管理者マニュアル

v9.0

SecurityGateway for Email Servers
管理者マニュアル

v9.0.3 - 7月 2023

目次

セクション 1

1 SecurityGateway

1.1 概要

MDaemon Technologiesは長年のメールサーバー技術を元にSMTPメールサーバーのセキュリティファイアウォールの開発を行ってきました。SecurityGateway for Email Serversはネットワークの入り口で、複数レイヤーでスパム、なりすまし、ウィルス、その他メールに関連した脅威を保護します。業界標準のSIEVEメールフィルタリング言語をベースに、SecurityGateway for Email Servers email security firewall は送受信メールのトラフィックのパフォーマンスと柔軟性を向上させます。

SecurityGateway email security firewallには様々なメリットがあります:

- **高い検出精度** – メールの中から脅威を複数のツールで分析する事によりSecurityGatewayは スパム対策 127, ウィルス対策 152, なりすまし対策 156, 不正使用対策 180 技術において99%のほぼ完全な検出率を誇っています。
- **シンプルな管理** –直観的な、タスク指向のインターフェースを持つランディングページがSecurityGatewayではメインセクションとして提供しています。ランディングページには一般のタスクのリストがあり、実行するタスクページへのリンクが表示されています。このアプローチは、管理者 49が最小の労力で一般の処置を実行することができます。さらに、管理責任は、ドメイン管理者に委任でき、その管理者が全体の管理に割り当てられると1つ以上のドメインを管理することができます。さらに、エンドユーザ 26は管理者と連絡をとることなく最終的なメッセージの処理を決定する権限が与えられます。 26
- **データ損失の防止** –受信メールトラフィックフィルタリングに加え、SecurityGatewayでは送信メールもフィルタリングします。使いやすいインターフェースは、ネットワーク外で機密情報の無許可の送信を感知して、防止するポリシーの生成を可能にします。
- **強力なフィルタリングエンジン**—SecurityGatewayの強力なフィルタリングエンジンは、SIEVEメールフィルタ言語に基づきます。付属のメッセージコンテンツフィルタ 202とSIEVEスクリプトエディタ 228を用いてさらに、管理者は彼ら自身のSIEVEスクリプトを作成することによって、SecurityGatewayの機能を広げることができます。
- **総合的なレポート** –メールトラフィックパターンと潜在的な問題をSecurityGatewayの総合的なレポート 262によって確認してください。すべてのレポートは、より深い解析を実行しポイント＆クリックでのドリルダウンをサポートします。
- **柔軟な防御レイヤー**– SecurityGatewayの複数のレイヤで防御操作の順序を調節したい管理者は、固有のメールパターンのセキュリティルールを優先する柔軟性もあります。

機能概要

SecurityGatewayでは、機能に該当する各メニューは、左側のボックスのナビゲーションに6つのメニューがあります。次は、6つのメインセクションの簡単な概要です。

ダッシュボード

SecurityGateway for Email Serversにログイン時の最初のページが、ダッシュボードです。ダッシュボードランディングページは、現在のステータスとアクティビティについて、最後の24時間のサマリレポート[262]を示します。

ダッシュボード上部はサーバステータスセクションです。このセクションは、SMTPサービスの動作を示し、開始/停止リンクがあります。ダッシュボードには、登録キーのユーザ数、登録[123]とアクティベーションを管理するためのリンク、現在のドメインとユーザ数を示します。さらにドメインとユーザを管理するドメインリスト[39]のリンクもあります。ソフトウェアアップデート[122]が利用可能な場合、このセクションではアップデートについてのリンクも提供します。次に、グローバル管理者向けに、ディスクの空き容量の一覧が表示されます。SMTPインバウンドとアウトバウンドセッションにおけるアクティブセッション数や、キューステータスセクションにはインバウンド、デリバリー、Badメッセージキューの中のメール数が一覧表示されています。同じセクションで、グローバル管理者向けに、管理者とユーザー用の隔離メールの数も表示されます。最後に、インバウンドとデリバリーキューのエントリには、キュー毎に凍結/解凍のオプションが表示されています。

サーバーステータスセクションの下はサーバー統計セクションです。このセクションでは6つのSecurityGatewayのグラフィックレポートが表示されています: 受信対送信メッセージ[262], メールで使用された帯域の総計[262], 適正vs.ジャンクメール[262], ジャンクメール分析[262], 上位のメール宛先[263], 上位のスパムドメイン[265] 各レポートは直前の24時間の統計を表示します。

ダッシュボードの左側には、ダッシュボードページのリンクがあり、さらにアカウント設定、隔離とメッセージログの管理をするためのアカウント[26]オプションのリンクがあります。

ドメイン管理者[49]は管理上のアクセス権を持つドメインについての統計およびオプションを参照することができます。

設定/ユーザ[38]

設定/ユーザメニューには、SecurityGatewayの主要な設定オプションが7つのセクションにあります。これらのセクションで、ドメインとユーザ設定、メール配信、隔離設定、バックアップとデータベース初期設定ほかのオプションを使用できます。設定/ユーザメニューには、次のサブセクションがあります。

- アカウント[38]
  設定/ユーザメニューのアカウントセクションには、SecurityGatewayのユーザアカウントとドメインに関連するオプションがあります。ドメインおよびユーザアカウントの作成、ユーザ検証ソース、ユーザオプションのデフォルト値など5つのアカウントに関連するリンクが、このセクションにあります。
- メール設定[65]
  メール設定セクションは、各種のメール関連の機能を決定する5つのページリンクを提供します。例えば、ユーザのメールアカウントが属するサーバを指定、隔離オプションの設定、各種のメール配信オプションの設定や他の技術的な設定を管理します。
- 免責事項(ヘッダ/フッタ)[98] – メッセージ免責事項は、サーバでインバウンド、アウトバウンドおよびローカルメールメッセージ本文の上部または下部に追加するテキストです。このページで免責事項の作成および管理をします。
- システム[103]
  設定/ユーザメニューのシステムセクションには、各種のシステム機能(例えば暗号化設定、HTTPインターフェースオプション、ディレクトリ位置、ディスク容量管理オプション)のリンクがあります。

- データベースメンテナンス 117
  このセクション内のオプションは、SecurityGatewayで自動保存するデータタイプとサイズ、自動バックアップ機能およびバックアップをサーバに復元するオプションを扱います。
- 登録 123
  登録ページは、製品が登録されるユーザ名または会社名含む製品登録情報、登録キーと登録の状態を示します。

詳細については、各々のセクションの下でセクション概要または個々のページを参照してください。

セキュリティ 126

セキュリティメニューは、ドメインとユーザをスパム、ウィルス、メール不正使用と他のセキュリティリスクから保護するために役立つ各種ツールの8つのセクションがあります。下記は、各々のセキュリティセクションの簡単な概要です。詳細は、個々のセクションを参照してください。

- スパム対策 127—セキュリティメニューのアンチスパムセクションには、スパムまたは迷惑メールを防止するのに役立つオプションがあります。このセクションには8つのアンチスパム機能があります。ヒューリスティック、ベイジアン解析、DNSとURIブラックリスト、グレーリストを使用してスパムの確認と防止するためのオプションがあります。
- ウィルス対策 152—セキュリティメニューのアンチウィルスセクションには、ウィルス感染しているメッセージを確認し、ユーザに到達することを防止するのに役立つオプションがあります。幅広いレベルでのウィルス対策を実現するため、SecurityGatewayは Clam AntiVirus（ClamAV™）とIKARUS Anti-Virusの2つのアンチウィルスエンジンに対応しています。ClamAVはメールゲートウェイに特化して開発されているopen source（GPL）アンチウィルスエンジンです。IKARUS Anti-Virusは潜在的な悪意ある脅威に対して安全にシステムを保護する機能を提供しています。従来型のウィルス対策と、最新技術の両方をご利用頂けます。 また、ウィルス対策には、さらににによるOutbreak Protection 128が使われており、ウィルスによる大規模感染を防ぐ事ができます。
- なりすまし対策 156— Anti-Spoofingセクションは、偽造される送信メッセージまたは"なりすまし"アドレスを確認するのに役立つツールがあります。このセクションには、6つの「なりすまし」対策があります。例えばDKIM 検証、Sender ID、Callback Verificationなどです。
- 不正利用対策 180— Anti-Abuseセクションには、スパムメッセージを中継するためにメールシステムを悪用または不適切に使用、帯域幅の大量使用、あまりの頻繁なサーバの接続などの防止に役に立つツールがあります。6つのツールがセクションにあります。
- フィルタリング— フィルタリングセクションにはメッセージ内容 202 および 添付ファイル 210と2つの機能があります。メッセージ内容のフィルタリングページでは、処置を行うためのルールを作成します。メッセージ内容のフィルタリングページでは、処置を実行するフィルタルールを作成します。特定の条件に一致するメッセージを拒否、コピー、異なるアドレスにリダイレクト、隔離などのルールを作成することができます。添付ファイルのフィルタリングページでは、指定したファイルが添付された時に、メッセージのブロックや隔離を指定できます。フィルタリングは全体またはドメイン単位で指定できます。
- ブラックリスト 213— ブラックリストは、ブロックまたは隔離をするメッセージのメールアドレス、ホストやIPアドレスの一覧です。デフォルトでは、それらのメッセージはSMTPセッション中に拒否されますが、ブラックリストページでは、隔離の設定を変更ができます。実行する処置は全体でもドメイン単位で指定でき、ブラックリスト自体も全体またはドメイン単位で指定できます。
- ホワイトリスト 221— ホワイトリストは、セキュリティ規制から除外するメッセージのメールアドレス、ホストやIPアドレスの一覧です。SecurityGatewayではヒューリスティックとベイジアン、DNSBL、DKIM検証などのセキュリティ機能が適切なホワイトリストにある場合には、送信者、ホスト、メッセージなどの除外するオプションがあります。各ホワイトリストは、全体またはドメイン単位で設定できます。

- Sieveスクリプト[228] ― SecurityGatewayは、Sieveメールフィルタリング言語を使用して、多くの機能を実現しており、Sieveスクリプトページでは、実行する機能と実行順序が表示されています。Sieveスクリプトエディタでは自身のカスタムスクリプトを作成できます。

メッセージ/キュー[248]

メッセージ/キューには2つの選択肢があります。

- メッセージログ[249]
  メッセージログには、ユーザが送信または受信するメッセージごとのエントリがあります。日付とメッセージが処理された時間、差出人と宛先とメッセージの件名の一覧を示します。配信の結果、隔離か拒否、仮に配信されない場合には理由、差出人がブラックリストにある、メッセージに規制された添付があるなどの一覧も示します。ログの各エントリも、メッセージのサイズとメッセージスコア[150]の一覧を示します。メッセージログから、各メッセージの詳細を見ることができ、その配信とメッセージコンテンツとソースの写しを参照することができます。SecurityGatewayのベイジアン学習機能の改善に役立つスパムまたは非スパムとしてメッセージを評価することもでき、より正確にメッセージを分類することもできます。
- メッセージキュー
  このセクションでは異なるメッセージキューのリンクとして、隔離(ユーザ)，隔離(管理)，配信用キューと不正メッセージがあります:。隔離(ユーザ)[250]は、特定のセキュリティ機能を通過しない受信メッセージの一時保存用のキューです。ユーザは、SecurityGatewayにログインが可能で隔離フォルダの内容を閲覧し、そこからメッセージの閲覧、削除あるいは通常の配信を行うように解放することができます。隔離(管理)[251]では、隔離(ユーザ)と類似していますが、送信メッセージとウィルスを含むメッセージ用です。管理者のみ管理のために隔離にアクセスをします。配信用キュー[251]では、配信不可および現在リトライしている配信待機中の全メッセージのキューです。このページから、任意のメッセージ閲覧、差出人へメッセージを戻す、メッセージ配信停止やキューで選択あるいは全部のメッセージの再配信を直ぐに行うことができます。不正メッセージ[252]では、反復的なループのあるメッセージ、最大メッセージホップカウント[78]に到達したような致命的なエラーにより配信できないメッセージキューです。 不正メッセージキューから、任意のメッセージを閲覧でき、差出人へメッセージを戻すことを試す、メッセージの削除や選択あるいは全メッセージの配信の再試行をすることができます。

ロギング[256]

ロギングメニューには、3つのセクションがあります。

- メッセージログ[256]
  これはメッセージ/キューセクションで述べたメッセージログの追加のリンクです。管理者向けに便宜的に両方で提供しています。
- ログファイル[257]
  ログフォルダ[110]に保存されるSecurityGatewayの各種のログファイルを閲覧するために、ログファイルセクションを使用することができます。メッセージログとは異なり、ログファイルはデータベースに保管されずソート可能な一覧や各イベントの個別のエントリを提供しません。代わりに、各種のSMTP接続からのコピーをもつプレーンテキストファイルとSecurityGatewayが実行する他の機能です。ログファイルセクションの全ログページでは、ログフォルダ内で現在のログファイルとロールオーバー[259]ログを持つログファイルを一覧にします。ページからは、任意のファイルリストを閲覧できます。ログファイルセクションの別のページでは、システムログ、送受信ログ、ウィルス更新ログなど、現在のSecurityGatewayのログファイルを閲覧するショートカットがあります。
- 設定[259]
  設定セクションではロギング設定ページのリンクがあります。それらのリンクはロギング初期設定とオプション構成に使用します。設定ページでは、送受信やHTTPログへ書き出すデータ内容のレベルを指定できます。また、標準セット、新規のログファイルセットを毎日作成、曜日に基づくログファイルと生成するログ

のタイプを選択できます。最後に、ログファイルの最大サイズ、ロールオーバーの回数、アーカイブ前に残存期間を選択できます。

レポート 262

レポートセクションは、SecurityGatewayのアクティビティを対話的で詳細なグラフィカルレポートで提供します。受信対送信メッセージ、受信したジャンクメールの分析表示、帯域幅レポート、累積的メッセージサイズによる上位の差出人、ウィルスレポートを生成できます。さらに、各々のレポートは、レポートのパラメータを指定できるオプションを提供します。例えば、固定あるいは範囲指定の時間、日あるいは月ごとの期間でのレポートを指定ができます。さらに、レポートでエントリに関連するデータのみ表示を限定し、メッセージログへのリンクをもつレポート内容の表形式の分析が各レポートの下にあります。例として、レポートの時間一覧から特定の時間に受信した全メッセージの表示、特定の日に受信したウィルスを持つ全メッセージ、ドメインの上位宛先によって受信された全メッセージのリンクを提供します。

システム要件

最新のSecurityGateway のシステム要件と推奨要件は www.mdaemon.comの SecurityGateway for Email Servers - システム要件 を参照してください。

サポート

www.mdaemon.com/Support/ でSecurityGatewayの最新技術サポート情報と、電話サポート、メールサポート、ナレッジベース、FAQ、コミュニティフォーラム、その他のヘルプ情報を提供しております。

SecurityGateway 9.0.3 - 7月 2023

1.2 バージョン9.0の新機能

特記事項

- 9.0.3 — Outbreak Protection機能が再び使用できるようになりました。Outbreak Protection 128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。
- 9.0.2 — 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。
- 9.0.0 — デフォルトでは、メールアドレスにプラス文字(+)が含まれていた場合に、サブアドレス 64としてみなされるようになりました。ユーザ検証プロセスでも、サブアドレスをエイリアスとして処理します。例えば、user+folder@example.com は、user@example.comユーザーのエイリアス user+folder@example.com = user@example.comとして解釈され、メールボックス名にプラス記号が含まれるユーザーを新たに作成する事はできません。メールボックス名にプラス文字(+)が含まれている既存ユーザーを自動削除することはありません。これは ユーザー検証ソース 52 ページでユーザー検証処理を実行する事で修正（名称変更や統合）が行われます。従来のように、メールアドレスにプラス文字(+)を含めたものを別アドレスとして認識させるには、ユーザーオプション 60 画面にて、"ユーザーのメールボックス名に、

プラス(+)記号の使用を許可する"オプションを有効にしてください。このオプションを有効にすることで、user+folder@example.comをuser@example.comのエイリアスではなく、ユーザー名として処理します。

主な新機能

From ヘッダスクリーニング 179

セキュリティ 126 の中のなりすまし対策 156 セクションへ、新しくFromヘッダスクリーニング 179 ページを追加しました。これは、メールが他の誰かからのものであると見せかける、スパムや攻撃でよく使われる一般的な手法に対抗するための機能です。

Webインターフェースの使い勝手の向上

- 検索ダイアログにて、*"検索条件の表示/非表示"*を追加し、メインツールバーに、*"検索をキャンセル"*ボタンを追加しました。
- メッセージ 249 ページに、(検索ヘッダパターン、結果、及び理由などを含めた)最大4つの検索条件を指定できるようになりました。ヘッダパターンでは、ボタンのトグルを使用して、AND/OR条件で区切ることができます。結果と理由は常にORで区切られます。
- ドメイン一覧 39 とユーザー一覧 47 のツールバーへ検索オプションを追加しました。
- ポップアップウィンドウのサイズの調整、最大化、移動が行えるようになりました。
- モバイルと親和性の高いリストエディタが追加されました。
- アーカイブされたメッセージの表示において、前へ/次へのボタンを追加しました。
- アーカイブ検索 90 ページの右下に、"メッセージをリストアしました"というステータスメッセージが表示されるようになりました。

管理者向けのダッシュボードページの向上

- グローバル管理者のダッシュボード 9 と、設定/ユーザ | システムの下のディスク容量 111 画面に、使用可能なディスク容量の表示を行なうようになりました。
- ダッシュボードページに、アクティブなSMTP Inbound及びOutboundセッションの数を表示できるようになりました。
- グローバル管理者のダッシュボードページに、管理隔離キューとユーザ隔離キューのメッセージ数を表示できるようになりました。
- ダッシュボードからInbound及びRemote配信キューを凍結する機能が追加されました。

追加の機能と変更点

- 設定 | システム | HTTPサーバ画面に、HTTPSレスポンスへHTTP Strict Transport Security (HSTS)ヘッダ 108 を付与する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有効です。HSTS対応のブラウザが、HSTSヘッダを受信した際、SSL証明書が有効であれば、このドメインへの今後のHTTP要求は自動的にHTTPS接続へと切り替わります。
- SecurityGatewayがWindowsの新しいバージョンで搭載されているTLS 1.3に対応しました。Windows Server2022やWindows 11では、デフォルトで TLS 1.3の使用が可能です。Windows 10 のバージョン 2004 (OS Build 19041) 以降の場合には、実験的にTLS1.3に対応する事ができ、次のレジストリを設定することにより、インバウンド接続において有効化することができます。:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityP
  roviders\SCHANNEL\Protocols\TLS 1.3\Server

DisabledByDefault (DWORD) = 0

Enabled (DWORD) = 1
```

- 隔離レポートに一覧表示されているメールの表示をユーザーに許可するかのオプションが追加されました。グローバル管理者は、設定/ユーザ≫メール設定≫ 隔離設定[71]画面か、ユーザー自身のメイン≫ アカウント≫ 設定[27]画面にて、メッセージの表示を行なえるようにするかの設定を行なえます。
- 認証情報を記憶[60]オプションが端末やブラウザで有効な時、アカウント ≫ 設定[27]画面で「この端末/ブラウザでは認証情報を記憶しない」オプションが利用できるようになりました。クリックすると、対象の端末では認証情報が記憶されなくなり、リンクは表示されなくなります。次回SecurityGatewayへサインインする際には、この端末で認証情報を記憶するオプションを再度使用できます。This option will also be available to Secure Messaging[95] users when Remember Me is currently active.アカウント毎のメイン | アカウント | ユーザオプション か、セキュアメッセージユーザーの設定画面にて、端末/ブラウザでの保存を無効化するオプションを追加しました。
- アカウント ≫ ユーザーオプション[60]と セキュアメッセージ ≫ 受信者オプション[95]画面に、サインイン及びセキュアメッセージサインイン画面に、管理者への連絡先情報を表示するオプションを追加しました。
- ユーザ検証ソースエディタ[55]に"保存とテスト"ボタンを追加しました。
- サインインページへCSRFTokenと、ウェブインターフェイスURLへセカンダリセッションIDを追加し、CSRF攻撃に対処できるようにしました。
- 認証情報を記憶[60]機能の一部として、公開鍵/秘密鍵の検証方法を追加しました。
- セキュアメッセージの通知メールのスタイルやわずかに異なる言語を更新しました。
- データベースのトランザクションを軽減し、データベースのサイズが大きくなることを防ぐようになりました。
- VBR認証ホスト"vbr.emailcertifcation.org"が廃止され、メッセージ証明書[146]設定から削除されました。
- アーカイブ ≫ コンプライアンス[91]画面に、"アクティブなアーカイブストアからだけメッセージを削除する"オプションを追加しました。このオプションは、"これより古いアーカイブされたメッセージを自動的に削除する"が有効な際に、適用されるオプションで、デフォルトでは有効となっており、動作は以前のバージョンから変更されません。
- Sieve処理の中で、IPフェースで「エラー」や「拒否」が発生した場合に、SMTPソケットを切断するようになりました。
- SecurityGatewayの起動時に、Inboundキュー内でロックされたメッセージがCrashDumps¥Inboundキューに移動されるようになりました。送信者へメッセージが送信された応答があった際、Inboundキュー内のメッセージもアンロックされます。SecurityGatewayのプロセスが異常終了したり、シャットダウンする前に通信が終了した際、メッセージがキュー内でロックされたままとなる可能性があります。送信者がSMTP DATAコマンドの応答を受信できなかった場合、メッセージは再度送信され。受信者は複数のメールを受信する可能性があります。ただし、これらのメッセージの内容は異常終了した際のデバックに役立ちます。このディレクトリに移動されたメッセージは、30日後に自動的に削除されます。
- LetsEncrypt[107] - out-fileに代わって、add-contentを使用するようにログ機能を変更しました。add-contentは、SecurityGatewayでログファイルを表示できるようにするデフォルトの

システムコードページを使用します。新しいログファイルが作成されるまで、ログファイルのエンコード方式は変更されません。

すべての変更とバグ修正の一覧については、Windowsスタートメニューの SecurityGatewayプログラムグループにあるリリースノートを参照してください。

バージョン8.5.0の新機能

特記事項

32bitのOSはサポート対象外となり、それに伴い32bit版のプログラムも終了となります。SecurityGateway 8.5.0からは、64bit版だけの対応となります。これにより、64bit版に集中した開発とテストが行えるようになり、64bit版に特化したライブラリの使用もできるようになりました。現在、サポートされている64bitのOS上で32bit版のSecurityGatewayを使用している場合、64bit版のSecurityGatewayをダウンロードを行ない、既存の環境へ上書きインストールするだけで対応可能です。

主な新機能

セキュアメッセージポータル 92

SecurityGatewayのセキュアメッセージ機能を使うと、メッセージをSecurityGatewayへ残したまま、ドメイン外のユーザーに安全に送信する事ができるようになります。これはメッセージ用のウェブポータルを生成する事で実現しています。メールが送信されると、宛先ユーザーへセキュアメッセージの到着通知と、セキュアメッセージ宛先 93 アカウントを生成するためのリンクが届きます。このリンクへアクセスする事で、受信者はSecurityGatewayサーバー上のメールを確認できます。セキュアメッセージは、ブラウザ経由で、HTTPSを使った暗号化通信で管理されます。セキュアメッセージのご利用にあたっては、正規のSSL証明書 106 と、HTTPSの有効化 103 (参照: HTTPSサーバー 108)が必要です。受信者はSecurityGatewayのポータルサイトからメールの確認や返信、オプションで、指定したユーザー一覧に対して新たにセキュアメッセージの作成 97 が行えます。 参照: セキュアメッセージの宛先アカウントに関する詳細は 宛先 93 と 受信者オプション 95 を参照して下さい。

ユーザー毎のメール配信

- ユーザーの編集 47 ページに新しく追加した、メール配信セクションでは、ドメイン用のデフォルトメールサーバーに代わって、ユーザーがメール送信時に使用するドメインメールサーバーを選択できるようになりました。
- ドメインプロパティ 41 ダイアログへ新しいオプションを追加しました: *指定したドメインのユーザー以外には、そのドメインに対してこのメールサーバは使用できません。*
- こうした設定はローカルユーザーがクラウドサービスを使っていたり社内サーバーを使っていたりするハイブリッドな環境で利用できるようにしたものです。また、これにより1つのドメインと1つのSecurityGatewayで、ビジネスで使用する複数ロケーションで稼働しているメールサーバーへも、正しくメール配信が行えるようになります。

パフォーマンスカウンター 266

SecurityGatewayはWindowsのパフォーマンスモニターで使用できる、各種パフォーマンスカウンターを搭載しました。これにより、SecurityGatewayの状態をリアルタイムに監視できるようになりました。アク

ティブなインバウンドとアウトバンドのSMTPセッション数や、キューに配信されているメール状況、サーバの稼働状態や、稼働時間、ドメイン数、ユーザー数などの情報が確認できます。

追加の機能と変更点

- ユーザオプション[60]画面に、強固なパスワードを要求するオプションが追加されました。この機能は、ユーザー編集[47]ページにてユーザ単位で無効化することもできます。
- ダッシュボードと登録ページに、使われているサービスプロバイダー/プライベートクラウドエディションのキーについての情報を表示するようになりました。
- 添付ファイルフィルタリング用の宛先ホワイトリスト[210]宛先アドレスやワイルドカード付アドレスの一覧で、添付ファイルの禁止や隔離の処理や関連したフィルタリング処理から除外するために使用します。
- Lets Encrypt - 実行毎にログファイルを削除しないようになりました。

すべての変更とバグ修正の一覧については、Windowsスタートメニューの SecurityGatewayプログラムグループにあるリリースノートを参照してください。

バージョン8.0.0の新機能

主な新機能

- SecurityGatewayは クラスタリング[112]環境でのActive-Activeのデータベースレプリケーションに対応しました。ただし、この機能を使用するには、外部のレプリケーション製品が必要で、このヘルプファイルでは詳細を記載してはおりません。クラスタリング環境でActive-Activeのレプリケーションを行うには、次のPDFを参照してください: SecurityGateway: Configuring Active-Active Database Replication
- 情報漏えい保護機能-医学用語の検索[201] 医学用語のリストを定義し、それぞれにスコアを割り当てることができます。メッセージをスキャンし、一致する用語すべてのスコアが合算されます。定義した閾値を超えるスコアを持つメッセージに対するアクションを指定できます。
- メッセージの処理中に、カスタムプロセス/スクリプトを実行し、スクリプトの結果に基づいたアクションを選択する機能が追加されました。
  - スクリプトは、設定 ≫ システム ≫ ディレクトリ[110]にある "Sieve実行パス"で指定したディレクトリに配置する必要があります。
  - 実行やテストで使用できる "execute[239]" Sieveキーワードが追加されました。
  - 最初のパラメータは、スクリプト名です。現時点では、.bat, .exe, そして、PowerShellがサポートされています。
  - 2つ目のパラメータは、プロセスに渡される引数です。message_filenameには、現在処理されているメッセージのRFC822ソースへのフルパスを指定します。
  - 例として、 if execute "Test.ps1" "-msg '${message_filename}'" { }
- ドメイン内のすべてのアーカイブメッセージをエクスポート[92]する機能が追加されました。

- 変更/監査ログ[257] - 設定の変更や誰がそれを行ったのかを記録する新しいログファイルが追加されました。
- ユーザーと管理者へ指定日時での隔離レポート送信[71]を行う機能を追加しました。
- メールで送付される隔離レポートへ最後に送った隔離レポートの後で新たに届いたメールのみをレポートするオプションを追加[71]しました。隔離レポートは対象のメールがない場合は生成されません。

追加の機能と変更点

- "パスワードを紛失[60]" を見直し、ユーザーパスワードを変更するリンク情報を持つメールを送信するようになりました。
- LetsEncrypt[103] - 新しい発行者を検索するようにスクリプトを更新しました。
- DKIM署名[163]に、SHA265ハッシュを使えるように更新しました。
- XMLRPC APIとPowerShellモジュールに、`GetServerSetting` と `PutServerSetting` メソッドを追加しました。
- 設定/ユーザ | メール設定 | Emailプロトコル[76]の画面に、SMTP接続とプロトコルタイムアウトの値を指定できる機能を追加しました。
- メッセージログ[256] | メッセージ情報 | メッセージ タブから添付ファイルをダウンロードできる機能を追加しました。
- 警告、確認、プロンプトのメッセージボックスを更新しました。
- 参考として、いくつかのPowerShellスクリプトのサンプルを docs¥API¥PowerShell Samples フォルダに用意しました。
- クラスター化された環境で、HELOドメイン[76]を(設定/ユーザ | メール設定 | Emailプロトコル)から、各サーバ毎に指定できるようになりました。この値は、クラスタ内の各サーバ独自に設定できます。
- Webインターフェースからデータベースに対するSQLコマンドを手動で実行[122]できるようになりました。この機能は、技術サポートからの案内があった時のみ使用し、実行前にはデータベースのバックアップを取得することを推奨します。
- 隔離レポートの通知メール[71]に、"ブラックリストドメイン"リンクを付けるオプションを追加しました。

すべての変更とバグ修正の一覧については、WindowsスタートメニューのSecurity Gatewayプログラムグループにあるリリースノートを参照してください。

バージョン7.0.0の新機能

特記事項

- メールプロトコル[76] ページ(設定 ≫ メール設定 ≫ メールプロトコル)で、*使用可能な場合ESMTPを使用するとESMTP SIZEコマンドパラメータを隠す*の2つのオプションが削除されました。どちらのオプションも周知され、使用できる場合には常に使用されるようになったためです。

- clamd.confファイル内にある設定内容で、多くの変更や廃止項目があったため、インストーラでclamd.confファイルを上書きするようになりました。もし、clamd.confファイルに個別の設定を加えている場合、インストール後にファイル内の再調整をお願いします。
- ログ設定[259]オプションのoption to "曜日に基づくログファイルを作成する"オプションが削除されました。もし、このオプションを選択されていた場合、バージョンアップ処理によって、"新規ログファイルセットを毎日作成する"オプションへと変更されます。

新機能と変更点

クラスタリング[112]

SecurityGatewayのクラスタリング機能は、ネットワークにある2台以上のSecurityGatewayサーバー間で設定を共有する目的で開発されました。これにより、複数のSecurityGatewayサーバー間で、メールの処理に対するソフトウェア・ハードウェアとしてのロードバランシングを行い、処理速度の向上や効率化を図る事ができるようになります。また、サーバーのハードウェア、ソフトウェアとしての冗長化も行えるため、メールシステムの可用性を向上される事ができます。SecurityGatewayのクラスタリング機能について知っておくべきポイントを紹介します(より詳細な情報はクラスタリング[112]を参照してください):

- クラスタリング機能では、単一のデータベースの共有を複数台のアクティブなSecurityGatewayのインスタンス/サーバで行えるようにします。
- 外部のFirebirdバージョン3データベースサーバは、手動でインストールと設定を行う必要があります。
- インストーラ—にオプションが追加され、初期インストール中に外部Firebirdサーバパラメータを指定できるようになりました。既存のインストール環境では、コマンドラインからsgdbtool.exeコマンドを使って外部のFirebirdデータベースサーバへと接続できるように設定できます。
- クラスタサーバ間で共有するストレージは、各サーバからUNCパスでアクセスできる共有フォルダの設定が必要です。これによりユーザーアカウンをSecurityGateway Windowsサービス[117]へ変更する必要も生じる場合があります。
- プライマリサーバーで、定期メンテナンスタスクを実行します。
- クラスタ内の各サーバには、それぞれ異なるレジストレーションキーが必要となります。

Firebird 3 データベースのアップグレード[114]

- SecurityGateway 7.0にはFirebird 2 と 3 のランタイムが含まれており、どちらもインストールされます。
- SecurityGateway 7.0の新規インストールではFirebird 3が使用されます。
- バージョンアップでは、Firebird 2 が継続して使用されます。
- 新しいクラスタリング[112]機能にはFirebird 3 データベースが必要です。
- Firebird 3と互換性があるようにデータベースをアップグレードするには、2.xランタイムを使用してバックアップし、3.xランタイムを使用して復元する必要があります。 管理者は、コマンドラインから\SecurityGateway\Appのsgdbtool.exeコマンドを使用して既存のデータベースをアップデートすることができます。データベースを変換するには、SecurityGatewayサービスを停止し、コマンドプロンプトから"**sgdbtool.exe convertfb3**"を実行します。

2段階認証

ユーザーオプション[60]で管理者は、ドメイン毎に2段階認証（2FA）の使用を許可したり、必須とすることができます。もし2段階認証を必須とした場合、ログイン時に2段階認証の設定画面が表示されます。または、2段階認証のため、メイン -> アカウント -> 2段階認証[27]から設定を行ないます。

セキュリティ侵害を受けたパスワードかをチェック[63]

SecurityGatewayは、サードパーティーサービスから過去にセキュリティ侵害を受けたパスワードリストを参照し、ユーザーのパスワードが該当していないかをチェックすることができます。サービスにパスワードを送信することなく、このチェックを行なうことができます。ユーザーのパスワードがこのリストに該当しても、アカウントがハッキングされているわけではありません。以前に誰かが同じパスワードを使って攻撃を受けたことがあることを意味しています。表示されたパスワードは、ハッカーの辞書攻撃に使用される可能性があります。他で使われたことの無いユニークなパスワードは、より安全となります。詳しくは、Pwned Passwordsを参照してください。

ドメイン管理者が新規ドメインを作成

管理者を編集[50]ページで新しいオプションが追加され、ドメイン管理者が新しくドメインを作成できるよう許可できるようになりました。管理者は作成したドメインのドメイン管理者として自動登録されます。作成を許可するドメイン数の上限もここで指定できます。

新しいSMTP拡張[103]

RequireTLS (RFC 8689)[104]

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[207]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。RequireTLSの要件と設定についてはREQUIRETLS（RFC 8689）の有効化[104]オプションを参照します。RequireTLSの説明はRFC 8689: SMTP Require TLS Optionを参照してください。

SMTP MTA-STS (RFC 8461) - Strict Transport Security[104]

IETFによるMTA-STSに関する取りまとめが完了したため、この機能を実装しました。SMTP MTA Strict TransportSecurity（MTA-STS）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、デフォルトで有効となります。設定についての詳細はMTA-STS（RFC 8461）の有効化[104]を参照してください。MTA-STSについては、RFC 8461: SMTP MTA Strict Transport Security (MTA-STS)にて詳細をご確認頂けます。

SMTP TLS Reporting (RFC 8460)[105]

TLSレポートは、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、SecurityGateway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、幾つかの設定が用意されています。TLSレポーティ

ング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。

追加の機能と変更点

- SecurityGatewayの管理画面を、より現代的な表示にアップデートしました。
- FusionCharts 表示コンポーネントをアップデートしました。
- 指定した送信者からのメールには、ウィルススキャン152を行わない設定が追加されました。
- ホワイトリストをブラックリストより優先する220オプションが追加されました。
- LetsEncryptに、マシンで実行されているPowserShellのバージョンを確認するようにさせ、もし正しいバージョンがインストールされていない場合にはエラーで返すようになりました。
- LetsEncryptは、PSModulePath環境変数をチェックして、SGモジュールパスが含まれているかを確認します。含まれていない場合は、セッションに追加します。
- LetsEncryptは、LetsEncryptシステムのステージングとライブを切り替える際、アカウントを削除し再作成するようになりました。
- LetsEncryptは、チャレンジが失敗したときにLetsEncryptからエラーを取得し、ログと画面にデータを書き込むようになりました。
- LetsEncryptは、コマンドラインから使用できる新しい -Stagingスイッチを持っています。このスイッチが使用されると、スクリプトはLetsEncryptステージングシステムへ証明書の要求行ないます。
- JSTreeライブラリーをバージョン3.3.8へとアップデートしました。
- SecurityGateway Windowsサービス117 に、実行するユーザーアカウントの指定ができるようになりました。
- SIEVE Variables Extension RFC-5229に対応しました。
- SIEVE Variables Extensionに、:eval修飾子を追加し、シンプルに設定できるようになりました。

  例:

```
require "securitygateway";
require "variables";
require "fileinto";

if header :matches "from" "*" {
    set :length "length" "${1}";
    set :eval "fileintovar" "${length} * 25 - 1 / 8+3";
    fileinto "${fileintovar}";
}
```

- "曜日に基づくログファイルを作成する"オプションが削除されました。もし、このオプションを選択されていた場合、バージョンアップ処理によって、"新規ログファイルセットを毎日作成する259"オプションへと変更されます。
- パスワード入力時に、入力したパスワードの表示をする/しないのオプションが追加されました。ユーザーオプション60 画面にて、このオプションを無効にすることもできます。

- Cyren AVアップデータが、ウィルス定義ファイルのダウンロード時にTLSを使用するようになりました。
- ログファイル名にコンピューター名を含む[259]オプションを追加しました。このオプションは、クラスタ構成にある複数のサーバがUNCパスを使って、同一のログ保存場所を使用する場合に必要です。
- インストーラへ、初期インストール時に外部のFirebirdサーバを指定するパラメータオプションが追加されました。
- Chilkatライブラリーをバージョン9.5.0.82へとアップデートしました。
- ログオプション[259]へ指定したIPアドレスからのSMTP/HTTP接続ログを記録しないオプションが追加されました。指定したIPアドレスからの不完全もしくは、拒否したSMTPメッセージはデータベースにも記録されません。もしメッセージの配信が行えた際には、データベースに記録されます。
- Sieveスクリプトの処理へ、SecurityGatewayがメッセージを配信するにあたり変更や特定をおこなうためのSMTPエンベロープSenderの指定に、"changesender"を使用することができるようになりました。
- Cyren AVエンジンをバージョン6.3.0r2へとアップデートしました。
- ClamAVをバージョン 0.102.4へと更新しました。

すべての変更とバグ修正の一覧については、WindowsスタートメニューのSecurityGatewayプログラムグループにあるリリースノートを参照してください。

バージョン6.5.0の新機能

特記事項

LetsEncrypt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。

新機能と変更点

- ClamAVのバージョンを0.102.0へとアップデートしました。
- Cyren AV エンジンが、Version 6.2.2 へとアップデートしました。
- 添付ファイルのフィルタリング[210]機能において、RAR形式の検索も行えるようになりました。
- アーカイブオプションとして、特定のメールアドレスとの内部メールと外部メール、全てのメールを含むジャーナルレポート[79]送信オプションが追加されました。
- RMail[191]処理を行なうためにトリガーとして使用される件名タグを削除する機能が追加されました。
- RMail[191]処理から予定表への会議招集メッセージを除外することができるようになりました。

- 外部サーバのFirebirdサーバを使用できるようになりました。sgdbtool.exeから、"-setdbconnect"パラメータを使って、データベースへのアクセスのためのIPアドレスやパス/エイリアス、ユーザー名、パスワードを指定できるようになりました。
- Webインターフェース内の「隔離メールに"ブラックリスト"リンクを含める」の記述を「*隔離リストとメールに"ブラックリスト"オプションを含める*[71]」へと変更し、ユーザーの隔離メールリスト表示に反映しました。
- XML API機能において、Sieve スクリプトを管理できるようになりました。
- XML API機能において、アーカイブ機能の有効化やアーカイブストアの管理を行えるようになりました。
- DKIM ADSPに関連する全ての設定項目が削除されました。
- TNEF（winmail.dat）形式のファイル内にある制限された添付ファイルのウィルスチェックが行えるようになりました。
- ドメインメールサーバからのメッセージであれば、SMTPセッションの認証が行われていなくても、DKIM署名（機能が有効になっていれば）を行うようになりました。
- ウィルススキャン[152]において、ドキュメント内のマクロの検出を行なうオプションが追加されました。
- レジストリへの反映が無効になっているため、64bitのWindowsOS上で稼働する32bit版のSecurityGatewayでも、"64bit版用としてのWindowsレジストリ"が使用されます。そのため、Wow6432bitノードに存在する可能性のあるレジストリキーと値は、HKEY_LOCAL_MACHINE¥SOFTWARE¥ALT-N Technologies¥SecurityGatewayにもコピーされるようになりました。

- すべての変更とバグ修正の一覧については、WindowsスタートメニューのSecurityGatewayプログラムグループにあるリリースノートを参照してください。

バージョン6.1.0の新機能

変更点と新機能

アーカイブコンプライアンス[91]

新しいアーカイブ画面ではアーカイブメールの保存や特定のユーザーが送信（オプションで受信）したメールを削除するまでの期間をコントロールするのに使用でき、「訴訟ホールド」オプションで、SecurityGatewayで指定した権限に関わらず、一時的にアーカイブメールが削除するのを防ぐ事ができるようになりました。

その他の新しいアーカイブ機能

- アカウント ≫ ユーザーオプション ≫ アクセスコントロール[60]へ、ユーザーはアカウント宛又はアカウントから送信したメールアーカイブを削除できるというオプションを新たに追加しました。このオプションはデフォルトで無効になっています。
- ユーザー設定[27]ページへ新しいリンクを追加し、ユーザー宛のメールやユーザーから送信した全てのアーカイブ済メールを削除できるようになりました。メールを削除する前に、確認ボックスが表示されます。

Office 365 / Azure AD ユーザー検証

ユーザー検証ソースとしてOffice 365/Azure Active これによりSecurityGatewayがOffice 365/Azure Active Directoryのユーザーを直接クエリしたり、関連するエイリアスを取得したり、パスワード認証する事ができるようになりました。Office 365/Azure Active Directoryのクエリを実行するには、最初に https://www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=1229の手順に沿って権限を付与する必要があります。

その他の変更点

- ブラックリストとホワイトリストの検索が行えるようになりました。
- 隔離レポートをスコアでソートする機能を追加しました。スパムスコアが低いものや誤検知と思われるメールはレポートの上位に表示されます。
- LetsEncryptで指定した証明書を削除するためのオプションを追加しました。SecurityGatewayと同じFQDNをサブジェクトとして保有しており、期限切れから30日を経過した証明書が対象となります。このオプションを使用するには、コマンドラインパラメータで -RemoveOldCertificatesを渡してください。
- LetsEncrypt: デフォルトでPowershellではSSLv3とTLS1.0のみに対応しています。アクティブセッションで TLS1.0,1.1, 1.2へ対応するための新しいコードを追加しました。PowerShellでクライアントのオペレーティングシステムで SSL/TLSプロトコルの対応を許可する事ができるようになりました。オペレーティングシステムのクライアントプロトコルでTLS1.0を無効化すると、PowerShellはTLS1.0を使用しなくなります。
- Chilkatライブラリをバージョン9.5.0.78へアップデートしました。

バージョン6.0.0の新機能

特記事項

SecurityGatewayは、Windows Vista または Windows Server 2008 以上で稼働するようになりました。マイクロソフト社によるセキュリティ修正プログラムの廃止や、必要な機能が搭載されていないことから、Windows XPやWindows 2003上での稼働ができなくなりました。

主な新機能

メッセージアーカイブ

長期間のメールアーカイブを行えるようになりました。アーカイブされたメールは、全文検索が可能になります。アーカイブされたメッセージは、設定可能なアーカイブストアに格納されます。

64bit バージョンのご提供

64bit版のオペレーティングシステム上で、SecurityGatewayの64bit版をご使用頂けるようになりました。64bit版では、搭載されたメモリーを有効に使用し、より多くの数のセッションを張れるようになりました。

情報漏えい保護機能の向上

情報漏洩保護 193 に向けたルールのテンプレートを60以上に増やし、ご利用頂けるようになりました。

その他の変更点と新機能

- Google G suiteへの対応が強化されました。ドメインメールサーバーが、Google G Suite (aspmx.l.google.com)へメール送信を行なう設定となっていた場合、Google G Suiteからの接続をドメインメールサーバからとして扱うことになりました。 これにより、SecurityGatewayをGoogle G Suiteの アウトバウントゲートウェイ として、使用できるようになりました。
- RFCに準拠していないメッセージや"'From' がDMARCと互換性がない場合、受信メッセージを拒否する"といったメッセージの受信を拒否するオプションが追加されました。
- メッセージログでの表示において、インバウンド/アウトバウンドのアイコンを更新しました。
- IPアドレスが異なっていても、各ドメイン毎に異なるサーバ証明書の使用が可能な、TLS Server Name Indication (SNI)に対応しました。複数のサーバ証明書が有効になっている場合、SecurityGatewayでは、サブジェクトの別名の項目に記載されたホスト名で対応するようになりました。
- 自己発行するサーバ証明書のキューサイズが大きくなりました。これは、SHA1に変わりSHA2を使用したり、サブジェクトの別名に実体のホスト名を自動的に含めるようになったからです。
- Cyren AVエンジンをバージョン 6.2.0r2 へと更新しました。このバージョンにより、これまでいくつかのスキャンエラーが発生していた問題が修正されます。
- SMTPコールバック検証において、STARTTLSを使った暗号化通信を行えるようになりました。
- ClamAV をバージョン 0.101.1 へと更新しました。

セクション 2

2 メイン

2.1 アカウント

アカウント用開始ページは、SecurityGatewayユーザアカウントでサインインすると最初に表示されるページです。ここには、アカウント設定とアカウント統計の2つのセクションがあります。アカウント設定セクションには、よく使われる機能へのリンクが含まれており、クリックすると、関連機能のページへ移動できます。アカウント統計セクションでは、直近24時間のアカウントのアクティビティに関連した4種類のレポートが表示されています。**適正vsジャンクメールレポート**では、アカウントについて処理された適正または正当なメッセージ対ジャンクメッセージの合計を示します。ジャンクメッセージは、スパム、なりすまし、ウィルスを含むなどとして識別されるメッセージです。**ジャンクメール分析レポート**は、受信したジャンクメールの総計とカテゴリのタイプを示します。**受信対送信メッセージレポート**では、受信したインバウンドメッセージと送信したアウトバウンドメッセージの総数を示します。**上位のスパムソースレポート**では、上位のスパムメッセージの差出人を示します。

左側のナビゲーションペインのメインヘッダー配下には、ユーザアカウントに関連するリンクが表示されています。

アカウント

- ランディングページ
  アカウント用のランディングページで、アカウント関連タスクや統計レポートへのリンクが表示されています。
- 2段階認証 [27] – 暗号化された接続でサインインした場合（SecurityGatewayへアクセスする際、ブラウザでhttps://を使ったアドレスを指定した場合）、2段階認証のメニューが、アカウントオプションとして表示されます。2段階認証は追加のセキュリティレイヤーで、パスワードに加え、アプリケーションで生成される特別なセキュリティコードを入力してサインインする手法です。注意点：2段階認証は、暗号化された接続を使っていた場合であっても利用できない場合があります。
- 設定 [27]
  このリンクは、パスワード変更、隔離設定、自動ホワイトリスト設定、ページ毎の表示数の指定が行える、アカウントページ設定ページに移動します。
- ホワイトリスト [30]
  パーソナルなホワイトリストを表示するリンクです。ホワイトリストへのアドレスの追加は、スパムあるいはブロックされる差出人のメッセージを誤って識別することから防止することに役立ちます。
- ブラックリスト [32]
  パーソナルなブラックリストを表示するリンクです。特定のアドレスから、以降メッセージを受信しないためにブラックリストへアドレスを追加します。

- 隔離内容を表示 [34]
  SecurityGatewayで受信された時、疑わしいと認識したメッセージを保存するフォルダです。このページから、隔離メッセージの閲覧、解放（メッセージに問題がなく配信されるべきメッセージ）、削除あるいはホワイトリスト [30] あるいはブラックリスト [32] へ差出人を追加することができます。
- メッセージログを表示 [35]
  送受信された全メッセージのログ表示のリンクです。このログにおいて、各メッセージの詳細の参照、スパムあるいは非スパムとしてのメッセージへフラグ付け、ホワイトリストあるいはブラックリストアドレスの指定ができます。

SecurityGatewayで指定されたアカウントのアクセスレベルによって利用できないオプションがあります。

2.1.1 2段階認証

暗号化された接続でサインインした場合（SecurityGatewayへアクセスする際、ブラウザでhttps://を使ったアドレスを指定した場合）、2段階認証のメニューが、アカウントオプションとして表示されます。2段階認証は追加のセキュリティレイヤーで、パスワードに加え、アプリケーションで生成される特別なセキュリティコードを入力してサインインする手法です。

2段階認証は、暗号化された接続を使っていた場合であっても利用できない場合があります。

2段階認証の設定

2段階認証を使用するには、Google Authenticatorアプリ（又はGoogle Authenticatorに互換性のある他のアプリ）をスマートフォン等のモバイル端末へインストールしておく必要があります。「Google Authenticator」をアプリとして検索してください。

1. In SecurityGatewayの、アカウントの中の2段階認証ページで、現在のパスワードを入力します。
2. 2段階認証をクリックします。QRコードとSecretを表示ボタンが表示されます。Secretを表示をクリックしてキーを確認します。
3. 認証アプリで、QRコードをスキャンを選択し、新しいアカウント設定を行います。または、手順2のSecretを表示で取得したキーを「設定キーを入力」で入力します。
4. QRコードをスキャンすると、アプリで5桁のセキュリティキーが表示されます。
5. SecurityGatewayで、認証コードを入力し、「ペアリングを検証」をクリックします。
6. 今後はSecurityGatewayへサインインする際、パスワード入力後、アプリケーションで表示されるコードを入力 する必要があります。

2段階認証の無効化

2段階認証を無効化するには、2段階認証ページでパスワードを入力し、**2段階認証を無効化**をクリックします。

2.1.2 設定

アカウント設定ページではパスワードの変更、隔離設定の初期値、自動ホワイトリストの有効化、ページへ表示するアイテム数の設定を行う事ができます。

オプションは、SecurityGateway用のアクセス権によって、利用できないものもあります。

パスワード変更

パスワード
パスワードの変更は、ここへ新しいパスワードを入力します。

パスワード(確認)
上のパスワード入力ボックスの新規パスワードを入力後、ここへ確認のための同じパスワードを入力してから、保存をクリックします。

隔離

ドメインでデフォルトの隔離設定を使用する
このオプションはデフォルトで選択されます。このオプションを選択することで、隔離 34 オプション設定を残しますが、オプションはメール管理者により通常設定されます。

隔離設定の指定を許可する
隔離設定を変更する場合は、このオプションを選択して、必要な設定を選択します。

サーバ上の隔離メッセージを保持する
このオプションを選択すると、SecurityGatewayでは、非常に疑わしいと思われる隔離 34 受信メッセージを後ほど調べるために保持します。

隔離フォルダの内容一覧のメールを送信する:
この選択するとSecurityGatewayで疑わしいメッセージを隔離する場合に、隔離フォルダの現在の内容一覧を定期的にメールで送信することができます。

しない
このオプションは、隔離されたメッセージの一覧をメールで受信しません。

指定時間ごと
特定の時間ごとにメールを受信する場合には、このオプションを選択して、送信間隔の時間を指定してください。

毎日
このオプションはデフォルトです。このオプションは、隔離されたメッセージの一覧を毎日送信します。

毎週
1週間に一度受信する場合は、このオプションを選択します。

隔離メールのソート:[宛先|送信者|件名]
隔離メールの一覧をどのようにソートするのかをこのオプションで指定します。デフォルトで一覧はメール受信日でソートされていますが、これを送信者や件名でソートする事ができます。

隔離リストとメールに「ブラックリスト」オプションを含める
このオプションを使用すると、隔離メールの一覧画面と隔離レポート通知へリンクが表示され、ここから送信元のアドレスをブラックリストへ追加できるようになります。

隔離リストとメールに「ブラックリストドメイン」オプションを含める
このオプションを使用すると、隔離メールの一覧画面と隔離レポート通知へリンクが表示され、ここから送信元のドメインをブラックリストへ追加できるようになります。

隔離メール内に"メッセージの表示"オプションを含める
このオプションを使用すると、隔離レポートメールへ「メッセージの表示」が含まれるようになり、ユーザーが隔離されたメールを確認できるようになります。

隔離メッセージのフィルタをメールサーバまたはクライアントで許可する
受信メッセージの隔離をしない場合には、このオプションを選択します。隔離されるはずのメッセージは、通常通り配信されます。これは、代わりにメッセージをサーバやクライアントでフィルタすることを許可する場合に便利です。隔離されたメッセージを確認するために、メッセージの`Subject`にタグを追加、あるいは特別なヘッダをメッセージに追加する2つのオプションを使用することができます。そのタグやヘッダで検索するためにサーバやメールクライアントにフィルタを作成することができます。

...件名に[*text*]のタグを付ける
このチェックボックスを選択すると、隔離オプションを選択した時に、隔離されるメッセージの件名`Subject`にテキストを追加します。追加するテキストデフォルトは、`"*** SPAM ***"`です。これは、必要なテキストに変更することができます。

... [*text*]のヘッダを追加
このチェックボックスを選択すると、隔離されるメッセージに特別のヘッダを追加することができます。多くのメールクライアントでは、メッセージプロパティおよびソース表示なしに、このヘッダを参照することはできませんが、さまざまなメールクライアントやサーバでは、それらのメッセージを特定のフォルダへ移動や削除することを行うために、これらのヘッダを探すためにフィルタを作成ができます。このオプションでのヘッダは、`"X-Spam-Flag: YES"`ですが、別のテキストに変更することができます。

オプション

このアカウントへのメールをアーカイブしない
対象アカウントのドメインでアーカイブをするよう設定されていた場合であっても、対象からのメールやアカウント宛のメールをアーカイブしない場合にはこのオプションを有効にします。このオプションは管理者のみが設定できます。

対象アカウントの全アーカイブ済メッセージを削除
対象ユーザーが送受信した、全てのアーカイブ済メールを削除するにはこのリンクをクリックします。アーカイブ済メールの削除を本当に行うかどうかの確認用ダイアログが表示されます。

送信先を自動的にホワイトリストに入れる
このチェックボックスを選択すると、メールメッセージを送信するアドレスは自動的にホワイトリスト 30 に追加されます。これは、送信アドレスからのメッセージが誤ってスパムで識別されないか、将来ブロックされないことを確認することに役立ちます。

このアカウント当てのメッセージでアンチスパムテストを実行しない
アカウント宛に送られるメッセージでアンチスパムテストをサーバで実行しない場合には、このチェックボックスを選択します。これはアンチスパムのテストの実行を禁止し、アカウントで受信する迷惑メール数が増大することになります。

アカウントを「ハイジャック検出」から除外
アカウントをハイジャックアカウント検出から除外するにはこのオプションを有効にします。定常的に短い時間で大量のメールを送信するアカウントには、この設定が必要な場合があります。

統計グラフを表示する時間
統計グラフをダッシュボートとランディングページ[26]へ表示する時間を選択するのにこのオプションを使用します。自動、手動、表示しない、を選択できます。

言語
システム生成のメッセージを送信する場合、サーバで使用する言語をドロップダウンリストから設定してください。

1ページに表示する項目数
このオプションは、ホワイトリストのアドレス、メッセージログのエントリなどページ単位での表示項目数を指定します。1ページで表示できない時には、各ページの下部にページ移動のコントロールがあります。

このデバイス/ブラウザで認証情報を記憶しない
SecurityGatewayへサインインする際、「*このデバイスで認証情報を記憶する*」オプションを使用していた場合、このオプションが表示されます。このデバイスやブラウザで認証情報を記憶しないようにする場合はリンクをクリックします。次回のサインインの際、*このデバイスで認証情報を記憶する*オプションの利用は継続できます。

2.1.3 ホワイトリスト

ホワイトリストはパーソナルなアドレスホワイトリストです。ホワイトリストへのアドレスの追加は、スパムあるいはブロックされる差出人のメッセージを誤って識別することから防止することに役立ちます。通常、1つずつこのリストにアドレスを追加しますが、テキストファイルから複数のアドレスをインポートする機能もあります。さらにホワイトリストにはエクスポート機能があり、カンマ区切り(CSV)ファイルで保存します。

ホワイトリストへアドレスを追加する

ホワイトリストへアドレスを追加するには、ページ上部のツールバーの**新規**をクリックします。これはアドレスを追加するためのホワイトリストエントリ[32]ページを開きます。(次を参照)

ホワイトリストのアドレスを編集する
ホワイトリストのアドレスを編集するには、編集するエントリをダブルクリックするか、ページ上部のツールバーの**編集**をクリックします。これは[ホワイトリストエントリ](#) 32ページで編集するエントリを開きます。

ホワイトリストのアドレスを削除する
ホワイトリストのアドレスを削除するには、削除するアイテムを選択してからページ上部のツールバーで**削除**をクリックします。複数のアイテムを削除する場合はCTRLキーを押しながらアイテムを選択します。選択後に削除をクリックすると、アイテム削除の確認ダイアログが現れます。

ホワイトリストへアドレスをインポートする
ホワイトリストへアドレスリストをインポートするには、ページ上部のツールバーの**読み込み**をクリックします。これはリストの読み込みを開きます。**参照**ボタンをクリックしてアドレスを含むテキストファイルを指定してから、**リストの読み込み**をクリックします。

テキストファイルでは1行に1つのアドレスとして、通常の形式以外あるいは読み込み処理を中断する文字を避けるために標準テキストエディタ(ノートパッドなど)を使用して作成する必要があります。

CSVファイルを使用したインポート
インポートされたアドレスごとに対応するコメントを追加する場合、アドレスの単純なリストを使う代わりに、アドレスをインポートで使用するCSVファイルを必要とします。CSVファイルを作成するために、ノートパッドのようなプレーンテキストエディタを使用することができます。単にフォーマットに従ってファイルを作成して、filename.csv.として保存してください。カラムのデータの順序を通知するために、CSVファイルの最初の行はマッピング行にする必要があります。このファイルの各々のアイテムは、引用句で含み、カンマで区切る必要があります。

形式:
CSVでは、2つのカラム(`Value`と`Comments`)が必要:`Value`カラムには、メールアドレス、`Comments`カラムには登録に関するメモが必要です。コメントのないエントリには、引用符を""にする必要があります。

例:CSVファイルの内容

```
"Value","Comments"
"myfriend@example.net","A comment about my friend."
"someone@example.org",""
"mister@domain.com","A comment about mister."
```

ホワイトリストからアドレスをエクスポート
ホワイトリストアドレスをエクスポートするには:

1. ページ上部のツールバーの**書き出し**をクリックします。ファイルのダウンロードダイアログが現れます。
2. **保存**をクリックします。
3. ファイル名と場所を指定します。
4. **保存**をクリックしてダイアログを閉じます。

ホワイトリスト エントリ

このページは新規アドレスの追加や既存のエントリの編集に使用します。**新規** あるいは**編集**をクリックする時に現れます。

エントリの一覧

メールアドレス:
最初のボックスに、ホワイトリストへ追加するメールアドレスを入力します。ドメインで、すべてのアドレスをホワイトリストにするために、アドレスの一部でアスタリスクを使用することができます。例えば、"*@example.org"は、example.orgでメッセージすべてをホワイトリストへ登録します。

コメント:
このフィールドをエントリについてのコメントに使用します。

保存して閉じる
入力を完了したら、ホワイトリストへエントリを保存するために**保存して閉じる**をクリックします。

閉じる
保存しないでホワイトリストエントリを閉じる場合には、このボタンをクリックします。

2.1.4 ブラックリスト

ブラックリストはパーソナルなアドレスブラックリストです。メール配信を防ぎたいアドレスをブラックリストへ追加する事ができます。通常、1つずつこのリストにアドレスを追加しますが、テキストファイルから複数のアドレスをインポートする機能もあります。さらにブラックリストにはエクスポート機能があり、カンマ区切り(CSV)ファイルで保存します。

ブラックリストへアドレスを追加する

ブラックリストへアドレスを追加するには、ページ上部のツールバーの**新規**をクリックし、アドレス追加用のブラックリストのエントリ 33ページを起動します。(次を参照)

ブラックリストのアドレスを編集する

ブラックリストのアドレスを編集するには、編集するエントリをダブルクリックするか、ページ上部のツールバーの**編集**をクリックします。これはブラックリストのエントリ 33ページで編集するエントリを開きます。

ブラックリストのアドレスを削除する

ブラックリストのアドレスを削除するには、削除するアイテムを選択してからページ上部のツールバーで**削除**をクリックします。複数のアイテムを削除する場合はCTRLキーを押しながらアイテムを選択します。選択後に**削除**をクリックすると、アイテム削除の確認ダイアログが現れます。

ブラックリストへアドレスをインポートする

ブラックリストへアドレスリストをインポートするには、ページ上部のツールバーの**読み込み**をクリックします。これはリストの読み込みを開きます。**参照**ボタンをクリックしてアドレスを含むテキストファイルを指定してから、**リストの読み込み**をクリックします。

テキストファイルでは1行に1つのアドレスとして、通常の形式以外あるいは読み込み処理を中断する文字を避けるために標準テキストエディタ(ノートパッドなど)を使用して作成する必要があります。

CSV ファイルを使用したインポート

インポートされたアドレスごとに対応するコメントを追加する場合、アドレスの単純なリストを使う代わりに、アドレスをインポートで使用するCSVファイルを必要とします。CSVファイルを作成するために、ノートパッドのようなプレーンテキストエディタを使用することができます。単にフォーマットに従ってファイルを作成して、filename.csv.として保存してください。カラムのデータの順序を通知するために、CSVファイルの最初の行はマッピング行にする必要があります。このファイルの各々のアイテムは、引用句で含み、カンマで区切る必要があります。

形式:

CSVでは、2つのカラム(ValueとComments)が必要:Valueカラムには、メールアドレス、Commentsカラムには登録に関するメモが必要です。コメントのないエントリには、引用符を""にする必要があります。

例:CSVファイルの内容:

```
"Value","Comments"
"myenemy@example.net","A comment about my enemy."
"someone@example.org",""
"mister@domain.com","A comment about mister."
```

ブラックリストからアドレスをエクスポート

ブラックリストアドレスをエクスポートするには:

1. ページ上部のツールバーの**書き出し**をクリックします。ファイルのダウンロードダイアログが現れます。
2. **保存**をクリックします。
3. ファイル名と場所を指定します。
4. **保存**をクリックしてダイアログを閉じます。

ブラックリストのエントリ

このページは新規アドレスの追加や既存のエントリの編集に使用します。**新規** あるいは**編集**をクリックする時に現れます。

エントリの一覧

メールアドレス:

最初のボックスに、ブラックリストへ追加するメールアドレスを入力します。ドメインで、すべてのアドレスをブラックリストにするために、アドレスの一部でアスタリスクを使用することができます。例えば、"*@example.org"は、example.orgで、誰からのメッセージすべてをブラックリストへ登録します。

コメント:

このフィールドをエントリについてのコメントに使用します。

保存して閉じる
入力を完了したら、ブラックリストへエントリを保存するために**保存して閉じる**をクリックします。

閉じる
保存しないでブラックリストエントリを閉じる場合には、このボタンをクリックします。

2.2 隔離内容を表示

隔離は、SecurityGatewayで配信するにはあまりに疑わしいことを思われる受信メッセージの一時的保存用の場所です。スパムと他の疑わしい、または不必要なメッセージの流入を受信から保護することに使用します。隔離されたメッセージはSecurityGatewayサーバで保持され、ログインを行い、閲覧、削除、通常配信で隔離から解放することができます。隔離を管理するために、SecurityGatewayでは、隔離フォルダのコンテンツを通知するメッセージを定期的に送信します。隔離設定は、設定 27 ページで管理することができます。

すべてのユーザが隔離にアクセスでき隔離設定を修正ができるというわけではありません。

隔離のエントリは、メッセージが隔離された日付と時間、差出人、宛先と件名のカラムがあります。さらに、メッセージが隔離された理由、サイズとSecurityGatewayがスパムと識別する内部スコアのカラムがあります。

隔離の上部には、処理を行うための、いくつかのボタンがあります。

- **更新**
  このボタンをクリックすると、参照を開始してから追加されたメッセージを表示するために隔離表示を更新できます。
- **検索**
  隔離をフィルタする特定のメッセージだけを表示するために、詳細な検索機能を使用します。メッセージが隔離された理由、ヘッダの特定のテキスト、日付または日付範囲などに基づいて検索することができます。
  隔離を検索するには: ツールバーの**検索**ボタンをクリックして検索ウィンドウを開き、検索条件を入力し**検索**ボタンをクリックします。検索ウィンドウの下に検索結果が現れます。隔離では、検索パラメータに一致したメッセージのみが表示されるようになります。検索ウィンドウを隠すには、ツールバーの**検索**ボタンを再度クリックします。検索を終了するには、検索ウィンドウのキャンセルをクリックして最初の隔離表示に戻します。
- **表示**
  メッセージを選び、このボタンをクリックすると、メッセージ情報画面を開きます。このタブには、Transcript、メッセージとソースの3つがあります。Transcriptタブには、SecurityGatewayとサーバまたはメッセージを送信しているクライアント間での通信の詳細な記録があります。メッセージタブにはメッセージの実際の内容、ソースタブにはヘッダやHTMLコードなどメッセージのソースがあります。
- **解放**
  メッセージを選択して、このボタンをクリックすると、隔離からメールを解放します。
- **ホワイトリスト**
  メッセージを選択して、このボタンをクリックすると、ホワイトリスト 30へ差出人を追加します。

- **削除**
  メッセージを選択して、このボタンをクリックするとメッセージを削除します。
- **ブラックリスト**
  メッセージを選択して、このボタンをクリックすると、ブラックリスト[32]へ差出人を追加します。
- **すべて削除**
  このボタンをクリックすると、隔離メッセージをすべて削除します。

2.3 メッセージログを表示

メッセージログには送受信したメッセージのエントリがあります。メッセージが処理された日時、差出人と宛先、メッセージの件名の一覧にします。さらに、配信、隔離や拒否などの結果も含まれます。配信されない場合には、差出人がブラックリスト、禁止された添付ファイルなどの理由を提示します。 各エントリには、メッセージサイズとスコアも表示します。メッセージスコアが、メッセージがスパムであるという可能性を決定するために、内部的にSecurity Gatewayによって使われます。

すべてのユーザがメッセージログにアクセスできるわけではありません。

メッセージログのツールバーには、作業を実行するための、いくつかのボタンがあります。

- **更新**
  このボタンをクリックすると、参照を開始してから追加されたメッセージを表示するために更新できます。
- **検索**
  メッセージログをフィルタする特定のメッセージだけ表示するために、詳細な検索機能を使用します。メッセージの送受信、ヘッダの特定のテキスト、日付または日付範囲などに基づいて検索することができます。
  メッセージログの検索をするには: ツールバーの**検索**ボタンをクリックして検索ウィンドウを開き、検索条件を入力し**検索**ボタンをクリックします。メッセージログの下に検索結果が現れます。検索ウィンドウを隠すには、ツールバーの**検索**ボタンを再度クリックします。検索を終了するには、検索ウィンドウの**キャンセル**をクリックして最初のメッセージログ表示に戻します。
- **詳細**
  メッセージを選び、このボタンをクリックするとメッセージ情報を開きます。これにはTranscript、メッセージとソースの3つのタブがあります。Transcriptタブには配信プロセスの写しがありSecurity Gatewayとサーバまたはメッセージを送信しているクライアントの通信についての詳細ログがあります。メッセージタブには、メッセージの実際の内容があります。これは、メッセージの古さ、メッセージが配信およびSecurity Gatewayでのデータ保持の設定により利用できない場合もあります。ソースタブにはヘッダやHTMLコードなどメッセージのソースがあります。ソースは、メッセージの古さやSecurity Gatewayが情報を保存しない設定の場合は利用できません。
- **再配信**
  一覧から1つまたは複数のメッセージを選択して、このボタンをクリックすると再配信を行います。Ctrl+ClickあるいはShift+クリックで複数のメッセージを選択できます。このオプションはデータベースからメッセージのコンテントが削除された場合には使用できません。
- **Spam**
  メッセージを選択して、このボタンをクリックするとスパムとしてマークします。これは以降のメッセー

ジでスパムの識別に役立ちます。このボタンは、一部のケースや、このオプションをサポートしていない場合には利用できない場合があります。

- **スパムではありません**
  メッセージを選択して、このボタンをクリックすると、非スパムとしてマークします。これは、以降スパムとして正規なメールを誤って識別しないようにできます。このボタンは、一部のケースや、このオプションをサポートしていない場合には利用できない場合があります。
- **ホワイトリスト**
  エントリを選択し、このボタンをクリックすると、差出人または宛先をホワイトリスト 30へ追加します。
- **ブラックリスト**
  エントリを選択し、このボタンをクリックすると、差出人または宛先をブラックリスト 32へ追加します。

セクション 3

3 設定/ユーザ

設定/ユーザ メニューには、SecurityGatewayの核となる7つの設定項目へのリンクが用意されています。ドメインとユーザアカウント、メール配信オプション、隔離設定、バックアップとデータベース設定、その他の設定ために使用します。セクション毎の概要は次の通りです。詳細はセクション概要またはセクション毎の個別ページをご覧ください。

アカウント 38
アカウントセクションには、ユーザアカウントとドメインに関するオプションがあります。ドメインとユーザアカウントの作成、ユーザ検証ソース指定、ユーザオプション設定が行えます。

メール設定 65
メール設定セクションにはメールに関する機能を管理する4つのリンクがあります。例えば、ユーザのメールアカウントが属するサーバの指定、隔離オプションの設定、さまざまなメール配信オプションの構成、その他技術的なオプション管理が行えます。

免責事項(ヘッダ/フッタ) 98
インバウンド、アウトバウンドおよびローカルメールメッセージにヘッダやフッタを追加することができます。 このページで免責事項の作成や管理を行う事ができます。

システム 103
設定/ユーザーメニューの中のシステムセクションからは、暗号化設定、HTTPインターフェース設定、ディレクトリ位置、ディスクの空き容量管理などシステム設定が行えます。

データベース 117
このセクションではSecurityGatewayで保存するデータの種類や容量、自動バックアップ、バックアップからの復元設定が行えます。

ソフトウェア更新 122
SecurityGatewayの最新バージョンが利用可能かどうかを確認します。ここから、手動で最新版の有無を確認したり、SecurityGatewayで自動確認を行うよう設定する事ができます。最新版が利用可能な場合、ウェブインターフェースから直接ダウンロードとインストールが行えます。

登録 123
登録ページでは、登録された名前や会社名、登録キー、製品といった登録情報の確認が行えます。

3.1 アカウント

設定/ユーザ 38 メニューのアカウントセクションには、SecurityGatewayユーザアカウントとドメインに関するオプションがあります。このセクションには次の5つのリンクがあります。

ドメイン 39 および ユーザ 45
ドメインおよびユーザを管理するための、ドメインリストとユーザリストです。ドメインリストを開くには、左側の枠でナビゲーションメニューの**設定/ユーザ**をクリックします。さらに、そのペインのアカウントセクションの**ドメインとユーザ**をクリックします。ユーザリストは、ドメインリストが選択し、ドメインリストのツールバーで**ユーザ**ボタンをクリックすると表示できます。

管理者 49
管理者リストは、SecurityGatewayで指定された、すべてのグローバルとドメイン管理者を管理するために使用します。グローバル管理者は、SecurityGatewayのほかの管理者アカウントおよび設定にわたる、すべての設定およびオプションの完全なコントロールを持ちます。ドメイン管理者は、権限を与えられたドメインに関連するすべての設定およびオプションにアクセスすることができます。違うドメインに特定のグローバル設定またはアクセス設定を編集することができません。

ユーザ検証ソース 52
このページはユーザ検証ソースの全てを管理する使用し、未知のローカルアドレスの妥当性を確認する使用されます。受信メッセージが未知のローカルユーザにアドレス指定される時は、SecurityGatewayではユーザのドメインが未知のアドレスが合法的かどうか照合するように構成されるユーザ検証ソースを問い合わせます。アドレスが有効である場合、SecurityGatewayはメッセージをドメインのドメインメールサーバ 65 に配信するアドレスおよび試みのためにユーザアカウントを作成します。アドレスが無効である場合、メッセージは拒否されます。

自動ドメイン生成 59
このページは、未知のドメインの未知のユーザに対する受信メッセージが既定のユーザ検証ソースによって確認することができる時には、自動的に新しいSecurityGatewayドメインを作成するか指定するために使用します。

ユーザオプション 60
ユーザがSecurityGatewayアカウントでログインした際、アクセスできるオプションをこのページで指定します。ユーザーオプションは、ドメイン毎か全体設定として指定できます。

3.1.1 ドメインとユーザ

3.1.1.1 ドメインリスト


ドメインリストでは、ドメインとユーザ管理が行えます。ドメインリストを開くには、左側のボックスでナビゲーションメニューの**設定/ユーザ**をクリックし、アカウントセクションで**ドメインとユーザ**をクリックします。右側のSecurityGatewayセットアップページのドメインセクション以下にある、ドメイン表示からもドメインリストを開くことができます。

ドメインリストは、2つのカラム(名前とユーザ) があります。名前カラムはドメインのすべての一覧を示し、ユーザカラムは各ドメインに属しているユーザアカウント数を一覧にします。ドメインのプロパティ[41]を閲覧または編集するためには、リストで必要なドメインをダブルクリックします。ドメインのユーザー覧[45]を閲覧するために、対応するドメインのユーザリンクをクリックします。

ページ上位のツールバーは、ドメインリストに関連した各種のタスクを開始する使用します。ほとんどのツールバーのボタンは、ボタンをクリックする前に、最初にリストからドメインを選択することが必要です。例外は新規、読み込みおよび書き出し、です。これらのボタンは、ドメインを選択することなくクリックすることができます。ツールバーには、10のオプションがあります。

新規
新規のSecurityGatewayドメインを作成するために使用するプロパティ[41]ダイアログを開くために**新規**をクリックします。プロパティでは、ドメインの名前、メールサーバおよび他の必要な設定の指定ができます。

編集
ドメインリストで現在選択されるドメインに対応するプロパティ[41]ダイアログを開くために、ツールバーのボタンの**編集**を使用します。あるいは、エントリをダブルクリックすることによって、プロパティダイアログを開くこともできます。

削除
ドメインを削除するために、リストからドメインを選択し**削除**をクリックします。ドメインを削除すると、削除の確認ボックスはが開きます。Ctrlキーを押しながら選択することで複数のドメインを選択することができます。

検索条件を表示/隠す
検索条件を表示をクリックし、ドメイン一覧の検索オプションを表示します。ドメイン名のボックスへテキストを入力し、検索をクリックすると、ドメイン一覧がフィルタされ、入力したテキストが含まれるドメイン名のみが表示されます。X検索を中止をクリックすると、検索を中止し、通常のドメイン一覧画面へ戻ります。

ユーザ
ドメインリストからエントリを選択し、ドメインのユーザリスト[45]を開くには、ツールバーの**ユーザ**をクリックします。ドメインリストと同様で、ユーザリストはドメインのユーザアカウントを管理するために使用します。

メッセージ
このボタンは、選択されたドメインについてメッセージログ[249]を開くために使用します。メッセージログには、ドメインで送受信されるメッセージごとにエントリが登録されています。メッセージログから任意のエントリについてメッセージ情報ページを開くことができ、SMTPセッション写しおよびメッセージのコンテントおよびソースを(利用できる場合)表示します。

隔離
選択されたドメインの隔離[250]ページを閲覧するために、**隔離**をクリックします。ドメインのすべての隔離されたメッセージは、一覧に表示され閲覧することができます。

ホワイトリスト
選択されたドメインのアドレスホワイトリスト[221]を閲覧するために、**ホワイトリスト**ボタンを使用します。

ブラックリスト
選択されたドメインのアドレスブラックリスト 213を閲覧するために、**ブラックリスト** ボタンを使用します。

インポート
ドメインリストにドメインをインポートするために、カンマで区切られたファイル(CSV)を使用することができます。読み込みは、ページ上部のツールバーで**インポート** をクリックします。これは、**インポートドメインダイアログ**を開きます。インポートするドメインが登録されているCSVファイルに探すために、このダイアログで**参照** ボタンを使用し、**ドメインの読み込み**をクリックします。

CSVファイル形式
ドメインリストにドメインを追加するためにCSVファイルを作成する場合、任意のテキストエディタ(例えばノートパッド)を使用することができます。下記の形式に従ってファイルを作成し、filename.csvとして保存します。

カラムのデータの順序を通知するために、CSVファイルの最初の行はマッピング行にする必要があります。マッピング行では2つのフィールドがサポートされます: DomainおよびMaxUsersです。両方のフィールドは引用符が必要で、カンマによって区切る必要があります。Domainフィールドはドメイン名前(例えばexample.com)のためで、MaxUsersフィールドは、ドメインに属する許可をするユーザアカウントの最大数です。すべてのドメイン名前で引用符をもつ必要があり、指定されるMaxUsers値がある場合、カンマによってドメイン名前で区切る必要があります。

CSVファイルの例:

```
"Domain","MaxUsers"
"domain.com", 50
"example.com"
"example.org", 10
```

エクスポート
ドメインリストのツールバーで**エクスポート** をクリックすることによって、ドメインのリストをエクスポートすることができます。これは、前述のインポートオプションで使用する同じ形式のCSVファイルでドメインを一覧にします。ドメインをエクスポートする方法は以下の通りです。

1. ページ上部のツールバーの**エクスポート** ボタンをクリックします。これによりファイルダウンロードのダイアログが現れます。
2. **保存** をクリックします。
3. ファイル名と保存場所を指定します。
4. **保存** をクリックし、**閉じる**をクリックします。

3.1.1.1.1 ドメインプロパティ

プロパティダイアログは、新規のSecurity Gatewayドメインを作成、または既存のドメインを編集するために使用します。ドメインリスト 39で**新規** をクリックするか、またはエントリ選択して編集をクリックすることによって、プロパティダイアログを開くことができます。プロパティには4つのプロパティ、検証、メールサーバ、管理者タブがあります。

ドメイン管理者[49]検証ソースとメールサーバー覧に対する読み取り権限を持っています。

プロパティ

プロパティタブは、ドメイン名、ドメインで許可するユーザアカウントの最大数および認証パスワードを指定するために使用されます。ユーザ制限およびパスワードは任意です。

ドメイン名:
このテキストボックスにドメイン名を登録します。例えば: "example.com", "domain.com"、など。これは、各ユーザのメールアドレスで使用されるドメインです。

ユーザ数の制限
このドメインでユーザ数を制限する場合、このチェックボックスをクリックし必要な数を登録します。このオプションは、デフォルトで使用停止です。

最大ユーザ:
このドメインユーザアカウントの数を制限する場合、制限ユーザ数オプションを有効にし、ここへユーザ数を登録します。

最大メッセージサイズを制限
対象ドメインのメッセージでSMTPで受信できる最大メッセージサイズを制限するには、このボックスを選択し、数値を入力します。デフォルトでこのオプションは無効になっており、全体のメール容量[76]制限が適用されています。

SMTP認証パスワード
SecurityGatewayを経由してメール送信する際、ユーザーまたはドメインメールサーバー[65]で認証を行う場合、ドメイン用のSMTP認証パスワードをこのオプションで指定します。このパスワードで認証を行うには、ドメインをログイン用ユーザー名として認証できるようにしてください。例えば、ドメインが「example.com」の場合で「1234Password」がパスワードである場合、認証は、「example.com」と「1234Password」にて行われます。パスワードオプションを空白にすると、認証にドメイン名のみを使用するため、認証に失敗します。

SMTP認証は管理者がCRAM-MD5認証を使用する場合にも便利です。この種類の認証はSecurityGateway側でパスワードを把握しておく必要が生じます。ユーザー検証ソースは使用できません。

多くの場合、各ユーザは、単に認証証明書として自分自身のアカウントメールアドレスおよびパスワードを使用します、しかし、ドメインのメールサーバが自身の証明書を持つことを必要とする場合がある、あるいは、複数ユーザが1セットの認証証明書を共有することを必要とする特定のメールサーバ構成があります。このオプションは、それらのタイプの要求を提供するために提供されます。

次のIPアドレスにこのドメインを割り当てる
ドメインを特定のIPに割り当てるにはこのボックスを選択し、IPアドレスとホスト名を空白で分けて入力します。対象ドメインからのメールはここで指定したIPアドレスを使って送信されます。HELOストリン

グ、SMTPホスト名で使用するドメイン名もここで指定できます。この値は Fully Qualified Domain Name（FQDN）でドメインのメールを送信する際のSMTP HELO/EHLOで使用されます。受信接続では、この値は複数ドメインが同じIPアドレスを使用している場合のみ使用され、FQDNはアルファベット順に使用されます。

ドメインエイリアス
ドメインのエイリアスを指定するために、このオプションを使用します。ドメインのユーザのすべては、各ドメインのエイリアスとして有効であるとみなされます。このオプションは、ドメインを複数登録している場合に便利です。例: altn.com、altn.us、altn.net

検証

検証タブは、ドメインで使用するユーザ検証ソース[52]を指定するために使用します。メッセージが、このドメインの不明なユーザ宛の場合に、アドレスが正規であるか確認するのにここで指定したソースを使用します。アドレスが見つかると、SecurityGatewayでは宛先ユーザー用のアカウントを生成します。

検証ソースに問い合わせしない、ユーザは手動で管理されます
特定のドメインに対して任意の検証ソースの問い合わせをしない場合、このチェックボックスを選択します。このオプションを選択する場合、そのドメインでは手動で、すべてのユーザを管理する必要があります。

有効なソース:
ここへは事前に作成した有効な検証ソースの一覧が表示されます。対象ドメイン用にソースを割り当てる場合は、一覧から対象のソースを選択し、"--->"の矢印をクリックします。

選択したソース:

ここへはドメインへ割り当てた検証ソースが一覧表示されます。ドメイン用のソースを削除するには、一覧から対象のソースを選択し、"<---"の矢印をクリックします。

プリファレンス: 上へ/下へ
検証ソースへの問合せは、選択したソース一覧の上から順番に実行されます。ソースの優先度を上げたり下げたりするには、対象のソースを選択し、上から下の矢印をクリックして、任意の場所へ移動させます。

肯定または否定の結果が分かり次第、SecurityGatewayではソースに対する問い合わせを停止します。例えば、3つのソースが示され、最初のソースでユーザが存在しないと示す場合、その結果を受け取り、その他2つのソースの問い合わせることなく、メッセージを拒否します。しかし、例えば検証ソースが一時的にダウンしている場合などの、致命的でないエラーが起因している場合、メッセージは後ほど再送するよう促す4xxエラーコードで返されます。

新規
このドメインで使用する新規ユーザ検証ソースを作成する場合、新しいユーザー検証ソース[55]画面を開くために、**新規**をクリックします。現れる新規のソースを作成した後に、利用できるソースリストを示します。 新しいソースを作成すると、有効なソースとして一覧へ表示されます。

メールサーバ

メールサーバタブは、ドメインについて使用されるドメインメールサーバ[65]を指定するために使用します。メッセージが照合されたこのドメインのユーザに届く時に、SecurityGatewayは、一覧に示される順番で、ここに示される選択されたサーバでメッセージを配信することを試みます。

有効なサーバ:
このボックスは、以前に作成したすべての利用できるドメインメールサーバの一覧を示します。このドメインへサーバを指定するために、リストから選択して"--->"をクリックします。

選択したサーバ:
このボックスは、このドメインに指定したすべてのドメインメールサーバー覧を示します。ドメインからサーバを削除するために、リストから選択して、"<---"をクリックします。

プリファレンス: 上へ/下へ

SecurityGatewayでは、上から順番にドメインメールサーバを使用します。サーバの問い合わせ順を変更するには、上へまたは下へボタンをクリックします。サーバは上から順番に問い合わせをします。

指定したドメインのユーザー以外には、そのドメインに対してこのメールサーバは使用できません。
サーバーを選択し、このボックスをクリックすると、サーバーはドメインのメール送信用には使用されず、指定したユーザーのみが使用できるようになります。特定のユーザーのみにこのサーバーを使用させるようにするには、ユーザーの編集 ≫ プロパティ[47]ページのメール配信オプションで、このサーバー用のユーザーを指定します。

新規
このドメインのために使用する新規のドメインメールサーバを作成する場合、新規のメールサーバ[66]画面を開くために**新規**をクリックします。新規サーバを作成すると、有効なサーバとして表示されます。

管理者

管理タブでは、対象ドメインの管理者[49]を指定できます。既に権限を持っているグローバル管理者はここへは表示されません。

有効な管理者:
このボックスは、コントロールを所有しているドメインに関係なく、以前に作成したすべての利用できるドメイン管理者の一覧を示します。このドメインを構成する許可を管理者に与えるために、リストから選択して"--->"をクリックします。

選択した管理者:
このボックスは、このドメインに管理する許可を所有しているすべてのドメイン管理者を示します。このドメインへ管理者レベルのアクセスを削除する場合、リストから選択して"<---"をクリックします。

新規
このドメインのために新規管理者[50]を作成する必要とする場合、新規の管理者画面を開くために**新規**をクリックします。管理者を作成すると、選択した管理者として表示されます。

3.1.1.2 ユーザリスト

ユーザリストは、ドメインのユーザアカウントを管理するために使用されます。リストを開くために、左側のボックスでナビゲーションメニューから**設定 / ユーザ**をクリックし、**ユーザと管理者**セクションでユーザリストを閲覧したいドメインをクリックします。ドメインリスト[39]で各ドメインのエントリからユーザリストを得ることもできます。

ユーザリストは、有効、名前、メールボックスの3つのカラムがあります。有効は、各ユーザエントリのチェックボックスがあり、ユーザのアカウントを有効/無効にすることができます。名前カラムはユーザのリアルネームを示します(例えばFrank Thomas)。メールボックスカラムは、ユーザのメールアドレス(例えば"frank@example.com"の"frank")をメールボックスの一部で示します。ユーザを編集するために、リストでユーザをダブルクリックするか、またはユーザを選択し、ページ上部のツールバーで**編集**をクリックします。これは、ユーザ編集[47]画面を開きます。

ページ上部のツールバーは、ユーザリストに関連した各種のタスクを開始するために使用されます。ほとんどのツールバーのボタンは、必要なボタンをクリックする前に、リストからユーザを選択することが必要です。例外は、前へ、読み込み、書き出しです。これらのボタンは、ユーザを選択することなくクリックすることができます。ツールバーは、次の11オプションがあります。

戻る
ドメインリスト[39]にユーザリストに戻す場合、前のページに戻るために、このボタンを使用することができます。

新規
新規ユーザ[47]ダイアログ(このドメインで新規のユーザアカウントを作成するために使用される)を開くために**新規**をクリックします。ユーザ編集[47]ダイアログのように、新規ユーザは、ユーザのメールボックス名、リアルネーム、パスワードおよび管理者権限を指定するところです。

編集
ユーザリストで現在選択されるユーザに対応するユーザ編集[47]ダイアログを開くために、ツールバーの**編集**ボタンを使用します。あるいは、同様に、エントリをダブルクリックすることによって、ユーザ編集ダイアログを開くことができます。

削除
ユーザを削除するために、ユーザをリストから選択し**削除**をクリックします。ユーザを削除する確認するボックスが開きます。CtrlおよびShiftキーを使用して複数のユーザを選択することができます。

検索条件を表示/隠す
検索条件を表示をクリックし、ユーザー覧の検索オプションを表示します。ユーザ名のボックスへテキストを入力し、**検索**をクリックすると、ユーザー覧がフィルタされ、入力したテキストが含まれるユーザのみが表示されます。**X検索を中止**をクリックすると、検索を中止し、通常のユーザー覧画面へ戻ります。

設定
このボタンは選択されたユーザの設定[27]ページを開き、ユーザのパスワードを変更、アカウントの隔離設定を設定するために使用することができます。ユーザで自動ホワイトリストをオンにし、SecurityGatewayにユーザがログインする時、ページに表示するアイテム数を指定します。

メッセージ
このボタンは、選択されたユーザに対してメッセージログを開くために使用します。メッセージログ[249]は、そのユーザ宛あるいは送信元のメッセージごとにエントリを持ちます。メッセージログからエントリにつきメッセージ情報ページを開くことができ、SMTPセッション写しおよびメッセージの内容およびソース(利用できる場合)を表示します。

隔離
選択されたユーザに対して隔離[250]ページを閲覧するために、隔離をクリックします。そのユーザのためのすべての隔離されたメッセージは、一覧を示されページから調査することができます。

ホワイトリスト
選択されたユーザのアドレスホワイトリスト[221]を閲覧するために、**ホワイトリスト**ボタンを使用します。これは、ユーザの個人的なホワイトリストで、アカウントのみに適用されます。

ブラックリスト
選択されたユーザのアドレスブラックリスト[213]を閲覧するために、**ブラックリスト**ボタンを使用します。これはユーザの個人的なブラックリストで、アカウントのみに適用されます。

インポート
ユーザリストにユーザの一覧を読み込むために、カンマで区切られた(CSV)ファイルを使用することができます。ページ上部でツールバーの**インポート**をクリックし、ユーザインポートダイアログを開きます。対象ユーザを含んでいるCSVファイルを**参照**ボタンから選択し、**ユーザのインポート**をクリックします。

ユーザインポートダイアログの一番下には、**自動的に存在しないドメインを作成する**オプションがあります。そのオプションを可能にする場合、インポートされているユーザの一覧で存在しないドメインについてメールアドレスを含む時に、新規のドメインが自動的に作成されます。そのオプションが無効にされる場合、SecurityGateway中で存在しないドメインのアドレスは無視されます; それらのエントリは、読み込まれません。

CSVファイル形式
ユーザリストにユーザを追加するためにCSVファイルを作成するために、テキスト・エディタ(例えばノートパッド)を使用することができます。下記の形式に従ってファイルを作成して、filename.csv.として保存します

カラムのデータの順序を通知するために、CSVファイルの最初の行はマッピング行にする必要があります。マッピングカラムにおける次のフィールドがサポートされます:

- **Email** - ユーザのメールアドレス(例えば"frank@example.com")。
- **MailBox** - メールアドレス("frank" of "frank@example.com")のメールボックス部分。
- **Domain** - アドレスのドメイン部分("example.com")。
- **FullName** - ユーザ("Frank Thomas"のような)のリアルネーム。
- **Password** - ユーザのパスワード(アカウントをまたはSecurityGatewayを通してのメールを送信する時ログイン認証で使用される)。
- **Enabled** - アカウントを使用可能または無効にするか指定します。使用可能なアカウントでは、このフィールドで1", "yes"または"true"を使用することができ、無効にする場合は、"0", "no"または"false"を使用することができます。

メール、メールボックスおよびドメインフィールドは、適切に処理されます、従って、それらのフィールドのいずれかの値がその前のフィールドと矛盾する場合、後の値が使用されます。例えば、Email

フィールドで"frank@ example.com"を使用し、Domainフィールドで"domain.com"を使用する場合、その場合、"frank@ domain.com"が使用されるアドレスです。

すべての行の全フィールドは引用句で持ち、カンマによって区切られていなければなりません。

CSVファイルの例:

```
"Email", "MailBox", "Domain", "FullName", "Password", "Enabled"
"frank@example.com", "frank", "example.com", "Frank Thomas",
"1234Password", "1"
"rip@example.com", "rip", "example.com", "Rip Collector",
"FoundAPenny", "yes"
"big@domain.com", "big", "domain.com", "Mister Big", "NumeroUno",
"1"
```

エクスポート
ツールバーで**エクスポート**をクリックすることによって、ドメインのユーザリストを書き出しすることができます。これは、前述のインポートオプションで使用する同形式のCSVファイルで、ドメインを一覧にします。ユーザリストをエクスポートする方法は次の通りです。

1. ページ上部のツールバーの**エクスポート**ボタンをクリックします。これによりファイルダウンロードのダイアログが現れます。
2. **保存**をクリックします。
3.
4. ファイル名と保存場所を指定します。
5. **保存**をクリックし、**閉じる**をクリックします。

3.1.1.2.1 ユーザの編集

ユーザ編集画面は、SecurityGatewayドメインの新規のユーザアカウント作成または既存ユーザを編集するために使用されます。ユーザリスト 45 で新規クリックするか、エントリを選択し**編集**をクリックすることで編集画面を表示できます。ユーザ編集に関してメールボックス名前、ユーザの名前、パスワード、さらにユーザを管理者 49 に指定できます。ユーザと関連する任意のエイリアスもここで指定することができます。

プロパティ

このアカウントを利用禁止にする
このアカウントを使用停止にする場合、このチェックボックスをクリックします。アカウントが使用停止にされる場合、SecurityGatewayでは、そのユーザでメッセージの送受信はできません。

メールボックス名:
このオプションは、ユーザのメールボックス名およびドメインを指定します(例:frank@ example.com)。SecurityGatewayアカウントにログインする時、ユーザのメールアドレスが使用されます。SMTP認証の使用で構成する場合、ユーザのメールクライアントのユーザ名またはログインパラメータとして使用されます。

リアルネーム:
このオプションはユーザの名前(例:"Frank Thomas")を指定します。

パスワード:
パスワードは、ユーザのアカウントおよびSMTP認証のためにサインインで使用します。

パスワード(確認):
新規のパスワードが登録される場合は、このスペースはパスワードが正しく入力されたことを確認するために使用されます。

強固なパスワード要件から除外する
強固なパスワード[62]要件からユーザーを除外する場合はこのチェックボックスを使用します。

管理者設定

アカウントを管理者にする

ユーザアカウントを作成または編集する時に、このチェックボックスをクリックし、下記でユーザに管理者[49]オプションを指定する場合、グローバルまたはドメイン管理者の1つを選びます。

グローバルな管理者
グローバル管理者[49]は、他の管理者アカウントおよび設定について、SecurityGatewayすべての設定およびオプションの管理を持ちます。そのために、アカウントをグローバル管理者として指定する前に、注意をしてください。

ドメイン管理者
ドメイン管理者は、権限を与えられたドメインに関連するすべての設定およびオプションにアクセスすることができます。グローバル設定を編集すること、または他のドメインに特定の設定にアクセスすることができません。ドメイン管理者を指定する場合、ユーザが管理する少なくとも一つの利用できるドメインを選択する必要があります。

有効なドメイン:
このボックスは、SecurityGatewayユーザがドメイン管理者アクセスを与えられたドメインの一覧を示します。ユーザに、これらのドメインの一つ以上を通じてコントロールを与えるために、リストからドメインを選択して、"--->"をクリックします。

選択したドメイン:
このボックスは、SecurityGatewayユーザがドメイン管理者アクセスを与えられたドメインの一覧を示します。このリストからドメインを削除するには、ドメインを選択して"<---"をクリックします。

作成できるドメイン
ドメイン管理者へ、ドメイン管理者して新しいドメインを作成できるようにするにはこのオプションを有効にします。

ドメイン作成数の上限:[xx]ドメイン
ドメイン管理者へドメイン作成を許可する場合、対象ユーザーが作成できるドメイン数の上限をここで指定できます。

メール配信

ドメインメールサーバを使用する
デフォルトで、ユーザーのメールは ユーザーのドメイン 41 として指定されたドメインメールサーバーを使って処理されます。ドメイン用に指定されたサーバーではなく、特定のサーバーを使ってこのユーザーのメールを処理する場合は下のオプションを選択してください。

選択したメールサーバーを使ってメールを配信する
このオプションを選択すると、対象ユーザーのメールは、ユーザーのドメイン用に指定されたドメインメールサーバーではなく指定したメールサーバーを使って配信されます。

有効な/選択したサーバー
ユーザーのメールを処理するサーバーを、有効なサーバーから選択し、矢印を使って選択したサーバーへ移動します。

エイリアス

ユーザと関連させる任意のエイリアスを指定するために、エイリアスタブを選択します。さらに、別々のユーザでなくエイリアスに変換する既存のSecurity Gatewayユーザをマージすることができます。

エイリアス:
エイリアスをユーザに割り当てるために、テキスト入力フィールドへ電子メールアドレスを入力し[**追加**]をクリックします。一覧からエイリアスを削除するには、必要なエントリを選択し、続いて[**削除**]をクリックします。

マージするユーザ:
別のユーザを指定したユーザと関連するエイリアスに変換する場合、マージユーザオプションを使用します。既に存在しているユーザのエイリアスが実際にある場合、ユーザ検証ソースが誤って、作成される別々のSecurity Gatewayユーザのもととなるインスタンスで必要です。

マージするユーザのテキストボックスへメールアドレスを入力することで、マージするアドレスを指定することができます。入力するとき、入力しているものにマッチするアドレスだけを一覧に表示します。

"ユーザをマージ" リンク
マージするユーザー覧において、エイリアスに変換するアドレスと関連するユーザを選択し、**ユーザをマージ**リンクをクリックします。関連したアドレスは、エイリアス一覧へ移動されます。

3.1.2 管理者

管理者リストでは、Security Gatewayで指定されたグローバル管理者とドメイン管理者全てが一覧表示されています。

グローバル管理者は、他の管理者アカウントやSecurity Gatewayすべての設定に対する権限を持ちます。そのため、アカウントをグローバル管理者として指定する場合は最新の注意を払って下さい。

ドメイン管理者は、権限を与えられたドメインに関連する設定およびオプションすべてにアクセスすることができます。グローバル設定を編集すること、または他のドメインに特定の設定にアクセスすることができ

ません。ドメイン管理者を指定する場合、ユーザが管理する少なくとも一つの利用できるドメインを選択する必要があります。

管理者リストは、有効、Emailおよびリアルネームの3つのカラムを持ちます。有効は各エントリのためのチェックボックスがあり、管理者アカウントを有効/無効にするために使用します。Emailカラムは管理者のメールアドレスを示しSecurityGatewayにロギングのためで使用されます。管理者アカウントは、SecurityGatewayドメインの1つに属しているローカルアカウントである必要はありません。

リアルネームカラムは、ユーザのリアルネーム(例えばFrank Thomas)を示します。

管理者を編集するには、リストでエントリをダブルクリックするか、エントリを選択してページ上部のツールバーで**編集**をクリックし、管理者を編集 50画面を開きます。

ページ上部のツールバーには、4つのオプションがあります。

新規
新規管理者アカウントを作成するために、新規管理者画面を開くには、**新規**をクリックします。この画面は、管理者を編集 50画面と一致します。

編集
リストで現在選択されるエントリに対応する管理者を編集 50画面を開くために、ツールバーの**編集**ボタンを使用します。あるいは、エントリをダブルクリックすることによって、画面を開くこともできます。

削除
管理者を削除するには、リストからエントリを選択して、**削除**をクリックします。削除を確認するボックスが現れます。Ctrlおよびシフトキーを用いて複数のエントリを選択することができます。

ドメイン:
リストで表示する管理者を選択のために、**ドメイン**ドロップダウンリストボックスを使用します。デフォルトでは、すべての管理者が表示されますが、グローバル管理者だけを表示するために"-- グローバル --"を選択、またはドメイン単位の管理者だけを表示するために、リストからドメインを選択するもことができます。

3.1.2.1 管理者を編集

管理者を編集画面は、既存のグローバルまたはドメイン管理者を編集または新規の管理者を作成するために使用されます。管理者 49ページで**新規**をクリック、またはリストでエントリを選択し**編集**をクリックすることで、この画面を表示できます。管理者を編集で、管理者をローカルアカウントまたは外部ユーザに指定し、管理のローカルメールボックスまたは外部のメールアドレス(パスワードおよびフルネーム)を指定します。ユーザをグローバルまたはドメイン管理に指定します。

プロパティ

ローカルユーザ -ローカルドメインのメンバー
管理者アカウントがSecurityGatewayドメインのうちの1つに属しているローカルアカウントに対応する場合、このオプションを選びます。

外部 -ローカルドメインのユーザでない
管理者が、ローカルユーザアカウントに対応する必要はありません。外部のメールアドレスをもつ外部ユーザにすることができます。この管理者を外部ユーザに指定する場合、このオプションを選びます。

メールボックスまたはメールアドレス
ローカルユーザオプションを上記で選択する場合、管理者のメールボックスを登録し、ローカルドメインをドロップダウンリストボックスから選びます。外部を選択する場合、管理者の外部のメールアドレスを登録します。いずれの場合においても、管理者のメールアドレスは、SecurityGatewayにログインに使用されます。

フルネーム:
管理者名(例えばFrank Thomas)を登録するために、この入力ボックスを使用します。

パスワード:
これは、管理者のパスワードで、SecurityGatewayにログインに使用します。

パスワード(確認):
新規のパスワードが登録される時、正しく入力されたことを確認するために、このボックスに再入力する必要があります。

このアカウントを利用禁止にする
管理者のアカウントを使用停止にする場合、このチェックボックスをクリックします。

タイプ

管理者タイプであるグローバルまたはドメインを指定するために、このオプションを使用します。

グローバル管理者
グローバル管理者は、他の管理者アカウントおよび設定にわたる、SecurityGatewayすべての設定およびオプションのコントロールを持ちます。この理由のために、アカウントをグローバル管理者として指定する場合には注意してください。

ドメイン管理者
ドメイン管理者は、権限を与えられたドメインに関連するすべての設定およびオプションにアクセスすることができます。グローバル設定を編集すること、または他のドメインに特定の設定にアクセスすることができません。ドメイン管理者を指定する場合、ユーザが管理する少なくとも一つの利用できるドメインを選択する必要があります。

有効なドメイン:
このボックスは、SecurityGatewayユーザがドメイン管理者アクセスを与えられることができるドメインのすべての一覧を示します。ユーザにこれらのドメインの一つ以上を通じてコントロールを与えるために、リストからドメインを選択して、"--->"をクリックします。

選択したドメイン:
このボックスは、SecurityGatewayユーザがドメイン管理者アクセスを与えられたドメインのすべての一覧を示します。このリストからドメインを削除するには、ドメインを選択して"<---"をクリックします。

作成できるドメイン
ドメイン管理者が新しくドメインを作成できるようにするにはこのオプションを有効にします。管理者は作成したドメインのドメイン管理者として自動登録されます。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。

ドメイン作成数の上限：[xx]ドメイン
ドメイン管理者によるドメイン作成を許可した場合、デフォルトでは5ドメインまでの作成が許可されます。この上限数を変更したい場合はここで数字を変更するか、無制限にする場合はこのオプションを無効化します。

3.1.3 ユーザ検証ソース

このページでは、不明なローカルアドレスを検査するための、ユーザー検証ソースを管理する事ができます。このページへは、左側のナビゲーションメニューから設定/ユーザーをクリックし、アカウントセクション内のユーザー検証ソースをクリックし、アクセスする事ができます。

受信メッセージが不明なローカルユーザに送られると、SecurityGatewayは、ドメイン用ユーザ検証ソースを使ってメールアドレスが正しいかどうかの検証を行います。アドレスが有効だった場合、SecurityGatewayは対象メールアドレス用のアカウントを作成し、ドメインメールサーバ[65]にメール配信を行います。アドレスが無効である場合、メッセージは拒否されます。新規アカウントが、このように作成されるたびに、SecurityGatewayへログインリンクを含んでいるようこそ[60]メッセージが、そのユーザにメールで送られます。

不明なローカルユーザからの送信メッセージについて、実際に受信メッセージで扱うように、SecurityGatewayではドメインのユーザ検証ソースを問い合わせます。さらに、ユーザがそのメールアドレスおよびパスワードを使用して接続を認証することを試みる時に、SecurityGatewayではユーザ検証ソースにそれらの認証証明書を渡します。ユーザが認証に失敗する場合、メッセージは拒否されます。認証が成功している場合、メッセージは配信のために受け取られ、SecurityGatewayアカウントはそのユーザのために作成されます。すでに存在するアカウントについて、SecurityGatewayではローカルユーザデータベースにユーザのログイン証明書を最初にチェックします。全く適合するものがない場合、検証ソースを確認します。

ユーザ検証ソースは、ドメインのプロパティ[41]画面の検証タブの一覧の順に使用されます。肯定、否定の結果が返されると、SecurityGatewayでは結果を受け取り、以降の問い合わせることを停止します。例えば、3つのソースあった場合、1つ目でユーザが存在しないと提示があった場合、その結果を受け取り、その他2つのソースを問い合わせることなく、メッセージを拒否します。しかしながら、検証ソースが一時的にダウンしているといった、致命的でないエラーが発生している場合は、メッセージは4xxエラーコードで返され、再配信されます。

検証ソースが正当なユーザだけを正しく検証できるよう構成されている事が重要です。検証ソースがオープンリレーまたはSecurityGatewayドメインのうちの1つに対して「汎用の」エイリアスを持つ場合、不明なユーザに対しあらゆる受信メールは、そのソースによって確認されます。これは、多くの誤ったユーザを作成するという結果になります。大部分の受信スパムが不正なユーザにアドレス指定を行われるという理由から、ソースによって誤って確認されます。これによって、急激に登録キーのユーザ制限に到達する可能性があります。

ユーザ検証ソースページは、1行毎に、説明、サーバ、ポート、タイプの4つ列で構成されています。説明は、検証ソースの説明用（例えば"Server X at example.com"）です。サーバカラムは検証ソースのホ

スト名またはIPアドレスを示します、ポートは各ソースが使用するポート、タイプは検証ソースのタイプで、SMTP認証(転送)、Active Directory/Exchange、MDaemon (Minger)またはLDAP、Office 365です。検証ソースを編集するには、エントリをダブルクリックするか、エントリを選択しページ上部のツールバーで編集をクリックします。これは、ユーザー検証ソースの編集画面が起動します。

LDAP以外のすべての検証タイプは、ダイナミック認証に対応しています。ユーザが認証されたりSecurity Gatewayにログインする際、ローカルのSecurity Gatewayへ認証情報が渡されますが、存在しない場合は検証ソースへ渡され認証されます。これでSecurity Gatewayで認証情報を別管理する事なくユーザーがSecurity Gatewayで認証したりログインできるようになります。

ログイン証明書は最初にチェックされますが、存在しない場合、証明書は認証のために検証ソースに渡されます。これは、特にSecurity Gateway用の証明書で個別のセットを記憶する必要なくSecurity Gatewayアカウントに認証するユーザまたはログインを可能にします。

認証でCRAM-MD5が使われていると、AUTHパスワードは、ダイナミック認証を行えません。

ページ上部ツールバーには、次の5つのオプションがあります。

新規
新しくユーザー検証ソースを作成するには新規をクリックします。ユーザ検証ソースを編集画面が起動します。

編集
リストで現在選択されるエントリに対応するユーザ検証ソースを編集画面を開くために、ツールバーの編集ボタンを使用します。あるいは、エントリをダブルクリックして画面を開くこともできます。

削除
検証ソースを削除するには、リストからエントリを選択し削除をクリックします。削除の確認するボックスが現れます。Ctrlおよびシフトキーを用いて複数のエントリを選択することができます。

ユーザを検証
"-- すべて --"をドメイン:ドロップダウンリストボックスで選択し、このボタンをクリックすると、過去に確認されたユーザでも、全ユーザーの検証をSecurity Gatewayで実行します。手動で追加されたユーザであっても、ユーザ検証ソースで確認できないユーザは削除されます。特定のドメインがドメイン:ボックスで選択されている場合、Security Gatewayでは、そのドメインのユーザだけを検証します。

オプション
ユーザー検証ソースオプションページでは応答のキャッシュを有効化したりユーザーの再検証までの時間を指定する事ができます。

この時間後にユーザーの再検証を行う[xx]時間
このオプションは、ユーザーが存在している場合に、定期的にユーザー情報をメンテナンスするのに役立ちます。指定した時間毎に検証済ユーザーは次の再検証時間を指定され、メールの

送受信のタイミングで再検証が求められます。無効化されたユーザーは削除されません。

この時間、検出失敗をキャッシュする [xx] 分
検証ソースでアカウントが存在しないと判断した際、このオプションは指定した時間の間その結果をキャッシュとして保持します。これにより検証ソースによる検証回数を抑える事ができます。

外部エイリアス用に常にデフォルトユーザー検証ソースを使用する
このオプションを有効にすると、不明なアドレスは全てデフォルトユーザー検証ソースで検証が行われます。ユーザー検証ソースが、アドレスを、ローカルドメインのユーザーの外部エイリアスであると判断すると、ローカルユーザーが必要に応じて生成され、エイリアスとユーザーが紐づけされます。この機能を利用するには、予めユーザー検証ソースを定義しておく必要があります。


全ての不明なアドレスが検証されるため、膨大な数の検証が行われます。

ドメイン:
リストでどのユーザ検証ソースを表示するか選択するには、**ドメイン:**ドロップダウンリストボックスを使用します。デフォルトでは、すべてのソースが表示されますが、デフォルトソース(ユーザ検証ソースを編集 55ダイアログ)に指定したソースだけを表示またはドメイン単位で検証ソースを表示するドメインをリストから選択できます。

3.1.3.1 ユーザー検証ソースオプション

この時間後にユーザーの再検証を行う [xx] 時間
このオプションは、ユーザーが存在している場合に、定期的にユーザー情報をメンテナンスするのに役立ちます。指定した時間毎に検証済ユーザーは次の再検証時間を指定され、メールの送受信のタイミングで再検証が求められます。無効化されたユーザーは削除されません。

この時間、検出失敗をキャッシュする [xx] 分
検証ソースでアカウントが存在しないと判断した際、このオプションは指定した時間の間その結果をキャッシュとして保持します。これにより検証ソースによる検証回数を抑える事ができます。

外部エイリアス用に常にデフォルトユーザー検証ソースを使用する
このオプションを有効にすると、不明なアドレスは全てデフォルトユーザー検証ソースで検証が行われます。ユーザー検証ソースが、アドレスを、ローカルドメインのユーザーの外部エイリアスであると判断すると、ローカルユーザーが必要に応じて生成され、エイリアスとユーザーが紐づけされます。この機能を利用するには、予めユーザー検証ソースを定義しておく必要があります。


全ての不明なアドレスが検証されるため、膨大な数の検証が行われます。

参照:

ユーザー検証ソース[52]

3.1.3.2 検証ソースを編集

ユーザ検証ソース[52]編集画面は、既存のユーザ検証ソースを編集または新規のソースを作成するために使用します。ユーザ検証ソースページで**新規**をクリック、またはリストでエントリをクリックし編集を選択することで、この画面に表示することができます。この画面でソース、ロケーション、接続するポート、任意の必要な認証証明書およびユーザを確認のためのソースを使用するSecurityGatewayドメインのタイプを指定します。

プロパティ

タイプ:
SMTP Verification（転送）[56], Active Directory/Exchange[56], MDaemon (Minger)、[56] LDAP、[57]Office 365[57]の中から、ユーザ検証ソースを選択します。後述の、説明、ホストまたはIP、ポートオプションは、検証ソースの4つのタイプすべてに適用されます。残りのオプションは、選択した検証ソースにより異なります。すべての検証タイプについて、不明なローカルユーザが確認される場合、SecurityGatewayアカウントが、そのユーザのために作成され、SecurityGatewayのログインリンクを含んでいるようこそ[60]メッセージを新規アカウントにメールで送ります。ユーザのメールアドレスおよびパスワードは、メッセージログ、メッセージ隔離などを閲覧するために、SecurityGatewayアカウントにログインに使用することができます。LDAPがダイナミック認証をサポートしないので、その検証タイプが選択される場合、SecurityGatewayにログインを可能にする前に、SecurityGatewayパスワードをユーザに提供する必要があります。

LDAP以外のすべての検証タイプは、ダイナミック認証をサポートします。ユーザが認証またはSecurityGatewayにログインを試みる時に、ローカルSecurityGatewayログイン証明書は最初にチェックされますが、存在しない場合、証明書は認証のために検証ソースに渡されます。これは、特にSecurityGateway用の証明書で個別のセットを記憶する必要なくSecurityGatewayアカウントに認証するユーザまたはログインを可能にします。

認証のCRAM-MD5[76]手順が使用される場合、AUTHパスワードは、動的に確認することができません。

説明:
検証ソースの説明（例えば、"example.comのサーバX"）のために、このテキストボックスを使用します。ユーザ検証ソース[52]ページで説明カラムに対応します。

ホストまたはIP:
これは、検証ソースのホスト名またはIPアドレス用です。このソースを問い合わせると、SecurityGatewayは、このロケーションに接続します。このオプションは、ユーザ検証ソースページでホストカラムに対応します。

ポート:
これは検証ソースに接続する場合、SecurityGatewayが使用するポートで、ユーザ検証ソースページでポートカラムに対応します。

SMTP検証(転送)

受信メッセージの不明なローカル受信者および送信メッセージの不明なローカル差出人を確認するためにSMTPを使用する場合、このタイプを選択します。コールバック検証[177]と同様で、SecurityGatewayはSMTPプロトコルを通してユーザを確認することを試みます。認証を試みる不明なローカル差出人について、SecurityGatewayでは認証のためにSMTP検証ソースにユーザの証明書を渡します。認証が成功する場合、メッセージはSecurityGatewayによって配信のために受け取られ、ユーザのためのアカウントが作成されます。すでに存在するアカウントについては、SecurityGatewayではローカルユーザデータベースに対してユーザのログイン証明書を最初にチェックします。一致がない場合、SMTP検証ソースをチェックします。

認証が必要
SMTP検証ソースが認証を必要とする場合、このチェックボックスをクリックします。下記のユーザ名およびパスワードを指定します。

ユーザ名:
SMTP検証ソースが認証を必要とする場合、ユーザ名をここに指定します。

パスワード:
SMTP検証ソースパスワードを、ここに入力します。

Active Directory/Exchange

不明なローカルユーザを確認するためにActive DirectoryまたはExchangeサーバを使用する場合、このタイプを選択します。前述であるSMTP検証と同様に、この検証タイプは、ダイナミック認証をサポートします。認証することを試みる不明なローカル差出人のために、SecurityGatewayは認証についてActive Directory/Exchangeサーバにユーザの証明書を渡します。認証が成功している場合、メッセージはSecurityGatewayによって配信のために受け取られ、ユーザのアカウントが作成されます。すでに存在するアカウントについては、SecurityGatewayはローカルユーザデータベースに対してユーザのログイン証明書を最初にチェックします。一致がない場合、SMTP検証ソースがチェックされます。

ユーザ名:
このテキスト入力ボックスは、検証ソースにログインに必要なActive Directory/Exchange/Windowsユーザ名です。

パスワード:
上記で指定されるActive Directory/Exchangeユーザ名に対応するパスワードを入力するために、このテキスト入力ボックスを使用します。

検索フィルタ:
これは、ユーザについてActive Directory/Exchangeサーバを問い合わせる時に使用する検索フィルタです。ほとんどの場合デフォルト検索フィルタで十分です。

MDaemon (Minger)

ユーザ検証ソースとしてMingerを使用しているMDaemonサーバを使用する場合、この検証タイプを選択します。これは、Mingerプロトコルの拡張したバージョンで、MDaemonサーバ専用です。従って、このオプションは、他のタイプのサーバで使用することができません。この検証タイプは、2つ前の検証タイプのようにダイナミック認証をサポートします。これは、ユーザがメールサーバログイン証明書を使用してSecurityGatewayアカウントを認証またはログインすることができることを意味します。

認証が必要
MDaemonサーバがMingerを使用する認証を必要とする場合、このチェックボックスをクリックします。

パスワード:
MDaemonサーバのMingerパスワードを、ここに入力します。

LDAP

ユーザを確認するためにLDAPサーバを使用する場合、この検証タイプを選択します。しかしながら、その他検証タイプとは異なり、ユーザのログイン証明書を認証するために、LDAPを使用することができません。結果的に、ダイナミック認証(または「オンザフライ」で認証すること)をサポートしません。そのために、認証するユーザを必要とする場合、LDAP検証ソースこと確認されるユーザは、ログインまたは、SecurityGatewayアカウントのパスワードを使用せずにSecurityGatewayを通してのメッセージを送信することができません。

Bind DN:
SecurityGatewayがユーザ名について問い合わせることができるように、LDAPサーバにアクセスを持つ識別名(DN)を入力します。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:
このパスワードは、認証のためにバインドDN値とともにLDAPサーバに渡されます。

ベースエントリDN:
これは、SecurityGatewayがユーザのためのActive Directoryを検索するディレクトリ情報ツリー(DIT)のルートDNまたはスタートポイントです。

検索フィルタ:
これは、ユーザについてLDAPサーバを問い合わせる時に、使用されるLDAP検索フィルタです。ほとんどの場合、デフォルト検索フィルタで充分です。

検索範囲:
これはLDAP検索の対象と範囲です。

ベースDNのみ
検索を上記で提供されるベースエントリDNだけに制限したい場合、このオプションを選択します。検索は、ツリー(DIT)でそのポイントの下へ進みません。

ベースDNの1レベル下
DITでベースエントリDNの1レベル下を検索する場合、このオプションを使用します。

ベースDNと全チャイルド
このオプションは、ベースDNからDITで最下位のチャイルドエントリまでチルドレン全部を検索範囲にします。これは、デフォルトオプションです。

Office 365

Office 365をユーザー検証ソースとして使用するにはこのオプションを選択し、下記の手順に沿って設定してください。

SecurityGatewayがOffice 365テナントへアクセスするため、Office 365のサービスはExchange Onlineである必要があります。お使いのOffice 365サービスにこの機能が含まれているかどうかを確認してください。

Office 365をユーザー検証ソースとして使用する場合は、SecurityGatewayはOffice 365のテナントへのアクセス権を持つサービスプリンシパルである必要があります。また、Office 365はAzure Active Directoryをディレクトリサービスとして指定している必要があります。以下の手順で、Office365をSecurityGatewayのユーザー検証ソースとして設定できます。

Azure Active Directoryにて:

1. Azure ADのアプリの登録画面へアクセスします。
2. 新規登録を選択します。
3. 名前のフィールドへアプリケーション名を入力します。
4. 登録を選択します。
5. アプリケーションIDを確認します。
6. APIアクセス権を選択します。
7. + を選択し、アクセス権を追加します。
8. Microsoftグラフを選択します。
9. アプリケーションのアクセス権を選択します。
10. Group.Read.AllとUser.Read.Allを選択します。
11. アクセス権の追加を選択します。
12. Grant admin consent for... ボタンを選択します。
13. はい、をクリックします。
14. 証明書と秘密鍵を選択します。
15. +をクリックして新しいクライアント署名を作成します。
16. 説明欄に説明を記入します。
17. 選択ボタンでパスワードの有効期間を選択します。
18. 生成されたパスワードを確認します。

SecurityGatewayにて:

1. SecurityGatewayへグローバル管理者でログインします。
2. **設定 / ユーザー**を選択します。
3. **アカウント**を選択します。
4. **ユーザー検証ソース**を選択します。
5. **新規**をクリックします。
6. **Office 365**を選択します。

7. 説明を記入します。
8. **ドメイン名** へ Office 365 のドメイン名を入力します。
9. 種類を選択します。

   ほとんどの場合、オプションは「全体」になります。
10. **サービスプリンシパル** へAzure ADのアプリケーションIDを入力します。

    Azure ADのアプリケーション登録の概要ページでアプリケーションIDが確認できます。
11. Azure ADで生成されたパスワードを入力します。

タイプ

このサーバをデフォルトのユーザ検証ソースにする
デフォルトユーザ検証ソースは、特に指定されるソースがなかったすべてのSecurity Gatewayドメインのために使用されます。自動ドメイン生成 59 機能により使用されます。

ユーザ検証ソースで使用するドメインを次から選択...
Security Gatewayドメインの1つ以上の検証ソースを指定するために、下記のオプションを使用します。複数の検証ソースがドメインに指定される場合、ドメインのプロパティ画面の検証 41 タブで問い合わせる順位を指定することができます。

有効なドメイン:
このボックスは、すべての利用可能なSecurity Gatewayドメインを示します。この検証ソースを利用するドメインを指定するために、リストから選択して"--->"をクリックします。

選択したドメイン:
このボックスは、ユーザを確認するために、このソースを利用する構成をしたすべてのSecurity Gatewayドメインを示します。このリストからドメインを削除するには、ドメインを選択して"<---"をクリックします。

3.1.4 自動ドメイン生成

デフォルトユーザ検証ソース 52 で不明なドメインのユーザーかどうかをSecurity Gateway側で自動検証する場合は、新しくSecurity Gatewayドメインを自動生成するかどうか、ここで指定してください。このページは、でよって確認ができる場合に、自動的に新規のSecurity Gatewayドメインを作成するかどうか指定するために、このページを使用しま不明なドメインの不明なユーザに関する受信メッセージがす。このページは、左側のナビゲーションメニューから**設定/ユーザ**をクリックし、アカウントセクションの**自動ドメイン生成**をクリックし、開く事ができます。

設定

自動ドメイン生成を有効にする
このオプションを有効にしていると、受信メッセージが不明なドメインで不明なアドレスの時は、SecurityGatewayではデフォルトユーザ検証ソース55へ問い合わせを行います。アドレスが有効である場合、SecurityGatewayがドメインとユーザーを自動生成します。自動ドメイン生成は少なくとも一つのデフォルトユーザ検証ソースが定義される必要があります。すべての不明なアドレスのためにクエリが作成され、多数のクエリが作成される可能性があります。この機能はデフォルトで無効となっています。

> この機能を使用する場合、検証ソースが正当なユーザだけを確認できるよう適切に構成されていることが重要です。例えば、検証ソースがオープンリレーである場合、不明なユーザやドメインに対する受信メールは、全てそのソースによって確認される事になります。これにより、無効なアドレス宛ての受信スパムによって、大量の無効なドメインやユーザーが自動生成されてしまいます。

3.1.5 ユーザオプション

このページではSecurityGatewayユーザーがログインした際にアクセスできるオプションを設定する事ができます。ユーザーオプションは全体またはドメイン毎に設定できます。

アクセスコントロール

パスワードの変更を許可する
ユーザーがSecurityGatewayアカウントのパスワードを設定27ページから変更できるようにするにはこのオプションを使用します。

ログイン画面に「パスワード紛失」リンクを表示する
デフォルトで、"パスワード紛失"リンクはログインページに現れ、これを使ってパスワード変更できます。SecurityGatewayアカウントと関連するアドレスにメールでリンクが送信されます。パスワード紛失リンクを表示しない場合は、このチェックボックスを解除します。

パスワード欄に"パスワードを表示"アイコンを表示する
それぞれのパスワード欄には目のアイコンが表示されており、これをクリックすると、入力したパスワードが表示されるようになります。ユーザーにパスワードを表示させ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。

ユーザへ隔離フォルダの表示と管理を許可する
このオプションを有効にすると、ユーザーは受信したメールで隔離されたものを確認・管理できるようになります。ユーザーは隔離内容を表示34ページからメールの解放や削除などの操作が行えます。

ユーザへ隔離設定の変更を許可する
設定 27 ページにある隔離設定の編集を各ユーザに許可する場合には、このオプションをクリックします。

ユーザへ自身宛てのメールもしくは送信したメールに対するログの表示を許可する
SecurityGatewayで各ユーザがメッセージログを表示 35 から自分のメッセージログを閲覧できるようにします。ユーザのメールアドレスの送受信メッセージすべてはログに表示されます。

これらのアカウント宛て、もしくは送信したメッセージアーカイブの参照や検索を許可する
デフォルトで、アカウント宛やアカウントから送信されたアーカイブメールは、各ユーザーが検索・閲覧できます。これを許可したくない場合は、このオプションを無効化してください。

これらのアカウントへ、もしくはアカウントからのアーカイブされたメッセージの削除をユーザーに許可する
ユーザーがアカウント宛のメールやアカウントから送信されたアーカイブメールの削除を行えるようにするには、このボックスをチェックしてください。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。

ユーザへ自身のメールアドレスに対するアンチスパムチェックを無効化する設定を許可する
ユーザーが自分あてのメールに対してスパムチェックを行わないように設定変更できるようにするにはこのオプションを使用します。ユーザーが設定 27 ページから自分あてのスパムチェックを無効化すると、DNSBL 138, URIBL 141, ヒューリスティックとベイジアン 132, Outbreak Protection 128 が実行されなくなります。

ユーザへ自身の"アカウントのハイジャック検出"機能を無効化する設定を許可する
デフォルトで、ユーザーは自分のアカウントをアカウントハイジャック検出 190 の対象外とする事はできません。このオプションを有効化する事で、ユーザーがハイジャック検出を無効化できるようになります。

ユーザに2段階認証の使用を許可する
ユーザーがSecurityGatewayアカウントへサインインする際2段階認証を必要とするにはこのオプションを有効化します。有効にすると、ユーザーがHTTPS接続で接続した際、2段階認証 27 ページがアカウントオプションの下に表示されます。2段階認証はエクストラのセキュリティレイヤーで、パスワードに加え、携帯用アプリで生成された特殊なセキュリティコードを使ってサインインを行うものです。

ユーザに2段階認証の使用を必須とする
全てのユーザーにサインインの2段階認証を必須と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、最初にユーザーがサインインした際、2段階認証の設定ページが表示されます。

ユーザに端末ごとに記憶させることを許可する(HTTPSが必須)
このオプションを有効にすると、ユーザーがHTTPSで接続した際「デバイスで認証情報を記憶する」オプションがサインインページへ表示されます。ユーザーがボックスをチェックすると、サインアウトではなくブラウザを閉じて終了した場合、同じデバイスであればサインインが次回以降自動で行われます。サインアウトを行った場合は次回接続時に再度サインインが必要です。ユーザー情報は、下記の「記憶できる日数」で指定した日数保持されます。指定した日数以降、ユーザーは再度サインインが必要です。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:** 端末やブラウザで認証情報を記憶オプションを有効にしていると、ユーザーの アカウント » 設定 27 ページで「*この端末/ブラウザでは認証情報を表示しない*」オプションが利用できるようになります。クリックすると、対象の端末では認証情報が記憶されません。

記憶できる日数(1日から365日)
ユーザーに端末ごとに記憶させることを許可する、のオプションを使っている場合、ここで再ログインまで何日間記憶するかを指定できます。デフォルトは30日間です。

サインインオプション

サインイン画面で「パスワードを紛失」リンクを表示
デフォルトで、サインインページには「パスワード紛失」リンクが表示されており、パスワード変更のためのリンクをここから送信できます。リンクはSecurity Gatewayのユーザーアカウントに紐づけられたアドレス宛に送信されます。「パスワード紛失」リンクを表示しない場合にはこのオプションを無効にしてください。

サインイン画面に、次の管理者への連絡先情報を表示する
このオプションを有効にし、下のボックスへテキストを入力すると、サインインページで管理者の連絡先情報やリンクとして表示できるようになります。入力するテキストには、アンカーやイメージといったHTMLを使用する事ができます。

デフォルト

このアカウント宛のメッセージでアンチスパムを実行しない
このオプションは設定[27]ページにある同名のユーザーオプションのデフォルト値です。これを有効化すると、デフォルトでサーバーはDNSBL[138], URIBL[141], ヒューリスティックとベイジアン[132],Outbreak Protection[128]を行わなくなります。

このアカウントに対する"アカウントのハイジャック検出"機能を無効化する
デフォルトでアカウントをアカウントハイジャック検出[190]の対象外とする場合はこのオプションを有効化します。短時間で大量のメールを送信するアカウントについてはこの設定から除外する必要が生じる場合があります。個々のアカウントのアカウント設定[27]ページから個別のオプションを設定できます。

送信先を自動的にホワイトリストに入れる
このオプションは、各ユーザの設定[27]ページで**送信先を自動的にホワイトリストに入れる**オプションのデフォルト設定を管理します。ユーザに許可する場合、そのユーザがメッセージを送信するすべてのアドレスは、自分のアドレスホワイトリストに追加され、ホワイトリスト[30]リンクに到着します。これは、それらのアドレスからそのユーザに対する今後の受信メッセージが誤ってスパムとしてフラグを付けないことに役に立ちます。

強固なパスワードを要求
新しいパスワードには最少8文字が必要で、最低1つづつ下記を含む必要があります:

- 大文字
- 小文字
- 数字
- 記号文字 e.g. ;,_.?/-=

ユーザーの編集[47]ページには、このアカウントには強固なパスワードを要求しない、というオプションがあり、これを使うと、特定のユーザーを、ここでの要件から除外できます。

統計グラフを表示するタイミング
ダッシュボード 9 と 開始ページ 26 で統計グラフをいつ表示するかを選択するにはこのオプションを使用します。自動、常時、手動、表示しない、のどれかを選択できます。

言語
システム通知で使用するデフォルトの言語を、ドロップダウンリストから選択します。このオプションは個々のユーザー用にも用意されており、ユーザー設定で個々のユーザーのデフォルト値を上書きできます。

サードパーティーサービスのセキュリティ侵害を受けたパスワードリストを使って、パスワードをチェックする
SecurityGatewayは、サードパーティーサービスから過去にセキュリティ侵害を受けたパスワードリストを参照し、ユーザーのパスワードが該当していないかをチェックすることができます。サービスにパスワードを送信することなく、このチェックを行なうことができます。ユーザーのパスワードがこのリストに該当しても、アカウントがハッキングされているわけではありません。以前に誰かが同じパスワードを使って攻撃を受けたことがあることを意味しています。表示されたパスワードは、ハッカーの辞書攻撃に使用される可能性があります。他で使われたことの無いユニークなパスワードは、より安全となります。詳しくは、Pwned Passwordsを参照してください。

ドロップダウンからパスワードが前回チェックされてからどの位の頻度でパスワードチェックを行うか指定します。次の中から選択できます:

- 行わない(パスワードのチェックは行われません。これはデフォルト設定です。)
- 最終確認からの日数
- 最終確認からの週
- 最終確認からの月

1ページに表示する項目数
このオプションは、SecurityGatewayで記録するホワイトリストアドレス、メッセージログのエントリなど、ページ単位で表示するアイテム数を指定します。各ページの下に1ページで表示できない多くのアイテムがある場合、別のページに移動するためのコントロールがあります。このオプションのデフォルト値は50です。

利用規約

ユーザーがログインする前に、以下の利用規約への同意を求める
このオプションを有効化し、ボックスへ利用規約などの文章を入力すると、ユーザーがSecurityGatewayへログインする度に同意を求めるウィンドウが表示されます。ユーザーはチェックボックスをクリックし規約へ同意する事ができます。

新規ユーザー

新規ユーザへWelcomeメッセージを送信する
新規のユーザが作成された際"welcome"メッセージを送信するにはこのオプションを有効化します。メールへはSecurityGatewayへのリンクが記載されており、ユーザはリンク先からログインする事で、アカウント初期設定や隔離フォルダの管理が行えるようになります。このオプションは、デフォルトで無効です。

新しいユーザーが作成された際、グローバル管理者へ通知メッセージを送信する
新規のユーザが作成された際グローバル管理者[49]へ通知を送るにはこのオプションを有効化します。

新しいユーザーのパスワードを、サードパーティーのセキュリティ侵害を受けたパスワードリストでチェックする
このオプションを有効にすると、新しいユーザーのパスワードを、前述の「サードパーティーサービスのセキュリティ侵害…」のオプションを使ってチェックします。

ユーザーのメールボックス名に、プラス(+)記号の使用を許可する
メールボックス名に、プラス(+)記号を含むユーザーを作成する必要がある場合に有効化します。このオプションが有効の場合には、メールボックス名をサブアドレスエイリアスとして解釈しません。例えば、frank.thomas+billing@example.comは、frank.thomas@example.comのエイリアスとしてではなく、そのままのユーザー名として認識されます。

（以下のサブアドレス[64]を参照してください。）

サブアドレス

サブアドレス（プラスアドレスとも呼ばれています）は、メールアドレスへタグやフォルダ名を追加する方法として広く知られている手法です。このシステムを使用する事で、宛先が*user+tag@domain*（例*frank.thomas+billing@example.com*）というメールは自動的にアドレスに含まれているフォルダへ格納されます。メールサーバーによっては、この処理を自動で行いますが、メールサーバーによっては、こうしたアドレスを単純にエイリアスとして処理し、また、メールサーバーによっては、サブアドレスに未対応で、こうしたアドレスを、アドレスプラスタグではなく、そのままのメールアドレスとして扱います。

例えば、サブアドレスに対応したメールサーバーでは、frank.thomas@example.comがIMAPで「billing」というフォルダを所有していた場合、frank.thomas+billing@example.com宛に届いたメールは、Frankに届き、対象フォルダへ自動的に配送されます。サーバーがサブアドレスをエイリアスとして処理した場合、メールは単純にFrankの受信フォルダへ配信されます。（ただし、Frankがメールフィルタで対象メールを「billing」フォルダへ自動で振り分ける可能性はあります。）サーバーがサブアドレスに未対応の場合、メールは「frank.thomas+billing」という不明なユーザー宛のものとして拒否されます。

SecurityGatewayでは、受信メールがこのような形式だった場合、+の文字を含むユーザーが実在するのか、またはユーザーのサブアドレスなのかをチェックします。ユーザーもエイリアスも存在しなかった場合や、ユーザーは見つかったが 再検証[54]が必要な場合、最適なユーザー検証ソース[52] にて検証が行われます。 ユーザー検証ソースはSecurityGatewayへ届いたフルメールアドレスを使用します。これはメールアドレスが対象アドレスを許可するのに使用されます。アドレスが検証されると、SecurityGatewayは必要に応じてユーザー又はユーザーのエイリアスを作成します。

最後に、ドメインメールサーバー[65]宛に配信されたメールについて、SecurityGatewayは元のメールに含まれているフルメールアドレスを常に使用します。例
.frank.thomas+billing@example.com

例外 – ドメイン

これらの設定を構成する時、ページ上部のドメイン:ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。ユーザオプションの設定を見直し編集するには、対応するドメインの表示 / 編集リンクをクリックする、あるいはデフォルトの全体の設定値をドメインの設定にリセットするには、リセットをクリックします。

3.2 メール設定


設定/ユーザメニューのメール設定セクションにはメール関連機能用の以下の5ページへのリンクがあります:

ドメインメールサーバ 65
このページは、ドメインメールサーバ全体の管理で使用します。ドメインメールサーバは、SecurityGatewayがゲートウェイとして実行しているメールサーバです。通常、これらはユーザがメールアカウントを持ち、メッセージが保存されるサーバです。SecurityGatewayが対象ドメイン内のユーザー宛のメールを受信すると、ドメインに紐づいたメールサーバー宛にメール配信を行います。

リモートPOPアカウント 67
リモートPOPアカウントオプションで、ドメインユーザに再配送用にリモートPOPメールボックスからメールをダウンロードするために、POP3プロトコルの使用を行う設定をします。収集されると、メッセージは、POPアカウント編集 68画面で提供される設定に従って解析され、実際にメッセージが従来のSMTPトランザクションを使用したサーバに到着したかのように有効なユーザに配信されます。

隔離設定 71
このページは、セキュリティ 126機能にある"...メッセージを隔離する"オプションを無効にすることを許可します。さらに、ユーザを個人的にドメインでデフォルト隔離オプションを無効に許可するか、隔離フォルダの内容の閲覧と管理を許可するか選択することができます。最後に、ユーザが隔離フォルダの内容の詳細をメールで受信する方法(受信しない、毎日または毎週)を選択することができます。

メール配信 74
メール配信ページのオプションは、SecurityGatewayは自ら送信メッセージの配信を処理、または他のサーバに処理を受け渡すか指定します。このページさらには、配信を中止し配信不能メッセージを差出人に戻す前に、致命的でないエラーに遭遇する送受信メールの配信の試みる時間を指定するオプションがあります。これらのオプションは、全体のオプションで、すべてのSecurityGatewayドメインに適用します。

Emailプロトコル 76
Emailプロトコルページには、メールのSecurityGatewayの技術的な処理を管理している各種のオプションがあります。例えば、メールを受信するために使用するポート、同時のSMTPセッションの最大数、SecurityGatewayがVRFYリクエストを受け入れるか、プレーンテキストパスワードの許可、その他詳細なオプションの設定を行います。

3.2.1 ドメインメールサーバ


このページは、ドメインメールサーバ全体の管理で使用します。ドメインメールサーバは、SecurityGatewayがゲートウェイとして実行しているメールサーバです。通常、これらはユーザがメールアカウントを持ち、メッセージが保存されるサーバです。SecurityGatewayがドメインの1つで照合されたユーザに対してメッセージを受信する時、そのドメインに関連したメールサーバにメッセージを配信することを試みます。各SecurityGatewayドメイン 39は、特にSecurityGatewayで指定した一つ以上ドメインメールサーバを持つか、またはデフォルトサーバ 66に指定するドメインメールサーバを使用します。メールサーバが一覧を示すドメインを開くには、左側のボックスのナビゲーションメニューで設定/ユーザをクリックし、そのペインのアカウントセクションのドメインサーバサーバをクリックします。

ドメインメールサーバページには、説明、サーバとポートの3つのカラムがあります。説明には、メールサーバ（例えば、サーバXのexample.com）の説明、サーバカラムには、メールサーバのホスト名またはIPアドレス、ポートカラムには、メッセージを送信する時に使用するポートの一覧を示します。
ドメインメールサーバを編集するには、エントリをダブルクリックするか、またはエントリを選択しページ上部のツールバーの**編集**をクリックします。これは、メールサーバを編集 66画面を開きます。

ページ上部ツールバーには、次の4つのオプションがあります。

新規
新規メールサーバ画面（新規のドメインメールサーバを作成するために使用）を開くために**新規**をクリックします。この画面は、メールサーバを編集 66画面と同じです。

編集
リストで現在選択されるエントリに対応するメールサーバを編集 66画面を開くために、ツールバーの**編集**ボタンを使用します。あるいは、エントリをダブルクリックすることでも画面を開くことができます。

削除
ドメインメールサーバを削除するには、リストからエントリを選択し**削除**をクリックします。削除を確認するボックスが現れます。CtrlおよびShiftキーを用いて複数のエントリを選択することができます。

ドメイン:
リストにドメインメールサーバの表示を選択するには、**ドメイン:**ドロップダウンリストボックスを使用します。デフォルトでは、すべてのサーバが表示されますが、デフォルトサーバ（メールサーバを編集 66画面で指定）として指定したサーバだけを表示するために、"-- デフォルト --"を選択することができまたは、そのドメインのメールサーバだけを表示するために、リストからドメインを選択することができます。

3.2.1.1 メールサーバを編集

メールサーバを編集画面は、既存のメインメールサーバ 65の編集または新規サーバを作成するために使用します。ドメインメールサーバページで**新規**をクリック、またはエントリを選択し**編集**をクリックすることで画面を表示することができます。この画面で、サーバの説明、ロケーション、接続ポート、必要な認証証明書、および使用するSecurityGatewayドメインを指定します。さらにデフォルトメールサーバを指定することもできます。

プロパティ

説明:
サーバの説明（例えば、サーバXのexample.com）に、このテキストボックスを使用します。ドメインメールサーバページで説明カラムに対応します。

ホストまたはIP:
これは、ホスト名またはメールサーバのIPアドレスです。ユーザのメールを配信することを試みる時に、SecurityGatewayでは、このロケーションに接続します。このオプションは、ドメインメールサーバページでサーバカラムに対応します。

ポート:
これはサーバに接続する時に、SecurityGatewayが使用するポートで、ドメインメールサーバページでポートカラムに対応します。

認証が必要
メールを送信する前に認証をドメインメールサーバが要求する場合、このチェックボックスをクリックします。ユーザ名およびパスワードを下記で指定します。

ユーザ名:
サーバが認証を必要とする場合、ユーザ名をここに指定します。

パスワード:
ドメインメールサーバパスワードをここに入力します。

タイプ

このサーバをデフォルトにする
デフォルトドメインメールサーバの1つを、このサーバにする場合、このチェックボックスをクリックします。デフォルトサーバは、特に関連したドメインメールサーバがない場合、すべてのSecurity Gatewayドメインのために使用されます。

このメールサーバで使用するドメインを次から選択...
Security Gatewayドメインに、このサーバを指定するためには、下記のオプションを使用します。複数のドメインメールサーバがドメインに指定される場合、ドメインのプロパティ画面のメールサーバタブ 41 で配信を試みる順位を指定することができます。

有効なドメイン:
このボックスは、すべての利用可能なSecurity Gatewayドメインの一覧を示します。このドメインメールサーバを使用するドメインを指定するために、リストから"--->"をクリックします。

選択したドメイン:
このボックスは、このメールサーバを使用するために構成したすべてのSecurity Gatewayドメインの一覧を示します。リストからドメインを削除するには、ドメインを選択し"<---"をクリックします。

3.2.2 リモートPOPアカウント

リモートPOPアカウントオプションから、Security GatewayがPOP3プロトコルを使ってPOPメールボックスからドメインユーザー宛のメールを代理受信するよう設定する事ができます。収集されたメッセージは、POPアカウント編集 68 画面で提供される設定に従って解析され、従来のSMTPトランザクションを使用してユーザに配信されます。

メールボックスで保存されPOP3プロトコルを使用して取り出されるメッセージは、通常はSMTPプロトコルを使用して配信されたメッセージに提供される重要なルーティング情報(メッセージの"**envelope**"と呼ばれることのある)がないことに注意をすることが重要です。これは、従来からPOPメールボックスが、全体のドメインまたは複数ユーザでなく、個人に関連することを意味するからです。メールボックス内のすべては同じ受信者を目的とすると仮定し、したがって、初期のルーティング情報は今後必要とされません。ルーティング情報を持たないメッセージについて、指定受信者を判定するために、各メッセージのヘッダを調べる解析 70 オプションをSecurity Gatewayで使用するようにします。関連したSecurity Gatewayドメインで有効な受信者を含むヘッダを持つメッセージは配信されます。有効な受信者のないメッセージは、POPメールボックスから削除され、Security Gatewayから削除されます。リモートPOPアカウントページは、行ごとに1つのエントリを示し、有効、説明、ホスト、ポートおよびドメインの5つのカラムを持ちます。

これらの各項目およびPOPアカウントのエントリの作成と編集の詳細な情報については、POPアカウント編集画面 68を参照してください。

ページ上部のツールバーには、次の5つのオプションがあります:

新規
新規POPアカウントのエントリを作成するPOPアカウント画面を開くには**新規**をクリックします。これは**POPアカウント編集**画面と同じです。

編集
一覧から選択しているアカウントのPOPアカウント編集 68画面を開くには、編集ボタンをクリックするか、またはエントリをダブルクリックします。

削除
POPアカウントを削除するには、一覧からエントリを選択して削除ボタンをクリックします。エントリの削除の確認ダイアログが現れます。複数のエントリを選択するにはCTRLやShiftキーを使用します。

すぐ確認する
選択したPOPアカウントの新規メッセージを確認するには、このボタンをクリックします。

ドメイン:
一覧に表示するPOPアカウントを表示するには**ドメイン:**ドロップダウンリストを使用します。デフォルトでは、すべてのアカウントを表示しますが、特定のドメインのPOPアカウントを表示するために指定することができます。

3.2.2.1 POPアカウントの編集

リモートPOPアカウント 67ページで新規又は編集ボタンを押すと、POPアカウントの編集ページが起動し、POPアカウントの作成や編集が行えます。POPアカウント編集画面には*ホストとオプション*、*解析*の2つのタブがあります。ホストおよびオプションタブで、POPアカウントと関連するホストおよびログイン情報、POPホストへの接続で利用するセキュリティプロトコルの指定、さらにSecurityGatewayでPOPアカウントからメールを収集する頻度を指定するために使用します。解析タブからは、SecurityGatewayが受信者アドレスおよび送信者IPアドレスの検索で使用するヘッダを指定できます。

ホストとオプション

このアカウントを利用禁止にする
POPアカウントを使用禁止にする場合、このチェックのチェックボックスを選択します。アカウントはリモートPOPアカウント 67一覧で今まで通り現れますが、SecurityGatewayでは今後メールを収集することを試みません。再びメール収集を開始するには、チェックボックスを解除します。

このドメインからメールを収集
このPOPアカウントが結びつけられるドメインを指定するために、このドロップダウンリストを使用します。受信者アドレスについてメッセージヘッダを解析する場合、SecurityGatewayでは、ヘッダでこのドメインのユーザを探します

メールボックス

説明
POPアカウントの名前あるいは説明に、この入力ボックスを使用します。これはPOPアカウント一覧で参照するためのものです。

ホストまたはIP
ここへPOPアカウントのドメインまたはIPアドレスを入力します(例えば: `pop.example.com`)。

ポート
これは、アカウントからメール収集する時、SecurityGatewayで使用するポートです。デフォルトポートは110番です。

ユーザ名
POPアカウントのログインまたはユーザ名を入力します。

パスワード
POPアカウントのパスワードを入力します。

セキュリティ

セキュアな接続を使用
SecurityGateway for Email Serversは、データや通信を保護するための最新の暗号化技術に対応しています。POPアカウントのメッセージ収集時、使用するオプションを選択してください。

しない
暗号化セッションにPOPホストが対応していない場合や、使用しない場合には、このオプションを使用します。

TLS,可能な場合
POPアカウントからメールを収集する場合、使用可能な場合、Transport Layer セキュリティ(TLS)暗号化を使用する場合、このオプションを選択します。POPホストがTLSをサポートしない場合、暗号化を使用することなく、SecurityGatewayは通常メッセージを収集します。これはデフォルトオプションです。

TLS
このPOPアカウントからメッセージを収集時、TLS暗号化を必要とする場合、このオプションを選択します。

SSL
このPOPアカウントからメッセージ収集時、SSL暗号化を必要とする場合、このオプションを使用します。

セキュアな認証(APOP)が必要
このアカウントからメールを取り出す時、APOPコマンドおよびCRAM-MD5認証を使用する場合、このチェックボックスを選択します。これは、クリアテキストパスワードを送信する必要のない認証を行う際に使用します。

メッセージ収集

サーバにメッセージを残す
このオプションを選択すると、SecurityGatewayでメッセージをダウンロードしますが、POPアカウントのホストサーバからメッセージを削除しません。

...指定日数より以前
これは削除される前にPOPホスト上に残すことができる日数です。

ホストによってはメールボックスへメールを保持できる期間を限定している場合があります。

ポーリング間隔: [xx] 分間
このオプションは、SecurityGatewayで新規メールのPOPホストをチェックする方法を管理します。5分ごとにチェックすること推奨します。

タイムアウト: [xx] 秒
これは、SecurityGatewayが中断する前にPOPホストからの応答を延期される秒数です。60秒を推奨します。

解析

宛先(RCPT)

これらのヘッダを受信者(RCPT)用に解析する:
受信者メールアドレス用の解析するためにSecurityGatewayで必要とするヘッダを指定するには、このオプションを使用します。ここで示されるすべてのヘッダは、アドレスのためにチェックされます。

受信者(RCPT)用に'Received'ヘッダを解析する
メッセージのSMTP envelope内で検出された受信者情報は'Received'ヘッダ内でも検出されるので、これは、これらのヘッダを解析を可能にすることができ、できる限り実際の受信者アドレスを収集します。各メッセージ内で見つけ出される'Received'ヘッダすべてから有効なアドレスを解析する場合、このチェックのチェックボックスを選択します。

最初の[xx]'Received:'ヘッダを省略する
サーバ構成によっては、'Received'ヘッダを解析するものの、最初の幾つかのヘッダについては解析をスキップしなくてはならない場合があります。この設定は、SecurityGatewayが解析を開始する前に省略する'Received'ヘッダの数を入力することができます。

IPアドレス

差出人のIPアドレス用に'Received'ヘッダを解析する
各メッセージ内で見つけ出される'Received'ヘッダのすべてから送信者のIPアドレスを解析する場合、このチェックボックスを選択します。送信者のIPアドレスを取得することは、各種のセキュリティルックアップやスパムブロックオプションについて便利です。

最初の[xx]'Received:'ヘッダを省略する
一部のサーバ構成で、'Received'ヘッダを解析するが、最初のヘッダから解析を省略することを必要とすることがあります。この設定は、SecurityGatewayが解析を開始する前に省略する'Received'ヘッダの数を入力することができます。

このヘッダを差出人のIPアドレス用に解析する:
送信者のIPとしてアドレスを解析する特定のヘッダを指定するために、このオプションを使用します。デフォルト値は、X-ORIGINATING-IPです。

3.2.3 隔離設定


隔離オプションページでは、セキュリティ[126]機能にある"...メッセージを隔離する"オプションを、全体またはドメイン毎に上書きする事ができます。また、各ユーザがドメイン用のにデフォルト隔離オプションを上書きできるかどうかや、隔離フォルダの内容の閲覧や管理を許可するかどうかをここで指定できます。最後に、ユーザが隔離フォルダの内容の詳細をメールで受信する頻度(受信しない、毎日または毎週)を選択することができます。

メッセージ

SecurityGatewayサーバで隔離メッセージを保持する
このオプションを選択すると、任意のセキュリティ[126]機能で指定される"...メッセージを隔離"基準に合っている任意のメッセージは、SecurityGatewayサーバで保有されます。これは、デフォルトオプションです。

隔離フォルダ内容一覧のメールをユーザへ送信する:
メッセージがSecurityGatewayサーバで隔離に保持される場合、このオプションは、隔離内容の一覧をユーザへメールで送信する頻度を指定します。

しない
隔離フォルダの内容一覧メッセージを各ユーザを送信しない場合、このオプションを選択します。

XX時間毎
このオプションを選択し、時間を指定すると、指定した間隔毎に隔離されたメールについてユーザーへ通知します。

毎日
このオプションが選択される場合、各アカウントは、毎日ユーザの隔離内容の要点をまとめるメッセージを毎日受信します。これはデフォルトオプションです。

毎週
1週間に1回メールを送信する場合、このオプションを選択します。

次の指定されたスケジュール:
追加をクリックして隔離レポートスケジューラーを起動し、隔離フォルダレポートが送信される予定日時を指定できます。

スケジュール

日
新しい予定の作成時、まずはメールを送信する日を選択します。選択肢は次の通りです: 毎日、平日(月～金)、週末(土曜日と日曜日)、指定の曜日。複数を選択したい場合は、それぞれの曜日用に個別の予定を作成してください。

開始
隔離レポートを送信する時間を入力します。時間は24時間の形式で00:00から23:59の間で指定してください。レポートを一日の中で一定間隔で送りたい場合は、終了と繰り返し間隔を指定してください。隔離レポートを一日に一回だけ送信したい場合は、終了と繰り返し間隔の項目は空白のままにして下さい。

終了
隔離レポートを一日の内で最後に送信する時間を指定します。時間は24時間の形式で00:01から23:59の間で指定してください。この値は、前述の開始時間よりも後にする必要があります。例えば、開始が10:00だった場合、ここでの値は10:01から23:59の間で指定する必要があります。もしも毎日繰り返し送信するのではなく、毎日一回だけレポートを送りたい場合は、ここでの値は空白にしてください。

繰り返し間隔
隔離レポートを、前述の開始時間から終了時間までの間で、どの位の間隔で送信するのかを指定します。毎日一回だけレポートを送りたい場合は、ここでの値は空白にしてください。

最後に送信されたメール以降の新しい隔離メールだけを含める
デフォルトで、隔離レポートには隔離フォルダ内の全てのメールの一覧が含まれます。このオプションを有効にすると、最後の隔離レポート以降に隔離フォルダへ追加されたメールの一覧のみがレポートに表示されます。対象となるメールがない場合、隔離レポートは生成されません。

選択が終了したら、保存して終了をクリックし、作成したエントリを隔離設定ページへ追加してください。

隔離メールをソート:[宛先|送信元|件名|スコア]
このオプションで隔離メールの一覧をどのようにソートするか選択する事ができます。デフォルトで受信したメールは受信日時でソートされますが、送信元や件名、スパムスコアでソートする事もできます。

隔離リストとメールに「ブラックリスト」オプションを含める
このオプションを使用すると、隔離メールの一覧画面と隔離レポート通知へリンクが表示され、ここから送信元のアドレスをブラックリストへ追加できるようになります。

隔離リストとメールに「ブラックリストドメイン」オプションを含める
このオプションを使用すると、隔離メールの一覧画面と隔離レポート通知へリンクが表示され、ここから送信元のドメインをブラックリストへ追加できるようになります。

隔離メール内に"メッセージの表示"オプションを含める
このオプションを使用すると、隔離レポートメールへ「メッセージの表示」が含まれるようになり、ユーザーが隔離されたメールを確認できるようになります。このオプションは次のメニューからもアクセスできます: メイン | アカウント | 設定

隔離メッセージのフィルタをメールサーバまたはクライアントに許可する
このオプションが選択される場合、各種のセキュリティ[126]機能で"...メッセージを隔離する"オプションを無効にします。隔離されたメッセージを受信者に送信する代わりに、隔離またはフィルタすることを受信者のクライアントまたはサーバに許可します。ページ上部のドメイン:ドロップダウンリストボックスを使用することにより、全体または個々のドメインに、このオプションを設定することができます。

...次の文字を件名に付ける [*text*]
隔離されたメッセージの件名にタグを追加する場合、このオプションを有効にします。このタグは、メッセージをフィルタするために、受信者のクライアントまたはサーバにより使用することができます。

...次のヘッダを追加 [*text*]
隔離されたメッセージにメッセージヘッダを追加したい場合、このオプションを有効にします。このヘッダは、メッセージをフィルタするために、受信者のクライアントまたはサーバにより使用することができます。デフォルトヘッダは以下の通りです。

```
"X-Spam-Flag: YES"
```

ユーザ

下記の2つのユーザオプション[60]は、ユーザオプションページの2つのオプションと同じものです。このページで行った設定は別ページへも反映されます。オプションは、便宜上、両方の場所で提供されます。

ユーザへ隔離フォルダの表示と管理を許可する
このオプションが有効にする場合、ユーザは隔離に置かれた受信メッセージを閲覧および管理することができます。これは、メッセージの解放および削除などを行う隔離を表示[34]ページを表示することを許可します。

ユーザへ隔離設定の変更を許可する
設定[27]ページにある隔離設定の編集を各ユーザに許可する場合は、このオプションをクリックします。

管理隔離(全てのドメイン)

このオプションでいつ管理隔離の一覧をメール通知するかを指定できます。オプションは上記のユーザー隔離とは別で指定します。

例外 - ドメイン

これらの設定を構成する時、ページ上部のドメイン:ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。隔離オプションの

設定を見直し編集するには、対象ドメインの**表示/編集**リンクをクリックします。全体のデフォルト設定値でドメイン設定を初期化するには、**リセット**をクリックします。

3.2.3.1 隔離レポートスケジューラ

隔離設定 71 ページで、「以下のスケジュール」オプションの下にある「追加」をクリックすると、隔離レポートスケジューラーが起動でき、隔離フォルダレポートが配信されるスケジュールをカスタマイズする事ができます。

スケジュール

日
新しい予定の作成時、まずはメールを送信する日を選択します。選択肢は次の通りです: 毎日、平日(月～金)、週末(土曜日と日曜日)、指定の曜日。複数を選択したい場合は、それぞれの曜日用に個別の予定を作成してください。

開始
隔離レポートを送信する時間を入力します。時間は24時間の形式で00:00から23:59の間で指定してください。レポートを一日の中で一定間隔で送りたい場合は、終了と繰り返し間隔を指定してください。隔離レポートを一日に一回だけ送信したい場合は、終了と繰り返し間隔の項目は空白のままにして下さい。

終了
隔離レポートを一日の内で最後に送信する時間を指定します。時間は24時間の形式で00:01から23:59の間で指定してください。この値は、前述の開始時間よりも後にする必要があります。例えば、開始が10:00だった場合、ここでの値は10:01から23:59の間で指定する必要があります。もしも毎日繰り返し送信するのではなく、毎日一回だけレポートを送りたい場合は、ここでの値は空白にしてください。

繰り返し間隔
隔離レポートを、前述の開始時間から終了時間までの間で、どの位の間隔で送信するのかを指定します。毎日一回だけレポートを送りたい場合は、ここでの値は空白にしてください。

最後に送信されたメール以降の新しい隔離メールだけを含める
デフォルトで、隔離レポートには隔離フォルダ内の全てのメールの一覧が含まれます。このオプションを有効にすると、最後の隔離レポート以降に隔離フォルダへ追加されたメールの一覧のみがレポートに表示されます。対象となるメールがない場合、隔離レポートは生成されません。

選択が終了したら、保存して終了をクリックし、作成したエントリを隔離設定ページへ追加してください。

3.2.4 メール配信

メール配信ページのオプションは、SecurityGatewayが送信メール配信を自分自身で行うのか、他のサーバーへ転送するのかを指定するのに使用します。このページでは、送受信メールで配信不能だったものを送信不能として返信する前にどのように処理するのかを指定するオプションも提供されています。このオプションは全体オプションとしてSecurityGatewayが管理している全てのドメインに適用されます。

リモートメール配信

常に直接すべての送信メールを受信メールサーバへ送信する
このオプションが選択される場合、SecurityGatewayは、受信者のメールサーバに直接各送信メッセージを配信することを試みる通常のSMTP配信処理(通常のDNSルックアップの実行、MXレコードのチェックなど)を使用します。このオプションはデフォルトで選択されます。

常に次に指定されるサーバへ各送信メールを送信する
別のサーバに、すべての送信メールを送信する場合、それらのメッセージを配信する処理を渡す場合、このオプションを選択します。

メールサーバ:
SecurityGatewayがすべてのメッセージを送信するためのメールサーバに、配信処理を渡すため、このオプションを使用します。ホストまたはIPアドレス(例えばmail.example.comまたは192.168.0.1)を入力することができます。

ポート
これは、指定されたサーバにメッセージを送信する時に、SecurityGatewayが使用するポートです。

上記メールサーバのアクセスに認証が必要
指定されたメールサーバが認証を必要とする場合、このチェックボックスをクリックして、ログイン証明書を下記で入力します。

ユーザ名:
認証が必要とされる場合、ユーザ名ログイン証明書をここに入力します。

パスワード:
上記で入力されるユーザ名に対応するパスワードを入力します。

リトライキュー

リトライキューオプションでは、例えば、受信者のメールサーバが一時的に利用できないような致命的でないエラーが発生したメールを、SecurityGatewayがどのように処理するのかを指定します。

最初の1時間で配信失敗後の再配信:[xx]分間(推奨 5分)
メッセージが配信できなかった後、最初の1時間の間に、SecurityGatewayで再配信を行う間隔です。デフォルト設定は5分です。

この時間内で送信されなかったメールについて送信者へ通知
デフォルトで、SecurityGatewayが1時間以内にメールを配信できなかった場合、送信者へメールが配信できていない旨を通知するメールを送信し、メールの再配送を続けます。通知メールを送ら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。

...送信者へ通知する際元のメールを含む
デフォルトで、最初の1時間の後にSecurityGatewayが「送信できなかった」メールを送る際、元のメールのコピーがメール本文に含まれます。元のメールを含まない場合はこのチェックボックスを無効にして下さい。

上記以降の再配信間隔: [xx] 分間(推奨: 240分)
メッセージが1時間で配信できなかった後、SecurityGatewayで更に配信を、この間隔に切り替えます。デフォルト設定は240分です。. SecurityGatewayはここで指定した間隔で、後述の配信不能メールオプションで指定した日数の間、メールの再送を続けます。

SMTP接続失敗をキャッシュ
デフォルトで、対象ホストへのSMTP接続に失敗すると、SecurityGatewayは「最初の1時間で配信失敗後の再配信: [xx] 分間」で指定した時間内にホストへの接続を試みます。この設定は、SecurityGatewayが、例えば最初の接続でオフラインである事が確認できた場合などに、ホストに対する無駄な接続の繰り返しを避けるのに役立ちます。SMTP失敗のキャッシュを行わない場合は、このチェックボックスを無効にして下さい。

配信不能メール

送信か受信かを問わず、対象メールサーバーがダウンしているといった、致命的でないエラーが原因でメール配信が行えない場合に、SecurityGatewayが配信を中止し配信不能メッセージを差出人に戻すまでのオプションをここで設定します。

指定日数後でも配信ができない場合は差出人へ配信結果を通知する(推奨: 5日間)
これは、配信を停止する前に、メッセージの配信を継続する日数です。指定日数後に配信を中止します。

メール送信について送信者へ通知
デフォルトで、SecurityGatewayがメールを配信できなかった場合、メッセージの配信ができないと、メール送信者へ通知します。通知メールを送ら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。

...送信者へ通知する際元のメールを含む
デフォルトで、SecurityGatewayが「送信できなかった」メールを送る際、元のメールのコピーがメール本文に含まれます。元のメールを含まない場合はこのチェックボックスを無効にして下さい。

3.2.5 Emailプロトコル

Emailプロトコルページでは SecurityGatewayによる技術的なメールの処理方法に関するオプション設定が行えます。例えば、メールを受信する際のポート設定、許可するSMTPセッションの最大数、SecurityGatewayでVRFYリクエストを受け付けるかどうか、プレインテキストパスワードを許可するかどうか、その他関連した設定がここで行えます。

サーバ

HELOドメイン名:
これは、SecurityGatewayがSMTP処理中に確認に使用するドメイン名(例えばmail.example.com、smtp.domain.com、など)です。これは、メール処理を行ったのがどのサーバーかを判断するのに必要な、Receivedヘッダ、authentication-resultsヘッダ、その他のヘッダで使用されます。注意点:SecurityGatewayをクラスタリング[112]環境で使用している場合は、このオプションを、クラスタ内のサーバー毎に重複しない値で設定して下さい。

SMTPポート(カンマ区切りで複数指定):
これらは、SecurityGatewayがSMTPメッセージを受信するポートです。カンマで区切ることによって、複数のポートを指定できます。デフォルトSMTPポートは、25です。

専用SSLポート(複数指定はカンマ区切り):
ここにメールを受信する専用のSSLポートを指定します。カンマで区切ることによって、複数のポートを指定することができます。デフォルトSSLポートは、465です。

MSAポート(カンマ区切りで複数指定):
このオプションは、MSAポートを指定します。複数ポートの指定は、カンマで区切ります。デフォルトMSAポートは、465です。

これらのIPへソケットをバインドする(複数指定はカンマ区切り):
SecurityGatewayを特定のIPアドレスにバインドする場合、ここに指定します。複数の指定をする場合は、カンマで区切ります。

同時SMTP受信セッションの最大数:
この値は、"Server Too Busy"メッセージで応答する前に、SecurityGatewayが受け取る同時受信SMTPセッションの数を制御します。デフォルト値は、100です。

同時SMTP送信セッションの最大値:
ここに入力される値は、メールを送信する時、作成される同時の送信SMTPセッションの最大数です。すべての待機メッセージが送信されるまで、各セッションは送信メッセージを送信します。例えば、このオプションが30のデフォルト値に設定される場合、30のセッションを同時に作成することができ、直ちに30の異なるメッセージを配信する試みをSecurityGatewayで可能にします。

同時POP受信セッションの最大数:
この値は、"Server Too Busy"メッセージで応答するまでに、SecurityGatewayが受け入れる同時POPセッションの数を指定します。

デフォルトドメイン:
ドメインをドロップダウンリストボックスから選択します。これは、ある人がドメイン名なしにログインを試みる場合、SecurityGatewayで使用されると仮定するドメイン、および全くドメインが指定されない場合、MAIL、RCPTおよびVRFYコマンドのために使用されるドメインです。さらに、外部の管理者[49]に警報およびメッセージを送信する時、SecurityGatewayでは、このドメインを使用します。

SMTPプロトコル設定

VRFYコマンドを受け付ける
VRFY[177]コマンドを許可する場合、このオプションを使用します。これは、デフォルトで無効です。

プレーンテキスト パスワードを許可する(SSLまたはCRAM-MD5は必要なし)
デフォルトで、SecurityGatewayはSMTP認証の間、送信されるプレーンテキスト パスワードを受け取ります。このオプションを無効にする場合、SSLまたは認証のCRAM-MD5メソッドは必要とされます。

CRAM-MD5認証を受け付ける
このオプションが有効な場合、SecurityGatewayでCRAM-MD5認証を受け付けます。これは、デフォルトで無効です。

応答やReceivedヘッダでソフト ウェアのバージョン情報を非表示とする
サーバーの応答やReceivedヘッダでSecurityGatewayのソフト ウェアバージョン情報を隠す場合はこのオプションを有効にします。これは、デフォルトで無効です。

RFC準拠のコマンドとヘッダをチェックする
RFCインターネット標準に準拠していないメッセージを拒否する場合、このオプションを有効にします。有効にする場合、SecurityGatewayは、コントロールまたは8ビット キャラクタを含むメッセージ、およびDate、Sender、あるいはFromヘッダの存在のないメッセージを拒否します。さらに、これらの必要なヘッダは対応する値を持つ必要があります－空のヘッダとして存在することはできません。これに準拠しないメッセージを拒否しない場合、このチェックボックスを解除します。

メッセージごとに指定数のRCPTコマンドを許可する: [xx] (RFCでは100)
これは、メッセージにつき許可するRCPTコマンド(すなわち受信者の数)の数です。デフォルト値は、100です。

許可するSMTPメッセージの最大値: [xx] KB (0 = 無制限)
ここに設定するサイズを超えるメールの受信を禁止します。この機能が有効な場合、SecurityGatewayはRFC-1870で指定されているESMTP SIZE commandを使用することを試みます。送信エージェントが、このSMTP機能拡張をサポートする場合、SecurityGatewayでは実際の配信の前にメッセージサイズを測定しメッセージを拒否します。送信エージェントが、このSMTP機能拡張をサポートしない場合、SecurityGatewayは、送信サーバでメッセージ送信の開始を許可する必要があります。しかし最大サイズに到達する場合、メッセージを拒否します。デフォルトは0で、サイズに制限がないことを意味します。

データ転送が指定サイズを超えた場合に接続を切る: [xx] KB (0 = なし)
SMTP接続中にデータ伝送が、このしきい値を超える場合、SecurityGatewayは接続を閉じます。このオプションのデフォルト値は0で、サイズの制限はありません。

コネクションタイムアウト: [xx] 秒 (推奨値: 30)
SecurityGatewayがSMTPコネクションをタイムアウトとするまでの秒数を指定します。

プロトコルタイムアウト: [xx] 秒 (推奨値: 300)
コネクションが確率した際、SecurityGatewayがホストがSMTPプロトコル用ダイアログを開始するまでどの位待つかを秒数で指定します。

ループ検出と管理

最大メールホップ数 (1-100):
RFCではメールサーバーが処理毎に各メールへスタンプを付与するよう規定しています。これらのスタンプは、設定ミスなどにより生じるメールのループ発生時の数と比較する対象となります。メールループが検出できないと、ループ配送でリソースが消費されてしまいます。メールの処理回数をカウントする事

で、ループと思われるメールが検出され、不正メッセージ[252]キューへ配信されます。このオプションのデフォルト値は20です。

3.3 アーカイブ

3.3.1 設定

メールアーカイブはSecurity Gatewayを通過するメールの監視と保管を行うための機能です。アーカイブされたメールは管理者やエンドユーザーから簡単に検索[90]することができます。

設定

メールアーカイブの有効化
ドメインの送受信メールのコピーを保存する場合はこのボックスを有効にします。メールはアーカイブストアへ保存されます。それぞれのアーカイブストア[86]では検索[90]が行え、1つのドメインと紐づいています。画面右上のドロップダウンリストで「ドメイン用」を選択する事で、ドメイン毎に設定を上書きする事ができます。

「ジャーナルレポート」とこのメールボックスへ送信された転送メールを許可:
1つ又はそれ以上のメールボックスでOffice 365のジャーナルレポートを許可したりアーカイブ用にメールを転送する場合はこのオプションを使用します。Security Gatewayはアーカイブが有効になっているドメインでのメールを、実際のヘッダで宛先メールアドレスから判定し、許可します。この時点で、送信者や宛先が正しいものかどうかを(必要に応じてユーザー検証を行った上で)判断し、ドメインのアーカイブが有効であれば、メールを対象ドメインのアーカイブストアへ保存します。注意点:受信メールはドメインメールサーバー[65]から受信したメールである必要があります。

メールジャーナリングを有効にする
メールのジャーナルレポートを生成するにはこのオプションを有効にします。ジャーナルレポートは下記のジャーナル対象とするメールに対して生成され、ジャーナル用メールアドレス宛てに送信されます。元のメールはジャーナルレポートへ添付され、ジャーナルレポートの本文には送信元メールアドレス、メール件名、メッセージID、宛先メールアドレス等の情報が含まれます。ジャーナル対象として、内部のメールのみにする(これがデフォルト設定です)、外部のメールのみにする、全てのメールにする、の3つから選択する事ができます。

アーカイブストア

アーカイブストアとはアーカイブメールの保存用コンテナです。各アーカイブストアは1つのドメインに紐づいています。

アーカイブストアの自動生成
Security Gatewayがアーカイブストアの生成管理を行えるようにするにはこのオプションを使用します。これは推奨設定です。

アーカイブストアの自動生成の設定を行うにはこちらをクリック

アーカイブストアの自動生成

ここではSecurity Gatewayがどの程度の頻度、期間、サイズ、メール数で、アーカイブストアを自動生成するのかを選択します。、

新しいアーカイブストアの作成...

年毎/四半期毎/月毎
ドメイン用に新しいアーカイブストアを、年毎、四半期毎、月毎に自動生成するには、このオプションのどれかを選択してください。

現在のアーカイブストアが次の場合:
ドメインの既存アーカイブストアが一定のサイズに到達したり、一定数のメール数に到達した際、新しいアーカイブストアを作成するにはこのオプションを選択します。片方又は両方のオプションを使用できます。両方のオプションを使用した場合、新しいアーカイブストアはどちらかの条件に一致した際生成されます。

[xx]又はそれ以上のメール本数
このボックスをチェックすると、ドメイン用のアーカイブストアは指定した本数のメールがアーカイブされると新規に作成されます。デフォルトは5百万通です。

[xx]又はこれを超えるギガサイズ
このボックスをチェックしギガバイトでサイズを入力すると、アーカイブストアは指定容量に到達する毎に新しく生成されます。

Security Gatewayは新しいアーカイブストアを生成する必要があるかどうかを数分毎に確認します。アーカイブストアの閾値がここでの設定を上回る場合もあります。

データベース

サーバー内部のFirebirdデータベースファイルを使用する
デフォルトで、Security Gatewayはアーカイブ用に内部のFirebirdデータベースファイルを使用します。

Firebirdデータベースサーバーのインスタンスへ接続
外部のFirebirdデータベースサーバーへ接続しアーカイブを行う場合はこのオプションを選択します。クラスタリング 112を使用している場合もこのオプションを使用します。

SecurityGatewayのデータベースとして同じサーバーを使用
*「Firebirdデータベースサーバーのインスタンスへ接続」*を選択した場合のデフォルトオプションです。 アーカイブ用に、Security GatewayはSecurity Gatewayデータベースとして設定したFirebirdデータベースサーバへ接続し、同じ認証情報を使用します。追加で必要な情報は、(後述の)データベースパス/エイリアス名だけで、これはアーカイブストアを自動生成するデータベースファイルを指定するためのものです。

Firebirdデータベースサーバーのインスタンスへ接続
データベースの管理に、異なるFirebirdデータベースサーバーへ接続するにはこのオプションを選択します。サーバーアクセスのために、サーバー名かIP、ポート、ユーザー名、パスワードの情報が必要です。また、自動でアーカイブストアを作成する際のデータベースファイルのパス/エイリアス情報も必要です。

データベースパス/エイリアス名:
アーカイブストア用にデータベースファイルを自動生成するパスを入力します。**注意点:** このパスはFirebirdデータベースサーバーへの相対パスで、ネットワークパスである必要はありません。例えば、C:\Databases\Archives\$DOMAIN$.fbdのように記述します。

アーカイブ名のマクロ
アーカイブ用のファイル名に次のマクロが使用でき、自動生成の際、各アーカイブに固有の名称を使用する事ができます。

$DOMAIN$, $YEAR$, $MONTH$, $QUARTER$ 例えばデータベースパスとして "C:\Databases\Archives\$DOMAIN$-$MONTH$.fbd" を指定した場合、"Example.com-September.fbd"のような名前のデータベースが生成されます。Firebirdサーバーで自動生成されない、C:¥Databases¥Archives¥フォルダを作成しておくよう注意してください。

Firebirdサーバーはデータベース作成時、動的にフォルダ生成を行う事はありません。そのため、データベースパスへマクロを使用する場合は、最初にFirebirdサーバー上で、対象フォルダを手動で作成しておく必要があります。例えば、データベースパスが "c:¥Databases¥Archives¥$Domain$¥archive.fbd"だった場合、"C:¥Databases¥Archives¥"フォルダへ各ドメイン用のサブフォルダを手動で作成する必要があります。このため、マクロの使用は、フォルダ名よりもファイル名で使用する事を推奨しています。

ストレージロケーション

データベース、メールコンテンツ、検索インデックスに異なるディレクトリを使用する
デフォルトで、アーカイブストアのデータは下記の「ディレクトリ」オプションで指定したフォルダへ、¥data¥と¥index¥の2つのサブフォルダと併せて配置されます。このチェックボックスで3つのフォルダ全ての場所をカスタマイズできます。

「Firebirdデータベースサーバーのインスタンスへ接続」を選択した場合、このオプション設定はメールのコンテンツと検索インデックスだけが保持される場所として設定されます。データベースの場所は、上記のデータベースパス/エイリアスで指定した場所となります。

ディレクトリ:
自動生成されるデフォルトのアーカイブストア用データベースフォルダは次の通りです。

..\SecurityGateway\Archive\$DOMAIN$\

パスの中の $DOMAIN$ マクロはアーカイブストアと紐づいたドメイン名へ変換され、(ドメイン、ユーザー、データ等の)メタデータが含まれるFirebirdデータベース、ARCHIVE.FBDが格納されます。アーカイブデータはこのファイルなしでリストアする事ができません。フォルダにはアーカイブされたコンテンツとインデックスが格納されている..¥dataと..¥indexのサブフォルダも格納されています。

クラスタリング[112]を使っていて、上記の「Firebirdデータベースサーバーのインスタンスへ接続」を選択していた場合、ここでの設定はデータベースファイルの場所ではなく、..¥dataと..¥indexの格納先としてのみ使用されます。データベースの場所は、上記のデータベースパス/エイリアスで指定した場所となります。また、ここで指定するディレクトリは、ネットワークでアクセスできる場所である必要があり、UNCファイルパスでの記述が必要です。

例: \\share01\databases\Archive\$Domain$\

上記の「異なるディレクトリを使用」を有効にした場合、次の場所を選択する事ができます:

データベースディレクトリ:
アーカイブデータベースファイルの場所を指定します。**注意点:** このオプションは、上記の*Firebirdデータベースサーバーのインスタンスへ接続*を選択していた場合は利用できません。この場合、データベースの場所は、上記のデータベースパス/エイリアスで指定した場所となります。

デフォルトのデータベースディレクトリの場所は次の通りです: ..\SecurityGateway\Archive\$DOMAIN$\

コンテンツディレクトリ:
アーカイブストアのコンテンツが自動生成されるデフォルトロケーションは次の通りです

..\SecurityGateway\Archive\$DOMAIN$\data

パスの中の $DOMAIN$ マクロはアーカイブストアと紐づいたドメイン名へ変換され、archive.sgd ファイルが格納された[..¥data」サブフォルダも生成されます。このファイルには圧縮形式のアーカイブデータが含まれています。アーカイブデータはこのファイルがないとリストアできません。

注意点: クラスタリング[112]を使っていて、上記の「Firebirdデータベースサーバーのインスタンスへ接続」を選択していた場合、ここで指定するディレクトリは、ネットワークでアクセスできる場所である必要があり、UNCファイルパスでの記述が必要です。(例. \\share01\databases\Archive\$Domain$\data)

インデックスディレクトリ:
アーカイブストアのインデックスが自動生成されるデフォルトロケーションは次の通りです

..\SecurityGateway\Archive\$DOMAIN$\index

パスの中の $DOMAIN$ マクロはアーカイブストアと紐づいたドメイン名へ変換されます。サブフォルダ「..¥index」にはCLucene Full Text Indexingエンジンで生成されたフルテキストインデックスが含まれています。フルテキストインデックスは何らかの理由で徐々に破損していきます。フルテキストインデックスは、アーカイブストア[86]画面のメンテナンスオプションから再構築する事ができます。

注意点： クラスタリング[112]を使っていて、上記の「Firebirdデータベースサーバーのインスタンスへ接続」を選択していた場合、ここで指定するディレクトリは、ネットワークでアクセスできる場所である必要があり、UNCファイルパスでの記述が必要です。（例. \\share01\databases\Archive\$Domain$\index）

アーカイブストアの管理を行うにはこちらをクリック
アーカイブストア[86]の画面へ移管するリンクで、ここからアーカイブストアの確認や管理が行えます。

例外 - ドメイン

画面右上の「ドメイン:」ドロップダウンリストで特定のドメインを選択すると、ドメインが設定の保存後、ここへ表示されます。表示/編集リンクでアーカイブ設定を行うか、初期化をクリックしてドメイン設定をデフォルト値へ初期化する事ができます。

3.3.1.1 アーカイブストアの自動生成

この画面ではSecurityGatewayが新しいアーカイブストアを自動生成する頻度を指定したり、既存のアーカイブストアが一定の期間、サイズ、メール本数に到達した際、新しいストアを自動生成するかどうかを設定できます。この画面は アーカイブ設定[79] ページ内の「アーカイブストアの自動生成を設定するにはこちらをクリック」リンクからアクセスする事ができます。

新しいアーカイブストアの作成...

年毎/四半期毎/月毎
ドメイン用に新しいアーカイブストアを、年毎、四半期毎、月毎に自動生成するには、このオプションのどれかを選択してください。

現在のアーカイブストアが次の場合：
ドメインの既存アーカイブストアが一定のサイズに到達したり、一定数のメール数に到達した際、新しいアーカイブストアを作成するにはこのオプションを選択します。片方又は両方のオプションを使用できます。両方のオプションを使用した場合、新しいアーカイブストアはどちらかの条件に一致した際生成されます。

[xx]又はそれ以上のメール本数
このボックスをチェックすると、ドメイン用のアーカイブストアは指定した本数のメールがアーカイブされると新規に作成されます。デフォルトは5百万通です。

[xx]又はこれを超えるギガサイズ
このボックスをチェックしギガバイトでサイズを入力すると、アーカイブストアは指定容量に到達する毎に新しく生成されます。

SecurityGatewayは新しいアーカイブストアを生成する必要があるかどうかを数分毎に確認します。アーカイブストアの閾値がここでの設定を上回る場合もあります。

データベース

サーバー内部のFirebirdデータベースファイルを使用する
デフォルトで、SecurityGatewayはアーカイブ用に内部のFirebirdデータベースファイルを使用します。

Firebirdデータベースサーバーのインスタンスへ接続
外部のFirebirdデータベースサーバーへ接続しアーカイブを行う場合はこのオプションを選択します。クラスタリング 112を使用している場合もこのオプションを使用します。

SecurityGatewayのデータベースとして同じサーバーを使用
*「Firebirdデータベースサーバーのインスタンスへ接続」*を選択した場合のデフォルトオプションです。 アーカイブ用に、SecurityGatewayはSecurityGatewayデータベースとして設定したFirebirdデータベースサーバへ接続し、同じ認証情報を使用します。追加で必要な情報は、(後述の)データベースパス/エイリアス名だけで、これはアーカイブストアを自動生成するデータベースファイルを指定するためのものです。

Firebirdデータベースサーバーのインスタンスへ接続
データベースの管理に、異なるFirebirdデータベースサーバーへ接続するにはこのオプションを選択します。サーバーアクセスのために、サーバー名かIP、ポート、ユーザー名、パスワードの情報が必要です。また、自動でアーカイブストアを作成する際のデータベースファイルのパス/エイリアス情報も必要です。

データベースパス/エイリアス名:
アーカイブストア用にデータベースファイルを自動生成するパスを入力します。 **注意点:** このパスはFirebirdデータベースサーバーへの相対パスで、ネットワークパスである必要はありません。例えば、`C:\Databases\Archives\$DOMAIN$.fbd`のように記述します。

アーカイブ名のマクロ
アーカイブ用のファイル名に次のマクロが使用でき、自動生成の際、各アーカイブに固有の名称を使用する事ができます。

$DOMAIN$, $YEAR$, $MONTH$, $QUARTER$ 例えばデータベースパスとして "`C:\Databases\Archives\$DOMAIN$-$MONTH$.fbd`" を指定した場合、"`Example.com-September.fbd`"のような名前のデータベースが生成されます。Firebirdサーバーで自動生成されない、C:¥Databases¥Archives¥フォルダを作成しておくよう注意してください。

Firebirdサーバーはデータベース作成時、動的にフォルダ生成を行う事はありません。そのため、データベースパスへマクロを使用する場合は、最初にFirebirdサーバー上で、対象フォルダを手動で作成しておく必要があります。例えば、データベースパスが "c:¥Databases¥Archives¥$Domain$¥archive.fbd"だった場合、"C:

> ¥Databases¥Archives¥"フォルダへ各ドメイン用のサブフォルダを手動で作成する必要があります。このため、マクロの使用は、フォルダ名よりもファイル名で使用する事を推奨しています。

ストレージロケーション

データベース、メールコンテンツ、検索インデックスに異なるディレクトリを使用する
デフォルトで、アーカイブストアのデータは下記の「ディレクトリ」オプションで指定したフォルダへ、¥data¥と¥index¥の2つのサブフォルダと併せて配置されます。このチェックボックスで3つのフォルダ全ての場所をカスタマイズできます。

> 「Firebirdデータベースサーバーのインスタンスへ接続」を選択した場合、このオプション設定はメールのコンテンツと検索インデックスだけが保持される場所として設定されます。データベースの場所は、上記のデータベースパス/エイリアスで指定した場所となります。

ディレクトリ:
自動生成されるデフォルトのアーカイブストア用データベースフォルダは次の通りです。

..\SecurityGateway\Archive\$DOMAIN$\

パスの中の `$DOMAIN$` マクロはアーカイブストアと紐づいたドメイン名へ変換され、(ドメイン、ユーザー、データ等の)メタデータが含まれるFirebirdデータベース、ARCHIVE.FBDが格納されます。アーカイブデータはこのファイルなしでリストアする事ができません。フォルダにはアーカイブされたコンテンツとインデックスが格納されている..¥dataと..¥indexのサブフォルダも格納されています。

> クラスタリング[112]を使っていて、上記の「Firebirdデータベースサーバーのインスタンスへ接続」を選択していた場合、ここでの設定はデータベースファイルの場所ではなく、..¥dataと..¥indexの格納先としてのみ使用されます。データベースの場所は、上記のデータベースパス/エイリアスで指定した場所となります。また、ここで指定するディレクトリは、ネットワークでアクセスできる場所である必要があり、UNCファイルパスでの記述が必要です。
>
> 例: `\\share01\databases\Archive\$Domain$\`

上記の「異なるディレクトリを使用」を有効にした場合、次の場所を選択する事ができます:

データベースディレクトリ:
アーカイブデータベースファイルの場所を指定します。**注意点**: このオプションは、上記の*Firebirdデータベースサーバーのインスタンスへ接続*を選択していた場合は利用できません。この場合、データベースの場所は、上記のデータベースパス/エイリアスで指定した場所となります。

デフォルトのデータベースディレクトリの場所は次の通りです: `..\SecurityGateway\Archive\$DOMAIN$\`

コンテンツディレクトリ:
アーカイブストアのコンテンツが自動生成されるデフォルトロケーションは次の通りです

..\SecurityGateway\Archive\$DOMAIN$\data

パスの中の `$DOMAIN$` マクロはアーカイブストアと紐づいたドメイン名へ変換され、archive.sgd ファイルが格納された[..¥data」サブフォルダも生成されます。このファイルには圧縮形式のアーカイブデータが含まれています。アーカイブデータはこのファイルがないとリストアできません。

注意点: クラスタリング[112]を使っていて、上記の「Firebirdデータベースサーバーのインスタンスへ接続」を選択していた場合、ここで指定するディレクトリは、ネットワークでアクセスできる場所である必要があり、UNCファイルパスでの記述が必要です。(例. `\\share01\databases\Archive\$Domain$\data`)

インデックスディレクトリ:
アーカイブストアのインデックスが自動生成されるデフォルトロケーションは次の通りです

..\SecurityGateway\Archive\$DOMAIN$\index

パスの中の `$DOMAIN$` マクロはアーカイブストアと紐づいたドメイン名へ変換されます。サブフォルダ「..¥index」にはCLucene Full Text Indexingエンジンで生成されたフルテキストインデックスが含まれています。フルテキストインデックスは何らかの理由で徐々に破損していきます。フルテキストインデックスは、アーカイブストア[86]画面のメンテナンスオプションから再構築する事ができます。

注意点: クラスタリング[112]を使っていて、上記の「Firebirdデータベースサーバーのインスタンスへ接続」を選択していた場合、ここで指定するディレクトリは、ネットワークでアクセスできる場所である必要があり、UNCファイルパスでの記述が必要です。(例. `\\share01\databases\Archive\$Domain$\index`)

3.3.2 アーカイブストア

このページではアーカイブメールを格納するアーカイブストアの管理が行えます。各アーカイブストアは1つのドメインとのみ関連付けできます。複数のアーカイブストアを1つのドメインで使用する事もできますが、1つのみがアクティブとなります。この画面は設定[79]で自動アーカイブストア生成ではなく手動でアーカイブストアを作成するよう設定した場合の、アーカイブストア作成にも使用できます。

アーカイブストアページには1行毎に1つのエントリが一覧表示されており、様々なカラムが表示できますが、関連するボタンをクリックすることで、表示・非表示を切り替えられます。

ページの上部にあるツールバーには次のオプションがあります。

新規
新しいアーカイブストア画面を起動したり、手動でアーカイブストアを作成するにはこのボタンをクリックします。この画面はアーカイブストアを編集[87]画面と同じです。

編集
ツールバーの編集ボタンからアーカイブストアの編集[87]画面を起動できます。一覧で選択したアーカイブストアに紐づいた設定画面が表示されます。同様に、エントリをダブルクリックしても、同じ画面を開く事ができます。

削除
1つ以上のアーカイブストアを削除するには、一覧からエントリを選択し、削除をクリックします。確認用のメッセージが起動します。CtrlとShiftキーで複数エントリの選択も行えます。

メンテナンス

アーカイブストアが持つ（アーカイブ済メールの検索[90]で使用している）フルテキストインデックスを再構築するには、アーカイブストアを選択し、メンテナンスとフルテキストインデックスの再構築をクリックします。再構築処理が完了するまでアーカイブ検索が行えなくなるため、本当に再構築を行うかどうかの確認用ダイアログボックスが起動します。

ドメイン:
ドメイン: のドロップダウンを使用して、表示するアーカイブストアを選択できます。「--全て--」を選ぶと全てが表示されます。デフォルトでは、全てのアーカイブストアが表示されます。

3.3.2.1 アーカイブストアの編集

アーカイブストア[86]画面でアーカイブストアを選択し、編集ボタンをクリックすると設定用のダイアログが起動します。この画面は設定[79]で自動アーカイブストア生成ではなく手動でアーカイブストアを作成するよう設定した場合の、アーカイブストア作成にも使用できます。

アーカイブストア

このアーカイブストアへのクエリ（検索）を有効にする
アーカイブ済メールの検索[90]画面からアーカイブストアの検索を許可する場合はこのオプションを有効にします。無効にしていると、検索クエリはアーカイブストアからの検索結果に何の結果も返しません。このオプションはデフォルトで有効です。

このドメインに対する新しいメッセージをここへ保存する
このオプションは、対象のアーカイブストアがドメイン用にアクティブなアーカイブストアかどうか、つまり、新規にアーカイブされたメールの格納先アーカイブストアであるかどうかを確認します。ドメインは関連するアーカイブストアを複数保持する事ができますが、同時にアクティブなのは1つのみとなります。例えば、現在のアーカイブストアが容量の上限に到達し、新しいアーカイブストアを作成するものの、古いアーカイブストアはアーカイブストア一覧[86]へ検索用に残しておくとします。このオプションは新しくアーカイブするメールの格納先を確認します。ドメイン用のアーカイブストアとしてアクティブではないアーカイブストアをこの画面でアクティブにすると、アクティブアーカイブストアが存在するという理由で、他のドメイン用アーカイブストアはアクティブではなくなります。

ドメインのアーカイブストアの自動生成[83]を使用yしている場合で、ドメインのアーカイブストア用のこのオプションを無効としていた場合、SecurityGatewayは必要に応じて、ドメイン用のアーカイブストアを生成します。自動アーカイブ機能を使用せず、ドメインのアクティブアーカイブストアを無効化する場合はドメイン用のアーカイブが削除されます。

ドメイン
アーカイブストアと関連付けられたドメインです。1つのドメインのみがアーカイブストアとリンクできます。このオプションは新しいアーカイブストアを手動で作成したときのみ選択できます。既存のアーカイブストアに対し、ドメインの変更はできません。

名前
参照用にアーカイブへ名前を付けるにはこのオプションを使用します。

データベース

サーバー内部のFirebirdデータベースファイルを使用する
デフォルトで、SecurityGatewayはアーカイブ用に内部のFirebirdデータベースファイルを使用します。

Firebirdデータベースサーバーのインスタンスへ接続
外部のFirebirdデータベースサーバーへ接続しアーカイブを行う場合はこのオプションを選択します。クラスタリング 112を使用している場合もこのオプションを使用します。

SecurityGatewayのデータベースとして同じサーバーを使用
*「Firebirdデータベースサーバーのインスタンスへ接続」*を選択した場合のデフォルトオプションです。アーカイブ用に、SecurityGatewayはSecurityGatewayデータベースとして設定したFirebirdデータベースサーバへ接続し、同じ認証情報を使用します。追加で必要な情報は、(後述の)データベースパス/エイリアス名だけで、これはアーカイブストアを自動生成するデータベースファイルを指定するためのものです。

Firebirdデータベースサーバーのインスタンスへ接続
データベースの管理に、異なるFirebirdデータベースサーバーへ接続するにはこのオプションを選択します。サーバーアクセスのために、サーバー名かIP、ポート、ユーザー名、パスワードの情報が必要です。また、自動でアーカイブストアを作成する際のデータベースファイルのパス/エイリアス情報も必要です。

データベースパス/エイリアス名:
アーカイブストア用にデータベースファイルを自動生成するパスを入力します。**注意点:** このパスはFirebirdデータベースサーバーへの相対パスで、ネットワークパスである必要はありません。例えば、`C:\Databases\Archives\$DOMAIN$.fbd`のように記述します。

アーカイブ名のマクロ
アーカイブ用のファイル名に次のマクロが使用でき、自動生成の際、各アーカイブに固有の名称を使用する事ができます。

$DOMAIN$, $YEAR$, $MONTH$, $QUARTER$ 例えばデータベースパスとして"`C:\Databases\Archives\$DOMAIN$-$MONTH$.fbd`"を指定した場合、"`Example.com-September.fbd`"のような名前のデータベースが生成されます。Firebirdサーバーで自動生成されない、C:¥Databases¥Archives¥フォルダを作成しておくよう注意してください。

Firebirdサーバーはデータベース作成時、動的にフォルダ生成を行う事はありません。そのため、データベースパスへマクロを使用する場合は、最初にFirebirdサーバー上で、対象フォルダを手動で作成しておく必要があります。例えば、データベースパスが"c:

¥Databases¥Archives¥$Domain$¥archive.fbd"だった場合、"C:¥Databases¥Archives¥"フォルダへ各ドメイン用のサブフォルダを手動で作成する必要があります。このため、マクロの使用は、フォルダ名よりもファイル名で使用する事を推奨しています。

ストレージロケーション

データベース、メールコンテンツ、検索インデックスに異なるディレクトリを使用する
デフォルトで、アーカイブストアのデータは下記の「ディレクトリ」オプションで指定したフォルダへ、¥data¥と¥index¥の2つのサブフォルダと併せて配置されます。このチェックボックスで3つのフォルダ全ての場所をカスタマイズできます。

「Firebirdデータベースサーバーのインスタンスへ接続」を選択した場合、このオプション設定はメールのコンテンツと検索インデックスだけが保持される場所として設定されます。データベースの場所は、上記のデータベースパス/エイリアスで指定した場所となります。

ディレクトリ:
自動生成されるデフォルトのアーカイブストア用データベースフォルダは次の通りです。

..\SecurityGateway\Archive\$DOMAIN$\

パスの中の $DOMAIN$ マクロはアーカイブストアと紐づいたドメイン名へ変換され、(ドメイン、ユーザー、データ等の)メタデータが含まれるFirebirdデータベース、ARCHIVE.FBDが格納されます。アーカイブデータはこのファイルなしでリストアする事ができません。フォルダにはアーカイブされたコンテンツとインデックスが格納されている..¥dataと..¥indexのサブフォルダも格納されています。

クラスタリング[112]を使っていて、上記の「Firebirdデータベースサーバーのインスタンスへ接続」を選択していた場合、ここでの設定はデータベースファイルの場所ではなく、..¥dataと..¥indexの格納先としてのみ使用されます。データベースの場所は、上記のデータベースパス/エイリアスで指定した場所となります。また、ここで指定するディレクトリは、ネットワークでアクセスできる場所である必要があり、UNCファイルパスでの記述が必要です。

例: \\share01\databases\Archive\$Domain$\

上記の「異なるディレクトリを使用」を有効にした場合、次の場所を選択する事ができます:

データベースディレクトリ:
アーカイブデータベースファイルの場所を指定します。**注意点**: このオプションは、上記の*Firebirdデータベースサーバーのインスタンスへ接続*を選択していた場合は利用できません。この場合、データベースの場所は、上記のデータベースパス/エイリアスで指定した場所となります。

デフォルトのデータベースディレクトリの場所は次の通りです: ..\SecurityGateway\Archive\$DOMAIN$\

コンテンツディレクトリ:
アーカイブストアのコンテンツが自動生成されるデフォルトロケーションは次の通りです

..\SecurityGateway\Archive\$DOMAIN$\data

パスの中の $DOMAIN$ マクロはアーカイブストアと紐づいたドメイン名へ変換され、archive.sgd ファイルが格納された[..¥data」サブフォルダも生成されます。このファイルには圧縮形式のアーカイブデータが含まれています。アーカイブデータはこのファイルがないとリストアできません。

注意点：クラスタリング[112]を使っていて、上記の「Firebirdデータベースサーバーのインスタンスへ接続」を選択していた場合、ここで指定するディレクトリは、ネットワークでアクセスできる場所である必要があり、UNCファイルパスでの記述が必要です。（例. \\share01\databases\Archive\$Domain$\data）

インデックスディレクトリ:
アーカイブストアのインデックスが自動生成されるデフォルトロケーションは次の通りです

..\SecurityGateway\Archive\$DOMAIN$\index

パスの中の $DOMAIN$ マクロはアーカイブストアと紐づいたドメイン名へ変換されます。サブフォルダ「..¥index」にはCLucene Full Text Indexingエンジンで生成されたフルテキストインデックスが含まれています。フルテキストインデックスは何らかの理由で徐々に破損していきます。フルテキストインデックスは、アーカイブストア[86]画面のメンテナンスオプションから再構築する事ができます。

注意点：クラスタリング[112]を使っていて、上記の「Firebirdデータベースサーバーのインスタンスへ接続」を選択していた場合、ここで指定するディレクトリは、ネットワークでアクセスできる場所である必要があり、UNCファイルパスでの記述が必要です。（例. \\share01\databases\Archive\$Domain$\index）

3.3.3 アーカイブ済メールの検索

この画面からキューが有効な[87]アーカイブストア内のメールを検索できます。SecurityGatewayは検索パラメーターの設定に沿って全てのメールを検索します。画面上部のドメイン:オプションを使用し、全てのドメインか特定のドメインを指定できます。 また、詳細オプションで、件名、本文、日付範囲、添付ファイル、サイズ、その他の属性を使って検索対象の絞り込みが行えます。

この画面では、メールの検索結果の表示やダウンロード、メールボックスへ対象メールのリストアが行えます。

検索のポイント
検索では？と＊ のワイルドカードが使用できます。

テキストの一部と＊ を使用すると、テキストを含む全ての結果が表示されます。例えば、send* は send, sender, sendingを含む全てのメッセージを返します。*.example.comの場合は、例えば mail.example.com, sg.example.comといった、@ example.com アドレスやexample.comドメインを含むメールを返します。

クォーテーションを使うと、完全一致の検索を行います。例えば、"Frank Thomas"はFrank Thomas という結果のみを返します。クォーテーションを使わない場合は、Frank、Thomas, Frank Thomas, Tomas Frankを含むメールを返します。

単語の前にマイナスマーク("-")をつけると、単語を含むメールを除外します。例えば、-John Smithは Smithを含むメールから、Johnを含むメールを除いたものを結果として返します。

必要に応じてフルテキストインデックスの再構築が必要な場合は、アーカイブストア[86]のメンテナンスオプションを使用できます。

.

3.3.4 アーカイブコンプライアンス

この画面ではアーカイブメールの保存や特定のユーザーが送信(オプションで受信)したメールを削除するまでの期間をコントロールするのに使用でき、「訴訟ホールド」オプションで、SecurityGatewayで指定した権限に関わらず、一時的にアーカイブメールが削除するのを防ぐ事ができます。

データ保持

少なくとも、この期間のアーカイブメッセージを保存する
このオプションを有効にすると、アーカイブされたメールは、他の設定や権限によらず最低指定日数は削除されません。

これより古いアーカイブされたメッセージを自動的に削除する
このオプションを有効にすると、アーカイブメールは、後述の訴訟ホールド等が設定されていなければ、指定日数以降に自動削除されます。

アクティブなアーカイブストアからだけメッセージを削除する
デフォルトで、*…アーカイブされたメッセージを自動削除*オプションはアクティブなアーカイブストアにのみ適用されます。インアクティブなものも含め、アーカイブされた古いメール全てを削除する場合は、このオプションを無効にして下さい。

訴訟ホールド

訴訟ホールドを有効化
訴訟ホールドを有効にすると、ユーザー権限や保存期間といった他の全ての構成に関わらず、アーカイブからメールを削除することはできません。

除外連絡先

特定のメールアドレスから送信(又は受信)したアーカイブメールを削除するには次のオプションを使用します。

メールアドレス:
アーカイブメールを削除したいユーザーのメールアドレスを指定します。デフォルトで、除外連絡先はこのアドレスから送信されたアーカイブメールのみを削除します。このアドレス宛てのメールも削除したい場合には、下記の「…この連絡先に送信された全てのメッセージも削除する」オプションを有効にしてください。

....この連絡先に送信された全てのメッセージも削除する
このアドレスからのメールだけでなく、この連絡先へ送信された全てのメールも削除するにはこのチェックボックスを有効にします。

自分自身に確認を送信する
メールの削除後に通知を送信するにはこのオプションを使用します。メールは自分自身、アーカイブメールが削除されたユーザー、指定アドレスへ送る事ができます。

この連絡先から/連絡先への全てのメッセージを削除するには、ここをクリックします。
除外連絡先を設定後、このリンクをクリックしアーカイブメールを削除する事ができます。

3.3.5 エクスポート

ドメイン毎にアーカイブされた全てのメールをエクスポートし、ダウンロード用にzip形式で圧縮するにはこのオプションを使用します。zipファイルのダウンロードが行える状態になると通知メールが指定したメールアドレスへ送信されます。

アーカイブ済メールをエクスポートするには、ドメインを選択し、ダウンロードリンクを通知するメールアドレスを指定し、エクスポートをクリックします。

3.4 セキュアメッセージ

3.4.1 設定

SecurityGatewayのセキュアメッセージ機能を使うと、メッセージをSecurityGatewayへ残したまま、ドメイン外のユーザーに安全に送信する事ができるようになります。これはメッセージ用のウェブポータルを生成する事で実現しています。メールが送信されると、宛先ユーザーへセキュアメッセージの到着通知と、セキュアメッセージ宛先 93 アカウントを生成するためのリンクが届きます。このリンクへアクセスする事で、受信者はSecurityGatewayサーバー上のメールを確認できます。セキュアメッセージは、ブラウザ経由で、HTTPSを使った暗号化通信で管理されます。セキュアメッセージのご利用にあたっては、正規のSSL証明書 106 と、HTTPSの有効化 103 (参照: HTTPSサーバー 108) が必要です。

受信者はSecurityGatewayのポータルサイトからメールの確認や返信、オプションで、指定したユーザー一覧に対して新たにセキュアメッセージの作成 97 が行えます。 参照: セキュアメッセージの宛先アカウントに関する詳細は 宛先 93 と 受信者オプション 95 を参照して下さい。

セキュアメッセージの送信

メールを通常の配信ではなくセキュアメッセージシステムを使って配信するには、コンテンツフィルタ 207 又は 情報漏えい保護 197 で、セキュアウェブメッセージとして送信、の処理を使用するルールを作成します。例えば、"[Secure Message]"から始まる件名のメールをセキュアメッセージとして送信する、といったルールを作成します。また、Sieveスクリプトでも、次のSieve処理 236 を使って手動で同様のルールを作成できます : `vnd.mdaemon.securewebmsg`.

セキュアメッセージの有効化

このチェックを入れる事でセキュアメッセージを有効化します。

セキュアメッセージ受信者を自動的に作成する
デフォルトで、セキュアメッセージを送信すると、セキュアメッセージ宛先[93]アカウントが自動生成され、アカウント宛にメールを閲覧するためのリンクが送信されます。全ての受信者アカウントを手動で作成する場合はこのオプションを無効化してください。

このオプションを無効化した場合、セキュアメッセージを送信するのに、最初に宛先アカウントを宛先[93]ページで手動で作成する必要があります。セキュアメッセージの送信ルールやスクリプトで、宛先が不明と判断された場合、メールは送信者へエラーとして戻されます。

例外 - ドメイン

画面右上の"ドメイン:"ドロップダウンリストで特定のドメインを選択すると、設定を保存した後ドメインがここでの一覧に表示されます。「表示/編集」をクリックすると、セキュアメッセージの設定を確認したり編集したりできます。リセットボタンをクリックすると、ドメインの設定を、デフォルトの全体設定へ戻す事ができます。

3.4.2 宛先

このページへは自動[92]又は手動で作成されたセキュアメッセージの宛先アカウントのエントリが一覧表示されています。新しく宛先を手動で追加するには、ツールバーの新規のボタンをクリックします。有効のコラムにあるチェックボックスを有効・無効にする事で、アカウントを素早く有効化・無効化する事ができます。メールアドレス、名前、パスワードといった、アカウントの設定を表示・編集するには、アカウントをダブルクリックするか、選択して編集をクリックして下さい。アーカイブの編集や言語、ページ毎に表示するメールの数を編集するには、アカウントを選択し設定[94]をクリックします。宛先アカウントのメッセージログ[35]を表示するには、アカウントを選択し、メッセージをクリックしてください。

宛先アカウントの作成と編集

宛先アカウントを手動で作成するには、ツールバーの**新規**をクリックします。アカウントを編集するには、対象アカウントを選択し**編集**をクリックします。

プロパティ

このアカウントを利用禁止にする
宛先アカウントを無効にするにはこのチェックボックスをクリックします。

関連するローカルドメイン:
アカウントと関連するドメインを選択します。自動で作成された宛先アカウントは、セキュアメッセージの送信者ドメインが設定されます。受信者オプション[95]ページでドメインのドロップダウンリストを使い特定の設定を行っていた場合、宛先アカウントの設定には、全体オプションではなくドメインオプションが使用されます。また、セキュアウェブポータルでは、セキュアメッセージを表示する際、関連するドメインのブランドとカスタムイメージ[111]が使用されます。更に、ドメイン管理者は、自分が権限を持っているドメインに属した宛先アカウントのみを確認する事ができます。最後に、ユーザーが複数のドメインに属していて、セキュアメッセージを同じ宛先に送信した場合、宛先ユーザーはドメイン毎に、異なる宛先アカウントを割り当てあれる事になります。

メールアドレス
宛先アカウントのメールアドレスで、セキュアメッセージポータルへのログインに使用します。

リアルネーム
宛先アカウントの名前を指定するのに使用します。自動でアカウントが作成された場合は、送信されたセキュアメッセージのToヘッダの名前の情報を自動で使用します。

メールの受信者に、自身のパスワードを設定できる招待状を送信します
セキュアメッセージの宛先アカウントを生成する際、このオプションを選択すると、宛先アカウントヘドメインのウェブポータル用のリンクが通知され、宛先アカウントが自身のパスワードを設定できます。アカウントでこのオプションを使用した場合、以下の、「受信者へのパスワードを使用する」のオプションが自動で有効になります。このオプションに戻した場合、通知メールが再度送信されます。

アカウント設定に使用するPIN番号を指定する
このオプションをクリックし6桁のPIN番号を入力すると、宛先アカウントがパスワードを設定する際このPIN番号の入力が必要となります。

このPIN番号は宛先アカウントへの招待メールへは記載されません。宛先アカウントに対しては、電話などの別の手段で予めPIN番号を連絡しておく必要があります。

受信者へのパスワードを指定する
宛先アカウントによるパスワード入力を行わせるには、ここでの設定が必要です。新しいパスワードには最少8文字が必要で、次の少なくとも1つは必要となります:

- 大文字
- 小文字
- 数字
- 記号文字　例. ;,_.?/-=

設定

宛先アカウントを選択し、ツールバーの設定をクリックすると、次のオプションを編集できます。

オプション

このアカウント向けのメールはアーカイブしない
この宛先アカウントが送受信したメールをアーカイブから除外するにはこのオプションを使用します。

このアカウントの全てのアーカイブされたメールを削除する
この宛先アカウントのアーカイブを全て削除するにはこのリンクをクリックします。

言語:
システム通知で使用するデフォルトの言語を、ドロップダウンリストから選択します。宛先アカウントはセキュアメッセージポータルで自分の設定を上書きする事もできます。受信者オプション 95 ページから、デフォルト値を設定できます。

1ページに表示する項目数:
宛先アカウントがウェブポータルで表示するメールの数をここで指定します。宛先アカウントはセキュアメッセージポータルで自分の設定を上書きする事もできます。受信者オプション[95]ページから、デフォルト値を設定できます。

3.4.3 受信者オプション

このページではセキュアメッセージ宛先アカウントへ適用する様々なオプションやデフォルト値の設定が行えます。また、ウェブポータルでセキュアメッセージの宛先アカウントが行える設定についてもここで指定する事ができます。

後述の、パスワード紛失、パスワードを表示、端末ごとの保存を許可、のオプションは、セキュアメッセージポータルのログインページにて調整できます。ただし、これは宛先アカウントがポータルへ適切なURLでアクセスした場合です: <SG BASE URL>/SecurityGateway.dll?view=login_ex 例: "https://sg.company.test:4443/securitygateway.dll?view=login_ex" これは宛先アカウントへ設定用に生成されるURLです。セキュアメッセージの宛先アカウントとしてサインインすると、クッキーが設定され、ユーザーが SecurityGatewayのベースURL（例. "view=login_ex"を追加せずに接続）、ユーザーはセキュアメッセージポータルへリダイレクトされます。クッキーがない状態でユーザーがベースURLへアクセスすると、ログインは行えますが、ログインページのオプション要素は 設定 ≫ アカウント ≫ ユーザーオプション[60] の設定に準拠します。そのため、セキュアメッセージの宛先アカウントへ公開するURLには、必ず最後に正しく「/SecurityGateway.dll?view=login_ex」を付けて案内してください。

アクセスコントロール

受信者に自身のパスワードの変更を許可する
デフォルトで宛先アカウントはセキュアメッセージングのウェブポータルで自分のパスワードを変更する事ができます。ユーザーのパスワード変更を禁止する場合はこのオプションを無効化してください。

ログイン画面に「パスワード紛失」リンクを表示する
デフォルトで、"パスワード紛失"リンクはセキュアメッセージングのウェブポータルログインページに現れ、これを使ってパスワード変更用のリンクを送信できます。パスワード紛失リンクを表示しない場合は、このチェックボックスを解除します。

パスワード欄に"パスワードを表示"アイコンを表示する
それぞれのパスワード欄には目のアイコンが表示されており、これをクリックすると、入力したパスワードが表示されるようになります。ユーザーにパスワードを表示させ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。

受信者に2段階認証の有効化を許可する
2段階認証はパスワード認証に加え、モバイル端末等で生成されるコードを入力する事で、追加のセキュリティレイヤーとして使用できます。ユーザーが2段階認証を使えるように許可するにはこのオプションを有効化します。有効にすると、ユーザーがHTTPS接続で接続した際、2段階認証[27] ページ

がアカウントオプションの下に表示され、宛先アカウントが選択すれば、設定用のページへ進む事ができます。

ユーザに2段階認証の使用を必須とする
全てのユーザーにサインインの2段階認証を必須と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、最初にユーザーがサインインした際、2段階認証の設定ページが表示されます。

受信者に端末ごとの保存(HTTPSでの接続が必要)を許可する
このオプションを有効にすると、ユーザーがHTTPSで接続した際「デバイスで認証情報を記憶する」オプションがサインインページへ表示されます。ユーザーがボックスをチェックすると、サインアウトではなくブラウザを閉じて終了した場合、同じデバイスであればサインインが次回以降自動で行われます。サインアウトを行った場合は次回接続時に再度サインインが必要です。ユーザー情報は、下記の「記憶できる日数」で指定した日数保持されます。指定した日数以降、ユーザーは再度サインインが必要です。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:** 端末やブラウザで認証情報を記憶オプションを有効にしていると、セキュアメッセージで「*この端末/ブラウザでは認証情報を表示しない*」オプションが利用できるようになります。クリックすると、対象の端末では認証情報が記憶されません。

受信者が参照できる日数の指定(1日から365日)
ユーザーに端末ごとに記憶させることを許可する、のオプションを使っている場合、ここで再ログインまで何日間記憶するかを指定できます。デフォルトは30日間です。

サインインオプション

サインイン画面で「パスワードを紛失」リンクを表示
デフォルトで、サインインページには「パスワード紛失」リンクが表示されており、パスワード変更のためのリンクをここから送信できます。リンクはSecurityGatewayのユーザーアカウントに紐づけられたアドレス宛に送信されます。「パスワード紛失」リンクを表示しない場合にはこのオプションを無効にしてください。

サインイン画面に、次の管理者への連絡先情報を表示する
このオプションを有効にし、下のボックスへテキストを入力すると、サインインページで管理者の連絡先情報やリンクとして表示できるようになります。入力するテキストには、アンカーやイメージといったHTMLを使用する事ができます。

デフォルト

言語:
システム通知で使用するデフォルトの言語を、ドロップダウンリストから選択します。宛先アカウントを宛先 93 ページで選択し、設定をクリックすると、宛先アカウント毎のオプションへアクセスできます。宛先アカウントはセキュアメッセージポータルで自分の設定を上書きする事もできます。

サードパーティーサービスのセキュリティ侵害を受けたパスワードリストを使って、パスワードをチェックする
SecurityGatewayは、サードパーティーサービスから過去にセキュリティ侵害を受けたパスワードリストを参照し、ユーザーのパスワードが該当していないかをチェックすることができます。サービスにパスワードを送信することなく、このチェックを行なうことができます。ユーザーのパスワードがこのリストに該当しても、アカウントがハッキングされているわけではありません。以前に誰かが同じパスワードを使って攻撃を受けたことがあることを意味しています。表示されたパスワードは、ハッカーの辞書攻撃に使用さ

れる可能性があります。他で使われたことの無いユニークなパスワードは、より安全となります。詳しくは、Pwned Passwordsを参照してください。

ドロップダウンからパスワードが前回チェックされてからどの位の頻度でパスワードチェックを行うか指定します。次の中から選択できます:

- 行わない(パスワードのチェックは行われません。これはデフォルト設定です。)
- 最終確認からの日数
- 最終確認からの週
- 最終確認からの月

1ページに表示する項目数:
宛先アカウントがウェブポータルで表示するメールの数をここで指定します。各ページの下に1ページで表示できない多くのアイテムがある場合、別のページに移動するためのコントロールがあります。

利用規約

ログインする前に、以下の利用規約に同意する必要があります
このオプションを有効化し、ボックスへ利用規約などの文章を入力すると、ユーザーがセキュアメッセージポータルへログインする度に同意を求めるウィンドウが表示されます。ユーザーはチェックボックスをクリックし規約へ同意する事ができます。

新しい受信者

セキュアメッセージの受信者として作成された際、グローバル管理者に通知する
新規のセキュアメッセージ宛先アカウントが作成された際グローバル管理者 49へ通知を送るにはこのオプションを有効化します。

新しい受信者のパスワードを、サードパーティーのパスワードリストでチェックする
デフォルトで、新しい宛先アカウントのパスワードを、前述の「サードパーティーサービスのセキュリティ侵害…」のオプションを使ってチェックされます。チェックを行わない場合は、このオプションを無効化してください。

例外 - ドメイン

これらの設定を構成する時、ページ上部のドメイン:ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。セキュアメッセージの設定を編集するには、対応するドメインの**表示/編集**リンクをクリックする、あるいはデフォルトの全体の設定値をドメインの設定にリセットするには、**リセット**をクリックします。

3.4.4 メッセージ作成

これはドメイン用の設定で、ドメインに紐づいたセキュアメッセージの宛先アカウントが事前に定義したローカルユーザーに対して新たなメッセージを作成できるようにするのに使用します。宛先アカウントはセキュアメッセージポータルからメールを作成し、ドロップダウンリストから宛先を選択する事ができます。注意点: 宛先アカウントは受信したセキュアメッセージへの返信はいつでも行う事ができます。

新しいメッセージの作成

セキュアメッセージの受信者へ、特定のローカルユーザーに対しての新しいメッセージの作成を許可する
ドメイン: の一覧からドメインを選択し、このチェックを入れると、ドメインに紐づいた[93]宛先アカウントが新たにメッセージを作成できるようになります。また、アカウントは使用可能なメールアドレスで選択したローカルアカウントに対するメールを作成できるようになります。ドメインの宛先アカウントがメッセージを作成できないようにするには、このボックスを無効にして下さい。無効にすると、宛先アカウントは受信したセキュアメッセージへの返信のみが行えるようになります。

使用可能なメールアドレス:
選択したドメインのユーザーが一覧表示されています。アドレスを選択し右向きの矢印をクリックすると、選択したメールアドレスへ移動します。

選択したメールアドレス:
選択したドメインのセキュアメッセージ宛先アカウントがメールを送信できるローカルアドレスの一覧です。

3.5 免責事項(ヘッダ/フッタ)

このページでは、全てのメッセージ免責事項を管理します。メッセージ免責事項とは、インバウンド、アウトバウンドおよびローカルメールメッセージの上部や下部に動的に追加するテキストです。管理者は免責事項を編集[99]からプレーンテキストや標準HTML、カスタムSecurity Gatewayタグを使った使用免責事項テンプレートを作成できます。免責事項テンプレートは、メールのHTML本文およびテキスト本文に適用され、テンプレートは特定のドメインまたはドメイン全体に適用することができます。Sieveスクリプト[228]が免責事項毎に作成され、任意のトリガーでテンプレートへリンクします。さらに、Sieveスクリプトページから、直接これらのsieveスクリプトを作成できます。

メッセージ免責事項ページでは、行毎のエントリが一覧表示されていて、有効、説明、タイプ、受信、送信、ローカル、ドメイン、の7つのカラムで構成されています。各カラムの詳細や免責事項の作成や編集については、免責事項を編集[99]を参照してください。

ページ上部のツールバーには、次のオプションがあります。

新規:
新規メッセージ免責事項を作成する新規免責事項を開くには新規ボタンをクリックします。この画面は免責事項を編集画面と同じです。

編集:
現在、選択しているエントリの免責事項を編集[99]画面を開くには、ツールバーの編集ボタンを使用します。また、エントリをダブルクリックしても、この画面を開くことができます。

削除:
1つまたは複数の免責事項を削除するには、一覧からエントリを選択して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が現れます。複数のエントリを選択するためにCtrlとShiftキーを使用できます。

ドメイン:
どのドメインの免責事項を一覧に表示するか、ドロップダウンリストからドメインを選択します。全体を表示する場合は"--すべて--"を選択します。デフォルトでは、「すべて」が選択されます。

3.5.1 免責事項を編集

メッセージ免責事項 98ページで新規又は編集ボタンを使うと、メッセージ免責事項テンプレートの作成や編集が行えます。ドメインとの関連付け、種類(ヘッダ、フッタ、カスタム)、インバウンド、アウトバウンド、ローカルメッセージのどれで使用するかの設定が行えます。

この免責事項を無効にする
免責事項を無効にする場合は、このチェックボックスを選択します。この場合でもメッセージ免責事項 98一覧に表示されたままですが、メッセージには追加しません。このチェックボックスを選択すると、再び使用を開始します。

このドメイン用の免責事項:
この免責事項を、SecurityGatewayドメインに関連づけ、あるいはドメインすべてに関連づけするGlobalを指定するには、このドリップダウンリストから指定します。

説明

説明
免責事項の名前または説明を指定します。これは参照用でメッセージ免責事項一覧に現れます。

タイプ

このオプションは免責事項のタイプを指定します。タイプ: ヘッダ, フッタまたはカスタム

ヘッダ
メッセージの上部、メッセージの本文の上部にメッセージ免責事項を追加する場合は、**ヘッダ**を選択します。

フッタ
メッセージの下部、メッセージ本文の下部にメッセージ免責事項を追加する場合は、**フッタ**を選択します。

カスタム
下記で要点をまとめた特別なSecurityGatewayタグを使用してカスタム免責事項を作成する場合、カスタムを選択します。カスタム免責事項を使って、本文の上部や下部にテキストを追加することができます。"<sg:ORIGINAL_BODY>"タグは、すべてのカスタム免責事項で必要です。

ルール

このオプションは免責事項を追加するメッセージのタイプを指定します。

受信メールに免責事項を追加
先に選択するドメインに予定されるすべての受信メッセージに免責事項を追加する場合、このオプションを選択します。これをグローバルな免責事項に指定した場合、ドメインに関係なく受信メッセージすべてに追加されます。

送信メールに免責事項を追加
先に選択するドメインに予定されるすべての送信メッセージに免責事項を追加する場合、このオプションを選択します。これをグローバルな免責事項に指定した場合、ドメインに関係なく送信メッセージすべてに追加されます。

ローカルメールに免責事項を追加
先に選択するドメインでの送受信メッセージに免責事項を追加する場合、このオプションを選択します。例えば、frank@example.comからhmudd@example.com宛のメッセージは、追加される免責事項を持ちますが、frank@example.comからbiff@example.net宛のメッセージには追加されません。これをグローバルな免責事項として指定した場合、ドメインのローカルメールすべてに追加されます。

免責事項タイプをカスタムに指定した場合、プレーンテキストテンプレートは"<sg:ORIGINAL_BODY>"タグを含むことができ、テンプレート内のどこでもメッセージの本文を設定することができます。すべての他のタグまたはHTML文字は、コードとして処理された代わりのプレーンテキストとして現れます。

プレーンテキストでのフッタテンプレートの例:

```
-------------------------------------------
The views in this message are not necessarily
those of example.com or its affiliates.
-------------------------------------------
```

プレーンテキストでのカスタムテンプレートの例:

```
The following message was sent by an employee
of example.com.
--
<sg:ORIGINAL_BODY Field="body:all">{Original Email}
</sg:ORIGINAL_BODY>
-------------------------------------------
The views in this message are not necessarily
those of example.com or its affiliates.
-------------------------------------------
```

HTMLテンプレート

HTML免責事項テンプレートを作成する場合は、プレインテキストオプションを無効化してください。HTMLテンプレートにはHTMLコードと、以下の特別なSecurityGatewayタグのみを含む事ができます。

HTMLヘッダテンプレートの例:

```
<HTML><HEAD>
<style type="text/css">
```

```
.blueboldtext { font-family: Geneva, fixed-width; font-size: 13;
color: #114477; font-weight: bold; }
</style></HEAD>
<BODY>
<DIV>This is my header text!</DIV>
<sg:HTML_ONLY><span class="blueboldtext">Only show this text in the
HTML body!</span></sg:HTML_ONLY>
<sg:TEXT_ONLY>Only show this text in the Plain Text
body!</sg:TEXT_ONLY>
<BR>
-------------<br />
</BODY></HTML>
```

HTMLカスタムテンプレートの例:

```
<DIV> </DIV>
<DIV>This is my header text!</DIV>
<br />----------</DIV>
<sg:ORIGINAL_BODY Field="body:all">{Original Email}
</sg:ORIGINAL_BODY>
<br />----------</DIV>
<DIV>This is my footer text!</DIV>
<DIV> </DIV>
<DIV>This text will be in html and text body<br />
<sg:HTML_ONLY>Only show this text in HTML message!</sg:HTML_ONLY>
<sg:TEXT_ONLY>Only show this text in Plain Text
message!</sg:TEXT_ONLY></DIV>
```

免責事項テンプレートへHTML, HEAD、BODYタグを追加する必要はありません。これらを追加すると、タグは、各メールの関連するタグと統合されます。

SecurityGatewayタグ

免責事項テンプレートで使用することができる3つのカスタムSecurityGatewayタグがあります。テンプレートタイプに関係なく、3つのタグすべてはHTMLテンプレートで使用することができます。カスタムタイププレーンテキストテンプレートは、"<sg:ORIGINAL_BODY>"タグのみ使用することができます。

<sg:ORIGINAL_BODY></sg:ORIGINAL_BODY>
このタグは、テンプレートで、オリジナル本文が配置されるところを示します。免責事項をヘッダまたはフッタに指定する時、タグは自動的に適切な場所で設定されます。カスタムタイプ免責事項について、メッセージ本文で表示する、このタグを手動で設定する必要があります。カスタマイズしたSieveスクリプト 228について、どこでも設定することができますが、存在する必要があります。

このタグは、HTML免責事項テンプレートの任意のタイプで使用することができます:ヘッダ、フッタまたはカスタム。選択されるタイプに関係なく、どこでこのタグが指示しても、メッセージの本文は常に現れます。プレーンテキストテンプレートに関して、カスタムタイプ免責事項だけで使用することができます。

<sg:HTML_ONLY></sg:HTML_ONLY>
このタグ内で設定される文字は、メール本文のHTMLタグでのみ表示され、テキスト形式の場合は表示されません。このタグは、プレーンテキスト免責事項テンプレートで使用することができません。

<sg:TEXT_ONLY></sg:TEXT_ONLY>
このタグ内で設定される文字は、テキスト形式の本文でのみ表示され、HTML形式の場合は表示されません。このタグは、HTML免責事項テンプレートで使用することができません。

Sieveスクリプト

ユーザ定義、カスタマイズした免責事項を追加する場合、Sieveスクリプト 228エディタを使用します。免責事項を使用するための条件は、他のSieveスクリプトと同じです。Sieveエディタを使用する場合、テンプレートの一部の文字は¥文字を必要とします。
次のSieveフィルタは、ユーザ定義の免責事項のサンプルです:

```
require ["SecurityGateway","body"];

if allof(body :text :contains "Make money now!")
{
disclaimer "text:
<HTML xmlns:sg = \"http://www.altn.com/Products/SecurityGateway-
Email-Firewall/\">
<HEAD><META http-equiv=\"Content-Type\" content=\"text/html;
charset=UTF-8\" />
</HEAD>
<BODY>
<DIV>This is my header text!</DIV>
<DIV>Another line of header text!</DIV>
<DIV> </DIV>
<DIV>---------<br />
<sg:ORIGINAL_BODY Field=\"body:all\">{Original Email}
</sg:ORIGINAL_BODY>
<br />---------</DIV>
<DIV> </DIV>
<DIV>This is my footer text!</DIV>
<DIV>Another line of footer text!</DIV>
<DIV> </DIV>
<DIV>This text will be in html and text body<br />
<sg:HTML_ONLY>Only show the image and this text in HTML
message!</sg:HTML_ONLY>
<sg:TEXT_ONLY>Only show this text in Plain Text
message!</sg:TEXT_ONLY></DIV>
</BODY></HTML> ."
; }
```

3.6 システム

設定/ユーザメニューのシステムセクションには、次のシステム関連機能のリンクがあります。

暗号化 103
このページは、SecurityGatewayの各種の暗号化設定を構成するために使用します。SecurityGatewayはSTARTTLS SMTP拡張でSecure Sockets Layer (SSL)プロトコルのサポートがあり、他人がメールを傍受して読み取ることを防止します。さらにHTTPSサポートがありウェブインターフェース向けに同じ保護を提供します。

HTTPサーバ 108
HTTPサーバページは、SecurityGatewayのウェブインターフェースに関連した各種の設定を構成するために使用されます。HTTPおよびHTTPSポートおよび他のHTTP関連する設定でSecurityGatewayによって作成されるログインリンクで使用されるホスト名を指定することができます。

ブランディング/カスタムイメージ 111
現在、ログイン画面およびナビゲーションサイドバーに現れるバナーイメージをカスタマイズすることができます。

ディレクトリ 110
このページは、各種ファイル形式を管理するために使用するフォルダの一覧です。このページでパスを変更することにより、フォルダの位置を変更することができます。

ディスクの空き 111
ディスクの空きページは、空きディスク容量を監視する構成に使用します。ディスクの空き容量が少ない場合、管理者に警告メッセージを送信またはメッセージ受信を停止することができるオプションがあります

設定を表示 112
このページは、現在のSecurityGateway設定のすべてを表示します。SecurityGatewayサーバに関する問題の診断またはテクニカルサポートに情報を送る場合に使用します。このページは、XMLファイルに現在の構成を保存するオプションがあります。

3.6.1 暗号化

SecurityGatewayは、データを保護する最新暗号化技術を実装しています。 Transport Layer Security (TLS)としても知られるSecure Sockets Layer(SSL)プロトコルは、STARTTLS SMTP拡張で、メールを第3者による盗聴から保護する事ができます。SecurityGatewayのHTTPSはこれと同様の機能をウェブ上で実現します。

SSLプロトコル(Netscape Communications社開発)は、サーバ/クライアントインターネット通信を確保するための標準方式です。TCP/IP接続のためにサーバ認証、データの暗号化および任意のクライアント認証を提供します。さらに、SSLが現在の主要なブラウザに組み込まれるので、有効なデジタル証明書をサーバにインストールすると、SecurityGatewayに接続する時、接続しているブラウザのSSL機能を起動させます。メールクライアントを使用して接続する場合、SecurityGatewayはSSL/TLS上のSTARTTLS SMTP機能拡張をサポートします。しかしながら、最初、SSLを使用するために構成されるクライアントを持つ必要があり、機能拡張をサポートする必要があります－多くでサポートしていますが、すべてのメールクライアントがサポートするわけではありません。

メールとHTTPSの暗号化

SMTPとHTTPSにおいて、SSLとSTARTTLSサポートを有効にする
下記の証明書選択ボックスで「有効な」証明書を使用しSSL/TLSプロトコルおよびSTARTTLS拡張のサポートを有効にするには、このチェックボックスをクリックします。このオプションは、HTTPを使用しSecurityGatewayのウェブインターフェースにログインする場合、有効な証明書がアクティブである必要があります。このオプションはデフォルトで無効です。

使用可能な場合は常にSTARTTLSでメッセージを送信する
SecurityGatewayが送信するSMTPメッセージについてSTARTTLS拡張を使用することを試みる必要がある場合、このオプションをクリックします。SecurityGateway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に配信されます。このオプションはデフォルトで無効です。

SSLネゴシエーションが失敗した際、1時間だけSSLを使わずに再送信を行う
このオプションはSMTPセッション中にSSLエラーが発生した際対象ホストを一時的にホワイトリストへ追加します。ホワイトリストは毎時間リセットされます。

REQUIRETLS (RFC 8689)を有効化
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[207]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
- 宛先ドメインのMXレコードが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
- 上記の要件を満たしていないメールは送信されず、送信者へ戻されます。

Enable MTA-STA (RFC 8461)を有効化
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、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ます。

```
v=STSv1; id=20200206T010101;
```

"id"の値は、ポリシーファイルの編集を行った際、都度変更してください。一般的にidには、タイムスタンプを使用します。

TLS Reporting (RFC 8460)を有効化
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 163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。

証明書の選択

このボックスは、作成したすべてのSSL証明書を一覧にします。SecurityGatewayは、自動署名される証明書を生成し、証明書の発行人またはCertificate Authority（CA: 認証局）が証明書の所有者と同じである意味します。これは、完全に有効で、許可されますが、CAが信頼されたCAリストに示さないので、一部のユーザに、SecurityGatewayのHTTP URLに接続する時はいつでも、サイトに進み証明書をインストールする質問が表示されることがあります。証明書をインストールし有効なCAとしてSecurityGatewayドメインを信頼することに同意する場合には、今後、接続時のセキュリティ警告メッセージを確認する必要はありません。その手続きに完了する必要があるかどうか、使用しているブラウザ、どんなセキュリティ規制があるかなどに依存します。

SSL証明書の作成
新規の証明書を作成するためには、証明書選択ボックス上部ツールバーで**新規**をクリックし、SSL証明書 106を開きます。既存の証明書を削除するには、証明書を選択し**削除**をクリックします。

SSL証明書の使用
SSL証明書をアクティブにするには、エントリを選択して[**アクティブにする**]をクリックします。

STARTTLSホワイトリスト
ここではSTARTTLSから除外するIPアドレス、ホスト、ドメインを指定します。STARTTLSはここで登録したエントリ宛のメールでは使用されず、STARTTLSを対象ホストやIPアドレスへ要求する事もありません。

STARTTLS要求リスト
STARTTLS要求リストの中のホストやIPアドレスに対するSMTP接続へはSTARTTLSを使用する必要があります。STARTTLSが使用できない場合や失敗した場合、メールの送信は行えません。

SSL証明書
ここでは新しいSSL証明書を作成できます。証明書を作成するには、暗号化 103ページにある証明書の選択ツールバーで新規をクリックし、証明書の情報を入力します。終了したら、保存して閉じるをクリックし、新しい証明書を追加します。

証明書の作成

ホスト名
ユーザが接続するホスト名を入力します(例えば、"mail.example.com")。

団体/会社名
証明書を「所有する」団体または会社名を入力します。

代替えホスト名(複数指定はカンマ区切り)
SecurityGatewayは、各ドメインについて異なる証明書をサポートしません。すべてのドメインは、単一の証明書を共有する必要があります。ユーザが接続している代替えホスト名、および、この証明書を代替えホスト名にも適用する必要がある場合、カンマ区切りドメイン名を、ここに入力します。ワイルドカードが使用できます(例えば"*.example.com")。

暗号キーの長さ
この証明書で暗号化キーの必要なビット長を選択します。暗号キーは長くなるほど、データ転送がより安全です。ただし、すべてのアプリケーションが512より長いキーに対応しているわけではない点にご注意下さい。

国/地域
サーバが存在する国または地域を選択します。

サードパーティーCAで発行された証明書の使用
SecurityGateway以外で生成された証明書を購入した場合でも、Microsoft管理コンソールでSecurityGatewayが使用する証明書ストアへインポートする事により、この証明書を利用する事がで

きます。証明書がWindowsへインポートされると、SecurityGateway上でも表示され、使用できるようになります。証明書は次の方法でインポートできます:

1. Windowsツールバーで、**スタート ≫ ファイル名を指定して実行...** を選択し、**mmc /a** と入力します。
2. OKをクリックするか、Enterキーを押します。
3. Microsoft管理コンソールで、メニューバーから**ファイル ≫ スナップインの追加/削除...**をクリックします(又はCtrl+Mを押してください)
4. *スナップインの追加/削除*ダイアログで、証明書をクリックし、追加をクリックします。
5. *証明書のスナップイン* ダイアログで、コンピューターアカウントを選択し、次へをクリックします。
6. *コンピューターの選択* ダイアログで、ローカルコンピューターを選択し、完了をクリックします。
7. OKをクリックします。
9. 左側の*証明書(ローカルコンピュータ)*で、インポートする証明書が自己発行の証明書だった場合は、信頼するルート証明機関をクリックし、証明書をクリックします。自己発行でない場合は、パーソナルをクリックしてください。
10. メニューバーで **アクション ≫ 全てのタスク ≫ インポート...** を選択し、次へをクリックします。
11. インポートする証明書のパスを入力(または必要に応じてブラウズボタンを使い)し、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。

Let's Encryptを使った証明書の管理

SecurityGatewayで SSL/TLSとHTTPS 103 を使用するためには、 SSL/TLS証明書 106 が必要です。証明書は 認証局(CA) 106 で発行される小さなファイルで、サーバーへ接続するクライアントやブラウザから検証を行ったり、サーバーへの接続にSSL/TLS/HTTPSで安全な接続を行ったりするのに使用します。Let's Encrypt は手動での証明書作成、署名、検証、インストール、更新にかかる複雑な処理を自動化できる無償の証明書を発行している認証局です。

Let's Encryptで証明書の管理を自動化するため、SecurityGatewayでは"SecurityGateway\LetsEncrypt"フォルダへPowerShellスクリプトを用意しています。スクリプトへ依存する、ACMESharpモジュールにはPowerShell 3.0 が必要で、スクリプトはWindows2003では動作しません。さらに、SecurityGateway HTTPサービスはポート80番を使用する必要があり、HTTPチャレンジが完了しないとスクリプトが動作しません。使用する際にはスクリプトを実行する前にPowerShellの実行ポリシーを設定しておく必要があります。スクリプトを実行すると、http-01にチャレンジに必要なファイルをSecurityGateway HTTP(テンプレート)フォルダへ格納するといったLet's Encryptで必要な全ての処理が行われます。SecurityGatewayで設定されたFQDNは証明書用のデフォルトドメインとして、証明書の取得、Windowsへのインポート、SecurityGatewayのXMLRPC APIを使った証明書の設定で使用されます。

デフォルトドメインのFQDN設定がSecurityGatewayを指していない場合、このスクリプトは動作しません。証明書で関連するホスト名を設定する事もできます。関連するホスト名はコマンドラインで渡す必要があります。

使用例:

```
.\SGLetsEncrypt.ps1 -UserName admin@domain.com -Password Password1 -
AlternateHostNames mail.domain.com,imap.domain.com,wc.domain.com -
ErrorEmailTo admin@domain.com
```

AlternateHostNames の一覧へデフォルトドメインのFQDNを入れ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"だった場合、関連するホスト名として"imap.example.com"を指定したとします。スクリプトを実行すると、"imap.example.com" だけが関連するホスト名として認識されます。さらに、関連するホスト名は、それぞれがHTTPチャレンジをパスする必要が生じます。チャレンジが完了しないと、処理が完了しません。

関連するホストを使用しない場合は、コマンドラインへ -AlternateHostNames パラメータを使用する事ができません。エラー発生時にメール通知が送信されないようにするには、コマンドラインで -ErrorEmailToを使用しないでください。

3.6.2 HTTPサーバ

HTTPサーバページは、SecurityGatewayのウェブインターフェースに関連した各種の設定を構成するために使用します。SecurityGatewayで使用するログインリンクのホスト名、HTTPおよびHTTPポート、その他のHTTP関連設定を行う事ができます。

サーバ

ホスト名(ログインリンク作成で使用):
これは、ユーザおよび管理者に送信するメッセージでログインリンクを作成する時に、SecurityGatewayにより使用されるホスト名です。例えば、SecurityGatewayの接続で必要とするURLが、http://sg.example.com:...である時、このボックスにsg.example.comを入力します。これらのリンクでhttpsを使用する場合、"https"を含むURL全体を入力します(例えば、https://sg.example.com:4443)。

HTTPポート(カンマ区切り):
これは、SecurityGatewayのウェブインターフェースが使用するHTTPポートです。ウェブブラウザを通してSecurityGatewayに接続する場合、URLにはコロンの後にポート番号が必要になります(例えば、http://sg.example.com:4000)。複数のポートは、カンマで区切る必要があります。デフォルトポートは、4000です。

HTTPSポート(カンマ区切り):
これは、SecurityGatewayがウェブインターフェースにHTTPS接続のために監視するポートです。このポートに接続しているユーザは、SecurityGatewayのURLでhttpsを使用して、コロンの後にポート番号が必要です(例: https://sg.example.com:4443)。複数のポートは、カンマで区切る必要があります。デフォルトポートは、4443です。

これらのIPへソケットをバインドする(カンマ区切り):
SecurityGatewayで特定のIPアドレスに受信を制限する場合、カンマで区切って指定します。

HTTPリクエストに対するスレッド数:
これは、SecurityGatewayがHTTPリクエストのために使用するスレッドです。デフォルト値は5です。

HTTP接続をHTTPS接続へリダイレクトする
全てのHTTPリクエストをHTTPSへリダイレクト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対象ドメイン用に、正規のSSL/TLS証明書 106 をインストールしておく必要があります。

HTTPS要求に対して、HSTSヘッダを追加する
デフォルトでHTTPSレスポンスにはHTTP Strict Transport Security (HSTS)ヘッダが含まれています。HSTS対応のブラウザはHSTSヘッダを受取りSSL証明書が正規のものである事を確認し、その後、同じドメインに対するHTTPリクエストがあった場合にはこれを自動でHTTPSへアップグレードします。

有効期間 [XX] 秒
これはHSTSヘッダへ含まれる「`max-age=`」パラメータの値です。HSTSポリシーをブラウザが記憶する期間を指定します。デフォルト設定は63072000秒または2年間です。

...サブドメインも含める
ヘッダへ「`includeSubDomains`」ディレクティブを含みたい場合はこのオプションを有効にします。これはブラウザでウェブサイトのサブドメインにもポリシーを適用する場合に使用します。

...ドメインをHSTSプリロードリストに追加する
HSTSヘッダへ`preload`ディレクティブを追加するにはこのオプションを有効化します。

> よく知られている全てのブラウザに搭載されているHSTSプリロードリストへドメインを追加したい場合を除いて、`preload`オプションを使用するべきではありません。HSTSプリロードリストへドメインが追加されると、ブラウザは対象ドメインやサブドメインの接続に、必ずHTTPSを使用する必要が生じてしまい、サブドメインの正規の接続を妨げてしまう場合があるためです。また、一度ドメインがHSTSプリロードリストへ追加されると、リストから削除するのが困難になったり、長い時間がかかる場合もあります。
>
> HSTSプリロードリストの詳細については、次のサイトをご覧下さい:
> https://hstspreload.org/

設定

セッションのタイムアウトを有効にする
このオプションを有効にする場合、ユーザまたは管理者は、下記で指定する時間内に操作が全く無い時ウェブインターフェースから自動的にログアウトします。このオプションは、デフォルトで有効です。

ユーザをログアウトする時間 [xx] 分
ユーザまたは管理者がウェブインターフェースで無操作を許可する時間です。この時間を超える場合には自動的ログアウトします。このオプションのデフォルト設定は15分です。

3.6.3 DNSサーバー

設定

WindowsのDNSサーバーを使用する
このオプションを選択すると、SecurityGatewayはWindowsのTCP/IP設定で指定されている全てのDNSサーバーを使用します。ルックアップの処理毎に各DNSサーバーへ問合せを行い、正しい結果を最初に確認するか、全てのサーバーへ問合せを行うまで、この処理を継続します。

手動で設定したDNSサーバーを使用する
SecurityGatewayで特定のDNSサーバーを手動で指定する場合はこのオプションを選択します。DNSルックアップを行う際には、ここで指定した全てのDNSサーバーを使用します。正しい結果を最初に確認するか、全てのサーバーへ問合せを行うまで、この処理を継続します。

3.6.4 IPv6

SecurityGatewayはOSが対応しているIPv6と機能レベルとデュアルスタックが使用できる場合はこれを自動検出します。これ以外の場合は、SecurityGatewayが両方のネットワークをそれぞれ監視します。

設定

... IPv4接続だけを許可
IPv4接続だけを許可する場合はこのオプションを選択します。

...IPv6接続だけを許可
IPv6接続だけを許可する場合はこのオプションを選択します。

...IPv4かIPv6両方の接続を許可
IPv4とIPv6の両方を許可す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、SecurityGatewayは可能な場合IPv6接続を優先します。

可能な場合は送信用IPv6ホストへ接続
SecurityGatewayが可能な場合に送信用のIPv6ホストへ接続するようにするにはこのオプションを選択します。

3.6.5 ディレクトリ

このページへは、SecurityGatewayが各種ファイルタイプの管理対象となるフォルダが一覧表示されています。下記でパスを変更し保存ボタンをクリックすることで、フォルダの場所を変更できます。

設定

添付ファイル:
これは、SecurityGatewayサーバで処理するメールに付随した添付ファイルの保存先フォルダです。

このフォルダの内容は、SecurityGatewayの内部バックアップ[120]とリストア[121]ファイルには含まれません。添付ファイルをバックアップする場合、サードパーティのバックアップソフトウェアまたは別の方法にて行います。

バックアップ:
これは、バックアップ[120]ファイルが保存されるところです。最適なパフォーマンスを実現するために、当社では、このフォルダを別の物理ディスクドライブに設定することを推奨します。

ログ:
SecurityGatewayのログファイルは、ここに保存されます。

Inboundキュー:
これは、SecurityGatewayが受信メッセージ用のメッセージキューとして使用するフォルダです。

Temp:
これは、処理用に使用する一時的なフォルダです。

ベイジアン学習 非スパム:
ベイジアン学習[132]機能を使用する時、これは非スパムメッセージが置かれるフォルダです。

ベイジアン学習 スパム:
ベイジアン学習[132]機能を使用する時、これはスパムメッセージが置かれるフォルダです。

クラッシュメモリダンプファイル:
`SecurityGateway.exe` プロセスがクラッシュした際自動生成される、メモリダンプの保存先フォルダです。

3.6.6 ディスク空き容量

ディスク空き容量ページでは、SecurityGatewayでの空きディスク容量監視の設定が行えます。ディスク空きが少ない場合、管理者に警告メッセージを送信しメッセージ受信を停止するオプションがあります。

空きディスク容量のチェックエンジンを有効にする
このオプションが有効にする時、SecurityGatewayはディレクトリ[110]ページで参照されるすべてのボリュームで利用可能な空きディスク容量を監視します。このオプションはデフォルトで有効です。

空き容量が指定サイズ以下になった際グローバル管理者へ警告を送信する [xx] KB
このオプションを有効にすると、ディスクの空き容量が、指定された値(MB)以下になると、警告メッセージがグローバル管理者[49]に送信されます。デフォルト値は1000MBで、オプションはデフォルトで有効です。

指定サイズに以下になった時にSMTPエンジンを無効にする [xx] MB
このオプションで、ディスク容量が指定される値以下になると、SecurityGatewayでSMTPエンジンを無効にしメッセージを受け入れません。デフォルト値は100MBで、オプションはデフォルトで有効です。

3.6.7 ブランディング/カスタムイメージ

このページでは、ログインページで現れるバナーイメージとナビゲーションサイドバーで使用されるイメージのカスタマイズ用オプションを使用できます。

カスタマイズ

デフォルト イメージを使 用
SecurityGatewayのデフォルト イメージを使 用 する場 合 は、このオプションを選 択します。

カスタムイメージを使 用
カスタムイメージの指 定をする場 合 、このオプションを選 択します。

ログインページイメージ

このセクションでは、デフォルト イメージサイズおよびカスタムイメージをアップロード するオプションを提 供しま す。

ナビゲーションサイド バーイメージ

これは、SecurityGatewayにサインインするとき、ナビゲーションサイド バーの上 部 に表 示 されるイメーこのセクションでは、デフォルト イメージサイズとカスタムイメージをアップロード するオプションを提 供します。

例外 – ドメイン

これらの設 定を構 成 する時 、ページ上 部 のド メイン:ドロップダウンリスト ボックスで特 定 のドメインを選 択 する場 合 、そのドメインの設 定を保 存 後 に、この一 覧 にドメインが表 示 されます。ブランディング/カスタム イメージ設 定を見 直し編 集 するには、対 応 するドメインの**表 示 / 編 集** リンクをクリック、あるいはデフォル トの全 体 の設 定 値 をドメインの設 定 にリセット するには、**リセット** をクリックします。

3.6.8 設定を表示

ナビゲーションメニューで**設 定 / ユーザ≫システム**で**設 定 を表 示** をクリックすると、現 在 の SecurityGateway設 定すべてを表 示します。SecurityGatewayサーバに関する問 題 の診 断 またはテ クニカルサポート に情 報 を送 る場 合 に使 用します。このページは、現 在 の構 成 をXMLファイルで保 存 する オプションがあります。ツールバーで**ＸＭＬファイルをダウンロード** をクリックし、XMLファイルに現 在 の構 成 を 保 存 することができます。**ファイルのダウンロード** ボックスで**保 存** をクリックし、ファイル保 存 のロケーション を選 択 し**保 存** をクリックします。

3.6.9 クラスタリング

SecurityGatewayのクラスタリング機 能 は、ネット ワークにある2台 以 上 のSecurityGatewayサーバー 間 で設 定を共 有 する目 的 で開 発されました。これにより、複 数 のSecurityGatewayサーバー間 で、メ ールの処 理 に対 するソフト ウェア・ハード ウェアとしてのロード バランシングを行 い、処 理 速 度 の向 上 や効 率 化 を図 る事 ができるようになります。また、サーバーのハード ウェア、ソフト ウェアとしての冗 長 化 も行 え るため、メールシステムの可 用 性 を向 上 される事 ができます。

自 社 環 境 でSecurityGatewayクラスタを使 用 するかどうかを決 定 するためのポイント をご紹 介 します。

ノード

SecurityGatewayクラスタではプライマリノード とセカンダリノード を使 用 します。1台 の SecurityGatewayサーバーがプライマリとなり、それ以 外 のサーバーは全 てセカンダリとなります。

- クラスターの各 ノード のSecurityGatewayは同 一 バージョンである必 要 があります。
- クラスターの各 ノード ではそれぞれのSecurityGatewayレジストレーションキーを保 持 する必 要 があります。複 数 ノード 間 で同 じキーを使 用 する事 はできません。

- クラスタの各ノードは同一ネットワーク内に配置している必要があります。物理的に離れた場所にあるノード間でのクラスタリングシステムには対応していません。
- クラスタの全ノードは同じタイムゾーン、同じ時間である必要があります。システム時間のずれにより問題が発生する場合があります。
- クラスタ内の全てのノードで設定変更が行えます。設定変更があった場合は全てのノードへ変更が通知されます。ただし、注意が必要な点として、HELO ドメイン名 76 はサーバー毎の設定で、クラスタ内のノード毎に個々の値を使う必要があります。
- ベイジアンなどのメンテナンス処理はプライマリノードで行う必要があります。

ルーティング

SecurityGatewayは特定のノードからのトラフィックのルーティング処理は行いません。第3者の提供するロードバランサーでトラフィックのルーティングを行う事をお勧めします。

ロードバランサーのスティッキーセッションは同一IPからの通信を同じホストへルーティングするのに必要です。スティッキーセッションはSecurityGatewayのウェブ管理画面へサインインするのに大変重要で、誰かがサーバーの中の1つへサインインすると、全てのセッションが同じサーバーに対しルーティングするようになります。

共有データベースとフォルダの格納先

SecurityGatewayクラスタでは、全てのサーバーが同じデータベースと特定のフォルダのセットを共有します。そのため、全てのノードは同じネットワークにいて、共有フォルダは全てのノードからアクセスできる必要があります。SecurityGatewayサービスは、デフォルトではローカルシステムアカウントとして稼働するため、サービス設定 117 でネットワークの場所へアクセス権を持つユーザーでサービスを実行するよう設定変更が必要となります。メールボックス、パブリックフォルダ、その他のフォルダはクラスタの各ノードがアクセスできる共有フォルダへ配置する必要があります。UNCパスを使う場合は、ネットワークロケーションへアクセス権を持つユーザーでMDaemonサービスを実行する必要がある点に注意してください。下記を参照してください: "SecurityGatewayがネットワークからアクセスできるデータフォルダを利用するための設定 114 "

アーカイブ

クラスタリングで アーカイブ 79 を使用するには、アーカイブ設定でネットワークパスを使ったFirebirdデータベースサーバーを使用するよう指定する必要があり、そうする事で全てのノードがアーカイブストアに接続できます。

証明書

- (証明書を含む)HTTPS設定はノード毎であり、クラスターへ追加したノード全てに設定する必要があります。証明書はデータベースではなく、各ノードへ格納されます。そのため、各ノードで同じ証明書を使用するには、証明書を各ノードへ手動でインポートし、それぞれのSecurityGatewayで証明書を使用するよう設定が必要です。
- STARTTLSホワイトリストとSTARTTLS要求リスト 103 設定は共有されます。
- SecurityGatewayのLetsEncryptオプションは現時点でセカンダリノードへは対応していません。

クラスタリングの設定

データベースのアップグレード

クラスタリングを使用するため、SecurityGatewayを従来バージョンから7.0以降のバージョンへアップデートした場合、同梱されているSGDBTool.exeを、SecurityGatewayデータベースファイルをFirebird 2.xからFirebird 3.xへの変換用に使用する必要があります。SecurityGateway 7.0以降を新規にインストールする場合、既にFirebird 3.x データベースは使用しているため、この手順はスキップできます。

データベースのアップグレードは次の手順で行います:

1. SecurityGatewayサービスを停止します。(SecurityGatewayスタートメニューから**SecurityGatewayを停止**を選択するか、サービスコンソールを使用します。)
2. Windowsの**コマンドプロンプト**を起動します。
3. \SecurityGateway\app\フォルダへ移動します。
4. **sgdbtool.exe -convertfb3** と入力し、**Enter**を押します。

この手順でFirebird 2.xデータベースファイルのバックアップコピーが"SecurityGateway.fb2"として保存されます。その後、Firebird 3.x runtimeを使ってリストアされたデータベースは"SECURITYGATEWAY.FBD"として保存されます。アーカイブ[79]を使用している場合、この手順は全てのアーカイブデータベースをアップグレードします。

ネットワークからアクセスできるデータフォルダを使用するためのSecurityGatewayの設定

SecurityGatewayクラスターの全てのノードは同じデータベースと複数フォルダのセットを共有します。そのため、全てのノードは同じネットワークに配置する必要があり、各ノードのWindowsサービス[117]で共有フォルダへアクセス権のあるアカウントを設定しておく必要があります。共有フォルダの内容を全てのノード間で共有するため新しい場所へコピーするには、手動で行う必要があります。SecurityGatewayは既存のファイルの移行は行いません。次の共有フォルダはディレクトリ[110]ページと(クラスタリングで唯一設定されるベイジアンレプリケーションを除く)クラスタリングページの両方から設定されます。

- **Message Data** (例. \\Share01\SecurityGateway\Messages\)
- **Message Logs/SMTP Transcripts** (例 \\Share01\SecurityGateway\Transcripts\)
- **Attachments** (例. \\Share01\SecurityGateway\Attachments\)
- **Bayesian Learning Non-spam** (例. \\Share01\SecurityGateway\BayesHam\)
- **Bayesian Learning Spam** (例. \\Share01\SecurityGateway\BayesSpam\)
- **Bayesian Replication** (例. \\Share01\SecurityGateway\BayesReplication)
  注意点: フォルダはクラスタリング内で重複できません。プライマリノードがベイジアンデータベースや他のノードでコピーされたデータの場所になります。

注意点: データベースの場所と認証情報はインストール中か、SGDBTool.exeを使用して設定します。(後述の"外部データベースサーバーを使用するようSecurityGatewayを設定[115]"を参照してください。)

アーカイブストア

If you are using the アーカイブ[79]を使用している場合はネットワークからアクセスできる場所へアーカイブストアを再配置し各アーカイブデータベースをFirebirdデータベースサーバーへ移動する必要があります。下記のクラスターでアーカイブを使用[116]を参照してください。

Firebird 3データベースサーバーの設定

クラスターを使用するためには、クラスター内の各ノードがネットワークからアクセスできる場所にFirebird 3データベースサーバーをインストールする必要があります。

Firebird 3 サーバーは次のように使用します:

1. Firebird 3 Database Serverをダウンロードします。
2. 全てのノードからアクセスできる端末でインストーラーを実行します。
3. License Agreementで承認を押し、**次へ**をクリックします。
4. 情報を読み、**次へ**をクリックします。
5. フォルダを選択し、**次へ**をクリックします。
6. コンポネントの選択で、**次へ**をクリックします。
7. スタートメニューフォルダを選択し(または**スタートメニューフォルダを作成しない**クリックし)、**次へ**をクリックします。
8. 追加タスクを選択をデフォルト値(例. SuperServerモード、サービスとして実行、クライアントライブラリをコピー)へ設定し、**次へ**をクリックします。
9. SYSDBAパスワード(″SYSDBA″ユーザー名でパスワードは後に必要)を入力し、**次へ**をクリックします。
10. **インストール**をクリックします。
11. **次へ**をクリックします。
12. **終了**をクリックします。

外部のデータベースサーバーを使用するためのSecurity Gateway設定

SecurityGatewayクラスタで、各ノードは前述のセクションで設定したFirebird 3 データベースサーバーを使った、同じデータベースへ接続するよう設定する必要があります。SecurityGatewayで外部データベースサーバーを使用するよう設定するには:

1. Firebirdサーバー上でデータベース用フォルダ(例 C:¥Databases)を作成します。
2. プライマリSecurityGateway データベースファイル(例. \SecurityGateway\App\SECURITYGATEWAY.FBD)を作成したフォルダへ移動します。
3. SecurityGatewayサーバーで、Windowsのコマンドプロンプトを起動します。
4. \SecurityGateway\app\フォルダへ移動します。
5. **sgdbtool.exe -setdbconnect**, と入力し、**Enter**を押します。
6. ″組み込みFirebirdデータベースを使用しますか Y/N?″ でNを押し、Enterを押します。
7. ″Firebirdサーバー IPを入力″でFirebirdサーバーのIPアドレス(例. 10.10.0.1)を入力し、**Enter**を押します。

8. "Firebirdサーバーポート（デフォルトは 3050）"で**Enter**を押します。
9. "Firebirdデータベースパスかエイリアス"でデータベースサーバーをコピーしたFirebirdサーバー（例．C:\Databases\SECURITYGATEWAY.FBD）のフルパスを入力し、**Enter**を押します。
10. "Firebirdデータベースン¥ユーザー名（デフォルトはSYSDBA）を入力"で**Enter**を押します。
11. "Firebirdデータベースパスワード（デフォルトはmasterkey）を入力"でFirebird 3 サーバーを作成した際のパスワードを入力し、**Enter**を押します。

プライマリSecurityGatewayノードが外部のデータベースサーバーへ接続できるようになります。

クラスタリングでのアーカイブ利用

クラスタリングで アーカイブ[79] を使用するには:

1. Firebirdサーバーのアーカイブデータベースファイル（例．"c:¥databases¥Archives¥Example.com," "..¥Archives¥company.com," 等）を作成します。
2. 各アーカイブストアのストレージロケーション[89]としてアクセスできるネットワークフォルダを作成します。
3. アーカイブストアの編集[89] にあるストレージローケーションで、新しいロケーションをUNCパスで指定します。
4. 各アーカイブストアを *Firebirdデータベースサーバーインスタンスへ接続* と設定し、各データベースファイルを *データベースパス/エイリアス名* で入力します。
5. アーカイブストアの自動生成[83] 設定を必要に応じて編集し、UNCパスとクラスタリングに対応したマクロの編集を行います。

クラスターへのノードの追加

新しい SecurityGatewayインストールをクラスタへ追加するには:

1. SecurityGatewayインストーラーを新しいノードとして使用する端末上で実行します。
2. インストール中に、"外部データベースサーバーへ接続"を選択し、前述のセクションで入力した情報を使用します。
3. インストール処理を通常通り行います。
4. Windowsサービス[117] セクションで認証情報と共有データフォルダへ接続するためのUNCファイルパスが正しいかどうかを確認します。
5. 新しい端末へ必要なSSL証明書をコピーします。

アクティブ/ アクティブデータベースレプリケーション

アクティブ/アクティブでのデータベースレプリケーションを使用するには、SecurityGatewayは対応しているものの、サードパーティーのレプリケーション製品を使用する必要があり、設定方法はこのヘルプの範囲外です。クラスタでアクティブ/アクティブでのデータベースレプリケーションを行う要件や手順については、次のPDF文書を参照してください。: SecurityGateway: アクティブ-アクティブデータベースレプリケーションの設定

3.6.10 Windowsサービス

デフォルトでSecurity Gateway Windowsサービスはローカルシステムアカウントで稼働します。しかし、このアカウントはネットワークドライブへアクセスする権限を持っていません。このため、例えばClustering[112]といった別のアカウントでサービスを実行し、このページのアカウント設定や権限設定を行う必要があります。

ローカルシステムアカウント
デフォルトでSecurity Gateway Windowsサービスはローカルシステムアカウントで実行されます。

このアカウント
サービスを異なるアカウントで実行するには、アカウントのログオン名とパスワード、ドメインを入力します。

3.7 データベース

設定/*ユーザー*メニューのデータベースセクションへは、次の4つのページへのリンクが掲載されており、Security Gatewayで保存するデータの種類や容量の設定、Security Gatewayデータベースのバックアップやリストアが行えます。

設定[120]– このページではデータベースの書き込みモードとして、データをディスクへ同期書き込みするか、非同期書き込みするかを指定します。

データ保持[118]– このページでは、Security Gatewayがメッセージデータベースレコード、メッセージ本文、各メッセージのSMTPセッションログをどの位の期間保持するかを指定します。同様に、メール本文が保持または削除される条件をここで指定できます。データベースメンテナンスは毎日深夜に実行され、このページで使用する値は、全て日数で指定します。

バックアップ[120]– バックアップページではSecurity Gatewayデータベースを自動でバックアップするスケジュールを指定します。バックアップ対象として、データベース全体なのか、設定のみなのかを選択できます。古いバックアップを保持する最大数もここで指定します。

復元[121]– 復元ページへはバックアップページでシステム用に保存された設定に沿って作成された、設定とデータベースバックアップが一覧表示されています。このページからファイルをダウンロードし、設定やデータベース全体を復元する事ができます。

3.7.1 設定

このページではデータベースの書き込みを、同期実行するか、非同期実行するか選択できます。

データベース書き込みモード

データは同期に書き込まれます。
このオプションを選択すると、データはすぐにディスクへ書き込まれます。データベース書き込み処理はデータが物理的にディスクへ書き込まれるまで完了しません。これはデフォルト設定で最も安全な方法です。

データは非同期に書き込まれます。
このオプションを選択すると、オペレーティングシステムがデータを物理的に書き込むタイミングをコントロールします。このオプションで高いパフォーマンスを期待できますが、停電やその他予期しないシステムやデータベースの停止により、データベースが破損する危険性があります。非同期での書き込みコードは同期での書き込みモードでパフォーマンスが低い場合にのみ推奨します。システム用の安定した電力供給（UPS）やデータベースのバックアップを併用するようにして下さい。

3.7.2 データ保持


SecurityGatewayでメッセージデータベースレコード、メッセージ内容および各メッセージのSMTPセッション写しの保管期間構成するために、このページを使用します。同様に、メッセージ内容がどんな状況のもとに保持または削除するか指定することができます。データベースメンテナンスは各真夜に行われ、このページの値すべて日数です。

メッセージデータベースレコード

下記でメッセージデータベースレコードを保持する期間を指定します。レポートは、この時間枠に限定されます。期間の長い時間枠は、巨大なデータベースとなります。

何もしない
メッセージデータベースレコードを削除しない場合、このオプションを選択します。

指定日数以前を削除する: [xx] 日
真夜中に各夜古いデータベースレコードを削除する場合、このオプションを選択し、各レコードを保持する日数を指定します。これはデフォルトオプションで、レコードを30日保持します。

メッセージ内容

デフォルトで、これ以降必要でない場合、例えば、メッセージが受信者に正常に配信される、メッセージが隔離から削除されるような時、各メールメッセージ内容は廃棄されます。ただし、メールメッセージ内容の保存はデバッグ目的で有効です、各種の状況のもとにメッセージ内容の自動削除を禁止する下記で提供されるオプションがあります。これらの全オプションは、デフォルトで無効です。


このオプションを有効化すると、パフォーマンスの低下やデータベースの肥大化を招きますのでご注意下さい。

正常な配信後メッセージ内容を削除しない
メッセージが正常に受信者のサーバに配信された後でも、メッセージ内容を保持する場合、このオプションを有効にします。

隔離から削除時にメッセージ内容を削除しない
隔離から削除された後で隔離されたメッセージ内容を削除しない場合、このオプションを有効にします。

メッセージが拒否された場合にメッセージの内容を削除しない
このオプションを有効にすると、メッセージを受信した後に拒否される場合であっても、SecurityGatewayはメッセージ内容を削除しません。

完全な配信失敗後にメッセージの内容を削除しない
受信者が無効のような永久的な配信失敗に遭遇するメッセージを保持する場合、このオプションを有効にします。

不完全なメッセージのメッセージ内容を削除しない
不完全なメッセージ内容を削除しない場合、このオプションを有効にします。

メッセージの写し

SMTPセッションおよびSIEVEルールエンジンの総合的なログはメッセージごとに維持されます。これらメッセージの写しは、トラブルシューティングおよびデバッギングの手助けとなります。ただし、データベースのサイズを増やします。

メッセージデータベースレコードで処理する(前の設定)
これはデフォルトオプションです。選択される場合、メッセージの写しは上記のメッセージデータベースレコードセクションで選択されるオプションに従って処理されます。古いメッセージデータベースレコードが削除される時に、セッション写しは同様に削除されます。

指定日数後にメッセージの写しを削除 [xx]日
特定の日数でメッセージの写しを保持する場合、このオプションを有効にし、保持する日数を指定します。

メッセージの写しを保持しない
メッセージの写しを保存しない場合、このオプションを選択します。

帯域の情報

指定日数後に帯域幅の情報を削除する[xx]日
このオプションを有効にし、各夜真夜中に、古い帯域幅使用情報を削除する場合、日数を指定します。

3.7.3 バックアップ

SecurityGatewayデータベースの自動バックアップをスケジュールに入れるために、バックアップページを使用します。全データベースまたは構成と設定のバックアップをスケジュールに入れることができます。同様に、保存する古いバックアップファイル数を指定することができます。同様に、保存する古いバックアップファイルの数を指定することができます。バックアップファイルは、復元 121ページで一覧にされます。

最適なパフォーマンスのために、バックアップフォルダ(ディレクトリ 110ページで指定)を、別の物理ディスクドライブに置くことをお勧めします。さらに、SecurityGatewayサービスが実行中、SecurityGatewayのデータベースファイルをサードパーティのバックアップソフトウェアまたは他の外部バックアップ手段を使用することは推奨しません。サービスが実行中、このページで提供される内部オプションは、定期的にデータベースのバックアップを取るための使用することができます。一部の外部バックアップ手続きを使用する場合、最初にサービスを中止するか、または単にSecurityGatewayによって内部的に作成されるバックアップファイルのバックアップを行うために、その外部手続きを使用します。最後に、SecurityGatewayの内部バックアップオプションは、添付ファイル 110のコンテンツのバックアップを取りません。添付ファイルのバックアップを取る場合、サードパーティのバックアップソフトウェアまたは他の外部の方法を使用してください。

自動バックアップ

自動バックアップを実行しない
これはデフォルトオプションです。選択時には自動的にデータベースまたはサーバ構成のバックアップ行いません。

指定日数ごとに指定時間で設定をバックアップする [xx]日 時間 [xx:xx]
SecurityGatewayの構成の書き出し/バックアップを取る場合、このオプションを選択します。しかし、全データベースのバックアップを取りません。自動書き出しから次に実行する日数と時刻を指定します。これらのファイルは復元 121ページで一覧にされ、"Export"から始まるファイル名を持ちます。

このバックアップ方法を使用時、SecurityGatewayの構成および設定のみバックアップされます。全データベースでなく、ユーザおよびドメイン情報を持ちます。従って、この種類のバックアップファイルからシステムを復元する場合、すべてのメッセージ、セッションの写し、レポート、メッセージログ、その他は失います。構成および設定のみ復元されます。

指定日数ごとに指定時間でデータベース全体をバックアップする [xx]日 時間 [xx:xx]
構成および設定、メッセージログ 249、レポート 262、写し、その他を含むSecurityGatewayの全データベースのバックアップを取る場合、このオプションを選択します。自動書き出しから次に実行する日数と時刻を指定します。これらのファイルは復元 121ページで一覧にされ、"Backup"から始まるファイル名を持ちます。

添付ファイル[110]フォルダのコンテンツは、バックアップファイルに含まれません。添付ファイルのバックアップを取る場合、サードパーティのバックアップソフトウェアまたは他の外部バックアップ手続きを使用します。さらに、全データベースをバックアップする時メッセージログ[256]は含まれますが、ログファイルは含まれません。ログファイル[257]のバックアップを取る場合、同様にサードパーティのバックアップソフトウェアまたは他の外部バックアップ手続きを使用します。

指定ファイル数をバックアップ: [xx]ファイルのみ(古いバックアップファイルは削除されます)
バックアップファイルの一定数だけを保存する場合は、このチェックボックスを選択し、ファイルの数を指定します。ファイルの最大数が到達すると、新規のバックアップファイルが作成される時には、最も古いファイルは削除されます。このオプションはデフォルトで無効です。

手動バックアップ

設定データをバックアップ/エクスポートするには、ここをクリックします。
手動でSecurity Gatewayの構成を書き出しは、このリンクをクリックします。このバックアップ方法は、**指定日数ごとに指定時間で設定をバックアップする**と機能は同じです。自動でなく手動で開始し、併せてスケジュールをしている自動バックアップがあります。

データベース全体をバックアップするには、ここをクリックします。
データベース全体をバックアップするには、ここをクリックします。手動でSecurity Gatewayの全体のデータベースをバックアップするには、このリンクをクリックします。このバックアップ方法は、上記の**指定日数ごとに指定時間で設定をバックアップする**オプションで機能的に全く同じです。自動でなく手動で開始し、併せてスケジュールをしている自動バックアップがあります。

3.7.4 復元

復元ページは、システム上で現在保存されるバックアップ[120]ページを使用して作成される構成およびデータベースバックアップファイル全部の一覧を示します。このページから、ファイルをダウンロード、削除、さらに構成または全データベースを復活させることができます。

バックアップファイルのアップロード

以前にダウンロードされたバックアップファイルをアップロードし、下記の復元リストに追加するために、参照とアップロードオプションを使用します。構成または全てのデータベースを復元するために、アップロードしたファイルを使用することができます。

参照
下記の復元リストにアップロードするデータベースまたは構成ファイルを参照するには、このボタンをクリックします。上記のファイルは以前に、このページからダウンロードされ、バックアップ[120]ページでオプションを使用し作成されました。

バックアップファイルをアップロードする
ファイルの場所を指定するために**参照**ボタンを使用した後に、ファイルを下記の**復元リスト**にアップロードするために、このボタンをクリックします。

復元

このリストは、バックアップ[120]ページから作成、または上記の**バックアップファイルのアップロード**オプションを使用してアップロードされるすべてのファイルがあります。各エントリは、ファイル名バックアップファイルが作成された日付および時間、サイズ、ダウンロード、ファイルの復元リンクがあります。"Export"から始まるファイル名は、設定データのみを含んでいるファイルです。"Backup"から始まるファイルは、全体のデータベースのバックアップファイルです。

各タイプのバックアップファイルに含まれる詳細については、バックアップ[120]ページを参照してください。

ダウンロード
ファイルをダウンロードするために、バックアップファイルのエントリで**ダウンロードリンク**をクリックします。ファイルは、再び、後で上記のバックアップファイルを、アップロードオプションを使用して復元リストにアップロードすることができます。ファイルのダウンロードは、リストから削除しません。

削除
バックアップファイルを削除するために、このリンクを使用します。SecurityGatewayからファイルを取り除くが、他の場所に保存する場合、ファイルを削除する前に、上記の**ダウンロード**オプションを使用します。

復元
対応するファイルからSecurityGatewayの構成または全体のデータベースを復元するために、このリンクをクリックします。そのバックアップファイルが作成された以降の変更は失います。復元が終了するまで、SecurityGatewayは利用できません。完了後、同様に再びログインしなければなりません。処理の確認が現れます。

3.7.5 詳細

テクニカルサポートに指示された時だけ、このページでデータベースへSQLステートメントを発行して下さい。実行する前に、データベースのバックアップ[120]を取得する事をお勧めします。

SQLステートメントを実行

SQLステートメント:
テクニカルサポートに指示された時には、ここへSQLステートメントを入力し、「実行」をクリックします。アクションに対する結果が、結果の下に表示されます。

3.8 ソフトウェア更新

このページではSecurityGatewayの更新バージョンの有無を確認する事ができます。最新バージョンの確認は、手動で行う事も、SecurityGatewayで自動で行うよう設定することもできます。最新版が利用できる状態の場合、ウェブインターフェースから直接ダウンロードし、インストールすることができます。

設定

定期的にソフトウェアのアップデートを確認する
自動的に真夜中に毎日ソフトウェアアップデートのチェックする場合、このチェックボックスを選択します。

すぐにソフトウェアアップデートを確認するには、ここをクリックしてください

ソフトウェアアップデートを手動でチェックするには、このリンクをクリックします。チェックの結果は、下記に更新ボックスに現れます。

更新

このボックスは、アップデートがチェックするソフトウェアの結果を含んでいます。ソフトウェアアップデートが利用可能な場合、全グローバル管理者[49]に通知と、ソフトウェアアップデート詳細ページのリンクが送付されます。ソフトウェアアップデートの詳細ページからjは、ダウンロードとインストールをすることができます。

ソフトウェア更新の詳細

アップデートチェックがソフトウェアアップデートが利用可能であることを示すときに、ソフトウェアアップデート詳細ページに対するリンクはダッシュボード[9]上、ソフトウェアアップデートページのアップデートセクションで提供されます。このページは、インストールされるソフトウェアの現行バージョン、利用可能であるバージョンおよび新規のバージョンのファイルサイズを表示します。さらにダウンロードおよびインストールへのリンク、アップデートの変更点の一覧を参照するリンクを提供します。

3.9 登録

このページへは、登録済のユーザー氏名や会社名、ライセンスキー、登録状況、ライセンスサイズ、他の関連する情報、といった、製品登録情報が表示されています。

SecurityGateway

このセクションは、SecurityGatewayの製品登録情報用です。

ライセンス名:
これは、ライセンスを登録される名前です。

会社名または代理店:
これは、会社またはライセンスの代理店です。

SecurityGateway登録キー:
このボックスは、登録キー用です。キーを入力した後に、**保存**をクリックします。

登録状況
このボックスには、ライセンスサイズおよび他の情報といった登録情報が表示されています。

設定
SecurityGatewayはMDaemon Technologiesからライセンスファイルの更新リクエストを受け取ると、稼働しているOSバージョンをレポートとして送信します。この情報は今後の対応するOSを決定するのに非常に役立ちます。この情報を送信したくない場合は、このオプションを無効にしてください。

セクション 4

4 セキュリティ

セキュリティメニューへは、ドメインやユーザーをスパム、ウィルス、メールの不正使用および他のセキュリティリスクから保護するための8つのセクションと各種ツールが用意されています。下記は、各セキュリティセクションの概要です。詳細な情報については、個々のセクションを参照してください。

スパム対策 127
セキュリティメニューのスパム対策セクションは、スパムまたは要求しない迷惑メールを防ぐのに役立つオプションがあります。このセクションには、ヒューリスティック、ベイジアン分析、DNSおよびURIブラックリスト、グレーリストを使用することによりスパムの確認と防のオプションである8つのスパム対策機能があります。

ウィルス対策 152
セキュリティメニューのアンチウィルスセクションは、ウィルス感染したメッセージを判定し、ユーザへの到達を防ぐ機能を提供しています。。

なりすまし対策 156
なりすまし対策のセクションは、偽造や「なりすまし」アドレスから送信されるメッセージを確認するツールを持ちます。このセクションには、例えばDKIM検証、Sender ID、コールバック検証など、6つのなりすまし対策機能があります。

不正使用対策 180
不正使用対策セクションは、スパムメッセージをリレーし大量の帯域幅の使用や必要以上に頻繁にサーバに接続するメールシステムの悪用または不適当な使用から防ぐツールがあります。不正使用対策セクションには6つのツールがあります。

フィルタリング
フィルタセクションは、2つの**メッセージコンテンツ** 202および**添付ファイルのフィルタリング** 210機能があります。メッセージコンテンツフィルタリングページは、多くの処置を実行するフィルタルールを作成に使用することができます。特定の条件に合致するメッセージを、拒否、別のアドレスへリダイレクト、隔離などのルールを作成することができます。添付ファイルフィルタリングページのオプションは、ファイルのうちの1つが添付される時に、それはメッセージにブロックされるかまたは隔離する特定タイプを指定するために使用することができます。グローバルまたはドメインごとに、フィルタ制限を規定することができます。

ブラックリスト 213
ブラックリストは、メールアドレス、ホストおよびメッセージを、ブロックまたは隔離するIPアドレスのリストです。デフォルトでは、それらのメッセージは、SMTPセッション中に、拒否されますが、その代わりに隔離するように、ブラックリスト処置ページで、この設定を変更することができます。管理される処置は、グローバルまたは特定のドメインに設定ができ、そして、ブラックリスト自体は同様にグローバルまたはドメイン規定としての設定できます。

ホワイトリスト 221
ホワイトリストは、メールアドレス、ホストおよびメッセージをセキュリティ制限から除外するIPアドレスのリストです。SecurityGatewayのセキュリティ機能には、ヒューリスティックおよびベイジアン、DNSBL、DKIM検証およびその他で適切なホワイトリストに現れる場合、送信者、ホスト、メッセージなど除外するオプションがあります。各ホワイトリストは、グローバルまたは特定のドメインとして設定することができます。

Sieveスクリプト [228]
SecurityGatewayではSieveメールフィルタリング言語を多くの機能で使用しており、Sieveスクリプトページではこれらの機能をどのように使用するべきかを指定する事ができます。また、Sieveスクリプトエディタを使って、個別にカスタマイズしたスクリプトを作成することもできます。

4.1 スパム対策

セキュリティ[126]メニューのスパム対策セクションでは、スパムや必要ない迷惑メールを防ぐのに役立つオプションを利用できます。このセクションには次の7つのスパム対策機能があります:

Outbreak Protection[128] – Outbreak Protection（OP）スパムやウィルスが発生してから数分以内で、自動的にメールインフラを先回りして保護することができる革命的なリアルタイムのスパム・ウィルス対策テクノロジです。Outbreak Protectionは、感染を防ぐ事に特化して設計されているので、SecurityGatewayに搭載されている従来のスパムやウィルス対策の代替品ではありません。従来のツールへ、保護レイヤーを追加します。

ヒューリスティックとベイジアン[132] – SecurityGatewayは、ヒューリスティックルールおよびベイジアン分類のためのオープンソースプロジェクト SpamAssassin™ をカスタマイズし、標準搭載しています。ヒューリスティックコンポーネントは、メッセージを、スパムメールによく見られる傾向と比較しスパム判定を行います。ベイジアンコンポーネントは、分析後、ユーザーから受け取ったスパムと非スパムメールを基にしたメールトークンのデータベースとメッセージを比較する事によりスパム判定を行います。

DNSブラックリスト（DNSBL）[138] – このセキュリティ機能では、（スパム送信元のサーバーー覧を管理している）DNSブラックリストサービスを指定し、送信メールがブラックリストに該当しないかどうかを調べるのに使用できます。接続IPが、このブラックリストの1つに該当していた場合、メッセージは拒否、隔離、またはフラグをつけます。

URIブラックリスト（URIBL）[141] – URIブラックリストは、メッセージ本文内で発見される統一資源識別子（URI: 通常ドメイン名またはウェブサイト）に基づいてスパムをブロックまたはタグを付けるために用いるように設計されたリアルタイムブラックリストです。URIブロックリスト、スパムURIリアルタイムブロックリスト（SURBL）などの別名でも知られ、メッセージヘッダの内容に基づいて、または、接続IPアドレスでスパムを確認するために使用されないという点で、URIBLはDNSブラックリストと異なります。代わりに、URIBLはメッセージ内容に基づいてスパムをブロックします。

グレーリスト[144] – グレーリストは、一時的なエラーが発生し、後で再び配信を試みる必要があることを送信メールサーバに知らせる動作をするスパム対策技術です。サーバが取り扱う正当なメール以外のメッセージ配信ができない場合、スパマーは一般的に後続の配信の試みをしないので、グレーリストは、ユーザが受信するスパムの量を減らために役立ちます。

メッセージ証明書[146] – メッセージ証明は、信頼するソースがメッセージに関連した認証された実体の妥当なメール実施法を保証または証明する処理です。従って、信頼するそのソースによって保証されるドメインから送信されるメッセージは、より少ない嫌疑で閲覧することができます。このように、合理的に送信ドメインが一組の妥当なメール実行法を支持して、スパムまたは他の問題のメッセージを送信しないことを保証することができます。

Backscatter Protection 148 - "Backscatter: 後方散乱"は、ユーザが一度も送信しなかったメールで応答メッセージ受信する関連します。ウィルスによって送信されるスパムメッセージまたはメッセージが偽造される"Return-Path"アドレスがあると、これは発生します。従って、これらのメッセージのうち1つが受信者のサーバによって拒絶される場合、あるいは、受信者がアカウントと関連する自動応答を持つ場合、応答メッセージは、ユーザの偽造されたアドレスへと指示します。後方散乱を防止するために、SecurityGatewayは特別な時間依存のコードを送信メッセージの"Return-Path"アドレスに生成して、差し込むプライベートキーを使用することができます。その時、これらのメッセージのうち1つが配信問題に遭遇し戻される場合、または自動応答が"mailer-daemon@..."またはNULL reverse pathで受け取られる時、SecurityGatewayは特別なコードを見て、ドメインのうちの1つによって送信されたメッセージに対する本物の自動化された応答であるということを知っています。メッセージが特別なコードがない場合、あるいはコードが満了した場合、記録され拒否することができます。

メッセージスコア 150 - SecurityGatewayは、メッセージを処理している間、実行するテストに基づいて各メッセージのメッセージスコアを計算します。効果的に"スパムスコア"(メッセージスコア)は、メッセージがスパムであるという可能性を決定するために用います。メッセージスコアページのオプションは、メッセージスコアが特定のしきい値を超過する時、管理する処置を指定するために使用します。しきい値をスパムとしてメッセージにタグを付け、隔離またはSMTPセッション中に拒否する設定をすることができます。

4.1.1 Outbreak Protection

Outbreak Protection (OP)は、自動的にスパムやウィルスからメールインフラを防御し、感染を防ぐ事ができる革命的なテクノロジーです。OPは、メッセージ内容を分析するわけではないため、メール本文や言語に依存しません。よってヒューリスティックルール、コンテントフィルタリング、署名のアップデートを必要としません。さらに、シードテキスト、巧妙なスペリング変更、社会工学戦略、言語バリアまたはエンコード技術の違いによって誤った挙動が起こる事もありません。OPはメッセージ構造の数学的解析およびSMTP上でのメッセージの振分け特徴に依存しメール送信にかかわる"patterns"を分析して、世界的に何百万ものメールメッセージから収集される類似したパターンと比較しサンプルをとり、リアルタイムに比較します。

メッセージはリアルタイムで世界的に分析されているので、保護は新規の発生の数分(しばしば秒単位)以内に提供されます。ウィルス用に従来のアンチウィルスベンダーが、ウィルスシグネチャの最新版を照合および提示する前に、しばしば発生の数時間後でとなるので、このレベルの保護が重大で、その最新版が製造され利用可能になるまでに、長い時間を要する可能性もあります。その間にOutbreak Protectionのないサーバは、その特定の発生の影響を受けやすくなります。同様に、スパムメッセージに対して、従来のヒューリスティックおよびコンテントベースのシステムによって認識される前に、スパムの分析と安全なフィルタリングルールを作成する多くの場合時間と努力が必要です。

Outbreak Protectionが従来のアンチウィルスおよびアンチスパム技術のための代替品でない点に注意することが重要です。実際には、OPは従来のSecurityGatewayに搭載されているヒューリスティック、署名、コンテンツを元にしたツールにもう一つのレイヤーを追加提供しています。OPは従来のツールによって更に確実に捕えられることができる旧式、固有、明確に対象とされたメッセージではなく、大規模な発生を処理するように設計されています。

Outbreak Protection は Recurrent-Pattern DetectionおよびZero-Hourテクノロジをベースにしています。これは、世界中の膨大なソースから毎日取得する数百万通のインターネット上のメール配信パターンを比較し、分析しています。この分析に、メール本文が依存する事はありません。

スパム対策

アンチスパムOutbreak Protectionを有効にする
Outbreak Protectionアンチスパムオプションは、デフォルトで有効です。受信メッセージは、継続中のスパム発生の一部であるかどうか確認するために分析されます。このセクションの残りのオプションは、発生の一部と発見されるメッセージを、どのように取り扱うか確定するために使用し、OP処理から免除される差出人を指定します。

Outbreak Protectionでスパムと判断した場合:
下記で選択されるオプションは、OPがメッセージをスパムで識別する時に、必要とする動作を確定します。

...メッセージを拒否
OPがスパム発生の一部であること確認する時、SMTP処理中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、隔離またはスパムとしてタグを付けされず、予定受信者に配信されサーバによって拒否されます。

...メッセージを隔離
このオプションが選択される時に、Outbreak Protectionはスパムと確定するメッセージを隔離します。

...メッセージを受け入れる
デフォルトで、OPは、スパムと確定するメッセージを受け取り、下記の**この値をスコアに追加**オプションに従ってメッセージスコアを調整します。

...次の文字を件名に付ける [*text*]
このオプションは、デフォルトで無効です。このオプションを有効にする場合、Outbreak Protectionがスパムであると確定する場合、メッセージのサブジェクトヘッダの先頭にテキストを追加します。追加されるデフォルトテキストは、次の"*** SPAM ***"ですが、別のテキストにすることができます。

SecurityGateway内で、下記の残り2つのOutbreak Protectionオプションを含むサブジェクトヘッダにテキストを任意に追加することができる別の場所があります。それらのオプションで指定されたテキストが一致する時に、メッセージが各オプションで基準を満たす場合でも、テキストはメッセージサブジェクトに追加されるだけです。ただし、他の設定で、オプションの一つ以上でテキストを変更する場合、そのカスタマイズされたテキストも同様に追加されます。例えば、"*SPAM*"に複数のオプションでテキストをセットする場合、複数のオプションで基準に適合にかかわらず、テキストはサブジェクトに追加されます。しかし、何か他のものにオプションのうちの1つでテキストを変更する場合(例えば、"*Junk email*")、両方のタグは追加されます。

...この値をスコアに追加 [XX]
このオプションを使用すると、Outbreak Protectionがスパムであると確定するメッセージのスコアに、指定されたポイント数を追加します。このオプションはデフォルトで使用可能で、メッセージスコアに5.5ポイントを追加します。

SecurityGatewayで拒否または隔離ではなくメッセージを受け取る構成がされる場合でも、他のセキュリティ126オプションおよびメッセージスコア150ページのオプションで構成した方法に応じて、メッセージスコアが十分に高い場合、今まで通り拒否あるいは隔離がされる場合があります。

Outbreak Protectionでスパムの可能性があると判断した時:
Outbreak Protectionは、明確な判定をすることができない一部のメッセージを"潜在的"スパムに分類します。下記で選択されるオプションは、OPがそれらのメッセージの取り扱いを確定します。

...メッセージを拒否
OPが潜在的スパムであると確定する時、SMTP処理中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が潜在的なスパムに分類されるだけなので、このオプションは、隔離またはタグを付けせず、完全にメッセージを拒否するので推奨されません。

...メッセージを隔離
このオプションが選択される場合、Outbreak Protectionは潜在的にスパムであるメッセージを隔離します。

...メッセージを受け入れる
デフォルトで、OPは潜在的にスパムであると確定するメッセージを受け取ります。選択する場合、同時に下記で"...**この値をスコアに追加**"オプションに従ってメッセージスコアを調整する構成することができます。

...次の文字を件名に付ける [*text*]
このオプションはデフォルトで無効です。このオプションを有効にする場合、Outbreak Protectionが潜在的にスパムであると確定する場合、メッセージのサブジェクトヘッダの先頭にテキストを追加します。追加されるデフォルトテキストは、"*** POTENTIAL SPAM ***"ですが、別のテキストにすることができます。

...この値をスコアに追加 [XX]
このオプションを使用すると、Outbreak Protectionが潜在的スパムであると確定するメッセージのスコアに、指定されたポイント数を追加します。このオプションはデフォルトで使用可能で、メッセージスコア150に2.0ポイントを追加します。

Outbreak Protectionでバルクメッセージと判断した時:
時々、既知のスパマーまたはボットネットから送信されていないので、Outbreak Protectionでは、正当なメーリングおよびニュースレターのようなスパムとして明確に識別することができない特定の多量な配信メッセージを確認します。OPは、この種のメッセージをスパムではなくバルクと分類します。下記のオプションは、これらのメッセージで取り扱いを管理します。

...メッセージを拒否
OPが"bulk"と分類する時、このオプションはSMTPセッション中に、メッセージを拒否します。一部の正当な広く配信するメッセージが拒否されることが生じる可能性がある理由から、このオプションは推奨されません。

...メッセージを隔離
Outbreak Protectionがバルクと分類するメッセージを隔離する場合、このオプションを選択します。

...メッセージを受け入れる
デフォルトで、"bulk"と分類されるメッセージが単に一定の極めて多量な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トである可能性があるので、バルクメッセージはOPによってブロックまたは隔離されません。

...次の文字を件名に付ける [*text*]
このオプションはデフォルトで無効です。このオプションを有効にする場合、Outbreak Protectionがバルクメールであると確定する時、メッセージのサブジェクトヘッダの先頭にテキストを追加します。追加されるデフォルトテキストは、"*** BULK ***"ですが、別のテキストにすることができます。

...この値をスコアに追加 [XX]
このオプションが有効な場合、OPがメッセージを"bulk"と分類する時、メッセージスコアは増加します。これはデフォルトで有効で、3.0ポイントが追加されます。

ホワイトリストの差出人からのメッセージを除外する
デフォルトで、ホワイトリスト(差出人)[221]からのメッセージは、Outbreak Protectionのアンチスパムオプションから免除されています。

認証されたセッションからのメッセージを除外する
このオプションはデフォルトで有効で、認証されたセッションを使用しているメッセージをOutbreak Protectionから除外します。

ドメインメールサーバからのメッセージを除外する
ドメインメールサーバ[65]から送信されるメッセージは、デフォルトでOutbreak Protectionから免除されています。これらのメッセージをOutbreak Protection規制から除外しない場合、このオプションを解除します。

ウィルス対策

Anti-Virus Outbreak Protectionを有効にする
Outbreak Protectionアンチウィルスオプションは、デフォルトで有効です。受信メッセージは、進行中のウィルス発生の一部であるかどうか確認するために分析されます。このセクションの残りのオプションは、発生の一部で発見されるメッセージの取り扱いを確定するために使用し、Anti-Virus Outbreak Protectionから免除される差出人を指定します。

Outbreak Protectionでメッセージの感染を判断した時:
下記の選択されるオプションは、感染時OPがメッセージを識別する場合、必要とされる動作を確定します。

...メッセージを拒否する
デフォルトでOutbreak Protectionがウィルス発生の一部であると確定する時に、SecurityGatewayはSMTPセッション中にメッセージを拒否します。

...メッセージを隔離する
Outbreak Protectionが感染しているメッセージを隔離する場合、このオプションを選択します。

ホワイトリストIPアドレスからのメッセージを除外する
ホワイトリストIPアドレス[226]またはホワイトリストホスト[223]からメッセージを受信時にAnti-Virus Outbreak Protectionから除外する場合、このチェックボックスを選択します。

ドメインメールサーバからのメッセージを除外する
ドメインメールサーバ[65]から送信されるメッセージは、このオプションが有効な場合に、Anti-Virus Outbreak Protectionから除外されます。

プロキシ設定

SecurityGatewayのOutbreak Protectionテクノロジは、HTTPを通してOutbreak Protectionオンラインサービスと通信することができる必要があります。必要に応じてOutbreak ProtectionのHTTPプロキシを定義するために、このセクションでオプションを使用することができます。

例外 – ドメイン

これらの設定を構成する時、ページ上部のドメイン:ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。Outbreak Protection設定を見直し編集するには、対応するドメインの**表示/編集**リンクをクリック、あるいはデフォルトの全体の設定値をドメインの設定にリセットするには、**リセット**をクリックします。

4.1.2 ヒューリスティックとベイジアン

SecurityGatewayは、一般に普及しているオープンソースSpamAssassin™(ヒューリスティックルールおよびベイジアン分類のためのプロジェクト)の高性能なカスタマイズされたバージョンを使用します。メッセージはこの処理に渡されて、内容に基づくスコアを設定します。内蔵されたSpamAssassinの代わりに、SecurityGatewayでは、外部のSpamAssassinデーモンの利用を許可します。

設定

メッセージ分析でヒューリスティックルールとベイジアン分類を使用する
デフォルトで、このオプションは有効です。そのメッセージは、ヒューリスティックルールおよびベイジアン分類法システムを通して渡され、結果に基づいてSpamAssassinスコアを設定することを意味します。このシステムを無効にし、このページの別のオプションを利用停止にする場合は、このチェックボックスを解除します。

ヒューリスティックルールを自動的に更新するオプションとSGSpamD設定[134]画面でベイジアン分類を管理するオプションを構成することができます。下記で"内蔵のローカルSpamAssassinエンジン(SGSpamD)を使用する"オプションで"SGSpamDの設定は、ここをクリック"[134]リンクを通じて画面を表示することができます。

SpamAssassinで戻されるスコアをメッセージスコアへ追加する
デフォルトで、このオプションは、メッセージスコアにSpamAssassinスコアを追加するために使用します。メッセージスコアオプションを使用する時に、最終的なメッセージスコアにSpamAssassinスコアを追加することを、スパム保護の別の階層を提供することができ、そして、SpamAssassinのみ、または他の個々のアンチスパムスコアリングオプションによって捕えられるのに十分な高さを記録しないスパムを捕える可能性を増やします。

SpamAssassinスコアが指定値以上の場合メッセージを拒否する
SpamAssassinスコアに対して除外する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。言い換えると、メッセージに対してのSpamAssassinスコアが、この値以上である時、メッセージは隔離または残りのアンチスパムおよびメッセージスコアリングオプションによって処理を継続するのではなく、SMTPセッション中に拒否されます。従って、下記の"SpamAssassinスコアが指定値以上の場合メッセージを隔離する"オプションと連動して、このオプションを使用する場合、隔離値より大きい値に除外するしきい値を常にセットする必要があります。それ以外のメッセージは、SpamAssassinスコアにより決して隔離されません。隔離する充分なスコアを持つメッセージは拒否されます。この除外しきい値に対するデフォルト値は、12.0です。

SpamAssassinスコアが指定値以上の場合メッセージを隔離する
SpamAssassinスコアに隔離用しきい値を指定する場合、このオプションを有効にします。この値以上のスコアをもつメッセージは隔離されます。隔離されたメッセージは、SecurityGatewayにサインインすることで、受信者または管理者によって閲覧と管理ができます。上記の"SpamAssassinスコアが指定値以上の場合メッセージを拒否する"オプションと連動して、このオプションを使用する場合、"SpamAssassinスコアで隔離する"オプションを"SpamAssassinスコアで拒否する"オプションより小さい値に常に設定します。このオプションのデフォルト値は、5.0です。

ヒューリスティックおよびベイジアンシステムのパフォーマンスを監視し、時間をかけて、必要性を満たすために両方の除外および隔離のしきい値を改善する必要があります。通常、比較的少ない検出漏れ(認められていないものを通り抜けるスパム)、および希に誤検出(スパムでないメッセージにスパムとしてフラグを付ける)を伴うデフォルト値は、大部分のスパムをキャッチします。デフォルトの除外をするしきい値12は、妥当なスタートポイントです。大部分のケースで正当なメッセージは、その高さを記録しません。

例外

指定サイズより大きいメッセージを除外する[xx]KB
大容量のメッセージをヒューリスティックおよびベイジアンシステムでスキャンを除外する場合、ここに値(キロバイト単位)で指定します。大容量のメッセージは、まれにスパムとみなされます。スキャンから除外することは、多くのリソースを節約することができます。

ホワイトリストの差出人からのメッセージを除外する
デフォルトでホワイトリスト 221にある差出人からメッセージを送信する場合、SecurityGatewayでメッセージのヒューリスティックおよびベイジアン処理から除外します。これらのメッセージを除外しない場合、このチェックボックスを解除します。

認証されたセッションからのメッセージを除外する
このオプションは、認証済みSMTPセッションの場合に、ヒューリスティックおよびベイジアンシステムからメッセージを除外するために使用します。このオプションはデフォルトで有効です。

ドメインメールサーバからのメッセージを除外する
ドメインメールサーバ 65から到着しているメッセージは、デフォルトでヒューリスティックおよびベイジアン処理から除外されます。それらのサーバから到着しているメッセージを、ヒューリスティックおよびベイジアンで処理する場合、このオプションを解除します。

場所(すべてのドメイン)

内蔵のローカルSpamAssassinエンジン(SGSpamD)を使用する
個別のデーモン-SecurityGatewayスパムデーモン(SGSpamD)として実行するSecurityGateway内蔵SpamAssassinエンジンを使用する場合、このオプションを選択します。SGSpamDを構成するために、SGSpamDの設定は、ここをクリック[134]リンクをクリックします。リモートロケーションで異なるSpamAssassinエンジン実行を使用する場合、下記のリモートSpamAssassinデーモンオプションを選択します。

リモートSpamAssassinデーモン(SpamD)を使用する
内蔵SGSpamDを使用するのではなく、リモートロケーションにあるSpamAssassinデーモンを使用しメッセージをスキャンする場合、このオプションを選択します。

ホストアドレス:
ここにリモートSpamDのIPアドレスを指定します。

ポート:
リモートSpamDを実行しているポートを指定するために、このオプションを使用します。

テスト
リモートSpamDに接続をテストするために、このボタンをクリックします。

例外 - ドメイン

これらの設定を構成する時、ページ上部の**ドメイン:**ドロップダウンリストボックスで、特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。ヒューリスティックおよびベイジアン設定を見直し編集するには、対応するドメインの**表示 / 編集**リンクをクリック、あるいはデフォルトの全体の設定値をドメインの設定にリセットするには、**リセット**をクリックします。

4.1.2.1 SGSpamD設定

ヒューリスティックルールシステムは、各メッセージの内容がスパムであるという可能性を判定するために一組の静的なルールとの比較によって利用します。各ルールは、特定の数値があり、各メッセージのSpamAssassinスコアは、メッセージと適合する各ルールの値に基づいて調整されます。ルールおよび値は、定期的に調整されて、スパムおよび迷惑メールにおける現在の傾向に遅れないように変更されます。指定された間隔で自動的にヒューリスティックルール更新チェックを、SecurityGatewayのSGSpamDを構成、または手動で更新チェックをすることができます。

ベイジアン分類は、時間とともにスパム認識の信頼性を向上するために、スパムおよび非スパムメッセージを分析するオプションで使用することができる統計処理です。手動でスキャンまたは指定間隔で自動的にスキャンができる、スパムメッセージおよび非スパムメッセージ用のフォルダを指定することができます。フォルダにあるメッセージすべては分析されインデックスが付けられる、または"Bayesian Learned"です。その結果、新規のメッセージは、スパムであるという可能性を判定するために統計学的に比較ができます。これは、同時にベイジアン比較の結果に基づくメッセージのSpamAssassinスコアを増加または減少させることができます。

ヒューリスティックルール更新

毎晩深夜にヒューリスティックルール更新をチェックする
自動的に毎晩真夜中に、ヒューリスティックルール更新をチェックする場合、このオプションを選択します。

指定時間ごとにヒューリスティックルール更新をチェックする [XX]時間
1日に1回ではなく、自動的にヒューリスティックルール更新を一定時間間隔でチェックする場合、このオプションを選択して時間間隔を指定します。

ヒューリスティックルール更新のチェックをしない
自動的にヒューリスティックルール更新のチェックをしない場合、このオプションを選択します。下記のすぐにヒューリスティックルール更新をするには、ここをクリックしますを使用し、手動で最新版をチェックすることができます。

更新処理の一部としてSA-更新を実行
MDaemon Technologiesからのアップデートに加えて、updates.spamassassin.orgからもアップデートの取得を行う場合、このチェックボックスを選択します。この機能は、SpamAssassinルールセットを常に最新な状態にします。このオプションは、デフォルトで有効です。

すぐにヒューリスティックルール更新をするには、ここをクリックします
ヒューリスティックルールを手動でチェックするには、このリンクをクリックします。

ベイジアン分類

ベイジアン分類法を有効にする
SGSpamDのベイジアン分類システムを有効にするには、このチェックボックスを選択します。各メッセージのSpamAssassinスコアを、現在既知のベイジアン統計との比較に基づいて調整する場合、この機能を使用します。

> ベイジアン分類子は、メッセージのSpamAssassinスコア調整を開始する前に、解析するためのスパムおよび非スパム両方のサンプルを必要とします。これは、ベイジアン比較をする時に、ベイジアン学習過程で集める統計の充分なプールを持つために必要です。一旦ベイジアン学習システムに分析するメッセージを渡すと、ベイジアン比較の結果を、各メッセージのSpamAssassinスコアに適用されることを開始する準備ができます。より多くのメッセージ分析を継続することにより、ベイジアン分類は、時間とともにより正確になります。

学習する必要のある非スパムメッセージ:
これは、ベイジアン分類器がメッセージを記録し始める前に、分析する必要がある「非スパム」に指定されるメッセージの数です。デフォルト値は、200のメッセージです。

学習する必要のあるスパムメッセージ:
これは、ベイジアン分類器がメッセージを記録し始める前に、分析する必要がある「スパム」に指定されるメッセージの数です。デフォルト値は、200のメッセージです。

ベイジアン学習

毎晩深夜にベイジアン学習をする
ベイジアン学習システムが、指定されたスパムおよび非スパムフォルダに含まれるメッセージを、1日に1回、自動的に毎晩真夜中に分析する必要がある場合、このオプションを選択します。

指定時間毎にベイジアン学習をする[XX]時間
ベイジアン学習システムが、指定されたスパムおよび非スパムフォルダに含まれるメッセージ分析を、自動的に毎晩真夜中ではなく、指定した時間ごとに行う場合、このオプションを選択し値を指定します。

ベイジアン学習をしない
ベイジアン学習をしない場合、このオプションを選択します。ただし、下記の"**すぐにベイジアン学習を実行するには、ここをクリック**"リンクをクリックすると、手動でベイジアン学習処理を、いつでも開始することができます。

既知のスパムディレクトリ(検出漏れ):
これは、スパムに指定されるメッセージを含んでいるフォルダのパスです。スパムメッセージは、このフォルダへ手動で置かれる、または自動ベイジアン学習オプションを使用し自動で置かれます。

非スパムディレクトリパス(誤検出):
これは、非スパムに指定されるメッセージを含んでいるフォルダのパスです。非スパムメッセージは、このフォルダへ手動で置かれる、または自動ベイジアン学習オプションを使用し自動で置かれます。

スパム転送アドレス:
ユーザがベイジアンシステムで学習するスパムメッセージを転送するアドレスを、このテキストボックスに指定します。SecurityGatewayが使用するデフォルトアドレスは"SpamLearn[@ AnySGDomain.com]"ですが変更することができます。このアドレスに送信されるメッセージは、SMTP AUTHを使用して認証済みセッションからSMTP経由で受信される必要があります。さらに、メッセージは"message/rfc822"タイプの添付ファイルとして、上記のアドレスに転送する必要があります。このメールアドレスに送信される別のタイプのメッセージは処理されません。最後に、このオプションにアドレスを入力する場合、メールボックスの一部を使用するだけです－"@ "またはドメイン一部は不要です。
例えば、"Spam"、"SpamLearn"、"SpamMail"などは、このオプションの利用で受け入れ可能なアドレスです。メッセージは、任意のSecurityGatewayドメインで、アドレスに転送することができます(例えば、SpamLearn@ example.com, SpamLearn@ company.mailなど)。

非スパム転送アドレス:
ユーザが、ベイジアンシステムで学習できる非スパムメッセージを転送するアドレスを、このテキストボックスに指定します。SecurityGatewayが使用するデフォルトアドレスは"NonSpamLearn[@ AnySGDomain.com]"ですが変更することができます。このアドレスに送信されるメッセージは、SMTP AUTHを使用して認証済みセッションからSMTP経由で受信する必要があります。さらに、メッセージは"message/rfc822"タイプの添付ファイルとして、上記のアドレスに転送する必要があります。このメールアドレスに送信される別のタイプのメッセージは処理されません。最後に、このオプションにアドレスを入力する場合、アドレスをメールボックスの一部で使用するだけです。"@ "またはドメイン一部は不要です。
例えば、"NonSpam", "NonSpamLearn", "GoodMail"などは、このオプションの利用で受け入れ可能なアドレスです。メッセージは、任意のSecurityGatewayドメインで、そのアドレスに転送することができます(例えば、NonSpamLearn@ example.com, NonSpamLearn@ company.mailなど)。

指定バイト数以上は学習しない[XX]バイト
通常、大容量のメッセージはスパムではないこと、ならびに分析に多くの処理を必要とする可能性があるので、50,000バイト以上のメッセージは、デフォルトで分析しません。このオプションを選択で、サイズの調整、あるいはサイズに関係なくメッセージ分析することができます。

すぐにベイジアン学習を実行するには、ここをクリック

手動でベイジアン学習処理を開始するには、このリンクをクリックします。

自動ベイジアン学習

ベイジアンを自動学習する
自動のベイジアン学習で、正当な(すなわち非スパム)メッセージおよびスパムに対してメッセージスコアのしきい値を指定することができます。非スパムしきい値より下の最終的なメッセージスコアをもつメッセージは、自動学習によって非スパムとみなされ、スパムしきい値より上のメッセージスコアは、スパムとみなされます。注意して使用する場合でも、しきい値の設定が慎重である場合、自動的に置き換えられるデータベースファイル(ベイジアンデータベースを下記で参照)から削除される期限切れのトークンを許可するので自動学習は有効なはずです。期限切れのトークンを回復する手動の再訓練の必要性を防止すると共に、一定の最新の供給を学習するためのベイジアン学習システムに渡すことができます。

次の値より小さいスコアのメッセージを適正なメッセージとする [XX](スコアを指定)
この値以下のメッセージスコアをもつメッセージは、ベイジアン学習の目的で正当/非スパムメッセージに分類されます。

...ドメインメールサーバおよび認証されたセッションからの非スパムのみ学習する
認証済みセッションを通じて、またはドメインメールサーバ[65]から到着するメッセージ限定で正当なメールの自動ベイジアン学習を適用する場合、このオプションを選択します。このオプションを使用する場合、ドメインメールサーバまたは認証済みソースから受信しない限り、最終的なメッセージスコアに関係なく、非ローカルソースからの受信メッセージは、ベイジアン学習に使用されません。ただし、任意の正当なメッセージを、上記の指定された"非スパム"フォルダリストへ、今まで通り手動でコピーすることができます。このように、同様に"非スパム"フォルダから学習する正当なメッセージをシステムに提供します。

次の値より大きいスコアのメッセージをスパムとする [XX](スコアを指定)
この値より上のメッセージスコアをもつメッセージは、ベイジアン学習の目的でスパムメッセージに分類されます。

...受信メッセージからスパムのみ学習する
スパムメールの自動ベイジアン学習を受信メッセージのみに適用する場合、このオプションを選択します。このオプションを使用する場合、最終的なメッセージスコアに関係なく、送信メッセージは、ベイジアン学習に使用しません。ただし、上記の"スパム"フォルダリストへ、手動でメッセージを今まで通り置くことができます。

ベイジアンデータベース

ベイジアン自動トークン失効を可能にする
下記で指定されるトークンの数に到達時はいつでも、このオプションは、ベイジアンシステムで自動的にデータベーストークンの失効を許可します。トークン制限の設定は、過度に大きくすると、ベイジアンデータベース処理が遅くなることを防止することができます。

ベイジアンデータベースのトークンの最大値:
これは、許可されるベイジアンデータベーストークンの最大数です。この値に到達した場合、ベイジアンシステムは、古いデータから削除をし、この値の75%、または100,000トークンのどちらかの高い数値まで減らします。失効するトークンの数に関係なく、トークンの数は、2つの値でどちらか大きい値以下にはなりません。注意:150,000データベーストークンほぼ8MBです。

詳細

メッセージ処理スレッドの最大値(1-6):
常にSGSpamDにより使用されるメッセージ処理スレッド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。1から6つのスレッドまでこの値をセットします。このデフォルトは4です。

スレッドごとのTCP接続の最大値(10-200):
これは、常に許可するメッセージ処理スレッドごとのSGSpamDに対するTCP接続の最大値です。10-200からこの値をセットします。このデフォルトは、200です。

4.1.3 DNSブラックリスト(DNSBL)

DNSブラックリスト(DNSBL)は、ユーザに届くスパムを防止の手助けと使用できます。このセキュリティ機能は、誰かがドメインのうち1つにメッセージを送信するごとに、スパムをリレーすると知られているサーバのリストを保持するチェックサービスで、ブラックリストにあるNS指定を可能にします。接続IPが、それらのサービスのいずれか一つによってブラックリストに載せられた場合、メッセージは拒否、隔離、またはフラグをつけます。

この機能の使用は、ユーザ宛に送信される大部分のスパムを防ぐことができます。ただし、一部のサイトは誤ってブラックリストに記載されます、従って、ブラックリストにあるIPアドレスから完全にメッセージを拒否するために使用する場合、この機能を使用することで若干の問題点を起こす可能性があります。ただし、SecurityGatewayの他のスパム防止機能(例えばURIブラックリスト、メッセージスコアおよびヒューリスティックおよびベイジアンオプション)と連動して使用する場合、今まで通りに最適な設定です。

設定

DNSBLクエリを有効にする
このオプションは、DNSブラックリストに対して受信メールをチェックするために使用します。SecurityGatewayは、サーバのIPアドレスを送信するために下記で一覧を示される各DNSBLホストを問い合わせます。ホストがクエリにIPアドレスがブラックリストにあると示している明白な結果で応答する場合、メッセージは拒否、隔離または受諾され下記オプションに従ってフラグを付けます。このオプションはデフォルトで有効です。

メッセージの送信サーバがリストに存在する場合:

...メッセージを拒否
このオプションを選択する場合、ブラックリストIPアドレスからの受信メッセージはSMTPセッション中に拒否します。オプションで、メッセージを拒否に対し、従来の"user unknown"応答を使用するのではなく、SecurityGatewayでは、メッセージが拒否されている接続サーバに示すブラックリストにある関連するカスタマイズされた応答を使用することができます。ホストエントリの作成時、下記でメッセージオプションを用いて各DNSBLホストと関連する応答を指定することができます。**メッセージの拒否で'user unknown'ではなく'message'を戻す場合** unknown'オプションを有効にすることで、従来の"user unknown"応答でなく、別の応答を送信するために、SecurityGatewayを構成することができます。

...メッセージを隔離
DNSブラックリストIPアドレスからのメッセージを隔離する場合、このオプションを選択します。

...メッセージを受け入れる
ブラックリストアドレスからのメッセージを受け入れ、サブジェクトにタグを付け、メッセージスコアの調整をすることができます。このオプションを使用することは、SecurityGatewayのDNSBLクエリの結果に基づいてそれ自身メッセージのフィルタをメールサーバまたはユーザに許可にすることができます。

...次の文字を件名に付ける [*text*]
このオプションを選択し、メッセージがブラックリストIPアドレスから到着する時に、メッセージのサブジェクトヘッダの始めに追加するテキストを指定します。デフォルトで、このオプションは無効です。このオプションを可能にする場合、"*** SPAM ***"はデフォルトでサブジェクトに追加されますが、このオプションの選択をする場合、テキストを編集することができます。

他のオプションで、サブジェクトヘッダにテキストをオプションとして追加することができます。例えば、Messメッセージスコア[150]およびURIブラックリスト(URIBL)[141]ページは、同様なオプションを持ちます。これらのオプションの指定されたテキストが合致する場合、そのメッセージが各オプションで基準を満たす場合であっても、テキストは一度メッセージのサブジェクトに追加されるだけです。ただし、別のオプションでテキストを変更する場合、そのカスタマイズされたテキストは同様に追加されます。従って、例えば、"*SPAM*"にこれらのオプン3つでテキストを設定する場合、オプションの1つ以上で基準に合致したかを問わず、そのテキストは一度サブジェクトに追加されるだけです。しかし、DNSBLオプションのテキストを"*DNS blacklisted*"に変更し、メッセージが、このオプションおよび他で基準に合致した場合、追加されるサブジェクトは*SPAM*および*DNS blacklisted*を持ちます。

...この値をスコアに追加 [XX] ポイント
DNSブラックリストである時、このオプションでメッセージスコアへ指定ポイントを追加します。このオプションはデフォルトで使用可能で、メッセージスコアに5.0ポイントを追加します。

SecurityGatewayが拒否または隔離ではなくメッセージを受け入れる構成をする時でも、他のセキュリティ[126]オプションおよびメッセージスコア[150]ページでオプションの構成により、メッセージスコアが十分に高い場合、今まで通り拒否または隔離される可能性があります。

除外

ホワイトリストの差出人からのメッセージを除外する
デフォルトで、ホワイトリスト[221]送信者から起こる場合、メッセージはDNSBLクエリから除外されます。このオプションを送信者がホワイトリストでもDNSBLホストの問い合わせをする場合、解除します

認証されたセッションからのメッセージを除外する
到着しているセッションが認証された時にメッセージをDNSBLクエリから除外する場合、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有効です。

ドメインメールサーバからのメッセージを除外する
ドメインメールサーバ[65]から到着しているメッセージは、常にDNSBLホストクエリから除外されます。

DNSBLホスト(全ドメイン)

新規ホスト:
DNSBLホスト一覧へ新規のホストを追加するには、ここで問い合わせるホスト(例えば、zen.spamhaus.org)を入力し、対応するメッセージを下記で追加し[追加]をクリックします。

メッセージ:
これは、ブラックリストアドレスからの拒否されたメッセージで、**メッセージを拒否する場合に'user unknown'ではなく'message'を戻す**オプションを下記で可能にした時、ブラックリストIPアドレスがSecurityGatewayによって見つけ出される場合にホストに問い合わせSMTPセッション中に接続サーバに戻されるブラックリストIPアドレスが見つけ出される場合にログで監視され上記で入力される新規ホストに対応するメッセージです。ブラックリストIPアドレスを含む場合、メッセージでIPマクロを使用することができます。

追加
新規ホストおよび対応するメッセージを入力後、DNSBLホストのリストに追加するために、このボタンをクリックします。

削除
DNSBLホストリストからエントリを削除する場合、エントリを選択し**削除**ボタンをクリックします。

接続IPを記載する最初のホストでDNSBLクエリを停止する
各メッセージのヘッダで含まれる複数のIPアドレスおよびこれらのアドレスに関して問い合わせられる複数のDNSBLホストがあります。デフォルトで、ブラックリストIPアドレスが見つけ出されるとすぐに、SecurityGatewayは特定のメッセージについてDNSBLホストを問い合わせて中止します。ブラックリストアドレスが見つかった後、すべてのアドレスおよび全DNSBLホストについてクエリの実行を継続する場合、このオプションを無効にします。

メッセージを拒否する場合に'user unknown'ではなく'message'を戻す
"...メッセージの拒否する"にDNSBLオプションを構成する時、ブラックリストIPアドレスが見つけ出される場合、デフォルトでDNSBLホストに相当する上記の一覧にされるショートメッセージは、ログファイルで監視されSMTPセッション中に接続しているサーバへ戻されます。代わりに標準"user unknown"メッセージを使用する場合、このオプションを解除します。

詳細(全ドメイン)

収集されたメッセージの'Received'ヘッダをチェックする
デフォルトで、SecurityGatewayは、実際に接続しているホストのIPアドレスに対して、メッセージを配信することを試みるDNSBLホストを問い合わせるだけです。同様にメッセージの受信されたヘッダの内部で見つけ出されるIPアドレスについてDNSBLクエリを実行する場合、このオプションを選択します。

この指定数だけReceived'ヘッダをチェックする
ブラックリストIPアドレスについてReceivedヘッダをチェックするSecurityGatewayを構成する場合、ヘッダのチェックする回数を制限する場合、このオプションに値を入力します。それらの全部をチェックする場合0を使用します。

指定した直近の'Received'ヘッダをスキップする (0=しない)
ブラックリストIPアドレスについてReceivedヘッダをチェックするSecurity Gatewayを構成する場合、最近のヘッダの一定数をスキップする場合、このオプションに値を入力します。特定のメールシステム構成によって、時々、ごく最近のヘッダはネットワーク上で信頼されたホストまたは他のコンピュータのIPアドレスを持ち、ブラックリストに対してチェックされる必要ありません。最新のヘッダのいずれもスキップしない場合、このオプションで0を使用します。

指定した古い'Received'ヘッダをスキップする (0=しない)
ブラックリストに記載されたIPアドレスに対して受信されたヘッダをチェックするために Security Gatewayを構成した場合、最も古いヘッダの一定数をスキップする場合、このオプションに値を入力します。たびたび、最も古いヘッダは、送信者の内蔵メールサーバで追加または正当に見えるよう偽造されたので、チェックする関連するアドレスを持ちません。最も古いヘッダをスキップしない場合、このオプションで0を使用します。

例外 - ドメイン

これらの設定を構成する時、ページ上部の**ドメイン:**ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。DNSブラックリスト設定を見直し編集するには、対応するドメインの**表示 / 編集**リンクをクリック、あるいはデフォルトの全体の設定値をドメインの設定にリセットするには、**リセット**をクリックします。

4.1.4 URIブラックリスト(URIBL)

URIブラックリストは、メッセージ本文内で発見される統一資源識別子(URI: 通常ドメイン名またはウェブサイト)に基づいてスパムをブロックまたはタグを付けるために用いるように設計されたリアルタイムブラックリストです。URIブロックリスト、スパムURIリアルタイムブロックリスト(SURBL)などの別名でも知られ、メッセージヘッダの内容に基づいて、または、接続IPアドレスでスパムを確認するために使用されないという点で、URIBLはDNSブラックリスト 138と異なります。代わりに、URIBLはメッセージ内容に基づいてスパムをブロックします。URIBLについては、www.surbl.orgをご覧ください。

設定

URIBLクエリを有効にする
デフォルトで、メッセージに関してURIBLクエリを実行します。これらのクエリを実行しない場合、このオプションを解除します。

メッセージがリストのURIを含む場合:

...メッセージを拒否
ブラックリストにあるURIを含む場合、SMTP処理中に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。これは、メッセージ本文におけるブラックリストURIを単なる参照では、メッセージそのものが、スパムであることを保証しないので、多くの状況において推奨されるオプションではありません。

...メッセージを隔離
ブラックリストにあるURIを含むメッセージを隔離する場合、このオプションを選択します。

...メッセージを受け入れる
ブラックリストにあるURIを含むメッセージを受け入れるが、スパムとしてのフラグ付け、サブジェクト行にタグを追加、メッセージスコアを調整する場合、このオプションを選択します。このオプションの使用は、Security GatewayのURIBLクエリの結果に基づいて、メールサーバまたは受信者で、メッセージのフィルタを許可します。これは、デフォルトオプションです。

...次の文字を件名に付ける [*text*]
メッセージにブラックリストにあるURIを含む時に、メッセージのサブジェクトヘッダの先頭にテキスト追加する場合、このオプションを有効にして、テキストを指定します。このオプションが有効な場合、サブジェクトに追加されるデフォルトテキストは、"*** SPAM ***"です。このオプションはデフォルトで無効です。

SecurityGatewayでは、サブジェクトヘッダにテキストを追加することができる他のオプションがあります。例えば、DNSブラックリスト(DNSBL 138)およびメッセージスコア 150ページは、このオプションを同様に持ちます。それらのオプションで指定されたテキストが一致する時に、メッセージが各オプションで基準を満たす場合でも、テキストはメッセージサブジェクトに追加されるだけです。ただし、他のオプションでテキストを変更する場合、そのカスタマイズされたテキストも同様に追加されます。例えば、これらの3つのオプションに"*SPAM*"をテキストとして設定する場合、複数のオプションで基準に適合にかかわらず、テキストは一度サブジェクトに追加されます。しかし、URIBLオプションのテキストを"*URI blacklisted*"に変更し、メッセージが、このオプションおよび他のオプションに基準に適合した場合、サブジェクトは、両方の*SPAM*および*URI blacklisted*を追加されます。

...URIBLエンジンによって戻されるスコアをメッセージスコアへ追加する
デフォルトで、URIBLクエリがメッセージでブラックリストあるURIを含む場合に、問い合わせたURIBL Hostに関連したスコアはメッセージスコアに追加されます。URIBLクエリの結果に基づいてメッセージスコアを調整しない場合、このオプションを解除します。

SecurityGatewayで拒否または隔離ではなく、メッセージを受け取る設定の場合でも、そのメッセージスコアが十分に高い場合、今まで通り拒否または隔離される可能性があります。他のセキュリティ 126オプションおよびメッセージスコア 150ページでオプションでの構成に依存します。

例外

ホワイトリストの差出人からのメッセージを除外する
デフォルトで、ホワイトリス 221にある差出人からのメッセージの場合、メッセージはURIBLクエリから除外されます。差出人がホワイトリストにある場合でもURIBLホストに問い合わせる時には、このオプションを無効にします。

認証されたセッションからのメッセージを除外する
SMTP到達しているセッションが認証された時、メッセージをURIBLクエリから除外したい場合、このオプションをチェックします。デフォルトでは、このオプションは無効です。

ドメインメールサーバからのメッセージを除外する
デフォルトで、URIBLクエリは、受信メールおよびドメインメールサーバ 65両方に対し実行します。ドメインメールサーバから到着しているメッセージをURIBLクエリから除外したい場合、このボックスを選択します。

URIブラックリスト(全ドメイン)
このセクションは、SecurityGatewayによって問い合わせるURIBLホストの一覧を示します。

新規
新規のURIブラックリストを追加するために、**新規**ボタンをクリックします。これは、URIブラックリストエディタ[143](下記参照)を開きます。

編集
URIブラックリストを編集するには、編集するエントリを選択し、**編集**ボタンをクリックします。これは、エントリ編集のためにURIブラックリストエディタ[143]を開きます。

削除
URIブラックリストを削除するには、削除したいエントリを選択し、**削除**ボタンをクリックします。

例外 – ドメイン

これらの設定を構成する時、ページ上部の**ドメイン**:ドロップダウンリストボックスで、特定のドメインを選択する場合、そのドメインは設定を保存した後、ここに一覧を示されます。URIブラックリスト設定を見直し編集するには、対応するドメインの**表示 / 編集**リンクをクリック、あるいはデフォルトの全体の設定値をドメインの設定にリセットするには、**リセット**をクリックします。

URIブラックリストエディタ

URIブラックリストページで**新規**または**編集**をクリックすると、新規URIブラックリストの追加や既存のブラックリスト編集のためにブラックリストエディタを開きます。

保存して閉じる
ブラックリストの設定の追加または変更後、このボタンで、変更を保存しエディタを閉じます。

閉じる
行った変更を保存しないで、エディタを閉じるには、このボタンをクリックします。

URIブラックリスト

このURIブラックリストに対しクエリを有効にする
URIブラックリストを有効/無効にするには、このオプションを使用します。エントリについて、このチェックボックスを解除する場合、リストから削除されませんが、SecurityGatewayによってURIブラックリストの問い合わせをしません。

URIBL名:
これは、問い合わせをする特定のURIブラックリストの名です。

ホスト名またはIP:
これは、メッセージで検出するURIを確認する時に、SecurityGatewayによって問い合わせる、このURIブラックリストエントリに対応するホスト名またはIPアドレスです。

スコア:
URIBLスコアは、このURIBLに関連した指定された数値で、クエリでメッセージがブラックリストにあるURIを検出した時に使われます。URIブラックリストページで[...**URIBLエンジンによって戻されるスコアをメッセージスコアへ追加する**]オプションを無効にしない限り、この数値は最終的なメッセージスコア[150]に追加されます。

Bitmask:
Bitmask数値は、複数のリストが単一のビットマスクされたリストに結合される時、どのリストまたはデータソースが問い合わせられているかについて識別する使用します。具体的には、SURBLデータソースのすべては、以下で結合されます: *multi.surbl.org*g。これに関する詳細な情報については、www.surbl.orgを参照してください。問い合わせするURIBLが単一のリストだけに情報を持つ場合、0が使われます。

クエリの実行前にIPアドレスのURIを解決する
このURIブラックリストを問い合わせる前にメッセージで含まれるURIのIPアドレスを解決したいか、または検索する場合、このオプションを使用します。DNSBL[138]に同様、一部のURIBLは、IPアドレスを保存しますが、送信するメールサーバのアドレスではなくメッセージで含まれるURIアドレスを保存します。

4.1.5 グレーリスト

グレーリストは、一時的なエラーが発生した送信メールサーバ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。その理論は、全体として、スパムツールが配信を再試行しないが、正当なメールでは再試行を行います。この技術を使用すると、メッセージが非ホワイトリストあるいは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によって拒否されます。さらに、指定した時間（分）以降の配信の試行も拒否されます。メッセージが拒否される時はスパマーが一般的にそれ以上配信の試みをしないので、グレーリストはユーザが受信するスパムの量を減らすことに役立ちます。しかし、スパマーが後ほど配信を再試行する場合も、その時までには、スパマーが識別される可能性もあり、他のスパム対策オプション（例えばDNSブラックリスト）は、適切にブロックします。

スパムを減らすグレーリストにもかかわらず、正当および重要なメッセージの遅延を起こす可能性があることに注意してください。しかし、グレーリストの有効期間が失効後、正当なメッセージは今まで通り配信され、差出人が指定された日数で、その受信者に別のメッセージを送信し失敗しない限り、これ以上の遅延は、再びその同じサーバ/差出人/受信者の組合せに対して行いません。メッセージが遅延する場合、送信サーバが、配信試みをする前に、どれほどの期間を待つか、知ることができない点に注意することが重要です。一時的なエラーコードでメッセージを故意に拒否することが、2,3分、または全日遅延する可能性があります。このようなことでグレーリストと関連する他の潜在的な問題のため、SecurityGatewayでは、デフォルトで、この機能は無効です。ただし、潜在的な問題を処理するように設計された、いくつかのオプションがあります。

最初に、一部の送信ドメインは、アウトバウンドメールを送信するために、メールシステムを使用します。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、各試行はグレーリストエンジンに対し新しい接続として扱われます。これは、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。Sender Policy Framework（SPF）ルックアップオプションを利用することによって、この問題は、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、グレーリストの効率は下がりますが、メールシステム問題を完全に解決することができます。

次に、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、大容量データベースを必要とします。SecurityGateway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、SecurityGatewayで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、ほとんど実用的な性能に影響しません。

最後に、正当な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。例えば、メッセージが、ホワイトリストの差出人から、または認証されたセッションを通じて到達している場合に除外するオプション、および、ドメインメールサーバから到着しているメッセージは、常に除外されています。

グレーリストに関する詳細な情報については、

http://en.wikipedia.org/wiki/Greylisting

設定

グレーリストを有効にする

グレーリスト機能を有効にするには、このオプションをクリックします。グレーリストは、デフォルトで無効です。

指定時間内に一時的なエラーで初期配信の試行を延期する

各サーバ/差出人/受信者の組合せ(「トリプレット」)が初期の配信試みの後、グレーリスト化される時間(分)を指定するには、このオプションを使用します。その時間の間、同じトリプレットによる任意の以降の配信試みは、一時的なエラーコードで拒否されます。指定された時間が経過した後、グレーリストデータベースレコードが失効しない限り、グレーリストの遅延は、そのトリプレットで実施されません。このオプションのデフォルト値は15分です。

指定日数以降で未使用のグレーリストデータベースレコードを削除する[xx]日

一度グレーリスト化されたトリプレットが、初期のグレーリスト期間を経過した後、そのトリプレットレコードに適合しているメッセージが、この日数の間に送信しない限り、遅延は発生しません。例えば、この数値が10日に設定される場合、10日ごとに、その同じサーバ/差出人/受信者の組合せに合致している少なくとも一つのメッセージが受信される限り、遅延はありません。ただし、その期間にメッセージ送信がない場合、レコードは失効し遅延から再び除外する前に、そのトリプレットは別のグレーリスト期間を通過しなければなりません。失効するまでの未使用レコードのデフォルトの期間は10日です。

グレーリスト(単にMAILおよびRCPT値を使用)の場合にIPアドレスを無視する

グレーリストパラメータのうちの1つとして送信サーバのIPアドレスを使用しない場合、このチェックボックスを選択します。これはメールサーバにより発生する可能性のある潜在的な問題を解決しますが、グレーリストの効率を減らします。このオプションはデフォルトで無効です。

SPFに処理を渡す接続に対しIPアドレスを無視する

このオプションを使用する場合、差出人および受信者だけが、送信サーバがSPF処理159を渡すグレーリストに使われ、IPアドレスは無視されます。このオプションはデフォルトで有効です。

除外

ホワイトリストの差出人からのメッセージを除外する

ホワイトリスト221にある差出人からのメッセージは、デフォルトでグレーリストから除外されます(配信が遅延しないことにより)。ホワイトリストにある差出人をグレーリストから除外しない場合、このチェックボックスを解除します。

認証されたセッションからのメッセージを除外する

デフォルトで、認証されたセッションを通じて到達しているメッセージは、グレーリストから除外されます。セッションが認証される場合にグレーリストからのメッセージを除外しない場合、このチェックボックスを解除します。

ドメインサーバからのメッセージを除外する
ドメインメールサーバ[65]から到着しているメッセージは、グレーリストから常に除外されます。

例外 - ドメイン
これらの設定を構成する時、ページ上部のドメイン:ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。グレーリスト設定を見直し編集するには、対応するドメインの**表示 / 編集**リンクをクリック、あるいはデフォルトの全体の設定値をドメインの設定にリセットするには、**リセット**をクリックします。

4.1.6 メッセージ証明書

メッセージ証明書とは対象のメールが正しく処理された事を保証もしくは証明するためのプロセスです。その結果、信頼できるソースによって保証されたドメインから送られたメールは、それほど疑う必要がなくなります。つまり、受信サーバーは送信元ドメインがメールの標準規格に適合しており、スパムや不正なメールを送信していないものである事を確認する必要があります。証明書はメールが誤検知などの不必要な理由によりスパムとして検出されるのを防ぐのに大変便利です。また、各メールに対する処理にかかるリソースを抑える事もできます。

SecurityGatewayは、MDaemon社が参加しているDomain Assurance Council（DAC）への登録を進めている、"Vouch-By-Reference"（VBR）と呼ばれる新しいインターネットメールプロトコルを含む、メッセージ証明書に対応しています。VBRはCertification Service Providers（CSP）や「認証局」を通じて、対象ドメインが正規のものであると保証するためのメカニズムを提供しています。

CSPによって保証を要求する差出人からのメッセージは信頼されているDKIM署名[163]またはSPF[159]サーバから送信される必要があります。これは、メッセージの送信が、偽造ではなく正規のドメインからであることを保証するために必要です。

受信メールの証明

Certification Service Provider（CSP）を指定していて、送信元がCSPで証明され、証明書も正規なものだった場合、そのドメインから受信したメールはSecurityGatewayのスパムチェックから一部除外されます。スパムチェックから除外する代わりに、対象ドメインからのメールはスパムである可能性が低いという事から、指定の値をスパムスコアから差し引く事もできます。

送信メールの証明

SecurityGatewayが対象ドメインの送信メールに証明書データを挿入する前に、ドメインを証明するためのCSPの設定が必要です。CSPへ登録を行った後、SecurityGatewayで対象ドメインの送信メールへ証明書を挿入するには:

1. ドメインが送信メールへDKIM[163]署名を付与するよう設定されているかどうかを確認してください。または、ドメインのDNSレコードが、メッセージをSPF[159]承認サーバから送信されていることを明示するために適切に構成されることを確認します。これは、メッセージがユーザから由来したことを保証するために必要です。受信サーバは、最初にメールが意図したドメインから送信されたものである事を確定できない限り、保証することができません。
2. SecurityGatewayでは、左のナビゲーションペインで、メッセージ証明書ページへ切り替えるために、**セキュリティ ≫メッセージ証明書**をクリックします。
3. ページの右上のドメイン:ドロップダウンリストボックスでドメインを選択します。

4. ページ下部の送信メッセージセクションにおいて、**送信メッセージに証明書データを挿入する**をクリックします。
5. メッセージオプションを保証する証明書サービスのホスト名で、テキスト入力ボックスで各ホストを区切って、ドメインのメールを保証する一つ以上CSPに対応するホストを入力します。
6. **保存**をクリックします。

VBRでは署名付きのメールをCSPへ送信する必要がありません。CSPはドメインの証明のみを行い、特定のメールに対して署名や証明を行いません。

受信メッセージ

このドメインに対しグローバルに定義したデフォルト設定を使用する
特定のドメインのメッセージ証明書設定を編集する場合、このドメイン宛の受信メッセージに対しグローバル設定を適用する場合、このオプションを選択します。ページの上部の**ドメイン**:ドロップダウンリストボックスからドメインを選択する場合に、このオプションを参照することができます。

このドメインで次のカスタム設定を使用する
特定のドメインのメッセージ証明書設定を編集する時に、グローバル設定の使用ではなく、このドメイン宛の受信メッセージに対する設定をカスタマイズする場合、このオプションをクリックします。このオプションは、ページの上部の"ドメイン"ドロップダウンリストボックスからドメインを選択した時だけ表示します。

受信メッセージの証明書を有効にする
デフォルトで、メッセージが信頼するCSPのうちの1つによって保証される差出人がである場合、SecurityGatewayは確認することを試みます。受信メッセージにメッセージ証明書を使用しない場合、このチェックボックスを解除します。

信頼する証明書サービスのホスト名(スペース区切り):
信頼するすべてのCSPのホスト名を、カンマ区切りで指定するために、このテキスト入力ボックスを使用します。

差出人が保証される場合:
信頼されたCSPの1つによって保証されるメッセージの差出人を判定する場合にSecurityGatewayを利用する場合、下記のオプションを選択します。

...スパムフィルタリングから除外
このオプションが選択される場合、証明された差出人からのメッセージはSecurityGatewayのスパム防止ツールの一部から免除されます。これは、デフォルトオプションです。

...この値を追加 [xx]
証明されたメッセージを免除しない場合、メッセージスコア150に追加される値を指定するために、このオプションを使用します。それらは、スパムである可能性がないので、証明されたメッセージが有益な調整を受信するように、これは負の数です。デフォルト設定は、"-3.0"です。

送信メッセージ

このセクションのオプションは、ページ上部でドメイン:ドロップダウンでドメインを選択している場合のみ利用可能です。送信メールについては、グローバルメッセージ証明書は使用できません。

送信メッセージに証明書データを挿入する
このドメインの送信メッセージのすべてにメッセージ証明書データを挿入する場合、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です。

メッセージを保証する証明書サービスのホスト名
テキスト入力ボックスに各ホストを区切って、ドメインのメールを保証する一つ以上CSPに対応するホストを入力するために、このテキストフィールドを使用します。

例外 – ドメイン

これらの設定を構成する時、ページ上部のドメイン:ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。メッセージ証明書の設定を見直し編集するには、対応するドメインの**表示 / 編集**リンクをクリックするか、デフォルトの全体の設定値をドメインの設定に上書きするのに、**リセット**をクリックします。

4.1.7 Backscatter Protection

Backscatter

Backscatter((BP):後方散乱メール)」は、一度も送信していないメールに対しての応答メールを意味します。スパムメールやウィルスメールで指定された「Return-Path」アドレスが偽装された結果、BackScatterメールが送信されます。結果としてこれらのメッセージが宛先サーバーで拒否されたり自動応答で返されたりすると、応答メールは偽装されたアドレスに対して送信されます。こうして、膨大なエラー通知や自動応答メールがユーザーのメールボックスをいっぱいにするまで送信されます。さらに、スパムやウィルスの制作者は、この事象を利用して、特定のサーバーに対してサービス不能(DoS)攻撃を仕掛ける場合もあります。

Backscatter Protection

Backscatterを防止するために、SecurityGatewayはBackscatter Protection(BP)という機能を搭載しています。BPは、正当な配信状態通知および自動応答者が、ユーザの発信メッセージの"Return-Path"アドレスに、特別な時間依存のコードを生成および挿入する方法をハッシュ計算しているプライベートキーを使用することによりアカウントに配信されることを確認するために役立ちます。これらのメッセージ1つが配信問題に遭遇し戻される場合、あるいは、自動応答が"mailer-daemon@...."あるいは無効なリバースパスで受信される場合、ドメインのうちの1つによって送信されたメッセージに対する本物の自動化されたリプライであるように、特別コードを参照および識別します。メッセージが特別なコードを含まない場合、またはコードが失効した場合、記録され拒否することができます。

設定

Backscatter Protectionを有効にする
Backscatter Protectionを有効にする場合、このチェックボックスを選択します。
SecurityGatewayはその時、すべての送信メッセージのリターンパスに特別なコードを生成し挿入を開始し、すべての返されたメッセージでそのコードを探します。Backscatter保護は、デフォルトで無効にされています。

このオプションを無効にしていると、SecurityGatewayで送信メールへBackscatter Protection用コードを挿入しません。ただし、有効なコードが付与されている受信メールが誤って拒否される事がないよう、DSNや自動応答メールは継続して確認します。

Backscatter Protection検証に失敗したメールを拒否する
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。特別なコードを含まない場合、または、コードのライフサイクルが失効した場合、"mailer-daemon@..."を持つメッセージまたはNULLリバースパスは失敗します。Backscatter Protection堅固な信頼性のため、メッセージが有効であってもなくても、誤検出または「グレーエリア」はありません。この理由で、送信メッセージすべてで特別BPコードを含むことを確認する限り、無効なメッセージを拒否するために、SecurityGatewayを構成することは安全確実です。すべての場合において、しかしながら、BP検証に失敗するメッセージを拒否しない選択をした場合でもBP検証の結果は記録されます。

Backscatter保護を使用可能にする場合、BP検証を失敗する自動応答メッセージを拒否する設定前に、約1週前に延期されます。Backscatter Protectionがアクティブにされる前、その期間中に送信されたメッセージに今まで通りDSNあるいは自動応答を受信する可能性があるからです。その期間中に無効なメッセージを拒否するために構成される場合、正当な応答メッセージは誤って拒否されます。1週間後に、無効なメッセージを拒否し始めることは信頼できます。新規のBPキーを作成するが、**前回のBackscatter Protection暗号キーを保持する**オプションの使用を選択しない場合、この同じ警告は適用されます。

指定日数毎に新規のBackscatter Protection暗号キーを作成する[xx]日
デフォルトによって新規のBackscatter Protection暗号化キーは、7日おきに生成されます。新規のキーは、すべて新規の送信メッセージについてBPコードを生成に使用します。

前回のBackscatter Protection暗号キーを保持する[xx]日
デフォルトでSecurityGatewayでは、新規の暗号化キーが生成されたあと、7日間、前の暗号化キーで生成されたBackscatter Protectionコードを含んでいるメッセージを確認することを継続します。これは、新規のキーが生成される時はいつでも、有効なメッセージが偶然に拒否されないことを確実にするのに役立ちます。このオプションを無効にすることは推奨しません(上記の[**Backscatter Protection検証に失敗したメールを拒否する**]オプションを参照)。

すぐに新規のBackscatter Protection暗号キーを作成するには、ここをクリックしてください
手動で新規のBackscatter Protectionキーを生成するために、このオプションをクリックします。上記の**前回のBackscatter Protection暗号キーを保持する[xx]日**オプションが有効にする場

合、前のキーによって生成されるコードを含んでいるメッセージは、そのオプションで指定される日数の間有効な状態を維持します。

例外

全体のホワイトリストにあるIPアドレスおよびホストからメッセージを除外
デフォルトでBackscatter Protectionが有効にする場合、グローバルのホワイトリスト[221]IPアドレスおよびホストから到着する、すべてのメッセージはBackscatter Protection規制から除外されます。ホワイトリストIPおよびホスト規制を厳守する場合、このチェックボックスを解除します。

認証されたセッションからのメッセージを除外する
受信メッセージが認証されたセッションを通じて送信されている場合、デフォルトでBackscatter Protection規制から除外されます。同様に認証されたセッションに、規制を適用する場合、このチェックボックスを解除します。

ドメインメールサーバからのメッセージを除外する
Backscatter Protectionが有効な場合、ドメインメールサーバ[65]からの受信メッセージは、デフォルトでBackscatter Protection規制から除外されます。ドメインメールサーバをBackscatter Protectionチェックから除外しない場合、このチェックボックスを解除します。

メッセージのReturn Path署名

指定日数毎に新規のBackscatter Protection暗号キーを作成する
デフォルトで新しいBackscatter Protection暗号キーは7日毎に生成されます。新しいキーは送信メール全てに使用されるBPコードとして使用されます。

前回のBackscatter Protection暗号キーを保持する
デフォルトでSecurityGatewayは新しく暗号キーが生成された後でも、7日間はこれを正規のものとして検証します。これで、正規のメールが誤って拒否されてしまう事がなくなります。このオプションを無効にするのはお勧めしていません。(上記のBackScatter Protection検証に失敗したメールを拒否、の下に記載されている注意事項をご確認下さい。)

下記のIPやドメインにはメールへreturn-pathの署名を行わないで下さい。
このオプションでBackscatter Protectionのreturn-path署名から除外するIPアドレスやドメイン名を指定します。

4.1.8 メッセージスコア

SecurityGatewayは、メッセージを処理している間、実行する若干のテストに基づいて各メッセージに対してメッセージスコアを計算します。そのスコアは、メッセージがスパムでいるという可能性を決定するために用いる「スパムスコア」です。ヒューリスティックおよびベイジアン[132]、DNSBL[138]、IDKIM検証 Verification[162]および多くの他のセキュリティ[126]オプションは、メッセージスコアを変更するために、設定することができます。メッセージのスコアが特定のしきい値を上回る場合、管理される処置を指定するために、このページでオプションを使用します。しきい値をスパムとしてメッセージにタグを付けるか、隔離またはSMTPセッション中に拒否を設定することができます。ホワイトリストの送信者からのメッセージ、認証済みセッション、または送信メッセージの場合、同様に、メッセージスコアからの制限を除外する設定ができます。メッセージスコアオプションはグローバルでも特定のドメインでも設定できます。

設定

最終的なメッセージセージスコアに基づく処理を有効にする
デフォルトで、下記で指定されるスコアのしきい値に従って、SecurityGatewayはスコアを、各メッセージに割り当て、そのスコアに基づき処置を行います。メッセージスコアに処置を行わない場合、このチェックボックスを解除します。

指定スコア以上でメッセージを拒否する[スコア]
デフォルトで、12.0以上の最終スコアをもつメッセージは、SMTPセッション中に拒否されます。これを選択する場合、この値を調整することができ、またはメッセージスコアで拒否しない場合、オプションを無効にすることができます。

指定スコア以上でメッセージを隔離する[スコア]
メッセージスコアが5.0以上では、デフォルトで隔離されます。この値は調整することができ、またはメッセージスコアで拒否しない場合、オプションを無効にすることができます。同様に上記の"**指定スコア以上でメッセージを拒否する**"オプションを使用している場合、スコアが、この隔離しきい値と上記の拒否しきい値の間の場合は、隔離されます。拒否しきい値以上のメッセージスコアは、拒否されます。

指定スコア以上でメッセージにSubjectタグを追加する[スコア]
最終スコアが、この値以上の時にメッセージのサブジェクトに一部のテキストを追加する場合、このオプションをクリックします。デフォルト値は5.0ですが、オプションはデフォルトで無効です。

Subjectタグ:

上記の"**指定スコア以上でメッセージにSubjectタグを追加する**"オプションが有効な場合、これはスコアが、指定するしきい値以上の場合に追加されるテキストです。このオプションで追加されるデフォルトテキストは"*** SPAM ***"です。

サブジェクトヘッダにテキストを任意に追加することができる別の設定があります。例えば、DNSブラックリスト(DNSBL)[138]およびURIブラックリスト(URIBL)[141]ページは、同様に、このオプションを持ちます。これらのオプションの指定されたテキストが合致する場合、そのメッセージが各オプションのもとに基準を満たす場合であっても、テキストは一度メッセージのサブジェクトに追加されるだけです。ただし、別のオプションでテキストを変更する場合、その変更したテキストは追加されます。従って、例えば、3つのオプションすべてに"*SPAM*"テキストを設定する場合、オプションのうちの1つ以上で基準に合致したか問わず、そのテキストは一度サブジェクトに追加されるだけです。しかし、"*URI blacklisted*"にURIBL任意のテキストを変更し、そのオプションと他のものとで基準に合致する場合、サブジェクトは"*SPAM*"および"*URI blacklisted*"を持ちます。

除外

ホワイトリストの差出人からのメッセージを除外する
メッセージが、ホワイトリスト[221]の差出人からの場合、デフォルトで、メッセージスコア制限から除外されます。ホワイトリストの差出人からのメッセージを除外しない場合は、このチェックボックスを解除します。

認証されたセッションからのメッセージを除外する
デフォルトで、認証されたSMTPセッションを通じて送信されているメッセージは、メッセージスコア制限から除外されます。これらのメッセージを除外しない場合、このチェックボックスを解除します。

ドメインメールサーバからのメッセージを除外する
ドメインメールサーバから到着しているすべてのメッセージをメッセージスコア制限から除外する場合、このチェックボックスを選択します。このオプションは、デフォルトで無効です。

例外 - ドメイン

これらの設定を構成する時、ページ上部のドメイン:ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。メッセージスコア設定を見直し編集するには、対応するドメインの**表示/編集**リンクをクリック、あるいはデフォルトの全体の設定値をドメインの設定にリセットするには、**リセット**をクリックします。

4.2 ウィルス対策

セキュリティ[126]メニューのアンチウィルスセクションでは、ウィルス感染したメールを検出しユーザーへの到達を防ぐためのオプションが設定できます。ユーザへ届くことを防止するオプションがあります。アンチウィルスセクションには2つの項目があります。

ウィルススキャン[152] - ウィルスに対して広範囲での対策を行うため、SecurityGatewayはClam AntiVirus (ClamAV™)およびIKARUSアンチウィルスの2つのアンチウィルスエンジンに対応しています。ClamAVは特にメールゲートウェイ用のオープンソース(GPL)アンチウィルスエンジンです。IKARUSアンチウィルスは、悪意のあるプログラムや潜在的な危険性のあるプログラムからシステムを保護する事ができます。2つのエンジンを搭載する事により、従来の方式と新しい方式の2通りを組み合わせたウィルス対策が行えます。さらに、SecurityGatewayでは、ウィルス感染を防ぐための追加レイヤーが、Outbreak Protection[128]で提供されています。

更新設定[155] - ウィルスの脅威が突然発生した場合、期限切れのウィルスデータベースではウィルスが検出できないリスクがあります。そのため、ウィルスシグニチャファイルの定期的なアップデートは大変重要です。更新の設定ページのオプションを使って、SecurityGatewayからウィルスのシグニチャファイルの自動アップデート、アップデートの即時確認、アンチウィルスのアップデートログの確認が行えます。

4.2.1 ウィルススキャン

ウィルス対策機能として、SecurityGatewayにはClam AntiVirus（ClamAV™）とIKARUSアンチウィルスの2つのアンチウィルスエンジンが搭載されています。ClamAVはオープンソース（GPL）でメールゲートウェイ用に特化したアンチウィルスのツールキットです。IKARUSアンチウィルスは悪意のあるプログラムや潜在的に危険性の高いプログラムから安定した保護機能を提供しています。これにより従来のアンチウィルス機能と最新の事前保護技術の両方を組み合わせています。SecurityGatewayには Outbreak Protection[128]も搭載されており、ウィルス感染を防ぐための追加レイヤーを提供しています。

設定

ウィルススキャンを有効にする
ウィルススキャンはデフォルトで使用可能です。ウィルスに対してメッセージをスキャンしない場合、このチェックボックスを解除します。

メッセージが感染していると判断した時:
メッセージにウィルスが検出された場合、必要とする処置を指定するために、このオプションを使用します。

後述の"感染したメッセージの駆除を試みる"オプションを有効にすると、直ちに拒否または隔離するのではなく、SecurityGatewayは最初に感染したメッセージを駆除(すなわち、ウィルスだけを削除)しようとします。成功すると、メッセージは通常通り配信されます。メッセージからウィルスだけを駆除できなかった場合、メッセージは拒否または隔離されます。

...メッセージを拒否
このオプションが選択される場合、ウィルスが検出されるとSMTPセッション中に拒否されます。これは、デフォルトオプションです。

1つのアンチウィルスエンジンでウィルスチェックが行えたならメッセージ通過を許可する
このオプションを有効にすると、1つのアンチウィルスエンジンでのスキャンに成功したメッセージが、その後のウィルスチェックを通過できるようになります。このオプションが有効でない場合は、どちらかのエンジンでスキャンに失敗した場合、メールは隔離されます。

...メッセージを隔離
拒否ではなく管理隔離 251で感染したメッセージを判別する場合、このオプションを選択します。

スキャンできないメッセージを隔離する
なんらかの理由でアンチウィルスエンジンによってスキャンできない場合、このオプションを選択します。この種のメッセージの一例は、パスワード保護されているZIPファイルの添付がある場合です。このオプションが無効にされる場合、スキャンできないメッセージは通常配信されます。このオプションは、デフォルトで有効です。

以下のファイルを除外
特定のファイルやファイルの種類をスキャンできないメッセージを隔離する設定から除外する場合はこのオプションを使用します。*.zip, secret?.zip, *.doc?のようなファイルマスクやワイルドカードが使用できます。

感染したメッセージの駆除を試みる

デフォルトで、SecurityGatewayでは、拒否や隔離でなく、感染したメールからウィルスの駆除を試みます。正常に駆除できると、メールは通常配信されます。メッセージから駆除ができない場合、上記で選択したオプションに応じて、拒否または隔離します。感染したメッセージから駆除をしない場合、このチェックボックスを解除します。その場合は感染しているメッセージは、直ちに拒否または隔離されます。

ウィルスのようなマクロを含むドキュメントを持つ添付ファイルにフラグを付ける

ウィルスのスキャンでドキュメントのマクロを検出するにはこのオプションを使用します。

除外

ホワイトリストIPアドレスからのメッセージはスキャンしない

ホワイトリストIPアドレス[226]から到着するメッセージを、ウィルススキャンから除外したい場合、このオプションを有効にします。

ドメインメールサーバからのメッセージはスキャンしない

ドメインメールサーバ[65]から届くメッセージのウィルススキャンを除外する場合は、このオプションを有効にします。

以下のリストにあるメールアドレスからのメッセージを除外する

特定の送信元アドレスから届くメールをウィルススキャンから除外したい場合、このオプションを有効にします。

ウィルススキャンエンジン(全ドメイン)

メッセージのスキャンにClamAVエンジンを使用する

デフォルトで、SecurityGatewayはClamAVアンチウィルスエンジンをメッセージのウィルススキャンに使用します。メッセージスキャンにClamAVエンジンを使用しない場合、このチェックボックスを解除します。

メッセージのスキャンにIKARUSアンチウィルスエンジンを使用する

デフォルトで、SecurityGatewayはIKARUSアンチウィルスをメッセージのウィルススキャンに使用します。メッセージスキャンにIKARUSアンチウィルスを使用しない場合、このチェックボックスを解除します。

これらのオプションが両方とも有効であるという事は、SecurityGatewayで、エンジン毎に1回づつ、合計二回各メッセージをスキャンすることを意味します。これは、1つのエンジンがウィルス検知に失敗した場合のエクストラレイヤーとなります。

例外 - ドメイン

これらの設定を構成する時、ページ上部のドメイン:ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。ウィルススキャン

設定を見直し編集するには、対応するドメインの**表示/編集**リンクをクリック、あるいはデフォルトの全体の設定値をドメインの設定にリセットするには、**リセット**をクリックします。

4.2.2 アップデートの設定

ウィルスの脅威が突如発生し、古いシグネチャデータベースのままでは、シグネチャに存在しないウィルス感染を起こす可能性があります。そのため、定期的にウィルスシグネチャ更新は非常に重要です。このページでは自動的にウィルスシグネチャの更新チェックを行ったり、緊急アップデートを実施したり、アップデートログの確認を行う事ができます。**注意点：このオプションはClam AVエンジンにのみ有効です。IKARUSアンチウィルスエンジンは10分毎に最新版のチェックを行います。**

シグネチャの更新

ウィルスシグネチャの自動更新を有効にする
SecurityGatewayが一定間隔でClamAVのシグニチャファイルのアップデートを確認できるようにするには、このオプションを使用します。最新のシグニチャファイルは、1時間又は1日に1回自動で確認できます。この自動アップデート機能はデフォルトで有効に設定されています。Use

毎時間 -指定時間後 [xx]分から1時間後
デフォルトで、時間（このオプションで指定）後の指定された時間（分）で、SecurityGatewayはClamAVのシグニチャファイルのアップデートチェックを行います。例えば、このオプションで29を使用する場合、1時間ごとのチェックは1:29、2:29のように実行されます。このオプションでランダムな値を生成するには[ランダムな時間を生成]をクリックします。

毎日 -時間 [xx:xx]
更新されたウィルスシグネチャについて、このオプションが指定され、1日につき1回を確認したい場合、このオプションを使用します。時間指定は24時間制で指定する必要があります。例えば、このオプションで13:05を使用する場合、デイリーチェックは午後1時05分に実行されます。このオプションでランダムな値を生成するには[ランダムな時間を生成]をクリックします。

すぐに更新されたウィルスシグネチャの更新をチェック
ウィルスシグネチャファイルのアップデートチェックをすぐに行うには、このリンクを使用します。この即時チェックは、上記で設定した自動アップデートチェックとは別に実行されます。

ClamAVの更新されたログファイルを表示
Clamアンチウィルスの最新版ログを閲覧するために、このリンクを選択します。

IKARUSアンチウィルス更新ログファイルを表示
IKARUSアンチウィルスの最新版ログを表示するにはこのリンクを使用します。

4.3 なりすまし対策

セキュリティ126メニューの「なりすまし対策」セクションでは、偽造や「なりすまし」アドレスからのメールを判定するためのツールをご利用いただけます。このセクションには以下の6つの「なりすまし」対策機能があります。

リバースルックアップ157 – これらのルックアップオプションを使用して、差出人のドメインが実際に存在するか、さらに送信サーバのIPアドレスが、そのドメインと関連付けされているかどうかを確認できます。

Sender Policy Framework (SPF)159 – SPFは、メールメッセージで偽造された差出人アドレスを確認する使用するオープンスタンダードです。具体的には、SMTP envelope差出人アドレスまたはリターンパスで見つけ出されるドメインを保護します。どのメールホストが、ドメインのためにメッセージを送信することを許可しているか、SPFポリシーが正確に見つけ出すドメインのDNSレコードを確認することで、これを実行します。ドメインはSPFポリシーを持ち、送信ホストはそのポリシーで一覧を示されない場合、偽造した場合に、そのアドレスを知ることができます。

DKIM検証 162– この機能で受信メールのDomainKeys Identified Mail (DKIM)署名を確認できます。受信メールが暗号で署名されていると、SecurityGatewayはパブリックキーを署名を付与したドメインから取得し、DKIM署名の正当性を検証します。DKIM署名が検証テストを通過すると、メールは通常配信処理の次のステップへ進み、メッセージスコア150が調整されます。DKIM検証は、メッセージ送信者の正当性の確認だけでなく、署名された時間と配信された時間との間で書き換えられていなかったかどうかも確認できます。

DKIM署名 163 - 署名オプションは、ドメインの送信メッセージへDomainKeys Identified Mail (DKIM)を使って暗号化した署名を付与するかどうかを指定するためのオプションです。ドメインのメッセージへの署名用のセレクタやキーの作成、使用するセレクタの選択もここで行えます。

DMARC165 – SecurityGatewayのDMARC検証とレポーティング用の設定が行える、DMARC検証、DMARCレポーティング、DMARC設定の3種類の画面があります。

コールバック検証 177 – これは、受信メッセージの差出人メールアドレスの正当性を判定するなりすまし対策です。これを実行するには、SecurityGatewayは、SMTPセッション中に、"MAIL From"ステートメントで渡されるドメインのメール交換器に接続し、その差出人アドレスが、そのドメインの有効なアドレスであるどうか照合を試みます。チェック結果が差出人のアドレスが存在しないことを示す場合、偽造されたアドレスから送信されているかのように、SecurityGatewayでメッセージを扱うことができ、従って、メッセージの拒否、隔離、またはメッセージを受け入れオプションで、メッセージスコア150を調整しサブジェクトにタグを追加します。

From ヘッダスクリーニング 179 – このページでは、メールを正規の送信元からだとだますための、スパム送信者からの不正な(偽装された)「From」ヘッダを持つメールを防ぐための設定が行えます。

4.3.1 リバースルックアップ

PTR

受信SMTP接続でリバースPTRレコードルックアップを実行する
デフォルトでSecurityGatewayは、すべての受信SMTP接続でポインタレコードルックアップを実行します。これを実行しない場合、このオプションを解除します。

PTRレコードの一致がない場合501を送信し接続を閉じる(注意)
このチェックボックスを選択する場合、SecurityGatewayは501エラーコード(パラメータまたは引数における構文エラー)を送信し、ドメインでPTRレコードがない場合、接続を閉じます。このオプションは、デフォルトで無効です。

PTRレコードの一致がない場合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(ポインタ)レコードのルックアップの結果が一致しない場合、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。このオプションは、デフォルトで無効です。

認証されたセッションでは懲罰的措置を除外する
このチェックボックスが有効な場合、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SecurityGatewayは、SMTP MAILコマンドの後まで受信SMTP接続でPTRルックアップを延期します。セッションが認証される場合、いかなる懲罰的な処置も差出人に対してとられません。このオプションは、デフォルトで無効です。

グローバルのホワイトリストのIPアドレスは厳罰処置を除外する
グローバルホワイトリストIPアドレス[38]をPTRレコードルックアップから除外する場合、このチェックボックスを選択します。このオプションはデフォルトで無効です。

HELO/EHLO

HELO/EHLOドメインでルックアップを実行する
デフォルトでSecurityGatewayは、セッションのHELO/EHLO処理の間、レポートされるドメイン名でルックアップを実行します。HELO/EHLOコマンドは、サーバにレポートされるドメイン名自体を確認するために、クライアント(送信マシン)により使用されます。このコマンドでクライアントに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。これらのルックアップを実行しない場合、このオプションを無効にします。

偽造された識別で501を送信し接続を閉じる(注意)
501エラーコードが送信し、ルックアップの結果が偽造されたIDが現れる場合に接続を閉じるには、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。

> リバースルックアップの結果でサーバが偽造されたIDである時、この結果は多くの場合で適切ではありません。それは、メールサーバが自身のIPアドレスと一致しない値で自身を認識することが非常に一般的だからです。これはISPによる制限や他の正当な理由により起こることです。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。さもないと、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。

ドメインが見つからない場合メールの受け入れを拒否する
ルックアップで"domain not found"という結果になる場合、このオプションを有効にすると、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)とともに、メッセージを拒否します。セッションでは通常どおり最後まで処理を続けます。このオプションはデフォルトで無効です。

...501エラーコードを送信する(通常は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有効にしてください。

...さらに接続を閉じる
リバースルックアップの結果が"ドメインが見つからない"である場合、セッションの進行を許可せず、即座に接続を切断する場合は、このチェックボックスをクリックしてください。

認証されたセッションでは懲罰措置を除外する
このチェックボックスが有効な場合、接続が認証されたものであるか確認するために、SecurityGatewayではSMTP MAILコマンドの後まで受信SMTP接続でルックアップを延期します。セッションが認証される場合、いかなる懲罰的な処置も差出人に対してとられません。このオプションは、デフォルトで無効です。

グローバルのホワイトリストIPアドレスおよびホストでは懲罰措置を除外する
HELO/EHLOドメインでグローバルホワイトリストIPアドレス[38]およびホワイトリストホスト[223]をルックアップから除外する場合、このチェックボックスを選択します。このオプションはデフォルトで無効です。

メール

MAILコマンドで渡される値でルックアップを実行する
デフォルトでSecurityGatewayは、メールトランザクションのMAILコマンド処理中に渡されるドメイン名でルックアップを実行します。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。MAIL値でルックアップを実行しない場合、このオプションを無効にします。

...偽造IDで501を送信し接続を閉じる(注意)
501エラーコードが送信し、ルックアップの結果が偽造されたIDが現れる場合に接続を閉じるには、このチェック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。

> リバースルックアップの結果でサーバが偽造されたIDである時、この結果は多くの場合で適切ではありません。それは、メールサーバが自身のIPアドレスと一致しない値で自身を認識することが非常に一般的だからです。これはISPによる制限や他の正当な理由により起こることです。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。さもないと、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。

ドメインが見つからない場合メールの受け入れを拒否する
デフォルトでは、MAIL値のルックアップで"domain not found"という結果になる場合、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)とともに、メッセージを拒否しま

す。セッションでは通常どおり最後まで処理を続けます。これらのメッセージを拒否しない場合は、チェックボックスを解除します。

...501エラーコードを送信する(通常は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有効にしてください。

...さらに接続を閉じる
ルックアップの結果が"ドメインが見つからない"である場合、セッションの進行を許可せず、即座に接続を切断する場合は、このチェックボックスをクリックしてください。

認証されたセッションからのメッセージを除外する
認証されたセッションを通じて到達しているメッセージは、デフォルトでMAILコマンド値のルックアップから除外されます。それらのメッセージを除外しない場合、このオプションを無効にします。

グローバルホワイトリストの差出人を除外する
任意のグローバルのホワイトリストにある差出人からのメッセージは、デフォルトでルックアップから除外されます。メッセージをそれらの差出人から除外しない場合、このチェックボックスを解除します。

設定

疑わしいメッセージへ警告ヘッダを挿入する
デフォルトで、SecurityGatewayはリバースルックアップに失敗する任意のメッセージに警告ヘッダを挿入します。受信メールサーバまたはクライアントは、メッセージをフィルタするために、このヘッダをオプションで使用することができます。疑わしいメッセージに警告ヘッダを挿入しない場合、このチェックボックスを解除します。

4.3.2 SPF検証

Sender Policy Framework (SPF)は、メールメッセージで偽造された送信者アドレスを確認するために用いるオープンスタンダードです。特に、SMTPエンベロープ送信者アドレスまたはリターンパスで見つかるドメインを保護します。どのメールホストがドメインのためにメッセージを送信することを許可されるかについて、正確に認定するためにSPFポリシーに関してドメインのDNSレコードをチェックすることによって、これを実行します。ドメインがSPFポリシーを持ち、送信ホストがそのポリシーで一覧にされない場合、アドレスが偽造されたことを知ることができます。

SPFについては www.open-spf.org を参照してください。

設定

SPFを使用し送信ホストを検証する
デフォルトで、SecurityGatewayは、送信ホストがその代りにメールを送信する権限を持つか確認するために、送信ドメインのDNSレコードをチェックします。これは、SMTP処理中に渡されるMAIL値で見つけ出されるドメインを使用します。SPF処理を使用しない場合、このチェックボックスを解除します。

SPF処理でHARD FAILを戻す場合:
メッセージのSPF処理がHARD FAILで結果になる場合、次の処置を行います。

...メッセージを拒否
デフォルトで、HARD FAILを受けているメッセージは、SMTPプロセス中に拒否されます。

...メッセージを隔離
HARD FAILを受けるメッセージを隔離する場合、このオプションを選択します。

...メッセージを受け入れる
HARD FAILを受けるメッセージを受諾する場合、このオプションを選択します。その時メッセージのサブジェクトにテキストを挿入することができ、そのメッセージスコアを変更することができます。

...次の文字を件名に付ける [*text*]
HARD FAIL結果を受けるメッセージを受け入れるSecurityGatewayを構成した時、メッセージのサブジェクトの先頭にテキストを追加するためには、このオプションを有効にし、テキストを指定します。有効な場合、サブジェクトに追加されるデフォルトテキストは"*** FRAUD ***"です。このオプションで、タグに基づいてメッセージをフィルタするために、受信者のメールサーバまたはクライアントに任せる可能性があります。このオプションはデフォルトで無効です。

SecurityGatewayでは他にも様々な機能で件名ヘッダへ文字列を付与します。例えば、SPF[159]やメッセージスコア[150]ページにもこのオプションがあります。これらのオプションとして指定した文字列にマッチした場合、複数の条件にマッチしているメッセージだった場合でも、タグはメールの件名に一度だけ付与されます。ただし、文字列がオプションによって異なる場合は、それぞれの独自タグが付与されます。例えば、このオプションのデフォルトテキストは「*** FRAUD ***」ですが、メッセージスコアのデフォルトテキストは「*** SPAM ***」です。2つのタグが異なるため、どちらのオプションにもマッチしたメールへは両方の文字列が追加されます。ただし、どちらかのオプションで追加した文字列を変更した場合、タグは一度だけ追加されます。

...メッセージスコアへ指定ポイントを追加 [xx] ポイント
デフォルトで、HARD FAIL結果を受けるメッセージを受諾するためにSecurityGatewayを構成する時に、この値はそのメッセージスコアに追加されます。最終スコアが十分に高い場合、メッセージスコア[150]設定に応じて、メッセージを隔離または拒否することができます。このオプションのデフォルト値は、5.0です。

SPF処理でSOFT FAILを戻す場合:
メッセージのSPF処理がSOFT FAILに結果としてなる時に、次の処置を行います。

...メッセージを拒否
SOFT FAILを受けているメッセージは、SMTPプロセス中に拒否されます。

...メッセージを隔離
SOFT FAILを受けるメッセージを隔離する場合、このオプションを選択します。

...メッセージを受け入れる
デフォルトで、SOFT FAILを受けるメッセージを受諾する場合、このオプションを選択します。その時メッセージのサブジェクトにテキストを挿入することができ、そのメッセージスコアを変更することができます。

...次の文字を件名に付ける [*text*]
SOFT FAIL結果を受けるメッセージを受け入れる構成した時、メッセージのサブジェクトの先頭にテキストを追加するためには、このオプションを有効にし、テキストを指定します。有効な場合、サブジェクトに追加されるデフォルトテキストは"*** FRAUD ***"です。このオプションで、タグに基づいてメッセージをフィルタするために、受信者のメールサーバまたはクライアントに任せる可能性があります。このオプションは、デフォルトで無効です。

...メッセージスコアへ指定ポイントを追加 [xx] ポイント
デフォルトで、SOFT FAIL結果を受けるメッセージを受諾するためにSecurityGatewayを構成する時に、この値はそのメッセージスコアに追加されます。最終スコアが十分に高い場合、メッセージスコア 150 設定に応じて、メッセージを隔離または拒否することができます。このオプションのデフォルト値は、2.0です。

SPF処理でPASSを戻す場合:

...メッセージスコアへ指定ポイントを追加 [xx] ポイント
メッセージのSPF処理がPASSに結果の時に、メッセージスコアを調整する場合、このオプションをクリックします。これは、負の数で、スコアを減らし有益な調整を与えます。

除外

ホワイトリストIPアドレスからのメッセージを除外する
グローバルIPホワイトリスト 226 へ記載されているIPアドレスをSPF処理から除外する場合、このチェックボックスをクリックします。このオプションは、デフォルトで無効です。

認証されたセッションからのメッセージを除外する
受信メッセージが認証されたセッションを使用する時に、デフォルトでSPF処理条件から除外されます。

ドメインメールサーバからのメッセージを除外する
ドメインメールサーバ 65 から到着しているメッセージは、デフォルトでSPF処理から免除されています。ドメインメールサーバをSPF条件から除外しない場合、このチェックボックスを解除します。

詳細

メッセージへ'Received-SPF'ヘッダを挿入する
デフォルトでメッセージにSPF結果を持つ"Received-SPF"ヘッダは、各メッセージに挿入されます。このヘッダを挿入しない場合、このチェックボックスを解除します。

...SPF結果が'none'の場合は挿入しない
デフォルトで、SPFルックアップの結果が"none"である時に、"Received-SPF"ヘッダは挿入されません。SPFデータが送信者のドメインについて見つけ出されない場合ヘッダを挿入しない場合、このオプションのチェックを解除します。

例外 – ドメイン

これらの設定を構成する時、ページ上部のドメイン:ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。SPF設定を見直し編集するには、対応するドメインの**表示 / 編集**リンクをクリック、あるいはデフォルトの全体の設定値をドメインの設定にリセットするには、**リセット**をクリックします。

4.3.3 DKIM検証

この画面では、SecurityGatewayで受信メールのDomainKey Identified Mail(DKIM)の検証を行うための設定が行えます。この機能が有効で、受信メッセージが暗号署名[163]されている場合、SecurityGateway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、メッセージスコア[150]を適宜調節します。

メッセージに署名がない場合や署名が無効だった場合、SecurityGatewayはFromヘッダのドメインのAuthor Domain Signing Practices(ADSP)レコードから、対象ドメインのメールが署名対象なのかどうかを判断します。ADSPレコードで正しい署名を必須としていてパブリックキーで署名の正当性が確認できなかった場合、メールは「Fail」結果として処理されます。デフォルトで、メールは拒否されますが、SecurityGatewayでは拒否する代わりに隔離又はメッセージスコア[150]を調整へと処理内容を変更できます。

最後に、SecurityGatewayは DKIM Author Domain Signing PracticesのInternet-Draft 06に対応しています。サイトの ADSPレコードが古いドラフトの構文を使用していたり、ADSPレコードが存在していなかったり、下記ADSPオプションが無効だったりしたために、署名がなかったり不正な署名が使われているメールはドメインがメールの一部にのみ署名していたものとして処理します。この時メールは「疑わしくはないもの」として処理されます。Internet-Draft 06 of the DKIM Author Domain Signing PracticesのInternet-Draft 06 については次のURLを参照してください。: tools.ietf.org

DKIMの詳細については次のURLを参照してください。: www.dkim.org

暗号の検証

DomainKeys Identified Mail (DKIM)を使用し生成された署名を検証する
デフォルトでSecurityGatewayは、DKIMを使用して署名[163]されたメッセージを照合します。メッセージでDKIM署名を照合しない場合、このチェックボックスを解除します。

検証でPASSを返す場合:

...メッセージスコアへ指定ポイントを追加 [xx] ポイント
メッセージがDKIM検証からPASS結果を受信する場合メッセージスコアを調整する場合、このオプションを使用します。デフォルトでこのオプションの値は、0.0に設定され、スコアの調整をしないことを意味します。これらのメッセージのスコアを調整する選択をする場合、このオプションで負の数を使用し、メッセージスコアに有益な調整を提供します。例えば、このオプションで-0.5を使用して、.5ポイント最終スコアを下げます。

除外

ホワイトリストIPからのメッセージを除外する
デフォルトで、ホワイトリストIPアドレス[226]から到着しているメッセージは、DKIM検証から免除されます。差出人がIPアドレスホワイトリストにある場合でもDKIM署名を照合する場合、このチェックボックスを解除します。

認証されたセッションからのメッセージを除外する
認証されたSMTPセッションにわたって到達しているメッセージは、デフォルトでDKIM/DK検証から除外されます。SMTPセッションが認証される時にもDKIM/DK署名を照合したい場合、このチェックボックスを解除します。

ドメインメールサーバからのメッセージを除外する
ドメインメールサーバ[65]のうちの1台から到着しているメッセージは、デフォルトでDKIM検証から除外されています。それらのサーバから到着しているメッセージでDKIM署名を照合したい場合、このチェックボックスを解除します。

DKIM検証オプション(全ドメイン)

Verifierはbody length count("l=" tag)を受け入れる
このオプションが有効な場合、受信メッセージのDKIM署名で見つけ出される時、SecurityGatewayはbody length count tagを受け取ります。実際のbody length countがこのタグで含まれている値より大きい場合、SecurityGatewayはタグで指定されている値を照合するだけです。メッセージの残りは、未検証のままです。これはある物がメッセージに追加されたことを示し、結果的に、その未検証の一部は疑わしいものと見なされます。実際のbody length countがこのタグで含まれている値未満の場合、署名は検証(すなわち、"FAIL"結果を受信します)を通過しません。これはメッセージの一部の一部が削除されたことを示します。そして、タグで指定されている値未満のbody length countを生じます。このオプションはデフォルトで無効です。

VerifierはSubjectヘッダを保護するために署名が必要
受信メッセージのDKIM署名が件名を保護する必要がある場合、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です。

例外 – ドメイン

これらの設定を構成する時、ページ上部のドメイン:ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。DKIM検証を見直し編集するには、対応するドメインの**表示/編集**リンクをクリック、あるいはデフォルトの全体の設定値をドメインの設定にリセットするには、**リセット**をクリックします。

4.3.4 DKIM署名

DomainKeys Identified Mail(DKIM)を使ってドメインの送信メールへ電子署名を付与する場合は送信メール署名のページのオプションを使用します。ドメインのメッセージに署名する際のセレクタおよびキーを作成してこのページで選択できます。すべてのキーは固有です – 指定されるセレクタに関係なく、ドメイン毎に異なるセレクタが使用されます。

DKIMの詳細について、以下を参照: www.dkim.org.

DKIM署名

DomainKeys Identified Mail (DKIM)を使用して送信メッセージに署名する
暗号によってドメインの送信メッセージに署名するDomainKeys Identified Mailを使用する場合、このオプションをクリックします。メールへ署名を行うには、SecurityGatewayがSMTP AUTHで認証さ

れたセッションか、ドメインメールサーバー[65]から受け取ったメールである必要があります。これは、署名するメッセージが正規のものである事を確認するためです。

このセレクタを使用してメッセージに署名する:
ドロップダウンリストから、ドメインの署名用に使用するパブリック/プライベートキーのペアを持つセレクタを選択します。新規のセレクタを作成する場合、**新規**ボタンをクリックし、入力ボックスへセレクタ名を入力して、**保存して閉じる**をクリックします。

新規
ドメインのメッセージに署名するために使用する新規のセレクタを作成するために、このボタンをクリックします。入力ボックスへセレクタを入力し**保存**をクリックして、閉じます。

削除
削除するセレクタをドロップダウンリストボックスから選択して、**削除**をクリックします。

このセレクタのDNS設定(パブリックキー)を表示
セレクタを上記のドロップダウンリストボックスから選択し、セレクタのDNS構成を閲覧するために、このリンクをクリックします。これは、ドメインのDNSレコードに置かれる必要があるDKIM情報です。DNSレコードに、この情報なしに、メッセージで署名を検査することはできません。

DNS構成ページは、次の情報を記載します:

DNSのDKIMセレクタレコード:
これは、他のサーバがドメインのDKIM署名メッセージを検査するために必要とする情報です。セレクタ、ドメイン、パブリックキーおよび他の必要な情報を含みます。

送信メッセージに署名する場合、ドメインのDNSレコード内でこの情報を置くことは必要にされます。これがない時には、受信サーバは、署名を検査するいかなる方法も持ちません。DNSレコードに含まれる詳細な情報および他のパラメータについては、www.dkim.org、およびdomainkeys.sourceforge.netのDomainKeys Distribution Optionsページを参照してください。

DKIM署名オプション(全ドメイン)

署名を指定日数誤に無効にする[xx]日("t=" tag, デフォルト 7日)
DKIM署名が有効であるとみなされる日数を制限するために、このオプションを使用します。期限切れの署名によるメッセージは、検証で常に失敗します。このオプションは、"x="がタグ署名に対応します。デフォルトで有効日数は7日に設定されます。

署名にクエリを含む("q=" tagを含む)
このオプションは、DKIM署名(q=dns)でクエリメソッドタグを含むために使用されます。デフォルトで含まれます。

署名にbody length count("l=" tag)含む
このオプションは、body length count("l=" tag)がDKIM署名で含まれるかどうかことコントロールします。このオプションは、デフォルトで有効です。

署名にオリジナルヘッダを含む("z=" tag)
DKIM署名でz=タグを含む場合、このオプションをクリックします。このタグはメッセージの本来のヘッダのコピーを含んで、その結果、非常に重要な署名を潜在的に作成することができます。このオプションは、デフォルトで無効です。

正規化

正規化は、DKIM署名が作成される前に、メッセージのヘッダと本文が正規の規格に変換され[正規化される]プロセスです。いくつかのメールサーバと転送システムは、メッセージの通常処理の間に、様々な小さな変更を行います。そのため、この機能が無ければ、各メッセージの署名が壊されてしまいます。現在、DKIMの署名と検証に使用される正規化メソッドには、[普通]と[緩和]という2つがあります。[普通]は最も厳しいメソッドで、変更を全く認めません。[緩和]は普通よりも緩い基準を持ち、多少の変化を許容します。

ヘッダの正規化:普通,緩和
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。[普通]はヘッダの変更を一切認めず、[緩和]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ひとつに変換、その他当たり障りのない変換を行います。デフォルトの設定は[普通]です。

本文の正規化:普通,緩和
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canonicalizationメソッドです。[普通]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。[緩和]は、メッセージの最後の空白行を許可をして、行の最後の空白を無視することで一行内の連続した空白をひとつにまとめ、その他の少ない変換を行います。デフォルトの設定は[普通]です。

4.3.5 DMARC

Domain-Based Message Authentication,レポーティング & 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、ドメイン所有者は宛先サーバーにDNSを通して、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、といったポリシーを通達できるようになります。宛先サーバーへメール受信時のDNSクエリによる送られるこのポリシーでは、ポリシーに準拠していないメールを隔離するのか、拒否するのか、何もしない(つまり通常通り処理する)のかを定義するのに使用します。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 » 不正使用対策 以下には、Security GatewayのDMARC検証、DMARCレポート、DMARC設定、のDMARCの検証とレポートに関連した3つの設定画面をご用意しています。

DMARC検証 170

DMARC検証処理の1つとして、Security Gateway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 166を取得します。更に、DMARCはSPF 159 やDKIM 162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、Security Gateway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SecurityGateway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=隔離"や"p=reject"といった制限ポリシーを使っていると、SecurityGatewayはオプションでメールを自動的にユーザーの隔離フォルダ[250]へ振り分けたり、件名へテキストを追加したり、メッセージスコア[150]を調整する事ができます。また、ドメインが制限ポリシーを使っていた場合に、SecurityGatewayはポリシーに応じて"X-SGDMARC-Fail-policy: 隔離"や"X-SGDMARC-Fail-policy: reject"をヘッダへ自動挿入します。これにより送信メールを特定のフォルダへ移動するなどの処理が、ヘッダに含まれる文字列をベースに、Sieveスクリプト[228]やメールサーバーのコンテンツフィルタリングシステムで行えるようになります。

DMARC検証はデフォルトで有効で、ほとんどのSecurityGateway設定で推奨しています。

DMARCレポーティング[173]

SecurityGateway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レポーティングでは、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SecurityGatewayは統計レポートのみを送信します。

DMARC設定[175]

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、SecurityGateway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、ドメインメールサーバー側で、メーリングリストメールのFrom:ヘッダをメーリングリストのアドレスへ書き換えるか、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設定を行ってください。お使いのメールサーバーがMDaemonの14.5以降の場合、宛先ドメインが制限DMARCポリシーを使っている場合、デフォルトでメーリングリストアドレスのFrom:ヘッダが置き換えられます。

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、最低限どちらか1つがDMARCを使用するよう正しく設定されている、SPF[159]とDKIM[163]のDNSレコードが必要です。DKIMを使っている場合は

SecurityGatewayの DKIM署名 163 オプションも設定する必要があります。また、ドメイン用のDMARC DNSレコードも必要です。特別なフォーマットのTXTレコードのDNSクエリにより、宛先サーバーはDMACポリシーや、使用している認証モード、統計レポートの受信を行うかどうか、レポート送付先アドレス、といった様々なオプションを確認する事ができます。正しくDMARCを設定し、DMARC XMLレポートの受信が始まったら、レポートの読み込みができるオンラインツールを活用して潜在的な問題の分析を行う事ができます。

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 Field

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用の _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** 隔離 **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=隔離 ポリシーへ移行するための準備が行えます。 p=隔離 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=隔離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** 隔離 **reject** —	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。

	Default: **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。	例: `_dmarc IN TXT "v=DMARC1;p=隔離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=隔離 ;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=隔離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** —	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=隔離ruf=mailto:dmarc-failures@example.com"`

	デフォルト値:
	none
	このタグがない場合、失敗レポートは送信されません。
		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=隔離 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

4.3.5.1 DMARC検証

DMARC検証処理の一部として、SecurityGatewayは受信メールのFrom:ヘッダ内のドメインに対してDMARC DNSクエリを実行します。これで、ドメインがDMARCを使っているかどうかと、もしも使っている場合は、ポリシーやその他DMARC関連情報が含まれているDMARC DNSレコード[166]の取得を行います。更に、DMARCはDMARC検証を通過するためのテストとして、各メールのSPF[159]とDKIM[162]を利用しており、DMARC検証を通過するには最低どちらかの検証を通過する必要があります。メールが検証を通過すると、SecurityGatewayは対象のメールについて、残りの配送とフィルタリングの処理を通常通りに行います。もしも検証に通過しなかった場合は、ドメインのDMARCポリシーとSecurityGateway側の設定との組み合わせで、その後の処理を決定します。

メールがDMARC検証に失敗し、DMARCドメインのポリシーが"p=none"の場合、対処される事なく、メールは通常通り配信されます。反対に、DMARCドメインが"p=quarantine"や"p=reject"のポリシーを定義していた場合、SecurityGatewayはメールを拒否したり、各ユーザの隔離フォルダ[250]へ自動振り分けしたり、件名へ文字列を追加したり、メッセージスコア[150]を調整する事ができます。更に、制限ポリシーで検証に失敗したメールについて、SecurityGatewayはポリシーに応じて"X-SGDMARC-Fail-policy: quarantine"や"X-SGDMARC-Fail-policy: reject"ヘッダを挿入します。これにより、メールを特定のフォルダへ配信するといった処理を、Sieveスクリプト[228]やメールサーバーのコンテンツフィルタでヘッダの有無を元に行う事ができます。

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、SecurityGatewayは受信メールのFrom:ヘッダ内のドメインに対してDMARC DNSクエリを実行し、DMARCレポート[173]で設定されていれば、統計及び失敗レポートを送信します。DMARCはメールの検証にSPF[159]とDKIM[162]を使用しているため、最低どちらかの機能が有効になっている必要があります。DMARC検証とDMARCレポートはデフォルトで有効で、ほとんどのSecurityGateway設定で使用されています。

DMARC対応を無効化すると、スパムやなりすまし、その他不正なメールをの受信数が増える可能性があります。環境によっては、メールサーバーのメーリングリストメールが他のサーバーで拒否されたり、メーリングリストメンバ

一がメーリングリストから外されてしまう場合があります。DMARCは必要がある場合以外無効化しない事をお勧めします。

検証結果がREJECTだった場合には:
受信メールがDMARC検証に失敗し、送信元ドメインのDMARC DNSレコードでp=rejectが定義されていた場合はここで指定した処理が行われます。

...メッセージを拒否
DMARC検証処理でREJECTが返された場合、このオプションでメッセージをSMTP処理中に拒否します。このオプションがデフォルトで選択されています。

メールを拒否する選択を行わなかった場合でも、メールはSPFやDKIM設定、メッセージスコアが許可されている閾値を越えた場合、など、他の要因で拒否される場合があります。

...メッセージを隔離
DMARC検証処理でREJECTが返された場合、拒否するのではなくメールを 隔離 250 する場合はこのオプションを選択します。このオプションと併せて、「...次の文字を件名に付ける」や「...この値をスコアに追加［xx］ポイント」を使用する事もできます。

...メッセージを受け入れる
DMARC検証処理でREJECTが返された場合、このオプションを選択すると、SecurityGatewayはメール受信を許可しますが、件名へ文字列を追加したり メッセージスコア 150 の調整を行う事ができます。

...次の文字を件名に付ける
DMARC検証処理でREJECTが返されたメールを受け付けたり隔離する場合、このオプションを有効にしメールのSubjectヘッダへ追加する文字列を指定する事ができます。 有効にした場合、Subjectに追加されるデフォルトテキストは"*** FRAUD ***"です。このオプションで、受信者のメールサーバまたはクライアントで、文字列を元にしたメールのフィルタリングが行えます。このオプションはデフォルトで無効です。

SecurityGatewayでは他にも様々な機能で件名ヘッダへ文字列を付与します。例えば、SPF 159 や メッセージスコア 150 ページにもこのオプションがあります。これらのオプションとして指定した文字列にマッチした場合、複数の条件にマッチしているメッセージだった場合でも、タグはメールの件名に一度だけ付与されます。ただし、文字列がオプションによって異なる場合は、それぞれの独自タグが付与されます。例えば、このオプションのデフォルトテキストは「*** FRAUD ***」ですが、メッセージスコアのデフォルトテキストは「*** SPAM ***」です。2つのタグが異なるため、どちらのオプションにもマッチしたメールへは両方の文字列が追加されます。ただし、どちらかのオプションで追加した文字列を変更した場合、タグは一度だけ追加されます。

...この値をスコアに追加 [xx] ポイント
DMARC検証処理でREJECTが返されたメールを受け付けたり隔離する場合、このオプションを有効にし メッセージスコア 150 へ指定したポイントを付与します。最終的なスコアがメッセージスコアで指定した閾値に到達すると、メールは設定に沿って隔離されるか拒否されます。デフォルトではメッセージスコアへ5.0ポイントが追加されます。

検証結果がQUARANTINEだった場合には:
受信メールがDMARC検証に失敗し、送信元ドメインのDMARC DNSレコードでp=QUARANTINEが定義されていた場合はここで指定した処理が行われます。

...メッセージを拒否
DMARC検証処理で隔離が返された場合、このオプションでメッセージをSMTP処理中に拒否します。

...メッセージを隔離
DMARC検証処理で隔離が返された場合、このオプションを選択しメールを拒否するのではなく 隔離 250 します。このオプションと併せて、「...次の文字を件名に付ける」や「...この値をスコアに追加 [xx] ポイント」を使用する事もできます。

...メッセージを受け入れる
DMARC検証処理で 隔離 250 が返された場合、このオプションを選択すると、SecurityGatewayはメール受信を許可しますが、件名へ文字列を追加したり メッセージスコア 150 の調整を行う事ができます。

...次の文字を件名に付ける
隔離ポリシードメインからのDMARC検証に失敗し、SecurityGatewayが対象メールを受信または隔離するよう設定していた場合、 このオプションを有効にしメールのSubjectヘッダへ追加する文字列を指定する事ができます。 有効にした場合、Subjectに追加されるデフォルトテキストは"*** FRAUD ***"です。このオプションで、受信者のメールサーバまたはクライアントで、文字列を元にしたメールのフィルタリングが行えます。このオプションはデフォルトで無効です。

SecurityGatewayでは他にも様々な機能で件名ヘッダへ文字列を付与します。例えば、SPF 159 や メッセージスコア 150 ページにもこのオプションがあります。これらのオプションとして指定した文字列にマッチした場合、複数の条件にマッチしているメッセージだった場合でも、タグはメールの件名に一度だけ付与されます。ただし、文字列がオプションによって異なる場合は、それぞれの独自タグが付与されます。例えば、このオプションのデフォルトテキストは「*** FRAUD ***」ですが、メッセージスコアのデフォルトテキストは「*** SPAM ***」です。2つのタグが異なるため、どちらのオプションにもマッチしたメールへは両方の文字列が追加されます。ただし、どちらかのオプションで追加した文字列を変更した場合、タグは一度だけ追加されます。

...この値をスコアに追加 [xx] ポイント
デフォルトで、隔離ポリシードメインからのDMARC検証に失敗し、SecurityGatewayが対象メールを受信または隔離するよう設定していた場合、このオプションで メッセージスコア 150 へ

指定したポイントを付与します。最終的なスコアがメッセージスコアで指定した閾値に到達すると、メールは設定に沿って隔離されるか拒否されます。デフォルトではメッセージスコアへ5.0ポイントが追加されます。

例外

ホワイトリストIPアドレスからのメッセージを除外する
デフォルトで、ホワイトリストのIPアドレス[226]から到着しているメッセージは、DMARC検証から免除されます。差出人がIPアドレスホワイトリストの場合でもDMARC検証を行う場合はチェックボックスを解除します。

認証されたセッションからのメッセージを除外する
デフォルトで、認証済SMTPセッションで届いたメールは、DMARC検証から免除されます。認証済SMTPセッションで届いたメールの場合でもDMARC検証を行う場合はチェックボックスを解除します。

ドメインメールサーバからのメッセージを除外する
ドメインメールサーバ[65]から到着しているメッセージは、デフォルトでDMARC検証から免除されます。差出人がドメインメールサーバからの場合でもDMARC検証を行う場合はチェックボックスを解除します。

4.3.5.2 DMARCレポート

SecurityGatewayがDMARCレコードについてDNSへ問い合わせを行う際、レコードにはドメイン管理者がドメインを名乗ったメッセージに関する統計レポートや失敗レポートを受け取るかどうかのタグが含まれています。DMARCレポートのオプションでは要求された種類のレポートを送るかどうかや、レポートに含むメタデータに関する設定を行う事ができます。統計レポートはUTCの深夜に日時で送られ、失敗レポートは、失敗が発生したタイミングでメッセージ毎に送信されます。 レポートは毎回zip圧縮されたXMLファイルの添付で送信され、受信者がレポートを閲覧するための様々なツールがインターネットにあります。デフォルトでSecurityGatewayは統計レポートのみを送信します。

画面のオプションはDMARC検証[170]画面の*"DMARC検証とレポートを有効にする"*オプションが有効な場合のみ使用できます。また、DMARCの仕様ではレポート受信者の提供するSTARTTLS[103]の使用を必須としています。できるだけSTARTTLSを有効化する事をお勧めします。

DMARCレポート

DMARC統計レポートを送信する
希望があった場合にDMARC統計レポートを送信するにはこのオプションを有効化します。受信メールのFrom:ドメインに対してDMARCのDNSクエリを実行した際、対象ドメインのDMARCレコードに"rua="タグ（例. rua=mailto:dmarc-reports@example.com）が含まれていると、ドメイン所有者がDMARC統計レポートの受信を希望しているという事になります。 SecurityGatewayはドメインやドメインを名乗ったメールといったDMARC関連情報を保持します。統計レポートの送信先メールアドレス、各メールの検証方法（SPF, DKIM, 両方）、メールが検証を通過したか失敗したか、送信サーバー、IPアドレス、適用されたDMARCポリシーなどの情報がログへ記録されます。UTCの深夜に、SecurityGatewayは保管されたデータを元にドメイン毎のレポートを生成し、必要なアドレスへ配信します。レポートが配信されると、保管されていたDMARCデータはクリアされ、SecurityGatewayはプロセス全体を再開します。

SecurityGatewayは統計レポートで使用するDMARCレポートのインターバルタグ（例．"ri="）には対応していません。SecurityGatewayは、前回のレポート生成後に蓄積されたデータを使って、毎日UTCの深夜に統計レポートを生成し送信します。

SecurityGatewayは統計レポート送信とDMARCデータのクリアを毎日UTCの深夜に実行する必要がある事から、SecurityGatewayをこの時間帯に停止させていた場合、レポートは生成されず、DMARCデータはクリアされません。DMARCのデータはSecurityGatewayが再度稼働したタイミングで蓄積されますが、次のUTC深夜のイベントまでレポートは生成されず、データもクリアされません。

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）
希望があった場合にDMARC失敗レポートを送信するにはこのオプションを有効化します。受信メールのFrom:ドメインに対してDMARCのDNSクエリを実行した際、対象ドメインのDMARCレコードに"ruf="タグ（例．ruf=mailto:dmarc-failure@example.com）が含まれていると、ドメイン所有者がDMARC失敗レポートの受信を希望しているという事になります。統計レポートと異なり、失敗レポートはトリガーとなるイベントが発生する度にリアルタイムで生成され、各インシデントの詳細と失敗の原因であるエラーの詳細が記録されます。レポートはドメイン管理者でメールシステムの問題解決や他の問題の発見といった目的で分析を行うのに使用されます。

失敗レポートを送信するきっかけとなる失敗の種類はドメインのDMARCレコードの"fo="タグに依存します。デフォルトで失敗レポートはDMARC検証に失敗（例． SPFとDKIMの両方で失敗）した全てのメールで生成されますが、ドメインは様々な"fo="タグでSPFに失敗した場合のみやDKIMに失敗した場合のみ、どちらかに失敗した場合、といった組み合わせで、失敗レポートの生成タイミングをコントロールできます。また、DMARCレコードの"ruf="タグの受信者数、"fo="タグの値、処理中に発生した認証失敗の数によって、1つのメールから複数の失敗レポートが生成される場合があります。SecurityGatewayが送信するレポートの上限を指定する場合は、後述の、*指定数字までのDMARC 'rua'や'ruf'を送信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おいてドメインのDMARCレコードにrf=iodef タグが含まれている場合であっても、SecurityGatewayではDMARCのデフォルトであるrf=afrf タグ（Abuseレポートフォーマットを使った認証失敗レポート）のみを使用できます。

DMARC失敗レポート対応のため、SecurityGatewayは 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に完全対応しています。

DMARC "fo="タグでSPF関連の失敗レポートを要求されると、SecurityGatewayはRFC 6522に沿ってSPF失敗レポートを配信します。つまり、仕様拡張がドメインのSPFレコードに存在している必要があり

ます。SPF失敗レポートはDMARC処理やRFC6522拡張の存在から独立して送ら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ると、SecurityGatewayはRFC 6651に沿ってDKIMの失敗レポートを配信します。つまり、DKIM署名のヘッダフィールドへ仕様拡張が存在しており、ドメインDNSへ正しいDKIMレポーティング用のTXTレコードを含んでいる必要があります。DKIM失敗レポートはRFC6651拡張やDMARC処理なく独立して送られる事はありません。

指定数字までのDMARC 'rua'や'ruf' を送信先として受け付ける
SecurityGatewayがDMARC統計レポートやDMARC失敗レポートの送信先を制限すうrには、ここで最大送信数を指定します。DMARCレコードの"rua="や"ruf="タグが指定した上限よりも多くのアドレスを指定していた場合、SecurityGatewayはレポートを最大宛先数に到達するまでレポートを一覧のアドレスへ送信します。デフォルトで最大宛先数は5に設定されています。

全レポートのコピー送信先アドレス:
全てのDMARC統計レポートやDMARC失敗レポート（fo=0 または fo=1 のみ）のコピーを送る1つまたはカンマ区切りの複数アドレスを指定します。

DMARCレポート メタデータ

送信するDMARCレポートへ含まれる企業や組織のメタデータ情報を指定するためのオプションです。

デフォルトドメイン
DMARCレポートを作成するSecurityGatewayドメインです。ドロップダウンリストからドメインを選択してください。

連絡先メールアドレス
レポート受信者が問い合わせる際のローカルメールアドレスをここで指定します。複数アドレスをカンマ区切りで指定できます。

連絡先情報
レポートに含む、ウェブサイト、電話番号といった、追加の連絡先情報を指定します。

Return-pathの指定
送信失敗の場合に備えてSecurityGatewayがレポートメールで使用するSMTP return path（戻り先アドレス）を指定します。こうした問題を無視する場合は noreply@<mydomain.com> を使用してください。

4.3.5.3 DMARC設定

DMARC設定ページにはDMARCレポートに含む情報、DMARC DNSレコードのログ、SecurityGatewayがDMARC用に使うPublic Suffixファイルの更新といった様々な設定オプションがあります。

DMARC設定

DMARC失敗レポートに、正規化されたDKIMヘッダを含める
DMARC失敗レポート[173]へDKIMの正規化ヘッダ[163]を含む場合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です。

DMARC失敗レポートに、正規化されたDKIM値を含める
DMARC失敗レポート[173]へDKIMの正規化された本文[163]を含む場合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です。

上記の2つのオプションは問題のデバッグにおいて便利ですが、処理中にメールの内容を公開してしまうリスクもあります。

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 SecurityGatewayはIPアドレスをDMARCレポート内で"X.X.X.X"へ置き換えます。IPアドレスをDMARCレポート内で公開する場合はこのオプションを無効にしてください。このオプションはDKIMの正規化された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'ヘッダの構成について、DMARCの要件と互換性のないメールの受信を拒否する場合は、このオプションを有効にします。メールの中には複数のFromヘッダを持つものや、1つのFromヘッダ内に複数メールアドレスが存在するものがあります。こうしたメールは現時点でDMARC処理から除外されます。この設定は、複数アドレスを1つのFromヘッダに持つメールが技術的にプロトコルの規定に反しているものではない事から、デフォルトで無効になっていますが、この設定を有効化する事で、DMARCによる保護を最大に生かす事ができます。この設定はDMARC検証[170]が有効な場合にのみ適用されます。

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 SecurityGatewayはDMARCレポート用のメールへbulkメールヘッダを挿入します。このヘッダ挿入を行わないようにするにはチェックボックスをクリアしてください。

ログファイルにすべてのDMARCレコードを含める
デフォルトでSecurityGatewayはDMARCがDNSクエリで取得した全てのDMARC DNSレコードをログへ記録します。全てのDMARCレコードをログへ含めない場合はこのオプションを無効化してください。

この日数より Public suffix file が古い場合、自動更新する
DMARCはDMARC DNSレコードのクエリを行う際、対象のドメインが信頼できるものかどうかを確認するためpublic suffix fileを必要とします。デフォルトでSecurityGatewayは保管したpublic suffix fileを15日毎に自動更新します。このオプションの値を変更する事で更新までの日数を増やしたり減らしたりする事ができます。ファイルの自動更新を行わない場合はこのオプションを無効化してください。

Public suffix file URL
This is the URL of the public suffix file that SecurityGateway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SecurityGatewayは http://publicsuffix.org/list/effective_tld_names.dat のファイルを使用しています。

Public suffix fileを今すぐ更新する
このボタンで上記の*Publix suffix file URL*からpublic suffix fileを手動更新します。

4.3.6 コールバック検証

コールバック検証は、受信メッセージの見せかけられた差出人の電子メールアドレスの有効性を確認するために利用する「なりすまし」対策です。これを実行するには、SecurityGatewayは、SMTPセッションの間、"MAIL From"ステートメントで渡されるドメインのメール交換器に接続し、その差出人のアドレスが、ドメインで有効アドレスであるか照合を試みます。チェックの結果で差出人アドレスが存在しない場合、SecurityGatewayでは、偽造されたアドレスから送信されているので、メッセージの拒否、隔離あるいはメッセージを受け入れ、オプションでメッセージスコア150を調整やタグを付ける扱いができますことができます。一般のコールバック検証にかかわる若干の潜在的な問題および欠点があるので、この機能はデフォルトで無効にされます。

コールバック検証に関する一般情報に関しては、Wikipedia.org.でコールバック検証記事を参照してください。

設定

差出人検証にコールバック検証を使用する
差出人電子メールアドレスの有効性を確認するためにコールバック検証を使用する場合、このチェックボックスを選択します。SecurityGatewayは、見せかけられた差出人のドメインに接続するためにSMTP"MAIL From"ステートメントに送信サーバによって渡される値を使用し、そのアドレスが存在を照合します。コールバック検証はデフォルトで無効です。

TVRFYコマンドを最初に試みる(差出人のメールサーバでサポートされている場合)
デフォルトで、サーバがそのコマンドをサポートすることを示す時、SecurityGatewayは差出人のアドレスを照合するSMTP "VRFY"コマンドの使用を最初に試みます。サーバは、SMTPセッションの初めに"250-VRFY"ステートメントでSecurityGatewayに応答することによりVRFYのサポートを示します。このオプションを無効にする場合、またはサーバでVRFYをサポートしない場合、SecurityGatewayでは、代わりに"MAIL From"および"RCPT To"コマンドを使用します。SecurityGatewayでは、メッセージを実際に送信されないにもかかわらず、当該のアドレスにメッセージを送信するように、差出人のアドレスで、これらのコマンドを使用してドメインにおいて有効であるか照合します。

このアドレスからメッセージを送信する:
これは、アドレスからNULLがサーバによって許可されない時、または"最初にアドレスからNULLを試みる"オプションを下記で無効にする場合、"MAIL From" SMTPステートメントで使用されるFromアドレスです。このオプションのデフォルト値は、"postmaster"です。追加するドメインの一部は、受信者ドメインです(例えばpostmaster@ RecipientsDomain.comです)。このオプションで完全なメールアドレスを指定する場合、代わりに、このアドレスが使用されます。例えば、このオプションで"xyz@ example.com"を使用すると、受信者ドメインを使用しないことを意味します。

メッセージは差出人のメールサーバに実際に送信されません。SecurityGatewayではメッセージを送信するように、サーバに接続し、MAIL FromおよびRCPT Toコマンドを送信しますが、送信することなく接続を終えます。参照テストによって、サーバが当該の差出人アドレスについてメッセージを受け入れる場合、SecurityGatewayでは、サーバでアドレスを有効であるとみなす確認をすることができます。

最初にアドレスからNULLを試みる
差出人のアドレスを照合する"MAIL From"および"RCPT To"コマンドを使用する時、SecurityGatewayでは、NULL値("MAIL From <>")でFromを使用することを最初に試みます。このオプションが無効にされる場合、またはサーバがNULLを許可しない場合、上記で指定される"このアドレスからメッセージを送信する:"を使用します。

差出人がコールバック検証に失敗する場合:
コールバック検証テストが差出人のアドレスが不正であることを示す場合、メッセージを拒否、隔離または受け入れることができ、オプションでタグを付け、さらにメッセージスコア 150 を調整することができます。コールバック検証に失敗するメッセージについて使用するオプションを下記で選択します。

...メッセージを拒否
このオプションが選択される場合、コールバック検証に失敗する差出人によるメッセージはSMTPセッション中に拒否されます。

...メッセージを隔離
コールバック検証に失敗するメッセージを隔離したい場合、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す。

...メッセージを受け入れる
コールバック検証に失敗するメッセージを受け入れるが、そのメッセージスコアを調整、またはサブジェクトにテキストを追加したい場合、このオプションを使用します。

...次の文字を件名に付ける [*text*]
差出人の電子メールアドレスがコールバック検証テストに失敗する時、メッセージのサブジェクトの先頭にテキストを追加する場合、このオプションを選択し、テキストを指定します。デフォルトでは、このオプションは無効です。有効にする場合、"*** CBV ***"はデフォルトでサブジェクトに追加されますが、オプション選択時にはテキストを編集することができます。

SecurityGatewayには、これ以外のオプションでサブジェクトヘッダにテキストを追加することができます。例えば、メッセージスコア 150 およびURIブラックリスト(URIBL) 141 ページでは同様なオプションを持ちます。これらのオプションで指定されたテキストで適合させる時、そのメッセージが各オプションで基準を満たす場合でも、テキストは一度メッセージのサブジェクトに追加されるだけです。ただし、他のオプションでテキストを変更する場合、その変更されたテキストが追加されます。例えば、これらの3つのオプションすべて"*SPAM*"にテキストを設定する場合、オプションのうちの1つ以上で基準に適合する場合でも、テキストは一度サブジェクトに追加されるだけです。しかし、"*DNS blacklisted*"にDNSBLオプションのテキストを変更、およびメッセージが、そのオプションおよび他の基準に適合する場合、サブジェクトには両方の"*SPAM*"および"*DNS blacklisted*"が追加されます。

...この値をスコアに追加 [xx] ポイント
デフォルトによって、コールバック検証チェックに失敗するメッセージは、1.0のポイントによって調整され、そのメッセージスコアを持ちます。選択する場合、この値を調整することができます、または、コールバック検証がスコアに影響しないようにする場合、オプションを無効にすることができます。

SecurityGatewayが拒否または隔離ではなく、メッセージを受け入れる構成する場合でも、そのメッセージスコアが十分に高い場合、他のセキュリティ[126]オプションおよびメッセージスコア[150]ページのオプションを構成により、今まで通り拒否または隔離することができます。

除外

ホワイトリストの差出人からのメッセージを除外する
ホワイトリスト差出人[221]からのメッセージは、コールバック検証からデフォルトで除外されています。ホワイトリスト差出人をコールバック検証要求から除外しない場合、このオプションを無効にします。

認証されたセッションからのメッセージを除外する
デフォルトで、認証されたセッションを通じて送信されているメッセージは、コールバック検証要求から除外されます。セッションが認証される時にも差出人を照合したい場合、このチェックボックスを解除します。

ローカルの差出人からのメッセージは常に除外する
ローカル差出人からのメッセージは、デフォルトでコールバック検証から除外されます。ローカル差出人を除外しない場合、このチェックボックスを解除します。

例外 – ドメイン

これらの設定を構成する時、ページ上部のドメイン:ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。コールバック検証の設定を見直し編集するには、対応するドメインの**表示 / 編集**リンクをクリック、あるいはデフォルトの全体の設定値をドメインの設定にリセットするには、**リセット**をクリックします。

4.3.7 Fromヘッダスクリーニング

このセキュリティ機能は、受信メッセージの「From:」ヘッダーを変更し、ヘッダーの名前の部分に名前とメールアドレスの両方を含めるようにします。これは、メールが他の誰かからのものであると見せかける、スパムや攻撃でよく使われる一般的な手法に対抗するための機能です。メーラーでは、メッセージの一覧を表示する際に、通常は送信者の名前だけを表示し、名前とメールアドレス両方は表示されません。メールアドレスを表示するには、まずメールを開くか、右クリックするか、メールにカーソルを合わせるなどの、他のアクションを取る必要があります。そのため、攻撃者は通常、「From:」ヘッダーで表示される部分には合法的な個人や会社名を使用し、一方で、不正なメールアドレスが表示されないようにします。例えば、メッセージの実際の「From:」ヘッダーは、`Honest Bank and Trust <lightfingers.klepto@example.com>` かもしれませんが、メーラー上では、送信者として`Honest Bank and Trust`のみが表示されます。この機能は、ヘッダーで名前とメールアドレス両方の部分を表示するように変更します。上記の例では、送信者は`"Honest Bank and Trust (lightfingers.klepto@example.com)" <lightfingers.klepto@example.com>`と表示され、メールが偽装されていると判断しやすくなります。

From ヘッダスクリーニング

表示名にメールアドレスを追加
このオプションを有効にすると、受信メッセージの「From:」ヘッダーのクライアント表示部分に、送信者の名前とメールアドレスの両方が含まれるように変更されます。新しいヘッダーの構造

は、"Sender's Name" <mailbox@example.com> から "Sender's Name (mailbox@example.com)" <mailbox@example.com>となります。これはローカルユーザー宛のメッセージにのみ適用され、このオプションはデフォルトでは無効になっています。このオプションを有効にする前に注意深く検討してください。なぜなら、ユーザーによっては、詐欺メールを判断しやすくなるとしても、それ以上に「From:」ヘッダーが変更されることを望まない場合もあるからです。

名前の前にメールアドレスを追加
上記の「表示名にメールアドレスを追加する」オプションを使用している時、「From:」ヘッダーで名前とメールアドレスを入れ替え、メールアドレスを先に表示する場合には、このオプションを有効にします。上記の例を使用すると、"Sender's Name" <mailbox@example.com> は"mailbox@example.com (Sender's Name)"と変換されます。

表示名にあるメールアドレスが、実際のものと異なっていた際に置き換える
スパムで使用されるもう1つの手法として、実際の送信元のメールアドレスではないにも関わらず、「From:」ヘッダーの表示部分に見かけ上合法的な名前とメールアドレスを入れるというものがあります。このオプションを使用すると、このようなメッセージの表示されるメールアドレスを実際の送信者のアドレスに置き換えることができます。例えば、"Frank's Company (frank@company.test)" <spoof@example.com> は"Frank's Company (spoof@example.com)" <spoof@example.com>に変更されます。

例外

認証されたセッションからのメッセージを除外する
デフォルトで、認証されたセッションを通じて送信されているメッセージは、Fromヘッダスクリーニングから除外されています。セッションが認証されていてもFromヘッダスクリーニングを適用するにはこのチェックボックスを解除します。

ドメインメールサーバからのメッセージを除外する
ドメインメールサーバ 65 から到着しているメッセージは、デフォルトでFromヘッダスクリーニングから除外されています。ドメインメールサーバからのメールにもFromヘッダスクリーニングを適用するにはこのチェックボックスを解除します。

例外 - ドメイン

ページ上部のドメイン:ドロップダウンリストボックスで特定のドメインを選択し、設定を行う事ができます。ドメイン設定を保存すると、ここへ対象ドメインが一覧表示されます。表示/編集をクリックして、対象ドメインのFromヘッダーのスクリーニング設定を確認または編集するか、リセットをクリックしてドメインの設定をデフォルトのグローバル値にリセットできます。

4.4 不正使用対策

セキュリティ 126 メニューの不正使用対策セクションでは、不正使用やスパムメールの配信、帯域の利用、頻繁な接続などの行為からメールシステムを保護するためのオプションが利用できます。不正使用のセクションには8つのアイテムがあります。

リレーコントロール 181 - ローカルドメイン宛でも、ローカルドメインからでもないメールが届くと、SecurityGatewayではこれを配信又は転送するのか確認します。リレーコントロールページでは、どのメ

ールを転送対象とするかどうかを指定します。リレーコントロールではSMTPのMAILやRCPTコマンドで渡すオプションの指定も行えます。

SMTP認証 183 - このページではSMTP認証オプションの設定が行え、SMTPで認証を行う事ができるようになります。ユーザーがメールの送信時に認証を行う事は、既知の正常な通信である事を確認する効果的な方法です。SMTP認証で、スパムや不正なユーザーによる第3者中継を防ぐことできるため、他の多くのセキュリティチェックをスキップできるようになります。

IPシールド 184 - IPシールドはSMTP MAIL FROMコマンドで確認されるドメインとIPアドレスの一覧です。一覧にあるドメインからのSMTP接続は、送信元サーバーのIPアドレスが許可されたIPアドレスの一覧に存在した場合にのみ受け付けられます。

ダイナミックスクリーニング 185 - この機能で、SecurityGatewayは送信サーバーの怪しいと思われる挙動を追跡し、対処する事ができます。例えば、ダイナミックスクリーニングを使って、「不明な宛先」エラーが指定した時間内に一定数を越えた場合に、その接続を拒否する事ができます。また、指定した分の間で一定数以上の接続や、認証失敗があった場合に、こうした接続を拒否する事もできます。ただし、ダイナミックスクリーニングは永久に機能するものではありません。対象IPアドレスは、拒否されてから、指定した分数の間だけ、接続をブロックされます。

ロケーションスクリーニング 187 - これは場所をベースにしたブロック用システムで、許可されていない国からの接続を拒否するためのオプションです。SecurityGatewayは接続元IPと関連付けられた国を検証し、制限されている国からの接続であった場合にこれをブロックします。デフォルトで、ロケーションスクリーニングは認証を試みている接続のみをブロックします。この機能は、例えば、全くユーザーが存在しないものの、メールを受信する可能性はある国からのアクセスを防ぐには大変便利です。この方法であれば、サーバーへログインしようとした接続のみを拒否する事ができます。

ターピット 188 - ターピットを使うと、指定した数を超えるRCPTコマンドを受け取った際、配信を遅らせる機能です。スパム送信者がスパムメールの送信を行いにくくなります。RCPTコマンドの上限や遅延させる秒数をここで指定できます。この技術の背景には、スパム送信者にとって送信に通常以上の時間がかかるメールは、再送する事をしない、という点が挙げられます。

帯域幅制限 189 - この機能でSecurityGatewayが、全体またはドメイン毎に使用できる帯域の指定が行えます。帯域幅制限機能でそれぞれの受信と送信SMTPセッションの帯域を管理できます。また、この制限からはホワイトリストにいる送信者、認証済セッション、ドメインメールサーバーを除外する事ができます。

アカウントハイジャック検出 190 - この画面のオプションで、サーバーのハイジャックされた可能性のあるアカウントを検出し、メール送信を自動で行えないようにする事ができます。例えば、スパム送信者が何らかの方法でアカウントのメールアドレスとパスワードを入手し、対象アカウントからスパムメールを送信する、といった状態を防ぐ事ができます。ここでは指定された分数の中で、アカウントが最大何通のメール送信を行うかを指定でき、オプションとして、この上限に到達した場合にアカウントを無効化する事もできます。

4.4.1 リレーの管理

メッセージがローカルドメイン以外から届いて、配信やリレーを要求された場合、SecurityGatewayではオープンリレーを許可しませんが、このページから必要に応じてドメインメールサーバ 65 のメールリレーを許可する事ができます。リレーの管理ではSMTPで渡されるMAILやRCPTコマンド内にローカルドメインを必ず含むよう指定するオプションもあります。

メールリレー

このサーバではメッセージをリレーしない...
スパム送信者は追跡されることのないようオープンリレーサーバーを悪用するため、メールリレーによって1つ以上のDNSBL[138]サービスのブラックリスト登録されてしまう可能性が高くなってしまう事から、SecurityGatewayでは自身のサーバー以外からのメールリレーを行いません。

...ドメインメールサーバから送信された場合を除く
メッセージをリレーする場合、ドメインに関連のないが、ドメインメールサーバ[65]によって送信される時には、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です。

ドメインメールサーバだけがローカルメールの送信が可能
デフォルトで、送信サーバがそのドメインに対して指定されるドメインメールサーバ[65]である時、SecurityGatewayは、ローカルドメインからメッセージを受け入れるだけです。ローカルメールの送信を各ドメインの指定されたメールサーバに制限しない場合は、このチェックボックスを解除します。

...ローカルアカウント宛のメッセージを除く
ドメインメールサーバ[65]からのメールではないローカルメールで、ローカルアカウント宛のメールを許可する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有効です。

...認証されたSMTPセッションで送信された場合を除く
ローカルドメインからのメッセージがドメインの指定されたメールサーバのうちの1台によって送信されない場合、このオプションが有効で、認証されたセッションを通じて送信されるメッセージはSecurityGatewayでメッセージを今まで通り受け入れます。これのサンプルは、直接送信メールをドメインメールサーバではなくSecurityGatewayを通して送信しているローカルユーザです。このオプションはデフォルトで有効です。

...ホワイトリストIPあるいはホストから送信された場合を除く
送信サーバがドメインメールサーバ[65]の1つでない場合でも、ホワイトリスト[221]IPアドレスおよびホストからのローカルメールを許可する場合は、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。

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
デフォルトでSecurityGatewayは、メッセージがローカルドメインから見せかけられる時に実際の有効なアカウントの示すメール値(差出人)がSMTP中に、処理を渡したことを照合します。アドレスが存在しない場合、メッセージは拒否されます。

...ドメインメールサーバから送信された場合を除く
ドメインメールサーバ[65]から送信されている時、メッセージを"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"オプションから除外する場合、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有効です。

...認証されたSMTPセッションで送信された場合を除く
認証されたSMTPメールセッションを通して送信されている時、メッセージを"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"オプションから除外する場合、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有効です。

...ホワイトリストIPあるいはホストから送信された場合を除く

ホワイトリスト 221 IPアドレスまたはホストから送信されている場合メッセージを"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..."オプションから除外する場合、このオプションを選択します。これはデフォルトで無効です。

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
SecurityGatewayでは、メッセージがローカルドメイン用に責任のある場合に、実際の有効なアカウントを示すSMTP処理中に渡されるRCPT値(すなわち受信者)を検証します。アドレスが存在しない場合、メッセージは拒否されます。

4.4.2 SMTP認証

このページではSMTPを拡張し認証を行えるようにしたSMTP認証の設定が行えます。この機能により、メール送信時にユーザーをログインさせ、対象のメール送信が正規なものであると証明する事ができます。SMTP認証は、アドレスを偽装しサーバを通してのメールをリレーしようとするスパマーなどをキャッチするためのセキュリティを、認証を行う事により省略できるようにしています。

SMTP認証

ローカルアカウントからメールが送信される場合、常に認証が必要
メッセージがローカルアカウントから送信を示す時はいつでも認証が必要な場合、このチェックボックスをクリックします。SMTPセッションが認証されない場合、メッセージは拒否されます。このオプションはデフォルトで無効です。

...メッセージがローカルアカウント宛である場合を除く
メールが上記のローカルアカウントオプションから送信される時、認証を有効にした時は常に必要とされる場合、受信者がローカルアカウントである場合にメッセージを指定条件から免除する場合、このオプションをクリックします。つまり、ローカルアドレスからのメッセージがローカルアドレスに存在する時に、認証は必要とされません。このオプションはデフォルトで無効です。

...メッセージがドメインメールサーバからの場合を除く
ローカルアカウントオプションからのメッセージの場合、ドメインメールサーバ 65 から到着するメッセージを認証から除外することが常に必要な場合、このオプションをクリックします。

...メッセージがホワイトリストのIPやホストからの場合を除く
メールがホワイトリストの IPアドレス 226 や ホスト 223 からのものだった場合にSMTP認証を必要としない場合は、このオプションを有効にします。

認証証明書はメール差出人の証明書と一致させることが必要
認証について自身の証明書だけを使用する送信者が必要な場合、このオプションを使用します。従って、例えば、frank@example.comはfrank@example.comアカウント証明書を使用し認証が許可されます。frank02@example.com証明書が有効だった場合であっても、frank02@example.comを使用して認証を試みる場合、許可にされません。このオプションはデフォルトで無効です。

'postmaster','abuse'および'webmaster'からのメールは認証が必要
メールがローカルドメインの一つでpostmaster、abuseまたはwebmasterからのメールの場合、認証はデフォルトで必要です。これは多くのスパマーおよび不当なユーザが、それらのアカウントまたはエイリ

アスが、サーバに存在しメールをリレー、またはそれらの信頼すべきアドレスの1つとしてを使用することを試みるため知っているからです。

例外 - ドメイン

これらの設定を構成する時、ページ上部のドメイン:ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。SMTP認証設定を見直し編集するには、対応するドメインの**表示 / 編集**リンクをクリック、あるいはデフォルトの全体の設定値をドメインの設定にリセットするには、**リセット**をクリックします。

4.4.3 IPシールド

IPシールドは、SMTP MAIL FROMコマンド中に確認する、ドメイン名とそれに紐づいたIPアドレスのリストです。一覧のドメインからのSMTP接続要求は、そのドメインに対応したIPアドレスと一致した場合のみ受け付けられます。

設定

IPシールドを有効にする
IPシールドを有効にするにはこのチェックを有効にします。

FROMヘッダをIPシールドデータベースで確認する
IPシールドで、SMTP MAILに加え、メールのFROMヘッダのアドレスを比較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。

このオプションは、例えば特定の設定を行ったメーリングリストからのメールなど、特定のメールで問題を起こす場合があります。そのため、必要な場合にのみこのオプションを使用してください。

現在の定義ドメイン/IPセット

これは、メッセージがドメインの1つから要求される場合、チェックされるドメインおよび関連するIPアドレスのリストです。メッセージを配信しているサーバのIPアドレスは、対応するドメインについて一覧を示す必要があります。

有効なローカルユーザ宛のメッセージを除外する
デフォルトで、メッセージが有効なローカルユーザに送られる時は、メッセージを配信しているサーバはIPシールドにチェックされません。ローカルユーザに送られる時、メッセージをIPシールドから除外しない場合、このチェックボックスを解除します。

新規
リストに新規のドメイン/IPアドレスエントリを追加するために、**新規**をクリックします。これは、IPシールドエントリページを開きます。

編集
既存のエントリの編集は、リストからエントリをダブルクリック、またはエントリをクリックし編集を選択します。これは、IPシールドエントリページで、そのエントリを開きます。

削除
リストからエントリを削除するには、エントリを選択し削除をクリックします。

IPシールドエントリ

ドメインとIP情報

これは、新規のIPシールドエントリを作成または既存のエントリを編集する時に、開くページです。

保存して閉じる
IPシールドエントリと関連するドメイン、IPアドレスとコメントの追加あるいは編集した後、"保存して閉じる"をクリックするとエントリを保存し、IPシールドページに戻ります。

閉じる
情報を保存しないでIPシールドページに戻るには、"閉じる"をクリックします。

ドメイン
IPシールドに追加するドメイン名を、ここから入力します。

IPアドレス
上記である一覧を示されるドメインと関連するIPアドレスを入力します。メッセージが、このドメインから要求する時に、メッセージの配信サーバのIPアドレスは、このものと一致する必要があります。

コメント
エントリに関連するコメントのために、このエリアを使用します。

例外

正しいローカルユーザー宛のメールを除く
正しいローカルユーザー宛のメールをIPシールドから除外するにはこのオプションを有効にします。

認証済セッションを除く
認証済セッションから送信された受信メールをIPシールドから除外するにはこのオプションを有効にします。

ドメインメールサーバーからのメールを除く
ドメインメールサーバー 65 から届いたメールはデフォルトでIPシールドから除外されています。ドメインメールサーバーからのメールを除外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。

4.4.4 ダイナミックスクリーニング

ダイナミックスクリーニング機能を使用して、SecurityGatewayは疑わしいアクティビティを確認して、それに応じて応答する送信サーバの反応を追跡することができます。例えば、ダイナミックスクリーニングを使って、指定された数の"未知の受信者"エラーがそのIPアドレスにてメールセッション中に発生すると、今後の接続からサーバに対してIPアドレスを禁止することができます。指定された時間数で指定された回数を超えるサーバに接続する差出人を禁止することができ、指定された回数を超える認証試みに失敗する差出人を禁止することもできます。ただし、ダイナミックスクリーニング禁止は、永久的でありません。IPアドレスは、禁止が一覧を示されて以後、通過した各IPアドレスおよび指定する時間数だけ禁止されます。

ダイナミックスクリーニング

ダイナミックスクリーニングを有効にする
ダイナミックスクリーニング機能をアクティブにするために、このオプションをクリックします。ダイナミックスクリーニングはデフォルトで無効です。

指定回数以上のRCPTコマンドで失敗したIPの接続を禁止する
ダイナミックスクリーニングが使用可能な時、指定された数のRCPT試みがSMTPセッション中に失敗する場合、IPアドレスは一時的に禁止されます。それは多くのRCPTコマンドを送信するスパマーの一般の戦術で多くは無効なアドレスです。このオプションのデフォルト値は10です。

[xx]分間で[xx]回 以上接続するIPを禁止する
このオプションは、一定の時間に指定回数でSecurityGatewayに接続する許可を指定します。指定された時間に、指定回数の接続を越える場合、一時的に禁止されます。このオプションはデフォルトで無効です。

指定回数の認証を失敗したIPを禁止:
これは、送信者が一時的に禁止される前に認証に失敗する回数です。誤ったパスワードを使用している人は、失敗した認証試みを起こす一例です。デフォルトで、送信者が3回を認証に失敗する場合、IPアドレスは一時的に禁止されます。失敗した試みの回数に関係なく、これらの送信者を禁止しない場合、このチェックボックスを解除します。

指定時間(分)IPの接続を禁止:
これは、上記の制限の1つに違反する時、IPアドレスが禁止される時間です。デフォルトIPアドレスが禁止される時間は、10分です。

IP禁止後SMTPセッションを閉じる
IPアドレスが禁止される時、デフォルトによってSMTPセッションは直ちに閉じます。つまり、セッションは通常のSMTPプロトコルにおける後続のステップによっても継続することを許可しません; 接続は切断されます。直ちに禁止されたIPアドレスとの接続を切断しない場合、このチェックボックスを解除します。

例外

ホワイトリストIPアドレスおよびホストからのメッセージを除外する
デフォルトで、すべてのホワイトリスト 221 IPアドレスおよびホストは、ダイナミックスクリーニング制限から除外します。これらの制限をサポートするためにホワイトリストIPおよびホストも必要とする場合、このチェックボックスを解除します。

認証されたセッションからのメッセージを除外する
受信メッセージが認証されたセッションを通じて送信されている時、デフォルトでダイナミックスクリーニング制限から除外します。同様に制限を認証されたセッションに適用しない場合、このチェックボックスを解除します。

ドメインメールサーバからのメッセージを除外する
ドメインメールサーバ 65 から到着しているメッセージは、デフォルトでダイナミックスクリーニングから除外します。ドメインメールサーバをダイナミックスクリーニング制限から除外しない場合、このチェックボックスを解除します。

禁止IP一覧

このエリアは、各々が禁止されてから現在禁止されたIPアドレスおよび期間の一覧を示します。エントリを選択し上記のツールバーで**削除**ボタンをクリックすることでエントリを削除できます。

4.4.5 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接続で使用できます。SecurityGateway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ます。デフォルトで、国別スクリーニングは認証用の通信のみをブロックしています。これは、例えば特定の国のユーザーはおらず、ただ、その国からのメール受信は行いたい、といった場合に便利です。この場合はサーバーへログインしようとする接続のみをブロックできます。

国別スクリーニングの有効化
国別スクリーニングを使用する場合は、このチェックボックスをクリックし、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。

...認証だけをブロック（認証を要求しないメールは許可されます）
デフォルトで、国別スクリーニングは認証しようとする受信接続のみをブロックします。認証を必須としない接続は許可されます。対象の国からの接続全てを拒否するには、このチェックボックスを解除してください。

メールへ 'X-SGOrigin-Country' ヘッダを追加
デフォルトで、国別スクリーニングが有効化されていると、SecurityGatewayは、コンテンツフィルタや他の目的のため、メールへ"X-SGOrigin-Country"ヘッダを挿入します。ヘッダには名前の代わりに2文字のISO 3166国と地域用コードが含まれます。メールへヘッダを挿入しない場合はチェックボックスを無効にして下さい。

全てを選択/選択解除
このボタンで一覧のすべての国を選択または選択解除します。

除外

ホワイトリストのIPアドレスからの接続を除外
デフォルトで、ホワイトリストのIPアドレス 226 からの接続は全て国別スクリーニングの制限から除外されています。ホワイトリストのIPからであっても国別スクリーニングを有効にする場合はこのチェックボックスを解除してください。

除外 - ドメイン

設定画面の上部にある「対象ドメイン」ドロップボックスから特定のドメインを選択すると、設定を保存した後、ドメインが一覧へ表示されます。表示/編集リンクでドメイン用の国別スクリーニング設定を確認したり編集したりする事ができます。リセットをクリックすると、ドメインの設定がデフォルトの全体設定で上書きされます。

4.4.6 ターピット

指定された数のRCPTコマンドがメッセージの差出人から受信されると、ターピットで故意に接続を減速することを可能にします。これは、スパマーがドメインに勝手に送りつけるバルクメール(スパム)を送信しようと試みを防止します。ターピットを開始する前に、許可されるRCPTコマンドの数、以降のRCPT commandが接続中に、そのホストから受信するごとに接続を遅延する秒数を指定することができます。この技術の背後の論法は、各メッセージを送信するためにスパマーに過度に長い一定の期間を利用する場合、将来に再び試みることを防止します。

ターピット設定

ターピットを有効にする
ターピット機能を有効にするには、このチェックボックスを選択します。ターピットは、デフォルトで無効です。

SMTP EHLO/HELOの遅延(秒単位):
EHLO/HELO SMTPコマンドに対するSecurityGatewayの応答を遅延させるために、このオプションを使用します。わずか10秒でも応答を遅延させ、受信されるスパムの量を減らすことで、処理時間の著しい量を節約することができます。頻繁に、スパマーはメッセージの急速な配信に依存し、従って、長い間EHLO/HELOコマンドに対する応答を待ちません。少ない遅延でも、スパムツールは応答を待たずに、時々断念します。MSAポート(メールプロトコル 76ページで指定)の接続は、この遅延から常に除外されています。このオプションのデフォルト設定は、0で、EHLO/HELOが遅れないことを意味します。

日別のHELO/EHLO遅延時間
EHLO/HELO遅延を指定した時、認証されたSMTPセッションが生じたIPアドレスは一日につき一回だけ遅延をします。この遅延は、セッションが認証される最初の時の直前に発生します。このオプションはデフォルトで無効です。

SMTP RCPTターピットしきい値:
SecurityGatewayでホストのターピットまたは遅延を開始する前に、メールセッション中に、特定のホストに対してSMTP RCPTコマンドの回数を指定するために、このオプションを使用します。例えば、この回数が10を設定され送信ホストが20のアドレス(すなわち20のRCPTコマンド)にメッセージを送信することを試みる場合、SecurityGatewayは通常最初の10個を許可し、下記でSMTP RCPTターピット遅延(秒単位)オプションで指定される秒数の各次のコマンド後、休止します。このオプションのデフォルト値は5です。

SMTP RCPTターピット遅延(秒単位):
SMTP RCPTターピットしきい値、ホストについて到達した時の、指定ホストでメールセッション中に、各次のRCPTコマンドは受信後、SecurityGatewayが休止する秒数です。各次のRCPTコマンドはデフォルトで10秒遅延します。

倍率:
この値は、基準ターピット遅延が時間とともに増加する乗数です。ターピットしきい値が到達される場合、ターピット遅延はセッションに適用され、各遅延は、セッションの次の遅延の期間に確定するこの値によって増やされます。例えば、ターピット遅延が10に、倍率が1.5に設定される場合、最初の遅延は10秒で、第2は15秒、第3の22.5、続いて33.75などです(すなわち10 x 1.5 = 15, 15 x 1.5 = 22.5)。デフォルト倍率は1で、遅延が増加しないことを意味します。

例外

ホワイトリストの差出人からのメッセージを除外する
デフォルトでホワイトリスト 221送信者から到着しているすべてのメッセージは、タービット制限から除外されます。同様にホワイトリスト送信者をタービットルールの対象とする場合、このチェックボックスを解除します。

認証されたセッションからのメッセージを除外する
認証されたセッションを通じて到着するメッセージは、デフォルトでタービットから除外します。このチェックボックスを解除すると、タービット制限は同様にそれらのメッセージに適用されます。

ドメインメールサーバからのメッセージを除外する
ドメインメールサーバ 65の1台から到着しているメッセージは、デフォルトでタービットから除外します。ドメインメールサーバをタービット制限から除外しない場合、このチェックボックスを解除します。

4.4.7 帯域幅制限

グローバルおよび個々のドメインについて、この帯域制限は、SecurityGatewayにより使用される帯域幅の消費を管理下に置くことを可能にします。帯域制限を使用して、各受信および送信SMTPセッションが進捗率をコントロールすることができます。さらに、ホワイトリスト差出人、認証されたセッションおよびドメインメールサーバを、これらの規制から除外することができます。帯域制限システムは、両方の送受信SMTPセッション(両方のオプションがデフォルトで無効にされるにもかかわらず)についての10のデフォルト値によって毎秒キロバイト(KB)で調整されます。

帯域制限が管理する前に、最高8KBのデータは送/受信できます。従って、下記で指定した総計に従い、これは制限を越える可能性があります。

帯域制限

受信SMTP接続を制限:[xx]KB/秒
受信SMTPセッションの帯域幅を制限する場合、このオプションをクリックします。このオプションのデフォルト値は毎秒10KBですが、デフォルトは無効です。

送信SMTP接続を制限:[xx]KB/秒
送信SMTPセッションの帯域幅を制限する場合、このオプションをクリックします。このオプションのデフォルト値は毎秒10KBですが、デフォルトは無効です。

除外

ホワイトリストの差出人からのメッセージを除外する
帯域制限からすべてのホワイトリスト送信者 221を除外する場合、このオプションを選択します。このオプションは、デフォルトで無効です。

認証されたセッションからのメッセージを除外する
セッションが認証される場合セッションを帯域制限から除外する場合、このオプションを使用します。このオプションは、デフォルトで無効です。

ドメインメールサーバからのメッセージを除外する
ドメインメールサーバ[65]を帯域制限から除外する場合、このチェックボックスを選択します。このオプションは、デフォルトで無効です。

例外 - ドメイン

これらの設定を構成する時、ページ上部のドメイン:ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。帯域制限設定を見直し編集するには、対応するドメインの**表示 / 編集**リンクをクリック、あるいはデフォルトの全体の設定値をドメインの設定にリセットするには、**リセット**をクリックします。

4.4.8 アカウントハイジャック検出

アカウントハイジャック検出

この画面のオプションを使うとハイジャックされた可能性のあるアカウントを検出し、メール送信させないように設定する事ができます。例えば、スパム送信者が何らかの方法でアカウントのメールアドレスとパスワードを取得したばくぁい、この機能を使う事でスパム送信者がアカウントを使ってスパム送信を行う事を防ぐ事ができます。ここでは、アカウントが指定した分数の間に最大何通のメール送信を行えるかと、最大値に到達した際アカウントを無効化するかどうかを設定できます。各ユーザーのアカウント設定ページ[27]から、「このアカウントをアカウントハイジャック検出から除外する、のオプションを有効化する事で、特定アカウントをハイジャック検出から除外する事もできます。ユーザーオプション[60]ページからは、ユーザーのデフォルト値を設定する事ができます。

アカウントハイジャック検出はセッションが認証済のローカルアカウントにのみ適用され、Postmasterアカウントが自動的に除外されます。

アカウントは次の時間内にこれ以上のメール送信はしない [xx] **メッセージを超える** [xx] **分間**
ローカルアカウントが指定した分の間に指定した数を超えるメールの送信を防ぐためのオプションです。アカウントが許可された数を超えるメールを送信した場合、SecurityGatewayは通信を遮断する事はしませんが、指定数を超えたメールを452エラーで指定時間を経過するまで一時エラーとします。その後、メールの再送を試みます。

この上限に達したアカウントを無効化する
許可されているメール送信数を超えたメール送信を行ったアカウントを無効化する場合はこのボックスを有効化します。この時、サーバーは552エラーを返し、接続は遮断され、アカウントはすぐに無効化されます。無効化されたアカウントはメールの送信や受信メールの確認を行う事はできませんが、SecurityGatewayは対象アカウント宛のメール受信を継続して行います。最後に、アカウントが無効化されていると、メールはpostmasterへ送られます。postmasterが届いたメールへ返信すると、アカウントは再度アクティブになります。

例外 - ドメイン

"ドメイン:" のドロップダウンで特定のドメインを選択している場合、設定を保存した後は選択したドメインだけが表示されます。表示/編集リンクから、アカウントハイジャック検出設定を確認したり編集する事ができます。リセットをクリックする事で、ドメインの設定はデフォルトの全体設定値で上書きされます。

4.5 RMail™

RMail™ とは RPost® の提供しているサービスで宛先側で特別なソフトウェアは必要ありません。RMailは企業規模、業界、職種を問わずご利用頂けます。

RMailサービスは RPost Registered Email® テクノロジをベースにした、メールの配信証明における世界標準サービスです。RMail サービスは、貴社のメールシステムへ次の機能を追加します:

- 重要なメールを記録し配信時や開封時に通知します。
- 配信、時間、内容を証明します。
- 機密メールや添付ファイルを簡単に暗号化して、セキュリティや法令順守を実現します。
- RMail™ で操作、配送、開封の処理やE-署名の付与を簡単に行えるようになります。

試用版のRPostアカウントを使って、ユーザーは月5通までの暗号化メールを送受信できます。追加が必要な場合はRPostから購入できます。メールの最大数を大きくするのに必要な情報や料金については、 RPost.com から詳しい情報を確認して下さい。

RMailサービスはセキュリティ | RMailページ 191 から設定でき、コンテンツフィルタルールのアクション 207 としても設定できます。

暗号化

RMail暗号化サービスを有効にする
RMailの暗号化サービス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。Security Gatewayでは、全てのメールでRMail暗号化を使用するか、特定の件名から始まるメールに対してのみRMail暗号化を使用するか選択する事ができます。

予定表の会議招集を除外する
会議招集メールをRMail処理から除外するにはこの設定を有効にします。

すべてのメッセージを暗号化する
RMailを使って全てのメールを暗号化す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だけを暗号化する...
RMailを使って指定したキーワードから始まる件名のメールだけを暗号化する場合はこのオプションを選択します。

次の件名から始まるメッセージを暗号化する...
上記の、これらのメッセージだけを暗号化する‥を選択すると、RMailは指定したキーワードから始まる件名のメールだけを暗号化します。キーワードの管理に、「追加/削除」ボタンを使用してください。

件名から対象タグを削除
RMail処理のきっかけとなったメールから対象の件名タグを削除する場合はこのオプションを有効にします。

次へ送るメッセージだけを暗号化する...
特定の宛先に対して送信するメールのみを暗号化対象とする場合はこのオプションを有効にします。

追跡 & 証明

RMail追跡 & 証明サービスを有効にする
RMailのメールの追跡と証明サービスを使う場合はこのボックスをクリックします。SecurityGatewayで、全てのメールを対象とするか、指定したキーワードを含むメールのみを対象にするかを選択できます。ユーザーはメールを追跡し、受信したタイムスタンプのレポートを受け取る事ができます。このレポートは、メールの到着及び開封証明として使用する事ができます。

予定表の会議招集を除外する
会議招集メールをRMailの追跡 & 証明サービスから除外するにはこの設定を有効にします。

すべてのメッセージを追跡する
RMailで全てのメールの追跡と証明サービスを使用す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だけを追跡する...
RMailを使って指定したキーワードのメールにて追跡と証明サービスを使用する場合はこのオプションを選択します。キーワードはメールの件名ヘッダか本文を対象にできます。

件名や本文に次の文字が含まれているメッセージを追跡する...
上記のこれらのメッセージだけを追跡する...を選択すると、RMailは指定したキーワードを件名か本文に含むメールのみで追跡と証明サービスを利用します。キーワードの管理に、「追加/削除」ボタンを使用してください。

件名から対象タグを削除
RMailの追跡 & 証明サービスのきっかけとなったメールから対象の件名タグを削除する場合はこのオプションを有効にします。

E-署名

RMail E-署名サービスを有効にする
RMailのE-署名サービスを使ってドキュメントへ署名を付与する場合はこのボックスをクリックします。SecurityGatewayでは、全てのメールでRMail暗号化を使用するか、指定のキーワードを含むメールに対してのみRMailE署名サービスを使用するかを選択できます。

予定表の会議招集を除外する
会議招集メールをRMailの署名サービスから除外するにはこの設定を有効にします。

すべてのメッセージに署名する
全てのメールへ電子署名を付与するにはこのオプションを選択します。

次のメッセージにだけ署名する...
指定したキーワードのメールのみ電子署名を使用する場合はこのオプションを選択します。キーワードはメールの件名ヘッダか本文を対象にできます。

件名や本文に次の文字が含まれているメッセージに署名する...
上記の次のメッセージにだけ署名する...を選択すると、指定したキーワードを件名か本文に含むメールでのみRMailのE署名サービスが有効になります。キーワードの管理に、「追加/削除」ボタンを使用してください。

件名から対象タグを削除
RMailの署名のきっかけとなったメールから対象の件名タグを削除する場合はこのオプションを有効にします。

4.6 情報漏えい保護

メッセージコンテンツフィルタリング[202]システムを元に、情報漏えい保護機能ではフィルタリングルールを使って、機密情報を含んだメールを検査し、配信を防ぐ事ができます。データの検索用に、多くのルールが予め用意されています：クレジットカード番号、銀行のアカウント情報、パスポート番号。これらのルールを有効化するとデフォルトでは送信メールにのみ適用され、ルールにマッチした場合は管理隔離[251]へ配信されます。こうしたルールは他のルール同様に管理されます。

このページでは情報漏えい保護ルールの管理が行えます。ここでは、ルールの作成や編集、削除が行え、チェックボックスをクリックするだけでルールの有効化や無効化が行えます。メッセージコンテンツフィルタリングルールと同様、情報漏えい保護ルールで処理されたメールをSecurity Gatewayがどのように処理するかを指定する事ができます。特定のヘッダの有無や、特定の送信者や受信者のチェック、ヘッダや本文に含まれる特定の文字列検索、メッセージサイズ、その他様々な条件に一致したメール検索のためのルールを作成する事ができます。メールがルールに一致した際、メールを拒否、削除、隔離、コピー、他のアドレスへの転送といった処理を行う事ができます。

情報漏えい保護ルールの一覧には、有効、説明、プレビューの3つの列が含まれています。有効の列には各エントリのチェックボックスが表示されており、ルールの有効化や無効化を行う事ができます。説明の列には作成時に付与したルールの名称が記載されています。プレビューには各ルールのアイコンが表示されており、マウスカーソルを合わせるとツールチップが表示されます。ツールチップには情報漏えい保護ルールエディタ[194]でルール作成時に使用したSieveスクリプト[228]が表示されます。

ページ上部のツールバーには次の4つのオプションがあります：

新規
新規をクリックすると情報漏えい保護ルールエディタ[194]が起動し、新しいルール作成が行えます。

編集
ルールを選択しツールバーの編集をクリックすると情報漏えい保護ルールエディタ[194]が起動します。ルールをダブルクリックし同様の画面を表示させる事もできます。

削除
1つまたは複数のルールを削除する場合は、対象のエントリを選択し、削除をクリックします。削除するかどうかを確認するためのダイアログが表示されます。複数エントリはCtrlとShiftキーで選択できます。

ドメイン：
ドメインのドロップダウンリストで一覧で表示するルールを選択できます。全てのドメインへ適用される全体ルールか、ドメイン専用のルールを表示できます。

情報漏えい保護ルールエディタ

情報漏えい保護ルールエディタで新しいルール作成や既存のルール編集が行えます。新しいルールを作成するには、新規をクリックしエディタ内で上から順に必要なオプションを設定します。完了したら、保存か閉じるで新しいルールを作成します。

ルールは有効
このボックスは新しいルール作成時チェックしておく必要があります。既存のルールについては、ルールを無効化する際このボックスをクリアします。無効化されたルールはSecurityGatewayでメールの検査に使用されません。このオプションは情報漏えい保護ルールー覧の有効の項目と同様です。

ドメイン:
このルールが適用されるドメインを選択するために、このオプションを使用します。"--グローバル--"を選択すると、SecurityGatewayは全てのドメインのメールをテストします。特定のドメインを選択すると、その特定のドメインの送受信メッセージだけがテストされます。

ルール名:
ここのルールの説明を入力します。このオプションは情報漏えい保護ルールー覧の説明の列に対応しています。

次の場合ルールを適用:

すべての条件が一致(AND)
下記で提供するテスト状況の全部を満たす場合に、メッセージがルールにマッチする場合、このオプションを選択します。これは、テスト条件に関して論理的"AND"を実行します。つまり、「条件Aが真で、且つ条件Bが真である場合、指定された処置を実行します」。

任意の条件が一致(OR)
下記で提供するテスト条件のいずれかを満たす時にメッセージがルールにマッチする場合、このオプションを選択します。これは、テスト条件に関して論理的"OR"を実行します。つまり、「条件A、または、条件Bが真である場合、指定された処置を実行します」。

条件:
このチェックボックスはルールについて提供したテスト条件の全部を示します。そして、メッセージがルールに合致する場合、管理される処置が続きます。ボックスでその条件をクリックすることによって、条件を編集することができます。条件の隣の"(Remove)"をクリックすることによって、条件を取り除くことができます。新規の条件を追加するには、下記の"**このルールの条件を追加するには、ここをクリックします**"リンクを使用します。

このルールの条件を追加するには、ここをクリックします
条件を追加するために、条件ボックスの下で**このルールの条件を追加するには、ここをクリックします**リンクをクリックします。条件を追加した後に、再びそのリンクをクリックすることによって、追加の条件を追加することができます。追加することができる条件の異なるタイプに関する情報については、ルールの条件 204を下記で確認します。

処理:
メッセージがルールの条件に合致する時に、実行する処置を、このリストから選択します。追加のデータが選択された処置へ必要な場合、対応するコントロールは、データを入力するために処置の下に現れます。追加できる処理の種類に関する情報は、後述の処理 197を参照してください。条件設定や処理の選択が完了したら、保存して閉じるをクリックすると、新しいルールが一覧へ追加されます。

ルール条件

ルールへテスト用の条件を追加する場合は、「このルールへ条件を追加するにはこちらをクリック」リンクから、ルール条件用の画面を起動します。テスト条件を使うには、まずメッセージの中で、テストや比較を行いたい属性やアイテムを指定します。次に、アイテムに含まれる特定の文字列、指定した文字列が完全一致で含まれているかどうか、特定のヘッダが存在するかどうか、といった、比較方法を指定します。テスト対象とする様々なアイテムは、数々の方法でテストする事ができます。アイテムとテスト方法を選択し、必要な情報を入力したら、保存と閉じるをクリックし、条件をルールへ追加します。

比較するアイテム:
メッセージ内でテストするためのアイテムは次の通りです。

- **MAIL (From)**— このテストではSMTPの「MAIL From」コマンドで渡される値を使用します。これはメールの送信元ですが、必ずしもメールのFromヘッダと一致する必要はありません。Fromヘッダに追加又は異なる情報が追加されている事はよくあります。9通りのテストや比較方法(下記を参照)に加え、「Is local user」や「Is not local user」を使ったテストも行えます。
- **RCPT (To)**— — このテストではSMTPの「RCPT To」コマンドで渡される値を使用します。これはメールの送信先ですが、必ずしもメールのToヘッダと一致する必要はありません。Toヘッダに追加又は異なる情報が追加されている事はよくあります。9通りのテストや比較方法(下記を参照)に加え、「Is local user」や「Is not local user」を使ったテストも行えます。
- MAIL及びRCPT— このアイテムはSMTPの「MAIL From」とSMTPの「RCPT To」両方のコマンドでメッセージが社内向け、外部向け、社内間(下記「追加のテスト方法」を参照)のどれに該当するのかを確認するのに使用します。
- **IP**— このアイテムを選択し、送信サーバーやクライアントのIPアドレスでのテストを行います。
- **HEADER**— 特定のヘッダを比較する場合はこれを選択します。選択すると、ヘッダ名のオプションが表示され、条件として使用するヘッダ名を指定する事ができます。9つの一般的な方法に加え、「ヘッダが存在」や「ヘッダが存在しない」を使用する事ができます。**注意点**: ヘッダ名を指定するとき、ヘッダ名にコロンは使用しないでください。例えば、ヘッダ名を「From」とする際、「From:」と入力しないでください。
- **Subject**— メールの`Subject` ヘッダです。メールの件名と比較してテストする場合はこのアイテムを選択します。
- **Body**—メールの本文と比較してテストする場合はBodyを選択します。
- **本文又は件名** — 件名又は本文がルールと一致した場合にTrueを返すにはこのアイテムを選択します。これはルールの作成を簡単にするためのアイテムで、本文の文字列を検索するためと件名の文字列を検索するための2つのルール又はOR条件を使ったルールと同じ条件のルールを効率よく作成する事ができます。

比較方法:
上記の比較するアイテムで選択されたアイテムのテストや比較の方法が、この一覧で確認できます。全部または一部のアイテムをテストする方法には様々な種類があります。MAILとRCPTアイテムは独自の比較方法を使用しており、Mail (From), RCPT (To), Headerでは別の方法でさらにテストが行えます。

一般的なテスト方法:
比較するアイテムで選択したアイテムのテストには、それぞれ検索値として以下のテスト方法の何れかを選択します。すべての比較方法はMAILとRCPTを除くすべての検索に使用できます。この2つについては独自の比較方式を使う必要があります。

- **含む**– この方法が選択される時、比較は、検索値が、上記比較するアイテムの文字列に完全又は部分一致した場合"True"です。例えば、比較するアイテムとしてMAIL (From)を選択する場合、"example.com"が検索文字で比較方法に「含む」を選び、その場合、"example.com"があるアドレスからのメッセージは、条件に合致します。
- **含まない**– 検索値が部分文字列または上記で指定される比較するアイテムの一部でない場合、一致または"True"です。例えば、比較するアイテムとしてMAIL (From)を選択する場合、"example.com"が検索文字で比較方法に「含まない」を選び、その場合、"example.com"があるアドレス以外からのメッセージは、条件に合致します。
- **単語を含む**– これは「含む」に似ていますが、単語の境界 処理を行っており、文字列が続いているもののみを対象とします。これにより、手動で `\b(word1|word2|word3)\b` のような正規表現用のフォーマットを作成する必要がなくなります。例えば、メール本文に「cat」という単語を含むものを検索する、というルールを作成した場合、「cat」という単語全体を使っているメッセージのみが一致します。本文にcatfishやcertificateのような単語を含んでいるものは一致対象とはなりません。
- **単語を含まない**– これは「含まない」に似ていますが、単語の境界 処理を行っており、文字列が続いているもののみを対象とします。これにより、手動で `\b(word1|word2|word3)\b` のような正規表現用のフォーマットを作成する必要がなくなります。例えば、メール本文に「cat」という単語を含むものを検索する、というルールを作成した場合、「cat」という単語全体を使っているメッセージのみが一致します。本文にcatfishやcertificateのような単語を含んでいるものは一致対象とはなりません。
- **等しい**– これは「含む」に似ていますが、比較は、検索値が、上記比較するアイテムの文字列に完全又は部分一致した場合"True"です。例えば、比較するアイテムとしてMAIL (From)を選択する場合、"example.com"が検索文字で比較方法に「含む」を選び、その場合、"example.com"があるアドレスからのメッセージは、条件に合致します。
- **同じでない**– この種類の比較は、先の方法の正反対です。比較するアイテムの値が必ずしも検索文字と同じでない場合、比較は合致(True)します。例えば、比較するアイテムとしてIPを選択する場合、それから、"192.168.0.1"が検索文字として「等しくない」を比較方法に選びます。その場合、そのIPアドレス以外から到着するメッセージは、条件に合致します。
- **次から始まる**– 上記で指定するアイテムの先頭からの値が検索文字と合致する条件をtrueとする場合、この比較を使用します。例えば、比較するアイテムとしてSubjectおよび検索文字を"[allstaff]"として選択する場合、"[allstaff]"で始まるSubject行を持つメッセージすべては条件に合致します。
- **次から始まらない**– これは、先の比較タイプの正反対です。上記で指定するアイテムの先頭からの値が検索文字と合致しない条件をtrueとする場合、この比較を使用します。例えば、比較するアイテムとしてSubjectおよび検索文字を"[allstaff]"として選択する場合、"[allstaff]"を先頭に持たないSubject行のメッセージすべては条件に合致します。
- **次で終わる**– この比較は、比較するアイテムの値が検索文字で終える時はいつも、条件が合致することを意味します。例えば、比較するアイテムとしてRCPT (To)を選択、および比較方法としての[次で終わる]」、". cn"を検索文字として指定する場合、". cn"をアドレス末尾にもつメッセージすべて条件に合致します。
- **次で終わらない**– この比較は、比較するアイテムの値が検索文字で終わらない時、条

件が合致することを意味します。例えば、比較するアイテムとしてRCPT（To）を選択、および比較方法としての[次で終わらない]、".cn"を検索文字として指定する場合、".cn"をアドレス末尾に持たないメッセージすべて条件に合致します。

- **正規表現の一致** – 前述のオプションを比較するため、**正規表現**を使用する場合、このオプションを選択します。

追加の比較方法:

- **ローカルユーザーである**– この比較方法は、上記のMAIL（From）およびRCPT（TO）オプションにだけ利用できます。アドレスがローカルSecurityGatewayユーザである時に条件が合致する必要がある場合、このオプションを選択します。例えば、比較するアイテムとしてMAIL（From）を選択する場合、ローカルユーザからのメッセージだけは、条件に合致します。
- **ローカルユーザーでない**– この比較方法は、上記のMAIL（From）およびRCPT（TO）オプションにだけ利用できます。アドレスがローカルSecurityGatewayユーザでない時に条件が合致する必要がある場合、このオプションを選択します。例えば、比較するアイテムとしてMAIL（From）を選択する場合、リモートユーザからのメッセージは、条件に合致します。ローカルユーザからのメッセージは合致しません。
- **ヘッダが存在** – 比較するアイテムとして選択されたヘッダを持つ時、このオプションを利用できます。このオプションを選択して、提供されるオプションでヘッダ名を指定する時に、指定されたヘッダがメッセージの中に存在する場合だけ、条件は合致します。例えば、ヘッダ名として"X-My-Custom-Header"を指定する場合、そのヘッダをもつすべてのメッセージは、条件に合致します。そのヘッダのないメッセージは、合致しません。
- **ヘッダが存在しない**–比較するアイテムとして選択されたヘッダを持つ時、このオプションを利用できます。このオプションを選択して、提供されるオプションでヘッダ名を指定する時に、指定されたヘッダがメッセージの中に存在しない場合だけ、条件は合致します。例えば、ヘッダ名として"X-My-Custom-Header"を指定する場合、そのヘッダを持たないすべてのメッセージは、条件に合致します。そのヘッダをもつメッセージは、合致しません。
- **メッセージが[Inbound|Outbound|Internal]である/ない**– この比較方法はMAILとRCPTにのみ使用できます。SMTPのMAIL FromとRCPT Toの値はメールが受信・送信・内部のメールか否かを検証するのに使用されます。

  Inbound– ローカルユーザー以外からローカルユーザー宛のメッセージ

  Outbound– ローカルユーザーからローカルユーザー以外へのメッセージ

  Internal– 同一ドメインのローカルユーザー間でのメッセージ

処置

ルールの条件を設定したら、ルールエディタの処置オプションでメールがルール条件にマッチした際の処置を選択します。選択できるアクションは次の7つです:

- **拒否** – ルールの条件に合致するメッセージを拒否する場合、この処置を選択します。このオプションを選択すると、メッセージを拒否する際の応答テキストを指定するためのSMTP応答オプションが表示されます。例えば、SMTPプロセス中にメッセージを拒否するルールにマッチした際、SMTP応答オプションで"We don't want your spam!"を使用すると、SecurityGatewayは"550 We don't want your spam!"を送信します。

- **破棄** – ルールの条件に合致する時に、この処置はメッセージを廃棄します。Reject処置とは異なって、このオプションはSMTP応答も配信失敗メッセージも送信しません。メッセージが削除されます。
- **隔離** –この処置が選択されると、受信者がローカルユーザの場合、ルールの条件にマッチしたメールは受信者の隔離[250]へ配信されます。受信者がリモートユーザである場合、メッセージは代わりに管理隔離[251]に入れられます。
- **隔離(管理)** – ルール条件にマッチするとメールは 管理隔離[251] へ配信されます。
- **リダイレクト** – この処置を使用することは、メッセージをルールの条件に合致する時に、異なるアドレスにリダイレクトします。メッセージをリダイレクトするメールアドレスを指定することができるように、Toオプションは処置の下に提供されます。リダイレクトされたメッセージは、最初の受信者に配信されません。処置で指定されるアドレスに送られます。
- **コピー**– メッセージを追加のメールアドレスへコピーする場合、このオプションを使用します。メッセージを送信する追加のメールアドレスを指定することができるように、Toオプションは処置の下で提供されます。これは、両方の最初の受信者を除いて、リダイレクトと類似し、処置で指定されるアドレスは、メッセージのコピーを受信します。メッセージを複数のアドレスへコピーする場合、各アドレスへ追加のルールを作成します。
- **注意(警告)を送信** – メッセージがルールの条件に合致する場合、メモまたは警報メールメッセージを送信するために、この処置を使用します。この処置が選択される時に、オプションはメモのTo, From, Subjectおよびメッセージテキスト(メッセージの本文)を指定するために提供されます。動的に特定の情報を含むメモで使用することができるマクロがあります。SecurityGatewayがメモのテキストでマクロを検出すると、対応する値でそのマクロを置き換えます。

  $SENDER$– これは、ルールに合致したメッセージのために使用されたSMTP MAIL Fromアドレスと置き換えられます。例えば、"sender@ example.net"。

  $SENDERMAILBOX$– このマクロは、SMTP MAIL Fromコマンドで渡されたメールアドレスのメールボックス部分だけと置き換えられます。例えば、"sender@ example.net"アドレスから"sender"。

  $SENDERDOMAIN$– このマクロは、SMTP MAIL Fromコマンドで渡されたメールアドレスのドメイン部分だけと置き換えられます。例えば、"sender@ example.net"アドレスから"example.net"。

  $RECIPIENT$– これは、ルールに合致したメッセージで使用されたSMTP RCPT Toアドレスと置き換えられます。例えば、"recipient@ example.com"。

  $RECIPIENTMAILBOX$– このマクロは、SMTP RCPT Toコマンドで渡されたメールアドレスのメールボックス部分だけと置き換えられます。例えば、"recipient@ example.com"アドレスの"recipient"部分です。

  $RECIPIENTDOMAIN$– このマクロは、SMTP RCPT Toコマンドで渡されたメールアドレスのドメイン部分だけと置き換えられます。例えば、"recipient@ example.com"アドレスの"example.com"部分です。

  $SUBJECT$– このマクロは、合致したメッセージのSubjectヘッダのコンテンツと置き換えられます。

  $MESSAGEID$– これは、メッセージのMessage-IDヘッダの値と置き換えられます。

  $DATESTAMP$– このマクロはメッセージの日付と置き換えられます。

  $CURRENTTIME$– SecurityGatewayがメモを作成する時に、これは現在の時刻と置き換えられます。

$HELONAME$– これは、合致したメッセージがSecurity Gatewayによって受信される時に、SMTPプロセス中に、渡されたHELOドメインです。

- **メッセージスコアに追加** – メッセージがルールの条件に一致した場合、メッセージに指定したポイントを追加するには、この処置を使用します。
- **Registered Email (RMail)で送信** – この処置を選択すると条件にマッチしたメールがRMailの Registered Emailで送信されます。

  暗号化 – メールを暗号化する場合はこのオプションを選択します。

  追跡と証明 – RMailの追跡と証明を使用する場合はこのオプションを選択します。

  E-署名 – RMailのE-署名でドキュメントへ署名を付与する場合はこのオプションを選択します。
- **メールをREQUIRETLS用にマーク** – メールで**RequireTLS**[104]を使うよう指定します。

- **セキュアウェブメールとして送信** – 通常のメール配信ではなく、Security Gatewayの セキュアメッセージ[92] ウェブポータルシステムでメールを送信する場合はこの処理を選択します。

正規表現

情報漏えい保護の ルール条件[195] では、比較するのに正規表現を使用する事ができます。正規表現(regexp)とは広い用途で使用されているシステムで、文字列はもちろん、文字列パターンにも対応います。正規表現(regexp)テキストパターンは、メタキャラクタと呼ばれるアルファベットの文字列や、(例えばabc, 123等の)特殊文字、又は両方の組み合わせで構成されています。パターンは文字列に対して使用され、マッチするかどうかを結果として返します。

Security Gatewayのregexps実装は、Perl互換の正規表現(PCRE)ライブラリを使用します。regexpの、この実装に関する詳細な情報は http://www.pcre.org/ および http://perldoc.perl.org/perlre.html を参照してください。

オライリーメディア社によって出版された*Mastering Regular Expressions, Third Edition* で正規表現を総合的に調べることができます。

メタキャラクタ

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。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	説明
\	メタキャラクタの前に使用すると、そのメタキャラクタをリテラルキャラクタとして扱います。これはメタキャラクタとして使用されている特殊文字を検索する場合に必要なものです。例えば[+]を検索する場合、[¥+]という表現が必要となります。

|	[または]の意味を持つキャラクタで、[|]で区切られたどれかのキャラクタにマッチします。例えば[abc|xyz]という表現は、[abc]または[xyz]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どの文字にもマッチします。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[^]には別の意味があります。対象文字列に合致することからかぎカッコの内で存続する文字を除外するために使用されます。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-&-123]または["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でなくグループ化の結果により置換されます。¥の後の数字はどのグループ表現を参照したいかを示します。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[1abc]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。

?	直前の文字が0回または1回現れることを表します。例えば、[1?abc]は[abc]または[1abc]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。

4.6.1 医学用語

情報漏えい保護[193]オプションではメール内の医学用語を検索し、スコアリング分析を元に特定の処理を実行させる事ができます。約2000の医学用語が事前設定されており、必要に応じて用語を追加したり削除したりする事で、ご自身の環境に最適な状態を作る事ができます。

各用語にはスコアが割り当てられており、メールは各用語と一致する文字列を検索し、対象用語のスコアの合計を算出します。計算されたスコアと同じ又は上回った場合のアクションを実行できます。隔離メールを選択し、RMail暗号化サービス[191]を適用する事もできます。また、受信メールを医学用語の検索対象から除外する事もできます。

設定

医学用語について送信されたメールを確認する
メールで医学用語をスキャンする場合はこのチェックをオンにします。各用語にはスコアが割り当てられていて、1通のメールに含まれる用語のスコア合計によって、特定の処理が指定されている場合は、対象の処理を実行します。

管理隔離するメッセージは、このスコア以上 [xx]
このオプションが有効で、メール内の医学用語スコアがここで指定している値と同じか値を超えた場合、メールは管理隔離[251]へ移動されます。

このスコア以上のメッセージには、RMail暗号サービスを使用する [xx]
このオプションが有効で、メール内の医学用語スコアがここで指定している値と同じか値を超えた場合、メールはRMail暗号化サービス[191]オプションを使って処理されます。

インバウンドメッセージを除外（受信者はローカルユーザーであり、送信者は別のドメインのユーザー）
このオプションは宛先がローカルユーザーで送信元が同じドメインのローカルユーザーでないメールを、医学用語検索から除外します。

内部メッセージを除外（送信者と受信者は同じドメイン内のユーザー）
このオプションは宛先と送信元がどちらも同じドメインのローカルユーザーのメールを、医学用語検索から除外します。

現在定義されている用語:

一覧には定義済の医学用語とこれに紐づいたスコアが表示されています。メールが医学用語の検索を行うためにスキャンされると、一覧の用語に割り当てられたスコアが加算されていき、総合スコアが算出されます。計算されたスコアと同じ又は上回った場合には、これに応じたアクションを実行できます。

用語の追加や編集
新規をクリックし、一覧へ新しい用語を追加するか、用語を選択し、編集をクリックしてから単語やスコアを変更します。用語とスコアを指定した後は、「保存して閉じる」をクリックします。

用語の削除
一覧から用語の削除を行うには、対象の用語を選択し削除をクリックします。用語の削除の確認を求めるダイアログが表示されるので、OKをクリックします。

医学用語一覧のインポート
医学用語の一覧をインポートするには:

1. プレーンテキストファイルを用意し、一行名に次のように記載します: `"Term","Score"`
2. 2行目から1行づつ用語とスコアを指定していきます。次のフォーマットになります: `"Abacavir sulfate","10"`
3. 完了したら、ファイルを".csv"の拡張子で保存します。例:`medical_terms.csv`
4. 医学用語のページで、インポートをクリックします。
5. ファイルを選択、をクリックし、作成したファイルを選択したら、開くをクリックします。
6. 現在使用している医学用語の一覧と、新しい一覧を差し替えたい場合は、既存の用語を削除、をクリックします。注意点: この操作により医学用語の一覧が全て削除され、新しい一覧に書き換えられます。単純に用途を追加したいだけであれば、このオプションは無効にしてください。
7. 用語のインポートをクリックします。
8. 閉じる、をクリックします。

医学用語一覧のエクスポート
現在定義している用語の一覧をエクスポートするには、エクスポートをクリックし、エクスポート先を選択し、保存をクリックします。

例外 - ドメイン

これらの設定を構成する時、ページ上部の**ドメイン**:ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。隔離オプションの設定を見直し編集するには、対象ドメインの**表示/編集**リンクをクリックします。全体のデフォルト設定値でドメイン設定を初期化するには、**リセット**をクリックします。

4.7 フィルタリング

4.7.1 メッセージ内容

このページは、メッセージコンテンツフィルタルールを管理するために使用されます。ここからルールの作成、編集、削除ができ、エントリのチェックボックスをクリックすることで、ルールを適用と停止ができます。フィルタルールは、SecurityGatewayが処理する各メッセージをテストする特定の基準を指定するために使用することができます。続いて、メッセージがルールに合致する場合、多くの処置を管理することができます。規定のヘッダの存在についてチェック、特定の送信者または受信者、ヘッダまたはメッセージ本文で特定のテキストの検索、メッセージのサイズに対するテストなどのするル

ールを作成することができますメッセージがルールのテストに合致する場合、ルールでメッセージを拒否、削除、隔離やコピー、別のアドレスへリダイレクトすることができます。

ルールが一覧を示すコンテンツフィルタは、3つの有効、説明およびプレビューカラムを持ちます。有効カラムには各エントリのチェックボックスを持ち、有効/無効の切り替えに使用します。説明カラムはルール名を持ちルールを作成する時に指定します。プレビューカラムは各ルールのためのアイコンを持ち、ポインタを重ねると、ルールについてヒントを示します。ヒントは、コンテンツフィルタルールエディタ[203]で作成されたルールで実際のSieve[228]スクリプトがあります。

ページ上部のツールバーには4つのオプションがあります:

新規
新規のルールを作成のためにコンテンツフィルタルールエディタ[203]を開くには新規クリックします。

編集
ルールを選択しコンテンツフィルタルールエディタ[203]で開には、ツールバーで**編集**をクリック、あるいは、ルールをダブルクリックします。

削除
ルールを削除するにはエントリをリストから選択し**削除**をクリックします。削除を確認するダイアログが現れます。CtrlおよびShiftキーを使用することで複数のエントリを選択することができます。

ドメイン:
ドメイン:ドロップダウンリストボックスで、表示するルールを指定できます。グローバルルール(すべてのドメインに適用されます)、または規定のドメインのルールを表示することができます。

コンテントフィルタルールエディタ

コンテンツフィルタルールエディタは、新規ルールの作成または既存のルールを編集するために使用します。新規ルールの作成は、コンテンツフィルタのツールバーで**新規**をクリックし、エディタで**上へ/下へ**オプションを設定します。設定を完了後には"**保存して閉じる**"をクリックします。

このルールを有効にする
このチェックボックスは、新規ルールを作成するためにチェックする必要があります。既存のルールについて、ルールを無効にするには、チェックボックスを解除します。メッセージをテストする時に、無効なルールはSecurityGatewayによって使用されません。このオプションは、コンテンツフィルタルール一覧で有効カラムに対応します。

ドメイン:
このルールが適用されるドメインを選択するために、このオプションを使用します。"--グローバル--"が選択される場合、SecurityGatewayドメインすべての送受信メッセージはルールに対してテストされます。特定のドメインが選択される場合、その特定のドメインの送受信メッセージだけがテストされます。

ルール名:
ここのルールの説明を入力します。このオプションはコンテンツフィルタルール一覧で説明カラムに対応します。

次の場合ルールを適用:

すべての条件が一致(AND)
下記で提供するテスト状況の全部を満たす場合に、メッセージがルールにマッチする場合、このオプションを選択します。これは、テスト条件に関して論理的"AND"を実行します。つまり、「条件Aが真、および、条件Bが真である場合、指定された処置を実行します」。

任意の条件が一致(OR)
下記で提供するテスト条件のいずれかを満たす時にメッセージがルールにマッチする場合、このオプションを選択します。これは、テスト条件に関して論理的"OR"を実行します。つまり、「条件Aが真、または、条件Bが真である場合、指定された処置を実行します。

条件:
このチェックボックスはルールについて提供したテスト条件の全部を示します。そして、メッセージがルールに合致する場合、管理される処置が続きます。ボックスでその条件をクリックすることによって、条件を編集することができます。条件の隣の"(Remove)"をクリックすることによって、条件を取り除くことができます。新規の条件を追加するには、下記の"**このルールの条件を追加するには、ここをクリックします**"リンクを使用します。

このルールの条件を追加するには、ここをクリックします
条件を追加するために、条件ボックスの下で**このルールの条件を追加するには、ここをクリックします**リンクをクリックします。条件を追加した後に、再びそのリンクをクリックすることによって、追加の条件を追加することができます。追加することができる条件の異なるタイプに関する情報については、ルールの条件 204を下記で確認します。

処理:
メッセージがルールの条件に合致する時に、実行する処置を、このリストから選択します。追加のデータが選択された処置へ必要な場合、対応するコントロールは、データを入力用に処置の下に表示されます。追加できる処理の種類に関する情報は、後述の処理 197を参照してください。条件設定や処理の選択が完了したら、保存して閉じるをクリックすると、新しいルールが一覧へ追加されます。

ルール条件

ルールへテスト用の条件を追加する場合は、「このルールへ条件を追加するにはこちらをクリック」リンクから、ルール条件用の画面を起動します。テスト条件を使うには、まずメッセージの中で、テストや比較を行いたい属性やアイテムを指定します。次に、アイテムに含まれる特定の文字列、指定した文字列が完全一致で含まれているかどうか、特定のヘッダが存在するかどうか、といった、比較方法を指定します。テスト対象とする様々なアイテムは、数々の方法でテストする事ができます。アイテムとテスト方法を選択し、必要な情報を入力したら、保存と閉じるをクリックし、条件をルールへ追加します。

比較するアイテム:
メッセージ内でテストするためのアイテムは次の通りです。

- **MAIL (From)**— このテストではSMTPの「MAIL From」コマンドで渡される値を使用します。これはメールの送信元ですが、必ずしもメールのFromヘッダと一致する必要はありません。Fromヘッダに追加又は異なる情報が追加されている事はよくあります。9通りのテストや比較方法(下記を参照)に加え、「Is local user」や「Is not local user」を使ったテストも行えます。
- **RCPT (To)**— — このテストではSMTPの「RCPT To」コマンドで渡される値を使用します。これ

はメールの送信先ですが、必ずしもメールのToヘッダと一致する必要はありません。Toヘッダに追加又は異なる情報が追加されている事はよくあります。9通りのテストや比較方法（下記を参照）に加え、「Is local user」や「Is not local user」を使ったテストも行えます。

- MAIL及びRCPT― このアイテムはSMTPの「MAIL From」とSMTPの「RCPT To」両方のコマンドでメッセージが社内向け、外部向け、社内間（下記「追加のテスト方法」を参照）のどれに該当するのかを確認するのに使用します。
- **IP**― このアイテムを選択し、送信サーバーやクライアントのIPアドレスでのテストを行います。
- **HEADER**― 特定のヘッダを比較する場合はこれを選択します。選択すると、ヘッダ名のオプションが表示され、条件として使用するヘッダ名を指定する事ができます。9つの一般的な方法に加え、「ヘッダが存在」や「ヘッダが存在しない」を使用する事ができます。**注意点：** ヘッダ名を指定するとき、ヘッダ名にコロンは使用しないでください。例えば、ヘッダ名を「From」とする際、「From:」と入力しないでください。
- **Subject**― メールのSubject ヘッダです。メールの件名と比較してテストする場合はこのアイテムを選択します。
- **Body**―メールの本文と比較してテストする場合はBodyを選択します。
- **本文又は件名** ― 件名又は本文がルールと一致した場合にTrueを返すにはこのアイテムを選択します。これはルールの作成を簡単にするためのアイテムで、本文の文字列を検索するためと件名の文字列を検索するための2つのルール又はOR条件を使ったルールと同じ条件のルールを効率よく作成する事ができます。

比較方法：
上記の比較するアイテムで選択されたアイテムのテストや比較の方法が、この一覧で確認できます。全部または一部のアイテムをテストする方法には様々な種類があります。MAILとRCPTアイテムは独自の比較方法を使用しており、Mail（From）, RCPT（To）, Headerでは別の方法でさらにテストが行えます。

一般的なテスト方法：
比較するアイテムで選択したアイテムのテストには、それぞれ検索値として以下のテスト方法の何れかを選択します。すべての比較方法はMAILとRCPTを除くすべての検索に使用できます。この2つについては独自の比較方式を使う必要があります。

- **含む**― この方法が選択される時、比較は、検索値が、上記比較するアイテムの文字列に完全又は部分一致した場合"True"です。例えば、比較するアイテムとしてMAIL（From）を選択する場合、"example.com"が検索文字で比較方法に「含む」を選び、その場合、"example.com"があるアドレスからのメッセージは、条件に合致します。
- **含まない**― 検索値が部分文字列または上記で指定される比較するアイテムの一部でない場合、一致または"True"です。例えば、比較するアイテムとしてMAIL（From）を選択する場合、"example.com"が検索文字で比較方法に「含まない」を選び、その場合、"example.com"があるアドレス以外からのメッセージは、条件に合致します。
- **単語を含む**― これは「含む」に似ていますが、単語の境界 処理を行っており、文字列が続いているもののみを対象とします。これにより、手動で \b(word1|word2|word3)\b のような正規表現用のフォーマットを作成する必要がなくなります。例えば、メール本文に「cat」という単語を含むものを検索する、というルールを作成した場合、「cat」という単語全体を使っているメッセージのみが一致します。本文にcatfishやcertificateのような単語を含んでいるものは一致対象とはなりません。
- **単語を含まない**― これは「含まない」に似ていますが、単語の境界 処理を行っており、文字列が続いているもののみを対象とします。これにより、手動で \b(word1|word2|

word3)\b のような正規表現用のフォーマットを作成する必要がなくなります。例えば、メール本文に「cat」という単語を含むものを検索する、というルールを作成した場合、「cat」という単語全体を使っているメッセージのみが一致します。本文にcatfishやcertificateのような単語を含んでいるものは一致対象とはなりません。

- **等しい**— これは「含む」に似ていますが、比較は、検索値が、上記比較するアイテムの文字列に完全又は部分一致した場合"True"です。例えば、比較するアイテムとしてMAIL (From)を選択する場合、"example.com"が検索文字で比較方法に「含む」を選び、その場合、"example.com"があるアドレスからのメッセージは、条件に合致します。
- **同じでない**— この種類の比較は、先の方法の正反対です。比較するアイテムの値が必ずしも検索文字と同じでない場合、比較は合致(True)します。例えば、比較するアイテムとしてIPを選択する場合、それから、"192.168.0.1"が検索文字として「等しくない」を比較方法に選びます。その場合、そのIPアドレス以外から到着するメッセージは、条件に合致します。
- **次から始まる**— 上記で指定するアイテムの先頭からの値が検索文字と合致する条件をtrueとする場合、この比較を使用します。例えば、比較するアイテムとしてSubjectおよび検索文字を"[allstaff]"として選択する場合、"[allstaff]"で始まるSubject行を持つメッセージすべては条件に合致します。
- **次から始まらない**— これは、先の比較タイプの正反対です。上記で指定するアイテムの先頭からの値が検索文字と合致しない条件をtrueとする場合、この比較を使用します。例えば、比較するアイテムとしてSubjectおよび検索文字を"[allstaff]"として選択する場合、"[allstaff]"を先頭に持たないSubject行のメッセージすべては条件に合致します。
- **次で終わる**— この比較は、比較するアイテムの値が検索文字で終える時はいつも、条件が合致することを意味します。例えば、比較するアイテムとしてRCPT (To)を選択、および比較方法としての[次で終わる]」、". cn"を検索文字として指定する場合、". cn"をアドレス末尾にもつメッセージすべて条件に合致します。
- **次で終わらない**— この比較は、比較するアイテムの値が検索文字で終わらない時、条件が合致することを意味します。例えば、比較するアイテムとしてRCPT (To)を選択、および比較方法としての[次で終わらない]、". cn"を検索文字として指定する場合、". cn"をアドレス末尾に持たないメッセージすべて条件に合致します。
- **正規表現の一致** — 前述のオプションを比較するため、正規表現 を使用する場合、このオプションを選択します。

追加の比較方法:

- **ローカルユーザーである**— この比較方法は、上記のMAIL (From)およびRCPT (TO)オプションにだけ利用できます。アドレスがローカルSecurity Gatewayユーザである時に条件が合致する必要がある場合、このオプションを選択します。例えば、比較するアイテムとしてMAIL (From)を選択する場合、ローカルユーザからのメッセージだけは、条件に合致します。
- **ローカルユーザーでない**— この比較方法は、上記のMAIL (From)およびRCPT (TO)オプションにだけ利用できます。アドレスがローカルSecurity Gatewayユーザでない時に条件が合致する必要がある場合、このオプションを選択します。例えば、比較するアイテムとしてMAIL (From)を選択する場合、リモートユーザからのメッセージは、条件に合致します。ローカルユーザからのメッセージは合致しません。
- **ヘッダが存在** — 比較するアイテムとして選択されたヘッダを持つ時、このオプションを利用できます。このオプションを選択して、提供されるオプションでヘッダ名を指定する時に、指定されたヘッダがメッセージの中に存在する場合だけ、条件は合致します。例えば、ヘッダ名として"X-My-Custom-Header"を指定する場合、そのヘッダをもつすべてのメッセージ

は、条件に合致します。そのヘッダのないメッセージは、合致しません。

- **ヘッダが存在しない**—比較するアイテムとして選択されたヘッダを持つ時、このオプションを利用できます。このオプションを選択して、提供されるオプションでヘッダ名を指定する時に、指定されたヘッダがメッセージの中に存在しない場合だけ、条件は合致します。例えば、ヘッダ名として"X-My-Custom-Header"を指定する場合、そのヘッダを持たないすべてのメッセージは、条件に合致します。そのヘッダをもつメッセージは、合致しません。
- **メッセージが[Inbound|Outbound|Internal]である/ない**— この比較方法はMAILとRCPTにのみ使用できます。SMTPのMAIL FromとRCPT Toの値はメールが受信・送信・内部のメールか否かを検証するのに使用されます。

  Inbound— ローカルユーザー以外からローカルユーザー宛のメッセージ

  Outbound— ローカルユーザーからローカルユーザー以外へのメッセージ

  Internal— 同一ドメインのローカルユーザー間でのメッセージ

処置

ルールの条件を設定したら、ルールエディタの処置オプションでメールがルール条件にマッチした際の処置を選択します。選択できるアクションは次の7つです:

- **拒否** – ルールの条件に合致するメッセージを拒否する場合、この処置を選択します。このオプションを選択すると、メッセージを拒否する際の応答テキストを指定するためのSMTP応答オプションが表示されます。例えば、SMTPプロセス中にメッセージを拒否するルールにマッチした際、SMTP応答オプションで"We don't want your spam!"を使用すると、SecurityGatewayは"550 We don't want your spam!"を送信します。
- **破棄** – ルールの条件に合致する時に、この処置はメッセージを廃棄します。Reject処置とは異なって、このオプションはSMTP応答も配信失敗メッセージも送信しません。メッセージが削除されます。
- **隔離** —この処置が選択されると、受信者がローカルユーザの場合、ルールの条件にマッチしたメールは受信者の隔離 250へ配信されます。受信者がリモートユーザである場合、メッセージは代わりに管理隔離 251に入れられます。
- **隔離(管理)**– ルール条件にマッチするとメールは 管理隔離 251 へ配信されます。
- **リダイレクト** – この処置を使用することは、メッセージをルールの条件に合致する時に、異なるアドレスにリダイレクトします。メッセージをリダイレクトするメールアドレスを指定することができるように、Toオプションは処置の下に提供されます。リダイレクトされたメッセージは、最初の受信者に配信されません。処置で指定されるアドレスに送られます。
- **コピー**– メッセージを追加のメールアドレスへコピーする場合、このオプションを使用します。メッセージを送信する追加のメールアドレスを指定することができるように、Toオプションは処置の下で提供されます。これは、両方の最初の受信者を除いて、リダイレクトと類似し、処置で指定されるアドレスは、メッセージのコピーを受信します。メッセージを複数のアドレスへコピーする場合、各アドレスへ追加のルールを作成します。
- **注意(警告)を送信** – メッセージがルールの条件に合致する場合、メモまたは警報メールメッセージを送信するために、この処置を使用します。この処置が選択される時に、オプションはメモのTo, From, Subjectおよびメッセージテキスト(メッセージの本文)を指定するために提供されます。動的に特定の情報を含むメモで使用することができるマクロがあります。

SecurityGatewayがメモのテキストでマクロを検出すると、対応する値でそのマクロを置き換えます。

$SENDER$– これは、ルールに合致したメッセージのために使用されたSMTP MAIL Fromアドレスと置き換えられます。例えば、"sender@example.net"。

$SENDERMAILBOX$– このマクロは、SMTP MAIL Fromコマンドで渡されたメールアドレスのメールボックス部分だけと置き換えられます。例えば、"sender@example.net"アドレスから"sender"。

$SENDERDOMAIN$– このマクロは、SMTP MAIL Fromコマンドで渡されたメールアドレスのドメイン部分だけと置き換えられます。例えば、"sender@example.net"アドレスから"example.net"。

$RECIPIENT$– これは、ルールに合致したメッセージで使用されたSMTP RCPT Toアドレスと置き換えられます。例えば、"recipient@example.com"。

$RECIPIENTMAILBOX$– このマクロは、SMTP RCPT Toコマンドで渡されたメールアドレスのメールボックス部分だけと置き換えられます。例えば、"recipient@example.com"アドレスの"recipient"部分です。

$RECIPIENTDOMAIN$– このマクロは、SMTP RCPT Toコマンドで渡されたメールアドレスのドメイン部分だけと置き換えられます。例えば、"recipient@example.com"アドレスの"example.com"部分です。

$SUBJECT$– このマクロは、合致したメッセージのSubjectヘッダのコンテンツと置き換えられます。

$MESSAGEID$– これは、メッセージのMessage-IDヘッダの値と置き換えられます。

$DATESTAMP$– このマクロはメッセージの日付と置き換えられます。

$CURRENTTIME$– SecurityGatewayがメモを作成する時に、これは現在の時刻と置き換えられます。

$HELONAME$– これは、合致したメッセージがSecurityGatewayによって受信される時に、SMTPプロセス中に、渡されたHELOドメインです。

- **メッセージスコアに追加** – メッセージがルールの条件に一致した場合、メッセージに指定したポイントを追加するには、この処置を使用します。
- **Registered Email (RMail)で送信** – この処置を選択すると条件にマッチしたメールがRMailの Registered Emailで送信されます。

  暗号化 – メールを暗号化する場合はこのオプションを選択します。

  追跡と証明 – RMailの追跡と証明を使用する場合はこのオプションを選択します。

  E-署名 – RMailのE-署名でドキュメントへ署名を付与する場合はこのオプションを選択します。

- **メールをREQUIRETLS用にマーク** – メールで**RequireTLS**[104]を使うよう指定します。

- **セキュアウェブメールとして送信** – 通常のメール配信ではなく、SecurityGatewayの セキュアメッセージ[92] ウェブポータルシステムでメールを送信する場合はこの処理を選択します。

正規表現

コンテンツフィルタルール[204]条件では、比較メソッドとして"正規表現"をサポートします。正規表現(regexp)は用途が広いシステムで、規定のテキスト文字列のためだけでなく、同様にテキストパターンの

検索を可能にします。正規表現(regexp)テキストパターンは、メタキャラクタおよび英数字テキストキャラクタとして知られる特殊文字または「リテラル」(すなわちabc、123、その他)の組合せから成ります。パターンは、どちらでも成功しているマッチの結果となったテキスト文字列に対してマッチするために使用されます。

SecurityGatewayのregexps実装は、Perl互換の正規表現(PCRE)ライブラリを使用します。egexpsの、この実装に関する詳細な情報は http://www.pcre.org/ および http://perldoc.perl.org/perlre.html を参照してください。

オライリーメディア社によって出版された*Mastering Regular Expressions, Third Edition* で正規表現を総合的に調べることができます。

メタキャラクタ

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。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	説明
\	メタキャラクタの前に使用すると、そのメタキャラクタをリテラルキャラクタとして扱います。これはメタキャラクタとして使用されている特殊文字を検索する場合に必要なものです。例えば[＋]を検索する場合、[¥＋]という表現が必要となります。
|	[または]の意味を持つキャラクタで、[|]で区切られたどれかのキャラクタにマッチします。例えば[abc|xyz]という表現は、[abc]または[xyz]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どの文字にもマッチします。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[^]には別の意味があります。対象文字列に合致することからかぎカッコの内で存続する文字を除外するために使用されます。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-&-123]または[″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でなくグループ化の結果により置換されます。¥の後の数字はどのグループ表現を参照したいかを示します。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[1abc]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。
?	直前の文字が0回または1回現れることを表します。例えば、[1?abc]は[abc]または[1abc]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。

4.7.2 添付ファイル

特定の種類の添付ファイルをブロックしたり隔離するには、このページのオプションを使用します。グローバルおよびドメインごとにフィルタ規制を定義することができます。

ブロックする添付ファイル

このセクションで、ブロックするファイルタイプを指定します。メッセージに、これらのファイルタイプの1つを添付ファイルを持つ場合、SMTP中に処理を拒否されます。

ブロックおよび隔離セクションで同じファイルタイプを指定する場合、指定するタイプの添付ファイルを持つメッセージは、**ブロック**されますが隔離されません。

追加
ブロックリストに新規のファイルタイプを追加するには、フィールドへ拡張子を入力し**追加**をクリックします。

削除
ブロックリストからファイルタイプを削除するには、リストから拡張子を選択し削除をクリックします。CTRLを使用して複数の選択をすることができます。

提案
これらのリンクは、ブロックリストに一般的なファイルタイプを追加します。単にリンクをクリックするとファイルタイプは追加されます。

実行ファイルをブロック:
このリンクは、ブロックリストにAPP, CMD, COM, DMG, EXE, HTA, PIF, SCR, および VBSを追加します。

画像ファイルをブロック:
このリンクを選択すると、ブロックリストに次のイメージファイルタイプBMP, GIF, JPG, PNG, TIF, TIFFを追加します。

動画ファイルをブロック:
これらの動画ファイルタイプ3GP、ASX、AVI、DIVX、M4U、MOV、MP4、MPEG、MPG、QT、RM、RTS、SWF、WM、WMVをブロックするために、このリンクを選択します。

サウンドファイルをブロック:
このリンクは、次のサウンドファイルAAC, AIF, AIFF, AU, CDR, M3U, M4A, MID, MIDI, MOD, MP3, OGG, RA, WAV, WAVEをブロックします。

圧縮ファイルをブロック:
このリンクは、ブロックリストに圧縮ファイルタイプGZ, GZIP, RAR, TAR, TAR.GZ, TGZ, ZIPを追加します。

次のメールアドレス宛のメールを除外する
このオプションを有効化し、添付ファイルブロックオプションから除外する宛先メールアドレスを追加します。メールアドレスのマスク指定も行えます。例: `*@company.mail`, `user*@company.mail`, `admin@*.mail`

隔離する添付ファイル

このセクションで隔離するファイルタイプを指定します。メッセージに、これらのファイルタイプの1つを添付ファイルを持つ場合、メッセージは受け入れられますが隔離をされます。

同じファイルタイプをブロックと隔離の両方で指定した場合、対象の添付ファイル付きのメールは、**ブロック**されますが隔離されません。

追加
隔離リストに新規のファイルタイプを追加するには、フィールドへ拡張子を入力し**追加**をクリックします。

削除
隔離リストからファイルタイプを削除するには、リストから拡張子を選択し追加をクリックします。CTRLを使用して複数の選択をすることができます。

提案
これらのリンクは、隔離リストに一般的なファイルタイプを追加します。単にリンクをクリックするとファイルタイプは追加されます。

実行ファイルを隔離する:
このリンクは、隔離リストにファイルタイプAPP, CMD, COM, DMG, EXE, HTA, PIF, SCR, VBSを追加します。

画像ファイルを隔離する:
このリンクは、隔離リストにファイルタイプBMP, GIF, JPG, PNG, TIF, TIFFを追加します。

動画ファイルを隔離する:
このリンクは、隔離リストにファイルタイプ3GP, ASX, AVI, DIVX, M4U, MOV, MP4, MPEG, MPG, QT, RM, RTS, SWF, WM, WMVを追加します。

サウンドファイルを隔離する:
このリンクは、隔離リストにファイルタイプAAC, AIF, AIFF, AU, CDR, M3U, M4A, MID, MIDI, MOD, MP3, OGG, RA, WAV, WAVEを追加します。

圧縮ファイルを隔離する:
このリンクは、隔離リストにファイルタイプGZ, GZIP, RAR, TAR, TAR.GZ, TGZ, ZIPを追加します。

次のメールアドレス宛のメッセージを除外する
添付ファイル隔離オプションから特定の宛先を除外するには、このオプションを有効化し、対象のメールアドレスを追加します。メールアドレスのマスク指定も行えます。例: `*@company.mail`, `user*@company.mail`, `admin@*.mail`

例外 – ドメイン

これらの設定を構成する時、ページ上部のドメイン:ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。添付ファイルのフィルタリング設定を見直し編集するには、対応するドメインの**表示/編集**リンクをクリック、あるいはデフォルトの全体の設定値をドメインの設定にリセットするには、**リセット**をクリックします。

4.8 ブラックリスト

ブラックリストは、メールをブロックしたり隔離したりする対象の電子メールアドレス、ホスト名、IPアドレスのリストです。デフォルトでメッセージはSMTPセッション中に拒否されますが、隔離するように[ブラックリスト処理](#) 220 ページで、この設定を変更することができます。こうした処理は、全体又はドメイン毎に行え、ブラックリスト自体も、全体又はドメイン毎に設定することができます。さらに、通常はブラックリストへ1項目を追加しますが、各ブラックリストはインポート機能を持ち、複数の項目を追加するためにカンマで区切られた値、CSVファイルを使用を使用することができます。最後に、各リストは同様にエクスポート機能が搭載されており、CSVファイルにブラックリストの内容を保存することができます。3種類のブラックリストがあり、全てはグローバルおよび特定のドメインに設定できます。

[アドレスブラックリスト](#) 213
特定の電子メールアドレスからメッセージをブロックまたは隔離するために、このブラックリストを使用します。

[ホストブラックリスト](#) 215
このブラックリストは、配信している特定のホスト(例えばmail.example.com、smtp.example.net、など)に基づくメッセージをブロックまたは隔離するために用います。

[IPブラックリスト](#) 218
IPブラックリストは、送信元ホストのIPアドレスに基づいて、メッセージをブロックまたは隔離します。

4.8.1 アドレス

特定のメールアドレスから届いたメールをブロックまたは隔離するには、ブラックリストを使用します。デフォルトでメッセージはSMTPセッション中に拒否されますが、隔離するように、[ブラックリストの処理](#) 220 ページで、この設定を変更することができます。アクションは全体や特定ドメインで処理する事ができ、ブラックリスト自身も、全体かドメイン毎に設定する事ができます。また、アイテムはブラックリストへ通常1つづつ登録できますが、インポート機能を使う事で、CSVファイルから複数の値を一括登録する事もできます。最後に、CSVファイルへブラックリストを保存するためのエクスポート機能も搭載されています。

ブラックリストへアドレスを追加

アドレスブラックリストにアドレスを追加するために、ページ上部のツールバーで**新規**をクリックします。これは、アドレス(下記参照)を追加するために、[ブラックリストのエントリ](#) 215 ページを開きます。

ブラックリスト アドレスを編集
ブラックリスト アドレスを編集するには、対象エントリをダブルクリックするか、エントリを選択しページ上部のツールバーで**編集**ボタンをクリックします。ブラックリスト のエントリ215ページでエントリが編集できるようになります。

ブラックリスト アドレスを削除
ブラックリスト アドレスを削除するには、必要なエントリを選択して、ページ上部のツールバーで**削除**をクリックします。CTRLキーを使用し複数のエントリを選択することができます。削除をクリックした後に、選択されたエントリの削除確認ボックスが表示されます。

ブラックリスト へアドレスをインポート
アドレスブラックリストにアドレスのリストをインポートするには、ページ上部のツールバーで**読み込み**をクリックします。これは、リストの読み込みページを開きます。**参照**ボタンでインポートするCSVファイルを選択し、**リストの読み込み**ボタンをクリックします。

CSVファイル形式
ブラックリストにアドレスを追加するためにCSVファイルを作成するために、任意のテキスト エディタ(例えばノート パッド)を使用することができます。下記の形式に従ってファイルを作成して、filename.csv.として保存します。各CSVファイルの最初の行はマッピング行で、データが現れる順番をサーバに通知します。このファイルの各項目は、引用符を持ちカンマで区切る必要があります。

グローバルブラックリスト へアドレスをインポート:
Valueカラムにはブラックリストに載せるメールアドレス、Typeカラムには"BlackListAddressGlobal"と指定し、Commentsカラムはエントリに関するメモを指定します。Commentsカラムはオプションで、カラムを持つ場合、コメントがないエントリには空の引用符""を使用します。

CSVファイルの例:

```
"Value","Type","Comments"
"address01@example.net","BlackListAddressGlobal","This is a comment
about the address."
"address01@example.org","BlackListAddressGlobal",""
"address02@example.net","BlackListAddressGlobal","This is another
comment."
```

特定のドメインのアドレスブラックリスト へアドレスをインポート:
Domainカラムは、このブラックリストが属するドメインです。例えば、example.comのブラックリストにアドレスを追加する必要がある場合、Domainカラムには "example.com"を使用します。Valueカラムは、ブラックリストに載せるメールアドレス、Typeカラムには"BlackListAddressDomain"と指定し、自分自身の参照のために、Commentsカラムはエントリに関して追加したい任意のメモを指定します。Commentsカラムはオプションで、コメントがないエントリには空の引用符""を使用します。

CSVファイルの例:

```
"Domain","Value","Type","Comments"
"example.com","address01@example.net","BlackListAddressDomain","This
is a comment about the address."
"example.com","address01@example.org","BlackListAddressDomain",""
```

```
"example.com","address02@example.net","BlackListAddressDomain","This
is another comment."
```

ブラックリストからアドレスをエクスポート

アドレスブラックリストのエクスポート:

1. ドメイン:ドロップダウンリストボックスで、グローバルまたは特定のドメインを選択します。
2. ページの上部のツールバーで書き出しを選択します。これはファイルのダウンロードダイアログを開きます。
3. **保存**をクリックします。
4. ファイル名とフォルダを選択します。
5. **保存**をクリックしダイアログを閉じます。

ブラックリストのエントリ

このページはブラックリストに新規のアドレスを追加および既存のエントリを編集に使用します。アドレスブラックリストで**新規**または**編集**をクリックで開きます。

リストエントリ

ドメイン:
このドロップダウンリストを使用して、特定のドメインのブラックリストまたはグローバルリストへアドレスを追加する場合はグローバルを選択します。

メールアドレス:
メッセージをブロックまたは隔離する電子メールアドレスをここに入力します。ブラックリスト処置 220ページの設定は、メッセージがブロックまたは隔離されるか判定します。そのドメインですべてのアドレスをブラックリストに登録するには、メールボックスの一部で、アスタリスクを使用することができます。例えば、"*@example.org"は、example.orgからのすべてのメッセージをブロックまたは隔離します。

コメント:
自分自身の参照のために、このエントリについて任意のコメントまたはメモにエリアを使用します。

保存して閉じる
エントリで完了する時に、ブラックリストにエントリを保存するために、[**保存して閉じる**]をクリックします。

閉じる
保存することなくブラックリストエントリページを閉じたい場合、このボタンを選択します。

4.8.2 ホスト

特定のホスト(例えば"mail.example.com")から届いたメールをブロックまたは隔離するには、ブラックリストを使用します。デフォルトでメッセージはSMTPセッション中に拒否されますが、隔離するように、ブラックリストの処理 220ページで、この設定を変更することができます。アクションは全体や特定ドメ

インで処理する事ができ、ホストブラックリスト自身も、全体かドメイン毎に設定する事ができます。また、アイテムはブラックリストへ通常1つづつ登録できますが、インポート機能を使う事で、CSVファイルから複数の値を一括登録する事もできます。最後に、CSVファイルへブラックリストを保存するためのエクスポート機能も搭載されています。

ブラックリストへホストを追加

ホストブラックリストにホストを追加するために、ページ上部のツールバーで**新規**をクリックします。これは、ホスト(下記参照)を追加するために、ブラックリストのエントリ217ページを開きます。

ブラックリストホストを編集

ブラックリストホストを編集するには、編集するエントリをダブルクリックし、またはエントリを選択しページ上部のツールバーで**編集**ボタンをクリックします。これは、ブラックリストのエントリ217ページでエントリを開きます。

ブラックリストホストを削除

ブラックリストホストを削除するには、必要なエントリを選択して、ページ上部のツールバーで**削除**をクリックします。CTRLキーを使用し複数のエントリを選択することができます。削除をクリックした後に、選択されたエントリの削除確認ボックスが表示されます。

ブラックリストへホストをインポート

ホストブラックリストにホストのリストをインポートするには、ページ上部のツールバーで**読み込み**をクリックします。これは、リストの読み込みページを開きます。**参照**ボタンでインポートするCSVファイルを選択し、**リストの読み込み**ボタンをクリックします。

CSVファイル形式

ブラックリストにホストを追加するためにCSVファイルを作成するために、任意のテキストエディタ(例えばノートパッド)を使用することができます。下記の形式に従ってファイルを作成して、filename.csv.として保存します。各CSVファイルの最初の行はマッピング行で、データが現れる順番をサーバに通知します。このファイルの各項目は、引用符を持ちカンマで区切る必要があります。

グローバルブラックリストへホストをインポート:
Valueカラムは、ブラックリストに載せるホスト(例えば mail.example.com, domain.comなど)、Typeカラムには"BlackListHostGlobal"と指定し、自分自身の参照のために、Commentsカラムはエントリに関して追加したい任意のメモを指定します。Commentsカラムはオプションで、カラムを持つ場合、コメントがないエントリには空の引用符""を使用します。

CSVファイルの例:

```
"Value","Type","Comments"
"example.net","BlackListHostGlobal","This is a comment about the
address."
"mail.domain.com","BlackListHostGlobal",""
"smtp.company.mail","BlackListHostGlobal","This is another comment."
```

特定のドメインのホストブラックリストへホストをインポート:
Domainカラムは、このブラックリストが属するドメインです。例えば、example.comのブラックリストにホストを追加する必要がある場合、Domainカラムには "example.com"を使用します。Valueカラムは、ブラックリストに載せるホスト、Typeカラムには"BlackListHostDomain"と指定し、自分自身の参照のために、Commentsカラムはエントリに関して追加したい任意のメモを指定します。Commentsカラムはオプションで、コメントがないエントリには空の引用符を使用します。

CSVファイルの例:

```
"Domain","Value","Type","Comments"
"example.com","example.net","BlackListHostDomain","This is a comment
about the address."
"example.com","mail.domain.com","BlackListHostDomain",""
"example.com","smtp.company.mail","BlackListHostDomain","This is
another comment."
```

ブラックリスト からホスト をエクスポート

ホスト ブラックリスト のエクスポート:

1. ドメイン:ドロップダウンリスト ボックスで、グローバルまたは特 定 のドメインを選 択します。
2. ページの上 部 のツールバーで書 き出しを選 択します。これはファイルのダウンロード ダイアログを開きます。
3. 保 存 をクリックします。
4. ファイル名 とフォルダを選 択します。
5. 保 存 をクリックしダイアログを閉じます。

ブラックリスト のエントリ

このページはブラックリスト に新 規 のホスト を追 加 および既 存 のエントリを編 集 に使 用します。ホスト ブラックリスト で新 規 または編 集 をクリックで開きます。

リスト エントリ

ドメイン:
このドロップダウンリスト を使 用して、特 定 のドメインのブラックリスト またはグローバルリスト へホスト を追 加する場 合 はグローバルを選 択します。

ホスト:
メッセージをブロックしまたは隔 離 するホスト を、ここに入 力します。ブラックリスト 処 置 220ページの設 定 は、メッセージがブロックまたは隔 離 されるか判 定します。すべての特 定ドメインのホスト をブラックリスト に登 録するには、ホスト 名 でアスタリスクを使 用することができます。例 えば、 `mail.example.org`, `smtp.example.org`からのすべてのメッセージをブロックまたは隔 離します。

コメント:
自 分 自 身 の参 照 のために、このエントリについて任 意 のコメント またはメモにエリアを使 用します。

保 存 して閉 じる
エントリで完 了 する時 に、ブラックリスト にエントリを保 存 するために、[保 存 して閉 じる]をクリックします。

閉 じる
保 存 することなくブラックリスト エントリページを閉 じたい場 合 、このボタンを選 択します。

4.8.3 IP

特定のIPアドレス（例："1.2.3.4," "192.168.0.1,"他）から届いたメールをブロックまたは隔離するには、ブラックリストを使用します。デフォルトでメッセージはSMTPセッション中に拒否されますが、隔離するように、ブラックリストの処理 220ページで、この設定を変更することができます。アクションは全体や特定ドメインで処理する事ができ、IPブラックリスト自身も、全体かドメイン毎に設定する事ができます。また、アイテムはブラックリストへ通常1つづつ登録できますが、インポート機能を使う事で、CSVファイルから複数の値を一括登録する事もできます。最後に、CSVファイルへブラックリストを保存するためのエクスポート機能も搭載されています。

ブラックリストへIPを追加

IPブラックリストにIPを追加するために、ページ上部のツールバーで**新規**をクリックします。これは、IPアドレス(下記参照)を追加するために、ブラックリストのエントリ 219ページを開きます。

ブラックリストIPを編集

ブラックリストIPアドレスを編集するには、編集するエントリをダブルクリックし、またはエントリを選択しページ上部のツールバーで**編集**ボタンをクリックします。これは、ブラックリストのエントリ 219ページでエントリを開きます。

ブラックリストIPアドレスを削除

ブラックリストIPアドレスを削除するには、必要なエントリを選択して、ページ上部のツールバーで**削除**をクリックします。CTRLキーを使用し複数のエントリを選択することができます。削除をクリックした後に、選択されたエントリの削除確認ボックスが表示されます。

ブラックリストへIPアドレスをインポート

アドレスブラックリストにIPアドレスのリストをインポートするには、ページ上部のツールバーで**読み込み**をクリックします。これは、リストの読み込みページを開きます。**参照**ボタンでインポートするCSVファイルを選択し、**リストの読み込み**ボタンをクリックします。

CSVファイル形式

ブラックリストにIPアドレスを追加するためにCSVファイルを作成するために、任意のテキストエディタ（例えばノートパッド）を使用することができます。下記の形式に従ってファイルを作成して、filename.csv.として保存します。各CSVファイルの最初の行はマッピング行で、データが現れる順番をサーバに通知します。このファイルの各項目は、引用符を持ちカンマで区切る必要があります。

グローバルブラックリストへIPアドレスをインポート:

Valueカラムは、ブラックリスト（CIDR表記法および*，?および# ワイルドカードをサポート）に載せるIPアドレス、Typeカラムには"BlackListIPGlobal"と指定し、自分自身の参照のために、Commentsカラムはエントリに関して追加したい任意のメモを指定します。Commentsカラムはオプションで、カラムを持つ場合、コメントがないエントリには空の引用符""を使用します。

CSVファイルの例:

```
"Value","Type","Comments"
"1.2.3.4","BlackListIPGlobal","This is a comment about the address."
"1.1.1.1","BlackListIPGlobal",""
"192.168.*.*","BlackListIPGlobal","This is another comment."
```

特定のドメインのIPアドレスブラックリストへIPアドレスをインポート:
Domainカラムは、このブラックリストが属するドメインです。例えば、example.comのブラックリストにIPアドレスを追加する必要がある場合、Domainカラムには"example.com"を使用します。Valueカラムは、ブラックリスト(CIDR表記法および*, ?および# ワイルドカードをサポート)に載せるIPアドレス、Typeカラムには"BlackListIPDomain"と指定し、自分自身の参照のために、Commentsカラムはエントリに関して追加したい任意のメモを指定します。Commentsカラムはオプションで、コメントがないエントリには空の引用符を使用します。

CSVファイルの例:

```
"Domain","Value","Type","Comments"
"example.com","1.2.3.4","BlackListIPDomain","This is a comment about
the address."
"example.com","1.1.1.1","BlackListIPDomain",""
"example.com","192.168.*.*","BlackListIPDomain","This is another
comment."
```

ブラックリストからIPアドレスをエクスポート

IPアドレスブラックリストのエクスポート:

1. **ドメイン**:ドロップダウンリストボックスで、グローバルまたは特定のドメインを選択します。
2. ページの上部のツールバーで書き出しを選択します。これはファイルのダウンロードダイアログを開きます。
3. **保存**をクリックします。
4. ファイル名とフォルダを選択します。
5. **保存**をクリックしダイアログを閉じます。

ブラックリストのエントリ

このページはブラックリストに新規のIPアドレスを追加および既存のエントリを編集に使用します。IPアドレスブラックリストで**新規**または**編集**をクリックで開きます。

リストエントリ

ドメイン:
このドロップダウンリストを使用して、特定のドメインのブラックリストまたはグローバルリストへIPアドレスを追加する場合はグローバルを選択します。

IPアドレス:
メッセージをブロックまたは隔離するIPアドレスをここに入力します。ブラックリスト処置 220ページの設定は、メッセージをブロックまたは隔離するか判定します。CIDR表記法が可能で、1つのエントリでアドレスのブラックリストブロックにワイルドカード:*, ?および# を使用することができます。

コメント:
自分自身の参照のために、このエントリについて任意のコメントまたはメモにエリアを使用します。

保存して閉じる
エントリで完了する時に、ブラックリストにエントリを保存するために、[**保存して閉じる**]をクリックします。

閉じる
保存することなくブラックリストエントリページを閉じたい場合、このボタンを選択します。

4.8.4 ブラックリスト設定

メッセージがSecurityGatewayのブラックリスト 213の条件と一致すると、このページで設定した処理が実施されます。デフォルトでメッセージはSMTPセッション中に拒否されますが、隔離するように、ブラックリストの処理ページで、この設定を変更することができます。処置は、全体またはドメイン毎に設定することができます。特定のドメインの処理の設定を行うには、ページ上部でドメインをドメイン:ドロップダウンリストボックスから選択し、設定を選択し**保存**をクリックします。

設定

ホワイトリストでの一致をブラックリストの一致よりも優先する
メールがホワイトリストとブラックリストの両方に一致した場合、ホワイトリスト 221の一致を優先するにはこのオプションを使用します。デフォルトでこのオプションは無効に設定されており、メールがホワイトリストとブラックリストの両方に一致した場合は、ブラックリストが優先されます。この場合、メッセージがブラックリストに一致する場合、の設定に基づいて、メールは拒否されたり隔離されたりします。

メッセージがブラックリストに一致する場合:
これは、受信メッセージがブラックリスト差出人からの場合、必要な処理です。

...メッセージを拒否
このオプションが選択される時に、ブラックリスト差出人のメッセージはSMTPセッション中に拒否されます。このオプションはデフォルトで有効です。

送信サーバから切断する
デフォルトでメッセージがSMTPセッションを拒否される時は、通常、継続を許可します。セッションを直ちに終了する場合、このチェックボックスを選択します。メッセージが拒否された後、SecurityGatewayは直ちに送信サーバから切断します。

...メッセージを隔離
メッセージを拒否する代わりに、ブラックリスト差出人からメッセージを隔離したい場合、このオプションを選択します。

例外 - ドメイン

これらの設定を構成する時、ページ上部のドメイン:ドロップダウンリストボックスで特定のドメインを選択する場合、そのドメインの設定を保存後に、この一覧にドメインが表示されます。ブラックリストの処理を見直し編集するには、対応するドメインの**表示 / 編集**リンクをクリック、あるいはデフォルトの全体設定値をドメインの設定としてリセットするには、**リセット**をクリックします。

4.9 ホワイトリスト

ホワイトリストは、メッセージをセキュリティ規制から除外するメールアドレス、ホストおよびIPアドレスのリストです。SecurityGatewayのヒューリスティックとベイジアン132、DNSBL138、DKIM検証IM162およびその他セキュリティ機能は、差出人、ホスト、メッセージなどに除外のオプションを持ちます。ホワイトリストは、グローバルおよび特定ドメインに設定することができ、通常はホワイトリストへ1項目を追加しますが、インポート機能で、複数の項目を追加するためにカンマで区切られた値CSVファイルの使用ができます。最後に、各リストはエクスポート機能を持ちCSVファイルにホワイトリストの内容を保存することができます。3種類のホワイトリストがあり、これらはグローバルまたは特定のドメインに設定することができます。

アドレスホワイトリスト221
特定のメールアドレスからのメッセージを除外するために、このホワイトリストを使用します。

ホストホワイトリスト223
このホワイトリストは、特定のホストを指定されたセキュリティ規制から除外、および特定の配信するホスト(例えばmail.example.com、smtp.example.netなど)を除外します。

IPホワイトリスト226
IPホワイトリストは特定のIPアドレスを指定されたセキュリティ規制から除外し、送信することを試みホストのIPアドレスに基づくメッセージを除外します。

4.9.1 アドレス

ホワイトリストアドレスは、多数のセキュリティ規制からメッセージを除外する差出人メールアドレスのリストです。SecurityGatewayのヒューリスティックとベイジアン132、DNSBL138L、DKIM検証162およびその他セキュリティ126機能は、差出人、ホスト、メッセージなどに除外のオプションを持ちます。ホワイトリストは、グローバルおよび特定のドメインに設定することができ、通常はホワイトリストへ1項目を追加しますが、インポート機能で、複数の項目を追加するためにカンマで区切られた値、CSVファイルを使用ができます。最後に、各リストはエクスポート機能を持ちCSVファイルにホワイトリストの内容を保存することができます。

ホワイトリストへアドレスを追加
アドレスホワイトリストにアドレスを追加するために、ページ上部のツールバーで**新規**をクリックします。これは、アドレス(下記参照)を追加するために、ホワイトリストのエントリ223を開きます。

ホワイトリストアドレスを編集
ホワイトリストアドレスを編集するには、編集するエントリをダブルクリックし、またはエントリを選択しページ上部のツールバーで**編集**ボタンをクリックします。これは、ホワイトリストのエントリ223ページでエントリを開きます。

ホワイトリスト アドレスを削除
ホワイトリスト アドレスを削除するには、必要なエントリを選択して、ページ上部のツールバーで**削除**をクリックします。CTRLキーを使用し複数のエントリを選択することができます。削除をクリックした後に、選択されたエントリの削除確認ボックスが表示されます。

ホワイトリスト へアドレスをインポート
アドレスホワイトリストにアドレスのリストをインポートするには、ページ上部のツールバーで**リストの読み込み**をクリックします。これは、リストの読み込みページを開きます。**参照**ボタンでインポートするCSVファイルを選択し、**リストの読み込み**ボタンをクリックします。

CSVファイル形式
ホワイトリストにアドレスを追加するためにCSVファイルを作成するために、任意のテキストエディタ(例えばノートパッド)を使用することができます。下記の形式に従ってファイルを作成して、filename.csv.として保存します。各CSVファイルの最初の行はマッピング行で、データが現れる順番をサーバに通知します。このファイルの各項目は、引用符を持ちカンマで区切る必要があります。

グローバルホワイトリスト へアドレスをインポート:
Valueカラムは、ホワイトリストに載せるメールアドレス、Typeカラムには"WhiteListAddressGlobal"と指定し、自分自身の参照のために、Commentsカラムはエントリに関して追加したい任意のメモを指定します。Commentsカラムはオプションで、カラムを持つ場合、コメントがないエントリには空の引用符""を使用します。

CSVファイルの例:

```
"Value","Type","Comments"
"address01@example.net","WhiteListAddressGlobal","This is a comment
about the address."
"address01@example.org","WhiteListAddressGlobal",""
"address02@example.net","WhiteListAddressGlobal","This is another
comment."
```

特定のドメインのアドレスホワイトリスト へアドレスをインポート:
Domainカラムは、このホワイトリストが属するドメインです。例えば、example.comのホワイトリストにアドレスを追加する必要がある場合、Domainカラムには "example.com"を使用します。Valueカラムは、ホワイトリストに載せるメールアドレス、Typeカラムには"WhiteListAddressDomain"と指定し、自分自身の参照のために、Commentsカラムはエントリに関して追加したい任意のメモを指定します。Commentsカラムはオプションで、コメントがないエントリには空の引用符を使用します。

CSVファイルの例:

```
"Domain","Value","Type","Comments"
"example.com","address01@example.net","WhiteListAddressDomain","This
is a comment about the address."
"example.com","address01@example.org","WhiteListAddressDomain",""
"example.com","address02@example.net","WhiteListAddressDomain","This
is another comment."
```

ホワイトリスト からアドレスをエクスポート
アドレスホワイトリストのエクスポート:

1. **ドメイン**:ドロップダウンリストボックスで、グローバルまたは特定のドメインを選択します。

2. ページの上部のツールバーで書き出しを選択します。これはファイルのダウンロードダイアログを開きます。
3. **保存**をクリックします。
4. ファイル名とフォルダを選択します。
5. **保存**をクリックしダイアログを閉じます。

ホワイトリストのエントリ

このページはホワイトリストに新規のアドレスを追加および既存のエントリを編集に使用します。アドレスホワイトリストで**新規**または**編集**をクリックで開きます。

リストエントリ

ドメイン:
このドロップダウンリストを使用して、特定のドメインのホワイトリストまたはグローバルリストへアドレスを追加する場合はグローバルを選択します。

メールアドレス:
メッセージをセキュリティ機能から除外する"ホワイトリスト差出人"に設定する電子メールアドレスをここに入力します。そのドメインですべてのアドレスをホワイトリストに登録するには、アドレスのメールボックスを一部で、アスタリスクを使用することができます。例えば、"*@example.org"は、example.orgからのすべてのメッセージをホワイトリストに登録します。

コメント:
自分自身の参照のために、このエントリについて任意のコメントまたはメモに使用します。

保存して閉じる
エントリを完了する時に、ホワイトリストにエントリを保存するために、[**保存して閉じる**]をクリックします。

閉じる
保存することなくホワイトリストエントリページを閉じたい場合、このボタンを選択します。

4.9.2 ホスト

ホストホワイトリストは、セキュリティ規制から特定のホスト(例えば、"mail.example.com")を除外するために使用します。SecurityGatewayのヒューリスティックとベイジアン[132]、DNSBL[138]、およびその他セキュリティ[126]機能へは、ホワイトリストを除外し、ホワイトリスト上のホストから届いたメールのチェックを除外するオプションを搭載しています。ホワイトリストへのホスト登録は、全体又はドメイン毎に設定する事ができます。また、アイテムはホワイトリストへ通常1つづつ登録できますが、インポート機能を使う事で、CSVファイルから複数の値を一括登録する事もできます。最後に、CSVファイルへホワイトリストを保存するエクスポート機能も搭載されています。

ホワイトリストへホストを追加
ホストホワイトリストにホストを追加するために、ページ上部のツールバーで**新規**をクリックします。これは、ホスト(下記参照)を追加するために、ホワイトリストのエントリ225ページを開きます。

ホストホワイトリストを編集
ホワイトリストホストを編集するには、編集するエントリをダブルクリックし、またはエントリを選択しページ上部のツールバーで**編集**ボタンをクリックします。これは、ホワイトリストのエントリ225ページでエントリを開きます

ホストをホワイトリストから削除
ホワイトリストホストを削除するには、必要なエントリを選択して、ページ上部のツールバーで**削除**をクリックします。CTRLキーを使用し複数のエントリを選択することができます。削除をクリックした後に、選択されたエントリの削除確認ボックスが表示されます。

ホワイトリストへホストをインポート
ホストホワイトリストへホストのリストをインポートするには、ページ上部のツールバーで**読み込み**をクリックします。これは、リストの読み込みページを開きます。**参照**ボタンでインポートするCSVファイルを選択し、**リストの読み込み**ボタンをクリックします。

CSVファイル形式
ホワイトリストにホストを追加するためにCSVファイルを作成するために、任意のテキストエディタ(例えばノートパッド)を使用することができます。下記の形式に従ってファイルを作成して、filename.csv.として保存します。各CSVファイルの最初の行はマッピング行で、データが現れる順番をサーバに通知します。このファイルの各項目は、引用符を持ちカンマで区切る必要があります。

グローバルホワイトリストへホストをインポート:
Valueカラムは、ホワイトリストに載せるホスト(例えば、mail.example.com, domain.comなど)、Typeカラムには"WhiteListHostGlobal"と指定し、自分自身の参照のために、Commentsカラムはエントリに関して追加したい任意のメモを指定します。Commentsカラムはオプションで、カラムを持つ場合、コメントがないエントリには空の引用符""を使用します。

CSVファイルの例:

```
"Value","Type","Comments"
"example.net","WhiteListHostGlobal","This is a comment about the
address."
"mail.domain.com","WhiteListHostGlobal",""
"smtp.company.mail","WhiteListHostGlobal","This is another comment."
```

特定のドメインのホストホワイトリストへホストをインポート:
Domainカラムは、このホワイトリストが属するドメインです。例えば、example.comのホワイトリストにホストを追加する必要がある場合、Domainカラムには"example.com"を使用します。Valueカラムは、ホワイトリスト(例えば mail.example.com, domain.comなど)に載せるホスト、Typeカラムには"WhiteListHostDomain"と指定し、自分自身の参照のために、Commentsカラムはエントリに関して追加したい任意のメモを指定します。Commentsカラムはオプションで、コメントがないエントリには空の引用符""を使用します。

CSVファイルの例:

```
"Domain","Value","Type","Comments"
```

```
"example.com","example.net","WhiteListHostDomain","This is a comment
about the address."
"example.com","mail.domain.com","WhiteListHostDomain",""
"example.com","smtp.company.mail","WhiteListHostDomain","This is
another comment."
```

ホワイトリストからホストをエクスポート

ホスト ホワイト リスト のエクスポート:

1. ドメイン:ドロップダウンリスト ボックスで、グローバルまたは特 定 のドメインを選 択します。
2. ページの上 部 のツールバーで書 き出しを選 択します。これはファイルのダウンロードダイアログを開きます。
3. 保 存 をクリックします。
4. ファイル名 とフォルダを選 択します。
5. 保 存 をクリックしダイアログを閉じます。

ホワイトリストのエントリ

このページはホワイト リスト に新 規 のホストを追 加 および既 存 のエントリを編 集 に使 用します。ホスト ホワイト リスト で新 規 または編 集 をクリックで開きます。

リスト エントリ

ドメイン:
このドロップダウンリストを使 用して、特 定 のドメインのホワイト リスト またはグローバルリスト へホストを追 加 する場 合 はグローバルを選 択します。

メールホスト:
「ホワイト リスト 差 出 人 」または「ホワイト リスト ホスト 」でセキュリティ機 能 からメッセージを除 外 するために設 定 したホストを、ここに入 力します。そのドメインですべてのホストをホワイト リスト に登 録 するには、ホスト の一 部 で、アスタリスクを使 用 することができます。例 えば、"*@ example.org"は、mail.example.org, smtp.example.orgからのすべてのメッセージをホワイト リスト に登 録します。

コメント:
自 分 自 身 の参 照 のために、このエントリについて任 意 のコメント またはメモに使 用します。

保 存 して閉 じる
エントリで完 了 する時 に、ホワイト リスト にエントリを保 存 するために、[保 存 して閉 じる]をクリックします。

閉 じる
保 存 することなくホワイト リスト エントリページを閉 じたい場 合 、このボタンを選 択します。

4.9.3 IP

IPホワイトリストは、セキュリティ規制から特定のIPアドレスを除外するために使用します。SecurityGatewayのヒューリスティックとベイジアン132、DNSBL138、DKIM検証162およびその他セキュリティ126機能へは、ホワイトリストを除外し、ホワイトリスト上のIPから届いたメールのチェックを除外するオプションを搭載しています。ホワイトリストへのIP登録は、全体又はドメイン毎に設定する事ができます。また、アイテムはホワイトリストへ通常1つづつ登録できますが、インポート機能を使う事で、CSVファイルから複数の値を一括登録する事もできます。最後に、CSVファイルへホワイトリストを保存するエクスポート機能も搭載されています。

ホワイトリストへIPを追加

IPホワイトリストにIPを追加するために、ページ上部のツールバーで**新規**をクリックします。これは、IPアドレス(下記参照)を追加するために、ホワイトリストのエントリ227ページを開きます。

ホワイトリストIPアドレスを編集

ホワイトリストIPを編集するには、編集するエントリをダブルクリックし、またはエントリを選択しページ上部のツールバーで**編集**ボタンをクリックします。これは、ホワイトリストのエントリ227ページでエントリを開きます。

ホワイトリストIPアドレスを削除

ホワイトリストIPアドレスを削除するには、必要なエントリを選択して、ページ上部のツールバーで**削除**をクリックします。CTRLキーを使用し複数のエントリを選択することができます。削除をクリックした後に、選択されたエントリの削除確認ボックスが表示されます。

ホワイトリストへIPアドレスをインポート

IPホワイトリストにIPのリストをインポートするには、ページ上部のツールバーで**読み込み**をクリックします。これは、リストの読み込みページを開きます。**参照**ボタンでインポートするCSVファイルを選択し、**リストの読み込み**ボタンをクリックします。

CSVファイル形式

ホワイトリストにIPアドレスを追加するためにCSVファイルを作成するために、任意のテキストエディタ(例えばノートパッド)を使用することができます。下記の形式に従ってファイルを作成して、filename.csv.として保存します。各CSVファイルの最初の行はマッピング行で、データが現れる順番をサーバに通知します。このファイルの各項目は、引用符を持ちカンマで区切る必要があります。

グローバルホワイトリストへIPアドレスをインポート:

Valueカラムは、ホワイトリストに載せるIPアドレス(CIDR表記法および*, ?および# ワイルドカードをサポート)、Typeカラムには"WhiteListIPGlobal"と指定し、自分自身の参照のために、Commentsカラムはエントリに関して追加したい任意のメモを指定します。Commentsカラムはオプションで、カラムを持つ場合、コメントがないエントリには空の引用符""を使用します。

CSVファイルの例:

```
"Value","Type","Comments"
"1.2.3.4","WhiteListIPGlobal","This is a comment about the address."
"1.1.1.1","WhiteListIPGlobal",""
"192.168.*.*","WhiteListIPGlobal","This is another comment."
```

特定のドメインのIPホワイトリストへIPアドレスをインポート::
Valueカラムは、ホワイトリスト（CIDR表記法および*，?および# ワイルドカードをサポート）に載せるIPアドレス、Typeカラムには"WhiteListIPDomain"と指定し、自分自身の参照のために、Commentsカラムはエントリに関して追加したい任意のメモを指定します。Commentsカラムはオプションで、コメントがないエントリには空の引用符を使用します。

CSVファイルの例:

```
"Domain","Value","Type","Comments"
"example.com","1.2.3.4","WhiteListIPDomain","This is a comment about
the address."
"example.com","1.1.1.1","WhiteListIPDomain",""
"example.com","192.168.*.*","WhiteListIPDomain","This is another
comment."
```

ホワイトリストからIPをエクスポート

IPホワイトリストのエクスポート:

1. **ドメイン**:ドロップダウンリストボックスで、グローバルまたは特定のドメインを選択します。
2. ページの上部のツールバーで書き出しを選択します。これはファイルのダウンロードダイアログを開きます。
3. **保存**をクリックします。
4. ファイル名とフォルダを選択します。
5. **保存**をクリックしダイアログを閉じます。

ホワイトリストのエントリ

このページはホワイトリストに新規のIPアドレスを追加および既存のエントリを編集に使用します。IPホワイトリストで**新規**または**編集**をクリックで開きます。

リストエントリ

ドメイン:
このドロップダウンリストを使用して、特定のドメインのホワイトリストまたはグローバルリストへIPを追加する場合はグローバルを選択します。

IPアドレス:
「ホワイトリスト差出人」または「ホワイトリストIPアドレス」でセキュリティ機能からメッセージを除外するために設定したIPアドレスを、ここに入力します。1つのエントリでブロックアドレスをホワイトリストに登録するために、CIDR表記法は許可され、ワイルドカード*，?および# を使用することができます。

コメント:
自分自身の参照のために、このエントリについて任意のコメントまたはメモに使用します。

保存して閉じる
エントリで完了する時に、ホワイトリストにエントリを保存するために、[**保存して閉じる**]をクリックします。

閉じる
保存することなくホワイトリストエントリページを閉じたい場合、このボタンを選択します。

4.10 Sieveスクリプト

Sieveは、高い拡張性と機能性を誇る標準規格のメールフィルタリング言語です。SecurityGatewayでは、コアの部分でSieveの拡張機能を使っており、メッセージコンテントフィルタ202機能のベースとしてもSieveを使用しています。さらに、様々な用途で使用できるカスタムスクリプトにも対応しています。Sieveスクリプトページで管理するSecurityGatewayの使用するスクリプトには2つのカテゴリがあります。

システム生成 – SecurityGatewayのコアな機能は、このスクリプトで実装されています。管理画面で設定変更が行われると、関連するSieveスクリプトがSieve Scriptページ上で修正されます。これはスクリプトを編集するための唯一の方法です。Sieveスクリプトは読み込み専用で、直接編集はできません。ただし、スクリプトの処理の順番は、矢印で変更する事ができます。

管理者定義 – カスタムスクリプトを作成するために、Sieveスクリプトページを使用することができます。柔軟なフィルタリング手順を提供するので、特定の必要性に応じたスクリプトを定義することができます。しかしながら、Sieveフィルタリング言語によりSMTPおよびスクリプティングの基本的な知識は、これらのスクリプトを作成するために必要です。SieveのSecurityGatewayの実装は、基本言語、いくつかのスタンダード拡張部分およびカスタム拡張239があります。

Sieveの基本情報とSecurityGatewayでどのように使われているかについては、ここやスクリプト作成230およびSecurityGateway Sieve拡張239ページで解説していますが、言語についての完全な説明は、このガイド以外にあります。Sieveに関する詳細な情報については、IETFウェブサイトでドキュメントを参照してください: Sieve: An Email Filtering Language (RFC-5228), Sieve's Copy Extension (RFC 3894), Sieve's Body Extension (RFC-5173), Sieve's Reject Extension (RFC-5429), Sieve's Variables Extension (RFC-5229), Spamtest and VirusTest Extensions (RFC-3685)

Sieveスクリプトリスト

Sieveスクリプトページは、すべてのシステム生成および管理者が定義したスクリプトのリストを含んでいます。このリストには6つのセクション、IP, HELO, AUTH, MAIL, RCPT, DATAがあります。これらのセクションは、関連あるセクションで一覧にされる各スクリプトで、各種のステージまたはSMTP処理のメールイベントに対応します。スクリプトは、一度に1セクションを処理し、最初にグローバルスクリプト、2番目にドメイン特定スクリプトで、一覧にされる順位で処理をします。リストで順位を変更するために、提供されたスクリプトと関連する上下矢印を使用して、スクリプトが各セクションで処理する順位をコントロールすることができます。

ページ上部ツールバーは、次の3つのオプションがあります。

新規
Sieveスクリプトエディタ229(スクリプトを作成するために使用)を開くために、**新規**をクリックします。

編集
Sieveスクリプト エディタ229で開くには、スクリプトを選択し、ツールバーで**編集**をクリックします。あるいは、単にスクリプトをダブルクリックすることができます。システム生成されたスクリプトは編集することはできませんが、レビューのためにスクリプト エディタを開くこと、または新規、カスタムルールにペーストすることができるようにスクリプトのテキストをコピーすることができます。

削除
カスタムスクリプトを削除するには、リストでスクリプトを選択し、ツールバーで削除をクリックします。スクリプトの削除の確認ボックスが現れます。システム生成のスクリプトは削除することができません。

スクリプト リストは、次の5つのカラムがあります。

有効
スクリプトのチェックボックスをチェックまたは解除することによってスクリプトを使用可能または使用不可にすることができるように、このカラムで一覧されたスクリプトにチェックボックスがあります。カスタムスクリプトだけは、このオプションで有効/無効にすることができます。システム生成されたスクリプトを有効または無効にするには、そのスクリプト(すなわちグレーリスト、IPシールド、ベイジアン自動学習など)と関連する機能に対応するインターフェースのコントロールを使用する必要があります。

範囲
このカラムは、スクリプトの範囲を一覧にします。範囲は、グローバルまたは特定のドメインです。グローバルのスクリプトは、すべてのメッセージについて処理されます。特定のドメインのスクリプトは、関連したドメインのメッセージのみ処理されます。

並び順
スクリプトは一覧にされる順位で処理されます。順位を変更する場合、このカラムで上下矢印を使用することができます。

スクリプト名
これは、スクリプトを確認するために用いるタイトルまたは説明を指定します。このカスタムスクリプトを作成する場合、スクリプト名を指定します。

スクリプト
マウスカーソルをアイコンの重ねると、ツールヒントとしてスクリプトのテキストが現れます。スクリプトのテキストを詳しく見るためには、Sieveスクリプト エディタ229で開くために、スクリプトをダブルクリックします。

Sieveスクリプト エディタ

Sieveスクリプト ページのツールバーで**新規**または**編集**をクリックするとSieveスクリプト エディタを開きます。Sieveスクリプトの新規作成または既存のスクリプト編集のために利用します。スクリプトの作成または編集でエディタを使用した後に、スクリプトを保存するには、ツールバーで[**保存して閉じる**]をクリックします。Sieveスクリプト ページに戻ります。

スクリプト プロパティ

このスクリプトの処理を有効にする
このチェックボックスは、Sieveスクリプト リストで有効カラムに対応します。デフォルトで、スクリプトを作成する時に、スクリプトは有効でスクリプト一覧に追加されることを意味し、下記で指定されるメールイベント中に処理されます。スクリプトを無効にする場合、このチェックボックスを解除します。無効にさ

れる時、スクリプトは一覧に今まで通り現れますが処理はされません。さらに、システム生成されたスクリプトは有効または無効にすることができません。それらは、特定のスクリプトに対応する各種のインターフェースページでオプションを通して管理する必要があります。

スクリプト名:
スクリプトのためにタイトルまたは説明を指定するために、このテキストボックスを使用します。システム生成されたスクリプトは名前を変えることができません。

メールイベント:
スクリプトを作成する場合、スクリプトで処理するメールイベントまたはSMTPセッションのステージを選択するために、このドロップダウンリストを使用します。例えば、ある物をメッセージの受信者と比較するスクリプトを作成する場合、SMTPセッションのRCPT段階が到達されるまでメッセージの受信者が不明なので、このオプションでRCPTかDATAを選択します。発生する順番に6つのメールイベントIP, HELO, AUTH, MAIL, RCPTおよびDATAがあります。

範囲:
スクリプトの範囲を指定するために、グローバルまたはドメインを使用します。グローバルが選択される場合、メッセージが送られるドメインに関係なく、スクリプトは処理されます。ドメインが選択される場合、スクリプトは指定するドメインだけのメッセージに対してテストされます。受信者のドメインがSMTP処理のそれらの段階以前に知られないので、RCPTまたはDATAメールイベントを選択する場合には、ドメインだけ選択ができます。

ドメイン:
スクリプトの範囲としてドメインを選択する場合、このドロップダウンリストが現れます。このスクリプトと関連する特定のドメインを選択するために使用します。

スクリプトテキスト:
Sieveメールフィルタリング言語を利用して実際のスクリプトのテキストを入力するために、このエリアを使用します。Sieve言語でのサンプルスクリプトおよび基本情報については、以下を参照: Sieveスクリプトの作成 230

4.10.1 Sieveスクリプトの作成

Sieve Scripts 228 や SecurityGateway Sieve拡張 239 ページに加え、このページではSieveメールフィルタリング言語とSecurityGateway上での実装に関する概要を説明します。最初にSieveスクリプトの基本を説明します。次にこの言語の様々な構成エレメント 232 について説明します。対応している、標準的なコントロール 233, テスト 234, アクション 236 コマンド一覧も紹介します。最後に、ページの下部にサンプルスクリプト 238 を紹介しているので、ご参照下さい。

Sieveメールフィルタリング言語に関する詳細な情報については、IETFウェブサイトでドキュメントを参照してください: Sieve: An Email Filtering Language (RFC-5228), Sieve's Copy Extension (RFC 3894), Sieve's Body Extension (RFC-5173), Sieve's Reject Extension (RFC-5429), Sieve's Variables Extension (RFC-5229), Spamtest and VirusTest Extensions (RFC-3685)

SecurityGatewayの電話やメールサポート、ナレッジベース、FAQ、フォーラム等の技術サポートやヘルプ情報については www.mdaemon.com/Support/ を参照してください。

Sieveスクリプトの要素

Sieveスクリプトは、基本的には次の4つの要素で構成されています。

1. Requirements(要件)ー この要素は、提供されたスクリプトに必要とされるSieve拡張を宣言するために使用されます。オプションの拡張に属しているコマンドがスクリプトで使用される場合、スクリプトの始めで必要な拡張を一覧にするrequireコントロールコマンドを使用する必要があります。セミコロンはrequireコマンドの引数の終わりで必要です。

   例:

   ```
   require "SecurityGateway";
   ```

   -and-

   ```
   require ["SecurityGateway", "fileinto"];
   ```

2. Conditions(条件)ー スクリプトのこの要素は、メッセージ中でテストする任意のタイプと、テストや比較の方法を宣言するのに使用します。

   例:

   ```
   if size :over 1M
   ```

   -and-

   ```
   if header :contains ["to", "cc"] "Frank Thomas"
   ```

3. アクションー これらは、必要とされる処置および指定された条件がTrueである場合、実行されるコマンドです。各Actionは、セミコロンが必要で、処置の各ブロックは、波括弧"{ "および"} "を含む必要があります。

   例:

   ```
   if size :over 1M { discard; }
   ```

   -and-

   ```
   if header :contains ["to", "cc"] "Frank Thomas" {
   bayes-learn "spam";
   fileinto "spam";
   }
   ```

4. コメントー 自分自身の参照のためにコメントをSieveスクリプトに含むことができます。使用することができる2種類のコメント、1行コメントおよび複数行コメントがあります。1行コメントは"# "から始めて、行の終わり(すなわち次のCRLF)まで継続します。複数行コメントは"/* "から始めて、複数の行にすることができ、"*/"で終わります。

例:

```
# discards messages over 1 mb
if size :over 1M { discard; }
```

-and-

```
if header :contains "from" "Frank Thomas" {
/* Frank Thomas sends mostly spam to us, so this script
will automatically move everything we get from him to
the user quarantine. */
fileinto "spam";
}
```

構成要素

文字列
テキスト文字列は1つダブルクォートで始めと終わりにおきます。例えば: ″Frank Thomas″。

バックスラッシュまたはダブルクォート引用符で囲まれた文字列内の文字にバックスラッシュまたはダブルクォートを含むには、もう一つバックスラッシュの後に存在する必要があります。従って、¥¥は¥と¥″として処理され、引用符で囲まれた文字列において″とみなされます。他の文字は文字列でエスケープキャラクタにはなりません。

文字列のリスト
スクリプトでグループの文字列を使用する場合、各引用符で囲まれた文字列をカンマで区切って、セットを角括弧に入れます。

例:

```
if header :contains ["to", "cc"] ["me@xyz.com", "you@xyz.com",
"us@xyz.com"]
```

ToまたはCCヘッダが3つのアドレスのうち、いずれかを含んでいる場合、このテストの結果はTrueです。

ヘッダ
ヘッダ名でコロンは不要です。

例:

```
if header :is "to:" (invalid)
if header :is "to" (valid)
```

テストリスト
文字列リストと同様に、グループを括弧に入れることによって、スクリプトで一群のテストを含むことができます。これは、それぞれ論理的な″AND″および″OR″ステートメントなので、全部または任意のTestコマンドを使用する時に必要です。

例:

```
if anyof (size :over 1M, header :contains "subject" ["big file",
"mega file"])
{
discard;
}
```

引数と比較タイプ
大部分のコマンドは、実行する内容について指定するために、一つ以上引数を必要とします。いくつかのタイプの引数（例えば位置引数、タグを付けられた引数およびオプションの引数）があります。タグを付けられた引数およびMatch Type引数、コロンで先行されます。:contains、:is、:matches:overおよび:underは、タグを付けられた引数のすべてのサンプルです。一部のタグを付けられた引数は、特定のコマンドに限られています。異なるタイプの引数の詳細について、以下を参照：RFC-5228

アクション
各処置は、セミコロンで区切る必要があり、そして、処置の各ブロックは、波括弧で囲む必要があります。

例：

```
if header :contains ["to", "cc"] "Frank Thomas" {
bayes-learn "spam";
fileinto "spam";
}
```

コントロールコマンド

Sieve言語で使用される3つのコントロールコマンドがあります。

require
このコントロールコマンドは、どのオプションの拡張をスクリプトで使用するか宣言するためにスクリプトの始めに使用されます。

例：

```
require ["SecurityGateway", "fileinto"];
```

if / elsif / else
`if` コマンドは、中心的なコントロールコマンドです。3つの相互関係あるコマンドが技術的にありますが、elsifおよびelseは、`if` で独立して使用することができません。`if` がスクリプトで遭遇される時に、テスト条件はTrueであるか判定するために評価されます。Trueの場合、関連する処置が実行されます。

`if` テストがfalseである場合、最初の `elsif` テストが評価されます。`elsif` がtrueである場合、そのテストと関連する処置が実行されます。`elsif` テストがfalseと判明する場合、続いて、それらの1つがtrueになるまで、処理は次のelsifに続きます。

ifおよびすべての `elsif` テストがfalseである場合、elseコマンドがある場合、そのコマンドの処置は実行されます。

stop
stopコントロールコマンドは、すべての処理を終わらせます。

テストコマンド

これらは、SieveのSecurityGatewayの実装でサポートされる標準テストコマンドです。bodyおよびenvelopeコマンドは拡張です。しかしスクリプトで、Testコマンドのいずれかを使用する場合には、requireコントロールコマンドで、これらを含む必要があります。さらに、SecurityGateway Sieve拡張 239ページで要点をまとめられるSecurityGateway拡張に含まれる追加されたテストコマンドがあります。

address
このコマンドで、含んでいる可能性のあるフレーズまたは名前ではなくヘッダでメールアドレスのみテストすることができます。例えば、"to"ヘッダで"Frank Thomas" <frank@ example.com>を含む場合、テストヘッダ: is "to" "frank@ example.com"の結果はfalseになります。しかし。アドレスだけが評価されるので、テストアドレス: is "to" "frank@ example.com"はtrueになります。

同様に、このコマンドで使用できるオプションのタグを付けられた引数":localpart", ":domain"および":all"があります。:localpart引数は、アドレス(例えば"frank@ example.com"の"frank")の左辺だけを評価します、:domain引数は、アドレス(例えば"example.com")のドメイン一部を使用するだけです、:allは全アドレスを使用します。これらの引数のいずれも含まれない場合、:allはデフォルトにより使用されます。

例:

```
require "fileinto";
if address :domain :is "from" "spammer.com" {
fileinto "spam";
}
```

allof
このテストは、論理的な"AND"で、処置のために評価される条件の全てがtrueである必要があります。

例:

```
if allof (header :contains "from" "J.Lovell", header :contains "to"
"Bubba")
{
fileinto "spam";
}
```

anyof
このテストは、論理的な"OR"で関連する処置のために評価される条件のいずれかがtrueである必要があります。

例:

```
if anyof (size :over 1M, header :contains "subject" "big file
attached")
```

```
{
reject "I don't want messages that claim to have big files.";
}
```

body
bodyテストコマンドは、オプションの拡張で、使用する任意のスクリプトの始めに、require "body"コントロールコマンドを使用する必要があります。このコマンドは、メッセージの本文に対して比較します。このコマンドの詳細は、以下を参照してください: Sieve's Body Extension (RFC-5173)

例:

```
require ["body", "fileinto"];
if body :text :contains "secret formula" {
fileinto "admin";
}
```

envelope
envelopeコマンドは、オプションの拡張で、使用する任意のスクリプトの始めに、require "envelope"コントロールコマンドを使用する必要があります。"from"またはto"がコマンドの引数として個々に使用される場合、このコマンドはSMTP MAIL FromおよびRCPT To envelopeパートに対して比較します。

```
require "envelope";
if envelope :is "from" "MrsFrank@company.com" {
redirect "frankshome@example.com";
}
```

exists
引数にリストされるヘッダがメッセージ内で存在する場合、このテストはtrueです。すべてのリストされたヘッダが存在する必要がありか、またはテストがfalseである必要があります。

例:

```
if exists "x-custom-header" {
redirect "admin@example.com";
}
```

-and-

```
if not exists ["from", "date"] {
discard;
}
```

false
このテストは、"FALSE"に常に評価します。

header
指定されたヘッダの値が引数によって設定される条件に適合させる場合、ヘッダテストはtrueに評価します。Match Type引数なしが指定される場合、:isはデフォルトにより使用されます。

例：

```
require "fileinto"
if header :is "x-custom-header" "01" {
fileinto "admin";
}
```

not
別のテストで、このコマンドの使用は、テストの結果が、テストの処置が必要とされる逆転することを意味します。例えば、テストif not exists ["from", "date"] { discard; }は、メッセージが"from"および"date"ヘッダ両方を含んでいない場合、discard処置が必要とされることを意味します。notコマンドが省略される場合、それはヘッダDIDが存在する場合、メッセージが廃棄されることを意味します。

size
sizeコマンドはタグを付けられた引数":over"および":under"を受け入れ数値によって適用される必要があります。これらの引数は、メッセージサイズが、テストでTRUEとなるよう指定される値より高いまたは低いか指定するために用います。メガバイトを示す値の後のM、キロバイトのK、またはバイトには文字を指定なしで使用することができます。

例：

```
if size :over 500K {
discard;
}
```

true
このテストは、"TRUE"に常に評価します。

spamtest
spamtest コマンドは、ietf.orgのSpamtest and VirusTest Extensions (RFC-3685)ドキュメントで定義されているSieve拡張です。この拡張に関する情報についてはそのドキュメントを参照してください。

virustest
virustestコマンドは、ietf.orgのSpamtest and VirusTest Extensions (RFC-3685)ドキュメントで定義されているSieve拡張です。この拡張に関する情報についてはそのドキュメントを参照してください。

アクションコマンド

これらの標準アクションコマンドは、SecurityGatewayによってサポートされます。fileintoおよびrejectコマンドは拡張で、従って、スクリプトで、どちらかのコマンドを使用する場合には、require controlコマンドで、これらを持つ必要があります。SecurityGateway Sieve拡張ページ 239で概説されるSecurityGateway拡張を通して利用可能な多くのその他actionコマンドがあります。

fileinto
fileintoアクションコマンドはオプションの拡張で、使用する任意のスクリプトの始めに、require "fileinto"コントロールコマンドを使用する必要があります。このコマンドは、2つの引数"spam"および"admin"を受け入れます。"spam"はメッセージをユーザー隔離 250 へ、"admin"は管理隔離 251 へ移動します。

例：

```
require "fileinto";
if header :contains "from" "Frank Thomas" {
fileinto "spam";
}
```

discard
この処置は、配信に状況通知を送信することなく確認なしでメッセージ削除します。

例：

```
if size :over 2M { discard; }
```

keep
この処置は、デフォルトロケーションにメッセージを保存します。

redirect
メッセージの本文または既存のヘッダを変更することなく、このコマンドは、メッセージを関連した引数で指定されているアドレスにリダイレクトします。このコマンドは:copyという追加の拡張機能に対応しており、メッセージをリダイレクトするのではなく、指定されたアドレスにコピーを送信できます。ここでは指定のアドレスへのコピー送信に加え、追加の処理を行う事ができます。

例：

```
require "copy";
if header :contains "subject" "Response to XYZ" {
redirect :copy "offers@example.com";
bayes-learn "ham";
}
```

reject
rejectアクションコマンドは追加の拡張機能であるため、使用するにはスクリプトの始めにrequire "reject"コントロールコマンドを使用する必要があります。このコマンドは、SMTP処理中に5xx応答コードでメッセージを拒否し引数で指定されている任意の短いメッセージを送信します。

```
require "reject";
if size :over 5M {
reject "No way! This message is too big for me to accept.";
}
```

vnd.mdaemon.securewebmsg
SecurityGatewayの セキュアメッセージ 92 ウェブポータルでメール送信を行う際にはこのアクションコマンドを使用します。

例：

```
require
["securitygateway","reject","fileinto","envelope","body","regex"];
if allof(header :matches "subject" "[Secure Message]*")
{
vnd.mdaemon.securewebmsg;
}
```

サンプルSieveスクリプト

"[SPAM]"を件名に含んでいるメッセージを拒否

```
require "reject";
if header :contains "subject" "[SPAM]"
{
reject "I don't want your spam";
}
```

特定のリアルネーム宛のメールを拒否

```
require ["SecurityGateway","reject"];
if header :contains "to" "Real Name"
{
bayes-learn "spam";
reject "I don't want your spam";
}
```

カスタムベイジアン自動学習

```
require ["SecurityGateway","comparator-i;ascii-numeric"];
if whitelisted
{
bayes-learn "ham";
}
elsif anyof(blacklisted,spamtotal :value "gt" :comparator "i;ascii-
numeric" "20.0")
{
bayes-learn "spam";
}
```

クレーリストDNSBLの一致

```
require "SecurityGateway"];
if not lookup "rblip" "all" {greylist;}
```

サイズの大きいメール受信時管理者に通知

```
require ["SecurityGateway"];
if size :over 1M
{
alert text:
To: admin@company.mail
From: postmaster@$RECIPIENTDOMAIN$
Subject: SecurityGateway Content-Filter Message
X-Attach-Msg: No
$RECIPIENT$ received a message larger that 1MB.
.
;
}
```

"[Secure Message]"から始まる件名のメールをセキュアメッセージとして送信

```
require
["securitygateway","reject","fileinto","envelope","body","regex"];
if allof(header :matches "subject" "[Secure Message]*")
{
vnd.mdaemon.securewebmsg;
}
```

4.10.2 Sieve拡張

SecurityGatewayのカスタムSieve拡張を使用するには、使用したいスクリプトの前に、requireコマンドを以下のように指定します:

```
require "SecurityGateway";
```

テストコマンド

ip

ipテストは、(例えばメールイベント 229中などの)SMTP処理中に実行することができます。

- **cidr**—2つ目の引数は、クライアントIPアドレスと比較するIPアドレスやパターンです。完全なIPアドレス、(例えば10.0.0.0/24といった)CIDRを使ったIPアドレスの範囲、?(任意の1文字)、*(任意の文字)、#(1桁の数値)といったワイルドカードを使用できます。

  サンプルコード: `if not ip :cidr "10.0.0.0/24" { greylist; }`

- **public**—クライアントIPアドレスがRFC-1918のプライベート サブネット でも、ループバックアドレスでも、DHCPによる自 動IPアドレスでもない場 合 はTrueとなり、それ以 外 はfalseとなります。(127.0.0.0/8、192.168.0.0/16、10.0.0.0/8、172.16.0.0/12、169.254.0.0/16)

  サンプルコード: `if ip "public" { greylist; }`

- **private**— publicの反 対 。
- **ssl**— クライアント がセキュアな(SSL)接 続 を正 常 に処 理 した場 合 trueです。
- **des**— クライアント がドメインメールサーバである場 合 trueです。

lookup

lookupテスト は最 初 の引 数 に応 じて呼 び出 されます:

- **ptr**— これが最 初 の引 数 である時 に、ルックアップテスト はいつでも実 行 することができます。第 2 引 数 は標 準 タグ引 数 か、"resolves"、"resolvestoclient"または"error"です。

  例: `if lookup "ptr" :matches "*.domain.com" { greylist; }.`

  - **resolves**— PTRレコード が存 在 する場 合 、trueを返 します。
  - **resolvestoclient**— PTRレコード がマッチする、つまりPTRホスト のAルックアップが、クライアント のIPアドレスを返 す場 合 、trueを返 します。
  - **error**— 一 時 的 なDNSクエリエラーがある場 合 、trueを返 します。

- **helo**— これが最 初 の引 数 で存 在 する場 合 、ルックアップテスト はHELOイベント やHELOイベント後 にのみ実 行 することができます。第 2 引 数 は、"resolves"、"resolvestoclient"または"error"です。
  - **resolves**— HELO引 数 が有 効 なIPまたはホスト 名 の場 合 、trueを返 します。
  - **resolvestoclient** – HELO引 数 がマッチする、すなわちHELO引 数 のAルックアップがクライアント のIPアドレスを返 す場 合 trueを返 します。
  - **error** – 一 時 的 なDNSクエリエラーがある場 合 、trueを返 します。

- **mail**— これが最 初 の引 数 で存 在 する場 合 、ルックアップテスト はMAILイベント やMAILイベント後 にのみ実 行 することができます。第 2 引 数 は、"resolves"、"resolvestoclient"または"error"です。
  - **resolves**— MAIL FROMドメインが有 効 なドメインで存 在 する場 合 、trueを返 します。
  - **resolvestoclient**— MAIL FROMドメインがマッチ、すなわち、MAIL FROM DOMAINのAルックアップが、クライアント のIPアドレスを返 す場 合 、Trueを返 します。
  - **error** – 一 時 的 なDNSクエリエラーがある場 合 、trueを返 します。

- **spf**— これが最 初 の引 数 で存 在 する場 合 、ルックアップテスト はMAILイベント やMAILイベント後 にのみ実 行 することができます。第 2 引 数 は、"pass"、"fail"または"error"です。
  - **pass**— 差 出 人 がSPFを渡 す場 合 、true、ニュートラルまたは失 敗 結 果 ではfalseを返 します。
  - **fail**— 差 出 人 がSPFに失 敗 する場 合 、true、ニュートラルまたはパス結 果 ではfalseを返 します。

- **error**— 処理中のエラー(通常DNSクエリエラー)がある場合trueを返します。

- **rblip**— これが最初の引数で存在する場合、ルックアップテストはいつでも実行することができます。第2引数は、“all”、“any”または“error”です。
  - **all**— クライアントIPアドレスが、すべてのDNSブラックリストをパスした場合、Trueを返します。
  - **any**— クライアントIPアドレスが、DNSブラックリストのどれかをパスした場合、Trueを返します。
  - **error**— 処理中のエラー(通常DNSクエリエラー)がある場合trueを返します。

- **rblhdr**— これが最初の引数で存在する場合、ルックアップテストはDATAイベントだけで実行することができます。第2引数は、“all”、“any”または“error”です。
  - **all**— 受信ヘッダが、すべてのDNSブラックリストをパスした場合、Trueを返します。
  - **any**— 受信ヘッダが、DNSブラックリストのどれかをパスした場合、Trueを返します。
  - **error**— 処理中のエラー(通常DNSクエリエラー)がある場合trueを返します。

port

portテストは、いつでも実行することができます。クライアントが実際に接続したポート番号と比較するポート番号です。

サンプルコード: `if port 25 { greylist; }`

auth

authテストが呼び出すことができる場合、最初の引数に依存します:

- **succeeded** — 認証が成功している場合、trueです。これが最初の引数で存在する場合、authテストはAUTHイベントまたはイベント後に実行することができます。
- **match** — 認証が成功しMAIL FROMアドレスが認証されたアカウントと一致する場合、trueです。これが最初の引数で存在する場合、authテストはMAILイベントまたはイベント後に実行することができます。

verify

verify testは、アドレスを確認します(参照: ユーザ検証ソース 52)。他の全てのテストとは異なり、このテストは、sieveフィルタに適用しない場合でも、常に実行されます。すなわち、あらゆるMAIL FROMおよびRCPT TOアドレスは、照合され、結果はキャッシュに入ります。verifyテストが呼び出すことができる場合、最初の引数に依存します。

- **from** — MAIL FROMアドレスが有効なローカルアドレスで存在する場合、trueです。これが最初の引数で存在する場合、verifyテストはMAILイベントまたはイベント後に実行することができます。
- **fromdomain** — MAIL FROMアドレスが有効なローカルドメインからの場合、trueです。これが最初の引数で存在する場合、verifyテストはMAILイベント、またはイベント後に実行することができます。

- **fail_from** – MAIL FROMアドレスを照合中エラーがある場合、trueです。これが最初の引数で存在する場合、verifyテストはMAILイベント、またはイベント後に実行することができます。
- **to** – RCPT TOアドレスが有効なローカルアドレスで存在する場合、trueです。これが最初の引数で存在する場合、verifyテストはRCPTイベントまたはイベント後に実行することができます。
- **todomain** – RCPT TOアドレスが有効なローカルドメインに存在する場合、trueです。これが最初の引数で存在する場合、verifyテストはRCPTイベントまたはイベント後に実行することができます。
- **fail_to** – RCPT TOアドレスを照合中エラーがある場合、trueです。これが最初の引数で存在する場合、verifyテストはRCPTイベントまたはイベント後に実行することができます。

dkim

dkimテストはDomainKeys Identified Mail (DKIM)[162]検証に対してチェックし、DATAイベントで実行することができます。

- **pass**
  メッセージがDKIMで署名され、署名が検証をパスする場合、trueを返します。
- **fail**
  DKIM処理がhard failを返す場合、trueを返します(SSPオプションが必要)。
- **error**
  DKIM処理におけるエラーがある場合、trueを返します。

cbv

cbvテストは、MAILイベントまたはイベント後に実行することができます。引数なしで、MAIL FROMアドレスがコールバック検証[177]をパスする場合、trueを返します。

- **error**– CBV処理のエラーがある場合、trueを返します。

spamtotal

spamtotalテストはメッセージスコア[150]に対してチェックして、実行することができます。しかしながら、ほとんどの場合、他の全てのフィルタがメッセージスコアへの寄与をすることができるように、DATAイベントの最後のフィルタで実行されます。

spamtotalテストは、単一の引数を持ちます:threshold値。メッセージスコアがthreshold以上である場合、true(それ以外はfalse)を返します。

OutbreakProtection

OutbreakProtectionテストは、DATAイベントで実行することができます。引数なしで、Outbreak Protection[128]がメッセージをスパム、ウィルスまたはバルクメールと分類する場合、trueを返します。

- **spam**
  Outbreak Protectionがメッセージをスパムと分類する場合、trueを返します。
- **virus**
  Outbreak Protectionがウィルスを含んでいるメッセージを分類する場合、trueを返します。

- **phish**
  Outbreak Protectionがメッセージをフィッシングメールと分類する場合、trueを返します。
- **suspect**
  Outbreak Protectionがメッセージを疑わしいスパムと分類する場合、trueを返します。
- **bulk**
  Outbreak Protectionがメッセージをバルクメールと分類する場合、trueを返します。
- **error**
  Outbreak Protection処理におけるエラーがある場合、trueを返します。

whitelisted

このテストは、免除されたalias:を持ちます(後方互換性のため)。このテストが実行されることができる時は、最初の引数に依存します。

- **all**
  引数はありません; クライアントがホワイトリスト[221]にある場合、trueを返します。これはいずれにしても呼び出すことができて、利用可能な情報を使用するだけです。例えば、IPイベント(最初のイベント)で呼び出される場合、PTRレコードに一致するホワイトリストにあるIPおよびホストだけが比較されます。
- **ip**
  クライアントがIPホワイトリスト[226]に示された場合、trueを返します。いずれにしても実行することができます。
- **host**
  クライアントがホストホワイトリスト[223]で示される場合、trueを返します。候補は、HELO引数またはPTRホストにすることができます。HELOイベントまたはイベント後に実行することができます。
- **mail**
  MAIL FROMがアドレスホワイトリスト[221]で存在する場合、trueを返します。MAILイベントまたはイベント後に実行することができます。
- **from**
  From:ヘッダがアドレスホワイトリスト[221]で存在する場合、trueを返します。DATAイベントで実行することができます。

blacklisted

このテストは、エイリアスを持ちます:blocklist(後方互換性のため)。引数および機能はホワイトリストテストで同一です。ただし、比較はブラックリスト[213]です。

vbr

vbr(すなわちメッセージ証明書[146])テストは、1つ引数を持ちます:

- 信用された証明書のカンマ区切りのリスト—メッセージが保証される場合、trueを返します。
- **error**— メッセージ証明書にエラーがある場合、trueを返します。

アクションコマンド

error

errorコマンドはRFC 3028に記載のrejectコマンドと同一です、ただし、2つの引数を持ちます。最初の引数がSMTPエラーコードで存在し、第2の引数がテキストメッセージで存在します。両方とも、現在のクライアントコマンドに応答して送信されます。

disconnect

disconnectコマンドは"error"コマンドと同一です。ただし、TCP/IPソケットを閉じます。これは、MDでシャットダウンオプションに類似しています。

greylist

greylistコマンドは、グレーリスト[144]を起動させます。

dynamicscreen

dynamicscreenコマンドは、ダイナミックスクリーニング[185]を起動させます。

tarpit

tarpitコマンドは、ターピット[188]を起動させます。

sign

signコマンドは、メッセージに署名[163]ヘッダを追加します。最初の引数は以下の通りです:

- **dkim**
  DKIM[163]でメッセージに署名します。第2の引数が使用するセレクタの名前です。
- **vbr**
  メッセージでVBR-Info:ヘッダ(メッセージ証明書[146]用)を含みます。第2の引数が、mv=parameterで含む信用された証人です。

throttle

throttleコマンドは、帯域制限[189]を起動させます。最初の引数が1秒ごとの文字単位の帯域幅制限です。

ipshield

ipshieldコマンドは、IPシールド[184]を起動させます。

spamscore

spamscoreコマンドはメッセージの現在のメッセージスコア[150]合計に最初の引数を追加します。spamtotalテストを参照。

tagheader

tagheaderコマンドは、メッセージ中のヘッダにタグを前に付加します。最初の引数が、修正するヘッダです。第2引数がヘッダ値で挿入するテキストです。

addheader

addheaderコマンドは、メッセージに新規のヘッダを追加します。最初の引数が追加するヘッダ、第2引数が値です。

removeheader

removeheaderコマンドは、メッセージからヘッダを削除します。最初の引数が、削除するヘッダです。

alert

alertコマンドは、メモを送信します。単一の引数は、from:, to:, subject:および他のヘッダを含んでいるメール本文です。全体の文字列が、マクロ展開に対するサブジェクトです。

changesender

changesenderアクションは、SecurityGatewayがメールを配信する際に使用するSMTP MAIL FROMコマンドの値を変更するのに使用されます。これは、例えば、内部でのみ使用するドメイン名が使用されている場合に、外部のドメイン名を使ってメール送信が必要な場合などに使用されます。

例:

```
require ["securitygateway", "envelope"];
if envelope :matches "From" "frank@internal.mail"
{
changesender "frank@example.com";
}
```

execute

- スクリプトは、設定 ≫ システム ≫ ディレクトリ110で設定した「Sieve Executable Path」ディレクトリに配置する必要があります。「execute」Sieveキーワードは、アクションやテスト用に使用されます。
- 最初のパラメーターはスクリプト名です。.bat, .exe, Powershellに対応しています。
- 2つ目のパラメーターはプロセスへ渡す引数です。message_filename sieve変数はRFC822の処理中のメールソースのフルパスで生成されます。

例:

```
require ["securitygateway","relational","comparator-i;ascii-
numeric"];
execute "Test.ps1" "-msg '${message_filename}'";

The text of the PowerShell script that will log the filename of each
message processed is...
```

```
param
(
    [string]$msg = ""
)

Add-Content -Path "c:\files_processed.txt" -Value $msg
Write-Host $msg
```

セクション 5

5 メッセージ/キュー

左側のメッセージ/キューメニューからは、メッセージログとメッセージキューの2つのセクションへアクセスできます。

メッセージログ 249

メッセージログへはユーザーが送受信した全てのメールについてのエントリが含まれています。一覧へは、送受信処理が行われた日時、送信者と宛先、件名が表示されます。また、配信処理の結果として、配信されたかどうか、隔離されたか、拒否されたか、配信できなかった場合は例えば送信者がブラックリストへ含まれているといった理由が表示されます。最後に、各エントリにはメールのサイズとメッセージスコア 150 が表示されます。

メッセージログからは各メッセージの詳細が表示され、メールの本文や(可能な場合は)ソース, Transcriptが確認できます。また、メールをスパムか非スパムかマークすることで、SecurityGatewayのベイジアン学習 134 精度を向上させ、メールの分析をより正確に行う事ができるようになります。

メッセージログへは ロギング 256 メニューからもアクセスできます。

メッセージキュー

このセクションには次の4つのメッセージキューへのリンクが掲載されています: 隔離済み(ユーザー) 250, 管理隔離 251, 配信用のキュー 251, 不正メッセージ 252

- 隔離済み(ユーザー) 250 はSecurityGatewayの各種 セキュリティ 126 機能を通過しなかったメールを、拒否したりタグを付ける代わりに、一時的に保留するためのキューです。ユーザーは隔離フォルダ内のメールを確認し、内容を閲覧したり、危険性のないメールを通常のメールと同様に配信する事ができます。
- 管理隔離 251 は隔離済み(ユーザー)に似ていますが、送信メール用でウィルス付きのメールを対象にしています。管理者 49 だけが管理隔離へアクセスできます。
- 配信用のキュー 251 配信用キューはリモートアドレスとの送受信待ちのメールで、配信が行えないメールやリトライシステム 76 内のメールもこの中に含まれます。このページから、キューで任意のメッセージを閲覧、メッセージを宛先不明で差出人に戻す、メッセージ配信の停止、または、直ちに、キューで選択したメッセージまたはすべてのメッセージの配信を再試行することができます。
- 不正メッセージ 252 キューはループし 最大メールホップ数 78 に到達してしまった、などの、致命的な処理エラーによって配信できなかったメール用のキューです。不正メッセージキューからは、キューのメール表示や送信者への返信、メールの削除、対象メールや全てのメールの再配信が行えます。

5.1 全てのメッセージ

メールログを表示するには、全てのメールをクリックします。メッセージログは、ユーザが送受信する全てのメッセージに関するエントリです。ここでは、メッセージが処理された日付と時間、差出人と宛先、件名が一覧表示されています。また、配信の有無、隔離、拒否といった結果、配信されない場合(例えば、差出人がブラックリストのアドレスである、添付ファイルの拡張子が禁止されている、などの)理由が表示されます。最後に、各エントリにはメールのサイズとメッセージスコア 150 も表示されます。

ページ上部のツールバーにあるボタンから、様々なタスクを実行できます。

- **更新**—ログの閲覧を開始した後に追加されたエントリを表示するため、メッセージログの表示を更新するには、このボタンをクリックします。
- **検索** – 特定のメールだけを表示するために、検索機能でフィルタを行います。メールの検索は対象のメールが送信用か受信用か、ヘッダ内の文字列、特定期間内か全ての期間か、等を基に行います。メッセージログを検索するには:
  ツールバーの**検索を表示**ボタンをクリックすると検索ウィンドウが起動します。続いて、検索基準を選択し、**検索**ボタンをクリックすると、検索が実行されます。検索ウィンドウが非表示になり、検索結果がメッセージログへ表示されます。検索を表示ボタンを再度クリックすると、検索条件を編集でき、X検索を中止をクリックすると、検索を中止し、通常のメッセージログの画面に戻ります。
- **詳細** – メールを選択しこのボタンをクリックするとメッセージ情報画面が起動します。この画面には、Transcript、メッセージ、ソースの3つのタブがあります。Transcriptタブでは、SMTPセッション、内部処理を含む、配信処理が表示されています。 メッセージタブにはメールの内容と、メール本文や添付をダウンロードするためのオプションが表示されています。 ここでの表示は、メール配信からの経過日数、メールの配信が正常に行われたかどうか、およびデータ保持 118 ページでオプションが有効かどうかによって異なります。ソースタブは、メッセージのヘッダ、HTMLコード、などを含むメッセージのソースがあります。ソースは、メッセージが古い、または、SecurityGatewayのデータ保持 118 オプションで、データを保存するよう設定されていない場合、利用できません。
- **再配信**—一覧から1つまたは複数のメッセージを選択し宛先に再送信するには、このボタンをクリックします。Ctrl+ClickまたはShift+Clickで複数のメッセージを選択できます。このオプションは、データベースからメッセージの内容が削除されていない場合に使用できます。
- **Spam**—メッセージを選択し、スパムとしてメッセージをマークするために、このボタンをクリックします。これにより、その後のSecurityGatewayによるスパム判定精度を向上する事ができます。ベイジアン学習 134 機能が無効な場合、このオプションは利用できません。
- **スパムではありません**—メッセージを選択し、このボタンをクリックすると、対象メッセージを非スパムとしてマークします。これで、SecurityGatewayによる誤検知が起こりにくくなります。ベイジアン学習 134 機能が無効な場合、このオプションは利用できません。
- **ホワイトリスト/ブラックリスト** – メールを選択し、ホワイトリスト 221 又は ブラックリスト 213 をクリックします。送信者のアドレスか、ドメインを、ユーザーリスト、ドメインリスト、全体リストの中で、どのリストへ追加するのかクリックします。

5.2 メッセージキュー

5.2.1 隔離済み(ユーザ)

隔離済み(ユーザー)は SecurityGatewayの各種 セキュリティ[126] 機能を通過しなかったメールを保留するためのキューで、メールサーバーやユーザーを不要なメールやスパム、その他の不正なメールから保護する役割を果たしています。SecurityGatewayのセキュリティ機能の多くは、特定の条件に一致したメールを、拒否する代わりに隔離するオプションを提供しています。隔離済み(ユーザー)の中のメールはSecurityGatewayで保留されていて、宛先ユーザーや管理者が対象のメールを管理する事ができます。ユーザーは隔離フォルダ内のメールを確認し、内容を閲覧したり、危険性のないメールを通常のメールと同様に配信する事ができます。

隔離済の送信メールやウィルス付きメールは 隔離済み(管理)[251] で保留され、 管理者[49] だけが対象のメールへアクセスできます。

隔離の各エントリは、メッセージが隔離された日時、差出人、宛先、件名を表示したカラムで構成されています。併せて、メッセージが隔離された理由、サイズおよびそのメッセージスコア[150]のカラムがあります。

隔離ページの上部にあるツールバーから、各種操作を行うためのボタンを使用する事ができます:

- **更新** – ページへアクセスしてから追加されたメールを表示するには、このボタンをクリックし、隔離メッセージの一覧を更新します。
- **検索** –特定のメッセージだけを表示するために、隔離(ユーザ)からフィルタをする検索機能を使用します。特定のメッセージだけを表示するために隔離(ユーザ)をフィルタするための検索機能があります。メッセージの送受信に基づくログの検索、任意のヘッダで特定のテキストを検索、日付および日付範囲などで検索することができます。隔離を検索するには:ツールバーの検索ボタンから検索ウィンドウを開きます。検索基準を選択し、検索を実行するために、そのウィンドウで検索ボタンをクリックします。検索結果は、メッセージログの検索ウィンドウの下に現れます。隔離は、検索パラメータに一致するメッセージだけを表示するためにフィルタされます。検索を保持したまま検索ウィンドウを隠すには、ツールバーの検索ボタンをクリックします。検索を完了する場合は、検索ウィンドウでキャンセルボタンをクリックすると、隔離ページに戻ります。
- **表示** –メッセージを選択し、このボタンをクリックすると、メッセージ情報画面が開きます。この画面は、Transcript、メッセージおよびソースの3つのタブを持ちます。Transcriptタブは、SMTPセッション、内部処理、などを含む配信処理の写しを含んでいます。メッセージタブは、メッセージの実際の内容を含んでいます。ソースタブは、メッセージのヘッダ、HTMLコード、などを含むメッセージのソースがあります。
- **解放** –メッセージを選択し、配信のために隔離から解放するために、このボタンをクリックします。
- **削除** – メッセージを選択し、削除するために、このボタンをクリックします。
- **全て削除** – すべての隔離されたメッセージを削除するために、このボタンを選択します。

5.2.2 隔離済み(管理)

管理隔離は隔離済み(ユーザー)[250]に似ていますが、受信メールではなく、ウィルス付きのメールやSecurity Gatewayの各種 セキュリティ[126]機能を通過せず、拒否されるのではなく隔離されたメールを保留する先として使用されます。隔離(ユーザ)とは異なり、管理者だけが隔離(管理)から対象メッセージにアクセスできます。管理者はフォルダ内のメールを確認し、内容を閲覧したり、危険性のないメールを通常のメールと同様に配信する事ができます。

管理隔離の各エントリは、メッセージが隔離された日時、差出人、宛先、件名を表示したカラムで構成されています。併せて、メッセージが隔離された理由、サイズおよびそのメッセージスコア[150]のカラムがあります。

管理隔離ページの上部にあるツールバーから、各種操作を行うためのボタンを使用する事ができます:

- **更新** – ページへアクセスしてから追加されたメールを表示するには、このボタンをクリックし、隔離メッセージの一覧を更新します。
- **検索** –特定のメッセージだけを表示するために、隔離(ユーザ)からフィルタをする検索機能を使用します。特定のメッセージだけを表示するために隔離(ユーザ)をフィルタするための検索機能があります。メッセージの送受信に基づくログの検索、任意のヘッダで特定のテキストを検索、日付および日付範囲などで検索することができます。管理隔離を検索するには: ツールバーの検索ボタンから検索ウィンドウを開きます。検索基準を選択し、検索を実行するために、そのウィンドウで検索ボタンをクリックします。検索結果は、メッセージログの検索ウィンドウの下に現れます。管理隔離は、検索パラメータに一致するメッセージだけを表示するためにフィルタされます。検索を保持したまま検索ウィンドウを隠すには、ツールバーの検索ボタンをクリックします。検索を完了する場合は、検索ウィンドウでキャンセルボタンをクリックすると、管理隔離ページに戻ります。
- **表示** –メッセージを選択し、このボタンをクリックすると、メッセージ情報画面が開きます。この画面は、Transcript、メッセージおよびソースの3つのタブを持ちます。Transcriptタブは、SMTPセッション、内部処理、などを含む配信処理の写しを含んでいます。メッセージタブは、メッセージの実際の内容を含んでいます。ソースタブは、メッセージのヘッダ、HTMLコード、などを含むメッセージのソースがあります。
- **解放** –メッセージを選択し、配信のために隔離から解放するために、このボタンをクリックします。
- **削除** – メッセージを選択し、削除するために、このボタンをクリックします。
- **全て削除** – すべての隔離されたメッセージを削除するために、このボタンを選択します。

5.2.3 配信用のキュー

配信用キューはリモートアドレスとの送受信待ちのメールで、配信が行えないメールやリトライシステム[76]内のメールもこの中に含まれます。このページから、キューで任意のメッセージを閲覧、メッセージを宛先不明で差出人に戻す、メッセージ配信の停止、または、直ちに、キューで選択したメッセージまたはすべてのメッセージの配信を再試行することができます。配信用キューリストの各エントリは、メッセージが受信または送信であるか、メッセージが受信された日付および時間、差出人、宛先、件名、サイズ、送信結果のカラムが表示されています。

配信用のキューの上部にあるツールバーから、各種操作を行うためのボタンを使用する事ができます:

- **更新** – ページへアクセスしてから追加されたメールを表示するには、このボタンをクリックし、隔離メッセージの一覧を更新します。
- **検索** –特定のメッセージだけを表示するために、隔離(ユーザ)からフィルタをする検索機能を使用します。メールが送信なのか受信なのか、ヘッダへ任意のテキストが含まれているかどうか、日付および日付範囲などで検索することができます。配信用キューを検索するには:ツールバーの検索ボタンから検索ウィンドウを開きます。検索基準を選択し、検索を実行するために、そのウィンドウで検索ボタンをクリックします。検索結果は、メッセージログの検索ウィンドウの下に現れます。配信用キューは、検索パラメータに一致するメッセージだけを表示するためにフィルタされます。検索を保持したまま検索ウィンドウを隠すには、ツールバーの検索ボタンをクリックします。検索を完了する場合は、検索ウィンドウでキャンセルボタンをクリックすると、元の一覧ページに戻ります。
- **表示** –メッセージを選択し、このボタンをクリックすると、メッセージ情報画面が開きます。この画面は、Transcript、メッセージおよびソースの3つのタブを持ちます。Transcriptタブは、SMTPセッション、内部処理、などを含む配信処理の写しを含んでいます。メッセージタブは、メッセージの実際の内容を含んでいます。ソースタブは、メッセージのヘッダ、HTMLコード、などを含むメッセージのソースがあります。
- **バウンス**– メールを選択しこのボタンをクリックすると、メールが送信者へ返送又は「バウンス」されます。対象のメールは目的の宛先へは配信されません。
- **配信を停止** – キュー内のメールを1つまたは複数選択し、このボタンをクリックすると、メールが「配信失敗」のステータスへと変更され、配信は行われません。ただし、ボタンをクリックした際、既にメールが配信処理中であった場合、メールの配信を中止する事はできません。
- **すべて停止** – これは配信を停止オプションに似ていますが、キューの中の全てのメールを対象にしている点が異なります。検索機能を使って一覧をフィルタしている場合は、表示されているメールだけが配信停止の対象になります。
- **配信を再試行** – キューのメールを選択しこのボタンをクリックすると、SecurityGatewayでリトライサイクル[76]を待つのではなく、すぐにメールの再配信を行います。
- **すべて再試行** – このボタンをクリックすると、SecurityGatewayでリトライサイクル[76]を待つのではなく、すぐにキューの中の全てのメールを再配信します。

5.2.4 不正メッセージ

不正メッセージ[252]キューはループし 最大メールホップ数[78]に到達してしまった、などの、致命的な処理エラーによって配信できなかったメール用のキューです。不正メッセージキューからは、キュー

のメール表示や送信者への返信、メールの削除、対象メールや全てのメールの再配信が行えます。不正メッセージ一覧の各エントリには、メールが受信か送信メールなのか、メールの受信日時、送信者、宛先、件名、サイズの情報が含まれています。

不正メッセージ一覧ページの上部にあるツールバーからタスク実行用のボタンを使用できます。

- **更新** – このボタンをクリックしメールの一覧を更新します。ページへアクセスした後に届いたメールを表示します。
- **検索** – 一覧をフィルタし特定のメールだけを表示できる検索機能を使用します。メールが送受信メールのどちらなのか、ヘッダに含まれる文字列、対象期間といった条件を元にメールを検索できます。不正メッセージの一覧を検索するには、ツールバーの検索をクリックし、検索画面を起動し、検索条件を選択し、最後に検索ボタンをクリックします。検索結果が検索ウィンドウの下部へ表示されます。不正メッセージの一覧は検索パラメータにマッチしたメールのみがフィルタされています。検索ウィンドウを非表示にするには、ツールバーの検索を再度クリックします。検索が終了したら、キャンセルをクリックし、通常のメール一覧ウィンドウへ戻ります。
- **表示** –メッセージを選択し、このボタンをクリックすると、メッセージ情報画面が開きます。この画面は、Transcript、メッセージおよびソースの3つのタブを持ちます。Transcriptタブは、SMTPセッション、内部処理、などを含む配信処理の写しを含んでいます。メッセージタブは、メッセージの実際の内容を含んでいます。ソースタブは、メッセージのヘッダ、HTMLコード、などを含むメッセージのソースがあります。
- **バウンス**–メールを選択しこのボタンをクリックすると、メールが送信者へ返送又は「バウンス」されます。対象のメールは目的の宛先へは配信されません。
- **削除** – メールを選択しこのボタンを押すと、不正メッセージキューから対象のメールが削除されます。削除ボタンのドロップダウンリストからは、選択メールのみを削除するのか一覧のメール全てを削除するのかを選択する事ができます。
- **配信を再試行** – キューのメールを選択し、このボタンをクリックすると、SecurityGatewayが再配信を実行します。この処理で、メールは 配信用のキュー 251 へ移動します。不正メッセージキューへ配信されるきっかけになったエラーを修正できていれば、配信は正常に行われます。エラーが残っている場合は、メールの配信に再度失敗し、メールは不正メッセージキューへ再度配送されます。
- **すべて再試行** – このボタンをクリックするとSecurityGatewayで不正メッセージキューの中の全てのメールを再配信します。これはキューの中に大量のメールがあり、その原因となるエラーを修正した際などに便利です。

セクション 6

6 ロギング

左側のロギングメニューからは、メッセージログ、ログファイル、設定の3つのセクションへアクセスできます。

メッセージログ 249

メッセージログには全ての送受信メール毎のエントリが含まれています。メールが処理された時間、送受信者、件名が、メッセージ毎に一覧表示されます。また、この画面では、配信済、隔離済、拒否、といった配送結果と、配送されなかった場合は、ブラックリストアドレス、禁止されている添付ファイル、といった理由が一覧表示されます。各エントリにはメールのサイズとメッセージスコア 150 も表示されます。

メッセージログからは、メール毎のセッション情報と(可能な場合は)本文とソースを確認できます。メールへスパム又は非スパムのマークを付けSecurityGatewayのベイジアン学習 134 機能やスパム判定基準へやくだつ情報を提供する事もできます。

メッセージログは、メッセージ/キュー 248 メニューからも表示できます。

ログファイル 257

ログファイルセクションから、ログフォルダ 110 にあるSecurityGatewayのログファイルを閲覧することができます。メッセージログとは異なり、ログファイルはデータベースで保存されず、各イベントについてソートできるリストおよび別々のエントリを提供します。その代わりに、SecurityGatewayが実行する各種のSMTP接続および他の機能の写しを含んでいるプレーンテキストファイルです。ログファイルセクションのすべてのログファイルページは、ログフォルダで含まれているログファイルの全てを一覧にし、現在のログファイルおよびロールオーバーファイル 259 を含んでいます。このページから、一覧にされるファイルのいずれかを閲覧することができます。ログファイルセクションの他のページは、SecurityGatewayの現在のログファイル、例えばシステムログ、受信および送信ログ、ウィルスアップデートログなど閲覧するショートカットを提供します。

設定 259

設定セクションはログの設定 259 ページへリンクしており、ここからログの初期設定やオプション設定を行う事ができます。ページで、受信、送信およびHTTPログの詳細度レベルや、ログファイルの種類として「スタンダードセット」「日付をファイル名の一部とした日別セット」「曜日をファイル名の一部とした曜日毎のセット」のどれかを選択することができます。最後に、ログファイルのメンテナンス設定として、別ファイルを生成するまでのログファイル最大容量や、ロールオーバー用のふぁいるの最大数、アーカイブするまでの期間、その他の設定を行う事ができます。

6.1 メッセージログ

メールログを表示するには、全てのメールをクリックします。メッセージログは、ユーザが送受信する全てのメッセージに関するエントリです。ここでは、メッセージが処理された日付と時間、差出人と宛

先、件名が一覧表示されています。また、配信の有無、隔離、拒否といった結果、配信されない場合(例えば、差出人がブラックリストのアドレスである、添付ファイルの拡張子が禁止されている、などの)理由が表示されます。最後に、各エントリにはメールのサイズとメッセージスコア[150]も表示されます。

ページ上部のツールバーにあるボタンから、様々なタスクを実行できます。

- **更新**—ログの閲覧を開始した後に追加されたエントリを表示するため、メッセージログの表示を更新するには、このボタンをクリックします。
- **検索**—特定のメールだけを表示するために、検索機能でフィルタを行います。メールの検索は対象のメールが送信用か受信用か、ヘッダ内の文字列、特定期間内か全ての期間か、等を基に行います。メッセージログを検索するには:
ツールバーの**検索を表示**ボタンをクリックすると検索ウィンドウが起動します。続いて、検索基準を選択し、**検索**ボタンをクリックすると、検索が実行されます。検索ウィンドウが非表示になり、検索結果がメッセージログへ表示されます。検索を表示ボタンを再度クリックすると、検索条件を編集でき、X検索を中止をクリックすると、検索を中止し、通常のメッセージログの画面に戻ります。
- **詳細**—メールを選択しこのボタンをクリックするとメッセージ情報画面が起動します。この画面には、Transcript、メッセージ、ソースの3つのタブがあります。Transcriptタブでは、SMTPセッション、内部処理を含む、配信処理が表示されています。 メッセージタブにはメールの内容と、メール本文や添付をダウンロードするためのオプションが表示されています。 ここでの表示は、メール配信からの経過日数、メールの配信が正常に行われたかどうか、およびデータ保持[118]ページでオプションが有効かどうかによって異なります。ソースタブは、メッセージのヘッダ、HTMLコード、などを含むメッセージのソースがあります。ソースは、メッセージが古い、または、SecurityGatewayのデータ保持[118]オプションで、データを保存するよう設定されていない場合、利用できません。
- **再配信**—一覧から1つまたは複数のメッセージを選択し宛先に再送信するには、このボタンをクリックします。Ctrl+ClickまたはShift+Clickで複数のメッセージを選択できます。このオプションは、データベースからメッセージの内容が削除されていない場合に使用できます。
- **Spam**—メッセージを選択し、スパムとしてメッセージをマークするために、このボタンをクリックします。これにより、その後のSecurityGatewayによるスパム判定精度を向上する事ができます。ベイジアン学習[134]機能が無効な場合、このオプションは利用できません。
- **スパムではありません**—メッセージを選択し、このボタンをクリックすると、対象メッセージを非スパムとしてマークします。これで、SecurityGatewayによる誤検知が起こりにくくなります。ベイジアン学習[134]機能が無効な場合、このオプションは利用できません。
- **ホワイトリスト/ブラックリスト**—メールを選択し、ホワイトリスト[221]又はブラックリスト[213]をクリックします。送信者のアドレスか、ドメインを、ユーザーリスト、ドメインリスト、全体リストの中で、どのリストへ追加するのかクリックします。

6.2 ログファイル

ログファイルセクションでは、ログフォルダ[110]に保存されているSecurityGartewayの各種ログファイルを閲覧できます。メッセージログと違って、ログファイルはデータベースで保存されず、各イベントはソートできる一覧として個々のエントリとして記録されます。その代わりに、SecurityGatewayが実行するSMTP接続や他の機能の処理をプレーンテキストとして記録しています。ログファイルセクションのすべてのログファイルページは、ログフォルダで含まれているログファイルの全てを一覧にし、現在のログファイル

およびロールオーバーファイル259を含んでいます。このページから、一覧にされるファイルのいずれかを閲覧することができます。ログファイルセクションの他のページは、SecurityGatewayの現在のログファイル、例えばシステムログ、受信および送信ログ、ウィルスアップデートログなど閲覧するショートカットを提供します。

ログファイルは、SecurityGatewayの内部バックアップオプションを使用して作成されるバックアップ120ファイル内に含まれません。しかし、アーカイブするために、ログの設定259ページのアーカイブ処理オプションを使用することができます。ログファイル別の場所に保存またはバックアップする場合、指定されたログ110ディレクトリ、でバックアップソフトウェアの実行または別の方法を使用する必要があります。

すべてのログファイル

すべてのログファイルページは、ディレクトリ110ページで指定されるログフォルダに含まれるログファイルすべてを一覧にします。SecurityGatewayで書き込まれる現在のファイルおよびロールオーバー259ログファイルが一覧表示されています。各エントリはファイルの名前、そのサイズ、変更日時の一覧です。一覧のファイルは、一覧でエントリをダブルクリック、またはエントリを選択しページ上部のツールバーで表示をクリックして閲覧することができます。ファイルを選択し**ダウンロード**ボタンをクリックしてファイルをダウンロードすることができます。エントリを選択して、**削除**ボタンをクリックするとファイルを削除することができます。

現在のログ

ログファイルセクションの残りになっているリンクは、SecurityGatewayにより使用される現在のファイルを表示します。それぞれのリンクをクリックして、下記ログファイルを閲覧できます。

- **システム**—システムログは、例えばSecurityGatewayサービス開始と停止、SMTP、SSL、HTTPおよび他のサービス初期化、発生しているシステムエラーなどのイベントです。
- **受信**—SecurityGatewayの受信ログは、すべての受信メッセージに対するセッションの写しを含んでいます。
- **送信**—このログは、すべての送信メッセージに対するセッションの写しを含んでいます。
- **ルーティング**—ルーティングログは、受信された後にユーザおよびサーバにメッセージの経路を定めているSecurityGatewayに関連したすべてのアクティビティを一覧表示しています。
- **変更**— SecurityGateway設定の変更全てと、変更した人が一覧表示されます。
- **アーカイブ**— このログには全ての アーカイブ86 関連のアクティビティが含まれます。
- **POP**—POPアカウント67に関連したアクティビティが含まれます。
- **HTTP**—このログは、すべてのHTTP関連のデータおよびアクティビティを含んでいます。
- **ClamAV更新**—ClamAV更新ログファイルは、ClamAVウィルスシグネチャアップデートに関する情報を一覧表示しています。
- **IKARUS Anti-Virusログ**— IKARUSウイルスシグネチャの更新、エンジンの状態、スキャンに関する3つのログファイルがあります。

6.3 ログの設定

ログの構成は、初期設定およびオプションを構成する使用します。ログの構成ページを表示するには、左側で**ロギング ≫設定 ≫ログ**の設定をクリックします。このページで、受信、送信およびHTTPログに書き込まれる情報の詳細レベルについて指定することができます。作成するログファイルのタイプを選択することができます。標準セットは、ファイル名に取り入れられる日付による毎日新規セット、あるいは、ファイル名に取り入れられる曜日による毎日新規のセットです。さらに、各種のログファイルメンテナンス、例えば、保存するまでのファイルサイズ、新規ファイルの開始、これらの"ロールオーバー"ファイルの数、アーカイブするまでの期間などの設定を選択することができます。すべてのログファイルは、ディレクトリ 110 ページで指定されるログフォルダに保存されます。

ログレベル

このセクションで選択されるオプションは、受信SMTP、送信SMTPおよびHTTPログファイル 257 のサイズを管理します。この設定は、システム、ルーティングまたはその他ログファイルに影響しません。

デバッグ
これは、受信、送信およびHTTPログファイル用のロギングオプションで最も詳細です。このオプションでは巨大なログファイルを作成するので、パフォーマンスに関して悪影響がある可能性があり、従って、通常、デバッグロギング方法にすべきではありません。問題をデバッグすることを試みる時には有用です。

情報
これはデフォルトオプションで、大半の状況に推奨される設定です。ロギングは、上記のデバッグオプションほど詳細ではありませんが、ログエントリは成功および失敗の両方のイベントについて作成されます。

警告
失敗したイベントおよび他の潜在的な問題を記録する場合、このオプションを選択します。

エラー
このオプションが選択される場合、失敗だけは記録されます。このログレベルの選択はパフォーマンスを高めます。

なし
任意の受信、送信またはHTTPイベントを記録しない場合、このオプションを選択します。このオプションは推奨されません。

ログモード

このセクションで選択するオプションは、ログファイルで使用されるネーミング規約を管理します。

ログファイルの標準セットを作成する
SecurityGatewayは、SecurityGateway-Inbound.log、SecurityGateway-Outbound.log、SecurityGateway-System.logなどの名前の付け方でログファイルの標準セットを作成します。

新規ログファイルセットを毎日作成する
これはデフォルトオプションです。このオプションは真夜中に各夜ログファイルの新規のセットを作成し日付が各ファイル名に取り入れられます。例えば: 2008年3月15日に作成される受信SMTPログファイルはSecurityGateway-20080315-Inbound.logとなります。

ログファイル名にコンピューター名を追加する
ログファイル名へコンピューター名を追加する場合はこのオプションを有効にします。このオプションはログフォルダがUNCパスの場合は必須で、クラスター[112]の複数サーバーが同じ場所のログファイルを使用する事も許可しています。

これらのIPアドレスからのSMTP又はHTTP接続をログ記録しない:
SMTPやHTTP接続をログに残したくないIPアドレスをこのオプションで指定します。指定されたIPアドレスからの不完全や拒否されたSMTPメールもデータベースへは記録されません。メールが送信を許可された場合は、ログがデータベースへ追加されます。

ログメンテナンス

このセクションのオプションは、ロールオーバーログファイル数の許可、ログファイルサイズ、既存のログファイルの上書き、古いログファイルのアーカイブする回数を管理します。

ログファイルの最大サイズ: [xx] KB (0 = サイズ制限なし)
ログファイルで許可する最大サイズ(KB単位)を指定するために、このオプションを使用します。ファイルが最大サイズに到達する時、*.OLDに名前を変え新規のファイルを開始します。これらの"ロールオーバー"ファイルの数は、下記で**ローテーションの最大値**オプションで確定されます。

ローテーションの最大値:
このオプションは、各ログファイルのロールオーバーファイル数を管理します。ログファイルが上記で指定される[ログファイルの最大サイズ]に到達する時、新規のロールオーバーファイルが作成されます。これらのファイルは、次のネーミング方式を使用します: "filename(1).old"、"filename(2).old"、"filename(3).old"、など。新規のロールオーバーファイルが作成されると、直近のデータが最初のファイルになるよう他のロールオーバーファイルの全ても名前が変更されます。例えば、"filename(1).old"が常に直近のロールオーバーファイルで、filename(2).old"は次に新しいファイルです。ファイルの最大値が到達すると、最も古いものが削除され、残りのファイルは通常に名前が変更されます。このオプションのデフォルト値は10です。

深夜にログファイル名が変更された場合に既存のログファイルに上書きする
上記の[曜日に基づくログファイルを作成する]オプションが選択される場合、真夜中の各夜SecurityGatewayは各ファイル名に曜日を取り入れているログファイルの新規のセットを作成します。この上書きをする場合、このオプションは同じ名前の既存ファイルを上書きするか、またはSecurityGatewayで古いファイルの終わりに新規データを追加するか指定します。例えば、このオプションが使用可能で日曜日の場合、"SecurityGateway-Sunday-Inbound.log"が存在する時には、ファイルは上書きされ、当日の情報だけを含んでいます。オプションが使用禁止の場合、当日のデータすべては、既存のファイルの終わりに追加されます。このオプションはデフォルトで無効です。

指定日数より古いログファイルを自動的にZIPでアーカイブする[xx]日(0 =しない)
このオプションで指定されている日数より古いすべてのログファイルを、各夜真夜中に圧縮しSecurityGatewayは¥Logs¥OldLogs¥ディレクトリ[110]へ移動します。このオプションのデフォルト値は14日です。

セクション 7

7 レポート

レポート セクションは、SecurityGatewayのアクティビティについて、インタラクティブで詳細なグラフィカルレポートを提供します。受信対送信メッセージの数、受信される迷惑メールのタイプの内訳を示しているレポート、帯域幅レポート、累積的なメッセージサイズによるトップの差出人、ウィルスリポートおよび示しているレポートを生成することができます。さらに、各レポートは、レポートのパラメータを指定するオプションを提供します。例えば、レポートは、時間、日または月による詳細データ、一定の期間(例えば日、週または月)、または日付の特定の範囲を使用して、特定のドメインまたはすべてのドメインについてのデータを持つことができます。さらに、下記に各レポートではレポート内容の内訳テーブルがあり、レポートでエントリに関連したデータだけを表示するためにログをフィルタするメッセージログ 256 へのリンクが提供されています。例えば、レポート一覧にされるある特定の時間で受信されるすべての受信メッセージ、特定の日で受信されるウィルスがあったすべてのメッセージ、ドメイン、その他についてトップの受信者による受信されるメッセージ全てについてのリンクが表示されています。レポートのパラメータを選択した後に、ページ上部のツールバーから表示をクリックするだけで新しいレポートが生成されます。

レポート メニューには6つのセクションがあります:

定期的なレポート

このセクションには統計レポートのオプションがあります:

- **統計レポート** – これは、サーバの有効性および健全なフィルタリングをすばやく突き止めることができる一般的な統計レポートです。毎晩または週単位の統計レポートを、すべてのグローバル管理者、すべてドメイン管理者あるいは手動で定義したメールアドレスに送信することができます。ドメイン管理者用のレポートは管理者が持つ管理権限のドメイン統計情報があります。

  統計レポート画面のスケジューリングセクションで、レポートを送信する間隔として毎夜あるいは毎週を指定するすることができます。続いて宛先セクションで、レポートをドメイン管理者全員に送信する場合に**すべてのグローバル管理者へ送信**、またはドメイン管理者へ送信する場合は**すべてのドメイン管理者へ送信**を選択します。特定の管理者へレポートの送信を除外する場合、除外する管理者のメールアドレスを**除外**セクションで指定します。レポートの受信を必要とする追加の電子メールアドレスを指定するには、**宛先の追加**オプションを使用します。

サマリ

サマリセクションのレポートは、標準的なサマリレポートで、受信対送信メッセージの数、適正対ジャンクメールの総数と種類、メールで使用された帯域幅の確認が行えます。

- **受信 vs.送信メッセージ**– このレポートは、レポートで指定される日付範囲において選択されたドメインについて、受信メッセージの合計および送信メッセージの合計を示します。グラフの下のテーブルには受信メッセージおよび送信メッセージのためにカラムがあります。各行は要約時間のレポートを表示する(時間、日または月)期間に対応します。メッセージログを開くために、テーブルでリンクをクリックし、そのエントリについて対応する時間中に、処理された受信または送信メッセージを表示します。レポートのエントリの数は、最大レコード設定によって制限されます。レポートが生成される場合、SecurityGatewayは最初の要約時間で開始し、最大レコード値が到達するまで継続します。最大レコード値が必要なだけ設定されない場合、レポートは指定される全体の日付範囲をカバーできません。新

規のレポートを生成するには、パラメータを指定し、レポートのツールバーで表示をクリックします。

- **適正メール対ジャンクメール**– このレポートは、レポートで指定される日付範囲において選択されたドメインについて妥当または正当なメッセージの合計対処理されるジャンクメッセージを示します。ジャンクメッセージは、ウィルスなどを含むスパム、なりすましとして確認されるメッセージです。グラフの下のテーブルには妥当なメッセージおよびジャンクメッセージについてカラムがあります。各行は要約時間のレポートを表示する(時間、日または月)期間に対応します。メッセージログを開くためにテーブルでリンクをクリックし、そのエントリについて対応する時間中に、処理されたジャンクメッセージを表示します。レポートのエントリの数は、最大レコード設定によって制限されます。レポートが生成される場合、SecurityGatewayは最初の要約時間で開始し、最大レコード値が到達するまで継続します。最大レコード値が必要なだけ設定されない場合、レポートは指定される全体の日付範囲をカバーできません。新規のレポートを生成するには、パラメータを指定し、レポートのツールバーで**表示**をクリックします。
- **ジャンクメール分析** – このレポートは、レポートで指定される日付範囲において選択されたドメインについて、すべてのジャンクメール、タイプによるカテゴリを示します。迷惑メールは、スパム[127], ウィルス[152], なりすまし[156], 不正使用、[180]不備、ユーザ6つのタイプに分類されます。不備カテゴリは、タイムアウトが発生するすべてのセッション、または、クライアントはソケットをクローズ、あるいは、データを送信する前に、終了コマンドを発行です。SMTPの調査は、このカテゴリに該当します。ユーザカテゴリは、ブラックリスト[213], コンテンツフィルタルール[202], 添付ファイルフィルタリング[210]およびカスタムSieveスクリプト[228]についてです。残りカテゴリは、対応するセキュリティ[126]セクションを参照します。グラフの下のテーブルにはタイプについてカラムがあります。各行は要約時間のレポートを表示する(時間、日または月)期間に対応します。メッセージログを開くためにテーブルでリンクをクリックし、そのエントリについて対応する時間中に、処理されたジャンクメッセージを表示します。レポートのエントリの数は、最大レコード設定によって制限されます。レポートが生成される場合、SecurityGatewayは最初の要約時間で開始し、最大レコード値が到達するまで継続します。最大レコード値が必要なだけ設定されない場合、レポートは指定される全体の日付範囲をカバーできません。新規のレポートを生成するには、パラメータを指定し、レポートのツールバーで**表示**をクリックします。
- **メールで使用された帯域の総計** – このレポートは、レポートで指定される日付範囲においてメールによって使用される帯域幅の量を示します。グラフの下のテーブルにはタイプについてカラムがあります。各行は要約時間のレポートを表示する(時間、日または月)期間に対応します。メッセージログを開くためにテーブルでリンクをクリックし、そのエントリ中に処理されたメッセージを表示します。レポートのエントリの数は、最大レコード設定によって制限されます。レポートが生成される場合、SecurityGatewayは最初の要約時間で開始し、最大レコード値が到達するまで継続します。最大レコード値が必要なだけ設定されない場合、レポートは指定される全体の日付範囲をカバーできません。このセクションのすべてのレポートと同様に、新規のレポートを生成するには、パラメータを指定し、レポートのツールバーで**表示**をクリックします。

受信メール

受信メールセクションのレポートは、受信メッセージのみを対象にしています。処理されたすべての受信メッセージの詳細レポート、メッセージの数によるトップのメール受信者のレポートおよび累積的なメッセージサイズによるトップの受信者のレポートを生成することができます。

- **処理をした受信メール**– このレポートは、レポートで指定される日付範囲において選択されたドメインについて処理される受信メッセージの総数を示します。グラフの下のテーブルには、要約時間のレポートを表示する(時間、日または月)期間に、処理される受信メッセ

ージの総数を示しているカラムがあります。特定の期間中に、処理された受信メッセージを表示するためにメッセージログを開くには、テーブルで時間期間リンクのいずれかをクリックします。レポートのエントリの数は、最大レコード設定によって制限されます。レポートが生成される場合、SecurityGatewayは最初の要約時間で開始し、最大レコード値が到達するまで継続します。最大レコード値が必要なだけ設定されない場合、レポートは指定される全体の日付範囲をカバーできません。新規のレポートを生成するには、パラメータを指定し、レポートのツールバーで**表示**をクリックします。

- **上位のメール宛先** – このレポートは、レポートで指定される日付範囲において、選択されたドメインで受信したメッセージのトップの受信者を示します。グラフの下のテーブルには、受信者のアドレスのカラムと受信者されたメッセージ数のカラムがあります。レポートの日付範囲において、特定のユーザによって受信されるメッセージを表示するメッセージログを開くには、受信者のアドレスをクリックします。新規のレポートを生成するには、パラメータを指定し、レポートのツールバーで**表示**をクリックします。
- **メッセージサイズの累積で上位の宛先** – このレポートは、累積的なメッセージサイズまたは帯域幅(レポートで指定される日付範囲における選択されたドメインについての受信メッセージ)によるトップのメール受信者を示します。グラフの下のテーブルには、受信者および各受信者が受信したメッセージサイズ総計のカラムがあります。レポートの日付範囲において、特定の受信者によって受信されるメッセージを表示するメッセージログを開くには、受信者をクリックします。新規のレポートを生成するには、パラメータを指定し、レポートのツールバーで**表示**をクリックします。

送信メール

送信メールセクションのレポートは、送信メッセージのみを対象にしています。 処理されたすべての送信メッセージの詳細レポート、メッセージの数によるトップのメール送信者のレポートおよび累積的なメッセージサイズによるトップの送信者のレポートを生成することができます。

- **処理をした送信メール**– このレポートは、レポートで指定される日付範囲において選択されたドメインについて処理される送信メッセージの総数を示します。グラフの下のテーブルには、要約時間のレポートを表示する(時間、日または月)期間に、処理される送信メッセージの総数を示しているカラムがあります。特定の期間中に、処理された送信メッセージを表示するためにメッセージログを開くには、テーブルで時間期間リンクのいずれかをクリックします。レポートのエントリの数は、最大レコード設定によって制限されます。レポートが生成される場合、SecurityGatewayは最初の要約時間で開始し、最大レコード値が到達するまで継続します。最大レコード値が必要なだけ設定されない場合、レポートは指定される全体の日付範囲をカバーできません。新規のレポートを生成するには、パラメータを指定し、レポートのツールバーで**表示**をクリックします。
- **上位のメール差出人** – このレポートは、レポートで指定される日付範囲において、選択されたドメインから送信したメッセージのトップの送信者を示します。グラフの下のテーブルには、送信者のアドレスのカラムと送信されたメッセージ数のカラムがあります。レポートの日付範囲において、特定のユーザによって送信されるメッセージを表示するメッセージログを開くには、送信者のアドレスをクリックします。新規のレポートを生成するには、パラメータを指定し、レポートのツールバーで**表示**をクリックします。
- **メッセージサイズの累積で上位の差出人** – このレポートは、累積的なメッセージサイズまたは帯域幅(レポートで指定される日付範囲における選択されたドメインについての送信メッセージ)によるトップのメール差出人を示します。グラフの下のテーブルには、差出人および各差出人が送信したメッセージサイズ総計のカラムがあります。レポートの日付範囲において、特定の差出人によって送信されるメッセージを表示するメッセージログを開くには、差出人をクリックします。新規のレポートを生成するには、パラメータを指定し、レポートのツールバーで**表示**をクリックします。

スパム対策

スパム対策セクションのレポートは、どのドメインがユーザに最も多くのスパムを送信しているか、さらに、どのユーザが最も多く受信しているか確認することができます。

- **上位のスパムドメイン**– このレポートは、レポートで指定される日付範囲において選択されたドメインにスパムメッセージを送信しているトップのドメインを示します。グラフの下のテーブルには、スパムを送信しているドメインのカラム、そのドメインから受信されるメッセージ数のカラムがあります。レポートの日付範囲においてユーザに特定のドメインによって送信されるメッセージを表示するメッセージログを開くには、リストでドメインをクリックします。新規のレポートを生成するには、パラメータを指定し、レポートのツールバーで**表示**をクリックします。
- **上位のスパム宛先** – このレポートは、レポートで指定される日付範囲において選択されたドメインについてスパムのトップの受信者を示します。グラフの下のテーブルには、受信されるスパムメッセージ数のカラム、受信者のアドレスカラムがあります。レポートの日付範囲において特定のユーザによって受信されるスパムメッセージを表示するメッセージログを開くには、受信者のアドレスをクリックします。新規のレポートを生成するには、パラメータを指定し、レポートのツールバーで**表示**をクリックします。

ウィルス対策

アンチウィルスセクションのレポートでは、SecurityGatewayで中止された送受信メッセージのウィルス数、およびどのウィルスが存在するか確認できます。

- **ブロックされたウィルス(受信)** – このレポートは、指定される日付範囲で選択されたドメインについて、SecurityGatewayによって中止されたウィルスを含んでいる受信メッセージの総数を示します。グラフの下のテーブルは、遮断されたウィルスをもつ受信メッセージの総数を示すカラムがあります。特定の期間中に、遮断されたウィルスをもつ受信メッセージを表示するメッセージログを開くには、テーブルで期間リンクをクリックします。レポートのエントリの数は、最大レコード設定によって制限されます。レポートが生成される場合、SecurityGatewayは最初の要約時間で開始し、最大レコード値が到達するまで継続します。最大レコード値が必要なだけ設定されない場合、レポートは指定される全体の日付範囲をカバーできません。新規のレポートを生成するには、パラメータを指定し、レポートのツールバーで**表示**をクリックします。
- **受信されたウィルス(名称)** – このレポートは、レポートで指定される日付範囲中に選択されたドメインのためにSecurityGatewayによって遮断された受信メッセージで、トップのウィルスを示します。グラフの下のテーブルには、遮断されるウィルスの名を一覧にしているカラムおよび各ウィルスの事例数を一覧にしているカラムがあります。ウィルスがレポートの日付範囲において遮断さえた特定のウィルスを持つ受信メッセージを表示するメッセージログを開くには、ウィルス名をクリックします。新規のレポートを生成するには、パラメータを指定し、レポートのツールバーで**表示**をクリックします。
- **ブロックされたウィルス(送信)** – このレポートは、指定される日付範囲において選択されたドメインから送信されたSecurityGatewayによって遮断されたウィルスを含んでいる送信メッセージの総数を示します。グラフの下のテーブルには、レポートを表示する(時間、日または月)各期間に、ウィルスをもつ送信メッセージの総数を示すカラムがあります。特定の期間中に、遮断されたウィルスをもつ送信メッセージを表示するメッセージログを開くには、テーブルで時間期間リンクをクリックします。レポートのエントリの数は、最大レコード設定によって制限されます。レポートが生成される場合、SecurityGatewayは最初の要約時間で開始し、最大レコード値が到達するまで継続します。最大レコード値が必要なだけ設

定されない場合、レポートは指定される全体の日付範囲をカバーできません。新規のレポートを生成するには、パラメータを指定し、レポートのツールバーで**表示**をクリックします。

- **送信されたウィルス(名称)** – このレポートは、指定される日付範囲において選択されたドメインから送信されたSecurityGatewayによって遮断される送信メッセージでトップのウィルスを示します。グラフの下のテーブルは、遮断されるウィルス名を一覧にするカラムと各ウィルスの事例数を一覧にするカラムがあります。レポートの日付範囲において遮断された特定のウィルスを含んでいる送信メッセージを表示するメッセージログを開くには、ウィルス名をクリックします。新規のレポートを生成するには、パラメータを指定し、レポートのツールバーで表示をクリックします。

パフォーマンスモニターカウンタ

ここで紹介したレポートオプションに加え、SecurityGatewayではWindowsパフォーマンスモニター用のパフォーマンスカウンタを複数ご用意しており、SecurityGatewayのステータスをリアルタイムで監視する事ができます。カウンターには、送受信用のSMTPセッション数、配信用のキュー内のメッセージ数、隔離されているメッセージ数、SecurityGatewayの稼働時間、ドメインとユーザーの数、といったものがあります。**注意点**: 次のカウンターについては1分おきに更新されます。: 配信用キュー, 管理隔離, ユーザー数, ドメイン数

カウンターを使用するには、Windowsで次の操作を行います:

1. コントロールパネルの中の管理ツールを開き、**パフォーマンスモニター** をダブルクリックします(または、**perfmon**を実行します)。
2. モニターツールの下の、**パフォーマンスモニター**をクリックし、ツールバーの「+」(追加)をクリックして、カウンターの追加用ダイアログを開きます。
3. 使用可能なカウンターで、**SecurityGateway**をクリックし、**追加 >>** をクリックし、全てのSecurityGateway用カウンターを追加します。全てのカウンターを追加するのではなく特定のカウンターのみ追加する場合は、SecurityGatewayグループを展開し、使用するカウンターを選択してから**追加 >>** をクリックします。
4. **OK**をクリックします。

注意点: 他のサーバー上で稼働しているSecurityGatewayのカウンターを利用する場合は、リモートレジストリサービスを有効化し、カウンターへ接続できるようファイアウォールを設定する必要があります。

索引

- F -

- G -

- H -

- I -

- L -

- M -

- O -

– P –

– R –

– S –

– T –

– U –

– V –

– W –

– Z –