

Trend Micro InterScan Messaging Security Suite™



安心を、ひとつ上のステージへ。



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」「URLフィルタ」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、コモンゲートウェイインタフェースアプリケーションを使用しているサーバで構築されているWebサイトにアクセスし、ID、パスワード等を入力した場合には、お客様がアクセスしたWebページのURLにお客様が入力したID、パスワード等が含まれた状態でトレンドマイクロのサーバに送信される場合があります。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/complianceand enforcement/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サイトからご確認ください。
<http://jp.trendmicro.com/jp/support/lifecycle/index.html>

著作権について

本書に関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が書面により事前に承諾している場合を除き、形態および手段を問わず本書またはその一部を複製することは禁じられています。本書の作成にあたっては細心の注意を払っていますが、本書の記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本書およびその記述内容は予告なしに変更される場合があります。

商標について

TRENDMICRO、ウイルスバスター、ウイルスバスター On-Line-Scan、PC-cillin、InterScan、INTERSCAN VIRUSWALL、ISVW、InterScan Web Manager、ISWM、InterScan Message Security Suite、InterScan Web Security Suite、IWSS、TRENDMICRO SERVERPROTECT、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、トレンドマイクロ・プレミアム・サポート・プログラム、License for Enterprise Information Security、LEISec、Trend Park、Trend Labs、InterScan Gateway Security Appliance、Trend Micro Network VirusWall、Network VirusWall Enforcer、Trend Flex Security、LEAKPROOF、Trend プロテクト、Expert on Guard、InterScan Messaging Security Appliance、InterScan Web Security Appliance、InterScan Messaging Hosted Security、DataDNA、Trend Micro Threat Management Solution、Trend Micro Threat Management Services、Trend Micro Threat Management Agent、Trend Micro Threat Mitigator、Trend Micro Threat Discovery Appliance、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、Smart Protection Network、およびSPNは、トレンドマイクロ株式会社の登録商標です。

本書に記載されている各社の社名、製品名、およびサービス名は、各社の商標または登録商標です。

Copyright ©2002-2009 Trend Micro Incorporated. All rights reserved.

P/N: IMSSUX-AE0300 (2009/09)

目次

はじめに	11
対象読者	12
InterScan MSS ドキュメント	12
ドキュメントの表記規則	13
 第 1 章 使用開始	15
InterScan MSS の管理コンソールを開く	16
オンラインヘルプを使用する	17
SSL を使用した管理コンソールの表示	17
SSL 証明書を作成する	17
設定ウィザードを使用して基本設定を実行する	19
設定ウィザードにアクセスする	19
管理コンソールのパスワードを変更する	27
検索エンジンとパターンファイルをアップデートする	28
アップデート元を指定する	28
手動アップデートを実行する	29
コンポーネントのアップデートをロールバックする	30
予約アップデートを設定する	31
InterScan MSS サービス	32
サービスを起動または停止する	33
エンドユーザメール隔離の管理コンソールを開く	34
ログオン名形式	34
 第 2 章 InterScan MSS の設定	35
IP フィルタサービス	36
Email Reputation Services を使用する	36

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	36
Email Reputation Services で使用するための MTA を準備する	37
ERS 管理コンソールを使用する	37
IP フィルタを設定する	41
手順 1: ERS および IP プロファイラを有効にする	41
手順 2: IP プロファイラのルールを有効にする	42
手順 3: ERS を設定する	50
手順 4: IP アドレスを承認済みリストへ追加する	51
手順 5: IP アドレスをブロックリストへ追加する	52
疑わしい IP アドレスおよびドメインを表示する	52
SMTP メッセージを検索する	53
SMTP 接続を有効にする	54
SMTP ルーティングを設定する	54
SMTP を設定する	55
接続を設定する	56
メッセージルールを設定する	58
ドメインベース配信について	61
ドメインベース配信を設定する	62
POP3 メッセージを検索する	64
POP3 の検索について	64
要件	65
POP3 の検索を有効にする	65
POP3 を設定する	66
 第 3 章 ポリシーの管理	 69
ポリシーの管理	70
Policy Manager の仕組み	70
共通のポリシーオブジェクトの設定	72
アドレスグループについて	74

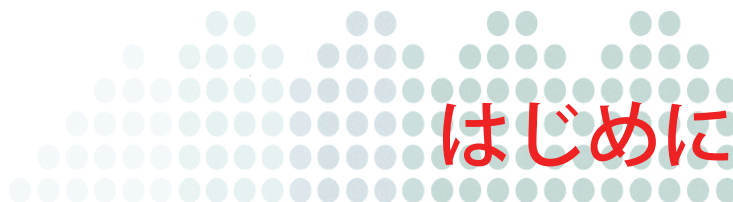
アドレスグループを作成する	74
ポリシー作成時にアドレスグループを追加する	76
アドレスグループを編集または削除する	79
アドレスグループをエクスポートする	81
キーワード表現リストを使用する	81
キーワードを設定する	82
通知リストを使用する	85
ポリシー通知を追加または変更する	86
スタンプを使用する	88
スタンプを作成する	88
DKIM 承認済みリストを使用する	89
Web レピュテーション承認済みリストを使用する	90
Web レピュテーション承認済みリストに追加する	91
内部アドレスを設定する	92
LDAP ユーザまたはグループを検索する	95
ポリシーを追加する	96
ルートを指定する	97
ルートを設定する	101
ルートの除外を設定する	103
検索条件を指定する	104
スパムメールの検索条件を選択する	109
承認済み送信者リストとブロックする送信者リストを設定する	110
スパムメール除外テキストルールを設定する	111
Web レピュテーションを設定する	112
添付ファイルの検索条件を選択する	113
メッセージサイズの検索条件を選択する	116
メッセージコンテンツの検索条件を選択する	116
「その他」の検索条件を指定する	117
受信者数の検索条件を選択する	117
メッセージ受信時間の検索条件を設定する	118

処理を指定する	118
件名タグを作成する	126
ポリシーを完成させる	127
既存のポリシーを変更する	129
グローバル DKIM 適用ルールのドメインリストを使用する	130
ポリシーの例 1	131
ポリシーの例 2	134
アスタリスクワイルドカードを使用する	137
検索除外を設定する	138
セキュリティ設定違反の除外を設定する	139
セキュリティ設定違反の検出時の処理を設定する	140
正しくない形式のメッセージの検索除外に対する検出時の処理を設定する ..	141
第 4 章 設定のバックアップ、復元、複製について	143
設定のインポート / エクスポート	144
InterScan MSS のバックアップ	145
InterScan MSS の復元	146
設定の複製	147
Control Manager エージェントを有効にする	148
Control Manager から設定を複製する	149
第 5 章 ネットワークの監視	151
ネットワークを監視する	152
統計の概要を表示する	152
システムの概要を表示する	152
統計を理解する	153
パフォーマンスの概要	155
検索パフォーマンス	156
IP フィルタパフォーマンス	157

レポートを作成する	158
レポート内容の種類	158
1 回限りのレポートを管理する	159
1 回限りのレポートを追加する	160
予約レポートを使用する	162
予約レポートを設定する	163
ログ	165
ログを設定する	165
ログのクエリを実行する	167
隔離とアーカイブ	173
隔離とアーカイブを設定する	173
隔離領域を管理する	174
メッセージのクエリを実行する	177
隔離されたメッセージを表示する	180
アーカイブされたメッセージを表示する	181
ユーザ隔離アクセスを設定する	181
エンドユーザメール隔離データベースを追加する	184
euqtrans ツールのコマンドラインオプション	185
イベント通知	185
通知を設定する	186
イベント条件および通知メッセージを設定する	188
エンドユーザメール隔離通知を設定する	189
通知を編集する	190
 第 6 章 エンドユーザメール隔離の使用	 191
エンドユーザメール隔離について	192
手順 1: LDAP を設定して有効にする	192
手順 2: エンドユーザメール隔離を有効にする	195
手順 3: エンドユーザメール隔離サービスを開始する	196

手順 4: ユーザ隔離アクセスを有効にする	196
手順 5: エンドユーザメール隔離の管理コンソールを開く	199
ログオン名形式	199
エンドユーザメール隔離を無効にする	200
第 7 章 管理タスクの実行	201
管理者アカウントを管理する	202
管理者アカウントを追加する	202
管理者アカウントを編集または削除する	204
接続を設定する	205
LDAP を設定する	206
POP3 を設定する	208
データベースを設定する	209
Control Manager を設定する	210
製品ライセンスを管理する	211
製品ライセンスを表示する	212
ライセンスを更新またはアクティベートする	213
製品をアクティベートする	214
第 8 章 トラブルシューティングとサポート情報	217
トラブルシューティング	218
InterScan MSS ポート	227
よくある質問 (Q&A)	227
Postfix MTA 設定	227
InterScan MSS コンポーネント	228
Email Reputation Services	229
IP プロファイラ	230
隔離とアーカイブ	232
エンドユーザメール隔離	233

スパムメール対策サービス	235
アップデート	235
その他	235
製品サポート情報	239
サポートサービスについて	239
製品 Q&A のご案内	240
セキュリティ情報	240
セキュリティ情報の入手先	240
トレンドマイクロへのウイルス解析依頼	241
ウイルス解析サポートセンター「TrendLabs」	241
 付録 A InterScan MSS スクリプト	 243
InterScan MSS スクリプトの使用	244
 付録 B 初期設定ディレクトリ	 247
初期設定のメールキュー	248
コンテンツフィルタ、ウイルスおよびプログラムのログ	249
一時フォルダ	249
通知受け取りフォルダ	249
 索引	 251



はじめに

Trend Micro InterScan Messaging Security Suite 7.1 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、Trend Micro InterScan Messaging Security Suite 7.1（以下、InterScan MSS）の機能、システム要件、および InterScan MSS の設定の方法について説明しています。

InterScan MSS のインストールおよびアップグレード方法については「Trend Micro InterScan Messaging Security Suite 7.1 インストールガイド」を参照してください。

この章の内容は次のとおりです。

- 12 ページの「対象読者」
- 12 ページの「InterScan MSS ドキュメント」
- 13 ページの「ドキュメントの表記規則」

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 や Microsoft Exchange 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。

InterScan MSS 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、システム要件、および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方法について説明しています。
- **管理者ガイド** — InterScan MSS のインストールと実行、およびインストール後の設定と管理方法について説明しています。
- **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、既知の制限事項、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、

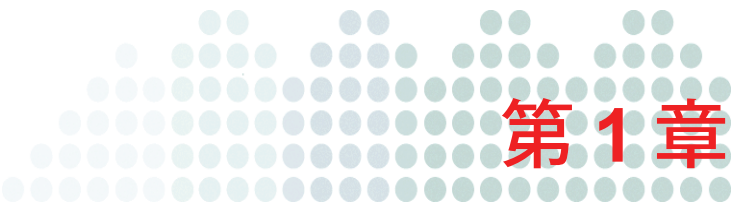
<http://www.trendmicro.co.jp/download/> から入手できます。

ドキュメントの表記規則

こ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
<u>注意：</u>	設定上の注意
<u>ヒント：</u>	推奨事項
<u>警告：</u>	避けるべき操作や設定についての注意

表 1. 本書で使用している表記規則



第1章

使用開始

この章では、Trend Micro InterScan Messaging Security Suite 7.1（以下、InterScan MSS）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。

- 16 ページの「InterScan MSS の管理コンソールを開く」
- 17 ページの「SSL を使用した管理コンソールの表示」
- 19 ページの「設定ウィザードを使用して基本設定を実行する」
- 27 ページの「管理コンソールのパスワードを変更する」
- 28 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」
- 32 ページの「InterScan MSS サービス」
- 34 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 を入力します。

- `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 : `imss7.1`

初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] をクリックします。

注意： Internet Explorer 7.0 を使用して管理コンソールにアクセスする場合、Internet Explorer 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。管理コンソールの IP アドレスを [信頼済みサイト] リスト (Internet Explorer の [インターネット オプション] → [セキュリティ]) に追加するか、メッセージを無視し [このサイトの閲覧を続行する] をクリックして処理を進めます。

ヒント： 管理コンソールへの不正アクセスを防ぐために、パスワードは定期的に変更してください。

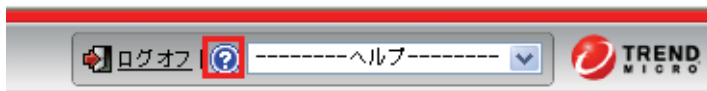
オンラインヘルプを使用する

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。

図 1-1. オンラインヘルプの目次へのアクセス



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. InterScan MSS 管理コンソール用に、次のように Tomcat SSL 証明書を作成します。

```
$IMSS_HOME/UI/javaJRE/bin/keytool -genkey -alias tomcat -keyalg RSA -sigalg SHA1withRSA -keystore $IMSS_HOME/UI/tomcat/sslkey/.keystore -validity 3652
```

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. エンドユーザメール隔離管理コンソール用に、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 3652 -sha1`
- 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`

設定ウィザードを使用して基本設定を実行する

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、次の手順で設定を行います。

手順 1: 通知を設定する

手順 2: アップデート元を設定する

手順 3: LDAP を設定する

手順 4: 内部アドレスを設定する

手順 5: Control Manager サーバを設定する

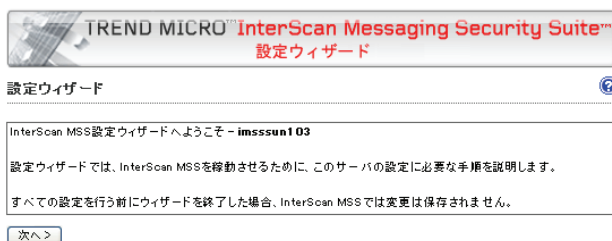
手順 6: アクティベートする

手順 7: 設定の概要を確認する

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。
- 管理コンソールにすで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: 通知を設定する

1. [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。

InterScan MSS
手順2/7

アップデート元

アップデート元を選択し、プロキシを設定することで、InterScan MSS が コンポーネントのアップデート および アクティベートを行えるようになります。

アップデート元

☒トレンドマイクロのアップデートサーバ

☐その他のインターネット上のサーバ

http://

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

プロキシタイプ: HTTP

プロキシサーバ:

ポート:

ユーザー:

パスワード:

< 戻る スキップ 次へ >

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、Trend Micro Control Manager (以下、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** — [アップデートおよび Web レピュテーションのクエリ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、ユーザー名、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。

InterScan MSS
手順 3 / 7

LDAP 設定

LDAP 設定は、ユーザグループ定義、管理者権限、または Web 隔離認証に LDAP を使用する場合にのみ入力します。Web 隔離ツールを使用するには、LDAP を有効にする必要があります。

LDAP 設定

LDAP サーバの種類: Microsoft Active Directory

☒ 有効 LDAP1

LDAP サーバ:
例: example.com または 192.168.10.1

待ちポート番号:

☐ 有効 LDAP2

LDAP サーバ:
例: example.com または 192.168.10.1

待ちポート番号:

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

キャッシュ生存期限 (分):

LDAP 管理者

LDAP 管理者アカウント:

パスワード:

基本識別名:
例: DC=fbo, DC=fboonet, DC=org

認証方法:
☒ 簡易
☐ 詳細: Active Directory に対して Kerberos 認証を使用する
 Kerberos 認証の初期設定のレルム:
 初期設定のドメイン:
 発行局 (KDC) および管理サーバ:
 発行局 (KDC) ポート番号:

< 戻る スキップ 次へ >

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。

表 1-1. LDAP 管理設定

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

- 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。

InterScan MSS
手順 4/7

内部アドレス

内部ドメイン (既知のユーザまたはドメイン) を定義します。InterScan MSS では、この情報に基づいて **メッセージが受信が送信か** を判断し、レポートやルールを作成を行います。

内部ドメインおよびユーザグループ

ドメインの入力

インポート

選択済み

LDAP: TRENDMASTER@mssgrp

*

< 戻る 次へ >

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。
2. 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。
 - [インポート] ボタンをクリックして、定義済みのドメイン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 では、1 つのテキストファイルからのみドメインをインポートできます。テキストファイルで、1 行に 1 つのドメイン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、ドメインを指定できます。たとえば、「*.com」または「*.example.com」のように指定します。

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。

The screenshot shows the 'Control Manager サーバの設定' (Control Manager Server Settings) window in InterScan MSS. The window has a title bar with 'InterScan MSS' and '手順5/7'. Below the title bar is a blue help icon. The main content area is titled 'Control Manager サーバの設定' and contains the following fields and options:

- A checkbox labeled 'Control Manager エージェントを有効にする' (Enable Control Manager Agent) is checked.
- A text field labeled 'サーバ:' (Server) is empty.
- Radio buttons for '通信プロトコル:' (Communication Protocol): 'HTTP ポート番号:' (HTTP Port Number) is selected with a value of '80', and 'HTTPS ポート番号:' (HTTPS Port Number) is unselected with a value of '443'.
- Text fields for 'Webサーバ認証:' (Web Server Authentication): 'ユーザ名:' (Username) is empty, and 'パスワード:' (Password) is masked with dots.
- A section titled 'プロキシ設定' (Proxy Settings) contains:
 - A checkbox labeled 'プロキシを有効にする' (Enable Proxy) is unchecked.
 - A dropdown menu for 'プロキシタイプ:' (Proxy Type) is set to 'HTTP'.
 - A text field for 'プロキシサーバ:' (Proxy Server) is empty.
 - A text field for 'ポート:' (Port) is empty.
 - A text field for 'ユーザ名:' (Username) is empty.
 - A text field for 'パスワード:' (Password) is masked with dots.

At the bottom of the window are three buttons: '< 戻る' (Back), 'スキップ' (Skip), and '次へ >' (Next).

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、[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 であり、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)」をアクティベートします。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。

InterScan MSS
手順6/7

アクティベート

検索とコンテンツのアップデートを有効にするには、**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。スパムメール対策に対する保護を有効にするには、スパムメール対策 (コンテンツ検索) IP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していない場合は、レジストレーションキーを使用してオンライン登録を実行してください。

[オンライン登録](#)

アクティベーションコードの入力	
InterScan MSS (ウイルス対策およびコンテンツフィルタ)	XX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX
スパムメール対策 (コンテンツ検索)	XX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX

[< 戻る](#) [次へ >](#)

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。

管理コンソールのパスワードを変更する

トレンドマイクロでは、管理コンソールへのアクセスに使用するパスワードを定期的に変更することをお勧めします。

管理コンソールのパスワードを変更するには

1. [管理] → [パスワード] の順に選択します。
2. 現在のパスワードと新しいパスワードを入力し、新しいパスワードを確認します。
パスワードには、4 ～ 32 文字の英数字を使用してください。
3. [保存] をクリックします。

警告： 初期設定の管理者パスワードをそのまま使用している場合、そのパスワードを直ちに変更することを強くお勧めします。

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します。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、Control Manager を使用して InterScan MSS を管理している場合は、Control Manager 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、アップデート元またはプロキシ設定を指定してください。

アップデート元を指定するには

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。

アップデート 

スケジュール **アップデート元**

コンポーネントをアップデートするためのアップデート元を選択します。InterScan MSS がネットワーク上のプロキシサーバにアクセスする必要がある場合は、プロキシの設定を行います。

アップデート元

☒ トrendマイクロのアップデートサーバ

☐ その他のインターネット上のサーバ

http://

プロキシ設定

☐ アップデートおよびWebレビデーションのクエリにプロキシサーバを使用する

プロキシタイプ: HTTP

プロキシサーバ:

ポート:

ユーザ名:

パスワード:

確定 キャンセル

3. [アップデート元] で、次のいずれかを選択します。
 - ・ トrendマイクロのアップデートサーバ — 最新コンポーネントの初期設定の提供元です。
 - ・ その他のインターネット上のサーバ — Control Manager サーバ等のアップデート元を指定します。

4. アップデートサーバ、製品登録サーバ、および Web レピュテーションサーバに接続する際、プロキシサーバを経由する必要がある場合、[アップデートおよび Web レピュテーションのクエリにプロキシサーバを使用する] を選択して、次の項目を設定します。
 - **プロキシタイプ** — [HTTP]、[SOCKS4]、または [SOCKS5] を選択します。
 - **プロキシサーバ** — プロキシサーバのホスト名または IP アドレスを入力します。
 - **ポート** — プロキシサーバがインターネットに接続するために使用するポートを入力します。
 - **ユーザ名** — プロキシサーバに管理者としてアクセスするためのユーザ名を入力します。
 - **パスワード** — 上記に対応するパスワードを入力します。
5. [保存] をクリックします。
設定ウィザードを使用している場合は、[次へ] 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する必要があります。

- 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。[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。

接続の有効化

☒ SMTP接続を許可する
 ☐ IPフィルタを有効にする
 ☐ ERS
 ☐ IPプロファイラ

コンポーネント 前回の表示更新: 2009/07/23 11:03:15

☐ 名前	現在のバージョン	利用可能なバージョン	アップデートスケジュール
☐ 検索エンジン	8.950.1092	8.700.1004	15 分
☐ ウイルスパターンファイル	6.157.00	6.157.00	15 分
☐ スパイウェアパターンファイル	0.773.00	0.773.00	15 分
☐ IntelliTrap パターンファイル IntelliTrap 除外ファイル	0.113.00 0.435.00	0.113.00 0.435.00	15 分
☐ スпамメール検索エンジン	5.600.1016	5.600.1016	15 分
☐ スпамメール判定ルール	16672.006	16780.005	15 分
☐ URLフィルタエンジン	3.000.1029	3.000.1027	15 分
InterScan MSS	Version 7.1 - Build_Linux_1230	該当なし	該当なし

管理下のサーバ設定

ホスト名	接続	検索サービス	ポリシーサービス	Web 隔離
------	----	--------	----------	--------

2. [コンポーネント] で、InterScan MSS がネットワークを保護するために使用するウイルス対策、スパイウェア対策、およびスパムメール対策のコンポーネントのバージョン番号を確認します。
3. 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。
4. [アップデート] 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

ウイルス対策とスパムメール対策のコンポーネントを定期的にダウンロードすることを忘れた場合は、ネットワークはインターネット上の脅威に対して無防備になります。アップデートプロセスを自動化するには、この画面で予約アップデートを設定します。ネットワークで利用できるインターネット帯域幅が限られている場合は、予約アップデートを混雑していない時間に実行するように設定します。

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。

アップデート ?

スケジュール
アップデート元

☒ 予約アップデートを有効にする

コンポーネントのアップデート

☒ ウイルス検索エンジン

☒ ウイルスパターンファイル

☒ スパイウェアパターンファイル
IntelliTrapパターンファイル
IntelliTrap除外ファイル
IntelliTrap除外ファイル

☒ スパムメール検索エンジン

☒ スパムメール判定ルール

☒ URLフィルタエンジン

アップデートスケジュール

☒ 間隔 (分) 15

☐ (毎時) 00

☐ (毎日) 0 : 00

☐ (毎週) 日曜日 0 : 00

保存 キャンセル

2. [予約アップデートを有効にする] チェックボックスをオンにします。

3. [コンポーネントのアップデート] で、アップデートするコンポーネントを選択します。すべてのコンポーネントをアップデートすることをお勧めします。
4. [アップデートスケジュール] で、アップデートの頻度を選択します。
 - **間隔 (分)** — 1 時間内に指定した間隔でアップデートを実行します。間隔 (分) を選択します。たとえば、15 を選択すると、毎時 0 分、15 分、30 分、45 分にアップデートされます。30 を選択すると、毎時 0 分と 30 分にアップデートされます。
 - **毎時** — 1 時間に 1 回アップデートを実行します。アップデートを実行する時刻 (分) を選択してください。たとえば、15 を選択すると、毎時 15 分にアップデートされます。
 - **毎日** — 1 日に 1 回アップデートを実行します。アップデートを実行する時刻 (時、分) を選択してください。
 - **毎週** — 1 週間に 1 回アップデートを実行します。アップデートを実行する曜日と時刻 (時、分) を選択してください。
5. [保存] をクリックします。

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についてはインストールまたは起動のいずれかを選択できます。

- **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 7.1 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します。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。

InterScan MSS サービスを開始または停止するには

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。

概要 [? 詳細な情報](#)

InterScan MSS (ウイルス対策およびコンテンツフィルタ) はアクティベートされていません。
セキュリティ対策を最新に保つためには、製品のアクティベーションが必要です。 [詳細な情報](#)

スパムメール対策 (コンテンツ検索) はアクティベートされていません。
セキュリティ対策を最新に保つためには、製品のアクティベーションが必要です。 [詳細な情報](#)

システム **統計**

接続の有効化

☒ SMTP接続を許可する ☐ IPフィルタを有効にする [?](#) ☐ POP3接続を許可する ☐ ERS ☐ IPプロファイラ [保存](#)

コンポーネント 前回の表示更新: 2009/07/23 9:34:18 [表示更新](#)

[アップデート](#) [ロールバック](#)

名前	現在のバージョン	利用可能なバージョン	アップデートスケジュール
☐ 検索エンジン	8.950.1092	8.700.1004	15 分
☐ ウイルスパターンファイル	6.157.00	6.157.00	15 分
☐ スパイウェアパターンファイル	0.773.00	0.773.00	15 分
☐ IntelliTrapパターンファイル IntelliTrap除外ファイル	0.113.00 0.435.00	0.113.00 0.435.00	15 分
☐ スпамメール検索エンジン	5.600.1016	5.600.1016	15 分
☐ スпамメール判定ルール	16672.006	16672.006	15 分
☐ URLフィルタエンジン	3.000.1029	3.000.1027	15 分
InterScan MSS	Version 7.1 – Build Linux1230	該当なし	該当なし

管理下のサーバ設定

ホスト名	接続	検索サービス	ポリシーサービス	Web隔離
post.tremice1.com	☒	☒ 開始	☒ 開始	☒ 開始

2. [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 設定の設定。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。181 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。

プログラムがインストールされているコンピュータから、またはネットワークを経由したりリモート操作で、エンドユーザメール隔離管理コンソールを表示できます。

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、インターネットブラウザに次の URL を入力します。

- 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`

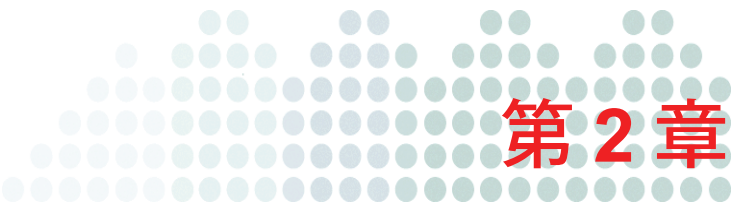
警告： セカンダリエンドユーザメール隔離サービスのすべての管理コンソールへ正常にアクセスするには、ネットワーク上にあるすべてのエンドユーザメール隔離サービスのシステム時間を同期させる必要があります。

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

InterScan MSS の設定

この章では、Trend Micro InterScan Messaging Security Suite 7.1（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。

- 36 ページの「IP フィルタサービス」
- 53 ページの「SMTP メッセージを検索する」
- 61 ページの「ドメインベース配信について」
- 64 ページの「POP3 メッセージを検索する」

IP フィルタサービス

IP フィルタサービスには、Email Reputation Services (ERS) 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。

- Email Reputation Services (ERS) 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。

Email 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。Email Reputation Services (ERS) 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

ERS および IP プロファイラからなる 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。

ERS の設定の詳細については、41 ページの「IP フィルタを設定する」を参照してください。

Email Reputation Services で使用するための MTA を準備する

契約する Email Reputation Services の種類に応じて適切な DNS クエリを実行するように MTA を設定します。

- **ERS Standard:** 550 レベルエラーコード (connection refused) で接続をブロックします。IP アドレスが標準レピュテーションデータベースに既知のスパムメール送信元として登録されている場合、MTA は接続を開始しようとするサーバにこのエラーコードを返します。
- **ERS Advanced:** 2 つの DNS クエリを実行するように MTA を設定します。MTA は、標準レピュテーションデータベースへの最初のクエリから応答を受信しなかった場合、動的レピュテーションデータベースへの 2 番目のクエリを実行します。肯定応答をこのデータベースから受信した場合は、MTA は、接続を一時的に拒否する 450 レベルのエラーコード (server temporarily unavailable, please retry) を返します。その際、応答をこのデータベースから受信します。

動的レピュテーションデータベースには、信用できないホストが一時的にスパムメールを送信している正当なメールサーバが記録されている場合があります。接続要求が正当な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。このプロセスにより、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。

一部のサーバには、疑わしい IP 接続を処理する追加オプションがあります。これらのオプションには、より詳細な検索を行うためのメッセージの絞り込みやルーティングなどがあります。

MTA またはファイアウォールの設定方法は、次のトレンドマイクロの Web サイトを参照してください。

<https://tmspn.securecloud.com/>

これらの設定方法は、製品 (MTA またはファイアウォール) のベンダが提供しています。詳細な設定および設定オプションについては、製品マニュアルを参照するか、テクニカルサポート組織に問い合わせてください。

注意： アクティベーションコードを挿入して設定方法の例のテキストを置き換えます。ダッシュ (-) を入力する必要はありません。

ERS 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、ERS 設定の作成や管理などの管理作業を実行する場合は、ERS 管理コンソールにログインします。

このセクションでは、ERS 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、ERS 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。

ERS 管理コンソールを開くには

1. Web ブラウザを開き、次のアドレスを入力します。

<https://tmspn.securecloud.com/>

2. Email Reputation Services のユーザ名とパスワードを使用してログオンします。Smart Protection Network ポータルが開き、[Email] タブが選択され、[一般] 画面が表示されます。
3. 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。[グローバルスパムメール情報] 画面が表示されます。

[グローバルスパムメール情報] 画面では、受信したスパムメールの量に基づいて、ISP のランクが付けられます。[ISP 毎の送信量] リストには、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が表示されます。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。[ISP 毎の送信量] リストには次の項目が表示されます。

表 2-1. ISP スパムメールリスト

列	説明
ランク (今週)	今週のグローバルランクをスパムメールの総量に基づいて表示します。
ランク (先週)	先週のグローバルランクをスパムメールの総量に基づいて表示します。
ASN	Autonomous System Number (ASN) は、1 社以上の通信事業者が運営する、明確に定義された単一のルーティングポリシーを持つ IP ネットワークのグループに対するグローバル一意識別子です。
ISP 名	特定の ASN に対する登録名。一部の ISP では複数の ASN を保有していることがあります。この場合、テーブルに複数個登録されます。
スパムメール量 (24 時間)	過去 24 時間内に送信されたスパムメールの推定総量。この総量は 1 時間ごと更新されます。

表 2-1. ISP スпамメールリスト (続き)

列	説明
ボットネット活動	メールサーバに対するボットネットの活動状況の指標。ボットネットとは、中央からスパムメール送信元によって制御されている、ウイルスに感染したコンピュータのグループのことであり、現在インターネット上で最大のスパムメール送信元となっています。この数値は、1 時間前からのボット数におけるパーセント比率の変化を示します。ボットネットの活動を確認するには、[有効なメールサーバ] リストにメールサーバを追加する必要があります。

4. リリースアップデート をクリックします。リリースアップデート画面が表示されます。
リリースアップデート画面には、新しいスパムメールに関する最新情報と、Email Reputation Services で使用可能な新機能が表示されます。次のタブをクリックすると情報が表示されます。
 - **スパムメール情報** 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。
 - **リリース情報** Email Reputation Services で使用可能な新機能の概要について説明します。
5. MTA と ERS データベースサーバ間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。サブメニューが表示されます。
 - b. 次のいずれかをクリックします。

表 2-2. レポートの種類

レポート	説明
クエリの割合	このレポートは、IP アドレスの一致を返したクエリのパーセント比率を表示します。IP アドレスの一致は、メールサーバとの接続を確立しようとする送信者が、既知のスパムメール送信元であることを示します。レポートは、個々のスパムメールメッセージではなく、接続に基づいて作成されます。
1 時間あたりのクエリ数	このレポートは、メールサーバがレピュテーションデータベースにクエリを実行した回数を表示します。
1 日あたりのクエリ数	このレポートは、メールサーバがレピュテーションデータベースにクエリを実行した 1 日あたりの回数を表示します。

表 2-2. レポートの種類 (続き)

レポート	説明
ボットネット レポート	このレポートは、有効なメールサーバとして登録されているサーバを発信元とする、過去 7 日間のスパムメール活動の簡単な概要を示します。指定した IP アドレスのいずれかにおいて、過去 7 日間にスパムメール活動が見つかった場合には、赤いロボットアイコンが表示されます。

6. ERS 設定によって提供される保護を管理するには
 - a. メニューから [ポリシー] を選択します。サブメニューが表示されます。
 - b. 次のいずれかをクリックします。

表 2-3. ポリシー設定

ポリシー	説明
設定	承認済み送信者リストとブロックする送信者リストを設定します。 国別または ISP 別の個々の IP アドレスおよび CIDR ごとに、リストを定義できます。 ・ 承認済み送信者：承認済み送信者からのメッセージを許可して、IP レベルのフィルタを無視します。承認済み送信者リストは MTA に適用されませんが、追加の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を設定したり、MTA に対して追加のフィルタを実行することができます。 ・ ブロックする送信者：特定の国、ISP、および IP アドレスからのメールメッセージを常にブロックするように ERS に指示します。
新規 ISP の リクエスト	トレンドマイクロでは、サービスに追加する他のインターネットサービスプロバイダ (ISP) に関する、お客さまからの助言をお待ちしています。 できる限り多くの ISP に関する情報を記入してください。この情報は、トレンドマイクロが ISP をサービスに追加するのに役立ちます。
Reputation 設定	ERS Standard と ERS Advanced の各設定を行います。 標準のお客さまには、[Standard 設定を有効にする] のみが表示されます。 詳細のお客さまには、[Dynamic 設定] セクションと [Standard 設定を有効にする] セクションの両方が表示されます。

7. 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、または ERS にメールサーバを追加するには、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 フィルタを設定するには、次の手順を実行します。

- 手順 1 — ERS 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 — ERS 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: ERS および IP プロファイラを有効にする

ERS 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。

IP フィルタの概要



IP フィルタを有効にする

☒ ERS ☒ IP プロファイラ

保存

ブロックされたドメインIPアドレス

表示更新 過去1日間 (過去24時間)

DHA変更

ドメイン	IPアドレス	破棄された接続数
最近1日間にブロックされたドメインまたはIPアドレスはありません。		

バウンスメール

ドメイン	IPアドレス	破棄された接続数
最近1日間にブロックされたドメインまたはIPアドレスはありません。		

ウイルス

ドメイン	IPアドレス	破棄された接続数
最近1日間にブロックされたドメインまたはIPアドレスはありません。		

スパムメール

ドメイン	IPアドレス	破棄された接続数
最近1日間にブロックされたドメインまたはIPアドレスはありません。		

手動

ドメイン	IPアドレス	破棄された接続数
最近1日間にブロックされたドメインまたはIPアドレスはありません。		

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、ERS 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、[メールレピュテーション] 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 ERS 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、ERS および IP プロファイラの動作を停止できません。ERS 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 7.1 インストールガイド」の「Email Reputation Services と IP プロファイラ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

すべての IP アドレスの動作を監視するためのルールが設定され、そのしきい値設定に従ってそれらがブロックされます。次のルールを設定できます。

- スパムメール
- ウイルス
- DHA 攻撃
- バウンスメール

警告： IP プロファイラのルールを有効にする前に、(メールメッセージを InterScan MSS に送信する) すべてのメールサーバの IP アドレスを IP フィルタの承認済みリストに追加します。IP フィルタの承認済みリストを設定するには、51 ページの「手順 4: IP アドレスを承認済みリストへ追加する」を参照してください。

スパムメールの IP フィルタの設定を指定するには

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。

ルール: IPプロファイラ設定

すべてのIPアドレスの動作を監視し、しきい値の設定に従ってブロックするルールが設定されています。

スパムメール ウイルス DHA攻撃 バウンスメール

☒ 有効にする

監視期間: 20 時間

比率: 80 %

総メール数: 1000

処理: 一時的にブロック

保存 キャンセル 既定値に戻す

スパムメール **ウイルス** DHA攻撃 バウンスメール

☒ 有効にする

監視期間: 20 時間

比率: 80 %

総メール数: 1000

処理: 一時的にブロック

保存 キャンセル 既定値に戻す

スパムメール ウイルス **DHA攻撃** バウンスメール

☒ 有効にする

設定例

監視期間: 20 時間

比率: 80 %

総メール数: 1000

送信先数: 100

存在しない受信者数: 0

(LDAPサービスが実行中の場合)

処理: 一時的にブロック

保存 キャンセル 既定値に戻す

スパムメール ウイルス DHA攻撃 **バウンスメール**

☒ 有効にする

監視期間: 20 時間

比率: 80 %

総メール数: 1000

処理: 一時的にブロック

保存 キャンセル 既定値に戻す

2. [スパムメール] タブをクリックします。[スパムメール] 画面が表示されます。
3. スパムメールのブロックを有効にするには、[有効にする] チェックボックスをオンにします。
4. 次の値を指定します。
 - **監視期間** — InterScan MSS でメールトラフィックを監視するうえで、スパムメールメッセージの割合が設定したしきい値を超えていないかどうかを確認する単位期間 (時間数)。
 - **比率 (%)** — スパムメールメッセージについて許可する割合 (分子) を入力します。
 - **総メール数** — しきい値の割合が算出されるスパムメールメッセージの総数を入力します。次の例で考えます。
監視期間: 1 時間、比率: 20、総メール数: 100

スパムメールのブロックが有効な間の 1 時間ごとで、受信したメッセージの 20% を超えるメッセージがスパムメールであり、かつメッセージの総数が 100 を超える場合に、InterScan MSS は配信元アドレスによるブロックを開始します。

5. [処理] で次のいずれかを選択します。

- **一時的にブロック** : その IP アドレスからのメールメッセージをブロックし、アップストリーム MTA に再試行を許可します。
- **常にブロック** : その IP アドレスからの今後のメールメッセージを永続的にブロックします。アップストリーム MTA は再試行を実行できません。

6. [保存] をクリックします。

ウイルスの IP フィルタの設定を指定するには

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。

ルール: IP プロファイラ設定

すべての IP アドレスの動作を監視し、しきい値の設定に従ってブロックするルールが設定されています。

スパムメール ウイルス DHA攻撃 バウンスメール

☒ 有効にする

監視期間: 20 時間

比率: 80 %

総メール数: 1000

処理: 一時的にブロック

保存 キャンセル 既定値に戻す

スパムメール **ウイルス** DHA攻撃 バウンスメール

☒ 有効にする

監視期間: 20 時間

比率: 80 %

総メール数: 1000

処理: 一時的にブロック

保存 キャンセル 既定値に戻す

スパムメール ウイルス **DHA攻撃** バウンスメール

☒ 有効にする

設定別

監視期間: 20 時間

比率: 80 %

総メール数: 1000

送信先数: 100

存在しない受信者数: 0
(LDAPサービスが実行中の場合)

処理: 一時的にブロック

保存 キャンセル 既定値に戻す

スパムメール ウイルス DHA攻撃 **バウンスメール**

☒ 有効にする

監視期間: 20 時間

比率: 80 %

総メール数: 1000

処理: 一時的にブロック

保存 キャンセル 既定値に戻す

2. [ウイルス] タブをクリックします。[ウイルス] 画面が表示されます。

3. ウイルスの脅威のブロックを有効にするには、[有効にする] チェックボックスをオンにします。
4. 次の項目を設定します。
 - **監視期間**： InterScan MSS でメールトラフィックを監視するうえで、ウイルス脅威のあるメールメッセージの割合が設定したしきい値を超えていないかどうかを確認する単位期間 (時間数)。
 - **比率 (%)**: ウイルス脅威のあるメールメッセージについて許可する割合 (分子) を入力します。
 - **総メール数** — しきい値の割合が算出されるウイルスに感染したメールメッセージの総数 (分母) を入力します。

次の例で考えます。
監視期間 : 1 時間、比率 : 20、総メール数 : 100
ウイルスのブロックが有効な間の 1 時間ごとで、受信したメッセージの 20% を超えるメッセージにウイルス脅威が含まれ、かつメッセージの総数が 100 を超える場合に、InterScan MSS は配信元 IP アドレスによるブロックを開始します。
5. [処理] で次のいずれかを選択します。
 - **一時的にブロック** : その IP アドレスからのメールメッセージをブロックし、アップストリーム MTA に再試行を許可します。
 - **常にブロック** : その IP アドレスからの今後のメールメッセージを永続的にブロックします。アップストリーム MTA は再試行を実行できません。
6. [保存] をクリックします。

ディレクトリハーベスト攻撃 (DHA) の設定を指定するには

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。

ルール: IPプロファイラ設定

すべてのIPアドレスの動作を監視し、しきい値の設定に従ってブロックするルールが設定されています。

スパムメール ウイルス DHA攻撃 バウンスメール

☒ 有効にする

監視期間: 20 時間

比率: 80 %

総メール数: 1000

処理: 一時的にブロック

保存 キャンセル 既定値に戻す

スパムメール ウイルス DHA攻撃 バウンスメール

☒ 有効にする

監視期間: 20 時間

比率: 80 %

総メール数: 1000

処理: 一時的にブロック

保存 キャンセル 既定値に戻す

スパムメール ウイルス DHA攻撃 バウンスメール

☒ 有効にする

設定例

監視期間: 20 時間

比率: 80 %

総メール数: 1000

送信先数: 100

存在しない受信者数: 0
(LDAPサービスが実行中の場合)

処理: 一時的にブロック

保存 キャンセル 既定値に戻す

2. [DHA 攻撃] タブをクリックします。[DHA 攻撃] 画面が表示されます。
3. ディレクトリハーベスト攻撃のブロックを有効にするには、[有効にする] チェックボックスをオンにします。
4. 次の項目を設定します。
 - **監視期間**: InterScan MSS でメールトラフィックを監視するうえで、DHA 攻撃を示すメールメッセージの割合が設定したしきい値を超えていないかどうかを確認する単位期間 (時間数)。
 - **比率 (%)**: DHA 脅威のあるメールメッセージについて許可する割合 (分子) を入力します。
 - **総メール数** — しきい値の割合が算出される DHA メールメッセージの総数 (分母) を入力します。

- **送信先数** — しきい値に許可される最大受信者数を入力します。
- **存在しない受信者数** — しきい値に許可される最大の存在しない受信者数を入力します。
DHA 攻撃には、受信者リスト内にランダムに生成されたメールアドレスが含まれることがあります。

注意： 実在しない受信者を識別するには、LDAP サービスが実行されている必要があります。

次の例で考えます。

監視期間：1 時間、比率：20、総メール数：100、送信先数：10 を超える、存在しない受信者数：5 を超える

DHA のブロックが有効な間の 1 時間ごとで、組織内の受信者以外の 5 人を超える受信者を含む 10 人を超える受信者に送信されたメッセージの 20% を超えるメッセージを受信し、かつメッセージの総数が 100 を超える場合に、InterScan MSS は配信元 IP アドレスによるブロックを開始します。

ヒント： 厳密に言うと、LDAP サーバは必須ではありません。InterScan MSS の DHA ルールは、Postfix から返された DHA の結果を取得することができます。Postfix が次にこれらの結果を LDAP サーバ経由またはその他の手段で FoxProxy に渡します。FoxProxy は結果を分析して DHA 攻撃かどうか判断します。

LDAP サーバは、ユーザのメールボックスが存在するかどうかを Postfix が調べる手段の 1 つにすぎません。

5. [処理] で次のいずれかを選択します。
 - **一時的にブロック**：その IP アドレスからのメールメッセージをブロックし、アップストリーム MTA に再試行を許可します。
 - **常にブロック**：その IP アドレスからの今後のメールメッセージを永続的にブロックします。アップストリーム MTA は再試行を実行できません。
6. [保存] をクリックします。

バウンスメールの設定を指定するには

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。

ルール: IPプロファイラ設定

すべてのIPアドレスの動作を監視し、しきい値の設定に従ってブロックするルールが設定されています。

スパムメール ウイルス DHA攻撃 バウンスメール

☒ 有効にする

監視期間: 20 時間

比率: 80 %

総メール数: 1000

処理: 一時的にブロック

保存 キャンセル 既定値に戻す

スパムメール ウイルス DHA攻撃 バウンスメール

☒ 有効にする

監視期間: 20 時間

比率: 80 %

総メール数: 1000

処理: 一時的にブロック

保存 キャンセル 既定値に戻す

スパムメール ウイルス DHA攻撃 バウンスメール

☒ 有効にする

監視期間: 20 時間

比率: 80 %

総メール数: 1000

送信先数: 100

存在しない受信者数: 0
(LDAPサービスが実行中の場合)

処理: 一時的にブロック

保存 キャンセル 既定値に戻す

2. [バウンスメール] タブをクリックします。[バウンスメール] 画面が表示されます。
3. バウンスメールのブロックを有効にするには、[有効にする] チェックボックスをオンにします。
4. 次の項目を設定します。
 - **監視期間**: InterScan MSS でメールトラフィックを監視するうえで、バウンスメールを示すメールメッセージの割合が設定したしきい値を超えていないかどうかを確認する単位期間 (時間数)。
 - **比率 (%)**: バウンスメールを示すメールメッセージについて許可する割合 (分子) を入力します。
 - **総メール数** — しきい値の割合が算出されるバウンスメールメッセージの総数 (分母) を入力します。

次の例で考えます。

監視期間 : 1 時間、比率 : 20、総メール数 : 100

バウンスメールのブロックが有効な間の 1 時間ごとで、受信したメッセージの 20% を超えるメッセージがバウンスメッセージであり、かつメッセージの総数が 100 を超える場合に、InterScan MSS は配信元アドレスによるブロックを開始します。

注意： バウンスメールをチェックするには、LDAP サービスが実行されている必要があります。

5. [処理] で次のいずれかを選択します。

- **一時的にブロック** : その IP アドレスからのメールメッセージをブロックし、アップストリーム MTA に再試行を許可します。
- **常にブロック** : その IP アドレスからの今後のメールメッセージを永続的にブロックします。アップストリーム MTA は再試行を実行できません。

6. [保存] をクリックします。

手順 3: ERS を設定する

ERS を設定するには

1. メニューから、[IP フィルタ] → [メールレピュテーション] の順に選択します。[メールレピュテーション] 画面が表示されます。

メールレピュテーション

Email Reputation Servicesでは、新しいスパムメールやフィッシングメールの発信元を特定する動的な評価データベースと共に、世界最大の、最も信頼されている評価データベースの1つを使用して、受信メールメッセージのIPアドレスを確認し、ソニーやポットネットの最初の出現時にそれらが実行されるのを阻止します。

メールレピュテーションの設定

☒ メールレピュテーションを有効にする

グローバルスパムメール情報およびレポートの表示、送信者IPアドレスの承認済みリストおよびブロックリストの作成または管理、管理タスクの実行、およびサービスの設定。
[メールレピュテーションのポータル](#)

サービスのレベルの設定

☐ 標準: 標準評価データベースを使用して、既知のスパムメールの発信元からのメッセージをブロックします。
[クリックすると詳細が表示されます。](#)

☒ 初期設定の推奨処理
 RBL+ Service のデータベースに一致するIPアドレスからの接続を常時拒否 (応答コード: 550)

☐ 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: (範囲 400 ~ 599、初期設定値=550)
 SMTPエラー文字列:

☒ 詳細: 標準評価データベースと動的評価データベースの両方を使用して、スパムメールの既知の発信元および疑わしい発信元からのメッセージをブロックします。
[クリックすると詳細が表示されます。](#)

☒ 初期設定の推奨処理
 RBL+ Service のデータベースに一致するIPアドレスからの接続を常時拒否 (応答コード: 550)
 Network Anti-Spam Service (GIL) のデータベースに一致するIPアドレスからの接続を一時拒否 (応答コード: 450)

☐ 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: (範囲 400 ~ 599、初期設定値=450)
 SMTPエラー文字列:

2. [メールレピュテーションを有効にする] チェックボックスをオンにします。
3. サービスのレベルに応じて、次のいずれかのオプションを選択し、設定を行います。

標準:

- **初期設定の推奨処理** — ERS は、RBL+ に一致する接続を常時拒否 (応答コード: 550) 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ブロックします。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。

詳細:

- **初期設定の推奨処理** — ERS 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ブロックします。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。

承認済みリスト

追加 削除		1-1 / 1		ページ 1	1 / 1
☐	ドメイン	IPアドレス	日時	ステータス	
☐	trendmicro.com	該当なし	2007/08/06 15:04:40		
表示: 15件/ページ					

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。

IP/ドメインの承認済みリストへの追加

☒ 有効にする

☒ ドメイン:

☐ IPアドレス:

3. [有効にする] チェックボックスをオンにします。

- 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。
- [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

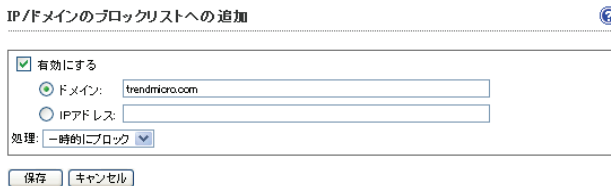
InterScan MSS では、ブロックリストに表示される IP アドレスがブロックされます。

ブロックリストに IP アドレスを追加するには

- 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。



- [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。



- [有効にする] チェックボックスをオンにします。
- ドメインまたは IP アドレスを入力します。
- [一時的にブロック] または [常にブロック] を選択します。
- [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。

疑わしい IP アドレスおよびドメインを表示する

検索条件に違反するメールメッセージを送信したにもかかわらず、メッセージの合計数が任意の期間に対して設定したしきい値を超えていないためにまだブロックされていない IP アドレスまたはドメインについて、InterScan MSS はログエントリを作成します。

疑わしい IP アドレスとドメインを表示するには

1. [IP フィルタ] → [疑わしい IP] の順にクリックします。
2. 次の条件のいずれかを選択してください。
 - [種類] で、IP フィルタで検出された脅威の種類の横にあるチェックボックスをオンにします。
 - [日時] で、InterScan MSS によって送信者をブロックした日付と時間の範囲を選択します。
 - 問い合わせる特定の IP アドレスがわかっている場合は、[IP アドレス] の横に入力します。
 - その IP アドレスの対応するドメイン名を表示するには、[ドメイン名を表示] チェックボックスをオンにします。
 - [表示件数] の横で、一度に画面に表示するログエントリの数を選択します。
3. [ログ表示] をクリックします。
4. 次のいずれかの処理を実行してください。
 - その IP アドレスを一時的にブロックするには、リストの対応するチェックボックスをオンにしてから、[一時的にブロック] をクリックします。
 - その IP アドレスを永続的にブロックするには、リストの対応するチェックボックスをオンにしてから、[常にブロック] をクリックします。
 - リストで同時に表示される項目数を変更するには、表の上部にあるドロップダウンボックスから新しい表示値を選択します。
 - 表を並べ替えるには、列のタイトルをクリックします。

SMTP メッセージを検索する

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します。

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 7.1 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 接続を有効にします。

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。

概要

InterScan MSS (ウイルス対策およびコンテンツフィルタ) はアクティベートされていません。
セキュリティ対策を最新に保つためには、製品のアクティベーションが必要です。 [詳細な情報](#)

スパムメール対策 (コンテンツ検索) はアクティベートされていません。
セキュリティ対策を最新に保つためには、製品のアクティベーションが必要です。 [詳細な情報](#)

システム **統計**

接続の有効化

☒ SMTP接続を許可する
 ☐ IPフィルタを有効にする
 ☐ POP3接続を許可する
 ☐ NRS
 ☐ IPプロファイラ
 [保存](#)

コンポーネント 前回の表示更新: 2007/11/17 9:27:21 [表示更新](#)

[アップデート](#) [ロールバック](#)

名前	現在のバージョン	利用可能なバージョン	アップデートスケジュール
☐ 検索エンジン	8.31.0.1.002	8.500.1.001	15 分
☐ ウイルスパターンファイル	4.197.00	4.829.00	15 分
☐ スパイウェアパターンファイル	0.451.00	0.553.00	15 分
☐ IntelliTrap パターンファイル IntelliTrap 除外ファイル	0.1.03.00 0.1.69.00	0.1.07.00 0.253.00	15 分
☐ スпамメール検索エンジン	3.8.1.026	5.0.1.023	15 分
☐ スпамメール判定ルール	1.49.46.000	1.555.0.002	15 分
InterScan MSS	Version 7.0- Build_Linux_x3138	該当なし	該当なし

管理下のサーバ設定

ホスト名	接続	検索サービス	ポリシーサービス	Web隔離
IMSS-JPLX01	☒	☒ 開始	☒ 開始	☒ 開始

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] 画面では、SMTP のグリーティングメッセージやメール処理キューの場所などの、MTA の SMTP 設定を実行します。InterScan MSS は、メッセージをいったんこのメール処理キューに保存してから、これらのメッセージをウイルス検索して配信します。

SMTP の設定を指定するには

1. [管理] → [InterScan MSS の設定] → [SMTP ルーティング] の順にクリックします。[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。
このオプションは、[SMTP]、[接続]、[メッセージルール]、および [ドメインベース配信] タブで行ったすべての設定を、同じ InterScan MSS 管理データベースに接続されているすべての検索サービスに適用します。
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。

SMTPルーティング 

☐ すべての検索サービスに適用

SMTP **接続** メッセージルール ドメインベース配信

SMTP インタフェース

IPアドレス:

ポート番号:

タイムアウト: 分 (非アクティブ状態の経過時間)

同時接続数: ☐ 無制限 ☒ 接続数 まで許可する

接続制御

コンピュータからサーバへの接続を許可または拒否できます。

☒ 次のリストに含まれているコンピュータを除くすべての接続を許可する

☐ コンピュータ別の指定

例: 192.168.1.0.1

☐ グループ別の指定

サブネットアドレス

サブネットマスク <<"/>

例: 10.123.123.123

サブネットマスク

例: 255.255.255.0

☐ 次のリストに含まれているコンピュータを除くすべての接続を拒否する

Transport Layer Security 設定

☐ Transport Layer Securityを有効にする

☐ TLSによるSMTP接続のみを許可する

CA証明書:

秘密鍵:

SMTPサーバ証明書:

3. [SMTP インタフェース] の設定を指定します。
 - IP アドレス — SMTP サーバに接続するためのインタフェースを選択します。
 - 127.0.0.1: SMTP サーバは、ローカルコンピュータの IP アドレスでのみ待機します。

- **すべてのインタフェース** — このコンピュータ上に複数の IP アドレスがある場合、SMTP サーバは使用可能なすべての IP アドレスで待機します。
 - **ポート番号** — SMTP サーバの待機ポートを入力します。
 - **タイムアウト**: {} 分 (非アクティブ状態の経過時間) — タイムアウト値を入力します。
 - **同時接続数** — [無制限] をクリックするか、[接続数 {} まで許可する] をクリックして最大接続数を入力します。
4. [接続制御] の設定を指定します。
- **次のリストに含まれているコンピュータを除くすべての接続を許可する** — 次の項目を使用して「拒否リスト」を設定します。
 - **コンピュータ別の指定** — IP アドレスを入力してから、[>>] をクリックしてその IP アドレスをリストに追加します。
 - **グループ別の指定** — サブネットアドレスとサブネットマスクを入力してから、[>>] をクリックしてそのグループをリストに追加します。
 - **インポート** — ファイルから「拒否リスト」をインポートする場合にクリックします。IP リストのテキストファイルのサンプルの内容は、次のとおりです。


```
192.168.1.1
192.168.2.0:255.255.255.0
192.168.3.1:255.255.255.128
192.168.4.100
192.168.5.32:255.255.255.192
```
 - **次のリストに含まれているコンピュータを除くすべての接続を拒否する** — 次の項目を使用して「許可リスト」を設定します。
 - **コンピュータ別の指定** — IP アドレスを入力してから、[>>] をクリックしてその IP アドレスをリストに追加します。
 - **グループ別の指定** — サブネットアドレスとサブネットマスクを入力してから、[>>] をクリックしてそのグループをリストに追加します。
 - **インポート** — ファイルから「許可リスト」をインポートする場合にクリックします。IP リストのテキストファイルのサンプルの内容は、次のとおりです。


```
192.168.1.1
192.168.3.1:255.255.255.128
192.168.4.100
192.168.5.32:255.255.255.192
```
5. [Transport Layer Security 設定] を指定します。
- a. [Transport Layer Security を有効にする] を選択します。

このオプションを使用すると、InterScan MSS SMTP サーバが SMTP クライアントに Transport Layer Security (TLS) サポートを提供できますが、クライアントが接続を確立する際に TLS 暗号化を使用する必要はありません。

- b. [TLS による SMTP 接続のみを許可する] を選択すると、InterScan MSS は安全な受信接続のみを受け入れます。

このオプションを使用すると、InterScan MSS SMTP サーバは TLS 接続を介してのみメッセージを受け入れることができます。

- c. 次のいずれかの横にある [参照] ボタンをクリックします。

- **CA 証明書** — 通常、CA 証明書は SMTP クライアントの確認に使用されます。しかし、InterScan MSS では、クライアントは確認されず、CA 証明書は TLS 接続の有効化にのみ使用されます。

このファイルは、公開鍵とともに提供されている場合に限りアップロードされます。それ以外の場合は、TLS 接続を有効化する際にこのファイルは必須とはなりません。

- **秘密鍵** — SMTP クライアントで、InterScan MSS SMTP サーバの公開鍵と暗号化鍵を使用して乱数が暗号化され、セッション鍵が生成されます。

InterScan MSS SMTP サーバは、公開鍵を使用してその乱数を復号化し、安全な接続を確立します。

TLS 接続を有効にするためにこの鍵をアップロードする必要があります。

- **SMTP サーバ証明書** — InterScan MSS SMTP サーバの公開鍵は、SMTP クライアントがセッション鍵を生成するために公開されます。

TLS 接続を有効にするためにこの鍵をアップロードする必要があります。

- d. [アップロード] をクリックして、そのファイルを InterScan MSS サーバ上に保存します。

6. [保存] をクリックします。

メッセージルールを設定する

InterScan MSS が処理できるメールメッセージの制限を設定して、メールリレーを制御するには、[メッセージルール] 画面ですべての項目を設定してください。

メールリレー

スパムメール送信者が InterScan MSS MTA をスパムメールの中継点として利用することを防止するために、ネットワーク上のメールアドレスを [リリードメイン] リストに追加して、リレー制御を設定してください。InterScan MSS は、メールメッセージを受信すると、そのメールの最終宛先を確認してこのリストと比較します。次の場合は、メッセージは破棄されます。

- 宛先ドメインがこのリストにない
- 宛先ドメインの親ドメインがこのリストにない
- ホストが [メッセージリレーの許可] リストにない

リリードメインの設定はドメインベース配信の設定とは異なります。詳細については、61 ページの「ドメインベース配信について」を参照してください。

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。

SMTPLルーティング ?

☐ すべての検索サービスに適用

SMTP 接続 **メッセージルール** ドメインベース配信

メッセージの制限

制限を設定しない場合は、「0」を入力してください。

最大メッセージサイズ (1 ~ 無制限) MB

最大受信者数 (1 ~ 99999)

リレードメイン

次に指定したドメインへのあらゆるホストからのメッセージをリレーすることができます。通常は、イントラネット内のすべてのメールサーバーを追加します。

ドメインの追加

例: example.com >>

 <<

メッセージリレーの許可

次に指定したホストは、リレー制限の対象から除外され、すべてのドメインにメッセージをリレーすることができます。

☐ ホストのみ

☒ ホストと同じサブネット

☐ ホストと同じIPクラス

☐ 指定のIPアドレス:

☒ コンピュータ別の指定

例: 192.168.1.0.1

☐ グループ別の指定

サブネットアドレス >>

例: 10.123.123.123

サブネットマスク <<

例: 255.255.255.0

3. [メッセージの制限] の設定を指定します。
 - ・ **最大メッセージサイズ** — メガバイト数を入力します。
 - ・ **最大受信者数** — 1 ~ 99999 の間で、受信者数を入力します。
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。

ヒント： インポート時に、最良の結果を得るには、正確なドメインとすべてのサブドメインの両方をインポートします。

ドメインリストのテキストファイルのサンプルの内容は、次のとおりです。

- **domain.com:** Imports the exact domain
- ***.domain.com:** Imports all sub-domains
- **domain.org:** Imports the exact domain

注意： インポートされたファイルは、1 行に 1 つのドメインを含むテキストファイルでなければなりません。ドメインを指定するときは、ワイルドカードを使用できます。

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について

InterScan MSS は、受信者のメールアドレスのドメイン名に基づいてルーティングテーブルを管理します。そして、このルーティングテーブルを使用して、ドメインベースの配信を通して (受信者メールアドレスに適合した) メールを指定された SMTP サーバに転送します。他のすべてのドメイン宛てのメッセージは、ドメインネームサーバ (DNS) のレコードを基にルーティングされます。

リリードドメインとドメインベース配信

SMTP ルーティングのメッセージルール用に設定するリリードドメインの設定は、ドメインベース配信の設定とは異なります。

リリードドメイン — InterScan MSS は、リリードドメイン宛てのメールメッセージだけを中継します。たとえば、リリードドメインとして domain.com だけが指定されている場合、InterScan MSS は domain.com ドメイン宛てに送信されたメールメッセージだけを中継します。

ドメインベース配信 — InterScan MSS は、ドメインベースでメールを配信します。たとえば、配信ドメインを domain.com と指定し、SMTP サーバの IP アドレスを 10.10.10.10、ポートを 25 とした場合、domain.com 宛てに送信されたメールはすべてポート 25 経由で SMTP サーバ 10.10.10.10 に配信されます。

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確認して、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。

ドメインベース配信リストをインポートするときには、1 行に 1 つのエントリを指定します。各エントリの内容は、次のようになります。

[ドメイン名], [サーバ名または IP アドレス] : [ポート番号]

たとえば、次のエントリはすべて有効です。

- domain1.com,192.168.1.1:2000
- domain2.net,192.168.2.2:1029
- domain3.com,smtp.domain3.com:25
- domain4.com,mail.domain4.com:2000

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。

SMTPルーティング

☐ すべての検索サービスに適用

SMTP 接続 メッセージルール **ドメインベース配信**

ドメインベース配信

追加 削除 インポート エクスポート 0-0 / 0 ページ 1

☐ ドメイン 配信方法

15件/ページ

保存 キャンセル

3. [ドメインベース配信] の下の [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。

送信先ドメイン

名前:

配信方法

送信先ドメインに対して使用する配信方法を設定します。
次のSMTPサーバにメールを転送する:

サーバアドレス ポート番号

OK 閉じる

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。

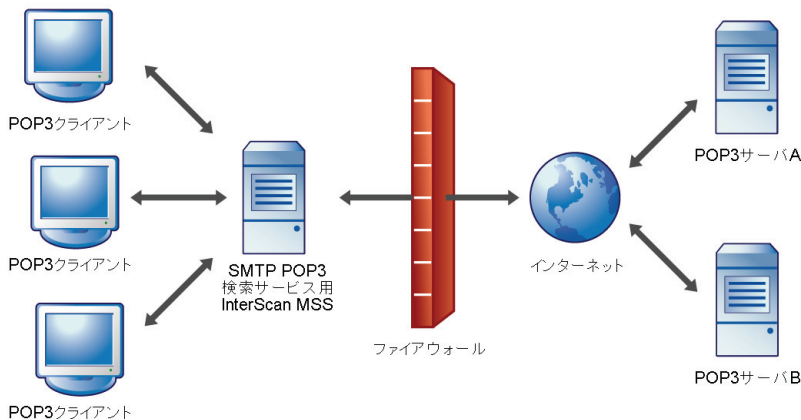
POP3 メッセージを検索する

SMTP トラフィックの他に、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 POP3 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 POP3 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、InterScan MSS サーバを除くネットワーク上の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 設定を指定します。

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。

概要 ?

 InterScan MSS (ウイルス対策およびコンテンツフィルタ) はアクティベートされていません。
セキュリティ対策を最新に保つためには、製品のアクティベーションが必要です。 [詳細な情報](#)

 スпамメール対策 (コンテンツ検索) はアクティベートされていません。
セキュリティ対策を最新に保つためには、製品のアクティベーションが必要です。 [詳細な情報](#)

システム 統計

接続の有効化

☒ SMTP接続を許可する
 ☐ IPフィルタを有効にする
 ☒ POP3接続を許可する
 ☐ NRS
 ☐ IPプロファイラ
 保存

コンポーネント 前回の表示更新: 2007/11/17 9:27:21 表示更新

アップデート ロールバック

名前	現在のバージョン	利用可能なバージョン	アップデートスケジュール
☐ 検索エンジン	8.31.0.1002	8.500.1.001	15 分
☐ ウイルスパターンファイル	4.197.00	4.829.00	15 分
☐ スパイウェアパターンファイル	0.451.00	0.553.00	15 分
☐ IntelliTrap パターンファイル IntelliTrap 除外ファイル	0.103.00 0.169.00	0.107.00 0.253.00	15 分
☐ スпамメール検索エンジン	3.8.1.026	5.0.1.023	15 分
☐ スпамメール判定ルール	1.49.46.000	1.555.0.002	15 分
InterScan MSS	Version 7.0- Build_Linux3138	該当なし	該当なし

管理下のサーバ設定

ホスト名	接続	検索サービス	ポリシーサービス	Web隔離
IMSSJPLX01		 開始	 開始	 開始

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 を設定する

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)、専用の接続を設定してカスタムポートを割り当てることもできます。

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。

接続 ?

コンポーネント LDAP **POP3** データベース Control Managerサーバ

一般的なPOP3接続

ユーザが要求した任意のPOP3サーバ

受信InterScan MSSポート:

専用のPOP3接続

受信POP3ポート	POP3サーバ	POP3サーバポート

メッセージテキスト

ユーザが受信しようとしているメッセージがフィルタされる場合、次のテキストがユーザに送信されます。通知は、[通知設定] 画面で選択した文字セットを使用して送信されます。

専用のPOP3接続

InterScan MSS受信POP3ポート番号:

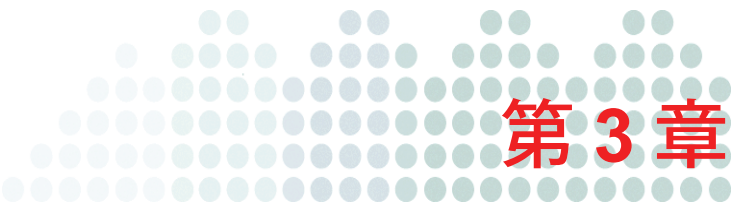
POP3サーバのサーバ名またはIPアドレス:

ポート番号:

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。



第3章

ポリシーの管理

本章では、InterScan MSS ポリシーの作成、変更、および管理の手順について説明します。

この章の内容は次のとおりです。

- 70 ページの「ポリシーの管理」
- 72 ページの「共通のポリシーオブジェクトの設定」
- 92 ページの「内部アドレスを設定する」
- 96 ページの「ポリシーを追加する」
- 97 ページの「ルートを指定する」
- 104 ページの「検索条件を指定する」
- 118 ページの「処理を指定する」
- 127 ページの「ポリシーを完成させる」
- 129 ページの「既存のポリシーを変更する」
- 131 ページの「ポリシーの例 1」
- 134 ページの「ポリシーの例 2」
- 137 ページの「アスタリスクワイルドカードを使用する」
- 138 ページの「検索除外を設定する」

ポリシーの管理

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。初期設定では、InterScan MSS には、ウイルスなどのインターネット上の脅威からネットワークを保護するためのグローバルウイルス対策ルールが組み込まれています。ウイルス対策ルールは、システムに害を与える可能性のある最も危険な種類のメッセージを対象としています。したがって、InterScan MSS でトラフィックにウイルスが含まれていないか最初に分析できるように、このルールを常にルールリストの一番上に配置しておく必要があります。

ウイルス対策ルールは、スパムメール対策に対応していません。適切にスパムメールに対処するには、検索条件にスパムメールを含むカスタムルールを設定して、IP フィルタ製品をアクティベートしてください。

注意： 新しいポリシーを作成する前に、内部アドレスが定義されていることを確認してください。

Policy Manager の仕組み

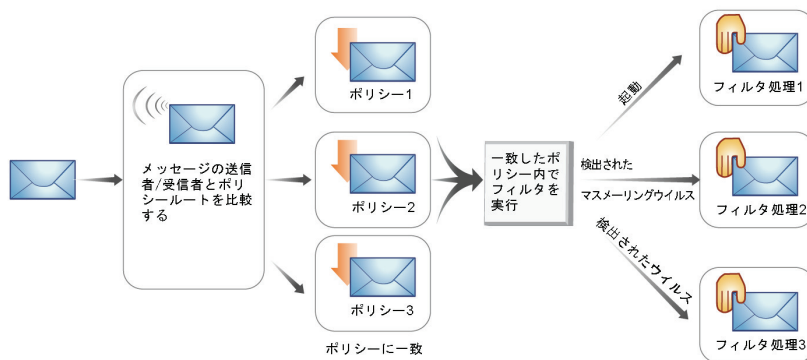
次の種類のポリシーに対して複数のルールを作成できます。ポリシーを使用して、メッセージングシステムに対するセキュリティ上の脅威を抑制し、生産性の低下を防ぎます。

- **ウイルス対策：**メッセージ内のウイルスおよびその他の不正プログラム (スパイウェアやワームなど) を検索します。
- **その他：**スパムメール / フィッシングメッセージ、メッセージコンテンツ、およびその他の添付ファイルの条件を検索します。

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。

図 3-1. Policy Manager のプロセスフローの簡略図



ポリシーの作成方法の詳細については、96 ページの「ポリシーを追加する」を参照してください。

ポリシーリストに表示されるポリシーのフィルタを実行するには

1. [ポリシー] → [ポリシーリスト] の順にクリックします。[ポリシー] 画面が表示されます。
2. 次の [フィルタ] オプションを設定します。
 - a. ルートの指定：
 - **すべてのルート**：すべてのポリシーを表示します。
 - **受信**：受信メッセージのみを監視するポリシーを表示します。
 - **送信**：送信メッセージのみを監視するポリシーを表示します。
 - **両方向**：「受信」、「送信」、「受信および送信」メッセージを監視するポリシーを表示します。
 - **POP3**：POP3 メッセージのみを監視するポリシーを表示します。
 - b. ポリシーが提供する保護の種類の指定：
 - **すべての種類**
 - **ウイルスと不正プログラム**
 - **スパムメール/フィッシングメール**

- Web レピュテーション
 - 添付ファイル
 - コンテンツ
 - サイズ
 - その他
- c. ポリシーが保護するユーザの指定:
- すべてのグループ
 - [ユーザまたはグループの検索]

共通のポリシーオブジェクトの設定

共通のポリシーオブジェクトとは、すべてのポリシーで共有できる項目です。これにより、管理者は簡単にポリシーを作成できるようになります。

表 3-1. 共通のポリシーオブジェクト

共通のポリシーオブジェクト	説明
アドレスグループ	複数のメールアドレスを 1 つのグループにまとめます。
キーワードおよび式	情報漏えいを防止し、スパムメールや中傷メールがネットワークに侵入するのをブロックするためのキーワードを作成します。
ポリシー通知	受信者またはメール管理者に、InterScan MSS がメッセージの添付ファイルに対して処理を実行したことや、メッセージが InterScan MSS ルールの検索条件に違反していることを通知するメッセージを作成します。
スタンプ	受信者に、InterScan MSS がメッセージの添付ファイルに対して処理を実行したことや、メッセージがルールの検索条件に違反していることを通知するスタンプを作成します。
DKIM 承認済みリスト	リストに一致したドメインからの DKIM 署名があるメッセージは、検索されたりスパムメールとしてマークされたりすることはありません。

表 3-1. 共通のポリシーオブジェクト

共通のポリシーオブジェクト	説明
Web レピュテーション 承認済み リスト	Web レピュテーション承認済みリストに記載されているドメインは、Web レピュテーションフィルタによって検索されたりブロックされたりすることはありません。ただし、他のフィルタにより、Web レピュテーション承認済みリストのメッセージがブロックされる場合があります。

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。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。

たとえば、企業のメールシステムを使用して送信しないようにする 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作成する

アドレスグループとは、組織内の複数のユーザのメールアドレスの集合です。アドレスグループを作成すると、各メールアドレスにルールを個別に適用する代わりに、複数のメールアドレスに一括してルールを適用できます。

ポリシーを作成する前、またはポリシー作成時に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。アドレスグループは、手動で作成することも、1行につき1つのメールアドレスが含まれているテキストファイルからインポートすることもできます。

ヒント： アドレスグループはポリシー作成時に作成できますが、ポリシーを作成する前に作成しておくことをお勧めします。

アドレスグループを作成するには

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

アドレスグループの追加

アドレスグループ > アドレスグループの追加

アドレスグループには、メールアドレスまたはワイルドカードメイン (例: *@example.com、*@*.example.com など) を含められます。

アドレスグループ名:		
アドレス:		追加
		インポート
		削除
		エクスポート

3. グループ名を入力して、次のいずれかを実行します。

個々のアドレスの追加：

- 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、「*@example.com」のように入力します。

アドレスリストのインポート：

- a. [インポート] をクリックします。アドレスグループをインポートする画面が表示されます。

- b. インポートするファイルパスとファイル名を入力するか、[参照] をクリックしてファイルを見つけます。
- c. 次のいずれかを選択します。
 - 現在のリストにマージする
 - 現在のリストを上書きする
- d. [インポート] をクリックします。

注意： InterScan MSS 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、「*@example.com」のように入力します。

4. [保存] をクリックします。[アドレスグループ] テーブルに新しいアドレスグループが表示された [アドレスグループ] 画面が現れます。

ポリシー作成時にアドレスグループを追加する

ポリシー作成時にアドレスグループを追加する

ポリシー作成時にルートを指定する際、アドレスグループを作成できます。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。

注意： InterScan MSS 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、「*@example.com」のように入力します。

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作成します。[手順 1: 受信者と送信者の選択] 画面が表示されます。
4. [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。

次の宛先への受信メッセージ ?

ルールを追加 > 次の宛先への受信メッセージ

保存 キャンセル

アドレスの選択

☐ すべてのユーザ
☒ 選択したアドレスのいずれか

LDAPユーザまたはグループの検索

メールアドレスの入力

アドレッシンググループの検索

アドレスグループの選択

選択済み

追加 >

保存 キャンセル

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。

次の宛先への受信メッセージ ?

ルールを追加 > 次の宛先への受信メッセージ

保存 キャンセル

アドレスの選択

☐ すべてのユーザ
☒ 選択したアドレスのいずれか

アドレスグループの選択

選択済み

追加 >

追加
編集
削除

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。

アドレスグループの追加



アドレスグループ > アドレスグループの追加

アドレスグループには、メールアドレスまたはワイルドカードメイン (例: *@example.com、*@*.example.com など) を含められます。

アドレスグループ名:		
アドレス:		追加
		インポート
		削除
		エクスポート

7. グループ名を入力して、次のいずれかを実行します。

個々のアドレスの追加:

- 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、「*@example.com」のように入力します。

アドレスリストのインポート:

- a. [インポート] をクリックします。アドレスグループをインポートする画面が表示されます。
- b. インポートするファイルパスとファイル名を入力するか、[参照] をクリックしてファイルを見つけます。
- c. 次のいずれかを選択します。
 - 現在のリストにマージする
 - 現在のリストを上書きする
- d. [インポート] をクリックします。

注意: InterScan MSS 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、「*@example.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

アドレスグループは、[アドレスグループ] 画面から編集または削除できます。既存のポリシーを編集して、編集または削除することもできます。

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] → [アドレスグループ] の順にクリックします。[アドレスグループ] 画面が表示されます。
2. アドレスグループを編集するには
 - a. [アドレスグループ] テーブルの既存のアドレスグループをクリックします。アドレスグループの追加 / 編集の画面が表示されます。
 - b. 必要に応じて、アドレスグループを編集します。
 - c. [保存] をクリックします。[アドレスグループ] 画面が表示されます。
3. アドレスグループを削除するには
 - a. アドレスグループの横にあるチェックボックスをオンにします。
 - b. [削除] をクリックします。

既存のポリシーの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。

次の宛先への受信メッセージ ?

ルールを追加 > 次の宛先への受信メッセージ

保存 キャンセル

アドレスの選択

☐ すべてのユーザ
☒ 選択したアドレスのいずれか

メールアドレスの入力 追加 >

選択済み

sujaatha@trendmaster.com	

保存 キャンセル

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。

次の宛先への受信メッセージ ?

ルールを追加 > 次の宛先への受信メッセージ

保存 キャンセル

アドレスの選択

☐ すべてのユーザ
☒ 選択したアドレスのいずれか

アドレスグループの選択 追加 >

選択済み

GROUP: lmsgrp	

追加 編集 削除

保存 キャンセル

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。

アドレスグループをエクスポートする

他の InterScan MSS サーバにインポートするアドレスグループをエクスポートします。既存のポリシーまたは [アドレスグループ] リストからエクスポートします。

アドレスグループをエクスポートするには

1. メニューから、[ポリシー] → [アドレスグループ] の順に選択します。[アドレスグループ] 画面が表示されます。
2. エクスポートするアドレスグループをクリックします。[アドレスグループ] 画面が表示されます。
3. [エクスポート] をクリックします。[ファイルのダウンロード] 画面が表示されます。
4. [保存] をクリックします。[名前を付けて保存] ダイアログボックスが表示されます。
5. アドレスグループをエクスポートする名前と場所を指定します。
6. [保存] をクリックします。

既存のポリシーからアドレスグループをエクスポートするには

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。[アドレスグループ] 画面が表示されます。
6. [エクスポート] をクリックします。[ファイルのダウンロード] 画面が表示されます。
7. [保存] をクリックします。[名前を付けて保存] ダイアログボックスが表示されます。
8. アドレスグループをエクスポートする名前と場所を指定します。
9. [保存] をクリックします。

キーワード表現リストを使用する

InterScan MSS では、件名、本文、またはヘッダのコンテンツに基づいて、メールメッセージに対する処理を実行できます。メッセージコンテンツを基準にフィルタを実行するには、キーワードまたは正規表現をキーワード表現リストに追加します。複数のキーワードリストを設定し、そのリストをいつでも有効にしたり無効にしたりすることができます。既存のリストとほとんど同じリストを設定する場合は、リストをコピーし、コピーしたリストを編集します。

コンテンツの検索条件を選択するには

1. 「その他」の（ウイルス対策でない）ポリシーを作成または変更します。
 - 新しいルールを作成する方法の詳細については、96 ページの「ポリシーを追加する」を参照してください。
 - 既存のルールを変更する方法の詳細については、129 ページの「既存のポリシーを変更する」を参照してください。
2. [検索条件] 画面の [コンテンツ] で、コンテンツの条件を適用するメールメッセージ部分の横のチェックボックスをオンにします。
3. コンテンツ条件を設定するメールメッセージ部分を指定するリンクをクリックします。次の 2 つの列が表示されている [キーワード] 画面が表示されます。
 - **利用可能**: キーワードは利用可能ですが、現在使用されていません。
 - **選択済み**: キーワードは現在使用中です。
4. ヘッダのキーワードを設定している場合は、キーワードを適用するヘッダ項目の横にあるチェックボックスをオンにします。
5. [追加] をクリックします。キーワード表現を管理する画面が表示されます。
6. キーワードを設定します。
7. [利用可能] リストで、有効にするキーワードリストをクリックします。
8. [➤] をクリックします。キーワードが [選択済み] リストに表示されます。

キーワードリストを利用可能な状態にしておき、InterScan MSS で一時的に使用しないようにするには、選択されたリストでキーワードをクリックしてから [◀] をクリックします。
9. [保存] をクリックします。ルールの追加リストが表示されます。

キーワードを設定する

キーワードおよび正規表現を設定して、InterScan MSS でメールメッセージのコンテンツを検索できるようにします。[キーワードおよび式] 画面で、またはルール作成時に、キーワードを作成できます。

ヒント: キーワードはポリシー作成時に作成できますが、ポリシーを作成する前に作成しておくことをお勧めします。

キーワードを作成するには

1. [ポリシー] → [キーワードおよび式] の順にクリックします。[キーワードおよび式] 画面が表示されます。
2. [追加] をクリックします。ルールを追加 / キーワード画面が表示されます。
3. [リスト名] の横に、わかりやすい名前を入力します。
4. [キーワード] の横で、次のいずれかを選択し、InterScan MSS が処理を実行するタイミングを指定します。
 - **指定した任意のキーワード**: メールメッセージのコンテンツが、リスト内の任意のキーワードに一致するとき。
 - **指定したすべてのキーワード**: メールメッセージのコンテンツが、リスト内のすべてのキーワードに一致するとき。
 - **指定した以外のキーワード**: メールメッセージのコンテンツが、リスト内のどのキーワードにも一致しないとき。
 - **合計スコアがしきい値を超える場合のみ**: [処理が実行される総メッセージスコア] の横に、許可されるキーワード表現の最大スコアを表す値を入力します。キーワードを追加すると、キーワードにスコアを設定できます。
5. キーワードを作成するには、[追加] をクリックします。[キーワードの追加] リストが表示されます。
6. キーワードを入力します。部分一致の場合は、キーワードを入力してください。完全一致を指定するには、キーワードの前後に「¥s」（「」は不要）を使用してください。
以下に例を示します。
 - 「keyword」は、「keywords」、「akeyword」などと一致します。
 - 「¥skeyword¥s」は、「keyword」とのみ一致します。
7. [保存] をクリックします。キーワード / 正規表現のリストが表示されます。
8. フィルタの使用時に、メールコンテンツの大文字 / 小文字が区別されるようにする場合は、[大文字と小文字の区別] のチェックボックスをオンにします。
9. [合計スコアがしきい値を超える場合のみ] を選択した場合は、ドロップダウンボックスからスコアを選択します。
10. [保存] をクリックします。テーブルに新しいキーワードが表示された [キーワードおよび式] 画面が現れます。

ポリシーの作成または変更時にキーワードを追加または編集するには

1. 「その他」の（ウイルス対策でない）ポリシーを作成または変更します。
 - 新しいルールを作成する方法の詳細については、96 ページの「ポリシーを追加する」を参照してください。
 - 既存のルールを変更する方法の詳細については、129 ページの「既存のポリシーを変更する」を参照してください。
2. [検索条件] 画面の [コンテンツ] で、コンテンツの条件を設定するメールメッセージ部分のリンクをクリックします。次の 2 つの列が表示されている [キーワード] 画面が表示されます。
3. [キーワード] 画面で [追加] または [編集] をクリックします。キーワード表現リストの設定画面が表示されます。
4. [リスト名] の横に、わかりやすい名前を入力します。
5. [キーワード] の横で、次のいずれかを選択し、InterScan MSS が処理を実行するタイミングを指定します。
 - **指定した任意のキーワード**: メールメッセージのコンテンツが、リスト内の任意のキーワードに一致するとき。
 - **指定したすべてのキーワード**: メールメッセージのコンテンツが、リスト内のすべてのキーワードに一致するとき。
 - **指定した以外のキーワード**: メールメッセージのコンテンツが、リスト内のどのキーワードにも一致しないとき。
 - **合計スコアがしきい値を超える場合のみ**: [処理が実行される総メッセージスコア] の横に、許可されるキーワード表現の最大スコアを表す値を入力します。キーワードを追加すると、キーワードにスコアを設定できます。
6. キーワードを作成するには、[追加] をクリックします。[キーワードの追加] リストが表示されます。
7. キーワードを入力します。部分一致の場合は、単純にキーワードを入力してください。完全一致を指定するには、キーワードの前後に「¥s」（「」は不要）を使用してください。
以下に例を示します。
 - 「keyword」は、「keywords」、「akeyword」などと一致します。
 - 「¥skeyword¥s」は、「keyword」とのみ一致します。
8. [合計スコアがしきい値を超える場合のみ] を選択した場合は、ドロップダウンボックスからスコアを選択します。
9. [保存] をクリックします。キーワード表現リストの設定画面が再び現れ、キーワードがリストで表示されます。

10. フィルタの使用時に、メールコンテンツの大文字 / 小文字が区別されるようにする場合は、[大文字と小文字の区別] のチェックボックスをオンにします。
11. [保存] をクリックして、ポリシーの変更または作成を続けます。

通知リストを使用する

受信者またはメール管理者に、InterScan MSS がメッセージの添付ファイルに対して処理を実行したことや、メッセージが InterScan MSS ルールの検索条件に違反していることを通知するには、通知を送信します。

ポリシー通知リストに追加する方法の詳細については、86 ページの「ポリシー通知を追加または変更する」を参照してください。

ポリシー通知を送信するには

1. ポリシーを作成または変更します。
 - 新しいルールを作成する方法の詳細については、96 ページの「ポリシーを追加する」を参照してください。
 - 既存のルールを変更する方法の詳細については、129 ページの「既存のポリシーを変更する」を参照してください。
2. ポリシーの変更または作成中に、[処理の選択] 画面の [監視] で、[ポリシー通知の送信] をクリックします。次の 2 つの列が表示されている [ポリシー通知] 画面が開きます。
 - **利用可能**: 通知メッセージは利用可能ですが、現在使用されていません。
 - **選択済み**: 通知メッセージは現在使用中です。
3. 通知を追加または変更します。
4. [利用可能] リストで、有効にする通知をクリックします。
5. [>] をクリックします。通知が [選択済み] リストに表示されます。

通知を利用可能な状態にしておき、InterScan MSS で一時的に使用しないようにするには、選択されたリストで通知をクリックしてから [<] をクリックします。
6. [保存] をクリックして、ポリシーの作成または変更を続けます。

ポリシー通知を追加または変更する

[ポリシー通知] 画面で、あるいはポリシー通知の作成または変更時に、ポリシー通知を作成します。

ヒント: キーワードはポリシー作成時に作成できますが、ポリシーを作成する前に作成しておくことをお勧めします。

ポリシー通知を追加または変更するには

1. [ポリシー] → [ポリシー通知] の順にクリックします。[ポリシー通知] 画面が表示されます。
2. [追加] をクリックします。[通知設定] 画面が表示されます。
3. 次の項目を設定します。
 - **通知名:** 通知のわかりやすい名前を入力します。
 - **差出人:** 送信者メールアドレスを入力します。
 - **宛先:** 受信者メールアドレスを入力し、[元のメール送信者] と [元のメール受信者] の横にあるチェックボックスの両方、またはいずれかをオンにします。各アドレスはセミコロン (;) で区切ります。
 - **件名:** 通知の件名を入力します。
 - **メッセージ:** 通知メッセージを入力します。
4. 元のメッセージを通知メッセージの添付ファイルとして送信するには、[メッセージの添付] の横にあるチェックボックスをオンにします。
5. メッセージに挿入できる変数の種類を表示するには、[変数リスト] をクリックします。
6. SNMP トラップを送信するには、以下を設定します。
 - a. 次のいずれかをクリックします。
 - **無効 (最初のラジオボタン):** トラップ ID を送信しないようにします。
 - **2 番目のラジオボタン:** 初期設定の SNMP トラップのいずれかを選択します。
 - **3 番目のラジオボタン:** カスタムのトラップ ID を入力します。
 - b. **メッセージ:** 通知メッセージを入力します。
7. [保存] をクリックします。

ポリシーの作成または変更時にポリシー通知を追加または変更するには

1. ポリシーを作成または変更します。
 - 新しいルールを作成する方法の詳細については、96 ページの「ポリシーを追加する」を参照してください。

- 既存のルールを変更する方法の詳細については、129 ページの「既存のポリシーを変更する」を参照してください。
2. [処理の選択] 画面の [監視] で、[ポリシー通知の送信] をクリックします。次の 2 つの列が表示されている [通知] 画面が開きます。
 - **利用可能**: 通知メッセージは利用可能ですが、現在使用されていません。
 - **選択済み**: 通知メッセージは現在使用中です。
 3. [追加] または [編集] をクリックします。通知の設定画面が表示されます。
 4. メール通知を送信するには、以下を設定します。
 - **通知名**: 通知のわかりやすい名前を入力します。
 - **差出人**: 送信者メールアドレスを入力します。
 - **宛先**: 受信者メールアドレスを入力し、[元のメール送信者] と [元のメール受信者] の横にあるチェックボックスの両方、またはいずれかをオンにします。各アドレスはセミコロン (;) で区切ります。
 - **件名**: 通知の件名を入力します。
 - **メッセージ**: 通知メッセージを入力します。
 5. 元のメッセージを通知メッセージの添付ファイルとして送信するには、[メッセージの添付] の横にあるチェックボックスをオンにします。
 6. メッセージに挿入できる変数の種類を表示するには、[変数リスト] をクリックします。
 7. SNMP トラップを送信するには、以下を設定します。
 - a. 次のいずれかをクリックします。
 - **無効 (最初のラジオボタン)**: トラップ ID を送信しないようにします。
 - **2 番目のラジオボタン**: 初期設定の SNMP トラップのいずれかを選択します。
 - **3 番目のラジオボタン**: カスタムのトラップ ID を入力します。
 - b. **メッセージ**: 通知メッセージを入力します。
 8. [保存] をクリックします。

スタンプを使用する

InterScan MSS がメッセージの添付ファイルに対して処理を実行したことや、メッセージがルール
の検索条件に違反していることを受信者に通知するには、メールメッセージ本文の先頭または末尾
にスタンプを追加します。

ヒント： スタンプは、本来の受信者が最終的に受信するメールにのみ追加してください。検索条
件に違反するメッセージを削除するルールを設定している場合は、スタンプを追加する
必要はありません。

ポリシーでスタンプを使用するには

1. ポリシーを作成または変更します。
 - 新しいルールを作成する方法の詳細については、96 ページの「ポリシーを追加する」を参照してください。
 - 既存のルールを変更する方法の詳細については、129 ページの「既存のポリシーを変更する」を参照してください。
2. [処理の選択] 画面でポリシーを作成または変更する際、[変更] の [本文にスタンプを挿入] または [本文に安全スタンプを挿入] の横にあるチェックボックスをオンにします。

スタンプを作成する

[スタンプ] 画面で、あるいはポリシーの作成または変更時に、スタンプを作成します。

ヒント： スタンプはポリシー作成時に作成できますが、ポリシーを作成する前に作成しておく
ことをお勧めします。

スタンプを作成するには

1. [ポリシー] → [スタンプ] の順にクリックします。[スタンプ] 画面が表示されます。
2. [追加] をクリックするか、スタンプリストから編集するスタンプを選択します。[新しいスタン
プ] 画面が表示されます。
3. [名前] の横に、スタンプの名前を入力します。
4. [挿入位置] の横の [メッセージ本文の末尾] または [メッセージ本文の先頭] をクリックします。
5. [テキスト] にメッセージを入力します。メッセージに挿入できる変数の種類を表示するには、
[変数リスト] をクリックします。

6. TNEF エンコードされたメッセージやデジタル署名付きのメッセージを破損する危険性を回避するには、[TNEF エンコードされたメッセージおよびデジタル署名されたメッセージにスタンプを挿入しない] を選択します。
7. [保存] をクリックして [スタンプ] 画面に戻ります。

ポリシーの作成または変更時にスタンプを作成するには

1. ポリシーを作成または変更します。
 - 新しいルールを作成する方法の詳細については、96 ページの「ポリシーを追加する」を参照してください。
 - 既存のルールを変更する方法の詳細については、129 ページの「既存のポリシーを変更する」を参照してください。
2. [処理の選択] 画面の [変更] で、[本文にスタンプを挿入] または [本文に安全スタンプを挿入] の横にある [編集] をクリックします。[スタンプ] 画面が開いて、使用可能なスタンプが表示されます。
3. 新しいスタンプを追加するには、[追加] をクリックします。既存のスタンプを変更するには、リストボックスでそのスタンプをクリックしてから [編集] をクリックします。編集画面が表示されます。
4. [名前] の横に、スタンプの名前を入力します。
5. [挿入位置] の横の [メッセージ本文の末尾] または [メッセージ本文の先頭] をクリックします。
6. [テキスト] にメッセージを入力します。メッセージに挿入できる変数の種類を表示するには、[変数リスト] をクリックします。
7. TNEF エンコードされたメッセージやデジタル署名付きのメッセージを破損する危険性を回避するには、[TNEF エンコードされたメッセージおよびデジタル署名されたメッセージにスタンプを挿入しない] を選択します。
8. [保存] をクリックして [スタンプ] 画面に戻ります。
9. [完了] をクリックします。

DKIM 承認済みリストを使用する

DKIM (DomainKeys Identified Mail) は、インターネット転送時のメールの検証方法を提供する、署名 / 暗号ベースのメール認証です。InterScan MSS は、メールが正当な送信元から送信されたことを認証することによって、ネットワークをスパムメールやフィッシングから保護します。認証されたメールメッセージはスパムメールとしてマークされないため、スパムメールに関する検索は実行されません。つまり、安全だと認識されているソースからのメールメッセージを検索する必要性が減るため、誤検出も減ります。

DKIM 承認済みリストを有効にするには

1. [ポリシー] → [DKIM 承認済みリスト] の順にクリックします。[DKIM 承認済みリスト] 画面が表示されます。
2. [ポリシーで使用するために DKIM 承認済みリストを有効にする] チェックボックスをオンにします。
3. リストに既知の安全なドメインを入力します。

手動:

- a. ドメイン名を入力します。
- b. [追加] をクリックします。

リストのインポート:

注意: DKIM 承認済みリストにテキストファイルをインポートする場合、各行に 1 つのドメインのみが記入されていることを確認してください。

- a. [インポート] をクリックします。[DKIM ホワイトリストのインポート] 画面が表示されます。
 - b. ファイルパスとファイル名を入力するか、[参照] をクリックしてファイルを見つけます。
 - c. 次のいずれかを選択します。
 - 現在のリストにマージする
 - 現在のリストを上書きする
 - d. [インポート] をクリックします。
4. [保存] をクリックします。

Web レピュテーション承認済みリストを使用する

Web レピュテーションを使用すると、メールメッセージに埋め込まれた不正 URL からネットワーク上のユーザを保護できます。Web レピュテーションでは、メールメッセージ内の URL を検索し、トレンドマイクロの Web レピュテーションデータベースにある既知の不正 URL と比較することによって、ユーザの保護を実現します。Web レピュテーション承認済みリストにより、管理者は、管理者が安全だと認識している URL の検索とブロックを省略できます。

Web レピュテーション承認済みリストを有効にするには

1. 「その他」の（ウイルス対策でない）ポリシーを作成または変更します。
 - 新しいルールを作成する方法の詳細については、96 ページの「ポリシーを追加する」を参照してください。
 - 既存のルールを変更する方法の詳細については、129 ページの「既存のポリシーを変更する」を参照してください。
2. [検索条件] 画面の [Web レピュテーション] で、[Web レピュテーション設定] をクリックします。[Web レピュテーション設定] 画面が表示されます。
3. [Web レピュテーション承認済みリストの使用を有効にする] チェックボックスをオンにします。
4. [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。
5. ポリシーの設定を続行します。

Web レピュテーション承認済みリストに追加する

Web レピュテーション承認済みリストに追加されたドメインは、InterScan MSS によって検索されません。管理者は、安全だとわかっているドメインのみを追加する必要があります。

Web レピュテーション承認済みリストにドメインを追加するには

1. [ポリシー] → [Web レピュテーション承認済みリスト] の順にクリックします。[Web レピュテーション承認済みリスト] 画面が表示されます。
2. 次のいずれかの方法で、[Web レピュテーション承認済みリスト] に入力します。

手動：

- a. ドメインを入力します。例：*.trendmicro.com
- b. [追加 >>] をクリックします。

リストのインポート：

注意： Web レピュテーション承認済みリストにテキストファイルをインポートする場合、各行に 1 つのドメインのみが記入されていることを確認してください。

- a. [インポート] をクリックします。[Web レピュテーション承認済みリストのインポート] が表示されます。
- b. ファイルパスとファイル名を入力するか、[参照] をクリックしてファイルを見つけます。
- c. 次のいずれかを選択します。

- ・ 現在のリストにマージする
 - ・ 現在のリストを上書きする
- d. [インポート] をクリックします。
3. [保存] をクリックします。

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。

- ・ 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。

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。

内部アドレス 

注意: 「既知の」ユーザセットまたはドメインセットを内部アドレスとして指定してください。これらは、レポートとルール作成時の「受信」および「送信」を包括します。

内部ドメインおよびユーザグループ

ドメインの入力 

インポート

>>

選択済み

2. [内部ドメインおよびユーザグループ] で、ドロップダウンボックスから次のいずれかを選択します。
 - **ドメインの入力**: ドメインを入力し、[>>] をクリックします。「@」やメールアドレスのユーザ名の部分を使用しないでください。たとえば、domainname や domainname1.domainname2 は有効ですが、user@domainname は無効です。

注意: ドメイン名にはワイルドカードを使用できます。たとえば、*.example.com を指定すると、example.com のすべてのサブドメインが含まれます。ただし、ユーザ名やアドレスのドメイン名部分に 2 つ以上のアスタリスクを使用したり、「@」記号を使用したりすることはできません。*.*@example.com と user@*.* は、どちらも無効です。

- **LDAP グループの検索**: LDAP グループを検索する画面が表示されます。個別の LDAP ユーザ名ではなく、LDAP グループ名をテキストボックスに入力して、[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。検索された LDAP グループを [選択済み] リストに追加するには、その LDAP グループをクリックしてから [>>] をクリックします。

詳細については、95 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。

注意： 内部アドレスに対して LDAP グループを選択する際、Microsoft Active Directory または Sun iPlanet Directory を LDAP サーバとして指定している場合は、LDAP グループの先頭または末尾、あるいはその両方にワイルドカードを使用できます。使用できるワイルドカードの例は、A*、*A、および *A* です。

Domino を LDAP サーバとして選択している場合は、末尾にしかワイルドカードを使用できません。使用できないワイルドカードの例は、*A および *A* です。

3. ファイルからドメインをインポートするには、[インポート] をクリックして、ファイルを選択します。

ヒント： 最良の結果を得るには、正確なドメインとすべてのサブドメインの両方をインポートします。

ドメインリストのテキストファイルのサンプルの内容は、次のとおりです。

- domain.com: Imports the exact domain
- *.domain.com: Imports all sub-domains
- domain.org: Imports the exact domain

注意： インポートされたファイルは、1 行に 1 つのドメインを含むテキストファイルでなければなりません。ドメインを指定するときは、ワイルドカードを使用できます。

4. [保存] をクリックします。

内部アドレスをエクスポートするには

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. [エクスポート] をクリックします。[ファイルのダウンロード] 画面が表示されます。
3. [保存] をクリックします。[名前を付けて保存] ダイアログボックスが表示されます。
4. 場所とファイル名を指定します。
5. [保存] をクリックします。

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 以降
- SUN Microsystems 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。

次の差出人からの受信メッセージ



ルールの追加 > 次の差出人からの受信メッセージ

保存 キャンセル

アドレスの選択

☐ すべてのユーザ

☒ 選択したアドレスのいずれか

メールアドレスの入力

メールアドレスの入力

LDAP ユーザまたはグループの検索

アドレスグループの選択

追加 >

選択済み

保存 キャンセル

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。137 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、92 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。

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、92 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、次の手順を実行します。

- 手順 1 — 97 ページの「ルートを指定する」
- 手順 2 — 104 ページの「検索条件を指定する」
- 手順 3 — 118 ページの「処理を指定する」
- 手順 4 — 127 ページの「ポリシーを完成させる」

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

ルールを追加するための最初の手順は、次の項目を設定することです。

- **ルート：** 受信者と送信者のメールアドレス、LDAP ユーザまたはグループ、あるいはアドレスグループが含まれた特定の「宛先」と「差出人」の組み合わせ。ルートの除外を設定することもできます。
- **ルートの種類：** SMTP トラフィック、POP3 トラフィック、またはすべてのトラフィックの方向です。

ルートを追加するには

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。[ルールの追加] 画面が表示されます。

ポリシー ?

フィルタ:

追加		コピー	削除	1-2 / 2 14 4 ページ 1		
ウイルス対策	その他の	ルール	処理	順序	変更日	ステータス
☒	☒	ウイルス対策ルール	トレンドマイクロの推奨処理	1	2007/11/17	✓
☐	☐	初期設定のスパムメール対策ルール	隔離	2	2007/11/17	✓

1-2 / 2 14 4 ページ 1

15件/ページ

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の条件が検索されます。

ルールの追加 ?

ポリシーリスト > 新規ルール

➤ 手順1: 受信者と送信者の選択 >>> 手順2 >>> 手順3 >>> 手順4

このルールの適用対象 送信メッセージ

< 戻る 次へ > キャンセル

宛先	受信者
差出人	送信者
除外	送信者から受信者

ルールの追加 ?

ポリシーリスト > 新規ルール

➤ 手順1: 受信者と送信者の選択 >>> 手順2 >>> 手順3 >>> 手順4

このルールの適用対象 送信メッセージ

< 戻る 次へ > キャンセル

宛先	受信者
差出人	送信者
除外	送信者から受信者

次の宛先への送信メッセージ

ルールの追加 > 次の宛先への送信メッセージ

受信者と送信者

送信

宛先 すべてのユーザ
(および)

差出人

< 戻る 次へ > キャンセル

保存 キャンセル

アドレスの選択

☒ すべてのユーザ

☐ 選択したアドレスのうち

メールアドレスの入力 追加 >

選択済み

保存 キャンセル

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
 - 受信メッセージと送信メッセージの両方
 - POP3
 - すべてのメッセージ
5. 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、137 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 POP3 ルートに適用されます。

3. 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。

6. [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。

既存のポリシーのルートを編集するには

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. 編集するポリシーの名前をクリックします。ポリシーの [概要] 画面が表示されます。
3. [受信者と送信者] の [編集] をクリックします。ポリシーの [受信者と送信者] 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
 - 受信メッセージと送信メッセージの両方
 - POP3
 - すべてのメッセージ

注意： グローバル DKIM 適用ルールで [このルールの適用対象] オプションを変更することはできません。

5. 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、137 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 POP3 ルートに適用されます。
 3. 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。
-

6. [保存] をクリックします。

ルートを設定する

ルートとは、受信者と送信者のメールアドレス、LDAP ユーザまたはグループ、あるいはアドレスグループが含まれた特定の「宛先」と「差出人」の組み合わせのことです。ルートの除外を設定することもできます。

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。

- 送信メッセージを設定する場合は、内部アドレスリストは送信者に適用されます。
- 受信メッセージを設定する場合は、内部アドレスリストは受信者に適用されます。

設定例

アスタリスク (*) ワイルドカードを使用して、特定の範囲のメールアドレスを含めることができます。以下に例を示します。

- `user@example.com`: 指定したアドレスだけが含まれます。
- `*@example.com`: example.com ドメインのユーザすべてが含まれます。

- ***@*.example.com**: example.com のサブドメインのユーザすべてが含まれます。たとえば、user1@accounting.example.com などが含まれます。
- ***@***: すべてのメールアドレスが含まれます。

ルートを設定するには

1. [受信者と送信者の選択] 画面で、次のいずれかをクリックします。
 - **受信者 / 送信者**: [受信者メッセージ] または [送信者メッセージ] を選択した場合に表示されます。
 - **ユーザ**: [受信メッセージと送信メッセージの両方] を選択した場合に表示されます。
2. [アドレスの選択] で、次のいずれかを選択します。
 - **すべてのユーザ**: このオプションを選択すると、受信者または送信者に関するすべての制限が解除されます。
 - **メールアドレスの入力**: 追加するメールアドレスを入力します。
 - **LDAP ユーザまたはグループの検索**: LDAP ユーザまたはグループ名を入力して、[検索] をクリックします。結果がリストボックスに表示されます。
 - **アドレスグループの選択**: すべての既存のアドレスグループがリストに表示されます。複数のルールで再利用する多数のメールアドレスがある場合は、[追加] をクリックしてアドレスグループを作成してください。
3. メールアドレスまたはメールアドレスグループを追加する場合は、[追加 >] をクリックします。LDAP グループまたはアドレスグループを追加する場合は、そのグループをリストボックスでクリックし、[追加 >] をクリックします。
4. [選択済み] リストからメールアドレスまたはメールアドレスグループを削除するには、ごみ箱のアイコンをクリックします。
5. [保存] をクリックします。

ヒント： 受信者または送信者として LDAP グループを選択する際、Microsoft Active Directory または Sun iPlanet Directory を LDAP サーバとして指定している場合は、LDAP グループの先頭または末尾、あるいはその両方にワイルドカードを使用できます。使用できるワイルドカードの例は、A*、*A、*A* です。Domino を LDAP サーバとして選択している場合は、末尾にしかワイルドカードを使用できません。使用できないワイルドカードの例は、*A および *A* です。

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常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。

ルートの除外を設定する

多数の送信者または受信者のグループに適用する一方で、ルールが適用されない特定のユーザを除外するようにルートを設定するには、次の手順を実行します。

ルートの除外を設定するには

1. [ルールの追加] 画面で、[除外] の横にあるリンクをクリックします。トラフィックの方向 (受信メッセージ、送信メッセージ、受信メッセージと送信メッセージの両方、またはすべてのメッセージ) に応じた除外画面が表示されます。
2. [アドレスの選択] で、[差出人 (送信者)] および [宛先 (受信者)] の両方について次のいずれかを選択します。
 - **メールアドレスの入力：** 追加するメールアドレスを入力します。
 - **LDAP ユーザまたはグループの検索：** LDAP ユーザまたはグループ名を入力して、[検索] をクリックします。結果がリストボックスに表示されます。
 - **アドレスグループの選択：** すべての既存のアドレスグループがリストに表示されます。同一ルール内の複数のルートで再利用する多数のメールアドレスがある場合は、[追加] をクリックしてアドレスグループを作成してください。
3. メールアドレスを追加する場合は、[追加 >] をクリックします。LDAP グループまたはアドレスグループを追加する場合は、そのグループをリストボックスでクリックし、[追加 >] をクリックします。
4. 送信者と受信者のペアをリストから削除するには、ごみ箱のアイコンをクリックします。
5. [保存] をクリックします。

検索条件を指定する

新しいルールの送信者と受信者を選択するか既存ルールの送信者と受信者を変更した後で、いくつかの条件に基づいてメールトラフィックのフィルタを実行するルールを設定します。

検索条件は、ウイルス対策ルールを作成しているか、他のルールを作成しているかによって異なります。

検索条件を指定するには

1. [手順 2: 検索条件の選択] 画面で、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。

ルールの追加 

ポリシーリスト > 新規ルール

手順1 >>> **手順2: 検索条件の選択** >>> 手順3 >>> 手順4

[戻る](#) [次へ](#) [キャンセル](#)

ウイルス検索
 ウイルス、スパイウェア、ワーム、トロイの木馬、およびその他の不正プログラムコードの検索方法を選択してください。

- ☒ 検索可能なすべてのファイル
- ☐ トレンドマイクロの推奨設定: 実際のファイルタイプによる識別 
- ☐ 特定のファイルタイプ

IntelliTrap
☒ IntelliTrapを有効にする 
☐ トレンドラボにIntelliTrapサンプルを送信する

スパイウェア検索

☐ スパイウェア	☐ アドウェア
☐ ダイヤラー	☐ ジョークプログラム
☐ ハッキングツール	☐ リモートアクセスツール
☐ パスワード解読アプリケーション	☐ その他 

受信者と送信者
 送信
 宛先 すべてのユーザ
 (および)
 差出人 すべてのユーザ

[戻る](#) [次へ](#) [キャンセル](#)

ウイルス対策ルール

- a. **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。
 - **検索可能なすべてのファイル**: すべてのファイルの検索を試行します。

- **トレンドマイクロの推奨設定**：実際のファイルタイプによる識別：トレンドマイクロの推奨設定を使用して、無害なファイル拡張子であるように偽装している可能性のある不正プログラムコードを識別します。
- **特定のファイルタイプ**：検索対象とする以下の種類のファイル拡張子のいずれかの横にあるチェックボックスをオンにします。
 - **アプリケーションおよび実行可能ファイル**：リンクをクリックして検索するサブタイプを選択します。
 - **文書**：リンクをクリックして検索するサブタイプを選択します。
 - **圧縮ファイル**：リンクをクリックして検索するサブタイプを選択します。
 - **指定のファイル拡張子**：テキストボックスに拡張子を入力します。拡張子の前にピリオド (.) を入力する必要はありません。拡張子にアスタリスク (*) ワイルドカードを使用することもできます。
- b. **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。
 - **IntelliTrap を有効にする**：自動実行型の圧縮ファイルを含むメールの添付ファイルを検索します。
 - **トレンドラボに IntelliTrap サンプルを送信する**：InterScan MSS で、IntelliTrap で検出した添付ファイルを持つメールメッセージを自動的に送信できます。
- c. **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。

[ポリシーリスト](#) > [新規ルール](#)

手順1 >>> 手順2: 検索条件の選択 >>> 手順3 >>> 手順4

次の場合にルールの実行を実行する: いずれかの条件に一致 (OR)

[戻る](#)
[次へ](#)
[キャンセル](#)

スパムメール/フィッシングメール

☐ スпамメール

☐ フィッシングメール

Webレビュテーション

☐ Webレビュテーション設定 

添付ファイル

☐ 名前または拡張子

☐ MIMEコンテンツタイプ

☐ 実ファイルタイプ

☐ サイズが MB

☐ 添付ファイル数

☐ パスワードで保護されたzipファイル (検索不能)

サイズ

☐ メッセージサイズが MB

コンテンツ

☐ 件名のキーワード

☐ 件名が空白

☐ 本文のキーワード

☐ ヘッダのキーワード

☐ 添付ファイルの内容のキーワード

その他

受信者と送信者

すべてのルート

宛先 すべてのユーザ
(および)

差出人 すべてのユーザ

[戻る](#)
[次へ](#)
[キャンセル](#)

- **スパムメール**: リンクをクリックして、スパムメール検出レベルを選択し、承認済み送信者とブロックする送信者、および除外テキストのリストを設定します。
 - **フィッシングメール**
- c. **Web レピュテーション**: メッセージ内の URL を検索して、フィッシングまたは他の不正な Web サイトから保護します。
- d. **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る添付ファイルなど、選択した条件に一致した添付ファイルを検索します。
- **名前または拡張子**: リンクをクリックして、特定のファイル名または拡張子名のフィルタを設定します。
 - **MIME コンテントタイプ**: リンクをクリックして、MIME コンテントタイプのフィルタを設定します。
 - **実ファイルタイプ**: リンクをクリックして、一般的な実行可能ファイル、文書、画像、メディア、圧縮ファイルのフィルタを設定します。
 - **サイズが {>, <, =} {size} {MB, KB, B}**: 特定のバイト数、キロバイト数、メガバイト数より大きい、小さい、または等しいサイズの添付ファイルのフィルタを選択します。ファイルサイズを表す値を入力します。
 - **添付ファイル数 {>, <, =} {number}**: 特定の数より大きい、小さい、または等しい添付ファイル数のフィルタを選択します。各メールメッセージの添付ファイルの総数を表す値を入力します。
 - **パスワードで保護された zip ファイル (検索不能)**: InterScan MSS で検索できないパスワードで保護されたファイルのフィルタを選択します。
- e. **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。
- **メッセージサイズが {>, <, =} {size} {MB, KB}**: 特定のキロバイト数、メガバイト数より大きい、小さい、または等しいサイズのメールメッセージのフィルタを選択します。メールメッセージサイズを表す値を入力します。
- f. **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。
- **件名のキーワード**: リンクをクリックしてキーワードリストを管理します。
 - **件名が空白**: 件名のないメールメッセージのフィルタを選択します。スパムメールには件名が含まれていない場合があります。
 - **本文のキーワード**: リンクをクリックしてキーワードリストを管理します。
 - **ヘッダのキーワード**: リンクをクリックしてキーワードリストを管理します。ヘッダには、件名、差出人、宛先、Cc、および指定可能な他のヘッダが含まれます。

- **添付ファイルの内容のキーワード**: リンクをクリックしてキーワードリストを管理します。
- g. **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。
 - **受信者の数が {>, <, =} {number}**: 受信者数のフィルタを選択します。各メールメッセージの受信者の総数を表す値を入力します。
 - **受信の時間帯**: リンクをクリックして、メッセージの受信日と時間帯を選択します。
 - **暗号化メッセージ**: InterScan MSS で検索できない暗号化されたメッセージのフィルタを選択します。

スパムメールの検索条件を選択する

スパムメールの検索条件には、スパムメール検出レベルのしきい値の設定、承認済み送信者およびブロックする送信者やテキスト除外ルールがリストに含まれます。

スパムメールの検出条件を設定するには

1. その他のルールタイプの [手順 2: 検索条件の選択] 画面の [スパムメール / フィッシングメール] で、[スパムメール] の横にあるチェックボックスをオンにします。
2. [スパムメール] をクリックします。[スパムメール] 画面が表示されます。
3. スパムメール検索を有効にするには、[スパムメールの検出レベルを指定する] チェックボックスをオンにします。このチェックボックスをオンにしなかった場合、ルールに違反するメールがあってもスパムメールと見なされません。ただし、ブロックする送信者リストに指定した送信者に対しては処理が実行されます。
4. 次のスパムメールの検出レベルを 1 つ選択するか、検出のしきい値を指定します。
 - **高**: より多くのスパムメールを検出します。InterScan MSS を通過してクライアントに到達するスパムメールが多すぎるときに設定します。
 - **中**: 標準の設定です。
 - **低**: より少ないスパムメールを検出します。InterScan MSS によってスパムメールと判定されるメールが多すぎるときに設定します。
 - **指定 {}**: メールメッセージがスパムメールかどうか判断する基準を示す 3.0 から 10.0 までのしきい値を設定できます。

注意： しきい値が高くなると、スパムメールの疑いが非常に高いメッセージでない限り InterScan MSS はスパムメールと見なしません。スパムメールの検出率は低くなりますが、また誤検出も少なくなります。InterScan MSS で正規のメールメッセージがスパムメールと見なされることが多すぎる場合（誤検出が多すぎる場合）は、しきい値を高く設定してください。

しきい値が低くなると、少しでもスパムメールの疑いがあるメッセージは InterScan MSS によってスパムメールと見なされます。スパムメールの検出率は高くなりますが、また誤検出も多くなります。多くのスパムメールが正規のメールとしてクライアントまで送信される場合、しきい値を低く設定してください。

5. [DKIM 承認済みリスト] をクリックして、DKIM 承認済みリストの使用を有効または無効にします。DKIM 承認済みリストに記載されているドメインから送信されたメッセージは、スパムメールとして検索されたりマークされたりすることはありません。
 6. 次のいずれかのリストの横にあるチェックボックスをオンにして、有効にします。
 - **承認済み送信者リスト：** このリストにある送信者からのメールメッセージはスパムメールとして検出されません。
 - **ブロックする送信者リスト：** このリストにある送信者からのメールはスパムメールとして検出されます。
 - **テキスト除外ルール：** このリスト内のいずれかのテキストを含むメールはスパムメールとして検出されません。
-

注意： リストの設定手順については、110 ページの「承認済み送信者リストとブロックする送信者リストを設定する」を参照してください。

7. [保存] をクリックして、検索条件の選択を続行します。

承認済み送信者リストとブロックする送信者リストを設定する

スパムメールフィルタの検索条件にさらに柔軟性を与えるために、InterScan MSS には以下のリストが用意されています。

- **承認済み送信者リスト：** このリストにある送信者からのメールメッセージはスパムメールとして検出されません。
- **ブロックする送信者リスト：** このリストにある送信者からのメールはスパムメールとして検出されます。

スパムメールの検索条件を選択する際に、リストを設定します。

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を設定するには

1. [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] の横にあるチェックボックスをオンにします。
2. アドレスを手動で追加するには、次の手順を実行します。
 - a. [メールアドレス] の横に、アドレスを入力します。複数のアドレスを追加するには、アスタリスク (*) ワイルドカードを使用します。
 - b. [追加] をクリックします。そのアドレスがリストに表示されます。
3. ローカルホストにあるファイルのアドレスグループを InterScan MSS サーバへインポートするには、次の手順を実行します。
 - a. [インポート] をクリックします。
 - b. [参照] をクリックして、ファイルを検索します。画面が表示されます。
 - c. [開く] をクリックします。
 - d. リストに既存のアドレスがある場合は、インポートするリストとこれらのアドレスをマージするか、インポートするリストでこれらのアドレスを上書きするかを選択します。
 - e. [インポート] をクリックします。
4. InterScan MSS サーバ上のファイルとしてアドレスグループをエクスポートするには、次の手順を実行します。
 - a. [エクスポート] をクリックします。[保存] 画面が表示されます。
 - b. [保存] をクリックします。
 - c. ファイルの名前と、ファイルを保存する場所を指定します。
 - d. [保存] をクリックします。ファイルが指定した場所に保存され、画面が表示されます。
 - e. [閉じる] をクリックします。
5. [保存] をクリックします。

スパムメール除外テキストルールを設定する

InterScan MSS では、除外テキストリスト内のテキストはスパムメールとして検出しません。必ず特定のキーワードを含むメールメッセージをユーザが受信するようにしたい場合は、このリストに関するルールを設定してください。

正規表現を使用して条件を定義します。以下の文字の前には、円記号 (¥) を入力してください。

¥ | () { } ^ \$ * + . ?

スパムメールの除外テキストルールを設定するには

1. スパムメールの検索条件を設定している場合は、[テキスト除外ルール] の [テキスト除外ルールに一致するメッセージを除外する] チェックボックスをオンにします。
2. 新しい除外テキストルールを追加するには、[追加] をクリックします。既存のルールを設定するには、リストボックスで設定するリストをクリックし、[編集] をクリックします。[テキスト除外ルール] 画面が表示されます。
3. [名前] の横に、除外テキストルールのわかりやすい名前を入力します。
4. [検索領域] の横で、メールメッセージの一部を選択します。

注意： [件名]、[差出人]、[宛先]、または [返信先] を検索領域として選択し、ヘッダの照合対象に [行の先頭] を使用する場合は、[行の先頭] にヘッダの内容のみを入力します。

例：

1. 検索領域として [差出人] を選択します。
2. [一致する文字列] で、[行の先頭] にメッセージ文字列を入力します。例：
test@trendmicro.com

検索領域として [すべてのヘッダ] を選択し、ヘッダの照合対象に [行の先頭] を使用する場合は、ヘッダ名も入力します。

例：

1. 検索領域として [すべてのヘッダ] を選択します。
2. [一致する文字列] で、[行の先頭] にヘッダ名とメッセージ文字列の両方を入力します。例：From: test@trendmicro.com

-
5. [大文字と小文字を区別する] のチェックボックスをオンにすると、テキストの大文字 / 小文字も区別します。
 6. [一致する文字列] の下のテキストボックスにテキスト文字列を入力します。[行の先頭] は行の最初で一致させる正規表現として使用されます。[行の末尾] は行の最後で一致させる正規表現として使用されます。
 7. [保存] をクリックします。

Web レピュテーションを設定する

Web レピュテーションを有効にし、メールメッセージ内の不正な URL からクライアントを保護するように設定します。

Web レピュテーションを有効にするには

1. 「その他」の（ウイルス対策でない）ポリシーを作成または変更します。
 - 新しいルールを作成する方法の詳細については、96 ページの「ポリシーを追加する」を参照してください。
 - 既存のルールを変更する方法の詳細については、129 ページの「既存のポリシーを変更する」を参照してください。
2. [検索条件] 画面の [Web レピュテーション] で、[Web レピュテーション設定] チェックボックスをオンにします。
3. [次へ] をクリックして、ポリシーの設定を続行します。

Web レピュテーションを設定するには

1. 「その他」の（ウイルス対策でない）ポリシーを作成または変更します。
 - 新しいルールを作成する方法の詳細については、96 ページの「ポリシーを追加する」を参照してください。
 - 既存のルールを変更する方法の詳細については、129 ページの「既存のポリシーを変更する」を参照してください。
2. [検索条件] 画面の [Web レピュテーション] で、[Web レピュテーション設定] をクリックします。[Web レピュテーション設定] 画面が表示されます。
3. 次の検出レベルを 1 つ選択するか、検出のしきい値を指定します。
 - **高**: より多くの Web サイトをブロックします。クライアントがアクセスする不正な Web サイトの数が多すぎる場合は、高感度レベルを選択します。
 - **中**: 標準の設定です。
 - **低**: 比較的少量の Web サイトをブロックします。InterScan MSS がブロックする正当な Web サイトの数が多すぎる場合は、低感度レベルを選択します。
4. Web レピュテーション承認済みリストにあるドメインの検索とブロックを省略するには、[Web レピュテーション承認済みリストの使用を有効にする] チェックボックスをオンにします。
5. [保存] をクリックして、検索条件の選択を続行します。

添付ファイルの検索条件を選択する

InterScan MSS では、メッセージに添付されているファイルに基づいて、メールトラフィックのフィルタを実行できます。添付ファイルの検索条件には、以下が含まれます。

添付ファイル名と拡張子の検索条件：

1. [検索条件] 画面の [添付ファイル] で、[名前または拡張子] の横にあるチェックボックスをオンにします。
2. [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。
3. [選択] の横で、次のいずれかを選択します。
 - **選択されたファイルをブロック**：選択した名前の添付ファイルが添付されているメールメッセージに対して処理を実行します。
 - **選択されたファイル以外をブロック**：選択した名前以外の添付ファイルが添付されているメールメッセージに対して処理を実行します。
4. 検索対象または検索対象外の添付ファイルの横にあるチェックボックスをオンにします。
5. 独自の添付ファイル名を追加するには、次のようにします。
 - a. [指定のファイル名] の横にあるチェックボックスをオンにします。
 - b. [インポート] をクリックして既存のテキストファイルからインポートします。別の画面が表示されます。

または、テキストボックスに添付ファイル名を入力します。複数の値がある場合はセミコロン (;) で区切ります。拡張子にアスタリスク (*) ワイルドカードを使用することもできます。
 - c. [インポート] をクリックします。
6. [保存] をクリックして、検索条件の選択を続行します。

MIME コンテンツタイプの検索条件を選択するには

1. [手順 2: 検索条件の選択] 画面の [添付ファイル] で、[MIME コンテンツタイプ] の横にあるチェックボックスをオンにします。
2. [MIME コンテンツタイプ] をクリックします。[MIME コンテンツタイプ] 画面が表示されます。
3. [選択] の横で、次のいずれかを選択します。
 - **選択された添付ファイルタイプ**：選択したタイプの添付ファイルが添付されているメールメッセージに対して処理を実行します。
 - **選択された添付ファイルタイプ以外**：選択したタイプ以外の添付ファイルが添付されているメールメッセージに対して処理を実行します。
4. フィルタを実行する MIME コンテンツタイプの横にあるチェックボックスをオンにします。
5. 独自の MIME タイプを追加するには、テキストボックスにその MIME タイプを入力します。複数の値がある場合はセミコロン (;) で区切ります。MIME タイプにアスタリスク (*) ワイルドカードを使用することもできます。

6. [保存] をクリックして、検索条件の選択を続行します。

実際のファイルタイプの検索条件を選択するには

1. [手順 2: 検索条件の選択] 画面の [添付ファイル] で、[実ファイルタイプ] の横にあるチェックボックスをオンにします。
2. [実ファイルタイプ] をクリックします。[添付ファイルの実際のファイルタイプ] 画面が表示されます。
3. [選択] の横で、次のいずれかを選択します。
 - **選択された添付ファイルタイプ**: 選択したタイプの添付ファイルが添付されているメールメッセージに対して処理を実行します。
 - **選択された添付ファイルタイプ以外**: 選択したタイプ以外の添付ファイルが添付されているメールメッセージに対して処理を実行します。
4. フィルタを実行する実ファイルタイプの横にあるチェックボックスをオンにします。
5. [保存] をクリックして、検索条件の選択を続行します。

添付ファイルサイズの検索条件を選択するには

1. [手順 2: 検索条件の選択] 画面の [添付ファイル] で、[サイズが {>, <, =} {size} {MB, KB, B}] の横にあるチェックボックスをオンにします。
2. 比較記号 (>, <, =) を選択します。
3. サイズを表す値を入力します。
4. メガバイト、キロバイト、バイト (MB、KB、B) のいずれかを選択します。
5. 検索条件の選択を続行します。

添付ファイル数の検索条件を選択するには

1. [手順 2: 検索条件の選択] 画面の [添付ファイル] で、[添付ファイル数 {>, <, =} {number}] の横にあるチェックボックスをオンにします。
2. 比較記号 (>, <, =) を選択します。
3. 添付ファイルの数を表す値を入力します。
4. 検索条件の選択を続行します。

パスワードで保護されたファイルのブロックを選択するには

1. [手順 2: 検索条件の選択] 画面の [添付ファイル] で、[パスワードで保護された zip ファイル] の横にあるチェックボックスをオンにします。

メッセージサイズの検索条件を選択する

InterScan MSS では、すべての添付ファイルを含む合計サイズに基づいて、メールメッセージに対する処理を実行できます。

メッセージサイズの検索条件を選択するには

1. [手順 2: 検索条件の選択] 画面の [サイズ] で、[メッセージサイズが {>, <, =} {size} {MB or KB}] の横にあるチェックボックスをオンにします。
2. 比較記号 (>, <, =) を選択します。
3. メールメッセージサイズを表す値を入力します。
4. メガバイト、キロバイト (MB、KB) のいずれかを選択します。
5. 検索条件の選択を続行します。

メッセージコンテンツの検索条件を選択する

InterScan MSS では、コンテンツおよびコンテンツが表示される場所に基づいて、メールメッセージに対する処理を実行できます。フィルタを実行するコンテンツの指定方法の詳細については、82 ページの「キーワードを設定する」を参照してください。

コンテンツの検索条件を選択するには

1. [ポリシー] → [ポリシーリスト] の順にクリックします。[ポリシー] 画面が表示されます。
2. 「その他」の (ウイルス対策でない) ポリシーを作成または変更します。
3. [手順 2: 検索条件の選択] 画面の [コンテンツ] で、コンテンツの条件を適用するメールメッセージ部分の横のチェックボックスをオンにします。
4. コンテンツ条件を設定するメールメッセージ部分を指定するリンクをクリックします。次の 2 つの列が表示されている [キーワード] 画面が表示されます。
 - ・ **利用可能**: キーワードは利用可能ですが、現在使用されていません。
 - ・ **選択済み**: キーワードは現在使用中です。
5. ヘッダのキーワードを設定している場合は、キーワードを適用するヘッダ項目の横にあるチェックボックスをオンにします。
6. [追加] をクリックします。キーワード表現を管理する画面が表示されます。

7. キーワードを設定します。
8. [利用可能] リストで、有効にするキーワードリストをクリックします。
9. [>>] をクリックします。キーワードが [選択済み] リストに表示されます。
キーワードリストを利用可能な状態にしておき、InterScan MSS で一時的に使用しないようにするには、選択されたリストでキーワードをクリックしてから [<<] をクリックします。
10. [保存] をクリックして、[手順 2: 検索条件の選択] 画面 を続行します。

「その他」の検索条件を指定する

InterScan MSS では、以下に基づいてメールトラフィックのフィルタを実行できます。

- 受信者数
- メッセージ受信時間
- メッセージ内容が暗号化されているかどうか

「その他」の検索条件を指定するには

1. [ポリシー] → [ポリシーリスト] の順にクリックします。[ポリシー] 画面が表示されます。
2. 「その他」の (ウイルス対策でない) ポリシーを作成または変更します。
 - 新しいルールを作成する方法の詳細については、96 ページの「ポリシーを追加する」を参照してください。
 - 既存のルールを変更する方法の詳細については、129 ページの「既存のポリシーを変更する」を参照してください。
3. [検索条件] の [その他] で、以下の横にあるチェックボックスをオンにします。
 - 受信者の数が {>, <, =} {number}: 受信者の数が指定した制限より小さい場合、制限を超える場合、または制限と等しい場合に、メッセージがブロックされます。
 - **受信の時間帯**: 指定された時間内にネットワークに侵入したメッセージをブロックします。
 - **暗号化メッセージ**: InterScan MSS で検索できない暗号化されたメッセージをブロックします。

受信者数の検索条件を選択する

InterScan MSS では、メッセージが配信される受信者数に基づいて、メールメッセージに対する処理を実行できます。

受信者数の検索条件を選択するには

1. [手順 2: 検索条件の選択] 画面の [その他] で、[受信者の数が {>, <, =} {number}] の横にあるチェックボックスをオンにします。
2. 比較記号 (>, <, =) を選択します。
3. 受信者数を表す値を入力します。
4. 検索条件の選択を続行します。

メッセージ受信時間の検索条件を設定する

InterScan MSS では、メールメッセージの到着時間に基づいて、メールメッセージに対する処理を実行できます。

時間範囲の検索条件を選択するには

1. [手順 2: 検索条件の選択] 画面の [その他] で、[受信の時間帯] の横にあるチェックボックスをオンにします。
2. [受信の時間帯] をクリックします。[時間帯] 画面が表示されます。
3. [選択] の横で、次のいずれかを選択します。
 - 選択した範囲内の任意の時間
 - 選択した範囲を除く任意の時間
4. 日時のドロップダウンボックスから、曜日、時間の範囲を指定します。
5. [追加] をクリックします。
6. [保存] をクリックして、検索条件の選択を続行します。

処理を指定する

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対して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するか Bcc 送信するよう指示します。

処理を設定するには

1. [手順 2: 検索条件の選択] 画面で [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。

「その他」のルール処理の指定：

ルールの追加 ?

ポリシーリスト > 新規ルール

手順1 >>> 手順2 >>> **手順3: 処理の選択** >>> 手順4

[戻る](#) [次へ](#) [キャンセル](#)

ルールに一致するメッセージはすべてログに記録されます。

インターセプト

☒ メッセージをインターセプトしない

☐ メッセージ全体を削除

☐ 隔離先 初期設定の隔離 [編集](#)

☐ 次の受信者に変更

☐ 中継 ホスト: ポート:

変更

☐ X-ヘッダの挿入
例: X-name : value

☐ 添付ファイルの削除 一致する添付ファイル [編集](#)

☐ 本文にスタンプを挿入 検索不能な添付ファイル [編集](#)

☐ 件名にタグを挿入

☐ 配信を保留 時刻 : :

監視

☐ ポリシー通知の送信

受信者と送信者

すべてのルート

宛先 すべてのユーザ

(および)

差出人 すべてのユーザ

検索条件

[戻る](#) [次へ](#) [キャンセル](#)

図 3-2. その他のルールの処理

1. [インターセプト] で、次のいずれかのオプションを選択します。
 - **メッセージをインターセプトしない**：InterScan MSS はメッセージに対して処理を実行しません。その他のルールがある場合、メッセージは処理されます。ルールがない場合、メッセージはネットワークに渡されます。
 - **メッセージ全体を削除**：メッセージとすべての添付ファイルを削除します。
 - **隔離先**：メッセージとその添付ファイルを、ドロップダウンボックスから選択した隔離領域に格納します。新しい隔離領域の作成手順については、173 ページの「隔離とアーカイブを設定する」を参照してください。

- **次の受信者に変更**：メッセージを別の受信者に送信します。受信者のメールアドレスを入力し、複数の受信者がある場合はセミコロン (;) で区切ります。
- **中継**：メッセージを特定のメールサーバに転送します。ネットワーク上にメッセージを処理できる安全なメッセージサーバがある場合は、[中継] を選択します。次の項目を設定します。
 - [ホスト] の横に、メールサーバの FQDN または IP アドレスを入力します。
 - [ポート] の横に、メールサーバがメールトラフィックを受信するポート番号を入力します。

注意： 中継後のメッセージは追跡できません。中継後のメッセージは、InterScan MSS で制御されないため、それ以上追跡できません。

2. [変更] で、必要に応じて次のチェックボックスをオンにします。

- **X-ヘッダの挿入**：ユーザが指定したメッセージをメールメッセージのヘッダに挿入します。
- **添付ファイルの削除**：InterScan MSS が実行する処理を選択します。
 - **一致する添付ファイル**：添付ファイルの検索条件に一致する添付ファイルのみを削除します。
 - **すべての添付ファイル**：すべての添付ファイルを削除します。
- **本文にスタンプを挿入**：テキストをメッセージの先頭または末尾に挿入します。ドロップダウンボックスから挿入するスタンプ名を選択するか、[編集] をクリックして [スタンプ] 画面に移動し、スタンプを管理します。
- **件名にタグを挿入**：メッセージの件名にテキストを追加します。[件名にタグを挿入] をクリックしてタグを編集します。
- **配信を保留**：指定した時刻まで配信を遅らせます。ドロップダウンボックスから、時間と分を選択します。

3. [監視] で、必要に応じて次のチェックボックスをオンにします。

- **ポリシー通知の送信**：1 人または複数の受信者にメールメッセージを送信します。通知の種類を選択するには、[ポリシー通知の送信] をクリックします。通知の作成方法については、85 ページの「通知リストを使用する」を参照してください。
- **変更済みメッセージの保存先**：メッセージをアーカイブ領域にアーカイブします。新しいアーカイブ領域の作成手順については、173 ページの「隔離とアーカイブを設定する」を参照してください。

- **BCC:** メッセージを別の受信者に Bcc で送信します。受信者のメールアドレスを入力し、複数のアドレスはセミコロン (;) で区切ります。[Bcc] オプションを選択すると、本来の受信者に知られることなく別の受信者にもメッセージを送信できます。

「ウイルス」ルールの基本処理の指定：

基本処理では、メッセージが「手順 2: 検索条件の選択」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できます。

ルールの追加 ?

ポリシーリスト > 新規ルール

手順1 >>> 手順2 >>> **手順3: 処理の選択** >>> 手順4

基本処理

特殊処理

インターセプト

☒ メッセージをインターセプトしない
☐ メッセージ全体を削除
☐ 隔離先 初期設定の隔離
☐ 次の受信者に変更
☐ 中継 ホスト: ポート:

変更

☐ InterScan MSSでウイルスが検出された場合:
☐ トレンドマイクロの推奨処理 - ファイルタイプ別の推奨処理
☐ ウイルス駆除不能な場合: 一致する添付ファイルを削除
☐ 添付ファイルを削除 一致する添付ファイルを削除
☐ X-ヘッダの挿入 例: X-name : value
☐ 本文にスタンプを挿入 検索不能な添付ファイル
☐ 本文に安全スタンプを挿入 検索不能な添付ファイル

受信者と送信者

すべてのルート
 宛先 すべてのユーザ
 (および)
 差出人 すべてのユーザ
 検索条件
 ウイルス, IntelliTrap

図 3-3. ウイルス対策ルールの基本処理

- [インターセプト] で、次のいずれかのオプションを選択します。
 - メッセージをインターセプトしない**: InterScan MSS はメッセージに対して処理を実行しません。その他のルールがある場合、メッセージは処理されます。ルールがない場合、メッセージはネットワークに渡されます。
 - メッセージ全体を削除**: メッセージとすべての添付ファイルを削除します。
 - 隔離先**: メッセージとその添付ファイルを、ドロップダウンボックスから選択した隔離領域に格納します。新しい隔離領域の作成手順については、173 ページの「隔離とアーカイブを設定する」を参照してください。
 - 次の受信者に変更**: メッセージを別の受信者に送信します。受信者のメールアドレスを入力し、複数の受信者がある場合はセミコロン (;) で区切ります。

- **中継**: メッセージを特定のメールサーバに転送します。ネットワーク上にメッセージを処理できる安全なメッセージサーバがある場合は、[中継] を選択します。次の項目を設定します。
 - [ホスト] の横に、メールサーバの FQDN または IP アドレスを入力します。
 - [ポート] の横に、メールサーバがメールトラフィックを受信するポート番号を入力します。

注意: 中継後のメッセージは追跡できません。中継後のメッセージは、InterScan MSS で制御されないため、それ以上追跡できません。

2. [変更] で、必要に応じて次のチェックボックスをオンにします。

注意: ウイルス対策ルールで利用できるのは、[InterScan MSS でウイルスが検出された場合] のオプションのみです。

- InterScan MSS でウイルスが検出された場合: チェックボックスをオンにして、InterScan MSS がウイルスまたはその他の不正プログラムを検出した場合の処理を有効にし、以下のいずれかをクリックします。
 - **トレンドマイクロの推奨処理**: InterScan MSS が、特定の種類のウイルス / 不正プログラムに対して事前設定された検索処理を自動的に使用できるようにします。
 - **ウイルス駆除不能な場合**: InterScan MSS が添付ファイルを駆除できない場合に、実行する処理を選択します。
 - **一致する添付ファイルを削除**: ウイルス / 不正プログラムが組み込まれた添付ファイルのみを削除します。
 - **すべての添付ファイルを削除**: すべての添付ファイルを削除します。
 - **添付ファイルを削除**: InterScan MSS が実行する処理を選択します。
 - **一致する添付ファイルを削除**: ウイルス / 不正プログラムが組み込まれた添付ファイルのみを削除します。
 - **すべての添付ファイルを削除**: すべての添付ファイルを削除します。
- **X-ヘッダの挿入**: ユーザが指定したメッセージをメールメッセージのヘッダに挿入します。

注意: X-ヘッダを追加するように複数のルールを設定した場合、X-ヘッダはメッセージに 1 度だけ表示されます。X-ヘッダは最終ルールで設定したように表示されます。

- **本文にスタンプを挿入**: テキストをメッセージの先頭または末尾に挿入します。ドロップダウンボックスから挿入するスタンプ名を選択するか、[編集] をクリックして [スタンプ] 画面に移動し、スタンプを管理します。
- **本文に安全スタンプを挿入**: クリーンなメールにテキストを挿入して、メールが安全であることを示します。ドロップダウンボックスから挿入するスタンプ名を選択するか、[編集] をクリックして [スタンプ] 画面に移動し、スタンプを管理します。

注意: [本文に安全スタンプを挿入] オプションは、[特殊処理] タブでは利用できません。

- **件名にタグを挿入**: メッセージの件名にテキストを追加します。[件名にタグを挿入] をクリックしてタグを編集します。
- **配信を保留**: 指定した時刻まで配信を遅らせます。ドロップダウンボックスから、時間と分を選択します。

3. [監視] で、必要に応じて次のチェックボックスをオンにします。

- **ポリシー通知の送信**: 1 人または複数の受信者にメールメッセージを送信します。通知の種類を選択するには、[ポリシー通知の送信] をクリックします。通知の作成方法については、85 ページの「通知リストを使用する」を参照してください。
- **変更済みメッセージの保存先**: メッセージをアーカイブ領域にアーカイブします。新しいアーカイブ領域の作成手順については、173 ページの「隔離とアーカイブを設定する」を参照してください。
- **BCC**: メッセージを別の受信者に Bcc で送信します。受信者のメールアドレスを入力し、複数のアドレスはセミコロン (;) で区切ります。[Bcc] オプションを選択すると、本来の受信者に知られることなく別の受信者にもメッセージを送信できます。

「ウイルス」ルールの特殊処理の指定:

特殊処理設定では、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できます。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。

注意: これらのオプションは、ウイルス対策ルールでのみ使用できます。

ルールの追加 

ポリシーリスト > 新規ルール

手順1 >>> 手順2 >>> **手順3: 処理の選択** >>> 手順4

[戻る](#) [次へ>](#) [キャンセル](#)

基本処理 **特殊処理**

☐	マスメーリング用処理を有効にする（他のすべての処理に優先されます）▼
☐	スパイウェア対策用処理を有効にする（他のすべての処理に優先されます）▼
☐	IntelliTrap用処理を有効にする（他のすべての処理に優先されます）▼

[戻る](#) [次へ>](#) [キャンセル](#)

- 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: 検索条件の選択] 画面で [スパイウェア検索] オプションの内 1 つでも選択した場合は、対応する処理を指定できます。詳細については、104 ページの「検索条件を指定する」を参照してください。メッセージ内でスパイウェア / グレー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: 検索条件の選択] 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。104 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。

件名タグを作成する

受信者に、InterScan MSS がメッセージの添付ファイルに対して処理を実行したことや、メッセージがルールの検索条件に違反していることを通知するには、件名の先頭に短いメッセージを追加します。本来の受信者が最終的に受信するメールに対してのみタグを追加します。検索条件に違反するメッセージを削除するルールを設定している場合は、タグの追加は必要ありません。

タグを追加するには

1. 処理の選択時に、[変更] 処理の [件名にタグを挿入] をクリックします。編集画面が表示されます。
2. [タグ] の横に、件名に挿入するテキストを入力します。
3. デジタル署名付きのメッセージを破損する危険性を回避するには、[デジタル署名されたメッセージにタグを挿入しない] を選択します。
4. [保存] をクリックして、処理の選択を続行します。
5. タグを使用するには、[変更] の [件名にタグを挿入] の横にあるチェックボックスをオンにします。

ポリシーを完成させる

ルールに対する処理を選択したら、そのルールに名前を付けて有効にします。また、ルールに検索する順序を示す番号も割り当てます。InterScan MSS では、将来参照する際に必要と思われるメモをそのルールに対して追加することもできます。既存のルールのこの情報を変更することもできます。

ルールを表示する際は、以下に注意してください。

-  緑のチェックマークは有効なルールを表します。
-  赤い X 印は保存されているルールが無効になっていることを表します。
-  灰色の X 印は、製品のルールおよびアクティベーションコードが無効になっていることを表します。

ルールを完成させるには

1. 以下のいずれかの方法を使用して、画面を開きます。
 - 新しいポリシーを作成する場合は、[手順 3: 処理の選択] 画面で [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。
 - 既存のポリシーを完成させる場合は、[ポリシー] → [ポリシーリスト] 画面でポリシーリストにあるポリシーの名前をクリックします。

ルールの追加



ポリシーリスト > 新規ルール

手順1 >>> 手順2 >>> 手順3 >>> 手順4: 名前と順序

[戻る](#) [完了](#) [キャンセル](#)

ルール	備考															
☒ 有効 ルール名: Test outgoing mails 順序番号: 3																
<table border="1"> <thead> <tr> <th>順序</th> <th>既存のルール</th> <th>処理</th> <th>変更日</th> <th>ステータス</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>グローバルウイルス対策ルール</td> <td>トレンドマイクロの推奨処理</td> <td>2007/08/07</td> <td></td> </tr> <tr> <td>2</td> <td>初期設定のスパムメール対策ルール</td> <td>隔離</td> <td>2007/08/07</td> <td></td> </tr> </tbody> </table>	順序	既存のルール	処理	変更日	ステータス	1	グローバルウイルス対策ルール	トレンドマイクロの推奨処理	2007/08/07		2	初期設定のスパムメール対策ルール	隔離	2007/08/07		
順序	既存のルール	処理	変更日	ステータス												
1	グローバルウイルス対策ルール	トレンドマイクロの推奨処理	2007/08/07													
2	初期設定のスパムメール対策ルール	隔離	2007/08/07													
受信者と送信者 通信 宛先: すべてのユーザ (および) 差出人: *@trendmaster.com 検索条件 件名が空白 処理 メッセージをインターセプトしない																

[戻る](#) [完了](#) [キャンセル](#)

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] フィールドで、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。

ルールの追加 

ポリシーリスト > 新規ルール

手順1 >>> 手順2 >>> 手順3 >>> **手順4: 名前と順序**

[戻る](#) [完了](#) [キャンセル](#)

ルール **備考**

作成日:
最終更新日:
備考:

Blocks outgoing email messages from trendmaster.com

[戻る](#) [完了](#) [キャンセル](#)

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. 新しいポリシーを作成している場合は、画面上の情報が正しいことを確認します。ルールについての情報が間違っている場合は、[戻る] をクリックして、変更を行います。
8. 新しいルールの作成を完了する場合は [完了] をクリックし、既存のルールを変更する場合は [保存] をクリックします。

既存のポリシーを変更する

ルールの変更は、ルールの作成とは異なる処理に従います。

既存のルールを変更するには

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. 編集するルールの名前をクリックします。ルールの [概要] 画面が表示されます。
3. [受信者と送信者] の [編集] をクリックします。
4. ルートを設定します。詳細については、97 ページの「ルートを指定する」を参照してください。
5. [検索条件] または [DKIM 検証を行うドメイン] で、[編集] をクリックします。
6. 検索を設定します。詳細については、次を参照してください。
 - ・ ウイルス対策およびその他のルールについて：104 ページの「検索条件を指定する」

- ・ グローバル DKIM 適用ルールについて : 130 ページの「グローバル DKIM 適用ルールのドメインリストを使用する」
7. [処理] で [編集] をクリックします。
 8. 処理を設定します。詳細については、118 ページの「処理を指定する」を参照してください。
 9. [保存] をクリックします。

グローバル DKIM 適用ルールのドメインリストを使用する

ドメインリストに記載されているドメインからの受信メッセージは、DKIM 検証に合格しなかったり、DKIM 署名がない場合、スパムメールとしてマークされます。

グローバル DKIM 適用ルールのドメインリストにドメインを追加するには

1. [ポリシー] → [ポリシーリスト] の順にクリックします。[ポリシー] 画面が表示されます。
2. [グローバル DKIM 適用ルール] リンクをクリックします。[ルールの概要] 画面が表示されます。
3. [DKIM 検証を行うドメイン] 行で [編集] をクリックします。[検索条件] 画面が表示されます。
4. 次のいずれかの方法で、[ドメインリスト] に入力します。

手動:

- a. ドメイン名を入力します。
- b. [追加] をクリックします。

リストのインポート:

注意: ドメインリストにテキストファイルをインポートする場合、各行に 1 つのドメインのみが記入されていることを確認してください。

- a. [インポート] をクリックします。[DKIM 適用リストのインポート] 画面が表示されます。
 - b. ファイルパスとファイル名を入力するか、[参照] をクリックしてファイルを見つけます。
 - c. 次のいずれかを選択します。
 - ・ 現在のリストにマージする
 - ・ 現在のリストを上書きする
 - d. [インポート] をクリックします。
5. [保存] をクリックします。

ポリシーの例 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します。

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. このルールをすべて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] 画面が再表示されます。

次の宛先への受信メッセージ



ルールの追加 > 次の宛先への受信メッセージ

保存 キャンセル

アドレスの選択

☐ すべてのユーザ
☒ 選択したアドレスのいずれか

LDAP ユーザまたはグループの検索

メールアドレスの入力
 宛先グループまたはアドレスグループの選択

追加 >

選択済み

保存 キャンセル

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] の横で、[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。

添付ファイルの名前または拡張子 

暗号化メッセージの初期設定ルール > 添付ファイルの名前または拡張子

選択: ▼

☐ 検索が推奨されるファイル拡張子 ▼

☐ 検索の検討が推奨されるファイル拡張子 ▼

☐ 指定のファイル名

完全なファイル名を使用し、各エントリをセミコロン (;) で区切って入力)

5. ブロックする、またはブロックを検討するファイルの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] 画面が再表示されます。

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適当なスタンプがない場合は、[編集] をクリックします。[スタンプ] 画面が表示されます。

スタンプ

新規ルール > スタンプ

完了

検索不能な添付ファイル

追加

編集

コピー

削除

完了

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。

スタンプ

スタンプ > 新しいスタンプ

名前:

挿入位置 ☒ メッセージ本文の末尾 ☐ メッセージ本文の先頭

テキスト: 変数リスト

☒ TNEFエンコードされたメッセージおよびデジタル署名されたメッセージにスタンプを挿入しない

保存 キャンセル

7. 必要な情報を入力します。
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。[手順 3: 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. ルール名と順序番号を入力します。
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] 画面で強調表示されています。

ポリシーの例 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します。

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] 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] 画面が再表示されます。
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。

次を除く受信メッセージ 

ルールの追加 > 次を除く受信メッセージ

アドレスの選択

差出人 (送信者)

宛先 (受信者)

メールアドレスの入力 

メールアドレスの入力 

差出人	宛先

9. [差出人 (送信者)] に「*@*」と入力してすべての送信者を指定します。

10. [宛先 (受信者)] 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] 画面が再表示されます。

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実行する] の横で、[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. 既存のリストに必要なキーワードがない場合は、[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。

キーワードの追加

新規ルール > キーワード > キーワードの追加

保存 キャンセル

キーワードと正規表現の任意の組み合わせを使用してキーワードを定義できます。

、*、|、(、)、[、]、^、\$、%、+、または?という文字の直前には、『*』と入力してください。

保存 キャンセル

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、新規キーワードリストの [リスト名] を入力し、[保存] をクリックします。新しく作成されたキーワードリストを含む [キーワード] 画面が再表示されます。
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] 画面が再表示されます。
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] 画面が再表示されます。件名のキーワードと本文のキーワードの両方が選択されていることを確認します。

コンテンツ	
☒	件名のキーワード
☐	件名が空白
☐	本文のキーワード
☐	ヘッダのキーワード
☐	添付ファイルの内容のキーワード

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. ルール名と順序番号を入力します。
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] 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。

メールアドレスでのワイルドカード

ワイルドカードは、メールアドレスのユーザ名またはドメイン名の部分に使用できます。次に有効な例を示します。

- ***@*** — すべてのメールアドレスを表します。
- ***@domain.tld**、**name@*.tld** — 前者は特定のドメイン名とトップレベルドメイン (TLD) を持つすべてのメールアドレスを表し、後者は特定のユーザ名と TLD を持つすべてのメールアドレスを表します。
- ***@*.tld** — 特定の TLD を持つすべてのメールアドレスを表します。

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の部分には使用できません。ワイルドカードは、他の文字列と組み合わせることはできず、単独で使用する必要があります。無効なワイルドカードの例は、次のとおりです。

- `name@domain.*.tld` — ワイルドカードでサブドメインを表すことはできません。
- `name@domain.*` — ワイルドカードで TLD を表すことはできません。
- `*name@domain.tld` — ワイルドカードとユーザ名の一部を組み合わせることはできません。

ファイル名でのワイルドカード

メールアドレスの場合と同じように、ファイル名でワイルドカード文字を使用できます。アスタリスクは、ファイル名の名前または拡張子の部分に使用できますが、名前や拡張子の一部と組み合わせることはできません。次に有効な例を示します。

- `*.*` — すべてのファイルを表します。
- `*.extension` — 特定の拡張子のすべてのファイルを表します。
- `name.*` — 特定の名前を持つすべての拡張子のファイルを表します。

無効なワイルドカードの例は、次のとおりです。

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

検索除外を設定する

場合によっては、DoS 攻撃の一環として送られてきた可能性のある特定種類のメールメッセージの検索を省略した方が望ましいことがあります。たとえば、非常にサイズの大きいファイルが添付されたメッセージを完全に検索するには、InterScan MSS サーバの多大なリソースを要します。また、何百人もの受信者宛てに送信されたメッセージは、ほとんどの場合スパムメールか何らかの攻撃が目的でしょう。

検索除外を設定すると、InterScan MSS のリソースを消費してこれらのメールメッセージを検索する代わりに、これらのメッセージに対して直ちに特定の処理を実行できます。

警告： 検索除外で指定した処理を有効にするには、グローバルウイルス対策ルールが有効であることを確認します。

正しくない形式のメッセージについては、検索除外が実行されると、InterScan MSS は検索を停止し、対応する処理を実行します。つまり、検索除外が実行されると、InterScan MSS はポリシールールを起動しません。

セキュリティ設定の違反については、InterScan MSS は検索除外の処理の実行後に検索を停止します。InterScan MSS は、他のポリシールールのチェックを続行します。

検索除外を設定するには

1. メニューから [ポリシー] → [検索の除外] の順に選択します。
2. いくつかの条件に基づいてメールメッセージの検索除外条件を設定するには、[除外] の下の [セキュリティ設定違反] リンクをクリックします。[セキュリティ設定違反] 画面が表示されて、ここで設定を行うことができます。
3. 除外の種類に対して処理を設定するには、[処理] の下の対応するリンクをクリックします。
 - 140 ページの「セキュリティ設定違反の検出時の処理を設定する」
 - 141 ページの「正しくない形式のメッセージの検索除外に対する検出時の処理を設定する」

セキュリティ設定違反の除外を設定する

この画面で設定したセキュリティ設定違反の検索除外は、すべての送信者と受信者に適用されます。

セキュリティ設定違反を設定するには

1. [検索の除外] 画面で、[除外] の下の [セキュリティ設定違反] をクリックします。[セキュリティ設定違反] 画面が表示されます。
2. InterScan MSS が検索できるメールメッセージの種類を制限するには、次の項目を設定します。
 - **メッセージの合計サイズが次の値を超える {} MB:** 最大メガバイト数を入力します。
 - **受信者の総数が次の値を超える {} 人:** 最大受信者数を入力します。
 - **圧縮ファイル内の埋め込み層の総数が次の値を超える {} 層:** 最大階層数を選択します。
 - **いずれか 1 つのファイルの解凍後の合計サイズが次の値を超える {} MB:** 最大メガバイト数を入力します。

- ・ **圧縮ファイル内のファイルの総数が次の値を超える {} ファイル**: 最大ファイル数を入力します。
3. [保存] をクリックします。[検索の除外] 画面が表示されます。

セキュリティ設定違反の検出時の処理を設定する

セキュリティ設定違反の検出時の処理を設定するには

1. [検索の除外] 画面で、[セキュリティ設定違反] の [処理] にある処理の名前のリンクをクリックします。処理を設定する画面が表示されます。
2. [インターセプト] で、次のいずれかのオプションを選択します。
 - ・ **メッセージをインターセプトしない**: InterScan MSS はメッセージに対して処理を実行しません。他のルールがある場合は、他のルールを使用してメッセージを処理します。
 - ・ **メッセージ全体を削除**: メッセージとすべての添付ファイルを削除します。
 - ・ **次の場所に隔離**: メッセージとその添付ファイルを、ドロップダウンボックスから選択した隔離領域に移動します。新しい隔離領域の作成手順については、173 ページの「隔離とアーカイブを設定する」を参照してください。
 - ・ **中継**: メッセージを特定のメールサーバに転送します。ネットワーク上にメッセージを処理できる安全なメッセージサーバがある場合は、[中継] を選択します。次の項目を設定します。
 - ・ [ホスト] の横に、メールサーバの FQDN または IP アドレスを入力します。
 - ・ [ポート] の横に、メールサーバがメールトラフィックを受信するポート番号を入力します。

注意: 中継後のメッセージは追跡できません。中継後のメッセージは、InterScan MSS で制御されないため、それ以上追跡できません。

3. [監視] で、必要に応じて次のチェックボックスをオンにします。
 - ・ **ポリシー通知の送信**: 1 人または複数の受信者に通知メッセージを送信します。通知の種類を選択するには、[ポリシー通知の送信] をクリックします。通知の作成方法については、85 ページの「通知リストを使用する」を参照してください。
 - ・ **保存先**: メッセージをアーカイブ領域にアーカイブします。新しいアーカイブ領域の作成手順については、173 ページの「隔離とアーカイブを設定する」を参照してください。
 - ・ **BCC**: メッセージを別の受信者に Bcc で送信します。受信者のメールアドレスを入力し、複数のアドレスはセミコロン (;) で区切ります。[Bcc] オプションを選択すると、本来の受信者に知られることなく別の受信者にもメッセージを送信できます。

4. [保存] をクリックします。

正しくない形式のメッセージの検索除外に対する検出時の処理を設定する

形式が正しくないメッセージの検索除外に対して検出時の処理を設定するには

1. [検索の除外] 画面で、[正しくない形式のメッセージ] の [処理] にある処理の名前のリンクをクリックします。処理を設定する画面が表示されます。
2. [インターセプト] で、次のいずれかのオプションを選択します。
 - メッセージをインターセプトしない: InterScan MSS はメッセージに対して処理を実行しません。メッセージは配信用に転送します。

注意: InterScan MSS は、他のルールが存在しても、他のルールを使用して正しくない形式のメッセージを検索しません。

- **メッセージ全体を削除:** メッセージとすべての添付ファイルを削除します。
- **次の場所に隔離:** メッセージとその添付ファイルを、ドロップダウンボックスから選択した隔離領域に移動します。新しい隔離領域の作成手順については、173 ページの「隔離とアーカイブを設定する」を参照してください。
- **中継:** メッセージを特定のメールサーバに転送します。ネットワーク上にメッセージを処理できる安全なメッセージサーバがある場合は、[中継] を選択します。次の項目を設定します。
 - [ホスト] の横に、メールサーバの FQDN または IP アドレスを入力します。
 - [ポート] の横に、メールサーバがメールトラフィックを受信するポート番号を入力します。

注意: 中継後のメッセージは追跡できません。中継後のメッセージは、InterScan MSS で制御されないため、それ以上追跡できません。

3. [監視] で、必要に応じて次のチェックボックスをオンにします。
 - **ポリシー通知の送信:** 1 人または複数の受信者にメールメッセージを送信します。通知の種類を選択するには、[ポリシー通知の送信] をクリックします。通知の作成方法については、85 ページの「通知リストを使用する」を参照してください。
 - **保存先:** メッセージをアーカイブ領域にアーカイブします。新しいアーカイブ領域の作成手順については、173 ページの「隔離とアーカイブを設定する」を参照してください。

- **BCC:** メッセージを別の受信者に Bcc で送信します。受信者のメールアドレスを入力し、複数のアドレスはセミコロン (;) で区切ります。[Bcc] オプションを選択すると、本来の受信者に知られることなく別の受信者にもメッセージを送信できます。
4. [保存] をクリックします。



第4章

設定のバックアップ、復元、複製について

本章では、Trend Micro InterScan Messaging Security Suite 7.1（以下、InterScan MSS）の設定のバックアップと復元の手順について説明します。複数の InterScan MSS 検索サービスを配置して、同時に Trend Micro Control Manager（以下、Control Manger）を使用している場合は、検索サービスごとに設定を再指定することなく、InterScan MSS の設定を複製することもできます。

この章の内容は次のとおりです。

- 144 ページの「設定のインポート / エクスポート」
- 146 ページの「InterScan MSS の復元」
- 147 ページの「設定の複製」

設定のインポート / エクスポート

[インポート / エクスポート] 画面を使用して、InterScan MSS の設定のバックアップを作成します。バックアップを保存しておくと、設定を InterScan MSS 7.1 サーバに簡単に再適用できます。同じ設定ファイルを対象の InterScan MSS 7.1 サーバにインポートすることによって、複数のサーバ間で設定を複製することもできます。

設定ファイルをエクスポートするには

1. メニューから [管理] → [インポート / エクスポート] の順に選択します。
2. [エクスポート] をクリックします。
3. ダイアログボックスが表示されたら、[保存] をクリックして、エクスポートしたファイルをコンピュータに保存します。
4. [インポート / エクスポート] 画面に戻るには、[戻る] をクリックします。

エクスポート中に、次の操作は行わないでください。

- 他の管理コンソール画面へのアクセス、または設定の変更
- データベース操作の実行
- いずれかの InterScan MSS サービスの開始または停止
- InterScan MSS に対するエンドユーザメール隔離データベースの登録または登録解除
- 他のエクスポートまたはインポートタスクの開始

設定ファイルをインポートするには

1. InterScan MSS 管理コンソールにログオンします。
2. メニューから [概要] を選択します。いずれのサービスも開始または停止していないことを確認します。開始または停止しているサービスがある場合は、操作が完了するまで待機します。
3. メニューから [管理] → [インポート / エクスポート] の順に選択します。
4. [設定ファイルのインポート] の [参照] をクリックし、ファイルを指定します。
5. [インポート] をクリックします。ドメインベースの配信設定など、InterScan MSS の元の設定とルールが削除され、インポートした設定とルールに置き換わります。

インポート/エクスポート



設定ファイルが正常にインポートされました。

戻る

インポート中に、次の操作は行わないでください。

- 他の管理コンソール画面へのアクセス、または設定の変更

- データベース操作の実行
- いずれかの InterScan MSS サービスの開始または停止
- InterScan MSS に対するエンドユーザメール隔離データベースの登録または登録解除
- 他のエクスポートまたはインポートタスクの開始

インポートが失敗すると、設定ファイルはインポートする前の設定にロールバックされます。

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、システム障害時に素早く 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 の設定のみを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上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、145 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. 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. 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。
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、145 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 サーバ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、145 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、145 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 サーバ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、145 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、145 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、145 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

Trend Micro Management Communication Protocol (以下、MCP) 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します。

Control Manager サーバを設定するには

1. メニューから [管理] → [接続] の順に選択します。初期設定では [コンポーネント] タブが表示されます。
2. [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。

接続

コンポーネント LDAP POP3 データベース **Control Managerサーバ**

Control Managerサーバの設定

InterScan MSSをControl Managerで管理するには、Control Managerエージェントを有効にしてControl Managerサーバの設定項目を入力してください。

☒ Control Managerエージェントを有効にする

サーバ:

通信プロトコル: ☐ HTTPポート番号: ☒ HTTPSポート番号:

Webサーバ認証:

ユーザ名:

パスワード:

プロキシ設定

☐ プロキシを有効にする

プロキシタイプ:

プロキシサーバ:

ポート:

ユーザ名:

パスワード:

3. 必要な情報を指定します。
4. [Control 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 MCP 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] をクリックします。[製品ディレクトリ] 画面が表示されます。
2. 製品ディレクトリツリーから、元になる InterScan MSS 検索サービスを指定します。
3. [設定] の上にマウスを置きます。ドロップダウンリストが表示されます。
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. 対象サーバの横のチェックボックスをオンにします。
6. [複製] ボタンをクリックします。



第5章

ネットワークの監視

本章では、Trend Micro InterScan Messaging Security Suite 7.1（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。

- 152 ページの「ネットワークを監視する」
- 158 ページの「レポートを作成する」
- 165 ページの「ログ」
- 173 ページの「隔離とアーカイブ」
- 185 ページの「イベント通知」

ネットワークを監視する

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。

統計の概要を表示する

[統計] タブには、次の情報が表示されます。

- ・ **パフォーマンスの概要** — InterScan MSS が処理した受信メッセージ数、送信メッセージ数、および合計メッセージ数。1 分あたりのメッセージ数という形式で処理速度も表示されます。
- ・ **検索パフォーマンス** — 検索条件別の違反数。複数の条件に一致するメッセージはそれぞれで違反数がカウントされます。列のパーセント値はメッセージの合計数を表します。
- ・ **IP フィルタパフォーマンス** — IP フィルタでブロックした脅威の種類別ブロック数と割合。

統計を表示するには

1. メニューから [概要] を選択します。
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 / 時間数を選択します。

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。

システムの概要を表示する

[概要] 画面の [システム] タブでは、InterScan MSS コンポーネントおよびサービスのステータスに関する情報を一目で把握できます。

システムの概要を表示するには

1. メニューから [概要] を選択します。
[システム] タブでは、以下を管理できます。
- ・ **接続の有効化** — 現在有効になっている接続 (SMTP、POP3、ERS、および IP プロファイラ)
接続を有効または無効にするには
 - a. 接続項目の横にあるチェックボックスをオンまたはオフにします。
 - b. [保存] をクリックします。

- **コンポーネント** — InterScan MSS がネットワークを保護するために使用するウイルス対策、スパイウェア対策、およびスパムメール対策のコンポーネントのバージョン番号
コンポーネントを手動でアップデートするには
 - a. アップデートするコンポーネントのチェックボックスをオンにします。
 - b. [アップデート] をクリックします。コンポーネントの以前のバージョンにロールバックするには
 - a. ロールバックするコンポーネントのチェックボックスをオンにします。
 - b. [ロールバック] をクリックします。ページを表示更新するには
 - [表示更新] をクリックしてアップデート元に接続すると、[利用可能なバージョン] 列に最新のコンポーネントのバージョンが表示されます。
- **管理下のサーバ設定** — この InterScan MSS 管理データベースに登録されている他の InterScan MSS サービス
管理下のサーバサービスを開始または停止するには
 - 変更するサービスの [開始] または [停止] をクリックします。管理下のサーバサービスを登録解除するには
 - 管理下のサービスがアクティブでない (InterScan MSS サーバから切断されている) 場合は、そのサービスの [接続] 列に [削除] ボタンが表示されます。管理下のサービスをこの InterScan MSS サーバから削除するには、[削除] をクリックします。
 - 管理下のサービスは、次のいずれかの理由で切断される場合があります。
 - 検索サービスが削除されている。
 - InterScan MSS マネージャサービスが停止している。
 - 検索サーバが停止している。

統計を理解する

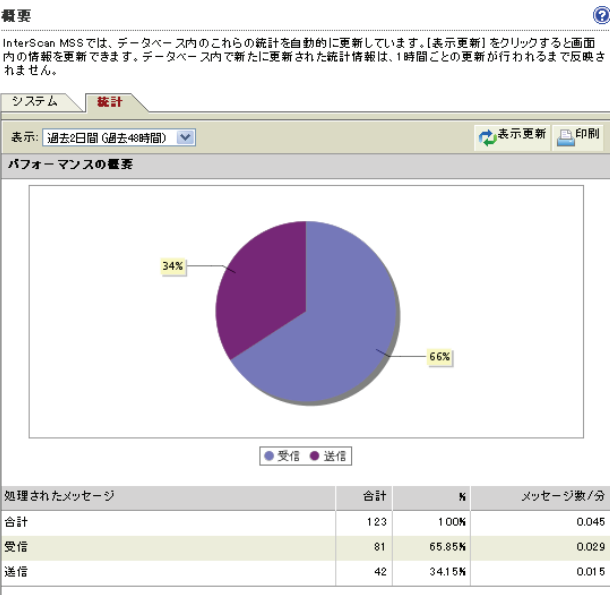
InterScan MSS では、パフォーマンス統計がグラフ形式および表形式で表示されます。この項では、値の算出方法、および [統計] タブの情報をグラフごとに分けて説明します。タブは [パフォーマンスの概要]、[検索パフォーマンス]、および [IP フィルタパフォーマンス] の 3 つにセクションに分かれています。

-
- 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
- ERS
- 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。

グラフ

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：

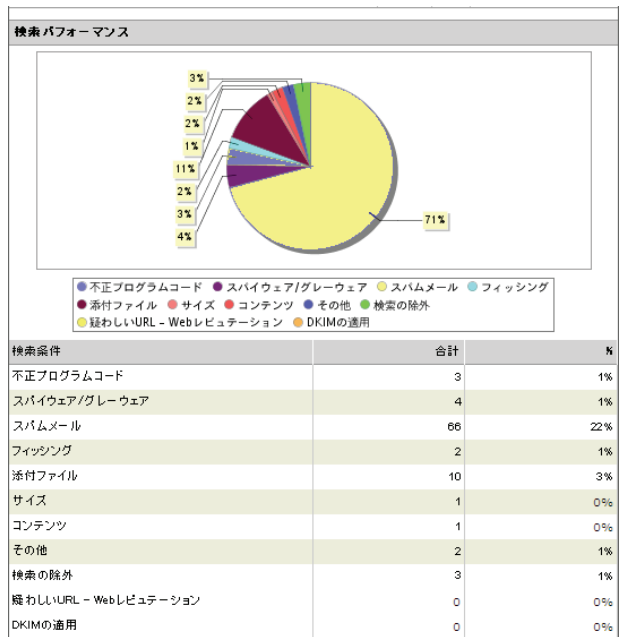
スパムメールメッセージの割合：71% = 66 / 93

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



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
- ERS

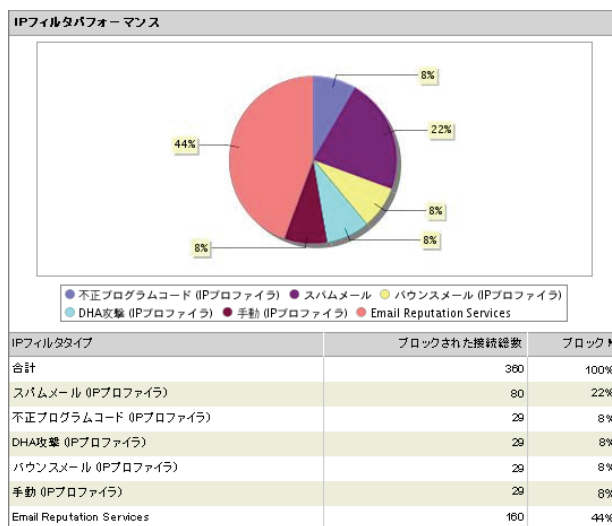
グラフおよび表で表示される値は、次のように算出されます。

値 = 特定の IP フィルタに一致したメッセージ件数 ÷ IP プロファイラおよび ERS 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 ERS 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 : $22\% = 80 / 360$



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。

表 5-1. レポート内容の説明

レポート内容	説明
ポリシーとトラフィックの概要	受信メッセージと送信メッセージの総数とサイズを表示します。また、特定の検索条件に一致するメッセージの数も表示します。
ウイルスと不正プログラムコードの概要	処理別のウイルスメッセージカウントの概要を表示します。
スパムメールの概要	スパムメール対策エンジン、ERS、IP プロファイラ、および処理別のスパムメールメッセージの総カウント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 プロファイラのブロックの概要」および「ERS のブロックの概要」が含まれます。「IP プロファイラのブロックの概要」は、IP プロファイラに届いて別の IP フィルタルールによってブロックされた送信者の接続の総数の概要を表示します。「ERS のブロックの概要」は、ERS に届いて ERS にブロックされた送信者の接続の総数を表示します。
トラフィックのメールアドレス [トップ 10]	送信および受信したメールメッセージのカウント総数によって順位付けた上位 10 のメールアドレスを表示します。
感染ウイルス名 [トップ 10]	検出カウントによって順位付けた上位 10 のウイルス名を表示します。
DHA 攻撃アドレスの IP アドレス [トップ 10]	ブロックされた DHA 攻撃のカウントによって順位付けた上位 10 の IP アドレスを表示します。
バウンスメール攻撃アドレスの IP アドレス [トップ 10]	ブロックされたバウンスメール攻撃のカウントによって順位付けた上位 10 の IP アドレスを表示します。

表 5-1. レポート内容の説明

レポート内容	説明
ウイルス受信者と送信者 [トップ 10]	受信および送信されたウイルスメッセージの総カウントによって順位付けた上位 10 のウイルス受信者と送信者を表示します。
最も頻繁に一致したルール [トップ 10]	各ルールに一致したメッセージの数によって順位付けた上位 10 のルール名を表示します。
スパムメール受信者 [トップ 10]	受信したスパムメールメッセージのカウント総数によって順位付けた上位 10 のスパムメール受信者のアドレスを表示します。
ERS によってブロックされた IP アドレス [トップ 10]	ERS によって切断された接続の数で順位付けた上位 10 のブロックされた IP アドレスです。
スパムメール送信元としてブロックされた IP アドレス [トップ 10]	ブロックされたスパムメールのカウントによって順位付けた上位 10 の IP アドレスです。
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 IP アドレス [トップ 10]	ブロックされたウイルスのカウントによって順位付けた上位 10 の IP アドレスです。
疑わしい URL が含まれたメッセージの送信者 [トップ 10]	疑わしい URL が含まれた受信メッセージ総数によって順位付けた上位 10 の送信者アドレスです。

1 回限りのレポートを管理する

1 回限りのレポートを生成すると、InterScan MSS の保護の概要を一目で把握できます。将来参照できるように、InterScan MSS はこの画面上の 1 回限りのレポートをすべて保持します。

InterScan MSS で、日次、週次、または月次レポートの自動作成を有効にすることもできます。

1 回限りのレポートを管理するには

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。[1 回限りのレポート] 画面が表示され、以前に生成した 1 回限りのレポートがリストに表示されます。
2. 表示内容を変更するには、次のいずれかの操作を実行します。
 - 表を並べ替えるには、下線の付いた任意の列見出しをクリックします。
 - リストに表示される項目が多すぎる場合は、リストの上部にある矢印ボタンをクリックして次のページに移動するか、表示するページの番号をドロップダウンリストから選択します。

- ・ リストで同時に表示される項目数を変更するには、表の下部にあるドロップダウンボックスから新しい表示値を選択します。
3. レポートを生成するには、[追加] をクリックします。レポートの生成プロセスには、数分かかります。レポートの生成が終了していない場合は、[出力] 列に [処理中] が表示されます。
 4. レポートを表示するには、[出力] の下で次の形式のいずれかをクリックします。
 - ・ **HTML** — 別のブラウザウィンドウでレポートを開きます。
 - ・ **CSV** — スプレッドシートアプリケーションで開くことができる、カンマ区切りの値のファイルとしてレポートを保存します。
 5. レポートを削除するには、そのレポートの横にあるチェックボックスをオンにしてから [削除] をクリックします。

注意： ERS レポートおよび IP プロファイラレポート内容は、これらの製品をアクティベートするまで出力できません。ERS および IP プロファイラをアクティベートする方法の詳細については、211 ページの「製品ライセンスを管理する」を参照してください。

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。[1 回限りのレポートの追加] 画面が表示されます。

1回限りのレポートの追加



名前:

日時: 2009/07/22 00 - 2009/07/23 00
年月日 時 年月日 時

☐ レポート内容

- ☐ ポリシーとトラフィックの概要
- ☐ ウイルスと不正プログラムコードの概要
- ☐ スпамメールの概要
- ☐ 送信者IPアドレスのブロックの概要
- ☐ トラフィックのメールアドレス [トップ10]
- ☐ 感染ウイルス名 [トップ10]
- ☐ DHA攻撃アドレスのIPアドレス [トップ10]
- ☐ バウンスメール攻撃アドレスのIPアドレス [トップ10]
- ☐ ウイルス受信者と送信者 [トップ10]
- ☐ 最も頻繁に一致したルール [トップ10]
- ☐ スпамメール受信者 [トップ10]
- ☐ ERSによってブロックされたIPアドレス [トップ10]
- ☐ スпамメール送信元としてブロックされたIPアドレス [トップ10]
- ☐ 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IPアドレス [トップ10]
- ☐ 疑わしいURLが含まれたメッセージの送信者 [トップ10]

- [名前] の横に、わかりやすい名前を入力します。
- [日時] の横で、レポートの対象となる期間を選択します。
- [レポート内容] の下で、レポートに記載する内容を選択します。
- [保存] をクリックします。レポートの生成プロセスには、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。

1回限りのレポート



1-1 / 1 ページ		
追加	削除	
レポート名	日時	出力
☐ ポリシーとトラフィックの概要	2007/08/06 17:09:25	処理中
10件/ページ		

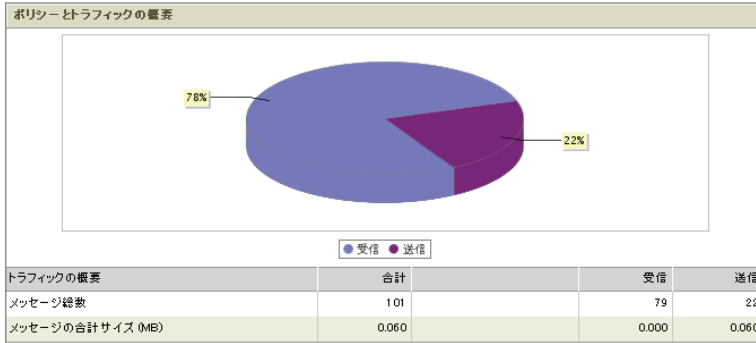
レポート作成後に、ハイパーリンク [HTML] および [CSV] がレポートテーブルに表示されます。

1回限りのレポート



1-3 / 3 ページ		
追加	削除	
レポート名	日時	出力
☐ トラフィックのメールアドレス [トップ10]	2007/08/06 17:11:47	HTML CSV
☐ ウイルスと不正プログラムコードの概要	2007/08/06 17:11:34	HTML CSV
☐ ポリシーとトラフィックの概要	2007/08/06 17:09:25	HTML CSV
10件/ページ		

7. レポートを HTML 形式で表示するには、[HTML] をクリックします。
8. 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うえにさらに 5 分程度かかる場合があります。

予約レポートを使用する

レポートを予約して、レポートの生成を自動化できます。InterScan MSS では、日次、週次、および月次レポートを用意しています。

予約レポートを管理するには

1. メニューから [レポート] → [予約レポート] の順に選択します。[保存された予約レポート] 画面が開き、[日次] タブが表示されます。
2. [週次] または [月次] タブをクリックして、対応するレポートを表示します。
3. レポートを表示するには、[出力] の下で次の形式のいずれかをクリックします。
 - **HTML** — 別のブラウザウィンドウでレポートを開きます。
 - **CSV** — スプレッドシートアプリケーションで開くことができる、カンマ区切りの値のファイルとしてレポートを保存します。
4. 表示内容を変更するには、次のいずれかの操作を実行します。
 - リストに表示される項目が多すぎる場合は、リストの上部にある矢印ボタンをクリックして次のページに移動します。

- リストで同時に表示される項目数を変更するには、表の下部にあるドロップダウンボックスから新しい表示値を選択します。
5. レポートを削除するには、そのレポートの横にあるチェックボックスをオンにしてから [削除] をクリックします。

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。

予約レポートの設定



レポートの種類	ステータス	スケジュール	設定	保存する数
日次レポート		2:00	設定	60
週次レポート		日曜日 2:00	設定	20
月次レポート		1日 2:00	設定	5

2. 次のいずれかのレポートの種類の [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。

日次レポートの設定 

予約レポートの設定 > 日次レポートの設定

☒ 日次レポートの作成

開始時刻: 2 時

☐ レポート内容

☒ ポリシーとトラフィックの概要
☒ ウイルスと不正プログラムコードの概要
☐ スпамメールの概要
☐ 送信者IPアドレスのブロックの概要
☐ トラフィックのメールアドレス [トップ10]
☐ 感染ウイルス名 [トップ10]
☐ DHA攻撃アドレスのIPアドレス [トップ10]
☐ バウンスメール攻撃アドレスのIPアドレス [トップ10]
☐ ウイルス受信者と送信者 [トップ10]
☐ 最も頻繁に一致したルール [トップ10]
☐ スпамメール受信者 [トップ10]
☒ ERSによってブロックされたIPアドレス [トップ10]
☐ スпамメール送信元としてブロックされたIPアドレス [トップ10]
☐ 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IPアドレス [トップ10]
☐ 疑わしいURLが含まれたメッセージの送信者 [トップ10]

保存 キャンセル

- 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。

- [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。

予約レポートの設定 

レポートの種類	ステータス	スケジュール	設定	保存する数
日次レポート		2:00	設定	60
週次レポート		日曜日 2:00	設定	20
月次レポート		1日 2:00	設定	5

保存 キャンセル

- 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。
- 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。

保存された予約レポート 

日次 週次 月次

 削除

保存されたレポート	出力
10件/ページ	

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。

保存された予約レポート 

日次 週次 月次

 削除

保存されたレポート	出力
☐ 2009/07/14	HTML CSV
☐ 2009/07/13	HTML CSV
☐ 2009/07/12	HTML CSV
☐ 2009/07/11	HTML CSV
☐ 2009/07/10	HTML CSV
☐ 2009/07/09	HTML CSV
15件/ページ	

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 — ログを設定する

手順 2 — ログのクエリを実行する

ログを設定する

InterScan MSS のログに記録される内容の詳細レベルと、ログが保存される期間を設定できます。また、検索サービスがローカルログを InterScan MSS 管理データベースに記録する頻度をアップデート期間として設定することもできます。

ログを設定するには

1. メニューから、[ログ] → [設定] の順に選択します。
2. [データベースへのログのレポート] で、次の項目を設定します。
 - **データベースのアップデート間隔** — InterScan MSS は、ここで設定した間隔で定期的にログを更新します。間隔には、1 ～ 60 の数字を選択します。60 を選択すると、InterScan MSS は 1 時間ごとにログを更新します。
 - **クエリ用にログを保存する日数** — InterScan MSS 管理データベースでレポートログを保存する日数を 1 ～ 60 の数字で入力します。
3. [ログファイル] で、次の項目を設定します。
 - **アプリケーションログの詳細レベル** — ログの詳細レベルを設定します。次のいずれかを選択します。
 - **標準** — ログの詳細度は標準です。このレベルでは、管理者が毎日の監視と管理作業を実行するのに必要とする基本的な情報が提供されます。
 - **詳細** — ログの詳細度は高くなります。すべての InterScan MSS プロセスで、ログに詳細情報が書き込まれます。このレベルのログには、Telnet セッション情報、一致するポリシー、実行されたフィルタ、および実行された処理が含まれます。
 - **診断** — 各イベントまたは各処理に対する総合的な情報です。[診断] レベルのログには、[詳細] レベルのすべての情報に加えて、SMTP ルーティング情報、および適用するポリシーを決定したルート一致情報が含まれます。
 - **デバッグ** — 最も完全で詳細なレベルのログが出力されます。デバッグログは、トラブルシューティングの場合にのみ使用することをお勧めします。

注意： 診断ログまたはデバッグログの出力は、InterScan MSS リソースを多く消費してシステムパフォーマンスを低下させる可能性があります。

- **ログファイルを保存する日数** — チェックボックスをオンにし、InterScan MSS でローカルログファイルを保存する日数を 1 ～ 150 の数字で入力します。InterScan MSS でログファイルが消去されないようにするには、このチェックボックスをオフにします。
- **サービス別ログファイルの最大サイズ** — チェックボックスをオンにし、プロセスやサービスのタイプごとにローカルログファイルのサイズ (MB) を 100 ～ 99999 の数字で入力します。サイズ制限をすべて解除するには、チェックボックスをオフにします。

注意： InterScan MSS のログファイルは、/opt/trend/imss/logs フォルダに格納されます。IP プロファイラのログファイルは、/opt/trend/ipprofiler/logs フォルダに格納されます。

それぞれのイベントの種類の日次ログファイルは午前 0 時に作成され、< 日付 >.< カウント > の接尾辞が付いています。1 日に 2 つ以上のログファイルがある場合は、< カウント > の接尾辞が増えます。

ログファイルのサイズが各サービスのログファイルの最大サイズを超える場合は、最も古いファイルが削除されます。

4. [保存] をクリックします。

ログのクエリを実行する

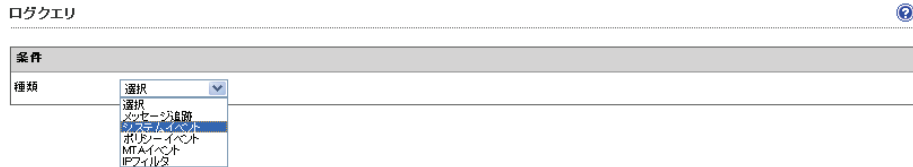
5 種類のイベントまたは情報のクエリを実行できます。

- **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ています。隔離されたメッセージの場合、クエリ結果では、一致したポリシーールルの名前および種類が表示されます。
- **システムイベント** — ユーザーアクセス、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ています。
- **ポリシーイベント** — 一致したポリシーールルの詳細、実行された処理、およびメッセージの詳細を記録しています。
- **MTA イベント** — 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ています。
- **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ています。

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。

メッセージ追跡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] の横の [メッセージ追跡] を選択します。メッセージのイベントログのクエリ画面が表示されます。
3. [日時] の横で、日付と時間の範囲を選択します。
4. 次のいずれかの追加情報を入力してください。
 - 件名
 - メッセージ ID
 - 送信者
 - 受信者

注意： いずれのフィールドでも、部分一致検索の場合はアスタリスクワイルドカードを使用します。

5. [ログ表示] をクリックします。日時、送信者、受信者、件名、およびポリシーの最終処理が各イベントに対して表示されます。
6. [日時] リンクをクリックして、次の情報を表示します。
 - 日時
 - 送信者
 - 受信者
 - 件名
 - 元のサイズ
 - メッセージ ID
 - 内部 ID
 - 検索サービス
 - 最終処理
 - 処理の詳細

7. 次のいずれかの処理を実行してください。
 - ・ リストで同時に表示される項目数を変更するには、表の上部にあるドロップダウンボックスから新しい表示値を選択します。
 - ・ クエリ結果を印刷するには、[現在のページを印刷] をクリックします。
 - ・ クエリ結果をカンマ区切りの値のファイルに保存するには、[CSV 形式で出力] をクリックします。

システムイベント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。
2. [種類] の横の [システムイベント] を選択します。システムイベントログのクエリ画面が表示されます。
3. [種類] の横にある 2 番目のドロップダウンボックスで、以下のいずれかを選択します。
 - ・ **すべてのイベント** — すべてのシステムイベントの日時と説明を表示します。
 - ・ **アップデート** — アップデートサーバから InterScan MSS 管理データベースへの検索エンジンとパターンファイルのアップデートが成功した日時を表示します。
 - ・ **サービスのステータス** — 検索サービスの開始または停止の日時と説明を表示します。
 - ・ **管理者アクティビティ** — InterScan MSS 設定の変更、管理者アカウントのログオンとログオフなど、管理者の主要なアクティビティの日時と説明を表示します。
 - ・ **エラー** — 検索エンジンやパターンファイルのアップデートの失敗など、InterScan MSS に発生したすべてのエラーの日時と説明を表示します。
4. [種類] の横にある 3 番目のドロップダウンボックスで、表示するサーバを選択します。
5. [日時] の横で、日付と時間の範囲を選択します。
6. [説明のキーワード] の横に、検索対象の用語を入力します。
7. [ログ表示] をクリックします。日時、コンポーネント、および説明が各イベントに対して表示されます。
8. 次のいずれかの処理を実行してください。
 - ・ リストで同時に表示される項目数を変更するには、表の上部にあるドロップダウンボックスから新しい表示値を選択します。
 - ・ 表を並べ替えるには、列のタイトルをクリックします。
 - ・ クエリ結果を印刷するには、[現在のページを印刷] をクリックします。
 - ・ クエリ結果をカンマ区切りの値のファイルに保存するには、[CSV 形式で出力] をクリックします。

ポリシーイベントログを表示するには

1. メニューから、[ログ] → [クエリ] の順に選択します。
2. [種類] の横の [ポリシーイベント] を選択します。ポリシーイベントログのクエリ画面が表示されます。
3. [種類] の横にある 2 番目のドロップダウンボックスで、ポリシーに関連する次の項目のいずれか、およびそのポリシーに対して設定したルールを選択します。
 - すべて
 - ウイルスまたは不正プログラムコード
 - スパムメール/フィッシングメール
 - Web レピュテーション
 - DKIM の適用
 - 添付ファイル
 - サイズ
 - コンテンツ
 - その他
 - 検索の除外
4. 次のいずれかの追加情報を入力してください。
 - 送信者
 - 受信者
 - ルール
 - 件名
 - 添付ファイル
 - メッセージ ID

注意： いずれかのテキストボックスを空白のままにすると、その項目についてのすべての結果が表示されます。

5. [ログ表示] をクリックします。日時、処理、ルール、およびメッセージ ID が各イベントに対して表示されます。
6. [日時] リンクをクリックして、次の情報を表示します。
 - 日時
 - 送信者

- 受信者
- 件名
- 元のサイズ
- 違反する添付ファイル
- ルールタイプ
- ルール
- 処理
- メッセージ ID
- 内部 ID
- 検索サービス

7. 次のいずれかの処理を実行してください。

- リストで同時に表示される項目数を変更するには、表の上部にあるドロップダウンボックスから新しい表示値を選択します。
- 表を並べ替えるには、列のタイトルをクリックします。
- クエリ結果を印刷するには、[現在のページを印刷] をクリックします。
- クエリ結果をカンマ区切りの値のファイルに保存するには、[CSV 形式で出力] をクリックします。

注意： - 「*A*;B*」は、A または B が含まれる文字列を表します。

- 「A*;B」は、A で開始する、または B で終了する文字列を表します。

- 「;」は、OR 演算を表します。

MTA イベント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。
2. [種類] の横の [MTA イベント] を選択します。MTA イベントログのクエリ画面が表示されます。
3. [日時] の横で、日付と時間の範囲を選択します。
4. [ログ表示] をクリックします。日時および MTA イベントの説明が表示されます。
5. 次のいずれかの処理を実行してください。
 - リストで同時に表示される項目数を変更するには、表の上部にあるドロップダウンボックスから新しい表示値を選択します。

- クエリ結果を印刷するには、[現在のページを印刷] をクリックします。
- クエリ結果をカンマ区切りの値のファイルに保存するには、[CSV 形式で出力] をクリックします。

IP フィルタのログを表示するには

1. メニューから、[ログ] → [クエリ] の順に選択します。
2. [種類] の横にある 2 番目のドロップダウンボックスで、IP フィルタに関連した次の項目のいずれかを選択します。
 - ERS
 - DHA 攻撃
 - バウンスメール
 - ウイルス
 - スпамメール
 - 手動 — ブロックするリストに指定した IP アドレスを参照します。
 - すべて
3. [日時] の横で、日付と時間の範囲を選択します。
4. [IP アドレス] の横に、検索対象の IP アドレスまたはドメイン名を入力します。
5. [ログ表示] をクリックします。各 IP アドレスまたはドメインに対する開始ブロック日時、最終ブロック日時、破棄された接続数の情報が表示されます。
6. 次のいずれかの処理を実行してください。
 - リストで同時に表示される項目数を変更するには、表の上部にあるドロップダウンボックスから新しい表示値を選択します。
 - クエリ結果を印刷するには、[現在のページを印刷] をクリックします。
 - クエリ結果をカンマ区切りの値のファイルに保存するには、[CSV 形式で出力] 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、受信者宛て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 を設定します。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、ユーザは隔離領域およびアーカイブ領域を管理し、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。

隔離およびアーカイブの設定 ?

隔離

アーカイブ

ディスク割り当て (検索サービスあたり) 100 MB

追加 削除

領域	保存日数	サイズ	アイテム	EUQ
☐ 初期設定の隔離	15 日	0MB	0	☒

保存

2. 隔離領域またはアーカイブ領域を設定するには、[隔離] タブ (初期設定) または [アーカイブ] タブをそれぞれクリックします。下の表に領域のリストが表示されます。
3. 検索サービスごとに、すべての隔離領域またはアーカイブ領域に許可される合計ディスクサイズを変更するには、[ディスク割り当て (検索サービスあたり)] の横に領域のサイズを入力し、次にドロップダウンボックスから [MB] または [GB] を選択します。
4. 隔離領域またはアーカイブ領域を追加するには、[追加] をクリックし、次の手順を実行します。
5. [名前] の横に、わかりやすい名前を入力します。
6. [メッセージの保存日数が次の日数を超えた場合に削除する] の横にあるテキストボックスに日数を入力します。この日数の後に InterScan MSS は隔離またはアーカイブされたメッセージを

削除します。この日数の間は削除されません。たとえば、15 と入力すると、隔離されたメッセージは 16 日後に削除されます。

7. [ウイルス対策ルール、フィッシング対策ルール、または Web レピュテーションルールに違反していないすべてのスパムメールおよびメールメッセージを EUQ データベースに同期させます (この領域でのみ)] を選択すると、エンドユーザメール隔離データベースにメッセージが自動的に保存されます。

注意： [ウイルス対策ルール、フィッシング対策ルール、または Web レピュテーションルールに違反していないすべてのスパムメールおよびメールメッセージを EUQ データベースに同期させます (この領域でのみ)] を選択すると、[隔離およびアーカイブの設定] 画面にある表の [エンドユーザメール隔離] 列にチェックマークが表示されます。

8. [保存] をクリックします。[隔離およびアーカイブの設定] 画面が再度表示されます。
9. 隔離領域またはアーカイブ領域を表示または変更するには、領域の名前をクリックし、上記の設定を行います。
10. 隔離領域またはアーカイブ領域を削除するには、その領域の横にあるチェックボックスをオンにしてから [削除] をクリックします。
11. 設定を変更したら、[保存] をクリックします。

隔離領域を管理する

InterScan MSS では、サーバ上の \$IMSS_HOME/queue/quarantine ディレクトリにメッセージを隔離できます。

ヒント： 後で分析して本来の受信者に送信する可能性のあるメッセージは、隔離しておくことをお勧めします。スパムメール検索条件に違反するメールやメッセージコンテンツ条件に違反するメールなど、メールの種類ごとに異なる隔離領域を作成してください。

隔離領域を変更する画面には、次のいずれかの画面から移動できます。

ポリシールールの [処理] 画面

ルールに対する処理を設定する場合は、次の手順を実行します。

1. [インターセプト] 処理の下 の [隔離先] の横にある [編集] をクリックします。[隔離] 画面が開いて、使用可能な隔離領域が表示されます。
2. 新しい隔離領域を追加するには、[追加] をクリックします。既存の隔離領域を変更するには、リストボックスで変更する隔離領域をクリックし、[編集] をクリックします。編集画面が表示されます。
3. [名前] の横に、隔離領域の名前を入力します。
4. 特定の日数が経過した後に隔離メールを自動的に削除するには、[メッセージの保存日数が次の日数を超えた場合に削除する] の横にあるテキストボックスに、1 から 60 の範囲で日数を入力します。この日数の後に InterScan MSS は隔離メッセージを削除します。この日数の間は削除されません。たとえば、15 と入力すると、隔離されたメッセージは 16 日後に削除されます。
5. [ウイルス対策ルール、フィッシング対策ルール、または Web レピュテーションルールに違反していないすべてのスパムメールおよびメールメッセージを EUQ データベースに同期させます (この領域でのみ)] を選択すると、エンドユーザメール隔離データベースにメッセージが自動的に保存されます。

注意： [ウイルス対策ルール、フィッシング対策ルール、または Web レピュテーションルールに違反していないすべてのスパムメールおよびメールメッセージを EUQ データベースに同期させます (この領域でのみ)] を選択すると、[隔離およびアーカイブの設定] 画面にある表の [エンドユーザメール隔離] 列にチェックマークが表示されます。

6. [保存] をクリックして、[隔離] 画面に戻ります。
7. [完了] をクリックして、処理の選択を続行します。
8. メッセージを隔離するには、[インターセプト] の下の [隔離先] オプションを選択して、ドロップダウンボックスから目的の隔離領域を選択します。

[隔離およびアーカイブ] → [設定]

1. [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] 画面が開き、初期設定では [隔離] タブが表示されます。
2. [ディスク割り当て (検索サービスあたり)] の横で次の手順を実行します。
 - a. 領域の最大サイズを入力します。
 - b. [MB] または [GB] を選択します。

注意： 隔離したメールメッセージの合計ディスクサイズが、検索サービスでの割り当てを超えた場合、割り当てサイズを超えないように最も古い隔離メッセージが削除されます。

3. 新しい隔離領域を追加するには、[追加] をクリックします。既存の隔離領域を変更するには、その領域名をクリックします。編集画面が表示されます。
4. [名前] の横に、隔離領域の名前を入力します。
5. 特定の日数が経過した後に隔離メールを自動的に削除するには、[メッセージの保存日数が次の日数を超えた場合に削除する] の横にあるテキストボックスに、1 から 60 の範囲で日数を入力します。この日数の後に InterScan MSS は隔離メッセージを削除します。この日数の間は削除されません。たとえば、15 と入力すると、隔離されたメッセージは 16 日後に削除されます。
6. [ウイルス対策ルール、フィッシング対策ルール、または Web レピュテーションルールに違反していないすべてのスパムメールおよびメールメッセージを EUQ データベースに同期させます (この領域でのみ)] を選択すると、エンドユーザーメール隔離データベースにメッセージが自動的に保存されます。

注意： [ウイルス対策ルール、フィッシング対策ルール、または Web レピュテーションルールに違反していないすべてのスパムメールおよびメールメッセージを EUQ データベースに同期させます (この領域でのみ)] を選択すると、[隔離およびアーカイブの設定] 画面にある表の [エンドユーザーメール隔離] 列にチェックマークが表示されます。

7. [保存] をクリックして、[隔離およびアーカイブの設定] 画面に戻ります。
8. [保存] をクリックします。

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。

ヒント： トレンドマイクロでは、ウイルス対策ルールに違反するメッセージや添付ファイルなど、ネットワークを危険にさらす可能性のあるアイテムは隔離することをお勧めします。隔離されたメッセージを再送信する前に、それがネットワークに脅威を与えないことを確認してください。

トレンドマイクロでは、後で参照するアイテムのみアーカイブしておくことをお勧めします。ウイルス対策ルールに違反するメールメッセージや添付ファイルなど、ネットワークにとって脅威となり得るアイテムは、隔離します。

隔離領域のクエリを実行するには

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。初期設定では [隔離] タブが表示されます。表示されない場合は、[隔離] をクリックします。
2. [条件] の下で、次の項目を設定します。
 - **検索** — 隔離領域、メールが隔離された理由、およびメールを検索した検索サービスを選択します。
 - **日付** — 日付と時間の範囲を選択します。
3. 次の項目に対する値を入力します。
 - **送信者**
 - **件名**
 - **受信者**
 - **添付ファイル**
 - **ルール**
 - **メッセージ ID**

注意： 複数の受信者または添付ファイルを含むメールのクエリを実行する場合は、「*<文字列>」と入力します（ここで<文字列>は受信者または添付ファイルのいずれかの名前を指します）。

4. [ログ表示] をクリックします。結果が画面の下部に表示され、日時、送信者、受信者、件名、およびこのメッセージを隔離した理由が示されます。
5. 表示内容を変更するには、次のいずれかの操作を実行します。
 - 表を並べ替えるには、任意の列見出しをクリックします（理由を除く）。
 - リストに表示される項目が多すぎる場合は、リストの上部にある矢印ボタンをクリックして次のページに移動するか、表示するページをドロップダウンリストから選択します。
 - リストで同時に表示される項目数を変更するには、表の下部にあるドロップダウンリストから新しい表示値を選択します。
6. 隔離されたメッセージの詳細を表示するには、そのアイテムの日時をクリックします。[隔離のクエリ] 画面が開いて、メールメッセージとそのすべての詳細情報が表示されます。
7. メッセージを再送信するには、クエリ結果表内のそのメッセージの横にあるチェックボックスをオンにしてから、[配信] または [再処理] をクリックします。

配信 — ウイルス検索ルール以外のすべてのルールを無視して、メッセージが受信者に直接送信されます。

再処理 — 現在のルールのみが無視されます。他のフィルタによってメッセージが再度隔離される場合があります。

ヒント： トレンドマイクロでは、ウイルス対策フィルタに違反するメールメッセージを再送信することをお勧めしません。再送信すると、ネットワークを危険にさらす可能性があります。

8. メッセージを削除するには、クエリ結果表内のそのメッセージの横にあるチェックボックスをオンにしてから [削除] をクリックします。

注意： 検索条件として [添付ファイル] が指定されている場合、InterScan MSS では添付ファイルのファイル名のみが記録および表示されます。ただし、特定のメールの添付ファイル数が、検索条件で指定されている最大数を超えた場合は、添付ファイル名は表示されません。

アーカイブ領域のクエリを実行するには

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。初期設定では [隔離] タブが表示されます。
2. [アーカイブ] タブをクリックします。
3. [条件] の下で、次の項目を設定します。

- ・ **検索** — アーカイブ領域、メールがアーカイブされた理由、およびメールを検索した検索サービスを選択します。
 - ・ **日付** — 時間の範囲を選択します。
4. 次の項目に対する値を入力します。
- ・ **送信者**
 - ・ **件名**
 - ・ **受信者**
 - ・ **添付ファイル**
 - ・ **ルール**
 - ・ **メッセージ ID**

注意： 複数の受信者または添付ファイルを含むメールのクエリを実行する場合は、「*<文字列>」と入力します（ここで<文字列>は受信者または添付ファイルのいずれかの名前を指します）。

5. [ログ表示] をクリックします。結果が画面の下部に表示され、日時、送信者、受信者、件名、およびこのメッセージをアーカイブした理由が示されます。
6. 表示内容を変更するには、次のいずれかの操作を実行します。
- ・ 表を並べ替えるには、任意の列見出しをクリックします（理由を除く）。
 - ・ リストに表示される項目が多すぎる場合は、リストの上部にある矢印ボタンをクリックして次のページに移動するか、表示するページをドロップダウンリストから選択します。
 - ・ リストで同時に表示される項目数を変更するには、表の下部にあるドロップダウンリストから新しい表示値を選択します。
7. アーカイブされたメッセージの詳細を表示するには、そのアイテムの日時をクリックします。[アーカイブのクエリ] 画面が開いて、メールメッセージとそのすべての詳細情報が表示されます。
8. メッセージを削除するには、クエリ結果表内のそのメッセージの横にあるチェックボックスをオンにしてから [削除] をクリックします。

注意： 検索条件として [添付ファイル] が指定されている場合、InterScan MSS では添付ファイルのファイル名のみが記録および表示されます。ただし、特定のメールの添付ファイル数が、検索条件で指定されている最大数を超えた場合は、添付ファイル名は表示されません。

隔離されたメッセージを表示する

隔離されたメッセージを表示するには

1. 隔離されたメッセージのクエリを実行したら、クエリ結果表内の隔離されたアイテムの日時をクリックします。以下の情報と共に [隔離のクエリ] 画面が表示されます。
 - 日時
 - メッセージ ID
 - 送信者
 - 理由
 - 受信者
 - ルール
 - 件名
 - 検索サービス
 - 元のサイズ
 - 内部 ID
 - 添付ファイル
2. [メッセージ表示] の横の [ヘッダ] または [メッセージ] をクリックします。
3. 次のボタンのいずれかをクリックします。
 - **リストに戻る** — クエリ画面に戻ります。
 - **配信** — メッセージを元の受信者に再送信します。
 - **再処理** — 再度メッセージを検索して、それに応じた処理を実行します。
 - **削除** — メッセージを削除します。
 - **ダウンロード** — メッセージをコンピュータに保存します。

ヒント: トレンドマイクロでは、ウイルス対策ルールに違反するメッセージまたは添付ファイルを保存することをお勧めしません。

アーカイブされたメッセージを表示する

アーカイブされたメッセージを表示するには

1. アーカイブされたメッセージのクエリを実行したら、クエリ結果表内のアーカイブされたアイテムの日時をクリックします。以下の情報と共に [アーカイブのクエリ] 画面が表示されます。
 - 日時
 - メッセージ ID
 - 送信者
 - 理由
 - 受信者
 - ルール
 - 件名
 - 検索サービス
 - 元のサイズ
 - 内部 ID
 - 添付ファイル
2. [メッセージ表示] の横の [ヘッダ] または [メッセージ] をクリックします。
3. 次のボタンのいずれかをクリックします。
 - リストに戻る — クエリ画面に戻ります。
 - 削除 — メッセージを削除します。
 - ダウンロード — メッセージをコンピュータに保存します。

ヒント： トレンドマイクロでは、ウイルス対策ルールに違反するメッセージまたは添付ファイルを保存することをお勧めしません。

ユーザ隔離アクセスを設定する

すべて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、そのユーザ宛て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. [管理] → [ユーザ隔離アクセス] の順にクリックします。[ユーザ隔離アクセス] 画面が表示されます。

ユーザ隔離アクセス

隔離されたスパムメールにアクセス可能なグループを指定します。これらのグループは、InterScan MSSサーバに対してLDAP認証を使用します。

☒ エンドユーザアクセスを有効にする ⓘ

☐ エンドユーザがEUGで隔離されたメールを直接配信することを許可する ⓘ

隔離されたスパムメールの保存日数: 7日 ▼

承認済み送信者の最大数の設定

エンドユーザ1人あたりの承認済み送信者の最大数: 50 ▼

ログインページのメッセージの指定

ログイン後にユーザに表示されるメッセージを入力します。改行を挿入するには「
」を使用します。HTMLを使用して、メッセージテキストのフォーマットを指定することもできます。

アクセスを有効にするLDAPグループの選択

☒ すべて有効にする

以下のLDAP検索でグループを選択します。

LDAPグループの検索 ▼

検索

選択したグループ

>> <<

保存 キャンセル

2. [エンドユーザアクセスを有効にする] をオンにします。
3. 隔離されたメッセージをエンドユーザが受信者に直接配信することを許可するには、[エンドユーザがEUGで隔離されたメールを直接配信することを許可する] をオンにします。メッセージは、ウイルス検索ルール以外のすべてのルールを無視します。
4. 隔離されたスパムメールを保持する日数を選択します。
5. エンドユーザが、隔離されたメールメッセージを精査するときに承認可能な送信者の最大数を選択します。
6. ユーザが隔離されたメールメッセージにアクセスした際に、ユーザのブラウザに表示されるログインページのメッセージを入力します。
7. 隔離されたスパムメールにLDAPグループのすべてのユーザがアクセスできるようにするには、[アクセスを有効にするLDAPグループの選択] で、[すべて有効にする] の横のチェックボックスをオンにします。

-
8. 個々の LDAP グループを追加するには、[すべて有効にする] チェックボックスをオフにし、次のいずれかを実行します。

グループを検索する場合

- a. 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。
- b. グループ名を入力します。
- c. [検索] をクリックします。下の表にグループが表示されます。
- d. 追加する LDAP グループをクリックします。
- e. [>] をクリックします。[選択したグループ] 表にグループが表示されます。

既存のグループを参照する場合

- a. ドロップダウンリストから、[LDAP グループの参照] を選択します。下の表にグループが表示されます。
 - b. 追加する LDAP グループをクリックします。
 - c. [>] をクリックします。[選択したグループ] 表にグループが表示されます。
9. [保存] をクリックします。

注意： LDAP グループに対してユーザ隔離アクセスを有効にする際、Microsoft Active Directory または Sun iPlanet Directory を LDAP サーバとして指定している場合は、LDAP グループの先頭または末尾、あるいはその両方にワイルドカードを使用できます。使用できるワイルドカードの例は、A*、*A、*A* です。Domino を LDAP サーバとして選択している場合は、末尾にしかワイルドカードを使用できません。使用できないワイルドカードの例は、*A、*A* です。

エンドユーザメール隔離データベースを追加する

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
- ・ さらに多くのユーザをエンドユーザメール隔離にアクセスさせる

エンドユーザメール隔離データベースがすで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。初期設定では [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。

接続

コンポーネント LDAP POP3 **データベース** Control Manager サーバ

InterScan MSS データベース

データベースのタイプ:	PostgreSQL
サーバ:	127.0.0.1
ユーザ名:	sa

EUQ データベース

登録 登録解除

☐	サーバ	ユーザ名
☐	10.148.20.76	sa

EUQ データベース設定

サーバ:

ポート:

ユーザ名:

パスワード:

OK 閉じる

4. 必要な情報を指定します。
5. [OK] をクリックします。

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か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。

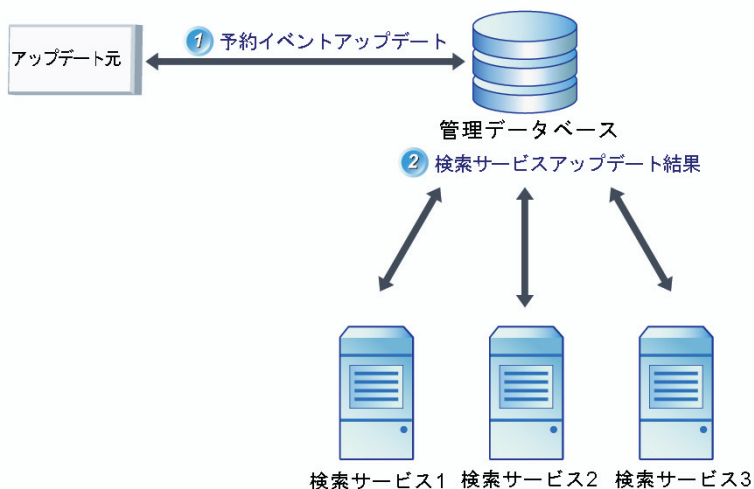


図 5-1. 検索エンジンおよびパターンファイルのアップデート

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がある、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。

通知 

イベント **通知設定** EUC通知

メール設定

宛先アドレス:
 複数のアドレスはセミコロン (;) で区切って入力してください。

送信者のメールアドレス:

サーバ名/IPアドレス:

SMTPポート番号:

文字コード: ▼

メッセージヘッダ:

メッセージフッタ:

SNMPトラップ

サーバ名 (IPまたはFQDN):

コミュニティ:

3. [メール設定] で、次の項目を設定します。
 - ・ **宛先アドレス** — 受信者のメールアドレスを入力します。
 - ・ **送信者のメールアドレス** — 送信者として表示されるメールアドレスを入力します。
 - ・ **サーバ名/IP アドレス** — ネットワーク上でメールを配信する SMTP サーバの完全修飾ドメイン名または IP アドレスを入力します。
 - ・ **SMTP ポート番号** — InterScan MSS が SMTP サーバに接続するために使用するポート番号を入力します。
 - ・ **文字コード** — InterScan MSS では、通知メッセージのエンコードにこの設定が使用されます。
 - ・ **メッセージヘッダ** — 通知の先頭に表示するテキストを入力します。
 - ・ **メッセージフッタ** — 通知の末尾に表示するテキストを入力します。
4. [SNMP トラップ] で、次の項目を設定します。

注意： SNMP トラップとは、管理上の注意が必要なイベントが発生したときに SNMP (Simple Network Management Protocol) サーバに送信される通知メッセージです。

- ・ **サーバ名** — SNMP サーバの完全修飾ドメイン名または IP アドレスを入力します。
- ・ **コミュニティ** — SNMP サーバのコミュニティ名を入力します。

注意： コミュニティとは、SNMP を実行するコンピュータおよび管理端末が属するグループです。すべての SNMP 管理端末に警告メッセージを送信するには、コミュニティ名として「public」を入力します。詳細については、SNMP のドキュメントを参照してください。

5. [保存] をクリックします。
設定ウィザードを使用している場合は、[次へ] 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 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。

通知 

イベント 通知設定 EUG通知

システムイベント通知	メール	SNMP
システムステータス		
次の間隔で通知: 10 分		
検索サービスの停止時間が次の長さを超えている場合: 10 分	☒	☐
検索サービスで利用できる空きディスク容量が次の値を下回った場合: 10240 MB	☒	☐
次の値を超える件数のメッセージが配信キューにある場合: 10000 メッセージ	☒	☐
次の値を超える件数のメッセージが再試行キューにある場合: 10000 メッセージ	☒	☐
予約アップデートイベント	メール	SNMP
ウイルス/スパイウェア/IntelliTrap パターンファイルの予約アップデート:		
失敗	☒	☐
成功	☒	☐
ウイルス検索エンジンの予約アップデート:		
失敗	☒	☐
成功	☒	☐
スパムメール検索エンジン/判定ルールの予約アップデート:		
失敗	☒	☐
成功	☒	☐
検索サービスアップデート結果	メール	SNMP
アップデートコンポーネントの適用に失敗した場合:	☒	☐

2. [システムステータス] で、次の項目を設定します。
 - ・ 次の間隔で通知 { } 分 — すべてのパフォーマンス通知の通知間隔を入力します。

それぞれの通知を編集するには、次のリンクをクリックします。

- **検索サービスの停止時間が次の長さを超えている場合** — 分数を入力します。
- **検索サービスで利用できる空きディスク容量が次の値を下回った場合** — メガバイト数を入力します。
- **次の値を超える件数のメッセージが配信キューにある場合** — メッセージ数を入力します。
- **次の値を超える件数のメッセージが再試行キューにある場合** — メッセージ数を入力します。

注意： [次の値を超える件数のメッセージが配信キューにある場合] および [次の値を超える件数のメッセージが再試行キューにある場合] の通知は、InterScan MSS が Postfix と共に実行される場合にのみ機能します。

3. [予約アップデートイベント] で、[失敗] と [成功] リンクをクリックして、コンポーネントのアップデートに関する通知を編集します。

注意： 予約アップデートイベントとは、アップデート元からの最新のエンジンおよびパターンファイルが InterScan MSS 管理データベースにアップデートされるイベントです。

4. [検索サービスアップデート結果] で、[アップデートコンポーネントの適用に失敗した場合] リンクをクリックして通知を編集します。

注意： 検索サービスアップデート結果とは、InterScan MSS 管理データベースから検索サービスへの最新のエンジンおよびパターンファイルのアップデートの結果です。

5. 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。
6. [保存] をクリックします。

エンドユーザメール隔離通知を設定する

エンドユーザメール隔離通知とは、エンドユーザメール隔離によって隔離されたユーザのメールメッセージに関する情報を通知するために InterScan MSS からユーザに送信される通知のことです。

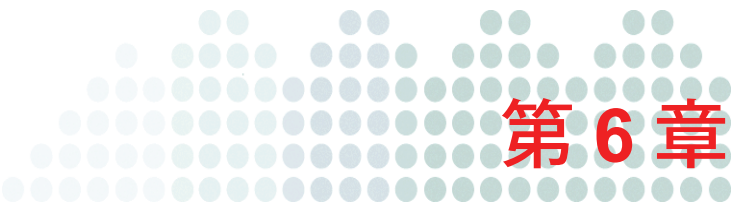
エンドユーザメール隔離通知を設定するには

1. メニューから [管理] → [通知] の順に選択します。初期設定では [イベント] タブが表示されません。
2. [EUQ 通知] をクリックします。
3. [エンドユーザメール隔離 (EUQ) 通知を有効にする] の横にあるチェックボックスをオンにします。
4. [通知スケジュール] で、次のいずれかの頻度を選択します。
 - **毎日** — ドロップダウンボックスから時刻を選択します。
 - **毎週** — ドロップダウンボックスから曜日と時刻を選択します。
5. [通知メールテンプレート] に、件名と通知内容を入力します。
通知に挿入できる変数のリストを表示するには、[変数リスト] をクリックします。
6. [保存] をクリックします。

通知を編集する

通知を編集するには

1. メニューから [管理] → [通知] の順に選択します。
2. 編集する通知をクリックします。その通知の編集画面が表示されます。
3. メールの件名とメッセージ、または SNMP メッセージを入力します。
通知に挿入できる変数のリストを表示するには、[変数リスト] をクリックします。
4. [保存] をクリックします。



第6章

エンドユーザメール隔離の使用

この章では、エンドユーザメール隔離 (EUQ) を使用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。

- 192 ページの「エンドユーザメール隔離について」
- 192 ページの「手順 1: LDAP を設定して有効にする」
- 195 ページの「手順 2: エンドユーザメール隔離を有効にする」
- 196 ページの「手順 3: エンドユーザメール隔離サービスを開始する」
- 196 ページの「手順 4: ユーザ隔離アクセスを有効にする」
- 199 ページの「手順 5: エンドユーザメール隔離の管理コンソールを開く」
- 200 ページの「エンドユーザメール隔離を無効にする」

エンドユーザメール隔離について

InterScan MSS では、スパムメールの管理効率を向上させるために、Web ベースのエンドユーザメール隔離機能を提供しています。Web ベースのエンドユーザメール隔離サービスを使用することで、エンドユーザは独自のスパムメール隔離を管理できます。スパムメールと判断されたメッセージは、隔離されます。これらのメッセージは、エンドユーザメール隔離エージェントによってデータベース内でインデックスが付けられます。これにより、エンドユーザはメッセージを再確認して、削除したり配信を許可したりできるようになります。

エンドユーザメール隔離を使用するには、次の操作を実行する必要があります。

192 ページの「手順 1: LDAP を設定して有効にする」

195 ページの「手順 2: エンドユーザメール隔離を有効にする」

196 ページの「手順 3: エンドユーザメール隔離サービスを開始する」

196 ページの「手順 4: ユーザ隔離アクセスを有効にする」

199 ページの「手順 5: エンドユーザメール隔離の管理コンソールを開く」

手順 1: LDAP を設定して有効にする

エンドユーザメール隔離を使用するには、LDAP を設定して、有効にする必要があります。

LDAP を有効にして設定するには

1. LDAP を設定して有効にするには、次の方法があります。
 - メニューから、[管理] → [InterScan MSS の設定] → [接続] を選択して、[LDAP] タブをクリックします。

接続 

コンポーネント **LDAP** POP3 データベース Control Managerサーバ

LDAP設定

ユーザグループ定義、管理者アカウント、またはエンドユーザメール隔離の認証にLDAPを使用する場合は、LDAP情報を入力します。

LDAPサーバの種類: Microsoft Active Directory

☒ 有効 **LDAP1**

LDAPサーバ:
例: example.comまたは192.168.10.1

待ちポート番号:
注意: LDAPサーバの種類がMicrosoft Active Directoryの場合、グローバルカタログポート3268を使用してください。

☐ 有効 **LDAP2**

LDAPサーバ:
例: example.comまたは192.168.10.1

待ちポート番号:
注意: LDAPサーバの種類がMicrosoft Active Directoryの場合、グローバルカタログポート3268を使用してください。

ポリシーサービスおよびEUQサービスのLDAPキャッシュ生存期間

キャッシュ生存期間 (分)

LDAP管理者

LDAP管理者アカウント:

パスワード:

基本識別名:
例: DC=foo, DC=fbonet, DC=org

認証方法:
☒ 簡易 
☐ 詳細: Active Directoryに対してKerberos認証を使用する

Kerberos認証の初期設定のレルム:

初期設定のドメイン:

発行行局 (KDC) および管理サーバ:

発行行局 (KDC) ポート番号:

- メニューから [管理] → [InterScan MSS の設定] → [設定ウィザード] の順に選択します。

InterScan MSS
 手順3/7

LDAP 設定

LDAP設定は、ユーザグループ定義、管理者権限、またはWeb隔離認証にLDAPを使用する場合にのみ入力します。Web隔離ツールを使用するには、LDAPを有効にする必要があります。

LDAP設定

LDAPサーバの種類: Microsoft Active Directory

☐ **有効 LDAP1**
 LDAPサーバ:
例: example.comまたは192.168.10.1

待機ポート番号: 389

☐ **有効 LDAP2**
 LDAPサーバ:
例: example.comまたは192.168.10.1

待機ポート番号: 389

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

キャッシュ生存期限 (分): 1440

LDAP管理者

LDAP管理者アカウント:

パスワード:

基本識別名:
例: DC=foo, DC=foonet, DC=org

認証方法:

☒ 簡易
☐ 詳細: Active Directoryに対してKerberos認証を使用する

Kerberos認証の初期設定のレルム:

初期設定のドメイン:

鍵発行局 (KDC) および管理サーバ:

鍵発行局 (KDC) ポート番号:

戻る
スキップ
次へ

2. すべての LDAP 設定を指定します。

194

手順 2: エンドユーザメール隔離を有効にする

エンドユーザメール隔離を有効にするには

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



隔離されたスパムメールにアクセス可能なグループを指定します。これらのグループは、InterScan MSS サーバに対してLDAP認証を使用します。

☒ エンドユーザアクセスを有効にする	
☐ エンドユーザがEUQで隔離されたメールを直接配信することを許可する	
隔離されたスパムメールの保存日数: 7日	
承認済み送信者の最大数の設定	
エンドユーザ1人あたりの承認済み送信者の最大数: 60	
ログインページのメッセージの指定	
ログイン後にユーザに表示されるメッセージを入力します。改行を挿入するには「 」を使用します。HTMLを使用して、メッセージテキストのフォーマットを指定することもできます。	
アクセスを有効にするLDAPグループの選択	
☒ すべて有効にする	
以下のLDAP検索でグループを選択します。	
LDAPグループの検索	検索
	選択したグループ
保存 キャンセル	

2. [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ます。
3. [保存] をクリックします。

手順 3: エンドユーザメール隔離サービスを開始する

エンドユーザメール隔離サービスを開始するには

1. メニューから [概要] を選択します。[システム] 画面が表示されます。
2. [管理下のサーバ設定] 表で、[Web 隔離] の [開始] をクリックします。

概要 

システム 統計

接続の有効化

☒ SMTP接続を許可する
 ☒ IPフィルタを有効にする

☒ POP3接続を許可する
 ... ☒ ERS ☒ IPプロファイラ

コンポーネント 前回の表示更新: 2009/07/23 14:03:02  表示更新

☐ 名前	現在のバージョン	利用可能なバージョン	アップデートスケジュール
☐ 検索エンジン	8.950.1.092	8.950.1.092	15 分
☐ ウイルスパターンファイル	6.157.00	6.157.00	15 分
☐ スパイウェアパターンファイル	0.773.00	0.773.00	15 分
☐ IntelliTrap パターンファイル IntelliTrap 除外ファイル	0.113.00 0.435.00	0.113.00 0.435.00	15 分
☐ スпамメール検索エンジン	5.600.1.016	5.600.1.016	15 分
☐ スпамメール判定ルール	16672.006	16672.006	15 分
☐ URLフィルタエンジン	3.000.1.029	3.000.1.027	15 分
InterScan MSS	Version 7.1 - Build Linux 1.230	該当なし	該当なし

管理下のサーバ設定

ホスト名	接続	検索サービス	ポリシーサービス	Web 隔離
post.tremic1.com	☒	☒ 停止	☒ 停止	☒ 開始

手順 4: ユーザ隔離アクセスを有効にする

ユーザ隔離アクセスを有効にして、InterScan MSS で誤ってスパムメールとして検出した可能性のある隔離されたスパムメールアイテムに、ユーザがアクセスできるようにします。クライアントは LDAP 認証を使用して、InterScan MSS のエンドユーザメール隔離サービスにアクセスします。

ユーザ隔離アクセスを設定して有効にするには

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。

ユーザ隔離アクセス



隔離されたスパムメールにアクセス可能なグループを指定します。これらのグループは、InterScan MSS サーバに対してLDAP認証を使用します。

☒ エンドユーザアクセスを有効にする	
☐ エンドユーザがEUQで隔離されたメールを直接配信することを許可する	
隔離されたスパムメールの保存日数: 7 日	
承認済み送信者の最大数の設定	
エンドユーザ1人あたりの承認済み送信者の最大数: 50	
ログインページのメッセージの指定	
ログイン後にユーザに表示されるメッセージを入力します。改行を挿入するには「 」を使用します。HTMLを使用して、メッセージテキストのフォーマットを指定することもできます。	
アクセスを有効にするLDAPグループの選択	
☒ すべて有効にする	
以下のLDAP検索でグループを選択します。	
LDAPグループの検索	検索
	選択したグループ >>> <<"/>
保存 キャンセル	

2. [エンドユーザアクセスを有効にする] をオンにします。
3. 隔離されたメッセージをエンドユーザが受信者に直接配信することを許可するには、[エンドユーザが EUQ で隔離されたメールを直接配信することを許可する] をオンにします。メッセージは、ウイルス検索ルール以外のすべてのルールを無視します。
4. 隔離されたスパムメールを保持する日数を選択します。
5. エンドユーザごとに承認済み送信者の最大数を選択します。
6. ユーザが隔離されたメールメッセージにアクセスした際に、ユーザのブラウザに表示されるログインページのメッセージを入力します。

7. 隔離されたスパムメールに LDAP グループのすべてのユーザがアクセスできるようにするには、[アクセスを有効にする LDAP グループの選択] で、[すべて有効にする] の横のチェックボックスをオンにします。
8. 個々の LDAP グループを追加するには、[すべて有効にする] チェックボックスをオフにし、次のいずれかを実行します。

グループを検索する場合

- a. 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。
- b. グループ名を入力します。
- c. [検索] をクリックします。下の表にグループが表示されます。
- d. 追加する LDAP グループをクリックします。
- e. [➤] をクリックします。[選択したグループ] 表にグループが表示されます。

既存のグループを参照する場合

- a. ドロップダウンリストから、[LDAP グループの参照] を選択します。下の表にグループが表示されます。
- b. 追加する LDAP グループをクリックします。
- c. [➤] をクリックします。[選択したグループ] 表にグループが表示されます。
- d. [保存] をクリックします。

手順 5: エンドユーザメール隔離の管理コンソールを開く

プログラムが配置されているコンピュータから、またはネットワークを経由したリモート操作で、エンドユーザメール隔離管理コンソールを表示できます。

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 を入力します。

- 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。

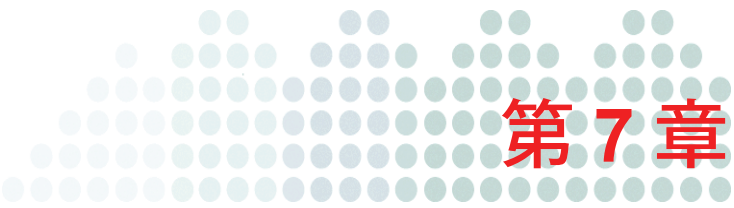
- **Microsoft Active Directory**
 - Kerberos を使用しない場合 `:user1@domain.com` (UPN) または `domain¥user1`
 - Kerberos を使用する場合 `:user1@domain.com`
- **Domino:** `user1/domain`
- **Sun iPlanet Directory:** `uid=user1, ou=people, dc=domain, dc=com`

エンドユーザメール隔離を無効にする

エンドユーザメール隔離を無効にする前に、隔離されたスパムメールの処理が必要なことをユーザに通知してください。

エンドユーザメール隔離を無効にするには

1. エンドユーザメール隔離の設定画面にアクセスするには、次の操作を実行します。
 - 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。
2. [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フにします。
3. [保存] をクリックします。



第7章

管理タスクの実行

この章では、アカウントの管理、デバイスの IP アドレスの変更、バックアップデータポートの使用などの重要な管理タスクを実行する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。

- 202 ページの「管理者アカウントを管理する」
- 205 ページの「接続を設定する」
- 211 ページの「製品ライセンスを管理する」
- 214 ページの「製品をアクティベートする」

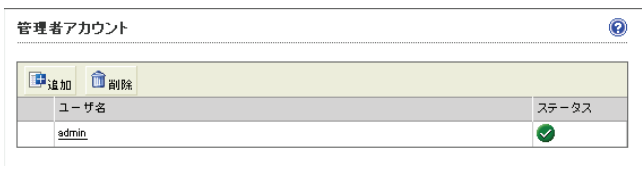
管理者アカウントを管理する

Trend Micro InterScan Messaging Security Suite 7.1 (以下、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。[管理者のアカウントの追加] 画面が開き、[認証] タブが表示されます。

3. 認証設定を指定します。
 - a. [アカウントを有効にする] を選択します。
 - b. 次の認証タイプを選択します。
 - **InterScan MSS 認証**: ユーザー名、新しいパスワードと確認のパスワードを入力します。
パスワードには、4 ～ 32 文字の英数字を使用してください。

- LDAP 認証: LDAP のユーザ名を入力します。
- c. [保存] をクリックします。
- 4. [権限] タブをクリックします。[権限] 画面が表示されます。

管理者のアカウントの追加 ?

認証

権限

アクセス領域	表示/変更	表示	権限なし
概要	☐	☐	☒
ポリシー	☐	☐	☒
IPフィルタ	☐	☐	☒
レポート	☐	☐	☒
ログ	☐	☐	☒
隔離およびアーカイブ	☐	☐	☒
管理	☐	☐	☒

5. 権限設定を指定します。
 - a. InterScan MSS 管理コンソールメニューに表示される次のアクセス領域のそれぞれに、[表示 / 変更]、[表示]、または [権限なし] のいずれかを選択します。
 - 概要
 - ポリシー
 - IP フィルタ
 - レポート
 - ログ
 - 隔離とアーカイブ
 - 管理
 - b. [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。カスタム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カスタム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

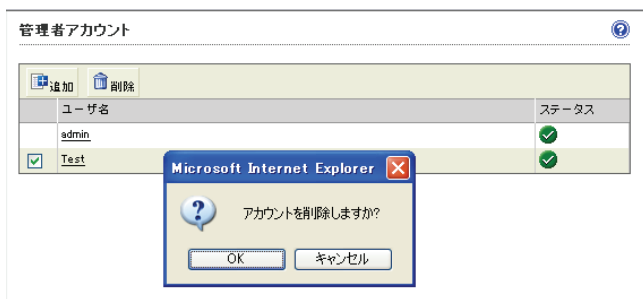
ロールが変更になった場合やその他の組織変更があった場合、カスタム管理者アカウントの権限を変更または削除できます。

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. 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. 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します。



注意： 削除できるのはカスタム管理者アカウントのみです。初期設定の InterScan MSS 管理者アカウントは削除できません。

接続を設定する

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。初期設定では [コンポーネント] タブが表示されます。

接続

コンポーネント LDAP POP3 データベース Control Manager サーバ

すべての検索サービスの設定

InterScan MSS マネージャポート: 15506

すべてのポリシーサービスの設定

ポリシーサービスポート: 5060

プロトコル: HTTP

キープアライブ: ☐ 有効

バックログされる要求数の上限: 100

保存 キャンセル

2. [すべての検索サービスの設定] で、InterScan MSS が検索サービスと通信するために使用するポート番号を入力します。

注意： ユーザがポート番号を設定していない場合、またはファイアウォールがこのポートを開けなかった場合、管理サーバは [概要] 画面で切断された状態で表示されます。また、管理サービスで変更は一切適用されません。

3. [すべてのポリシーサービスの設定] で、次の項目を設定します。
 - **ポリシーサービスポート：** InterScan MSS がポリシーサービスと通信するために使用するポート番号を入力します。ポリシーサービスが InterScan MSS との通信に使用する初期設定のポート番号は 5060 です。
 - **プロトコル：** 検索サービスがポリシーサービスとの通信に使用するプロトコルの種類として [HTTP] または [HTTPS] を選択します。
 - **キープアライブ：** このチェックボックスをオンにすると、検索サービスとポリシーサービス間の常時アクティブな接続が維持されるためポリシー検索が強化されます。
 - **バックログされる要求数の上限：** InterScan MSS が後で処理できるまで保持する要求の最大数を入力します。
4. [保存] をクリックします。

LDAP を設定する

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関する LDAP 設定を行います。InterScan MSS グループごとに最大で 2 台の LDAP サーバを有効にできます。

バックアップ LDAP サーバを利用できるようにするには、2 台の LDAP サーバを設定します。

LDAP を設定するには

1. [管理] → [InterScan MSS の設定] → [接続] の順に選択します。初期設定では [コンポーネント] タブが表示されます。
2. [LDAP] タブをクリックします。
3. [LDAP サーバの種類] で、ネットワーク上の LDAP サーバの種類として次のいずれかを選択します。
 - Microsoft Active Directory
 - Domino
 - Sun iPlanet Directory
4. [有効 LDAP1] のチェックボックスをオンにします。
5. [LDAP サーバ] に、サーバの名前または IP アドレスを入力します。
6. [待機ポート番号] に、LDAP サーバがアクセス要求の待機ポートとして使用するポート番号を入力します。
7. 必要に応じて [有効 LDAP2] の下の項目を設定します。
8. [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] に、キャッシュ生存期限を分単位で入力します。

キャッシュ生存期限：この値によって LDAP クエリの結果がキャッシュに保持される期間が決まります。長い期間を指定すると、ポリシー実行中の LDAP クエリが強化されます。ただし、LDAP サーバの変化に対するポリシーサーバの反応は低下します。期間を短くすると、InterScan MSS が LDAP クエリをさらに頻繁に実行する必要があるため、パフォーマンスは低下します。

9. [LDAP 管理者] に、管理者アカウント、対応するパスワードおよび基本識別名を入力します。
LDAP サーバの種類別のこのセクションで指定する内容については、以下の表を参照してください。

表 7-1. LDAP サーバの種類

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@domain.com (UPN) または domain¥user1 Kerberos を使用する場合： user1@domain.com	dc=domain, dc=com	簡易 詳細 (Kerberos 使用)
Domino	user1/domain	該当なし	簡易
Sun iPlanet Directory	uid=user1, ou=people, dc=domain, dc=com	dc=domain, dc=com	簡易

10. 次のいずれかの認証方法を選択します。
- 簡易
 - 詳細：Active Directory に対して Kerberos 認証を使用します。次の項目を設定します。
 - **Kerberos 認証の初期設定のレルム**：クライアントの初期設定の Kerberos レルムを指定します。Windows のドメイン名を大文字で指定する必要があります (Kerberos 認証では大文字と小文字が区別されます)。
 - **初期設定のドメイン**：レルムに対応するインターネットドメイン名を指定します。
 - **鍵発行局 (KDC) および管理サーバ**：レルムの鍵発行局のホスト名または IP アドレスを指定します。通常はドメインコントローラの情報を指定します。
 - **鍵発行局 (KDC) ポート番号**：発行局に関連付けられたポート番号を指定します。
11. [保存] をクリックします。
設定ウィザードを使用している場合は、[次へ] をクリックします。

注意： IBM Domino と Sun iPlanet では、簡易認証方式のみがサポートされます。

LDAP 管理者アカウントのドメイン名を DNS で解決できる場合は、初期設定のレルムに入力した値がどんな値でも Kerberos 認証は成功します。
LDAP 管理者アカウントのドメイン名が解決できない場合は、Kerberos 認証では初期設定のレルムを使用してチェックを行います。

POP3 を設定する

InterScan MSS では、SMTP トラフィックの他に、クライアントが POP3 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。

ヒント： POP3 メッセージフィルタを使用するには、[概要] → [システム] 画面で [POP3 接続を許可する] を有効にします。このオプションは、初期設定では選択されていません。

POP3 を設定するには

1. [管理] → [InterScan MSS の設定] → [接続] の順に選択します。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. インターネット上の任意の POP3 サーバ (接続先 POP3 サーバ情報を接続クライアントが指定する場合) からの接続を設定するには、InterScan MSS が受信 POP3 接続用に使用するポート番号を [一般的な POP3 接続] に入力します。
4. 特定の POP3 サーバ (接続先 POP3 サーバ情報を InterScan MSS で指定する場合) からの接続を設定するには、次の手順を実行します。
 - a. [専用の POP3 接続] の下の [追加] をクリックします。[専用の POP3 接続] 画面が表示されます。
 - b. InterScan MSS が受信 POP3 接続用に使用するポート番号、POP3 サーバの IP アドレス、および POP3 サーバのポート番号を入力します。
 - c. [OK] をクリックします。
 - d. 既存の接続を変更するには、その接続名をクリックします。
5. [メッセージテキスト] で、ユーザが受信しようとしているメールメッセージがフィルタに一致して隔離または削除された場合に InterScan MSS からユーザに送信されるメッセージを編集します。
6. [保存] をクリックします。

注意： InterScan MSS のデーモンが正しく動作するためには、検索サービスの受信ポートが待機状態になっている必要があります。

一般的な POP3 サービスを設定する

一般的な POP3 サービスでは、POP3 クライアントは USER コマンドを使用してログオンし、値を区切るために UserServerSeparator 文字を使用して、ユーザ名、実際の POP3 サーバ、オプションのポート番号を指定します。

例 1: UserServerSeparator 文字「#」を使用して、ユーザ「User1」をサーバ「Server1」に接続する場合、クライアントは次の USER コマンドを発行します。

```
USER User1#Server1
```

例 2: Server1 上のポート 2000 に接続する場合は、次のコマンドが使用されます。

```
USER User1#Server1#2000
```

注意： ポート番号を指定しないと、InterScan MSS では初期設定値の 110 を使用します。

次の例では、Outlook で一般的な POP3 を設定する方法を示します。

1. InterScan MSS 検索サービスの IP アドレス「192.168.11.147」で、POP3 サーバアドレスを指定します。
2. ユーザ名「test123#192.168.11.252」を入力します。
3. POP3 ポートを 110 に設定します。

専用の POP3 サービスを設定する

専用の POP3 サービスでは、POP3 サービスは常に特定の POP3 サーバに接続されます。InterScan MSS では、このサービスを POP3 ログオン、および AUTH コマンドを使用したすべての種類のログオンに使用します。このサービスについては、クライアントの接続先となり得る特定の POP3 サーバごとに、プロキシ上で個別のポートを設定する必要があります。

次の例では、Outlook で専用の POP3 を設定する方法を示します。

1. InterScan MSS 検索サービスの IP アドレス「192.168.11.147」で、POP3 サーバアドレスを指定します。
2. ユーザ名「test123」を入力します。
3. POP3 ポートを 1100 に設定します。これは、InterScan MSS の専用の POP3 サービスが待機するポートです。

データベースを設定する

データベースを設定するには

1. [管理] → [InterScan MSS の設定] → [接続] の順に選択します。初期設定では [コンポーネント] タブが表示されます。
2. [データベース] タブをクリックします。表の上部に、InterScan MSS 管理データベースの種類、データベースサーバの名前または IP アドレス、およびユーザ名が表示されます。

3. エンドユーザメール隔離データベースを InterScan MSS に登録するには、[EUQ データベース] の下の [登録] をクリックします。

注意： エンドユーザメール隔離データベースをインストールするには、インストーラを使用する必要があります。インストーラは、インストール後データベースを自動的に InterScan MSS に登録します。

4. エンドユーザメール隔離データベースサーバの完全修飾ドメイン名または IP アドレス、ポート番号、管理者のユーザ名およびパスワードを入力します。
5. [OK] をクリックします。
6. 既存のデータベースを変更するには、そのデータベース名をクリックします。
7. 既存のデータベースの登録を InterScan MSS から解除する場合、データベースの横のチェックボックスをオンにして、[登録解除] をクリックしてください。

注意： データベースはいつでも再登録することができます。データベースの登録解除によって、データベースが削除されたり、実際のデータベースサーバに影響したりすることはありません。InterScan MSS でそのデータベースを使用しなくなるだけです。

Control Manager を設定する

Control Manager 5.0 (Patch 3 以上) を使用して InterScan MSS を管理するために、InterScan MSS サーバの Control Manager/MCP エージェントを有効にし、Control Manager サーバを設定します。Control Manager サーバと InterScan MSS の間にプロキシサーバが配置されている場合は、プロキシを設定してください。Control Manager サーバと InterScan MSS の間にファイアウォールが配置されている場合は、ポート転送がファイアウォールのポート転送機能と連携するように設定してください。

Control Manager を設定するには

1. [管理] → [InterScan MSS の設定] → [接続] の順に選択します。初期設定では [コンポーネント] タブが表示されます。
2. [Control Manager サーバ] タブをクリックします。
3. [Control 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。
4. [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。

5. [通信プロトコル] で、[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 であり、HTTPS 用の初期設定ポート番号は 443 です。
6. [Web サーバ認証] に、Control Manager Web サーバにアクセスするためのアクセスアカウント情報を入力します。
7. [プロキシ設定] で [プロキシを有効にする] を選択します。
8. [プロキシタイプ] で、プロキシサーバが使用するプロトコルとして [HTTP]、[SOCKS4]、または [SOCKS5] を選択します。
9. プロキシサーバの完全修飾ドメイン名または IP アドレス、ポート番号、およびユーザ名とパスワードを入力します。
10. [保存] をクリックします。

設定ウィザードを使用している場合は、[次へ] をクリックします。

エージェントを有効にした場合、しばらくするとエージェントが Control Manager サーバに登録されます。エージェントを無効にした場合、InterScan MSS が直ちに Control Manager サーバからログオフします。登録状況の変更については、Control Manager 管理コンソールで確認してください。

Control Manager の詳細については、Control Manager のドキュメントを参照してください。

Control Manager から登録を解除するには

1. [管理] → [InterScan MSS の設定] → [接続] の順に選択します。初期設定では [コンポーネント] タブが表示されます。
2. [Control Manager サーバ] タブをクリックします。
3. [全エージェントを登録解除] ボタンをクリックします。

製品ライセンスを管理する

InterScan MSS では、次のコンポーネントを使用できます。

- **ウイルス対策およびコンテンツフィルタ** : 基本的なウイルス検索とフィルタ機能です。この製品は、InterScan MSS プログラムそのものと考えられます。
- **スパムメール対策 (コンテンツ検索)** : オプションのスパムメールフィルタで、メールの内容からスパムメールを判定します。
- **IP フィルタ** : オプションのスパムメール対策機能で、既知のスパムメール送信者を IP アドレスから判定します。IP フィルタには、以下が含まれます。

- **ERS: Email Reputation Services (ERS)** は、受信メール接続の IP アドレスをトレンドマイクロの Smart Protection Network に転送して、広範なレピュテーションデータベースと照合することで、スパムメールがコンピュータネットワークに侵入する前に検出してブロックすることを目的としたものです。
- **IP プロファイラ**：IP プロファイラを使用すると、しきい値を設定して、潜在的なインターネットの脅威を検出したときの InterScan MSS の対処方法を決定することができます。
 - **スパムメール**：不要な広告コンテンツが含まれるメール。
 - **ウイルス**：トロイの木馬プログラムなどの各種のウイルス脅威。
 - **DHA (ディレクトリハーベスト攻撃)**：ユーザのメールアドレスを収集し、スパムメール用のデータベースに追加するためにスパムメール発信者が使用する手法。
 - **バウンスメール**：送信したメールが相手に届かずに、不達で送り返されたメールメッセージ。

管理コンソールから InterScan MSS 製品をアクティベートできます。製品ライセンスの有効期限が切れている場合は、ライセンスを更新して新しいアクティベーションコードを入手し、管理コンソールからコードを指定する必要があります。製品がアクティベートされない場合は、その機能は無効になります。

製品ライセンスを表示する

既存のライセンスを表示するには

1. [管理] → [製品ライセンス] の順に選択します。各ライセンスの簡単な概要が表示されます。
 - **製品**
 - **バージョン**
 - **製品版**：ライセンス契約に同意いただき、ライセンスされた製品を購入していることを意味します。
 - **体験版**：試用期限が設定された体験版の製品を使用していることを意味します。取得したアクティベーションコードによって試用期間が異なります。

試用期間の期限が切れる 14 日前から、管理コンソールに警告メッセージが表示されます。

試用期間後も InterScan MSS を使用してネットワークの保護を継続するには、InterScan MSS の製品版を購入して、新しいアクティベーションコードを指定する必要があります。

- **アクティベーションコード**: xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx という形式の 31 文字の英数字からなるコード。製品版購入時に取得したアクティベーションコードを [製品ライセンス] ページで入力します。
 - **ステータス**: その製品の有効期限が切れているか、アクティベートされているかを示します。
 - **ライセンスの有効期限**: トレンドマイクロのアップデートサーバから最新の検索エンジンとパターンファイルをダウンロードできなくなる日付。最新の Web からの脅威に対してネットワークを保護するには、販売店に連絡してライセンスを更新する必要があります。
2. [詳細情報をオンラインで確認] をクリックすると、各ライセンスの詳細情報が表示されます。
 3. 最新のライセンスステータスを確認するには、[ステータス更新] をクリックします。

ライセンスを更新またはアクティベートする

ライセンスの更新には 2 つの方法があります。

- **新しいアクティベーションコードを取得する**: 販売店に問い合わせでライセンス契約を更新し、新しいアクティベーションコードを入手し、[製品ライセンス情報] 画面でそのコードを指定します。
- **既存のアクティベーションコードの有効期限を延長する**: 販売店に問い合わせでライセンス契約を更新し、アクティベーションコードの有効期限を延長し、ライセンスのステータスを手動で延長するか、InterScan MSS によって自動的に延長されるまで待ちます。

新しいアクティベーションコードを使用して更新するには

1. [管理] → [製品ライセンス] の順に選択します。各ライセンスの簡単な概要が表示されます。
2. [アクティベーションコード] の横にある [新規入力] をクリックします。[アクティベーションコードの新規入力] 画面が表示されます。
3. [新しいコード] の横に、新しいコードを入力します。
4. [アクティベート] をクリックします。管理コンソールからトレンドマイクロの Web サイトにアクセスし、ライセンスをアクティベートすることができます。トレンドマイクロの Web サイトにアクセスできない場合は、ネットワーク設定を確認し再試行してください。

既存のアクティベーションコードを使用して更新するには

1. [管理] → [製品ライセンス] の順に選択します。各ライセンスの簡単な概要が表示されます。
2. 更新するライセンスについて、[詳細情報をオンラインで確認] をクリックします。
3. [ステータス更新] をクリックします。管理コンソールからトレンドマイクロの Web サイトにアクセスし、ライセンスをアクティベートします。トレンドマイクロの Web サイトにアクセスできない場合は、ネットワーク設定を確認し再試行してください。

現在のライセンスの有効期限前の 90 日目、60 日目、30 日目、0 日目と、現在のライセンスの有効期限後の毎日、InterScan MSS によって自動的にライセンスのステータスがチェックされ、有効期限が延長されている場合はライセンスのステータスが更新されます。

ヒント： InterScan MSS によってライセンスのステータスが自動的に更新されるまで待つことができます。ただし、アクティベーションコードの有効期限を延長後、直ちに手動で更新することをお勧めします。

製品をアクティベートする

アクティベーションコードをお持ちでない場合は、製品に添付されているレジストレーションキーを使用してオンラインで登録してください。

次の画面のいずれかを使用して製品をアクティベートします。

- 設定ウィザードの手順 6
- [管理] → [製品ライセンス]

設定ウィザードの手順 6 からアクティベートするには

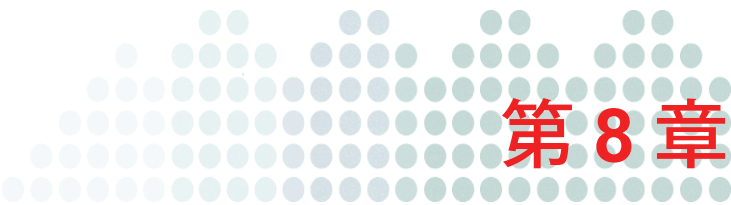
1. アクティベーションコードを持っていない場合は、[オンライン登録] をクリックします。登録が完了すると、トレンドマイクロからアクティベーションコードがメールで送信されます。
2. アクティベーションコードを入力して次のいずれかをアクティベートします。
 - InterScan MSS (ウイルス対策およびコンテンツフィルタ)
 - スパムメール対策 (コンテンツ検索)
3. [次へ] をクリックします。

注意： アクティベーションコードは、XX-XXXX-XXXX-XXXX-XXXX-XXXX という形式で送られてきます。

[管理] → [製品ライセンス] からアクティベートするには

1. [管理] → [製品ライセンス] の順に選択します。各ライセンスの簡単な概要が表示されます。
2. [アクティベーションコード] の横にある [新規入力] をクリックします。[アクティベーションコードの新規入力] 画面が表示されます。
3. [新しいコード] の横に、新しいコードを入力します。

4. [アクティベート] をクリックします。管理コンソールからトレンドマイクロの Web サイトにアクセスし、ライセンスをアクティベートすることができます。トレンドマイクロの Web サイトにアクセスできない場合は、ネットワーク設定を確認し再試行してください。



第8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 7.1 (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。

- 218 ページの「トラブルシューティング」
- 227 ページの「よくある質問 (Q&A)」
- 239 ページの「製品サポート情報」
- 239 ページの「サポートサービスについて」
- 240 ページの「製品 Q&A のご案内」
- 240 ページの「セキュリティ情報」
- 241 ページの「トレンドマイクロへのウイルス解析依頼」
- 241 ページの「ウイルス解析サポートセンター「TrendLabs」」

トラブルシューティング

表 8-1 に、InterScan MSS のインストール、設定、または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、「Trend Micro InterScan Messaging Security Suite 7.1 インストールガイド」を参照してください。

表 8-1. 問題のトラブルシューティング

問題	推奨される解決策
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 227 ページの表 8-2 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、244 ページの「InterScan MSS スクリプトの使用」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 8-1. 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、Email Reputation Services (以下、ERS)、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	ERS 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、HTTP クエリと有効な DNS 設定が必要です。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するには 1. 次のコマンドを使用します。 <pre>nslookup licenseupdate.trendmicro.com</pre> このコマンドを実行すると、InterScan MSS サーバの IP アドレスが返されます。 インターネットへの接続にプロキシサーバが必要な場合は、プロキシ設定をチェックして、HTTP 要求が確実に http://licenseupdate.trendmicro.com に到達できることを確認します。 管理コンソールからプロキシ設定を確認するには 1. [管理] → [アップデート] の順にクリックします。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文字セットを選択します。
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。

表 8-1. 問題のトラブルシューティング

問題	推奨される解決策
[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が発生した。 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。
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。
Web レピュテーションを有効にした後、メッセージの検索時間が非常に長くなる。	Web レピュテーションでは、トレンドマイクロ Web レピュテーションサーバにクエリを実行する必要があります。InterScan MSS 検索サービスから外部ネットワークへの HTTP 接続を確認してください。インターネットへの接続にプロキシサーバが必要な場合は、[アップデート元] 画面でプロキシを設定します。 1. [管理] → [アップデート] → [アップデート元] の順にクリックします。[アップデート元] 画面が表示されます。 2. [アップデートおよび Web レピュテーションのクエリ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ます。 3. プロキシを設定します。 4. [保存] をクリックします。 Web レピュテーションに関する問題については、 /opt/trend/imss/log フォルダの wrsagent.* ファイルを確認してください。

表 8-1. 問題のトラブルシューティング

問題	推奨される解決策
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	次の手順を実行してください。 - 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 を入力します。 - プライマリエンドユーザメール隔離サービス — <code>https://<サーバ IP アドレス>:8447</code> - セカンダリエンドユーザメール隔離サービス — <code>https://<サーバ IP アドレス>:8446</code> - 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 サーバは、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 サーバが起動していない場合、ユーザは、次の通常の IP アドレス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。 <code>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/</code>

表 8-1. 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	次の手順を実行してください。 - 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。 - 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。 - メニューから、[管理] → [InterScan MSS の設定] → [接続] → [LDAP] を選択します。 - 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。 - 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。 [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ます。 - 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。 - 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、34 ページの「ログオン名形式」を参照してください。 - 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。 - メニューから、[ログ] → [設定] の順に選択します。 - 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。 - メニューから [概要] 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。 - 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。 /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。

表 8-1. 問題のトラブルシューティング

問題	推奨される解決策
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。
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では、管理者がアクセスを許可するようにエンドユーザメール隔離を設定している場合にのみ、ユーザは隔離されたメールメッセージにアクセスできます。エンドユーザに隔離領域が表示されるようにするには 1. [隔離およびアーカイブ] → [設定] の順に選択します。 2. エンドユーザメール隔離に同期させる隔離領域のリンクをクリックします。 3. [ウイルス対策ルール、フィッシング対策ルール、または Web レピュテーションルール] に違反していないすべてのスパムメールおよびメールメッセージを EUQ データベースに同期させます (この領域でのみ)。これにより、エンドユーザが、エンドユーザメール隔離コンソールからメールの表示と管理を行うことができます。] チェックボックスをオンにします。 このオプションを有効にすると、この領域内の不正でないメッセージ (ウイルス対策ルール、フィッシング対策条件、または Web レピュテーションを起動しないメッセージ) がすべてエンドユーザメール隔離データベースに同期されます。これにより、エンドユーザが、エンドユーザメール隔離管理コンソールからメッセージの表示と管理を行うことができます。エンドユーザは不正なメッセージにアクセスすることはできません。
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。

表 8-1. 問題のトラブルシューティング

問題	推奨される解決策
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: <code>/opt/trend/ipprofiler/config</code>)。 2. <code>foxproxy.ini</code> を開きます。 3. <code>log_level</code> 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。 <code>/opt/trend/ipprofiler/script/foxproxyd restart</code> 5. ログファイルを開くには、次のように入力します。 <code>/opt/trend/ipprofiler/logs/foxproxy-general.****</code>
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します。 1. 次のコマンドを入力します。 <code>ps -ef grep named</code> 2. サービスが稼働していない場合は、起動します。
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. <code>foxproxy.ini</code> を開きます。 2. <code>report_send_interval</code> の値を変更します。 3. FoxProxy を再起動するには、次のように入力します。 <code>/opt/trend/ipprofiler/script/foxproxyd restart</code>

表 8-1. 問題のトラブルシューティング

問題	推奨される解決策
FoxDNS が機能しない	BIND サービスが稼働していることを確認します。 - 次のコマンドを入力します。 <code>ps -ef grep named</code> - 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。 <code>foxmsg.****</code> <code>foxnullmsg.****</code> <code>foxreport.****</code> 次の手順で、ログファイルが存在することを確認します。 - 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: <code>/opt/trend/imss/log/</code>)。 - 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。 <code>ps -ef grep imssmgr</code> - 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。 <code>ps -ef grep foxproxy</code> - 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「<code>t_foxhuntersetting</code>」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。 <code>record: 'Type' = 1 および 'enable' = TRUE</code>
管理コンソールから ERS を有効にした後で、ERS が機能しない	ERS 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。ERS 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 ERS 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。

表 8-1. 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] 画面の設定は、各検索サービスの Postfix に自動的に適用されません。 設定をすべての検索サービスに適用するには 1. [管理] → [InterScan MSS の設定] → [SMTP ルーティング] の順にクリックします。[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. [保存] をクリックします。 数分後に、各検索サービス上の InterScan MSS マネージャプロセスによって設定が Postfix に同期されます。InterScan MSS マネージャを直ちに再起動するには、次のコマンドを使用します。 /opt/trend/imss/script/S99MANAGER restart InterScan MSS マネージャプロセスによって同期されない場合は、ローカルの設定ファイル /opt/trend/imss/config/imss.ini で、enable_postset_thd キーが「yes」に設定されているか空白になっていることを確認します。
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 分待ってから、リストを再度確認してください。
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。

InterScan MSS ポート

表 8-2. InterScan MSS ポート

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
ポリシーサーバ	5060	SOAP 待機ポート
検索サービス	110	POP3 待機ポート

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には、[すべての検索サービスに適用] オプションを有効にします。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には、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します。以下に例を示します。

```
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。

データベースのテーブル `tb_postfixconfig` で、`fieldname` 列の下にパラメータ名を見つけることができます。

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 -d imss -U sa > YYYYMMDD.HHMMSS.backup` — データベースをバックアップします。
- `psql -U sa -d imss < ./YYYYMMDD.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、このコマンドを使用します。
- `vacuumfull` — データベースの使用頻度が低い、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。

LDAP が起動していない場合、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 サーバが起動していなくても機能します。
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。
- InterScan MSS では、各ルールのクエリを約 1 分実行します。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。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か、LDAP サーバのポートにアクセスできない場合。

Email Reputation Services

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、ERS 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 ERS 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。

注意： ドメインを DNS サービスで解決できない場合、そのドメインは承認済みリストでは機能しません。

ERS のアクティベーションコードを指定するには、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指定するか、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、ERS 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。

ERS 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 Email Reputation Service. See [http://www.mail-abuse.com/cgi-bin/lookup?ip_address=\\$rbl_what\\${rbl_reason?;\\$rbl_reason}](http://www.mail-abuse.com/cgi-bin/lookup?ip_address=rbl_what{rbl_reason?;$rbl_reason})
APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.r.mail-abuse.com 550 Service unavailable; \$rbl_class [\$rbl_what] blocked using Trend Micro RBL+. See [http://www.mail-abuse.com/cgi-bin/lookup?ip_address=\\$rbl_what\\${rbl_reason?;\\$rbl_reason}](http://www.mail-abuse.com/cgi-bin/lookup?ip_address=rbl_what{rbl_reason?;$rbl_reason})
- imss_rbl_reply.user
APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.q.mail-abuse.com 450 error message; \$rbl_class [\$rbl_what] blocked using Trend Micro Email Reputation Service. See [http://www.mail-abuse.com/cgi-bin/lookup?ip_address=\\$rbl_what\\${rbl_reason?;\\$rbl_reason}](http://www.mail-abuse.com/cgi-bin/lookup?ip_address=rbl_what{rbl_reason?;$rbl_reason})
"APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.r.mail-abuse.com 450 error message; \$rbl_class [\$rbl_what] blocked using Trend Micro RBL+. See [http://www.mail-abuse.com/cgi-bin/lookup?ip_address=\\$rbl_what\\${rbl_reason?;\\$rbl_reason}](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 のステータスを監視するのはどのプロセスですか。FoxProxy の機能が停止したとき、復旧するのはどのプロセスですか。

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 クエリを実行するのはどのプロセス / コンポーネントですか。

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、ユーザは DNS サーバをセントラルコントローラにインストールすることを選択できます。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、コンピュータ上にすでに 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。

InterScan MSS 7.1 がメールを「Foxhunter_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 7.1 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 つにすぎません。

隔離とアーカイブ

クエリの実行に特殊文字を使用できますか。

はい、クエリの実行には次の特殊文字を使用できます。

- アスタリスク (*) — 0 個以上の文字の検索にワイルドカード文字として使用します。メールアドレスまたはファイル名の検索にアスタリスク (*) を使用できます。

メールアドレスを検索する場合、次の例を参照してください。

* — すべてのメールアドレスを表します。

@domain.tld、name@.tld — 前者は特定のドメイン名とトップレベルドメイン (TLD) を持つすべてのメールアドレスを表し、後者は特定のユーザ名と TLD を持つすべてのメールアドレスを表します。

@.tld — 特定の TLD を持つすべてのメールアドレスを表します。

ファイル名を検索する場合、次の例を参照してください。

. — すべてのファイルを表します。

*.extension — 特定の拡張子のすべてのファイルを表します。

name.* — 特定の名前を持つすべての拡張子のファイルを表します。

- セミコロン (;) — 複数の受信者または添付ファイルの検索時に区切り文字として使用します。

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メッセージを再処理します。したがって、通知メールメッセージがポリシー違反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メッセージにはメッセージ ID がありません。

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。

Microsoft 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 Microsoft Exchange Server を Active Directory と共にインストールしている場合、次の操作を実行できます。

- 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。
- すべての InterScan MSS サービスを再起動します。

英語以外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。

次の手順を実行してください。

- 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英語以外の言語で入力します。
- [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。文字コードとして英語以外の言語を選択します。

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ポート 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

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 またはホスト名を指定できます。

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

- \$IMSS_Home/imss/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、サービスを個別に停止します。

InterScan MSS のスクリプトの詳細については、244 ページの「InterScan MSS スクリプトの使用」を参照してください。

- サーバの IP アドレスを変更します。

- c. このサーバにデータベースサービスがインストールされている場合は、データベースサービスを開始します。InterScan MSS によってデータベースがインストールされている場合は、次のコマンドを使用します。
- ```
$IMSS_Home/imss/script/dbctl.sh start
```
- d. `odbc.ini` ファイルおよび `euqodbc.ini` ファイルの IP アドレスを変更します。これらのファイルは、InterScan MSS 設定フォルダ (`$IMSS_Home/imss/config/`) にあります。
- e. `%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。
- f. 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。
- g. 次のコマンドを使用して、すべての InterScan MSS サービスを起動します。
- ```
$IMSS_Home/imss/script/imssstart.sh
```

InterScan MSS では分割メールメッセージをどのように処理するのですか。

`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` に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。
 - 既存のルールをクリックして、ルールを編集します。
 - [編集] 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пам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。
 - 既存のルールリンクをクリックして、ルールを編集します。
 - [編集] 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。カスタム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、なぜ直ちに適用されないのですか。

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。

ヒント： 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пам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せん。

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
```

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 7.1 で InterScan MSS のリレーの制約を設定できますか。

いいえ。InterScan MSS 7.1 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 Linux 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メッセージが常に添付ファイルとして受信されるのはなぜですか。メールの本文がディスクレーマーまたはスタンプに置き換えられるのはなぜですか。

スタンプの文字コードがメールメッセージのコンテンツの文字コードと異なる場合、InterScan MSS では、メッセージを検索した後にスタンプをメッセージ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、メッセージ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メッセージが作成されます。メッセージ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、「差出人」、「宛先」、または「件名」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「差出人」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. [編集] 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。

暗号化メッセージにメッセージサイズの検索条件を使用できないのはなぜですか。

InterScan MSS では、暗号化メッセージを特殊な種類のメッセージとして処理します。ほとんどの検索条件は適用されません。InterScan MSS では、暗号化メッセージを検索したり暗号化メッセージに対して処理を実行するために、暗号化メッセージの検索条件を使用する必要があります。

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。

製品 Q&A

<http://esupport.trendmicro.co.jp/corporate/search.aspx>

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。

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、フランス、メキシコ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 1000 名以上のスタッフが、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 7.1 (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。

- 244 ページの「InterScan MSS スクリプトの使用」

InterScan MSS スクリプトの使用

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。

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。

表 A-1. InterScan MSS スクリプト

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
regipro.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] 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。
S99CLEANEXPIRE		管理コンソールの [隔離およびアーカイブ] → [設定] 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

表 A-1. InterScan MSS スクリプト

スクリプト	パラメータ	説明
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 / restart	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。
S99SCHEDULED	start / stop	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	すべてまたは承認済み送信者	エンドユーザメール隔離データベースのデータまたは承認済み送信者を転送します。
imssstart.sh		すべての InterScan MSS のサービスを開始します。
S99WRSAGENT	start / stop / restart	WRS エージェントサービス

表 A-1. InterScan MSS スクリプト

スクリプト	パラメータ	説明
db_maintain.sh	{vacuum reindex analyze all } [vacuum] - 管理データベースおよびすべてのエンドユーザメール隔離データベースをクリーンナップします。 [reindex] - 管理データベースおよびすべてのエンドユーザメール隔離データベースを再インデックス化します。 [analyze] - 管理データベースおよびすべてのエンドユーザメール隔離データベースを分析します。 [all] - クリーンナップ、再インデックス化、分析。	データベースを管理するために 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。

初期設定ディレクトリ

この付録では、Trend Micro InterScan Messaging Security Suite 7.1（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。

- 248 ページの「初期設定のメールキュー」
- 249 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」
- 249 ページの「一時フォルダ」
- 249 ページの「通知受け取りフォルダ」

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。

表 B-1. 初期設定の InterScan MSS メールの場合

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=	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。
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。

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。

通知受け取りフォルダ

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

1 回限りのレポート

管理 159

追加 160

AJP 227

APOP 66

Control Manager

エージェントの有効化 148

設定の複製 149

Control Manager サーバの設定

設定 25

Control Manager の設定

設定 210

ERS

MTA 設定 37

アクティベーションコード 36

管理コンソール 37

使用 36

設定 50

有効化 41

InterScan MSS

サービス 32

サービスの起動 / 停止 33

スクリプト 244

バックアップ 145

復元 146

IP フィルタ

ウイルスの設定 44

スパムメールの設定 43

設定 41

ディレクトリハーベスト攻撃 (DHA) の設定 46

バウンスメールの設定 48

IP フィルタサービス

概要 36

IP プロファイラ

有効化 41

ルールの有効化 42

LDAP

設定と有効化 192

LDAP 設定

設定 22、206

LDAP ユーザまたはグループ

検索 95

MIME コンテンツタイプ

検索条件 114

MTA

ERS での使用 37

POP3 検索

有効化 65

POP3 設定

設定 66、208

POP3 待機ポート 227

POP3 メッセージ

検索 64

Readme ファイル 12

SMTP の設定

設定 55

SMTP メッセージ

検索 53

SMTP ルーティング 55

設定 54

SOAP サーバ 227

SSL

使用 17

証明書の作成 17

TrendLabs 241

対象読者 12

あ

アーカイブされたメッセージ

表示 181

アクティベート

製品 214

ライセンス 213

アスタリスクワイルドカード

使用 137

アップデート

検索エンジン 28

自動 31

手動 29

パターンファイル 28

アップデート元

指定 28

設定 21

アドレスグループ

削除 79

追加 76

編集 79

理解 74

例 74

イベント条件

設定 188

イベント通知 185

インストール

SSL の使用 17

インポートに関する注意 144

ウィザード 19

ウイルス対策ルール 105

ウイルスの設定

設定 44

疑わしい IP アドレス

表示 52

エクスポートに関する注意 144

エンドユーザメール隔離 192

開始 196

管理コンソール 34、199

管理コンソールを開く 199

無効化 200

有効化 195

エンドユーザメール隔離通知

設定 189

オンラインヘルプ 12

アクセス 17

か

開始

エンドユーザメール隔離 196

隔離されたメッセージ

表示 180

隔離とアーカイブ 173

設定 173

隔離領域

管理 174

管理

1 回限りのレポート 159

管理者アカウント 202

キーワードリスト 81

製品ライセンス 211

通知リスト 85

ポリシー 70

管理コンソール 16

管理コンソールのパスワード

変更 27

管理者アカウント

管理 202

削除 204

追加 202

編集 204

キーワード

設定 82

キーワードリスト

管理 81

基本設定 19

許可された送信者 61

クエリ

MTA イベントログ 171

アーカイブ領域 178

隔離領域 177

システムイベントログ 169

ポリシーイベントログ 170

メッセージ 177

メッセージ追跡ログ 168

クエリ、ログ 167

検索

POP3 メッセージ 64

SMTP メッセージ 53

検索エンジン

アップデート 28

検索条件 115

MIME コンテントタイプ 114

拡張子 114

実ファイルタイプ 115

指定 104

スパムメール 109

添付ファイル 113

添付ファイルサイズ 115

添付ファイル数 115

添付ファイル名 114

メッセージサイズ 116

検索除外

設定 138

検出時の処理

暗号化メッセージの設定 140

他の検索除外の設定 141

件名タグ

追加 126

更新 213

ライセンス 213

コマンド 244

さ

サービス

IP フィルタサービス 36

削除

アドレスグループ 79

管理者アカウント 204

作成

レポート 158

実ファイルタイプ 115

指定

アップデート元 28

検索条件 104

処理 118

特殊処理 125

ルート 97

手動アップデート 29

承認済み送信者リスト

設定 110

承認済みリスト

IP アドレスの追加 51

スパムメール除外テキストルール

設定 111

スパムメール対策

アクティベーションコード 36

スパムメールの設定

設定 43

製品ライセンス

管理 211

表示 212

セキュリティ設定違反

検出時の処理の設定 140

除外設定 139

接続設定

設定 56、205

設定 103

Control Manager サーバの設定 25

Control Manager の設定 210

ERS 50

IP フィルタ 41

IP フィルタ、ウイルスの設定 44

IP フィルタ、スパムメールの設定 43

IP フィルタ、バウンスメールの設定 48

LDAP 設定 22、206

POP3 設定 66、208

SMTP の設定 55

SMTP ルーティング 54

アップデート元 21

暗号化メッセージの検出時の処理 140

エンドユーザメール隔離通知の設定 189

隔離とアーカイブの設定 173

キーワード 82

検索除外 138

承認済み送信者リスト 110

スパムメール除外テキストルール 111

セキュリティ設定違反検出時の処理 140

セキュリティ設定違反の除外 139

接続設定 56、205

通知設定 20、186

通知メッセージ 188

ディレクトリハーベスト攻撃 (DHA) の設定 46

ドメインベース配信の設定 62

内部アドレス 24、92

ブロックする送信者リスト 110

メッセージルールの設定 58

ユーザ隔離アクセス 181

予約レポート 163
ルート 101
ログの設定 165
設定、イベント条件 188
設定ウィザード 19
アクセス 19
その他のルール 107

た

他の検索除外の検出時の処理の設定 141
注意
インポート 144
エクスポート 144
追加
1 回限りのレポート 160
管理者アカウント 202
通知
イベント 185
通知設定
設定 20、186
通知メッセージ
設定 188
通知リスト
管理 85
ディレクトリハーベスト攻撃 (DHA) の設定
設定 46
テクニカルサポート 239
添付ファイルサイズ
検索条件 115
ドキュメント
InterScan MSS 関連 12

特殊処理
指定 125
ドメイン
表示 52
ドメインベースの配信 62
ドメインベース配信の設定
設定 62
トラブルシューティング 218
imssps デーモン 218
IP フィルタ 224
エンドユーザメール隔離管理コンソールへの
アクセス 222
エンドユーザメール隔離通知 223
エンドユーザメール隔離の隔離されたメッ
セージ 223
製品の起動 219
メール通知 219
トランスポート層 57

な

内部アドレス
設定 24、92

は

バウンスメールの設定
設定 48
パスワード
InterScan MSS 管理コンソール初期設定 16
管理コンソール 27
パターンファイル
アップデート 28

バックアップ

InterScan MSS 145

表示

アーカイブされたメッセージ 181

疑わしい IP アドレス 52

隔離されたメッセージ 180

製品ライセンス 212

ドメイン 52

フィルタ

例 74

復元

InterScan MSS 146

複製、設定 147

ブロックする送信者リスト

設定 110

ブロックリスト

IP アドレスの追加 52

変更

管理コンソールのパスワード 27

編集

アドレスグループ 79

管理者アカウント 204

ポリシー

完成 127

管理 70

追加 96

例 1 131

例 2 134

ポリシー通知

追加 86

編集 86

ま

メールリレー 58

メッセージサイズ

検索条件 116

メッセージルールの設定

設定 58

や

ユーザ隔離アクセス

設定 181

有効化 196

ユーザ名

InterScan MSS 管理コンソール初期設定 16

有効化

Control Manager エージェント 148

ERS 41

IP プロファイラ 41

IP プロファイラのルール 42

POP3 検索 65

エンドユーザメール隔離 195

ユーザ隔離アクセス 196

よくある質問

InterScan MSS コンポーネント 228

IP プロファイラ 230

Postfix 227

エンドユーザメール隔離 233

予約アップデート 31

予約レポート

使用 162

設定 163

ら

ライセンス 213

 アクティベート 213

ルート

 指定 97

 除外設定 103

 設定 101

ルートの除外 103

レポート

 1 回限りの追加 160

 1 回限りのレポートの管理 159

 作成 158

 内容 158

ロールバック

 コンポーネント 30

ログ 165

 MTA イベントのクエリ 171

 クエリ 167

 システムイベントのクエリ 169

 設定 165

 ポリシーイベントのクエリ 170

 メッセージ追跡のクエリ 168

