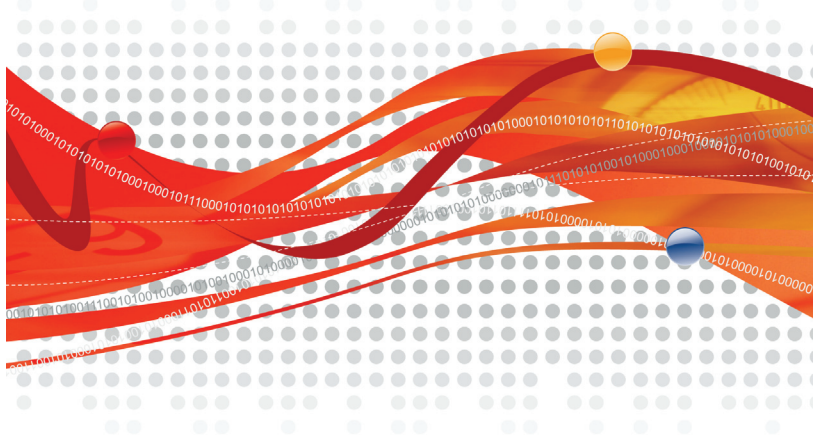
Trend Micro ServerProtect™



クイックスタートガイド

安心を、ひとつ上のステージへ。

TREND MICRO™

※注意事項

トレンドマイクロへのお客様情報の送信について

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

輸出規制について

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

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

2008年12月現在、米国により定められる禁輸国は、キューバ、イラン、北朝鮮、スーダン、シリアが含まれています。

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

複数年契約について

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

著作権について

商標について

P/N: SPFFFF-AE0203 (2009/10)

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、すべての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。

本章で説明する内容には、次の項目が含まれます。

ここでは、ServerProtect 5.8 の Microsoft Windows に対する OS のサポートについて説明します。

次の表では、ServerProtect 5.8 でサポートされる Windows システムのバージョンについて説明します。

表 1-1. Microsoft Windows Server システムに対する ServerProtect のサポート

バージョン	種類
Windows 2000 Server	Server SP4
	Advance Server SP4
Windows Server 2003	Standard Server x86 および x64、SP1 または SP2
	Standard Server x86 および x64 R2、SP1 または SP2
	Storage Server x86 および x64、SP1 または SP2
	Storage Server x86 および x64 R2、SP1 または SP2
	Standard Server x86 および x64、SP1 または SP2
	Standard Server x86 および x64 R2、SP1 または SP2
	Datacenter Server x86 および x64、SP1 または SP2
	Datacenter Server x86 および x64、SP1 または SP2
Windows Server 2008	Standard Server x86 および x64、SP2
	Enterprise Server x86 および x64、SP2
	DataCenter Server x86 および x64、SP2

この表を使用すると、ServerProtect コンポーネントが提供する、Windows Server プラットフォームに対するサポートを正確に特定できます。たとえば、「32 ビット Windows Server 2008 ファミリプラットフォーム」は、Windows Server 2008 Standard、Enterprise Server、DataCenter Server、および Web Server の x86 エディションを意味することになります。特に記載されていない限り、Windows Server 2008 Standard、Enterprise Server、および DataCenter Server は Hyper-V なしのものです。

ServerProtect バージョン 5.8 の追加機能

- Windows 2000 Server、Windows Server 2003 のほとんどのバージョン、Windows Server 2003 R2、Windows Server 2008、および Windows Server 2008 R2 などの Microsoft Windows サーバプラットフォームをサポートします (30 ページの「推奨システム要件」参照)。
- VMware ESX/ESXi サーバがサポートされます。
- 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。これには、感染ファイルに対する処理として隔離、削除、拡張子変更を実行するためのオプションがあります。
- Novell Open Enterprise Server 2 環境で一般サーバを実行できます。
- 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、ServerProtect5.58 と 5.7 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 一般サーバの間で通信する際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 エージェントを ServerProtect 5.8 に対応したバージョンにアップグレードできます。

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。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 Windows または NatWare 一般サーバに接続します。

ServerProtect アーキテクチャ

ServerProtect 5 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。

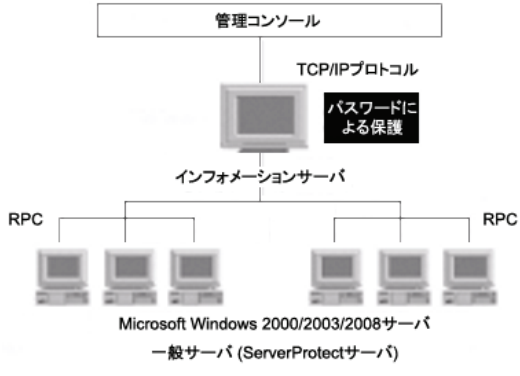


図 1-1. ServerProtect の 3 層アーキテクチャ

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。管理コンソールのメイン画面は、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。52 ページの「一般サーバのインストール」参照

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**
  (52 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」参照)
- **管理コンソールからのインストール**
  (55 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」参照)
- **Microsoft SMS を使用したインストール**
  (57 ページの「Microsoft SMS による配信」参照)
- **サイレントモードでのインストール**
  (63 ページの「サイレントモードでのインストール」参照)

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。ServerProtect をインストールする前に、第 2 章「インストール」の説明をよくお読みください。

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、75 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、移動、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。

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、116 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、120 ページの「手動検索 (ScanNow)」を参照してください。

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、112 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、112 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、96 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。以前のバージョンで提供されていたウイルス対策機能に加えて、ServerProtect 5.8 では、ウイルスカテゴリに応じたスパイウェアパターンファイルが利用できるようになりました。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、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、113 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 [ウイルス駆除前に感染ファイルのバックアップを作成する] オプションを選択しておくと、ファイルのバックアップコピーが自動的に作成されます。

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、113 ページの「ウイルスに対する処理の設定」参照、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： [ウイルス駆除] 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、保存されるログファイルのサイズを制限することができます。初期設定のサイズは 10000 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。

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、82 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 5.8 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。

注意： ServerProtect のバージョン 5.8 では、配信によるプログラムファイルのアップデートがサポートされるようになりました

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。86 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。92 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。

注意： 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、97 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、112 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。トレンドマイクロ製品では、パターンファイルのアップデート作業を簡易化するための予約アップデート機能を実装しています。詳細については、88 ページの「予約ダウンロードの設定」参照 および 93 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 の設定については、116 ページの「リアルタイム検索の設定」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

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、116 ページの「リアルタイム検索の設定」および 120 ページの「手動検索 (ScanNow)」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、112 ページの「ウイルス検索」を参照してください。

注意： 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、112 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。詳細については、120 ページの「手動検索 (ScanNow)」を参照してください。

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わからないとき、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。新しい設定内容は、パターンファイル、検索エンジンのアップデートにより適用されます。

トレンドマイクロの推奨処理の設定については、113 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。116 ページの「リアルタイム検索の設定」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 2000 Server、2003、および 2008 Server 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

インストール

本章で説明する内容には、ServerProtect 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。

本章で説明する内容には、次の項目が含まれます。

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： 古い一般サーバをインストールし、それを ServerProtect 5.8 インフォメーションサーバに登録することはできません。

推奨システム要件

ServerProtect をインストールするには、次の要件を満たしている必要があります。

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

- CPU: 2.5GHz Intel Pentium IV プロセッサ、3.0GHz EM64T Intel プロセッサ、または 2.0GHz AMD Athlon 64 ビットプロセッサ (または同等)
- メモリ :
  - 512MB (最小)、1GB (推奨)
    - Windows 2000 Server SP4
    - Windows 2000 Advanced Server SP4
    - Windows Server 2003 Standard Edition、x86 および x64、SP1 または SP2
    - Windows Server 2003 Enterprise Edition、x86 および x64、SP1 または SP2
    - Windows Server 2003 R2 Standard Edition、x86 および x64、SP2
    - Windows Server 2003 R2 Enterprise Edition、x86 および x64、SP2
  - 1GB (最小)、2GB (推奨)
    - Windows Storage Server 2003、x86 および x64、SP1 または SP2
    - Windows Server 2003 Datacenter Edition、x86 および x64、SP1 または SP2
    - Windows Storage Server 2003 R2、x86 および x64、SP2
    - Windows Server 2003 R2 Datacenter Edition、x86 および x64、SP2
    - Windows Server 2008 Standard Edition、x86 および x64 または SP2 (Hyper-V なし)
    - Windows Server 2008 Enterprise Edition、x86 および x64 または SP2 (Hyper-V なし)
    - Windows Storage Server 2008、x86 および x64 または SP2 (Hyper-V なし)

- Windows Server 2008 Datacenter Edition、x86 および x64 または SP2 (Hyper-V なし)
- Windows Server 2008 Standard Edition、Hyper-V、x64 または SP2
- Windows Server 2008 Enterprise Edition、Hyper-V、x64 または SP2
- Windows Storage Server 2008、Hyper-V、x64 または SP2
- Windows Server 2008 Datacenter Edition、Hyper-V、x64 または SP2
- Windows Server 2008 Standard Edition、x86 および x64 または SP2 (サーバコアモード)
- Windows Server 2008 Enterprise Edition、x86 および x64 または SP2 (サーバコアモード)
- Windows Storage Server 2008、x86 および x64 または SP2 (サーバコアモード)
- Windows Server 2008 Datacenter Edition、x86 および x64 または SP2 (サーバコアモード)

特定の Windows Server OS の正式な名称については、10 ページの「Microsoft Windows Server システムに対する ServerProtect のサポート」参照してください。

- ハードディスク空き容量 : 500MB
- ネットワークプロトコルおよびサービス : TCP/IP、Microsoft Network、および RPC サービスが Windows Server ファミリ OS で実行されている必要があります。

注意 : 他のウイルス対策製品がインストールされている場合は、あらかじめアンインストールしてから ServerProtect の一般サーバをインストールしてください。

インフォメーションサーバ

- CPU: 2.5GHz Intel Pentium IV プロセッサまたは 3.0GHz EM64T Intel プロセッサまたは 2.0GHz AMD Athlon 64 ビットプロセッサ (または同等)
- メモリ :
    - 512MB (最小)、1GB (推奨)
        - Windows 2000 Server SP4
        - Windows 2000 Advanced Server SP4
        - Windows Server 2003 Standard Edition、x86 および x64、SP1 または SP2
        - Windows Server 2003 Enterprise Edition、x86 および x64、SP1 または SP2
        - Windows Server 2003 R2 Standard Edition、x86 および x64、SP2
        - Windows Server 2003 R2 Enterprise Edition、x86 および x64、SP2
    - 1GB (最小)、2GB (推奨)
        - Windows Storage Server 2003、x86 および x64、SP1 または SP2
        - Windows Server 2003 Datacenter Edition、x86 および x64、SP1 または SP2
        - Windows Storage Server 2003 R2、x86 および x64、SP2
        - Windows Server 2003 R2 Datacenter Edition、x86 および x64、SP2
        - Windows Server 2008 Standard Edition、x86 および x64 または SP2 (Hyper-V なし)
        - Windows Server 2008 Enterprise Edition、x86 および x64 または SP2 (Hyper-V なし)
        - Windows Storage Server 2008、x86 および x64 または SP2 (Hyper-V なし)
        - Windows Server 2008 Datacenter Edition、x86 および x64 または SP2 (Hyper-V なし)
        - Windows Server 2008 Standard Edition、Hyper-V、x64 または SP2
        - Windows Server 2008 Enterprise Edition、Hyper-V、x64 または SP2
        - Windows Storage Server 2008、Hyper-V、x64 または SP2
        - Windows Server 2008 Datacenter Edition、Hyper-V、x64 または SP2

特定の Windows Server OS の正式な名称については、10 ページの「Microsoft Windows Server システムに対する ServerProtect のサポート」参照してください。

- ハードディスク空き容量 : 500MB
- インストールをローカルに実行する場合は、CD-ROM ドライブが必要です。

- ネットワークプロトコルおよびサービス : TCP/IP、Microsoft Network、および Remote Procedure Call (RPC) サービスが Windows Server ファミリ OS で実行されている必要があります。
- 上記のサービスはインストール済みのコンピュータで実行される必要があります。
  ServerProtect のインフォメーションサーバと一般サーバ間でのコンポーネントアップデートの配置を最適化するために最小で 128Kbps の割り当て済み帯域幅をお勧めします。
  RPC over 名前付きパイププロトコルまたは RPC over TCP が機能しない場合、自動的に別のプロトコルである名前付けパイプまたは TCP に切り替えられます。Windows Server を管理するには、インフォメーションサーバがインストールされている必要があります。

管理コンソール

- CPU: 2.5GHz Intel Pentium IV プロセッサまたは 3.0GHz EM64T Intel プロセッサまたは 2.0GHz AMD Athlon 64 ビットプロセッサ (または同等)

サーバ環境 :

- メモリ :
    - 512MB (最小)、1GB (推奨)
        - Windows 2000 Server SP4
        - Windows 2000 Advanced Server SP4
        - Windows Server 2003 Standard Edition、x86 および x64、SP1 または SP2
        - Windows Server 2003 Enterprise Edition、x86 および x64、SP1 または SP2
        - Windows Server 2003 R2 Standard Edition、x86 および x64、SP2
        - Windows Server 2003 R2 Enterprise Edition、x86 および x64、SP2
    - 1GB (最小)、2GB (推奨)
        - Windows Storage Server 2003、x86 および x64、SP1 または SP2
        - Windows Server 2003 Datacenter Edition、x86 および x64、SP1 または SP2
        - Windows Storage Server 2003 R2、x86 および x64、SP2
        - Windows Server 2003 R2 Datacenter Edition、x86 および x64、SP2
        - Windows Server 2008 Standard Edition、x86 および x64 または SP2 (Hyper-V なし)
        - Windows Server 2008 Enterprise Edition、x86 および x64 または SP2 (Hyper-V なし)
        - Windows Storage Server 2008、x86 および x64 または SP2 (Hyper-V なし)
        - Windows Server 2008 Datacenter Server、x86 および x64 または SP2 (Hyper-V なし)
        - Windows Server 2008 Standard Edition、Hyper-V、x64 または SP2
        - Windows Server 2008 Enterprise Edition、Hyper-V、x64 または SP2
        - Windows Storage Server 2008、Hyper-V、x64 または SP2
        - Windows Server 2008 Datacenter Server、Hyper-V、x64 または SP2

ハードディスク空き容量 : 500MB

クライアント環境 :

- メモリ :

    - 256MB (最小)、512MB (推奨)
        - Windows 2000 Professional SP4 (512MB (最小)、1GB (推奨))
        - Windows XP Professional SP2 または SP3 (32 ビットおよび 64 ビット)
        - Windows XP Home SP2 または SP3
    - 1GB (最小)、2GB (推奨)
        - Windows Vista Home/Business/Ultimate SP1 または SP2 (32 ビットおよび 64 ビット)

ハードディスク空き容量 : 500MB

特定の Windows Server OS については、10 ページの「Microsoft Windows Server システムに対する ServerProtect のサポート」参照してください。

- ハードディスク空き容量 : 500MB
- 解像度 1024x768 以上のモニタ
- CD-ROM ドライブ
- ネットワークプロトコルおよびサービス : TCP/IP、Microsoft Network、および RPC サービスが Windows Server ファミリ OS で実行されている必要があります。

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。最新の情報については弊社の「最新版ダウンロード」サイトにある最新の Readme をご参照ください。

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は、41 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

	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 2000 Professional	×	×	○
Windows 2000 Server/Advance Server	○	○	○
Windows Server 2003 ファミリ (32 ビット)	○	○	○
Windows Server 2003 ファミリ (64 ビット)	○ (WOW64)	○	○ (WOW64)
Windows Server 2008 ファミリ (32 ビット、Hyper-V なし)	○	○	○
Windows Server 2008 ファミリ (64 ビット、Hyper-V)	○ (WOW64)	○	○ (WOW64)
Windows Server 2008 ファミリ (64 ビット、Hyper-V なし)	○ (WOW64)	○	○ (WOW64)

表 2-1.　Microsoft Windows 環境でのインストール (続き)

	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、サーバコアモード)	×	○	×
Windows Server 2008 ファミリ　(64 ビット、サーバコアモード)	×	○	×
Windows XP デスクトップファミリ	×	×	○
Windows Vista デスクトップファミリ	×	×	○

注意： Windows Server 2008 ファミリとは、Standard、Enterprise、および Datacenter の各エディションを指します。

注意： Windows Server 2003 ファミリとは、Standard Edition、Enterprise Edition、Storage Server、および Datacenter Server を指します。

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。ファイアウォールが、通信を開始できるように正しく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。

管理コンソールでは、起動時にポート 1000 が待ち受けに使用されます。このポートが他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 が他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 が他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)
- 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)

- RPC over 名前付きパイプの場合は 137 ～ 139 を開きます。
  - 137 (UDP)
  - 138 (UDP)
  - 139 (TCP)

これらのポートは、ServerProtect が RPC over 名前付きパイププロトコルを使用して通信できるようにするために開かれます。

- 3628 (TCP) を開きます。

3628 番ポートは、イベントメッセージの受信に使用されます。

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) (名前付きパイプの場合)
- 139 番 (TCP) (名前付きパイプの場合)

- 名前付きパイプの場合は 137 ～ 139 を開きます。
  - 137 (UDP プロトコル)
  - 138 (UDP プロトコル)
  - 139 (TCP)

これらのポートは、ServerProtect が RPC over 名前付きパイププロトコルを使用して通信できるようにするために開かれます。

Microsoft Windows 環境でのインストール

Windows 環境のサーバで構成されるネットワークに ServerProtect を導入する場合、インストール計画は単純です。

Microsoft Windows 環境で ServerProtect を配信するには

1. インフォメーションサーバをインストールします (49 ページの「インフォメーションサーバのインストール」参照)。
2. インフォメーションサーバと同一のコンピュータ上に一般サーバをインストールします (52 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」参照)。
3. 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ます (47 ページの「管理コンソールのインストール」参照)。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。

   注意： 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。
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。
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。(55 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」参照)。

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。

注意： 管理コンソールを使用したインストール方法では、インフォメーションサーバと同一コンピュータにインストールされている一般サーバプログラムがコピーされます。そのため 32 ビット OS から 64 ビット OS へのインストールはできません。インストールプログラムを使用して一般サーバのみをインストールする方法を採ってください。

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 36 ページの「インストール計画」をよくお読みください。

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 setup.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。

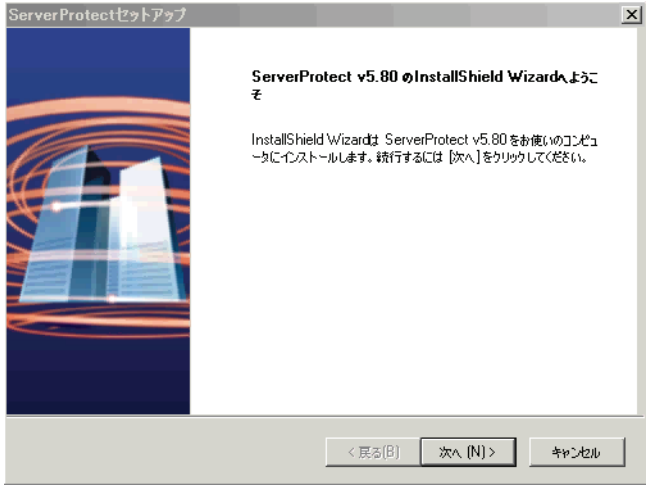


図 2-1. ServerProtect セットアップの初期画面

[次へ] 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。

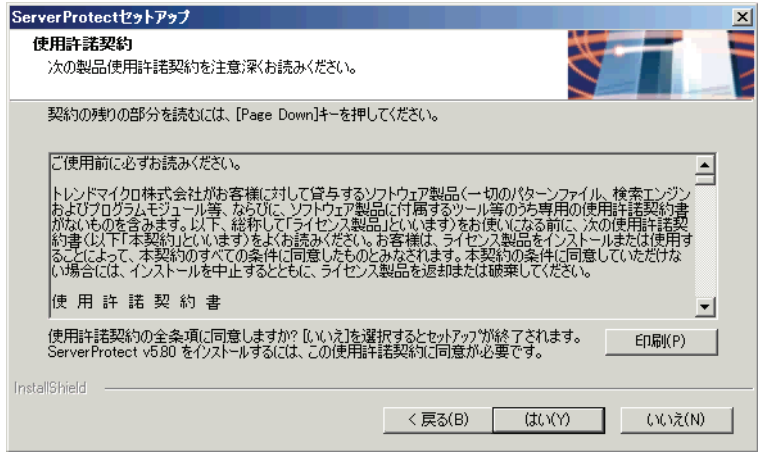


図 2-2.　使用許諾契約書

[はい] 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。

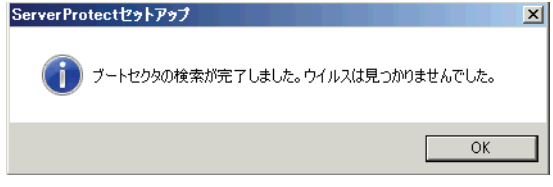


図 2-3.　ウイルス検索の結果

[OK] をクリックしてセットアップを続行します。

4. [ユーザの情報] ダイアログボックスが表示されます。

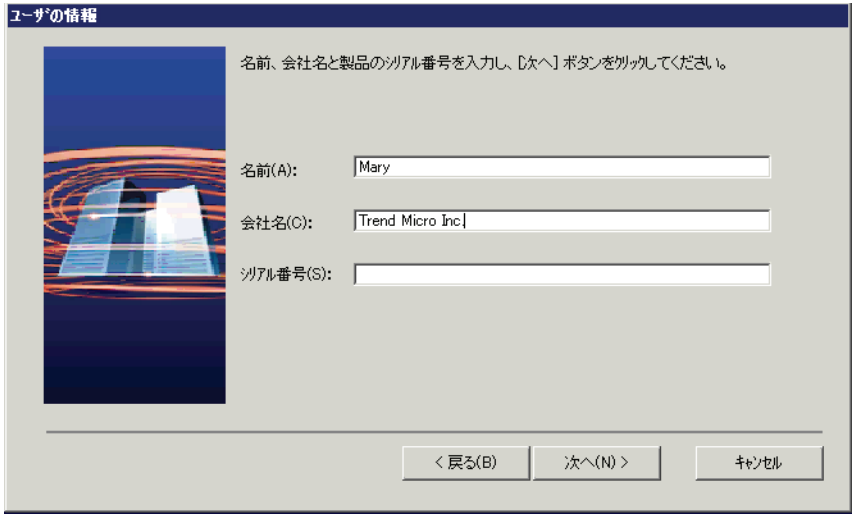


図 2-4.　ユーザの情報

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。

5. [コンポーネントの選択] ダイアログボックスが表示されます。

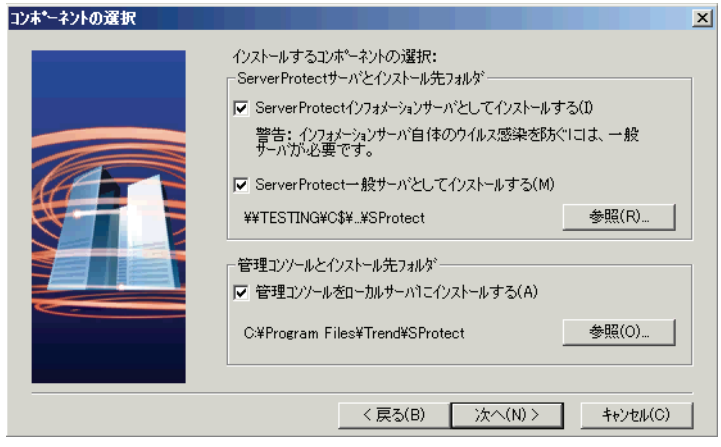


図 2-5.　コンポーネントの選択

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

[次へ] 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。

---

6. 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、[ログオン情報の入力] ダイアログボックスが表示されます。[ログオン情報] の　[ドメイン名]、[ユーザ名]、[パスワード]、および　[パスワードの確認入力] テキストボックスにそれぞれのデータ入力し、[次へ] をクリックしてください。

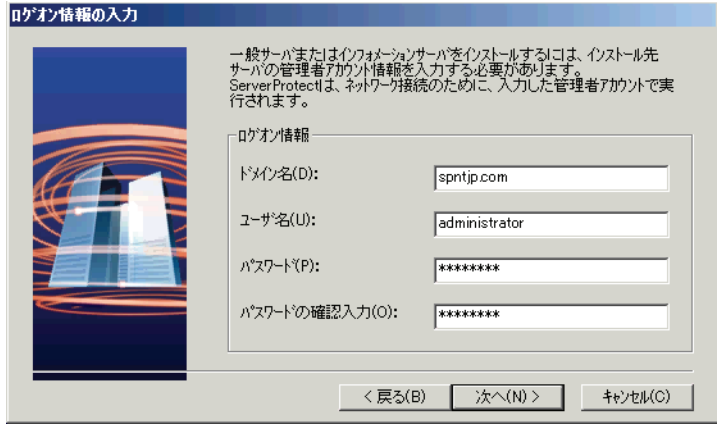


図 2-6.　ログオン情報の入力

7. 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 2-4. 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。

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. [コンポーネントの選択] ダイアログボックスで [管理コンソールをローカルサーバにインストールする] チェックボックスをオンにします (図 2-6 参照)。[参照] 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 2003 または Windows Server 2003 が実行されている Windows コンピュータにインストールする必要があります。(30 ページの「推奨システム要件」参照)。

   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、[個人用プログラムグループ] を選択します。それ以外の場合は [共通プログラムグループ] を選択します。
4. [プログラムフォルダの選択] ダイアログボックスが表示されます。プログラムアイコンを追加するフォルダを確認してください。必要に応じて変更することができます。

   [次へ] をクリックします。
5. [ファイルコピーの開始] 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。正しければ [次へ] 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 [戻る] 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。
6. すべてのファイルがコピーされると、[ServerProtect セットアップ] 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。

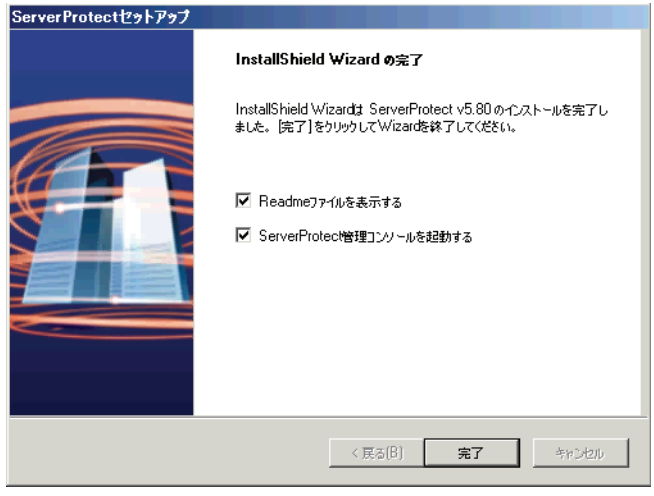


図 2-7.　セットアップの完了

[終了] をクリックしてセットアップを終了します。

7. 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ダイアログボックスが表示されます (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)。

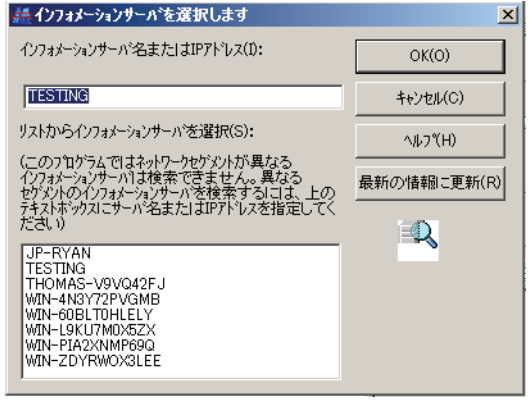


図 2-8.　インフォメーションサーバ選択

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。

[OK] をクリックして変更内容を保存します。

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. [コンポーネントの選択] ダイアログボックスで [ServerProtect インフォメーションサーバとしてインストールする] チェックボックスをオンにします (図 2-5 参照)。
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、[参照] ボタンをクリックします。[ServerProtect インストール先の選択] ダイアログボックスが表示されます。

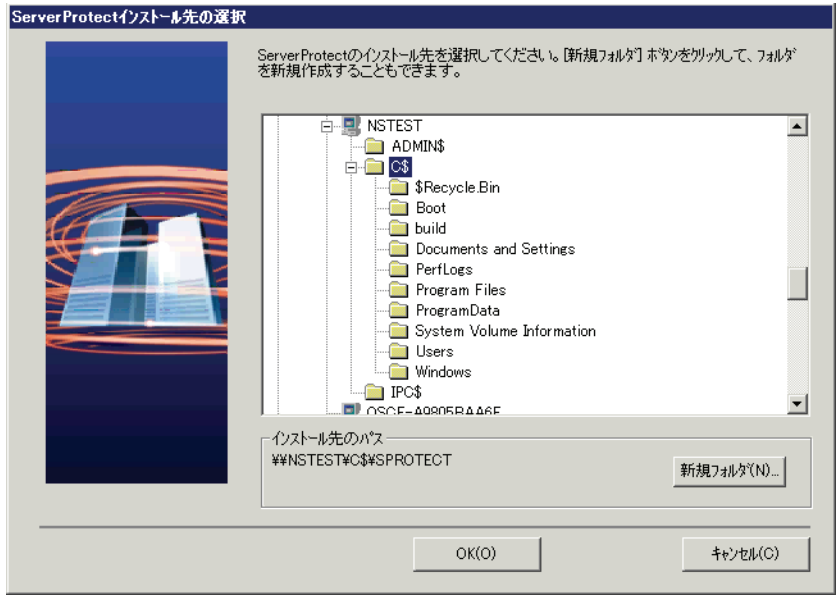


図 2-9.　ServerProtect インストール先の選択

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、[新規フォルダ] ボタンをクリックします。[OK] をクリックして [コンポーネントの選択] ダイアログボックスに戻ります (図 2-5 参照)。

4. [次へ] をクリックします。[ログオン情報の入力] 画面が表示されます。[ログオン情報] の [ドメイン名]、[ユーザ名]、[パスワード]、および [パスワードの確認入力] テキストボックスに有効なデータを入力し、[次へ] をクリックしてください。[インフォメーションサーバのセットアップ] ダイアログボックスが表示されます。

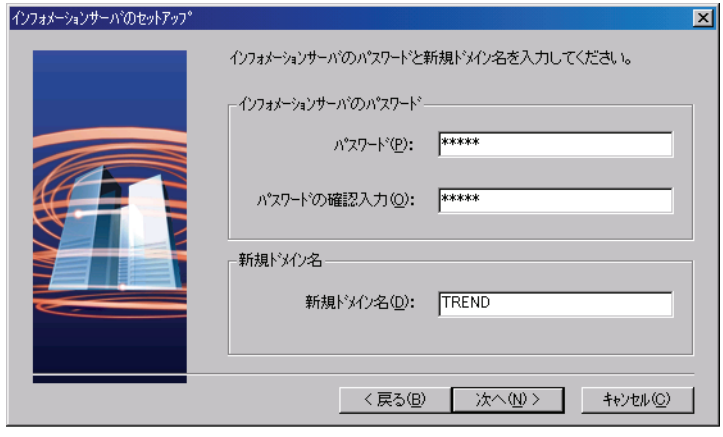


図 2-10. インフォメーションサーバのセットアップ

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。
[次へ] ボタンをクリックします。

5. [ファイルコピーの開始] 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。正しければ [次へ] 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 [戻る] 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。

6. 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 セットアップ] 画面が表示されます。

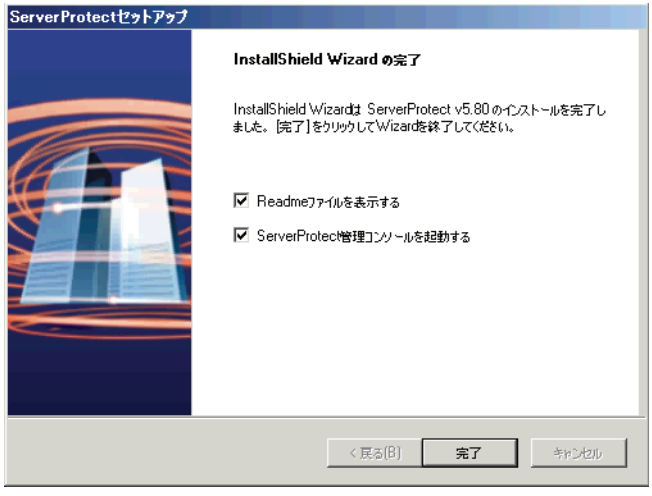


図 2-11.　セットアップの完了

[完了] をクリックしてセットアッププログラムを終了します。

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. [コンポーネントの選択] ダイアログボックス (図 2-5 参照) で [ServerProtect 一般サーバとしてインストールする] 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、[参照] ボタンをクリックします。
3. [ServerProtect インストール先の選択] ダイアログボックスが表示されます。

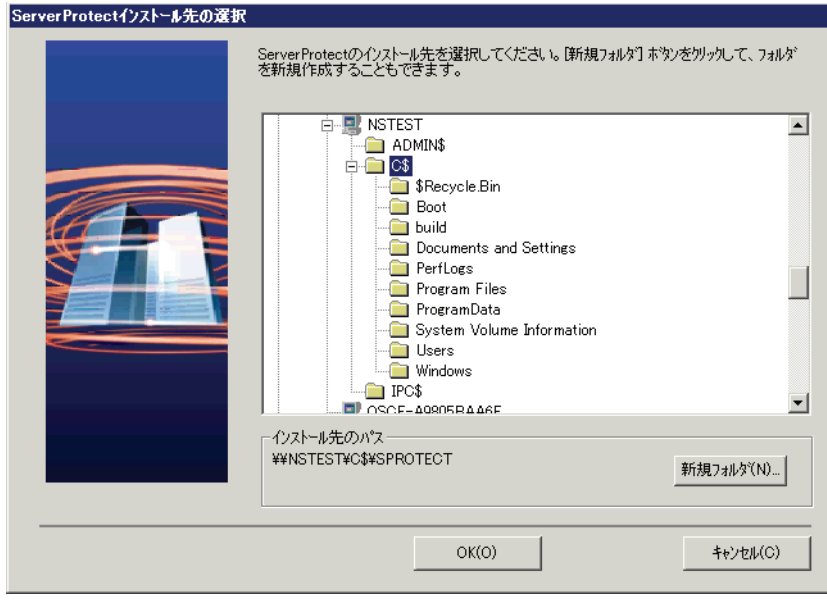


図 2-12.　Windows Server でのインストール先の選択

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。
[OK] をクリックします。

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、[新規フォルダ] ボタンをクリックして [OK] をクリックします。

5. [コンポーネントの選択] ダイアログボックス (図 2-6 参照) で [次へ] ボタンをクリックします。
6. [コンポーネントの選択] 画面の [次へ] をクリックします。

   [ログオン情報の入力] 画面が表示されます。
   ログオン情報を、[ドメイン名]、[ユーザ名]、[パスワード] および [パスワードの確認入力] テキストボックスにそれぞれ入力します。
   [次へ] をクリックします。

7. [ServerProtect インストール先の選択] ダイアログボックスが表示されます。

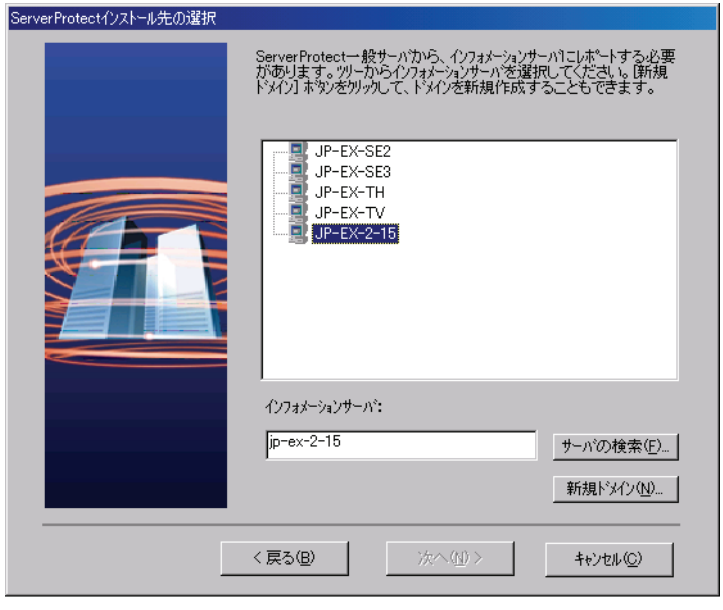


図 2-13.　[ServerProtect インストール先の選択] ダイアログボックス

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、[サーバの検索] ボタンをクリックします。
- 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。

---

8. [ServerProtect インフォメーションサーバパスワードの入力] ダイアログボックスが表示されます。

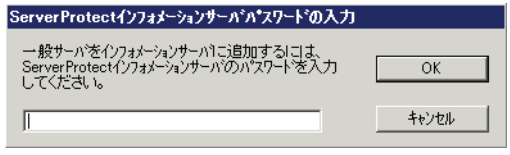


図 2-14. ServerProtect インフォメーションサーバパスワードの入力

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。

9. ServerProtect ドメインを新規作成するには、[新規ドメイン] をクリックします。[ドメイン名] 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。
   [次へ] をクリックします。

10. [ファイルコピーの開始] 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。正しければ [次へ] 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 [戻る] 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。

11. 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、[セットアップの完了] ダイアログボックスが表示されます (図 2-12 参照)。

    [完了] 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。

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 [ドメイン] → [SPNT の新規インストール] 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、[SPNT の新規インストール] 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。[サーバをドメインに追加] ダイアログボックスが表示されます。
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。
   - [サーバ名] テキストボックスにサーバ名を入力します。

[追加] 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手順 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、[削除] をクリックします。[すべて削除] 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ダイアログボックスを閉じるには [キャンセル] をクリックします。

注意： 実行元サーバとインストールするサーバの OS が異なるプラットフォームの場合、[OK] をクリックしたときに、「この操作を完了できませんでした」というメッセージが表示されます。イベントログには、「you cannot install a new ServerProtect from 32-bit source server on a 64-bit target server and vice versa」(ServerProtect を 32 ビットのサーバから 64 ビットのサーバに新規インストールすることも、その逆もできません) というメッセージが表示されます。

注意： 管理コンソールから一般サーバを追加する場合、移動による追加と新規インストールによる追加があり、手順が異なります。移動による追加とは、一般サーバを単にインフォメーションサーバ間で移動することです。新規インストールによる追加とは、一般サーバのソフトウェア自体をリモートインストールし、新規一般サーバとして登録することです。

Microsoft SMS による配信

Windows Server プラットフォーム上の Microsoft Systems Management Server (SMS) 2003 を使用して ServerProtect をインストールできます。

注意： この方法による一般サーバの配信は、Windows Server コンピュータに Microsoft SMS ソフトウェアがインストールされていることが前提です。

次に示す配信手順では、Microsoft SMS を使用して ServerProtect 一般サーバを配信する方法を説明します。

Microsoft SMS により ServerProtect を配信するには

1. Microsoft SMS 管理コンソールを開きます。
2. SMS 管理コンソールのアイコンバーで [パッケージ] をクリックします。
3. メインメニューから [動作] → [新規] → [定義に基づくパッケージ] の順に選択します。[定義に基づくパッケージの作成ウィザードの開始] 画面が表示されます。

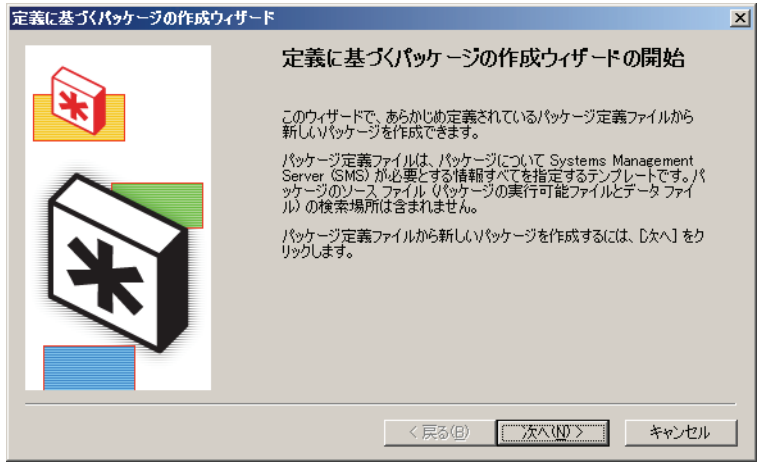


図 2-15. [定義に基づくパッケージの作成ウィザード] 画面

4. [次へ] をクリックします。[パッケージ定義] 画面が表示されます。

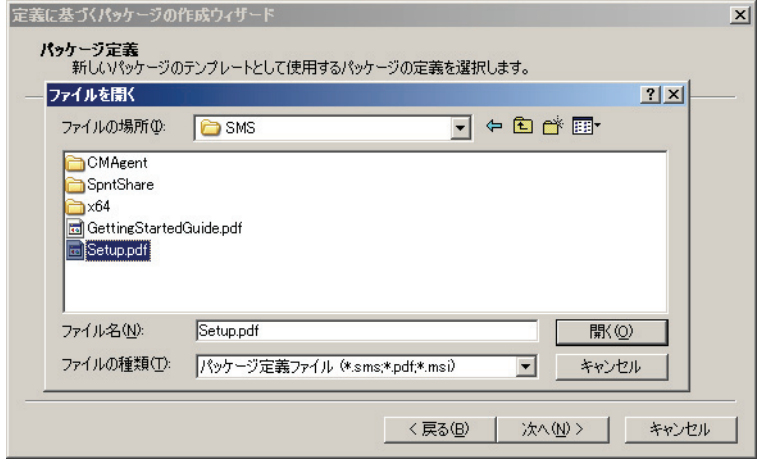


図 2-16. [ファイルを開く] 画面

5. [参照] をクリックして、ServerProtect のインストールに使用するパッケージ定義ファイル (PDF) を指定します。PDF ファイルを選択し、[開く] をクリックします。

ServerProtect ソフトウェアをインストールするための PDF があるディレクトリは、初期設定では次のとおりです。

< ドライブ >:¥program files¥Trend¥SProtect¥SMS¥

この PDF ファイルは、[パッケージ定義] 画面には「ServerProtect」と表示されます。

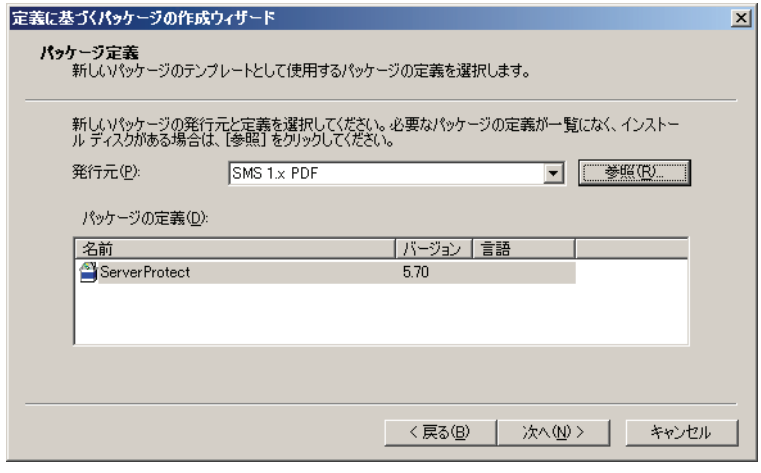


図 2-17. [パッケージ定義] 画面

6. [次へ] をクリックすると、[ソース ファイル] 画面が表示されます。

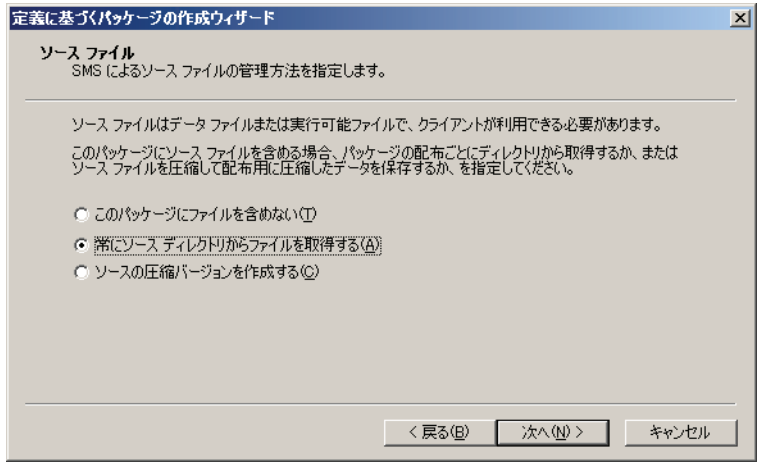


図 2-18. [ソース ファイル] 画面

7. [常にソース ディレクトリからファイルを取得する] オプションを選択して、[次へ] をクリックします。[ソース ディレクトリ] 画面が表示されます。

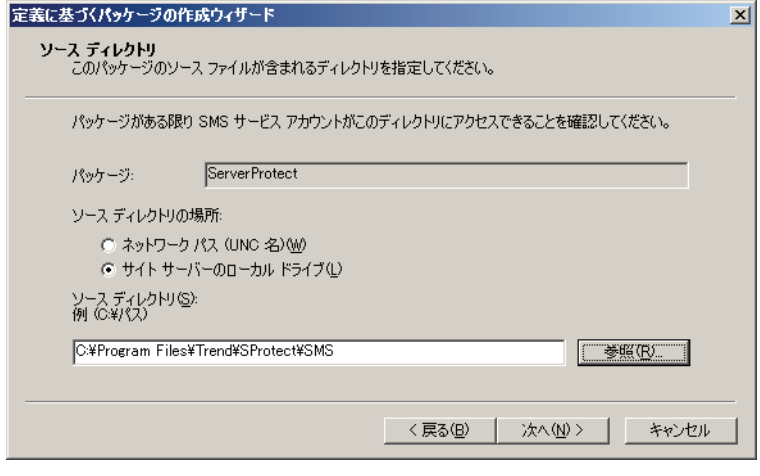


図 2-19. [ソース ディレクトリ] 画面

8. [サイト サーバーのローカル ドライブ] オプションを選択します。

9. [参照] をクリックして、ServerProtect のインストールに使用するパッケージ定義ファイル (PDF) があるディレクトリを指定します。ディレクトリを選択して、[次へ] をクリックします。[定義に基づくパッケージの作成ウィザードの完了] 画面が表示されます。

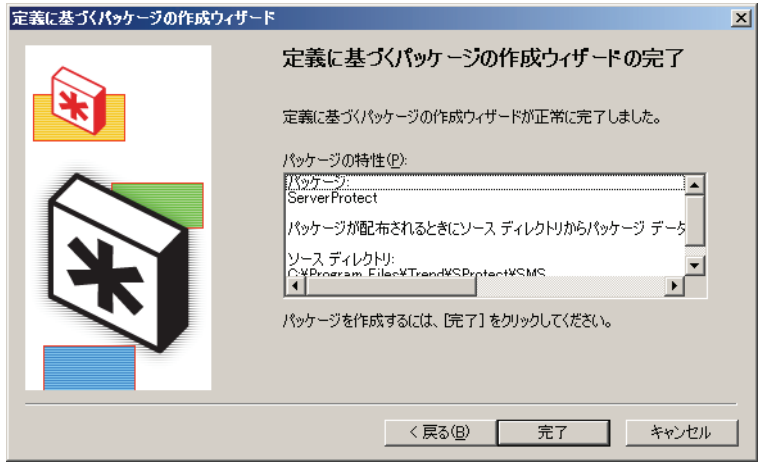


図 2-20. [定義に基づくパッケージの作成ウィザードの完了] 画面

10. [完了] をクリックしてパッケージを作成します。
11. ソフトウェアをインストールするサーバを選択するには、SMS 管理コンソールのエクスプローラツリーで、[パッケージ] → [ServerProtect] → [配布ポイント] の順に選択します。

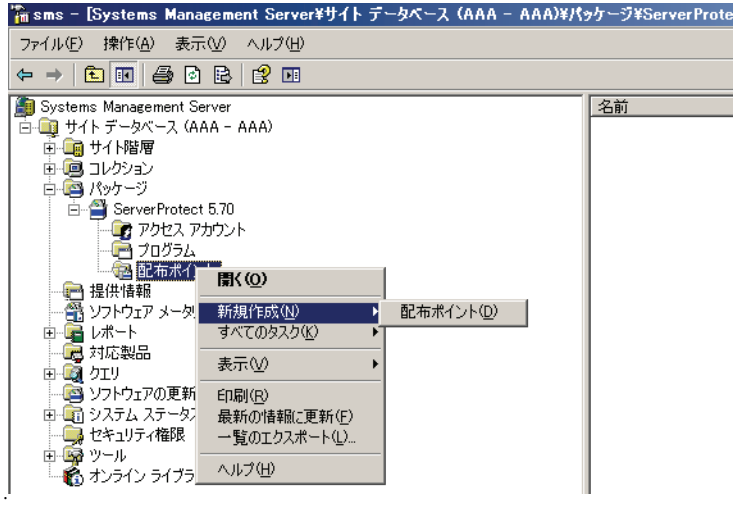


図 2-21.　SMS 管理コンソールの画面

12. [配布ポイント] を右クリックして、[新規作成] → [配布ポイント] の順に選択します。

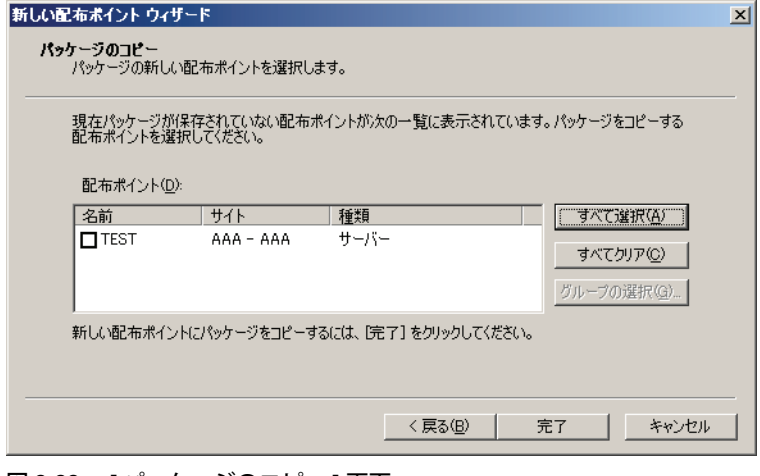


図 2-22.　[パッケージのコピー] 画面

13. 配布ポイントを選択して [完了] をクリックし、パッケージを配布ポイントにコピーします。
14. ServerProtect を複数のサーバにインストールするには、SMS 管理コンソールのエクスプローラツリーで [提供情報] を右クリックします。

15. [新規] → [提供情報] の順に選択します。[提供情報のプロパティ] 画面が表示されます。

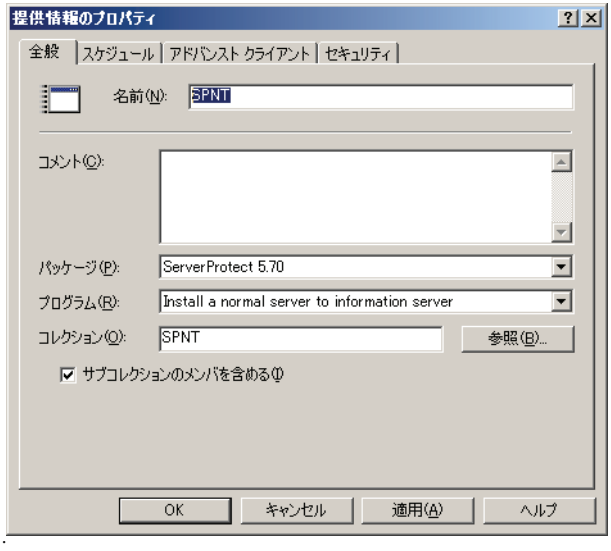


図 2-23. [提供情報のプロパティ] 画面

16. [全般] で、次の操作を実行します。
    a. [名前] ボックスに、該当する提供情報の名前を入力します。
    b. [パッケージ] リストから、配信するパッケージを選択します。
    c. [プログラム] リストから、配信するプログラムを選択します。
    d. [参照] をクリックして、プログラムの配信先サーバの [コレクション] を見つけて選択します。
17. [OK] をクリックして、サーバのコレクションにプログラムを配信します。

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、49 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。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 -f2c:¥log.txt -SMS -s -m"SPNT5"
   ```

   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"SPNT5"
   ```

   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 の削除

一般サーバのアンインストール

Windows Storage Server 2003/Server 2003 から一般サーバをアンインストールするには、次の 2 つの方法があります。

Windows 環境における一般サーバのアンインストール

Microsoft Windows 環境で一般サーバをアンインストールする方法は、次の 2 通りあります。

Windows 環境において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 [ドメイン] → [ServerProtect のアンインストール] の順に選択します。

Windows 環境において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 の [スタート] メニューから、[設定] → [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 管理コンソール] 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 2 種類の登録がそれぞれ必要です。

- プログラム管理コンソールからの製品版の登録
- 製品に同梱された FAX 登録用紙を使った FAX ユーザ登録
  (ライセンス形態によっては、登録用紙による FAX ユーザ登録が必要ない場合もあります)

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 [実行] → [製品版へのアップグレード] 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。

FAX ユーザ登録

ServerProtect 製品版をお使いの場合は、製品パッケージに同梱された FAX 登録用紙に必要事項を記入して、記載されている宛て先まで FAX 送信してください (ライセンス形態によっては、登録用紙による FAX 登録が必要ない場合もあります)。FAX でのユーザ登録により、トレンドマイクロが提供するさまざまなサポートサービスを受けることができます。サポートサービス内容の詳細については、製品パッケージに同梱されている「スタンダードサポート サービスメニュー」をご覧ください。

トレンドマイクロのサポートサービスは、FAX 登録用紙のサポート窓口の欄にご記入いただいた宛て先に提供されます。登録内容に変更が生じた場合は、カスタマーセンターへご連絡ください。

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 ドメインの管理
- インフォメーションサーバの管理
- 一般サーバの管理
- アップデートの設定
- アップデートファイルの配信
- タスクの管理
- 通知メッセージの設定
- ウイルス検索
- リアルタイム検索
- 手動検索　(ScanNow)
- 予約検索　(タスク検索)

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 管理コンソール] 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。

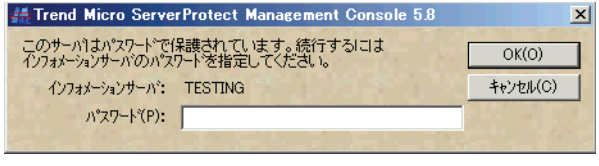


図 3-1.　インフォメーションサーバへのログオン

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。

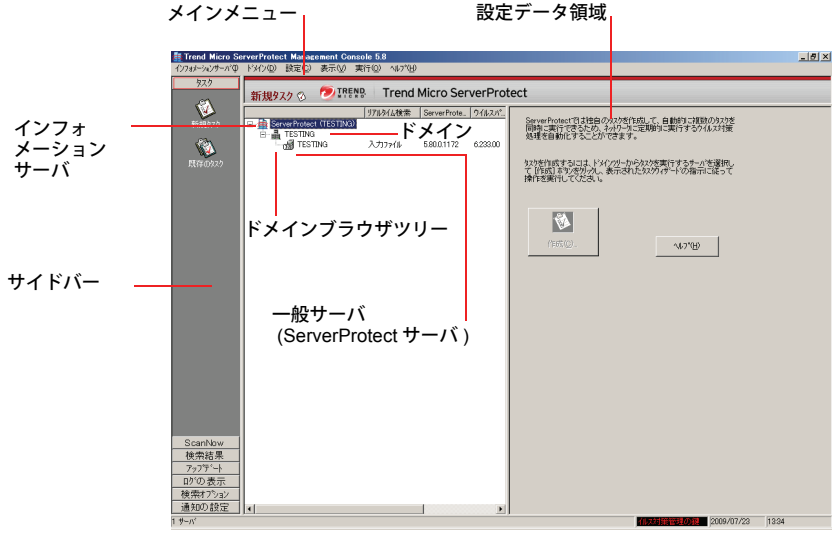


図 3-2.　管理コンソールのメイン画面構成

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。

- メインメニューは、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。
- サイドバーは、アプリケーションウィンドウの一番左側、メインメニューの下にあります。ここには 7 つの項目があり、それぞれユーザが使用できるオプションのグループを示します。
- ドメインブラウザツリーは、サイドバーの左、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とドメイン要素、各ドメインがホストしているすべての一般サーバが含まれます。
- 設定データ領域は、メインウィンドウの一番右側にある薄いグレーの背景色の画面です。ウイルス検索の設定およびログレポートシステムに関するデータ情報、コントロール UI 要素の表示に使用されます。

メインメニュー

画面上部のメインメニューには、次の 6 つ項目が表示されます。

- **インフォメーションサーバ**: インフォメーションサーバに関する情報を設定します。たとえば、インフォメーションサーバに関する情報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選択や移動です。
- **ドメイン**: 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。
- **設定**: 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。
- **表示**: ServerProtect のログファイル、検索結果、ウイルス情報を表示します。
- **実行**:
  - タスクの作成または修正
  - 手動検索　(ScanNow)
  - コンポーネントのアップデートまたはロールバック
  - インフォメーションサーバパスワードの変更
  - ドメインまたはサーバの検索
- **ヘルプ**: ヘルプシステム、ServerProtect の製品情報にアクセスします。

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。

[タスク] グループ

新規タスク: 新規タスクを作成します。

既存のタスク: 既存のタスクを表示、実行、修正、削除します。

[検索] グループ

ScanNow: 手動検索を設定、実行します。

[検索結果] グループ


リアルタイム検索 : リアルタイム検索の結果を表示します。


ScanNow: 手動検索の結果を表示します。


タスク検索 : タスクによって実行された検索結果を表示します。

[アップデート] グループ


アップデート : 最新のパターンファイル、検索エンジン、プログラムをダウンロードし、ネットワーク上に配置された一般サーバに配信します。


ロールバック : ネットワーク上で以前に実行した配信をロールバックし、前のバージョンに戻します。

[ログの表示] グループ


ログの表示 : 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。

[検索オプション] グループ


リアルタイム検索 : ネットワーク上のリアルタイム検索を設定します。


検索除外リスト : 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。


書込み禁止リスト : 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。

[通知の設定] グループ


一般の警告 : 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。


アウトブレークアラート : 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。

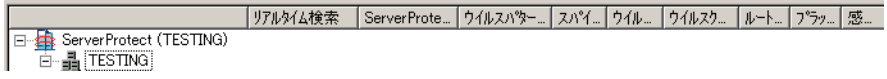
ドメインブラウザツリー

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 (ServeProtect 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


大規模感染予防モードの 32 ビット Microsoft Windows Server タイプの一般サーバ


大規模感染予防モードの 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、大規模感染予防モードの 32 ビット Microsoft Windows の一般サーバ


ウイルスに感染した、大規模感染予防モードの 64 ビット Microsoft Windows の一般サーバ

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。

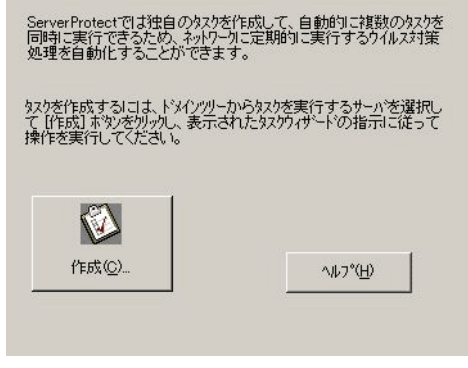


図 3-3.　設定データ領域

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 [検索結果] 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、全角文字で 25 文字まで使用することができます。

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 [ドメイン] → [新規ドメインの追加] 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 [新規ドメインの追加] を選択します。

   [ドメインの新規作成] ダイアログボックスが表示されます。

図 3-4.　ドメインの新規作成

2. 新しいドメインの名前を [ドメイン名] フィールドに入力します。

3. 次のいずれかの操作を実行して、このドメインに追加するネットワーク上のサーバを選択します。
   - 画面の左のリストからサーバを選択します。
   - [サーバ名] フィールドにサーバ名を入力します。
4. [追加] ボタンをクリックします。
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、[削除] をクリックします。[すべて削除] 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 [ドメインのリネーム] を選択します。
   - メインメニューから [ドメイン] → [ドメインのリネーム] の順に選択します。
   - キーボード上の <F2> キーを押します。

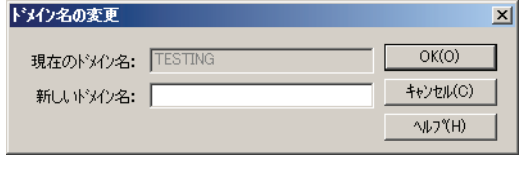


図 3-5. ドメイン名の変更

3. [ドメイン名の変更] 画面が表示されます。新しいドメイン名を [新しいドメイン名] 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 [ドメインの削除] を選択します。
   - メインメニューから [ドメイン] → [ドメインの削除] 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、76 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。

注意： 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 [インフォメーションサーバ] → [インフォメーションサーバの選択] 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 ダイアログボックスが表示されます。
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ウィンドウに表示されます。リストのサーバ表示を更新するには、[最新の情報に更新] ボタンをクリックします。

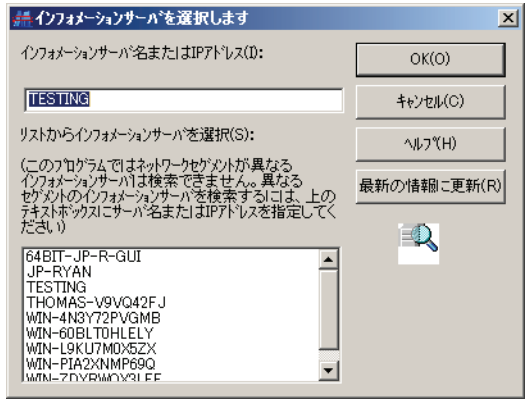


図 3-6.　インフォメーションサーバの選択

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： [一般サーバを他のインフォメーションサーバに移動] 機能を使用して、古い一般サーバを 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 [一般サーバを他のインフォメーションサーバに移動] 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 [ドメイン] → [一般サーバを他のインフォメーションサーバに移動] の順に選択します。[実行先インフォメーションサーバの選択] ダイアログボックスが表示されます。
   - 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。[一般サーバを他のインフォメーションサーバに移動] ダイアログボックスが表示されます。
   - [ユーザ名] および [パスワード] フィールドに値を入力します。[OK] ボタンをクリックします。

   [実行先インフォメーションサーバの選択] ダイアログボックスが表示されます。
2. 移動先のインフォメーションサーバを選択し、[OK] をクリックします。
3. 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。

- **ServerProtect プログラム** : ServerProtect 5.8 のアプリケーションプログラムを配信できます。ユーザは、ServerProtect アプリケーションをアップグレードする新しいオプションを選択できるようになりました。
  - ActiveUpdate サーバからのダウンロードは 2009 年現在予定されていません。インストールした ServerProtect 5.8 インフォメーションサーバから配信のみ可能です。
- **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 プラットフォーム)**: 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。
- **ダメージ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。
- **ダメージクリーンナップテンプレート** : ダメージクリーンナップテンプレートは、ダメージクリ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次の図で説明します。

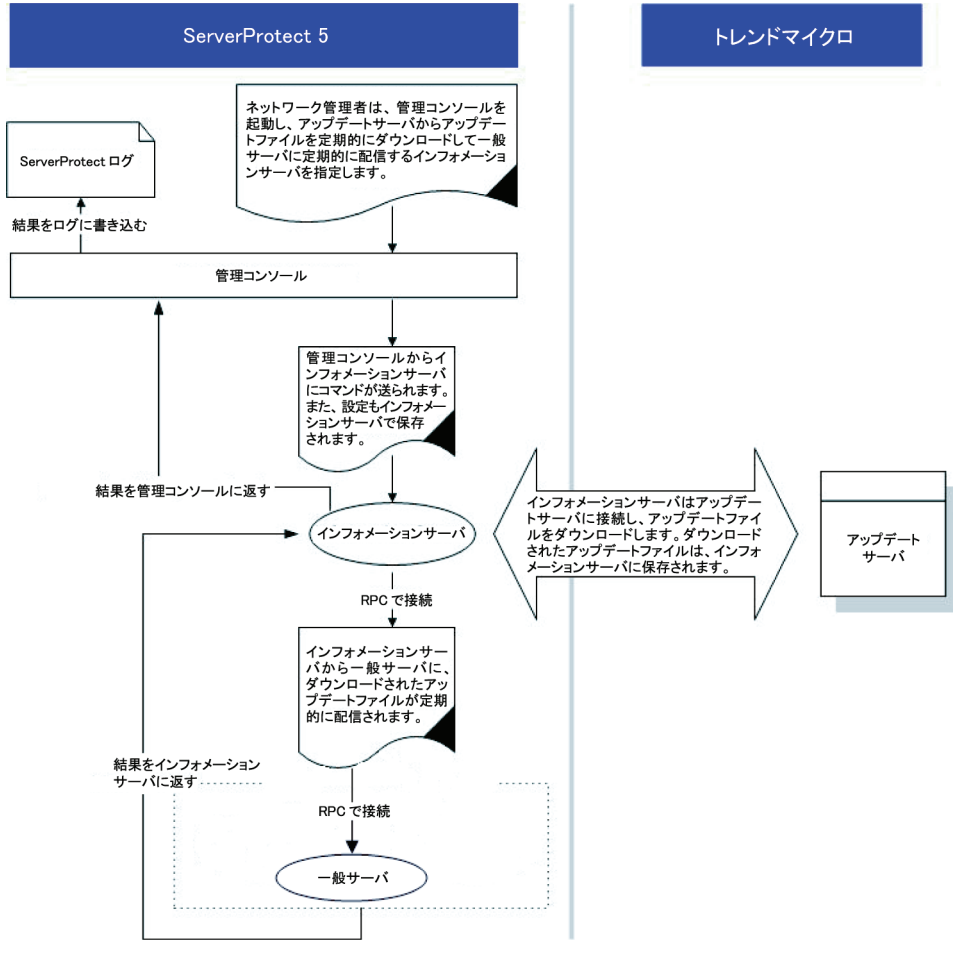


図 3-7.　ダウンロードと配信の流れ

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 [アップデート] → [アップデート] の順に選択します。
   - メインメニューから [実行] → [アップデート] の順に選択します。
2. [アップデート] メイン画面が表示されます。

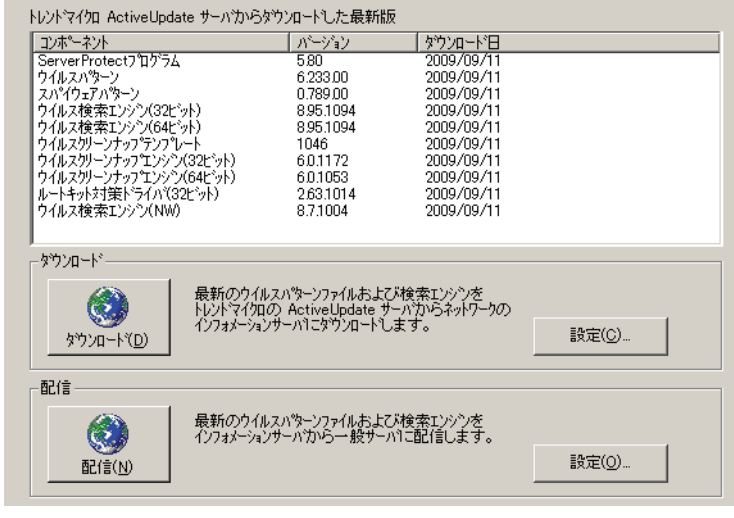


図 3-8.　[アップデート] メイン画面

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、[アップデート] 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)
- ダメージクリーンナップテンプレートのバージョン

- ダメージクリ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 [アップデート] → [アップデート] の順に選択します。
   - メインメニューから [実行] → [アップデート] の順に選択します。
2. [ダウンロード] グループの [設定] ボタンをクリックします。[ダウンロードオプション] 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、[インターネット] オプションを選択し、次の URL を指定します。

   ```
   http://spnt58-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。

   ```
   C:¥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 [アップデート] → [アップデート] の順に選択します。
   - メインメニューから [実行] → [アップデート] の順に選択します。
2. [ダウンロード] で [設定] ボタンをクリックします。[ダウンロード] ダイアログボックスが表示されます。
3. [ローカルまたはネットワークドライブ] 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. [ユーザ名] および [パスワード] 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. [ダウンロード] 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。
   - C:¥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 [アップデート] → [アップデート] の順に選択します。
   - メインメニューから [実行] → [アップデート] の順に選択します。
2. [アップデート] ダイアログボックスで [ダウンロード] 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 [ダウンロード] 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 [ダウンロード] ボタンをクリックすると、「HTTP 接続エラーが発生しました」または「HTTP 認証エラーが発生しました」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、90 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 [アップデート] → [アップデート] の順に選択します。
   - メインメニューから [実行] → [アップデート] の順に選択します。
2. [ダウンロード] で [設定] ボタンをクリックします。[ダウンロードオプション] ダイアログボックスが表示されます。
3. [予約設定] タブをクリックします。

図 3-9.　ダウンロードオプション - 予約設定

4. [予約] グループの [検索周期] リストで、ダウンロードを実行する周期を選択します。
   - [週 1 回] 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。
   - [毎日] 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。
   - [毎時間] 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 [なし] 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、[再試行] 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 [回数] と [遅延] に指定します。
6. [OK] をクリックして設定を保存します。
   ダウンロードされたファイルは `C:¥Program Files¥Trend¥Sprotect¥SpntShare` ディレクトリに保存されます。

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 [アップデート] → [アップデート] の順に選択します。
   - メインメニューから [実行] → [アップデート] 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 [アップデート] ダイアログボックスで [設定] ボタンをクリックします。[ダウンロードオプション] ダイアログボックスが表示されます。

図 3-10. ダウンロードオプション - ダウンロード元

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 [アップデート] → [アップデート] の順に選択します。
   - メインメニューから [実行] → [アップデート] の順に選択します。
2. [ダウンロード] で [設定] ボタンをクリックします。[ダウンロードオプション] ダイアログボックスが表示されます。

3. [プロキシの設定] タブをクリックします。

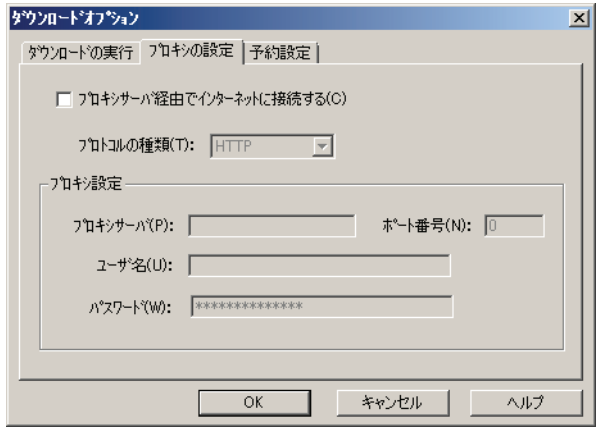


図 3-11. ダウンロードオプション - プロキシの設定

4. [プロキシサーバ経由でインターネットに接続する] チェックボックスをオンにします。
5. [プロトコルの種類] 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. [プロキシ設定] グループで、次の操作を実行してください。
   - [プロキシサーバ]、[ポート番号] 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。
   - [ユーザ名] および [パスワード] 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 [アップデート] → [アップデート] の順に選択します。
   - メインメニューから [実行] → [アップデート] の順に選択します。
2. [配信] ボタンをクリックします。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 [はい] をクリックします。[配信] ダイアログボックスが表示されます。

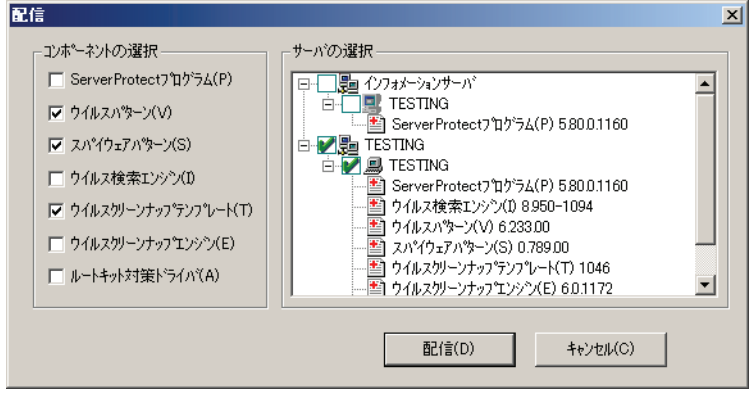


図 3-12. 配信

[コンポーネントの選択] グループの多数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。[ウイルスパターン]、[スパイウェアパターン]、および [ダメージクリーンナップテンプレート] の各チェックボックスは、初期設定でオンになっています。
[サーバの選択] 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、[コンポーネ

ントの選択] グループに表示される使用可能なチェックボックスは、[ServerProtect プログラム]、[ウイルスパターン]、[スパイウェアパターン]、[ウイルス検索エンジン]、[ダメージクリーンナップテンプレート]、[ダメージクリンナップエンジン] 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、[ルートキット対策ドライバ] 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、[コンポーネントの選択] 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、[サーバの選択] 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。[配信] 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、97 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、97 ページの「新規タスクの作成」を参照してください。

注意： 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 [アップデート] → [アップデート] の順に選択します。
   - メインメニューから [実行] → [アップデート] の順に選択します。
2. [配信] グループの [設定] ボタンをクリックします。[配信オプション] ダイアログボックスが表示されます。

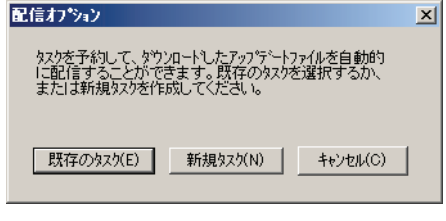


図 3-13. 配信オプション

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 [新規タスク] をクリックします。
   - 既存のタスクを編集する場合は [既存のタスク] をクリックします。

   タスクの新規作成と編集についての詳細は、97 ページの「新規タスクの作成」、および 103 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： 配信内容をロールバックするにあたり、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は、両者をロールバックする必要があります。

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 [アップデート] → [ロールバック] の順に選択します。
   - メインメニューから [実行] → [ロールバック] の順に選択します。

   [ロールバック] の設定画面が表示されます。

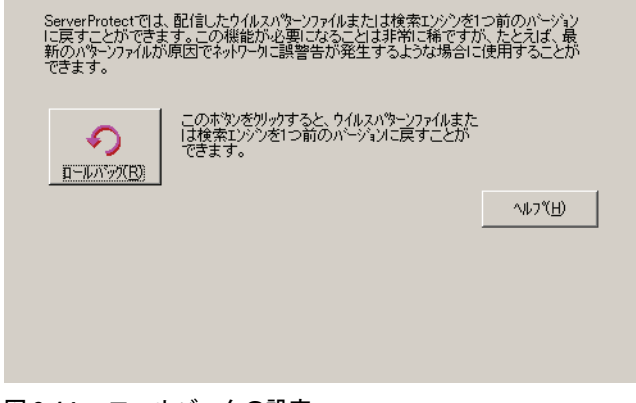


図 3-14. ロールバックの設定

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

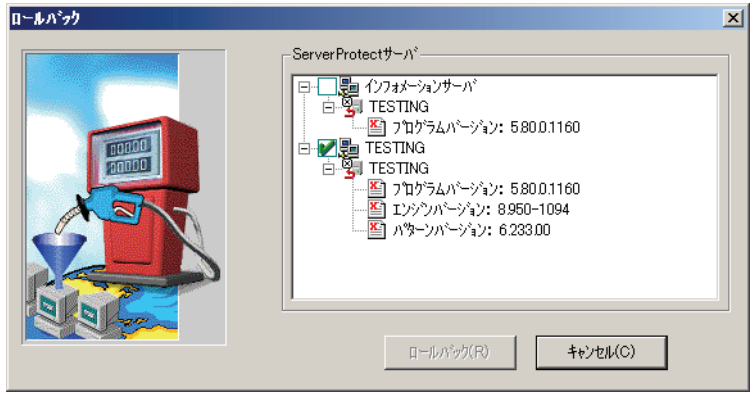


図 3-15. ロールバック

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、[ロールバック] 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。

- **リアルタイム検索設定**
  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。
- ScanNow
  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。実行すると指定したドライブ / ディレクトリの検索対象ファイルすべてに対する検索が開始されます。
- **ログの削除**
  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。
- **ログのファイル出力**
  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。
- **ログの印刷**
  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。
- **統計の実行**
  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。
- **配信**
  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。

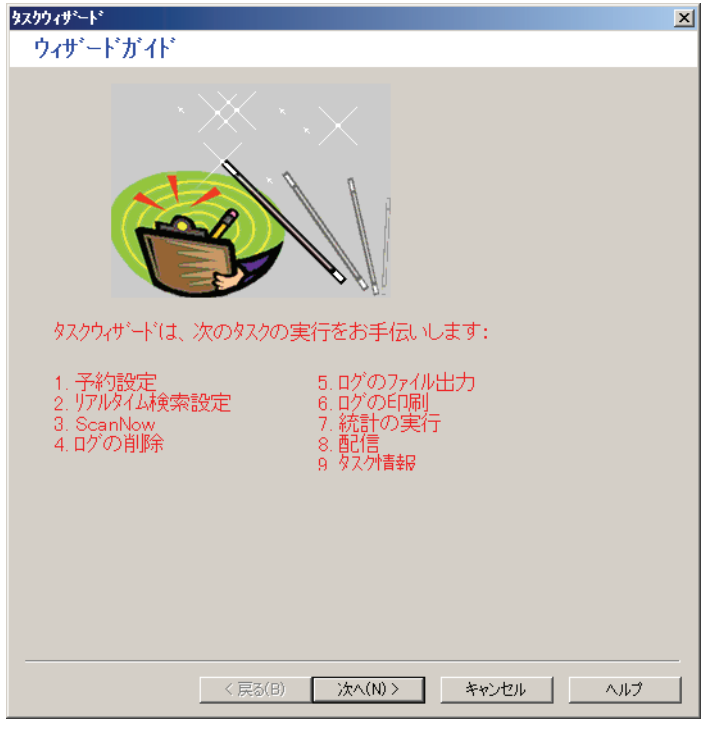


図 3-16.　タスクウィザード

初期設定のタスク

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。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。

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 [実行] → [タスクの作成] の順に選択します。
- サイドバーから [タスク] → [新規タスク] の順に選択します。

3. [作成] ボタンをクリックします。[タスクの新規作成] ダイアログボックスが表示されます。

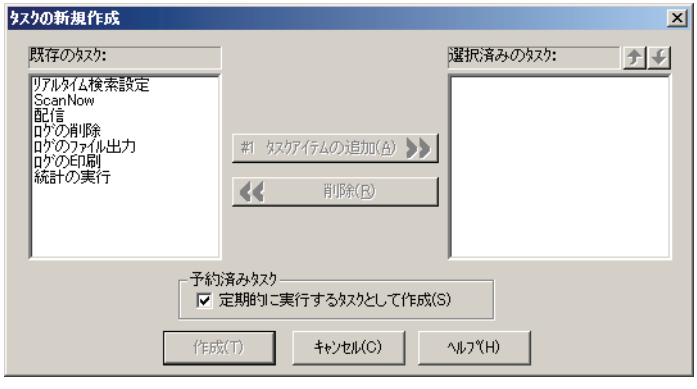


図 3-17. タスクの新規作成

4. 左の [既存のタスク] 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. [#n タスクアイテムの追加] ボタンをクリックして、手順 4 で選択した機能を [選択済みのタスク] 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、[既存のタスク] 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。

注意： 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、[選択済みのタスク] 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。

このタスクを予約して自動的に実行したい場合は、必ず [定期的に実行するタスクとして作成] オプションを有効にしてください。

6. [作成] 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。

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. 97 ページの「新規タスクの作成」の手順 1 ～ 6 を実行します。[予約済みタスク] の [定期的に実行するタスクとして作成] 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 3-16 を参照)。[タスクウィザード] ダイアログボックスが表示されます。
2. [次へ] ボタンをクリックします。[予約設定] ダイアログボックスが表示されます。

図 3-18. 予約設定

3. [予約設定] グループの [周期] リストで、ダウンロードを実行する周期を選択します。
   - [月 1 回] 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。
   - [週 1 回] 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。
   - [毎日] 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。

- [毎時間] を選択した場合は、タスクの実行時刻 (分) を指定します。

4. [次へ] 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。

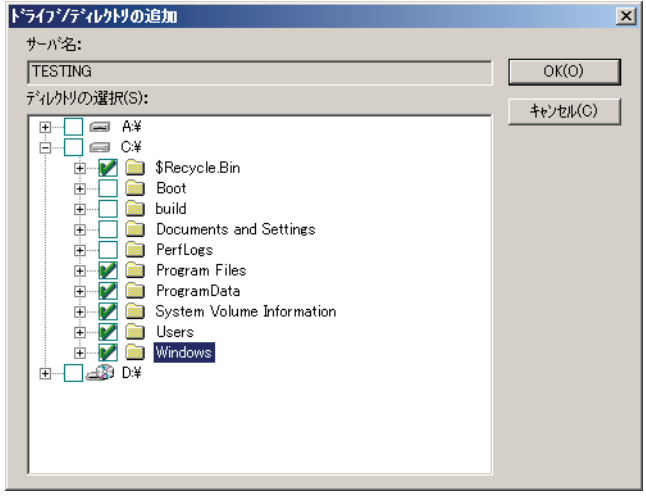


図 3-19. ドライブ / ディレクトリの追加

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 [タスク情報] では、タスク名と所有者を指定します。作成したタスクは、[デフォルトのタスクとして作成する] 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。

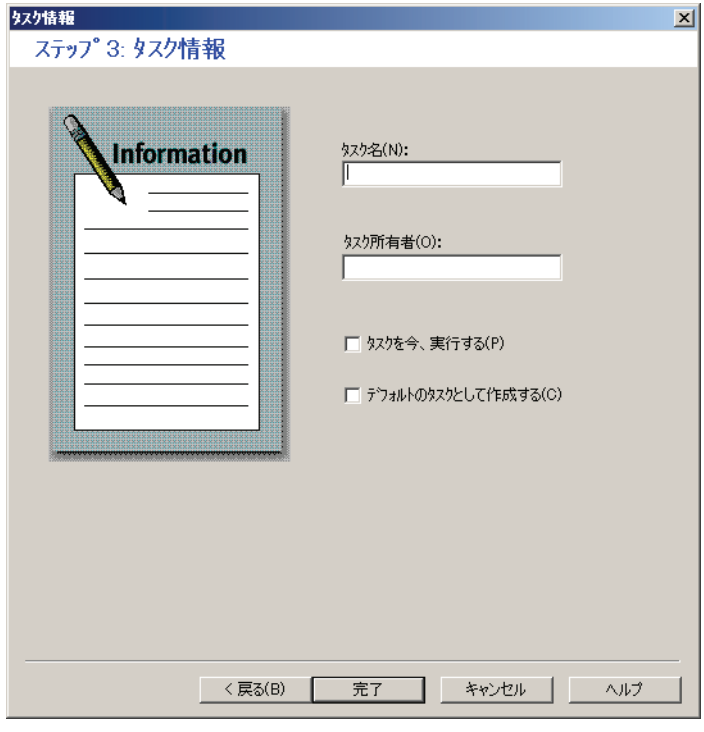


図 3-20.　タスク情報

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. [タスク名] にタスク名を入力します。
2. [タスク所有者] 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、[タスクを今、実行する] 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、[デフォルトのタスクとして作成する] チェックボックスをオンにします。
5. [完了] 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 [タスク] → [既存のタスク] の順に選択します。
- メインメニューから [実行] → [既存のタスク] 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。

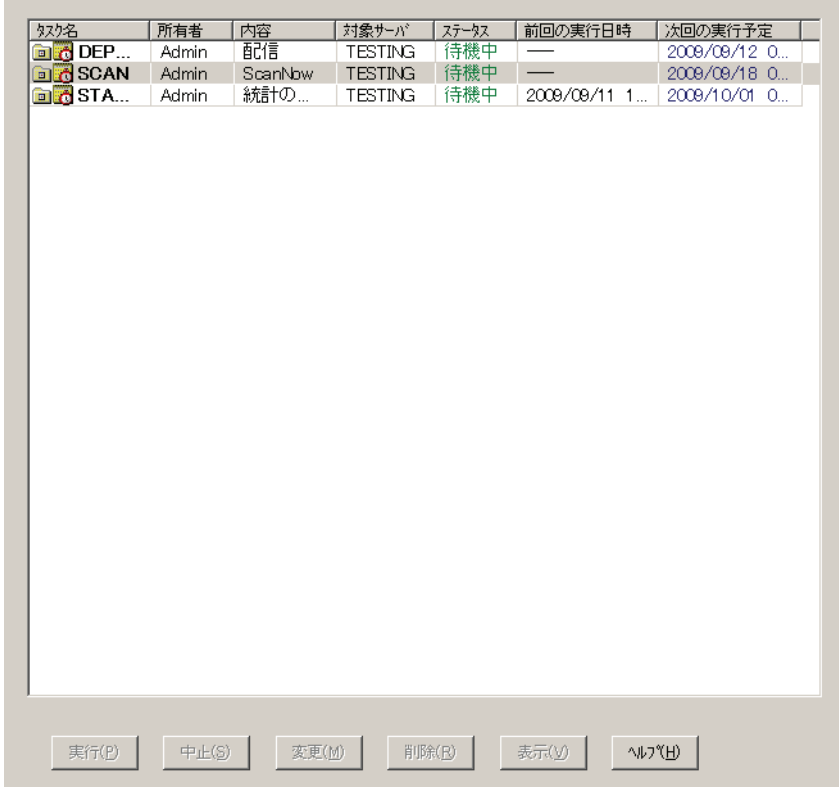


図 3-21. 既存のタスクを表形式で表示

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、[前回の実行日時] および [次回の実行予定] 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

[既存のタスク] リストには、定義された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することができます。

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 [タスク] → [既存のタスク] の順に選択します。
   - メインメニューから [実行] → [既存のタスク] の順に選択します。

   [既存のタスク] 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、[実行] 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 [タスク] → [既存のタスク] の順に選択します。
   - メインメニューから [実行] → [既存のタスク] の順に選択します。

   [既存のタスク] リストが表示されます。
2. [既存のタスク] リストで修正したいタスクを選択します。
3. [変更] ボタンをクリックします。[タスクの変更] ダイアログボックスが表示されます。

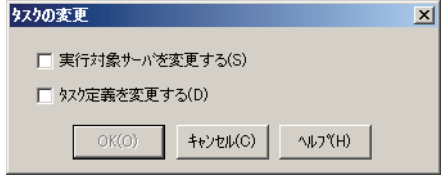


図 3-22. タスクの変更

4. いずれかまたは両方のオプションを有効にします。
   - [実行対象サーバを変更する] 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。

- [タスク定義を変更する] 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. [タスクを実行するサーバの選択] 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. [追加] をクリックします。

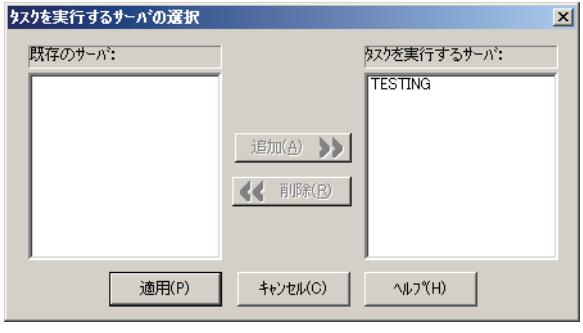


図 3-23. タスクを実行するサーバの選択

3. [適用] ボタンをクリックします。

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. [既存のタスク] 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。

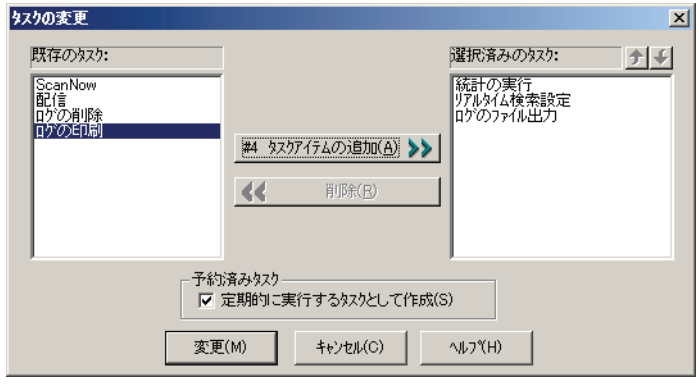


図 3-24.　タスクの変更

2. [#n タスクアイテムの追加] ボタンをクリックして、手順 1 で選択した機能を [選択済みのタスク] 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 [定期的に実行するタスクとして作成] チェックボックスを有効にしてください。

注意： 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、[選択済みのタスク] 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. [変更] 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

既存タスクの属性を [既存のタスク] 画面で表示することができます。これによって、タスクを実行する前にタスクの内容を確認することができます。

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 [実行] → [既存のタスク] の順に選択します。

- サイドバーから [タスク] → [既存のタスク] の順に選択します。

2. [既存のタスク] リストで表示するタスクを選択します。
3. [表示] ボタンをクリックします。または [既存のタスク] 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。[タスク情報の表示] ダイアログボックスが表示されます。

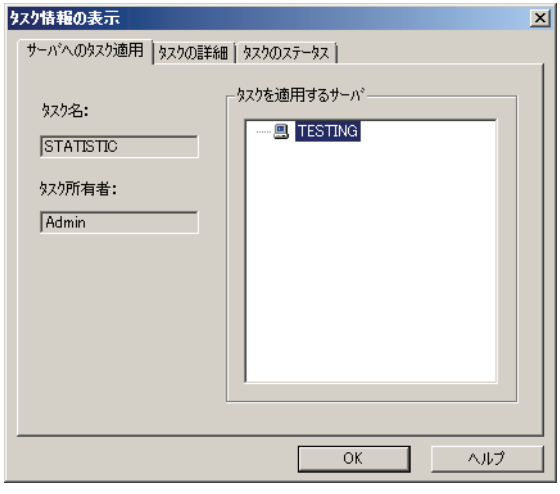


図 3-25. タスク情報の表示

このダイアログボックスには [サーバへのタスク適用]、[タスクの詳細]、[タスクのステータス] という 3 つのタブがあります。

- **サーバへのタスク適用**
  タブの左側にタスク名とタスク所有者が表示されます。[タスクを適用するサーバ] 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。
- **タスクの詳細**
  タスクを構成するすべての機能が表示されます。
  [タスク実行順序] リストボックスの機能アイコンをクリックすると、右の [タスクの定義] 欄に機能の定義が表示されます。
- **タスクのステータス**
  [タスクを適用するサーバ] 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。[ステータス]、[前回の実行日時]、および [次回実行予定] 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 [タスク情報の表示] ダイアログボックスを閉じます。

既存のタスクの削除

[既存のタスク] リストには、定義されているすべてのタスクの情報が表示されています。このリストを使用してタスクの定義を削除することができます。

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 [実行] → [既存のタスク] の順に選択します。
   - サイドバーから [タスク] → [既存のタスク] の順に選択します。
2. [既存のタスク] リストで削除するタスクを選択します。
3. [削除] 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することができます。警告方法についての詳細は、110 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。

- **ウイルス感染**
  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**
  サーバ上でスパイウェアに感染したファイルが検出された場合

- **書込み禁止ファイルの変更の試み**
  書込み禁止の設定を変更しようとした場合
- **リアルタイム検索設定の変更**
  ServerProtect の設定に変更があった場合
- **サービスの起動 / 停止**
  ServerProtect が起動 / 停止された場合
- **ウイルスパターンの有効期限切れ**
  パターンファイル (ウイルスパターン) の期限が切れた場合
- **スパイウェアパターンの有効期限切れ**
  パターンファイル (スパイウェアパターン) の期限が切れた場合

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 [設定] → [通知] → [一般の警告] の順に選択します。
   - 左のサイドバーから [通知の設定] → [一般の警告] の順に選択します。

   画面の右側に [一般の警告] の設定データ領域が表示されます。

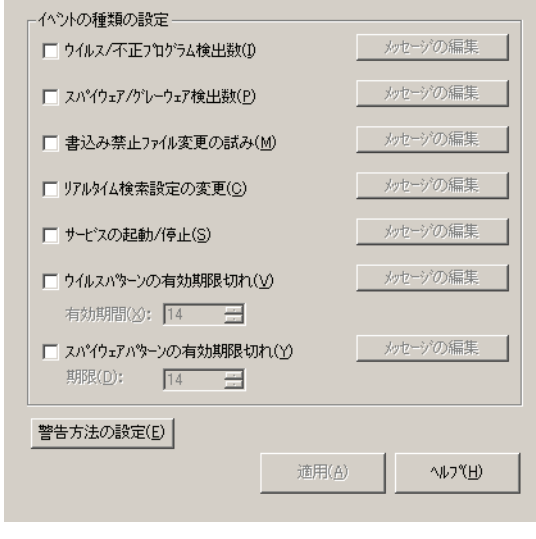


図 3-26. 一般の警告の設定

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 [メッセージの編集] ボタンをクリックします。[警告メッセージの編集] 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。
6. [警告方法の設定] 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、110 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 [通知の設定] → [アウトブレークアラート] の順に選択します。
   - メインメニューから [設定] → [通知] → [アウトブレークアラート] の順に選択します。

   [アウトブレークアラート] の設定画面が画面の右側に表示されます。

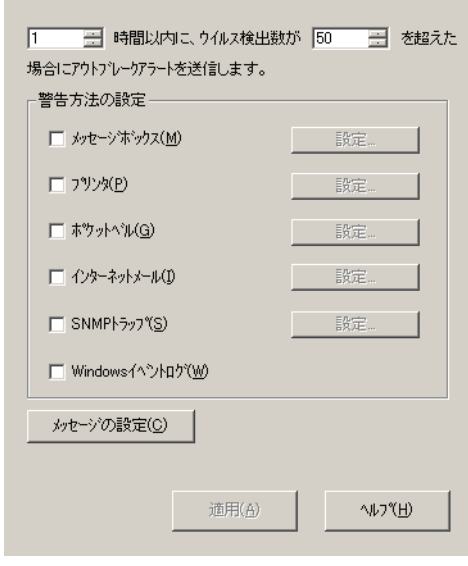


図 3-27. アウトブレークアラートの設定

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 [設定] 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、110 ページの「警告方法の設定」を参照してください。
6. [警告メッセージ] グループの [メッセージの設定] 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。
7. [適用] 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。

- **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。
- **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。

- **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。
- **インターネットメール**
  ウイルスの検出時にメールメッセージが送信されます。
- **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 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 [通知の設定] → [アウトブレークアラート] の順に選択します。
   - メインメニューから [設定] → [通知] → [アウトブレークアラート] 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 [設定] → [通知] → [一般の警告] の順に選択して、[警告方法の設定] をクリックします。
   - サイドバーから [通知の設定] → [一般の警告] の順に選択して、[警告方法の設定] をクリックします。
3. [インターネットメール] チェックボックスをオンにし、対応する [設定] ボタンをクリックします。[インターネットメール警告の設定] ダイアログボックスが表示されます。

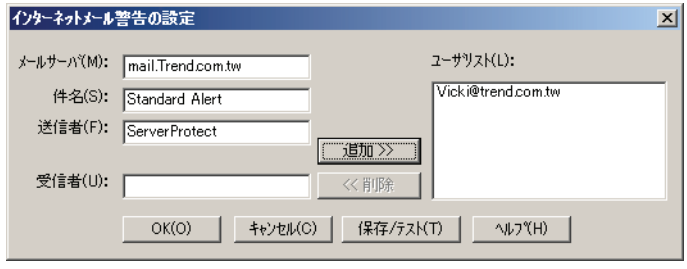


図 3-28. インターネットメール警告の設定

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 [メールサーバ] に入力します。
   b. メッセージの件名を [件名] に入力します。
   c. メッセージの [送信者] 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 [受信者] テキストボックスに入力します。[追加] 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 [削除] 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 [保存 / テスト] 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、移動 、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についての詳細は、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。[検索結果] 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「ログ情報の表示」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。

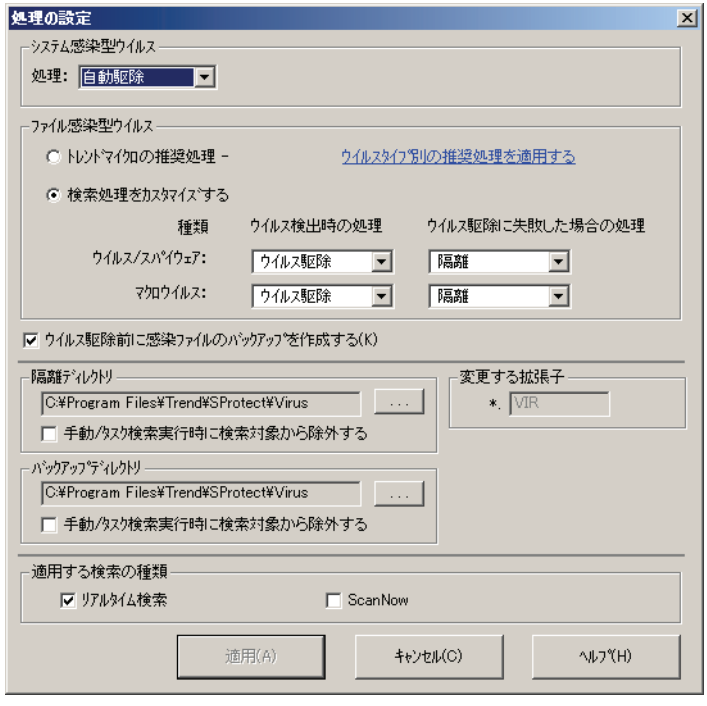


図 3-29.　ウイルス検索処理の設定

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　[処理の設定] ボタンをクリックします。[ウイルス検索処理の設定] 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. [システム感染型ウイルス] グループの　[処理] 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。[自動駆除] または　[放置 (手動処理)] のいずれかを選択することができます。
3. [ファイル感染型ウイルス] 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。

- [検索処理をカスタマイズする] 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、[ウイルス検出時の処理]、および [ウイルス駆除に失敗した場合の処理] リストから適切な処理を選択します。詳細については 18 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についての詳細は、25 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： [ウイルス駆除] を選択した場合は、 [ウイルス駆除前にバックアップを作成する] 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。詳細については、オンラインヘルプの「ディレクトリ除外リスト」トピックを参照してください。

選択された検索の種類が [適用する検索の種類] ダイアログボックスに表示されます。

4. [適用] 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。検索プロファイルについての詳細は、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、103 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。手順については、116 ページの「リアルタイム検索の設定」および 120 ページの「手動検索 (ScanNow)」を参照してください。
2. [プロファイルの保存 / 削除] ボタンをクリックすると、[プロファイルの保存 / 削除] ダイアログボックスが表示されます。

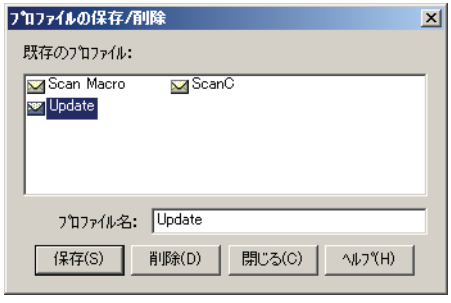


図 3-30.　プロファイルの保存 / 削除

3. プロファイルの名前を [プロファイル名] テキストボックスに入力します。
4. [OK] 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 [ScanNow] → [ScanNow] の順に選択します。
   - メインメニューから [実行] → [ScanNow] の順に選択します。
   - サイドバーから [検索オプション] → [リアルタイム検索] の順に選択します。
   - メインメニューから [設定] → [検索オプション] → [リアルタイム検索] の順に選択します。
2. [プロファイルの保存 / 削除] ボタンをクリックすると、[プロファイルの保存 / 削除] ダイアログボックスが表示されます。
3. [既存のプロファイル] 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. [削除] 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、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。リアルタイム検索を実行することで、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。

リアルタイム検索の設定

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 24 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 [検索オプション] → [リアルタイム検索] の順に選択します。
   - メインメニューから [設定] → [検索オプション] → [リアルタイム検索] の順に選択します。

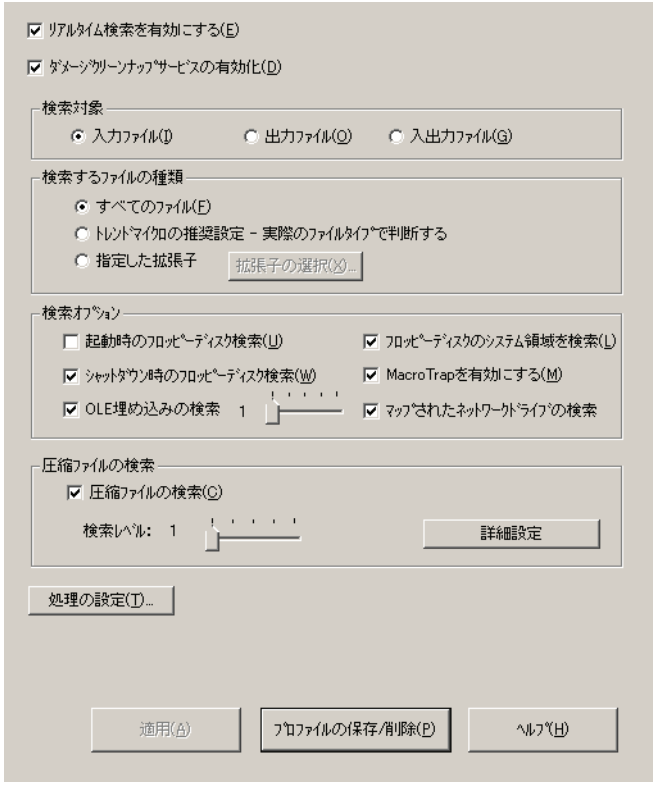


図 3-31. リアルタイム検索の設定

3. 画面上部の [リアルタイム検索を有効にする] チェックボックスをオンにします。
4. [ダメージクリーンナップサービスの有効化] チェックボックスをオンにして、ダメージクリ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. [検索対象] グループで、検索するファイルの方向を選択します。
   - **入力ファイル**: サーバにコピーされるファイルを検索します。
   - **出力ファイル**: サーバからコピーされるファイルを検索します。
   - **入出力ファイル**: サーバ上の入力、出力、両方向のファイルを検索します。
6. [検索するファイルの種類] グループで検索対象のファイルを選択します。

- **すべてのファイル** : すべてのファイルを検索します。
- **トレンドマイクロの推奨設定** : 実際のファイルタイプを識別することによってファイルが検索されます。

  詳細については、25 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。
- **指定した拡張子を持つファイル** : 指定された種類のファイルのみを検索します。[拡張子の選択] 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。ファイルの種類の選択についての詳細は、125 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. **[検索オプション]** 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

   各検索オプションについての詳細は、116 ページの「リアルタイム検索の設定」を参照してください。
8. 圧縮ファイルを検索する場合は、[圧縮ファイルの検索] チェックボックスをオンにしてください。また、[検索レベル] 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 [指定した拡張子を持つファイル] 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. [処理の設定] ボタンをクリックして、リアルタイム検索中に検出したウイルス感染ファイルに対する ServerProtect の処理を設定します。処理の設定についての詳細は、113 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. [適用] ボタンをクリックして設定を保存するか、または [プロファイルとして保存] 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 [実行] → [ScanNow] の順に選択します。

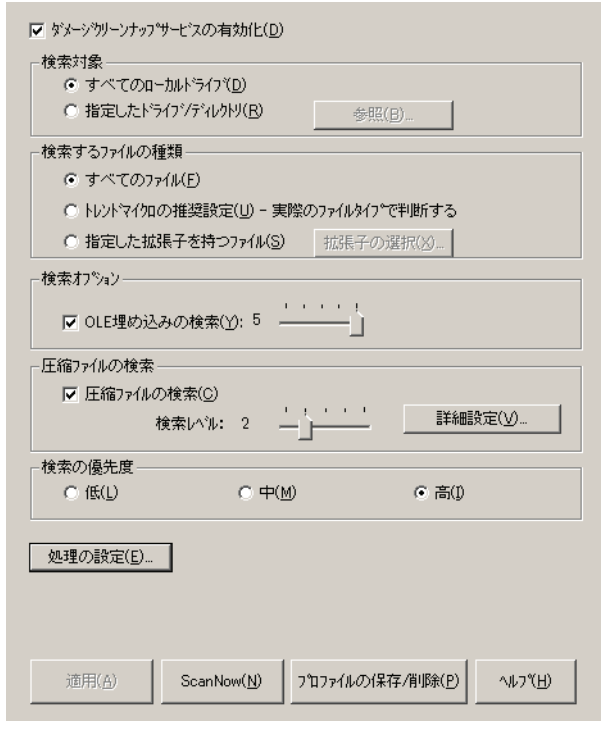


図 3-32. 手動検索の設定

3. [ダメージクリーンナップサービスの有効化] 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. [検索対象] グループで次のオプションを選択します。
   - **すべてのローカルドライブ** : サーバ上のすべてのドライブが検索されます。
   - **指定したドライブ / ディレクトリ** : 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 [参照] ボタンをクリックして、[ドライブ / ディレクトリの追加] 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。

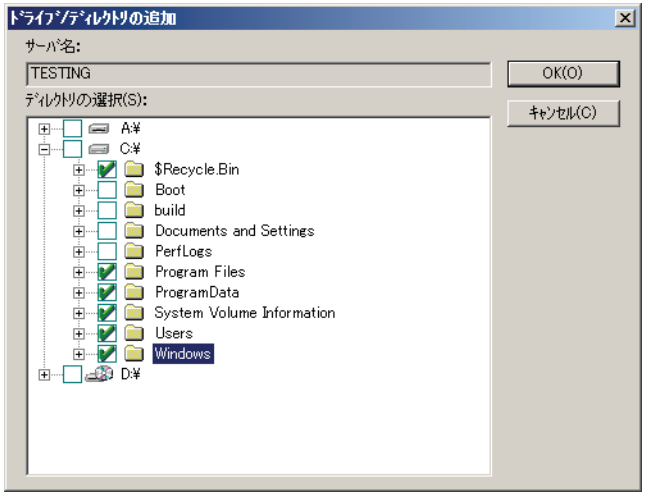


図 3-33.　ドライブ / ディレクトリの追加

5. [検索するファイルの種類] グループで次のオプションを選択します。
   - **すべてのファイル** : すべてのファイルを検索します。
   - **トレンドマイクロの推奨設定** : 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、25 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。
   - **指定した拡張子を持つファイル** : 指定された種類のファイルのみを検索します。
     [拡張子の選択] 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。ファイルの種類の選択についての詳細は、125 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、[検索オプション] グループで [OLE 埋め込みの検索] 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、[圧縮ファイルの検索] チェックボックスをオンにします。[検索レベル] 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 [指定した拡張子を持つファイル] 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 [検索の優先度] 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。[低]、[中]、[高] から選択してください。
9. [処理の設定] 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。処理の設定についての詳細は、113 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. [適用] ボタンをクリックして設定内容を適用するか、または [プロファイルの保存 / 削除] 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 [プログラム] → [アクセサリ] → [エクスプローラ] 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] をクリックすると、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、97 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検索を実行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. [リアルタイム検索] または [ScanNow] の設定画面で、[検索するファイルの種類] の [指定した拡張子を持つファイル] を選択し、[拡張子の選択] をクリックして、検索するファイルの種類を指定します。[検索対象ファイルの選択] ダイアログボックスが表示されます。

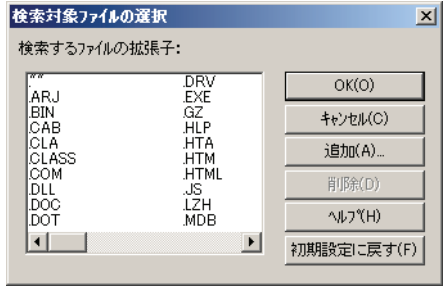


図 3-34. 検索対象ファイルの選択

2. 次のいずれかの操作を実行してください。
   - [追加] ボタンをクリックします。[ファイル拡張子の追加] ダイアログボックスが表示されます。

図 3-35. ファイル拡張子の追加

   追加するファイル拡張子をテキストボックスに入力して [OK] をクリックします。
   - 初期設定値を使用する場合は、[初期設定に戻す] ボタンをクリックします。または、[キャンセル] 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)			
.ARJ	.BIN	.CAB	.CLA
.CLASS	.COM	.DLL	.DOC
.DOT	.DRV	.EXE	.GZ
.HLP	.HTA	.HTM	.HTML
.JS	.LZH	.MDB	.MPP
.MPT	.MSG	.OCX	.OFT
.OVL	.PIF	.POT	.PPS
.PPT	.RAR	.RTF	.SCR
.SHS	.SYS	.TAR	.VBS
.VSD	.VST	.XLA	.XLS
.XLT	.Z	.ZIP	

- 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 [削除] ボタンをクリックします。

3. [OK] をクリックして [検索対象ファイルの選択] ダイアログボックスを閉じます。

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 5.8 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 や 5.7 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 のインフォメーションサーバは、古い一般サーバ (バージョン 5.58 および 5.7) に対する一般サーバの追加または移動要求を拒否するので、アップグレードする必要のある古い一般サーバを、アップグレードするインフォメーションサーバにすべて移動してください。

   警告： 一般サーバが 64 ビットコンピュータである場合、32 ビットコンピュータから実行するリモートアップグレードは失敗します。この問題を解決するには、ローカルインストール、サイレントインストール、またはプログラムの配信によってアップグレードを実行して、64 ビットコンピュータ上の ServerProtect 5.7 一般サーバをアップグレードします。

   注意： また、「一般サーバの追加」または「一般サーバの移動」機能を使用して、古い一般サーバを追加することはできません。

   注意： 「プログラムの配信」機能を使用して ServerProtect 5.7 一般サーバをアップグレードする場合は、ServerProtect 5.7 一般サーバに、「プログラムのアップデート」機能を有効にするビルド 1095 以降のホットフィックスまたはパッチが適用されていることを確認してください。

   注意： 配信用プログラムが格納されている次のフォルダを削除した場合、プログラムの配信はできません。
   xxxxxx¥spntshare¥ServerProtect¥

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、130 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」参照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、130 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」参照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。
   - ServerProtect 5.8 のプログラム配信機能を使用して、アップグレードを実行する。

注意： 5.7 バージョンの ServerProtect 一般サーバがインストールされているサーバネットワークシステムの場合は、すべての SPNT5.7 一般サーバにパッチを適用して、プログラムの配信機能を有効にしてください。詳細については、トレンドマイクロのテクニカルサポートまでお問い合わせください。SPNT 5.58 では、この機能が既にあるので、このような問題は発生しません。

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まったく同じです。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、41 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 [コンポーネントの選択] ウィンドウを次に示します。

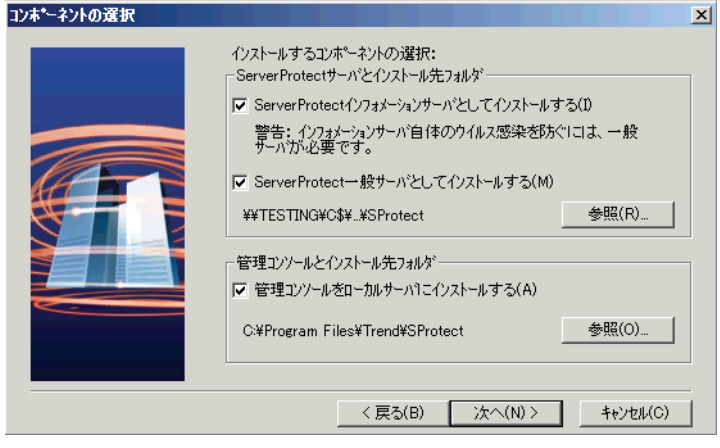


図 4-1. ServerProtect の [コンポーネントの選択] ウィンドウ

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わ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、[参照] をクリックして [ServerProtect インストール先の選択] ウィンドウを表示します。50 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、[コンポーネントの選択] ウィンドウが再表示され、選択をやり直すよう求められます。

注意： Trend Micro Control Manager エージェントがインストールされている場合は、インフォメーションサーバのインストール後にアップグレードしてください。

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 [コンポーネントの選択] ウィンドウが表示されます。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) [参照] 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、41 ページの「ServerProtect パッケージのインストール」参照を参照してください。

警告： 一般サーバが 64 ビットコンピュータである場合、32 ビットコンピュータから実行するリモートアップグレードは失敗します。この問題を解決するには、ローカルインストール、サイレントインストール、またはプログラムの配信によってアップグレードを実行して、64 ビットコンピュータ上の ServerProtect 5.7 一般サーバをアップグレードします。

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。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"SPNT5"
   ```

例 :

   a. インストール先サーバで、SMS フォルダをドライブ「M」にマップします。
   b. コマンドプロンプトを開きます。
   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"SPNT5"
   ```

   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。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]
   ServerTargetUNCPath=D$¥Utility¥AntiVirus¥SProtect
   ```

   ここで、
   ServerTargetUNCPath: 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
```

ここで、
XXXX-XXXX-XXXX-XXXX-XXXX: シリアル番号を示します。

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、63 ページの「サイレントモードでのインストール」参照を参照してください。

プログラムの配信機能を使用した、一般サーバのアップグレード

配信機能を使用したアップグレードの実行は、サーバネットワークシステム内の古い一般サーバをアップグレードするための最も効率の良い方法です。新しい一般サーバプログラムコードは、スパイウェアパターンファイとウイルスパターンファイル、検索エンジンと DCE サービスなどのウイルス対策要素とともに、インフォメーションサーバの 1 つにダウンロードされ、システムに配信されます。サーバネットワーク管理者が実行すべき唯一の作業は、プログラムの UI 要素でそうするように選択することだけです。

注意： 「プログラムの配信」機能を使用して ServerProtect 5.7 一般サーバをアップグレードする場合は、ServerProtect 5.7 一般サーバに、「プログラムのアップデート」機能を有効にするビルド 1095 以降のホットフィックスまたはパッチが適用されていることを確認してください。詳細については、トレンドマイクロのサポート Web サイトを参照してください。

注意： プログラムの配信時、インフォメーションサーバと管理コンソールのファイルが一般サーバにすべてコピーされます。この操作では、インフォメーションサーバサービスと管理コンソールアプリケーションは作成されません。

ServerProtect 5.8 のアップグレード機能を使用するには

1. ServerProtect 5.7 をアップグレードする場合、バージョン 5.7 の一般サーバのバイナリビルドが 1095 以上であることを確認してください。
2. インフォメーションサーバが Trend Micro Control Manager Server に接続されている場合は、次の操作を実行します。
   - メインコンソールから [アップデート] → [アップデート] の順にクリックするか、メインメニューから [実行] → [アップデート] の順に選択します。
   - [設定] をクリックして、[ダウンロードオプション] ダイアログボックスを表示します。
   - [ダウンロード元] を [インターネット] に変更し、ダウンロード URL を次のものに変更します。

   `http://spnt58-p.activeupdate.trendmicro.co.jp/activeupdate/japan`

   - [OK] をクリックして設定を適用します。
   - [ダウンロード] をクリックします。

- ダウンロードが完了したら、<ServerProtect のホームディレクトリ >¥SpntShare¥ にある server.ini に次の情報が含まれていることを確認します。

注意： ServerProtect インフォメーションサーバの初期設定のパスは `C:¥program files¥Trend¥Sprotect¥SpntShare` です。

[Info_186_50000_4_5121]

Version=5.8

Update_Path=serverprotect/spnt580/auspnt50.zip, 43914

Min=5.0

Max=6.0

Path=ServerProtect/SPNT58J.zip, xxxxxxxx

[Info_2_50000_4_1]

Version=5.8

Update_Path=serverprotect/spnt580/auspnt50.zip, 43914

Min=5.0

Max=6.0

Path=ServerProtect/SPNT58J.zip, xxxxxxxx

※「xxxxxxxx」にはファイルサイズが記載されます。

3. 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 [アップデート] → [アップデート] の順に選択します。
   - メインメニューから [実行] → [アップデート] の順に選択します。
4. [配信] をクリックします。確認画面が表示されます。[はい] をクリックして手動アップデート配信に進みます。[配信] 画面が表示されます。

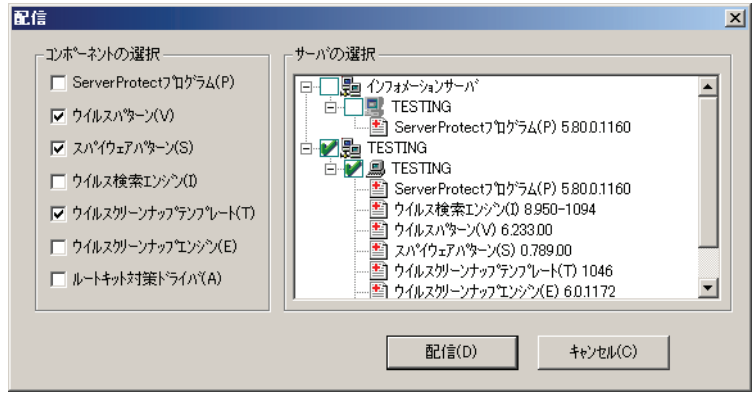


図 4-2.　[配信] 画面

5. ダウンロードと配信によって一般サーバ機能がアップグレードされるようにするには、ServerProtect プログラムの項目のチェックボックスをオンにするだけで済みます。このオプションは、アプリケーションの初期化の際に初期設定として選択された 3 つのウイルス対策コンポーネントには含まれていないことに注意してください。[配信] をクリックして [配信] 画面を閉じ、アップグレード操作を完了します。

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 ヵ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 Manger を使用すれば、サーバのグループにリモートから同一のタスクを実行したり、同一の内容を設定できます。大規模なネットワークを運用している場合、Control Manager はサーバの設定にかかる時間を大幅に節約します。

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。

• 144 ページの「Trend Micro Control Manager エージェントの機能」

Trend Micro Control Manager とは

Control Manager は、インストールされる場所やプラットフォームに関係なく、ウイルス対策製品やファイルセキュリティ製品を 1 点から集中管理することを可能にするソフトウェア管理ソリューションです。Control Manager を使用することにより、企業におけるウイルス対策ポリシーやファイルセキュリティポリシーを一貫して実施することができます。

Control Manager ではネットワーク全体を包括的に表示できるので、目標のウイルス対策戦略を効率的に作成するために、ServerProtect を含むトレンドマイクロ製品およびサービスをどのように配置すればよいか判断することができます。

Control Manager の Web ベースの管理コンソールを使用して、ネットワーク上のウイルスの活動や対応するトレンドマイクロ製品のパフォーマンスを監視することができます。

ウイルスに攻撃されると、Control Manager の Web ベースの管理コンソールは中央の司令塔として機能し、アウトブレークの監視、ウイルス対策の実施、公開直後のパターンファイルのダウンロード / 配信など、一貫したアウトブレーク対策を実現します。

Control Manager は、トレンドマイクロ エンタープライズ プロテクション ストラテジーの中核となる製品です。ウイルスの発生から終息までの一連のプロセスを、ウイルスの「アウトブレーク ライフサイクル」と捉え、このサイクル全体をトレンドマイクロがトータルにサポートします。

Control Manager には次のような機能と特長があります。

- アウトブレーク対策
- 安全な通信インフラストラクチャ
- タスク委任機能
- コマンド追跡
- リアルタイムでのウイルス対策製品管理
- エージェントインストールの集中管理
- アップデートの集中管理
- 設定の一元化
- ログレポートの一元化

Trend Micro Control Manager エージェントのインストール、削除

Control Manager エージェントをインストールするには、次の 2 つの作業を実行します。

1. Control Manager サーバからの公開鍵の取得
2. インフォメーションサーバへのエージェントのインストール

エージェントをインストールする前に、次の情報を準備してください。

- Control Manager サーバの FQDN (完全修飾ドメイン名) または IP アドレス
- インストール先 ServerProtect インフォメーションサーバ上の共有ドライブ
  エージェントをインストールするには、インストール先サーバに少なくとも 1 つの共有ドライブが必要です。
- Control Manager サーバでの管理者権限を持つアカウント (ユーザ ID) の情報
- エージェントの登録先 Control Manager サーバに格納されている公開鍵 の場所

公開鍵の取得

Control Manager エージェントをインストールするための第 1 の作業は、公開鍵の取得です。

セットアップファイルと公開鍵を取得するには、次の手順に従ってください。

1. Web ブラウザで Control Manger の管理コンソールにアクセスします。

   `https://<コンピュータ名>/ControlManager`

   <コンピュータ名> は Control Manager サーバの IP アドレスまたはホスト名です。
   Control Manger 管理コンソールの初期画面が表示されます。
2. Control Manager 管理コンソールへのアクセス権を持つユーザ ID とパスワードを入力します。
   Control Manager 管理コンソールへのアクセスには、Administrator、Power User または Operator の権限が必要です。
3. Control Manager 管理コンソールの上部のメニューから [製品] をクリックします。
4. [運用管理] → [設定] → [製品エージェントの追加 / 削除] をクリックします。
5. [製品エージェントの追加 / 削除] 画面で、[公開暗号鍵] を右クリックします。表示されるメニューで [対象をファイルに保存] をクリックします。[名前を付けて保存] 画面で、公開鍵 (E2EPublic.dat) を保存する場所を指定します。エージェントのインストール先サーバからアクセスできる場所に、公開鍵を保存してください。

エージェントのインストール

Control Manager エージェントをインストールするための第 2 の作業は、各 ServerProtect インフォメーションサーバへの Control Manager エージェントのインストールです。

Control Manager エージェントをインストールするには、次の手順に従ってください。

1. Windows の管理者アカウント (ドメイン管理者権限が必要) を使用してインフォメーションサーバが実行されているコンピュータにログオンします。
2. ServerProtect の CD-ROM の CMAgent フォルダ内にある Setup.exe をダブルクリックし、セットアッププログラムを起動します。

   [Trend Micro Control Manager Agent for ServerProtect] 画面が表示されます。
3. 初期画面で [次へ] をクリックします。画面に表示される使用許諾契約書をよくお読みください。同意する場合は [はい] をクリックします。同意いただけない場合、セットアップを続行することはできません。
4. [ユーザ ID] に、Control Manager サーバのユーザ名を入力します。Administrator、Power User または Operator の権限が必要です。ここで使用するアカウントは、インストール後も必要になります。このアカウントが故意に、または誤って削除された場合、エージェントを管理できなくなります。

   注意： エージェントのインストールでは、root アカウントを指定することをお勧めします。
5. [メッセージルーティングパスの設定] 画面で、受信および送信メッセージ用の経路を設定します。

   受信メッセージは次のいずれかの方法で受信できます。

   - **ホスト**: すべての発信元からのメッセージを受け入れます。
   - **IP ポート転送**: このオプションを選択する場合、Control Manager の通信で使用するためにマッピングされている IP アドレスまたはポート番号を入力します。
   - **プロキシサーバ**: このオプションを選択する場合、プロキシサーバの IP アドレス、ポート番号、種類 (HTTP または SOCKS 4/5) を指定します。必要に応じて、[認証が必要] チェックボックスをオンにし、ユーザ名とパスワードを入力します。

   送信メッセージは、直接またはプロキシサーバを介して送信することができます。
   受信および送信メッセージ用の経路を設定したら、 [次へ] をクリックします。
6. Control Manager サーバとの間にセキュリティで保護された通信を確立するため、[インポート] をクリックし、登録先 Control Manger サーバの公開鍵「E2EPublic.dat」を指定します。
7. 画面の指示に従い、インストールを完了します。

エージェントの削除

ServerProtect インフォメーションサーバが実行されたコンピュータから、Control Manager エージェントを削除するには、次の手順に従ってください。

1. インフォメーションサーバが実行されているコンピュータで、[スタート] → [設定] → [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。
2. [Trend Micro Control Manager Agent for ServerProtect] → [削除] の順にクリックします。確認のメッセージが表示されます。
3. ServerProtect 用 Control Manager エージェントを削除するには、[はい] をクリックします。
4. [閉じる] をクリックします。

Trend Micro Control Manager エージェントの機能

ServerProtect 用 Control Manager エージェントの機能について説明します。ServerProtect 用 Control Manager エージェントには、ServerProtect を管理するためのさまざまな機能が用意されています。

注意： Control Manager の管理コンソールからは、ServerProtect 管理コンソールの一部の機能のみが利用できます。

設定の一元化

製品ディレクトリおよび階層管理構造を使用した集中管理設定によって、1 つの管理コンソールからウイルスレスポンスおよびファイルセキュリティの処理を調整できます。これによって、組織のウイルス対策およびファイルセキュリティ対策の実施において一貫性を保つことができます。

アウトブレーク対策

大規模感染予防サービスは、Control Manager を介して利用できるトレンドマイクロのサービスです。このサービスを利用することにより、新種ウイルスに対応するパターンファイルが配布される前であっても、ウイルスへの対策を講じることができます。ウイルスの発生からパターンファイルが配信されるまでの期間、ポリシーファイルを使用してウイルスに対処することで、感染の拡大を阻止し、システムの被害を最小限に抑え、システム停止に至らないよう防ぐことができます。

大規模感染予防サービスは、トレンドマイクロ エンタープライズ プロテクション ストラテジーの中核となるサービスです。このサービスでは、新世代の脅威からネットワークを保護するセキュリティの手法が提供されます。

注意： トレンドマイクロ エンタープライズ プロテクション ストラテジーの詳細については、トレンドマイクロ Web サイト (www.trendmicro.co.jp) を参照してください。

大規模感染予防サービスの機能は、次のとおりです。

- 新しい脅威に関するタイムリーな通知
- アウトブレークの状況に関する継続的かつ包括的な報告
- 発生する脅威に応じて用意される、ウイルスから保護するための推奨方法
- 各ウイルスに対応する製品設定 (ポリシー) の迅速な配信

安全な通信インフラストラクチャ

Control Manager では、Secure Socket Layer (SSL) プロトコルを使用して構築された通信インフラストラクチャが使用されます。Control Manager では、使用するセキュリティ設定に応じて、認証を使用してまたは認証を使用せずにメッセージを暗号化できます。

安全な設定とコンポーネントのダウンロード

安全な設定機能を使用することによって、管理コンソールに対するアクセスのセキュリティレベルを設定できます。コンポーネントのダウンロード機能では、次のコンポーネントをダウンロードできます。

- ウイルスパターンファイル
- 検索エンジン

タスク委任

システム管理者は、Control Manager 管理コンソールのユーザに、権限がカスタマイズされた個別のアカウントを与えることができます。ユーザアカウントによって、各ユーザが Control Manager ネットワークで実行可能な表示と処理が定義されます。管理者は、ユーザログを使用して、アカウントの使用状況を追跡できます。

コマンド追跡

コマンド追跡機能を使用すると、Control Manager 管理コンソールを使用して実行されたすべてのコマンドを監視できます。コマンド追跡は、ウイルスパターンファイルのアップデートや配信などの長期にわたるコマンドが Control Manager によって正常に実行されたかどうかの判別に役立ちます。

オンデマンドでのウイルス対策製品管理

Control Manager では、リアルタイムでウイルス対策製品を管理できます。Control Manager ではただちに、あらかじめ定義されているウイルス検索処理を管理化の製品に対して実行し、管理コンソールで行われた設定の変更を対象の管理下の製品に適用します。システム管理者は、管理コンソールから手動検索を実行できます。この機能は、ウイルスのアウトブレーク発生時には不可欠です。

アップデートの集中管理

スパムメール判定ルール、ウイルスパターンファイル、検索エンジンなどのウイルス対策製品およびファイルセキュリティ対策製品のアップデートを集中管理することによって、不正プログラムに対する最新の保護措置をすべての製品に対して講じることができます。1 つの管理コンソールからネットワーク全体の保護ステータスを確認できます。

監視の一元化

監視の一元化によって、ウイルス対策製品およびファイルセキュリティ製品のパフォーマンスの概要を総合的なログとレポートを使用して確認できます。Control Manager によって対象のすべての管理下の製品のログが収集されるため、個々の製品のログを確認する必要はありません。

Control Manager のタスクは、ServerProtect のタスクとは異なります。ServerProtect のタスクは、ユーザによって設定内容が定義され、また、作成後も使用できるように保存されます。Control Manager のタスクは、あらかじめ定義されており、すぐに実行されます。ServerProtect のタスクと Control Manager のタスクは、互いに競合することなく、同時に実行できます。

Control Manager の管理コンソールを使用して、次の Control Manager のタスクを実行することができます。

- ScanNow 開始
- リアルタイム検索開始
- パターンファイル / テンプレートの配信

  このコマンドは、ウイルスパターンファイル、ダメージクリーンナップテンプレート、およびスパイウェアパターンファイルを一緒に配信します。

- エンジンの配信

  このコマンドは、ウイルス検索エンジン、ダメージクリーンナップエンジン、および 32 ビットのルートキット対策ドライバを配信します。

- プログラムファイル配信

  このコマンドは、プログラムファイルを一般サーバに配信します。一般サーバが既にバージョン 5.8 である場合、このコマンドでは何も実行されません。

図 5-1.　[サービス] 画面

[サービス] 画面は、トレンドマイクロ 大規模感染予防サービスとの主要なインタフェースとして、また、大規模感染予防ポリシーを適用する主要な手段としての役割を果たします。

大規模感染予防ポリシー

大規模感染予防ポリシー (OPP) は、アウトブレークコマンダーを使用して ServerProtect に適用できる設定の集まりです。トレンドマイクロでは、発生するウイルスアウトブレークに応じてこのポリシー設定を作成し、大規模感染予防サービスの一環として Control Manager ユーザに提供します。

ネットワークセキュリティを確保するため、このポリシー設定は、アウトブレークの原因に対し特別に作成され、該当製品のみに提供されます。たとえば、メールを感染経路とするウイルスが原因の場合、メッセージングシステム用の設定のみを含むポリシー内容になります。

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。

製品サポート情報

ServerProtect のユーザ登録により、さまざまなサポートサービスを受けることができます。

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

サポートサービスについて

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

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

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

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

製品 Q&A のご案内

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

製品 Q&A

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

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

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

セキュリティ情報

セキュリティ情報の入手先

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

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

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

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

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

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

トレンドマイクロへのウイルス解析依頼

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

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

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

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

```
https://inet.trendmicro.co.jp/esolution/supform.asp
```

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

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

ウイルス解析サポートセンター「TrendLabs」

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

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

付録 A

製品版へのアップグレード

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。

- [ソフトウェア体験版] ダイアログボックス
- シリアル番号リストの確認
- 製品版へのアップグレード

[ソフトウェア体験版] 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 [ソフトウェア体験版] 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。

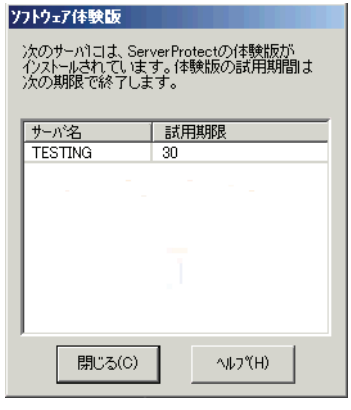


図 A-1.　ソフトウェア体験版

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 [ヘルプ] → [バージョン情報] の順に選択します。[ServerProtect 管理コンソールのバージョン情報] ダイアログボックスが表示されます。

図 A-2.　管理コンソールのバージョン情報

2. [シリアル番号] ボタンをクリックします。[シリアル番号リスト] 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。

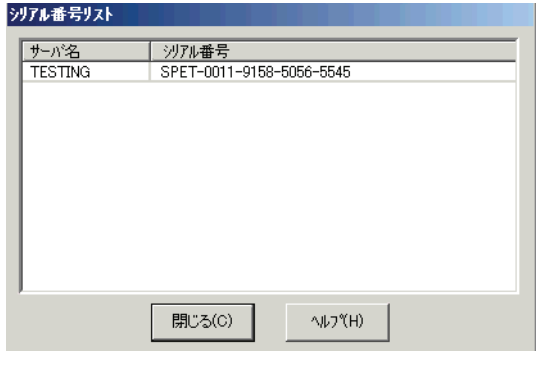


図 A-3.　シリアル番号リスト

3. 確認したら、[閉じる] をクリックします。さらに [OK] をクリックして [ServerProtect 管理コンソールのバージョン情報] 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 [実行] → [製品版へのアップグレード] を選択します。[新しいシリアル番号の入力] ダイアログボックスが表示されます。

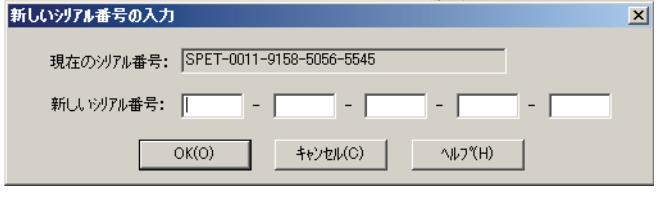


図 A-4.　新しいシリアル番号の入力

3. [新しいシリアル番号] 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] ボタンをクリックして変更内容を保存します。

索引

英数字

あ

か

さ

た

は

ま

や

ら