MailScreen 管理者マニュアル

日付	バージョン	版数
2017/2	3.3.3	初版

目次

1. 紹介

本章は、MailScreen(以下、MailScreen)に対する全般的な紹介を目的とし、MailScreen 概要、システム機能、用語の定義等を記述します。

1.1. MailScreen とは？

MailScreen は、社内から外部へ発信されるメールに対する統制と管理機能を提供する情報漏洩遮断システムです。

社内のメールを外部へ送信する前にメールのタイトル、送信者、受信者、本文と添付ファイルなどの重要な情報が含まれているかどうかのフィルタリングを実行し、設定に応じて添付ファイルの暗号化、添付ファイルリンク変換、決裁、送信遅延、遮断等のポリシーを適用し、企業の内部情報の流出を防止します。

MailScreen は一般的に2つの方式で設置します。ブリッジ(Bridge)方式は、 [図 1 ネットワーク構成 – Bridge]のようにメールサーバの前に物理的に設置します。プロキシー(Proxy)方式は、メールサーバが Smart Host の設定でメールが MailScreen で転送されるようにします。

図 1 ネットワーク構成– Bridge

1.2. Web-Admin とは?

Web-Admin は、MailScreen を管理する Web アプリケーションで、管理者の UI アクセシビリティを高め、メール検索、設定、ポリシー管理等の作業が可能です。

次の [図 2 Web-Admin 画面]は、Web-Admin の画面全体を示したものです。Web-Admin 画面は大きく、メインメニュー、リストメニュー、内容画面に分類されます。

メインメニューには SMTP Filter、ウィルス管理、ユーザ管理、環境設定、システム状態があり、メインメニューを選択するとリストメニュー領域に詳細メニューが表示されます。

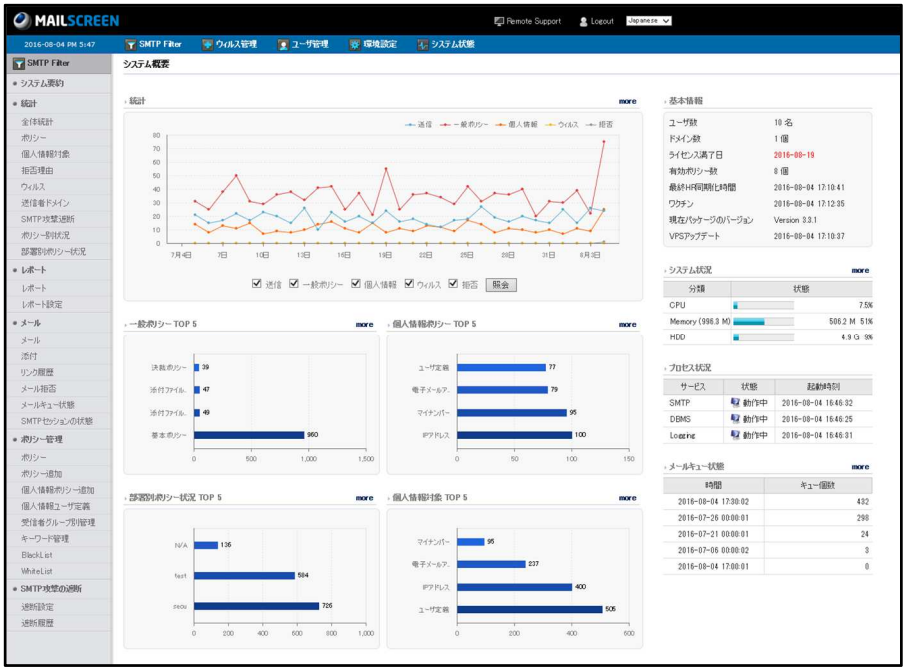


図 2 Web-Admin 画面

1.3. MailScreen の主な機能

MailScreen は、次のような機能を持っています。

- **便利な管理環境**

  MailScreen の制御と管理をより簡単にするために Web-Admin を提供しています。Web Admin は、MSIE、Firefox ブラウザと互換性があり、韓国語、英語、日本語などの言語インターフェイスをサポートします。Web-Admin を介して MailScreen サーバのすべての管理機能を実行することができ、サーバの状態と機能の動作に関連した重要なイベントに対する監査を記録/保存/検索できます。

- **企業内部情報漏えい防止**

  電子メールのヘッダと本文の内容、添付ファイルなどに対してリアルタイムで context パターンを検索します。ポリシーに基づいて添付ファイルの暗号化、添付ファイルリンク変換、送信遅延、決裁、ルーティング別指定、転送等の 9 種に細分化されたメール処理機能で強力な内部情報漏洩防止機能を提供しています。

- **バックアップおよび災害予防環境を提供**

  MailScreen は、データ損失に備えたバックアップおよび復元機能を提供しており、安全なサービスを提供するために、周期的にシステムの状態を自己診断テストしています。また、監査およびメール保存位置、サービス、メールキュー、DBMS の状態検査時の異常を発見した場合、管理者に警告メールを送信します。

1.4. クライアントシステム要件

次は MailScreen が動作するためのクライアントの推奨動作環境です。

表 1 Web-Admin 使用環境

H/W	Display：解像度 1024 x 768
S/W	MSIE 8.0 以上、 Firefox 3.0 以上
	SSL 通信およびクッキー(cookie)/JavaScript 使用可能
OS	UTF-8 文字列をサポートする運用環境

1.5. 用語説明

- **SMTP(Simple Mail Transfer Protocol)**
  メールを送受信するために使用されます。ユーザが送信したメールを別の場所に転送する役割を担当します。 自身が A という会社に所属しているとしたときに、ユーザが外部ユーザにメールを送ることは、A 社の内部 SMTP でメールを送信することです。一旦ユーザのメールを受信した A 社の内部 SMTP はメールの受信者メールドメインを参照して、適切な外部 SMTP サーバを探し、そこにユーザのメールを送信します。送信試みが成功して外部 SMTP がメールを受信した場合、外部ユーザはメールをもたらすことができるようになります。つまり、SMTP は郵便局と似たような概念といえます。詳細は RFC821 を参照してください。

- **MUA(Mail User Agent)**
  メールを送信する主体。ほとんどが Outlook Express または Becky 等のメールクライアントプログラムを意味するが、SMTP もメールを他の SMTP で発送するときは MUA と見なされます。

- **メールサーバ**
  メールを処理する会社内のメールサーバ。特別な言及がない場合は、以後の説明で表示されるメールサーバは、MailScreen と連動した会社メールサーバを指します。

- **リレー(Relay)**
  SMTP がメールを受信した後、そのメールを再度受信者メールドメインが担当する SMTP に伝達してくれる行為です。MailScreen の場合は、受信者メールドメインがメールサーバでない場合でも、メールを受信して外部メールサーバに転送する場合は、これをオープンリレーとします。

- **マイム(MIME： Multipurpose Internet Mail Extensions)**
  制限されたメール標準を拡張させメール内容に多種なオブジェクト(テキスト、HTML、添付ファイル、多言語メッセージ等)を含めるための規格です。この規格を利用すると、単一のメールにテキストと HTML、添付ファイルを同時に含めることができます。RFC822 を参照してください。

- **スキャナ(Scanner)**
  MailScreen のフィルタリングに関与してフィルタリングを実行するモジュールを指します。

- **発送**
  メールを送信する行為を指します。

■ **受信**

メールを受信する行為または登録されていないドメインの送信者から登録されたドメインの受信者がメールを受けること。

■ **受信者**

メールを受信するように指定されたユーザまたはそのユーザのメールアドレスを指します。

■ **発信者**

メールを送ったことが指定されたユーザまたはそのユーザのメールアドレスを指します。

■ **正規式**

文字列間の関係を示す規則を表現する方法で、特定の規則を持った文字列を検索したり変換したりするときに使用されます。MailScreen は、正規式処理のために PCRE を使用しています。詳細については http://pcre.org を参照してください。

■ **コピー**

MailScreen が受信したメールのコピーです。コピーは、サーバに保存されて、復旧、分析等に使用されます。

■ **拒否**

メールが SMTP 段階で受信が拒否されること。MailScreen にメールを送信しようとしていた SMTP または送信者はメールの送信に失敗したという応答コードが表示されます。発送主体が通常の SMTP であれば、この場合与えられた試行回数だけ一定間隔でメール送信を試みます。メールが拒否されるとコピーを保存しません。

■ **復旧**

MailScreen によって遮断されたメールを必要により元の受信者がメールを受信できるようにメールサーバに送信する行為を指します

■ **ブリッジモード**

ユーザが送信したメールがメールサーバに転送される途中のネットワークデータ(パケット)を奪い、MailScreen が処理するようにした設置方式です。

■ **SSO(Single Sign On)**

Web ベースのサービス間で相互認証を共有することです。例えばサイト A と B があるとすると、ユーザが A にログインし、B にログインしていなかったとしても A にログインした情報を共有して B のサービスも自由に利用できるようにする方法です。

■ **CIDR(Classless Inter-Domain Routing)**

000.000.000.000/N の形式でサブネットを含んだ IP アドレスを表記する方式です。http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing を参照してください。

■ **エンベロープ情報、SMTP エンベロープ(SMTP Envelope Data)**

SMTP がメールを受信するときにはエンベロープ情報とメールデータを必要とします。メールデータとはヘッダを含むメール内容(メール原本)を含んでいます。エンベロープ情報は、送信者と受信者を指定します。SMTP 標準はエンベロープ情報の送受信者とメールデータのヘッダに指定された送受信者の情報が一致していなくても受信を許可します。SMTP はメールデータの受信者を無視し、エンベロープ情報の受信者がメールを受信するユーザだと見なされます。

- **FQDN(Fully Qualified Domain Name)**
  DNS に登録されたドメイン名。ホスト名とドメイン名、TLD(Top Level Domain)で構成されます。例えばホスト名 www に対する jiran.com の FQDN は、www.jiran.com です。URL とは異なる概念で、ドメイン名またはホスト名と呼ばれることもあります。

- **MX(Mail eXchange)**
  メールサー(SMTP)の DNS 情報です。ドメインの MX レコードを検索するとメールサーバの情報を知ることができます。

1.6. 文書規約

本書で使用される各種の表記規則を定義します。

- **太文字**
  参照する他の文書のタイトルまたは文書内各章の番号およびタイトル、強調する内容を表示します。

- **[ ]**
  ボタンまたは選択するメニューを表示します。

- **‘ シングルクォーテーション’**
  パラメータ項目を表示するときに使用します。

- **注意事項**
  ユーザが注意する事項に対して説明するときに表示します。

- **>**
  下位メニューに移動する場合、移動順序を表すために使用します。

- ***斜体***
  上段のメインメニューを表示するとき使用します。

2. ログイン

MailScreen の管理業務を実行するためには、まず Web-Admin ページにログインをする必要があります。

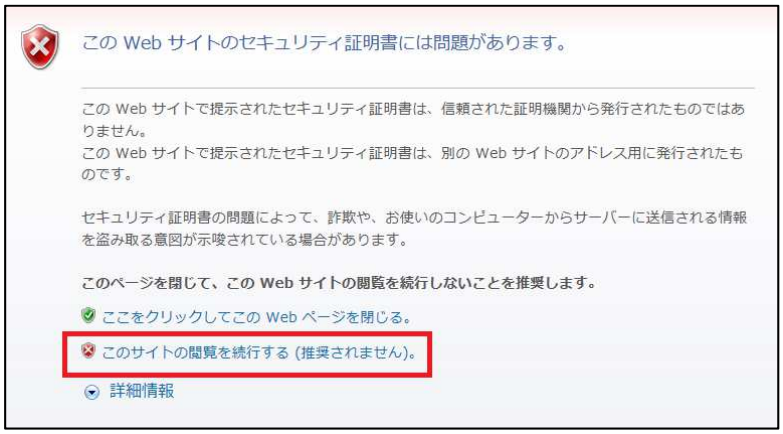
2.1. ログイン

設定方法

1. 管理者の Web ブラウザを起動します。
2. Web ブラウザのアドレス入力欄に 'http://<MailScreen が設置されている IP またはドメイン名>'、または 'https://<MailScreen が設置されている IP またはドメイン名>'を入力します。

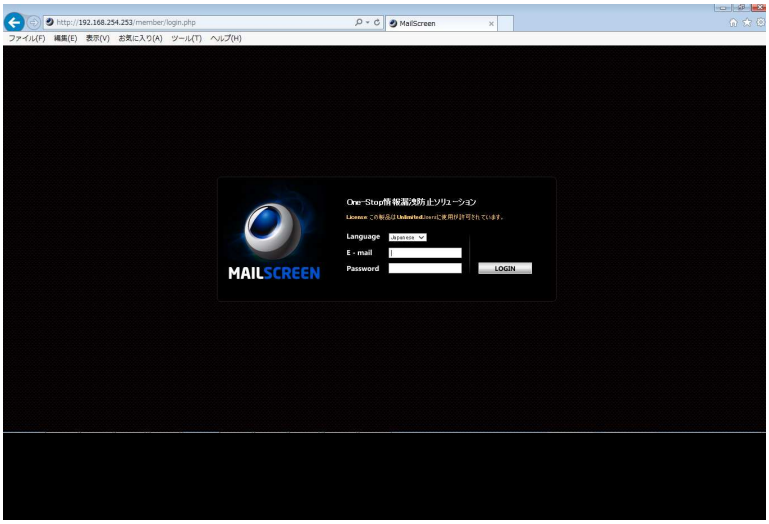
注意事項

× 'https://'を入力した場合、セキュリティ認証の警告メッセージ画面が出力されたとき[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。



/

3. ログインページが出力されると次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 画面で使用する言語

→ E-mail：空白ではない 1 文字以上の E-mail アカウント

→ Password：英大小文字と数字および特殊文字で構成された 8～40 文字

4. 入力した E-mail アカウントとパスワードでログインに成功した場合、統計画面が出力され失敗した場合には失敗したことを知らせる結果画面が出力されます。

注意事項

- × Password 規則情報は*環境設定*>システム>アクセス制御の 'パスワード複雑度検査およびパスワード最小長さ'設定によって組み合わせ規則が変更されることがあります。
- × *環境設定*>システム>アクセス制御の 'アカウントロック'値以上ログインに失敗した場合、該当アカウントは、'アカウントロックの時間'の間非活性化されます。
- × 非活性化された後、1回追加で間違った時点から 'アカウントロックの時間'が追加されます。
- × 非活性化終了後、アカウントが活性化になった状態でログインに成功した場合に限りログイン失敗の回数カウントが初期化されます。
- × ログインに成功した後、一定時間 Web-Admin を使用してセキュリティ管理活動を行わない場合は、ログインしていたセッションは終了されます。

3. ユーザ管理

MailScreen を利用して内部情報漏洩を防止するためには、まずはユーザ情報を登録しなければなりません。本章ではユーザ管理のための情報の設定方法について説明します。

3.1. ユーザ管理

MailScreen のユーザは個人ユーザとスーパー管理者、ログ閲覧者、決裁者で区分されます。ユーザ権限に応じた説明は次のとおりです。

権限	説明
スーパー管理者	MailScreen のすべての機能を実行できます。
ログ閲覧者	統計およびメール管理機能のみ実行できます。
決裁者	ユーザの決裁権者に設定された場合、権限が生成され、自身が送信したメールおよび被決裁者が送信したメールのうち、ポリシーが適用されたメールについて照会および決裁関連機能のみ実行できます。
個人ユーザ	一般ユーザを意味し MailScreen にアクセスする権限および管理権限がありません。

3.1.1. ユーザ管理

設定方法

1. *ユーザ管理*>ユーザ管理をクリックします。
   ユーザ管理リスト画面が出力されます。
2. ユーザリストの上部および下部の機能説明です。

→ 1_[削除]:選択したユーザを削除します。ただし、自分自身の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。追加の詳細説明は、3.1.2 ユーザ追加を参照してください。

→ 3_[ファイル保存]:ユーザリストをエクセルファイルとして保存します。

→ 4_リスト数設定:ページごとの表示されるユーザ数を設定します。

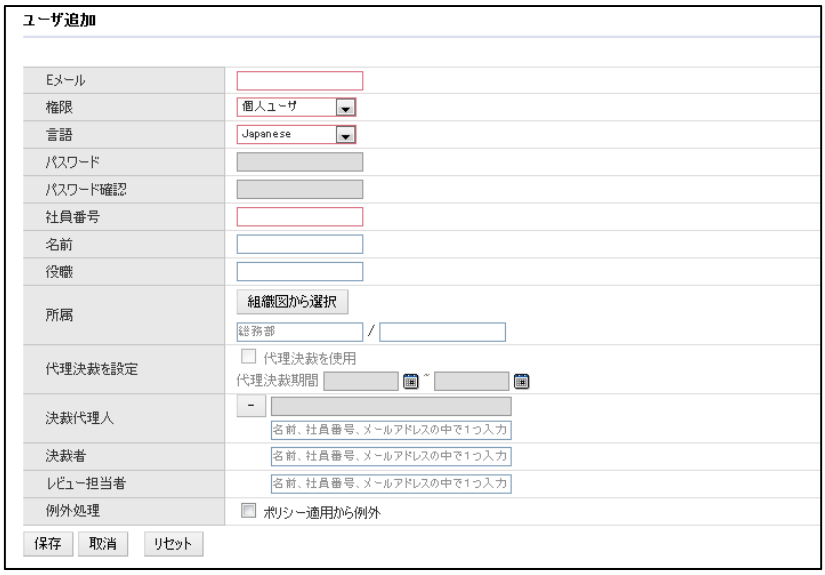
→ 5_情報修正:ユーザ情報の'名前(E メール)'をクリックするとユーザ情報を修正できます。情報変更項目は 3.1.2 ユーザ追加を参考してください。

→ 6_[検索]:検索条件(名前、Eメール、社員番号、権限、所属、決裁者)を選択し、検索用語を入力します。[検索]ボタンをクリックすると検索されたユーザ情報が画面に表示されます。

3.1.2. ユーザ追加

設定方法

1. *ユーザ管理*>ユーザ管理をクリックします。
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. ユーザの追加画面で次の値を入力します。



→ メール:ユーザの E メールでログインとメール受信に使用されます。

→ 権限:権限(スーパー管理者、決裁者、ログ閲覧者、個人ユーザ)を設定します。

スーパー管理者	MailScreen のすべての機能を実行できます。
ログ閲覧者	統計およびメール管理機能のみ実行できます。
決裁者	ユーザの決裁権者で設定される場合、権限が生成されて、自身が送信したメールおよび被決裁者が送信したメールのうち、ポリシーが適用されたメールに対して照会および決裁関連機能のみ実行できます。
個人ユーザ	一般ユーザを意味し、MailScreen にアクセスする権限および管理権限がありません。

→ 言語:画面表示に使用する言語を設定します。3 種類の言語(English、Korean、Japanese)をサポートします。

→ パスワード:ログインに使用するパスワードを設定します。パスワードは英大小文字、特殊文字と数字を含む 8~40 文字以下で構成する必要があります。ユーザの権限が個人ユーザの場合、[*環境設定*>システム>アクセス制御>ログイン情報>ログイン方法]を[登録アカウント検査]に設定しなければパスワードを設定することができません。

→ パスワード確認:パスワード項目に入力した情報を再入力します。

→ 社員番号:ユーザに付与された社員番号を入力します。社員番号は英大小文字、特殊文字と数字を含む 1~32 文字以下で構成する必要があります。

→ 名前:ユーザ名を入力します。

→ 役職:ユーザの役職を入力します。

→ 所属：ユーザの所属情報を入力します。[組織図から選択]ボタンをクリックすると既に入力されている組織図リスト画面で所属情報を選択できます。

→ 代理決裁を設定：決裁者が決裁業務を行えない場合、決裁代理人に決裁要請が行われます。決裁代理人および決裁の委任可否と決裁代理期間を入力します。

→ 決裁代理人：決裁代理人を設定します。1人だけ設定できます。

→ 決裁者：決裁者を設定します。空欄に入力することにより追加でき、最大 5 人まで設定できます。[−]ボタンにより削除することができます。

→ レビュー担当者：レビュー担当者を設定します。ポリシー追加時にポリシー通知オプションおよび通知方法に BCC で通知メールが送信されます。空欄に入力することにより追加でき、最大 5 人まで設定できます。[−]ボタンにより削除することができます。

→ 例外処理：ポリシー適用の例外可否を設定します。例外設定した場合、該当ユーザはポリシーの適用を受けません。

注意事項

× 赤枠で作られた入力欄は必須入力項目です。

× パスワード規則情報は*環境設定*>システム>アクセス制御の 'パスワード複雑度検査およびパスワード最小長さ'設定により組み合わせ規則が変更できます。

× 決裁代理人、決裁者、レビュー担当者は既に登録されているユーザの中からのみ設定できます。

× 決裁代理人は決裁の代理期間中のみ適用されます。

× 決裁代理人の設定時の代理決裁期間は必須項目です。

× スーパー管理者および決裁者、ログ閲覧者は権限とそれに伴う責任について適切に教育を受けなければならず、すべての管理者の指示と行動の手順に従って正確に義務を履行する必要があります。

× 決裁者情報はポリシー設定項目のうち（4.1.2 ポリシー追加を参照）'人事情報の決裁者に決裁要請'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ますので正確に記入する必要があります。

× 代理決裁を設定できるのは権限が個人ユーザではできません。

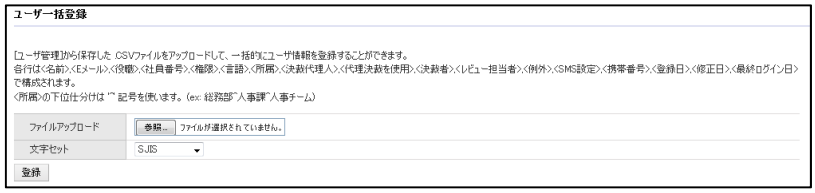
4. [保存]ボタンをクリックします。[リセット]ボタンをクリックした場合、入力されたすべての情報が初期化されます。

3.1.3. ユーザー括登録

CSV ファイルを利用して複数のユーザ情報を一括に登録できます。

設定方法

1. *ユーザ管理*>ユーザー括登録をクリックします。
2. ユーザの一括登録画面で次のオプションを設定した後、[参照]ボタンをクリックして 。CSV 形式のファイルをアップロードします。



→ 文字セット：アップロードファイルの文字セットがシステムの文字セットと異なる場合、一括登録時に文字化けすることがありますので、アップロードファイルの文字セット

を設定します。ユーザが設定の容易さのためにデフォルトで*環境設定*>システム>基本情報>言語設定での値が自動的に選択されます。

-

注意事項

- × 一括登録時のファイルは、CSV ファイル形式を持つ必要があります。
- × ファイルに保存されている人事情報はユーザの追加項目と同じ順で保存されている必要があります。
- × 社員番号は英大小文字と一部の特殊文字、数字を含む 1～32 文字以下で構成する必要があります。
- × ユーザ情報の所属は、各段階で '^'の区切り文字で表示されている必要があります。ex)総務部^人事課^人事チーム
- × アップロードファイルのユーザと既に登録されたユーザが重複する場合は、登録内容を更新します。
- × 既に登録されたユーザがアップロードファイルに存在しない場合は、既存ユーザは削除されます。
- × ただし、スーパー管理者/ログ閲覧者アカウントは、追加および修正、削除はされません。
- × 新しく登録されたユーザは、規定の権限が個人ユーザとなり、決裁者もしくは決裁代理で指定されたユーザのみ決裁者として自動的に設定・割り当てられます。

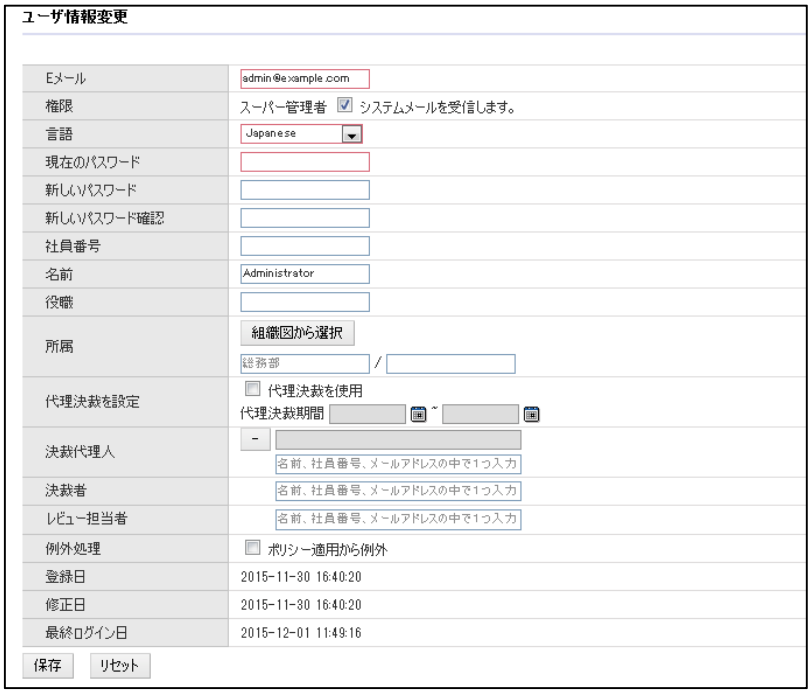
3. 下部の [登録]ボタンをクリックします。

3.1.4. ユーザ情報変更

現在ログインされているユーザの情報を変更します。

設定方法

1. *ユーザ管理*>ユーザ情報変更をクリックします。
2. 現在ログインしているユーザの情報変更画面が出力されます。各項目の詳細説明は、3.1.2 ユーザ追加を参照してください。



注意事項

× 社員番号、役職、所属、決裁者、レビュー担当者項目は、ポリシーに影響を与えますのでスーパー管理者を除いて変更することはできません。

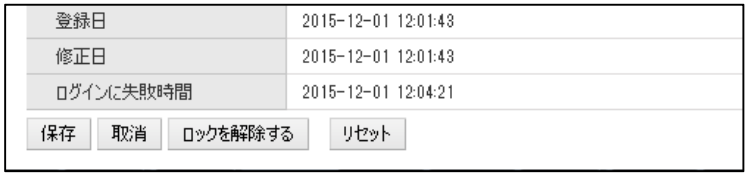
3. 情報を修正した後 [保存]ボタンをクリックします。

3.1.5. ユーザアカウントロック解除

ユーザがログイン失敗回数を超えた場合、アカウントがロックされます。アカウントがロックされた場合、アカウントのロックを解除します。

設定方法

1. *ユーザ管理*>アカウントがロックされたユーザを検索>ユーザ情報の変更をクリックします。
2. 現在のアカウントがロックされているユーザの情報変更画面が出力されます。各項目の詳細説明は 3.1.2.ユーザの追加を参照してください。



注意事項

× 社員番号、役職、所属、決裁者、レビュー担当者項目は、ポリシーに影響を与えますのでスーパー管理者を除いて変更することはできません。

× アカウントがロックされた場合は、最後のログイン時間、もしくはログイン失敗時間で確認することができます。

3. 下部の[ロック解除]ボタンをクリックします。

3.1.6. ユーザ情報連動

組織図を連動するために連動ページを提供します。

設定方法

1. *ユーザ管理*>ユーザ情報連動をクリックします。
2. 連動設定画面が出力されます。各項目を設定した後、下部の[保存]ボタンをクリックします。

→ DBMS 接続情報:連動する DBMS の情報を設定します。

- DBMS 種類:連動するサーバの種類にあわせて Oracle、MSSQL、Mysql のいずれかを選択します。
- DBMS ユーザ名前:アクセス可能なユーザ名を設定します。
- DBMS ユーザパスワード:上記のユーザのパスワードを設定します。
- DBMS 接続:サーバ情報を入力します。Oracle の場合、サーバ IP:ポート/SID、MSSQL、Mysql の場合は、サーバ IP:ポートの形式です。
- [接続テスト]ボタンをクリックし連動するサーバとの接続が成功していることを確認します。
- 各項目の値が1つでも存在していない場合は保存時にエラーが発生します。

→ ユーザ情報の同期のオプション:連動時のオプションを選択します。

- ユーザ情報のオプション:社員番号を使用しない場合、ユーザ情報 DBMS 社員番号フィールド必須チェックを外します。また、連動するサーバが ANSI_NULL、 ANSI_WARNING のオプションを必要とする場合にはチェックを行います。

→ ユーザ情報クエリ:MailScreen で提供するビューに合わせてクエリを作成します。

- 各クエリに対して[テスト]ボタンをクリックしてテストを行うことができます。Select 文にのみ適用され結果は 1 Row に通知出力されます。テスト時にクエリが存在しないか適切でなかったクエリの場合はエラーを通知します。

注意事項

× ユーザ情報連動設定時は DBMS との同期に影響があります。正確に設定していない場合は、ユーザ管理が困難となります。

4. ポリシー管理

MailScreen は、適用および管理のためのポリシーを細分化して提供しています。メールのヘッダとタイトル、本文内容を検査してフィルタリングするポリシー、SMTP 段階で IP およびドメイン、E メールをフィルタリングする Black/WhiteList、重要な取引先のような許可された宛先をあらかじめ登録して管理する許可受信先ポリシー、マイナンバー、クレジットカード番号などの個人情報保護管理ポリシーに区分されます。細分化されたポリシーに柔軟なポリシーの適用と容易な管理をすることができます。

注意事項

× MailScreen は、ポリシーに設定されたフィルタの検査時、英大小文字を区別しません。したがって、BlackList および WhiteList、ポリシー追加、許可受信先登録の時に注意してください。

4.1. ポリシー

ポリシーは、企業の情報漏洩防止を目的としており、MailScreen を通過するすべてのメールを検査、処理し企業の情報漏洩を防止します。

4.1.1. ポリシー管理

設定方法

1. *SMTP Filter*>ポリシー管理>ポリシーをクリックします。
2. ポリシーの一覧画面が出力されます。
3. ポリシーの一覧リストの上部および下部の機能説明です。

→ 1_[検索]：'ポリシー名/適用対象（適用対象および所属）/フィルタ内容（フィルタリング値）/例外対象（例外対象および所属）/フィルタ動作/使用可否/フィルタ種類/添付の処理'のうち、検索値を選択または入力した後、[検索]ボタンをクリックします。各項目に詳細については、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。詳細については、4.1.2 ポリシー追加を参照してください。

→ 4_[個人情報ポリシー追加]:個人情報ポリシーを追加します。詳細については、4.2 個人情報ポリシー管理を参照してください。

→ 5_リスト数設定:ページごとの表示されるポリシー一覧の数を設定します。

→ 6_優先順位:ポリシーの優先順位を設定します。最初のポリシーの優先順位が最も高いです。

→ 7_使用可否:使用可否を設定します。

→ 情報変更:ポリシー変更項目のうち、ポリシー名をクリックすればポリシー内容を変更することができます。情報変更項目は、4.1.2.ポリシー追加を参照してください。

注意事項

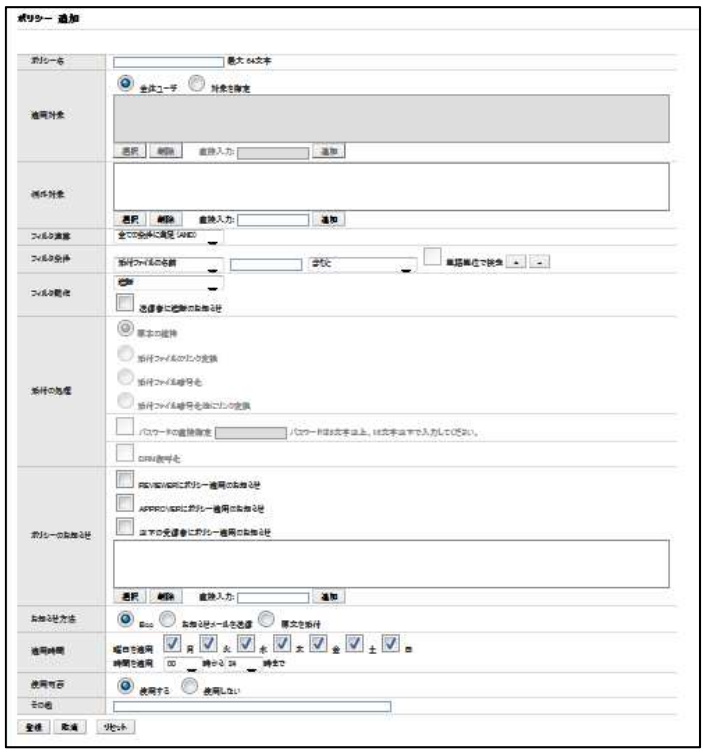
× ユーザの使いやすさのために基本ポリシーを提供しています。変更/削除が可能です。

× 設置言語が英語または日本語の場合は、すべてのメールに対して送信遅延を標準で提供しています。

4.1.2. ポリシー追加

設定方法

1. *SMTP Filter*>ポリシー管理>ポリシー>[ポリシー追加]ボタンまたは *SMTP Filter*>ポリシー管理>ポリシー追加をクリックします。
2. ポリシーの追加画面で次の値を入力します。



→ ポリシー名:ポリシーの名前を入力します。最大 50 文字まで入力することができます。

→ 適用対象:ポリシーが適用される対象を設定します。

- 全体ユーザ:MailScreen を通して送信されるすべてのユーザのメールに対してポリシーが適用されます。

- 対象を指定：指定された所属またはユーザが送信したメールに対してポリシーが適用されます。
  - ✓ [選択]：既に登録された組織図リストで選択できます。
  - ✓ [削除]：選択した所属またはユーザを削除します。
  - ✓ 直接入力：ポリシーの適用対象を直接入力できます。人事情報に存在しない社員に対するポリシーを設定できます。 'E メール'または'@ドメイン' 形式 ‘で入力する必要があります。

→ 例外対象：ポリシーが適用されない対象を設定します。適用対象より優先順位が高く、例外対象に設定された所属または社員が送信したすべてのメールは、該当ポリシーが適用されません。

- 対象指定：指定された所属またはユーザが送信したメールに対してポリシーが適用されます。
  - ✓ [選択]：既に登録された組織図リストで選択できます。
  - ✓ [削除]：選択した所属またはユーザを削除します。
  - ✓ 直接入力：ポリシーの適用対象を直接入力できます。人事情報に存在しない社員に対するポリシーを設定できます。 'E メール'または '@ドメイン' 形式' で入力する必要があります。

→ フィルタ演算：メールや添付ファイル処理動作を実行するためのフィルタポリシー条件を設定します。

- すべての条件に満足(AND)：該当ポリシーに設定されたすべてのフィルタ条件を満たしている場合ポリシーを実行します。
- 1 個以上の条件に満足(OR)：該当ポリシーに設定されたフィルタのうち少なくとも1つ以上を満たしている場合ポリシーを実行します。

→ フィルタ条件：フィルタ条件は、フィルタリング対象、フィルタリング値、フィルタリング条件で構成されます。[+][−]ボタンを使用してフィルタ条件を追加・削除することができます。1つのポリシーにフィルタ条件の個数は制限をもっていませんが、最大 10 個までを設定することを推奨します。

- フィルタリング対象：メールのヘッタおよび本文内容、添付ファイルのようにフィルタリング対象を設定します。
  - ✓ タイトル：メールタイトルをチェックします。
  - ✓ 本文：メール本文の内容をチェックします。メール本文がいくつかのマイムで構成される場合すべてのマイムをチェックします。
  - ✓ 本文+添付ファイルの内容：メール本文および添付ファイルに対してフィルタリングを実行します。
  - ✓ ヘッダ送信者：メールの送信者(From)をチェックします。ヘッダ送信者とはユーザが Outlook 等のメールクライアントを通してメールを開いたときに表示される送信者情報を指します。
  - ✓ ヘッダ受信者：メールの受信者(To)をチェックします。ヘッダ受信者はヘッダ送信者とは対称に受信者情報を指します。
  - ✓ エンベロープ From： SMTP に伝達されるメールの Envelope Mail From 情報をチェックします。送信者がメールを送信するときに、メールを受信する SMTP は Envelope Mail 情報とメール内容を転送されます。この情報には

送信者、受信者情報があり、ヘッダ送信者、受信者情報とは異なる情報です。

- ✓ RCPT TO：SMTP に伝達されるメールの Envelope Mail To 情報をチェックします。
- ✓ Cc：メール参照者(CC)をチェックします。
- ✓ 外部の受信者：外部受信者とは受信者のドメインが MailScreen に登録されていないドメインを使用している受信者を指します。メール受信者のうち外部受信者の存在可否をチェックします。
- ✓ Content-type：メールの本文の形式情報をチェックします。Boundary 情報もこれに該当します。
- ✓ Reply-To：メールヘッダに書き込まれた返送アドレスをチェックします。
- ✓ X-Mailer：メールを送信するクライアントプログラム名をチェックします。
- ✓ IP：送信メールサーバの IP アドレスをチェックします。0～255 の数字を用いた正しい形式(x.x.x.x)の必要があり(dot)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チェックします。各ヘッダにその値にフィルタ値を対照する方式でチェックします。
- ✓ 受信者の全体数(名)：メール受信者数をチェックします。この数は To、Cc、Bcc に含まれたすべての受信者の合計値です。
- ✓ メール全体サイズ(KB)：メール全体のサイズをチェックします。Kbytes 単位で入力します。
- ✓ 添付ファイルの名前：添付されたすべてのファイルの名前をチェックします。対象の特性上 '空白ならば'条件はサポートしていません。
- ✓ 添付ファイルのサイズ(KB)：添付されたすべてのファイルのサイズをそれぞれチェックします。Kbytes 単位で入力します。
- ✓ 添付ファイルの個数(個)：添付されたすべてのファイルの数をチェックします。
- ✓ 添付ファイルの形式：添付されたファイルの形式（拡張子）をチェックします。
- ✓ 添付ファイルの内容：添付されたファイルの内容をチェックします。
- ✓ 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チェックします。
- ✓ キーワード：*SMTPFilter*>ポリシー管理>キーワード管理に登録されたデータを指します。キーワード内容は大小文字を区別せずに本文と添付ファイルをチェックします。キーワードリストから選択可能で適用回数を指定することができます。条件としては「含む」だけをサポートします。そのため条件を設定するエリアは非表示となります。
- ✓ 受信者グループ：*SMTPFilter*>ポリシー管理>受信者グループ別管理に登録されたデータを指します。受信者グループの受信者のリストを外部宛先で大小文字を区別せずにチェックします。受信者グループリストから選択可能です。仕組み上「含む」「含まない」のみサポートします。

注意事項

- ✕ データベースとしてキーワード、もしくは受信者グループが存在していないときにフィルタリング対象に選択した場合、それぞれの管理ページに移動するメッセージが表示され「OK」をクリックするとそれぞれのページに移動します。

- フィルタリング値:フィルタリング対象をチェックするために比較される値です。
- フィルタリング条件:フィルタリング値がフィルタリング対象にマッチされることを判断する基準です。
  - ✓ 含むと:フィルタリング対象の値にフィルタリング値が含まれていたり、一致したりした場合、マッチするものと判断します。
  - ✓ 含まない場合:フィルタリング対象の値にフィルタリング値が含まれていない場合は、マッチするものと判断します。
  - ✓ 一致すると:フィルタリング対象の値とフィルタリング値が正確に一致すると、マッチするものと判断します。
  - ✓ 始まると:フィルタリング対象の値がフィルタリング値で始まるとマッチするものと判断します。
  - ✓ 終わると:フィルタリング対象の値がフィルタリング値で終わるとマッチするものと判断します。
  - ✓ 正規式にマッチされる場合:正規式とは、特定の規則を持った文字列の集合を表現するために使用する形式言語で文字列の検索と置換をサポートします。この条件を選択した場合、スーパー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、意図とは別の方法で、より多くのメールをフィルタリングする結果をもたらすことができますので、常に注意する必要があります。正規式の構文の詳細については http://pcre.org/pcre.txt を参考にします。
  - ✓ 空白なら:フィルタリング対象の値が空白で構成されている場合、マッチするものと判断します。主に題タイトルが空白の場合をチェックするときに使用します。
  - ✓ より大きい場合:フィルタリング対象の値がフィルタリング値より大きい場合、マッチするものと判断します。
  - ✓ と同じ場合:フィルタリング対象の値とフィルタリング値が同じであればマッチするものと判断します。
  - ✓ より小さい場合:フィルタリング対象の値がフィルタリング値よりも小さい場合、マッチするものと判断します。

→ 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。各動作により入力項目が異なります。 'メールを保存しない'オプションを選択した場合、該当メールの原本は、サーバに保存されません。ただし、'メールを保存しない'オプションは、*環境設定*>システム>基本情報>言語のシステム言語が'korean'で設定された場合にのみ有効になります。

- 送信遅延:フィルタリングされたメールの送信を遅延させます。送信遅延時間は、最小 5 分からで最大 31 日まで設定できます。送信遅延オプションに対する追加説明は、7.3.4 送信遅延を参照してください。

注意事項

× 送信遅延時間が*環境設定*>システム>基本情報>メール保存期間設定の 'メール履歴'または 'メールのコピー'の保存期間より長い場合は、該当メールは、送信遅延されずに送信がキャンセルされます。該当オプションを確認後、遅延時間を設定してください。

× 内部ドメイン(*環境設定*>メールサーバ>メールサーバに登録されているドメイン)の受信者の場合、送信遅延ポリシーが適用されません。

× 送信遅延の有効期限または発信者/管理者による [すぐに送信]時、該当ポリシーの詳細条件(ex、添付の処理方法等)が適用されて送信されます。

- 遮断:受信者にメールを送信しません。'送信者に遮断のお知らせ'オプションを選択した場合、送信者に遮断のお知らせメールが送信されます。
- 通過:受信者にメールを直ちに送信します。特定メールに対してポリシーの適用の除外、監視の用途で多く使用される動作です。通過時、該当ポリシーの詳細条件(ex、添付の処理方法等)が適用されて送信されます。
- 決裁:メールの送信遅延を行い決裁者の決裁に応じて送信または遮断します。
  - ✓ 人事情報の決裁者に決裁要請:*ユーザ管理*>ユーザ管理の人事情報に登録された決裁者に決裁を要請します。
  - ✓ (特定指定者)に決裁を要求:所属に関係無く必要に応じて決裁者を指定できます。
  - ✓ 自動の処理オプション:設定値により一定時間以後に自動的に承認または却下されます。

注意事項

× '人事情報の決裁者に決裁要請'に設定した場合、人事情報に登録されている決裁者に決裁要請が行われます。よって人事情報登録時に決裁者情報を正確に記入する必要があります。決裁者情報がない場合、*環境設定*>フィルタリング>誤送信防止>決裁の '基本決裁者のメール'で設定した決裁者に決裁メールが送信されます。この 2 項目とも決裁者が指定されていない場合は、該当メールの決裁要請は、無期限待機することになるため人事情報と環境設定では必ず決裁者を指定するようにしてください。

× 送信者が決裁者の場合、自動的に承認され決裁処理が省略されます。

× 送信者がレビュー担当者のうちの 1 人であった場合、レビュー担当者リストから送信者は省略されます。

× 受信者にレビュー担当者が存在している場合、レビュー担当者リストから受信者は省略されます。

× すべてのレビュー担当者が送信者/受信者に含まれて除外される場合、ポリシー適用通知も省略されます。

× 人事情報に登録されている多数の決裁者の一人だけ決裁すれば決裁処理が完了します。

× 自動処理オプションを設定していない場合、決裁者が決裁要請メールに対する処理を実行するまで無期限待機します。

× メールの保存期間(*環境設定*>システム>基本情報>メールの保存期間設定のメール履歴とコピーの設定値)の後までメールの処理が行われない場合、該当メールは、決裁なしで削除されます。

× 決裁の待機期間満了または送信者/管理者による決裁承認時、該当ポリシーの詳細条件(ex、添付の処理方法等)が適用されて送信されます。

× 送信者に決裁待ちの通知が送信された場合、メール内に表示されている[決裁キャンセル]ボタンを使用して決裁キャンセルが可能です。

- ルーティング指定:指定されたサーバにメールが送信されます。
  - ✓ サーバ IP/ポート:転送するサーバ IP とポート番号を入力します。サーバ IP は 0～255 の数字と '.'で構成され、完全な IP 情報を入力でき、ポートは 1～49151 の値で入力することができます。[アクセステスト]ボタンをクリックすると接続テストを行うことができます。

→ 添付の処理：メールの添付ファイルのセキュリティ機能をメール処理とは別に提供しています。遮断機能を除いたメール処理機能（通過、決裁、送信遅延、ルーティング）と混合して使用することができます。'パスワードの直接指定'オプションを利用してポリシーごとのパスワードを手動で設定することができます。

- 原本の維持：添付ファイル原本を保持します。
- 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をサーバに保存した後、ファイルをダウンロードできるリンクを生成し、メールに挿入します。メール受信者は挿入された特定 URL を介してのみ添付ファイルをダウンロードすることができます。添付ファイルのリンク変換オプションに対する詳細説明は 7.3.5 添付ファイルの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圧縮暗号化します。添付ファイル暗号化オプションについては 7.3.3 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混合したものでフィルタリングされたメールの添付ファイルを圧縮暗号化後、サーバに保存、ファイルをダウンロードできるリンクを生成してメールに挿入します。メール受信者は特定 URL を介して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、圧縮解凍時には特定パスワードを使用します。
- パスワードの直接指定：暗号化、リンク変換、暗号化後のリンク変換時に使用されるパスワードを直接指定します。パスワードは 6 文字以上、16 文字以下で入力する必要があります。

注意事項

× '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'を設定した場合、設定したパスワードは、添付ファイルを圧縮するときに使用されるものであり、リンク変換時には設定したパスワードは使用しません。

→ ポリシーのお知らせ：フィルタリングされたメールがポリシーによって処理された事を通知します。お知らせメールの使用可否と受信対象者を設定します。

- REVIEWER にポリシー適用のお知らせ：*ユーザ管理*>ユーザ管理の人事情報で設定したレビュー担当者にポリシーお知らせメールを送信します。
- APPROVER にポリシー適用のお知らせ：*ユーザ管理*>ユーザ管理の人事情報で設定された決裁者にポリシーのお知らせメールを送信します。
- 以下の受信者にポリシー適用のお知らせ：所属に関係なく必要に応じてポリシーお知らせ対象者を設定します。
  - ✓ [選択]：既に登録された組織図リストから受信対象者を選択できます。
  - ✓ [削除]：選択された受信対象者を削除します。
  - ✓ 直接入力：ポリシー適用のお知らせ対象者を直接入力できます。適用対象/例外対象とは異なり、対象者にのみ設定することができるため 'E メール'形式で入力する必要があります。[追加]ボタンにより設定します。

→ お知らせ方法：ポリシーのお知らせ方法を設定します。

- BCC：ポリシーが適用され、メールを BCC 形式でポリシーお知らせ対象に送信します。
- お知らせメールを送信：ポリシーが適用され、メールのタイトルと簡単な情報が含まれているお知らせメールをポリシーお知らせ対象に送信します。ポリシーお知らせメールのテンプレートは、*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にします。

- 原文を添付:お知らせメールにポリシーが適用されたメールの原文を添付して送信します。

→ 適用時間:ポリシーが適用され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。

→ その他:該当ポリシーの追加的な説明を入力します。

3. [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、ポリシー一覧の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と、設定した情報がすべて初期化されます。

4.1.3. 受信者グループ別管理

受信を許可するメールまたはドメインリストの機能を拡張しグループ化する機能です。ポリシー追加時にフィルタリング条件で活用されます。例えば、ポリシーを追加するときに許可された受信先の時に添付ファイルの暗号化、もしくは許可された受信先以外の時に上司に参照のお知らせを送信するような活用ができます。

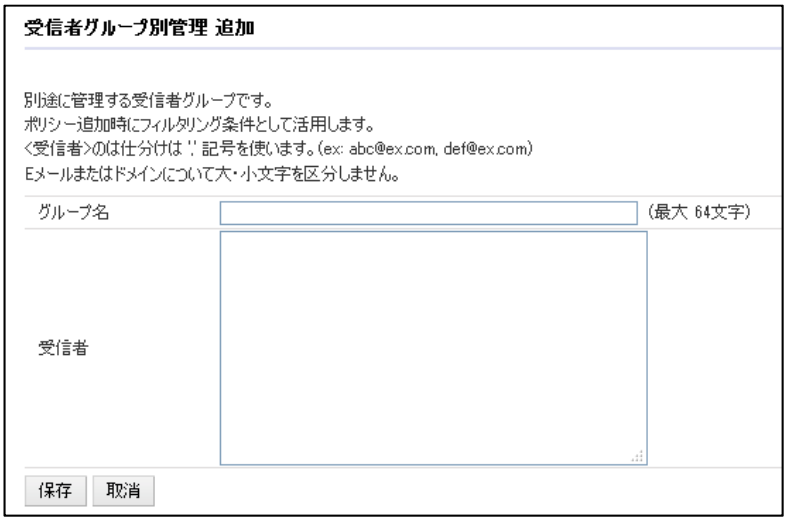
注意事項

× 旧バージョンの許容宛先機能を削除したために、受信者のグループデータに移行する必要があります。不明な場合弊社サポートまでお問い合わせください。

設定方法

1. *SMTP Filter*>ポリシー管理>受信者グループ別管理をクリックします。
2. 受信者グループ別管理画面が出力されます。
3. 受信者グループ別管理の上部および下部の機能説明です。

→ 1_[追加]:受信者のグループを登録します。[追加]ボタンをクリックすると、グループの追加画面が表示されます。



- グループ名：英数字に関係なく最大 64 文字まで入力することができます。
- 受信者：メール形式で入力する必要があります。複数のメールアドレスを入力するときは、区切り文字' 、' を使用します。英数字に関係なく最大 5000 文字まで入力することができます。

→ 2_[削除]：選択したグループを削除します。既にポリシーで使用している場合は削除できません。

→ 3_[ファイル保存]：検索されたグループリストをファイルで保存します。

→ 4_リスト数の設定：ページごとの表示されるグループリストの数を設定します。

→ 5_[検索]：検索語を入力した後、検索ボタンをクリックします。グループ名、受信者情報と比較された検索結果を示しています。

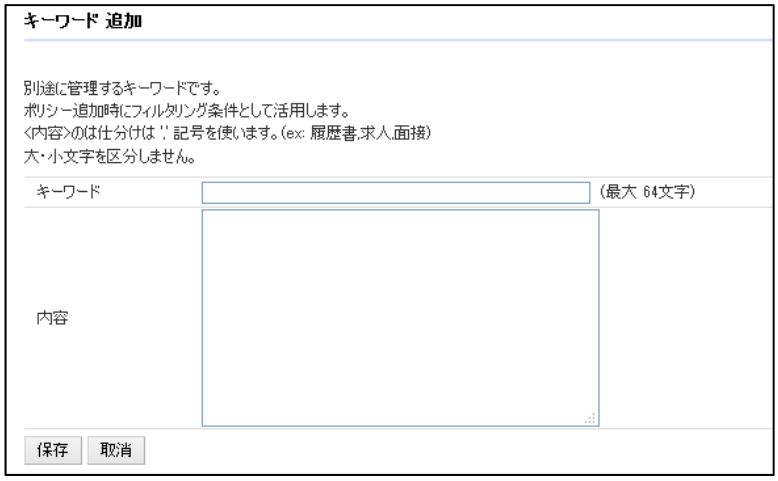
4.1.4. キーワード管理

グループ化した文字列をキーワード名で個別管理し、ポリシー追加時にフィルタ条件に活用することができます。例えば、フィルタリング対象が「本文」でフィルタ条件が「含めると」の時、フィルタリング値に異なる複数個の登録が必要であった場合、条件を複数回入力する必要がありました。この不便さを改善するためにポリシーの追加/修正を容易に行うことに機能追加しました。

設定方法

1. *SMTP Filter*>ポリシー管理>キーワード管理をクリックします。
2. キーワード管理画面が出力されます。
3. キーワード管理の上部および下部の機能説明です。

→ 1_[追加]:キーワードを登録します。[追加]ボタンをクリックすると、キーワードの追加画面が表示されます。



- キーワード:英数字に関係なく最大 64 文字まで入力することができます。
- ないよう:区切り文字'、'を使用します。英数字に関係なく最大 5000 文字まで入力することができます。

→ 2_[削除]:選択したキーワードを削除します。既にポリシーで使用している場合は削除できません。

→ 3_[ファイル保存]:検索されたキーワードのリストをファイルで保存します。

→ 4_リスト数の設定:ページごとの表示されるキーワードリストの数を設定します。

→ 5_[検索]:検索語を入力した後、検索ボタンをクリックします。キーワード名、内容と比較された検索結果を示しています。

4.2. 個人情報ポリシー管理

社内メールを通して外部へ送信されるすべてのメールの本文と添付ファイルをチェックして、個人情報項目が含まれているかをチェックします。チェック結果、個人情報を含まれている場合は、該当メールの送信を一時保留し、ポリシーに基づいてメールを処理します。企業内の個人情報の漏洩を根本的に防止するために提供する機能です。

4.2.1. 個人情報ポリシー追加

設定方法

1. *SMTP Filter*>ポリシー管理>ポリシーリスト>[個人情報ポリシー追加]ボタン、または *SMTP Filter*>ポリシー管理>個人情報ポリシー追加をクリックします。
2. 個人情報ポリシー追加画面で次の値を入力します。個人情報検出回数、個人情報検索の対象と個人情報対象を除きポリシー追加項目と同じです。各項目の説明は、4.1.2 ポリシー追加を参照してください。

→ 個人情報検出回数：個人情報検出回数を設定します。設定した回数以上に個人情報が検出されればポリシーが適用されます。例として個人の情報検出回数を 5 回以上に設定した場合は次のとおりとなります。

検索対象	個人情報対象	メールの個人情報内容		ポリシー適用
本文と添付	マイナンバー クレジットカード番号 IP アドレス	本文	マイナンバー 4 回	O
本文				X
添付		添付	クレジットカード番号 3 回	X
タイトル		タイトル	IP1 回	X

→ 個人情報検索対象：検索対象を本文と添付ファイル、本文、添付ファイル、タイトルの中から選択します。設定された検索対象にのみ個人情報を取得します。

→ 個人情報対象：個人情報の対象を設定します。基本的に提供する項目の'ユーザ定義'項目を設定する場合は、*SMTP Filter*>ポリシー管理>個人情報ユーザ定義で設定した対象が適用されます。個人情報ユーザ定義の詳細説明は、4.2.2 個人情報ユーザ定義を参照してください。

3. [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画面に切り替わります。[リセット]ボタンをクリックした場合は設定した情報がすべて初期化されます。

4.2.2. 個人情報ユーザ定義

基本的に提供する個人情報項目以外にユーザが追加で個人情報項目を定義できる機能です。個人情報ユーザ定義により柔軟な個人情報保護ポリシーを設定できます。

設定方法

1. *SMTP Filter*>ポリシー管理>個人情報ユーザ定義をクリックします。
2. 個人情報ユーザ定義画面が出力されます。
3. 個人情報ユーザ定義の上部および下部の機能説明です。

→ 1_[登録]：個人情報を検出するための正規式と説明を登録します。正規式とは、特定の規則を持つ文字列の集合を表現するために使用する形式言語で、文字列の検索と置換を支援します。正規式は、意図とは異なるより多くのメールをフィルタリングする結果をもたらすことがありますので常に注意しなければなりません。[正規式テスト]ボタンを利用して事前に動作を確認してみることを推奨します。正規式構文についての詳細情報は http：//pcre.org/pcre.txt を参考にしてください。説明と正規式ポリシー使用可否を選択し [登録]ボタンをクリックします。

注意事項

× 'ポリシー反映'オプションをチェックしてもシステムにすぐ適用されるのではなくて個人の情報ポリシーの中 'ユーザ定義'オプションが設定されていなければなりません。

→ 2_[正規式テスト]：入力した正規式の動作を事前にテストすることができます。フィルタリングしようとする文字列とこれを検出することができる正規式を入力した後、[正規式テスト]ボタンをクリックします。検出結果を通知します。

→ 3_[削除]：選択した個人情報ユーザ定義を削除します。

→ 4_[ファイル保存]：個人情報ユーザ定義リストをエクセルファイルで保存します。

→ 5_リスト数設定： ページごとの表示される個人情報ユーザ定義リストの数を設定します。

→ 6_[変更]：すでに登録された個人情報ユーザ定義を修正することができます。登録されている個人情報ユーザ定義（正規式、使用可否、説明）を修正した後、[変更]ボタンをクリックします。

→ 7_[検索]：検索条件（正規式、使用可否、説明）を選択し、検索用語を入力します。[検索]ボタンをクリックすると検索された個人情報ユーザ定義が画面に表示されます。

4.3. SMTP ポリシー

SMTP 段階のポリシーは、Black List と White List に区分されます。Black List は送信者 E メールまたは送信サーバ IP 情報を確認してメール受信を拒否します。White List は Black List とは対照的に送信者 E メールまたは送信サーバ IP 情報を確認してメール受信を許可します。

注意事項

× White List は Black List より優先適用されることに注意してください。

4.3.1. Black List 管理

設定方法

1. *SMTP Filter*>ポリシー管理>Black List をクリックします。
2. Black List 画面が出力されます。
3. Black List 上部と下部の機能説明です。

→ 1_[登録]:Black List を追加します。E メールまたはドメイン、IP 形式で構成された Black List と説明を入力した後、[登録]ボタンをクリックします。

注意事項

× IP アドレスを入力する場合、完全な IP アドレスまたはワイルドカード(‘*’ 文字)による IP アドレスの指定が可能です。

× ワイルドカードは必ず ‘.’ の後に使用する必要があります。‘.’ 文字ではなく '10.0.1*'のように設定する場合、IP アドレスではなく E メールアドレスとして認識されます。

× ワイルドカードを利用して IP を設定する場合、ワイルドカードの右側のすべての文字は無視されます。したがって、'10.0*.'や'10.0.*.100'が同じ意味になることを注意してください。

× '10.0.*'を指定する場合は、IP アドレスの左側から検査するため'210.0.0.1'は、フィルタリングされません。

→ 2_[削除]:選択した Black List を削除します。

→ 3_[ファイル保存]:Black List をエクセルファイルに保存します。

→ 4_リスト数設定:ページごとに表示される Black List の数を設定します。

→ 5_[検索]:検索条件(Black List、登録パス、説明)を選択し、検索語を入力します。[検索]ボタンをクリックすると検索されたユーザ情報が画面に表示されます。

4.3.2. White List 管理

White List 登録、削除、ファイル保存および検索機能は、Black List と同様となります。4.3.1 Black List 管理を参照してください。

4.4. SMTP 攻撃の遮断

認可されていないユーザによる不法リレーの試みを事前に検知・遮断してオープンリレーサーバに悪用されないようにします。一定時間 SMTP AUTH に失敗した IP は一時的に接続が遮断されます。

4.4.1. 遮断設定

SMTP 攻撃遮断機能の有効化、攻撃検知の関連機能を設定します。

設定方法

1. *SMTP Filter*>SMTP 攻撃の遮断>遮断設定をクリックします。
2. 遮断設定画面が出力されます。

→ 遮断機能：SMTP 遮断機能の使用可否を設定します。

- 遮断有効化：SMTP 遮断機能が有効になります。'検知間隔'・'AUTH 認証失敗'項目の設定値を基準に SMTP AUTH に数回失敗した IP は MailScreen への接続を一時的に遮断します。
- ログのみ記録：検知間隔、AUTH 認証失敗項目の設定値を基準に SMTP AUTH に数回失敗した IP 関連ログのみを記録します。
- 使用しない：SMTP 遮断機能を使用しません。

→ 遮断サービス：遮断サービスを設定します。

- SMTP：該当 IP で MailScreen に試みられる SMTP(25)、SMTPS(465)、SMTP Submission(587)サービス接続を遮断します。
- ALL：該当 IP で MailScreen に試みられるすべての接続を遮断します。

→ 検知間隔：AUTH 認証の失敗検知間隔を設定します。3 分～300 分まで設定できます。

→ AUTH 認証失敗：認証の失敗回数を設定します。検知間隔中に認証失敗回数を超過した場合、遮断機能と遮断サービス設定に基づいて動作します。1 回～20 回まで設定できます。

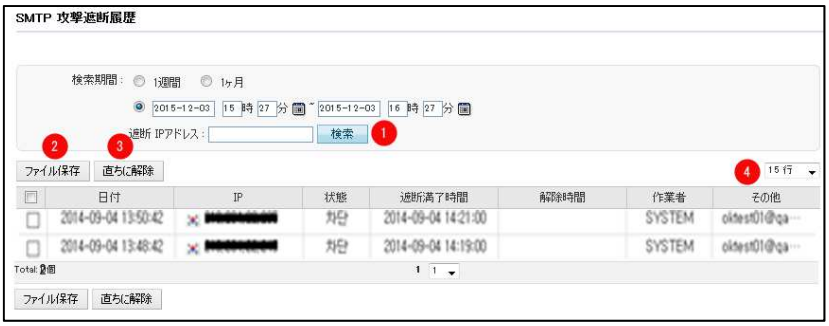
→ 遮断解除：遮断された接続 IP に対して一定時間が経過した後、自動的に遮断解除されます。

4.4.2. 遮断履歴

SMTP 遮断設定によって遮断された IP の履歴を照会することができます。

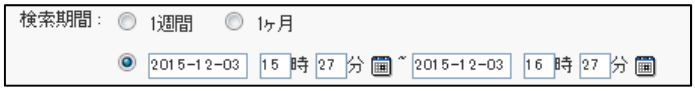
設定方法

1. *SMTP Filter*>SMTP 攻撃の遮断>遮断履歴をクリックします。
2. 遮断履歴リスト画面が出力されます。
3. リスト上部と下部の機能説明です。



→ 1_[検索]:検索期間と遮断 IP アドレスを設定した後、[検索]ボタンをクリックします。設定された項目に検索された情報を表示します。

- 検索期間:検索期間を設定します。



  - ✓ 1 週間:今日を基準に過去 1 週間の遮断履歴を検索します。
  - ✓ 1 ヶ月:今日を基準に過去1ヵ月間の遮断履歴を検索します。
  - ✓ 詳細期間:検索日付を詳細に指定して検索します。
- 遮断 IP アドレス:検索しようとする遮断 IP アドレス情報を入力します。

注意事項

- × 検索開始時間は、検索終了時間よりも大きくすることはできません。
- × 検索時間設定の時、年-月-日まで入力する必要があります。年は 4 桁からなる数値を入力する必要があり、月は 1～12、日は 1～31、時間は 0～23、分は 0～59 の値です。

→ 2_[ファイル保存]:遮断履歴リストをエクセルファイルに保存します。

→ 3_[直ちに解除]:選択した IP の遮断を直ちに解除します。

→ 4_リスト数設定:ページごとに表示される遮断履歴リスト数を設定します。

5. メール管理

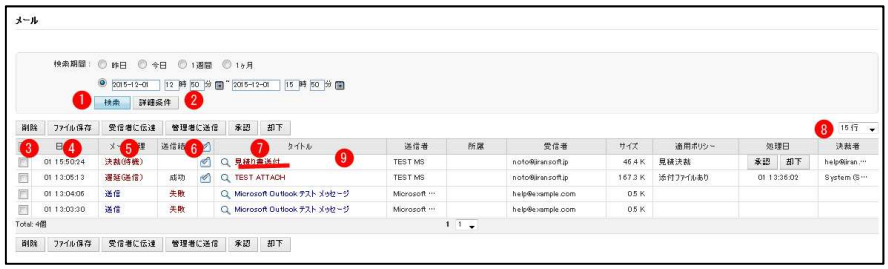
MailScreen は、処理したメールに対して監査、メール原本等を保存して提供しています。

5.1. Web-Admin メール管理

5.1.1. メール

設定方法

1. *SMTP Filter*>メール>メールをクリックします。
2. メールリストが出力されます。
3. メールリスト上段と下部の機能説明です。



1_[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致したメールを検索します。

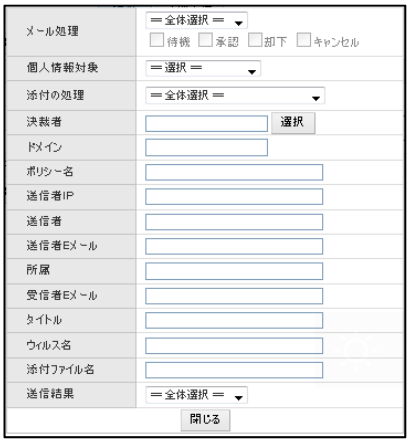
- 検索期間:検索期間を設定します。

- ✓ 昨日:昨日 00 時 00 分から 23 時 59 分 59 秒までの送信メールを検索します。
- ✓ 今日:今日 00 時 00 分から現在まで送信メールを検索します。
- ✓ 1 週間:今日を基準に過去 1 週間の送信メールを検索します。
- ✓ 1 ヶ月:今日を基準に過去1ヶ月間の送信メールを検索します。
- ✓ 詳細期間:検索時間をより詳細に設定します。

注意事項

- × 検索開始時間は、検索終了時間より大きくすることはできません。
- × 検索時間設定の時、年-月-日まで入力する必要があります。年は 4 桁からなる数値を入力する必要があり、月は 1～12、日は 1～31、時間は 0～23、分は 0～59 の値です。

→ 2_[詳細条件]:検索のための詳細な条件を設定します。[詳細条件]ボタンをクリックすると詳細条件を設定するための画面が出力されます。



- メール処理：送信、通過、遅延等のメールが処理された状態を検索条件に設定します。決裁を選択した場合、'待機/承認/却下'項目が有効になります。
- 個人情報対象：選択した個人情報保護ポリシー（マイナンバー、クレジットカード番号等）が適用されたメールを検索します。'全体選択'は、個人情報保護ポリシーが適用されたすべてのメールを検索します。
- 添付の処理：メールの添付ファイルが処理された方式（原本の維持、添付ファイル暗号化、添付ファイルのリンク変換、添付ファイル暗号化後にリンク変換）を検索条件で設定します。
- 決裁者：メールを決裁した決裁者を検索条件で設定します。直接入力するか、[選択]ボタンをクリックして組織図から選択します。
- ドメイン：送信者の E メールドメインを検索条件に設定します。ドメインを a.com に設定し、送信者 E メールを user@b.com に設定した場合、検索がされないことに注意する必要があります。
- ポリシー名：メールに適用されたポリシーを検索条件に設定します。
- 送信者 IP：送信者の IP アドレスを検索条件に設定します。
- 送信者：送信者名を検索条件に設定します。
- 送信者 E メール：送信者 E メールを検索条件に設定します。
- 所属：送信者の所属を検索条件に設定します。
- 受信者 E メール：受信者 E メールを検索条件に設定します。
- タイトル：メールタイトルを検索条件に設定します。
- 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に設定します。
- 添付ファイル名：添付ファイル名を検索条件に設定します。
- 送信結果：送信結果を検索条件に設定します。

注意事項

× 大量のメールを検索する場合、一般的に検索条件を詳しく指定するほど検索効率が良くなり早く結果を照会することができます。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、タイトル、ウィルス名、添付ファイル名）の場合、値の一部のみ入力しても検索が可能ですが、これにより検索速度に影響を与える可能性がありますので、注意してください。

→ 3_[削除]：選択したメール履歴を削除します。

→ 4_[ファイル保存]：メール履歴をエクセルファイルに保存します。

→ 5_[受信者に伝達]：選択したメールを受信者に再送します。受信者に再送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る必要があります。原本メールがサーバに保存されている場合、メールタイトル前に  があります。

→ 6_[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します。管理者に再送するためには 5 の機能のようにメールの原本がサーバに保存されている必要があります。

→ 7_[承認]/[却下]：決裁要請メールを承認/却下できます。決裁要請の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。*環境設定*>フィルタリング>誤送信防止の決裁関連オプションに応じ決裁理由を入力します。

→ 8_リスト数設定：ページごとの表示されるメール履歴リスト数を設定します。

→ 9_メールタイトル：原本メールがサーバに保存されている場合は、メールのタイトルをクリックすると該当メールの原本の詳細を見ることができます。もし、メール原本が保存されていない場合は、受信者の情報と送信結果等の簡単な情報のみを表示することになります。

- [原文ダウンロード]：メール原本を PC に保存することができます。
- [クローズ]：メール詳細表示画面を終了します。
- [受信者に伝達]：受信者の E メールアカウントに再送信します。
- [管理者に送信]：現在ログインしている管理者の E メールアカウントに再送信します。

- ヘッダ：メールのヘッダ情報です。
- 原文：メールのヘッダを含む原文をテキストそのまま表示します。この時マイムデコーディングは行いません。
- 内容：メールのヘッダを除外した内容を表示します。メールのマイムが multipart/alternative の場合、text/html に該当する部分のみを HTML 形式で出力されます。
- 受信者：メールの受信者情報と送信成功可否/送信日付を表示します。
- お知らせ：パスワード情報お知らせ、決裁待機、承認、却下等のメール処理に関連したお知らせメールが送信された場合に、タブが作成され、お知らせメール受信者情報と送信成功可否、送信日付、お知らせ区分情報を表示します。
- 添付：メールに添付ファイルがある場合にのみタブが生成されます。メールに添付されたファイルリストを表示し、添付ファイル名をクリックするとダウンロードすることができます。
- View images：オプションをチェックすると、メール詳細表示の状態で本文に含まれている画面イメージを表示します。
- 遮断根拠：個人情報ポリシーにフィルタリングされたメールの時は、タブが生成されメールの根拠を表示します。選択された個人情報の検索対象と個人情報対象にマッチされた文字について赤文字で示します。また、[PREV]、[NEXT]ボタンを使用し、フォーカスが移動し、根拠を示します

注意事項

× メールが添付ファイルを含む場合、出力する内容が多くなり、ブラウザの反応が遅くなる場合があります。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>メール確認のサイズ制限を設定します。

5.1.2. 添付

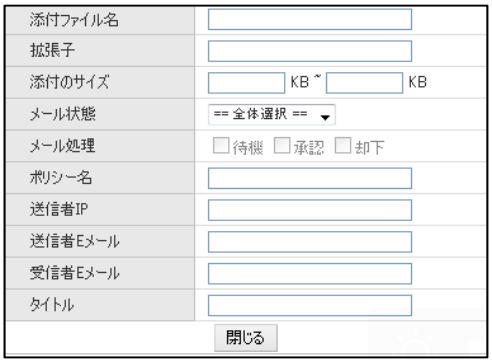
メールに添付された添付ファイルに対する履歴管理です。

設定方法

1. *SMTP Filter*>メール>添付をクリックします。
2. 添付リストが出力されます。
3. 添付リスト上部、下部の機能説明です。

→ 1_[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ったメールを検索します。検索期間項目の説明は、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詳細条件を設定するための画面が出力されます。



- 添付ファイル名：添付ファイル名を検索条件に設定します。
- 拡張子：添付ファイルの拡張子を検索条件に設定します。ドット(‘.’)を除いた拡張子情報を入力します。
- 添付のサイズ：添付ファイルのサイズを検索条件に設定します。
- メール状態：転送、通過、決裁、送信遅延等、メールが処理された状態を検索条件に設定します。
- メール処理：メール状態が決裁の場合に限り、メール処理項目が有効化されます。
- ポリシー名：メールに適用されたポリシーを検索条件に設定します。
- 送信者 IP：送信者の IP アドレスを検索条件に設定します。
- 送信者 E メール：送信者 E メールを検索条件に設定します。
- 受信者 E メール：受信者 E メールを検索条件に設定します。
- タイトル：メールタイトルを検索条件に設定します。

→ 3_[ファイル保存]：添付履歴をエクセルファイルに保存します。

→ 4_リスト数設定：ページごとの表示されるメール履歴リストの数を設定します。

→ 5_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することができます。

→ 6_タイトル：、メール原本がサーバに保存されている(メールタイトルの前に 表示)メールタイトルをクリックすると該当メールの原本を詳細に見ることができます。メール詳細表示の詳細については 5.1.1 メールを参照してください。

5.1.3. リンク履歴

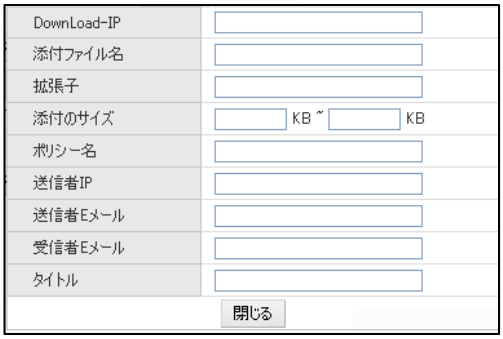
リンク変換された添付ファイルのうち、受信者がダウンロードしたファイルのリストを管理します。

設定方法

1. *SMTP Filter*>メール>リンク履歴をクリックします。
2. リンク履歴リストが出力されます。
3. リンク履歴リストの上部、下部の機能説明です。

→ 1_[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致したメールを検索します。検索期間項目の説明は 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詳細条件を設定するための画面が出力されます。



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

→ 3_[ファイル保存]：リンク履歴をエクセルファイルに保存します。

→ 4_リスト数設定：ページごとの表示されるメール履歴のリスト数を設定します。

→ 5_添付ファイル名：添付ファイル名をクリックした場合、該当添付ファイルをダウンロードすることができます。

→ 6_タイトル：メール原本がサーバに保存されている（メールタイトルの前に 表示）タイトルをクリックするとメールの原本を詳細に見ることができます。メール詳細表示の詳細については 5.1.1 メールを参照してください。

5.1.4. メール拒否

MailScreen に流入されたメールの中で、SMTP によって拒否された場合、その履歴をメール拒否で確認することができます。

注意事項

× メール拒否履歴のうち、送信者と受信者列は~、もしくは空白の場合もあります。情報を得る前にメールが拒否され、その情報を提供していないために拒否された場合がこれに該当します。

設定方法

1. *SMTP Filter*>メール>メール拒否をクリックします。
2. 拒否の履歴リストが出力されます。
3. 拒否履歴リスト上部、下部の機能説明です。

→ 1_[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致したメールを検索します。検索期間項目の説明は 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次の検索条件を設定するための画面が出力されます。

- 送信者 IP：送信者 IP を検索条件に設定します。
- 送信者 E メール：送信者 E メールを検索条件に設定します。
- 受信者 E メール：受信者 E メールを検索条件に設定します。

- 拒否理由コード：拒否理由のコードを検索条件に設定します。拒否理由コードは次のとおりです。

コード	説明
100	メールサイズ制限の超過
101	送信者メールアドレス MX Record エラー
102	不法 Relay 使用
103	*1)送信者メールアドレスパターン検査あるいは Black List
104	*2)受信者メールアドレスパターン検査あるいは不良受信者
105	Null Sender メール
106	最大同報数制限超過
108	*3)メールアドレスに空白を含む
110	受信者 MailBox 存在なし
111	同じ送受信者 E メール
112	Null Receiver メール
113	SMTP 通信時間超過
114	無効な送信者メールアドレス
115	無効な受信者メールアドレス
116	RBL(Real-time Black List)に登録された IP
118	IP 当たり最大同時接続数超過
119	Reverse DNS エラー
120	認証失敗制限数超過
121	最大 Hop 数超過
122	最大 Rset 数制限超過
123	認証情報と送信者メール情報が一致しない
124	TLS 強制適用ドメイン
125	E メールアドレス(ID)長さ制限超過
126	E メールアドレス長さ制限超過

*1)一般的な Black List または *SMTP Filter*>ポリシー管理>Black List 設定の送信者メールアドレスパターン検査によって拒否される場合

*2)受信者メールアドレスにスペースや Tab 文字などの無効な文字が含まれている場合

*3)メールアドレスにスペースや Tab 文字が含まれている場合

注意事項

- × 詳細条件を利用した検索を実行すると、拒否理由コードを除くすべての条件は、一部の文字のみ入力しても検索が可能です。
- × 拒否理由コードは、3 桁の拒否コードを入力する必要があります。
- × 拒否メール履歴は、メール環境と MailScreen の設定に応じて表示速度が流動的ですが、検索時に適切な検索条件を与えて検索速度を向上させることができます。速度を向上する検索条件は、検索期間と拒否理由コードです。

→ 3_[ファイル保存]：メール拒否履歴をエクセルファイルに保存します。

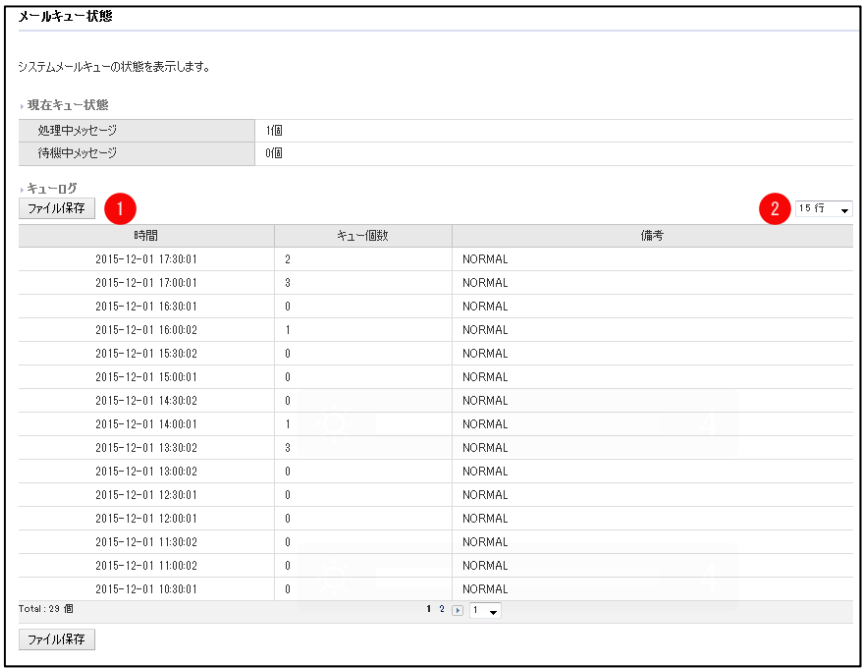
→ 4_リスト数設定：ページごとに表示されるメール履歴リスト数を設定します。

5.1.5. メールキュー状態

MailScreen で正常メールと判断されたメールは、実メールサーバに送信されます。しかし、ネットワーク状況やメール処理量等の原因によりすぐに処理できない場合は、メールをキューに蓄積し、後で送信を試みるようになります。メールキューの状態を確認し蓄積されたキューの状況を把握することによりシステムの処理状況を判断することができます。

設定方法

1. *SMTP Filter*>メール>メールキュー状態をクリックします。
2. メールキュー状態リストが出力されます。メールキューリスト上部、下部の機能説明です。



→ 現在キュー状態：現在のキューの状態情報です。

- 処理中メッセージ：キューで処理中のメッセージ総数です。
- 待機中メッセージ：受信するメールサーバが応答しない状況のときに、キューに待機しているメッセージ数です。システム使用率が 100%、あるいはシステムダウン、DNS クエリ情報を得ることができない場合にキューがたまる現象が発生します。

→ キューログ：キューのログです。キュー状態は 30 分単位で検査されます。

- 1_[ファイル保存]：キューログをエクセルファイルに保存します。
- 2_ページ数設定：ページごとの表示されるキューログの数を設定します。

注意事項

× 備考欄には、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'よりも、現在未処理のメールキューが多いときに表示されます。キューにあまりにも多くのメールが蓄積され、処理が遅延しているという意味で原因を見つけ解決しないとユーザのメールが送/受信で遅延される結果をもたらすことになります。MailScreen は、キューが指定した数以上に蓄積されれば E メールで警告を送信するように設定することができます。オプションの詳細については 7.1.1 基本情報のシステム監視項目を参照してください。

5.2. モバイルメール管理

MailScreenは、モバイル端末用ウェブ決裁機能を提供しています。決裁者はモバイル端末を利用して時間と場所に関係なくメールを管理することができます。

注意事項

× モバイル端末用 Web-Admin が最適化されたモデルは iPhone 6s、iPhone5s/5、Galaxy S/K/U です。これ以外のモデルでは画面が正常に表示されない場合があります。

5.2.1. ログイン

モバイル端末を利用してメール管理をするためにはモバイル端末用 Web-Admin にログインする必要があります。モバイル端末用 Web-Admin は Web-Admin と同様のログイン方法を提供しています。

設定方法

1. モバイルウェブブラウザを実行します。
2. ウェブブラウザアドレスの入力ダイアログに 'http://<MailScreen が設置された IP またはドメイン名>'を入力します。
3. ログインページが出力されると次の情報を入力した後[ログイン]ボタンをクリックします。それぞれの項目の説明は **2.1 ログイン**を参考にしてください。

4. 入力した E-mail アカウントとパスワードでログインに成功した場合は、メール管理画面が出力されます。失敗した場合は失敗したことを知らせる画面が出力されます。

5.2.2. メール管理

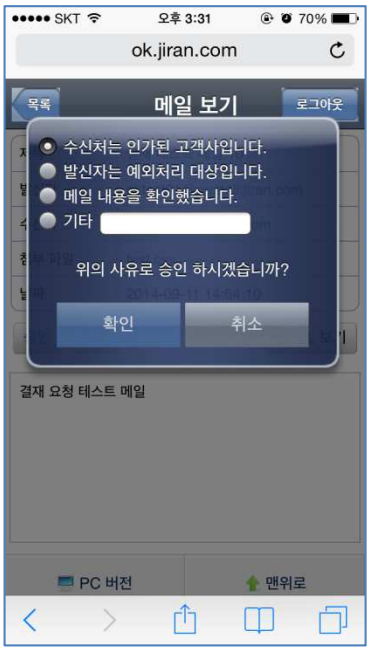
モバイル端末用 Web-Admin は MailScreen で処理するメールに対する決裁 UI だけを提供します。

設定方法

1. モバイル端末用 Web-Admin にログインします。
2. メール管理画面が出力されます。各機能に対する説明は次のとおりです。

→ 1_メール分類タブ（待機/承認/却下/全体）：決裁要請メールをタブで分類しています。待機/承認/却下/全体のうちタブを選択すると該当メールリストが出力されます。

→ 2_[承認]/[却下]：決裁待機メールを選択した後[承認]ボタン、または[却下]ボタンを利用して決裁します。**環境設定>フィルタリング>誤送信防止**の決裁関連オプションにより決裁事由を入力します。



→ 3_[検索]：送受信者情報(名前、E メール)、メールタイトルについての検索機能を提供します。[検索]ボタンをクリックして検索キーを入力した後[確認]ボタンをクリックします。

→ 4_メール詳細ビュー：メールタイトルを選択するとメール詳細ビューが実行されます。次画面はメールビューが実行された画面です。各項目に対する説明は次のとおりです。

- タイトル：メールのタイトルです。
- 送信者：送信者名および E メールアカウントです。
- 受信者：受信者名および E メールアカウントです。
- 添付ファイル：メールに添付されたファイルリストです。添付ファイル名をクリックすると添付ファイルをダウンロードできます。
- [HTML ビュー]/[TEXT ビュー]：メールの内容を HTML、または TEXT 形式で確認することができます。[HTML ビュー]ボタンをクリックすると[TEXT ビュー]ボタンが活性化になります。

→ 5_[情報変更]:暗号および携帯電話情報、決裁メール受信等の情報を修正することができます。情報変更項目についての説明は次のとおりです。

- アカウントのパスワードを変更:該当アカウントに対するパスワードを変更します。新しいパスワードとパスワードの確認情報を入力します。
- 決裁委任:決裁委任機能の使用可否、決裁を委任する E メール情報、決裁委任期間を設定します。決裁委任機能を使用する場合、該当決裁者に要請される決裁メールは委任者のメールアカウントに送信されます。

6. ウィルス管理

MailScreen は、内部情報漏洩防止のほかに、ウィルスメールを検出して治療する機能をサポートしています。ウィルスを検出するためにワクチンエンジンのほか、MailScreen ウィルス対策チームが新しいウィルスの出現を認知し、そのパターンを分析した後、実際のワクチンパターンの配布が行われるまでウィルスメールを遮断する VPS 機能を提供しています。

6.1. ウィルス管理

6.1.1. ウィルス検査設定

設定方法

1. *ウィルス管理*>ウィルス検査設定をクリックします。
2. ウィルス検査設定画面が出力されます。各項目に対する説明は次のとおりです。

→ 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、設置時の環境や設定により、上の設定画面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'を選択するとメールを治療した後受信者に送信します。ワームの特性上、治療されたメールは、意味のないゴミメールになるので推奨しません。

→ 最終アップデート時間：最後にワクチン更新された時間です。

→ [リアルタイムアップデート]：ワクチンは、毎時更新されますが、直接リアルタイム更新も行うことができます。

注意事項

× ワクチンエンジンをすべて選択した場合、メールの量によりシステムに負荷を与えることがありますので注意してください。

× ワクチンエンジンは、比較的多くのデータをサーバから取得するため更新時間がか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 フィルタの設定

設定方法

1. ワクチン>VPS フィルタをクリックします。
2. VPS フィルタの管理画面が出力されます。各機能に対する説明は次のとおりです。

→ 1_[検索]：VPS フィルタを検索します。ウィルス名を入力し[検索]ボタンをクリックします。検索された VPS 情報が画面に表示されます。

→ 2_[削除]；選択した VPS フィルタを削除します。

→ 3_[ファイル保存]：VPS フィルタリストをエクセルファイルに保存します。

→ 4_[リアルタイムアップデート]：VPS フィルタをリアルタイム更新します。

→ 5_リスト数設定：ページごとの表示される VPS フィルタリストの数を設定します。

7. 環境設定

7.1. システム情報

システム運用のための多種な環境を設定します。

7.1.1. 基本情報

システム情報と画面構成、ジャーナルリング、言語のような基本情報を設定します。

設定方法

1. *環境設定*>システム>基本情報をクリックします。
2. 基本情報設定画面が出力されます。各項目を設定した後下部の[設定]ボタンをクリックします。

→ システム情報

- HostName：MailScreen が設置されてサーバに割り当てられたホスト名を設定します。ホスト名は、HTTP://を除いた A.HOST.COM のような形式である必要があり、この情報は MailScreen 内部の作業時に参照されます。HostName は、MailScreen 中央サーバに登録されていますので任意に変更するとライセンス取得、更新が動作しません。
- 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。ライセンス有効期間が満了された場合、'ポリシー追加禁止'のような使用に制約があります。ライセンスが登録されると区分（製品が納品された形態）/満了日/ドメイン数/ユーザ数を確認することができます。
  - ✓ [ダウンロード]：ボタンをクリックすると中央サーバに登録されているライセンスを取得します。保守契約が更新されたり、ドメイン数、ユーザ数の追加等でライセンスが更新されたりした場合に使用します。
- システムメール：送信者の名前・送信者 E メールアドレスを設定します。この情報は MailScreen がユーザにメールを送信するときに使用されます。

→ 画面設定： Web-Admin で表示される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：メール管理機能のうちメール詳細表示のデフォルト値を設定します。
  - ✓ 基本値：メール詳細表示で基本的に出力する情報を設定します。
  - ✓ サイズ制限：メールの原文を表示するとき、最大何 Kbytes まで読み取るかを設定します。基本の項目のうち、原文を選択するときだけに適用される項目で '0'を設定した場合、原文読み込みサイズは制限なしです。
- ロゴの設定：Web-Admin ページで表示されるロゴを設定します。各サイトのロゴを変更できます。PNG 拡張子をサポートしており、'ユーザが設定したロゴを使用'をチェックした後[参照]ボタンをクリックしてイメージをアップロードします。画面に表示されている推奨サイズより大きいときはアップロードできません。
- モバイルロゴ：モバイルデバイスの Web-Admin ページで表示されるロゴを設定する機能として各サイトのロゴを変更できます。PNG 拡張子をサポートしており'ユーザが設定したロゴを使用'をチェックした後、[参照]ボタンをクリックしてイメージをアップロードします。画面に表示されている推奨サイズより大きいときはアップロードできません。
- イメージリンク：Web-Admin 左上のイメージをクリックした時に接続されるリンクアドレスを設定します。
- 時間形式：時間を出力するとき使用する形式を設定します。Web-Admin は列が制限された画面の幅に多く情報を出力するために状況に応じて複数の形式

を使用しており、これをそれぞれの国の慣習に応じて設定できるようにサポートしています。形式文字列の種類と用途は 11.1.1 時間の形式文字、11.1.2 時間形式適用範囲を参照してください。

- ✓ 年月日　時分秒　時間帯：時間帯を含む日付と時間を示した形式は Y-m-d H:i:s T です。
- ✓ 年月日　時分秒：年月日を含む日付と時間を示した形式は Y-m-d H:i:s です。
- ✓ 年月日のみ：年月日だけ含む日付を示した形式は Y-m-d です。
- ✓ 日付と時分秒：日時間だけ示した形式は d H:i:s です。

- 検索時間：*SMTP Filter*>メールのメール関連の履歴(メール/添付/リンク履歴/メール拒否)照会時、一定時間までのメールのみを検索して画面に出力します。
- 検索方法：検索時に作業制限時間と検索結果の出力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わらない場合、強制終了されます。検索範囲を狭めて再度検索するようにします。
  - ✓ 検索結果の出力：設定した場合、検索結果が降順でソートされます。
- リモートサポート URL：Web-Admin 右上 Remote Support にリンクされた URL を設定します。Remote Support を押すと遠隔で技術支援を受ける事が出来ます。（日本での販売では対応しておりません）

→ 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 パッケージについて自動でアップデートする機能です。アップデート内容は*環境設定*>維持保守>エンジン自動アップデートにおいて照会が可能です。

注意事項

× 顧客の要求により MailScreen パッケージをカスタマイズする場合は、該当オプションを必ず'使用しない'に設定しなければなりません。そうでない場合は、次の自動アップデート時、場合により顧客カスタマイズで変更した履歴が喪失する場合があります。

- 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。[テスト]ボタンをクリックした場合、該当サーバとの接続可否を確認することができます。

→ ジャーナリング：ジャーナリング機能によりメールアーカイブソリューションと連携できます。

- 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：管理者の便宜のために、アカウントを利用するジャーナリング方法とサーバを利用するジャーナリング方法を提供します。選択方法に応じて下部の'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'項目を設定する必要があります。

- 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。1件のメールに複数の受信者がある場合は1件のメールのみジャーナルされます。送信メールアドレスと転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。 1件のメールに複数の受信者がある場合は、送/受信者のエンベロープ情報(Envelop MAIL FROM、RCPT TO)をそのまま利用するため、受信者数だけジャーナルされます。サーバアドレスとポート番号を設定します。

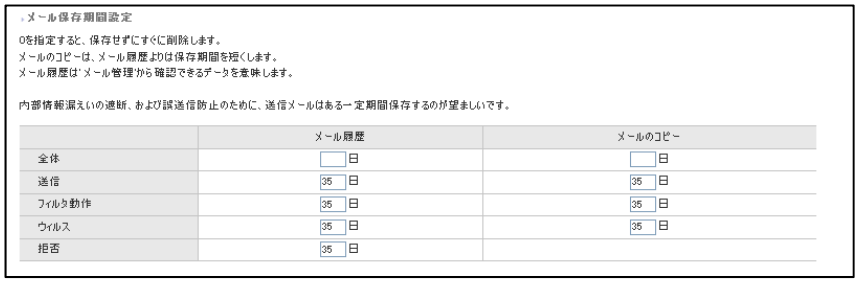
注意事項

× ジャーナリングサーバの問題でジャーナリングメール送信が継続的に失敗してキュー保存時間を超えた場合、元の送信者にメールが転送されますのでジャーナリングサーバに問題が生じないように注意する必要があります。

→ 言語設定：システムで使用される言語を設定します。

- システム：Web-Admin を表現するインターフェイスの基本的な言語を設定します。
- デコーディング文字セット：フィルタエンジンがメールを解析するときに、メール内部に文字セット情報がない場合、強制的に指定する文字セットです。メールの実際文字セットとこの情報が一致しない場合、メールの分析に失敗する可能性があることに注意してください。
- 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テンプレート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）項目に適用します。
- 送信：送信されたメールのうちポリシーを通過したり'通過'ポリシーによって送信されたりしたメールの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：ウィルス感染メールのログとメールコピーの保存期間を設定します。
- 拒否：発信拒否されたメールのメールログとメールコピーの保存期間を設定します。

注意事項

× メールコピーの保存期間は、常にメール履歴ログの保存期間より小さいか同じに設定する必要があります。

× フィルタ動作は、内部の重要情報が外部に漏洩するのを防止するためにポリシーが適用されたメールを意味します。したがって、フィルタ動作メール履歴や

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'より短く設定することはできません。

× メール受信量に応じて多くの保存領域が必要になる場合があります。メールのサイズを平均 500Kbytes と想定したとき次の方法を使用すると1日の必要な保存領域を計算することができます。

(500 <一日に受信されたメール数>) / 1024 / 1024

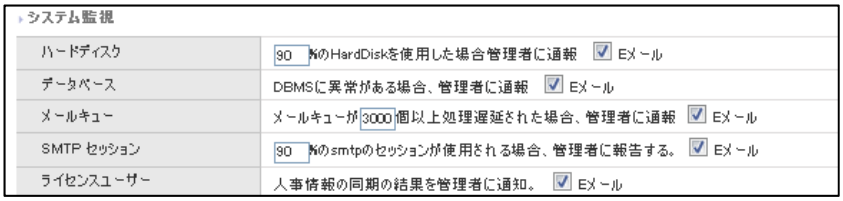
→ データ保存期間設定:システムログと統計データの保存期間を設定します。システムログは MailScreen で動作する各種プログラムが自分の動作状態に対して内部的に記録するログを指しており、ほとんどがテキストファイルとして記録されます。統計データはメールの IP、ポリシー、受信者、送信者等で統計構成したデータを指します。統計データは保存容量を多く必要とするので設定されたデータ保存期間情報を利用して定期的に削除されます。

→ メールの syslog 設定:ログサーバを別に運用する場合、メールログを送信できます。リモートサーバにオプションを選択してサーバ情報を入力します。

注意事項

× リモートサーバの syslogd(rsyslogd)デーモンが実行されていない、ネットワーク接続が異常で配信に失敗しても、ローカルサーバの/var/log/maillog には記録を残します。

→ システム監視:サーバの重要な状況を監視しシステムに問題が発生した場合は、メールで通報します。ハードディスク容量、データベース状態、メールキュー状態、SMTP セッション状態、登録ユーザ数を監視しスーパー管理者にメールを送信します。



- ハードディスク:設定した割合以上にハードディスクが使用された場合は、お知らせ機能が動作します。保存領域が不足するとメールログとメールコピーの保存等の作業が円滑に行われないため、このオプションは常にオンにすることを推奨します。
- データベース:DBMS テーブルのサイズ過多、テーブルの破損等の異常が発生した場合に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数以上のメールが蓄積された場合は、お知らせ機能が動作します。メールキューの状態は、*SMTP Filter*>メール>メールキュー状態で確認可能です。
- SMTP セッション:システムが許容した同時接続数の使用率が設定した基準を超過した場合にお知らせ機能が動作します。SMTP セッション状態は*SMTPFilter*>メール>SMTP セッションの状態で確認可能です。システムが許容

する最大同時接続数は*環境設定*>フィルタリング>SMTP>セッション設定で設定できます。

- ライセンスユーザー: 人事情報連動とユーザー括登録時に登録されたライセンスユーザ数を超過する場合、またはエラー発生時に 1 日 1 回スーパー管理者に通知します。

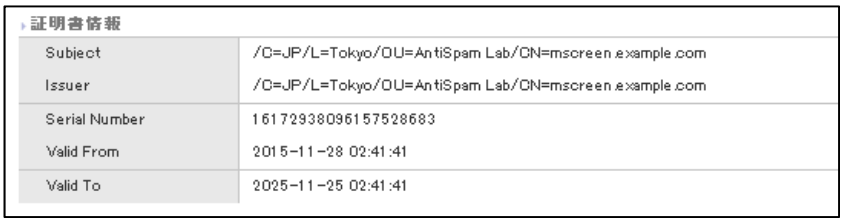
7.1.2. 証明書情報

証明書は Web-Admin 接の時に 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用されます。初期設置時に MailScreen は自己署名証明書を提供しています。

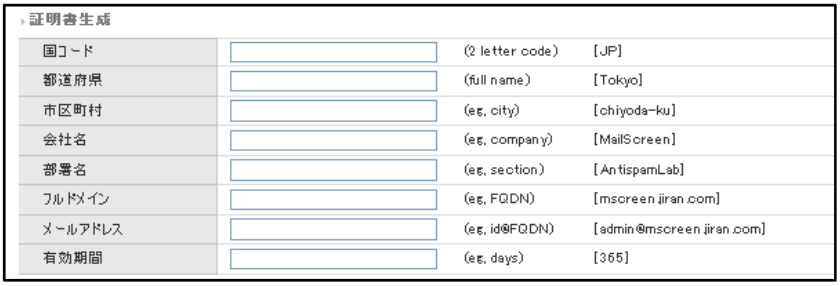
設定方法

1. *環境設定*>システム>証明書をクリックします。
2. 証明書の設定画面が出力されます。各項目の説明は次のとおりです。

→ 証明書情報：証明書情報を Subject(主体)、Issuer(発行者情報)、Serial Number(シリアル番号)、Valid From(有効開始時間)、Valid To(有効満了時間)の項目として表示されます。



→ 証明書生成：自己認証証明書を生成します。次の各項目を入力した後、[設定]ボタンをクリックします。

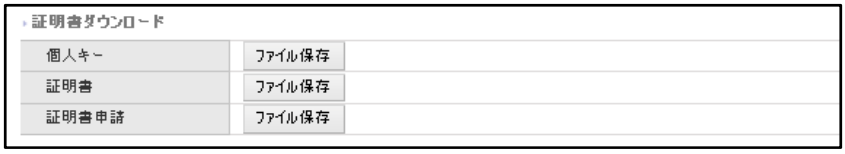


- 国コード：2 桁からなる ISO 形式の国コードを入力します。
- 都道府県：会社が位置する都道府県を入力します。
- 市区町村：会社が位置する市区町村を入力します。
- 会社名：下のホスト名を所有する会社名を入力します。
- 部署名：会社内の部署名を入力します。
- フルドメイン：サーバの DNS 参照に使用されているフルドメインを入力します。IP アドレスとポート情報は入力することはできません。'http://'や'https://'も含まれてはいけません。
- メールアドレス：証明書の管理者メールアドレスを入力します。
- 有効期間：証明書の有効期間を入力します。入力制限値は 1825 です。

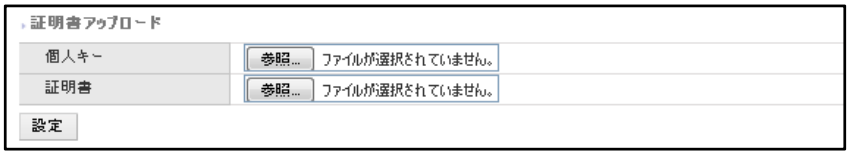
注意事項

✕ MailScreen が提供する証明書はセキュリティには問題ありませんが、認証局発効の公的証明書ではないため、ブラウザで安全ではない証明書という警告が表示されますが無視することができます。

→ 証明書ダウンロード：サーバに保存された証明書をダウンロードします。証明書要求を認証局に送信したりサーバの再設置をしたりする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：ローカルの証明書をアップロードします。認証局から認証を受けた証明書、または既に使用されている証明書をサーバに保存するときに使用します。証明書と個人キー（秘密鍵）は1組で構成されていますので証明書と該当個人キーを同時にアップロードする必要があります。



7.1.3. アクセス制御

Web-Admin ログイン方法やアクセス制御 IP を設定します。

設定方法

1. *環境設定*>システム>アクセス制御をクリックします。
2. アクセス制御設定画面が出力されます。各項目を設定した後、下部の[設定]ボタンをクリックします。

→ ユーザログイン：パスワードの強度のチェック、およびパスワードの長さなどのログイン関連オプションを設定することができます。

- パスワード複雑度検査：ユーザのパスワードが適切な構成（英大小文字、特殊文字、数字がそれぞれ 1 文字以上含む）で構成されているかを検査します。
- パスワード最小長さ：ユーザ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を使用する場合、有効期間が過ぎたパスワードの場合、必ず異なるパスワードに変更しなければ他の機能が利用できなくなります。
- 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。有効期間が経過したユーザはログイン直後に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した場合、アカウントのロックアウトを実行します。
- アカウントロックの時間：アカウントロックアウトの時間を設定します。最小 1、最大 99 まで入力することができます。

→ 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。

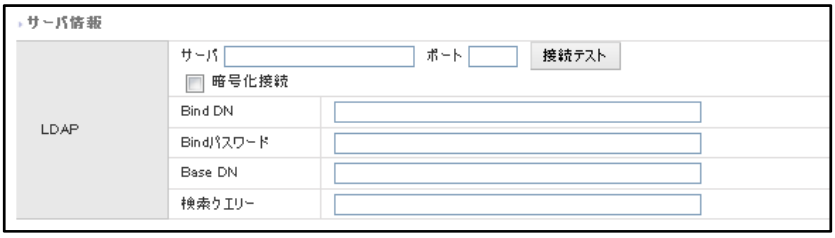
- ログイン方法：'登録アカウント検査'と'LDAP'、'POP3'から選択できます。
  - ✓ 登録アカウント検査：MailScreen サーバにユーザとして登録された ID とパスワードを識別情報として使用します。
  - ✓ POP3：POP3 サーバに登録されたユーザアカウントとパスワードを識別情報として使用します。POP3 サーバ情報は*環境設定*>メールサーバ>メールサーバで設定します。
  - ✓ LDAP：次項で説明するサーバ情報に登録されている LDAP サーバに登録されたユーザアカウントとパスワードを識別情報として使用します。
- 検査値：ログイン時の識別情報を Email ID(例 test)のみを使用するか、ドメイン情報を含む Full Email Address(例 test@test.com)を使用するかを設定します。
- テスト：設定内容に応じてログイン可能かをあらかじめテストすることができます。E メールとパスワードを入力し[接続テスト]ボタンをクリックします。

注意事項

× スーパー管理者/ログ閲覧者は'POP3'、'LDAP'ログイン方法から除外され、ID と Password 方法でのみログインする必要があります。

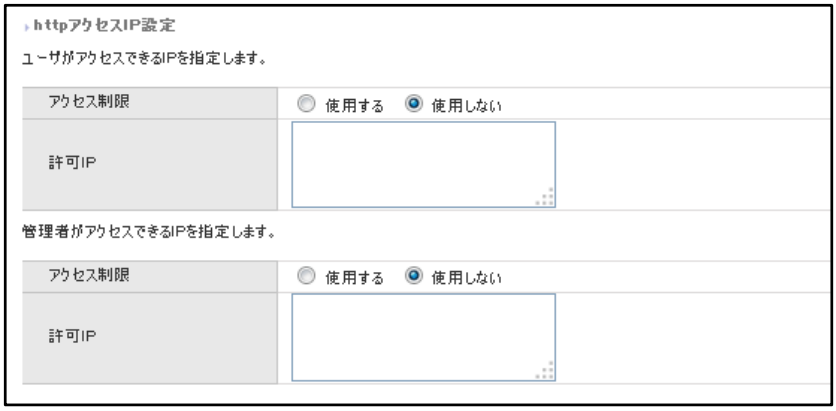
× 'LDAP'または'POP3'アカウントでログインする場合、MailScreen サーバに登録されているユーザの ID と比較し、権限を附与します。登録されていないユーザの場合、個人のユーザ権限が付与されます。

→ サーバ情報：上記のログイン情報の項目でログイン方法を'LDAP'に設定した場合は LDAP サーバの情報を入力します。



- 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、検索クエリを入力します。'暗号化接続'を設定すると LDAP サーバとの通信は、SSL 通信を利用することになります。

→ 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。



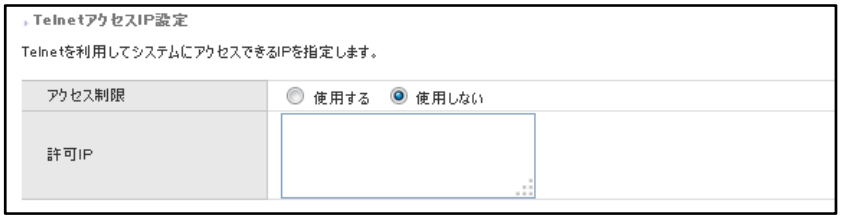
- アクセス制限 : アクセス制限機能の使用可否を設定します。
- 許可 IP : 許可 IP のリストは、アクセス制限を使用するに設定されている場合に適用されます。IP アドレスは1行に1IP を入力する必要がありクラス単位での入力も可能です。クラス単位で入力する場合、IP アドレスは″.″(ドット)で終わる必要があります。例えば'10.0.0.'を入力すると'10.0.0.1'から'10.0.0.255'までを意味します。ただし、IP range での入力方式はありません。

注意事項

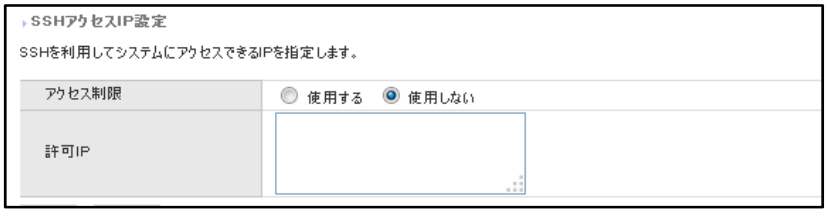
× HTTP アクセス制限機能を使用する場合は、内部ネットワークのセキュリティのためにユーザ(決裁者、個人ユーザ)と管理者(スーパー管理者、ログ閲覧者)は別に設定する必要があります。

× アクセス制限を使用するに設定した場合、現在接続しているスーパー管理者の IP は自動的に許可 IP に追加されます。

→ Telnet アクセス IP 設定 : Telnet を利用してシステムにアクセスする IP を制限します。各項目の説明は、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 を使用してシステムにアクセスする IP を制限します。各項目の説明は、上記の HTTP アクセス IP 設定を参照してください。



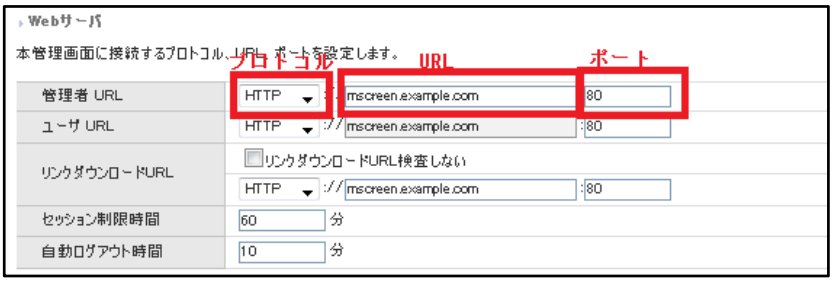
7.1.4. サービス

MailScreen の各サービスを制御して設定します。

設定方法

1. *環境設定*>システム>サービスをクリックします。
2. サービス設定画面が出力されます。各項目を設定した後下部の[設定]ボタンをクリックします。

   → Web サーバ:サーバに Web 基本のアクセス URL とセッション、自動ログアウト時間を設定します。

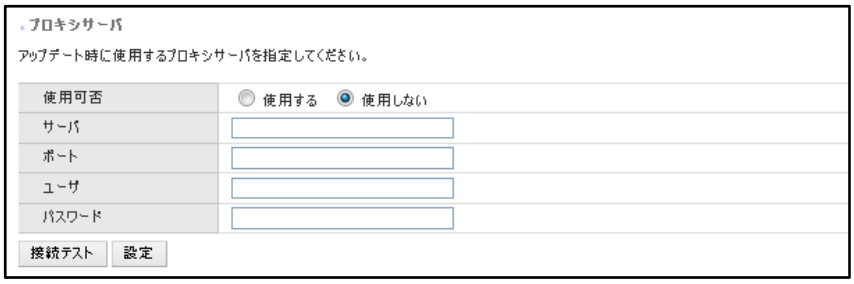


- 管理者 URL:権限がスーパー管理者/ログ閲覧者のとき Web-Admin にアクセスできる URL とポート、プロトコル情報を設定します。
  - ✓ プロトコル:HTTP または HTTPS を選択することができます。HTTPS はセキュリティが強化され、通信データが暗号化されます。HTTPS を使用するには証明書が必要であり、公的証明書がない場合は 9.1.2 証明書情報を参考にして自己署名証明書を作成することができます。
  - ✓ URL:基本的に MailScreen サーバに割り当てられたドメインと Web-Admin URL は同様ですが、別のアドレスを使用しなければならない場合、Web-Admin にアクセス可能な URL を設定します。
  - ✓ ポート:Web-Admin に接続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 がデフォルト値です。
- ユーザ URL:権限が決裁者/個人ユーザのユーザが Web-Admin にアクセスするための URL とポート、プロトコル情報を設定します。各項目の説明は、管理者 URL と同様です。
- リンクダウンロード URL:送信メールのポリシーによって、'添付ファイルリンク変換' が適用されたとき、添付ファイルをダウンロードするためのリンク URL を入力します。添付ファイルリンク変換の説明は 7.3.5 添付ファイルのリンク変換を参照してください。
  - ✓ リンクダウンロード URL 検査しない: リンク変換により添付ファイルのダウンロード時に要求される URL、ポートとアクセスする URL、ポートが一致するかを確認する機能の使用可否を設定します。

    この確認作業とは、リンクダウンロード用の URL は添付ファイル名等の情報から自動的に暗号化した形で提供されます。その暗号化した URL が正常に復号化されるかを一度確認する作業を言います。
- セッション制限時間:セッションが生成された後、制限時間が経過するまで、ユーザがページを要求していない場合、セッションが破棄され再ログインをする必要があります。

- 自動ログアウト時間：ログイン後、マウスまたはキー入力がない状態で指定の時間以上経過した場合、自動ログアウトされます。

→ プロキシサーバ：中央サーバとのパターン・ウィルス、エンジン等のアップデート時に使用するプロキシサーバを設定します。

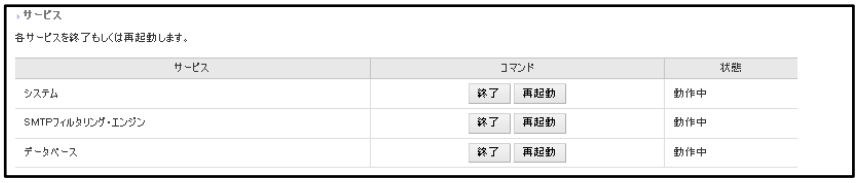


- 使用可否：プロキシサーバの使用可否を設定します。
- サーバ：プロキシサーバの IP または Hostname を入力します。
- ポート：ポートを入力します。
- ユーザ：プロキシサーバに認証が必要な場合、ユーザ情報を入力します。
- パスワード：プロキシサーバに認証が必要な場合、ユーザパスワードを入力します。
- 「接続テスト」ボタンを使用して適切なプロキシサーバとの接続確認が可能です。

注意事項

× プロキシサーバに誤った情報を設定すると、中央サーバとの通信が行われずにパッケージの一部機能が動作しないことがありますので注意してください。

→ サービス：MailScreen の各サービスを制御できます。



- システム：MailScreen が設置されているサーバを再起動させたり、終了させたりします。
- 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させたり終了させたりします。SMTP フィルタリングエンジンが終了した場合、メール受信ができませんので注意してください。
- データベース：DBMS を再起動させたり、終了させたりします。DBMS が終了した場合、Web-Admin の一部動作（メール管理、統計等）に問題が発生することを注意してください。

→ 時刻同期：システムの時刻を同期します。

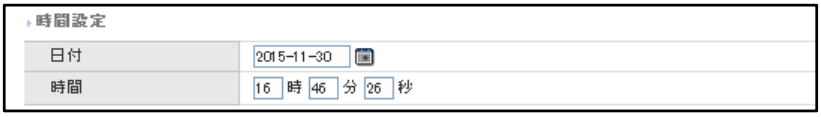
- 使用可否：時刻同期機能の使用可否を設定します。
- 使用ポート：ネットワーク環境により NTP または TIME を選択します。

- タイムサーバ：0.0.0.0～255.255.255.255 間の IP アドレス、またはサーバのホスト（HTTP：//を除いた HOST.COM 形式）情報を入力します。[テスト]ボタンをクリックすると入力したサーバの正常動作可否を検証します。
- 同期間隔：同期を実行する周期を選択します。

注意事項

× 時刻同期機能は、データログと同期等を実行するのにあたり、非常に重要な役割を果たします。システムがインストールされ、地域に応じた有効な同期サーバとポートを設定してください。

→ 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することができます。



注意事項

× 日付の設定時、年-月-日まで入力する必要があります。年は 4 桁からなる数値を入力する必要があり、月は 1～12、日は 1～31 の値のみ入力することができます。

× 時間設定、時間は 0～23、分は 0～59、秒は 0～59 の値のみ入力することができます。

→ 時間帯（タイムゾーン）：システムの Timezone を設定します。変更しようとする Timezone を選択し[設定]ボタンをクリックします。

注意事項

× Timezone 変更後、システムが再起動されるため Web-Admin に再アクセスするまで少なくとも 1 分～最大数分掛かります。

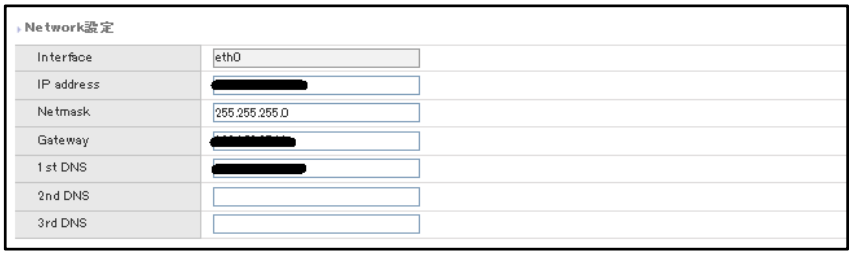
7.1.5. ネットワーク

MailScreen が設置され、サーバのネットワーク情報が変更された場合、変更された情報を設定します。

設定方法

1. *環境設定*>システム>ネットワークをクリックします。
2. ネットワーク設定画面が出力されます。各項目の説明は次のとおりです。

→ Network 設定：ネットワーク情報を設定します。インターフェイス情報はデフォルトのため無効化されています。0.0.0.0～255.255.255.255 の値で構成される IP address、Netmask、Gateway、1stDNS、2ndDNS、3rdDNS を設定します。ただし、DNS は IP ではなくドメインを入力することもできます。



注意事項

✕ IP、Netmask、Gateway は Web-Admin 接続と密接な関係がありますので修正するとき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 に変更するとこれ以上 test というドメイン名では接続ができません。DNS test での IP アドレスを 20.1.1.1 に変更すると再接続が可能です。しかし Netmask 等の情報を変更した場合にはこのような方法でも接続ができない場合がありますので、設定時には注意が必要です。

✕ DNS 情報は内部的な作業のために必要であり、通常のポリシー適用のために非常に重要な情報ですので、速度が速く安定して動作する DNS サーバを設定するようにします。

→ SMTP ブリッジ：MailScreen をメールサーバとブリッジ接続する場合に設定します。

- メールサーバ IP：設定した送信元であて先に向かうメールにポリシーを適用します。この項目は、メールサーバとのブリッジを構成するために設定します。次の項目を入力した後[追加]ボタンをクリックします。
  - ✓ 送信元：送信元 IP 情報を設定します。IP は単一 IP アドレスまたは CIDR 表記でサブネットを指定でき、指定可能な CIDR は 8 から 32 までです。
  - ✓ あて先：あて先 IP 情報を設定します。すべての外部へのあて先を設定したい場合は'ANY'を入力します。

✓ ポート：SMTP(25)、Submission(587)、SMTPS(465)ポートのうちから選択するか、管理者が任意にポートを入力します。

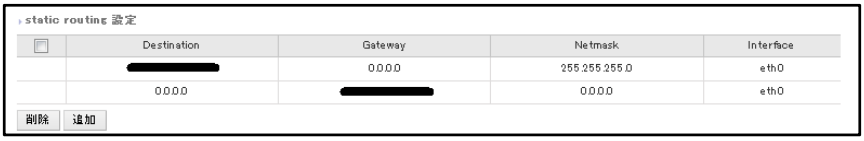
- SMTP バイパス IP：指定した IP から送信したメールは、ポリシーを適用せずに通過させます。IP は単一 IP アドレスまたは CIDR 表記でサブネットを指定することができ、指定可能な CIDR は 8 から 32 までです。
- MTU 設定 : Network Interface の MTU 値を設定します。最小値は、576、最大値は 1500 です。

注意事項

✕ SMTP ブリッジは、メールサーバとブリッジ構成のために設定することで、メールサーバと MailScreen サーバをクロスケーブルで接続するなどの追加作業が必要とされるためベンダーの技術サポートが必要です。

✕ 587、465 ポートを選択すると選択したポートでメールトラフィックが転送されるため *環境設定*>フィルタリング>SMTP>詳細機能設定の'SMTP Submission ポート(587)と'SMTPS ポート(465)'が使用するに設定されている必要があります。

→ static Routing 設定：MailScreen サーバのネットワークインターフェイスは、合計 4 つですが、サービスを提供するために、2 つネットワークインターフェイスを使用します。残り 2 つのネットワークインターフェイスの Routing を設定することができる機能です。



- [追加]：新しい Routing 情報を設定することができる情報入力画面が出力されます。

✓ Type：Host または Network を選択します。

✓ Destination：0.0.0.0～255.255.255.255 のあて先アドレスを入力します。

✓ Gateway：0.0.0.0～255.255.255.255 の Gateway アドレスを入力します。

✓ Netmask：Type を'Network'で選択した場合有効になります。0.0.0.0～255.255.255.255 の Netmask 値を入力します。

✓ Interface：ネットワークインターフェイスを選択します。

- [削除]：選択した Routing 情報を削除することができます。

7.2. フィルタリング

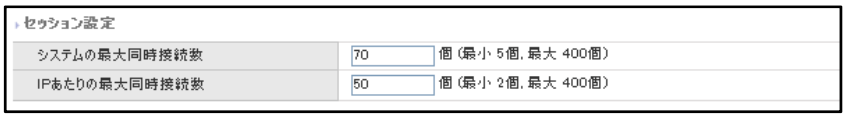
7.2.1. SMTP

セッションとメールデータ受信のための接続制御などの SMTP エンジン関連の設定をします。

設定方法

1. *環境設定*>フィルタリング>SMTP をクリックします。
2. SMTP 設定画面が出力されます。各項目を設定した後下部の[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。

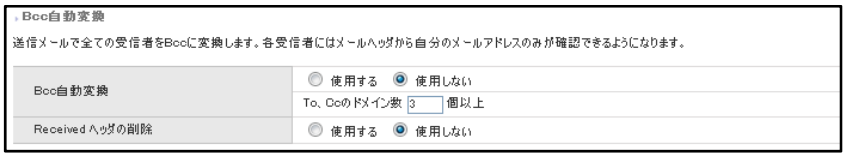


- システムの最大同時接続数：MailScreen の SMTP エンジンに同時に接続できる最大セッション数を設定します。設定された値を超過した接続要求は接続が拒否されます。
- IP あたりの最大同時接続数：1つの IP で同時に接続できる最大セッションの数を設定します。設定した IP あたりの最大同時接続数はシステム最大同時接続数より小さいことが必要です。

注意事項

× *環境設定*>フィルタリング>SMTP>詳細機能設定>SMTPS ポート（465）が「使用する」の時は、SMTPS セッションと同様な設定が適用されます。

→ Bcc 自動変換：受信者情報（メールアドレス）を保護するために外部に発信されたメールのすべての受信者（To、Cc）をBCC（Bcc）に強制的に変換する機能です。例えば受信者項目（To）が test@gmail.com、test@hotmail.com のメールを送信すると受信者情報が隠れて（Bcc）に自動的に変換され、メールの受信者（test@gmail.com）は、他の受信者情報（test@hotmail.com）を確認することができません。

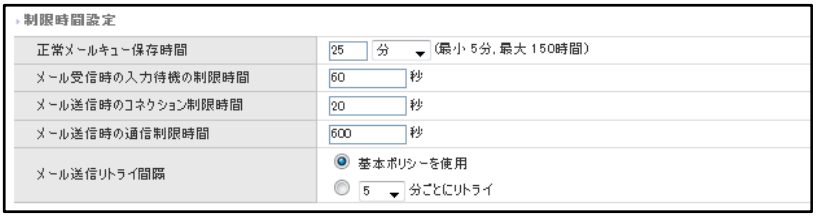


- Bcc 自動変換：使用するに設定した場合、送信メールのすべての受信者（To、Cc）を Bcc（Bcc）に自動的に変換させます。
  - ✓ To、Cc のドメイン数：To、Cc に含まれているドメイン数を設定します。'1'に設定する場合は、同じドメインを使用して受信者（To、Cc）に対しても Bcc に変換させます。
- Received ヘッダの削除：メールを受信するとヘッダに Received 情報（SMTP 接続情報）が記録され、この情報を削除します。

注意事項

× *環境設定*>メールサーバ>メールサーバに登録されているドメイン受信者の場合は、Bcc 自動変換が適用されません。

→ 制限時間設定：メールを送信するために、セッションを接続し、データを転送する各過程の時間を制限します。



- 正常メールキュー保存時間：SMTP が受信したメールのうち正常と判断されたメールは、送信キューに移動された後受信者に送信されます。この時、送信が直ちに成功しなかった場合はリトライキューに移されて一定間隔で再送を試みるようになります。通常メールキューの保存時間は、リトライキューの蓄積する時間を設定します。キューの保存時間を超過しても通常の送信ができない場合は、送信者に送信失敗メールを送信し通常メールキューに待機中となっていたメールは削除されます。
- 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することが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した場合、メール受信失敗として処理しセッションを終了させます。データが受信されると待機時間は 0 に初期化され、メール受信を継続することになります。
- 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、メールを設定されているメールサーバに転送するときの接続制限時間を設定します。この時間を超過した場合、接続失敗と見な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、メールを設定されているメールサーバに転送するときの通信制限時間を設定します。この時間を超過した場合、送信失敗と見な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、メールを設定されたメールサーバに転送することに失敗した場合、その後一定時間が経過後に再送信を試みるようになります。この時 '基本ポリシーを使用'(初期には送信を細かく試みるようになるが、時間が経過するとリトライ間隔が広がるポリシー)を使用すると内部的に設定された時間間隔で送信リトライします。'分ごとにリトライ'を選択すると指定した時間毎に送信をリトライします。

注意事項

× 制限時間を設定するときに時間をあまり短く設定すると円滑なメール受信が妨げられ、あまりに長く設定すると1つのメールを処理するのにかかる時間が長くなり SMTP 性能が低くなる可能性があります。設定するときには注意しなければなりません。

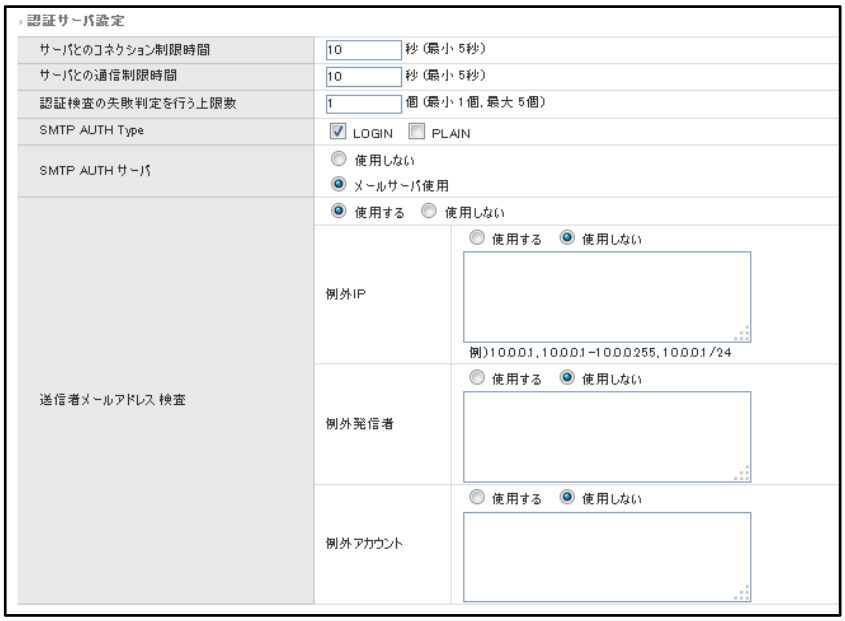
× 通常メールキューの保存時間があまりに大きければキューに多くのメールが蓄積されることがありますからシステムに負荷がかかることがあります。

→ 制限項目設定：SMTP がメールを受信したときにメールのサイズ、同報することができる数、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えた場合は、SMTP 接続を終了して受信を拒否します。最小値は'1'、最大値は'70'です。

- 最大同報数制限：一回の SMTP 接続により複数の受信者を指定する場合（RCPT TO）、許可する受信者数を設定します。受信されたメールの同報数がこの値を超えた場合、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 Received または Delivered 項目があります。この部分は実際のメールが送信された経路を意味し HOP が多いメールは、複数の経路を経由したことを意味します。多くのサーバを経由したメールは、スパムの可能性が高いので指定された 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 サーバなどの認証サーバとの接続時制限時間を設定します。設定された値を越えるとユーザが存在するものと見なします。



- サーバとのコネクション制限時間：外部の認証サーバと接続時の時間制限を設定します。認証を要請するサーバとの接続には制限時間中に行う必要があります。
- サーバとの通信制限時間：外部サーバとの通信時時間制限を設定します。認証を要請するサーバと接続が行われた後、データを確認し接続を終了するプロセスは通信制限時間内に行う必要があります。
- 認証検査の失敗判定を行う上限数：MUA が送信者の認証に失敗したとき、メール受信を拒否します。アカウント情報をランダムに代入してアカウント情報を取得した後 MailScreen サーバをスパム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 Authentication Type を設定します。認証方式は、LOGIN、PLAIN のみ支援されます。
- SMTP AUTH サーバ：認証を依頼する 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 により行われます。MailScreen は、MUA が送ってくる認証情報を SMTP AUTH サーバに転送して認証に成功したメールのみを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 が送ってくる認証情報をメールサーバに問い合わせ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

ールサーバにより追加できます。MUA が送ってくる認証の情報のうち ID にドメインが含まれている場合、該当するサーバを、ドメインがない場合はメールサーバの最初のサーバを認証サーバとして使用します。

注意事項

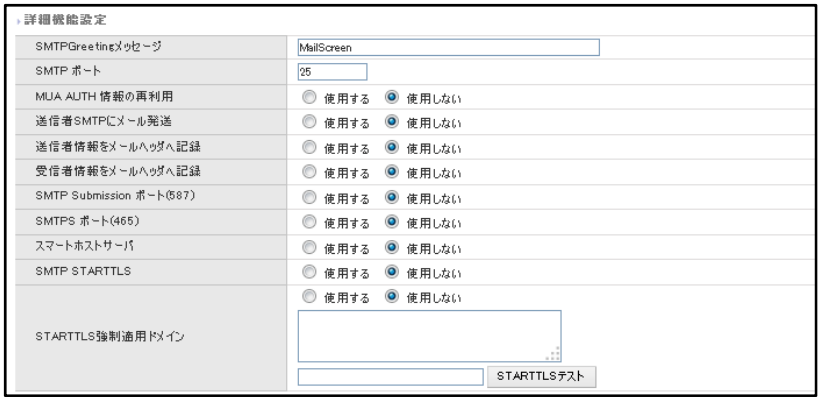
✕ MailScreen は、MUA がメールを送信するとき SMTP AUTH 情報の使用可否と SMTP AUTH サーバオプションに応じてメールを受信または拒否します。これについての説明は、次の表を参照してください。

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	不使用	認証失敗でメール受信拒否
使用	メールサーバ利用	メールサーバで認証のリトライ後、成功の時受信
未使用	不使用	認証無くメール受信
未使用	メールサーバ利用	認証無くメール受信

- 送信者メールアドレス検査：認証段階で認証アカウントとメールの送信者情報を確認し異なる場合、その SMTP 接続を終了させ送信拒否ログとして残します。
  - ✓ 例外 IP：例外 IP として登録され、送信者は検査を行いません。0.0.0.0～255.255.255.255 の有効な IP を 1 行ずつ入力します。
  - ✓ 例外発信者：例外発信者として登録されたメールの送信者は検査を行いません。@を含む有効なメールアドレスを1行ずつ入力します。
  - ✓ 例外アカウント：メールのドメイン情報に関係なく、例外アカウントに登録された送信者は検査を行いません。@を除くアカウントを 1 行ずつ入力します。

→ 返信メール設定：MailScreen は、受信者にメール送信が失敗した場合、送信者に返信メール(NDR： Non Delivery Report)を送信します。受信メールサーバからの拒否により送信に失敗した場合、拒否原因に応じた応答コードを含めます。返信メール機能の使用可否と返信メール発信者を設定します。

→ 詳細機能設定：その他 SMTP の動作を設定します。



- SMTPGreeting メッセージ：外部の送信主体が MailScreen SMTP サーバに接続したときに出力す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 が MailScreen にメールを送信したときに使用した SMTP AUTH 情報を MailScreen が送信者の SMTP サーバへ転送するときに再利用します。

注意事項

× MUA AUTH 情報の再利用オプションは、MUA がメールを送信するとき SMTP AUTH 情報を利用するかにより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転送します。次の表はこれに対する説明を簡略に示したものです。

MUA の SMTP AUTH 情報使用可否	MUA AUTH 情報の再利用オプション	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'のポリシーによってフィルタリングされたメールは、MUA AUTH 情報の再利用オプションが適用されません。

× MUA AUTH 情報の再利用オプションを使用する場合、*環境設定*>システム>基本情報>メール保存期間設定>メールのコピーの保存期間を、*環境設定*>フィルタリング>SMTP>制限時間設定>正常メールキュー保存時間以上に設定する必要があります。

- 送信者 SMTP にメール発送：このオプションを有効にした場合、MailScreen は、処理したメール送信者のドメインを確認、*環境設定*>メールサーバ>メールサーバに登録されている送信者の SMTP サーバに転送します。この時、登録されているメールサーバ情報に 'メール送信時に SMTP AUTH を使用'オプションが有効になっており SMTP AUTH ID と SMTP AUTH Password が登録されている場合はこの情報を利用してメールサーバに認証を実行します。

注意事項

× 'MUA AUTH 情報再利用'オプションは、'送信者 SMTP にメール発送'オプションより優先順位が高く、MUA がメールを送信するときに SMTP AUTH 情報を使用するかにより適用可否が変わります。MUA が SMTP AUTH 情報を使用しない場合、SMTP AUTH 情報がないため MUA AUTH 再利用オプションは、適用されません。次の表はこれに対する説明を簡略に示したものです。

MUA の SMTP AUTH 情報使用可否	MUA AUTH 情報の再利用オプション	送信者 SMTP にメール発送	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 でメール発送

- 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 項目を追加して送信者 IP とエンベロープ情報メール送信者を記録します。送信者の IP 情報は Received ヘッダを分析して得ることができますが、X-Original-SENDERIP オプション使用して容易に確認が可能です。
- 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ープ情報メール受信者を記録します。

注意事項

× 一般的に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を取得するには To ヘッダを確認すればよいのですが、このヘッダは発信者が任意に設定することが可能です。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 MailScreen は、この過程を省略し、容易にメールを分析できるように X-Original-*ヘッダを提供しています。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 に転送するエンベロープ情報をもとに得られます。実際のメール送受信は、このエンベロープ情報をもとに行われ、メールヘッダに含まれた情報と一致しないことがあります。

- SMTP Submission ポート(587)：SMTP Submission ポートの 587 番ポートの使用可否を設定します。
- SMTPS ポート(465)：SMTPS ポートの 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。スマートホストサーバオプションを'使用する'に設定した場合は、メールの送信時に参照するルーティング経路です。

  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

注意事項

× 本機能を'使用する'に設定した場合、*環境設定*>メールサーバ>スマートホストでスマートホストサーバ情報が設定されていることを確認するようにします。設定されていない場合、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 接続の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は、常に STARTTLS を介してメールを送信するように強制します。適用ドメインは、1 行ずつ記入する必要があります。この設定を使用するには、まず SMTP STARTTLS を'使用する'に設定する必要があります。

7.2.2. Scanner

スキャナーは SMTP が受信したメールを受け取り、フィルタリングを実行します。

設定方法

1. *環境設定*>フィルタリング>Scanner をクリックします。
2. スキャナー設定画面が出力されます。各項目を設定した後、下部の[設定]ボタンをクリックします。

→ フィルタリング設定：スキャナーがフィルタリングを実行する方式を設定します。

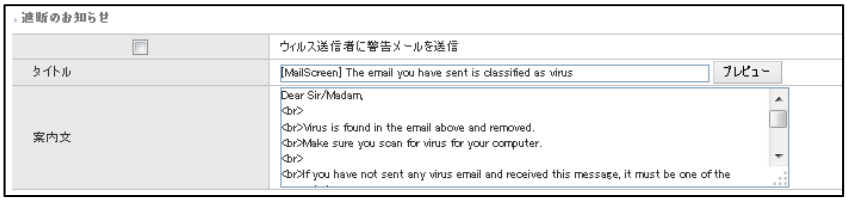
- メール本文の検索サイズ：メール本文をフィルタリングするメール本文が大きすぎるとフィルタリング性能が低下する場合があります。これを防止するために、フィルタリングを適用するメールの本文のサイズを指定してこの範囲内の内容のみを対象としてフィルタリングを実行します。

注意事項

× メール本文は、ヘッダ情報を除外した部分を指します。正確には各マイムのメッセージに該当する text/plain または text/html 等のパーツでそのヘッダ情報を除外した部分です。添付等のメッセージではなく、マイムパーツには該当がありません。

- Content-ID 署名ファイルのサイズ：メール本文に署名あるいは名刺等のイメージ形式で挿入された内容（例： Content-ID：XXXXX）の最小サイズを設定します。 一般的に、本文内のイメージファイルは、添付ファイルとして認識してフィルタリングを実行しますが、設定値よりも小さいサイズのイメージがメール本文に挿入されたときには、添付関連フィルタ条件で例外として処理されます。
- VPS フィルタ：VPS フィルタの適用可否を設定します。VPS に関した詳細説明は 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：ウィルスメールを検知した場合、送信者に遮断の警告メールの送信可否を設定します。警告メールを送信する場合、警告メールに関するいくつかの事項を設定でき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することができます。



注意事項

× ウィルスメール送信者のＥメールアドレスは受信できないか、他人のＥメールアドレスを盗むため、使用に注意してください。

7.3. 誤送信防止

誤送信防止は、外部へ送信されるメールの誤送信防止と重要な内部情報が流出されるのを防止するための機能です。内部ユーザが送信したすべてのメールは、フィルタリングされポリシーが適用され、各ポリシーのメール処理方式に応じて添付ファイル暗号化、添付ファイルリンク変化、送信遅延等の処理が行われます。

注意事項

× 誤送信防止メニューのいくつかの設定に応じてお知らせメールの文言と機能ボタンの有効可否が変わるので次の各機能の説明を注意してお読みになり設定してください。

7.3.1. 添付ファイルのダウンロード制限

指定した IP または IP 帯域のデバイス(モバイル/Web ブラウザ)のみ原本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 帯域ではなく、デバイスからアクセスする場合、メール詳細画面の原本タブが無効にされ、ダウンロードボタンおよび添付タブの添付ダウンロードリンクが解除され、原本および添付ファイルのダウンロードを行なうことができなくなります。

設定方法

1. *環境設定*>フィルタリング>誤送信防止をクリックします。
2. 誤送信防止の設定画面が出力されます。各項目を設定した後下部の[設定]ボタンをクリックします。

→ ダウンロード制限:添付ファイル時ダウンロード IP の制限機能の使用可否を設定します。

→ 許容 IP アドレス:原本を見る、および添付ファイルのダウンロードを許可する IP 情報を入力します。1行ずつに1つの IP(0.0.0.0-255.255.255.255)情報を入力する必要がありD クラス以上を省略して"."(ドット)で終わる IP アドレス帯域を入力できます。例えば'10.0.0.'と入力すると'10.0.0.1'から'10.0.0.255'までが適用されます。

7.3.2. テンプレート設定

お知らせメールについてテンプレート種類を選択できます。

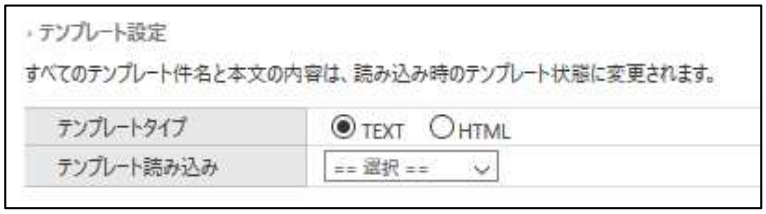
注意事項

× ウィルスお知らせメールとリンク変換方法が本文に挿入されたリンクファイルテンプレートについては HTML 形式/TEXT 形式で送信します。

設定方法

1. ***環境設定*>フィルタリング>誤送信防止**をクリックします。

2. 誤送信防止設定画面が出力されます。各項目を設定した後下部の「設定」ボタンをクリックします。



→ テンプレート種類: TEXT または HTML を選択できます。

- TEXT :HTML が除去された一般テキスト形式で送信します。
- HTML : HTML 形式で送信します。

→ テンプレート読み込み:サンプルテンプレートを提供します。変更時誤送信防止ページ内のすべてのテンプレート編集ダイアログのタイトルと本文内容が該当サンプルの形式に変更します。

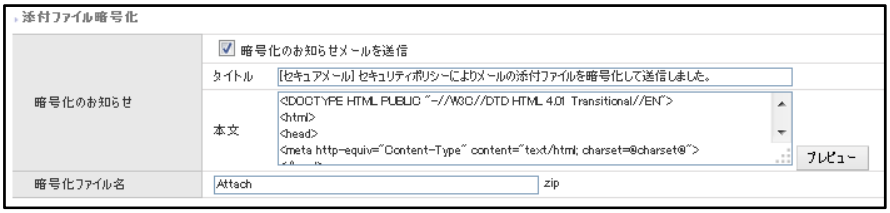
- English:英語の HTML サンプルテンプレートに変更します。
- Japanese HTML:日本語の HTML サンプルテンプレートに変更します。
- Japanese TEXT:日本語の TEXT サンプルテーブルに変更します。
- Korean:韓国語の HTML サンプルテンプレートに変更します。

7.3.3. 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、圧縮ファイルに対するパスワード情報はランダムに生成され、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>添付ファイル暗号化設定により一定時間後受信者に暗号化お知らせメールを送信することができます。

設定方法

1. *環境設定*>フィルタリング>誤送信防止をクリックします。
2. 誤送信防止の設定画面が出力されます。各項目を設定した後下部の[設定]ボタンをクリックします。



→ 暗号化のお知らせメールを送信:暗号化お知らせメール送信の可否、送信者に送信される暗号化お知らせメールのタイトルと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することができ、送信者に送信される暗号化お知らせメールは次のとおりです。

→ 暗号化ファイル名:送信される圧縮ファイル名を設定できます。最大 32 文字まで可能とし、拡張子は「.zip」に自動設定されます。拡張子を除いたファイル名を入力します。

- [パスワード送信]ボタン：パスワード送信をクリックすると受信者にパスワード情報を含めた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]ボタン：*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'受信者に X 分後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る場合は受信者にパスワードお知らせメールが自動転送されます。[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の自動送信オプションが設定されていても受信者にはパスワードが送信されません。設定された時間後に、[パスワード送信キャンセル]をクリックすると受信者にはパスワードがすでに送信されているために意味がありません。

7.3.4. 送信遅延

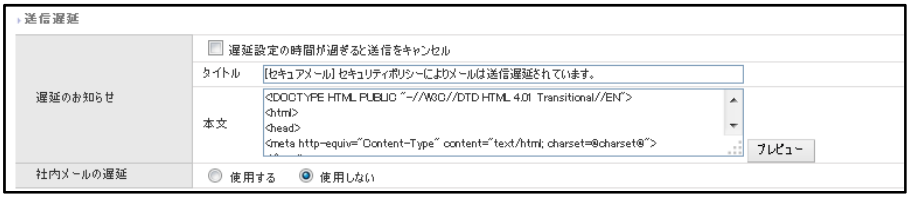
送信遅延機能は、誤送信防止のためにフィルタリングされたメールの送信を一時的に遅延させます。送信者には送信の遅延お知らせメールを送信してメール内容と受信者、CC 等を再度確認できるようにし、遅延お知らせメールの'今すぐ送信'または'送信キャンセル'オプションを利用してメールが誤送信されるのを防止します。

注意事項

- × 送信者が送信遅延されたメールに対して何も操作を実行しない場合、設定された時間が経過すると MailScreen は、自動的に受信者にメールを送信またはキャンセルします。したがって、送信遅延されたメールに対して送信者がメールの内容を必ず再度確認するようにお勧めします。
- × 受信者が内部受信者（MailScreen に登録されたドメインを使用しているメールアカウント）の場合、メールは送信遅延されません。

設定方法

1. *環境設定*>フィルタリング>誤送信防止をクリックします。
2. 誤送信防止の設定画面が出力されます。各項目を設定した後下部の[設定]ボタンをクリックします。



→ 遅延設定の時間が過ぎると送信をキャンセル：遅延時間が経過すると送信をキャンセルます。ポリシー追加時に設定した送信の遅延オプションよりも優先されます。

→ 社内メールの遅延：メールサーバに登録されたドメインの受信者にも送信時の遅延を適用することができます。

→ 遅延のお知らせ：遅延お知らせメールのタイトルと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することができます。遅延お知らせメールプレビュー画面は、次のとおりです。

- [今すぐ送信]：送信遅延されたメールが受信者にすぐに送信されます。
- [送信キャンセル]：送信遅延されたメールは受信者に送信されません。

7.3.5. 添付ファイルのリンク変換

メールの添付ファイルをダウンロード可能な形式のリンクに変換させます。リンク変換された添付ファイルは、ダウンロード時、設定によりパスワード情報が要求されることがあります。

注意事項

× 添付ファイルリンク変換のいくつかのオプションは、添付ファイルの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機能は、大容量のメール送信のためのものではなく、誤送信防止のために提供される機能です。したがってメール全体のサイズが約 50MB 以上の場合は、サーバとネットワークの状況により正常に処理されない場合がありますので注意してください。

設定方法

1. *環境設定*>フィルタリング>誤送信防止をクリックします。
2. 誤送信防止設定画面が出力されます。各項目を設定した後下部の[設定]ボタンをクリックします。

→ GIAGPOD 連動：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発送されず、メール詳細を読む時のダウンロード有効/無効/パスワード送信機能は提供していません。GIGAPOD に関する説明は http://www.tripodworks.co.jp/product/gigapod/ を参照してください。

- 使用しない：GIGAPOD と連携しません。
- UTF-8 として連携：UTF-8 エンコーディングを使用して GIGAPOD と連携します。GIGAPOD 2010 以降の製品に対応します。
- Shift-JIS として連携：Shift-JIS エンコーディングを使用して GIGAPOD と連携します。GIGAPOD OFFICEHARD で使用します。

→ リンク制御：添付ファイルへのリンクを制御します。

- ダウンロードウェブブラウザー制限：本機能は、許可された受信者以外のユーザがダウンロード URL を悪用して添付ファイルをダウンロードするのを防止しようと提供する機能です。例えば、許可された受信者が最初にダウンロードした PC や Web ブラウザ以外の他の PC や他の Web ブラウザではダウンロードできません。次にこれに対する説明を示した表です 。

区分	1st ダウンロード	2nd ダウンロード	3rd ダウンロード
PC	A pc	B pc	A pc
ブラウザ	IE	IE	Firefox
ダウンロード	可	不可	不可

- 全てのファイルリンクを一斉に無効化：すべてのメールの添付ファイルへのリンクが無効になります。既存にすでに送信されたか今後送信するメールに対して一括して Download URL を無効化するために使用します。つまり、サーバ上に存在するすべての添付ファイルを一括的にダウンロード禁止にすることができます。

→ リンクにパスワードを適用：添付ファイルリンク変換時にパスワードを適用します。パスワードが適用される場合、送信者にパスワードお知らせメールが送信され受信者には直接パスワードメールを送信したり*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により受信者にパスワードお知らせメールが自動的に送信したりすることができます。受信者は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ときパスワード情報を入力してからダウンロードが可能です。1通のメールに複数の添付ファイルが含まれている場合、それぞれのファイルに別々の URL が生成されこの時のパスワードは同じものが要求されます。ただし、'添付ファイ

ル暗号化した後リンク変換'動作が適用される場合には添付ファイル暗号化だけが適用されダウンロード時にはパスワードが要求されません。

→ リンク有効期間：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は削除され、ダウンロードすることができなくなります。

→ リンク伝達方法： 添付ファイルリンク内容の伝達する方法を設定します。添付で挿入時 HTML または TXT ファイルで添付ファイルリンクを提供します。本文に挿入時は受信者に送信されるメール上段にリンクファイルテンプレートを追加して送信します。

→ 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のリンクメールのテンプレートを設定します。メールの本文とタイトルについて編集できます。[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。リンク変換メールは、次のとおりです。

→ リンクの変換ファイル名：送信するリンクの変換ファイル名を設定できます。最大 32 文字まで可能で、拡張子は[.html/.txt]に自動的に設定されます。拡張子を除いたファイル名を入力します。

→ リンク変換のお知らせ：メールの送信者に送信されるリンク変換お知らせメールのテンプレートを設定します。メールの本文とタイトルについて編集できます。[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。リンク変換お知らせメールは、次のとおりです。

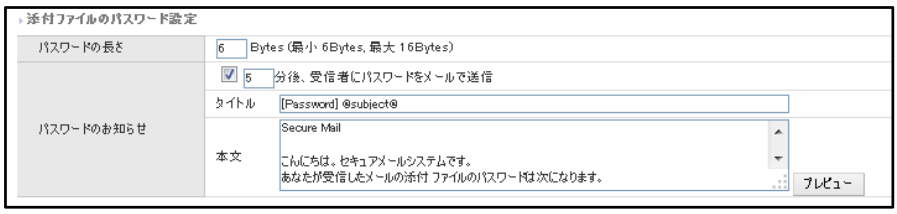
- [パスワード送信]ボタン：*環境設定*>フィルタリング>誤送信防止>添付ファイルのリンク変換の'リンクにパスワードを適用'項目が'使用する'にチェックされている場合、添付ファイルへのリンク変換時にパスワードが適用され、リンク変換お知らせメールの[パスワード送信]ボタンが有効化されます。もし'使用する'にチェックされていない場合は、パスワード関連ボタン（パスワード送信/パスワード送信をキャンセル）は有効になりません。パスワード送信ボタンをクリックすると受信者にパスワードお知らせメールが送信されます。
- [パスワード送信をキャンセル]ボタン：*環境設定*>フィルタリング>誤送信防止>添付ファイルのリンク変換 'リンクにパスワードを適用' が'使用する'にチェックされており、*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'受信者に X 分後パスワードをメールで送信' が設定されている場合、リンク変換お知らせメールで[パスワード送信をキャンセル]ボタンが有効化されます。' パスワード送信をキャンセル' 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せん。
- [添付ファイルを有効化]ボタン：添付ファイルのリンクが無効になっている場合、送信者が[添付ファイルを有効化]ボタンをクリックすると該当メールの添付ファイルリンクが有効化され、受信者は添付ファイルをダウンロードできます。
- [添付ファイルを無効化]ボタン：該当メールの添付ファイルリンクを無効化させます。送信者が[添付ファイルを無効化]ボタンをクリックした場合、受信者は該当メールの添付ファイルをダウンロードできません。誤送信防止のために添付ファイルを廃棄する効果があります。
- [サイトショートカット]ボタン：Web-Admin ページから直接リストを検索してメール詳細情報を使用した受信者別ダウンロード状況等を確認することができます。

7.3.6. 添付ファイルのパスワード設定

添付ファイル暗号化と関連したオプションを設定します。

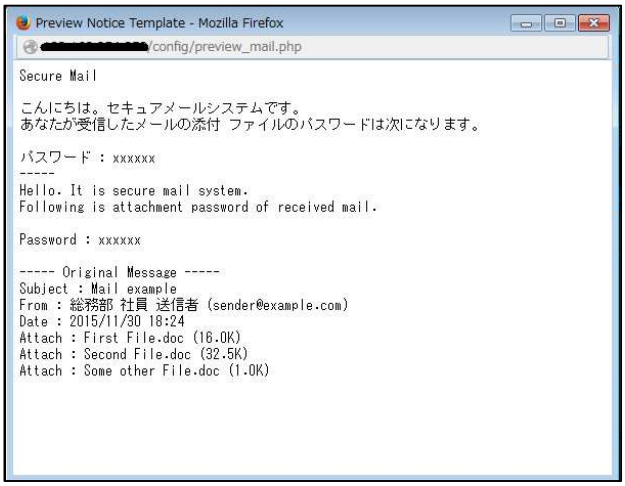
設定方法

1. *環境設定*>フィルタリング>誤送信防止をクリックします。
2. 誤送信防止設定画面が出力されます。各項目を設定した後下部の[設定]ボタンをクリックします。



→ パスワードの長さ：添付ファイルが暗号化されたとき、パスワードの長さを設定します。最小 6 から最大 16 まで設定できます。パスワードはランダムに毎回新たに生成され 0-9a-zA-Z が混在して生成されます。

→ パスワードのお知らせ：パスワードお知らせテンプレートと受信者に自動的に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' オプションは、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的に送信されます。[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事前に確認することができます。パスワードお知らせメール画面は次のとおりです。



7.3.7. 遮断

外部へ送信されるメールを遮断します。外部へ流出してはならない重要な情報にこの動作を適用させると情報流出を防止できます。

設定方法

1. *環境設定*>フィルタリング>誤送信防止をクリックします。
2. 誤送信防止設定画面が出力されます。各項目を設定した後下部の[設定]ボタンをクリックします。

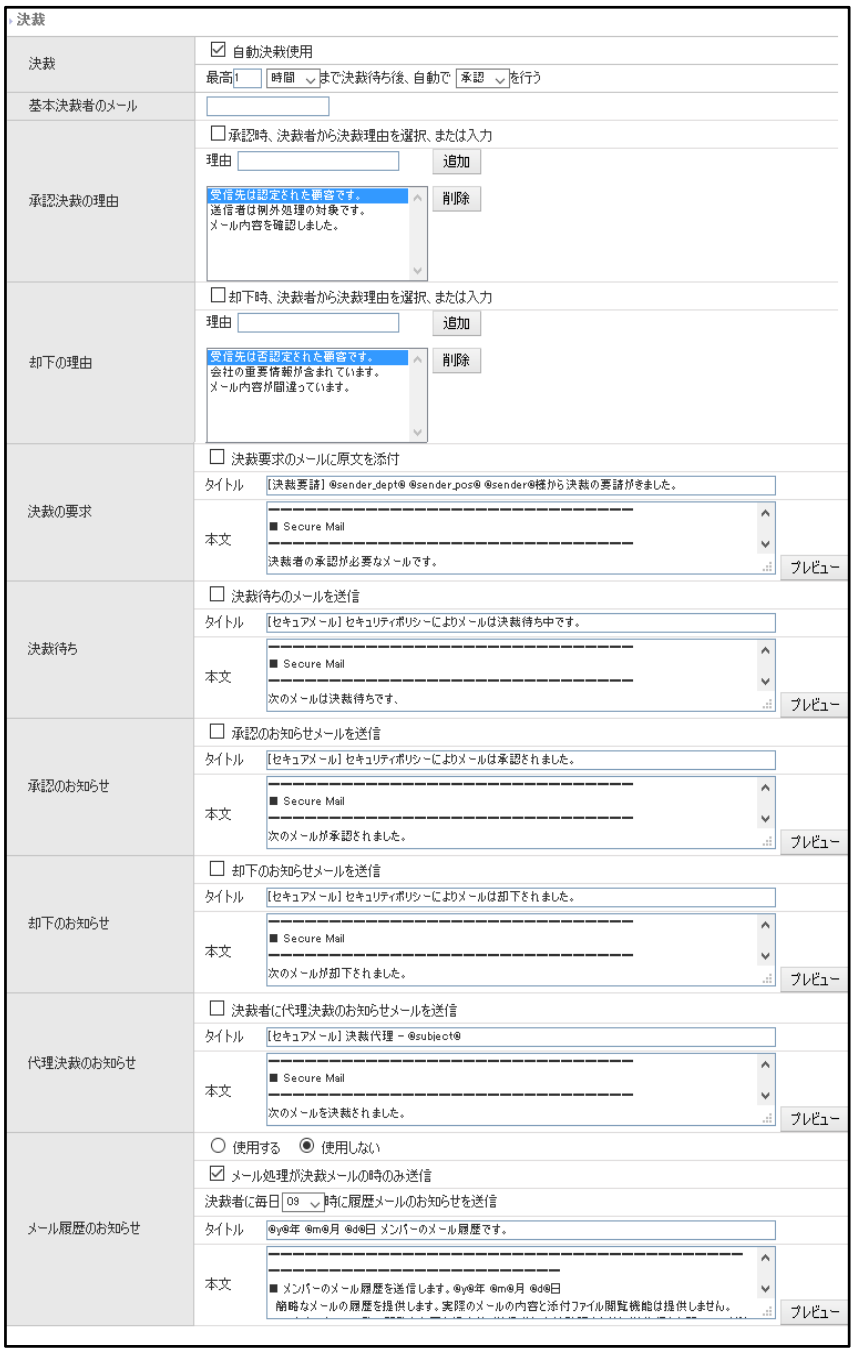
→ 遮断のお知らせ：送信者が受ける遮断お知らせメールの内容とタイトルテンプレートを変更できます。[プレビュー]ボタンをクリックすると編集された内容を確認することができます。遮断お知らせメールプレビュー画面は次のとおりです。

7.3.8. 決裁

メールの送信を保留し MailScreen で指定されている決裁者に決裁を要求します。決裁者は決裁要求メールにより送信者が送信したメールを確認することができます。決裁者が承認した場合、該当メールは受信者に送信され、却下した場合は、該当メールは送信が遮断されます。もし決裁者の承認なしに一定時間が経過すると *SMTP Filter*>ポリシー管理>ポリシー追加時の設定オプション、または *環境設定*>フィルタリング>誤送信防止>決裁で設定したオプションにより自動的に承認または却下されます。

設定方法

1. *環境設定*>フィルタリング>誤送信防止をクリックします。
2. 誤送信防止設定画面が出力されます。各項目を設定した後下部の[設定]ボタンをクリックします。



→ 決裁：決裁の関連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保留されている状態で決裁満了時間が経過すると自動的に決裁する機能を活性化します。承認/却下可否は下の自動決裁設定またはポリシーで設定した自動決裁設定に従います。
- 自動決裁設定：指定した時間、決裁の待機中のメールを自動的に承認または却下するように設定します。

→ 基本決裁者のメール：基本決裁者のメール情報を設定します。ポリシー追加時に決裁者が指定されていない場合、本項目の基本決裁者に決裁が要求されます。

→ 承認決裁の理由 : メールの承認理由を設定します。この機能は、モバイルウェブを通じて支援されている機能であり、各メールの決裁理由は *SMTP Filter*>メールで該当メールのメール詳細表示で確認することができます。

- 承認時、決裁者が決裁理由を選択、または入力 : 決裁者は承認理由を入力することによりメールの承認をすることができます。
- [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ます。[削除]ボタンを使用して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。各項目に対する説明は'承認決裁の理由'と同じです。

→ 決裁の要求 : 決裁要求に関連した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求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 : 決裁要求メールのタイトルと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することができます。決裁要求メールのプレビュー画面は次のとおりです。

  - ✓ 承認 : 決裁者が承認ボタン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送信されます。
  - ✓ 却下 : 決裁者が却下ボタン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送信されます。
  - ✓ メール確認 : 決裁者がメール確認ボタンをクリックすると該当メールのメール詳細確認画面が表示され該当メールのヘッダ、原文、内容、転送結果、添付ファイル名等を確認することができます。
  - ✓ 決裁する : 決裁者が決裁するボタンをクリックするとメール管理ページに移動し決裁者はこの機能を使用して容易に決裁要求メールをすべて確認することができます。

→ 決裁待ち : 決裁待機メール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 : 送信者に決裁待ちお知らせメールが送信されます。
- テンプレート : 決裁待ちメールのタイトルと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することができます。決裁待ちメールのプレビュー画面は次のとおりです。

→ 承認のお知らせ：承認のお知らせメール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：決裁者が承認する場合、もしくは自動的に承認された場合、送信者に承認のお知らせメールが送信されます。
- テンプレート：承認のお知らせメールのタイトルと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することができます。承認のお知らせメールのプレビュー画面は次のとおりです。

→ 却下のお知らせ：却下の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：決裁者が却下する場合、もしくは自動的に却下された場合、送信者に却下のお知らせメールが送信されます。
- テンプレート：却下のお知らせメールのタイトルと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することができます。却下のお知らせメールのプレビュー画面は次のとおりです。

→ 代理決裁のお知らせ：代理の決裁お知らせメール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ことを知らせるお知らせメールが送信されます。
- テンプレート：代理決裁のお知らせメールのタイトルと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することができます。代理決裁のお知らせメールのプレビュー画面は次のとおりです。

→ メール履歴のお知らせ：被決裁者の昨日分のメール送信履歴を収集し決裁者に送信する送信履歴お知らせメールを設定できます。

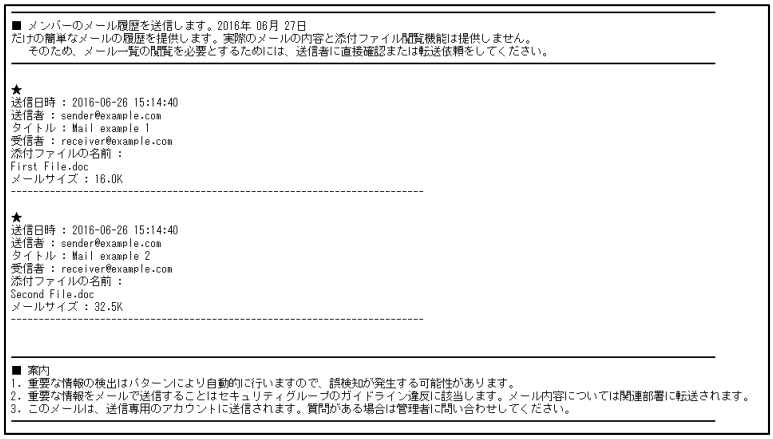
注意事項

× メール送信履歴は被決裁者のメール内ポリシーに適応されたメールに限り、決裁者本人のメールデータは除外されます。

× メール送信履歴は簡単な表で提供され、別途リンクによるメール内容および添付ファイル内容閲覧機能は提供しません。

- 使用可否：メール履歴のお知らせメールを送信するか否かの選択を行います。
- メール処理が決裁メールの時のみ送信：メール処理が決裁処理の送信履歴だけを収集し送信します。
- 決裁者に毎日[ ]時に履歴メールのお知らせを送信：決裁者に、指定された時間自動的に送信履歴お知らせメールが送信されます。

- テンプレート：送信履歴お知らせメールのタイトルと本文について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することができます。送信履歴お知らせメールのプレビュー画面は次のとおりです。



7.3.9. 通過

特定メールを通過させます。本機能を利用して特定メールをポリシーから例外適用することができます。統計およびメール管理を通じて通過されたメールのみを分析して社内から外部へ流出されるメールに対して容易にモニタリングを行うことができます。通過機能と関連した設定は 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

特定メールを指定されたルーティングサーバに送信します。特定メールを別の独立したサーバで収集したり経由したりするときルーティング指定機能を利用します。ルーティング指定機能と関連した設定は 4.1.2 ポリシー追加を参照してください。

7.3.11. ポリシー適用お知らせ

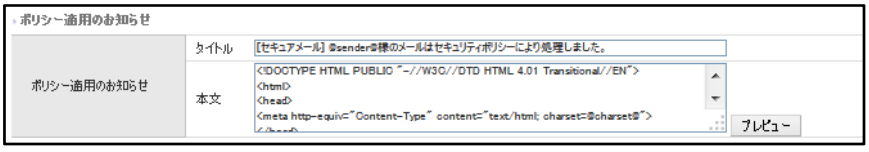
外部に送信されるメールにポリシーが適用された場合、該当メールを送信者に知らせします。

注意事項

× ポリシー適用お知らせテンプレートを変更する場合エンジン自動アップデート時変更履歴が初期化される場合がありますので注意する必要があります。

設定方法

1. *環境設定*>**フィルタリング**>**誤送信防止**をクリックします。
   誤送信防止設定画面が出力されます。各項目を設定した後下部の[設定]ボタンをクリックします。



→ ポリシー適用のお知らせ：送信者が受けるポリシー適用のお知らせメールの内容とタイトル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することができます。ポリシー適用のお知らせメールプレビュー画面は次のとおりです。

7.4. メールサーバ

MailScreen で処理したメールをメールサーバに送信するとき、発信者のドメインを参照してどのサーバで送信するかを決定します。つまり、メールが MUA から MailScreen 導入前に配信すべきメールサーバ情報を設定します。

7.4.1. メールサーバ管理

設定方法

1. *環境設定*>メールサーバ>メールサーバをクリックします。
2. メールサーバ管理画面が出力されます。
3. メールサーバ管理画面の上部、下部の説明は次のとおりです。

→ 1_[検索]：検索条件(ドメイン、サーバ IP、ポート)を選択した後検索語を入力します。[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。

→ 2_[追加]：メールサーバを追加します。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。

→ 3_[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。

→ 4_[ファイル保存]：検索されたメールサーバリストをエクセルファイルに保存します。

→ 5_リスト数設定：ページごとの出力するメールサーバ数を設定します。

→ 6_[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変更することができます。情報変更項目は 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。

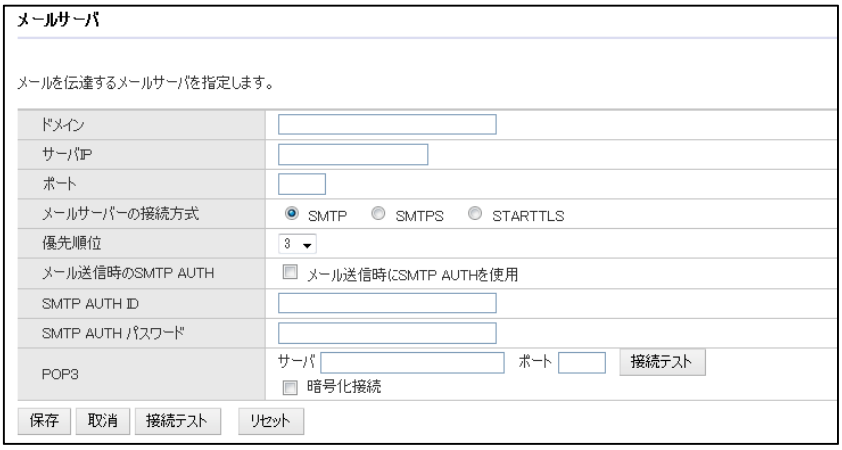
注意事項

× メールサーバを誤って設定するとメールが正常に受信されないなどの問題が発生します。注意する必要があります。

× メールサーバとの接続テスト時、ネットワーク環境がよくない場合、有効なメールサーバでも検証失敗というメッセージが表示されることがあります。

設定方法

1. *環境設定*>メールサーバ>メールサーバをクリックします。
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. メールサーバ追加画面で次の値を入力します。



→ ドメイン:メールサーバのドメイン情報を入力します。

→ サーバ IP:転送するサーバの 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 で入力することができ、1つのドメインにメールサーバは最大 5 個まで登録することができます。

→ ポート:1～49151 のポート情報を入力します。省略した場合 25 で設定されます。

→ 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 の中から選択します。

→ 優先順位:1～5 の優先順位を設定します。優先順位は数字が大きいほど高く1つのドメインに複数台のメールサーバが設定されている場合、優先順位が高いメールサーバが優先的に使用されます。

→ メール送信時の SMTP AUTH:メールを送信するときに、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は、以下の 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 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。

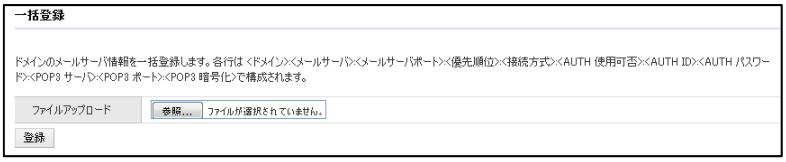
→ POP3:POP3 サーバ情報を入力します。*環境設定*>システム>アクセス制御>ログイン情報で POP3 を設定した場合ログイン時に使用される情報です。

4. [保存]ボタンをクリックします。現在の作業を取り消したい場合、[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との接続をテストします。[リセット]ボタンをクリックすると入力されたすべての情報が初期化されます。

7.4.3. 一括登録

設定方法

1. *環境設定*>メールサーバ>一括登録をクリックします。
2. メールサーバー括登録画面で[参照]ボタンをクリックして該当ファイルを設定後[登録]ボタンをクリックします。



注意事項

- ✕ 1つのドメインで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ラインに1つのメールサーバ情報を設定し各フィールドの区分は':'文字で構成します。
  (ex)a.com:10.0.0.1:25:1:test:password

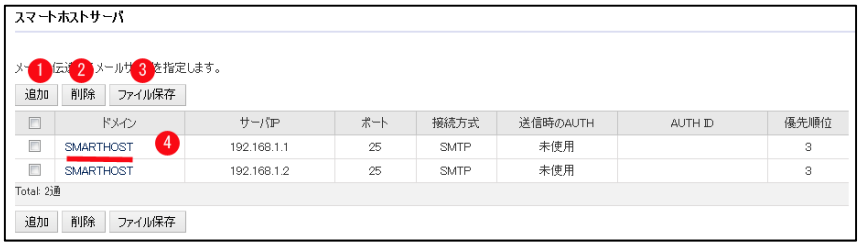
3. 失敗した場合エラーメッセージが出力され、成功した場合登録されたドメインリストが画面に出力されます。

7.4.4. スマートホスト

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'に設定した場合参照されるサーバ情報を管理します。

設定方法

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. スマートホスト管理画面が出力されます。
3. スマートホスト管理画面の上部、下部の説明は次のとおりです。



→ 1_[追加]:スマートホストサーバを追加します。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。

→ 2_[削除]:選択したスマートホストを削除します。

→ 3_[ファイル保存]:スマートホストサーバリストをエクセルファイルに保存します。

→ 4_情報修正:スマートホストサーバの情報のうち、ドメイン名をクリックすると情報を変更できます。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。

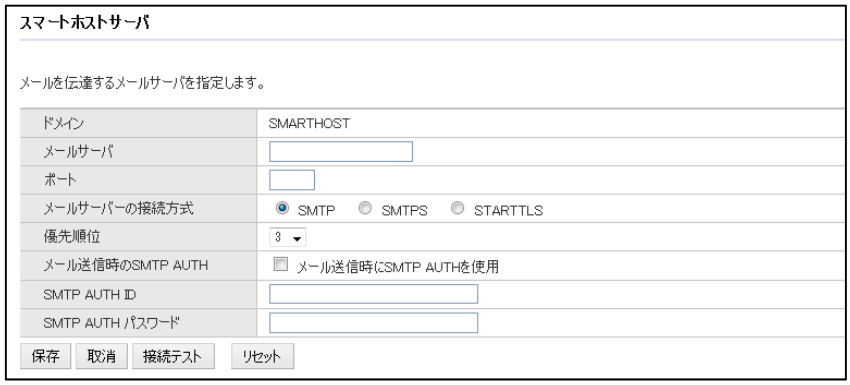
注意事項

- ✕ *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、スマートホストサーバをすべて削除した場合、スマートホスト機能が正常動作されない場合がありますので注意してください。

7.4.5. スマートホスト追加

設定方法

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. リストメニューの [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画面で次の値を入力します。



→ ドメイン：スマートホストサーバのドメイン情報は、メールを送信するのには意味がない情報です。デフォルト値（SMARTHOST）に固定しています。

→ メールサーバ：メールを転送するサーバ 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 のポート情報を入力します。省略した場合 25 で任意に設定されます。

→ 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 の中から選択します。

→ 優先順位：1～5 の優先順位を設定します。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：メールを送信するときメールサーバに AUTH 認証を要請します。オプションを設定する場合は、以下の SMTP AUTH ID とパスワードを入力必要があります。

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

→ 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。

4. [保存]ボタンをクリックします。現在の作業を取り消したい場合は、[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との接続をテストします。[リセット]ボタンをクリックすると入力されたすべての情報が初期化されます。

注意事項

× 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良くない場合は有効なサーバでも検証失敗というメッセージが表示される場合があります。

7.4.6. リレー

MailScreen のデフォルトのリレーポリシーは不許可です。したがって、MailScreen を介してメールを送信するためにはリレー設定が必要です。もし、MailScreen で許可されていないユーザのメール送信を許可する場合、スパマーが迷惑メールサーバとして悪用する可能性があるからです。メール送信のため MailScreen に接続するユーザの IP アドレスまたは IP アドレス帯域は、リレーを許可するように登録します。

設定方法

1. *環境設定*>メールサーバ>リレーをクリックします。
2. リレーの管理画面の上部、下部の説明は次のとおりです。

→ 1_[登録]：許可もしくは遮断で設定する IP または IP 帯域を登録します。

- IP：0.0.0.0-255.255.255.255 の IP を設定します。IP アドレスの入力時、D クラス以上を省略して"."(ドット)で終わる IP アドレス帯域を入力できます。例えば '10.0.0.'を入力すると'10.0.0.1'から'10.0.0.255'まで適用します。
- 区分：リレーの許可可否を設定します。
- 満了日：リレー適用時間を制限します。満了時間を経過したリレー設定は動作しません。
- メモ：リレーの関連説明を入力します。

注意事項

× 1つの動作(allow/deny)に重複 IP 設定を許可しません。例えば 10.0.0.1 が許可で登録されている状態で'10.'を再度許可で登録できません。'10.'は、'10.0.0.1'を含むため互いに重複した IP であると見なすためです。反対の場合の登録も許可されません。

× さらに詳しく記入した IP が高い優先順位を持ちます。例えば'10.'を拒否で登録し'10.0.0.1'を許可で登録すると'10.'台のすべての IP は拒否されますが '10.0.0.1'は許可されます。

→ 2_[削除]：選択したリレーIP をリストから削除します。

→ 3_リスト数設定：ページごとの表示されるリレーIP リストの数を設定します。

→ 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ラインに1つのドメインを'@x.x'形式で設定する必要があります。

→ 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ラインに1つのメールアカウントを'x@x.x'形式で設定する必要があります。

注意事項

× リレーの許可するドメインとメールアカウント情報が外部に流出された場合 MailScreen サーバがオープンリレーで悪用される場合がありますので十分に注意する必要があります。

7.5. 維持保守

MailScreen を常に最適化された状態を維持するためにエンジン自動アップデート、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 パッケージの更新が必要な場合は、自動的に中央のエンジンアップデートサーバから必要なデータをダウンロードしてパッチします。エンジン自動アップデートは毎時間パッチの存在有無を確認しています。

注意事項

- × 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と[リアルタイムアップデート]ボタンが表示されます。
- × アップデート履歴がある場合は、[変更履歴表示]ボタンが生成されログ内容より詳細なアップデート履歴を確認することができます。

設定方法

1. *環境設定*>維持保守>エンジン自動アップデートをクリックします。
2. エンジン自動アップデート管理画面の上部、下部の説明は次のとおりです。

→ 1_パッケージバージョン情報：現在パッケージ、最新パッケージバージョンと自動アップデート設定情報を表示します。

→ 2_リスト数：ページごとの表示されるログのリストを設定します。

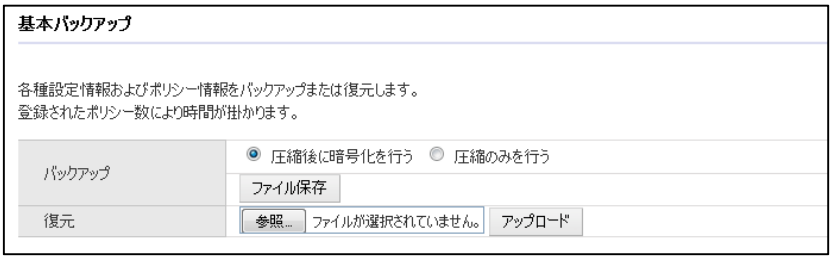
→ 3_アップデートログ：自動アップデートされた履歴を時間、状態、説明項目を利用して表示します。

7.5.2. 基本バックアップ

データ損失に備える目的で提供される機能で、Web で簡単にバックアップ・復元が可能です。自動的にバックアップされるように設定されているリストは、管理者が追加したポリシー、Black list/White list、環境設定値等です。

設定方法

1. *環境設定*>維持保守>基本バックアップをクリックします。
2. 基本バックアップ画面の機能の説明は次のとおりです。



→ バックアップ：バックアップファイルを圧縮のみ行うか、圧縮後暗号化まで行うかを選択した後[ファイル保存]ボタンをクリックします。

→ 復元：[参照]ボタンをクリックした後バックアップされたファイルを選択し、[アップロード]ボタンをクリックします。

注意事項

× 新しいバージョンにアップグレードする時に万が一のデータ損失に備えて、基本バックアップを行ってください。

× メールデータと DB データはバックアップされません。

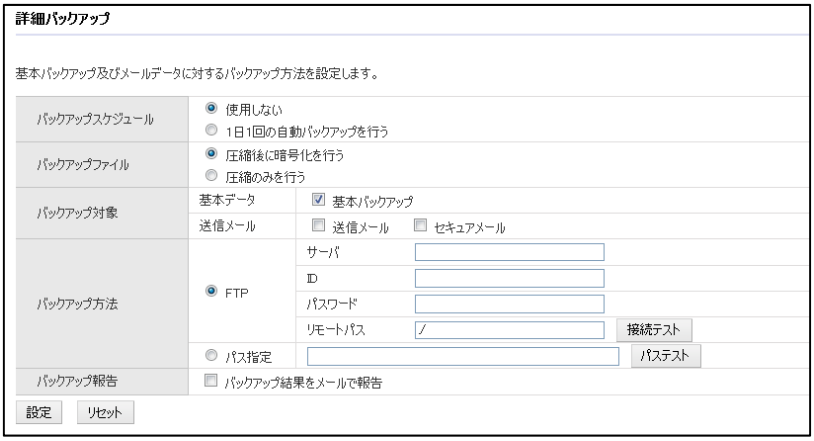
× 復元作業は、同じバージョンでバックアップされたデータで実行する必要があり下位バージョンや上位バージョンでバックアップされたデータを復元する場合、サービスが正常に動作しないことがあります。

7.5.3. 詳細バックアップ

メールデータと DB データまでバックアップすることができます。

設定方法

1. *環境設定*>維持保守>詳細バックアップをクリックします。
2. 詳細バックアップ画面機能の説明は次のとおりです。



→ 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。

→ バックアップファイル：バックアップファイルを圧縮のみ行うか圧縮後暗号化までを行うかを選択します。

→ 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をバックアップします。
- 送信メール：送信メールまたはセキュアメールのログと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 サーバで転送または内部パスを指定します。

- FTP：FTP サーバでバックアップファイルを転送・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に移動するディレクトリを入力します。移動せずにログイン後デフォルトで設定されたディレクトリにバックアップを記録する場合、“./”だけを入力します。［接続テスト］ボタンをクリックすると入力した FTP 情報が正しいか否かのテストすることができます。
- パス指定：MailScreen が設置されたサーバの内部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、生成されたフォルダ内にバックアップファイルが保存されます。バックアップに経過した時間、処理結果等の情報をスーパー管理者アカウントに E メールを送信することができます。

→ バックアップ報告：バックアップに経過した時間、処理結果等の情報をメールでスーパー管理者のアカウントに送信します。

注意事項

- × 詳細バックアップは、前日データのみをバックアップし、メールデータと DB データまでのバックアップを実行します。
- × *環境設定*>システム>基本情報の'メール保存期間と'データ保存期間'で設定した期間を周期でバックアップすることを推奨します。サイトにより保存期間が短い時間蓄積するログとデータの量が多い場合は保存期間とバックアップ期間を減少するようにしてください。
- × 詳細バックアップにより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/sniper/web-aux/tools/restore [DIR|FILE]コマンドを利用します。データ量により数分から数時間かかることがあります。
- × バックアップファイルは、次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

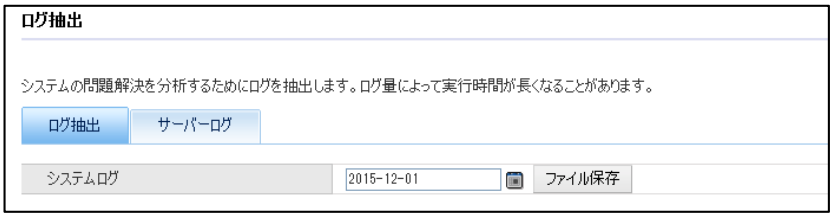
7.5.4. ログ抽出

システムに問題が生じた場合、問題を分析するためにシステムログを抽出する機能を提供しています。

設定方法

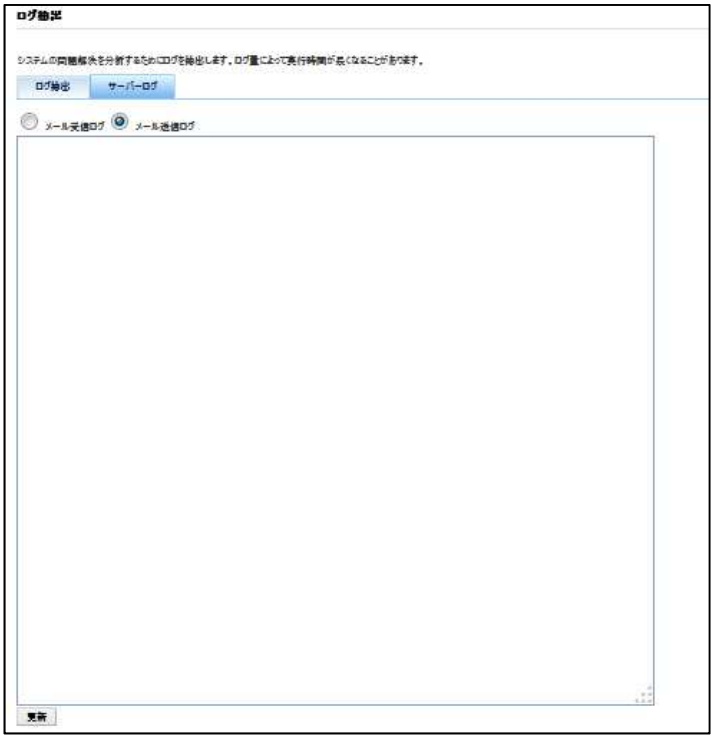
1. *環境設定*>維持保守>ログ抽出をクリックします。
2. ログ抽出画面の機能の説明は次のとおりです。

→ ログ抽出:システム運用と動作と関連したシステムログを抽出します。



- システムログ:抽出しようと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[再読込]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[再読込]ボタンをクリックします。

7.5.5. パッケージパッチ

手動パッチが必要な場合は、パッチファイルにより直接適用する機能を提供しています。自動更新機能とは関係なく必要な場合にのみ使用することができます。

設定方法

1. ***環境設定*>維持保守>パッケージパッチ**をクリックします。
2. パッケージパッチ画面のパッチ適用・パッチ履歴機能の説明は次のとおりです。

→ 1_[適用]:提供されたパッチファイルをアップロードした後に適用します。

→ 2_[ファイル保存]:検出されたパッチ履歴をエクセルファイルに保存します。

→ 3_[パッチ履歴]:本メニューにより適用されたパッチ履歴を示します。パッチ名をクリックすることによりパッチスクリプトのログを確認することができます。

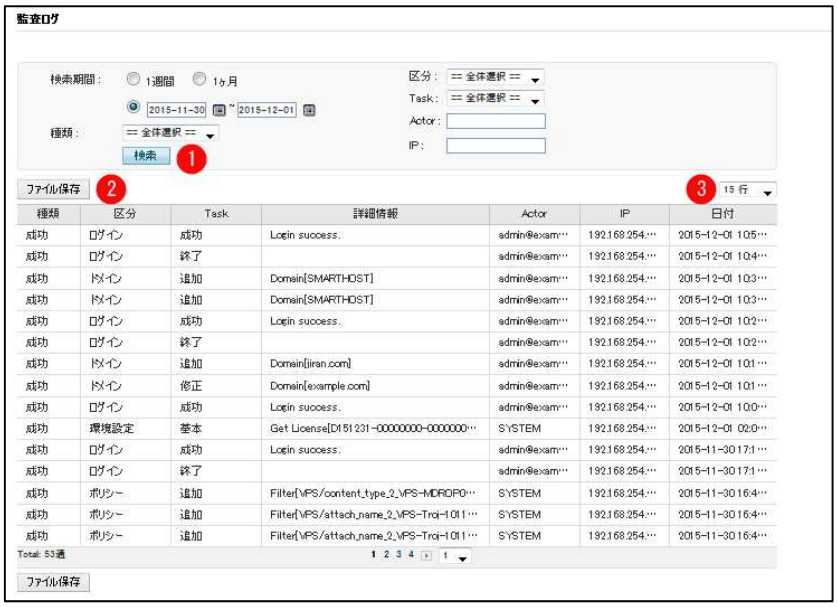
→ 4_[検索]:パッチ履歴を検索します。パッチ名前・作業者n検索条件を設定した後、[検索]ボタンをクリックします。

7.5.6. イベントログ

ユーザ、メール等とオブジェクトへの変更作業や、ログインのようにセキュリティ上の理由での重要な作業に対してイベントログを残し照会する機能を提供しています。イベントログはシステムで自動削除されません。 イベントログはカテゴリに応じて監査ログとシステムログに分かれています。システムログは「バックアップ、VPS、ワクチン、エンジン、データ整合性チェック、システムチェック、維持保守」です。他のカテゴリは監査ログとして分類されます。

設定方法

1. *環境設定*>イベントログをクリックします。
2. イベントログ画面が出力されます。
3. イベントログ画面の機能の説明は次のとおりです。



→ 1_[検索]：イベントログを検索します。検索期間、区分、種類、Task、Actor、IP から検索条件を設定した後[検索]ボタンをクリックします。

→ 2_[ファイル保存]：検索されたイベントログをエクセルファイルに保存します。

→ 3_リスト数設定：ページごとの表示されるイベントログの数を設定します。

8. システム概要、および統計

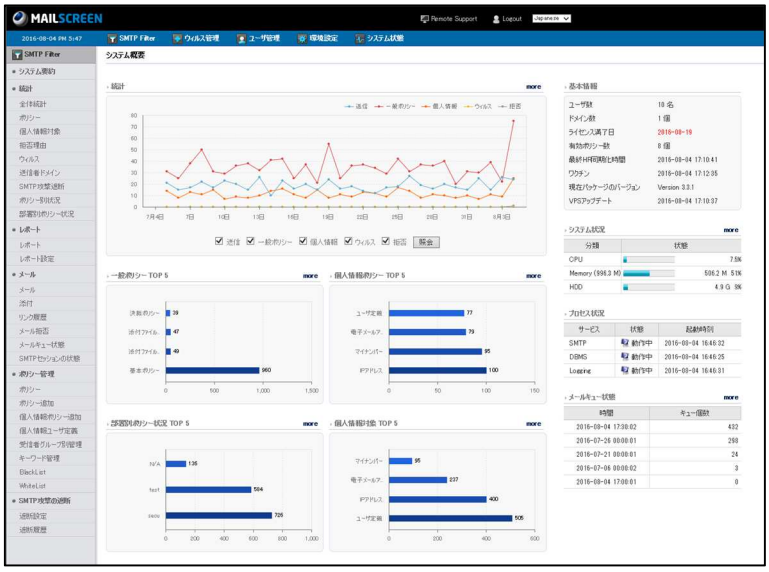
MailScreen は、全体システム状況、および全体統計とポリシー、拒否事由の項目に対する統計を提供します。

8.1. システム要約

システムの現在状況を直観的に分かるようにシステム状況を提供します。簡単な統計、現在システム、プロセス、アップデート状況等を確認することができます。

設定方法

1. *SMTP Filter*>システム要約をクリックします。
2. システム概要画面が出力されます。



→ 統計：送信、一般ポリシー、 個人情報、ウィルス、拒否されたメールに対して直近 30 日間の簡略な統計情報を表示します。メール処理項目を選択して照会ボタンをクリックすることにより項目のグラフだけ照会できます。

→ 一般ポリシーTOP 5：直近 30 日間で最も多く適応された一般ポリシーを降順で最大 5 個まで表示します。

→ 個人情報ポリシーTOP 5：直近 30 日間で最も多く適用された個人情報ポリシーを降順で最大 5 個まで表示します。

→ 部署別ポリシー状況 TOP 5：直近 30 日間で最も多く適用された部署を降順で最大 5 個まで表示します。

→ 個人情報対象 TOP 5：直近 30 日間で最も多くフィルタリングされた個人情報対象を降順で最大 5 個まで表示します。

→ 基本情報：現在サーバに設置されているパッケージに対して簡略な基本情報を表示します。

→ システム状況：CPU、メモリー等現在のシステム状況を簡略な情報で表示します。

→ プロセス状況：現在稼動中のサービスと状態を簡略に表示します。

→ メールキュー状態：現在キュー状態を表示します。

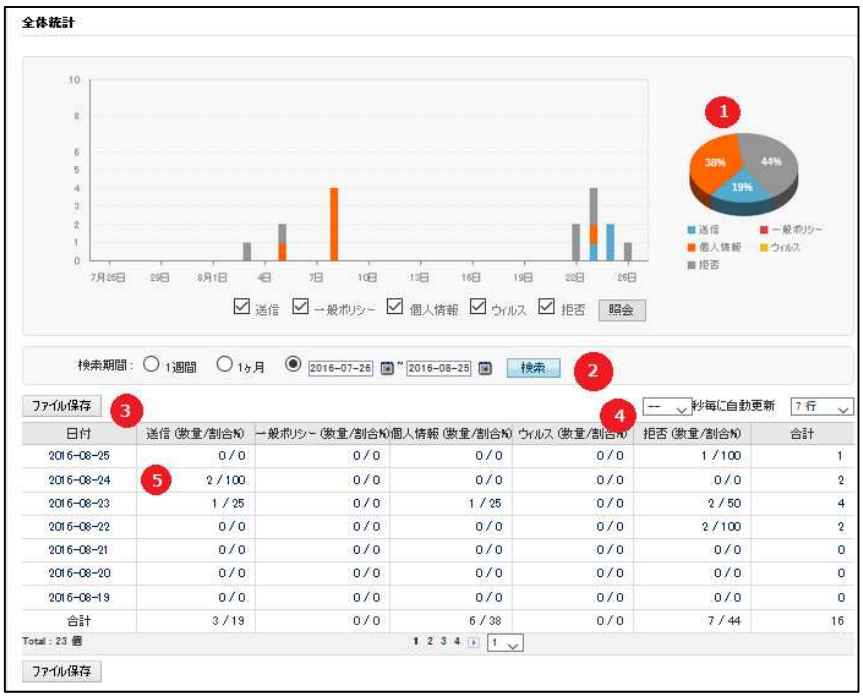
8.2. 統計管理

8.2.1. 全体統計

MailScreen を通過するメールの送信、一般ポリシー、個人情報、ウィルス、拒否メールの統計を確認することができます。それぞれのメール数と全体に対する比率が"/"で区分され、日付の降順で整列されます。

設定方法

1. *SMTP Filter*>統計>全体統計をクリックします。
2. 全体統計管理画面が出力されます。
3. 全体統計管理画面の上部、下部の機能です。



→ 1_グラフ：送信、一般ポリシー、個人情報、ウィルス、拒否項目の統計を円/棒グラフで表現します。メール処理項目を選択して照会ボタンをクリックすると選択した項目のグラフだけ照会できます。

→ 2_[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。

→ 3_[ファイル保存]：統計内容をエクセルファイルに保存します。

→ 4_再読込設定：ページを自動で更新します。サーバの状態をリアルタイムでモニタリングすることが可能です。更新は現在のデータ以外は必要がないため検索期間の終了日付が今日であり 1 ページだけで動作します。自動更新機能は、1回設定することにより常時適用されますのでカレンダーによる検索期間を選択する等の作業が必要な場合には、先に更新機能を中止する必要があります。

→ 5_日付と合計に設定されたリンクをクリックした時、その日のメールを検索し、*SMTPFilter*>メールのページに移動します。送信メール数のリンクをクリックした時、その日の送信メールだけを検索し *SMTPFilter*>メールのページに移動します。フィルタ動作欄の場合は、その日の送信・ウィルス・その他のメールの種類だけを検索し、

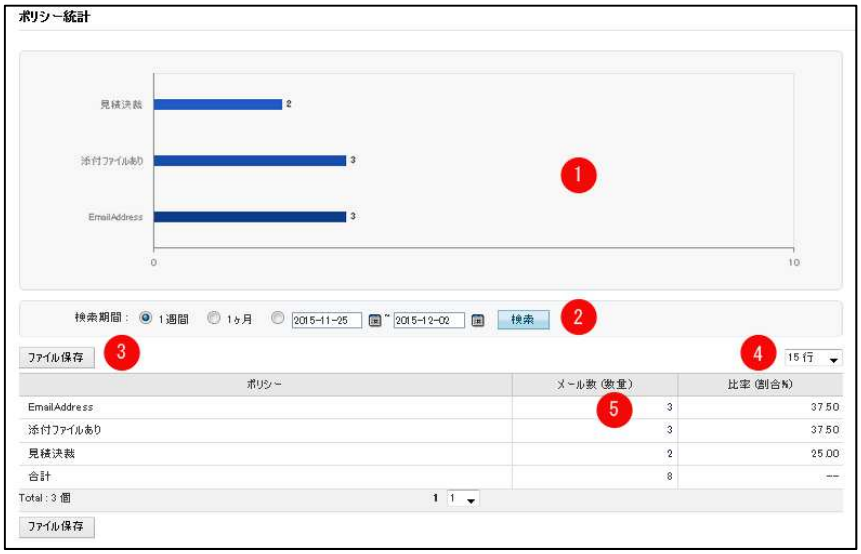
SMTPFilter>メールのページに移動し、ウィルス欄の場合はその日のウィルスメールだけを検索し、*SMTPFilter*>メールのページに移動します。拒否メール数のリンクをクリックした時、*SMTPFilter*>メール>メール拒否のページに移動します。

8.2.2. ポリシー

MailScreen を通過するメールのうち、ポリシー別に処理されたメールの統計を表示します。最も多く適用されたポリシーから降順で整列されます。

設定方法

1. *SMTP Filter*>統計>ポリシーをクリックします。
2. ポリシー統計管理画面が出力されます。
3. ポリシー統計管理画面の上部、下部の機能です。



→ 1_グラフ：ポリシーの統計を棒グラフで表現します

→ 2_[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。　一般ポリシーと個人情報ポリシーを区分し照会できます。

→ 3_[ファイル保存]：統計内容をエクセルファイルに保存します。

→ 4_リスト数設定：ページごとの表示される統計のリストを設定します。

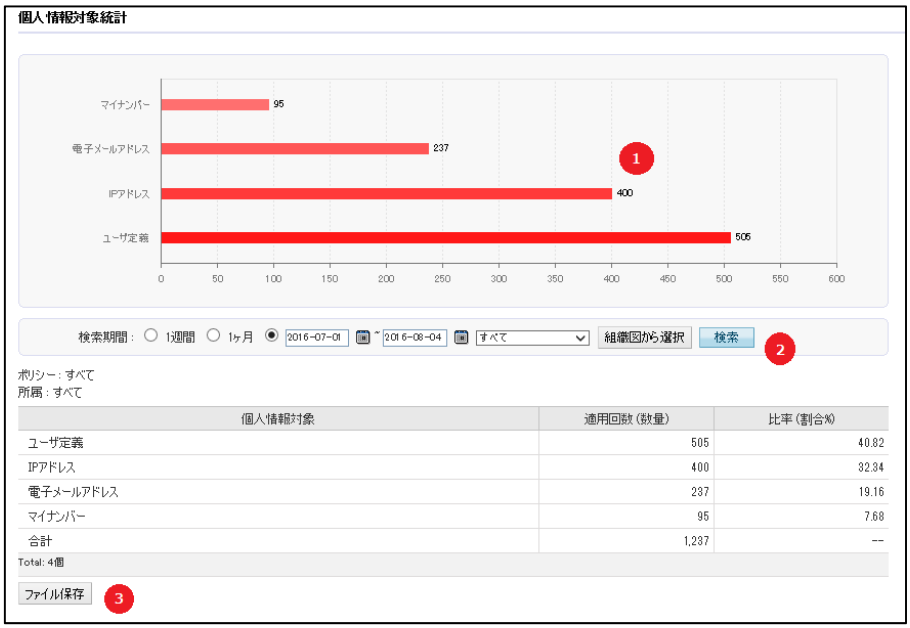
→ 5_メール数をクリックした時、検索期間内、そのポリシーで検索した *SMTPFilter*>メールのページに移動します。

8.2.3. 個人情報対象

MailScreen を通過したメールで個人情報ポリシーに適用されたメールに対して個人情報対象の適用回数に対する統計を表示します。最も多く適用された個人情報ポリシーから降順でソートされます。

設定方法

4. ***SMTP Filter*>統計>個人情報対象**をクリックします。
5. 個人情報対象統計管理画面が出力されます。
6. 個人情報対象統計管理画面の上部、下部の機能です。



→ 1_グラフ：個人情報対象に対する統計を棒グラフに表現します。

→ 2_[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。個人情報ポリシーと部署を区分し照会できます。

→ 3_[ファイルに保存] ：統計内容をエクセルファイルに保存します。

8.2.4. 拒否理由

MailScreen で受信拒否されたメールの統計を表示します。

設定方法

1. *SMTP Filter*>統計>拒否理由をクリックします。
2. 拒否理由統計管理画面が出力されます。
3. 拒否理由統計管理画面の上部、下部の機能です。

→ 1_グラフ：拒否理由の統計を棒グラフで表示します。

→ 2_[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。

→ 3_[ファイル保存]：統計内容をエクセルファイルに保存します。

→ 4_リスト数設定：ページごとの表示される統計のリストを設定します。

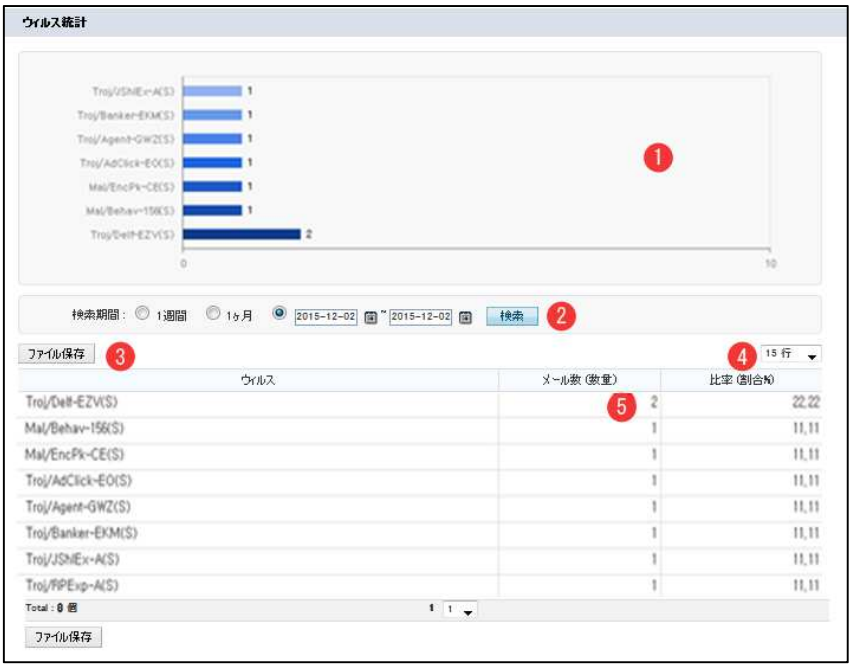
→ 5_メール数のリンクをクリックした時、検索期間内、拒否の理由で検索した *SMTPFilter*>メール拒否のページに移動します。

8.2.5. ウィルス

MailScreen を通じて送信されたメールのうちウィルスメールの統計を表示します。

設定方法

1. *SMTP Filter*>統計>ウィルスをクリックします。
2. ウィルス統計管理画面が出力されます。
3. ウィルス統計管理画面の上部、下部の機能です。



→ 1_グラフ：ウィルスの統計を棒グラフで表示します。

→ 2_[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。

→ 3_[ファイル保存]：統計内容をエクセルファイルに保存します。

→ 4_リスト数設定：ページごとの表示される統計のリストを設定します。

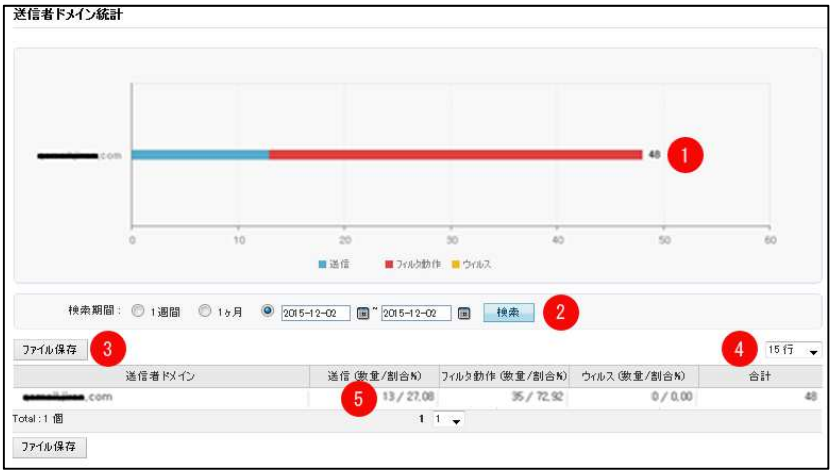
→ 5_メール数のリンクをクリックした時、検索期間内、ウィルスで検索した SMTPFilter>メールページに移動します。

8.2.6. 送信者ドメイン

MailScreen を通じて送信されたメールの送信者ドメインの統計を表示します。どのドメインがメールを最も多く送信するのかの状況を確認することができます。

設定方法

1. *SMTP Filter*>統計>送信者ドメインをクリックします。
2. 送信者ドメイン統計管理画面が出力されます。
3. 送信者ドメイン統計管理画面の上部、下部の機能です。



→ 1_グラフ：送信者ドメインの統計を棒グラフで表示します。

→ 2_[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。

→ 3_[ファイル保存]：統計内容をエクセルファイルに保存します。

→ 4_リスト数設定：ページごとの表示される統計のリストを設定します。

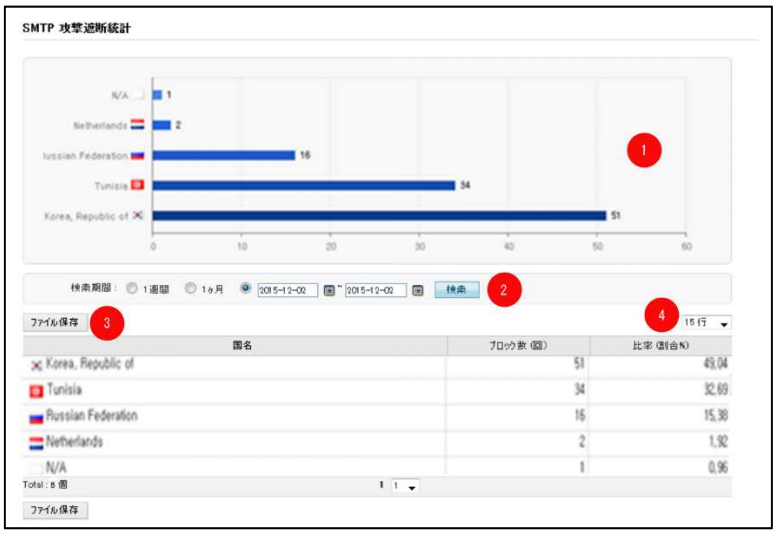
→ 5_合計欄のリンクをクリックした時は、検索期間内のそのドメインに送信されたメールを検索して、*SMTPFilter*>メールのページに移動します。送信の場合は、その日の送信メールを、フィルタ動作の場合は、その日の送信、ウィルスその他のメールの種類のみを検索して、*SMTPFilter*>メールのページに移動します、ウィルスの場合、その日のウィルスメールだけを検索して、*SMTPFilter*>メールのページに移動します。

8.2.7. SMTP 攻撃遮断

MailScreen を通じて不正リレーを試みるために SMTPAUTH へのログインを試み、多数の失敗があった IP の統計を表示します。どこの国からの SMTP 攻撃が最も多いかについての状況を確認することができます。

設定方法

1. *SMTP Filter*>統計>SMTP 攻撃遮断をクリックします。
2. SMTP 攻撃遮断統計管理画面が出力されます。
3. SMTP 攻撃遮断統計管理画面の上部、下部の機能です。



→ 1_グラフ：SMTP 攻撃を遮断するための統計を棒グラフで表示します。

→ 2_[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。

→ 3_[ファイル保存]：統計内容をエクセルファイルに保存します。

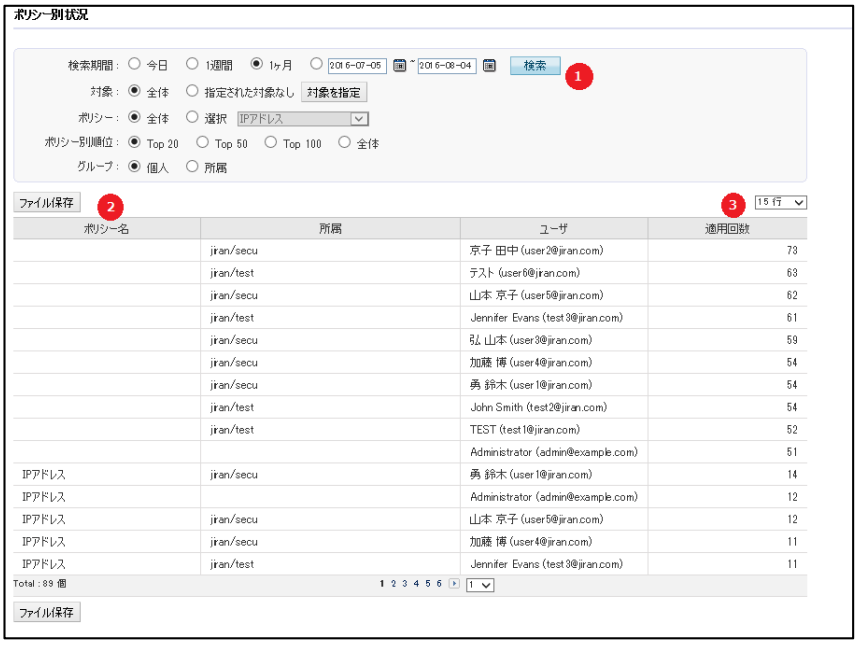
→ 4_リスト数設定：ページごとの表示される統計のリストを設定します。

8.2.8. ポリシー別状況

MailScreen を通過して送信されたメールに対してポリシーを基準に個人または、所属の統計を表示します。

設定方法

1. ***SMTP Filter*>統計>ポリシー別状況**をクリックします。
2. ポリシー別状況画面が出力されます。
3. ポリシー別状況画面の上部、下部の機能です。



→ 1_[検索]：設定したオプションによってポリシー別状況を検索します。検索期間、対象、ポリシー、ポリシー別順位、グルーピングの検索条件を設定した後、[検索]ボタンをクリックします。

注意事項

× 「対象」でチェックされた部署は該当部署を除いたすべての下位部署を対象にします。選択した部署の下位部署が存在しない場合、結果なし と表示されます。「グルーピング」を個人に選択して該当ユーザの情報を確認してください。

× 「グルーピング」を個人に選択した場合は表にユーザ項目が表示されます。

× 「グルーピング」を所属に選択した後、「対象」を指定して検索した時、チームは選択した対象の下位部署 1 depth だけ表示します。適用回数は下位部署すべての適用回数を合計した結果です。

→ 2_[ファイルに保存]：統計内容をエクセルファイルに保存します。

→ 3_リスト数設定：ページごとの表示される統計のリストを表示します。

8.2.9. 部署別ポリシー状況

MailScreen を通過して送信されたメールに対して部署別に適用されたポリシーの統計を表示します。それぞれの部署がどのようなポリシーを多く適用しているかの状況が確認できます。

設定方法

1. ***SMTP Filter*>統計>部署別ポリシー状況**をクリックします。

2. 部署別ポリシー状況画面が出力されます。
3. 部署別ポリシー状況画面の上部、下部の機能です。

→ 1_[検索]：統計内容を検索します。検索期間、対象、ポリシーの検索条件を設定した後、[検索]ボタンをクリックします。

注意事項

× 「対象」でチェックされた部署は該当部署を除いたすべての下位部署を対象にします。選択した部署の下位部署が存在しない場合、結果なし と表示されます。「グルーピング」を個人に選択して該当ユーザの情報を確認してください。

→ 2_[ファイルに保存]：統計内容をエクセルファイルに保存します。

→ 3_リスト数設定：ページごとの表示される統計のリストを表示します。

9. レポート

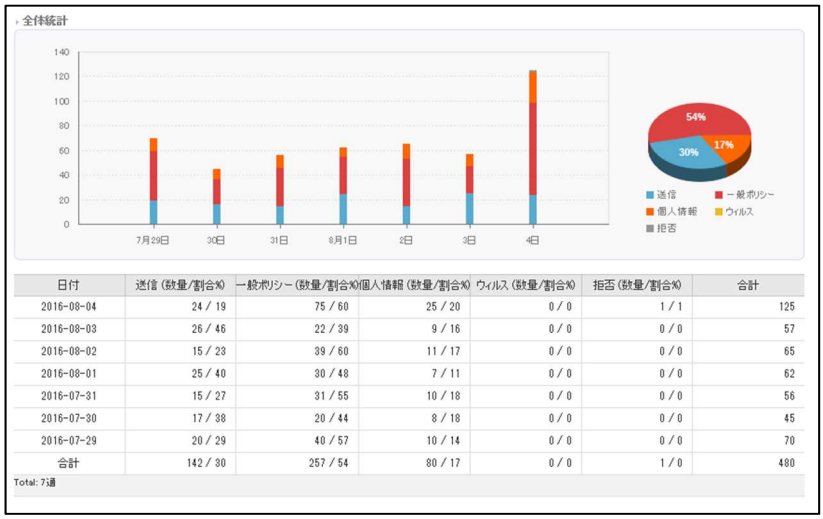
MailScreen は全体統計およびポリシー別、ユーザ別、部署別統計をデイリーレポートで提供します。

9.1. レポート

レポート設定ページから指定された設定によりリポートを Web から確認できます。

設定方法

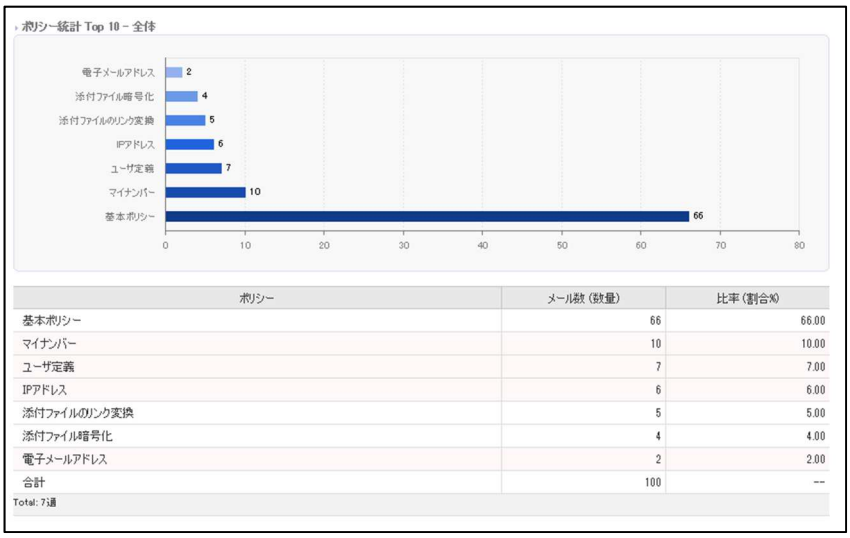
1. ***SMTP Filter*>レポート>レポート**をクリックします。
2. レポート画面の機能に対する説明は次のとおりです。
   → 1_要約情報:
   - 全体統計:1週間 MailScreen を通過したメールの送信、一般ポリシー、個人情報、ウィルス、拒否に対する統計およびデータを確認できます。



日付	送信 (数量/割合%)	一般ポリシー (数量/割合%)	個人情報 (数量/割合%)	ウィルス (数量/割合%)	拒否 (数量/割合%)	合計
2016-08-04	24 / 19	75 / 60	25 / 20	0 / 0	1 / 1	125
2016-08-03	26 / 46	22 / 39	9 / 16	0 / 0	0 / 0	57
2016-08-02	15 / 23	39 / 60	11 / 17	0 / 0	0 / 0	65
2016-08-01	25 / 40	30 / 48	7 / 11	0 / 0	0 / 0	62
2016-07-31	15 / 27	31 / 55	10 / 18	0 / 0	0 / 0	56
2016-07-30	17 / 38	20 / 44	8 / 18	0 / 0	0 / 0	45
2016-07-29	20 / 29	40 / 57	10 / 14	0 / 0	0 / 0	70
合計	142 / 30	257 / 54	80 / 17	0 / 0	1 / 0	480

Total: 7通

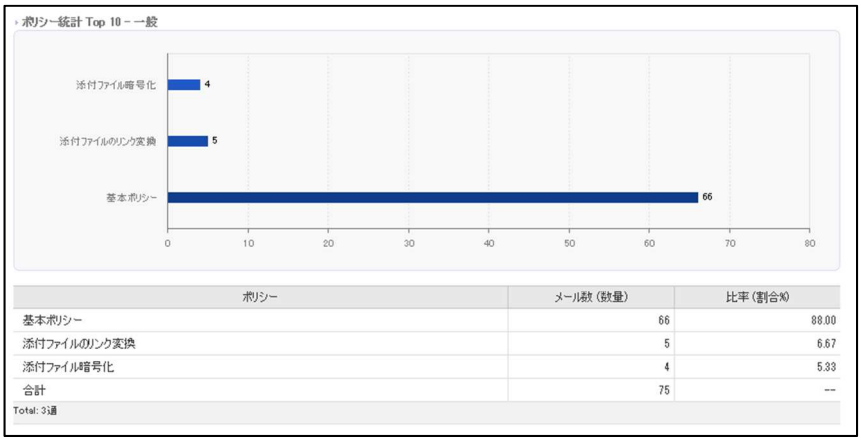
- ポリシー統計 Top 10 – 全体：当日を基準にすべてのポリシーに対する Top 10 統計グラフと表で確認できます。



ポリシー	メール数（数量）	比率（割合%）
基本ポリシー	66	66.00
マイナンバー	10	10.00
ユーザ定義	7	7.00
IPアドレス	6	6.00
添付ファイルのリンク変換	5	5.00
添付ファイル暗号化	4	4.00
電子メールアドレス	2	2.00
合計	100	--

Total: 7通

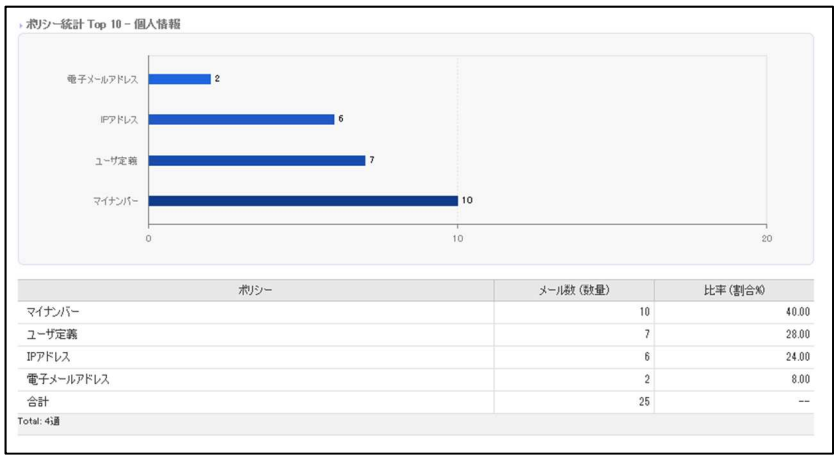
- ポリシー統計 Top 10 – 一般：当日を基準に一般ポリシーに対する Top 10 統計グラフと表で確認できます。



ポリシー	メール数（数量）	比率（割合%）
基本ポリシー	66	88.00
添付ファイルのリンク変換	5	6.67
添付ファイル暗号化	4	5.33
合計	75	--

Total: 3通

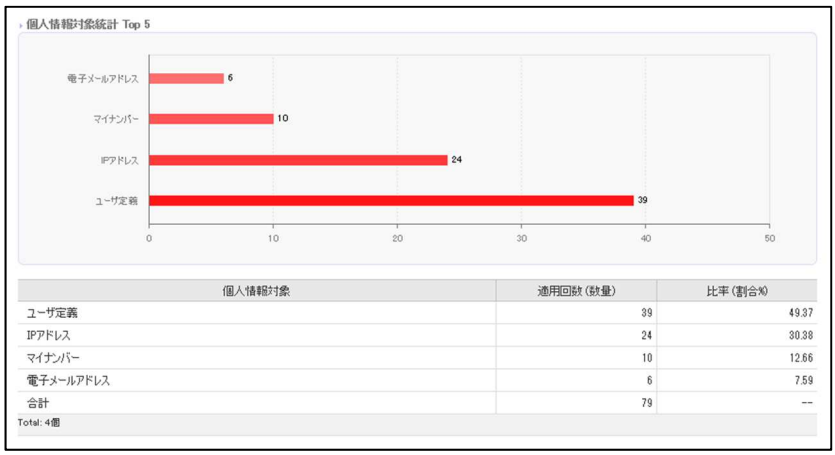
- ポリシー統計 Top 10 – 個人情報：当日を基準に個人情報ポリシーに対して Top 10 統計グラフと表で確認できます。



ポリシー	メール数 (数量)	比率 (割合%)
マイナンバー	10	40.00
ユーザ定義	7	28.00
IPアドレス	6	24.00
電子メールアドレス	2	8.00
合計	25	--

Total: 4通

- 個人情報対象統計 Top 5：当日を基準に個人情報ポリシーに適応されたメールについて、個人情報対象の適応回数 Top 10 統計グラフと表で確認できます。

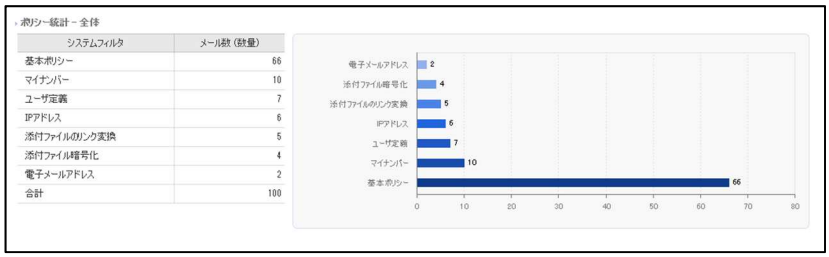


個人情報対象	適用回数 (数量)	比率 (割合%)
ユーザ定義	39	49.37
IPアドレス	24	30.38
マイナンバー	10	12.66
電子メールアドレス	6	7.59
合計	79	--

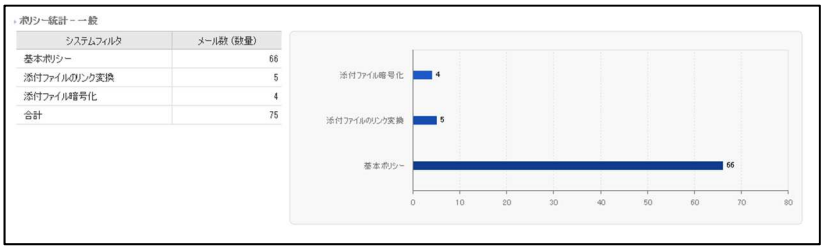
Total: 4個

→ 2_詳細統計：

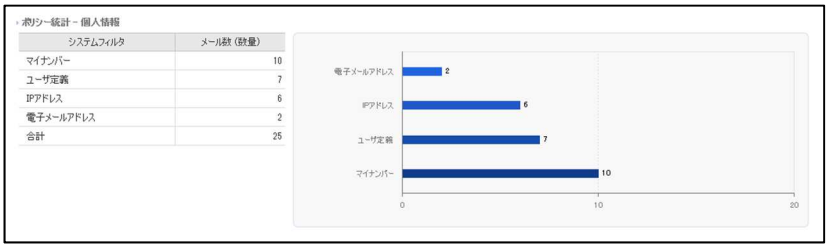
- ポリシー統計 – 全体：当日を基準にすべてのポリシーに対して統計グラフと表で確認できます。



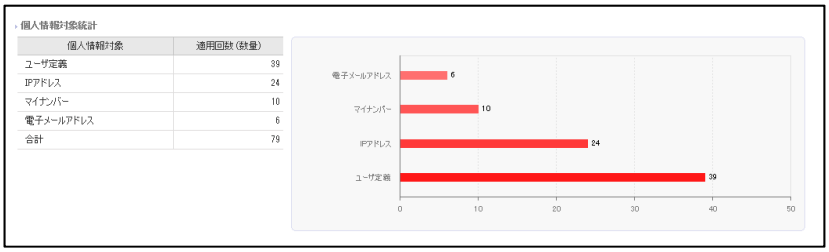
- ポリシー統計 – 一般：当日を基準に一般ポリシーに対して統計グラフと表で確認できます。



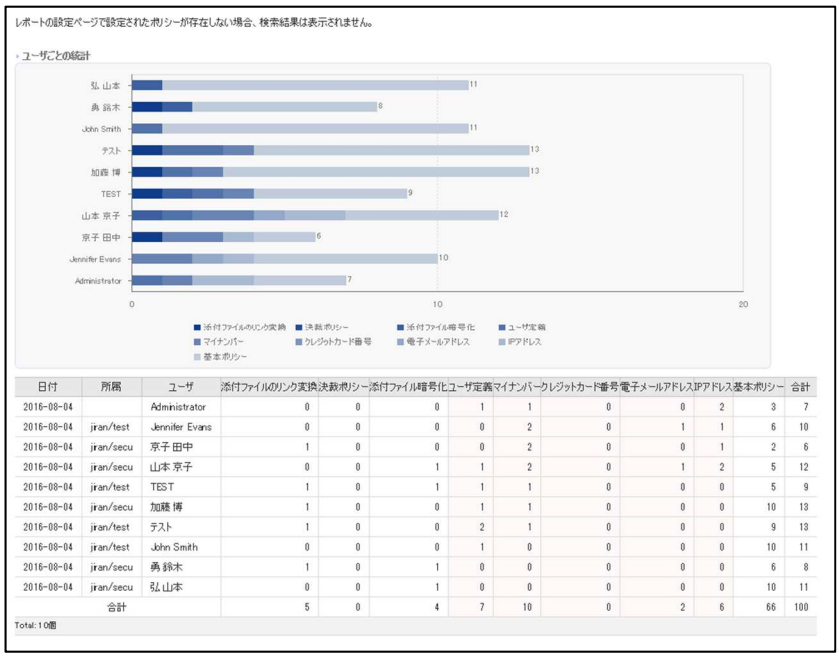
- ポリシー統計 – 個人情報：当日を基準に個人情報ポリシーに対して統計グラフと表で確認できます。



- 個人情報対象統計：当日を基準に、個人情報ポリシーに適応されたメールについて個人情報対象の適応回数が統計グラフと表で確認できます。



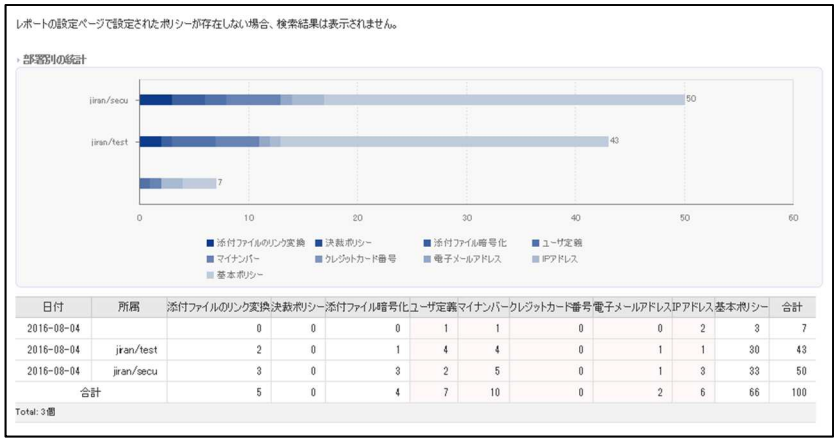
→ 3_ユーザごとの統計：レポート設定で設定したポリシーに限りユーザごとの統計をグラフと表で確認できます。



日付	所属	ユーザ	添付ファイルのリンク変換	決裁ポリシー	添付ファイル暗号化	ユーザ定義	マイナンバー	クレジットカード番号	電子メールアドレス	IPアドレス	基本ポリシー	合計
2016-08-04		Administrator	0	0	0	1	1	0	0	2	3	7
2016-08-04	jiran/test	Jennifer Evans	0	0	0	0	2	0	1	1	6	10
2016-08-04	jiran/secu	京子 田中	1	0	0	0	2	0	0	1	2	6
2016-08-04	jiran/secu	山本 京子	0	0	1	1	2	0	1	2	5	12
2016-08-04	jiran/test	TEST	1	0	1	1	1	0	0	0	5	9
2016-08-04	jiran/secu	加藤 博	1	0	0	1	1	0	0	0	10	13
2016-08-04	jiran/test	テスト	1	0	0	2	1	0	0	0	9	13
2016-08-04	jiran/test	John Smith	0	0	0	1	0	0	0	0	10	11
2016-08-04	jiran/secu	勇 鈴木	1	0	1	0	0	0	0	0	6	8
2016-08-04	jiran/secu	弘 山本	0	0	1	0	0	0	0	0	10	11
合計			5	0	4	7	10	0	2	6	66	100

Total: 10個

→ 4_部署別の統計：レポート設定で設定したポリシーに限り部署別の統計をグラフと表で確認できます。



日付	所属	添付ファイルのリンク変換	決裁ポリシー	添付ファイル暗号化	ユーザ定義	マイナンバー	クレジットカード番号	電子メールアドレス	IPアドレス	基本ポリシー	合計
2016-08-04		0	0	0	1	1	0	0	2	3	7
2016-08-04	jiran/test	2	0	1	4	4	0	1	1	30	43
2016-08-04	jiran/secu	3	0	3	2	5	0	1	3	33	50
合計		5	0	4	7	10	0	2	6	66	100

Total: 3個

9.2. レポート設定

レポート設定ページで指定された設定によりレポートを Web から確認できます。

設定方法

1. ***SMTP Filter*>レポート>レポート設定**をクリックします。
2. レポート設定画面が出力されます。各項目を設定した後、最下部の[保存]または[保存してレポート送信]ボタンをクリックします。

注意事項

× [保存]ボタンをクリックした時には、設定した送信時間の昨日分のデータを基準に作成したレポートメールが送信されます。

× [保存してレポート送信]ボタンをクリック時には、当日のデータを基準に作成したレポートメールが送信されます。

× レポート対象曜日はレポート作成データを基準にしています。

→ 送信設定

- 送信可否:使用可否を設定します。
- レポート対象曜日:レポート対象になる曜日を設定します。
- 送信時間:レポートメールを送信する時間を設定します。

→ 受信者を設定:レポートメールの受信者を設定します。

→ レポートポリシー設定:ユーザ別/部署別ポリシー統計に含めるポリシーを設定します。

10. システム状態

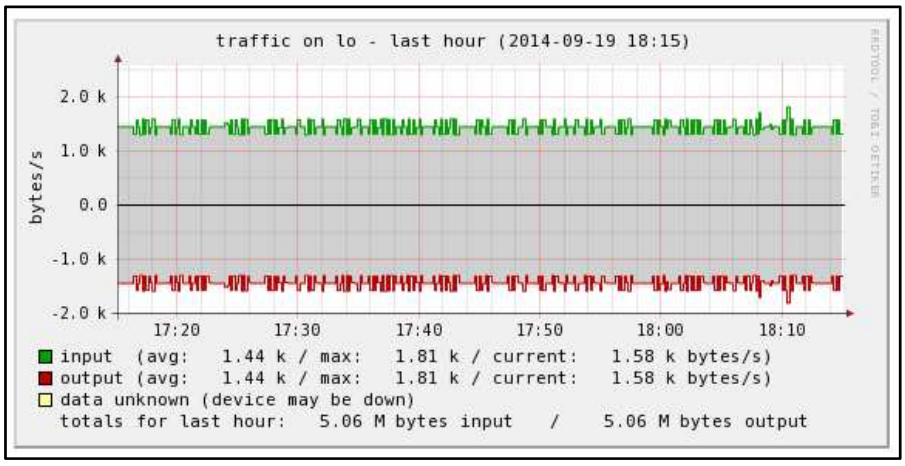
MailScreen サーバのシステム状態をグラフで提供します。

10.1. 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。eth で始まる場合は外部との通信のために使われた使用率であり、br で始まる場合はブリッジモードにおけるネットワーク使用率、lo は loopback に対する情報、すなわち localhost から localhost への情報です。

設定方法

1. *システム状態*>ネットワーク使用率>lo、eth0 のうち状態を照会する項目をクリックします。
2. last hour、last 6hour、last day、Last week、Last month、Last year を基準にサーバのネットワークデバイスの使用率のグラフが画面に出力されます。

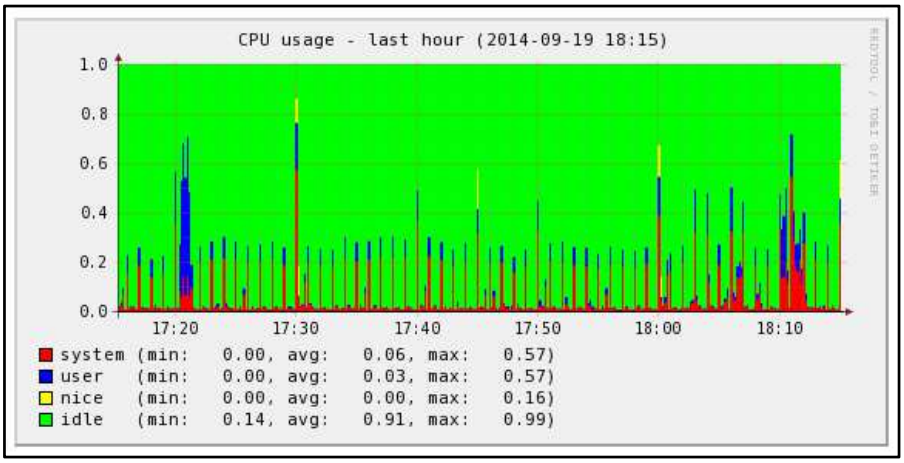


10.2. システムリソース

MailScreen が設置されているサーバのシステム使用率を表示します。

設定方法

1. *システム状態*>システムリソース>CPU、プロセス、システム負荷、ユーザ数、メモリー、スワップ領域のうち状態を照会する項目をクリックします。
2. last hour、last day、Last week、Last month、Last year を基準にサーバのシステム使用率のグラフが画面に出力されます。

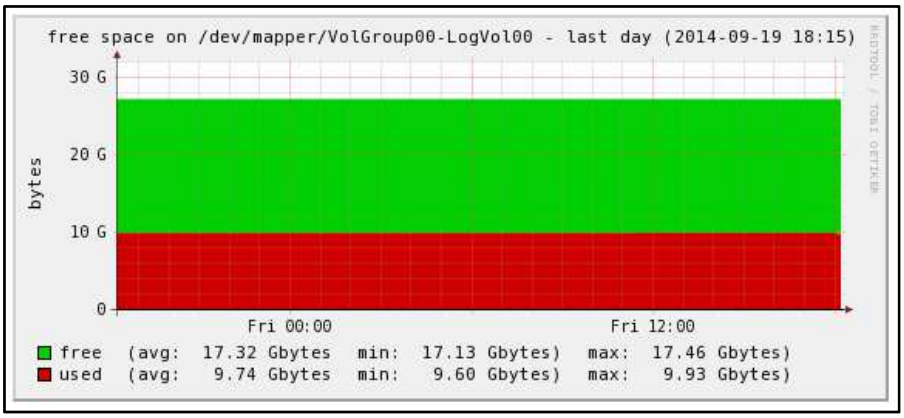


10.3. ディスク使用率

サーバのディスクの使用状態を表示します。ディスクの空き領域が不足すればメール処理を正確にされないことがありますのでディスク空き領域は重要な意味を持ちます。

設定方法

1. *システム状態*>ディスク使用率>**/、/boot** のうち状態を照会する項目をクリックします。
2. last day、Last week、Last month、Last year を基準にサーバのシステム使用率のグラフが画面に出力されます。



11. Appendix

11.1. 参照

11.1.1. 時間の形式文字

MailScreen がサポートする時間の形式文字は次のとおりです。

形式の文字	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	スウォッチ インターネット時間	000から999
d	日、前に0がつく2桁	01から31
D	曜日、 3字文字	MonからSun
F	月、 January、 March等の完全な文字の表現	Januaryから December
g	時、 0がつかない12時間形式	1から12
G	時、 0がつかない24時間形式	0から23
h	時、 0がつく12時間形式	01から12
H	時、 0がつく24時間形式	00から23
i	分、 0がつく形式	00から59
j	日、 0がつかない形式	1から31
L(小文字 'L')	曜日、完全な文字の表現	SundayからSaturday
m	月、数字表現、 0がつく形式	01から12
M	月、短い文字表現、 3文字	JanからDec
n	月、数字表現、0がつかない形式	1から12
O	グリニッジ時間(GMT)との差	+0200
r	RFC 2822形式の日付	Thu、 21 Dec 2000 16:01:07 +0200
s	秒、0がつく形式	00から59
S	日 表現のための英語序数接尾語、 2文字	st、 nd、 rdやth
t	与えられた月の日数	28から31
T	機器標準の時間帯設定	EST、 MDT
U	UNIXEpoch(January 1 1970 00:00:00 GMT)からの秒	1165306680
w	曜日、数字型	0(日曜日)から6(土曜日)
W	ISO-8601年の月曜日に始まる年	42(年度の 42週目)
y	年度、 2桁数の表現	99、 03
Y	年度、 4桁数の表現	1999、 2003
z	年度の日数(0から始まる)	0から365
Z	タイムゾーンのオフセット秒。 UTCから西のオフセットは常に負数であり、UTCから東のオフセットは常に正数	43200から43200

11.1.2. 時間形式適用範囲

環境設定>システム>基本情報で設定された時間形式が影響を与える範囲を説明します。説明されない「年月日のみ表記された日付」は、その他の日付が表記されるすべてのページに影響を与えます。

時間帯を含めた日付、時間	*ウィルス管理*>ウィルス検査設定>最後アップデート時間 *ウィルス管理*>VPSフィルタ>最終VPS有効アップデート時間
年月日を含んだ日付、時間	*SMTP Filter*>メール>メールの日付ツールチップ *SMTP Filter*>メール>添付の日付ツールチップ *SMTP Filter*>メール>リンク履歴の日付ツールチップ *SMTP Filter*>メール>メール拒否の日付ツールチップ *SMTP Filter*>メール>メールキュー状態 *SMTP Filter*>メール>SMTPセッションの状態 *SMTP Filter*>ポリシー管理>Black List *SMTP Filter*>ポリシー管理>White List *SMTP Filter*>システム要約>アップデート状況>ワクチン *SMTP Filter*>システム要約>メールキュー状態 *SMTP Filter*>ポリシー管理>受信者グループ別管理の日付ツールチップ *SMTP Filter*>SMTP攻撃の遮断>遮断履歴>日付/遮断満了時間/解除時間 *ユーザ管理*>ユーザ管理>登録日ツールチップ *ユーザ管理*>ユーザ情報変更>登録/修正/最後ログイン時間 *環境設定*>維持保守>エンジン自動アップデート>時間 *環境設定*>イベントログ>日付
年月日表記された日付	*SMTP Filter*>システム要約>システム状況>ライセンス満了日 *SMTP Filter*>統計>全体統計 *SMTP Filter*>ポリシー管理>受信者グループ別管理 *ユーザ管理*>ユーザ管理>ユーザ登録日 *環境設定*>システム>基本情報>システム情報>ライセンス満了日
日表記された日付、時間	*SMTP Filter*>メール>メール *SMTP Filter*>メール>添付 *SMTP Filter*>メール>リンク履歴 *SMTP Filter*>メール>メール拒否

11.1.3. 添付ファイル本文フィルタリング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 CP949 互換文字列(EUC-KR、KSC5601、 US ASCII、 ISO-8859-1 位)である場合のみ可能です。EUC-KR、または KSC5601、KSX1001 の説明は RFC1557、 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、CP 949 は http://www.microsoft.com/globaldev/reference/dbcs/949.mspx を参照してください。 MailScreen は、次のような形式の添付ファイルに対する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-Office96 バージョン以降をサポートします。

拡張子	説明
.doc、 .docx	マイクロソフトワード 95、 97、 2000、 XP(2002)、 2003、 2007、 2010、 2013
.ppt、 .pptx	マイクロソフトパワーポイント 95、 97、 2000、 XP(2002)、 2003、 2007、 2010、 2013
.xls、 .xlsx	マイクロソフトエクセル 95、 97、 2000、 XP(2002)、 2003、 2007、2010、 2013
.hwp	ハングルとコンピューターアレハングル 2.x、 3.x、 96、 97、ワーディアン 、 2002、 2004、 2005、 2007
.pdf	Adobe Acrobat 4.x、 5.x、 6.x、 7.x、 8.x (PDF 1.x支援)
.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ワード 1.x、 2.x
.rtf	Rich Text Format
.hwn	ハンディーソフトグループウェア
.hwx	ハンディーソフトグループウェア
.mdi	Microsoft Document Imaging
.msg	Microsoft Outlook Message
.wpd	ワードパーフェクト 4.x - 13.x
.dwg	Autodesk Drawing File R11-R14、 2000、 2004、 2005
.sxw	Open Office Document Text
.swf	Flash Movie File 2 - 8
.zip	圧縮ファイル
.tar	圧縮ファイル
.gz	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	TEXTファイル
.mp3	マルチメディアファイル、 MPEG Audio Stream - Layer

11.2. 注意事項

システム性能に影響を与える設定について説明し、より多くのメール受信量に対応し、円滑な管理のための情報を提供しています。

- **ウィルスメール送信**

  基本的に MailScreen は、ウィルスメールを治癒した後、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「送信メールのウィルス駆除後送信」オプションを設定している場合はメールを送信します。しかし、最近は、メールウィルス傾向がメール Bomb の状態が多く存在しますのでこのオプションを設定する場合は、メールサーバの負荷とユーザの不便を引き起こす可能性がありますのでなるべく使用しないようにしてください。

- **メールサイズ制限**

  フィルタリングエンジンがメールをチェックするときに、メールサイズが大きい場合負荷が加重されます。サイズが大きいメールは、同報の場合が多いため、瞬間的に負荷が集中しますいので、フィルタリングを適用するメールのサイズを制限することを推奨します。メールは、その性質上平均 20-30Kbytes 程度の大きさで報告されますので、これを参考として*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。

- **分散の環境**

  MailScreen が分散をサポートするように設置されれば次の UI は使用不可となります。

  → *環境設定*>サービス>サービス制御

  → *環境設定*>サービス>時間設定

  → *環境設定*>サービス>時間帯

11.3. 問題解決

- **Q: 出力するとき画面に表示される内容と出力結果が一致しません。**

  A: Microsoft Internet Explorer(以下 MSIE)などの一部の Web ブラウザは、Web ページを出力するときデスクトップイメージとパターン色を印刷しません。MSIE の場合は、「ツール」メニュー>インターネットオプション>詳細設定タブ>印刷>背景色とイメージ印刷をチェックした後、画面を出力すると正しく結果が得ることができます。

- **Q:ログイン ID とパスワードを正しく入力したがログインできません。**

  A:MailScreen は管理者とユーザに対しての識別、認証機能を提供しています。パスワード検証時に*環境設定*>システム>アクセス制御の 「アカウントロック」の値以上失敗した場合は、「アカウントロック時間」の設定値の間ログインできないように画面を非活性化させますので、「アカウントロック時間」値経過後再度ログインを試みてください。

・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。

2017 年 2 月 初 版
トライポッドワークス株式会社