Trend Micro InterScan Messaging Security Suite™

安心を、ひとつ上のステージへ。

TREND MICRO™

管理者ガイド

※注意事項

トレンドマイクロへのお客様情報の送信について

- 「Webレピュテーションサービス」「フィッシング詐欺対策」「有害サイト規制/URLフィルタリング」では、Webサイトの安全性の判定のために、お客様がアクセスしたURLの情報等(ドメイン、IPアドレス等を含む)を暗号化してトレンドマイクロのサーバに送信します。
  サーバに送信されたURL情報は、Webサイトの安全性の確認、および本機能の改良の目的にのみ利用されます。
  また、これらの機能を有効にしたうえで、Webページにアクセスした場合、以下の事象がおこることがあります。
  (a)お客様がアクセスしたWebページのWebサーバ側の仕様が、お客様が入力した情報等をURLのオプション情報として付加しWebサーバへ送信する仕様の場合、URLのオプション情報にお客様の入力した情報（ID、パスワード等）などを含んだURLがトレンドマイクロのサーバに送信される。
  この場合、トレンドマイクロでは、お客様がアクセスするWebページの安全性の確認のため、これらのお客様より受領した情報にもとづき、お客様がアクセスするWebページのセキュリティチェックを実施します。
- 「ファイルレピュテーションサービス」では、ファイルの安全性の判定のために、ファイルのハッシュ値等の情報をトレンドマイクロのサーバに送信します。ファイルそのものや、ファイルの内容に関する情報は送信しません。
- 「ソフトウェア安全性評価サービス」では、プログラムの安全性の判定のために、プログラムの情報をトレンドマイクロのサーバに送信します。
- 「ウイルストラッキング/TrendCareプログラム」では、検出されたウイルス/脅威名、検出数、国/地域、感染元となったWebサイトのURLを、統計を取るためにトレンドマイクロのサーバに送信します。
- 「迷惑メール対策ツール」では、弊社製品の改良の目的および迷惑メールの判定精度の向上のため、トレンドマイクロのサーバに該当メールを送信します。また、迷惑メールの削減、迷惑メールによる被害の抑制を目指している政府関係機関に対して迷惑メール本体を開示する場合があります。
- 「E-mailレピュテーションサービス」では、スパムメールの判定のために、送信元のメールサーバの情報等をトレンドマイクロのサーバに送信します。
- 「スマートフィードバック」では、脅威に関する情報を収集、分析し保護を強化するために、ファイルのチェックサム、アクセスされたWebアドレス、サイズやパス等のファイル情報、実行ファイルの名前等の情報をトレンドマイクロのサーバに送信します。

輸出規制について

本製品は、外国為替及び外国貿易法、U.S. Export Administration Regulations、およびその他の国における輸出規制品目に該当している場合があります。したがって、本製品が輸出規制品目に該当する場合、適正な政府の許可なくして、禁輸国もしくは貿易制裁国の企業、居住者、国民、または、取引禁止者、取引禁止企業に対して、輸出もしくは再輸出できません。このような規制についての情報は以下のWebサイトから見つけることができます。

「http://www.treas.gov/ofac/」、および「http://www.bis.doc.gov/complianceandenforcement/ListsToCheck.htm」

2008年12月現在、米国により定められる禁輸国は、キューバ、イラン、北朝鮮、スーダン、シリアが含まれています。

あなたは本製品に関連した米国輸出管理法令の違法行為に対して責任があります。本契約の同意により、あなたは、あなたが米国により現時点で禁止されている国の居住者もしくは国民ではないこと、別途本製品を受け取ることが禁止されていないことを確認します。また、大量破壊を目的とした、核兵器、化学兵器、生物兵器、ミサイルの開発、設計、製造、生産を行うために使用しないことに同意します。

複数年契約について

- お客様が複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。
- 複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。
- 各製品のサポート提供期間は以下のWebサイトからご確認いただけます。
  http://jp.trendmicro.com/jp/support/lifecycle/index.html

著作権について

商標について

P/N: IMSSUX-AE0200_R2 (2009/08)

目次

はじめに 9

ドキュメント 10

対象読者 10

ドキュメントの表記規則 11

第 1 章 使用開始 13

InterScan MSS の管理コンソールを開く 14

オンラインヘルプを使用する 14

SSL を使用した管理コンソールの表示 16

SSL 証明書を作成する 16

設定ウィザードでの基本設定の実行 18

設定ウィザードにアクセスする 18

手順 1: 通知設定 19

手順 2: アップデート元を設定する 21

手順 3: LDAP を設定する 22

手順 4: 内部アドレスを設定する 24

手順 5: Control Manager サーバを設定する 25

手順 6: アクティベートする 26

手順 7: 設定の概要を確認する 27

InterScan MSS サービス 27

サービスを起動または停止する 28

エンドユーザメール隔離の管理コンソールを開く 30

ログオン名形式 31

第 2 章 設定 33
IP フィルタサービス 34
Trend Micro Network Reputation Services を使用する 34
スパムメール対策のアクティベーションコードを使用する 34
NRS で使用するための MTA を準備する 35
NRS 管理コンソールを使用する 37
IP フィルタを設定する 38
手順 1: NRS および IP プロファイラを有効にする 39
手順 2: IP プロファイラのルールを有効にする 40
手順 3: NRS を設定する 42
手順 4: IP アドレスを承認済みリストへ追加する 43
手順 5: IP アドレスをブロックリストへ追加する 43
IP フィルタログのクエリを実行する 45
SMTP メッセージの検索 46
SMTP 接続を有効にする 46
SMTP ルーティングを設定する 47
SMTP を設定する 48
接続を設定する 49
メッセージルールを設定する 51
ドメインベース配信を設定する 52
POP3 メッセージの検索 54
POP3 の検索について 55
要件 56
POP3 の検索を有効にする 56
POP3 設定を行う 58
ポリシーを管理する 60
Policy Manager の仕組み 60

アドレスグループについて 62
アドレスグループを管理する 63
アドレスグループを追加する 63
アドレスグループを編集または削除する 65
LDAP ユーザまたはグループを検索する 68
内部アドレスを設定する 72
ポリシーを追加する 74
ルートを指定する 74
検索条件を指定する 78
処理を指定する 82
優先順位を指定する 86
例 1 88
例 2 92
アスタリスクワイルドカードを使用する 96
検索エンジンとパターンファイルをアップデートする 98
アップデート元を指定する 98
手動アップデートを実行する 99
コンポーネントのアップデートをロールバックする 100
予約アップデートを設定する 101
ログを設定する 103

第 3 章 設定のバックアップ、復元、複製について 105

InterScan MSS のバックアップ 106
InterScan MSS の復元 109
設定の複製 111
Control Manager エージェントを有効にする 111
Control Manager から設定を複製する 112

第 4 章 保守 115
ネットワークの監視 116
統計を表示する 116
統計を理解する 117
パフォーマンスの概要 118
検索パフォーマンス 119
IP フィルタパフォーマンス 120
レポートを作成する 121
レポート内容の種類 121
1 回限りのレポートを追加する 122
予約レポートを設定する 125
ログ 128
ログのクエリを実行する 128
隔離とアーカイブ 130
隔離とアーカイブを設定する 130
隔離およびアーカイブされたメッセージのクエリを実行する 131
ユーザ隔離アクセスを設定する 133
エンドユーザメール隔離データベースを追加 / 削除する 134
エンドユーザメール隔離データベースを追加する 135
エンドユーザメール隔離データベースを削除する 137
euqtrans ツールのコマンドラインオプション 137
イベント通知 138
通知を設定する 139
イベント条件および通知メッセージを設定する 140
管理者アカウントの管理 143
管理者アカウントを追加する 143
管理者アカウントを編集または削除する 144

検索サービスおよびポリシー接続の設定 146

第 5 章　トラブルシューティングとサポート情報 147

トラブルシューティング 148
よくある質問 (Q&A) 156
Postfix MTA 設定 156
InterScan MSS コンポーネント 157
NRS 158
IP プロファイラ 160
隔離とアーカイブ 164
エンドユーザメール隔離 165
スパムメール対策サービス 167
アップデート 168
その他 168
製品サポート情報 175
サポートサービスについて 175
製品 Q&A のご案内 176
セキュリティ情報 176
セキュリティ情報の入手先 176
トレンドマイクロへのウイルス解析依頼 177
トレンドマイクロへのスパムメールの報告 178
ウイルス解析サポートセンター「TrendLabs」 178

付録 A　InterScan MSS スクリプト 179

InterScan MSS スクリプトの実行 180

付録 B　初期設定ディレクトリ 183

初期設定のメールキュー 184
コンテンツフィルタ、ウイルスおよびプログラムのログ 185
一時フォルダ 185
通知受取フォルダ 186

索引 187

はじめに

Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) 7.0 管理者ガイドをお読みいただきありがとうございます。本書では、InterScan MSS の起動および実行方法について説明しています。ユーザインタフェースの各フィールドの詳細な設定情報については、オンラインヘルプを参照してください。オンラインヘルプには管理コンソールからアクセスできます。

この章の内容は、次のとおりです。

- 10 ページの「ドキュメント」
- 10 ページの「対象読者」
- 11 ページの「ドキュメントの表記規則」

ドキュメント

InterScan MSS には、次のドキュメントが付属しています。

- インストールガイド — InterScan MSS の機能概要やシステム要件を説明し、さまざまなネットワーク環境における InterScan MSS の配置およびアップグレード手順を提供します。
- 管理者ガイド — InterScan MSS のインストール、およびインストール後の InterScan MSS の設定および管理の実行について説明します。
- オンラインヘルプ — 各フィールドの設定手順、およびユーザインタフェースを使用してすべての機能を設定する方法について説明します。オンラインヘルプにアクセスするには、管理コンソールを開いて、ヘルプアイコン () をクリックしてください。
- Readme ファイル — 他のドキュメントには記載されていない可能性のある最新の製品情報を提供します。トピックには、機能の説明、インストールのヒント、既知の問題、および製品のリリースの履歴などが含まれます。

インストールガイド、管理者ガイド、および Readme ファイルは、http://www.trendmicro.co.jp/download から入手できます。

対象読者

InterScan MSS のドキュメントは、中規模から大規模企業の IT 管理者およびメール管理者を対象に書かれています。本書は、読者の方に、次の知識を含め、メールメッセージングネットワークの専門的な知識があることを前提としています。

- SMTP および POP3 プロトコル
- Postfix などの Message Transfer Agent (MTA)
- LDAP
- データベース管理

本書は、読者の方に、ウイルス対策またはスパムメール対策技術についての知識があることを前提としていません。

ドキュメントの表記規則

情報を簡単に検索し、理解できるように、InterScan MSS のドキュメントでは、次の表記規則を使用しています。

表記	説明
注意：	設定上の注意
ヒント：	推奨事項
警告：	避けるべき操作や設定についての注意

第 1 章

使用開始

この章では、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) 7.0 の管理コンソールへのアクセス方法について説明します。また、インストール後にすぐに実行する作業の手順についても示します。

この章の内容は次のとおりです。

- 14 ページの「InterScan MSS の管理コンソールを開く」
- 16 ページの「SSL を使用した管理コンソールの表示」
- 18 ページの「設定ウィザードでの基本設定の実行」
- 27 ページの「InterScan MSS サービス」
- 30 ページの「エンドユーザメール隔離の管理コンソールを開く」

InterScan MSS の管理コンソールを開く

InterScan MSS 管理コンソールは、プログラムがインストールされているサーバから、またはネットワークを介してリモートに、Web ブラウザに表示できます。

Web ブラウザで管理コンソールを表示するには、次の URL にアクセスします。

- https://< サーバ IP アドレス >:8445

IP アドレスを使用する代わりに、サーバの完全修飾ドメイン名 (FQDN) を使用することもできます。

初期設定のログオンアカウント情報は次のとおりです。

- ユーザ名 :admin
- パスワード :imss7.0

はじめて管理コンソールを開いたら、ログオンアカウント情報を入力し、[ログオン] ボタンをクリックします。

注意： Internet Explorer (IE) 7.0 を使用して管理コンソールにアクセスする場合、IE ではアクセスがブロックされ、別の Web アドレスから証明書が発行されたことを示すポップアップダイアログが表示されます。このメッセージを無視し、[このサイトの閲覧を続行する] をクリックして操作を続行します。

ヒント： ポリシーの不正改ざんを防ぐために、パスワードは定期的に変更してください。

オンラインヘルプを使用する

InterScan MSS 管理コンソールには、ユーザインタフェースの各項目について説明するオンラインヘルプが用意されています。

InterScan MSS 管理コンソールから指定ページのオンラインヘルプにアクセスするには、ページの右上隅にあるヘルプアイコン () をクリックします。

オンラインヘルプの「目次」にアクセスするには、ページヘッダの右にある [ログオフ] ハイパーリンク横のヘルプアイコン () をクリックします。

SSL を使用した管理コンソールの表示

InterScan MSS 管理コンソールは、SSL を使用する暗号化通信をサポートしています。InterScan MSS のインストールには初期設定の証明書が含まれているため、インストールが終了した後は SSL 通信が実行できるようになっています。ただし、セキュリティを強化するために、独自の証明書を作成することをお勧めします。

独自の証明書を使用する場合は、次のファイルを置き換えてください。

$IMSS_HOME/UI/tomcat/sslkey/.keystore

SSL 証明書を作成する

次の手順を実行してください。

1. 次のように Tomcat SSL 証明書を作成します。

   keytool -genkey -alias tomcat -keyalg RSA -keystore /opt/trend/imss/UI/tomcat/sslkey/.keystore

   Tomcat における SSL 設定の詳細については、次のサイトにアクセスしてください。

   http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html

2. 次のように Apache SSL 証明書を作成します。

   a. 秘密鍵および Certificate Signing Request (CSR) を作成します。

      openssl req -new > new.cert.csr

   b. 鍵からパスフレーズを削除します。

      openssl rsa -in privkey.pem -out new.cert.key

   c. 自己署名証明書を作成します。

      openssl x509 -in new.cert.csr -out new.cert.cert -req -signkey new.cert.key -days 1825

d. 証明書と鍵を Apache のパスにコピーします。

```
cp new.cert.cert $IMSS_HOME/UI/apache/conf/ssl.crt/server.crt
cp new.cert.key $IMSS_HOME/UI/apache/conf/ssl.key/server.key
```

設定ウィザードでの基本設定の実行

InterScan MSS には、InterScan MSS を実行するために必要な基本設定項目を簡単に設定できる、設定ウィザードが用意されています。

設定ウィザードでは、次の 7 つの手順で設定を行います。

手順 1: 通知設定
手順 2: アップデート元
手順 3: LDAP 設定
手順 4: 内部アドレス
手順 5: Trend Micro Control Manager (以下、Control Manager) サーバの設定
手順 6: アクティベート
手順 7: 設定の概要

設定ウィザードにアクセスする

次のいずれかの方法でウィザードにアクセスします。

- 管理コンソールのログオン画面で [設定ウィザードを開く] チェックボックスがオンになっていることを確認します。この状態でログオンすると、ウィザードが開きます。

- 管理コンソールに既にログオンしている場合は、[管理]→[InterScan MSS の設定]→[設定ウィザード] の順に選択します。新しいウィンドウにウィザードが表示されます。

手順 1: 通知設定

1. 最初の画面の内容を読んでから、[次へ] をクリックします。[通知設定] 画面が表示されます。

2. 次の通知関連の設定を行います。これらの設定は、InterScan MSS ですべての初期設定のシステム通知およびポリシーイベント通知に使用されます。

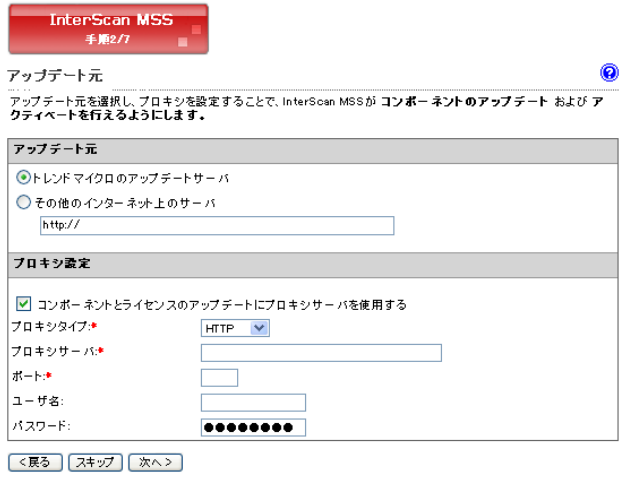
   - メール設定 — 送信者および受信者のアドレス、InterScan MSS がメールの配

信に使用するサーバの名前、SMTP サーバポート、文字コード、メッセージに追加するヘッダまたはフッタを入力します。

- SNMP トラップ — ネットワークに SNMP サーバが配置されている場合は、そのサーバの名前とコミュニティ名を入力します。

手順 2: アップデート元を設定する

1. [次へ] をクリックします。[アップデート元] 画面が表示されます。

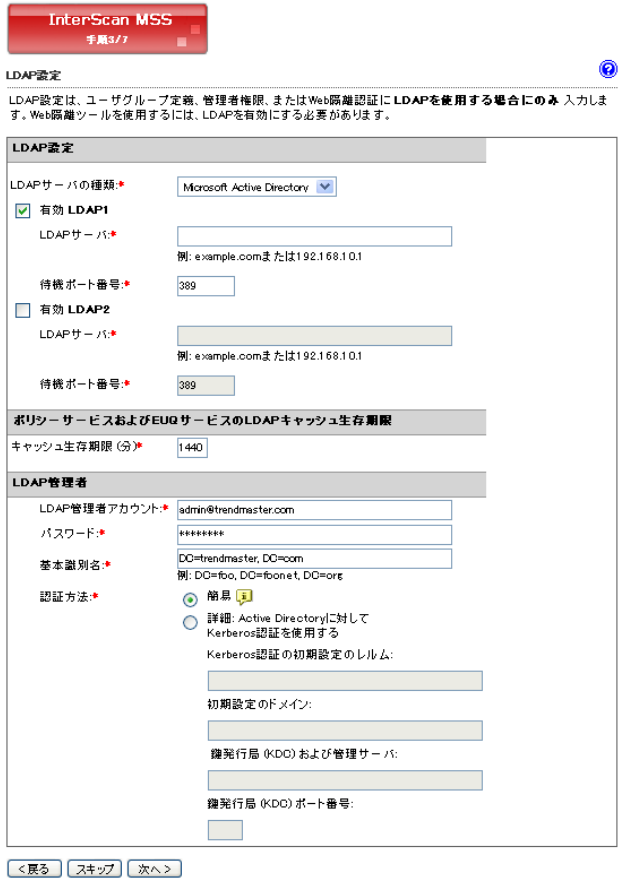


2. 次のアップデート設定を行います。これらの設定は、どのプロキシ (使用する場合) を介してインターネットにアクセスし、InterScan MSS が最新のコンポーネントをどこから受け取るかを決定します。

   - アップデート元 — トレンドマイクロから直接アップデートを受け取る場合は、[トレンドマイクロのアップデートサーバ] をクリックします。または、[その他のインターネット上のサーバ] をクリックし、アップデート元の URL を入力します。アップデート元にはトレンドマイクロのアップデートサーバ上のアップデートが確認できるサーバを指定します。お使いの環境に合うアップデート元を指定できます。また、Control Manager サーバが使用できる場合にはその URL を入力することもできます。
   - プロキシ設定 — [コンポーネントとライセンスのアップデートにプロキシサーバを使用する] チェックボックスをオンにして、プロキシの種類、サーバ名、ポート、ユーザ名、パスワードを設定します。

手順 3: LDAP を設定する

1. [次へ] をクリックします。[LDAP 設定] 画面が表示されます。



2. 次の操作を実行して、LDAP 設定を有効にします。

   a. [LDAP サーバの種類] で、次のいずれかを選択します。

      - Microsoft Active Directory
      - Domino

- Sun iPlanet Directory

b. 片方または両方の LDAP サーバを有効にするには、[有効 LDAP1] または [有効 LDAP2] の横のチェックボックスをオンにします。

c. LDAP サーバの名前と、これらのサーバの待機ポートの番号を入力します。

d. [ポリシーサービスおよび EUQ サービスの LDAP キャッシュ生存期限] の下の [キャッシュ生存期限(分)] の横に、有効時間を表す数値を入力します。

e. [LDAP 管理者] の下に、管理者アカウントとパスワード、および基本識別名を入力します。LDAP 管理設定に指定すべき項目の詳細については、表 1-1 を参照してください。

LDAP サーバ	LDAP 管理者アカウント (例)	基本識別名 (例)	認証方法
Active Directory	• Kerberos を使用しない場合 : user1@imsstest.com (UPN) または imsstest¥user1 • Kerberos を使用する場合 : user1@imsstest.com	dc=imsstest,dc=com	• 簡易 • 詳細 (Kerberos 使用)
Domino	user1/imsstest	該当なし	簡易
Sun iPlanet Directory	uid=user1,ou=people,dc=imsstest,dc=com	dc=imsstest,dc=com	簡易

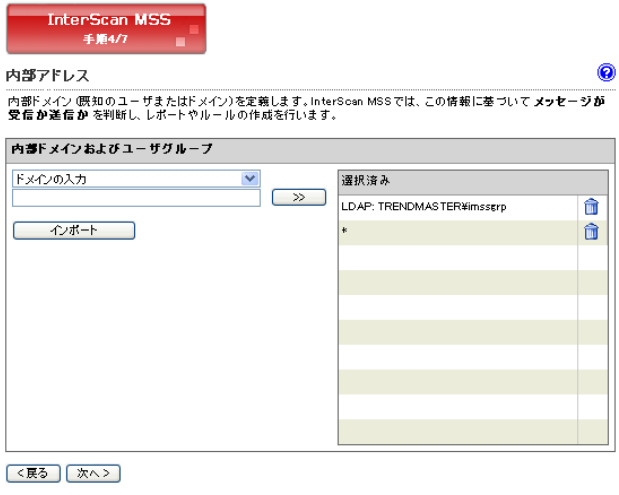
表 1-1. LDAP 管理設定

f. [認証方法] については、[簡易] または [詳細] をクリックします。Active Directory の [詳細] 認証を選択した場合は、Kerberos 認証の初期設定のレルム、初期設定のドメイン、KDC と管理サーバ、および KDC ポート番号を設定します。

注意 : LDAP 設定は、LDAP をユーザグループの定義、管理者権限、またはエンドユーザメール隔離の認証に使用する場合のみ指定します。エンドユーザメール隔離を使用するには、LDAP を有効にする必要があります。

手順 4: 内部アドレスを設定する

1. [次へ] をクリックします。[内部アドレス] 画面が表示されます。



2. InterScan MSS では、内部アドレスを使用して、ポリシーまたはイベントが受信用であるか、または送信用であるかを判断します。

   - 送信メッセージのルールを設定している場合、内部アドレスのリストは送信者に適用されます。
   - 受信メッセージのルールを設定している場合、内部アドレスのリストは受信者に適用されます。

   内部ドメインとユーザグループを定義するには、次のいずれかを実行します。

   - ドロップダウンリストから [ドメインの入力] を選択し、テキストボックスにドメインを入力して [>>] をクリックします。
   - ドロップダウンリストから [LDAP グループの検索] を選択します。LDAP グループを選択する画面が表示されます。検索する LDAP グループ名をテキストボックスに入力し、[検索] をクリックします。検索結果がリストボックスに表示されます。その LDAP グループ名を [選択済み] リストに追加するには、[>>] をクリックします。

手順 5: Control Manager サーバを設定する

1. [次へ] をクリックします。[Control Manager サーバの設定] 画面が表示されます。

2. Control Manager を使用して InterScan MSS を管理する場合は、次の操作を実行します。

   a. [Control Manager エージェントを有効にする] を選択します (Control Manager エージェントは、初期設定で InterScan MSS とともにインストールされています)。

   b. [サーバ] に Control Manager の IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。

   c. [通信プロトコル] では [HTTP ポート番号] または [HTTPS ポート番号] を選択し、対応するポート番号を入力します。HTTP アクセス用の初期設定ポート番号は 80 で、HTTPS 用の初期設定ポート番号は 443 です。

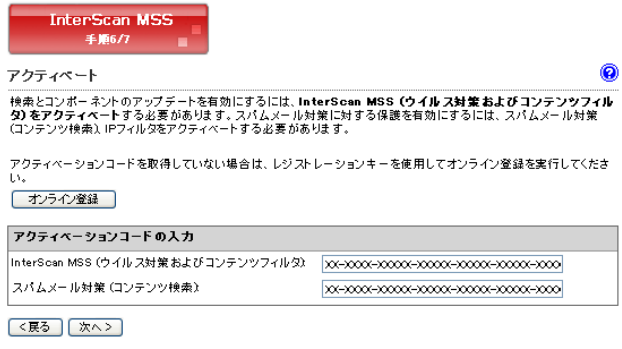
   d. Web サーバの認証が必要な場合は、[Web サーバ認証] に Web サーバのユーザ名とパスワードを入力します。

e. InterScan MSS と Control Manager の間にプロキシサーバが配置されている場合は、[プロキシを有効にする] を選択します。

f. プロキシサーバのポート番号、ユーザ名、およびパスワードを入力します。

手順 6: アクティベートする

1. [次へ] をクリックします。[アクティベート] 画面が表示されます。検索およびアップデート機能を有効にするには、「InterScan MSS (ウイルス対策およびコンテンツフィルタ)」をアクティベートする必要があります。アクティベーションコードを取得するには、支給されたレジストレーションキーを使用してオンラインで製品を登録します。



2. 製品のアクティベーションコードを入力します。アクティベーションコードを取得していない場合、[オンライン登録] をクリックして、トレンドマイクロのオンライン登録サイトの指示に従ってください。

手順 7: 設定の概要を確認する

1. [次へ] をクリックします。[設定の概要] 画面が表示されます。

2. 設定が正しい場合は、[完了] をクリックします。

   設定を変更する場合は、[戻る] をクリックしながら画面を移動して、設定を変更してください。

InterScan MSS サービス

検索サービスおよびポリシーサービスは、InterScan MSS を使用してネットワークの保護を開始する際に必ず起動する必要があります。ただし、エンドユーザメール隔離サービスのインストールまたは起動については選択できます。

- 検索サービス — SMTP/POP3 トラフィックの検索を実行します。
- ポリシーサービス — 検索サービスのルールのリモートストアとして機能し、ルールの検索を強化します。
- エンドユーザメール隔離サービス — Web ベースのコンソールをホストし、エンドユーザが受信したスパムメールを各自で表示、削除、および解除できるようにします。

これらのサービスの詳細については、「Trend Micro InterScan Messaging Security Suite インストールガイド」を参照してください。

サービスを起動または停止する

InterScan MSS を正常にインストールし種々の設定を完了した後に、サービスを起動して不正プログラムやその他の脅威の検索を実行する必要があります。また、アップグレードまたはバックアップ機能を実行する前に、InterScan MSS サービスを停止する必要があります。

1. メニューから [概要] を選択します。初期設定で [システム] タブが選択された状態で [概要] 画面が表示されます。

2. [管理下のサーバ設定] セクションで [開始] ボタンまたは [停止] ボタンをクリックして、目的のサービスを起動または停止します。

エンドユーザメール隔離の管理コンソールを開く

エンドユーザメール隔離管理コンソールにアクセスする前に、次の項目が実行済みであることを確認してください。

1. LDAP の設定。22 ページの「手順 3: LDAP を設定する」を参照してください。
2. ユーザ隔離アクセスの有効化。133 ページの「ユーザ隔離アクセスを設定する」を参照してください。

エンドユーザメール隔離管理コンソールは、プログラムがインストールされたコンピュータから、またはネットワークを介してリモートで表示できます。

ネットワーク上の他のコンピュータからエンドユーザメール隔離管理コンソールを表示するには、次の URL にアクセスします。

- プライマリエンドユーザメール隔離サービス — https://< サーバ IP アドレス >:8447
- セカンダリエンドユーザメール隔離サービス — https://< サーバ IP アドレス >:8446

警告： セカンダリエンドユーザメール隔離サービスのすべての管理コンソールへ正常にアクセスするには、ネットワーク上にあるすべてのエンドユーザメール隔離サービスのシステム時間を同期させる必要があります。

IP アドレスを使用する代わりに、サーバの完全修飾ドメイン名 (FQDN) を使用することもできます。

ログオン名形式

エンドユーザメール隔離管理コンソールにアクセスするためのユーザログオン名の形式は、LDAP 設定時に選択した LDAP サーバの種類によって異なります。サポートされている 3 種類の LDAP サーバに対するログオン名形式例は、次のとおりです。

- Microsoft Active Directory
    - Kerberos を使用しない場合 — user1@imsstest.com (UPN) または imsstest¥user1
    - Kerberos を使用する場合 — user1@imsstest.com
- Domino — user1/imsstest
- Sun iPlanet Directory — uid=user1, ou=people, dc=imsstest, dc=com

第 2 章

設定

この章では、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) の起動および実行に必要なさまざまな設定について説明します。詳細については、管理コンソールからアクセスできるオンラインヘルプを参照してください。

- 34 ページの「IP フィルタサービス」
- 46 ページの「SMTP メッセージの検索」
- 54 ページの「POP3 メッセージの検索」
- 60 ページの「ポリシーを管理する」
- 98 ページの「検索エンジンとパターンファイルをアップデートする」
- 103 ページの「ログを設定する」

IP フィルタサービス

IP フィルタサービスには、Trend Micro Network Reputation Service (以下、NRS) と IP プロファイラという、2 つのコンポーネントがあります。

- NRS は、接続層でスパムメール送信者をフィルタします。
- IP プロファイラは、高度なプロファイル (SMTP IDS) を使用してメールサーバを攻撃から保護します。

ヒント： メッセージングインフラストラクチャの最前線の防御として、IP フィルタのインストールをお勧めします。

メールメッセージングシステムには、通常、既存の IP アドレスブロック機能、スパムメールフィルタ機能、ウイルスフィルタ機能などの多層構造が備わっていることがほとんどですが、他の IP アドレスブロック機能はメッセージング環境から完全に削除することをお勧めします。IP フィルタは、使用されるすべてのアプリケーションフィルタ機能よりも先行して動作する必要があります。

Trend Micro Network Reputation Services を使用する

トレンドマイクロでは、既知のスパムメール送信者の IP アドレスリストを中央データベースで管理しています。NRS は、このデータベース内に保存された IP アドレスをブロックすることでスパムメールをフィルタします。

スパムメール対策のアクティベーションコードを使用する

NRS および IP プロファイラから成る IP フィルタサービスでは、スパムメール対策 (コンテンツ検索) と同じライセンスが使用されます。スパムメール対策 (コンテンツ検索) の製品版を購入すると、製品登録の際にアクティベーションコードが発行されます。

アクティベーションコードにより、登録時に指定したサービスにアクセスできます。スパムメール対策 (コンテンツ検索) を有効にすると、IP フィルタのライセンス情報が表示されます。

NRS の設定の詳細については、38 ページの「IP フィルタを設定する」を参照してください。

NRS で使用するための MTA を準備する

MTA を準備して NRS で使用するには

- Trend Micro RBL+ Service — 550 レベルエラーコード (Connection refused) で接続を拒否するように MTA を設定します。このエラーコードは、肯定応答を RBL+ データベースから受信したことを示しています。RBL+ データベースには、スパムメール送信者またはメール送信をすべきでない送信元のリストが含まれます。このリストに含まれるスパムメール送信者からのメールの標準的な処理方法は、接続を全面的に拒否することです。

  詳細については、次の URL を参照してください。

  http://www.trendmicro.com/jp/products/nrs/rbl/evaluate/overview.htm

- Trend Micro Network Anti-Spam Service — 2 つの DNS クエリ (QIL データベースおよび RBL+ データベースに対するクエリ) を実行するように MTA を設定します。

  QIL データベースは、リアルタイムな動的データベースで、ここにはスパムメールを送信する疑わしい IP アドレスが格納されています。これらの IP アドレスからスパムメールの送信が停止されると、これらの IP アドレスは QIL データベースから削除されます。QIL データベースから肯定応答を受信しなかった場合、MTA は 2 番目のクエリを RBL+ データベースに対して行います。RBL+ データベースには、変動のより少ない IP アドレスのブラックリストがあります。

  MTA は、450 レベルのエラーコード (server temporarily unavailable, please retry) で接続を一時的に拒否します。その際、肯定応答をこのデータベースから受信します。このデータベースに記録された IP アドレスには、背後に信用できないホストが存在し、一時的にスパムメールを送信することがあります。接続要求が正規のメールサーバからのものである場合、それは再度キューに入り、後でメッセージの送信

を試行します。これにより、そのリストの期限が切れるまでメールの配信が少し遅れますが、そのメールが永遠にブロックされることはありません。

詳細については、次の URL を参照してください。

http://www.trendmicro.com/jp/products/nrs/nas/evaluate/overview.htm

NRS 管理コンソールを使用する

グローバルスパムメール情報へのアクセス、レポートの表示、承認済み送信者 IP リストおよびブロックする送信者 IP リストの作成または管理、管理作業の実行を行う場合は、NRS 管理コンソールにログオンします。

このセクションでは、NRS 管理コンソールを使用するための基本的な手順を説明します。各画面の設定に関する詳細な手順については、NRS 管理コンソールのオンラインヘルプを参照してください。ヘルプ画面の右上隅にあるヘルプアイコンをクリックして、オンラインヘルプにアクセスします。

NRS 管理コンソールを使用するには

1. Web ブラウザを開き、次のアドレスにアクセスします。

   https://nrs.nssg.trendmicro.com/

2. メニューから [グローバルスパムメール情報] を選択します。
3. 次のいずれかのタブをクリックします。
   - スパムメールアラート — 現在のスパムメールの手口に関する簡単な概要と説明、および組織に対する影響を示します。また、新しい手口がどのように配置されているか、この手口がどのようにトレンドマイクロシステムを通過するか、これらの新しい脅威に対してトレンドマイクロがどのように対応しているかについてを説明します。
   - ISP スパム TOP.x — 特定の週内に上位 100 の ISP から送信されたスパムメールの総量。一番多くのスパムメールを送信しているネットワークが上位にランク付けられます。ISP のランクは毎日変わります。
4. MTA と NRS データベースサーバ間のクエリの動作をまとめたレポートを表示するには、次の操作を実行します。
   a. メニューから [レポート] を選択します。
   b. [クエリの割合]、[1 時間あたりのクエリ数]、または [1 日あたりのクエリ数] をクリックします。

5. 承認済み送信者 IP リストおよびブロックする送信者 IP リストを作成または管理するには、メニューから [ポリシー] を選択します。国別または ISP 別の個々の IP アドレスおよび CIDR ごとに、承認済み送信者を定義できます。

6. ISP をリストに追加するには、メニューから [新規 ISP のリクエスト] を選択します。

パスワードまたはアクティベーションコードを変更するには、メニューから [管理] を選択します。

IP フィルタを設定する

IP フィルタを完全に設定するには、次の手順を実行します。

手順 1: NRS および IP プロファイラの有効化
手順 2: IP プロファイラのルールの有効化
手順 3: NRS の設定
手順 4: IP アドレスの承認済みリストへの追加
手順 5: IP アドレスのブロックリストへの追加

手順 1: NRS および IP プロファイラを有効にする

NRS および IP プロファイラを有効にするには

1. メニューから、[IP フィルタ]→[概要] の順に選択します。[IP フィルタの概要] 画面が表示されます。

2. [IP フィルタを有効にする] チェックボックスをオンにします。これにより、NRS および IP プロファイラのチェックボックスが両方オンになります。
3. 必要がなければ、[NRS] または [IP プロファイラ] チェックボックスをオフにします。

4. [保存] をクリックします。

注意： その後に IP フィルタを無効にする場合には、手動で NRS および IP プロファイラをアンインストールしてください。IP フィルタを管理コンソールから無効にしても、InterScan MSS から IP プロファイラの登録を解除するだけで、NRS および IP プロファイラの動作を停止できません。NRS と IP プロファイラのアンインストールの詳細については、「Trend Micro InterScan Messaging Security Suite インストールガイド」の「IP プロファイラと NRS のアンインストール」のセクションを参照してください。

手順 2: IP プロファイラのルールを有効にする

IP プロファイラは、4 種類の攻撃を防御できます。

IP プロファイラのルールを有効にするには

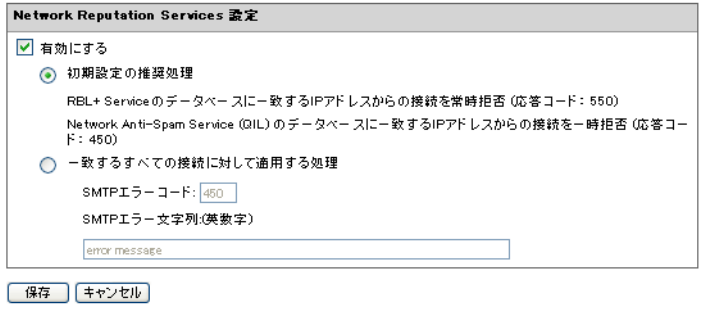
1. メニューから、[IP フィルタ]→[ルール] の順に選択します。[ルール] 画面には、脅威の種類ごとに 4 つのタブがあります。

2. 必要なタブを選択して、その脅威に対するルールを設定します。
3. [有効にする] チェックボックスをオンにします。
4. 必要なパラメータを指定します (詳細については、オンラインヘルプを参照してください)。
5. [保存] をクリックします。

手順 3: NRS を設定する

NRS を設定するには

1. メニューから、[IP フィルタ]→[NRS] の順に選択します。[NRS] 画面が表示されます。



2. [有効にする] チェックボックスをオンにします。
3. 次のいずれかの横にあるラジオボタンをクリックします。
   - 初期設定の推奨処理 — NRS は、RBL+ に一致する接続を常時拒否 (応答コード : 550) し、Zombie に一致する接続を一時的に拒否 (応答コード : 450) します。
   - 一致するすべての接続に対して適用する処理
     - SMTP エラーコード — 特定の SMTP コードを持つ接続を拒否します。SMTP コードを入力します。
     - SMTP エラー文字列 — SMTP エラーコードに関連したメッセージを入力します。

     注意： 上記の SMTP エラーコードとエラー文字列は、アップストリーム MTA に送信され、エラーコードやエラー文字列をログファイルに記録するなど、事前に設定された必要な処理を実行します。
4. [保存] をクリックします。

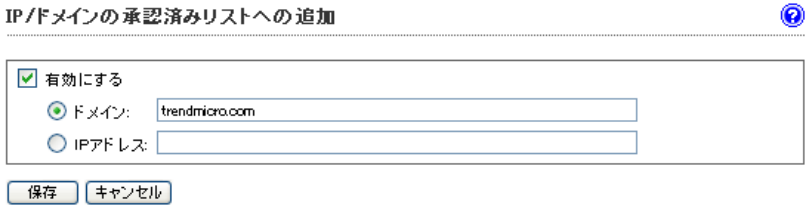
手順 4: IP アドレスを承認済みリストへ追加する

InterScan MSS では、承認済みリストに表示されている IP アドレスやドメインはフィルタされません。

承認済みリストに IP アドレスを追加するには

1. メニューから、[IP フィルタ]→[承認済みリスト] の順に選択します。[承認済みリスト] 画面が表示されます。

2. [追加] をクリックします。[IP/ ドメインの承認済みリストへの追加] 画面が表示されます。



3. [有効にする] チェックボックスをオンにします。
4. 承認済みリストへ追加するドメインまたは IP アドレスを入力します。
5. [保存] をクリックします。承認済みリストに指定したドメインまたは IP アドレスが表示されます。

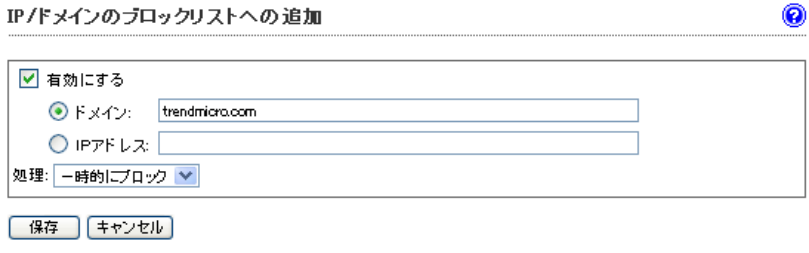
手順 5: IP アドレスをブロックリストへ追加する

InterScan MSS では、ブロックリストに表示される IP アドレスがブロックされます。

ブロックリストに IP アドレスを追加するには

1. メニューから、[IP フィルタ]→[ブロックリスト] の順に選択します。[ブロックリスト] 画面が表示されます。

2. [追加] をクリックします。[IP/ ドメインのブロックリストへの追加] 画面が表示されます。



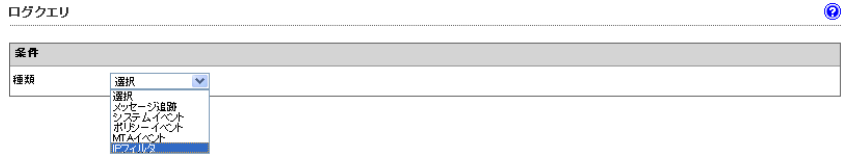
3. [有効にする] チェックボックスをオンにします。
4. ドメインまたは IP アドレスを入力します。
5. [一時的にブロック] または [常にブロック] を選択します。
6. [保存] をクリックします。ドメインまたは IP アドレスがブロックリストに追加されます。

IP フィルタログのクエリを実行する

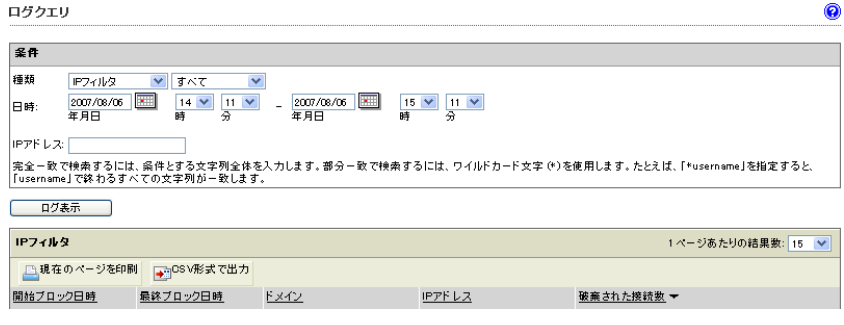
IP フィルタでは、ネットワークでイベントが発生したときに、これらのイベントを記録します。IP フィルタの処理履歴をクエリできます。

IP フィルタのログをクエリするには

1. メニューから、[ログ]→[クエリ] の順に選択します。[ログクエリ] 画面が表示されます。
2. [種類] として、[IP フィルタ] を選択します。



3. 検索データを指定します (すべてのデータを表示するには、空欄のままにしておきます)。初期設定では、完全一致で検索されます。複数の異なる条件を指定する場合はセミコロン (;) で区切ります。
4. [ログ表示] をクリックして、結果を確認します。



SMTP メッセージの検索

InterScan MSS は、Postfix、sendmail、および qmail の 3 種類の MTA をサポートしています。

InterScan MSS で Postfix を使用していて、複数の検索サービスが配置されている場合には、検索サービスの SMTP ルーティングの設定を一元的に管理できます。InterScan MSS 管理コンソールから、SMTP 設定を行い、同じ設定内容をすべての検索サービスに適用できます。

sendmail または qmail を使用している場合、各 MTA 設定ファイルの SMTP 設定を手動で行う必要があります。詳細については、「Trend Micro InterScan Messaging Security Suite インストールガイド」の「MTA の準備」を参照してください。

SMTP 接続を有効にする

InterScan MSS がネットワーク上の受信および送信トラフィックの検索を開始する前に、SMTP 接続を有効にする必要があります。

SMTP 接続を有効にするには

1. メニューから [概要] を選択します。初期設定では [システム] タブが表示されます。

2. [SMTP 接続を許可する] チェックボックスをオンにします。
3. [保存] をクリックします。

SMTP ルーティングを設定する

SMTP ルーティングを設定するには、次の 4 つの手順を実行します。

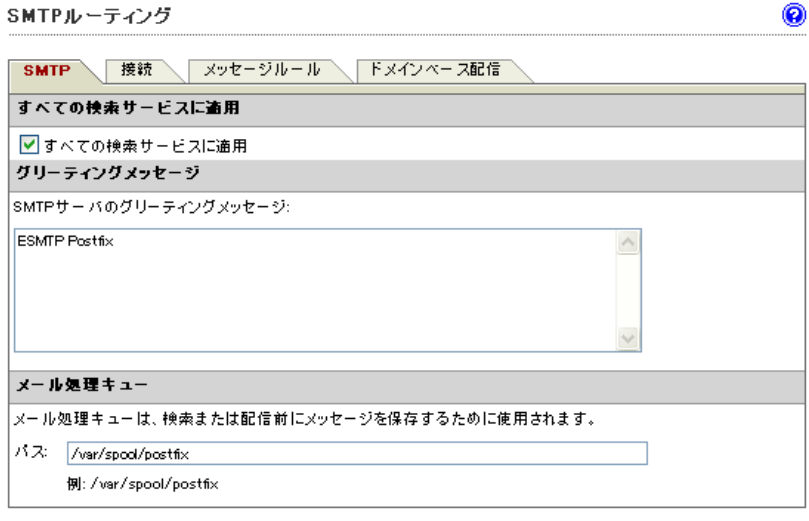
手順 1: SMTP の設定
手順 2: 接続の設定

手順 3: メッセージルールの設定
手順 4: ドメインベース配信の設定

SMTP を設定する

SMTP の設定を指定するには

1. メニューから、[管理]→[InterScan MSS の設定]→[SMTP ルーティング] を選択します。[SMTP ルーティング] 画面が表示されます。



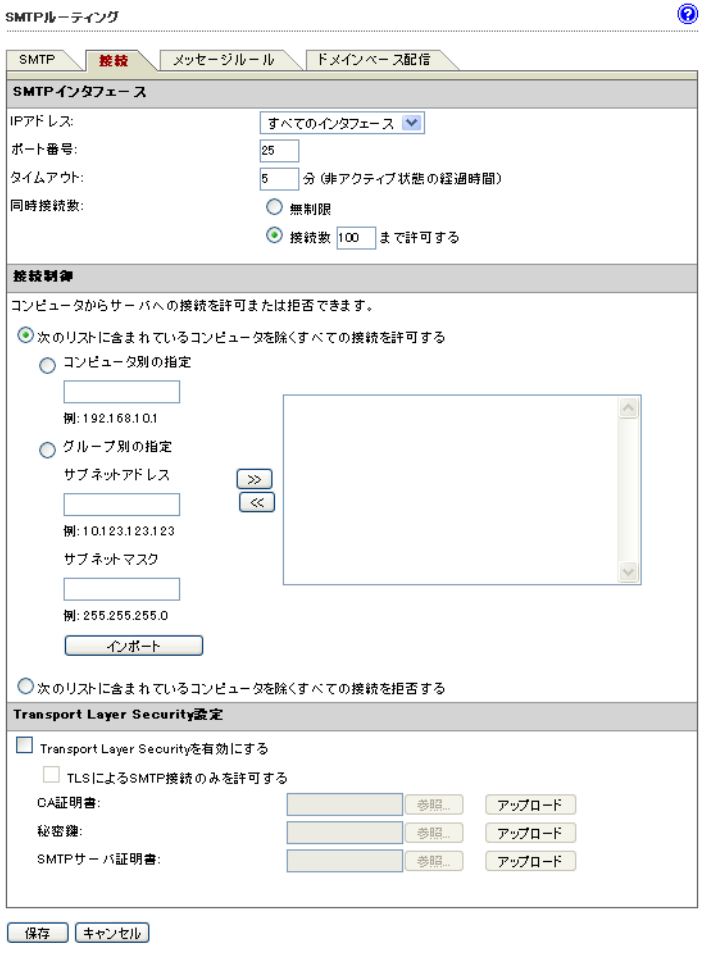
2. [すべての検索サービスに適用] チェックボックスをオンにします。
3. [SMTP サーバのグリーティングメッセージ] (セッションが確立された際に表示されるメッセージ) を指定します。
4. [メール処理キュー] の [パス] を指定します。
5. [保存] をクリックします。

接続を設定する

接続の設定を指定するには

1. メニューから、[管理]→[InterScan MSS の設定]→[SMTP ルーティング] を選択します。

2. [接続] タブをクリックします。[接続] 画面が表示されます。



3. [SMTP インタフェース] および [接続制御] のパラメータを指定します。

4. [Transport Layer Security 設定] のパラメータを指定します。

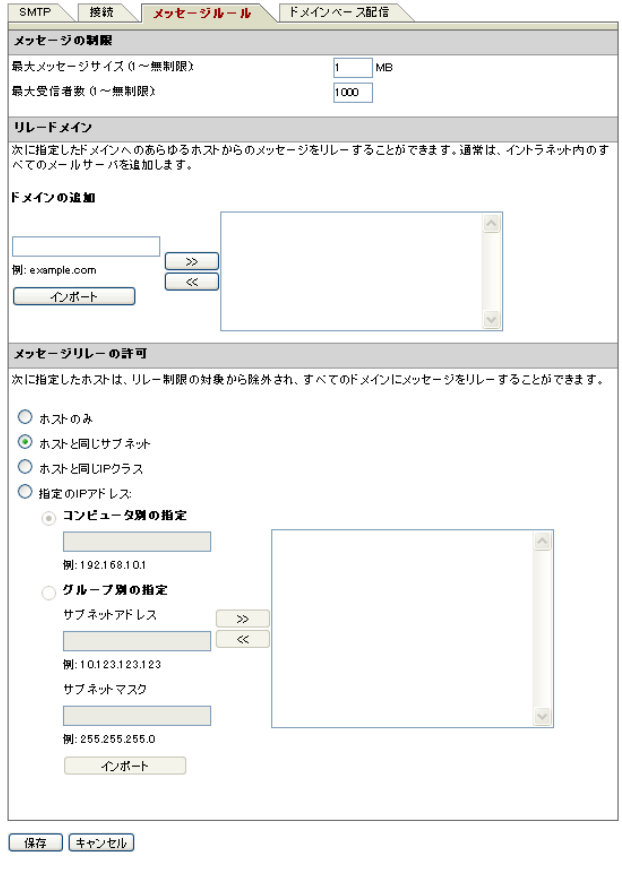
5. [保存] をクリックします。

メッセージルールを設定する

メッセージルールを指定するには

1. メニューから、[管理]→[InterScan MSS の設定]→[SMTP ルーティング] を選択します。

2. [メッセージルール] タブをクリックします。[メッセージルール] 画面が表示されます。



3. [メッセージの制限] のパラメータを指定します。

4. [リレードメイン] を指定します。メッセージは、リストされているドメインにリレーされます。
5. [メッセージリレーの許可] を指定します。
6. [保存] をクリックします。

ドメインベース配信を設定する

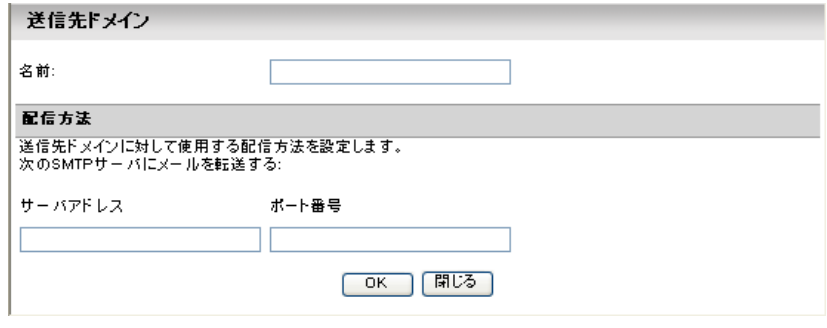
次に配信の設定に進みます。InterScan MSS は、受信者のメールドメインを検索して、一致したドメインの次の SMTP ホストにメールを送信します。

ドメインベースの配信を指定するには

1. メニューから、[管理]→[InterScan MSS の設定]→[SMTP ルーティング] を選択します。

2. [ドメインベース配信] タブをクリックします。[ドメインベース配信] 画面が表示されます。

3. [追加] をクリックします。[送信先ドメイン] 画面が表示されます。



4. [送信先ドメイン] および [配信方法] を指定します。
5. [OK] をクリックします。
6. [保存] をクリックします。

POP3 メッセージの検索

SMTP トラフィックのほかに、InterScan MSS では、ネットワーク内のクライアントがメッセージを受信する際に、ゲートウェイで POP3 メッセージを検索できます。企業で POP3 メールが使用されていない場合でも、従業員がコンピュータ上にあるメールクライアントを使用して個人の POP3 メールアカウントにアクセスすることがあります。POP3 メールアカウントの例には、Hotmail や Yahoo などがあります。それらのアカウントからのメッセージを検索しなければ、ネットワーク上に脆弱ポイントが生じる場合があります。

POP3 の検索について

InterScan MSS の POP3 検索サービスは、メールクライアントと POP3 サーバとの間に配置されたプロキシサーバ として機能し、クライアントがメッセージを受信した際にメッセージを検索します。

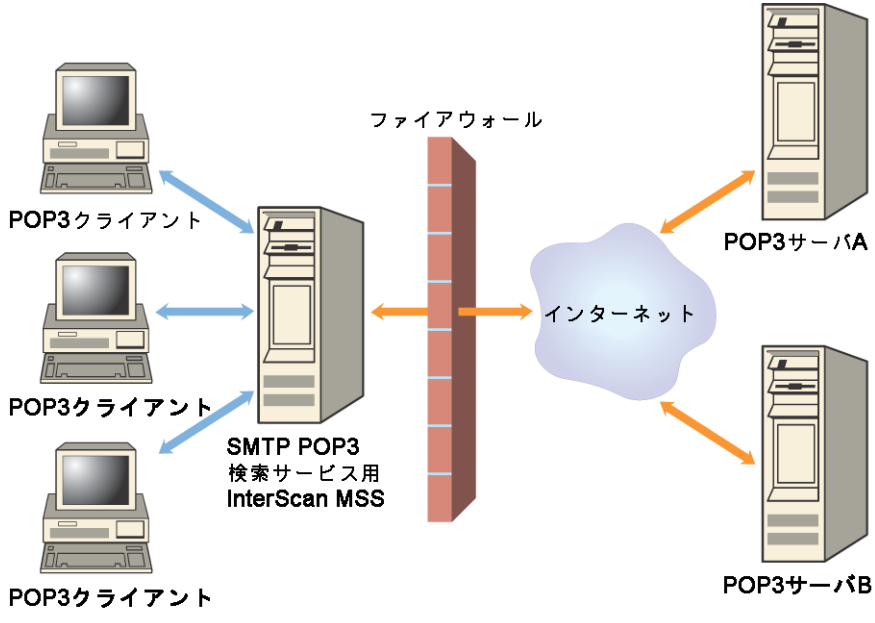


図 2-1.　POP3 メッセージを検索する

POP3 トラフィックを検索するには、メールクライアントを InterScan MSS サーバの POP3 プロキシに接続するように設定します。InterScan MSS サーバの POP3 プロキシは、POP3 サーバに接続してメッセージを取り込んで検索します。

設定可能な接続の種類は、次のとおりです。

- 一般的な接続 — 同じポートを使用して、異なる POP3 サーバにアクセスできます。ポートは通常 110 で、これは POP3 トラフィックの初期設定のポートです。

- 専用の接続 — 特定のポートを使用して、POP3 サーバにアクセスします。POP3 サーバで、APOP や NTLM などの安全なログオンを使用した認証が必要な場合は、これらの接続を使用します。

要件

InterScan MSS による POP3 トラフィックの検索には、ネットワークにファイアウォールがインストールされ、ネットワーク上の InterScan MSS を除くすべてのコンピュータからの POP3 要求をブロックするように設定されている必要があります。この設定により、すべての POP3 トラフィックがファイアウォールを通過して InterScan MSS へ渡され、InterScan MSS で POP3 のデータフローが確実に検索されます。

POP3 の検索を有効にする

InterScan MSS が POP3 トラフィックの検索を開始する前に、POP3 検索を有効にして、POP3 設定を指定する必要があります。

POP3 の検索を有効にするには

1. メニューから [概要] を選択します。初期設定では [システム] タブが表示されます。

2. [POP3 接続を許可する] の横のチェックボックスをオンにします。
3. [保存] をクリックします。

POP3 設定を行う

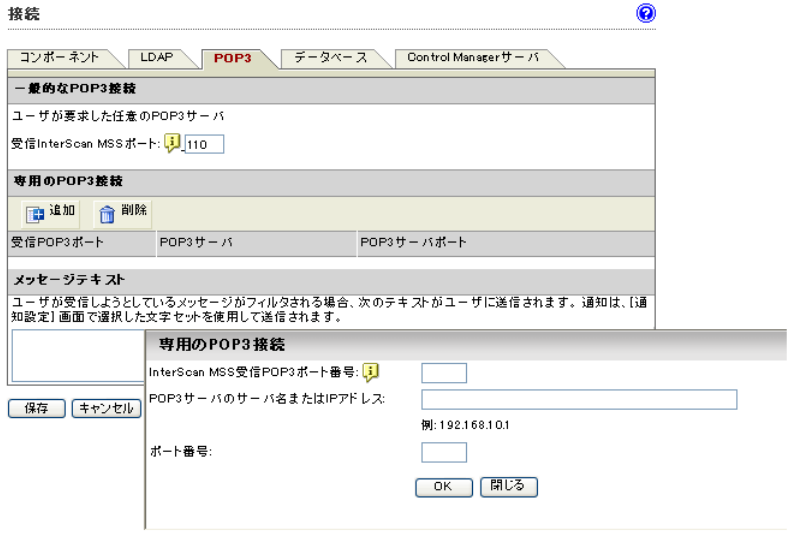
クライアントが使用する InterScan MSS サーバのポートを指定して、POP3 トラフィックを取り込むことができます。初期設定の POP3 ポートは「110」です。しかし、ユーザが認証済みの接続を介して POP3 サーバにアクセスする必要がある場合 (APOP コマンドや NTLM を使用する場合)、ポートの割当てをカスタマイズした専用の接続を設定することもできます。

POP3 接続を追加するには

1. メニューから、[管理]→[InterScan MSS の設定]→[接続] を選択します。初期設定では [コンポーネント] タブが表示されます。
2. [POP3] タブをクリックします。

3. 次のいずれかを実行します。

   - ユーザが初期設定のポート 110 と異なる POP3 サーバを要求した場合、それを許可するには、InterScan MSS の受信ポート番号を入力します。
   - 認証用に特定のポートを使用して POP3 サーバにアクセスするには、[追加] をクリックして新規の専用 POP3 接続を作成します。必要な情報を入力して、[OK] をクリックします。



4. [保存] をクリックします。

ポリシーを管理する

InterScan MSS ポリシーとは、受信および送信メールメッセージに適用されるルールのことです。ルールを作成して、組織のウイルス対策などのセキュリティを強化します。この項では、Policy Manager による InterScan MSS ポリシーの管理について概要を説明します。

Policy Manager の仕組み

複数のウイルス対策などのルールを作成して、フィルタを実行し、メッセージングシステムに対するセキュリティ上の脅威を抑制し、生産性の低下を防ぎます。

InterScan MSS ポリシーには、次のコンポーネントが含まれます。

- ルート — ポリシーが適用される送信者および受信者のメールアドレスのセットまたはグループ。アスタリスク (*) を使用してワイルドカード表現を作成し、ルートの設定を簡単にします。
- フィルタ — 特定のルートに適用されるルールまたはルールのセット。検索条件とも呼ばれます。InterScan MSS には、一般的なウイルスやその他の脅威に対処する定義済みのフィルタがあります。これらの定義済みフィルタを変更したり、専用のフィルタを定義できます。
- 処理 — フィルタの条件に一致した場合、InterScan MSS が実行する処理。フィルタの結果に応じて、最終的にメッセージを処理する方法が決定されます。

ポリシーの作成方法の詳細については、74 ページの「ポリシーを追加する」を参照してください。

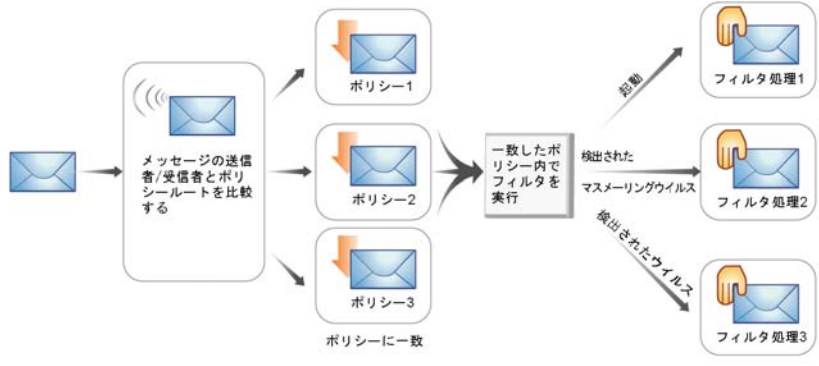


図 2-2.　Policy Manager のプロセスフローの簡略図

アドレスグループについて

アドレスグループとは、ポリシーが適用されるメールアドレスのリストのことです。

たとえば、企業のメールシステムを使用して送信されないようにブロックする 3 種類のコンテンツを特定し、これらのコンテンツを検出する 3 つのフィルタを定義するとします。

- 企業の極秘財務データ (FINANCIAL)
- 就職活動のメッセージ (JOBSEARCH)
- VBS スクリプトウイルス (VBSCRIPT)

企業内で次のアドレスグループを検討します。

- すべての幹部
- すべての人事部門
- すべての IT 開発スタッフ

ポリシーで使用するフィルタは、次のようにこれらのグループに適用するとします。

アドレスグループ	FINANCIAL	JOBSEARCH	VBSCRIPT
すべての幹部	適用しない	適用する	適用する
すべての人事部門	適用する	適用しない	適用する
すべての IT 開発スタッフ	適用する	適用する	適用しない

幹部、人事スタッフ、および IT 開発者には、財務情報、就職活動関連の文書、および VBS ファイルを送信する正当な理由がそれぞれあるので、これらのグループには一部のフィルタを適用しません。

InterScan MSS では、メールアドレスによって組織のメンバーを識別し、メンバーに適用するポリシーを決定します。正確で完全なアドレスグループを定義することで、適切なポリシーをグループ内の各メンバーに確実に適用できます。

アドレスグループを管理する

アドレスグループにより、複数のメールアドレスを 1 つのグループにまとめ、グループ内のすべてのアドレスに同じポリシーを適用できます。

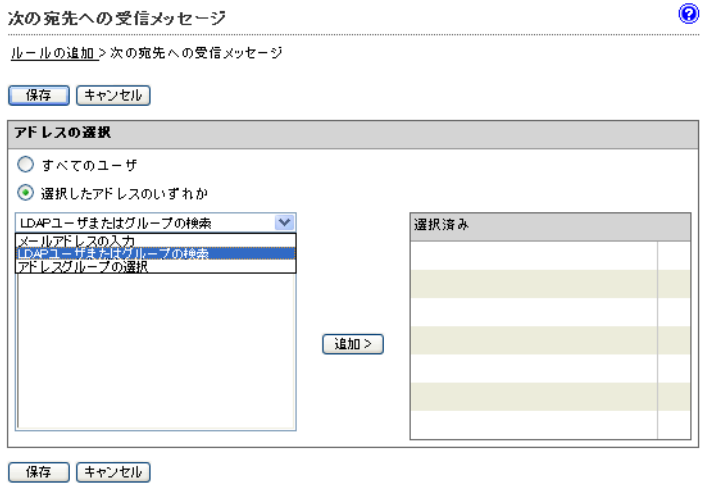
アドレスグループを追加する

ポリシー作成でルートを指定する際に、アドレスグループを作成できます。既存のポリシーを変更する際に、アドレスグループを追加することもできます。そのためには、メールアドレスを個別に追加したり、テキストファイルからインポートします。新規ポリシーを作成する際にアドレスグループを追加するには、次の手順に従ってください。

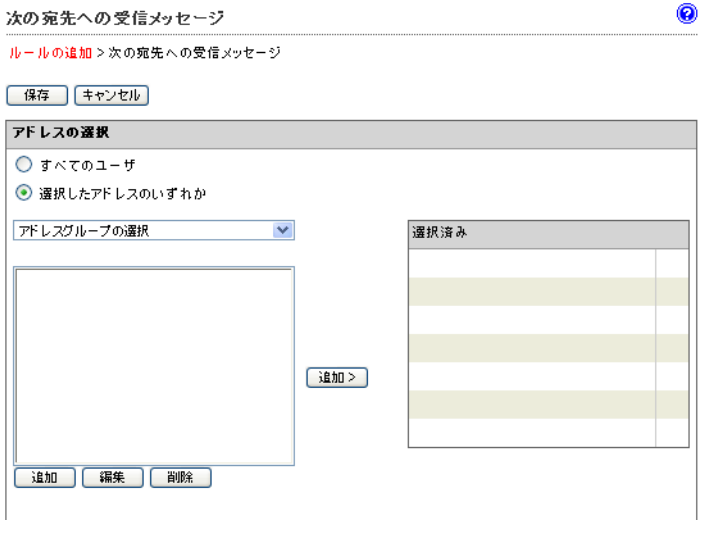
アドレスグループを追加するには

1. メニューから、[ポリシー]→[ポリシーリスト] の順に選択します。
2. [追加] ボタンをクリックします。
3. ドロップダウンリストから [ウイルス対策] または [その他] を選択し、ウイルス対策ルールまたはその他の脅威に対するルールを個別に作成します。

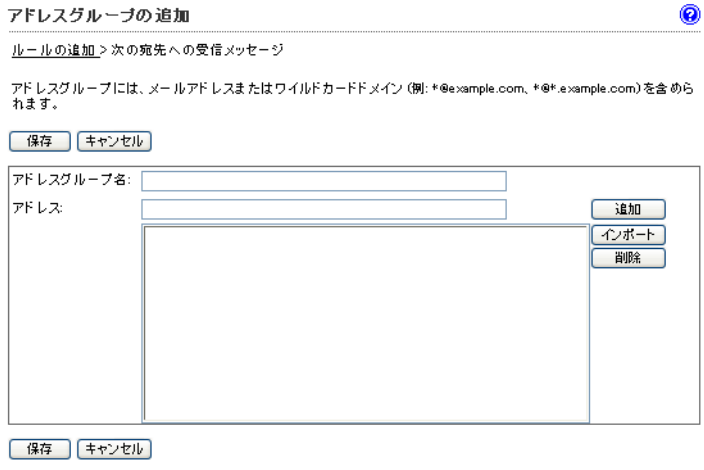
4. [受信者] または [送信者] リンクをクリックします。[アドレスの選択] 画面が表示されます。



5. ドロップダウンリストから [アドレスグループの選択] を選択します。



6. [追加] ボタンをクリックします。[アドレスグループの追加] 画面が表示されます。



7. グループ名を入力して、次のいずれかを実行します。

   - メールアドレスを入力して、[追加] をクリックし個々にメールアドレスを追加します。ワイルドカード文字を使用して、メールアドレスを指定できます。たとえば、「*@hr.com」のように入力します。
   - [インポート] ボタンをクリックして、定義済みのメールアドレスのリストが記載されたテキストファイルをインポートします。

   注意： InterScan MSS 7.0 では、メールアドレスをインポートできるのは 1 つのテキストファイルからのみです。テキストファイルで、1 行に 1 つのメールアドレスのみが記載されていることを確認します。ワイルドカード文字を使用して、メールアドレスを指定できます。たとえば、「*@hr.com」のように入力します。

8. [保存] をクリックします。

アドレスグループを編集または削除する

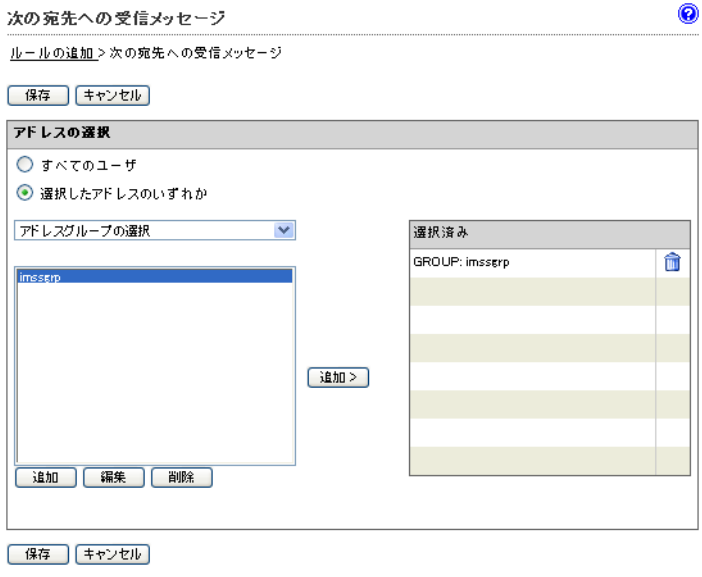
アドレスグループを編集または削除するには、既存のポリシーを編集します。

アドレスグループを編集または削除するには

1. メニューから、[ポリシー]→[ポリシーリスト] の順に選択します。
2. 既存のポリシーのリンクをクリックします。
3. [受信者と送信者] リンクをクリックします。

4. [受信者] または [送信者] リンクをクリックします。[アドレスの選択] 画面が表示されます。

5. ドロップダウンリストから [アドレスグループの選択] を選択します。



6. 必要なアドレスグループを選択し、[編集] または [削除] ボタンを必要に応じてクリックします。

LDAP ユーザまたはグループを検索する

ポリシーのルートを指定する際に、個々のメールアドレスまたはアドレスグループを入力せずに、LDAP ユーザまたはグループを検索することもできます。

InterScan MSS では、次の 3 種類の LDAP サーバをサポートしています。

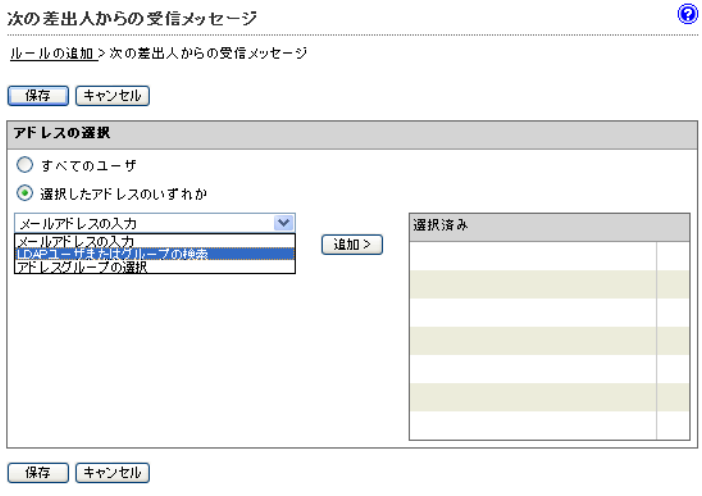
- Microsoft Active Directory 2000 または 2003
- IBM Lotus Domino 6.0 以上
- SUN One LDAP

新規ポリシーを作成する際に LDAP ユーザまたはグループを追加するには、次の手順に従ってください。

LDAP ユーザまたはグループを追加するには

1. メニューから、[ポリシー]→[ポリシーリスト] の順に選択します。
2. [追加] ボタンをクリックします。
3. ドロップダウンリストから [ウイルス対策] または [その他] を選択し、ウイルス対策ルールまたはその他の脅威に対するルールを個別に作成します。

4. [受信者] または [送信者] リンクをクリックします。[アドレスの選択] 画面が表示されます。



5. ドロップダウンリストから [LDAP ユーザまたはグループの検索] を選択します。

6. 検索する LDAP ユーザまたはグループを入力します。

注意： 1. 検索する際には、アスタリスク (*) ワイルドカードを使用できます。96 ページの「アスタリスクワイルドカードを使用する」を参照してください。

2. 内部アドレスを追加する際には、LDAP グループも検索できます。詳細については、72 ページの「内部アドレスを設定する」を参照してください。

7. [検索] ボタンをクリックします。

8. LDAP サーバ上に適合するレコードが存在する場合、LDAP ユーザまたはグループが表示されます。

9. そのユーザまたはグループを選択して [追加] ボタンをクリックし、それを受信者または送信者のリストに追加します。

内部アドレスを設定する

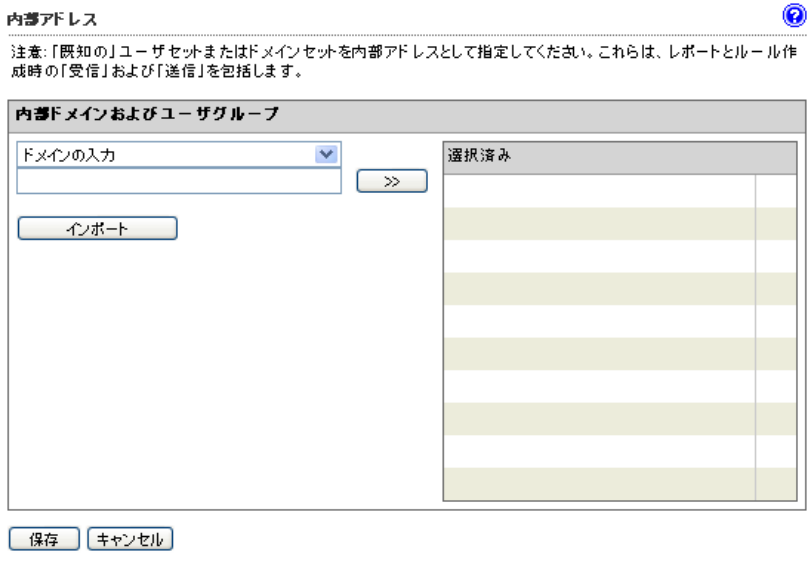
InterScan MSS では、レポートとルールを作成する際に、どのポリシーとイベントが受信用、送信用であるかを判断するために、内部アドレスが使用されます。

新規ルールを追加したり既存ルールを変更する際に受信メッセージまたは送信メッセージを選択する場合、次のように送信者および受信者を [内部アドレス] リストに入れてください。

- 送信メッセージのルールを設定している場合、内部アドレスのリストは送信者に適用されます。
- 受信メッセージのルールを設定している場合、内部アドレスのリストは受信者に適用されます。

内部アドレスを設定するには

1. メニューから、[ポリシー]→[内部アドレス] の順に選択します。[内部アドレス] 画面が表示されます。



2. 次のいずれかを実行します。

   - 内部ドメイン名を入力し、[>>] ボタンをクリックして内部アドレスのリストにドメインを追加します。

注意： 内部アドレスを追加する際には、LDAP グループも検索できます。詳細については、68 ページの「LDAP ユーザまたはグループを検索する」を参照してください。

   - [インポート] ボタンをクリックし、内部ドメインのリストをテキストファイルからインポートします。

3. [保存] をクリックします。

ポリシーを追加する

ポリシーを作成する前に、内部アドレスが設定されていることを確認します。詳細については、72 ページの「内部アドレスを設定する」を参照してください。

ポリシーを作成するには、次の 4 つの手順を実行してください。

手順 1: ルートを指定する
手順 2: 検索条件を指定する
手順 3: 処理を指定する
手順 4: 優先順位を指定する

ヒント： ウイルスがまん延しないように、すべてのメッセージを確実に検索するために、「すべてのメッセージ」に適用するウイルス対策ルールを少なくとも 1 つ保持することをお勧めします。ウイルス対策ルールのルートを指定する際には、ドロップダウンリストから [すべてのメッセージ] を選択します。

ルートを指定する

新しいポリシーを追加するには

1. メニューから、[ポリシー]→[ポリシーリスト] の順に選択します。[ポリシーリスト] 画面が表示されます。
2. [追加] をクリックします。

3. ドロップダウンリストから [ウイルス対策] または [その他] を選択します。

注意： ウイルス対策ルールにより、スパイウェア、ワームなどのウイルスおよびその他の不正プログラムについてメッセージが検索されます。その他のルールにより、スパムメールやフィッシングメッセージ、メッセージの内容、およびその他の添付ファイルが検索されます。

4. [ルールの追加] 画面が表示されます。

5. [このルールの適用対象] の横にあるドロップダウンリストからポリシールートの種類を選択します

   - 受信メッセージ
   - 送信メッセージ
   - 受信と送信の両方
   - POP3
   - すべてのメッセージ (ウイルス対策ルールを作成する際にのみ適用)

6. 受信者と送信者を選択します。

   - 受信メッセージの場合は、内部アドレスの範囲内にある、受信者のアドレスを指定します(例 : 内部アドレスは「*@example.com」で、有効な受信者は「jim@example.com」、「bob@example.com」などです)。
   - 送信メッセージの場合は、内部アドレスの範囲内にある、送信者のアドレスを指定します(例 : 内部アドレスは「*@example.com」で、有効な送信者は「jim@example.com」、「bob@example.com」などです)。
   - 受信メッセージと送信メッセージの両方の場合において、ルールは、メールアドレスに一致する受信者または送信者に適用されます。

注意 : 1. メールアドレスを指定する際には、アスタリスク (*) ワイルドカードを使用できます。詳細については、96 ページの「アスタリスクワイルドカードを使用する」を参照してください。

2. POP3 が選択されている場合、ルートを設定できません。ルールはすべてのルートに適用されます。

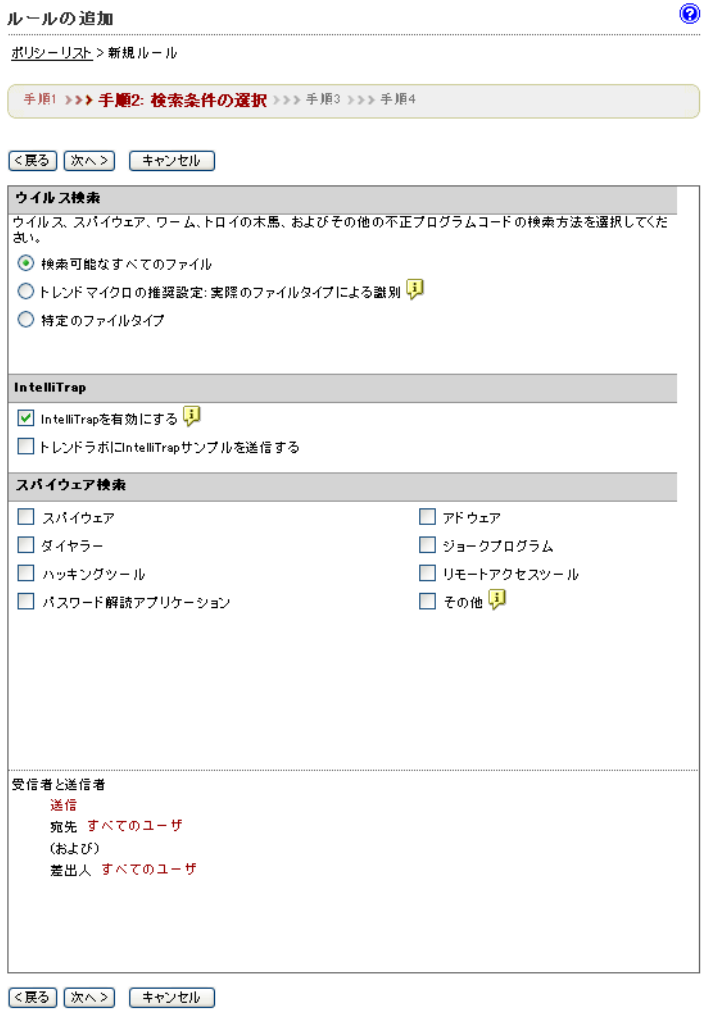
3. ウイルス対策ルールに対して [すべてのメッセージ] を選択した場合、そのルールは任意の送信者から任意の受信者へのすべてのメッセージに適用されます。

検索条件を指定する

検索条件を指定するには

1. [次へ] をクリックします。[手順 2: 検索条件の選択] 画面が表示されます。

2. 必要に応じて、チェックボックスをオンにします。ウイルス対策ルールおよびその他のルールに対する検索条件のカテゴリは、次のとおりです。



- ウイルス対策ルール

- ウイルス検索 — ウイルスやその他の不正プログラムを含むメッセージおよび特定のファイルタイプを検索する初期設定の方法を設定します。また、トレンドマイクロの推奨設定を使用して、害のないファイル拡張子名で装った不正コードを特定します。
- Intellitrap — 圧縮ファイルのウイルス / 不正プログラムを検索し、サンプルを TrendLab に送信して調査します。

- スパイウェア検索 — スパイウェア、アドウェアなどのその他の種類の脅威を検索します。

- その他のルール

- スパムメール / フィッシングメール — スパムメールおよびフィッシングメッセージと識別されたメッセージを検索します。スパムメールとは、主に広告を目的とした迷惑メールのことです。一方、フィッシングメッセージは、信頼できる団体に見せかけた送信者から発信されます。
- 添付ファイル — 特定の拡張子が付いた添付ファイルや特定の実際のファイルタイプに属す添付ファイルなど、選択した条件に一致した添付ファイルを検索します。
- サイズ — 指定されたメッセージサイズに一致するメッセージを検索します。
- コンテンツ — 件名、本文、ヘッダ、添付ファイルのコンテンツキーワード表現のリンク内で指定された表現と一致するキーワード表現を持つメッセージを検索します。
- その他 — 指定された受信者数と一致するメッセージを検索します。また、指定された時間内に受信したメッセージを検索します。

処理を指定する

処理を設定するには

1. [次へ] をクリックします。[手順 3: 処理の選択] 画面が表示されます。

注意： この手順で表示されるユーザインタフェースは、作成しているルールの種類に応じて異なります。ウイルス対策ルールには 2 つのタブがあり、基本処理と特殊なウイルスに対する処理を設定できます。

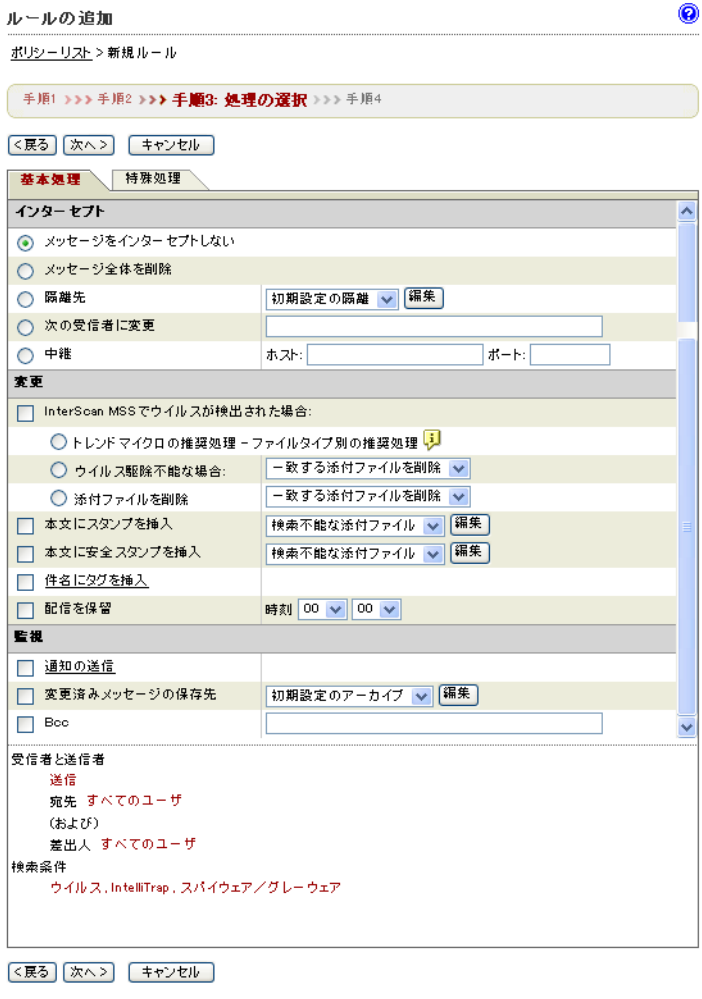
2. ウイルス対策ルールとその他のルールの両方に対する基本処理は、同様の処理ですが、オプションが多少異なります。次のカテゴリから必要な処理を選択します。

   - インターセプト — メッセージをインターセプトして受信者に送信されないようにすることができます。インターセプトを選択すると、インターセプトされたメッセージに実行する処理を指定できます。
   - 変更 — スタンプの挿入や件名にタグを付けるなど、メッセージや添付ファイルに対する変更を指示します。
   - 監視 — さらに解析する場合、通知を送信し、メッセージをアーカイブに保管し、メッセージを Bcc 送信するよう指示します。

ウイルス対策ルールの処理を指定するには

各タブをクリックして、基本処理または特殊なウイルスに対する処理を指定します。

1. 基本処理 — メッセージが「手順 2: 検索条件」で指定した検索条件と一致した場合の初期設定処理を指定します。



2. 特殊処理 — メッセージが次の基準のいずれかに一致した場合の処理を指定します。この画面で指定する処理は、[基本処理] タブで指定した初期設定の処理に優先します。

   - マスメーリング — マスメーリングメッセージが検出されると、InterScan

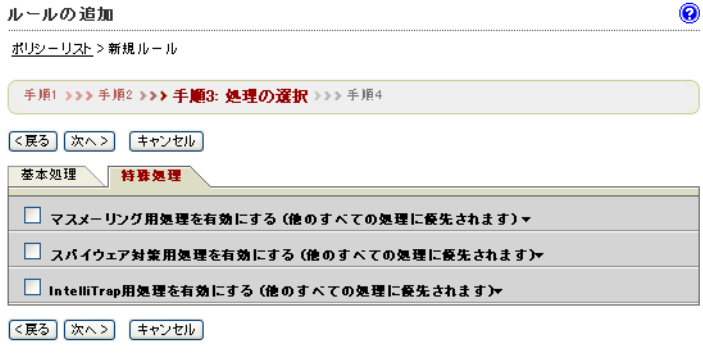
MSS はこのセクションで指定した処理を実行します。

- スパイウェア — [手順 2: 検索条件] 画面で [スパイウェア検索] オプションのうちひとつでも選択した場合は、対応する処理を指定できます。78 ページの「検索条件を指定する」を参照してください。スパイウェアが検出されると、ここで指定した処理が実行されます。

> **注意：** 処理が選択されていない場合、[スパイウェア検索] の条件に一致するメッセージに対して初期設定の処理が実行されます。

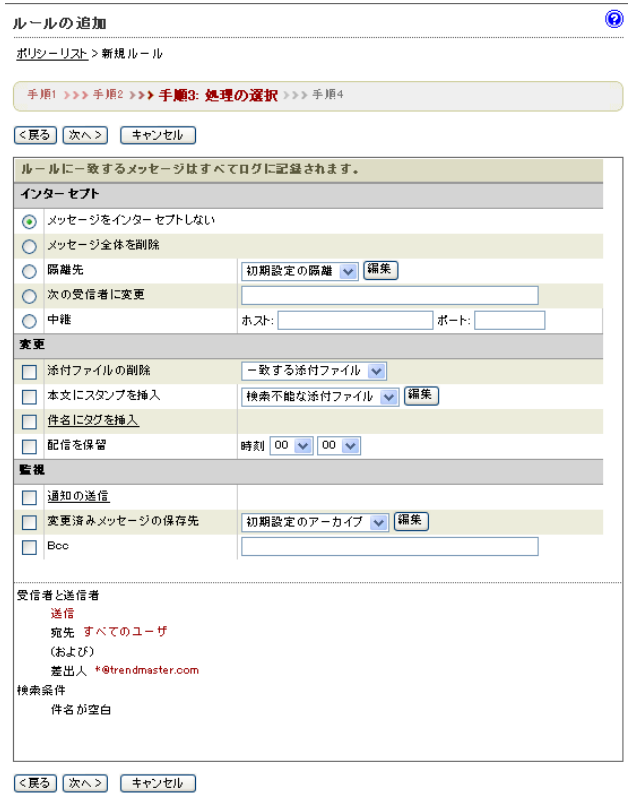
- IntelliTrap — [手順 2: 検索条件] 画面で [IntelliTrap] オプションが選択されている場合、対応する処理を指定できます。78 ページの「検索条件を指定する」を参照してください。

> **注意：** 処理が選択されていない場合、[IntelliTrap] の条件に一致するメッセージに対して初期設定の処理が実行されます。



その他のルールの処理を指定するには

その他のルールを作成する際、[処理の選択] 画面は次のように表示されます。



優先順位を指定する

ルールの優先順位を設定することにより、作成したポリシーのリストに対してメッセージが一致する順序を制御できます。

優先順位を指定するには

1. [次へ] をクリックします。[手順 4: 名前と順序] 画面が表示されます。

2. [有効] チェックボックスをオンにして、ルールを有効にします。
3. [ルール名] フィールドにルールの名前を入力します。
4. [**順序番号**] フィールドに、検索を実行する優先順位を指定します。指定した順番でメッセージにルールが適用されます。

5. [備考] タブをクリックします。[備考] 画面が表示されます。

6. 備考を入力して、新しいルールを他のルールと区別します。
7. [完了] をクリックします。

例 1

特定のファイル名または拡張子を持つ添付ファイルを削除して、該当する受信メッセージに説明のスタンプを挿入して受信者に送信するルールを作成する方法。

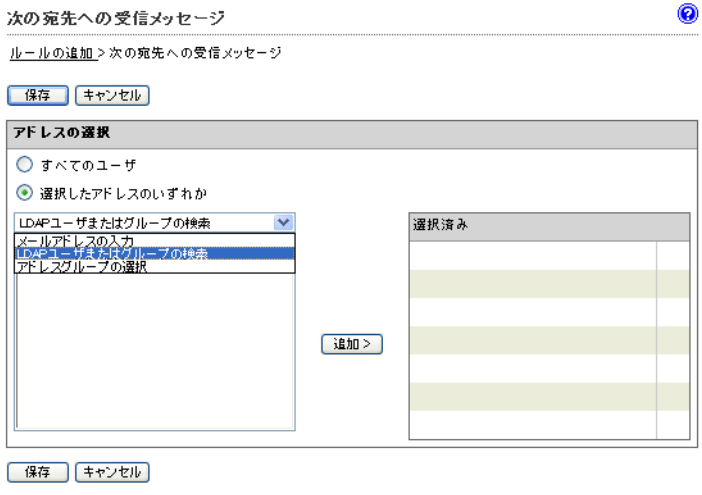
手順 1: ルートを指定する

1. メニューから、[ポリシー]→[ポリシーリスト] の順に選択します。
2. [追加] をクリックします。
3. ドロップダウンリストから [その他] を選択します。[手順 1: 受信者と送信者の選択] 画面が表示されます。
4. [このルールの適用対象] の横にある、ドロップダウンリストから [受信メッセージ] を選択します。
5. [受信者] リンクをクリックします。[アドレスの選択] 画面が表示されます。

a. このルールを任意の受信者に適用するには、[すべてのユーザ] を選択します。

b. このルールを特定の受信者に適用するには、[選択したアドレスのいずれか] を選択し、メールの宛先のアドレスまたはグループを指定します。

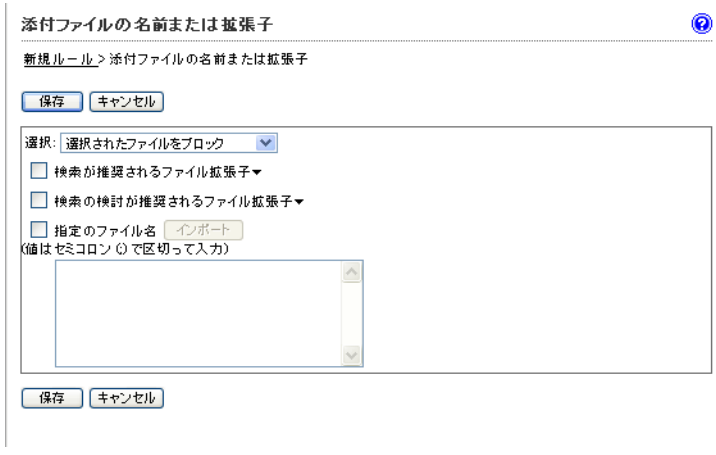
c. [保存] をクリックします。[手順 1: 受信者と送信者の選択] 画面が表示されます。



手順 2: 検索条件を指定する

1. [次へ] をクリックします。[手順 2: 検索条件の選択] 画面が表示されます。
2. [次の場合にルールの処理を実行する] の横にある [いずれかの条件に一致 (OR)] を選択します。
3. [名前または拡張子] 条件を有効にするには、その横のチェックボックスをオンにします。

4. [名前または拡張子] をクリックします。[添付ファイルの名前または拡張子] 画面が表示されます。



5. [検索が推奨されるファイル拡張子] または [検索の検討が推奨されるファイル拡張子] を選択します。

6. [保存] をクリックします。[手順 2: 検索条件の選択] 画面が表示されます。

手順 3: 処理を指定する

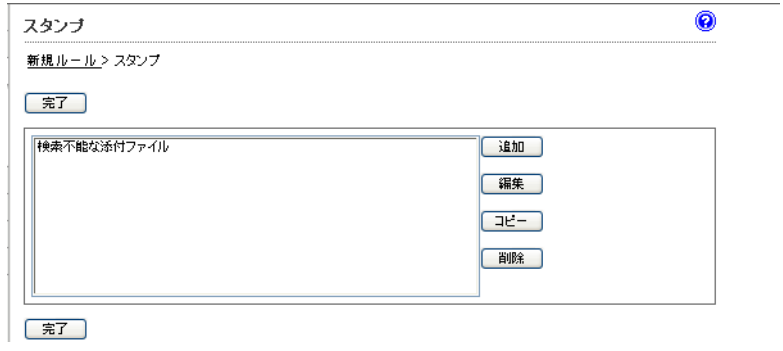
1. [次へ] をクリックします。[手順 3: 処理の選択] 画面が表示されます。

2. [変更] の下で、[添付ファイルの削除] 処理を有効にするには、その横のチェックボックスをオンにします。

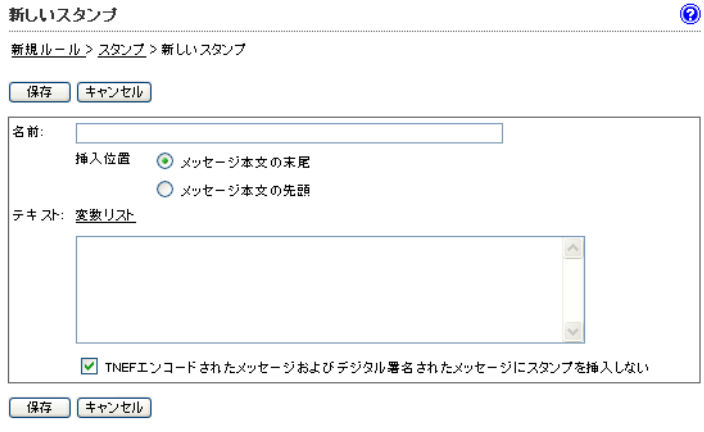
3. [一致する添付ファイル] が選択されてない場合、ドロップダウンリストから選択します。

4. [本文にスタンプを挿入] チェックボックスをオンにします。

5. ドロップダウンリストに利用できる適切なスタンプがない場合、[編集] をクリックします。[スタンプ] 画面が表示されます。



6. [追加] をクリックして、新しいスタンプを作成します。[新しいスタンプ] 画面が表示されます。



7. 必要な情報を指定します。
8. [保存] をクリックします。[スタンプ] 画面が再表示されます。
9. [完了] をクリックします。[処理の選択] 画面が再表示されます。
10. ドロップダウンリストから新しく作成したスタンプを選択します。

手順 4: 優先順位を指定する

1. [次へ] をクリックします。[手順 4: 名前と順序] 画面が表示されます。
2. ルールの名前と順序の番号を入力します。
3. [完了] をクリックします。新しく作成したルールは、[ポリシーリスト] 画面で強調表示されています。

例 2

件名または本文に特定のキーワードを含むメッセージを隔離するルールを作成して、このルールを管理者を除くすべての受信者に適用する方法。

手順 1: ルートを指定する

1. メニューから、[ポリシー]→[ポリシーリスト] の順に選択します。[ポリシーリスト] 画面が表示されます。
2. [追加] をクリックします。
3. ドロップダウンリストから [その他] を選択します。[手順 1: 受信者と送信者の選択] 画面が表示されます。
4. [このルールの適用対象] の横にある、ドロップダウンリストから [受信メッセージ] を選択します。
5. [受信者] リンクをクリックします。[アドレスの選択] 画面が表示されます。
6. [すべてのユーザ] を選択します。
7. [保存] をクリックします。[手順 1: 受信者と送信者の選択] 画面が表示されます。

8. [除外] 横の [送信者から受信者] リンクをクリックします。[次を除く受信メッセージ] 画面が表示されます。

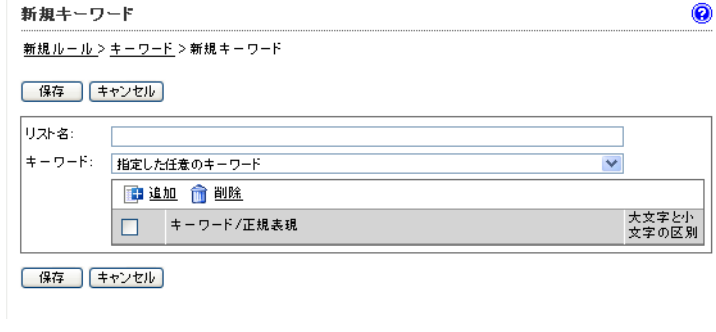
9. [差出人 (送信者)] の下に、「*@*」と入力して任意の送信者を指定します。
10. [宛先 (受信者)] の下に、管理者のメールアドレスを入力します。
11. [追加] をクリックします。リストに送信者と受信者のペアが表示されます。
12. 他の管理者または受信者を追加するには、手順 9 ～ 11 を繰り返します。
13. すべての必要な受信者を追加したら、[保存] をクリックします。[手順 1: 受信者と送信者の選択] 画面が表示されます。

手順 2: 検索条件を指定する

1. [次へ] をクリックします。[手順 2: 検索条件の選択] 画面が表示されます。
2. [次の場合にルールの処理を実行する] の横にある [いずれかの条件に一致 (OR)] を選択します。
3. [コンテンツ] の下の [件名のキーワード] 条件を有効にするには、その横のチェックボックスをオンにします。

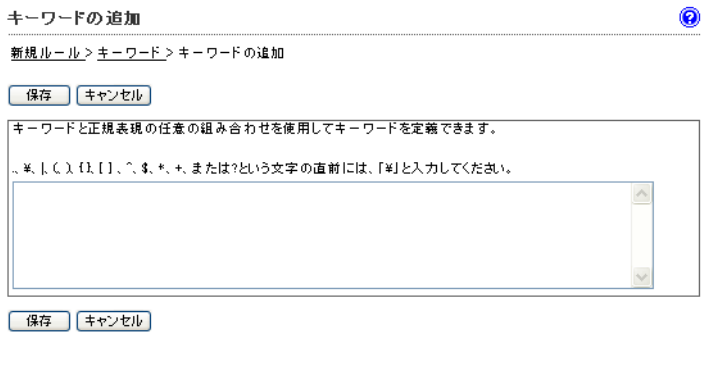
4. [件名のキーワード] をクリックします。[キーワード] 画面が表示されます。

5. 既存のリストから必要なキーワードが使用できない場合、[追加] をクリックして新しいキーワードリストを作成します。[新規キーワード] 画面が表示されます。



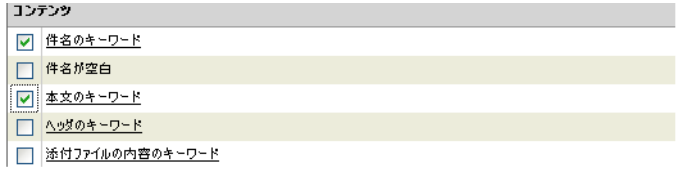
6. 必要な情報を指定します。

7. 個々のキーワードを追加するには、[追加] をクリックします。[キーワードの追加] 画面が表示されます。



8. 必要なキーワードを入力して、[保存] をクリックします。[新規キーワード] 画面が再表示されます。
9. 手順 7 と 8 を繰り返して、キーワードを追加します。
10. すべての必要なキーワードを追加したら、[保存] をクリックします。[キーワード] 画面に新しく作成したキーワードリストが追加されて、再表示されます。
11. 新しいリストを選択し、[>>] をクリックしてリストを [選択済み] ボックスに挿入します。
12. [保存] をクリックします。[手順 2: 検索条件の選択] 画面が表示されます。
13. [本文のキーワード] 条件を有効にするには、その横のチェックボックスをオンにします。
14. [本文のキーワード] をクリックします。[キーワード] 画面が表示されます。
15. 新しいキーワードリストを選択し、[>>] をクリックしてリストを [選択済み] ボックスに挿入します。

16. [保存] をクリックします。[手順 2: 検索条件の選択] 画面が表示されます。[件名のキーワード] と [本文のキーワード] が両方とも選択されていることを確認します。



手順 3: 処理を指定する

1. [次へ] をクリックします。[手順 3: 処理の選択] 画面が表示されます。
2. [インターセプト] の下で、[隔離先] を選択します。
3. 初期設定の隔離領域を使用するか、ドロップダウンリストをクリックして使用したい隔離領域を選択します。

手順 4: 優先順位を指定する

1. [次へ] をクリックします。[手順 4: 名前と順序] 画面が表示されます。
2. ルールの名前と順序の番号を入力します。
3. [完了] をクリックします。新しく作成したルールは、[ポリシー] リストの画面で強調表示されています。

アスタリスクワイルドカードを使用する

ルートを定義する際のメールアドレス、およびファイル名には、アスタリスク (*) をワイルドカードとして使用できます。

メールアドレスのワイルドカード

ワイルドカードは、メールアドレスの名前またはドメインの部分に表現できます。有効なワイルドカードの例は、次のとおりです。

- *@* — すべてのメールアドレスの有効な表現です。
- *@domain.tld、name@*.tld — 名前全体またはドメイン (トップレベルのドメイン (TLD) を除く) の有効な表現です。
- *@*.tld — 名前およびドメイン (TLD 以外) の両方の有効な表現です。

ワイルドカードは、サブドメインやトップレベルドメインに表現することはできません。また、ワイルドカードは単独で表現する必要があり、他の文字とともに表現することはできません。無効なワイルドカードの例は、次のとおりです。

- name@domain.*.tld — サブドメインの無効な表現です。
- name@domain.* — トップレベルドメインの無効な表現です。
- *name@domain.tld — 名前の一部に使用した無効な例です。

ファイル名のワイルドカード

ワイルドカードをメールアドレスと同様の方法でファイル名に使用できます。アスタリスクをファイル名の名前または拡張子の部分に使用します。ただし、名前や拡張子の一部として使用することはできません。以下は、有効なワイルドカードの例です。

- *.* — すべてのファイル名の有効な表現です。
- *. 拡張子 — 特定の拡張子を持つすべてのファイル名の有効な表現です。
- 名前 .* — 特定の名前で、任意の拡張子を持つファイル名の有効な表現です。

無効なワイルドカードの例は、次のとおりです。

- * 名前 .* — ファイル名の無効な表現です。
- 名前 .* 拡張子 — 拡張子の無効な表現です。

検索エンジンとパターンファイルをアップデートする

最新の不正プログラムからネットワークを常時保護するには、検索エンジン、ウイルスパターンファイルなどの InterScan MSS コンポーネントが定期的にアップデートされるようにします。コンポーネントのアップデートは、手動または予約による実行を選択できます。

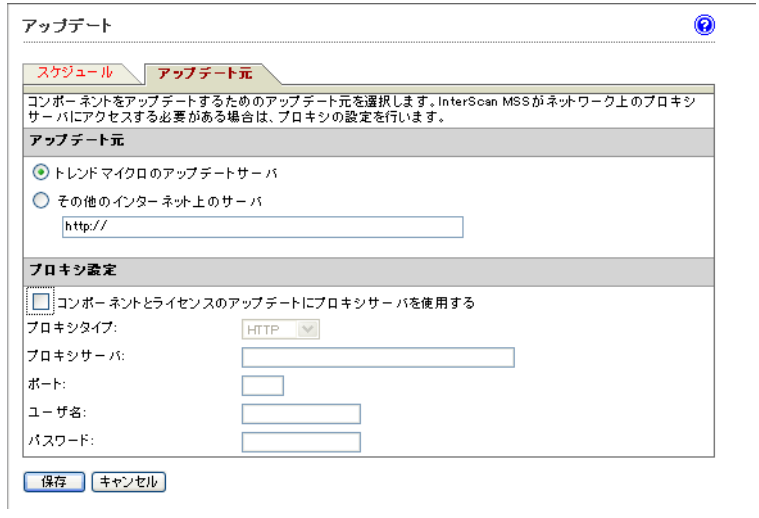
アップデート元を指定する

検索エンジンおよびパターンファイルをアップデートする前に、アップデート元を指定する必要があります。初期設定では、トレンドマイクロのアップデートサーバからコンポーネントをダウンロードします。トレンドマイクロのアップデートサーバは、最新コンポーネントの唯一のアップデート元です。ただし、Trend Micro Control Manager (以下、Control Manager) を使用して InterScan MSS を管理している場合、Control Manager のサーバからコンポーネントをアップデートできます。

InterScan MSS の設定時に設定ウィザードを使用してアップデート元を指定しなかった場合、次のようにアップデート元またはプロキシ設定を入力してください。

1. メニューから [管理]→[アップデート] を選択します。[アップデート] 画面が表示されます。

2. [アップデート元] タブをクリックします。



3. アップデート元を選択して、必要な情報を入力します。

4. [保存] をクリックします。

手動アップデートを実行する

次のような状況の場合、InterScan MSS コンポーネントの手動アップデートを実行できます。

- InterScan MSS のインストールまたはアップグレードの直後
- ネットワークセキュリティが不正プログラムの新たな危険にさらされている恐れがあり、すぐにコンポーネントをアップデートしたい場合

手動アップデートを実行するには

1. メニューから [概要] を選択します。初期設定で [システム] タブが選択された状態で [概要] 画面が表示されます。

2. すべてのコンポーネントをアップデートするには、最初の列のヘッダにある ([名前] フィールドの隣にある) チェックボックスをオンにします。すべてのコンポーネントではなく、特定のコンポーネントをアップデートするには、必要なコンポーネントの横にあるチェックボックスをオンにします。

3. [アップデート] ボタンをクリックします。

コンポーネントのアップデートをロールバックする

InterScan MSS のコンポーネントをアップデートした後にシステムに障害が発生した場合、旧バージョンにロールバックできます。

コンポーネントのアップデートをロールバックするには

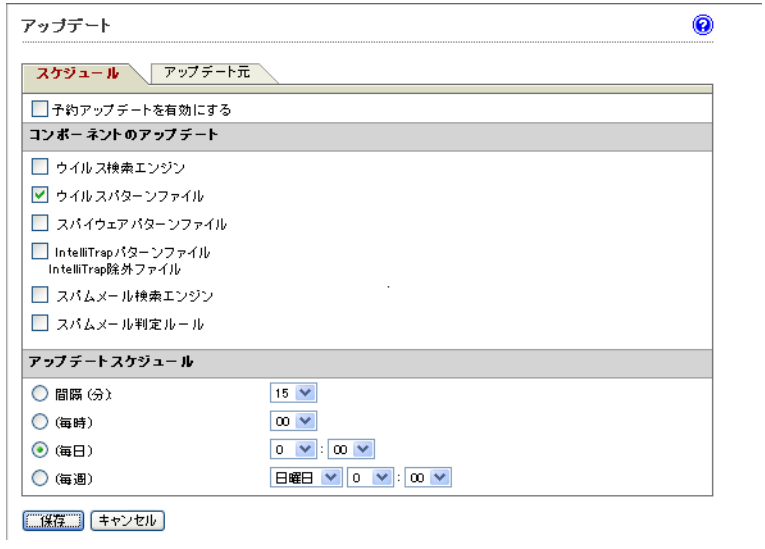
1. メニューから [概要] を選択します。[概要] 画面に、初期設定で選択された [システム] タブが表示されます。
2. すべてのコンポーネントを旧バージョンにロールバックするには、最初の列のヘッダにある ([名前] フィールドの隣にある) チェックボックスをオンにします。すべてのコンポーネントではなく、特定のコンポーネントをロールバックするには、必要なコンポーネントの横にあるチェックボックスをオンにします。
3. [ロールバック] ボタンをクリックします。

予約アップデートを設定する

InterScan MSS が指定した間隔で自動的にコンポーネントをアップデートするように指定するには、アップデートの予約を設定します。

予約アップデートを設定するには

1. メニューから [管理]→[アップデート] を選択します。[アップデート] 画面に、初期設定で選択された [スケジュール] タブが表示されます。



2. 必要な情報を指定します。
3. [保存] をクリックします。

ログを設定する

InterScan MSS がクエリ用のデータベースログとトラブルシューティング用のアプリケーションログを保持する期間を指定するには、ログを設定します。

1. メニューから [ログ]→[設定] を選択します。[ログの設定] 画面が表示されます。

2. 必要な情報を指定します。
3. [保存] をクリックします。

第 3 章

設定のバックアップ、復元、複製について

本章では、システム障害に備えて、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) の設定のバックアップと復元の手順を説明します。Trend Micro Control Manager (以下、Control Manger) を使用して、一度に複数の InterScan MSS 検索サービスを配置した場合、検索サービスごとに InterScan MSS の設定を行わずに設定の複製を作成できます。

この章の内容は次のとおりです。

- 106 ページの「InterScan MSS のバックアップ」
- 109 ページの「InterScan MSS の復元」
- 111 ページの「設定の複製」

InterScan MSS のバックアップ

InterScan MSS をインストールし、必要な設定を行った後、常に設定内容のバックアップを作成しておくと、システム障害時にすばやく InterScan MSS を復元できます。

次のように、全体または最小限の InterScan MSS のバックアップを実行することができます。

- 全体 — /opt/trend に格納されたすべての InterScan MSS のローカル設定やバイナリファイル、および /var/imss に格納されたデータベース関連ファイルをバックアップします。
- 最小限 — /opt/trend/imss/config に格納された InterScan MSS の設定のみバックアップします。

注意： 1. 本書で説明するバックアップおよび復元の手順は、オールインワン配置の場合を対象としています。分散配置の場合にバックアップが必要な内容は、次のとおりです。
a. データベースがインストールされたコンピュータ上のデータベースファイルまたはテーブル
b. InterScan MSS コンポーネントがインストールされた各コンピュータのローカルのバイナリファイルおよび設定ファイル

2. 最小限のバックアップを実行する際、InterScan MSS の復元後に、以前の HotFix、Patch または Service Pack のインストールが必要になる場合があります。

全体のバックアップを実行するには

1. すべての InterScan MSS 関連プロセスを停止します。
   - /opt/trend/imss/script/S99ADMINUI stop
   - /opt/trend/imss/script/S99IMSS stop
   - /opt/trend/imss/script/S99POLICY stop
   - /opt/trend/imss/script/S99MANAGER stop
   - /opt/trend/imss/script/S99CMAGENT stop
   - /opt/trend/imss/script/S99EUQ stop
   - /opt/trend/imss/script/S99SCHEDULED stop
   - /opt/trend/imss/script/S99FOXDNS stop
2. Postfix を停止します。
3. /opt/trend/ および /var/imss/ フォルダのバックアップを作成します。
4. Postfix 設定ファイル main.cf および master.cf のバックアップを作成します。
5. Postfix を起動します。
6. すべての InterScan MSS 関連プロセスを起動します。
   - /opt/trend/imss/script/S99ADMINUI start
   - /opt/trend/imss/script/S99IMSS start
   - /opt/trend/imss/script/S99POLICY start
   - /opt/trend/imss/script/S99MANAGER start
   - /opt/trend/imss/script/S99CMAGENT start
   - /opt/trend/imss/script/S99EUQ start
   - /opt/trend/imss/script/S99SCHEDULED start
   - /opt/trend/imss/script/S99FOXDNS start

最小限のバックアップを実行するには

1. すべての InterScan MSS 関連プロセスを停止します。詳細については、107 ページの「全体のバックアップを実行するには」を参照してください。
2. Postfix を停止します。
3. /opt/trend/imss/config フォルダのバックアップを作成します。
4. すべてのデータベーステーブルのバックアップを作成します。
5. Postfix を起動します。
6. すべての InterScan MSS 関連プロセスを起動します。詳細については、107 ページの「全体のバックアップを実行するには」を参照してください。

InterScan MSS の復元

システム障害に備えて、事前に作成した全体または最小限のバックアップに従って、InterScan MSS を復元できます。

全体の復元を実行するには

1. 1 台のコンピュータに InterScan MSS を新規インストールし、IP アドレス、データベースユーザ名、およびパスワードは元のものと同じにします。
2. すべての InterScan MSS 関連プロセスを停止します。詳細については、107 ページの「全体のバックアップを実行するには」を参照してください。
3. Postfix を停止します。
4. 以前のバックアップを使用して、/var/imss/ フォルダおよび /opt/trend/ フォルダを復元します。
5. Postfix 設定ファイルを復元します。
6. Postfix を起動します。
7. すべての InterScan MSS 関連プロセスを起動します。詳細については、107 ページの「全体のバックアップを実行するには」を参照してください。

最小限の復元を実行するには

1. 1 台のコンピュータに InterScan MSS を新規インストールし、IP アドレス、データベースユーザ名、およびパスワードは元のものと同じにします。
2. すべての InterScan MSS 関連プロセスを停止します。詳細については、107 ページの「全体のバックアップを実行するには」を参照してください。
3. Postfix を停止します。
4. 以前のバックアップを使用して、/opt/trend/imss/config/ フォルダを復元します。
5. Postfix 設定ファイルを復元します。

6. 以前のデータベーステーブルのバックアップを、新しいデータベースにインポートします。

7. すべての InterScan MSS 関連プロセスを起動します。詳細については、107 ページの「全体のバックアップを実行するには」を参照してください。

設定の複製

InterScan MSS の複数の検索サービスが管理データベースを共有せずそれぞれが独立して存在する場合、Control Manager を使用することにより、すべての検索サービスに設定を複製でき、それぞれ個別に設定する必要がなくなります。複数の検索サービスが同一の管理データベースを共有して存在する場合は、設定の複製は不要です。

Control Manger を使用して設定を複製する場合は、次の手順に従ってください。

手順 1: InterScan MSS 設定のバックアップを作成します。詳細については、106 ページの「InterScan MSS のバックアップ」を参照してください。

手順 2: Control Manager エージェントを有効にします。

手順 3: Control Manager 管理コンソールから設定を複製します。

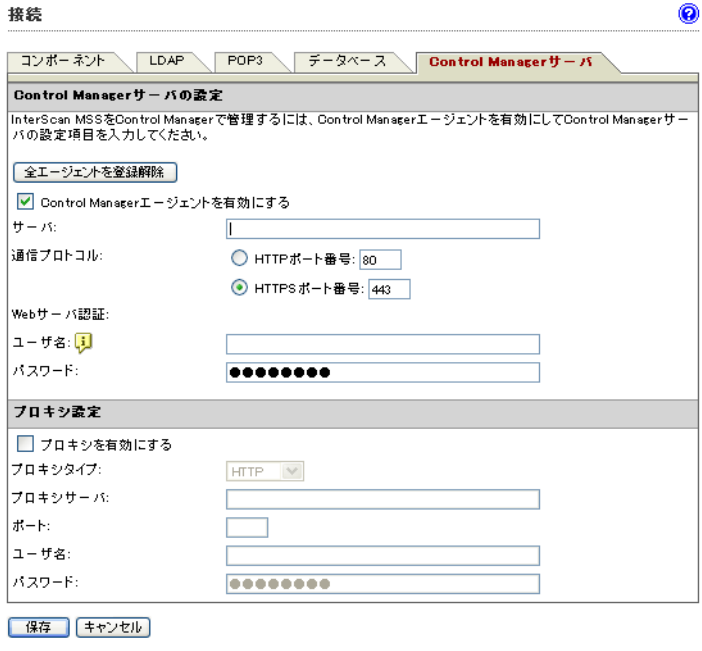
Control Manager エージェントを有効にする

Control Manager エージェントは、InterScan MSS のインストール時に自動的にインストールされます。Control Manager と統合するには、管理コンソールから Control Manager サーバの情報を設定し、エージェントを有効にする必要があります。

Control Manager サーバを設定するには

1. メニューから [管理]→[接続] を選択します。初期設定で［コンポーネント］タブが表示されます。

2. [Control Manager サーバ] タブをクリックします。[Control Manager サーバの設定] 画面が表示されます。



3. 必要な情報を指定します。
4. [Contol Manager エージェントを有効にする] チェックボックスをオンにします。
5. [保存] をクリックします。

Control Manager から設定を複製する

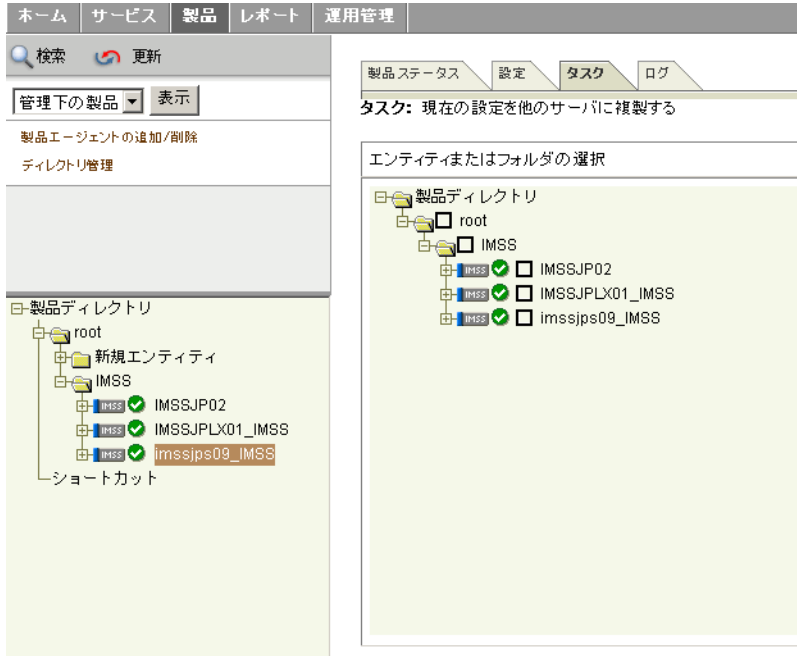
InterScan MSS 管理コンソールから Control Manager エージェントを有効にした後、Control Manager 管理コンソールにログオンして、InterScan MSS 設定の複製を開始できます。

InterScan MSS 設定を複製するには

1. Control Manager メニューから [製品] を選択します。
2. ユーザインタフェースの左側にある製品ディレクトリから、元になる InterScan MSS 検索サービスを特定します。
3. ［タスク］タブをクリックします。
4. ドロップダウンリストから [設定の複製] を選択します。

5. [次へ] をクリックします。

6. 対象サーバの横のチェックボックスをオンにします。



7. [複製]ボタンをクリックします。

第 4 章

保守

本章では、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) の日常的な保守タスクの実行に必要な一般手順を説明します。管理コンソールのフィールドの詳細については、オンラインヘルプを参照してください。

この章の内容は次のとおりです。

- 116 ページの「ネットワークの監視」
- 128 ページの「ログ」
- 130 ページの「隔離とアーカイブ」
- 138 ページの「イベント通知」
- 143 ページの「管理者アカウントの管理」
- 146 ページの「検索サービスおよびポリシー接続の設定」

ネットワークの監視

InterScan MSS には、ネットワークトラフィックを監視できるツールセットが用意されています。InterScan MSS コンポーネントのパフォーマンスについての統計など、有用な情報を取得でき、さまざまな検索条件に一致するメッセージの分析を表示するレポートも作成できます。

統計を表示する

InterScan MSS 検索サービスや IP プロファイラのパフォーマンスについて、最大過去 7 日間分の統計を入手できます。こうした統計には、有用な情報が含まれており、InterScan MSS ポリシーの管理やネットワークのセキュリティ向上に役立ちます。

統計を表示するには

1. メニューから [概要] を選択します。初期設定で［システム］タブが表示されます。
2. ［統計］タブをクリックします。
3. ［表示］ドロップダウンリストから必要な過去の日数を選択します。

注意： InterScan MSS では、毎時 15 分にデータベース内の統計情報が自動的に更新されます。[表示更新] をクリックすると画面内の情報を更新できます。データベース内で新たに更新された統計情報は、1 時間ごとの更新が行われるまで画面に反映されません。
たとえば、午後 4 時に［表示更新］をクリックしても、InterScan MSS によるデータベースの次回のアップデート時刻は午後 4 時 15 分です。InterScan MSS では、要求を処理するのに 2 分かかるため、新しい結果が反映されるのは、午後 4 時 17 分です。

統計を理解する

InterScan MSS では、パフォーマンス統計がグラフ形式および表形式で表示されます。この項では、値の算出方法、および［統計］タブの情報をグラフごとに分けて説明します。タブは [パフォーマンスの概要]、[検索パフォーマンス]、および [IP フィルタパフォーマンス] の 3 つにセクションに分かれています。

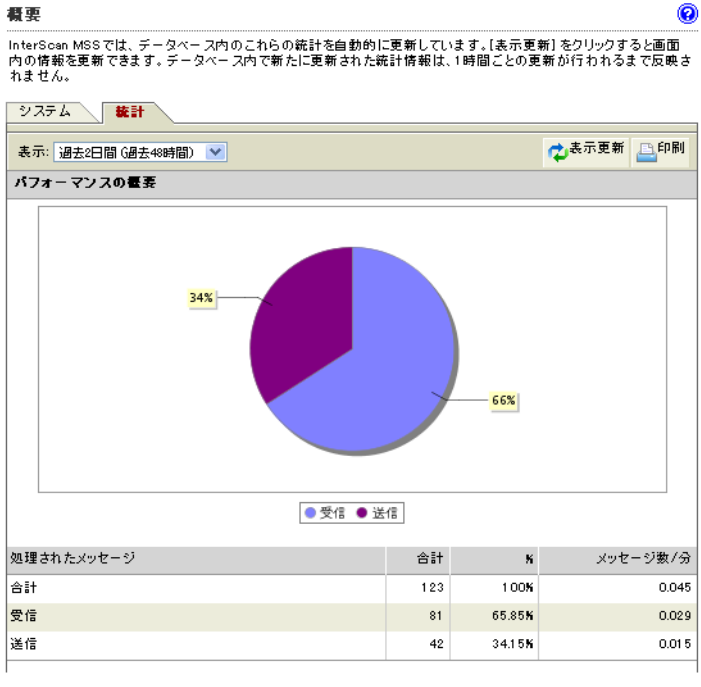
注意： 1. グラフと表では、示される同一種類の脅威の値 (%) の算出方法が異なります。

2. 表では、それぞれの検索条件または IP フィルタタイプに一致したメッセージ合計数が、重複してカウントされます。たとえば、1 件のメッセージが 2 つ以上の検索条件に一致した場合 (例 : スパムメールと添付ファイル)、このメッセージは 2 回カウントされます。つまり、スパムメールの合計数と添付ファイルの合計数にそれぞれ 1 回ずつカウントされます。ただし、グラフの値は重複してカウントされません。

パフォーマンスの概要

このセクションでは、ネットワーク内での受信および送信メッセージの合計件数、およびメッセージ総件数に対するそれぞれのメッセージの割合をパーセンテージで表示します。合計件数は、次のコンポーネントごとに分けられ、昇順で表示されます。

- IP プロファイラ
- Trend Micro Network Reputation Services (以下、NRS)
- 検索エンジン



検索パフォーマンス

このセクションでは、ポリシールールで指定されたさまざまな検索条件に一致したメッセージの合計件数が表示され、対応する割合がパーセントで表示されます。

- 図

  値 = 特定の検索条件に一致したメッセージ件数 ÷ あらゆる検索条件に一致したメッセージ件数

  例 :

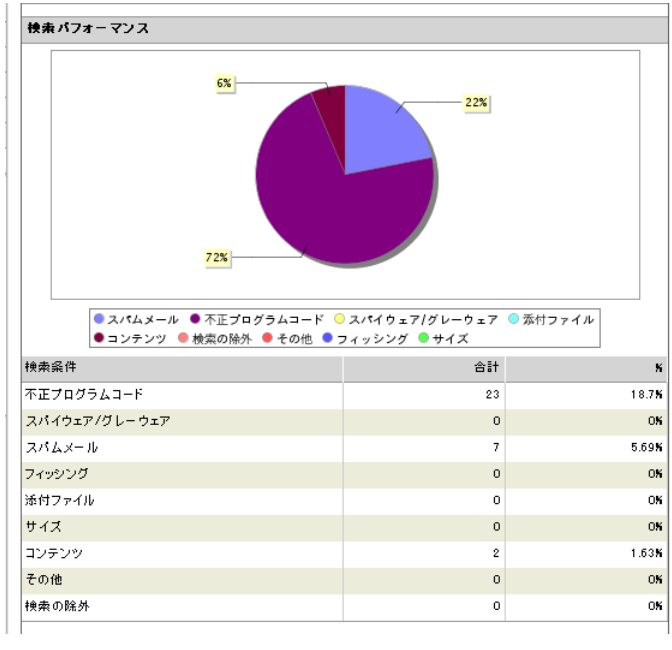
  スパムメールメッセージの割合 : 71% = 66 / 93

- 表

  値 = 特定の検索条件に一致したメッセージ件数 ÷ 処理されたメッセージ合計件数

  例 :

  スパムメールメッセージの割合 : 22% = 66 / 300



検索条件	合計	%
不正プログラムコード	23	18.7%
スパイウェア/グレーウェア	0	0%
スパムメール	7	5.69%
フィッシング	0	0%
添付ファイル	0	0%
サイズ	0	0%
コンテンツ	2	1.63%
その他	0	0%
検索の除外	0	0%

IP フィルタパフォーマンス

本セクションでは、次の理由でブロックされた接続数を表示します。

- 4 種類の IP フィルタルール (スパムメール、ウイルス、DHA 攻撃、およびバウンスメール攻撃)
- 手動で入力された IP アドレス
- NRS

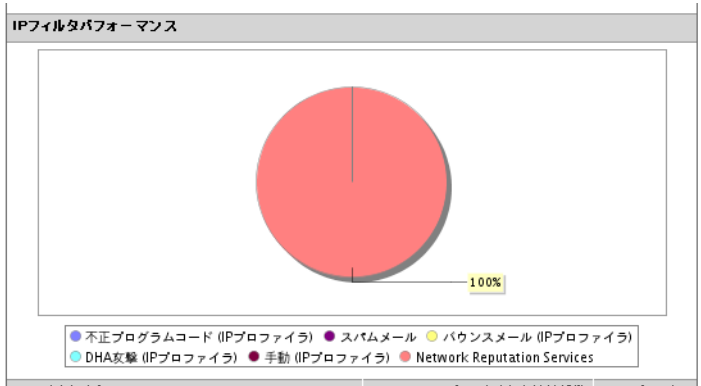
グラフおよび表で表示される値は、次のように算出されます。

値 = 特定の IP フィルタに一致したメッセージ件数 ÷ IP プロファイラまたは NRS によってブロックされたメッセージ合計件数

例 :

IP フィルタおよび NRS によってブロックされたメッセージ合計件数 = 360

スパムメールメッセージの割合 : 22% = 80 / 360



IPフィルタタイプ	ブロックされた接続総数	ブロック %
合計	81	100%
スパムメール (IPプロファイラ)	0	0%
不正プログラムコード (IPプロファイラ)	0	0%
DHA攻撃 (IPプロファイラ)	0	0%
バウンスメール (IPプロファイラ)	0	0%
手動 (IPプロファイラ)	0	0%
Network Reputation Services	81	100%

レポートを作成する

必要に応じて、1 回限りのレポートの作成、または指定した間隔で実行する予約レポートを選択できます。InterScan MSS では、レポートごとに柔軟に内容を指定でき、HTML または CSV 形式で結果を表示または保存するオプションを提供しています。

レポート内容の種類

レポートに記載する内容の種類を次の中から選択できます。

レポート内容	説明
ポリシーとトラフィックの概要	受信および送信メッセージの合計件数と合計サイズを表示します。また、特定の検索条件に一致したメッセージ数も表示します。
ウイルスと不正プログラムコードの概要	処理ごとにウイルスメッセージ件数の概要を示します。
スパムメールの概要	スパムメール検索エンジン、NRS、IP プロファイラおよび処理ごとにスパムメール合計件数の概要を表示します。
送信者 IP アドレスのブロックの概要	「IP プロファイルによるブロックの概要」および「NRS によるブロックの概要」が含まれます。前者は、IP プロファイラに到達し、他の IP フィルタルールによってブロックされた送信者接続合計数の概要を表示します。後者は、NRS に到達し、NRS によってブロックされた送信者接続合計数を表示します。
トップ 10 のトラフィックのメールアドレス	送信および受信メッセージ数でトップ 10 のメールアドレスを表示します。
トップ 10 の感染ウイルス名	ウイルス検出数で、トップ 10 の感染ウイルス名を表示します。
トップ 10 の DHA 攻撃アドレスの IP アドレス	DHA 攻撃によるブロック数で、トップ 10 の IP アドレスを表示します。

表 4-1.　レポート内容の説明

レポート内容	説明
トップ 10 のバウンスメール攻撃アドレスの IP アドレス	バウンスメール攻撃によるブロック数で、トップ 10 の IP アドレスを表示します。
トップ 10 のウイルス受信者と送信者	受信および送信ウイルスメッセージ合計件数で、トップ 10 のウイルス受信者および送信者をそれぞれ表示します。
トップ 10 の最も頻繁に一致したルール名	ルールに一致したメール件数で、トップ 10 のルール名を表示します。
トップ 10 のスパムメール受信者	受信スパムメールの合計件数で、トップ 10 のスパムメール受信者アドレスを表示します。
NRS によってブロックされたトップ 10 の IP アドレス	NRS によって切断された接続数で、トップ 10 のブロックされた IP アドレス。
スパムメール送信元としてブロックされたトップ 10 の IP アドレス	スパムメール送信元としてブロックされた数で、トップ 10 の IP アドレス。
ウイルスまたは不正コードの送信元としてブロックされたトップ 10 の IP アドレス	ウイルスの送信元としてブロックされた数で、トップ 10 の IP アドレス。

表 4-1.　レポート内容の説明

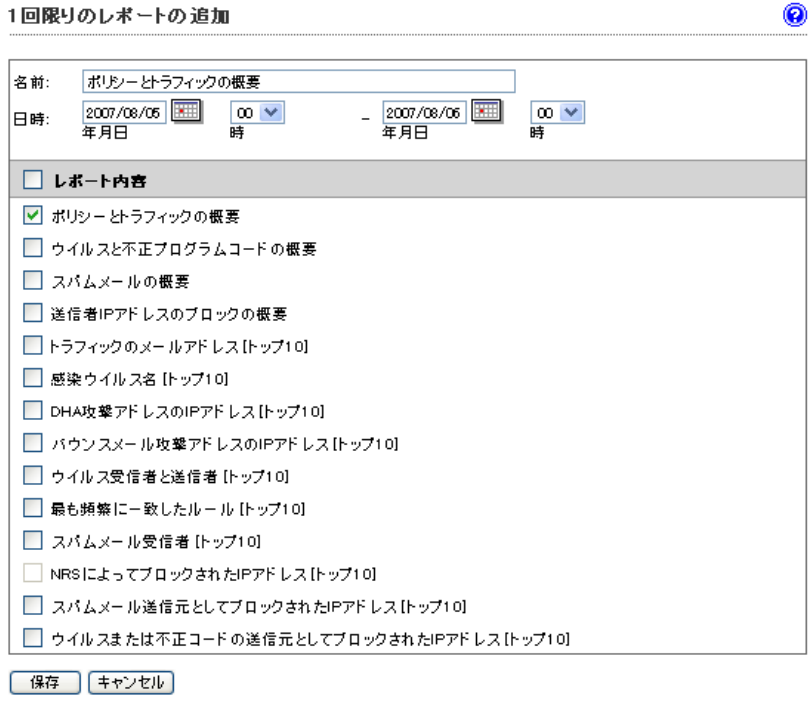
1 回限りのレポートを追加する

必要に応じて 1 回限りのレポートを作成すると、ネットワークのトラフィックを監視するのに役立ちます。

1 回限りのレポートを作成するには

1. メニューから、[レポート]→[1 回限りのレポート] の順に選択します。

2. [追加] をクリックします。



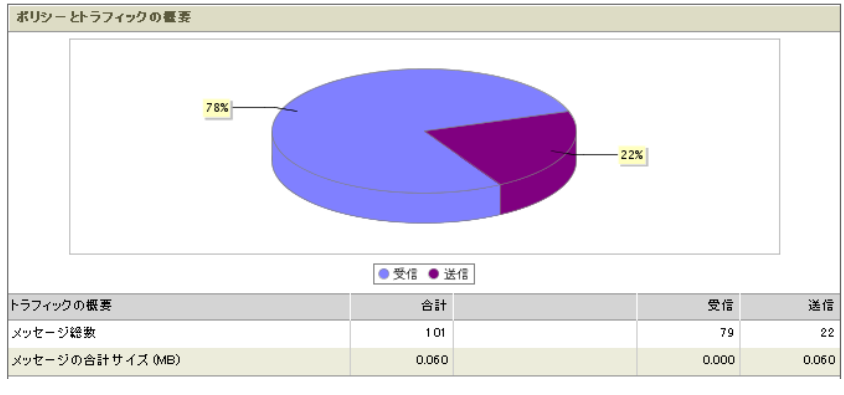
3. 必要な情報を指定します。

4. [保存] をクリックします。レポートの作成に数分かかります。レポートテーブルに、「処理中」というメッセージが表示されます。

レポート作成後に、ハイパーリンク [HTML] および [CSV] がレポートテーブルに表示されます。

5. レポートを HTML 形式で表示するには、[HTML] をクリックします。

6. データを csv ファイルにエクスポートするには、[CSV] をクリックします。



注意： レポートの作成は 1 回に 5 分かかります。レポート作成の所要時間は、レポートデータの収集や必要な計算を行った上にさらに 5 分程度かかる場合があります。

予約レポートを設定する

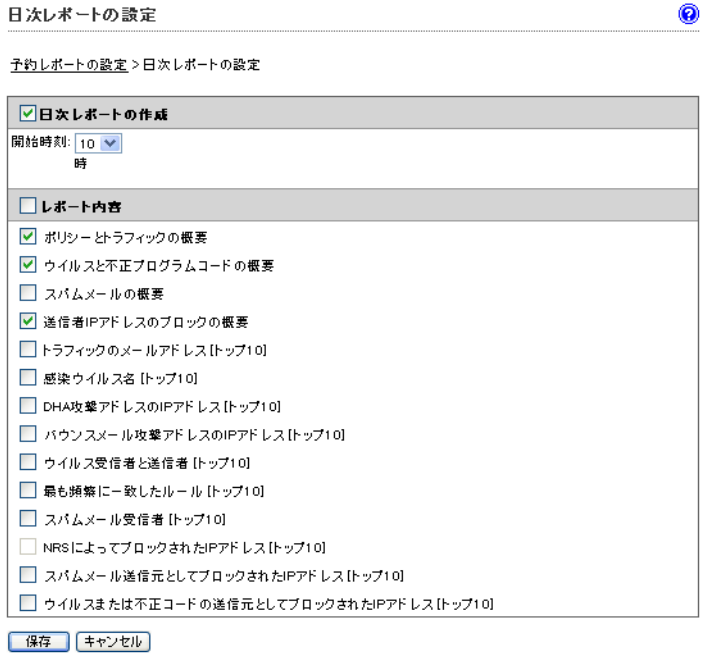
指定した間隔に従って予約レポートが自動的に作成されます。

予約レポートを作成するには

1. メニューから、[レポート]→[設定] の順に選択します。[予約レポートの設定] 画面が表示されます。

2. 次のいずれかのレポートの種類から [設定] リンクをクリックします。
   - 日次レポート
   - 週次レポート
   - 月次レポート

   [レポート設定] 画面が表示されます。



3. レポートの設定を指定します。

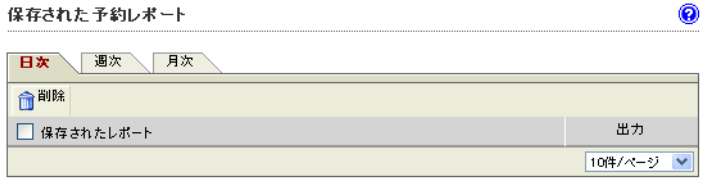
注意： 月次レポートを設定する際、レポートの作成日に 29 日、30 日、または 31 日を選択した場合、InterScan MSS では、月の日数に合わせた月末にレポートが作成されます。たとえば、レポートの作成日を 31 日と選択した場合、InterScan MSS では、2 月には 28 日 (または 29 日)、4 月、6 月、9 月および 11 月には 30 日にレポートが作成されます。

4. [保存] をクリックします。レポートのステータスが変更されます。

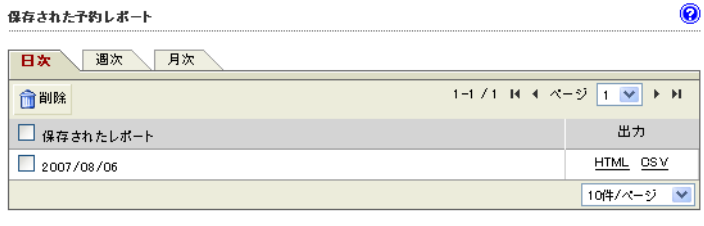
5. 保存する数をレポートの種類ごとに指定します。[保存] をクリックします。

6. メニューから、[レポート]→[予約レポート] の順に選択します。[予約レポート] 画面が表示されます。

注意： レポートはまだ作成されていません。



7. レポート作成後に、[HTML] または [CSV] をクリックするとレポートを表示できます。



ログ

ログは、さまざまな種類のイベントや InterScan MSS 内の情報のフローを監視できる有効な手段です。また、トラブルシューティングの際の重要な情報源となります。

ログを有効にして情報を活用するには

手順 1: ログを設定します。詳細については、103 ページの「ログを設定する」を参照してください。

手順 2: ログのクエリを実行します。

ログのクエリを実行する

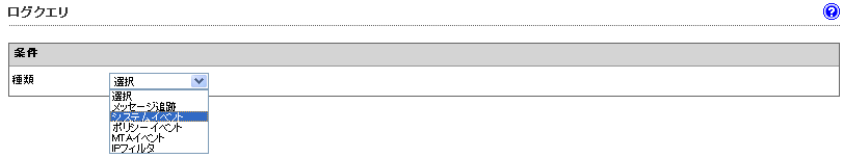
5 種類のイベントまたは情報のクエリを実行できます。

- メッセージ追跡 — 送信者、受信者、メッセージサイズ、および InterScan MSS によって実行された最終的な処理など、メッセージの詳細を記録します。隔離されたメッセージの場合、クエリ結果では、一致したポリシールールの名前および種類が表示されます。
- システムイベント — ユーザアクセス、ルールの変更、Control Manager エージェントの登録など、システムイベントの時間を記録します。
- ポリシーイベント — 一致したポリシールールの詳細、実行された処理、およびメッセージの詳細を記録します。
- MTA ログ — セントラルコントローラがインストールされたローカルコンピュータ上の Postfix の接続詳細を記録します。
- IP フィルタ — クエリ対象 IP アドレスからのメールメッセージのブロックを開始および停止した時間を記録します。

InterScan MSS では、大部分のログのクエリに対して、ワイルドカード (*) と完全一致をサポートしています (たとえば、名前に A または B を含むメール受信者を表示するには、受信者を「*A*;*B*」に設定します)。初期設定では、完全一致が使用されます。検索条件を空欄にしておくと、すべてのログが表示されます。複数条件のアイテムがある場合は、セミコロン (;) を使用して、受信者と添付ファイルのエントリを区切ります。

ログのクエリを実行するには

1. メニューから、[ログ]→[クエリ] の順に選択します。[ログクエリ] 画面が表示されます。
2. [種類] ドロップダウンリストで、クエリするログの種類を選択します。



3. クエリの詳細を指定します。
4. [ログ表示] をクリックします。

隔離とアーカイブ

隔離とアーカイブは、メッセージが特定のルールと一致した際に InterScan MSS が実行するように設定できる処理です。通常、メッセージの隔離設定では、メッセージを解析してから、削除するか、受信者宛に解除するかを判断します。一方で、アーカイブでは参照用にメッセージを保存できます。

注意： エンドユーザメール隔離を使用するには、まず LDAP を設定する必要があります。詳細については、22 ページの「手順 3: LDAP を設定する」を参照してください。

隔離とアーカイブを設定する

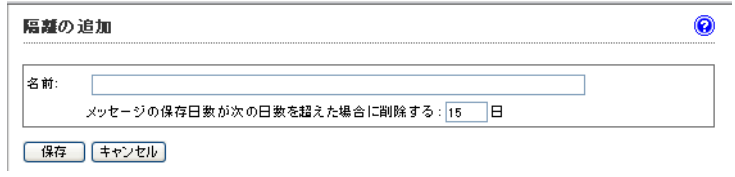
隔離とアーカイブを設定すると、ユーザはそれらの領域を管理し、隔離またはアーカイブされたメッセージの保存用に、検索サービスごとのディスク容量を割り当てることができます。

隔離とアーカイブを設定するには

1. メニューから、[隔離およびアーカイブ]→[設定] の順に選択します。[隔離およびアーカイブの設定] 画面が表示されます。

2. 検索サービスごとにディスク割り当てを指定します。

3. [追加] をクリックします。[隔離の追加] 画面が表示されます。



4. 必要な情報を指定します。

5. [保存] をクリックします。アーカイブを設定するには、[アーカイブ] タブをクリックします。

隔離およびアーカイブされたメッセージのクエリを実行する

隔離またはアーカイブされたメッセージに対して実行される処理の判断が下される前に、クエリを実行できます。メッセージの詳細を表示した後、隔離されたメッセージの場合は InterScan MSS からの解除または削除、アーカイブされたメッセージの場合は削除を選択できます。

隔離されたメールまたはアーカイブされたメールを管理するには

1. メニューから、[隔離およびアーカイブ]→[クエリ] の順に選択します。[隔離およびアーカイブのクエリ] 画面が表示されます。

2. [隔離] タブで、検索条件を指定します。

3. [ログ表示] をクリックします。

4. 結果アイテムのタイムスタンプのリンクをクリックします。アイテムの詳細が [隔離のクエリ] 画面に表示されます。

5. [解除] をクリックすると、メールが隔離から解除され、[削除] をクリックすると、隔離から削除されます。

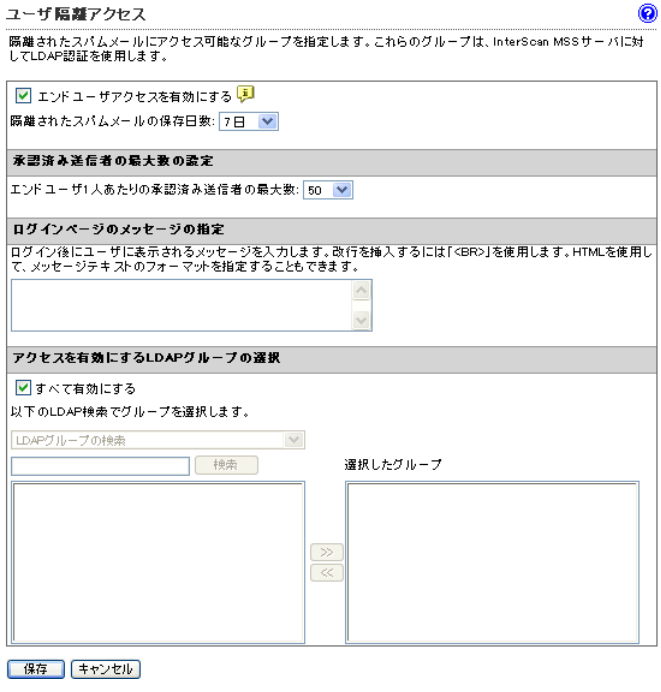
6. アーカイブされたメッセージのクエリを実行するには、[隔離およびアーカイブ] 画面上の [アーカイブ] タブをクリックし、適宜、検索条件を指定します。

ユーザ隔離アクセスを設定する

すべてのユーザまたは選択されたエンドユーザに、エンドユーザメール隔離管理コンソールへのアクセス権を付与できます。アクセス権を付与されたユーザは、https://< **対象サーバの IP アドレス** >:8447 にアクセスすることで、そのユーザ宛のスパムメールを管理できます。

ユーザ隔離アクセスを設定するには

1. メニューから [管理]→[ユーザ隔離アクセス] の順に選択します。[ユーザ隔離アクセス] 画面が表示されます。



2. 必要な設定を指定します。
3. [エンドユーザアクセスを有効にする] チェックボックスをオンにして、機能を有効にします。
4. [保存] をクリックします。

エンドユーザメール隔離データベースを追加 / 削除する

既存のエンドユーザメール隔離データベースがある場合、次の項目を実行する際に、新しいエンドユーザメール隔離データベースを追加する場合があります。

- 負荷分散を実行するには
- さらに多くのユーザをエンドユーザメール隔離へアクセスさせるには

また、エンドユーザメール隔離データベースの数を減らすことも可能です。

エンドユーザメール隔離データベースを追加する

エンドユーザメール隔離データベースを追加するには、次の手順を実行します。

手順 1: エンドユーザメール隔離データベースの設定
手順 2: エンドユーザデータの再構築

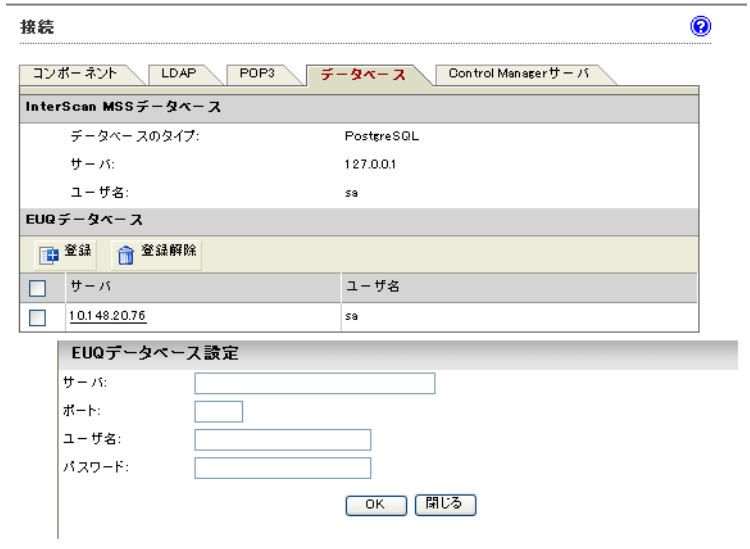
手順 1: エンドユーザメール隔離データベースの設定

エンドユーザメール隔離データベースが既にインストールされていても、まだ登録が完了していない場合は、管理コンソールからこのデータベースを登録できます。それ以外の場合は、InterScan MSS のインストールプログラムを実行して、新しいエンドユーザメール隔離データベースをシステムに追加してください。

エンドユーザメール隔離データベースを登録するには

1. メニューから、[管理]→[InterScan MSS の設定]→[接続] を選択します。初期設定で［コンポーネント］タブが表示されます。
2. ［データベース］タブをクリックします。

3. [登録]ボタンをクリックします。[EUQ データベース設定] 画面が表示されます。



4. 必要な情報を指定します。

5. [OK] をクリックします。

手順 2: エンドユーザデータの再構築

元のエンドユーザのデータをそのまま保持するには、セントラルコントローラの $IMSS_HOME/script ディレクトリから、euqtrans スクリプトを実行し、エンドユーザメール隔離データベースの負荷を再分散します。このスクリプトは以下の操作を実行します。

- 承認済みリストの転送
- 隔離されたメールに関する情報の転送

注意： 新しいエンドユーザメール隔離データベースの追加後、euqtrans スクリプトを実行しない場合、エンドユーザは、以前隔離したメールメッセージの一部にアクセスできない可能性があります。

エンドユーザメール隔離データベースを削除する

エンドユーザメール隔離データベースを削除するには、次の手順を実行します。

手順 1: エンドユーザメール隔離データベースの削除
手順 2: エンドユーザデータの再構築

手順 1: エンドユーザメール隔離データベースの削除

管理コンソールを使用して、システムからエンドユーザメール隔離データベースの登録を解除することはできますが、削除することはできません。データベースの登録を解除するということは、データベースはそのまま残りますが、InterScan MSS により使用されることはなくなるということを意味します。

エンドユーザメール隔離データベースの登録を解除するには

1. メニューから、[管理]→[InterScan MSS の設定]→[接続] を選択します。初期設定で［コンポーネント］タブが表示されます。
2. ［データベース］タブをクリックします。
3. 不要なエンドユーザメール隔離データベースサーバの横のチェックボックスをオンにします。
4. [登録解除] をクリックします。
5. [OK] をクリックして登録解除を確認します。

手順 2: エンドユーザデータの再構築

セントラルコントローラの $IMSS_HOME/script ディレクトリから、euqtrans スクリプトを実行して、承認済み送信者リストと、隔離されたメールメッセージに関する情報をこのデータベースから別のデータベースに移動し、移動先のデータベースの負荷を再分散します。

euqtrans ツールのコマンドラインオプション

euqtrans スクリプトには、以下のコマンドラインオプションがあります。

all — 個々の承認済み送信者リストと、隔離されたメールメッセージに関する情報を、更新後のテーブルおよびデータベースマッピングに基づいて、削除されたデータベースから新しい場所 (データベース) に転送します。

approvedsender — 個々の承認済み送信者リストを、新しいマッピングに基づいて、削除されたデータベースから新しい場所 (データベース) に転送します。

イベント通知

次のカテゴリのイベント発生時には、ユーザ自身または特定のメールユーザに、メールまたは SNMP 通知を送信するように設定できます。

- システムステータス — ある InterScan MSS のパフォーマンスが要求レベルを下回った場合に通知します。たとえば、検索サービスの動作が停止した場合、または配信キュー内のメッセージ数が指定値を超えた場合です。
- 予約アップデートイベント — 管理データベースに対して、InterScan MSS による検索エンジンまたはパターンファイルの予約アップデートがアップデート元から実行できる場合、または実行できない場合に通知します。

- 検索サービスアップデート結果 — 任意の検索サービスに対して、InterScan MSS による検索エンジンまたはパターンファイルのアップデートができない場合に通知します。

注意： コンポーネントのアップデート手順は 2 つです。
1. 予約時間に、InterScan MSS 管理データベースがまずアップデート元に新しい検索エンジンまたはパターンファイルがないかどうかをチェックします。
2. その後、InterScan MSS 検索サービスが、コンポーネントのアップデートがないどうか一定の間隔で管理データベースをチェックします。初期設定の間隔は 3 分です。

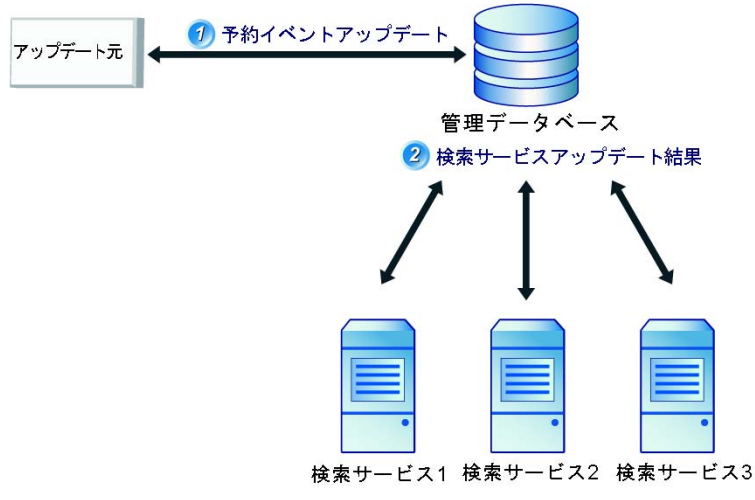


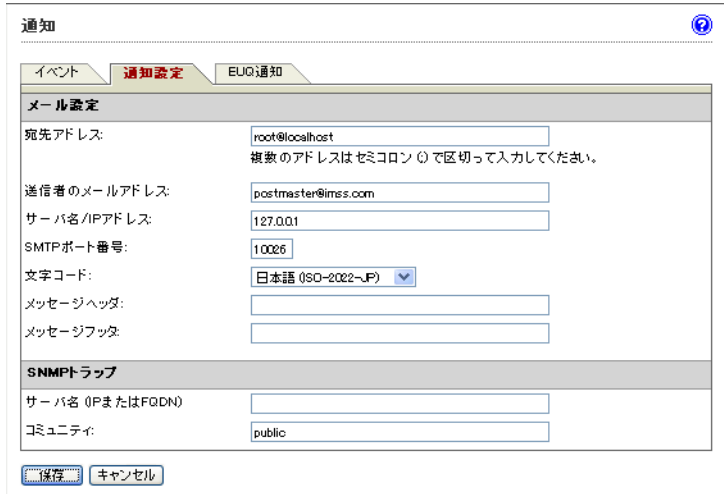
図 4-1. 検索エンジンおよびパターンファイルのアップデート

通知を設定する

通知を設定すると、イベントが発生した際に通知メッセージを配信する必要のある、送信者、受信者、およびその他の設定を指定できます。

通知を設定するには

1. メニューから [管理]→[通知] を選択します。初期設定で［イベント］タブが表示されます。
2. ［通知設定］タブをクリックします。



3. 必要な情報を指定します。
4. [保存] をクリックします。

イベント条件および通知メッセージを設定する

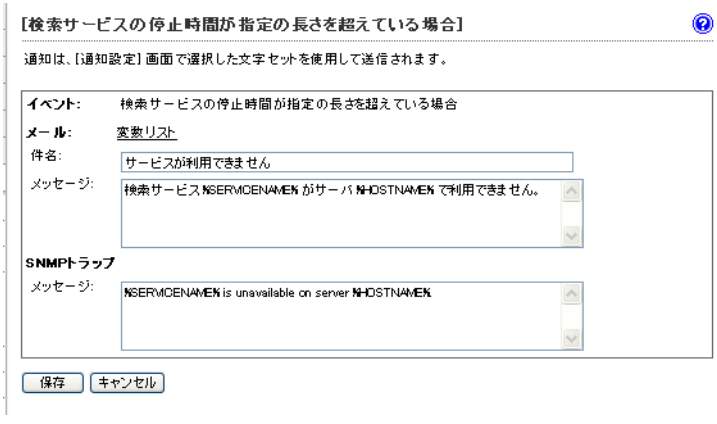
InterScan MSS により通知メッセージが送信される際の条件を設定し、イベントごとにメッセージの内容をカスタマイズできます。

条件およびメッセージ内容を設定するには

1. メニューから [管理]→[通知] を選択します。初期設定で［イベント］タブが表示されます。

2. [システムステータス] セクションで、必要な条件を指定します。
3. 希望する通知の受信方法に従って、[メール]、[SNMP]、または両方のチェックボックスをオンにします。

4. メッセージの内容をカスタマイズするには、特定のイベントのハイパーリンクをクリックします。メッセージの編集画面が表示されます。



5. 必要な情報を入力します。

6. [保存] をクリックします。

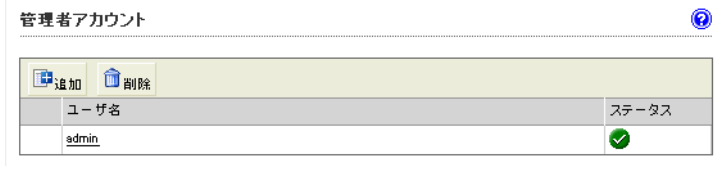
管理者アカウントの管理

InterScan MSS 管理上のボトルネックを減らすために、新しく管理者アカウントを作成し、管理コンソールのさまざまな領域への権限を割り当てることによって、管理タスクを他のスタッフに委任できます。

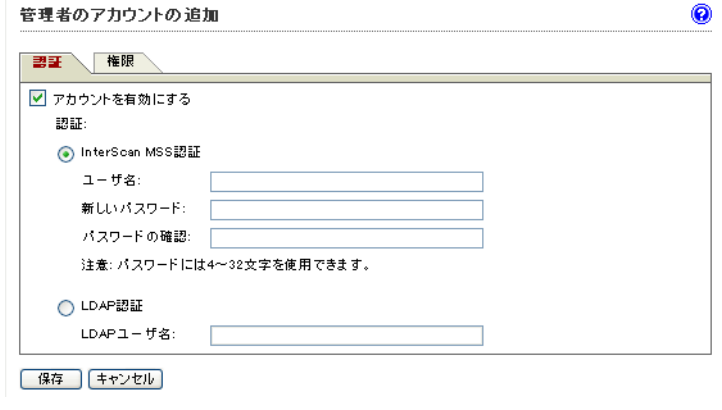
管理者アカウントを追加する

管理者アカウントを追加するには

1. メニューから [管理]→[管理者アカウント] を選択します。[管理者アカウント] 画面が表示されます。

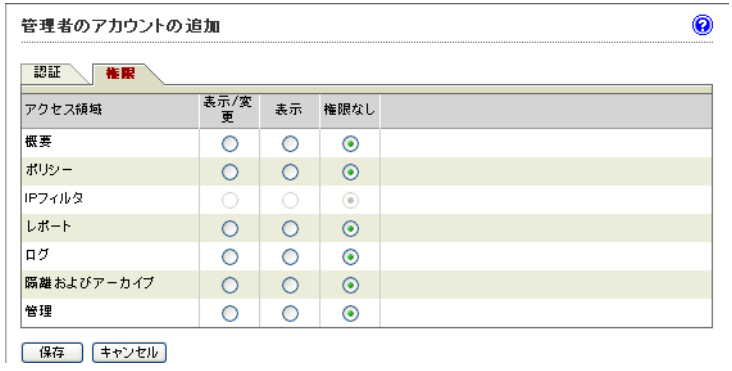


2. [追加] をクリックします。[管理者アカウント] 画面が表示されます。



3. [認証] タブに必要な情報を指定します。

4. ［権限］タブをクリックします。[権限] 画面が表示されます。



5. 管理コンソールのさまざまな領域へアクセスするのに必要な権限を選択します。

6. [保存] をクリックします。

注意： 1. 初期設定の InterScan MSS 管理者アカウントのみが新規管理者アカウントを追加できます。委任管理者アカウントは、管理領域へのフル権限を割り当てられても、新規管理者アカウントを追加することはできません。

2. フル権限を与えられた委任管理者アカウントは、各自の InterScan MSS パスワードを変更できるだけです。初期設定の管理者アカウントのパスワードを忘れた場合、トレンドマイクロのテクニカルサポートへ連絡してパスワードを再設定してください。

管理者アカウントを編集または削除する

ロールが変更になった場合やその他の組織変更があった場合、委任の権限を変更または削除できます。

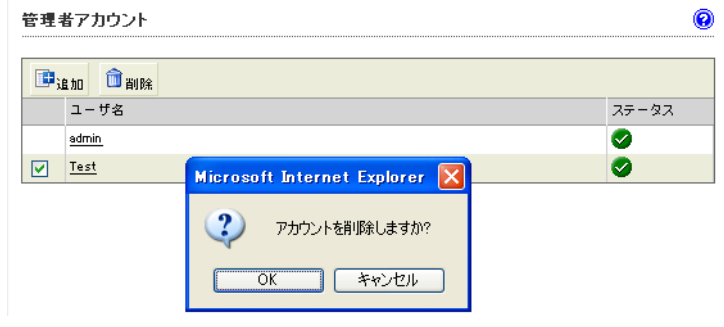
管理者アカウントを編集するには

1. メニューから [管理]→[管理者アカウント] を選択します。[管理者アカウント] 画面が表示されます。

2. 管理者アカウントを編集するには、アカウント名のハイパーリンクをクリックします。
3. 必要な変更を実行します。
4. [保存] をクリックします。

管理者アカウントを削除するには

1. 管理者アカウントを削除するには、削除対象のアカウントの横のチェックボックスをオンにします。
2. [削除] をクリックします。
3. [OK] をクリックして削除を確認するか、または [キャンセル] をクリックして作業を中止します。



注意： 委任管理者アカウントのみ削除または委任でき、初期設定の InterScan MSS 管理者アカウントを削除または委任できません。

検索サービスおよびポリシー接続の設定

検索サービスを有効にしてメッセージを受信し、ポリシーサービスによるルール検索のパフォーマンスを向上させるには、接続設定を行います。

検索サービスおよびポリシー接続を設定するには

1. メニューから、[管理]→[InterScan MSS の設定]→[接続] を選択します。初期設定で［コンポーネント］タブが表示されます。

2. 必要な設定を指定します。
3. [保存] をクリックします。

第 5 章

トラブルシューティングとサポート情報

この章では、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) の一般的な問題のトラブルシューティング、トレンドマイクロの製品 Q&A の検索、およびトレンドマイクロサポートへの問い合わせの方法について説明します。

この章の内容は次のとおりです。

- 148 ページの「トラブルシューティング」
- 156 ページの「よくある質問 (Q&A)」
- 175 ページの「製品サポート情報」
- 175 ページの「サポートサービスについて」

トラブルシューティング

表 5-1 に、InterScan MSS の設定および管理で発生する可能性のある問題の一般的なトラブルシューティングの方法を示します。解決策についても、この表を参照してください。この表を見ても問題が解決しない場合は、トレンドマイクロの製品 Q&A を確認してください。

InterScan MSS の配置に関するトラブルシューティングについては、InterScan MSS の「インストールガイド」を参照してください。

問題	推奨される解決策
一般的な問題	
管理コンソールまたはその他のコンポーネントにアクセスできない	ターゲットポートがファイアウォール承認済みリストに存在していません。ファイアウォールで 155 ページの表 5-2 に示されるポートを開きます。 管理コンソールにアクセスできない場合は、次の操作を実行してください。 **1. セントラルコントローラプロセス S99ADMINUI を開始する前に、データベースプロセス dbctl.sh を開始します。** **2. それでも管理コンソールにアクセスできない場合は、セントラルコントローラプロセス S99ADMINUI を再起動します。** 詳細については、180 ページの「InterScan MSS スクリプトの実行」を参照してください。
管理コンソールへのアクセスが行われない	管理コンソールの URL が、Internet Explorer で信頼されたサイトではありません。URL を信頼されたサイトに追加します。
imssps デーモンは実行中だが、接続を拒否する	imssps デーモンが実行中の場合、ポリシーサービスが機能しています。ポリシーサービスと検索サービス間の接続を確認して、LDAP 設定を確認してください。

表 5-1. 問題のトラブルシューティング

問題	推奨される解決策
製品 (InterScan MSS、スパムメール対策、IP フィルタ) を起動できない、またはコンポーネントをアップデートできない	ネットワークにプロキシサーバが使用されている場合は、プロキシ設定を確認してください。 Trend Micro Network Reputation Services (以下、NRS) を起動するには、InterScan MSS をトレンドマイクロに接続する必要があります。この処理には、DNS クエリが必要です。したがって、DNS サーバが使用できなかったり、接続に問題がある場合は、起動に失敗します。 DNS サーバの設定を確認してください。 管理コンソールから DNS の設定を確認するには **1. メニューから [管理] → [アップデート] の順に選択します。初期設定では [スケジュール] タブが表示されます。** **2. [アップデート元] タブをクリックします。** **3. プロキシを設定します。** **4. [保存] をクリックします。**
メール通知が正しく表示されない	通知メッセージに ASCII 以外の文字を使用している場合、通知メッセージの文字コードが正しく設定されていないと文字化けする場合があります。管理コンソールで、適切な文字コードを設定してください。 **文字セットを変更するには** **1. 管理コンソールメニューから、[管理] → [通知] → [通知設定] の順に選択します。** **2. [文字コード] の横から、メッセージをエンコードする際の言語を選択します。**
InterScan MSS でメッセージログをクエリできない	InterScan MSS 検索サービスでは、ログをローカル時刻で記録します。メッセージログをクエリするには、すべてのコンピュータの日時を InterScan MSS と同期させます。
[概要] 画面でサーバが切断されていると表示される	管理対象サーバは、次のいずれかの理由で切断される場合があります。 • **検索サービスがネットワークから削除されていた。** • **InterScan MSS マネージャサービスが停止していた。** • **ネットワーク接続の問題。** マネージャサービス待機ポートのファイアウォール設定を確認します。[管理]→[InterScan MSS の設定]→[接続]→[コンポーネント]→[InterScan MSS マネージャポート] の順にクリックします。

表 5-1.　問題のトラブルシューティング

問題	推奨される解決策
隔離されたメールまたはアーカイブされたメールの詳細な情報を表示する場合は、添付ファイルの情報を利用できないことがある	起動されたルールが添付ファイルに関するものであった場合にのみ、InterScan MSS では添付ファイル情報が記録されます。InterScan MSS でメールが隔離された理由を確認してください。
InterScan MSS でメールが受信されない	**1. InterScan MSS 検索サービスが実行中であるかどうか確認します。** **2. 別のアプリケーションが、必要なポートを使用しているかどうか確認します。ポート 25 を解放します。**
サービスが通常通り実行されない	データベースが起動していないか、または InterScan MSS サービスが起動した後でデータベースが起動しました。すべての InterScan MSS サービスを再起動します。
エンドユーザメール隔離の問題	
エンドユーザメール隔離管理コンソールにアクセスできない	次の項目を実行してください。 **1. 正しい URL とポート番号を使用していることを確認します。** ネットワーク上の他のコンピュータからエンドユーザメール隔離管理コンソールを表示するには、次の URL にアクセスします。 **・ プライマリエンドユーザメール隔離サービス - https://<サーバ IP アドレス >:8447** **・ セカンダリエンドユーザメール隔離サービス - https://<サーバ IP アドレス >:8446** **2. ネットワーク上の各エンドユーザメール隔離サービスのシステム時間が同期されていることを確認します。** エンドユーザメール隔離サービスの最初のインスタンスである、プライマリエンドユーザメール隔離サービスは、ポート 8447 (HTTPS) を待機中に Apache Web Server (httpd) を実行します。 この Web Server は、エンドユーザメール隔離クライアントおよびすべてのエンドユーザメール隔離サービスの負荷分散のための接続ポイントとして機能します。 Apache サーバがダウンしている場合、ユーザは、通常の IP アドレス (https://{ プライマリエンドユーザメール隔離サービスの IP アドレス }:8447/) からエンドユーザメール隔離コンソールにアクセスできなくなります。

表 5-1. 問題のトラブルシューティング

問題	推奨される解決策
ユーザがエンドユーザメール隔離管理コンソールにログインできない	次の項目を実行してください。 **1.** LDAP サーバで、ユーザアカウントが適切なグループにあることを確認してください。承認済みグループのユーザアカウントのみが、エンドユーザメール隔離にアクセスできます。 **2.** LDAP とユーザメール隔離アクセスの設定を InterScan MSS 管理コンソールで確認してください。 **a.** メニューから、[管理] → [InterScan MSS の設定] → [接続] → [LDAP] を選択します。 **b.** すべての設定内容、特に LDAP の種類とサーバ情報を確認してください。Kerberos 認証を使用している場合、すべての InterScan MSS コンピュータと LDAP サーバの時間が同期していることを確認してください。 **c.** メニューから [管理] → [ユーザ隔離アクセス] の順に選択します。 **d.** [ユーザ隔離アクセス] を有効にします。 **e.** 適切な LDAP グループが [選択したグループ] の下に表示されており、ユーザアカウントが選択したグループに属していることを確認します。 **3.** ユーザが適切なログイン名とパスワードを使用していることを確認します。詳細については、31 ページの「ログオン名形式」を参照してください。 **4.** 上記の設定を確認しても問題が解決しない場合は、次の操作を実行してください。 **a.** メニューから、[ログ] → [設定] の順に選択します。 **b.** アプリケーションログのレベルを [デバッグ] に設定します。 **c.** メニューから [管理] を選択します。[システム] タブから、エンドユーザメール隔離サービスを再起動します。 **d.** エンドユーザメール隔離管理コンソールに再度ログインするようユーザに要求します。 **e.** /opt/trend/imss/logs にあるログファイル imssuieuq.yyyymmdd をトレンドマイクロサポートに送信します。
エンドユーザメール隔離通知が隔離されたメールの情報を正しく表示しない	文字セットが適切であることを確認してください。 **1.** [管理] → [通知] → [通知設定] の順に選択します。 **2.** [文字コード] の横から、通知情報を適切に表示する文字セットを選択します。

表 5-1.　問題のトラブルシューティング

問題	推奨される解決策
隔離されたメールメッセージの一部がエンドユーザメール隔離管理コンソールに表示されない	エンドユーザメール隔離管理コンソールからアクセスできるのは、InterScan MSS がスパムメールまたはフィッシングメールと判定したメールのみです。 エンドユーザメール隔離管理コンソールでは、ウイルス対策ルールなどルールに違反した隔離メールを表示できません。
Kerberos 認証で LDAP を有効にできない	Kerberos プロトコルでは、Kerberos サーバと InterScan MSS の間で時間を同期させる必要があります。 すべてのコンピュータの日時を InterScan MSS と同期させます。
IP フィルタの問題	
FoxProxy が起動しない	FoxProxy が起動しない理由は、複数あります。理由を調べるには、IP プロファイラのログを表示します。 **IP プロファイラのログを表示するには** **1.** IP プロファイラの設定ファイルがあるディレクトリに移動します (初期設定 :/opt/trend)。 **2.** foxproxy.ini を開きます。 **3.** log_level の値を 4 に変更します。 **4.** FoxProxy を再起動するには、次のように入力します。 /opt/trend/ipprofiler/script/foxproxyd restart **5.** ログファイルを開くには、次のように入力します。 /opt/trend/ipprofiler/logs/foxproxy-general.****
FoxProxy に接続できない	FoxProxy が稼働中で、ポート 25 にバインドしていることを確認します。
FoxProxy のメールメッセージの処理が遅い	FoxProxy がメールを受信すると、FoxDNS で DNS クエリを実行します。BIND サービスが稼働していない場合、FoxProxy は DNS クエリがタイムアウトになるまで待機し続けます。 **FoxDNS がインストールされているコンピュータで BIND サービスが稼働していることを確認** **1.** 次のコマンドを入力します。 ps -ef | grep named **2.** サービスが稼働していない場合は、起動します。

表 5-1.　問題のトラブルシューティング

問題	推奨される解決策
FoxProxy がブロックしている接続を表示できない	5 分ごとに、FoxProxy はブロックされた接続に関する情報を InterScan MSS サーバに送信します。 接続情報が表示されるまで、少なくとも 5 分間待機してください。 **この時間の値を変更するには** **1.** foxproxy.ini を開きます。 **2.** report_send_interval の値を変更します。
FoxDNS が機能しない	**BIND サービスが稼動していることを確認** **1.** 次のコマンドを入力します。 ps -ef | grep named **2.** サービスが稼働していない場合は、起動します。
IP プロファイラのログ情報がまったくない	次の IP プロファイラ関連のログファイルは、InterScan MSS 管理データベースにあります。 • foxmsg.**** • foxnullmsg.**** • foxreport.**** **次の手順で、ログファイルが存在することを確認** **1.** InterScan MSS がインストールされているコンピュータ上の log ディレクトリに移動します (初期設定 :/opt/trend/imss/log/)。 **2.** ファイルが存在しない場合、次のコマンドを使用して、InterScan マネージャが稼働しているかどうかを確認します。 ps -ef | grep imssmgr **3.** 次のコマンドで、FoxProxy が稼働しているかどうかを確認します。 ps -ef |grep foxproxy **4.** IP プロファイラが有効になっていることを確認します。 InterScan MSS データベースの「t_foxhuntersetting」テーブル内で、次のように表示されている必要があります。 record:`Type' = 1 and 'enable' = TRUE

表 5-1.　問題のトラブルシューティング

問題	推奨される解決策
管理コンソールから NRS を有効にした後で、NRS が機能しない	NRS が機能しない理由として、次の可能性が考えられます。 • **スパムメール対策が有効になっていません。NRS はスパムメール対策と同じアクティベーションコードを共有しています。スパムメール対策が有効になっていない場合は、スパムメール対策を有効にしてから NRS を有効にします。** • **検索サービスがインストールされているコンピュータは、インターネットにアクセスできません。MTA はアクティベーションコードの検証に関する DNS クエリの応答を取得できません。検索サービスをインストールしているコンピュータが、インターネットへアクセスできることを確認してください。** スパムメール対策を有効にして、スパムメール対策をインストールしているコンピュータが、インターネットへアクセスできることを確認してください。
管理コンソールの [SMTP ルーティング] 画面上の MTA 設定が Postfix 設定ファイルに書き込まれない	初期設定では、[SMTP ルーティング] 画面の設定では Postfix に書き込まれません。次の手順に従って、この機能を有効にします。 InterScan MSS 設定ディレクトリに移動します (初期設定 :/opt/trend/imss/config)。 InterScan MSS 設定ファイル imss.ini を開きます。 enable_postset_thd の値を [yes] に変更するか、空欄のままにします。 次のコマンドを使用して、InterScan MSS マネージャを再起動します。 /opt/trend/imss/script/S99MANAGER restart
IP プロファイラがブロックリストの IP アドレスをブロックしない	変更が有効になるまで 1 分ほどかかります。 1 分お待ちください。
ブロックされた IP アドレスが [概要] ページに表示されない	[概要] ページには、過去 24 時間の上位 10 のブロックされた IP アドレスが種類別に表示されます。たとえば、本日の 16:12 時点では、[概要] ページには、昨日の 16:00 から本日の 16:00 までのデータが表示されます。 1 時間後に [概要] ページを表示してください。

表 5-1.　問題のトラブルシューティング

モジュール	ポート	説明
Admin UI	8445	Tomcat 待機ポート (HTTPS)
Bind	53	ネームドメインサーバ
EUQ UI	8009	Tomcat AJP (負荷分散) ポート
EUQ UI	8446	Tomcat 待機ポート
EUQ UI	8447	負荷分散用
マネージャ	15505	SOAP サーバ
MTA	25	SMTP
MTA	465	SSMTP (SSL)
ポリシーサーバ	5060	SOAP 待機ポート
検索サービス	10024	POP3 待機ポート

表 5-2. コンポーネントで使用されるポート

よくある質問 (Q&A)

Postfix MTA 設定

Postfix に複数の検索サービスを配置した場合、これらの Postfix インスタンスを一元管理する方法はありますか。一部の Postfix インスタンスの設定を個別に例外とすることはできますか。

管理コンソールからすべての Postfix コンピュータを制御する場合は、[すべての検索サービスに適用] オプションを有効にする必要があります。メニューから、[管理] →[SMTP ルーティング]→[SMTP] の順に選択します。

一部の Postfix 設定に例外を設ける場合は、imss.ini で detach_key_postfix キーを検索し、管理コンソールから適用しないキーを追加できます。例 :

detach_key_postfix=smtpd_use_tls:smtpd_enforce_tls:queue_directory

管理コンソールを使用せずに MTA 設定を変更するにはどうしたらいいですか。

InterScan MSS 設定ファイルを変更して、次のキーを追加します。

1. imss.ini を開きます。
2. 次の変更を実行します。

```
detach_key_postfix=smtpd_use_tls:queue_directory:{Parameter1:{Parameter2}:::{Parameter n}
```

上記のパラメータは、管理コンソールを介して実行された設定によって上書きされることはありません。main.cf を手動で変更します。

注意 : {Parameter1:{Parameter2}:::{Parameter n} は、コロンを使用してパラメータを区切ることによって、1 つ以上のパラメータを使用できることを意味します。

警告 : 設定ファイルを変更する際は、十分に注意してください。

InterScan MSS コンポーネント

セントラルコントローラをあるコンピュータから別のコンピュータへ移動できますか。

はい。まず、InterScan MSS インストールスクリプトを実行して、セントラルコントローラをコンピュータからアンインストールします。次に、InterScan MSS インストールスクリプトを実行して、セントラルコントローラを別のコンピュータにインストールします。

どのようにデータベースを設定、管理できますか？

以下のコマンドを使用して、データベースを管理できます。

- pg_dump imss > YYMMDD.HHMMSS.backup : データベースをバックアップします。
- psql imss < YYMMDD.HHMMSS.backup : エラーが発生した場合に、最新のデータを取り出します。
- vacuum : 頻繁にアクセスされるテーブルまたは大量のデータがあるテーブル上のデータベースをクリーンナップします。メールトラフィックが小さい、またはデバイスがネットワークに接続されていないときに使用します。
- vacuumfull : データベースの使用頻度が高くない、またはデバイスがネットワークに接続されていないときに、データベース全体をクリーンナップします。
- redirect_stderr= and log_rotate_***= : 古いデータベースログエントリをシステムログにリダイレクトする場合は、postgresql.conf でこれらのオプションを有効にします。ログファイルにダッシュ「-」で始まる名前を付けることができます。

IP フィルタやその他のログデータは SQL を使用して削除することもできます。また、管理コンソールの [ログ]→[設定] 画面でログの保存期間を設定できます。

LDAP がダウンしている場合、InterScan MSS ポリシーサービスは機能しますか。

はい、ポリシーサービスは、LDAP サーバがダウンしていても機能します。

次にそのような 3 つの例を示します。

- InterScan MSS は通常通り機能し続けます。

- LDAP サーバは起動しているが、LDAP サーバのポートにアクセスできない場合。
- ポリシーサーバに LDAP ユーザまたはグループの期限切れでないキャッシュがある場合。

- ポリシーサーバが LDAP 関連のルールを無視し、他のルールの処理を続行します。
  - LDAP サーバは起動しているが、LDAP サーバのポートにアクセスできない場合。
  - ポリシーサーバにルールの有効なキャッシュがない場合。
- InterScan MSS では、各ルールのクエリを約 1 分実行します。これにより、メッセージの検索処理が遅くなり、メールキューが長くなる場合があります。
  - LDAP サーバがダウンしている場合。
  - ポリシーサーバにルールの有効なキャッシュがない場合。

NRS

特定の IP アドレスまたはドメインをブロックしないようにするには、NRS をどのように設定するのですか。

IP アドレスまたはドメインを NRS の承認済みリストに追加します。追加の手順は、次のとおりです。

- 管理コンソールにログオンします。
- [IP フィルタ]→[承認済みリスト] の順にクリックします。
- ブロックしない IP アドレスまたはドメインを承認済みリストに追加します。

NRS のアクティベーションコードを入力するには、どうしたらいいですか。

インストール中にアクティベーションコードを入力するか、インストール後にアクティベーションコードを変更します。
アクティベーションコードを変更するには、NRS と同じコンピュータにある Postfix 設定ファイルを編集します。これらのファイルは、main.cf、imss_rbl_reply、および imss_rbl_reply.user です。

注意： imss_rbl_reply.user ファイルは存在しない場合があります。存在する場合は変更してください。存在しない場合は、ファイルの変更を省略します。

NRS をインストールした後、3 つの設定ファイル内に同様のコンテンツが次のように設定されます。

- **main.cf**

  smtpd_client_restrictions = reject_rbl_client APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.r.mail-abuse.com,reject_rbl_client APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.q.mail-abuse.com

- **imss_rbl_reply**

  APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.q.mail-abuse.com 450 Service temporarily unavailable; $rbl_class [$rbl_what] blocked using Trend Micro Network Reputation Service.Please see http://www.mail-abuse.com/cgi-bin/lookup?ip_address=rbl_what{rbl_reason?; $rbl_reason}

  APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.r.mail-abuse.com 550 Service unavailable; $rbl_class [$rbl_what] blocked using Trend Micro RBL+.Please see http://www.mail-abuse.com/cgi-bin/lookup?ip_address=rbl_what{rbl_reason?; $rbl_reason}

- **imss_rbl_reply.user**

  APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.q.mail-abuse.com 450 error message; $rbl_class [$rbl_what] blocked using Trend Micro Network Reputation Service.Please see http://www.mail-abuse.com/cgi-bin/lookup?ip_address=rbl_what{rbl_reason?; $rbl_reason}

"APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.r.mail-abuse.com 450 error message; $rbl_class [$rbl_what] blocked using Trend Micro RBL+.Please see http://www.mail-abuse.com/cgi-bin/lookup?ip_address=rbl_what{rbl_reason?; $rbl_reason}

これらの 3 つのファイルで、古いアクティベーションコードを新しいアクティベーションコードに置き換えます。上記の例で示されている古いアクティベーションコードは、APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R です。

注意： アクティベーションコードには、ダッシュ (-) を入力する必要はありません。

設定ファイルを編集した後に、コマンドを使用して Postfix を再起動します。

```
# postfix stop
# postfix start
```

IP プロファイラ

FoxProxy ログを削除するにはどうしたらいいですか。

ログ削除プログラムが IP プロファイラのインストールディレクトリ内にあります (初期設定 :/opt/trend/ipprofiler/bin/TmFoxPurgeLog)。
ログの削除機能に関する設定は設定ファイル foxproxy.ini に記載されています。
キーは次のとおりです。

- log_purge
- log_purge_unit
- log_purge_num

FoxProxy のステータスはどのように監視されますか。FoxProxy の機能が停止したとき、どのように復旧されますか。

FoxProxy は、マルチプロセスプログラムです。メインプロセスは、子プロセスのみを監視します。子プロセスの機能が停止した場合、メインプロセスが対応します。ただし、メインプロセスの機能が停止している場合には、子プロセスには復旧措置が取られません。
FoxProxy で問題が発生した場合には、メインプロセスが実行中であることを確認してください。

DNS クエリはどのように実行されますか？

DNS クエリは FoxProxy から直接実行されます。

既存の DNS サーバがインストーラによって検出されなかった場合、DNS サーバが自動的にセントラルコントローラにインストールされます。IP プロファイラをインストールする際に、セントラルコントローラの IP アドレスの入力を求められます。

ブロックリストまたは承認済みリストに追加された IP アドレスのドメイン名が常に表示されていないのはなぜですか。

InterScan MSS では、ブロックリストまたは承認済みリストに追加された IP アドレスのドメイン名は解決されません (追加されたドメイン名の IP アドレスは InterScan MSS によって解決されます)。

[IP フィルタ] の [疑わしい IP] 画面にも、ブロックされる IP アドレスの接続情報が表示されるのはなぜですか。

[IP フィルタ]→[疑わしい IP] 画面には、正常な接続の情報がすべて表示されます。したがって、現在 IP アドレスがブロックリストに含まれている場合でも、この IP アドレスのブロックされていなかった以前の接続が表示されます。

IP プロファイラはメールをどのように処理するのですか。

IP フィルタによって、送信元の IP アドレスが安全な IP アドレスかどうか判断します。InterScan MSS 検索サービスによって、InterScan MSS ポリシーサービスに一致したポリシーがないかどうか確認されます。要求された順序で、メールにポリシーが適用されます。メールの隔離、削除、または配信をポリシーが指定する場合は、処理が実行され、残りのポリシーは適用されません。

IP プロファイラは既存の BIND サーバを使用できますか。

はい。IP プロファイラには BIND サーバが必要です。ユーザが InterScan MSS をインストールするとき、コンピュータ上に既に BIND サーバが存在する場合は、IP プロ

ファイラはこの BIND サーバを使用します。BIND サーバが存在しない場合は、InterScan MSS によって新しい BIND サーバがインストールされます。

IP プロファイラが正常に機能することを確認するには、BIND 9.x をどのように設定すればいいですか。

インストールまたは移行時に BIND 9.x をインストールしていない場合、後から IP プロファイラを使用するには、次の手順に従ってください。

a. バージョン 9.x より前の BIND サーバが存在する場合は、対象のコンピュータでその BIND サーバをアンインストールします。

b. コマンド tar -xvf imss.tar を実行して、bind.tar ファイルを取得します。

c. bind.tar を指定のフォルダにコピーします。

d. コマンド tar -xvf bind.tar を実行してファイルを抽出します。

e. cd コマンドを入力して bind フォルダにディレクトリ変更します。フォルダの外部では、次の項目を表示できます。

```
bash-2.03# pwd
/export/home/bob
bash-2.03# ls
bind bind.tar
```

f. 次のコマンドを実行します。

```
chgrp -R imss bind
chown -R imss bind
chmod -R 555 bind


cp -f bind/named.conf /etc
cp -f bind/rndc.key /etc


mkdir -p /var/named
chmod 770 /var/named
```

g. 名前付きグループまたはユーザが存在しない場合は、次のコマンドを実行します。

```
groupadd named
useradd -g named -s /bin/false -d /var/named named
```

h. 次のコマンドを実行して BIND サーバを設定します。

```
chown named:named /var/named
mkdir -p /var/run/named
chmod 770 /var/run/named
chown named:named  /var/run/named

chown named:named  /etc/named.conf
chown named:named  /etc/rndc.key
chmod 555 /etc/named.conf
chmod 555 /etc/rndc.key
```

i. 次のように foxdns.ini を変更します。

```
vi $IMSS_HOME/config/foxdns.ini
#$IMSS_HOME is /opt/trend/imss/ by default.
#modify the following item:
# /export/home/bob/bind is the folder for bind
dig_path=/export/home/bob/bind/dig
rndc_path=/export/home/bob/bind/rndc
named_pid_path=/var/run/named/named.pid
named_db_path=/var/named/ipprofiler
```

j. 「bash-2.03# /export/home/bob/bind/named」を入力して BIND サーバを実行します。

k. $IMSS_HOME/script で S99FOXDNS を再起動します。

InterScan MSS 7.0 がメールを「7.0Foxhunter_proxy@domain」に送信するのは、どのようなときですか。

InterScan MSS は、次の 3 つの状態になると、メールを「Foxhunter_proxy@domain」に送信します。

- FoxProxy が「不完全な」メッセージを受信した場合。
- FoxProxy が「Null」メッセージを受信した場合。
- FoxProxy が接続を拒否した場合、5 分ごとに統計メールを送信します。foxproxy.ini 内の report_send_interval (秒単位) 設定を変更して、時間間隔を設定できます。

受信トラフィックが DHA 攻撃であるかどうかの分析に LDAP サービスは必要ですか。

技術的には、LDAP サービスは必須ではありません。InterScan MSS 7.0 の DHA ルールは、Postfix から返された結果に依存しています。その結果は、分析用の IP プロファイラのサブモジュールである FoxProxy に代わりに渡されます。LDAP サーバは、Postfix が受信者のメールボックスの存在をチェックするための方法の 1 つに過ぎません。

隔離とアーカイブ

検索にはどのような特殊文字を使用できますか。

ワイルドカードとしてアスタリスク (*) を使用します。また、受信者や添付ファイル名を区切るにはセミコロン (;) を使用します。

ユーザがメッセージの詳細を表示するときに、メッセージ ID なしの隔離されたメッセージがあるのはなぜですか。

InterScan MSS は、セキュリティ上の理由で通知メールを再処理します。したがって、通知メールがポリシー設定によって隔離された場合、InterScan MSS によって作成されたこの通知メールにはメッセージ ID がありません。

InterScan MSS で通知メールを検索しない場合は、次のように通知メールの検索を無効にできます。

a. imss.ini の [general-notification] セクションで次の設定を変更します。

NotificationSkipScan=1

b. コマンド $IMSS_Home/script/S99IMSS restart を入力して InterScan MSS デーモンを再起動します。

警告： ポリシー設定に起因するセキュリティ漏えいのリスクが存在するため、トレンドマイクロでは通知メールの検索を無効にすることはお勧めしません。

エンドユーザメール隔離

Kerberos を使用している場合、ユーザがエンドユーザメール隔離コンソールに「domain¥user_name」の省略名でログインできないのはなぜですか？

Kerberos サーバでは domain¥user_name 形式のユーザ名を受け入れることができません。Kerberos では user_name@domain.xxx という形式のユーザ名を使用する必要があります。

Exchange Server をインストールして、ユーザごとに複数のメールアドレスを設定している場合、1 人のユーザに対する複数のメールアドレスを確認するためには、エンドユーザメール隔離をどのように有効化すればいいですか。

1 つの Exchange Server を Active Directory とともにインストールしている場合、次の操作を実行できます。

a. InterScan MSS 管理データベースで tb_global_setting テーブルを開き、LDAP-->mail_attr の値を「mail」から「proxyAddresses」に置き換えます。

b. すべての InterScan MSS サービスを再起動します。

中国語のエンドユーザメール隔離通知を送信するには、どうしたらいいですか。

次の項目を実行してください。

a. 管理コンソールメニューから、[管理]→[通知]→[EUQ 通知] の順にクリックします。

[EUQ 通知] 画面が表示されます。エンドユーザメール隔離通知の件名とコンテンツを中国語で入力します。

b. [管理]→[通知]→[通知設定] の順にクリックします。

[通知設定] 画面が表示されます。文字コードとして中国語を選択します。

LDAP サーバが Active Directory の場合、LDAP アクセスの速度を速くするにはどうすればいいですか。

アクセス速度を速くするには 2 通りの方法があります。どちらの方法を使用するかは、使用するポート番号が 389 か、3268 かによって決まります。

Active Directory は、グローバルカタログに 3268 を使用します。グローバルカタログに対する LDAP クエリは、別のドメインコントローラへの参照を使用しないため、アクセス速度が速くなります。

ヒント： トレンドマイクロでは、LDAP クエリにはポート 3268 を使用することをお勧めします。

Active Directory は、LDAP クエリに 389 を使用します。あるドメインコントローラで、アイテムのクエリが実行できない場合は、LDAP 参照メカニズムを使用して、別のドメインコントローラでクエリを実行します。社内のドメイン数が 1 つだけの場合またはポート 3268 を利用できない場合は、ポート 389 を使用してください。

LDAP クエリにポート 3268 を使用するには

a. [管理]→[InterScan MSS の設定]→[接続] の順にクリックします。[接続] 画面が表示されます。

b. [LDAP] タブをクリックします。

c. LDAP 待機ポートを 3268 に設定します。

LDAP クエリにポート 389 を使用するには

a. [管理]→[InterScan MSS の設定]→[接続] の順にクリックします。[接続] 画面が表示されます。

b. [LDAP] タブをクリックします。

c. LDAP 待機ポートを 389 に設定します。

d. $IMSS_HOME¥config にある imss.ini ファイルに次のキーを追加します。

```
[LDAP-Setting]
DisableAutoChaseReference=yes
```

e. すべての InterScan MSS サービスを再起動します。

InterScan MSS では、Active Directory に対してどのような形式のユーザログオン名をサポートしていますか。

Active Directory では、次のようなログオン名形式がサポートされています。

- 例 1:bob@imsstest.com

注意： ログオン名は (このような形で表示されますが) メールアドレスではありません。

- 例 2 (Windows 2000 以前):IMSSTEST¥bob

注意： Windows 2000 以前の形式は、Kerberos 認証ではサポートされていません。

スパムメール対策サービス

スパムメールの検出レベルはどのように決められるのですか。

InterScan MSS のメッセージをスパムメールとして分類するしきい値 (3.0 ～ 10.0 の間) を指定します。しきい値が高いと、スパムメールの疑いが強い場合でなければメッセージはスパムメールとして分類されません (これによりスパムメール検出レベルは低下しますが、誤検出は少なくなります)。しきい値が低いと、スパムメールの疑いがそれほど強くない場合でもメッセージをスパムメールとして分類します (これによりスパムメール検出レベルは向上しますが、誤検出は多くなります)。

アップデート

パターンファイルはどのようにロールバックするのですか。

[概要] ページで [ロールバック] ボタンをクリックしてください。

その他

SMTP over TLS (Transport Layer Security) を使用するには、何をすればいいですか？

[管理]→[InterScan MSS の設定]→[SMTP ルーティング] 画面で TLS の証明書をアップロードし、設定を有効にします。

InterScan MSS 7.0 では、Postfix TLS 機能を使用します。すべての設定は、設定ファイル main.cf に書き込まれます。詳細については、以下を参照してください。

http://www.postfix.org/TLS_README.html

データベースサーバをホスト名で参照することはできますか。

はい。「**IP アドレス￥インスタンス**」や「**ホスト名￥インスタンス**」のように指定できます。

サーバの IP アドレスを変更できますか。

はい。

サーバの IP アドレスを変更するには

a. $IMSS_Home/script/imssstop.sh stop コマンドを実行して、すべての InterScan MSS サービスを停止するか、次のスクリプトを実行してサービスを個別に停止します。

S99IMSS stop

S99Policy stop

S99EUQ stop

S99CMAGENT stop

S99ADMINUI stop

S99FOXDNS stop

S99MONITOR stop

S99MANAGER stop

dbctl.sh stop

それぞれのスクリプトの詳細については、付録 B を参照してください。

b. サーバの IP アドレスを変更します。

c. InterScan MSS 設定フォルダの ODBC.ini および EUQ.ini の IP アドレスを変更します。

d. $IMSS_HOME/UI/adminUI/ROOT/WEB-INF/struts-config-common.xml でデータベース URL およびユーザ名 / パスワードを変更します。

e. 次のデータベースデータを変更します。

- tb_component_list: コンピュータ名とすべての検索サービスの IP アドレスを指定します。
- tb_euq_db_info: エンドユーザメール隔離データベースのコンピュータ設定を指定します。
- tb_global_setting: [cmagent] name [ConfigUrl] セクションで、管理コンソールの URL を変更します。

f. $IMSS_Home/script にあるスクリプトを実行してすべての InterScan MSS サービスを再起動します。

次のスクリプトから始めます。

```
dbctl.sh start
S99MANAGER start
```

残りのサービスは、任意の順序で再起動できます。

```
S99IMSS start
S99Policy start
S99EUQ start
S99CMAGENT start
S99ADMINUI start
S99FOXDNS start
S99MONITOR start
```

InterScan MSS では分割メールをどのように処理するのですか。

InterScan MSS では、imss.ini ファイル内で BypassMessagePartial=yes に設定されている場合、InterScan MSS は分割メールに特別な処理を行わないでメールが配信されます (初期設定)。

キーが no と設定されている場合は、分割メールを正しくない形式のメッセージとして拒否します。

ポリシー設定の際に、InterScan MSS でインポートできるのはどのようなファイル形式ですか。

InterScan MSS では、1 行に 1 項目だけを含むテキストファイルのみをインポートできます。次は、管理コンソールからテキストファイルをインポートする方法の例です。

a. 検索する添付ファイルを指定する場合

- メニューから、[ポリシー]→[ポリシーリスト] の順にクリックします。
- 既存のルールのリンクをクリックして、ルールを編集します。
- [検索条件] リンクをクリックします。

- [添付ファイル] セクションの下にある [名前または拡張子] リンクをクリックします。
- [指定のファイル名] チェックボックスをオンにします。
- [インポート] をクリックします。インポートされたファイルは、1 行に 1 つのファイル名または拡張子を含むテキストファイルでなければなりません。

b. スパムメール検出を設定する場合

- メニューから、[ポリシー]→[ポリシーリスト] の順にクリックします。
- 既存のルールのリンクをクリックして、ルールを編集します。
- [検索条件] リンクをクリックします。
- [スパムメール] リンクをクリックします。
- [承認済み送信者リスト] または [ブロックする送信者リスト] チェックボックスをオンにします。
- [インポート] をクリックします。インポートされたファイルは、1 行に 1 つのメールアドレスを含むテキストファイルでなければなりません。

新しく作成した管理者アカウントが [ユーザ隔離アクセス]、[管理者アカウント]、または [製品ライセンス情報] ページにアクセスできないのはなぜですか。

初期設定の InterScan MSS 管理者アカウントだけが、[ユーザ隔離アクセス]、[管理者アカウント]、または [製品ライセンス情報] ページにアクセスする権限を持っています。委任された管理者のアカウントでは、これらのページにアクセスできません。

InterScan MSS 設定への変更は、なぜただちに有効にならないのですか。

管理コンソールから設定を変更した時間と InterScan MSS サーバ上で変更が実際に更新される時間との間にわずかなずれがあります。

ポリシー設定は 3 分以内に再読み込みされます。この設定をより速く読み込むには、必要に応じて、InterScan MSS 管理データベースの tb_global_setting テーブルで policy_server=>dbChangePollIntervalInSecs 設定を変更してください。

その他の一般的な設定については、imssmgr により、1 分以内に管理コンソールから変更した新しい設定が再度読み込まれます。

トレンドマイクロでは、管理コンソールから設定を変更した直後に InterScan MSS へメールを送信しないことをお勧めします。

次の項目の最大数に制限がありますか。

- 各ルールの送信者と受信者
- 1 つのアドレスグループ内のメールアドレス
- スパムメール判定ルールの承認済み送信者とブロックする送信者

技術的に、各ルールの合計サイズに 640KB という 1 つの制限があります。合計サイズには、ルールルート (送信者と受信者)、ルールフィルタ (検索条件)、ルール処理などが含まれます。各メールアドレスまたは各 LDAP アカウントは 20 文字で構成されることを前提としており、InterScan MSS では、ルールルートで少なくとも 10,000 の送信者と受信者をサポートできます。

1 つのアドレスグループのメールアドレス最大数は 10,000 です。

スパムメール判定ルールの承認済み送信者とブロックする送信者の最大数は 5,000 です。

ログのパスを変更するにはどうしたらいいですか。

一部のログのパスを変更する場合は、必要に応じて、imss.ini の次のキーを検索して初期設定を変更してください。

```
[general]
sys_log_path=/opt/trend/imss/log
event_log_path=/opt/trend/imss/log
policy_evt_log_path = /opt/trend/imss/log
[policy_server]
log_path = /opt/trend/imss/log
...
[logs]
log_path=/opt/trend/ipprofiler/logs
```

サードパーティのアップストリームサーバがインストールされていない場合、InterScan MSS 7.0 で InterScan MSS のリレーの制約を設定できますか。

いいえ、InterScan MSS 7.0 では InterScan MSS のリレーの制約は設定できません。これは、InterScan MSS が UNIX プラットフォーム上の MTA を持たないためです。サードパーティの MTA を使用した場合のみ、リレーの制約を設定できます。

InterScan MSS 検索サービスのアクセス制御リスト (ACL) を変更するには、どうしたらいいですか。

imss.ini の次の設定を変更できます。

- パラメータ smtp_allow_client_ip に対象となる IP アドレスを追加します。
- または、open_to_all_connections=yes を設定して ACL チェックを無効にします。
- 他のコンピュータが検索サービスに接続できることを確認するには、対象の IP アドレスをパラメータ proxy_smtp_server_ip に挿入します。

詳細については、imss.ini のコメントを参照してください。

特定の送信者からのメールが常に添付ファイルとして受信されます。メールの本文もディスクレーマーまたはスタンプに置き換えられています。これはどうしてですか。

スタンプの文字コードがメールのコンテンツの文字コードと異なる場合、InterScan MSS では、メールを検索した後にスタンプをメール本文に挿入するという問題が発生します。このような場合、InterScan MSS では、メールの本文にスタンプを挿入し、オリジナルのメッセージを添付ファイルにした新しいメールが作成されます。メールのコンテンツが変更されることはありません。

コンテンツフィルタのルールを作成する際に、「from」、「to」、または「subject」などのフィールドが空の場合に一致させる、ヘッダのキーワード表現はどのように指定すればいいですか。

トレンドマイクロでは、空のヘッダを表すキーワードの正規表現として、「^(¥s)*$」を使用することをお勧めします。「^(¥s)*$」は、空のヘッダまたは空白文字を表します。
たとえば、メールの「from」ヘッダが空白であるか確認したい場合、ルールの検索条件を次のように編集できます。

a. 管理コンソールで、[ポリシー]→[ポリシーリスト] の順にクリックします。
b. 既存のルールのリンクをクリックして、ルールを編集します。
c. [検索条件] リンクをクリックします。
d. [コンテンツ] セクションの下にある [ヘッダのキーワード] をクリックします。

e. [追加] をクリックして新しいキーワード表現を作成します。

f. コンテンツを「^(¥s)*$」として追加します。

製品サポート情報

InterScan MSS のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「スタンダードサポート サービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話、FAX、メールなどをご利用ください。サポートセンターの連絡先は、「スタンダードサポート サービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意： サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

製品 Q&A のご案内

トレンドマイクロの Web サイトでは、製品 Q&A の情報を提供しています。これは、トレンドマイクロの製品に関する技術的な質問と、それに対する回答を集めたものです。製品 Q&A には、次の URL からアクセスできます。

中小 / 中堅企業のお客さま

http://esupport.trendmicro.co.jp/supportjp/smb/search.do

大企業のお客さま

http://esupport.trendmicro.co.jp/supportjp/enterprise/search.do

製品 Q&A では、お使いの製品名およびキーワードを指定して、知りたい情報を検索できます。たとえば製品のマニュアル、ヘルプ、Readme ファイルなどに記載されていない情報が必要な場合に、製品 Q&A を利用してください。

トレンドマイクロでは製品 Q&A の内容を常に更新し、新しい情報を追加しています。

セキュリティ情報

セキュリティ情報の入手先

トレンドマイクロでは、最新のセキュリティ情報をインターネットで公開しています。トレンドマイクロのセキュリティ情報 Web サイトでは、ウイルスやインターネットセキュリティに関する最新の情報を入手できます。セキュリティ情報 Web サイトは、次の URL からアクセスできます。

http://www.trendmicro.co.jp/vinfo/

管理コンソールからセキュリティ情報サイトにアクセスすることもできます。セキュリティ情報サイトにアクセスするには、管理コンソールの画面の右上にあるリストボックスから[セキュリティ情報] リンクを選択します。

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

- ウイルス名やキーワードから検索できるウイルスデータベース
- コンピュータウイルスの最新動向に関するニュース
- 現在流行中のウイルスや不正プログラムの情報
- デマウイルスまたは誤警告に関する情報
- ウイルスやネットワークセキュリティの予備知識

セキュリティ情報 Web サイトに定期的にアクセスして、流行中のウイルス情報などを入手することをお勧めします。メールによる定期的なウイルス情報配信を希望する場合は、警告メール配信の登録フォームを利用してメールアドレスを登録してください。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出 / 駆除できない場合などに、感染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロのウイルスデータベース検索サイトにアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

http://www.trendmicro.co.jp/vinfo/virusencyclo/default.asp

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

http://inet.trendmicro.co.jp/esolution/attach_agreement.asp

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

トレンドマイクロへのスパムメールの報告

トレンドマイクロでは、できるだけ最新のスパムメールデータベースを提供できるように、スパムメールが検出されずに受信された場合、そのメールをトレンドマイクロの次のメールアドレスに転送するようにお願いしています。

jp-spam@support.trendmicro.com

また、通常のメールがスパムメールとして検出（誤検出）された場合は、そのメールを次のメールアドレスに転送してください。

jp-false@support.trendmicro.com

注意： お客さまから転送されたメールはスパムメールの検出精度向上のための用途にのみ使用します。お客さまからのメールに含まれる個人情報は、スパムメール検出精度向上のための作業後、すみやかに削除します。

ウイルス解析サポートセンター「TrendLabs」

トレンドマイクロのウイルス解析サポートセンター「TrendLabs」(トレンドラボ) は、フィリピンセンターを本部として、米国、日本、台湾、ドイツ、アイルランド、中国の各国センターで構成されています。24 時間体制でウイルスの活動を監視するウイルス解析エンジニアを含む 800 名以上 (2006 年 1 月現在) のスタッフが、セキュリティに関する最新の情報を収集し、高品質なサービスとソリューションを迅速かつ効果的に世界各国のトレンドマイクロのパートナーとお客さまに提供しています。

「TrendLabs」では、品質保証の ISO9001:2000 認定 (フィリピン)、国際規格 COPC-2000 規格 (フィリピン)、英国の国家規格 ITIL: BS15000 (ドイツ)、情報セキュリティマネージメントの英国規格 BS7799 (フィリピン) を取得しています。

InterScan MSS スクリプト

この付録では、コマンドラインから実行する Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) スクリプトとそれに関連するパラメータのリストについて説明します。

この付録の内容は次のとおりです。

- 180 ページの「InterScan MSS スクリプトの実行」

InterScan MSS スクリプトの実行

InterScan MSS スクリプトを使用することで、コマンドラインから管理タスクを実行できます。

スクリプト、関連するパラメータ、およびその機能のリストについては、表 A-1 を参照してください。

注意： 表に記載されているすべてのスクリプトは、/$IMSS_Home/imss/script にあります。例外として、foxproxyd のみが、/$IMSS_Home/ipprofiler/script にあります。

スクリプト	パラメータ	説明
foxproxyd	start / stop / restart	IP プロファイラサービス
dbctl.sh	start / stop / restart	Postgres データベースサービス
imsstop.sh		すべての InterScan MSS サービスを強制的に停止します。
postfixctl.sh	start / stop / reload / restart	Postfix デーモン
regippro.sh	reg / unreg	管理データベースに IP プロファイラを登録、または管理データベースから IP プロファイラの登録を解除します。
S99ADMINUI	start / stop / restart	セントラルコントローラ
S99CLEANEUQ		管理コンソールの [管理]→[ユーザ隔離アクセス] での設定に従って、エンドユーザメール隔離および管理データベースから期限切れの隔離データを削除します。

表 A-1.　InterScan MSS スクリプト

スクリプト	パラメータ	説明
S99CLEANEXPIRE		管理コンソールの [隔離およびアーカイブ]→[設定] での設定に従って、エンドユーザメール隔離および管理データベースから期限切れの隔離データおよびアーカイブされたデータを削除します。
S99CMAGENT	start / stop / restart	CMAgent サービス
S99DIGEST		エンドユーザメール隔離通知メッセージを送信します。
S99EUQ	start / stop / restart	エンドユーザメール隔離サービス
S99FOXDNS	start / stop / restart	Foxdns サービス
S99IMSS	start / stop / restart	InterScan MSS 検索サービス
S99MANAGER	start / stop / restart	マネージャサービス
S99MONITOR	start / stop / restart	マネージャ監視サービス
S99POLICY	start / stop / restart	ポリシーサービス
S99REPORT	[option] start / stop / restart [option]: • **-s** — 一元化されたレポート機能を生成します (管理コンソールで設定された 1 回限りのレポートおよび予約レポートすべてを含みます)。 • **-h** — 1 時間ごとの個別のトラフィックデータを生成します。 • **-t** — 1 時間ごとのトラフィックデータを生成します。 • **-d** — データベースのログ管理を実行します。	関連するレポートを生成するために S99SCHEDULED によって使用されます。 注意 : **このスクリプトだけで実行しないでください。**
S99UPDATE	start / stop	予約アップデートを実行するために S99SCHEDULED によって使用されます。 注意 : **このスクリプトだけで実行しないでください。**

表 A-1.　InterScan MSS スクリプト

スクリプト	パラメータ	説明
S99SCHEDULED		予約タスクを開始します。
forceUpdate.sh	DBDSN ユーザ名パスワード	ポリシー設定を再読み込みするようにポリシーサーバに通知します。
euqtrans		エンドユーザメール隔離データベースのデータを転送します。

表 A-1.　InterScan MSS スクリプト

初期設定ディレクトリ

この付録では、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) のメール処理で使用する初期設定のディレクトリの場所について説明します。

この付録の内容は次のとおりです。

- 184 ページの「初期設定のメールキュー」
- 185 ページの「コンテンツフィルタ、ウイルスおよびプログラムのログ」
- 185 ページの「一時フォルダ」
- 186 ページの「通知受取フォルダ」

初期設定のメールキュー

表 B-1 には、InterScan MSS で管理されるメールメッセージを保存するさまざまなメールディレクトリが示されています。

通常のメールのキュー	大きいメールのキュー	説明
queue_malform=/opt/trend/imss/queue/malform		正しくない形式のメッセージを保存します。
queue_archive=/opt/trend/imss/queue/archive		アーカイブされたメッセージを保存します。
queue_quarantine=/opt/trend/imss/queue/quarantine		隔離されたメッセージを保存します。
queue_notify=/opt/trend/imss/queue/notify	queue_notify_big=/opt/trend/imss/queue/notifybig	通知メッセージを保存します。
queue_postpone=/opt/trend/imss/queue/postpone	queue_postpone_big=/opt/trend/imss/queue/postponebig	遅延メッセージを保存します。
queue_deliver=/opt/trend/imss/queue/deliver	queue_deliver_big=/opt/trend/imss/queue/deliverbig	最終配信のメッセージを保存します。
queue_reprocess=/opt/trend/imss/queue/reprocess	queue_reprocess_big=/opt/trend/imss/queue/reprocessbig	再処理が保留中のメッセージを保存します。
queue_handoff=/opt/trend/imss/queue/handoff	queue_handoff_big=/opt/trend/imss/queue/handoffbig	中継が保留中のメッセージを保存します。

表 B-1. 初期設定の InterScan MSS メールの場所

通常のメールのキュー	大きいメールのキュー	説明
queue_undeliverable=/opt/trend/imss/queue/undeliverable		配信できなかったメッセージを保存します。
queue_unnotify=/opt/trend/imss/queue/unnotify		配信できなかった通知メッセージを保存します。

表 B-1.　初期設定の InterScan MSS メールの場所

コンテンツフィルタ、ウイルスおよびプログラムのログ

InterScan MSS の多くのモジュールは、トラブルシューティングの目的でログ情報を次のフォルダに書き込みます。

/opt/trend/imss/log

一時フォルダ

InterScan MSS では、アプリケーションによって生成されたすべての一時ファイルを一時フォルダに保存します。

/opt/trend/imss/temp/

注意： このディレクトリの設定は変更できません。

通知受取フォルダ

InterScan MSS では、次のフォルダにすべての通知メッセージを保存して受け取ってから、指定された SMTP 通知サーバに通知メッセージを配信します。

/opt/trend/imss/queue/notify/ および /opt/trend/imss/queue/notifybig

SMTP 通知サーバを設定するには

[管理]→[通知]→[通知設定] の順に選択します。

注意： queue_notify_big キューは大きいメールメッセージ用です。

索引

英数字

AJP 155
APOP 58
MTA
  NRS での使用 35
NRS
  MTA 設定 35
  アクティベーションコード 34
  管理コンソール 37
  使用 34
POP3 待機ポート 155
SMTP ルーティング 48
SOAP サーバ 155
SSL 証明書 16
TrendLabs 178

あ

アドレスグループ
  例 62
インストール 13、33、105、115
  SSL の使用 16
ウィザード 18
エンドユーザメール隔離
  管理コンソール 30

か

管理コンソール 14
基本設定 18
許可された送信者 52
検索条件 78
コマンド 180

さ

スパムメール対策
  アクティベーションコード 34
接続 49
設定ウィザード 18

た

テクニカルサポート 175
ドメインベースの配信 52
トラブルシューティング 148
  imssps デーモン 148
  IP フィルタ 152
  エンドユーザメール隔離管理コンソールへのアクセス 151
  エンドユーザメール隔離通知 151
  エンドユーザメール隔離の隔離されたメッセージ 152
  製品の起動 149
  メール通知 149
トランスポート層 50

は

パスワード
  InterScan MSS 管理コンソール初期設定 14
フィルタ
  例 62

や

ユーザ名
InterScan MSS 管理コンソール初期設定 14
よくある質問
InterScan MSS コンポーネント 157
IP プロファイラ 160
postfix 156
TLS 168
エンドユーザメール隔離 165