TREND MICRO

ServerProtect™ for Storage 6.0

クイックスタートガイド

Endpoint Security

※注意事項

トレンドマイクロ（トレンドマイクロ株式会社およびその子会社を含みます）へのお客さま情報の送信について

(1)「Webレピュテーションサービス」、「フィッシング詐欺対策」、「ペアレンタルコントロール/URLフィルタリング」および「Trend ツールバー」等について
①トレンドマイクロでは、お客さまがアクセスしたWebページの安全性の確認のため、お客さまより受領した情報にもとづき、お客さまがアクセスするWebページのセキュリティチェックを実施します。なお、お客さまがアクセスしたURLの情報等(ドメイン、IPアドレス等を含む)は、暗号化してトレンドマイクロのサーバに送信されます。サーバに送信されたURL情報は、Webサイトの安全性の確認、および当該機能の改良の目的にのみ利用されます。
②当該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のでご注意ください。
(a)お客さまがアクセスしたWebページのWebサーバ側の仕様が、お客さま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さまの入力した情報（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、当該Webページのセキュリティチェックが実施されます。
(b)お客さまがアクセスするWebページのセキュリティチェックを実施する仕様になっていることから、お客さまがアクセスするWebサーバ側の仕様によっては、URLのオプション情報に含まれる内容により、お客さまの最初のリクエストと同様の処理が行われます。
③Webサイトのセキュリティ上の判定はトレンドマイクロの独自の基準により行われております。当該機能において判定されたWebサイトのアクセス可否の最終判断につきましては、お客さまにてお願いします。

(2) Trend Micro Smart Protection Network（「スマートフィードバック」、「ファイルレピュテーションサービス」、「脅威情報の送信」および「ウイルスストラッキング」等を含みます）について
脅威に関する情報を収集、分析し保護を強化するために、お客さまのコンピュータに攻撃を試みる脅威に関連すると思われる情報を収集して、トレンドマイクロに送信することがあります。送信された情報はプログラムの安全性の判定や統計のために利用されます。また情報にお客さまの個人情報や機密情報等が意図せず含まれる可能性がありますが、トレンドマイクロがファイルに含まれる個人情報や機密情報自体を収集または利用することはありません。お客さまから収集された情報の取り扱いについての詳細は、<http://jp.trendmicro.com/jp/about/privacy/spn/index.html>をご覧ください。

(3)「迷惑メール対策ツール」について
トレンドマイクロ製品の改良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。

(4)「E-mailレピュテーションサービス」について
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。

(5)「ユーザービヘイビアモニタリング」について
トレンドマイクロ製品の改良目的のために、お客さまがトレンドマイクロ製品をどのような設定にして利用しているのかがわかる設定の情報およびお客さまがトレンドマイクロ製品をどのように操作したのかがわかる操作履歴の情報を、匿名でトレンドマイクロのサーバに送信します。

(6)「製品使用情報の送信」について
お客さまへのサポートサービスの提供、製品の改良および統計的処理のために、ご利用製品のライセンス情報および製品の使用環境情報を、トレンドマイクロのサーバに送信されることがあります。

輸出規制について

お客さまは、本製品およびそれらにおいて使用されている技術（以下「本ソフトウェア等」といいます）が、外国為替および外国貿易法、輸出貿易管理令、外国為替令および省令、ならびに、米国輸出管理規則に基づく輸出規制の対象となる可能性があること、ならびにその他の国における輸出規制対象品目に該当している可能性があることを認識の上、本ソフトウェア等を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しないものとします。
お客さまは、2015年3月現在、米国により定められる禁輸国が、キューバ、イラン、北朝鮮、スーダン、シリアであること、禁輸国に関する情報が、以下のウェブサイトにおいて検索可能であること、ならびに本ソフトウェア等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ることを認識の上、違法行為が行われないよう、適切な手段を講じるものとします。
http://www.treas.gov/offices/enforcement/ofac/
http://www.bis.doc.gov/complianceandenforcement/liststocheck.htm
また、お客さまが本ソフトウェア等を使用する場合、米国により現時点で輸出を禁止されている国の居住者もしくは国民ではないこと、および本ソフトウェア等を受け取ることが禁止されていないことを認識し、お客さまは、本ソフトウェア等を、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するものとします。

複数年契約について

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

著作権について

商標について

P/N: SPEM66779/141120_JP (2015/11)

目次

第 1 章

ServerProtect について

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

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

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

Trend Micro ServerProtect for Storage (以下、ServerProtect for Storage) は、NetApp デバイス、EMC Celerra、VNX/VNXe シリーズ、および ICAP 検索サービスをサポートするストレージデバイスにウイルス対策ソリューションを提供するために開発された ServerProtect の拡張版です。

本章で説明する内容には、次の項目が含まれます。

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) を使用して相手先サーバに接続します。

ServerProtect アーキテクチャ

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

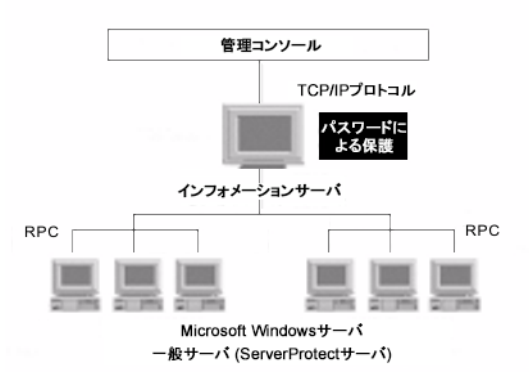


図 1-1. ServerProtect の 3 層アーキテクチャ

管理コンソール

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

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

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

ヒント： 管理コンソールを使用して、1 つまたは複数の一般サーバをリモートでインストールできます。詳細については、51 ページの「一般サーバのインストール」を参照してください。

インフォメーションサーバ

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

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

インフォメーションサーバに関する注意点

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

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

一般サーバ

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

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

- セットアッププログラムからのインストール (詳細については、51 ページの「セットアッププログラムからの一般サーバのインストール」を参照してください)。
- 管理コンソールからのインストール (詳細については、54 ページの「管理コンソールからの一般サーバのインストール」を参照してください)。
- サイレントモードでのインストール (詳細については、56 ページの「サイレントモードでのインストール」を参照してください)。

最適なインストール方法は、インストールする環境に応じて異なります。詳細については、51 ページの「一般サーバのインストール」を参照してください。

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

ServerProtect ドメイン

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

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

ネットワーク保護を管理するための最も効率的な方法は、すべてのサーバを、関連する ServerProtect ドメインにグループ化することです。たとえば、一般サーバを効率的に管理するために、「NS」というドメインを作成することができます。詳細については、71 ページの「ServerProtect ドメインの管理」を参照してください。

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

ServerProtect ドメインには次の機能があります。

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

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

ServerProtect for Storage アーキテクチャの概要

ServerProtect for Storage は、ServerProtect ファミリ製品である ServerProtect for Network Appliance filers と Trend Micro ServerProtect for EMC Celerra（以下、ServerProtect for EMC Celerra）を 1 つに統合します。また、Internet Content Adaptation Protocol（ICAP）を使用したセキュリティをストレージデバイスに提供します。

RPC 検索サービスを実行する ServerProtect for Storage

ここでは、RPC 検索サービスを実行する ServerProtect for Storage の 7-Mode および Cluster-Mode での製品アーキテクチャと、RPC 検索サービスを実行する ServerProtect for Storage の構成フローについて説明します。

7-Mode での製品アーキテクチャ

7-Mode デバイスとは、Data ONTAP 7-Mode で構成されたコンピュータのことを指します。

RPC 検索サービスを実行する ServerProtect for Storage では、「オンアクセス」モードを使用してスキャンサーバ上でウイルス検索が実行されます。インフォメーションサーバによってスキャンサーバが管理されます。

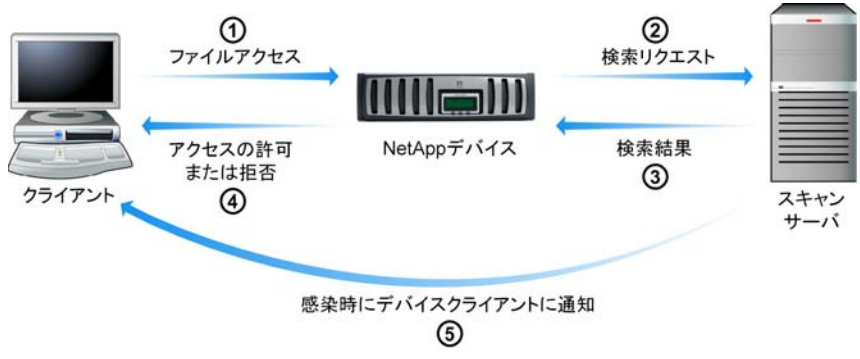


図 1-2. 7-Mode での ServerProtect for Storage の製品アーキテクチャ

クライアントが NetApp 7-Mode デバイス上のファイルにアクセスしようとしたり、NetApp 7-Mode デバイスに新しいファイルを格納しようとしたりすると、NetApp 7-Mode デバイスは ServerProtect に検索要求を出します。ファイル名の拡張子がファイル検索基準に一致すると (.EXE ファイルや .VBS ファイルなど)、NetApp 7-Mode デバイスからスキャンサーバに手動検索リクエスト (ScanNow) が送信されます。検索結果がスキャンサーバから NetApp 7-Mode デバイスに返され、その結果に応じてユーザは、ファイルを開いたり保存したりすることを許可されたり、ファイルへのアクセスを拒否されたりします。

Cluster-Mode での製品アーキテクチャ

Cluster-Mode デバイスとは、Data ONTAP Cluster-Mode で構成されたコンピュータのことを指します。これは C-Mode デバイスとも呼ばれます。Cluster-Mode Antivirus Connector (AV Connector) は、NetApp で提供されるエージェントプログラムであり、Cluster-Mode デバイスを管理するために一般サーバとともにインストールされます。これは、NetApp では Clustered Data ONTAP Antivirus Connector と呼ばれます。

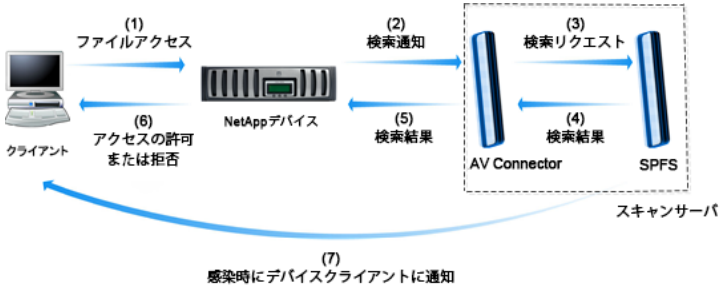


図 1-3. Cluster-Mode での ServerProtect for Storage の製品アーキテクチャ

Cluster-Mode では、クライアントが NetApp Cluster-Mode デバイス上のファイルにアクセスしようとしたり、NetApp Cluster-Mode デバイスに新しいファイルを格納しようとしたりすると、Cluster-Mode デバイスは ServerProtect に検索要求を出します。ファイル名の拡張子がファイル検索基準に一致すると (.EXE ファイルや .VBS ファイルなど)、Cluster-Mode デバイスから Cluster-Mode AV Connector に検索通知が送信されます。Cluster-Mode AV Connector はスキャンサーバに検索リクエスト (ScanNow) を送信します。検索結果がスキャンサーバから Cluster-Mode AV Connector に返され、Cluster-Mode AV Connector から Cluster-Mode デバイスに送信されます。検索結果に応じてユーザは、ファイルを開いたり保存したりすることを許可されたり、ファイルへのアクセスを拒否されたりします。

NetApp デバイスのファイル検索基準および Cluster-Mode を設定する方法については、NetApp デバイスのドキュメントを参照してください。

注意： ウイルスに感染するファイルの種類は限られているため、適切なファイル検索基準を設定することでスキャンサーバのパフォーマンスを最適化できます。これにより、帯域幅の使用を節約して、検索時間を最小限に抑えることができます。ServerProtect for Storage での効率的で安全なファイル検索方法については、33 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。

ファイルがウイルスに感染している場合、ServerProtect for Storage は指定された処理を実行します。検索処理については、118 ページの「一般サーバのウイルス検索」を参照してください。たとえば、ServerProtect for Storage が駆除処理を実行するように設定されており、感染ファイルが駆除可能である場合は、次が実行されます。

1. スキャンサーバが感染ファイルの駆除処理を実行し、ウイルスが駆除されたことを NetApp デバイスに通知します。
2. NetApp デバイスは、ウイルス駆除されたファイルへのアクセスをクライアントに許可し、元のファイルとウイルス駆除されたファイルを置き換えます。

注意： NetApp デバイスは、登録されたスキャンサーバを「信頼」しています。そのため、一般サーバ (ファイルサーバやデータサーバ) としても機能しているスキャンサーバからファイルを受信しても、NetApp デバイスではそのファイルの検索をリクエストしません。NetApp デバイスと一般サーバの両方を保護するには、ServerProtect のリアルタイム検索を「入出力ファイル」に設定してください。リアルタイム検索の「入出力ファイル」への設定方法については、125 ページの「検索の設定」を参照してください。

構成の概要

ここでは、ServerProtect for Storage の 7-Mode での構成フローについて説明します。

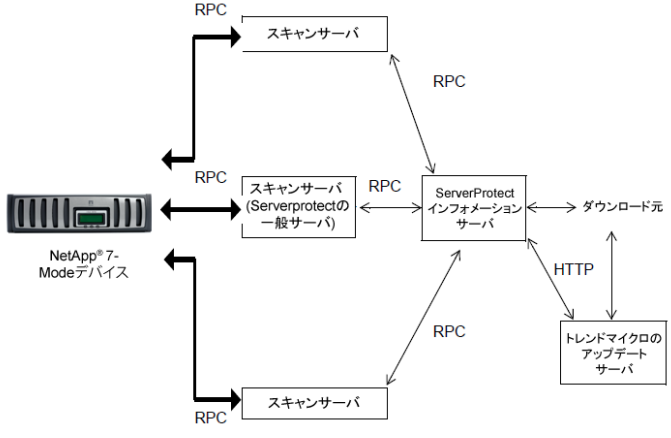


図 1-4.　ServerProtect for Storage の 7-Mode での構成フロー

ServerProtect for Storage は、RPC (リモートプロシージャコール) 経由で NetApp 7-Mode デバイスと通信するエージェントを使用します。このエージェントは次の機能を実行します。

- 一般サーバを「スキャンサーバ」として NetApp 7-Mode デバイスに登録します。これにより、スキャンサーバの可用性と場所を NetApp 7-Mode デバイスに通知します。
- NetApp 7-Mode デバイスのファイル検索リクエストを監視します。
- 検索結果を NetApp 7-Mode デバイスに返します。
- NetApp 7-Mode デバイスからのクエリに回答します。
- パターンファイルや検索エンジンのアップデートについて NetApp 7-Mode デバイスに通知します。
- NetApp 7-Mode デバイスと通信して、スキャンサーバと NetApp 7-Mode デバイスとの間の接続状態を確認します。

Cluster-Mode の構成フローは 7-Mode と同様です。ただし、ServerProtect for Storage が NetApp 7-Mode デバイスではなく、NetApp Cluster AV Connector と通信します。

注意： NetApp 向けの ServerProtect for Storage の問い合わせ先および技術サポート提供は販売店となります。詳しくは、製品ページをご覧ください。
http://www.go-tm.jp/spfs

EMC CAVA 検索サービスを実行する ServerProtect for Storage

EMC VNX/VNXe ウイルス対策システムの主なコンポーネントを次に示します。

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

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

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

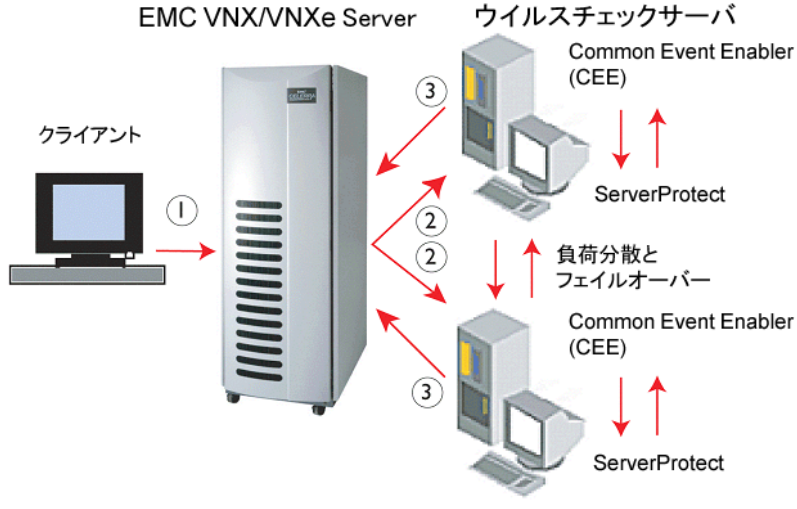


図 1-5.　EMC CAVA 検索サービスを実行する ServerProtect for Storage のアーキテクチャ

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

1. Windows クライアントを実行するユーザやアプリケーションは、CIFS (Common Internet File System) プロトコルを使用して、EMC VNX/VNXe からファイルにアクセスします。
2. クライアントがファイルを変更しようとしたり、ファイルを閉じようとしたり、EMC VNX/VNXe システムにファイルを格納しようとすると、EMC VNX/VNXe File Server からリクエストが発行されます。
3. File Server 上の VC クライアントは、AV サーバの CEE に UNC (Universal Naming Convention) パス名を送信することでウイルスチェックを要求します。
4. リクエストはラウンドロビン方式で AV サーバに送信されます。
5. AV サーバでは、CEE が ServerProtect に対して、リアルタイム検索機能を使用してファイルのウイルスを検索するように要求します。

6. 検索結果は、次のように単純化して表示されます。
   - 感染なし : ファイルがウイルスに感染していないか、ウイルスは駆除されました (ファイルを開くことができます)。
   - 感染 : ファイルがウイルスに感染していて、駆除できません (ファイルへのアクセスは拒否されます)。

EMC VNX/VNXe の保護は、ServerProtect for Storage の主な機能です。ServerProtect for Storage では、ウイルス検索が「オンアクセス」モードで実施され、Windows Server 2008 および Windows Server 2012 が稼働する個別のコンピュータ (AV サーバ) 上で実行されます。この AV サーバが File Server を保護します。これが、一般サーバの保護を目的とする ServerProtect の通常のバージョンとは異なる点です。

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

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

構成の概要

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

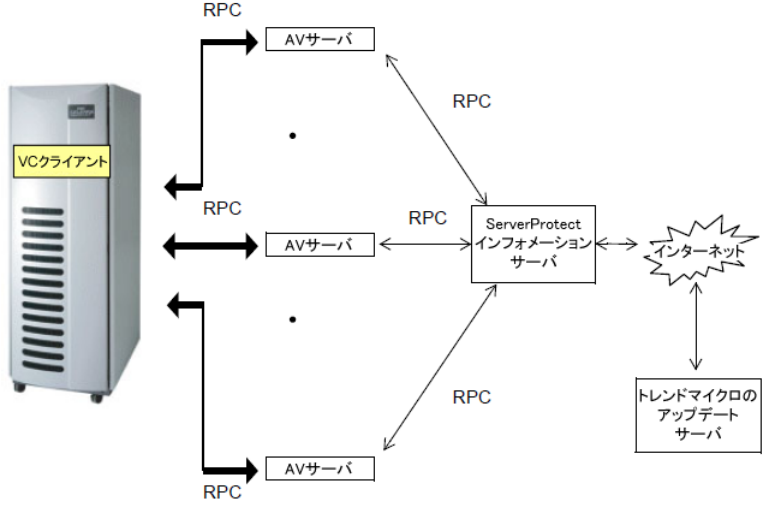


図 1-6. ServerProtect for Storage 構成フロー

ServerProtect は次の機能を実行します。

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

EMC VNX/VNXe の特別な機能

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

この設定は変更しないことを強くお勧めします。リアルタイム検索の詳細については、125 ページの「リアルタイム検索」を参照してください。ファイルがウイルスに感染している場合、事前に設定された内容に応じて、AV サーバは次のいずれかの処理を実行します。

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

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

ICAP 検索サービスを実行する ServerProtect for Storage

ServerProtect for Storage では、Internet Content Adaptation Protocol (ICAP) を使用して、ストレージデバイスと ICAP 検索サービス間の通信を行います。ここでは、ServerProtect for Storage での ICAP 検索サービスのワークフローについて説明します。

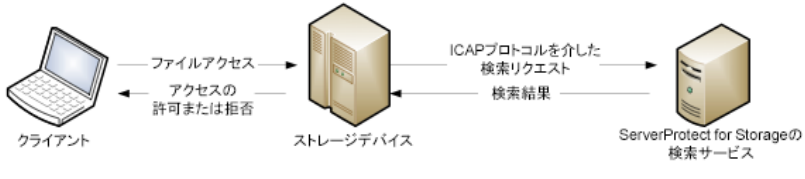


図 1-7. ServerProtect での ICAP 検索サービスのワークフロー

クライアントがストレージデバイス内のファイルにアクセスしようとすると、ストレージデバイスは ICAP を介して ServerProtect に検索リクエストを送信します。ServerProtect はファイルのウイルスを検索し、検索結果に応じて、ファイルへのアクセスを許可または拒否します。

感染したファイルに対する処理

ServerProtect for Storage の ICAP 検索サービスは、次の検索処理を実行します。

- **ウイルス駆除** : ICAP 検索サービスは感染ファイルを駆除して、駆除済みのファイルをストレージデバイスに戻します。
- **ブロック** : 感染ファイルを駆除できない場合、ICAP 検索サービスは感染ファイルをストレージデバイスに戻さず、ファイルを駆除できないことをストレージデバイスに通知します。

配信

ServerProtect for Storage を使用すると、複数のストレージデバイスに複数のスキャンサーバを配信できるようになります。ServerProtect for Storage の ICAP 検索サービスでは、複数のストレージデバイスからのリクエストを処理できます。同様に、ストレージデバイスは、複数の ServerProtect for Storage ICAP 検索サービスに検索リクエストを送信できます。

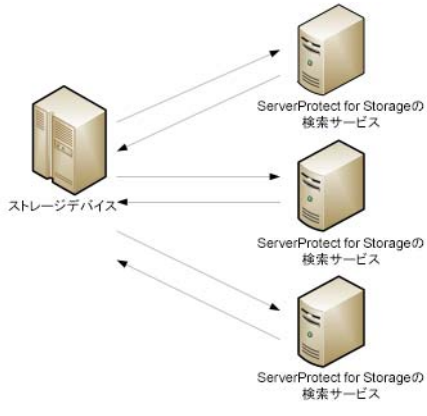


図 1-8. ストレージデバイスから複数の ServerProtect ICAP 検索サービスに検索リクエストを送信可能

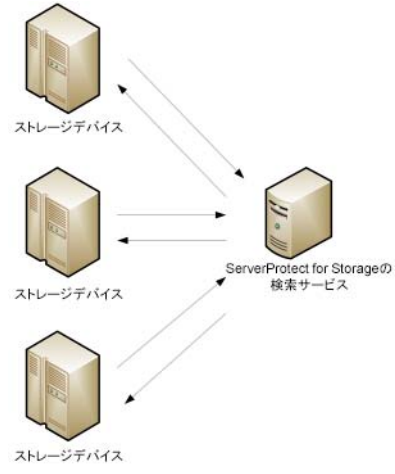


図 1-9. ServerProtect ICAP 検索サービスで複数のストレージデバイスからの検索リクエストを処理可能

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、125 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、128 ページの「手動検索 (ScanNow)」を参照してください。

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

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

- **相互補完** : ウイルスを含むファイルが誤ってダウンロード、またはコピーされようとした場合、リアルタイム検索によってウイルスが検出されます。何らかの理由でリアルタイム検索が停止されていた場合は、手動検索 (ScanNow) を実行することにより、ウイルスを検出することができます。
- **効率的なファイル検索** : 特定のファイルタイプが検索対象になるように設定し、システムリソースへの影響を最小限に抑えることができます。詳細については、118 ページの「一般サーバのウイルス検索」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、118 ページの「一般サーバのウイルス検索」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、101 ページの「タスクの管理」を参照してください。

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

ウイルスを検出した場合

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

処理には、次の 5 種類があります。

- **放置 (手動処理)**: 手動検索で、処理を実行せずファイルをそのままにします。ただしウイルスが検出されたことはログエントリとして記録されます。リアルタイム検索では、検索対象が「出力ファイル」または「入出力ファイル」の場合、ServerProtect は検出されたファイルを「書込み禁止」として扱い、ファイルの複製や変更ができないようにします。詳細については、119 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** : 感染したファイルの拡張子を .vir に変更してファイル名を変更します。これによりファイルが実行されたり、開かれたりしないようにします。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、ファイルのバックアップコピーを自動的に作成しておくことをお勧めします。

  ICAP 検索サービスで感染ファイルを駆除すると、駆除したファイルがストレージデバイスに戻されます。
- **ブロック (ICAP 検索サービスのみ)**: 感染ファイルを駆除できない場合、ICAP 検索サービスは感染ファイルをストレージデバイスに戻さず、ファイルを駆除できないことをストレージデバイスに通知します。

ウイルスに関するすべてのイベントと処理については、ログファイルに記録されます。詳細については、119 ページの「ウイルスに対する処理の設定」、またはオンラインヘルプの「ログ情報の表示」トピックを参照してください。

注意 : [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。

注意： ServerProtect for Storage の ICAP 検索サービスは、感染ファイルに対して駆除とブロックの処理のみを実行します。

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

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

アップデート / 配信

ServerProtect は、最新版のコンポーネント (パターンファイル、検索エンジン、プログラム) をダウンロード / 配信するためのアップデート機能を実装しています。日々増え続ける新種ウイルスに対応し、効果的なウイルス対策を実施するには、最新のウイルスパターンファイルおよび検索エンジンを使用することが重要です。ServerProtect ではウイルス対策に不可欠なアップデートを簡単に実行できます。詳細については、89 ページの「アップデートの設定」を参照してください。

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

ServerProtect のアップデート機能には、次の特長があります。

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

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

1. トレンドマイクロのアップデートサーバからアップデートファイルをダウンロードします。詳細については、92 ページの「アップデートファイルのダウンロード」を参照してください。
2. ダウンロードしたアップデートファイルをネットワーク上の一般サーバへ配信します。詳細については、97 ページの「アップデートファイルの配信」を参照してください。

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

ヒント： 予約アップデートタスクを作成することで、アップデートを自動化することができます。詳細については、103 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、118 ページの「一般サーバのウイルス検索」を参照してください。

注意： 日々増え続ける新種ウイルスに対応し、効果的なウイルス対策を実施するため、パターンファイルは常に最新版をお使いください。トレンドマイクロでは、予約アップデートをサポートすることによって、パターンファイルのアップデートを容易にしています。詳細については、99 ページの「予約配信の設定」を参照してください。

MacroTrap

マクロウイルスはオペレーティングシステムではなく、アプリケーションに依存します。そのため MS-DOS、Windows、Macintosh、OS/2 と、使用環境を問わずに感染を拡大します。ServerProtect では、トレンドマイクロの MacroTrap 技術を採用し、マクロウイルスの脅威からネットワークユーザを守ります。MacroTrap の設定の詳細については、125 ページの「検索の設定」を参照してください。

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

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

圧縮ファイル

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

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

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

- LZEXE (.exe)
- DIET (.com)
- UNIX PACKED (.z)
- UNIX COMPACKED (.z)
- UNIX LZW (.Z)
- UUENCODE
- BINHEX
- BASE64

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、125 ページの「検索の設定」を参照してください。

ダメージクリーンナップサービス

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

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

OLE 埋め込みの検索

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

OLE には多くの利点がありますが、ウイルス感染の危険性も無視できません。ServerProtect では、トレンドマイクロのウイルス検索技術により OLE 埋め込みオブジェクトを検索対象とすることができます。詳細については、118 ページの「一般サーバのウイルス検索」を参照してください。

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

トレンドマイクロの推奨設定

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

.zip ファイル、.exe ファイルなどの実行ファイルの場合、ファイルタイプはファイルコンテンツによって判断されます。実行ファイルでない .txt ファイルなどの場合、ファイルタイプはファイルのヘッダによって判断されます。詳細については、118 ページの「一般サーバのウイルス検索」を参照してください。

トレンドマイクロの推奨設定を使用すると、たとえば次のような利点があります。

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

トレンドマイクロの推奨処理

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

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

トレンドマイクロの推奨処理を使用した場合、次のような利点があります。

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

トレンドマイクロの推奨処理の設定については、119 ページの「ウイルスに対する処理の設定」を参照してください。

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

その他の機能

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

集中管理

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

インストール時のネットワークセキュリティ

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

ウイルスアウトブレークへの迅速な対応

ServerProtect によって保護されているサーバの共有フォルダにウイルスの侵入が試みられた場合、ネットワーク上の感染源のコンピュータを特定するメッセージボックスが表示されます。このメッセージボックスの情報には、検索の種類、ウイルスの名前、感染したファイルの名前、関連するコンピュータの名前または ID、およびユーザ名なども含まれます。また、検出されたウイルスに対する処理、および感染元についても表示されます。詳細については、112 ページの「通知メッセージの設定」を参照してください。

感染ファイルに対する柔軟な処理

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

最新のウイルス検索技術

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

ウイルス検索の統計

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

互換性

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

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

第 2 章

ServerProtect for Storage のインストール

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

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

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

システム要件

最新の情報については、次の Web サイトを参照してください。

http://www.trendmicro.co.jp/jp/business/products/spfs/index.html#requirement

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

インストール計画

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

ServerProtect では Microsoft Windows プラットフォームがサポートされます。ServerProtect をネットワークに初めてインストールする場合は、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し、その管理下に一般サーバを設定してください。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。詳細については、13 ページの「ServerProtect ドメイン」を参照してください。

注意： 異なる拠点に多数のサーバを配置している場合は、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。詳細については、12 ページの「インフォメーションサーバに関する注意点」を参照してください。

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

表 2-1.　Microsoft Windows 環境でのインストール

OS	インフォメーションサーバ	一般サーバ	管理コンソール
Windows Server 2008 ファミリ　(32 ビット)	○	○	○
Windows Server 2008 ファミリ　(64 ビット)	○ (WOW64)	○	○ (WOW64)
Windows Server 2012 ファミリ	○	○	○
Windows 2012 Server R2 ファミリ	○ (WOW64)	○	○ (WOW64)
Windows Vista デスクトップファミリ	×	×	○
Windows 7 デスクトップファミリ	×	×	○
Windows 8 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 Storage Server の各エディションを指します。

Server 2012 ファミリとは、Foundation、Essentials、Standard、および Datacenter の各エディションを指します。

Windows Vista デスクトップファミリとは、Business、Enterprise、および Ultimate の各エディションを指します。

Windows 7 デスクトップファミリとは、Professional、Enterprise、および Ultimate の各エディションを指します。

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

Windows Server2008 R2 ファミリとは、Standard、Enterprise、および Datacenter Server の各エディションを指します。

Windows Server 2012 ファミリおよび Windows 2012 Server R2 ファミリとは、Standard、Essentials、Foundation、Storage、および Datacenter Server の各エディションを指します。

注意： Hyper-V は、Windows Server 2008 (64 ビット) および Windows Server 2012 でサポートされます。

ServerProtect コンポーネントによって使用されるポート番号

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

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

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

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

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

インフォメーションサーバによって使用されるポート番号

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

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

- 5005 番 (TCP) もしくは、5006 ～ 5014 番の間の空いているポートいずれか
- 3000 番 (UDP) もしくは、3001 ～ 3009 番の間の空いているポートいずれか
- 137 番 (UDP) (名前付きパイププロトコル経由の RPC を使用する場合)
- 138 番 (UDP) (名前付きパイププロトコル経由の RPC を使用する場合)
- 139 番 (TCP) (名前付きパイププロトコル経由の RPC を使用する場合)

- 445 番 (TCP) (名前付きパイププロトコル経由の RPC を使用する場合)
- 3628 番 (TCP) (イベントメッセージの受信用)

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

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

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

WAN 接続のネットワーク

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

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

ServerProtect のインストール

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

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 38 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 を挿入して 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。

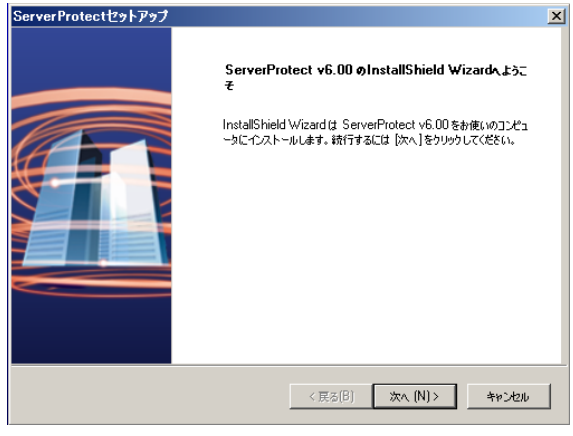


図 2-1.　ServerProtect セットアップの初期画面

2. [次へ] をクリックします。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。

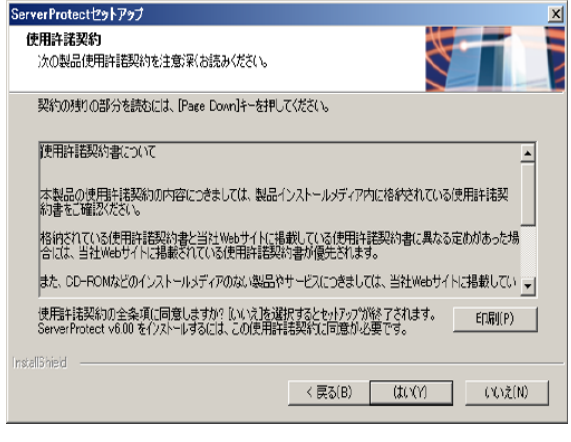


図 2-2.　使用許諾契約書

3. [はい] をクリックします。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。

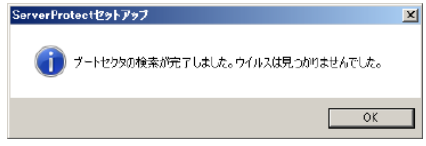


図 2-3.　ウイルス検索の結果

4. [OK] をクリックしてセットアップを続行します。[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

5. ユーザ情報および製品のシリアル番号を入力します。

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

6. [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

7. ServerProtect for Storage の完全なパッケージをインストールするには、すべてのチェックボックスをオンにします。

注意： 一般サーバをインストールする場合は、インストールする検索サービスの種類も選択する必要があります。EMC VNX/VNXe を保護する場合は、[EMC CAVA] を選択します。RPC を使用して NetApp デバイスを保護する場合は、[RPC] を選択します。ICAP をサポートするストレージデバイスを保護する場合は、[ICAP] 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
```

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

---

8. ポップアップダイアログで [はい] をクリックして、一般サーバのインストールを続行します。
9. 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を入力し、[次へ] をクリックしてください。

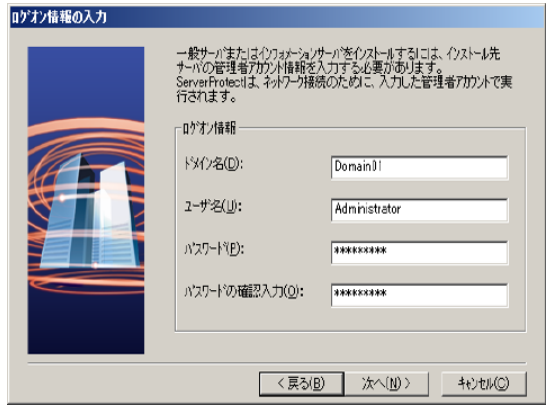


図 2-6.　ログオン情報の入力

10. 次の各項の指示に従ってインストールを完了します。

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] 画面で、[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。詳細については、45 ページの「コンポーネントの選択」を参照してください。

3. インフォメーションサーバのインストール先のサーバ / フォルダを指定するには、[参照] ボタンをクリックします。[ServerProtect インストール先の選択] 画面が表示されます。

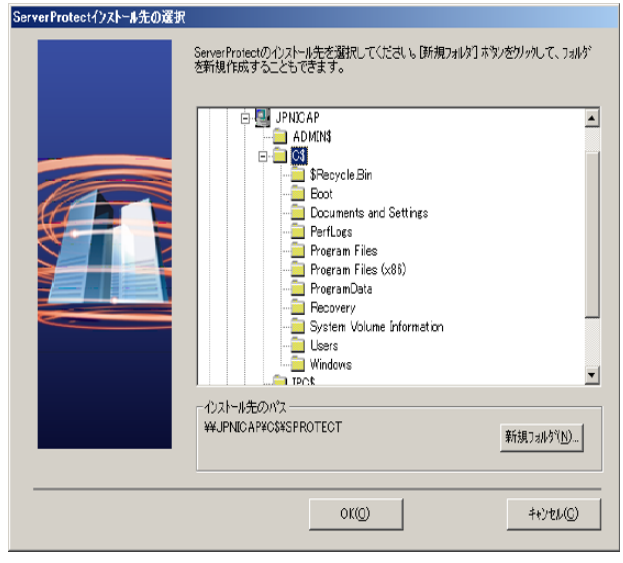


図 2-7. ServerProtect インストール先の選択

4. サーバツリーから対象サーバをダブルクリックし、ServerProtect インフォメーションサーバファイルのインストールパスを選択します。新しいフォルダにインストールしたい場合は、[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] 画面に戻ります (詳細については、45 ページの「コンポーネントの選択」を参照してください)。

5. [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] 画面が表示されます。

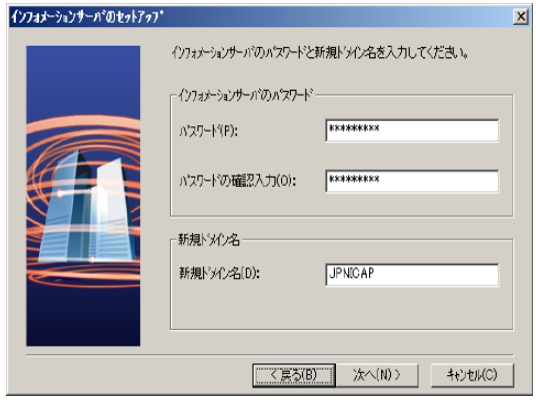


図 2-8.　インフォメーションサーバのセットアップ

6. インフォメーションサーバのパスワードを入力し、要求に応じてパスワードを確認します。このパスワードによって、管理コンソールからインフォメーションサーバへ接続しようとする場合に、不正なアクセスを防止することができます。
7. [次へ] をクリックします。[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。

8. 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。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。

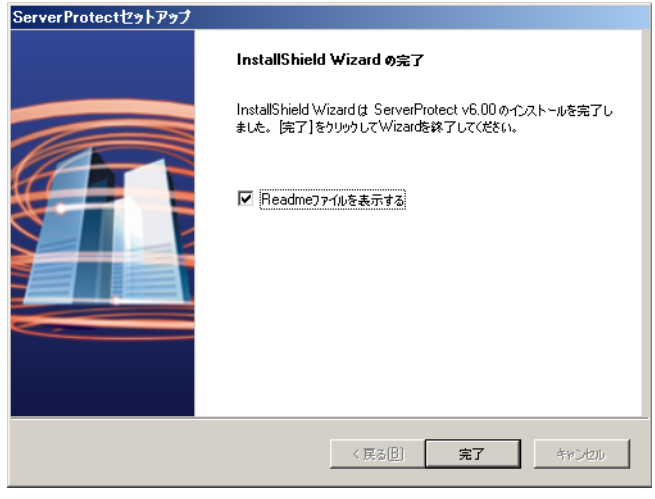


図 2-9.　セットアップの完了

9. [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。

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 2-5 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 環境にインストールする必要があります。

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

3. Windows の [スタート] メニューに自分がログオンした場合にのみ ServerProtect プログラムを表示する場合は、[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。
5. [次へ] をクリックします。プログラムフォルダを選択するための画面が表示されます。
6. プログラムのインストール先のフォルダを選択し、[次へ] をクリックします。

   [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。
7. 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。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。

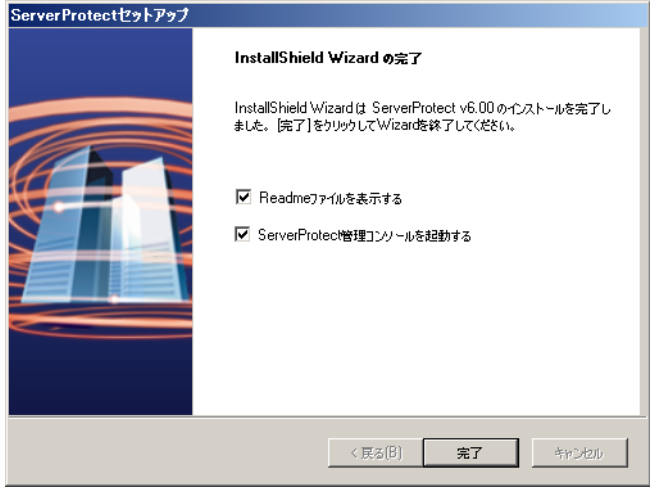


図 2-10. セットアップの完了

8. [完了] をクリックしてセットアップを終了します。インフォメーションサーバを選択するための画面が表示されます。

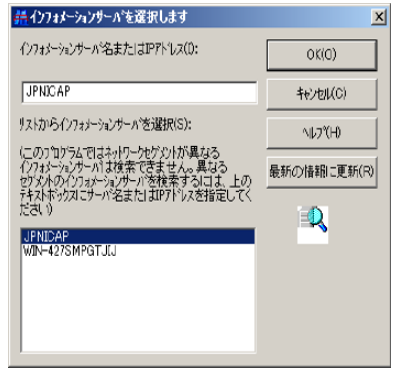


図 2-11. インフォメーションサーバ選択

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

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

10. [OK] をクリックして変更内容を保存します。

一般サーバのインストール

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

セットアッププログラムからの一般サーバのインストール

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

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

1. セットアッププログラムを起動し、前述の各コンポーネント共通の手順を実行します。
2. [コンポーネントの選択] 画面で [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て、インストールする検索サービスの種類を選択します。詳細については、45 ページの「コンポーネントの選択」を参照してください。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。[ServerProtect インストール先の選択] 画面が表示されます。

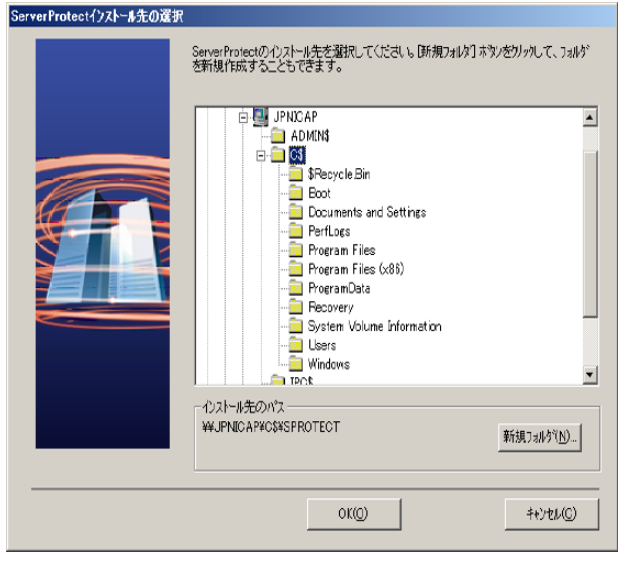


図 2-12. Windows Server でのインストール先の選択

3. 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。
4. 対象サーバをダブルクリックします。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。
5. 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。
6. [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 [次へ] ボタンをクリックします。[ログオン情報の入力] 画面が表示されます。
7. 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。

8. [次へ] をクリックします。[インフォメーションサーバの選択] 画面が表示されます。

図 2-13. [インフォメーションサーバの選択] 画面

9. 次のいずれかの操作を実行してインフォメーションサーバを指定します。
   - 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] 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。

---

10. [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。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。

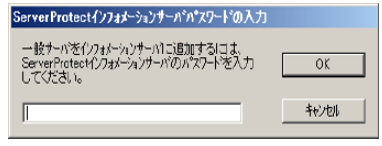


図 2-14. ServerProtect インフォメーションサーバパスワードの入力

11. 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。[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。

12. 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。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を示す画面が表示されます (図 2-10 参照)。

13. [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。

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

1. ドメインブラウザツリーから、サーバの追加先ドメインを選択します。次のいずれかの操作を実行してください。
   - メインメニューから [ドメイン] → [SPFS 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、[SPFS の新規インストール] を選択します。
2. 既存の一般サーバ (実行元サーバ) およびインストールする検索サービスの種類をリストから選択し、[OK] をクリックします。

   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] 画面が表示されます。
4. 次のいずれかの操作を実行して、ドメインに追加するサーバを選択します。
   - 左のリストボックスでサーバ名を選択します。
   - [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] 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画面を閉じるには、[キャンセル] をクリックします。

サイレントモードでのインストール

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

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

1. インフォメーションサーバをインストールします。詳細については、46 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. 初期設定のインストールパスで SMS フォルダを検索し、共有します。

   注意： 読み取り権限と書き込み権限を付与して SMS フォルダを共有します。

   インストール先のサーバからこのフォルダにアクセス可能であることを確認してください。複数のサイレントインストールを実行したい場合、インストール先のサーバ上で SMS フォルダを割り当てます。
3. インストール先のサーバで、SMS フォルダ、またはそのフォルダにマップされているドライブに移動して Setup.ini ファイルを開き、次のいずれかの行をファイルの最後に追加して検索サービスの種類を指定します。
   - 一般サーバを RPC 検索サービスとしてインストールする場合 :

     ```
     [CommonSection]
     NormalServerType=1
     ```
   - 一般サーバを ICAP 検索サービスとしてインストールする場合 :

     ```
     [CommonSection]
     NormalServerType=2
     ```
   - 一般サーバを EMC CAVA 検索サービスとしてインストールする場合 :

     ```
     [CommonSection]
     NormalServerType=4
     ```

   注意： Setup.ini で NormalServerType が指定されていない場合、一般サーバは初期設定で EMC CAVA 検索サービスとしてインストールされます。
4. 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"SPFS"`

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"SPFS"
```

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。

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、ServerProtect を D:¥Utility¥AntiVirus¥SProtect というパスにインストールするには、次の手順を実行します。

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

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

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

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

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

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

インフォメーションサーバ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。

RPC 検索サービスまたは ICAP 検索サービスを実行する ServerProtect for Storage のインストール

ここでは、RPC 検索サービスまたは ICAP 検索サービスを実行する ServerProtect for Storage のインストールプロセスについて説明します。

インストールするには、次の手順を実行します。

1. インフォメーションサーバをインストールします。詳細については、46 ページの「インフォメーションサーバのインストール」を参照してください。
2. 一般サーバをインストールします。詳細については、51 ページの「セットアッププログラムからの一般サーバのインストール」を参照してください。
3. 管理コンソールをインストールします。詳細については、49 ページの「管理コンソールのインストール」を参照してください。ネットワーク内の他の Windows コンピュータまたはデスクトップ システム コンピュータに、管理コンソールを追加インストールすることもできます。

   ヒント： インフォメーションサーバを管理することができるのは、1 つの管理コンソールからのみです。

4. パターンファイルおよび検索エンジンを最新版にアップデートします。詳細については、92 ページの「アップデートファイルのダウンロード」と 89 ページの「アップデートの設定」を参照してください。
5. 複数の一般サーバを管理するための ServerProtect ドメインを作成します。詳細については、71 ページの「ServerProtect ドメインの新規作成」を参照してください。
6. 管理コンソールを使用して、他の一般サーバを追加インストールします (詳細については、54 ページの「管理コンソールからの一般サーバのインストール」を参照してください)。

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

EMC CAVA 検索サービスを実行する ServerProtect for Storage のインストール

ここでは、EMC CAVA 検索サービスを実行する ServerProtect for Storage のインストールプロセスについて説明します。

EMC CAVA 検索サービスを実行する ServerProtect for Storage のインストールを開始する前に

EMC CAVA 検索サービスを実行する ServerProtect for Storage の機能を正しく動作させるには、EMC CAVA 検索サービスを実行する ServerProtect for Storage のインストールを開始する前に、次のインストール前作業を順番に実行することが重要です。

1. AV ユーザアカウントと AV グループを Windows ドメインサーバで設定する。詳細については、EMC 社から提供されている CEE のマニュアルを参照してください。
2. ServerProtect 一般サーバをインストールする各サーバに、EMC Common Event Enabler (CEE) (Common Anti-Virus Agent (CAVA) とも呼ばれる) をインストールする。詳細については、EMC 社から提供されている CEE のマニュアルを参照してください。

EMC CAVA 検索サービスを実行する ServerProtect for Storage のインストール

ServerProtect 一般サーバをインストールする Windows Server 上に CEE または VEE がインストールされていることを確認します。ServerProtect for Storage 一般サーバは、EMC ウイルス対策システムの一部です。

インストールするには、次の手順を実行します。

1. Common Event Enabler (CEE) がインストールされていることを確認します。
2. 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、46 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。
3. 一般サーバをインストールします。詳細については、51 ページの「セットアッププログラムからの一般サーバのインストール」を参照してください。
4. 管理コンソールをインストールします。詳細については、49 ページの「管理コンソールのインストール」を参照してください。ネットワーク内の他の Windows コンピュータまたはデスクトップ システム コンピュータに、管理コンソールを追加インストールすることもできます。

ヒント： インフォメーションサーバを管理することができるのは、1 つの管理コンソールからのみです。

5. パターンファイルおよび検索エンジンを最新版にアップデートします。詳細については、92 ページの「アップデートファイルのダウンロード」と 89 ページの「アップデートの設定」を参照してください。
6. 複数の一般サーバを管理するための ServerProtect ドメインを作成します。詳細については、71 ページの「ServerProtect ドメインの新規作成」を参照してください。
7. 管理コンソールを使用して、他の一般サーバを追加インストールします (詳細については、54 ページの「管理コンソールからの一般サーバのインストール」を参照してください)。

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

ServerProtect のアンインストール

一般サーバのアンインストール

一般サーバをアンインストールする方法は 2 種類あります。

一般サーバをリモートでアンインストールするには

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

一般サーバをローカルでアンインストールするには

1. Windows の [コントロールパネル] → [プログラムと機能] を選択します。
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 [コントロールパネル] → [プログラムと機能] 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 [コントロールパネル] → [プログラムと機能] を選択します。
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、次の登録が必要です。

- プログラム管理コンソールからの製品版の登録

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

製品版の登録

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

1. ドメインブラウザツリーでサーバを選択します。
2. メインメニューから [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。

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。

- 139 ページの「ICAP 検索サービスの使用」
- 142 ページの「検索対象ファイルの種類 (拡張子) の選択」
- 145 ページの「Control Manager への登録」

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 Micro ServerProtect 管理コンソール] → [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。

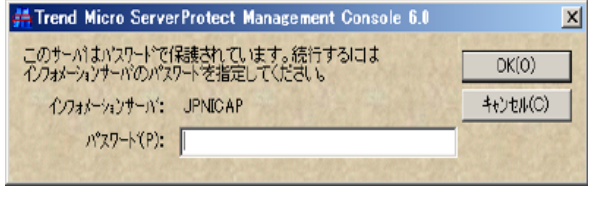


図 3-1. インフォメーションサーバへのログオン

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。

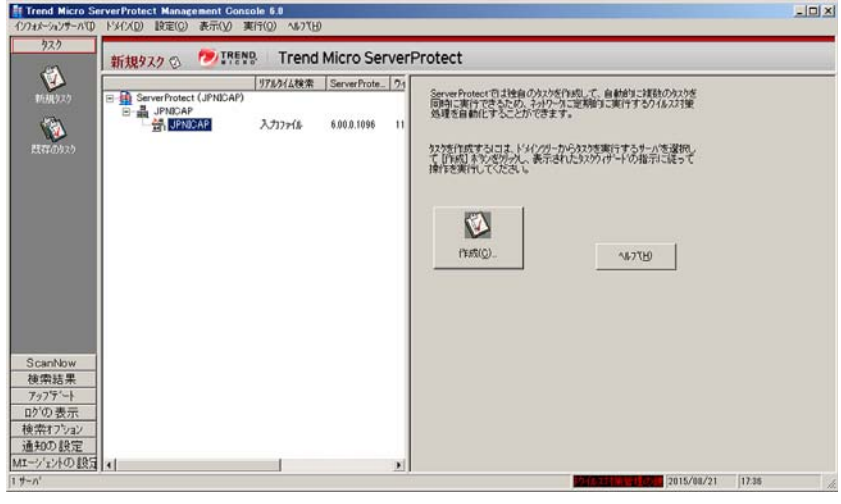


図 3-2.　管理コンソールのメイン画面構成

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

メインメニュー

画面上部のメインメニューには、次の項目が表示されます。

- [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設定を行います。たとえば、インフォメーションサーバのバックアップや復元、ネットワーク上のインフォメーションサーバの移動です。
- [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] / [既存のタスク] : タスクの作成または修正を実行します。
  - [ScanNow] : 手動検索 (ScanNow) を実行します。
  - [アップデート] / [ロールバック] : コンポーネントのアップデートまたはロールバックを実行します。
  - [Control Manager (CM) エージェントの設定]: Trend Micro Control Manager (以下、Control Manager) の設定を登録、登録解除、および実行します。
  - [製品版へのアップグレード] : 新しいシリアル番号を入力し、期限が切れたシリアル番号を更新します。
  - [パスワードの変更] : インフォメーションサーバのパスワードを変更します。
  - [ドメインの検索] : ドメインまたはサーバを検索します。
  - [STOP マークのサーバに接続] : 一般サーバが実行されており、1 台のインフォメーションサーバにより管理されているが、管理コンソールに STOP が表示されている場合に使用します。
  - [デバッグ情報の作成] : 詳細なデバッグ情報が含まれるログファイルを管理し、それをトレンドマイクロのテクニカルサポートへ送信します。
- [ヘルプ] : ヘルプシステムを開いたり、ServerProtect の製品情報を表示します。

サイドバー

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

[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、または削除します。

[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] : リアルタイム検索および EMC CAVA 検索サービスの結果を表示します。

 [ストレージ検索サービス] : RPC 検索サービスおよび ICAP 検索サービスの結果を表示します。

 [ScanNow] : 手動検索結果を表示します。

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

 [ロールバック] : 以前の配信内容にロールバックします。

[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] : リアルタイム検索を設定します。

 [ストレージ検索サービス] : ストレージ検索サービスによるウイルス検索を設定します。

 [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。

[Control Manager エージェントの設定] グループ

 [Control Manager エージェントの設定] : Control Manager での登録または登録解除の際に Control Manager を設定します。

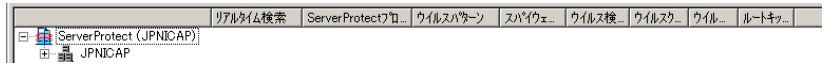
ドメインブラウザツリー

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

- ヘッダ
- インフォメーションサーバ
- ドメイン
- 一般サーバ

ヘッダ

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



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

インフォメーションサーバ

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

 インフォメーションサーバ

ドメイン

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

 ServerProtect ドメイン

 ウイルスに感染した一般サーバを含む ServerProtect ドメイン

一般サーバ

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

32 ビット Microsoft Windows Server タイプの一般サーバ

64 ビット Microsoft Windows Server タイプの一般サーバ

ウイルスに感染した 32 ビット Microsoft Windows Server タイプの一般サーバ

ウイルスに感染した 64 ビット Microsoft Windows Server タイプの一般サーバ

接続が切断、またはサービスが無効にされた一般サーバ

設定データ領域

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

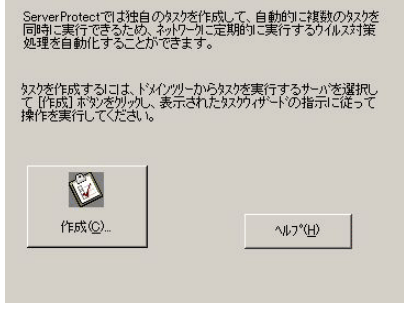


図 3-3.　設定データ領域

ServerProtect ドメインの管理

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

注意： あるドメイン内のサーバの 1 つでウイルスが検出されると、ドメインアイコンが変化します。これは、ウイルスがネットワーク全体に広がることを阻止するための警告です。変化したアイコンを削除するには、管理コンソールの [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 文字まで使用することができます。全角文字は使用することができません。ドメイン名には半角英数字で 50 文字まで、中国語、日本語、または韓国語などの全角文字では 25 文字まで使用できます。

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。

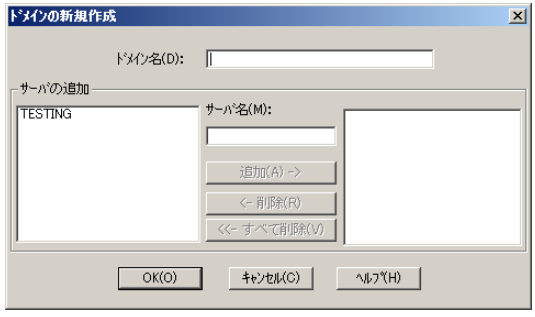


図 3-4.　[ドメインの新規作成] ダイアログボックス

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. ドメインに追加するサーバを識別します。次のいずれかの操作を実行してください。
   - 画面の左のリストからサーバを選択します。
   - [サーバ名] フィールドにサーバ名を入力します。
4. [追加] 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。

[ドメイン名の変更] ダイアログボックスが表示されます。

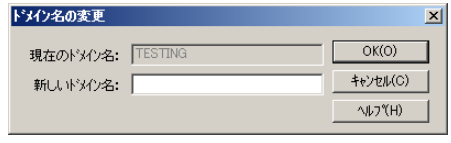


図 3-5.　[ドメイン名の変更] ダイアログボックス

3. 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、71 ページの「ServerProtect ドメインの新規作成」を参照してください。

インフォメーションサーバの管理

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

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

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

インフォメーションサーバの選択

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

インフォメーションサーバを選択するには

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

   コンピュータに複数のネットワークインタフェースカード (NIC) がインストールされている場合、プライマリ NIC に接続されているインフォメーションサーバのみがリストボックスダイア

ログに表示されます。リストのサーバ表示を更新するには、[最新の情報に更新] ボタンをクリックします。

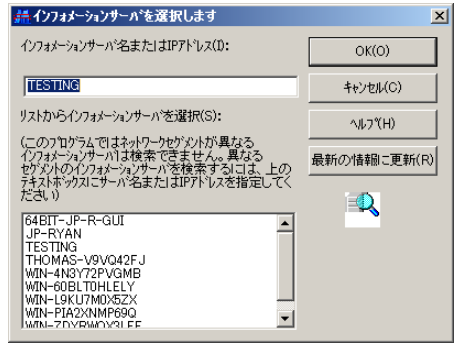


図 3-6.　インフォメーションサーバの選択

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 ServerProtect 一般サーバを ServerProtect 6.0 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] 画面が表示されます。
2. 移動先のインフォメーションサーバを選択し、[OK] をクリックして送信します。[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。
3. [ユーザ名] および [パスワード] に値を入力し、[OK] をクリックします。
4. [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。
5. 移動先のインフォメーションサーバを選択し、[OK] をクリックします。
6. 移動の確認を求めるダイアログボックスが表示されます。選択したインフォメーションサーバに一般サーバを移動するには [OK] をクリックします。

スキャンサーバにおける NetApp デバイスの管理

RPC 検索サービスを実行するスキャンサーバにより、複数の NetApp 7-Mode デバイスと Cluster-Mode AV Connector を同時に保護できます。ServerProtect の管理コンソールを使用して、NetApp 7-Mode デバイスおよび Cluster-Mode AV Connector をスキャンサーバに追加します。

また、複数のスキャンサーバを NetApp デバイスに割り当てると、負荷分散ができます (詳細については、79 ページの「1 台の NetApp デバイスに対する複数のスキャンサーバの使用」を参照してください)。

スキャンサーバへの NetApp 7-Mode デバイスおよび Cluster-Mode AV Connector の追加

NetApp 7-Mode デバイスを ServerProtect for Storage に追加するには、次が必要です。

- Backup Operator 権限以上の NetApp 7-Mode デバイス用アカウント
- NetApp 7-Mode デバイスの名前または IP アドレス

NetApp 7-Mode デバイスを追加するには

1. 一般サーバを右クリックし、ドメインブラウザツリーから [デバイスリスト] を選択します。
   [デバイスリスト] 画面が表示されます。
2. [追加] をクリックします。
   [デバイスの追加] 画面が表示されます。

図 3-7.　[デバイスの追加] 画面 (1)

3. 次の手順に従ってください。
   - [デバイスモード] ドロップダウンリストから [7-Mode Devices] を選択します。
   - [名前または IP アドレス] テキストボックスに、NetApp 7-Mode デバイスの名前または IP アドレスを入力します。
   - [ドメイン名] テキストボックスに、NetApp 7-Mode デバイスが存在するドメインの名前を入力します。

注意： このドメイン名は、NetApp 7-Mode デバイスがユーザ認証に使用する Windows ドメインのことを指します。

- [ユーザ名] および [パスワード] テキストボックスに、NetApp 7-Mode デバイスのログオン認証情報 (Backup Operator 権限以上が必要) を入力します。

4. [OK] をクリックします。

NetApp Cluster-Mode AV Connector を ServerProtect に追加するには、次が必要です。

- Cluster-Mode AV Connector で管理されているすべての Cluster-Mode デバイスで権限を持つユーザに追加されているアカウント

NetApp Cluster-Mode AV Connector を追加するには

1. 一般サーバを右クリックし、ドメインブラウザツリーから [デバイス リスト] を選択します。
   [デバイスリスト] 画面が表示されます。
2. [追加] をクリックします。
   [デバイスの追加] 画面が表示されます。

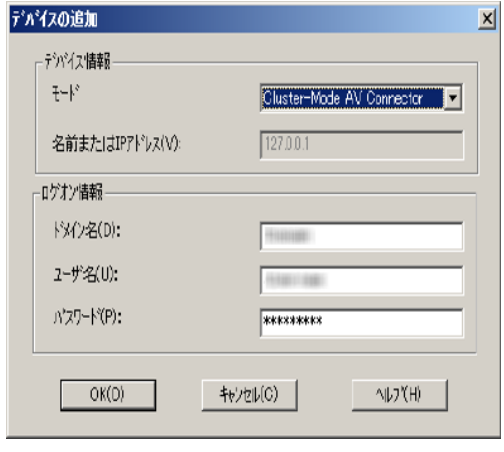


図 3-8. [デバイスの追加] 画面 (2)

3. 次の手順に従ってください。
   - [デバイスモード] ドロップダウンリストから [Cluster-Mode AV Connector] を選択します。
   - [ドメイン名] テキストボックスに、NetApp Cluster-Mode AV Connector が存在するドメインの名前を入力します。
   - [ユーザ名] および [パスワード] テキストボックスに、NetApp Cluster-Mode AV Connector のログオン認証情報を入力します。

注意： Cluster-Mode AV Connector で複数の Cluster-Mode デバイスを管理している場合、このログオンアカウントは、Cluster-Mode AV Connector で管理されている全てのデバイスで特権ユーザ (privileged user) として設定されている必要があります。AV Connector の詳細については、NetApp デバイスのドキュメントを参照してください。

4. [OK] をクリックします。

注意： Windows Server 2008 以降の OS 上に ServerProtect をインストールしている場合は、デバイスとスキャンサーバを特定の指定ドメインに追加し、それらの IP アドレスを正引きゾーンと逆引きゾーンに追加します。

さらに、デバイスとスキャンサーバが異なるドメイン内にある場合は、ドメインの信頼関係を設定することで、それら 2 つのドメインを信頼リストに追加する必要があります。

1 台の NetApp デバイスに対する複数のスキャンサーバの使用

ServerProtect for Storage は、NetApp デバイスを使用する組織に対して、スケーラブルなエンタープライズ用ウイルス検索ソリューションを提供します。

大量の入力ファイルが NetApp デバイスにある場合、NetApp デバイスで複数のスキャンサーバを追加して登録すると、登録されているスキャンサーバに負荷が均等に分散されます。

NetApp デバイスでは、ファイルがスキャンサーバにラウンドロビン方式で送信されます。たとえば、3 台のスキャンサーバがある環境で、NetApp デバイスに入力ファイルが 4 つある場合、1 台目のスキャンサーバが 1 つ目のファイルを検索します。そして、2 台目のスキャンサーバが 2 つ目のファイルを検索します。さらに、3 台目のスキャンサーバが 3 つ目のファイルを検索し、1 台目のスキャンサーバが 4 つ目のファイルを検索します。

負荷が均等に分散されると、それぞれのスキャンサーバの負荷が軽減されます (負荷分散)。

1 台の NetApp デバイスに対し複数のスキャンサーバが動作していることを確認するには

1. 確認対象となる NetApp デバイス上でコマンドプロンプトを開きます。
2. コマンドプロンプトで、次のコマンドを入力します。

   ```
   netapp> vscan scanners
   ```

   NetApp デバイスではスキャンサーバのリストが IP アドレスと NetBIOS 名別に表示されます。

スキャンサーバからの NetApp 7-Mode デバイスまたは Cluster-Mode AV Connector の削除

NetApp 7-Mode デバイスまたは Cluster-Mode AV Connector を変更、アップグレード、または名前変更する際、場合によっては、NetApp 7-Mode デバイスまたは Cluster-Mode AV Connector をスキャンサーバから削除する必要があります。NetApp 7-Mode デバイスまたは Cluster-Mode AV Connector を削除するには、次の手順を実行してください。

1. スキャンサーバを右クリックし、ドメインブラウザツリーから [デバイス リスト] を選択します。[デバイスリスト] 画面が表示されます。
2. 1 つ以上の NetApp 7-Mode デバイスまたは Cluster-Mode AV Connector をリストから選択します。複数の NetApp 7-Mode デバイスまたは Cluster-Mode AV Connectors を選択するには、<Ctrl> キーを押しながら選択します。
3. [削除] をクリックします。[デバイスの削除] 確認画面が表示されます。
4. [OK] をクリックします。

NetApp 7-Mode デバイスまたは Cluster-Mode AV Connector のオプションの設定

ここでは、NetApp 7-Mode デバイスまたは Cluster-Mode AV Connector に関連する設定を管理コンソールで設定する際に必要な情報について説明します。

NetApp 7-Mode デバイスまたは Cluster-Mode AV Connector の情報の変更

NetApp 7-Mode デバイスまたは Cluster-Mode AV Connector のシステム情報を変更するには、RPC 検索サービスを実行する ServerProtect for Storage で、NetApp 7-Mode デバイスまたは Cluster-Mode AV Connector のログオン情報を変更する必要があります。

RPC 検索サービスを実行する ServerProtect for Storage で、NetApp 7-Mode デバイスのシステム情報を変更するには、次の情報が必要です。

- Backup Operator 権限以上の NetApp 7-Mode デバイス用アカウント
- NetApp 7-Mode デバイスの名前または IP アドレス

NetApp 7-Mode デバイスの情報を更新するには

1. スキャンサーバを右クリックし、ドメインブラウザツリーから [デバイス リスト] を選択します。[デバイスリスト] 画面が表示されます。
2. リストから NetApp 7-Mode デバイスを 1 つ以上選択します。NetApp 7-Mode デバイスを複数選択するには、<Ctrl> キーを押しながら選択します。
3. [ログオン情報] をクリックします。[ログオン情報] 画面が表示されます。
4. 次の手順に従ってください。
   a. [ドメイン名] テキストボックスに、NetApp 7-Mode デバイスが存在するドメインの名前を入力します。
   b. [ユーザ名] および [パスワード] テキストボックスに、NetApp 7-Mode デバイスのログオン認証情報 (Backup Operator 権限以上が必要) を入力します。
5. [適用] をクリックして、NetApp 7-Mode デバイスの情報を変更します。確認画面が表示されます。
6. [OK] をクリックします。

ServerProtect for Storage で、Cluster-Mode AV Connector のシステム情報を変更するには、次の情報が必要です。

- Cluster-Mode AV Connector で管理されているすべての Cluster-Mode デバイスで権限を持つユーザに追加されているアカウント

Cluster-Mode AV Connector のシステム情報を変更する手順は、NetApp 7-Mode デバイスのシステム情報を変更する手順と同じです。

一般サーバとしてのスキャンサーバの使用

理想的な設定は、主に NetApp デバイスを保護するスキャンサーバとしてコンピュータを機能させることですが、スキャンサーバを組織の一般サーバ (ファイルサーバやデータサーバなど) として機能させることが必要になる場合もあります。

スキャンサーバを一般サーバとして使用するように選択すると、一般サーバのリアルタイム検索機能が初期設定で有効になります。

リアルタイム検索には、次のオプションがあります。

- 入力ファイル (初期設定)
- 出力ファイル
- 入出力ファイル

注意： 最高レベルのセキュリティを実現するには、リアルタイム検索を「入出力ファイル」に設定してください。ただし、コンピュータをスキャンサーバとしてのみ実行する場合は、初期設定 (入力ファイル) を使用できます。

リアルタイム検索を「入出力ファイル」に設定するには、次の手順を実行します。

1. ドメインブラウザツリーで、インフォメーションサーバ、ドメイン、または一般サーバ (スキャンサーバ) 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。

[リアルタイム検索設定] 画面が表示されます。

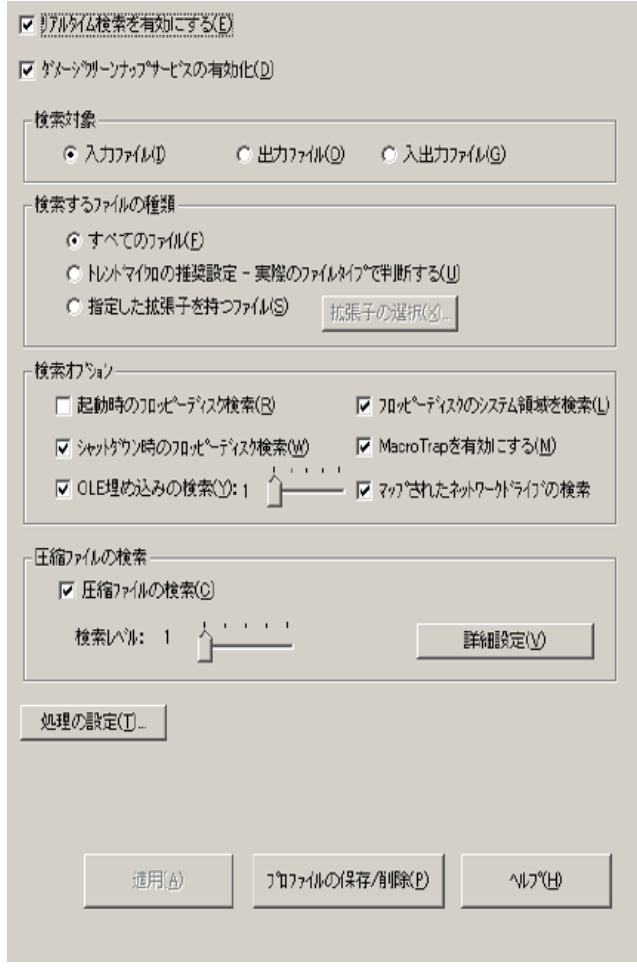


図 3-9.　[リアルタイム検索設定] 画面

3. [検索対象] で、[入出力ファイル] をクリックします。
4. [適用] をクリックします。

リアルタイム検索の詳細については、125 ページの「リアルタイム検索」を参照してください。

感染時の NetApp デバイスクライアントへの通知

ServerProtect では、NetApp デバイスのクライアントが感染ファイルをアップロードしたりアクセスした場合にユーザとネットワーク管理者に通知できます。通知機能は初期設定で有効になっています。

NetApp デバイスのクライアントが感染したことをユーザに通知するには、次の手順を実行してください。

1. スキャンサーバを右クリックし、ドメインブラウザツリーから [デバイス リスト] を選択します。[デバイスリスト] 画面が表示されます。
2. [オプション] をクリックします。[グローバルデバイスオプション] 画面が表示されます。

図 3-10. [グローバルデバイスオプション] 画面

3. [感染時にデバイスクライアントに通知する] を選択します。
4. [OK] をクリックします。

注意： この設定はデバイスリストにあるすべての NetApp デバイスに影響します。

NetApp デバイスのステータスの表示

管理コンソールから NetApp デバイスに関するステータスを表示できます。次のいずれかの理由により、NetApp デバイスがオフラインとして表示される場合があります。

- NetApp デバイスが終了しているか応答しない
- ネットワークが利用できない
- NetApp デバイスがインフォメーションサーバに正常に登録されなかった

NetApp デバイスのステータスを表示するには、次の手順を実行してください。

1. スキャンサーバを右クリックし、ドメインブラウザツリーから [デバイスリスト] を選択します。[デバイスリスト] 画面が表示されます。

図 3-11. [デバイスリスト] 画面

2. [デバイス リスト] にある [デバイス 名] フィールド、[ステータス] フィールド、および [モード] フィールドを調べることで、NetApp デバイスのステータスを確認します。

   7-Mode デバイス、Cluster-Mode AV Connector、または Cluster-Mode デバイスに対してオンライン / オフラインが表示されます。

NetApp デバイス RPC 接続に関するステータス通知の設定

ServerProtect では、NetApp デバイスへの RPC 接続が成功したときや失敗したときにネットワーク管理者に通知できます。

NetApp デバイス RPC 接続に関するステータス通知を設定するには、次の手順を実行してください。

1. ドメインブラウザツリーで、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。
   - サイドバーから [通知の設定] → [一般の警告] の順にクリックします。

3. [デバイスの RPC 接続の成功 / 失敗] を選択します。

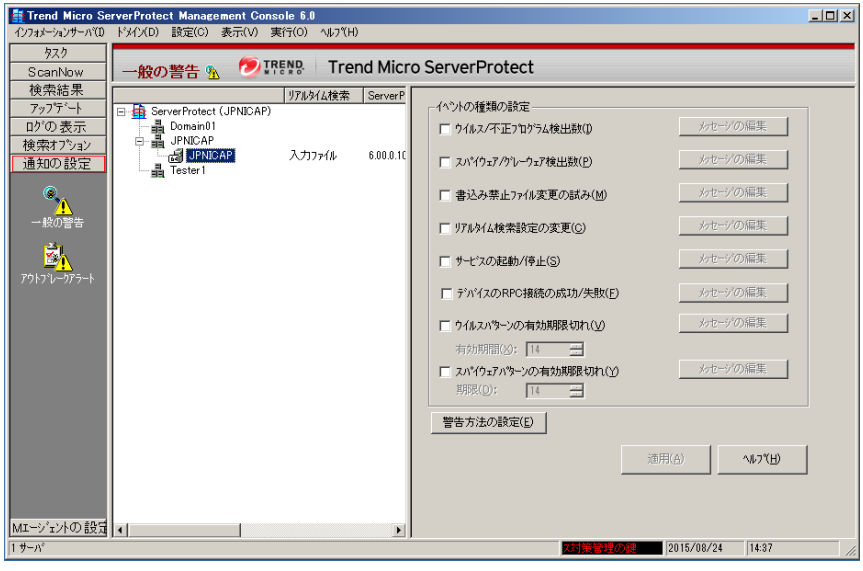


図 3-12. 一般の警告の設定

4. [メッセージの編集] をクリックして、カスタマイズされた通知メッセージを設定します。

注意： 詳細については、112 ページの「通知メッセージの設定」を参照してください。

NetApp デバイスへの新規コンポーネントアップデートの通知

アップデートで新規コンポーネント (検索エンジンやパターンファイル) をスキャンサーバにダウンロードする場合、以前検索したファイルのキャッシュをフラッシュするようにスキャンサーバで NetApp デバイスに通知します。これにより、最新のウイルスパターンファイルですべてのファイルが検索されるようになります。そうすると各 NetApp デバイスでは、新規アップデートがアップデートサーバで利用できるようになるまで、以前検索したファイルのキャッシュが再構築されます。

アップデートのダウンロード手順については、92 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。

注意： NetApp 向けの ServerProtect for Storage の問い合わせ先および技術サポート提供は販売店となります。詳しくは、製品ページをご覧ください。
http://www.go-tm.jp/spfs

スキャンサーバの ICAP クライアントリストの管理

ICAP 検索サービスを実行するスキャンサーバは、ICAP クライアントを含むストレージデバイスを保護します。スキャンサーバでは、任意の ICAP クライアントから検索リクエストを受け入れるか、ICAP クライアントリストに含まれているクライアントからのみ検索リクエストを受け入れるかを設定できます。

検索リクエストを受け入れる ICAP クライアントを設定するには

1. 一般サーバを右クリックし、ドメインブラウザツリーから [ICAP クライアントリスト] を選択します。

   [ICAP クライアントリスト] 画面が表示されます。

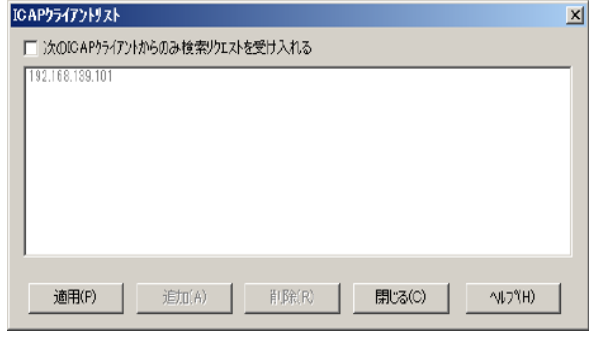


図 3-13. ICAP クライアントリスト

2. 次のいずれかの操作を実行します。
   - ICAP クライアントリストに含まれているクライアントからのみ検索リクエストを受け入れるには、[次の ICAP クライアントからのみ検索リクエストを受け入れる] チェックボックスをオンにします。

- 任意の ICAP クライアントから検索リクエストを受け入れるには、[次の ICAP クライアントからのみ検索リクエストを受け入れる] チェックボックスをオフにします。

3. [適用] をクリックします。

ICAP クライアントを ICAP クライアントリストに追加するには

1. 一般サーバを右クリックし、ドメインブラウザツリーから [ICAP クライアントリスト] を選択します。

   [ICAP クライアントリスト] 画面が表示されます。

2. [追加] をクリックします。

   [ICAP クライアントアドレスの追加] 画面が表示されます。

3. 次のいずれかの操作を実行します。
   - 単一の ICAP クライアントを追加するには、[IP アドレス / ホスト名] を選択し、IP アドレスまたはホスト名を入力します。
   - 複数の ICAP クライアントを追加するには、[IP 範囲] を選択し、IP 範囲を入力します。
4. [OK] をクリックします。

ICAP クライアントまたは IP 範囲を ICAP クライアントリストから削除するには

1. 一般サーバを右クリックし、ドメインブラウザツリーから [ICAP クライアントリスト] を選択します。

   [ICAP クライアントリスト] 画面が表示されます。

2. リストで ICAP クライアントまたは IP 範囲を選択します。エントリを複数選択するには、<Ctrl> キーを押しながら選択します。

   [ICAP クライアントアドレスの追加] 画面が表示されます。

3. [削除] をクリックします。

アップデートの設定

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

コンポーネントのアップデート

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

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

ダウンロードと配信の流れ

ServerProtect ネットワークでのアップデートファイルのダウンロードと配信の要求に対する ServerProtect の処理の流れについて図 3-14 で説明します。

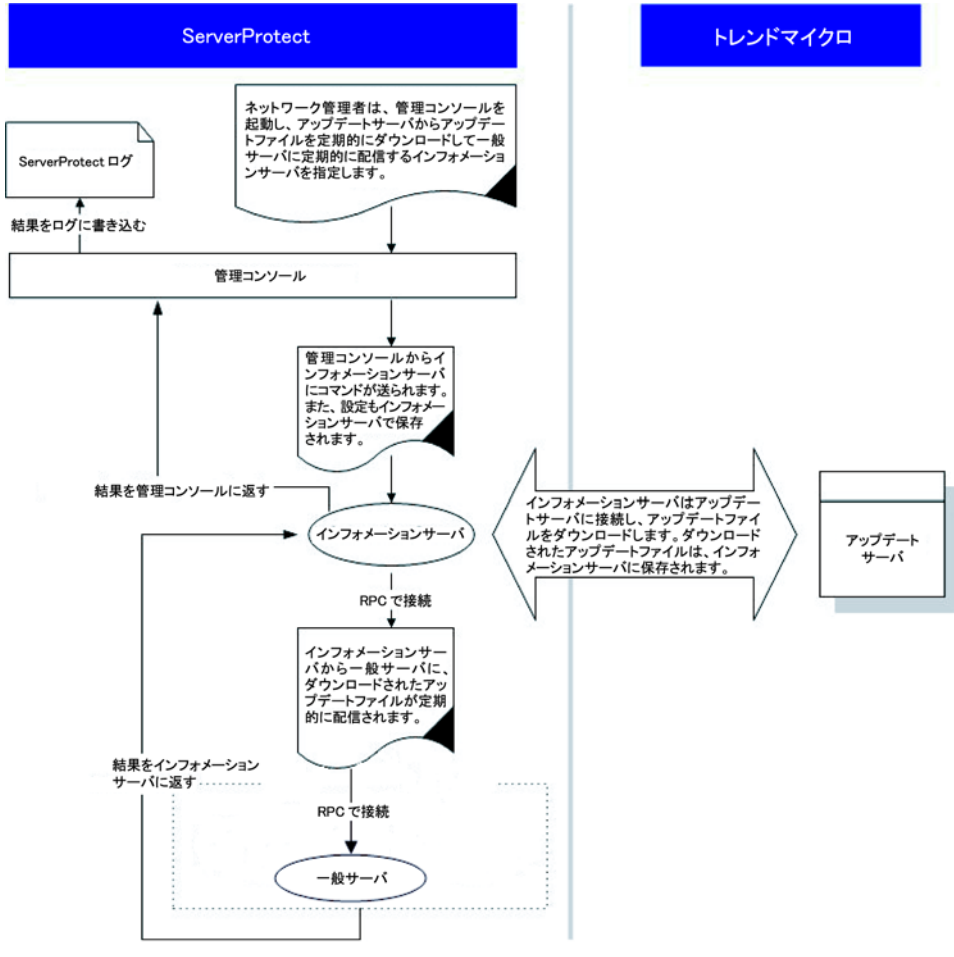


図 3-14.　ダウンロードと配信の流れ

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。

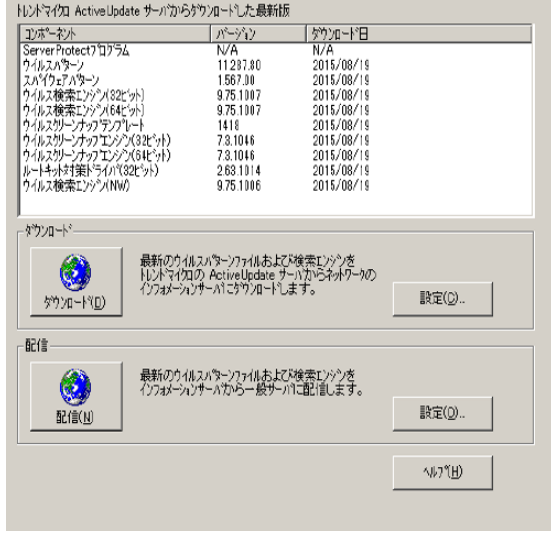


図 3-15. [アップデート] メイン画面

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)

- ウイルスクリーンナップテンプレートのバージョン
- ウイルスクリーンナップエンジンのバージョン (32 ビットおよび 64 ビット)
- ルートキット対策ドライバのバージョン (32 ビットのみ)

アップデートファイルのダウンロード

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

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

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

ダウンロード元の指定

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

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

1. 次のいずれかの操作を実行してください。
   - サイドバーから [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://spfs60-p.activeupdate.trendmicro.co.jp/activeupdate/japan
   ```

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

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

ローカルまたはネットワークドライブをダウンロード元に設定するには

1. 次のいずれかの操作を実行してください。
   - サイドバーから [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] 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. [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。
   - `<ドライブ>:¥Program Files¥Trend¥SProtect¥` にある `SpntShare` フォルダをインフォメーションサーバの共有フォルダに設定します。
   - ネットワークサーバに共有フォルダを作成し、SpntShare フォルダにあるすべてのファイルをコピーします。

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

ダウンロードの実行

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

ダウンロードを実行するには、次のオプションを選択してください。

1. 次のいずれかの操作を実行してください。
   - サイドバーから [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、「送信元にネットワークの問題があります」または「HTTP タイムアウトが発生しました」というメッセージが表示される場合があります。詳細については、95 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。

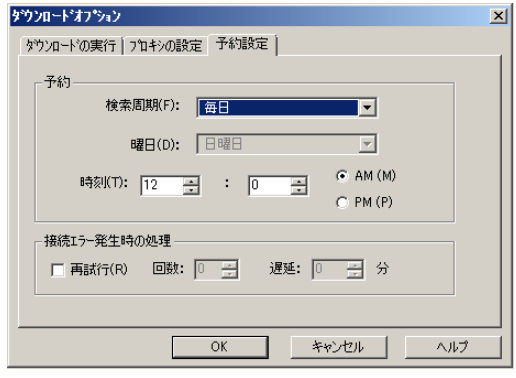


図 3-16. [ダウンロードオプション] - [予約設定]

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] をクリックします。ダウンロードされたファイルは、次のディレクトリに保存されます。

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

ダウンロードの設定

最新のアップデートファイルをダウンロードする手順について説明します。

ダウンロードを設定するには、次の手順に従ってください。

1. 次のいずれかの操作を実行してください。
   - サイドバーから [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。

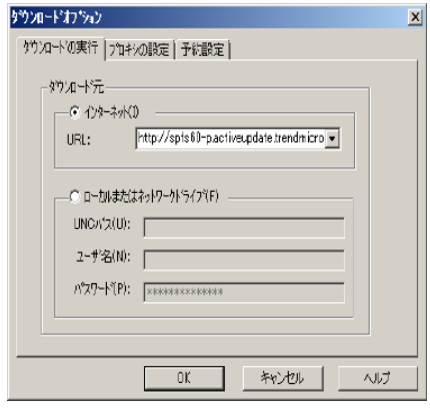


図 3-17. [ダウンロードオプション] - [ダウンロードの実行]

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。

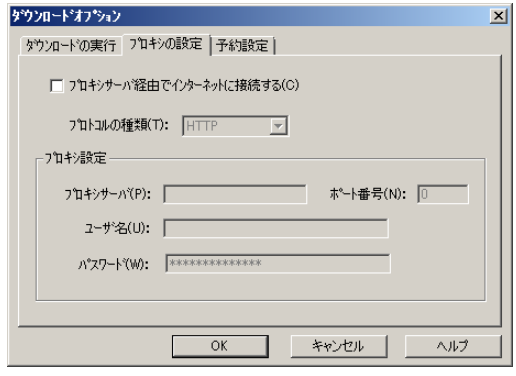


図 3-18. [ダウンロードオプション] - [プロキシの設定]

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] 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] 画面が表示されます。

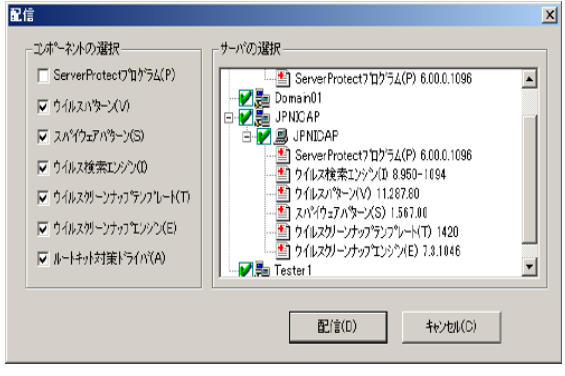


図 3-19. [配信]

[コンポーネントの選択] グループのチェックボックスは、一般サーバに配信可能なコンポーネントを示しています。[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]、[ウイルスクリーンナップテンプレート]、[ウイルスクリーンナップエンジン]、および [ルートキット対策ドライバ] 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]、[ウイルスクリーンナップテンプレート]、[ウイルスクリーンナップエンジン] 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、103 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、103 ページの「新規タスクの作成」を参照してください。

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

予約配信を設定するには、次の手順に従ってください。

1. 次のいずれかの操作を実行してください。
   - サイドバーから [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。

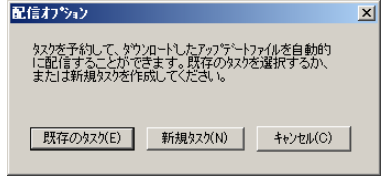


図 3-20. [配信オプション] ダイアログボックス

3. 次のいずれかの操作を実行してください。
   - タスクを新規作成する場合は [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の詳細については、103 ページの「新規タスクの作成」および 109 ページの「既存のタスクの変更」を参照してください。

配信した更新内容のロールバック

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

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

既に配信した更新内容をロールバックするには、次の手順に従ってください。

1. 次のいずれかの操作を実行してください。
   - サイドバーから [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。

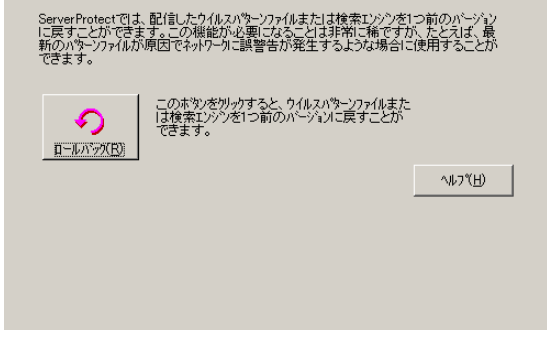


図 3-21. ロールバックの設定

2. [ロールバック] 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。

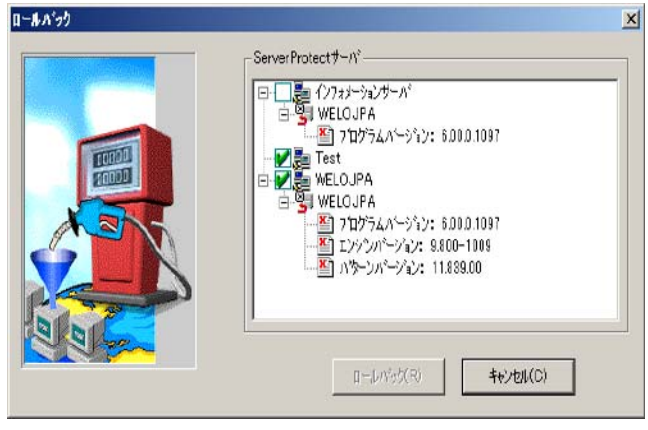


図 3-22. [ロールバック] ダイアログボックス

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

3. ロールバックする対象をツリーから選択し、[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。
- [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 3-23.　[タスクウィザード] ダイアログボックス

初期設定のタスク

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

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

詳細については、以下の製品 Q&A を参照してください。
http://esupport.trendmicro.com/solution/ja-JP/1102106.aspx

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。

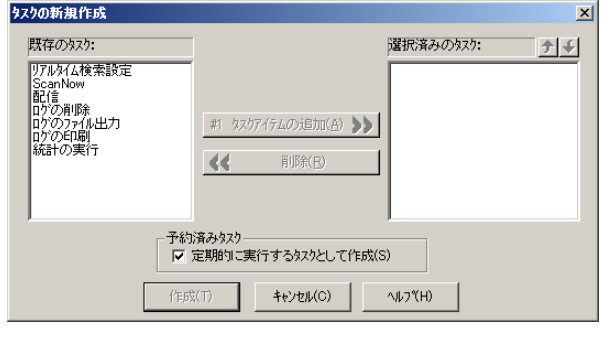


図 3-24. [タスクの新規作成] ダイアログボックス

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。

ヒント： 機能の実行順序を変更するには、順序を変更する機能を選択し、[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。

---

6. このタスクを予約して自動的に実行したい場合は、必ず [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。
7. [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。[キャンセル] をクリックすると、変更内容が保存されずに、[タスクの新規作成] ダイアログボックスが閉じます。

予約タスクの作成

予約タスクを作成することで、設定にかかる手間や時間を省くことができます。

予約タスクを作成するには、次の手順に従ってください。

1. 103 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 3-24 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] 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 3-25. [予約設定] ダイアログボックス

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。

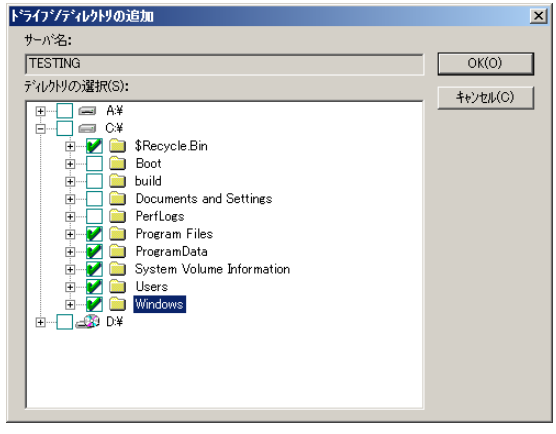


図 3-26. [ドライブ / ディレクトリの追加] ダイアログボックス

初期設定タスクの作成

タスクウィザードの最後に表示される [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。

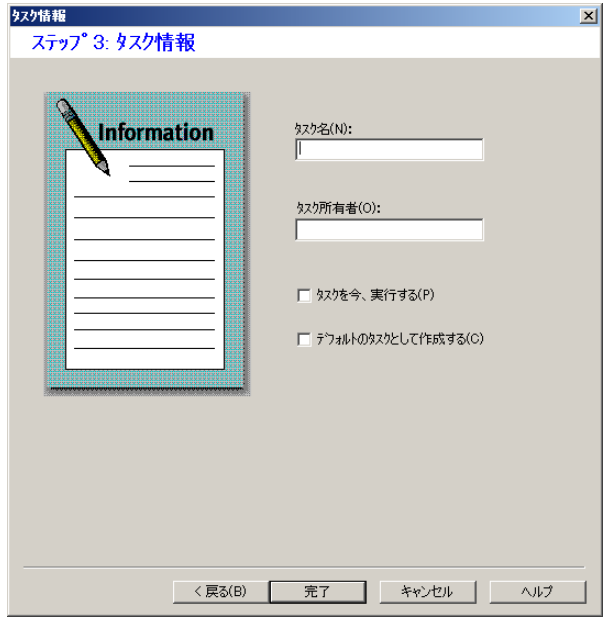


図 3-27. [タスク情報] ダイアログボックス

タスクの作成を終了するには、次の手順に従ってください。

1. [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。

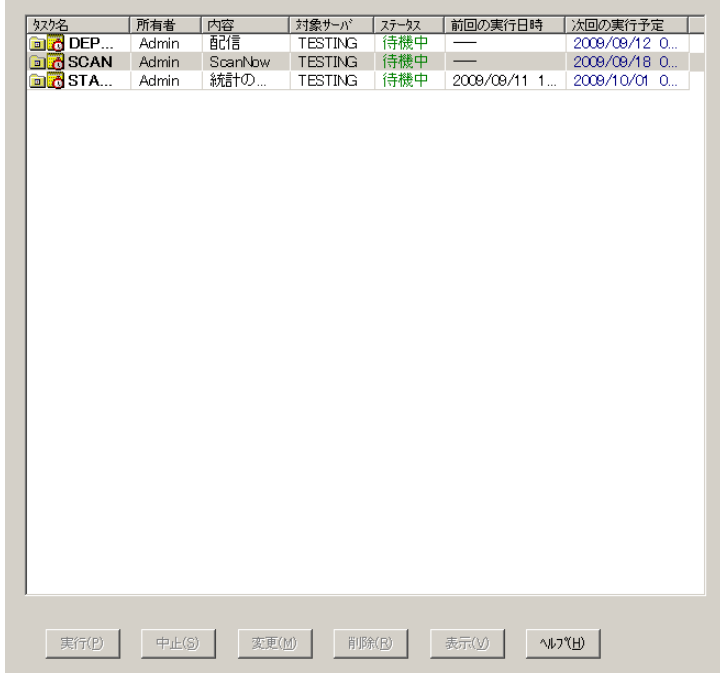


図 3-28. 既存のタスクを表形式で表示

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

既存のタスクを実行するには、次の手順に従ってください。

1. 次のいずれかの操作を実行してください。
   - サイドバーから [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] 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。

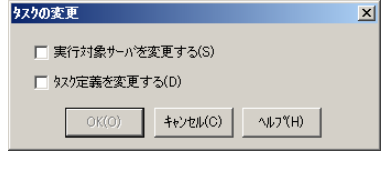


図 3-29. [タスクの変更] ダイアログボックス

4. 次のいずれかの操作を実行してください。
   - [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。

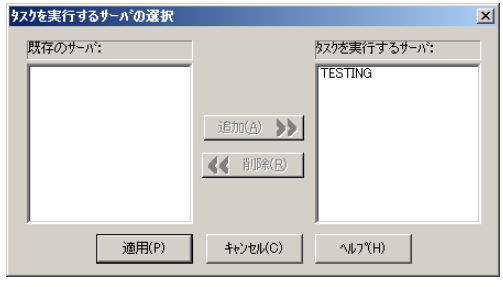


図 3-30. [タスクを実行するサーバの選択] ダイアログボックス

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

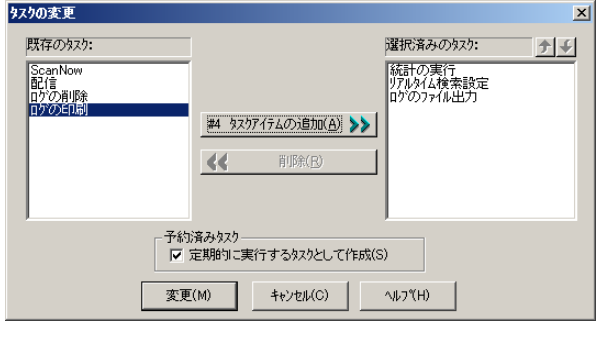


図 3-31. [タスクの変更] ダイアログボックス

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。

ヒント： 機能の実行順序を変更するには、順序を変更する機能を選択し、[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

既存タスクの属性は [既存のタスク] ダイアログボックスに表示され、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。

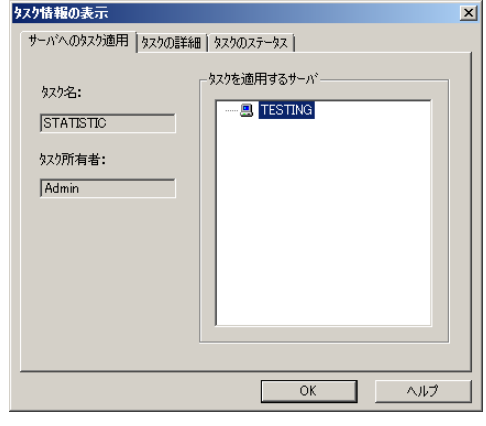


図 3-32. [タスク情報の表示] ダイアログボックス

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。[対象サーバ] 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選択すると、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] : [対象サーバ] 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情報が表示されます。このリストを使用してタスクの定義を削除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できます。警告方法の詳細については、116 ページの「警告方法の設定」を参照してください。

一般の警告

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

通知イベント

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

- **ウイルス不正プログラムの検出** : サーバ上に感染ファイルを検出した場合
- **スパイウェア / グレーウェアの検出** : サーバ上にスパイウェア / グレーウェア感染ファイルを検出した場合
- **書込み禁止ファイルの変更の試み** : 書込み禁止ファイルの変更の試みを検出した場合
- **リアルタイム検索設定の変更** : リアルタイム検索設定の変更を検出した場合
- **サービスの起動 / 停止** :ServerProtect の起動 / 停止イベントを検出した場合
- **デバイスの RPC 接続の成功 / 失敗** : NetApp デバイスへの RPC 接続に関するステータス
- **ウイルスパターンの有効期限切れ** : ウイルスパターンファイルの有効期限切れを検出した場合
- **スパイウェアパターンの有効期限切れ** : スパイウェアパターンファイルの有効期限切れを検出した場合

一般の警告の発行を設定するには、次の手順に従ってください。

1. ドメインブラウザツリーからインフォメーションサーバ、ドメイン、または一般サーバを選択します。
2. 次のいずれかの操作を実行してください。
   - メインメニューから [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。

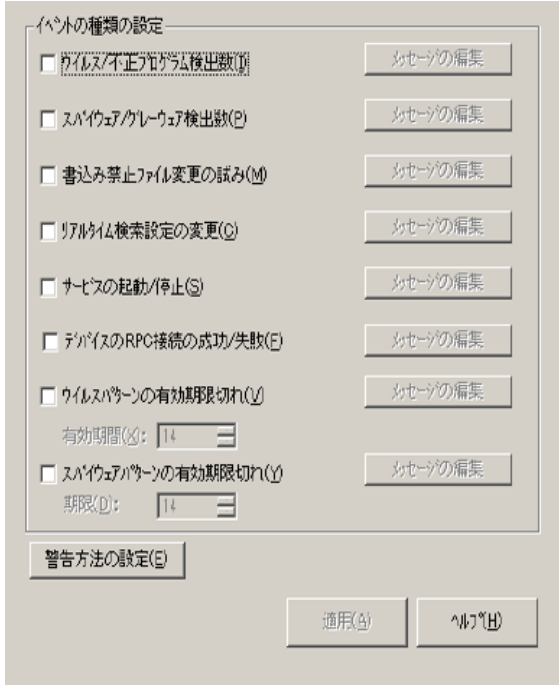


図 3-33. 一般の警告の設定

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。(日本語での入力も可能です。)
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、116 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。
   - 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。

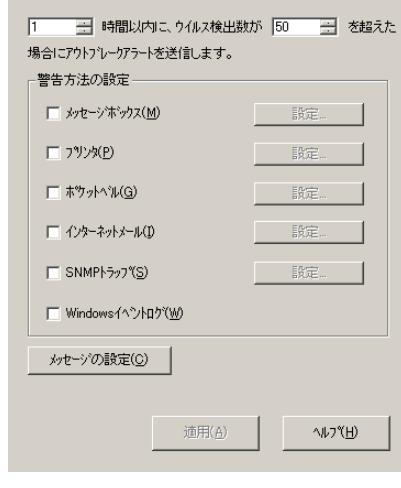


図 3-34. アウトブレークアラートの設定

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、116 ページの「警告方法の設定」を参照してください。
6. [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。(日本語での入力も可能です。)
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。

- Message box (メッセージボックス): 管理者のコンピュータに、標準的な Windows ポップアップメッセージボックスが表示されます。
- Printer (プリンタ): メッセージがローカルまたはネットワークプリンタに送信されます。
- Pager (ポケットベル) : メッセージがポケットベルに送信されます。この機能を使用するには、ServerProtect が動作しているサーバにモデムが接続されている必要があります。
- Internet Mail (インターネットメール): ユーザ設定に応じて、メールメッセージを送信できます。
- SNMP Trap (SNMP トラップ): SNMP トラップ対応の管理コンソールを使用しているネットワーク管理者に、SNMP トラップによる警告メッセージが送信されます。
- Windows Event Log (Windows イベントログ): ウイルスの検出が Windows のイベントログに書き込まれます。

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

インターネットメール (メール) 警告を設定するには

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

   アウトブレークアラートを設定するには

   次のいずれかの操作を実行してください。

   - サイドバーから [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。

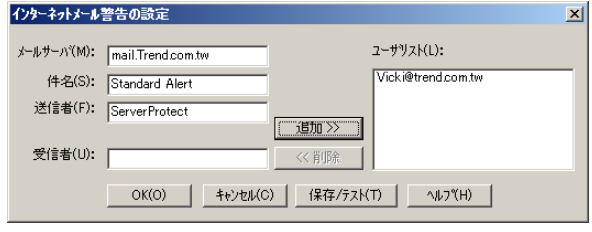


図 3-35. [インターネットメール警告の設定] ダイアログボックス

4. 次の操作を実行してください。
   a. メールサーバソフトウェアが動作しているサーバを [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。

一般サーバのウイルス検索

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

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

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

また、次の処理を設定することができます。

- 検索するファイルの種類を選択する
- 書込み禁止リストを使用して、指定したファイルまたはディレクトリがユーザに変更されたり削除されないように設定する。書込み禁止リストの設定についての詳細は、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。

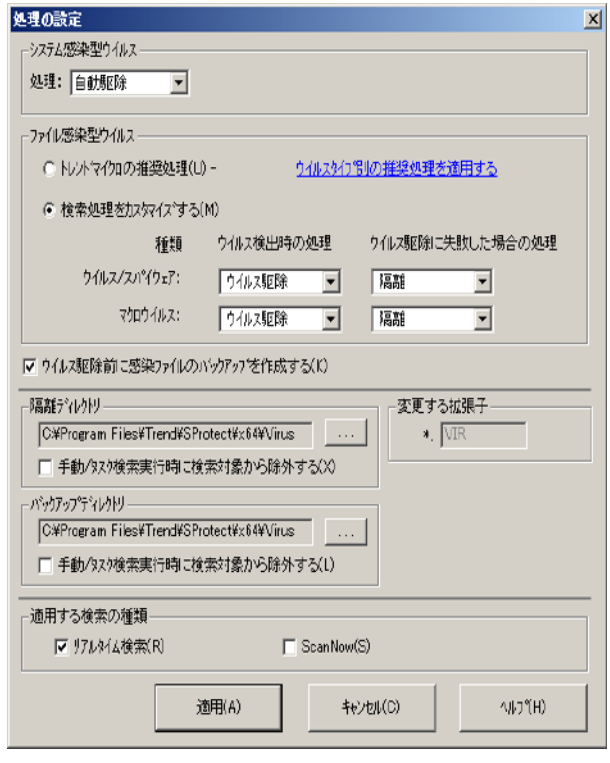


図 3-36.　一般サーバの [処理の設定] ダイアログボックス

任意のウイルスに対する処理を設定するには、次の手順に従ってください。

1. リアルタイム検索または手動検索設定領域で [処理の設定] ボタンをクリックします。[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、27 ページの「ウイルスを検出した場合」を参照してください。トレンドマイクロの推奨設定の詳細については、33 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、[ウイルス駆除前に感染ファイルの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「検索対象から除外するディレクトリ」の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。

注意： EMC CAVA 検索サービスは、リアルタイム検索を使用して EMC VNX/VNXe サーバを保護します。一般サーバを EMC CAVA 検索サービスとしてインストールしている場合は、リアルタイム検索の設定が EMC CAVA 検索サービスにも適用されます。

検索プロファイル

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

予約検索タスクなどタスクを作成する際には、既存の検索プロファイルを選択することも、独自の検索プロファイルを作成することもできます。詳細については、109 ページの「既存のタスクの変更」を参照してください。

プロファイルを保存するには、次の手順に従ってください。

1. リアルタイム検索または手動検索の設定を実行します。詳細については、125 ページの「検索の設定」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。

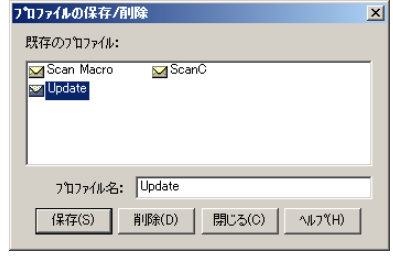


図 3-37. [プロファイルの保存 / 削除] ダイアログボックス

3. プロファイルの名前を [プロファイル名] フィールドに入力します。
4. [保存] 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。
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。

ストレージデバイスのウイルス検索

ServerProtect for Storage のストレージデバイスのウイルス検索には、RPC 検索サービス、EMC CAVA 検索サービス、および ICAP 検索サービスの 3 種類があります。

RPC 検索サービスおよび EMC CAVA 検索サービスでは感染ファイルに対する処理として、放置 (手動処理)、削除、拡張子変更、隔離、ウイルス駆除の 5 つの処理から選択することができます。ICAP 検索サービスでは、感染ファイルに対して 2 種類の処理のみを実行できます。

RPC 検索サービスと EMC CAVA 検索サービスでのウイルスに対する処理の定義

EMC CAVA 検索サービスと RPC 検索サービスを実行する ServerProtect では、ストレージデバイスで検出された感染ファイルに対して実行する処理を設定できます。

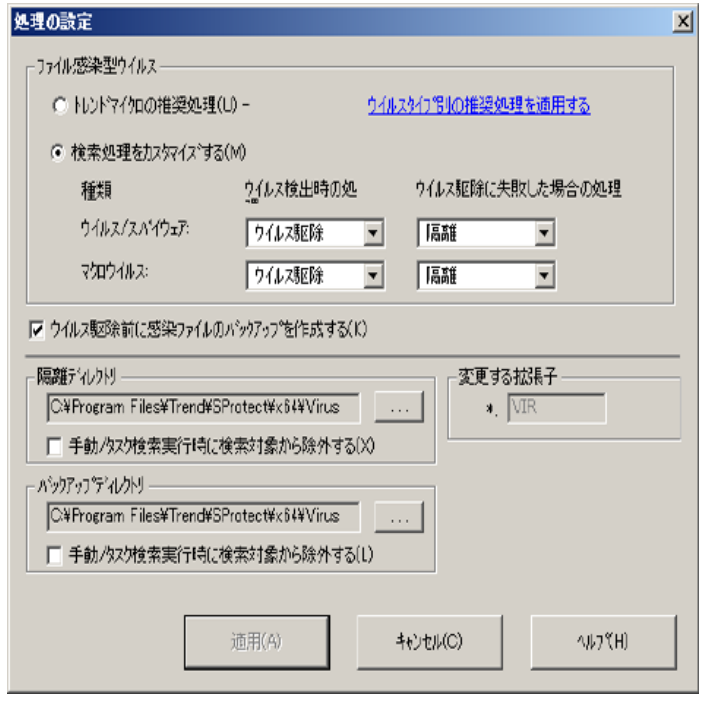


図 3-38.　[処理の設定] ダイアログボックス

RPC 検索サービスと EMC CAVA 検索サービスでのウイルスに対する処理を定義するには

1. [ストレージ検索サービス] の設定データ領域で　[処理の設定] をクリックします。[処理の設定] ダイアログボックスが表示されます。
2. [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。

- [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、27 ページの「ウイルスを検出した場合」を参照してください。トレンドマイクロの推奨設定の詳細については、33 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、[ウイルス駆除前に感染ファイルの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「検索対象から除外するディレクトリ」の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。

3. [適用] ボタンをクリックして、設定を保存します。

注意： EMC CAVA 検索サービスは、リアルタイム検索を使用して EMC VNX/VNXe サーバを保護します。一般サーバを EMC CAVA 検索サービスとしてインストールしている場合は、EMC CAVA 検索サービスの設定がリアルタイム検索にも適用されます。

ICAP 検索サービスでのウイルスに対する処理の定義

ICAP 検索サービスを実行する ServerProtect では、ストレージデバイスで検出された感染ファイルに対して実行する処理を設定できます。

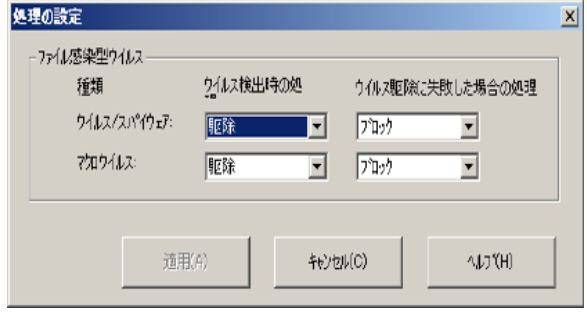


図 3-39.　[処理の設定] ダイアログボックス

ICAP 検索サービスでのウイルスに対する処理を定義するには

1. [ストレージ検索サービス] の設定データ領域で [処理の設定] をクリックします。[処理の設定] ダイアログボックスが表示されます。
2. [ファイル感染型ウイルス] グループで、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、27 ページの「ウイルスを検出した場合」を参照を参照してください。
3. [適用] ボタンをクリックして、設定を保存します。

リアルタイム検索

リアルタイム検索は、ウイルスの侵入をリアルタイムで検出します。これにより、すべての入力ファイル、出力ファイルが監視され、ウイルス感染ファイルがサーバからコピーされたり、またはサーバにコピーされることを未然に防止することができます。

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。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。詳細については、32 ページの「OLE 埋め込みの検索」を参照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。

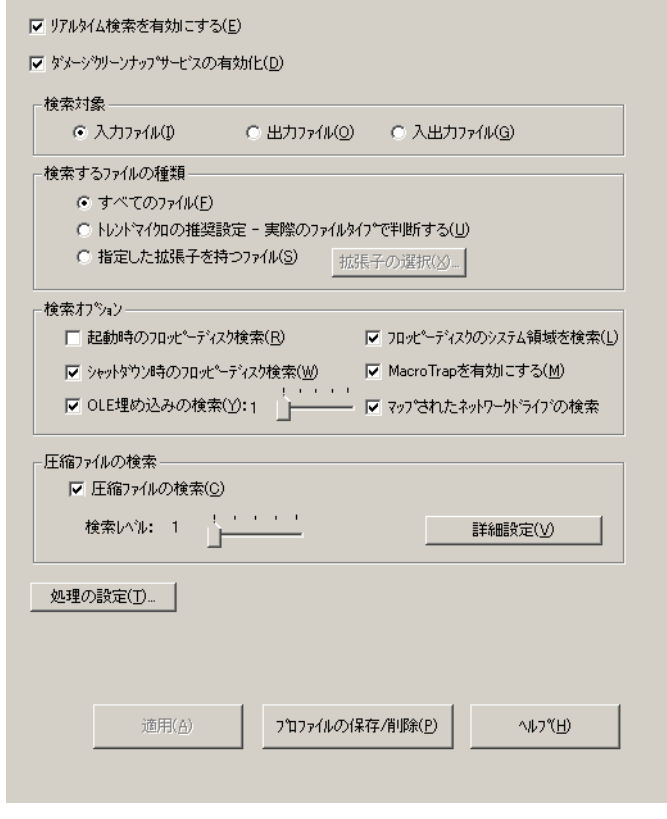


図 3-40. リアルタイム検索の設定

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、ダメージクリーンナップエンジンで、トロイの木馬およびトロイの木馬プロセスを検索して削除できるように

します。32 ビットおよび 64 ビットのプラットフォームがサポートされます。このサービスを無効にする場合は、チェックボックスをオフにします。

5. [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] : 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、33 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。詳細は、142 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

   各検索オプションの詳細については、125 ページの「検索の設定」を参照してください。
8. 圧縮ファイルを検索する場合は、[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、感染ファイルに対する処理を設定します。詳細については、119 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 [プロファイルの保存 / 削除] 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。

注意： EMC CAVA 検索サービスは、リアルタイム検索を使用して EMC VNX/VNXe サーバを保護します。一般サーバを EMC CAVA 検索サービスとしてインストールしている場合は、リアルタイム検索の設定が EMC CAVA 検索サービスにも適用されます。

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。

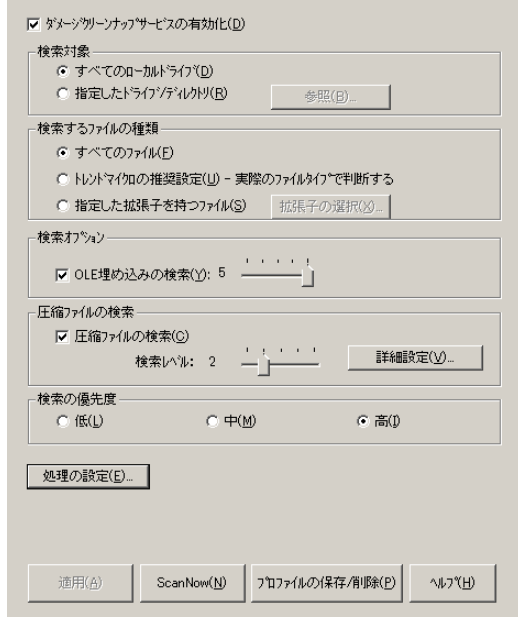


図 3-41. 手動検索の設定

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。

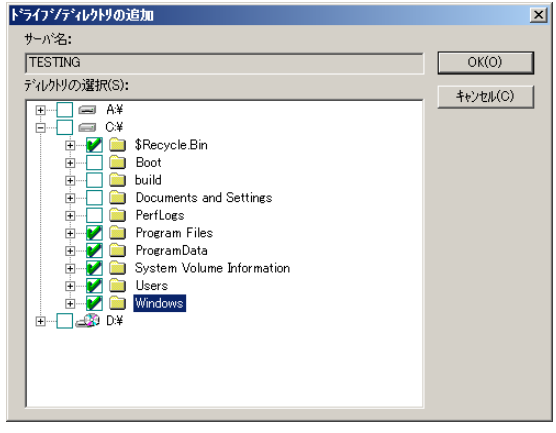


図 3-42. [ドライブ / ディレクトリの追加] ダイアログボックス

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、33 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。詳細は、142 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。ただし、ServerProtect 以外に CPU リソースを消費するプロセスがない場合は、[低] や [中] に設定していても CPU 使用率は高くなります。
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。詳細については、119 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 [すべてのプログラム] → [アクセサリ] → [エクスプローラー] の順に選択します。Windows エクスプローラが起動します。
2. ServerProtect をインストールしたフォルダをクリックします。32 ビット OS の場合、初期設定では次のフォルダにインストールされています。

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

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

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

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

ScanNow を停止するには、次の手順に従ってください。

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

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

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

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

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

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

   32 ビット OS の場合

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

   64 ビット OS の場合

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

4. [OK] をクリックします。ScanNow の実行が停止されます。

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

予約検索 (タスク検索)

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

予約検索の設定

予約タスクを使用して、ScanNow またはリアルタイム検索の予約を設定することができます。詳細については、103 ページの「新規タスクの作成」を参照してください。

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

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

RPC 検索サービスの使用

ストレージのウイルス検索で RPC モードがサポートされる場合は、RPC 検索サービスを使用します。

RPC 検索サービスの設定

RPC 検索サービスでは、次のオプションを指定できます。

- 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
- 処理の設定

RPC 検索サービスを設定するには

1. ドメインブラウザツリーで、RPC 検索サービスを実行する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ます。
   - サイドバーから [検索オプション] → [ストレージ検索サービス] の順に選択します。

- メインメニューから [実行] → [ストレージ検索サービス] の順に選択します。

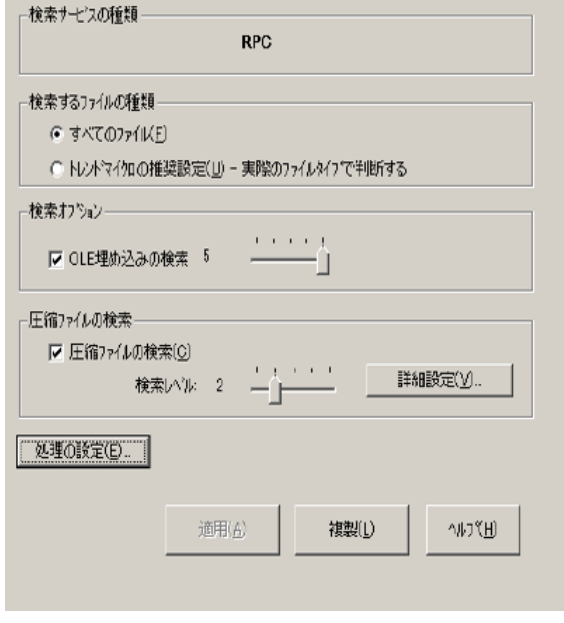


図 3-43. RPC 検索サービスの設定

3. [検索するファイルの種類] グループで、次のいずれか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、33 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。
4. 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。
5. 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。

6. [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。詳細については、123 ページの「RPC 検索サービスと EMC CAVA 検索サービスでのウイルスに対する処理の定義」を参照してください。
7. [適用] をクリックして変更を保存します。

RPC 検索サービスの設定を複製するには

1. ドメインブラウザツリーで、RPC 検索サービスを実行する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ます。
   - サイドバーから [検索オプション] → [ストレージ検索サービス] の順に選択します。
   - メインメニューから [実行] → [ストレージ検索サービス] の順に選択します。
3. [複製] をクリックします。
   [設定の複製先サーバの選択] 画面が表示されます。

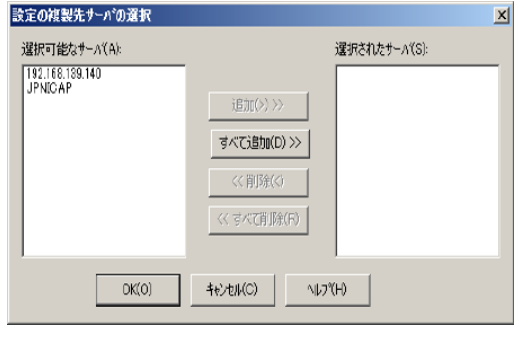


図 3-44. 設定の複製

4. [選択可能なサーバ] から一般サーバを 1 つ以上選択します。一般サーバを複数選択するには、<Ctrl> キーを押しながら選択します。

注意： [選択可能なサーバ] に表示される一般サーバの検索サービスの種類は、元の一般サーバの検索サーバの種類と同じです。

5. 次のいずれかの操作を実行します。
   - [追加] をクリックして、選択した一般サーバを [タスクを実行するサーバ] に追加します。
   - [選択可能なサーバ] 内のすべての一般サーバを [タスクを実行するサーバ] に追加するには、[すべて追加] をクリックします。

6. [OK] をクリックします。

注意： この手順では、隔離ディレクトリとバックアップディレクトリは複製されません。

EMC CAVA 検索サービスの使用

ストレージのウイルス検索で EMC CAVA がサポートされる場合は、EMC CAVA 検索サービスを使用します。

EMC CAVA 検索サービスの設定

EMC CAVA 検索サービスでは、次のオプションを指定できます。

- リアルタイム検索を有効にする
- ダメージクリーンナップサービスの有効化
- 検索方向
- 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
- 処理の設定

注意： EMC CAVA 検索サービスは、リアルタイム検索を使用して EMC VNX/VNXe サーバを保護します。一般サーバを EMC CAVA 検索サービスとしてインストールしている場合は、EMC CAVA 検索サービスの設定がリアルタイム検索にも適用されます。

EMC CAVA 検索サービスを設定するには

1. ドメインブラウザツリーで、EMC CAVA 検索サービスを実行する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ます。
   - サイドバーから [検索オプション] → [ストレージ検索サービス] の順に選択します。

- メインメニューから [実行] → [ストレージ検索サービス] の順に選択します。

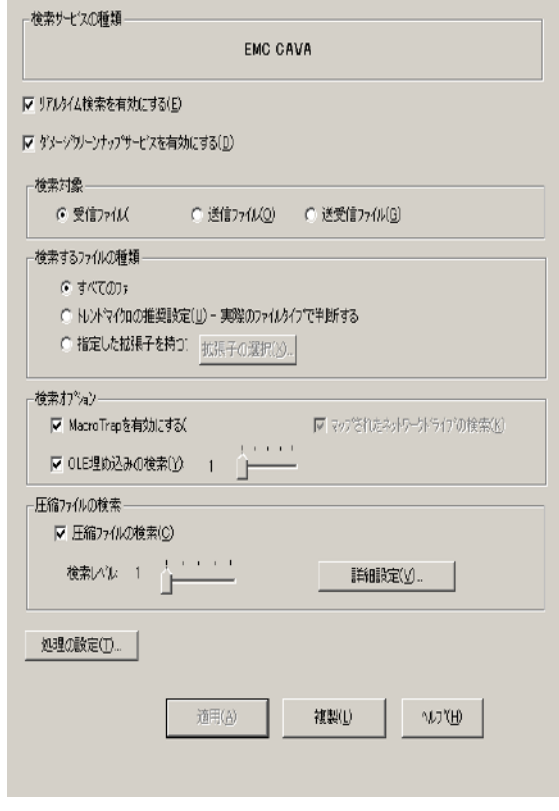


図 3-45. EMC CAVA 検索サービスの設定

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、ダメージクリーンナップエンジンで、トロイの木馬およびトロイの木馬プロセスを検索して削除できるようにします。32 ビットおよび 64 ビットのプラットフォームがサポートされます。このサービスを無効にする場合は、チェックボックスをオフにします。
5. [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、次のいずれか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、33 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。

     [指定した拡張子を持つファイル] を選択した場合、[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。詳細は、142 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。
   - OLE 埋め込みの検索
   - MacroTrap を有効にする
   - マップされたネットワークドライブの検索

   各検索オプションの詳細については、125 ページの「検索の設定」を参照してください。
8. 圧縮ファイルを検索する場合は、[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、感染ファイルに対する処理を設定します。詳細については、123 ページの「RPC 検索サービスと EMC CAVA 検索サービスでのウイルスに対する処理の定義」を参照してください。
10. [適用] をクリックして変更を保存します。

EMC CAVA 検索サービスの設定を複製するには

1. ドメインブラウザツリーで、EMC CAVA 検索サービスを実行する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ます。
   - サイドバーから [検索オプション] → [ストレージ検索サービス] の順に選択します。
   - メインメニューから [実行] → [ストレージ検索サービス] の順に選択します。

3. [複製] をクリックします。
   [設定の複製先サーバの選択] 画面が表示されます。

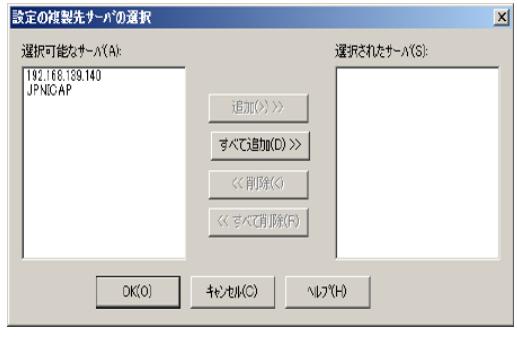


図 3-46.　設定の複製

4. [選択可能なサーバ] から一般サーバを 1 つ以上選択します。一般サーバを複数選択するには、<Ctrl> キーを押しながら選択します。

注意： [選択可能なサーバ] に表示される一般サーバの検索サービスの種類は、元の一般サーバの検索サーバの種類と同じです。

5. 次のいずれかの操作を実行します。
   - [追加] をクリックして、選択した一般サーバを [タスクを実行するサーバ] に追加します。
   - [選択可能なサーバ] 内のすべての一般サーバを [タスクを実行するサーバ] に追加するには、[すべて追加] をクリックします。
6. [OK] をクリックします。

注意： この手順では、隔離ディレクトリとバックアップディレクトリは複製されません。

ICAP 検索サービスの使用

ストレージのウイルス検索で ICAP モードがサポートされる場合は、ICAP 検索サービスを使用します。

ICAP 検索サービスの設定

ICAP 検索サービスでは、次のオプションを指定できます。

- 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
- 処理の設定
- オプション

ICAP 検索サービスを設定するには

1. ドメインブラウザツリーで、ICAP 検索サービスを実行する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ます。
   - サイドバーから [検索オプション] → [ストレージ検索サービス] の順に選択します。
   - メインメニューから [実行] → [ストレージ検索サービス] の順に選択します

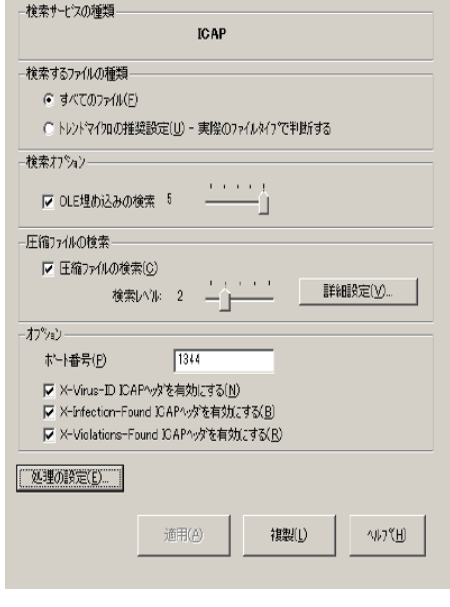


図 3-47. ICAP 検索サービスの設定

3. [検索するファイルの種類] グループで、次のいずれか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、33 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。
4. 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。
5. 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。
6. [オプション] で、次の操作を実行します。
   - [ポート番号] にポート番号を入力します。スキャンサーバは、このポート番号を使用して ICAP クライアントから ICAP サーバへの接続を待ち受けます。
   - ["X-Virus-ID" ICAP ヘッダを有効にする] をオンにします。ウイルスが検出されると、ICAP 応答に X-Virus-ID ICAP 拡張子ヘッダが追加されます。
   - ["X-Infection-Found" ICAP ヘッダを有効にする] をオンにします。ウイルスが検出されると、ICAP 応答に X-Infection-Found ICAP 拡張子ヘッダが追加されます。
   - ["X-Violations-Found" ICAP ヘッダを有効にする] をオンにします。ウイルスが検出されると、ICAP 応答に X-Violations-Found ICAP 拡張子ヘッダが追加されます。
7. [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。詳細については、124 ページの「ICAP 検索サービスでのウイルスに対する処理の定義」を参照してください。
8. [適用] をクリックして変更を保存します。

ICAP 検索サービスの設定を複製するには

1. ドメインブラウザツリーで、ICAP 検索サービスを実行する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ます。
   - サイドバーから [検索オプション] → [ストレージ検索サービス] の順に選択します。
   - メインメニューから [実行] → [ストレージ検索サービス] の順に選択します。
3. [複製] をクリックします。

[設定の複製先サーバの選択] 画面が表示されます。

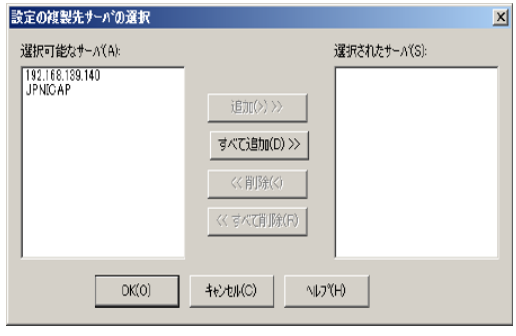


図 3-48.　設定の複製

4. [選択可能なサーバ] から一般サーバを 1 つ以上選択します。一般サーバを複数選択するには、<Ctrl> キーを押しながら選択します。

注意： [選択可能なサーバ] に表示される一般サーバの検索サービスの種類は、元の一般サーバの検索サーバの種類と同じです。

5. 次のいずれかの操作を実行します。
   - [追加] をクリックして、選択した一般サーバを [タスクを実行するサーバ] に追加します。
   - [選択可能なサーバ] 内のすべての一般サーバを [タスクを実行するサーバ] に追加するには、[すべて追加] をクリックします。
6. [OK] をクリックします。

注意： この手順では、ポート番号は複製されません。

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。

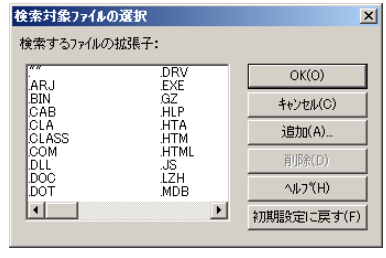


図 3-49. [検索対象ファイルの選択] ダイアログボックス

2. 次のいずれかの操作を実行してください。
   - [追加] 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。

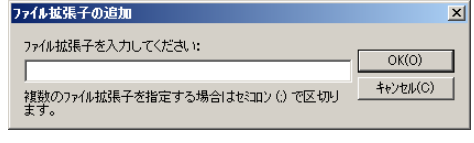


図 3-50. [ファイル拡張子の追加] ダイアログボックス

     検索対象ファイルの拡張子を入力し、[OK] をクリックします。
   - 初期設定値を使用する場合は、[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)	.BIN	.CAB	.CLA
.ARJ	.COM	.DLL	.DOC
.CLASS	.DRV	.EXE	.GZ
.DOT	.HTA	.HTM	.HTML
.HLP	.LZH	.MDB	.MPP
.JS	.MSG	.OCX	.OFT
.MPT	.PIF	.POT	.PPS
.OVL	.RAR	.RTF	.SCR
.PPT	.SYS	.TAR	.VBS
.SHS	.VST	.XLA	.XLS
.VSD	.Z	.ZIP	
.XLT			

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

検索対象ファイルの拡張子を除外するには、次の手順に従ってください。

1. 左のサイドバーから [検索オプション] → [検索除外リスト] の順に選択します。
2. メインメニューから [設定] → [検索オプション] → [検索除外リスト] の順に選択します。
3. [検索対象から除外するファイル拡張子] で [追加] 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。

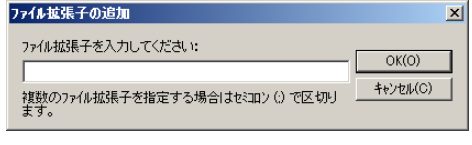


図 3-51. [ファイル拡張子の追加] ダイアログボックス

4. 検索から除外するファイルの拡張子を入力します。複数のファイル拡張子を指定する場合は、セミコロン (;) で区切ります。
5. [OK] をクリックします。

6. 既に入力したファイル拡張子を削除するには、該当するファイル名を [検索対象から除外するファイル拡張子] から選択し [削除] をクリックします。
7. [適用] ボタンをクリックします。

Control Manager への登録

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。

ServerProtect を Control Manager に統合するには、この製品を Control Manager に登録する必要があります。Control Manager の詳細については、154 ページの「Trend Micro Control Manager とは」を参照してください。

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

1. Windows の [スタート] メニューで [Trend Micro ServerProtect 管理コンソール] をクリックします。
2. 次のいずれかの操作を実行してください。
   - サイドバーで [Control Manager エージェントの設定] をクリックします。
   - メインメニューから [実行] → [Control Manager (CM) エージェントの設定] の順に選択します。

[Control Manager エージェントの設定] 画面が表示されます。

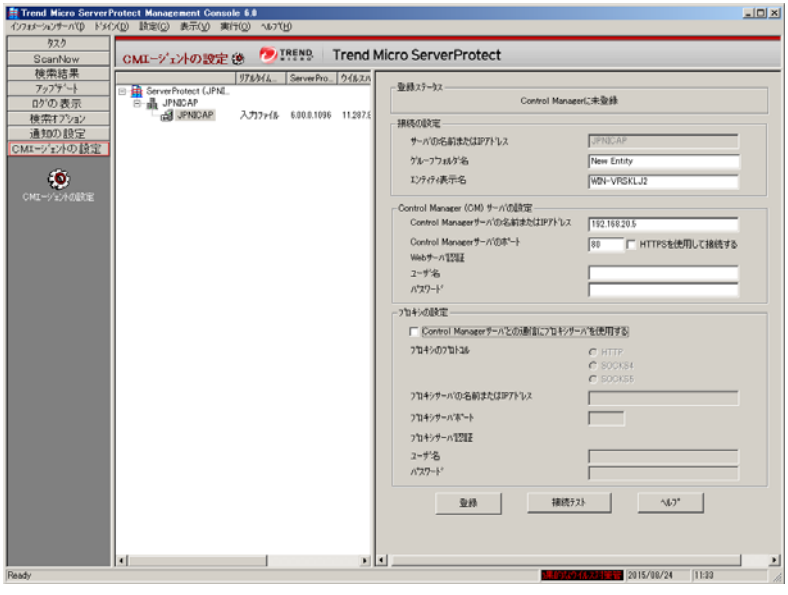


図 3-52.　[Control Manager エージェントの設定] 画面

3. サーバの　[登録ステータス] が　[Control Manager に未登録] であることを確認します。
4. 右画面の　[接続の設定] で、次のフィールドに情報を入力します。
   - [グループフォルダ名]: Control Manager 製品ツリーで ServerProtect を識別するための分かりやすい名前を入力します。グループフォルダ名の最大長は 19 文字です。
   - [エンティティ表示名] : ServerProtect インフォメーションサーバの名前を入力します。この名前は ServerProtect インフォメーションサーバを識別するために Control Manager サーバの製品ディレクトリに表示されるものなので、慎重に指定してください。一意の分かりやすい名前を指定すると、Control Manager の製品ディレクトリで ServerProtect サーバを見つけやすくなります。エンティティの表示名の最大長は 64 文字です。

注意：　[サーバの名前または IP アドレス] フィールドには、ServerProtect がインストールされたコンピュータのホスト名または IP アドレスが自動的に入力されます。

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

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

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

6. Trend Micro Control Manager サーバへのアクセスにプロキシサーバを使用する場合は、[プロキシの設定] で [Control Manger サーバとの通信にプロキシサーバを使用する] を選択して、次の情報を設定します。
   - [プロキシのプロトコル] : プロキシのプロトコルを選択します。
   - [プロキシサーバの名前または IP アドレス] : プロキシサーバの名前または IP アドレスを入力します。
   - [プロキシサーバポート] : プロキシサーバのポート番号を入力します。
   - [ユーザ名] および [パスワード]: プロキシサーバで認証が必要な場合は、プロキシサーバ用のユーザ名とパスワードを入力します。

   ヒント： [登録] ボタンをクリックする前に [接続テスト] ボタンをクリックして、指定した内容で ServerProtect から Control Manager サーバに接続できるかどうか確認することを強くお勧めします。

7. [接続テスト] をクリックして、入力した情報を使用して ServerProtect から Control Manager サーバに接続できるかどうかを確認します。ServerProtect から Control Manager サーバに接続

できない場合は、入力した設定を確認してください。また、ServerProtect コンピュータと Control Manager サーバとの接続状態も確認してください。

8. 設定を保存して ServerProtect コンピュータを Control Manager に登録するには、[登録] をクリックします。

Control Manager での ServerProtect ステータスの確認

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

1. Web ブラウザで次の URL を指定します。

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

   <Control Manager のサーバ名 > は Control Manager サーバの IP アドレスまたはホスト名です。

2. メニューバーで [製品] をクリックします。
3. ツリー内で、ServerProtect の Control Manager への登録時に入力したグループフォルダ名を展開します。
4. 登録したサーバがリストにあるかどうかを確認します。

Control Manager からの登録解除

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

1. Windows の [スタート] メニューで [Trend Micro ServerProtect 管理コンソール] をクリックします。
2. 次のいずれかの操作を実行してください。
   - サイドバーで [Control Manager エージェントの設定] をクリックします。
   - メインメニューから [実行] → [Control Manager (CM) エージェントの設定] の順に選択します。

     [Control Manager エージェントの設定] 画面が表示されます。
3. [登録解除] をクリックします。

第 4 章

体験版および ServerProtect for Storage のトラブルシューティング

ServerProtect は、シリアルをお持ちでない場合に、体験版として使用できます。本章では、体験版からのアップグレードおよび ServerProtect for Storage のトラブルシューティングについて紹介します。

本章で説明する内容には、次の項目が含まれます。

ServerProtect 体験版のアップグレード

ソフトウェアの自動アップデート機能とテクニカルサポートを活用するには、登録バージョンの ServerProtect for Storage にアップグレードしてください。体験版 ServerProtect を製品版 ServerProtect にアップグレードする方法の詳細については、付録を参照してください。

RPC 検索サービスを実行する ServerProtect for Storage のトラブルシューティング

ここでは、よくある質問と、その解決に役立つトラブルシューティング情報を提供します。

NetApp デバイスで ServerProtect for Storage スキャンサーバが認識されない

説明 :

NetApp デバイスに電源を投入した後、ServerProtect for Storage スキャンサーバからイベント 213が返されます。このイベントの説明は次のとおりです。

NetApp デバイスに接続を追加できません。ネットワークパスが見つかりませんでした。「vscan scanners」コマンドを NetApp デバイスで実行すると、次のメッセージが返されます。

```
"No virus scanners are registered with the device."
```

RPC 検索サービスを実行する ServerProtect for Storage では、継続してパターンファイルアップデートをトレンドマイクロのアップデートサーバから取得できます。

解決策 :

次の条件が満たされていることを確認してください。

- RPC (リモートプロシージャコール) がサーバで有効になっている
- Vscan が NetApp デバイスで「オン」になっている
- CIFS (Common Internet File System) の初期設定共有 (C$) が存在している

上記の条件について確認したら、次の操作を実行します。

1. スキャンサーバを右クリックし、ドメインブラウザツリーから [デバイスリスト] を選択します。[デバイスリスト] 画面が表示されます。
2. リストから NetApp デバイスを 1 つ以上選択します。NetApp デバイスを複数選択するには、<Ctrl> キーを押しながら選択します。
3. [ログオン情報] をクリックします。[ログオン情報] 画面が表示されます。
4. 情報が正しいことを確認します。正しくなければ、再入力してください。

5. [OK] をクリックします。

上記の手順を実行したら、NetApp デバイスでスキャンサーバの登録を繰り返します。管理者アカウントのパスワードを変更した直後は、NetApp デバイスの電源を投入して起動するまで変更内容が有効にならないことがあります。

大きなファイルを NetApp デバイスで検索すると、スキャンサーバでファイルの検索は完了するが、元のリクエストが失われてしまう

説明 :

RPC 検索サービスを実行する ServerProtect for Storage で大きなファイルを NetApp デバイスにおいて検索すると、次のメッセージが表示されます。

```
"[Server] completed scan on [FileName] but original request was not found."
```

解決策 :

ファイルのサイズが大きすぎて検索時間がタイムアウトすると、この現象が発生します。NetApp デバイスとスキャンサーバとの間のタイムアウト時間を長くすることで、この問題を解決してください。

NetApp デバイスとスキャンサーバとの間のタイムアウト時間を長くするには、スキャンサーバで次の手順を実行してください。

1. Regedit を実行します。
2. 次のキーを参照します。

   ```
   HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ServerProtect¥CurrentVersion¥Engine¥Devices
   ```

3. 種類が DWORD である「ScanDeviceTimeOut」のデータ値を適切なタイムアウト時間に設定します。

「ScanDeviceTimeOut」値の単位は秒です。この値は、スキャンサーバがファイルを検索する際のタイムアウト値になります。

注意 : ServerProtect での初期設定のタイムアウト時間は 24 秒です。

この警告を無効にするには、種類が DWORD である「ScanTimeOutLog」を次の場所に追加します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ServerProtect¥CurrentVersion¥Engine¥Devices
```

「ScanTimeOutLog」に指定可能な値は次のとおりです。

1: タイムアウトにより検索されなかったファイルをログに記録します。

0: タイムアウトにより検索されなかったファイルをログに記録しません。

RPC 検索サービスを実行する ServerProtect for Storage を設定してすべての種類のファイルを検索する

説明 :

すべての種類のファイルを検索するように ServerProtect for Storage を設定する方法を教えてください。

解決策 :

NetApp デバイス上のすべてのファイルを検索するには、NetApp デバイスの拡張子欄の内容を変更します。これにより、すべてのファイル拡張子がサポートされるようになります。

NetApp デバイスの拡張子欄ですべての種類のファイルがサポートされるようにするには、NetApp デバイスのコマンドプロンプトで次を入力します。

```
filer> vscan extensions add ???
```

注意 : これにより、拡張子に関係なく、NetApp デバイスですべての種類のファイルが検索されるようになります。NetApp デバイスのワイルドカードは疑問符 (?) です。アスタリスク (*) ではありません。

NetApp デバイスの拡張子欄にファイル拡張子を追加するには、NetApp デバイスのコマンドプロンプトで次を入力します。

```
filer> vscan extensions add vbs
```

これにより、拡張子が「.VBS」のファイルが NetApp デバイスで検索されるようになります。「vbs」の部分は任意の 3 文字の拡張子で置換できます。

すべてのファイルを検索すると、NetApp デバイスのパフォーマンスが低下し、ウイルス検索時間が長くなることがあります。ウイルスに感染しやすいファイルを検索することをお勧めします。

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 か所から実施できるため、ウイルス対策およびファイルセキュリティ戦略を、より効率的に管理できます。

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

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

本章で説明する内容には、次の項目が含まれます。

Trend Micro Control Manager 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 Management Communication Protocol について

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

MCP には次の新機能があります。

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

ネットワーク負荷とパッケージサイズの低減

TMI は XML ベースのアプリケーションプロトコルを使用します。XML のプロトコルデザインにはある程度の拡張性と柔軟性がありますが、通信プロトコルのデータ形式の標準として XML を採用すると、次の点で不利益が生じます。

- CGI の名前 / 値のペアやバイナリ構造などの他のデータ形式と比べて、XML の解析にはより多くのシステムリソースが必要となります (プログラムがサーバやデバイスに大きな負荷を与えます)。
- XML では、情報の伝送に必要なエージェントの負荷が他のデータ形式に比べて格段に大きくなります。
- データが必要とするリソースが多いため、データ処理のパフォーマンスが低くなります。
- 他のデータ形式に比べてパケット伝送に時間がかかり、伝送速度が遅くなります。
- MCP のデータ形式は、これらの問題を解決するために考案されました。MCP のデータ形式は BLOB (バイナリ) ストリームで、各項目は名前 ID、型、長さ、および値で構成されています。

この BLOB 形式には次の利点があります。

- **XML よりも小さいデータ転送サイズ** — 各データ型で、情報の格納に必要なバイト数が抑えられます。このデータ型には、整数型、符号なし整数型、ブール型、浮動小数点型があります。

- **解析の高速化** — 固定バイナリ形式を使用して、各データ項目を 1 つずつ簡単に解析できます。XML に比べてパフォーマンスが数倍高くなります。
- **設計の柔軟性の向上** — 各項目は名前 ID、型、長さ、および値で構成されており、設計の柔軟性も考慮されています。項目の順序は任意で、補助項目は必要な場合にのみ通信プロトコルに含めることができます。

データ伝送にバイナリストリーム形式を採用したことに加えて、圧縮 / 非圧縮に関係なく、一度の接続で複数の種類のデータをパックして送信できます。このデータ転送形式により、ネットワーク帯域幅を温存でき、スケーラビリティも向上します。

NAT およびファイアウォールトラバーサルのサポート

IPv4 ネットワーク上の限定された IP アドレスを使用して、より多くのエンドポイントコンピュータをインターネットに接続するために、NAT (ネットワークアドレス変換) デバイスが広く使用されています。NAT デバイスは、NAT デバイスに接続するコンピュータへのプライベート仮想ネットワークを形成することによりこれを可能にします。NAT デバイスに接続する各コンピュータには、専用のプライベート仮想 IP アドレスが 1 つ割り当てられます。NAT デバイスは、このプライベート IP アドレスを実際の IP アドレスに変換してからインターネットに要求を送信します。これにより問題が起こる場合があります。接続している各コンピュータは仮想 IP アドレスを使用していますが、多くのネットワークアプリケーションがそのことを認識していないためです。これは通常、予期しないプログラムの不具合やネットワーク接続の問題を引き起こします。

Control Manager 2.5/3.0 以上のエージェントと連携する製品には 1 つの前提条件があります。サーバは、サーバからエージェントへの接続を開始することでエージェントに到達できるという事実に依存しています。どちら側からでも相互にネットワーク接続を開始できるので、これは双方向通信製品と呼ばれます。この前提条件は、エージェントが NAT デバイスの背後にある場合や、Control Manager サーバが NAT デバイスの背後にある場合には当てはまりません。この接続は NAT デバイスにのみルーティング可能で、NAT デバイスの背後にある製品や、NAT デバイスの背後にある Control Manager サーバにはルーティングできないためです。この問題の一般的な解決方法の 1 つとして、NAT デバイス上に特定のマップ関係を構築し、受信要求を各エージェントに自動的にルーティングする方法があります。ただし、この解決方法ではユーザの関与が必要となり、大規模な製品配置が必要な場合はうまく機能しません。

MCP では、一方向通信モデルを採用することでこの問題に対応します。一方向通信では、エージェントのみがサーバへのネットワーク接続を開始できます。サーバはエージェントへの接続を開始できません。この一方向通信はログのデータ転送に適しています。一方、サーバからのコマンド発行は、受動モードで実行されます。つまり、コマンド配信は、エージェント側からサーバに対して使用可能なコマンドのポーリングが行われて初めて実現します。

HTTPS のサポート

MCP 統合プロトコルでは、業界標準の通信プロトコル (HTTP/HTTPS) が採用されています。

HTTP/HTTPS には TMI に比べて次の利点があります。

- IT 部門の大多数のスタッフが HTTP/HTTPS に精通しているため、通信に関する問題の特定やその解決方法の調査が容易になります。
- ほとんどの企業環境では、パケットを通過させるためにファイアウォールで新しいポートを開く必要がありません。
- SSL/TLS や HTTP ダイジェスト認証など、HTTP/HTTPS 用に構築された既存のセキュリティメカニズムを使用できます。

MCP を使用することで、次の 3 つのセキュリティレベルを Control Manager に適用できます。

- **低** — HTTP 通信が使用されます。
- **中** — HTTPS がサポートされている場合は HTTPS 通信が使用され、HTTPS がサポートされていない場合は HTTP 通信が使用されます。
- **高** — HTTPS 通信が使用されます。

一方向および双方向通信のサポート

MCP では一方向および双方向通信がサポートされます。

一方向通信

NAT トラバーサルは、現在のネットワーク環境において、より重要な問題になっています。この問題に対応するため、MCP では一方向通信を使用します。一方向通信では、Control Manager エージェントが接続を開始し、サーバからのコマンドをポーリングします。それぞれの要求は CGI に類似したコマンドクエリまたはログの送信です。ネットワークへの影響を軽減するために、接続は可能な限り開かれたまま維持されます。以降の要求では既存の開かれた接続が使用されます。接続が閉じられた場合でも、同じホストへの SSL 対応のすべての接続は、セッション ID のキャッシュ機能により、再接続にかかる時間が大幅に短縮されます。

双方向通信

双方向通信は、一方向通信に代わる方法です。一方向通信を基本としながら、サーバからの通知を受信するチャネルが追加されています。この追加チャネルも HTTP プロトコルに基づいています。双方向通信では、Control Manager エージェントによるサーバからのコマンド受信とその処理のリ

アルタイム性が向上します。Control Manage エージェント側では、Control Manager サーバからの通知を受信するために、CGI に類似した要求を処理できる Web サーバまたは CGI 互換のプログラムが必要です。

クラスタノードのサポート

管理者はさまざまなケースで、特定の製品インスタンスを 1 つの論理ユニットにグループ化したり、クラスタ化したりすることが必要になる場合があります (たとえば、クラスタ環境にインストールされた製品で、インストール済みのすべての製品インスタンスを 1 つのクラスタグループにまとめる場合など) 。しかし、Control Manager サーバの観点からは、正式な登録手順を経た製品インスタンスはそれぞれ独立した管理ユニットとみなされ、各管理ユニットはどれも違いがありません。MCP を使用する場合、Control Manager ではクラスタノードがサポートされます。

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。

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。

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。

- 手動検索の実行 (ScanNow の開始)
- 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。

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

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

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

サポートサービスについて

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

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

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービスの継続をご希望される場合は、契約満了前に更新されることをお勧めします。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.com/ja-jp/enterprise/default.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

トレンドマイクロ「セキュリティ情報」

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/jp/security-intelligence/index.html`

管理コンソールからセキュリティ情報 Web 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 Web 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不正プログラム情報検索サイト「セキュリティデータベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

```
http://about-threats.trendmicro.com/ThreatEncyclopedia.aspx?language=jp
```

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

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

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

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

脅威解析・サポートセンター TrendLabs (トレンドラボ)

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

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

付録 A

製品版へのアップグレードとよくある質問

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

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

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

本章で説明する内容には、次の項目が含まれます。

[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。

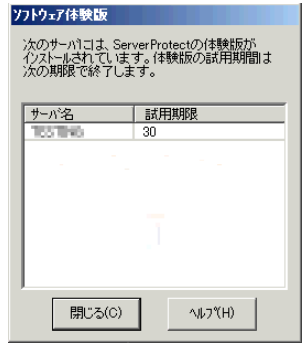


図 A-1.　[ソフトウェア体験版] ダイアログボックス

シリアル番号リストの確認

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

シリアル番号リストを表示するには、次の手順に従ってください。

1. メインメニューから [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。

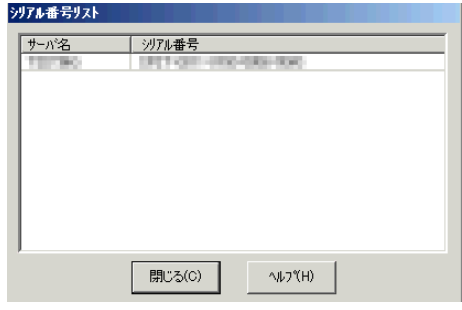


図 A-3.　シリアル番号リスト

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] をクリックして変更内容を保存します。

よくある質問

Virus Scan for NetApp デバイス

- **ServerProtect では、NetApp デバイス内のウイルスを検出できないのに、その他の場所では検出できるのはなぜですか。**

  ウイルス検索対象のファイル拡張子を NetApp デバイス上で指定する必要があります。NetApp デバイスのコンソールで、「vscan」コマンドを使用して、現在登録されているファイル拡張子を確認できます。

- **ServerProtect では、検索除外リストに追加済みのディレクトリ / ファイルが検索されるのはなぜですか。**

  ServerProtect では、NetApp デバイス上で検索除外リストに追加されているディレクトリ / ファイルであっても、NetApp デバイスによって要求されたすべてのファイルが検索されます。

- **NetApp デバイスに接続しているのに、デバイス上のウイルスを検索できません。**

  Vscan が NetApp デバイスで有効になっているかどうかを確認してください。Vscan を有効にすると、すべての Vfiler 上でのウイルス検索も有効になります。

- **各 Vfiler 上でウイルス検索を有効にするにはどうしたらいいですか。**

  Vscan が NetApp デバイスで有効になっているかどうかを確認してください。Vscan を有効にすると、すべての Vfiler 上でのウイルス検索も有効になります。

注意： NetApp 向けの ServerProtect for Storage の問い合わせ先および技術サポート提供は販売店となります。詳しくは、製品ページをご覧ください。
http://www.go-tm.jp/spfs

ServerProtect のアップグレード

- **ServerProtect を以前のバージョンにロールバックできますか。**

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

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

ServerProtect のウイルス検索

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

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

- **書込み禁止リストが機能しません。**

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

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

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

- **ログの詳細情報の結果に、駆除不能なウイルスであっても、そのウイルスが駆除可能と表示されます。**

  [処理の設定] 画面で [処理] が [ウイルス駆除] に設定されている場合、ウイルスは正確に駆除可能または駆除不能と表示されます。ただし、[処理] が [ウイルス駆除] に設定されていない場合、ログの詳細情報では、ウイルスは常に駆除可能と表示されます。

その他

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

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

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

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

- **システムトレイに一般サーバのアイコンが見当たりません。**

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

- **一般サーバのパターンファイルと検索エンジンが表示されません。**

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

- **Admin.ini の「ExcludeUNCPath」を有効にしても、検索除外リストに任意の文字を登録できません。**

  ExcludeUNCPath が Admin.ini で有効にされていても、ユーザアクセス制御 (UAC) が有効になっていると管理コンソールに設定が反映されない場合があります。ExcludeUNCPath の詳細については、以下の製品 Q&A を参照してください。
  http://esupport.trendmicro.com/solution/ja-JP/1306534.aspx

- **Windows ログインアカウントのパスワードを空白にすると、ServerProtect にログイン失敗のエラーが表示されるのはなぜですか。**

  Windows の初期設定ではユーザアカウントの制限があり、空白のパスワードではリモートログインが許可されないため、Windows ログインアカウントのパスワードが設定されていない場合、ServerProtect にログイン失敗のエラーが表示されます。

索引

英数字

あ

か

さ

た

は

ら