ウイルスバスター™ コーポレートエディション

インストールガイド

安心を、ひとつ上のステージへ。

TREND MICRO™

トレンドマイクロへのお客様情報の送信について

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

輸出規制について

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

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

2008年12月現在、米国により定められる禁輸国は、キューバ、イラン、北朝鮮、スーダン、シリアが含まれています。
あなたは本製品に関連した米国輸出管理法令の違法行為に対して責任があります。本契約の同意により、あなたは、あなたが米国により現時点で禁止されている国の居住者もしくは国民ではないこと、別途本製品を受け取ることが禁止されていないことを確認します。また、大量破壊を目的とした、核兵器、化学兵器、生物兵器、ミサイルの開発、設計、製造、生産を行うために使用しないことに同意します。

複数年契約について

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

http://jp.trendmicro.com/jp/support/lifecycle/index.html

著作権について

P/N: OSFFFF-AE0112 (2009/07)

目次

はじめに

はじめに

トレンドマイクロ 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.) インストールガイドへようこそ。本書では、ウイルスバスター Corp. サーバのインストール要件と手順、およびサーバとクライアントのアップグレード方法について説明しています。

注意： クライアントのインストールについては、管理者ガイドを参照してください。

この章で説明する内容には、次の項目が含まれます。

ウイルスバスター Corp. 付属のドキュメント

ウイルスバスター Corp. に付属するドキュメントは以下のとおりです。

表 1.　ウイルスバスター Corp. 付属のドキュメント

ドキュメント	説明
インストールガイド	ウイルスバスター Corp. サーバをインストールし、サーバとクライアントをアップグレードするための要件および手順を説明した PDF ドキュメント
管理者ガイド	使用開始にあたっての情報、クライアントのインストール手順、およびウイルスバスター Corp. サーバとクライアントの管理について説明した PDF ドキュメント
ウイルスバスター Corp. 用スマートスキャン クイックスタートガイド	スマートスキャンの概念、スマートスキャンを使用するために必要な環境の準備、およびスマートスキャンクライアントの管理について説明した PDF ドキュメント
ヘルプ	WebHelp 形式または CHM 形式にコンパイルされた、操作手順、使用にあたってのアドバイス、および目的別の作業手順を提供するオンラインヘルプ。このヘルプには、ウイルスバスター Corp. サーバ、ウイルスバスター Corp. クライアント、ポリシーサーバのコンソール、およびウイルスバスター Corp. サーバセットアップからアクセスできます。
Readme ファイル	既知の問題のリストと基本的なインストール手順が含まれています。ヘルプや印刷物では見られない、最新の製品情報も含まれています。
製品 Q&A	問題解決およびトラブルシューティング情報の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の情報を得ることができます。製品 Q&A にアクセスするには、以下の Web サイトをご覧ください。 http://esupport.trendmicro.co.jp/

最新のドキュメントおよび Readme ファイルは、次の Web サイトからダウンロードできます。

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

対象読者

ウイルスバスター Corp. 付属のドキュメントは、次のユーザを対象としています。

- **ウイルスバスター Corp. 管理者**： サーバおよびクライアントのインストールと管理を含むウイルスバスター Corp. 管理の責任者。ネットワーキングおよびサーバ管理についての高度な知識を持つユーザであることが想定されています。
- **Cisco NAC 管理者** : Cisco NAC サーバおよび Cisco のネットワーク機器を使用したセキュリティシステムの設計および管理責任者。対象機器の使用経験があるユーザであることが想定されています。
- **エンドユーザ**： 使用しているコンピュータにウイルスバスター Corp. クライアントをインストールしているユーザ。コンピュータ初心者から上級ユーザまでを対象としています。

ドキュメントの表記規則

情報を簡単に特定して理解できるようにするため、ウイルスバスター Corp. 付属のドキュメントでは次の表記規則を使用しています。

表 2.　ドキュメントの表記規則

表記規則	説明
注意： テキスト	設定上の注意事項または推奨事項について説明します。
ヒント： テキスト	ベストプラクティス情報およびトレンドマイクロの推奨事項について説明します。
警告： テキスト	ネットワーク上のコンピュータが損傷を受ける可能性のある操作について警告します。

用語

次の表は、ウイルスバスター Corp. 付属のドキュメントで使用されている正式な用語を示しています。

表 3.　ウイルスバスター Corp. の用語

用語	説明
クライアント	ウイルスバスター Corp. クライアントプログラム
クライアントコンピュータまたはエンドポイント	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
クライアントユーザ (またはユーザ)	クライアントコンピュータでウイルスバスター Corp. クライアントを使用する人
サーバ	ウイルスバスター Corp. サーバプログラム
サーバコンピュータ	ウイルスバスター Corp. サーバがインストールされているコンピュータ
管理者 (またはウイルスバスター Corp. 管理者)	ウイルスバスター Corp. サーバを管理する人
コンソール	ウイルスバスター Corp. サーバおよびクライアントを設定および管理するためのユーザインタフェース。 ウイルスバスター Corp. サーバプログラム用のコンソールを「Web コンソール」、クライアントプログラム用のコンソールを「クライアントコンソール」といいます。
セキュリティリスク	ウイルス / 不正プログラム、スパイウェア / グレーウェア、および Web からの脅威の総称
製品サービス	ウイルス対策、ダメージクリーンナップサービス、Web レピュテーションおよびスパイウェア対策を含みます。これらはすべてウイルスバスター Corp. サーバのインストール時にアクティベートされます。
ウイルスバスター Corp. サービス	Microsoft 管理コンソール (MMC) によってホストされるサービス。たとえば、OfficeScan Master Service の ofcservice.exe などです。
プログラム	ウイルスバスター Corp. クライアント、Cisco Trust Agent、およびプラグインマネージャを含みます。

表 3.　ウイルスバスター Corp. の用語 (続き)

用語	説明
コンポーネント	セキュリティ上の脅威の検索、検出、および処理を実行するものです。
クライアントのインストールフォルダ	ウイルスバスター Corp. クライアントのファイルが含まれるコンピュータ上のフォルダ。インストール時の初期設定を受け入れると、インストールフォルダは次のいずれかの場所に設定されます。 C:¥Program Files¥Trend Micro¥OfficeScan Client C:¥Program Files (x86)¥Trend Micro¥OfficeScan Client
サーバのインストールフォルダ	ウイルスバスター Corp. サーバのファイルが含まれるコンピュータ上のフォルダ。インストール時の初期設定を受け入れると、インストールフォルダは次のいずれかの場所に設定されます。 C:¥Program Files¥Trend Micro¥OfficeScan C:¥Program Files (x86)¥Trend Micro¥OfficeScan たとえば、サーバのインストールフォルダで ¥PCCSRV の下にあるファイルのフルパスは次のようになります。 C:¥Program Files¥Trend Micro¥OfficeScan¥PCCSRV¥< ファイル名 >
スマートスキャンクライアント	スマートスキャンを使用するように設定されているウイルスバスター Corp. クライアント
従来型スキャンクライアント	従来型スキャンを使用するように設定されているウイルスバスター Corp. クライアント

第 1 章

トレンドマイクロ ウイルスバスター コーポレートエディションのインストールの計画

この章で説明する内容には、次の項目が含まれます。

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、OS 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。最新のシステム要件については、弊社 Web サイトやサポート窓口にご確認ください。

新規インストール要件

以下は、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.) サーバと Web コンソールの要件です。

ウイルスバスター Corp. サーバ

以下は、ウイルスバスター Corp. サーバを新規インストールする場合の要件です。

表 1-1. ウイルスバスター Corp. サーバシステム要件

リソース	要件
OS	Windows 2000 ・ Microsoft Windows 2000 Server Service Pack 4 ・ Windows 2000 Advanced Server Service Pack 4 ・ Microsoft Cluster Server 2000 役割ベースの管理機能を使用するには次のコンポーネントをインストールします。 ・ Microsoft パッチ KB890859 ・ Microsoft パッチ KB924270 ・ Windows 2000 Authorization Manager Runtime Windows 2003 ・ Windows Server 2003 Standard/Enterprise/Datacenter Edition Service Pack 2、32 ビットおよび 64 ビットバージョン ・ Windows Server 2003 R2 Standard/Enterprise/Datacenter Edition Service Pack 2、32 ビットおよび 64 ビットバージョン ・ Windows Storage Server 2003 R2、32 ビットおよび 64 ビットバージョン ・ Microsoft Cluster Server 2003 Windows 2008 ・ Windows Server 2008 Standard/Enterprise/Web Edition Service Pack 1、32 ビットおよび 64 ビットバージョン ・ Microsoft Cluster Server 2008 ※ Windows 2008 が、Server Core 環境で実行されている場合はウイルスバスター Corp. をインストールできません。

表 1-1.　ウイルスバスター Corp. サーバシステム要件（続き）

リソース	要件
仮想化	ウイルスバスター Corp. サーバは、次の仮想化アプリケーションでホストされている Windows 2000/2003/2008 のゲスト OS にインストールできます。 ・ VMware ESX/ESXi Server 3.5 (サーバエディション) ・ VMware Server 1.0.3 以降 (サーバエディション) ・ VMware Workstation および Workstation ACE Edition 6.0 また、Microsoft Virtual Server 2005 R2 Service Pack 1 でホストされている Windows 2000 および 2003 (32 ビット) のゲスト OS にもサーバをインストールできます。
ハードウェア (Windows Server 2008)	**プロセッサ** ・ 最低 1GHz Intel Pentium または同等の x86 プロセッサ、および 1.4GHz の x64 プロセッサ (2GHz を推奨) ・ 統合スマートスキャンサーバをインストールする場合は、最低 1.86GHz Intel Core2Duo ・ AMD ™ 64 および Intel 64 プロセッサアーキテクチャ RAM ・ 最低 512MB、2GB を推奨 ・ 統合スマートスキャンサーバをインストールする場合は最低 1GB **ハードディスク空き容量** ・ ウイルスバスター Corp. サーバ、ウイルスバスター Corp. クライアント、Policy Server for Cisco NAC、および統合スマートスキャンサーバをローカルでインストールする場合には、最低 2.8GB ・ ウイルスバスター Corp. サーバ、ウイルスバスター Corp. クライアント、および統合スマートスキャンサーバをリモートからインストールする場合には、最低 3.2GB **その他** ・ ギガビットネットワークインタフェースカード (NIC) ・ 解像度 800x600、256 色以上をサポートするモニタ

表 1-1.　ウイルスバスター Corp. サーバシステム要件（続き）

リソース	要件
ハードウェア (他のすべてのプラットフォーム)	**プロセッサ** • 800MHz Intel Pentium または同等の CPU • 統合スマートスキャンサーバをインストールする場合は、最低 1.86GHz Intel Core2Duo RAM • 最低 512MB、1GB を推奨 • 統合スマートスキャンサーバをインストールする場合は最低 1GB **ハードディスク空き容量** • ウイルスバスター Corp. サーバ、ウイルスバスター Corp. クライアント、Policy Server for Cisco NAC、および統合スマートスキャンサーバをローカルでインストールする場合には、最低 2.8GB • ウイルスバスター Corp. サーバ、ウイルスバスター Corp. クライアント、および統合スマートスキャンサーバをリモートからインストールする場合には、最低 3.2GB **その他** • ギガビットネットワークインタフェースカード (NIC) • 解像度 800x600、256 色以上をサポートするモニタ

Web サーバ	• Microsoft Internet Information Server (IIS)
	  • Windows 2000: バージョン 5.0
	  • Microsoft Windows Server 2003: バージョン 6.0
	  • Microsoft Windows Server 2008: バージョン 7.0
	• Apache Web サーバ 2.0.x
	注意： Apache Web サーバがコンピュータに存在しても、バージョンが 2.0.x ではない場合、ウイルスバスター Corp. はバージョン 2.0.63 をインストールして使用します。既存の Apache Web サーバは削除されません。

その他	• サーバコンピュータにおける管理者またはドメイン管理者アクセス • サーバコンピュータにインストールされた Microsoft Networks を共有するファイルおよびプリンタ • Cisco Trust Agent (CTA) をウイルスバスター Corp. サーバと同じコンピュータ上にインストールする場合は、ウイルスバスター Corp. サーバを Windows Server 2003 x64 Edition にはインストールしないでください。CTA の要件の詳細については管理者ガイドを参照してください。

Web コンソール

以下は、Web コンソールの起動およびアクセスの要件です。

表 1-2.　Web コンソールの要件

リソース	要件
ハードウェア	**プロセッサ** 300MHz Intel Pentium または同等の CPU **RAM** 最低 128MB **ハードディスク空き容量** 最低 30MB **その他** 解像度 800x600、256 色以上をサポートするモニタ
ブラウザ	Microsoft Internet Explorer 6.0 以上

アップグレードの要件

このバージョンのウイルスバスター Corp. では、次のバージョンからのアップグレードがサポートされています。

- 8.x
  - 8.0
  - 8.0 Service Pack 1

  バージョン 8.x からアップグレードする場合、サーバおよびクライアントでこのバージョンのウイルスバスター Corp. を実行するためにコンピュータリソースの追加が必要になる場合があります。詳細については、18 ページの「ウイルスバスター Corp. 8.x サーバ」および 20 ページの「ウイルスバスター Corp. 8.x クライアント」を参照してください。
- 7.x
  - 7.3
  - 7.0

  バージョン 7.x からアップグレードする場合、サーバおよびクライアントでこのバージョンのウイルスバスター Corp. を実行するためにコンピュータリソースの追加が必要になる場合があります。詳細については、20 ページの「ウイルスバスター Corp. 7.x サーバ」および 21 ページの「ウイルスバスター Corp. 7.x クライアント」を参照してください。

ウイルスバスター Corp. 8.x サーバ

バージョン「8.x」でサポートされている OS はすべてこのバージョンでサポートされています。

アップグレードする前に、次のタスクを実行してください。

1. 必要な Microsoft Service Pack を適用します。
   - Windows 2000 Server に対して Service Pack 4
   - Windows Server 2003 に対して Service Pack 2

2. このバージョンのウイルスバスター Corp. を実行するためにサーバコンピュータでリソースの追加が必要かどうかを確認します。詳細は次の表を参照してください。

表 1-3. ウイルスバスター Corp. 10 と 8.x サーバの最低要件の違い

リソース	ウイルスバスター Corp. 8.x サーバの要件	ウイルスバスター Corp. 10 サーバの要件
プロセッサ	800MHz Intel Pentium または同等の CPU	統合スマートスキャンサーバをインストールする場合は、1.86GHz Intel Core2Duo
RAM	512MB	統合スマートスキャンサーバをインストールする場合は 1GB
ディスク空き容量	1GB	• ウイルスバスター Corp. サーバ、ウイルスバスター Corp. クライアント、Policy Server for Cisco NAC、および統合スマートスキャンサーバをローカルでインストールする場合には、2.8GB • ウイルスバスター Corp. サーバ、ウイルスバスター Corp. クライアント、および統合スマートスキャンサーバをリモートからインストールする場合には、3.2GB
Web サーバ	Apache Web サーバ 2.0 以上	Apache Web サーバ 2.0.x
ブラウザ (Web コンソールおよび Web インストールページ用)	Microsoft Internet Explorer 5.5 Service Pack 1 以上	Microsoft Internet Explorer 6.0 以上

ウイルスバスター Corp. 8.x クライアント

バージョン「8.x」でサポートされている OS はすべてこのバージョンでサポートされています。

Windows XP Professional および Windows Server 2008 を実行するクライアントには、追加の Microsoft Service Pack が必要です。アップグレードする前に、次の Service Pack を適用してください。

- Windows XP Professional に対して Service Pack 2 以上
- Windows Server 2003 に対して Service Pack 2
- Windows Server 2008 に対して Service Pack 1

他のサポート対象 OS の場合、バージョン 8.x とこのバージョンに必要な Service Pack は同じものです。

ウイルスバスター Corp. 7.x サーバ

次の OS を実行しているウイルスバスター Corp.「7.x」サーバは、アップグレード可能です。

- Windows 2000 Server
- Windows Server 2003

次の OS を実行しているウイルスバスター Corp. サーバは、アップグレードできません。

- Windows NT シリーズ

アップグレードする前に、次のタスクを実行してください。

1. 必要な Microsoft Service Pack を適用します。
   - Windows 2000 Server に対して Service Pack 4
   - Windows Server 2003 に対して Service Pack 2

2. このバージョンのウイルスバスター Corp. を実行するためにサーバコンピュータでリソースの追加が必要かどうかを確認します。詳細は次の表を参照してください。

表 1-4. ウイルスバスター Corp. 10 と 7.x サーバの最低要件の違い

リソース	ウイルスバスター Corp. 7.x サーバの要件	ウイルスバスター Corp. 10 サーバの要件
プロセッサ	300MHz Intel Pentium II プロセッサまたは同等の CPU	• 800MHz Intel Pentium または同等の CPU • 統合スマートスキャンサーバをインストールする場合は、1.86GHz Intel Core2Duo
RAM	128MB	• 512MB • 統合スマートスキャンサーバをインストールする場合は 1GB
ディスク空き容量	• ウイルスバスター Corp.7.3 の場合 600MB • ウイルスバスター Corp.7.0 の場合 300MB	• ウイルスバスター Corp. サーバ、ウイルスバスター Corp. クライアント、Policy Server for Cisco NAC、および統合スマートスキャンサーバをローカルでインストールする場合には、2.8GB • ウイルスバスター Corp. サーバ、ウイルスバスター Corp. クライアント、および統合スマートスキャンサーバをリモートからインストールする場合には、3.2GB
Web サーバ	Apache Web サーバ 2.0 以上	Apache Web サーバ 2.0.x
ブラウザ (Web コンソールおよび Web インストールページ用)	Microsoft Internet Explorer 5.5 Service Pack 1 以上	Microsoft Internet Explorer 6.0 以上

ウイルスバスター Corp. 7.x クライアント

次の OS を実行しているウイルスバスター Corp.「7.x」クライアントは、アップグレード可能です。

- Windows 2000
- Windows XP Professional
- Windows XP Home
- Windows Server 2003

次の OS で実行されているウイルスバスター Corp. 7.x クライアントは、アップグレードできません。

- Windows 95
- Windows 95 OSR2
- Windows 98
- Windows 98 SE
- Windows Me
- Windows NT 4.0
- Intel Itanium アーキテクチャ OS

サポートされていないオペレーティングシステムを実行しているクライアントがあり、それらのクライアントの管理を継続する場合には、ウイルスバスター Corp. 7.x サーバを残してください。詳細については、31 ページの「サポートされていない OS」を参照してください。

ヒント： クライアントの OS は、ウイルスバスター Corp. 7.x サーバの Web コンソールで確認できます。 [クライアント] をクリックし、[プラットフォーム] 列に進みます。

Windows 2000

Windows 2000 で動作するクライアントをアップグレードする前に、次のタスクを実行してください。

1. Service Pack 4 以上を適用します。
2. このバージョンのウイルスバスター Corp. を実行するためにクライアントコンピュータでリソースの追加が必要かどうかを確認します。詳細は次の表を参照してください。

表 1-5. ウイルスバスター Corp. 10 と 7.x クライアントの最低要件の違い

リソース	ウイルスバスター Corp. 7.x クライアントの要件	ウイルスバスター Corp. 10 クライアントの要件
プロセッサ	150MHz Intel Pentium または同等の CPU	300MHz Intel Pentium または同等の CPU

表 1-5.　ウイルスバスター Corp. 10 と 7.x クライアントの最低要件の違い（続き）

リソース	ウイルスバスター Corp. 7.x クライアントの要件	ウイルスバスター Corp. 10 クライアントの要件
RAM	64MB	256MB
ディスク空き容量	• ウイルスバスター Corp.7.3 の場合 160MB • ウイルスバスター Corp.7.0 の場合 80MB	350MB

Windows XP Professional、Windows XP Home、および Windows Server 2003

Windows XP Professional、XP Home、および Server 2003 で動作するクライアントをアップグレードする前に、次のタスクを実行してください。

1. 必要な Microsoft Service Pack を適用します。
   - Windows XP Professional に対して Service Pack 2 以上
   - Windows XP Home に対して Service Pack 3
   - Windows Server 2003 に対して Service Pack 2 以上
2. このバージョンのウイルスバスター Corp. を実行するためにクライアントコンピュータでリソースの追加が必要かどうかを確認します。詳細は次の表を参照してください。

表 1-6.　ウイルスバスター Corp. 10 と 7.x クライアントの最低要件の違い

リソース	ウイルスバスター Corp. 7.x クライアントの要件	ウイルスバスター Corp. 10 クライアントの要件
ディスク空き容量	• ウイルスバスター Corp.7.3 の場合 160MB • ウイルスバスター Corp.7.0 の場合 80MB	350MB
RAM	128MB	256MB

製品バージョンとアクティベーション

製品版および体験版

ウイルスバスター Corp. の製品版、または体験版のいずれかをインストールできます。製品版、体験版にはそれぞれ異なる種類のアクティベーションコードが必要です。アクティベーションコードをお持ちでない場合は、ユーザ登録を行ってください。

製品版

製品版では、すべての製品機能とテクニカルサポートが提供されます。サポート契約失効後の更新猶予期間 (通常 90 日) も設定されています。更新猶予期間を過ぎてもサポート契約を更新しないと、テクニカルサポートやアップデートされたコンポーネントの提供を受けられなくなります。その場合、検索エンジンでは、古いバージョンのパターンファイルを使用して検索が行われます。これらの古いバージョンのコンポーネントでは、最新のセキュリティリスクから十分にコンピュータを保護できない場合があります。サポート契約の失効前または後にメンテナンス更新の購入によってサポート契約を更新してください。

体験版

体験版には、すべての製品機能が含まれます。体験版は、いつでも製品版にアップグレードできます。体験期間終了までに製品版にアップグレードしない場合は、ウイルスバスター Corp. はアップデートや検索など、すべてのクライアント機能が使用できなくなります。

レジストレーションキーおよびアクティベーションコード

インストール時に、次のサービスのアクティベーションコードを入力します。

- ウイルス対策
- ダメージクリーンナップサービス (オプション)
- Web レピュテーションおよびスパイウェア対策

注意： 以前の製品で「Web 評価」と呼んでいた機能を、本製品から「Web レピュテーション」に名称変更しています。

アクティベーションコードをお持ちでない場合は、製品付属のレジストレーションキーを使用してください。自動的に、ユーザ登録を行うことができるトレンドマイクロの Web サイトにリダイレクトされます。

https://olr.trendmicro.com/registration/jp/ja/login.aspx

ユーザ登録後、トレンドマイクロからアクティベーションコードが送信されます。

レジストレーションキーもアクティベーションコードもお持ちでない場合は、トレンドマイクロの販売代理店にお問い合わせください。詳細については、109 ページの「製品サポート情報」を参照してください。

注意： 登録については次の Web サイトを参照してください。
http://esupport.trendmicro.co.jp/supportjp/viewxml.do?ContentID=JP-27757

新規インストールの注意事項

ウイルスバスター Corp. サーバの新規インストールを実行する場合には、次の項目にご注意ください。

- 25 ページの「ウイルスバスター Corp. サーバの場所」
- 26 ページの「リモートインストール」
- 26 ページの「サーバパフォーマンス」
- 26 ページの「専用サーバ」
- 27 ページの「インストール時に検索方法を指定」
- 28 ページの「ネットワークトラフィック」
- 29 ページの「他社製のセキュリティソフトウェア」
- 29 ページの「Active Directory」
- 30 ページの「Web サーバ」

ウイルスバスター Corp. サーバの場所

ウイルスバスター Corp. はさまざまなネットワーク環境に柔軟に対応できます。たとえば、ウイルスバスター Corp. サーバとクライアントの間にファイアウォールを設置したり、単一のネットワークファイアウォールの背後にサーバとすべてのクライアントを配置することができます。サーバとクライアントの間にファイアウォールを配置する場合は、クライアントとサーバの待機ポート間のトラフィックを許可できるようにファイアウォールを設定してください。

注意： ネットワークアドレス変換を使用するネットワーク上のウイルスバスター Corp. クライアントを管理する際に、問題が発生する可能性があります。この潜在的な問題の解決については、管理者ガイドおよびウイルスバスター Corp. サーバのヘルプを参照してください。

リモートインストール

リモートインストールにより、1 つのコンピュータから別のコンピュータにウイルスバスター Corp. をインストールできます。リモートインストールでは、対象コンピュータがサーバのインストール要件を満たしているかどうかをセットアッププログラムが検査します。

インストールを円滑に進めるため、以下のことを事前に行ってください。

- 各対象コンピュータで、ローカルシステムアカウントではなく管理者アカウントを使用してリモートレジストリサービスを開始する必要があります。リモートレジストリサービスは、Microsoft 管理コンソール (MMC) から管理します ([スタート] → [ファイル名を指定して実行] の順にクリックし、「services.msc」と入力)。
- コンピュータのホスト名やログオン情報のメモをとります (ユーザ名やパスワード)。
- コンピュータがウイルスバスター Corp. サーバのシステム要件を満たしていることを確認します。詳細については、14 ページの「新規インストール要件」を参照してください。

サーバパフォーマンス

大規模なネットワーク環境では、中小規模のネットワーク環境に比べ、サーバに対してより高い性能が要求されます。理想的には、ウイルスバスター Corp. サーバコンピュータは、最低でも 2GHz のデュアルプロセッサと、2GB 以上の RAM が必要です。

1 つのウイルスバスター Corp. サーバが管理できるネットワーク上のコンピュータクライアントの数は、使用可能なサーバリソースやお使いのネットワークトポロジなどの要因によって異なります。お使いのサーバで管理できるクライアントの数については、トレンドマイクロの販売代理店にお問い合わせください。

ウイルスバスター Corp. サーバで管理可能なクライアント数は一般的に次のとおりです。

- 2GHz のデュアルプロセッサと 2GB の RAM を備えたウイルスバスター Corp. サーバ : 3000 ～ 5000 クライアント
- 3GHz のデュアルプロセッサと 4GB の RAM を備えたウイルスバスター Corp. サーバ : 5000 ～ 8000 クライアント

専用サーバ

ウイルスバスター Corp. サーバをインストールするコンピュータを選択する場合、次の点について考慮してください。

- コンピュータの CPU 処理量
- コンピュータで実行されている他の機能

対象コンピュータに他の機能がある場合、重要なアプリケーションや、リソースを大量に消費するアプリケーションが起動していないコンピュータを選択してください。

インストール時に検索方法を指定

このウイルスバスター Corp. のバージョンでは、スマートスキャンと従来型スキャンのいずれかを使用するようにクライアントを設定できます。

従来型スキャン

従来型スキャンは、以前のすべてのウイルスバスター Corp. バージョンで使用されていた検索方法です。従来型スキャンクライアントでは、クライアントコンピュータ上にすべてのウイルスバスター Corp. コンポーネントが格納され、ローカルのすべてのファイルが検索されます。

スマートスキャン

スマートスキャンでは、クラウドに保存された脅威のシグネチャが利用されます。スマートスキャンモードでは、ウイルスバスター Corp. クライアントが最初にセキュリティリスクをローカルで検索します。クライアントが検索時にファイルの危険性を判定できない場合には、スマートスキャンサーバに接続します。

スマートスキャンには、次の機能や利点があります。

- クラウド内での高速でリアルタイムなセキュリティステータスルックアップ機能 (自身のセキュリティステータスを確認する機能) の提供
- 新たな脅威に対する保護を提供するのにかかる全体時間の短縮
- パターンアップデートで消費されるネットワーク帯域幅の削減。パターン定義の大部分のアップデートはクラウドにのみ配信します。多数のエンドポイントに配信する必要はありません。
- 企業全体のパターン配信に伴うコストとオーバーヘッドの削減
- エンドポイントにおけるカーネルメモリ消費量の低下。

検索方法の設定

ウイルスバスター Corp. サーバの新規インストールを実行し、インストール後に Web コンソールで検索方法を変更していない場合には、インストールするすべてのクライアントが従来型スキャンを使用します。各クライアントのインストール後に、すべてのクライアントまたは特定数のクライアントがスマートスキャンを使用するように設定できます。詳細については、ウイルスバスター Corp. 用スマートスキャン クイックスタートガイドで検索方法の設定のガイドラインを参照してください。

ネットワークトラフィック

インストール計画を作成する際は、ウイルスバスター Corp. が生成するネットワークトラフィックについて考慮してください。次のような場合、サーバによってトラフィックが生成されます。

- トレンドマイクロのアップデートサーバに接続して、最新のコンポーネントの有無を確認してダウンロードするとき
- 最新のコンポーネントをダウンロードするようにクライアントに通知するとき
- クライアントに設定の変更を通知するとき

次のような場合、クライアントでトラフィックが生成されます。

- 起動時
- コンポーネントをアップデートするとき
- 設定のアップデート時、および HotFix のインストール時
- セキュリティリスクの検索時
- スタンドアロンモード / 標準モードを切り替えるとき
- 従来型スキャン / スマートスキャンを切り替えるとき

コンポーネントアップデート時のネットワークトラフィック

ウイルスバスター Corp. はコンポーネントをアップデートする場合、大量のネットワークトラフィックを生成します。ウイルスバスター Corp. では、コンポーネントをアップデートするときに生じるネットワークトラフィックを軽減するために、コンポーネントの複製が実行されます。ウイルスバスター Corp. は、フルパターンファイルをダウンロードせず、「差分」パターンファイル (フルパターンファイルのより小さいバージョン) のみをダウンロードし、現行のウイルスパターンファイルに統合します。

定期的にアップデートされたクライアントは、差分パターンファイルのみをダウンロードします。そうでない場合は、フルパターンファイルをダウンロードする必要があります。

トレンドマイクロでは定期的に新しいパターンファイルを公開しています。また、トレンドマイクロは、損害を与える可能性があり、実際に流布しているウイルス / 不正プログラムを検出するとただちに新しいパターンファイルを公開します。

アップデートエージェントとネットワークトラフィック

クライアントとウイルスバスター Corp. サーバ間のネットワークに、低帯域幅または「トラフィックが多い」セグメントが存在する場合、選択したウイルスバスター Corp. クライアントを、アップデートエージェントまたはその他のクライアントのアップデート元として指定することができます。これによって、すべてのクライアントへのコンポーネント配信の負担を分散できます。

たとえば、20 台以上のコンピュータを備えたリモートオフィスがある場合は、アップデートエージェントを指定して、ウイルスバスター Corp. サーバからのアップデートを複製し、ローカルネットワーク上の他のコンピュータのローカルディストリビューションポイントとして機能させます。アップデートエージェントに関する詳細は、管理者ガイドを参照してください。

Trend Micro Control Manager およびネットワークトラフィック

Trend Micro Control Manager (以下、Control Manager) は、トレンドマイクロのゲートウェイ、メールサーバ、ファイルサーバ、およびデスクトップ向けの製品およびサービス製品を管理します。Control Manager の Web ベースの管理コンソールにより、ネットワーク全体の製品やサービスを 1ヵ所から監視することができます。

Control Manager を使用して、1ヵ所から複数のウイルスバスター Corp. サーバを管理します。Control Manager サーバが高速かつ安全にインターネットに接続されている場合、トレンドマイクロのアップデートサーバからコンポーネントをダウンロードできます。次に、Control Manager は、インターネット接続が不確実または不可能な 1 台以上のウイルスバスター Corp. サーバにコンポーネントを配信することができます。

Control Manager に関する詳細は、Control Manager のドキュメントを参照してください。

他社製のセキュリティソフトウェア

ウイルスバスター Corp. サーバをインストールするコンピュータから、他社製のエンドポイントセキュリティソフトウェアを削除してください。これらのアプリケーションは、ウイルスバスター Corp. サーバのインストールを妨げたり、パフォーマンスに影響する可能性があります。他社製のセキュリティソフトウェアを削除したら、セキュリティリスクからのコンピュータの保護を維持するためにすぐにウイルスバスター Corp. サーバおよびクライアントをインストールしてください。

注意： ウイルスバスター Corp. は他社製のウイルス対策製品のサーバコンポーネントを自動的にアンインストールすることはできませんが、クライアントコンポーネントはアンインストールできます。詳細については、管理者ガイドを参照してください。

Active Directory

役割ベースの管理およびセキュリティコンプライアンスの機能を利用するために、すべてのウイルスバスター Corp. サーバが Active Directory ドメインに属しているかどうかを確認します。

Web サーバ

ウイルスバスター Corp. の Web サーバには、次の機能があります。

- ユーザからの Web コンソールへのアクセスが可能になります。
- クライアントからの命令を受け入れ可能になります。
- クライアントによるサーバ通知への応答が可能になります。

IIS Web サーバまたは Apache Web サーバを使用することができます。IIS Web サーバを使用する場合は、サーバコンピュータで Microsoft IIS ロックダウンツールが実行されていないことを確認してください。セットアップがインストール時に、自動的に IIS サービスを停止します。

Apache Web サーバを使用する場合は、管理者アカウントのみが Apache Web サーバに作成されます。Web サーバを実行する別のアカウントを作成し、ハッカーから Apache Web サーバへの攻撃が発生した場合にウイルスバスター Corp. サーバが脆弱化するのを防止してください。

Apache Web サーバのアップグレード、パッチ、セキュリティに関する問題についての最新情報は http://www.apache.org を参照してください。

アップグレードの注意事項

ウイルスバスター Corp. サーバおよびクライアントをアップグレードするときには、次の事項に注意してください。

- 30 ページの「ウイルスバスター Corp. の設定」
- 31 ページの「サポートされていない OS」
- 32 ページの「アップグレード時に検索方法を指定」

ウイルスバスター Corp. の設定

ウイルスバスター Corp. サーバのアップグレードの前に、ウイルスバスター Corp. のデータベースと重要な設定ファイルをバックアップします。ウイルスバスター Corp. サーバデータベースは、ウイルスバスター Corp. プログラムディレクトリ以外の場所にバックアップしてください。

ウイルスバスター Corp. データベースと設定ファイルをバックアップおよび復元するには

1. ウイルスバスター Corp. 「8.x」/「7.x」Web コンソールで、[管理] → [データベースバックアップ] に進み、データベースをバックアップします。

   詳細な手順については、この製品バージョンの管理者ガイドまたはサーバのヘルプを参照してください。

   警告： 他のバックアップツールやアプリケーションを使用しないでください。

2. Microsoft 管理コンソールから、OfficeScan Master Service を停止します。
3. 以下の <「サーバのインストールフォルダ」>¥PCCSRV フォルダのファイルとフォルダは、手動でバックアップしてください。
   - ofcscan.ini: グローバルクライアント設定が含まれます。
   - ous.ini: ウイルス対策コンポーネント配信用のアップデート元情報が含まれます。
   - Private フォルダ: ファイアウォールとアップデート元設定が含まれます。
   - Web¥tmOPP フォルダ: 大規模感染予防設定が含まれます。
   - Pccnt¥Common¥OfcPfw2.dat: ファイアウォール設定が含まれます。
   - Download¥OfcPfw2.dat, OfcPfw3.dat: ファイアウォール配信設定が含まれます。
   - Log フォルダ: システムイベントおよび接続検証ログが含まれます。
   - Virus フォルダ: 隔離されたファイルが含まれます。
   - HTTPDB フォルダ: ウイルスバスター Corp. データベースが含まれます。
4. ウイルスバスター Corp. サーバをアップグレードします。詳細については、44 ページの「ウイルスバスター Corp. サーバおよびクライアントのアップグレード」を参照してください。
5. サーバのアップグレード後に、次の手順を実行してください。
   a. 対象コンピュータ上の <「サーバのインストールフォルダ」>¥PCCSRV フォルダにバックアップファイルをコピーします。これをウイルスバスター Corp. サーバデータベースおよび関連ファイル / フォルダに上書きします。
   b. OfficeScan Master Service を再起動します。

サポートされていない OS

ウイルスバスター Corp. 10 クライアントでは、Windows 95/98/Me/NT、および Itanium アーキテクチャプラットフォームはサポートされなくなりました。ウイルスバスター Corp. 7.x からこのバージョンへアップグレードする予定で、これらの OS で動作するウイルスバスター Corp. 7.x クライアントがある場合には、次の点に注意してください。

1. すべてのウイルスバスター Corp. 7.x サーバを、本バージョンにアップグレードしないでください。
2. サポートされていない OS で動作するクライアントを管理するために、最低 1 つのウイルスバスター Corp. 7.x サーバ (親サーバ) を指定してください。
3. 他のサーバをアップグレードする前に、次の作業を実行してください。
   a. 各サーバで Web コンソールを開いて、メインメニューで [クライアント] をクリックします。
   b. クライアントツリーで、移動するクライアントを選択し、[移動] をクリックします。
   c. [選択したクライアントを別のウイルスバスター Corp. サーバに移動する] で親サーバのコンピュータ名 /IP アドレスとサーバ待機ポートを指定します。
   d. [移動] をクリックします。

ウイルスバスター Corp. サーバがアップグレード済みで、サポートされていないクライアントは移動していない場合には、94 ページの「Client Mover for Legacy Platforms の使用」の手順を参照してください。

アップグレード時に検索方法を指定

このウイルスバスター Corp. のバージョンでは、スマートスキャンと従来型スキャンのいずれかを使用するようにクライアントを設定できます。

ウイルスバスター Corp. サーバを、自動クライアントアップグレードを有効にして以前のバージョンからアップグレードする場合、このサーバが管理するすべてのクライアントは、アップグレード後に自動的に従来型スキャンを使用するようになります。アップグレード後に、すべてのクライアントまたは特定数のクライアントがスマートスキャンを使用するように設定できます。詳細については、ウイルスバスター Corp. 用スマートスキャン クイックスタートガイドで検索方法の設定のガイドラインを参照してください。

スマートスキャンを導入する予定がない場合や、すべてのクライアントをアップデートしてから導入する場合には、44 ページの「ウイルスバスター Corp. サーバおよびクライアントのアップグレード」を参照してください。

インストールとアップグレードのチェックリスト

ウイルスバスター Corp. サーバのインストールまたはアップグレード時には、セットアップから次の情報が求められます。

表 1-7.　インストールのチェックリスト

インストール情報	情報が要求されるインストールの種類			
	ローカル / サイレント新規インストール	リモート新規インストール	ローカル / サイレントアップグレード	リモートアップグレード
インストールパス 初期設定のサーバインストールパスは次のとおりです。 ・ C:¥Program Files¥Trend Micro ¥OfficeScan ・ C:¥Program Files (x86)¥Trend Micro ¥OfficeScan (x64 タイプのプラットフォームの場合) 初期設定のパスを使用しないように選択した場合はインストールパスを選択してください。パスが存在しない場合には、セットアップによって作成されます。	あり	あり	なし	あり
プロキシサーバ設定 ウイルスバスター Corp. サーバがプロキシサーバを介してインターネットに接続している場合、次を指定します。 ・ プロシキタイプ (HTTP または SOCKS 4) ・ サーバ名 /IP アドレス ・ ポート番号 ・ プロキシ認証アカウント情報	あり	あり	なし	あり

表 1-7.　インストールのチェックリスト（続き）

インストール情報	情報が要求されるインストールの種類			
	ローカル / サイレント新規インストール	リモート新規インストール	ローカル / サイレントアップグレード	リモートアップグレード
Web サーバの設定 Web サーバ (Apache または IIS Web サーバ) は、Web コンソール CGI を実行し、クライアントからの命令を可能にします。以下を指定します。 • HTTP ポート番号 : 初期設定のポート番号は 8080 です。IIS 既定 Web サイトを使用している場合は、HTTP サーバの TCP ポートを確認してください。 **警告 :** 多くのハッカーおよびウイルス / 不正プログラムの攻撃は、ポート 80 および 8080 を使用する HTTP を介して行われます。これらのポート番号は多くの企業が HTTP 通信用の TCP ポートとして初期設定で使用しています。現在これらの初期設定ポート番号を使用している場合は、別のポート番号を使用してください。 セキュリティで保護された接続を有効にしている場合 • SSL 証明書の有効期間 • SSL ポート番号　(初期設定 : 4343)	あり	あり	なし	あり

表 1-7.　インストールのチェックリスト（続き）

インストール情報	情報が要求されるインストールの種類			
	ローカル / サイレント新規インストール	リモート新規インストール	ローカル / サイレントアップグレード	リモートアップグレード
登録 アクティベーションコードを取得するためにユーザ登録を行ってください。登録を行うには、次の情報が必要です。 更新ユーザ ・ オンライン登録アカウント (ログオン名とパスワード) アカウントのないユーザ ・ レジストレーションキー	あり	あり	あり	あり
アクティベーション 次の製品サービスのアクティベーションコードを取得します。 ・ ウイルス対策 ・ ダメージクリーンナップサービス ・ Web レピュテーションおよびスパイウェア対策	あり	あり	あり	あり
統合スマートスキャンサーバのインストール 統合サーバのインストールを選択した場合には、次を指定します。 ・ SSL 証明書の有効期間 ・ SSL ポート	あり	あり	あり	あり

表 1-7.　インストールのチェックリスト（続き）

インストール情報	情報が要求されるインストールの種類			
	ローカル / サイレント新規インストール	リモート新規インストール	ローカル / サイレントアップグレード	リモートアップグレード

リモートインストール先
ウイルスバスター Corp. サーバをインストール / アップグレードするコンピュータを指定します。次の情報を準備します。
・ コンピュータ名または IP アドレスのリスト
・ (任意) 対象コンピュータまたは IP アドレスのリストを含んだテキストファイル
テキストファイルの内容の例 :
`us-user_01`
`us-admin_01`
`123.12.12.123`
	なし	あり	なし	あり

リモートインストール先コンピュータの解析 セットアップは、対象コンピュータの解析を実行する前に、次の情報を求めます。 ・ 対象コンピュータに対して「サービスとしてログオン」権限を持つ管理者アカウントのユーザ名とパスワード	なし	あり	なし	あり
その他のウイルスバスター Corp. プログラムのインストール Cisco Trust Agent をインストールする場合には、次の情報を用意します。 ・ Cisco Trust Agent 証明書ファイル	あり	なし	なし	なし

表 1-7.　インストールのチェックリスト（続き）

インストール情報	情報が要求されるインストールの種類			
	ローカル / サイレント新規インストール	リモート新規インストール	ローカル / サイレントアップグレード	リモートアップグレード
管理者アカウントのパスワード セットアップによって、Web コンソールのログオン用ルートアカウントが作成されます。以下を指定します。 ・ ルートアカウントのパスワード 不正なアンインストールやウイルスバスター Corp. クライアントのアンロードを防ぐために、次を指定します。 ・ クライアントのアンインストール / アンロード用パスワード	あり	あり	なし	なし
クライアントインストールパス ウイルスバスター Corp. クライアントをインストールするクライアントコンピュータのディレクトリを指定します。以下を指定します。 ・ インストールパス : 初期設定のクライアントインストールパスは $ProgramFiles¥Trend Micro¥OfficeScan Client です。初期設定のパスを使用しないように選択した場合はインストールパスを選択してください。パスが存在しない場合には、インストール時にセットアップによって作成されます。 ・ クライアント通信ポート番号 : ウイルスバスター Corp. によってポート番号がランダムに生成されます。生成されたポート番号を使用するか、新しい番号を指定してください。	あり	あり	なし	なし

表 1-7.　インストールのチェックリスト（続き）

インストール情報	情報が要求されるインストールの種類			
	ローカル / サイレント新規インストール	リモート新規インストール	ローカル / サイレントアップグレード	リモートアップグレード
プログラムフォルダのショートカット ウイルスバスター Corp. サーバのインストールフォルダへのショートカットは、Windows の [スタート] メニューから表示されます。初期設定のショートカット名は、[ウイルスバスター コーポレートエディションサーバ - < サーバ名 >] です。初期設定のフォルダ名を使用しない場合は、別の名前を指定します。	あり	なし	なし	なし

表 1-7.　インストールのチェックリスト（続き）

インストール情報	情報が要求されるインストールの種類			
	ローカル / サイレント新規インストール	リモート新規インストール	ローカル / サイレントアップグレード	リモートアップグレード
ポリシーサーバのインストール Policy Server for Cisco NAC のインストールを選択する場合は、次の情報を準備します。 ・ インストールパス : 初期設定のインストールパスを使用しない場合は、ポリシーサーバをインストールするローカルコンピュータ上の場所を指定します。 ・ Web サーバ設定 : 選択した Web サーバに次の設定を指定します。 　・ HTTP ポート番号 (初期設定 : 8081) 　・ セキュリティで保護された接続を有効にしている場合 : SSL 証明書の有効期間 ・ SSL ポート番号 (初期設定 : 4344) Web コンソールパスワード : ポリシーサーバコンソールにログオンするためのパスワードを指定します。 ・ ACS サーバ認証 : ACS サーバは、ネットワークアクセスデバイス経由で、クライアントからのウイルスバスター Corp. クライアントウイルス対策データを受信し、評価用に外部ユーザデータベースに渡します。ログオンアカウント情報 (ユーザ名とパスワード) を指定してください。	あり	なし	なし	なし

テストインストールの計画

実環境にインストールする前に、限定された環境下で試験的にインストールを実行 (テストインストール) することをお勧めします。テストインストールによって、各機能の動作を確認し、実環境にインストールした後に必要となるサポートレベルを決定するための情報を得ることができます。インストール担当チームは、インストールの手順の予行演習と改善の機会を得ることができます。また、インストール計画が企業のセキュリティの方針に見合っているかを確認することもできます。

ウイルスバスター Corp. インストールのサンプルについては、113 ページの「サンプル配信」を参照してください。

テスト環境の選択

実環境に類似した環境を選択するようにしてください。実環境に類似した役割を果たすネットワークトポロジの種類をシミュレーションしてみてください。

ロールバック計画の作成

インストールやアップグレードで問題が発生した場合に備えて、復旧またはロールバック計画を作成してください。

テストインストールの評価

テストインストールで成功した点や失敗した点をリスト化します。陥りやすい過ちを明らかにして、しかるべき計画を作成します。実環境でのインストール計画に、このインストール評価計画を組み込んでください。

互換性についての既知の問題

ここでは、他社製アプリケーションがインストールされたコンピュータ上にウイルスバスター Corp. サーバをインストールする際に発生する可能性のある、互換性の問題について説明します。詳細については、他社製アプリケーションのドキュメントを参照してください。

Microsoft Small Business Server

Microsoft Small Business Server および Microsoft Internet Security Acceleration server (ISA) が動作するコンピュータにウイルスバスター Corp. サーバをインストールする場合は、ISA によって使用されているポート番号をメモに記録してください。初期設定では、ウイルスバスター Corp. サーバも ISA も同じポート 8080 を使用します。

ウイルスバスター Corp. サーバをインストールする場合は、別のサーバ待機ポートを選択してください。

Microsoft IIS ロックダウンツールおよび URLScan

Microsoft IIS ロックダウンツールまたは URLScan を使用する場合は、次のウイルスバスター Corp. に関連するファイルのロックダウンが、ウイルスバスター Corp. クライアントとサーバ間の通信をブロックする可能性があります。

- 設定 (.ini) ファイル
- データ (.dat) ファイル
- ダイナミックリンクライブラリ (.dll) ファイル
- 実行可能ファイル (.exe) ファイル

URLScan によるクライアントサーバ間の通信障害を防ぐには

1. ウイルスバスター Corp. サーバがインストールされているコンピュータの World Wide Web Publishing サービスを停止します。
2. URLScan の設定ファイルを変更し、上記で指定したファイルの種類を許可します。
3. World Wide Web Publishing サービスを再起動します。

Microsoft Exchange Server

ウイルスバスター Corp. は、クライアントが検索するすべてのファイルにアクセスする必要があります。Microsoft Exchange Server がローカルディレクトリのメッセージをキューに入れるため、Exchange Server がメッセージを処理できるように、これらのディレクトリを検索から除外する必要があります。

ウイルスバスター Corp. は、Microsoft Exchange 2000/2003 のすべてのディレクトリを自動的に検索から除外します。この設定は Web コンソールから設定できます ([ネットワーク上のコンピュータ] → [グローバルクライアント設定] → [ウイルス / 不正プログラム検索設定])。Microsoft Exchange 2007 に関する検索除外の詳細については、次の Web サイト (英語) を参照してください。
http://technet.microsoft.com/en-us/library/bb332342.aspx

SQL Server

Microsoft SQL Server のデータベース検索が可能です。ただしこの検索によって、データベースにアクセスするアプリケーションのパフォーマンスを低下させる場合があります。SQL Sever データベースとそのバックアップフォルダは、リアルタイム検索の対象から除外することを検討してください。データベースの検索が必要な場合、業務時間外などの影響が少ない時間帯に手動で実行することをお勧めします。

インターネット接続ファイアウォール (ICF)

Microsoft Windows Server 2003 では、インターネット接続ファイアウォール (ICF) と呼ばれる組み込みファイアウォールが搭載されています。ICF の使用をご希望の場合は、ウイルスバスター Corp. 待機ポートを ICF 例外リストに追加してください。例外リストの設定方法の詳細については、お使いのファイアウォールのドキュメントを参照してください。

第 2 章

トレンドマイクロ ウイルスバスター コーポレートエディションのインストールとアップグレード

この章で説明する内容には、次の項目が含まれます。

ウイルスバスター Corp. サーバの新規インストールの実行

新規インストールを実行するには、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.) サーバの新規インストール要件を満たすコンピュータでセットアップを実行します。インストール画面と設定オプションについては、55 ページの「セットアップのインストール画面」を参照してください。

サーバのインストール後、ウイルスバスター Corp. サーバを Web コンソールから設定し、次にウイルスバスター Corp. クライアントをコンピュータにインストールします。

クライアントの新規インストール方法と手順については、管理者ガイドまたはウイルスバスター Corp. サーバのヘルプを参照してください。

ウイルスバスター Corp. サーバおよびクライアントのアップグレード

ネットワーク帯域幅やウイルスバスター Corp. サーバが管理するクライアント数に応じて、クライアントアップグレードをグループ単位でタイミングをずらすか、サーバのアップグレード直後にすべてのクライアントをアップグレードします。

クライアントのアップグレードとスマートスキャンの導入を同時に実施するように計画している場合は、ウイルスバスター Corp. 用スマートスキャン クイックスタートガイドを参照してください。

すべてのクライアントが、アップグレード後に従来型スキャンを使用する場合は、次のアップグレード方法を使用します。

- 45 ページの「アップグレード方法 1: 自動クライアントアップグレードの無効化」
- 48 ページの「アップグレード方法 2: ウイルスバスター Corp. 10 サーバへのクライアントの移動」
- 50 ページの「アップグレード方法 3: 自動クライアントアップグレードの有効化」

アップグレード方法 1: 自動クライアントアップグレードの無効化

自動クライアントアップグレードを無効にすることで、サーバを先にアップグレードしてから、クライアントをグループ単位でアップグレードできます。多数のクライアントをアップグレードする場合はこのアップグレード方法を使用します。

パート 1: ウイルスバスター Corp. 8.x または 7.x サーバのアップデート設定と権限の指定

ウイルスバスター Corp. 8.x の場合 :

1. [アップデート] → [ネットワーク上のコンピュータ] → [自動アップデート] の順に選択します。
2. 次のオプションを無効にします。
   - ウイルスバスター Corp. サーバが新しいコンポーネントをダウンロード後、ただちにクライアントのコンポーネントのアップデートを開始する
   - 再起動時、またはウイルスバスター Corp. サーバへの接続時にコンポーネントアップデートの開始を許可する (スタンドアロンモードのクライアントを除く)
3. [ネットワーク上のコンピュータ] → [クライアント管理] の順に選択します。
4. クライアントツリーから、ルートアイコン を選択してすべてのクライアントを選択します。
5. [設定] → [権限とその他の設定] の順にクリックして、[その他の設定] タブに進みます。
6. [クライアントはコンポーネントのアップデートが可能ですが、クライアントプログラムのアップグレードと HotFix の配信を禁止] をオンにします。
7. [すべてのクライアントに適用] をクリックします。

ウイルスバスター Corp. 7.x の場合 :

1. [アップデート] → [クライアントアップデート] → [自動アップデート] へ進みます。
2. 次のオプションを無効にします。
   - ウイルスバスター Corp. サーバでダウンロード完了後、クライアントに新しいコンポーネントをただちに配信する
   - クライアントの再起動時に配信する (ウイルスバスター Corp. クライアントのみ、スタンドアロンモードのクライアントを除く)
3. メインメニューで [クライアント] をクリックします。
4. クライアントツリーから、ルートアイコン を選択してすべてのクライアントを選択します。
5. [クライアント権限] をクリックします。
6. [アップデート設定] で [プログラムのアップグレードと HotFix の配信を禁止] をオンにします。
7. [すべてに適用] をクリックします。

ヒント： ネットワーク環境が複雑な場合や、クライアント数が多い場合は、設定をオンラインクライアントに配信するのに時間がかかる場合があります。アップグレード前に、設定をすべてのクライアントに配信するのに十分な時間を割り当ててください。設定を適用していないクライアントは自動的にアップグレードされます。

パート 2: ウイルスバスター Corp. サーバのアップグレード

ウイルスバスター Corp. サーバのアップグレードの詳細については、55 ページの「セットアップのインストール画面」を参照してください。

ウイルスバスター Corp. サーバの設定は、インストール完了直後にクライアントをアップグレードする前に、Web コンソールを使用して設定できます。ウイルスバスター Corp. の詳細な設定手順については、管理者ガイドとウイルスバスター Corp. サーバのオンラインヘルプを参照してください。

パート 3: ウイルスバスター Corp. クライアントのアップグレード

1. [ネットワーク上のコンピュータ] → [クライアント管理] へ進みます。
2. クライアントツリーからアップグレードするクライアントを選択します。ドメインを選択するか、ドメインの特定のクライアントを選択することで、アップグレードするタイミングをずらします。

   ヒント： アップデートエージェントを先にアップグレードします。アップデートエージェントを利用することで、他のクライアントのアップデート元として機能するため、ウイルスバスター Corp. サーバへのトラフィックを削減できます。

3. [設定] → [権限とその他の設定] の順にクリックして、[その他の設定] タブに進みます。
4. [クライアントはコンポーネントのアップデートが可能ですが、クライアントプログラムのアップグレードと HotFix の配信を禁止] をオフにします。
5. [アップデート] → [ネットワーク上のコンピュータ] → [自動アップデート] の順に選択します。
6. 次のオプションを有効にします。
   - ウイルスバスター Corp. サーバが新しいコンポーネントをダウンロード後、ただちにクライアントのコンポーネントのアップデートを開始する
   - 再起動時、またはウイルスバスター Corp. サーバへの接続時にコンポーネントアップデートの開始を許可する (スタンドアロンモードのクライアントを除く)

アップグレード結果 (オンラインクライアント)

自動アップグレード

次のいずれかのイベントが発生すると、オンラインクライアントのアップグレードが開始されます。

- ウイルスバスター Corp. サーバが新しいコンポーネントをダウンロードし、クライアントにアップデートするように通知
- クライアントプログラムの再ロード
- クライアントコンピュータが再起動し、ウイルスバスター Corp. サーバへ接続
- Windows 2000、2003、および XP Professional を実行するクライアントコンピュータが、ログオンスクリプトセットアップ (AutoPcc.exe) を使用するようにログオンスクリプトを変更したサーバへログオン
- クライアントでの予約アップデートの実行 (予約アップデートの権限があるクライアントのみ)

手動アップグレード

上記のいずれのイベントも発生しない場合、次の任意のタスクを実行してクライアントをただちにアップグレードします。

- Client Packager によって作成した EXE または MSI クライアントパッケージを作成および配信します。

  注意 : クライアントパッケージの作成手順については、管理者ガイドを参照してください。

- クライアントコンピュータ上で [アップデート] を実行するようにクライアントユーザに指示します。
- クライアントコンピュータで Windows 2000、2003、XP Professional、2008 または Vista (Vista Home 以外のすべてのエディション) が実行されている場合は、ユーザに次の手順を実行するように指示してください。
  - サーバコンピュータに接続します。
  - ¥¥< サーバコンピュータ名 >¥ofcscan に移動します。
  - AutoPcc.exe を起動します。
- クライアントコンピュータで Windows XP Home または Vista Home が実行されている場合、AutoPcc.exe を右クリックして、[管理者として実行] を選択するようにユーザに指示してください。
- 手動クライアントアップデートを開始します。

手動クライアントアップデートを開始するには

1. [アップデート] → [ネットワーク上のコンピュータ] → [手動アップデート] の順に選択します。
2. [クライアントを手動で選択する] を選択し [選択] をクリックします。
3. 表示されたクライアントツリーで、アップグレードするクライアントを選択します。
4. クライアントツリーの上部にある [コンポーネントアップデートの開始] をクリックします。

アップグレード結果 (オフラインクライアント)

オフラインクライアントは、オンラインになったときにアップグレードされます。

アップグレード結果 (スタンドアロンモードクライアント)

スタンドアロンモードクライアントは、オンラインになったときにアップグレードされるか、クライアントにアップデート権限がある場合には、予約アップデートの実行時にアップグレードされます。

アップグレード方法 2: ウイルスバスター Corp. 10 サーバへのクライアントの移動

ウイルスバスター Corp. 10 サーバの新規インストールを実行し、次にクライアントをこのサーバに移動します。クライアントの移動時、自動的にウイルスバスター Corp. 10 にアップグレードされます。

パート 1: ウイルスバスター Corp. 10 サーバの新規インストールの実行と、それに続くサーバの設定

1. 特定のコンピュータでウイルスバスター Corp. 10 サーバの新規インストールを実行します。詳細については、55 ページの「セットアップのインストール画面」を参照してください。
2. ウイルスバスター Corp. 10 の Web コンソールを開き、[アップデート] → [ネットワーク上のコンピュータ] → [自動アップデート] の順に選択します。
3. 次のオプションを有効にします。
   - ウイルスバスター Corp. サーバが新しいコンポーネントをダウンロード後、ただちにクライアントのコンポーネントのアップデートを開始する
   - 再起動時、またはウイルスバスター Corp. サーバへの接続時にコンポーネントアップデートの開始を許可する (スタンドアロンモードのクライアントを除く)

4. [ネットワーク上のコンピュータ] → [クライアント管理] へ進みます。
5. クライアントツリーから、ルートアイコンを選択します。
6. [設定] → [権限とその他の設定] の順にクリックして、[その他の設定] タブに進みます。
7. [クライアントはコンポーネントのアップデートが可能ですが、クライアントプログラムのアップグレードと HotFix の配信を禁止] をオフにします。
8. [すべてのクライアントに適用] をクリックします。
9. 次のウイルスバスター Corp. 10 サーバの情報を記録します。クライアントの移動時に、ウイルスバスター Corp.「8.x」/「7.x」サーバでこれらの情報を指定します。
   - コンピュータ名または IP アドレス
   - サーバ待機ポート

     サーバ待機ポートを表示するには、[管理] → [接続設定] に進みます。ポート番号が画面に表示されます。

パート 2: ウイルスバスター Corp. クライアントのアップグレード

ウイルスバスター Corp. 8.x の場合 :

1. Web コンソールを開き、[アップデート] → [概要] に進みます。
2. [通知のキャンセル] をクリックします。この機能によりサーバの通知キューがクリアされ、ウイルスバスター Corp. 10 サーバへクライアントを移動する際の問題を防ぐことができます。

警告 : 以降の手順もすぐに実行してください。クライアントを移動する前にサーバ通知キューが更新された場合、クライアントを正常に移動できない場合があります。

3. [ネットワーク上のコンピュータ] → [クライアント管理] へ進みます。
4. クライアントツリーから、アップグレードするクライアントを選択します。ドメインを選択するか、ドメインの特定のクライアントを選択することで、アップグレードするタイミングをずらします。

ヒント : アップデートエージェントを先にアップグレードします。アップデートエージェントを利用することで、他のクライアントのアップデート元として機能するため、ウイルスバスター Corp. サーバへのトラフィックを削減できます。

5. [クライアントツリー管理] → [クライアントの移動] をクリックします。
6. ウイルスバスター Corp. 10 サーバのコンピュータ名 /IP アドレスとサーバ待機ポートを [選択したクライアントを別のウイルスバスター Corp. サーバに移動する] で指定します。
7. [移動] をクリックします。

ウイルスバスター Corp. 7.x の場合 :

1. Web コンソールで [クライアント] をクリックします。
2. クライアントツリーから、アップグレードするクライアントを選択します。ドメインを選択するか、ドメインの特定のクライアントを選択することで、アップグレードするタイミングをずらします。

   ヒント : アップデートエージェントを先にアップグレードします。アップデートエージェントを利用することで、他のクライアントのアップデート元として機能するため、ウイルスバスター Corp. サーバへのトラフィックを削減できます。

3. [移動] をクリックします。
4. ウイルスバスター Corp. 10 サーバのコンピュータ名 /IP アドレスとサーバ待機ポートを [選択したクライアントを別のウイルスバスター Corp. サーバに移動する] で指定します。
5. [移動] をクリックします。

アップグレード結果

- オンラインクライアントの移動とアップグレードが開始されます。
- オフラインクライアントは、オンラインになったときに移動およびアップグレードされます。ウイルスバスター Corp. 8.x/7.x サーバは、これらのクライアントの管理を継続します。
- スタンドアロンモードクライアントは、オンラインになったときに移動およびアップグレードされるか、クライアントにアップデート権限がある場合には、予約アップデートの実行時に移動およびアップグレードされます。

注意 : ウイルスバスター Corp. 7.x または 8.x サーバは、すべてのクライアントをアップグレードした後にアンインストールできます。

アップグレード方法 3: 自動クライアントアップグレードの有効化

ウイルスバスター Corp. サーバをこのバージョンにアップグレードすると、サーバがアップグレードを管理するすべてのクライアントにサーバからただちに通知が送信されます。

サーバが管理するクライアントが少数の場合、クライアントを即座にアップグレードできるようにすることを検討してください。また、前述のアップグレード方法を使用することもできます。

パート 1: ウイルスバスター Corp. 8.x または 7.x サーバでの設定

ウイルスバスター Corp. 8.x の場合 :

1. [アップデート] → [ネットワーク上のコンピュータ] → [自動アップデート] の順に選択します。
2. 次のオプションを有効にします。
   - ウイルスバスター Corp. サーバが新しいコンポーネントをダウンロード後、ただちにクライアントのコンポーネントのアップデートを開始する
   - 再起動時、またはウイルスバスター Corp. サーバへの接続時にコンポーネントアップデートの開始を許可する (スタンドアロンモードのクライアントを除く)
3. [ネットワーク上のコンピュータ] → [クライアント管理] へ進みます。
4. クライアントツリーから、ルートアイコンを選択します。
5. [設定] → [権限とその他の設定] の順にクリックして、[その他の設定] タブに進みます。
6. [クライアントはコンポーネントのアップデートが可能ですが、クライアントプログラムのアップグレードと HotFix の配信を禁止] をオフにします。
7. [すべてのクライアントに適用] をクリックします。

ウイルスバスター Corp. 7.x の場合 :

1. [アップデート] → [クライアントアップデート] → [自動アップデート] へ進みます。
2. 次のオプションを有効にします。
   - ウイルスバスター Corp. サーバでダウンロード完了後、クライアントに新しいコンポーネントをただちに配信する
   - クライアントの再起動時に配信する (ウイルスバスター Corp. クライアントのみ、スタンドアロンモードのクライアントを除く)
3. メインメニューで [クライアント] をクリックします。
4. クライアントツリーから、ルートアイコンを選択してすべてのクライアントを選択します。
5. [クライアント権限] をクリックします。
6. [アップデート設定] で [プログラムのアップグレードと HotFix の配信を禁止] をオフにします。
7. [すべてに適用] をクリックします。

ヒント : ウイルスバスター Corp. サーバをアップグレードする前に、設定をすべてのクライアントに配信するための十分な時間を割り当ててください。

パート 2: ウイルスバスター Corp. サーバのアップグレード

ウイルスバスター Corp. サーバのアップグレードの詳細については、55 ページの「セットアップのインストール画面」を参照してください。

アップグレード結果

- オンラインクライアントは、サーバのアップグレードが完了するとただちにアップグレードされます。
- オフラインクライアントは、オンラインになったときにアップグレードされます。
- スタンドアロンモードクライアントは、オンラインになったときにアップグレードされるか、クライアントにアップデート権限がある場合には、予約アップデートの実行時にアップグレードされます。

サイレントインストール / アップグレードの実行

複数のウイルスバスター Corp. サーバが同一のインストール設定を使用する場合は、それらをサイレントモードでインストールまたはアップグレードします。サイレントインストールには 2 つの手順があります。

1. セットアップを起動し、インストール設定を .iss ファイルに記録して応答ファイルを作成します。サイレントインストールを実行するすべてのサーバで、応答ファイルの設定内容が使用されます。

   重要 :

   - セットアップは、ローカルインストール画面のみを表示します (新規インストールまたはアップグレード)。表示される関連スクリーンについては、55 ページの「セットアップのインストール画面」を参照してください。
   - ウイルスバスター Corp. サーバをこのバージョンにアップグレードする場合は、ウイルスバスター Corp. サーバがインストールされているコンピュータ上で応答ファイルを作成してください。
   - 新規インストールの場合は、ウイルスバスター Corp. サーバがインストールされていないコンピュータ上で応答ファイルを作成してください。
2. コマンドプロンプトからセットアップを実行し、サイレントインストールに使用する応答ファイルの場所を指定します。

セットアップの設定を応答ファイルに記録するには

注意： この手順では、ウイルスバスター Corp. がインストールされるわけではありません。セットアップ設定を応答ファイルに記録するだけです。

1. コマンドプロンプトを開き、setup.exe ファイルのあるディレクトリに移動します。たとえば、「CD C:¥OfficeScan Installer¥setup.exe」と入力します。
2. 次のように入力します。

   ```
   setup.exe -r
   ```

   -r パラメータを指定することで、セットアップが起動し、インストールの詳細が応答ファイルに記録されます。
3. セットアップウィザードでは、インストール操作を進めてください。
4. これらが完了したら、%windir% に作成される応答ファイル (setup.iss) を確認してください。

サイレントインストールを実行するには

1. インストールパッケージと setup.iss を、対象コンピュータにコピーします。
2. 対象コンピュータでコマンドプロンプトを開き、インストールパッケージのあるディレクトリに移動します。
3. 次のように入力します。

   ```
   setup.exe -s <-f1 パス >setup.iss <-f2 パス >setup.log
   ```

   例 : C:¥setup.exe -s -f1C:¥setup.iss -f2C:¥setup.log
   説明 :

   - **-s**: セットアップを起動してサイレントインストールを実行します。
   - **<-f1 パス >setup.iss**: 応答ファイルのパスにスペースが含まれている場合は、パスを引用符 (") で囲ってください。たとえば次のようにします。
     -f1"C:¥osce script¥setup.iss"
   - **<-f2 パス >setup.log**: インストール後に作成されるログファイルのパスにスペースが含まれている場合は、パスを引用符 (") で囲ってください。たとえば次のようにします。
     -f2"C:¥osce log¥setup.log"
4. <Enter> キーを押します。セットアップによって、サーバはコンピュータにサイレントインストールされます。
5. インストールが正常に行われたか確認するには、対象コンピュータ上のウイルスバスター Corp. プログラムのショートカットを確認してください。ショートカットが作成されていない場合は、再度インストールを試みてください。

体験版からのアップグレード

体験版の有効期限が近くなると、ウイルスバスター Corp. では、[概要] 画面に通知メッセージが表示されます。ウイルスバスター Corp. の体験版から製品版へのアップグレードは、Web コンソールを使用して、設定情報をすべて保持したまま実行できます。製品版ライセンスを購入すると、レジストレーションキーまたはアクティベーションコードが発行されます。

体験版からアップグレードするには

1. ウイルスバスター Corp. の Web コンソールを開きます。
2. [管理] → [製品ライセンス] をクリックします。 [製品ライセンス] 画面が表示されます。
3. アクティベーションコードをお持ちの場合は、[新しいコード] にアクティベー ションコードを入力し、[保存] をクリックします。
4. アクティベーションコードをお持ちでない場合は、[オンライン登録] をクリックし、レジストレーションキーを使用して、アクティベーションコードを入手します。

セットアップのインストール画面

以下は、ウイルスバスター Corp. サーバをローカル、リモート、またはサイレントでインストール、アップグレードするための、インストール画面 (順番に並んでいます) のリストです。.

表 2-1. インストール画面とタスク

画面	ローカル / サイレント新規インストール	リモート新規インストール	ローカル / サイレントアップグレード	リモートアップグレード
ようこそ	✓	✓	✓	✓
「使用許諾契約書」	✓	✓	✓	✓
「インストール先」	✓	✓	✓	✓
「事前検索」	✓	✓	✓	✓
インストールステータス (コンピュータ解析) **注意：** 解析が完了するまでには、HTTP サーバの初期化などに時間がかかる場合があります。	✓		✓	
「インストールパス」	✓	✓		✓
「プロキシ設定」	✓	✓		✓
「Web サーバ設定」	✓	✓		✓
「サーバコンピュータの識別」	✓	✓		✓

表 2-1.　インストール画面とタスク（続き）

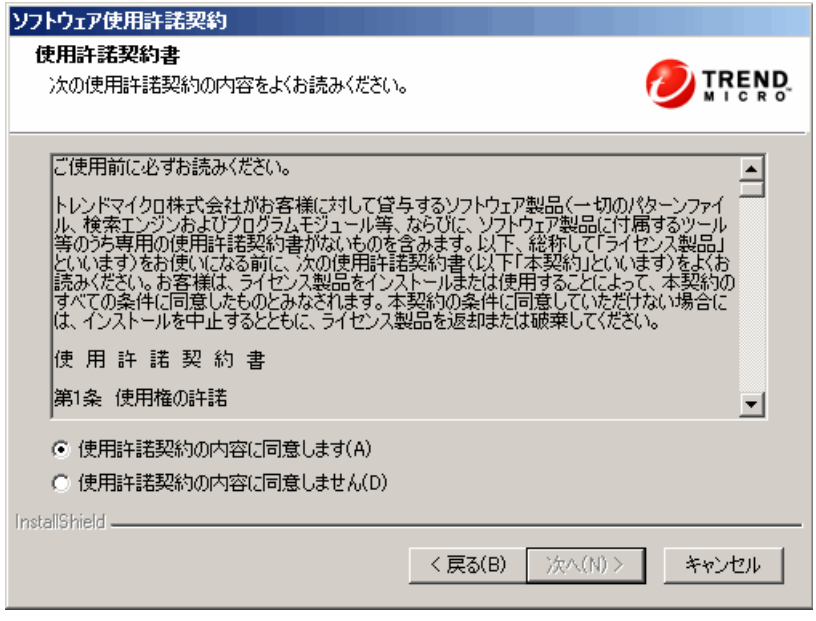
画面	ローカル / サイレント新規インストール	リモート新規インストール	ローカル / サイレントアップグレード	リモートアップグレード
「登録とアクティベーション」	✓	✓	✓	✓
「統合スマートスキャンサーバのインストール」	✓	✓	✓	✓
「リモートインストール先」		✓		✓
「対象コンピュータ分析」		✓		✓
「ウイルスバスター Corp. プログラム」	✓	✓		✓
「Cisco Trust Agent のインストール / アップグレード」	✓			
「Cisco Trust Agent のライセンス」	✓			
「トレンドマイクロ ウイルストラッキングセンターへのウイルス情報送信」	✓	✓		
「管理者アカウントのパスワード」	✓	✓		
「クライアントのインストールパス」	✓	✓		
「ウイルス対策機能」	✓	✓		

表 2-1.　インストール画面とタスク（続き）

画面	ローカル / サイレント新規インストール	リモート新規インストール	ローカル / サイレントアップグレード	リモートアップグレード
「スパイウェア対策機能」 ローカルアップグレードを実行しているときには、Web レピュテーションおよびスパイウェア対策ライセンスが以前にアクティベートされている場合、この画面は表示されません。	✔	✔	✔	✔
「プログラムフォルダのショートカット」	✔			
「インストール情報」	✔	✔	✔	✔
ウイルスバスター Corp. サーバインストール	✔	✔	✔	✔
「ポリシーサーバのインストール」	✔			
「トレンドマイクロウイルスバスター コーポレートエディション サーバのインストールの完了」	✔	✔	✔	✔

使用許諾契約書

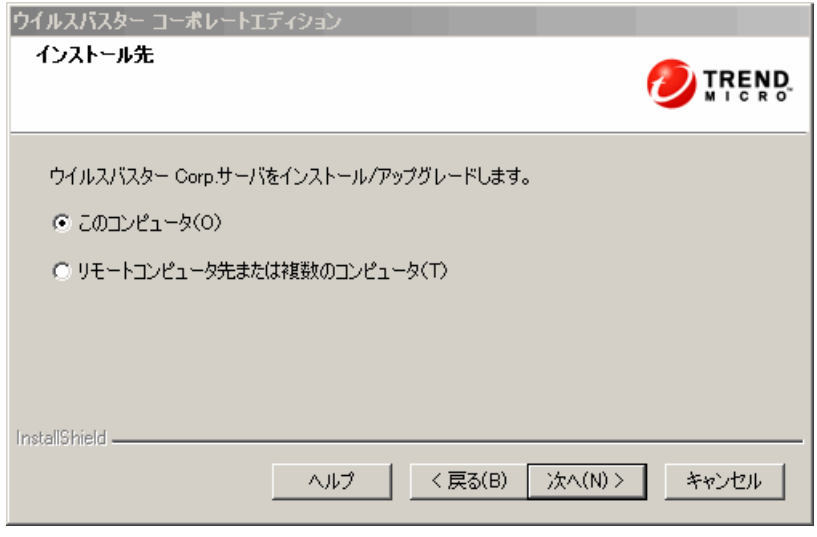
図 2-1.　[使用許諾契約書] 画面



インストールを続行するには使用許諾契約をお読みいただき、使用許諾契約の条項に同意いただく必要があります。使用許諾契約の条項に同意いただけない場合には、インストールを続行することはできません。

インストール先

図 2-2.　[インストール先] 画面



セットアップを実行し、ウイルスバスター Corp. サーバを、セットアップを起動したコンピュータか、ネットワークの他のコンピュータにインストールします。対象コンピュータに旧バージョンのウイルスバスター Corp. が検出された場合には、アップグレードするように求められます。このバージョンにアップグレードできるのは、ウイルスバスター Corp. の以下のバージョンのみです。

- 8.0
- 8.0 Service Pack 1
- 7.3
- 7.0

リモートインストール / アップグレードの注意

リモートからインストール / アップグレードを行う場合は、セットアップによって対象コンピュータがサーバインストール / アップグレードの要件を満たしているか確認されます。続行する前に、次の確認を行ってください。

- インストール先コンピュータに管理者権限があることを確認します。
- コンピュータのホスト名やログオン情報のメモをとります（ユーザ名やパスワード）。

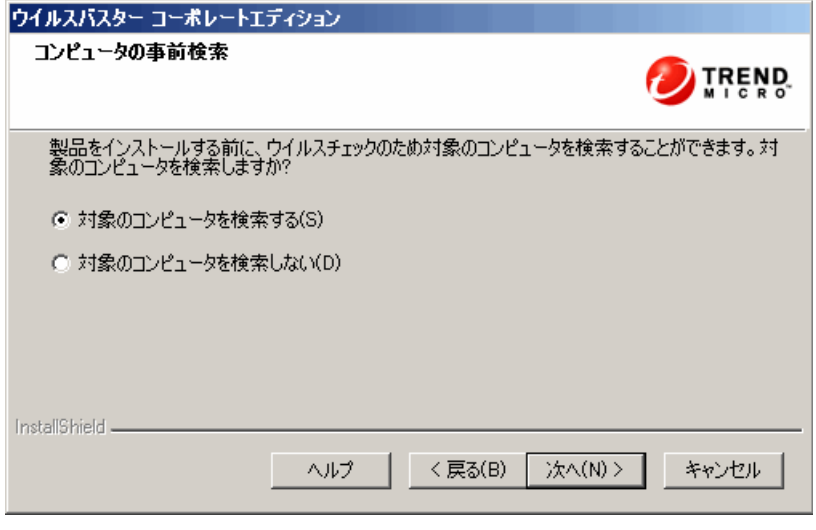
- 対象コンピュータがウイルスバスター Corp. サーバのインストール要件を満たしていることを確認します。
- このサーバが Web サーバの場合は、コンピュータに Microsoft IIS サーバ 5.0、6.0、または 7.0 がインストールされていることを確認します。Apache Web サーバを選択した場合、対象コンピュータにこのサーバが存在しない場合にはセットアップによって自動的にインストールされます。

ローカルアップグレードの場合、前のインストールからサーバ名、プロシキサーバ情報、およびポート番号などの元の設定が維持されます。アップグレード時にこれらの設定を変更することはできません。アップグレード後に、ウイルスバスター Corp. Web コンソールからこれらの設定を変更してください。

リモートアップグレードの場合は、すべての設定を再入力する必要があります。ただしこれらの設定は、サーバのアップグレード後は無視され、前のバージョンの設定が使用されます。

事前検索

図 2-3.　[コンピュータの事前検索] 画面



ウイルスバスター Corp. サーバのインストールを開始する前に、セットアップによって対象コンピュータのウイルスおよび不正プログラムを検索することができます。セットアップは、コンピュータの最も脆弱な次の場所を検索します。

- システム領域とシステムディレクトリ (システム領域感染型ウイルスが対象)
- Windows フォルダ
- Program Files フォルダ

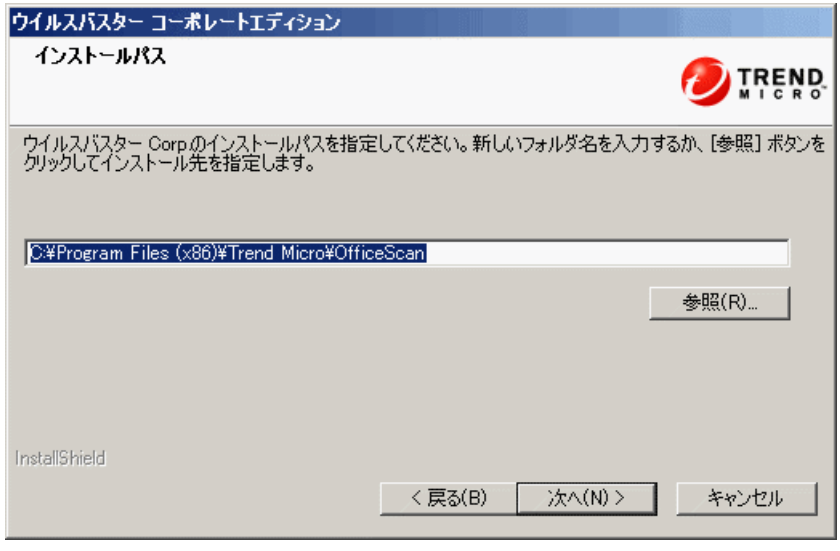
セットアップは、検出されたウイルス / 不正プログラムやトロイの木馬プログラムに対して次のような処理を実行できます。

- **削除**: 感染したファイルを削除します。
- **駆除**: 駆除できるファイルはフルアクセスを許可する前に駆除し、駆除できないファイルは次のような特別処理をします。
- **拡張子変更**： 感染ファイルの拡張子を「vir」に変更します。ユーザはそのファイルを開くことはできませんが、一定のアプリケーションと関連づければ開くことは可能です。ただし拡張子を変更した感染ファイルを開くと、ウイルス / 不正プログラムが作動する可能性があります。
- **放置**: 感染ファイルに対して何もしないでフルアクセスを許可します。ユーザはそのファイルに対してコピー、削除、または開く操作を行うことができます。

ローカルインストールを実行している場合は、[次へ] をクリックすると検索が実行されます。リモートインストールを実行している場合は、実際のインストールの直前に検索が実行されます。

インストールパス

図 2-4.　[インストールパス] 画面

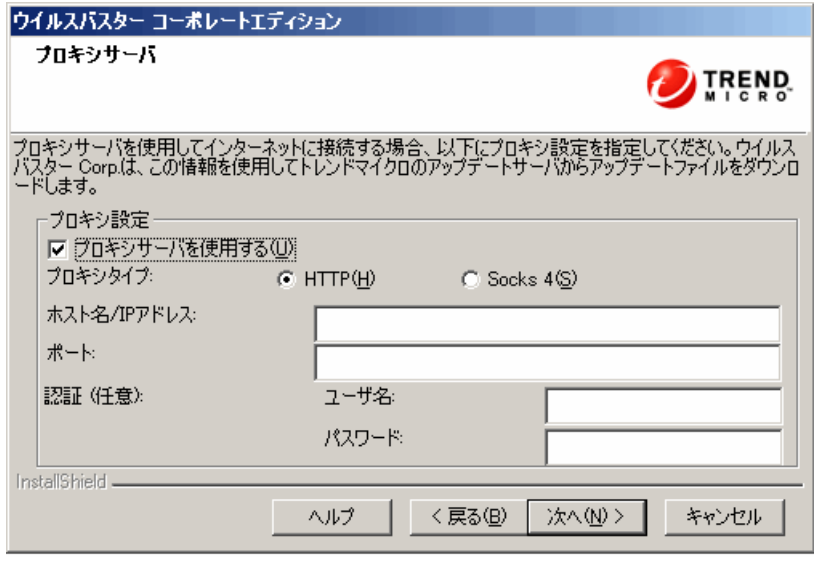


初期設定のインストールパスを使用するか、新しいパスを指定します。

指定したインストールパスは、リモート新規インストールを実行する場合にのみ適用されます。リモートアップグレードの場合は、ウイルスバスター Corp. は以前のバー ジョンの設定を使用します。

プロキシ設定

図 2-5.　[プロキシサーバ] 画面



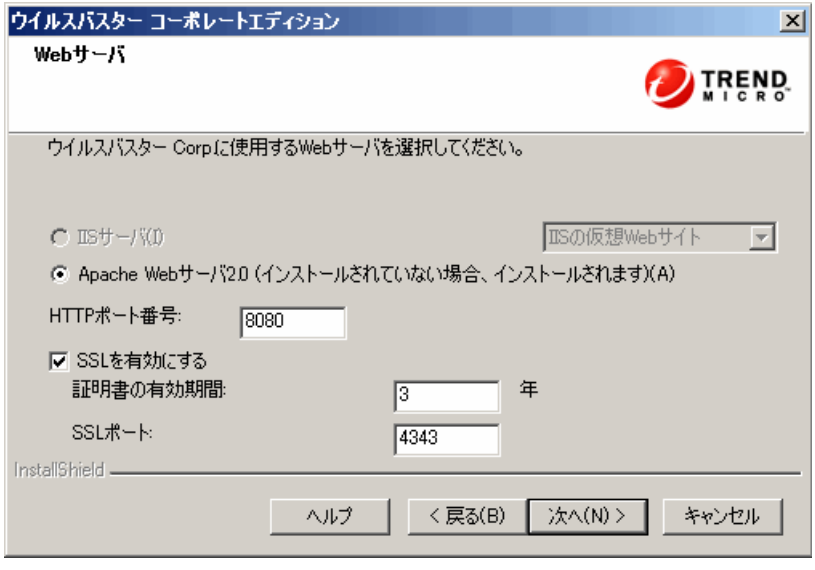
ウイルスバスター Corp. サーバでは、クライアント - サーバ間の通信や、トレンドマイクロのアップデートサーバへの接続およびアップデートのダウンロードに HTTP プロトコルが使用されます。プロキシサーバによってネットワークのインターネットトラフィックが処理されている場合、ウイルスバスター Corp. サーバがアップデートをトレンドマイクロのアップデートサーバからダウンロードできるように、プロキシの設定が必要です。

インストール時にプロシキ設定の指定をスキップして、インストール後にウイルスバスター Corp. Web コンソールから指定することができます。

プロシキ設定は、リモート新規インストールを実行している場合にのみ適用されます。リモートアップグレードの場合は、ウイルスバスター Corp. は以前のバージョンの設定を使用します。

Web サーバ設定

図 2-6.　[Web サーバ] 画面



ウイルスバスター Corp. サーバでは Web コンソールがホストされ、管理者はコンソールの Common Gateway Interface (CGI) を実行し、クライアントからの命令を受け入れることができます。Web サーバは、この命令をクライアントの CGI に変換し、OfficeScan Master Service に転送します。

Web サーバ設定は、リモート新規インストールを実行している場合にのみ適用されます。リモートアップグレードを実行している場合は、ウイルスバスター Corp. は以前のバージョンの設定を使用します。

Web サーバ

IIS と Apache Web サーバの両方が対象コンピュータにインストールされていることがセットアップによって検出された場合、2 つの Web サーバのいずれかを選択できます。対象コンピュータに両方とも存在しない場合は、IIS を選択することはできず、ウイルスバスター Corp. によって Apache Web サーバ 2.0.63 が自動的にインストールされます。

Apache Web サーバを使用している場合

- Apache Web サーバ 2.0.x が必須で、Windows 2000、XP、2003、および 2008 でのみ使用できます。Apache Web サーバがコンピュータに存在しても、バージョンが 2.0.x ではない場合、ウイルスバスター Corp. はバージョン 2.0.63 をインストールして使用します。既存の Apache Web サーバは削除されません。
- SSL が有効で Apache Web サーバ 2.0.x が存在する場合、Apache Web サーバで SSL 設定を事前設定する必要があります。
- 初期設定では、管理者アカウントが Apache Web サーバ上に作成される唯一のアカウントです。

ヒント： Web サーバ実行用に別のアカウントを作成することをお勧めします。これを行わない場合、悪意のある第三者から Apache Web サーバへの攻撃が発生した場合にウイルスバスター Corp. サーバが脆弱化する可能性があります。

- Apache Web サーバをインストールする前に、Apache の Web サイトでアップグレード、パッチおよびセキュリティ問題の最新情報を参照してください。

IIS Web サーバを使用している場合

- Windows 2000 の場合は Microsoft Internet Information Server (IIS) のバージョン 5.0、Windows Server 2003 の場合はバージョン 6.0、および Windows Server 2008 の場合はバージョン 7.0 が必要です。
- Microsoft IIS ロックダウンツールが動作するコンピュータへ Web サーバをインストールしないでください。正常なインストールを妨げることがあります。詳細については、IIS のドキュメントを参照してください。

HTTP ポート

Web サーバは、クライアントの要求を HTTP ポートで待機し、この要求を OfficeScan Master Service に転送します。このサービスは、指定されたクライアント通信ポートのクライアントに情報を返します。セットアップは、インストール時にクライアントの通信ポート番号をランダムに生成します。

ウイルスバスター Corp. は、HTTP サーバが TCP トラフィックに使用するポート番号と同じものを使用します。多くの組織では、これがポート 80 または 8080 に設定されています。ウイルスバスター Corp. の初期設定のポートは 8080 です。

SSL を有効にしている場合、ウイルスバスター Corp. は HTTP ポートではなく SSL ポート (初期設定のポートは 4343) を使用します。

SSL サポート

Web コンソールとサーバ間およびサーバとトレンドマイクロのアップデートサーバ間の通信をセキュリティで保護する場合には、SSL (Secure Socket Layer) を有効にしてください。SSL は、ハッカーに対抗して、保護の拡張階層を提供します。ウイルスバスター Corp. では、Web コンソールで指定されたパスワードがウイルスバスター Corp. サーバへ送信される前に暗号化されますが、ハッカーはパケットを盗聴し、復号化することなく「再現」してコンソールへのアクセスに成功する場合があります。SSL トンネリングによって、ネットワークで送信されるパケットをハッカーが盗聴するのを防ぐことができます。

使用する SSL バージョンは、Web サーバがサポートするバージョンに応じて異なります。

SSL を選択した場合、SSL 接続に必須の SSL 証明書がセットアップによって自動的に作成されます。証明書には、サーバ情報、公開鍵、および秘密鍵が含まれています。

各 SSL 証明書の有効期間は 3 年です。管理者は期限切れの証明書を使用することはできます。ただし、同じ証明書を使用して SSL 接続を要求するたびに警告メッセージが表示されます。

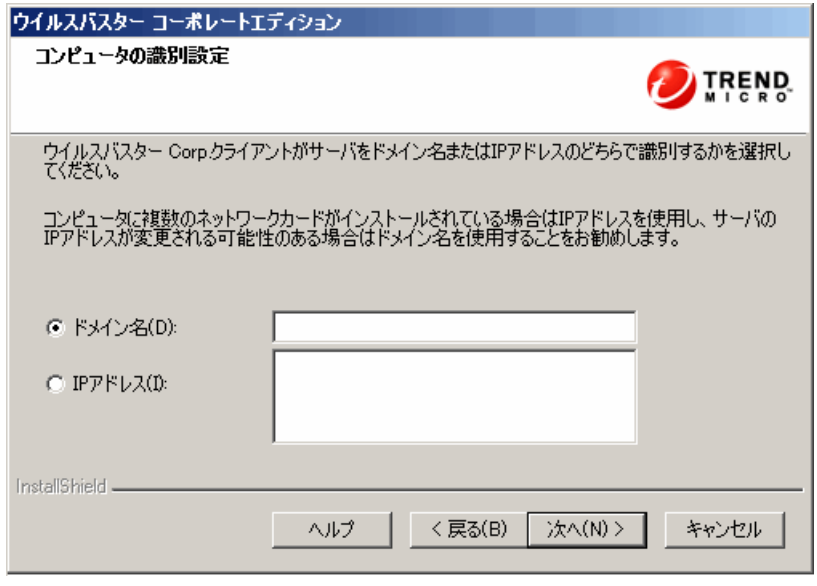
SSL を使用した通信の動作

1. 管理者は情報を Web コンソールから SSL 接続経由で Web サーバに送信できます。
2. Web サーバは、必要な証明書を使用する Web コンソールに応答します。
3. ブラウザは、RSA 暗号化を使用して鍵の交換を実行します。
4. Web コンソールは、Web サーバに RC4 暗号化を使用してデータを送信します。

RSA 暗号化は、安全性が高いですが通信速度が低下します。したがって、この方式は鍵交換のみに使用し、より高速な代替方式である RC4 をデータ転送に使用します。

サーバコンピュータの識別

図 2-7.　[コンピュータの識別設定] 画面



この画面で指定した設定は、新規のリモートインストールを実行している場合にのみ適用されます。リモートアップグレードの場合は、ウイルスバスター Corp. は以前のバージョンの設定を使用します。

ウイルスバスター Corp. クライアントがサーバコンピュータをドメイン名、IP アドレスのどちらで識別するかを指定します。

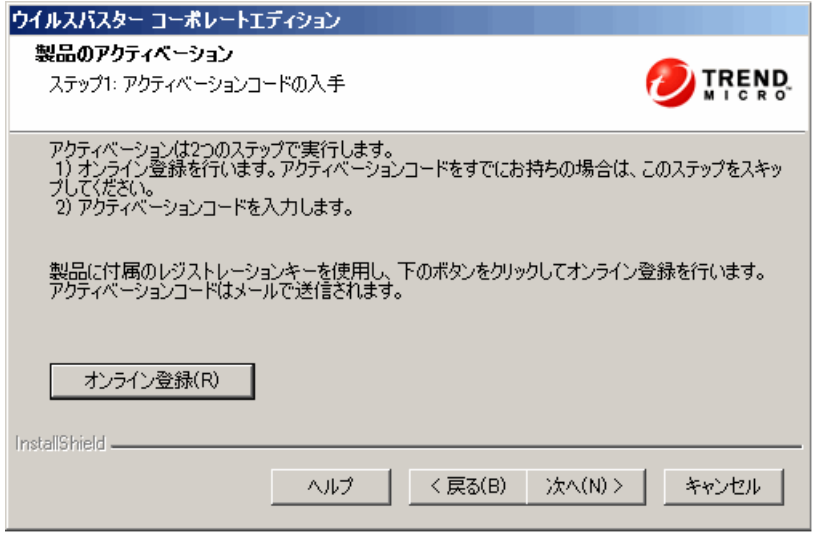
サーバコンピュータが IP アドレスで識別される場合に、その IP アドレスを変更すると、ウイルスバスター Corp. サーバとクライアントでの通信が不能になります。通信を復元するには、すべてのクライアントを再インストールする方法しかありません。サーバコンピュータがドメイン名で識別されているときに、そのドメイン名を変更した場合にも、同様の状況になります。

ほとんどのネットワークでは、サーバコンピュータの IP アドレスがドメイン名よりも変更される可能性が高いため、サーバコンピュータは、一般にドメイン名で識別するのが望ましい方法です。また、ウイルスバスター Corp. が DHCP サーバから IP アドレスを取得する場合には、IP アドレスを変更することはお勧めできません。

静的 IP アドレスを使用している場合は、サーバを IP アドレスで識別します。さらに、サーバコンピュータに複数のネットワークインタフェースカード (NIC) がある場合には、クライアント / サーバ間の正常な通信を維持するために、ドメイン名ではなく IP アドレスの 1 つを使用することを検討してください。

登録とアクティベーション

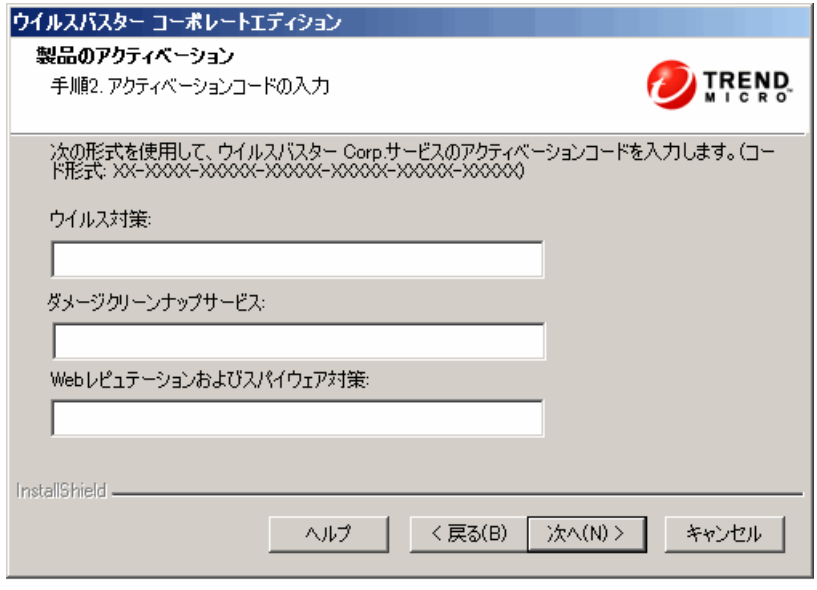
図 2-8. 製品登録画面



製品付属のレジストレーションキーを使用してウイルスバスター Corp. を登録し、次にアクティベーションコードを取得します。登録を完了して、アクティベーションコードを取得している場合には、この手順を省略してください。

アクティベーションコードがない場合には、[オンライン登録] をクリックします。セットアップによって、トレンドマイクロの製品登録 Web サイトが表示されます。登録フォームへの入力後、トレンドマイクロよりアクティベーションコードを含んだメールが送付されます。これで、インストールを続行できます。

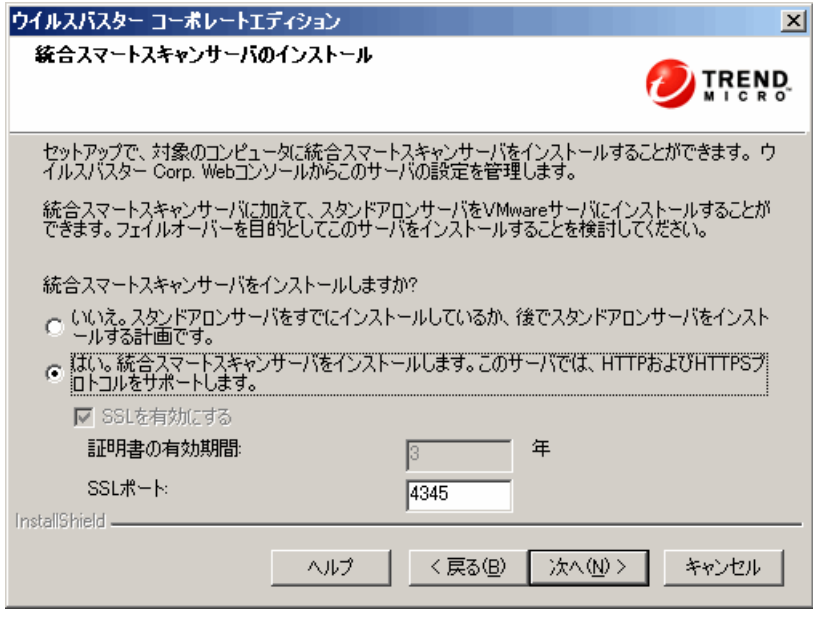
図 2-9.　[製品のアクティベーション] 画面



すでにアクティベーションコードを取得している場合には、インストール作業を続行して、アクティベーションコードを指定します。アクティベーションコードは大文字と小文字が区別されます。

統合スマートスキャンサーバのインストール

図 2-10.　[統合スマートスキャンサーバのインストール] 画面



ウイルスバスター Corp. スマートスキャンソリューションでは、複数の軽量パターンファイルを使用して、従来の不正プログラム対策およびスパイウェア対策パターンファイルと同等の保護機能が実現されています。これらのパターンファイルは、トレンドマイクロのアップデートサーバから配信され、スマートスキャンサーバおよびウイルスバスター Corp. サーバで使用することができます。

スマートスキャンサーバではスマートスキャンパターンがホストされ、1 時間ごとにアップデートされます。スマートスキャンパターンには、大部分のパターン定義が含まれています。スマートスキャンクライアントでは、このパターンファイルはダウンロードされません。クライアントでは、スマートスキャンサーバに検索クエリを送信し、潜在的脅威が検証されます。

注意：　スマートスキャンソリューションで使用されるもう 1 つのパターンファイルは、スマートスキャンエージェントパターンと呼ばれ、ウイルスバスター Corp. サーバでホストされ、クライアントにダウンロードされます。

クライアントが企業ネットワークに接続可能な場合、ローカルスマートスキャンサーバに検索クエリを送信できます。セットアップには、ローカル用のスマートスキャンサーバが含まれており (統合スマートスキャンサーバと呼びます)、ウイルスバスター Corp. サーバがインストールされているコンピュータと同じコンピュータにインストールされます。統合サーバの設定は、ウイルスバスター Corp. サーバの Web コンソールで管理します。

フェイルオーバーの目的で、複数のローカルのスマートスキャンサーバをインストールしてください。統合サーバに加えて、スタンドアロンのスマートスキャンサーバを VMware サーバにインストールすることができます。スタンドアロンサーバは、統合サーバと同じ機能および能力を持ちます。スタンドアロンサーバには、専用の管理コンソールがあり、ウイルスバスター Corp. の Web コンソールからは管理できません。スタンドアロンサーバについては、ウイルスバスター Corp. 用スマートスキャン クイックスタートガイドを参照してください。

ヒント： 統合スマートスキャンサーバとウイルスバスター Corp. サーバは同じコンピュータ上で実行されるため、2 つのサーバのトラフィックがピークになるときには、コンピュータのパフォーマンスが著しく低下する場合があります。ウイルスバスター Corp. サーバへのトラフィックを減らすには、スタンドアロンスマートスキャンサーバをプライマリスキャンソースに割り当てて、統合サーバをバックアップソースに割り当てます。クライアントの検索ソースの設定については、管理者ガイドを参照してください。

ライセンス

次のサービスについて、スマートスキャンを使用するためのライセンスをアクティベートします。

- ウイルス対策
- Web レピュテーションおよびスパイウェア対策

ウイルスバスター Corp. のライセンスの詳細については、68 ページの「登録とアクティベーション」を参照してください。

これらのライセンスをアクティベートしない場合でも、統合スマートスキャンサーバをインストールすることはできますが、クライアントでスマートスキャンを使用できなくなり、スマートスキャンサーバに接続できなくなります。ライセンスとアクティベーションに関する問題については、トレンドマイクロの代理店にお問い合わせください。

クライアントの接続プロトコル

クライアントは HTTP および HTTPS プロトコルを使用して統合スマートスキャンサーバに接続できます。HTTPS ではより安全な接続が可能ですが、HTTP では消費される帯域幅が少なくなります。

セキュリティで保護された接続に使用される SSL ポート番号は、ウイルスバスター Corp. サーバに使用する Web サーバ (Apache または IIS) によって異なります。詳細については、64 ページの「Web サーバ設定」を参照してください。

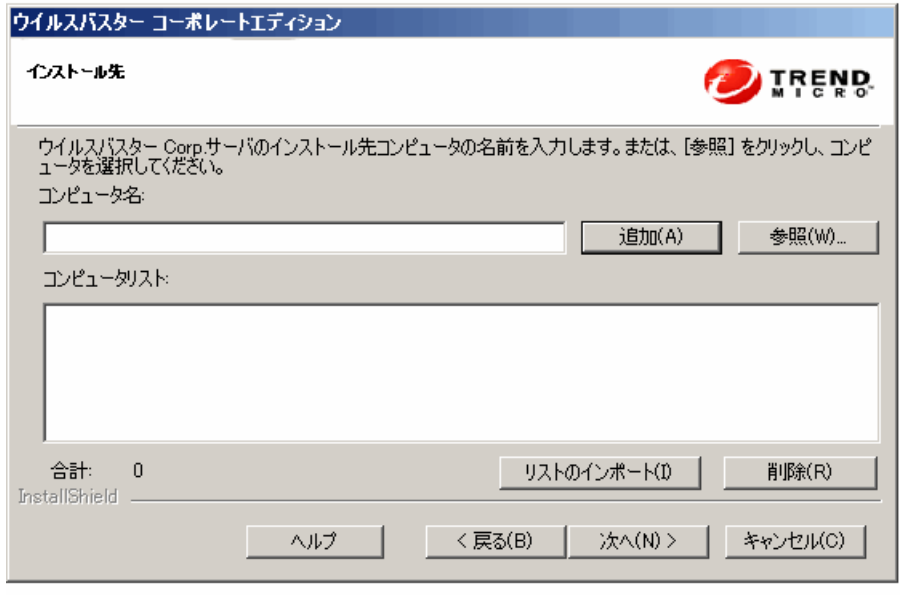
表 2-2. ウイルスバスター Corp. サーバおよび統合スマートスキャンサーバの SSL ポート番号

ウイルスバスター Corp. Web サーバの設定	ウイルスバスター Corp. サーバの SSL ポート	統合スマートスキャンサーバの SSL ポート
Apache Web サーバで SSL が有効	4343	4343
Apache Web サーバで SSL が無効	該当なし	4345
IIS 既定 Web サイトで SSL が有効	443	443
IIS 既定 Web サイトで SSL が無効	該当なし	443
IIS 仮想 Web サイトで SSL が有効	4343	4345
IIS 仮想 Web サイトで SSL が無効	該当なし	4345

クライアントがプロキシサーバ経由で統合サーバに接続する場合、Web コンソールから内部プロキシを設定する必要があります。プロキシの設定については、管理者ガイドを参照してください。

リモートインストール先

図 2-11.　リモートインストール先画面



ウイルスバスター Corp. をインストールする対象コンピュータを指定します。コンピュータのホスト名と IP アドレスを手動で入力することができます。 [参照] をクリックして、ネットワーク上のコンピュータを探します。

コンピュータ名は、[リストのインポート] をクリックしてテキストファイルからインポートすることができます。複数のコンピュータに同時にインストールする場合で、すべてのコンピュータに解析で異常がない場合には、テキストファイルに記載されている順番でウイルスバスター Corp. サーバがインストールされます。

テキストファイルには次の指定をします。

- 1 台のコンピュータ名を 1 行に指定します。
- UNC　(汎用命名規則) 形式を使用します　(例 : ¥¥test)。
- 「a」から「z」、「A」から「Z」、「.」 (ピリオド)、および「-」 (ハイフン) の文字のみを使用してください。

リモートインストールを確実に実行するためのヒント

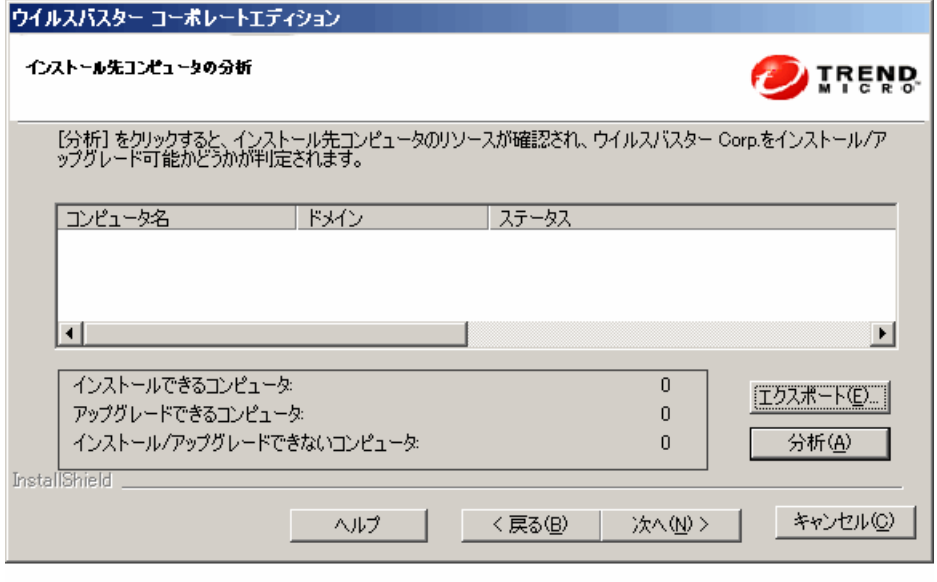
- インストール先コンピュータに管理者権限があることを確認します。

- コンピュータのホスト名やログオン情報のメモをとります（ユーザ名やパスワード）。
- 対象コンピュータがウイルスバスター Corp. サーバのインストールのシステム要件を満たしていることを確認します。
- このサーバが Web サーバの場合は、コンピュータに Microsoft IIS サーバ 5.0、6.0、または 7.0 がインストールされていることを確認します。Apache Web サーバを選択した場合、対象コンピュータにこのサーバが存在しない場合にはセットアップによって自動的にインストールされます。
- セットアップを起動したコンピュータを対象コンピュータに指定しないようにします。代わりに、そのコンピュータでローカルインストールを実行します。

対象コンピュータを指定済みの場合は、[次へ] をクリックします。セットアップによって、コンピュータがウイルスバスター Corp. のインストール要件を満たしているかどうかがチェックされます。

対象コンピュータ分析

図 2-12. [インストール先コンピュータの分析] 画面



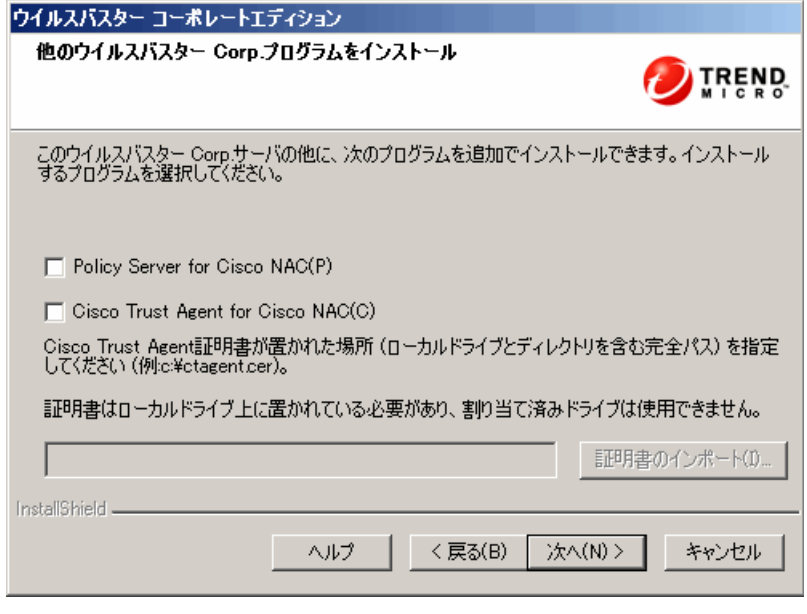
セットアップは、リモートインストールの続行を許可する前に、選択された対象コンピュータにウイルスバスター Corp. サーバをインストールできるかどうかを判定します。分析を開始するには、[分析] をクリックします。セットアップが、対象コンピュータへログオンするために使用する管理者のユーザ名とパスワードを要求する場合があります。分析後、画面に結果が表示されます。

複数のコンピュータにインストールする場合には、最低 1 つのコンピュータが分析で問題なければインストールが続行されます。セットアップは、そのコンピュータにウイルスバスター Corp. サーバをインストールし、分析で問題が発生したコンピュータは無視します。

リモートインストール時に、インストールの進行状況はセットアップを開始したコンピュータにのみ表示され、対象コンピュータには表示されません。

ウイルスバスター Corp. プログラム

図 2-13.　ウイルスバスター Corp. プログラムのインストール画面



次のウイルスバスター Corp. プログラムをインストールするように選択します。

ウイルスバスター Corp. クライアント

クライアントプログラムは、セキュリティリスクに対して実際の保護を提供します。したがって、ウイルスバスター Corp. サーバコンピュータをセキュリティリスクから保護するには、クライアントプログラムが必要になります。サーバのインストール時にクライアントをインストールするように選択する方法は、サーバを自動的に保護できるため便利です。また、サーバのインストール後にクライアントをインストールする手間を省けます。

注意： サーバのインストール後、クライアントをネットワーク上の他のコンピュータにインストールします。クライアントのインストール方法については、管理者ガイドを参照してください。

ウイルスバスター Corp. をアップグレードしている場合は、この画面が表示されません。

トレンドマイクロまたは他社製のエンドポイントセキュリティソフトウェアがサーバコンピュータに現在インストールされている場合には、ウイルスバスター Corp. によって、自動的にそのソフトウェアをアンインストールして、ウイルスバスター Corp. クライアントと置き換えることが可能な場合と、可能でない場合があります。ウイルスバスター Corp. が自動的にインストールするソフトウェアのリストについては、サポート担当者にお問い合わせください。ソフトウェアが自動的にアンインストールされない場合には、ウイルスバスター Corp. のインストールを続ける前に手動でアンインストールしてください。

Cisco Network Admission Control (NAC) プログラム

Cisco Network Admission Control (以下、NAC) は、主に、管理権限とウイルス対策およびセキュリティポリシーを施行することによりネットワーク内のセキュリティリスクを管理します。このソフトウェアでは、ネットワークとセキュリティ関連の通信が可能です。

Cisco NAC には、ウイルスバスター Corp. と同様にサーバコンポーネント (Policy Server for Cisco NAC) およびクライアントコンポーネント (Cisco Trust Agent、以下 CTA) があります。Cisco NAC を使用するには、Cisco NAC をサポートする Cisco ルータが必要で、Cisco Admission Control Server (以下、ACS) へ接続する必要があります。

注意： Cisco NAC プログラムは、ウイルス対策サービスをアクティベートしないと使用できません。

リモートサーバインストールを実行する場合、ポリシーサーバまたは CTA をインストール / アップグレードすることはできません。リモートインストールの実行後、ウイルスバスター Corp. の Web コンソールから CTA をクライアントにインストールし、ウイルスバスター Corp. セットアップパッケージからポリシーサーバインストーラを実行してポリシーサーバをインストールします。Cisco NAC の設定については、管理者ガイドを参照してください。

Policy Server for Cisco NAC

ウイルスバスター Corp. Web コンソールと同様に、Policy Server for Cisco NAC もネットワーク管理ポリシーを設定するための Web ベースのコンソールです。ポリシーサーバは、クライアントパターンファイルや検索エンジンが最新版であることを絶えず確認します。

ウイルスバスター Corp. サーバとポリシーサーバは、同一のコンピュータで同一の初期設定 Web サイトを使用して実行するか、別のコンピュータで実行することができます。これらを同じコンピュータにインストールする場合、サーバのインストール時に同時にインストールすることができます。また、ポリシーサーバを後からインストールすることもできます。ポリシーサーバを他のコンピュータにインストールする場合、そのコンピュータでポリシーサーバインストーラを実行します。

ポリシーサーバインストーラは、ウイルスバスター Corp. セットアップパッケージから実行します。

Cisco Trust Agent (CTA) for Cisco NAC

CTA は、ウイルスバスター Corp. サーバ内にホストされ、クライアントにインストールされるプログラムで、このプログラムによってウイルスバスター Corp. クライアントから Cisco ACS へウイルス対策情報の報告が可能になります。

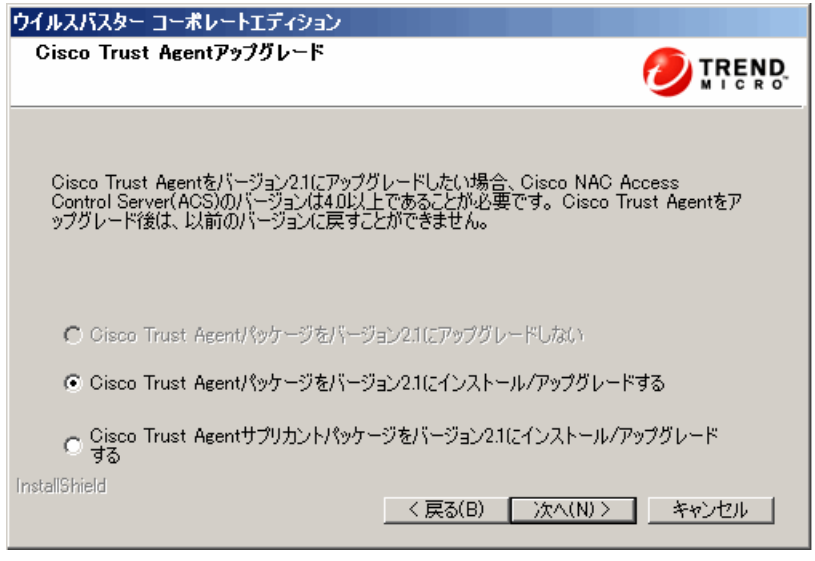
サーバのインストール時にこのオプションを選択すると、ウイルスバスター Corp. サーバは管理対象のすべてのクライアントに CTA を自動的にインストールします。次の画面では、CTA と CTA サプリカントのどちらをインストールするか選択を求められます。これらの 2 つのバージョンの違いは、サプリカントパッケージがレイヤ 2 認証をコンピュータとエンドユーザに提供していることのみです。

このオプションを選択しない場合でも、Web コンソールから CTA をクライアントにインストールすることができます ([Cisco NAC] → [エージェント配信])。ただしこの方法では、新規クライアントをサーバに追加するたびにこの操作を行う必要があります。Web コンソールから CTA をインストールする方法については、ウイルスバスター Corp. サーバのヘルプを参照してください。

CTA のインストールでは証明書ファイル (.cer) が必要です。CTA はこのファイルを使用して Cisco ACS との暗号化通信セッションを作成します。証明機関 (以下、CA) サーバは証明書ファイルを生成します。トレンドマイクロの販売代理店に証明書ファイルを要求し、サーバインストール時や Web コンソール ([Cisco NAC] → [クライアント認証ファイル]) で証明書を入力します。

Cisco Trust Agent のインストール / アップグレード

図 2-14. [Cisco Trust Agent アップグレード] 画面



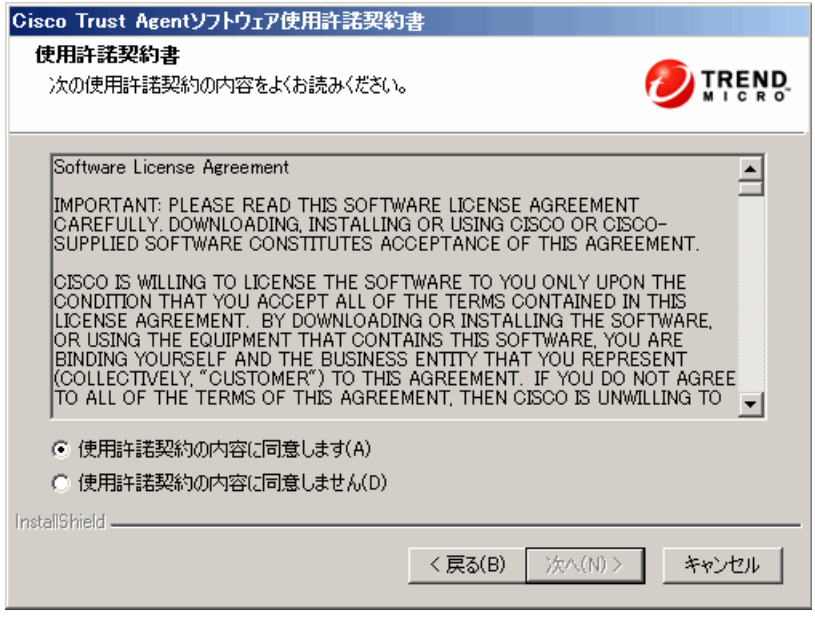
新規インストールを実行する場合は、前の画面で Cisco Trust Agent のインストールを選択する場合のみ、この画面が表示されます。CTA パッケージを選択してクライアントにインストールしてください。

アップグレードしている場合は、あらかじめ CTA をインストールした場合のみ、この画面が表示されます。CTA を現在のバージョン (2.1) にアップグレードするかどうか選択してください。アップグレードする場合は、CTA アップグレードパッケージを選択してください。

サーバのインストール時に、CTA のインストールを選択しなかった場合でも、Web コンソールから CTA をインストールすることができます。

Cisco Trust Agent のライセンス

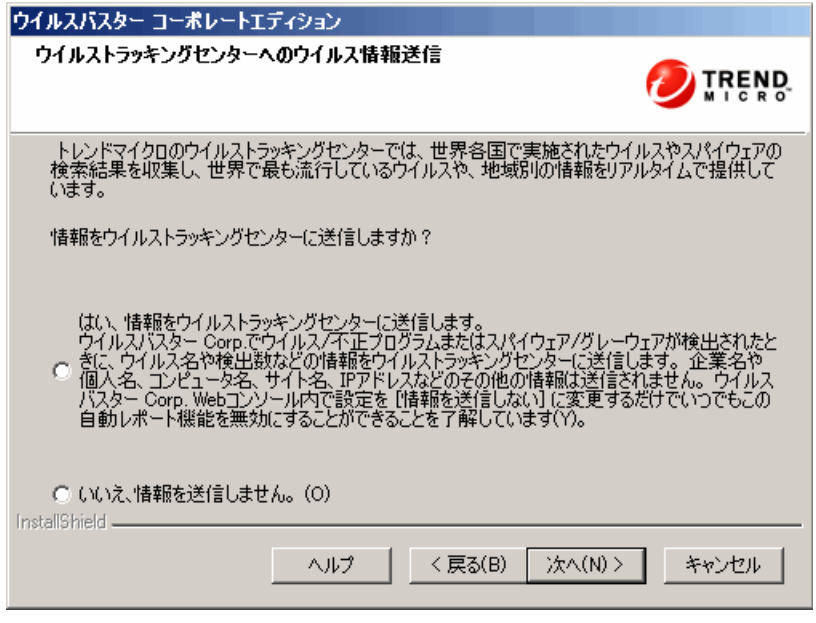
図 2-15.　Cisco Trust Agent の使用許諾契約書画面



インストールを続行するには使用許諾契約をお読みいただき、使用許諾契約の条項に同意いただく必要があります。

トレンドマイクロ ウイルストラッキングセンターへのウイルス情報送信

図 2-16. [ウイルストラッキングセンターへのウイルス情報送信] 画面



セキュリティリスクの検索結果はウイルストラッキングプログラムへ送信することができ、セキュリティリスク大規模感染の傾向分析の向上に役立てることができます。このプログラムに参加すると、セキュリティリスクの進行および拡散について詳しい情報を入手できます。

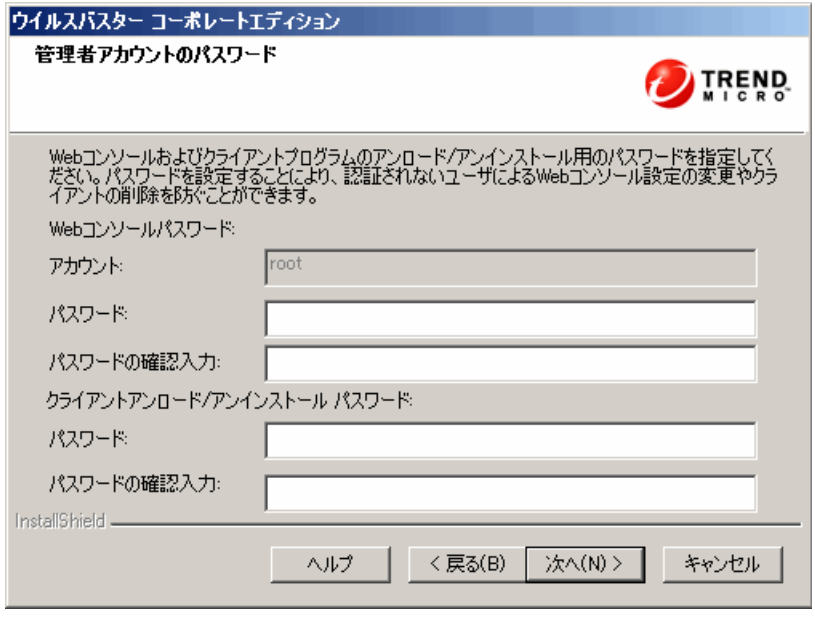
このプログラムへの参加は Web コンソールからいつでも中止できます。

現在のトレンドマイクロリアルタイムマップを表示するには、次のサイトにアクセスします。

http://wtc.trendmicro.com/japanese/

管理者アカウントのパスワード

図 2-17. [管理者アカウントのパスワード] 画面



以下を実行するためのパスワードを指定します。

Web コンソールへのアクセス

セットアップによって、インストール時にルートアカウントが作成されます。ルートアカウントには、ウイルスバスター Corp. Web コンソールのすべての機能に対する完全なアクセス権があります。管理者は、このアカウントを使用してログオンすることで、他のユーザが Web コンソールへログオンするために使用できるカスタムユーザアカウントを作成できます。ユーザは、アカウントのアクセス権限に応じて 1 つまたは複数の Web コンソールの機能を設定または表示できます。

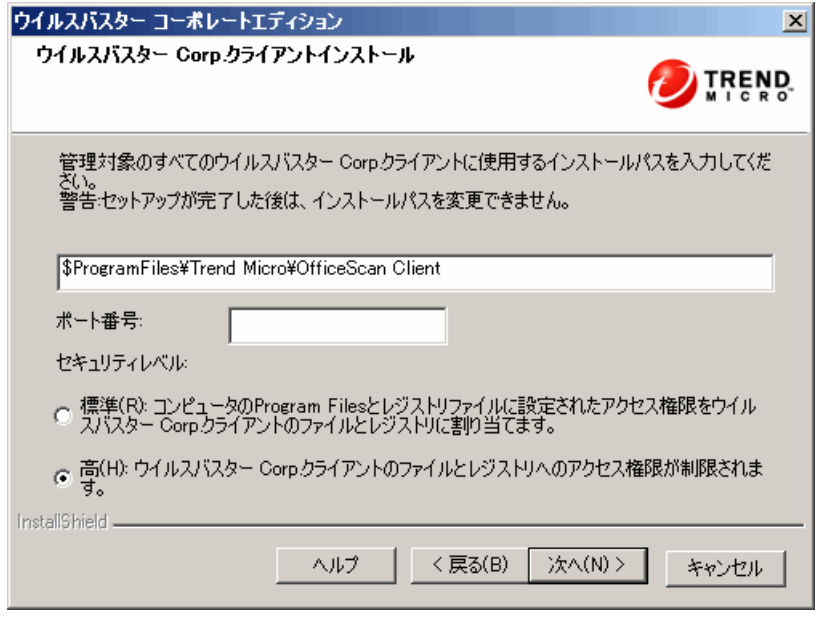
ユーザとウイルスバスター Crop. 管理者のみが知っているパスワードを指定する必要があります。パスワードを忘れた場合は、パスワードの再設定についてサポート担当者にお問い合わせください。

ウイルスバスター Corp. クライアントのアンロードとアンインストール

ウイルスバスター Corp. クライアントのアンインストールやアンロードが不正に行われないように、パスワードを指定します。クライアントのアンインストールやアンロードは、クライアントの機能に問題がある場合にのみ実行し、即座にインストール / 再読み込みを行います。

クライアントのインストールパス

図 2-18.　[ウイルスバスター Corp. クライアントインストール] 画面



初期設定のクライアントインストール設定をそのまま使用するか、別のクライアントインストールパスを指定します。インストールディレクトリに十分なディスクの空き容量がない場合には、パスを変更します。

ヒント：　トレンドマイクロは初期設定を使用することを推奨します。

別のインストールパスを指定する場合、静的パスを入力するか変数を使用します。クライアント上に存在しないディレクトリが入力したパスに含まれている場合には、セットアップによってクライアントインストール時に自動的にディレクトリが作成されます。

静的クライアントインストールパスを入力するには、ドライブパスにドライブ文字を含めて入力します。たとえば、C:¥Program Files¥Trend Micro¥OfficeScan Client のようになります。

注意： クライアントのインストールパスは、ウイルスバスター Corp. サーバのインストールが終了した後に変更することはできません。インストールされるすべてのウイルスバスター Corp. クライアントには、同じインストールパスが使用されます。

クライアントインストールパスに変数を指定する場合には、次の変数を使用します。

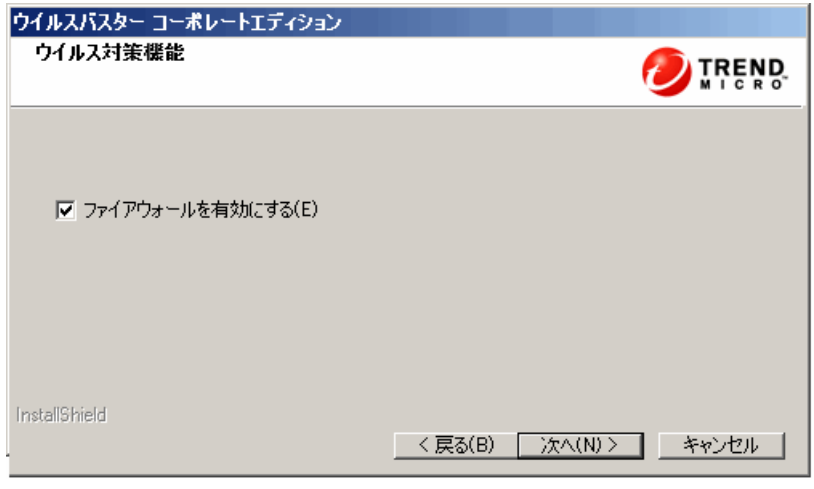
- $BOOTDISK: コンピュータが起動するハードディスクのドライブ文字。初期設定は C:¥ です。
- $WINDIR: Windows ディレクトリ。初期設定は C:¥Windows です。
- $ProgramFiles: Program Files ディレクトリは、自動的に Windows で設定され、多くの場合ソフトウェアのインストールに使用されます。初期設定は C:¥Program Files です。

また、この画面では次の設定をします。

- ポート番号 : セットアップは、ウイルスバスター Corp. サーバがクライアントとの通信に使用するポート番号をランダムに生成します。別のポート番号を指定することもできます。
- クライアントのセキュリティレベル : ウイルスバスター Corp. のインストール後、セキュリティレベルをウイルスバスター Corp. コンソールから変更することができます ([ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [権限とその他の設定] → [その他の設定])。
  - **標準** : クライアントは、クライアントコンピュータでウイルスバスター Corp. クライアントのフォルダ、ファイルおよびレジストリへの読み取り / 書き込みアクセスが可能です。
  - **高** : クライアントは、ウイルスバスター Corp. クライアントのフォルダ、ファイル、およびレジストリへのアクセスが制限されます (初期設定)。 [高] を選択すると、Windows 2000/XP/Server 2003 を実行するクライアントコンピュータについては、ウイルスバスター Corp. のフォルダ、ファイル、およびレジストリのアクセス権限設定が Program Files フォルダから継承されます。

ウイルス対策機能

図 2-19. [ウイルス対策機能] 画面



この画面は、ウイルス対策サービスをアクティベートする場合にのみ、表示されます。

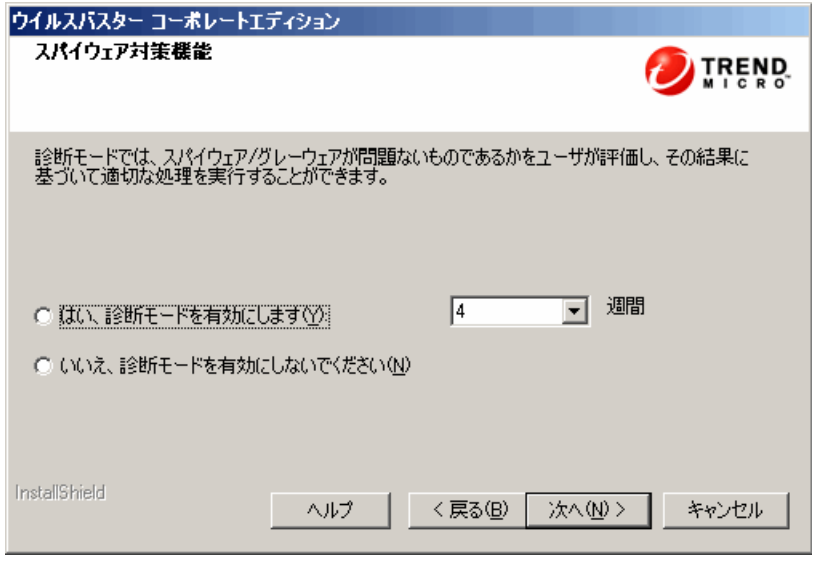
ウイルスバスター Corp. のファイアウォール

ウイルスバスター Corp. のファイアウォールは、ステートフルインスペクション、高性能のネットワークウイルス検索、および駆除を使用してネットワーク上のクライアントとサーバを保護します。IP アドレス、ポート番号、プロトコルなどによって接続をフィルタする複数のルールを作成し、それらのルールを異なるユーザのグループに適用します。

ファイアウォールは無効にして、後からウイルスバスター Corp. サーバ Web コンソールから有効にすることもできます。

スパイウェア対策機能

図 2-20. [スパイウェア対策機能] 画面



この画面は、Web レピュテーションおよびスパイウェア対策サービスをアクティベートする場合にのみ、表示されます。

診断モードでは、サーバによって管理されているすべてのクライアントの手動検索、予約検索、リアルタイム検索、および ScanNow で検出された、スパイウェア / グレーウェアのログが記録されますが、スパイウェア / グレーウェアコンポーネントは駆除されません。駆除は、プロセスを終了するか、レジストリ、ファイル、Cookie およびショートカットを削除します。

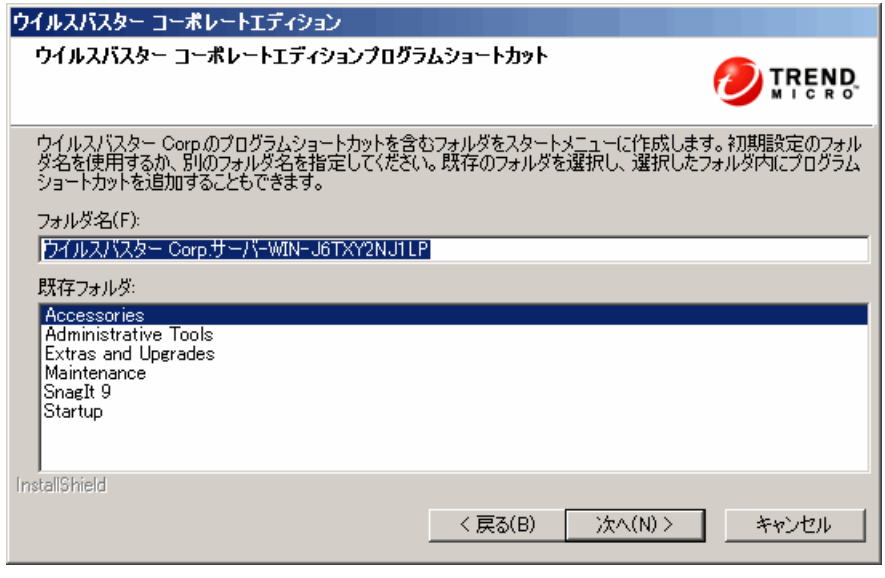
診断モードでは、トレンドマイクロがスパイウェア / グレーウェアとして検出したアイテムを評価でき、その評価に基づいて、適切な処理を設定できます。たとえば、検出されたスパイウェア / グレーウェアがセキュリティリスクではないと見なされる場合には、スパイウェア / グレーウェアの承認リストに追加できます。

インストール後に診断モードで推奨されているいくつかの処理については、管理者ガイドを参照してください。

診断モードが特定の期間にのみ適用されるように設定するには、この画面で週単位の期間を指定します。インストール後、診断モードの設定は Web コンソールで変更できます ([ネットワーク上のコンピュータ] → [グローバルクライアント設定] → [スパイウェア / グレーウェア検索設定のみ])。

プログラムフォルダのショートカット

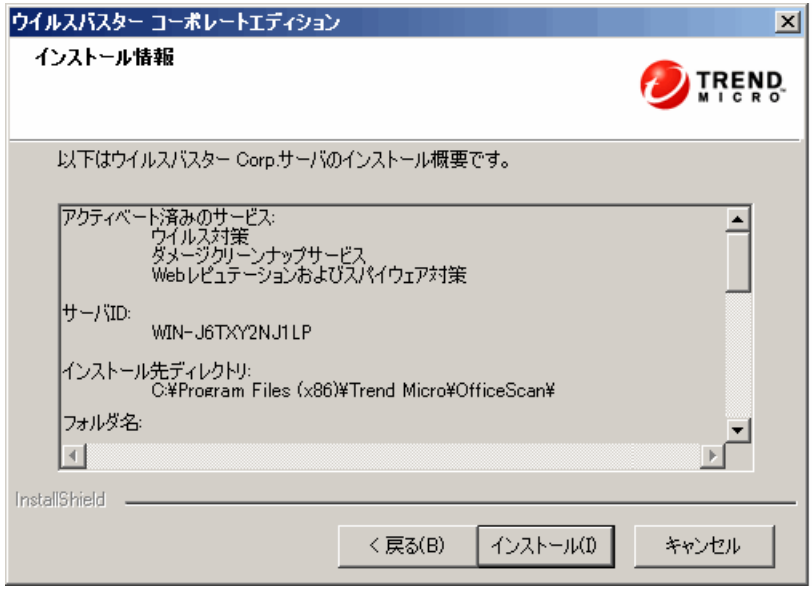
図 2-21.　プログラムのショートカット画面



初期設定のフォルダ名をそのまま使用するか、または新しい名前を指定します。既存のフォルダを選択して、そこにプログラムのショートカットを追加することも可能です。

インストール情報

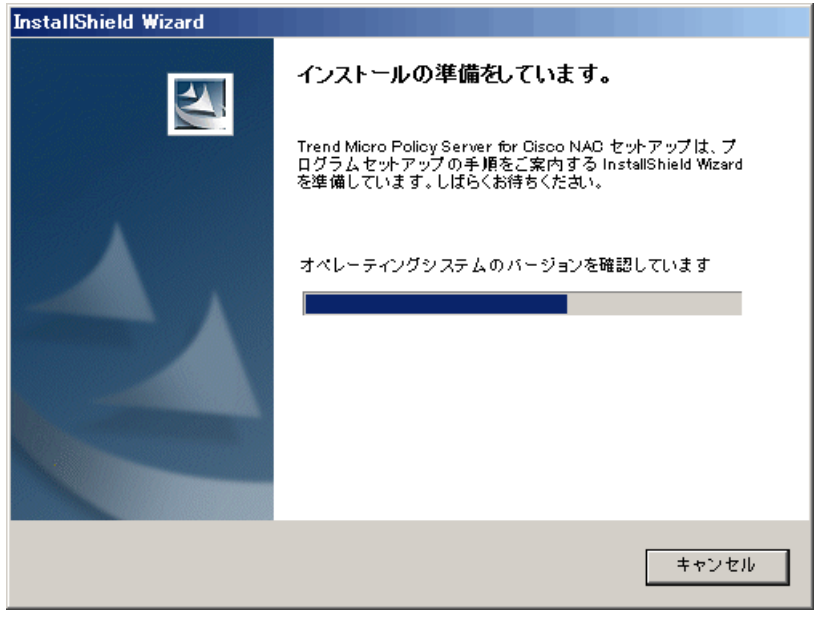
図 2-22. [インストール情報] 画面



この画面は、インストール設定の概要を表示します。インストール情報が正しいことを確認し、[戻る] をクリックして設定やオプションを変更します。インストールを開始するには、[インストール] をクリックします。

ポリシーサーバのインストール

図 2-23.　ポリシーサーバのインストール画面



Policy Server for Cisco NAC のインストールを選択すると、この画面が表示されます。ポリシーサーバのインストール画面に表示される設定およびオプションは、ウイルスバスター Corp. サーバのインストール時に指定した設定とほとんど同じです。

- **使用許諾契約書**：使用許諾契約の内容に同意して続行します。
- **インストールパス**：初期設定のインストールパスをそのまま使用するか、ポリシーサーバをインストールするローカルコンピュータ上の場所を指定します。
- **Web サーバ**：IIS または Apache Web サーバを使用するかどうかを指定します。
- **Web サーバ設定**：選択した Web サーバの設定を指定します。
- **Web コンソールパスワード**：ポリシーサーバコンソールにアクセスするためのパスワードを指定します。このコンソールは、ウイルスバスター Corp. から起動できますが、ウイルスバスター Corp. サーバコンソールとは別のものです。

- **ACS サーバ認証**: ACS サーバは、ネットワークアクセスデバイス経由で、クライアントからのウイルスバスター Corp. クライアントウイルス対策データを受信し、評価用に外部ユーザデータベースに渡します。また、ACS サーバは、処理後に、評価の結果をネットワークアクセスデバイスに渡します。評価結果には、ウイルスバスター Corp. クライアントへの命令が含まれている場合もあります。
- **インストール情報**: インストール情報を確認します。

トレンドマイクロウイルスバスター コーポレートエディションサーバのインストールの完了

図 2-24. インストールの完了画面

インストールを完了したら、製品や既知の問題などの基本情報を記載した Readme ファイルを参照してください。

また、Web コンソールを起動して、ウイルスバスター Corp. の設定を開始することもできます。

インストール後のタスク

インストール後には以下のタスクを行ってください。

- 91 ページの「サーバのインストールまたはアップグレードの確認」
- 93 ページの「ウイルスバスター Corp. コンポーネントのアップデート」
- 93 ページの「初期設定の確認」
- 94 ページの「Client Mover for Legacy Platforms の使用」。Windows 95、98、Me、NT、または Itanium アーキテクチャが動作するクライアントの場合のみ、このタスクを実行してください。
- 96 ページの「Control Manager へのウイルスバスター Corp. の登録」。Control Manager への登録は、新しくインストールされたウイルスバスター Corp. サーバにのみ適用されます。
- 97 ページの「プラグインマネージャのインストール」

サーバのインストールまたはアップグレードの確認

インストールまたはアップグレードの完了後に、以下の事項を検証してください。

表 2-3. ウイルスバスター Corp. のインストールまたはアップグレード後に確認する事項

確認事項	詳細
ウイルスバスター Corp. サーバのショートカット	サーバコンピュータの Windows の [スタート] メニューにウイルスバスター Corp. サーバのショートカットがあること。
プログラムのリスト	サーバコンピュータのコントロールパネルの [プログラムの追加と削除] のリストにウイルスバスター Corp. サーバが含まれていること。
ウイルスバスター Corp. Web コンソール	Internet Explorer ブラウザに次の URL を入力すること。 • HTTP 接続 : http://< ウイルスバスター Corp. サーバ名 >:< ポート番号 >/OfficeScan • HTTPS 接続 : https://< ウイルスバスター Corp. サーバ名 >:< ポート番号 >/OfficeScan < ウイルスバスター Corp. サーバ名 > の部分は、ウイルスバスター Corp. サーバの名前または IP アドレスが入ります。 Web コンソールのログオン画面が表示されます。

表 2-3. ウイルスバスター Corp. のインストールまたはアップグレード後に確認する事項（続き）

確認事項	詳細
ウイルスバスター Corp. サーバサービス	Microsoft 管理コンソールに次のウイルスバスター Corp. サービスが表示されていること。 ・ OfficeScan Master Service （起動している必要があります) ・ Trend Micro Smart Scan Server (統合スマートスキャンサーバをインストールした場合。スタートアップのタイプは「手動」) ・ Trend Micro Policy Server for Cisco NAC （インストールした場合) ・ OfficeScan Active Directory Integration Service （役割ベースの管理が正常に機能している場合) ・ OfficeScan Control Manager Agent
ウイルスバスター Corp. サーバプロセス	Windows タスクマネージャを開いたとき、次のウイルスバスター Corp. プロセスが実行されていること。 ・ OfcService.exe ・ DBServer.exe ・ iCRCService.exe (統合スマートスキャンサーバをインストールした場合) ・ OfcCMAgent.exe （ウイルスバスター Corp. サーバが Control Manager に登録済みの場合)
サーバのインストールログ	サーバインストールログ OFCMAS.LOG は、%windir% に存在します。
レジストリキー	次のレジストリキーが存在すること。 HKEY_LOCAL_MACHINE¥Software¥TrendMicro¥OfficeScan
プログラムフォルダ	ウイルスバスター Corp. サーバファイルが <「サーバのインストールフォルダ」> にあること。

ウイルスバスター Corp. コンポーネントのアップデート

ウイルスバスター Corp. のインストールまたはアップグレード後、サーバのコンポーネントをアップデートしてください。

注意： このセクションでは手動アップデートの方法を紹介します。予約アップデートまたはアップデート設定についての詳細は、ウイルスバスター Corp. サーバのヘルプを参照してください。

ウイルスバスター Corp. サーバをアップデートするには

1. ウイルスバスター Corp. の Web コンソールを開きます。
2. メインメニューで、[アップデート] → [サーバ] → [手動アップデート] をクリックします。 [手動アップデート] 画面に、現在のコンポーネント、これらのバージョン番号、およびこれらの最終アップデート日時が表示されます。
3. アップデート対象コンポーネントを選択します。
4. [アップデート] をクリックします。アップデートサーバに新しいコンポーネントがあるかどうかが確認されます。アップデートが進行し、ステータスが表示されます。

初期設定の確認

初期設定でウイルスバスター Corp. をインストールします。これらの設定がセキュリティ要件に適合していない場合は、Web コンソールで設定を変更します。Web コンソールで可能な設定の詳細については、ウイルスバスター Corp. サーバのヘルプと管理者ガイドを参照してください。

検索設定

ウイルスバスター Corp. は、クライアントをセキュリティリスクから保護するために複数の検索の種類を備えています。 [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] →{ 検索の種類 } へ進むと、Web コンソールから検索設定を変更することができます。

グローバルクライアント設定

ウイルスバスター Corp. は、サーバに登録されたすべてのクライアント、または特定の権限を持つすべてのクライアントに適用される複数の種類の設定を備えています。 [ネットワーク上のコンピュータ] → [グローバルクライアント設定] の順に進んで、Web コンソールからグローバルクライアント設定を変更することができます。

クライアント権限と設定

初期設定のクライアント権限には、クライアントコンソールの [メール検索] と [ツールボックス] タブの表示も含まれています。 [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [権限とその他の設定] の順に進んで、Web コンソールから初期設定のクライアント権限を変更することができます。

Client Mover for Legacy Platforms の使用

ウイルスバスター Corp. クライアントでは、Windows 95/98/Me/NT、および Itanium アーキテクチャプラットフォームはサポートされなくなりました。ウイルスバスター Corp. クライアントがこれらのプラットフォームのいずれかで実行されている場合に、クライアント管理用サーバをバージョン 10 にアップグレードすると、次のようになります。

- ウイルスバスター Corp. クライアントはアップグレードされません。
- ウイルスバスター Corp. 10 サーバは、クライアントの管理を停止します。クライアントのステータスは「切断」となります。
- ウイルスバスター Corp. 10 サーバは、unsupCln.txt という名前のファイルにクライアントの情報を保存します。このファイルは、同じバージョンのサーバにクライアントを「移動」するために使用します。「移動」とは、新しいクライアント管理用サーバを指定することを意味します。
- ウイルスバスター Corp. 10 サーバのコンピュータでは、これらのサポート対象外プラットフォームで Client Mover というツールを実行する必要があります。このツールは、新しいサーバに管理されることをクライアントに通知し、クライアントの移動が成功したかどうかを確認します。クライアントは通知を受け取ると、新しい親サーバに登録します。

クライアントを移動するには

1. 新しい親サーバを準備します。移動するクライアントのバージョンと同じバージョンのサーバを準備します。
2. サーバのコンピュータ名、IP アドレス、および待機ポートをメモに記録します。これらの詳細情報は、クライアントを移動するときに必要になります。

   サーバの待機ポートは、サーバの Web コンソールで [管理] → [接続設定] へ進むことで調査できます。
3. ウイルスバスター Corp. 10 サーバのコンピュータで、< サーバのインストールフォルダ >¥PCCSRV¥Admin¥Utility¥ClientMover へ進み、clientmover.exe を実行します。
4. コマンドウィンドウで次のコマンドを入力します。

   ClientMover /P:<ExportDataPath> /S:<ServerIP:port> /N

説明 :

- ExportDataPath: クライアント情報を含むこのファイル (unsupCln.txt) のパスとファイル名。
- ServerIP:port: 新しい親サーバの IP アドレスとサーバの待機ポートです。
- /N: 通知を実行しクライアントを新しい親サーバに移動するコマンドです。このコマンドは、/V コマンドと連携して使用します。

例 :

ClientMover /P:"C:¥Program Files¥TrendMicro¥OfficeScan¥PCCSRV¥Private¥unsupcln.txt" /S:123.12.12.123:23456 /N

5. /V コマンドを使用し、ツールがクライアントを移動させるのに成功したかどうかを確認します。このコマンドは、ウイルスバスター Corp. 10 サーバの IP アドレスと新しい親サーバとを比較します。IP アドレスが同じであれば、ツールではクライアントを移動できなかったことを意味します。

   例 :

   ClientMover /P:"C:¥Program Files¥Trend Micro¥OfficeScan¥PCCSRV¥Private¥unsupcln.txt" /S:123.12.12.123:23456 /V

6. 結果をチェックします。

   a. ¥PCCSRV¥Private¥ にあるログにアクセスします。ログファイル名は unsupcln.txt.log.<date_time> です。

      例 : unsupcln.txt.log.20080101_123202

   b. また、同一フォルダでウイルスバスター Corp. が unsupcln.txt ファイルをアップデートし、またそのバックアップをとったかどうかを確認します。バックアップファイル名は unsupcln.txt.bak です。

   アップデートされた unsupcln.txt ファイルのエントリ例を次に示します。

   ```
   ------------------------------------------------------------
   x12xx345-6xxx-78xx-xx91-234x567x8x91 1234567891 23456 0
   ------------------------------------------------------------
   ```

   説明 :

   - 「x12xx345-6xxx-78xx-xx91-234x567x8x91」はクライアントの GUID です。
   - 「1234567891」は 10 進数形式のクライアント用 IP アドレスです。

- 「23456」はクライアントの待機ポートです。
- 「0」は結果で、通知が完了したことを意味します。

  他には次のような結果が考えられます。

  - 1 = クライアントへの通知は成功
  - 2 = クライアントへの通知は失敗
  - 3 = 確認成功
  - 4 = 確認失敗

unsupcln.txt.log.<date_time> ファイルのエントリ例を次に示します。

```
------------------------------------------------------------
x12xx345-6xxx-78xx-xx91-234x567x8x91 123.12.12.123:23456
Unable to send the notification. Please check the network or
client status.
------------------------------------------------------------
```

説明 :

- 「x12xx345-6xxx-78xx-xx91-234x567x8x91」はクライアントの GUID です。
- 「123.12.12.123:23456」はクライアントの IP アドレスと待機ポートです。
- 結果は「Unable to send the notification. Please check the network or client status.」です。

7. 現在のクライアントのステータスを確認せずに通知または検証を強制するには、/F コマンドを使用します。

Control Manager へのウイルスバスター Corp. の登録

新しくインストールしたウイルスバスター Corp. サーバを Control Manager サーバで管理する場合、インストール後、Control Manager にウイルスバスター Corp. を登録します。 [管理] → [Control Manager 設定] の順に進むと、ウイルスバスター Corp. の Web コンソールから登録できます。詳細については、ウイルスバスター Corp. サーバのオンラインヘルプを参照してください。

プラグインマネージャのインストール

プラグインマネージャにより、外部で開発されたプラグインプログラムも、利用可能になればすぐに使用を始めることができます。プラグインマネージャでは、ウイルスバスター Corp. サーバとクライアント両方のプラグインプログラムをウイルスバスター Corp. の Web コンソール上に表示します。プラグインプログラムは Web コンソールからインストールして管理します。たとえば、クライアントにクライアント用プラグインプログラムを配信できます。

Web コンソールのメインメニューで、[プラグインマネージャ] をクリックして、プラグインマネージャのダウンロードを実行します。セットアップ画面の指示に従ってインストールを完了してください。プラグインマネージャのインストールが正常に完了したら、使用可能なプラグインプログラムを確認します。

注意： インストールの要件と手順については、プラグインマネージャの Readme ファイルを参照してください。

サーバのアンインストールの実行

ウイルスバスター Corp. サーバで問題が発生した場合、アンインストールプログラムを使用し、コンピュータからウイルスバスター Corp. サーバを安全に削除してから、ウイルスバスター Corp. を再インストールします。

サーバをアンインストールする前の作業

サーバをアンインストールする前に、そのサーバが管理するクライアントを同じバージョンのウイルスバスター Corp. サーバに移動してください。サーバを後から再インストールすることを計画している場合には、サーバデータベースと設定ファイルをバックアップすることについて検討してください。

他のウイルスバスター Corp. サーバへのクライアントの移動

ウイルスバスター Corp. の Web コンソールには、サーバで管理されているクライアントを他のウイルスバスター Corp. サーバへ移動するオプションがあります。

他のウイルスバスター Corp. サーバへクライアントを移動するには

1. 他のウイルスバスター Corp. サーバに関する次の情報をメモに記録します。これらの情報は、クライアントを移動するときに必要になります。
   - コンピュータ名または IP アドレス
   - サーバ待機ポート

     サーバ待機ポートを表示するには、[管理] → [接続設定] に進みます。ポート番号が画面に表示されます。
2. アンインストールするサーバの Web コンソールで、[ネットワーク上のコンピュータ] → [クライアント管理] に進みます。
3. クライアントツリーで、アップグレードするクライアントを選択し、[クライアントツリー管理] → [クライアントの移動] の順にクリックします。
4. [選択したクライアントを別のウイルスバスター Corp. サーバに移動する] で、ウイルスバスター Corp. 10 サーバのコンピュータ名 /IP アドレスとサーバ待機ポートを指定します。
5. [移動] をクリックします。

すべてのクライアントが移動され、他のウイルスバスター Corp. サーバですでに管理されている場合には、ウイルスバスター Corp. サーバを安全にアンインストールできます。

ウイルスバスター Corp. のデータベースと設定ファイルのバックアップと復元

アンインストールの前にウイルスバスター Corp. のデータベースと重要な設定ファイルをバックアップします。ウイルスバスター Corp. サーバデータベースは、ウイルスバスター Corp. プログラムディレクトリ以外の場所にバックアップしてください。

ウイルスバスター Corp. データベースと設定ファイルをバックアップおよび復元するには

1. ウイルスバスター Corp. Web コンソールを介して、データベースのバックアップを行います ([管理] → [データベースバックアップ])。手順については、管理者ガイドまたはウイルスバスター Corp. サーバのヘルプを参照してください。

   警告： 他のバックアップツールやアプリケーションを使用しないでください。

2. Microsoft 管理コンソールから、OfficeScan Master Service を停止します。
3. 以下の <「サーバのインストールフォルダ」>¥PCCSRV フォルダのファイルとフォルダは、手動でバックアップしてください。
   - ofcscan.ini: グローバルクライアント設定が含まれます。
   - ous.ini: ウイルス対策コンポーネント配信用のアップデート元情報が含まれます。

- Private **フォルダ**： ファイアウォールとアップデート元設定が含まれます。
- Web¥tmOPP **フォルダ**： 大規模感染予防設定が含まれます。
- Pccnt¥Common¥OfcPfw2.dat: ファイアウォール設定が含まれます。
- Download¥OfcPfw2.dat, OfcPfw3.dat: ファイアウォール配信設定が含まれます。
- Log **フォルダ**: システムイベントおよび接続検証ログが含まれます。
- Virus **フォルダ**: 隔離されたファイルが含まれます。
- HTTPDB **フォルダ**: ウイルスバスター Corp. データベースが含まれます。

4. ウイルスバスター Corp. サーバのアンインストールを実行します。詳細については、97 ページの「サーバのアンインストールの実行」を参照してください。
5. 新規インストールを実行します。詳細については、44 ページの「ウイルスバスター Corp. サーバの新規インストールの実行」を参照してください。
6. セットアップの終了後、Microsoft 管理コンソール (MMC) を開きます ([スタート] → [ファイル名を指定して実行] をクリックし、「services.msc」と入力)。
7. [OfficeScan Master Service] を右クリックし、[停止] をクリックします。
8. 対象コンピュータ上の <「サーバのインストールフォルダ」>¥PCCSRV フォルダにバックアップファイルをコピーします。これをウイルスバスター Corp. サーバデータベースおよび関連ファイル / フォルダに上書きします。
9. OfficeScan Master Service を再起動します。

ウイルスバスター Corp. サーバのアンインストール

アンインストールプログラムを使用して、ウイルスバスター Corp. サーバおよび統合スマートスキャンサーバをアンインストールします。

アンインストールプログラムで問題が発生した場合には、手動でサーバをアンインストールします。

注意： ウイルスバスター Corp. クライアントのアンインストール手順については、管理者ガイドを参照してください。

アンインストールプログラムを使用してウイルスバスター Corp. サーバをアンインストールするには

1. サーバコンピュータで新規インストールを実行した場合、この手順は省略してください。

   旧バージョンからこのバージョンにサーバをアップグレードした場合：

a. プラグインマネージャが現在インストールされている場合、プラグインマネージャをアンインストールします。

b. プラグインマネージャがインストールされていない場合、HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥OfficeScan¥service¥ の AOS レジストリキーを削除します。

2. アンインストールプログラムを実行します。アンインストールプログラムには、次の 2 種類の方法でアクセスできます。

方法 A

a. ウイルスバスター Corp. サーバコンピュータ上で、[スタート] → [プログラム] → [ウイルスバスター Corp. サーバ] → [ウイルスバスター Corp. のアンインストール] をクリックしてください。確認画面が表示されます。

b. [はい] をクリックします。サーバのアンインストールプログラムでは、管理者パスワードが求められます。

c. 管理者パスワードを入力し、[OK] をクリックします。サーバのアンインストールプログラムがサーバファイルの削除を開始します。確認のメッセージが表示されます。

d. [OK] をクリックしてアンインストールプログラムを閉じます。

方法 B

a. Windows の [プログラムの追加と削除] 画面で、ウイルスバスター Corp. サーバプログラムをダブルクリックします。

b. コントロールパネルの [プログラムの追加と削除] をクリックします。[ウイルスバスター Corp. サーバ] を探してダブルクリックします。管理者パスワードが求められるまで、画面に表示される指示に従います。

c. 管理者パスワードを入力し、[OK] をクリックします。サーバのアンインストールプログラムがサーバファイルの削除を開始します。確認のメッセージが表示されます。

d. [OK] をクリックしてアンインストールプログラムを閉じます。

サーバを手動でアンインストールするには

パート 1: 統合スマートスキャンサーバのアンインストール

1. Microsoft 管理コンソール (MMC) を開き、OfficeScan Master Service を停止します。
2. コマンドプロンプトを開いて、<「サーバのインストールフォルダ」>¥PCCSRV に進みます。
3. 次のコマンドを実行します。

```
SVRSVCSETUP.EXE -uninstall
```

このコマンドによって、ウイルスバスター Corp. 関連のサービスがアンインストールされますが、設定ファイルやウイルスバスター Corp. データベースは削除されません。

4. <「サーバのインストールフォルダ」>¥PCCSRV¥private and open ofcserver.ini に移動します。
5. 次のように設定を変更します。

表 2-4. ofcserver.ini の設定

設定	手順
WSS_INSTALL=1	1 を 0 に変更
WSS_ENABLE=1	この行を削除
WSS_URL=https://< コンピュータ名 >:4345/tmcss/	この行を削除

6. <「サーバのインストールフォルダ」>¥PCCSRV and open OfUninst.ini に移動します。次の行を削除します。
   - IIS Web サーバを使用している場合

     ```
     [WSS_WEB_SERVER]
     ServerPort=8082
     IIS_VhostName=Smart Scan Server (Integrated)
     IIS_VHostIdx=5
     ```

     注意： IIS_VHostidx の値は、次の行の「isapi」の値と同じになる必要があります。

     ROOT=/tmcss,C:¥Program Files¥Trend Micro¥OfficeScan¥PCCSRV¥WSS¥isapi,,< 値 >

     ```
     [WSS_SSL]
     SSLPort=<SSL ポート >
     ```

   - Apache Web サーバを使用している場合

     ```
     [WSS_WEB_SERVER]
     ServerPort=8082
     [WSS_SSL]
     ```

```
SSLPort=<SSL ポート >
```

7. コマンドプロンプトを開いて、<「サーバのインストールフォルダ」>¥PCCSRV に進みます。
8. 次のコマンドを実行します。

```
Svrsvcsetup -install

Svrsvcsetup -enablessl

Svrsvcsetup -setprivilege
```

9. 次の項目が削除されているかどうかを確認します。
   - Microsoft 管理コンソールの Trend Micro Smart Scan Server service
   - スマートスキャンサーバのパフォーマンスカウンタ
   - スマートスキャンサーバの (統合) Web サイト

パート 2: ウイルスバスター Corp. サーバのアンインストール

1. レジストリエディタを開いて、次の手順を実行します。

警告： 次の手順ではレジストリキーの削除が必要です。レジストリキーを正しく変更しないと、システムに重大な問題が生じる可能性があります。常にバックアップコピーを作成してからレジストリキーを変更してください。詳細については、レジストリエディタのヘルプを参照してください。

   a. HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥ に移動します。
   b. ofcservice ハイブが削除されているかどうかを確認します。
   c. HKEY_LOCAL_MACHINE¥SOFTWARE¥Trend Micro¥OfficeScan¥ に移動し、OfficeScan ハイブを削除します。

      64 ビットコンピュータの場合は、このパスが
      HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432node¥
      Trend Micro¥OfficeScan¥ になります。

   d. HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥ に移動し、OfficeScan Management Console-< サーバ名 > フォルダを削除します。
2. <「サーバのインストールフォルダ」>¥PCCSRV フォルダに移動し、PCCSRV フォルダの共有を解除します。
3. サーバコンピュータを再起動します。
4. <「サーバのインストールフォルダ」>¥PCCSRV フォルダに移動し、PCCSRV フォルダを削除します。

5. インターネットインフォメーションサービス (IIS) のコンソールで、ウイルスバスター Corp. の Web サイトを削除します。
   a. IIS コンソールを開きます。
   b. サーバ名を展開します。
   c. ウイルスバスター Corp. を別の Web サイトにイントールしている場合は、[Web サイト] フォルダに進み、ウイルスバスター Corp. を削除します。
   d. ウイルスバスター Corp. の仮想ディレクトリを既定の Web サイトにインストールしている場合は、[既定の Web サイト] フォルダに進み、ウイルスバスター Corp. の仮想ディレクトリを削除します。

第 3 章

サポート情報

この章で説明する内容には、次の項目が含まれます。

トラブルシューティングのリソース

ケース診断ツール

トレンドマイクロのケース診断ツール (CDT) は、問題が発生した場合にお客さまの製品から必要なデバッグ情報を収集します。そして、製品のデバッグステータスをオンまたはオフに自動的に切り替えて、問題のカテゴリに従って必要なファイルを収集します。トレンドマイクロはこの情報を使用して、製品に関連する問題をトラブルシューティングします。

このツールと関連マニュアルの入手については、サポート担当者にお問い合わせください。

インストールログ

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.) が自動的に生成するインストールファイルを、インストールの問題を解決するために使用してください。

表 3-1. インストールログファイル

ログファイル	ファイル名	場所
サーバのローカルインストール / アップグレードログ	OFCMAS.LOG	%windir%
サーバのリモートインストール / アップグレードログ	OFCMAS.LOG (セットアップを起動したコンピュータ上にある) OFCMAS.LOG (対象コンピュータ上にある)	%windir%
クライアントのインストールログ	OFCNT.LOG	MSI パッケージ以外のすべてのインストール方法は %windir% MSI パッケージのインストール方法は %temp%

サーバのデバッグログ

次のサーバタスクを実行する前にデバッグログを有効にすることができます。

- サーバをアンインストールして、再度インストールします。

- ウイルスバスター Corp. を最新バージョンにアップグレードします。
- リモートインストール / アップグレードを実行します (デバッグログは、リモートコンピュータではなく、セットアップを開始したコンピュータで有効です)。

警告： デバッグログはサーバの性能に影響を与え、大量のディスク空き容量を消費する可能性があります。必要な時にのみデバッグログ生成を有効にし、デバッグデータが不要になった場合はただちに無効にしてください。ファイルサイズが巨大になった場合はログファイルを削除してください。

ウイルスバスター Corp. サーバのデバッグログを有効にするには

1. < サーバのインストールフォルダ >¥PCCSRV¥Private にある LogServer フォルダを C:¥ へコピーします。
2. ofcdebug.ini という名前で、次のコンテンツを含むファイルを作成してください。

   [debug]

   DebugLevel=9

   DebugLog=C:¥LogServer¥ofcdebug.log

   debugLevel_new=D

   debugSplitSize=10485760

   debugSplitPeriod=12

   debugRemoveAfterSplit=1
3. ofcdebug.ini を C:¥LogServer へ保存します。
4. 適切なタスクを実行します (サーバのアンインストール / 再インストール、新しいサーババージョンへのアップグレード、またはリモートでのインストール / アップグレード)。
5. C:¥LogServer で ofcdebug.log を確認します。

クライアントのデバッグログ

ウイルスバスター Corp. クライアントをインストールする前に、デバッグログを有効にすることもできます。

警告： デバッグログはクライアントの性能に影響を与え、大量のディスク空き容量を消費する可能性があります。必要な時にのみデバッグログを有効にし、デバッグデータが不要になった場合はただちに無効にしてください。ファイルサイズが巨大になった場合はログファイルを削除してください。

ウイルスバスター Corp. クライアントコンピュータのデバッグログを有効にするには

1. ofcdebug.ini という名前で、次のコンテンツを含むファイルを作成してください。

   [Debug]
   Debuglog=C:¥ofcdebug.log
   debuglevel=9
   debugLevel_new=D
   debugSplitSize=10485760
   debugSplitPeriod=12
   debugRemoveAfterSplit=1

2. ofcdebug.ini ファイルをクライアントに送信し、C:¥ フォルダ内に保存するように指示してください。LogServer.exe ファイルは、クライアントのコンピュータが起動するたびに自動的に起動します。コンピュータの起動時に LogServer.exe コマンドウィンドウが開き、ウイルスバスター Corp. に対してデバッグログ生成の中止を要求しますが、ユーザに対してこのウィンドウを閉じないように指示してください。ユーザがコマンドウィンドウを閉じた場合には、¥OfficeScan クライアント内にある LogServer.exe を起動すると再度デバッグログ生成を開始できます。
3. それぞれのクライアントコンピュータに対し、C:¥ 内の ofcdebug.log を確認します。
4. ウイルスバスター Corp. クライアントのデバッグログを無効にするには、ofcdebug.ini ファイルを削除してください。

製品サポート情報

ウイルスバスター Corp. のユーザ登録により、さまざまなサポートサービスを受けることができます。

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

サポートサービスについて

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

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

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

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

製品 Q&A のご案内

ウイルスバスター Corp.10 に関するよくあるお問い合わせを、以下の製品 Q&A にまとめています。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ので、ぜひご活用ください。

http://esupport.trendmicro.co.jp/Pages/JP-2074993.aspx

セキュリティ情報

セキュリティ情報の入手先

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

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

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

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

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

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

トレンドマイクロへのウイルス解析依頼

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

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

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

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

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

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

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

ウイルス解析サポートセンター「TrendLabs」

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

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

付録 A

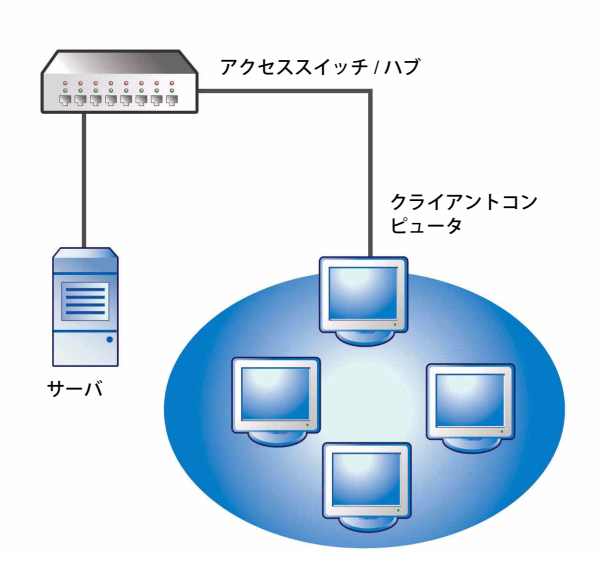
サンプル配信

このセクションでは、ネットワークトポロジおよび使用可能なネットワークリソースに基づいた、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.) の最良の配信方法を説明します。組織内でウイルスバスター Corp. の配信を計画する際のリファレンスとしてお使いいただけます。

基本的なネットワーク

図 A-1. はウイルスバスター Corp. サーバとクライアントが直接接続されている、基本的なネットワークについて説明しています。多くのビジネスネットワークは、LAN (または WAN) の接続速度が、10Mbps、100Mbps、1Gbps のエリアでこの設定を行っています。このシナリオでは、ウイルスバスター Corp. システム要件を満たし、十分なリソースを持つコンピュータが、ウイルスバスター Corp. サーバのインストール対象となる第一候補のコンピュータとなります。

図 A-1.　基本的なネットワークトポロジ



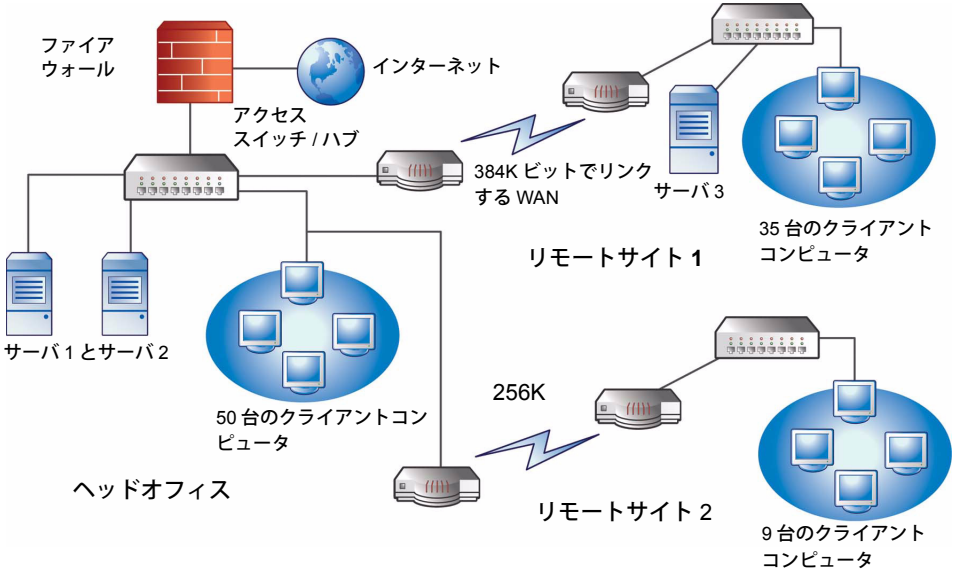
複数サイトのネットワーク

異なる帯域幅で複数のアクセスポイントや複数のリモートサイトを持つネットワークについては、次の検討を行ってください。

- オフィスやネットワーク帯域幅の見地から統合地点を分析します。
- オフィスごとに現在の帯域幅を利用するか判断します。

これにより、ウイルスバスター Corp. の最良の配信方法が明確になってきます。図 A-2. は複数サイトのネットワークトポロジを説明しています。

図 A-2.　複数サイトのネットワークトポロジ



ネットワーク情報 :

- リモートサイト 1 WAN リンクはビジネスアワーで平均約 70％の利用。このサイトには 35 台のクライアントコンピュータがあります。
- リモートサイト 2 WAN リンクはビジネスアワーで平均約 40％の利用。このサイトには 9 台のクライアントコンピュータがあります。
- サーバ 3 はリモートサイト 1 のグループでファイルサーバおよびプリントサーバとしてのみ使用されています。このコンピュータはウイルスバスター Corp. サーバのインストール先候補になる可能性はありますが、特別な管理には適さないかもしれません。サーバはすべて Windows 2000 を起動しています。ネットワークでは Active Directory を使用していますが、主にネットワーク認証に使用しています。
- ヘッドオフィス、リモートサイト 1、リモートサイト 2 のクライアントコンピュータは、すべて Windows 2000 または Windows XP を起動しています。

タスク :

1. ウイルスバスター Corp. サーバをインストールするコンピュータを判別します。インストールの手順については 44 ページの「ウイルスバスター Corp. サーバの新規インストールの実行」を参照してください。
2. クライアントの使用可能なインストール方法を判別し、要件を満たさない方法は除外してください。クライアントのインストール方法の詳細については、管理者ガイドを参照してください。

   使用可能なインストール方法

   - ログオンスクリプトセットアップ

     ローカルトラフィックに問題がないため WAN を設置していない場合は、ログオンスクリプトセットアップを使用するとよいでしょう。ただし、各コンピュー タに 50MB 以上のデータを転送する場合は、この選択は実行できません。

   - Web コンソールからのリモートインストール

     この方法はヘッドオフィスで LAN 接続されているすべてのコンピュータに有効です。これらのコンピュータはすべて Windows 2000 を起動しているため、コンピュータへのパッケージ配信は簡単です。

     この 2 つのリモートサイトは低速でリンクされているため、ビジネスアワーにウイルスバスター Corp. 配信する場合は、使用可能な帯域幅に影響を与えるおそれがあります。大半の人が働いていないビジネスアワー以外の時間であれば、全部のリンク容量を使用してウイルスバスター Corp. を配信できます。ただし、ユーザがコンピュータの電源を切っていると、これらのコンピュータへのウイルスバスター Corp. 配信は正常に行われません。

   - クライアントパッケージの配信

     リモートサイトへの配信については、クライアントパッケージ配信が最良の選択と思われます。ただし、リモートサイト 2 ではこの選択を正しく簡単に実行できるローカルサーバがありません。すべての選択を詳しく見てみると、この選択が大半のコンピュータに最良な方法です。

ヘッドオフィスの配信

ヘッドオフィスで実行するのに最も簡単なクライアント配信方法は、ウイルスバスター Corp. Web コンソールからのリモートインストールです。手順については、管理者ガイドを参照してください。

リモートサイト 1 の配信

リモートサイト 1 への配信には、Microsoft の分散ファイルシステム (DFS) の設定が必要です。DFS の詳細については、http://support.microsoft.com/?kbid=241452 を参照してください。DFS の設定後に、リモートサイト 1 のサーバ 3 は、既存の DFS 環境を複製するか、新しい環境を作成して DFS を有効にする必要があります。

配信方法として適しているのは、Microsoft Installer Package (MSI) 形式で作成したクライアントパッケージを DFS 共有に配信する方法です。手順については、管理者ガイドを参照してください。そのクライアントパッケージは、予約アップデート時にサーバ 3 に複製されるため、クライアントパッケージ配信の帯域幅への影響は最小限に抑えられます。

クライアントパッケージは Active Directory の機能を利用して配信することもできます。詳細については、管理者ガイドを参照してください。

コンポーネントアップデートが WAN に与える影響を最小限に抑える場合:

1. リモートサイト 1 のアップデートエージェントとして機能するクライアントを指定します。
   a. Web コンソールを開き、[ネットワーク上のコンピュータ] → [クライアント管理] の順に選択します。
   b. クライアントツリーで、アップデートエージェントとして機能するクライアントを選択し、[設定] → [アップデートエージェント設定] の順にクリックします。
2. リモートサイト 1 のクライアントで、アップデートエージェントからコンポーネントをアップデートするものを選択します。
   a. [アップデート] → [ネットワーク上のコンピュータ] → [アップデート元] と選択していきます。
   b. [ユーザ指定アップデート元] を選択して、[追加] をクリックします。
   c. 表示される画面で、リモートサイト 1 のクライアントコンピュータの IP アドレスの範囲を入力します。
   d. [アップデート元] をオンにし、ドロップダウンリストから指定されたアップデートエージェントを選択してください。

リモートサイト 2 の配信

リモートサイト 2 の重要な問題は帯域幅の低さです。しかし、ビジネスアワーでは帯域幅の 60%が空いています。帯域幅を 40%利用しているビジネスアワーでは、約 154K ビットの帯域幅が使用可能です。

ウイルスバスター Corp. クライアントをインストールする最良の方法は、リモートサイト 1 で使用したものと同じ MSI フォーマットのクライアントパッケージを使用することです。ただし使用できるサーバがないため、分散ファイルシステム (DFS) は使用できません。

ひとつの選択として他社製の管理ツールを使う方法がありますが、これにより管理者は物理的にアクセスせずに、リモートコンピュータ上の共有ディレクトリを設定または作成することができます。この共有ディレクトリを 1 台のコンピュータで作成した後に、クライアントパッケージを共有ディレクトリにコピーすれば、クライアントを 9 台のコンピュータにインストールするよりも経費が抑えられます。

別の Active Directory ポリシーを使用することもできますが、再度、ソースとして DFS 共有は指定しません。

これらの方法は、インストールトラフィックをローカルネットワーク内に保持し、WAN に与えるトラフィックを最小限に抑えています。

コンポーネントアップデートが WAN に与える影響を最小限に抑えるため、アップデートエージェントとして機能するクライアントを指定することができます。詳細については、117 ページの「リモートサイト 1 の配信」を参照してください。

付録 B

以前のトレンドマイクロ ウイルスバスター コーポレートエディションの機能

このセクションでは、トレンドマイクロ 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.) の以前のバージョンに存在した機能で、このバージョンでは使用できないものについて説明します。

表 B-1. 以前のウイルスバスター Corp. の機能

機能	使用可否		ウイルスバスター Corp. 10 での状況
	「8.x」	「7.x」	
Trend Micro OfficeScan for Wireless	不可	可	Trend Micro OfficeScan for Wireless は、プラグインプログラムの Trend Micro ウイルスバスター モバイルセキュリティに置き換えられています。
PDA Protection Manager	不可	可	PDA Protection Manager は、プラグインプログラムの Trend Micro ウイルスバスター モバイルセキュリティに置き換えられています。
DCS 検索 (クライアント起動)	不可	可	DCS 検索は、検索時に自動的に実行されます。

表 B-1. 以前のウイルスバスター Corp. の機能（続き）

機能	使用可否		ウイルスバスター Corp. 10 での状況
	「8.x」	「7.x」	
DCS クリーンナップ (サーバ起動)	不可	可	DCS クリーンナップは、検索時に自動的に実行されます。
予約駆除 (グローバルクライアント設定)	不可	可	予約駆除は、検索時に自動的に実行されます。
ウイルスアウトブレークモニタ	不可	可	ウイルスアウトブレークモニタ設定は、[通知] → [管理者通知] → [アウトブレーク通知] → [共有フォルダセッション] で指定します。
ファイアウォールアウトブレークモニタ	不可	可	ファイアウォールアウトブレークモニタ設定は、[通知] → [管理者通知] → [アウトブレーク通知] → [ファイアウォール侵害] で指定します。
ウイルスバスター Corp. 監視サービス	可	可	ウイルスバスター Corp. 監視サービス機能 (ウイルスバスター Corp. クライアントサービスが予定外に停止した場合に再起動します) は、ウイルスバスター Corp. クライアントで実行されます。サービスの再起動設定は、Web コンソールの [グローバルクライアント設定] 画面で指定します。

索引

英数字

あ

か

さ

た

な

は

や

ら