TREND MICRO

ServerProtect™ for EMC Celerra 5.8 Patch2

クイックスタートガイド

Endpoint 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://success.trendmicro.com/jp/solution/000207383

法人向け製品のサポートについて

- 法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。
- 法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

著作権について

商標について

P/N: SPEM56717/141014_JP_R3 (2023/5)

プライバシーと個人データの収集に関する規定

トレンドマイクロ製品の一部の機能は、お客さまの製品の利用状況や検出にかかわる情報を収集してトレンドマイクロに送信します。この情報は一定の管轄区域内および特定の法令等において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客さまが関連機能を無効にする必要があります。

ServerProtect for EMC Celerra により収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次の Web サイトを参照してください。
https://www.go-tm.jp/data-collection-disclosure

重要： データ収集の無効化やデータの削除により、製品、サービス、または機能の利用に影響が発生する場合があります。ServerProtect for EMC Celerra における無効化の影響をご確認の上、無効化はお客さまの責任で行っていただくようお願いいたします。

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシー (Global Privacy Notice) に従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

目次

第 1 章

ServerProtect について

ServerProtect は、ファイルサーバの情報資産を守るウイルス対策ソフトウェアです。ServerProtect は、さまざまな種類のウイルスからネットワーク全体を保護することを目的に設計されており、最先端のウイルス検索技術を採用することによって、ネットワークをウイルス感染から防ぐことができます。検出した感染ファイルは自動的に処理することができるので、ウイルス感染がネットワーク全体に広がる危険を未然に防ぐことができます。

ServerProtect では、複数の Microsoft Windows サーバを管理コンソールから一元管理できます。管理コンソールを使用して、同一の ServerProtect ドメイン内にあるサーバを同時に設定したり、各サーバについてのウイルスに関する総合的なレポートを作成することができます。

ServerProtect の管理コンソールから管理者がウイルス対策を設定、監視、管理できるため、一貫したウイルス対策が実現します。また、管理コストも削減できます。

ServerProtect for EMC Celerra は、EMC Celerra File Server システムにウイルス対策ソリューションを提供するために開発された ServerProtect の拡張版です。拡張性と信頼性の高い ServerProtect for EMC Celerra により、ウイルスやトロイの木馬などの不正コードから Celerra File Server システムを保護します。ServerProtect for EMC Celerra では、ウイルス検索、パターンファイルアップデート、イベントレポート、ウイルス対策設定などの多くの機能を、直観的に使用できる Windows ベースのコンソールから集中管理できます。

本章で説明する内容には、次の項目が含まれます。

ServerProtect for EMC Celerra 5.8 の新機能

- Windows Server 2008、Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019 など、ほとんどのバージョンの Microsoft Windows Server プラットフォームをサポートします (詳細については、34 ページの「システム要件」を参照してください)。
- VMware ESX/ESXi 3.5/4.0/4.1 サーバをサポートします。
- ウイルスの感染を検出するためのスパイウェアパターンファイルがサポートされます。スパイウェアパターンファイルを使って、スパイウェア、ウイルス、およびファイルを検出、削除、および隔離することができます。
- インストールプログラムまたは配信プログラムを実行することで、ServerProtect for EMC Celerra 5.58 からアップグレードできます。
- インフォメーションサーバと Windows 一般サーバ間の通信のセキュリティが向上します。
- 最新のダメージクリーンナップエンジンおよびルートキット対策モジュールによって、Generic Clean 機能が提供されます。
- Trend Micro Control Manager 7.0 をサポートします。
- Trend Micro Management Communication Protocol (MCP) (ServerProtect for EMC Celerra 5.8 Patch 2 で使用可能) をサポートします。

ServerProtect のしくみ

ServerProtect では、ファイルサーバネットワークのすべての活動が監視されます。ServerProtect で、そのドメイン内のファイルへのアクセスが検出されると、そのファイルがウイルスに感染していないかどうかが必ずチェックされます。

ウイルス感染が検出された場合、通知 (警告) を発行するとともに、設定に従って処理を実行します。また、処理についてのログも記録されます。

ServerProtect では独自の検索プロファイルを作成することができるので、頻繁に使用する設定を繰り返し行う必要はありません。複数の検索オプションをプロファイルとして保存できるので、作成したプロファイルを選択するだけで、特定の検索設定をいつでも再現して使用することもできます。

ServerProtect のサーバ管理方法

ServerProtect は、管理コンソール、インフォメーションサーバ (ミドルウェア)、一般サーバで構成される 3 層アーキテクチャを採用しています。ServerProtect for EMC Celerra では、次のコンポーネントを使用してセキュリティを強化しています。

- Celerra File Server 上に配置された Data Mover (VC (ウイルスチェック) クライアントを含む)
- Celerra File Server とは別のコンピュータ上に配置された AV (ウイルス対策) サーバ (ServerProtect for EMC Celerra および Celerra Event Enabler (CEE) を含む)

これらのコンポーネントが一緒になって、強力で費用対効果の高い、一元管理されるウイルス対策セキュリティシステムを形成します。

管理コンソールは、システムコンポーネントを設定するための、Windows ベースの使いやすいユーザインタフェースを提供します。管理コンソールから送信したリクエストは、インフォメーションサーバを経由し、一般サーバへ届けられます。

通信方法

管理コンソールは TCP/IP (伝送制御プロトコル / インターネットプロトコル) を使用して、パスワード入力によりインフォメーションサーバにログオンします。インフォメーションサーバは RPC (リモートプロシージャコール) を使用して相手先サーバに接続します。

ServerProtect アーキテクチャ

ServerProtect で採用する 3 層アーキテクチャは、管理コンソール、インフォメーションサーバ、一般サーバの 3 種類のコンポーネントによって構成されます。次の図は、この 3 層の各コンポーネント間の関係を示したものです。

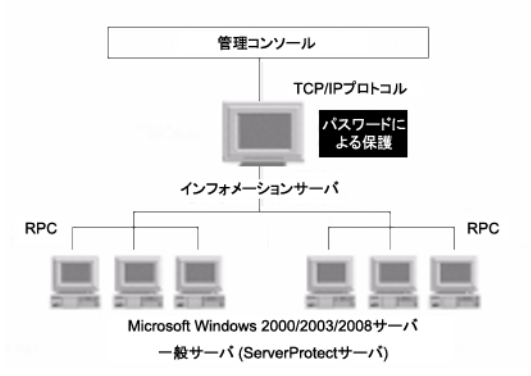


図 1-1. ServerProtect の 3 層アーキテクチャ

管理コンソール

管理コンソールは、ServerProtect を操作するためのユーザインタフェースを提供し、ネットワーク管理者による複数のドメイン、サーバの集中管理を実現します。指定したドメイン内の一般サーバを一度に設定したり、すべてのサーバのウイルスレポートを統合的に生成したりできます。管理コンソールは、主に次の部分から構成されます。

- メインメニュー
- サイドバー (ショートカットバー)
- ドメインブラウザツリー
- 設定データ領域

ドメインブラウザツリーには、ドメイン内のすべての ServerProtect 一般サーバが、それぞれのサーバのステータス情報と共に表示されます。このステータス情報には、ウイルスパターンファイル、検索エンジン、OS の種類とバージョン、リアルタイム検索の方向などが含まれます。管理者は、メイン画面のフレームを自由に調整し、必要なステータス情報を表示することができます。

ヒント： 管理コンソールを使用して、1 つまたは複数の一般サーバをリモートでインストールできます。詳細については、47 ページの「一般サーバのインストール」を参照してください。

インフォメーションサーバ

インフォメーションサーバは、管理コンソールと一般サーバ間の重要な情報や通信を制御するために特別に指定されたサーバ (ミドルウェア) です。インフォメーションサーバは、複数の一般サーバの情報制御を簡易化します。これにより、管理コンソールを使用してインフォメーションサーバ管理下のすべての一般サーバを簡単に集中管理することができます。

警告： 同一コンピュータ上に一般サーバをインストールしない場合、インフォメーションサーバはウイルスから保護されないのでご注意ください。

インフォメーションサーバに関する注意点

- ServerProtect をネットワークに導入する際、初回のインストールで、インストール先のサーバをインフォメーションサーバとしてセットアップする必要があります。他の一般サーバはそのインフォメーションサーバの管理下となるように設定してください。
- インフォメーションサーバは、一般サーバを管理する上で必ず 1 つ以上の ServerProtect ドメインを必要とします。
- インフォメーションサーバが管理できるサーバの数は、理論上は、使用可能なネットワーク帯域幅以外の制限を受けません。ただし、1 つのインフォメーションサーバが管理する一般サーバ数を少なくした方が、管理は容易になります。
- 異なる拠点に多数のサーバを配置している場合、拠点ごとにインフォメーションサーバを 1 台配置することをお勧めします。

注意： インフォメーションサーバと管理コンソールは、ServerProtect のネイティブ 32 ビットコンポーネントです。ただし、64 ビットプラットフォーム上では、ServerProtect のこれらのコンポーネントは、Windows On Windows (WOW) 64 モードで実行されます。

一般サーバ

一般サーバは、ServerProtect がインストールされた、ネットワーク上の Windows 環境のサーバです。ServerProtect のアーキテクチャでは、ウイルスを最前線で防御する役割を果たし、また、ウイルス検索処理が実際に実行される場所でもあります。一般サーバは、実際のウイルス対策機能を提供し、インフォメーションサーバによって管理されます。

ServerProtect では、複数の方法により一般サーバをインストールすることができます。一般サーバのインストール方法は次のとおりです。

- **セットアッププログラムからのインストール**
  詳細については、47 ページの「セットアッププログラムからの一般サーバのインストール」を参照してください。
- **管理コンソールからのインストール**
  詳細については、50 ページの「管理コンソールからの一般サーバのインストール」を参照してください。
- **サイレントモードでのインストール**
  詳細については、52 ページの「サイレントモードでのインストール」を参照してください。

最適なインストール方法は、インストールする環境に応じて異なります。詳細については、47 ページの「一般サーバのインストール」を参照してください。

注意： OS が 32 ビットの場合、ServerProtect の 32 ビットバイナリの一般サーバコンポーネントがインストールされます。OS が 64 ビットの場合、ServerProtect の 64 ビットバイナリの一般サーバコンポーネントがインストールされます。

ServerProtect ドメイン

ServerProtect ドメインは一般サーバの仮想的なグループで、サーバの識別および管理を簡略化するために用いられます。ドメインはネットワーク管理の必要に応じて作成、名前変更、または削除することができます。

同一ドメイン内の一般サーバは同一のインフォメーションサーバに割り当てられます。一方、インフォメーションサーバ側では、複数のドメインを管理することができます。

ネットワーク保護を管理するための最も効率的な方法は、すべてのサーバを、関連する ServerProtect ドメインにグループ化することです。たとえば、一般サーバを効率的に管理するために、「NS」というドメインを作成することができます。詳細については、64 ページの「ServerProtect ドメインの管理」を参照してください。

警告： **ServerProtect ドメインの概念は、Microsoft Windows ドメインとは異なります。ServerProtect のドメインは、単に ServerProtect が動作しているサーバを論理的にグループ化したものです。**

ServerProtect ドメインには次の機能があります。

- **ドメインフィルタ**：ネットワーク管理者は、インフォメーションサーバのフィルタを設定して、管理コンソールのドメインブラウザツリーに表示される項目を指定することができます。
- **柔軟なドメイン管理**：コンソールにログオンした後、必要に応じてドメインを追加、名前変更、または削除することができます。

注意： 管理コンソールの主な機能は、多数のインフォメーションサーバから複数の一般サーバを一元管理することです。ただし、1 つの管理コンソールから同時に接続および管理できるのは、1 つのインフォメーションサーバのみです。

ServerProtect for EMC Celerra アーキテクチャの概要

Celerra ウイルス対策システムの主なコンポーネントを次に示します。

- Celerra File Server 上に配置された Data Mover (VC (ウイルスチェック) クライアントを含む)
- Celerra File Server とは別のコンピュータ上に配置された AV (ウイルス対策) サーバ (ServerProtect for EMC Celerra および Common Event Enabler (CEE) を含む)

検索は、Celerra File Server 上ではなく、別の AV サーバ上で実行されます。そのため、ウイルス検索が Celerra File Server の処理能力に影響を与えることはありません。Celerra File Server サーバに複数の AV サーバを接続すると、検索の負荷が均等に分散されます。検索リクエストとファイルは、「ラウンドロビン」方式で AV サーバに送信されます。こうして負荷を均等に分散することで、検索のパフォーマンスが向上します。

RPC (リモートプロシージャコール) 接続は、Celerra File Server と AV サーバとの間で一定した接続を維持して、ウイルスに感染していないファイルのみが EMC データストレージシステムに保存されることを 24 時間保証します。

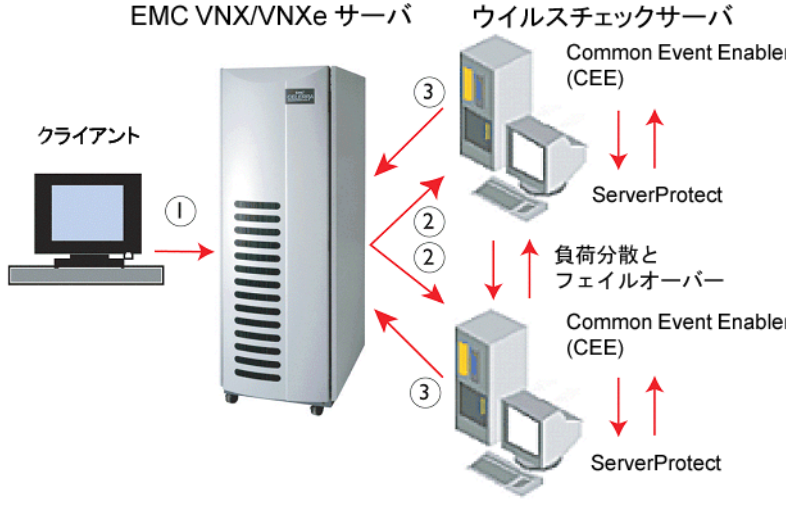


図 1-2. EMC Celerra 検索プログラムアーキテクチャを使用した ServerProtect for Storage

次に、ServerProtect と Celerra によるウイルス対策システムのワークフローについて説明します。

1. Windows クライアントを実行するユーザやアプリケーションは、CIFS (Common Internet File System) プロトコルを使用して、Celerra からファイルにアクセスします。
2. クライアントが Celerra システムのファイルの内容を変更しようとしたり、ファイルを閉じようとしたり、Celerra システムにファイルを格納しようとすると、Celerra File Server からリクエストが発行されます。
3. Celerra File Server 上の VC クライアントは、AV サーバの CEE に UNC (Universal Naming Convention) パス名を送信することでウイルスチェックを要求します。

4. リクエストはラウンドロビン方式で AV サーバに送信されます。
5. AV サーバでは、CEE が ServerProtect に対して、リアルタイム検索機能を使用してファイルのウイルスを検索するように要求します。
6. 検索結果は、次のように単純化して表示されます。
   - 感染なし : ファイルがウイルスに感染していないか、ウイルスは駆除されました (ファイルを開くことができます)。
   - 感染 : ファイルがウイルスに感染していて、駆除できません (ファイルへのアクセスは拒否されます)。

ServerProtect for EMC Celerra は、EMC Celerra File Server を保護することを主な目的としています。ServerProtect for EMC Celerra では、ウイルス検索が「オンアクセス」モードで実施され、Windows Server 2008、Windows Server 2012、Windows Server 2016、または Windows Server 2019 が稼働する個別のコンピュータ (AV サーバ) 上で実行されます。この AV サーバが Celerra File Server を保護します。これが、一般サーバの保護を目的とする ServerProtect の通常のバージョンとは異なる点です。

クライアントが Celerra Server でファイルを閉じようとしたり、ファイルの修正や保存を実行しようとすると、Celerra Server の VC クライアントは、AV サーバの CEE に UNC (Universal Naming Convention) パス名を送信することでウイルスチェックを要求します。次に、CEE が ServerProtect に対して、リアルタイム検索モードでファイルを検索するように要求します。

ファイルがウイルスに感染している場合、ServerProtect は指定された処理を実行します。CEE からファイルのウイルスが正常に駆除されたことが報告されると、Celerra File Server は、クライアントにそのファイルへのアクセスを許可するか、または接続されたデータストレージシステムにそのファイルを保存します。

構成の概要

ServerProtect for EMC Celerra は、RPC (リモートプロシージャコール) 経由で Celerra File Serve と通信します。

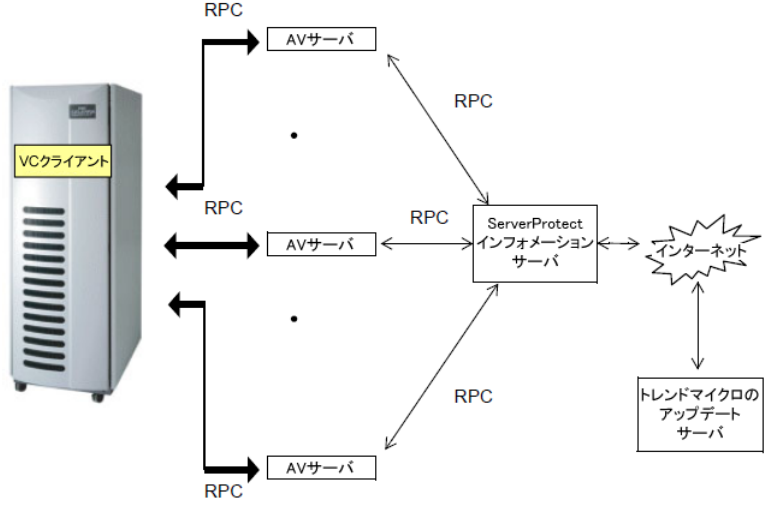


図 1-3.　ServerProtect for EMC Celerra 構成フロー

ServerProtect は次の機能を実行します。

- CEE と連携することで、Celerra File Server の AV サーバになります。
- Celerra File Server 上の VC クライアントに、CEE と ServerProtect がインストールされていて、リアルタイム検索サービスが動作していることを通知します。
- VC クライアントからのファイル検索リクエストを監視します。
- CEE から VC クライアントに検索結果を返すようにします。
- パターンファイルや検索エンジンのアップデートについて VC クライアントに通知します。
- VC クライアントと通信して、AV サーバと Celerra File Server との間の接続状態を確認します。
- VC クライアントと連携して、ラウンドロビン方式で複数の AV サーバに負荷を分散します。

EMC Celerra の特別な機能

ユーザが Celerra File Server 上のファイルにアクセスしようとすると、AV サーバは検索リクエストを受信します。次に、AV サーバは、ServerProtect のリアルタイム検索機能を使用してファイルを検索します。Celerra File Server システムと AV サーバの両方を保護するために、ServerProtect のリアルタイム検索機能の初期設定は「入出力ファイル」になっています。

この設定は変更しないことを強くお勧めします。リアルタイム検索の詳細については、104 ページの「リアルタイム検索」を参照してください。ファイルがウイルスに感染している場合、事前に設定された内容に応じて、AV サーバは次のいずれかの処理を実行します。

- **放置** : リアルタイム検索で、修正処理を実行せずファイルをそのままにします (後述の警告を参照してください)。
- **削除** : 感染したファイルを削除します。
- **拡張子変更** : ファイルの拡張子を「.VIR」に変更して、感染したファイルの名前を変更します。
- **ウイルス駆除** : 検出されたファイルからウイルスコードを取り除きます。
- **隔離** : 感染したファイルを指定されたフォルダに移動します。

警告 : ウイルス駆除、削除、および隔離の処理のみ使用することをお勧めします。放置は選択しないでください。ファイルがウイルスに感染した場合、ウイルスの処理に放置が設定されていると、ウイルスに感染したままのファイルが Celerra File Server システムに入ることになります。

リアルタイム検索と手動検索 (ScanNow)

ServerProtect では、リアルタイム検索と手動検索 (ScanNow) という異なる方法のウイルス検索により、強力なウイルス対策を実現しています。

リアルタイム検索は、サーバ上のすべての入力ファイル、出力ファイルを監視し、ウイルスの侵入をリアルタイムで検出します。詳細については、104 ページの「リアルタイム検索」を参照してください。

手動検索は、ウイルスに感染したと思われるサーバや、すぐに確認を必要とするサーバをチェックする場合に効果的です。詳細については、108 ページの「手動検索 (ScanNow)」を参照してください。

ヒント： ウイルス対策効果を高めるため、リアルタイム検索と手動検索 (ScanNow) を併用していただくことをお勧めします。

リアルタイム検索および手動検索 (ScanNow) には次の特長があります。

- **相互補完**：ウイルスを含むファイルが誤ってダウンロード、またはコピーされようとした場合、リアルタイム検索によってウイルスが検出されます。何らかの理由でリアルタイム検索が停止されていた場合は、手動検索 (ScanNow) を実行することにより、ウイルスを検出することができます。
- **効率的なファイル検索**：特定のファイルタイプが検索対象になるように設定し、システムリソースへの影響を最小限に抑えることができます。詳細については、100 ページの「ウイルス検索」を参照してください。
- **効率的で柔軟なファイル検索**：ServerProtect では、管理者に多様な検索オプションを用意しており、それぞれの環境に適切なウイルス対策設定を可能にします。詳細については、100 ページの「ウイルス検索」を参照してください。

タスクの使用

ServerProtect では複数のタスクを自由に作成し、必要なときに実行することができます。自動的にタスクが開始されるように予約することもできます。

次のような用途でタスクを使用することができます。

- アップデートファイルの配信
- リアルタイム検索の実行
- ScanNow の実行
- ログの削除 / 出力 / 印刷
- ウイルス検索の統計

ServerProtect のタスクには、次のような利点があります。

- 複数のジョブの各一般サーバへの同時展開
- ネットワーク上のウイルス対策保守作業の自動化
- ウイルス対策管理の効率化およびウイルス対策ポリシー管理の強化

タスクはタスクの管理を担当する「所有者」に割り当てられます。詳細については、83 ページの「タスクの管理」を参照してください。

ServerProtect サーバをインストールすると、「ScanNow」、「統計の実行」、「配信」の 3 つの初期設定のタスク (デフォルトのタスク) が自動的に作成されます。この 3 つのタスクは、ネットワークのウイルス対策管理に不可欠です。初期設定のタスクについて、実行先のサーバを変更したり、定義内容を編集することも可能です。

ウイルスを検出した場合

ServerProtect では、ウイルスが検出されたファイルに対する処理を選択できます。特定の種類のウイルスに対応するために、処理を自由に選択できます。ダメージクリーンナップエンジンは、Generic Clean 機能が追加されたことで、より強力になっています。

処理には、次の 5 種類があります。

- **放置 (手動処理)**: 手動検索で、処理を実行せずファイルをそのままにします。ただしウイルスが検出されたことはログエントリとして記録されます。リアルタイム検索では、検索対象が「出力ファイル」または「入出力ファイル」の場合、ServerProtect は検出されたファイルを「書込み禁止」として扱い、ファイルの複製や変更ができないようにします。詳細については、101 ページの「ウイルスに対する処理の設定」を参照してください。
- **削除** : 検出されたファイルを削除します。
- **拡張子変更** : 検出されたファイルの拡張子を変更し、ファイルを実行したり開いたりできないようにします。初期設定では拡張子は「.vir」に変更されます。既に「.vir」が存在する場合は、「.v01」、「.v02」のように変更されます (「.v99」まで)。
- **隔離** : 指定した隔離ディレクトリに、検出されたファイルを移動します。また、隔離したファイルの拡張子を変更して、誤って開いたり実行したりできないようにすることも可能です。
- **ウイルス駆除** : 検出されたファイルからウイルスコードを取り除きます。まれに駆除過程でファイルが壊れる場合があります。駆除前に [Backup infected file before cleaning] オプションを選択して、ファイルのバックアップコピーを自動的に作成しておくことをお勧めします。

ウイルスに関するすべてのイベントと処理については、ログファイルに記録されます。詳細については、101 ページの「ウイルスに対する処理の設定」、またはオンラインヘルプの「ログ情報の表示」トピックを参照してください。

注意 : [Clean] を選択する場合、駆除できなかった場合の処理も指定してください。

注意： 「トレンドマイクロの推奨処理」を使用した場合、スパイウェアに感染したファイルに適用される処理の実際の効果は「放置」と同じものになります。隔離処理を行いたい場合は、検索処理をカスタマイズしてください。

ログと検索結果

ネットワーク上のウイルス対策ポリシーに関する情報を、管理コンソールを使用して一元的に記録、表示できる機能は、ウイルス対策集中管理システムならではの特長といえます。ネットワーク管理者にとって、サーバを監視しながらこのような情報に簡単にアクセスできることは非常に便利です。

ServerProtect では、ウイルス検索およびアップデート / 配信に関する総合的な情報を管理者に提供します。これらの情報は、参照 / 出力用にログファイルとして保存されます。たとえば最も検出数の多いウイルスは何か、ネットワークにウイルスを頻繁に侵入させたユーザはだれかなど、ネットワーク上のウイルス検索についての統計を分析することができます。またログ情報をデータベースや表計算ソフトに書き出して、詳細に分析することができます。

ServerProtect では、一般サーバのログデータベースファイルの初期設定サイズが 10MB に制限されています。この制限値を超えたり所定の日数が経過すると、ログファイルのバックアップが実行されます。初期設定のサイズは 10,000 エントリで、最大で 10MB までになっています。いずれかの制限を超えた場合、既存のログファイルは自動的に別のファイル名に変更され、新規にログファイルが作成されます。ただし、ServerProtect では、日数が設定されていなければ経過日数制限は適用されません。ログファイルのバックアップの設定の詳細については、オンラインヘルプの「ログデータベースのバックアップオプションの設定」を参照してください。

検索結果画面では、検出された感染ファイルに対して処理を直接実行できるため、ウイルス感染が起こった場合に便利です。ログファイルの詳細については、ServerProtect 管理コンソールから ServerProtect のオンラインヘルプを参照してください。ウイルスログの詳細については、オンラインヘルプの「ログ情報の表示」および「インフォメーションサーバログの表示」を参照してください。

アップデート / 配信

ServerProtect は、最新版のコンポーネント (パターンファイル、検索エンジン、プログラム) をダウンロード / 配信するためのアップデート機能を実装しています。日々増え続ける新種ウイルスに対応し、効果的なウイルス対策を実施するには、最新のウイルスパターンファイルおよび検索エンジンを使用することが重要です。ServerProtect ではウイルス対策に不可欠なアップデートを簡単に実行できます。詳細については、70 ページの「アップデートの設定」を参照してください。

注意： トレンドマイクロでは、アップデートファイルを随時リリースしています。定期的に更新し、常に最新版をお使いください。

ServerProtect のアップデート機能には、次の特長があります。

- **コンポーネントのアップデート** : ServerProtect には、アップデート用のさまざまなウイルス対策ユーティリティが用意されています。これには、新しく追加されたスパイウェアパターンファイルとウイルスパターンファイル、ダメージクリーンナップエンジンとダメージクリーンナップテンプレート、ルートキット対策ドライバなどがあります。
- **アップデートの自動化** : 一連のアップデート作業を定期的に実行するタスクを作成することで、アップデートを自動化することができます。
- **柔軟なファイルダウンロード** : トレンドマイクロのアップデートサーバからのダウンロードをインフォメーションサーバが実行し、他のサーバがインフォメーションサーバからアップデートファイルを取得するように設定できます。
- **集中配信** : 管理コンソールを使用してネットワーク上の各サーバにアップデートファイルを配信することができます。
- **ファイアウォールおよびプロキシサーバへの対応** : ServerProtect は、主要なファイアウォールおよびプロキシサーバと共存できます。
- **ログ情報** : アップデート処理に関するログが記録され、必要なときに参照できます。
- **ロールバック** : 配信したアップデートファイルで問題が生じた場合、コンポーネントを配信前のバージョンに戻すことができます。ロールバック処理は、プログラムバージョン、ウイルスパターンファイルおよびウイルス検索エンジンでのみ実行できます。

ServerProtect では、アップデートを次の 2 段階の手順で実行します。

1. トレンドマイクロのアップデートサーバからアップデートファイルをダウンロードします。詳細については、73 ページの「アップデートファイルのダウンロード」を参照してください。
2. ダウンロードしたアップデートファイルをネットワーク上の一般サーバへ配信します。詳細については、79 ページの「アップデートファイルの配信」を参照してください。

この効率的な方法により、ダウンロード時間およびネットワーク帯域幅の使用を節約しています。

ヒント： 予約アップデートタスクを作成することで、アップデートを自動化することができます。詳細については、85 ページの「新規タスクの作成」を参照してください。

ウイルス検出技術

ServerProtect で採用している、高度なウイルス検出技術について説明します。

パターンマッチング

既存のウイルスパターン (個々のウイルスに特有な特徴) を識別するために、ServerProtect ではパターンマッチングと呼ばれる方法を駆使して、ウイルスパターンの広範なデータベースと検索対象ファイルを照合します。感染が疑われるファイルでは、ファイルの主要部分について、ウイルスコードに該当する文字列がないかどうか、トレンドマイクロが蓄積してきたウイルスパターン情報と比較されます。

ポリモーフィック型 (ミューテーション型) のウイルスについては、ウイルスに感染していると思われるファイルを、テンポラリ領域で復号化し、実行します。ServerProtect では、復号化されたコードを含むファイル全体から、ポリモーフィック型ウイルスの文字列を検索します。

ウイルスが検出された場合、ServerProtect は、あらかじめユーザが定義した処理を実行します。ServerProtect が実行する処理には、ウイルス駆除、削除、放置 (手動処理)、隔離、拡張子変更があります。処理の設定では、システム領域感染型およびファイル感染型のウイルスでそれぞれ異なる内容を指定することができます。詳細については、100 ページの「ウイルス検索」を参照してください。

注意： 日々増え続ける新種ウイルスに対応し、効果的なウイルス対策を実施するため、パターンファイルは常に最新版をお使いください。トレンドマイクロでは、予約アップデートをサポートすることによって、パターンファイルのアップデートを容易にしています。詳細については、80 ページの「予約配信の設定」を参照してください。

MacroTrap

マクロウイルスはオペレーティングシステムではなく、アプリケーションに依存します。そのため MS-DOS、Windows、Macintosh、OS/2 と、使用環境を問わずに感染を拡大します。ServerProtect では、トレンドマイクロの MacroTrap 技術を採用し、マクロウイルスの脅威からネットワークユーザを守ります。MacroTrap の設定の詳細については、104 ページの「検索の設定」を参照してください。

注意： MacroTrap は、ネットワークユーザによるマクロウイルスの受信や送信を防ぎます。

MacroTrap は、ルールベース方式により、文書に保存されているマクロコードを 1 つずつ検査していきます。マクロウイルスのコードは、通常は見えないテンプレートの一部に組み込まれて、ドキュメントと一緒に配信されます (たとえば Microsoft Word の場合 *.dot テンプレートファイル)。MacroTrap は、このテンプレートをチェックして、ウイルスのようなアクションを実行する命令、たとえばテンプレートの一部を他のテンプレートにコピーする命令 (複製) や、害を及ぼすおそれのあるコマンドを実行する命令 (破壊) などを探して、変種 / 亜種のマクロウイルスの存在を突き止めます。

圧縮ファイル

トレンドマイクロの検索エンジンは、圧縮ファイル内のウイルスを検出することができます。ServerProtect では 5 レベル (階層) までの多重圧縮に対応します。6 レベル (階層) 以上圧縮されたファイルは検索できません。

ServerProtect で使用しているトレンドマイクロの VSAPI 検索エンジンで対応する圧縮形式およびエンコード形式には、次の形式が含まれます (このリストは検索エンジンのアップデートに伴って変更される場合があります)。

- PKZIP (.zip) および PKZIP_SFX (.exe)
- LHA (.lzh) および LHA_SFX (.exe)
- ARJ (.arj) および ARJ_SFX (.exe)
- CABINET (.cab)
- TAR
- GNU ZIP (.gz)
- RAR (.rar)
- PKLITE (.exe または .com)

- LZEXE (.exe)
- DIET (.com)
- UNIX PACKED (.z)
- UNIX COMPACKED (.z)
- UNIX LZW (.Z)
- UUENCODE
- BINHEX
- BASE64
- Microsoft Office Open XML形式（.docx、.xlsx、.pptx、.one)

注意： トレンドマイクロの検索エンジンでは、ZIP 形式のファイルの場合、最初の階層 (圧縮ファイルを 1 回解凍して得られるファイル) のウイルスに限り、手動で解凍することなくプログラムにより駆除処理が実行されます。他の圧縮ファイルの場合、ウイルス駆除の前に、ファイルの解凍が必要です。

圧縮ファイル設定の詳細については、104 ページの「検索の設定」を参照してください。

ダメージクリーンナップサービス

ダメージクリーンナップサービス (DCS) は、トロイの木馬を検出し、変更されたシステムファイルを修復します。また、トロイの木馬の関連プロセスを停止させ、トロイの木馬によってシステムに仕掛けられたファイルを削除します。

注意： スパイウェアに感染したファイルが検出された場合、適用できるのは「放置」処理のみです。ファイルは、何の処理も行われずに放置されます。スパイウェア感染に対しては、駆除機能は適用されません。

OLE 埋め込みの検索

Microsoft Office では、OLE と呼ばれる Windows のしくみを利用して、異なるアプリケーションで作成されたデータを 1 つの文書にまとめることが可能です。たとえば Excel で作成したスプレッドシートに Word 文書を埋め込んだり、PowerPoint で作成したプレゼンテーション資料に Excel スプレッドシートを埋め込むことなどができます。

OLE には多くの利点がありますが、ウイルス感染の危険性も無視できません。ServerProtect では、トレンドマイクロのウイルス検索技術により OLE 埋め込みオブジェクトを検索対象とすることができます。詳細については、100 ページの「ウイルス検索」を参照してください。

ヒント： OLE 埋め込みの検索では、1 から 5 までの検索レベルを指定できます。手動検索 (ScanNow) の場合、推奨する検索レベルは 2 です。リアルタイム検索の場合、推奨する検索レベルは 1 です。検索レベルを高くするとサーバのパフォーマンスに影響しますのでご注意ください。

トレンドマイクロの推奨設定

「トレンドマイクロの推奨設定」には、検索対象ファイルをファイルタイプで判断するための設定が含まれます。ウイルス感染の危険がある特定のファイルタイプのみが検索対象となり、すべてのファイルを検索する場合に比べて効率的です。トレンドマイクロの推奨設定では、検索対象ファイルを拡張子だけではなく実際のファイルタイプで判断することができます。

.zip ファイル、.exe ファイルなどの実行ファイルの場合、ファイルタイプはファイルコンテンツによって判断されます。実行ファイルでない .txt ファイルなどの場合、ファイルタイプはファイルのヘッダによって判断されます。詳細については、100 ページの「ウイルス検索」を参照してください。

トレンドマイクロの推奨設定を使用すると、たとえば次のような利点があります。

- **パフォーマンスの最適化**：トレンドマイクロの推奨設定は最低限のシステムリソースしか使用しないため、コンピュータ上の重要なアプリケーションのパフォーマンスに影響しません。
- **検索時間の短縮**：トレンドマイクロの推奨設定はファイルタイプを正しく識別するため、感染の危険があるとされるファイルだけを検索します。そのため、すべてのファイルを検索する場合に比べ、検索時間が大幅に短縮されます。この検索時間の違いは、特に手動検索 (ScanNow) の実行時に顕著になります。

トレンドマイクロの推奨処理

ウイルスの処理または特定のウイルスに対して最適な検索処理が不明な場合は、「トレンドマイクロの推奨処理」を使用することをお勧めします。

ウイルスの種類に応じて検索処理をカスタマイズするにはウイルスの知識が必要となり、場合によっては面倒な作業を伴います。検索処理そのものについてよく分からないとき、またはどの種類のウイルスにどの設定が適しているか判断できないときは、トレンドマイクロの推奨処理を使用することをお勧めします。

トレンドマイクロの推奨処理を使用した場合、次のような利点があります。

- **時間の節約と保守のしやすさ**：トレンドマイクロの推奨処理ではトレンドマイクロが推奨する検索処理が適用されます。このため、検索処理をカスタマイズするための時間を節約できます。
- **更新可能な検索処理**：ウイルスの作成者はウイルスによるコンピュータへの攻撃方法を常に変化させています。ウイルスによる最新の脅威と最新の攻撃方法からコンピュータを保護するため、トレンドマイクロの推奨処理の設定内容は随時見直されます。

トレンドマイクロの推奨処理の設定については、101 ページの「ウイルスに対する処理の設定」を参照してください。

注意： 「トレンドマイクロの推奨処理」を使用した場合、スパイウェアに対する処理は放置 (手動処理) になります。

その他の機能

管理者が、より柔軟にネットワークのウイルス対策を実施できるように、ServerProtect では、次のような機能も用意しています。

集中管理

ServerProtect では、Windows ベースのコンソール (管理コンソール) により、ネットワーク上の複数のサーバに対するウイルス対策を集中管理するための操作環境が用意されています。管理コンソールは 32 ビットまたは 64 ビットの Windows OS で使用できます。詳細は動作要件などをご覧ください。

インストール時のネットワークセキュリティ

一般サーバまたはインフォメーションサーバのインストール時に、インストール先サーバの管理者アカウント情報が要求されます。

ウイルスアウトブレークへの迅速な対応

ServerProtect によって保護されているサーバの共有フォルダにウイルスの侵入が試みられた場合、ネットワーク上の感染源のコンピュータを特定するメッセージボックスが表示されます。このメッセージボックスの情報には、検索の種類、ウイルスの名前、感染したファイルの名前、関連するコンピュータの名前または ID、およびユーザ名なども含まれます。また、検出されたウイルスに対する処理、および感染元についても表示されます。詳細については、94 ページの「通知メッセージの設定」を参照してください。

感染ファイルに対する柔軟な処理

感染ファイルに対する処理のオプションとして、ウイルス駆除前に感染ファイルのバックアップを作成したり、ウイルス駆除されたファイルをメールでユーザに返信するなどの処理を選択することができます。

最新のウイルス検索技術

トレンドマイクロの推奨処理、トレンドマイクロの推奨設定、OLE 埋め込みの検索など、検索速度や効率を向上するための技術が新たに採用されています。

ウイルス検索の統計

ServerProtect では、ウイルス検索結果の各項目について、指定された期間内のネットワーク上の統計を表示することができます。この項目には、感染ユーザ数、感染ファイルの検出数、トップ 10 ウイルス、トップ 10 感染ユーザ、駆除不能ウイルス数、駆除不能ファイル数などがあります。

互換性

ServerProtect は、Microsoft Windows Server 2008、2008 R2、2012、2012 R2、2016、および 2019 の OS に対応しています。また、ServerProtect では、Network File System (NFS) ドライバ、およびトレンドマイクロのアップデートサーバに対しては SOCKS 4 がサポートされます。

ServerProtect では、32 ビットおよび 64 ビットの OS がサポートされます。ServerProtect では、32 ビットおよび 64 ビットの Windows Server が自動的に検出されます。OS が 32 ビットの場合、ServerProtect の 32 ビットバイナリの一般サーバコンポーネントがインストールまたはアンインストールされます。OS が 64 ビットの場合、ServerProtect の 64 ビットバイナリの一般サーバコンポーネントがインストールまたはアンインストールされます。

第 2 章

ServerProtect for EMC Celerra のインストール

本章で説明する内容には、ServerProtect for EMC Celerra を正しくインストールしていただくために必要な次の情報が含まれています。インストールの前によくお読みください。

注意： ServerProtect インフォメーションサーバをインストールするには、管理者権限を持つアカウントでログオンする必要があります。

注意： 古いバージョンの一般サーバをインストールして ServerProtect インフォメーションサーバに登録することはお勧めしません。

システム要件

最新の情報については、次の Web サイトを参照してください。

https://www.trendmicro.com/ja_jp/business/products/user-protection/sps/endpoint/server-protect.html#requirement

注意： システム要件に記載されている OS の種類やハードディスク容量などは、OS のサポート終了、弊社製品の改良などの理由により、予告なく変更される場合があります。

インストール計画

ServerProtect のインストール計画について説明します。インストールを開始する前に、インストールする環境に応じた適切な計画を選択してください。次のインストール計画は、主に LAN 環境で ServerProtect を運用する場合を前提にしています。WAN 環境での運用を予定している場合の詳細については、37 ページの「WAN 接続のネットワーク」を参照してください。

インストール環境の特定

本バージョンの ServerProtect では、Microsoft Windows プラットフォームがサポートされます。初めて ServerProtect をインストールする場合は、先にインフォメーションサーバをセットアップし、その管理下に一般サーバをセットアップしてください。インフォメーションサーバは、一般サーバを管理する上で必ず 1 つ以上の ServerProtect ドメインを必要とします。

注意： 広範囲の場所に多数のサーバを配置している場合、拠点ごとにインフォメーションサーバをセットアップしてください。

Microsoft Windows プラットフォームの各環境でインストール可能な ServerProtect コンポーネントは次のとおりです。

表 2-1.　Microsoft Windows 環境でのインストール

OS	インフォメーション サーバ	一般 サーバ	管理 コンソール
Windows Server 2008 ファミリ　(32 ビット)	○	○	○
Windows Server 2008 ファミリ　(64 ビット)	○ (WOW64)	○	○ (WOW64)
Windows Server 2008 Core　(32 ビット)	×	○	×
Windows Server 2008 Core　(64 ビット)	×	○	×
Windows Server 2008 R2 ファミリ	○ (WOW64)	○	○ (WOW64)
Windows Server 2012 ファミリ	○ (WOW64)	○	○ (WOW64)
Windows Server 2012 R2 ファミリ	○ (WOW64)	○	○ (WOW64)
Windows Server 2016 ファミリ	○ (WOW64)	○	○ (WOW64)
Windows Server 2019 ファミリ	○ (WOW64)	○	○ (WOW64)
Windows 8 デスクトップファミリ	×	×	○

注意： Windows 8 デスクトップファミリとは、Windows 8、Windows 8 Pro、および Windows 8 Enterprise を指します。

Windows Server 2008 ファミリおよび Windows Server 2008 R2 ファミリはどちらも、Standard、Enterprise、Datacenter の各エディションおよび Storage Server を指します。

Windows Server 2012 ファミリおよび Windows Server 2012 R2 ファミリはどちらも、Standard、Essentials、Foundation、Datacenter の各エディションおよび Storage Server を指します。

Windows Server 2016 ファミリとは、Standard、Essentials、Datacenter の各エディションおよび Storage Server を指します。

Windows Server 2019 ファミリとは、Standard、Essentials、Datacenter の各エディションおよび Windows Server IoT 2019 を指します。

注意： Hyper-V は、Windows Server 2008 および Windows Server 2012 でサポートされます。

ServerProtect コンポーネントによって使用されるポート番号

ここでは、ファイアウォールの設定について説明します。ServerProtect コンポーネントをインストールする前に、ファイアウォールが適切に設定されていることを確認してください。

管理コンソールがインストールされているコンピュータ向けのファイアウォール設定

1000 ～ 1009 番ポート (TCP) は、管理コンソールでインフォメーションサーバからのイベントメッセージの受信に使用されます。

管理コンソールは、起動時にポート 1000 を待ち受けます。このポートが特定のプログラムで使用されている場合、管理コンソールでは 1001 ～ 1009 で空いているポートが 1 つ使用されます。

- 1000 ～ 1009 番 (TCP) もしくは、1001 ～ 1009 番の間の空いているポートいずれか。

インフォメーションサーバによって使用されるポート番号

5005 番ポート (TCP) は、管理コンソールからのコマンドの受信に使用されます。もしポート 5005 が特定のプログラムで使用されている場合、ServerProtect は自動的に 5006 ～ 5014 番の間で空いているポートを探します。

3000 番ポート (UDP) は、ブロードキャストメッセージの受信に使用されます。ポート 3000 が特定のプログラムで使用されている場合、3001 ～ 3009 番の間で空いているポートが使用されます。

- 5005 番 (TCP) もしくは、5006 ～ 5014 番の間の空いているポートいずれか
- 3000 番 (UDP) もしくは、3001 ～ 3009 番の間の空いているポートいずれか
- 137 番 (UDP) (名前付きパイププロトコル経由の RPC を使用する場合)
- 138 番 (UDP) (名前付きパイププロトコル経由の RPC を使用する場合)
- 139 番 (TCP) (名前付きパイププロトコル経由の RPC を使用する場合)
- 445 番 (TCP) (名前付きパイププロトコル経由の RPC を使用する場合)
- 3628 番 (TCP) (イベントメッセージの受信用)
- 10319 番 (TCP) (Control Manager エージェントを使用する場合)

一般サーバがインストールされている Windows コンピュータのファイアウォール設定

インフォメーションサーバからのコマンドを受信できるように設定してください。使用する通信方法によって必要なポートが変わります。

- 5168 番 (TCP) (TCP/IP 経由の RPC の場合)
- 137 番 (UDP) (名前付きパイプの場合)
- 138 番 (UDP) (名前付きパイププロトコル経由の RPC を使用する場合)
- 139 番 (TCP) (名前付きパイププロトコル経由の RPC を使用する場合)
- 445 番 (TCP) (名前付きパイププロトコル経由の RPC を使用する場合)

WAN 接続のネットワーク

必要なネットワークパフォーマンスを確保するため、ネットワークセグメントごとにインフォメーションサーバを配置することをお勧めします。

管理コンソールはインフォメーションサーバとの通信に TCP/IP を使用します。イントラネットでは、任意の接続ポイントから簡単に ServerProtect を管理することができます。

ServerProtect のインストール

ServerProtect が全く導入されていない環境では、まず管理コンソール、インフォメーションサーバ、一般サーバプログラムを一括してインストールすることをお勧めします。

ここでは、ServerProtect のインストール手順について説明します。一般サーバと他のウイルス対策ソフトが共存している環境はサポートされません。他のウイルス対策ソフトが先にインストールされている場合には、必ず事前にアンインストールしてください。

インストールを開始する前に

他のサーバソフトウェアと同様、ServerProtect のインストールやアップグレードは、業務時間外などユーザへの影響が少ない時間帯に、データのバックアップを作成した上で実行することをお勧めします。ネットワークへのインストールを実行する前に、関連するサーバコンピュータ間のネットワーク接続が確立されていることを確認してください。

また、プログラムをまずテストサーバにインストールすることをお勧めします。これによって、実環境のサーバにインストールする前にインストールの問題点を解決できます。インストールする前に詳細については、34 ページの「インストール計画」を参照してください。

注意： ServerProtect をインストールするには、管理者権限を持つアカウントでログオンする必要があります。

ServerProtect パッケージのインストール

管理コンソール、インフォメーションサーバ、一般サーバを含む ServerProtect パッケージをインストールするには、Windows プラットフォームコンピュータでセットアッププログラムを実行してください。

注意： システム共有 (c$ など) が有効になっていない場合、インストールに失敗します。一時的に有効にしてください。

ServerProtect をインストールするには、次の手順に従ってください。

1. ServerProtect の CD-ROM を CD-ROM ドライブに挿入し PROGRAM フォルダ内にある SPEMC58.exe を実行します。ServerProtect セットアッププログラムの初期画面が表示されます。

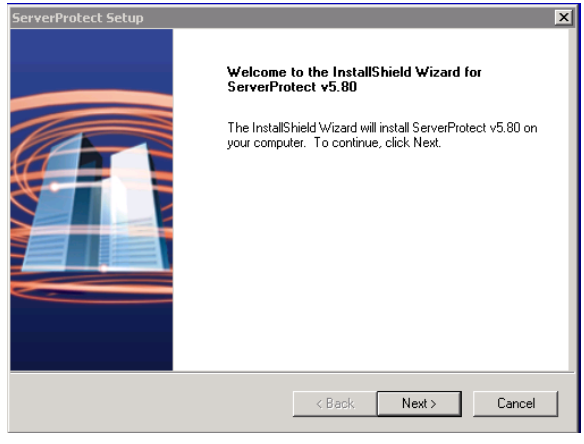


図 2-1. ServerProtect セットアップの初期画面

[Next] をクリックします。

2. 使用許諾契約書が表示されます。セットアップを続行するには、使用許諾契約に同意していただく必要があります。

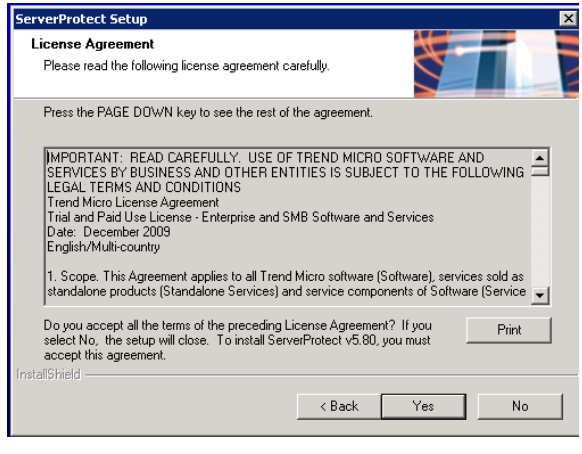


図 2-2. 使用許諾契約書

[Yes] をクリックします。

3. セットアッププログラムにより、ローカルのシステム領域のウイルス検索が実行されます。

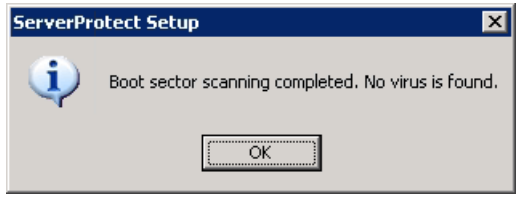


図 2-3.　ウイルス検索の結果

[OK] をクリックしてセットアップを続行します。

4. [User Information] ダイアログボックスが表示されます。

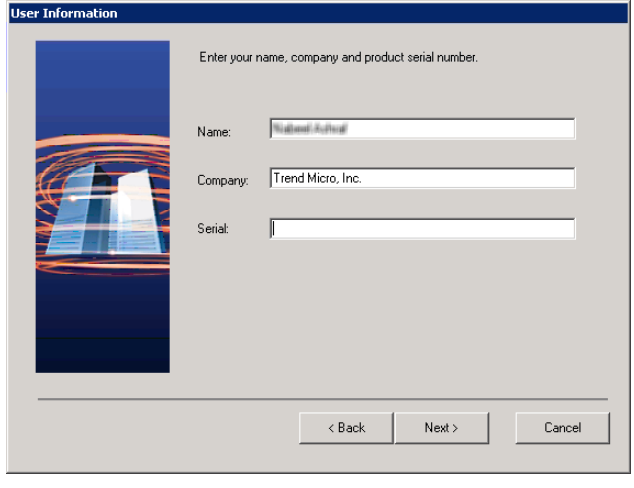


図 2-4.　ユーザの情報

5. ユーザ情報および製品のシリアル番号を入力します。

   シリアル番号がない場合は、空白のままセットアップを続行することができます。シリアル番号を入力しない場合は 30 日体験版としてインストールされます。間違ったシリアル番号を入力すると、「間違ったシリアル番号が入力されたので再試行してください」という意味のメッセージが表示されます。

6. [Select Components] ダイアログボックスが表示されます。

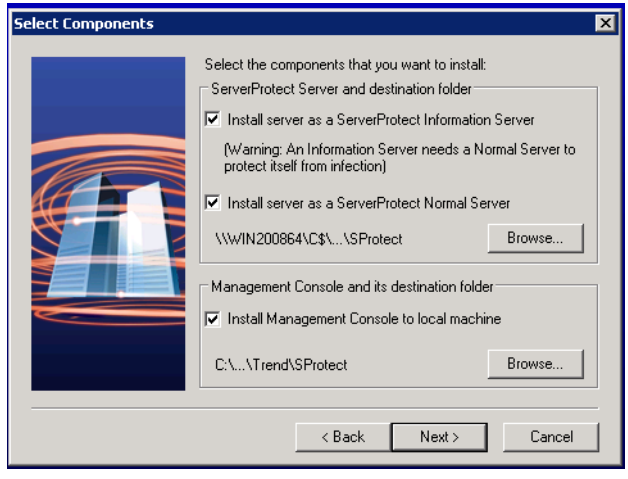


図 2-5.　コンポーネントの選択

7. ServerProtect のパッケージ一式をインストールするには、すべてのチェックボックスをオンにします。

   一般サーバをインストールする場合、インストールする検索プログラムの種類を選択する必要があります。EMC VNX/VNXe を保護する場合は、[EMC CAVA] を選択します。インストールするコンポーネントを選択します。インストール先フォルダとして隠しシステム共有ドライブ (**C$**、**D$** など) を選択できます。

   初期設定のインストールパスは次のとおりです。

   ```
   <ドライブ>:¥Program Files¥Trend¥SProtect
   ```

   [Next] をクリックします。

注意： インフォメーションサーバのインストール先コンピュータ上でウイルス対策を実施するため、同一コンピュータ上に一般サーバをインストールすることをお勧めします。

---

8. ポップアップダイアログで [Yes] をクリックし、一般サーバのインストールを続行します。
9. [Next] をクリックします。一般サーバまたはインフォメーションサーバのインストールを選択した場合、[Input Logon Information] ダイアログボックスが表示されます。

   [Logon Information] の [Domain name]、[User name]、[Password] および [Confirm Password] テキストボックスにそれぞれのデータを入力し、[Next] をクリックしてください。

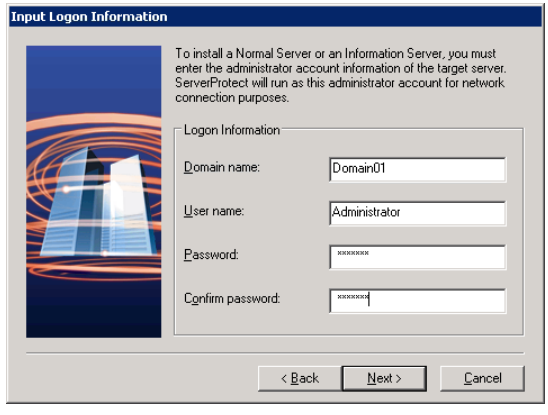


図 2-6. ログオン情報の入力

10. 1 回のセットアップでインフォメーションサーバ、一般サーバ、管理コンソールの 3 つのコンポーネントをインストールする場合は、図 2-5 にあるチェックボックスすべてを ON にします。それ以外の場合は、インストールするコンポーネントのチェックボックスだけを ON にします。各コンポーネントのインストールについては、次の「管理コンソールのインストール」、「インフォメーションサーバのインストール」、「一般サーバのインストール」を参照してください。

インフォメーションサーバのインストール

インフォメーションサーバは、管理コンソールからのコマンドを実行します。また、インフォメーションサーバドメイン単位で一般サーバを管理します。

インフォメーションサーバをインストールするには

1. セットアッププログラムを起動し、前述の各コンポーネント共通の手順を実行します。
2. [Select Components] 画面で、[Install server as a ServerProtect Information Server] チェックボックスをオンにします（詳細については、41 ページの「コンポーネントの選択」を参照してください)。

3. インフォメーションサーバのインストール先のサーバ / フォルダを指定するには、[Browse] ボタンをクリックします。

   [ServerProtect Install Path Selection] 画面が表示されます。

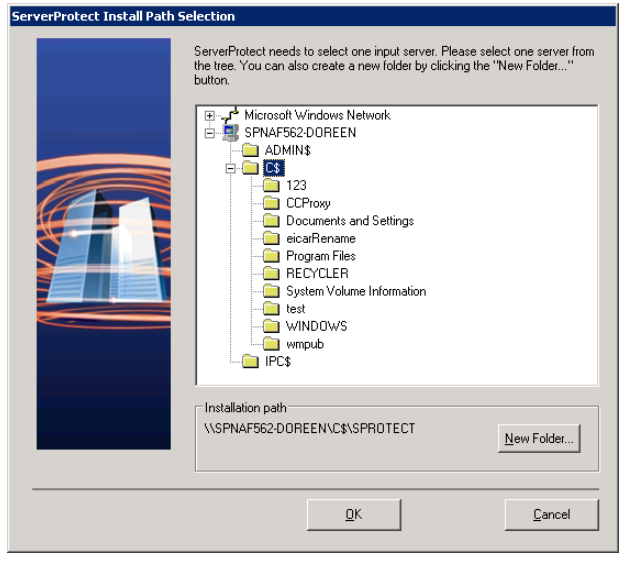


図 2-7.　ServerProtect インストール先の選択

4. サーバツリーから対象サーバをダブルクリックし、ServerProtect インフォメーションサーバファイルのインストールパスを選択します。新しいフォルダにインストールしたい場合は、[New Folder] ボタンをクリックします。[OK] をクリックして、[Select Components] 画面に戻ります　(詳細については、41 ページの「コンポーネントの選択」を参照してください)。

5. [Next] をクリックします。[Input Logon Information] 画面が表示されます。[Logon Information] の [Domain name]、[User name]、[Password]、および [Confirm Password] テキストボックスに有効なデータを入力し、[Next] をクリックしてください。[Setup Information Server] 画面が表示されます。

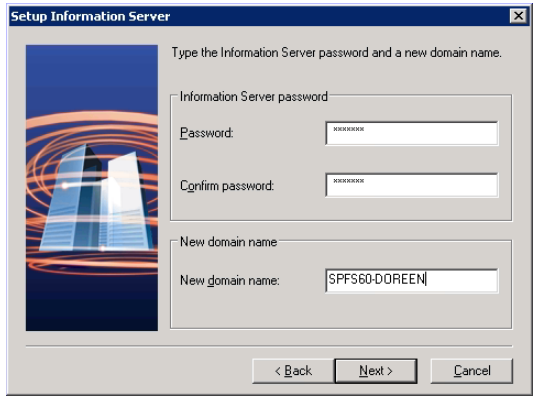


図 2-8.　インフォメーションサーバのセットアップ

6. インフォメーションサーバのパスワードを入力し、要求に応じてパスワードを確認します。このパスワードによって、管理コンソールからインフォメーションサーバへ接続しようとする場合に、不正なアクセスを防止することができます。
7. [Next] をクリックします。[Start Copying Files] ダイアログボックスが表示されるので、その内容を確認します。

8. 正しければ [Next] ボタンをクリックしてセットアップを続行します。内容を修正する場合は [Back] ボタンをクリックして戻ります。セットアッププログラムにより、ファイルのコピーが開始されます。すべてのファイルがコピーされ、サービスが正常に起動すると、[ServerProtect Setup] 画面が表示されます。

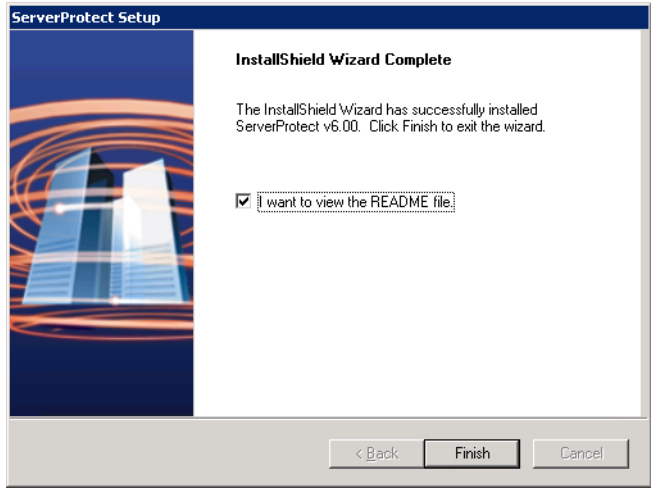


図 2-9.　セットアップの完了

9. [Finish] をクリックしてセットアッププログラムを終了します。

管理コンソールのインストール

管理コンソールのインストール先は、他のコンポーネントのインストール先と同じコンピュータでも別のコンピュータでも構いません。

管理コンソールをインストールする場合は、次の手順に従ってください。

1. セットアッププログラムを起動し、前述の各コンポーネント共通の手順を実行します。
2. [Select Components] ダイアログボックスで [Install Management Console to local machine] チェックボックスをオンにします (図 2-5 参照)。[Browse] ボタンをクリックしてインストールパスを変更することができます。管理コンソールは、Windows Storage Server 環境にインストールする必要があります。

注意： 現在、管理コンソールのリモートインストールはサポートされていません。

---

3. Windows の [スタート] メニューに自分がログオンした場合にのみ ServerProtect プログラムを表示する場合は、[Personal program folder] を選択します。それ以外の場合は [Common program] を選択します。
4. [Next] をクリックします。[Select Program Folder] ダイアログボックスが表示されます。
5. プログラムのインストール先フォルダを選択し、[Next] をクリックします。

   [Start Copying Files] ダイアログボックスが表示されるので、その内容を確認します。
6. 正しければ [Next] ボタンをクリックしてセットアップを続行します。内容を修正する場合は [Back] ボタンをクリックして戻ります。セットアッププログラムにより、ファイルのコピーが開始されます。
7. すべてのファイルがコピーされると、[ServerProtect Setup] 画面が表示されます。このダイアログボックスには 2 つのオプションがあります。1 つは Readme ファイルを表示するオプション、もう 1 つは ServerProtect 管理コンソールを起動するオプションです。

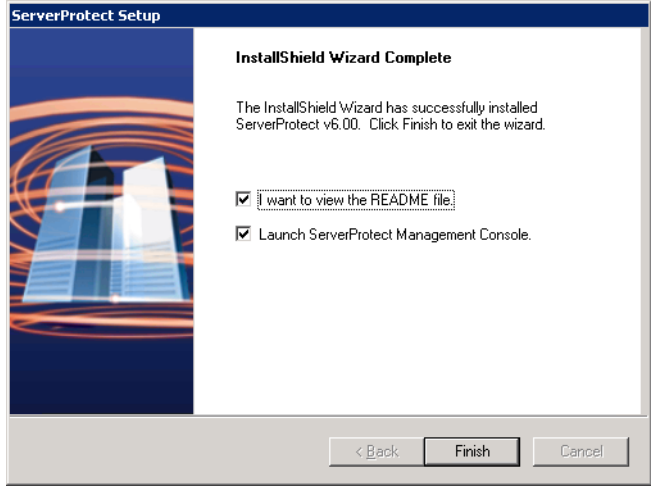


図 2-10. セットアップの完了

[Finish] をクリックしてセットアップを終了します。

8. 管理コンソールに接続するインフォメーションサーバを選択するための画面が表示されます (インフォメーションサーバと同一のコンピュータ上に管理コンソールをインストールした場合は表示されません)。

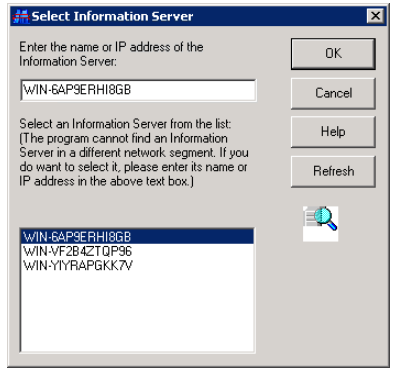


図 2-11. インフォメーションサーバ選択

9. 次のいずれかの操作を実行してインフォメーションサーバを指定します。
   - リストからサーバを選択する
   - テキストボックスにサーバ名を入力する
   - テキストボックスに IP アドレスを入力する

注意： ServerProtect がインストールされているネットワークとは異なるネットワークセグメントに対象となるサーバが含まれる場合、そのサーバはリストに表示されません。

---

10. [OK] をクリックして変更内容を保存します。

一般サーバのインストール

一般サーバを初めてインストールする場合、セットアッププログラムから実行します。既に一般サーバがインストールされている環境に、追加で一般サーバをインストールする場合は、管理コンソールを使用することができます。

セットアッププログラムからの一般サーバのインストール

セットアッププログラムからは、一般サーバをローカルまたはリモートでインストールすることができます。Microsoft Windows の一般サーバのインストール手順について説明します。

セットアッププログラムから Windows 一般サーバをインストールするには

1. セットアッププログラムを起動し、前述の各コンポーネント共通の手順を実行します。
2. [Select Components] 画面 (図 2-5 参照) で [Install server as a ServerProtect Normal Server] チェックボックスをオンにします。

   一般サーバのインストール先のサーバ / フォルダを指定するには、[Browse] ボタンをクリックします。
3. [ServerProtect Install Path Selection] 画面が表示されます。

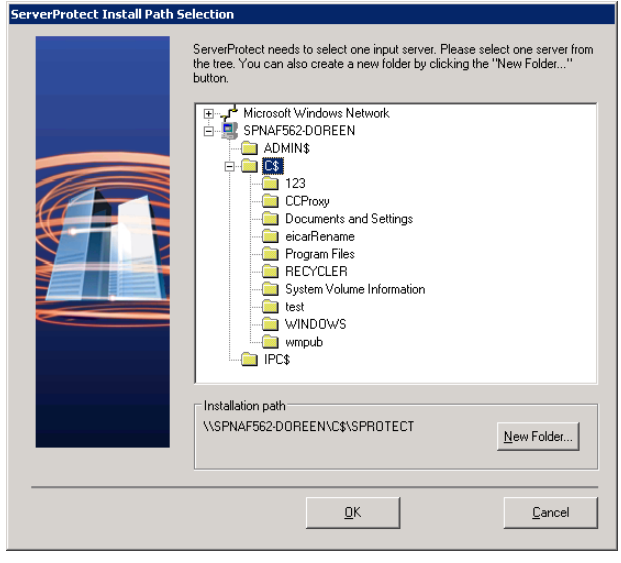


図 2-12. Windows Server でのインストール先の選択

   サーバツリーを展開し、インストール先のサーバを選択します。
   対象サーバをダブルクリックします。
4. 選択したサーバのローカルドライブがツリーに表示されます。

   一般サーバのインストールパスを指定し、[OK] をクリックします。インストールパスを新しいフォルダに変更したい場合は、[New Folder] ボタンをクリックして [OK] をクリックします。
5. [Select Components] ダイアログボックス (図 2-5 参照) で [Next] ボタンをクリックします。
6. [Select Component] 画面の [Next] をクリックします。
7. [Input Logon Information] 画面が表示されます。

8. ログオン情報を、[Domain name]、[User name]、[Password] および [Confirm Password] テキストボックスにそれぞれ入力します。
9. [Next] をクリックします。[Select Information Server] 画面が表示されます。

図 2-13. [Select Information Server] 画面

10. 次のいずれかの操作を実行してインフォメーションサーバを指定します。
    - テキストボックスにインフォメーションサーバの名前または IP アドレスを入力し、[Find Server] をクリックします。
    - ブラウザツリーでインフォメーションサーバのインストール先サーバをダブルクリックします。

注意： ServerProtect がインストールされているネットワークとは異なるネットワークセグメントにインストール先サーバがある場合、そのサーバがリストに表示されないことがあります。その場合、サーバ名または IP アドレスを入力してください。

---

11. [Input ServerProtect InformationServer password] ダイアログボックスが表示されます。

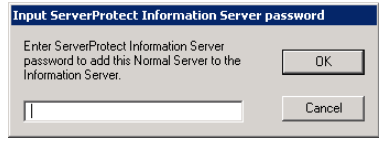


図 2-14. ServerProtect インフォメーションサーバパスワードの入力

12. インフォメーションサーバのパスワードを入力し、[OK] をクリックします。このパスワードは、インフォメーションサーバのインストール時に指定したパスワードです。
13. ServerProtect ドメインを新規作成するには、[New Domain] をクリックします。[Name] に作成するドメインの名前を入力し、[OK] をクリックしてください。

    インフォメーションサーバにドメインが作成されていない場合、次の手順に進むことができません。

    [Next] をクリックします。[Start Copying Files] ダイアログボックスが表示されるので、その内容を確認します。
14. 正しければ [Next] ボタンをクリックしてセットアップを続行します。内容を修正する場合は [Back] ボタンをクリックして戻ります。セットアッププログラムにより、ファイルのコピーが開始されます。ファイルがすべてコピーされ、サービスが正常に起動すると、[ServerProtect セットアップ] 画面が表示されます (図 2-11 参照)。
15. [Finish] をクリックします。ServerProtect のアイコン () が Windows のタスクトレイに追加されます (このアイコンは、検索プログラムが起動していることを示します)。

管理コンソールからの一般サーバのインストール

この時点では、管理コンソールがログオンしているインフォメーションサーバは既に少なくとも 1 つの一般サーバを管理していると想定されます。このサーバは、新しい一般サーバをインストールする際の実行元サーバとして使用されます。そのため、インストールするサーバと同じ種類のサーバである必要があります。ドメイン内に初期設定の実行元サーバと同じ種類の一般サーバがある場合、それが選択されます。

管理コンソールから Microsoft Windows 一般サーバをインストールするには

注意： 管理コンソールから Windows 一般サーバをインストールする場合、実行元サーバとインストールするサーバの OS が同じプラットフォームであることを確認します。たとえば、実行元サーバの OS が 32 ビットの場合は、インストールするサーバの OS も 32 ビットである必要があります。

インストール先サーバに ServerProtect が既にインストールされていないことを確認します。

1. ドメインブラウザツリーから、サーバの追加先ドメインを選択します。次のいずれかの操作を実行してください。
   - メインメニューから [Domain] → [Install New (s)] の順に選択します。
   - 手順 1 で選択したドメインを右クリックし、[Install New (s)] を選択します。
2. ファイルのコピー元となる既存の一般サーバ (実行元サーバ) をリストから選択し、[OK] をクリックしてください。

   実行元サーバとして選択できるのは、インストールする一般サーバと同じ種類の一般サーバのみです。インストールする一般サーバと同じ種類の既存の一般サーバが 1 台のみの場合、実行元サーバとして自動的に選択されます。
3. 確認のダイアログボックスが表示されたら、[OK] をクリックします。[Add Server (s) to Domain] 画面が表示されます。
4. 次のいずれかの操作を実行して、ドメインに追加するサーバを選択します。
   - 左のリストボックスでサーバ名を選択します。
   - [Server name] テキストボックスにサーバ名を入力します。
   - [Add] ボタンをクリックしてサーバ名を右のリストボックスに表示させます。
5. 新しいドメインに追加するサーバがすべて右のリストボックスに表示されるまでステップ 4 を繰り返します。既に追加したサーバを削除する場合は、その名前を右のリストボックスで選択し、[Remove] をクリックします。[Remove All] をクリックすると、右のリストボックス内のサーバがすべて削除されます。
6. 変更内容を保存するには、[OK] をクリックし、サーバを追加せずに画面を閉じるには、[Cancel] をクリックします。

サイレントモードでのインストール

Microsoft Windows 環境での一般サーバのリモートインストールにサイレントモードを使用することができます。

Windows 環境でサイレントモードを使用して ServerProtect をインストールするには

1. インフォメーションサーバをインストールします。詳細については、42 ページの「インフォメーションサーバのインストール」を参照してください。
2. インフォメーションサーバのインストールディレクトリ配下の SMS フォルダを共有します。

   注意： 読み取りおよび書き込み権限のある SMS フォルダを共有します。

   インストール先のサーバからこのフォルダにアクセス可能であることを確認してください。複数のサイレントインストールを実行したい場合、インストール先のサーバ上で SMS フォルダを割り当てます。
3. インストール先のサーバでコマンドプロンプトを起動し、割り当て済みの SMS フォルダまたはドライブに移動し、次のコマンドを入力します。

   ```
   < ドライブ名 >:¥setup -SMS -s -m"SPEMC"
   ```

例 (ドライブ「M」にマップする場合の手順)

a. インストール先サーバで、SMS フォルダをドライブ「M」に割り当てます。
b. コマンドプロンプトを起動します。
c. 「M:」と入力し、M ドライブに移動します。
d. 次のように入力します。

   ```
   M:¥setup -SMS -s -m"SPEMC"
   ```

e. <Enter> キーを押します。

サイレントインストールが実行され、インストール先のサーバがインフォメーションサーバに登録されます。

サイレントインストールでは、一般サーバは「SMS」ドメインにインストールされます。この時点でドメイン名を変更することはできませんが、すべての一般サーバのインストールが完了した後、「SMS」以外のドメイン名に変更することができます。

ServerProtect のインストール先のパスを指定することもできます。たとえば、「D:¥Utility¥AntiVirus¥SProtect」にインストールしたい場合、次の手順に従ってください。

1. 実行元フォルダの、Setup.ini ファイルを開きます。
2. 次の行を追加します。

   ```
   [CommonSection]
   ServerTargetLocalPath=D:¥Utility¥AntiVirus¥Sprotect
   ```

   説明 :
   ServerTargetLocalPath: 一般サーバのインストールパス

インストールする一般サーバにシリアル番号を登録するには、実行元フォルダの Setup.ini ファイルに次の行を追加します。

```
[CommonSection]
ServerTargetSN=XXXX-XXXX-XXXX-XXXX-XXXX
```

説明 :
XXXX-XXXX-XXXX-XXXX-XXXX: 有効なシリアル番号

インフォメーションサーバ上でのドメインコントローラの使用により、「SMS」ドメインの配下に一般サーバを登録できない場合があります。この問題を解決するには、サイレントインストールを使用する前に、IP アドレスを指定してください。

IP アドレスを指定するには、次の手順に従ってください。

1. SMS フォルダの Setup.ini ファイルを開きます。
2. 「AgentName」に記述されたホスト名を IP アドレスに変更し、ファイルを保存します。

ServerProtect for EMC Celerra のインストール

ServerProtect for EMC Celerra をインストールする前に

1. ServerProtect for EMC Celerra の機能を正しく動作させるには、ServerProtect for EMC Celerra をインストールする前に、次のインストール前作業を順番に実行することが重要です。AV ユーザアカウントと AV グループを Windows のドメインサーバで設定します。詳細については、EMC 社から提供されている CEE のマニュアルを参照してください。
2. ServerProtect 一般サーバのインストール先の各サーバに、EMC Celerra Event Enabler (CEE) /EMC VNX Event Enabler (VEE) (Common Anti-Virus Agent (CAVA) とも呼ばれる) をイン

ストールします。詳細については、EMC 社から提供されている CEE のマニュアルを参照してください。

ServerProtect for EMC Celerra のインストール

警告： **ServerProtect の対象 Windows Server 2008/NT Server に CEE がインストールされていないと、ServerProtect for EMC Celerra はインストールできません。**

インストールするには、次の手順を実行します。

1. インフォメーションサーバをインストールします。詳細については、42 ページの「インフォメーションサーバのインストール」を参照してください。
2. 一般サーバをインストールします。詳細については、47 ページの「セットアッププログラムからの一般サーバのインストール」を参照してください。
3. 管理コンソールをインストールします。詳細については、45 ページの「管理コンソールのインストール」を参照してください。ネットワーク内の他の Windows コンピュータまたはデスクトップシステムコンピュータに、管理コンソールを追加インストールすることもできます。

   ヒント： インフォメーションサーバを管理することができるのは、1 つの管理コンソールからのみです。1 つのインフォメーションサーバを複数の管理コンソールから同時に管理することはできません。

4. パターンファイルおよび検索エンジンを最新版にアップデートします。詳細については、73 ページの「アップデートファイルのダウンロード」と 70 ページの「アップデートの設定」を参照してください。
5. 複数の一般サーバを管理するための ServerProtect ドメインを作成します。詳細については、65 ページの「ServerProtect ドメインの新規作成」を参照してください。
6. 管理コンソールを使用して、他の一般サーバを追加インストールします。詳細については、50 ページの「管理コンソールからの一般サーバのインストール」を参照してください。

手順 1 から手順 3 は、初回セットアップ時、同時に実行することができます。

ServerProtect の削除

一般サーバのアンインストール

一般サーバをアンインストールする方法は 2 種類あります。

一般サーバをリモートでアンインストールするには

1. 管理コンソールから、アンインストールする一般サーバを選択します。
2. メインメニューから [Domain] → [Uninstall ServerProtect] の順に選択します。

一般サーバをローカルでアンインストールするには

1. Windows デスクトップで [コントロールパネル] → [プログラムの追加と削除] の順に選択します。Windows Server 2008 をご利用の場合は、[コントロールパネル] → [プログラムと機能] からアンインストールを行います。
2. アンインストールする一般サーバを選択し、[削除] ボタンをクリックします。

インフォメーションサーバのアンインストール

インフォメーションサーバはローカルでのみアンインストールできます。

Windows Server 環境からインフォメーションサーバを削除するには

1. Windows の [スタート] メニューから [コントロールパネル] を選択し、[プログラムの追加と削除] を選択します。
2. [ServerProtect インフォメーションサーバ] を選択し、[追加と削除] ボタンをクリックします。

管理コンソールのアンインストール

管理コンソールはローカルでのみアンインストールできます。

Windows 環境から管理コンソールを削除するには

1. Windows の [スタート] メニューから [コントロールパネル] を選択し、[プログラムの追加と削除] を選択します。Windows Server 2008 をご利用の場合は、[コントロールパネル] → [プログラムと機能] からアンインストールを行います。
2. [ServerProtect Management Console] を選択し、[追加と削除] ボタンをクリックします。

ServerProtect のユーザ登録

有効なシリアル番号を入力せずに ServerProtect をインストールすると、30 日体験版としてインストールされます。30 日間の試用期間後も継続して使用するには、体験版から製品版にアップグレードする必要があります。

ServerProtect では、次の登録が必要です。

- プログラム管理コンソールからの製品版の登録

注意： 体験版プログラムはすべてサポートサービスの対象外です。体験版の動作に関するお問い合わせについて、サポートセンターでは回答いたしかねますので、あらかじめご了承ください。製品版の購入、製品の追加購入について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。

製品版の登録

シリアル番号を入力して、体験版から製品版にアップグレードするには、次の手順に従ってください。

1. ドメインブラウザツリーでサーバを選択します。
2. メインメニューから [Do] → [Update Serial Number] の順に選択します。
3. テキストボックスにシリアル番号を入力します。
4. [OK] をクリックして変更内容を保存します。

第 3 章

ServerProtect の管理

本章では、ServerProtect の管理に欠かせない主要な機能について説明します。その他の管理ツールについては、管理コンソールのオンラインヘルプを参照してください。

本章で説明する内容には、次の項目が含まれます。

管理コンソールとは

ServerProtect では、1 つの管理コンソールから複数の Microsoft Windows サーバを管理することができます。管理コンソールはパスワードで保護され、権限のある管理者のみが ServerProtect の設定を変更できます。

管理コンソールを起動する

管理コンソールは、ネットワーク上の、32 ビットまたは 64 ビット Windows サーバまたはデスクトップコンピュータで実行できます。

管理コンソールを起動するには、次の手順に従ってください。

1. Windows の [スタート] メニューから [Trend ServerProtect Management Console] → [ServerProtect Management Console] の順に選択します。選択したインフォメーションサーバにログオンするための管理パスワードの入力が要求されます。

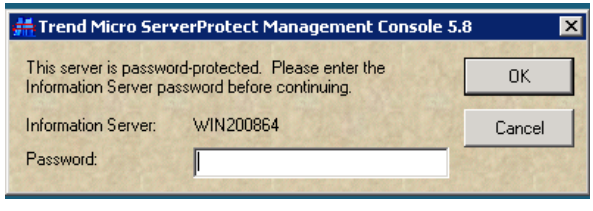


図 3-1.　インフォメーションサーバへのログオン

注意： 複数のインフォメーションサーバを管理している場合は、操作を続行する前にサーバの選択が求められます。

2. インフォメーションサーバのインストール時に指定した有効なパスワードを入力します。[OK] をクリックします。パスワードは大文字 / 小文字を区別し、一度に 1 つのインフォメーションサーバにしかログオンできません。
3. ServerProtect を初めてシステム上で実行する場合は、トレンドマイクロのアップデートサーバで新しいアップデートをダウンロードおよび配信できる可能性があることを伝えるメッセージボックスが表示されます。ServerProtect を使用してネットワークでウイルス検索を実行する前に、アップデートの実行をお勧めします。

管理コンソールのメイン画面

ServerProtect 管理コンソールには直観的なユーザインタフェースが用意されており、ServerProtect の設定、管理に必要なすべての機能に簡単にアクセスできるようになっています。

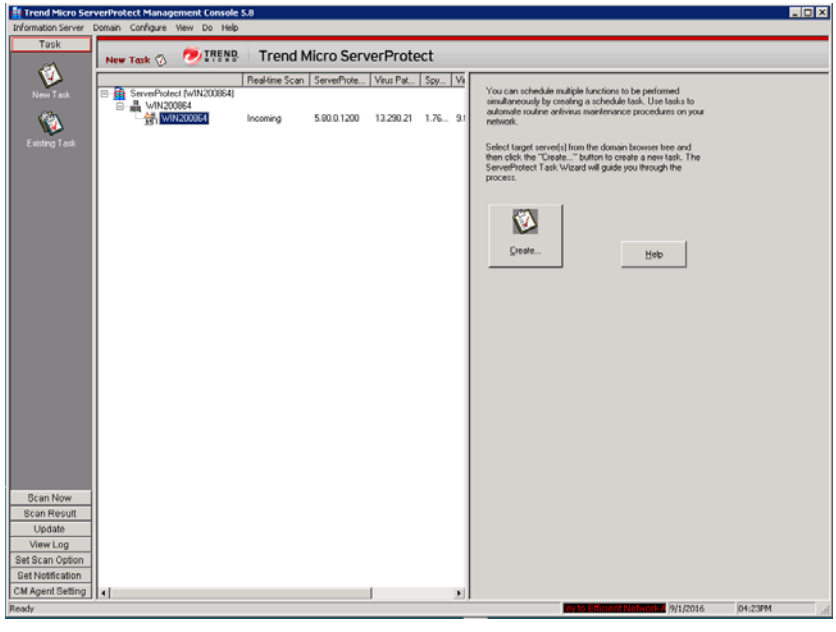


図 3-2.　管理コンソールのメイン画面構成

管理コンソールのメイン画面は、主に次の 4 つの部分から構成されます。

- **メインメニュー**：タイトルバーの下にあります。6 つのサブメニューがあり、それぞれユーザが選択できる多数のメニュー項目が含まれています。
- **サイドバー**：アプリケーションダイアログボックスの左側、メインメニューの下にあります。ここには 8 つの項目があり、それぞれユーザが選択できる追加のオプションがあります。
- **ドメインブラウザツリー**：サイドバーの右、メインメニューの下にあります。ツリービューには、ServerProtect の項目が分類されて示されます。これには、インフォメーションサーバ、ドメイン要素、一般サーバが含まれます。
- **設定データ領域**：メインウィンドウの右側にある薄いグレーの背景色の画面です。ウイルス検索およびログレポートシステムを設定するための情報および UI 要素が表示されます。

メインメニュー

画面上部のメインメニューには、次の項目が表示されます。

- [Information Server] : インフォメーションサーバの設定を行います。たとえば、インフォメーションサーバのバックアップや復元、ネットワーク上のインフォメーションサーバの移動です。
- [Domain] : ドメインブラウザツリーに表示されているドメインとサーバの構成を変更します。
- [Configure] : 検索およびログファイルの設定を修正したり、管理コンソールの表示更新間隔を設定します。
- [View] : ServerProtect のログファイル、検索結果、ウイルス情報を表示します。
- [Do] :
  - [Create Task] / [Existing Task] : タスクの作成または修正を実行します。
  - [Scan Now] : 手動検索 (ScanNow) を実行します。
  - [Update] / [Rollback] : コンポーネントのアップデートまたはロールバックを実行します。
  - [Control Manager (CM) Agent Settings] : Trend Micro Control Manager (以下、Control Manager) の設定を登録、登録解除、および実行します。
  - [Update Serial Number] : 新しいシリアル番号を入力し、期限が切れたシリアル番号を更新します。
  - [Change Password] : インフォメーションサーバのパスワードを変更します。
  - [Find Domain] : ドメインまたはサーバを検索します。
  - [Connect to Server with STOP Sign] : 一般サーバが実行されており、1 台のインフォメーションサーバにより管理されているが、管理コンソールに STOP が表示されている場合に使用します。
  - [Create Debug Info] : 詳細なデバッグ情報が含まれるログファイルを管理し、それをトレンドマイクロのテクニカルサポートへ送信します。
- [Help] : ヘルプシステムを開いたり、ServerProtect の製品情報を表示します。

サイドバー

サイドバーは ServerProtect の画面の左にあり、7 つのグループで構成されます。サイドバーは、プログラムのさまざまな機能へのショートカットを提供しています。

[Task] グループ

 [New Task] : 新規タスクを作成します。

 [Existing Task] : 既存のタスクを表示、実行、修正、または削除します。

[Scan] グループ

 [Scan Now] : 手動検索を設定、実行します。

[Scan Result] グループ

 [Real-time Scan] : リアルタイム検索と EMC CAVA 検索の結果を表示します。

 [ScanNow] : 手動検索結果を表示します。

 [Task Scan] : タスク検索結果を表示します

[Update] グループ

 [Update] : アップデートをダウンロードし、一般サーバに配信します。

 [Rollback] : 以前の配信内容にロールバックします。

[View Log] グループ

 [View Log]: ネットワーク上でこれまでに発生したウイルス対策イベントの履歴を表示します。

[Set Scan Option] グループ

 [Real-time Scan] : リアルタイム検索を設定します。

 [Exclusion List] : ServerProtect のウイルス検索エンジンで検索対象から除外するファイル、ディレクトリを定義します。

 [Deny Write List] : 特定のファイルやディレクトリを変更できないようにします。

[Notification Group] グループ

 [Standard Notification] : 感染ファイルの検出など通知イベントが発生した場合に発行する警告を設定します。

 [Outbreak Notification] : アウトブレークアラートを設定します。アウトブレークアラートは、設定した期間内に設定数を超えるウイルスが発生すると発行されます。

[CM Agent Setting] グループ

 [CM Agent Setting]: Control Manager での登録または登録解除の際に Control Manager を設定します。

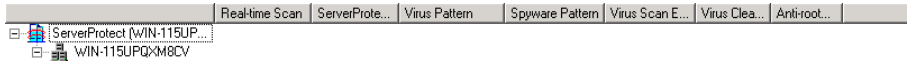
ドメインブラウザツリー

ドメインブラウザツリーには、ServerProtect が保護しているネットワークの構成が表示されます。構成要素には、ルート (ServerProtect 製品アイコン)、ブランチ (ドメイン)、ノード (ServerProtect 一般サーバ) が含まれます。ドメインブラウザツリーは次の 4 つの項目で構成されています。

- ヘッダ
- インフォメーションサーバ
- ドメイン
- 一般サーバ

ヘッダ

ドメインブラウザツリーの上にある欄では、パターンファイル、検索エンジン、プログラムの各バージョン、リアルタイム検索の方向などの情報を表示します。



ツリーアイコンを右クリックすると、選択したコンポーネントへの設定を変更できます。ドメインブラウザツリーの枠のサイズは調整できます。

インフォメーションサーバ

インフォメーションサーバは、管理下にある一般サーバの情報と通信を制御します。


インフォメーションサーバ

ドメイン

ドメインは、ServerProtect ネットワーク上のサーバをグループ化したものです。ドメインに含まれている一般サーバはドメイン内で一括して管理されます。ServerProtect ドメインは、Windows のドメインとは異なるものです。


ServerProtect ドメイン


ウイルスに感染した一般サーバを含む ServerProtect ドメイン

一般サーバ

一般サーバは、ネットワーク上にある ServerProtect がインストールされたサーバを指します。ServerProtect では、一般サーバはインフォメーションサーバによって管理されます。

- 32 ビット Microsoft Windows Server タイプの一般サーバ
- 64 ビット Microsoft Windows Server タイプの一般サーバ
- ウイルスに感染した 32 ビット Microsoft Windows Server タイプの一般サーバ
- ウイルスに感染した 64 ビット Microsoft Windows Server タイプの一般サーバ
- 接続が切断、またはサービスが無効にされた一般サーバ

設定データ領域

ServerProtect 画面の右側にあるのが設定データ領域です。設定データ領域では設定データを入力したり、企業ネットワークに関する各種情報を表示したりできます。

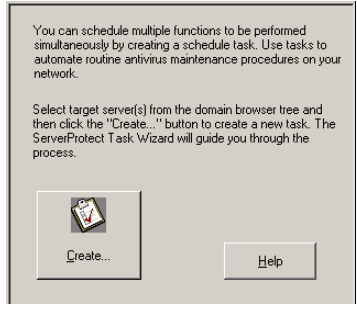


図 3-3.　設定データ領域

ServerProtect ドメインの管理

ServerProtect ドメインは一般サーバの仮想的なグループで、サーバの識別および管理を簡略化するために用いられます。ドメインはネットワーク管理の必要に応じて作成、名前変更、または削除することができます。

注意： あるドメイン内のサーバの 1 つでウイルスが検出されると、ドメインアイコンが変化します。これは、ウイルスがネットワーク全体に広がることを阻止するための警告です。変化したアイコンを削除するには、管理コンソールの [Scan Result] のログをすべて削除する必要があります。または、これらすべてのログを開きます。

ServerProtect ドメインの新規作成

ServerProtect のセットアッププログラムで初期設定のドメインをインストールした後で、ネットワークの必要に応じていつでも管理コンソールから新規ドメインを作成できます。

ドメイン名には半角英数文字で 50 文字まで使用することができます。全角文字は使用することができません。全角を使用すると Trend Micro Control Manager エージェントのインストール時にエラーが発生します。

新規ドメインを作成するには、次の手順に従ってください。

1. 次のいずれかの操作を実行してください。
   - ドメインを追加するサーバを選択します。メインメニューから [Domain] → [Add New Domain] の順に選択します。
   - ドメインブラウザツリーのルートを右クリックし、ポップアップメニューから [Add New Domain] を選択します。

   [Create New Domain] ダイアログボックスが表示されます。

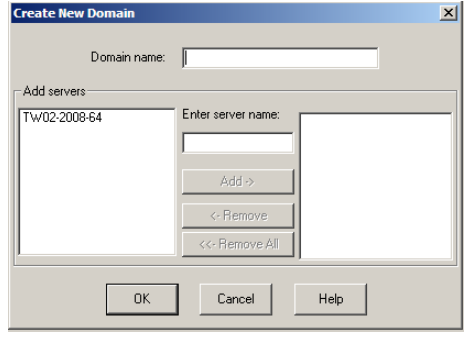


図 3-4. [Create New Domain] ダイアログボックス

2. 新しいドメインの名前を [Domain name] フィールドに入力します。
3. ドメインに追加するサーバを識別します。次のいずれかの操作を実行してください。

- 画面の左のリストからサーバを選択します。
- [Enter server name] フィールドにサーバ名を入力します。

4. [Add] をクリックします。
5. 新しいドメインに追加するサーバがすべて右のリストに表示されるまで手順 3 と 4 を繰り返します。既に追加したサーバを削除するには、右のリストでその名前を選択し、[Remove] をクリックします。[Remove All] をクリックすると、右のリストに追加したすべてのサーバが削除されます。
6. [OK] ボタンをクリックして変更内容を保存します。

ServerProtect ドメイン名の変更 (リネーム)

サーバ名と同じドメイン名は、ServerProtect のインストール時に作成された初期設定のドメイン名です。ドメインの名前は、必要に応じて管理コンソールで変更することができます。

ドメインの名前を変更するには、次の手順に従ってください。

1. ドメインブラウザツリーで名前を変更するドメインを選択します。
2. 次のいずれかの操作を実行してください。
   - ドメインアイコンを右クリックし、ポップアップメニューで [Rename Domain] を選択します。
   - メインメニューから [Domain] → [Rename Domain] の順に選択します。
   - キーボード上の <F2> キーを押します。

   [Rename a Domain] ダイアログボックスが表示されます。

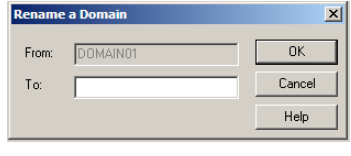


図 3-5. [Rename a Domain] ダイアログボックス

3. 新しいドメイン名を [To] テキストボックスに入力し、[OK] ボタンをクリックします。

ServerProtect ドメインの削除

不要になった空のドメイン (一般サーバを含まないドメイン) を削除することができます。一般サーバが含まれているドメインを削除することはできません。

ドメインを削除するには、次の手順に従ってください。

1. ドメインブラウザツリーから削除するドメインのアイコンを選択します。
2. 次のいずれかの操作を実行してください。
   - ドメインアイコンを右クリックし、ポップアップメニューから [Delete Domain] を選択します。
   - メインメニューから [Domain] → [Delete Domain] の順に選択します。
   - キーボード上の <Delete> キーを押します。

注意： 削除するドメインは空でなければなりません。サーバが含まれているドメインを削除することはできません。

ドメイン間での一般サーバの移動

管理上の都合で、一般サーバをあるドメインから別のドメインに移動 (あるドメインから削除して別のドメインに追加) することが必要になる場合があります。ドメインブラウザツリー上の一般サーバアイコンをドメイン間でドラッグ & ドロップすれば、一般サーバを移動できます。

ServerProtect ドメインを作成して、一般サーバを移動することもできます。詳細については、65 ページの「ServerProtect ドメインの新規作成」を参照してください。

インフォメーションサーバの管理

インフォメーションサーバは、管理している一般サーバにデータを保存したり配信します。Windows Server ネットワークでは、一般サーバから Windows サーバに警告メッセージが送信されます。

インフォメーションサーバは情報配信システムとして機能するため、1 台のインフォメーションサーバが管理可能なサーバ数はネットワークの帯域幅によって決まります。

ヒント： WAN 環境のような大規模ネットワーク環境では、ネットワークセグメントごとにインフォメーションサーバをインストールすることをお勧めします。セグメントごとにインストールすることで、トラフィックへの影響を最小限に抑えることが可能です。

インフォメーションサーバの選択

管理コンソールでは、複数のインフォメーションサーバを管理し、サーバを切り替えて表示 / 設定することができますが、1 つのインフォメーションサーバに複数の管理コンソールからログオンすることはできません。管理コンソールからインフォメーションサーバにログオンできない場合は、他の管理コンソールからログオンされていないかどうかを確認してください。

インフォメーションサーバを選択するには

1. プログラムのメインメニューから [Information Server] → [Select Information Server] の順に選択します。インフォメーションサーバを選択するための画面が表示されます。
2. 次のいずれかの操作を実行してください。
   - インフォメーションサーバとして使用するサーバの名前または IP アドレスを入力します。
   - リストからインフォメーションサーバを選択します。

   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) がインストールされている場合、プライマリ NIC に接続されているインフォメーションサーバのみがリストボックスダイアログに表示されます。リストのサーバ表示を更新するには、[Refresh] ボタンをクリックします。

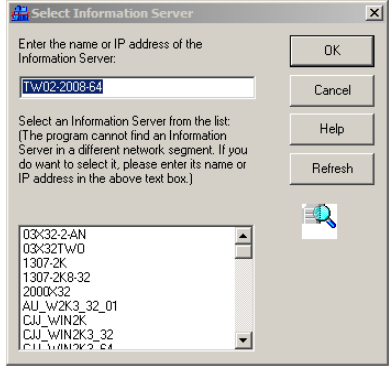


図 3-6.　インフォメーションサーバの選択

3. [OK] をクリックして変更を保存します。

一般サーバの管理

ServerProtect のアーキテクチャでは、一般サーバはウイルスを最前線で防御する存在で、インフォメーションサーバによって管理されます。ServerProtect の 3 層アーキテクチャでは、最下層に位置付けられます。ここでは一般サーバの管理について説明します。

ドメイン間での一般サーバの移動

ServerProtect ドメイン間で一般サーバを移動する場合は、ドメインブラウザツリーで一般サーバを選択して、ドメイン間でドラッグ & ドロップします。

インフォメーションサーバ間での一般サーバの移動

インフォメーションサーバ間で一般サーバを移動することもできます。この機能は、インフォメーションサーバの負荷を軽減する場合に特に便利です。

インフォメーションサーバを移動するには、次の手順に従ってください。

注意： [Move NS (s) to Another IS] 機能を使用して、古い ServerProtect 一般サーバを ServerProtect 5.8 のインフォメーションサーバに移動することはできません。

---

1. 次のいずれかの操作を実行してください。
   - 対象サーバのアイコンを右クリックし、ポップアップメニューから [Move NS (s) to Another IS] を選択します。
   - 移動する一般サーバを選択して、メインメニューから [Domain] → [Move NS (s) to Another IS] の順に選択します。[Select Destination Information Server] 画面が表示されます。
2. 移動先のインフォメーションサーバを選択し、[OK] をクリックして送信します。[Move NS (s) to Another IS] ダイアログボックスが表示されます。
3. [User Name] および [Password] に値を入力し、[OK] をクリックします。
4. [Select Destination Information Server] ダイアログボックスが表示されます。
5. 移動先のインフォメーションサーバを選択し、[OK] をクリックします。
6. 移動の確認を求めるダイアログボックスが表示されます。選択したインフォメーションサーバに一般サーバを移動するには [OK] をクリックします。

アップデートの設定

トレンドマイクロのアップデートサーバから、ServerProtect コンポーネントをアップデートすることができます。ServerProtect のアップデートは、ダウンロードと配信という 2 段階のプロセスで構成されます。

コンポーネントのアップデート

ServerProtect では、次のコンポーネントのアップデートが可能です。

- **ウイルスパターンファイル** : トレンドマイクロのウイルス対策ソフトウェアでは、パターンマッチングによるウイルス検出方式を採用しています。コンピュータ上のファイルが調査され、数千もの既知のコンピュータウイルスの「シグネチャ」を含むウイルスパターンファイルと比較されます。コンピュータ上のファイルがパターンファイルに一致すると、ウイルス対策ソフトウェアによって感染ファイルとして検出されます。
- **スパイウェアパターンファイル** : スパイウェアパターンファイルは、ファイル、メモリ内のプログラムとモジュール、Windows レジストリ、および URL ショートカット内のスパイウェア / グレーウェアを識別します。
- **検索エンジン (32 および 64 ビットの Windows)**: 検索エンジンは、実際に個々のファイルのウイルスを検索するソフトウェアのコンポーネントです。
- **ウイルスクリーンナップエンジン (32 ビットおよび 64 ビットの Windows)**: トロイの木馬およびトロイの木馬プロセスを検索して削除するエンジンです。32 ビットおよび 64 ビットのプラットフォームがサポートされます。
- **ウイルスクリーンナップテンプレート** : ウイルスクリーンナップテンプレートは、ウイルスクリーンナップエンジンで、トロイの木馬のファイルおよびプロセスを駆除できるように、これらのファイルおよびプロセスの識別に使用されます。
- **ルートキット対策ドライバ (32 ビットの Windows のみ)**: ルートキット対策ドライバは、ダメージクリーンナップエンジンで使用されるカーネルモードドライバで、ルートキットによる潜在的なリダイレクトを回避する機能を提供します。

ダウンロードと配信の流れ

ServerProtect ネットワークでのアップデートファイルのダウンロードと配信の要求に対する ServerProtect の処理の流れについて図 3-7 で説明します。

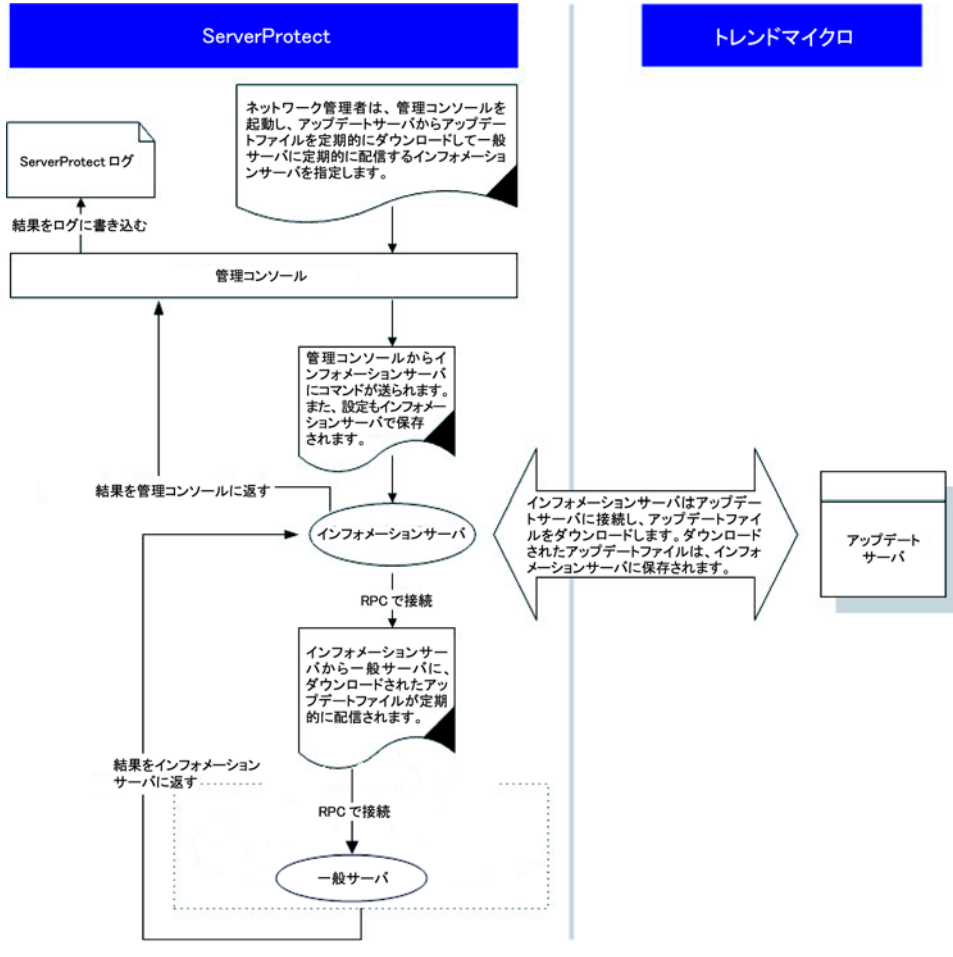


図 3-7.　ダウンロードと配信の流れ

アップデートファイルの現行バージョンの表示

ServerProtect では、インフォメーションサーバで現在使用されているウイルスパターンファイルバージョンなど確認できます。

インフォメーションサーバに保存されているパターンファイル、検索エンジン、プログラムの現行バージョンを表示させるには、次の手順に従ってください。

1. 次のいずれかの操作を実行してください。
   - サイドバーから [Update] → [Update] の順に選択します。
   - メインメニューから [Do] → [Update] の順に選択します。
2. [Update] メイン画面が表示されます。

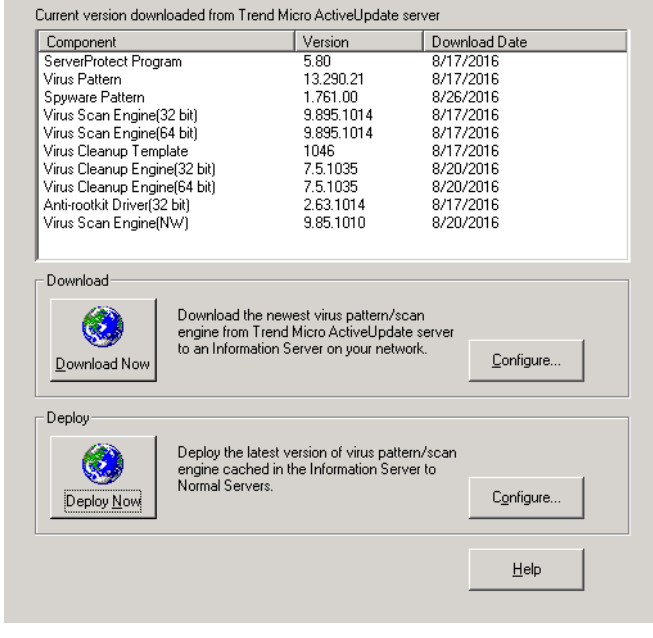


図 3-8. [Update] メイン画面

インフォメーションサーバで配信用に保持されているウイルスパターンファイルおよび検索エンジンのバージョン情報は、[Update] 画面の上部に表示されます。

- ServerProtect のバージョン
- ウイルスパターンファイルのバージョン
- スパイウェアパターンファイルのバージョン
- ウイルス検索エンジンのバージョン (32 ビットおよび 64 ビット)
- ウイルスクリーンナップテンプレートのバージョン
- ウイルスクリーンナップエンジンのバージョン (32 ビットおよび 64 ビット)
- ルートキット対策ドライバのバージョン (32 ビットのみ)

アップデートファイルのダウンロード

日々増え続ける新種ウイルスに対応し、効果的なウイルス対策を実施するため、トレンドマイクロのアップデートサーバから定期的にアップデートファイルをダウンロードしてください。トレンドマイクロでは、通常、ウイルスパターンファイルをほぼ毎日、スパイウェアパターンは毎週リリースしています (ウイルスの動向により、リリースの頻度は異なります)。検索エンジンの更新はパターンファイルの更新ほど頻繁ではありません。

トレンドマイクロのアップデートサーバからアップデートファイルをダウンロードしたら、指定したネットワークドライブをネットワーク上の他のインフォメーションサーバのダウンロード元 (ミラー) として機能させることで、ダウンロードにかかる負荷を軽減することができます。

アップデートファイルをネットワーク上のドライブからダウンロードする方法は、複数のインフォメーションサーバを必要とするイントラネットなどの大規模ネットワーク環境で理想的な方法と考えられます。他のサーバからアップデートファイルをダウンロードする前に、ダウンロード元サーバにアップデートファイルがあることを確認する必要があります。

ダウンロード元の指定

アップデート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ダウンロードするか、またはネットワーク上に指定したドライブからコピーすることができます。ネットワーク上のドライブからファイルをコピーする場合は、ダウンロード元フォルダを事前に作成しておく必要があります。

インターネット経由でトレンドマイクロのアップデートサーバからアップデートファイルをダウンロードするには

1. 次のいずれかの操作を実行してください。
   - サイドバーから [Update] → [Update] の順に選択します。
   - メインメニューから [Do] → [Update] の順に選択します。
2. [Download] グループの [Configure] ボタンをクリックします。[Download Option] ダイアログボックスが表示されます。
3. 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する場合、[Internet] オプションを選択し、次の URL を指定します。

   `http://spemc58-p.activeupdate.trendmicro.com/activeupdate/`
4. [OK] をクリックします。ダウンロードされたファイルは、インフォメーションサーバの次のディレクトリに保存されます。

   `<ドライブ>:¥Program Files¥Trend¥SProtect¥SpntShare`

ローカルまたはネットワークドライブをダウンロード元に設定するには

1. 次のいずれかの操作を実行してください。
   - サイドバーから [Update] → [Update] の順に選択します。
   - メインメニューから [Do] → [Update] の順に選択します。
2. [Download] で [Configure] をクリックします。[Download Option] ダイアログボックスが表示されます。
3. [From a local or network drive] をクリックします。
4. UNC パスを入力して、ネットワーク上の他のサーバからダウンロードしたアップデートファイルの保存先を指定します。ダウンロード元サーバを識別するために、パスはドライブマップ形式ではなく UNC 形式で指定してください。

   たとえば、次のように指定します。

   `¥¥servername¥foldername`
5. [User name] および [Password] にダウンロード元サーバにアクセスするユーザ名とパスワードを指定します。アップデート元には、既にアップデートファイルのコピーをダウンロードしたことのあるサーバを指定する必要があります。

6. [OK] をクリックします。

警告： **ローカルまたはネットワークドライブからアップデートファイルをダウンロードするには、まずダウンロード元フォルダを作成する必要があります。**

ダウンロード元フォルダを作成するには

1. [Download Now] ボタンをクリックして、インターネット経由でのアップデートを実行します。
2. 次のいずれかの操作を実行してください。
   - <ドライブ>:¥Program Files¥Trend¥SProtect¥ にある SpntShare フォルダをインフォメーションサーバの共有フォルダに設定します。
   - ネットワークサーバに共有フォルダを作成し、SpntShare フォルダにあるすべてのファイルをコピーします。

SpntShare フォルダをダウンロード元に指定しない場合は、インターネット経由でアップデートを実行するたびに、指定したインフォメーションサーバの SpntShare フォルダにあるすべてのファイルを、ダウンロード元に指定した共有フォルダにコピーする必要があります。

ダウンロードの実行

トレンドマイクロのアップデートサーバまたはネットワーク上の別のインフォメーションサーバから最新のウイルスパターンファイルと検索エンジンをダウンロードすることができます。

ダウンロードを実行するには、次のオプションを選択してください。

1. 次のいずれかの操作を実行してください。
   - サイドバーから [Update] → [Update] の順に選択します。
   - メインメニューから [Do] → [Update] の順に選択します。
2. [Update] ダイアログボックスで [Download Now] ボタンをクリックします。ダイアログボックスに、アップデート完了までの残り時間を表すプログレスバーが表示されます。

注意： 初めて [Download Now] ボタンをクリックしてダウンロードを実行する場合は、まずダウンロード設定を指定する必要があります。ダウンロード設定を実行せずに [Download Now] ボタンをクリックすると、「送信元にネットワークの問題があります」または「HTTP タイムアウトが発生しました」というメッセージが表示される場合があります。詳細については、77 ページの「ダウンロードの設定」を参照してください。

ServerProtect では、ダウンロードのイベントはインフォメーションサーバログに記録されます。

予約ダウンロードの設定

予約ダウンロードを設定して、トレンドマイクロまたはネットワーク上の他のサーバから最新のアップデートファイルを定期的にダウンロードすることができます。

予約ダウンロードを設定するには

1. 次のいずれかの操作を実行してください。
   - サイドバーから [Update] → [Update] の順に選択します。
   - メインメニューから [Do] → [Update] の順に選択します。
2. [Download] で [Configure] ボタンをクリックします。[Download Option] ダイアログボックスが表示されます。
3. [Schedule Setting] タブをクリックします。

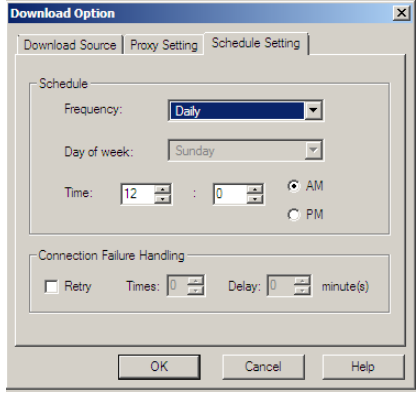


図 3-9. [Download Option] - [Schedule Setting]

4. [Schedule] グループの [Frequency] リストで、ダウンロードを実行する周期を選択します。[Weekly] を選択する場合は、ダウンロードを実行する曜日と実行時刻を指定します。[AM]、[PM] のいずれかも選択してください。[Daily] を選択する場合は、ダウンロードの実行時刻を指定します。[AM]、[PM] のいずれかも選択してください。[Hourly] を選択する場合は、ダウンロードの実行時刻 (分) を指定します。予約ダウンロードを設定しない場合は [None] を選択します。

5. エラー発生時に ServerProtect でダウンロードサーバに再接続させる場合は、[Retry] チェックボックスをオンにします。ダウンロードの処理に失敗した場合に、ServerProtect が再試行する回数と実行間隔 (分) を [Times] と [Delay] に指定します。
6. [OK] をクリックします。ダウンロードされたファイルは、次のディレクトリに保存されます。

   ```
   C:¥Program Files¥Trend¥Sprotect¥SpntShare
   ```

ダウンロードの設定

最新のアップデートファイルをダウンロードする手順について説明します。

ダウンロードを設定するには、次の手順に従ってください。

1. 次のいずれかの操作を実行してください。
   - サイドバーから [Update] → [Update] の順に選択します。
   - メインメニューから [Do] → [Update] の順に選択します。
2. ダウンロードの設定を変更するには、表示された [Update] ダイアログボックスで [Configure] ボタンをクリックします。[Download Option] ダイアログボックスが表示されます。

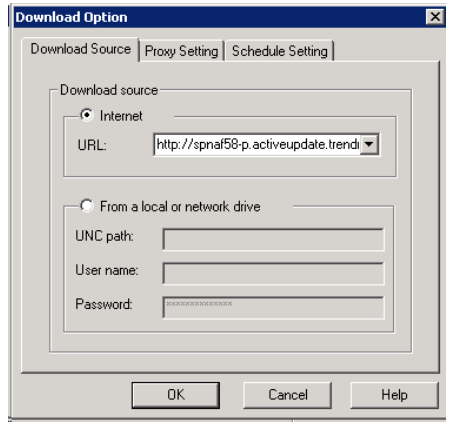


図 3-10. [Download Option] - [Download Source]

プロキシサーバ設定

プロキシサーバ経由でインターネットに接続している場合は、インターネットからアップデートファイルをダウンロードする前に、プロキシサーバの情報を入力する必要があります。

プロキシサーバを設定するには、次の手順に従ってください。

1. 次のいずれかの操作を実行してください。
   - サイドバーから [Update] → [Update] の順に選択します。
   - メインメニューから [Do] → [Update] の順に選択します。
2. [Download] で [Configure] ボタンをクリックします。[Download Option] ダイアログボックスが表示されます。
3. [Proxy Setting] タブをクリックします。

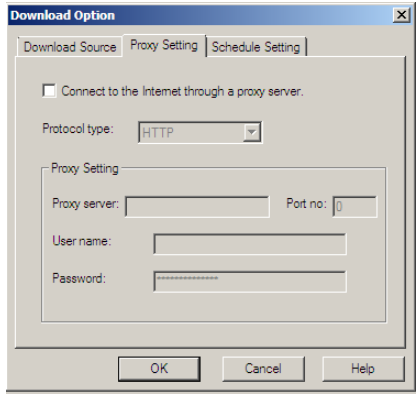


図 3-11. [Download Option] - [Proxy Setting]

4. [Connect to the Internet through a proxy server] チェックボックスをオンにします。
5. [Protocol type] リストから、ダウンロードに使用するプロトコルを選択します。[HTTP] または [SOCK4] のいずれかを選択してください。
6. [Proxy Setting] グループで、次の操作を実行してください。
   - [Proxy Server]、[Port no] テキストボックスに、使用するプロキシサーバ名とポート番号を入力します。
   - [User name] および [Password] テキストボックスに、プロキシサーバへのログインに必要なユーザ名とパスワードを入力します。
7. [OK] をクリックします。

アップデートファイルの配信

複数の一般サーバにアップデートファイルを配信するように設定した場合、インフォメーションサーバは個々の一般サーバにコマンドを送信し、アップデートファイルのコピーを取得するように要求します。

配信の実行

配信機能は、インフォメーションサーバに保存されたアップデートファイルを他の一般サーバに配信するときに使用します。

アップデートファイルの配信を実行するには、次の手順に従ってください。

1. 次のいずれかの操作を実行してください。
   - サイドバーから [Update] → [Update] の順に選択します。
   - メインメニューから [Do] → [Update] の順に選択します。
2. [Deploy Now] をクリックします。配信の実行を確認するダイアログボックスが表示されます。アップデートを手動で配信する場合は [Yes] をクリックします。[Deploy] ダイアログボックスが表示されます。

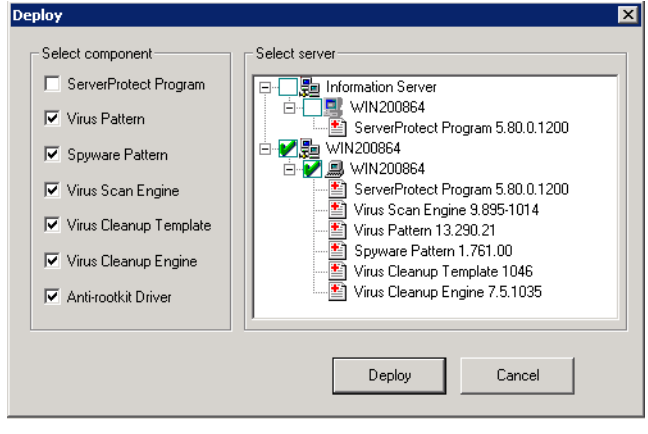


図 3-12. [Deploy]

[Select component] グループのチェックボックスは、一般サーバに配信可能なコンポーネントを示しています。[Virus pattern]、[Spyware pattern]、[Virus Scan Engine]、[Virus Cleanup Template]、[Virus Cleanup Engine]、および [Anti-rootkit Driver] は、初期設定でオンになっています。[Select server] 画面では、ダウンロードされた ServerProtect ウイルス対策の各要素の

バージョン情報がツリービューとして表示されます。64 ビットの Windows サーバの場合、[Select Component] グループに表示される使用可能なチェックボックスは、[Server protect program]、[Virus pattern]、[Spyware pattern]、[Virus Scan Engine]、[Virus Cleanup Template]、[Virus Cleanup Engine] です。32 ビットの Windows サーバの場合、64 ビットの Windows サーバのこれら 6 つの要素に加えて、[Anti-rootkit Driver] のチェックボックスも表示されます。

3. 目的のウイルス対策機能を適用するには、[Select Component] グループでそのコンポーネントのチェックボックスをオンにし、[Select server] ツリービューで配信対象の一般サーバのチェックボックスをオンにします。[Deploy] をクリックしてダウンロードされた要素を配信します。

予約配信の設定

予約配信タスクを設定して一般サーバに最新のアップデートファイルを配信します。

ServerProtect では配信タスクが初期設定として用意されています。詳細については、84 ページの「初期設定のタスク」を参照してください。

予約タスクの詳細については、85 ページの「新規タスクの作成」を参照してください。

ヒント： アップデートファイルのダウンロードおよび配信を予約して自動実行する時刻を設定する場合は、必ず配信時刻よりも前にダウンロード時刻を設定してください。

予約配信を設定するには、次の手順に従ってください。

1. 次のいずれかの操作を実行してください。
   - サイドバーから [Update] → [Update] の順に選択します。
   - メインメニューから [Do] → [Update] の順に選択します。
2. [Deploy] グループの [Configure] ボタンをクリックします。[Deploy Option] ダイアログボックスが表示されます。

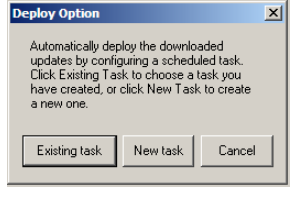


図 3-13. [Deploy Option] ダイアログボックス

3. 次のいずれかの操作を実行してください。
   - タスクを新規作成する場合は [New task] をクリックします。
   - 既存のタスクを編集する場合は [Existing task] をクリックします。

   タスクの新規作成と編集の詳細については、90 ページの「既存のタスクの実行」および 90 ページの「既存のタスクの変更」を参照してください。

配信した更新内容のロールバック

ServerProtect では、パターンファイル、検索エンジン、プログラムを更新した後で、1 世代に限り更新前のバージョンに戻すことができます。プログラムバージョン、ウイルスパターンファイルおよび検索エンジンのみ、ロールバックできます。ロールバック機能は、ソフトウェアの互換性の問題や、ダウンロード時にファイルが壊れた場合などに利用します。

注意： インフォメーションサーバから一般サーバへパターンファイルおよび検索エンジンファイルを配信した場合、両者をロールバックできます。

既に配信した更新内容をロールバックするには、次の手順に従ってください。

1. 次のいずれかの操作を実行してください。
   - サイドバーから [Update] → [Rollback] の順に選択します。
   - メインメニューから [Do] → [Rollback] の順に選択します。

   [Rollback] の設定画面が表示されます。

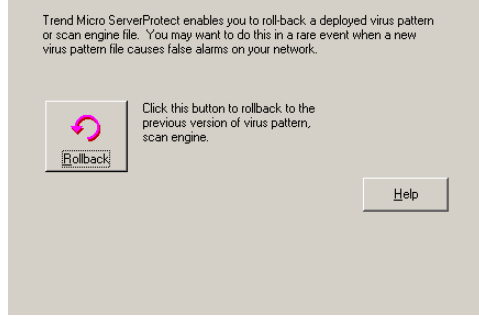


図 3-14. ロールバックの設定

2. [Rollback] をクリックします。ServerProtect のロールバックモジュールがロードされます。

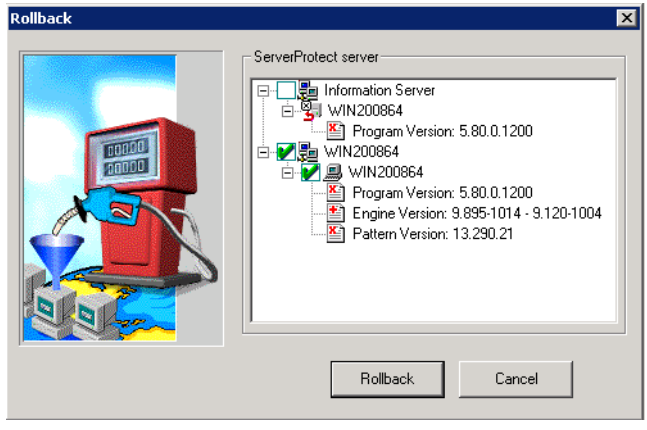


図 3-15. [Rollback] ダイアログボックス

画面には、ServerProtect で現在使用されているウイルスパターンファイルと検索エンジンについての情報が表示されます。バージョンについての情報も表示されます。

3. ロールバックする対象をツリーから選択し、[Rollback] をクリックします。

注意： プログラムバージョン、ウイルスパターンファイルおよび検索エンジンを、1 つ前のバージョンよりも前のバージョンにロールバックすることはできません。

タスクの管理

ServerProtect ではタスクを自由に作成または編集して、一般サーバで複数のジョブを自動的に開始するよう予約することができます。タスクを利用することでネットワーク上での保守作業が自動化され、ウイルス対策管理の効率が向上します。また、ウイルス対策ポリシーの管理にも役立てることができます。

一度に複数の手順を実行するタスクを定義することで、ウイルス対策ソフトウェアの管理を自動化することができます。

タスクはタスクの管理を担当する「所有者」に割り当てられます。

ServerProtect タスクウィザード

ServerProtect のタスクウィザードは直観的なインタフェースを提供しており、タスクを簡単に定義することができます。次の機能をタスクで扱うことができます。

- [Real-time Scan setting] : サーバ上でアクセスされるすべてのファイルをチェックする検索方法です。タスクにさまざまなリアルタイム検索オプションを設定することができます。
- [Scan Now] : サーバを常時監視するリアルタイム検索に対して、ScanNow は手動で実行する検索です。
- [Purge logs] : データベースから削除するログの種類を定義します。あらかじめ設定した期間より古いウイルスログを自動削除することができます。
- [Export logs] : 他のアプリケーションで使用できるように CSV ファイルでログを出力します。
- [Print logs] : 特定の条件に一致したログを印刷するネットワークプリンタを選択します。
- [Run statistics] : サーバ上のウイルス検索に関する統計を収集し表示します。

- [Deploy] ：ウイルスパターンファイルと検索エンジンのアップデートファイルを他の ServerProtect サーバに配信する予約を設定します。

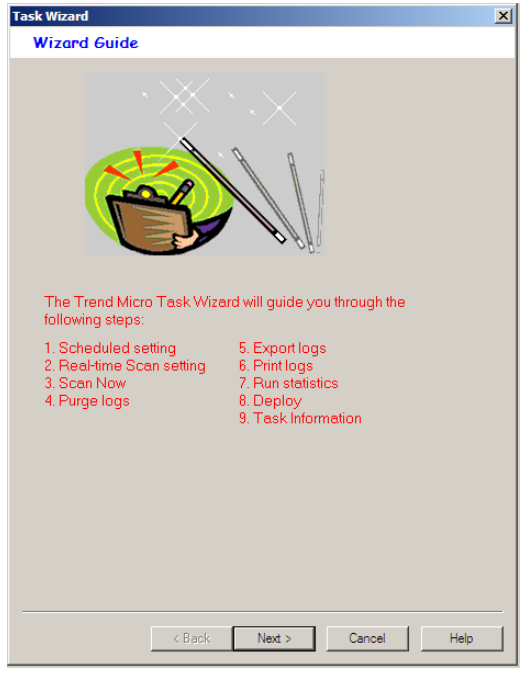


図 3-16.　[Task Wizard] ダイアログボックス

初期設定のタスク

すべての一般サーバインストールでは、初期設定タスクが ServerProtect により作成されます。ServerProtect サーバをインストールすると、[ScanNow] (タスク名：SCAN)、[Statistics] (タスク名：STATISTIC)、[Deploy] (タスク名：DEPLOY) の 3 つの初期設定のタスクが自動的に作成されます。初期設定のタスクは変更可能ですが、タスク名やタスク所有者名を変更することはできません。

注意： 初期設定の配信タスク「DEPLOY」を利用してスパイウェアパターンを予約配信するためには、配信タスクを編集する必要があります。

詳細については、以下の製品 Q&A を参照してください。
https://success.trendmicro.com/jp/solution/1102106

新規タスクの作成

タスクは、保守、設定手順を自動化する 1 つの方法です。

新規タスクを作成するには、次の手順に従ってください。

1. ドメインブラウザツリーからインフォメーションサーバ、ドメイン、一般サーバのいずれかのアイコンを選択します。
2. 次のいずれかの操作を実行してください。
   - メインメニューから [Do] → [Create Task] の順に選択します。
   - サイドバーから [Task] → [New Task] の順に選択します。
3. [Create] ボタンをクリックします。[Create New Task] ダイアログボックスが表示されます。

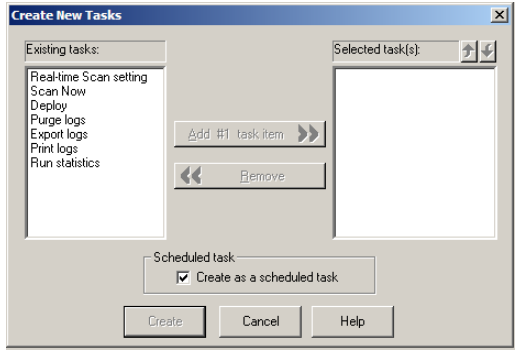


図 3-17. [Create New Task] ダイアログボックス

4. 左の [Existing tasks] リストボックスでタスクに含めたい機能を選択します。
5. [Add #n Task Item] ボタンをクリックして、手順 4 で選択した機能を [Selected task (s)] リストボックスに追加します (「#n」はタスクアイテムの番号を示します)。また、[Existing tasks] リストからさらに機能を選択することも、既に選択した機能を削除することもできます。

ヒント： 機能の実行順序を変更するには、順序を変更する機能を選択し、[Selected task(s)] リストボックスの上にある上下の矢印アイコンをクリックします。配信機能は常にこのリストの最後である必要があります。

---

6. このタスクを予約して自動的に実行したい場合は、必ず [Create as a scheduled task] オプションを有効にしてください。

7. [Create] ボタンをクリックすると、選択した機能からタスクを作成するためのウィザードが起動します。[Cancel] をクリックすると、変更内容が保存されずに、[Create New] ダイアログボックスが閉じます。

予約タスクの作成

予約タスクを作成することで、設定にかかる手間や時間を省くことができます。

予約タスクを作成するには、次の手順に従ってください。

1. 85 ページの「新規タスクの作成」の手順 1 ～ 6 を実行します。[Scheduled task] の [Create as a scheduled task] チェックボックスがオンになっていることを確認します (図 3-17 を参照)。[Task Wizard] ダイアログボックスが表示されます。
2. [Next] をクリックします。[Schedule Settings] ダイアログボックスが表示されます。

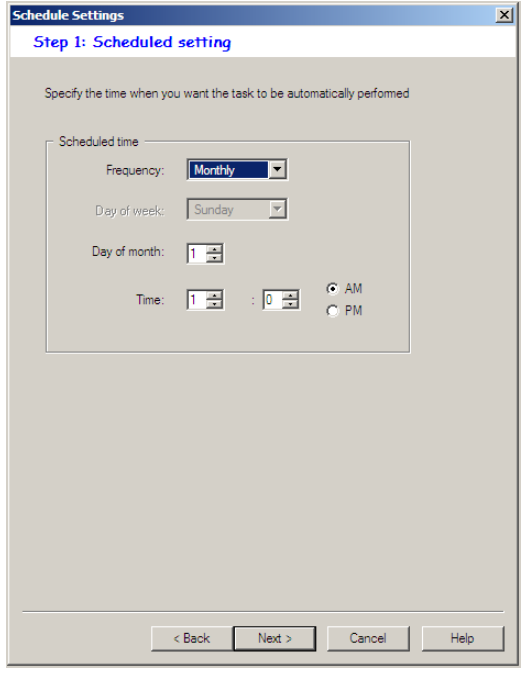


図 3-18. [Schedule Settings] ダイアログボックス

3. [Scheduled time] グループの [Frequency] リストで、ダウンロードを実行する周期を選択します。[Monthly] を選択する場合、タスクを実行する日付と実行時刻を指定します。[AM]、[PM] のいずれかも選択してください。[Weekly] を選択する場合は、タスクを実行する曜日と実行時刻を指定します。[AM]、[PM] のいずれかも選択してください。[Daily] を選択する場合は、タスクの実行時刻を指定します。[AM]、[PM] のいずれかも選択してください。[Hourly] を選択した場合は、タスクの実行時刻 (分) を指定します。
4. [Next] をクリックして、タスクウィザードの設定を続行します。

手動検索対象の指定

検索タスクは特定のドライブで実行する必要があります。検索対象には、すべてのローカルドライブ、または特定のドライブ / ディレクトリを選択することができます。ネットワーク上のドライブを選択することも可能です。

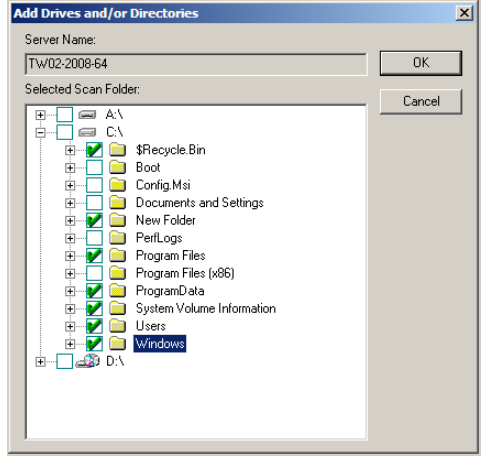


図 3-19. [Add Drives and/or Directories] ダイアログボックス

初期設定タスクの作成

タスクウィザードの最後に表示される [Task Information] では、タスク名と所有者を指定します。作成したタスクは、[Created as default task] オプションを有効にすることで、初期設定のタスクとして他のサーバに適用することができます。一般サーバを追加すると、追加されたサーバでは既存の初期設定タスクが継承されます。

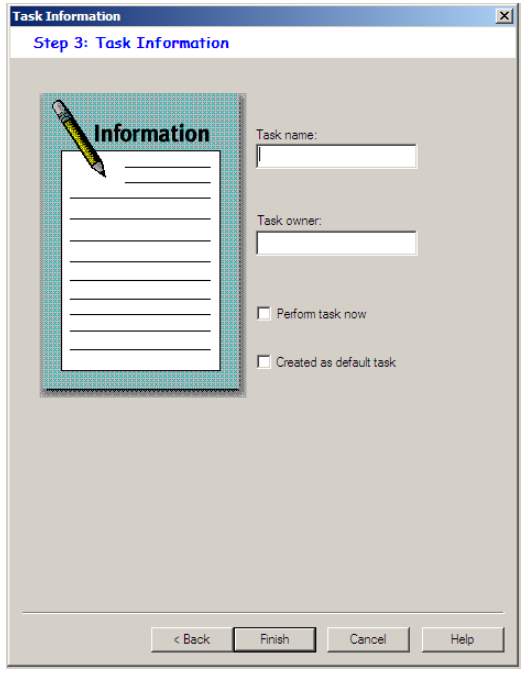


図 3-20. [Task Information] ダイアログボックス

タスクの作成を終了するには、次の手順に従ってください。

1. [Task name] にタスク名を入力します。
2. [Task Owner] にタスクの作成者または所有者を入力します。
3. タスクをすぐに実行したい場合は、[Perform task now] チェックボックスをオンにします。
4. 初期設定のタスクとして他のサーバに適用する場合は、[Created as default task] チェックボックスをオンにします。
5. [Finish] ボタンをクリックし、タスクへの設定の変更を保存し、タスクウィザードを閉じます。

既存のタスクリストを表示する

既存のタスクリストには、既に定義されているタスクに関する情報が表示されます。このリストを使用して定義されたタスクを実行、修正、削除、表示することができます。

既存のタスクを表示するには、次のいずれかの操作を実行してください。

- サイドバーから [Task] → [Existing Task] の順に選択します。
- メインメニューから [Do] → [Existing Task] の順に選択します。

既存のタスクリストが表示され、項目が表形式で表示されます。次の図に、さまざまな項目を示します。各項目のヘッダをクリックすると、リスト項目が並べ替えられます。

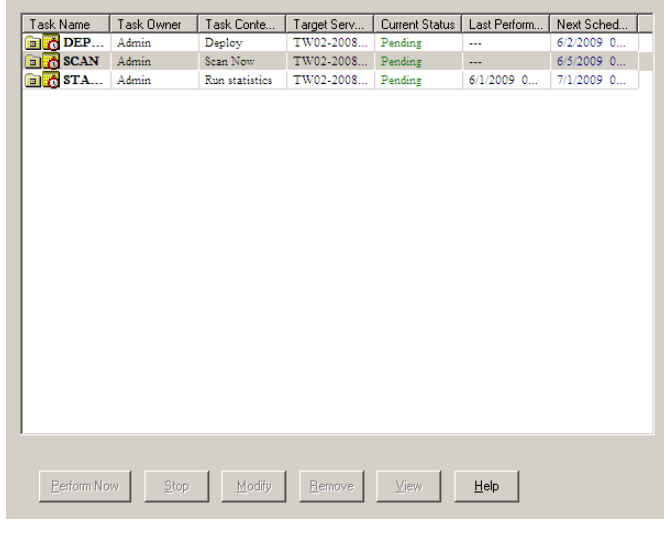


図 3-21. 既存のタスクを表形式で表示

注意： タスクが適用されるサーバが異なる時間帯 (タイムゾーン) にある場合、[Last Perform Time] および [Next Schedule] に表示される日付 / 時刻には各サーバの現地時刻が反映されます。

既存のタスクの実行

[Existing Task] リストには、定義されているすべてのタスク情報が表示されます。このリストを使ってタスクを実行できます。

既存のタスクを実行するには、次の手順に従ってください。

1. 次のいずれかの操作を実行してください。
   - サイドバーから [Task] → [Existing Task] の順に選択します。
   - メインメニューから [Do] → [Existing Task] の順に選択します。

   [Existing Task] リストには、現在 ServerProtect で定義されているすべてのタスクが表示されます。
2. 実行するタスクを選択し、[Perform Now] ボタンをクリックします。

既存のタスクの変更

既存のタスクを変更して利用することで、タスクの新規作成、設定にかかる時間を節約することができます。

既存のタスクを変更するには、次の手順に従ってください。

1. 次のいずれかの操作を実行してください。
   - サイドバーから [Task] → [Existing Task] の順に選択します。
   - メインメニューから [Do] → [Existing Task] の順に選択します。

   [Existing Task] リストが表示されます。
2. [Existing Task] リストで修正したいタスクを選択します。
3. [変更] をクリックします。[Modify Task] ダイアログボックスが表示されます。

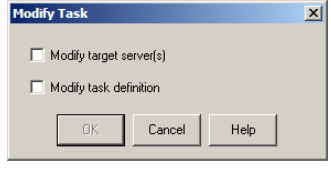


図 3-22. [Modify Task] ダイアログボックス

4. 次のいずれかの操作を実行してください。
   - [Modify target server (s)] チェックボックスをオンにすると、タスクの実行先サーバを変更できます。
   - [Modify task definition] チェックボックスをオンにすると、既存タスクの定義内容を変更できます。
5. [OK] をクリックします。

既存のタスクの実行対象サーバを変更するには、次の手順に従ってください。

1. [Select Servers to Apply Tasks] 画面で、タスクを実行するサーバを選択して追加します。
2. [Add] をクリックします。

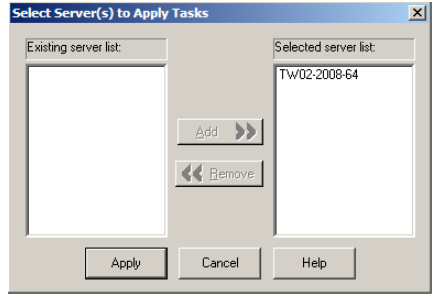


図 3-23. [Select Servers to Apply Tasks] ダイアログボックス

3. [Apply] ボタンをクリックします。変更内容を保存せずに画面を閉じるには、[Cancel] をクリックします。

既存のタスクのタスク定義を変更するには、次の手順に従ってください。

1. [Existing Tasks] リストから、変更するタスクに含めたい機能を選択します。

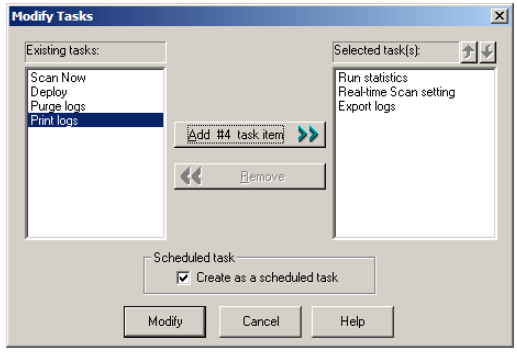


図 3-24. [Modify Task] ダイアログボックス

2. [Add #n Task Item] ボタンをクリックして、手順 1 で選択した機能を [Selected task (s)] リストボックスに追加します (「#n」はタスクアイテムの番号を示します)。

   このタスクを予約して自動的に実行したい場合は、必ず [Create as a scheduled task] チェックボックスを有効にしてください。

ヒント： 機能の実行順序を変更するには、順序を変更する機能を選択し、[Selected task (s)] リストボックスの上にある上下の矢印アイコンをクリックします。配信機能は常にこのリストの最後である必要があります。

---

3. [Modify] ボタンをクリックすると、選択した機能からタスクを作成するためのウィザードが起動します。

既存のタスクの表示

既存タスクの属性は [Existing Task] ダイアログボックスに表示され、タスクを実行する前に内容を確認できます。

既存のタスクを表示するには、次の手順に従ってください。

1. 次のいずれかの操作を実行してください。
   - メインメニューから [Do] → [Existing Task] の順に選択します。
   - サイドバーから [Task] → [Existing Task] の順に選択します。

2. [Existing Task] リストで表示するタスクを選択します。
3. [View] ボタンをクリックします。または [Existing Task] の画面の表から任意のタスクのエントリをダブルクリックします。[View Task Information] ダイアログボックスが表示されます。

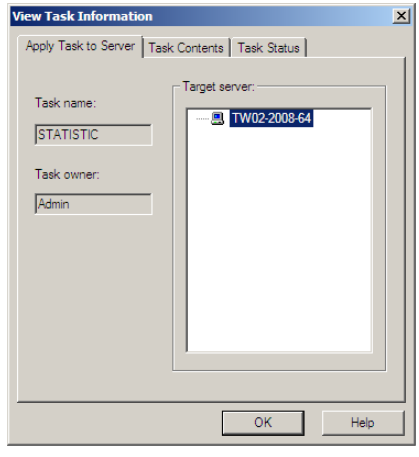


図 3-25. [View Task Information] ダイアログボックス

このダイアログボックスには [Apply Task to Server]、[Task Contents]、[Task Status] という 3 つのタブがあります。

- [Apply Task to Server]: タブの左側にタスク名とタスク所有者が表示されます。[Target server] には、タスクを実行するネットワーク上のすべてのサーバが表示されます。
- [Task Contents]: タスクを構成するすべての機能が表示されます。[Task sequence] リストボックスの機能アイコンを選択すると、右の [task definition] 欄に機能の定義が表示されます。
- [Task Status]: [Target Server] には、タスクを実行するネットワーク上のすべてのサーバが表示されます。[Current Status]、[Last Perform Time]、および [Next Schedule] の各フィールドには、タスクのステータス、前回の実行日時などが表示されます。

4. [OK] ボタンをクリックして、[View Task Information] ダイアログボックスを閉じます。

既存のタスクの削除

[Existing Task] リストには、定義されているすべてのタスク情報が表示されます。このリストを使用してタスクの定義を削除できます。

既存のタスクを削除するには、次の手順に従ってください。

1. 次のいずれかの操作を実行してください。
   - メインメニューから [Do] → [Existing Task] の順に選択します。
   - サイドバーから [Task] → [Existing Task] の順に選択します。
2. [Existing Task] リストで削除するタスクを選択します。
3. [Remove] ボタンをクリックします。

通知メッセージの設定

ウイルス検出時にウイルス対策ソフトウェアからユーザまたは管理者に通知を送信する機能は、ユーザや管理者にとって非常に役立つものです。ServerProtect では、通知内容と送信者を必要に応じて設定することができます。

ServerProtect には一般の警告とアウトブレークアラートの 2 種類の警告があります。それぞれの警告について、管理者に通知する方法を選択できます。警告方法の詳細については、97 ページの「警告方法の設定」を参照してください。

一般の警告

指定されたサーバで指定されたイベントが検出された場合に、一般の警告が生成されます。ServerProtect にはメッセージにテキストを追加したり、カスタマイズされたメッセージを作成するオプションがあります。

通知イベント

ServerProtect ネットワーク上のサーバで、次のいずれかのイベントが発生した場合、通知を発行するよう設定することができます。

- **ウイルス不正プログラムの検出** : サーバ上に感染ファイルを検出した場合
- **スパイウェア / グレーウェアの検出** : サーバ上にスパイウェア / グレーウェア感染ファイルを検出した場合

- **書込み禁止ファイルの変更の試み** : 書込み禁止ファイルの変更の試みを検出した場合
- **リアルタイム検索設定の変更**リアルタイム検索設定の変更を検出した場合
- **サービスの起動 / 停止** :ServerProtect の起動 / 停止イベントを検出した場合
- **ウイルスパターンの有効期限切れ** : ウイルスパターンファイルの有効期限切れを検出した場合
- **スパイウェアパターンの有効期限切れ** : スパイウェアパターンファイルの有効期限切れを検出した場合

一般の警告の発行を設定するには、次の手順に従ってください。

1. ドメインブラウザツリーからインフォメーションサーバ、ドメイン、または一般サーバを選択します。
2. 次のいずれかの操作を実行してください。
   - メインメニューから [Configure] → [Notifications] → [Standard Alert] の順に選択します。
   - 左のサイドバーから [Set Notification] → [Standard Alert] の順に選択します。

   画面の右側に [Standard Alert] の設定データ領域が表示されます。

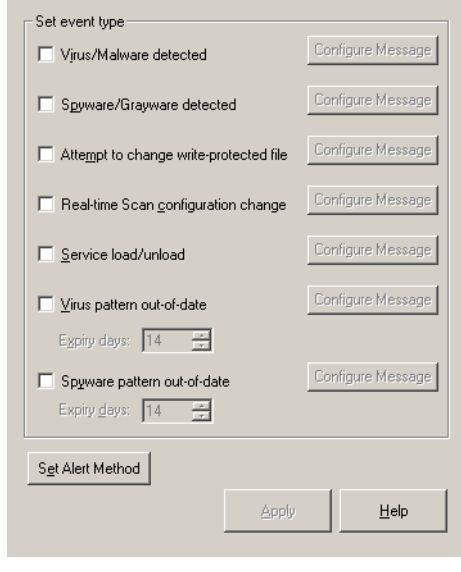


図 3-26. 一般の警告の設定

3. 通知対象とするウイルスイベントまたはプログラムイベントのチェックボックスを有効にします。

4. 選択した通知方法の右側にある [Configure Message] ボタンをクリックします。[Configure Alert Message] ダイアログボックスが表示されます。
5. 警告メッセージの内容を入力したら、[OK] をクリックしてダイアログボックスを閉じます。(日本語での入力も可能です。)
6. [Set Alert Method] ボタンをクリックして、通知方法を選択します。詳細については、97 ページの「警告方法の設定」を参照してください。

注意： 警告メッセージの詳細については、オンラインヘルプを参照してください。

アウトブレークアラート

ウイルスのアウトブレークとは、短期間に大量のウイルスイベントが発生することを意味します。システム管理者が定義した条件を超える数のウイルスイベントが発生すると、アウトブレークアラートが発行され、システム管理者に通知されます。

システム管理者、または他に通知が必要な受信者がアウトブレークアラートを受信することで、ウイルスに対して迅速に対応することができます。アウトブレークアラートに使用するメッセージはカスタマイズが可能です。

アウトブレークアラートを設定するには、次の手順に従ってください。

1. ドメインブラウザツリーからインフォメーションサーバ、ドメイン、一般サーバのいずれかのアイコンを選択します。
2. 次のいずれかの操作を実行してください。
   - 左のサイドバーから [Set Notification] → [Outbreak Alert] の順に選択します。
   - メインメニューから [Configure] → [Notifications] → [Outbreak Alert] の順に選択します。

[Outbreak Alert] の設定画面が画面の右側に表示されます。

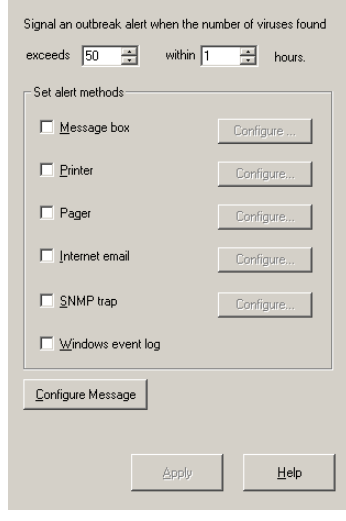


図 3-27. アウトブレークアラートの設定

3. ウイルスのアウトブレークを定義します。アウトブレークアラート送信の条件とするウイルスの検出数と時間を入力します。
4. ウイルスのアウトブレークアラートの通知に使用する方法 (警告方法) を選択します。
5. 選択した警告方法の右側にある [Configure] ボタンをクリックし、送信先の情報を入力します。各警告方法の詳細については、97 ページの「警告方法の設定」を参照してください。
6. [Configure Message] ボタンをクリックし、ウイルスのアウトブレークが発生した場合に表示するメッセージを設定することができます。(日本語での入力も可能です。)
7. [Apply] ボタンをクリックして、変更内容を保存します。

警告方法の設定

ServerProtect では、ウイルスイベント発生時にさまざまな方法でシステム管理者または特定のユーザに通知することができます。警告は次の方法で通知することができます。

- Message box (**メッセージボックス**): 管理者のコンピュータに、標準的な Windows ポップアップメッセージボックスが表示されます。
- Printer (**プリンタ**): メッセージがローカルまたはネットワークプリンタに送信されます。

- Pager (ポケットベル): メッセージがポケットベルに送信されます。この機能を使用するには、ServerProtect が動作しているサーバにモデムが接続されている必要があります。
- Internet Mail (インターネットメール): ユーザ設定に応じて、メールメッセージを送信できます。
- SNMP Trap (SNMP トラップ): SNMP トラップ対応の管理コンソールを使用しているネットワーク管理者に、SNMP トラップによる警告メッセージが送信されます。
- Windows Event Log (Windows イベントログ): ウイルスの検出が Windows のイベントログに書き込まれます。

複数の警告方法を設定することもできます。メールを使用した通知の設定手順については、次に説明します。インターネットメール以外の通知方法の設定手順については、オンラインヘルプを参照してください。

インターネットメール (メール) 警告を設定するには

1. ドメインブラウザツリーからインフォメーションサーバ、ドメイン、一般サーバのいずれかのアイコンを選択します。
2. 次の操作を実行して、警告方法を設定するための画面を表示します。

   アウトブレークアラートを設定するには

   次のいずれかの操作を実行してください。

   - サイドバーから [Set Notification] → [Outbreak Alert] の順に選択します。
   - メインメニューから [Configure] → [Notifications] → [Outbreak Alert] の順に選択します。

   一般の警告を設定するには

   次のいずれかの操作を実行してください。

   - メインメニューから [Configure] → [Notifications] → [Standard Alert] の順に選択して、[Set Alert Method] をクリックします。
   - サイドバーから [Set Notification] → [Standard Alert] の順に選択して、[Set Alert Method] をクリックします。

3. [Internet mail] チェックボックスをオンにし、対応する [Configure] ボタンをクリックします。[Configure Internet Mail] ダイアログボックスが表示されます。

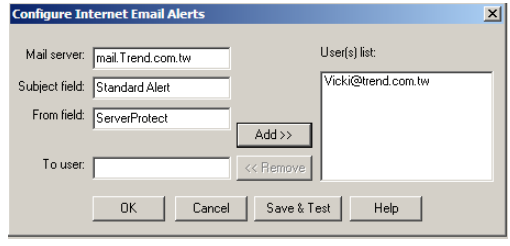


図 3-28. [Configure Internet Mail] ダイアログボックス

4. 次の操作を実行してください。
   a. メールサーバソフトウェアが動作しているサーバを [Mail Server] に入力します。
   b. メッセージの件名を [Subject field] に入力します。
   c. メッセージの [From field] テキストボックスに送信者のメールアドレスを入力します。
5. メールの送信先を [To user] テキストボックスに入力します。[Add] ボタンをクリックし、受信者アドレスをユーザリストに追加します。ユーザを選択して [Remove] ボタンをクリックすると、受信者を削除することができます。
6. 設定が完了したら、画面の下にある [Save & Test] ボタンをクリックして設定内容で正しく動作するか確認してください。設定が正しければ、ユーザリストで指定したアドレスにテストメールが送信されます。
7. 設定が完了したら [OK] ボタンをクリックして設定変更を保存します。

注意： 警告メッセージの設定の詳細については、オンラインヘルプを参照してください。

ウイルス検索

ServerProtect の一般サーバのウイルス検索には、リアルタイム検索、手動検索 (ScanNow)、予約検索 (タスク検索) の 3 種類があります。

リアルタイム検索は、サーバ上の入力ファイル、出力ファイルを監視し、ウイルスの侵入をリアルタイムで検出します。手動検索は、ウイルスの危険にさらされたと思われる場合や、すぐに情報が欲しい場合にサーバをチェックするのに有効な方法で、実行するとすぐに検索を開始します。予約検索は、ServerProtect サーバにウイルス感染ファイルがないかを、定期的または指定した日時に自動的に検索します。

ServerProtect では感染ファイルに対する処理として、放置 (手動処理)、削除、拡張子変更、隔離、ウイルス駆除の 5 つの処理から選択することができます。

また、次の処理を設定することができます。

- 検索するファイルの種類を選択する
- 書込み禁止リストを使用して、指定したファイルまたはディレクトリがユーザに変更されたり削除されないように設定する書込み禁止リストの設定の詳細については、オンラインヘルプを参照してください。

注意： 検索結果は検索結果ログで確認することができます。[Scan Result] 画面から感染ファイルに対して直接処理を実行できます。つまり、ウイルス感染イベントの発生時に適切な処理を実行できます。詳細については、オンラインヘルプの「Viewing Scan Result Information」トピックを参照してください。

ウイルスに対する処理の設定

ServerProtect では、リアルタイム検索または手動検索によりネットワーク上で検出されたウイルス感染ファイルに対してどのような処理を実行するかを設定することができます。

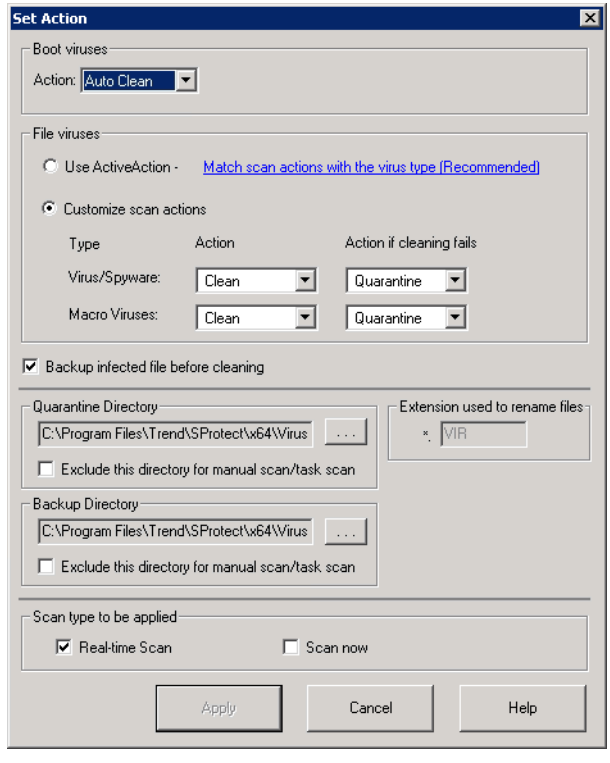


図 3-29.　一般サーバの [Set Action] ダイアログボックス

任意のウイルスに対する処理を設定するには、次の手順に従ってください。

1. リアルタイム検索または手動検索設定領域で　[Set Action] ボタンをクリックします。[Set Action] ダイアログボックスが表示されます。

注意：　スパイウェアでは、駆除処理はサポートされていません。ウイルスに対する処理が駆除 / 削除である場合、スパイウェアでは削除処理のみが実行されます。

---

2. [Boot Viruses] グループの [Action] ドロップダウンリストから、システム感染型ウイルスの検出時の処理を選択します。[Auto Clean] または [Bypass] のいずれかを選択することができます。
3. [File Viruses] グループで、次のいずれかの操作を実行してください。
   - スパイウェアの感染を処理する設定として実行可能なのは「放置」のみであり、「ウイルス駆除」はスパイウェアの感染を処理する場合はサポートされていません。

     注意： 「トレンドマイクロの推奨処理」を使用した場合、スパイウェアに対する処理は放置 (手動処理) になります。

   - [Customize scan actions] オプションを選択して、ファイル感染型ウイルスとマクロウイルスのそれぞれについて、[Action]、および [Action if cleaning fails] リストから適切な処理を選択します。詳細については、22 ページの「ウイルスを検出した場合」を参照してください。トレンドマイクロの推奨設定の詳細については、28 ページの「トレンドマイクロの推奨設定」を参照してください。

     注意： [Clean] を選択した場合は、[Backup infected file before cleaning] オプションを有効にすることをお勧めします。ウイルス駆除によって元のファイルが壊れて使えなくなる場合があるからです。

     バックアップディレクトリおよび隔離ディレクトリを検索対象から除外する必要があります。選択された検索の種類が [Scan type to be applied] ダイアログボックスに表示されます。
4. [Apply] ボタンをクリックして、設定を保存します。

検索プロファイル

リアルタイム検索および手動検索の設定を検索プロファイルとして保存し、検索タスクを新規作成したり、既存のタスクの変更に利用することができます。また、必要のなくなったプロファイルを削除することもできます。検索プロファイルは手動検索およびリアルタイム検索タスクの設定時に適用されます。検索プロファイルの詳細については、オンラインヘルプの「検索プロファイルの設定」トピックを参照してください。

予約検索タスクなどタスクを作成する際には、既存の検索プロファイルを選択することも、独自の検索プロファイルを作成することもできます。詳細については、90 ページの「既存のタスクの変更」を参照してください。

プロファイルを保存するには、次の手順に従ってください。

1. リアルタイム検索または手動検索の設定を実行します。詳細については、104 ページの「検索の設定」を参照してください。
2. [Save As/ Delete Profile] ボタンをクリックすると、[Save/Delete Profile] ダイアログボックスが表示されます。

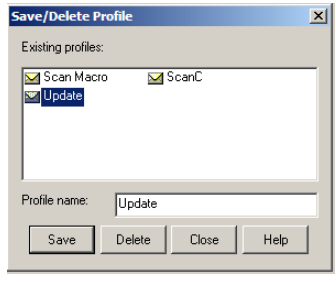


図 3-30. [Save/Delete Profile] ダイアログボックス

3. プロファイルの名前を [Profile name] フィールドに入力します。
4. [Save] をクリックして変更を保存します。

プロファイルを削除するには、次の手順に従ってください。

1. 次のいずれかの操作を実行してください。
   - サイドバーから [Scan Now] → [Scan Now] の順に選択します。
   - メインメニューから [Do] → [Scan Now] の順に選択します。
   - サイドバーから [Set Scan option] → [Real-time Scan] の順に選択します。
   - メインメニューから [Configure] → [Scan Options] → [Real-time Scan] の順に選択します。
2. [Save As/ Delete Profile] ボタンをクリックすると、[Save/Delete Profile] ダイアログボックスが表示されます。
3. [Existing Profiles] リストで対象となるプロファイルの名前を選択します。
4. [Delete] ボタンをクリックします。

リアルタイム検索

リアルタイム検索は、ウイルスの侵入をリアルタイムで検出します。Celerra File Server システムと AV サーバの両方を保護するために、ServerProtect のリアルタイム検索機能の初期設定は「入出力ファイル」になっています。これにより、すべての入力ファイル、出力ファイルが監視され、ウイルス感染ファイルがサーバからコピーされたり、またはサーバにコピーされることを未然に防止することができます。

ストレージデバイスから次のイベントを受信すると、EMC CAVA はストレージデバイス内のファイルにリアルタイム検索を実行します。

- ストレージデバイスでファイルの名前が変更された。
- ストレージデバイスにファイルがコピーまたは保存された。
- ストレージデバイスでファイルが変更され閉じられた。

リアルタイム検索の実行条件をより厳密に定義したい場合は、お使いのストレージデバイスのドキュメントを参照してください。

検索の設定

リアルタイム検索では、次のオプションを指定することができます。

- **起動時のフロッピーディスク検索** : コンピュータを起動すると、フロッピーディスクドライブ内のディスクのシステム領域感染型ウイルスも検索されます。こうすることで、ウイルスに感染したディスクからのコンピュータの起動を防止できます。
- **シャットダウン時のフロッピーディスク検索** : コンピュータをシャットダウンするときにフロッピーディスクドライブをチェックし、ディスクがあればシステム領域感染型ウイルスを検索します。
- **フロッピーディスクのシステム領域を検索** : コンピュータのフロッピーディスクのシステム領域を検索し、システム領域感染型ウイルスからシステムを保護します。
- **MacroTrap を有効にする** :ServerProtect は MacroTrap 技術を駆使して、Microsoft Office ファイルおよびテンプレートに潜むマクロウイルスからの感染を防止します。
- **OLE 埋め込みの検索** :Microsoft Office の埋め込みファイルを検索することができます。ServerProtect では、最大 5 重に埋め込まれた OLE オブジェクトを検索することができます。詳細については、27 ページの「OLE 埋め込みの検索」を参照してください。
- **マップされたネットワークドライブの検索** : ServerProtect では、ネットワークドライブを検索対象に選択することができます (あらかじめネットワークドライブを割り当てておく必要があります)。

リアルタイム検索を設定するには、次の手順に従ってください。

1. ドメインブラウザツリーからインフォメーションサーバ、ドメイン、または一般サーバを選択します。
2. 次のいずれかの操作を実行してください。
   - サイドバーから [Set Scan option] → [Real-time Scan] の順に選択します。
   - メインメニューから [Configure] → [Scan Options] → [Real time Scan] の順に選択します。

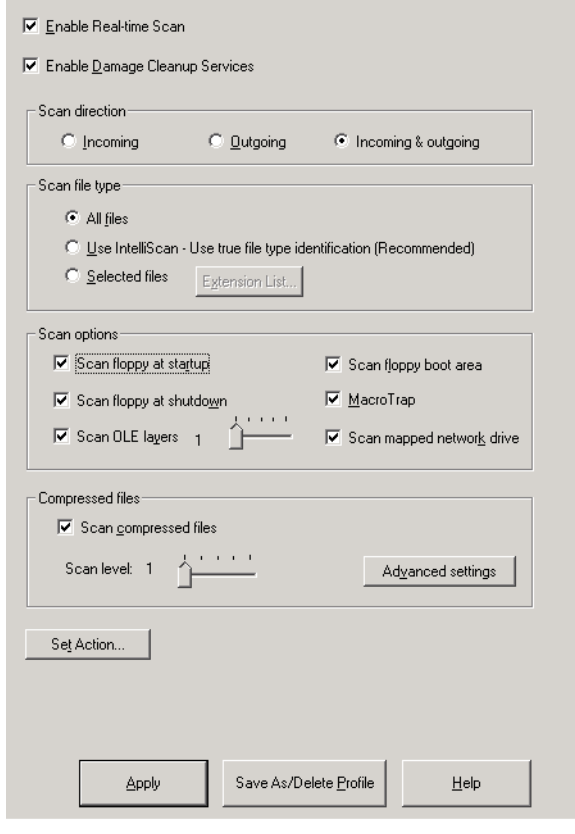


図 3-31. リアルタイム検索の設定

3. 画面上部の [Enable Real-time Scan] チェックボックスをオンにします。

4. [Enable Damage Cleanup Services] チェックボックスをオンにして、ダメージクリーンナップエンジンで、トロイの木馬およびトロイの木馬プロセスを検索して削除できるようにします。32 ビットおよび 64 ビットのプラットフォームがサポートされます。このサービスを無効にする場合は、チェックボックスをオフにします。
5. [Scan direction] グループで、検索するファイルの方向を選択します。
   - [Outgoing] : サーバからコピーされるファイルを検索します。
   - [Incoming and Outgoing] : サーバ上の入力、出力、両方向のファイルを検索します。

注意： EMC CAVA では [Incoming] オプションはサポートされません。[Incoming & Outgoing] を選択して、両方向のファイルを検索することをお勧めします。

---

6. [Scan file type] グループで検索対象のファイルを選択します。
   - [All files] : すべてのファイルを検索します。
   - [IntelliScan] : トレンドマイクロが推奨する設定に基づいて検索を実行します。

     詳細については、28 ページの「トレンドマイクロの推奨設定」を参照してください。
   - [Selected files] : 指定された種類のファイルのみを検索します。

     [Extension List] ボタンをクリックして検索するファイルの種類を定義します。詳細は、113 ページの「検索対象ファイルの種類 (拡張子) の選択」を参照してください。
7. [Scan options] グループでウイルス検索の動作を設定することができます。次のオプションがあります。
   - 起動時のフロッピーディスク検索
   - シャットダウン時のフロッピーディスク検索
   - OLE 埋め込みの検索
   - フロッピーディスクのシステム領域を検索
   - MacroTrap を有効にする
   - マップされたネットワークドライブの検索

   各検索オプションの詳細については、104 ページの「検索の設定」を参照してください。
8. 圧縮ファイルを検索する場合は、[Scan compressed files] チェックボックスをオンにしてください。また、[Scan level] を調整して、検索する圧縮階層数を 1 ～ 5 の間で選択します。圧縮ファイルの詳細設定については、オンラインヘルプを参照してください。

注意： 手順 5 で [Selected files] を選択した場合は、拡張子リストで必ず圧縮ファイルの拡張子を選択してください。

---

9. [Set Action] ボタンをクリックして、感染ファイルに対する処理を設定します。詳細については、101 ページの「ウイルスに対する処理の設定」を参照してください。
10. [Apply] ボタンをクリックして設定を保存するか、または [Save As/Delete Profile] ボタンをクリックして、設定を適用せずにプロファイルとして保存し、後で利用することができます。

手動検索 (ScanNow)

手動検索では、必要なときに検索を実行できます。コンピュータウイルスに感染したと思われるコンピュータや、すぐに情報を必要とするコンピュータをチェックする場合に効果的です。

手動検索では、次のオプションを指定することができます。

- 検索対象
- 検索するファイルの種類
- 検索オプション
- 圧縮ファイルの検索
- 検索の優先度
- 検索処理

手動検索を開始するには

1. ドメインブラウザツリーからインフォメーションサーバ、ドメイン、または一般サーバをクリックします。
2. 次のいずれかの操作を実行して、手動検索 (ScanNow) の設定画面 (図 3-34) を表示します。
   - サイドバーから [ScanNow] → [ScanNow] の順に選択します。

- メインメニューから [Do] → [ScanNow] の順に選択します。

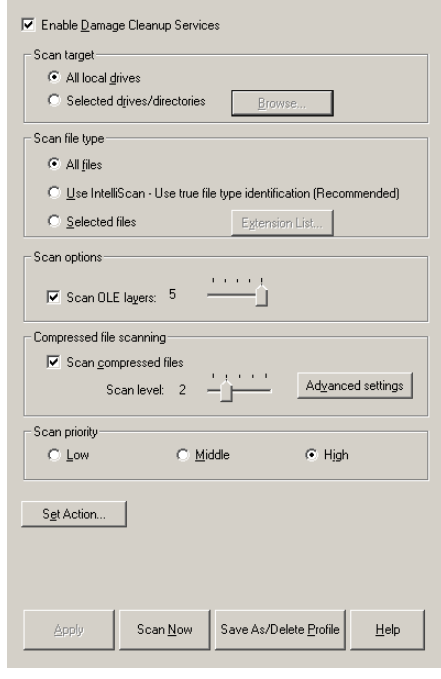


図 3-32. 手動検索の設定

3. [Enable Damage Cleanup Service] チェックボックスをオンにして、このサービスを有効にします。無効にする場合は、チェックボックスをオフにします。
4. [Scan target] グループで次のオプションを選択します。
   - [All local drives] : サーバ上のすべてのドライブが検索されます。
   - [Selected drives/directories] : 選択したドライブまたはディレクトリだけを検索する場合は

[Browse] ボタンをクリックして、[Add Drives and/or Directories] ダイアログボックスを表示します。ウイルス検索を実行するドライブまたはディレクトリの名前の前にあるチェックボックスをオンにし、選択が終わったら [OK] をクリックします。

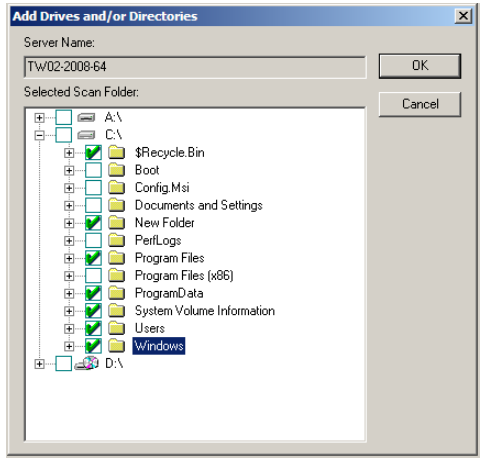


図 3-33. [Add Drives and/or Directories] ダイアログボックス

5. [Scan file type] グループで次のオプションを選択します。
   - [All files]: すべてのファイルを検索します。
   - [Use IntelliScan]: トレンドマイクロが推奨する設定に基づいて検索を実行します。

     詳細については、28 ページの「トレンドマイクロの推奨設定」を参照してください。
   - [Selected files]: 指定された種類のファイルのみを検索します。

     [Extension List] ボタンをクリックして検索するファイルの種類を定義します。詳細は、113 ページの「検索対象ファイルの種類 (拡張子) の選択」を参照してください。
6. OLE 埋め込みオブジェクトを検索対象に含める場合は、[Scan options] グループで [Scan OLE layers] チェックボックスをオンにします。スライダを調整して、検索レベル (階層数) を 1 ～ 5 の間で指定することもできます。ServerProtect では、最大 5 レベル (階層) まで検索対象に含めることができます。
7. 圧縮ファイルを検索する場合は、[Scan compressed files] チェックボックスをオンにします。[Scan level] スライダを調整して、検索レベル (階層数) を 1 ～ 5 の間で指定することもできます。圧縮ファイルの詳細設定については、オンラインヘルプを参照してください。

注意： 手順 4 で [Selected files] を選択した場合は、拡張子リストに必ず圧縮ファイルの拡張子を含めてください。

8. 検索中に使用する [Scan priority] を設定します。これは ServerProtect を実行するために確保しておく CPU リソースの量を設定するものです。[Low]、[Middle]、[High] から選択してください。ただし、ServerProtect 以外に CPU リソースを消費するプロセスがない場合は、[Low] や [Middle] に設定していても CPU 使用率は高くなります。
9. [Set Action] ボタンをクリックして、感染ファイルに対する処理を設定します。詳細については、101 ページの「ウイルスに対する処理の設定」を参照してください。

必要なファイル検索設定を指定し、[OK] をクリックします。

10. [Apply] ボタンをクリックして設定内容を適用するか、または [Save As Profile] ボタンをクリックして、検索パラメータをプロファイルとして保存します。

ScanNow ツールの実行 (Windows 一般サーバ)

ScanNow ツールを使用して、管理コンソールにアクセスせずに Windows Server ファミリサーバのウイルス検索を実行できます。ScanNow ツールが起動すると、管理コンソールで設定されている手動検索の検索対象、検索するファイルの種類などの設定でウイルス検索が実行されます。

ScanNow ツールを起動するには、次の手順に従ってください。

1. 一般サーバで [スタート] メニューから [すべてのプログラム] → [アクセサリ] → [エクスプローラー] の順に選択します。Windows エクスプローラが起動します。
2. ServerProtect をインストールしたフォルダをクリックします。32 ビット OS の場合、初期設定では次のフォルダにインストールされています。

   ```
   C:¥Program Files¥Trend¥SProtect
   ```

   64 ビット OS の場合、初期設定では次のフォルダにインストールされています。

   ```
   C:¥Program Files¥Trend¥SProtect¥x64
   ```

3. ScanNow.exe をダブルクリックします。ScanNow が実行されます。

ScanNow を停止するには、次の手順に従ってください。

1. 一般サーバで [スタート] メニューから、[ファイル名を指定して実行] を選択します。[ファイル名を指定して実行] ダイアログボックスが表示されます。
2. [参照] をクリックして、ScanNow.exe ファイルの場所を指定します。

   32 ビット OS の場合、初期設定では次のフォルダにインストールされています。

   ```
   C:¥Program Files¥Trend¥SProtect
   ```

   64 ビット OS の場合、初期設定では次のフォルダにインストールされています。

   ```
   C:¥Program Files¥Trend¥SProtect¥x64
   ```

3. ScanNow ツールを、「stop」スイッチを付けて実行します。[名前] テキストボックスに次のように入力してください。

   32 ビット OS の場合

   ```
   C:¥Program Files¥Trend¥SProtect¥ScanNow.exe /STOP
   ```

   64 ビット OS の場合

   ```
   C:¥Program Files¥Trend¥SProtect¥x64¥ScanNow.exe /STOP
   ```

4. [OK] をクリックします。ScanNow の実行が停止されます。

注意： ScanNow.exe のパスと「/STOP」スイッチの間には、半角スペースが必要です。

予約検索 (タスク検索)

予約検索では、設定されたスケジュールに従ってウイルス検索が実行されます。これにより、一般サーバのウイルス検索を自動化することができます。手動検索 (ScanNow) またはリアルタイム検索の予約を設定するには、予約タスクを使用します。

予約検索の設定

予約タスクを使用して、ScanNow またはリアルタイム検索の予約を設定することができます。詳細については、85 ページの「新規タスクの作成」を参照してください。

注意： ServerProtect サーバのインストール時には、初期設定で毎週金曜日にすべてのローカルディレクトリのウイルスを検索するよう設定されています。

必要に応じて、初期設定のタスクを編集したり、新規タスクを作成したりできます。新規タスクの作成には、ServerProtect のタスクウィザードを利用できます。

検索対象ファイルの種類 (拡張子) の選択

リアルタイム検索、手動検索 (ScanNow)、予約検索 (タスク検索) の設定時にファイルの拡張子を選択し、ウイルス検索の対象とするファイルの種類を選択することができます。ウイルスは、特定の種類のファイルにのみ感染します。この機能を利用して、ウイルス感染が確認されていないファイルの種類を検索対象から除外することができます。

検索するファイルの拡張子を追加するには、次の手順に従ってください。

1. [Real-time Scan] または [Scan Now] の設定画面で、[Scan file type] の [Selected files] を選択し、[Extension List] をクリックして、検索するファイルの種類を指定します。[Select Files for Scanning] ダイアログボックスが表示されます。

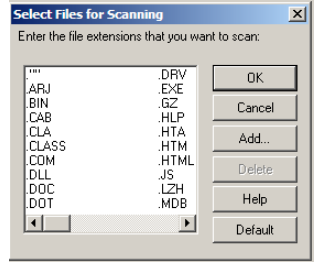


図 3-34. [Select Files for Scanning] ダイアログボックス

2. 次のいずれかの操作を実行してください。
   - [Add] をクリックします。[Add Program File Extension] ダイアログボックスが表示されます。

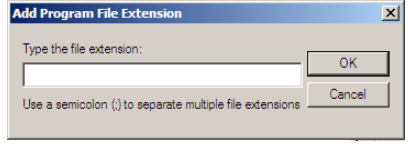


図 3-35. [Add Program File Extension] ダイアログボックス

検索対象ファイルの拡張子を入力し、[OK] をクリックします。

- 初期設定値を使用する場合は、[Default] ボタンをクリックします。または、[Cancel] をクリックすると、変更内容が保存されずに画面が閉じます。

  検索対象とする拡張子の初期設定は、トレンドマイクロの推奨する設定値です。この設定によってほとんどの環境で十分なウイルス対策を実施できます (ウイルス対策の動向により、初期設定の拡張子リストに追加が必要な場合もあります)。初期設定値には、次の拡張子が含まれます。

"" (拡張子なし)	.BIN	.CAB	.CLA
.ARJ	.COM	.DLL	.DOC
.CLASS	.DRV	.EXE	.GZ
.DOT	.HTA	.HTM	.HTML
.HLP	.LZH	.MDB	.MPP
.JS	.MSG	.OCX	.OFT
.MPT	.PIF	.POT	.PPS
.OVL	.RAR	.RTF	.SCR
.PPT	.SYS	.TAR	.VBS
.SHS	.VST	.XLA	.XLS
.VSD	.Z	.ZIP	
.XLT			

- 拡張子をリストから削除する場合は、削除する拡張子を選択して [Delete] ボタンをクリックします。

注意： EMC Celerra File Server システムでの設定と同様に、ServerProtect で、検索設定の [Scan file type] に、Scan file type ウイルス検索対象のファイル拡張子を指定する必要があります。

検索対象として指定されているファイル拡張子のリストは、EMC Celerra File Server システム上の viruschecker.conf ファイルに保存されます。

検索対象ファイルの拡張子を除外するには、次の手順に従ってください。

1. 左のサイドバーから [Set Scan Option] → [Exclusion List] の順に選択します。
2. メインメニューから [Configure] → [Scan Options] → [Exclusion List] の順に選択します。

3. [Excluded file extension list] で [Add] をクリックします。[Add Program File Extension] ダイアログボックスが表示されます。

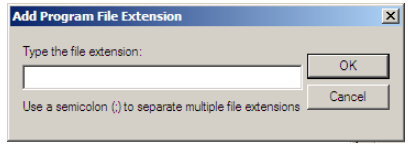


図 3-36. [Add Program File Extension] ダイアログボックス

4. 検索から除外するファイルの拡張子を入力します。複数のファイル拡張子を指定する場合は、セミコロン (;) で区切ります。
5. [OK] をクリックします。
6. 既に入力したファイル拡張子を削除するには、該当するファイル名を [Excluded file extension list] から選択し [Remove] をクリックします。
7. [Apply] ボタンをクリックします。

第 4 章

既存の ServerProtect のアップグレード

ServerProtect では、製品の以前のバージョンからのアップグレードと移行がサポートされています。古いバージョンの設定は、新しいバージョンのアプリケーションに移行できます。

バージョン 5.58 のインストールプログラムは、一般サーバ、インフォメーションサーバ、管理コンソールなど、既存の ServerProtect コンポーネントを検出できます。このアップグレードおよび移行機能は、ServerProtect インストールプログラムの必要不可欠な部分です。本章では、キーとなるコンセプトを紹介し、この機能の使用方法について説明します。

本章で説明する内容には、次の項目が含まれます。

ServerProtect のアップグレード機能の概要

多くの場合、ServerProtect 5.58 など、ネットワークサーバシステムに既にインストールされている古いバージョンがあります。ServerProtect 5.8 に組み込まれているアップグレード機能は、ユーザが目的を達成するのに役立つ数多くのオプションを提供します。この概要では、それらのオプションについて説明し、関連するキーコンセプトを紹介します。

1. ServerProtect 5.8 インフォメーションサーバは、ServerProtect 5.58 一般サーバを管理できます。そのため、インフォメーションサーバをアップグレードして、古い一般サーバを継続して管理することができます。

   注意： 「一般サーバの追加」または「一般サーバの移動」機能を選択して、古いバージョンの一般サーバをバージョン 5.8 のインフォメーションサーバに追加することはできません。

2. ServerProtect のインストールを開始し、最新バージョンである ServerProtect 5.8 のインフォメーションサーバがインストールされるよう正しい選択を行います。既存のインフォメーションサーバをアップグレードするには、インストール時に同じインストール先サーバを選択するだけで済みます。詳細については、119 ページの「インストールパッケージを使用した、ServerProtect のローカルアップグレード」を参照してください。
3. 最新バージョンの管理コンソールがインストールされていない場合は、管理コンソールコンポーネントをインストールします。詳細については、119 ページの「インストールパッケージを使用した、ServerProtect のローカルアップグレード」を参照してください。
4. この時点では、管理コンソールとインフォメーションサーバの準備はできています。一般サーバは、次の方法でアップグレードできます。
   - インストールパッケージを使用して、ローカルにアップグレードを実行する。
   - インストールパッケージを使用して、ネットワーク経由でリモートにアップグレードを実行する。
   - サイレントモードインストールを使用して、アップグレードを実行する。サイレントモードインストールは、一般サーバのみがインストールされているコンピュータのアップグレードに使用してください。他のコンポーネントがインストールされていることが検出されると、サイレントインストーラは終了し、何も実行しません。一般サーバをアップグレードするときはこの方法を使用することをお勧めします。この方法を使用すると、リモートの実行先コンピュータでインフォメーションサーバが誤ってアップグレードされることを回避できます。

この章の以降の説明では、総合的な情報を提供することに主眼を置きます。主な目的は一般サーバのアップグレードの実行方法について説明することですが、他のコンポーネントのアップグレードの詳細や、関連するキーコンセプトについても紹介し、ユーザが効率的かつ円滑にアップグレードを実行できるように支援します。

インストールパッケージを使用した、ServerProtect のローカルアップグレード

アップグレード機能は ServerProtect インストールプログラムの必要不可欠な部分なので、ユーザインタフェースで使用されている用語と実際のプログラムの動作は全く同じです。ServerProtect をローカルにアップグレードすることは、最も容易で信頼できるオプションです。さらに、管理コンソールコンポーネントをインストールまたはアップグレードするための唯一の方法でもあります。

ローカルアップグレードセッションを開始するには、インストールパッケージを使用して、ローカルコンピュータでインストールセッションを起動します。詳細については、38 ページの「ServerProtect のインストール」を参照してください。インストールプログラムは、手順全体を通じてユーザを導きます。ServerProtect の [Select Components] 画面を次に示します。

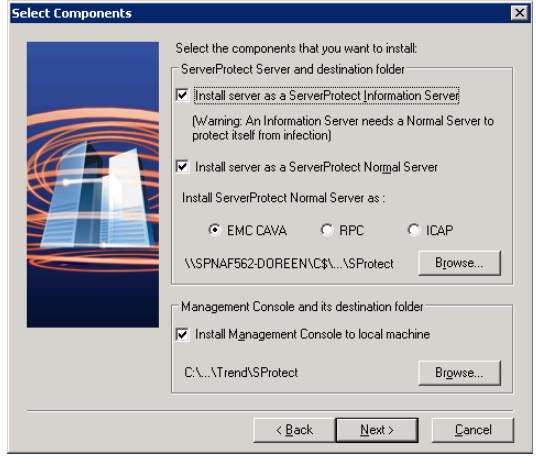


図 4-1. ServerProtect の [Select Components] 画面

注意： アップグレードを正常に実行するには、システム内に存在することが分かっているコンポーネントをすべて選択する必要があります。

該当するオプションのチェックボックスをオンにし、[Browse] をクリックして、[ServerProtect Installation Path Selection] 画面を表示します (詳細については、43 ページの「ServerProtect インストール先の選択」を参照してください)。ローカルコンピュータ上のアップグレード対象のフォルダに移動します。プログラムファイルがコピーされ、関連するすべてのサービスが開始されると、インストールプログラムはアップグレードを完了します。

注意： アップグレードする ServerProtect コンポーネントを選択する際、既に最新バージョンになっているものも含め、既存のすべてのコンポーネントを選択してください。そうしないと、操作を続行するには他のコンポーネントを選択する必要があることを伝えるメッセージボックスが表示されます。そして、[Selection Component] 画面が再表示され、選択をやり直すよう求められます。

注意： Trend Micro Infrastructure (TMI) CMAgent を最新製品リリースのインフォメーションサーバにインストールすると、Management Communication Protocol (MCP) CMAgent に自動的にアップグレードされます。

インストールパッケージを使用した、ServerProtect のリモートアップグレード

ServerProtect をリモートでアップグレードする方法は、ローカルでの方法と大きな違いはありません。ServerProtect インストールプログラムが起動したら、契約条件に同意し、正しいシリアル番号を入力します。すると、ServerProtect の [Select Components] 画面が表示されます。アップグレードの候補として一般サーバを選択し、(ローカルコンピュータ内を探すのではなく) [Browser] ボタンを使用して実行先のサーバを指定します。ユーザは、接続されているサーバネットワークシステムに移動し、アップグレード対象の一般サーバまたはインフォメーションサーバを検索することができます。そして、ローカルアップグレードのときと同じアップグレード操作を実行します。詳細については、38 ページの「ServerProtect のインストール」を参照してください。

注意： 管理コンソールコンポーネントのリモートインストールまたはアップグレードはサポートされていません。

サイレントモードインストールの実行による一般サーバのアップグレード

Microsoft Windows 環境では、DOS コマンドラインウィンドウでプログラムを実行すると、一定のメリットがあることはよく知られています。Windows シェルは、スクリプトファイル内のコマンドを解釈することが可能であるので、特定のタスクを自動化するためのスクリプトファイルを作成できます。ServerProtect 5.8 では、インストールプログラムをサイレントモードで起動できるので、ユーザはこの利点を活用できます。

注意： サイレントインストールは、一般サーバのみが存在するサーバのアップグレードに使用してください。他のコンポーネントがインストールされていることが検出されると、サイレントインストーラは終了し、何も実行しません。

サイレントモードを使用して ServerProtect をインストールするには

1. インフォメーションサーバをインストールします。
2. 初期設定のインストールパスで SMS フォルダを検索し、共有します。

   注意： 読み取りおよび書き込み権限のある SMS フォルダを共有します。

   一般サーバとしてインストールしたいサーバからこのフォルダにアクセスできることを確認してください。複数のサイレントインストールを実行する場合、インストール先のサーバに SMS フォルダをマッピングします。
3. インストール先のサーバでコマンドプロンプトを開き、SMS フォルダまたはフォルダをマップされたドライブに移動して次のコマンドを入力します。

   ```
   < ドライブ名 >:¥setup -SMS -s -m"SPEMC"
   ```

例 :

a. インストール先サーバで、SMS フォルダをドライブ「M」に割り当てます。
b. コマンドプロンプトを開きます。
c. たとえば、M ドライブに移動するには、次のように入力します。

   ```
   M:¥setup -SMS -s -m"SPEMC"
   ```

d. <Enter> キーを押します。

サイレントインストールが実行され、インストール先のサーバがインフォメーションサーバに登録されます。

サイレントインストールでは、一般サーバは「SMS」ドメインにインストールされます。サイレントインストール中にドメイン名を変更することはできませんが、一般サーバがすべてインストールされると、SMS ドメインの名前を変更できます。

また、ServerProtect をインストールするパスを指定することもできます。たとえば、ServerProtect を D:¥Utility¥AntiVirus¥SProtect というパスにインストールするには、次の手順を実行します。

1. SMS フォルダで Setup.ini ファイルを探します。
2. 次の行を追加します。

   ```
   [CommonSection]
   ServerTargetLocalPath=D:¥Utility¥AntiVirus¥Sprotect
   ```

   ここで、
   ServerTargetLocalPath: 一般サーバをインストールする場所を設定します。

インストールされた一般サーバのライセンスを取得するには、SMS フォルダの Setup.ini ファイルに次の行を追加します。

```
[CommonSection]
ServerTargetSN=XXXX-XXXX-XXXX-XXXX-XXXX
```

説明 :
XXXX-XXXX-XXXX-XXXX-XXXX: 有効なシリアル番号

インフォメーションサーバでドメインコントローラが使用されているため、「SMS」ドメインに一般サーバを登録できない場合があります。この問題を解決するには、サイレントインストールを実行する前に、IP アドレスを設定します。

IP アドレス指定してインストールするには

1. SMS フォルダで Setup.ini ファイルを探します。
2. AgentName の横にあるホスト名をその IP アドレスで置き換えて、ファイルを保存します。

注意 : アップグレードをサイレントモードで実行する際は、アップグレードする必要のあるすべてのインストール先サーバが含まれるように、SMS フォルダの共有について注意を払ってください。この強力なツールの使用に関する詳細については、52 ページの「サイレントモードでのインストール」を参照してください。

第 5 章

Trend Micro Control Manager との連携による ServerProtect の管理

Trend Micro Control Manager (以下 Control Manager) は、ウイルス対策を集中管理したり、ネットワーク全体に分散されているコンテンツにセキュリティ対策を実施する強力なツールです。管理、監視、および配信を 1 か所から実施できるため、ウイルス対策およびファイルセキュリティ戦略をより効率的に管理できます。

Control Manager では、Web ベースの管理コンソールが用意され、Microsoft Internet Explorer を使用して操作することができます。ServerProtect の管理コンソールと異なり、Control Manager 管理コンソールでは、複数のインフォメーションサーバを同時に管理できるため、ウイルス対策戦略の管理に、より高度で柔軟な制御が追加されます。

ServerProtect インフォメーションサーバの管理対象は、その配下に登録された一般サーバのみです。Control Manager の場合、インフォメーションサーバのグループを管理することができ、結果的に、その配下の一般サーバも管理対象になります。特に大規模なネットワークでは、Control Manager を使用することで、管理の簡易化が実現します。

本章で説明する内容には、次の項目が含まれます。

Trend Micro Control Manager

Control Manager は、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で動作するトレンドマイクロの各製品およびサービスを一元管理する集中管理コンソールです。Control Manager の Web ベースの管理コンソールを使用することで、ネットワーク全体の管理下の製品およびサービスを 1 か所から監視できます。

Control Manager により、システム管理者は、感染、セキュリティ違反、ウイルスの検出ポイントなどの活動を監視し、報告できるようになります。コンポーネントをダウンロードしてネットワーク全体に配信することで、最新の一貫した保護を実現できます。Control Manager には手動アップデートと予約アップデートの両方が用意されており、柔軟性を高めるため、製品をグループまたは個別に設定して管理することができます。

Control Manager MCP エージェント

Control Manager Management Communication Protocol (MCP) エージェントは、トレンドマイクロの管理下の製品向けの次世代エージェントです。MCP は Trend Micro Management Infrastructure (TMI) に代わるもので、Control Manager は MCP を使用して ServerProtect と通信します。

MCP には次の機能があります。

- ネットワーク負荷とパッケージサイズの低減
- NAT およびファイアウォールトラバーサルのサポート
- HTTPS のサポート
- 一方向および双方向通信のサポート
- シングルサインオン (SSO) のサポート
- クラスタノードのサポート

これらの機能については、Control Manager のドキュメントを参照してください。

本バージョンの ServerProtect にアップグレードすると、TMI エージェントは MCP エージェントに自動的に置き換えられます。

サポートされる Control Manager のバージョン

本バージョンの ServerProtect がサポートする Control Manager、および Apex Central のバージョンについては、以下をご確認ください。

https://success.trendmicro.com/jp/solution/1302988

Control Manager の統合の概要

このトピックでは、Control Manager 7.0 と本バージョンの ServerProtect 間の統合範囲について説明します。

次の表に示す機能の詳細については、Control Manager のドキュメントを参照してください。

表 5-1.　統合の概要

統合機能	詳細
登録	ServerProtect 管理コンソールから (MCP エージェント経由)
シングルサインオン	サポートされません
ライセンス管理	サポートされません
コマンド追跡	サポートされます
Control Manager から配信されるコンポーネント	すべてのコンポーネント
Control Manager から管理および配信されるポリシー	なし
ユーザ / エンドポイントディレクトリに表示される情報	なし
アドホッククエリ	アドホッククエリを実行して製品情報およびログを表示するときに、次のデータビューのいずれかを選択します。 ・ 製品のステータス情報 ・ 製品のイベント情報 ・ ウイルス / 不正プログラム情報 ・ スパイウェア / グレーウェア情報
製品に固有のダッシュボードウィジェット	なし

表 5-1.　統合の概要

統合機能	詳細
他の管理下の製品と共有されている ダッシュボードウィジェット	なし
静的レポートテンプレート	なし
カスタムレポートテンプレート (事前定義済み)	• TM- 管理下の製品の接続 / コンポーネントステータス • TM- 脅威の概要 (全体) • TM- スパムメール検出の概要 • TM- スパイウェア / グレーウェア検出の概要 • TM- 脅威の兆候の検出概要 • TM- ウイルス / 不正コード検出の概要
イベント通知	なし
情報漏えい対策 (DLP) イベントの管理	該当なし
不審オブジェクトと IOC ファイルの管理	該当なし

Control Manager への登録

注意： 次の機能は、ServerProtect for EMC Celerra 5.8 Patch 2 以降のリリースでサポートされます。

ServerProtect と Control Manager を統合するには、製品を Control Manager に登録する必要があります。

ServerProtect を Control Manager に登録するには、次の手順に従ってください。

1. Windows の [スタート] メニューから [Trend ServerProtect Management Console] → [ServerProtect Management Console] の順に選択します。
2. 次のいずれかの操作を実行してください。
   - サイドバーの [CM Agent Setting] をクリックします。
   - メインメニューから [Do] → [Control Manager (CM) Agent Setting] の順に選択します。

   [CM Agent Setting] 画面が表示されます。サーバの [Registration Status] は [Not Registered with Control Manager] です。

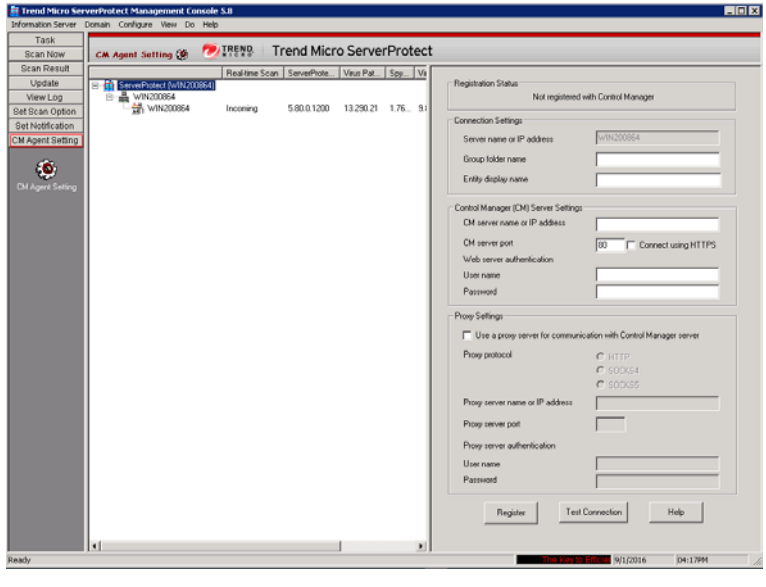


図 5-1. [CM Agent Setting] 画面

3. 右画面の [Connection Settings] で、次の情報を入力します。
   - [Group folder name] : Control Manager 製品ツリーで ServerProtect を識別するための分かりやすい名前を入力します。グループフォルダ名の最大長は 19 文字です。
   - [Entity display name] : ServerProtect インフォメーションサーバの名前を入力します。この名前は ServerProtect インフォメーションサーバを識別するために Control Manager サーバの製品ディレクトリに表示されるものなので、慎重に指定してください。一意の分かりやすい名前を指定すると、Control Manager の製品ディレクトリで ServerProtect サーバを見つけやすくなります。エンティティの表示名の最大長は 64 文字です。

注意： [Server name or IP address] には、ServerProtect をインストールしたコンピュータのホスト名または IP アドレスが自動的に表示されます。

4. [Control Manager (CM) Server Settings] で、次の情報を入力します。
   - [CM server name or IP address]: Control Manager (CM) サーバの名前または IP アドレスを入力します。
   - [CM server port] : MCP エージェントが Control Manager との通信に使用する、Control Manager (CM) サーバのポート番号を入力します。

     Control Manager のセキュリティ設定が中 (Control Manager と管理下の製品の MCP エージェントとの間で HTTPS および HTTP 通信が可能) または高 (Control Manager と管理下の製品の MCP エージェントとの間で HTTPS 通信のみ可能) の場合は、[Connect using HTTPS] を選択します。
   - [User name] および [Password]: ネットワークで認証が必要な場合は、Internet Information Services (IIS) サーバの認証情報を入力します。

注意： IIS サーバの認証を使用する場合は、Control Manager からコンポーネントをアップデートするように ServerProtect を設定できません。アップデートサーバ (トレンドマイクロのアップデートサーバまたは独自に設定したアップデートサーバ) の URL を、[Scheduled Update] または [Manual Update] 画面にダウンロード元として指定する必要があります。

5. プロキシサーバを使用して Control Manager サーバにアクセスする場合は、[Proxy Setting] で [Use a proxy server for communication with the Control Manager server] を選択し、次の情報を入力します。
   - [Proxy Protocol] : プロキシのプロトコルを選択します。
   - [Proxy server name or IP address]: プロキシサーバの名前または IP アドレスを入力します。
   - [Proxy server port] : プロキシサーバのポート番号を入力します。
   - [User name] および [Password] : プロキシサーバで認証が必要な場合は、プロキシサーバ用のユーザ名とパスワードを入力します。
6. [Test Connection] をクリックし、指定した情報で ServerProtect から Control Manager サーバに接続できることを確認します。ServerProtect から Control Manager サーバに接続できない場合は、入力した設定を確認してください。また、ServerProtect コンピュータと Control Manager サーバとの接続状態も確認してください。
7. [Register] をクリックして設定を保存し、ServerProtect を登録します。

Control Manager での ServerProtect ステータスの確認

ServerProtect のステータスを Control Manager 管理コンソールで確認するには、次の手順に従ってください。

1. Web ブラウザで次の URL を指定します。

   https://<Control Manager のサーバ名 >/Webapp/login.aspx

   <Control Manager のサーバ名 > は Control Manager サーバの IP アドレスまたはホスト名です。
2. メニューバーで [Products] をクリックします。
3. ツリー表示で、ServerProtect を Control Manager に登録する際に指定したグループフォルダ名を展開します。
4. 登録したサーバがリストにあるかどうかを確認します。

Control Manager からの登録解除

別の Control Manager サーバに切り替える場合は、現在の Control Manager サーバから ServerProtect を登録解除して、新しいサーバに登録します。

ServerProtect コンピュータを Control Manager から登録解除するには、次の手順に従ってください。

1. Windows の [スタート] メニューから [Trend ServerProtect Management Console] → [ServerProtect Management Console] の順に選択します。
2. 次のいずれかの操作を実行してください。
   - サイドバーの [CM Agent Setting] をクリックします。
   - メインメニューから [Do] → [Control Manager (CM) Agent Setting] の順に選択します。

   [CM Agent Setting] 画面が表示されます。
3. [Unregister] をクリックします。

第 6 章

トラブルシューティングとテクニカルサポート

本章では、ユーザ登録やトレンドマイクロのテクニカルサポートについて説明します。

本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

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。

セキュリティニュース

トレンドマイクロ「セキュリティニュース」

トレンドマイクロでは、最新のセキュリティニュース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ニュースでは、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。セキュリティニュースは、次の URL からアクセスできます。

https://www.trendmicro.com/ja_jp/security-intelligence/breaking-news.html

- ウイルス名やキーワードから検索できる脅威データベース
- 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

セキュリティニュース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専門のスタッフが解析し、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。

http://downloadcenter.trendmicro.com/index.php?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。

付録 A

製品版へのアップグレードとよくある質問

ServerProtect はシリアル番号を入力しないでインストールした場合、30 日体験版としてインストールされます。体験版では、使用できるのはインストール後 30 日間に限定されます。30 日経過後は、ServerProtect をインストールした分のライセンスをご購入いただくか、プログラムをコンピュータから削除する必要があります。

体験版プログラムはすべてトレンドマイクロサポートサービスの対象外です。体験版の動作に関するお問い合わせについて、サポートサービスセンターでは回答いたしかねますので、あらかじめご了承ください。製品版の購入、製品の追加購入についてはトレンドマイクロ営業部か販売代理店までお問い合わせください。

本章では、製品ライセンスの購入後、シリアル番号を登録する方法について説明します。

本章で説明する内容には、次の項目が含まれます。

[Software Evaluation Period] ダイアログボックス

ServerProtect を体験版としてインストールした場合、管理コンソールを起動するたびに [Software Evaluation Period] ダイアログボックスが表示されます。このダイアログボックスには、ネットワーク上のどのサーバが体験版を使用しているかが表示されます。また、期限が切れるまでの日数も表示されます。

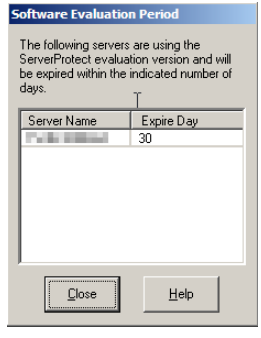


図 A-1. [Software Evaluation Period] ダイアログボックス

シリアル番号リストの確認

管理コンソールを使用して、管理下のすべての一般サーバのシリアル番号を表示することができます。

シリアル番号リストを表示するには、次の手順に従ってください。

1. メインメニューから [Help] → [About] の順に選択します。[About ServerProtect Management Console] ダイアログボックスが表示されます。

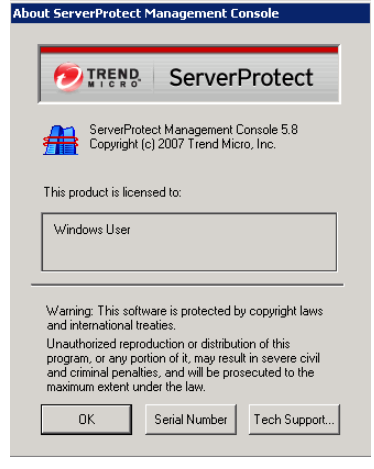


図 A-2. [About ServerProtect Management Console] ダイアログボックス

2. [Serial Number] ボタンをクリックします。[Serial Number List] ダイアログボックスが表示されます。表示内容には、ネットワーク上の ServerProtect 一般サーバすべてと、そのシリアル番号が含まれます。

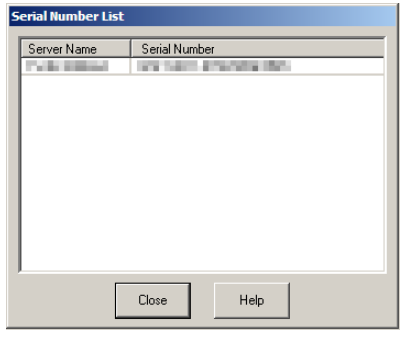


図 A-3. [Serial Number List] ダイアログボックス

3. 確認したら、[Close] をクリックします。さらに [OK] をクリックして [About ServerProtect Management Console] ダイアログボックスを閉じます。

製品版へのアップグレード

体験版としてインストールした後で、ServerProtect の製品版をお買い上げいただいた場合でも、管理コンソールからシリアル番号を登録することで、既にインストールされている ServerProtect を引き続きご利用いただけます。ServerProtect を再インストールする必要はありません。

製品版へのアップグレードを実行するには、次の手順に従ってください。

1. ドメインブラウザツリーで製品版にアップグレードする一般サーバを選択します。
2. メインメニューから [Do] → [Update Serial Number] を選択します。[Enter New Serial Number] ダイアログボックスが表示されます。

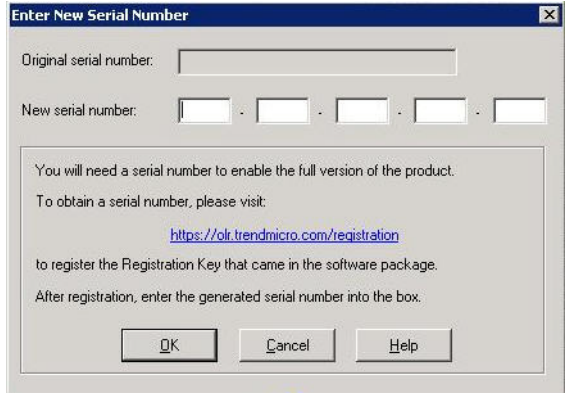


図 A-4. [Enter New Serial Number] ダイアログボックス

3. [New serial number] テキストボックスに有効なシリアル番号を入力します。
4. [OK] をクリックして変更内容を保存します。

よくある質問

ServerProtect のアップグレード

- **管理コンソールを 5.58 から 5.8 に移行しましたが、管理コンソールが正常に動作しません。どのように対処したらいいですか。**

  インフォメーションサーバのバージョンをチェックしてください。管理コンソールとインフォメーションサーバの ServerProtect バージョンは同じである必要があります。ServerProtect 5.8 管理コンソールを使用して、ServerProtect 5.58 インフォメーションサーバを管理することはできません。また、この逆も当てはまります。
  すべての一般サーバをバージョン 5.8 に移行することもお勧めします。一般サーバにインストールされている ServerProtect のバージョンは、それらを管理するインフォメーションサーバのバージョン以上である必要があります。ServerProtect 5.8 管理コンソールでは、ServerProtect 5.58 一般サーバのタスク設定を変更できません。

- **ServerProtect を 5.8 から 5.58 にロールバックすることは可能ですか。**

  いいえ。アップグレード後に ServerProtect を前のバージョンにロールバックすることはできません。

- **ServerProtect 5.58 管理コンソールと ServerProtect 5.58 一般サーバを同じサーバコンピュータにインストールしました。配信プログラムを使用して、それらを別々にアップグレードできますか。**

  いいえ。一般サーバと管理コンソールが同じサーバコンピュータにインストールされている場合、配信プログラムでは、それらが一緒にアップグレードされます。

- **管理コンソールから、ServerProtect 5.31 を 5.8 にアップグレードできますか。**

  いいえ。管理コンソールからのアップグレードは、ServerProtect バージョン 5.8 以前ではサポートされていません。既存の ServerProtect バージョンを削除し、セットアッププログラムから ServerProtect 5.8 をインストールすることは可能です。

- **インストールパッケージを使用して、既存の管理コンソールをリモートで移行することはできますか。**

  いいえ。リモートの移行 / インストールは、管理コンソールではサポートされていません。リモートインストール / 移行では、管理コンソールはアップグレードされません。

注意： 最新のウイルス対策を実現するために、インストール後、ただちにウイルスパターンファイルとウイルス検索エンジンをアップデートすることをお勧めします。また、初期設定の配信タスクを変更し、アップデートコンポーネントとしてスパイウェアパターンファイル、ウイルスクリーンナップテンプレート、ウイルスクリーンナップエンジン、およびルートキット対策ドライバを追加してください。

ServerProtect のウイルス検索

- **[Scan Result] でファイル名とファイルパスが正しく表示されずに切り捨てられ、[Restore] ボタンが無効になっています。**

  [Scan Result] 画面におけるファイル名とファイルパスのエントリフィールドでは、最大で 256 文字までのファイル名 (ファイルパスも含む) を表示できます。256 文字を超えると、ファイル名またはファイルパスは切り捨てられ、[Restore] ボタンが無効になります。

- **書込み禁止リストが機能しません。**

  リアルタイム検索が無効になっている場合、書込み禁止リストは機能しません。書込み禁止リストを有効にするには、リアルタイム検索を有効にしてください。

- **通知用のポップアップメッセージボックスを表示するように警告方法を設定したのに、ポップアップ通知メッセージが表示されません。**

  Windows Server 2008 以降、Windows はメッセージサービスをサポートしていません。
  そのため、Windows Server 2008 以降ではポップアップメッセージ警告機能は動作しません。

その他

- **CMAgent をインストールすると、Control Manager に古いログが存在します。これらはどこからきたものでしょうか。**

  Control Manager エージェントをインストールすると、既存のすべてのログが Control Manager サーバに送信されます。ただしこれにより、ネットワークトラフィックが増加する場合があります。重複を避けるために、管理コンソールからすべてのログを削除してから CMAgent をインストールしてください。

- **異なるネットワークセグメントに属する複数のネットワークカードを持つコンピュータシステムに、インフォメーションサーバをインストールしました。管理コンソールを開くと、インフォメーションサーバリストにインフォメーションサーバが表示されず、インフォメーションサーバと一般サーバ間のリンクが壊れています。**

  インフォメーションサーバがインフォメーションサーバリストに表示されないのは、インフォメーションサーバ / 一般サーバが正しいネットワークに接続しようとする際、そのネットワークに到達できないことが原因です。この問題を解決するには、インフォメーションサーバと一般サーバの両方をアンインストールし、それらを再インストールしてください。

- **システムトレイに一般サーバのアイコンが見当たりません。**

  リモートデスクトップ接続を使用している場合、システムトレイに一般サーバのアイコンが表示されないことがあります。

- **一般サーバのパターンファイルと検索エンジンが表示されません。**

  一般サーバがインフォメーションサーバから切断されている場合、一般サーバのパターンファイルと検索エンジン、およびその他の関連情報は管理コンソールに表示されません。一般サーバとインフォメーションサーバの間のリンクが壊れている場合、管理コンソールのステータス画面に十字形の記号が表示されます。

- **Admin.ini で「ExcludeUNCPath」を有効にしても、単語を除外リストに登録できません。**

  Admin.ini で ExcludeUNCPath を有効にしても、ユーザアクセス制御 (UNC) が有効な場合、行った設定が管理コンソールに反映されないことがあります。

- **Windows のログインパスワードを空白にすると、ServerProtect にログイン失敗のエラーが表示されます。**

  Microsoft Windows にはユーザアカウントの制限があり、リモートログインのパスワードが必要です。そのため、パスワードを設定していない場合、ServerProtect にログイン失敗のエラーが表示されます。

索引

英数字

あ

か

ら