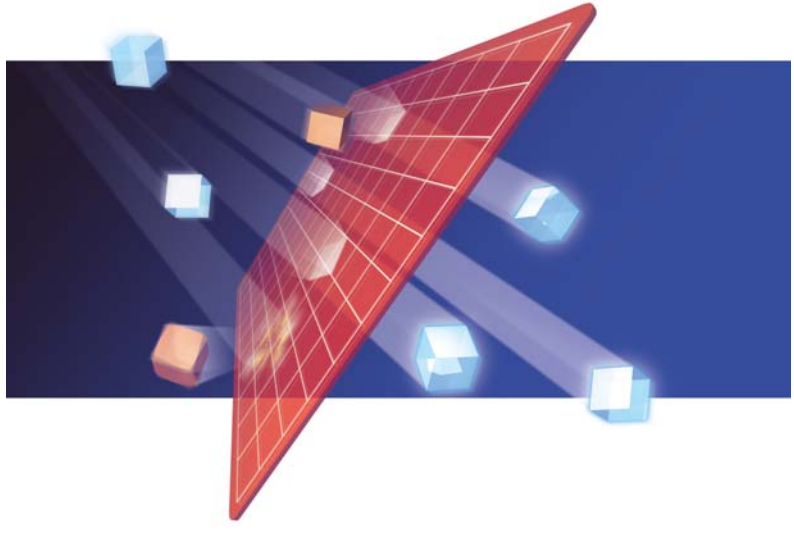
Trend Micro InterScan VirusWall™
スタンダードエディション



クイックスタートガイド

TREND MICRO™

P/N: ISSEUX-AE0102 (2007/08)

目次

InterScan VirusWall の概要 7
このガイドについて 7
製品ドキュメント 7
新機能 9

第 1 章　配置 11
インストールのトポロジ 12
SMTP VirusWall を配置する 13
POP3 VirusWall を配置する 17
POP3 (ポートマッピング) 18
FTP VirusWall を配置する 20
FTP スタンドアロンモードの配置 21
FTP ポートマッピングモードの配置 23
HTTP VirusWall を配置する 25
HTTP VirusWall スタンドアロンモード 25
HTTP VirusWall 依存モード 26
HTTP リバースプロキシモード 28

第 2 章　インストール 31
概要 32
インストール前のチェックリスト 33
システム要件 34
InterScan VirusWall をインストールする 37
新規インストールを実行する 38
InterScan VirusWall をアクティベートする 42

管理者パスワードを設定する 44
事前設定 45
通知設定 48
インストールを開始する 49
インストール後のタスク 51
インストール後のチェックリスト 51

第 3 章 以前のリリースからの移行 57

移行パス 58
2 つの移行方法 58
同じコンピュータ上でバージョン 3.8x からアップグレードする 58
バージョン 3.8x 用の移行ツールを使用する 60
異なるコンピュータ上でバージョン 3.8x からアップグレードする 61
異なるコンピュータ上でバージョン 5.0 からアップグレードする 66

第 4 章 基本的な操作 73

InterScan VirusWall Web コンソール 74
Web コンソールへアクセスする 75
Web コンソールをナビゲートする 76
[概要] 画面 77
[SMTP] メニュー 79
[HTTP] メニュー 83
[FTP] メニュー 87
[POP3] メニュー 89
[大規模感染予防] メニュー 92
[管理] メニュー 93
InterScan VirusWall を起動 / 停止する 95

InterScan VirusWall をテストする 96
EICAR テストウイルスを使用したウイルス対策のテスト 96
コンテンツフィルタをテストする 98
リアルタイムパフォーマンスモニタを使用する 100
InterScan VirusWall コンポーネントをアップデートする 102
アップデートのサブメニュー 103
アップデートできるコンポーネント 103
差分アップデートと全体アップデート 105
コンポーネントを手動でアップデートする 106
手動アップデート機能を使用する 106
[概要] 画面を使用してコンポーネントを表示およびアップデートする 107
アップデートを予約する 109
アップデートを使用するために InterScan VirusWall を設定する 110
通知設定 111
パスワードの管理 112

第 5 章　トラブルシューティングとサポート 115

概要 116
トラブルシューティング 117
インストールと移行 117
ライセンスとアクティベーション 122
ユーザインタフェース 123
よくある質問 125
インストール 125
隔離 126
隔離アイテムに対してクエリを実行する 128
SMTP および POP3 の隔離に対して利用可能なクエリ条件 128

隔離アイテムを移動または削除する 130
隔離アイテムを再送信、または検索して再送信する 131
隔離ディレクトリパスを変更する 132
古い隔離アイテムを削除する 132
ログを用いたセキュリティインシデントの分析 134
ログクエリを実行する 136
クエリ結果テーブル 138
クエリ結果をエクスポートする 139
ログを削除する 140
その他のログ 141
製品サポート情報 143
サポートサービスについて 143
製品 Q&A のご案内 144
セキュリティ情報 145
セキュリティ情報の入手先 145
トレンドマイクロへのウイルス解析依頼 146
ウイルス解析サポートセンター「TrendLabs」..... 146

付録 A　用語集 147

InterScan VirusWall の概要

Trend Micro InterScan VirusWall スタンダードエディション (以下、InterScan VirusWall)の「クイックスタートガイド」へようこそ。このドキュメントでは、InterScan VirusWall のセットアップ、および基本的な設定と管理に必要な情報をシステム管理者に提供します。

このガイドについて

「Trend Micro InterScan VirusWall スタンダードエディション クイックスタートガイド」は、以下の章で構成されています。

- 第 1 章「配置」では、インストールのトポロジ、SMTP、POP3、FTP、HTTP の各トラフィックへの InterScan VirusWall の配置について説明します。
- 第 2 章「インストール」では、インストール計画、システム要件、インストール手順、およびインストール後のタスクについて説明します。
- 第 3 章「以前のリリースからの移行」では、InterScan VirusWall for UNIX 3.8x から InterScan VirusWall への移行手順を、構成設定の移行方法も含めて説明します。
- 第 4 章「基本的な操作」では、Web コンソールとそのメニューオプションのほか、InterScan VirusWall サービスの開始 / 停止や InterScan VirusWall の主要機能のテストなどの基本タスクについて説明します。
- 第 5 章「トラブルシューティングとサポート」では、すみやかにタスクを開始するためのソリューションとテクニカルサポートを受ける方法について説明します。

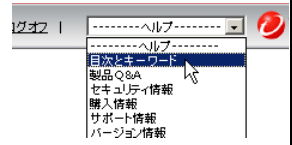
製品ドキュメント

この「クイックスタートガイド」の他に、以下のドキュメントにアクセスして InterScan VirusWall の関連情報を得ることができます。

表 1. InterScan VirusWall のドキュメント一覧

ドキュメント	内容	アクセス先
Readme ファイル	システム要件、他のドキュメント、および機能のリストには記載されていない最新情報	・インストールフォルダ (インストール後に Readme ファイルを表示できます) ・以下のトレンドマイクロのダウンロードサイト : http://www.trendmicro.co.jp/download/
Trend Micro InterScan VirusWall スタンダードエディション SMTP 設定ガイド	ウイルス検索、フィッシング対策、スパムメール対策、スパイウェア / グレーウェア対策、コンテンツフィルタ、および IntelliTrap を使用して SMTP トラフィックを保護するように、この製品を設定するためのガイド	・製品 CD-ROM ・以下のトレンドマイクロのダウンロードサイト : http://www.trendmicro.co.jp/download/
Trend Micro InterScan VirusWall スタンダードエディション HTTP 設定ガイド	ウイルス検索、フィッシング対策、スパムメール対策、スパイウェア / グレーウェア対策、URL ブロック、および URL フィルタを使用して HTTP トラフィックを保護するように、この製品を設定するためのガイド	
Trend Micro InterScan VirusWall スタンダードエディション FTP/POP3 設定ガイド	ウイルス検索、スパイウェア / グレーウェア対策を使用して FTP トラフィックを保護し、ウイルス検索、フィッシング対策、スパムメール対策、スパイウェア / グレーウェア対策、コンテンツフィルタ、および IntelliTrap を使用して POP3 メールトラフィックを保護するように、この製品を設定するためのガイド	
Trend Micro InterScan VirusWall スタンダードエディション リファレンス マニュアル	システムチェックリスト、移行テーブル、初期設定値、大規模感染予防サービスに関する情報	

表 1. **InterScan VirusWall のドキュメント一覧 (続き)**

オンラインヘルプ	製品の機能、タスク、Q&A、一般的な問題のトラブルシューティングに関する情報 ユーザインタフェースの各ページにおける状況依存の情報と各画面の目的に関する情報 	Web コンソール :  メインのオンラインヘルプにアクセスするには [ヘルプ] ドロップダウンメニューで [目次とキーワード] をクリックします。

新機能

InterScan VirusWall は最新のセキュリティの脅威からネットワークを保護する新機能を備えています。今回のリリースで追加された機能には、スパムメール対策、スパイウェア / グレーウェアの対策、BOT の脅威やフィッシングの対策、コンテンツフィルタ機能、ファイルタイプに応じた HTTP および FTP のファイルブロック、HTTP および FTP 検索用のメール通知、Web コンソールを介した送信メールディスクレーマの指定機能、大規模感染予防サービス (OPS) による保護などがあります。

表 2. **InterScan VirusWall の新機能**

新機能	説明
HTTP 遅延検索	サイズの大きいファイルを検索中、クライアント / サーバの接続が切断しないようにします。
SMTP/POP3 ファイル全体検索	特殊な種類のメールウイルスを識別するために、すべてのメールを検索します。
SMTP、HTTP、FTP および POP3 トランザクションログ	送信元 IP アドレス、送信者および受信者メールアドレス、接続時間、InterScan VirusWall が実行したメールに対する処理、関連エラーメッセージなど、SMTP、HTTP、FTP および POP3 プロトコル接続情報のログが可能
隔離メールの「再送信」と「検索および再送信」	管理者が、隔離メールを再送信、または検索してから再送信できるようにします。

表 2. **InterScan VirusWall の新機能 (続き)**

新機能	説明
Network Reputation Services (NRS)	スパムメール検出の精度を向上
URL フィルタエンジンおよびゲートウェイのスパイウェアを検索するスパイウェア監視パターンファイル	スパムメール検出の精度を向上
Trend Micro Control Manager (以下、Control Manager) との統合	Control Manager サーバ管理コンソールから InterScan VirusWall を管理可能
Trend Micro InterScan VirusWall for Small and Medium Businesses 5.0 からの移行	大部分の設定を維持しながら、バージョン 5.0 から 6.02 へ簡単にアップグレード
パターンファイルおよびエンジンのアップデート通知設定	パターンファイルやエンジンなどのコンポーネントをアップデートする際に、管理者に対するアップデート通知メールの送信を有効または無効に設定可能
ログ / 隔離メンテナンスの通知	InterScan VirusWall のログまたは隔離フォルダのいずれかが設定された容量を超えると管理者に通知

第 1 章

配置

この章では、以下のトピックについて説明します。

- 12 ページの「インストールのトポロジ」
- 13 ページの「SMTP VirusWall を配置する」
- 17 ページの「POP3 VirusWall を配置する」
- 20 ページの「FTP VirusWall を配置する」
- 25 ページの「HTTP VirusWall を配置する」

インストールのトポロジ

トレンドマイクロは、適切に設定されたファイアウォールの直後、またはネットワークアドレス変換 (NAT) とファイアウォールタイプと同等の他の保護を提供するセキュリティデバイスの直後に InterScan VirusWall をインストールすることをお勧めします。

目的に応じて InterScan VirusWall を設定することにより、多様なトポロジに対応できます。このトポロジは、1 つのサーバに InterScan VirusWall をインストールして全サービスをそのサーバ上で有効にする統合配置から、各種類のサーバ (HTTP、FTP、SMTP、および POP3) で InterScan VirusWall の 1 つのインスタンスをインストールして各サーバ上の関連するサービスだけを有効にする、完全に分散されたサーバ固有の配置まで多岐にわたります。

表 1-1. 可能な InterScan VirusWall トポロジの配置

単一の統合配置	InterScan VirusWall を 1 つのサーバにインストールし、そのサーバ上で SMTP VirusWall、POP3 VirusWall、FTP VirusWall、および HTTP VirusWall を有効化します。
メッセージング /Web 配置	InterScan VirusWall を 1 つのサーバにインストールし、そのサーバ上で SMTP VirusWall と POP3 VirusWall を有効化します。
	InterScan VirusWall を 1 つのサーバにインストールし、そのサーバ上で FTP VirusWall と HTTP VirusWall を有効化します。
スタンドアロン配置	InterScan VirusWall を 4 つの異なるサーバにインストールし、各サーバで 1 つのサービスだけを有効化します。

以降の図は、InterScan VirusWall のインストール前後における標準的なネットワーク設定を示しています。

SMTP VirusWall を配置する

InterScan VirusWall の SMTP フィルタサービス (SMTP VirusWall) では、受信 SMTP トラフィックと送信 SMTP トラフィックの両方をチェックしてウイルスを調べます。SMTP VirusWall は、既存の SMTP サーバと同じコンピュータにインストールするか、専用のコンピュータにインストールすることができます。

- SMTP サーバが別のコンピュータにある場合は、InterScan VirusWall のホスト名 (または IP アドレス) とポート番号を指定します (図 1-4「トポロジ A: 受信メールパスと送信メールパス (InterScan VirusWall と SMTP サーバを異なるコンピュータにインストール)」(16 ページ) を参照)。
- SMTP サーバが同じコンピュータにある場合は、受信 SMTP 接続の待機に使用するポート番号を変更し、InterScan VirusWall に対してこのポート番号とホスト名を指定します (図 1-6「トポロジ B: InterScan VirusWall インストール後 (SMTP VirusWall とメールサーバを同じコンピュータにインストール)」(17 ページ) を参照)。
- SMTP サーバが Sendmail であり、InterScan VirusWall と同じコンピュータにある場合は、Sendmail パスを特定して、-bs フラグを追加する必要があります。ポート設定は必要ありません (図 1-5「Web コンソールの [SMTP 設定] 画面」(16 ページ) を参照)。

新規にインストールした、待機ポート 25 の InterScan VirusWall サーバにファイアウォールの SMTP サービス (ポート 25) を再度割り当てます。次に、コマンドモード (シングルサーバ環境) または受信メール転送 (マルチサーバ環境) を使用して、検索済みのメールを 1 つ以上の内部メールサーバに転送します。

図 1-2「トポロジ A: InterScan VirusWall インストール後の受信メールパス (SMTP VirusWall と SMTP サーバを異なるコンピュータにインストール)」(14 ページ) と図 1-3「トポロジ A: InterScan VirusWall インストール後の送信メールパス (SMTP VirusWall と SMTP サーバを異なるコンピュータにインストール)」(15 ページ) で示されるトポロジの提案を使用するには、内部メールサーバの IP アドレスを変更する必要があります。クライアントの送信メール設定では、それぞれの送信メールサーバへの接続が継続されるため、変更は必要ありません。

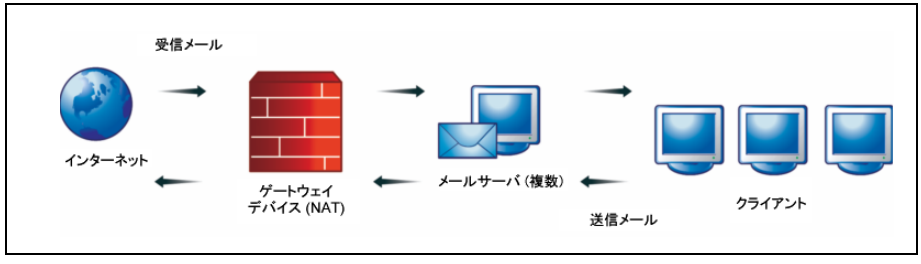


図 1-1.　トポロジ A: InterScan VirusWall をインストールする前の受信メールパス

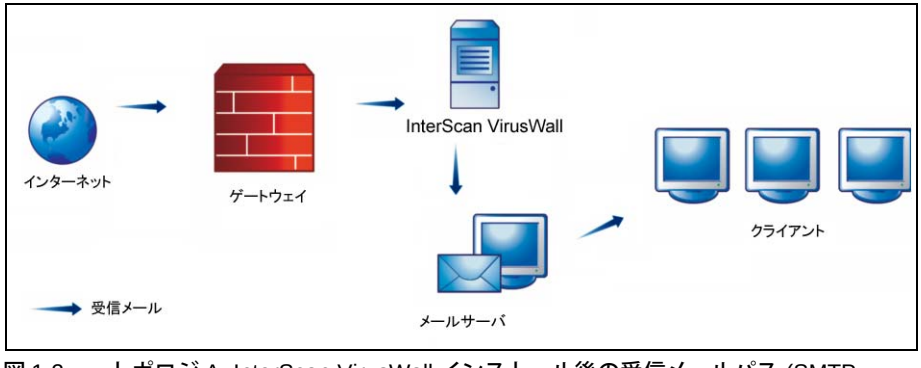


図 1-2.　トポロジ A: InterScan VirusWall インストール後の受信メールパス (SMTP VirusWall と SMTP サーバを異なるコンピュータにインストール)

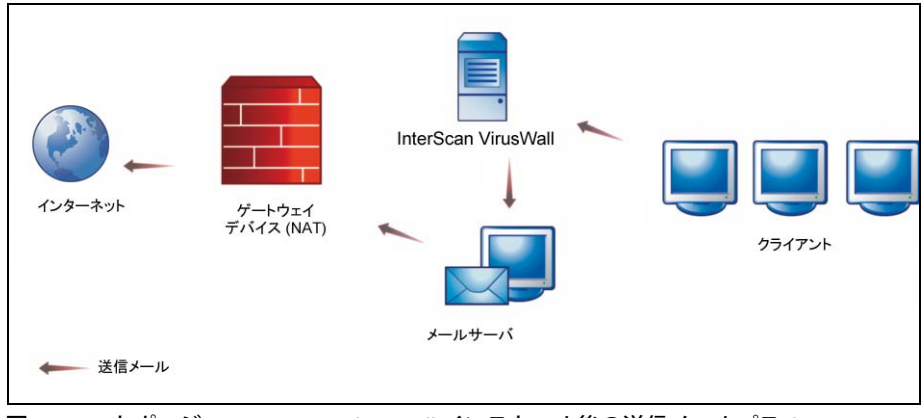


図 1-3.　トポロジ A: InterScan VirusWall インストール後の送信メールパス (SMTP VirusWall と SMTP サーバを異なるコンピュータにインストール)

InterScan VirusWall と SMTP サーバが同じコンピュータにインストールされていない場合は、図 1-4「トポロジ A: 受信メールパスと送信メールパス (InterScan VirusWall と SMTP サーバを異なるコンピュータにインストール)」(16 ページ) に示すように、元の SMTP サーバを InterScan VirusWall と置換し、メールを InterScan VirusWall から元の SMTP サーバに転送することができます。

このような配置の場合、受信メールは最初に InterScan VirusWall に配信され、InterScan VirusWall は受信メールを検索してから元の SMTP サーバに転送します。送信メールも最初に InterScan VirusWall に配信され、InterScan VirusWall は送信メールを検索してから元の SMTP サーバに転送されます。SMTP サーバはそのメールをインターネットに送信します。

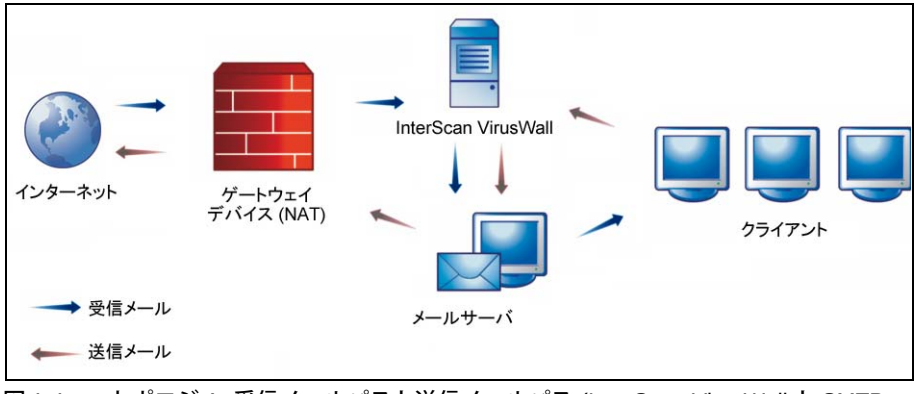


図 1-4.　トポロジ A: 受信メールパスと送信メールパス (InterScan VirusWall と SMTP サーバを異なるコンピュータにインストール)

SMTP サーバが Sendmail であり、InterScan VirusWall と同じコンピュータにある場合は、Sendmail パスを特定して、-bs フラグを追加します。ポート設定は必要ありません (図 1-5「Web コンソールの [SMTP 設定] 画面」(16 ページ) を参照)。

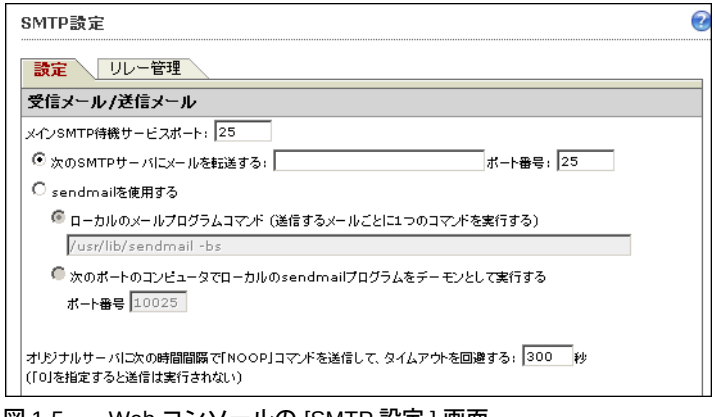


図 1-5.　Web コンソールの [SMTP 設定] 画面

[SMTP 設定] 画面で [次のポートのコンピュータでローカルの sendmail プログラムをデーモンとして実行する] を選択する前に、そのコンピュータの Sendmail または他の SMTP メールデーモンを正しく設定する必要があります。

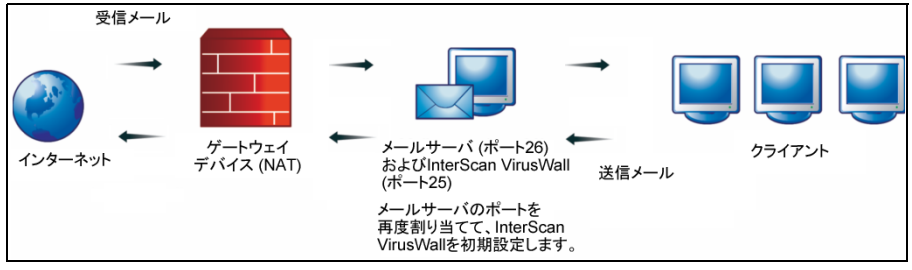


図 1-6. トポロジ B: InterScan VirusWall インストール後 (SMTP VirusWall とメールサーバを同じコンピュータにインストール)

POP3 VirusWall を配置する

標準的な POP3 トポロジでは、クライアントが InterScan VirusWall からメールを直接受信できるように、クライアントコンピュータの POP3 設定を変更する必要があります。クライアントのアカウント名を Mailbox_name から以下に変更します。

```
Mailbox_name#POP3_server[#Port_number]
```

たとえば、以下のように変更します。

```
joedoe#externalpop3.com[#110]
```

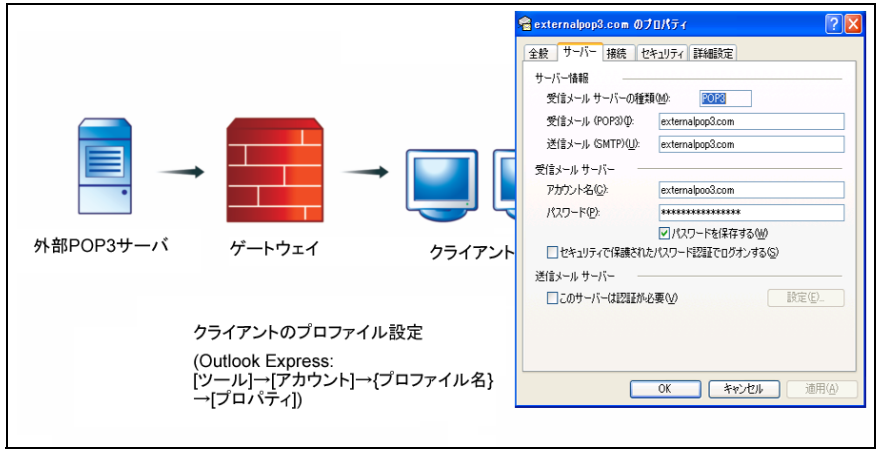


図 1-7.　InterScan VirusWall インストール前の POP3 トポロジと POP3 設定

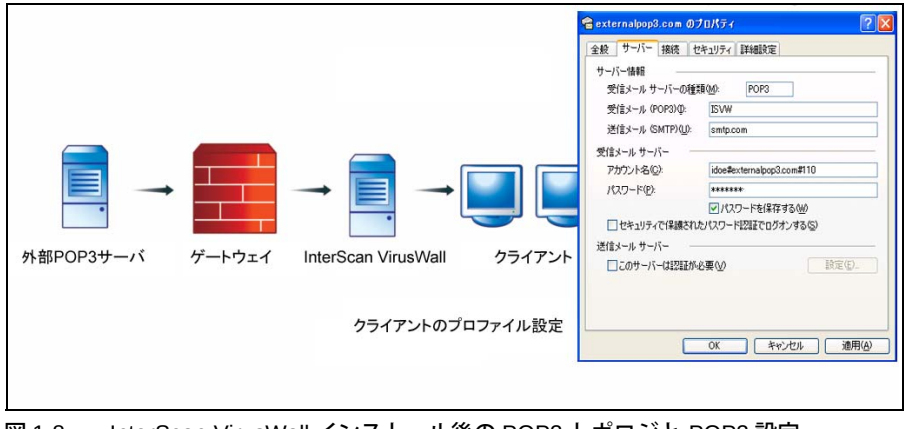


図 1-8.　InterScan VirusWall インストール後の POP3 トポロジと POP3 設定

POP3 (ポートマッピング)

InterScan VirusWall がポートマッピングサーバとして機能する場合は、InterScan VirusWall の待機ポートとその特定の POP3 サーバにポートがマップされます。このトポロジに必要な変更は、次のとおりです。

- Web コンソールで [POP3]→[設定] の順に選択し、InterScan VirusWall で使用するポートを受信 POP3 ポートとして指定します。
- クライアントコンピュータの POP3 設定で、InterScan VirusWall サーバの名前とポート番号を受信メールサーバの名前とポート番号として指定します。

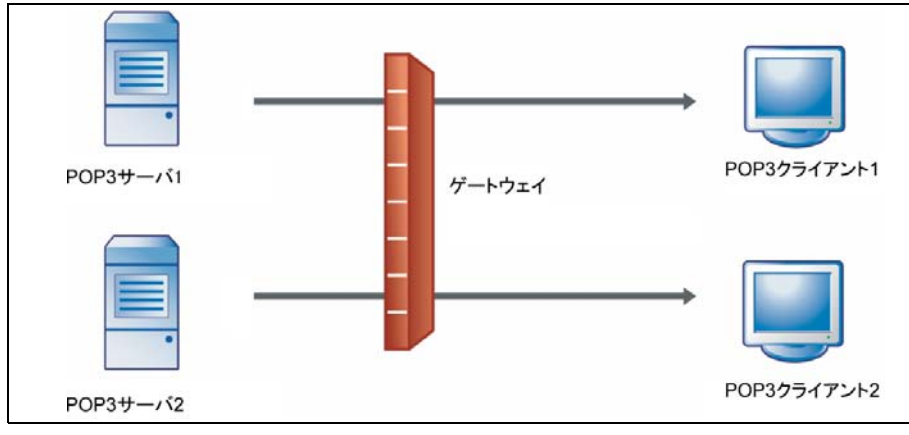


図 1-9.　InterScan VirusWall インストール前の POP3 トポロジ

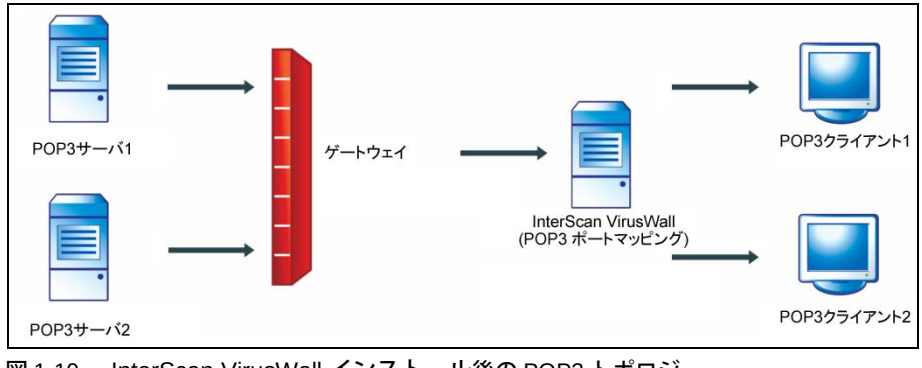


図 1-10.　InterScan VirusWall インストール後の POP3 トポロジ

FTP VirusWall を配置する

InterScan VirusWall の FTP 検索機能 (FTP VirusWall) を使用するには 2 つの方法があります。

1. スタンドアロンモード - 図 1-14「独立したプロキシサーバがあるスタンドアロンモードでの FTP 配置」(22 ページ) に示すように、FTP VirusWall は要求元のクライアントとリモートサイト間のプロキシサーバとして動作し、すべてのトランザクションを仲介します。
2. ポートマッピングモード - FTP VirusWall は、LAN 内の特定のサーバの前に配置された見張り役として動作します。

いずれの場合も、FTP VirusWall はすべての転送内容を調べて、ウイルス、不正な Java アプレット、不正な ActiveX コントロール、およびスパイウェア / グレーウェアがないかチェックします。FTP VirusWall は、既存の FTP サーバと同じコンピュータにインストールするか、専用のコンピュータにインストールすることができます。あるいは単独の FTP プロキシとしてインストールすることができます。

プロキシとして動作するようにインストールし設定した場合は (図 1-12)、FTP VirusWall は次のことを行います。

- LAN 内から発行されたすべての FTP 要求を受信します。
- その要求をリモート FTP サーバに渡します。
- リモート FTP サーバによって開かれたデータポートを使用して、データを受信します。
- ウイルスとスパイウェア / グレーウェアを検索します。
- クリーンなファイルを要求元のクライアントに配信します。

スタンドアロンモードの場合、InterScan VirusWall は FTP プロキシサーバとして機能します。ユーザは、次のように入力して、指定された FTP サーバに FTP VirusWall 経由で接続します。

{ ユーザ名 }@{FTP サーバ IP アドレス }:{ ポート番号 }

ポートマッピングモード (FTP プロキシを使用) では、InterScan VirusWall は既存の FTP プロキシサーバを補完する役割を果たします。プロキシサーバを使用しない場合、FTP VirusWall に接続しているクライアントは、Web コンソールの [FTP 設定] 画面で指定されている実際の FTP サーバにリダイレクトされます。

注意： FTP サーバとクライアントコンピュータ間のすべての FTP セッションは FTP VirusWall 経由で渡されますが、エンドユーザはこの処理を認識しません。

FTP スタンドアロンモードの配置

図 1-14「独立したプロキシサーバがあるスタンドアロンモードでの FTP 配置」(22 ページ) に示すように、FTP プロキシサーバがないトポロジで FTP VirusWall を配置できます。FTP VirusWall が FTP サーバとは別のコンピュータに配置されているスタンドアロンモードでは、Web コンソールの [FTP の設定] 画面 ([FTP]→[設定]) にある [FTP サーバ設定] の [オリジナル FTP サーバの場所] で、[user@host] を使用 を選択します。[user@host を使用] を選択すると、FTP VirusWall は FTP サーバとそのホスト名を使用して通信します。

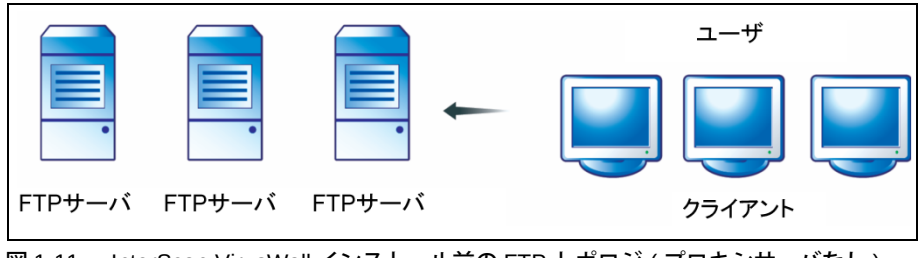


図 1-11.　InterScan VirusWall インストール前の FTP トポロジ (プロキシサーバなし)

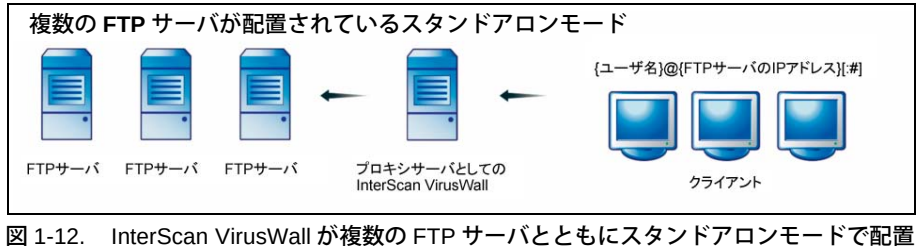


図 1-12.　InterScan VirusWall が複数の FTP サーバとともにスタンドアロンモードで配置されている FTP トポロジ

FTP プロキシサーバが独立した専用のコンピュータである場合は、FTP VirusWall をスタンドアロンモードで配置することもできます。最初のシナリオのように、このシナリオでは、[FTP の設定] 画面 ([FTP]→[設定]) の [FTP サーバ設定] で [user@host を使用] (初期設定) を選択します。FTP VirusWall はトラフィックを検索し、トラフィックを最終的に配信するために、FTP プロキシサーバのコンピュータに転送します。

図 1-13.　InterScan VirusWall インストール前の FTP トポロジ (プロキシサーバあり)

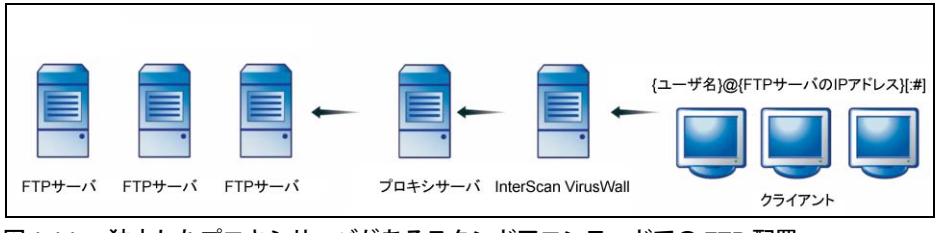


図 1-14.　独立したプロキシサーバがあるスタンドアロンモードでの FTP 配置

FTP ポートマッピングモードの配置

ポートマッピングモードでは、Web コンソールの [FTP の設定] 画面 ([FTP]→[設定]) にある [FTP サーバ設定] の [サーバの場所] で、元の FTP サーバの IP アドレスとポートを設定します (図 1-15 を参照)。

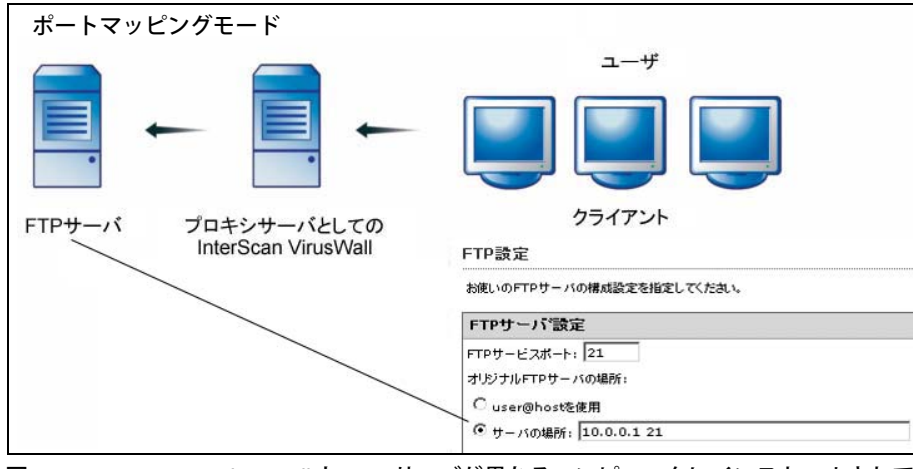


図 1-15. InterScan VirusWall と FTP サーバが異なるコンピュータにインストールされているポートマッピングモードにおける、InterScan VirusWall インストール後の FTP トポロジ。FTP サーバの Web コンソール設定を表示

FTP サーバと FTP VirusWall が同じコンピュータにインストールされているポートマッピングモードで、FTP VirusWall を配置する場合、Web コンソールの [FTP の設定] 画面 ([FTP]→[設定]) にある [FTP サーバ設定] の [サーバの場所] で、FTP サーバの絶対パスを設定します (24 ページの図 1-17「ポートマッピングモードにおける、InterScan VirusWall インストール後の FTP トポロジ (実際の FTP サーバにマッピング)」を参照)。

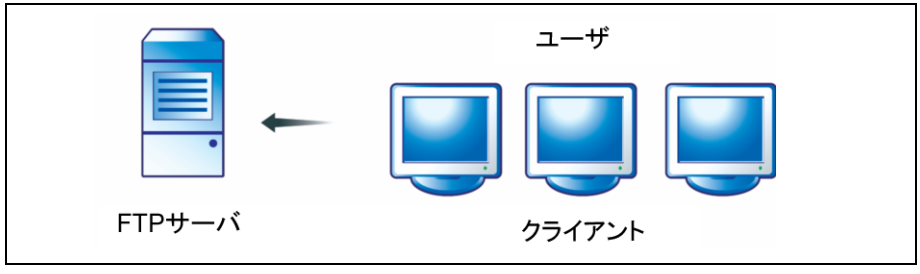


図 1-16.　FTP サーバが 1 つだけの簡単な FTP トポロジ

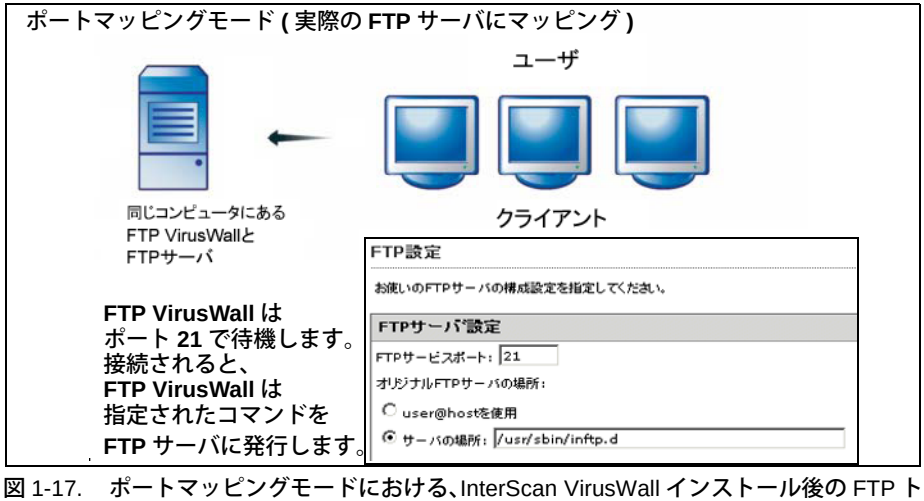


図 1-17.　ポートマッピングモードにおける、InterScan VirusWall インストール後の FTP トポロジ (実際の FTP サーバにマッピング)

HTTP VirusWall を配置する

InterScan VirusWall (HTTP VirsWall) は 3 つのモードで配置できます。

- スタンドアロンモード
- 依存モード
- リバースプロキシモード

HTTP VirusWall スタンドアロンモード

スタンドアロンモードの場合、InterScan VirusWall は、HTTP プロキシサーバとして機能するサーバ、または既存サーバから HTTP トラフィックを受信するゲートウェイデバイスの直後に配置されます。

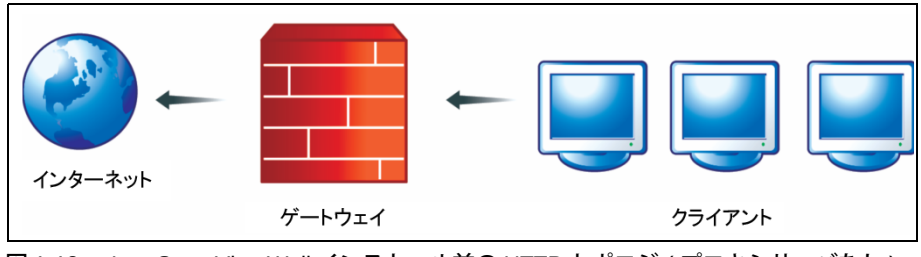


図 1-18.　InterScan VirusWall インストール前の HTTP トポロジ (プロキシサーバなし)

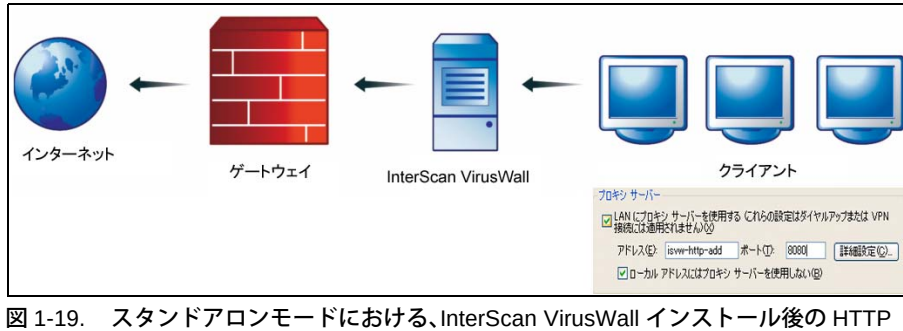


図 1-19.　スタンドアロンモードにおける、InterScan VirusWall インストール後の HTTP トポロジ (プロキシサーバなし)

HTTP VirusWall 依存モード

依存モードの場合、InterScan VirusWall は、クライアントコンピュータと HTTP プロキシサーバの間に配置されます。

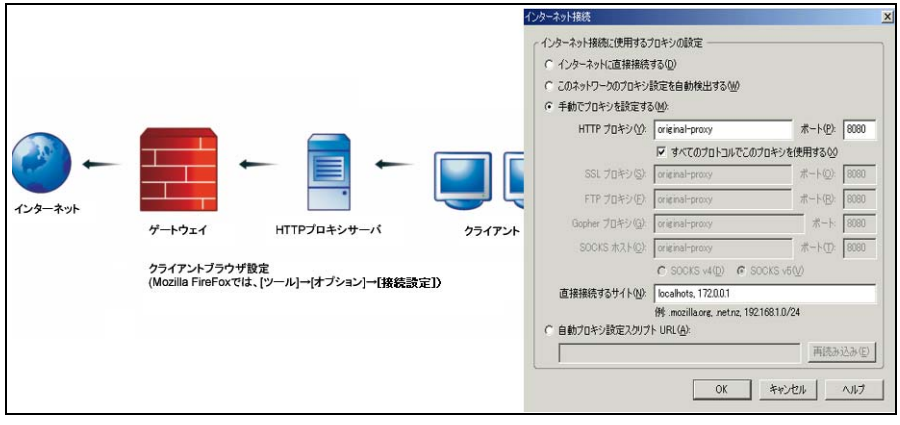


図 1-20.　InterScan VirusWall インストール前の HTTP トポロジ (プロキシサーバあり)

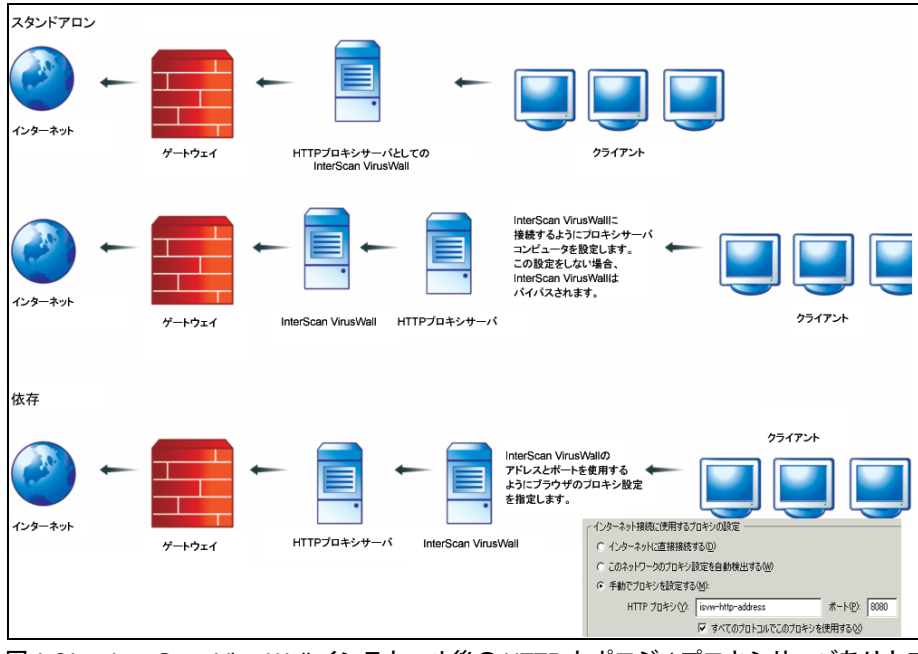


図 1-21.　InterScan VirusWall インストール後の HTTP トポロジ (プロキシサーバありとプロキシサーバなし)

HTTP リバースプロキシモード

リバースプロキシでは、外部のクライアントおよびイントラネットユーザはコンテンツサーバを利用できますが、このコンテンツサーバへの監視されていない、直接的なアクセスはファイアウォールによって阻止されます。このモードは通常、インターネット間でデータを交換する e- コマーストランザクションや分散アプリケーションに関連する Web サイトで使用されます。またクライアントが離れた場所から Web サーバにファイルをアップロードする場合などに使用されます。Web サーバはこのトポロジによって保護されます。このトポロジの場合、InterScan VirusWall は、コンテンツサーバからネットワーク内外のクライアントへ送られる HTTP トラフィックを検索します。

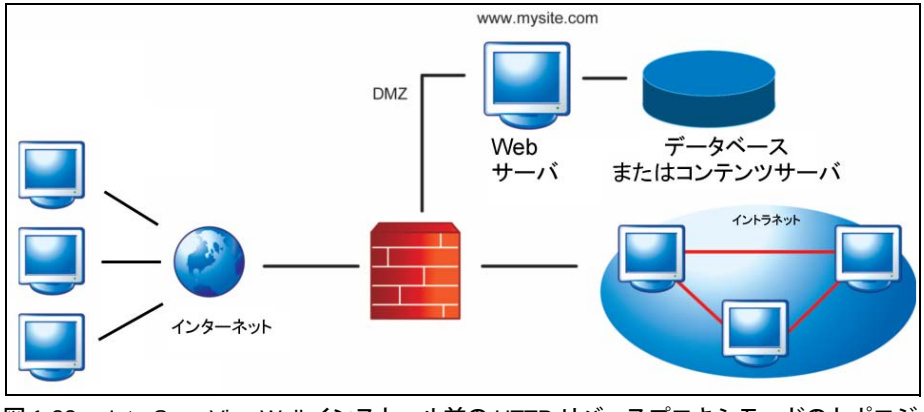


図 1-22.　InterScan VirusWall インストール前の HTTP リバースプロキシモードのトポロジ

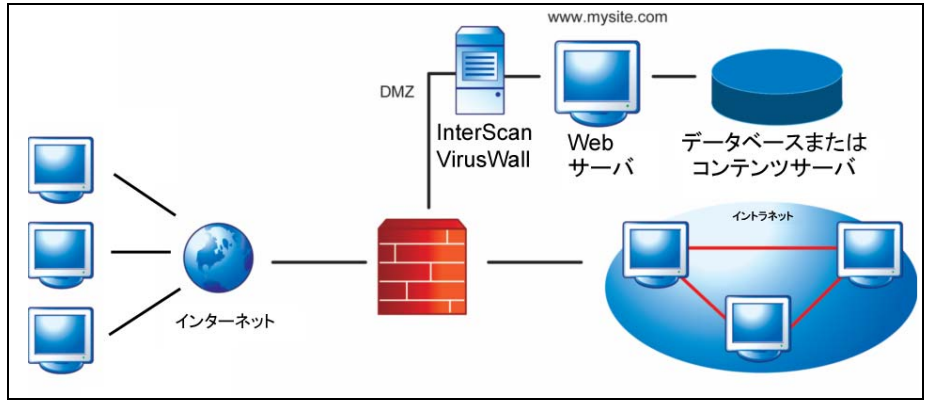


図 1-23. InterScan VirusWall インストール後の HTTP リバースプロキシモードのトポロジ

第 2 章

インストール

この章では、以下のトピックについて説明します。

- 33 ページの「インストール前のチェックリスト」
- 34 ページの「システム要件」
- 37 ページの「InterScan VirusWall をインストールする」
- 51 ページの「インストール後のタスク」

概要

Trend Micro InterScan VirusWall スタンダードエディション (以下、InterScan VirusWall) のインストールに要する時間は約 10 分です。インストールは、InterScan VirusWall を配置するコンピュータで実行してください。既存のサーバと連携して機能するように InterScan VirusWall を設定するには、さらに 10 分を必要とします。

本バージョンでは、既存の InterScan VirusWall ユーザがバージョン 3.8x または 5.0 から移行するのを支援する移行ツールを利用できます。

この章では、インストール計画、最小および推奨のシステム要件、実際のインストールプロセス、および重要なインストール後のタスクについて説明します。

インストール前のチェックリスト

InterScan VirusWall をインストールする前に、以下を実行してください。

- ☐ **1.** InterScan VirusWall をインストールするコンピュータで、バージョン 3.8x、5.0、または 6.0 以外の InterScan VirusWall があればこれをアンインストールします。
- ☐ **2.** リアルタイム検索の製品を削除するか、次の項目を製品の検索除外リストに追加します。
  - InterScan VirusWall のインストール先のパス
  - 4 つのそれぞれのプロトコルの隔離パス (各パスは一意である必要があります)
- ☐ **3.** root でログオンします。
- ☐ **4.** InterScan VirusWall が初期設定で使用する以下のポートが、すでに使われていないことを確認してください。新規インストールを実行する場合のみ適用できます (# netstat -an コマンドを実行すると、使用中のすべてのポートが表示されます)。
  - FTP: 21 ☐
  - SMTP: 25 ☐
  - POP3: 110 ☐
  - HTTP: 8080 ☐

  注意： Web コンソールの場合、初期設定のポート番号は HTTP では 9240、HTTPS では 9241 です。ただし、インストール時に別のポート番号を指定できます。
- ☐ **5.** InterScan VirusWall をはじめてインストールする場合は、SMTP VirusWall が有効なドメインとして認識するドメインのリストを作成します。SMTP は、これらのドメインを宛先とするメールだけを配信します。

システム要件

表 2-1.　最小システム要件と推奨システム要件

要件	最小	推奨
CPU	Intel Pentium 4、1.6GHz プロセッサ	ハイパースレッディングテクノロジをサポートする Intel Pentium 4、3.0GHz 以上
メモリ	• 512MB (HTTP URL フィルタを使用しない場合) • 2GB (HTTP URL フィルタを使用する場合)	1GB 以上
ハードディスクの空き領域	プログラムのインストール先ドライブに 4GB 注意 : InterScan VirusWall のインストールプログラムは、システムおよびインストール先ドライブのディスクの空き領域をチェックします。サーバに最小ディスク領域を確保できない場合、インストールプロセスは開始されません。	隔離ファイルとログファイル用にプログラムのインストール先ドライブに 20GB
ネットワークインタフェース	10/100/1000 全二重 NIC	10/100/1000 全二重 NIC
モニタ / ディスプレイ	800 x 600 の解像度、256 色	1024x768 以上の解像度、ハイカラー (16 ビット)
Web コンソールへのアクセスに使用するインターネットブラウザ	Microsoft Internet Explorer 6.0	N/A

表 2-1.　最小システム要件と推奨システム要件 (続き)

要件	最小	推奨
OS	・ Red Hat Enterprise Linux (AS、ES、WS) 3.0 (アップデートパッケージ 4) 必要なインストールパッケージクラスタ : 最小システム （Minimal） ・ Red Hat Enterprise Linux (AS、ES、WS) 4.0 (アップデートパッケージ 2) 必要なインストールパッケージクラスタ : 最小システム （Minimal） ・ SUSE Linux Enterprise server 9 ・ SUSE Linux Enterprise server 10 ・ SUSE Linux Enterprise server 10、64 ビット ・ SUSE Linux Enterprise desktop 10、64 ビット ・ SUSE Linux Professional 10.0 ・ SUSE Linux Professional 10.1 ・ Turbolinux 8 Server 必要なインストールパッケージクラスタ : 基本システム ・ Turbolinux 10 Server 必要なインストールパッケージクラスタ : 基本システム	N/A

表 2-1.　最小システム要件と推奨システム要件 (続き)

要件	最小	推奨
追加で必要なライブラリ	Glibc-2.3.4 Libstdc++-3.4.4 Libstdc++-2-libc6.1-1 libstdc++-libc6.2-2.so.3 (参考) 上記のライブラリは、以下のようなパッケージファイルに含まれています。 Red Hat Enterprise Linux : glibc-2.3. ～ .rpm、libstdc++-3.4. ～ .rpm、compat-libstdc++- ～ .rpm SUSE Linux Enterprise server: glibc-2.3. ～ .rpm、libstdc++-3.4. ～ .rpm、compat- ～ .rpm Turbolinux Server: glibc-2.3. ～ .rpm、libstdc++-3.4. ～ .rpm、libstdc++-compat- ～ .rpm (～の部分はリリースバージョンで、ディストリビューションによって異なります)	N/A

InterScan VirusWall をインストールする

次の 3 種類のインストールシナリオを利用できます。このセクションでは、新規インストールのみを扱います。以前のバージョンからのアップグレードについては、第 3 章「以前のリリースからの移行」を参照してください。

新規インストール

以前のバージョンがインストールされていないコンピュータに本バージョンをインストールする場合で、設定をインポートしないときは、この手順を使用します (38 ページの「新規インストールを実行する」を参照)。

同じコンピュータ上でのバージョン 3.8x からのアップグレード

InterScan VirusWall 3.8x がインストールされているコンピュータに本バージョンをインストールする場合で、バージョン 3.8x の設定をインポートするときは、この手順を使用します (58 ページの「同じコンピュータ上でバージョン 3.8x からアップグレードする」を参照)。

異なるコンピュータ上でのバージョン 3.8x からのアップグレード

新しいコンピュータに本バージョンをインストールする場合で、InterScan VirusWall for UNIX 3.8x がインストールされている別のコンピュータの設定を移行するときは、この手順を使用します。移行ツールを使用してバージョン 3.8x の設定を移行し、インストール時にインポートします (66 ページの「異なるコンピュータ上でバージョン 5.0 からアップグレードする」を参照)。

バージョン 5.0 からのアップグレード

新しいコンピュータに本バージョンをインストールする場合で、Trend Micro InterScan VirusWall for Small and Medium Businesses 5.0 がインストールされている別のコンピュータの設定を移行するときは、この手順を使用します。移行ツールまたはコマンドラインを使用してバージョン 5.0 の設定を移行し、インストール時にインポートします。

バージョン 6.0 からのアップグレード

InterScan VirusWall スタンダートエディション (バージョン 6.0) をアップグレードする場合は、この手順を使用します。インストーラにより、以前のバージョン 6.0 の設定がすべてインポートされます。

新規インストールを実行する

InterScan VirusWall の新規インストールを実行するには

1. root でログオンします。
2. プログラムの tar.gz ファイルを製品 CD-ROM またはトレンドマイクロのダウンロードサイトから取得し、インストール先コンピュータの任意のディレクトリにコピーします。次のコマンドを実行して tar.gz ファイルを解凍します。

   tar xvzf {tar.gz ファイル名 }

   例 :
   tar xvzf ISVW_lnx_release.tar.gz
3. 次のディレクトリとファイルが解凍されます。

   ./setup.tar.gz
   ./setup.sh
   ./isvw.tar.gz
   ./README.txt
   ./tool/
   ./tool/isvw-migration

4. 次のコマンドを実行して、インストールを開始します。

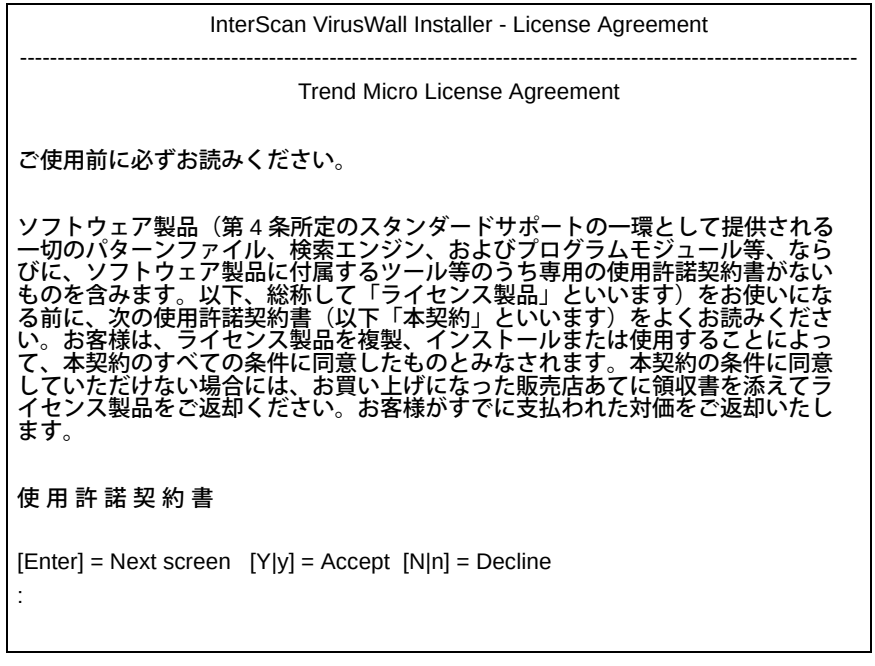
```
# ./setup.sh
```

次の画面が表示されます。

```
                    InterScan VirusWall Installer - Main Menu
------------------------------------------------------------------------------------------------------------
Welcome to the Trend Micro InterScan VirusWall Installer


Your current system configuration:


InterScan VirusWall -------- [Not installed]


1. Install InterScan VirusWall
2. Exit installation


Enter option number [1]:
```

図 2-1. インストーラ メインメニュー

5. 使用許諾契約の内容を表示して同意するには、「1」を入力して <Enter> キーを押すか、単に <Enter> キーを押します。次の画面が表示されます。


InterScan VirusWall Installer - License Agreement

Trend Micro License Agreement

ご使用前に必ずお読みください。

ソフトウェア製品（第 4 条所定のスタンダードサポートの一環として提供される一切のパターンファイル、検索エンジン、およびプログラムモジュール等、ならびに、ソフトウェア製品に付属するツール等のうち専用の使用許諾契約書がないものを含みます。以下、総称して「ライセンス製品」といいます）をお使いになる前に、次の使用許諾契約書（以下「本契約」といいます）をよくお読みください。お客様は、ライセンス製品を複製、インストールまたは使用することによって、本契約のすべての条件に同意したものとみなされます。本契約の条件に同意していただけない場合には、お買い上げになった販売店あてに領収書を添えてライセンス製品をご返却ください。お客様がすでに支払われた対価をご返却いたします。

使 用 許 諾 契 約 書

[Enter] = Next screen [Y|y] = Accept [N|n] = Decline

:

図 2-2. InterScan VirusWall 使用許諾契約書 (1 ページ目)

6. 使用許諾契約を読んだ後に、[y] を選択して同意します。

7. 実行するインストールの種類を選択します。ここでは「新規インストール」を説明するため、以下の画面ではオプション 1 を選択します (設定の移行に関する詳細については、58 ページの「同じコンピュータ上でバージョン 3.8x からアップグレードする」と 66 ページの「異なるコンピュータ上でバージョン 5.0 からアップグレードする」を参照)。

```
InterScan VirusWall Installer - Installation Type
-------------------------------------------------------------------------------------------------------

Please select an installation type:

1. Install as a fresh installation
2. Install using configuration settings of previously installed version
3. Exit installation

Enter option number: 1
```

図 2-3. インストールの種類の選択

新規インストールを選択すると、インストーラによってシステムチェックが実行されます。

```
InterScan VirusWall Installer - System Check
-------------------------------------------------------------------------------------------------------
Checking the system . . .
The Linux kernel verion is [2.6.9-5.EL].

System check completed successfully.

[Enter] = Continue installation   [Ctrl+c] = Exit installation

:
```

図 2-4. システムチェック

InterScan VirusWall をアクティベートする

InterScan VirusWall はアクティベートした場合に限り、ネットワーク全体を保護できます。アクティベートしなければ、検索エンジンおよびパターンファイルのアップデートと大規模感染予防サービスを受けることはできません。InterScan VirusWall は、インストール後に InterScan VirusWall Web コンソールから、またはインストール中にアクティベートできます。

ヒント： インストール中に InterScan VirusWall をアクティベートすることをお勧めします。これによって、インストールおよび設定直後から、InterScan VirusWall による適切な保護が可能になります。

インストール中に InterScan VirusWall をアクティベートするには

1. [System Check] 画面で <Enter> キーを押します (図 2-4「システムチェック」(41 ページ) を参照)。次の画面が表示されます。

```
                InterScan VirusWall Installer - Product Activation
---------------------------------------------------------------------------------------------------

InterScan VirusWall must be activated in order to receive pattern and engine
updates as well as Outbreak Alerts.
Do you have the Activation Code for this product?

[Y|y] = Yes     [N|n] = No      [Ctrl+c] = Exit installation

:
```

図 2-5. 製品のアクティベーション

2. アクティベーションコードを入手していて、インストール中に入力する場合は、「y」と入力して <Enter> キーを押します。[Please enter the Activation Code] プロンプトが表示されます。

```
InterScan VirusWall Installer - Product Activation
----------------------------------------------------------------------------------------------------

Please enter the Activation Code
(Activation Code format: xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx)

[Enter] = Continue installation   [Ctrl+c] = Exit installation

:
```

図 2-6. アクティベーションコードの入力

3. コマンドプロンプト (:) に正しいアクティベーションコードを入力し、<Enter> キーを押します。[Activation Success] 画面が表示されます (41 ページの図 2-7「アクティベーションの成功」)。

```
InterScan VirusWall Installer - Activation Success
----------------------------------------------------------------------------------------------------

InterScan VirusWall has been successfully activated. The product
can now receive pattern and engine updates and Outbreak Prevention
Policy alerts.

[Enter] = Continue installation  [Ctrl+c] = Exit installation

:
```

図 2-7. アクティベーションの成功

4. <Enter> キーを押して続行してください。パスワードが空白の場合は、管理者パスワードの入力画面が表示されます (図 2-8「管理者パスワードの入力」)。

注意： インストール中に製品をアクティベートしない場合は、インストーラは初期設定では体験版をインストールします。アクティベーションコードは、インストール後に Web コンソールから入力できます ([管理]→[製品ライセンス情報])。

管理者パスワードを設定する

InterScan VirusWall Web コンソールを使用するには、管理者パスワードを設定する必要があります。管理者パスワードは、以下の管理者パスワードの入力画面で設定できます。

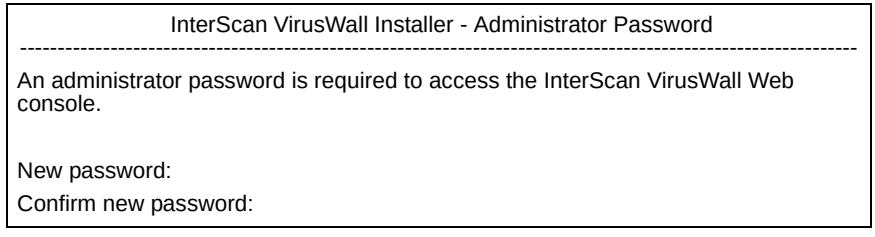


図 2-8.　管理者パスワードの入力

事前設定

Web コンソールの管理者パスワードを入力すると、以下の [Installation List] 画面が表示されます。

```
InterScan VirusWall Installer - Installation List
--------------------------------------------------------------------------------

        Web Console addresses:
          - HTTP address:        All Interfaces
          - HTTP port:           9240
          - HTTPS address:       All Interfaces
          - HTTPS port:          9241

        Installation path:       /opt/trend

        Administrator password:  ********

1. Modify Web console addresses
2. Modify installation path
3. Modify administrator password
4. Continue with installation
5. Exit installation

Enter option number [4]:
```

図 2-9. インストールオプションの確認

この画面には HTTP と HTTPS プロトコル用に選択したポートとインタフェース、および初期設定の InterScan VirusWall インストールパスが表示されます。図 2-9「インストールオプションの確認」(45 ページ) に示すように、この画面には InterScan VirusWall インストールパスと Web コンソールに関する次の情報が表示されます。

- HTTP IP アドレス
- HTTP ポート番号
- HTTPS IP アドレス
- HTTPS ポート番号

この画面から、以下を選択できます。

1. Web コンソールアドレスの修正
2. インストールパスの修正
3. 管理者パスワードの修正
4. インストールの続行
5. インストールの中止

ヒント：管理者パスワードは後で Web コンソールから変更できますが、インストール中にインストールパスまたは Web コンソールのアドレスを修正する場合はこの画面で行ってください。後から変更する場合は、再インストールが必要になります。

上記の設定を変更するか「4」を入力してインストールを続行した場合、InterScan VirusWall 検索サービスを選択するように求める画面が表示されます。「y」を入力して <Enter> キーを押すか、単に <Enter> キーを押して、InterScan VirusWall のインストールで検索する各サービスを有効にします。以下の画面では 4 つのプロトコルオプションがすべて表示されます。

```
InterScan VirusWall Installer - Preconfiguration
---------------------------------------------------------------------------------------------------
Services Configuration

Type y or n to select the services to enable. (You can also do this after installation,
from the Web console.)

[Ctrl+c] = Exit installation

Enable SMTP scanning? (y/n) [y]:
Enable HTTP scanning? (y/n) [y]:
Enable FTP scanning? (y/n) [y]:
Enable POP3 scanning? (y/n) [y]:
```

図 2-10.　インストール事前設定画面 1、サービス設定

次のインストール画面ではリレー設定に関する情報が表示され、ネットワークにあるドメインのリストを入力するように促されます。InterScan VirusWall では、入力されたドメインを宛先とするメールのみを受信します。

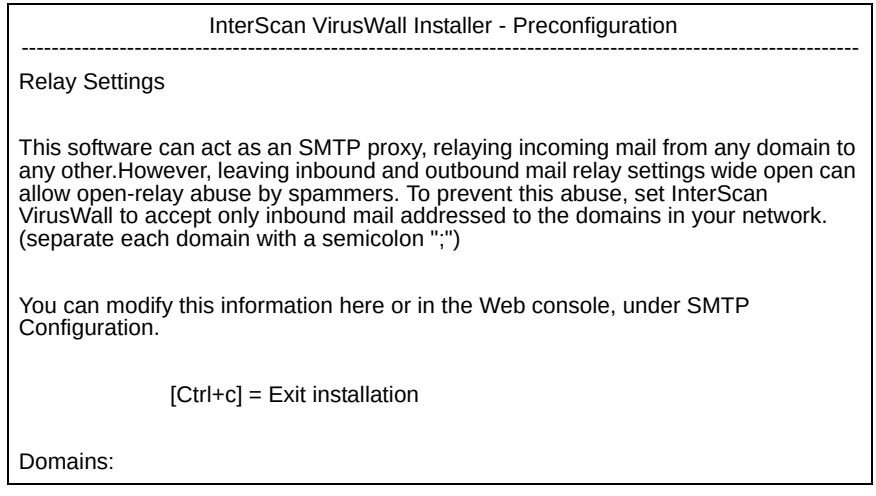


図 2-11.　インストール事前設定画面 2、リレー設定

ヒント： スパムメール送信者がユーザのメールサーバを利用するのを防ぐために、リレー設定を使用することを強くお勧めします。

通知設定

リレー対策設定の内部ドメインを入力すると、以下の画面が表示されます。

```
                    InterScan VirusWall Installer - Preconfiguration
--------------------------------------------------------------------------------------------------------------

Notification Settings


InterScan VirusWall requires the following information in order to send the
notification messages by email. You can also modify this information after
installation, in the Web console, under Administration > Notification Settings.


                        [Ctrl+c] = Exit installation


SMTP server:
```

図 2-12. インストール事前設定画面 3、通知設定

SMTP server: プロンプトで、SMTP サーバのアドレス (例 : smtp1.example.com または 11.4.121.121) を入力し、<Enter> キーを押します。インストーラはアドレスを記録し、SMTP ポート番号と管理者のメールアドレスの入力を求めます。

```
Port[25]:
Administrator email address (separate multiple entries with a semicolon (;))
: isvw_administrator@isvw
Sender email address(isvw@mail_sample)
:
```

図 2-13. SMTP サーバポート番号、管理者および送信者のメールアドレスを入力するためのプロンプトが表示されている、通知設定画面の下部

インストールを開始する

SMTP ポート番号と管理者メールアドレスを入力すると、入力した内容を確認してからインストールを開始するように求める画面が表示されます。

```
                    InterScan VirusWall Installer - Confirmation
------------------------------------------------------------------------------------------------------------

Installer is ready to install InterScan VirusWall.

1. Return to Main Menu
2. Start installation
3. Exit Installation

Enter option number [2]:
```

図 2-14.　インストール開始の確認

「2」を入力して <Enter> キーを押すか、単に <Enter> キーを押して、インストールを開始します。インストーラがファイルのコピーを開始し、ファイルコピーの何パーセントが完了したかを示す以下の画面が表示されます。

```
Copying files...

    100%


Starting ISVW6 services:
                                                                    [ OK ]
```

図 2-15.　ファイルのコピー

インストーラは入力した設定を使用して、InterScan VirusWall をインストールします。インストールが完了すると、以下の画面が表示されます。

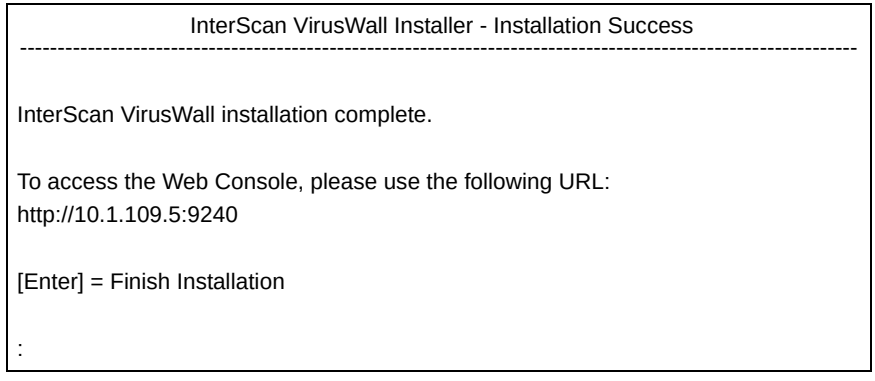


図 2-16.　インストールの成功

InterScan VirusWall Web コンソールの URL が、[Installation Success] 画面に表示されます。この URL をサポートされている Web ブラウザ (34 ページの「システム要件」を参照) のアドレスフィールドにコピーし、InterScan VirusWall Web コンソールを表示します。

ヒント：後から使用できるように、インストールを終了する前に、InterScan VirusWall Web コンソールの URL を記録しておくことをお勧めします。

InterScan VirusWall はインストールされました。Web コンソールを使用して、いくつかのタスクを実行する必要があります。以下のセクションでは、このタスクについて説明します。

インストール後のタスク

InterScan VirusWall をインストールした後は、いくつかのタスクをただちに実行して、設定がすべて完了し、正しく機能していることを確認できます。

注意： これらのタスクの実行方法については、オンラインヘルプまたは対応する設定ガイド (設定ガイドのリストについては、8 ページの表 1、「InterScan VirusWall のドキュメント一覧」) を参照してください。

インストール後のチェックリスト

- ☐ 製品のアクティベート (インストール中にアクティベートされていない場合)
- ☐ サービスの有効化 (ウイルス検索、スパムメール検出、コンテンツフィルタ)
- ☐ コンポーネントのアップデート (パターンファイル、検索エンジン) と予約アップデートの設定
- ☐ 通知の設定 (通知サーバ、ポート、管理者メール、および文字セット)
- ☐ プロキシ設定の構成 (実行しているサービスによって異なる)
  詳細については、53 ページの「プロキシサーバの設定」を参照
- ☐ 大規模感染予防サービスの設定
  詳細については、53 ページの「大規模感染予防サービスの設定」を参照)
- ☐ プロトコル別の検索の設定
  詳細については、53 ページの「プロトコル別の検索の設定」を参照)
- ☐ インストールのテスト (EICAR テストウイルスを入手して、有効なすべてのプロトコルでテストします。
  詳細については、96 ページの「InterScan VirusWall をテストする」を参照)
- ☐ 追加インスタンスの追加 (任意)
  詳細については、55 ページの「追加インスタンスのインストール」を参照

製品のアクティベート

インストール中に InterScan VirusWall をアクティベートしなかった場合は、アクティベートします。または、30 日の体験期間を開始します。

サービスの有効化

ウイルス検索、スパムメール検出、およびコンテンツフィルタを有効にして開始します。設定するプロトコルについては、対応する設定ガイドを参照してください。

- Trend Micro InterScan VirusWall スタンダードエディション SMTP 設定ガイド
- Trend Micro InterScan VirusWall スタンダードエディション HTTP 設定ガイド
- Trend Micro InterScan VirusWall スタンダードエディション FTP/POP3 設定ガイド

これらのマニュアルはすべて、InterScan VirusWall に同梱されている製品 CD-ROM または次のトレンドマイクロ製品のダウンロードサイトから、Adobe Acrobat 形式 (PDF) で入手できます。

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

コンポーネントのアップデート

パターンファイルと検索エンジンをアップデートし、ウイルスパターンファイル、検索エンジン、およびスパムメール判定ルール / エンジンの予約アップデートを設定します (詳細については、102 ページの「InterScan VirusWall コンポーネントをアップデートする」を参照)。

通知の設定

通知サーバ、ポート、管理者のメールアドレス、文字コードなどの通知設定を行います (詳細については、111 ページの「通知設定」を参照)。

プロキシサーバの設定

自社のニーズに合わせて製品の初期設定を変更します。システムにインストールされているサービスとプロキシサーバに応じて、インストール後の InterScan VirusWall の設定時に以下の情報が必要になる場合があります。

- 現在の SMTP サーバの IP アドレスとポート番号
- 現在の POP3 サーバの IP アドレスとポート番号
- 現在の HTTP プロキシサーバの IP アドレスとポート番号
- InterScan VirusWall を HTTP プロキシサーバとして設定する場合に InterScan VirusWall で使用するポート番号
- 現在の FTP プロキシサーバの IP アドレスとポート番号
- InterScan VirusWall を FTP プロキシサーバとして設定する場合に InterScan VirusWall で使用するポート番号

インターネット接続のためにプロキシが必要な場合は、登録 / アクティベーション、アップデートの各サービスに対してプロキシ情報を設定します (詳細については、93 ページの「[管理] メニュー」を参照)。

大規模感染予防サービスの設定

大規模感染予防サービスを有効にするには

1. 左側のメニューで [大規模感染予防]→[ステータス] の順に選択します。
2. [大規模感染予防サービスを有効にする] 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。

プロトコル別の検索の設定

SMTP プロトコルが有効な場合 :

- SMTP の送受信トラフィックを設定します。
- SMTP 検索、IntelliTrap、フィッシング対策、スパムメール対策、スパイウェア対策、およびコンテンツフィルタに対してポリシーと通知を設定します。

HTTP プロトコルが有効な場合 :

- HTTP の動作モードを設定します。
- HTTP 検索、フィッシング対策、スパイウェア対策、URL ブロック、および URL フィルタの設定に対してポリシーと通知を設定します。

FTP プロトコルが有効な場合 :

- FTP の動作モードを設定します。
- FTP 検索とスパイウェア対策に対してポリシーと通知を設定します。

POP3 プロトコルが有効な場合 :

- POP3 IP アドレスおよび接続を設定します。
- POP3 検索、IntelliTrap、フィッシング対策、スパムメール対策、スパイウェア対策、およびコンテンツフィルタに対してポリシーと通知を設定します。

インストールのテスト

EICAR テストファイルを入手して、インストールが正しく機能していることを確認します。

- SMTP プロトコルが有効な場合 :
  - SMTP の送受信検索をテストします。
  - SMTP の送受信コンテンツフィルタをテストします。
- POP3 プロトコルが有効な場合は、POP3 の検索とコンテンツフィルタ設定をテストします。
- HTTP プロトコルが有効な場合 :
  - HTTP のダウンロードとアップロード検索をテストします。
  - HTTP URL ブロックと URL フィルタをテストします。
- FTP プロトコルが有効な場合は、FTP のダウンロード / アップロード検索をテストします。

追加インスタンスのインストール

必要に応じて、InterScan VirusWall のその他のインスタンスをネットワークにインストールします。

共通の配置方法は、InterScan VirusWall のインスタンスを各プロトコルのサーバに 1 つ配置し、各サーバで関連する検索サービスのみを有効にすることです。たとえば InterScan VirusWall のインスタンスを 1 つ、以下のサーバにインストールします。

- SMTP サーバ
- POP3 サーバ
- FTP サーバ
- HTTP サーバ

この方法を使用すると配置の管理が容易になり、各サーバの帯域幅が節約されます。

第 3 章

以前のリリースからの移行

この章では、以下のトピックについて説明します。

- 58 ページの「移行パス」
- 58 ページの「同じコンピュータ上でバージョン 3.8x からアップグレードする」
- 60 ページの「バージョン 3.8x 用の移行ツールを使用する」
- 66 ページの「異なるコンピュータ上でバージョン 5.0 からアップグレードする」

移行パス

この製品のリリースでは、InterScan VirusWall for UNIX 3.8x、および Trend Micro InterScan VirusWall for Small and Medium Businesses 5.0 から Trend Micro InterScan VirusWall スタンダードエディション (以下、InterScan VirusWall) にアップグレードできます。

2 つの移行方法

バージョン 3.8x から本バージョンへの移行には 2 つの方法があります。1 つは、バージョン 3.8x がインストールされている同じコンピュータに本バージョンを直接インストールする方法です (58 ページの「同じコンピュータ上でバージョン 3.8x からアップグレードする」を参照)。

バージョン 3.8x がインストールされているコンピュータ以外のコンピュータに本バージョンをインストールする場合は、このリリースに同梱されている移行ツールを使用できます。移行ツールはバージョン 3.8x の設定を取得し、別のコンピュータに本バージョンをインストールする際に利用するために、取得した設定を設定ファイルに格納します。この移行ツールの使用について詳しくは、66 ページの「異なるコンピュータ上でバージョン 5.0 からアップグレードする」を参照してください。

同じコンピュータ上でバージョン 3.8x からアップグレードする

このインストール方法での最初の手順は、38 ページの「新規インストールを実行する」に概要が示されている新規インストールの手順と同じです。この手順に従ってバイナリファイルのアーカイブを解凍して、セットアップコマンドを実行し、使用許諾契約を表示して同意します。これらの手順を完了すると、InterScan VirusWall インストールプログラムによって以前のインストールの存在が検出され、次の画面が表示されます。

```
InterScan VirusWall Installer - Upgrade
----------------------------------------------------------------------------------------------------

An earlier version of InterScan VirusWall is installed on this system.

Migrate configuration settings from previous version? (y/n) [y]:
```

図 3-1.　アップグレードの確認

注意：「y」を入力した場合、古いインストールの InterScan VirusWall for UNIX 3.8x は完全に削除されます。

「y」を入力して <Enter> キーを押すか、単に <Enter> キーを押して、同じコンピュータでバージョン 3.8x インストールからアップグレードします。インストールスクリプトはバージョン 3.8x インストールから設定オプションを取得し、このタスクの完了時に警告を通知します。

```
InterScan VirusWall Installer - Upgrade
----------------------------------------------------------------------------------------------------

An earlier version of InterScan VirusWall is installed on this system.
Migrate configuration settings from previous version? (y/n) [y]:y
INF: The collection of ISUX 3.x options are done.
```

図 3-2.　バージョン 3.8x からのオプションの収集

インストーラによって古い InterScan VirusWall 3.8x が削除され、新規インストールのようにインストールが続行されますが、前のバージョンの設定を使用している点が異なります。新規インストールについて詳しくは、37 ページの「InterScan VirusWall をインストールする」を参照してください。

バージョン 3.8x 用の移行ツールを使用する

以下に説明するように、移行によって InterScan VirusWall for UNIX 3.8x の一部の設定を保護できます。

カテゴリ	設定する対象
プロトコル設定	FTP、HTTP、および SMTP
ウイルス検索設定	FTP、HTTP、および SMTP*
* ファイルタイプ別のファイルブロックおよび送信メールブロックを除きます。	

プロトコル設定の移行

ツールによって、バージョン 3.8x の intscan.ini から本バージョンの Config.xml に、SMTP、FTP、および HTTP のプロトコル設定が移行されます。

注意： パフォーマンス設定は移行されません。

ウイルス検索設定

移行ツールでは、SMTP、FTP、および HTTP のウイルス検索設定が移行されます。

注意： SMTP 検索では、ファイルタイプ別のファイルブロックおよび送信メールブロックは移行できません。

移行対応表

このツールでバージョン 3.8x から移行できる設定の詳しいリストについては、「Trend Micro InterScan VirusWall スタンダードエディション リファレンスマニュアル」の移行対応表を参照してください。

移行レポート

移行レポートは次の場所に置かれています。

/var/log/MigrationReport.log

異なるコンピュータ上でバージョン 3.8x からアップグレードする

別のコンピュータに以前のバージョン 3.8x がインストールされている場合は、InterScan VirusWall に付属している移行ツールを使用すると、バージョン 3.8x から多くの設定をインポートできます。

ツールを見つけるには、次に示すように、まず新規インストール対象のコンピュータ上にプログラムの tar.gz ファイルを解凍します。

```
$ tar xvzf ISVW6_lnx_GM_####.tar.gz
```

移行ツールのファイル名は、isvw-migration で、このファイルは次の tool ディレクトリに配置されています。

{ インストールディレクトリ }/tool/isvw-migration

移行ツールを使用してバージョン 3.8x 設定を移行するには

1. 移行先のコンピュータから InterScan VirusWall 3.8x が配置されているコンピュータに、isvw-migration ツールをコピーします。
2. バージョン 3.8x のコンピュータに root としてログオンします。
3. そのコンピュータから次のコマンドを実行します。

   isvw-migration { エクスポートファイル名 }

ここでエクスポートファイル名は、InterScan VirusWall 3.8x の設定を一時的に保管するために移行ツールが作成するファイル名です。ツールによって、InterScan VirusWall for Unix 3.8x の設定が名前を指定したファイルにインポートされ、次のメッセージが表示されます。

```
# ./isvw-migration export_my_ISVW_3.8_settings.out

INF: The collection of ISUX 3.x options are done.
```

図 3-3. 移行ツールが InterScan VirusWall 3.8x の設定を正常に抽出すると、このメッセージが表示される

4. InterScan VirusWall をインストールするために、この新しいファイルを移行先のコンピュータにコピーします。

5. root として移行先のコンピュータにログオンして、次のコマンドを実行すると、インストールが開始します。

```
# ./setup.sh
```

次の画面が表示されます。

```
                    InterScan VirusWall Installer - Main Menu
------------------------------------------------------------------------------------------------------------
Welcome to Trend Micro InterScan VirusWall Install Script

Your Current System Configuration:

InterScan VirusWall ---------- [Not installed]

1. Install InterScan VirusWall
2. Exit installation

Enter option number [default: 1]:
```

図 3-4. インストーラのメインメニュー

6. 使用許諾契約の内容を表示して同意するには、「1」を入力して <Enter> キーを押すか、単に <Enter> キーを押します。次の画面が表示されます。

```
InterScan VirusWall Install Script - License Agreement
------------------------------------------------------------------------------------------------------------

                    Trend Micro License Agreement

ご使用前に必ずお読みください。

ソフトウェア製品（第 4 条所定のスタンダードサポートの一環として提供される一切のパターンファイル、検索エンジン、およびプログラムモジュール等、ならびに、ソフトウェア製品に付属するツール等のうち専用の使用許諾契約書がないものを含みます。以下、総称して「ライセンス製品」といいます）をお使いになる前に、次の使用許諾契約書（以下「本契約」といいます）をよくお読みください。お客様は、ライセンス製品を複製、インストールまたは使用することによって、本契約のすべての条件に同意したものとみなされます。本契約の条件に同意していただけない場合には、お買い上げになった販売店あてに領収書を添えてライセンス製品をご返却ください。お客様がすでに支払われた対価をご返却いたします。

使 用 許 諾 契 約 書

[Space] = Next screen   [Y|y] = Accept  [N|n] = Decline
:
```

図 3-5. InterScan VirusWall 使用許諾契約書 (1 ページ目)

7. 使用許諾契約を読んだ後に、同意するには [y] を選択します。次の画面が表示されます。

```
InterScan VirusWall Install Script - Setup Type
------------------------------------------------------------------------------------------------------------

Please select a setup type.

1. Fresh Installation
2. Migrate from configuration settings of previous version
3. Exit installation

Enter option number:
```

図 3-6. セットアップの種類の選択

8. [2. Migrate from configuration settings of previous version] オプションを選択します。

```
InterScan VirusWall Install Script - Migration File
-----------------------------------------------------------------------------------------------
Please input the configuration file
:
```

図 3-7. 設定ファイルの指定

9. InterScan VirusWall 3.8x がインストールされているコンピュータでの移行ツールの実行時にツールによって作成されたファイルの完全な絶対パスとファイル名を入力します。たとえば、次のようになります。

   /root/Desktop/export_my_ISVW_3.8_settings.out

   <Enter> キーを押し、再び <Enter> キーを押して続行してください。インストーラは設定をインポートし、システムチェックを実行して、新しくインポートした設定を使用してインストールを継続します (その他のインストール画面に関する詳細については、37 ページの「InterScan VirusWall をインストールする」を参照)。

同じコンピュータ上でバージョン 5.0 からアップグレードする

このインストール方法では、最初の手順は、38 ページの「新規インストールを実行する」に説明されている、新規インストールの方法と同じです。この手順に従ってバイナリファイルのアーカイブを解凍して、セットアップコマンドを実行し、使用許諾契約を表示して同意します。これらの手順を完了すると、InterScan VirusWall インストールプログラムによって以前のインストールの存在が検出され、次の画面が表示されます。

```
InterScan VirusWall Install Installer - Upgrade
-----------------------------------------------------------------------------------------------
An earlier version of InterScan VirusWall is installed on this system.

Migrate configuration settings from previous version? (y/n) [y]:
```

図 3-8. アップグレードの確認

注意：「y」を入力した場合、古いインストールの InterScan VirusWall 5.0 は完全に削除されます。

「y」を入力して <Enter> キーを押すか、単に <Enter> キーを押して、同じコンピュータでバージョン 5.0 インストールからアップグレードします。インストールスクリプトは、バージョン 5.0 インストールから設定オプションを取得します。

インストーラによって古い InterScan VirusWall 5.0 が削除され、新規インストールのようにインストールが続行されますが、前のバージョンの設定を使用している点が異なります。新規インストールについての詳細は、37 ページの「InterScan VirusWall をインストールする」を参照してください。

InterScan VirusWall 5.0 用の移行ツールを使用する

次に説明するように、移行ツールによって InterScan VirusWall 5.0 の一部の設定を保持できます。

カテゴリ	設定する対象
プロトコル設定	FTP、HTTP、SMTP、および POP3
ウイルス検索	FTP、HTTP、SMTP、および POP3
スパムメール対策設定	SMTP および POP3
コンテンツフィルタ設定	SMTP および POP3
URL ブロック設定	HTTP

プロトコル設定の移行

ツールによって、バージョン 5.0 の設定ファイルから、バージョン 6.02 の Config.xml に、SMTP、FTP、HTTP、および POP3 のプロトコル設定が移行されます。

注意： パフォーマンス設定は移行されません。

ウイルス検索設定の移行

移行ツールでは、SMTP、FTP、HTTP、および POP3 のウイルス検索設定が移行されます。

スパムメール対策およびコンテンツフィルタ設定の移行

移行ツールでは、SMTP および POP3 のスパムメール対策およびコンテンツフィルタ設定が移行されます。

URL ブロック設定の移行

移行ツールでは、HTTP の URL ブロック設定が移行されます。

移行対応表

このツールでバージョン 5.0 から移行できる設定の詳しいリストについては、「Trend Micro InterScan VirusWall スタンダードエディション リファレンスマニュアル」の第 3 章を参照してください。

移行レポートとログ

移行レポートは次の場所に置かれています。

```
/var/log/isvw_migration_report.txt
```

移行ログは次の場所に置かれています。

```
/var/log/migr5to6.log
```

異なるコンピュータ上でバージョン 5.0 からアップグレードする

別のコンピュータ上に以前のバージョン 5.0 がインストールされている場合は、InterScan VirusWall に付属している移行ツールを使用すると、バージョン 5.0 から多くの設定をインポートできます。

ツールを利用するには、以下に示すように、まず新規インストール対象のコンピュータ上にプログラムの tar.gz ファイルを解凍します。

```
$ tar xvzf {tar.gz ファイル名 }
```

移行ツールのファイル名は、isvw-migr5to6 で、このファイルは次の tool ディレクトリに配置されています。

{ インストールディレクトリ }/tool/isvw-migr5to6

移行ツールを使用してバージョン 5.0 設定を移行するには

1. 移行先のコンピュータから InterScan VirusWall 5.0 が配置されているコンピュータに、isvw-migr5to6 ツールをコピーします。
2. バージョン 5.0 のコンピュータに root としてログオンします。
3. そのコンピュータから以下のコマンドを実行します。

   isvw-migr5to6 -o { エクスポートファイル名 }

   ここでエクスポートファイル名は、InterScan VirusWall 5.0 の設定を一時的に保管するために移行ツールが作成するファイル名です。ツールによって、InterScan VirusWall 5.0 の設定が名前を指定したファイルにインポートされます。
4. InterScan VirusWall をインストールするために、この新しいファイルを移行先のコンピュータにコピーします。

5. root として移行先のコンピュータにログオンして、以下のコマンドを実行すると、インストールが開始します。

```
# ./setup.sh
```

次の画面が表示されます。

```
                    InterScan VirusWall Installer - Main Menu
------------------------------------------------------------------------------------------------------------
Welcome to Trend Micro InterScan VirusWall Install Script

Your Current System Configuration:

InterScan VirusWall ---------- [Not installed]

1. Install InterScan VirusWall
2. Exit installation

Enter option number [default: 1]:
```

図 3-9. インストーラのメインメニュー

6. 使用許諾契約の内容を表示して同意するには、「1」を入力して <Enter> キーを押すか、単に <Enter> キーを押します。次の画面が表示されます。

```
InterScan VirusWall Installer - License Agreement
------------------------------------------------------------------------------------------------------------

                    Trend Micro License Agreement

ご使用前に必ずお読みください。

ソフトウェア製品（第 4 条所定のスタンダードサポートの一環として提供される一切のパターンファイル、検索エンジン、およびプログラムモジュール等、ならびに、ソフトウェア製品に付属するツール等のうち専用の使用許諾契約書がないものを含みます。以下、総称して「ライセンス製品」といいます）をお使いになる前に、次の使用許諾契約書（以下「本契約」といいます）をよくお読みください。お客様は、ライセンス製品を複製、インストールまたは使用することによって、本契約のすべての条件に同意したものとみなされます。本契約の条件に同意していただけない場合には、お買い上げになった販売店あてに領収書を添えてライセンス製品をご返却ください。お客様がすでに支払われた対価をご返却いたします。

使 用 許 諾 契 約 書

[Enter] = Next screen   [Y|y] = Accept  [N|n] = Decline
:
```

図 3-10. InterScan VirusWall 使用許諾契約書 (1 ページ目)

7. 使用許諾契約を読んだ後に、同意するには [y] を選択します。次の画面が表示されます。

```
InterScan VirusWall Install Script - Setup Type
------------------------------------------------------------------------------------------------------------

Please select an installation type.

1. Install as a Fresh Installation
2. Install using configuration settings of previously installed version
3. Exit installation

Enter option number:
```

図 3-11. セットアップの種類の選択

8. [2] オプションを選択します。次の画面が表示されます。

```
InterScan VirusWall Installer - Migration File
----------------------------------------------------------------------------------------------------
Please enter the configuration file path and file name
:
```

図 3-12. 設定ファイルの指定

9. InterScan VirusWall 5.0 がインストールされているコンピュータでの移行ツールの実行時にツールによって作成されたファイルの完全な絶対パスとファイル名を入力します。たとえば、次のようになります。

   /root/Desktop/export_my_ISVW_5.0_settings.out

   <Enter> キーを押し、再び <Enter> キーを押して続行してください。インストーラは設定をインポートし、システムチェックを実行して、新しくインポートした設定を使用してインストールを継続します (その他のインストール画面に関する詳細については、37 ページの「InterScan VirusWall をインストールする」を参照)。

バージョン 6.0 からアップグレードする

バージョン 6.0 からバージョン 6.02 にアップグレードする場合、インストーラにより以前の設定がすべてインポートされます。

バージョン 6.02 にアップグレードするには

1. InterScan VirusWall のインストール先コンピュータに root としてログオンします。

2. バージョン 6.02 インストールが格納されているディレクトリから、次のコマンドを実行します。

   ./setup.sh

   次の画面が表示されます。

```
InterScan VirusWall 6 (build #2554) is installed.
The package you are installing is build #2559.

1. Uninstall InterScan VirusWall
2. Upgrade build #2554 to newer build
3. Exit
Enter option number:
```

3. オプション 2 を選択して、<Enter> キーを押すと、次の画面が表示されます。

```
Enter option number: 2
Setup is upgrading InterScan VirusWall...
Shutting down ISVW6 services:                    [  OK  ]

      100%    ************************************************

Starting ISVW6 services:                         [  OK  ]
Build upgrade succeeded.
Press Enter to exit...
```

4. 終了する場合は、<Enter> キーを押します。

第 4 章

基本的な操作

この章では、以下のトピックについて説明します。

- 74 ページの「InterScan VirusWall Web コンソール」
- 75 ページの「Web コンソールへアクセスする」
- 95 ページの「InterScan VirusWall を起動 / 停止する」
- 96 ページの「InterScan VirusWall をテストする」
- 100 ページの「リアルタイムパフォーマンスモニタを使用する」
- 102 ページの「InterScan VirusWall コンポーネントをアップデートする」
- 111 ページの「通知設定」
- 112 ページの「パスワードの管理」

InterScan VirusWall Web コンソール

図 4-1. [概要] 画面の [コンポーネントのバージョン] および [ウイルス対策] が表示されている InterScan VirusWall Web コンソール

Web コンソールのメインメニューは、10 のメニュー項目で構成されています。[概要] 以外のコンソールの各メニュー項目には、複数のサブメニュー項目があります。一方、[概要] 画面には、プロトコルごとのタブとステータスタブの 5 つのタブがあります。初期設定の[概要] 画面 ([ステータス] タブ) には、以下に示す展開 / 折り畳み可能な 6 つのセクションがあります。

- 大規模感染予防サービス
- コンポーネントのバージョン
- ウイルス対策
- スパムメール対策
- スパイウェア対策
- その他

各メニュー項目の概要と、各サブメニュー画面で実行可能なさまざまなタスクの概要については、76 ページの「Web コンソールをナビゲートする」を参照してください。

Web コンソールへアクセスする

Trend Micro InterScan VirusWall スタンダードエディション (以下、InterScan VirusWall) のインストールが完了すると、インストール時に有効にしたサービスと基本サービスが自動的に開始されます。

ヒント： InterScan VirusWall は適切な一連の初期設定値で実行されるように設定されていますが、新しくインストールしたソフトウェアのインスタンスの Web コンソールにはじめてアクセスする場合には、InterScan VirusWall の Web コンソールを開いて設定を確認することをお勧めします。

以下のブラウザを使用して Web コンソールにアクセスします。

- Microsoft Internet Explorer 6.0

Web コンソールにアクセスするには

1. Web ブラウザを開いて InterScan VirusWall の URL を入力し、続けてインストール時に設定したポート番号を入力します。初期設定のポート番号は 9240 (HTTP) および 9241 (HTTPS) です。
   - http://{InterScan VirusWall サーバの IP アドレス }:9240
   - https://{InterScan VirusWall サーバの IP アドレス }:9241

注意： この URL は、インストール時に Web コンソールにバインドした IP アドレスとポート番号によって決定されます。

2. インストール時に指定した管理者パスワードを入力し、[ログオン] をクリックします。Web コンソールの [概要] 画面が表示されます。

Web コンソールをナビゲートする

このセクションでは、Web コンソールの各種のメニュー項目について説明し、さまざまな画面をナビゲートして実行するタスクについて解説します。これらのタスクの詳しい実行方法については、InterScan VirusWall の設定ガイドを参照してください。3 つの設定ガイドは、次のとおりです。

- Trend Micro InterScan VirusWall スタンダードエディション SMTP 設定ガイド
- Trend Micro InterScan VirusWall スタンダードエディション HTTP 設定ガイド
- Trend Micro InterScan VirusWall スタンダードエディション FTP/POP3 設定ガイド

[概要] 画面

[概要] メニュー項目を使用すると、InterScan VirusWall とその 4 つのサービスのステータス概要をすばやく確認できます。[概要] をクリックすると、[ステータス] タブが選択された状態で [概要] 画面が表示されます。初期設定では、Web コンソールにログオンするとこの [概要] 画面が表示されます。

図 4-2.　すべてのサブセクションが閉じた状態の [概要] 画面

表 4-1. [概要] 画面のタブ

タブ	利用可能な情報	タスク
ステータス	製品とライセンスの情報 サービスステータス 大規模感染予防サービスのステータス パターンファイルとエンジンの現在のバージョン 以下の統計 : ・ ウイルス、スパムメール、スパイウェア / グレーウェアが検索されたファイル ・ フィルタ処理された URL とコンテンツ ・ ウイルスに感染しているファイル (IntelliTrap で検出されたファイルを含む) ・ スパムメール ・ スパイウェア / グレーウェアファイル ・ フィッシング活動	InterScan VirusWall コンポーネントの最新バージョンにアップデートします。 パターンファイルの以前のバージョンにロールバックします。
メール (SMTP)	送受信メール通信の SMTP 検索で検出されたウイルス、スパイウェア、スパムメール、およびフィッシングメールの数	SMTP トラフィックの検索を有効または無効にします。
メール (POP3)	受信メール通信の POP3 検索で検出されたウイルス、スパイウェア、スパムメール、およびフィッシングメールの数	POP3 トラフィックの検索を有効または無効にします。
Web (HTTP)	以下の HTTP 検索の統計 : ・ ウイルス / 不正プログラムの検出 ・ スパイウェア / グレーウェアの検出 ・ URL ブロック / フィッシング対策 ・ URL フィルタ	HTTP トラフィックの検索を有効または無効にします。
ファイル転送 (FTP)	ウイルス / 不正プログラムおよびスパイウェア / グレーウェア検出の FTP 検索の統計	FTP トラフィックの検索を有効または無効にします。

[SMTP] メニュー

[SMTP] メニュー項目を使用すると、SMTP のセキュリティ設定とルール設定を行うことができます。

図 4-3.　[対象] タブが選択されている [SMTP 検索 (受信)] 画面

ヒント：不正プログラム検索およびスパイウェア対策検索には、SMTP 送受信トラフィックの個別のサブメニューがあります。

[SMTP]メニューでは、SMTP トラフィックの不正プログラム検索、フィッシング対策検索、スパムメール対策検索、スパイウェア対策検索、およびコンテンツフィルタに対して対象、処理、および通知を選択できます。また、IntelliTrap の圧縮ファイル検索を最適化し、InterScan VirusWall が SMTP サーバと連動する方法を設定できます。

ヒント： これらの画面のオプションすべての詳しい使用方法については、「Trend Micro InterScan VirusWall スタンダードエディション SMTP 設定ガイド」(このソフトウェアに同梱の Adobe Acrobat ドキュメント) または InterScan VirusWall オンラインヘルプを参照してください。

表 4-2. [SMTP] のサブメニュー項目

サブメニュー	説明	タスク
検索 > 受信 > 送信 (ウイルス / 不正プログラム検索のこと)	SMTP 送受信トラフィックのリアルタイムのウイルス / 不正プログラム検索	SMTP 経由で送受信されるメッセージのウイルス / 不正プログラム検索を有効または無効にします。 検索対象の添付ファイルタイプを指定します。 感染ファイルの処理を指定します (駆除、削除、または放置)。 受信メールと送信メールの両方に対して、管理者や送信者、受信者などの特定の個人に送信される通知のカスタマイズや、ウイルス検出時にメールに挿入する通知スタンプのカスタマイズを行います。
IntelliTrap	自動的に実行可能な、圧縮ファイル内の疑わしい不正プログラムコードを検出します。	SMTP IntelliTrap を有効または無効にします。 IntelliTrap で検出された不正プログラムの処理を指定します ([感染した添付ファイルを隔離して配信]、[感染した添付ファイルを削除して配信]、または [そのまま配信])。 ヒューリスティック検索で圧縮ファイルのセキュリティリスクが検出されたときに管理者、送信者、または受信者へ送信する通知メッセージをカスタマイズします。

表 4-2. [SMTP] のサブメニュー項目 (続き)

サブメニュー	説明	タスク
フィッシング対策	SMTP メールのフィッシング活動を検出します。	SMTP のフィッシング対策を有効または無効にします。 既知のフィッシングサイトへのリンクを含むすべてのメッセージに対して実行する処理を定義します ([隔離]、[削除]、[放置])。 フィッシングメールの検出時に管理者または受信者へ送信する通知メッセージをカスタマイズします。 疑わしいフィッシング URL を TrendLabs へ報告します。
スパムメール対策 Network Reputation Services コンテンツ検索	SMTP メールサーバ経由で送信されたスパムメールを検出します。	SMTP のスパムメール対策用 Network Reputation Services およびコンテンツ検索を有効または無効にします。 NRS サービスレベルを設定します。 スパムメール検出レベルを [低]、[中]、[高] のいずれか、または [商用]、[健康]、[宗教] などのカテゴリ別に最適化します。 キーワード除外リストを定義します (識別されたキーワードを含むメッセージはスパムメールと見なされません)。または、承認済み送信者リストやブロックする送信者リストをメールアドレスまたはドメイン名によって定義します。 信頼度レベルに基づいて、スパムメールに対して実行する処理を指定します。 スパムメールの検出時に管理者または受信者へ送信する通知メッセージをカスタマイズします。

表 4-2. [SMTP] のサブメニュー項目 (続き)

サブメニュー	説明	タスク
スパイウェア対策 > 受信 > 送信	送受信されるメールメッセージのスパイウェアを検出して、特定の処理を実行できます。	送受信される SMTP メールメッセージの SMTP スパイウェア検索を有効または無効にします。 スパイウェア検索から除外するファイル名またはファイル名の拡張子を指定します。 スパイウェア / グレーウェアを検索します。 検索対象のスパイウェア / グレーウェアの種類を指定します。 スパイウェアの処理を指定します(スパイウェア / グレーウェアを隔離して配信、スパイウェア / グレーウェアを駆除して配信、またはそのまま配信)。 SMTP 検索時にスパイウェアが検出されると、選択された受信者へ自動的に通知されます。
コンテンツフィルタ	SMTP サーバを介してネットワークで送受信される情報のリアルタイム監視および管理を実行します。	SMTP のコンテンツフィルタを有効または無効にします。 キーワードと添付ファイルフィルタを指定し、メールメッセージの内容自体に基づいてメッセージの配信を評価および制御します。
設定	InterScan VirusWall サーバが SMTP サーバ経由の送受信メールをプロキシサーバとして経路指定する方法を一定の制限および制約とともに設定できます。	主要サービスポートを指定します。 受信メールの転送方法と送信メールの配信方法を指定します。 処理されたメッセージを追跡します。 送受信メールをキューに入れます。 同時クライアント接続の数、送受信メッセージのサイズ、メッセージ送信の試行頻度、およびその他の詳細設定を行います。

[HTTP] メニュー

[HTTP] メニュー項目では、HTTP ゲートウェイセキュリティの維持に役立つ機能を利用できます。

HTTP メニューでは、HTTP トラフィックの不正プログラム検索、フィッシング対策検索、およびスパイウェア対策検索に対して対象、処理、および通知を選択できます。また、URL ブロックおよび URL フィルタのルールおよびポリシーを設定し、InterScan VirusWall が HTTP サーバと連動する方法を設定できます。これらの画面のオプションすべての詳しい使用方法については、「Trend Micro InterScan VirusWall スタンダードエディション HTTP 設定ガイド」(このソフトウェアに同梱の Adobe Acrobat ドキュメント) または InterScan VirusWall オンラインヘルプを参照してください。

表 4-3. [HTTP] のサブメニュー項目

サブメニュー	説明	タスク
検索	HTTP トラフィックにおいてアップロード / ダウンロード時にウイルスその他のセキュリティリスクを検索する方法を指定できます。	HTTP 検索を有効または無効にします。 検索対象のファイルタイプを指定します。 MIME タイプの除外リストを作成します。 大きなファイルの処理方法を指定して、パフォーマンス上の問題やブラウザのタイムアウトを回避できるようにします。 感染ファイルの処理を指定します (駆除、削除、ブロック、または放置)。 感染ファイルの検出時にユーザのブラウザに表示するメッセージをカスタマイズします。

表 4-3. [HTTP] のサブメニュー項目 (続き)

サブメニュー	説明	タスク
フィッシング対策	Web サイトの閲覧中に発生したフィッシング試行への対処方法を指定できます。	HTTP のフィッシング対策を有効または無効にします。 URL をブロックするカテゴリを設定します (例 : フィッシング、スパイウェア、ウイルス流布、不正サイトの各サイト)。 ブロックまたは許可など、既知のすべてのフィッシングサイトに対する処理を定義します。 既知のフィッシングサイトの検出時にユーザのブラウザに表示するメッセージをカスタマイズします。 疑わしいフィッシング URL を TrendLabs へ送信します。
スパイウェア対策	HTTP トラフィックを検索して、各種の不正プログラムのアップロード / ダウンロードを検出します。	HTTP のスパイウェア対策を有効または無効にします。 スパイウェア / グレーウェアの除外リストを作成します。 スパイウェア / グレーウェアを検索します。 検索対象のスパイウェア / グレーウェアの種類を指定します。 スパイウェア / グレーウェアの検出時に実行する処理を設定します (ファイルブロック、ファイル隔離、またはファイルダウンロード許可)。 スパイウェア / グレーウェアの検出時にユーザのブラウザに表示するメッセージをカスタマイズします。

表 4-3.　[HTTP] のサブメニュー項目 (続き)

サブメニュー	説明	タスク
URL ブロック	ユーザ設定リストを使用して、望ましくないコンテンツを含む Web サイトへのアクセスをブロックします。 特定の URL を除外リストへ追加することにより、その URL へのアクセスを許可できます。	HTTP の URL ブロックを有効または無効にします。 Web サイト、URL キーワード、IP アドレス、または文字列によって定義される「マッチング」URL リストを定義します。一方のリストではブロックする URL を指定し、もう一方のリストではブロックから除外する URL を指定します。 ブロックまたは除外するサイトのリストをインポートします。 ブロックする URL へのアクセス時にユーザのブラウザに表示するメッセージをカスタマイズします。
URL フィルタルール	URL カテゴリのフィルタ基準となるルールを設定できます。	HTTP の URL フィルタを有効または無効にします。 ルールを適用する時間帯を設定します (業務時間、業務時間外)。
URL フィルタ設定	InterScan VirusWall データベースの URL カテゴリ全体に URL フィルタを適用する方法を定義します。	URL サブカテゴリを別のカテゴリへ移動します (例 : [アダルト / 成人向き] を [会社が禁止するサイト] から [業務に無関係なサイト] へ移動)。 Web サイト、URL キーワード、または文字列で照合される URL フィルタの除外リストを作成またはインポートします。この対象には、禁止コンテンツカテゴリに分類されている URL も含まれます。 設定を適用する日時を指定します。 再分類のために URL を TrendLabs へ送信します。

表 4-3. [HTTP] のサブメニュー項目 (続き)

サブメニュー	説明	タスク
設定	HTTP 検索サービスの設定を行います。	スタンドアロンモード、依存モード、リバースプロキシモードのいずれで InterScan VirusWall を実行するかを決定します。 HTTP 待機ポートを指定します。 FTP over HTTP の匿名ログオンで使用するメールアドレスを指定します。 HTTP リクエストのログを可能にします。

[FTP] メニュー

[FTP] メニュー項目では、FTP サーバで送受信されるファイル転送のセキュリティ強化を促進する機能を利用できます。

FTP メニューでは、FTP トラフィックの不正プログラム検索およびスパイウェア対策検索に対して対象、処理、および通知を選択できます。また、InterScan VirusWall が FTP サーバと連動する方法を設定できます。これらの画面のオプションすべての詳しい使用方法については、「Trend Micro InterScan VirusWall スタンダードエディション FTP/POP3 設定ガイド」(このソフトウェアに同梱の Adobe Acrobat ドキュメント) または InterScan VirusWall オンラインヘルプを参照してください。

表 4-4. [FTP] のサブメニュー項目

サブメニュー	説明	タスク
検索	すべてのファイルタイプまたは指定されたファイルタイプをチェックして、ウイルスその他の不正プログラムの有無を確認します。チェック対象のファイルには、圧縮されたボリューム内の個別ファイルも含まれます。	FTP 検索を有効または無効にします。 検索対象のファイルを指定します。 圧縮された添付ファイルを検索対象に含めるかどうか、含める場合はその検索方法を指定します。 感染ファイルの処理を指定します (駆除、隔離、ブロック、または放置)。 感染ファイルの検出時に管理者またはユーザへ送信する通知メッセージをカスタマイズします。

表 4-4. [FTP] のサブメニュー項目 (続き)

サブメニュー	説明	タスク
スパイウェア対策	FTP のファイル転送時におけるスパイウェア / グレーウェア検索の設定を記録します。	FTP のスパイウェア対策を有効または無効にします。 スパイウェア / グレーウェアの除外リストを作成します。 スパイウェア / グレーウェアを検索します。 特定のカテゴリに基づいてスパイウェア / グレーウェアを検索します。 スパイウェア / グレーウェアの検出時に実行する処理を指定します (ブロック、隔離、許可)。 スパイウェア / グレーウェア検出時にユーザのブラウザに表示するメッセージをカスタマイズします。
設定	FTP サーバと連動するように FTP VirusWall を設定します。	スタンドアロンモードまたは FTP プロキシモードのいずれかを選択します。 ・ ネットワーク上に FTP プロキシサーバがなく、システムの FTP プロキシサーバとして FTP VirusWall を機能させる場合はスタンドアロンモードを選択します。 ・ 既存の FTP プロキシサーバがあり、このサーバを引き続き使用する場合は FTP プロキシモードを選択します。 PASV モードを有効にし、FTP サービスポートを指定します。 許可する最大接続数を指定します。 ブラウザのタイムアウトを回避するために、送信バイト数と受信バイト数を指定します。 接続の確立時にユーザにメッセージを通知します。

[POP3] メニュー

[POP3] メニューは [SMTP] メニュー項目とほぼ同じですが、[POP3] メニューでは [検索] および [スパイウェア対策] サブメニューが受信と送信に細分化されていない点が異なります。

POP3 メニューでは、POP3 トラフィックの不正プログラム検索、フィッシング対策検索、スパムメール対策検索、スパイウェア対策検索、およびコンテンツフィルタに対して対象、処理、および通知を選択できます。また、IntelliTrap の実際のファイルタイプによるマッチングを最適化し、InterScan VirusWall が POP3 サーバと連動する方法を設定できます。これらの画面のオプションすべての詳しい使用方法については、「Trend Micro InterScan VirusWall スタンダードエディション FTP/POP3 設定ガイド」(このソフトウェアに同梱の Adobe Acrobat ドキュメント) または InterScan VirusWall オンラインヘルプを参照してください。

表 4-5. [POP3] のサブメニュー項目

サブメニュー	説明	タスク
検索 (ウイルス / 不正プログラム検索のこと)	POP3 トラフィックのリアルタイムウイルス / 不正プログラム検索を実行します。	POP3 ウイルス / 不正プログラム検索を有効または無効にします。 検索する添付ファイルを指定します。 圧縮された添付ファイルを検索対象に含めるかどうか、含める場合はその検索方法を指定します。 感染ファイルの処理を指定します(駆除、削除、または放置)。 管理者や受信者などの特定の個人に送信される通知のカスタマイズや、ウイルス検出時にメールに挿入する通知スタンプのカスタマイズを行います。

表 4-5. [POP3] のサブメニュー項目 (続き)

サブメニュー	説明	タスク
IntelliTrap	自動的に実行可能な、圧縮ファイル内の疑わしい不正プログラムコードを検出します。	POP3 IntelliTrap を有効または無効にします。 IntelliTrap で検出された BOT の処理を指定します (隔離、削除、または放置)。 ヒューリスティック検索で圧縮ファイルのセキュリティリスクが検出されたときに管理者または受信者へ送信する通知メッセージをカスタマイズします。
フィッシング対策	POP3 メールのフィッシング攻撃を検出します。	POP3 のフィッシング対策を有効または無効にします。 既知のフィッシングサイトへのリンクを含む全メッセージに対して実行する処理を定義します(隔離、削除、または放置)。 フィッシングメールの検出時に管理者または受信者へ送信する通知メッセージをカスタマイズします。 疑わしいフィッシング URL を TrendLabs へ報告します。
スパムメール対策	POP3 メールサーバ経由で送信されたスパムメールメッセージを検出します。	POP3 のスパムメール対策を有効または無効にします。 スパムメール検出レベルを [低]、[中]、[高] のいずれか、または [商用]、[健康]、[宗教] などのカテゴリ別に最適化します。 キーワード除外リストを定義します (識別されたキーワードを含むメッセージはスパムメールと見なされません)。または、承認済み送信者リストやブロックする送信者リストをメールアドレスまたはドメイン名によって定義します。 スパムメールの検出時に管理者または受信者へ送信する通知メッセージをカスタマイズします。

表 4-5. [POP3] のサブメニュー項目 (続き)

サブメニュー	説明	タスク
スパイウェア対策	受信スパイウェアを検出して特定の処理を実行できます。	POP3 のスパイウェア対策を有効または無効にします。 スパイウェア検索から除外するファイル名またはファイル名の拡張子を指定します。 スパイウェア / グレーウェアを検索します。 検索対象のスパイウェア / グレーウェアの種類を指定します。 スパイウェアの処理を指定します (隔離、削除、または放置)。 POP3 検索時にスパイウェアが検出されると、選択された受信者へ自動的に通知されます。
コンテンツフィルタ	POP3 サーバを介してネットワークで受信される情報のリアルタイム監視および管理を実行します。	POP3 のコンテンツフィルタを有効または無効にします。 キーワードと添付ファイルフィルタを指定し、メールメッセージの内容自体に基づいてメッセージの配信を評価および制御します。
設定	InterScan VirusWall の POP3 プロキシサーバで POP3 トラフィックを処理する方法を設定できます。	InterScan VirusWall POP3 プロキシサーバのバインド先の POP3 IP アドレスを指定します。 許可するローカル同時接続数、POP3 クライアントが InterScan VirusWall への接続に使用するポート (初期設定のポートは 110)、および安全なパスワード認証の設定を指定します。

[大規模感染予防] メニュー

トレンドマイクロは、脅威を防止し、同時に TrendLabs でその対策を開発するトレンドマイクロ 大規模感染予防サービス (以下、大規模感染予防サービス) を提供しています。

図 4-4.　[大規模感染予防 - 現在の接続状況] 画面

表 4-6.　[大規模感染予防] のサブメニュー項目

サブメニュー	説明	タスク
ステータス	[大規模感染予防] の実施を通知します。	大規模感染予防を有効または無効にします。 大規模感染予防ステータスを表示します。
設定	大規模感染予防設定を表示および変更できます。	大規模感染予防ポリシーの有効期限の初期設定を手動で変更します。

大規模感染予防サービスの詳しい説明については、「Trend Micro InterScan VirusWall スタンダードエディション リファレンスマニュアル」を参照してください。

[管理] メニュー

[管理] メニュー項目を使用すると、InterScan VirusWall インストールの Control Manager 設定、通知設定、パスワード、ライセンス、およびプロキシ設定を管理できます。

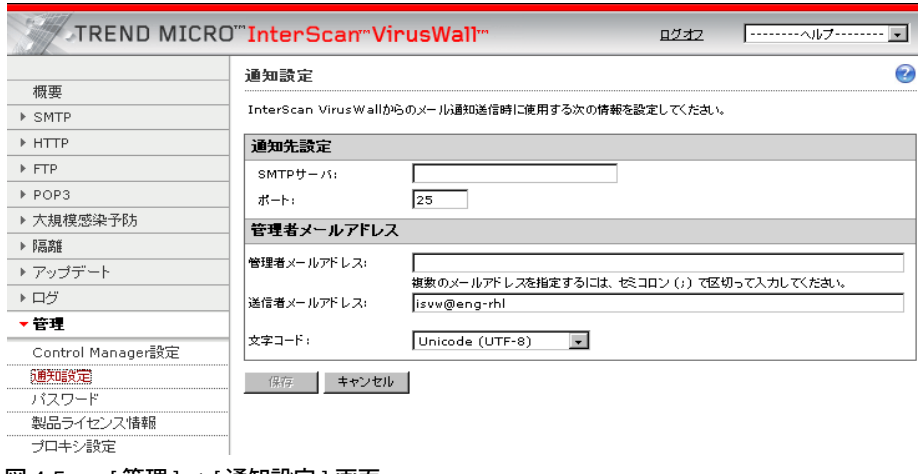


図 4-5.　[管理] → [通知設定] 画面

[管理] のサブメニューは、以下のようなさまざまな目的に使用できます。

- InterScan VirusWall で管理者通知を送信できるようにメールサーバおよびメールアドレス情報を提供します。
- 管理者パスワードを変更します。
- 製品をアクティベートする、または製品ライセンスを更新します。
- プロキシ設定を変更します。

表 4-7. [管理] のサブメニュー項目

サブメニュー	説明	タスク
Control Manager 設定	管理者が Control Manager サーバより管理コンソールを使用して、InterScan VirusWall を管理できるようにします。	Control Manager サーバへの InterScan VirusWall の登録または登録解除を行います。 InterScan VirusWall を Control Manager サーバに登録するための設定を指定します。
通知設定	InterScan VirusWall からメール通知を送信するときに使用する設定を指定します。	以下の設定を指定します。 ・ SMTP サーバ ・ ポート ・ 管理者のメールアドレス ・ 通知の受信に使用する文字コード
パスワード	InterScan VirusWall へのログオンに使用するパスワードを変更できます。	古いパスワード、新しいパスワード、および新しいパスワードの確認を指定して現在のパスワードを変更します。
製品ライセンス情報	InterScan VirusWall のサポート契約と製品ライセンスに関する情報を表示します。	ライセンスのアップグレードの指示を表示します。 ライセンス情報をオンラインで表示します。 新しいアクティベーションコードを入力します。 画面上の情報をアップデートします。
プロキシ設定	プロキシサーバを使用してインターネットに接続する場合は、パターンファイル、エンジン、およびライセンスのアップデートに使用する設定を指定できます。	プロキシサーバを有効または無効にします。 プロキシ設定を指定します。 接続をテストします。

InterScan VirusWall を起動 / 停止する

初期設定では、インストールの完了後、インストール時に選択した InterScan VirusWall のすべてのサービスが自動的に開始されます。Web コンソールの [概要] 画面から各サービスを個別に有効または無効にできます。

設定ファイルを変更し、その変更を有効にしたい場合などの特定の状況では、すべてのサービスを同時に再起動することを推奨します。

すべてのサービスを再起動するには

1. InterScan VirusWall のインスタンスを配置するコンピュータに root としてログオンします。
2. 以下のコマンドを実行します。

   ```
   # /etc/init.d/isvw6 restart
   ```

   Linux コンピュータはすべての InterScan VirusWall サービスを停止して再起動します。また、コマンドラインからメインの InterScan VirusWall サービスを停止できます。

InterScan VirusWall サービスを停止するには

1. InterScan VirusWall のインスタンスを配置するコンピュータに root としてログオンします。
2. 以下のコマンドを実行します。

   ```
   # /etc/init.d/isvw6 stop
   ```

   InterScan VirusWall サービスが停止します。

警告： InterScan VirusWall サービスを停止した場合は、InterScan VirusWall はネットワークトラフィックを検索しません。

InterScan VirusWall をテストする

インストールの完了後は、設定に習熟し、プログラムの仕組みを理解するために InterScan VirusWall のインストールをテストします。このセクションでは、ウイルス対策とコンテンツフィルタの機能をテストする操作手順を示します。

EICAR テストウイルスを使用したウイルス対策のテスト

EICAR (European Institute for Computer Antivirus Research) は、テスト「ウイルス」を開発しました。このテストウイルスを使用すると、InterScan VirusWall のインストールと設定をテストできます。このテストウイルスは実際には活動しないテキストファイルであり、そのバイナリパターンは大部分のウイルス対策ベンダのウイルスパターンファイルに組み込まれています。このファイルはウイルスではありません。このファイルにプログラムコードは含まれていないので、テストウイルスが危害を加えたり、増殖したりすることはありません。

コンピュータ上に EICAR テストウイルスを置いて使用すると、ウイルス感染をシミュレートできます。これにより、InterScan VirusWall のウイルス駆除 / 削除機能を確認できます。InterScan VirusWall は、EICAR テストファイル、ZIP 形式の EICAR テストファイル、および 2 回 ZIP された EICAR テストファイルに対して処理を実行します。インシデントは SMTP ウイルスログに記録されます。

次のセクションでは、SMTP VirusWall のウイルス対策機能をテストします。SMTP VirusWall のテストに習熟したら、他のプロトコルの検索サービス (HTTP VirusWall、FTP VirusWall、および POP3 VirusWall) に進んでテストを行えます。

テストウイルスを入手するには

- 以下の URL からファイルをダウンロードします。
  - http://www.trendmicro.co.jp/download/test-virus.asp
  - http://www.eicar.org/anti_virus_test_file_htm

注意： ZIP 形式の EICAR テストファイル (eicar_com.zip) と 2 回 ZIP された EICAR テストファイル (eicarcom2.zip) は、EICAR の Web サイトからダウンロードすることもできます。

または

- 次の文字列をテキストファイルに入力し、独自の EICAR テストウイルスを作成して eicar.com と命名します。

  X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

EICAR テストウイルスを使用して InterScan VirusWall をテストするには

1. eicar.com、eicar_com.zip、および eicarcom2.zip の各ファイルを添付したメールメッセージを送信します。メール送信用に指定したメールクライアントを使用します。
2. このメールを受信します。メール受信用に指定したメールクライアントまたはこれに相当するクライアントを使用します。

   添付ファイルを開くと、そのファイルは駆除できないために削除したことを知らせるメッセージが表示されます。
3. SMTP ウイルスログを確認します。

   a. Web コンソールを開いて [ログ]→[クエリ] の順にクリックします。[ログクエリ] 画面が表示されます。

   b. 以下のドロップダウンメニューの設定を選択します。
      - プロトコル : SMTP
      - ログの種類 : ウイルス / 不正プログラム

- 期間 : すべて

c. [ログ表示] をクリックします。[SMTP ウイルスログ] 画面が表示されます。

d. テストウイルスログのエントリの詳細を確認します。

コンテンツフィルタをテストする

ブロックのトリガとして設定したキーワードを件名やメールの本文に含むメールメッセージを送信することにより、SMTP のコンテンツフィルタ機能をテストします。SMTP VirusWall は、メッセージを隔離し、SMTP キーワードフィルタログにインシデントを記録します。

注意 : SMTP のコンテンツフィルタのテストが完了したら、同じ方法を使用して、POP3 のコンテンツフィルタ機能をテストできます。

コンテンツフィルタ機能をテストするには

1. Web コンソールで、[SMTP]→[コンテンツフィルタ] の順にクリックします。[対象] タブで [キーワード] セクションに移動し、任意のキーワードを入力して [追加] をクリックします。InterScan VirusWall によりキーワードが右側のリストに追加されます。
2. 件名と本文に手順 1 のキーワードを含むメールメッセージを送信します。メール送信用に指定したメールクライアントまたはこれに相当するクライアントを使用します。
3. このメールメッセージを受信します。メール受信用に指定したメールクライアントまたはこれに相当するクライアントを使用します。

   このメールはフィルタ処理されたために表示されません。
4. SMTP キーワードフィルタログを確認します。

   a. Web コンソールを開いて [ログ]→[クエリ] の順にクリックします。[ログクエリ] 画面が表示されます。

   b. 以下のポップアップメニューの設定を選択します。

      - プロトコル : SMTP

- ログの種類 : キーワードフィルタ
- 期間 : すべて

c. [ログ表示] をクリックします。[SMTP キーワードフィルタログ] 画面が表示されます。

d. コンテンツフィルタのログエントリの詳細、特に手順 1 のキーワードを含む [件名] 列のエントリの詳細を確認します。

5. InterScan VirusWall に対して隔離のクエリを実行します。

a. Web コンソールで [隔離]→[クエリ] の順にクリックします。[隔離クエリ] 画面が表示されます。

b. テストメールを送信した日付、手順 1 の送信者のメールアドレス、手順 2 の受信者のメールアドレス、件名としての手順 1 のキーワードを [条件] で入力することにより、クエリの範囲を限定します。

c. [クエリ] をクリックします。

[クエリ結果] パネルに、メールが隔離された日時、送信者と受信者のメールアドレス、メールの件名、メールが隔離された理由が表示されます。

リアルタイムパフォーマンスモニタを使用する

InterScan VirusWall にはコマンドラインのパフォーマンスモニタツールが付属しています。このツールを使用すると、SMTP、HTTP、および POP3 プロトコルのプロセス数、スレッド数、接続数、プロセス開始時刻、および 1 分あたりの要求数を表示できます。FTP では、パフォーマンスモニタを使用すると、マスタプロセス ID、下位プロセス数、開始時刻、および下位プロセスの次の情報を表示できます。

- 有効な接続数
- 利用可能な接続数
- 1 分あたりの検索ファイル
- 下位プロセスの開始時刻

パフォーマンスモニタを開始するには

1. InterScan VirusWall のインスタンスがインストールされているコンピュータに root としてログオンします。
2. InterScan VirusWall インストールディレクトリの「perform」サブディレクトリに移動します。たとえば、初期設定のインストールパスを使用している場合は、以下に表示されるパスになります。

   ```
   /opt/trend/isvw/perform
   ```

3. ls コマンドを実行して、正しいディレクトリであることを確認します。ファイルリストに isvw-perform ファイルが表示された場合は、正しいディレクトリです。
4. パフォーマンスモニタを開始するには、次のコマンドを実行します。

   ```
   # watch "./isvw-perform"
   ```

5. パフォーマンスモニタを停止するには、<Ctrl>+<c> キーを押します。

パフォーマンスモニタが読み込まれます。図 4-6 に、パフォーマンスモニタの出力例を示します。

```
                    *** InterScan VirusWall - Performance Monitor ***

*** SMTP/POP3/HTTP Services ***

Service      Process   Threads   Connections   Requests      Start Time
             ID                                (per min.)
================================================================================
SMTP(on)  4267       20          0              0            06/27/06 18:09:03
POP3(on)  4268       20          0              0            06/27/06 18:09:03
HTTP(on)  4289       14          -              0            06/27/06 18:09:03


*** FTP Service ***

Service          Master          Child          Start Time
                  Process ID     Processes
================================================================================
FTP(on)          4303             2              06/27/06 18:09:02

Child            Active          Available      Scanned        Start Time
Process ID       Connections     Connections    Files(per min.)
================================================================================
14276            1               5              4              06/27/06 18:09:02
14277            1               5              0              06/27/06 18:10:48
--------------------------------------------------------------------------------------------------------------------------------
Total:           2               10             4
```

図 4-6.　パフォーマンスモニタの出力例

InterScan VirusWall コンポーネントをアップデートする

新しい不正プログラムや疑わしい不快な Web サイトは日々開発されて仕掛けられているため、InterScan VirusWall では、要望に応じた、または自動的なソフトウェアのアップデートを実施して、最新のパターンファイルや検索エンジン、URL フィルタデータベースを提供しています。その際、ネットワークサービスを中断したり、コンピュータを再起動したりする必要はありません。InterScan VirusWall では、これは、アップデートサーバに直接ポーリングし、アップデートを予定に従って、または手動でダウンロードすることによって実行されます。

注意： InterScan VirusWall をアクティベートしている場合、またはその製品が 30 日の体験期間である場合にのみ、コンポーネントをアップデートできます。

新しいウイルスやその他のインターネットの脅威が作成されたり、一般にリリースされたり、検出されたりすると、トレンドマイクロは証拠となるシグニチャを収集し、その情報をウイルスおよびその他のパターンファイルに組み込みます。

トレンドマイクロは週に数回ファイルをアップデートします。また、広範囲な脅威の変種が複数リリースされた場合には、1 日に数回ファイルをアップデートします。初期設定では、InterScan VirusWall は 1 週間に最低 1 回アップデートを確認します。特に障害を与えるウイルスが一般に検出されたり、または活発に循環している場合は、トレンドマイクロでは、その脅威の検出手順が利用可能になるとすぐに (通常、2 ～ 3 時間以内) 新しいパターンファイルをリリースします。

アップデートのサブメニュー

左側のメニューでは、[アップデート] に 2 つのサブメニューがあります。製品をインストールした直後、または必要に応じて InterScan VirusWall コンポーネントを適宜アップデートするには、[手動アップデート] を使用します。InterScan VirusWall コンポーネントを自動アップデートするために予定を設定するには、[予約アップデート] を使用します。

表 4-8. [アップデート] のサブメニュー

サブメニュー	説明	タスク
手動アップデート	必要に応じてコンポーネントをアップデートします。	アップデートするコンポーネントを選択します。 選択したコンポーネントを以前のアップデートにロールバックします。
予約アップデート	InterScan VirusWall コンポーネントの定期的なアップデートを予約します。	予約アップデート機能を有効または無効にします。 アップデートするコンポーネントを選択します。 予約アップデートを設定します。

アップデートできるコンポーネント

表 4-9 では、アップデートできる 7 種類の InterScan VirusWall コンポーネントを表示して説明します。

表 4-9. InterScan VirusWall がアップデートできるコンポーネント

コンポーネント	説明	ファイル例
ウイルスパターンファイル	トレンドマイクロで既知であるウイルス / 不正プログラムの最新パターンのコレクションです。	lpt$vpn.755
ウイルス検索エンジン	ウイルス検索エンジンは、ウイルス / 不正プログラム検索を実行するコンポーネントです。ロールバック機能は検索エンジンに適用されません。	libvsapi.so

表 4-9. InterScan VirusWall がアップデートできるコンポーネント (続き)

コンポーネント		説明	ファイル例
フィッシングパターンファイル		トレンドマイクロで既知になっているフィッシングサイトの最新のリストです。	PhishB.ini
IntelliTrap パターンファイル			
	禁止リスト (IntelliTrap パターンファイル)	圧縮ファイル内の不正プログラムの最新のパターンリストです。	Tmblack.101
	許可リスト (IntelliTrap 除外パターンファイル)	不正プログラムを含まない圧縮ファイルの最新のリストです (除外リスト)。	Tmwhite.102
スパイウェアパターンファイル		トレンドマイクロで既知であるスパイウェア / グレーウェアプログラムの最新パターンのコレクションです。	tmaptn.275
スパムメール判定ルール / スパムメール検索エンジン			
	全体ルール	最新のスパムメール判定ルールです。	tm013974.rul tm013974.sig tm013974.phi tm013974.hsh tm013974.exp
	差分ルール	最新のスパムメール判定ルールの差分アップデートです (105 ページの「差分アップデートと全体アップデート」を参照)。	tm013972.sig tm013972.phi tm013972-000001.hsh tm013972.exp
	エンジン	最新のスパムメール検索エンジンです。	libtmaseng.so
URL フィルタデータベース			
	全体データベース	フィルタのカテゴリに関連する可能性のある URL の最新の全体データベースです。	ratings.rat
	差分データベース (差分アップデート)	フィルタのカテゴリに関連する可能性のある URL のデータベースの最新の差分アップデートです。	ratings.tst

差分アップデートと全体アップデート

アップデートは、多くのトレンドマイクロ製品に共通の機能です。トレンドマイクロのアップデート Web サイトに接続すると、アップデートによって、ウイルスパターンファイル、検索エンジン、プログラムファイルの最新のダウンロードがインターネット経由で提供されます。

アップデートでは、スパムメール判定ルールおよび URL フィルタデータベースの差分アップデートがサポートされます。アップデートは、ファイル全体を毎回ダウンロードする代わりに、パターンファイルの新規部分のみをダウンロードして、既存のコンポーネントファイルに追加できます。この効率的なアップデート方法により、InterScan VirusWall の配置をアップデートしてパターンファイルを環境全体に配信するために必要な帯域幅を大幅に低減できます。

注意： 差分アップデートは設定またはロールバックできません。差分アップデートの時間、日付、およびパターン番号情報は、参照用にのみ表示されます。

コンポーネントを手動でアップデートする

コンポーネントを手動でアップデートするには、次の 2 つの方法があります。

- [手動アップデート] 画面でのアップデート
- [概要] 画面でのアップデート

手動アップデート機能を使用する

左側のメニューから [アップデート]→[手動アップデート] の順に選択して、[手動アップデート] 画面を表示します。以下の図 4-7 に示すように、利用可能な新しいパターンファイルの番号が赤字で Web コンソールに表示されます。

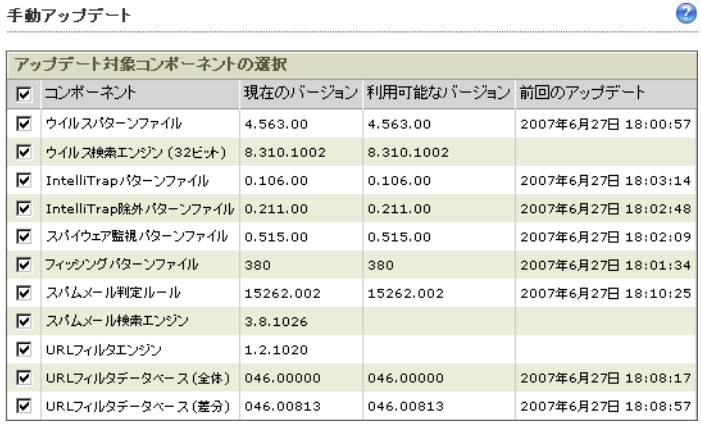


図 4-7.　2 つの期限切れコンポーネントが示されている [手動アップデート] 画面の詳細

すべての期限切れコンポーネントをアップデートする

初期設定では、[手動アップデート] ページの読み込み時に、すべてのコンポーネントのチェックボックスがオンになっています。期限切れになったコンポーネント、つまり、最後の列に赤い太字のパターンバージョン番号を持つコンポーネントをアップデートするには、単に [アップデート] をクリックします。チェックボックスをオフにする必要はありません。

パターンをロールバックする

[手動アップデート] 画面ではまた、パターンがある種の問題の原因となりうる場合に、パターンをロールバックできます。一度にロールバックできるのは 1 つのパターンだけです。

注意： ロールバックできるのはパターンファイルだけです。エンジンはロールバックできません。

パターンファイルを前のバージョンにロールバックするには

1. 左側のメニューから [アップデート]→[手動アップデート] の順に選択します。[手動アップデート] 画面が表示されます。
2. ロールバックするパターンを除き、すべてのコンポーネントをオフにします (コンポーネント列のヘッダの左側にあるテーブル上部のチェックボックスをオフにすると、すべてのコンポーネントを同時にオフにできる)。
3. ロールバックするパターンが 1 つだけオンになっていることを確認した後、[ロールバック] をクリックします。そのパターンが前のバージョンにロールバックされます。

[概要] 画面を使用してコンポーネントを表示およびアップデートする

コンポーネントを手動でアップデートする 2 番目の方法は、[概要] 画面からアップデートする方法です。この手順は、[手動アップデート] 画面からのアップデートで説明した手順ととてもよく似ています。 [手動アップデート] 画面のように、[概要] 画面にもアップデート機能とロールバック機能がありますが、これらの機能のボタンはセクションの上部に表示されます。

図 4-8「[概要] 画面 (上) と [手動アップデート] 画面 (下) でのコンポーネントアップデートセクションの比較」で示されるように、主な違いは 2 つの画面のテーブルの表示と画面の構成方法です。

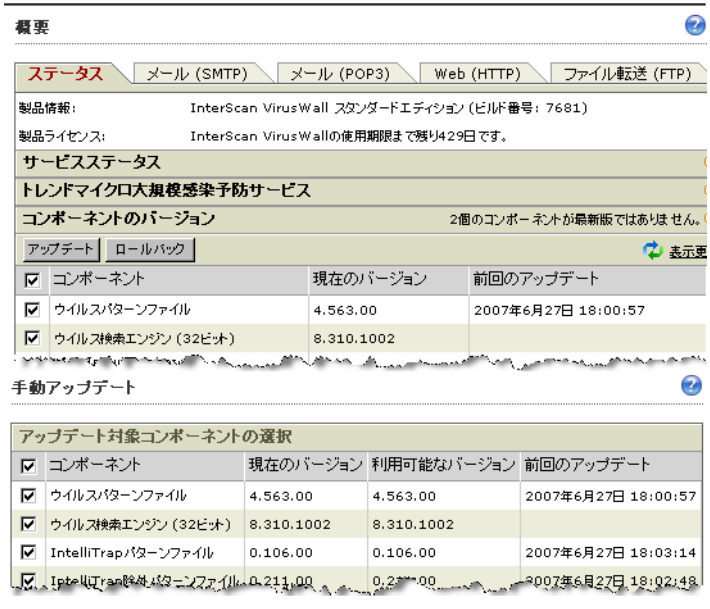


図 4-8. [概要] 画面 (上) と [手動アップデート] 画面 (下) でのコンポーネントアップデートセクションの比較

[概要] 画面からコンポーネントを手動でアップデートするには

1. 左側のメニューで [概要] を選択します。[概要] 画面が表示されます。
2. [コンポーネントのバージョン] が開いていない場合は、そのセクションの展開 / 折り畳みアイコン ( ) をクリックします。[コンポーネントのバージョン] が開くと、アップデートが必要なすべてのコンポーネントのバージョン番号が黒の太字フォントで表示されています。
3. アップデートするコンポーネントを選択して [アップデート] をクリックします。InterScan VirusWall で手動アップデートが実行されます。

[概要] 画面でパターンをロールバックする手順は、[手動アップデート] 画面の手順と同じです (107 ページの「パターンをロールバックする」を参照)。2 つの画面間の表示の主な違いは [ロールバック] ボタンの場所です。

アップデートを予約する

コンポーネントをアップデートする 2 番目の方法は、自動アップデートするためのに予定を設定することです。より厳密に言えば、アップデートを自動的に確認することです。InterScan VirusWall は定期的にアップデートサーバに接続して、コンポーネントのいずれかでアップデートが必要かどうか、つまり期限切れであるかどうかを確認します。いずれかのコンポーネントでアップデートが必要な場合には、予約アップデート機能によってアップデートが実行されます。

自動アップデートを予約するには

1. 左側のメニューで [アップデート]→[予約アップデート] の順に選択します。[予約アップデート] 画面が表示されます。
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. 自動アップデートを実行するコンポーネントを選択します。

ヒント： トレンドマイクロでは、7 種類すべてのアップデートを選択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、自動アップデートチェックの頻度と時間を選択します。頻度に関するオプションは次のとおりです。

   - 分
   - 時間
   - 日
   - 曜日

   これらのオプションの右フィールドは動的に設定されます。左側で行った選択と一致する適切なオプションを反映するために変更されます。表 4-10 には、頻度のさまざまなオプションに対する右側オプションの表示が示されます。

表 4-10. 頻度とアップデート時間に関する予約アップデートのオプション

頻度オプション	右側のオプション
分	15 分
時間	1 時間
日	1 日ごと 00 : 00 (hh:mm)
曜日	日曜日 00 : 00 (hh:mm)

5. [保存] をクリックします。

ヒント：帯域幅に対する要求が低い期間中に、自動アップデートを設定して実行することをお勧めします。

アップデートを使用するために InterScan VirusWall を設定する

予約アップデートを設定すると、主要なトレンドマイクロのアップデートサーバと通信したり、またはプロキシサーバ経由で通信したりできます。プロキシサーバを使用している場合は、以下の手順に従って、そのサーバ経由で自動アップデートを行うために InterScan VirusWall を設定できます。

InterScan VirusWall を設定してプロキシサーバ経由でアップデートにアクセスするには

1. 左側のメニューで [管理]→[プロキシ設定] の順に選択します。[プロキシ設定] 画面が表示されます。
2. [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] の横のチェックボックスをオンにします。その他のフィールドが選択できるようになります。
3. 次のオプションからプロキシプロトコルを選択します。
   - HTTP
   - SOCKS4
   - SOCKS5
4. [ホスト名 /IP アドレス] に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。
5. ポートフィールドでポートを変更するか、初期設定の 8080 をそのまま使用します。
6. プロキシサーバで認証を使用している場合は、[プロキシサーバの認証] の該当するフィールドにユーザ ID およびパスワードを入力します。
7. InterScan VirusWall に必要なアカウント情報がすべてあることを確認するために、[接続のテスト] をクリックして認証をテストします。InterScan VirusWall は、認証を使用してサーバに接続できることを確認します。
8. [保存] をクリックします。

通知設定

あらゆるタイプの通知を送信する前に、InterScan VirusWall は、メールサーバを使用するためにメールサーバに関する必要な情報を設定する必要があります。この設定は以下の 2 つの方法で実施できます。

- インストール中 (48 ページの「通知設定」を参照)
- Web コンソール経由

Web コンソールで通知に関するメールサーバ情報を提供するには

1. 左側のメニューで [管理]→[通知設定] の順に選択します。[通知設定] 画面が表示されます。
2. [設定] にメールサーバのホスト名または IP アドレスを入力します。
3. [管理者メールアドレス] に管理通知を受信する人物のメールアドレスを入力します (複数のエントリを入力する場合はセミコロン (;) で区切る)。
4. [送信者メールアドレス] に通知の送信者として使用する InterScan VirusWall のメールアドレスを入力します (たとえば、interscan_viruswall@< ドメイン名 >)。
5. 最後に、[文字コード] ドロップダウンメニューから文字コードを選択します。InterScan VirusWall では、この文字セットをテキスト形式のメールに使用します。
6. [保存] をクリックします。

パスワードの管理

最低 90 日に 1 回の頻度でパスワードを変更すると効果的です。Web コンソールにログオンするために必要な管理者パスワードを Web コンソールから変更できます。

管理者パスワードを変更するには

1. 左側のメニューで [管理]→[パスワード] の順に選択します。[パスワードの設定] 画面が表示されます。
2. [現在のパスワード] に現在のパスワードを入力します。
3. [新しいパスワード] に新しいパスワードを入力し、[パスワードの確認入力] にそのパスワードを再度入力します。

4. [保存] をクリックします。以下の条件を確認するためにパスワードが評価されます。

   - [現在のパスワード] のパスワードが、正しい現在のパスワードであること
   - [新しいパスワード] と [パスワードの確認入力] に入力されたパスワードが一致すること
   - 新しいパスワードの長さが最低 4 文字の英数字であり、32 文字を超えないこと

   新しいパスワードが前述の条件またはその他の InterScan VirusWall セキュリティ条件を満たしていない場合には、エラーメッセージが表示されます。すべての条件が満たされている場合は、確認メッセージが表示されます。

第 5 章

トラブルシューティングとサポート

この章では、Trend Micro InterScan VirusWall スタンダードエディション (以下、InterScan VirusWall) のインストール時、設定時、または使用開始時に発生する問題の解決に役立つ情報を提供します。

この章では、以下のトピックについて説明します。

- 117 ページの「インストールと移行」
- 122 ページの「ライセンスとアクティベーション」
- 123 ページの「ユーザインタフェース」
- 125 ページの「よくある質問」
- 126 ページの「隔離」
- 134 ページの「ログを用いたセキュリティインシデントの分析」
- 143 ページの「製品サポート情報」
- 143 ページの「サポートサービスについて」
- 144 ページの「製品 Q&A のご案内」
- 145 ページの「セキュリティ情報」
- 146 ページの「ウイルス解析サポートセンター「TrendLabs」」

概要

問題がこの章の問題リストに記載されていない場合は、使用するプロトコルの設定ガイドを参照してください。設定ガイドは、次のとおりです。

- Trend Micro InterScan VirusWall スタンダードエディション SMTP 設定ガイド
- Trend Micro InterScan VirusWall スタンダードエディション HTTP 設定ガイド
- Trend Micro InterScan VirusWall スタンダードエディション FTP/POP3 設定ガイド

さらに支援を必要とする場合は、143 ページの「製品サポート情報」を参照してください。

トラブルシューティング

インストールと移行、ライセンスとアクティベーション、およびユーザインタフェースに関するトラブルシューティングの詳細については、以下の表を参照してください。

インストールと移行

表 5-1. インストールと移行に関するトラブルシューティング

問題	説明、考えられる原因、対策
インストールに失敗する	・ システム要件を満たしていません。34 ページの「システム要件」を参照してください。 　・ OS のバージョンや Service Pack が要件を満たしていない場合は、インストールを続行できません。 　・ インストール先ディスクの空き領域が不足しています。InterScan VirusWall をインストールするハードディスクには最低 2GB の空き領域が必要です。空き領域を増やすか、十分なディスク領域があるサーバに InterScan VirusWall をインストールしてください。 ・ バージョン 3.8x 以外の InterScan VirusWall の前バージョンがすでにインストールされています。最初に InterScan VirusWall をアンインストールしてから、セットアップをもう一度実行します。 ・ InterScan VirusWall のインストールに必要な権限がありません。管理者権限でログオンしてインストールを実行してください。 ・ 他のアプリケーションが必要なポートを使用しています。# netstat -an コマンドを実行すると、使用中のすべてのポートが表示されます。 ・ これらの要件を満たしていてもインストールに失敗する場合は、トレンドマイクロのサポートにお問い合わせください。

表 5-1.　インストールと移行に関するトラブルシューティング (続き)

問題	説明、考えられる原因、対策
Postfix の問題 RBL (リアルタイムブラックホールリスト) などの Postfix の高度な機能を利用していますが、InterScan VirusWall と同じコンピュータで Postfix を使用すると問題が発生します。	環境が以下であると仮定します。 インターネット→ InterScan VirusWall → Exchange サーバ →クライアント (受信) クライアント→ Exchange サーバ→ InterScan VirusWall → インターネット (送信) 1. SMTP VirusWall が配置されているコンピュータ上で Postfix の 2 つのインスタンスを開始します。インスタンスの 1 つは SMTP VirusWall の前に、もう 1 つは SMTP VirusWall の後です。 2. SMTP VirusWall がインストールされているコンピュータのトポロジは次のようにする必要があります。 Postfix → InterScan VirusWall → Postfix 3. このソリューションに SMTP VirusWall をインストールした後のユーザ環境は次のとおりです。 受信 : インターネット→ *Postfix (localhost/25) (RBL+ の使用) → InterScan VirusWall (localhost/10025) → Postfix (localhost/10026)* → Exchange サーバ→クライアント 送信 : クライアント→ Exchange (SmartHost から ISVW Port 10025) → *InterScan VirusWall (localhost/10025) → Postfix (localhost/10026)* →インターネット (下線付き部分は、DMZ 内の InterScan VirusWall サーバ)

表 5-1.　インストールと移行に関するトラブルシューティング (続き)

問題	説明、考えられる原因、対策
インストール中に設定を移行できない	・ InterScan VirusWall を新しいコンピュータにインストールするときに、InterScan VirusWall for UNIX 3.8x から設定を移行するために使用した設定ファイルが破損していた。 ・ InterScan VirusWall for UNIX 3.8x がインストールされているコンピュータで、設定ファイルを新規に生成します。生成の手順については、66 ページの「異なるコンピュータ上でバージョン 5.0 からアップグレードする」の手順 1 ～ 4 を参照してください。 ・ 新しいコンピュータに InterScan VirusWall を再度インストールします。前述のトピックの手順 5 ～ 18 を参照してください。 ・ InterScan VirusWall をインストールするコンピュータに、InterScan VirusWall 3.8x のインスタンスが不適切にインストールされています。 ・ InterScan VirusWall をインストールするコンピュータで設定ファイルを生成します。66 ページの「異なるコンピュータ上でバージョン 5.0 からアップグレードする」の手順 1 ～ 3 を参照してください。 ・ このコンピュータに InterScan VirusWall を再度インストールします。InterScan VirusWall を再インストールする手順については、58 ページの「同じコンピュータ上でバージョン 3.8x からアップグレードする」を参照してください。 ・ これらの手順に従っても移行に失敗する場合は、トレンドマイクロのサポートにお問い合わせください。
インストール直後に CPU 使用率が 100% になる	これは正常な現象であり、InterScan VirusWall を正しく実行する前に、検索エンジン、スパムメール対策エンジン、設定ファイル、ログファイル、読み込みパターンなどのコンポーネントの初期化が必要なために発生します。 推奨環境の場合、初期化は数分で完了します (34 ページの「システム要件」を参照)。その後、CPU の使用率は正常な状態に戻ります。

表 5-1.　インストールと移行に関するトラブルシューティング (続き)

問題	説明、考えられる原因、対策
サービスを開始 / 停止できない	サービスを停止できない場合は、95 ページの「InterScan VirusWall を起動 / 停止する」の手順に従ってください。この手順の実行後にサービスを開始または停止できない場合は、トレンドマイクロのテクニカルサポートにお問い合わせください。
同じコンピュータ上の ServerProtect との互換性の問題	InterScan VirusWall のインスタンスをインストールする同じコンピュータに Trend Micro ServerProtect for Linux 2.5 (以下、ServerProtect) をインストールしている場合は、ServerProtect が InterScan VirusWall をブロックしないように ServerProtect のリアルタイム検索除外リストに InterScan VirusWall を追加する必要があります。 ServerProtect のリアルタイム検索除外リストに InterScan VirusWall を追加するには 1. ServerProtect の Web コンソールを開きます。 2. ServerProtect の Web コンソールの左側のメニューで [Scan Options] → [Exclusion List] の順に選択します。[Exclusion List - Real-time Scan] 画面が表示されます (以下の図 5-1 を参照)。 3. [Input directory path] に InterScan VirusWall インストールのインストールディレクトリを入力します。 4. 追加ボタン (>>) をクリックします。InterScan VirusWall インストールディレクトリパスが、右の [Directories to exclude] に表示されます。 5. 画面の下部にある [Save] をクリックします。

表 5-1.　インストールと移行に関するトラブルシューティング (続き)

問題	説明、考えられる原因、対策

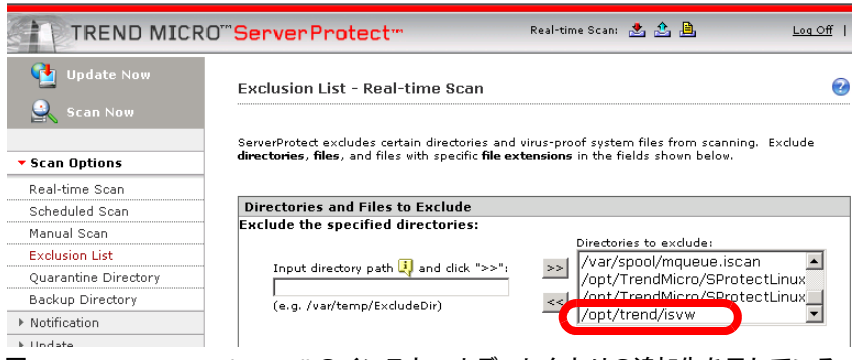


図 5-1.　InterScan VirusWall のインストールディレクトリの追加先を示している ServerProtect の [Exclusion List - Real-time Scan] 画面

ライセンスとアクティベーション

表 5-2. ライセンスとアクティベーションに関するトラブルシューティング

問題	説明、考えられる原因、対策
ライセンスをアップデートできない	・ ライセンスをアップデートする前に製品をアクティベートしてください。 ・ 体験版の InterScan VirusWall を使用してライセンスをアップデートすることはできません。 ・ バックエンドのライセンスのオンラインアップデートサーバでシステムまたはプログラムの例外エラーが発生する場合は、数分待ってから再試行してください。問題が解決しない場合は、トレンドマイクロのテクニカルサポートにお問い合わせください。 ・ 「Config.xml¥Common¥ProductRegistration¥OnLineUpdate¥Server¥Source」に保存された不適切なサーバ URL が原因でライセンスをアップデートできない場合は、設定をチェックしてから再試行してください。 ・ 使用しているアクティベーションコードがオンラインアップデートのライセンスサーバにない場合は、有効なアクティベーションコードを入力してから再試行してください。 ・ ライセンスをオンラインでアップデートできない場合は、ネットワークの状態を確認してください。プロキシサーバを使用している場合は、そのプロキシサーバが製品登録サーバに接続できるかどうかをチェックしてください。問題が解決しない場合は、トレンドマイクロのテクニカルサポートにお問い合わせください。
アクティベーションに関する問題	・ 以下の理由により、無効なアクティベーションコードを使用しています。 　・ 製品版または体験版のアクティベーションコードを使用して、製品をすでにアクティベートしている可能性があります。 　・ 使用している体験版または製品版のアクティベーションコードが失効しています。 　・ 製品版をインストールした場合、体験版のアクティベーションコードを使用した可能性があります。その逆も考えられます。 ・ 引き続きアクティベーションに失敗する場合は、トレンドマイクロのサポートにお問い合わせください。

ユーザインタフェース

表 5-3.　ユーザインタフェースに関するトラブルシューティング

問題	説明、考えられる原因、対策
テキストボックスに日本語を入力した後に Web コンソールが正しく表示されない	ブラウザのエンコードをチェックしてください。Internet Explorer では、[表示]→[エンコード] の順にクリックして [Unicode (UTF-8)] を選択すると、Web コンソールで日本語などの 2 バイト文字を正しく表示できます。
Web コンソールが開かない	InterScan VirusWall がインストールされているコンピュータをチェックします。クエリキャッシュファイルのために十分な空き領域が確保されていることを確認してください。
Web コンソールの管理者パスワードを忘れた	・ トレンドマイクロのテクニカルサポートへ連絡して、パスワードの再設定を要請してください。 ・ テクニカルサポートを受けることができるのは、登録済みのお客さまに限られます。ご使用の InterScan VirusWall が登録されていない場合は、パスワードを回復できません。

IP 変換に関連する URL ブロックの問題	・ 初期設定では、たとえば www.badsite.com などのドメイン名でサイトをブロックする場合、InterScan VirusWall はドメインを IP アドレスに変換してその情報を格納するため、ユーザはその IP アドレスでサイトにアクセスできません。しかし、この機能によってネットワークの負荷が増える可能性があります。
	ドメイン名のみでサイトをブロックする場合は、設定ファイル Config.xml でオプションの 1 つを変更できます。次の例のように、Config.xml はインストールディレクトリに配置されています。
	/opt/trend/isvw/Config.xml
	ドメインから IP への変換機能を無効にするには、Config.xml の次の行を編集してください。
	`<Value Name="ip_translate" string="yes" type="string" int="0" />`
	この行を次のように変更します。
	`<Value Name="ip_translate" string="no" type="string" int="0" />`

表 5-3.　ユーザインタフェースに関するトラブルシューティング (続き)

問題	説明、考えられる原因、対策
InterScan VirusWall コンピュータ上の DNS での変更に関連する HTTP 検索の問題	InterScan VirusWall がインストールされているコンピュータ上で管理者が DNS 設定を変更した場合は、HTTP VirusWall サービスは動作を停止します。 サービスを再び開始するには 1. 左側のメニューで [概要] を選択します。[概要] 画面が表示されます。 2. [概要] 画面の [Web (HTTP)] タブで [HTTP トラフィックを有効にする] チェックボックスをオフにし、再びオンにします。
HTTP 待機ポートの変更における遅延	・ SMTP では、待機ポートを変更した場合、ただちに設定が適用されます。ただし、HTTP では、わずかに遅延します。 ・ HTTP では、待機ポートを変更した場合、InterScan VirusWall が HTTP 検索タスクを強制終了して再起動するように、HTTP 検索タスクによって要求されます。このタスクの再起動時にポート変更が適用されます。このプロセスには数秒かかりますが、どのような場合でも 1 分を超えることはありません。
アップデートが終了してはじめて HTTP で接続が受け入れられる	・ InterScan VirusWall で検索エンジンまたは URL フィルタデータベースのアップデートを実行する場合、このプロセスには数分かかる可能性があります。 ・ その間、HTTP プロセスでは接続を受け入れることができません。 ・ アップデートが完了してはじめて、HTTP プロセスで再び接続を受け入れることができます。 この理由から、ユーザに不便を感じさせないようにするために、Web トラフィックが絶対的に少ない期間中にこれら 2 つのコンポーネントのアップデートを予約することをお勧めします。

よくある質問

インストール

Q. InterScan VirusWall をリモートでインストールできますか。

A. いいえ。InterScan VirusWall のこのリリースでは、ローカルインストールのみがサポートされています。

Q. InterScan VirusWall では、サイレントインストールまたはコンポーネントインストールがサポートされていますか。

A. いいえ。このリリースでは、サイレントインストールまたはコンポーネントインストールはサポートされていません。

隔離

[隔離] メニューの画面を使用すると、InterScan VirusWall で隔離されたファイルを管理できます。これらの画面を使用すると、[クエリ] メニューでは、隔離フォルダに対してメールメッセージとファイルに関するクエリを実行できます。[設定] メニューでは、隔離ディレクトリパスを変更できます。[メンテナンス] メニューでは、隔離中の古いファイルを削除するための条件を設定できます。

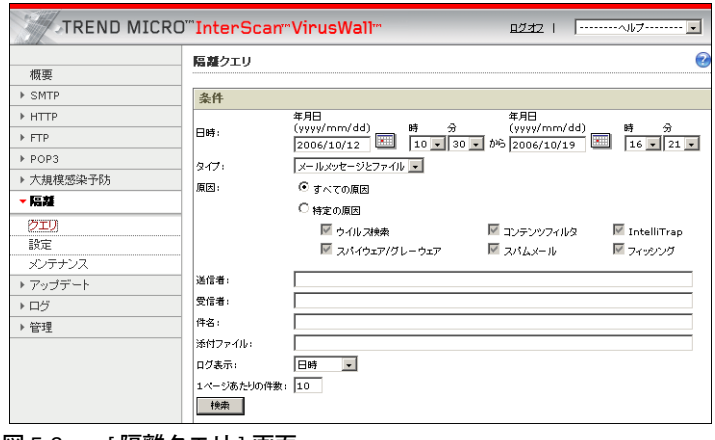


図 5-2.　[隔離クエリ] 画面

以下の表では、隔離サブメニューとそれぞれのサブメニューを使用して実行できるタスクを一覧表示しています。

表 5-4.　[隔離] のサブメニュー項目

サブメニュー	説明	タスク
クエリ	SMTP/POP3 の隔離されたメールメッセージおよび添付ファイルの詳細を確認できます。	日付、種類、理由、送信者、受信者、件名、および添付ファイルによってクエリ条件を指定します。 任意のクエリ条件でソート結果を並べ替えます。同時に、ページあたりのエントリ数を制限します。 隔離されたアイテムの管理 - 隔離されたメールを移動、削除、再送信、または再検索してから再送信します。 **注意：** InterScan VirusWall では、SMTP および POP3 隔離のみのクエリがサポートされます。
設定	隔離ディレクトリを変更できます。	SMTP、HTTP、POP3、および FTP の隔離対象を格納する隔離ディレクトリを変更します。
メンテナンス	削除するまで隔離ディレクトリに感染ファイルを格納している期間を指定できます。	隔離ファイルを削除します。 自動的に削除する時間を予約します。 **注意：** InterScan VirusWall では、SMTP および POP3 の隔離のみのクエリのメンテナンスがサポートされます。

隔離アイテムに対してクエリを実行する

InterScan VirusWall では、個別のプロトコルで処理を設定する場合に選択した設定に基づいて、後で検討するためにメールメッセージまたはファイルを隔離ディレクトリに移動できます。Web コンソールから SMTP および POP3 の隔離に対してクエリを実行できます。さらに、これらの 2 つの隔離を管理できます。

ヒント： このリリースでは、Web コンソールからの HTTP および FTP 隔離ディレクトリに対するクエリと管理がサポートされていません。ただし、HTTP および FTP の隔離に手動でアクセスして、コマンドラインでそれらのコンテンツを管理できます。

表 5-5 では、初期設定の隔離ディレクトリを隔離の種類別に一覧表示しています。

表 5-5. 隔離の種類別の初期設定の隔離ディレクトリパス

隔離の種類	初期設定のディレクトリパス
SMTP 検索	/opt/trend/isvw/quarantine/smtp
POP3 検索	/opt/trend/isvw/quarantine/pop3
HTTP 検索	/opt/trend/isvw/quarantine/http
FTP 検索	/opt/trend/isvw/quarantine/ftp

SMTP および POP3 の隔離に対して利用可能なクエリ条件

[隔離クエリ] 画面のクエリ定義フィールドを使用すると、クエリに次の条件を指定できます。

- 開始日時および終了日時 (分単位)
- タイプ :
  - メールメッセージ
  - メールメッセージとファイル
  - ファイル

- 原因 (InterScan VirusWall がそのアイテムを隔離する理由):
    - ウイルス検索
    - コンテンツフィルタ
    - IntelliTrap
    - スパイウェア / グレーウェア
    - スパムメール
    - フィッシング

隔離アイテムがメールメッセージまたは添付ファイルである場合に限り、次の条件が適用されます。

- 送信者
- 受信者
- 件名
- 添付ファイル

これらの条件に加えて、結果のソート順序を次のオプションから選択して指定できます。

- 日時
- 送信者
- 受信者
- 件名
- 原因
- プロトコル

また、表示する 1 ページあたりのエントリ数を指定できます (初期設定は 10)。

SMTP および POP3 の隔離ディレクトリのコンテンツに対してクエリを実行するには

1. 左側のメニューで [隔離]→[クエリ] の順に選択します。[隔離クエリ] 画面が表示されます。

2. ここで説明した条件フィールドのいずれかを選択して、クエリの条件を入力します。
3. [検索] をクリックします。InterScan VirusWall は、指定した条件を使用して隔離に対してクエリを実行し、画面の下部にある [クエリ結果] にクエリ結果のページを返します。

結果が複数ページにわたる場合には、ページ情報がリストの上部と下部に表示されます。矢印をクリックして、複数ページを移動します。列ヘッダのいずれかをクリックすると、結果テーブルで結果をソートできます。

隔離アイテムを移動または削除する

結果リストから 1 つまたは複数のアイテムを選択して、削除または移動できます。また、結果リストですべてのアイテムを選択して、削除または移動できます。

SMTP/POP3 隔離結果リストで 1 つまたは複数のアイテムを削除するには

1. 129 ページの「SMTP および POP3 の隔離ディレクトリのコンテンツに対してクエリを実行するには」に示すように隔離クエリを実行します。
2. 削除する 1 つまたは複数のアイテム横のチェックボックスをオンにします (結果リストの上部または下部のナビゲーションバーで [合計 x 件] チェックボックスをオンにすると、結果リストですべてのアイテムを選択できる)。
3. [削除] をクリックします。隔離で選択したすべてのアイテムが削除されます。

SMTP/POP3 隔離結果リストで 1 つまたは複数のアイテムを移動するには

1. 129 ページの「SMTP および POP3 の隔離ディレクトリのコンテンツに対してクエリを実行するには」に示すように隔離クエリを実行します。
2. 1 つまたは複数のアイテムを選択し、それらのアイテムの横のチェックボックスをオンにして移動します (結果リストの上部または下部のナビゲーションバーで [合計 x 件] チェックボックスをオンにすると、結果リストですべてのアイテムを選択できる)。
3. [移動] をクリックします。初期設定の移動ディレクトリが表示されている [隔離アイテムの移動] 画面が表示されます。

4. 初期設定の移動ディレクトリを必要なディレクトリと置き換えるか、または初期設定をそのまま使用します。
5. [移動] をクリックします。選択したアイテムが指定した場所に移動します (結果リストに戻るには [戻る] をクリック)。

隔離アイテムを再送信、または検索して再送信する

結果リストから 1 つまたは複数の項目を選択して再送信、または検索して再送信できます。また、結果リストですべての項目を選択して、削除または移動できます。

隔離した SMTP 項目または POP3 項目を再送信するには

1. 129 ページの「SMTP および POP3 の隔離ディレクトリのコンテンツに対してクエリを実行するには」に示すように隔離クエリを実行します。
2. 項目の横のチェックボックスをオンにして、再送信する項目を 1 つまたは複数選択します (結果リストの上部または下部のナビゲーションバーで [合計 x 件] チェックボックスをオンすると、結果リストにあるすべての項目を選択できます)。
3. [再送信] をクリックすると確認メッセージが表示されます。
4. [OK] をクリックします。

選択した項目が、元の受信者に送信されます。送信した項目は、クエリ結果画面には表示されなくなります。イベントログを表示し、再送信の処理結果を確認します。

隔離した SMTP 項目および POP3 項目を検索して再送信するには

1. 129 ページの「SMTP および POP3 の隔離ディレクトリのコンテンツに対してクエリを実行するには」に示すように隔離クエリを実行します。
2. 項目の横のチェックボックスをオンにして、検索して再送信する項目を 1 つまたは複数選択します (結果リストの上部または下部のナビゲーションバーで [合計 x 件] チェックボックスをオンすると、結果リストにあるすべての項目を選択できます)。
3. [検索および再送信] をクリックすると確認メッセージが表示されます。
4. [OK] をクリックします。

選択した項目が、検索されて再送信されます。送信した項目は、クエリ結果画面には表示されなくなります。イベントログを表示し、検索と再送信の処理結果を確認します。

注意： 再送信の処理または検索と再送信の処理に要する時間は、さまざまな要因に左右されます。たとえば、選択した項目の数、ネットワークの接続速度、InterScan VirusWall サーバの処理能力で変化します。

隔離ディレクトリパスを変更する

[隔離フォルダ設定] 画面の 4 つの隔離ディレクトリのいずれのパスも変更できます。

注意： この機能では、相対パスではなく、絶対パスのみがサポートされます。

1 つまたは複数の隔離ディレクトリのパスを変更するには

1. 左側のメニューで [隔離]→[設定] の順に選択します。SMTP、POP3、HTTP、および FTP の 4 つの各隔離ディレクトリごとに現在のパスを表示している [隔離フォルダ設定] 画面が表示されます。
2. 絶対パスを使用して示されるフィールドの任意のパスを編集します。
3. [保存] をクリックします。

古い隔離アイテムを削除する

[隔離ファイルメンテナンス] 画面を使用すると、SMTP および POP3 の古い隔離アイテムを手動で削除できます。または、このような隔離アイテムの隔離日数に基づいて、隔離の自動削除を設定できます。

SMTP および POP3 の古い隔離アイテムを削除するには

1. 左側のメニューで [隔離]→[メンテナンス] の順に選択します。[手動] タブが表示されている [隔離ファイルメンテナンス] 画面が表示されます。

2. [ファイルの保存日数が次の日数を超えた場合に削除する] チェックボックスで日数を編集するか、初期設定の 7 日をそのまま使用します。
3. [今すぐ削除] をクリックします。指定した日数より古い SMTP および POP3 の隔離アイテムすべてが削除されます。

[自動] タブから、SMTP および POP3 の隔離アイテムの自動削除を設定できます。この設定を行うには次の手順に従ってください。

SMTP および POP3 の隔離アイテムの隔離日数に基づく自動削除を設定するには

1. 左側のメニューで [隔離]→[メンテナンス] の順に選択します。[手動] タブが表示されている [隔離ファイルメンテナンス] 画面が表示されます。
2. [自動] タブを選択します。
3. [自動] タブで、[自動削除を有効にする] チェックボックスがオンになっていない場合にはオンにします。
4. [処理] セクションの [ファイルの保存日数が次の日数を超えた場合に削除する] チェックボックスで日数を編集するか、または初期設定の 7 日をそのまま使用します。
5. [保存] をクリックします。指定した日数より古い SMTP および POP3 の隔離アイテムすべてが定期的に削除されます。

ログを用いたセキュリティインシデントの分析

[ログ] メニューを使用して、InterScan VirusWall で検出されたセキュリティの脅威のインシデントをログ検索できます。

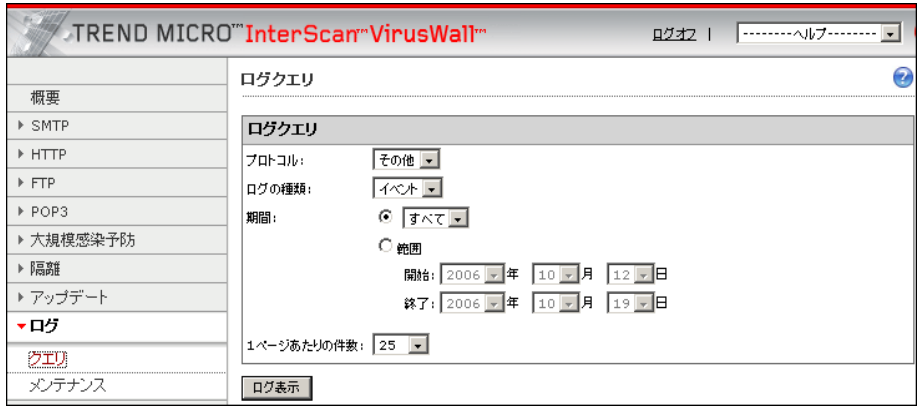


図 5-3. [ログクエリ] 画面

[ログ] メニューを選択して、[クエリ] および [メンテナンス] サブメニューを開きます。[ログクエリ] 画面を使用して、利用可能な次の 6 種類の InterScan VirusWall ログのいずれかをログ検索します。

- ウイルス / 不正プログラムのログ
- スパイウェア / グレーウェアのログ
- 添付ファイルフィルタのログ
- キーワードフィルタのログ
- スパムメール対策のログ
- フィッシング対策のログ

表 5-6.　[ログ] のサブメニュー項目

サブメニュー	説明	タスク
クエリ	InterScan VirusWall の自動ログ機能に対してクエリを実行します。 **注意：** このリリースでは、Web コンソールからのシステムログ、接続ログ、またはデバッグログに対するクエリがサポートされていません。	プロトコル、ログの種類、および期間の条件を指定してクエリを実行します。 表示するページあたりのエントリ数を指定します。 ログ表示画面を使用してログを参照し、1 ページに表示する項目数を再指定します (10、25、50、100)。 テキスト、CSV (カンマ区切り値)、または XML ファイルとしてログ検索結果をエクスポートします。
メンテナンス	特定の基準に従って古いログを削除します。 **注意：** このリリースでは、Web コンソールからのシステムログ、イベントログ、または接続ログに対するメンテナンスがサポートされていません。	削除対象のログを指定します。 n 日以上経過したログは削除します (n は日数)。 対象ログの自動削除を有効または無効にします。

ログクエリを実行する

[ログクエリ] 画面のクエリ定義フィールドを使用すると、クエリに次の条件を指定できます。

- プロトコル :
  - SMTP
    - ログの種類 :
      - ウイルス / 不正プログラム
      - スパイウェア / グレーウェア
      - 添付ファイルフィルタ
      - キーワードフィルタ
      - スパムメール対策
      - フィッシング対策
  - POP3
    - ログの種類 :
      - ウイルス / 不正プログラム
      - スパイウェア / グレーウェア
      - 添付ファイルフィルタ
      - キーワードフィルタ
      - スパムメール対策
      - フィッシング対策
  - HTTP
    - ログの種類 :
      - ウイルス / 不正プログラム
      - スパイウェア / グレーウェア
      - URL ブロック

        - URL フィルタ
        - URL アクセス
    - FTP
        - ログの種類 :
            - ウイルス / 不正プログラム
            - スパイウェア / グレーウェア
    - その他 (イベントログのみ)
- 期間 :
    - すべて
    - 今日
    - 昨日
    - 先週
    - 先月
    - 昨年
    - 範囲

また、表示する 1 ページあたりのエントリ数を指定できます (初期設定は 25、オプションは 10、25、50、または 100)。

ログのコンテンツに対してクエリを実行するには

1. 左側のメニューで [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. ここで説明した条件フィールドのいずれかを選択して、クエリの条件を入力します。
3. [ログ表示] をクリックします。InterScan VirusWall は、指定した条件を使用して選択したログに対してクエリを実行し、独立した画面にクエリ結果のページを返します。

結果が複数ページにわたる場合には、ページ情報がリストの上部に表示されます。図 5-4「1 日の時間範囲に基づいたイベントログに対するクエリのログクエリ結果」で示すように、矢印アイコンをクリックするか、またはドロップダウンメニューでページ番号を選択して、複数ページを移動します。

図 5-4.　1 日の時間範囲に基づいたイベントログに対するクエリのログクエリ結果

クエリ結果テーブル

クエリ結果が表示される列は、クエリを実行したログの種類に応じて異なります。たとえば、イベントログのクエリ結果テーブルは 2 つの列のみで構成されます。上記の図 5-4 に示すように [日付] と [イベント] になります。

139 ページの表 5-7、「ログクエリで表示されるログの種類別の情報」 に示すように、その他のログの種類では異なる情報が表示されます。

表 5-7. ログクエリで表示されるログの種類別の情報

ログの種類	表示される列						
SMTP/POP3 ウイルス / 不正プログラム	日時	ウイルス / 不正プログラム名	種類	送信者	受信者	件名	コンテンツの処理
SMTP/POP3 スパイウェア	日時	スパイウェア / グレーウェア名	種類	送信者	受信者	件名	コンテンツの処理
SMTP/POP3 添付ファイルフィルタおよびキーワードフィルタ	日時	送信者	受信者		件名		処理
SMTP/POP3 スパムメール対策およびフィッシング対策	日時	送信者	受信者		件名	メッセージの処理	
HTTP ウイルス / 不正プログラム	日時	ウイルス / 不正プログラム名		種類	ファイル名	クライアント IP	処理
HTTP スパイウェア	日時	スパイウェア / グレーウェア名		種類	ファイル名	クライアント IP	処理
HTTP URL ブロックおよび URL フィルタ	日時	クライアント IP	URL		ブロックルール		
HTTP URL アクセス	日時	クライアント IP	ドメイン名			パス	
FTP ウイルス	日時	ウイルス / 不正プログラム名		種類	ファイル名	ユーザ ID	処理
FTP スパイウェア	日時	スパイウェア / グレーウェア名		種類	ファイル名	ユーザ ID	処理
イベント	日時	イベント					

クエリ結果をエクスポートする

スプレッドシートまたは Web ベースのアプリケーションなど、さまざまなプログラムで使用するために、ログクエリ結果をテキスト、XML、または CSV 形式でエクスポートできます。

ログクエリ結果をエクスポートするには

1. 137 ページの「ログのコンテンツに対してクエリを実行するには」で説明するように、クエリを作成して実行します。
2. ログクエリ結果テーブルの上部にある [ファイル出力] ハイパーリンクをクリックします。[ログファイルの出力] ポップアップウィンドウが開きます。

3. [出力ファイルタイプ] ドロップダウンメニューの次に示すオプションからファイルタイプを選択します。
   - テキスト
   - XML
   - CSV
4. [ファイル出力] をクリックします。ブラウザは、ファイルのダウンロード時に初期設定の処理を実行します。たとえば、ファイルをコンピュータに保存するかどうかを確認するダイアログボックスが開くことがあります。

ログを削除する

[ログメンテナンス] 画面を使用すると、すべてのログ、1 つまたは複数の種類のログすべて、または選択した日数より古いログを手動で削除できます。また、この画面では、同じ条件に基づくログの自動削除も設定できます。

ログを手動で削除するには

1. 左側のメニューで [ログ]→[メンテナンス] の順に選択します。[手動] タブが表示されている [ログメンテナンス] 画面が表示されます。
2. [対象] で、削除するログの種類を選択するか、[すべてのログ] を選択してすべての種類を選択します。
3. [処理] で、次のオプションのいずれかを選択します。
   - 上記で選択されているログをすべて削除する
   - 上記で選択されているログのうち、n 日以上経過したログを削除する
4. 時間ベースのオプションを選択した場合は、削除トリガとして使用する日数を入力するか、初期設定値の 30 日をそのまま使用します。

5. [今すぐ削除] をクリックします。設定した条件に一致するすべてのログが削除され、この処理を確認する [完了] メッセージボックスが表示されます ([ログメンテナンス] 画面に戻るには [戻る] をクリック)。

注意 : Web コンソールから、システムログ、イベントログ、接続ログ、またはデバッグログは削除できません。

自動ログメンテナンス (削除) の設定は、手動でのログの削除の設定ととてもよく似ています。

自動ログメンテナンスを設定するには

1. 左側のメニューで [ログ]→[メンテナンス] の順に選択します。[手動] タブが表示されている [ログメンテナンス] 画面が表示されます。
2. [自動] タブを選択します。
3. [自動] タブで、[自動削除を有効にする] チェックボックスをオンにします。
4. 削除条件を選択します (140 ページの「ログを手動で削除するには」を参照)。
5. [保存] をクリックします。自動ログメンテナンスの条件が記録され、それに応じて定期的にログが削除されます。

その他のログ

Web コンソールで管理できるログの他に、InterScan VirusWall は次のログを記録します。

- システムログ - サービスの開始と停止、システムエラー、例外などに関する情報。ログファイル名 : systemlog.yyyymmdd.nnnn
- デバッグログ (有効な場合) - トレンドマイクロのテクニカルサポートによる要求時にのみ使用されるデバッグ情報。ログファイル名 : debuglog.yyyymmdd.nnnn

- 接続ログ - SMTP 接続 / 切断ログ。ログファイル名 : connectlog.yyyymmdd.nnnn

ヒント：トレンドマイクロのテクニカルサポートが特定のトラブルシューティングを目的としてデバッグログを実行するように求める場合を除き、デバッグログを実行しないことをお勧めします。

製品サポート情報

InterScan VirusWall 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、契約満了期間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 (トラブルシューティング) 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。

http://esupport.trendmicro.co.jp/supportjp/supportcentral/supportcentral_adv_ja.do

図 5-5.　製品 Q&A の Web サイト

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/supform.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、フィリピンを本拠地に、米国、欧州、日本、中国、台湾にわたる 800 名以上 (2006 年 1 月現在) のエンジニアから構成されています。ウイルス情報の収集、調査、解析やサポートを年中無休 24 時間の体制で行っています。

「TrendLabs」の本拠地、フィリピンのマニラ近くにあるラボは、高度な技術水準と最新設備を備えており、管理とサービス提供の手続きにおいて品質保証の国際基準を満たす ISO9001:2000 認定を取得しています。

用語集

この用語集では、このドキュメントまたはオンラインヘルプで使用される特別な用語について説明しています。

用語	説明
DNS	ドメインネームシステム（Domain Name System）- ホスト名を IP アドレスに変換するために主にインターネット上で使用されている汎用的なデータクエリサービス。
DNS 名前解決	DNS クライアントが DNS サーバにホスト名とアドレスデータを要求するときのプロセス。基本的な DNS 設定では、サーバが初期設定された名前解決プロセスを実行します。たとえば、リモートサーバは、現在のゾーンにあるコンピュータ上のデータについて別のサーバに問い合わせます。リモートサーバ上のクライアントソフトウェアはリゾルバに問い合わせます。リゾルバは、データベースファイルからの要求に応答します。
DoS (Denial of Service) 攻撃	大きな添付ファイルがあるメールメッセージを大量に送信してネットワークリソースを妨害し、メッセージングサービスの停滞や停止を引き起こします。
DOS ウイルス	「COM」および「EXE」ファイル感染ウイルスとも呼ばれます。DOS ウイルスは、*.COM または *.EXE 拡張子を持つ DOS 実行可能プログラムファイルに感染します。元のプログラムコード部分を上書きしたり不注意に破壊する場合を除き、大部分の DOS ウイルスは、他のホストプログラムに感染して増殖と拡大を試みます。

用語	説明
Ethernet	Xerox 社のパロアルト研究所で考案されたローカルエリアネットワーク (LAN) テクノロジです。Ethernet は、CSMA/CD テクノロジを使用するベストエフォート型配信システムです。Ethernet は、太い同軸ケーブル、細い同軸ケーブル、ツイストペアケーブル、光ファイバケーブルなど、さまざまなケーブルスキームで使用できます。Ethernet は、コンピュータをローカルエリアネットワークに接続するための規格です。Ethernet の最も一般的な形式は 10BaseT と呼ばれます。銅のツイストペアケーブルを使用し、ピーク時の伝送速度は 10Mbps です。
FTP	あるコンピュータのユーザが別のコンピュータとの間で TCP/IP ネットワークを介してファイルを双方向に転送できるクライアント / サーバのプロトコルです。また、ユーザがファイルを転送するために実行するクライアントプログラムのことも表します。
HTML ウイルス	Web ページの情報の作成に使用される HTML (Hyper Text Markup Language)、オーサリング言語を標的にするウイルスです。ウイルスは Web ページに常駐し、ユーザのブラウザを介してダウンロードされます。
HTTP	ハイパーテキスト転送プロトコル（Hypertext Transfer Protocol）- HTML 文書の交換のために WWW（World Wide Web）上で使用されるクライアント / サーバの TCP/IP プロトコル。通常はポート 80 を使用します。
HTTPS	ハイパーテキスト転送プロトコルセキュリティ（Hypertext Transfer Protocol Secure）- セキュリティで保護されたトランザクションの処理に使用される HTTP の強化版です。

用語	説明
ICMP (Internet Control Message Protocol)	ゲートウェイまたは送信先ホストは、たとえばデータグラム処理におけるエラーをレポートするために、送信元ホストと通信することがあります。このような場合に、ICMP (Internet Control Message Protocol) プロトコルが使用されます。ICMP は、IP の基本サポートを上位レベルプロトコルであるように使用しますが、実際に ICMP は IP の不可欠な要素であり、すべての IP モジュールで実装されていなければなりません。ICMP メッセージはさまざまな状況で送信されます。たとえば、データグラムが宛先に到達できない、ゲートウェイにデータグラムを転送するバッファリング能力がない、より短いルートでトラフィックを送信するようにゲートウェイがホストに指示できる場合などです。インターネットプロトコルは、完全に信頼できるように設計されていません。これらの制御メッセージの目的は、通信環境における問題に関してフィードバックを提供することであり、IP の信頼性を確保することでありません。
IMAP	インターネットメッセージアクセスプロトコル（Internet Message Access Protocol）- クライアントがサーバ上で電子メールメッセージにアクセスして操作することを可能にするプロトコル。IMAP を使用すると、リモートメールフォルダ（メールボックス）の操作をローカルメールボックスの操作を行うのと同様に実行できます。
「in the wild」	活発に巡回している既知のウイルスを表します。
IP	インターネットプロトコル -「IP アドレス」も参照してください。
IPSec (IP セキュリティ)	IETF (Internet Engineering Task Force) によって作成されたセキュリティ標準。通信のセキュリティを保護するために必要なあらゆるもの (認証、完全性、機密性) を提供し、大規模ネットワークでも鍵交換を実行可能にするプロトコルスイートです。「DES-CBC」、「ESP/AH」も参照してください。
IP アドレス	ネットワーク上にあるデバイスのインターネットアドレス。一般に、123.123.123.123 などピリオド (.) で表記します。
IP ゲートウェイ	ルータとも呼ばれます。ゲートウェイは、IP データグラムを、最終的な宛先に到達するまでネットワークから別のネットワークに転送するプログラム、または専用デバイスです。

用語	説明
JavaScript ウイルス	JavaScript は、Web 開発者がスクリプトを使用して、ブラウザに表示される HTML ページに動的コンテンツを追加できるように、Netscape によって開発された簡単なプログラミング言語です。Javascript は、Sun Microsystems の Java プログラミング言語のいくつかの機能を共有していますが、独自に開発されました。 JavaScript ウイルスは、HTML コードの JavaScript を標的にするウイルスです。これによりウイルスを Web ページに常駐させ、ユーザのブラウザを介してユーザのデスクトップにウイルスをダウンロードすることができるようになります。 「Vbscript ウイルス」も参照してください。
Java アプレット	Java アプレットは、HTML ページに埋め込まれている小規模な移植可能な Java プログラムで、HTML ページが表示されると自動的に実行できます。Java アプレットを使用すると、Web 開発者は、広範囲な機能を備えた対話型の動的な Web ページを作成できます。 不正プログラムの作成者は、攻撃のための媒体手段として Java アプレットを使用してきました。しかし大部分の Web ブラウザは、ブラウザのセキュリティ設定を「高」に変更することによって、これらのアプレットが実行されないように設定できます。
Java ファイル	Java は、Sun Microsystems によって開発された汎用プログラミング言語です。Java ファイルは Java コードを含みます。Java は、プラットフォームに依存しない Java「アプレット」の形式で、インターネットのプログラミングをサポートします (アプレットは、HTML ページに挿入できる、Java プログラミング言語で記述されたプログラムです。Java 対応ブラウザを使用してアプレットを含むページを表示すると、アプレットのコードはシステムに転送され、ブラウザの Java 仮想マシンで実行されます)。
Java 不正コード	Java で記述された、または Java に埋め込まれているウイルスコードです。「Java ファイル」も参照してください。
LHA ファイル形式	LHA は無料のデータ圧縮ユーティリティで、主に日本でよく使用されています。LHA で圧縮されているファイルの拡張子は、.lha または .lzh です。

用語	説明
MAC (Media Access Control) アドレス	Ethernet アダプタなどの、ネットワークインタフェースカードを一意に識別するアドレス。Ethernet については、MAC アドレスは IEEE によって割り当てられた 6 オクテットのアドレスです。LAN または他のネットワークでは、MAC アドレスはコンピュータの一意のハードウェア番号です (Ethernet LAN では、MAC アドレスは Ethernet アドレスと同じ)。コンピュータ (またはインターネットプロトコルでのホスト) からインターネットに接続すると、対応テーブルで、IP アドレスが LAN 上のコンピュータの物理的 (MAC) アドレスに関連付けられます。MAC アドレスは、通信プロトコルにおけるデータリンク制御 (DLC) レイヤの媒体アクセス制御サブレイヤによって使用されます。物理デバイスのタイプに応じて、MAC サブレイヤが異なります。
MacroTrap	文書と関連して保存されるすべてのマクロコードに対してルールに基づく検査を実行するトレンドマイクロのテクノロジ。マクロウイルスのコードは一般に、多くの文書とともに移動する非表示テンプレート（Microsoft Word 文書の .dot など）の一部に含まれています。MacroTrap は、ウイルスに似た動作を行う主な命令を探してテンプレートを調べ、マクロウイルスの痕跡があるかどうかをチェックします。対象となる主な命令には、テンプレートの一部を別のテンプレートにコピーする命令（複製）または潜在的に危険なコマンドを実行する命令（破棄）などがあります。
Mbps	100 万ビット毎秒。データ通信における帯域幅の単位です。
Microsoft Office ファイル	Microsoft Excel、Word などの Microsoft Office ツールで作成されたファイルです。
MTA (メール転送エージェント)	メールメッセージの配信を担当するプログラムです。「SMTP サーバ」も参照してください。
MX レコード	DNS リソースレコードタイプの一種。特定ドメインのメールを処理できるホストを示します。
NetBIOS (Network Basic Input Output System)	ネットワーク機能などの機能を DOS (ディスクオペレーティングシステム) BIOS (basic input/output system) に追加するアプリケーションプログラムインタフェース (API) です。
OSPF (Open Shortest Path First)	インターネット標準の内部ゲートウェイプロトコルの 1 つである、リンク状態型ルーティングプロトコルです。OSPF ルータでは最短のパスを使用して、インターネットトポグラフィの各ノードにデータを送信します。

用語	説明
PASSIVE FTP	ローカルエリアネットワーク内のクライアントに、ランダムな上位ポート番号 (1024 以上) を使用したファイル転送の初期化を許可する、FTP プロトコルの設定です。
POP3	Post Office Protocol, version 3 - クライアントコンピュータが、一時的な接続 (永続的なネットワーク接続を使用しないモバイルコンピュータなど) を介してサーバから電子メールを取得する際に使用するメッセージングプロトコルのことです。
POP3 サーバ	POP3 メールをホストするサーバ。ネットワーク内のクライアントはそのサーバから POP3 メールを取得します。
Q&A	よくある質問 - 特定の話題に関する質問と回答のリストです。
SMTP	Simple Mail Transfer Protocol - 一般に Ethernet を介してコンピュータ間で電子メールを転送するためのプロトコルです。サーバ対サーバのプロトコルであることから、メッセージへのアクセスには別のプロトコルが使用されます。
SMTP サーバ	メールメッセージを送信先にリレーするサーバです。
SNMP	Simple Network Management Protocol - 管理上注意すべき状態について、ネットワークに接続されているデバイスの管理をサポートするプロトコルです。
SNMP トラップ	トラップとは、コンピュータプログラムのエラーや他の問題を処理するプログラミングメカニズムです。SNMP トラップでは、ネットワークデバイスの監視に関連するエラーを処理します。 「SNMP」を参照してください。
SOCKS4	ファイアウォールを横断するアプリケーションユーザの透過的なアクセスを可能にするためにファイアウォールホストで TCP (Transmission Control Protocol) セッションをリレーするプロトコルです。
SSL (Secure Socket Layer)	SSL (Secure Socket Layer) は、アプリケーションプロトコル (HTTP、Telnet、FTP など) と TCP/IP の間に層を成すデータセキュリティを提供するために、Netscape によって設計されたプロトコルです。このセキュリティプロトコルは、データの暗号化、サーバの認証、メッセージの完全性、および任意の TCP/IP 接続のクライアント認証を実現します。
TCP	Transmission Control Protocol - IP (インターネットプロトコル) と一緒に最も一般的に使用されるネットワークプロトコルです。コンピュータシステムとインターネットの接続を管理します。

用語	説明
TCP/IP (Transmission Control Protocol/Internet Protocol)	ローカルおよび広域ネットワークの両方でピアツーピア接続機能をサポートする、通信プロトコルのセット。通信プロトコルは、異なる OS を使用するコンピュータ間の通信を可能にします。インターネット上のコンピュータ間でデータを転送する方法を制御します。
Telnet	TCP/IP (Transmission Control Protocol/Internet Protocol) 上で実行されるリモートログイン用のインターネット標準プロトコル。この用語は、リモートログインセッションのターミナルエミュレータとして機能するネットワークソフトウェアを指すこともあります。
UDP (User Datagram Protocol)	TCP/IP プロトコルスイートのプロトコル。UDP (User Datagram Protocol) によって、アプリケーションプログラムはリモートコンピュータにある他のアプリケーションプログラムにデータグラムを送信できるようになります。一般的に UDP は、信頼できないコネクションレスのデータグラムサービスを提供するプログラムで、配信と複製の検出は保証されていません。UDP では応答確認を使用したり、到着順序を管理したりすることはしません。
URL	Uniform Resource Locator - オブジェクトの場所を指定するための標準的な方法。通常は「www.trendmicro.co.jp」など、インターネット上の Web ページの場所を指定します。URL は DNS を使用して IP アドレスにマップされます。
VBscript ウイルス	VBscript (Microsoft Visual Basic スクリプト言語) は簡単なプログラミング言語で、Web 開発者は VBscript を使用して、ブラウザに表示される HTML ページにインタラクティブな機能を追加できます。たとえば、開発者は「詳細についてはここをクリックしてください」というボタンを追加できます。 VBscript ウイルスは、HTML コードの VBscript を標的にするウイルスです。これによりウイルスを Web ページに常駐させ、ユーザのブラウザを介してユーザのデスクトップにウイルスをダウンロードすることができるようになります。 「JavaScript ウイルス」も参照してください。
VLAN (Virtual Local Area Network)	単一のブロードキャストドメインを構成するデバイスの (物理的ではない) 論理的なグループです。VLAN のメンバーは、物理的なサブネットワークの場所で識別されるのではなく、送信データのフレームヘッダにあるタグを使用して識別されます。VLAN は、IEEE 802.1Q 規格で記述されています。

用語	説明
VPN (Virtual Private Network)	VPN は、在宅勤務者やモバイル通信の利用者が、企業のネットワークや別のインターネットサービスプロバイダ (ISP) にアクセスできるようにする、簡単で費用効果が高い安全な方法です。インターネットを介した安全なプライベート接続は、専用プライベート回線よりも費用効果が高くなります。VPN は、トンネリングや暗号化などの技術と規格によって可能になりました。
VSI (Virtual Security Interface)	VSD グループ内の複数のレイヤ 2 物理インタフェースにリンクされている、レイヤ 3 の論理エンティティです。VSI は、VSD グループのマスタとして機能するデバイスの物理インタフェースと結合します。VSI は、フェイルオーバーが発生し、VSD グループ内の別のデバイスが新しいマスタになると、そのデバイスの物理インタフェースにシフトします。
Web	World Wide Web。Web またはインターネットとも呼びます。
Web サーバ	Web サイトで実行されているサーバプロセス。サーバプロセスでは、リモートブラウザからの HTTP 要求に応答して Web ページを送信します。
WINS (Windows Internet Naming Service)	WINS は、IP アドレスを Windows NT サーバベースのネットワークにある NetBIOS コンピュータ名にマップするためのサービスです。WINS サーバは、Windows ネットワーク環境で使用される NetBIOS 名を、IP ベースのネットワークで使用される IP アドレスにマップします。
「Zip of Death」	解凍時、非常に大きく (たとえば 1000%) 拡大するファイル、または数千の添付ファイルを含む ZIP ファイル。圧縮ファイルは、検索時に解凍する必要があります。巨大なファイルによって、ネットワークが停滞したり停止したりする可能性があります。
ZIP ファイル	WinZip などのアーカイブプログラムを使用して、1 つ以上のファイルから作成される圧縮アーカイブ (または「ZIP ファイル」) です。
アーカイブ	.zip ファイルなどの、対応プログラムによって展開 (分離) できる 1 つまたは (通常は) 複数の個別ファイルと情報を含む単一のファイルです。
アクティベーションコード	トレンドマイクロ製品のアクティベートに使用される、ハイフンを含む 37 文字のコードです。アクティベーションコードの例 : SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 「レジストレーションキー」も参照してください。

用語	説明
アクティベート	登録処理が完了してからソフトウェアを有効にすることです。トレンドマイクロ製品は、製品のアクティベーションが終わるまで操作できません。インストール中または、インストール後に [製品ライセンス情報] 画面でアクティベートします。インストール後は Web コンソールを使用します。
圧縮ファイル	WinZip などの対応プログラムによって展開できる 1 つまたは複数の個別ファイルと情報を含む単一のファイルです。
アップデート	アップデートは、多くのトレンドマイクロ製品に共通の機能です。トレンドマイクロのアップデート Web サイトに接続すると、アップデートによって、ウイルスパターンファイル、検索エンジン、プログラムファイルの最新のダウンロードがインターネット経由で提供されます。
アドウェア	プログラムが動作中に広告バナーを表示する、広告を目的としたソフトウェアです。アドウェアは「バックドア」をインストールします。ユーザが知らないうちにユーザのコンピュータを追跡するメカニズムは「スパイウェア」と呼ばれます。
アドレス	ネットワークアドレス (「IP アドレス」を参照) またはメールアドレスのことです。メールメッセージの送信元または宛先を指定する文字列です。
暗号化	暗号化は、対象の受信者だけが読み取ることのできる形式にデータを変更するプロセスです。メッセージを解読する場合は、暗号化されたデータの受信者が適切な復号鍵を持っている必要があります。通常の暗号化スキームでは、送信者と受信者は同じ鍵を使用して、データの暗号化と復号を行います。公開鍵暗号化スキームでは 2 つの鍵を使用します。誰でも使用できる公開鍵と、それに対応する秘密鍵です。秘密鍵は作成したユーザだけが所有します。この方法を使用すると、所有者の公開鍵を使用して暗号化されたメッセージを誰もが送信できますが、メッセージの解読に必要な秘密鍵は所有者のみが保持しています。PGP (Pretty Good Privacy) と DES (Data Encryption Standard) は、最も一般的な公開鍵暗号化スキームです。
インストールスクリプト	UNIX バージョンのトレンドマイクロ製品をインストールするために使用されるインストール画面です。
インストールディレクトリ	主要なアプリケーションファイルが格納される格納先のディレクトリ。例 : C:¥Program Files¥Trend Micro¥ISVW

用語	説明
インターネットプロトコル (IP)	データグラムと呼ばれるデータの基本単位を定義するインターネットの標準プロトコル。データグラムは、コネクションレスのベストエフォート型配信システムで使用されます。インターネットプロトコルでは、インターネットを介したシステム間の情報の受け渡し方法を定義します。
イントラネット	組織外のインターネットで提供されているサービスと同様のサービスを組織内で提供するネットワーク。しかし、インターネットに接続する必要はありません。
ウイルス	コンピュータウイルスは、感染するための特異な機能を持つプログラム、つまり 1 つの実行可能コードです。コンピュータウイルスは、生物学上のウイルスのように急速に伝染するため、多くの場合根絶が困難です。 複製に加え、一部のコンピュータウイルスは次の共通特性を備えています。ウイルスペイロードを配信する破壊ルーチンです。ペイロードは一方でメッセージまたは画像を表示しながら、ファイルの破壊やハードドライブの再フォーマットを行い、場合によっては他を破壊する原因にもなります。ウイルスが破壊ルーチンを含まない場合でも、格納領域とメモリを使い尽くし、コンピュータのパフォーマンス全体を低下させて、トラブルの原因を作る可能性があります。
ウイルスキット	インターネットから入手できる、ウイルスを作成して実行するためのソースコードのテンプレートです。
ウイルスシグニチャ	ウイルスシグニチャは、特定のウイルスを識別する一意のビット列です。ウイルスシグニチャは、トレンドマイクロのウイルスパターンファイルに格納されています。トレンドマイクロの検索エンジンは、メールメッセージの本文や HTTP ダウンロードの内容など、ファイル内のコードをパターンファイル内のシグニチャと比較します。一致が見つかると、ウイルスが検出され、セキュリティポリシーに従って処理 (駆除、削除、隔離など) されます。
ウイルストラップ	分析のためにウイルスコードのサンプルを取得するためのソフトウェアです。
ウイルス作成者	ウイルスコードを記述する人のことで、コンピュータハッカーの別名です。
ウイルス対策	コンピュータウイルスを検出し駆除するためのコンピュータプログラムです。

用語	説明
エンドユーザ使用許諾契約 (EULA)	エンドユーザ使用許諾契約 (EULA) は、ソフトウェア発行元とソフトウェアユーザ間で交わされる法的な契約です。エンドユーザ使用許諾契約では、通常、ユーザ側の規定の概要を示します。ユーザは、インストール中に「同意する」を選択しなければ、契約を拒否できます。「同意しない」を選択した場合、ソフトウェア製品のインストールは終了します。 多くのユーザは、一部の無料ソフトウェアのインストール中に表示される EULA の確認画面で「同意する」を選択して、気づかずにスパイウェアやアドウェアのコンピュータへのインストールに同意しています。
オーディオ / ビデオファイル	音楽などのサウンドやビデオ映像を含むファイルです。
オープンソース	一般ユーザが、ライセンスの制限を受けることなく、無料で使用、変更できるプログラミングコードです。
大文字小文字の区別	単語と大文字小文字の両方が一致するテキストの検索です。たとえば、大文字小文字の区別を有効にした状態で「dog」をコンテンツフィルタに追加すると、「Dog」を含むメッセージはフィルタ基準に一致せず、「dog」を含むメッセージはフィルタ基準に一致します。
大文字小文字を区別する	「大文字小文字の区別」を参照してください。
オンラインヘルプ	管理コンソールなどの設定画面から参照できる製品の機能概要、使用手順などを説明したドキュメントです。
隔離	メールメッセージ、感染した添付ファイル、感染した HTTP ダウンロード、または感染した FTP ファイルなどの感染したデータを、サーバ上の分離されたディレクトリ（隔離ディレクトリ）に置くことです。
仮想 IP アドレス (VIP アドレス)	VIP アドレスは、ある IP アドレスで受信したトラフィックを、パケットヘッダの宛先ポート番号に基づいて、別のアドレスにマップします。
管理者	「システム管理者」のことです。新しいハードウェアとソフトウェアの設定、ユーザ名とパスワードの割り当て、ディスクの空き容量や他の IT リソースの監視、バックアップの実行、ネットワークセキュリティの管理などの活動を担当する組織内の人物です。
管理者アカウント	管理者レベルの権限を有するユーザ名とパスワードです。
(管理) ドメイン	共通のデータベースとセキュリティポリシーを共有するコンピュータのグループです。

用語	説明
管理者メールアドレス	通知と警告を管理するために、トレンドマイクロ製品の管理者が使用するアドレスです。
キー入力記録型	キー入力記録型は、すべてのキーボード入力を監視し記録するプログラムです。従業員を監視する会社や子供を監視する親が使用する、正規のキー入力記録プログラムがあります。しかし犯罪者もキー入力の記録を使用して、ログオンアカウント情報やクレジットカード番号などの貴重な情報を選別します。
キャッシュ	最近アクセスしたデータを格納する小規模な高速メモリ。同じデータに対する後続アクセスを高速化するために使用されます。この用語は、ほとんど場合、プロセッサメモリのアクセスに適用されますが、ネットワークを介してアクセス可能なデータのローカルコピーなどにも適用されます。
キュー	処理速度よりも速くメールを受信しているとき、リソースに対する複数の要求を一定の順序に配列するために使用するデータ構造。メッセージは、FIFO（先入れ先出し）方式でキューの最後尾に追加されキューの先頭から処理されます。
共有ドライブ	複数のユーザによって使用されるコンピュータの周辺デバイス。これを使用すると、ウイルスの危険にさらされる可能性が高くなります。
駆除	ファイルまたはメッセージからウイルスコードを除去することです。
クッキー	名前、傾向、興味などのインターネットユーザに関する情報を格納するメカニズム。この情報は、後から利用できるように Web ブラウザに格納されます。ブラウザに cookie が保存されている Web サイトに次回アクセスすると、ブラウザは cookie を Web サーバに送信します。Web サーバはその cookie を使用して、カスタマイズされた Web ページを表示できます。たとえば、名前を表示して開始する Web サイトにアクセスする場合などです。
クライアント	ある種のプロトコルを使用して別のコンピュータのシステムまたはプロセス（「サーバ」）にサービスを要求し、そのサーバから応答を受け取るコンピュータのシステムまたはプロセスです。クライアントは、クライアント / サーバソフトウェアアーキテクチャの一部です。

用語	説明
グループファイルタイプ	共通のテーマを持つファイルのタイプ。次のタイプがあります。 - オーディオ / ビデオファイル - 圧縮ファイル - 実行可能ファイル - 画像ファイル - Java ファイル - Microsoft Office ファイル
グレーウェア	正規であるが、望ましくない、または悪意のある可能性があるソフトウェアのカテゴリです。ウイルス、ワーム、トロイの木馬などの脅威とは違い、グレーウェアは感染したり、増殖したり、データを破壊したりすることはありませんが、プライバシーを侵害する可能性があります。グレーウェアの例には、スパイウェア、アドウェア、リモートアクセスツールなどがあります。
ゲートウェイ	情報元と Web サーバとのインタフェースです。
検索	特定の基準に一致する項目を見つけるために、ファイル内の項目を順番に検査することです。
検索エンジン	ホスト製品内でウイルス検索と検出を実行するモジュールのことです。
公開鍵暗号方式	各ユーザが公開鍵と秘密鍵と呼ばれる一組の「鍵」を取得する暗号化スキームです。各ユーザの公開鍵は公開されますが、秘密鍵は公開されません。メッセージは、対象の受信者の公開鍵を用いて暗号化され、その受信者の秘密鍵でのみ復号化できます。「認証」と「デジタル署名」も参照してください。
誤検出	実際にはスパムメールではないのに、スパムメールフィルタで「検出」されてスパムメールと判定されたメールメッセージです。
コンテンツ違反	コンテンツフィルタポリシーをトリガしたイベントです。
コンテンツフィルタ	メールメッセージを検索して、会社の人事管理や IT のメッセージングポリシーで禁止された嫌がらせのメール、不快な言葉、成人向けコンテンツ（単語や字句）を調べることです。

用語	説明
サーバ	別の (クライアント) プログラムにサービスを提供するプログラム。クライアントとサーバ間の接続は、通常、ネットワーク経由によるメッセージの受け渡しによって行われ、プロトコルを使用してクライアントの要求とサーバの応答をエンコードします。サーバはデーモンとして、要求の到着を待機しながら連続的に動作するか、多くの特定のサーバを制御する上位レベルのデーモンによって呼び出されます。
サーバファーム	サーバファームは、Web サーバ、メール、またはその他の必要な TCP/IP ベースのサービスを実行するために、クライアントが独自のコンピュータを設置するネットワークです。この際、24 時間世界中からアクセスされるリース契約の常時インターネット接続を利用します。さまざまなオフィスへの接続に高価な専用回線を使用せずに、サーバをサーバファームネットワークに配置して、リース契約の回線のわずかな費用でサーバをインターネットに高速接続します。
削除	すべてを削除することです。ログの古いエントリを処分する場合などに使用します。
サブネットマスク	大規模なネットワークでは、サブネットマスクによってサブネットワークを定義できます。たとえば、クラス B のネットワークがある場合、サブネットマスク 255.255.255.0 では、ピリオドで区切られた最初の 2 つの部分がネットワーク番号、3 番目の部分がサブネット番号を表します。4 番目の部分はホスト番号を表します。クラス B のネットワークでサブネットを使用しない場合は、サブネットマスク 255.255.0.0 を使用します。 1 つのネットワークは、メインネットワークのサブセットを形成する、1 つ以上の物理ネットワークにサブネット化できます。サブネットマスクは、ネットワーク内のサブネットワークを表すために使用される IP アドレスの一部です。サブネットマスクを使用すると、通常は利用できないネットワークアドレス領域を使用できます。また意図しない限り、ネットワークトラフィックがネットワーク全体に送信されないようにすることもできます。サブネットマスクは複雑な機能であるため、使用する際は細心の注意を払う必要があります。「IP アドレス」も参照してください。
シグニチャ	「ウイルスのシグニチャ」を参照してください。

用語	説明
シグニチャベースのスパムメール検出	メッセージの内容をスパムメールのデータベースと比較して、メールメッセージがスパムメールであるかどうかを判断する方法。スパムメールと識別されるためには、メッセージに正確に一致する部分が見つかる必要があります。シグニチャベースのスパムメール検出は、誤検出率はほぼゼロですが、スパムメールシグニチャファイルのテキストに正確に一致しない「新しい」スパムメールは検出されません。 「ルールベースのスパムメール検出」も参照してください。 「誤検出」も参照してください。
システム領域感染型ウイルス	システム領域感染型ウイルスは、コンピュータのブートセクタ (OS) を攻撃するウイルスです。コンピュータシステムは、感染ディスクを使用してフロッピードライブからシステムを起動するときに、ほとんどの場合システム領域感染型ウイルスに攻撃されます。ハードドライブに感染するウイルスが原因で、ブートが失敗する場合があります。 また、実行可能プログラムからブートセクタに感染可能なウイルスもいくつかあります。これらは複合感染型ウイルスと呼ばれますが、比較的まれです。システムが感染すると、システム領域感染型ウイルスはそのコンピュータからアクセスされるすべてのディスクへの感染を試みます。システム領域感染型ウイルスは、通常正常に削除できます。
実行可能ファイル	いつでも実行可能な機械語のプログラムを含むバイナリファイルです。
実際のファイルタイプ	トレンドマイクロの推奨設定で使用されるウイルス検索技術で、偽装可能なファイル名拡張子に関係なく、ファイルヘッダを調べてファイルにある情報の種類を特定します。
受信	自社のネットワークに転送されてくるメールメッセージまたはその他のデータです。
受信者	メールの宛先人または宛先エンティティのことです。
承認する送信者	ネットワークへのメッセージの送信が常に許可されている送信者です。
ジョークプログラム	ユーザを苛立たせたり、必要以上に警戒させたりする実行可能プログラムです。ウイルスとは異なり、ジョークプログラムは自己増殖することはないので、簡単にシステムから削除できます。

用語	説明
処理 (「対象」と「通知」も参照)	以下の場合に実行される操作です。 ・ ウイルスが検出されたとき ・ スパムメールが検出されたとき ・ コンテンツ違反が発生したとき ・ ブロックされた URL にアクセスしようとしたとき ・ ファイルブロックがトリガされたとき 処理には通常、駆除と配信、隔離、削除、あるいは配信 / 転送などがあります。配信 / 転送はお勧めしません。ウイルスに感染したメッセージを配信したりウイルスに感染したファイルを転送したりすると、ネットワークを危険にさらす可能性があります。
信頼するドメイン	メッセージがスパムメールかどうかを考慮せずに、トレンドマイクロ製品によって常にメッセージが受信されるドメイン。
信頼するホスト	正常に動作し、たとえばネットワークを経由するスパムメールをリレーしないと信頼されているため、ネットワークを経由するメールをリレーすることが許可されているサーバです。
スクリプト	呼び出して一緒に実行できるプログラミングコマンドのセットです。「スクリプト」と同義で使用されている他の用語には、「マクロ」、「バッチファイル」などがあります。
スタンプ	「スパムメール」などの識別子をメールメッセージの件名フィールドに挿入することです。
ステータスバー	コンピュータへのファイルのロードなどの特定処理のステータスや進行状況を表示するユーザインタフェースの機能です。
スパイウェア	広告を目的としたソフトウェアで、通常はシステムに追跡ソフトウェアをインストールします。追跡ソフトウェアは、ユーザに関する情報を第三者に送信できます。スパイウェアの脅威は、収集されたデータやその使用方法をユーザが管理できないことです。
スパムメール	製品やサービスを宣伝するための一方的なメールメッセージです。
スパムメール対策	フィルタメカニズムのことです。広告、ポルノ、「迷惑」メールを識別して配信を防ぎます。
スパムメール判定ルールおよびエンジン	スパムメールの検出とフィルタに使用するトレンドマイクロのツールです。

用語	説明
セキュリティアソシエーション	セキュリティパラメータインデックスと宛先アドレスの組み合わせです。Authentication Header と Encapsulating Security Payload プロトコルの両方で必要です。「セキュリティパラメータインデックス」も参照してください。
セキュリティゾーン	セキュリティゾーンは、アクセスポリシーを介した送受信トラフィックの規制を必要とする 1 つ以上のネットワークセグメントの集まりです。
セキュリティホール	ソフトウェアの脆弱性やセキュリティホールを利用するコードです。脆弱なコンピュータに繁殖し複雑なルーチンを実行できます。
設定	ウイルス感染メールを隔離するか削除するかの選択など、トレンドマイクロ製品の動作方法を決定する選択オプションです。
増殖	自己複製のこと。このドキュメントで使用されているように、この用語は自己複製可能なウイルスやワームのことを表します。
送信	自社のネットワークを離れて外部のインターネットに転送されるメールまたはその他のデータです。
送信者	別のユーザやエンティティにメールを送信しているユーザです。
ゾーン	ゾーンには、セキュリティ基準が適用されるネットワークスペースのセグメント（セキュリティゾーン）、VPN トンネルインタフェースがバインドされる論理セグメント (トンネルゾーン)、特定の機能を実行する物理エンティティまたは論理エンティティ (機能ゾーン) があります。
待機ポート	データ交換のためのクライアント接続要求に利用されるポートです。
対象 (「処理」および「通知」も参照)	メールメッセージで検出されるウイルスなど、違反イベントについて監視される活動の範囲。たとえば、ネットワークを通過するすべてのファイルをネットワーク検索の対象にしたり、特定のファイル名拡張子を持つファイルだけを対象にしたりできます。
ダイヤラー	トロイの木馬の一種。実行されると、ユーザのシステムをコール課金型サイトに接続し、ユーザは知らない間に思いも寄らない電話料金が請求されます。

用語	説明
通知 (「処理」と「対象」も参照)	次の 1 つまたは複数に転送されるメッセージ。 - システム管理者 - メッセージ送信者 - メッセージ、ファイルダウンロード、またはファイル転送の受信者 通知の目的は、禁止されている操作が実行されたことまたは試行されたこと (試行された HTTP ファイルダウンロードでウイルスが検出されるなど) を連絡することです。
ディスクレーマ	メールの先頭または最後尾に挿入されるメッセージ。メッセージは、メールの内容に関する法律厳守や守秘義務の条項を表します。ディスクレーマの例を参照するには、Web コンソールの [SMTP]→[設定]→[リレー管理] 画面にアクセスします。
デーモン	明示的に呼び出されないで、ある状態の発生を待機しているプログラムです。状態の発生元はデーモンの存在を意識する必要はありません。
デジタル署名	公開鍵暗号方式と呼ばれる技術を使用して、送信者とメッセージデータを識別して証明する、メッセージに追加される付加データです。「公開鍵暗号方式」と「認証」も参照してください。
添付ファイル	メールメッセージに添付されたファイルです。
登録	トレンドマイクロの [オンライン登録] 画面で製品のレジストレーションキーを使用して、トレンドマイクロ製品のユーザとして登録するプロセスです。 https://olr.trendmicro.com/registration/jp/ja/login.aspx
ドメイン名	tellsitall.com のようにローカルホスト名とドメイン名で構成されるシステムの完全名。ドメイン名は、インターネット上のどのホストについても一意のインターネットアドレスを特定できるものである必要があります。「名前解決」と呼ぶこのプロセスは、ドメインネームシステム (DNS) を使用します。
トラフィック	インターネットとネットワーク間を流れる送受信データです。
トリガ	活動を発生させるイベント。たとえば、トレンドマイクロの製品がメールメッセージでウイルスを検出した場合、メッセージの各ディレクトリへの配置、システム管理者、メッセージ送信者、メッセージ受信者への通知の送信がトリガされます。

用語	説明
トレンドマイクロの推奨設定	実際のファイルタイプを認識してファイルヘッダを検査し、不正なコードが存在する可能性があるファイルタイプのみを検索することでパフォーマンスを最適化するトレンドマイクロの検索技術。実際のファイルタイプの認識によって、安全な拡張子名で偽装された不正なコードを識別することができます。
トロイの木馬	一見すると害のないプログラムのように見せる不正プログラム。トロイの木馬は実行可能プログラムで増殖はしません。しかしシステムに常駐して、侵入者のためにポートを開くなど、不正な動作を実行します。
認証	人物またはプロセスの身元を検証することです。認証によって、デジタルデータ伝送が目的の受信者に確実に配信されます。また、受信者に対して、メッセージとメッセージ元が安全であることが保証されます。 認証の最も単純な形式では、特定のアカウントにアクセスするためにユーザ名とパスワードが要求されます。認証プロトコルは、DES (Data Encryption Standard) アルゴリズムなどの秘密鍵暗号方式、またはデジタル署名を用いる公開鍵システムを基にすることもできます。 「公開鍵暗号方式」および「デジタル署名」も参照してください。
ネットワークアドレス変換 (NAT)	セキュリティで保護された IP アドレスを、アドレスプールにある一時的な外部の登録 IP アドレスに変換するための規格です。これによって、非公開に IP アドレスが割り当てられた信頼するネットワークが、インターネットにアクセスできるようになります。つまり、ネットワーク内のすべてのコンピュータに対応する登録 IP アドレスを取得する必要はありません。
ネットワークウイルス	増殖するために、TCP、FTP、UDP、HTTP などのネットワークプロトコルやメールプロトコルを使用するウイルスの種類。ネットワークウイルスは、多くの場合、システムファイルの変更やハードディスクのブートセクタの改変は行いません。代わりに、クライアントコンピュータのメモリに感染し、ネットワークに大量のトラフィックを送りつけて、ネットワーク速度を遅くしたり、ネットワーク全体をダウンさせる可能性があります。
パーティション	ディスクを論理的に分割した部分です (ディスクを物理的に分割した部分である「セクタ」も参照してください)。

用語	説明
ハードディスク (またはハードドライブ)	関連する読み書きヘッドと電子機器が付属し、中心軸のまわりを回転する 1 つ以上の固定された磁気ディスクで、ハードディスクまたはフロッピーディスクの読み書きとデータの格納に使用されます。ほとんどのハードディスクは取り外せないようにドライブに接続されています（固定ディスク）。これ以外に、取り外しができるリムーバブルディスクもあります。
パスワードクラッカー	失効した、または忘れてしまったパスワードの回復に使用するアプリケーションプログラム。このようなアプリケーションは、侵入者がコンピュータまたはネットワークリソースに権限のないままアクセスするために使用される場合があります。
パターンファイル (オフィシャルパターンリリースとも呼ぶ)	パターンファイルはオフィシャルパターンリリース (OPR) とも呼ばれ、確認されたウイルスパターンファイルを最終的に編集したものです。パターンファイルは、最新のウイルス脅威を完全に防御するために、一連の厳しいテストに合格したことが保証されています。このパターンファイルは、最新の検索エンジンで使用すると最も効果的です。
ハッカー	「ウイルスの作成者」を参照してください。
ハッキングツール	攻撃される可能性があるセキュリティの脆弱性を見つけるために、コンピュータシステムやネットワークの侵入テストを可能にするハードウェアとソフトウェアなどのツールです。
ハブ	このハードウェアは、(通常は Ethernet 接続を介して) ネットワークコンピュータとともに使用されます。ハブは共通の配線ポイントとして機能し、情報が中央の 1 つの場所を通ってネットワーク上の他のコンピュータに流れるようにします。これによって、集中管理が可能となります。ハブは、Ethernet の物理層で信号をリピートするハードウェアデバイスです。ハブは標準的なバス型ネットワーク (Thinnet など) の動作を保ちますが、星型の中央にハブを配置するスター型トポロジを形成します。この構成によって集中管理が可能になります。
パラメータ	ある範囲の値（1 ～ 10 の数）などの変数です。
非武装地帯 (DMZ)	2 つの軍隊の間にある戦闘が行われていない領域を指す軍事用語が由来です。DMZ Ethernet は、異なる組織によって管理されるネットワークとコンピュータを接続します。DMZ Ethernet は、外部または内部の場合があります。外部 DMZ Ethernet は、ルータで地域ネットワークをリンクします。

用語	説明
ファイアウォール	特別なセキュリティ対策を施したゲートウェイコンピュータ。外部ネットワーク（特にインターネット）との接続やダイヤルイン回線のサービスに使用されます。
ファイルタイプ	ファイルに格納されているデータの種類です。大部分の OS では、ファイル名拡張子を使用してファイルタイプを判断します。ファイルタイプは、ユーザインタフェースでファイルを表す適切なアイコンや、ファイルを表示、編集、実行、または印刷する際に使用する適切なアプリケーションを選択するために使用されます。
ファイル感染ウイルス	ファイル感染ウイルスは、実行可能プログラム (通常、.com または .exe 拡張子を持つファイル) に感染します。このようなウイルスの大部分は、他のホストプログラムに感染して増殖しようとします。しかしウイルスによっては、オリジナルコードの一部を上書きして、感染したプログラムを不注意から破壊します。これらの少数のウイルスは非常に有害で、事前に設定された時間にハードドライブをフォーマットしようとしたり、不正な操作を実行しようとしたりします。 多くの場合、ファイル感染ウイルスは感染ファイルから正常に削除できます。ただし、ウイルスがプログラムのコードの一部を上書きした場合は、オリジナルファイルは復元できません。
ファイル名拡張子	ファイルに格納されるデータの種類を表すファイル名の一部 (.dll や .xml など) です。ファイルが保持するデータの種類をユーザに知らせるだけでなく、ファイル名拡張子は通常、ファイルの実行時に起動するプログラムを決定するために使用されます。
フィルタ基準	メッセージや添付ファイルが (もしあれば) 配信されるかどうかを判定するための、次のようなユーザ指定のガイドライン - メールの本文と添付ファイルのサイズ - メールの件名における単語または文字列の存在 - メールの本文における単語または文字列の存在 - 添付ファイルの件名における単語または文字列の存在 - 添付ファイルのファイルタイプ
不快なコンテンツ	みだらな言葉、性的な嫌がらせ、人種上の嫌がらせ、嫌がらせのメールなどの他人を不快にさせるメッセージや添付ファイル中の単語または字句です。
複合的な脅威による攻撃	「Nimda」または「Code Red」など、企業ネットワークの複数の侵入ポイントや脆弱性を利用する複合型の攻撃です。

用語	説明
複合感染型ウイルス	システム領域感染型ウイルスとファイル感染型ウイルスの両方の特徴を持つウイルスです。
不正プログラム (不正ソフトウェア)	ウイルス、ワーム、トロイの木馬などのように、危害を与えることを目的として開発されるプログラムまたはファイルです。
ブラウザ	Internet Explorer などのハイパーテキストの読み取りを可能にするプログラムです。ブラウザを使用すると、ノード (ページ) のコンテンツを表示したり、1 つのノードから別ノードに移動することができます。ブラウザは、リモート Web サーバに対するクライアントのように動作します。
プロキシ	アクセスに時間または費用がかかる可能性がある他のサーバで利用可能なアイテムのキャッシュを提供するプロセスです。
プロキシサーバ	特殊な接頭辞がついた URL を受け入れる WWW サーバ。ローカルキャッシュまたはリモートサーバのいずれかから文書を取得するために使用され、その URL を要求元に返します。
ブロック	ネットワークへの侵入を防ぐことです。
ブロックする送信者	ネットワークへのメッセージの送信が許可されない送信者です。
ペイロード	感染したコンピュータ上でウイルスが実行する処理のこと。ウイルスの処理には、メッセージの表示や CD ドライブの取り出しなどの比較的害が少ないものと、ハードディスクドライブ全体の削除などの破壊的なものがあります。
ポート	通信システム内の論理チャネルまたはチャネルのエンドポイント。同じコンピュータ上の同じネットワークインタフェース上にある異なる論理チャネルを区別するために使用されます。各アプリケーションプログラムには、一意のポート番号が関連付けられています。
ホスト	ネットワークに接続されたコンピュータです。
マクロ	アプリケーションの特定の機能を自動化するためのコマンドです。
マクロウイルス	マクロウイルスは、多くの場合アプリケーションマクロとしてエンコードされ、文書内に含まれています。他の種類のウイルスと異なり、OS に固有なものではなく、メールの添付ファイル、Web のダウンロード、ファイル転送、連携アプリケーションを介して拡大します。
マスメーリング型 (ワームとも呼ぶ)	大量のネットワークトラフィックを発生させるため、深刻な被害を及ぼす可能性の高い不正なプログラムです。

用語	説明
メッセージ	メッセージヘッダおよびメッセージ本文にメッセージ件名を含むメールメッセージです。
メッセージキュー	検索を待機するメッセージ数です。
メッセージサイズ	メッセージとその添付ファイルが占める KB または MB の値です。
メッセージの件名	「第 3 四半期の結果」または「金曜日のランチ」などのメールメッセージのタイトルまたはトピックです。
メッセージ本文	メールメッセージの内容です。
ライセンス	トレンドマイクロ製品を使用するための法的な許可です。
リモートアクセスツール (RAT)	正当なシステム管理者がネットワークをリモートで管理できるようにする、ハードウェアおよびソフトウェアのことです。ただし、このようなツールは、侵入者がシステムのセキュリティを突破しようとして使用する場合もあります。
リレー	他のさまざまなポイントを経由して伝送することです。
リレー対策	ホストが別のホストのネットワークを介したピギーバッキングを行わないようにするメカニズムです。
リンク (ハイパーリンクとも呼ぶ)	あるハイパーテキスト文書内の任意の点から別の文書内の任意の点または同じ文書内の別の場所への参照。リンクは通常、下線付きの青色のテキストなど、異なる色や異なるテキストのスタイルによって区別されます。マウスでクリックするなどでリンクをアクティブにすると、ブラウザはリンク先を表示します。
ルータ	このハードウェアデバイスは、ローカルエリアネットワーク (LAN) から電話回線の長距離回線にデータを配信します。ルータはトラフィックの監視役としても動作し、許可されたコンピュータのみがデータをローカルネットワークに送信できるようにし、非公開の情報を安全を維持できます。ルータは、これらのダイヤルインおよびリースによる接続のサポートに加え、エラーの処理、ネットワーク使用率の統計の維持、セキュリティ問題の処理も行います。

用語	説明
ルールベースのスパムメール検出	メールメッセージをスパムメールと考えるかどうかを判断するための、メッセージ特質のヒューリスティック評価に基づくスパムメール検出です。スパムメール対策エンジンがメールメッセージを検査するときは、メールの内容とルールファイルのエントリとを比較して一致があるかどうか検索します。ルールベースのスパムメール検出は、シグニチャベースのスパムメール検出よりも高い検出率を有しますが、誤検出率も高くなっています。 「シグニチャベースのスパムメール検出」も参照してください。 「誤検出」も参照してください。
レジストレーションキー	ハイフン (-) を含む 22 桁の英数字で構成されるコード。トレンドマイクロの顧客データベースに登録するために使用されます。レジストレーションキーの例 : SM-27RT-UY4Z-39HB-MNW8 「アクティベーションコード」も参照してください。
ローカルエリアネットワーク (LAN)	Ethernet など、オフィス環境内のリソースを通常は高速で相互接続するネットワーク技術です。ローカルエリアネットワークは、1 つの建物内でコンピュータのグループを接続するために使用される短距離ネットワークです。10BaseT Ethernet は、最も一般的に使用される LAN の形式です。ハブと呼ばれるハードウェアデバイスが共通の配線ポイントとして機能し、ネットワーク経由でデータをコンピュータからコンピュータへ送信できるようにします。LAN は通常、500m 未満の距離に制限されており、地理的に狭い領域において、低価格で広帯域幅のネットワーク機能を実現します。
ロードバランシング	ロードバランシングは、並列演算処理の効率を向上させることを目的として、複数のプロセッサに作業をマッピング (または再マッピング) することです。
論理爆弾	アプリケーションまたは OS に密かに挿入されたコード。指定された条件と一致するたびに、コードは破壊活動やセキュリティの脅威となる活動を実行します。
ワークステーション (クライアントとも呼ぶ)	一度に 1 人が使用するように設計された汎用コンピュータ。通常はパーソナルコンピュータよりも高いパフォーマンスを実現します。特にグラフィックスにおいて、同時に複数のタスクを実行できる処理能力と機能が優れています。
ワーム	他のプログラムに寄生しないプログラム (またはプログラムセット) で、自身の機能のコピーやそのセグメントを別のコンピュータに広めることができます。

用語	説明
ワイルドカード	コンテンツフィルタに関連して使用され、アスタリスク（*）が任意の文字を表します。たとえば、*ber という表現は、barber、number、plumber、timber などを表します。この用語の由来はカードゲームです。カードゲームでは、「ワイルドカード」とされる特定のカードを、カードデッキにある任意の数字またはトランプマークの代わりに使用できます。