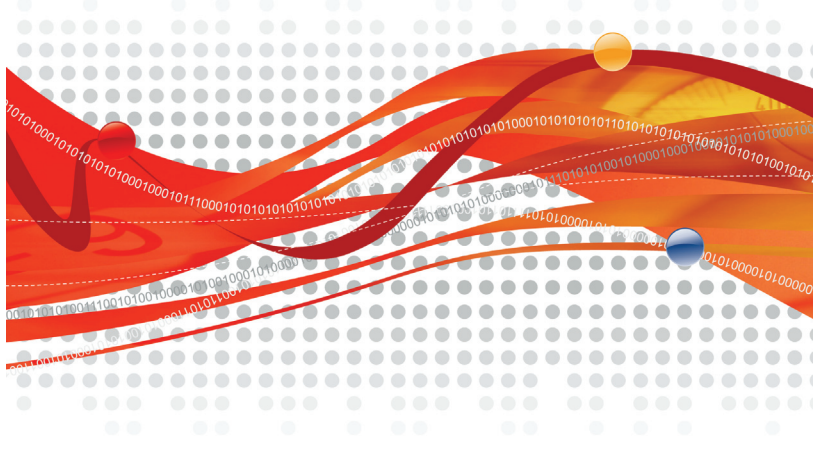
Trend Micro
InterScan VirusWall™
スタンダードエディション



安心を、ひとつ上のステージへ。

TREND MICRO™

クイックスタートガイド

※注意事項

トレンドマイクロへのお客様情報の送信について

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

輸出規制について

本製品は、外国為替及び外国貿易法、U.S. Export Administration Regulations、およびその他の国における輸出規制品目に該当している場合があります。したがって、本製品が輸出規制品目に該当する場合、適正な政府の許可なくして、禁輸国もしくは貿易制裁国の企業、居住者、国民、または、取引禁止者、取引禁止企業に対して、輸出もしくは再輸出できません。このような規制についての情報は以下のWebサイトから見つけることができます。
「http://www.treas.gov/offices/enforcement/ofac/」および「http://www.bis.doc.gov/complianceandenforcement/ListsToCheck.htm」
2009年7月現在、米国により定められる禁輸国は、キューバ、イラン、北朝鮮、スーダン、シリアが含まれています。
あなたは本製品に関連した米国輸出管理法令の違法行為に対して責任があります。本契約の同意により、あなたは、あなたが米国により現時点で禁止されている国の居住者もしくは国民ではないこと、別途本製品を受け取ることが禁止されていないことを確認します。また、大量破壊を目的とした、核兵器、化学兵器、生物兵器、ミサイルの開発、設計、製造、生産を行うために使用しないことに同意します。

複数年契約について

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

著作権について

商標について

P/N: ISSENT-AE0104 (2009/10)

目次

はじめに

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 インストールのセットアップ、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

この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「製品の概要」では、InterScan VirusWall の概要、機能と利点、および新機能について説明します。
- 第 2 章「インストールの計画」では、インストール計画、システム要件、およびインストール前のタスクについて説明します。
- 第 3 章「インストール」では、インストールおよび移行の手順について説明します。
- 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。

InterScan VirusWall のドキュメント

このクイックスタートガイドの他に、InterScan VirusWall には次のドキュメントが用意されています。

- **管理者ガイド** — 製品の設定やトラブルシューティングなど、InterScan VirusWall の管理に関する詳細な解説書です。
- **オンラインヘルプ** — オンラインヘルプの目的は、製品の主要なタスク、使用方法のヒント、および有効なパラメータ範囲や最適値などの実際の運用環境特有の情報を提供することです。オンラインヘルプは、InterScan VirusWall の Web コンソールからアクセスできます。
- **Readme ファイル** — オンラインドキュメントやマニュアルにはない最新の製品情報が記載されています。新しい機能、インストールのヒント、既知の問題、およびリリースの履歴などについて説明します。

  クイックスタートガイド、管理者ガイド、および Readme ファイルの最新版は次の Web サイトからダウンロードできます。

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

- **製品 Q&A** — 問題の解決方法やトラブルシューティング情報を集めたオンラインデータベースです。製品の既知の問題に関する最新情報が提供されています。製品 Q&A には、次の Web サイトからアクセスできます。

  `http://esupport.trendmicro.co.jp/`

対象読者

InterScan VirusWall のドキュメントは、以下を含むセキュリティシステムについて基本的な知識があることを前提としています。

- HTTP および FTP プロトコル
- データベース構造

ウイルス対策や Web セキュリティテクノロジに関する知識は必要ありません。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

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

表 1.　本書で使用している表記規則

第 1 章

製品の概要

Trend Micro InterScan VirusWall スタンダードエディション (以下、InterScan VirusWall) は、企業ネットワークのゲートウェイウイルス対策、スパムメール対策、およびコンテンツ管理の機能を提供するオールインワンのソリューションです。ウイルス対策、スパムメール検出、またはコンテンツフィルタのためにアプリケーションを個々にインストールする必要はありません。使いやすい 1 つのアプリケーションでこれらの機能をすべて利用できます。

- InterScan VirusWall のリアルタイム検索サービス (SMTP VirusWall、POP3 VirusWall、FTP VirusWall、および HTTP VirusWall) では、メールや Web、ローカルエリアネットワーク (LAN) でのファイル転送におけるセキュリティの脅威がチェックされます。
- InterScan VirusWall では、SMTP および POP3 トラフィックに対するヒューリスティック方式によるスパムメール対策とコンテンツ検索を利用できます。
- InterScan VirusWall は、容易にセットアップできるように設定が簡素化され、毎日の保守を最低限に抑えられるので、時間や IT リソースが限られ、リアルタイムのウイルス / スパムメール予防サービスを必要とする管理者に特に有用です。

機能と利点

InterScan VirusWall の機能および利点は、次のとおりです。

表 1-1. InterScan VirusWall の機能と利点

機能	説明
オールインワンの防御	ウイルス対策、スパムメール対策、スパイウェア / グレーウェア対策、フィッシング対策、IntelliTrap (ボット対策)、コンテンツフィルタ、大規模感染予防サービス、URL ブロック、URL フィルタ、および SMTP 用メールレピュテーション IntelliTrap は、リアルタイム、ルールベース、およびパターン認識の検索エンジンのテクノロジです。IntelliTrap は、最大で 20 階層の深さまで圧縮された、16 の主要な圧縮形式のファイルで既知のウイルスを検出して削除します。
自動的な脅威対策	簡単で使いやすい大規模感染予防による全面的な保護
スケーラビリティ	4 つの全サービスを 1 つのサーバにインストールするか、または複数のサーバに分散インストールするかを選択することにより、中小企業にも大企業にも適した配置が可能
ゲートウェイ保護	インターネットゲートウェイでの不正プログラムの予防
柔軟な設定	検索対象ファイル、感染ファイル / メッセージに対する処理、および感染ファイル / メッセージの通知メッセージの受信者を指定可能
集中管理	全社的なインターネットセキュリティポリシーを実施する、ローカルシステムまたはリモートシステムからアクセス可能な Web ベースのコンソール
自動的な保守	導入先固有のニーズを満たすように設定し自動化された、アップデート、レポート、警告などのタスク

表 1-1. InterScan VirusWall の機能と利点 (続き)

機能	説明
簡単なインストール	インストールウィザードがインストールおよび一部の設定タスクを簡素化 InterScan VirusWall のセットアッププログラムには、同時にインストールされるすべての製品のシステム要件、ディスク容量要件、必要な Service Pack または Patch、実行する必要があるサービス、および使用可能である必要のあるポートに関して、他のトレンドマイクロ製品およびサードパーティ製コンポーネントとの互換性を確認する機能が追加されました。この機能を使用すると、InterScan VirusWall は、体験版環境で他の製品と共存できるようになります。
ローカルレポート	レポートでは、多くの種類のトラフィック違反の概要を示すことができるようになりました。レポートには、発生したウイルスおよびウイルスの発生日時と場所が含まれます。レポートに、指定した期間内に違反が生じたユーザを、違反の種類と頻度と共に含めることもできます。InterScan VirusWall では、SMTP、HTTP、POP3、および FTP プロトコルについてレポートを生成できます。レポートを予約することも、1 回限りのレポートを生成することもできます。
InterScan VirusWall 6.0、6.02 ユーザ向けの移行ツール	InterScan VirusWall 6.0、6.02 のユーザは、InterScan VirusWall 7.0 へのアップグレード時に設定を簡単に移行できます。

新機能

InterScan VirusWall は最新の不正プログラム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、スパイウェア、グレーウェア、ボット、およびフィッシングへの対策、URL フィルタおよび URL ブロック、および大規模感染予防サービスによる保護などがあります。

バージョン 7.0 の新機能のリスト

新機能	説明
Web レピュテーションを使用したフィッシング対策	本製品には、Web レピュテーション、URL フィルタ、およびフィッシングパターンファイルを使用したフィッシング対策が用意されています。Web レピュテーションでは、新たな Web からの脅威に対してエンドユーザが保護されます。また、Web レピュテーションでは、評価スコアが URL に割り当てられます。アクセスされる URL ごとに、Web レピュテーションで評価スコアがクエリされ、このスコアがユーザ指定の検出レベルより上か下かによって、その URL へのアクセスの許可やブロック、またはウイルス検索の実行が決定されます。
Windows ユーザ / グループのサポート (ドメインコントローラエージェントおよび サーバを使用したユーザの識別)	ユーザ ID 設定では、InterScan VirusWall 経由で HTTP 接続を行っている組織内の個々のユーザおよびグループを識別できます。トレンドマイクロのドメインコントローラエージェントは、Windows ベースのディレクトリサービスでユーザに透過的なユーザ識別を提供します。ドメインコントローラエージェントは、ドメインコントローラサーバと通信し、最新のユーザログオン情報を収集して InterScan VirusWall に提供します。この情報は、特定のユーザおよびグループに適用される URL フィルタおよび URL ブロックのポリシーの作成に使用できます。
ユーザ / グループベースの URL ブロックおよび URL フィルタのポリシー設定	URL ブロックおよび URL フィルタのルールを、特定のコンピュータ、ユーザ、またはグループに適用できます。InterScan VirusWall は、ネットワーク内の Active Directory サーバと通信するドメインコントローラエージェントと呼ばれるプラグインを使用して、ポリシーを設定できるユーザまたはグループを特定します。この機能には、ID 設定、Microsoft Active Directory サービスのサポート、ポリシーアイテムの管理、およびユーザまたはグループ単位のログおよびレポートが含まれます。

バージョン 7.0 の新機能のリスト

新機能	説明
改善されたレポート作成機能	レポートでは、多くの種類のトラフィック違反の概要を示すことができるようになりました。レポートには、発生したウイルスおよびウイルスの発生日時と場所が含まれます。レポートに、指定した期間内に違反が生じたユーザを、違反の種類と頻度と共に含めることもできます。InterScan VirusWall では、SMTP、HTTP、POP3、および FTP プロトコルについてレポートを生成できます。レポートを予約することも、1 回限りのレポートを生成することもできます。
インストール時のシステム要件確認機能	InterScan VirusWall のセットアッププログラムには、同時にインストールされるすべての製品のシステム要件、ディスク容量要件、必要な Service Pack または Patch、実行する必要があるサービス、および使用可能である必要のあるポートに関して、他のトレンドマイクロ製品およびサードパーティ製コンポーネントとの互換性を確認する機能が追加されました。この機能を使用すると、InterScan VirusWall は、体験版環境で他の製品と共存できるようになります。
以前のバージョンからの容易な移行	バージョン 6.0 または 6.02 から本バージョンへ簡単に移行できます。
Trend Micro Control Manager 5.0 のサポート	Trend Micro Control Manager 5.0 がサポートされます。

第 2 章

インストールの計画

Trend Micro InterScan VirusWall スタンダードエディション (以下、InterScan VirusWall) をインストールし設定して、物理ネットワークのさまざまなセットアップをサポートできます。InterScan VirusWall は、容易にセットアップできるように設定が簡素化され、毎日の保守を最低限に抑えられるので、時間や IT リソースが限られ、リアルタイムのウイルス / スパムメール予防サービスを必要とする管理者に特に有用です。

この章では、インストール計画、システム要件、インストール前に実行する必要があるタスクについて説明します。

インストールの概要

InterScan VirusWall のゲートウェイ用アプリケーションには、LAN との間のメール (SMTP と POP3)、Web (HTTP)、およびファイル転送 (FTP) のウイルスを調べるリアルタイム検索サービスが含まれています。

すべてのサービスを同一コンピュータにインストールできます。ただし、通常は、複数のサービスを同一サーバでアクティブにしないことをお勧めします。サーバの通常の動作に加え、リアルタイムでネットワークトラフィックストリームを検索すると、CPU およびディスクへの負担が大きくなる可能性があるためです。セットアップを数回繰り返し実行して InterScan VirusWall を複数のサーバにインストールしてから、各サーバの各サービスをアクティブにする方法がより一般的です。たとえば、セットアップを 1 回実行して SMTP サービスと POP3 サービスを SMTP サーバでアクティブにし、セットアップをもう一度実行して HTTP サービスを別の HTTP プロキシサーバでアクティブにし、さらにセットアップを実行して、FTP サービスを別の FTP サーバでアクティブにします。

システム要件

注意： 詳細は、弊社の「最新版ダウンロード」サイトにある最新の Readme を参照してください。

ドメインコントローラエージェントの要件

表 2-1. ドメインコントローラエージェントの要件

要件	説明
ドメインコントローラエージェント	• ドメインコントローラエージェントを実行するよう指定されたコンピュータ (ドメインコントローラサーバと同じ OS 上で実行することをお勧めします)。 • ドメインコントローラエージェントのコンピュータは Windows ドメインに属している必要があります。 • ドメインコントローラエージェントコンピュータで、TCP ポート 65015 上の受信トラフィックを許可するようにファイアウォールを設定する必要があります。

表 2-1. ドメインコントローラエージェントの要件 (続き)

要件	説明
ドメインコントローラサーバ	• Active Directory がインストールされている Windows 2000、2003、または 2008 プラットフォーム。 • ドメインコントローラサーバのログオンイベントの監査を有効にします。 1. [スタート] → [コントロール パネル] → [管理ツール] の順に選択します。 2. [ドメイン コントローラ セキュリティ ポリシー] をクリックします。 3. 左側の画面で [ローカル ポリシー] を開き、[監査ポリシー] を選択します。 4. [アカウント ログオン イベントの監査] が有効になっていることを確認します。 管理者ガイドの「トラブルシューティングとサポート」の章を参照してください。 • ドメインコントローラサーバのセキュリティログのログローテーション / リサイクルを有効にします。 1. [スタート] → [コントロール パネル] → [管理ツール] の順に選択します。 2. [イベント ビューア] をクリックします。 3. 左側の画面で [イベント ビューア] を開き、[セキュリティ] を選択します。 4. [操作] → [プロパティ] の順に選択して、[セキュリティのプロパティ] 画面を開きます。 5. ログサイズが適切に設定されていて、[イベントを上書きする] オプションが選択されていることを確認します。 • ドメインコントローラサーバにファイアウォールが設定されている場合は、RPC およびリモートイベントアクセス用に TCP ポート 135 および TCP ポート 445 で受信トラフィックを許可するように除外を設定します。
InterScan VirusWall	• InterScan VirusWall のユーザ ID 設定を IP アドレスおよびユーザ名に設定します (管理者ガイドの「管理」の章を参照してください)。 • ドメインコントローラエージェントコンピュータの IP アドレス。 • ドメイン管理者権限のあるユーザアカウント。

表 2-1. ドメインコントローラエージェントの要件 (続き)

要件	説明
Windows クライアント	• クライアントコンピュータで実行されているリモートレジストリサービス。 • ドメインアカウントを使用したログオン。 • ファイアウォールが設定されている場合は、TCP ポート 445 で受信 RPC トラフィックを許可するように除外を設定します。

事前計画

初期設定では、InterScan VirusWall は、処理する SMTP メッセージの受信にポート 25、HTTP プロキシにポート 8080、FTP プロキシサーバにポート 21、POP3 受信メッセージにポート 110 をそれぞれ使用します。

インストールされているサービスおよびシステムで使用しているプロキシサーバに応じて、次の情報の把握が必要な場合があります。

- 現在の SMTP サーバの IP アドレス
- 現在の SMTP サーバのポート番号 (通常は 25)
- 現在の POP3 サーバの IP アドレス
- 現在の POP3 サーバのポート番号 (通常は 110)
- 現在の HTTP プロキシサーバの IP アドレス (設定する場合)
- 現在の HTTP プロキシサーバのポート番号
- 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 (設定する場合)
- 現在の FTP プロキシサーバのポート番号
- 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

インストール先を決定する

InterScan VirusWall は、元のサーバと同じコンピュータにインストールすることも、別のコンピュータにインストールすることもできます。ほとんどの場合、インストール先を決めるうえで最も重要な点は、追加負荷を適切に処理できるだけの十分なリソースがインストール先のコンピュータにあるかどうかということです。

InterScan VirusWall をインストールする前に、サーバで処理するピークトラフィック負荷と平均トラフィック負荷を評価し、結果をコンピュータ全体の能力と比較する必要があります。両者の測定値が近いほど、InterScan VirusWall を専用コンピュータにインストールする可能性が大きくなります。考慮する別の要素として、ネットワーク帯域幅、現在の CPU 負荷、CPU 速度、システムメモリの総容量と使用可能な容量、および仮想メモリスペースの総量があります。リアルタイムでウイルスのネットワークプロトコルを 1 つ以上検索すると、リソースを集中利用する可能性があります。追加負荷を処理する能力がないコンピュータには、InterScan VirusWall をインストールしないでください。

セットアップの選択

同じコンピュータ : InterScan VirusWall をメールサーバまたは Web サーバと同じコンピュータにインストールする際、ほとんどの場合に、元のサーバが使用するポートの変更と InterScan VirusWall での初期設定の使用が必要になります。

通常の初期設定は次のとおりです。FTP: 21、SMTP: 25、HTTP:80、POP3: 110

専用コンピュータ : InterScan VirusWall が検索するサーバとは別のコンピュータに InterScan VirusWall をインストールする場合、既存サーバのポート番号を変更する必要はありません。ただし、InterScan VirusWall コンピュータの新しい IP アドレス (またはホスト名) を反映するようにクライアントの変更が必要になる場合があります。クライアントを変更しない場合は、次の点を検討してください。

- 2 台のコンピュータ間で IP アドレス (またはホスト名) を入れ替えて、InterScan VirusWall で元の IP アドレス (またはホスト名) を使用できるようにします。
- 論理上、インターネット、メールサーバ、および HTTP プロキシサーバの中間になるように InterScan VirusWall をインストールします。

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。これらのトポロジは、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、複数のサーバで InterScan VirusWall インストールを実行して各サーバ上の目的のサービスだけを有効にする、スタンドアロンまで多岐にわたります。

想定されるトポロジには次のようなものがあります。

- 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
- メッセージング /Web 配置 :
  - メッセージングサーバの場合は、InterScan VirusWall を別のハードウェアにインストールし、インストール時に SMTP および POP3 ウイルス検索を有効化
  - Web セキュリティ配置の場合は、InterScan VirusWall のインストール時に HTTP および FTP ウイルス検索オプションを有効化
- 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

以降のページでは、InterScan VirusWall のインストール前後の一般的なネットワークセットアップを示しながら、想定されるいくつかのインストールトポロジを説明します。ニーズに最適なトポロジを使用するか、ここで説明する方法を応用してお使いのネットワークに固有のインストールを計画してください。

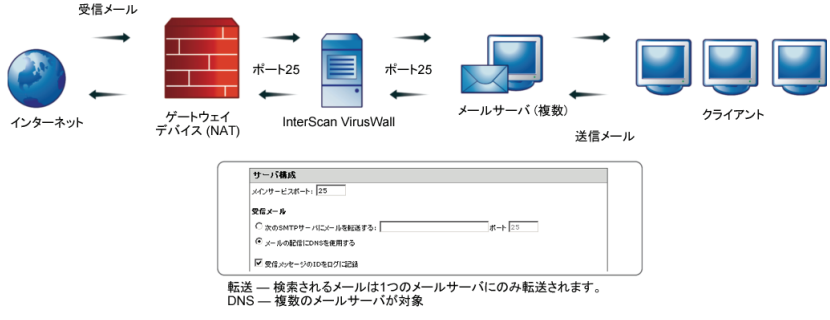
SMTP

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、受信メール転送 (シングルサーバ環境) または DNS (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。DNS を使用する場合は、内部 MX レコードが正しく設定されていることを確認します。

これらの作業で、内部メールサーバの IP アドレスを変更する必要はありません。また、クライアントコンピュータではそれぞれのメールサーバへの接続が継続されるため、これらのコンピュータの設定も変更不要です。

InterScan VirusWall のインストール前

InterScan VirusWall のインストール後 (InterScan VirusWall とメールサーバを異なるコンピュータにインストール)



InterScan VirusWall のインストール後 (InterScan VirusWall とメールサーバを同じコンピュータにインストール)

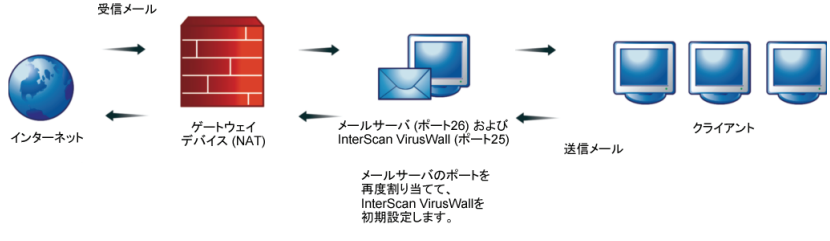


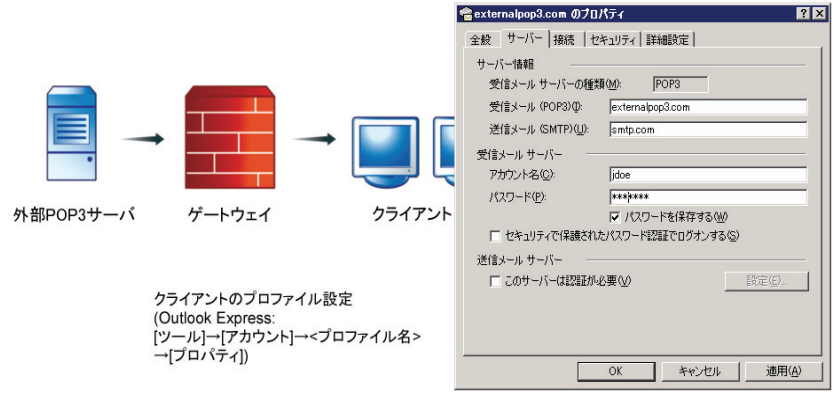
図 2-1. SMTP インストールトポロジ

POP3

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。クライアントのメールボックス名を { メールボックス名 } {POP3 サーバ } { ポート番号 } に変更します。

たとえば、「joedoe」から「joedoe#externalpop3.com#110」に変更します。

InterScan VirusWall のインストール前



InterScan VirusWall のインストール後

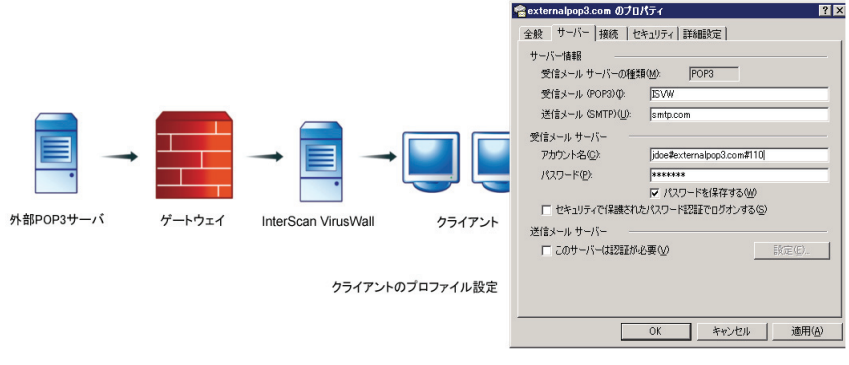


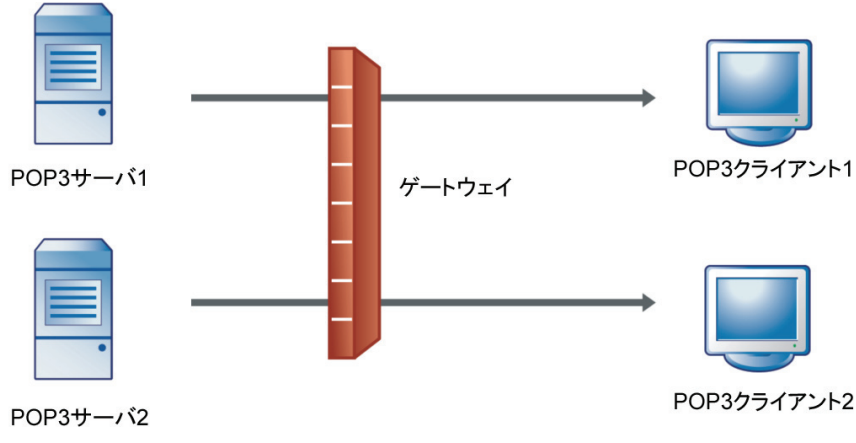
図 2-2.　標準的な POP3 インストールトポロジ

POP3 (ポートマッピング)

InterScan VirusWall をポートマッピングサーバとして設定する場合、ポートは InterScan VirusWall および特定の POP3 サーバの待機ポートにマップされます。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。

InterScan VirusWall のインストール前



InterScan VirusWall のインストール後

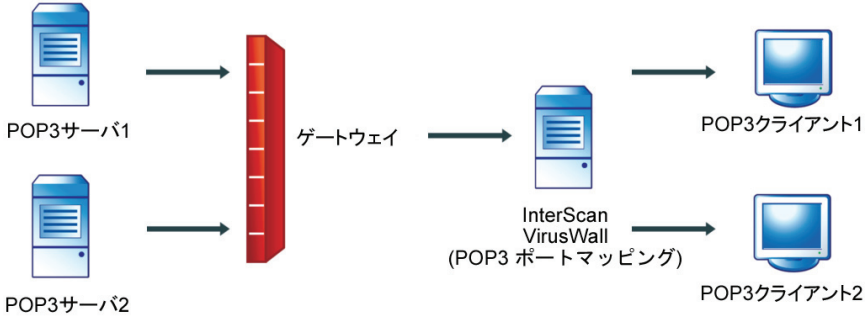


図 2-3. InterScan VirusWall がポートマッピングサーバとして機能する POP3

FTP

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。指定された FTP サーバに FTP VirusWall 経由で接続するには、ユーザは次のように入力します。< ユーザ名 >@<FTP サーバ IP アドレス >:< ポート番号 >

依存プロキシモード (既存の FTP プロキシサーバと連動) 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、InterScan VirusWall の Web コンソールの [FTP] の [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。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。

InterScan VirusWall のインストール前 (プロキシサーバあり)

InterScan VirusWall のインストール後 (プロキシサーバあり)

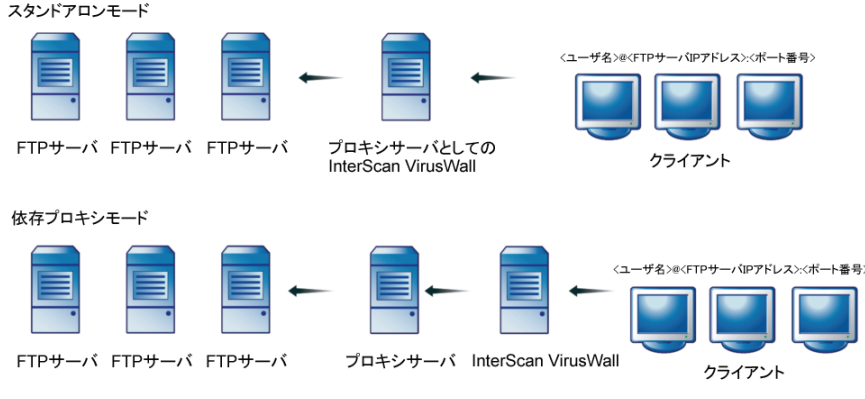
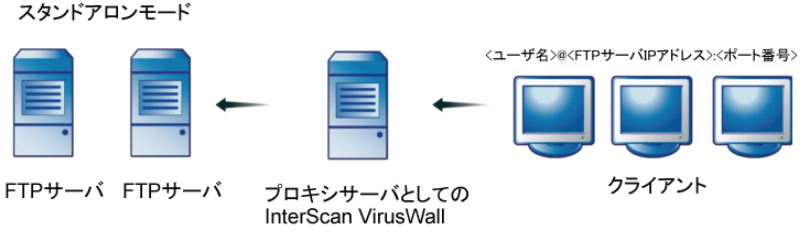


図 2-4. プロキシサーバを使用した FTP のインストールトポロジ

InterScan VirusWall のインストール前 (プロキシサーバなし)

InterScan VirusWall のインストール後 (プロキシサーバなし)



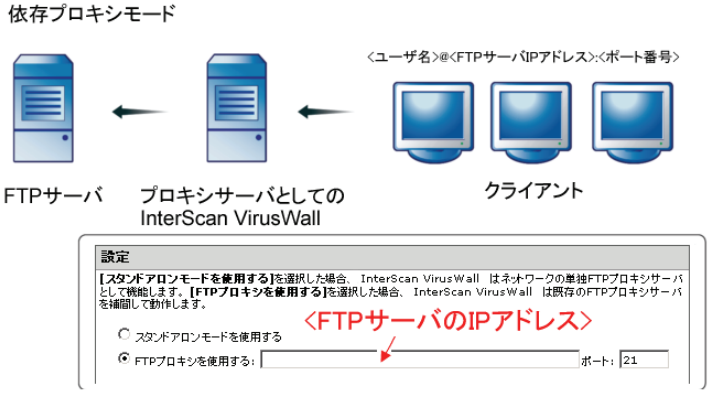


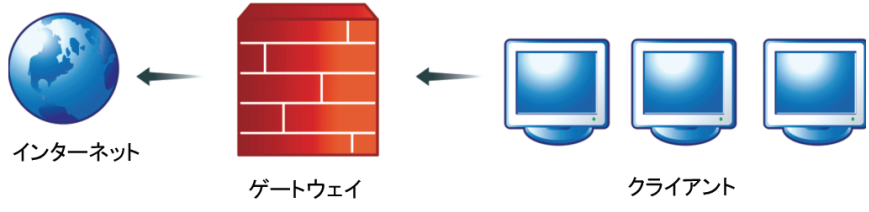
図 2-5. プロキシサーバを使用しない **FTP** のインストールトポロジ

HTTP

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、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。

依存プロキシモードの場合、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。

InterScan VirusWall のインストール前 (プロキシなし)



InterScan VirusWall のインストール後 (プロキシなし) スタンドアロンモード

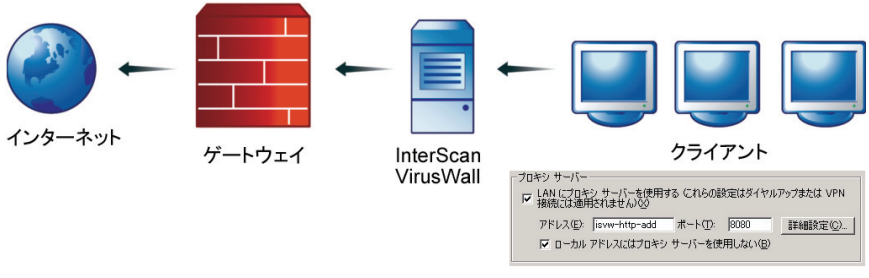
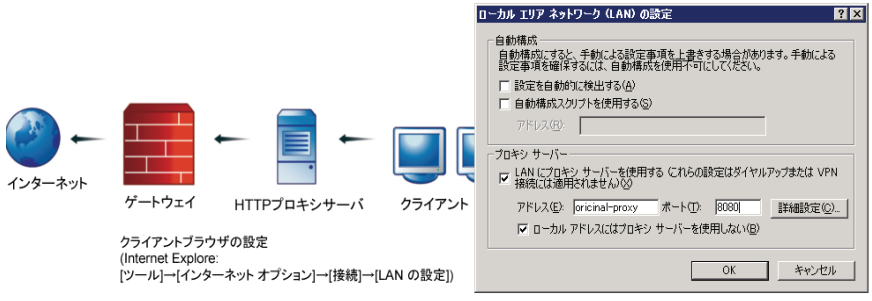


図 2-6. プロキシサーバを使用しない HTTP のインストールトポロジ (スタンドアロンモード)

InterScan VirusWall のインストール後、InterScan VirusWall を指すようにブラウザクライアントのプロキシ設定を変更する必要があります。

InterScan VirusWall のインストール前 (プロキシあり)



InterScan VirusWall のインストール後 (プロキシあり)

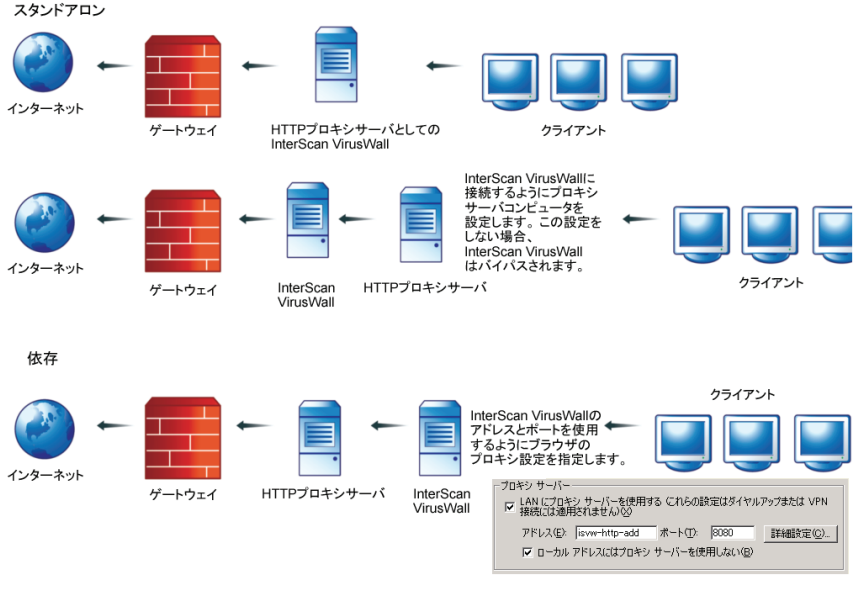
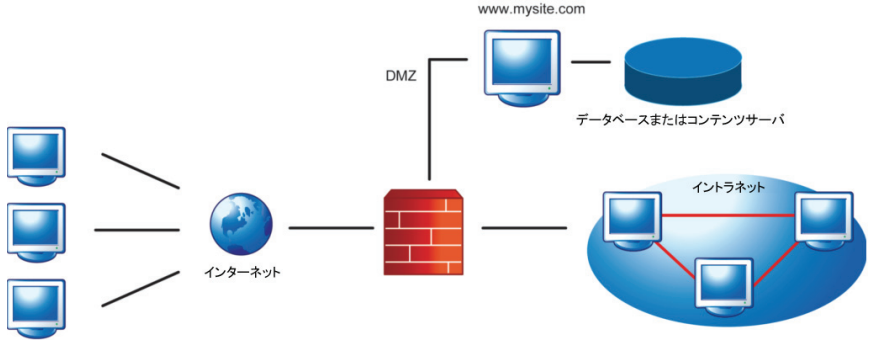


図 2-7.　プロキシサーバを使用した HTTP のインストールトポロジ (依存プロキシモード)

HTTP リバースプロキシ

リバースプロキシ配置では、内部および外部の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。

InterScan VirusWall のインストール前



InterScan VirusWall のインストール後

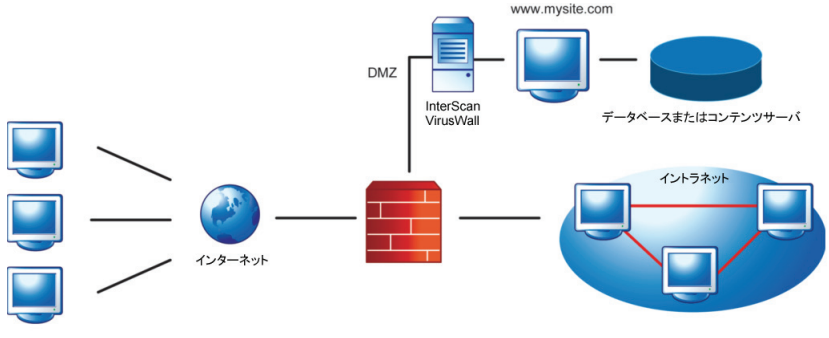


図 2-8.　InterScan VirusWall をリバースプロキシとして使用した HTTP のインストールトポロジ

InterScan VirusWall のインストール前の作業

1. InterScan VirusWall をインストールするコンピュータで、ウイルス対策製品やスパイウェア対策製品など、リアルタイム検索を実行している他の製品を削除します。製品の削除を望まない場合は、その製品の検索除外リストに次の事項を追加します。
   - InterScan VirusWall のインストール先のパス
   - SMTP、POP3、HTTP、および FTP プロトコルの隔離パス
   - Windows の Temp フォルダ
2. 管理者権限でコンピュータにログオンします。
3. InterScan VirusWall で使用する次の初期設定のポート番号が使用されていないことを確認します。
   - SMTP: 25
   - POP3: 110
   - HTTP: 8080
   - FTP: 21

   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。
4. InterScan VirusWall を初めてインストールする場合、および SMTP を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、これらのドメインにアドレス指定された受信メールだけを配信します。

第 3 章

インストール

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する必要があります。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 ～ 15 分を必要とします。

この章では、InterScan VirusWall をインストールするための手順を示します。また、本バージョンに移行する手順についても説明します。移行は次のバージョンについてサポートされています。

- InterScan VirusWall 6.0 または 6.02

この章に必要な情報が記載されていない場合は、管理者ガイドを参照してください。

インストールシナリオ

InterScan VirusWall をセットアップするには、セットアップファイルを起動して InstallWizard の指示に従います。

次のインストールシナリオを利用できます。

- 34 ページの「InterScan VirusWall を新規インストールする」

  InterScan VirusWall を初めてインストールする場合は、この手順を使用します。

- 「以前のバージョンがインストールされているコンピュータにインストールする」

  InterScan VirusWall 6.0 または 6.02 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、以前のバージョンの設定を本バージョンに移行するときは、この手順を使用します。

- 「新しいコンピュータにインストールして以前のバージョンの設定を移行する」

  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、以前のバージョンの InterScan VirusWall がインストールされている別のコンピュータから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 6.0 または 6.02 の設定を移行し、インストール時にインポートできます。

- 「以前のバージョンからのコマンドラインによる移行」

  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、以前のバージョンの InterScan VirusWall がインストールされているコンピュータからコマンドラインを使用して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以前のバージョンの設定を移行し、インストール時にインポートします。

InterScan VirusWall を新規インストールする

新規インストール時の URL ブロックおよびフィルタのグローバルポリシーについては、インターネットセキュリティグループに対して初期設定で 12 のカテゴリが選択されます (管理者ガイドを参照)。

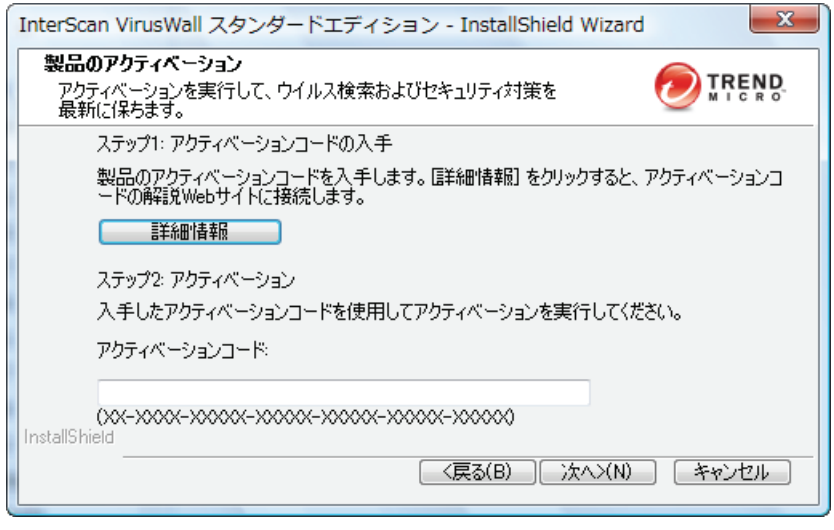
InterScan VirusWall を新規インストールするには

1. `setup.exe` をダブルクリックしてインストールプロセスを開始します。
2. 開始ウィンドウが表示されたら、[次へ] をクリックします。
3. [使用許諾契約] 画面で、契約書全体をよく読み、[使用許諾契約の内容に同意します] を選択して、インストールを続行します。

画面上で契約書全体をスクロールするか、または契約書を印刷できます。 [使用許諾契約の内容に同意しません] を選択すると、インストールプロセスは終了します。

4. [セットアップの種類] 画面で、[新規インストール] を選択して [次へ] をクリックします。
5. 図 3-1 の [製品のアクティベーション] 画面で、以下のいずれかの手順を実行します。
   - [アクティベーションコード] テキストボックスに製品のアクティベーションコードを入力して [次へ] をクリックします。
   - アクティベーションコードを入力しないで [次へ] をクリックします。

図 3-1. [製品のアクティベーション] 画面



アクティベーションコードを入力しないで [次へ] をクリックすると、情報が不足していることを警告するメッセージと、30 日間有効の InterScan VirusWall 体験版がインストールされることを通知するメッセージが表示されます。[OK] をクリックしてインストールを続行します。

[インストール先フォルダの指定] 画面が表示され、InterScan VirusWall のインストール先ディレクトリのパスを示します。

6. このインストール先のパスを変更する場合は、[参照] をクリックして別の場所を指定します。
7. 初期設定のパスを受け入れるか、新しいインストール先を選択したら、[次へ] をクリックします。
8. [Web コンソール URL の設定] 画面で、Web コンソールのバインド先を指定します。

   初期設定を図 3-2 に示します。

図 3-2.　[Web コンソール URL の設定] 画面

9. [次へ] をクリックします。
10. [管理者パスワードの設定] 画面で、4 ～ 32 文字のパスワードを入力して確認し、[次へ] をクリックします。
11. [検索サービスの設定] 画面で、インストール完了後に開始する InterScan VirusWall サービスを選択します。

    初期設定では、すべてのサービスが選択されています (図 3-3 を参照)。選択したら、[次へ] をクリックします。

図 3-3.　[検索サービスの設定] 画面

12. [リレー先の設定] 画面で、受信メールを受け入れるドメインを指定します。

    InterScan VirusWall では、これらのドメインにアドレス指定された受信メールだけが受け入れられます。

13. [HTTP Web レピュテーションの情報を送る] 画面で、感染 URL に関するフィードバックを匿名で送信するかどうかを指定し、[次へ] をクリックします。

14. [ウイルストラッキングセンターの設定] 画面で、ウイルストラッキングセンターに InterScan VirusWall で検出されたウイルスの情報を送信するかどうかを指定し、[次へ] をクリックします。

15. [設定の確認] 画面で、現在の設定を確認して、[次へ] をクリックします。

    設定を変更する場合は、[戻る] をクリックして前の画面に戻ります。

    [インストールステータス] 画面には、このソフトウェアのインストールの進行状況が表示されます。

16. [セットアップの完了] 画面で、Readme ファイルの表示または Web コンソールの起動を選択して　[終了] をクリックします。

    - Readme ファイルの表示を選択すると、新しいウィンドウで Readme ファイルが表示されます。
    - Web コンソールの起動を選択すると、Web ブラウザのウィンドウが自動的に開き、InterScan VirusWall のログオンページが表示されます。

アップグレードとして InterScan VirusWall をインストールする

InterScan VirusWall では、次の 2 種類のアップグレードがサポートされます。

- 以前のバージョンがインストールされているコンピュータにインストールする
- 新しいコンピュータにインストールして以前のバージョンの設定を移行する

これらのアップグレードシナリオの詳細については、管理者ガイドを参照してください。

以前のバージョンがインストールされているコンピュータにインストールする

セットアッププログラムでは、以前のバージョンの InterScan VirusWall 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の InterScan VirusWall をインストールできます。サポートされているバージョンは次のとおりです。

- InterScan VirusWall 6.0 または 6.02

> **注意：** InterScan VirusWall 7.0 のセットアッププログラムで InterScan VirusWall 6.0 または 6.02 が検出され、それらが同じ言語バージョンである場合、セットアッププログラムによりビルドのアップグレードを確認するようプロンプトが表示されます。InterScan VirusWall 7.0 のセットアッププログラムにより、InterScan VirusWall 6.0 または 6.02 が異なる言語バージョンであることが検出された場合、異なる言語バージョンをアンインストールしてから、インストールを続行するようにプロンプトが表示されます。

このアップグレードシナリオの詳細については、管理者ガイドを参照してください。

以前のバージョンがインストールされているコンピュータにインストールするには

1. `setup.exe` をダブルクリックしてインストールプロセスを開始します。
2. 開始画面が表示されたら、[次へ] をクリックします。
3. [使用許諾契約] 画面が表示されたら、契約書全体をよく読み、[使用許諾契約の内容に同意します] を選択して、インストールを続行します。
4. 以前のバージョンから設定を移行するには、[アップグレードインストール] チェックボックスをオンにします。

設定を移行する場合は、インストールの開始前に設定ファイルのバックアップを作成することをお勧めします。InterScan VirusWall のインストールプログラムによって以前のバージョンの InterScan VirusWall が完全に削除されます。

5. [次へ] をクリックします。
6. [製品のアクティベーション] 画面で、次のいずれかを選択します。
   - [アクティベーションコード] フィールドに製品のアクティベーションコードを入力して [次へ] をクリックします。
   - アクティベーションコードを入力しないで [次へ] をクリックします。

     アクティベーションコードを入力しないで [次へ] をクリックすると、情報が不足していることを警告するメッセージと、30 日間有効の InterScan VirusWall 体験版がインストールされることを通知するメッセージが表示されます。[OK] をクリックしてインストールを続行します。
7. このインストール先のパスを変更する場合は、[インストール先の指定] 画面に移動し、[参照] をクリックして別の場所を指定します。
8. 初期設定のパスを受け入れるか、新しいインストール先を選択したら、[次へ] をクリックします。
9. [Web コンソール URL の設定] 画面で、Web コンソールのバインド先を指定します。
10. [次へ] をクリックします。
11. [管理者パスワード] 画面で、4 ～ 32 文字のパスワードを入力して確認し、[次へ] をクリックします。
12. [検索サービスの設定] 画面で、インストール完了後に開始する InterScan VirusWall サービスを選択し、[次へ] をクリックします。
13. リレーされるメールをブロックするには、[リレー先の設定] 画面に移動して、受信メールを受け入れるドメインを [ドメイン名] フィールドで指定します。
14. [次へ] をクリックします。
15. Web レピュテーションデータベースの向上に役立てるため、[HTTP Web レピュテーションの情報を送る] 画面に移動し、このチェックボックスをオンにして、感染した URL についての匿名情報を送信してください。
16. [次へ] をクリックします。
17. [ウイルストラッキングセンターの設定] 画面で、ウイルストラッキングセンターに InterScan VirusWall で検出されたウイルスの情報を送信するかどうかを選択し、[次へ] をクリックします。
18. [設定の確認] 画面で現在の設定を確認して、[次へ] をクリックします。

[設定の確認] 画面で [次へ] をクリックすると、以前のバージョンの InterScan VirusWall がアンインストールされることを示すメッセージが表示されます。

19. [セットアップの完了] 画面で、Readme ファイルの表示、Web コンソールの起動、または移行レポートの表示を選択して [終了] をクリックします。

    インストールの開始時に移行レポートの作成を選択した場合は、[ファイル出力] をクリックします。レポートが新しいウィンドウで表示されます。

新しいコンピュータにインストールして以前のバージョンの設定を移行する

新しいコンピュータに本バージョンをインストールしたら、セットアッププログラムを使用して、以前のバージョンの InterScan VirusWall がインストールされている別のコンピュータから設定を移行できます。移行は次のバージョンについてサポートされています。

- InterScan VirusWall 6.0 または 6.02

本バージョンの InterScan VirusWall では、隔離ファイルをバージョン 6.0 および 6.02 の InterScan VirusWall から移行できます。この移行は、次の 2 つのシナリオのいずれかに該当します。

- 初期設定の隔離パスが変更されていない場合は、以前のバージョンの隔離ファイルが、本バージョンの InterScan VirusWall によって、その初期設定のパスのルートパスに移動されます。たとえば、InterScan VirusWall を `D:¥ISVW` にインストールして隔離ファイルの初期設定を変更しなかった場合は、本バージョンの InterScan VirusWall によって、`D:¥ISVW¥quarantine¥xxx` にあるすべての隔離ファイルが `D:¥Relocated_ISVW6_Quarantine_Folder¥xxx` に移動されます。さらに、本バージョンの InterScan VirusWall で使用される隔離パスは、元のインストールのまま維持されます。
- 初期設定の隔離パスを変更した場合は、InterScan VirusWall 6.0x の隔離ファイルは、本バージョンの InterScan VirusWall によって、新しい場所に移動されません。本バージョンの InterScan VirusWall によって生成された新しい隔離ファイルは、InterScan VirusWall 6.0x の場合と同じパスに保存されます。

注意： 以前のバージョンから本バージョンに設定を移行する際、インストールプログラムにより、URL フィルタのルールについて以前のバージョンで選択した URL カテゴリが移行されます。

新しいコンピュータにインストールしてバージョン 6.0x の設定を移行する

以前に InterScan VirusWall をインストールしたことがないコンピュータに本バージョンをインストールして、バージョン 6.0 または 6.02 がインストールされているコンピュータの設定を使用する場合は、その設定をファイルにエクスポートできます。このファイルはインストールプロセスで使用され、保存された設定がインストール先コンピュータにインポートされます。

本バージョンをインストールしてバージョン 6.0x の設定を移行するには

1. 移行ツールを見つけてコピーします。
   - InterScan VirusWall 6.0x から本バージョンに移行する場合、InterScan VirusWall 7.0 のインストールパッケージのディレクトリ < インストールパッケージ >¥other にある isvw-migr6to7.exe という名前のツールを見つけて、それを InterScan VirusWall 6.0x がインストールされているコンピュータにコピーしてください。
2. コマンドラインで次のように入力します。
   - InterScan VirusWall 6.0x から本バージョンに移行する場合 :
     `isvw-migr6to7 -o [< 移行設定ファイル名 >]`
     例 : `isvw-migr6to7 -o c:¥ISVW6-package.out`

   注意 : InterScan VirusWall 7.0 の移行ツールでは、絶対パス名と相対パス名の両方がサポートされています。

3. ネットワーク経由でこのファイルにアクセスできない場合は、< 移行設定ファイル名 > のファイルをリムーバブルメディアにコピーします。これにより、InterScan VirusWall をインストールするコンピュータでそのファイルにアクセスできます。
4. InterScan VirusWall をインストールするコンピュータで、setup.exe をダブルクリックしてインストールプロセスを開始します。
5. 開始画面が表示されたら、[次へ] をクリックします。
6. [使用許諾契約] 画面が表示されたら、契約書全体をよく読み、[使用許諾契約の内容に同意します] を選択して、インストールを続行します。
7. [セットアップの種類] 画面が表示されたら、[リモートコンピュータの以前のバージョンから設定を移行する] チェックボックスをオンにします。
8. [次へ] をクリックします。
9. [製品のアクティベーション] 画面で、次のいずれかを選択します。

- [アクティベーションコード] フィールドに製品のアクティベーションコードを入力して [次へ] をクリックします。
- アクティベーションコードを入力しないで [次へ] をクリックします。

  アクティベーションコードを入力しないで [次へ] をクリックすると、情報が不足していることを警告するメッセージと、30 日間有効の InterScan VirusWall 体験版がインストールされることを通知するメッセージが表示されます。[OK] をクリックしてインストールを続行します。

10. このインストール先のパスを変更する場合は、[インストール先の指定] 画面に移動し、[参照] をクリックして別の場所を指定します。
11. 初期設定のパスを受け入れるか、新しいインストール先を選択したら、[次へ] をクリックします。
12. [Web コンソール URL の設定] 画面で、Web コンソールのバインド先を指定します。
13. [次へ] をクリックします。
14. [管理者パスワード] 画面で、4 ～ 32 文字のパスワードを入力して確認し、[次へ] をクリックします。
15. [検索サービスの設定] 画面で、インストール完了後に開始する InterScan VirusWall サービスを選択します。
16. [次へ] をクリックします。
17. リレーされるメールをブロックするには、[リレー先の設定] 画面に移動して、受信メールを受け入れるドメインを [ドメイン名] フィールドで指定します。
18. [次へ] をクリックします。
19. Web レピュテーションデータベースの向上に役立てるため、[HTTP Web レピュテーションの情報を送る] 画面に移動し、このチェックボックスをオンにして、感染した URL についての匿名情報を送信してください。
20. [次へ] をクリックします。
21. [ウイルストラッキングセンターの設定] 画面で、ウイルストラッキングセンターに InterScan VirusWall で検出されたウイルスの情報を送信するかどうかを選択し、[次へ] をクリックします。
22. [設定の確認] 画面で現在の設定を確認して、[次へ] をクリックします。
23. [セットアップの完了] 画面で、Readme ファイルの表示、Web コンソールの起動、または移行レポートの表示を選択して [終了] をクリックします。

    インストールの開始時に移行レポートの作成を選択した場合は、[ファイル出力] をクリックします。レポートが新しいウィンドウで表示されます。

以前のバージョンからのコマンドラインによる移行

新しいコンピュータに本バージョンをインストールしたら、コマンドラインを使用して、以前のバージョンの InterScan VirusWall がインストールされている別のコンピュータから設定を移行できます。移行は次のバージョンについてサポートされています。

- InterScan VirusWall 6.0 または 6.02

InterScan VirusWall 6.0x の設定を InterScan VirusWall 7.0 がインストールされているコンピュータに移行するには

1. 移行ツールを見つけてコピーします。
   - InterScan VirusWall 6.0x から本バージョンに移行する場合、InterScan VirusWall 7.0 のインストールパッケージのディレクトリ < インストールパッケージ >¥other にある isvw-migr6to7.exe という名前のツールを見つけて、それを InterScan VirusWall 6.0x がインストールされているコンピュータにコピーしてください。
2. コマンドラインで次のように入力します。
   - InterScan VirusWall 6.0x から本バージョンに移行する場合 :
     `isvw-migr6to7 -o [< 移行設定ファイル名 >]`
     例 : `isvw-migr6to7 -o c:¥ISVW6-package.out`

   注意 : InterScan VirusWall 7.0 の移行ツールでは、絶対パス名と相対パス名の両方がサポートされています。

3. ネットワーク経由でこのファイルにアクセスできない場合は、< 移行設定ファイル名 > のファイルをリムーバブルメディアにコピーします。これにより、InterScan VirusWall をインストールするコンピュータでそのファイルにアクセスできます。
4. InterScan VirusWall 7.0 がインストールされているコンピュータで、コマンドウィンドウを開きます。
5. <InterScan VirusWall 7.0 インストールパス >¥Others に移動し、コマンドウィンドウで、次のコマンドで移行ツールを実行します。

   `isvw-migr6to7 -p [< 移行設定ファイル名 >] -i [<InterScan VirusWall 7.0 インストールパス >]`

   例 : `isvw-migr6to7 -p c:¥ISVW5-package.out -i "c:¥Program Files¥Trend Micro¥InterScan VirusWall 7"`

   移行が正常に終了すると、移行の成功メッセージが表示されます。また、InterScan VirusWall 7.0 インストールディレクトリに移行レポートが作成されます。

6. InterScan VirusWall サービスを再起動します。

   75 ページの「InterScan VirusWall を起動 / 停止する」を参照してください。

インストールが正常に終了したことを確認する

Windows タスクマネージャを使用して、InterScan VirusWall が正常にインストールされており、正しく機能していることを確認します。InterScan VirusWall が正しくインストールされており、適切に機能している場合は、Windows タスクマネージャで、次の 8 個の InterScan VirusWall サービスが実行されているはずです。

表 3-1. InterScan VirusWall の初期設定のサービス

サービス	サービスの説明
isvw-svr.exe	すべてのプロトコル通知に使用します。
isvw-smtp.exe	ウイルス検索、スパムメール、およびコンテンツフィルタを含む SMTP ストリームの検索に使用します。
isvw-scan.exe	ウイルス検索、スパムメール、およびコンテンツフィルタを含む POP3 ストリームの検索に使用します。
isvw-pop3.exe	POP3 プロトコルコマンドの処理に使用します。
isvw-main.exe	主要な InterScan VirusWall プロセスに使用します。監視機能を果たし、InterScan VirusWall プロセスの実行が中断されないようにします。また、アップデートタスクも実行します。
isvw-http.exe	ウイルス検索、URL フィルタ、URL ブロック、およびフィッシング対策を含む HTTP ストリームの検索に使用します。
isvw-ftp.exe	ウイルス検索を含む HTTP ストリームの検索に使用します。
isvw-agent.exe	Control Manager サーバへの登録に使用するエージェント。

注意： Web コンソールの [概要] 画面でプロトコルを無効にすると、対応するサービスの実行が停止されます。このような場合、そのサービスを Windows タスクマネージャで確認することはできなくなります。

インストール後の作業

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： これらのタスクの操作手順については、オンラインヘルプを参照してください。

1. InterScan VirusWall をアクティベートします (セットアップ中に完了していない場合)。または、30 日の体験期間を開始します。
2. 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。
3. 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 / スパムメール検索エンジンの予約アップデートを設定します。
4. 通知サーバ、ポート、管理者のメールアドレス、優先する文字セットなどの通知設定を設定します。
5. 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
6. タスク :
   a. 大規模感染予防サービスを設定します。
   b. インターネット接続のためにプロキシが必要な場合は、アクティベーション、アップデートおよびウイルストラッキングセンターの各サービスに対してプロキシ情報を設定します。
   c. 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。

d. 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。

e. 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。

f. 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。

g. 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は、SMTP の送受信検索をテストします。
   - SMTP プロトコルが有効な場合は、SMTP の送受信の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 の受信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は、HTTP のダウンロード / アップロード検索をテストします。
   - HTTP プロトコルが有効な場合は、HTTP の 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。

7. 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。

第 4 章

基本的な操作

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) のサービスの開始 / 停止や主要機能、そのテストなどの作業について説明します。

注意： 実行可能な InterScan VirusWall の全タスクの詳細については、オンラインヘルプを参照してください。オンラインヘルプでは、InterScan VirusWall の運用の最適化に役立つトピックも参照できます。

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。各メニュー項目の概要と、サブメニュー項目をクリックすると表示される各画面で実行可能なさまざまなタスクの概要については、49 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。

図 4-1.　[概要] 画面が表示されている InterScan VirusWall Web コンソール

Web コンソールにアクセスする

InterScan VirusWall のインストールが完了すると、インストール時に選択したサービスと基本サービスが自動的に開始されます。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、InterScan VirusWall のコンソールを開いて設定を確認する必要があります。

以下のいずれか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、7.0、および 8.0

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://<IP アドレス >:< ポート番号 >
   - https://<IP アドレス >:< ポート番号 >

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 コンソールの各種メニュー項目について説明し、さまざまな画面で実行するタスクについて解説します。これらのタスクの実行方法の詳細は、管理者ガイドを参照してください。

概要

[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。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。[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] 画面が開きます。

図 4-2.　[概要] 画面


TREND MICRO
InterScan™VirusWall™
ログオフ
--------ヘルプ--------
概要
SMTP
HTTP
FTP
POP3
大規模感染予防
隔離
アップデート
レポート
ログ
管理
概要
InterScan VirusWallの使用期限まで残り54日です。 詳細な情報...
ステータス
メール (SMTP)
メール (POP3)
Web (HTTP)
ファイル転送 (FTP)
製品情報:
InterScan VirusWall スタンダードエディション (ビルド番号: 1242)
製品ライセンス:
InterScan VirusWallの使用期限まで残り54日です。
サービスステータス
トレンドマイクロ大規模感染予防サービス
コンポーネントのバージョン
8個のコンポーネントが最新版ではありません。
ウイルス対策
0件の感染ファイルが今日検出されました。
スパムメール対策
0通のスパムメールが今日検出されました。
スパイウェア対策
0個のスパイウェア/グレーウェアが今日検出されました。
その他

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	4 つの各プロトコルの現在のステータス 製品とライセンスの情報 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 トラフィックを有効または無効にします。

SMTP

[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] 画面

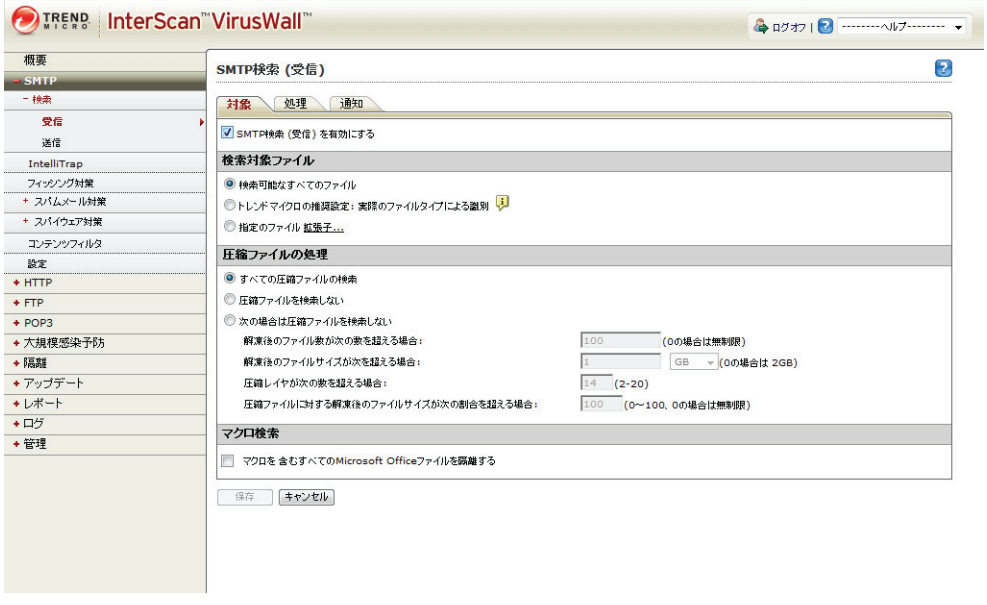


表 4-2.　[SMTP] のサブメニュー項目

サブメニュー	説明	タスク
検索 > 受信 > 送信	SMTP トラフィックのリアルタイム送受信検索を実行します。	送受信される SMTP メールメッセージの SMTP 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 ([感染したアイテムを駆除して配信]、[感染したアイテムを隔離して配信]、[メッセージ全体を削除]、[感染したアイテムを削除して配信]、[そのまま配信])。 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、ウイルス検出時のメールの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。
フィッシング対策	SMTP メールのフィッシング試行を検出します。	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。

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
スパムメール対策 > コンテンツ検索 > メールレピュテーションサービス	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コンテンツ検索およびメールレピュテーションサービスを有効または無効にします。 [低]、[中]、[高] のいずれかの検出レベルを設定します。すべてのカテゴリに対して同じ検出レベルを設定するか、または [商用]、[健康]、[宗教] などのカテゴリ別に異なる検出レベルを設定します。 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、承認する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。 判定の確実性レベルに基づいて、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。
スパイウェア対策 > 受信 > 送信	送受信 SMTP 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 / グレーウェアを削除して配信]、または [そのまま配信])。 スパイウェア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
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。	メイン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設定します。

HTTP

[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。

図 4-4.　[対象] タブが選択されている [HTTP 検索] 画面

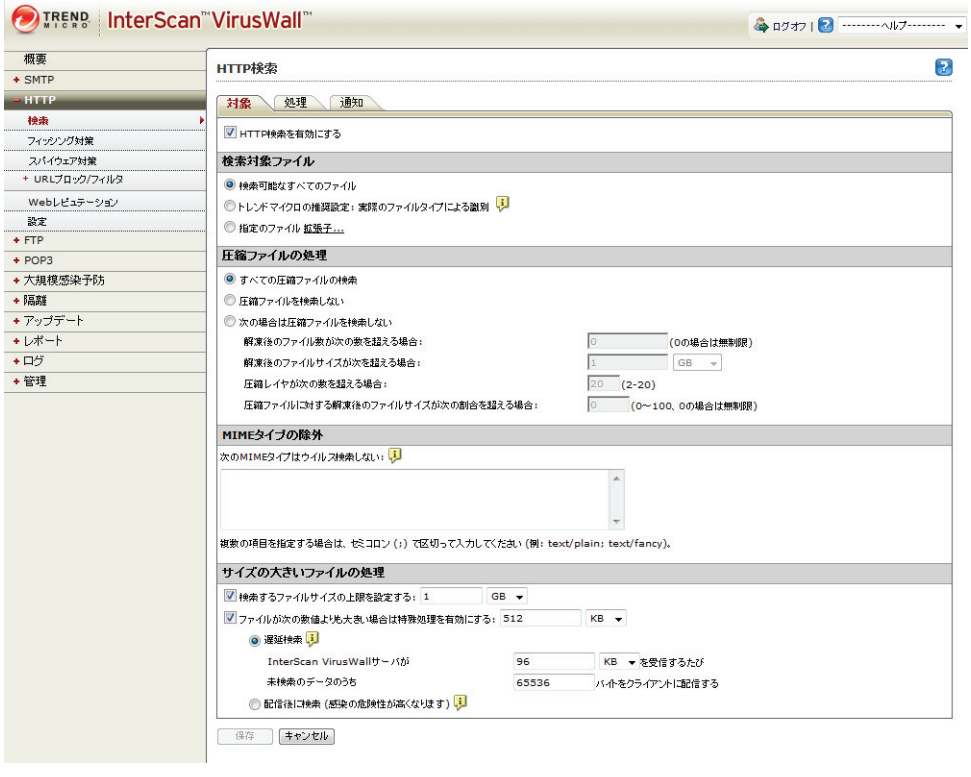


表 4-3.　[HTTP] のサブメニュー項目

サブメニュー	説明	タスク
検索	HTTP トラフィックを検索してアップロード / ダウンロードにおけるウイルスその他のセキュリティリスクを検出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]、[隔離]、[ブロック]、または　[そのまま配信])。 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。
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。

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
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。 スパイウェアまたはグレーウェアの検出時に実行する処理を設定します ([隔離]、[ファイルブロック]、または [ダウンロード許可 (推奨しません))。 スパイウェアまたは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。
URL ブロック / フィルタ	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、または文字列を含むリストを定義します。1 つのリストではブロックする URL を指定し、もう 1 つ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 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 (業務時間外、業務時間内)。

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
	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 / 成人向け] 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。禁止コンテンツカテゴリに分類されている URL も対象になります。 設定を適用する日時を指定します。 URL カテゴリの見直し依頼を TrendLabs へ送信します。
Web レピュテーション	URL 要求のクエリを実行して、URL カテゴリに関する情報を返します。 また、Web レピュテーションでは、評価スコアが URL に割り当てられます。	URL フィルタでは、その URL カテゴリに関する情報を使用してフィルタ処理が実行されます。 InterScan VirusWall では、URL 評価スコアを使用し、このスコアがユーザ指定の検出レベルより上か下かに基づいて、特定の処理が実行されます。
設定	HTTP サーバの設定を指定できます。	スタンドアロンモード、依存プロキシモード、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 要求のログを可能にします。

FTP

[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を強化する機能を利用できます。

図 4-5.　[対象] タブが選択されている [FTP 検索] 画面

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。圧縮されたボリューム内の個別ファイルもチェックの対象になります。	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。 添付の圧縮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 [そのまま配信])。 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。
スパイウェア対策	FTP のファイル転送時にスパイウェア / グレーウェアをブロックできます。	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。 スパイウェアまたはグレーウェアの検出時に実行する処理を指定します ([隔離]、[ブロック]、[ダウンロード許可])。 スパイウェアまたは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 4-4.　[FTP] のサブメニュー項目 (続き)

サブメニュー	説明	タスク
設定	FTP サーバの設定方法を指定できます。	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。 接続の確立時に送信するメッセージをカスタマイズします。

POP3

わずかな違いはありますが、[POP3] メニュー項目は [SMTP] メニュー項目とほぼ同じです。例外は、[検索] および [設定] サブメニュー項目です。

図 4-6. [対象] タブが選択されている [POP3 メール検索] 画面

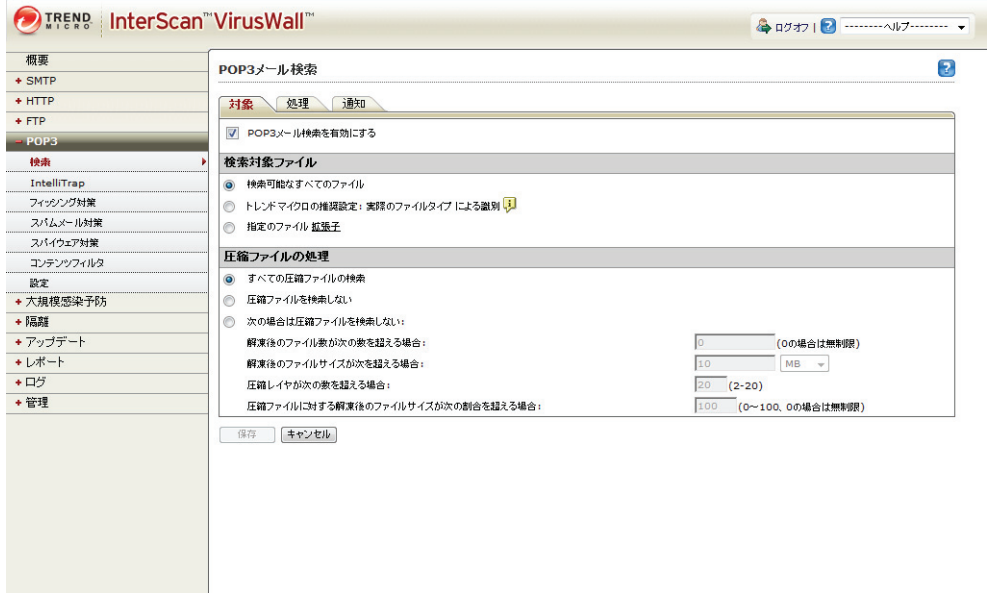


表 4-5.　[POP3] のサブメニュー項目

サブメニュー	説明	タスク
検索	POP3 トラフィックのリアルタイム検索を実行します。	POP3 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。 添付の圧縮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 ([感染したアイテムを駆除して配信]、[感染したアイテムを隔離して配信]、[メッセージ全体を削除]、[感染したアイテムを削除して配信]、または [そのまま配信])。 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、ウイルス検出時のメールの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。	POP3 の 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
フィッシング対策	POP3 メールのフィッシング試行を検出します。	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。 [低]、[中]、[高] のいずれかの検出レベルを設定します。すべてのカテゴリに対して同じ検出レベルを設定するか、または [商用]、[健康]、[宗教] などのカテゴリ別に異なる検出レベルを設定します。 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、承認する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　([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 / グレーウェアを削除して配信]、または　[そのまま配信])。 スパイウェア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。
コンテンツフィルタ	POP3 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。	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 の 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。 許可する同時クライアント接続数、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

最新のパターンファイルでも未対応の新たなウイルスによる広範囲の感染が報告された際に、ウイルスの蔓延からネットワークを保護するための予防策を実施するサービスです。

図 4-7.　[大規模感染予防サービス - ステータス] 画面

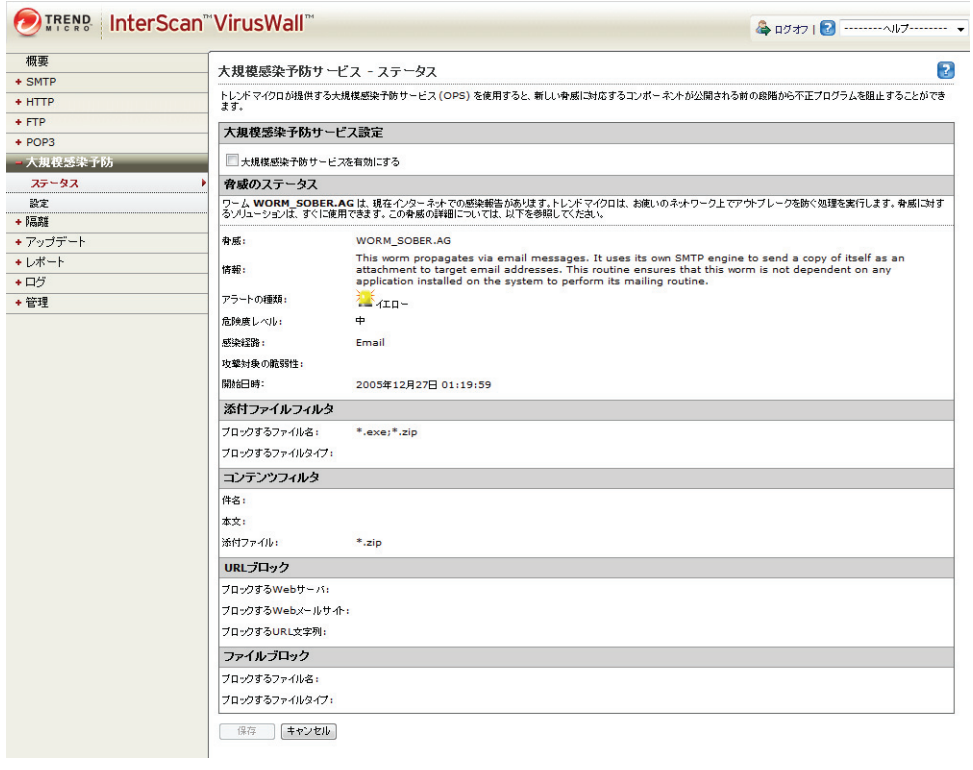


表 4-6.　[大規模感染予防] のサブメニュー項目

サブメニュー	説明	タスク
ステータス	アクティブな大規模感染予防ポリシーの実施を通知します。	大規模感染予防サービスを有効または無効にします。 大規模感染予防サービスステータスを表示します。
設定	大規模感染予防サービス設定を表示および変更できます。	大規模感染予防サービスポリシーの有効期限の初期設定を手動で変更します。

隔離

[隔離] メニュー項目を使用すると、InterScan VirusWall によって隔離されたファイルを管理できます。

図 4-8.　[隔離クエリ] 画面

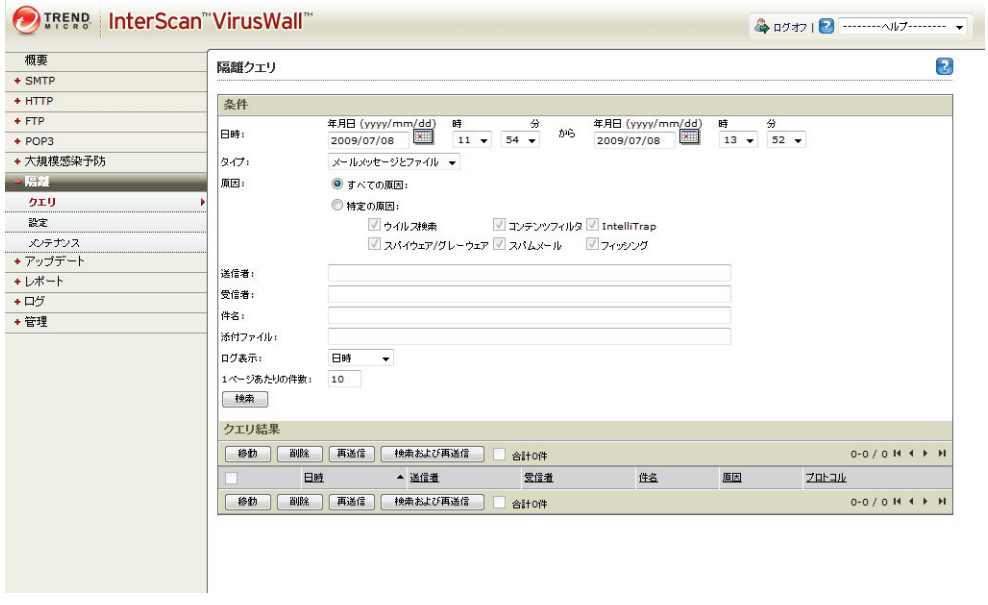


表 4-7.　[隔離] のサブメニュー項目

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。	日時、タイプ、原因、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、ページあたりの件数を制限します。
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。

表 4-7.　[隔離] のサブメニュー項目 (続き)

サブメニュー	説明	タスク
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。

アップデート

新しい不正プログラムや不快な 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。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。

図 4-9.　[手動アップデート] 画面

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	要望に応じてコンポーネントをアップデートできます。	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できます。	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。

ログ

[ログ] メニュー項目を使用すると、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 4-10.　[ログクエリ] 画面

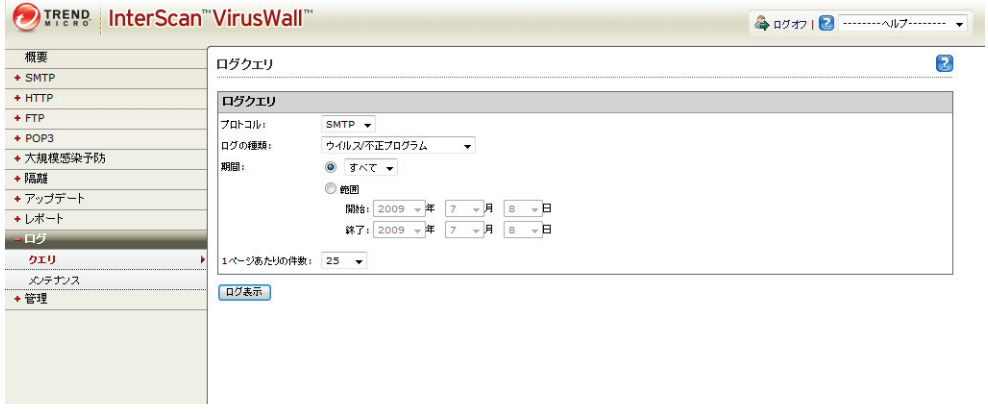


表 4-9.　[ログ] のサブメニュー項目

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できます。	プロトコル、ログの種類、期間、および 1 ページあたりの件数を指定して　[ログ表示] をクリックします。 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、XML、または CSV ファイルとしてログ検索結果を出力ポートします。
メンテナンス	特定の基準に従って古いログを削除できます。	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。

ローカルレポート

InterScan VirusWall のレポートには、すべての種類のトラフィック違反をまとめることができます。HTTP Web 違反について、指定した期間内に違反したユーザを表示することもできます。レポートには次の情報を含めることができます。

- 発生したウイルス
- ウイルスの発生日時と送信元
- 指定された期間　(最大 6ヵ月) の違反ユーザおよび違反の種類と頻度

図 4-11.　[すべてのレポート] 画面

表 4-10.　[レポート] のサブメニュー項目

サブメニュー	説明	タスク
すべてのレポート	新しいレポートプロファイルを作成できます。	レポートプロファイル名と、そのレポートプロファイルを有効にするかどうかを指定します。 レポートプロファイルに含めるレポートオプションを選択します。 レポートを生成するタイミングを指定します。 レポートの頻度を指定します。 既存のレポートプロファイルを変更します。 レポートプロファイルを削除します。
メンテナンス	InterScan VirusWall で保持するレポートの最大数を指定できます。	InterScan VirusWall で保持するレポートの最大数を指定します。

管理

[管理] メニュー項目を使用すると、InterScan VirusWall インストールの通知設定、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。ウイルストラッキングプログラムに参加することもできます。

図 4-12. [通知設定] 画面

表 4-11. [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	Trend Micro Control Manager (以下、Control Manager) サーバと Web コンソールを使用して InterScan VirusWall を管理できます。	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。

表 4-11. [管理] のサブメニュー項目 (続き)

サブメニュー	説明	タスク
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優先文字コード • 通知の送信者のメールアドレス
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。	現在のパスワード、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。
ユーザ識別	IP アドレスか、プロキシ認証を利用したユーザ / グループ名によって識別できます。	ユーザロールの識別、グループへの HTTP アクセスルールの適用、およびユーザまたはグループ固有の URL フィルタ / ブロックのポリシーの作成を実行できます。

表 4-11. [管理] のサブメニュー項目 (続き)

サブメニュー	説明	タスク
ウイルストラッキング	全世界の顧客から集めたウイルス検索結果を統合し、リアルタイムの統計を集計して、リアルタイムマップに表示するトレンドマイクロのプログラム。	ウイルストラッキングプログラムに参加するかどうかを選択します。 TrendLabs に送信された標準的なサンプルデータを表示します。 各大陸や選択した国のウイルスの傾向を表示します。

InterScan VirusWall を起動 / 停止する

InterScan VirusWall には、次の 4 つのサービスがあります。SMTP VirusWall、POP3 VirusWall、FTP VirusWall および、HTTP VirusWall です。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。ただし、特定のサービスのリアルタイム検索を有効または無効にすることにより、InterScan VirusWall の各サービスを個別に制御することもできます。インストール時に選択していないサービスを開始する場合、またはインストール時に選択したサービスを停止する場合は、Web コンソールの [概要] 画面で対象のサービスを手動で有効または無効にします。

すべてのサービスを再起動する

1. [コントロール パネル] で [管理ツール] をクリックし、[管理ツール] 画面を開きます。
2. [サービス] アイコンをクリックし、[サービス] 画面を開きます。
3. [TrendMicro InterScan VirusWall] に移動し、[サービスの再起動] をクリックします。

   通常、[InterScan VirusWall] は [自動] に設定されています。

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、プログラムのしく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。

テストウイルスを使用したウイルス検索のテスト

EICAR (European Institute for Computer Antivirus Research) では、InterScan VirusWall のインストールおよび設定のテストに使用できる、テスト用「ウイルス」を開発しています。このテストウイルスは単独では実行でき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。これはウイルスではなく、プログラムコードをまったく含みません。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。

コンピュータ上でテストウイルスを使用して、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 / 削除が正常に動作するかどうかを確認できます。次に説明するテスト手順では、EICAR テストファイル (eicar.com)、ZIP 形式の EICAR テストファイル (eicar_com.zip)、および 2 回 ZIP された EICAR テストファイル (eicarcom2.zip) を用意し、これらが InterScan VirusWall で正しく検出され、処理されることを確認します。まずは SMTP VirusWall のウイルス対策機能をテストします。

SMTP VirusWall のテストを十分に行ったら、他のプロトコルのテストに進んでください。テストウイルスを入手するには

テストウイルスを入手するには、次のいずれかを行ってください。

- 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
  - 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。

- 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. 以下のようにログクエリの条件を設定します。
      - 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

ブロック対象の特定のキーワードを件名やコンテンツ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。メールは隔離され、インシデントが SMTP キーワードフィルタログと隔離クエリに記録されます。

注意 : SMTP のコンテンツフィルタのテストが完了したら、このセクションで説明した方法を使用して、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、[追加] をクリックします。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. 以下のようにログクエリの条件を設定します。

- 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、手順 1 のキーワードを [件名] で入力することにより、クエリの範囲を限定します。

c. [検索] をクリックします。クエリが実行され、結果が表示されます。

[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原因が表示されます。

リアルタイム検索モニタを使用する

InterScan VirusWall のリアルタイム検索モニタでは、SMTP 検索機能のリアルタイム監視と、Windows パフォーマンスモニタを使用した SMTP および FTP パフォーマンスデータへのアクセスが可能です。

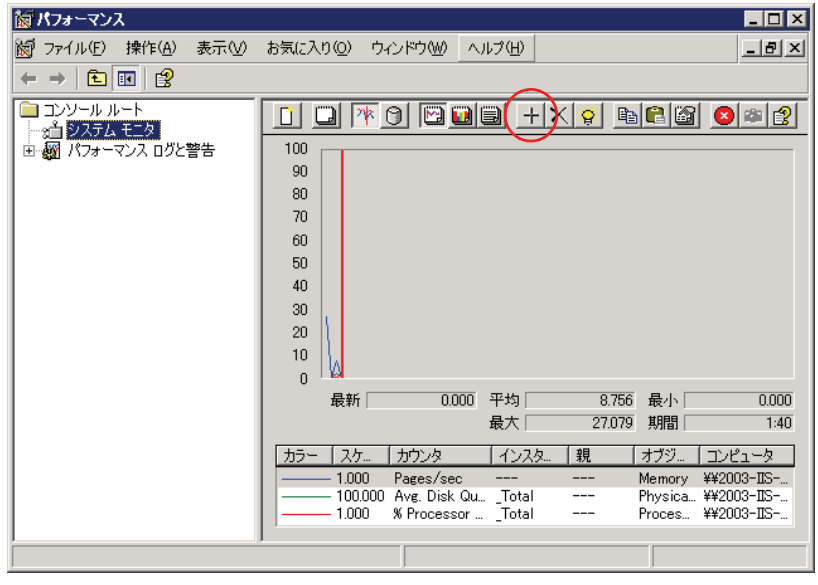
リアルタイム検索モニタを実行するには

1. Windows の [スタート] メニューで、[プログラム] → [InterScan VirusWall] → [InterScan VirusWall リアルタイム検索モニタ] の順に選択します。

SMTP 経由でメールを送信すると、統計および活動に関するリアルタイムの情報がモニタパネルに表示されます。

2. [パフォーマンスモニタ] をクリックして Windows パフォーマンスモニタを開きます。

図 4-13.　Windows パフォーマンスモニタ

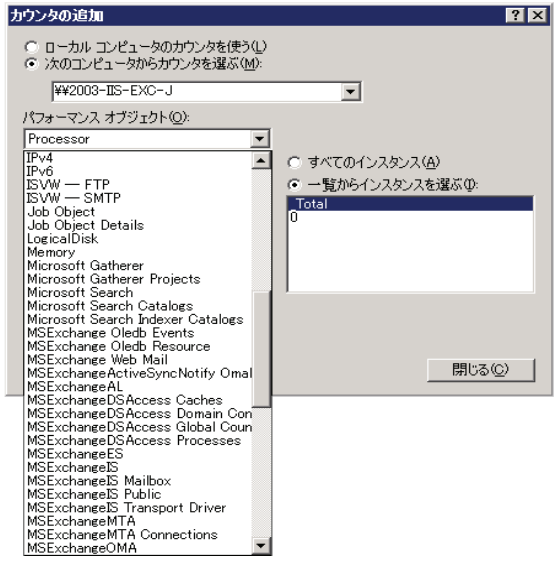


Windows パフォーマンスモニタにカウンタを追加するには

1. Windows パフォーマンスモニタの画面で「+」をクリックします (図 4-13 の丸で囲まれたアイテムを参照)。

   [カウンタの追加] 画面が表示されます。

図 4-14. [カウンタの追加] 画面



2. [次のコンピュータからカウンタを選ぶ] オプションを選択して、InterScan VirusWall がインストールされているコンピュータを選択します。
3. [パフォーマンス オブジェクト] ドロップダウンリストから [ISVW - FTP] または [ISVW - SMTP] を選択します。
4. [すべてのカウンタ] を選択します。または [一覧からカウンタを選ぶ] を選択し、追加するカウンタを選択します。
5. [追加] をクリックします。
6. [閉じる] をクリックして Windows パフォーマンスモニタへ戻ります。
7. グラフ表示、ヒストグラム表示、またはレポート表示でパフォーマンスデータを表示します。

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可能性のある問題の解決に役立つ情報を提供します。

この章に問題に対する解決策が記載されていない場合は、管理者ガイドを参照してください。

トラブルシューティング

表 5-1. 問題の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。18 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、インストールは続行されますが、警告メッセージが表示されます。 • 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 1GB 以上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。 • 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。 • 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。
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、スパムメール検索エンジン、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。その後、CPU の使用率は正常な状態に戻ります。

表 5-1.　問題の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
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 に格納されている不適切なサーバ 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	• 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再度アクティベートしないでください。 • 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ている場合は、体験版のアクティベーションコードを使用しないでください。その逆も同様です。 • 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。

表 5-1.　問題の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
Web コンソールの問題	• テキストボックスに中国語や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場合は、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 [UTF-8] を選択すると、Web ユーザインタフェースで中国語や日本語などの 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場合は、InterScan VirusWall がインストールされているコンピュータを確認します。Web コンソールを開く前に、クエリキャッシュファイルを保存するための十分な領域を確保しておく必要があります。 • Web コンソールのパスワードを忘れた場合は、トレンドマイクロのテクニカルサポートへ連絡し、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、登録済みのお客様に限られます。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。
InterScan VirusWall のアンインストール後も、一部のフォルダが削除されません。	アンインストール中に開かれたままになっていたフォルダは削除されません。手動で削除してください。「ログ」フォルダおよび「隔離」フォルダは、アンインストール後も保持されます。
プロセスのクラッシュ時など、障害やエラーのログはどこで確認できるのでしょうか。	• Windows のシステムログおよび InterScan VirusWall のシステムログを使用してください。 • InterScan VirusWall のシステムログで、「終了処理中です ...」行を間に挟まずに 2 つの「初期化中です ...」行が続いている場合は、クラッシュの発生を意味します。 • デバッグログが有効になっている場合は、デバッグログにさらに詳しい情報が含まれています。

データを収集してトレンドマイクロのサポートに送信する

トレンドマイクロのテクニカルサポートに問い合わせる前に、必ず、ドメインコントローラエージェントのデバッグログおよび InterScan VirusWall HTTP デーモンのデバッグログを収集してください。これらのログの詳細については、管理者ガイドを参照してください。

よくある質問

質問：

アップデート通知を有効にするにはどうすればよいですか。

回答：

1. InterScan VirusWall サービスを停止します。
2. `config.xml` を開き、`/Root/common/ActiveUpdate/notification/SuccessEnable` の値を「1」に設定し、

   次に、

   `/Root/common/ActiveUpdate/notification/FailEnable` の値を「1」に設定します。
3. InterScan VirusWall サービスを再起動します。

質問：

InterScan VirusWall をインストールまたはアンインストールしようとするとエラーメッセージが表示されるのはなぜですか。

回答：

InterScan VirusWall をインストールしようとしているコンピュータに、リアルタイムウイルス検索ソフトウェアがインストールされ、有効になっていることが考えられます。InterScan VirusWall をインストールしようとしているコンピュータまたは InterScan VirusWall をアンインストールしようとしているコンピュータに、リアルタイムウイルス検索ソフトウェアがインストールされていると、エラーメッセージが表示されます。InterScan VirusWall をインストールまたはアンインストールする前に、一時的にリアルタイムウイルス検索を無効にする必要があります。

質問：

InterScan VirusWall 7.0 のインストール後、システムイベントログに表示される `MFC80.dll` エラーを解決するにはどうすればよいですか。

回答：

Microsoft Visual C++ 2005 Redistributable Package (x86) をインストールする必要があります。このパッケージは、次の場所からダウンロードできます。

http://go.microsoft.com/fwlink/?linkid=65127&clcid=0x409

パッケージをダウンロードしたら、対象のコンピュータで vcredist_x86.exe を実行します。これにより、Visual C++ ライブラリが共有アセンブリとしてインストールされます。

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。

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

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

製品 Q&A のご案内

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

製品 Q&A

`http://esupport.trendmicro.co.jp/corporate/search.aspx`

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

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

セキュリティ情報

セキュリティ情報の入手先

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

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

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

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

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

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

トレンドマイクロへのウイルス解析依頼

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

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

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

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

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

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

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

ウイルス解析サポートセンター「TrendLabs」

トレンドマイクロのウイルス解析サポートセンター「TrendLabs」(トレンドラボ) は、フィリピンセンターを本部として、米国、日本、台湾、ドイツ、アイルランド、中国、フランス、メキシコの各国センターで構成されています。24 時間体制でウイルスの活動を監視するウイルス解析エンジニアを含む 1000 名以上のスタッフが、セキュリティに関する最新の情報を収集し、高品質なサービスとソリューションを迅速かつ効果的に世界各国のトレンドマイクロのパートナーとお客さまに提供しています。

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

索引

英数字

あ

か

さ

た

な

は

や

ら