MAILSCREEN V2.5 管理者マニュアル

（両面印刷のための空白ページです）

「 目　 次 」

1. 概要

1.1. MAILSCREENとは？

MAILSCREENは、社内から社外に送信されるメールに対する制御と管理ができるメール誤送信防止及び、情報漏洩対策用のメールセキュリティシステムです。

社内メールを社外に送信する前に、送信者・宛先をチェックし、件名・本文・添付ファイルに重要な情報が含まれているかどうかをチェックし、フィルタリングすることが可能です。

添付ファイル暗号化、添付ファイルのリンク変換、決裁、送信遅延、遮断など、様々なポリシーを適用する事で、情報漏洩の防止に役立ちます。

MAILSCREENの設置構成は、一般的に2種類の方式に分かれます。ブリッジ(Bridge)方式は「図1」のように、物理的にメールサーバの通信経路上に設置する方式です。プロキシ(Proxy)方式は「図2」にように物理的位置は任意で、メールクライアント（MUA）のSMTP設定（メールサーバ）をMAILSCREENに変更し、MAILSCREENからメールサーバに送信されるようにする方式です。（通信経路上に設置する必要はありません。）

図 1　ネットワーク構成 – ブリッジ接続

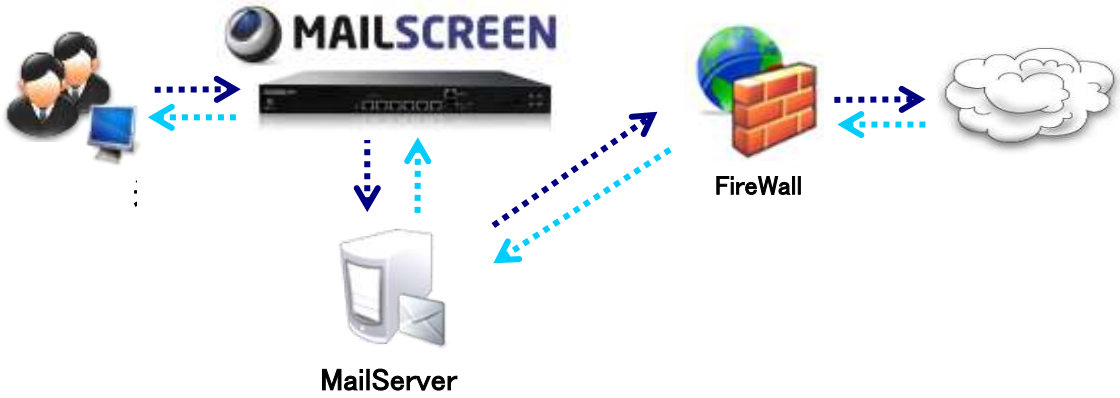


図 2　ネットワーク構成 –プロキシ接続

1.2. Web-Adminとは？

Web-Adminは、WebブラウザからMAILSCREENの操作・管理ができる管理UI（User Interface）です。メール確認、設定、ポリシー管理などの操作を簡単に行えるUIを提供しています。
「詳細設定」と**「かんたん設定」**のいずれかのメニューを選択できます。

「図1」は、**「詳細設定」**の画面です。

Web-Adminの画面は、主にメインメニュー・リストメニュー・設定画面に区分されます。

メインメニューにて1つのメニューを選択すると、リストメニューに詳細メニューが表示されます。

図 1 Web-Admin「詳細設定」画面

「図2」は**「かんたん設定」**の画面です。ログイン時に「UI Mode」で選択が可能です。**「かんたん設定」**は、必要最低限設定しなければならない設定メニューをまとめたもので、簡単に設定ができるメニューです。

図2 Web-Admin「かんたん設定」画面

1.3. MAILSCREENの主な機能

MAILSCREENは、以下の主要機能を提供します。

- 操作が簡単なWeb-Admin
  Web-Adminは、MSIE、FirefoxなどのWebブラウザに対応し、日本語、韓国語、英語の3種類の多言語インターフェースを提供します。Web-AdminではMAILSCREENの全ての管理が可能であり、サーバの状態と動作に関する項目を設定・保存・確認できます。
  また、スマートフォンでも管理ができるようにスマートフォン用のページも提供しています。（決裁に関する機能のみ）

- 企業内部からの外部への情報漏洩を防止
  送信メールのヘッダ、本文内容、添付ファイルなどに対して、リアルタイムでコンテキストパターン検索を行います。ポリシーによって、添付ファイル暗号化、添付ファイルのリンク変換、送信遅延、決裁、ルーティング指定などのメール処理機能を提供し、メールによる社内情報漏洩を防止できます。

- バックアップ及び障害対策のための環境を提供
  MAILSCREENは、データ消失対策としてバックアップ及び復元機能を提供しております。また、セキュアなサービス利用のために周期的なシステムチェックが行われ、監査及びメール保存領域、サービス、メールキュー、DBMSの状態検査時に異常を発見した場合は管理者に警告メールを送信します。

1.4. クライアント・スペック

下記は、MAILSCREENを運用管理するためのクライアント・スペックです。

表 1 Web-Admin 使用環境

クライアント環境	H/W	Display： 画面サイズ1024 X 768 以上
	S/W	Microsoft Internet Explorer 8.0 以上 Firefox 3.0 以上
		SSL通信及びクッキー(cookie)/JavaScript 使用可能
	OS	UTF-8 文字コードをサポートするオペレーティングシステム

2. ログイン

MAILSCREENを管理するために、Web-Adminページにログインします。

2.1. ログイン

使用方法

1. Webブラウザを起動します。
2. Webブラウザのアドレスバーに

‘http://<MAILSCREENのIP、或いはドメイン名>’

または

‘https://<MAILSCREENのIP、或いはドメイン名>’

を入力します。

3. **‘https://’**を入力し、MAILSCREENに導入されているサーバ証明書が独自証明書の場合には、セキュリティ認証の警告メッセージが表示されますが、**「このサイトの閲覧を続行します（推奨されません）。」**をクリックします。

4. ログインページが表示されたら、下記の情報を入力した後、「ログイン」ボタンをクリックします。

→ Language： Web-Admin画面で利用する言語を選択します。

→ UI Mode：「詳細設定」と「かんたん設定」のいずれか一つを選択します。

→ E-mail： ログイン用のメールアドレス

→ Password： 英文大・小文字と数字、特殊文字で構成された8から40文字の文字

5. メールアドレスとパスワードを入力してログインすると、統計画面が表示されます。アカウント認証に失敗した場合はログインエラーの画面が表示されます。

注意

- ログインに失敗した回数が、**環境設定>システム>アクセス制御>ユーザログイン>アカウントロック**で設定されている回数を超えた場合、該当アカウントは、「アカウントロックの時間」で設定されている時間だけ、無効化（アカウントロック）されます。
- 無効化された後で、再度ログインを試してログイン失敗した場合は、無効化の時間が「アカウントロックの時間」分だけ無効化の時間が加算されます。また、ログインに成功した場合のみ、ログイン失敗回数のカウントが初期化されます。
- ログインに成功した後、Web-Admin にて管理・操作がないまま、一定時間が経つと、ログインされているセッションが終了して自動ログアウトされます。

3. ユーザ管理

MAILSCREENを利用するためにはユーザ情報を登録する必要があります。

3.1. ユーザ管理

ユーザは、個人ユーザとスーパー管理者、決裁者、ログ閲覧者に分かれます。スーパー管理者はMAILSCREENの設定と管理が全て可能であり、決裁者はポリシーにより決裁待機されたメールの決裁のみ可能、ログ閲覧者はログ参照のみ可能です。

3.1.1. ユーザ管理

ユーザ情報を管理します。

使用方法

1. **「ユーザ管理>ユーザ管理」**を選択します。
2. ユーザ管理リスト画面が表示されます。下記に、リストに出力される各情報について説明します。

→ 名前: 各ユーザの名前

→ Eメール:ユーザのメールアドレス(ログインIDとして使用)

→ 社員番号:ユーザの社員番号

→ 権限:ユーザの権限

→ 言語:Web-Adminで使用する言語(デフォルト言語)

→ 所属:所属グループまたは部署

→ 決裁者:該当ユーザの決裁者

→ 例外:ポリシー適用の例外対象有無。例外対象ならY、例外対象でなければNで表示されます。

→ 登録日:ユーザを登録した日付

3. ユーザリストの上下にある各機能について説明します。

→ 1.削除： 選択されたユーザを削除します。

注意

✖ 現在ログイン中のカレントアカウントは削除できません。

→ 2.追加： ユーザを追加します。「追加」に関する詳細は **3.1.2 ユーザ追加**を参照してください。

→ 3.ファイル保存： ユーザリストをExcelファイルとして保存します。

→ 4.リスト数の設定： 1ページ当り表示されるユーザリストの表示数を設定します。

→ 5.情報修正： ユーザ情報の中でメールアドレスをクリックすると、ユーザ情報の修正が可能になります。情報修正の各項目は、**3.1.2ユーザ追加**を参照してください。

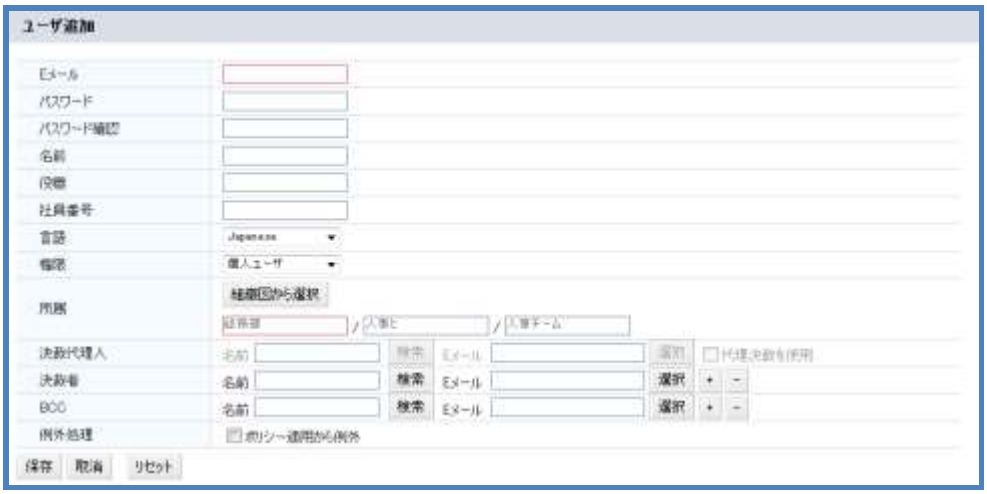
→ 6.検索： 検索条件(名前、メールアドレス、権限、所属、決裁者)を選択した後、キーワードを入力します。

3.1.2. ユーザ追加

ユーザを追加します。

使用方法

1. **「ユーザ管理>ユーザ管理」**を選択します。
2. ユーザリストメニューの「追加」ボタンをクリックします。
3. ユーザ追加画面が表示されたら、下記の情報を入力した後、**「保存」** ボタンをクリックします。



→ Eメール：メールアドレスを入力します。（ログインID、メール通知用として使用）

→ パスワード： ログインに使用するパスワードとして、英文大文字、小文字と特殊文字（又は数字）を含めた8文字から40文字の範囲で設定します。

→ パスワード確認： 「パスワード」に入力した値をもう一度入力します。

→ 名前： ユーザの名前

→ 役職： ユーザの役職

→ 社員番号： ユーザの社員番号

→ 言語： Web-Adminで使用するデフォルト言語をEnglish、Korean、Japaneseの中から一つ選択します。

→ 権限： 権限をスーパー管理者、決裁者、ログ閲覧者、個人ユーザの中から一つ選択します。

スーパー管理者	MAILSCREENシステムに対して全てのシステム権限を持ちます。
決裁者	決裁者が、決裁が必要なメールのみ管理ができます。決裁待機と送信遅延状態のメールに対し、決裁と送信などの管理ができます。
ログ閲覧者	メールのログと統計の管理ができます。
個人ユーザ	一般的なユーザで、Web-Adminへのアクセス権限と管理権限がありません。

→ 所属： ユーザの所属を入力します。「組織図から選択」をクリックすると、既存に入力されていた組織図リストがポップアップで表示され、簡単に所属情報を入力できます。

→ 決裁代理人： 決裁者が決裁できない場合に、決裁者の代わりに決裁を行う代理人を設定します。

→ 決裁者： 決裁者情報を入力します。「+」「-」ボタンを利用して追加できます。最大10名まで追加可能です。

→ BCC： BCC情報を入力します。ポリシーを追加すると、ポリシーお知らせのオプションとお知らせ方法により、BCCに設定したユーザにお知らせメールが配信されます。「+」「−」を利用して追加できます。

→ 例外処理： ポリシーを適用させないユーザを設定します。例外設定をした場合、該当ユーザはポリシーに適用されなくなります。

注意

- ✖ 赤い枠で囲まれている入力欄は、必須入力項目です。
- ✖ スーパー管理者と決裁者、ログ閲覧者は権限とそれに伴う責任に関して適切な教育を受ける必要があり、全ての管理者指針及び手続きに正確に従って役目を果す必要があります。
- ✖ 決裁者情報は、ポリシー設定項目の中で（**4.1.2 ポリシー追加**を参照）‘人事情報決裁者に決裁要請’を設定した場合、ユーザ情報に登録されている決裁者に決裁要請が行われるので、正確に記入してください。

4. **「保存」**ボタンをクリックします。**「リセット」**ボタンをクリックすると入力された全ての情報が初期化されます。

3.1.3. ユーザー括登録

CSVテキストファイルを使用してユーザ情報を一括して登録できます。

使用方法

1. **「ユーザ管理>ユーザー括登録」**を選択します。

2. 「ユーザー括登録画面」でそれぞれのオプションを設定して、「参照」ボタンをクリックし、CSV形式のファイルをアップロードします。

→ ファイルアップロード： ファイルの内容を登録する時にオプションを設定します。

- ファイルに存在しないユーザは削除： 既に登録されているユーザの中で、CSVファイルにないユーザは削除します。

注意

- ✖ 一括登録時のファイルは、CSV 形式ファイルのみ可能です。
- ✖ ファイルに保存されている情報は、下記の順で記録されている必要があります。
  – メールアドレス、名前、役職、社員番号、言語、権限、 携帯電話番号、所属、決裁代理人の名前、決裁代理人のメールアドレス、決裁者の名前、決裁者のメールアドレス、BCC の名前、BCC メールアドレス、例外処理
- ✖ 言語設定時、日本語は ‘ja’、英語は ‘en’、韓国語は ‘ko’ に設定してください。
- ✖ 権限と例外処理は数字形式で設定してください。

権限	個人ユーザ： 1、 決裁者： 2、 ログ閲覧者： 3、 スーパー管理者： 9
例外処理	例外処理： 1、 例外処理しない： 0

- ✖ 所属の下位区分は ‘^’ のみ使用可能
  例） 総務部^人事課^人事チーム

→ メールのお知らせ：登録されたユーザにお知らせメールが配信されます。お知らせメールの件名と本文テンプレートを変更する事が可能です。また、「プレビュー」 ボタンをクリックして確認ができます。

- 新しく追加される決裁者にパスワードお知らせメールを送信：IDとログインパスワード、MAILSCREEN接続情報に関するお知らせメールが配信されます。

3. 下の「登録」ボタンをクリックします。

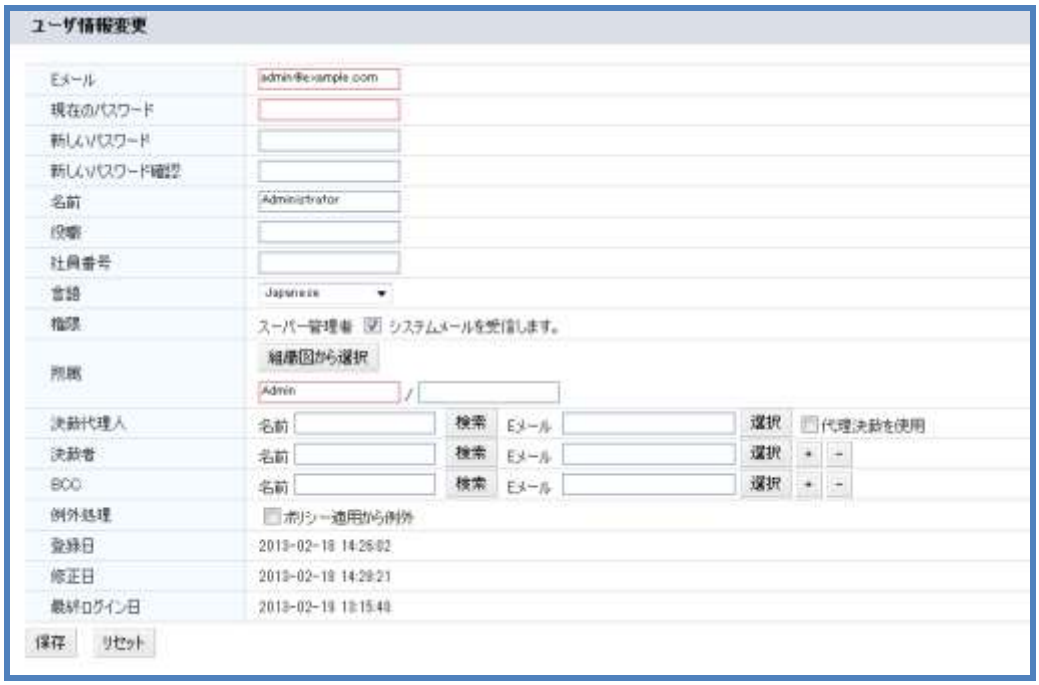
3.1.4. ユーザ情報の変更

ユーザ情報を変更します。

使用方法

1. **「ユーザ管理>ユーザ情報変更」**を選択します。

2. 現在ログインしているユーザの情報を変更できる画面が表示されます。各項目に関する詳細は、 **3.1.2ユーザ追加**を参照してください。



3. 各項目を修正した後、「保存」ボタンをクリックします。

4. ポリシー管理

MAILSCREENはポリシーを種類別に分けて適用できます。メールのヘッダ、件名、本文内容を検査してフィルタリングするポリシー、SMTPレベルでIPとドメイン、メールをフィルタリングするBlack/White List、主要取引先など、許容した宛先を予め登録して管理する許容宛先ポリシーに分けられます。より詳細で柔軟なポリシー適用と管理が可能になります。

注意

- MAILSCREEN は、ポリシー適用時のフィルタ検査では、英文大文字と小文字を区別しないので、Black List と White List、 ポリシー追加、許容宛先の登録時に注意してください。

4.1. ポリシー

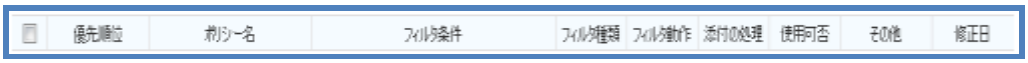
ポリシーは、MAILSCREENを通過する全ての送信メールに対して検査を行います。

4.1.1. ポリシー管理

ポリシーリストを表示します。

使用方法

1. 「**SMTP Filter>ポリシー管理>ポリシー**」を選択します。
2. 各ポリシーのリストが表示されます。
3. ポリシーリストの各項目について、下記に説明します。



→ 優先順位：全てのポリシーに対して、優先順位を設定できます。リストの上位にあるポリシーほど優先順位が高くなります。

→ ポリシー名：ポリシーの名前

→ フィルタ条件：ポリシーを適用するためのフィルタ条件

→ フィルタ種類：フィルタの種類（誤送信防止のみ固定）

→ フィルタ動作：メールがフィルタ条件に合致した場合の処理方法

→ 添付の処理：条件に合致した場合の添付ファイルの処理方法

→ 使用可否：ポリシーの適用可否

→ その他：ポリシーに関するコメント

→ 修正日：ポリシーの修正日付

4. ポリシーリストの関連機能について、下記に説明します。

→ 1.検索： 「ポリシー名/適用対象(適用対象と所属)/フィルタ内容(フィルタ値)/例外対象(例外対象と所属)/メール処理/使用可否/フィルタ種類/添付処理」の中で、内容を入力した後、「検索」ボタンをクリックします。各項目に関する詳細は **4.1.2ポリシー追加**を参照してください。

→ 2.削除： 選択したポリシーを削除します。

→ 3.ポリシー追加： ポリシーを追加します。詳細は **4.1.2ポリシー追加**を参照します。

→ 4.リスト表示数の設定： 1ページ当り表示されるリストの表示数を設定します。

→ 5.ポリシー修正： ポリシー名をクリックすると、ポリシーの内容を修正できます。修正できる内容については、**4.1.2ポリシー追加**を参照してください。

4.1.2. ポリシー追加

ポリシーを追加します。

使用方法

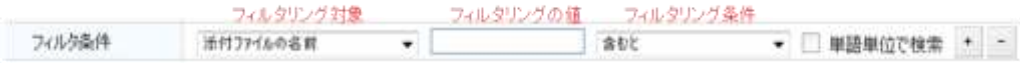
1. 「SMTP Filter>ポリシー管理>ポリシー追加」を選択します。
2. 下記に、「ポリシー追加」ページの各項目について説明します。

→ ポリシー名： ポリシーの名前を入力します。(最大64バイト)
→ 適用対象： ポリシーを適用する対象を設定します。
・全体ユーザ： 該当ポリシーを全ユーザに対して適用します。全ユーザが送信する全てのメールに対してポリシーが適用されます。
・対象を指定： 選択したユーザのみを対象にしてポリシーが適用されます。「選択」ボタンをクリックすると、組織図リストがポップアップで表示されます。ポリシーを適用する対象を選択して「確認」をクリックします。
・直接入力： ポリシー適用対象を、メールアドレスまたは '@ドメイン' 形式で直接入力します。組織図リストにないユーザに対してもポリシーを設定できます。
→ 例外対象： ポリシー適用から除外する対象を設定します。ポリシーが適用される対象より優先順位が高く、例外対象に設定されたグループ(所属)やユーザが送信したメールは該当ポリシーが適用されなくなります。
・対象指定： 例外対象に設定するユーザを選択できます。「選択」ボタンをクリックすると、組織図リストがポップアップで表示されます。ポリシー適用の例外対象を選択して「確認」をクリックします。
・直接入力： ポリシー適用の例外対象を、メールアドレスまたは '@ドメイン' 形式で直接入力します。組織図リストにないユーザに対してもポリシーを設定する事ができ

ます。

→ フィルタ演算： メールと添付ファイル処理のためのフィルタ演算条件を設定します。AND条件、OR条件のどちらかを選択します。

→ フィルタ条件： フィルタ条件は、フィルタリング対象、フィルタリングの値、フィルタリング条件で構成されます。フィルタ条件は、「+」「−」ボタンを利用して追加可能で、1つのポリシーに最大10個まで入力できます。



- フィルタリング対象： メールのヘッダと本文内容、添付ファイルなど、フィルタリング対象を設定します。

  - ✓ タイトル： メールの件名やタイトル
  - ✓ 本文： メール本文の内容を検査します。メール本文が複数のMIMEで構成されている場合は全てのMIMEを検査します。
  - ✓ ヘッダ送信者： メールの送信者（From）を検査します。ヘッダ送信者とは、ユーザがMS Outlookなどのメールクライアントを利用してメールを確認した時に表示される送信者情報を示します。
  - ✓ ヘッダ受信者： メールの受信者(To)を検査します。ヘッダ受信者とは、ヘッダ送信者の反対側の受信者情報を示します。
  - ✓ エンベロープ送信者： SMTPに送信されるメールのEnvelope Mail From情報を検査します。送信者がメールを送信してメールを受信するSMTPはEnvelope Mail情報とメール内容を受信しますが、この情報には、送信者、受信者情報があり、ヘッダ送信者、ヘッダ受信者情報とは異なります。
  - ✓ エンベロープ受信者： SMTPに送信されるメールのEnvelope Mail To情報を示す。
  - ✓ Cc： メールの参照者(Cc)を検査します。
  - ✓ 外部の受信者： 外部の受信者とは、受信者のドメインがMAILSCREENに登録されていない（**「環境設定>メールサーバ>メールサーバ」**に登録されているメールドメイン以外）受信者を示します。メール受信者の中で外部受信者の存在有無を検査します。
  - ✓ 許容宛先の未登録受信者： 許容宛先とは、**「SMTP Filter>ポリシー管理>許容された受信者」**に登録されている、メール受信が許容されたユーザを示す。外部メール受信者の中で、許容宛先に登録されているかを検査します。

注意

- ✖ フィルタ条件が ‘含むと’ の場合、フィルタリング対象メールの全ての受信者が許容宛先に登録されている必要があります。
- ✖ フィルタ条件が ‘含まない場合’ の場合、フィルタリング対象メールの受信者の中で 1 人以上が「許容された受信者」リストに登録されていない必要があります。

- ✓ Content-type：メールの本文形式情報を検査します。Boundary情報もこれに含まれます。
- ✓ Reply-To：メールヘッダに記入されている返送アドレスを検査します。
- ✓ X-Mailer：メールを送信するクライアントソフトの名前を検査します。
- ✓ IP：送信メールサーバの IP アドレスを検査します。IP アドレス形式(x.x.x.x)で、「.」または数字で終わる必要があります。
- ✓ ヘッダ全体：メール全体ヘッダの値を検査します。 各ヘッダ単位に、実際の値とフィルタリング値を比較・照合する方式で検査します。
- ✓ 受信者の全体数(名)：メール受信者数を検査します。 この数は To、 Cc、 Bcc に含まれている全ての受信者を合わせた値です。
- ✓ メール全体サイズ：Kbytes 単位でメール全体サイズを検査します。
- ✓ 添付ファイルの名前：添付された全てのファイルの名前を検査します。
- ✓ 添付ファイルのサイズ(KB)：全ての添付ファイルに対して、それぞれのファイルサイズを検査します。 Kbytes 単位で入力します。
- ✓ 添付ファイルの個数(個)：添付ファイル数を検査します。
- ✓ 添付ファイルの形式：添付ファイルの種類(拡張子)を検査します。
- ✓ 添付ファイルの内容：添付ファイルの内容を検査します。
- ✓ パスワードが設定された添付ファイル：パスワードが設定された添付ファイルの有無を検査します。

- フィルタリングの値：フィルタリング対象と比較・照合するための比較対象値を入力します。
- フィルタリング条件：フィルタリング対象とフィルタリング値がどのように一致するかどうかの判断条件を設定します。
  - ✓ 含むと：フィルタリング対象にフィルタリング値が含まれているか、一致している場合。
  - ✓ 含まない場合：フィルタリング対象にフィルタリング値が含まれていないか、一致しない場合。
  - ✓ 一致すると：フィルタリング対象とフィルタリング値が完全に一致する場合。
  - ✓ 始まると：フィルタリング対象がフィルタリング値で始まる場合。
  - ✓ 終わると：フィルタリング対象がフィルタリング値で終わる場合
  - ✓ 正規式にマッチされる場合：正規式とは、一定のルールを持つ文字列集合を表現するのに使用する式であり、文字列の検索と置換えがサポートされます。この条件を選択すると、管理者は直接正規式を入力する必要があります。正規式は、想定以上に多くのメールをフィルタリングする場合がありますので、使用する場合には注意してください。
  - ✓ 空白なら：フィルタリング対象が空白の場合

→ フィルタ動作：フィルタリングされたメールを処理する方法を設定します。

各フィルタ動作により、入力項目が異なります。

- **送信遅延**：条件に一致したメールの送信を遅延させます。各ポリシーは送信遅延設定が可能です。送信遅延オプションに関する詳細は、**7.3.3 送信遅延**を参照してください。

- **遮断**：条件に一致したメールは遮断します。(送信しません)。「送信者に遮断のお知らせ」オプションを選択した場合、送信者に遮断したことをお知らせするメールが配信されます。

- **通過**： 条件に一致したメールは通過します。特定メールに対してポリシー適用を除外する場合やモニタリングする場合に使用します。.

- **決裁（オプション）**： 条件に一致したメールは、決裁者の決裁が必要となり、承認されたメールがのみ送信されます。却下の場合には送信しません。

- **ルーティング**： 条件に一致したメールは指定されたメールサーバに転送します。

→ 添付の処理： 添付ファイルに対するセキュリティ機能を付加するために、メール処理とは別に添付ファイルに対する機能を提供します。
遮断を除いたメール処理機能(送信遅延、通過、 決裁（オプション）、ルーティング)と同時に適用して使用できます。
‘パスワードの直接指定’ はオプションを使用してポリシー別にパスワードを直接設定することができます。

- 原本の維持： 添付ファイルをそのまま維持します。
- 添付ファイルのリンク変換： フィルタリングされたメールの添付ファイルがサーバに保存された後、ダウンロードするリンクが作成され、該当メールに挿入されます。メール受信者は、挿入された特定 URL からのみ添付ファイルをダウンロードできます。添付ファイルのリンク変換オプションに関する詳細は **7.3.4 リンク変換**を参照してください。
- 添付ファイル暗号化：フィルタリングされたメールの添付ファイルをパスワード付き圧縮・暗号化します。添付ファイルの暗号化オプションに関しては、**7.3.2 添付ファイル暗号化**を参照してください。
- 添付ファイル暗号化後にリンク変換： 暗号化とリンク変換機能を合わせた機能です。フィルタリングされたンメールの添付ファイルがパスワード付き圧縮・暗号化した後にサーバへ保存、そのファイルをダウンロードするリンクが作成されて、メールに挿入されます。 メール受信者は特 URL から暗号化された添付ファイルをダウンロードすることができます。圧縮を解凍する時は、パスワードを使用する必要があります。
- パスワードの直接指定： 暗号化、 リンク変換、 暗号化後にリンク変換時に使用するパスワードをを直接指定します。
直接指定しない場合には、MAILSCREEN がランダムにパスワードを自動生成します。

注意

- ✖ ‘添付ファイル暗号化後にリンク変換’ オプションと ‘パスワードの直接指定’ を設定する場合、設定したパスワードは添付ファイルを圧縮・暗号化する時に使用されます。
リンク変換には設定したパスワードは使用しません。
- ✖ ‘添付ファイル暗号化後にリンク変換’ オプションを設定した場合、添付ファイル暗号化お知らせ（**7.3.2 添付ファイル暗号化**参照）が解除されている場合は暗号化後にリンク変換お知らせメールは送信されません。

→ ポリシーのお知らせ： メールがポリシーによってフィルタリング処理されたことをお知らせするメールです。お知らせメールの使用可否及び受信対象者を設定できます。

- BCC にポリシー適用のお知らせ： BCC として設定したユーザにポリシーお知らせメールを配信します。
- ポリシー参照者にポリシー適用のお知らせ：「選択」 ボタンをクリックすると、組織図リストがポップアップで表示されます。ポリシーお知らせの対象者を選択します。 所属に関係なく参照が可能であり、「削除」ボタンを使用して設定した対象を削除することができます。
- 直接入力： ポリシーお知らせの対象を直接入力します。 特定対象にお知らせメールを送信します。メールアドレス形式で入力してください。

→ お知らせ方法： ポリシーお知らせ方法を設定します。

- BCC： ポリシーが適用されたメールを BCC 形式でポリシーお知らせ対象に配信します。
- お知らせメールを送信： ポリシーが適用されたメールの件名と簡略な情報を含んでいるお知らせメールをポリシー適用お知らせ対象に配信します。ポリシーお知らせメールに対するテンプレートは**「環境設定>フィルタリング>誤送信防止>ポリシー適用のお知らせ」**を参考してください。
- 原文を添付： お知らせメールにメール原文を添付して配信します。

→ 適用時間： ポリシーを適用する時間を設定します。

- 曜日を適用： ポリシーが適用される曜日を設定します。
- 時間を適用： ポリシーが適用される時間を設定します。

→ 使用可否： ポリシーの使用可否を設定します。

→ 備考： 該当ポリシーの追加説明（コメント）を入力します。

3. 下の「登録」 ボタンをクリックすると、入力された情報がポリシーリストに追加されます。「取消」ボタンをクリックするとポリシーリスト表示画面に切り替わります。「リセット」 ボタンをクリックする場合は設定した情報が全て初期化され、再度入力画面に戻ります。

4.1.3. 許容宛先管理

送信先をを許容するメールアドレスとドメインのリストです。 ポリシー追加時にフィルタリング条件として活用できます。例えば、ポリシーを追加する時に許容宛先のみに対して添付ファイル暗号化をする、許容された受信者が含まれていない場合に、CCでお知らせをする、等の活用をすることができます。

使用方法

1. **「SMTP Filter>ポリシー>許容された受信者」**をクリックします。
2. 許容された受信者のリストが表示されます。
3. 下記に、リストの上にある項目名について説明します。

→ E メール: 許容された受信者のメールアドレスです。

→ 説明: 許容された受信者に関する説明です。

→ 日付: 許容された受信者が登録された日付です。

4. 下記に、許容された受信者リストの関連機能について説明します。

→ 検索: ‘E メール’ または ‘説明’ 項目の内容と一致するリストを検索します。 キーワードを入力した後、「検索」ボタンをクリックします。

→ ファイル保存: 検索されたリストをファイルとして保存します。

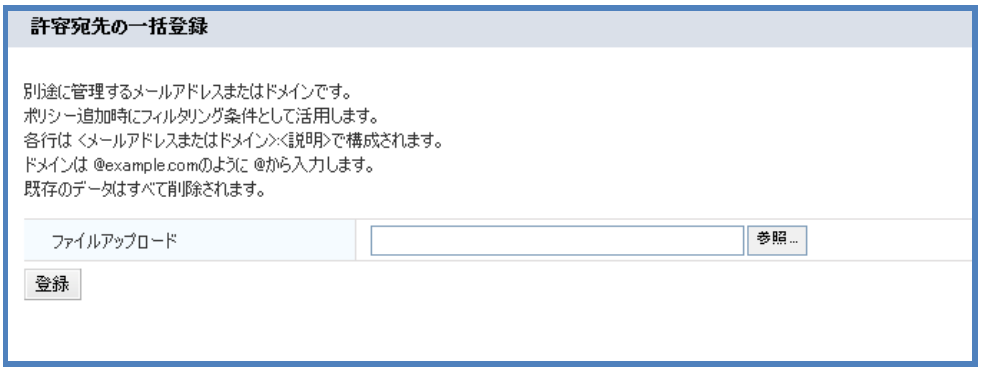
→ リスト数設定: 1 ページ当りに表示されるリストの表示数を設定します。

4.1.4. 許容宛先の一括登録

許容される受信者を一括登録します。 各行に <Eメール>(50文字以下):<説明> または <@ドメイン>(50文字以下):<説明>が記入された.txt ファイルをアップロードします。最大10万リストまで登録が可能です。

使用方法

1. **「SMTP Filter>ポリシー管理>許容宛先の一括登録」**をクリックします。
2. 許容宛先の一括登録画面が表示されます。
3. 「参照...」 ボタンをクリックして許容宛先を保存しておいたファイルを選択した後、「登録」 ボタンをクリックします。



注意

- ✖ 一括登録すると、既存データはすべて消去され、新しいデータのみ登録がされますので、ご注意ください。但し、新しく登録されるデータが 0 件の場合は、既存データは維持されます。

4.2. SMTP ポリシー

SMTPレベルのポリシーは、Black ListとWhite Listに区分されます。 Black Listは送信者のメールアドレスまたは送信サーバ IP 情報をチェックしてメール送信を拒否します。 White Listは Black Listとは逆に送信者のメールアドレスまたは送信サーバ IP 情報をチェックしてメール送信を許可します。

注意

- ✖ White List は Black List より優先適用されます。

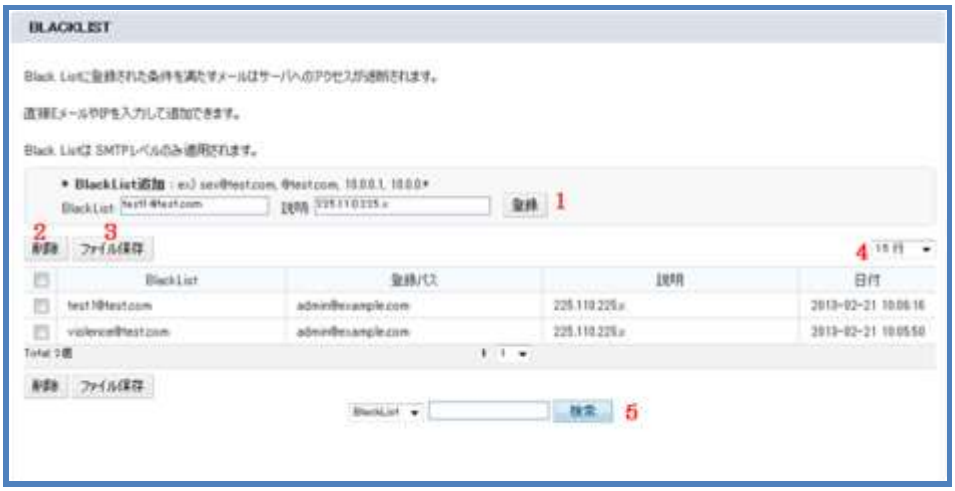
4.2.1. Black List 管理

使用方法

1. 「SMTP Filter>ポリシー管理>Black List」を選択します。
2. Black List ページが表示されます。
3. 下記に、Black List 情報の各項目について説明します。

→ Black List: Black List の IP やドメイン、またはメールアドレスです。
→ 登録パス: 登録者を示します。
→ 説明: Black List に関する説明です。
→ 日付: 登録日付です。

4. 下記に、Black List の関連機能について説明します。



→ 登録: Black List を追加します。Black List の IP かメールアドレスと説明を入力した後、「登録」ボタンをクリックします。

注意

- ✖ IP アドレスを入力する場合、ワイルドカード(‘*’ 文字)による IP アドレス指定が可能です。
- ✖ ワイルドカードは必ず ‘.’ の次に使用する必要があります。 ‘.’ の次でなく ‘10.0.1*’ のように設定した場合、メールアドレスとして認識されますので、ご注意ください。
- ✖ ワイルドカードを利用して IP を設定する場合、ワイルドカード右側の

文字は全部無視されます。 例えば、‘10.0.*’と‘10.0.*.100’ が同じデータとして扱われるので、ご注意ください。

✖ ‘10.0.*’を指定する場合、 IP アドレスの左側から検査しますので‘210.0.0.1’はフィルタリングされません。

→ 削除: 選択した Black Listを削除します。

→ ファイル保存: Black ListをExcelファイルとして保存します。

→ リスト数設定: 1ページ当り表示されるBlack Listの表示数を設定します。

→ 検索: 検索条件(Black List、 登録パス、 説明)を選択した後、キーワードを入力します。「検索」ボタンをクリックすると検索した情報がページに表示されます。

4.2.2. White List 管理

White Listの登録、削除、ファイル保存、検索機能はBlack List管理と同様の使用方法なので、 **4.2.1 Black List管理**を参照してください。

5. メール管理

MAILSCREENは処理したメールの監査記録(ログ)とメールの原本の保存機能を提供しています。

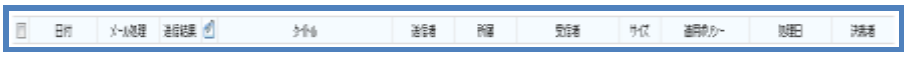
5.1. メール管理

5.1.1. メール履歴

送信メールの監査記録(ログ)を表示します。

使用方法

1. 「SMTP Filter>メール>メール」を選択します。
2. メール履歴リストが表示されます。
3. 下記に、メール履歴リストに表示される各項目について説明します。



→ 日付: メールが送信された日付です。

→ メール処理: 送信遅延、通過、遮断、決裁(待機)、決裁(承認)、決裁(却下)、などのメール処理状態を示します。

→ 送信結果: メール送信結果が表示されます。(成功、失敗、送信中)

→ : 添付ファイル有無を示すアイコンです。 マウスカーソルを乗せるとTooltip で添付ファイルリストが表示されます。ファイルが添付されていないメールは 項目が空白になります。

→ タイトル: メールの件名です。

→ 送信者: 送信者の名前とメールアドレスです。

→ 所属: 送信者の所属です。

→ 受信者: 受信者の名前とメールアドレスです。

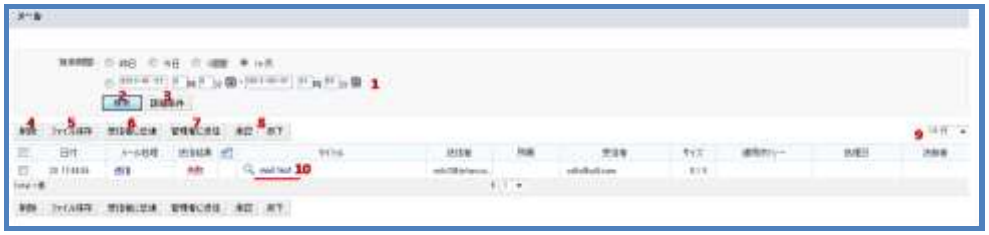
→ サイズ: メールの全体サイズです。

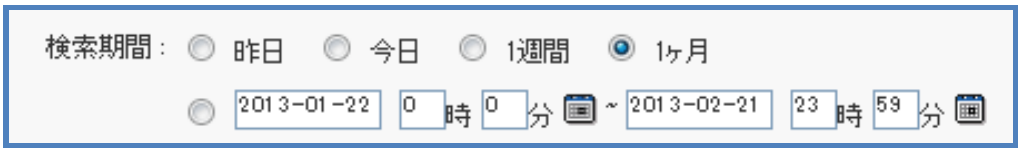
→ 適用ポリシー: メールに適用されたポリシーの名前です。

→ 処理日: 決裁メールの場合、決裁処理された日付が表示されます。

→ 決裁者: 決裁者の名前とメールアドレスです。

4. 下記に、メール履歴リストの上下にある関連機能について説明します。





- 昨日：前日の 00 時 00 分から 23 時 59 分 59 秒まで送信されたメールを検索します。
- 今日：今日の 00 時 00 分から現時点まで送信されたメールを検索します。
- 1 週間：現在日付を基準で 1 週間に送信されたメールを検索します。
- 1 ヶ月：現在日付を基準で 1 ヶ月間に送信されたメールを検索します。
- 詳細期間：検索時間を更に詳細に設定します。

注意

✖ 検索期間にて、検索開始日が終了日より、後の日付になってはいけません。

✖ 検索期間は、年-月-日の形式で入力してください。 年は 4 桁、月は 1～12、 日は 1～31、 時は 0～23、分は 0～59 の範囲です。

→ 1. 検索期間：検索期間を設定します。

→ 2. 検索：「検索」ボタンをクリックすると、検索期間と詳細条件に合うメールを検索します。

→ 3. 詳細条件：検索のための詳細条件を設定します。「詳細条件」ボタンをクリックすると、その下に詳細条件を設定する入力欄が表示されます。

- メール処理： 送信、通過、遮断、送信遅延などメールが処理された状態を条件として設定します。
- 添付の処理：メールの添付ファイルが処理された方式(原本維持、 暗号化、リンク変換、 暗号化後リンク変換)を検索条件として設定します。
- 決裁者：メールを決裁した決裁者を検索条件として設定します。 直接入力するか、「選択」ボタンをクリックして組織図リストから選択します。(決裁オプションが有効の場合に表示)
- メール処理：メール状態で「決裁」を選択した場合、有効化されます。承認、待機、 却下の中から選択します。(決裁オプションが有効の場合に表示)
- ドメイン：送信者のメールアドレスのドメインを検索条件として設定します。例えば、ドメインを a.com に設定して、送信者メールアドレスを user@b.com に設定した場合は検索されないのでご注意ください。
- ポリシー名：メールに適用されたポリシーを検索条件として設定します。
- 送信者 IP：送信者の IP アドレスを検索条件として設定します。
- 送信者 E メール：送信者メールアドレスを検索条件として設定します。
- 所属：送信者の所属を検索条件として設定します。
- 受信者 E メール：受信者のメールアドレスを検索条件として設定します。
- タイトル：メールの件名を検索条件として設定します。
- ウィルス名：ウィルスメールの場合、ウィルス名を検索条件として設定します。
- 添付ファイル名：添付ファイル名を検索条件として設定します。
- 送信結果：送信結果を検索条件として設定します。

注意

- ✖ 大量のメールを検索する場合には、検索条件を詳しく指定するほど検索効率が高まり、検索スピードが向上します。しかし、いくつかの条件(ポリシー名、 送信者 IP、 送信者、 送信者 E メール、 所属、 受信者 E メール、 件名、 ウィルス名、 添付ファイル名)の場合検索スピードに影響を与える場合があります。
- ✖ 一部の条件 (ポリシー名、送信者 IP、送信者、 送信者 E メール、 所属、 受信者 E メール、 件名、 ウィルス名、 添付ファイル名)は値の一部のみ入力しても検索が可能です。例えば ‘あ’ だけ入力しても ‘あいうえお’ が検索されます.

→ 4. 削除: 選択したメール履歴を削除します。

→ 5. ファイル保存: メール履歴をExcelファイルとして保存します。

→ 6. 受信者に伝達: 選択したメールを受信者に再送信します。 受信者に再送信するためには選択したメールの原本がサーバに保存されていなければなりません。メールの原本がサーバに保存されている場合、メール件名の前に  が表示されています。

→ 7. 管理者に送信: 選択したメールを現在ログインしている管理者に再送信します。 管理者に再送信するためには、上記の「6.」機能と同様にメールの原本がサーバに保存されていなければなりません。

→ 8. 承認/却下: 決裁要請メールを承認/反却できます。決裁要請メールを選択した後、「承認」ボタンまたは「却下」 ボタンをクリックします。

→ 9. リスト数の設定: 1ページ当りに表示されるメール履歴リストの表示数を設定します。

→ 10. メール件名: メールの原本がサーバに保存されている(メール件名の前に  表示) メール件名をクリックすると、該当のメールの原本の詳細内容を確認できます。

- 「原本ダウンロード」: メールの原本を PC にダウンロードします。
- 「クローズ」: メール詳細表示ページを終了します。
- 「受信者に伝達」: 受信者の E メールアドレスに再送信します。
- 「管理者に送信」: 現在ログインしている管理者のメールアドレスに再送信します。
- ヘッダ: メールのヘッダ情報です。
- 原本: メールのヘッダを含めた原文がそのまま表示されます。この時 MIME デコーディングはされません。

注意

✖ メールにファイルが添付されている場合、表示される内容が多くなる可能性があり、Web ブラウザに負荷が掛かる恐れがあります。これを防止するためには、**「環境設定>システム>基本情報>画面設定>メール確認>サイズ制限」**にて制限するサイズを設定してください。

- 内容: メールのヘッダ以外の内容が表示されます。メールの MIME が multipart/alternative の場合、text/html に該当する部分のみ HTML 形式で力されます。
- 送信結果: 受信者に送信した結果を確認できます。

5.1.2. 添付履歴

メールに添付された添付ファイルのダウンロード履歴(ログ)を表示します。

使用方法

1.「SMTP Filter>メール>添付」を選択します。

2. 添付履歴リストが表示されます。

3. 下記に、メール履歴リストの上下にある各機能について説明します。

→ 日付: メールが送信された日付です。

→ メール処理: 決裁(待機)、決裁(承認)、決裁(却下)、送信、通過、遮断などのメールが処理された状態を示します。

→ 添付ファイル名: 添付ファイルの名前です。

→ 添付サイズ: 添付ファイルのサイズです。

→ タイトル: メールの件名です。

→ 送信者: 送信者の名前とメールアドレスです。

→ 受信者: 受信者の名前とメールアドレスです。

→ 適用ポリシー: ポリシーが適用されているメールの場合、ポリシー名が表示されます。

4. 下記に、添付履歴リストの上下にある関連機能について説明します。

→ 1. 検索期間: 検索範囲の期間を入力します。検索期間の各項目に関する説明は **5.1.1.メール**を参照してください。

→ 2. 詳細条件: 検索のための詳細条件を設定します。「詳細条件」ボタンをクリックすると、その下に詳細条件を設定する入力欄が表示されます。

- 添付ファイル名: 添付ファイル名を検索条件として設定します。
- 拡張子: 添付ファイルの拡張子を検索条件として設定します。
- 添付のサイズ: 添付ファイルのサイズを検索条件として設定します。
- メール状態: 添付ファイル暗号化、送信、送信遅延などメールが処理された状態を検索条件として設定します。
- メール処理: メール状態が決裁の場合、この項目が有効化されます。(決裁オプションが有効の場合に表示))
- ポリシー名: 適用されたポリシーの名前を検索条件として設定します。
- 送信者 IP: 送信者の IP アドレスを検索条件として設定します。
- 送信者 E メール: 送信者のメールアドレスを検索条件として設定します。

- 受信者 E メール：受信者のメールアドレスを検索条件として設定します。
- タイトル：メールの件名を検索条件として設定します。

→ 3. 検索：「検索」ボタンをクリックすると、検索期間と詳細条件に合うメールを検索します。

→ 4. ファイル保存：添付履歴をExcelファイルとして保存します。

→ 5. リスト数設定：1ページ当りに表示されるリストの表示数を設定します。

→ 6. 添付ファイル名：添付ファイル名をクリックすると、該当添付ファイルをダウンロードできます。

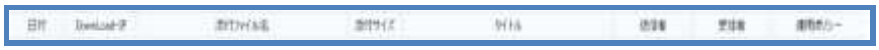
→ 7. タイトル：メールの原本がサーバに保存されている場合は、メール件名の前に が表示されています。メールの件名をクリックすると該当メールの原本が確認できます。原本メールの詳細確認に関しては、**5.1.1メール**を参照してください。

5.1.3. リンク履歴

リンク変換された添付ファイルのダウンロード履歴（ログ）を表示します。

使用方法

1. 「**SMTP Filter>メール>リンク履歴**」を選択します。
2. リンク履歴リストが表示されます。
3. 下記に、リンク履歴リストページに表示されるリストの各項目について説明します。



→ 日付：添付ファイルをダウンロードした日付です。

→ DownLoad-IP：添付ファイルをダウンロードした PC の IP です。

→ 添付ファイル名：ダウンロードされた添付ファイル名です。

→ 添付サイズ：添付ファイルのサイズです。

→ タイトル：メールの件名です。

→ 送信者：送信者の名前とメールアドレスです。

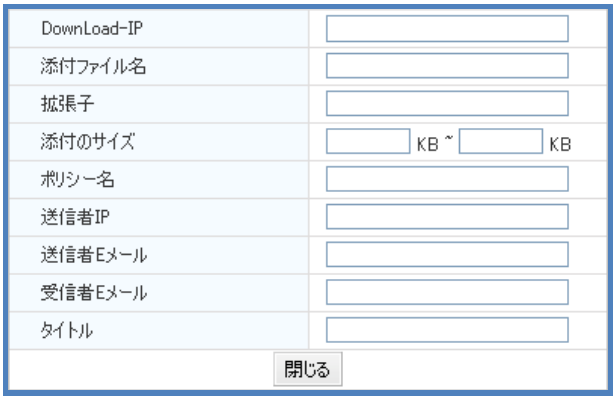
→ 受信者：受信者の名前とメールアドレスです。

→ 適用ポリシー：適用されたポリシー名が表示されます。

4. 下記に、リンク履歴リストの上下にある関連機能について説明します。

→ 1. 検索期間： 検索範囲の期間を設定します。検索期間項目に関する説明は **5.1.1 メール履歴**を参照してください。

→ 2. 詳細条件： 検索のための詳細条件を設定します。**「詳細条件」**ボタンをクリックすると、その下に詳細な検索条件を設定する入力欄が表示されます。



- DownLoad-IP： 添付ファイルをダウンロードした IP を検索条件として設定します。
- 添付ファイル名： 添付ファイルの名前を検索条件として設定します。
- 拡張子： 添付ファイルの拡張子を検索条件として設定します。
- 添付ファイルサイズ： 添付ファイルのサイズを検索条件として設定します。
- ポリシー名： 適用されたポリシーの名前を検索条件として設定します。
- 送信者 IP： 送信者の IP アドレスを検索条件として設定します。
- 送信者 E メール： 送信者 E メールを検索条件として設定します。
- 受信者 E メール： 受信者 E メールを検索条件として設定します。
- タイトル： メール件名を検索条件として設定します。

→ 3. 検索：「検索」ボタンをクリックすると、検索期間と詳細条件に合うメールを検索します。

→ 4. ファイル保存： リンク履歴をExcelファイルとして保存します。

→ 5. リスト数設定： 1ページ当りに表示されるメール履歴リストの表示数を設定します。

→ 6. 添付ファイル名： 添付ファイルをダウンロードするには、添付ファイル名をクリックします。

→ 7. タイトル： メールの原本がサーバに保存されている場合、メール件名の前に  が表示されています。メールの件名をクリックすると該当メールの原本が確認できます。メールの原本の詳細確認に関しては、**5.1.1メール**を参照してください。

5.1.4. 拒否履歴

SMTPレベルで拒否されたメールの履歴(ログ)を表示します。

注意

✖ メール拒否履歴の中で送信者と受信者欄は空白になっている場合があります。これは該当情報を得る前にメールが拒否されたか、その情報を提供しない事から拒否された場合です。

使用方法

1. 「SMTP Filter>メール>メール拒否」を選択します。
2. メール拒否履歴リストが表示されます。
3. 下記に、メール拒否リストページに表示されるリストの各項目について説明します。

→ 日付: メールが送信された日付です。

→ 送信者 IP: 送信者 IP です。

→ 送信者: 送信者の E メールアドレスです。

→ 受信者: 受信者の E メールアドレスです。

→ 拒否コード: 拒否された事由を示すコード番号です。

コード	説明
100	指定された E メール制限サイズを超過
101	送信者 E メールドメインに DNS MX が存在しない
102	受信者 E メールに転送が許可されていない
103	*1) Black List に登録された送信者
104	*2)不審なユーザに登録された受信者
105	MAIL FROM コマンドに入力された値がない
106	RCPT TO コマンド利用回数制限値を超過
108	*3) 誤った文字が含まれた E メール
111	同一送受信者の E メール
112	存在しない受信者 E メール
113	SMTP 通信時間を超過
114	送信者メールアドレス形式の間違い
115	受信者メールアドレス形式の間違い
119	送信者 IP に Reverse DNS が存在しない。
120	認証(AUTH LOGIN/PLAIN) 失敗
121	最大 Hop 数超過

*1 Black List によって拒否された場合です。

*2 特定受信者への受信遮断によって拒否される場合です。 送信者を対象で検査する Black List とは少々異なります。

*3 メールアドレスに空白やTab文字が含まれている場合です。

→ 拒否理由：メール受信が拒否された理由です。

4. 下記に、メール拒否履歴リストの上下にある各機能について説明します。

→ 1. 検索期間：検索範囲の期間を設定します。検索期間項目に関する説明は **5.1.1 メール履歴**を参照してください。

→ 2. 詳細条件：検索のための詳細条件を設定します。**「詳細条件」**ボタンをクリックすると、その下に詳細な検索条件を設定する入力欄が表示されます。

- 送信者 IP：送信者 IP を検索条件として設定します。
- 送信者 E メール：送信者メールアドレスを検索条件として設定します。
- 受信者 E メール：受信者メールアドレスを検索条件として設定します。
- 拒否理由コード：拒否理由コードを検索条件として設定します。

注意

✖ 詳細条件を利用して検索する時、拒否理由コード以外の全ての条件は、一部の文字のみ入力しても検索ができます。

✖ 拒否理由コードは 3 桁で正確に入力してください。

✖ 検索期間と拒否理由コードを使用する事で検索スピードを向上できます。

→ 検索：「検索」ボタンをクリックすると検索期間と詳細条件に合うメールが検索されます。

→ ファイル保存：拒否履歴をExcelファイルとして保存します。

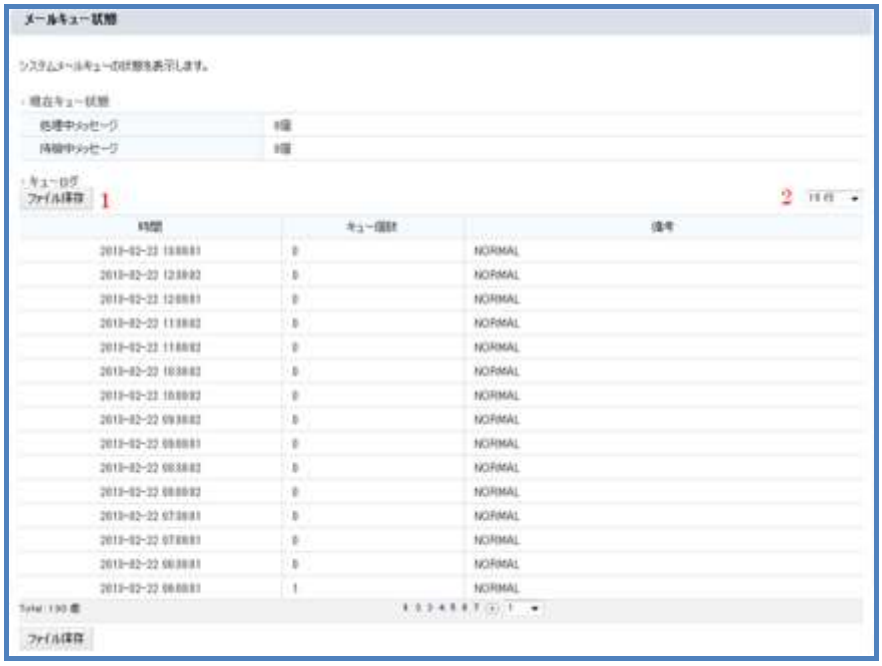
→ リスト数設定：1ページ当りに表示されるリストの表示数を設定します

5.1.5. メールキュー状態

MAILSCREENから正常メールとして判断されたメールは、転送先のメールサーバに送信されます。 しかし、ネットワーク状況により即時に処理できない時、MAILSCREENはメールをキューに保存し、後で送信を行います。
メールキューの状態を表示します。

使用方法

1. 「**SMTP Filter>メール>メールキュー状態**」を選択します。
2. メールキュー状態のリストが表示されます。 各項目に関して説明します。



→ 現在キュー状態: 現在キューの状態です。

- 処理中メッセージ: キューで処理中の全体メールの数です。
- 待機中メッセージ: メールサーバから応答がない場合、蓄積されているメール数を示します。システム使用率 100%、またはシステムダウン、DNS クエリ情報を読み取れなかった場合にキューが蓄積されるようになります。

→ キューログ: キューに関するログです。

- 時間: キュー状態を検査した時間です。
- キュー個数: 未処理中のキュー数です。
- 備考: 「備考」には、 NORMAL または WARNING が表示されます。 WARNING は**「環境設定>システム>基本情報>システム監視」**に設定された‘メールキュー個数’より、未処理中のメールキュー個数が多い場合に表示され、メール処理が遅延されている状態ですので、原因を把握し、解決する必要があります。オプションに関する詳細説明は **7.1.1 基本情報**の「システム監視」を参照してください。
- 1. ファイル保存: キューログを Excel ファイルとして保存します。
- 2. ページ数設定: 1 ページ当りに表示されるキューログ数を設定します。

6. ウィルス管理

ウィルスメールを探知して駆除する機能を提供しています。ウィルス探知のワクチンエンジンの他に、専任のウィルス担当チームが新しく発生したウィルスを探知し、そのパターンを分析した上、ワクチンパターンの配布を行うまでの間、ウィルスメールを遮断するVPS機能を提供します。

6.1. ウィルス

6.1.1. ウィルス検査設定

ウィルス検査に関する各種情報を設定します。

使用方法

1. **「ウィルス管理>ウィルス検査設定」**を選択します。
2. ウィルス検査設定ページが表示されます。 下記に、各項目について説明します。

→ ワクチン: ウィルスを検査するワクチンエンジンの種類を選択します。 使用可能なワクチンは、設置時の環境及び設定により、上記のページ内容と異なる場合があります。

→ 感染メール処理: 感染されたメールを処理する方法を選択します。'駆除後仮保管' を推奨します。('駆除後送信' を選択した場合は、ウイルスを駆除した後の状態で送信されるためです。)

→ 最終アップデート時間: 最終ワクチンアップデート時刻です。

→ 「リアルタイムアップデート」: ワクチンは毎回定時にアップデートされますが、このボタンをクリックする事で、リアルタイムアップデートを即時に行います。

注意

✖ リアルタイムアップデート時に、ワクチンエンジンが大量のデータをサーバから読み込むため、時間が掛かる場合があります。

3. 「設定」 ボタンをクリックします。

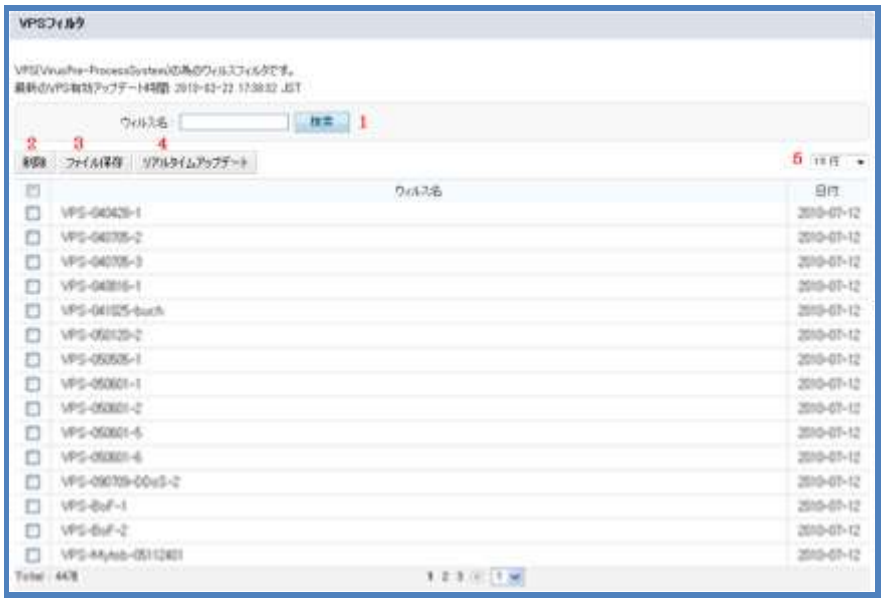
6.2. VPS

6.2.1. VPS フィルタ設定

VPSに関する各種情報を設定します。

使用方法

1. **「ウィルス管理>VPS フィルタ」**を選択します。
2. VPS フィルタ管理画面が表示されます。下記に、各機能について説明します。



→ 検索： VPS フィルタを検索します。 ウィルス名を入力した後、「検索」ボタンをクリックします。 検索された VPS フィルタ情報が画面に表示されます。

→ 削除： 選択した VPS フィルタを削除します。

→ ファイル保存： VPS フィルタリストを Excel ファイルとして保存します。

→ リアルタイムアップデート： VPS フィルタをリアルタイムでアップデートします。

→ リスト数設定： 1 ページ当りに表示されるリストの表示数を設定します。

7. 環境設定

7.1. システム情報

システム運用のための様々な設定機能を提供します。

7.1.1. 基本情報

システム情報と画面構成、ジャーナリング、言語など基本情報を設定します。

使用方法

1. **「環境設定>システム>基本情報」**を選択します。
2. 基本情報設定ページが表示されます。 各項目を設定した後、下の「設定」ボタンをクリックします。

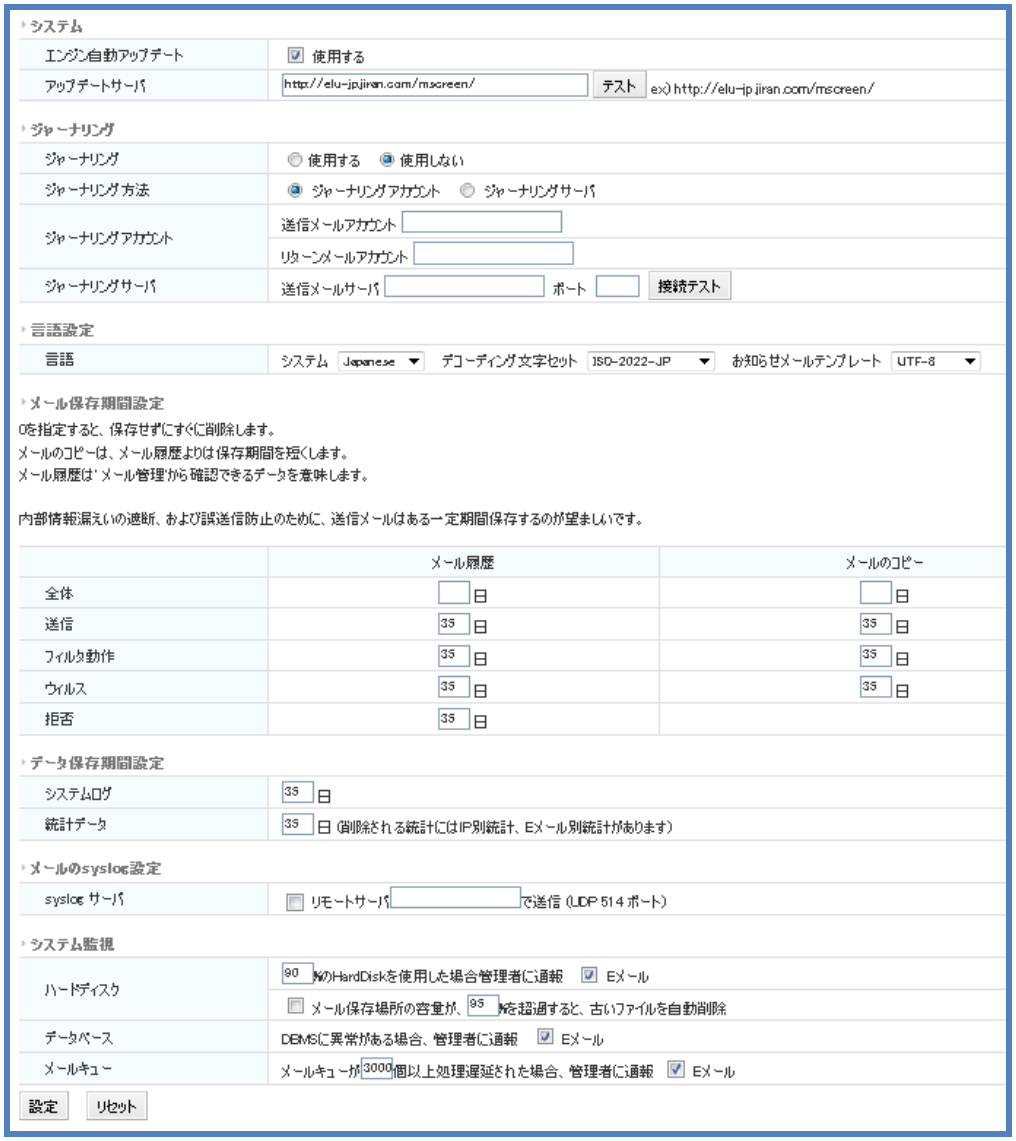
→ システム情報

- ホスト名： MAILSCREEN のホスト名を設定します。 ホスト名は FQDN 名（A.HOST.COM の形式）で入力する必要があります。この情報は MAILSCREEN 内部作業時に参照されます。このホスト名は MAILSCREEN ライセンスサーバに登録されていますので任意で変更する場合、ライセンスの読み込みと更新が動作しなくなります。
- ライセンス： パッケージに設定されているライセンスです。 ライセンスが登録されたら、製品が納品された方式/満了日/ドメイン数/ユーザ数を確認できます。
  - ✓ ダウンロード： ボタンをクリックすると、ライセンスサーバに登録されているライセンスを読み込みます。 メンテナンス契約が更新されたか、ドメイン数、 ユーザ数追加などでライセンスが更新された場合に使用します。
  - ✓ 更新リクエスト： ボタンをクリックすると、ライセンスサーバにライセンス更新リクエストを行います。
- システムメール： 送信者名及び送信者メールアドレスを設定します。 この情報は MAILSCREEN からユーザにメール（例：お知らせメールなど）が送信される時の送信者情報として使われます。

→ 画面設定： 下記に、基本画面について設定します。

- ブラウザタイトル：Web ブラウザのタイトルバーに表示される内容を設定します。
- メール確認：メール詳細確認機能に関して設定します。
  - ✓ 基本値：メール詳細確認で表示される範囲を設定します。
  - ✓ サイズ制限：メールの原文を最大何 Kbytes まで表示するかを設定します。「基本値」で「原文」を選択した場合に設定する項目であり、サイズ制限を行わない場合は、'0' に設定してください。
- ロゴの設定：Web-Admin ページに表示されるロゴを、ファイル種類 '.png' で設定します。'ユーザが設定したロゴを使用' のチェックをして「参照」ボタンで画像をアップロードします。
- モバイルロゴ：スマートフォンでの Web-Admin ページに表示されるロゴを、ファイル種類 '.png' で設定します。'ユーザが設定したモバイルロゴを使用' のチェックをして「参照」ボタンで画像をアップロードします。
- イメージリンク：Web-Admin の左上の画像をクリックした時に接続されるリンク情報を設定します。
- 時間形式： 時刻の表示形式を設定します。 Web-Admin は画面によって多くの情報が表示されるため、多様な時間表示形式を使用しています。

- 検索時間：**「SMTP Filter>メール>メール」**または**「SMTP Filter>メール>メール拒否」**を選択し、送信メールと送信拒否メールの最新ログ表示の時間を設定します。設定されている時間（分）の最新メールログをログ検索画面に表示します。
- 検索方法：検索時に作業制限時間と検索結果表示方法について設定します。
  - ✓ 検索制限時間：検索作業が制限時間内に終了しない場合に強制強制終了される時間を設定します。
  - ✓ 検索結果の出力：検索結果を日付順にソートします。
- リモートサポート URL：Web-Admin 右上にある Remote Support にリンクされる URL を設定します。（現在、MAILSCREEN では本機能はサポートしておりません。）
- Copyright：著作権関連表示を設定します。



→ システム：エンジン自動アップデートを設定します。

- エンジン自動アップデート：MAILSCREEN パッケージを自動アップデートします。 アップデート履歴は**「環境設定>維持保守>エンジン自動アップデート」**で確認できます。

注意

✖ 個別カスタマイズ要求によって MAILSCREEN パッケージをカスタマイズする場合は、「エンジン自動アップデート」は、必ずチェックを解除してください。チェックを入れると、自動アップデート時に個別カスタマイズで変更した履歴が消去される場合があります。

- アップデートサーバ：アップデートサーバ情報を入力します。（デフォルトの URL は変更しないでください）「テスト」 ボタンをクリックすると、該当サーバとの接続有無を確認できます。

→ ジャーナリング：シャーナリング機能を使用する事で、別メールアーカイブソリューション製品と連携できます。

- ジャーナリング：使用可否を設定します。
- ジャーナリング方法：アカウントを使用するジャーナリング方法とサーバを使用するジャーナリング方法があります。 選択によって下の「ジャーナリングアカウント」または「ジャーナリングサーバ」に必要な情報を設定します。
- ジャーナリングアカウント：ジャーナリングのためのアカウント情報を入力します。 一件のメールに複数の受信者がいる場合は一件のメールのみジャーナリングされます。 送信メールアドレスと返送メールアドレスを入力します。
- ジャーナリングサーバ：ジャーナリングのためのサーバ情報を入力します。一件のメールに複数の受信者がいる場合は、送・受信者の Envelop 情報(Envelop MAIL FROM、 RCPT TO)がそのまま使用されますので、受信者数分にジャーナリングされます。 サーバアドレスとポート番号を設定してください。

注意

✖ ジャーナリングサーバに問題が起こり、ジャーナリングメール送信が連続的に失敗、キュー保存時間が超過する場合、送信者にメールが返送されます。ジャーナリングサーバに問題が起こらないように、ご注意ください。

→ 言語設定：システムで使用する言語を設定します。

- システム：Web-Admin で使用、表示する基本言語を設定します。
- デコーディング文字セット：フィルタリング・エンジンがメールを解析する時、メール内容に文字セット情報がない場合に強制的に指定する文字セットです。文字セット情報がないメールの実際の文字セットと、この情報が一致しないと、 メール分析に失敗する場合がありますので、ご注意ください。
- お知らせメールテンプレート：ポリシー適用お知らせメールに適用される文字セットを設定します。

→ メール保存期間設定：メールのコピーとメールログをサーバに保存する期間を設定します。

- 全体：全体(送信、フィルタ動作、ウィルス、拒否)の項目に適用します。

- 送信：送信されたメールの中で、ポリシーにより通過、受信完了したメールに対して、メールログとメールコピーの保存期間を設定します。
- フィルタ動作：ポリシーが適用されたメールに対して、メールログとメールコピーの保存期間を設定します。
- ウィルス：ウィルスに感染されたメールに対して、メールログとメールコピーの保存期間を設定します。
- 拒否：送信拒否されたメールに対して、メールログとメールコピーの保存期間を設定します。

注意

- ✖ メールコピーの保存期間は、メールのログ保存期間より小さい日数か、同じ日数に設定する必要があります。
- ✖ 「フィルタ動作」とは、社内の重要情報が外部に漏洩される事を防止するためにポリシーが適用されたメールのことです。フィルタ動作メールログとメールコピーの保存期間は「環境設定>フィルタリング>誤送信防止>添付ファイルのリンク変換」の ‘リンク有効期間’ より小さい日数を設定する事はできません。
- ✖ メール流量によって、多くの保存領域が必要になります。メールのサイズを平均 500Kbytes とすると、下記の方式で一日の必要な保存領域を計算できます。

  (500 ＊ <一日に送信されるメール数>) / 1024 / 1024

→ データ保存期間設定：システムログと統計データの保存期間を設定します。「システムログ」とは、MAILSCREEN で動作する各種プログラムが記録するログのことです。「統計データ」とは、メールの IP、ポリシー、受信者、送信者などの統計を指します。統計データは設定されたデータ保存期間情報を使用して周期的に古いデータは削除されます。

→ メールの syslog 設定：他に Syslog サーバが稼働している場合、MAILSCREEN のメールログを転送することができます。「リモートサーバ」にチェックを入れ、サーバ情報を入力します。

注意

- ✖ もし、リモートサーバの syslogd デーモンの実行やネットワーク接続に異常があって送信に失敗したとしても、MAILSCREEN 内の /var/log/maillog に、メールログは残ります。

→ システム監視：MAILSCREEN の稼働状況をモニタリングし、もし、システムに問題が発生した場合は管理者宛にメールで通知します。

- ハードディスク：設定した閾値を超えた場合、お知らせ機能が動作します。保存領域が足りないと、メールログとメールのコピー保存が円滑に行われないので、常にこの機能を使用する事を推奨します。
- データベース：データベースのテーブルサイズが異常に増加、テーブル損傷があった場合、このお知らせ機能が動作します。

- メールキュー: メールキューに指定した個数以上のメールが待機された場合、このお知らせ機能が動作します。 メールキュー状態は「SMTP Filter>メール>メールキュー状態」で確認ができます。

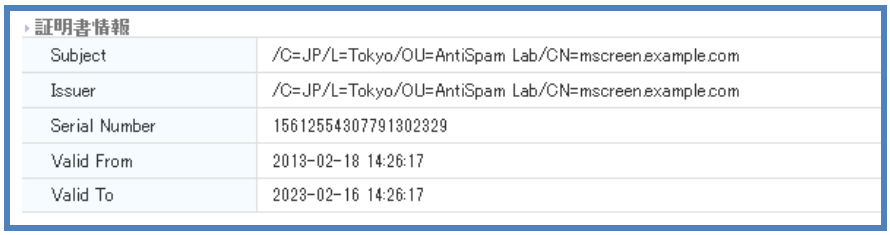
7.1.2. 証明書情報

本証明書は、 Web-Admin に接続時 HTTPS プロトコルを使用するWebブラウザとの通信のために使われます。 MAILSCREENは、独自証明書機能を提供します。
また、第三者機関発行のサーバ証明書もサポートします。

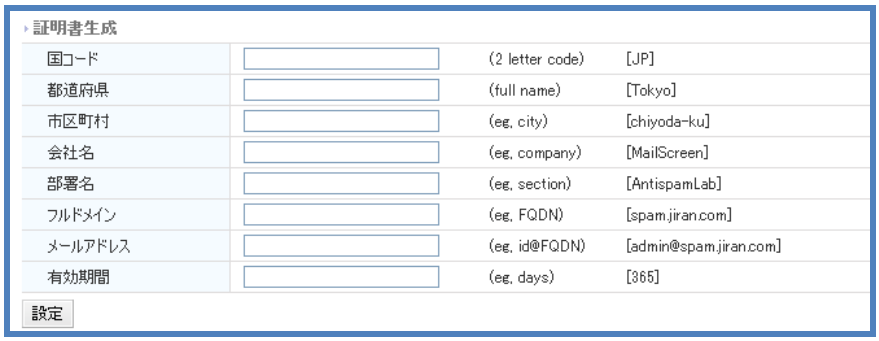
使用方法

1. 「環境設定>システム>証明書」を選択します。
2. 証明書設定ページが表示されます。 下記に、各項目について説明します。

   証明書情報: 証明書情報が Subject(主体)、Issuer(発行者)、 Serial Number(一連番号)、 Valid From(有効時間の始め)、 Valid To(有効期間満了) で表示されます。



→ 証明書生成: 自体証明書が生成されます。 次の各項目を入力した後、「設定」ボタンをクリックします。



- 国コード: 2 文字で構成されている ISO 形式の国コードを入力します。
- 都道府県: 会社の住所の中で都道府県に当たる部分を入力します。
- 市区町村: 会社の住所の中で市区町村に当たる部分を入力します。
- 会社名: 「フルドメイン」を所有した会社の名前を入力します。
- 部署名: 部署名を入力します。
- フルドメイン: サーバの DNS 確認に使われる FQDN を入力します。
  IP アドレスとポート情報は入力できません。
- メールアドレス:管理者のメールアドレスを入力します。
- 有効期間: 証明書の有効期間を入力します。 入力制限値は 1825 です。

注意

✖ MAILSCREEN が提供する独自証明書はセキュリティ上問題はありませんが、パブリック証明書ではないので、Web ブラウザでは '安全では

ない証明書’という警告が表示される場合があります。

→ 証明書ダウンロード: サーバに保存されている証明書をダウンロードします。 証明書の作成の為にファイルを認証機関に送るか、サーバの再設置のために証明書をバックアップする場合に使用します。ダウンロードする項目の「ファイル保存」ボタンをクリックします。

→ 証明書アップロード: ローカルにある証明書をアップロードします。 認証機関で認証を受けた証明書または既に使われている証明書をサーバに保存する場合に使用します。証明書と個人キーはセットで構成されていますので、一緒にアップロードしてください。

7.1.3. アクセス制御情報

Web-Admin ログイン方法とアクセス制御を設定します。

使用方法

1. **「環境設定>システム>アクセス制御」**を選択します。
2. アクセス制御設定ページが表示されます。 各項目を設定した後、下の「設定」ボタンをクリックします。

→ ユーザログイン: パスワード複雑度検査とパスワードの長さなど、ログイン関連オプションを設定します。

- パスワード複雑度検査: ‘使用する‘にすると、パスワードが英語大・小文字、 特殊文字または数字をそれぞれ 1 文字以上ずつ含む組み合わせで構成されているかどうかを検査します。‘使用しない‘にすると、検査はしません。
- パスワード最小長さ: パスワードの最小の長さを設定します。

- パスワード変更強制化: パスワード変更強制化を '使用する 'にすると、有効期間が過ぎたパスワードは、パスワードを変更する必要があります。
- パスワード有効期間: ユーザのパスワードの有効期間を設定します。 有効期間が過ぎたユーザがログインすると、パスワード変更ページに移動します。
- アカウントロック: 設定されたログイン失敗回数を超過するとアカウントがロックされます。
- アカウントロックの時間: アカウントがロックされる時間を設定します。 最小 1、 最大 99 まで入力できます。

→ ログイン情報: ログイン時に使用する識別情報を設定します。

- ログイン方法: '登録されたユーザ' と 'LDAP'、'POP3' の中で1つ選択します。
  - ✓ 登録されたユーザ: MAILSCREEN サーバに登録された ID とパスワードを認証情報として使用します。
  - ✓ 'POP3' サーバ: POP3 サーバに登録されたユーザアカウントとパスワードを認証情報として使用します。 POP3 サーバ情報は**「環境設定>メールサーバ>メールサーバ」**で設定します。
  - ✓ LDAP: サーバ情報に登録されている LDAP サーバに登録されたユーザアカウントとパスワードを認証情報として使用します。

注意

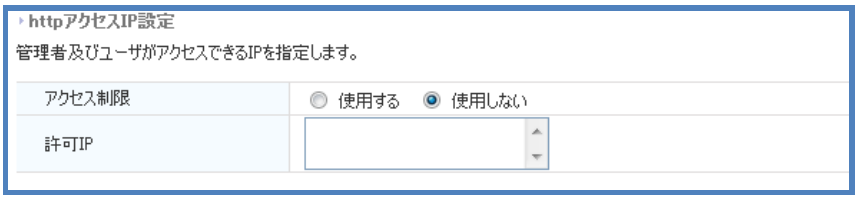
- ✖ スーパー管理者は 'POP3'、'LDAP' ログイン方法から除外されるので、 ID と Password でログインする必要があります。
- ✖ 'LDAP' または 'POP3' アカウントでログインする場合、MAILSCREEN サーバに登録されているユーザの ID と比べて権限を与えます。

- 検査値: ログイン時に認証情報を Email-ID(例: test)のみ使用するか、ドメイン情報を含めた Full Email Address(例: test@test.com)を使用するか設定します。
- テスト: 設定内容でログインができるか、あらかじめテストできます。 メールアドレスとパスワードを入力して「接続テスト」ボタンをクリックします。

→ サーバ情報: 上のログイン情報項目でログイン方法を 'LDAP' に設定した場合 、LDAP サーバ情報を入力する必要があります。

- LDAP: LDAP サーバとポート、暗号化接続可否、Bind DN、 Bind パスワード、 Base DN の値を入力します。 '暗号化接続' を設定すると LDAP サーバとの通信は SSL 通信を利用するようになります。

→ HTTP アクセス IP 設定: HTTP を利用して Web-Admin にアクセスする IP を制限します。



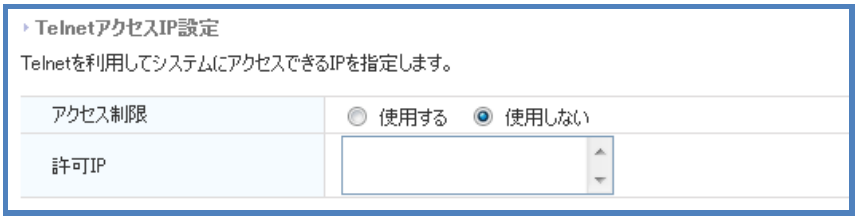
- アクセス制限: アクセス制限機能の使用、不使用を設定します。

許可 IP: 許可 IP リストは「アクセス制限」を「使用する」に設定した場合に設定します。IP アドレスは1行に1つずつ入力する必要があり、クラス単位も許可されます。 クラス単位で入力する場合、 IP アドレスは "."で終わる必要があります。 例えば、'10.0.0.' を入力すると'10.0.0.1' から '10.0.0.255' までの値で認識されます。但し、 IP 範囲での入力方式は提供しません。

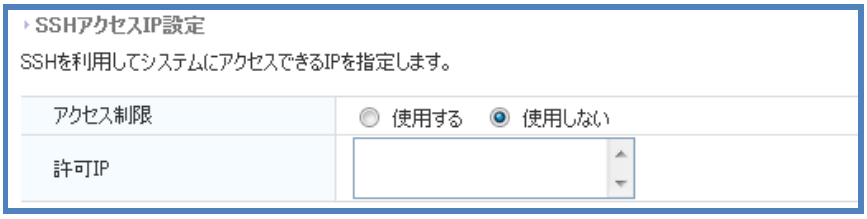
注意

✖ アクセス制限を使用すると、現在接続したスーパー管理者の IP は自動で許可 IP に追加されます。

→ Telnet アクセス IP 設定: Telnet を利用して Web-Admin にアクセスする IP を制限します。 各項目に関する説明は上記の「HTTP アクセス IP 設定」を参照してください。



→ SSH アクセス IP 設定: SSL を利用して Web-Admin にアクセスする IP を制限します。 各項目に関する説明は上記の「HTTP アクセス IP 設定」を参照してください。



7.1.4. サービス情報

MAILSCREENの各サービスの制御、各種設定行います。

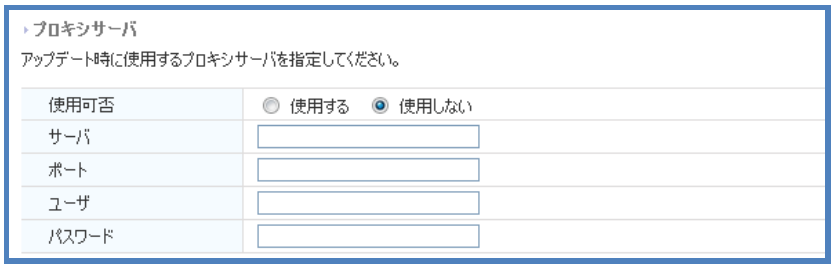
使用方法

1. **「環境設定>システム>サービス」**を選択します。
2. サービス設定ページが表示されます。 各項目を設定した後、下の「設定」ボタンをクリックします。

→ Web サーバ: Web からサーバにアクセスする URL とセッション、 自動ログアウト時間を設定します。

- 管理者 URL:スーパー管理者/決裁者/ログ閲覧者の権限を持つユーザが Web-Admin にアクセスできる URL とポート、プロトコル情報を設定します。
  - ✓ プロトコル: HTTP または HTTPS を選択します。HTTPS を使用するためには、証明書が必ず必要であり、パブリック証明書がない場合、**7.1.2 証明書情報**を参照して独自証明書を作成することができます。
  - ✓ URL: 基本的に MAILSCREEN サーバに割り当てられたドメインと Web-Admin URL は同一ですが、他のアドレスを使わなければならない場合は Web-Admin にアクセス可能な URL を入力します。
  - ✓ ポート: Web-Admin にアクセスするポートを設定します。 プロトコルが HTTP の場合には 80、 HTTPS の場合には 443 が基本値です。
- ユーザ URL: 登録されたユーザがメール履歴にアクセスできる URL とポート、プロトコル情報を設定します。 各項目に関する説明は管理者 URL と同一です。
- リンクダウンロード URL: 送信されたメールの中でポリシーによって '添付ファイルのリンク変換' が適用された場合、添付ファイルをダウンロードするリンク URL を入力します。 添付ファイルのリンク変換に関する説明は **7.3.4 リンク変換**を参照してください。
- セッション制限時間: セッションが生成された後、この指定した制限時間以上、ユーザがなにも操作しない場合、セッションが破棄されます。その後、再ログインする必要があります。
- 自動ログアウト時間: ログイン後、無操作のまま、この指定時間が過ぎると、自動ログアウトされます。

→ プロキシサーバ: ライセンスサーバ、アップデートサーバとのパターンとウィルス、エンジンなど外部との接続に使用するプロキシサーバを設定します。

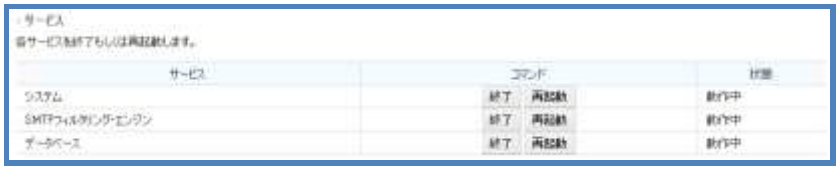


- 使用可否：プロキシサーバの使用可否を設定します。
- サーバ：プロキシサーバの IP または ホスト名を入力します。
- ポート：ポート番号を入力します。
- ユーザ：プロキシサーバに認証が必要な場合、ユーザ情報を入力します。
- パスワード：プロキシサーバに認証が必要な場合、ユーザパスワードを入力します。

注意

✖ プロキシサーバに誤った情報を設定するとライセンスサーバ等との通信ができなくなり、パッケージの一部機能が動作しない場合がありますす、ご注意ください

→ サービス制御：MAILSCREEN の各サービスを制御します。

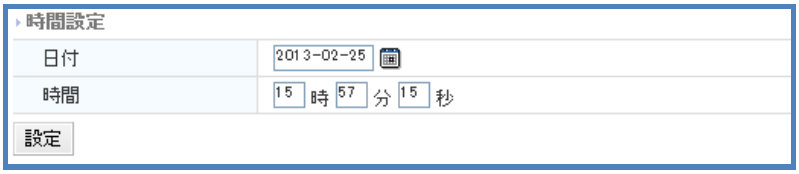


- システム：MAILSCREEN 本体サーバを再起動またはシャットダウンします。
- SMTP フィルタリング・エンジン：SMTP フィルタリング・エンジンを再起動または終了します。SMTP フィルタリング・エンジンが終了すると、メール送受信ができないので、ご注意ください。
- データベース：データベースを再起動または終了します。データベースが終了すると、Web-Admin の一部動作(メール管理と統計など)に問題が発生するので、ご注意ください。

→ 時刻同期：システムの時刻を同期化します。

- 使用可否：時間同期化機能の使用可否を設定します。
- 使用ポート：ネットワーク環境によって、NTP または TIME を選択します。
- タイムサーバ：0.0.0.0～255.255.255.255 の IP またはサーバのホスト名（HOST.COM 形式）情報を入力します。「テスト」ボタンで入力したサーバの正常動作可否を検証します。
- 同期間隔：同期化を実行する間隔を選択します。

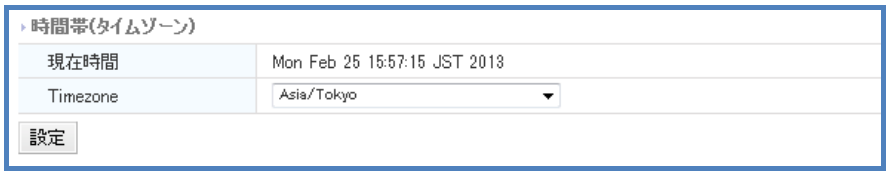
→ 時間設定: システムの日付と時間を設定します。 カレンダーアイコンをクリックして日付を指定するか、直接入力します。



注意

- ✖ 日付設定は、年-月-日まで入力する必要があります。 年は 4 桁、月は 1～12、 日は 1～31 の値のみ入力できます。
- ✖ 時間設定は、時は 0～23、 分は 0～59、秒は 0～59 の値のみ入力できます。

→ 時間帯(タイムゾーン): システムの Timezone を設定します。 変更する Timezone を選択した後、「設定」ボタンをクリックします。



注意

- ✖ Timezone を変更するとシステムが再起動します。ご注意ください。

7.1.5. ネットワーク情報

MAILSCREENのネットワーク情報を設定します。

使用方法

1. **「環境設定>システム>ネットワーク」**を選択します。
2. Network 設定画面が表示されます。 下記に、各項目について説明します。

→ Network 設定: ネットワーク情報を設定します。 インターフェース情報はデフォルトなので無効化されています。 0.0.0.0～255.255.255.255 の範囲の値で構成された IP address、 Netmask、 Gateway、 1st DNS、 2nd DNS、 3rd DNS を設定します。 DNS は IP の代わりにドメインを入力できます。

注意

- ✖ IP、 Netmask、 Gateway は Web-Admin 接続と直接関係があるので修正には正確な情報を入力する必要があります。 例えば、 ドメイン名 'test' の IP アドレスを '10.1.1.1' から '20.1.1.1' に変更すると、その以降は、'test' というドメイン名では接続できなくなります。 DNS で 'test' に対する IP アドレスを '20.1.1.1' に変更してから、接続が可能になります。しかし Netmask などの情報を変更した場合には、このような方法でも接続が不可能なことがありますのでご注意ください。
- ✖ DNS 情報は内部的な作業のために必要であり、正常なポリシー適用のために非常に重要な情報ですので、早くて安定的に動作する DNS サーバを設定してください。

→ SMTP ブリッジ: MAILSCREEN をメールサーバとブリッジ接続で構成する場合に設定します。

- メールサーバIP: 指定した「送信元」から「あて先」までのメールに対するフィルタリングを行う。 この項目は、メールサーバとブリッジ接続を構成するために設定する。 配送するメールサーバを指定する設定ではないので、注意してください。

- 追加された項目をダブルクリックし、修正ができます。

  - ✓ 送信元: 送信元のIP情報を設定する。 IPは単一のIPアドレス、あるいはCIDR 表記としてサブネットを指定できます。 指定可能なCIDRは8～32まで。
  - ✓ あて先: あて先のIP情報を設定する。 外部へ送信される全てのあて先を設定する場合、'ANY'を入力する。
  - ✓ ポート: SMTP(25)、Submission(587)、SMTPS(465)、あるいは 直接ポートを選択し、必要なポートを入力する。
  - ✓ [追加] ボタン: 上記の送信元、あて先、ポート情報を設定した後、[追加]ボタンをクリックすると、下のリストボックスに設定内容が追加されます。
  - ✓ [削除] ボタン: リストボックスから削除するメールサーバのIP情報を選択した後、[削除]ボタンをクリックすると、リストから内容が削除されます。

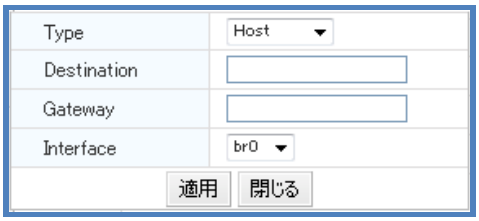
- SMTP バイパス(Bypass) IP: ここで指定されたIPから送信されたメールは、処理せずに通過します。 IPは、単一なIPアドレス、あるいはCIDR表記としてサブネットを指定できます。 指定可能なCIDRは8～32までになります。

注意

- ✖ SMTPブリッジは、メールサーバとブリッジ接続のために設定する。ネットワーク構成によっては、メールサーバとMAILSCREENをクロスケーブルで接続するなど追加作業が必要になります。
- ✖ 587、465ポートを選択すると、選択したポートでネットワークトラフィックを監視するようになるので、該当ポートは有効になっている必要がある。 [環境設定>フィルタリング>SMTP]設定を参照してください。

→ static routing 設定: MAILSCREEN のネットワークインターフェースは複数設定可能ですが、サービスを提供するために 2 つのネットワークインターフェースしか使用しません。 残りのネットワークインターフェースは使用しませんが、カスタマイズ等で、インターフェースを使用する場合、そのインターフェースに対する Routing を設定できます。

- 「追加」: 新しい Routing 情報を設定する入力画面が表示されます。



- ✓ Type: Host または Network を選択します。
- ✓ Destination: 0.0.0.0～255.255.255.255 の範囲で宛先アドレスを入力します。
- ✓ Gateway : 0.0.0.0～255.255.255.255 の範囲で Gateway アドレスを入力します。
- ✓ Interface: ネットワークインターフェースを選択します。

- 「削除」: 選択した Routing 情報を削除します。

7.2. フィルタリング情報

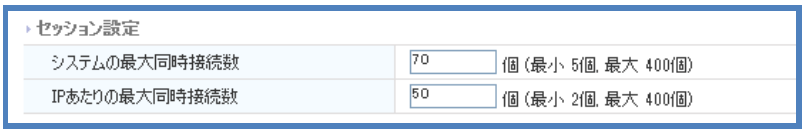
7.2.1. SMTP

セッション及びメールのアクセス制御など、 SMTP エンジンに関する基本情報を設定します。

使用方法

1. 「環境設定>フィルタリング>SMTP」をクリックします。
2. SMTP 設定画面が表示されます。 各項目を設定した後、下の「設定」ボタンをクリックします。

→ セッション設定: SMTP セッションを設定します。



- システム最大同時接続数: MAILSCREEN の SMTP エンジンに同時に接続できる、最大セッション数を設定します。 設定された値を超過した接続リクエストは接続が拒否されます。
- IP あたりの最大同時接続数: 一つの IP で同時に接続できる、最大セッション数を設定します。 設定された IP 当たり最大同時接続数はシステム最大同時接続数より、小さいか同じでなければなりません

→ BCC 自動変換: 受信者情報(メールアドレス)を保護するために、送信メールの全ての受信者(To、Cc)を Bcc に強制変換する機能です。 例えば、受信者 (To) が test@gmail.com、 test@hotmail.com のメールを送信すると受信者情報が Bcc に自動変換されてメールの受信者(test@gmail.com)は他の受信者情報(test@hotmail.com)を確認する事ができません。

- BCC 自動変換: '使用する' に設定する場合、送信する全ての受信者(To、 Cc)を Bcc に自動変換します。
  - ✓ To、 Cc のドメイン数: To、 Cc に含まれたドメインの数を設定します。 '1' に設定すると、同じドメインを使用する受信者(To、 Cc)に対しても Bcc変換させます。
- Received ヘッダ削除: メールを受信するとヘッダに Received 情報(SMTP 接続情報)が記録されますが、この情報を削除します。

→ 制限時間設定: セッションを接続してメールデータを送信する各過程の時間を制限します。

注意

✖ 制限時間を設定する場合、時間を必要以上に短く設定すると、円滑なメール受信に支障をきたします。 反対に、必要以上に長く設定すると、1 通のメール処理に時間が掛かりすぎるので SMTP の性能が落ちる場合があります。

- 正常メールキュー保存時間: SMTP が受信したメールの中で正常と判断されたメールは送信キューに移動、送信されます。直ちに送信が成功できなかった場合、再送信キューに移動、その後、一定間隔で再送信が行われます。「正常メールキュー保存時間」は、この再送信キューで待機する時間です。「正常メールキュー保存時間」の時間を超過しても正常に送信できない場合は、メールは削除され、送信者に送信失敗メールが配信されます。

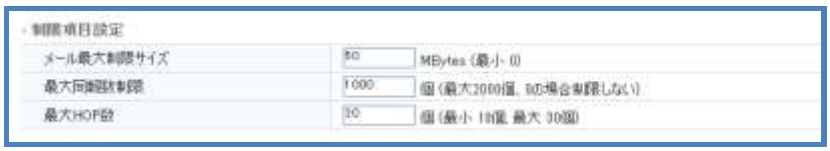
注意

✖ 正常メールキュー保存時間を必要以上に長く設定すると、キューにメールが溜まりすぎ、システムに負荷が掛かる場合がありますので、ご注意ください。

- メール受信時の入力待機の制限時間: セッションが接続された後、入力待機状態を維持できる最大時間を設定します。 入力待機状態が設定された時間を超過する場合、メール受信失敗に処理されセッションは終了します。データを受信したら、待機時間は再度 0 に初期化され、 メール受信を続行します。
- メール送信時のコネクション制限時間: ポリシーが適用されたメールをメールサーバに送信する時の接続制限時間を設定します。 この時間を超過する場合は、接続失敗として処理され、再送信されます。
- メール送信時の通信制限時間: ポリシーが適用されたメールをメールサーバに送信する時の通信制限時間を設定します。 この時間を超過する場合は、送信失敗として処理され、再送信されます。

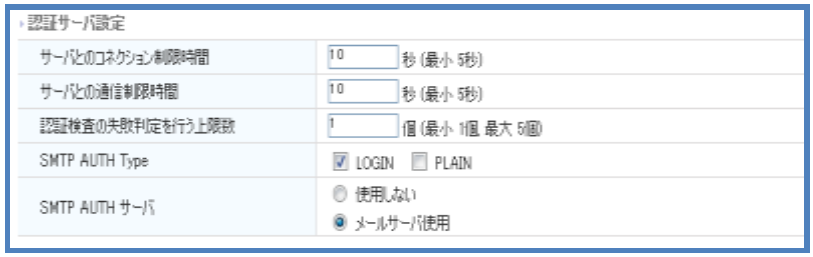
- メール送信リトライ間隔: ポリシーが適用されたメールをメールサーバに送信するのに失敗した場合、一定時間が経過した後で再度送信を試すようになります。この時、'基本ポリシーを使用'(最初は、頻繁に送信を試すが、時間が経つほどその間隔が遅れるポリシー)を選択すると、内部的に設定された間隔ごとに送信を試します。 '_分ごとにリトライ'を選択すると指定した時間が経過するたびに送信を試します。

→ 制限項目設定: SMTP がメールを受信する時にメールサイズと同報数、 Hop 数を制限します。



- メール最大制限サイズ: メールサイズが設定値を超過する場合、SMTP 接続を終了して受信を拒否します。 最小値は '0'、 最大値は '99' です。 '0' の場合には、無制限です。ただし、無制限にした場合、サーバの負荷が大きくなるため、注意が必要です。
- 最大同報数制限: 一回の SMTP 接続で、複数の受信者を指定する場合(RCPT TO)、 許容する受信者数を設定します。 受信されたメールの同補数がこの値を超過する場合、 SMTP 接続を終了して受信を拒否します。
- 最大 HOP 数: メールヘッダには Received または Delivered 項目があります。 この部分が、実際メールが送信されたパスを示し、 Hop の多いメールは多くのパスを通過した事を意味します。 多くのサーバを経由したメールは SPAM である可能性が比較的に高いので、指定した Hop 数以上のメールは受信を拒否します。

→ 認証サーバ設定: SMTP AUTH 認証サーバとの接続に関して、 接続制限時間や通信制限時間を設定します。



- サーバとのコネクション制限時間: 外部認証サーバと接続時、時間制限を設定します。 認証を依頼するサーバとの接続は接続制限時間内で完了する必要があります。
- サーバとの通信制限時間: 外部サーバと通信時、時間制限を設定します。認証を依頼するサーバと接続された後、データを確認して接続を終了する過程は通信制限時間内に完了する必要があります。
- 認証検査の失敗判定を行う上限数: MUA が送信者認証に失敗した時、メール受信を拒否します。 アカウント情報をランダムで入れ替えてアカウント情報を取得した後、MAILSCREEN サーバを SPAM 送信サーバに悪用しようとする攻撃から保護するための設定です。
- SMTP AUTH Type: SMTP Authentification Type を設定します。
  認証方式は LOGIN、 PLAIN のみサポートします。

- SMTP AUTH サーバ：認証を実施する SMTP AUTH サーバを設定します。認証は通常ユーザのメールクライアントプログラム(MUA)とメールサーバ間の SMTP AUTH を通じて行われます。 MAILSCREEN は MUA が送ってくる認証情報を SMTP AUTH サーバに送信して認証に成功したメールのみ受信して処理します。
  - ✓ 使用しない：SMTP AUTH を使用しません。
  - ✓ メールサーバ使用：MUA から送信される認証情報をメールサーバにクエリして送信者を認証します。 メールサーバは**「環境設定>メールサーバ>メールサーバ」**で追加できます。 MUA から送信される認証情報の中で ID にドメインが含まれていたら、その該当サーバに対して認証を行い、ドメインがなければメールサーバ登録の中で一番目のサーバが認証サーバとして使用されます。

注意

✖ MAILSCREEN は MUA からメールを受信する際、 SMTP AUTH 情報の使用可否と SMTP AUTH サーバのオプションによってメールを受信または拒否します。 これに関する説明は下記の表を参照してください。

MUAの SMTP AUTH 情報使用可否	SMTP AUTH サーバオプション	メール受信
使用	使用しない	認証失敗でメール受信拒否
使用	メールサーバ使用	メールサーバに認証成功した場合に受信する
未使用	使用しない	認証なしにメール受信
未使用	メールサーバ使用	認証なしにメール受信

→ 返送メール設定：MAILSCREEN は受信者にメール送信が失敗した場合、送信者に返送メール(NDR：Non Delivery Report)を配信します。 受信メールサーバからの拒否によって送信に失敗した場合は拒否原因に対する応答コードを含みます。 返送メール機能の使用可否及び返送メール送信者を設定します。

→ 詳細機能設定：その他の SMTP の動作を設定します。

- SMTP Greeting メッセージ: 外部の送信元が MAILSCREEN サーバに接続した時に表示されるメッセージを設定します。
- SMTP ポート: SMTP ポート情報を設定します。
- MUA AUTH 情報の再利用: MUA(Mail User Agent)が MAILSCREEN にメールを送信する時に使用した SMTP AUTH 情報を、MAILSCREEN が送信者の SMTP サーバに送信時に再使用します。

注意

- MUA AUTH 情報の再使用オプションは、 MUA がメールを送信時に使用した SMTP AUTH 情報を再使用して送信者 SMTP サーバから認証を受ける事なので、 MUA がメールを送信時に SMTP AUTH 情報を使用するかどうかによって適用可否が変わります。 オプションが適用されない場合、一般的な方法でメールを処理して受信者に送信します。これらに関する説明は下記の表を参照してください。

MUAの SMTP AUTH 情報使用可否	MUA AUTH 情報再使用オプション	オプション適用可否
使用	使用	適用
未使用	使用	未適用

- メール処理が ‘ルーティング指定’であるポリシーによってフィルタリングされたメールは MUA AUTH 情報再使用オプションは適用されません。

- 送信者 SMTP にメール送信: このオプションを有効化すると、MAILSCREEN は処理したメールの送信者ドメインを確認し、**「環境設定>メールサーバ>メールサーバ」**に登録してある送信者の SMTP サーバに送信します。その時、登録されていたメールサーバ情報に ‘メール送信時 SMTP AUTH を使用’ オプションが有効になっていて SMTP AUTH ID と SMTP AUTH Password が登録されている場合、この情報を利用してメールサーバに認証を行います。

注意

- 「MUA AUTH 情報の再利用」は「送信者 SMTP にメール送信」より優先順位が高く、 MUA がメールを送信する時、 SMTP AUTH 情報の使用可否によって適用可否が変わります。 もし、MUA が SMTP AUTH 情報を使用しない場合 SMTP AUTH 情報がないので「MUA AUTH 情報の再利用」オプションは適用されません。これらに関する説明は下記の表を参照してください。

MUAの SMTP AUTH 情報使用可否	MUA AUTH 情報再の再利用	送信者 SMTPにメール送信	適用されるオプション
使用	使用	使用	MUA AUTH 情報の再利用
未使用	使用	使用	送信者 SMTP にメール送信

- 送信者情報をメールヘッダへ記録: MAILSCREEN が処理したメールのヘッダに X-Original-SENDERIP と X-Original-MAILFROM を追加して、それぞれ送信者 IP とエンベロップ情報のメール送信者を記録します。 送信者の IP 情報は Received ヘッダを分析して取得できますが、X-Original-SENDERIP オプションで簡単に確認ができます。
- 受信者情報をメールヘッダへ記録: MAILSCREEN が処理したメールのヘッダに X-Original-RCPTTO を追加してエンベロップ情報のメール受信者を記録します。

注意

- 通常は、メール送信者に関する情報を取得するには、From、Received ヘッダを、 受信者に関する情報は To ヘッダを確認すると可能ですが、これらのヘッダは送信者が任意に構成する事が可能です。 正確なメール送受信者情報を取得するには、メールを受信したメールサーバのログを確認する必要があります。
  MAILSCREEN はこの過程を省き、簡単にメール分析ができるように X-Original-* ヘッダを提供します。
  MAILSCREEN が X-Original-* ヘッダに記録する情報は送信者がメール送信のために MAILSCREEN に伝えたエンベロップ情報を元に取得でき、メールヘッダに含まれた情報と一致しない場合もあります。 実際メール送受信はこのエンベロップ情報を持って実行されるので、もっと正確な情報と言えます。

- SMTP Submission ポート(587): SMTP Submission ポートである 587 番ポートの使用可否を設定します。
- SMTPS ポート(465): SMTPS ポートである 465 番ポートの使用可否を設定します。

- スマートホストサーバ: 送信者のドメインが MAILSCREEN に登録されていない場合、スマートホストサーバを参照します。 下記は、スマートホストサーバオプションを ‘使用する’ に設定した場合に、メール送信時に参照する順番です。
  ①登録されたドメインのメールサーバ → ②スマートホスト → ③DNS MX Record

注意

✖ 本機能を ‘使用する’ に設定すると、**「環境設定>メールサーバ>スマートホスト」**にスマートホストサーバ情報が設定されているか確認するようになります。 もし、設定されていなかったら **7.4.5 スマートホスト追加**を参照して情報を追加してください。

- SMTP STARTTLS: SSL を使用した SMTP 接続暗号化の使用可否を設定します。
- STARTTLS 強制適用ドメイン: 指定したドメインに関してはいつも STARTTLS でメール送信を行うように強制します。 適用ドメインは1行に1つずつ記入する必要があります。 もし、 user@example.com のメールサーバが mail.example.com の場合、 E メールドメインである example.com のみ記入してください。 この設定を使用するには、先に SMTP STARTTLS を ‘使用する’ に設定してください。

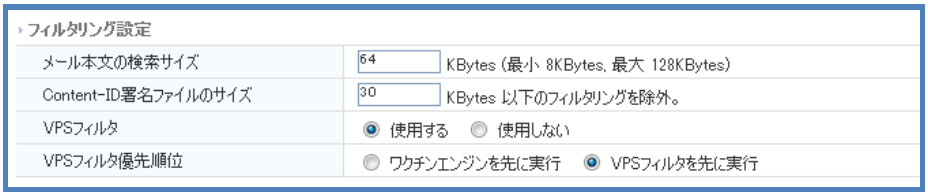
7.2.2. Scanner

Scannerは SMTPが受信したメールを受け取り、フィルタリングを行います。

使用方法

1. **「環境設定>フィルタリング>Scanner」**を選択します。
2. Scanner 設定ページが表示されます。 各項目を設定した後、下の「設定」ボタンをクリックします。

→ フィルタリング設定: Scanner がフィルタリングを行う方式を設定します。



- メール本文の検索サイズ: メール本文をフィルタリングする場合、メール本文が長すぎるとフィルタリング性能が落ちるケースがあります。 これを防止するためにフィルタリングを適用するメール本文サイズを指定して、この範囲内の内容のみを対象にしてフィルタリングを行います。

注意

✖ メール本文とはヘッダ情報を除いた部分を指しますが、もっと正確に

は各 MIME の中でメッセージに該当する text/plain または text/html などのパートで、そのヘッダ情報を除いた部分です。 添付などメッセージではない MIME では該当しません。

- Content-ID 署名ファイルのサイズ： メール本文に挿入された署名または名刺画像の内容(例： Content-ID： XXXXX)の最小サイズを設定します。通常は本文内の画像ファイルは添付ファイルとして認識されフィルタリングが行われますが、設定値より小さなサイズの画像がメール本文に挿入された場合は、添付関連フィルタリング条件で例外として処理されます。
- VPS フィルタ： VPS フィルタ適用可否を設定します。 VPS に関する詳細説明は 6.2 VPS を参照してください。
- VPS フィルタ優先順位： VPS フィルタとワクチンエンジンの優先順位を設定します。

→ 遮断のお知らせ： ウィルスメールが探知された場合に、遮断お知らせの表示可否を設定します。 警告メールを送信する場合、警告メールに関する一部事項を設定する画面が表示されます。「プレビュー」ボタンをクリックすると設定した警告メールを確認できます。

注意

✖ ウィルスメール送信者の E メールアドレスは受信不可、他人の E メールアドレスを盗用している可能性があるので、その点にはご注意ください。

7.3. 誤送信防止

誤送信防止は社外に送信されるメールの内部情報漏洩を防止するための機能です。 ユーザが送信した全てのメールはフィルタリングされ、ポリシーが適用されます。そして、各ポリシーのメール処理方式によって添付ファイルの暗号化、 添付ファイルのリンク変換、 送信遅延などの処理が行われます。

注意

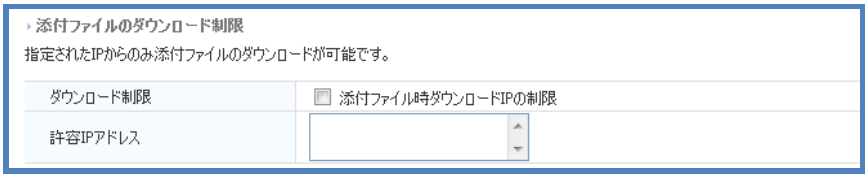
✖ 「誤送信防止」メニューの一部設定により、お知らせメールの内容と機能ボタンの有効化可否が変わりますので、下記の各機能に関する説明を注意してお読みください。

7.3.1. 添付ダウンロード制限

指定した IP のデバイス(スマートフォン/Webブラウザ)でのみ、メールと添付ファイルのダウンロードを許可します。 もし、許可IP または IPの範囲ではないデバイスから接続される場合、メール詳細確認の原文タブが無効化され、ダウンロードボタンと添付タブの添付ファイルダウンロードリンクが削除され、原文と添付ファイルをダウンロードできなくなります。

使用方法

1. **「環境設定>フィルタリング>誤送信防止」**を選択します。
2. 誤送信防止の設定ページが表示されます。各項目を設定した後、下の「設定」ボタンをクリックします。



→ ダウンロード制限: 添付ファイルがダウンロード可能な IP の制限可否を設定します。

→ 許容 IP アドレス: 原文表示及び添付ダウンロードを許可する IP 情報を入力します。 1行に一つの IP アドレス(0.0.0.0～255.255.255.255)を入力する必要があり、 D クラス以下は略して “.”で終わる IP アドレス範囲を入力できます。例えば ’10.0.0.’ を入力すれば ’10.0.0.1’から ’10.0.0.255’ までが適用されます。

7.3.2. 添付ファイル暗号化

メールの添付ファイルを圧縮、暗号化して送信します。 この時、圧縮ファイルのパスワード情報はランダムで生成され(ポリシー毎の固定パスワードの設定も可能)、 送信者には暗号化お知らせメールが送信されます。**「環境設定>フィルタリング >誤送信防止>添付ファイルのパスワード設定」**で一定時間後に受信者にもパスワードお知らせメールが送信されるように設定できます。

使用方法

1. **「環境設定>フィルタリング>誤送信防止」**を選択します。
2. **「添付ファイル暗号化」**にて、各項目を設定した後、下の 「設定」 ボタンをクリックします。

→ 暗号化のお知らせ：暗号化お知らせメールの送信可否と件名・本文のテンプレートを設定します。「プレビュー」ボタンをクリックすると、編集された内容を確認できます。

- パスワード送信：「パスワード送信」をクリックすると、受信者にパスワードお知らせメールが送信されます。
- パスワード送信キャンセル：「パスワード送信キャンセル」ボタンをクリックすると、パスワードお知らせメールが送信キャンセルされます。

  キャンセルした場合、**「環境設定>フィルタリング>誤送信防止>添付ファイルのパスワード設定」**の‘x 分後、受信者にパスワードをメールで送信’オプションがチェックされていても、パスワードお知らせメールが送信されません。しかし、‘x 分後、受信者にパスワードをメールで送信’で設定されていた時間が経過した後、「パスワード送信キャンセル」をクリックしても、既にパスワードは送信済みですのでキャンセルできません、ご注意ください。

7.3.3. 送信遅延

送信遅延とは、誤送信防止のために、フィルタリングされたメールの送信を一時的に遅延させる機能です。送信者には送信遅延お知らせメールを送信して、メール内容、宛先、CCなどを、一度確認する事ができるようにします。送信遅延のお知らせメールにて‘直ちに送信’または‘送信キャンセル’オプションを利用してメールの誤送信を防止します。

注意

- ✖ 送信者が、送信遅延されたメールに対して、何のオプションも適用させないと、設定された時間が経過後、自動で受信者にメールが送信されます。スーパー管理者または決裁者は、送信者がメール内容をもう一度確認するように運用指導してください。
- ✖ 送信遅延は、社内（メールサーバ登録されいているドメイン）間のメー

ルに関しては、遅延機能は動作しません。
あくまでも、社外（外部ドメイン）への送信時に機能します。
社内、社外が混在した宛先の場合でも、社内には送信遅延せず、社外宛のメールのみ送信遅延します。ご注意ください。

使用方法

1. **「環境設定>フィルタリング>誤送信防止」**を選択します。
2. **「送信遅延」**にて、各項目を設定した後、ページ下の「設定」ボタンをクリックします。

→ 遅延のお知らせ： 送信遅延お知らせメールの件名・本文テンプレートを設定します。「プレビュー」ボタンをクリックすると、編集された内容を確認できます。

- 今すぐ送信： 送信遅延されているメールが受信者に直ちに送信されます。
- 送信キャンセル： 送信遅延されているメールの送信をキャンセルし、受信者に送信されません。

7.3.4. リンク変換

メールの添付ファイルをダウンロードできるリンクを作成します。 リンク変換された添付ファイルはダウンロード時、 設定によってパスワードが要求される場合があります。

注意

- ✖ 添付ファイルリンク変換のいくつかのオプションは、添付ファイル暗号化後のリンク変換にも影響を与えます。
- ✖ 添付ファイルリンク変換は大容量メール送信のための機能ではなく、誤送信防止のために提供する機能です。 メール全体サイズが約 70MB 以上の場合、サーバ及びネットワーク状況によって正常に処理

されない場合もありますので、ご注意ください。

使用方法

1. **「環境設定>フィルタリング>誤送信防止」**を選択します。
2. **「添付ファイルのリンク変換」**にて、各項目を設定した後、ページ下の「設定」ボタンをクリックします。

→ GIGAPOD 連携: リンクに変換した添付ファイルをオンラインストレージ GIGAPOD に保存します。 この時、パスワードお知らせメールは送信されず、 メール詳細確認時にダウンロード有効/無効/パスワード送信機能が使用できません。GIGAPOD に関する説明は、下記のウェブサイトを参照してください。
＊ GIGAPOD 紹介ページ: http://www.tripodworks.co.jp/product/gigapod/

- 使用しない: MAILSCREEN 独自の URL リンク変換機能を使用します。
- UTF-8: UTF-8 エンコードを使用して GIGAPOD と連携します。 GIGAPOD2010 以降で使用します。
- Shift-JIS: Shift-JIS エンコード使用して GIGAPOD と連携します。 GIGAPOD OFFICEHARD で使用します。

→ GIGAPOD サーバ: GIGAPOD サーバ情報を入力します。「テスト」ボタンをクリックするとサーバとの接続状態をテストします。

→ GIGAPOD ログイン ID: GIGAPOD ログイン ID を入力します。

→ GIGAPOD ログインパスワード: GIGAPOD ログイン でのパスワードを入力します。

→ GIGAPOD ログインパスワード確認: GIGAPOD ログインでのパスワードをもう一度入力します。

→ ファイルリンクパスワード: 添付ファイルのリンク変換時に適用されるパスワードを入力します。 受信者がメールのリンクを参照して添付ファイルをダウンロードするには、パスワード入力が必要になります。ただし、フィルタ追加時 ‘添付ファイル暗号化後にリンク変換’ 動作が適用される場合には添付ファイル暗号化のパスワードが優先され、このファイルリンクパスワードは使用しません。

→ ファイルリンクパスワード確認: ファイルリンクパスワードをもう一度入力します。

→ ファイルリンク期限: 添付ファイルのリンク有効期間を設定します。 メールが送信された日付を基準にして設定された期間が経過すると、該当メールの添付ファイルリンクからダウンロードができなくなります。

→ GIGAPOD 連携の場合、MAILSCREEN 側で設定した、リンクパスワード、有効期限が GIGAPOD 側の設定より優先されます。

→ ファイルリンクのファイル名: 添付ファイルがリンク変換される場合、メール受信者は添付ファイルの代わりに添付ファイルをダウンロードできるリンクを含んだ html ファイルを添付として受けるようになります。 この時、添付される html ファイルの名前を設定します。

→ GIGAPOD エラー時の通知方法: GIGAPOD 連携エラーが発生した場合、管理者にメールを送信します。

→ リンクファイルのテンプレート: 受信者に送信される添付ファイルリンクメールのテンプレートを設定します。 メールの件名・本文に対して編集することができます。「プレビュー」ボタンをクリックすると編集された内容を確認することができます。

7.3.5. 添付ファイルのパスワード設定

添付ファイル暗号化に関するオプションを設定します。

使用方法

1. **「環境設定>フィルタリング>誤送信防止」**を選択します。
2. **「添付ファイルのパスワード設定」**にて各項目を設定した後、ページ下の「設定」ボタンをクリックします。

→ パスワード長さ: 添付ファイルが暗号化される時のパスワードの長さを設定します。6 文字から 16 文字まで設定できます。 パスワードは、毎回新しく生成されますが、指定した長さで 0-9a-zA-Z が含まれます。

→ パスワードのお知らせ: パスワードお知らせのテンプレートと受信者への自動パスワードお知らせオプションを設定します。 ‘「 」分後、受信者にパスワードをメールで送信’ にチェックを入れたら、指定された時間にパスワードお知らせメールが受信者に自動で送信されます。「プレビュー」 ボタンをクリックすると、編集したテンプレート内容をあらかじめ確認できます。

7.3.6. 遮断

社外に送信されるメールを遮断します。この機能を適用させる事で情報漏洩を防止できます。

使用方法

1. **「環境設定>フィルタリング>誤送信防止」**を選択します。
2. 「遮断」にて、各項目を設定した後、ページ下の 「設定」 ボタンをクリックします。

→ 遮断お知らせ: 送信者が受ける遮断お知らせメールの件名・内容テンプレートを変更できます。「プレビュー」 ボタンをクリックすると、編集された内容を確認できます。

7.3.7. 決裁（オプション機能）

メール送信を待機させた後、MAILSCREENに指定されている決裁者に決裁を要請します。決裁者は決裁要請メールを通じて送信者から送られたメールを確認できます。決裁者が承認すると、メールは受信者に送信され、却下した場合は、メールは送信されません。もし、決裁者からの承認が行われず、一定時間が経過すると、**「SMTP Filter>ポリシー管理>ポリシー追加」**でのオプション、または**「環境設定>フィルタリング>誤送信防止>決裁」**でのオプションによって自動承認または却下されます。

使用方法

1. **「環境設定>フィルタリング>誤送信防止」**を選択します。
2. 「決裁」にて、各項目を設定した後、ページ下の「設定」ボタンをクリックします。

→ 決裁：決裁に関するオプションを設定します。

- 自動決裁使用：決裁が必要なメールが待機中のまま決裁満了時間が経過すると、自動で決裁が行われる機能を有効化します。 時間と処理内容を設定してください。承認/却下設定は「自動決裁使用」またはポリシーで設定した自動決裁設定に従います。

→ 基本決裁者のメール：基本決裁者のメールアドレスを入力します。 ポリシー追加の際、決裁者が指定されない場合は基本決裁者に決裁が要請されます。

→ 承認決裁の理由：メールに対する承認理由を設定します。各メールの決裁理由は**「SMTP Filter>メール」**で該当メールを詳細に確認できます。

- 承認時、決裁者が決裁理由を選択または入力：決裁者がメールに対して承認を行うには、承認理由を入力する必要があります。

- 追加/削除：「追加」 ボタンを使用して承認理由を追加することができ、「削除」ボタンで既存の承認理由を削除できます。

→ 却下の理由： メールに対する却下理由を設定します。 各項目に関する説明は ‘承認決裁の理由’と同様です。

→ 決裁の要求： 決裁要請に関するオプションを設定します。

- 決裁要求のメールに原文を添付： メールの原文が決裁要請メールの添付ファイルに含まれて送信されます。
- テンプレート： 決裁要請メールの件名・本文のテンプレートを変更できます。「プレビュー」 ボタンをクリックすると編集された内容を確認できます。

✓ 承認： 決裁者が「承認」をクリックすると、該当メールは受信者に送信され、送信者に承認お知らせメールが配信されます。

✓ 却下： 決裁者が「却下」をクリックすると、該当メールは受信者に送信が遮断され、送信者に却下お知らせメールが配信されます。

✓ メール確認： 決裁者が「メール確認」をクリックすると、該当のメールのメール詳細確認ページが表示され、該当メールのヘッダ、 原文、内容、 送信結果、 添付ファイル名などを確認できます。

✓ 決裁する： 決裁者が「決裁する」をクリックすればメール管理ページに移動し、決裁者は全ての決裁要請メールを確認できます。

→ 決裁待ち： 決裁待機メールの送信オプションを設定できます。

- 決裁待ちのメールを送信： 送信者に決裁待機お知らせメールが配信されます。
- テンプレート： 決裁待機メールの件名・本文のテンプレートを変更できます。「プレビュー」 ボタンをクリックすると、編集された内容を確認できます。

→ 承認のお知らせ： 承認お知らせメールの送信オプションを設定できます。

- 承認のお知らせメールを送信： 決裁者がメールを承認したか、自動で承認された場合、送信者に承認お知らせメールが配信されます。
- テンプレート： 承認お知らせメールの件名・本文のテンプレートを変更できます。「プレビュー」 ボタンをクリックすると編集された内容を確認できます。

→ 却下のお知らせ： 却下お知らせメール送信オプションを設定できます。

- 却下のお知らせメールを送信： 決裁者がメールを却下したか、自動で却下された場合、送信者に却下お知らせメールが配信されます。

- テンプレート：却下お知らせメールの件名・本文のテンプレートを変更できます。「プレビュー」ボタンをクリックすると編集された内容を確認できます。

→ 代理決裁のお知らせ：代理決裁お知らせメールの送信オプションを設定できます。

- 決裁者に代理決裁のお知らせメールを送信：代理決裁者がメールを決裁した場合、決裁者に代理決裁されたという旨のお知らせメールが配信されます。
- テンプレート：代理決裁お知らせメールの件名・本文のテンプレートを変更できます。「プレビュー」ボタンをクリックすれば編集された内容を確認できます。

7.3.8. ポリシー適用のお知らせ

外部に送信されるメールにポリシーが適用された場合、該当メールの送信者に本メッセージをお知らせします。

注意

✖ エンジン自動アップデート時に、変更したポリシー適用のお知らせテンプレートが初期化される場合がありますので、ご注意ください。

使用方法

1. 「**環境設定>フィルタリング>誤送信防止**」を選択します。
2. 「ポリシー適用のお知らせ」にて、各項目を設定した後、ページ下の「設定」ボタンをクリックします。

→ ポリシー適用のお知らせ：送信者が受信するポリシー適用のお知らせメールの件名・本文テンプレートを変更できます。「プレビュー」ボタンをクリックすると編集された内容を確認できます。

7.3.9. 通過

メールを通過させます。 本機能を使用して特定メールをポリシーから例外対象に適用することができます。 統計とメール管理でメールを分析して社内から社外に送信されるメールをモニタリングできます。通過機能に関する設定は **4.1.2ポリシー追加**を参照してください。

7.3.10. ルーティング指定

メールを指定されたルーティングサーバに転送します。 特定メールを別サーバに保存する場合に本機能を使用します。ルーティング指定機能に関する設定は**4.1.2ポリシー追加**を参照してください。

7.4. メールサーバ

MAILSCREENからメールサーバにリレー送信する為のメールサーバ情報を設定します。
送信者のドメインを参照して、どのメールサーバを使用するかを判断します。

7.4.1. メールサーバ管理

メールサーバの情報を設定します。

使用方法

1. **「環境設定>メールサーバ>メールサーバ」**を選択します。
2. メールサーバ管理ページが表示されます。
3. 下記に、メールサーバ管理ページの上下にある関連機能について説明します。

→ 検索： 検索条件(ドメイン、サーバ IP、 ポート)を選択して、キーワードを入力します。「検索」 ボタンをクリックすると検索されたメールサーバ情報が画面に表示されます。

→ 追加： メールサーバを追加します。 メールサーバ追加に関する詳細説明は **7.4.2 メールサーバ追加**を参照してください。

→ 削除： 選択したメールサーバ情報をリストから削除します。

→ ファイル保存： 検索されたメールサーバリストを Excel ファイルとして保存します。

→ リスト数設定： 1 ページ当りに表示されるリストの表示数を設定します。

→ 変更： メールサーバ情報の中でドメイン名をクリックすると、メールサーバ情報を修正することができます。メールサーバ情報修正に関する詳細説明は、**7.4.2 メールサーバ追加**を参照してください。

7.4.2. メールサーバ追加

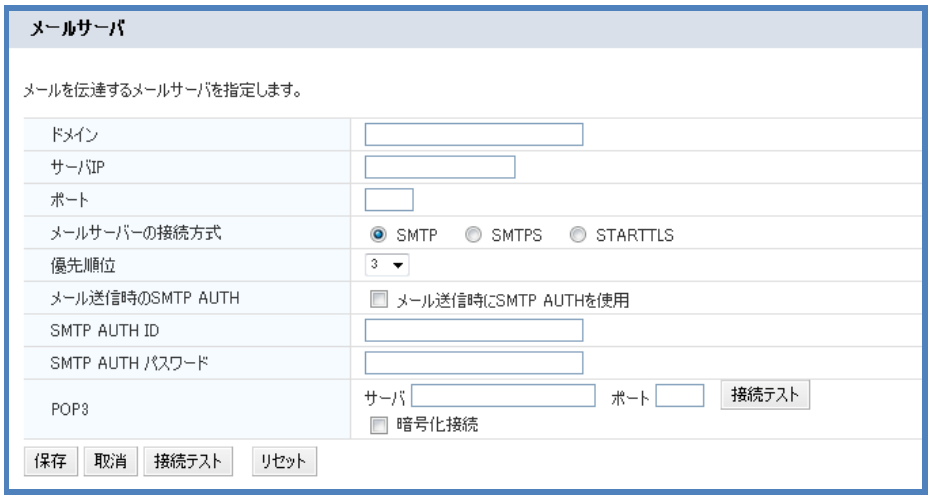
メールサーバを追加します。

注意

- ✖ メールサーバの設定に誤りがあると、メールが正常に送信されないなど問題が発生するのでご注意ください。
- ✖ メールサーバとの接続テスト時、ネットワーク環境が円滑でない場合は、有効なメールサーバにも関わらず検証失敗というメッセージが出る場合があります。

使用方法

1. **「環境設定>メールサーバ>メールサーバ」**を選択します。
2. メールサーバリストメニューの「追加」ボタンをクリックします。
3. メールサーバ追加ページで、各項目を設定した後、「保存」ボタンをクリックします。



→ ドメイン: メールサーバのドメイン情報を入力します。

→ 送信者のメールアドレスの@以降のドメイン情報を入力します。

→ サーバ IP: メールを配送するサーバの IP(0.0.0.0～255.255.255.255) またはホスト名を入力します。 ホスト名は FQDN で入力する事ができ、1つのドメインにはメールサーバを最大 5 個まで登録できます。

→ ポート: 1～49151 の間のポート情報を入力します。 入力しない場合は自動で 25 に設定されます。

→ メールサーバの接続方式: メールサーバに接続する方式を選択します。 SMTP、SMTPS、 STARTTLS の中で選択します。

→ 優先順位:優先順位を 1～5 の中で設定します。数字が大きいほど優先順位が高く、一つのドメインに複数台のメールサーバが追加されたら、優先順位が高いメールサーバが優先で使用されます。

→ メール送信時の SMTP AUTH: メールを送信する時、メールサーバに AUTH 認証を要請します。 オプションを設定する場合、併せて SMTP AUTH ID とパスワードを入力する必要があります。

→ SMTP AUTH ID: 50 文字以内の有効な ID を入力します。

→ SMTP AUTH パスワード: メールサーバに認証を受けるための有効な パスワードを入力します。

→ POP3: POP3 サーバ情報を入力します。**「環境設定>システム>アクセス制御>ログイン情報」**で POP3 に設定する場合、 ログイン時に使用される情報です。

3. 「保存」 ボタンをクリックします。 現在の作業をキャンセルしたい場合 「取消」ボタンをクリックします。「接続テスト」ボタンをクリックすると、設定したメールサーバへの接続テストが行われます。「リセット」 ボタンをクリックする場合、入力された全ての情報が初期化されます。

7.4.3. メールサーバ 一括登録

メールサーバ情報を、CSVテキストファイルで一括登録します。

使用方法

1. **「環境設定>メールサーバ>一括登録」**を選択します。
2. メールサーバー括登録ページで「参照...」 ボタンをクリックして、サーバ情報ファイルを選択した後「登録」 ボタンをクリックします。

注意

- 1つのドメインに対して、メールサーバは最大 5 個まで登録が可能です。
- テキストファイルは1行に一つのメールサーバ情報を入力して各フィールドは ':' 文字で区分する。
  <ドメイン>:<メールサーバ>:<メールサーバポート>:<優先順位>:<AUTH 使用可否>:<AUTH ID>:<AUTH パスワード> (ex)a.com:10.0.0.1:25:1:test:password

3. 失敗した場合は失敗メッセージが表示され、 成功した場合は登録されたユーザ情報リストが画面に表示されます。

7.4.4. スマートホストサーバ

「環境設定>フィルタリング>SMTP>詳細機能設定」のスマートホストサーバオプションを '使用する' に設定する場合に参照されるサーバ情報を設定します。

使用方法

1. **「環境設定>メールサーバ>スマートホスト」**を選択します。

2. スマートホスト管理ページが表示されます。
3. 下記に、スマートホスト管理ページの上下にある関連機能について説明します。

→ 追加：スマートホストサーバを追加します。 スマートホストサーバの追加に関する詳細説明は **7.4.5 スマートホスト追加**を参照してください。

→ 削除：選択したスマートホストを削除します。

注意

✖ **「環境設定>フィルタリング>SMTP>詳細機能設定」**のスマートホストサーバオプションを ‘使用する’ に設定して、スマートホストサーバを全削除する場合はスマートホスト機能が正常動作しない場合がありますので、ご注意ください。

→ ファイルで保存：スマートホストサーバリストをExcelファイルとして保存します。

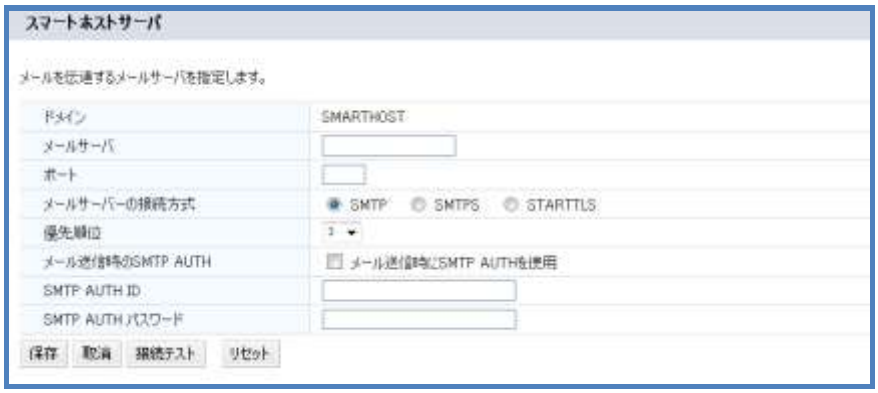
→ 修正：スマートホストサーバ情報の中でドメイン名前をクリックすると、情報を修正することができます。 情報変更項目は **7.4.5スマートホスト追加**を参照してください。

7.4.5. スマートホスト追加

スマートホストを追加します。

使用方法

1. **「環境設定>メールサーバ>スマートホスト」**をクリックします。
2. 「追加」 ボタンをクリックします。
3. スマートホストサーバの追加ページで、各項目を設定します。



→ ドメイン: スマートホストサーバのドメイン情報は、メール送信とは関係がない情報です。デフォルト値(SMARTHOST)に固定します。

→ メールサーバ: メールを配送するサーバ IP(0.0.0.0 ～ 255.255.255.255)または FQDN 形式のホスト名を入力します。

→ ポート: 1～49151 の間のポート情報を入力します。 省略する場合は自動で 25 に設定されます。

→ メールサーバの接続方式: メールサーバに接続する方式を選択します。SMTP、 SMTPS、 STARTTLS の中で 1 つを選択します。

→ 優先順位: 優先順位を 1～5 の間で設定します。 優先順位は数字が大きいほど高くなります。

→ メール送信時の SMTP AUTH: SMTP AUTH メールを送信する時、メールサーバに AUTH 認証を要求します。 オプションを設定する場合、下の SMTP AUTH ID とパスワードを入力する必要があります。

→ SMTP AUTH ID: 50 字以内の有効な ID 情報を入力します。

→ SMTP AUTH パスワード:認証用のパスワードを入力します。

4. 「保存」ボタンをクリックします。 現在の作業をキャンセルしたい場合、「キャンセル」ボタンをクリックします。「接続テスト」ボタンをクリックすると、設定したメールサーバへの接続テストが行われます。「リセット」ボタンをクリックする場合、入力された全ての情報が初期化されます。

注意

✖ スマートホストサーバとの接続テスト時、ネットワーク環境が円滑でない場合、正常なサーバでも検証失敗というメッセージが出る場合があります。

7.4.6. リレー

MAILSCREENのリレーの基本設定は不許可になっていますので、MAILSCREENを経由してメールを送信するためにはリレー設定が必要です。 MAILSCREENで許可されないユーザによるSPAMメールサーバとして悪用される恐れがあるためです。メール送信のためにMAILSCREENに接続するユーザの IP アドレスはリレーを許可するように登録してください。

使用方法

1. 「**環境設定>メールサーバ>リレー**」を選択します。
2. 下記に、リレー管理ページの上下にある各機能について説明します。

→ 1. 登録: IP アドレスに対して、許可または不許可の設定を登録します。

- IP: 0.0.0.0～255.255.255.255 の IP を設定します。IP アドレス入力時、D クラス以下を “.” で終わる IP アドレス範囲で入力できます。 例えば、‘10.0.0.’ を入力すれば ‘10.0.0.1’ から ‘10.0.0.255’ までの範囲を意味します。
- 区分: allow: 許可 または deny: 不許可を設定します.

注意

- ✖ 1つの動作(許可:allow 又は、不許可:deny)に重複 IP 設定はできません。例えば 10.0.0.1 が許可で登録されている状態で、‘10.’ を改めて許可に登録する事はできません。‘10.’ は ‘10.0.0.1’ を含むので、お互いに重複された IP として識別するためです。 反対の場合も登録が許可されません。
- ✖ より正確に登録した IP アドレスほど高い優先順位を持ちます。 例えば ‘10.’ を不許可に登録して、‘10.0.0.1’ を許可に登録したとすれば、‘10.’ 範囲の全ての IP は拒否されるが、‘10.0.0.1’ は許可されます。

→ 2. リスト数設定: 1 ページ当りに表示されるリストの表示数を設定します。

→ 3. 削除：選択したリレーIP をリストから削除します。

→ 4. ドメイン：リレーを許可するドメインアドレスを設定します。

- ドメイン：１行に１つのドメインを‘@abcd.com’形式で設定する必要があります。

注意

✖ もし、リレー許可ドメイン設定情報が社外に漏洩した場合、MAILSCREEN サーバがオープンリレーとして悪用される恐れがありますので、注意してください。

→ 5. メールアカウント：リレーを許可するメールアカウントを設定します。

- メールアカウント：１行に１つのメールアカウントを‘abcd@abcd.com’形式で設定する必要があります。

注意

✖ リレー許可ドメイン設定のように、リレー許可メールアカウント情報が社外に漏洩した場合、MAILSCREEN サーバがオープンリレーとして悪用される恐れがありますので、注意してください。

7.5. メンテナンス

MAILSCREENは、エンジン自動アップデート及びバックアップ機能を提供します。

7.5.1. エンジン自動アップデート

MAILSCREENは、アップデートが必要な場合、 自動でアップデートサーバからデータをダウンロードし、パッチを適用します。 エンジン自動アップデートは毎回定時（毎時11分）に新しいパッチの存在有無を確認します。

注意

- ✖ アップデートサーバに新しいバージョンのパッチが存在する場合、「リアルタイムアップデート」 ボタンが生成されます。

使用方法

1. **「環境設定>維持補修>エンジン自動アップデート」**を選択します。
2. 下記に、エンジン自動アップデートページの上下にある各機能について説明します。
   - → パッケージバージョン情報： 現在パッケージ、最新パッケージのバージョンと自動アップデート設定情報が表示されます。
   - → 変更内容表示：「変更内容表示」 ボタンをクリックすると、詳細なアップデート変更履歴が確認できます。
   - → リスト数： 1 ページ当りに表示されるリストの表示数を設定します。
   - → アップデートログ： 自動アップデートされた履歴が時間、状態、説明項目で表示されます。

7.5.2. 基本バックアップ

データ損失に備えて提供する機能であり、Web-Adminで簡単にバックアップと復元を行えます。バックアップされるのは、ポリシー、 black list/white list、 環境設定の各種設定情報です。

使用方法

1. **「環境設定>維持保守>基本バックアップ」**を選択します。
2. 下記に、基本バックアップ画面の機能について説明します。

- → バックアップ： バックアップを ‘圧縮後に暗号化で行う’ か ‘圧縮のみ’ かを選択した後 「ファイル保存」 ボタンをクリックします。

注意

- ✖ 新しいバージョンにアップグレードする時は、万一のデータ紛失に備えて基本バックアップを行ってください。
- ✖ メールデータと 統計データはバックアップされません。

→ 復元：「参照…」ボタンをクリックして、バックアップされているファイルを選択し、「アップロード」ボタンをクリックします。

注意

- ✖ 復元作業は、現バージョンと同じバージョンでバックアップされたデータで行わなければなりません。現バージョンと違うバージョンでバックアップされたデータを復元する場合、サービスが正常動作しない場合があります。

7.5.3. 詳細バックアップ

メールデータと DB データ、環境設定情報をバックアップします。

使用方法

1. **「環境設定>維持保守>詳細バックアップ」**を選択します。
2. 下記に、詳細バックアップページの機能に関して説明します。

→ バックアップスケジュール： バックアップスケジュールを設定します。

注意

- ✖ 詳細バックアップは、前日のデータのみを対象にして、メールデータと DB データ、環境設定情報をバックアップします。
- ✖ **「環境設定>システム>基本情報」**の ‘メール保存期間設定’と ‘データ保存期間設定’メニューで設定した期間を間隔にしてバックアップする事を推奨します。

- 詳細バックアップでバックアップされたデータを復元するには、システムコンソールにログインして /sniper/web-aux/tools/restore 「DIR|FILE」コマンドを使用します。 データの量によって数分から数時間まで掛かる場合があります。
- バックアップファイルは下記のような形式で生成されます。

backup. (config/sqls/emls). 日付(yyyymmdd). IP(xxx. xxx. xxx. xxx). dat

又は

backup. (config/sqls/emls). 日付(yyyymmdd). IP(xxx. xxx. xxx. xxx).tar.gz

→ バックアップファイル: バックアップを '圧縮後に暗号化で行う' か '圧縮のみ' かを選択します。

→ バックアップ対象: バックアップデータを選択します。

- 基本データ: MAILSCREEN を起動するために必要な基本的なデータです。
- 送信メール: 送信メールまたはフィルタ適用メールのログ、メールコピーをバックアップします。

→ バックアップ方法: FTP サーバまたは MAILSCREEN 内部パスを指定します。

- FTP: FTP サーバにバックアップファイルを送信、保存します。
  - ✓ サーバ: バックアップファイルを保存する FTP サーバの IP アドレスまたはドメイン名を入力します。
  - ✓ ID: FTP サーバのログイン ID を入力します。
  - ✓ パスワード: FTP サーバのログインパスワードを入力します。
  - ✓ リモートパス: FTP サーバにログインした後、移動するディレクトリーを入力します。 移動せずにログインしてデフォルトて設定されたディレクトリーにバックアップするには "./"のみを入力します。「接続テスト」ボタンをクリックすると、入力した FTP 情報が正しいかテストできます。
- パス指定: MAILSCREEN 本体内にバックアップファイルが保存されます。該当位置に 'yyyymmdd' の形式のフォルダが生成され、そのフォルダ内にバックアップファイルが保存されます。

→ バックアップ情報: バックアップに掛かった時間、 処理結果などの情報をスーパー管理者にメールで送信します。

7.5.4. ログ抽出

システムに問題が起こった場合、問題を分析するためにシステムログを取得する機能を提供します。

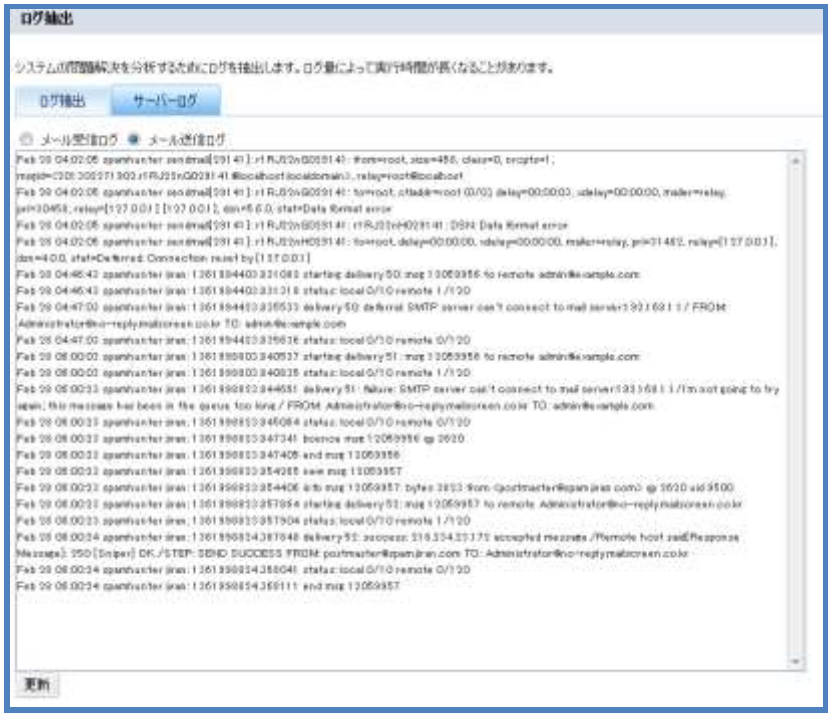
使用方法

1. **「環境設定>維持補修>ログ抽出」**を選択します。
2. 下記に、ログ抽出ページの各機能に関して説明します。

→ ログ抽出：システム運用と動作に関するシステムログを取得します。

- システムログ： 取得する日付を直接入力するか、カレンダーアイコンをクリックして日付を選択した後「ファイル保存」ボタンをクリックします。

→ サーバーログ： SMTP エンジンのログをリアルタイムで確認します。



- メール受信ログ： リアルタイムでメール受信ログを確認します。 メール受信ログを選択した後、「更新」ボタンをクリックします。
- メール送信ログ： メール送信ログを確認します。 メール送信ログを選択した後、「更新」ボタンをクリックします。

7.5.5. イベントログ

ユーザ情報、メールなどの変更作業や、 ログインなどセキュリティ上の重要な作業においてイベントログを残し、これらを確認できる機能を提供します。 イベントログはシステムで自動削除されません。

使用方法

1. **「環境設定>イベントログ」**を選択します。
2. イベントログページが表示されます。
3. 下記に、イベントログページの各機能について説明します。

→ 種類: 作業が成功したか失敗したかを示します。

→ 区分: 作業内容を区分して表示します。 作業の区分は、ログイン、 ユーザ、ドメイン、 ポリシー、 環境設定、 バックアップ、 VPS、 ワクチン、 エンジン、 メール、 添付ファイル、 データ脆弱性検査、システム検査、System Maintenanceがあります。

→ Task: 区分毎の作業内容です。Task の、「区分」は、'成功' '追加'、'削除'、'修正'、'アップデート'、'System Maintenance' があります。

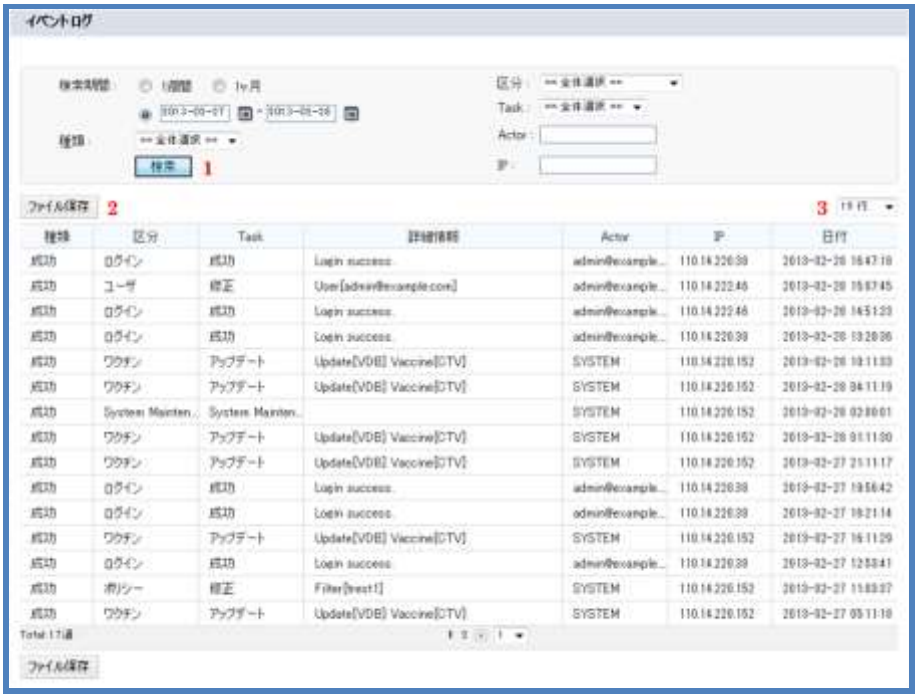
→ 詳細情報: 各Taskに関する詳細内容です。

→ Actor: 作業者 ID です。

→ IP: 作業者の IP アドレスです。

→ 日付: 作業が行われた日付です。

4. 下記に、イベントログリストの上下にある各機能について説明します。



→ 検索： イベントログを検索します。 検索期間、種類、区分、Task、Actor、IP 項目にて検索条件を設定した後、「検索」 ボタンをクリックします。

→ ファイル保存： 検索されたイベントログを Excel ファイルとして保存します。

→ リスト数設定： 1 ページ当りに表示されるリストの表示数を設定します。

8. システム概要と統計

MAILSCREENは全体システム状況と統計とポリシー、拒否理由などの項目で統計を提供します。

8.1. システム概要

現在のシステム状況を一目で分かるようにシステム概要ページを提供します。 簡易な統計、現在システムとプロセス、 アップデート状況などを確認できます。

使用方法

1. 「SMTP Filter>システム概要」を選択します。
2. システム概要ページが表示されます。

→ 統計： メール全体の状況を送信、フィルタ動作、、ウィルス、拒否で分けてグラフで表示します。

→ システム状況： 現在システムの稼働状況を CPU、メモリーなどで表示します。

→ プロセス状況： 現在起動中のサービス状態を表示します。

→ アップデート状況： 現在サーバに設置されているパッケージバージョンと最新パッケージバージョンなどアップデート関連情報を表示します。

→ メールキュー状態： 現在キュー状態を表示します。

→ 最近のウィルス： 最近のメールの中で、ウィルスメールの情報を表示します。

8.2. 統計管理

8.2.1. 全体統計

MAILSCREENを通過したメールの全体状況を、送信、フィルタ動作、ウィルス、拒否などの種類で確認できます。各種のメール数と全体に対する割合が、日付（降順）でソートされます。

使用方法

1. 「SMTP Filter>統計>全体統計」を選択します。
2. 全体統計ページが表示されます。
3. 下記に、全体統計に表示される各項目に関して説明します。

日付	送信 (数量/割合%)	フィルタ動作 (数量/割合%)	ウィルス (数量/割合%)	拒否 (数量/割合%)	合計

→ 日付： 統計が生成された日付です。

→ 送信(数量/割合%)： ポリシーが適用されず、正常に社外メールサーバに送信されたメールです。

→ フィルタ動作(数量/割合%)： ポリシーによって添付ファイル暗号化、 添付ファイルのリンク変換、送信遅延、遮断などフィルタ動作が適用されたメールです。

→ ウィルス(数量/割合%)： ウィルスが探知されたメールです。

→ 拒否(数量/割合%)： SMTP エンジンから接続自体が拒否されたメールです。

→ 合計： 送信、フィルタ動作、ウィルス、拒否など全てのメールの合計です。

4. 下記に、全体統計ページでの各機能に関して説明します。

→ グラフ: 送信、フィルタ動作、ウィルス、拒否など各統計をグラフで表示します。

→ 検索: 統計内容を検索します。 検索期間を設定した後、「検索」ボタンをクリックします。

→ ファイル保存: 統計内容を Excel ファイルとして保存します。

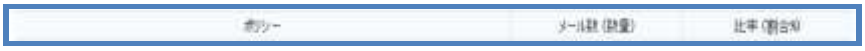
→ 更新間隔設定: リストの内容を自動で更新しますので、サーバ状態をリアルタイムでモニタリングできます。 更新は現在のデータ以外には必要がないので、検索期間終了日は使用当日になり、一番目のページでのみ動作します。更新機能は一度設定するとずっと適用されるので、カレンダーを使って検索期間を選択するなどの作業が必要な場合は、先に更新機能を中止してください。

8.2.2. ポリシー

MAILSCREENを通過したメールの中で、ポリシーにより遮断されたメールを統計で表示します。一番多く適用されたポリシーから降順にソートされます。

使用方法

1. 「SMTP Filter>統計>ポリシー」を選択します。
2. ポリシー統計ページが表示されます。
3. 下記に、ポリシー統計リストの各項目に関して説明します。



→ ポリシー: ポリシー名です。

→ メール数(数量): ポリシーが適用されたメールの数です。

→ 比率(割合%): 全体メールとポリシーが適用されたメールを割合(%)で表示します。

4. 下記に、ポリシー統計リストの上下にある各機能に関して説明します。

→ グラフ: ポリシーに関する統計をグラフで表示します。

→ 検索: 統計内容を検索します。検索期間を設定した後、「検索」ボタンをクリックします。

→ ファイル保存: 統計内容を Excel ファイルとして保存します。

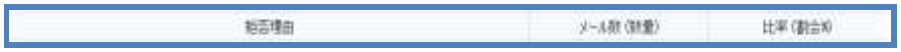
→ リスト数設定: 1 ページ当りに表示されるリストの表示数を設定します。

8.2.3. 拒否理由

MAILSCREENから受信拒否されたメールの統計を表示します。

使用方法

1. **「SMTP Filter>統計>拒否理由」**を選択します。
2. 拒否理由統計ページが表示されます。
3. 下記に、拒否理由統計リストの各項目に関して説明します。

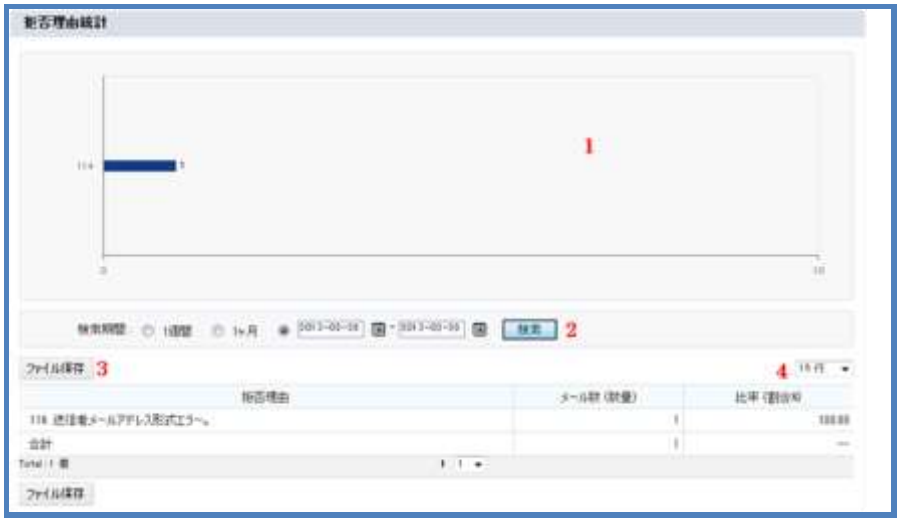


→ 拒否理由: メールが拒否された理由です。

→ メール数(数量): SMTP エンジンからメール受信が拒否されたメールの数です。

→ 比率(割合%):全体メールと受信拒否されたメールを割合(%)で表示します。

4. 下記に、拒否理由統計リストの上下にある各機能に関して説明します。



→ グラフ: 拒否理由メールの統計をグラフで表示します。

→ 検索: 統計内容を検索します。 検索期間を設定した後、「検索」ボタンをクリックします。

→ ファイル保存: 統計内容を Excel ファイルとして保存します。

→ リスト数設定: 1 ページ当りに表示されるリストの表示数を設定します。

8.2.4. 送信者ドメイン

MAILSCREENを経由して送信されたメールの送信者ドメインに関する統計を表示します。

使用方法

1. **「SMTP Filter>統計>送信者ドメイン」**を選択します。
2. 送信者ドメイン統計ページが表示されます。
3. 下記に、送信者ドメイン統計リストの各項目に関して説明します。

→ 送信者ドメイン: 送信者ドメインです。

→ フィルタ動作(数量/割合%): ポリシーによって、添付ファイル暗号化、 添付ファイルのリンク変換、 送信遅延、遮断などの誤送信動作が適用されたメールです。

→ ウィルス(数量/割合%): ウィルスが探知されたメールです。

→ 合計: 送信、フィルタ動作、ウィルス、拒否など全てのメールの合計です。

4. 下記に、送信者ドメイン統計リストの上下にある各機能に関して説明します。

→ グラフ: 送信者ドメイン統計をグラフで表示します。

→ 検索: 統計内容を検索します。検索期間を設定した後、「検索」ボタンをクリックします。

→ ファイル保存: 統計内容を Excel ファイルとして保存します。

→ リスト数設定: 1 ページ当りに表示されるリストの表示数を設定します。

9. システム状態

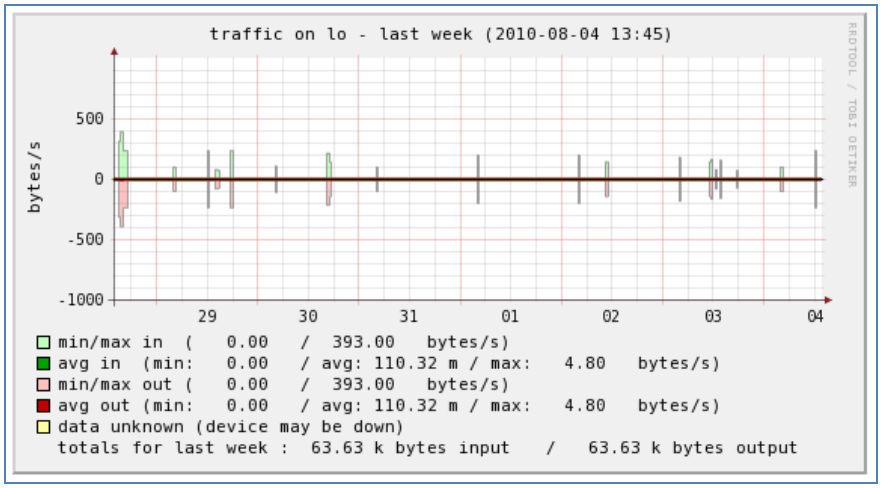
MAILSCREENサーバのシステム状況をグラフで確認できます。

9.1. ネットワーク使用率

MAILSCREENが設置されたサーバのネットワーク使用率を表示します。

使用方法

1. 「システム状態>ネットワーク使用率>lo、eth0、br0」の中で状況を確認する項目をクリックします。
2. last hour、last 6 hour、last day、Last week、Last month、Last year を基準にしてサーバのネットワークデバイスとの使用率に関するグラフが表示されます。

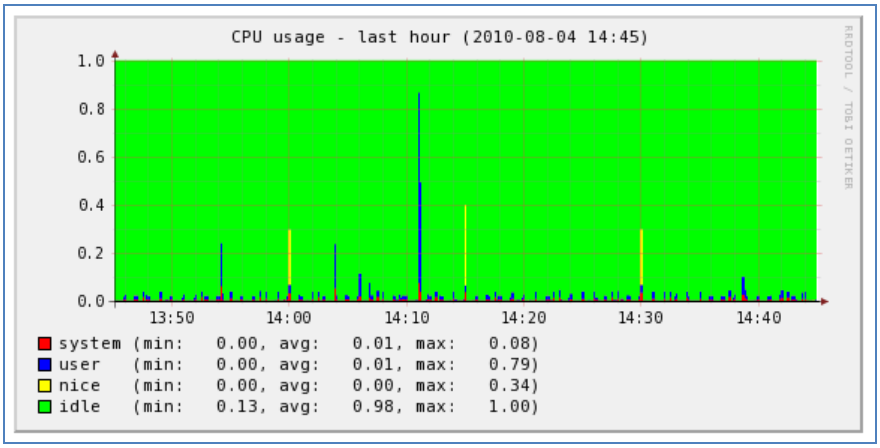


9.2. システムリソース

MAILSCREENのシステムリソース使用率を表示します。

使用方法

1. **「システム状態>システムリソース」**にて CPU、プロセス、システム負荷、ユーザ数、 メモリー、スワップ領域の中で状況を確認する項目をクリックします。
2. last hour、 last day、 Last week、 Last month、 Last year を基準にしてサーバのシステムリソース使用率に関するグラフが画面に表示されます。

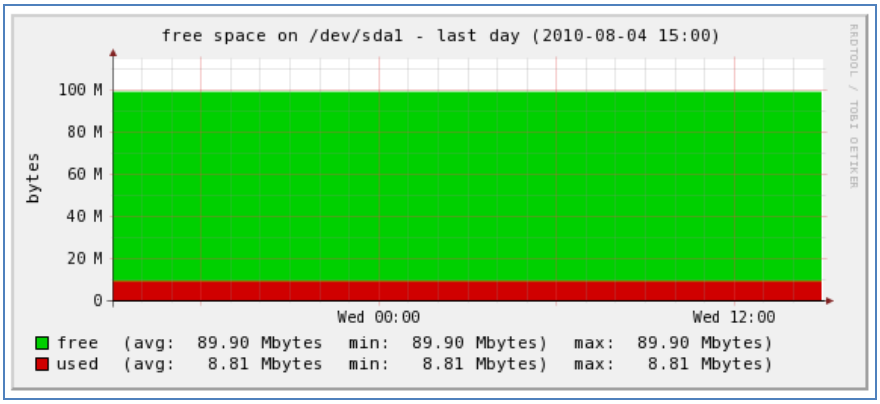


9.3. ディスク使用率

サーバのハードディスクの使用状況を表示します。 ハードディスクの空き領域が足りないと、メール処理を正常に処理できないので、空き領域を確保する必要があります。

使用方法

1. **「システム状態>ディスク使用率」**にて、/sniper、/boot、 /の中で状況を確認する項目をクリックします。
2. last day、 Last week、 Last month、 Last year を基準にしてサーバのハードディスク使用率に関するグラフが表示されます。



10. Appendix

10.1. 参照

10.1.1. 時間形式文字

MAILSCREENがサポートする時間形式文字は下記の通りです。

形式文字	説明	返還値(例)
a	午前と午後、 小文字	am、 pm
A	午前と午後、 大文字	AM、 PM
B	スワッチインターネット時間	000 から 999
d	日、2桁	01 から 31
D	曜日、 3文字	Mon から Sun
F	月、 January、 March などのフル文字	January から December
g	時、 0が付かない 12時間形式	1 から 12
G	時、 0が付かない 24時間形式	0 から 23
h	時、 0が付く 12時間形式	01 から 12
H	時、 0が付く 24時間形式	00 から 23
i	分、 0が付く形式	00 から 59
j	日、 0が付かない形式	1 から 31
l(小文字 ‘L’)	曜日、 フル表示形式	Sunday から Saturday
m	月、 数字表示、 0が付く形式	01 から 12
M	月、 短縮表示、 3文字	Jan から Dec
n	月、 数字表示、 0が付かない形式	1 から 12
O	グリニッジ時間(GMT)との差	+0200
r	RFC 2822 形式日付	Thu、 21 Dec 2000 16:01:07 +0200
s	秒、 0が付く形式	00 から 59
S	日表示の英語接尾語、 2文字	st、 nd、 rd ・・・ th
t	与えられた月の日数	28 から 31
T	マシンの標準時間帯設定	EST、 MDT
U	UNIX Epoch(January 1 1970 00:00:00 GMT) からの秒	1165306680
w	曜日、 数字	0(日曜日) から 6(土曜日)
W	ISO-8601 年度の週次、 週は月曜日から始まる	42(年の42番目の週)
y	年、 2 桁表示	99、 03
Y	年、 4 桁表示	1999、 2003
z	年の日次 (0 から始める)	0 から 365
Z	標準時間帯のオフセット秒、 UTCから西の方のオフセットは常に－(マイナス)で、東のオフセットは常に＋(プラス)	-43200 から 43200

10.1.2. 時間形式の適用範囲

「環境設定>システム>基本情報」で設定された時間形式が表示される範囲について説明します。

日付、 時間のみ表示	SMTP Filter>メール>メール履歴 SMTP Filter>メール>添付履歴 SMTP Filter>メール>メールリンク SMTP Filter>メール>拒否履歴
年月日を含んだ日付、 時間を表示	SMTP Filter>メール>拒否履歴日付ツールチップ SMTP Filter>メール>メール履歴日付ツールチップ SMTP Filter>メール>メール履歴>ファイル保存でファイル名に日付、時間 SMTP Filter>ポリシー>Black List SMTP Filter>ポリシー>White List ライセンス満了警告メール
時間帯を含んだ日付、 時間	SMTP Filter>メール>キュー状態 バックアップ結果お知らせメール ウィルス管理>ウィルス検査設定 ウィルス管理>VPS フィルタップデート日付

10.1.3. 添付ファイルの内容フィルタリングのサポートファイル形式

添付ファイル内容フィルタリングは、添付ファイルの内容が CP 949 互換文字列(EUC-KR、KSC5601、US ASCII、ISO-8859-1 位)の場合にのみ可能です。EUC-KR または KSC 5601、KSX1001 に対します説明は、RFC 1557、http://en.wikipedia.org/wiki/Extended. Unix. Code#EUC-KR、http://www.standard.go.kr/code02/user/0B/03/SerKS. View.asp を参照し、CP 949は http://www.microsoft.com/globaldev/reference/dbcs/949.mspx を参照してください。MAILSCREENは、下記のような形式の添付ファイルに関してフィルタリングをサポートします。

(MS-Office (.doc、.ppt、.xls) ファイルは MS-Office 96バージョン以上をサポートします。

拡張子	説明
.doc, .docx	Microsoft Word 95、97、2000、XP(2002)、2003、2007
.ppt, .pptx	Microsoft PowerPoint 95、97、2000、XP(2002)、2003、2007
.xls, .xlsx	Microsoft Excel 95、97、2000、XP(2002)、2003、2007
.hwp	Hangul Word Processor Document 2.x、3.x、96、97、2002、2004、2005、2007
.pdf	Adobe Acrobat 4.x、5.x、6.x、7.x、8.x (PDF 1.xサポート)
.ods	Open Office スプレッドシート 1.x、2.x
.odp	Open Office プレゼンテーション 1.x、2.x
.odt	Open Office Word 1.x、2.x
.rtf	Rich Text Format
.hwd	Presentation
.jtd	一太郎:日本で使われるワードプロセッサー
.mdi	Microsoft Document Imaging
.msg	Microsoft Outlook Message
.wpd	Wordパーフェクト 4.x 、13.x
.dwg	Autodesk Drawing File R11-R14、2000、2004、2005
.swf	Flash Movie File 2 - 8
.zip	圧縮ファイル
.tar	圧縮ファイル
.gzip	圧縮ファイル
.alzip	圧縮ファイル
.bzip	圧縮ファイル
.xml	Xml ファイル
.html	Html ファイル
.mht	MHT ファイル
.chm	CHM ファイル
.eml	EML ファイル
.mime	MIME ファイル
.txt	テキストファイル
.text	テキストファイル
.mp3	Multimedia File、MPEG Audio Stream Layer

10.2. 注意事項

システム性能に影響を及ぼす設定に関して説明し、円滑な管理のための情報を提供します。

■ **ウィルスメール送信**

基本的にMAILSCREENはウィルスメールを駆除した後、そのコピーのみを保存してメールサーバには送信しません。もし、「ウィルス管理>ウィルス検査設定」で ‘受信メールのウィルス駆除後、自動送信’ オプションを設定する場合には、メールを送信します。
しかし、最近はメールウィルスが爆発的に増えているので、このオプションを設定する場合、メールサーバの負荷とユーザの不便を引き起こす恐れがあるので、なるべく使用しない事を推奨します。

■ **メールサイズ制限**

フィルタリング・エンジンがメールを検査する時、メールサイズが大きい場合は負荷が掛かります。大きいサイズのメールは一時的に負荷が高くなるので、フィルタリングするメールサイズを制限する事を推奨します。 メールは平均 20、30Kbytes 程度のサイズですので、これらを参考に、**「環境設定>フィルタリング> Scanner」**のフィルタリング設定で ‘メール本文の検索サイズ’ を適切に設定するようにします。

■ **分散環境**

MAILSCREENを、分散処理として設置した場合、次の UIは使用できなくなりますので、ご参考ください。

環境設定>サービス>サービス制御

環境設定>サービス>時間帯

・本書はトライポッドワークス株式会社（以下弊社）が作成したもので、すべての権利は弊社が所有します。
弊社に無断で本書の一部または全部を転載、複製、改変を行うことは禁じられています。
・本書に記載されている他社製のソフトウェア及び周辺機器は、一般に各社の登録商標です。
・本書に記載された内容は予告なく変更される場合がありますので、あらかじめご了承ください。
・改良のため予告なく本製品の仕様を変更することがありますので、あらかじめご了承ください。
・本製品は日本国内でのみ使用することを前提としており、外国の規格などには準拠しておりません。
日本国外で使用された場合、弊社はいかなる責任も負いかねます。
・本製品は本書に記載された使用方法に沿ってご使用ください。特に、注意事項として記載された事項に反した使用はおやめください。

2013 年 2 月 初 版

トライポッドワークス株式会社