TREND MICRO

ウイルスバスター™ ビジネスセキュリティ 10.0

Service Pack 1

インストールガイド

Protected Cloud

Web Security

※注意事項

複数年契約について

・お客さまが複数年契約（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。

https://esupport.trendmicro.com/ja-jp/support-lifecycle/end-of-support/default.aspx

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDI オプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポートプレミアム、Air サポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、および Securing Your Connected World は、トレンドマイクロ株式会社の登録商標です。

本ドキュメント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。

P/N: WFEM108678_190617_JP (2019/08)

目次

はじめに

第 1 章：インストールとアップグレードの準備

第 2 章：ビジネスセキュリティサーバのインストール

索引

はじめに

『ウイルスバスター ビジネスセキュリティインストールガイド』にようこそ。このドキュメントでは、ウイルスバスター ビジネスセキュリティ (以下、ビジネスセキュリティ) の操作を実行するための要件と手順について説明します。

- ビジネスセキュリティサーバのインストール
- ビジネスセキュリティサーバおよびエージェントのアップグレード

エージェントのインストールの詳細については、管理者ガイドを参照してください。

ビジネスセキュリティのドキュメント

ビジネスセキュリティのドキュメントには次のものがあります。

表 1. ビジネスセキュリティのドキュメント

ドキュメント	説明
インストールガイド	ビジネスセキュリティサーバのインストール要件と手順、およびサーバとエージェントのアップグレード要件と手順について説明しているドキュメントです (PDF または冊子)。
管理者ガイド	使用開始にあたっての情報、エージェントのインストール手順、およびビジネスセキュリティサーバとエージェントの管理について説明しているドキュメントです (PDF)。
ヘルプ	WebHelp (HTML ファイル) で、「使用方法」、使用に関するアドバイス、およびフィールド固有の情報を提供します。
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。ヘルプや印刷されたドキュメントには記載されていない最新の製品情報が含まれている場合もあります。
製品 Q&A	問題の解決策およびトラブルシューティング情報を提供するオンラインデータベースです。製品の既知の問題に関する最新情報を参照できます。製品 Q&A には、次の Web サイトからアクセスできます。 http://tmqa.jp/biz

最新版の PDF ドキュメントと Readme は次のサイトからダウンロードできます。

http://tmqa.jp/biz10_dlcenter

対象読者

ビジネスセキュリティのドキュメントは、次のユーザを対象としています。

- セキュリティ 管理者: ビジネスセキュリティサーバおよびエージェントのインストールと管理をはじめ、ビジネスセキュリティの管理責任を持つユーザ。 これらのユーザには、ネットワークとサーバ管理に関する高度な知識を備えていることが求められます。

- エンドユーザ: コンピュータにセキュリティエージェントがインストールされているユーザ。個々のコンピュータスキルのレベルは初心者から上級者まで広範にわたります。

ドキュメントの表記規則

情報を簡単に見つけ理解できるように、ビジネスセキュリティ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	設定に関する注意事項または推奨事項を示します。
 ヒント	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を示します。
 警告!	ネットワーク上のコンピュータに害を及ぼす可能性のあるアクティビティについて警告を示します。

第 1 章

インストールとアップグレードの準備

この章では、ウイルスバスター™ ビジネスセキュリティのインストールとアップグレードの前に必要な準備について説明します。

製品の概要とサポートされる機能

ウイルスバスター ビジネスセキュリティの概要は次のとおりです。

- ローカルネットワーク上のエンドポイント (デスクトップ、ポータブル、およびサーバ) を保護するように設計されています。以下の機能が含まれるほか、テクニカルサポート、不正プログラム/ウイルスのパターンファイルのダウンロード、リアルタイム検索、および 1 年間のプログラムのアップデートが付属します。

サポートされる機能は次のとおりです。

- コンポーネントのアップデート
- デバイスコントロール
- ウイルス/スパイウェア対策
- ファイアウォール
- Web レピュテーション
- URL フィルタ
- 機械学習型検索
- 挙動監視
- ユーザツール
- POP3 メール検索
- スパムメール対策 (POP3)

ウイルスバスター ビジネスセキュリティの登録

詳細については、付属の「製品サポートガイド」をご覧ください。

ビジネスセキュリティネットワーク

ビジネスセキュリティは次のコンポーネントで構成されます。

- 15 ページの「ビジネスセキュリティサーバ」
- 17 ページの「エージェント」
- 17 ページの「Web コンソール」

ビジネスセキュリティサーバ

ビジネスセキュリティの中核になるのはビジネスセキュリティサーバです。ビジネスセキュリティサーバは Web コンソールをホストします。この Web コンソールは、ビジネスセキュリティを集中管理する Web ベースのコンソールです。ビジネスセキュリティサーバは、エージェントをネットワーク上のクライアントにインストールし、エージェント/サーバの関係を形成します。ビジネスセキュリティサーバでは、セキュリティステータス情報の表示、エージェントの表示、システムセキュリティの設定、およびコンポーネントのダウンロードを集中管理できます。ビジネスセキュリティサーバにはデータベースも配置されており、エージェントから報告されたインターネット脅威の検出ログがこのデータベースに格納されます。

ビジネスセキュリティサーバには次の重要な機能があります。

- コンピュータにエージェントをインストールし、監視および管理します。
- エージェントが必要とするコンポーネントをダウンロードします。ビジネスセキュリティサーバは、初期設定で、トレンドマイクロのアップデートサーバからコンポーネントをダウンロードしてエージェントに配信します。

スキャンサーバ

ビジネスセキュリティサーバにはスキャンサーバと呼ばれるサービスがあり、ビジネスセキュリティサーバのインストール時に自動的にインストールされます。このため、別途インストールする必要はありません。スキャンサーバは、`iCRCService.exe` という名前のプロセスで実行され、Microsoft 管理コンソールには Trend Micro Smart Scan Service と表示されます。

セキュリティエージェントがスマートスキャンという検索方法を使用しているとき、スキャンサーバが、このエージェントで検索をより効率良く実行できるように支援します。スマートスキャンプロセスの説明を次に示します。

- セキュリティエージェントは、従来のウイルスパターンファイルの軽量版であるスマートスキャンエージェントパターンファイルを使用してクライアントでセキュリティ上の脅威を検索します。スマートスキャンエージェントパターンファイルには、ウイルスパターンファイルにある脅威のシグネチャのほとんどが含まれています。

- 検索時にファイルのリスクを特定できない場合、セキュリティエージェントはスキャンサーバに検索クエリを送信して、リスクを検証します。スキャンサーバは、スマートスキャンパターンファイルを使用してリスクを検証します。このパターンファイルにはスマートスキャンエージェントパターンファイルにない脅威のシグネチャが含まれています。

- セキュリティエージェントは、検索のパフォーマンスを向上するために、スキャンサーバにより提供される検索クエリの結果を「キャッシュ」します。

スキャンサーバは、脅威の定義の一部を保持することで、セキュリティエージェントでのコンポーネントのダウンロードによる帯域幅の消費を削減します。ウイルスパターンファイルをダウンロードする代わりに、セキュリティエージェントでは、大幅にサイズが削減されたスマートスキャンエージェントパターンファイルをダウンロードします。

セキュリティエージェントがスキャンサーバに接続できない場合、スキャンサーバと同じ機能を持つ Trend Micro Smart Protection Network に検索クエリを送信します。

ビジネスセキュリティサーバからスキャンサーバを個別にアンインストールすることはできません。スキャンサーバを使用する必要がない場合は、次の手順を実行します。

1. ビジネスセキュリティサーバコンピュータで、Microsoft 管理コンソールを開き、Trend Micro Smart Scan Service を無効にします。

2. Web コンソールで、[管理] > [グローバル設定] > [デスクトップ/サーバ] タブに移動し、[スマートスキャンサービスを無効にする] オプションを選択して、セキュリティエージェントを従来型スキャンに切り替えます。

エージェント

エージェントはセキュリティ上の脅威からクライアントを保護します。クライアントには、デスクトップおよびサーバが含まれます。ビジネスセキュリティエージェントは次のとおりです。

表 1-1. ビジネスセキュリティエージェント

エージェント	説明
セキュリティエージェント	デスクトップとサーバをセキュリティ上の脅威および侵入から保護します。

エージェントはレポートを作成し、そのエージェントのインストール元となるビジネスセキュリティサーバにレポートを送信します。エージェントは、イベントのステータス情報をリアルタイムでビジネスセキュリティサーバに送信し、最新のクライアント情報を提供します。エージェントがレポートするイベントは、脅威の検出、起動、停止、検索の開始、アップデートの完了などです。

Web コンソール

Web コンソールは、企業ネットワーク全体におけるセキュリティエージェント監視の中枢です。このコンソールの初期設定と初期値は、セキュリティ要件や仕様に応じて変更できます。Web コンソールでは、Java、CGI、HTML、HTTP などの標準的なインターネット技術が使用されています。

Web コンソールを使用して、次のタスクを実行できます。

- セキュリティエージェントをエンドポイントにインストールする。
- 同時設定や同時管理を目的として、エージェントを論理グループ化する。
- エンドポイントに対してウイルス検索およびスパイウェア検索を設定し、手動検索を開始する。
- 脅威に関連した活動についての通知を受信したり、ログレポートを表示したりする。

- エンドポイントで脅威が検出された場合は、通知を受信し、メールメッセージ、SNMP トラップ、または Windows イベントログを介してウイルス大規模感染の警告を送信する。

第 2 章

ビジネスセキュリティサーバのインストール

この章では、ビジネスセキュリティサーバをインストールするために必要な情報について説明します。

インストールとアップグレードの要件

システム要件については、次の Web サイトを参照してください。

https://www.trendmicro.com/ja_jp/small-business/worry-free-standard.html#requirement

ビジネスセキュリティサーバのインストールに関して考慮すべき事項

ビジネスセキュリティサーバをインストールするときは、次の点について考慮してください。

- 20 ページの「ビジネスセキュリティサーバの IPv6 の要件」
- 21 ページの「ビジネスセキュリティサーバの配置場所」
- 22 ページの「クライアントの数」
- 22 ページの「ネットワークトラフィック」
- 24 ページの「専用サーバ」
- 24 ページの「互換性の問題」

ビジネスセキュリティサーバの IPv6 の要件

ビジネスセキュリティサーバの IPv6 の要件は次のとおりです。

- IPv4 エージェントと IPv6 エージェントを管理する場合は、サーバに IPv4 アドレスと IPv6 アドレスの両方を指定して、サーバをホスト名で識別する必要があります。サーバが IPv4 アドレスで識別されている場合、IPv6 シングルスタックエージェントはサーバに接続できません。IPv4 シングルスタッククライアントが IPv6 アドレスで識別されているサーバに接続する場合にも、同様の問題が発生します。
- サーバが IPv6 エージェントのみを管理する場合は、IPv6 アドレスを使用することが最低要件となります。サーバはホスト名または IPv6 アドレス

で識別できます。サーバがホスト名で識別されている場合は、完全修飾ドメイン名 (FQDN) を使用することをお勧めします。これは、IPv6 シングルスタック環境では、WINS サーバがホスト名を対応する IPv6 アドレスに変換できないためです。

- `ping` や `nslookup` コマンドなどを使用して、ホストマシンの IPv6 または IPv4 アドレスを取得できることを確認します。
- ビジネスセキュリティサーバを IPv6 シングルスタックコンピュータにインストールする場合は、IPv4 アドレスと IPv6 アドレスを変換できる DeleGate などのデュアルスタックプロキシサーバを設定します。プロキシサーバをビジネスセキュリティサーバとインターネットの間に設置して、トレンドマイクロがホストするサービス (たとえばアップデートサーバ、オンライン登録 Web サイト、Trend Micro Smart Protection Network など) にサーバが正常に接続できるようにします。

ビジネスセキュリティサーバの配置場所

ビジネスセキュリティは、さまざまなネットワーク環境に適合できます。たとえば、ファイアウォールをビジネスセキュリティサーバとセキュリティエージェントをインストールしたクライアントの間に配置することも、単一のネットワークファイアウォールの裏側にビジネスセキュリティサーバとすべてのクライアントを配置することもできます。

複数のネットワーク環境を管理している場合は、ビジネスセキュリティサーバをメインのネットワーク環境と管理対象の各ネットワーク環境に配置して、その間の帯域幅使用率を削減したり、パターンファイルの配信率の上昇を加速させることをお勧めします。

クライアントで Windows ファイアウォールが有効な場合、ビジネスセキュリティは Windows ファイアウォールを除外リストに自動的に追加します。

注意

ファイアウォールをビジネスセキュリティサーバとクライアントの間に配置する場合は、クライアントの待機ポートとビジネスセキュリティサーバの待機ポートの間のトラフィックを許可するようにファイアウォールを設定する必要があります。

クライアントの数

クライアントとは、セキュリティエージェントをインストールしているコンピュータを指します。デスクトップ、サーバ、ポータブルコンピュータなどがあり、在宅勤務をするユーザに属するものが含まれます。

単一のビジネスセキュリティサーバでは、最大で 2,500 台のクライアントを管理できます。それより多くのクライアントがある場合は、ビジネスセキュリティサーバがインストールされたコンピュータを複数台用意することをお勧めします。

ネットワークトラフィック

ビジネスセキュリティでは、ビジネスセキュリティサーバとエージェントが相互に通信するときに、ネットワークトラフィックが発生します。

ビジネスセキュリティサーバ/スキャンサーバでは、次のときにトラフィックが発生します。

- 設定の変更をエージェントに通知するとき
- アップデートされたコンポーネントをダウンロードするようにエージェントに通知するとき
- アップデートされたコンポーネントを確認およびダウンロードするためにトレンドマイクロのアップデートサーバに接続するとき
- スマートスキャンを使用するエージェントから受診した検索クエリに応答するとき
- Trend Micro Smart Protection Network にフィードバックを送信するとき

エージェントでは、次のときにトラフィックが発生します。

- 起動するとき
- 停止するとき
- ログを生成するとき
- 予約アップデートを実行するとき

- 手動アップデート ([今すぐアップデート]) を実行するとき
- 検索クエリでスキャンサーバに接続するとき

注意

その他すべての処理でも少量のトラフィックが発生します。

コンポーネントのアップデート中のネットワークトラフィック

ビジネスセキュリティサーバでは、コンポーネントをアップデートするときに大量のネットワークトラフィックが発生します。コンポーネントのアップデート中に発生するネットワークトラフィックを減らすため、ビジネスセキュリティサーバはコンポーネントの複製を実行します。ビジネスセキュリティサーバは、アップデートされた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なバージョン) のみをダウンロードして、ダウンロード後に古いパターンファイルとマージします。

定期的にアップデートされるビジネスセキュリティサーバは、差分パターンファイルのみをダウンロードします。それ以外の場合、フルパターンファイルをダウンロードします。

トレンドマイクロでは、新しいパターンファイルを定期的にリリースしています。また、有害で感染が拡大しているウイルス/不正プログラムが確認された場合にも迅速にリリースしています。

ネットワーク帯域幅を削減するためにアップデートエージェントを使用する

セキュリティエージェントとビジネスセキュリティサーバ間のネットワークで「帯域幅が狭い」または「トラフィックが大きい」部分を確認した場合、特定のセキュリティエージェントをその他のエージェントのアップデート元 (アップデートエージェント) として機能するように設定できます。これにより、すべてのエージェントにコンポーネントを配信する際の負荷を分散できます。

たとえば、ネットワークを場所ごとにセグメント化している場合で、セグメント間のネットワークのトラフィック負荷が大きい場合に、セグメントごとに 1 つ以上のセキュリティエージェントがアップデートエージェントとして機能するよう設定することをお勧めします。

専用サーバ

ビジネスセキュリティサーバをインストールするクライアントを選択するときは、次の点を考慮してください。

- クライアントの CPU 処理量
- クライアントで他の機能が実行されるかどうか

対象クライアントで他の機能が実行される場合は、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を実行していない別のクライアントを選択してください。

互換性の問題

このセクションでは、特定のサードパーティアプリケーションで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。ビジネスセキュリティサーバおよびその他のビジネスセキュリティのコンポーネントをインストールする際、同じコンピュータにインストールされているすべてのサードパーティアプリケーションのドキュメントを必ず参照してください。

他のエンドポイントセキュリティソフトウェア

ビジネスセキュリティサーバをインストールする前に、対象コンピュータから他のエンドポイントセキュリティソフトウェアをアンインストールしておくをお勧めします。アンインストールが実施されていない場合、インストールがブロックされたり、インストール後にビジネスセキュリティサーバのパフォーマンスが影響を受けたりする可能性があります。

Windows SBS および EBS 2008 でのセキュリティアプリケーション

ビジネスセキュリティは、Windows Small Business Server (SBS) 2008 と Windows Essential Business Server (EBS) 2008 の両方と互換性があります。ただし、セキュリティアプリケーションがこれらの OS にインストールされていたりこれらの OS で管理されていたりすると、その一部がビジネスセキュリティと競合する場合があります。このため、そのようなセキュリティアプリケーションの削除が必要になることがあります。

セキュリティエージェントと Windows Defender

セキュリティエージェントをインストールすると、Windows Defender が無効になります。

データベースへの脅威検索

データベースに対して脅威の検索を実施する際、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が低下する可能性があります。データベースおよびそのバックアップフォルダをリアルタイム検索から除外することをお勧めします。データベースを検索する必要がある場合は、影響を最小限に抑えるため、ピーク外の時間帯に手動検索を実行するか検索を予約してください。

他のファイアウォールアプリケーション

ビジネスセキュリティのファイアウォールをインストールする前に、次のような他のファイアウォールアプリケーションを削除するか無効にすることをお勧めします。

- Windows インターネット接続ファイアウォール (ICF)
- Windows ファイアウォール (WF)

ただし、ICF や他のサードパーティのファイアウォールを実行する場合は、ビジネスセキュリティサーバの待機ポートをファイアウォール除外リストに追加してください (待機ポートについては 25 ページの「ビジネスセキュリティのポート」、除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)。

ビジネスセキュリティのポート

ビジネスセキュリティは次のポートを使用します。

- サーバ待機ポート (HTTP ポート): ビジネスセキュリティサーバにアクセスするために使用します。初期設定では、ビジネスセキュリティは次のいずれかを使用します。
  - IIS サーバの初期設定 Web サイト: HTTP サーバの TCP ポートと同じポート番号

- IIS サーバの仮想 Web サイト: 8059
- Apache サーバ: 8059

- クライアント待機ポート: セキュリティエージェントがビジネスセキュリティサーバからコマンドを受信する際に使用します。ランダムに生成されたポート番号です。

  待機ポートは、インストール中にのみ変更できます。

警告!

現在のサイバー犯罪者は、HTTP を使用してポート 80 や 8080 を攻撃します。ほとんどの組織で、このポートが HTTP 通信用の初期設定の TCP (Transmission Control Protocol) ポートとして一般的に使用されているためです。組織でこれらのポートのいずれかを HTTP ポートとして現在使用している場合は、別のポート番号を使用することをお勧めします。

注意

スキャンサーバに接続するためにセキュリティエージェントが使用しているポートを調べるには、サーバがインストールされているフォルダにある SSCFG.ini を開きます。

- スキャンサーバポート: スキャンサーバが、検索クエリに関してセキュリティエージェントと通信するために使用します。

表 2-1. スキャンサーバポート

ポートの種類	IIS の既定	IIS 仮想	事前インストール済みの APACHE	APACHE の新規インストール
非 SSL ポート	Web サーバの非 SSL ポート	8082～65536 の範囲の最初の開いているポート	Web サーバの非 SSL ポート	Web サーバの非 SSL ポート
SSL ポート SSL を使用	Web サーバの SSL ポート	4345～65536 の範囲の最初の開いているポート	なし	Web サーバの SSL ポート

ポートの種類	IIS の既定	IIS 仮想	事前インストール済みの APACHE	APACHE の新規インストール
SSL ポート SSL を使用しない	4345～65536 の範囲の最初の開いているポート	4345～65536 の範囲の最初の開いているポート	なし	4345～65536 の範囲の最初の開いているポート

- Trend Micro Security (for Mac) 通信ポート: Trend Micro Security (for Mac) サーバが、Mac クライアントと通信するために使用します。初期設定はポート 61617 です。
- SMTP ポート: ビジネスセキュリティサーバが、管理者にレポートと通知をメールで送信するために使用します。初期設定はポート 25 です。
- プロキシポート: プロキシサーバ経由の接続に使用します。

インストールチェックリスト

ビジネスセキュリティサーバのインストール時に、次の情報が求められます。

表 2-2. インストールチェックリスト

情報	初期設定値	使用する値
ビジネスセキュリティサーバ (スキャンサーバを含む)		
アクティベーションコード	トレンドマイクロが提供	
インストールパス	次のいずれか (OS によって異なる): • C:\Program Files \TrendMicro\Security Server • C:\Program Files (x86)\Trend Micro \Security Server	

情報	初期設定値	使用する値
スキャンサーバデータベースパス	ビジネスセキュリティサーバのインストールパスと同じ (カスタマイズ可能)	
IPv4/IPv6 アドレス	ユーザ指定	
完全修飾ドメイン名 (FQDN)	ユーザ指定	
NetBIOS (ホスト) 名	ユーザ指定	
Web サーバ	いずれかを選択: • Apache • IIS (既定 Web サイト) • IIS (仮想 Web サイト)	
待機ポート (HTTP)	8059	
待機ポート (HTTPS)	4343	
Web コンソールパスワード	ユーザ指定	
セキュリティエージェントのアンインストール/アンロードパスワード	ユーザ指定	
(オプション) メールで送信されるビジネスセキュリティサーバのレポートおよび通知の SMTP 設定		
IPv4/IPv6 アドレス	ユーザ指定	
完全修飾ドメイン名 (FQDN)	ユーザ指定	
NetBIOS (ホスト) 名	ユーザ指定	
ポート	25	
受信者	ユーザ指定	

情報	初期設定値	使用する値
(オプション) トレンドマイクロがホストするサービスに対するビジネスセキュリティサーバ接続のプロキシ設定		
IPv4/IPv6 アドレス	ユーザ指定	
完全修飾ドメイン名 (FQDN)	ユーザ指定	
NetBIOS (ホスト) 名	ユーザ指定	
認証ユーザ名	ユーザ指定	
認証パスワード	ユーザ指定	
セキュリティエージェント		
待機ポート	インストールプログラムがランダムに生成	
インストールパス	次のいずれか (OS によって異なる): • C:\Program Files \TrendMicro\Security Agent • C:\Program Files (x86)\Trend Micro \Security Agent	
(オプション) セキュリティエージェント機能のプロキシ認証 (挙動監視、Web レピュテーション、およびスマートスキャン) **注意** セキュリティエージェントは、Internet Explorer で設定されたプロキシ設定を使用します。		
認証ユーザ名	ユーザ指定	

情報	初期設定値	使用する値
認証パスワード	ユーザ指定	

ビジネスセキュリティサーバのインストール

ビジネスセキュリティサーバのインストールには、次のフェーズがあります。

フェーズ	主なタスク

フェーズ 1: ビジネスセキュリティサーバのインストールを開始する	• インストール前のガイドラインを読みます。
	• インストールパッケージを実行します。
	• 使用許諾契約の条件に同意します。
	• セットアップの種類を選択します。
	  • 標準 (推奨)
	  • 最小
	  • カスタム
	• アクティベーションコードを指定します。

フェーズ	主なタスク
フェーズ 2: 選択したセットアップの種類に応じて設定する	標準または最小インストールの場合は、次のような基本設定を設定します。 • ビジネスセキュリティサーバのインストール場所 • 管理者アカウントパスワード • SMTP サーバ設定と通知の受信者 • Trend Micro Smart Protection Network

	カスタムインストールの場合は、次のようなカスタマイズ可能な設定を設定します
	• 基本設定
	  • ビジネスセキュリティサーバのインストール場所
	  • スマートスキャンサーバデータベースの場所
	  • セキュリティエージェントをビジネスセキュリティサーバと同じコンピュータにインストールするか
	• ビジネスセキュリティサーバの設定
	  • Web サーバ
	  • 管理者アカウントパスワード
	  • SMTP サーバ設定と通知の受信者
	  • Trend Micro Smart Protection Network
	  • 一般プロキシ設定
	• セキュリティエージェントの設定
	  • セキュリティエージェントインストールパス
	  • 有効にするセキュリティエージェント機能
	  • 追加サービスのためのプロキシ設定

フェーズ 3: インストールプロセス	インストールが終了するまで待ち、セットアップを閉じます。

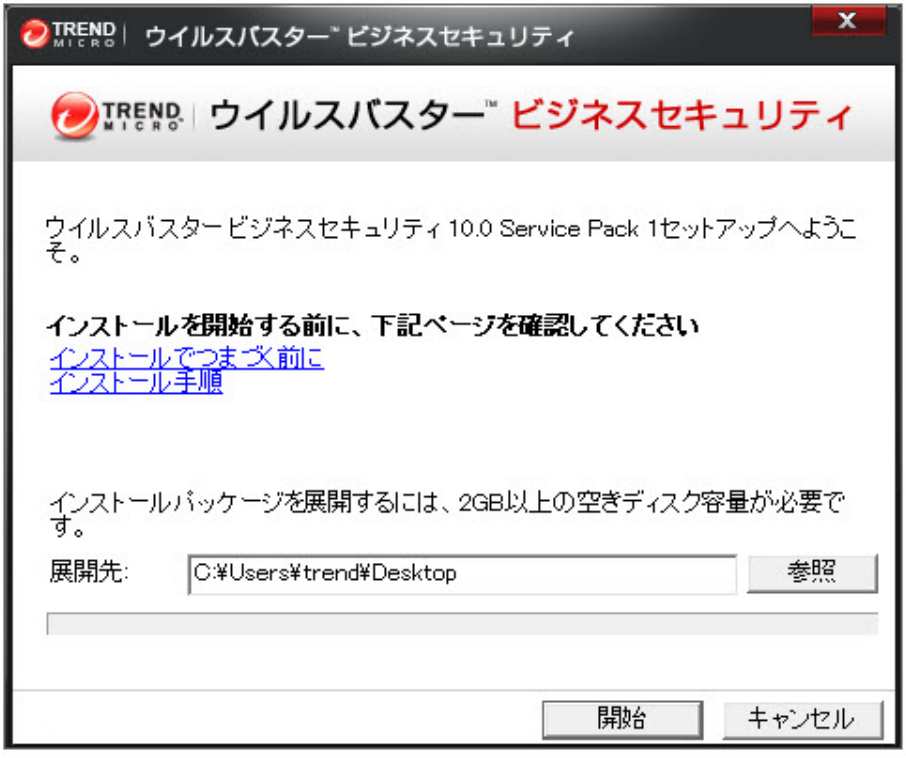
フェーズ 1: ビジネスセキュリティサーバのインストールを開始する

始める前に

- ドメインまたはローカルの管理者権限を持つアカウントを使用してコンピュータにログオンします。
- ビジネスセキュリティをインストールする前に、実行中のアプリケーションはすべて閉じてください。他のアプリケーションの実行中にインストールした場合、インストールプロセスに通常より長い時間がかかることがあります。
- IIS をロックする可能性のあるアプリケーションを実行しているコンピュータにビジネスセキュリティサーバをインストールしないでください。インストールに失敗するおそれがあります。詳細については、IIS のドキュメントを参照してください。
- ビジネスセキュリティサーバをインストールするためにコンピュータを再起動する必要はありません。インストールが完了したら、すぐに Web コンソールで設定を実行し、セキュリティエージェントをクライアントにインストールしてください。

インストールパッケージを実行する

インストールパッケージ (.exe ファイル) をダブルクリックします。

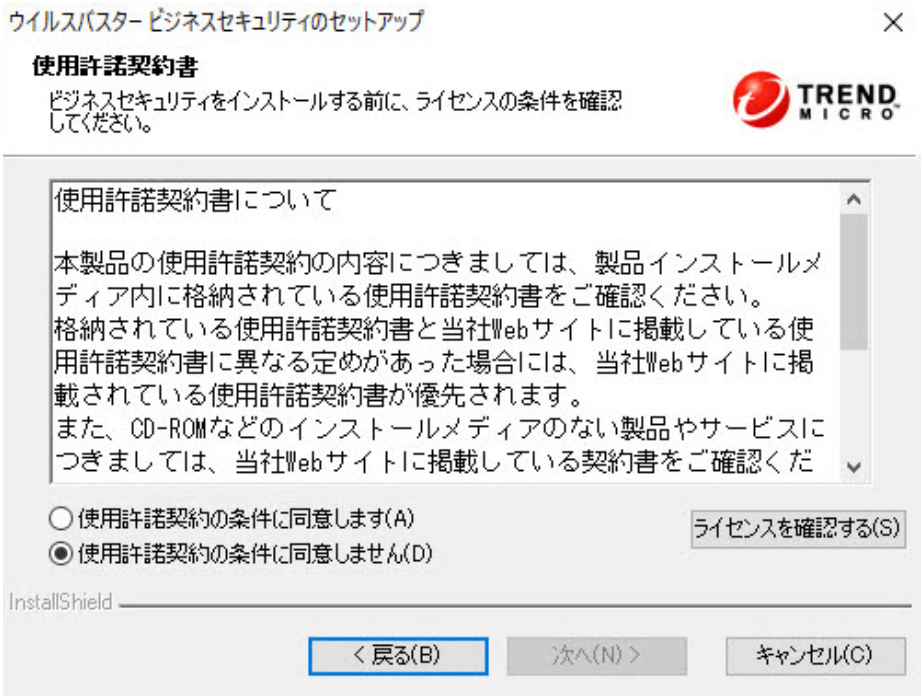


インストールファイルは、.exe ファイルと同じディレクトリに展開されます。パスを変更するには、[参照] をクリックし、ディレクトリを指定します。

[開始] をクリックすると、ファイルの展開が始まります。展開ステータスは、画面下部のステータスバーに表示されます。展開が完了すると、インストーラの初期画面が表示されます。

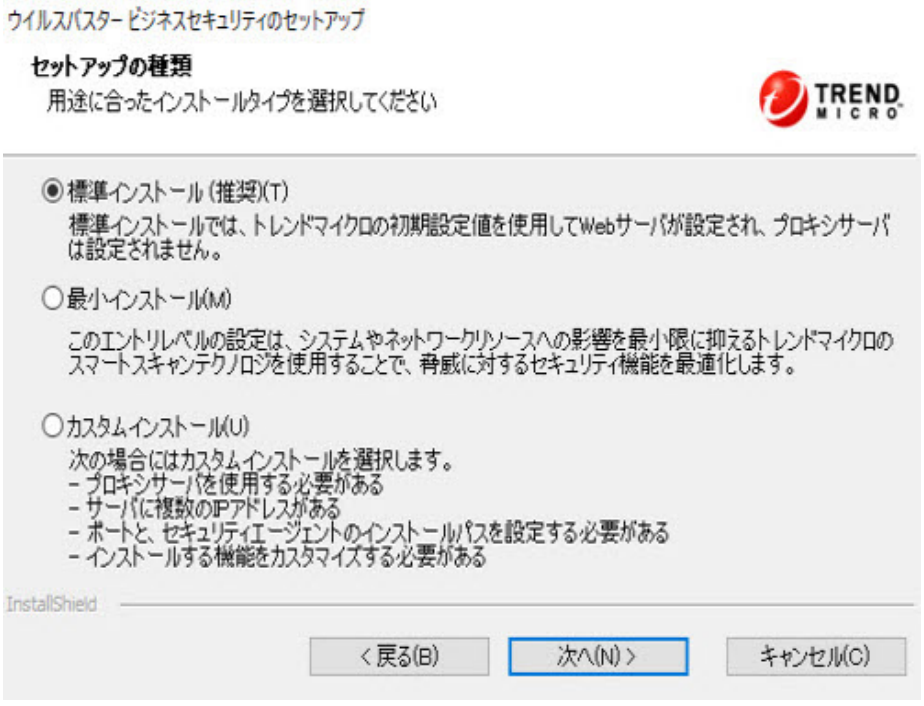

ウイルスバスター ビジネスセキュリティのセットアップ
ビジネスセキュリティセットアップウィザードへようこそ。
このウィザードでは、コンピュータにアプリケーションをインストールする手順を案内します。続行するには、[次へ] をクリックしてください。
注意:
- すべてのWebブラウザおよびアプリケーションを終了してから [次へ] をクリックすることをお勧めします。
- 次の画面が表示されるまでに数分かかる場合があります。
< 戻る(B)
次へ(N) >
キャンセル(C)

使用許諾契約書



使用許諾契約書を読みます。条件に同意する場合は、[使用許諾契約の条件に同意します] を選択します。

セットアップの種類



次のいずれかのオプションを選択します。

標準インストール (推奨)

この方法は、最大で 100 台のエージェントを管理するビジネスセキュリティサーバに適しています。

- インストール後に、次の機能が自動的に有効になります。
  - ウイルス/スパイウェア対策
  - 挙動監視 (Windows 7 などのデスクトッププラットフォームのみ)
  - Web レピュテーション

- URL フィルタ
- スマートスキャン

注意

セキュリティエージェントが、スマートスキャンを実行するための最小システム要件を満たしている必要があります。要件のリストについては、https://www.trendmicro.com/ja_jp/small-business/worry-free-standard.html#requirement を参照してください。

- ビジネスセキュリティサーバをインストールするコンピュータにセキュリティエージェントがインストールされていない場合、自動的にセキュリティエージェントがインストールされます。

注意

セキュリティエージェントをネットワーク内の他のクライアントにインストールし、Web コンソールから管理します。セキュリティエージェ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。

- 別のエンドポイントセキュリティソフトウェアがコンピュータにインストールされている場合は、セットアップでまずそのソフトウェアがアンインストールされ、その後、セキュリティエージェントがインストールされます。

注意

一部のエンドポイントセキュリティソフトウェアは、検出のみが可能で、アンインストールできません。この場合は、まずこのソフトウェアを手動でアンインストールする必要があります。

アンインストールできるエンドポイントセキュリティソフトウェア、または、検出のみが可能でアンインストールできないエンドポイントセキュリティソフトウェアのリストについては、次の Web サイトを参照してください。

http://tmqa.jp/biz

最小インストール

- インストール後に、ウイルス対策/スパイウェア対策機能のみが有効になります。

- ビジネスセキュリティサーバをインストールするコンピュータにセキュリティエージェントがインストールされていない場合、自動的にセキュリティエージェントがインストールされます。

注意

セキュリティエージェントをネットワーク内の他のクライアントにインストールし、Web コンソールから管理します。セキュリティエージェ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。

- 別のエンドポイントセキュリティソフトウェアがコンピュータにインストールされている場合は、セットアップでまずそのソフトウェアがアンインストールされ、その後、セキュリティエージェントがインストールされます。

注意

一部のエンドポイントセキュリティソフトウェアは、検出のみが可能で、アンインストールできません。この場合は、まずこのソフトウェアを手動でアンインストールする必要があります。

アンインストールできるエンドポイントセキュリティソフトウェア、または、検出のみが可能でアンインストールできないエンドポイントセキュリティソフトウェアのリストについては、次の Web サイトを参照してください。

http://tmqa.jp/biz

カスタムインストール

企業のネットワークセキュリティ戦略に合わせて、ビジネスセキュリティサーバとエージェントをより柔軟に設定できます。この方法は、ビジネスセキュリティサーバが多数のエージェントを管理する場合に適しています。

- ビジネスセキュリティサーバをインストールするコンピュータにセキュリティエージェントがインストールされていない場合、自動的にセキュリティエージェントがインストールされます。

注意

セキュリティエージェントをネットワーク内の他のクライアントにインストールし、Web コンソールから管理します。セキュリティエージェ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。

- 別のエンドポイントセキュリティソフトウェアがコンピュータにインストールされている場合は、セットアップでまずそのソフトウェアがアンインストールされ、その後、セキュリティエージェントがインストールされます。

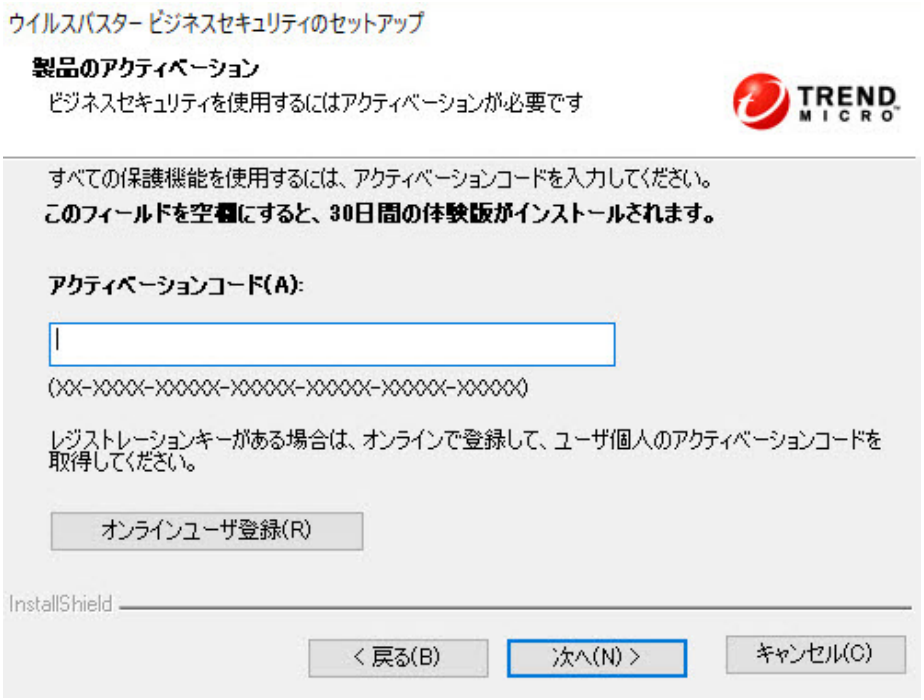
注意

一部のエンドポイントセキュリティソフトウェアは、検出のみが可能で、アンインストールできません。この場合は、まずこのソフトウェアを手動でアンインストールする必要があります。

アンインストールできるエンドポイントセキュリティソフトウェア、または、検出のみが可能でアンインストールできないエンドポイントセキュリティソフトウェアのリストについては、次の Web サイトを参照してください。

http://tmqa.jp/biz

製品のアクティベーション



[アクティベーションコード] フィールドにアクティベーションコードを入力します。

アクティベーションコードをお持ちでない場合は、お使いのビジネスセキュリティをまだ登録していない可能性があります。[オンラインユーザ登録] ボタンをクリックして、新しいブラウザウィンドウを開きます。登録画面上の手順に従います。または、[次へ] をクリックして、体験版をインストールします。30 日体験版の期間が終了する前に製品版へアップグレードすると、すべてのプログラム設定が維持されます。

セットアップの概要

セットアップの [概要] 画面には、ビジネスセキュリティサーバまたはセキュリティエージェントをインストールするために設定する必要があるコンポーネントが表示されます。

[次へ] をクリックした後は、選択したセットアップの種類によって異なります。

- 標準/最小インストールを選択した場合
  - 42 ページの「標準または最小インストール用に設定する」
  - 63 ページの「フェーズ 3: インストールプロセス」
- カスタムインストールを選択した場合

- 47 ページの「カスタムインストール用に設定する」
- 63 ページの「フェーズ 3: インストールプロセス」

フェーズ 2: セットアップの種類に応じて設定する

フェーズ 2 で必要な設定は、フェーズ 1 で選択したセットアップの種類によって異なります。

- 42 ページの「標準または最小インストール用に設定する」
- 47 ページの「カスタムインストール用に設定する」

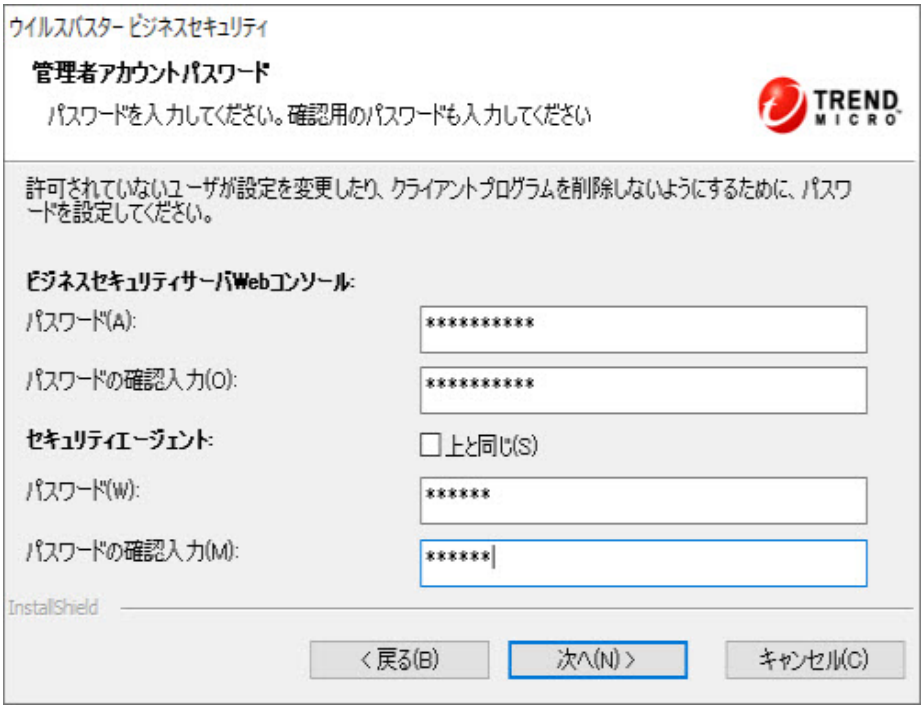
標準または最小インストール用に設定する

標準または最小インストールを実行している場合は、次の画面が順番に表示されます。

インストール場所

初期設定では、ビジネスセキュリティのインストールフォルダは `C:¥Program Files¥Trend Micro¥Security Server` または `C:¥Program Files (x86)¥Trend Micro¥Security Server` です。ビジネスセキュリティを別のフォルダにインストールする場合は、[参照] をクリックします。

管理者アカウントパスワード



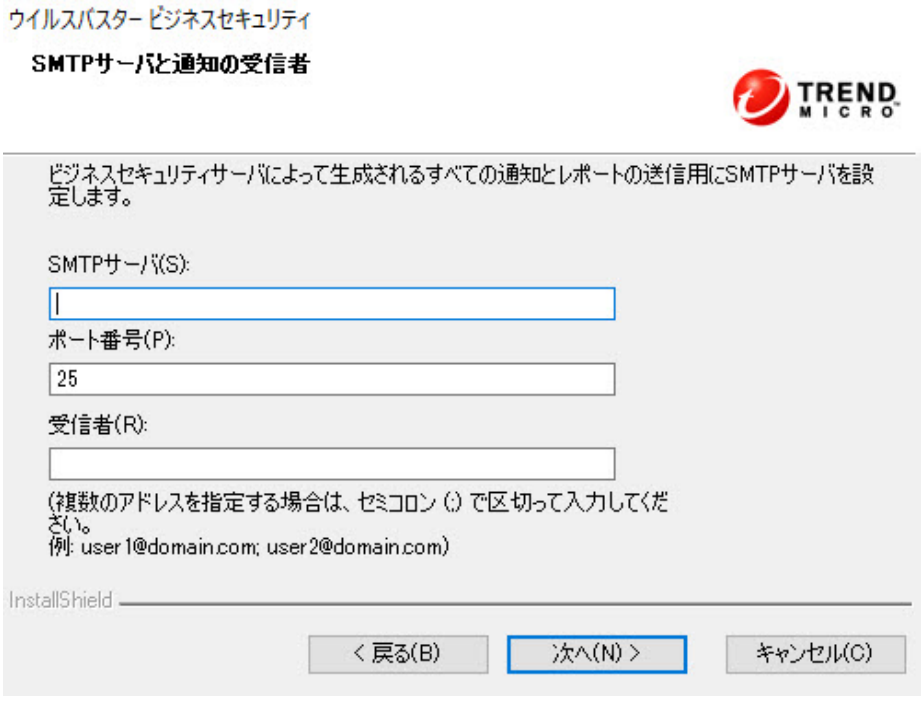
ビジネスセキュリティサーバの Web コンソールとセキュリティエージェントには異なるパスワードを指定します。

- ビジネスセキュリティサーバの Web コンソール:Web コンソールにログオンするときに必要です。
- セキュリティエージェント:クライアントからセキュリティエージェントをアンインストールまたはアンロードするときに必要です。

注意

パスワードフィールドには 1～24 文字入力できます。大文字と小文字が区別されます。

SMTP サーバと通知の受信者



次の情報を指定します。

- SMTP サーバ: メールサーバの IP アドレス

  注意

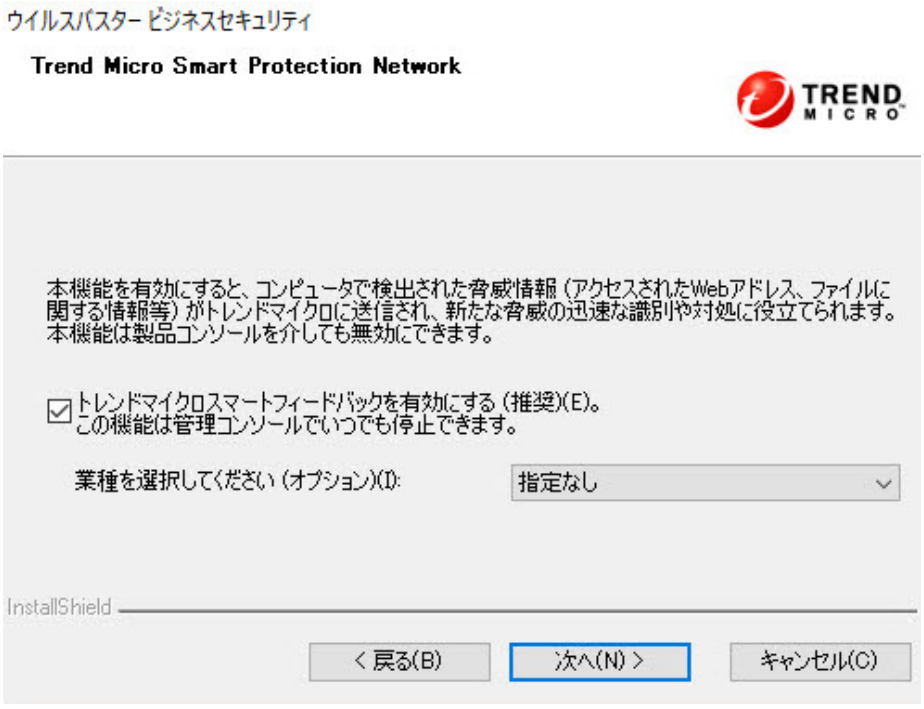
  SMTP サーバがビジネスセキュリティと同じコンピュータ上にあり、ポート 25 を使用している場合、インストールプログラムにより SMTP サーバの名前が検出され、[SMTP サーバ] フィールドと [ポート番号] フィールドが更新されます。

- ポート番号: SMTP サーバが通信に使用するポートです。

- 受信者: アラート通知を送信するために SMTP サーバが使用するメールアドレスです。2 人以上が通知を受信する必要がある場合は、複数のメールアドレスを入力できます。

インターネットサービスプロバイダのメールサーバの設定を参照してください。これらの設定がわからない場合は、次の手順に進んでください。インストール後に SMTP 設定を更新できます。手順については、管理者ガイドを参照してください。

Trend Micro Smart Protection Network



Trend Micro Smart Protection Network のフィードバックプログラムに参加するかどうかを選択します。

このオプション機能は、トレンドマイクロに不正プログラムの感染に関するフィードバックを提供します。世界中のビジネスセキュリティのフィード

バックデータを使用して不正プログラム対策ソリューションの有効性を高めるために、初期設定値のままにすることをお勧めします。Web コンソールで、後からキャンセルすることもできます。

カスタムインストール用に設定する

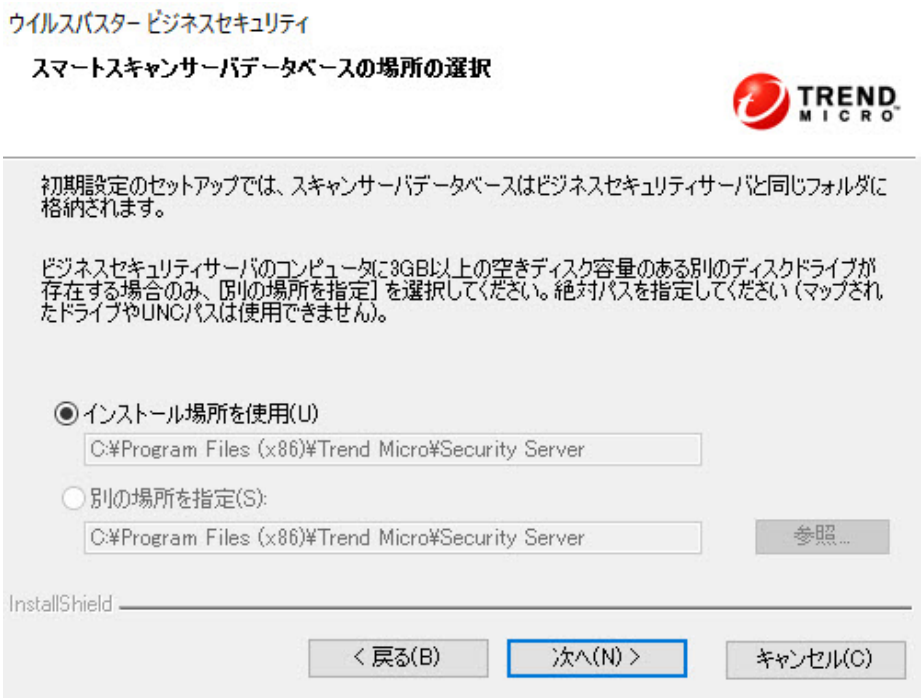
カスタムインストールを実行している場合は、次の画面が順番に表示されます。

インストール場所

初期設定では、ビジネスセキュリティのインストールフォルダは `C:¥Program Files¥Trend Micro¥Security Server` または `C:¥Program Files`

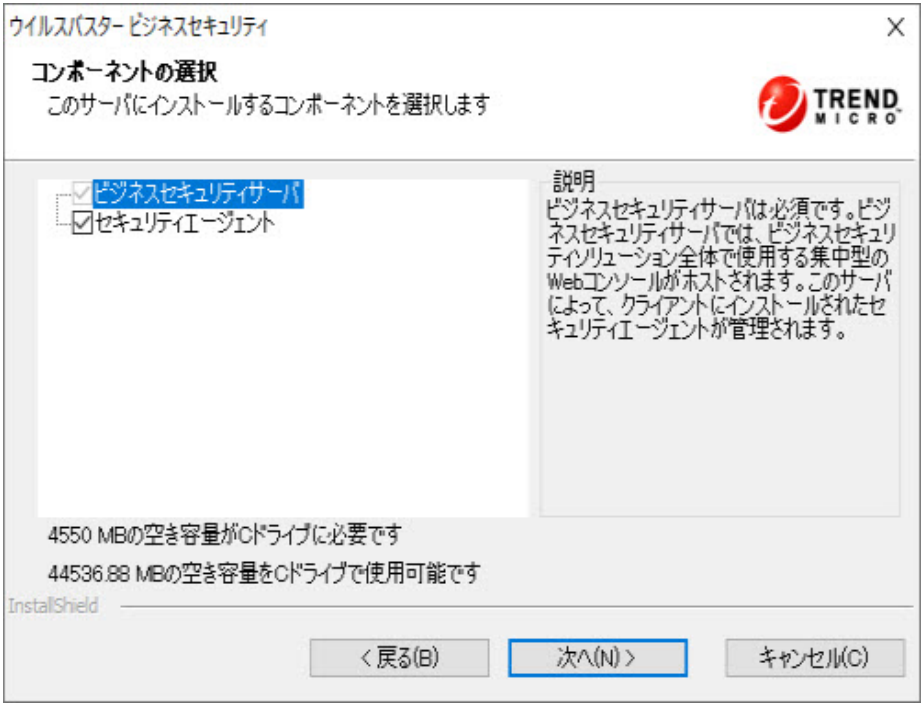
(x86)¥Trend Micro¥Security Server です。ビジネスセキュリティを別のフォルダにインストールする場合は、[参照] をクリックします。

スマートスキャンサーバデータベースの場所



[インストール場所を使用] を選択してスキャンサーバデータベースをビジネスセキュリティサーバと同じフォルダに保存するか、[別の場所を指定] を選択してビジネスセキュリティサーバ上の他の場所の絶対パスを入力します。マップ済みのドライブや UNC パスを指定することはできません。

コンポーネントの選択



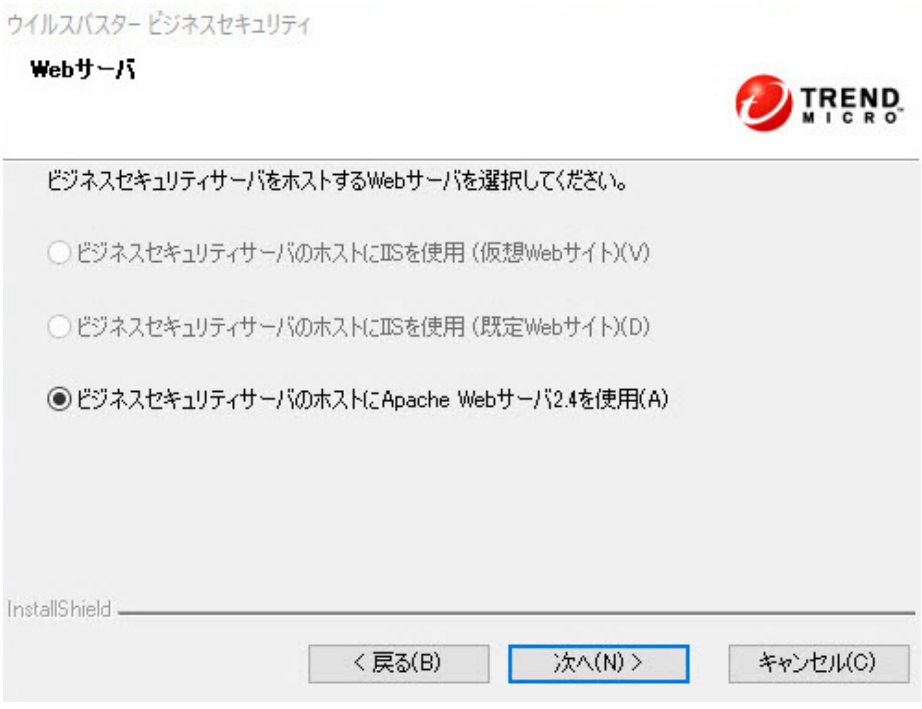
対象コンピュータにインストールするコンポーネントを選択します。

- ビジネスセキュリティサーバ (必須): ビジネスセキュリティサーバは集中型の Web ベース管理コンソールをホストします。
- セキュリティエージェント (オプション): デスクトップとサーバを保護するエージェントです。

ビジネスセキュリティサーバの設定

[ビジネスセキュリティサーバの設定] 画面では、設定が必要なビジネスセキュリティサーバの設定が表示されます。

Web サーバ



新規インストールでは、対象コンピュータに Web サーバが存在するかどうかが確認されます。

シナリオ	結果	注意

IIS Web サーバと Apache Web サーバの両方が検出	• 標準インストールまたは最小インストールの場合は、自動的に IIS が使用されます。
	• カスタムインストールの場合:
	  • Apache Web サーバのバージョンがサポートされていない場合は、セットアップで自動的に IIS が使用されます。
	  • Apache Web サーバのバージョンがサポートされている場合は、2 つの Web サーバのいずれかを選択できます。
		コンピュータで Windows 7、8.1、または 10 が実行されている場合、トレンドマイクロはカスタムインストールで Web サーバに Apache を選択することをお勧めします。

IIS Web サーバのみが検出	• 標準インストールまたは最小インストールの場合は、自動的に IIS が使用されます。 • カスタムインストールの場合は、2 つの Web サーバのいずれかを選択できます。Apache を選択すると、Apache バージョン 2.4 が自動的にインストールされます。	

シナリオ	結果	注意

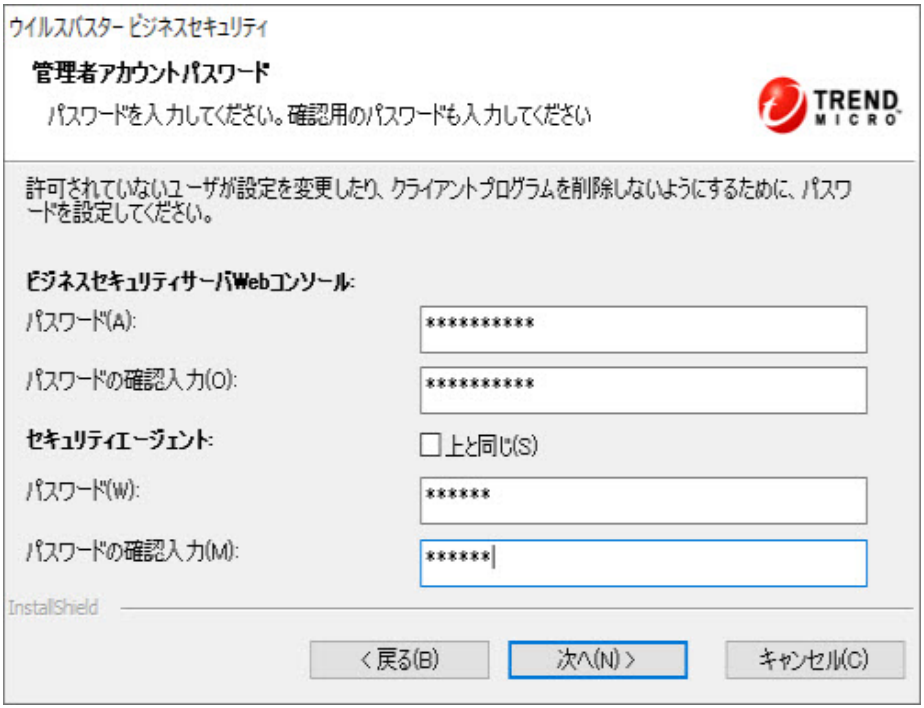
Apache Web サーバのみが検出	• Apache バージョンが 2.4 の場合は、既存の Apache が使用されます。
	• 他の Apache バージョンが存在する場合は、インストールを続行できません。次の処置を検討してください。
	  • Apache を使用しているアプリケーションがない場合は、Apache をアンインストールします。
	  • Apache をバージョン 2.4 にアップグレードします。
	  • ビジネスセキュリティサーバを別のコンピュータにインストールします。
		次のプラットフォームには IIS があり、ビジネスセキュリティサーバでサポートされています。
		• Windows Server 2008/2008 R2
		• Windows SBS 2008
		• Windows EBS 2008
		• Windows SBS 2011 Standard/Essentials
		• Windows Server 2012/2012 R2
		• Windows Server 2016
		これらのプラットフォームで IIS を検出できない場合は、(初期設定で、またはシステム管理者により) IIS が無効になっている可能性があります。この場合は、IIS を有効にします。

どちらの Web サーバも検出されない	Apache Web サーバ 2.4 が自動的にインストールされます。	

Apache が Web サーバとして現在使用されている場合、アップグレードの処理は次のようになります。

- Apache Web サーバがビジネスセキュリティ 9.x セットアッププログラムによってインストールされた場合は、Apache バージョンが 2.4 に自動的にアップグレードされます。
- 既存の Apache バージョンが他のプログラムによってインストールされた場合は、その Apache バージョンが保持されます。

管理者アカウントパスワード



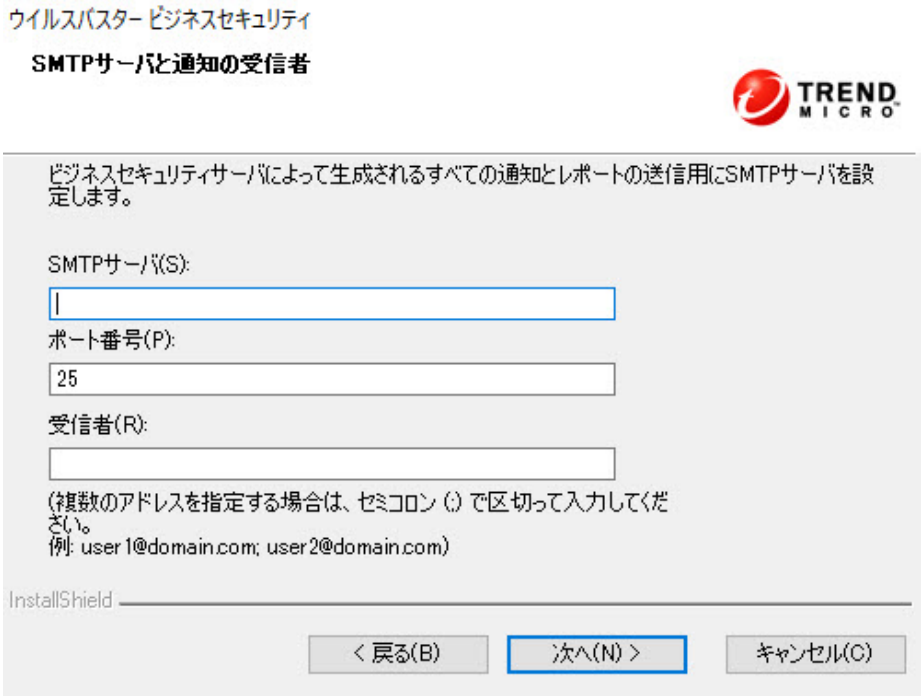
ビジネスセキュリティサーバの Web コンソールとセキュリティエージェントには異なるパスワードを指定します。

- ビジネスセキュリティサーバの Web コンソール:Web コンソールにログオンするときに必要です。
- セキュリティエージェント:クライアントからセキュリティエージェントをアンインストールまたはアンロードするときに必要です。

注意

パスワードフィールドには 1～24 文字入力できます。大文字と小文字が区別されます。

SMTP サーバと通知の受信者



次の情報を指定します。

- SMTP サーバ: メールサーバの IP アドレス

  注意

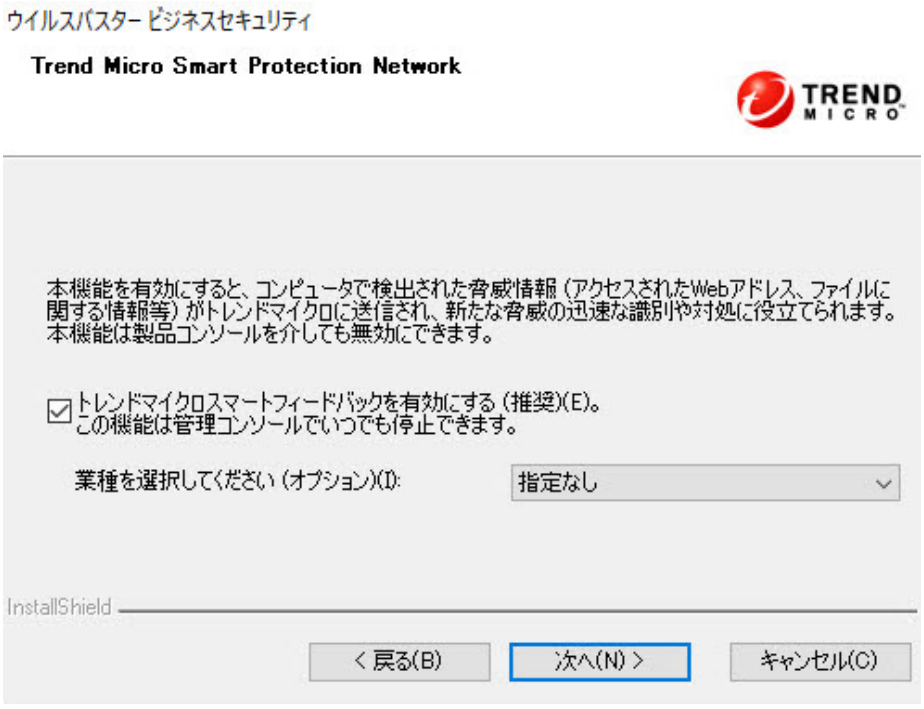
  SMTP サーバがビジネスセキュリティと同じコンピュータ上にあり、ポート 25 を使用している場合、インストールプログラムにより SMTP サーバの名前が検出され、[SMTP サーバ] フィールドと [ポート番号] フィールドが更新されます。

- ポート番号: SMTP サーバが通信に使用するポートです。

- 受信者: アラート通知を送信するために SMTP サーバが使用するメールアドレスです。2 人以上が通知を受信する必要がある場合は、複数のメールアドレスを入力できます。

インターネットサービスプロバイダのメールサーバの設定を参照してください。これらの設定がわからない場合は、次の手順に進んでください。インストール後に SMTP 設定を更新できます。手順については、管理者ガイドを参照してください。

Trend Micro Smart Protection Network

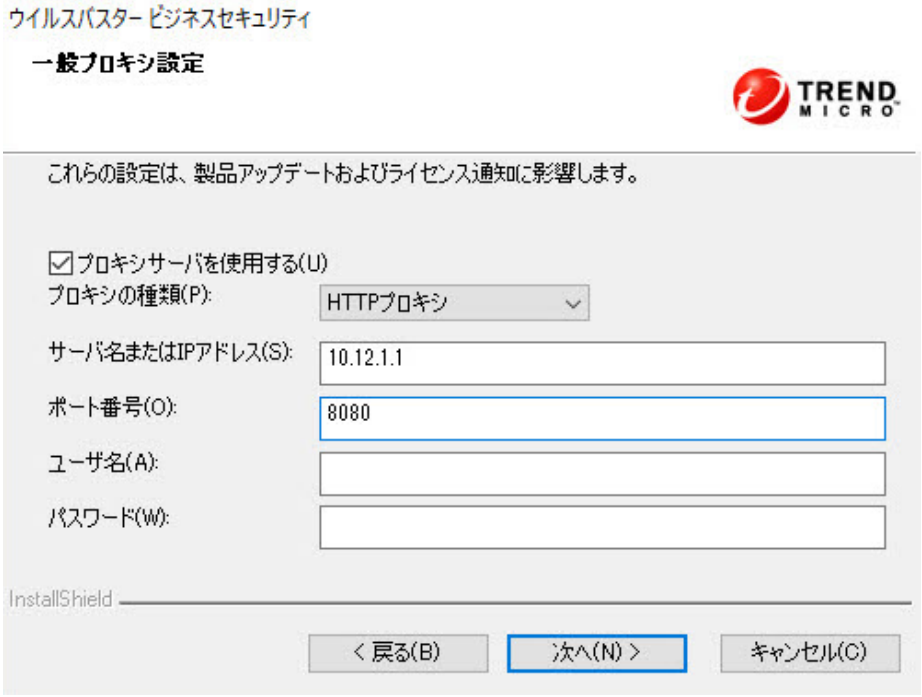


Trend Micro Smart Protection Network のフィードバックプログラムに参加するかどうかを選択します。

このオプション機能は、トレンドマイクロに不正プログラムの感染に関するフィードバックを提供します。世界中のビジネスセキュリティのフィード

バックデータを使用して不正プログラム対策ソリューションの有効性を高めるために、初期設定値のままにすることをお勧めします。Web コンソールで、後からキャンセルすることもできます。

一般プロキシ設定



プロキシサーバがインターネットにアクセスする必要がある場合は、[プロキシサーバを使用する] チェックボックスをオンにし、次の情報を指定します。

- プロキシの種類
- サーバ名または IP アドレス
- ポート番号

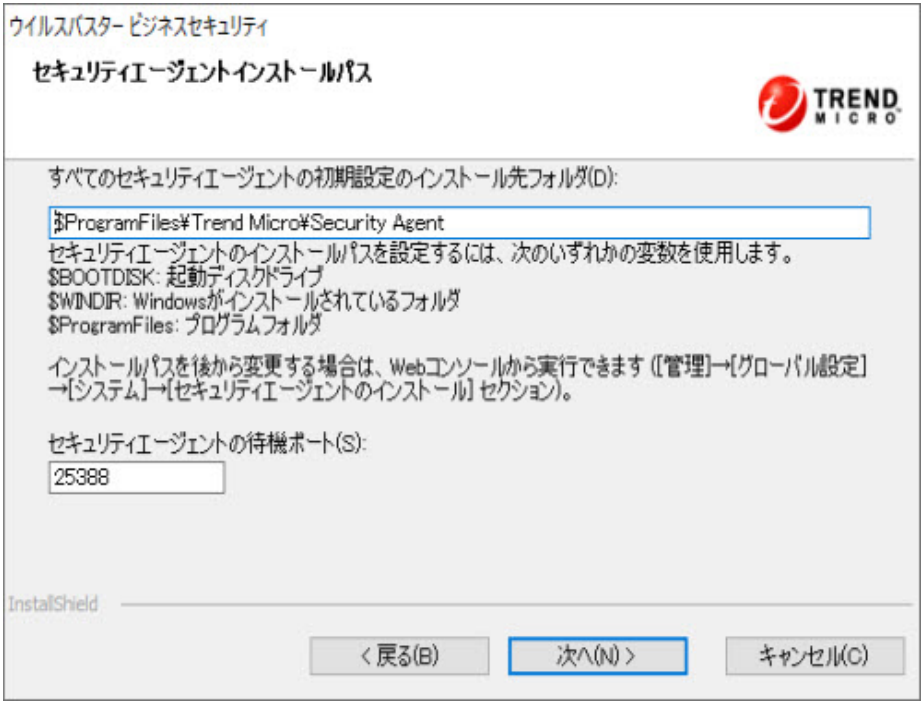
- ユーザ名とパスワード: プロキシサーバで認証が必要な場合のみ指定します。

セキュリティエージェント設定

[セキュリティエージェント設定] 画面では、設定が必要なセキュリティエージェントを表示します。

ビジネスセキュリティサーバをインストールしたら、セキュリティエージェントをネットワーク内のクライアントにインストールします。セキュリティエージェントをインストールする方法 については、管理者ガイドを参照してください。

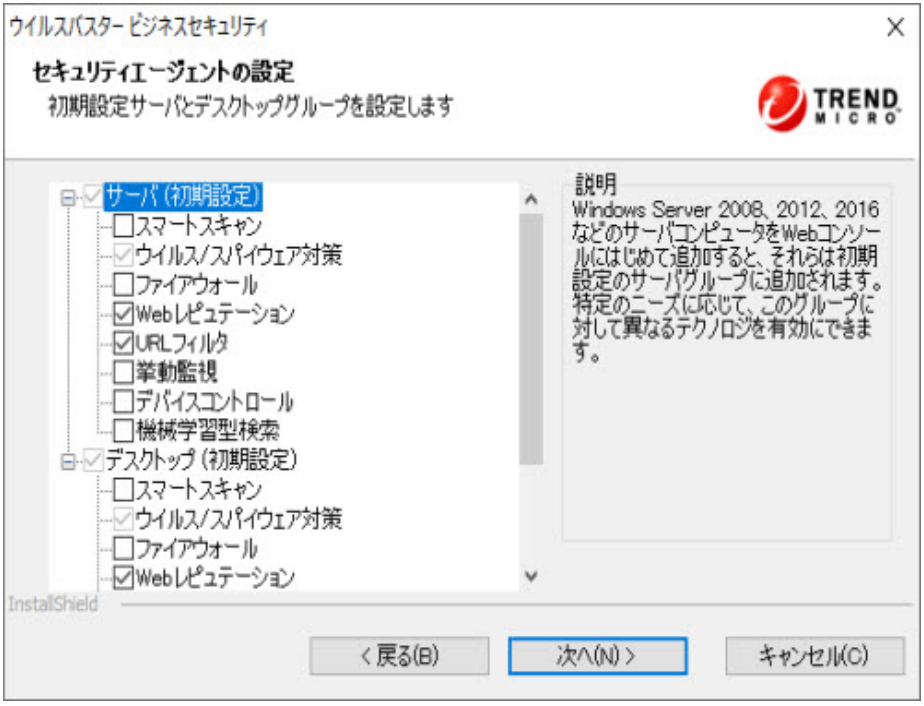
セキュリティエージェントインストールパス



次の項目を設定します。

- インストールパス: セキュリティエージェントのファイルがインストールされているインストール先フォルダ
- セキュリティエージェントの待機ポート: セキュリティエージェントとビジネスセキュリティサーバの通信に使用されるポート番号

セキュリティエージェントの設定



サーバとデスクトップのセキュリティエージェントを設定します。

- サーバ (初期設定): Windows サーバプラットフォーム (Windows Server 2008 など) にインストールしたセキュリティエージェントは、最初に Web コンソールに追加したときに、この初期設定のサーバグループに追加されます。ニーズに応じて、このグループに対して異なる機能を有効にできます。
- デスクトップ (初期設定): Windows デスクトッププラットフォーム (Windows 7 など) にインストールしたセキュリティエージェントは、最初に Web コンソールに追加したときに、この初期設定のデスクトップグループに追加されます。ニーズに応じて、このグループに対して異なる機能を有効にできます。

各グループで、次のコンポーネントを設定できます。

- スマートスキャン: スマートスキャンでは、ネットワーク内の集中型のスキャンサーバが使用されるため、クライアントの検索処理の負荷が軽減されます。
- ウイルス/スパイウェア対策: ファイルのアクセス時または作成時に不正プログラムコードについて検索します。
- ファイアウォール: クライアントとネットワークの間に障壁を作成することにより、不正プログラムの攻撃やネットワークウイルスからクライアントを保護します。
- Web レピュテーション: Web ドメインの信頼性と、いくつかの識別要素に基づいたレピュテーションスコアの割り当てにより、不正な Web サイトをブロックします。
- URL フィルタ: 会社のポリシーに基づいて指定されたカテゴリの Web サイト (ポルノやソーシャルネットワーキングなど) をブロックします。
- 挙動監視: プログラムの挙動を分析して、既知および未知の両方の脅威を予防的に検出します。
- デバイスコントロール: 外部ストレージデバイスおよびネットワークリソースへのアクセスを調整します。
- 機械学習型検索: 高度な機械学習テクノロジを使用して脅威情報を関連付け、デジタル DNA フィンガープリントや API マッピングなどのファイル機能を使用した詳細なファイル分析により、未知のセキュリティリスクを検出します。

追加サービスのためのプロキシ設定

スマートスキャン、Web レピュテーション、および挙動監視サービスでは、クライアントコンピュータ上の Internet Explorer で使用しているプロキシサーバのアドレスとポートを使用します。そのプロキシサーバで認証が必要な場合は、ログオン資格情報を設定します。

フェーズ 3: インストールプロセス

ファイルのコピー開始

[ファイルのコピー開始] 画面には、ビジネスセキュリティのインストール中に使用されるすべてのパラメータの概要が表示されます。

インストール設定を確認する場合は、[戻る] をクリックします。インストールに進むには、[次へ] をクリックします。

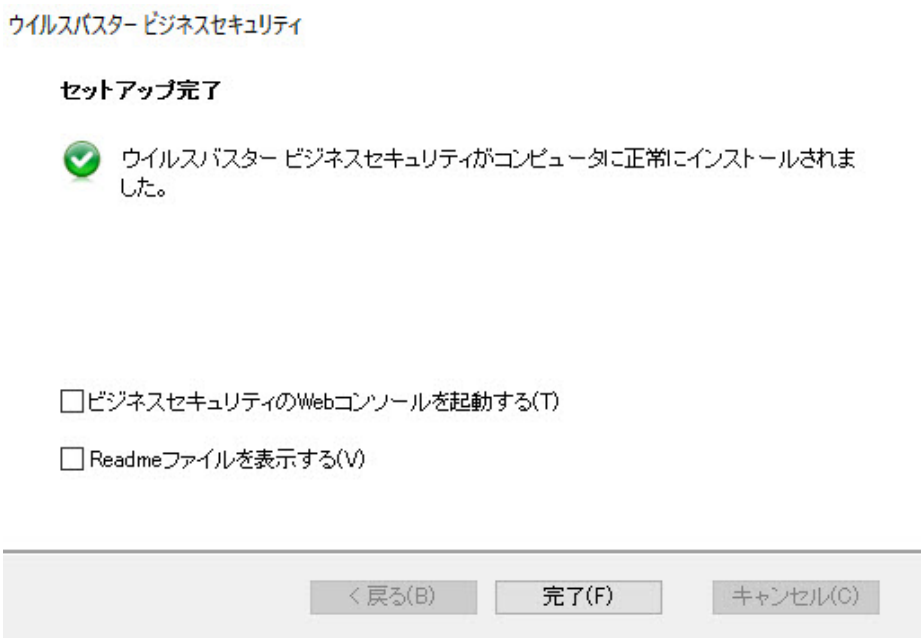
サードパーティコンポーネントのインストール

この画面には、インストールするサードパーティコンポーネントが表示されます。[次へ] をクリックすると、選択したコンポーネントのインストールを開始します。

セットアップステータス

インストール処理全体が完了するには、時間がかかる場合があります。インストール中は、進行状況がステータス画面に表示されます。

セットアップ完了



オプションで、チェックボックスをオンにして次の操作を実行します。

- ビジネスセキュリティの Web コンソールを起動する
- Readme ファイルを表示する

[完了] をクリックしてインストール手順を終了します。

サイレントインストールを使用して複数のビジネスセキュリティサーバをインストールする

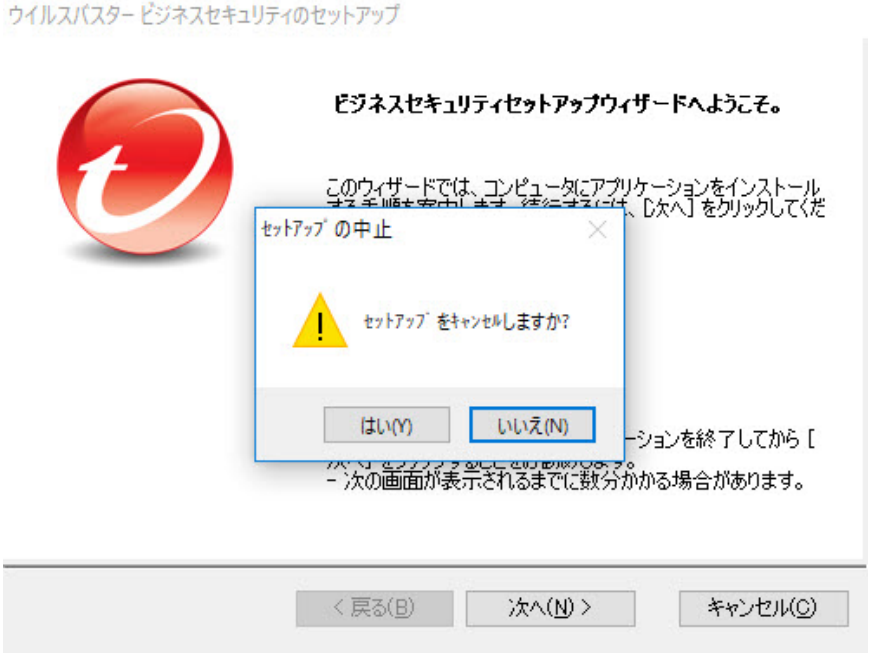
サイレントインストールを使用すると、別々のネットワーク上で同一のインストールを複数実行できます。1 回のセットアップウィザードセッションで

インストール設定を記録し、その設定を使用して自動インストールを生成できます。

インストールセッションを記録する

手順

1. ビジネスセキュリティのファイルをハードディスクに ダウンロードして展開します。セットアップウィザードがインストール設定の収集を開始したら、[キャンセル] > [はい] > [終了] をクリックします。



2. コマンドプロンプトモードで、ビジネスセキュリティのセットアップファイルを展開したディレクトリに移動します (例: `C:¥Extract¥WFBS¥CSM`)。

3. プロンプトで「`Setup.exe /r /f1"c:\silent-install.iss"`」と入力し、[入力] をクリックします。

セットアップウィザードが再度開始します。入力が C ドライブの「silent-install.iss」ファイルに記録されます。

4. 画面上の手順に従います。手順は 30 ページの「ビジネスセキュリティサーバのインストール」の説明と同じです。

5. 記録セッションの最後に、次の確認画面が表示されます。[終了] をクリックして記録セッションを終了し、コマンドプロンプトモードに戻ります。

サイレントインストールを開始する

手順

1. コマンドプロンプトモードで、ビジネスセキュリティのセットアップファイルを展開したディレクトリに移動します (例: `C:¥Extract¥WFBS¥CSM`)。

2. プロンプトで「`Setup.exe /s /f1"c:\silent-install.iss"`」と入力し、<Enter> キーを押します。

   ビジネスセキュリティのサイレントインストールが自動的に開始します。かかる時間は標準インストールと同じです。

   サイレントインストール中は、進行状況を知らせるインジケータが表示されません。

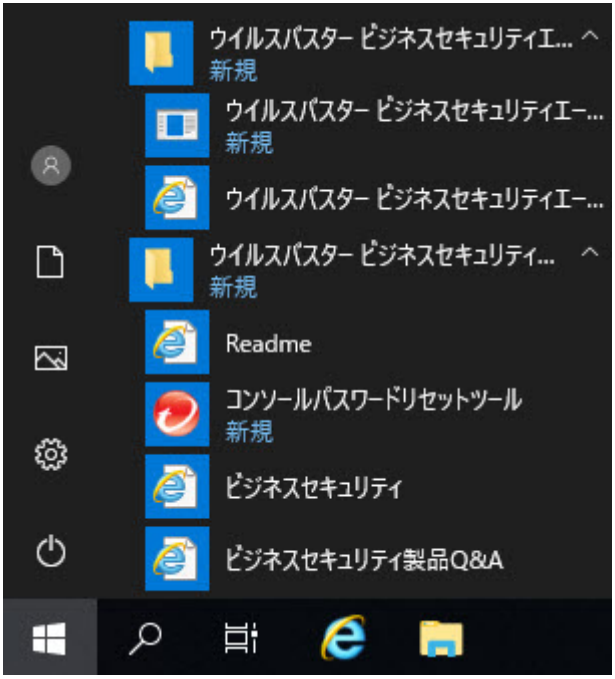
3. インストールが成功したことを確認するには、「`c:¥setup.log`」ファイルを開きます。`ResultCode=0` である場合、インストールは成功しています。

4. ネットワークのすべてのコンピュータ上で手順 1～3 を繰り返します。

インストールを確認する

手順

- [スタート] > [すべてのプログラム] の順にクリックして、ビジネスセキュリティサーバとセキュリティエージェントがリストに表示されることを確認します。



- [スタート] > [コントロールパネル] > [プログラム] > [プログラムのアンインストール] の順にクリックして、ビジネスセキュリティサーバとセキュリティエージェントがリストに表示されることを確認します。
- サーバ URL (`https://{サーバ名}:{ポート番号}/SMB`) を使用して Web コンソールにログオンします。

注意

SSL (Security Socket Layer) を使用していない場合は、「`https`」ではなく「`http`」と入力します。

第 3 章

ビジネスセキュリティサーバおよびエージェントのアップグレード

この章では、ビジネスセキュリティサーバおよびエージェントをアップグレードするために必要な情報について説明します。

インストールとアップグレードの要件

システム要件については、次の Web サイトを参照してください。

https://www.trendmicro.com/ja_jp/small-business/worry-free-standard.html#requirement

アップグレードに関する考慮事項

ビジネスセキュリティサーバおよびエージェントをアップグレードするときは、次の点について考慮してください。

- 72 ページの「アップグレードのための IPv6 要件」
- 73 ページの「推奨アップグレード方法」

アップグレードのための IPv6 要件

ビジネスセキュリティサーバの IPv6 の要件は次のとおりです。

- アップグレードするビジネスセキュリティサーバは、Windows 7、8.1、10、Server 2008、2012、2012 R2、2016、2019、または SBS 2008/2011 にインストールされている必要があります。
- IPv6 アドレスをビジネスセキュリティサーバに割り当てます。また、サーバはホスト名で識別する必要があります。完全修飾ドメイン名 (FQDN) を使用することをお勧めします。サーバを IPv6 アドレスで識別する場合、サーバが現在管理しているすべてのクライアントがサーバとの接続を失います。サーバを IPv4 アドレスで識別する場合、エージェントを IPv6 シングルスタッククライアントに配信できません。
- 「ping」や「nslookup」コマンドなどを使用して、ビジネスセキュリティサーバのホストマシンの IPv6 または IPv4 アドレスを取得できることを確認します。

推奨アップグレード方法

最新バージョンのビジネスセキュリティにアップグレードするときに、クライアントの設定を保持できます。アップグレードに失敗した場合に既存の設定を簡単に復元できるように、トレンドマイクロは次のことを推奨します。

- ビジネスセキュリティサーバデータベースのバックアップ
- ビジネスセキュリティサーバからのすべてのログファイルの削除

ビジネスセキュリティサーバデータベースをバックアップする

手順

1. ビジネスセキュリティサーバの「Trend Micro Security Server Master Service」を停止します。
2. Windows エクスプローラで、ビジネスセキュリティサーバフォルダに移動し、`¥PCCSRV¥HTTPDB` の内容を別の場所 (同じサーバ上の別のフォルダ、別のコンピュータ、リムーバブルドライブなど) にコピーします。

ビジネスセキュリティサーバからログファイルを削除する

手順

1. [レポート] > [管理] > [ログの手動削除] の順に移動します。
2. 削除するログの種類の、[次の日数を経過したログを削除] を 0 に設定します。
3. 次のいずれかの方法を選択してログを削除します。
   - 各ログの種類で [削除] をクリックします。
   - [すべて削除] をクリックして、すべてのログを削除します。

以前のバージョンからのアップグレード

このバージョンでは、次のバージョンのビジネスセキュリティからのバージョンアップのみをサポートしています。

- 10.0
- 9.x (すべてのサービスパックを含む)

ネットワーク帯域幅、およびビジネスセキュリティサーバが管理するエージェント数に応じて、グループ内でエージェントバージョンアップの日時をずらすことも、またはサーバアップグレード後すぐにすべてのエージェントをアップグレードすることもできます。

アップグレード方法 1: インストールパッケージを使用してアップグレードする

本バージョン用のインストールパッケージを取得して、ビジネスセキュリティサーバコンピュータで「`biz10sp1.exe`」を実行します。既存のビジネス

セキュリティサーバがコンピュータ上に存在することが検出されると、次の図のようにアップグレードが求められます。

画面上の指示に従い、ビジネスセキュリティサーバをアップグレードします。

アップグレードの完了後:

- オンラインのセキュリティエージェントがただちにアップグレードされます。
- オフラインのセキュリティエージェントは、オンラインになったときにアップグレードされます。

  セキュリティエージェントをオンラインにするため、ユーザにネットワークに接続するよう指示します。長期間オフラインになっているセキュリティエージェントについては、エンドポイントからセキュリティ

エージェントをアンインストールし、管理者ガイドで説明されている適切なエージェントのインストール方法 (Client Packager など) を使用してセキュリティエージェントをインストールするようにユーザに指示します。

注意

本バージョンにアップグレードした後は、アップデートエージェント権限を除いて、以前のすべてのクライアントの設定が保持されます。このため、アップグレードを行うと、アップデートエージェントとして割り当てられていたセキュリティエージェントは、割り当てを解除されます。Web コンソールからアップデートエージェントとして再割り当てしてください。

詳細については、http://tmqa.jp/biz10_KB_1309419 を参照してください。

アップグレード方法 2: セキュリティエージェントをビジネスセキュリティサーバ 10.0 Service Pack 1 に移動する

ビジネスセキュリティサーバの新規インストールを実行してから、セキュリティエージェントをこのサーバに移動します。セキュリティエージェントを移動すると、自動的にバージョン 10.0 Service Pack 1 にアップグレードされます。

手順 1: ビジネスセキュリティサーバ 10.0 Service Pack 1 の新規インストールを実行する

手順

1. コンピュータでビジネスセキュリティ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、30 ページの「ビジネスセキュリティサーバのインストール」を参照してください。
2. ビジネスセキュリティサーバ 10.0 Service Pack 1 の情報を記録します。エージェントを移動するときに、サポートされるバージョンのビジネスセキュリティサーバでこの情報を指定します。
   - ホスト名または IP アドレス

- サーバ待機ポート

  サーバ名は、ビジネスセキュリティサーバの Web コンソール画面上部に表示されています。サーバ名をクリックすると、ポート番号が表示されます。

手順 2: エージェントをアップグレードする

手順

1. サポートされるバージョンのビジネスセキュリティサーバの Web コンソールで、[セキュリティ設定] に移動します。
2. セキュリティエージェントを移動するには、グループを選択してからエージェントを選択します。

   ヒント

   隣接する複数のセキュリティエージェントを選択するには、選択範囲内の最初のエージェントをクリックして、<Shift> キーを押しながら選択範囲内の最後のエージェントをクリックします。隣接していないエージェントの範囲を選択するには、選択範囲内の最初のエージェントをクリックして、<Ctrl> キーを押しながら選択するエージェントをクリックします。

3. [クライアントツリーの管理] > [クライアントの移動] の順にクリックします。

   新しい画面が表示されます。

4. エージェントの移動先のビジネスセキュリティサーバ 10.0 Service Pack 1 のホスト名と待機ポートを入力します。
5. [移動] をクリックします。

アップグレードの結果

- オンラインのエージェントの移動とアップグレードが開始されます。アップグレード後、セキュリティエージェントは、エンドポイントの OS

に応じてビジネスセキュリティサーバ 10.0 Service Pack 1 の [デスクトップ (初期設定)] または [サーバ (初期設定)] の下にグループ化されます。エージェントは新しいグループの設定を継承します。

- オフラインのエージェントは、オンラインになったときにアップグレードされます。エージェントをオンラインにするため、ユーザにネットワークに接続するよう指示します。長期間オフラインになっているセキュリティエージェントについては、エンドポイントからセキュリティエージェントをアンインストールし、管理者ガイドで説明されている適切なエージェントのインストール方法 (Client Packager など) を使用してセキュリティエージェントをインストールするようにユーザに指示します。

製品版にアップグレードする

次の操作を実行するには、Web コンソールの [ライセンス] 画面を使用します。

- 製品の体験版から製品版へのアップグレード

体験版と製品版

体験版の有効期限が近づくと、Web コンソールの [最新ステータス] 画面に通知メッセージが表示されます。Web コンソールを使用して、体験版から製品版にアップグレードできます。設定は保存されます。製品版を購入すると、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送信されます。

製品版にアップグレードする

手順

1. Web コンソールで、[管理] > [ライセンス] に移動します。
2. アクティベーションコードがある場合は、[新規入力] をクリックし、[新しいアクティベーションコード] フィールドにアクティベーションコードを入力して、[アクティベート] をクリックします。

付録 A

テクニカルサポート

ここでは、次の項目について説明します。

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

https://success.trendmicro.com/jp/technical-support

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2 つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/ をご覧ください。

- 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- Web 攻撃およびオンラインのトレンド情報
- 不正プログラムの週次レポート

製品サポート情報

製品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「製品サポートガイド」または「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、電話またはお問い合わせ Web フォームをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「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、サポートサービス継続を希望される場合は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。

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不正プログラム情報検索サイト「脅威データベース」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。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

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。

https://success.trendmicro.com/jp/virus-and-threat-help

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。

メールレピュテーションについて

スパムメールやフィッシングメールなどの送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

注意

サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

脅威解析・サポートセンター TrendLabs (トレンドラボ)

TrendLabs (トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 か所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

索引