィンドウが起動するので、一覧にはないヘッダ条件をここで指定します。MESSAGE SIZEを選択すると、「contains」と「THIS TEXT」リンクが「is greater than」と「0 KB」へ置き換えられます。

contains / is greater than
contains や**is greater than** をクリックし、ヘッダ検証時の条件の種類を選択します。例えば、ヘッダが存在するかどうか、特定のテキストを含んでいるか、特定のテキストから始まったり特定のテキストで終わっているか、などです。具体的には、次の条件の中から選択する事ができます。: **starts with**, **ends with**, **is equal to**, **is not equal to**, **contains**, **does not contain**, **exists**, **does not exist**, **is greater than**, **is less than** 。「is greater than」と「is less than」オプションはHEADERリンクが「MESSAGE SIZE」の場合のみ有効です。

THIS TEXT / 0 KB
MDaemonがフィルタ用に選択したヘッダ内を検索するのに、検索対象とする文字列を入力して下さい。HEADERオプションがMESSAGE SIZEと設定されている場合、リンクは"0 KB"と表示され、フィルタ条件ダイアログボックスが起動し "Message size in KB"の指定を行うためのボックスが表示されます。

[+] [x] and
フィルタルールで条件を2つ以上設定する場合は **[+]** をクリックします。これで新しい行が追加され、フィルタの拡張用に "HEADER," "contains," "THIS TEXT" コンポネントも表示されます。複数条件のフィルタルール付きメッセージをテストする際、デフォルトでメッセージはルールと一致するそれぞれの条件を通過しなくてはなりません。条件のどれかに一致させたい場合は、「and」をクリックし「or」を選択します。フィルタルールが複数行ある場合、削除したい行がある場合は、対象の行の隣にある**[x]**をクリックして下さい。

フィルタアクション

フィルタリングルールの下のセクションにあるリンクをクリックすると、メールがフィルタ条件に一致した場合に実施するアクションの設定が行えます。

move message to
フィルタのアクション先を指定する場合は、"**move message to**" をクリックします。次の中から選択する事ができます: **move message to**, **delete message**, **redirect message to**, forward message to。

THIS FOLDER / EMAIL
アクションで"move message to"を選択した際、 **THIS FOLDER** をクリックすると、メッセージの保存先フォルダを選択できます。メールをリダイレクトや転送するよう選択した場合は、EMAILをクリックし、宛先メールアドレスを入力して下さい。リダイレクトされたメールは、メールヘッダや本文への変更は行われません。唯一の変更点はSMTP envelopeの宛先です。転送メールでは、新しいメールがSubjectと本文を元のメールから引用した状態で作成されます。

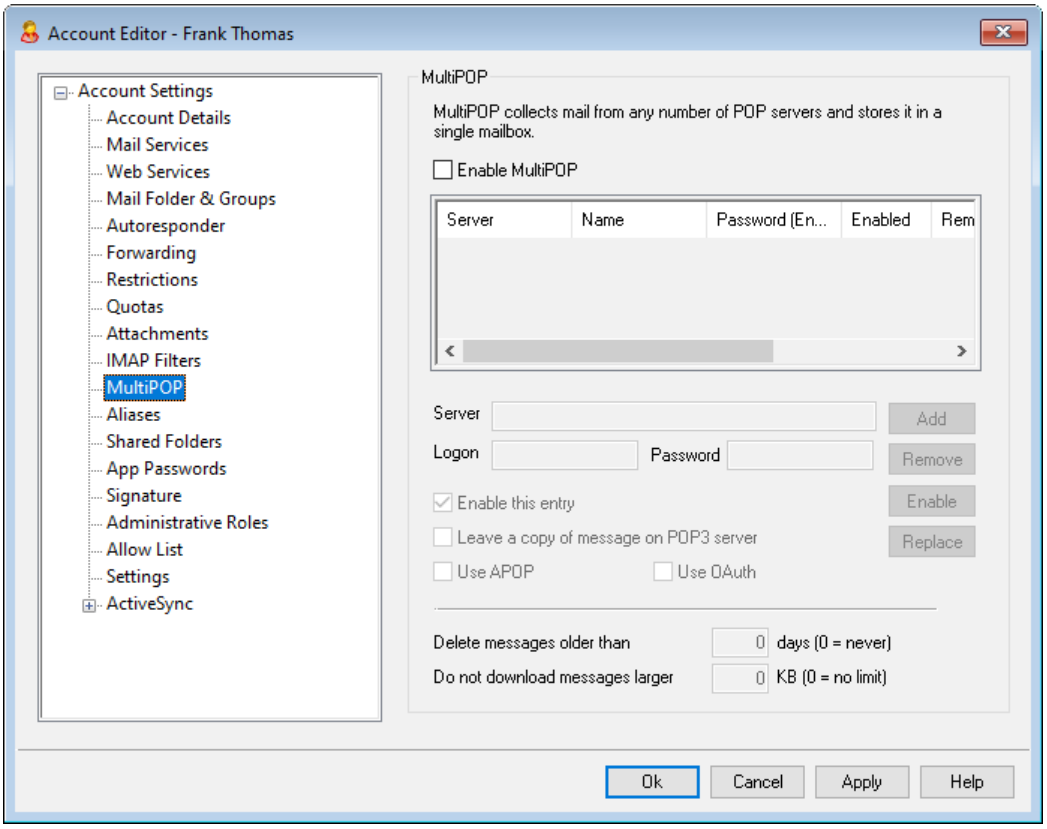
フィルタを追加

新しいフィルタの設定が完了したら、このボタンを押し、*既存のIMAPフィルタルール一覧*へ新しいルールを追加します。

公開

ルール作成後、公開をクリックしてルールをアカウントのドメインに所属する全アカウントに対してコピーします。ルールを他のアカウントへコピーするかどうかの確認ダイアログが表示されます。

5.1.1.11 MultiPOP



MultiPOP機能により、POP3のホスト/ユーザ/パスワードの組み合わせで、複数のソースからのメール収集を行うことができます。これはメールアドレスを複数持っているユーザーが、一カ所でメールを管理したい場合に役立つ機能です。MultiPOPで収集されたメールは、ユーザのメールボックスへ配信される前に、ローカルキューに配置されるため、他のメールと同様に、自動応答やコンテンツフィルタを適用する事ができます。MultiPOPのスケジュールオプションは、 設定 ≫ イベントスケジューリング ≫ メールスケジュールオプション ≫ MultiPOP収集[350]からアクセスできます。

MultiPOPを有効にする
MultiPOPを有効にするには、このチェックボックスを有効にします。ユーザーがMDRA[321]で自分のMultiPOP設定を編集できるようにするには、アカウントのWebサービス[656]ページで「*…MultiPOP設定を編集*」を有効にしてください。このオプションとwebサービス設定のどちらも有効の場合、Webmail[291]のメールボックスページが有効化され、ユーザーが自分のMultiPOPメールボックス設定を行えるようになります。MultiPOPサーバーの有効化/無効化の全体設定は、設定 » サーバー設定 » MultiPOP[130]から行えます。このオプションが無効の場合、アカウントオプションが有効であってもMultiPOPは利用できません。

MultiPOPエントリを作成又は編集

サーバ名
メールを収集するPOP3サーバを入力してください。標準のPOP3ポート以外のポートで接続する必要がある場合は、サーバー名の後に“:[port]”を付与します。例えば、“mail.example.com:1000”といった形式です。Gmailや Microsoft（Office）365からメール

収集を行う場合は、"pop.gmail.com:995"や"outlook.office365.com:995"を使用します。

ログオン名
指定されたサーバでメールアカウントにアクセスするPOP3ユーザ名またはログオン名を入力してください。

パスワード
指定されたサーバでメールアカウントにアクセスするのに使用されるPOP3かAPOPのパスワードを入力してください。

APOPを使用
対応するホストからのメールを検索する際のAPOP認証にMultiPOPエントリを使用する場合は、このチェックボックスをクリックしてください。

OAuthを使用
GmailやOffice365からメール収集を行う際にはこの認証方式を選択します。サーバー設定 » MultiPOP の中の、MultiPOP OAuth 2.0 instructions 130 で詳細をご確認下さい。**注意点**: GmailやOffice 365をOAuthで使用できるようにするには、対象アカウントがWebmailへサインインし、メールボックスページでGmailやOffice 365の認証を行う必要があるため、アカウントのWeb サービス 656 ページで「*…MultiPOP設定を編集*」を有効にする必要があります。

POP3サーバにメッセージのコピーを残す
収集したメールのコピーをサーバに残す場合は、このチェックボックスをクリックしてください。これは、後で再び別のロケーションからメールを検索する場合に便利な機能です。全てのユーザーに対してこのオプションを上書きする、つまり、MDaemonにダウンロードした後POP3サーバーから常にメールを削除するためには、設定 » サーバー設定 » MultiPOP 130 の「*MultiPOPで収集後、常にサーバーからメールを削除*」オプションを有効にして下さい。

追加
このボタンをクリックすると、入力した値がMultiPOPのリストに追加されます。

削除
このボタンをクリックすると、リストから選択されたMultiPOPエントリが削除されます。

有効/無効
このスイッチを切り替えることにより、このエントリのMultiPOPを有効にするか、このエントリをスキップするかのコントロールをすることができます。

置換
このエントリを編集する場合は、一覧からエントリを選択し、目的の変更を行った後に、このボタンをクリックして変更を適用してください。

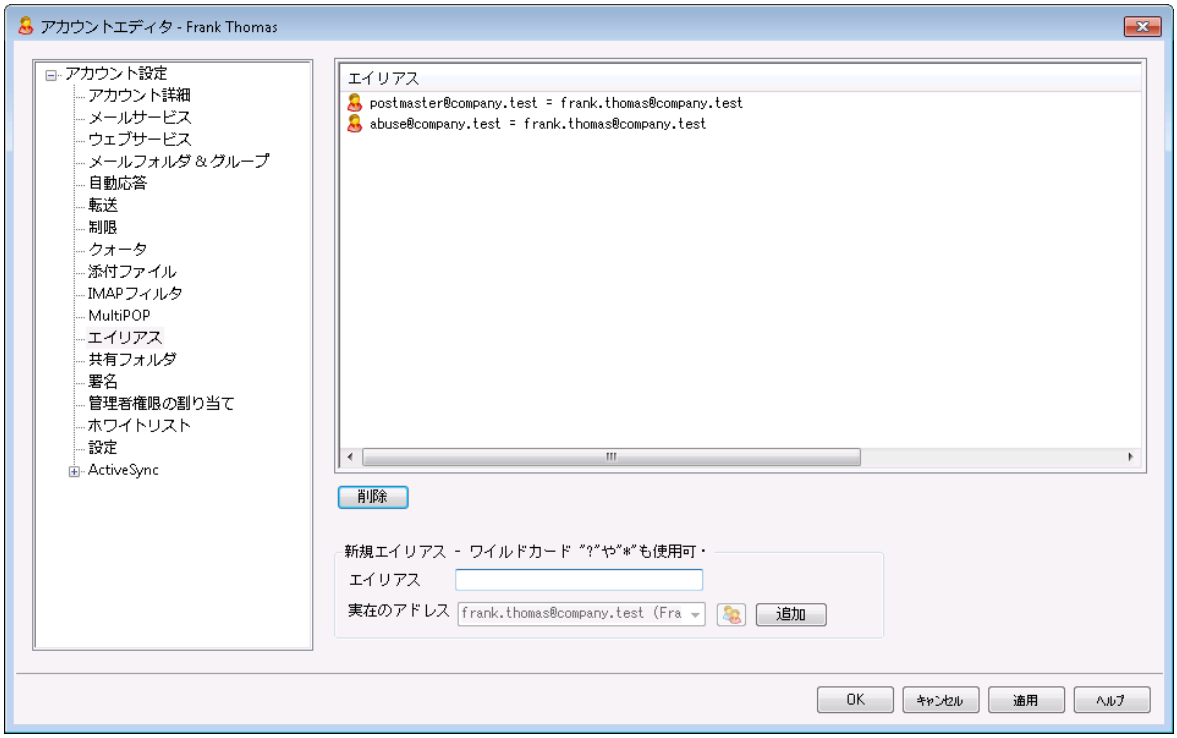
指定日数より古いメッセージを削除 [XX] 日 (0 = 削除しない)
この値は削除されるまでのMultiPOPホストに残す日数を指定します。古いメッセージを削除しない場合は0を指定します。

ダウンロードするメッセージの最大 [XX] KB (0 =無制限)
ダウンロードするメールの最大サイズを指定します。

参照:

サーバー設定 » MultiPOP 130
スケジュール 350 » 130 MultiPOP収集 350

5.1.1.12 エイリアス



この画面にはアカウントと関連するすべてのアドレスエイリアス 757 が一覧表示されており、ここからエイリアスの追加や削除が行えます。

エイリアスの削除

アカウントからエイリアスを削除するには、一覧でエイリアスを選択し、**削除**をクリックします。

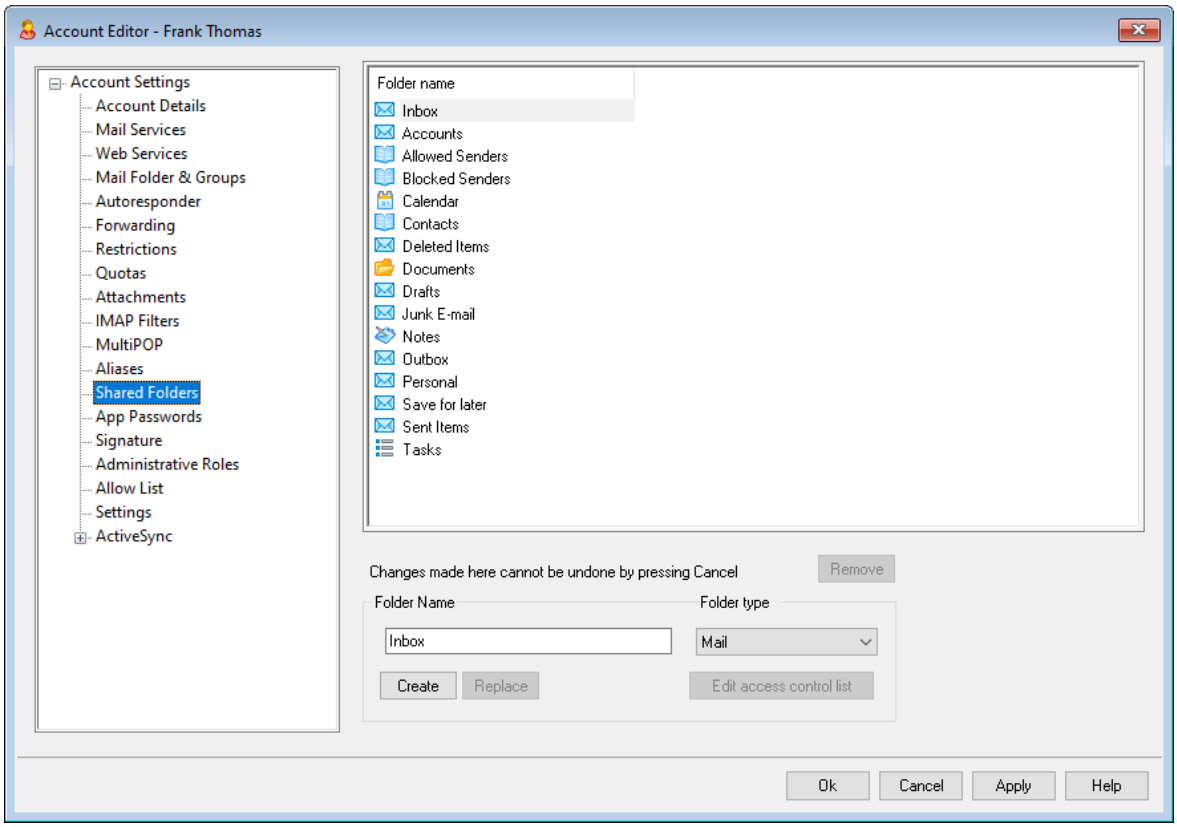
エイリアスの追加

アカウントに新規エイリアスを追加するには、新規エイリアスのテキストボックスへアカウントに関連づけるエイリアスを入力し、**追加**をクリックします。1文字や1語を示すワイルドカード"?"および"*"が利用できます。

参照:

アカウントエディタ ≫ エイリアス 757

5.1.1.13 共有フォルダ



この画面は、設定 ≫ サーバ設定 ≫ パブリックと共有フォルダ の パブリックと共有フォルダ 107 画面で 共有フォルダを有効にする オプションが有効な場合に利用できます。共有フォルダはパブリックフォルダマネージャ 283 で管理できます。

この上部セクションには、他のMDaemonユーザやグループ 712 と共有することができる、すべてのIMAPフォルダを表示します。アカウントが最初に作成される際、このエリアは、フォルダを追加するために フォルダ名 と作成 オプション(またはIMAPフィルタ 670 のオプション)を使用するまで、このフィールドはInboxを持つだけです。このリスト中のサブフォルダは、フォルダとサブフォルダ名がスラッシュで区切られます。

削除
表示されているリストからIMAP共有フォルダを削除するには、目的のフォルダを選択し、削除 ボタンをクリックしてください。

フォルダ名
新しいフォルダをリストに追加する場合は、このオプションでフォルダ名を指定し作成ボタンをクリックします。新しいフォルダをリスト中のフォルダのサブフォルダにする場合は、親フォルダの名前、区切り記号とスラッシュ、新しいフォルダ名の順に付けてください。例えば、親フォルダの名前が“My Folder”の場合、新しいサブフォルダの名前が“My New Folder”であれば“My Folder/My New Folder”となります。サブフォルダにしない場合は、新しいフォルダの名前は単に“My New Folder”となります。

フォルダの種類
このドロップダウンリストから必要なフォルダのタイプ(メール、予定表、連絡先など)を選びます。

作成
フォルダ名を入力したら、このボタンをクリックして新しいフォルダをリストに加えてください。

置換
共有フォルダを編集する場合は、そのエントリをクリックして必要な変更を行い[置換]をクリックしてください。

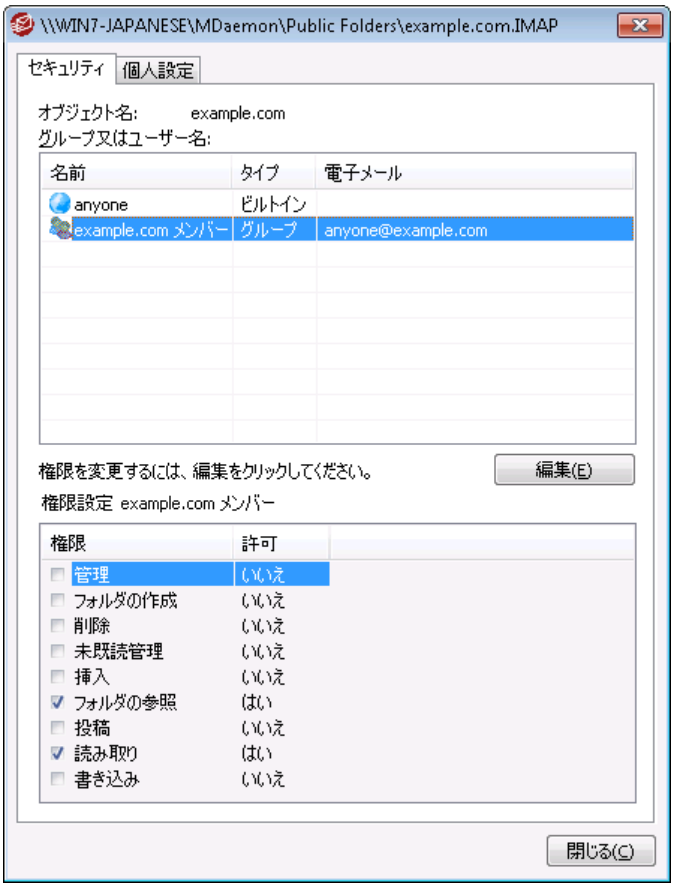
アクセスコントロールリストの編集
フォルダを選択しこのボタンをクリックすると、このフォルダ用の アクセスコントロールリスト 285ダイアログが開きます。 アクセスコントロールリストはフォルダへアクセスできるユーザーやグループを指定し、対象ユーザーやグループ毎にアクセス権を設定するのに使用します。

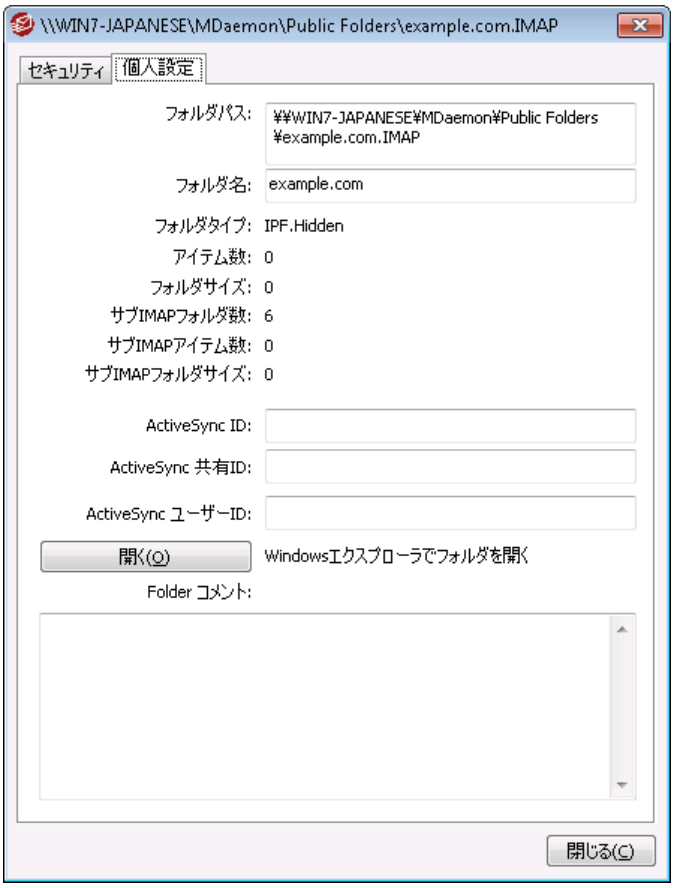
参照:

アクセスコントロールリスト 285
パブリックフォルダマネージャ 283

5.1.1.13.1 アクセスコントロールリスト

アクセスコントロールリスト（ACL）は、ユーザーやグループのパブリック及び共有フォルダ 105に対するアクセス権を設定するのに使用します。パブリックフォルダマネージャ 283のACLを編集ボタンか、アカウントエディタの 共有フォルダ 676 にある*アクセスコントロールリストの編集*ボタンをクリックし、この機能にアクセスできます。





セキュリティ

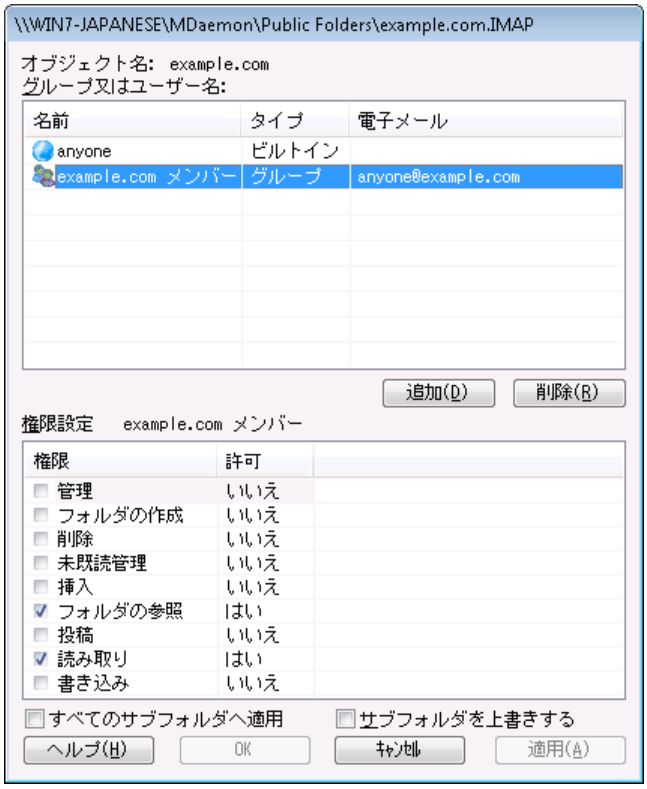
このタブにはフォルダに関連付けられたグループやユーザーの一覧と、詳細なアクセス権が表示されます。グループやユーザーを選択すると、下にあるアクセス権ウィンドウからそれぞれのアクセス権 288 が確認できます。アクセス権を編集するには編集 287 をクリックします。

個人設定

このタブにはフォルダのパスや名前、種類、サイズといった、プロパティが表示されます。

ACLエディタ

ACLのセキュリティタブで編集をクリックすると、ACLエディタが起動し、アクセス権の編集が行えます。



オブジェクト名
ACLアクセス権が適用されるオブジェクトやフォルダ名です。

グループ又はユーザー名
何らかのアクセス権限を持つグループやユーザーです。グループやユーザーを選択すると、権限設定ウィンドウにアクセス権が表示されます。アクセス権に並んで表示されているボックスをクリックする事で、対象のアクセス権限を割り当てる事ができます。

追加
一覧に表示されていないグループやユーザーを追加するには、追加 289をクリックします。

削除
グループやユーザーを削除するには対象のエントリを選択し、削除をクリックします。

<グループやユーザー>の権限設定
アクセス権限の隣にあるボックスをクリックする事で、上部で選択したグループやユーザーに対象のアクセス権限を割り当てる事ができます。

次のアクセス権限を選択できます。

管理者 – ユーザは、このフォルダのACL(アクセスコントロールリスト)を管理することができます。

作成 – ユーザは、このフォルダ中でサブフォルダを作成することができます。

削除 – ユーザは、このフォルダからメッセージを削除することができます。

未既読管理 – ユーザは、このフォルダのメッセージの既読/未読の状態を変更することができます。

挿入 – ユーザは、このフォルダにメッセージを追加したりコピーすることができます。

ルックアップ – ユーザは、IMAPフォルダの個人的なリストの中で、このフォルダを見ることができます。

投稿 – ユーザは、このフォルダに直接メールを送ることができます(フォルダが許可されている場合)。

読み込み – ユーザは、このフォルダを開いて、その内容を見ることができます。

書き込み – ユーザは、このフォルダのメッセージのフラグを変更することができます。

全てのサブフォルダへ適用
このフォルダのアクセス権を作成済のサブフォルダ全てに適用する場合はこのオプションを有効にします。フォルダのユーザー及びグループアクセス権がサブフォルダへ適用され、競合するアクセス権は上書きされます。しかし、現在既に設定されているアクセス権が削除される事はありません。

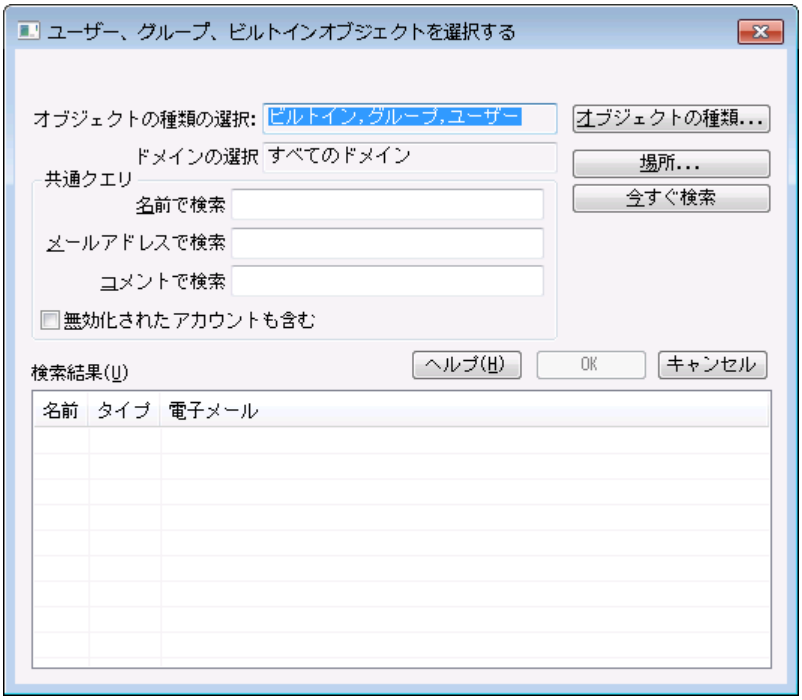
例えば

上位のフォルダがユーザーAとユーザーBに特定のアクセス権を割り当てており、サブフォルダはユーザーBとユーザーCにアクセス権を割り当てていたとします。このオプションではユーザーAのアクセス権をサブフォルダにも適用し、ユーザーBのサブフォルダに対する既存のアクセス権を上書きし、ユーザーCに対しては何の処理も行いません。そのため、サブフォルダはユーザーAとユーザーB、ユーザーCに対するアクセス権を持つことになります。

サブフォルダを上書きする
この設定を有効にすると、サブフォルダの全てのアクセス権が上位フォルダのアクセス権で上書きされます。サブフォルダのアクセス権は上位フォルダと同じものに設定されます。

グループやユーザーの追加

ACLエディタで追加をクリックし、グループやユーザーの追加用画面から検索や追加を行う事で、アクセスコントロールリストへグループやユーザーを追加できます。



オブジェクトの種類の選択
オブジェクトの種類をクリックし、追加したいグループやユーザーの種類を、ビルトイン、グループ、ユーザーの中から選択します。

場所の指定
場所をクリックし検索対象のドメインを選択します。ここでは全てのMDaemonドメインや特定のドメインを選択できます。

共通クエリ
このオプションを使用し、ユーザー名やメールアドレス、アカウントの説明[650]の一部を指定する事で、検索範囲を狭くする事ができます。オブジェクトの種類や場所に一致する全てのグループやユーザーを対象に検索を行う場合は、この項目を空白にして下さい。

無効化されたアカウントも含む
検索対象に無効化されたアカウント[650]も含む場合はこれをチェックします。

今すぐ検索
検索条件を指定した後、今すぐ検索をクリックし検索を行います。

検索結果
検索実行後、検索結果からグループやユーザーを選択し、OKをクリックする事で、対象グループやユーザーをACLへ追加できます。

アクセス権はMDaemonのACL(アクセスコントロールリスト)サポートによってコントロールされます。ACLは、IMAP4(インターネットメッセージアクセスプロ

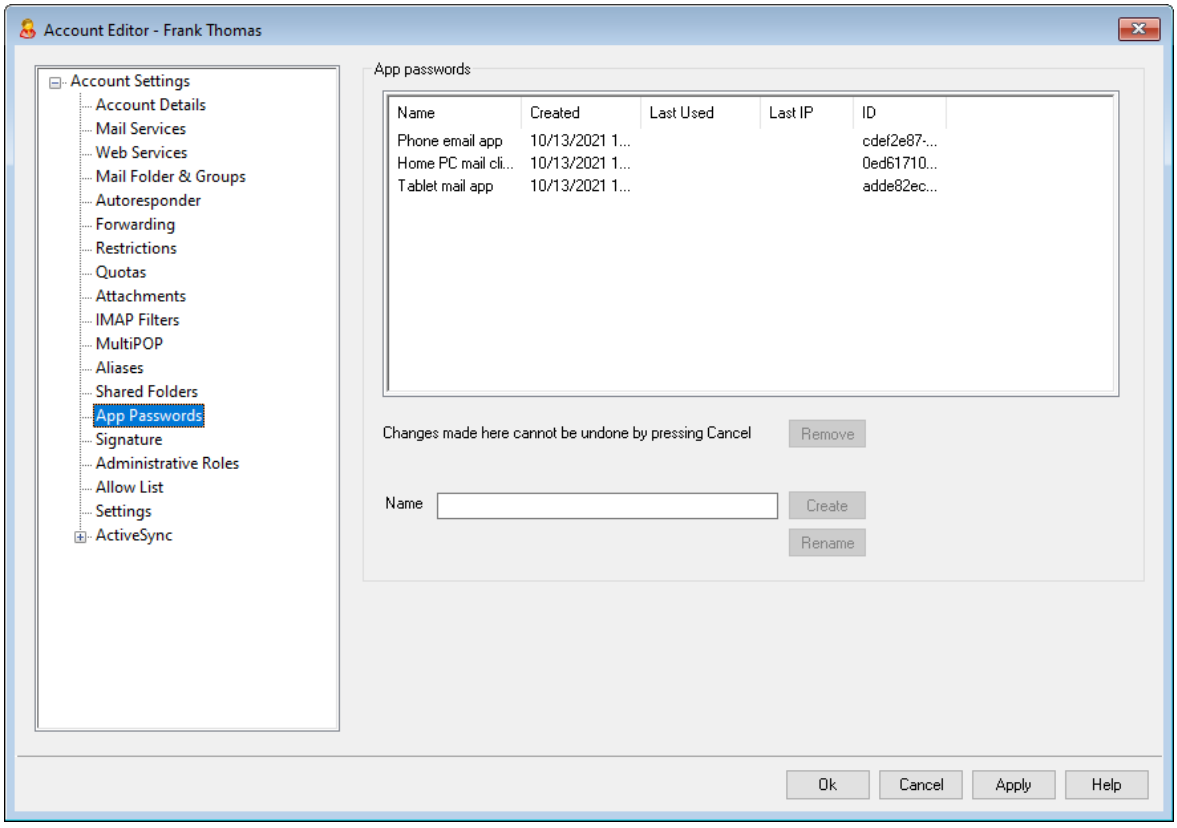
トコル)の拡張機能で、IMAPメールボックスにアクセス権限を割り当てるためのもので、これを使って他ユーザーにもフォルダに対するアクセス権限を与える事ができるようになっています。メールクライアントがACLに対応していない場合であっても、このダイアログからアクセス権限の設定が行えます。

ACLはRFC 2086で定義されており、次のサイトからご覧頂けます: http://www.rfc-editor.org/rfc/rfc2086.txt.

参照:

パブリックフォルダマネージャ 283
パブリックフォルダについて 105
パブリックと共有フォルダ 107
アカウントエディタ » 共有フォルダ 676
メーリングリスト » パブリックフォルダ 273

5.1.1.14 Appパスワード



Appパスワード

Appパスワードとは、メーラーやアプリで使用する、非常に強力なランダム生成されたパスワードで、メールアプリケーションのような2段階認証 656 (2FA)を使用できない場合であっても、これをより安全に利用するためのものです。 2FAを使用するとWebmailや MDaemon Remote Administration (MDRA)へ安全にサインインする事ができますが、メーラーは認証アプリを入力しなかった場合であってもバックグラウンドでメールへアクセスする必要がある事から、2FAを利用できません。Appパスワード機能を使う事で、アカウントパスワードを2FAに保護されている場合であっても、アプリで使用する強力で安全なパスワードを作成する事ができます。Appパスワードはメーラーでのみ使用でき、WebmailやMDRAへのログインには使用できません。つまり、Appパスワードが何らかの方法で不正に盗まれた場合であっても、認証されていないユーザーがアカウントのパスワードや他の設定を変更する事はできず、ユーザー本人は、アカウントへパスワードと2FAでログインし、盗まれたAppパスワードを削除し、新しいAppパスワードを必要に応じて作成する事ができます。

ユーザーのAppパスワードの利用を許可しない場合は、ユーザーのWebサービスページにある*...appパスワードの編集* 656 オプションを無効化する事ができます。Appパスワードを全ユーザーに対して無効化したい場合は、パスワードページの*appパスワードを有効にする* 778 オプションを無効化してください。

Appパスワードの要件と推奨設定

- Appパスワードを生成するには、アカウントの2FAが有効になっている必要があります。(ただし必要に応じてこの要件を無効化 778 する事もできます。)
- Appパスワードはメーラーでのみ使用できます - WebmailやMDRAへのサインインへは使用できません。
- Appパスワードは作成時に一度だけ表示されます。後から再取得は行えず、作成時にアプリケーションへ入力する必要があります。
- メーラー毎にAppパスワードは異なるものを使用する事をお勧めします。また、アプリケーションの利用を終了する際や端末を紛失したり盗難にあったりした際にはAppパスワードの削除をお勧めします。
- 各Appパスワードは、作成日、最終利用日時、アカウントのメールから最終アクセスした際のIPアドレスが併せて表示されます。最終利用日やIPアドレスのデータが疑わしい場合には、Appパスワードを削除し、再度作成する事をお勧めします。
- アカウントパスワードを変更すると、全てのAppパスワードは自動削除されます。ユーザーは古いAppパスワードを継続して利用する事はできません。

Appパスワードの作成と利用

Appパスワードの作成と管理はWebmailから次の手順で行えます(この情報はWebmailのヘルプファイルからも確認できます)。Appパスワードは作成時に一度しか表示されないため、まず最初に、メーラーやクライアントアプリでパスワードを入力できるようにして下さい。

1. アプリやメーラーでAppパスワードが入力できるよう準備します。
2. Webmailへサインインし、**オプション** ≫ **セキュリティ**をクリックします。
3. **現在のパスワード**へアカウントパスワードを入力します。
4. **新しいAppパスワード**をクリックします。
5. アプリケーション名(例. 携帯メーラー)を入力し、OKをクリックします。

6. メーラーでパスワードをコピー/貼付けるか、手動で入力するか、テキストファイルなどへ貼り付ける等を必要に応じて行います。パスワードをコピーして後ほど使用する場合には、メーラーへ入力後、コピーしたパスワードを忘れずに削除しておく事をお勧めします。完了したら、OKをクリックします。

何らかの理由で、他のユーザー用にAppパスワードの作成や削除を行う場合、このページのオプションを使って同様の操作が行えます。Webmailの場合と同様、Appパスワードは作成時に一度しか表示されません。そのため、他のユーザー用に、パスワードはすぐに入力するか、別の場所へコピーしておく必要があります。

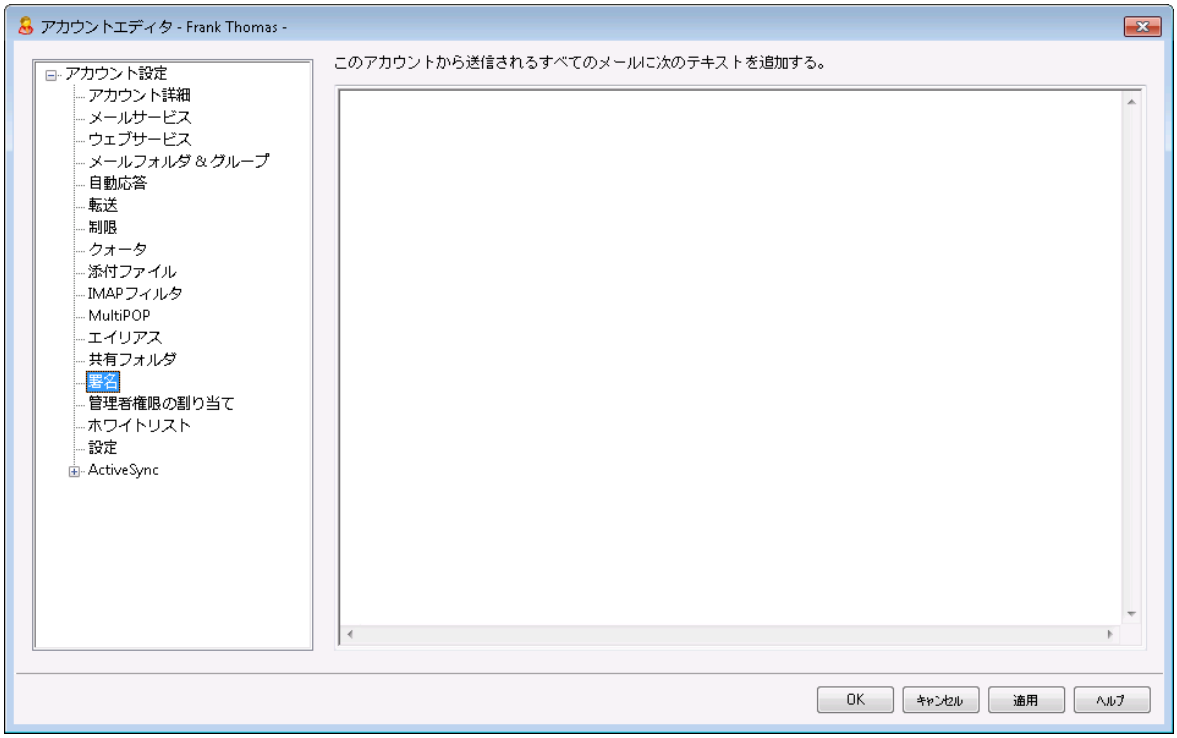
アカウントエディタの設定[693]ページへ「*SMTP, IMAP, ActiveSync等へのログインにAppパスワードを必須とする*」ためのオプションがあります。

Appパスワードを必須にする事で、アカウントのパスワードを、SMTPやIMAP等での辞書攻撃やブルートフォース攻撃から保護する事ができます。Appパスワードは、例えばパスワードが漏えいしてしまった場合でも、本来のパスワードではなく、MDaemonは正しいAppパスワードのみを受け付けるため、パスワードを取得した攻撃者はこれが本来のパスワードでない事を確認できません。更に、MDaemonアカウントがActive Directory[747]認証を使用しており、Active Directoryがパスワードの連続失敗によりアカウントをロックしたとしても、このオプションを使う事でMDaemonからロックされる事がなくなります。MDaemonはAppパスワードのみで認証を行い、ActiveDirectoryへの問合せを行う事がないためです。

参照:

パスワード[778]
アカウントエディタ ≫ 設定[693]

5.1.1.15 署名



署名

アカウントから送信する全メールの一番下に追加される署名を、この画面で設定できます。この署名は、例えばWebmailや他のメーラーの署名追加オプション、署名/フッタ[120]オプション、メーリングリストフッタ[271]といった、他の署名やフッタの後に挿入されます。デフォルト[120]/ドメイン[184]署名やメーリングリスト用フッター[271]は、アカウント署名の後に追加されます。

WebmailやRemote Administration[321]へアクセスできるユーザーは、そこからでも署名の編集が行えます。

署名マクロ

MDaemonの署名機能はマクロに対応しており、送信者の連絡先情報や、パブリック連絡先に登録してある送信者連絡先情報を、署名へ追加する事ができます。これにより、デフォルトやドメイン毎の署名も、送信者情報を個別に指定できるようになります。 例えば、 $CONTACTFULLNAME$ は送信者の氏名を挿入し、$CONTACTEMAI LADDRESS$ は送信者のメールアドレスを挿入します。パブリック連絡先は、Webmail, MDaemon Connector, ActiveSyncから編集できます。空の値は送信者の連絡先情報が存在しない場合に使用されます。利用できるマクロは次の通りです。

ユーザーはMDaemon署名を、 $SYSTEMSIGNATURE$ マクロでデフォルト/ドメイン署名へ、$ACCOUNTSIGNATURE$ マクロでアカウント署名へ変換できます。

Signature Selector	
$SYSTEMSIGNATURE$	デフォルト署名[120]またはドメイン署名をメッセージに配置する。両方が存在する場合は、ドメイン署名[184]が使用される。

$CLIENTSIGNATURE$	メッセージにデフォルトクライアント署名[125]またはドメインクライアント署名[188]を入れる。両方が存在する場合は、ドメインクライアント署名を使用する。
$ACCOUNTSIGNATURE$	アカウント署名[686]をメッセージに配置する。
名前とID	
Full name	**$CONTACTFULLNAME$**
First name	**$CONTACTFIRSTNAME$**
Middle name	**$CONTACTMIDDLENAME$,**
Last name	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
Suffix	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Yomi First Name	**$CONTACTYOMIFIRSTNAME$**
Yomi Last Name	**$CONTACTYOMILASTNAME$**
Account name	**$CONTACTACCOUNTNAME$**
Customer ID	**$CONTACTCUSTOMERID$**
Government ID	**$CONTACTGOVERNMENTID$**
File as	**$CONTACTFILEAS$**
メールアドレス	
Email address	**$CONTACTEMAILADDRESS$**
Email address 2	**$CONTACTEMAILADDRESS2$**
Email address 3	**$CONTACTEMAILADDRESS3$**
電話とFAX番号	
Mobile phone	**$CONTACTHOMEMOBILE$**
Mobile phone 2	**$CONTACTMOBILE2$**
Car phone	**$CONTACTCARPHONENUMBER$**
Home phone	**$CONTACTHOMEPHONE$**
Home phone 2	**$CONTACTHOMEPHONE2$**
Home fax	**$CONTACTHOMEFAX$**
Other phone	**$CONTACTOTHERPHONE$**
インスタントメッセージとウェブ	

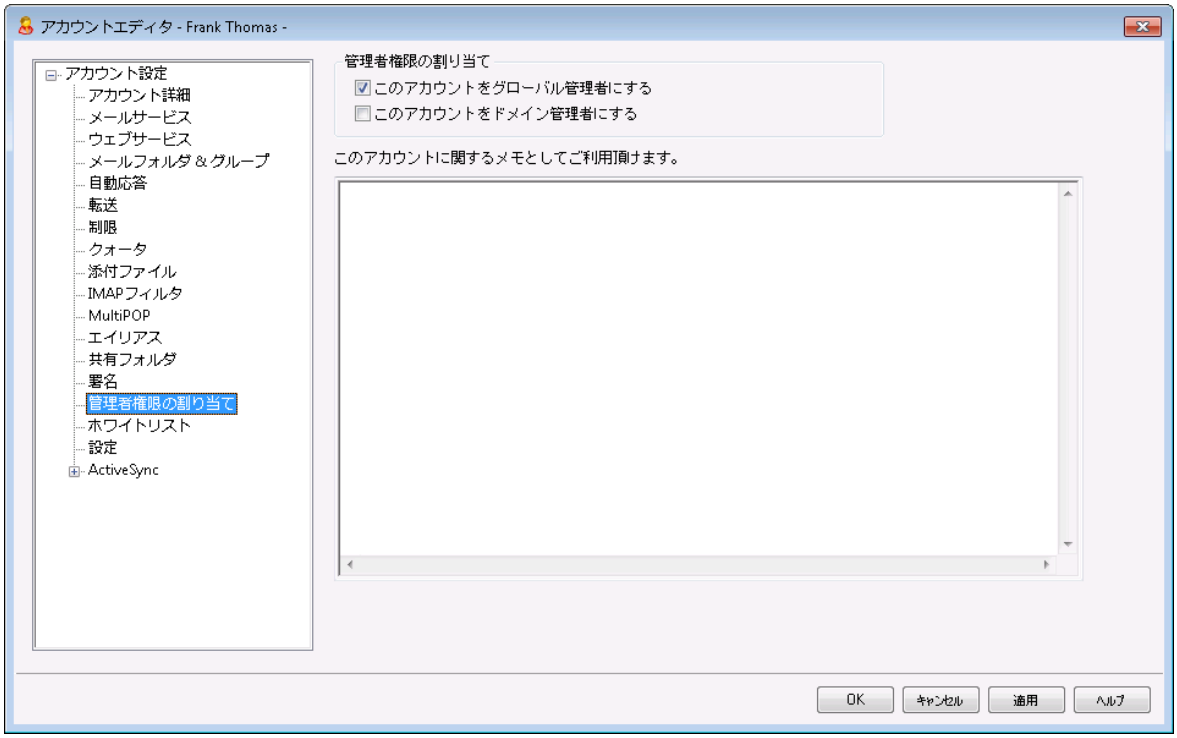
IM Address	**$CONTACTIMADDRESS$**
IM Address 2	**$CONTACTIMADDRESS2$**
IM Address 3	**$CONTACTIMADDRESS3$**
MMS Address	**$CONTACTMMSADDRESS$**
Home web address	**$CONTACTHOMEWEBADDRESS$**
住所	
Home address	**$CONTACTHOMEADDRESS$**
Home city	**$CONTACTHOMECITY$**
Home state	**$CONTACTHOMESTATE$**
Home zip code	**$CONTACTHOMEZIPCODE$**
Home country	**$CONTACTHOMECOUNTRY$**
Other address	**$CONTACTOTHERADDRESS$**
Other city	**$CONTACTOTHERCITY$**
Other state	**$CONTACTOTHERSTATE$**
Other zip code	**$CONTACTOTHERZIPCODE$**
Other country	**$CONTACTOTHERCOUNTRY$**
仕事関連	
Business Name	**$CONTACTBUSINESSCOMPANY$**
Yomi Business Name	**$CONTACTYOMICOMPANYNAME$**
Business title	**$CONTACTBUSINESSTITLE$**
Business office	**$CONTACTBUSINESSOFFICE$**
Business department	**$CONTACTBUSINESSDEPARTMENT$**
Business manager	**$CONTACTBUSINESSMANAGER$**
Business assistant	**$CONTACTBUSINESSASSISTANT$**
Business assistant phone	**$CONTACTBUSINESSASSISTANTPHONE$**
Business main phone	**$CONTACTBUSINESSMAINPHONE$**
Business phone	**$CONTACTBUSINESSPHONE$**
Business phone 2	**$CONTACTBUSINESSPHONE2$**
Business IP phone	**$CONTACTBUSINESSIPPHONE$**
Business fax	**$CONTACTBUSINESSFAX$**

Business pager	**$CONTACTBUSINESSPAGER$**
Business radio	**$CONTACTBUSINESSRADIO$**
Business address	**$CONTACTBUSINESSADDRESS$**
Business city	**$CONTACTBUSINESSCITY$**
Business state	**$CONTACTBUSINESSSTATE$**
Business zip code	**$CONTACTBUSINESSZIPCODE$**
Business country	**$CONTACTBUSINESSCOUNTRY$**
Business web address	**$CONTACTBUSINESSWEBADDRESS$**
その他	
Spouse	**$CONTACTSPOUSE$**
Children	**$CONTACTCHILDREN$**
Categories	**$CONTACTCATEGORIES$**
Comment	**$CONTACTCOMMENT$**

参照:

デフォルト署名 120
ドメイン署名 184
メーリングリストのフッタ 271

5.1.1.16 管理者権限の割り当て



管理者権限の割り当て

アカウントは全体管理者です
ユーザーにサーバーレベルの管理権限を与えるにはこのオプションを有効にします。全体管理者に与えられる権限には次のものがあります:

- サーバー設定、全ユーザーへ、Remote Administration経由でのフルアクセス権限
- MDaemonドメイン全ての全ユーザーを、インスタントメッセージの連絡先として追加する権限
- 読み取り専用のフラグが付いている場合も含め、全てのメーリングリストへ投稿する権限
- メンバーでないものも含め、全てのメーリングリストに対する投稿権限

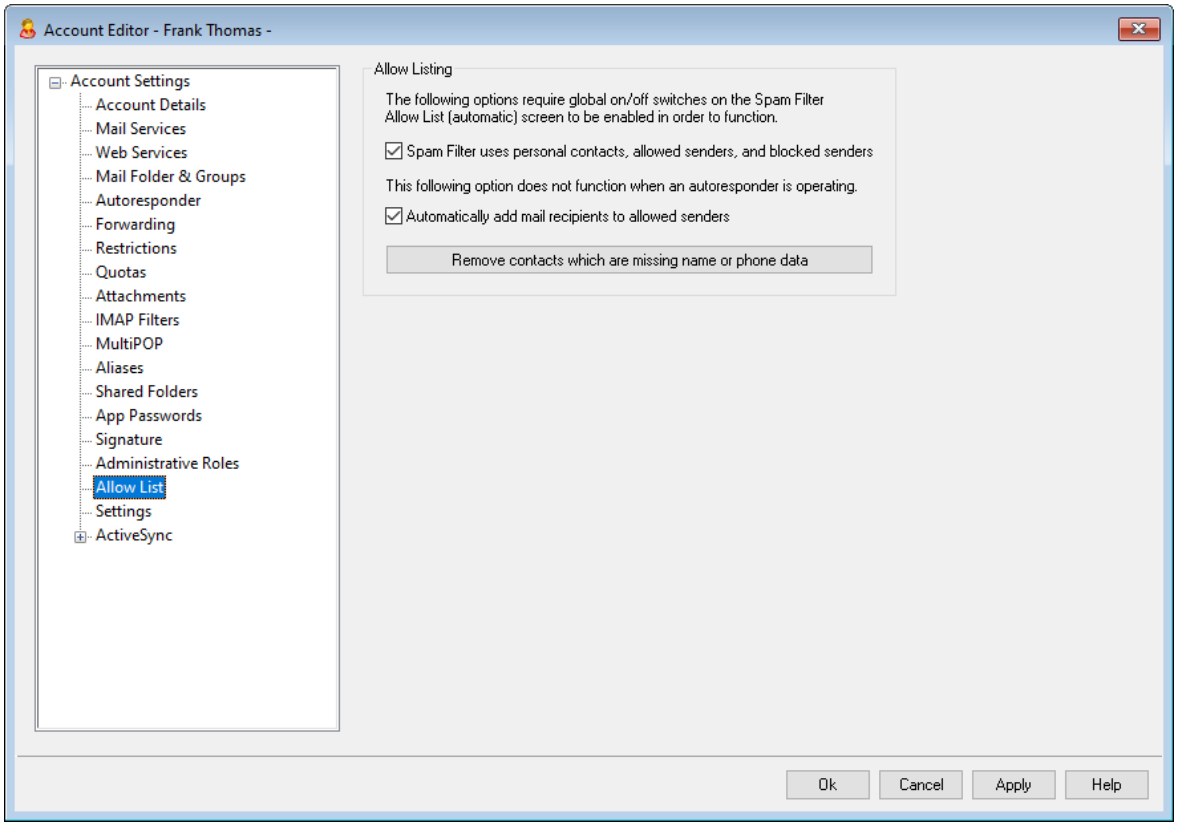
ユーザーはMDaemonのファイルやオプション全てに対して全アクセス権を持つことになります。Remote Administrationでの管理者権限に関する詳細は、Remote Administration 321を参照してください。

アカウントはドメイン管理者です
ユーザーをドメイン管理者として指定するにはこのチェックボックスをクリックします。ドメイン管理者は全体管理者と似ていますが、管理権限が所属ドメインであり、ウェブサービス 656ページでの権限に限定されている点が異なります。

このアカウントで異なるドメインも管理できるようにするには、Remote Administration 321 ウェブ画面の、ドメインマネージャ ≫ 管理者ページから設定が行えます。

このアカウント のメモ
この画 面 ではアカウント に関 する非 公 開 のメもや情 報 を記 載 します。アカウント 詳 細 650 の説 明 と異 なり、管 理 者 メモは他 の公 開 連 絡 先 情 報 と同 期 したり、Active Directory のフィールド と関 連 付 けられる事 はありません。

5.1.1.17 許可リスト



許 可 リスト

スパムフィルタは個 人 の連 絡 先 、許 可 リスト 、ブロックリスト を使 用
スパムフィルタの 許 可 リスト（自 動） 627 画 面 ではスパムフィルタでメール送 信 者 がローカルの宛 先 ユーザーの個 人 連 絡 先 や許 可 リスト フォルダに含 まれていた場 合 に、メールを自 動 で許 可 リスト へ追 加 するための全 体 設 定 オプションを使 用 する事 ができます。また、ここでは送 信 者 が宛 先 ユーザーのブロックリスト へ含 まれていた場 合 に、これを自 動 でブロックリスト として登 録 する事 もできます。スパムフィルタの全 体 オプションを有 効 にしていて、アカウント へこれらの設 定 を適 用 したくない場 合 は、このチェックボックスを無 効 にしてください。全 体 設 定 は無 効 化 され、このオプションは利 用 できなくなります。

メールの宛 先 を許 可 リスト へ自 動 追 加 する
ローカルではないアドレスへメール送 信 を行 う度 にアカウント の許 可 リスト フォルダを更 新 するにはこのオプションを選 択 します。上 記 の、*スパムフィルタで個 人 連 絡 先* 、*許 可 リスト* 、*ブロックリスト を使 用* のオプションと併 用 する事 により、スパムフィルタの誤 検 知 は劇 的 に減 少 します。許 可 リスト（自 動） 627

にある、許可リスト連絡先を自動で更新するオプションを、この機能を利用する前に有効化しておく必要があります。

このオプションは、アカウントで自動応答を使用していると無効になります。

名前または電話データのない連絡先を削除する
アカウントのデフォルト連絡先フォルダからメールアドレスのみの連絡先情報を全て削除する場合はこのボタンをクリックします。連絡先情報として最低限名前か電話番号を入力していないデータは削除されます。このオプションはMDaemon 11以前の自動許可リスト追加オプションを使っていたユーザーが、連絡先を整理できるよう搭載したオプションです。MDaemonの以前のバージョンでは、アドレスは許可リストではなくメイン連絡先へ追加されていました。これは結果として連絡先フォルダに不必要なデータを大量に保持する事になります。

メールアドレスのみの連絡先であっても正規なものである場合がある事から、このオプションの利用は慎重に行って下さい。

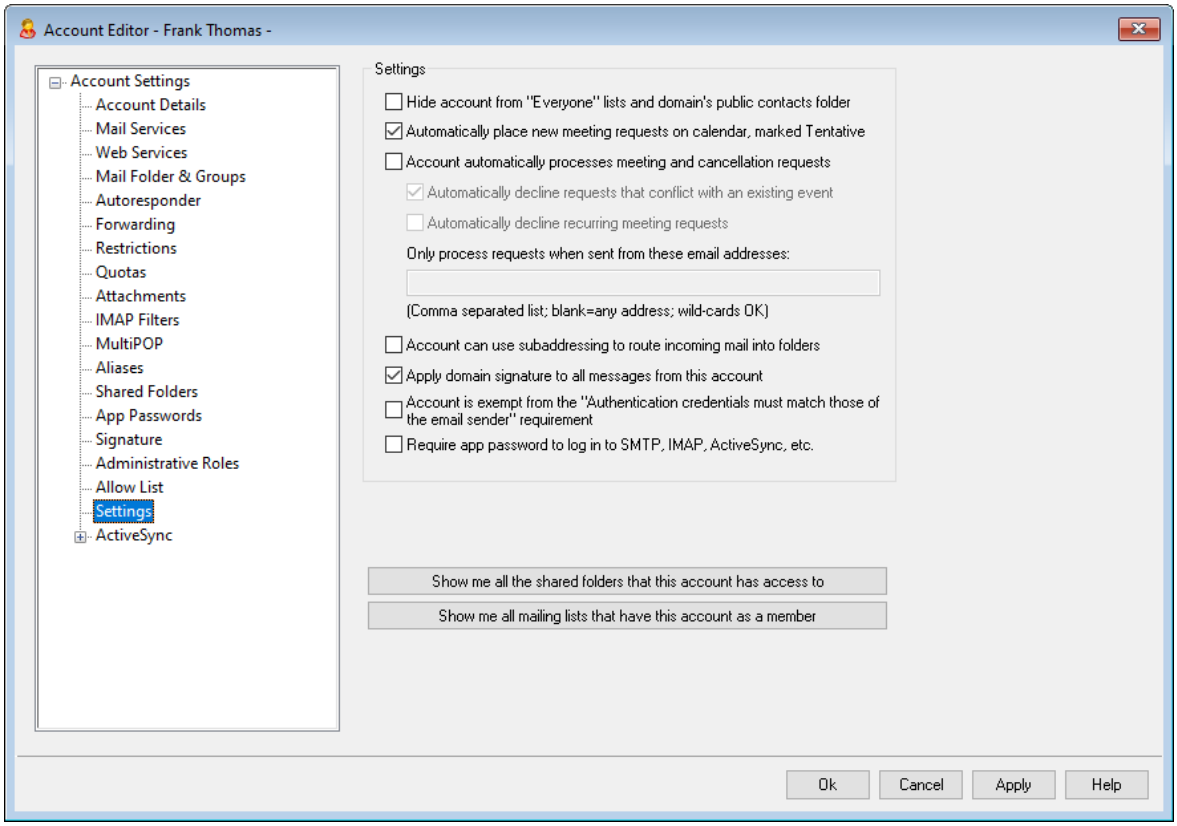
新しいアカウントとグループ用デフォルトの設定

この画面のオプションは新規アカウント[722]や特定のグループ[712]のデフォルト値として使用され、テンプレートプロパティ ≫ 許可リスト[743]へ連動しています。

参照:

許可リスト（自動）[627]
テンプレートマネージャ[721]
テンプレートプロパティ ≫ 許可リスト[743]

5.1.1.18 設定



設定

"Everyone"メーリングリストとドメインのパブリック連絡先からアカウントを隠す
MDaemonは、ドメインの全ユーザー及び全ドメインの全ユーザー用に、"Everyone@"と"MasterEveryone@"メーリングリスト[248]を自動で作成、管理します。デフォルトで、MDaemonは、このメーリングリストへ全アカウントを登録しますが、特定のアカウントをこのメーリングリストメンバーから外す場合、このチェックボックスをクリックすると、アカウントはメーリングリストへ含まれず、このリストへ送られたメールも外したアカウントに対しては配信されません。アカウントは、ドメインのパブリック連絡先でも非表示となります。

自動的に新しい会議招集を予定表に追加し、暫定予定としてマークする
デフォルトでアカウントが新しい会議招集を受け取ると、会議の予定がユーザーの予定表へ、暫定予定としてマークされた状態で追加されます。

自動的に会議招集とキャンセルの処理を受けつける
ミーティング要求や変更、キャンセル処理を自動的にする場合は、このオプションを選択します。ミーティング要求を受信するとカレンダーが自動的に更新されます。このオプションはデフォルトで、すべてのアカウントでは無効になっています。

既存のイベントと競合するリクエストは自動的に拒否する
会議招集とキャンセル処理を自動処理する設定になっている場合に、既存のイベントと競合する会議の招集があった際、自動で拒否するオプションです。競合するイベントも自動で受け付ける場合はこのオプションを外して下さい。

繰返し予定の要求を拒否する
会議招集とキャンセル処理を自動処理する設定になっている場合で、繰返しイベントの場合にのみ拒否したい場合はこのチェックボックスをクリックします。

これらのメールアドレスから送信された要求のみ処理する
特定のアドレスからのリクエストのみを処理する場合は、対象アドレスを指定します。アドレスが複数ある場合はカンマで区切ります。ワイルドカード（例．*@example.com）が使用できます。これをブランクにすると全てのアドレスが許可されます。

受信メールを対応するメールフォルダへ届けるサブアドレス機能の使用を許可する
サブアドレス[694]の利用を許可する場合はこのオプションをクリックして下さい。

このアカウントからのメールへドメイン署名を付与する
アカウントが所属するドメインのドメイン署名[184]が設定されていると、このオプションでユーザーからの全てのメールへ追加されます。これはデフォルトで有効です。

アカウントを「認証情報とSender情報との一致を求める」設定から除外します
SMTP認証[476]の「認証情報はメール送信者と一致」オプションからアカウントを除外するにはこのオプションを使用します。 このオプションはデフォルトで無効になっています。

SMTP, IMAP, ActiveSync等へのログインにAppパスワードを必須とする
このテンプレートを使用しているアカウントがSMTP, IMAP, ActiveSync, それ以外のメールサービスへのログインを行うのに、メーラー側でAppパスワード[683]を必須とする場合はこのオプションをクリックします。アカウントの通常のパスワード[778]は、WebmailやRemote Adminへのログインには必要です。

Appパスワードを必須にする事で、アカウントのパスワードを、SMTPやIMAP等での辞書攻撃やブルートフォース攻撃から保護する事ができます。Appパスワードは、例えばパスワードが漏えいしてしまった場合でも、本来のパスワードではなく、MDaemonは正しいAppパスワードのみを受け付けるため、パスワードを取得した攻撃者はこれが本来のパスワードでない事を確認できません。 更に、MDaemonアカウントがActive Directory[747]認証を使用しており、Active Directoryがパスワードの連続失敗によりアカウントをロックしたとしても、このオプションを使う事でMDaemonからロックされる事がなくなります。MDaemonはAppパスワードのみで認証を行い、ActiveDirectoryへの問合せを行う事がないためです。

このアカウントがアクセスできる全ての共有フォルダを表示
このアカウントがアクセス権を持つ共有フォルダの一覧を表示するには、このボタンをクリックします。

このアカウントがメンバーであるメーリングリストを表示
このアカウントがメンバーとなっているメーリングリスト[245]の一覧を表示するには、このボタンをクリックします。

サブアドレス

サブアドレスとは、アカウントのメールアドレスの、メールボックス名の中にフォルダ名を含むシステムです。このシステムを使用すると、特別なフィルタリングを使うことなく、mailbox+folder名の組み合わせで届いたメールは、アドレスに含まれるアカウントの持つフォルダ（そのフォルダが実際に存在するとし）に自動的に割り振られます。

例えば、bill.farmer@example.com が"stuff"と呼ばれるIMAPメールフォルダを持つ場合、"bill.farmer+stuff@example.com"にアドレス指定され到着しているメールは、そのフォル

ダに自動的に割り振られます。サブフォルダは追加された"+"文字で区切られるフォルダおよびサブフォルダ名を持つことで指定することができ、アンダーラインはフォルダ名でスペースを置き換えるために使用されます。したがって、上記のサンプルを利用して、billの"stuff"フォルダが"my older stuff"と呼ばれれるサブフォルダを持つ場合、"bill.farmer+stuff+my_older_stuff@example.com"にアドレス指定されるメッセージはbillの"¥stuff¥my older stuff¥"メールフォルダに自動的に割り振られます。

サブアドレスが"+"文字の使用を必要とするので、"+"を含むメールボックスはサブアドレス指定することができません。よって、上記のサンプルで実アドレスが bill.farmer@example.comの代わりに bill+farmer@example.comである場合、サブアドレス指定することができません。さらに、サブアドレスでアドレスエイリアスを使用することができません。しかしながら、全体のアドレスエイリアスされた形式を参照するエイリアスを作成することができます。したがって、"alias+stuff@example.com"が許可されない場合でも、"bill.farmer+stuff@example.com"に指し示すために"alias@example.com"の使用は問題ありません。

セキュリティ上の弱点または不正使用を防止するために、サブアドレスに含まれるIMAPフォルダは当な手続をとる必要があります。サブアドレス指定されたメッセージが、サブアドレスで定義されるフォルダの名前に一致するフォルダがないアカウントに到着する場合、サブアドレスは不明なメールアドレスとして処理されて、他のMDaemon設定に基づく処理をされます。例えば bill.farmer@example.comが"stuff"という名前のフォルダを持たず、メッセージが"bill.farmer+stuff@example.com"宛に到着する場合、不明なユーザにアドレス指定されたようにメッセージを処理します。

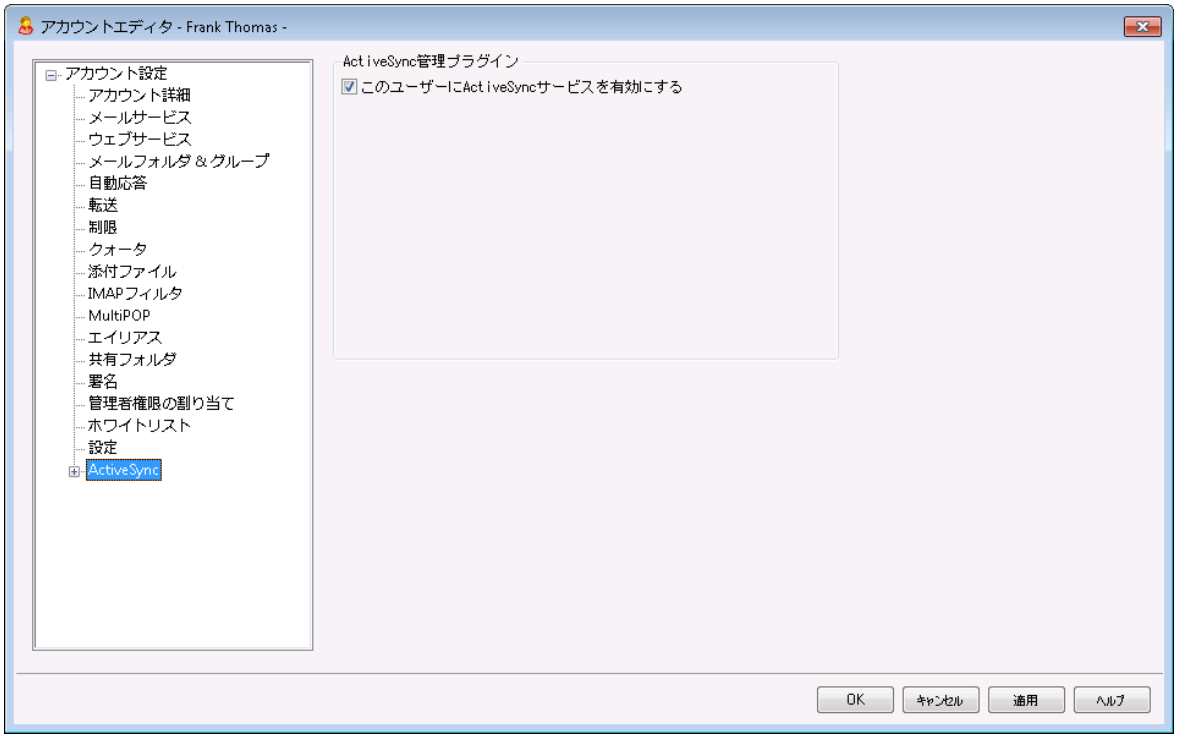
サブアドレスを有効にする
アカウントにサブアドレスの利用を許可する場合はこのチェックボックスをクリックします。

デフォルトで、アカウントごとのサブアドレス機能は無効になっています。しかし、この機能は、初期設定 459の[**その他**]画面から、[**すべてのアカウントのサブアドレス機能を無効にする**]を選択することで無効にすることができます。オプションからサブアドレス機能を無効にした場合、個別のサブアドレスが設定してある場合でも、サブアドレスは有効になりません。

参照:

許可リスト（自動） 627
Remote Administration 321
テンプレートマネージャ 721
パスワード 778

5.1.1.19 ActiveSync for MDaemon



アカウント エディタのActiveSync for MDaemonではActiveSyncの有効化や無効化、アカウント別設定 697、デフォルト ポリシーの適用 702 ユーザー毎のActiveSyncクライアント 703の管理が行えます。

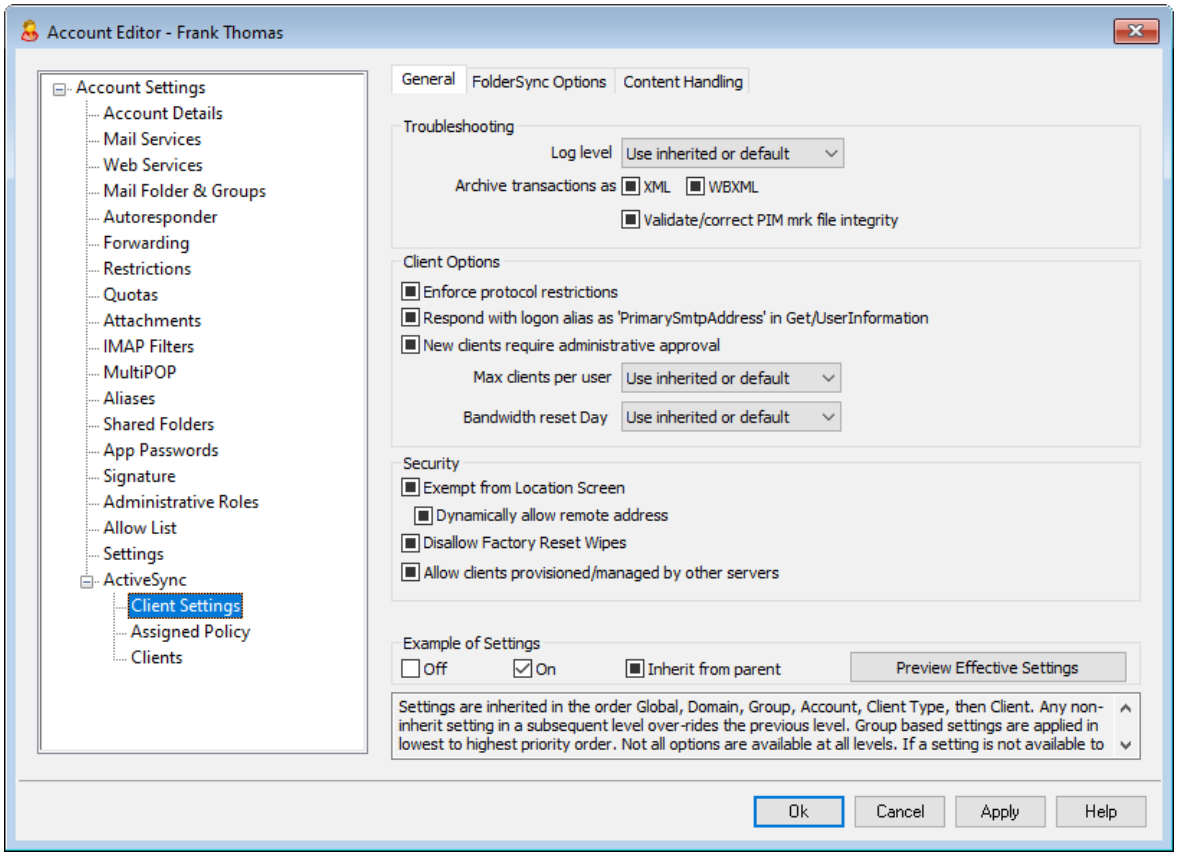
このユーザーにActiveSyncサービスを有効にする

アカウントがActiveSyncクライアントでメールやPIMデータへアクセスできるようにするには、このオプションを有効にします。

参照:

アカウントエディタ ≫ ActiveSync ≫ クライアント設定 697
アカウントエディタ ≫ ActiveSync ≫ 割り当て済ポリシー 702
アカウントエディタ ≫ ActiveSync ≫ クライアント設定 703

5.1.1.19.1 クライアント設定



ここではアカウントに関連付けられたActiveSync クライアント設定が行えます。デフォルトで各オプションは所属するドメインの設定値を引き継ぎます。ここでの設定はドメイン設定 397を上書きします。また、クライアント 703の設定オプションを使うと、特定のクライアントにおいては、アカウントレベルでの設定値を上書きします。

全般

トラブルシューティング

ログレベル

ActiveSync for MDaemonはログデータ量に応じた、6つのレベルのログに対応しています。

デバッグ 最も詳細なログで、記録できる全ての情報が含まれており、問題の診断にのみ使用されます。

情報 通常のログで、一般的な操作が詳細なしで記録されます。これはデフォルトのログレベルです。

警告 警告、エラー、クリティカルエラー、起動と終了がログに記録されます。

エラー エラー、クリティカルエラー、起動と終了がログに記録されます。

クリティカル　クリティカルエラー、起動と終了がログに記録されます。

なし　起動と終了だけがログに記録されます。

継承　デフォルトで、ログレベルの設定はクライアント設定の階層から継承されます。そのため、クライアントは設定をクライアントタイプから引継ぎ、クライアントタイプはアカウントから引継ぎ、アカウントはグループから引継ぎます。全体のクライアント設定は 診断 393 ダイアログのログレベル設定を元にしています。

トランスアクションを [XML | WBXML]としてアーカイブ
XMLやWBXMLデータをアーカイブするには、*XMLと WBXMLをアーカイブ...* のオプションを使用します。これはデバッグの際役立ちます。全体オプションはデフォルトで無効になっています。

PIM mrkファイルの整合性を確認する
クライアントのPIMデータの整合性テストを実施し、iCal UIDの重複や空の要求フィールドといった、同期を妨げているものがないかどうかを確認します。この全体設定はデフォルトで無効になっています。

クライアントオプション

プロトコル制限を強制する
クライアントで許可されているプロトコルバージョン以外のアクセスを拒否する場合はこのオプションを有効にします。デフォルトでこのオプションは無効になっており、プロトコル制限は異なるプロトコルのクライアントを拒否していません。プロトコル制限は単純に、クライアントに対して使用するべきプロトコルを伝えるのみの機能を提供しています。クライアントがそれでも制限されているプロトコルを使った場合、MDaemonはその接続を受け入れます。詳細は次のページをご覧下さい: プロトコル制限 395

Get/UserInformationへの応答でログオンエイリアスを'PrimarySmtpAddress' として使用する
サービスがSettings/Get/UserInformationリクエストに対する応答としてエイリアスやセカンダリアドレスをプライマリアドレスとして利用できるようにします。これはiOS 9.xへアップデートした際エイリアスからメールを送信できなくなった事に対する対処です。このオプションによって使用に反した応答を受け取る場合があります。

新しいクライアントは管理者の承認が必要
新しいクライアントがアカウントとの同期を開始する前に、管理者による承認を必要とする場合はこのオプションを有効にします。 クライアント 422 一覧で認証待ちのクライアントが確認でき、管理者は同じ画面から承認が行えます。この設定はデフォルトで無効になっています。

ユーザー毎の最大クライアント
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域リセット日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスク

と同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

セキュリティ

ロケーションスクリーンから除外する
ActiveSyncクライアント設定で端末をロケーションスクリーニング[520]から除外する場合はこのオプションを有効化します。これにより認証済ユーザーは、例えば認証がブロックされている場所へ出張しているような場合であっても、ActiveSync経由でアカウントへアクセスする事ができるようになります。端末を除外するためには、チューニング画面にあるこの日数を超えて認証されなかった端末を自動削除[381]設定の時間内に、ActiveSyncを使った接続と認証を行っておく必要があります。

リモートアドレスを動的に除外
接続元のリモートIPアドレスをロケーションスクリーニングの除外リストへ追加する事ができます。このオプションは、同じIPアドレスを使って接続する他のクライアントがある場合に便利です。

ユーザー毎の最大クライアント数
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域の統計情報をリセットする日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

他のサーバーで管理されているクライアントへの接続を許可する
デフォルトで、ActiveSyncサーバーが特定のクライアントへデータやポリシーを送信する際、対象クライアントが他のActiveSyncサーバーからも管理されている事が分かった場合も、クライアントはMDaemonへアクセスする事ができます。しかし、このような環境の場合、適用するポリシーが他のActiveSyncサーバーと競合する可能性があります。一般的に、クライアントはポリシーが競合した場合、厳しい方へ合わせる傾向があります。こうしたクライアントからの接続を制限する場合は、このオプションを無効化して下さい。

工場出荷時への完全ワイプを無効化
オン/はい、を設定すると、ActiveSyncクライアントの完全ワイプが行えなくなります。クライアントでリモートからの完全ワイプを許可する場合、最初にこのオプションを無効化して下さい。このオプションはデフォルトで無効に設定されています。クライアントページの次の項目を参照して下さい:
ActiveSyncクライアントの完全ワイプ[422]

フォルダ同期オプション

フォルダ同期オプション

除外

ユーザの [許可リスト/ブロックリスト] フォルダ
デフォルトでユーザーの許可リストとブロックリストの連絡先フォルダは端末と同期を行いません。これらはMDaemonがスパムからシステムを自動的に保護するのを支援する目的で使用されます。そのため、許可リストやブロックリストは端末上に連絡先として表示する必要性はありません。

デフォルト以外のメールフォルダ
デフォルトで、ユーザーが作成したメールフォルダとデフォルトメールフォルダは全て端末と同期します。同期するのを受信箱や送信箱、削除済アイテム、下書き、といった、デフォルトのメールフォルダのみにしたい場合はこのオプションを有効にして下さい。ユーザーが作成したフォルダは同期対象に含まれません。 このオプションはデフォルトで無効になっています。

デフォルト以外のPIMフォルダ
デフォルトで、(連絡先、予定表、仕事などの) PIMフォルダは全て端末と同期します。同期するのをデフォルトのPIMフォルダのみにしたい場合はこのオプションを有効にして下さい。このオプションが有効な場合で、ユーザーが複数の予定表を保有してる場合デフォルトの予定表のみが同期対象となります。 このオプションはデフォルトで無効になっています。

含む

パブリックフォルダの階層
ユーザーがアクセス権を持っている パブリックフォルダ[283] をユーザーのActiveSync用端末のフォルダー覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
パブリックフォルダ[283] をユーザーが検索できるようになります。 これはデフォルトで許可されています。

パブリックフォルダの横断 (フォルダ名の公開)
デフォルトで、クライアントがパブリックのサブフォルダへのアクセスや同期を行うには、サブフォルダと上位のパブリックフォルダ[283]全てに対してルックアップ権限[285]が必要です。上位のフォルダに対するアクセス権がない場合、その中のサブフォルダに対しては、例え設定上は許可されていても、アクセスする事はできません。クライアントからこうしたサブフォルダへアクセスできるようにする場合は、このオプションを有効にします。注意点: このオプションを有効化すると、上位のフォルダもクライアントへ許可する事となり、セキュリティのリスクを招く恐れがあります。 このオプションはデフォルトで無効になっています。

許可するパブリックフォルダの最大数
端末で処理するパブリックフォルダ数を制限する場合はこのオプションを使用します。制限が設定されると、サーバーは最大数に到達するまでフォルダー覧を処理し、これを超えるとその後のデータを送りません。処理するフォルダの順番を決める事はできません。デフォルトで、全体での最大数は設定されていません。

共有フォルダも含める

ユーザーがアクセス権を持っている 共有フォルダ[107] をユーザーのActiveSync用端末のフォルダー一覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
共有フォルダ[676] をユーザーが検索できるようになります。これはデフォルトで許可されています。

コンテンツ処理

コンテンツ処理オプション

クライアントにフラグ付けされたメール用にタスク・リマインダーを作成
このオプションでMDaemonはフラグが付いたアイテムごとに仕事を作成し、リマインダーをユーザーへ送信できるようになります。この設定の全体値はデフォルトで有効です。

予定を編集した際、常にミーティングのアップデートを送信
クライアントの中には、ミーティングを編集した際、更新情報を適切に送信しないものもあります。このオプションを使うとActiveSyncサービスへ、ミーティングが開催者によって更新された際、更新情報を送信するよう促す事ができるようになります。これはミーティングの更新情報の送信に失敗しているクライアント[422]やクライアントタイプ[438]に限定して使用するべきで、更新情報が重複して送られてしまう可能性があります。また、このオプションはクライアントとクライアントタイプの設定ページでのみ利用できます。

全ての送信メールで開封確認を要求
クライアントから送信される全てのメールで開封確認要求を行うにはこのオプションを有効にして下さい。これはデフォルトで無効になっています。

送信者からリクエストされた際送信済メールについて開封確認を送信
サーバー側で開封確認要求を検出し、既読フラグがついたメールの開封通知を送信するにはこのオプションを使用します。これはデフォルトで無効になっています。

ReplyToアドレスに指定したエイリアスとして送る
クライアントによっては、エイリアスを使ったメール送信を許可していません。この機能は Exchange ActiveSync（EAS）プロトコル[395] 16.xで追加されたものですが、クライアントの中には16.xに対応していないものもあります。例えば、Windows用OutlookはEAS 14.0だけを使用しており、ユーザーが関連するアドレスを指定して送信する事のみ許可しており、生成されたメールはユーザーの選択を正しく反映していません。このオプションでは、ReplyToのアドレスがユーザー用の正しいエイリアス[757]であれば、これを使ってメール送信を行います。この設定の全体値はデフォルトで有効です。

デフォルトの連絡先にパブリック連絡先を仮想的に統合する
パブリック連絡先をユーザーの端末上でデフォルトの連絡先と統合したい場合はこのオプションを有効にします。これは仮想的な統合で、実際には連絡先フォルダへデータのコピーは行っていません。これはグローバルアドレス帳（GAL）の検索機能に対応していないクライアントにとって便利な機能です。これはデフォルトで無効になっています。

Junk-Emailフォルダへ移動したメールの送信者をブロックする
有効にすると、クライアントが特定のメールを自分のJunk Emailフォルダへ移動した際、対象のメール送信者がブロックされた送信者連絡先フォルダへ追加されます。

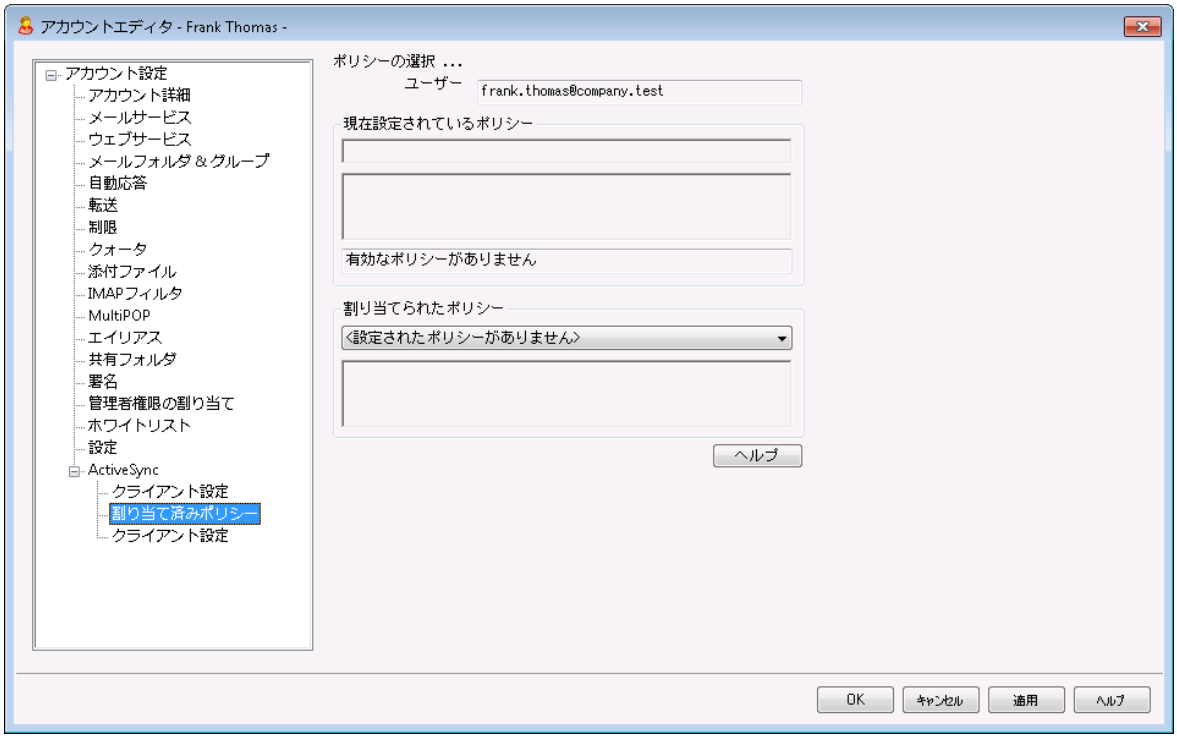
ミーティング要求が許可/拒否された際、ミーティング要求に対する応答の送信を強制的に行う
このオプションを使用すると、クライアントがミーティング要求に対して、許可や拒否、その他のアクションを選択した際、ミーティング要求に対する応答を開催者へ送信します。これは、こうした更新情報を自動送信する事ができない特定のクライアント用の機能です。

有効な設定をプレビュー
このボタンは全てのクライアント設定（ドメイン397, アカウント413, クライアント422）に対して使用できます。画面のオプションはデフォルト値をその上位の画面から引き継いでいるため、この機能は表示されている画面の現在の設定確認を行う際にもご利用頂けます。

参照:

ActiveSync ≫ ドメイン397
アカウントエディタ ≫ ActiveSync ≫ クライアント設定703

5.1.1.19.2 割り当て済ポリシー



ここではActiveSyncクライアントがアカウントへの接続時に使用する、デフォルトのActiveSyncポリシー405を設定します。デフォルトでポリシー設定はドメインのポリシー210設定を引き継ぎますが、アカウン

ト毎にここで設定を上書きする事ができます。更に、特定の異なるクライアント[703]へ割り当てたポリシーは、このアカウント毎の設定を上書きできます。

ActiveSyncポリシーの割り当て

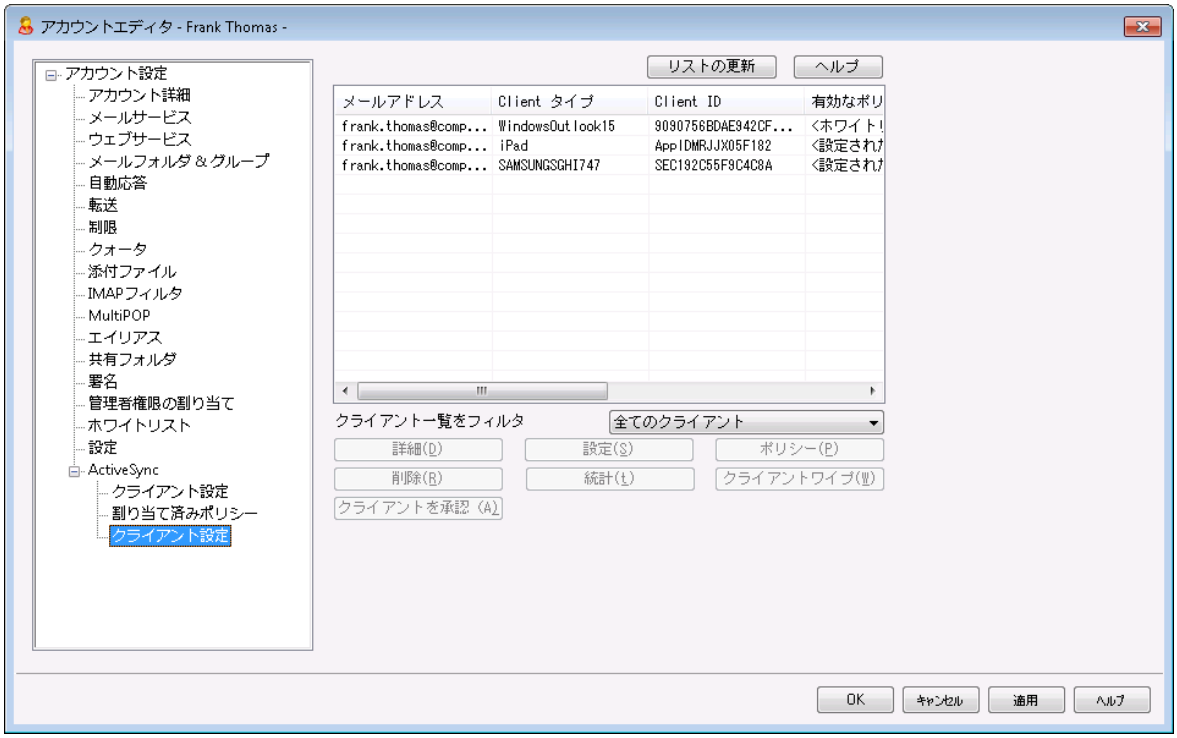
アカウントへポリシーを割り当てるには、**割り当てポリシー**ドロップダウンリストからポリシーを選択し、OKか適用をクリックします。

> 全てのActiveSyncデバイスがポリシーを常に認識したり適用したりできるわけではありません。ポリシー又は同時に適用された特定のポリシーを無視する場合や、変更を適用するのにデバイスの再起動が必要となる場合があります。また、新しいポリシーをデバイスに適用しても、デバイスへ実際にポリシーが適用されるのは次にActiveSyncサーバーへ接続したタイミングとなります。ポリシーはデバイス側から接続するまで、「プッシュ」配信は行われません。

参照:

ActiveSync ≫ ポリシーマネージャ[405]
ActiveSync ≫ ドメイン[397]
アカウントエディタ ≫ ActiveSync ≫ クライアント[703]

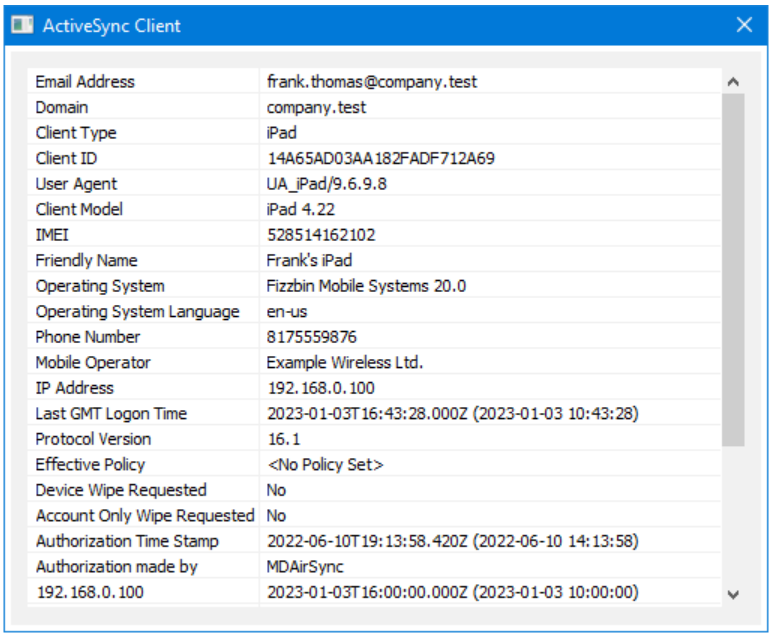
5.1.1.19.3 クライアント



この画面ではユーザーアカウントと関連付けられたActiveSyncクライアントの情報が表示されています。ここから各クライアントに対するActiveSyncポリシー[702]の適用、様々なクライアント設定のコントロー

ル、クライアントの削除、リモートワイプ、MDaemon内のクライアント統計情報の初期化などの処理が行えます。

ActiveSync Client Details



エントリを選択し**詳細**をクリック(またはエントリをダブルクリック)すると、クライアント詳細ダイアログが起動します。この画面では、Clientタイプ、Client ID、最終ログイン時間、といった、クライアントの情報を確認できます。

クライアント設定

クライアントを右クリックし**クライアント設定のカスタマイズ**をクリックするとクライアント設定の管理画面が起動します。デフォルト設定はClientタイプの設定を継承していますが、この値は任意のものへ変更する事ができます。デバイスのクライアント設定の管理を参照してください。

ActiveSyncポリシーの適用

ポリシー405は次のように端末へ適用します:

1. 一覧から端末を右クリックします。.
2. **ポリシーの適用**をクリックすると、ポリシーの割り当てダイアログが起動します。
3. **割り当てポリシー**のドロップダウンリストからポリシーを選択します。
4. **OK**をクリックします。

統計

エントリを右クリックし、**統計を表示**をクリックすると、クライアント統計ダイアログが起動し、クライアント様々な統計情報を確認できます。

統計のリセット

クライアントの統計情報を初期化するには、統計、統計のリセットをクリックし、確認メッセージでOKをクリックします。

ActiveSyncクライアントの削除

ActiveSyncクライアントを削除するには、クライアントを右クリックし 削除 をクリックし、はい、をクリックします。これにより、クライアントとMDaemonに関連した全ての同期情報が削除されます。今後ユーザーが同じActiveSyncクライアントで同期を行った場合、MDaemonは対象クライアントを初めて同期を行うクライアントとして取扱います。全てのデータはMDaemonと再同期されます。

ActiveSyncクライアントの完全初期化

選択したActiveSyncクライアントへ ポリシー 405 が適用されると、クライアントはポリシーを適用し、応答した後に完全初期化を利用できます。ActiveSyncクライアントを完全に初期化するには、クライアントを一覧から選択し完全初期化をクリックします。次回クライアントが接続すると、MDaemonは全てのデータを削除するか、工場出荷時の設定をリストアします。クライアントによっては、ダウンロード済アプリなど、全てのデータを削除してしまう場合があります。また、クライアントのActiveSyncエントリがMDaemonに残っている間は、クライアントがMDaemonへ接続する度に再度初期化が実行されます。クライアントを削除する際には、これをブロックリスト 391 へ追加し、今後の接続を行わないようにします。最後に、初期化済のデバイスを再度接続する場合は、デバイスを右クリックし、ワイプアクションを中止、をクリックします。同時にブロックリストからも削除して下さい。

アカウントのActiveSyncクライアントのワイプ

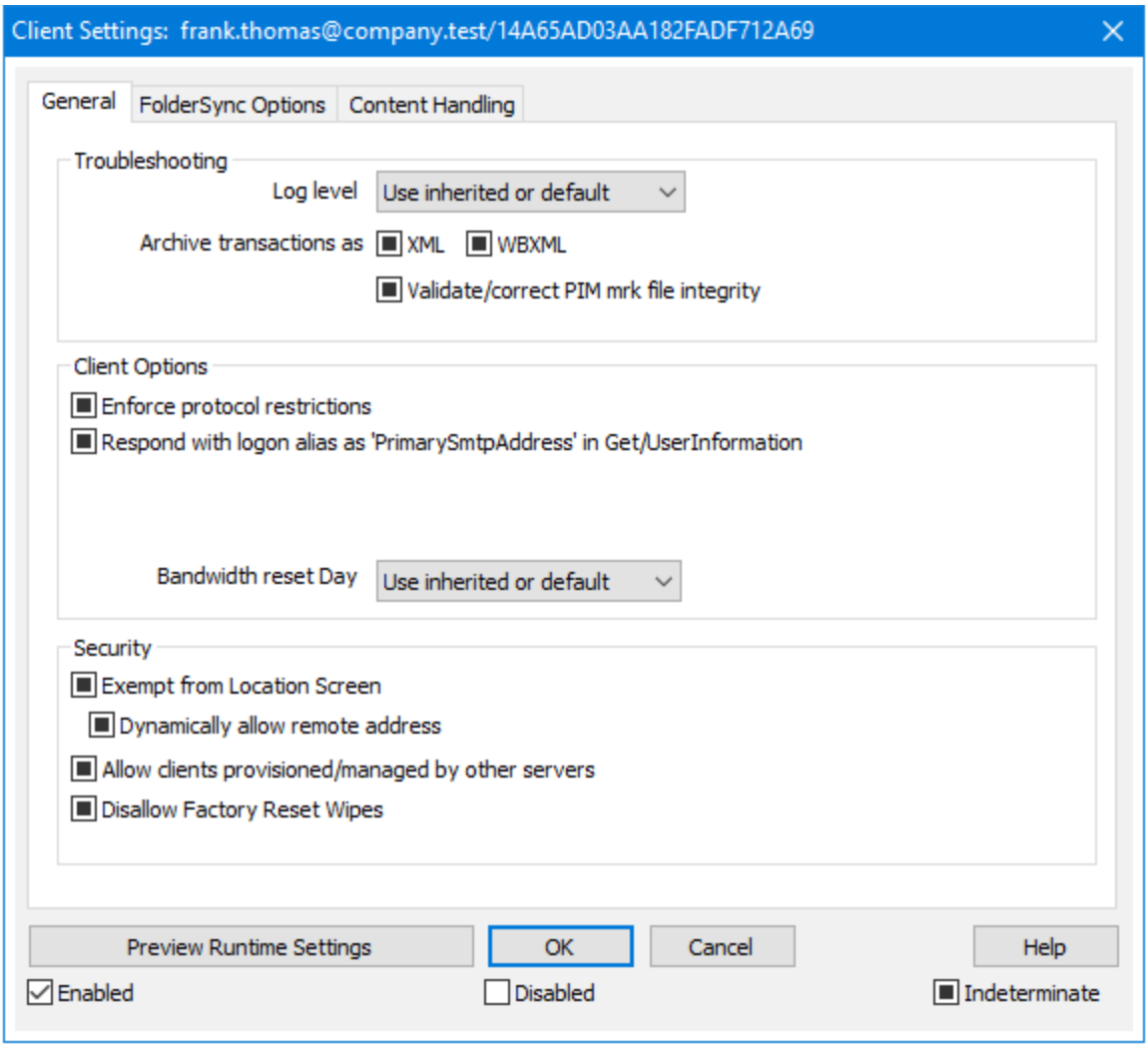
クライアントから、メール、予定表、連絡先といった、アカウントのデータのみを削除する場合は、右クリックし、**クライアントからメールとPIMのアカウントワイプ**をクリックします。 アカウントワイプオプションは完全初期化ににていますが、全てのデータを初期化するのではなく、メールや予定表、連絡先といったアカウント関連データのみを対象にします。その他の、アプリや写真、音楽などは端末上に残ります。

クライアントの承認

ActiveSyncクライアント設定 384 の*"新規クライアントは管理者の承認が必要"*オプションが承認が必要と設定されていた場合、クライアントを選択し クライアントの同期を許可、 をクリックすることでクライアントのサーバーとの同期を承認します。

デバイスのクライアント設定の管理

デバイスレベルのクライアント設定画面では端末毎の設定が管理できます。



デフォルトでこの画面の全てのオプションは「継承又はデフォルト」と設定されており、各オプションがClientタイプクライアント設定 438の関連オプションの設定を継承します。同様に、この画面で行った設定変更はデバイスのクライアントレベル設定を上書きします。

全般

トラブルシューティング

ログレベル

ActiveSync for MDaemonはログデータ量に応じた、6つのレベルのログに対応しています。

デバッグ 最も詳細なログで、記録できる全ての情報が含まれており、問題の診断にのみ使用されます。

情報 通常のログで、一般的な操作が詳細なしで記録されます。これはデフォルトのログレベルです。

警告	警告、エラー、クリティカルエラー、起動と終了がログに記録されます。
エラー	エラー、クリティカルエラー、起動と終了がログに記録されます。
クリティカル	クリティカルエラー、起動と終了がログに記録されます。
なし	起動と終了だけがログに記録されます。
継承	デフォルトで、ログレベルの設定はクライアント設定の階層から継承されます。そのため、クライアントは設定をクライアントタイプから引継ぎ、クライアントタイプはアカウントから引継ぎ、アカウントはグループから引継ぎます。全体のクライアント設定は 診断 393 ダイアログのログレベル設定を元にしています。

トランスアクションを [XML | WBXML]としてアーカイブ
XMLやWBXMLデータをアーカイブするには、*XMLと WBXMLをアーカイブ...* のオプションを使用します。これはデバッグの際役立ちます。全体オプションはデフォルトで無効になっています。

PIM mrkファイルの整合性を確認する
クライアントのPIMデータの整合性テストを実施し、iCal UIDの重複や空の要求フィールドといった、同期を妨げているものがないかどうかを確認します。この全体設定はデフォルトで無効になっています。

クライアントオプション

プロトコル制限を強制する
クライアントで許可されているプロトコルバージョン以外のアクセスを拒否する場合はこのオプションを有効にします。デフォルトでこのオプションは無効になっており、プロトコル制限は異なるプロトコルのクライアントを拒否していません。プロトコル制限は単純に、クライアントに対して使用するべきプロトコルを伝えるのみの機能を提供しています。クライアントがそれでも制限されているプロトコルを使った場合、MDaemonはその接続を受け入れます。詳細は次のページをご覧下さい: プロトコル制限 395

Get/UserInformationへの応答でログオンエイリアスを'PrimarySmtpAddress' として使用する
サービスがSettings/Get/UserInformationリクエストに対する応答としてエイリアスやセカンダリアドレスをプライマリアドレスとして利用できるようにします。これはiOS 9.xへアップデートした際エイリアスからメールを送信できなくなった事に対する対処です。このオプションによって使用に反した応答を受け取る場合があります。

新しいクライアントは管理者の承認が必要
新しいクライアントがアカウントとの同期を開始する前に、管理者による承認を必要とする場合はこのオプションを有効にします。 クライアント 422 一覧で認証待ちのクライアントが確認でき、管理者は同じ画面から承認が行えます。この設定はデフォルトで無効になっています。

ユーザー毎の最大クライアント
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用

できません。

帯域リセット日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

セキュリティ

ロケーションスクリーンから除外する
ActiveSyncクライアント設定で端末をロケーションスクリーニング 520から除外する場合はこのオプションを有効化します。これにより認証済ユーザーは、例えば認証がブロックされている場所へ出張しているような場合であっても、ActiveSync経由でアカウントへアクセスする事ができるようになります。端末を除外するためには、チューニング画面にあるこの日数を超えて認証されなかった端末を自動削除 381設定の時間内に、ActiveSyncを使った接続と認証を行っておく必要があります。

リモートアドレスを動的に除外
接続元のリモートIPアドレスをロケーションスクリーニングの除外リストへ追加する事ができます。このオプションは、同じIPアドレスを使って接続する他のクライアントがある場合に便利です。

ユーザー毎の最大クライアント数
MDaemonアカウント毎に管理できるActiveSyncクライアントの数を制限するには、ここで最大クライアント数を入力します。この全体オプションは、デフォルトで無制限です。このオプションは、全体、ドメイン毎、アカウントのクライアント設定画面で利用できますが、個々のクライアント画面では利用できません。

帯域の統計情報をリセットする日
ActiveSyncの帯域の利用統計を、毎月特定の日にリセットするにはこのオプションを使用します。リセット処理は深夜のメンテナンス処理の一つとして実行され、システムログへ他のメンテナンスタスクと同様に記録されます。全体オプションはデフォルトで「0（リセットしない）」に設定されており、使用統計はリセットされません。例えば、ユーザーやクライアントのキャリアで課金用にデータをリセットする日に合わせてリセットしたい場合には、下位のオプションで任意の設定を行って下さい。

他のサーバーで管理されているクライアントへの接続を許可する
デフォルトで、ActiveSyncサーバーが特定のクライアントへデータやポリシーを送信する際、対象クライアントが他のActiveSyncサーバーからも管理されている事が分かった場合も、クライアントはMDaemonへアクセスする事ができます。しかし、このような環境の場合、適用するポリシーが他のActiveSyncサーバーと競合する可能性があります。一般的に、クライアントはポリシーが競合した場合、厳しい方へ合わせる傾向があります。こうしたクライアントからの接続を制限する場合は、このオプションを無効化して下さい。

工場出荷時への完全ワイプを無効化
オン/はい、を設定すると、ActiveSyncクライアントの完全ワイプが行えなくなります。クライアントでリモートからの完全ワイプを許可する場合、最初にこのオプションを無効化して下さい。このオプションはデフォルトで無効に設定されています。クライアントページの次の項目を参照して下さい:
ActiveSyncクライアントの完全ワイプ 422

フォルダ同期オプション

フォルダ同 期 オプション

除 外

ユーザの [許 可 リスト /ブロックリスト] フォルダ
デフォルト でユーザーの許 可 リスト とブロックリスト の連 絡 先 フォルダは端 末 と同 期 を行 いません。これらはMDaemonがスパムからシステムを自 動 的 に保 護 するのを支 援 する目 的 で使 用 されます。そのため、許 可 リスト やブロックリスト は端 末 上 に連 絡 先 として表 示 する必 要 性 はありません。

デフォルト 以 外 のメールフォルダ
デフォルト で、ユーザーが作 成 したメールフォルダとデフォルト メールフォルダは全 て端 末 と同 期 します。同 期 するのを受 信 箱 や送 信 箱 、削 除 済 アイテム、下 書 き、といった、デフォルト のメールフォルダのみにしたい場 合 はこのオプションを有 効 にして下 さい。ユーザーが作 成 したフォルダは同 期 対 象 に含 まれません。 このオプションはデフォルト で無 効 になっています。

デフォルト 以 外 のPIMフォルダ
デフォルト で、(連 絡 先 、予 定 表 、仕 事 などの) PIMフォルダは全 て端 末 と同 期 します。同 期 するのをデフォルト のPIMフォルダのみにしたい場 合 はこのオプションを有 効 にして下 さい。このオプションが有 効 な場 合 で、ユーザーが複 数 の予 定 表 を保 有 してる場 合 デフォルト の予 定 表 のみが同 期 対 象 となります。 このオプションはデフォルト で無 効 になっています。

含 む

パブリックフォルダの階 層
ユーザーがアクセス権 を持 っている パブリックフォルダ 283 をユーザーのActiveSync用 端 末 のフォルダー 覧 へ含 むにはこのオプションを有 効 にします。これはデフォルト で有 効 です。

検 索 を許 可 する
パブリックフォルダ 283 をユーザーが検 索 できるようになります。 これはデフォルト で許 可 されています。

パブリックフォルダの横 断 (フォルダ名 の公 開)
デフォルト で、クライアント がパブリックのサブフォルダへのアクセスや同 期 を行 うには、サブフォルダと上 位 のパブリックフォルダ 283 全 てに対 してルックアップ権 限 285 が必 要 です。上 位 のフォルダに対 するアクセス権 がない場 合 、その中 のサブフォルダに対 しては、例 え設 定 上 は許 可 されていても、アクセスする事 はできません。クライアント からこうしたサブフォルダへアクセスできるようにする場 合 は、このオプションを有 効 にします。注 意 点 : このオプションを有 効 化 すると、上 位 のフォルダもクライアント へ許 可 する事 となり、セキュリティのリスクを招 く恐 れがあります。 このオプションはデフォルト で無 効 になっています。

許 可 するパブリックフォルダの最 大 数
端 末 で処 理 するパブリックフォルダ数 を制 限 する場 合 はこのオプションを使 用 します。制 限 が設 定 されると、サーバーは最 大 数 に到 達 するまでフォルダー 覧 を処 理 し、これを超 えるとその後 のデータを送 りません。処 理 するフォルダの順 番 を決 める事 はできません。デフォルト で、全 体 での最 大 数 は設 定 されていません。

共 有 フォルダも含 める

ユーザーがアクセス権を持っている 共有フォルダ[107] をユーザーのActiveSync用端末のフォルダー一覧へ含むにはこのオプションを有効にします。これはデフォルトで有効です。

検索を許可する
共有フォルダ[676] をユーザーが検索できるようになります。これはデフォルトで許可されています。

コンテンツ処理

コンテンツ処理オプション

クライアントにフラグ付けされたメール用にタスク・リマインダーを作成
このオプションでMDaemonはフラグが付いたアイテムごとに仕事を作成し、リマインダーをユーザーへ送信できるようになります。この設定の全体値はデフォルトで有効です。

予定を編集した際、常にミーティングのアップデートを送信
クライアントの中には、ミーティングを編集した際、更新情報を適切に送信しないものもあります。このオプションを使うとActiveSyncサービスへ、ミーティングが開催者によって更新された際、更新情報を送信するよう促す事ができるようになります。これはミーティングの更新情報の送信に失敗しているクライアント[422]やクライアントタイプ[438]に限定して使用するべきで、更新情報が重複して送られてしまう可能性があります。また、このオプションはクライアントとクライアントタイプの設定ページでのみ利用できます。

全ての送信メールで開封確認を要求
クライアントから送信される全てのメールで開封確認要求を行うにはこのオプションを有効にして下さい。これはデフォルトで無効になっています。

送信者からリクエストされた際送信済メールについて開封確認を送信
サーバー側で開封確認要求を検出し、既読フラグがついたメールの開封通知を送信するにはこのオプションを使用します。これはデフォルトで無効になっています。

ReplyToアドレスに指定したエイリアスとして送る
クライアントによっては、エイリアスを使ったメール送信を許可していません。この機能は Exchange ActiveSync（EAS）プロトコル[395] 16.xで追加されたものですが、クライアントの中には16.xに対応していないものもあります。例えば、Windows用OutlookはEAS 14.0だけを使用しており、ユーザーが関連するアドレスを指定して送信する事のみ許可しており、生成されたメールはユーザーの選択を正しく反映していません。このオプションでは、ReplyToのアドレスがユーザー用の正しいエイリアス[757]であれば、これを使ってメール送信を行います。この設定の全体値はデフォルトで有効です。

デフォルトの連絡先にパブリック連絡先を仮想的に統合する
パブリック連絡先をユーザーの端末上でデフォルトの連絡先と統合したい場合はこのオプションを有効にします。これは仮想的な統合で、実際には連絡先フォルダへデータのコピーは行っていません。これはグローバルアドレス帳（GAL）の検索機能に対応していないクライアントにとって便利な機能です。これはデフォルトで無効になっています。

Junk-Emailフォルダへ移動したメールの送信者をブロックする
有効にすると、クライアントが特定のメールを自分のJunk Emailフォルダへ移動した際、対象のメー

ル送信者がブロックされた送信者連絡先フォルダへ追加されます。

ミーティング要求が許可/拒否された際、ミーティング要求に対する応答の送信を強制的に行う
このオプションを使用すると、クライアントがミーティング要求に対して、許可や拒否、その他のアクションを選択した際、ミーティング要求に対する応答を開催者へ送信します。これは、こうした更新情報を自動送信する事ができない特定のクライアント用の機能です。

有効な設定をプレビュー

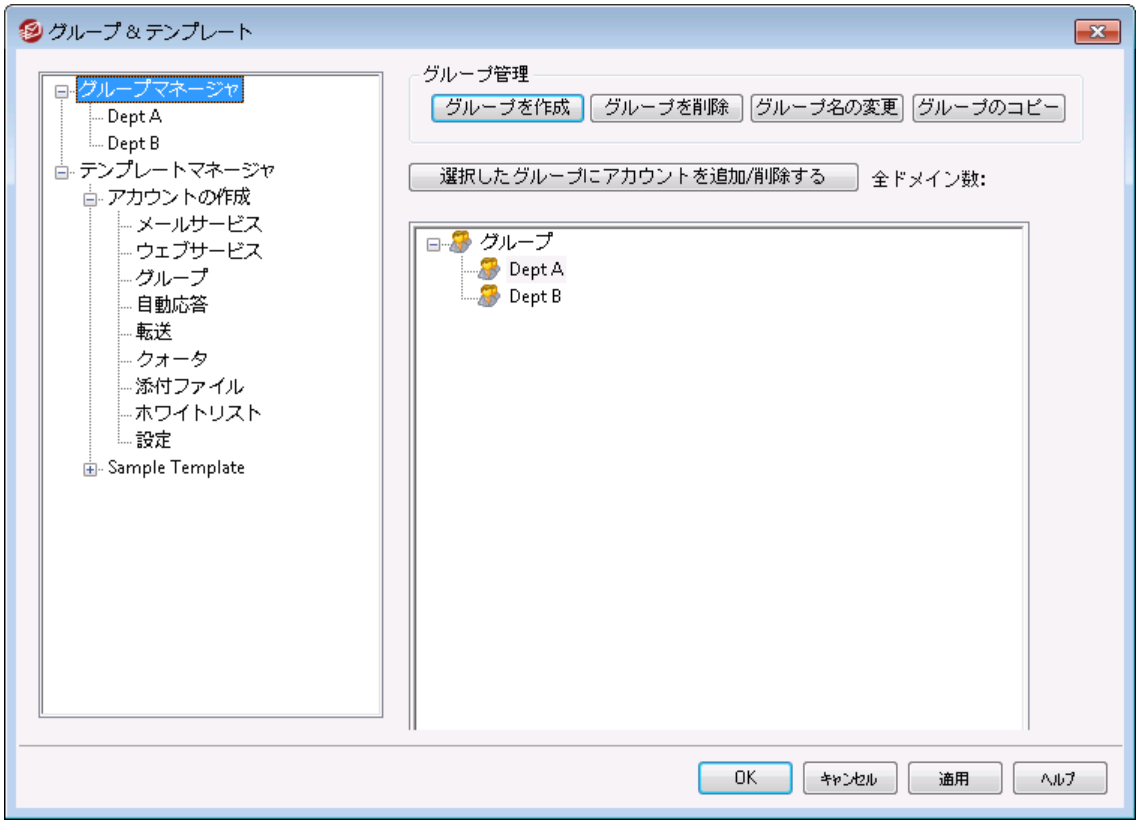
このボタンは全てのクライアント設定（ドメイン397, アカウント413, クライアント422）に対して使用できます。画面のオプションはデフォルト値をその上位の画面から引き継いでいるため、この機能は表示されている画面の現在の設定確認を行う際にもご利用頂けます。

参照:

ActiveSync ≫ クライアント設定384
ActiveSync ≫ ドメイン397
ActiveSync ≫ アカウント413

5.2 グループ & テンプレート

5.2.1 グループマネージャ



グループマネージャ (アカウント ≫ グループ &テンプレート ≫ グループマネージャ) はアカウントグループの作成や所属するアカウントの管理を行うのに使用します。グループには様々なユーザーや機能を指定できます。例えば、グループプロパティ[714]ではアカウントテンプレート[721]をグループに適用でき、グループメンバーの様々なアカウント設定をコントロールできます。また、グループメンバーがMDaemon Instant Messenger[292]やインスタントメッセージを利用できるかどうかも指定できます。更に、コンテンツフィルタもグループに対応しており、メッセージ送信者や宛先がグループのメンバーかどうかを元にルール条件[590]を作成できます。最後に、共有フォルダ[105]に対しては、特定のグループへアクセスコントロールリスト[285]による権限設定が行え、グループメンバーはアクセス権を共有する事ができます。

下の一覧からグループを選択し、「アカウントを追加/削除」ボタンをクリックする事で、アカウントをグループへ追加する事ができます。各ユーザーのメールフォルダ & グループ[653]画面からもユーザーをグループへ追加できます。

グループ管理

グループを作成

新しいアカウントグループを作成する場合は、グループを作成をクリックし、新しいグループ名と説明を入力した後、OKボタンをクリックします。新しいグループ名がグループ一覧と左側の画面へ表示されます。

グループを削除
グループを削除するには、対象グループを選択し、グループを削除をクリックします。確認画面が表示されるので、はい、をクリックします。

グループ名を変更
グループ名を変更するには、対象グループを選択し、グループ名を変更をクリックします。新しい名前を入力して、OKボタンをクリックします。

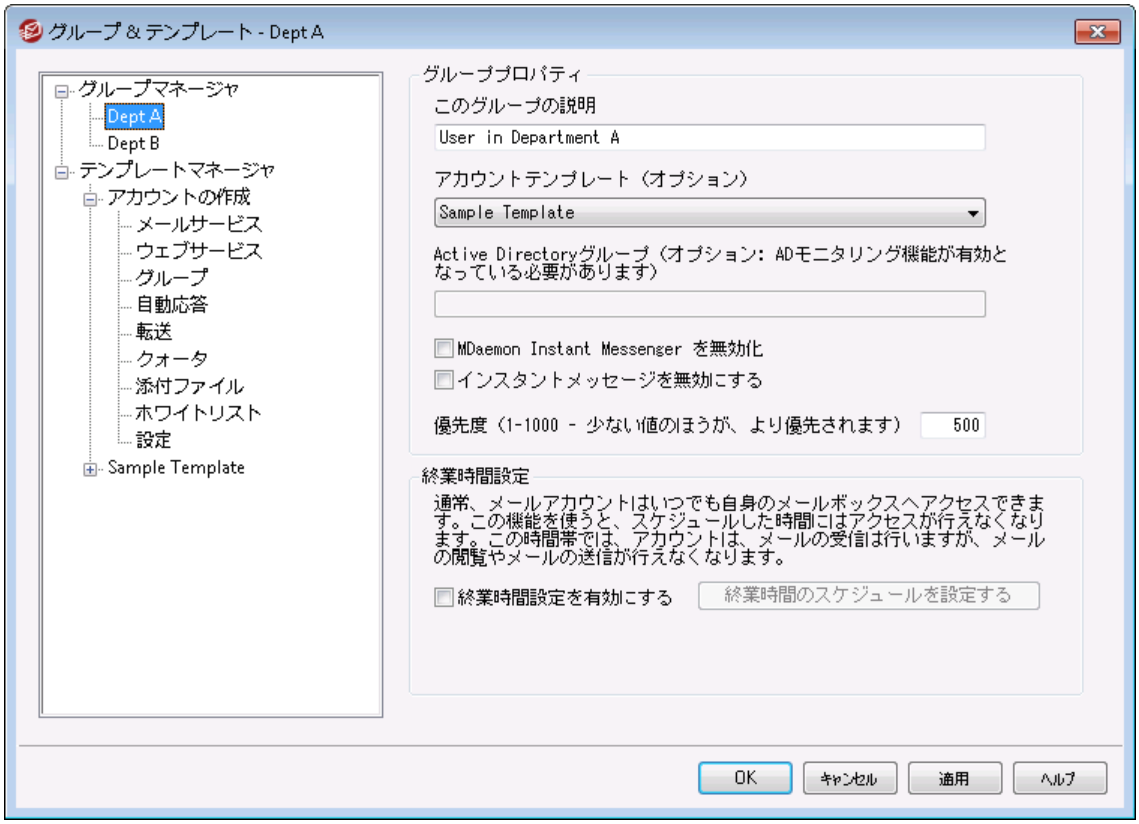
グループをコピー
他のグループと同じ設定のグループを生成するには、一覧からグループを選択し、このボタンをクリックし、新しいグループ名を指定します。

選択したグループにアカウントを追加/削除する
グループメンバーの管理は、対象グループを選択し、このボタンをクリックします。アカウントの隣のチェックボックスをクリックし、外したいメンバーのチェックボックスを解除します。OKボタンをクリックします。

参照:

メールフォルダ & グループ 653
新しいコンテンツフィルタルールの作成 590
共有フォルダ 105

5.2.1.1 グループプロパティ



グループプロパティ（**アカウント » グループ &テンプレート... »** [グループ名])では、グループマネージャ[712]で作成したグループの管理が行えます。グループマネージャからグループプロパティ画面を起動するには、編集したいグループを選択するか、左側のグループ名をクリックして下さい。

ここでは、グループへアカウントテンプレート[721]を適用し、グループメンバーの細かなアカウント設定をコントロールできます。また、グループはActive Directoryグループとリンクさせる事もでき、メンバーがMDaemon Instant Messenger (MDIM)[292]の利用を行えるかどうかや、優先度などの設定も行えます。グループメンバーの設定は、アカウントエディタのグループマネージャか、メールフォルダ & グループ[653]から行えます。

グループプロパティ

このグループの説明
後で参照しやすくするための簡単な説明を入力します。この情報は通常グループ作成時に登録しますが、この画面からいつでも編集する事ができます。

アカウントテンプレート（オプション）

グループメンバーのアカウント設定をコントロールするための アカウントテンプレート[721] を作成している場合は、このドロップダウンリストからテンプレートを選択できます。アカウントテンプレートがグループと紐づけられると、テンプレートプロパティ[723] のアカウント設定が、グループに属しているアカウントへ適用されます。テンプレートはアカウントエディタの個々のアカウント設定よりも、優先されます。ユーザーがグループから削除されると、アカウント設定は新規アカウントテンプレート[722]の値に基づいて変更されます。

アカウントが異なるテンプレートへ関連付けられた複数のグループへ所属している場合、テンプレートプロパティ[723]の値が競合していない限り全てのテンプレートの値が使用されます。複数テンプレートが同じプロパティに対して設定していた場合は、一覧で最初のテンプレートの値を使用します。

Active Directoryグループ（オプション -ADモニタリングが必要です。）
グループをActive Directoryグループとリンクするにはこのオプションを使用して下さい。Active Directoryグループのメンバーはアカウントグループへ自動的に追加されます。これを機能させるためには Active Directoryモニタリング[752]が有効である必要があります。

グループへアカウントを追加するトリガーとして、任意のActive Directory属性を使用する事ができますが、通常は "memberOf" 属性が使われます。この設定は、メモ帳などでActiveDS.datを直接開いて変更できます。この機能はデフォルトで無効になっています。有効にする場合は、ActiveDS.datを編集し、グループのトリガーとして使う属性を定義するか、"Groups=%memberOf%"の行にあるコメントを外して下さい。

MDaemon Instant Messengerを無効化

グループメンバーによるMDIMの利用を無効にするにはこの設定を有効にします。

インスタントメッセージを無効にする
WCIMの使用は許可するものの、インスタントメッセージ機能を無効にしたい場合はこのオプションを使用します。

優先度（1-1000 -少ない値の方がより優先されます）
複数グループに所属するユーザーがグループ毎の設定で競合するのを避けるため、グループの優先度（1-1000）を設定します。例えば同じ項目を持つ異なるグループに所属するアカウントがいた場合、2つのグループ設定が異なると、優先度の値が小さい方のグループ設定を優先します。例えば、優先度が1のグループは、優先度が10のグループと比べて、全てにおいて優先されます。アカウントがリンクしていたアカウントテンプレートから外れた場合、アカウント次に高い優先度のテンプレートが適用されます。他に所属しているグループ設定がない場合、アカウントの作成テンプレート[722]が適用されます。

Create Client Signature
Click this button if you wish to add a client signature to be used for members of the group. See: Group Client Signature[716]

終業時間設定

終業時間設定はアカウントがメールを送信したりメールボックスにアクセスしたりしない時間帯をスケジュールするのに使用します。終業時間の間のアクセスは許可されず、IMAP、POP、SMTP、Webmailでアクセスしようとすると、エラーメッセージが返されます。MDaemonはアカウントに届いたメールを受信しますが、アカウントはメールを送信したり、メールクライアントから届いたメールへアクセスする事はできません。

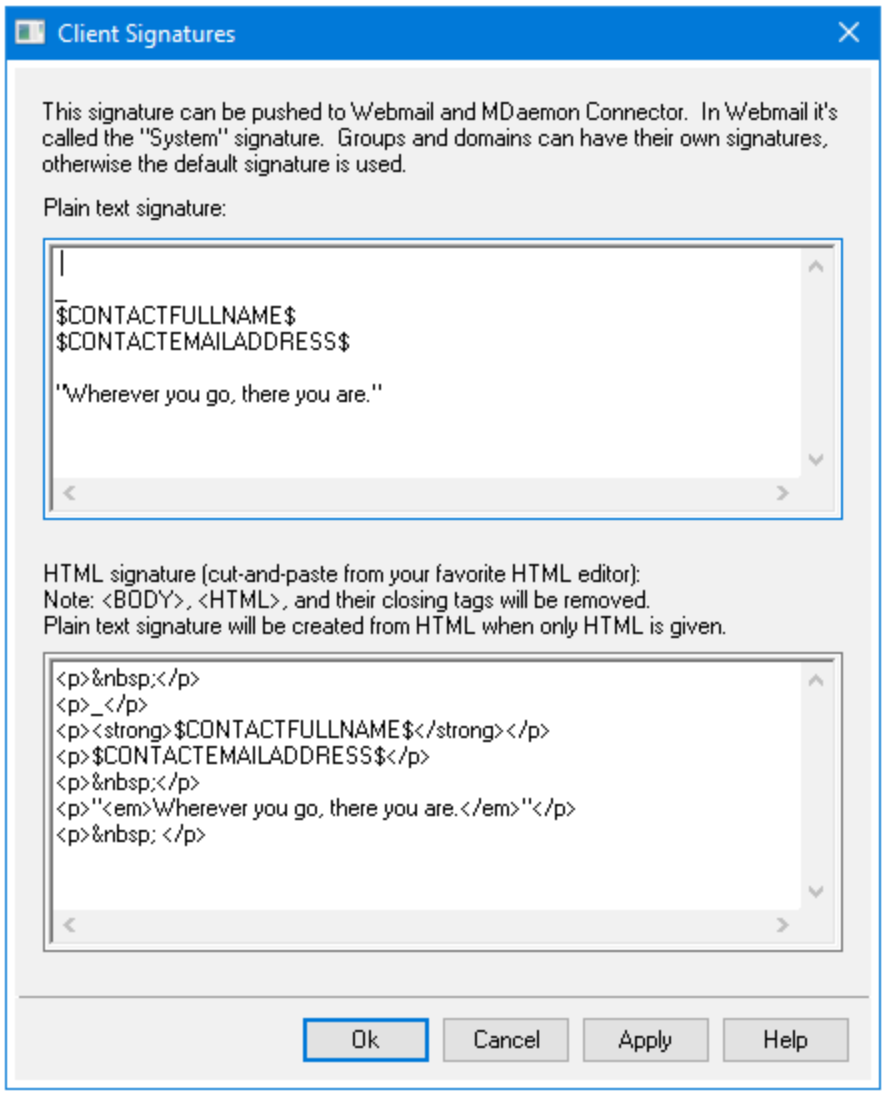
アカウントに終業時間設定を適用するには:

1. **終業時間設定を有効にする**をクリックします。
2. **終業時間の設定をスケジュールする**をクリックします。
3. 開始と終了の日時や、曜日の設定を行います。
4. **Ok**をクリックします。
5. グループマネージャ[712]で対象のアカウントを指定します。

参照:

グループマネージャ 712
メールフォルダ & グループ 653
テンプレートマネージャ 721
テンプレートプロパティ 723

5.2.1.1.1 クライアント署名



クライアント署名をグループ単位で設定できるようになりました。クライアント署名は、MDaemon Webmail[316]かMDaemon Connector[371]を使用しているメンバーに送られます。グループクライアント署名は、デフォルトのクライアント署名[125]を上書きするドメインクライアント署名[188]も上書きします。グループ及びクライアント署名の設定には、MDaemonの管理画面の アカウント | グループ&テンプレート から指定します。クライアント署名の削除では、エディタで署名をブランクにします。

テキスト形式の署名

ここではテキスト形式の 署名を指定します。もしもHTML形式の署名を使いたい場合は、次の*HTML形式の署名*を使って下さい。署名が両方に設定されていた場合、MDaemonはメッセージのフォーマットに応じて適した方の署名を使用します。html形式の署名が指定されていない場合は形式を問わずテキスト形式の署名が追加されます。

HTML形式の署名（ご使用のHTMLエディタからコピーして貼りつけて下さい）

ここではtext/html形式のメッセージで使う HTML 署名を指定します。署名 がこことテキスト形式の署名の両方で設定されている場合は、MDaemonはメッセージのフォーマットに応じて適した方の署名を使用します。テキスト形式の署名が指定されていない場合はhtml形式の署名が追加されます。

html 署名はhtmlコードを手動で入力するか、HTMLエディタからコピーしたものを貼り付けて下さい。HTML署名の中に画像ファイルを含む場合は、$ATTACH_INLINE:path_to_image_file$マクロを使用して下さい。

例:

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \images\mr_t_and_arnold.jpg$">
```

MDaemonのRemote Administration[321]でも、複数の方法で署名へ画像を追加できます。

- Remote Administrationの署名/フッタ画面で、HTMLエディタの「画像」ツールバーをクリックし、アップロードタブを選択します。
- Remote Administrationの署名/フッタ画面で、HTMLエディタのツールバーにある「画像の追加」ボタンをクリックします。
- Chrome, FireFox, Safari, MSIE 10+では、HTMLエディタの署名/フッタ画面へ画像をドラッグ&ドロップできます。
- Chrome, FireFox, MSIE 11+ではHTMLエディタの署名/フッタ画面へクリップボードの画像をコピーして貼り付けできます。

<body></body> と <html></html> タグは許可されておらず、使用した場合は削除されます。

署名マクロ

MDaemonの署名機能はマクロに対応しており、送信者の連絡先情報や、パブリック連絡先に登録してある送信者連絡先情報を、署名へ追加する事ができます。これにより、デフォルトやドメイン毎の署名も、送信者情報を個別に指定できるようになります。 例えば、 $CONTACTFULLNAME$ は送信者の氏名を挿入し、$CONTACTEMAILADDRESS$ は送信者のメールアドレスを挿入します。パブリック連絡先は、Webmail, MDaemon Connector, ActiveSyncから編集できます。空の値は送信者の連

絡先情報が存在しない場合に使用されます。利用できるマクロは次の通りです。

ユーザーはMDaemon署名を、$SYSTEMSIGNATURE$ マクロでデフォルト/ドメイン署名へ、$ACCOUNTSIGNATURE$ マクロでアカウント署名へ変換できます。

Signature Selector	
$SYSTEMSIGNATURE$	デフォルト署名 120またはドメイン署名をメッセージに配置する。両方が存在する場合は、ドメイン署名 184が使用される。
$CLIENTSIGNATURE$	メッセージにデフォルトクライアント署名 125またはドメインクライアント署名 188を入れる。両方が存在する場合は、ドメインクライアント署名を使用する。
$ACCOUNTSIGNATURE$	アカウント署名 686をメッセージに配置する。
名前とID	
Full name	**$CONTACTFULLNAME$**
First name	**$CONTACTFIRSTNAME$**
Middle name	**$CONTACTMIDDLENAME$,**
Last name	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
Suffix	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Yomi First Name	**$CONTACTYOMIFIRSTNAME$**
Yomi Last Name	**$CONTACTYOMILASTNAME$**
Account name	**$CONTACTACCOUNTNAME$**
Customer ID	**$CONTACTCUSTOMERID$**
Government ID	**$CONTACTGOVERNMENTID$**
File as	**$CONTACTFILEAS$**
メールアドレス	
Email address	**$CONTACTEMAILADDRESS$**
Email address 2	**$CONTACTEMAILADDRESS2$**
Email address 3	**$CONTACTEMAILADDRESS3$**
電話とFAX番号	
Mobile phone	**$CONTACTHOMEMOBILE$**
Mobile phone 2	**$CONTACTMOBILE2$**

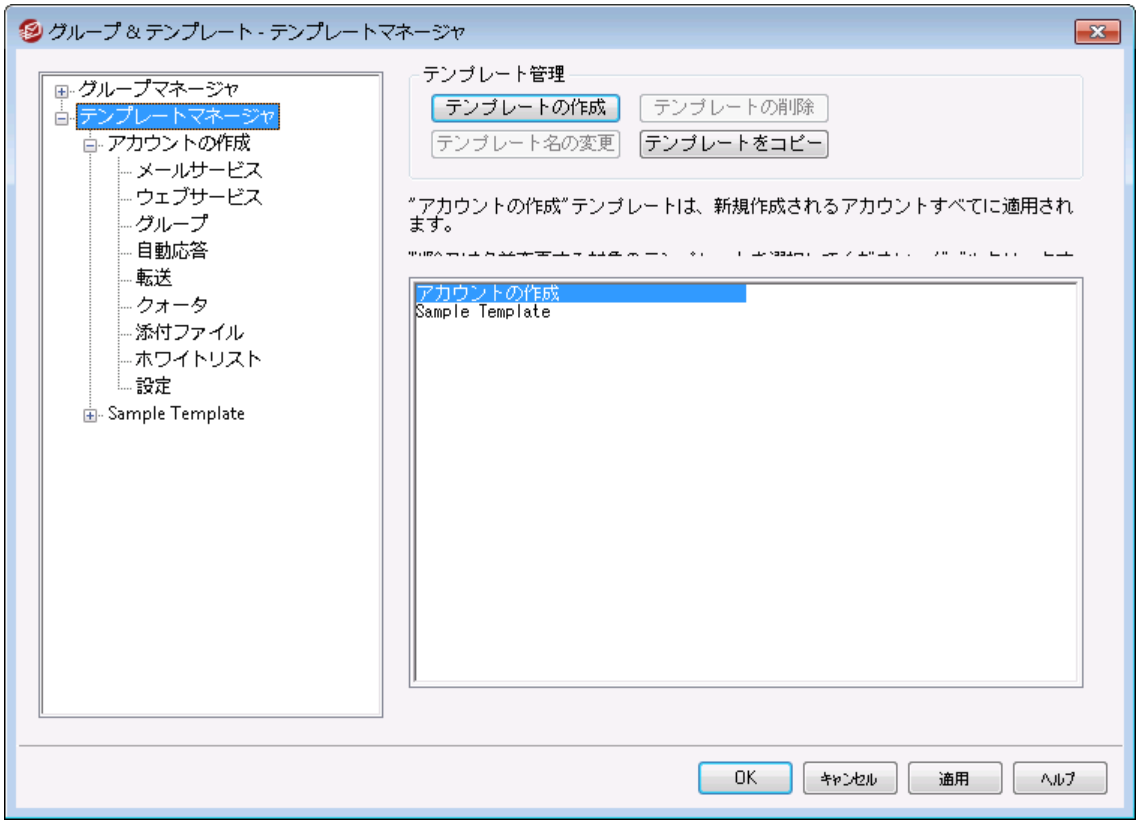
Car phone	**$CONTACTCARPHONENUMBER$**
Home phone	**$CONTACTHOMEPHONE$**
Home phone 2	**$CONTACTHOMEPHONE2$**
Home fax	**$CONTACTHOMEFAX$**
Other phone	**$CONTACTOTHERPHONE$**
インスタント メッセージとウェブ	
IM Address	**$CONTACTIMADDRESS$**
IM Address 2	**$CONTACTIMADDRESS2$**
IM Address 3	**$CONTACTIMADDRESS3$**
MMS Address	**$CONTACTMMSADDRESS$**
Home web address	**$CONTACTHOMEWEBADDRESS$**
住所	
Home address	**$CONTACTHOMEADDRESS$**
Home city	**$CONTACTHOMECITY$**
Home state	**$CONTACTHOMESTATE$**
Home zip code	**$CONTACTHOMEZIPCODE$**
Home country	**$CONTACTHOMECOUNTRY$**
Other address	**$CONTACTOTHERADDRESS$**
Other city	**$CONTACTOTHERCITY$**
Other state	**$CONTACTOTHERSTATE$**
Other zip code	**$CONTACTOTHERZIPCODE$**
Other country	**$CONTACTOTHERCOUNTRY$**
仕事関連	
Business Name	**$CONTACTBUSINESSCOMPANY$**
Yomi Business Name	**$CONTACTYOMICOMPANYNAME$**
Business title	**$CONTACTBUSINESSTITLE$**
Business office	**$CONTACTBUSINESSOFFICE$**
Business department	**$CONTACTBUSINESSDEPARTMENT$**
Business manager	**$CONTACTBUSINESSMANAGER$**
Business assistant	**$CONTACTBUSINESSASSISTANT$**

Business assistant phone	**$CONTACTBUSINESSASSISTANTPHONE$**
Business main phone	**$CONTACTBUSINESSMAINPHONE$**
Business phone	**$CONTACTBUSINESSPHONE$**
Business phone 2	**$CONTACTBUSINESSPHONE2$**
Business IP phone	**$CONTACTBUSINESSIPPHONE$**
Business fax	**$CONTACTBUSINESSFAX$**
Business pager	**$CONTACTBUSINESSPAGER$**
Business radio	**$CONTACTBUSINESSRADIO$**
Business address	**$CONTACTBUSINESSADDRESS$**
Business city	**$CONTACTBUSINESSCITY$**
Business state	**$CONTACTBUSINESSSTATE$**
Business zip code	**$CONTACTBUSINESSZIPCODE$**
Business country	**$CONTACTBUSINESSCOUNTRY$**
Business web address	**$CONTACTBUSINESSWEBADDRESS$**
その他	
Spouse	**$CONTACTSPOUSE$**
Children	**$CONTACTCHILDREN$**
Categories	**$CONTACTCATEGORIES$**
Comment	**$CONTACTCOMMENT$**

参照:

デフォルトクライアント署名 125
デフォルト署名 120
ドメインマネージャ ≫ 署名 184
アカウントエディタ ≫ 署名 686
ドメインマネージャ ≫ Webmail設定 176
MCクライアント設定 ≫ 署名 371

5.2.2 テンプレートマネージャ



テンプレート マネージャ（アカウント ≫ グループ & テンプレート... ≫ テンプレート マネージャ）では、グループ[712] に所属しているアカウントの設定を行うための、アカウント テンプレートの作成や管理が行えます。テンプレートで管理されたグループに所属しているアカウントは、該当の設定箇所はアカウント エディタ上ではロックされます。アカウント設定は各テンプレートのプロパティ[723]画面で確認できます。テンプレートの詳細は、テンプレート名をダブルクリックするか、左側からテンプレート名を選択して頂く事でアクセスする事ができます。

テンプレート マネージャ

テンプレートを作成

アカウント テンプレートを作成するには、テンプレートを作成をクリックし、テンプレート名を入力した後、OKをクリックします。新しいテンプレートが一覧と左側に表示されます。

テンプレートを削除

テンプレートを削除する場合は、テンプレートを一覧から選択し、テンプレートを削除をクリックします。確認用のウィンドウで、はい、をクリックするとテンプレートが削除されます。

テンプレート名の変更

アカウント テンプレート名を変更するには、テンプレート名の変更をクリックし、テンプレート名を入力した後、OKをクリックします。

テンプレートのコピー
テンプレートを他のテンプレートと同じ設定で作成するには、対象のテンプレートを選択しこのボタンをクリックし、テンプレート名を指定します。

テンプレート一覧

テンプレートマネージャの下の部分へ、テンプレートが一覧表示されます。テンプレートをクリックして上部ボタンから削除や名前変更が行えます。テンプレートをダブルクリックすると、テンプレートのプロパティ[723]画面が表示され、アカウント用の設定が行えます。 *アカウントの作成* テンプレートは特別なテンプレートで必ず一番上に表示されます。

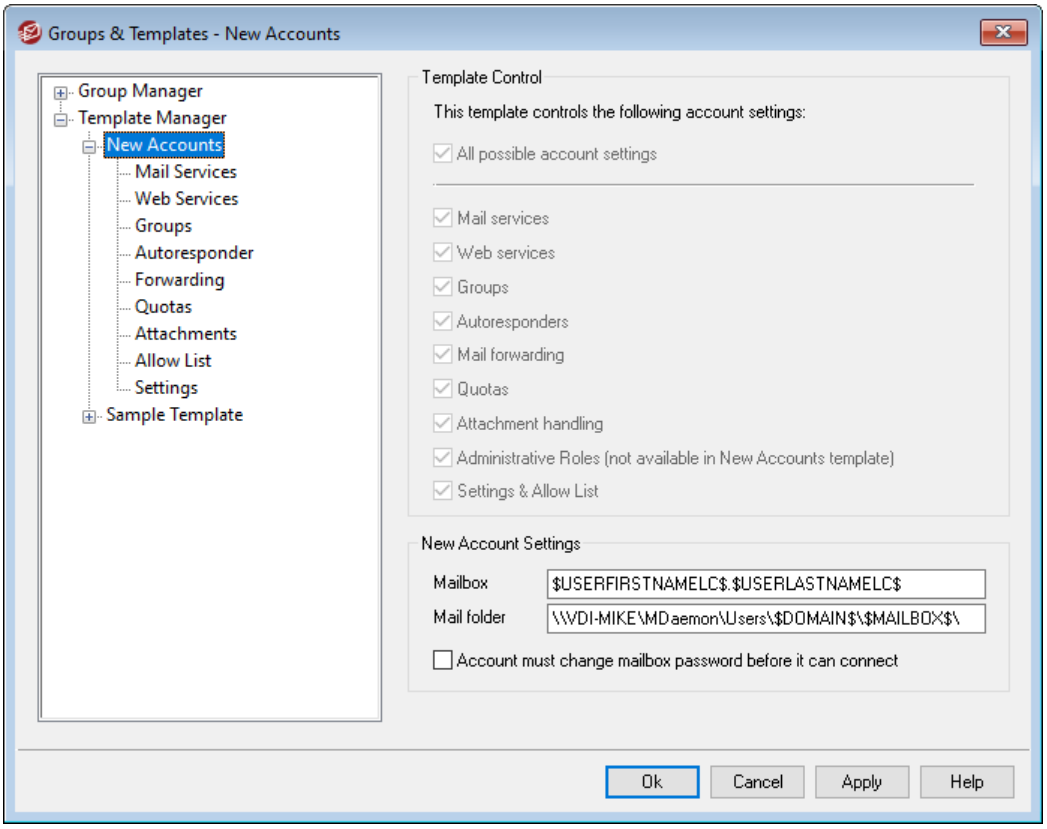
アカウントの作成テンプレート

アカウントの作成 テンプレートは特別なテンプレートで、新しいアカウントを追加した際適用される設定が含まれています。他のテンプレートのようにアカウントの設定をロックしたりコントロールしたりするのではなく、アカウントの作成テンプレートは新しく追加したアカウントの初期設定として使用されます。初期設定値はアカウントエディタを使って個別に変更が行えます。 管理者権限の割り当て[742]画面のオプションなど、テンプレート設定の幾つかは、アカウントの作成テンプレートでは利用できません。

参照:

テンプレートプロパティ[723]
グループマネージャ[712]

5.2.2.1 テンプレートプロパティ



テンプレートプロパティは テンプレートマネージャ[721] で画面左側のテンプレート名をクリックするとアクセスできます。それぞれのテンプレートのプロパティでは、アカウント設定をカテゴリ毎に調整できます。アカウントテンプレートに関連付けされた グループ[712] に所属しているユーザーは、このテンプレートによって管理され、アカウントエディタの該当箇所はロックされます。アカウントが異なるテンプレートへ関連付けられた複数グループに所属している場合、全てのテンプレートの値で競合していないもの全てが使用されます。複数テンプレートが同じプロパティに対して設定されていた場合、一覧の中で最初のテンプレートの値が使用されます。

テンプレートコントロール

すべてのアカウント設定を行えるようにする
このテンプレートで グループ[712] に所属したアカウント設定をコントロールする場合はこのボックスをクリックします。アカウントエディタで行った設定はグループメンバーのアカウント設定で置き換えられます。特定のアカウント設定オプションを優先したい場合は、このチェックボックスを無効化します。

アカウント設定
このセクションにはテンプレートを使用するグループ用のアカウント設定カテゴリの一覧が表示されます。各オプションは同じ名前のテンプレート画面に対応しています。オプションが選択されると、テンプレート画面がグループメンバーのアカウントエディタに代わって使用されます。

新規アカウント設定

このオプションは 新規アカウントテンプレート[722] でのみ利用できます。ここでは新しいアドレスのメールアドレスを元にしたメールフォルダの自動生成を行うための、特別なマクロ[724] が使用できます。

メールボックス
ここでは新しいアドレスのメールアドレスを元に *メールボックス*[650] を設定します。テンプレートの値に使用されるマクロの一覧については、後述の テンプレートマクロ[724] を参照してください。"$USERFIRSTNAMELC$.$USERLASTNAMELC$" がこのオプションのデフォルトです。例えば、example.comドメインに"Michael Mason"というアカウントを作成すると、メールアドレスは"michael.mason@example.com"の形式で作成されます。

メールフォルダ
新しいアカウントのメール用に生成されるデフォルトの *メールフォルダ*[653] を設定します。各アカウントの*メールフォルダ*にはメッセージが保管されます。例えば、"...\$DOMAIN$\$MAILBOX$\"と設定されている場合は、"michael.mason@example.com"用に"...\example.com\michael.mason\"というメールボックスが生成されます。

MDaemonは基本的なフォルダハッシュに対応しています。NTFSでは、同じフォルダへ多くのフォルダを保持する事がパフォーマンスの問題を引き起こす場合があります。ユーザー数が多い環境でユーザーフォルダを$DOMAIN$¥$MAILBOX$¥というデフォルト値よりも更に分割したい場合には$MAILBOXFIRSTCHARSn$というマクロを使用します。このマクロの"n"には1から10までの数字を指定し、最大10分割できます。デフォルトの*メールフォルダ*パスを例えば次のように変更する事で、簡単なフォルダハッシュが行えます。

```
C:
\MailboxRoot\$MAILBOXFIRSTCHARS4$\$MAILBOXFIRSTCHARS
2$\$MAILBOX$\
```

アカウントは接続前にパスワード変更が必要
このオプションでは新しいアカウントがPOP、IMAP、SMTP、Webmail、RemoteAdministrationへアクセスする際、ユーザーにパスワード変更を行わせるかどうかを指定します。ユーザーはWebmailやRemote Administrationへ接続は行えますが、処理を行う前にパスワード変更が必要になります。ただし、ユーザーがWebmailやRemote Administrationでパスワード変更できるようにするには、管理者がウェブサービス[728]画面で、ウェブアクセス権限として「パスワードの編集」を許可しておく必要があります。パスワード変更後は、このオプションはアカウントのアカウント詳細[650]画面から無効化しても構いません。

パスワード変更が簡単に行えなかったり不可能だったりする環境もあるため、このオプションを有効化する際には事前アナウンスをお勧めします。

テンプレートマクロ

以下はアカウント設定を自動化するのに使用できるマクロのリファレンスです。

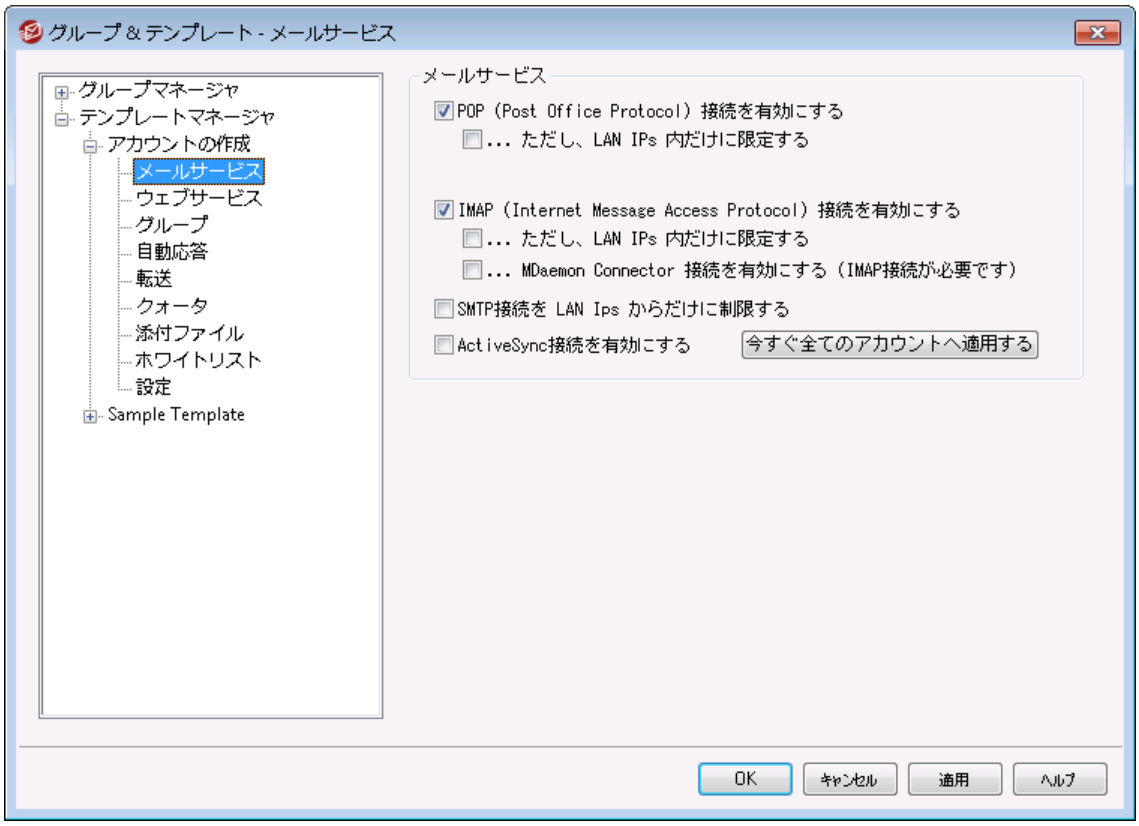
$DOMAIN$	この変数はアカウント用のドメイン名に置き換わります。

$DOMAINIP$	この変数はアカウントが所属しているドメインのIPv4アドレスです。
$DOMAINIP6$	この変数はアカウントが所属しているドメインのIPv6アドレスです。
$MACHINENAME$	この変数はドメインマネージャのホスト名＆IPで指定されているデフォルトドメインのホスト名です。新規インストールを行った場合、このマクロはデフォルトのアカウント情報用スクリプト（NEW USERHELP.DAT）でも使用されます。
$USERNAME$	この変数はアカウント用のフルネームです。このフィールドは"$USERFIRSTNAME$ $USERLASTNAME$"と同じものです。
$USERFIRSTNAME$	この変数はアカウントの名（First Name）です。
$USERFIRSTNAMELC$	この変数はアカウントの名（First Name）を小文字に変換したものです。
$USERLASTNAME$	この変数はアカウントの姓（Last Name）です。
$USERLASTNAMELC$	この変数はアカウントの姓（Last Name）を小文字に変換したものです。
$USERFIRSTINITIAL$	この変数はアカウントの名（First Name）の最初の文字です。
$USERFIRSTINITIALLC$	この変数はアカウントの名（First Name）の最初の文字を小文字に変換したものです。
$USERLASTINITIAL$	この変数はアカウントの姓（Last Name）の最初の文字です。
$USERLASTINITIALLC$	この変数はアカウントの姓（Last Name）の最初の文字を小文字に変換したものです。
$MAILBOX$	この変数はアカウント用のメールボックス名になります。この値はPOP3メールセッションで渡されるUSERコマンドとしても使用されます。
$MAILBOXFIRSTCHARSn$	"n"には1から10までの数字を指定し、メールボックス名の最初の"n"文字がサブフォルダとして展開されます。

参照:

テンプレートマネージャ[721]
グループマネージャ[712]

5.2.2.1.1 メールサービス



テンプレートのこの画面はアカウントエディタのメールサービス[654]機能と関連しています。テンプレートがこのアカウント設定をコントロールする[723]と設定されていた場合、テンプレートを使用するグループ[714]に所属するアカウントのメールサービス設定はこの画面の設定でコントロールされます。

メールサービス

POP (Post Office Protocol)を使用する
この設定が有効の場合、アカウントはPost Office Protocol (POP)を使ってメールへアクセスできるようになります。このプロトコルは、全てのメールクライアントが対応しているプロトコルです。POPを使用しない場合はこのチェックボックスをクリアしてください。

...ただし、LAN IP 内だけに限定する
ユーザーがLAN IPアドレス[554]からの接続の場合のみPOP経由でのアクセスを許可する場合は、このオプションを有効にして下さい。

IMAP (Internet Message Access Protocol)を使用する
この設定が有効の場合、アカウントはInternet Message Access Protocol (IMAP)を使ってメールへアクセスできるようになります。IMAPはPOP3よりも広い目的に対応したプロトコルで、サーバー側でメールを管理し、複数のクライアントから接続することができます。多くのメールクライアントソフトウェアが、このプロトコルに対応しています。

...ただし、LAN IP内だけに限定する
ユーザーがLAN IPアドレス[554]からの接続の場合のみIMAP経由でのアクセスを許可する場合は、このオプションを有効にして下さい。

...MDaemon Connectorを有効にする (IMAPが必要です)
このオプションは新規アカウントテンプレートでのみ使用できます。MDaemon Connector[353]を使って、新規に作成したアカウントがMicrosoft Outlookでデータ共有できるようにするには、このオプションを有効にします。注意: このオプションはMDaemon Connectorがアクティベーションされている場合のみ有効です。

SMTPアクセスをLAN IPだけに限定する
SMTPアクセスをLAN IPに限定する場合はこの設定を有効にしてください。これによりネットワークに接続していないアカウントからのメール送信を防ぐ事ができます。外部IPアドレスでメール送信を行うと、接続は拒否され、通信が閉じられます。

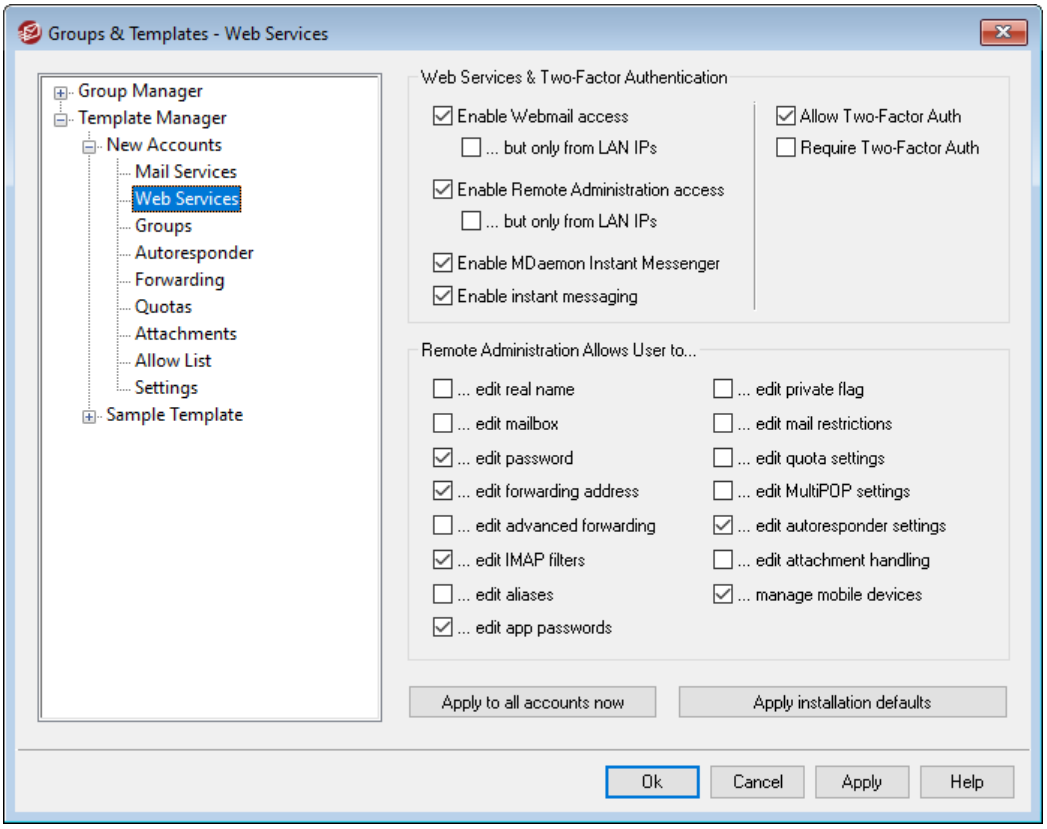
ActiveSyncアクセスを有効にする
このオプションは新規アカウントテンプレートでのみ利用できます。アカウントがActiveSyncを使ってメールや連絡先、予定表やその他のデータをMDaemon/Webmailと同期できるようにする場合はこのチェックボックスを有効にして下さい。この設定はアカウントエディタのActiveSync for MDaemon[696]にある*ユーザーのActiveSyncサービスを有効にする*オプションと同じものです。

今すぐ全てのアカウントへ適用
このオプションは新規アカウントテンプレートでのみ利用できます。このボタンをクリックすると、画面の設定がMDaemonアカウントのメールサービス[654]とActiveSync for MDaemon[696]画面の設定値を上書きします。

参照:

テンプレートプロパティ[723]
グループプロパティ[714]
新規アカウントテンプレート[722]
アカウントエディタ ≫ メールサービス[654]

5.2.2.1.2 ウェブサービス



テンプレートのこの画面はアカウントエディタのウェブサービス[656]機能と関連しています。テンプレートがこのアカウント設定をコントロールする[723]と設定されていた場合、テンプレートを使用するグループ[714]に所属するアカウントのウェブサービスオプションはこの画面の設定でコントロールされます。

ウェブサービス & 2段階認証

Webmailアクセスを有効にする
このテンプレートでコントロールされているアカウントが、ブラウザを使ってWebmail[291]へアクセスし、メール、予定表、その他の機能を利用できるようにするには、この設定を有効にします。

LAN IPからの場合のみ許可
ユーザーがLAN IPアドレス[554]からの接続の場合のみWebmailへのアクセスを許可する場合は、このオプションを有効にして下さい。

Remote Administrationへのアクセスを有効にする
このテンプレートでコントロールされているアカウントが、Remote Administration[321]で、設定変更を行えるようにするにはこの設定を有効にします。ユーザは以下の項目で有効にした設定のみを編集することが可能です。

この機能が有効で、Remote Administrationサーバーが稼働していると、ユーザーはMDaemon用のドメインとRemote Administration用ポート[322](例. http://example.com:1000)をブラウザで指定する事により Remote Administrationにログインすることができます。まずログオン画面が表示され、次にユーザが編集の許可を与えられている設定画面が表示されます。ユーザに必要な作業は、選択した設定を変更して、[変更を保存]ボタンをクリックするだけです。そして、ブラウザから

ログアウトしてブラウザを閉じます。 ユーザーがWebmailに対するアクセス権も与えられている場合、Webmailの詳細オプションメニューからもRemote Administrationへアクセスする事ができます。

（アカウントエディタの管理者権限の割り当て[690]画面で指定する）全体あるいはドメイン管理者としてのアクセス権限が与えられているユーザの場合、Remote Administrationにログオンしたあとに表示される画面が異なります。

...ただし、LAN IP内だけに限定する
ユーザーがLAN IPアドレス[554]からの接続の場合のみWebmail経由でのアクセスを許可する場合は、このオプションを有効にして下さい。

MDaemon Instant Messengerを有効にする
新しく追加したアカウントがデフォルトで MDIM[292] を使用できるようにするにはこの設定を有効にします。このオプションはアカウントの作成テンプレート[722]でのみ利用できます。グループプロパティ[714]にもこれに似たオプションがあり、MDIMへアクセスするグループメンバーの設定が行えます。

インスタントメッセージを有効にする
新しく追加したアカウントがデフォルトでMDIMのインスタントメッセージも利用できるようにする場合は、このオプションをクリックします。このオプションはアカウントの作成テンプレート[722]でのみ利用できます。グループプロパティ[714]にもこれに似たオプションがあり、インスタントメッセージへアクセスするグループメンバーの設定が行えます。

2段階認証

MDaemonはWebmailやMDaemonのRemote Administrationウェブ画面へサインインするのに、2段階認証（2FA）に対応しています。HTTPSでWebmailへサインインするアカウントはWebmailのオプション >> セキュリティ画面から2段階認証のアクティベートが行えます。コードはモバイル端末やタブレットへインストールした認証アプリで取得できます。この機能はGoogle認証に対応した全てのクライアントで使用できます。アカウントの2FA設定についての詳細は、Webmailのヘルプを参照して下さい。

2段階認証を許可
デフォルトで新規アカウントはWebmailの2段階認証（2FA）機能の設定や使用が許可されています。新しく追加したアカウントでデフォルトで2FAを使用させたくない場合は、このチェックボックスを無効にして下さい。この設定はアカウント毎のウェブサービス[656]ページから個別に設定する事もできます。

2段階認証を必須とする
新しく作成した全てのアカウントで2段階認証（2FA）の使用を必須とする場合はこのオプションを有効化して下さい。2FAを必須とすると、これを使用するよう設定を行っていないアカウントは、次回Webmailへログインした際、設定ページへリダイレクトされます。2FAの設定に関する詳細は、Webmailのヘルプを参照して下さい。

Remote Administrationで行える設定

リアルネーム
この機能を有効にすると、ユーザは*姓名*[650]を変更することが許可されます。

メールボックス
この機能を有効にすると、ユーザは*メールボックス名*[650]を変更することが許可されます。

メールボックス名はアカウントのメールアドレスの一部で、他のアドレスとの重複がない一意の値でもあるため、これを変更するという事は、実際のメールアドレスを変更していることを意味します。これにより、今後のメールが古いアドレスへ転送され、結果として拒否されたり、削除されたり、これと似た処理が行われてしまう可能性が生じます。

パスワード
ユーザがアカウントのメールパスワードの変更できるようにする場合、このチェックボックスを選択します。パスワード要件については パスワード[778]を参照してください。

転送アドレス
この機能を有効にすると、ユーザは転送[663]アドレスの設定を編集できるようになります。

転送先詳細
この機能を有効にすると、ユーザは*詳細な転送設定*[663]を編集できるようになります。

IMAPフィルタ
このコントロールを使用すると、ユーザは自身のIMAPフィルタ[670]を作成、管理できます。

エイリアスを編集
Remote Administrationからアカウントに関連した エイリアス[675] を編集できるかどうかを指定します。

Appパスワードを編集
デフォルトで、ユーザーはそれぞれ Appパスワード[683] を編集できます。ユーザーに編集させないようにするにはこのチェックボックスを無効にしてください。

プライベートフラグ
このオプションは、ユーザがRemote Administrationから、アカウントエディタの設定[693]画面にある[*アカウントを「Everyone」メーリングリスト、共有カレンダ、VRFYで非表示にする*]オプションを編集できるかどうかを指定します。

メール制限
制限[664] 画面の送信/受信メール制限を編集できるかどうかコントロールします。

クォータ設定
アカウントにクォータ[666]設定の変更を許可する場合は、このチェックボックスを選択してください。

MultiPOP設定
新規のMultiPOP[673]エントリを追加したり、それらのエントリに対してMultiPOP収集の有効化/無効化を行えるよう、アカウントに権限を与える場合はこの設定を有効にします。

自動応答の設定
ユーザにアカウントの自動応答[660]の追加、編集、または削除を許可する場合は、このチェックボックスを選択してください。

添付ファイル処理の編集
ユーザが、添付ファイル[669]画面の中の添付ファイル処理オプションを編集できるようにする場合、このチェックボックスを選択します。

モバイルデバイスの管理
アカウント所有者がRemote Administrationを使ってActiveSyncデバイスの設定を行えるようにするにはこのボックスをチェックします。

今すぐ全てのアカウントへ適用

このオプションは アカウントの作成テンプレート[722] を使用している場合のみ有効です。ウェブサービスがアカウントテンプレートで管理されていない全てのMDaemonアカウントに設定を適用する場合はこのボタンをクリックします。

インストール時のデフォルト設定を読み込む

このオプションは アカウントの作成テンプレート[722] でのみ利用できます。アカウントの作成テンプレートをインストール時のデフォルト設定にリセットします。これはテンプレートの設定のみを変更し、既存のアカウント設定の変更は行いません。

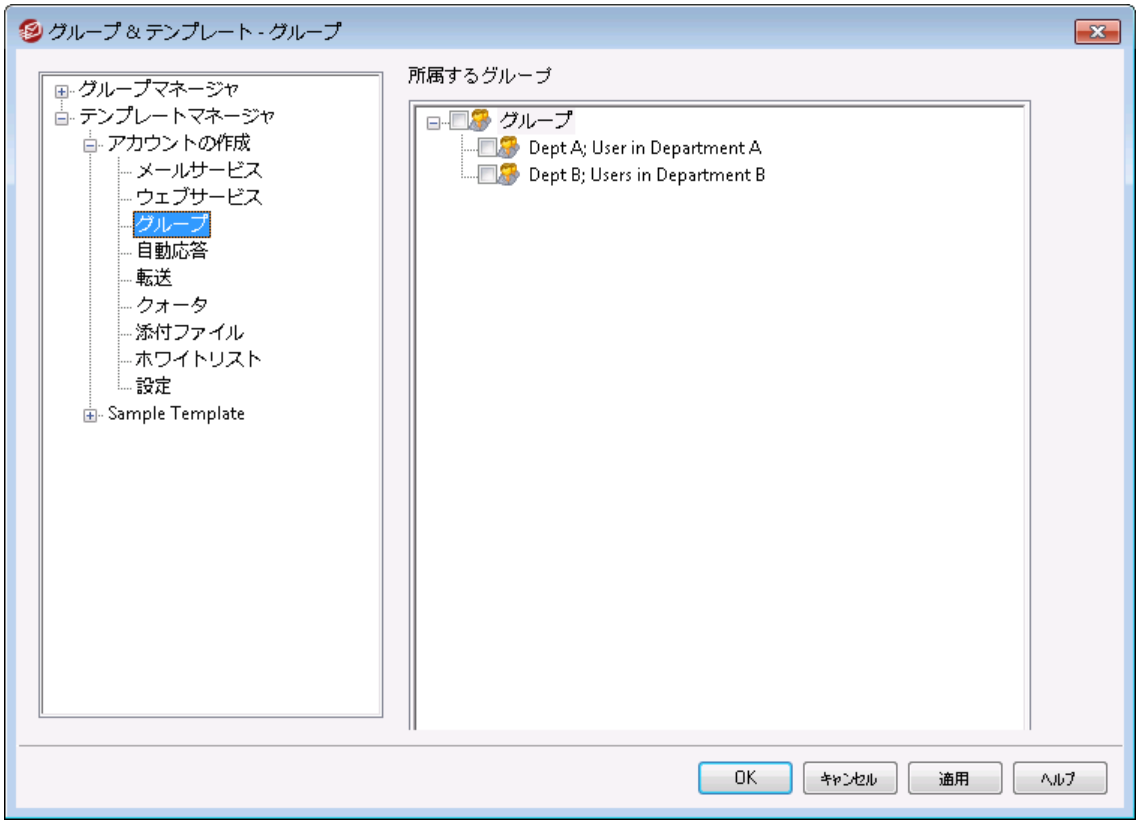
アカウントの作成テンプレートを読み込む

このオプションはカスタムテンプレートを使用している場合のみ使用できます。この画面で行った設定を、アカウントの作成テンプレート[722]のウェブサービス画面で指定したデフォルト値へ戻すにはこのボタンをクリックします。

参照:

テンプレートプロパティ[723]
グループプロパティ[714]
アカウントの作成テンプレート[722]
アカウントエディタ ≫ ウェブサービス[656]

5.2.2.1.3 グループ



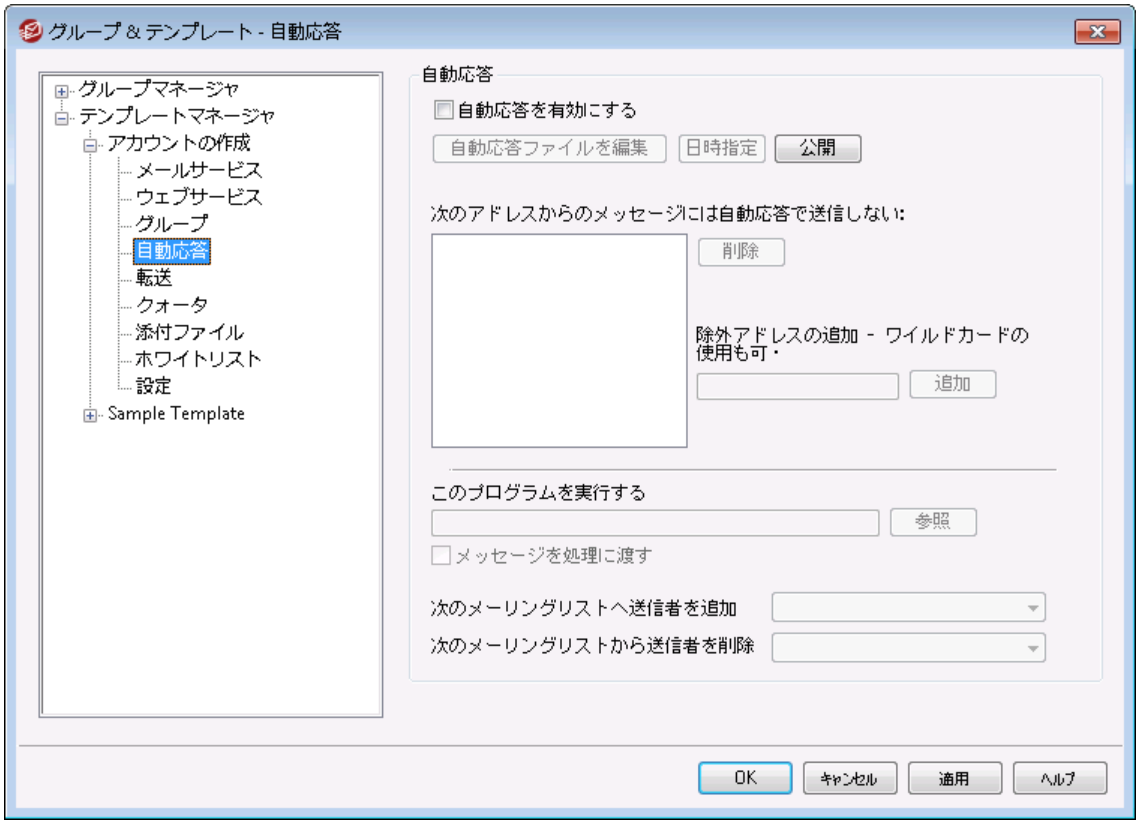
グループメンバー

この画面は新規アカウントテンプレート[722]と、アカウントエディタのメールフォルダとグループ[653]にある、対応グループメンバーセクションでのみ利用できます。この画面で1つかそれ以上のグループを選択すると、新しいアカウントは対象グループへ自動で追加されます。

参照:

新規アカウントテンプレート[722]
グループマネージャ[712]
グループプロパティ[714]

5.2.2.1.4 自動応答



自動応答は、例えば、プログラムの実行、メーリングリストに送信者を追加、自動的に生成されたメッセージでの応答など、受信メールによって特定のイベントを発生するのに便利な機能です。自動応答で最も一般的な使用方法は、メールの受信者が休暇中ですぐに対応できず、できるだけ早く返信する、といった内容の返信を自動で送信するというものです。Webmail[291]またはRemote Administration[321]へのWebアクセス[656]を使って、MDaemonユーザは、自動応答メッセージの作成や自動応答の利用期間のスケジュール設定が行えます。最後に、自動応答はユーザーの¥data¥フォルダにあるOOF.mrkファイルの内容を元にしています。このファイルは多数のマクロに対応しており、その結果として、自動応答機能へ高い柔軟性を搭載しています。

メッセージがリモートソースからの場合、自動応答は常に引き継がれます。ただし、ユーザーが属するドメインから送信されるメッセージについては、自動応答 ≫ 設定[765]画面の、メールに自動応答するオプションが有効な場合のみ実行されます。自動応答メールは、送信者毎に1日1回までと制限する事もできます。

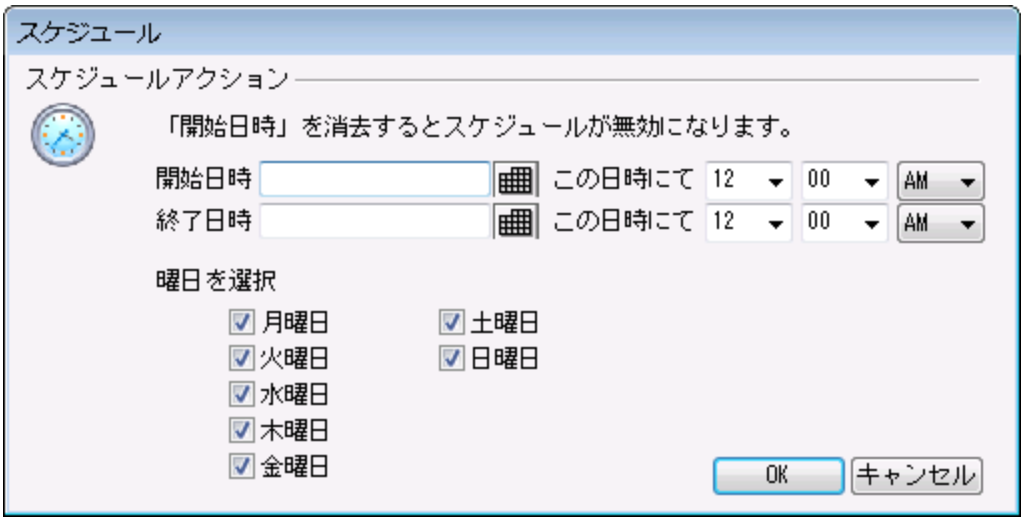
自動応答

自動応答を有効にする
このコントロールを有効にすると自動応答機能が開始されます。詳細は自動応答[761]を参照してください。

自動応答ファイルの編集
自動応答スクリプトを開いて編集する場合はこのボタンをクリックします。このファイルはユーザーの¥data¥フォルダにあるOOF.mrkファイルです。

スケジュール

このボタンをクリックするとスケジュールダイアログが開き、自動応答の開始と終了の日時やアクティブにしておく曜日をここで設定できます。自動応答を継続的に起動させたい場合は、スケジュールを空欄にしてください。



公開
アカウントの自動応答ファイルを他のアカウントへコピーするにはこのボタンをクリックします。自動応答をコピーしたいアカウントを選択し、OKをクリックします。

次のアドレスからのメッセージには自動応答で返信しない
ここには、自動応答から除外するアドレスを入力してください。

場合によって、自動応答メッセージを送ったメールアドレスで、更に自動応答メールが返信される場合があります。これは、「ピンポン」のように、2台のサーバ間でメールが絶えず行ったり来たりする状態を生み出してしまう可能性があります。こうしたアドレスを確認した場合は、送受信し合ってしまう先程のような状態を避けるため、ここで対象アドレスを登録しておきます。同様なオプションが自動応答 ≫ オプション 765 画面にもあり、自動応答メールは、送信者毎に1日1回までと制限する事もできます。

削除
このボタンをクリックすると、除外リストで選択したエントリを削除することができます。

除外アドレスの追加 -ワイルドカード使用可
[除外アドレスの追加]テキストボックスにアドレスを入力してこのボタンをクリックすると、除外リストにそのアドレスが追加されます。

実行するプログラム

このプログラムを実行する

新規のメールが、このアカウントに届く時、実行するプログラムのパスおよびファイル名を指定するために、このフィールドを使用します。注意は、このプログラムが適切に終了し無人で実行することができる必要があります。任意のコマンドラインパラメータは、必要に応じて実行可能なパスの後に登録することができます。

メッセージを処理に渡す

このオプションを選択すると、[実行するプログラム]フィールドで指定した処理は、最初に利用できるコマンドラインパラメータとして、実行されるメッセージの名前を渡されます。自動応答が、メールを他の場所へ転送しているアカウントに設定され、そして自分のメールボックスにローカルのコピーを保持していない時は(転送 663 参照)、この機能は無効になります。

デフォルトでは、MDaemonはコマンドラインの最後のパラメータとしてメッセージファイル名を渡します。$MESSAGE$マクロを使って、この動作を変更することができます。例えば、メッセージファイル名が置かれるべき場所にこのマクロを使うとします。すると、logmail /e /j /message=$MESSAGE$ /qのような複雑なコマンドラインの使用が可能になり、より柔軟な設定ができるようになります。

メーリングリスト

次のメーリングリストへ送信者を追加

このフィールドにメーリングリストのアドレスを入力すると、メールの送信者は自動的にメーリングリストのメンバーに追加されます。これは、自動的にメーリングリストを作成する場合に非常に便利な機能です。

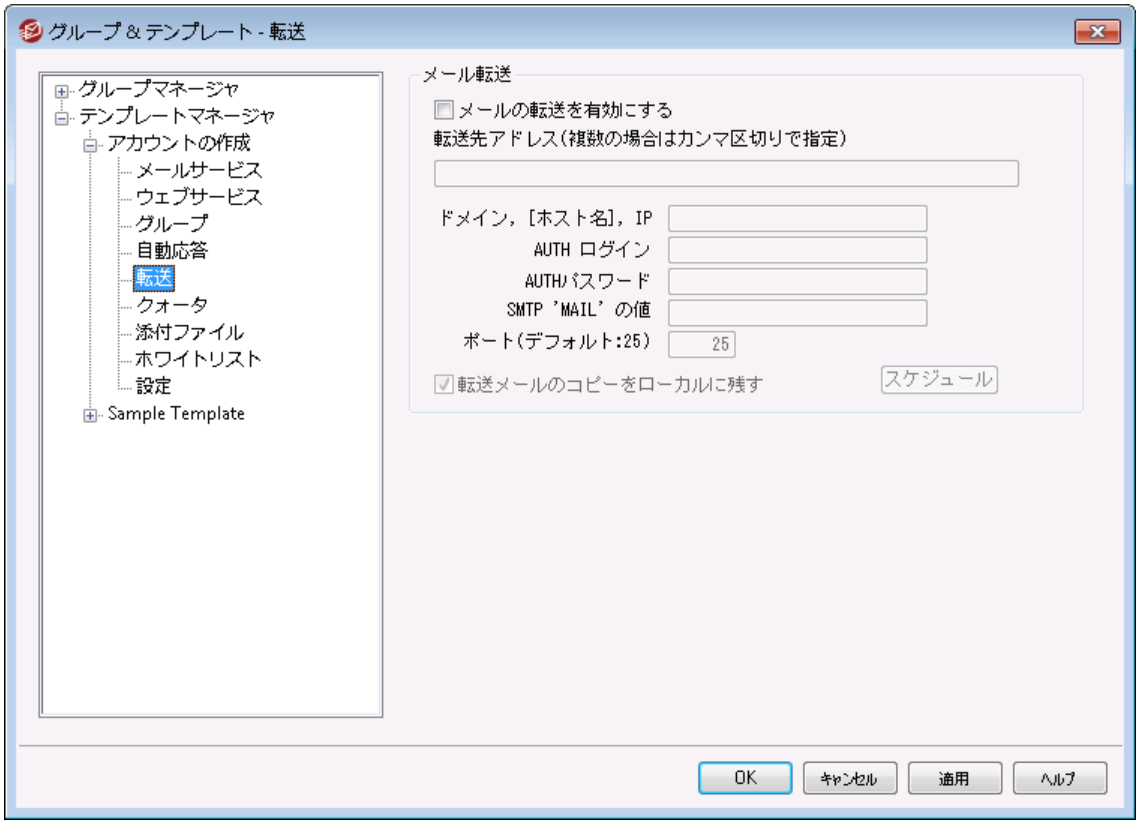
次のメーリングリストから送信者を削除

このフィールドにメーリングリストのアドレスを入力すると、メールの送信者は自動的にメーリングリストから削除されます。

参照:

テンプレートプロパティ 723
グループプロパティ 714
アカウントの作成テンプレート 722
アカウントエディタ ≫ 自動応答 660

5.2.2.1.5 転送



このテンプレート画面はアカウントエディタの転送[663]機能に対応しています。テンプレートがこのアカウント設定をコントロールする[723]と設定されていた場合、テンプレートを使用するグループ[714]に所属したアカウントのオプションはこの画面の設定でコントロールされます。

メール転送

メールの転送を有効にする
次の転送先アドレスで指定したアドレスに、メッセージを転送する場合、このチェックボックスを選択します。Webmail[291]またはRemote Administration[321]に対するWebアクセス権限[656]をもつMDaemonユーザは、管理者に設定変更を依頼するのではなく、自分自身で転送設定を行う事ができます。

転送先アドレス(複数の場合はカンマ区切りで指定)
このアカウントの受信メッセージのコピーを転送する必要あるアドレスで指定するために、このフィールドを使用します。上記のメール転送を有効にするオプションが有効の場合、受信メールのコピーが自動生成され、ここで指定されているアドレスへ転送されます。複数アドレスへの転送は、カンマ区切りで指定します。

ドメイン, [ホスト名], IP
転送メールを特定のドメインのMXサーバといった他のサーバを経由させるには、このオプションを有効にし、ここにそのドメインを入力してください。転送メールの送信に特定のホストを経由させる場合は、カギかっこでその値を入力してください。(例: [host1.example.com])

AUTHログイン/パスワード
転送に必要なログイン/パスワード認証情報を入力します。

SMTP 'MAIL'の値
アドレスをここで指定すると、受付ホストとのSMTPセッション中に、"MAIL From"ステートメントとして、実際の送信者の代わりにここで指定した値が使用されます。空のSMTP"MAIL From"ステートメント(すなわち"MAIL FROM <>")を必要とする場合、このオプションに"[trash]"を入力します。

使用するTCPポート
MDaemonは、ここで指定されるTCPポートを使用して転送されたメッセージを送信します。デフォルトSMTPポートは25です。

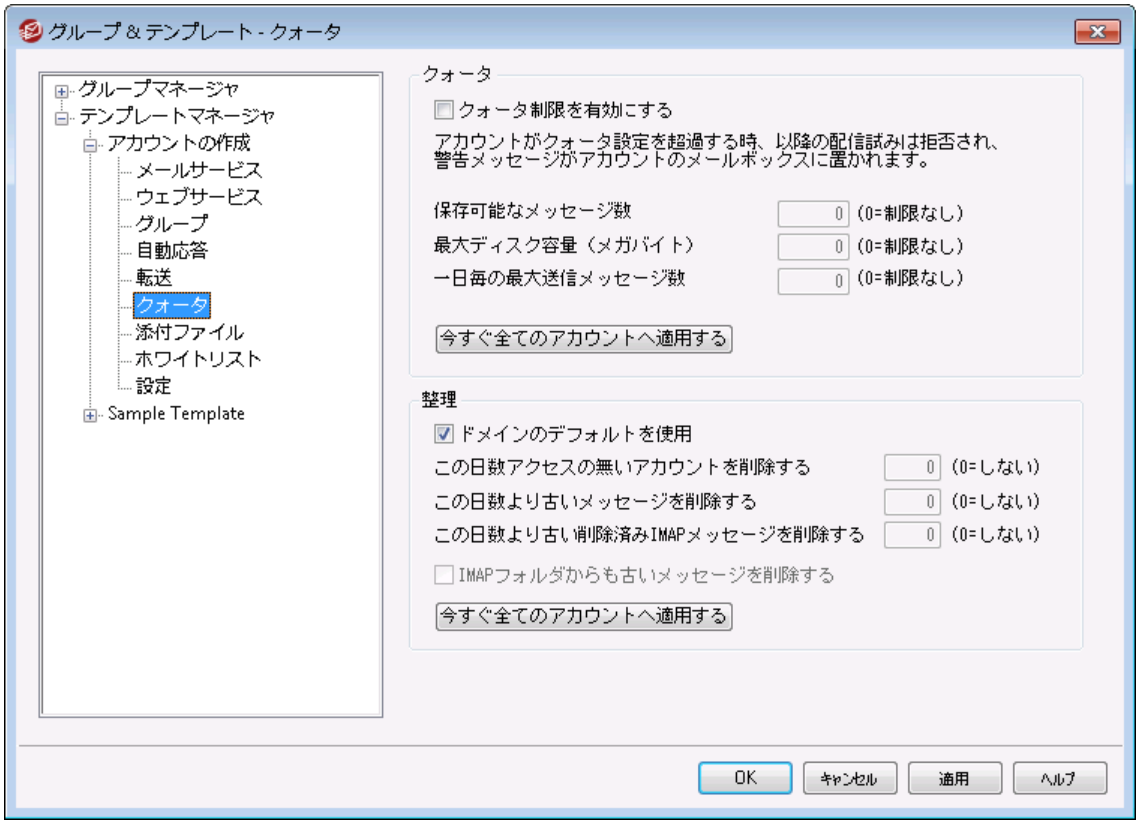
転送メールのコピーをローカルに残す
デフォルトで、転送されたメール毎のコピーは、ローカルユーザのメールボックスに通常配信されます。このチェックボックスを選択しないと、ローカルコピーは保持されません。

スケジュール
このボタンでメールの転送スケジュールを作成します。開始日時と終了日時、曜日の指定が行えます。

参照:

テンプレートプロパティ 723
グループプロパティ 714
アカウントの作成テンプレート 722
アカウントエディタ ≫ 転送 663

5.2.2.1.6 クォータ



テンプレートのこの画面はアカウントエディタのクォータ[666]機能と関連しています。テンプレートがこのアカウント設定をコントロールする[723]と設定されていた場合、テンプレートを使用するグループ[714]に所属するアカウントのクォータオプションはこの画面の設定でコントロールされます。

クォータ

クォータ制限を有効にする
アカウントで保存ができるメッセージの最大数、あるいはアカウントが使用できるディスクの最大容量（アカウントの¥Files¥フォルダにファイル添付を含む）を制限するには、このチェックボックスを選択します。アカウントに対するメール配信が試みられる場合、最大メッセージ数またはディスク容量限界を超えると、メッセージは拒否され、警告メッセージがユーザのメールボックスに設定されます。MultiPOP[673]収集がアカウントの最大を超える場合、類似した警告は発行され、アカウントのMultiPOPエントリは、自動的に切り替えられます（しかし、データベースには残ります）。

> "アカウント » アカウント設定 » クォータ[738]"の*クォータ設定値に対して次のパーセントを超えたら警告メールを送信する*オプションを使用すると、クォータ制限に近づいたアカウントに対して警告メールが送信されます。アカウントが指定した保存する最大メール数や最大ディスク容量の制限値に対して、指定したパーセンテージを超えると、深夜に対象アカウントに対する警告メールが送信されます。メールはアカウントのメール数、メールボックスのサイズ、使用済のパーセンテージと残りのパーセンテージを情報として含みます。さらに、既存の警告メールがアカウントのメールボックスに残っていた場合は、その後更新された警告メールで、既存のメールが上書きされます。

保存可能なメッセージ数
アカウントに対して保存することができるメッセージの最大数を指定するために、このオプションを使用します。オプションで0(ゼロ)をすると、メッセージ数の制限はありません。

最大ディスク容量(メガバイト)
アカウントで¥Documents¥フォルダで保存するファイル添付を含むディスク容量の最大量を指定するために、このオプションを使用します。オプションで0(ゼロ)をすると、メッセージ数の制限はありません。

一日毎の最大送信メッセージ数
アカウントが一日にSMTPを使って送信できる最大メッセージ数を指定する場合はこのオプションを使用します。この値に到達すると、深夜にカウンターがリセットされるまで、メッセージを送信する事ができなくなります。0を指定すると、アカウントが送信できるメッセージ数は無制限になります。

今すぐ全てのアカウントへ適用
このボタンで行った設定を、アカウントテンプレートでクォータ設定が行われていない全てのMDaemonアカウントへ適用します。これによりアカウントのデフォルトクォータ値は初期化されます。このオプションは新規アカウントテンプレート[722]でのみ利用できます。

整理
このセクションのオプションは、このアカウントがMDaemonによって削除される、アクティブでなくなる場合に指定するために用います。アカウントに関係ある古いメッセージが一定量の時間の後、削除されるかどうか、指定することもできます。MDaemonは毎晩深夜に、この設定で指定された期間を過ぎたすべてのメッセージとアカウントを削除、または休止状態制限に到達した場合、完全にアカウントを削除します。

ドメインデフォルトを使用
デフォルトの整理設定はドメイン毎に行い、ドメインマネージャの設定[193]画面からアクセスできます。テンプレートで管理しているアカウントに対する設定をドメインのデフォルト設定値で上書きするにはこのチェックボックスをクリアし、次のオプションで任意の値を設定してください。

次の日数非アクティブのアカウントを削除(0 = 削除しない)
このドメインに属するアカウントが指定日数の間、未使用のままである場合、このアカウントは削除されます。0(ゼロ)の値を指定すると、アカウントが使用されていなくても削除しません。

この日数より古いメールを削除(0 = 削除しない)
この値は、メッセージがMDaemonによって自動的に削除される前に、ユーザのメールボックスに残す日数を指定できます。0(ゼロ)の値を指定すると、メッセージの経過日数に関係なく削除されないことを意味します。 **注意点:** このオプションは「IMAPフォルダからも古いメッセージを削除する」オプションが有効になっていない限り、IMAPフォルダへは適用されません。

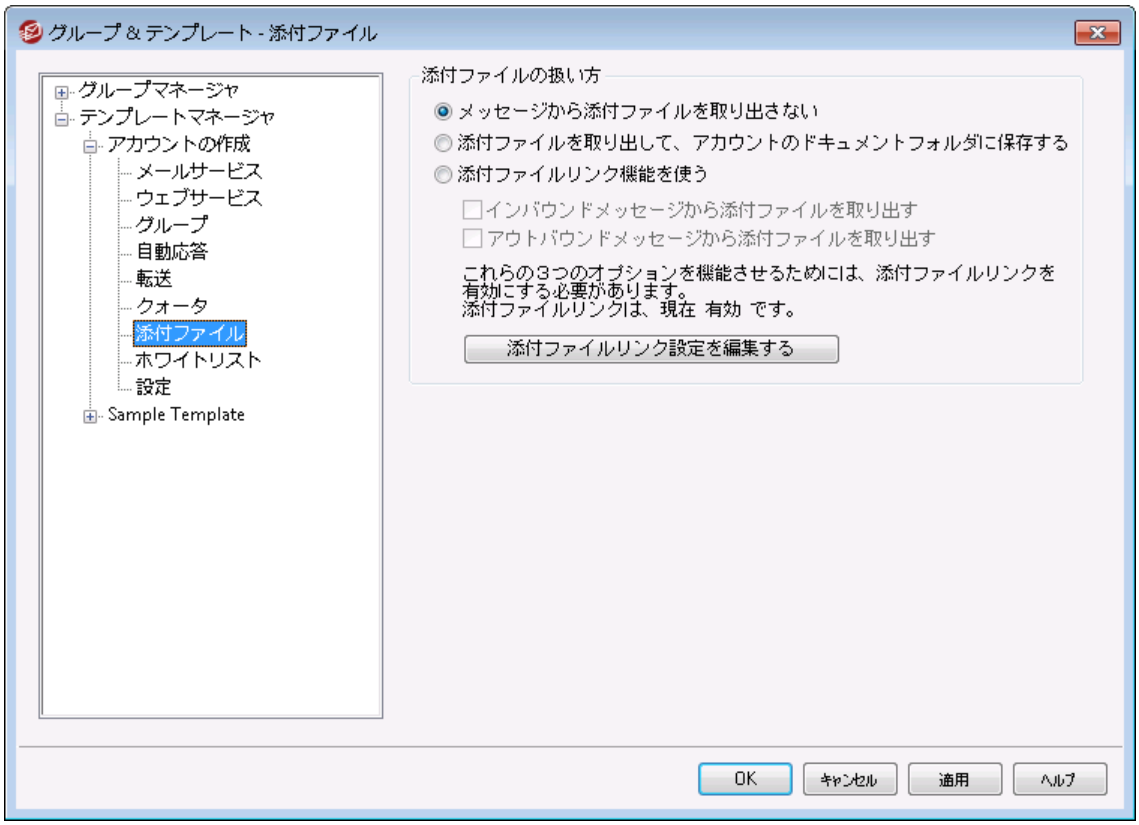
この日数よりも古い削除済IMAPメールを削除(0 = 削除しない)
このコントロールを使用して、ユーザのフォルダ内で削除のためにフラグを付けるIMAPメッセージを、何日間フォルダ内に残すかを指定してください。ここで指定された日数よりも長い期間フラグのあるメッセージは、メールボックスから削除されます。0(ゼロ)の値を指定すると、削除のためにフラグされたIMAPメッセージは古さにかかわらず、決して削除されないことを意味します。

IMAPフォルダからも古いメッセージを削除する
この日数よりも古いメールを削除を、IMAPフォルダ内のメッセージにも適用する場合は、このチェックボックスをクリックしてください。このコントロールが無効の場合は、IMAPフォルダ内のメッセージは、古さによって削除される事はありません。

参照:

テンプレートプロパティ 723
グループプロパティ 714
新規アカウントテンプレート 722
アカウントエディタ » クォータ 666
アカウント設定 » クォータ 782

5.2.2.1.7 添付ファイル



テンプレートのこの画面はアカウントエディタの添付ファイル 669 機能と関連しています。テンプレートがこの画面をコントロールする 723 と設定されていた場合、テンプレートを使用するグループ 714 に所属するアカウントの添付ファイルオプションはこの画面の設定でコントロールされます。

添付ファイル処理

メッセージから添付ファイルを取り出さない
このオプションが有効の場合、添付ファイルはテンプレートで管理しているアカウントのメールからは取り出されません。添付ファイル付のメッセージは通常のメールと同様に処理され、添付ファイルはメッセージに組み込まれたままの状態となります。

添付ファイルを取り出してアカウントのドキュメントフォルダへ保存する
設定されている場合、MDaemonはアカウント宛の受信メールへBase64 MIMEフォーマットの添付ファイルがあった場合、これを自動的に取り出します。取り出されたファイルは受信メールからは削除され、アカウントのドキュメントフォルダへ保存されます。メッセージ本文の中に、取り出されたファイル名が追加されます。このオプションでは保存された添付ファイルへのリンクを提供する事はありませんが、ユーザーはWebmail[291]からドキュメントフォルダへアクセスする事ができます。

添付ファイルリンク機能を使う
添付ファイルが付いている送受信メールに対して添付ファイルリンク機能を使用するにはこのオプションを選択します。

> このオプションが有効でも 添付ファイルリンク[333]ダイアログで添付ファイルリンク機能が無効になっていた場合、添付ファイルは取り出される事はありません。

インバウンドメッセージの添付ファイルを展開する
このオプションが有効の場合、添付ファイルは受信メールから取り出され、添付ファイルリンク[333]で指定された場所へ保存されます。メッセージ本文の中に、URLリンクが追加され、これをクリックするとファイルをダウンロードできます。セキュリティのため、URLリンクはダイレクトアクセスURLではありません。代わりにリンクには一意の識別子（GUID）が含まれていて、サーバー側で実際のファイルとリンクしています。GUIDマップは`AttachmentLinking.dat`ファイルで管理されています。このオプションはデフォルトで有効です。

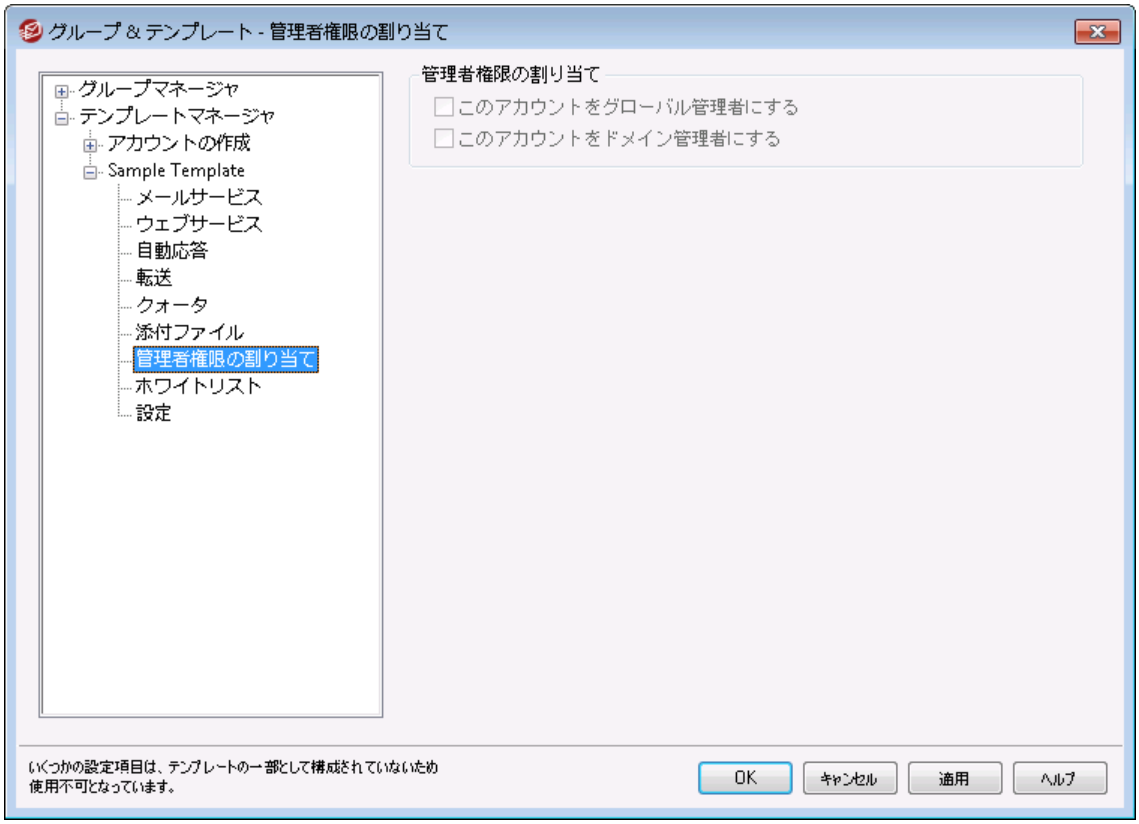
アウトバウンドメッセージの添付ファイルを展開する
このオプションを有効にすると、添付ファイルリンク機能で送信メールから添付ファイルを取り出す事ができます。アカウントがメールを送信すると、添付ファイルは取り出され、ファイルをダウンロードするためのURLが代わりに追加されます。

添付ファイルリンク設定を編集する
このボタンをクリックすると 添付ファイルリンク[333] ダイアログが起動します。

参照:

テンプレートプロパティ[723]
グループプロパティ[714]
アカウントの作成テンプレート[722]
添付ファイルリンク[653]
アカウントエディタ ≫ 添付ファイル[669]

5.2.2.1.8 管理者権限の割り当て



管理者権限の割り当て

アカウントは全体管理者です
ユーザーにサーバーレベルの管理権限を与えるにはこのオプションを有効にします。全体管理者に与えられる権限には次のものがあります:

- Remote Administration経由でのサーバー設定、全ユーザー、全ドメインへのフルアクセス権限
- MDaemonドメイン全ての全ユーザーを、インスタントメッセージの連絡先として追加する権限
- 読み取り専用のフラグが付いている場合も含め、全てのメーリングリストへ投稿する権限
- メンバーでないものも含め、全てのメーリングリストに対する投稿権限

ユーザーはMDaemonのファイルやオプション全てに対して全アクセス権を持つことになります。Remote Administrationでの管理者権限に関する詳細は、Remote Administration 321を参照してください。

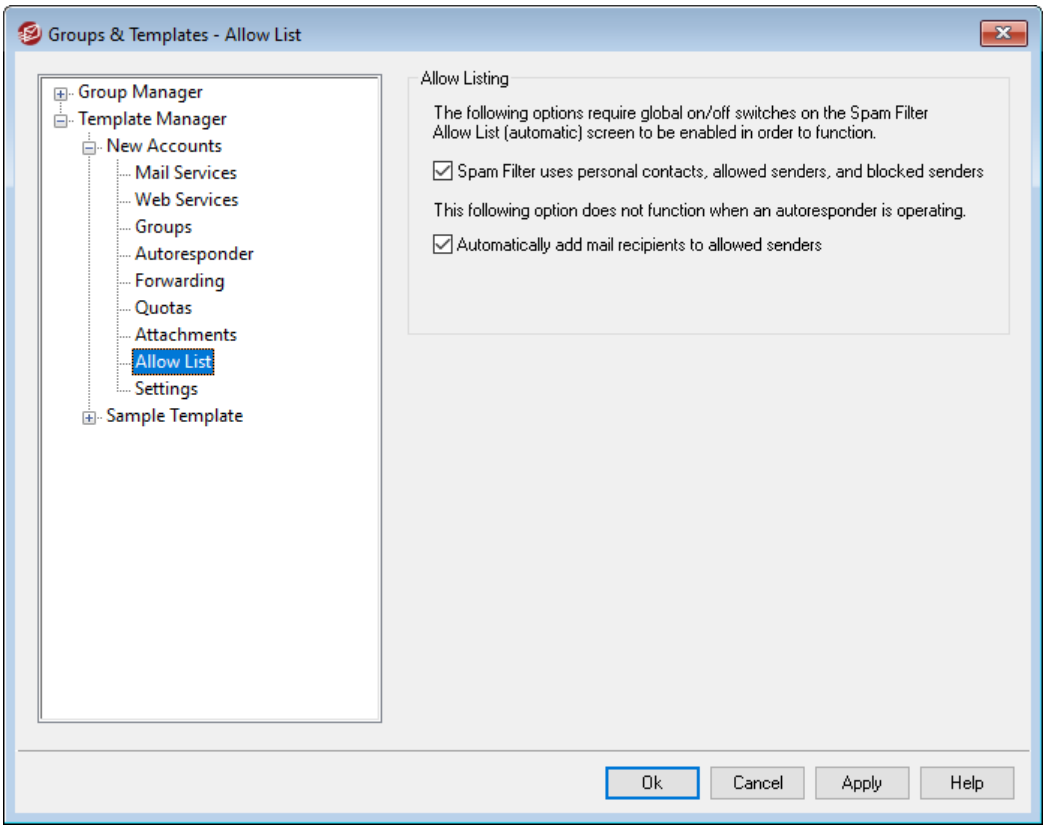
アカウントはドメイン管理者です
ユーザーをドメイン管理者として指定するにはこのチェックボックスをクリックします。ドメイン管理者は全体管理者と似ていますが、管理権限が所属ドメインであり、ウェブサービス 656ページでの権限に限定されている点が異なります。

この画面はアカウントの作成テンプレート[722]では利用できません。管理者権限を新しいアカウントへ自動で割り当てる事はできません。管理者権限をアカウントへ割り当てるためには、この画面でアクセスを許可したカスタマイズテンプレートを対象アカウントへ割り当てるか、手動でアカウントエディタの管理者権限の割り当て[690]から管理者権限を割り当てる必要があります。

参照:

テンプレートプロパティ[723]
グループプロパティ[714]
アカウントの作成テンプレート[722]
アカウントエディタ » 管理者権限の割り当て[690]

5.2.2.1.9 許可リスト



このテンプレート画面のオプションはアカウントエディタの許可リスト[691]画面へ対応しています。テンプレートがこの画面をコントロールする[723]と設定されていた場合、テンプレートを使用するグループ[714]に所属するアカウントの許可リストオプションはこの画面の設定でコントロールされます。

許可リスト

スパムフィルタは個人の連絡先、許可リスト、ブロックリストを使用
スパムフィルタの 許可リスト（自動）627 画面ではスパムフィルタでメール送信者がローカルの宛先ユーザーの個人連絡先や許可リストフォルダに含まれていた場合に、メールを自動でローカルユーザーの許可リストへ追加する全体オプションを使用できます。また、ここでは送信者が宛先ユーザーのブロックリストへ含まれていた場合に、これを自動でブロックリストとして登録する事もできます。スパムフィルタの全体オプションを有効にしていて、アカウントへこれらの設定を適用したくない場合は、このチェックボックスを無効にしてください。全体設定が無効の場合、このオプションは利用できなくなります。

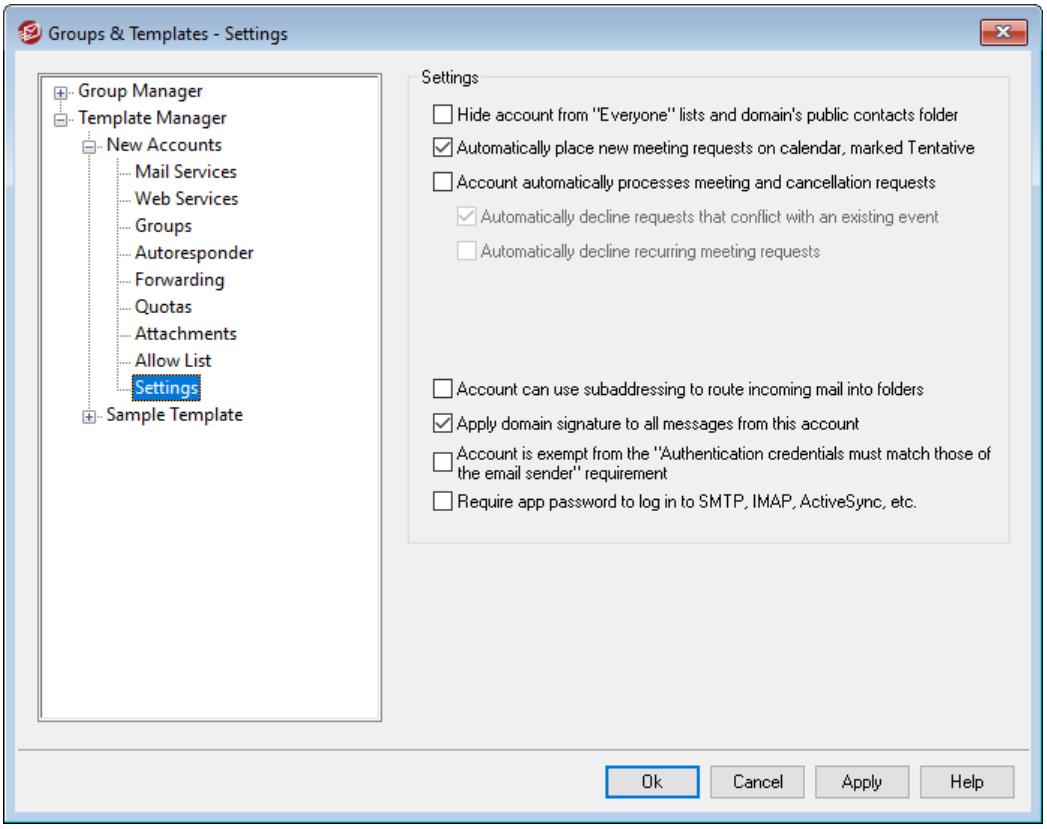
メールの宛先を許可リストへ自動追加する
ローカルではないアドレスへメール送信を行う度にアカウントの許可リストフォルダを更新するにはこのオプションを選択します。上記の、*スパムフィルタで個人連絡先、許可リスト、ブロックリストを使用*のオプションと併用する事により、スパムフィルタの誤検知は劇的に減少します。許可リスト（自動）627にある、許可リスト連絡先を自動で更新するオプションを、この機能を利用する前に有効化しておく必要があります。

このオプションは、アカウントで自動応答を使用していると無効になります。

参照:

テンプレートプロパティ 723
グループプロパティ 714
新規アカウント用テンプレート 722
アカウントエディタ ≫ 許可リスト 691

5.2.2.1.10 設定



このテンプレート画面のオプションは、アカウントエディタの設定 693 画面へ対応しています。テンプレートがこの画面をコントロールする 723 と設定されていた場合、テンプレートを使用するグループ 714 に所属するアカウント設定がこのテンプレートでコントロールされます。

設定

"Everyone"メーリングリスト、共有予定表、VRFYコマンドからアカウントを隠す
MDaemonは各ドメイン用に、メンバー全員を含む"everyone@ "メーリングリストを自動で作成、管理します。デフォルトで、MDaemonは、全てのアカウントを含むこのリストを自動生成します。このアカウントをリストから除外する場合、このチェックボックスをクリックします。アカウントは、共有予定表の表示やVRFY 82 結果から外されます。

自動的に会議リクエストを予定としてカレンダーへ追加する
デフォルトで、新しく会議のリクエストを受け取ると、会議はユーザーの予定表へ、予定ありとして自動追加されます。デフォルト設定を新しいアカウントで有効化したくない場合は、この設定を無効にして下さい。

自動的に会議招集とキャンセルの処理を受けつける
ミーティング要求や変更、キャンセル処理を自動的にする場合は、このオプションを選択します。ミーティング要求を受信するとカレンダーが自動的に更新されます。

既存のイベントと競合するリクエストは自動的に拒否する
会議招集とキャンセル処理を自動処理する設定になっている場合に、既存のイベントと競合する会議の招集があった際、自動で拒否するオプションです。競合するイベントも自動で受け付ける場合はこのオプションを外して下さい。

繰返し予定の要求を拒否する
会議招集とキャンセル処理を自動処理する設定になっている場合で、繰返しイベントの場合にのみ拒否したい場合はこのチェックボックスをクリックします。

受信メールを対応するメールフォルダへ届けるサブアドレス機能の使用を許可する
サブアドレス[694]の利用を許可する場合はこのオプションをクリックして下さい。

このアカウントからのメールへドメイン署名を適用する
アカウントが所属するドメインのドメイン署名[184]が設定されていると、このオプションでユーザーからの全てのメールへ追加されます。

アカウントを「認証情報はメール送信者と一致」要件から除外する
SMTP認証[476]の「認証情報はメール送信者と一致」オプションからアカウントを除外するにはこのオプションを使用します。

SMTP, IMAP, ActiveSync等へのログインにAppパスワードを必須とする
このテンプレートを使用しているアカウントがSMTP, IMAP, ActiveSync, それ以外のメールサービスへのログインを行うのに、メーラー側でAppパスワード[683]を必須とする場合はこのオプションをクリックします。アカウントの通常のは、WebmailやRemote Adminへのログインにパスワード[778]は必要です。

Appパスワードを必須にする事で、アカウントのパスワードを、SMTPやIMAP等での辞書攻撃やブルートフォース攻撃から保護する事ができます。Appパスワードは、例えばパスワードが漏えいしてしまった場合でも、本来のパスワードではなく、MDaemonは正しいAppパスワードのみを受け付けるため、パスワードを取得した攻撃者はこれが本来のパスワードでない事を確認できません。更に、MDaemonアカウントがActive Directory認証を使用しており、Active Directoryがパスワードの連続失敗によりアカウントをロックしたとしても、このオプションを使う事でMDaemonからロックされる事がなくなります。MDaemonはAppパスワードのみで認証を行い、ActiveDirectoryへの問合せを行う事がないためです。

参照:

テンプレートプロパティ[723]
グループプロパティ[714]
新規アカウントテンプレート[722]
アカウントエディタ » 設定[693]

5.3 アカウント設定

5.3.1 Active Directory

アカウント » アカウント設定 » Active Directoryにあるオプションを使って、MDaemonは、Active Directoryを監視し、関連付けられたMDaemonアカウントの作成や編集、削除、無効といった処理を自動で行う事ができます。更に、パブリック連絡先情報は最新のActive Directoryへ保存された情報を元に更新されます。Active Directoryで変更されたアカウントの住所や電話番号、連絡先情報などのフィールドは、パブリック連絡先として更新され保持されます。

アカウント作成

Active Directoryを監視するように設定すると、MDaemonは指定された間隔でActive Directoryの変更をチェックし、新規のActive Directoryアカウントが作成されると同時に、MDaemonにも新しいアカウントを作成します。このMDaemonで作成される新しいアカウントには、Active Directoryでのフルネーム、ログオン、メールボックス、説明、有効/無効などの設定がそのまま引き継がれます。

デフォルトでは、Active Directoryの監視により作成された新しいMDaemonアカウントは、MDaemonのデフォルトドメインに追加されます。あるいは、"UserPrincipalName"というActive Directory属性に含まれるドメインに追加することも可能です。このオプションを使用する場合、アカウントがまだMDaemonに存在しないドメインを要求した場合、自動的に新しい ドメイン 165 が作成されます。

Active Directoryのグループを*検索フィルタ* 749 で監視する事もでき、グループへ追加されたユーザーやユーザーに関連付けられたグループがあった場合、MDaemonでは新規ユーザーを作成します。グループからユーザーを削除した場合は、MDaemon上で対象アカウントを(削除ではなく)無効化します。

アカウント削除

Active Directoryからアカウントが削除された場合、以下のアクションを行うようにMDaemonを設定することができます。[何もしない]、[関連するMDaemonアカウントを削除する]、[関連するMDaemonアカウントを無効にする]、[関連するMDaemonアカウントをフリーズする(アカウントでのメールの受信は行われるが、ユーザは収集とアクセスができない)]。

アカウント更新

MDaemonがActive Directoryアカウントでの変更を検知すると、それに関連するMDaemonアカウントのプロパティは自動的に更新されます。

Active DirectoryでのMDaemonとの同期

「すぐに完全なAD同期を実行」オプションを使って、MDaemonにActive Directoryのデータベースをチェックさせ、すぐに変更を同期させる事ができます。その後Active Directoryアカウントに加えられる変更は、自動的にMDaemonアカウントに反映されます。

Active Directory認証

MDaemonのActive Directory機能によって作成されたアカウントは、デフォルトでActive Directory (AD)認証を使用します。Active Directory認証を利用すると、MDaemonがアカウントのパスワードを自身のデータベースに持つ必要がなくなります。代わりに、アカウント所有者は自分のWindowsログイン/パスワード証明書を使用し、MDaemonは関連したアカウントの認証をWindowsに渡します。

Active Directory認証を使用するには、Windowsのドメインが、モニタリング 752 されている必要があります。このドメインはMDaemonがアカウントの認証を行う際に使用するWindowsドメインです。多くの場合MDaemonは自動的にこのWindowsドメインを検索し設定します。しかしながら、ここでは異なるドメインや、特定のドメインに制限するのではなくすべてのWindowsドメインを横断的に認証させ

る"NT_ANY"を設定する事もできます。ここを空白にすると、MDaemonは新しく作成されたアカウントに対してAD認証を行いません。その代わり、ランダムなパスワードが生成され、メールアカウントにアクセスする前に手動でそのパスワードを編集する必要があります。

継続的なモニタリング

Active DirectoryのモニタリングはMDaemonが終了しても継続されます。Active Directoryでのすべての変更は追跡され、MDaemonが再起動した際に処理されます。

Active Directoryのファイルセキュリティ

大きな特徴としてMDaemonのActive Directory機能は、Active Directoryスキーマファイルへ影響を与えません。すべてのモニタリングはActive DirectoryからMDaemonへの一方通行です。MDaemonがディレクトリに変更を加えることはありません。

Active Directoryのテンプレート

Active Directoryの変更によりMDaemonが関連するアカウントの追加や修正を行う際には、Active Directoryテンプレート("/app/ActiveDS.dat")が使用されます。これによりMDaemonのアカウントにActive Directoryの属性がリンクされます。例えば、デフォルトではActive Directoryの"cn"という属性とMDaemonの"FullName"フィールドがリンクされています。しかしこれらのリンクはハードコードされたものではありません。テンプレートはテキストエディタなどで簡単に編集することができ、フィールドの配置も変更することができます。例えば、"FullName=%givenName% %sn%"はデフォルト設定の[FullName=%cn%]の代わりとして使用することができます。詳細に関してはActiveDS.datを参照してください。

パブリックアドレス帳の更新

Active Directoryモニタリングは Active Directoryを定期的に確認し、全てのパブリック連絡先を最新の状態に保持するのにも使用できます。アカウントの郵便番号や電話番号、会社の連絡先などの一般的なフィールドはパブリック連絡先に生成され、データはActive Directory上で変更が発生する度に更新されます。この機能を有効にする場合は、Active Directory » モニタリング[752]にある"*Active Directoryを監視し、パブリックアドレス帳を更新する*"を使用して下さい。

この機能により、数々の連絡先情報が監視できます。パブリックアドレス帳フィールドの全部は、ActiveDS.DAT内のActive Directoryの属性に関連付けされます。このファイルにはいくつかの新しいマッピングテンプレートが含まれており、特定の連絡先フィールドとActive Directory属性を紐づけるのに使用できます。(例えば `%fullName%` をフルネームフィールド、`%streetAddress%` を番地、といった形です。)

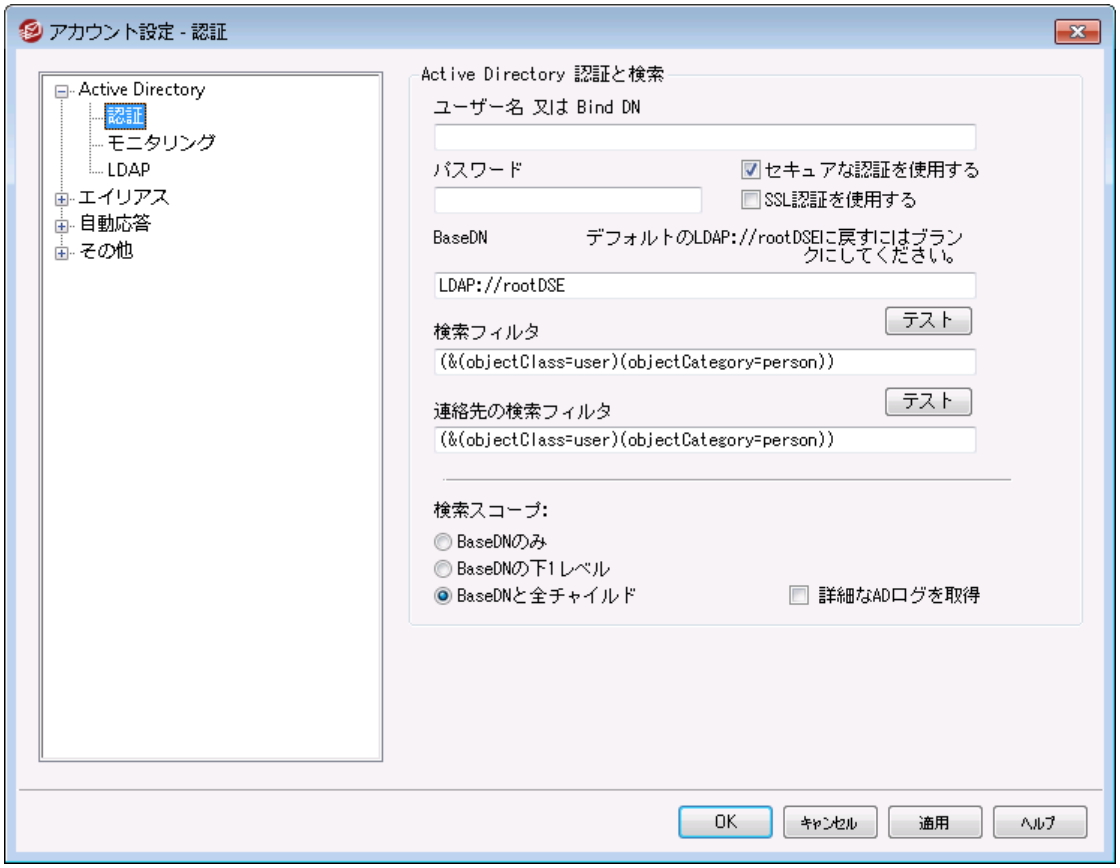
MDaemonはアカウントの特定を行うため、メールアドレスとActive Directory属性とを紐づける必要があります。関連付けされていない場合は、何も行いません。デフォルトで、MDaemonはメールアドレスを、MDaemonが内部でもつデフォルトドメイン[165]用の(ActiveDS.datで定義された)メールボックステンプレートと関連付けしています。`ActiveDS.dat` の中の"abMappingEmail"のコメントを外し、(例えば%mail%などの)属性とActive Directory属性を関連付けすることもできます。ただし、この値は、ローカルユーザーアカウントとして認識させるために、メールアドレスを含んでいなくてはならない点を注意して下さい。

この機能は存在していない場合は連絡先情報を生成し、存在している場合は既存の連絡先情報をアップデートします。更に、この機能はActive Directory以外で行った変更を上書きしてしまう点を注意して下さい。関連付けされていない連絡先情報はそのまま残されます。最後に、MDaemonアカウントで非表示[693]として設定されていない連絡先情報は作成又はアップデートされます。

参照:

Active Directory ≫ モニタリング 752
Active Directory ≫ 認証 749

5.3.1.1 認証



全ての設定を正しく機能させるためには Active Directory へ特殊なアクセス権が必要となる場合があります。

Active Directory 認証と検索

ユーザー名 又は Bind DN
ログオン用の Windows アカウントか、MDaemon が LDAP で Active Directory をバインドする際に使用する DN です。Active Directory はバインド時 Windows アカウントか UPN の使用を許可しています。

Windowsログインではなく DNを使用する場合は、後述の「セキュアな認証を使用する」オプションを無効化する必要があります。

パスワード
上記のBind DNオプションで使用するDNやWindowsログインに対応したパスワードを指定します。

セキュアな認証を使用する
Active Directory検索の際セキュアな認証を使用するにはこのオプションを有効にします。上記のBind DNでWindowsログオンではなくDNを使用している場合、このオプションは利用できません。

SSL認証を使用する
Active Directory検索の際SSL認証を使用するにはこのオプションを有効にします。

このオプションを使用するにはWindowsネットワークやActive Directory環境へSSLサーバーとその基盤が必要となります。ネットワークでSSLが利用可能かどうか不明な場合や、このオプションを利用可能かどうか判断できない場合は、IT管理者へ確認して下さい。

Active Directory検索

Base DN
これはMDaemonがActive Directoryアカウントや変更点を検索する際のディレクトリインフォメーションツリー(Directory Information Tree =DIT)の開始点、あるいは識別名(Distinguished Name =DN)です。デフォルトでは、MDaemonはRoot DSE(Active Directory階層の最上段)から検索を開始します。Active Directory内でよりユーザアカウントに近い場所を開始点に選ぶことにより、DITの検索やアカウントの変更に費やす時間を短縮することができます。このフィールドをブランクにしておくと、デフォルト値であるLDAP://rootDSEが復元されます。

検索フィルタ
アカウントやアカウント変更用に、Active Directoryのモニタリングや検索で使用するLDAP検索フィルタです。このフィルタを使用することにより、Active Directoryのモニタリングの対象とするユーザアカウントをより正確に絞り込む事ができます。

Active Directoryのグループを検索フィルタで監視する事もでき、グループへ追加されたユーザーやユーザーに関連付けられたグループがあった場合、MDaemonでは新規ユーザーを作成します。グループからユーザーを削除した場合は、MDaemon上で対象アカウントを(削除ではなく)無効化します。例えば、'MyGroup'というグループ用の検索フィルタは次のようになります:

```
(|(&(ObjectClass=group)(cn=MyGroup))(&(objectClass=user)
(objectCategory=person)
(memberof=cn=MyGroup,ou=me,dc=domain,dc=com)))
```

'ou='や'dc='の値は実際のネットワークに合わせて変更してください。

連絡先検索フィルタ
連絡先検索に異なる検索フィルタを使用するにはこのオプションを使用します。上記の検索フィルタオプションと同じテキストをこのフィールドに使用すると、1つのクエリのみで全てのデータをアップデートします。検索フィルタが異なる場合、2つの異なるクエリが必要です。

テスト
このボタンをクリックすると検索フィルタ設定をテストできます。

検索スコープ:

Active Directoryを検索する際の検索範囲です。

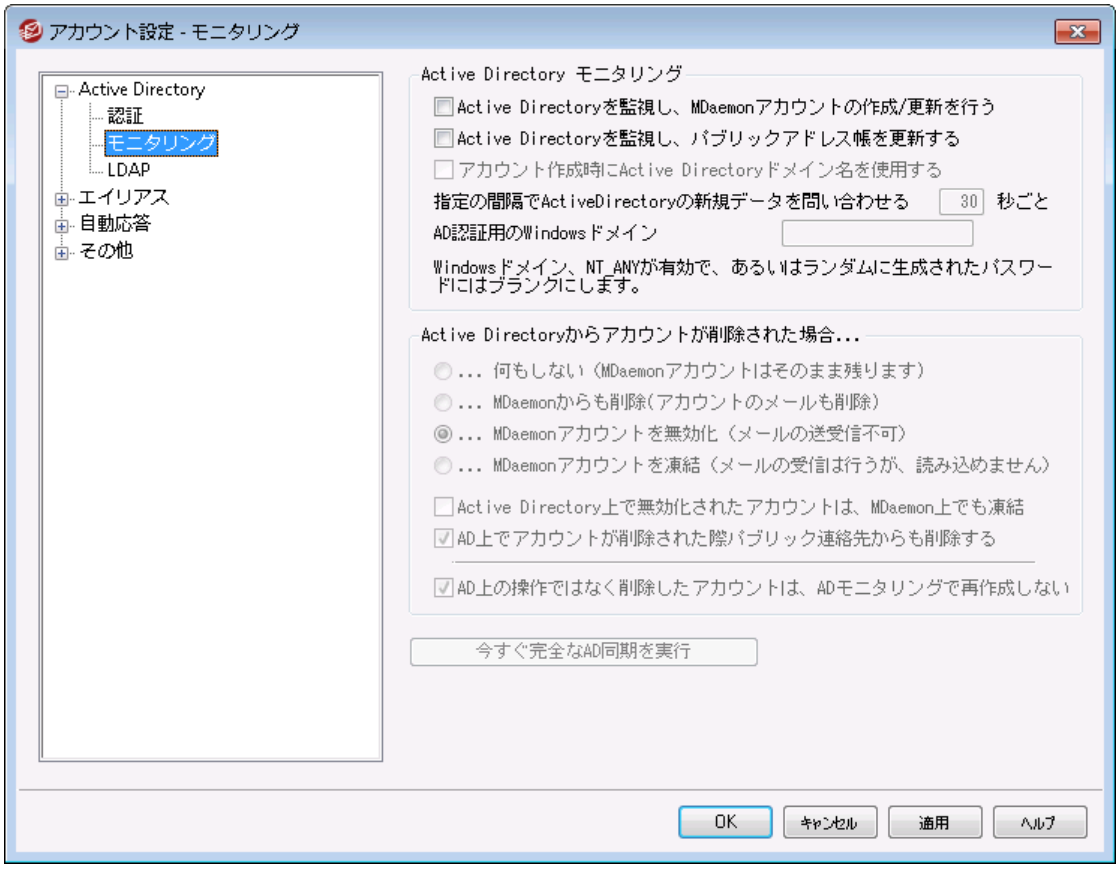
ベースDNのみ
上記のベースDNだけに検索範囲を指定する場合、このオプションを選びます。検索は、ツリー(DIT)でそのポイントより下に進みません。

ベースDNの下1レベル
DIT内の指定されたDNの1レベル下までActive Directory検索範囲を広げる場合、このオプションを使用します。

ベースDNとすべてのチャイルド
このオプションは検索範囲を提供されたDNから最下層のチャイルドエントリまでとします。これは上記のデフォルトRoot DSEと組み合わせるデフォルトオプションで、Root DSE以下の全てのDITが検索対象となります。

詳細なADのログを取得
デフォルトで、MDaemonはActive Directoryに対して詳細なロギングを使用します。通常のADロギングを使用する場合、このチェックボックスを解除します。

5.3.1.2 モニタリング



Active Directoryモニタリング

Active Directoryを監視し、MDaemonアカウントの作成/更新を行う
Active Directoryを監視し、Active Directoryが更新された際MDaemonアカウントの作成や更新を行うには、このオプションをクリックします。

Active Directoryを監視し、パブリックアドレス帳を更新する
Active Directory内の最新情報を元に全てのパブリック連絡先レコードを最新の状態にしておくにはこのオプションを使用します。一般的なフィールドである郵便番号、住所、電話番号、仕事の連絡先情報などはパブリック連絡先レコードとして取り込まれ、Active Directory上で更新される毎にアップデートされます。この方法で数多くの連絡先フィールドを監視する事ができます。Active Directory属性と関連付けられたパブリック連絡先情報のフィールド情報は、ActiveDS.datファイルで確認できます。より詳細な情報は、パブリックアドレス帳の更新 748を参照して下さい。

アカウント作成時にActive Directoryのドメイン名を使用する
Active Directoryのモニタリングの結果として作成された新しいアカウントを、"UserPrincipalName"というActive Directory属性に含まれるドメインに追加する場合は、このオプションを使用します。このオプションを使用する場合、アカウントがMDaemonに存在しないドメインを要求した場合、自動的に新しいドメイン 165が作成されます。新しいアカウントをMDaemonのデフォルトドメイン 165に追加する場合は、このオプションを解除してください。

指定間隔で新規データをActive Directoryに対し問い合わせる [XX] 秒ごと
MDaemonがActive Directoryの変化をモニタする間隔を秒数で指定します。

AD認証用のWindowsドメイン
Active Directoryモニタリングで作成したアカウントのユーザー認証にAD認証を使用する場合、ここでWindowsドメイン名を指定します。このフィールドをブランクにすると、ランダムに生成されたパスワードが割り当てられ、メールアカウントにアクセスするためには手動でそのパスワードを編集する必要があります。

Active Directoryでアカウントが削除された場合:
MDaemonアカウントに関連したActive Directoryアカウントが削除された場合のアクションを以下の選択肢から1つ選びます。

...何もしない
Active Directoryからアカウントが削除されても、その変更をMDaemonに反映しない場合は、このオプションを選択してください。

...MDaemonからも削除(アカウントのメールも削除)
Active Directoryアカウントが削除されると同時にMDaemonアカウントも削除する場合は、このオプションを選択してください。

MDaemonのアカウントは完全に削除されます。アカウントに関連したメッセージ、フォルダ、アドレス帳、カレンダーなどもすべて削除されてしまいますので注意してください。

...アカウントを無効化(メールの送受信不可)
Active Directoryアカウントが削除されると同時にMDaemonアカウントを無効にする場合は、このオプションを選択してください。この場合、MDaemonアカウントはサーバから削除されませんが、メールの送受信やアカウントへのアクセスができなくなります。

...アカウントを凍結(受信はできるが収集不可)
このオプションでは、そのアカウントへのメールは受信されますが、アカウントは完全にロックされアクセスすることができなくなります。例えば、このアカウントへのメールは送信者に戻されたりMDaemonによって削除されたりすることはありませんが、アカウントの使用者は(そのアカウントが凍結されている間は)、メールにアクセスすることができません。

Active Directory上で無効化されたアカウントはMDaemonでも凍結する
デフォルトでは、Active Directoryアカウントが無効になると、MDaemonも関連アカウントを無効にします。この場合、アカウントにアクセスすることができず、メールの送受信もできなくなります。しかし、アカウントを無効にする代わりに凍結する場合は、このオプションを選択します。MDaemonでは、凍結したアカウント宛てのメールはこれまで通り受け入れますが、ユーザーはメールの収集や送信のためにアクセスすることができません。

AD上でアカウントが削除された際パブリック連絡先からも削除する
デフォルトで、対応するアカウントがActive Directoryから削除されると、パブリック連絡先からも対象のアカウントは削除されます。ただし、連絡先は元々このアカウントがActive Directory連携機能で作成[748]された場合のみ削除されます。対応するアカウントがActive Directoryから削除されてもパブリック連絡先からは削除したくない場合はこのオプションを無効化してください。

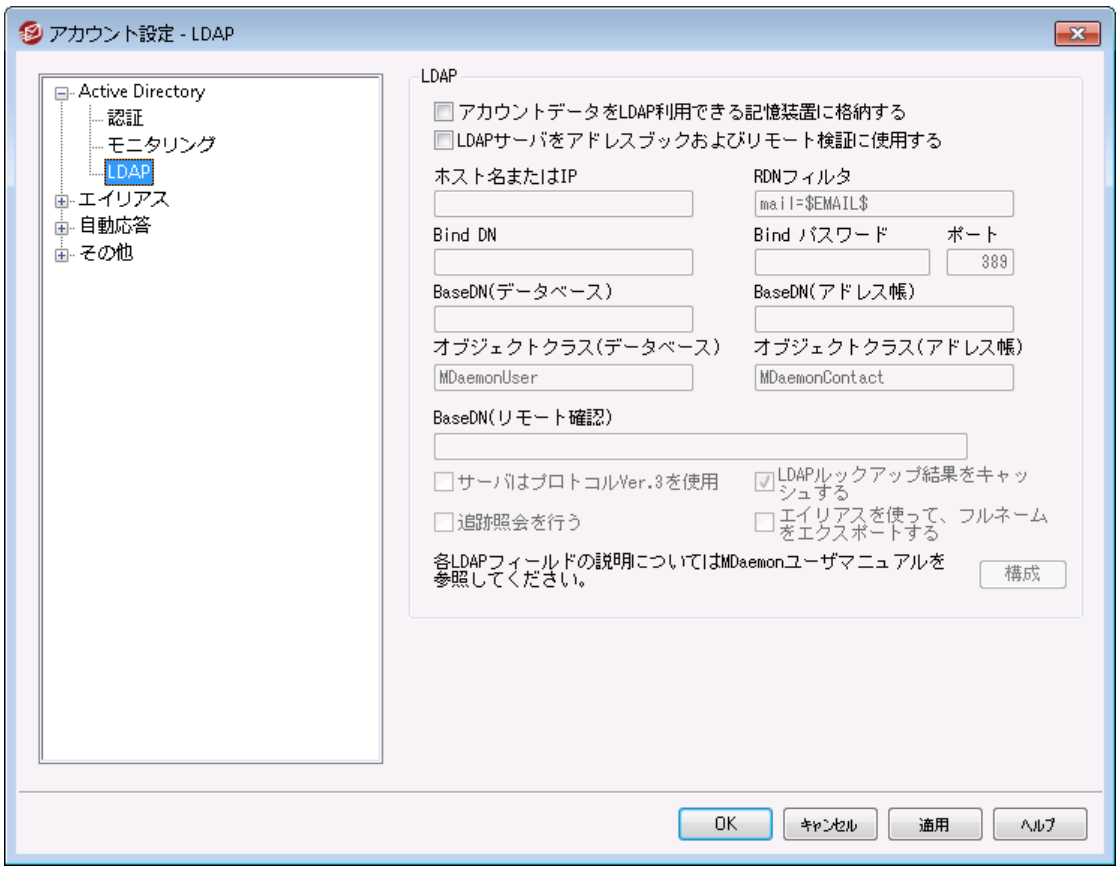
AD上の操作ではなく削除したアカウントはADモニタリングで再作成しない
（MDaemon管理画面から手動で削除した場合など）Active Directory以外でMDaemonをアカウントを削除すると、デフォルトでアカウントは今後のActive Directoryモニタリングで再作成される事はありません。アカウントを再作成したい場合はこのオプションを無効化してください。

すぐに完全なActive Directory同期を実行
このボタンをクリックすると、MDaemonはActive Directoryデータベースをチェックして、必要に応じてMDaemonアカウントを作成、編集、削除します。すでにMDaemonに存在するアカウントがActive Directoryアカウントと一致した場合、それらはリンクされます。

参照:

Active Directory 747
Active Directory ≫ 認証 749

5.3.1.3 LDAP



MDaemonはLightweight Directory Access Protocol (LDAP)に対応しています。「アカウント ≫ アカウント設定 ≫ LDAP」からLDAPの設定画面へアクセスする事ができ、ここからMDaemonがLDAPサーバー間とでユーザーアカウント全てを同期するよう設定する事ができます。MDaemonはMDaemonアカウントが追加や削除される度にLDAPサーバーと通信し、LDAPユーザーデータベースを正確に、継続的に管理する事ができます。これによりメールの利用ユーザーはLDAPを共有の全体アドレス帳として使用できるようになり、全てのMDaemonユーザーの情報も、連絡先と併せて格納されるようになります。

また、LDAPサーバーを、ローカルのUSERLIST.DATやODBC互換のデータベースに代わってMDaemonユーザーデータベース[771]として利用する事もできます。複数のMDaemonサーバーを異なる場所に所有しており、それらのユーザー情報を一元管理する際などにも、この方法が便利です。各MDaemonサーバーはローカルでユーザー情報を管理するのではなく、1つの同じLDAPサーバーへ接続するよう設定しておきます。

LDAP

アカウントデータをLDAPがアクセスできる記憶域に格納する
ローカルのUSERLIST.DATシステムや、ODBCではなく、LDAPサーバをMDaemonのユーザデータベースとして使用する場合は、このチェックボックスをクリックしてください。異なった場所に複数のMDaemonサーバが存在しており、それらサーバー間で1つのユーザデータベースを共有する場合には、この方法でユーザ情報を管理できます。それぞれのMDaemonサーバは、ユーザ情報を個々に管理するのではなく全体で共有するよう、同じLDAPサーバに接続するよう構成して下さい。

LDAPサーバをアドレスブック及びリモート認証のために使用する
アカウントデータベースの管理に、LDAPサーバではなくUSERLIST.DATやODBCを使用する場合であっても、このチェックボックスを有効にすることで、すべてのユーザ名、メールアドレス、およびエイリアスをLDAPサーバ上でも更新し続けることができます。これで、LDAPアドレス帳に対応しているメーラーは、LDAPを全体的なアドレス帳として使用することができます。

この機能によって、リモートのバックアップサーバからのアドレス情報確認や認証用に、メールボックス、エイリアス、メーリングリストのデータベースを最新に保つ事ができます。より詳しい情報は以下の[ベースエントリDN(リモート確認)]を参照してください。

LDAPサーバプロパティ

ホスト名またはIP
LDAPサーバのホスト名かIPアドレスを入力してください。

RDNフィルタ
このコントロールは、各ユーザのLDAPエントリ用のRDN(relative distinguished name)を生成するために使用されます。RDN(relative distinguished name=相対的な識別名)は各エントリのDN(distinguished name=識別名)中の左端のコンポーネントです。すべてのピアエントリ(共通の直近の親を共有する仲間)に対して、RDNは一意でなければなりません。したがって、起こり得る競合を避けるために、それらのRDNとして、各ユーザのメールアドレスを使用することをお勧めします。各ユーザのLDAPエントリが作られる際、このコントロール(例えば、mail=$EMAIL$)の中で、属性の値として$EMAIL$マクロを使用すると、それはユーザのメールアドレスと置き換えられます。ユーザのDNは、RDNとベースエントリDNから構成されます。

BindDN
MDaemonが、ユーザのエントリを追加や変更できるように、LDAPサーバへの管理上のアクセス権を与えたいエントリのDNを入力してください。これはバインド操作の認証のために使用されるDNです。

Bindパスワード
このパスワードは、認証用にBind DNと併せて渡される値です。

ポート
LDAPサーバがモニタしているポートを指定してください。MDaemonは、LDAPサーバにアカウント情報を投稿する際このポートを使用します。

ベースエントリDN（データベース）
USERLIST.DATファイルではなくLDAPサーバをユーザデータベースとして使用する際には、MDaemonのすべてのユーザエントリで使用されるBaseエントリ（ルートDN）を入力してください。ベースエントリDNは、各ユーザの識別名（DN）を生成するためRDN（RDNフィルタを参照）に結合されます。

ベースエントリDN（アドレス帳）
LDAPデータベースのアドレス帳とアカウント情報を同期する際には、MDaemonユーザのすべてのアドレス帳エントリで使用されるベースエントリ（ルートDN）を入力してください。ベースエントリDNは、各ユーザの識別名（DN）を構築するためにRDN（RDNフィルタを参照）に結合されます。

オブジェクトクラス(データベース)
MDaemonの各ユーザのユーザデータベースエントリが属するオブジェクトクラスを指定してください。各エントリはその値として[objectclass=]という属性を含みます。

オブジェクトクラス(アドレス帳)
MDaemonの各ユーザのLDAPアドレス帳のエントリが属するオブジェクトクラスを指定してください。各エントリはその値として[objectclass=]という属性を含みます。

ベースエントリDN（リモート確認）

ドメインゲートウェイとバックアップサーバの一般的な問題として、到着するメッセージの受信者が有効なものかどうかを判断できる手段がない点が挙げられます。例えば、example.comのuser1@example.comにメッセージが到達した場合、バックアップサーバはメールボックス、エイリアス、あるいはメーリングリストがexample.comの[user1]として実際に存在するものか判断する手段を持ちません。このように通常バックアップサーバは、すべてのメッセージを受け入れるしか方法がありません。MDaemonは、これらのアドレスを照合して、この問題を解決する方法があります。すべてのメールボックス、エイリアス、メーリングリストに使用されるベースエントリDNを指定することにより、LDAPサーバはこれらの情報を最新の状態に保つことができます。これにより、バックアップサーバは指定されたドメインにメッセージが受信されるたびにLDAPサーバに問い合わせを行い、その受信者のアドレスが

サーバーはプロトコルVer. 3を使用
MDaemonがサーバー間とLDAPプロトコルVer.3を使うようにするには、このチェックボックスをクリックします。

追跡照会を行う
LDAPサーバーでは、要求されたオブジェクトを所持してはいないものの、クライアントから参照できるオブジェクトを管理している場合があります。MDaemonにこのような参照情報を追跡させたい場合は、このオプションを有効にして下さい。このオプションはデフォルトで無効になっています。

LDAPルックアップ結果をキャッシュする
デフォルトでMDaemonはLDAPルックカップ結果をキャッシュしています。キャッシュを行いたくない場合はこのオプションを無効化して下さい。

エイリアスを使ってフルネームをエクスポートする
LDAPのアドレス帳へエクスポートしたエイリアス以外のアドレスはCNフィールドへ姓名が挿入されます。ただし、エイリアスの場合、ここへ(エイリアスではなく)本当のメールアドレスが挿入されます。ここで、本当のメールアドレスではなく、姓名を挿入するにはこのチェックボックスを有効にして下さい。このオプションはデフォルトで無効になっています。

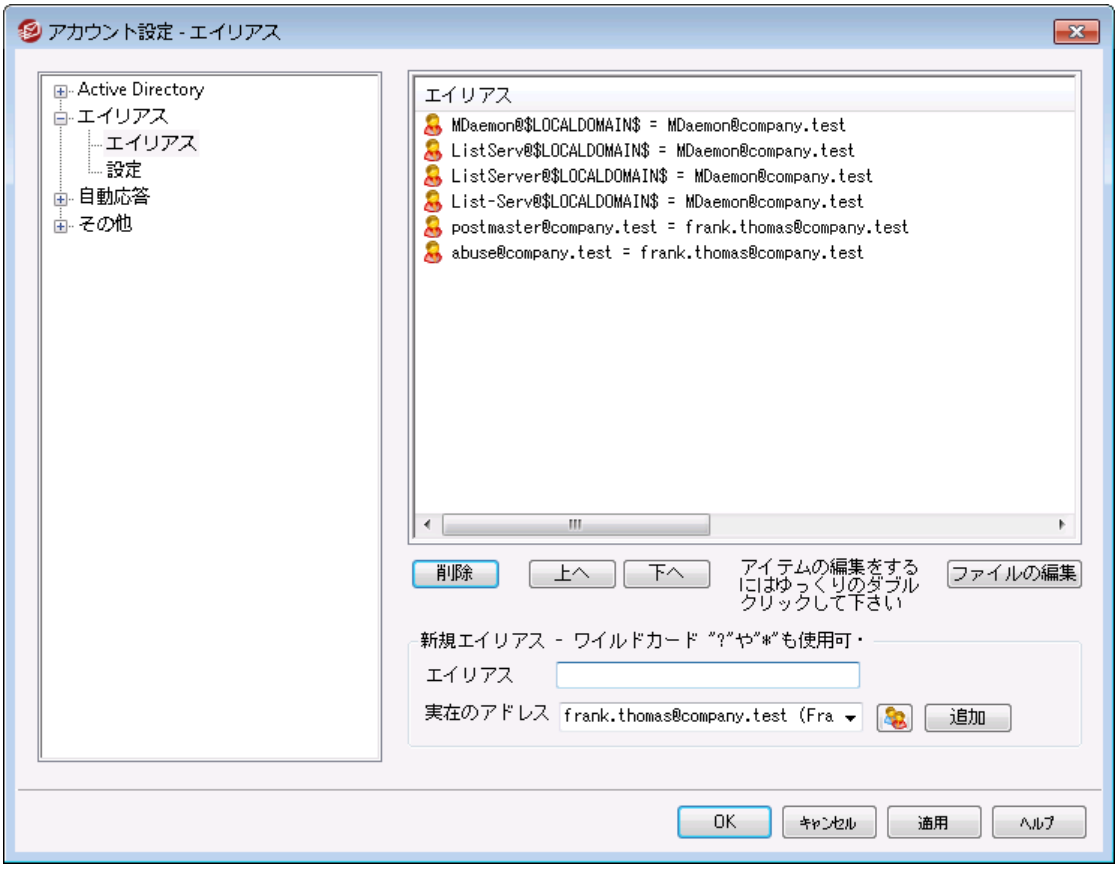
構成
このボタンをクリックして、テキストエディタでLDAP.dat構成ファイルを開いてください。それぞれのMDaemonのアカウントフィールドに対応するLDAPの属性名を指定することができます。

参照:

アカウントデータベースオプション 771

5.3.2 エイリアス

5.3.2.1 エイリアス



エイリアス機能を使うと、アカウントやメーリングリスト用に、代替メールボックス名を作成することができ、複数のメールボックス名を1つのユーザアカウントやリストで使用する場合に便利です。エイリアスがない場合、各アドレスに対して別々のユーザアカウントを作成しなければならず、メールを転送したり、作成したアカウントを他のアカウントと関連付けるためには、複雑なフィルタルール使用しなければなりません。

例えば、user1@example.comでドメイン内の全決済処理を行っており、全員に billing@example.comへ決済についての連絡を行ってほしい場合、エイリアスを使って、billing@example.com宛てのメールをuser1@example.comへ配信するよう設定を行う事ができます。複数のドメインを管理していて、ドメインに依らずPostmaster宛ての全てのメールをuser1@example.comへ送信したい場合、このアドレスに対するエイリアスとして、ワイルドカードを使ったPostmaster@*を使用する事もできます。

現在のエイリアス

このウィンドウには、既存のすべてのアドレスエイリアスが表示されます。

削除
このボタンをクリックすると、既存のエイリアスリストから選択されたエントリを削除することができます。

上へ
エイリアスは表示されている順番で処理されます。リストの中のエイリアスを選択し、このボタンをクリックすると、そのエイリアスの順番を上げることができます。

下へ
エイリアスは表示されている順番で処理されます。リストの中のエイリアスを選択し、このボタンをクリックすると、そのエイリアスの順番を下げることができます。

ファイルの編集
Alias.datをテキストエディタで開き、手動で検索や編集を行いたい場合はこのボタンをクリックします。必要な変更を行うと、MDaemonがそのファイルをリロードします。

エイリアス
以下の[本当のアドレス]に対するエイリアスとして使用するメールアドレスを入力してください。?と*を含むワイルドカードを使用することができます。また、アドレスエイリアスで"@$LOCALDOMAIN$"というローカルドメインのみに対応するワイルドカードを使用することもできます。例えば、"user1@example.*""*@$LOCALDOMAIN$"または"user1@$LOCALDOMAIN$"などをエイリアスとして使用することができます。

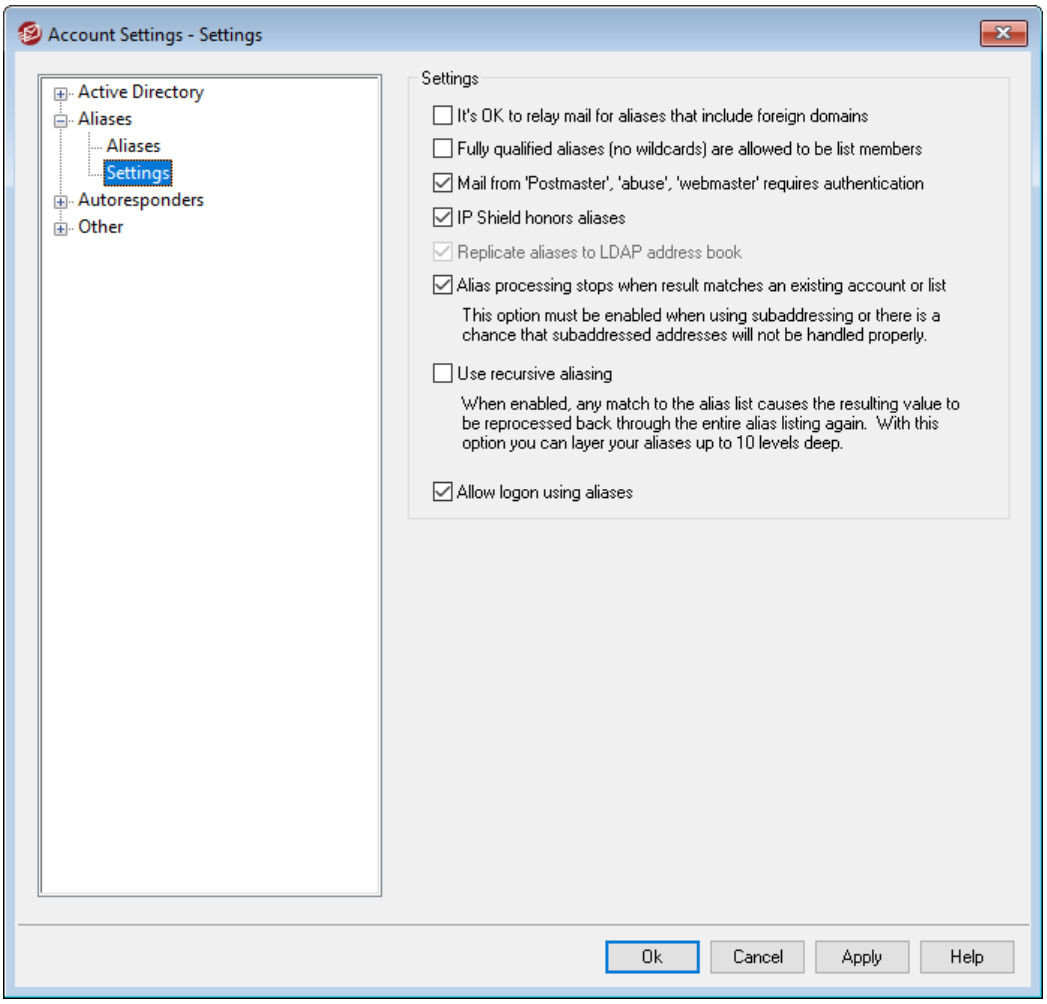
本当のアドレス
ドロップダウンリストからアカウントを選択するか、アカウント用のアカウントアイコンを使用するか、あるいはフィールドに新しいアドレスやメーリングリストを入力してください。このアドレスは、対応したエイリアスに対応して届いたメールを、実際受信するメールアドレスです。

追加
[追加]ボタンをクリックして、エイリアスを一覧に登録します。[エイリアス]と[本当のアドレス]のアドレスは一組となり、[現在のエイリアス]ウィンドウに表示されます。

参照:

エイリアス ≫ 設定 759
アカウントエディタ ≫ エイリアス 675

5.3.2.2 設定



設定

外部ドメインを含むエイリアスに対してメールのリレーを許可する
ローカル以外のドメインを持つエイリアスにメールのリレーをMDaemonに許可する場合、このチェックボックスを選択します。このオプションは、それらのエイリアスのために[リレー制御](#) 466 で[メッセージリレーを許可しない]オプションを無効にします。

正規のエイリアス(ワイルドカード不可)をリストメンバーとして許可する
エイリアスを、MDaemonのメーリングリストのメンバーにする場合は、このチェックボックスを選択してください。このコントロールが有効でない場合は、実際に存在するアカウントしかメンバーにできません。
注意： このコントロールが有効であっても、ワイルドカードを含むアドレスエイリアスはメンバーにできません。

'Postmaster,' 'abuse,' 'webmaster'からのメールは認証が必要
このオプションが使用可能な時、MDaemonが受け入れる前に、MDaemonは"postmaster@...", "abuse@..."または"webmaster@..."エイリアスのいずれから要求しているメッセージまたは認証す

るアカウントを必要とします。スパマーおよびハッカーは、これらのアドレスが存在する可能性があるということを知っています。その結果、システムを通してのメールを送信する1つを使用することを試みることができます。このオプションは、メール送信や他の無許可のユーザを禁止します。便宜のために、このオプションはSMTP認証画面でも利用可能です: セキュリティ ≫ セキュリティ設定。ここでの設定の変更は、同様にSMTP認証[476]も変更します。

IPシールドはエイリアスを受け入れる
デフォルトで、IPシールド[474]は受信メールが正規のドメイン/IPの組み合わせかどうかの確認に、エイリアスも受け入れています。IPシールドはエイリアスを実際のアカウントへ変換するため、シールドの通過にも問題なく対応しています。このオプションを無効にすると、IPシールドはアドレスエイリアスをそのままのアカウントのアドレスとして認識してしまいます。したがって、エイリアスのIPアドレスはIPシールドを侵害することになり、メッセージは拒否されてしまいます。このオプションはIPシールド画面で反映します。ここでの変更はIPシールドも変更します。

LDAPアドレス帳にエイリアスを複製
エイリアスの複製をLDAPのアドレス帳にコピーする場合は、このチェックボックスを選択してください。エイリアスの複製は、LDAPのリモート認証機能の動作には欠かせないものですが、リモート認証を使用しないのであれば複製の必要はありません。リモート検証を使用していない場合、処理時間を節約するためにこの機能を問題なく無効にすることができます。リモートLDAP検証の詳細については LDAP[754]を参照して下さい。

エイリアス処理は結果が既存のアカウントまたはリストにマッチする時に停止
このオプションが有効な場合、受信メッセージの受信者が既存のアカウントまたはメーリングリストにマッチする時、エイリアス処理は中止します。これは、通常は、ワイルドカードを持つエイリアスに適用されます。
例えば、"*@example.com=user1@example.com"にセットされるエイリアスを持つ場合、このオプションは、エイリアスに実際にサーバに存在しないアドレスだけに適用します。したがって、アカウント"user2@example.com"を持つ場合、そして、エイリアスがそれらのメッセージに適用しないので、user2に対象にされるメッセージは依然として届けられます。しかし、ワイルドカードエイリアスがそれらのメッセージに適用されるので、一部の存在しないアカウントまたはリストに対象にされるメッセージは"user1@example.com"に送信されます。このオプションは、デフォルトで有効です。

サブアドレス[694]を使用する場合には、メッセージを扱うことに関する潜在的問題を回避するために、このオプションは使用可能でなければなりません。

反復したエイリアスを使用
エイリアスを繰り返し処理する場合、このチェックボックスを選択してください。これによりエイリアスマッチの結果をすべてのエイリアスリストで再度処理することができます。エイリアスのネストは10プロセスまで可能です。例えば、以下のような設定が可能です。

```
user2@example.com = user1@example.com
user1@example.com = user5@example.net
user5@example.net = user9@example.org
```

これは、一つのエイリアスと論理的に一致します。

```
user2@example.com = user9example.org
```

同様に、以下のエイリアスとも同じ値になります。

```
user1@example.com = user9example.org
```

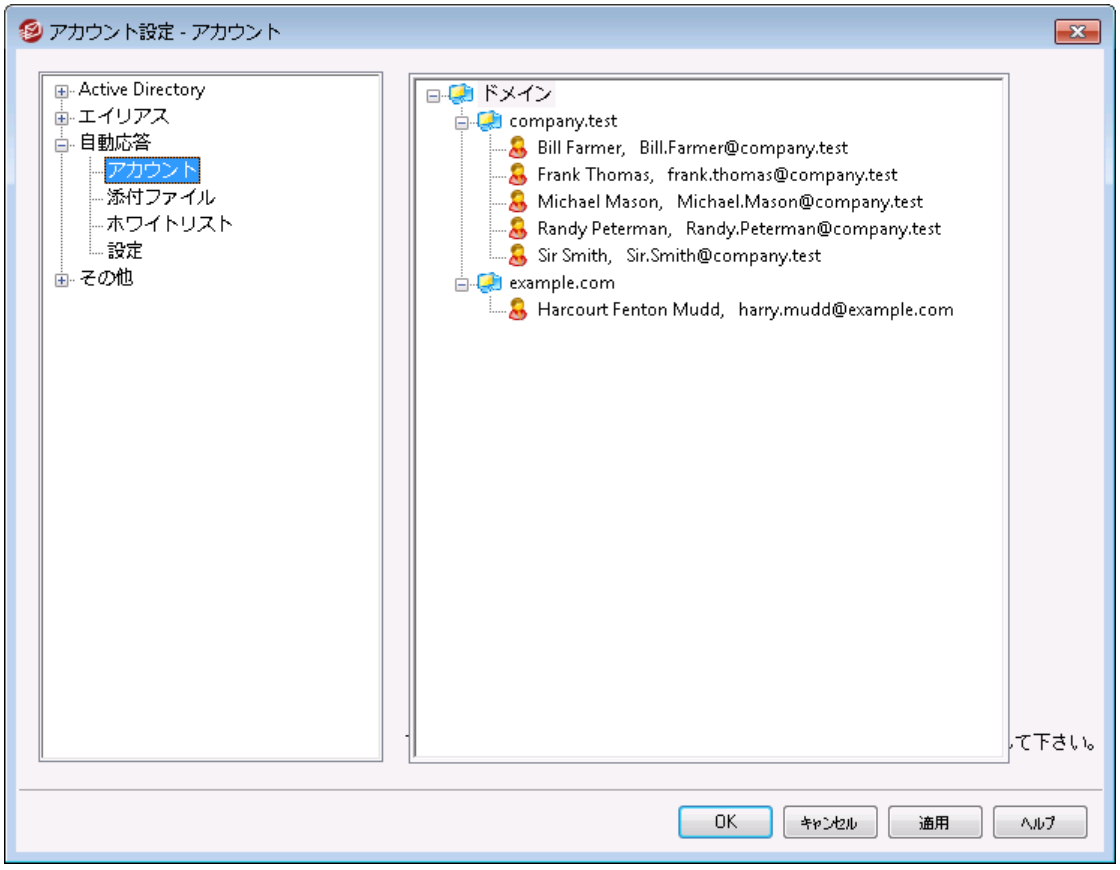
エイリアスによるログオンを許可
デフォルトで、ユーザーは実際のメールボックス名の代わりにエイリアス[757]を使ったログオンが許可されています。許可しないようにするには、このチェックボックスを無効にしてください。

参照:

エイリアス[757]

5.3.3 自動応答

5.3.3.1 アカウント



自動応答は、例えば、プログラムの実行、メーリングリストに送信者を追加、自動的に生成されたメッセージでの応答など、メールの受信をきっかけとして特定のイベントを発生させるのに便利な機能です。自動応答で最も一般的な使用方法は、メールの受信者が休暇中の場合などに、受信メールに対し、事前に定義したメッセージで自動的に応答することです。Webmail[291]やRemote Administration[321]へのWebアクセス[656]が行えるMDaemonユーザは、自動応答メッセージを構成や自動応答の利用期間をスケジュールする事ができます。最後に、自動応答はユーザーの¥data¥フォルダ

にあるOOF.mrkファイルの内容を元にしています。このファイルは多数のマクロに対応しており、その結果として、自動応答機能へ高い柔軟性を搭載しています。

メッセージがリモートソースからの場合、自動応答は常に引き継がれます。ただし、ユーザーが属するドメインから送信されるメッセージについては、自動応答 ≫ 設定[765]画面の、メールに自動応答するオプションが有効な場合のみ実行されます。自動応答メールは、送信者毎に1日1回までと制限する事もできます。

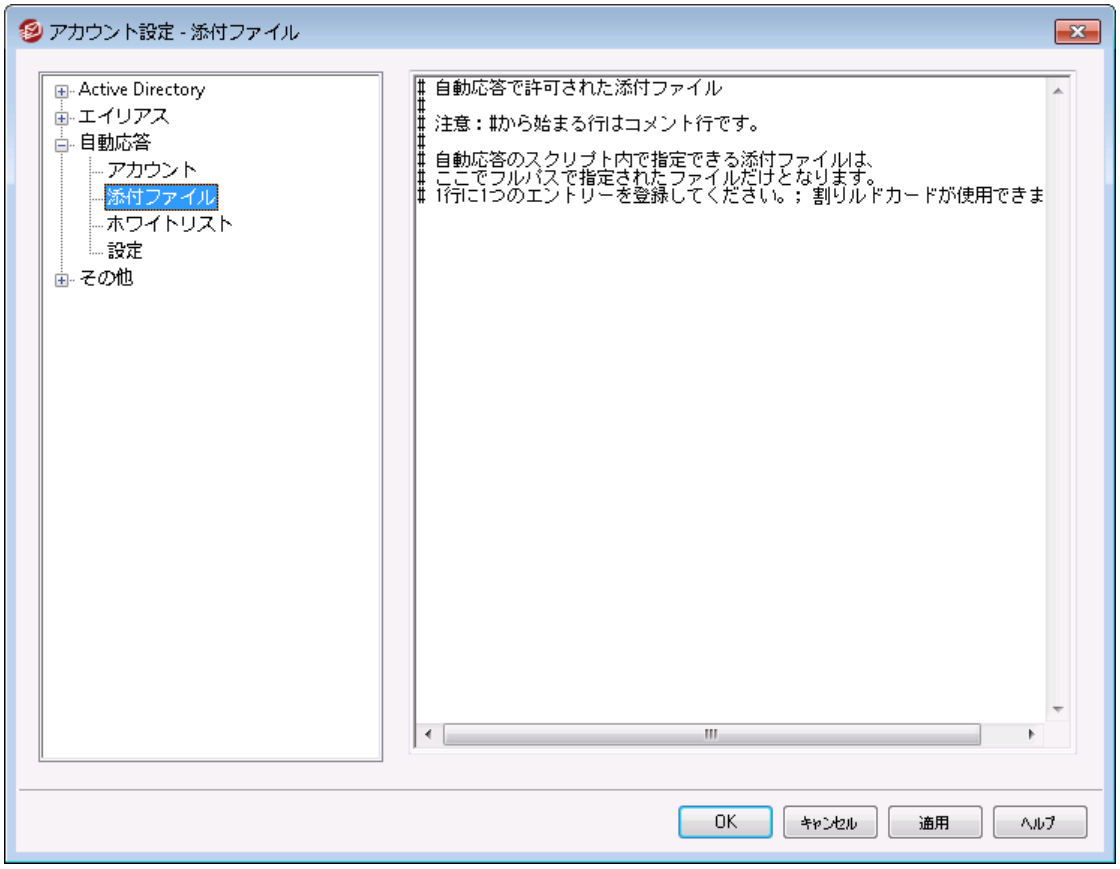
アカウントリスト

ここへは自動応答を使用する事ができるローカルユーザーが一覧表示されます。一覧から対象アカウントをダブルクリックすると、自動応答[660]画面が起動します。

参照:

自動応答 ≫ 除外リスト[764]
自動応答 ≫ 設定[765]
自動応答スクリプトの作成[766]
アカウントエディタ ≫ 自動応答[660]

5.3.3.2 添付ファイル

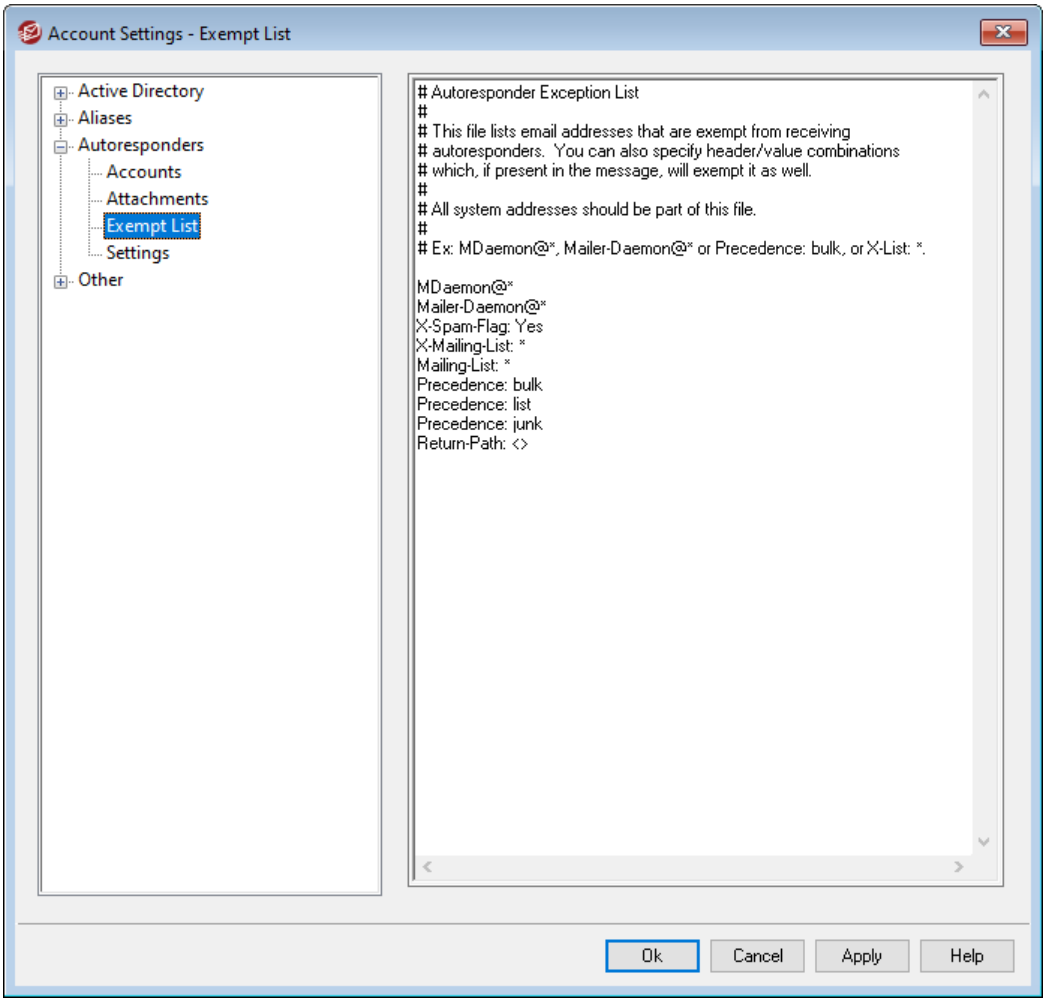


自動応答スクリプト[766]の添付ファイルとして使用するファイルのフルパスをここで指定します。自動応答スクリプト内の**%SetAttachment%** マクロが添付ファイル名へ差し替えられます。

参照:

自動応答 ≫ アカウント[761]
自動応答 ≫ 除外リスト[764]
自動応答 ≫ 設定[765]
自動応答スクリプトの作成[766]
アカウントエディタ ≫ 自動応答[660]

5.3.3.3 除外リスト



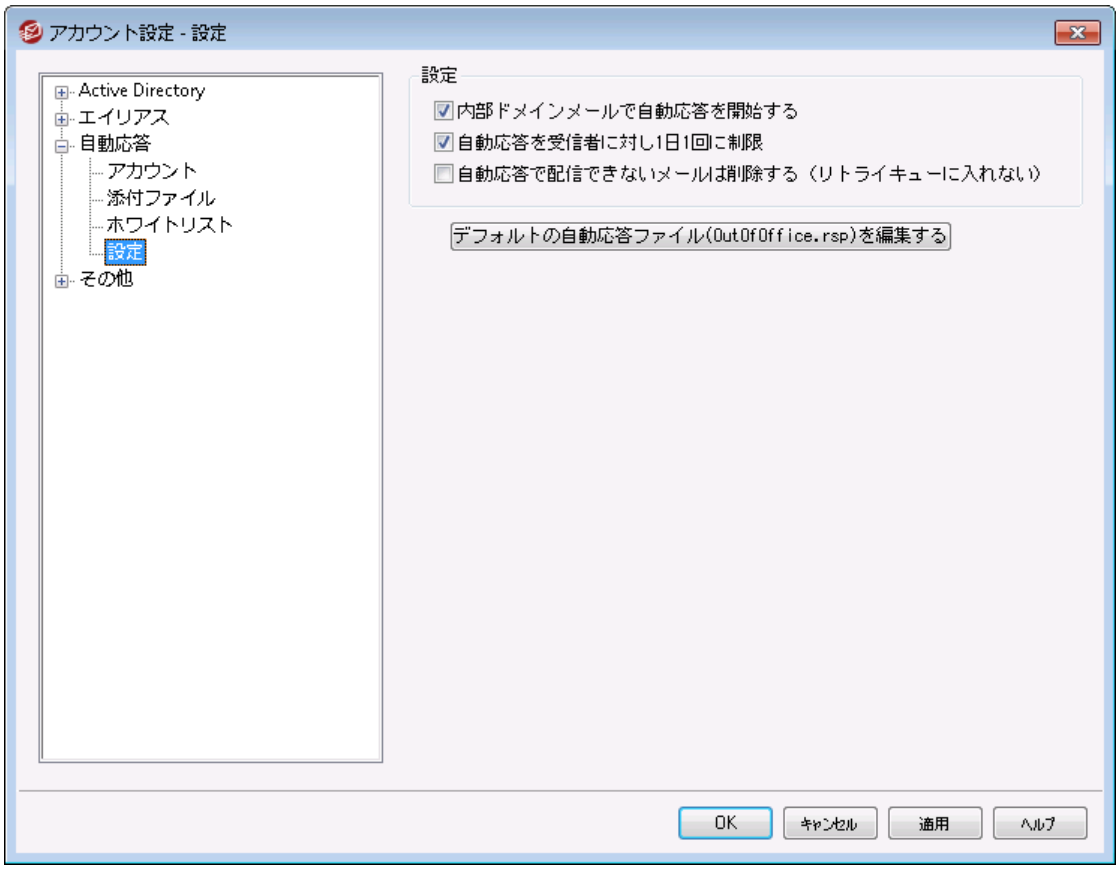
自動応答 ≫除外リストでは自動応答の受信を行わないアドレスの全体設定を行います。このリストのエントリからのメッセージでは、自動応答を受信しません。メールアドレスおよびヘッダ/値ペアを登録できます。1行につき1つのアドレスまたはヘッダ/値ペアを登録します。ワイルドカードが利用可能です。

メールループや他の問題を避けるために、(mdaemon@*やmailer-daemon@*などの)システムアドレスは全て登録して下さい。

参照:

[自動応答 ≫ アカウント](#) 761
[自動応答 ≫ 設定](#) 765
[自動応答スクリプトの作成](#) 766
[アカウントエディタ ≫ 自動応答](#) 660

5.3.3.4 設定



設定

内部ドメインメールで自動応答を開始する
デフォルトで、ローカルおよびリモートメールで、自動応答が実行されます。ユーザーと同じドメイン内のメールに対しては自動応答を送信しない場合はこのオプションを無効にして下さい。

自動応答を受信者に対し1日1回に制限
デフォルトで、自動応答は、特定のアドレスだけに対して一日当たりの1つの応答メッセージを生成します。これは、メールを受けるたびに同じ不要な自動応答を受けることからの人々が何度も同日中にメッセージを送ることを防ぎます。その日1をすでに受信場合であっても、毎回の自動応答メッセージ送信する場合、このチェックボックスを解除します。

このオプションは、自動応答メールが、別の自動応答メールを使っているアドレスへ送信されてしまう事によって発生する、メールループを防ぐ事にも役立ちます。両アドレスが自動応答を互いに送り合うのを許可する代わりに、送信者毎に、自動応答メールの送信を1日1回までと制限する事ができます。

自動応答で配信できないメールは削除（リトライキューには入れない）
配信できない自動応答メールがリモートキューで期限切れとなった場合、リトライキュー[794]へ入れるのではなく対象メールを削除する場合はこのオプションを有効にします。

デフォルト自動応答ファイルを編集（OutOfOffice.rsp）
これはデフォルトの自動応答メッセージファイルです。ファイルの内容はアカウントの oof.mrk ファイル[660]へ、メッセージが存在しなかったり空だった場合にコピーされます。

参照:

自動応答 ≫ アカウント[761]
自動応答 ≫ 除外リスト[764]
自動応答スクリプトの作成[766]
アカウントエディタ ≫ 自動応答[660]

5.3.3.5 自動応答メッセージの作成

oof.mrkというプレインASCIIテキストファイルは、自動応答の結果として配信されるメール内容を定義するためのテキストファイルです。自動応答スクリプトが自動応答によって実行されると、スクリプトファイルが処理され、マクロがスキャンされ、自動応答のきっかけとなったメールからの実際のデータへ置き換えられます。"# "から始まる行は、コメントとして無視されます。

以下のサンプルスクリプトや、MDaemonの¥app¥フォルダのoof.mrkファイルを参照して下さい。

自動応答スクリプトのマクロ

$HEADERS$	このマクロは、受信メッセージのヘッダの全部と置き換えられます。すぐこのマクロの前のテキストは、各展開する行の開始時に複製されます。
$HEADER:XX$	このマクロは、"xx"で指定したヘッダの値として展開されます。例えば：受信メールへ"TO: joe@example.com"というヘッダがある場合、$HEADER:TO$マクロはjoe@example.comに展開します。元のメールに"SUBJECT: This is the subject"があると、$HEADER:SUBJECT$マクロは"This is the subject"で置き換えられます。
$BODY$	このマクロはメッセージ本文へ置き換えられます。異なった言語のキャラクタセットを保持する方法として、MDaemonはメッセージ本文を純粋なテキストではなくバイナリデータとして読み込みます。その結果として、メッセージ本文のバイトレベルでのコピーができるようになります。
$BODY-AS-TEXT$	$BODY$マクロと同様、このマクロはメール本文全体を展開しますが、メッセージ本文をバイナリではなくテキストとして読み込む点が異なります。このマクロテキストは、各展開する行の開始時に複写されます。つまり、スクリプトは">>$BODY-AS-TEXT$"を用いて、生成されたメールの各行を複写しますが、

各行は">>"から開始されます。テキストをこのマクロの右に追加することもできます。

$SENDER$ このマクロは、受信メッセージの"From:"ヘッダに含まれるフルアドレスを決定します。

$SENDERMAILBOX$ このマクロは、送信者のメールボックスです。メールボックスは、"@"シンボルの左に対するメールアドレスの部分です。

$SENDERDOMAIN$ このマクロは、送信者のドメインです。これは、"@"シンボルの右のメールアドレスの部分です。

$RECIPIENT$ このマクロは、メッセージ受信者のフルアドレスを決定します。

$RECIPIENTMAILBOX$ このマクロは、メッセージ受信者のメールボックスです。メールボックスは、"@"シンボルの左に対するメールアドレスの部分です。

$RECIPIENTDOMAIN$ このマクロは、メッセージ受信者のドメインです。これは、"@"シンボルの右のメールアドレスの部分です。

$SUBJECT$ このマクロは、"Subject:"ヘッダの値です。

$MESSAGEID$ Tのマクロは、"Message-ID"ヘッダの値です。

$CONTENTTYPE$ このマクロは、"Content-Type"ヘッダの値です。

$PARTBOUNDARY$ このマクロは、マルチパートメッセージ用の"Content-Type"ヘッダの中のMIME"Part-Boundary"の値です。

$DATESTAMP$ このマクロは、RFC-2822スタイル日付-タイムスタンプ行に展開します。

$ACTUALTO$ メッセージの中には、再フォーマットやエイリアス変換に先立って、オリジナルユーザによる宛先メールボックスやホストを示す"ActualTo"フィールドを含むものがあります。このマクロはその値を置き換えます。

$ACTUALFROM$ メッセージの中には、再フォーマットやエイリアス変換に先立って、オリジナルのメールボックスやホストを示す"ActualFrom"フィールドを含むものがあります。このマクロはその値を置き換えます。

$REPLYTO$ "ReplyTo"ヘッダで検出した値です。

$PRODUCTID$ MDaemonのバージョン情報の文字列です。

AR_START 自動応答の開始日時を返します。

AR_END 自動応答の終了日時を返します。

ヘッダ置き換えマクロ

以下は、自動応答メッセージのヘッダをコントロールマクロの一覧です。

%SetSender%
例: %SetSender%=mailbox@host.org
実際に自動応答メッセージ、このマクロは、自動応答メッセージヘッダを作成する前に、本来のメッセージの送信者を再設定します。このように、このマクロは、自動応答メッセージのTOヘッダをコントロールします。例えば、本来のメッセージの送信者が"pooky@domain.com"で、受信者の自動応答者は、それを"user2@example.com"に変えるために、%SetSender% マクロを使用するある場合、自動応答メッセージのTOヘッダは、"user2@example.com"にセットされます

%SetRecipient%
例: %SetRecipient%=mailbox@host.org
実際に自動応答メッセージ、このマクロは、自動応答メッセージヘッダを作成する前に、本来のメッセージの宛先を再設定します。このように、このマクロは、自動応答メッセージのFROMヘッダをコントロールします。例えば、本来のメッセージの受信者が"michael@example.com"で、Michaelのアカウントをmichael@example.comに変える% SetRecipient% マクロを使用する自動応答者を持つ場合、自動応答メッセージのFROMヘッダは、"michael.mason@example.com"にセットされます。

%SetReplyTo%
ex: %SetReplyTo%=mailbox@example.com
自動応答メッセージのReplyToヘッダの値をコントロールします。

%SetSubject%
ex: %SetSubject%=Subject Text
本来のメッセージのサブジェクトの値を置き換えます。

%SetMessageId%
ex: %SetMessageId%=ID String
メッセージのID文字列を変更します。

%SetPartBoundary%
ex: %SetPartBoundary%=Boundary String
boundaryを変更します。

%SetContentType%
ex: %SetContentType%=MIME type
メッセージのcontent-typeを示された値に変えます。

%SetAttachment%
ex: %SetAttachment%=filespec
指定されたファイルを、新しく生成された自動応答メッセージに添付します。添付ファイル763画面で指定されたファイルのみが自動応答に添付されます。

自動応答スクリプトのサンプル

自動応答スクリプトマクロを用いた、シンプルなoof.mrkと呼ばれる自動応答スクリプトは、次のようなものです。

```
$SENDER$  様

ただいま休暇中につき、'$SUBJECT$' に関するメールを読むことができません。
宜しくお願いします。

$RECIPIENT$
```

さらに、ヘッダ置換マクロを使ってこのスクリプトを展開し、$SENDER$宛てに返信する自動応答メールのヘッダの一部をコントロールできます。

```
$SENDER$  様

ただいま休暇中につき、'$SUBJECT$' に関するメールを読むことができません。
あしからずご了承ください。

$RECIPIENT$

%SetSubject%=RE: $SUBJECT$
%SetAttachment%=c:\photos\me_on_vaction.jpg
```

このスクリプトで、自動応答メールの件名の前には"RE: "が追加され、指定のファイルが添付されます。

"%SetSubject%=RE: $SUBJECT$" というマクロは以下のように実行されます。

1. $SUBJECT$部は展開して、最初のメッセージのサブジェクトテキストと取り替えられます。これは次の文字列と同意義になります。

   ```
   %SetSubject%=RE: Original Subject Text
   ```

2. 次に、MDaemonが内部バッファにある元の件名を、新しい件名と置き換えます。それ以降、スクリプトの"$SUBJECT$"の使用は、新規の結果を返送します。

新しいマクロを配置する際の注意事項 - 新しいマクロは返信スクリプトの最後に配置して下さい。これは思わぬ悪影響を避けるために必要な処理です。
例えば、%SetSubject%マクロが応答スクリプトの3行目にある$SUBJECT$マクロの前にあると、Subjectテキストは$SUBJECT$マクロが展開される前に変更されることになります。つまり、$SUBJECT$はオリジナルメッセージの"Subject:"ヘッダではなく、%SetSubject%で設定した値に置き換わってしまいます。

参照:

自動応答スクリプトの作成 766
自動応答 ≫ アカウント 761
自動応答 ≫ 除外リスト 764
自動応答 ≫ 設定 765
アカウントエディタ ≫ 自動応答 660

5.3.3.5.1 自動応答のサンプル

自動応答スクリプトマクロを用いた、シンプルなoof.mrkと呼ばれる自動応答スクリプトは、次のようなものです。

```
$SENDER$ 様

ただいま休暇中につき、'$SUBJECT$'に関するメールを読むことができません。
宜しくお願いします。

$RECIPIENT$
```

さらに、ヘッダ置換マクロを使ってこのスクリプトを展開し、$SENDER$宛てに返信する自動応答メールのヘッダの一部をコントロールできます。

```
$SENDER$ 様

ただいま休暇中につき、'$SUBJECT$'に関するメールを読むことができません。
あしからずご了承ください。

$RECIPIENT$

%SetSubject%=RE: $SUBJECT$
%SetAttachment%=c:\photos\me_on_vaction.jpg
```

このスクリプトで、自動応答メールの件名の前には"RE: "が追加され、指定のファイルが添付されます。

"%SetSubject%=RE: $SUBJECT$" というマクロは以下のように実行されます。

1. $SUBJECT$部は展開して、最初のメッセージのサブジェクトテキストと取り替えられます。これは次の文字列と同意義になります。

   ```
   %SetSubject%=RE: Original Subject Text
   ```

2. 次に、MDaemonが内部バッファにある元の件名を、新しい件名と置き換えます。それ以降、スクリプトの"$SUBJECT$"の使用は、新規の結果を返送します。

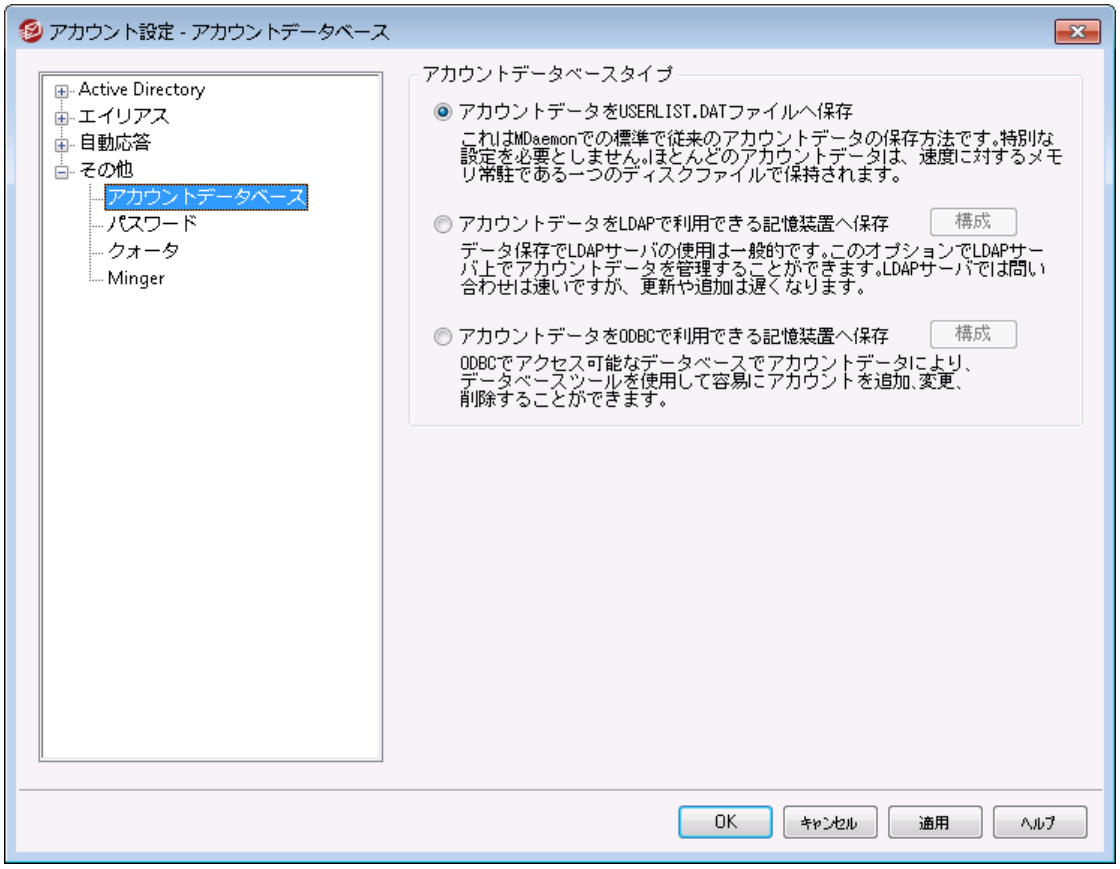
新しいマクロを配置する際の注意事項 - 新しいマクロは返信スクリプトの最後に配置して下さい。これは思わぬ悪影響を避けるために必要な処理です。
例えば、%SetSubject%マクロが応答スクリプトの3行目にある$SUBJECT$マクロの前にあると、Subjectテキストは$SUBJECT$マクロが展開される前に変更されることになります。つまり、$SUBJECT$はオリジナルメッセージの"Subject:"ヘッダではなく、%SetSubject%で設定した値に置き換わってしまいます。

参照:

自動応答スクリプトの作成 766
自動応答 ≫ アカウント 761
自動応答 ≫ 除外リスト 764
自動応答 ≫ 設定 765
アカウントエディタ ≫ 自動応答 660

5.3.4 その他

5.3.4.1 アカウントデータベース



(アカウント ≫ アカウント 設定にある)アカウント データベースダイアログではMDaemonがODBC、LDAP、ローカルUSERLIST.DATのうち、どの方法でユーザーアカウントを管理するのかを指定することができます。

アカウント データベースの種 類

アカウント データをUSERLIST.DATファイルへ保 存
MDaemonにアカウント データベースとして、内 部 のUSERLIST.DATファイルを使 用 する場 合 は、このオプションを選 択 してください。これは、MDaemonのデフォルト 設 定 であり、MDaemonユーザアカウント情 報 のすべてをローカルに格 納 します。大 部 分 の情 報 が1 つのファイルに保 存 され、効 率 と速 度 を向 上 させるためにメモリに常 駐 します。

アカウント データをLDAPアクセシブルスト アへ保 存
MDaemonユーザデータベースとして、ODBCやローカルのUSERLIST.DATシステムではなくて、LDAPサーバを使 用 する場 合 は、このオプションを選 択 してください。異 なった場 所 に複 数 のMDaemonサーバが存 在 し、サーバで1 つのユーザデータベースを共 有 する場 合 、この方 法 はアカウント データの管 理 方 法 として有 効 な方 法 です。それぞれのMDaemonサーバは、ユーザ情 報 をローカルに格 納 するのではなく全 体 で共 有 するために、同 じLDAPサーバに接 続 するように構 成 されます。LDAPサーバは反 応 も高 速 でクエリにも効 果 的 ですが、新 しいデータの更 新 や挿 入 の速 度 は遅 くなります。

構 成
LDAPアカウント データオプションが選 択 されている時 、このボタンをクリックするとLDAP画 面 754が起 動 し、LDAPサーバー設 定 を行 う事 ができます。

アカウント データをODBCアクセシブルスト アへ保 存
MDaemonのアカウント データベースとしてODBC互 換 のデータベースを使 用 する場 合 は、このオプションを選 択 してください。

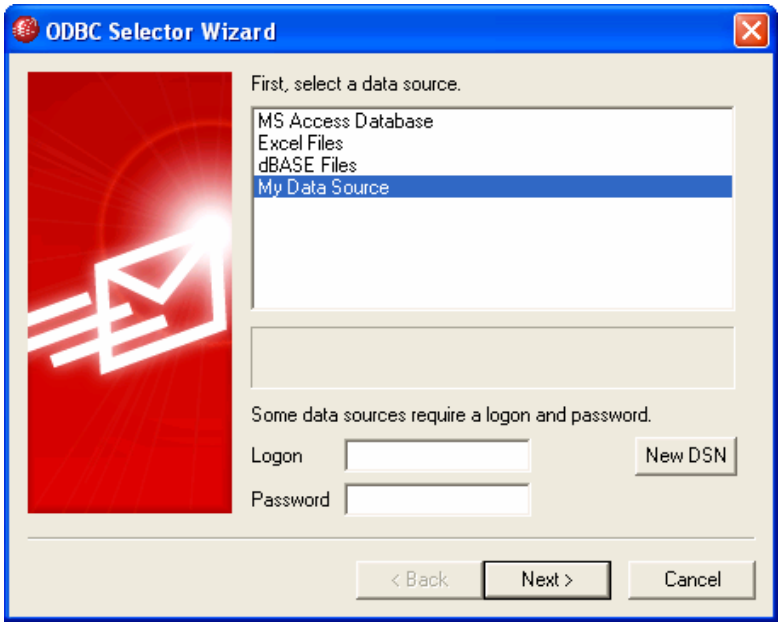
構 成
ODBCアカウント データオプションがされている時 、このボタンをクリックするとODBC選 択 ウィザード 772が起 動 し、ODBC準 拠 のデータベース選 択 や設 定 を行 う事 ができます。

5.3.4.1.1 ODBC選択ウィザード

MDaemonアカウント データベースとしてODBC準 拠 のデータソースを選 択 したり構 成 したりする際 には、ODBC選 択 ウィザードを使 用 します。

アカウントデータベースをＯＤＢＣアクセシブルストアへ移行する

1. アカウント データベースダイアログ(アカウント ≫ アカウント 設定 » アカウント データベース)で、アカウントデータをＯＤＢＣアクセシブルストアへ保 存 を選 択 し構 成 をクリックしてODBC選 択 ウィザードを開 きます。

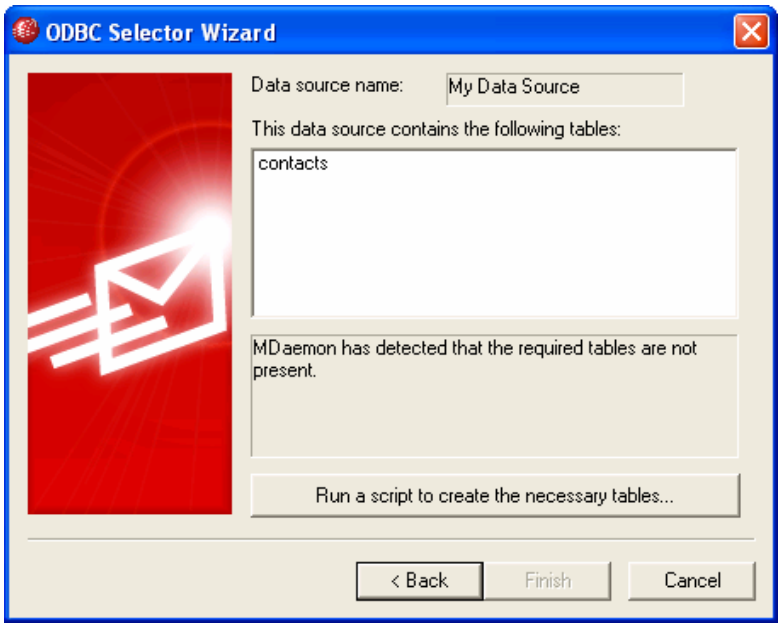


2. アカウントデータベースに使用するデータソースを選択してください。互換データソースがリストされていない場合、**新しいDSN**を選択し、新規ODBCデータソース[774]に記載されている説明にしたがって、新しいデータソースを作成してください。

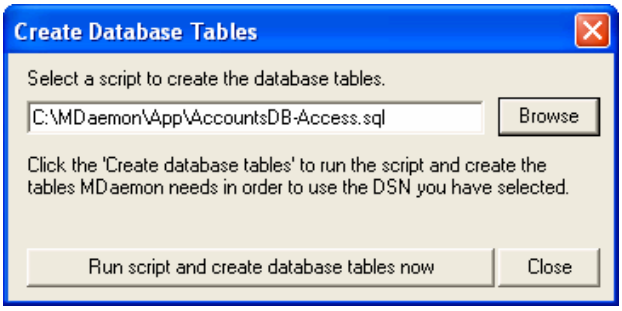
3. **ログオン**および**パスワード**が必要な場合は入力してください。

4. **次へ**をクリックします。

5. データソースにMDaemonが必要とするテーブルがすでに含まれている場合は、手順 8.へ進んでください。それ以外は**必要なテーブルを作成するスクリプトを実行...**をクリックします。



6. データベースアプリケーション用のテーブルを作成するために使用するファイルへのパスを入力してください。または 参照 をクリックしてそのファイルへのパスを指定してください。¥MDaemon¥app¥ フォルダは、いくつかの一般的なデータベース用のスクリプトを含みます。



7. スクリプトを実行し、データベースのテーブルを作成します。 をクリックして**OK**をクリックして閉じる をクリックします。

8. 完了 をクリックし、**OK**をクリックして、アカウント データベースオプションダイアログを閉じてください。

9. データベース移動ツールは、すべてのユーザアカウントをODBCデータソースへ移動して、MDaemonを終了します。OKをクリックして、MDaemonを再起動してください。新しいODBCアカウント データベースの使用を開始できます。

参照:

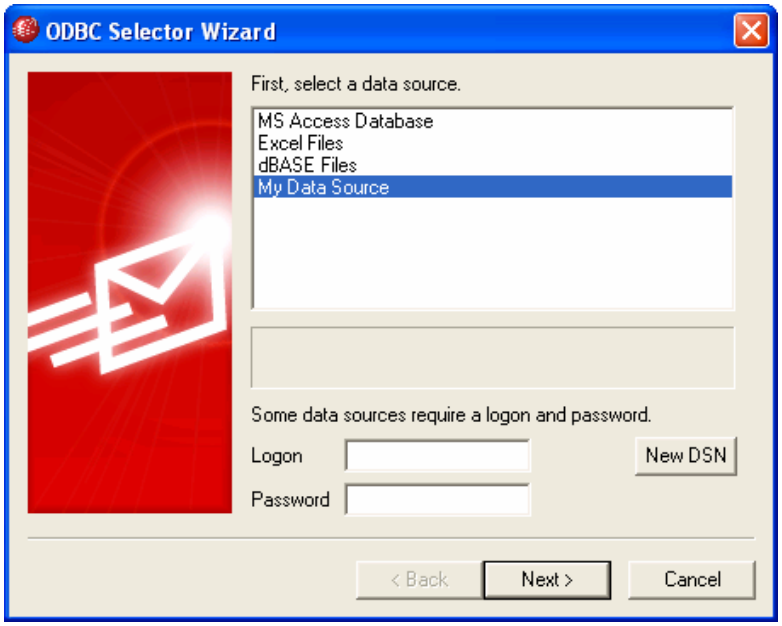
アカウントデータベース 771
新しいＯＤＢＣデータソースの作成 774

5.3.4.1.1.1 新しいODBCデータソースの作成

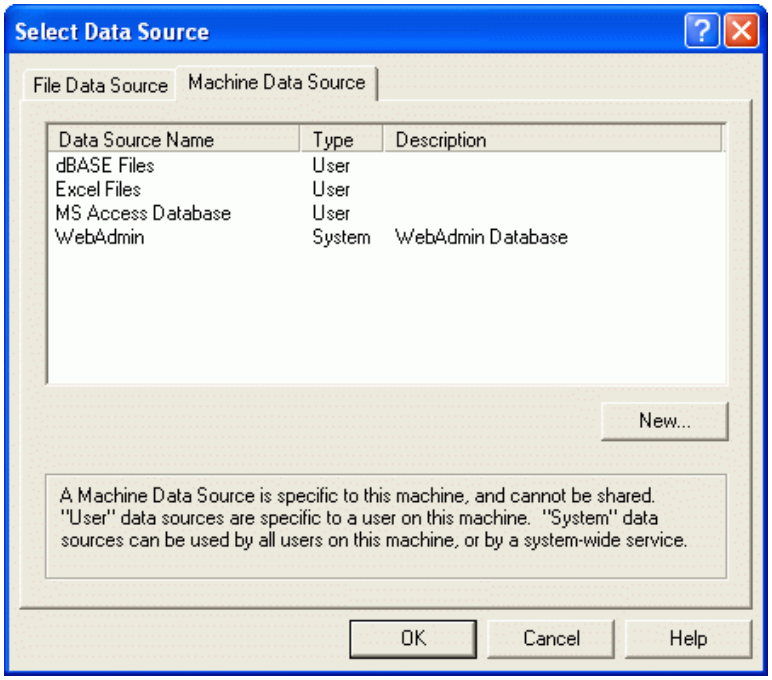
新しいODBCデータソースを作成するには:

1. アカウント データベースダイアログ（アカウント ≫ アカウント設定 ≫ アカウント データベース）で、ODBC アクセシブルストアへ保存 をクリックして、構成 ボタンをクリックして、ODBC選択ウィザードを開いてください。

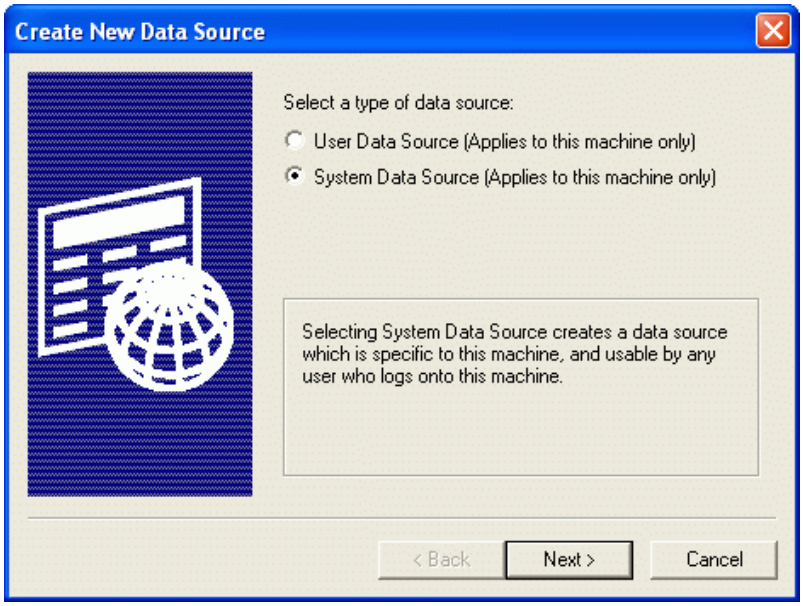
2. 新しいＤＳＮ をクリックして、データソース選択ダイアログを開きます。



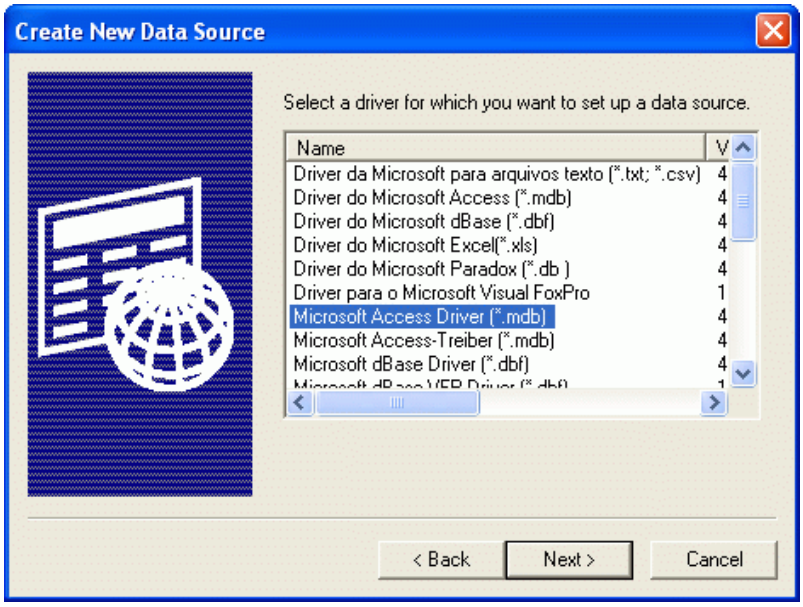
3. コンピュータデータソース 画面に切り替え、新規作成... ボタンをクリックしデータソースの新規作成を開いてください。



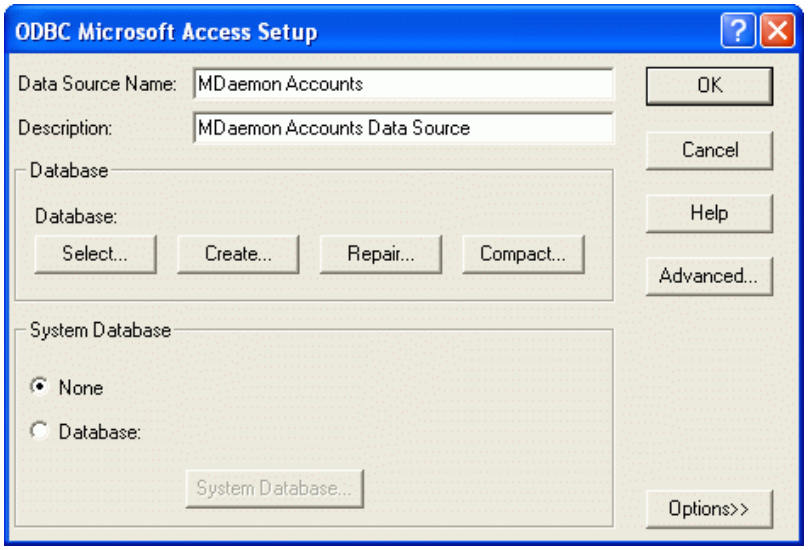
4. システムデータソースを選択して次へをクリックします。



5. データソースを設定するデータベースドライバを選択して次へをクリックします。



6. 完了をクリックして、ドライバ固有の設定ダイアログを表示します。このダイアログは選択したドライバによって表示が異なります。（次の例はMicrosoft Access設定ダイアログです）

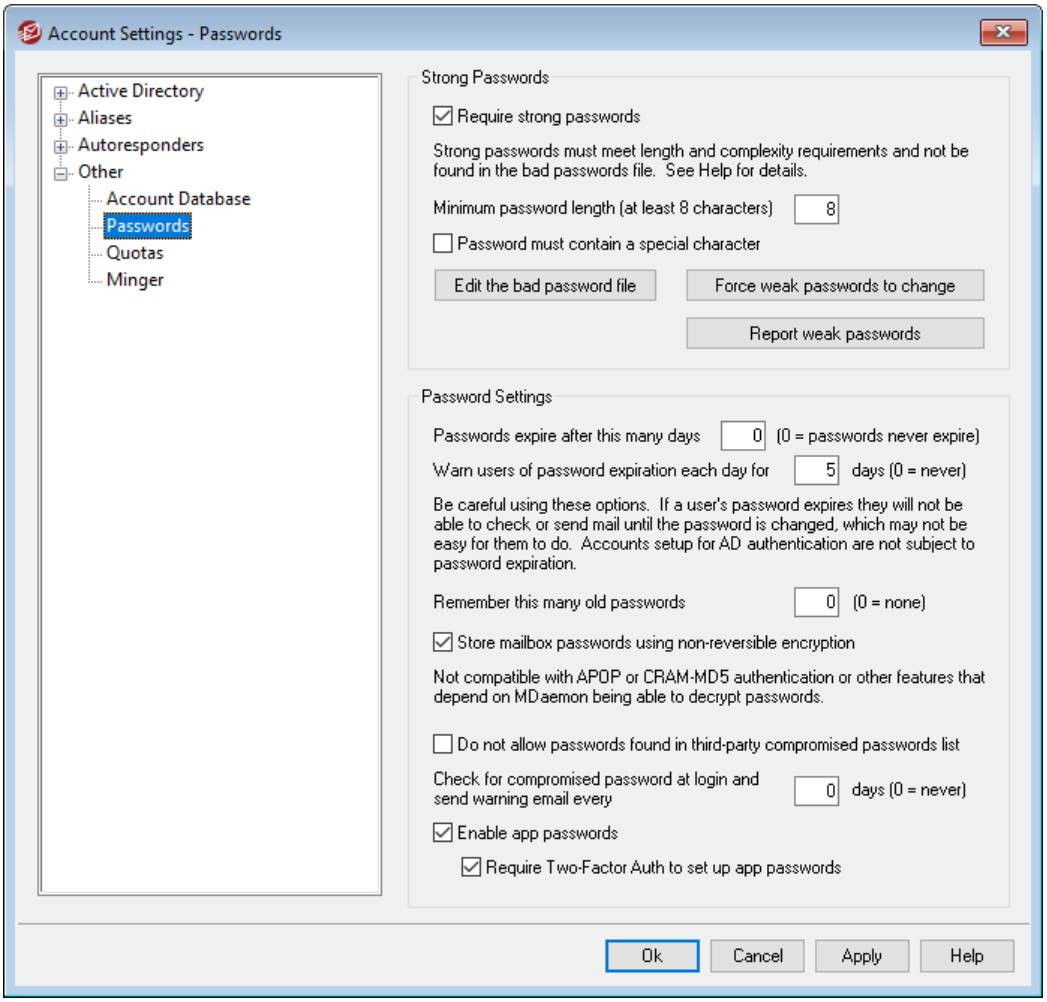


7. データソース名を指定してください。ドライバ固有のダイアログ(データベースの指定や作成、ディレクトリやサーバの選択など)が必要とするその他の情報を指定してください。
8. OKをクリックして、ドライバ固有のダイアログを閉じてください。
9. OKをクリックして、データソースの選択ダイアログを閉じます。

参照:

アカウントデータベース 771
ＯＤＢＣ選択ウィザード － アカウントデータベース 772

5.3.4.2 パスワード



パスワード強度

強固なパスワードを求める
デフォルトで、MDaemonは新しいアカウントの作成時やパスワードの変更時、強固なパスワードを要求します強固なパスワードを要求しない場合には、このチェックボックスを外して無効にして下さい。

強固なパスワードの条件:
- 最少文字数以上である事
- 大文字、小文字を含むこと
- 文字と数字を含むこと

- 記号を含むこと(下記の記号オプションが設定されていた場合)
  - 名前やメールボックス名を含まないこと
  - 使用禁止パスワードファイルに含まれていないこと

最少のパスワード長（8文字以上）
ここでは強固なパスワード要件となる最少パスワード文字数を設定します。最低8文字以上である必要がありますが、より長い文字数を推奨します。新規インストール時のデフォルト文字数は10です。この設定は、新しいパスワード要件に満たない長さのパスワードを使っているアカウントに対して、パスワードの変更を自動で強制変更するよう求める事はありませんが、ユーザーが次にパスワードを変更しようとした際、新しいパスワード要件を求めるようになります。

最少設定に関わらず、パスワードは15文字以上にすることもできます。

パスワードに記号を含む事を必須とする
デフォルトで、新規のMDaemonインストールでは、強固なパスワードとして、最低1つ以上、次の記号が含まれている必要があります: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~ 記号を強固なパスワードで必須としない場合には、このオプションを無効に設定して下さい。

使用禁止パスワードファイルを編集
このボタンで使用禁止パスワードファイルの編集を行います。ファイルの中のエントリー覧は大文字小文字を区別し、パスワードとして使用できない文字が記載されています。より複雑なエントリや、除外設定を行う場合は正規表現 595 を使う事ができます。! から始まるエントリは、正規表現として扱われます。

脆弱なパスワードの変更を強制
脆弱なパスワードを使っている全てのアカウントに対しパスワードの変更を強制するにはこのボタンをクリックします。これにより脆弱なアカウントはパスワードを変更するまでロックアウトされます。パスワードは管理者がMDaemonの管理画面から変更するもできますし、ユーザーがWebmailやRemote Administrationから変更する事もできます。ユーザーが古いパスワードでログインすると、その直後に、パスワード変更を求める画面へ転送されます。 **注意点**: このオプションは「復号できない暗号化方式を使ってパスワードを保存する」オプションを使っている場合は使用できません。

脆弱なパスワードの報告
このボタンをクリックすると、脆弱なパスワードを使っているMDaemonアカウントのレポートを生成します。レポートはOKを押すと、指定のアドレスへメールで送信されます。 **注意点**: このオプションは「復号できない暗号化方式を使ってパスワードを保存する」オプションを使っている場合は使用できません。

パスワードオプション

指定日数後のパスワードを期限切れとする（0=パスワードを無期限にする）
アカウントへパスワード変更を行わずにアクセスできる最大日数を設定する場合はこのオプションを使用します。デフォルト値は0で無期限と設定されています。例えばこの値を30へ変更すると、ユーザーは、パスワードを最後に変更してから30日以内にパスワード変更が必要になります。パスワードが変更されると、タイマーがリセットされます。ユーザーのパスワード期限が過ぎると、POP, IMAP, SMTP, Webmail, Remote Administrationへのログインは行えなくなります。ただし、ユーザーは、パスワード期限の処理が行われる前に、パスワード変更が行えるよう、WebmailやRemote Administrationへのアクセスは行えます。Outlook, Thunderbirdなどからパスワード変更は行えません。また、多くのメールクライアントは、詳細なエラーメッセージを表示しない場合もあり、管理者がログイン失敗の理由を調査しなくてはならない場合もあります。

ユーザーがWebmailやRemote Administrationでパスワードを変更できるようにするには、最初にウェブサービス[728]画面で"...パスワードの編集"許可を与えておく必要があります。また、パスワードの変更が簡単には行えないユーザーもいるため、このオプションを使用する前にパスワードの変更方法についてはアナウンスやトレーニングが求められる場合もあります。

指定日数ごとにユーザーのパスワード期限を警告する[xx]日間経過後(0=しない)
パスワードの変更期限が近いアカウントに日別の通知を行います。このオプションはパスワード変更の何日前からユーザーへ通知するかを指定するのに使用します。

パスワードの履歴を記憶する(0=しない)
MDaemonが記憶するユーザー毎の古いパスワードの数をここで指定します。ユーザーがパスワードを変更する際、古いパスワードの再利用は、ここで指定した回数分できなくなります。オプションはデフォルトで0(記憶しない)設定となっています。

復号化のできない暗号化方式を使ってパスワードを保存する
メールボックスのパスワードを復元できない暗号化方式で暗号化し保管するにはこのオプションを有効にして下さい。これにより、パスワードはMDaemon、管理者、攻撃者の誰からも復元できなくなります。これを有効にすると、MDaemonはbcryptパスワードハッシュを使用します。これは今までよりも長いパスワード(72文字まで)を許可しており、アカウントのエクスポートやインポートの際には、パスワAPOP & CRAM-MD5[82]認証や弱いパスワード検出などMDaemonによって復元する機能がある場合もあり、この機能との互換性はありません。復元できないパスワードはデフォルトで有効です。

脆弱なパスワード

MDaemonはサードパーティーサービスが提供する脆弱なパスワード一覧を使ってユーザーパスワードを確認します。この確認はパスワードをサービスへ配信する事なく行う事ができ、ユーザーのパスワードが一覧に存在していた場合であっても、パスワードがハッキングされたという事ではありません。これは、どこかの誰かが同じ文字列をパスワードに使用していた事があり、悪用された事がある事を示唆しています。公開されているパスワードは辞書攻撃でハッカーが使用している場合もあり、使用された事のないパスワードの利用はより安全です。Pwned Passwordsにて詳細をご覧頂けます。

サードパーティーの脆弱なパスワードリストにあるパスワードの使用は許可しない
脆弱なパスワード一覧の中の文字列をパスワードとして使用する事を許可しない場合はこのオプションを有効にしてください。

ログイン時に脆弱なパスワードを確認し脆弱な場合には都度警告メールを送信する[xx]日経過後(0=送信しない)
このオプションを使用すると、各ユーザーのパスワードが、指定日数毎に、ユーザーがログインするタイミングで脆弱なパスワード一覧に該当しないか確認されます。脆弱なパスワードを使用していた場合、警告メールがアカウントとpostmaster宛に送信されます。警告メールの本文は¥MDaemon¥App フォルダの中のテンプレートを編集しカスタマイズできます。ユーザーのパスワード変更方法は、パスワードをMDaemonが保持しているのかActive Directory[747]が保持しているのかにより異なるため、CompromisedPasswordMD.datとCompromisedPasswordAD.datの2種類のテンプレートを用意しています。マクロはメールの個別設定や件名、あて先の変更などに使用する事ができます。

Appパスワード

Appパスワード[683]とは、メーラーやアプリで使用する、非常に強力なランダム生成されたパスワードで、メールアプリケーションのような2段階認証[656](2FA)を使用できない場合であっても、これをより安全に利用するためのものです。参照: Appパスワード[683].

Appパスワードを有効にする

デフォルトで、全ユーザーはWebmailへ2段階認証でログインすればAppパスワードを使用できます。ユーザーのAppパスワードの利用を許可しない場合は、ユーザーのWebサービスページにある *...appパスワードの編集*[656] オプションを無効化する事ができます。

Appパスワードの設定に2段階認証を必須とする

デフォルトで、新しいAppパスワードを作成するには、Webmailへ2段階認証[656](2FA)でサインインする必要があります。この要件を無効にするのはお勧めしません。全体管理者[690]は、MDRAにおけるこの要件からは除外されていますが、MDRAやWebmailへのサインインには、毎回2FAを使用する事をお勧めします。

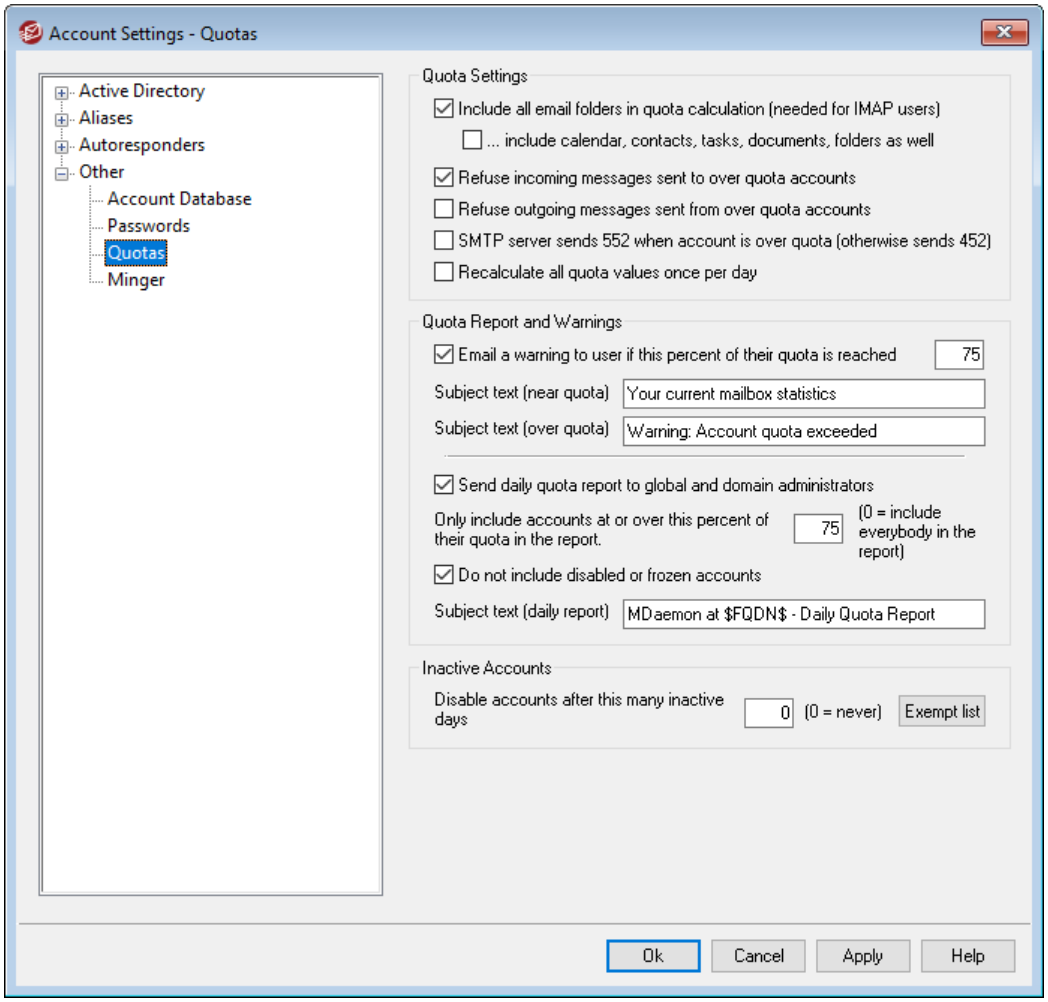
アカウントエディタの設定[693]ページへ「*SMTP, IMAP, ActiveSync等へのログインにAppパスワードを必須とする*」ためのオプションがあります。

Appパスワードを必須にする事で、アカウントのパスワードを、SMTPやIMAP等での辞書攻撃やブルートフォース攻撃から保護する事ができます。Appパスワードは、例えばパスワードが漏えいしてしまった場合でも、本来のパスワードではなく、MDaemonは正しいAppパスワードのみを受け付けるため、パスワードを取得した攻撃者はこれが本来のパスワードでない事を確認できません。更に、MDaemonアカウントがActive Directory[747]認証を使用しており、Active Directoryがパスワードの連続失敗によりアカウントをロックしたとしても、このオプションを使う事でMDaemonからロックされる事がなくなります。MDaemonはAppパスワードのみで認証を行い、ActiveDirectoryへの問合せを行う事がないためです。

参照:

アカウントエディタ ≫ アカウントの詳細[650]
アカウントエディタ ≫ ウェブサービス[656]
アカウントエディタ ≫ Appパスワード[683]
正規表現[595]

5.3.4.3 クォータ



クォータ設定

クォータ計算においてすべてのメールフォルダを含む (IMAPユーザーむけ)
このチェックボックスを有効にすると、全てのメールフォルダにある全メッセージファイルが、アカウントに割り当てられたサイズやメール件数の上限の対象となります。チェックが無効な場合には、INBOX内のメッセージファイルだけが上限に対してのカウント対象となります。この機能は一般的にIMAPユーザーに対してのみ有効です。

...予定表、連絡先、仕事、ドキュメントフォルダも含む
クォータ算出において、予定表、連絡先、タスク、ドキュメントのフォルダも含める場合、このチェックボックスを選択しまします。

クォータ超過のアカウント宛ての受信メールを拒否
デフォルトでは、割り当てられたクォータ設定値に到達したアカウントにメールが届くと、MDaemonはそのアカウントが自身のメールボックス内のメール削除等の整理が行われるまで、当該アカウント宛てのメール受信を拒否します。クォータ超過したアカウントへのメール受信を拒否したくない場合には、このチェックを外します。

クォータ超過のアカウントからの送信メールを拒否
このチェックボックスを有効にすると、クォータ超過したアカウントからのメール送信を拒否するようになります。クォータ超過したアカウントは、自身のメールボックス内のメール削除等の整理が行われるまで、メール送信が行えません。このオプションはデフォルトで無効になっています。

アカウントのクォータ超過時にSMTPサーバから552を送信する(デフォルト:452)
デフォルトでは、SMTPプロセス処理の中で、クォータ[666]を超えたアカウントに対して、MDaemonでは452エラーコード("Requested action not taken: insufficient system storage")を送信します。このコードは、一時的なエラーを示しており、サーバが後にメールを再送するという意味を持ちます。一時的なエラーコードではなく、("Requested mail action aborted: exceeded storage allocation")という552恒久エラーコードを送信するには、このチェックボックスを有効にします。

一日に一度全てのクォータ値を再計算する
デフォルトで、キャッシュされたクォータ値は下記の*"...日次クォータレポートを送信する"*オプションが有効だった場合のみ、送信のタイミングでリセットされます。クォータ値を日次のメンテナンス処理の中で一日に一度再計算するにはこのオプションを有効にしてください。

クォータのレポートと警告

クォータ設定値に対して、次のパーセントを超えたら警告メールを送信する
日次メンテナンスとクリーンアップ処理[450]で、MDaemonはアカウントエディタ[666]で指定した、*保存するメッセージ数*や*最大ディスク容量*のクォータ制限に対し、このパーセンテージに到達しているかどうかをチェックし、到達している場合、警告メッセージがアカウントに送信されます。件名(クォータ上限に近い)オプションで、このメールの件名を設定できます。メッセージには、アカウントの現在の保存メッセージ数、メールボックスのサイズ、使用済のパーセンテージと残りのパーセンテージが含まれます。さらに、既に届いている警告メッセージがある場合には、新しい警告メッセージで既存のメッセージを上書きします。警告メッセージを送らない場合は、このオプションを無効にします。新しい警告メッセージがユーザーの受信箱へ配置されると、エントリがシステムログへ記録され、警告メッセージの配信を後に確認できるようになります。メールが既に存在していて更新されただけの場合はログへ記録は残りません。ログエントリが上書きで追加されている場合、ユーザーは受信箱からメールを削除している事を意味しています。このオプションを無効化すると、クォータの警告メールはユーザーへ配信されません。

> クォータ上限が近い時に送信されるメールテンプレート(MDaemon¥app¥NearQuota.dat)はクォータ上限に近い場合に送信される警告メールへ使用されます。ユーザーアカウントに関連した全てのマクロ(例 $EMAIL$, $MAILBOX$, $DOMAIN$, 等)がテンプレートで使用できます。

件名(クォータ上限に近い)

上記で指定したクォータのパーセントを超えたら送信する警告メールの件名です。

件名(クォータ超過)
「クォータ制限に近い」警告メールの件名と同様に、ユーザーアカウントがクォータ超過の場合にもメール通知が行われます。ここでは「クォータ超過」警告メールの件名を指定します。

グローバル管理者とドメイン管理者に日次のクォータレポートを送信する
毎日グローバル管理者とドメイン管理者に対してクォータレポートを送る場合は、このチェックボックスを選択し、値を入力します。このレポートには全ユーザーのクォータ統計とクォータ制限に対する規定のパーセンテージに到達したユーザー情報が記載されます。全員のクォータ統計をレポートに記載する場合は、0を入力して下さい。

無効や凍結されたアカウントを除く
デフォルトでクォータレポートへ無効化されたアカウントや凍結されたアカウントは含まれません。これもレポートへ含むにはチェックボックスを無効にしてください。

件名（日次レポート）:

このオプションはMDaemonが管理者へ送る日次クォータレポートの件名をカスタマイズする場合に使用します。レポート自体のカスタマイズを行うには `MDaemon\APP` フォルダの`QuotaReport.dat` を確認してください。

非アクティブアカウント

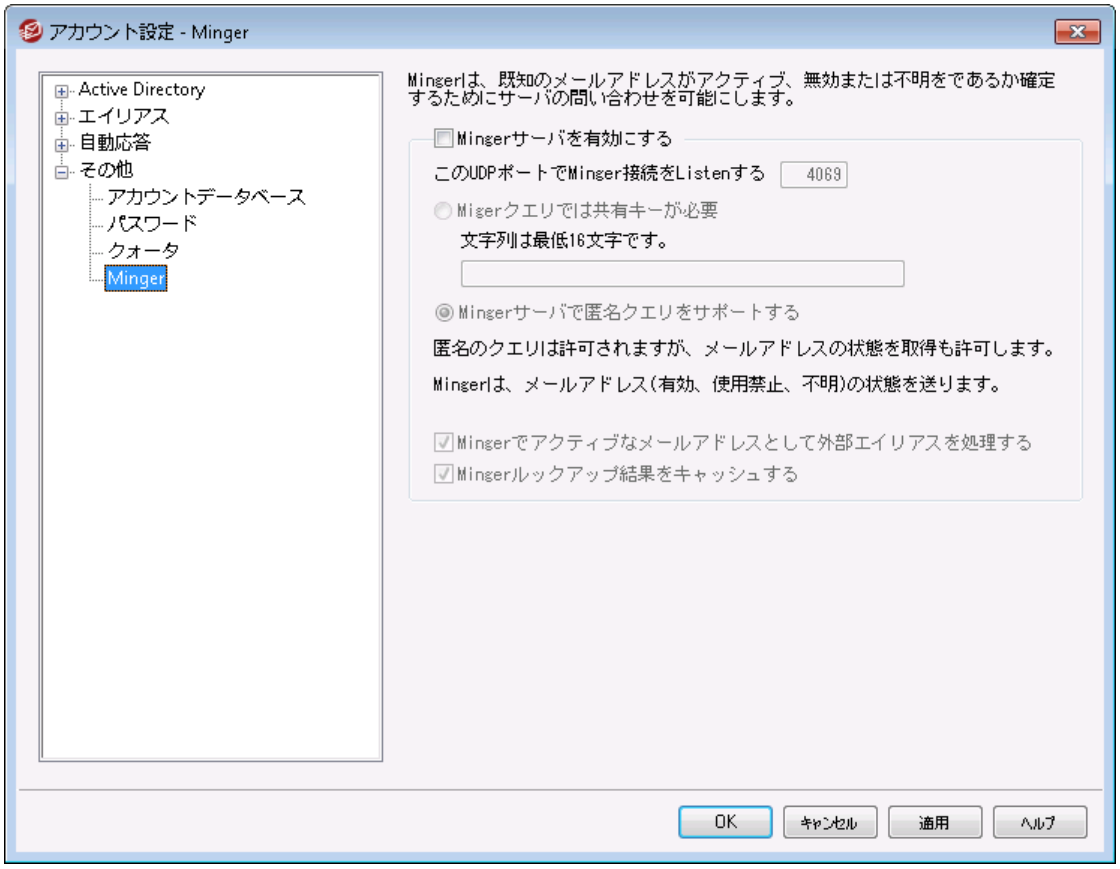
この日数を超える非アクティブアカウントを無効化する（0=無効化しない）
指定した日数非アクティブだったアカウントを自動で無効化する場合はこのオプションを使用します。非アクティブな日数が最大値に到達すると、アカウントは無効になり、対象アカウント宛てのメールは`postmaster`へ送信されます。このメールへ返信を行うと、アカウントは再度アクティブになります。この処理は毎日深夜のクリーンアップイベントの一つとして実行されます。デフォルトは0で無効化しない設定になっています。

除外リスト
このリストへ追加したアカウントは非アクティブな場合に無効化される対象から除外されます。

参照:

アカウントエディタ ≫ クォータ 666
テンプレートマネージャ ≫ クォータ 738

5.3.4.4 Minger



アカウント ≫ アカウント設定にある、MingerはMDaemon Technologiesが開発したメールアドレス検証プロトコルです。元々はfingerプロトコルに基づき、Mingerは柔軟に、メールアドレスが正規なものかどうかサーバへ問い合わせるための、シンプルで効果的なメカニズムです。有効性のためにMingerはTCPではなくUDPを使用し、セキュリティについては認証を要求することもでき、一方で匿名でのクエリにも対応しています。Mingerダイアログボックスでは、MDaemonのMingerサーバの有効/無効の指定や、ポート番号の変更(デフォルト値は4069)、共有秘密のシステムを通して認証を要求や匿名のクエリを有無を選択できます。MDaemonにもMingerクライアントがドメインゲートウェイシステム(検証 235参照)に組み込まれています。MDaemonがゲートウェイやバックアップサーバとして稼動しているドメインごとに、Mingerサーバの設定が行えるため、MDaemonは外部サーバへ接続し、受信メールのドメインが正規かどうかを判断できます。この機能で、宛先全部が正規であると誤って判断されることを防ぎます。

以下でMingerプロトコルの最新のドラフトを知ることができます:

http://tools.ietf.org/html/draft-hathcock-minger-06

Mingerサーバ

Mingerサーバを有効にする
MDaemonのMingerサーバを有効にする場合はチェックボックスをクリックします。

このUDPポートをMinger接続でリスンする
これは、Mingerサーバが接続のためにリスンするポートです。Internet Assigned Numbers Authority（IANA）は、Mingerクライアントおよびサーバ用にTCPおよびUDPポート4069を確保し割り当てます。既にMinger用として定義されているポートの変更は推奨していません。

Mingerクエリでは共有キーが必要
非公開システム用に認証を行う場合には、このオプションを選択し、16文字以上のテキストを入力してください。このオプションが選択されていると、Mingerサーバは非認証クエリを拒否します。

Mingerサーバで匿名クエリをサポートする
匿名のMingerクエリをサポートする場合にはこのオプションを選択します。クライアントはアドレス検証前に認証する必要がありません。これはSMTP VRFYコマンドやSMTPの[コールバック]や[コールフォワード]を使った場合に似た動きとなりますが、Mingerはより効果的で、TCPを介してSMTPセッションがドロップされることや、それによるログが大量発生するようなことはありません。

Mingerは外部からのエイリアスを有効なメールアドレスとみなす
このチェックボックスがチェックされる時に、あたかもアクティブな既知のアドレスであるかのように、Minger は外部のエイリアス(外部アドレスに示しているエイリアス)を扱います。同様に、このオプションの設定の状態に関係なくクエリがSecurityGatewayからMDaemonまで到達する時に、この動作は強制されます。

Mingerルックアップ結果をキャッシュする
デフォルトで、MDaemonはMingerルックアップ結果をキャッシュにいれます。キャッシュしない場合、このオプションを無効にします。

5.4 アカウントのインポート

5.4.1 テキストファイルからアカウントをインポート

アカウント ≫ インポート ≫ カンマ区切りのテキストファイルからアカウントをインポート メニューか、アカウントマネージャのインポートボタンのクリックで、このアカウント生成機能へアクセスできます。 この方法は、アカウントをインポートして、そのメールアカウントを自動的に生成することができる簡単な方法です。MDaemonは、テキストファイルを読み込んで、最低限ユーザの苗字か名前があれば、新しいメールアカウントを作成します。アカウントのテンプレート値（ アカウントの作成テンプレート 722を参照して下さい）の適正値を重要視しているのであれば、苗字か名前だけでもユニーク(一意の)アカウントを作成することはできますが、その他の色々なオプションを設定することにより、アカウントの作成のデフォルトを書き換えることができます。すべてのフィールドはカンマで区切ってください。

ユーザーのエントリ毎に1行、テキストをカンマで区切って下さい。最初の行は、列名です。サンプルファイルは以下のようになります。

```
"Mailbox", "FullName", "MailDir", "AllowAccess"
"arvel", "Arvel Hathcock", "C:\Mail\Arvel\", Y
"michael", "Michael Mason", "C:\Mail\Michael\", N
```

1行名にある各行のフィールド名は、MDaemonがデータの紐付けを行うために使用し、順不同で指定できます。各フィールド名には、引用符が必要です。

すべてのString(文字列)値が引用符が必要で、最初の文字にy, Y, 1, t, または Tが含まれない場合は、boolフィールドの値はFALSEとして扱われます。

苗字と名前はそれぞれフルネームとして受け入れられます。しかし、それらにカンマを使用することはできません。

インポート処理を行った後に、MDaemonはTXIMPORT.LOGというファイルを作成します。これには、インポートの結果の詳細(どのアカウントが成功して、どれが失敗したかなど)が含まれます。アカウントのインポートに失敗する一般的な理由としては、既存のアカウントのメールボックス、名前、ディレクトリ情報との競合、または既存のエイリアスとの競合、あるいはメーリングリスト名との競合などが考えられます。

フィールドマッピングに関する詳しい情報は、¥API¥ディレクトリにあるMD-API.HTMLファイルの中のMD_ImportUserInfo()とMD_ExportAllUsers()の記述を参照してください。

以下がMDaemonのアカウントの各フィールドと紐付けできる列名の一覧です:

フィールド名	種類
MailBox	string
Domain	string
FullName	string
MailDir	string
Password	string
AutoDecode	bool
IsForwarding	bool
AllowAccess	bool
AllowChangeViaEmail	bool
KeepForwardedMail	bool
HideFromEveryone	bool
EncryptMail	bool
ApplyQuotas	bool
EnableMultiPOP	bool
MaxMessageCount	int
MaxDiskSpace	int
FwdAddress	string

FwdHost	string
FwdSendAs	string
FwdPort	string
NTAccount	string
MailFormat	string
AutoRespScript	string
AutoRespProcess	string
AddToList	string
RemoveFromList	string
PassMessageToProcess	bool
MaxUIDLCount	int
MaxMessageSize	int
RecurseIMAP	bool
MaxInactive	int
MaxMessageAge	int
MaxDeletedIMAPMessageAge	int
Comments	string
UserDefined	string

参照:

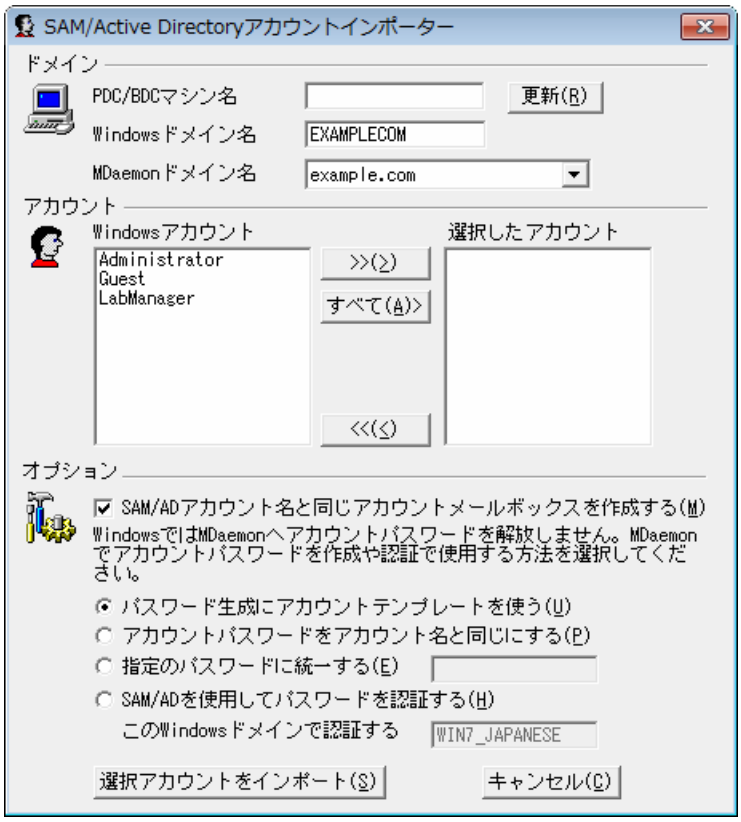
Windowsアカウントの統合 788

5.4.2 Windowsアカウントの統合

MDaemonはWindowsアカウントの統合に対応しています。これにはMDaemonのアカウントメニュー（アカウント ≫ インポート ≫ SAM/Active directoryからアカウントのインポート）からアクセスできるSAM/Active Directoryインポートエンジンが含まれています。更に、ユーザーのActive Directory（AD）認証にも対応しています。Windowsドメインをアカウントのパスワードフィールドに指定する事で、MDaemonはリアルタイムにWindowsセキュリティシステムを使用してアカウントを動的に認証します。こうしたスキームにより、Windowsで変更したアカウントのパスワードでMDaemonのパスワードは常にアップデートされます。そのため、ユーザーは認証情報を一元管理できます。この機能を使う事で、新しくインストールした際のアカウント設定も簡単に行えます。

MDaemonを実行しているアカウントのセキュリティコンテキストは**SE_TCB_NAME**権限（例．“OSの一部として振る舞う”）を含まなくてはなりません。サービスがローカルシステムアカウントで稼働している場合はこの権限がデフォルトです。それ以外の場合は、MDaemonが稼働しているWindowsのユーザーマネージャで権限の設定を行う必要があります。

SAM/Active Directoryアカウント インポーター



ドメイン

PDC/BDCマシン名
このフィールドには、MDaemon がWindowsアカウント データベース情報を読み込むマシン名を指定できます。¥¥<DEFAULT>を指定すると、MDaemonはローカルマシンからデータを読み込みます。

更新
このボタンをクリックすると、Windowsアカウント リストが更新されます。

Windowsドメイン名
アカウントをインポートするドメイン名を入力してください。

MDaemonドメイン名
ドロップダウンリストから、アカウントをインポートするMDaemonドメインを選択してください。

アカウント

Windowsアカウント
このウィンドウには、Windowsアカウント データベースから収集されたすべてのアカウント名が含まれます。

選択アカウント
このウィンドウには、インポートするために選択したすべてのアカウント名が含まれます。

>>
このボタンをクリックすると、選択されたアカウントがWindowsアカウント ウィンドウから**選択アカウント** ウィンドウへ移動します。

<<
このボタンをクリックすると、選択されたアカウントが**選択アカウント** ウィンドウから削除されます。

オプション

SAM/ADアカウント名と同じアカウントメールボックスを作成する
このスイッチは、インポートされたユーザのWindowsアカウント名を、強制的にMDaemonのメールボックスの値として使うようにします。この方法により、アカウントの作成テンプレート 726マクロを正確に設定しなければならない、などの心配がなくなります。

パスワード生成にアカウントテンプレートを使う
このオプションは、アカウントテンプレート設定(アカウントの詳細 726)を使用して、インポートしたアカウント用のパスワードを生成します。

アカウントパスワードをアカウント名と同じセットにする
このスイッチは、アカウント名をアカウントのパスワードとして使用します。

すべてのパスワードを固定する
このスイッチは、すべてのインポートしたアカウントに、静的なパスワード値を指定します。

SAM/ADを使用してパスワードを認証する
このオプションを有効にすると、インポートしたアカウントがAD認証を使用するようになります。指定されたパスワードではなく、MDaemonはNTデータベースから取得したUSERとPASSの値をリアルタイムで取得し認証を行います。

このWindowsドメインで認証する
MDaemonが動的な接続認証を行う時に使用する、Windowsドメインの名前を入力してください。**これは、ドメインコントローラのマシン名ではありません。Windowsドメインの実際の名前です。**

アカウントをADで認証するよう構成すると、最初の¥¥記号に続くWindowsドメイン名が、アカウントのPASSWORDフィールド内で、暗号化されずにUSERLIST.DAT ファイル内に保存されます。例えば、アカウントがALTNと呼ばれるWindowsドメイン上で、AD認証を行うよう構成されていると、アカウントのパスワードフィールドは¥¥ALTNとなります。ドメイン名の前の¥¥記号は、パスワードフィールドが実際にWindows ドメインの名前を含み、メールクライアントによって与えられるUSERおよびPASSの値は、そのドメインのアカウントデータベースを使って認証されることを示します。そのため、アカウントがAD認証を行うよう構成されていない限り、パスワードを¥¥で始めるべきではありません。言い換えれば、通常のパスワードは¥¥で始まってはいけないということです。¥¥で始まるパスワードは、パスワードではなくWindowsドメイン名として扱われます。

アカウント エディタの アカウント の詳 細 650でアカウント のパスワード フィールド に2 つのバックスラッシュおよびW indow sドメイン名 の組 合 せを登 録 すること ができます。アカウント の動 的 認 証 に必 ずしもインポーターを使 用 する必 要 はありません。

参照:

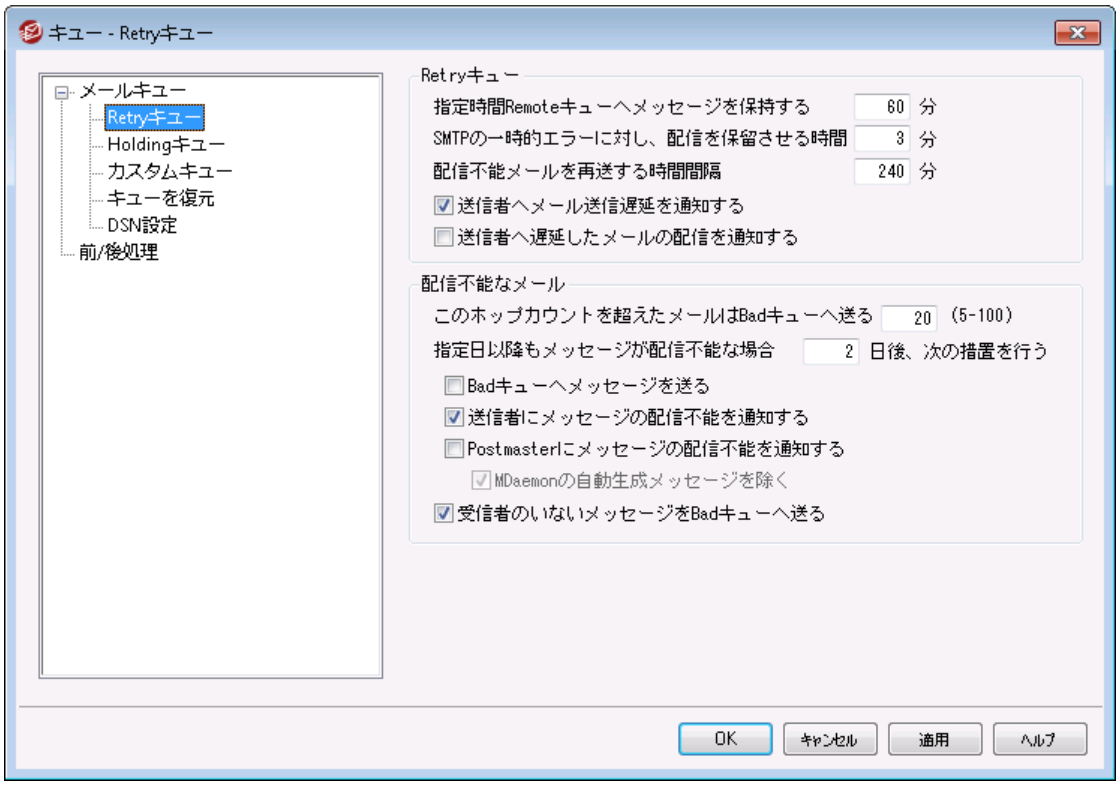
テキストファイルからアカウントをインポート 786
アカウントエディタ ≫ アカウント 650

セクション 6

6 キューメニュー

6.1 メールキュー

6.1.1 Retryキュー



キュー ≫ メールキュー にあるRetryキューダイアログでは、送信先サーバーが一時的に使用できないといった致命的ではないエラーの際、MDaemonが対象のメールをどのように処理するかを設定する事ができます。

Retryキュー

指定時間リモートキューへメッセージを保持するXX分
この設定では、メッセージがリモートキューから削除されリトライキューに置かれる前に、リモートキューに保持する時間を指定します。リモートキューは、一般的にリトライキューより頻繁にメールを配信することを試みます。

SMTPの一時エラーに対し配信を保留する時間　XX分
MDaemonがメール配信時にSMTP一時(4xx)エラーで送信できなかった場合に、ここで指定した時間配信処理を保留します。これはMDaemonがすぐに何度も配信処理を繰り返してしまう事を防ぎます。デフォルトで保留時間は3分と設定されています。保留を無効にする場合は、0を設定してください。

配信に失敗したメールを再送する時間間隔 xx 分
この設定はリトライキューのメッセージがどのくらいの頻度で処理されるかを決定します。

送信者へメール送信遅延を通知
デフォルトでMDaemonはメールが一時的なエラーで送信できず、リトライキューへ配信された場合、送信者へ通知を送ります。遅延についての通知を送信しない場合はこのオプションを無効に設定して下さい。

送信者へ遅延したメールの配信を通知
配信が遅延していたメールが配信された時、通知を行うにはこのオプションを有効にして下さい。これはデフォルトで無効に設定されています。

配信不能メール

このホップカウントを超えたメールをbadキューへ送る (5-100)
RFC標準ではメールサーバーは各メールに処理した時間をスタンプとして残すよう定めています。このスタンプは、設定ミスなどが起因したメールループ対策としてカウントされます。 メールループが把握できていない場合、メールの配信処理が多くのリソースを消費してしまう場合もあります。メールが処理された回数をカウントする事で、このようなメールが検出され、badキューへ配信されます。懸念事項としては、メールが指定回数以上のメールサーバーで処理された場合、宛先に届かず、メールループが続いてしまうという点です。多くの場合、ここではデフォルト値がメールループを防ぐのに最適な設定であり、変更する必要はありません。

指定日以降もメールが配信不能の場合:
この設定では、メッセージが削除される前にリトライキューに残す日数を指定します。ここに0(ゼロ)を指定すると、メッセージは1回だけ送信を行った後、すぐに送信元へ送り返されます。デフォルトは2日間です。

Badキューへメールを送る
このオプションが有効な場合は、メッセージが[メッセージが次の期間配信できない場合]設定で指定された日数に達すると、そのコピーを不正(BAD)メッセージディレクトリに移動します。

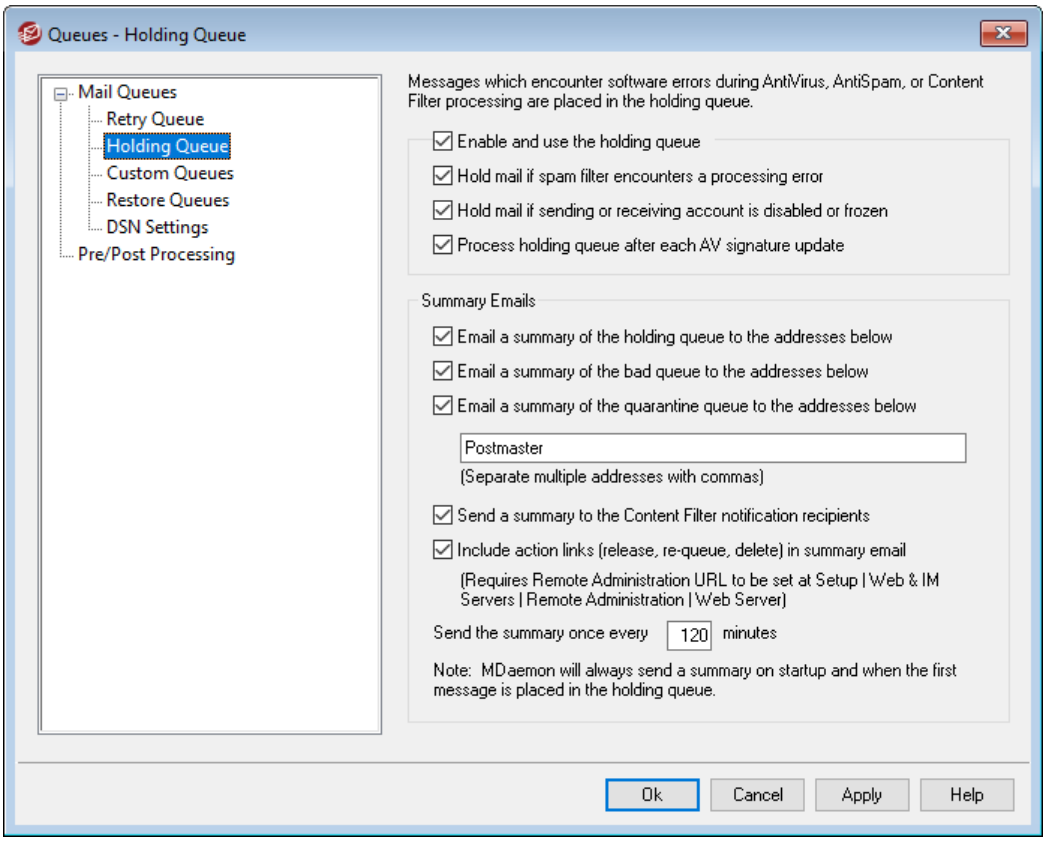
送信者へメールの配信失敗を通知
「指定日以降もメールが配信不能の場合」で設定した限度数に到達したメールがあると、このオプションを有効化する事でMDaemonはメールの送信者へメールがサーバーから削除された旨を通知するDelivery Status Notification 801を送信します。

Postmasterへメールの配信失敗を通知
このスイッチが有効な場合は、メッセージがリトライシステムから削除された時に、Postmasterに通知されます。

....MDaemonの自動生成メッセージを除く
デフォルトで、リトライシステムは、MDaemon自動生成メッセージが配信に失敗した場合にはpostmasterには通知しません。しかし、Postmasterにとっては、そのような情報が役立つ場合があるので、通知する必要がある場合があります。自動で生成されたメールの配信に失敗した場合も、これをPostmasterに通知する場合は、このチェックボックスを解除してください。自動生成メッセージには、返却確認の通知、自動応答生成メッセージ、アカウント処理の結果などがあります。

受信者のいないメッセージをBadキューへ送る
このオプションが有効な時、受信者のいないメッセージはBadキューへ移動されます。このオプションが無効の時、対象メールは削除されます。このオプションはデフォルトで有効です。

6.1.2 Holdingキュー



キュー ≫ メールキューメニューのHoldingキュー は、AntiVirusやアンチスパム、コンテンツフィルタの処理中にエラーを起こすようなメールを受信するのに使用されます。処理中に先のエラーが発生した場合、該当メールはHoldingキューに移動され、配信されることがありません。

管理者が削除するまで、メッセージはHoldingキューに置かれます。[**Holdingキューの処理**]ボタンは、メインユーザ画面と同じくキューメニューにあります。またメイン画面左側のHoldingキューを右クリックしてメニューから[**再度キューに入れる**]を選択することによりメールを処理することもできます。Holdingキューを処理すると、すべてのメールはリモートまたはローカルキューに移動され、通常のメール処理が行われます。メールがHoldingキューに送られる原因となったエラーがまだ存在する場合、メールは再びHoldingキューに戻されます。エラーの発生を無視してメールを配信する場合は、メイン画面左側のHoldingキューを右クリックして、メニューから[**解放**]を選択することにより、そのメールを配信することができます。Holdingキューからメールを解放する際には、メールにウィルスを含む可能性がある、あるいはコンテンツフィルタのアンチスパムやアンチウィルスエンジンによって適切にフィルタリングされないことを確認するダイアログが表示されます。

Holdingキュー

Holdingキューを有効にする
Holdingキューを使用するには、このチェックボックスを有効にしてください。AntiVirusやコンテンツフィルタの処理中に、ソフトウェア例外を引き起こすようなメールがこのキューに移動されます。

スパムフィルタ処理にてエラーが発生した場合メールを保留する
スパムフィルタのエラー発生時、メールをHoldingキューへ移動する場合は、このオプションを有効にしてください。

送信または受信するアカウントが無効化または凍結されていた場合、メールを保留する
このオプションが有効の場合、MDaemonは送信または受信するアカウントが無効化や凍結されていた場合にメールを保留します。

各AV署名更新後Holdingキューを処理する
このオプションを有効にすると、AntiVirus[587]のウィルスシグネチャが更新されるごとに、自動的にHoldingキューが処理されます。

サマリーメール

次のアドレスへHoldingキュー内のメッセージサマリーを送信
Holdingキューのサマリーを定期的に1つかそれ以上のアドレスに対してメールで送信するにはこのオプションを選択し、下のスペースへアドレスを入力します。

次のアドレスへBadキュー内のメッセージサマリーを送信
Badキューのサマリーを定期的に1つかそれ以上のアドレスに対してメールで送信するにはこのオプションを選択し、下のスペースへアドレスを入力します。

次のアドレスへ隔離キュー内のメッセージサマリーを送信
隔離キューのサマリーを定期的に1つかそれ以上のアドレスに対してメールで送信するにはこのオプションを選択し、下のスペースへアドレスを入力します。

サマリーメールの宛先
Holdingキューに含まれるメールのサマリを一定の間隔でメール送信する場合は、チェックボックスを有効にして、送信先のアドレスを入力してください。複数のアドレスを指定する場合は、カンマで区切って入力してください。

通知メールはMDaemonの起動時、Holdingキューに最初にメールが入った時、そして下にある[**サマリーを次の時間ごとに送る**]オプションで指定された間隔で送信されます。

この通知メールがソフトウェアエラーを引き起こすような場合、リモートの宛先へは通知が送られない場合があります。その場合でも、ローカルの宛先には通知メールが送られます。

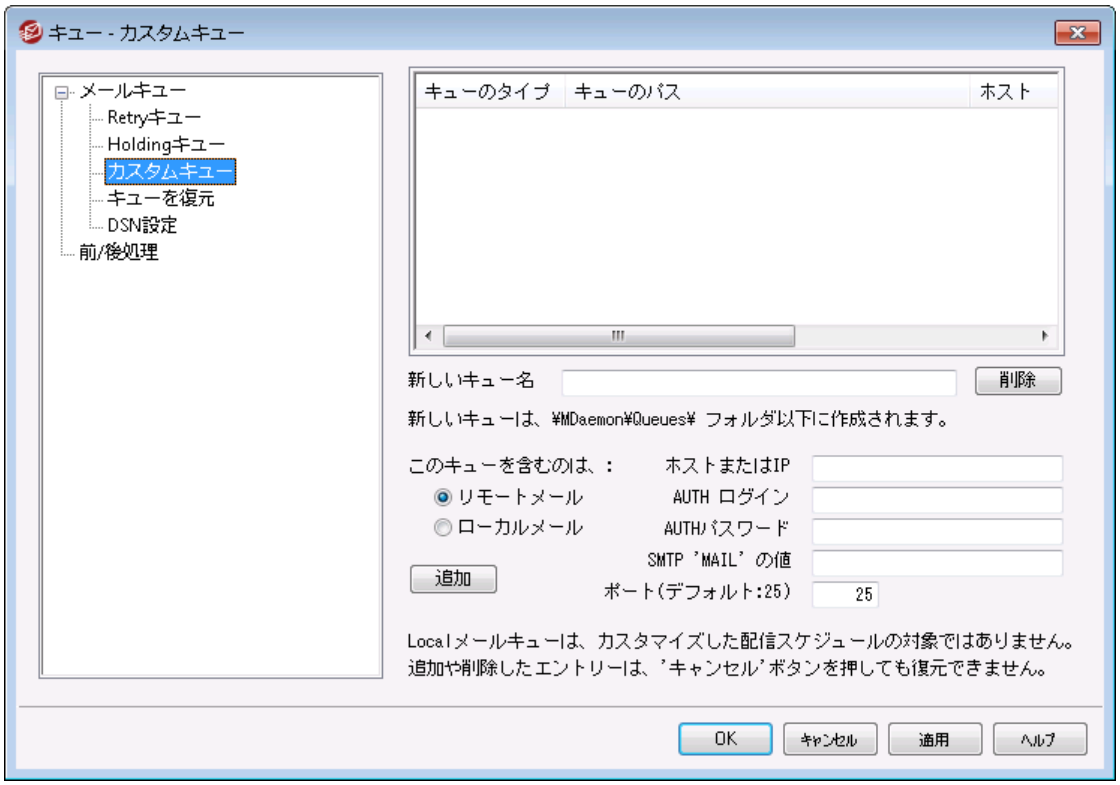
コンテンツフィルタの通知受信者へサマリーを送信
通知メールのコピーをコンテンツフィルタの通知受信者[606]にも送信する場合は、このオプションを有効にしてください。

サマリーメール内へアクションリンク(開放、再度キューに入れる、削除)を含む
デフォルトで、holding、隔離、Badキューについてのサマリーメールには、開放、再度キューへ入れる、削除、のリンクが、それぞれのメール用に使用されています。サマリーメールでリンクを表示させないようにするには、このオプションを無効にしてください。

> リンクを生成するには Remote Administration URL 322 を設定しておく必要があります。

サマリーを次の時間ごとに送る XX 分
MDaemonからHoldingキューの通知メールを指定した宛先やコンテンツフィルタの宛先に送るまでの間隔をここで指定します。

6.1.3 カスタムキュー



ローカルやリモート用のカスタムメールキューは、キュー ≫ メールキューで作成します。カスタムキューに対応している事で、MDaemonは、メール送信用の複数のロケーションを監視する事ができます。新規のキューを作成しローカルまたはリモートを指定することができます。また、メッセージをカスタムメールキューに自動的に配置するコンテンツフィルタルールの使用もでき、リモートキューについて、キューでの処理を行う頻度をコントロールするカスタムスケジュールを作成するイベントスケジューラ 347 を使用することができます。

カスタムキュー

ここへはそれぞれのカスタムキューのエントリが表示され、ファイルパスとキューがローカルかリモートかを確認できます。

削除
リストからキューを削除する場合は、対象エントリを選択し、**削除**ボタンをクリックしてください。

カスタムキューを削除すると、これに対応したカスタムスケジューラやコンテンツフィルタのルールなども削除されます。

新規キュー名称
新しいメールキューの名称を入力します。キューはMDaemonの ¥MDaemon¥Queues¥ フォルダへ作成されます。

このキューは次の選択を含む...

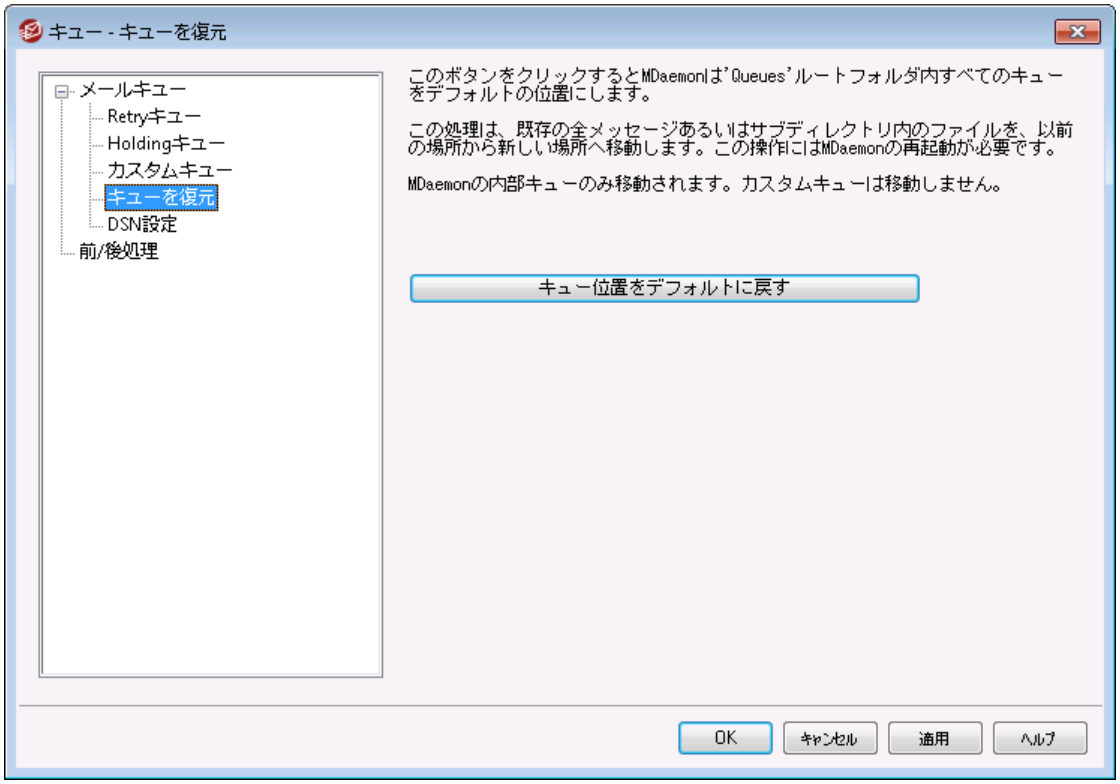
...リモートメール
カスタムメールキューをリモートで使用する場合は、このオプションを選択してください。

キュー認証情報
リモートキュー用の*ホスト名又はIP*, *AUTHログオン/パスワード*, *SMTP 'MAIL'値*, *ポート* をここで指定します。指定された場合、キューの中メール配信にはこの設定が使用されます。ただし、環境によってはキューの中のメール毎に独自の配信用データを保持している場合もあり、その場合、独自のデータがここでの設定よりも優先されます。

...ローカルメール
カスタムメールキューをローカルで使用する場合は、このオプションを選択してください。 **注意点**: ローカルメールキューはカスタム配信スケジュールの対象外です。

追加
名前とキューのタイプを選択し、**追加**ボタンをクリックすると、カスタムキューのリストに追加されます。

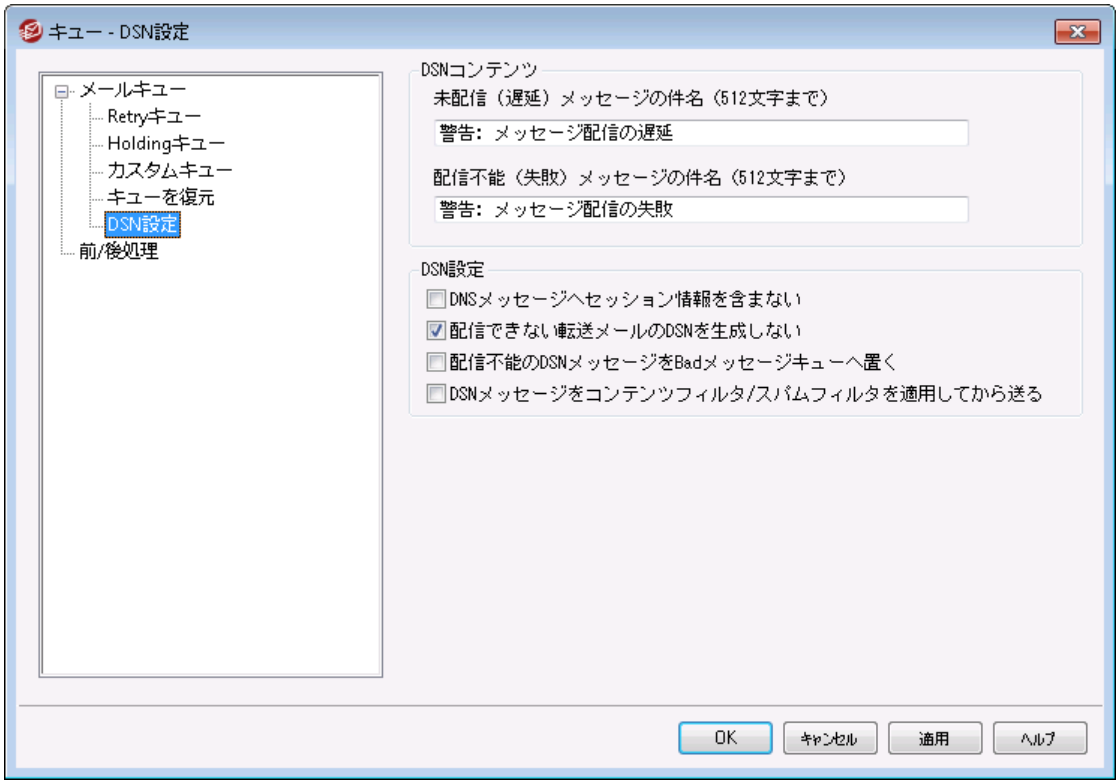
6.1.4 キューを復元



キュー位置をデフォルトに戻す
新規MDaemonインストール時のデフォルトでは、Remote, Local, Rawなどのメッセージキューを¥MDaemon¥Queues¥に保存します。以前のバージョンのMDaemonでは他の場所に保存されていました。インストールされたMDaemonが古いフォルダロケーションを使用していて、新しい場所にメッセージキューを移動する場合は、このボタンをクリックすれば、すべてのキューとファイルおよびメッセージが自動的に移動されます。この変更を有効にするためにはMDaemonを再起動する必要があります。

カスタムキュー[798]は、この操作では移動できません。

6.1.5 DSN設定



MDaemonでは、一時的又は恒久的に、メッセージ配信で問題が生じた場合、不達メール（DSN）をメールの送信者へ送ります。この画面ではDSNメッセージに関連する様々なオプションが設定できます。この画面へは、キュー ≫ メールキュー/DSN... ≫ DSN設定からアクセスできます。

DSNコンテンツ

未配信（遅延）メッセージの件名（512文字まで）
配送時の問題によりメール送信が遅延している場合に送信されるDSNメッセージの件名を指定します。例えば、MDaemonがメール送信しようとした際、受信側のメールサーバーが応答しない場合などに、MDaemonは再送を試みた上で、このDSNメッセージをメールの送信元へ送ります。DSNメールのカスタマイズ 802 を参照して下さい。

配信不能（失敗）メッセージの件名（512文字まで）
MDaemonがメール配信できない問題があった場合に送信するDSNメッセージの件名を指定します。例えば、宛先メールアドレスが存在しないため、受信側のメールサーバーがメッセージを拒否した場合等に、MDaemonは配信をやめ、このDSNメッセージを送信元へ送ります。DSNメールのカスタマイズ 802 を参照して下さい。

DSN設定

DSNメッセージへセッション情報を含まない
配信エラーや警告メッセージを含むSMTPセッション情報をメッセージに入れない場合はこのオプションをクリックします。このオプションはデフォルトで無効になっています。

配信できない転送メールのDSNを生成しない
このオプションが有効な時、転送メールが配信不能や失敗、期限切れを起こした場合は Retryキュー[794] からBadキューへメールを移動し、元の送信者にはDSNメッセージの配信を行いません。このオプションはデフォルトで有効になっています。

配信不能なDSNメールをBadキューへ配信する
配信不能なDelivery Status Notificationメールを再配信するのではなくBadキューへ配信する場合はこのオプションを選択します。

この設定はMDaemonが生成したDSNメールに対してのみ適用されます。

DSNメールをコンテンツフィルタやスパムフィルタ経由で送信
DSNメールをコンテンツフィルタやスパムフィルタ経由で配信するにはこのオプションを有効にします。このオプションはデフォルトで無効になっています。

DSNメールのカスタマイズ

遅延したり配信に失敗した「読み取り可能な」DSNメールは `\MDaemon\App\` フォルダへ `DSNDelay.dat` や DSNFail.datというファイルを生成する事でカスタマイズできます。これをNotepadなどのテキストエディタで編集し、使いたいテキストを入力します。次のマクロがカスタムテキストとして利用できます:

$SESSIONID$ - 配信時のセッションID値に置き換えられます

$QUEUEID$ - メールのメールキューID値に置き換えられます

$MESSAGEID$ - message-idヘッダ値へ置き換えられます

$RETRYDAYS$ - キューに保持できる時間(日)に置き換えられます

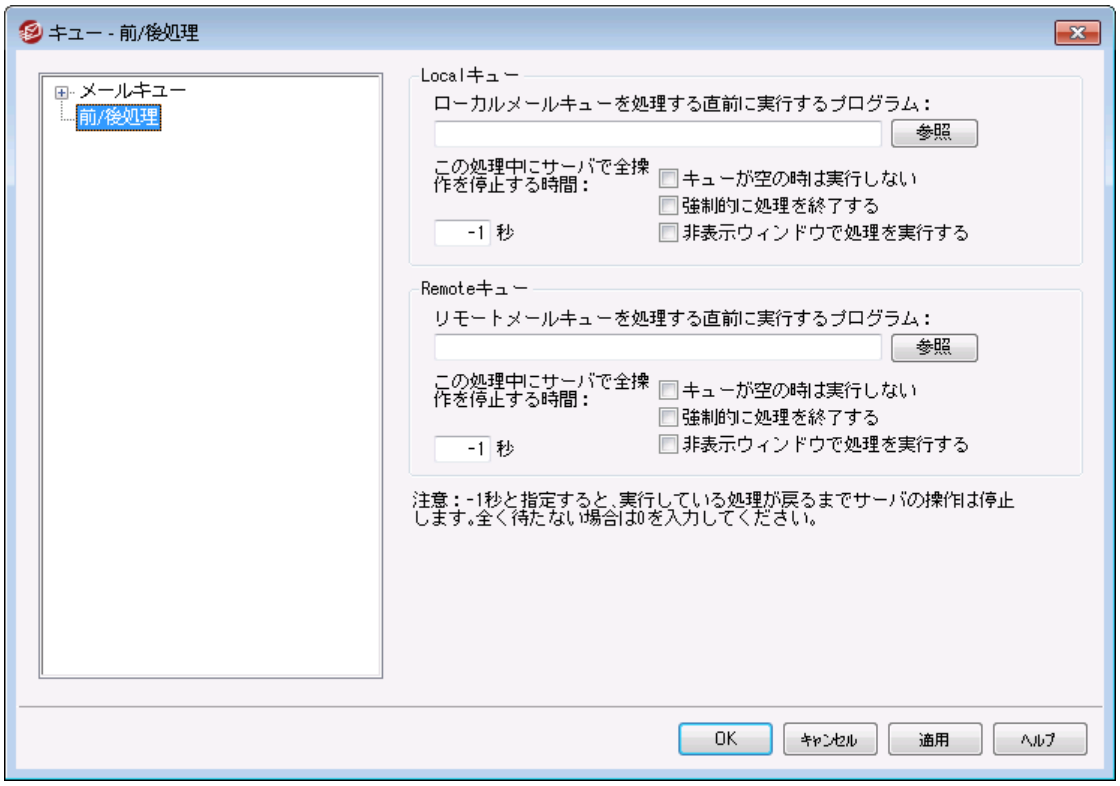
$RETRYHOURS$ - キューに保持できる時間(時間)に置き換えられます

ファイルをロードするにはMDaemonを再起動する必要があります。

参照:

Retryキュー[794]

6.2 前/後処理



ローカルキューとリモート キュー前 / 後 処 理

ローカル/リモート キューを処 理 する直 前 に実 行 するプログラム
このフィールドは、ローカルまたはリモート のメッセージキューにある、RFC-2822メッセージの処 理 と配信 の直 前 に実 行 される、プログラム名 とそのプログラムへのパスを指 定 します。その実 行 ファイルへの完 全 なパスの情 報 が分 からない場 合 は、MDaemonは最 初 に、MDaemonディレクトリ、そしてWindows Systemディレクトリ、Windowsディレクトリと検 索 して、最 後 にPATH環 境 変 数 でリストアップされているディレクトリを検 索 します。

...この処 理 中 にサーバで全 操 作 を停 止 する時 間
ここで入 力 された値 は、指 定 されたプログラムが実 行 している間 、MDaemonがどのように動 作 するかを決 定 します。MDaemonは、プログラム処 理 スレッドの戻 り待 つ間 、ここで指 定 した秒 数 だけ、自分 の処 理 を停 止 するように構 成 することができます。指 定 した秒 数 以 内 にプログラムの処 理 が戻 ってきた場 合 、MDaemonは即 座 に自 分 の処 理 を開 始 します。この値 に0(ゼロ)を入 力 した場 合 、MDaemonは一 切 操 作 を停 止 しません。この値 に[-1]を入 力 した場 合 、MDaemonは、いくらプログラムの処 理 に時 間 がかかろうと、処 理 が戻 るまで自 分 の処 理 を停 止 します。

キューが空 の時 は実 行 しない
キューが空 の時 に、指 定 したプログラムを実 行 させたくない場 合 は、このオプションを有 効 にしてください。

強制的に処理を終了する
時々、実行しているプロセスが、自分でシャットダウンしない場合があります。このオプションは、[この処理中にサーバで全操作を停止する時間]で指定された時間を経過すると、MDaemonに強制的にセッションを終了させます。この値が -1 に設定されている場合、このオプションは作動しません。

非表示ウィンドウで処理を実行する
プロセスウィンドウを最小化して実行する場合は、このチェックボックスを有効にしてください。

6.3 キュー/統計マネージャ

MDaemonのキューと統計マネージャはキュー» キュー/統計マネージャ メニューを選択することによってアクセスすることが可能です。キューと統計マネージャには、4つの画面があります。それぞれの画面は、特定の目的のために明確に作業できるようにデザインされ、きわめて使い易いシンプルな構成です。

キューページ 805

デフォルトの画面はキューページです。このページからMDaemonのすべての標準メールキューおよびユーザアカウント メールボックスフォルダを簡単に管理できます。任意のキューまたはユーザをクリックするだけで、指定されたキューに含まれるすべてのメッセージのリストが、各メッセージの関連情報とともに表示されます。この関連情報は、送信者、受信者、[Deliver-To]ヘッダの内容、メッセージの件名、サイズなどです。また、フォルダ間のメッセージの移動およびコピー、あるいはメッセージの削除を簡単にするコントロールも提供されています。

ユーザページ 807

デフォルト画面はキューページです。このページからMDaemonのすべての標準メールキューおよびユーザアカウント メールボックスフォルダを簡単に管理できます。任意のキューまたはユーザをクリックするだけで、指定されたキューに含まれるすべてのメッセージのリストが、各メッセージの関連情報とともに表示されます。この関連情報は、送信者、受信者、[Deliver-To]ヘッダの内容、メッセージの件名、サイズ、などです。また、フォルダ間のメッセージの移動およびコピー、あるいはメッセージの削除を簡単にするコントロールも提供されています。

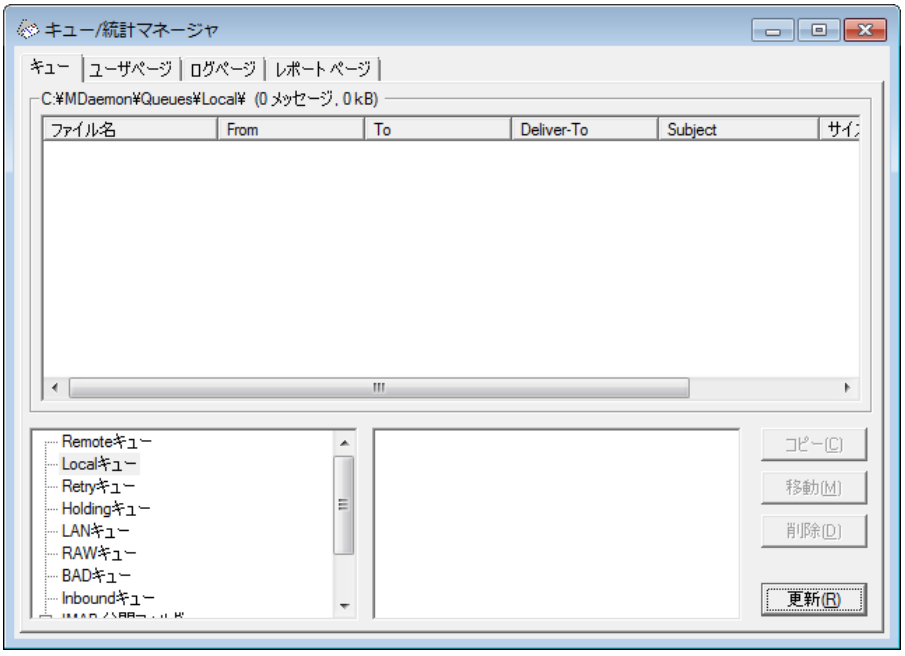
ログページ 809

このダイアログにより MDaemonのログファイルをシンプルなリスト形式で表示することが可能です。この機能は、選択されたログファイルをコラムリストに要約するため、MDaemon のメール処理の履歴を素早く確認することができます。コラムリストには、メッセージのタイプ(内部向けPOP、DomainPOP、RFC-2822、など)、メール処理中に接続されているホスト、送信者、受信者、メッセージサイズ、各メッセージが処理された日付、処理が成功したかどうか、などが含まれています。また、リストのエントリに関するログの詳細部分も、目的のエントリをダブルクリックするだけで確認することが可能です。これにより、処理が行われたログの一部が表示されます。ログページで表示されるログは、テキストファイルとして保存が可能ですが、データベースに使用するためにカンマ区切り形式で保存することもできます。

レポート ページ 811

最後のタブはレポート ページです。この機能により、すべてのMDaemonの構成設定を含む、プレーンテキスト形式のレポートを作成することができます。MDaemonにはオプション設定および構成の数が多いので、この機能により構成の変更を管理する処理のスピードアップを図ることができ、また構成の問題点を診断する補助にもなります。さらに、このレポートは含まれる情報のコピーや貼り付け(右クリックのショートカットメニューを使用)ができる、編集可能なテキスト形式で表示されます。また、レポートを保存する前に注釈や他の情報をファイルに追加することも可能です。

6.3.1 キューページ



キューページのリスト ボックス

キューまたはユーザがメッセージキューエリアまたはユーザー 覧 ボックスから選 択される場 合 、選 択されたキュー内 で含 まれているすべてのメッセージファイルの一 覧 はこのページでメインリスト ボックスで表 示されます。このリスト には、各 メッセージのファイル名 、送 信 者 、受 信 者 、[Deliver-To]ヘッダの内 容 、メッセージの件 名 、サイズ、および現 在 の場 所 にいつからあるか(日 付 および時 間 でリスト される) が含 まれています。

このボックスの上 には、現 在 表 示されているディレクト リへの完 全 なファイルパスと同 時 に、表 示されているメッセージ数 およびディレクト リのサイズも表 示されます。

1 つ以 上 のファイルをリスト から選 択し、その下 の対 応 するボタンをクリックすることによってコピー、移 動 、または削 除 することができます。

また、これらのファイルはキューページのリスト ボックスから直 接 編 集 することもできます。編 集 するファイルをダブルクリック(または右 クリックショート カット から[編 集]を選 択) すると、W i n d o w sのメモ帳 で開 かれ編 集 可 能 になります。

キューと統 計 マネージャでデフォルト として、メモ帳 以 外 のエディタでファイルを開 きたい場 合 は、¥MDaemon¥app¥ディレクト リにある[mdstats.ini]ファイルを編 集 してください。[QueueOptions]セクションの Editor= キーを Editor=MyEditor.exe に変 更 します。

*.exeファイルのパスがカレント パスでない場 合 は、ファイル名 の一 部 としてそのパスを含 める必 要 があります。

リスト ボックス内 では、縦 横 のスクロールバーを使 用して移 動 するか、リスト ボックスをクリックし矢 印 キーを使 用して移 動 することができます。キューページのリスト ボックスに含 まれる情 報 は、列 を選 択してソートすることが可 能 です。リスト をソート する列 の見 出しをクリックすることで列 を昇 順 でソート します。同 じ列

の見出しを再度クリックすると降順でソートします。また、ポインタを列見出しの間の線上に置き、両向きの矢印になったらドラッグして、その列のサイズを変更することも可能です。

ファイルの選択

ファイルを個別に選択 目的のファイルをクリックします。

連続する複数ファイルの選択 連続するファイルのリストで選択する最初のファイルをクリックし、SHIFT キーを押しながら連続するファイルのリストで最後のファイルをクリックしてください。
あるいは、SHIFT キーを押しながら、矢印、HOME、END、PAGE UP、PAGE DOWNキーを使用することもできます。

連続しない複数ファイルの選択 ファイルリストからファイル選択時にCTRLキーを押しながらクリックしてください。

メッセージキュー

この左下のフィールド内のエントリをクリックすると、指定されたキューに含まれる全ファイルのリストがキューページのリストボックスに表示されます。ユーザフォルダ オプションをクリックした場合、メッセージキューセクションの右側にあるユーザリストボックスにMDaemonの全ユーザのリストが表示されます。

ユーザリストボックス

このボックスには、メッセージキューセクション(左下のペイン)でユーザフォルダ オプションがクリックされた時に、MDaemonの全ユーザのリストが表示されます。ユーザ名をクリックすると、ユーザのメールボックスフォルダに入っているすべてのメッセージファイルが表示されます。

更新

MDaemonが稼動している場合、メッセージファイルは常に転送され続けるのでメールキューは動的に変化します。そのため、定期的にこのボタンを押して、表示されるファイルのリストを更新してください。

[MDstats.ini]ファイルを編集すると、表示されるリストを自動的に更新することができます。MDaemonの¥app¥ディレクトリにある[MDstats.ini]ファイルを開き、[QueueOptions]セクションの[AutoRefresh]キーを編集して、次の更新までの経過秒数を設定します。ここに0(ゼロ)を入力すると、リストは自動的に更新されなくなります。

例: AutoRefresh=15 (リストは15秒ごとに更新されます)

コピー

1つ以上のファイルが選択されている場合、ファイルを別のキューまたはユーザのメールボックスフォルダにコピーするにはこのボタンをクリックしてください。このボタンをクリックすると、メッセージのコピーダイアログが開きますので、そこで選択したファイルのコピー先を指定してください。

移動

1つ以上のファイルが選択されている場合、ファイルを別のキューまたはユーザのメールボックスフォルダに移動するにはこのボタンをクリックしてください。このボタンをクリックすると、メッセージの移動ダイアログが開きますので、そこで選択したファイルの移動先を指定してください。

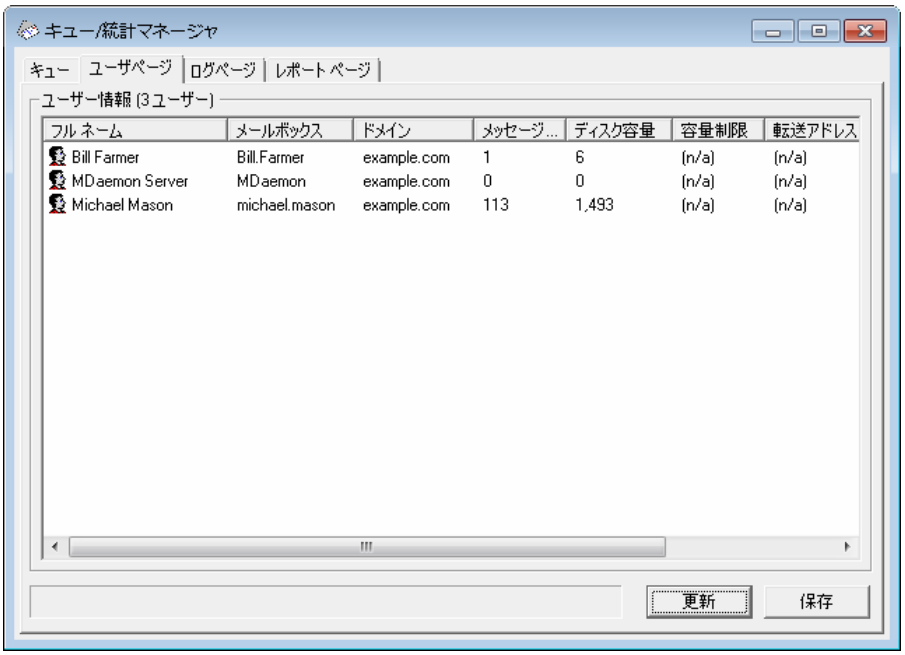
他のキューにコピーあるいは移動されたファイルは、元のファイル名を保持しない場合が多くあります。コピー先のキューにすでに存在する同じ名前のファイルを上書きしないように、MDaemonは常に次に使えるファイル名の候補を計算しています。これはコピー先のフォルダにあるHIWATER.MRKによって計算されます。

削除
1つ以上のファイルがキューステータスリストボックスで選択されている場合、そのファイルを削除するにはこのボタンをクリックしてください。このボタンをクリックすると、選択されたファイルを本当に削除するかを尋ねる確認ボックスが開きます。

MDaemonの稼動中は、メッセージファイルが絶えず転送され続けているので、メールキューは動的に変化します。そのため、ファイルをコピー、移動、または削除する際に[試行するアクションが完了できません]というメッセージを受ける場合があります。これは目的のアクションが開始される前に、作業しようとしているメッセージファイルがすでにMDaemonによって削除されている場合に起こります。[更新]ボタンをクリックすることにより、リストボックスに表示されている現在のファイルのリストを更新することができます。

メッセージの編集中にそのメッセージがキューから送り出されることを防ぐためには、[Mdstats.ini]ファイルを編集してください。MDaemonの¥app¥ディレクトリにある[Mdstats.ini]ファイルを開き、[QueueOptions]セクションのLockOnEdit=No キーを LockOnEdit=Yes に変更します。これにより、メッセージの編集中には必ずLCKファイルが作成されることになり、編集が完了するまでメッセージはキューから送り出されることがありません。

6.3.2 ユーザページ



ユーザ情報
ユーザページでは、MDaemonの全アカウントがユーザ情報のボックスの中に一覧表示されています。ここには、各ユーザのフルネーム、メールボックス名、アカウントが属するドメイン、メールボックスの中のメッセージ数、メール形式、アカウントが使用するディスク容量(キロバイト単位)、転送アドレス、最後にメールがチェックされた日付などの情報が含まれています。表示されている情報は絶えず変化しているので、[更新]ボタンをクリックして情報を更新してください。

リストボックス内では、縦横のスクロールバーを使用して移動するか、リストボックスをクリックし矢印キーを使用して移動することができます。ユーザ情報リストボックスに含まれる情報は、列を選択してソートすることが可能です。リストをソートする列の見出しをクリックすると、列の昇順(A-Z)でソートされます。同じ列の見出しを再度クリックすると、次にリストは降順(Z-A)でソートされます。また、ポインタを列見出しの間の線上に置き、両向きの矢印になったらドラッグして、その列のサイズを変更することも可能です。さらに、エントリをダブルクリックするとMDStatsはキューページに移動して、メールボックスフォルダのコンテンツを表示します。

この一覧では、デフォルトではファイル数ではなくメール本数を表示しており、また、サイズも、ディレクトリの全てのファイルを含んだ容量ではなく、メールが使用しているディスク容量を表示しています。これはMDaemonがレポートするクォータ情報です。メールだけでなく全てのファイルの数や全てのファイルを含んだディスク容量を表示するよう設定変更も行えます。その場合は、MDaemonの¥app¥ディレクトリにある[MDstats.ini]ファイルを開き、[UserOptions]セクションのShowQuota=Yes キーをShowQuota=No に変更してください。

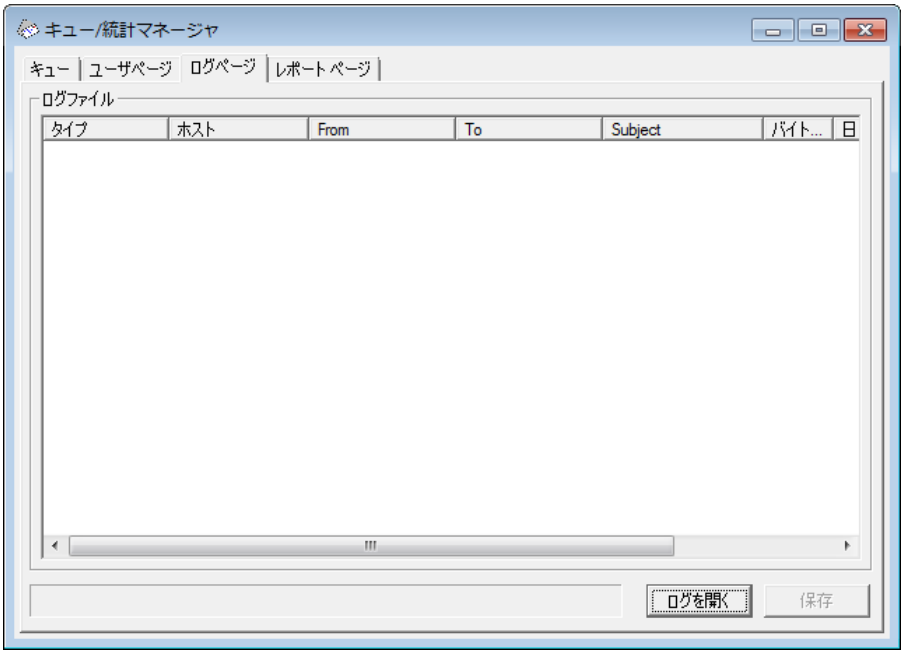
ユーザ情報を判断するために読み込む[hiwater.mrk]というファイルがユーザフォルダにあります。キューおよび統計マネージャのユーザ情報が正しく表示できなくなる恐れがありますので、不必要にこのファイルを削除しないでください。

更新
メールボックスに含まれるメッセージ数、およびアカウントが消費するディスク容量などのユーザ情報は常に変化しています。ユーザ情報リストボックス内の情報を簡単に更新するには[更新]ボタンをクリックしてください。これにより、表示されている情報が即座に更新されます。

インジケーター
ユーザ情報リストは時に非常に大きくなるため、ユーザ情報リストボックスの下には、大きなファイルがロードされる時にプログラムが実行中であることを視覚的に示すインジケーターがあります。

保存
ユーザ情報リストボックスに含まれる情報は、データベースに使用するためにカンマ区切り形式で保存することができます。あるいはプレーンなASCII テキストファイルとしても保存が可能です。データを保存するには[保存]ボタンをクリックしてください。Windowsの[名前を付けて保存]ダイアログで、ファイル名および保存場所を指定した後、ファイルをカンマ区切り形式またはプレーンなテキストファイルのどちらで保存するかを尋ねてきます。

6.3.3 ログページ



ログレポート
ログレポートリストボックスは、[ログを開く]ボタンと、その後のWindowsのファイルダイアログから選択したMDaemonのログファイルの詳細を表示します。ログレポート画面では、非常に大きなログ情報を含むMDaemonが行ったメール処理の履歴を、ソートすることなく簡単かつ素早く確認することができます。このリストボックスには、色々な情報をシンプルな形式に振り分けた内容が表示されます。その内訳には、メッセージのタイプ(内部向けPOP、DomainPOP、RFC-2822など)、メール処理中にMDaemonが接続しているホスト、送信者、受信者、メッセージサイズ、メッセージが処理された日付、および処理が成功したかどうか、などが含まれています。

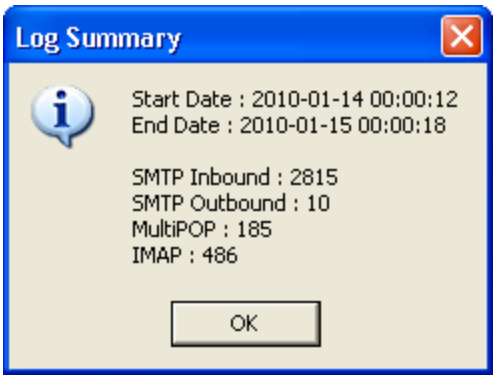
また、リスト内のエントリをダブルクリックすると、そのエントリのログに関する詳細な情報を見ることができます。これは、処理が行われた際のログの一部を表示するものです。右クリックのショートカットメニューを使用すれば、このログの詳細をテキストエディタにコピーや貼り付け、保存、編集することが可能です。

リストボックス内では、縦横のスクロールバーを使用して移動するか、リストボックスのどこかをクリックし矢印キーを使用して移動することができます。また、ポインタを列見出しの間の線上に置き、両向きの矢印になったらドラッグして、その列のサイズを変更することも可能です。

ログページでは、MDaemonのロギング≫ ログモードで選択できる[**メールセッションの詳細をログ**]または[**メールセッションの概要をログ**]のオプションを使用して、編集されたログファイルを表示することができます。しかし[**メールセッションの概要をログ**]オプションではなく、[**メールセッションの詳細をログ**]オプションを使用することを強く推奨します。[**メールセッションの概要をログ**]形式を使用する場合、ログレポートには表示される情報は非常に少ないものになります。またログページそのものが、詳細ログをMDaemonのアクティビティのサマリ表示に要約しますが、必要に応じて(エントリをダブルクリックすることで)各処理の詳細を表示することもできます。

ログを開く
Windowsの[開く]ダイアログを開き、表示するログファイルを選択するにはこのボタンをクリックしてください。すでにログファイルがログレポートリストボックスに表示されている時にこのボタンをクリックすると、すでに表示されているファイルに新しいファイルを追加するオプションを提供します。

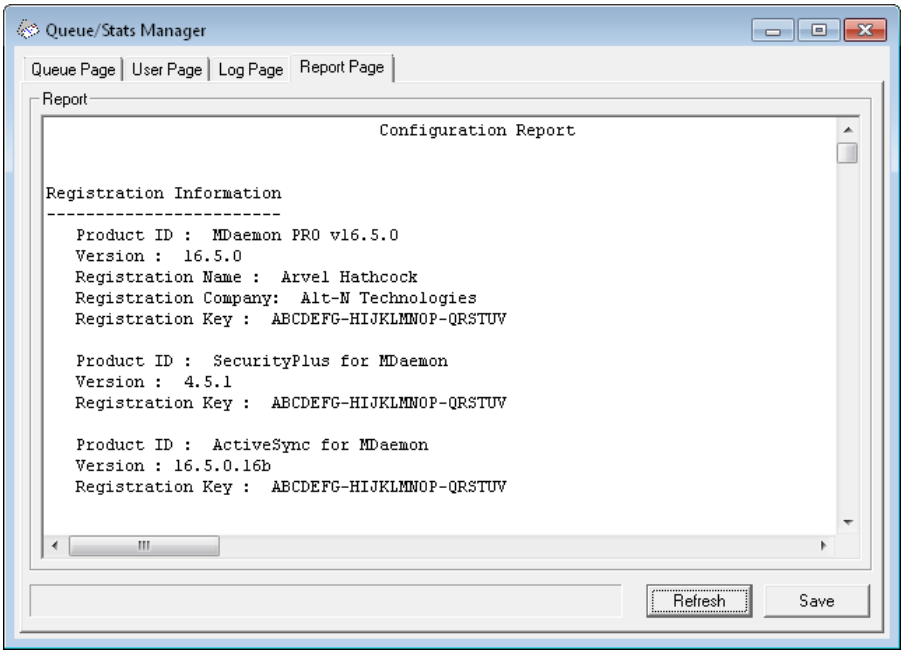
ログが表示された後、選択されたログのサマリを含むメッセージボックスが開きます。ログレポートをテキストファイルとして保存と、ログサマリはこれに追加されます。



インジケーター
ログファイルは時に非常に大きくなるため、ログレポートリストボックスの下には、大きなファイルがロードあるいは保存される時にプログラムが実行中であることを視覚的に示すインジケーターがあります。

保存
ログファイルリストボックスに含まれる情報は、データベースに使用するためにカンマ区切り形式で保存することができます。あるいはプレーンなASCIIテキストファイルとしても保存が可能です。データを保存するには[保存]ボタンをクリックしてください。Windowsの[名前を付けて保存]ダイアログで、ファイル名および保存場所を指定した後、ファイルをカンマ区切り形式またはプレーンなテキストファイルのどちらで保存するかを尋ねてきます。

6.3.4 レポートページ



レポート
レポートページを開くと、MDaemon内のすべての設定をリストする包括的なレポートを読みやすいテキストフォーマットで作成します。この機能は、管理者がMDaemonの多くの設定内容をチェックする時間を大幅に短縮し、考えられる構成の問題点を素早く解決する補助にもなります。

このレポートを移動するには、スクロールバーまたはカーソルキーを使用してください。また、レポート表示はテキストエディタでもあり、ファイルに保存する前にレポートに表記する注釈や特記事項の挿入も可能です。さらに、マウスを右クリックし開くメニューから選択を行ったり、ショートカットメニューを使用して、この画面からまたはこの画面への切り取り、コピー、および貼り付けなども行うことができます。

更新
このボタンをクリックすると、現在表示されているMDaemon設定のレポートを更新することができます。

インジケーター
キューと統計マネージャの他の画面と同様、レポートページにも大きなファイルがロードまたは保存される時にプログラムが実行中であることを視覚的に示すインジケーターがあります。

保存
現在表示されているレポートを保存するには、このボタンをクリックしてください。このボタンをクリックすると、標準の[名前を付けて保存]ダイアログが開きますので、ファイル名と保存場所を指定してください。

6.3.5 キューと統計マネージャのカスタマイズ

6.3.5.1 MDstats.ini ファイル

キュー/統計マネージャのカスタマイズ

以下は、MDaemonの¥app¥ディレクトリにある[MDstats.ini]ファイルで変更可能な設定のリストです。

[MDaemon]

AppDir=C: \mdaemon\app\	MDaemonの¥app¥ディレクトリの場所です。

[QueueOptions]

Editor=NOTEPAD.EXE	メッセージがダブルクリックされたとき、または右クリックで編集が選択された時に使用するエディタを指定します。
LockOnEdit=No	メッセージを編集する際にLCKファイルを作成するかどうかを指定します。これによりメッセージの編集中にそのメッセージがキューから送り出されることを防ぎます。
AutoRefresh=Yes	メッセージリストの次回の自動更新までの時間(秒単位)です。 0(ゼロ)は自動更新を行いません。
ShowDirectories=Yes	リストボックスにメッセージと共にキューのサブディレクトリを表示します。ディレクトリは<DirectoryName>として表示されます。

[UserOptions]

ShowQuota=Yes	ユーザリストにクォータ情報(MDaemonが計算するのと同様のメッセージカウントおよびディスク容量)を表示するか、またはファイル情報(ファイル数および合計ディスク容量)を表示するかを決定します。

[LogOptions]

ShowUnknown=Yes	MDStatsが、内部向けまたは外部向け、SMTPまたはPOPかを決定できなかったセッションを表示します。
ShowSmtpInbound=Yes	MDStatsが、内部向けまたは外部向け、SMTPまたはPOPかを決定できなかったセッションを表示します。
ShowPopInbound=Yes	内部向けPOPセッションを表示します(メールチェック)
ShowSmtpOutbound=Yes	外部向けSMTPセッションを表示します。
ShowPopOutbound=Yes	外部向けPOPセッション(MultiPOP、DomainPOP)を表示します。

ShowRFC822=Yes	RFC822ローカルメール配信を表示します。
ShowSmtpHelo=Yes	内部向けSMTPセッションにおける、ホストコラムのHELOドメインを表示します。
IgnoreEmptyPop=Yes	メールの配信がないときはメールチェックを無視します。
ShowImap=Yes	IMAPセッションを表示します。
[Remap]	ドライブ文字を再度マッピングします: MDaemonを実行中のマシンとは別のマシンからMDStatsを実行するため。
C:=\\server\c	MDaemon.iniから読み込む際に、C: を ¥¥server¥c に置き換えます。
[Special]	
OnlyOneInstance=No	MDStatsのいずれか1つのインスタンスのみを実行します。再度開こうとすると、すでに実行されているインスタンスをアクティブにすることになります。

参照:

MDStatsコマンドラインパラメータ 813

6.3.5.2 MDStatsコマンドラインパラメータ

注意: すべてのコマンドは大文字小文字を区別しません。

数字1から8	キューページで指定されたキューを表示します = Remote Queue = Local Queue = Retry Queue = LAN Queue = RAW Queue = Bad Queue = SmtpIn Queue = Save Queue
/L[N] [InputFile] [OutputFile]	ログファイルレポートを作成します。[L]の後に[N]を指定すると、カンマ区切りのファイルとして保存しません。

/A	ログファイルレポートを作成する際、新情報を出力ファイルに上書きせずに追加します。

セクション 7

7 MDaemonの追加機能

7.1 MDaemonとテキストファイル

MDaemonはデータの保持やテンプレート生成、各種設定ファイルにおける柔軟性を維持するため、多くのプレインテキストファイルを使用しています。ファイルの作成は ファイル >> 新規 のメニューから行えます。これは自動応答や、RAWファイルなどのMDaemonの様々な機能用にデータを作成するにあたり便利にお使い頂けます。

MDaemonファイルの編集

MDaemonの多くのデータファイルは、プレーンテキストでNotePad(メモ帳)を使用して編集ができます。これらのファイルはMDaemonから[ファイル >> 開く >> 空のテキスト]を選択して開くことができます。デフォルトでは、MDaemonのインストールフォルダにある\app\ の*.txtファイルを参照します。ファイルの種類を選択するドロップダウンメニューで、[すべてのファイル]を選択する事で、全ファイルを見ることができます。

7.2 メールによるリモートサーバのコントロール

MDaemonのシステムアカウントである"MDaemon@<MDaemon's Domain>"宛てに特殊な形式のメールを送る事で、MDaemonの持つ多くの機能に対してリモートアクセスできます。サーバに送信されるメールは、一般ユーザ同様にメール用ディレクトリに格納されます。

こうしたコントロール用メールの一部は正規のアカウントを必要とします。正規のアカウントを必要とするコマンドは、SMTPプロセスの中でSMTP認証を通過する必要があります。

メールで使用できるコマンドは、大きく2つのカテゴリに分類されます。メーリングリスト 816 および通常のメールコントロール 819 です。

参照:

メーリングリストコントロール 816
通常のメールコントロール 819

7.2.1 メーリングリストのコントロール

これらのコマンドはサーバにアカウントがなくとも使用できます。[カッコ] 内に含まれるパラメータはオプションです。例えば: "name [address]"は"Michael"のみ、オプションのパラメータと共に"Michael user1@example.com"と指定する事もできます。メッセージはコマンドと関連パラメータを1行づつ本文にいれた状態で "mdaemon@[MDaemon domain]" 宛てに送信されます。

コマンド	パラメータ	説明

SUBSCRIBE	listname [address] [{real name}] [(pass)]	送信者が、実在しており、リモートからの購読開始が許可されていれば、対象メーリングリストのメンバーシップに追加されます。
		オプションのアドレスがリスト名の後に指定されると、購読メッセージの［FROM］フィールドにあるアドレスではなく、その指定されたアドレスがリストのメンバーシップに追加されます。
		ユーザのリアルネームは購読者として{カッコ}内に追加することができます（例：{ Bill F} ）。リストのパスワードがこのコマンドに続く場合（それを囲む括弧が必要です）は、そのコマンドはリストの購読解除機能がオフになっていても受け入れられます。
		例：
		`SUBSCRIBE list@example.com`
		`SUBSCRIBE list@example.com me@example.com {Bill F}`
		`SUBSCRIBE list@example.com you@example.org (PASS)`

UNSUBSCRIBE
Or
SIGNOFF
	listname [address] [(pass)]	送信者は指定されるメーリングリスト（実在し、その送信者を現在のメンバーとして含む）のメンバーから削除されます。オプションのアドレスがリスト名の後に指定されると、購読中止メッセージの[FROM]フィールドにあるアドレスではなく、その指定されたアドレスがリストのメンバーシップから削除されます。リストのパスワードがこのコマンドに続く場合（それを囲む括弧が必要です）は、そのコマンドはたとえこのリストの購読中止機能がオフになっていても受け入れられます。
		例：
		`UNSUBSCRIBE list@example.com (listPASS)`
		`SIGNOFF list@example.com me@example.com`

DIGEST	listname [address]	送信者はリストからのメールをダイジェスト形式で受信するように設定されます。オプションのアドレスがリスト名の後に指定されると、そのアドレスはダイジェストモードに設定されます。
		例：
		`DIGEST list@example.com`
		`DIGEST list@example.com user1@example.com`

NORMAL	listname [address]	送信者はリストからのメールをノーマル（ダイジェストではない）形式で受信するように設定されます。オプションのアドレスがリスト名の後に指定されると、そのアドレスはノーマル形式で受信するように設定されます。

例:

```
NORMAL list@example.com
NORMAL list@example.com user1@altn.com
```

NOMAIL	listname [address]	このコマンドは[アドレス]をnomailモードに設定します。アカウントはサスペンド状態になり、その後リストのトラフィックを受信することはありません。アドレスが指定されていない場合、メッセージの送信者が使用されます。 例: `NOMAIL list@example.com me@example.com`

MAIL	listname [address]	このコマンドは[アドレス]をnomailモードから標準モードに切り替えます。アドレスが指定されていない場合、メッセージの送信者が使用されます。
		
		例:
		`MAIL list@example.com`
		`MAIL list@example.com me@example.com`

REALNAME	listname [address] {real name}	このコマンドは[listname]というリストのメンバーの[アドレス]にリアルネーム値を設定します。リアルネームは{ }で囲まれている必要があります。 例: `REALNAME list@example.com {Bill Farmer}`
LIST	[listname] [list password]	メーリングリストに関する情報提供を行います。リスト名の指定がない場合、全てのリストのサマリ情報が送信されます。リストパスワードが指定されている場合は、対象のリストに関するより詳細な情報が提供されます。 例: `LIST list@example.com Lz$12`

参照:

メールによるリモートサーバーのコントロール 816
通常のメールコントロール 819

7.2.2 一般的なメールコントロール

システムアカウントにメール送信し、一般的なメールコマンドを実行できます。メッセージ本文にはコマンドと関連パラメータが1行毎に記載された状態で "mdaemon@[MDaemon domain]" 宛てに送信します。

コマンド	パラメータ	説明
HELP	なし	[NEWUSERHELP.DAT]のコピーが処理されてメッセージ送信者へ返信されます。
STATUS	なし	サーバの動作および現在の状態に関するレポートがメッセージ送信者へ返信されます。このステータスレポートに含まれる情報はプライベートとみなされるため、メール送信ユーザは管理者権限を持つユーザである必要があります。 例: STATUS

参照:

メールによるリモートサーバコントロール 816
メーリングリストコントロール 816

7.3 RAWメッセージの仕様

7.3.1 RAWメッセージの仕様

MDaemonではRAWメールとして知られるシンプルで強力なメール形式に対応しています。RAWメールシステムの目的は、MDaemonのようなソフトウェアシステムが、より複雑な RFC-2822に準拠したメールを作成できるよう、シンプルで標準的なフォーマットを提供する事です。RAWのようなメール配送エージェントを使用する事で、クライアントソフトウェアは、インターネットでメール基準の順守を維持するための複雑な作業から、サーバーを解放することができるようになります。

RAWメールは、必須もしくはオプションで求められるテキストヘッダと、それに続くメッセージ本文で構成されます。ほとんどのヘッダはトークンとそれに続く <> 記号で囲まれた値から構成されており、ヘッダの各行は、<CRLF>で終わる文字列の組み合わせで構成されています。ヘッダとメール本文は空の行で分離されており、大文字小文字の区別はありmせん。また、[From]と[To]のみが必須のヘッダ項目となります。ヘッダや本文で使われる全ての文字列はプレーンなASCIIテキストで、(例えば[my-message.raw]のように)[.raw]の拡張子で終わるファイルである必要があります。メールを配信用に

キューへ送るには、MDaemonのRAWキュー(通常はC:¥MDaemon¥Queues¥Raw)に[*.raw]ファイルを配置します。

コンテンツフィルタを回避

デフォルトでは、RAWメッセージは通常のメッセージと同じようにコンテンツフィルタによってフィルタリングされます。RAWメッセージをフィルタから回避する場合は、ファイルの前をpあるいはPから始めます。例えば、[P_my-message.raw]というファイルは、コンテンツフィルタを回避しますが、[my-message.raw]というファイルはコンテンツフィルタによってフィルタリングされます。

コンテンツフィルタを回避させると、DKIMはメールへ署名を行いません。MDaemonが全てのメールへ署名を追加するよう設定している場合、これは潜在的な配信エラーの原因となる場合があります。コンテンツフィルタを回避したRAWメールへ署名を追加するには、この後に説明するx-flag=signオプションを使用してください。

RAW ヘッダ

From <mailbox@example.com>	このフィールドは送信者のメールアドレスを含みます。
To <mailbox@example.com [, mailbox@example.com]>	このフィールドは受信者のメールアドレスを含みます。受信者が複数の場合はカンマでそれぞれを区切ることによって指定することができます。
ReplyTo <mailbox@example.com>	このメッセージに対する返信の送信先を指定するオプション項目です。
CC <maibox@example.com[, mailbox@example.com]>	このメッセージのカーボンコピー受信者のオプションのリストです。カーボン受信者が複数の場合は、カンマでそれぞれを区切ることによって指定することができます。
Subject <text>	オプションのメール件名です。
Header <Header: Value>	メッセージ内に明示的にヘッダと値の組み合わせを配置することができます。これにより、カスタムあるいは他の標準的でないヘッダを[*.raw]メッセージに入れることが可能になります。

RAW でサポートされる特別なフィールド

添付ファイルとエンコード

x-flag=attach <filepath, method> [-x]

例: x-flag=attach <c:¥utils¥pkzip.exe, MIME> -x

このX-FLAGは、<> 内の2つのパラメータと共に[ATTACH]値を指定します。最初のパラメータは、メッセージへ添付されるべきファイルの完全なパスです。2番目のパラメータは、カンマによって最初のパラメータと区切られ、メッセージを添付する時に使用されるエンコードの方法を指定しま

す。MDaemonは、このパラメータの2つの値をサポートします。MIME方法は、インターネット標準のBase 64のメッセージエンコードを使用するようにサーバへ指示します。ASCIIの方法は、そのメッセージにファイルをインポートするようにサーバへ指示します。文字列の最後のオプションの[-X]パラメータは、ファイルが添付された場合そのファイルをディスクから削除するようにサーバへ指示します。

配信状況通知

x-flag=confirm_delivery

このフラグを含むRAWメッセージをRFC-2822メールに変換する時に、文字列は[Return-Receipt-To: <sender@example.com>]という構成へ変換されます。

特定ヘッダと値の組み合わせをRFC-2822メッセージへ挿入する

header <header: value>

RAWファイルから生成されるRFC-2822メッセージに特定のヘッダと値の組み合わせを挿入する場合は、前述のHEADERマクロを使用する必要があります。例えば、[Delivered-By: mail-machine@domain.com]というヘッダを、RFC-2882メッセージに挿入する場合は、RAWメッセージ内に[header <Delivered-By: mail-machine@example.com>]と入力します。[header]マクロには、フィールドおよび値の両方が必要なことに注意してください。RAWメッセージには、必要なだけ[header]マクロを入れることができます。

DK/DKIM署名されたRAWメッセージ

x-flag=sign

このコマンドを[*.raw]ファイルに含めると、そのRAWメッセージはDK/DKIM署名されたことになります。これはコンテンツフィルタを迂回するように構成したRAWメッセージ([p]あるいは[P]で始まるファイル名)に対してのみ使用してください。フィルタを通して処理される正常なRAWメッセージに対しては、このコマンドを使用しないでください。これらのメッセージは通常に署名されます。

コンテンツフィルタで生成されるすべてのRAWメッセージは、自動的にx-flag=signコマンドを使用します。

サンプルRAW メールメッセージ

サンプル 1:

```
from <mdaemon@altn.com>
to <user01@example.com>

Hello John!
```

サンプル 2:

```
from <user01@example.com>
to <user09@example.net>
subject <Requested Files>
X-FLAG=CONFIRM_DELIVERY
X-FLAG=ATTACH <c:\docs\files\data01.zip, MIME> -X
```

```
Here are all those files you asked for.
```

7.4 セマフォファイル

MDaemonには、セマフォファイルという機能が搭載されており、これを使って特定のアクションを実行する事ができるため、幅広い目的で使われています。MDaemonは定期的に¥APPディレクトリをスキャンしセマフォファイルの有無を確認します。セマフォファイルが見つかると関連するアクションを実行し、その後セマフォファイルを削除します。これにより、管理者や開発者は、MDaemonのインターフェイスで実際に作業することなく、MDaemonを簡単に操作することができます。セマフォファイルとそれぞれの目的は次の通りです。

FILENAME	ACTION
ACLFIX.SEM	ACLファイルのクリーンナップ処理を実行します。
ADDUSER.SEM	このセマフォは新規アカウントを作成します。これにより、ユーザデータベースの再構築を行うことなく、新しいレコードをUSERLIST.DATファイルの末尾に追加することができます。 このファイルの各行は、MDaemon API（MDaemonの¥docs¥API¥フォルダ内のMD-API.html を参照）のアカウント管理機能で定義されているフォーマットと一致する必要があります。複数の新規アカウントの追加も可能で、1行に1つのアカウントレコードを指定します。 MDaemon は1行ずつファイルを処理し、各新規アカウントを追加して行きます。更新中にADDUSER.LCKファイルを作成して、ファイルをロックすることも可能です。これにより、MDaemonはADDUSER.LCKファイルが削除されるまで、ADDUSER.SEMファイルを処理しません。ADDUSER.SEMファイルのサンプルは、APPディレクトリのADDUSER.SMPをテキストエディタで開いて参照することができます。
ALERT.SEM	ファイルが作成された時にWebmailにログオン中の全ユーザへ、セマフォファイルの内容を表示するポップアップウィンドウを開きます。しかし、全ユーザへ瞬時に表示されるわけではありません。ユーザごとのブラウザがWebmailサーバへリクエストを送信した時点で表示されます。 注意: 他のセマフォファイルとは異なり、このファイルはWebmail特有のものです。これはMDaemonの¥app¥ディレクトリではなく¥MDaemon¥WorldClient¥ディレクトリに配置する必要があります。
ALIAS.SEM	エイリアスデータファイルをリロードします。
AUTORESPEXCEPT.SEM	自動応答の例外ファイルをリロードします。
BATV.SEM	バックスキャッタ保護（BATV）データファイルをリロードします。

BAYESLEARN.SEM
このSEMは手動でベイジアン学習を開始します。これはスパムフィルタのベイジアン画面にある[学習する]ボタンと同じ動作をします。
注意: これによりベイジアン学習が無効の場合でも、ベイジアン学習が開始されます。

BLACKLIST.SEM
ブロックリストデータファイルをリロードします。

CFILTER.SEM
コンテンツフィルタルールを再ロード、コンテンツフィルタのキャッシュデータの消去、スパムフィルタの 許可リスト（フィルタなし）630をリロードします。

CLEARQUOTACOUNTS.SEM
ユーザのクォータチェックの結果は、MDaemonのquotacounts.datファイルに保存されます。このキャッシュデータをクリアする場合は、このSEMファイルに、ユーザのメールアドレスを追加し、¥appフォルダに配置してください。アスタリスク(*)が記載されている場合は、ファイル全体が削除され、キャッシュにあるクォータカウントが無効になります。

DELUSER.SEM
このセマフォファイルを使用してユーザアカウントを削除することができます。削除するアカウントのアドレスを含むテキストファイルを(1行に1アカウント)作成して、ファイル名をDELUSER.SEMに変更してMDaemonの¥appディレクトリに移動します。MDaemonでアカウント削除し、その後でDELUSER.SEMファイルも削除します。アカウントを削除してメールフォルダの削除は行わない場合は、アドレスへ「^」を追加して下さい。(例 frank@example.com^)

DNS.SEM
Windows DNS servers94とスパムフィルタのDNS設定をリロードします。.

DOMAINSHARING.SEM
ドメイン共有データファイルをリロードします。

EDITUSER.SEM
このセマフォは時間のかかる再構築を行うことなく、USERLIST.DATファイル内の特定ユーザーレコードを更新するために使用されます。USERLIST.DATファイル内の特定のレコード更新をするためには、EDITUSER.SEMというファイル名でファイルを作成し、一行一ユーザー毎に更新用のレコードを記入します。各レコードはUserlist File Formatで説明されている通り、USERLIST.DATファイルのフォーマットと同じである必要がありますが、元のレコードと同じメールアドレスとカンマから始まる必要があります。MDaemonはEDITUSER.SEMファイルを一行毎に処理します。EDITUSER.LCKファイルを作成し、MDaemonがEDITUSER.LCKを削除するまではEDITUSER.SEM処理を行わないようにする事もできます。EDITUSER.SEMのサンプルを確認するには、/APP/フォルダ内のEDITUSER.SMPをテキストエディタで開いて下さい。

EXITNOW.SEM
MDaemonを終了します。

GATEWAYS.SEM
最適なパフォーマンスのために、MDaemonではゲートウェイのリストをメモリに置きます。MDaemonのAPP ディレクトリへGATEWAYS.SEMを作成すると、GATEWAYS.DATがリロードされます。

GREYLIST.SEM	グレーリスティングデータファイルをリロードします。
GROUPS.SEM	アカウントグループデータファイルをリロードします。
GRPLIST.SEM	メーリングリスト名の内部キャッシュをリロードします。
HANGUPG.SEM	接続されているRASセッションを暫定的に切断させます。MDaemonは処理中のメールセッションの終了を待ち、RASセッションを切断します。
HANGUPR.SEM	RASデバイスを無条件に切断します。これは接続中のメールセッションに関係なく即時に無条件に切断します。
HOSTSCREEN.SEM	ホストスクリーンデータファイルをリロードします。
IPSCREEN.SEM	IPスクリーンデータファイルをリロードします。
IPSHIELD.SEM	IPShield.datはアクセススピード向上のためにメモリへキャッシュされます。IPSHIELD.SEMはこのファイルをメモリへリロードするのに使用できます。
LDAPCACHE.SEM	LDAPとゲートウェイのユーザーデータファイルをリロードします。
LOCKSEMS.SEM	ユーザがLOCKSEMS.SEMを削除するまで、セマフォファイルの処理を停止します。
LOGSETTINGS.SEM	ログファイル設定をリロードします。
MDSPAMD.SEM	すべての設定データを再初期化し、スパムフィルタ許可リストおよびMDSPAMDを再ロードします。
MINGER.SEM	Minger[785]の停止と再起動を行います。
MXCACHE.SEM	MXキャッシュのデータファイルをリロードします。
NODNSBL.SEM	DNSBLの許可リストファイルをリロードします。
NOPRIORITY.SEM	NoPriority.datファイルを強制的にリロードします。

ONLINE.SEM	RASを使用してISPへの接続に成功すると、MDaemonはこのセマフォファイルを作成します。接続が終了すると、MDaemonはそのセマフォファイルを削除します。これは MDaemonがRASサブシステムを使用するタイミングを知りたい場合に便利です。
POSTDIAL.SEM	このファイルは、MDaemonによって開始された接続が終了した直後に作成されます。
PREDIAL.SEM	MDaemonでRAS/DUNを使用する前に、このファイルを作成します。これは、外部アプリケーションが、MDaemonでいつダイアルアップポートを解放するか検出する際に使用されます。
PRIORITY.SEM	優先メールデータファイルをリロードします。
PROCBAD.SEM	Badキュー内のメール配信を開始します。
PROCDIG.SEM	メーリングリストダイジェストの構造および配信を始めます。
PROCHOLDING.SEM	Holdingキュー内のメール配信を開始します。
PROCNOW.SEM	リモートメールのチェックを開始し、Remoteキューにあるメールの配信をします。
PROCREM.SEM	MDaemonは即座にメール処理モードに入り、すべてのリモートメールを処理します。
PROCRETR.SEM	Retryキュー内のメール配信を開始します。
PRUNE.SEM	古いメールとアカウントの消去プログラムを実行します。
PUBLICSUFFIX.SEM	Public Suffix 499 ファイルをリロードします。
QUEUE.SEM	このセマフォファイルはメールキューの有効化/無効化を行うのに使用されます。ファイルには任意の行数を記入できますが、各行に次の値が必要です: ENABLE INBOUND, ENABLE REMOTE, ENABLE LOCAL, DISABLE INBOUND, DISABLE REMOTE, DISABLE LOCAL
RESTART.SEM	MDaemonを再起動します。

RESTARTCF.SEM	CFEngine.exe(コンテンツフィルタの実行プログラム)を再起動します。
RESTARTWC.SEM	MDaemon Webmailの停止と再起動を行います。これはMDaemon Webmailが内蔵ウェブサーバー[295]で動作している場合のみ機能します。
RELOADCACHE.SEM	コンテンツフィルタの設定とファイル以外のすべてのキャッシュされた設定をリロードします。
REVERSEEXCEPT.SEM	リバースルックアップの例外ファイルをリロードします。
SCHEDULE.SEM	スケジュールデータファイルをリロードします。
SPAMHONEYPOTS.SEM	スパムハニーポットデータファイルをリロードします。
SPF.SEM	SPF, DKIMおよびVBRデータファイルをリロードします。
SUPPRESS.SEM	ブロックリスト設定をリロードし、ドメイン設定のキャッシュをクリアします。
TARPIT.SEM	DynamicScreen.datファイルをリロードし、ターピットをリロードします。
TRANSLAT.SEM	ヘッダ変換データファイルをリロードします。
TRAY.SEM	システムトレイ内のMDaemonアイコンを再描画します。
TRUST.SEM	信頼されたドメインおよびIPアドレスは、最適なパフォーマンスのため、メモリに常駐します。手動でこれらの設定を再ロードする場合に、TRUST.SEMを作成します。
UPDATEAV.SEM	アンチウィルスの定義ファイルアップデートを開始します。
UPDATESA.SEM	スパムフィルタアップデートを開始します。
USERLIST.SEM	USERLIST.DATファイルをリロードします。これは、USERLIST.DATファイルに対する修正を行い、MDaemonにリロードさせることが必要な場合に使用してください。
WATCHDOG.SEM	MDaemonは約10～20秒の間隔で、このセマフォファイルをチェックし、APPディレクトリから削除します。このファイルは、外部アプリケーションが、MDaemonの稼働状態をチェックするために使われます。このファイルが、APP ディレクトリ内に20秒以上ある場合は、MDaemonが実行されていないことを意味します。

7.5 ルートスリップ

一般的に、キューで待機していているメッセージのヘッダには、正しい宛先に配信するため必要とされる情報が全て含まれています。ファイルに保存されているヘッダ(例えば X-MDaemon-Deliver-To ヘッダ)は、MDaemonへ場所と配信先で、メッセージ配信を指示します。しかし、この情報の代わりに特定の代替情報によって、ファイルの送信先を示すことが必要で便利な場合があります。ルートスリップは、そのようなメカニズムを提供します。ルートスリップは、あるメッセージファイルが、どこへまたは誰に送信されるべきかという具体的な指示をMDaemonに与えるファイルです。ルートスリップが、特定のメッセージファイルに用意されると、[.MSG]ファイルにある情報ではなく、ルートスリップによって設定される情報が、どこの誰にそのメッセージを送信するべきかをコントロールします。

ルートスリップファイルは、.RTE拡張子を持ちます。例えば、送信待ちしているメッセージファイルが[MD0000.MSG]である場合、このメッセージに対応するルートスリップファイルは[MD0000.RTE]となり、そのメッセージファイルと同じディレクトリ(メールキュー)に配置される必要があります。

ルートスリップのフォーマットは以下のようになります。

```
[RemoteHost]
DeliverTo=example.net
```

ルートスリップのこのセクションは、対応している[.MSG]ファイルが送信されるサーバをMDaemonに指示します。MDaemonは、できるだけ短い時間でメッセージをルートするために、このホストへ直接接続しようとします。1つのホストのみが指定可能です。

```
[Port]
Port=xxx
```

このスイッチは、TCP/IP接続および配信の試行が行われるべきポートを指定します。SMTPメールのデフォルトポートは25です。

```
[LocalRcpts]
Rcpt0=address@example.com
Rcpt1=other-address@example.com
Rcpt2=yet-another-address@example.com

[RemoteRcpts]
Rcpt0=address@example.net
Rcpt1=other-address@example.net
Rcpt2=yet-another-address@example.net
```

これらのセクションで、関連した[.MSG]ファイルのコピーを受信するローカルおよびリモート受信者を、何人でも指定することができます。ローカルとリモート受信者アドレスは、別々に管理され対応する[LocalRcpts]および[RemoteRcpts]セクションに配置される必要があります。

ルート スリップは、メールの配信またはリダイレクトに対する有効なメカニズムではありますが、一般的には必要ありません。
MDaemonがルート スリップを利用する1つの場合として、[ルートされる]メーリングリスト メールが挙げられます。リスト メッセージのコピーをリモート ホストへ振り分けするように設定されたメーリングリストがある場合、ルート スリップは、この処理を実行するために採用されます。メールが大量の配信先を持つ場合、ルート スリップは非常に効率的なメール配信方法です。なぜなら、そのメールの受信者は何人でも指定でき、メッセージのコピーは1つしか必要ないからです。しかし、すべてのリモート ホストで、この種のルーティングが許可されているわけではありません。そのメールのコピーを最終的に各アドレスへ配信するのはそれらのリモート ホストなので、いくつかのホストは指定することが可能な受信者の数に上限を設定します。

セクション 8

8 SSL証明書の作成と利用

SSL & TLSダイアログから証明書を作成すると、MDaemonは自己発行の証明書を生成します。言い換えると、証明書又は証明機関(CA)は証明書の保有者と同じものになります。これは有効な証明書ではありますが、証明機関は、信頼できる証明機関としてユーザーリストへ含まれていないため、ユーザがWebmailやRemote AdministrationのHTTPSのURLに接続する場合に、証明書のインストールや閲覧続行を行うかどうかを尋ねるダイアログが表示されます。ユーザが証明書のインストールに同意し、Webmailのドメインを有効な証明機関とすれば、WebmailやRemote Administrationに接続する度セキュリティ警告が表示される事はなくなります。

MDaemonにMicrosoft Outlookのようなメールクライアント経由で接続する場合は、証明書のインストールに関するオプションは表示されません。証明書が有効なものではなくても、一時的にその証明書を使用するかどうかの選択を行うことになります。メールクライアントを起動してサーバに接続するたびに、有効ではない証明書を使用するかどうかの選択を行わなければなりません。これを避けるために、Let's Encrypt[541]のような証明機関からの証明書を使用するか、証明書をエクスポートして、ユーザに対してメールやその他の方法でそれを配布する必要があります。ユーザは配布された証明書を手動でインストールすることにより、警告メッセージの表示を回避することができます。

証明書の作成

MDaemonの中で証明書を作成するには

1. MDaemonの **セキュリティ** ≫ **セキュリティ設定** ≫ **SSL & TLS** ≫ **MDaemon**を選びSSL & TLSダイアログを表示します。
2. **SSL, STARTTLSおよびSTLSを有効にする**を選択します。
3. **証明書を作成**をクリックします。
4. **[ホスト名]**というテキストボックスで証明書が属するドメインを入力します(例えば"mail.example.com")。
5. **[組織/会社名]**というテキストボックスに、証明書の所有者である組織あるいは会社名を入力します。
6. ホスト別名にユーザがWebmailサーバに接続する時に使用すると思われるすべてのドメイン名を入力します(例えば"*.example.com", "example.com", "mail.altn.com")。
7. ドロップダウンリストから暗号キーのビット長を選択します。
8. サーバが所在する国または地域を選択します。
9. OKをクリックします。

サードパーティー証明書の利用

MDaemon以外の認証局から購入・入手した証明書は、Microsoft Management Consoleを使用してMDaemon用証明書の保管エリアにインポートする事で、使用できるようになります。Windows XPでの操作は:

1. Windowsの**スタート** ≫ **ファイル名を指定して実行…**を選択し、テキストボックスに**mmc /a**と入力します。
2. **OKをクリックします。**

3. コンソールで、**ファイル ≫ スナップインの追加と削除(Ctrl+M)** をメニューから選びます。
4. スタンドアロン画面の **追加..** をクリックします。
5. スタンドアロン スナップインダイアログで、**証明書**をクリックして**追加**をクリックします。
6. 証明書スナップインダイアログで、コンピュータアカウントを選び 次へをクリックします。
7. コンピュータの選択で、ローカルコンピュータを選択して、完了をクリックします。
8. 閉じるをクリックしてOKをクリックします。
9. 証明書(ローカルコンピュータ)の左側で、インポートされた証明書が自己署名されたものであれば **信頼されたルート証明機関**の下の**証明書**フォルダをクリックします。自己署名されたものではない場合は**個人**フォルダをクリックします。
10. メニューから **アクション ≫ すべてのタスク ≫ インポート** をえらびます。**次へ**をクリックします。
11. テキストボックスにインポートする証明書のファイルパスを入力するか、**参照**ボタンをクリックしてファイルを探します。そして**次へ**をクリックします。
12. **次へ**をクリックし、**完了**をクリックします。

> MDaemonは、Personal Information Exchange format(PKCS #12)を使った秘密鍵を持つ証明書のみを表示します。インポートした証明書が一覧に表示されていない場合は、証明書のキーと秘密鍵の両方を含む、*.PEMファイルをインポートする必要がある場合があります。この方法でファイルをインポートすると、PKCS #12形式に変換されます。

証明書の管理にLet's Encryptを使用する

Let's Encryptとは、セキュアなウェブサイト向けに、従来手動で行っていた証明書の生成、検証、署名、インストール、更新といった複雑な処理を自動化し、無償の証明書を発行している認証局(CA)です。

Let's Encryptの自動処理で証明書を管理するのに、Let's Encrypt[541]画面にてMDaemon¥LetsEncryptフォルダに格納されたPower Shellスクリプトを簡単に実行するためのオプションを用意しています。スクリプトを実行するとLet's Encrypt用に、Webmail HTTPフォルダへhttp-01チャレンジに必要なファイルの配置を含む、全ての設定が行われます。ここでは、証明書用のドメインとしてデフォルトドメイン[165]の**SMTPホスト名**[167]が関連するホスト名と併せて使用され、証明書の取得と受信、Windowsへのインポート、MDaemon, Webmail, Remote Administrationでこれらの証明書を使用するためのMDaemon設定が行われます。更に、スクリプトはMDaemon¥Logs¥フォルダへLetsEncrypt.logというログも生成します。このログはスクリプト実行の度に削除され再生成され、スクリプトの開始時間が記録されます。通知用の管理者アドレスへは、エラー発生時にはメールでの通知も行われます。詳細についてはLet's Encrypt[541]を参照してください。

参照:

SSL & TLS 523

セクション 9

9 用語集

ACL Access Control List(アクセスコントロールリスト)の略称です。ACLは、IMAPメールフォルダ毎にアクセス権を設定するための、IMAP(インターネット メッセージ アクセス プロトコル)の拡張機能です。この機能により、メールサーバにアカウントを持っている他のユーザへ、フォルダへのアクセス権を与えることができます。さらに、各ユーザがそれらのフォルダを管理する範囲を決定することができます。例えば、メッセージの削除をさせるかどうか、既読あるいは未読のフラグを付けるか、フォルダへのメッセージのコピー、新しいサブフォルダの作成などの作業範囲を指定することができます。ACLをサポートするメールクライアントのみが、このアクセスと許可の設定を共有使用することができます。しかし、メールクライアントがACLをサポートしない場合は、MDaemonのGUIからこれらの設定を行うことができます。現時点では、ACLをダイレクトにサポートするメールクライアントはわずかですが、Insightコネクタと呼ばれるwww.bynari.netから提供される素晴らしいユーティリティにより、Microsoft Outlookへこの機能を追加することができます。

ACLに関するより詳しい情報は、以下のサイトでご覧になることができます:

http://www.rfc-editor.org/rfc/rfc2086.txt

ASCII ASCIIは[American Standard Code for Information Interchange(情報交換用米国標準コード)]の頭文字語です。それは世界標準のコードで、すべての大文字小文字のラテン文字、数字、7桁の2進数としての句点などを含み、それぞれの文字には0～127までの数字が割り当てられています(0000000～1111111)。例えば、大文字のMはASCIIコードでは77です。大部分のコンピュータが、テキストを表すのにASCIIコードを使用します。これによりデータを他のコンピュータに移すことが可能になります。また、ほとんどのテキストエディタとワードプロセッサがASCII形式でファイルを保存することができます。しかし、ほとんどのデータファイル(特に数値を含むもの)は、ASCII形式では保存できません。

より大きな文字セットは7ビットの代わりに8ビットを使用するので、128文字が追加されています。これらの追加的な文字は、シンボルと英語ではない文字のために使用されます。DOSオペレーティングシステムは拡張ASCIIあるいはhigh-ASCIIというASCIIのスーパーセットを使用します。

ATRN TRNまたはODMRを参照してください。

添付ファイル(Attachment) メールに添付されるファイルです。ほとんどのメールシステムはテキストの送信のみをサポートするので、添付ファイルがバイナリファイルやフォーマット済みのテキストファイル(例えば、ワードプロセッサのドキュメントなど)の場合は、そのファイルはまずテキストにエンコードされてから送信され、受信されてからデコードされます。エンコードにはいくつかの方法がありますが、2つのものが一般的に普及しています。1つはMIME(Multipurpose Internet Mail Extensions)で、もう1つはUuencode(Unix-to-Unix)です。入力メッセージに関して、デコード処理を受信者のメールクライアントで行うか、あるいはメッセージをローカルユーザに送る前に添付ファイルを自動的にデコードして特定の場所に保存するかを行うようにMDaemonを設定することができます。

バックボーン(Backbone) ネットワークの中で主要なパスを形成する接続や回線のこと。大きいネットワークにおける非バックボーン回線の方が、より小さいネットワークのバックボーン回線よりも太い場合があるので、この言葉は相対的な意味合いを持ちます。

帯域幅(Bandwidth) 一定の時間内にネットワークやモデムを通して処理されるデータの量は、通常、bps(ビーピーエス)で測定されます。1ページの英文テキストは約1万6000ビットで、高速なモデムであれば約1～2秒で処理することができます。フルモーションでフルスクリーンの動画は、圧縮率にもよりますが、約1,000万bpsの速度が必要となります。

帯域幅は高速道路に例えることができます。高速道路は接続回線を表し、そこを移動する車は回線を流れるデータを表します。高速道路が広ければ(帯域幅が大きければ)、そこを走る車の台数も増やすことができます。

ボー(Baud) ボーレートとは、1秒あたりに転送するビット数(bps)を単位とした通信速度のことです。それはモデム送信できるデータの速度を表します。通常、高速なモデムはbpsで表されますが、より遅いモデムはボーレートで表されます。高速接続ではそれぞれの信号が1ビット以上をエンコードするので、[ボーレート]と[bps]は必ずしも同義語であるというわけではありません。

ビット(Bit) ビットとは2進数の0と1の桁数です。これはコンピュータにおける情報量の最小単位です。通常、それはbps(ビーピーエス)のように小文字の[b]で表されます。1ページの英文テキストは約1万6000ビットになります。

ビットマップ(Bitmap) インターネット上あるいはコンピュータ上で見られるほとんどの画像はビットマップ形式です。ビットマップは、全体像が見えないくらいに極端に画面に近づいたり、極端に拡大しない限り、絵のように見えるビット(ドット)の配置(ビットマップ)です。ビットマップ形式のファイルには、BMP、JPEG、GIF、PICT、PCX、TIFFなどがあります。ビットマップ画像は大量のドットで構成されているので、拡大すればするほど滑らかさがなくなりギザギザな画像になります。ベクター画像(CorelDraw、ポストスクリプト、またはCAD形式などで作成される)は、ランダムなドットではなく、数学的に生成された幾何学形状ですので、拡大する際にはより良い結果を得ることができます。

Bps Bits Per Second=ビット数/秒]は、コンピュータデータが移動する速度を表します。例えば、33.6kbpsのモデムは1秒間に3万3600ビットのデータを移動することができます。1秒あたりのキロビット(1,000ビット)は[Kbps]、1秒あたりのメガビット(1,000,000ビット)は[Mbps]として表されます。

ブラウザ(Browser) [ウェブブラウザ]の略語で、ウェブページを表示するために使用され、HTMLコード、テキスト、ハイパーテキストリンク、イメージ、JavaScriptなどを解釈します。最も流通しているブラウザは、インターネット エクスプローラとネットスケープ コミュニケータです。

バイト(Byte) 1セットのビット(通常8ビット)が1つの文字を表します。通常8ビットのセットが1バイトとなりますが、それ以上のビット数の場合もあります。[バイト]は大文字の[B]で省略されます。

キャッシュ(Cache) キャッシュには色々なタイプがありますが、すべては一度呼び出したデータを一定期間保存して、同じデータへの呼び出しが発生した場合高速に呼び出すために使用されます。例えば、ウェブブラウザは、訪問したウェブサイトのページ、画像、URL、その他の要素をキャッシュに保存します。再度同じページを訪問すると、キャッシュされたページが表示されるので、ブラウザは同じ要素を再びダウンロードする必要がありません。ハードディスクのキャッシュメモリへのアクセスの方が、インターネットへのアクセスよりはるかに高速なので、ブラウズ速度を飛躍的に向上させます。

MDaemonのIPキャッシュは、メールを送った相手のドメインのIPアドレスを保存します。これにより、同じドメインに再びメールを送るとき、このアドレスを再度ドメイン検索する必要がなくなります。これにより、配信処理が飛躍的に向上します

Common Gateway Interface]は、ウェブサーバが同じマシン上のもう1つのソフトウェア(CGIプログラム)との間で、どのように通信するかという方法を規定する1セットの規則です。CGI規格にしたがってデータの入出力を行うプログラムであれば、どんなソフトウェアでもCGIプログラムになり得ます。通常、CGIプログラムはウェブサーバからデータを取り出し、例えばメールにフォームの内容を挿入するといった処理を行う小さなプログラムです。CGIプログラムは、ウェブサイトの[cgi-bin]ディレクトリに保存され、必要に応じて呼び出され、URLに表示されます。

cgi-bin CGIプログラムが保存されるウェブサーバ上のディレクトリの最も一般的な名前です。[cgi-bin]のbinとはbinary(バイナリ)の意味で、多くのプログラムがバイナリデータを参照するために使用し

ます。実際に、ほとんどのcgi-binプログラムはテキストファイルで、他の場所からのプログラムによって実行されるスクリプトです。

CIDR ［Classless Inter-Domain ルーティング］は、クラスA、BおよびCに基づいた、新しいIPアドレス指定方式です。CIDR IPアドレスは、通常のIPアドレスの後ろにIPプリフィックスと呼ばれるスラッシュ(/)と数字が付加されたものです。例えば以下のようになります。

123.123.0.0/12

IPプリフィックスは、いくつのアドレスがCIDRアドレスとしてカバーされているかを定義します。より少ない数字がより多くのアドレスをカバーしていることを示します。上記の例では、[/12]というプリフィックスは、以前のクラスCにおける4,096ものアドレスを解決するために使用することができます。

CIDRアドレスは、ルーティングテーブルのサイズを減少させ、より多くのIPアドレスを組織の中で利用可能にします。

CIDRに関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

クライアント(Client) サーバのソフトウェアに接続して、そこからデータの取得や、そこへデータを送信するために使用されるソフトウェアプログラムです。通常、サーバはLANネットワークまたはその他の場所の他のコンピュータ上にあります。それぞれのクライアントプログラムは、特定の1種類以上のサーバプログラムで動作するように設計されます。そして、各サーバは特定の種類のクライアントを必要とします。ウェブブラウザはウェブサーバで通信する特定の種類のクライアントになります。

Common Gateway Interface: 上記のCGIの項目を参照してください。

クッキー(Cookie) コンピュータ用語上のクッキーとは、ウェブサーバからブラウザに送られ、ブラウザ内に保存され、再度同じサイトを訪れたり同じサイトの別のページにジャンプする際に、様々な形で利用されるデータのことを指します。ウェブサーバがブラウザからクッキーの要求を受け取ると、そのクッキーに含まれている情報を使用して、ユーザに送り返す情報のカスタマイズや、ユーザのリクエストの記録を取ったりという処理を行います。通常、クッキーはユーザ名、パスワード、ユーザの好み、買物カゴなど保存するために使用されます。これにより、サイトの運営者は誰であるか、あるいはそこで何をしたかという情報を得ることができます。

ブラウザの設定によって、クッキーの受け入れの可否や、クッキーを保存しておく時間などを指定することができます。通常、クッキーは一定の時間を経過すると削除されるように設定されており、またブラウザが閉じるまでメモリに保存されます。また、それらはハードドライブにも保存されます。

クッキーはハードドライブを読み込むことができません。しかし、特定のウェブサイトにおける行動に関連した情報を取りまとめるために使用することができます。これはクッキーがなければできないことです。

ダイアルアップ接続(Dial-up Networking) Windowsにおけるコンポーネントによって、モデム経由でコンピュータをネットワークに接続することができます。コンピュータがローカルエリアネットワーク(LAN)経由でインターネットへ接続されていない限り、ダイアルアップ接続(DUN)をPOPに接続して、インターネット サービス プロバイダ(ISP)にログオンしないと、インターネットにアクセスできません。接続先のISPは、ゲートウェイアドレスや接続するコンピュータのIPアドレスなどの情報を必要とする場合があります。

ダイアルアップ接続はマイコンピュータ アイコンから開くことができます。それぞれのオンラインサービスごとに、異なったダイアルアップ接続を設定することができます。設定が終了したら、プロファイルのショートカットをデスクトップにおけば、次回接続する時にはそのアイコンをダブルクリックするだけで、簡単に接続することができます。

デフォルト(Default) この言葉は、コンピュータプログラムにおける初期設定値という意味で使用されます。デフォルト設定は、ユーザによる指定や設定が一切ない場合に使用される設定です。例えば、ネットスケープ コミュニケータにおけるデフォルトのフォント設定は[Times]です。この設定は変更しない限り[Times]のままです。デフォルト設定には、通常ほとんどの人々が選択すると思われる値が設定されています。

また、デフォルトという言葉は動詞としても頻繁に使用されます。カスタム設定が機能しないとか、プログラムがタスクを完了するために必要なビットデータを欠いているなどの場合、その特定の設定や動作が[デフォルトする]ことがあります。

DHCP [Dynamic Host Control Protocol]の頭文字です。ネットワークサーバが、ネットワークでつながれたコンピュータに動的なIPアドレスを割り当てる場合に、このプロトコルを使用します。DHCPサーバは、コンピュータから接続されるのを待って、次に、格納されているリストからIPアドレスをそのコンピュータに割り当てます。

DHCPに関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc2131.txt

ドメインゲートウェイ(Domain Gateway) 以下の[ゲートウェイ]の項目を参照してください。

ドメイン名(Domain Name) これはインターネットのウェブサイトを識別する一意の名前です。例えば、[mdaemon.com]はMDaemon Technologies社のドメイン名です。各ドメイン名はドットによって2つ以上に切り離されます。一番右の部分は最も一般的な要素で、一番左の部分は最も特定的な要素です。また、各ドメイン名は1つのサーバのIPアドレスとだけ結びつきますが、逆に1つのサーバには、複数のドメイン名が存在する場合があります。例えば、[mail.mdaemon.com]、[mdaemon.com]、[example.com]はすべて[mdaemon.com]と同じサーバと結び付けることができますが、逆に[mdaemon.com]を複数の異なったサーバに結び付けることはできません。しかし、メインサーバが落ちるか、他の理由で利用不可能になった場合、クライアントを代替のサーバにリダイレクトするための方法はあります。

また、登録されたドメイン名が、実際のマシン上に存在しないというのは良くあることです。この理由としては、ドメイン名の所有者が、まだウェブサイトを開設していない、あるいはドメインをメールの利用のためだけに使用しているので、ウェブサイト開く必要がない場合などが挙げられます。後者の場合には、リストされたドメイン名のメールを処理する実際のマシンがあるはずです。

さらに、[ドメイン名]を省略して、単に[ドメイン]と呼ぶ場合も良くあります。しかし、[ドメイン]という言葉は、Windows NTドメインや値のクラスのように他の意味を持っていますので、混乱しないようにこの区別をしっかりと持っていてください。

ドメイン名に関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc1034.txt

http://www.rfc-editor.org/rfc/rfc1035.txt

DomainPOP MDaemonサーバの機能の一部としてMDaemon Technologies社によって開発されたDomainPOPは、メールサービスを単一のISPのPOPメールボックスからLANやワークグループ全体に提供することを可能にします。過去においては、会社のメールサーバがインターネットと継続的に接

続していない場合、インターネット経由のメールサービスをワークグループへ提供する唯一の方法は、個人がそれぞれのメールボックスを持つことしかありませんでした。しかし、DomainPOPでは必要なメールボックスは1つだけです。ISPはDomainPOPによって定期的に収集されるメールボックスの中に会社のドメインへのすべてのメールをプールします。次に、DomainPOPはメッセージを分析して、目的の受信者を決定し、適切なローカルユーザのメールボックスにメールを配信します。したがって、メールはただ1つのダイアルアップISPアカウントからネットワーク全体に提供されます。

ダウンロード(Download) コンピュータが別のコンピュータからデータを検索、あるいはデータを得る処理を指します。例えば、インターネットからの情報は、他のコンピュータからそれをダウンロードすることによって得ることができます。この逆はアップロードです。情報を別のコンピュータに送る場合、その行為をアップロードと呼びます。

ドライバ(Diver) ハードウェアデバイスとデータのやり取りを行う小さなプログラムを指します。ドライバは、コンピュータと他のプログラムが、デバイスをコントロールし、認識するために必要な情報を含んでいます。Windowsベースのコンピュータでは、ドライバはダイナミックリンクライブラリ(DLL)ファイルとしてパッケージされている場合があります。マッキントッシュの場合は、ほとんどのハードウェアデバイスはドライバを必要としません。しかし、ドライバが必要な場合は、通常、機能拡張マネージャの中にあります。

DUN 上記の[ダイアルアップ接続]の項目を参照してください。

(電子)メール(Email) (電子)メールは[E-mail]、[e-mail]、[email]とも表記され、すべて同じ意味です。メールは通信ネットワーク上のテキストメッセージの伝達方法です。ほとんどのコンピュータネットワークには、何らかの形式のメールシステムがあります。1つのコンピュータネットワークの範囲内に限定されるメールシステムもありますが、他のネットワークやインターネットへのゲートウェイを持つシステムもあります。これにより、複数のロケーションへの通信を可能にし、世界中にメールを送信することが可能になります。

ほとんどのメールシステムが何らかの形式のメールクライアントを含んでいます。このメールクライアントは、メッセージを構成するためのテキストエディタと他のツール、およびメールを受け取り、それをその適切な目的地に配信するための1つ以上のサーバを含んでいます。一般的に、メッセージはクライアントで作成され、メッセージで指定されるメールのアドレスへの配信のためにサーバに渡され、そのメッセージを最終的に配信する責任がある別のサーバに渡されます。メッセージの目的地がローカルアドレスの場合は、それは他のサーバに渡されずにオリジナルのサーバに保存されます。そして、メッセージの受信者はそのサーバに接続して、メールクライアントを使用することによって、メッセージを検索することができます。クライアントから目的のサーバまでメールメッセージを送信する全体のプロセスにかかる時間は、通常2～3秒から数分以内です。

また、メールメッセージは、テキスト以外にファイルを添付することもできます。これらの添付ファイルは、画像、テキストファイル、プログラムファイル、他のメールメッセージなど、どのような形式のものでも可能です。しかし、多くのメールシステムは、テキストファイルの送信のみをサポートしているので、添付ファイルは送信前にまずエンコードされ(テキスト形式に変換され)、目的地に到着した後にデコードされなければなりません。通常、この処理は送信側と受信側のメールクライアントによって自動的に行われます。

すべてのインターネットサービスプロバイダ(ISP)は、メールサービスを提供しています。また、多くのISPは、他のメールシステムのユーザとメールを交換することができるように、ゲートウェイをサポートします。多くの異なったメールシステムによって様々なプロトコルが使用されていますが、いくつかの共通仕様があるので、ほとんどすべてのユーザがメッセージを交換することができます。

メールアドレス(Email Address) メールアドレスとは、メールの送信先であるネットワーク上の電子的なメールボックスを特定する名前や文字列です。メールのアドレスは、メッセージが送受信される場所となります。メールサーバは、メッセージを適切な目的地に配信するためにメールアドレスを必要と

します。異なったタイプのネットワークには、異なった形式のメールアドレスが存在しますが、インターネット上では、[mailbox@ example.com]のような形式に統一されています。

例えば、以下のようなアドレスになります。

Frank.Thomas@altn.com

Eメールクライアント(Email Client) メールクライアントは、(単純にメールクライアント、またはクライアントと呼ばれる場合もあります)は、メールの送信、受信、整理などを行うためのソフトウェアです。メールシステムは、クライアント/サーバ構造に基づくので、クライアントと呼ばれます。クライアントは、メールを作成してそれをサーバに送ります。サーバはそのメールを受信者のサーバに送り、受信者のクライアントがそれを検索し受信します。通常、メールクライアントはユーザのマシンにインストールされる独立したソフトウェアですが、MDaemonのようにウェブブラウザから利用できるWebmailクライアントを組み込んでいる製品もあります。この場合は、ブラウザをクライアントとして利用できるので、クライアントソフトウェアを個別のマシンにインストールする必要がなくなります。これはメールの携帯性と利便性を大いに高めます。

暗号化(Encryption) 安全対策として、ファイル内の情報を暗号化やスクランブルをかけたりすることができます。これにより、そのファイルがデコードあるいは解読される時だけ、その内容を読み取ることができます。暗号化は、第三者からのメールの傍受を防ぐために使用することができる技術です。メッセージは、送信時にエンコードされ、受信された後にデコードされます。

イーサネット(Ethernet) イーサネットはローカルエリアネットワーク(LAN)で使用される、最も一般的なタイプの接続です。イーサネットで最も一般的に使用されている形式が10BaseTと100BaseTです。10BaseTイーサネットは最大10Mbps(メガビット/秒)の速度で有線あるいは無線接続でデータを転送することができます。100BaseTイーサネットは最大100Mbps(メガビット/秒)でデータを転送します。ギガビットイーサネットは、データを最大1,000Mbpsで転送することができます。

ETRN [Extended TURN]の頭文字です。自分のSMTPサーバから他のSMTPサーバに対して、メールの送信や、送信待ちメールのデキューのリクエストを行うSMTPの拡張機能です。SMTP自体にはメールをリクエストする機能がないので(通常、メールはIMAPプロトコルあるいはPOPによってリクエストされます)、このETRNリクエストを使用することにより、リモートサーバにSMTPセッションの開始を要求して、そこに格納されているメールをリクエスト内で指定されたホストに送信させることができます。

TURNコマンドをこの目的に使用するのは安全性の上で危険な場合があります。それは、このコマンドによりSMTPセッションがリバースされ、実際にはメールを送信してもらいたいサーバに対して、格納しているメールを何の認証もなしにすぐに送信してしまうことがあるからです。そこで、ETRNはセッションをリバースするのではなく、新しいSMTPセッションを開始します。これにより、リクエストを行う相手のサーバが[成りすまし]のホストである場合は、送信サーバは本当のホストに対しての配信を行い続けることができます。現在、Authenticated(認証) TURN(ATRN)という新しい規格が提案されています。これはTURNコマンドのようにSMTPセッションをリバースしますが、その前に認証を必要とします。この新しい規格はオンデマンド メール リレー(ODMR)です。MDaemonサーバは、ETRNとODMRのATRNの両方をサポートします。

ETRNに関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc1985.txt

ODMRに関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc2645.txt

FAQ [Frequently Asked Questions(よくある質問)]の頭文字です。FAQは、最も一般的な質問に対する答えを集めた問答集です。それは通常、質問の後に答えが続く形のリスト形式で表示

されます。より規模が大きいFAQでは、リストの最初の部分に質問のすべてがリストされ、そこから質問の答えが(ハイパーリンクなどで)参照できるような形式になっています。FAQは、初歩的なテクニカルサポートや使用方法のヘルプとして使用され、そこで答えを見つけることができれば、テクニカルサポートに連絡して問題を解決するよりも、はるかに時間と労力を節約することができます。

File Transfer Protocol　以下のFTPの項目を参照してください。

ファイアウォール(Firewall)　ファイアウォールとは、安全上の手段としてコンピュータネットワークを複数の部分に切り離すか、あるいはアクセス権を特定のユーザのみに制限する場合に、ソフトウェアかハードウェアかどちらかの方法で防護壁(ファイアフォール)を付けることを指します。例えば、ネットワークでホスティングしているウェブサイトにおいて、ホームページは一般に公開するが、従業員専用のページには従業員のアクセスのみを許可する場合などが考えられます。これを達成するために、パスワードの要求や特定のIPアドレスからの接続のみを許可するなどの方法がありますが、いずれにしろこの従業員専用のページはファイアウォールの後ろにある(守られている)ことになります。

FTP　[File Transfer Protocol]の頭文字です。これは、あるコンピュータから別のコンピュータへ、インターネットを経由してファイルを転送する一般的な、そして効率的な方法です。この目的のために設計された特定のクライアント/サーバアプリケーションを[FTPサーバ]と[FTPクライアント]と呼びます。例えば[FileZilla]は最も一般的なクライアントの一つです。通常、FTPクライアントは、ファイルの転送以外にも多くの機能を備えているので、とても便利な製品です。ウェブブラウザの中にはFTPをサポートする製品もありますが、それはダウンロードだけの場合もあります。さらに、ほとんどのFTPサーバがファイルをダウンロードするために誰でもログオンできる[公開FTP]であり、ユーザ名に[anonymous]を、パスワードに自分のメールアドレスを使用することによりログオンすることができます。しばしば、ログオンせずにファイルをダウンロードできる公開FTPサイトがあります。それらは、リンクをクリックするだけで接続することができます。FTPをサポートするブラウザでFTPサイトに接続するには、URL欄で[http://…]ではなくて[ftp://…]を入力してください。

FTPに関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc959.txt

ゲートウェイ(Gateway)　ゲートウェイとは、2つのアプリケーションあるいはネットワーク間でやりとりされるデータの、異なったプロトコルを翻訳する、コンピュータハードウェアまたはソフトウェアのことを指します。また、ゲートウェイは、あるシステムから別のシステムへのアクセスの手段を記述するために使用されます。例えば、ISPはインターネットへのゲートウェイとなります。

MDaemonメッセージングサーバーのドメインゲートウェイ機能は、他のドメインへのメールゲートウェイとして機能します。これはインターネットに常時接続していないドメインと、サーバが落ちた場合に備えてバックアップサーバを必要とするドメインにとって便利な機能です。

GIF　[Graphics Interchange Format]は、イメージファイルの一般的な形式であり、インターネット上の最も一般的な形式でもあります。GIFはインデックスされた色、または特定のパレットを使用します。これにより、ファイルサイズを大幅に減少することができます。特に、画像が広い範囲で同じ色を使用している場合に効果が大きくなります。ファイルサイズが減少することにより、システム間の転送速度が向上するので、インターネットで頻繁に使用されています。GIFの圧縮方式は、元々コンピュサーブによって開発されたものです。そのためGIFはコンピュサーブGIFと呼ばれる場合があります。

Graphical User Interface　以下の[GUI]の項目を参照してください。

GUI　Graphical User Interfaceの頭文字です。GUIはコマンド行でテキストを入力する代わりに、画面上のグラフィカルな要素をクリックすることによって、コンピュータあるいはアプリケーションとのコミュニケーションを可能にします。Microsoft WindowsとMacintoshのオペレーティングシステムは両方ともGUIベースで、最初にGUIを世に出したのはアップルですが、元々のアイデアはゼロックスが開発したものです。

Host ホストとはネットワーク上の他のコンピュータのサーバとして機能するコンピュータを意味します。ホストマシンはウェブサーバ、メールサーバ、あるいは他のサービスを実行し、通常はそれらを同時に実行します。また、ホストは[ホストする]という動詞で使用されることも良くあります。例えば、メールサーバを実行するマシンはメールを[ホスティング]している、といったように使われます。

ピアツーピアのネットワークでは、お互いが同時にホストとクライアントの役割を果たします。例えば、マシンがネットワークプリンタをホストしているとします。と同時に、クライアントとしてメールの収集や、他のホストからファイルをダウンロードすることが可能です。

HTML Hypertext Markup Language]の頭文字です。それはwwwで使用されるハイパーテキスト文書を作成するために使用されるコード化された言語です。HTML文書はユーザのブラウザが解釈できるコードとタグの形式を含むプレーンテキスト文書であり、ウェブページをテキストと色を含む完全なページとして表示することができます。例えば、ブラウザが<B>テキスト</B>というHTML文書を受け取った場合、[テキスト]という文字が太字で表示されます。プレーンテキストファイルのサイズは非常に小さいので、インターネット上で高速に転送することができます。

HTTP [Hypertext Transfer Protocol]の頭文字です。HTTPはインターネット上でコンピュータ間のハイパーテキストファイルを転送するために使用されるプロトコルです。HTTPは通信を行うコンピュータの片方でHTTPサーバを必要とし、もう片方でクライアントプログラム(通常はウェブブラウザ)を必要とします。

HTTPに関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc2616.txt

ハイパーテキスト(Hypertext) ハイパーリンクを含むテキストあるいは同じドキュメントや別のドキュメントへのジャンプを含むドキュメントはハイパーテキストと呼ばれます。また、このテキストはハイパーテキストリンク、あるいは単にリンクと呼ばれる場合もあります。ハイパーテキストは、単語や語句に埋め込まれたリンクであり、それをクリックすることによりブックマークされた位置に移動したり、そこにリンクされているドキュメントを表示させることができます。通常、ハイパーテキストリンクは色つきの下線で表示されますが、それは必ずしも必要なものではありません。ハイパーテキストは、普通のテキストと同じように見えることがありますが、多くの場合はマウスポインタをそこに乗せると、そのポインタがグラフィカルに変化します。

Hypertext Markup Language 上記の[HTML]の項目を参照してください。

IMAP [Internet Message Access Protocol]の頭文字です。スタンフォード大学によって開発された、IMAPはメールメッセージを管理して、検索するのに使用されるプロトコルです。IMAPの最新版は、IMAP4であり、POP3と似ていますが、多くの付加機能があります。IMAP4はユーザのローカルマシンにおけるメール管理機能ではなく、サーバにおける管理プロトコルとして最もよく知られています。IMAP4ではメールがサーバにある状態で、それをキーワードで検索、フォルダを整理、ダウンロード先を特定することを含めた様々な機能があります。このように、IMAPはユーザのマシンに対する要求が少なく、メールを集中管理できるので、複数のロケーションからアクセスすることができます。

IMAPに関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc2060.txt

IMAP4 ACL extension 上記の[ACL]の項目を参照してください。

インターネット(Internet) インターネットは、核戦争でも破壊することができない通信ネットワークとして1969年に米軍によって開発されました。現在では、それは世界中で数百万のコンピュータを繋ぐネットワークとなっています。インターネットは分散的なネットワークとして設計され、どんな会社、組織、または国によっても支配されません。インターネット上の各ホスト(またはマシン)は、独立した存

在であり、ユーザが要求するあらゆる情報やサービスを提供することができます。それでもやはり、インターネット上でやりとりされるほとんどの情報は[バックボーン]を経由します。バックボーンとは、非常に太い帯域幅によって非常に高速な接続を提供する、最も大きいISP(インターネットサービスプロバイダ)や組織によってコントロールされる回線です。ほとんどのユーザが、このバックボーンに接続しているAOLなどのオンラインサービスやISPを経由してインターネットにアクセスします。

多くの人々が、WWW(ワールドワイドウェブ)とインターネットが同じものだと考えていますが、実際にはそうではありません。WWWはインターネットではなく、インターネットの一部でしかありません。WWWは目に見える存在であり、商業にも利用される最もポピュラーな部分ではありますが、それでもやはりWWWの一部でしかありません。

イントラネット(Intranet) イントラネットは、会社や組織のネットワークで厳密に管理される、小さなプライベートなインターネットです。イントラネットの構成は組織によって大きく異なりますが、多くの場合はインターネットで利用可能な機能を含みます。そこにはメールシステム、ファイルディレクトリ、ブラウズできるウェブページや記事などを始めとする、様々な機能があります。イントラネットとインターネットの大きな違いは、イントラネットは比較的小さな、組織やグループに限られたネットワークであるということです。

IP [Internet Protocol](例えばTCP/IP)の頭文字語です。インターネットプロトコルにより、インターネット上でデータの転送が可能になります。同じインターネットプロトコルを使用すれば、各マシンのプラットフォームやオペレーティングシステムの種類にかかわらず、データの転送を行うことができます。また、[IP]という用語は、[IPアドレス]のさらなる簡略名として一般的に使用されています。現在の標準のインターネットプロトコルはIPバージョン4(IPv4)です。

IPに関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc791.txt

IPアドレス(IP Address) IPアドレスはインターネットプロトコルアドレスという意味で、IP番号と呼ばれることもあります。IPアドレスは、特定のTCP/IPネットワークやネットワーク上のホストあるいはマシンを特定するために使用されます。それは0～255までの数字を使用した、ドットで分けられている4つの数字を含む32ビットの数値アドレスです(例えば、[127.0.0.1]のようになります)。独立したネットワークでは、各コンピュータは一意のIPアドレスを持たなければなりません。またそのIPアドレスは無作為に割り当てることができます。しかし、インターネット上のあらゆるコンピュータには、重複を避ける意味から登録されたIPアドレスがなければなりません。それぞれのインターネットIPアドレスは、静的なものと動的なものがあります。静的なアドレスは、インターネット上のコンピュータの位置が常に同じである固定的アドレスです。動的なアドレスは、ダイアルアップでインターネットにアクセスした際に、ISPによって一時的に割り当てられる可変的なアドレスです。しかし、場合によっては、ダイアルアップのアカウントに静的なアドレスを割り当てることも可能です。

ISPや大企業などは、通常ひとかたまりで複数のIPアドレスをInterNIC登録サービスに要求し、彼らのネットワークのユーザがアクセスする際に、同じようなアドレスが利用できるようにします。これらのIPアドレスのセットはA、B、Cの3つのクラスに分けられます。クラスAとクラスBは非常に大きい組織で使用され、それぞれ1,600万と6万5000のホストをサポートします。クラスCはより小さいネットワークで使用され、255のホストをサポートします。現在、クラスAとクラスBは利用可能なアドレスが不足してきており、得るのが非常に難しくなっています。その結果、多くの会社は代替策として、複数のクラスCのセットを使用しなければなりません。このIPアドレス不足のために、現在では新しい[CIDR]と呼ばれるプロトコルが、古いシステムの代わりに徐々に使われ始めています。

現在の標準IPとIPv4に関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc791.txt

IPバージョン6(Ipv6)に関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc2460.txt

CIDRに関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

IP Number See *IP Address* above.

ISP [Internet Service Provider]の頭文字です。インターネット サービス プロバイダ(ISP)は、インターネットへのアクセスとサービスをエンドユーザに提供する会社です。ほとんどのISPが、WWWアクセス、メール、ニュースグループ、ニュースサーバなどの複数のインターネットサービスを提供しています。通常、ユーザはダイアルアップ経由、あるいはその他の方法でISPに接続します。そして、ISPはその接続をインターネットのバックボーンに繋がるルータに渡します。

Java サンマイクロシステムズ社によって開発されたJavaは、C/C++のような構文を備えたネットワーク指向のコンピュータプログラミング言語ですが、機能の代わりにクラスの周りで構築されます。インターネット アプリケーションでは、それは一般的にアプレットのプログラミングに使用されます。アプレットとはウェブページに埋め込まれている小さなプログラムです。これらのプログラムは、通常のHTML言語や他のスクリプト言語は達成できないような多くの機能をブラウザ上で実行するために、ウィルスなどの心配もなく、ウェブページから自動的にダウンロードされます。Javaは効率的かつ簡単に使用できるので、多くのソフトウェアやハードウェアの開発者の間では非常にポピュラーになってきています。

JavaScript JavaScriptはHTMLの能力を拡張し、対話的なウェブページを作成するためのスクリプト言語として、ネットスケープ社によって開発されたものです。Javaとはまったく別の物ですので混同しないようにご注意ください。JavaScriptは、非常にスリムで簡単なプログラミング言語で、Javaやその他の言語よりはるかに簡単に使用できますが、機能的にはある程度制限されます。多少の制限はありますが、ウェブサイトへ対話的な要素を加える場合には非常に役に立ちます。例えば、データをサーバに送る前に事前処理する場合や、ウェブページ上のリンクや要素によってユーザに対して対話的な処理を行いたい場合などに役立ちます。また、ユーザが選択したプラグインやアプレットをコントロールするために使用することもできます。それにより、多くの機能を実行することができます。JavaScriptは、HTMLドキュメントのテキストに埋め込まれ、ウェブブラウザによって解釈され実行されます。

JPEG [Joint Photographic Experts Group]という、この形式を開発したグループの頭文字です。JPEGは、高解像度の画像やファイルをGIF形式よりもはるかに効率的に圧縮するファイル形式です。GIFは同じような色が広範囲で規則正しく繰り返し使われているような画像に適していますが、JPEGは多くの色数を使用した画像の圧縮に適しています。JPEGはインターネット上の高解像度の写真や画像などに最も一般的に使用されている形式です。

Kbps この頭文字は[1秒あたりのキロビット数]を表し、一般的にモデム速度(例えば、56Kbps)を表すために使用されます。それは毎秒、転送され処理されるデータのキロビット(1,000ビット)数です。これは[キロビット]であり[キロバイト]ではないことに注意してください。キロバイトはキロビット×8の単位です。(8キロビット=1キロバイト)

キロバイト(Kilobyte) 1キロバイト(1KあるいはIKB)は1,000バイトのデータの集まりです。正確には1,024バイト(2の10乗 = 1024)ですが、一般的には簡単な数値として1,000バイトに切り下げられています。

LAN [Local Area Network]の頭文字です。LANは、1つの建物内などに限定されるネットワークで、通常は、有線か無線などのメディアによって、すべてのノード(コンピュータまたはワークステーション)を接続します。LANは多くの大企業に採用され、従業員や事務所間の情報管理と情報共有を大幅に簡素化しています。多くのLANで、何らかの形式のメールやチャットシステムが利用され、部署ごとに別々の装置などを抱えることを避けるためにプリンタなどの装置を共有することができます。ネットワークのノードが、電話回線や電波あるいは衛生中継などで結ばれる場合は、それはLANではなくてWAN(ワイド エリア ネットワーク)と呼ばれます。

待ち時間(Latency) ネットワーク接続を経由してデータパケットを転送するのに要する時間です。データパケットが転送されると、パケットが転送先のコンピュータに受け取られたという確認を転送元のコンピュータが待つ[待ち時間]が生じます。帯域幅と同様に、この待ち時間は接続回線の速度を測定する要素の1つとなります。

LDAP Lightweight Directory Access Protocolの頭文字です。LDAPは、ディレクトリ アクセス プロトコル(DAP)を簡素化したオンライン ディレクトリ プロトコルです。このディレクトリシステムは、次のようなレベルの階層構造で構成されます。ルートまたは開始ディレクトリ、国、組織、組織的なユニット、そしてそのユニット内の個人です。それぞれのLDAPエントリは識別名(DN=distinguished name)と呼ばれる一意の識別子がある属性の集まりです。LDAPはオープンなプロトコルであり、効率的であり、また多くのサーバを接続する能力を持っているので、メールアドレス、組織、ファイルなどの情報を持つ世界中のディレクトリに対して、どんなプラットフォーム上のどんなアプリケーションでも接続することを事実上可能にします。

LDAPに関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc2251.txt

リンク(Link) 上記の[ハイパーリンク]の項目を参照してください。

リストサーバ(List server) 1つのアドレスにメールを送信するだけで、複数の受信者にメールを配信することを可能にするサーバアプリケーションです。リスト サーバによって管理されているメーリングリストにメールが送信されると、それは自動的にリストのメンバーに配信されます。メーリングリストは、通常、普通のメールアドレス(例えば、 listname@example.com)を持ちますが、そのアドレスは特定の受信者やメールボックス用ではなく、受信者の全体のリスト用のアドレスになります。ユーザがメーリングリストに加入すると、リスト サーバは自動的にそのアドレスをリストに追加して、それ以降のメールを、追加されたアドレスを含むすべてのアドレス(メンバー)に配信します。ユーザがメーリングリストから脱退すると、リスト サーバはそのアドレスを削除して、それ以上リスト メッセージを受け取らないようにします。

[listserv]という単語は、しばしば一般的にメーリングリスト サーバを示す用語として使用されます。しかし、[ListservR]はL-Soft international社の登録商標であり、1986年にBitnetのためにエリック ーマスによって開発されたプログラムです。他のリスト サーバに加えて、MDaemonサーバは、リスト サーバに関する一通りの機能をすべて備えています。

ログオン名(Logon) サーバなどにアクセスするため、あるいは自分の身元を明らかにするために使用される、一意のコードあるいは一連の文字列です。多くの場合、パスワードとログオン名は1組のセットとなっていなければなりません。

[ログオン名]と同じ意味で使用される用語には、ログオン、ユーザ名、ユーザID、サインイン

メールボックス(Mailbox) 特定のメールアドレスに割り当てられた、ハードディスクなどの記憶装置上の、メールのデータが保存される場所です。どんなメールシステムでも、各ユーザはそのユーザ宛てのメールを受け取って保存する、メールサーバ上の個人的なメールボックスを持っています。また、メールアドレスの一番左側の部分を[メールボックス]と呼ぶ場合もあります。例えば、[Frank@altn.com]の[altn.com]はドメイン名で、[Frank]はメールボックスです。

メーリングリスト(メーリングリスト) メーリングリストはメールグループとも呼ばれ、1つのメールアドレスから配信できるメールアドレスのグループです。例えば、[listname@ example.com]のようなアドレスになります。リストサーバが、そのメーリングリスト宛てのメールを受け取ると、それは自動的にそのリストのメンバー(すなわち、グループに含まれているアドレス)のすべてに配信されます。MDaemonサーバは、メーリングリストに関する広範囲な機能を装備しています。例えば、リストの公開/非公開の選択(誰でもそのリストに参加や投稿ができるかどうか)、モデレート機能(メールがリストに配信される前に管理者によって許可されなければならない)、ダイジェスト形式で配信する、個々のメールとして配信するなど、これ以外にも色々な使用方法が用意されています。

メガバイト(Megabyte) 1メガバイトは、正確には1,048,576バイトですが、一般的には簡単な数値として100万バイトに切り下げられています。(例えば、[20MB]のように) メガバイトは[MB]と表されます。

MIME Multipurpose Internet Mail Extensionsの頭文字で、1992年にインターネット エンジニアリング タスクフォース(IETF)によって策定されました。MIMEは標準のインターネットメールへテキストではないファイルを添付するために使用されるエンコード規格です。一般的にはメールで送信できるのはテキストファイルのみなので、非テキストファイルを送信する場合は、最初にプレーンテキストへエンコードして、メールに添付して送信し、その後受信された後に受信側でデコードされます。したがって、MIME規格を使用してファイルの送受信が行えるメールプログラムは、MIME互換のプログラムであるといえます。MIMEでエンコードされたファイルが添付として送信される場合、一般的には送信されるファイルのタイプと、デコードする際に使用されるべき方法の両方が、メッセージの一部として指定されます。MIMEには、あらかじめ定義された[image/jpeg]や[text/plane]などの多くの内容タイプがあります。しかし、あなた自身のMIMEタイプを定義することも可能です。

また、MIME規格をウェブサーバで使用することにより、サーバがウェブブラウザに送信するファイルを特定することができます。ウェブブラウザでは様々なMIMEタイプをサポートするので、HTML形式以外のファイルの表示/出力することが可能になります。さらに、ブラウザのMIMEタイプのリストと、各タイプを扱うために使用されるソフトウェアをアップデートすることによって、新しいファイル形式を容易にサポートすることができます。

MIME に関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc2045.txt

http://www.rfc-editor.org/rfc/rfc2046.txt

http://www.rfc-editor.org/rfc/rfc2047.txt

http://www.rfc-editor.org/rfc/rfc2048.txt

http://www.rfc-editor.org/rfc/rfc2049.txt

ミラーリング(Mirror) あるサーバ上にあるファイルのコピーがある別の場所のサーバ(通常はFTPサーバ)を指します。あるサーバ上にあるファイルのコピーがある別の場所のサーバ(通常はFTPサーバ)を指します。あるサーバ上にあるファイルのコピーがある別の場所のサーバ(通常はFTPサーバ)を指します。また、[ミラー]という意味は、1つのファイルが同時に複数のハードディスクに書き込まれる構成であることを指します。これは、1つのハードディスクに支障をきたした場合、重要なデータを失わずにコンピュータを作動させ続けることができるという、冗長性を高めるための手段として使用されます。

モデム(Modem) [modulator-demodulator]の頭文字語から由来しています。モデムはコンピュータに接続され、電話回線を経由して他のコンピュータにデータを転送するための装置です。モデムは、コンピュータのデジタルデータをアナログ形式に変調して、そのデータを他のモデムに送信します。送信されたデータは、受信したモデムによって復調され、デジタルデータに変換されます。つまり、モデ

ムは[アナログ/デジタル変換器]ということができます。データの転送速度はボーレート(例えば、9600ボーなど)、あるいは1秒あたりのキロビット数(例えば、28.8Kbpsなど)のどちらかで表されます。

MultiPOP MDaemonメッセージングサーバーのコンポーネントで、POP3プロトコルを使って、MDaemonユーザーが外部のメールサーバからメールを代理収集するための機能です。MDaemonのアカウントを持つユーザーは、他のサーバから一斉にメールを収集するように構成することができます。これにより、他の場所にメールアドレスを持っているMDaemonアカウントのユーザが、MDaemonアカウントでメールを収集、プールすることができるようになります。その結果、すべてのメールを1つのメールボックスに格納することが可能になります。

Network 複数のコンピュータが何らか方法で接続されている状態を指します。ネットワークの目的は、複数のシステム間でリソースと情報の共有を行うことにあります。例えば、プリンタ、DVD-ROMドライブ、ハードディスク、個々のファイルなどの共有を行うことができます。

様々なタイプのネットワークの中でも、最も広く定義されているタイプは、ローカル エリア ネットワーク(LAN)とワイド エリア ネットワーク(WAN)です。LANでは、個々のコンピュータ(あるいはノード)が、通常は同じ建物内などの近くに位置しています。通常はケーブルなどの有線で接続されていますが、最近では無線などのワイヤレス接続も増えてきています。WANのノードは、通常、遠く離れていて(別のビルや都市など)、電話回線、人工衛星、その他の形式で接続されています。

インターネット自体もネットワークです。それはしばしば、ネットワーク中のネットワークと表現されます。

Network Address Translation Network Address Translationの頭文字です。NATは2つのIPアドレスを1セットとして1つのネットワークで使用します。そのうちの1つは発信用で、もう1つは受信用です。これは主にファイアウォール的な対策として使用され、ネットワークセキュリティを確実なものにします。LANの外側に対するIPアドレスとLANの内側で実際にそのコンピュータに割り振られているIPアドレスを別なアドレスとして運用することができます。そして、インターネットとネットワークの間に、ハードウェア的あるいはソフトウェア的に、両方のアドレスを[翻訳]する装置を設置します。この方法により、LANに接続している複数のコンピュータが、1つのIPアドレスを共有してインターネットに接続することが可能になります。したがって、ネットワークの外側からは、間に置かれている翻訳装置によって認証あるいは許可されない限り、LAN に接続されているコンピュータに接続することは一切できなくなります。

Network Interface Card(NIC) [Network Interface Card]の頭文字です。NICはコンピュータがネットワークに接続するために必要な装置です。NICにより、通常はモデム(ほとんどのホームコンピュータで、電話回線によるダイアルアップでネットワークへ接続する)による一時的な接続の代わりに、常時接続の環境を提供します。ほとんどのNICがイーサネットやトークン リングあるいはTCP/IPなどの特定のタイプのネットワークとプロトコルのために設計されます。

NNTP Network **N**ews **T**ransfer **P**rotocol (NNTP) の頭文字です。NNTPはUSENETニュースグループのメッセージの配信に使用されるプロトコルです。現在、多くの一般的なブラウザとメールクライアントには、NNTPクライアントが標準装備されています。

NNTPに関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc977.txt

ノード(Node) ネットワークに接続する単一のコンピュータを指します。

ODMR On-Demand Mail Relay の頭文字です。ODMRはISPへの断続的な接続環境でもメールサーバを有効にするために設計された新しいプロトコルです。これにより静的なIPアドレスを持たなくても、それを持つメールサーバと同様にメールの受信やETRNコマンドの使用ができます。例えば、システムに静的なIPアドレスが割り当てられている場合は、ESMTP ETRNコマンドを使用することができますが、動的なIPアドレスを割り当てられているシステムには、解決策が全くありません。ODMRはこ

の問題を解決します。特に、ODMRは(過去のTURNコマンドのように)SMTPセッションをリバースしながらも、リクエストしているサーバの認証を必要とするセキュリティ機能が付加された、認証TURNコマンド(ATRN)を取り入れています。これにより、動的なIPアドレスを持つSMTPサーバがISPに接続して、複数のホストのメールをPOPやIMAP経由で収集するのではなく、SMTP経由で配信することを可能にします。これは、静的なIPアドレスや専用オンライン接続を所有するだけのコストをかけられない会社に対して、低コストで自身のメールサーバを構築するという広範囲な需要に対する解決策となります。

ODMRに関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc2645.txt

OEM Original Equipment Manufacturer (OEM) の頭文字です。相手先商標製造会社(OEM)は、その意味がしばしば誤解されていることがあります。OEMとは、企業が他の企業の設備や製品を使用して、その製品を自社のものとしてパッケージし、異なるブランドで販売する手法です。例えば、デル コンピュータ社は、複数の異なる企業からコンピュータの部品を購入し、それらを1つの自社製品の中に組み込み、自社のブランドとして販売しているOEMの典型的な例です。また、デルコンピュータ社に部品を販売する企業も、他社からその部品を仕入れている場合はOEMとなります。すなわち、実際のオリジナルメーカーでないので、[OEM]という呼称は正しいものではなく、[パッケージャー]あるいは[カスタマイザー]と呼ばれるべきです。にもかかわらず、多くの人々は[OEM]という呼称を、実際のハードウェアメーカーに対して使用しています。にもかかわらず、多くの人々は[OEM]という呼称を、実際のハードウェアメーカーに対して使用しています。

オンザフライ(On the fly) [オンザフライ]は一般的に、2つの異なった意味で使用されます。最初の意味として、それは緊急に処理することができるか、あるいは何かのタスクの実行中に簡単に行うことができるという意味があります。例えば、会計ソフトは売上の数字を入力している間に、その入力をいったん中止して、新しい科目を[オンザフライ]で作成することができます。2番目の意味としては、あるものが動的あるいは自動で(静的あるいは手動の代わりに)生成される意味で使用されます。例えば、ウェブページに格納されている[クッキー]は、同じユーザがページに戻ってくる時に、そのユーザ用にカスタマイズしたページを[オンザフライ]で自動的に作成し表示します。

Original Equipment Manufacturer OEM を参照。

パケット(Packet) ネットワーク上でやりとりされるコンピュータデータのユニットです。LAN上のコンピュータあるいはインターネットからのデータを受け取るときは、それは通常パケットという単位で受信されます。オリジナルのファイルやメッセージは、このパケット単位に分割され、送信され、受信されたあとに元に戻るように再結合されます。各パケットには、データのソース情報や目的地情報を含むヘッダ、データ内容、およびエラーチェック情報などが含まれています。また、パケットには番号が付けられ、一緒に送られたパケットと関連付けして間違いなく結合されるようになっています。このパケット送受信の処理は[パケット交換]と呼ばれています。また、パケットは一般的に[データグラム]とも呼ばれます。

パケット交換(Packet Switching) ネットワークかインターネット上のパケット送受信のプロセスです。1つの経路で連続したストリームによりデータを送信する(アナログの電話などの)サーキット交換と比べて、パケット交換ではデータがパケット単位に分割さるので、必ずしもすべてのデータが目的地まで同じ経路を通る必要はありません。さらに、データが分割されているので、複数のユーザが異なったファイルを、同時に1つの経路に送信することも可能になります。

パラメータ(Parameter) パラメータは、文字あるいは値です。コンピュータ用語では、それはユーザやプログラムによって他のプログラムに渡される任意の値を意味します。例えば、名前、パスワード、好みの設定、フォントサイズなどはすべてパラメータになります。プログラミング用語では、パラメータは処理のためにサブルーチンやファンクションに渡される値を意味します。

PDF Portable Document Format（PDF）の頭文字です。PDFはアドビシステムズ社によって開発された、非常に圧縮率の高い、マルチプラットフォームファイル形式で、様々なアプリケーションからのドキュメント形式、テキスト、および画像などをキャプチャーすることができます。これは様々なOSのコンピュータが混在している環境で、ドキュメントを同一に表示し、正確にプリントするという、通常のワープロソフトではなし得ない作業を可能にします。PDFファイルを閲覧するために必要なアプリケーションであるAdobe Acrobat Readerが、アドビシステムズ社から無料で配布されています。また、ウェブブラウザにもPDFファイルを閲覧するためのプラグインがあります。これにより、PDFファイルをダウンロードしてからプログラムを開いて閲覧するという作業ではなく、ブラウザ上で直接そのファイルを閲覧することが可能になります。

解析(Parse) 言語学における解析の意味は、言語を分析するために文法的な要素に分割することです。例えば、文を動詞、形容詞、名詞などに分割することをいいます。

コンピュータ用語では、解析とは、コンピュータ言語の命令をコンピュータが理解できるような部品に分割することを言います。コンパイラにおける解析は、開発者が書いたプログラム命令文を分割し、より新しいプログラムを開発し、実行可能なプログラムを作成するために使用されます。

MDaemonサーバをはじめ、他の製品においても、しばしばメッセージの宛先やフィルタなどのツールを通しての処理のために解析をします。

Ping Packet Internet Groper]の頭文字です。それは、特定のIPアドレスが相手に届いているか、あるいは受信可能かを判定するために使用される、基本的なインターネット プログラムです。それは、インターネット コントロール メッセージ プロトコル(ICMP)のEchoリクエストを送信して、その応答を待つことによって行われます。IPアドレスを確認するためにpingコマンドを実行するには、DOSプロンプトで[ping]と入力した後に続けて、確認するIPアドレスやドメインを入力します。例えば[ping 192.0.2.0]のように入力します。

ICMPに関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc792.txt

http://www.rfc-editor.org/rfc/rfc862.txt

ポップ(POP) Post Office Protocol]の頭文字です。POP(一般的に、POP3として表されます)は、メールサーバからメールを検索するために最も一般的に使用されるメール プロトコルです。POPプロトコルは多くのメール クライアントで使用され、いくつかのクライアントでは、より新しいIMAPプロトコルがサポートされる場合もあります。POP2は、1980年代の半ばに標準規格となり、メールの送信にはSMTPを必要としました。POP2に代わって登場した新バージョンであるPOP3は、SMTPのあるなしに関わらず使用することができます。

POP3に関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc1939.txt

ポート(Port) TCP/IP、UDPネットワーク、およびインターネットでは、ポートは論理接続のエンドポイントであり、0～65536の数字で指定されます。ポート0～1024は、特定のプロトコルとサービスのために予約されています。例えば、ウェブサーバは通常ポート80を使用し、SMTPサーバはポート25を使用します。またPOPサーバもメールの送受信にポート25を使用します。一般に、1つのプログラムに対して各マシンの1つのポートのみが使用されるか、バインドされます。インターネットをブラウズするとき、しばしばサーバは非デフォルト ポートを使用する場合があります。この場合、URLの後に続いてコロン(:)で区切ってポート番号を指定します。例えば、[www.example.com:3000]のようになります。

また、周辺装置やハードウェアを接続するために使用されるコンピュータのソケットに関してもポートを使用することができます。例えば、シリアルポート、パラレルポート、USBポートなどです。

さらに、特定のプラットフォームやマシンを、別のプラットフォームで稼動させるプログラムを作成する場合の処理においてポートが使用される場合があります。例えば[Windowsアプリケーションを UNIXにポートする]、または[アプリケーションのためにユニックスポートを作成する]などです。

ポスト(Post) メールやニュースグループのようなインターネット通信において、他のユーザが閲覧できるようにネットワーク通信システムに入力されるメッセージを指します。例えば、メーリングリストやニュースグループにメッセージを表示することを[ポストする]といいます。

PPP Point to Point Protocol]の頭文字です。PPPはダイアルアップ接続のためのインターネット標準規格です。それは、モデム接続がインターネットで他のシステムに接続して、どのようにデータのパケットを交換するかを定義する規則です。

PPPに関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc1661.txt

プロトコル(Protocol) コンピュータ用語では、プロトコルは、サーバとアプリケーションが通信するための1セットのガイドラインあるいは標準規格です。例えば、TCP/IP、SLIP、HTTP、POP3、SMTP、IMAP、FTPなどの多くの異なった目的に使用される、多くの異なったプロトコルがあります。

レジストリ(Registry) コンピュータにインストールされたソフトウェアに関する構成情報を格納するためにMicrosoft Windowsで使用されるデータベースです。これには、ユーザ設定、ファイル拡張子の関連付け、デスクトップ バックグラウンド、カラーチャート、およびその他多くの情報が含まれています。レジストリには、以下の6つの部分があります:

HKEY_User 各ユーザのユーザ情報。

HKEY_Current_User 現在のユーザが選択したもの。

HKEY_Current_Configuration ディスプレイとプリンタの設定情報。

HKEY_Classes_Root ファイルの関連付けとOLE情報。

HKEY_Local_Machine ハードウェア、OS、インストールされたアプリケーションの設定情報。

HKEY_Dyn_Data 実行データ。

プログラムがコンピュータにインストールされるとき、通常、インストーラは自動的にレジストリに何らかの情報を書き込みます。また、Windowsに備えられているregedit.exeプログラムを使用することによって、手動でレジストリを編集することができます。しかし、レジストリに間違った設定を行うと、コンピュータが正常に機能しなくなったり、まったく起動しなくなったりするので、レジストリを書き換える際には十分な注意が必要です。

RFC Request For Comments の頭文字です。RFCは、インターネットに関する様々な規格や仕様などを策定するためのものです。新しい標準仕様やプロトコルなどは、[RFC]としてインターネットで提案され発表されます。インターネット エンジニアリング タスク フォースは、提案された新しい標準仕様などを討議する場であり、最終的にはその規格の設立を行います。標準仕様が確立されて、一層の[コメント]を[要求される]ことがなくても、その仕様はRFCと特定の数字と共に保有されます。例えば、RFC-822(現在はRFC-2822でサポート)はメールのための公式の標準仕様、またはRFCです。[標準仕様]として公式に採用されるそれらのプロトコルは、公式な標準仕様番号が与えられ、インターネット オフィシャル プロトコル スタンダード(STD-1あるいはRFC-3700)にリストされます。インターネットには非常に多くのRFCが存在しますが、権威がある情報元は、http://www.rfc-editor.org にあるRFCエディタです。

インターネット オフィシャル プロトコル スタンダードに関しては以下のサイトを参照してください。

http://www.rfc-editor.org/rfc/std/std1.txt

RTF Rich Text Format の頭文字です。RTFは、ほとんどすべてのワードプロセッサでサポートされる、Microsoftによって開発された一般的なファイル形式です。RTFは、プレーンテキスト形式と比べて、形式情報、フォント情報、テキストカラーなどの情報を保有することが可能です。ワード2000の文書形式(*.doc)や、Adobe PDFなどの他のファイル形式と比べると、RTFファイルのファイルサイズは非常に大きい場合があります。

サーバ(Server) 他のコンピュータで稼動しているクライアント ソフトウェアに特定のサービスを提供するコンピュータ、またはプログラムを指します。例えば、SMTPサーバのような特定のソフトウェアやそのソフトウェアが実行されているマシンをサーバと呼びます。単一のマシンは、異なった多くのサーバプログラムを同時に実行することができます。例えば、ネットワークのサーバが、ウェブサーバ、メールサーバ、FTPサーバ、ファックスサーバ、およびその他のものを一斉に実行している場合などがあります。

SMTP Simple Mail Transfer Protocol. の頭文字です。SMTPはインターネット上のサーバ間で、あるいはクライアントとサーバ間でメールを送信する際の主要なプロトコルです。SMTPはプログラムのメール送信方法と受信方法のルールのセットから成り立っています。サーバがSMTP経由でメールを受信すると、通常、そのメールはサーバに保存され、そして、POP、IMAP、または他のプロトコルを経由してクライアントから検索することができます。

SMTPに関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc2821.txt

スパム(Spam) スパムとはジャンクメールのことを指します。スパムは求められていない大量のメールを示すのに最も一般的に使用されますが、あらゆる迷惑メールを示す場合にもしばしば使用されます。スパムの送信者は、様々なソースから数百、数千、または何十万ものメールアドレスを得て、それを利用してメッセージや勧誘メールをばらまきます。また、ニュースグループなどへ商品の広告や勧誘などのメッセージを無差別に投稿する行為もスパムと呼ぶことができます。

サーバのリソースを長時間に渡って消費してしまうことなどから、スパムはインターネットで深刻な問題になっています。また、スパムの送信者は様々なテクニックを駆使して、その発信元を偽装しようとします。例えば、メールを様々なサーバを踏み台にして他人のアドレスから送信されたように偽装するテクニックを使用するので、これらを防止するためのテクニックもまた挑戦であるかもしれません。MDaemonサーバは、スパムを防止するために、ブロッカ、IPシールディング、IPスクリーニング、リレーコントロール、その他の多くの機能を備えています。

ジャンクメールをスパムと呼ぶようになった由来は、一般に、ポピュラーなモンティパイソンのスケッチに、バイキングの歌と共に[Spam spam spam spam, spam spam spam spam…]と書かれていたことから来ているといわれています。しかし、Hormel社製のミート缶詰がすべて同じスパムという名前であることから来ているという説もあります。どちらが本当の説なのかは誰も分からないようです。

TCP/IP Transmission Control Protocol/Internet Protocol (TCP//IP)は、インターネットの基礎となるプロトコルです。それはホストを接続するためにインターネット上で使用される、コミュニケーションプロトコルの基礎的なセットです。それはまた、ローカル エリア ネットワークで最も一般的に使用されるプロトコルでもあります。それは、2層構造のシステムで、上層のTCPはネットワーク上でパケットを送信するためにファイルを分割や結合する役割を果たします。下層のIPは、パケットのアドレスを指定して適切な目的地に送信するための役割を果たします。

TCPは以下に記述されています。

TCP - http://www.rfc-editor.org/rfc/rfc793.txt

IP - http://www.rfc-editor.org/rfc/rfc791.txt

Telnet インターネット サイトへログオンするコマンドやプログラムは、以前はTelnetアクセスをサポートしていました。Telnetコマンドは、Telnetサーバに対する迅速なログオンを提供します。そのサーバにアカウントがあれば、ファイル、メールなどの許可されたリソースにアクセスすることができます。Telnetが使用されなくなりつつある理由は、それがUnixコマンドを使用するコマンドライン プログラムであるということです。

Telnetに関するより詳しい情報は、以下のサイトでご覧になることができます。

http://www.rfc-editor.org/rfc/rfc854.txt

http://www.rfc-editor.org/rfc/rfc855.txt

ターミナル(Terminal) ターミナルはリモートコンピュータにコマンドを送信するためのデバイスです。また、ターミナルはキーボード、ディスプレイ スクリーンおよび単純な回路により構成されます。しかし、パソコンは、しばしば端末を[エミュレート]するために使用されます。

Tiff Tagged Image File Format. Tagged Image File Formatの頭文字です。それは様々なコンピュータ プラットフォームのために、普遍的な図形翻訳機能として作成された画像ファイル形式です。TIFFは1ビットから24ビットまでの色数を扱うことができます。

UDP User Datagram Protocol の頭文字です。UDPは、データ転送に使用されるTCP/IPのセットを作成するプロトコルの1つです。UDPはパケットを受信側に確実に届けるという保証がないので、コネクションレスのプロトコルとして知られています。

UDPに関するより詳しい情報は、以下のサイトでご覧になることができます。

UDP is addressed in RFC-768, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc768.txt

Unix UNIXは、1960年代にベル研究所によって開発されたオペレーティングシステムです。多くのユーザが同時に使用できるように設計され、インターネット上のサーバのおける最もポピュラーなオペレーティングシステムです。現在、UNIXをベースとしたOSとしてLinuxを始めとして、GNU、Ultrix、XENIX、など異なった多くのオペレーティングシステムがあります。

URL Uniform **R**esource **L**ocatorの頭文字です。URLは、インターネット上のあらゆるファイルやサーバに存在するものです。その上、サーバかファイルにアクセスするためにウェブ ブラウザに入力するアドレスがURLです。URLには空白を含むことはできず、常にスラッシュ(/)を使用します。そして[://]によって2つの部分に分けられます。最初の部分は使用されているプロトコル、あるいはリソースを表します(例えば、http、telnet、ftpなど)。2番目の部分はファイルやサーバのインターネット アドレスになります(例えば、www.altn.com、127.0.0.1など)。

Uuencode UUencodeは、インターネット上で広く使用されているテキスト ベースのバイナリ暗号化プロトコルです。バイナリデータのファイルを、暗号化されたテキストに変換します。UnixからUnixへのエンコードを行いますが、必ずしもUnixに限るわけではありません。それは異なったプラットフォーム間でファイル転送するために使用される普遍的なプロトコルになりました。また、メールで一般的に使用されるエンコード手法でもあります。

WAN Wide Area Network, Wide Area Networkの頭文字です。WANは、ローカル エリア ネットワーク(LAN)と同じようなものですが、LANよりも広いエリアで使用され、ビル間あるいは都市間のネットワークを意味します。WANはLANを内部連結して構成される場合もあります。世界最大のWANとしてはインターネットが挙げられます。

Zip .zipというファイル拡張子を持つ、圧縮されたファイルを意味します。[ジッピング]とは、1つ以上のファイルを1つのアーカイブファイルに圧縮することを意味し、これによりディスク容量を節約し、より高速な通信を行うことができます。しかし、ジップファイルを使用するためには、WinZipやPKZIPなどの適切なプログラムが必要です。インターネット上の様々なサイトで、複数の圧縮や解凍の機能を持つシェアウェアやフリーウェアが提供されています。

索引

- 2 -

- A -

- B -

– C –

– D –

- E -

- F -

– G –

– H –

– I –

– J –

– L –

- M -

– N –

– O –

– P –

- Q -

- R -

- S -

– T –

– U –

– V –

– W –

– X –

– Z –