TREND MICRO™

侵入防御ファイアウォール

インストールガイド

Endpoint Security

※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

・「フィッシング詐欺対策」「URL フィルタ」では、Web サイトが安全かどうかの判定のために、お客さまがアクセスした URL の情報を暗号化してトレンドマイクロのサーバに送信します。
サーバに送信された URL 情報は、Web サイトの安全性の確認、および本機能の改良の目的にのみ利用されます。
また、これらの機能を有効にしたうえで、コモンゲートウェイインタフェースアプリケーションを使用しているサーバで構築されている Web サイトにアクセスし、ID、パスワード等を入力した場合には、お客様がアクセスした Web ページの URL にお客様が入力した ID、パスワード等が含まれた状態でトレンドマイクロのサーバに送信される場合があります。この場合、トレンドマイクロでは、お客様がアクセスする Web ページの安全性の確認のため、これらのお客様より受領した情報にもとづき、お客様がアクセスする Web ページのセキュリティチェックを実施します。
・「ソフトウェア安全性評価サービス」では、プログラムが安全かどうかの判定のために、プログラムの情報をトレンドマイクロのサーバに送信します。
・「ウイルストラッキング/TrendCare プログラム」では、検出されたウイルス/脅威名、検出数、国/地域、感染元となった Web サイトの URL を、統計を取るためにトレンドマイクロのサーバに送信します。
・「迷惑メール対策ツール」では、弊社製品の改良目的および迷惑メールの撲滅のため、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。

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ウェブサイトから見つけることができます。
「http://www.treas.gov/ofac/」、および「http://www.bis.doc.gov/complianceandenforcement/ListsToCheck.htm」
2008 年 11 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。

著作権について

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

商標について

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

本書に記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。
Copyright © 2008 Trend Micro Incorporated. All rights reserved.

P/N: IDFFFF-AE0200 (2009/2)

目次

侵入防御ファイアウォールについて

侵入防御ファイアウォールは、侵入防御システムにより、機密情報、アプリケーション、コンピュータ、またはネットワークセグメントを保護するセキュリティポリシーを作成し、施行できます。サーバコンポーネント (「サーバプラグイン」) は、ウイルスバスター コーポレートエディション (以下、ウイルスバスター Corp.) サーバにインストールされます。サーバプラグインにより、ウイルスバスター Corp.クライアントのクライアントコンポーネント (「クライアントプラグイン」) が配信され管理されます。

サーバプラグイン

サーバプラグイン (プラグインモジュールを管理するウイルスバスター Corp.の管理サーバ) は、ウイルスバスター Corp. Web コンソール内に組み込まれた管理システムです。管理者はこのサーバプラグインを使用して、包括的な侵入防止セキュリティポリシーを作成および管理し、脅威を追跡して、その脅威に対して実行された防御処理のログを記録できます。

ダッシュボード

サーバプラグインダッシュボードには、次の機能が備わっています。

- ドリルダウン機能を使用した、システム、イベント、およびコンピュータに関するさまざまなレポート機能
- ドリルダウン機能を使用した、主要な測定内容のトレンドグラフ
- ドリルダウン機能を使用した、詳細イベントログ機能、および他のシステムとのイベント相関におけるログ転送機能
- 複数のダッシュボードレイアウトを保存する機能

監視ツール

監視ツールには、ファイアウォール、IPS、およびシステムイベントのイベント表示ツール、最近のアクティビティを集約した一連のレポートが含まれます。

コンピュータのリスト

[コンピュータ] 画面とウイルスバスター Corp. Web コンソールの [ネットワーク上のコンピュータ] 画面のクライアントツリー構造は同じです。サーバプラグインに表示されるリストは、侵入防御ファイアウォールのさまざまなルール、フィルタ、およびステートフル設定を適用する際に使用されます。

セキュリティプロファイル

セキュリティプロファイルは、1 台以上のコンピュータに適用されるセキュリティルールを設定し、指定できるポリシーテンプレートです。このコンパクトで管理可能なルールセットを使用すると、包括的なセキュリティの提供が容易になり、数千というルールを管理する必要がなくなります。初期設定のセキュリティプロファイルでは、一連の共通のコンピュータ設定に対して必要なルールが提供されるため、迅速に配信できます。

ファイアウォールルール

高度な双方向のステートフルファイアウォールは、TCP、UDP、および ICMP など、すべてのネットワークプロトコルに全般的なサポートを提供します。ファイアウォールルールは、すべて設定可能で、インタフェースごとにトラフィックを許可/拒否することも、許可された IP または MAC アドレスへの通信を制限することもできます。

IPS (侵入防御システム) フィルタ

ディープパケットインスペクションでは、コンピュータが送受信するアプリケーションデータを調査しますが、これによってソフトウェアの脆弱性が攻撃から保護されます。IPS フィルタを使用すると、コンテンツベースでのデータをブロックしたり、ログに記録したり、編集することが可能になります。IPS フィルタは、予期されるアプリケーションデータを定義し、コンテンツベースで不正なデータをブロックすることにより、脆弱性に対する既知および不明な攻撃から保護します。

セキュリティアップデート: IPS フィルタの継続的なアップデートにより、既知および不明な攻撃に対して最新で包括的な保護が自動的に提供されます。

ステートフル設定

侵入防御ファイアウォールのステートフル設定メカニズムでは、トラフィック履歴との関連における各パケット、TCP および IP ヘッダ値の正当性、および TCP 接続状態の推移が分析されます。UDP および ICMP などのステートレスなプロトコルの場合、侵入防御ファイアウォールでは、履歴トラフィック分析に基づいた擬似ステートフルメカニズムが実行されます。ステートフルメカニズムによって、パケットは次のように処理されます。

- 静的ファイアウォールルール条件によってパケットの通過が許可された場合、パケットはステートフルルーチンに渡されます。
- パケットが既存の接続に属しているかどうかを判断するには、パケットの調査が実行されます。調査では、ステートフルメカニズムによって作成された接続テーブルで、エンドポイントと一致するかどうかをチェックします。
- TCP ヘッダの正当性 (シーケンス番号やフラグの組合せなど) が調査されます。

再使用可能なコンポーネント

侵入防御ファイアウォールでは、アプリケーションの種類、IP リスト、MAC アドレスリスト、およびポートリストの独立型のセットを使用します。これらのコンポーネントは、侵入防御ファイアウォールシステムの複数のエレメント (ファイアウォールルール、IPS フィルタ、セキュリティプロファイルなど) で使用できます。これによって、新規のルール、フィルタ、またはプロファイルが作成されるたびに同じ情報を入力する必要がなくなります。

クライアントプラグイン

クライアントプラグイン (プラグインモジュールが対応するウイルスバスター Corp.のクライアント PC) は、ウイルスバスター Corp.クライアント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された、高パフォーマンスで、スペースをとらないソフトウェアコンポーネントです。サーバプラグインによって配信されたセキュリティプロファイルを、送受信ネットワークトラフィックに適用し、攻撃の前兆を示すプロトコル異常やコンテンツがないか監視します。クライアントプラグインは、必要に応じて、トラフィックをブロックまたは修正することで脅威の侵入を防止し無効にします。

システム要件

サーバプラグイン

(プラグインモジュールを管理するウイルスバスター Corp.の管理サーバ)

- **メモリ:** 最小 512MB の RAM (1GB 推奨)
- **ディスク容量:** 最小 1.5GB (6GB 推奨)
- **Web ブラウザ:** Internet Explorer 6 以上 (Cookie を有効にする)
- Adobe Acrobat Reader 5 以上 (ヘルプの表示に必要)
- **OS:** Microsoft Windows Server 2003 Service Pack 2、Microsoft Storage Server 2003 Service Pack 2、Microsoft Cluster Server 2003 Service Pack 2、Microsoft Windows 2000 Server Service Pack 4
- **前提条件:**
  - **Microsoft Windows 2000:** MDAC 2.81、Windows Installer 3.1、Microsoft .NET Framework 2.0 以上 (SQL Server 2005 Express のインストールに必要)
  - **Microsoft Windows 2003:** Microsoft .NET Framework 2.0 以上 (SQL Server 2005 Express のインストールに必要)

サーバプラグインにより、Microsoft SQL Server 2005 Express (英語版) が自動的にインストールされます。

クライアントプラグイン

(プラグインモジュールが対応するウイルスバスター Corp.のクライアントPC)

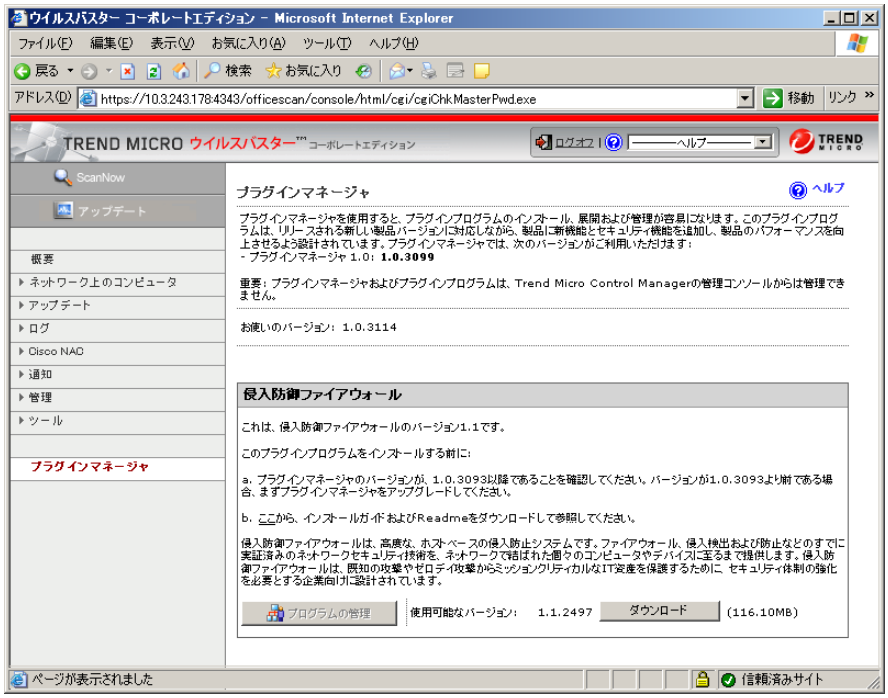
- **メモリ:** 最小 128MB の RAM
- **ディスク容量:** 最小 50MB (主にログ用に 100MB 推奨)
- **OS:** Microsoft Windows 2000 Professional Service Pack 3/4 (32 ビット)、Microsoft Windows XP Service Pack 2/3 (32/64 ビット)、Microsoft Windows Vista/Vista Service Pack 1(32/64 ビット)

注意: システム要件の詳細については、Readme をご参照ください。

注意: システム要件に記載されているオペレーティングシステムの種類やハードディスク容量などは、本ドキュメント作成時点の情報です。システム要件は、オペレーティングシステムのサポート終了や、弊社製品の改良、検索エンジンやパターンファイルのバージョンアップなどに伴い、変更、追加、または削除される場合があります。また、製品の運用環境によっては、ログファイルの保存、他のソフトウェアとの共存などにより、必要となるメモリサイズやハードディスク容量も異なりますので、ご注意ください。最新の情報については、弊社 Web サイトやサポート窓口にご確認ください。

インストール

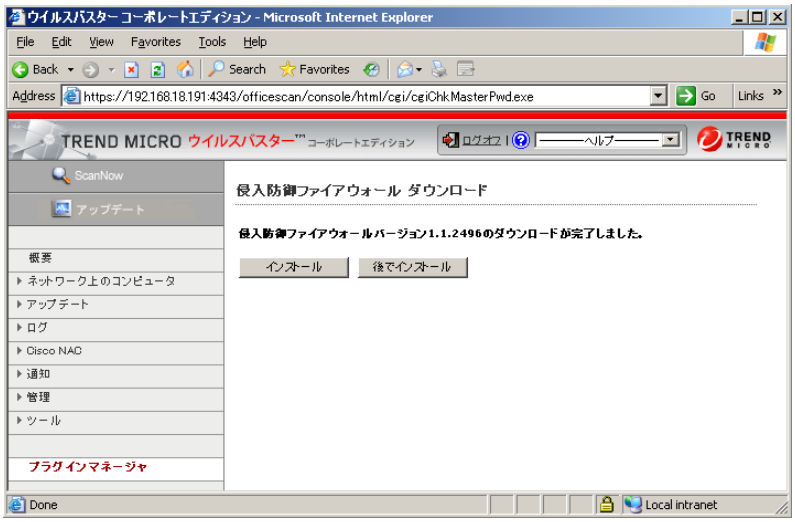
1. 侵入防御ファイアウォールをダウンロードする



ウイルスバスター Corp.プラグインマネージャから [侵入防御ファイアウォール] を選択して [ダウンロード] をクリックします。

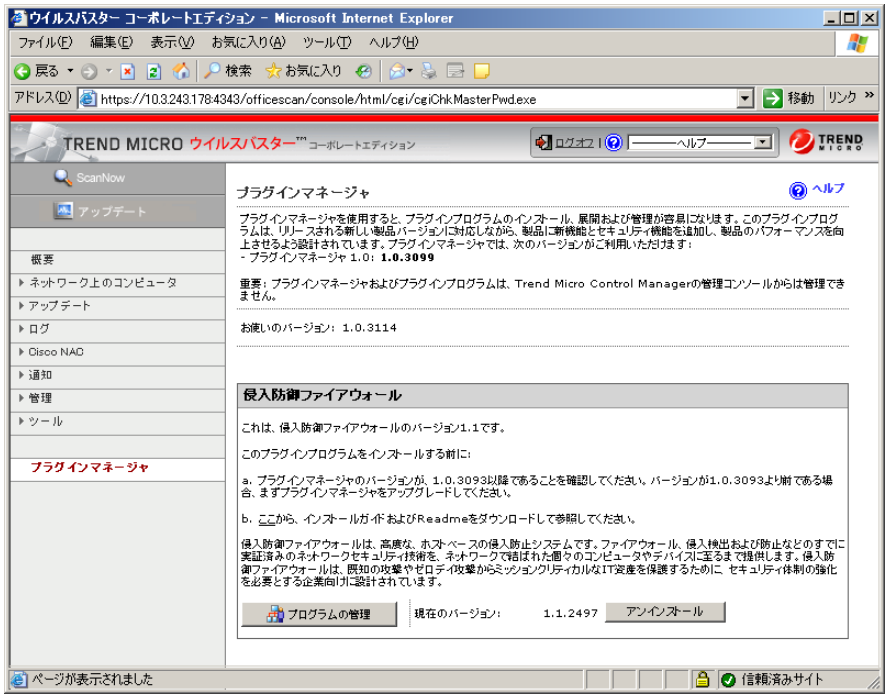
ダイアログボックスで、[OK] をクリックしてダウンロードを確認し、ダウンロードが完了するまで待ちます。

2. 侵入防御ファイアウォールをインストールする



[インストール] をクリックします。新規インストールの場合またはアクティベーションコードを使用してライセンスを更新する場合は、使用許諾契約書に同意するように求められます。使用許諾契約書を読み、契約書に同意して続行します。

インストールには数分かかります。



侵入防御ファイアウォールサーバプラグインのインストールが完了したら、[プログラムの管理] をクリックして、侵入防御ファイアウォールのアクティベーションを実行します。

侵入防御ファイアウォールサーバプラグインを初めて実行する際に、証明書の警告が表示される場合があります。これは、サーバプラグインがウイルスバスター Corp.サーバとは異なる Web サーバで実行されているためです。この証明書に同意しても安全です。警告が表示されたら、[証明書のインストール] ボタンをクリックして、初期設定の場所にインストールします。

サーバプラグインのアップグレード

侵入防御ファイアウォールサーバプラグインの新規バージョンが使用可能かどうかは、[プラグインマネージャ] 画面に表示されます。新規バージョンは現行バージョンの上に表示されます。新規バージョンにアップグレードするには、[ダウンロード] ボタンをクリックします。新規バージョンのダウンロードを終了すると、ボタンが [アップグレード] に変わります。[アップグレード] をクリックして、サーバプラグインをアップグレードします。

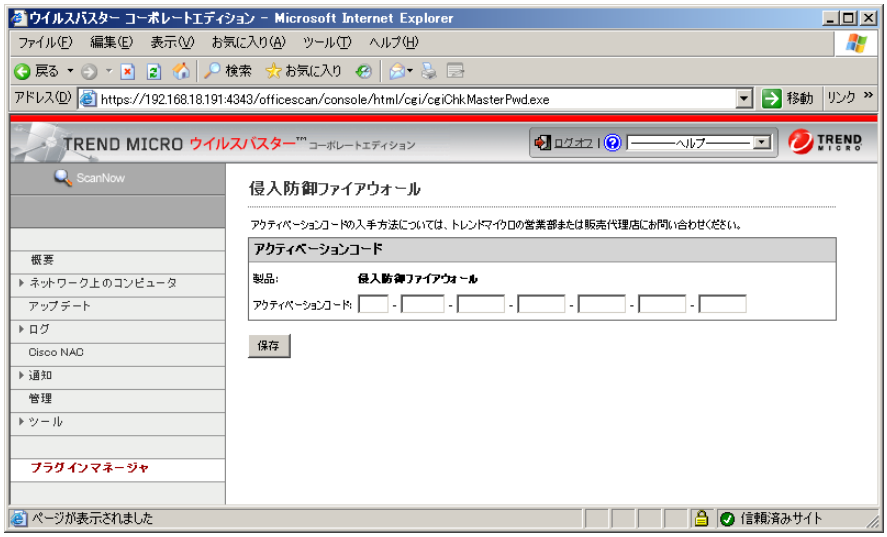
侵入防御ファイアウォールサーバプラグインのアクティベーション

1. セキュリティ証明書をインストールする

侵入防御ファイアウォールサーバプラグインのアクティベーションを初めて実行する際に、Microsoft Security 証明書の警告が表示される場合があります。

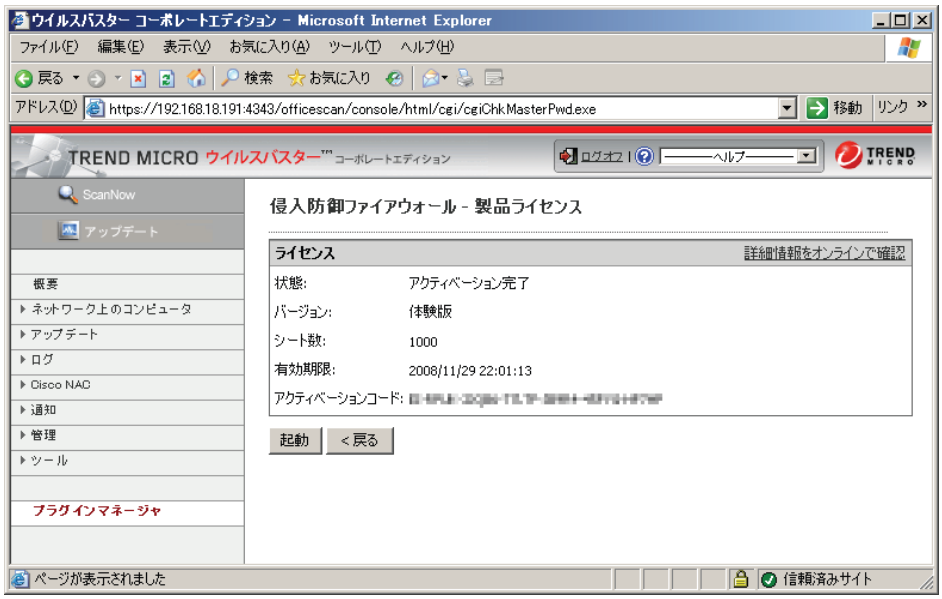
[証明書の表示] をクリックしてから、[証明書の情報] 画面で [証明書のインストール] をクリックします。証明書のインポートウィザードの指示に従って、証明書を証明書ストアにインポートします。

2. アクティベーションコードを入力する



侵入防御ファイアウォールのアクティベーションコードを入力し、[保存] をクリックして登録を完了します。

> アクティベーションコード全体をすばやく入力するには、最初のコードエントリボックスでクリックしてから、あらかじめコピーしておいたアクティベーションコード全体を貼り付けます。アクティベーションコードがない場合は、トレンドマイクロの営業担当者またはサポートに連絡してください。



[起動] をクリックして、侵入防御ファイアウォールを起動します。

ローカルアップデート元を指定した侵入防御ファイアウォールサーバコンポーネントのインストール

ウイルスバスター Corp.サーバがインターネットに接続できない場合、ウイルスバスター Corp.サーバ (ローカルホスト) に侵入防御ファイアウォールコンポーネントをインストールして、ウイルスバスター Corp.のローカルアップデート元を指定する必要があります。

注意: 続行する前に、トレンドマイクロからインストールパッケージを入手します。インストールパッケージには、侵入防御ファイアウォールコンポーネントのセットアップファイルが含まれています。

ローカルアップデート元を指定して侵入防御ファイアウォールをインストールするには

1. ウイルスバスター Corp.サーバ上に、仮想ディレクトリ「IDF」を作成します。
   - IIS Web サーバを使用している場合は、[インターネット インフォメーション サービス (IIS) マネージャ] 画面を開いて、[既定の Web サイト] を右クリックします。次に [新規作成]→[仮想ディレクトリ] の順に選択します。
   - Apache Web サーバを使用している場合は、httpd.conf ファイル内の新規仮想ディレクトリを指定して、Apache サービスを再起動します。httpd.conf ファイル内の仮想ディレクトリ「IDF」の例を以下に示します。

```
#IDF Plug-in Active Update
Alias /IDF "C:/TmUpdate/IDF/"
<Directory "C:/TmUpdate/IDF">
Options None
AllowOverride None
Order allow,deny
Allow from all
</Directory>
```

2. トレンドマイクロから入手したインストールパッケージを展開します。
3. 「activeupdate」フォルダを仮想ディレクトリにコピーします。画面に表示される指示に従い、ディレクトリ内のすべての既存フォルダの上書きに同意します。

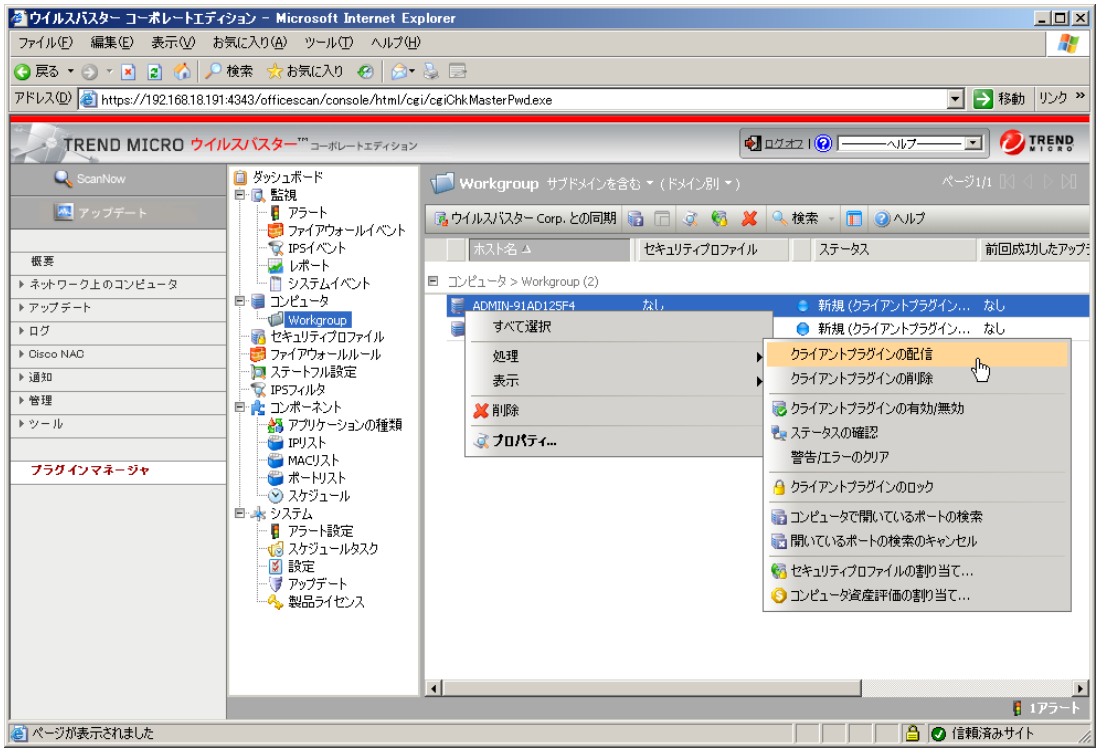
ウイルスバスター Corp.のローカルアップデート元を指定するには

1. ウイルスバスター Corp. Web コンソールにログオンして、[アップデート]→[サーバ]→[アップデート元] の順に選択します。[サーバアップデート元] 画面が表示されます。
2. [その他のアップデートサーバ] を選択し、表示されたフィールドに「http://localhost:8080/IDF/activeupdate」と入力します。[保存] をクリックします。
3. ウイルスバスター Corp.プラグインマネージャサービス (OfficeScan Plug-in Manager) を再起動して、変更を反映します。
4. ウイルスバスター Corp. Web コンソールに再度ログオンして、[プラグインマネージャ] をクリックします。
5. 画面上の指示に従って、ウイルスバスター Corp.サーバ上に侵入防御ファイアウォールプラグインをダウンロードしてインストールします。
6. インストールが完了したら、[プログラムの管理] をクリックして、侵入防御ファイアウォールの設定画面にアクセスします。
7. アクティベーションコードを入力して、製品を登録します。製品登録が完了すると、侵入防御ファイアウォールプラグインの [はじめに] ページが表示されます。

侵入防御ファイアウォールクライアントプラグインのインストール

クライアントプラグインを配信する

侵入防御ファイアウォール管理コンソールから、[コンピュータ] に進み、クライアントプラグインのインストール先であるコンピュータ (またはドメイン) を右クリックします。[処理] メニューから、[クライアントプラグインの配信] を選択します。



選択されたコンピュータにクライアントプラグインが配信されるまで待ちます。このプロセスの間、コンピュータの [ステータス] 列に、クライアントプラグインが配信中であるというメッセージが表示されます。

クライアントプラグインの配信が完了すると、コンピュータの [ステータス] 列に「管理対象 (オンラインのクライアントプラグイン)」というメッセージが表示されます。

エンタープライズクライアントファイアウォール (ECF) から侵入防御ファイアウォールへの移行

侵入防御ファイアウォールのファイアウォールとウイルスバスター Corp.エンタープライズクライアントファイアウォール (ECF) は、別個のファイアウォールで、一度にどちらか 1 つしか使用できません。移行中にコンピュータを公開したままにせずに、ウイルスバスター Corp.ファイアウォールから侵入防御ファイアウォールのファイアウォールに切り替えるには、次の指示に従ってください。

> 侵入防御ファイアウォールでは IPS (侵入防御システム) または IDS (侵入検知システム) 機能のみを使用して、ウイルスバスター Corp.エンタープライズクライアントファイアウォールの使用を続行するユーザもいます。そのような場合は、サーバプラグインがクライアントプラグインと通信できるように、次の手順を実行する必要があります (最後の手順「ウイルスバスター Corp.エンタープライズクライアントファイアウォールを無効にする」を除く)。

1. ウイルスバスター Corp.ファイアウォール設定を変更する

ウイルスバスター Corp.エンタープライズクライアントファイアウォールをセキュリティレベル「中」または「高」に設定して使用している場合、次のクライアントポートをサーバプラグインに対して開く必要があります。これにより、ウイルスバスター Corp.ファイアウォールが有効になっている間も侵入防御ファイアウォールサーバプラグインが侵入防御ファイアウォールクライアントプラグインと通信できるようになります。

TCP 4118 (サーバプラグインからクライアントプラグインへの通信に使用するポート)
TCP 4119 (サーバプラグイン Web コンソールのポート)
TCP 4120 (クライアントプラグインからサーバプラグインへの通信に使用するポート)

ウイルスバスター Corp.ファイアウォール設定を変更するには

1. 新規のウイルスバスター Corp.ファイアウォールポリシーを侵入防御ファイアウォールポリシーという名前で作成します (ウイルスバスター Corp.ファイアウォールポリシーおよびプロファイルの作成についての詳細は、ウイルスバスター Corp.のオンラインヘルプを参照してください)。
2. ポリシーに新規例外を追加します。
   名前: 侵入防御ファイアウォール例外
   処理: ネットワークトラフィックを許可
   方向: 受信および送信
   プロトコル: TCP
   ポート: 特定のポート番号:
   - **4118** (サーバプラグインからクライアントプラグインへの通信に使用するポート)
   - **4119** (サーバプラグイン Web コンソールのポート)
   - **4120** (クライアントプラグインからサーバプラグインへの通信に使用するポート)

   IP アドレス: ウイルスバスター Corp.サーバの IP アドレス
3. 新規のウイルスバスター Corp.ファイアウォールプロファイルを侵入防御ファイアウォールポリシーという名前で作成します。
   - ポリシーを侵入防御ファイアウォールプロファイルに設定します。
   - このプロファイルは、侵入防御ファイアウォールに切り替えられるすべてのコンピュータに適用する必要があります。

2. 適切なセキュリティプロファイルをコンピュータに割り当てる

侵入防御ファイアウォールには次の 3 つの事前定義されたセキュリティプロファイルが含まれています。Windows ノートパソコンプロファイル、Windows ワークステーションプロファイル、およびウイルスバスター Corp.サーバプロファイルです。

セキュリティプロファイルは、ファイアウォールルール、IPSフィルタ、およびステートフル設定のセットで構成されています (前述の「侵入防御ファイアウォールについて」を参照)。セキュリティプロファイルのプロパティは、[セキュリティプロファイル] 画面のセキュリティプロファイルをダブルクリックすると参照できます。使用可能なタブをクリックすると、セキュリティプロファイルがどのフィルタやルールなどを適用しているか参照できます。

セキュリティプロファイルは、同様のニーズを持つ複数のコンピュータで再利用することを目的としています。セキュリティプロファイルの例をコピーしてから (セキュリティプロファイルを右クリックして [複製] を選択)、ニーズに合うようにカスタマイズできます。侵入防御ファイアウォールには、安全なスタートポイントとして 3 つのセキュリティプロファイルがあります。

コンピュータのリストを確認し、適切なセキュリティプロファイルを割り当てます (右クリックメニューで [処理]→[セキュリティプロファイルの割り当て...] で選択した機能を使用)。

3. ドメインコントローラIPリストを編集する

Windows ドメインを使用している場合、ドメインコントローラの IP リストのプロパティを編集して、ドメインコントローラすべての IP アドレスを追加する必要があります。[コンポーネント]→[IP リスト] の順に選択し、[ドメインコントローラ] の IP リストをダブルクリックします。ドメインコントローラの IP アドレスを追加します。

4. ウイルスバスター Corp.エンタープライズクライアントファイアウォールを無効にする

ウイルスバスター Corp.エンタープライズクライアントファイアウォール (ECF) を安全に無効にすることができます。

ウイルスバスター Corp.ファイアウォールを無効にするには

1. ウイルスバスター Corp. Web コンソールを開きます。
2. [管理]→[製品ライセンス] の順に選択します。
3. [追加サービス] で [無効] ボタンをクリックします。
4. ログオフしてから、ウイルスバスター Corp. Web コンソールにログオンして、正しいファイアウォールステータスを表示します。

侵入防御ファイアウォールのアンインストール

侵入防御ファイアウォールクライアント/サーバプラグインのアンインストール手順については、管理者ガイドの「アンインストール方法」の項を参照してください。

サーバプラグインインストールのトラブルシューティング

エラーメッセージ:「続行できません。トレンドマイクロのプラグインマネージャはバージョン 1.0.1332 以上を使用する必要があります。」
解決策: トレンドマイクロのプラグインマネージャのバージョンを確認します。バージョン 1.0.1332 以上をダウンロードしてインストールできない場合は、サポートに問い合わせてください。プラグインマネージャは、侵入防御ファイアウォールをインストールする前にアップグレードする必要があります。

エラーメッセージ：「続行できません。最小 1,500MB のディスクの空き容量が必要ですが、*n* しかありません。」
解決策: ディスクの空き容量を増やしてから、インストールを再度実行してください。ウイルスバスター Corp.サーバがインストールされているディスクドライブと同じドライブの空き容量が必要です。

エラーメッセージ:「Windows Installer バージョン 3.1 以上が必要です。」
解決策: Windows Update を実行し、Windows Installer を最新バージョンにしてください。

エラーメッセージ：「Microsoft Data Access Components (MDAC) バージョン 2.81 以上が必要です。」
解決策: 次のリンク先から、MDACをダウンロードしてインストールします。
http://www.microsoft.com/downloads/details.aspx?displaylang=ja&FamilyID=78cac895-efc2-4f8e-a9e0-3a1afbd5922e
(MDACは、Windows Update中にはインストール/アップデートされません。)

エラーメッセージ:「Microsoft .NET Framework バージョン 2.0 以上が必要です。」
解決策: Windows Updateを使用するか、または次のリンク先から、Microsoft .NET 2.0 をダウンロードしてインストールします。http://www.microsoft.com/downloads/details.aspx?FamilyID=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=ja

エラーメッセージ:「続行できません。システムディレクトリが見つかりませんでした。」
解決策: サポートに問い合わせてください。エラーの診断に使用されるログの収集においてサポートが提供されます。

エラーメッセージ:「アドオンレジストリキー {キー名} に書き込みができません。レジストリ権限を確認して、再度入力してください。」
解決策: プラグインマネージャサービスのアクセス権をチェックして、レジストリへの書き込みに必要な特権があることを確認してください。

エラーメッセージ:「SQL インストールに失敗しました。次の場所でログをチェックします。{システムドライブ}:¥Program Files¥Microsoft SQL Server¥90¥Setup Bootstrap¥LOG¥Files」
解決策: ユーザのシステムがSQL Server Express 2005 のハードウェアおよびソフトウェア要件 (次のURLを参照) を満たしていることを確認してください。http://msdn.microsoft.com/ja-jp/library/ms143680.aspx
要件を満たしている場合は、エラーメッセージの該当ログを調査してください。SQLSetup*x_x*_Core(Local).log ファイルに次の内容に類似したエラーが含まれる場合があります。

"{システムドライブ}:¥Program Files¥Microsoft SQL Server¥90¥Setup Bootstrap¥LOG¥Files¥SQLSetup0004_D-A-13_.NET Framework 2.0.log" to cab file : "{システムドライブ}:¥Program Files¥Microsoft SQL Server¥90¥Setup Bootstrap¥LOG¥SqlSetup0004.cab" Error Code : 2”

この場合は、Microsoft .NET Framework 2.0 を再インストールします。.NET インストールエラーと考えられます。解決できない場合は、サポートに問い合わせてください。

他の SQL エラーの場合は、サポートに連絡して、エラーメッセージの該当ディレクトリにあるログファイルを送信してください。

エラーメッセージ:「侵入防御ファイアウォールのインストールに失敗しました。{ログ名} のログを確認してください。」
解決策: 予期せぬ一般エラーが発生しました。エラーメッセージの該当ログを調べて、必要であればサポートに問い合わせてください。

侵入防御ファイアウォールのインストールに失敗しても、SQL Server Express 2005 は正常にインストールされ、システム内にそのままインストールされている可能性があります。以降の侵入防御ファイアウォールのインストール手順では、この最初のインスタンス SQL Server Express が使用されます。侵入防御ファイアウォールを再インストールせずに、SQL のこのインスタンスを削除するには、次のコマンドを実行して、データベースインスタンスを手動でアンインストールします。

"{システムドライブ}:¥Program Files¥Trend Micro¥OfficeScan¥PCCSRC¥Admin¥Utility¥SQL¥SQL.EXE" /qn REMOVE=SQL_Engine INSTANCENAME=IDF

データベースが削除されたら、次のディレクトリが存在しないこと、または IDF.mdf ファイルが削除されていることのいずれかを確認します (必要な場合は IDF.mdf および IDF_log.LDF を削除してください)。

{システムドライブ}:¥Program Files¥Microsoft SQL Server¥MSSQL.1¥MSSQL¥Data

また、次のディレクトリが削除されていることも確認してください (削除されていない場合は削除してください)。

{システムドライブ}:¥Program Files¥Trend Micro¥OfficeScan¥Addon¥Intrusion Defense Firewall