TREND MICRO™

ServerProtect™ for Storage 6.0 Patch 3

クイックスタートガイド

※注意事項

複数年契約について

・お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。

・複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

https://success.trendmicro.com/ja-JP/solution/KA-0009810

法人向け製品のサポートについて

・法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。

・法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

著作権について

本ドキュメントに関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が事前に承諾している場合を除き、形態および手段を問わず、本ドキュメントまたはその一部を複製することは禁じられています。本ドキュメントの作成にあたっては細心の注意を払っていますが、本ドキュメントの記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本ドキュメントおよびその記述内容は予告なしに変更される場合があります。

商標について

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

先得、Trend Micro One、Workforce One、Security Go、Dock 365、TrendConnect、TREND MICRO FORUM、トレンドマイクロ知恵袋、Trend Cloud One、Trend Service One、および Accelerating You は、トレンドマイクロ株式会社の登録商標です。

本ドキュメントに記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

Copyright © 2025 Trend Micro Incorporated. All rights reserved.

P/N: SPEM69975/250121_JP(2025/04)

プライバシーと個人データの収集に関する規定

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

トレンドマイクロ ServerProtect により収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次の Web サイトを参照してください。

https://www.go-tm.jp/data-collection-disclosure

重要

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

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

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

目次

第 1 章：トレンドマイクロ ServerProtect の使い方を始める

トレンドマイクロ ServerProtect の紹介 3

ServerProtect のしくみ 3

ServerProtect のサーバ管理方法 4

サーバ間の通信方法 4

ServerProtect アーキテクチャ 5

管理コンソール 5

インフォメーションサーバ 6

インフォメーションサーバに関する注意点 6

一般サーバ 7

ServerProtect ドメイン 8

ServerProtect for Storage アーキテクチャの概要 9

RPC 検索サービスを実行する ServerProtect for Storage 9

7-Mode での製品アーキテクチャ 9

Cluster-Mode での製品アーキテクチャ 10

構成の概要 13

EMC CAVA スキャナーを使用した ServerProtect for Storage アーキテクチャ概要 14

構成の概要 17

EMC VNX/VNXe の特別な機能 18

ICAP 検索サービスを実行する ServerProtect for Storage 19

感染したファイルに対する処理 19

配信 20

リアルタイム検索と手動検索 (ScanNow) 21

タスクの使用 22

ウイルスを検出した場合 23

ログと検索結果 25

アップデートファイルの配信 26

ウイルス検出技術 27
パターンマッチング 27
MacroTrap 28
MacroTrap の動作原理 28
圧縮ファイル 29
ダメージクリーンナップサービス 30
OLE 埋め込みの検索 30
トレンドマイクロの推奨設定 31
トレンドマイクロの推奨処理 32
ActiveAction を選択するタイミング 32
マップされたネットワークドライブの検索 33
その他の機能 33
集中管理 33
インストール時のネットワークセキュリティ 33
ウイルスアウトブレークへの迅速な対応 33
感染ファイルに対する柔軟な処理 34
NetworkTrap ツール 34
最新のウイルス検索技術 34
ウイルス検索の統計 34
互換性 34

第 2 章：ServerProtect for Storage をインストールしています

システム要件 39
インストール計画 39
インストール環境の特定 39
ServerProtect コンポーネントによって使用されるポート番号 43
WAN 接続のネットワーク 45
ServerProtect のインストール 45
インストールを開始する前に 45
ServerProtect パッケージのインストール 46
インフォメーションサーバのインストール 51
管理コンソールのインストール 54
一般サーバのインストール 58
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 58

管理コンソールからの一般サーバのインストール 62
サイレントモードで ServerProtect をインストールする ... 64
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 67
EMC CAVA スキャナーを使用した ServerProtect for Storage のインストール 68
EMC CAVA スキャナーを使用した ServerProtect for Storage をインストールする前に 68
EMC CAVA スキャナーを使用した ServerProtect for Storage のインストール 69
ServerProtect のアンインストール 70
一般サーバの削除 70
インフォメーションサーバのアンインストール 70
管理コンソールのアンインストール 70

第 3 章：ServerProtect の管理

管理コンソールとは 75
管理コンソールを開く 75
管理コンソールのメイン画面 76
メインメニュー 77
サイドバー 78
ドメインブラウザツリー 80
設定データ領域 82
管理する ServerProtect ドメイン 82
ServerProtect ドメインの新規作成 83
ServerProtect ドメイン名の変更 (リネーム) 85
ServerProtect ドメインの削除 85
ドメイン間での一般サーバの移動 86
インフォメーションサーバの管理 86
インフォメーションサーバの選択 87
一般サーバの管理 88
ドメイン間での一般サーバの移動 88
一般サーバの移動 89

スキャンサーバにおける NetApp デバイスの管理 89
NetApp 7-Mode デバイスを追加中 90
Cluster-Mode AV Connector の追加 92
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 94
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 95
NetApp 7-Mode デバイスまたは Cluster-Mode AV Connector のオプションの設定 96
NetApp 7-Mode デバイスまたは Cluster-Mode AV Connector の情報の更新 96
一般サーバとしてのスキャンサーバの使用 97
感染時の NetApp デバイスクライアントへの通知 100
NetApp デバイスのステータスの表示 101
NetApp デバイスの RPC 接続に関するステータス通知の設定 102
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 103
スキャンサーバの ICAP クライアントリストの管理 103
ICAP クライアントからの検索リクエストを受け入れる .. 103
ICAP クライアントの ICAP クライアントリストへの追加 104
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 105
アップデートの設定 105
コンポーネントのアップデート 105
ダウンロードと配信の流れ 107
アップデートファイルの現行バージョンの表示 108
アップデートファイルのダウンロード 110
ダウンロード元の設定 110
トレンドマイクロのアップデートサーバをダウンロードソースとして設定する 111
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として設定 111
ダウンロード元フォルダの作成 112
ダウンロードの実行 113

予約ダウンロードの設定 114
ダウンロードオプションの設定 115
ダウンロードの設定を構成する 115
プロキシサーバ設定 116
アップデートファイルの配信 118
配信の設定 118
予約配信の設定 120
以前の配信処理のロールバック 121
タスクの管理 124
ServerProtect タスクウィザード 124
初期設定のタスク 125
新規タスクの作成 126
タスクを作成します 126
予約タスクの作成 127
手動検索対象の指定 129
初期設定タスクの作成 130
既存のタスクリストを表示する 131
既存タスクの実行 133
既存のタスクの変更 133
既存タスクの変更 133
既存のタスクの実行対象サーバを変更する 134
既存のタスクのタスク定義を変更する 135
既存タスクの表示 136
既存のタスクの削除 138
通知メッセージの設定 138
一般の警告 139
通知イベント 139
一般の警告の設定 139
アウトブレークアラート 141
アウトブレークアラートの設定 141
警告方法の設定 143
インターネットメール (メール) 警告を送信するための設定 144
一般サーバのウイルス検索 145
ウイルスに対する処理の設定 147

検索プロファイル 149
スキャンプロファイルの保存 149
スキャンプロファイルの削除 150
ストレージデバイスのウイルス検索 151
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 152
ICAP 検索サービスでのウイルスに対する処理の定義 154
リアルタイム検索 155
リアルタイム検索の設定 156
手動検索 (ScanNow) 159
ScanNow 検索の設定 160
ScanNow ツールの実行 (Windows 一般サーバ) 164
ScanNow ツールを実行する 164
ScanNow ツールを停止する 164
予約検索 (タスク検索) 165
予約検索の設定 165
RPC 検索サービスの使用 166
RPC 検索サービスの設定 166
RPC 検索サービスの設定の複製 168
EMC CAVA 検索サービスの使用 170
EMC CAVA 検索サービスの設定 170
EMC CAVA 検索サービスの設定の複製 174
ICAP 検索サービスの使用 176
ICAP 検索サービスの設定 176
ICAP 検索サービスの設定の複製 179
検索対象ファイルの種類 (拡張子) の選択 180
スキャン対応ファイル拡張子 182
ファイル拡張子を検索対象から除外する 184

第 4 章：既存の ServerProtect のアップグレード

ServerProtect アップグレード機能の概要 187
インストールパッケージを使用した、ServerProtect のローカルアップグレード 188
インストールパッケージを使用した、ServerProtect のリモートアップグレード 190
サイレントモードインストールの実行による一般サーバのアップグレード 191
サイレントモードでのインストール 191
ServerProtect for NetApp または EMC Celerra のアップグレード 194
ServerProtect 体験版のアップグレード 195
の RPC スキャナーを使用した ServerProtect のトラブルシューティング 195

第 5 章：ServerProtect を Trend Micro Control Manager で管理する

Control Manager 統合サマリー 200
Trend Micro Control Manager に登録する 201
Control Manager での ServerProtect ステータスの確認 204
Control Manager からの登録解除 204

第 6 章：テクニカルサポート

トラブルシューティングのリソース 208
サポートポータルの利用 208
脅威データベース 208
製品サポート情報 208
サポートサービスについて 209
トレンドマイクロへのウイルス解析依頼 209
メールレピュテーションについて 210
ファイルレピュテーションについて 210
Web レピュテーションについて 210
その他のリソース 211
最新版ダウンロード 211

付録 A：ServerProtect 製品版へのアップグレード

[ソフトウェア体験版] ダイアログボックス 214
シリアル番号リストの確認 214
シリアル番号の入力 216
よくある質問 217
Virus Scan for NetApp デバイス 217
ServerProtect のアップグレード 218
ServerProtect のウイルス検索 219
その他 219

索引

索引 221

第 1 章

トレンドマイクロ™ServerProtect™の使い方を始める

注意

本ドキュメントは英語版を翻訳したものです。翻訳ソフトウエアにより機械的に翻訳した内容が含まれます。

最新の情報は英語版のページでご確認ください。表示言語は、画面右上の言語名をクリックして切り替えられます。

本章で説明する内容には、次の項目が含まれます。

- 3 ページの「トレンドマイクロ™ServerProtect™の紹介」
- 3 ページの「ServerProtect のしくみ」
- 5 ページの「ServerProtect アーキテクチャ」
- 21 ページの「リアルタイム検索と手動検索 (ScanNow)」
- 22 ページの「タスクの使用」
- 23 ページの「ウイルスを検出した場合」
- 25 ページの「ログと検索結果」
- 26 ページの「アップデートファイルの配信」

- 27 ページの「ウイルス検出技術」
- 33 ページの「その他の機能」

トレンドマイクロ™ServerProtect™の紹介

トレンドマイクロ™ServerProtect™は、企業ネットワーク上のファイルサーバを保護するための受賞歴のある最新世代のソフトウェアです。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。ServerProtect は新しいファイル感染を検出し、既存ファイル内のウイルスを識別し、サーバまたはワークステーションに未知のウイルスがネットワーク環境に侵入したことを示す活動を検出します。

ServerProtect では、複数の Microsoft Windows および Novell NetWare ネットワーク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、同一ドメイン内にあるサーバを同時に設定したり、すべてのサーバについてのウイルスに関する総合的なレポートを作成することができます。

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

トレンドマイクロ 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。

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。

サーバ間の通信方法

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

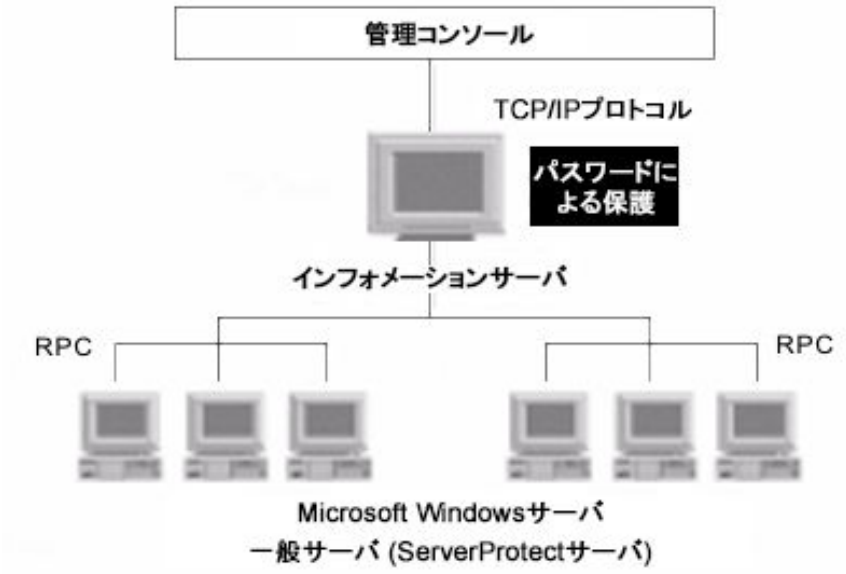


図 1-1. ServerProtect の 3 層アーキテクチャ

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。 管理コンソールには次の部分があります。

- 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。58 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

ベンチマークテストの結果、情報サーバは最大 250 台の通常サーバを管理できることが確認されました。この数値はレファレンス/参照情報としてのみ使用されます。情報サーバは、利用可能な帯域幅に応じて、より多くの通常サーバを管理することができます。

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。これらのサーバは、システムの実際のウイルス対策機能を実行し、情報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を使用します。58 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。
- 管理コンソールの使用。62 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。

- サイレントモードを使用しています。64 ページの「サイレントモードで ServerProtect をインストールする」を参照してください。

記載されている各インストール方法は、特定の会社のニーズに合わせて調整できます。58 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。

警告!

セットアッププログラムからサーバーを個別にインストールするのは時間がかかるため、トレンドマイクロは ServerProtect 管理コンソールからサーバーをインストールすることを推奨します。

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 ServerProtect ドメインを作成することができます。 詳しくは 82 ページの「管理する ServerProtect ドメイン」を参照してください。

警告!

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

ServerProtect ドメインには次の機能があります。

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

注意

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

ServerProtect for Storage アーキテクチャの概要

ServerProtect for Storage は、ServerProtect ファミリーの 2 つの製品、ServerProtect for Network Appliance devices と ServerProtect for EMC Celerra を統合します。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検索サーバが管理されます。

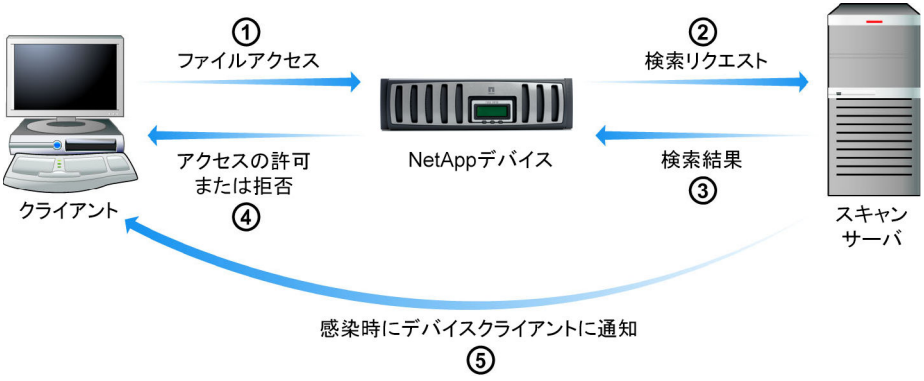


図 1-2. ServerProtect for Storage 製品アーキテクチャ 7-Mode

ユーザが NetApp 7-Mode デバイスでファイルにアクセスしたり新しいファイルを保存しようとすると、NetApp 7-Mode デバイスはウイルスチェックを実行します。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 (Scan Now) 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。

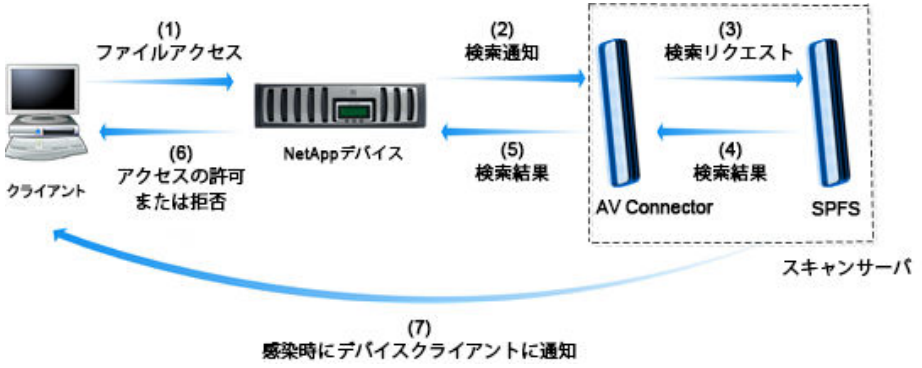


図 1-3. ServerProtect for Storage 製品アーキテクチャ (クラスターモード)

Cluster-Mode では、ユーザがファイルにアクセスしたり、新しいファイルを NetApp Cluster-Mode デバイスに保存しようとすると、Cluster-Mode デバイスがウイルスチェックを行います。ファイル名の拡張子がファイル検索基準 (例えば、".EXE"や".VBS"ファイル) に一致する場合、Cluster-Mode デバイスは Cluster-Mode AV コネクタに検索通知を送信します。Cluster-Mode AV コネクタは検索要求 (今すぐ検索) を検索サーバに送信します。検索サーバは検索結果を Cluster-Mode AV コネクタに返し、Cluster-Mode AV コネクタはそれを Cluster-Mode デバイスに送信します。検索結果に応じて、ユーザはファイルを開く、保存する、またはアクセスを拒否されることがあります。

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、31 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。

ファイルにウイルスが含まれている場合、ServerProtect for Storage は指定されたアクションを実行します。検索アクションの詳細については 145 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。例えば、ファイルがクリーン可能であり、ServerProtect for Storage がクリーンアクションを実行するように設定されている場合、次のことが発生します。

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検索サーバを「信頼」します。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検索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。リアルタイム検索を「入出力ファイル」に設定するには、155 ページの「リアルタイム検索」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。

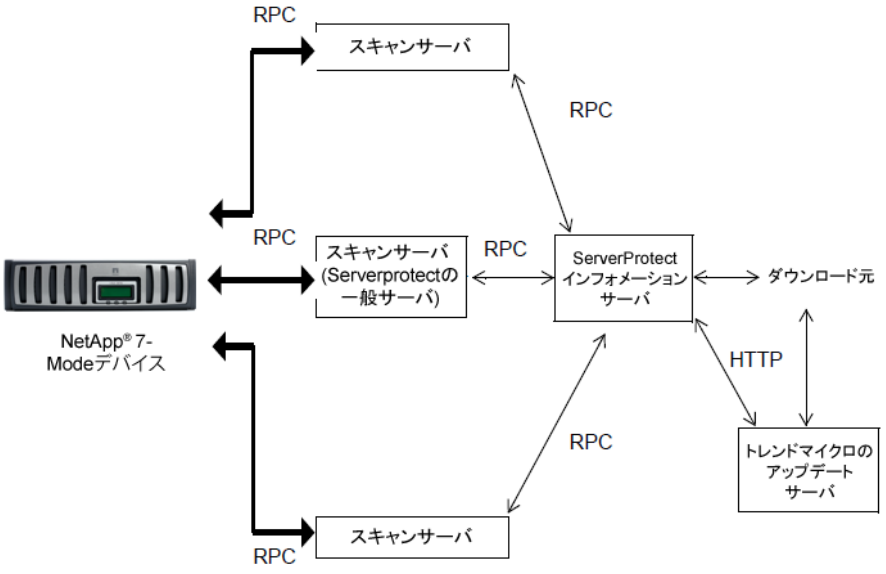


図 1-4. ServerProtect for Storage の 7-Mode における組織フロー

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。

EMC CAVA スキャナーを使用した ServerProtect for Storage アーキテクチャ概要

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、ファイルサーバではなく、別の AV サーバで行われます。これにより、ウイルス検索がファイルサーバの処理能力に影響を与えないようにします。複数の AV サーバをファイルサーバに接続することで、検索の負荷が均等に分散されます。検索要求とファイルは AV サーバに「ラウンドロビン」方式で送信されます。これにより、負荷が均等に分散され、検索性能が向上します。

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。

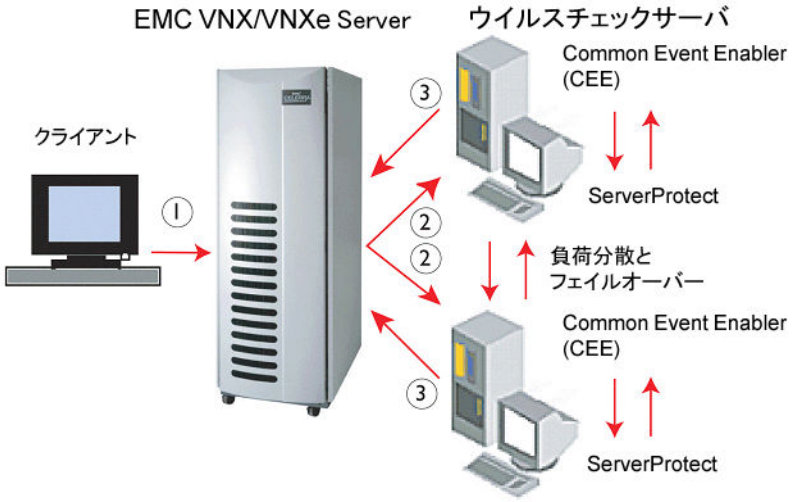


図 1-5. EMCCAVA スキャナーアーキテクチャを使用した ServerProtect for Storage

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. EMC VNX/VNXe 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 ファイルサーバを保護することが SPFS の主な目的です。SPFS では、ウイルススキャンは「オンアクセス」モードで行われ、Windows Server 2008、2012、2016、2019、2022、または 2025 を実行している別のマシン (AV サーバ) で行われます。AV サーバはファイルサーバを保護します。これは通常版の ServerProtect とは異なり、通常のサーバを保護することに重点を置いています。

注意

Microsoft Windows サーバ 2008 および 2008 R2 は、Storage 6.0 Patch 3 の ServerProtect 以降サポートされなくなりました。

クライアントがサーバ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 サーバの 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。

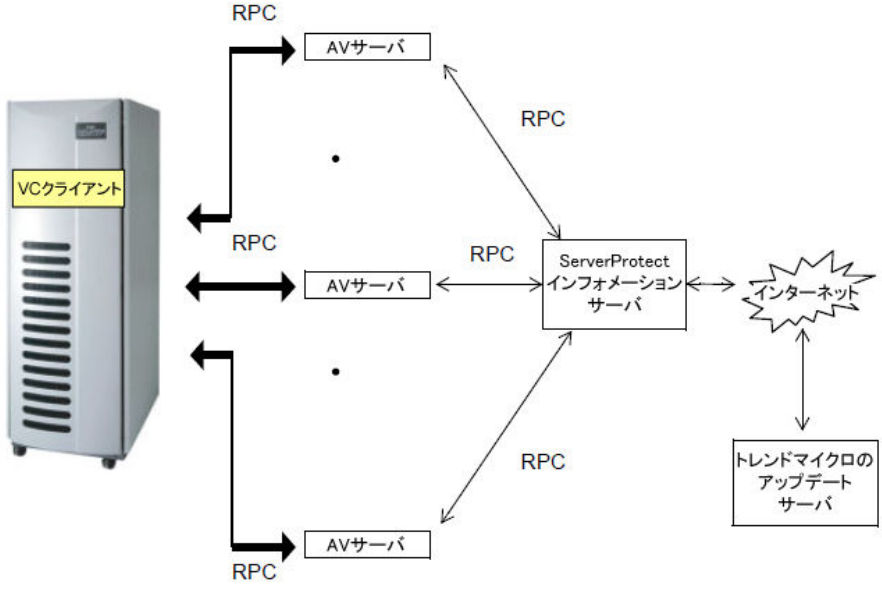


図 1-6. ServerProtect for EMC Celerra 構成フロー

ServerProtect は次の機能を実行します。

- CEE と連携することで、EMC VNX/VNXe File Server の AV サーバになります
- EMC 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 サーバは検索要求を受信します。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、155 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。
- [名前変更]: 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!

トレンドマイクロは、[放置]アクションを使用するのではなく、[ウイルス駆除]、[削除]、[隔離]アクションのみを使用することを推奨します。ファイルが感染しており、ウイルスアクションが[放置]に設定されている場合、ファイルは EMC VNX/VNXe ファイルサーバシステムに入った後も感染したままになります。

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対して複数の検索サーバーを展開できます。 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。

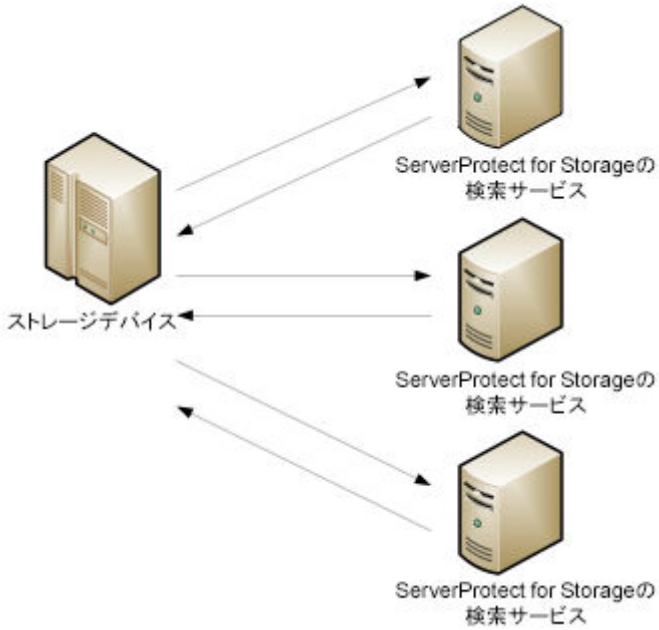


図 1-8. ストレージデバイスから複数の ServerProtect ICAP 検索サービスに検索リクエストを送信可能

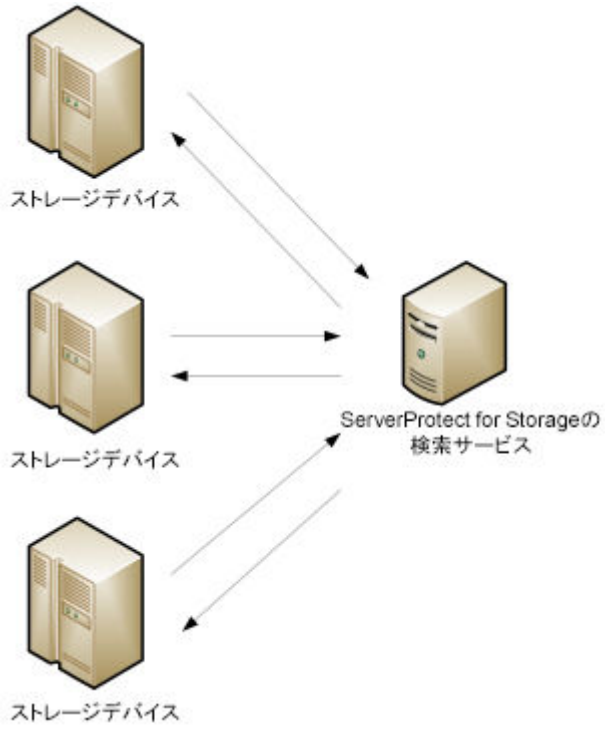


図 1-9. ServerProtect ICAP 検索サービスで複数のストレージデバイスからの検索リクエストを処理可能

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で継続的に実行され、ウイルス保護の最大レベルを提供します。サーバ上のすべてのファイル I/O イベントが監視され、感染したファイルがサーバにコピーされたり、サーバからコピーされたりするのを防ぎます。155 ページの「リアルタイム検索」を参照してください。

今すぐ検索は手動のウイルス検索です (つまり、起動後すぐに実行されます)。今すぐ検索を使用して、コンピュータウイルスにさらされた可能性がある、

または即座に情報が必要なサーバを確認してください。159 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]: デフォルトでは、リアルタイム検索はファイルを検索するように設定されています。これにより、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。145 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。 145 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/消去/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、タスクの維持を担当する「タスクオーナー」に割り当てられます。124 ページの「タスクの管理」を参照してください。

ServerProtect をサーバに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) が既に存在します。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 は、感染ファイルに対してソフトウェアが取るアクションの種類を設定することができます。以前のバージョンで提供されていたウイルス対策保護に加えて、ServerProtect 5.8 ではスパイウェアパターンファイルが利用可能になり、独自のウイルスカテゴリを形成します。特定の種類のウイルスを処理するための具体的なアクション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、ジェネリッククリーン機能を含むことでより強力になりました。

処理には、次の 5 種類があります。

- [放置]: 手動検索の場合、ServerProtect はファイルをスキップし、修正措置を行いません。ただし、ウイルスの検出はプログラムのログエントリに記録されます。リアルタイム検索の場合、検索方向が[出力]または[受信 & 送信]に設定されている場合、ServerProtect はファイルを「書き込み拒否」として扱い、複製や変更から保護します。詳細は 147 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]: 感染したファイルは削除されました。
- [拡張子変更]: 感染したファイルの拡張子は.vir に変更されます。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。駆除前にファイルのバックアップを作成することができます。

  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、オンラインヘルプの「ログ情報の表示」トピックおよび 147 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

[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

64 ビット OS では、ServerProtect は 32 ビットウイルスと 64 ビットウイルスの両方を検出します。

注意

ServerProtect 5.8 はスパイウェアに感染したファイルに対するクリーンアクションをサポートしていません。ActiveAction を使用する場合、スパイウェアに感染したファイルに適用されるアクションの実際の効果は[放置]アクションと同等になります。

注意

ICAP スキャナの場合、ServerProtect ストレージ専用[ウイルス駆除]そして[ブロック]感染ファイルに対する処理。

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 は、スキャン、ファイル更新、および結果の展開に関する包括的な情報を提供します。さらに、ServerProtect は、情報をログファイルとして保存し、参照または出力することができます。たとえば、ネットワーク上のウイルススキャンに関するスキャン統計を分析することができます。これらの統計には、最も一般的なウイルスや、ネットワークにウイルスを導入したユーザに関する情報が含まれます。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。

各通常サーバでは、ServerProtect はログデータベースファイルがデフォルトのサイズ制限である 10MB を超えるか、設定された日数を経過した場合にバックアップをサポートします。ログファイルのデフォルトサイズは 10,000 エントリ、または最大 10MB です。ログファイルが 10,000 エントリまたは 10MB を超えた場合、どちらか小さい方のサイズで、ServerProtect は自動的にログファイルの名前を変更し、新しいログファイルを作成します。ただし、ServerProtect は設定されていない限り、日数制限を課しません。ログバックアップの設定に関する情報は、オンラインヘルプの**ログデータベースバックアップオプションの設定**トピック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。ウイルスログに関する詳細は、オンラインヘルプの「ログ情報の表示および情報サーバログの表示」トピックを参照してください。

アップデートファイルの配信

トレンドマイクロは、トレンドマイクロアンチウイルスソフトウェアのアップグレードおよびアップデート配信モジュールです。トレンドマイクロソフトウェアのメンテナンスを簡素化し、ネットワークのアンチウイルスセキュリティの総コストを削減します。毎月開発されるウイルスの数が多いため、効果的なウイルス対策ポリシーは、最新の脅威に対応できるウイルスパターンファイルおよび検索エンジンファイルの使用に依存しています。105 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]:トレンドマイクロには、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。ServerProtect アップデート用バージョン 5.8 には、新たに追加されたスパイウェアパターンファイルやその他の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、ダメージクリーンナップテンプレート、およびルートキット対策ドライバが含まれます。
- [スケジュールされた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]: インフォメーションサーバを指定して、トレンドマイクロ アップデートサイトからアップデートをダウンロードさせ、他のサーバがそれ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の互換性]: 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。

- [ログ情報を更新]: ServerProtect によって、アップデート処理に関するすべての活動がログファイルに記録され、将来の参照のために利用できます。
- [ロールバックオプション]: 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、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。110 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. ダウンロードした更新をネットワーク上の他の通常サーバーに展開します。118 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が節約されます。

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。126 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 は高度なウイルス検出技術を使用しています。このセクションでは、この最先端技術をサポートするツールと、IT 専門家がどのようにそれを活用できるかを紹介します。

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。

そのようなウイルスが見つかった場合、ServerProtect は以前に指定した方法で対処します。ServerProtect ウイルスのアクションには、[ウイルス駆除](自動クリーン)、[削除]、[放置](無視)、[隔離](移動)、または[拡張子変更]が含まれます。ウイルスのアクションは、ブートウイルスとファイルウイルスの両方に対してカスタマイズできます。145 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

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を最新の状態に保つことが重要です。毎年千以上の新しいウイルスが作成されています。トレンドマイクロは、スケジュールされた更新をサポートすることでパターンファイルの更新を簡単にします。詳細は 120 ページの「予約配信の設定」をご覧ください。

MacroTrap™

ServerProtect では、トレンドマイクロの MacroTrap™技術を採用し、Microsoft™ Office ファイルとテンプレート内の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。マクロウイルスは最も急速に拡散するコンピュータウイルスです。これらのウイルスは、電子メールで頻繁にやり取りされるファイルに潜んでいるため、簡単に拡散します。MacroTrap の設定情報については 156 ページの「リアルタイム検索の設定」を参照してください。

注意

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

MacroTrap の動作原理

MacroTrap は、ドキュメントに関連付けられて保存されているすべてのマクロコードをルールベースで検査します。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*.dot)。トレンドマイクロ MacroTrap は、このドキュメントをチェックして、ウイルスのようなアクションを実行する命令を探します。ウイルスのようなアクションの例としては、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) などがあります。

圧縮ファイル

圧縮ファイルアーカイブ (つまり、多くの個別の圧縮ファイルで構成された単一のファイル) は、メールやインターネットでファイルを配布するための好ましい形式です。一部のウイルス対策ソフトウェアはこれらの種類のファイルを検索できないため、圧縮ファイルアーカイブは保護されたネットワークやコンピュータにウイルスを「密輸」する方法として使用されることがあります。

トレンドマイクロ検索エンジンは圧縮アーカイブ内のファイルを検索できます。さらに、他の圧縮ファイルで構成された圧縮ファイルも最大 5 層まで検索できます。

ServerProtect で使用しているトレンドマイクロの検索エンジンで対応する圧縮形式には、次の形式が含まれます。

- ARJ (.arj) および ARJ_SFX (.exe)
- BINHEX
- BASE64
- CABINET (.cab)
- DIET (.com)
- GNU ZIP (.gz)
- LHA (.lzh) および LHA_SFX (.exe)
- LZEXE (.exe)
- Microsoft Office Open XML 形式 (.docx, .xlsx, .pptx, .one)
- PKLITE (.exe または.com)
- PKZIP (.zip) および PKZIP_SFX (.exe)

- RAR (.rar)
- TAR
- UNIX COMPACKED (.z)
- UNIX LZW (.Z)
- UNIX PACKED (.z)
- UUENCODE

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。

圧縮ファイルの構成情報については、156 ページの「リアルタイム検索の設定」および 160 ページの「ScanNow 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™ Object Linking and Embedding (OLE) を使用すると、Microsoft Office™ファイルを自分自身の中に埋め込むことができます。つまり、Excel スプレッドシートの中に Microsoft Word 文書を持つことができ、その Excel

スプレッドシートを Microsoft™ PowerPoint プレゼンテーションに埋め込むことができるということです。

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。この問題に対処するために、トレンドマイクロは最先端の ServerProtect ウイルス保護を補完する新しい検索機能「OLE レイヤー検索」を追加しました。145 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。 トレンドマイクロ 推奨する検索レベルは、手動検索 (ScanNow) の場合は 2、リアルタイム検索の場合は 1 です。 検索レベルを低く設定すると、サーバのパフォーマンスが向上します。

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。145 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、サーバー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。160 ページの「ScanNow 検索の設定」 を参照してください。

トレンドマイクロの推奨処理

ウイルスの処理または特定のウイルスに対して最適な検索処理が不明な場合は、トレンドマイクロの推奨処理を使用することをお勧めします。検索の実行とリアルタイム検索の両方に対して ActiveAction を設定できます。

ActiveAction を選択するタイミング

トレンドマイクロ は、ウイルス処理に不慣れな場合や、特定のウイルスに最適な検索処理が不明な場合に、トレンドマイクロの推奨処理を選択することをお勧めします。

ウイルスはそれぞれ大きく異なるため、各ウイルスの種類に応じた適切な処理が必要です。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。このため、トレンドマイクロは ActiveAction の使用を推奨します。

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。

- [検索時間の短縮]: 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。
- [メンテナンスからの解放]: トレンドマイクロの推奨処理では、推奨された検索処理を使用するため、処理の失敗を心配することなく、他の作業に専念できます。
- [更新可能な検索処理]: トレンドマイクロには、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の新しい ActiveAction スキャンアクションが含まれています。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。

ActiveAction の構成情報については、147 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。

マップされたネットワークドライブの検索

ServerProtect は 1 つまたは複数のネットワークドライブを検索できます。共有ネットワークフォルダはこの機能を選択する前にマッピングする必要があります。これは、リアルタイム検索がローカルドライブと同様にマッピングされたドライブを検索して保護するため、感染のリスクを減らすのに役立ちます。156 ページの「リアルタイム検索の設定」を参照してください。

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 サーバで使用できます。

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。138 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。

NetworkTrap ツール

特定のウイルスは、できるだけ多くの接続されたユーザを感染させるために共有フォルダを積極的に探します (このタイプのウイルスの例としては `PE.FunLove.4099` があります)。NetworkTrap ツールを使用すると、フォルダを共有し、Bait フォルダの内容を新しく作成された共有フォルダに自動的にコピーします (Bait フォルダにはウイルスが感染しやすいファイルが含まれています)。この共有フォルダは、新しいウイルス通知と連携して効果的なウイルストラップを作成します。このトピックの詳細については、オンラインヘルプの「NetworkTrap ツール」セクションを参照してください。

最新のウイルス検索技術

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

ウイルス検索の統計

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

互換性

ServerProtect は、Microsoft Windows Server 2008、2008 R2、2012、2012 R2、2016、2019、2022、および 2025 の OS に対応しています。また、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。

注意

Microsoft Windows Server 2008 および 2008 R2 は、Storage 6.0 Patch 3 に対して ServerProtect 以降サポートされなくなりました。

ServerProtect は 32 ビットおよび 64 ビットの OS と互換性があります。ServerProtect は 32 ビットおよび 64 ビットの Windows サーバを自動的に検出します。 OS が 32 ビットの場合、ServerProtect の一般サーバコンポーネントの 32 ビットバイナリ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 の一般サーバコンポーネントの 64 ビットバイナリ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 をインストールしています

この章には、ネットワーク上に ServerProtect for Storage を正常にインストールするための以下の情報が含まれています。

- 39 ページの「システム要件」
- 39 ページの「インストール計画」
- 45 ページの「ServerProtect のインストール」
- 67 ページの「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」
- 68 ページの「EMC CAVA スキャナーを使用した ServerProtect for Storage のインストール」
- 70 ページの「ServerProtect のアンインストール」

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

トレンドマイクロは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

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。

https://success.trendmicro.com/ja-JP/solution/KA-0016321

注意

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。

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、45 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

トレンドマイクロ ServerProtect では Microsoft Windows および Novell NetWare 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、管理下の一般サーバを管理するために少なくとも 1 つの ServerProtect ドメインを持っている必要があります。8 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。6 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。

注意

Microsoft Windows サーバ 2008 および 2008 R2 は、Storage 6.0 Patch 3 の ServerProtect 以降、サポートされていません。

表 2-1. Microsoft Windows 環境でのインストール

OS	インフォメーションサーバ	一般サーバ	管理コンソール
Windows Server 2008 ファミリ (32 ビット)	○	○	○
Windows Server 2008 ファミリ (64 ビット)	○ (WOW64)	○	○ (WOW64)
Windows Server 2008 Core (32 ビット)	いいえ	○	いいえ
Windows Server 2008 Core (64 ビット)	いいえ	○	いいえ
Windows Server 2008 R2 ファミリ	○ (WOW64)	○	○ (WOW64)
Windows Server 2012 ファミリ	○ (WOW64)	○	○ (WOW64)
Windows Server 2012 R2 ファミリ	○ (WOW64)	○	○ (WOW64)
Windows Server 2016 ファミリ	○ (WOW64)	○	○ (WOW64)
Windows Server 2019 ファミリ	○ (WOW64)	○	○ (WOW64)
Windows Server 2022 ファミリ	○ (WOW64)	○	○ (WOW64)
Windows Server 2025 ファミリ	○ (WOW64)	○	○ (WOW64)

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 Vista デスクトップファミリ	いいえ	いいえ	○
Windows 7 デスクトップファミリ	いいえ	いいえ	○
Windows 8 デスクトップファミリ	いいえ	いいえ	○
Windows 10 デスクトップファミリ	いいえ	いいえ	○
Windows 11 デスクトップファミリ	いいえ	いいえ	○

注意

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 10 デスクトップファミリとは、Windows 10、Windows 10 Pro、Windows 10 Enterprise を指します。

Windows 11 デスクトップファミリとは、Windows 11、Windows 11 Pro、Windows 11 Enterprise を指します。

Windows Server 2008 ファミリおよび Windows Server 2008 R2 ファミリとは、Standard、Enterprise、Storage、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 Server 2012 R2 ファミリの両方は、Standard、Essentials、Foundation、Storage、および Datacenter Server の各エディションを指します。

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

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

Windows Server 2022 ファミリとは、Standard、Essentials、IoT、および Datacenter Server の各エディションを指します。

Windows Server2025 ファミリとは、Standard、Essentials、IoT、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 または 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
  - TCP プロトコルの場合はポート 1000～1009 を開きます

    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。
- インフォメーションサーバによって使用されるファイアウォール設定
  - TCP プロトコルの場合はポート 5005～5014 を開きます。

    ポート 5005 は管理コンソールからのコマンドを受信するために使用されます。通常、ポート 5005 を開く必要があります。特定のプログラムが使用している場合は、5006 から 5014 の間で使用可能なポートを見つけてファイアウォールを開いてください。
  - UDP プロトコルの場合は 3000～3009 を開きます

    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。
  - 137～139 および 445 を名前付きパイプ経由の RPC のために開きます
    - 137 (UDP)

- 138 (UDP)
- 139 (TCP)
- 445 (TCP)

注意

これらのポートは、ServerProtect が名前付きパイププロトコルを介してリモートプロシージャコール (RPC) を使用して通信できるように開かれています。

- 3628 (TCP) を開きます

  ポート 3628 は、イベント応答メッセージの受信に使用されます。

- Netware で SPX/TCP のために 1921 を開く

  ポート 1921 は、SPX/TCP プロトコルを介して Netware と通信するために使用されます。

- 一般サーバがインストールされている Windows コンピュータのファイアウォール設定
  - インフォメーションサーバからの待ち受け TCP/IP 経由の RPC の場合は 5168 を開きます

    ポート 5168 は、インフォメーションサーバからのコマンドの受信に使用されます。

  - 名前付きパイプの場合は 137～139 および 445 を開きます。
    - 137 (UDP)
    - 138 (UDP)
    - 139 (TCP)
    - 445 (TCP)
- 通常サーバを使用した Netware マシンのファイアウォール設定
  - ポート 9921 (SPX/TCP) を開きます

このポートは、インフォメーションサーバからのコマンドの受信に使用されます。

WAN 接続のネットワーク

ServerProtect は、WAN 全体の複数の場所から管理できます。ただし、必要なネットワークパフォーマンスを確保するため、トレンドマイクロは、管理するノーマルサーバと同じネットワークドメインのワークグループ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。

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 がインストールされたことがない、またはすでにアンインストールされたサーバネットワークシステムの場合、ユーザは管理コンソール、情報サーバ、通常サーバのインストールを含む完全な ServerProtect パッケージのインストールを選択することをお勧めします。この方法でインストールされたプログラムは、ServerProtect がすぐに運用可能であり、インストール操作自体が簡単かつスムーズに実行されることを保証します。

このセクションでは、ServerProtect 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 ServerProtect をよくお読みください。39 ページの「インストール計画」を参照してください。

注意

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

ServerProtect パッケージのインストール

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

手順

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。

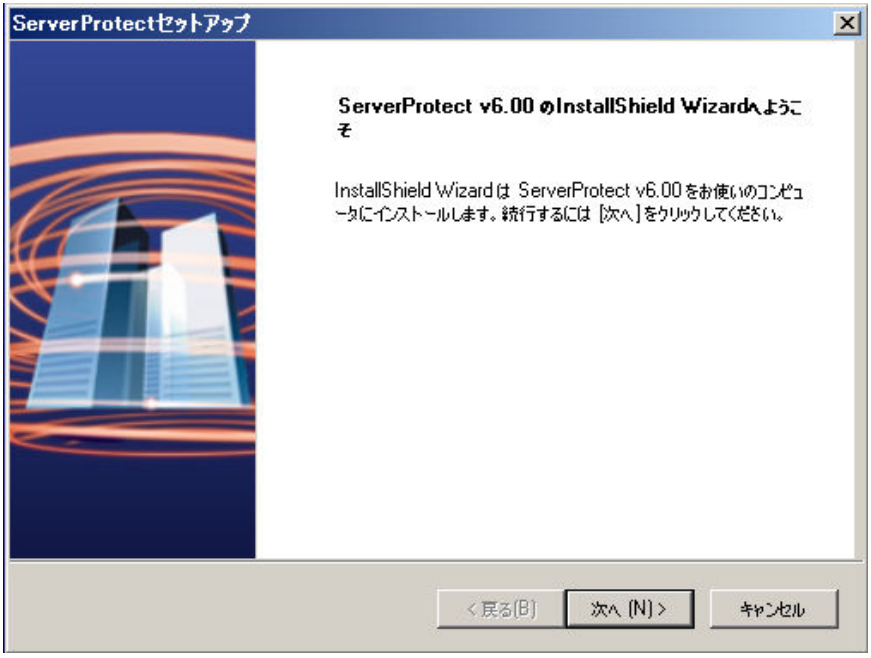


図 2-1. ServerProtect セットアップの初期画面

2. [次へ] をクリックします。 [使用許諾契約書] 画面が表示されます。 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。

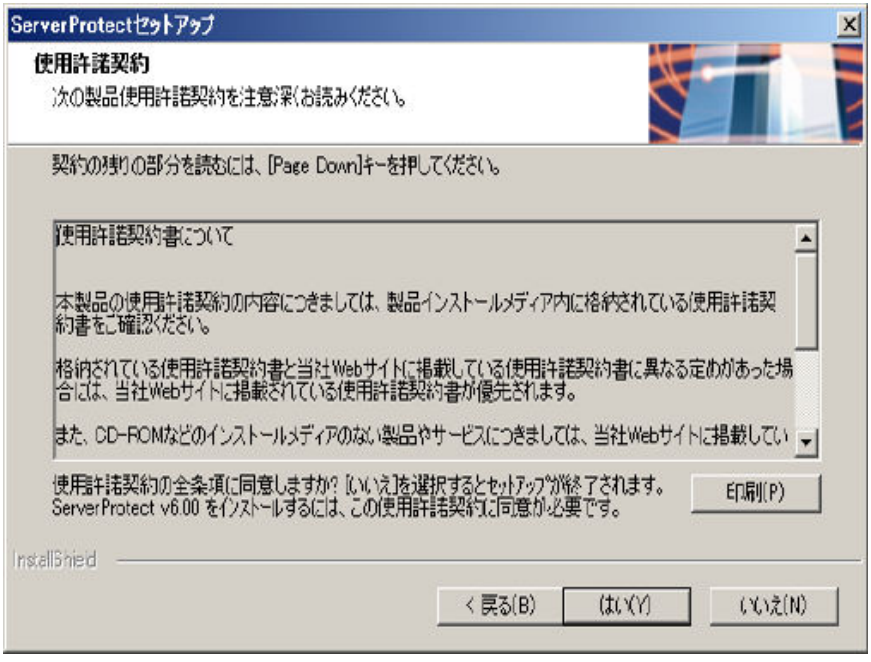


図 2-2. 使用許諾契約書

3. [[○]] をクリックします。 ServerProtect 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。

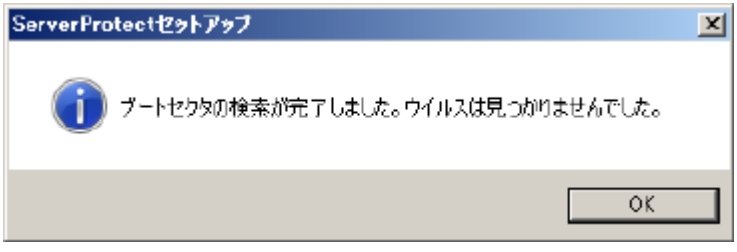


図 2-3. ウイルス検索の結果ウィンドウ

4. [OK]をクリックして続行します。[ユーザの情報]画面が表示されます。

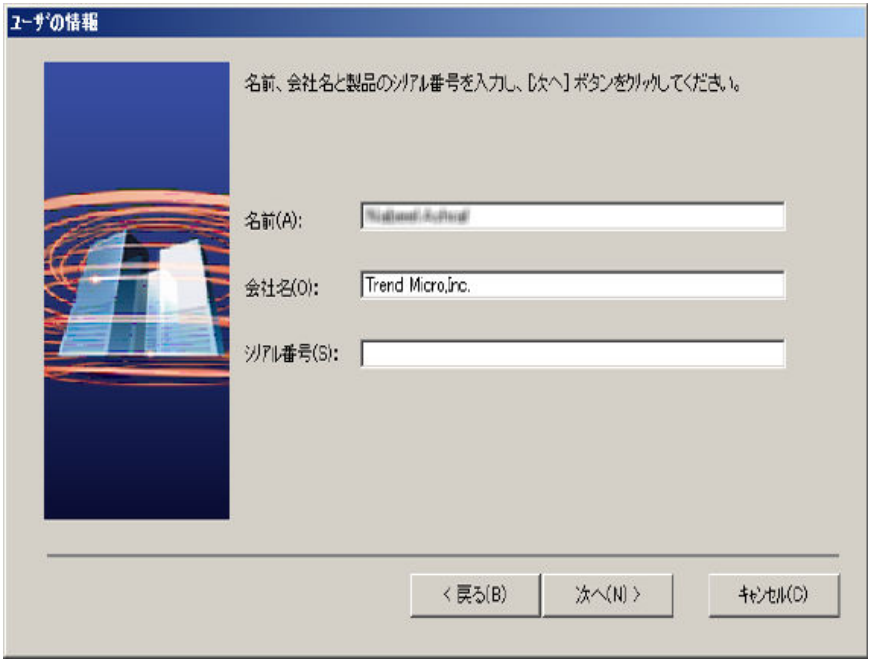


図 2-4. ユーザの情報

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。ServerProtect 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. [次へ]をクリックして続行します。[コンポーネントの選択]画面が表示されます。

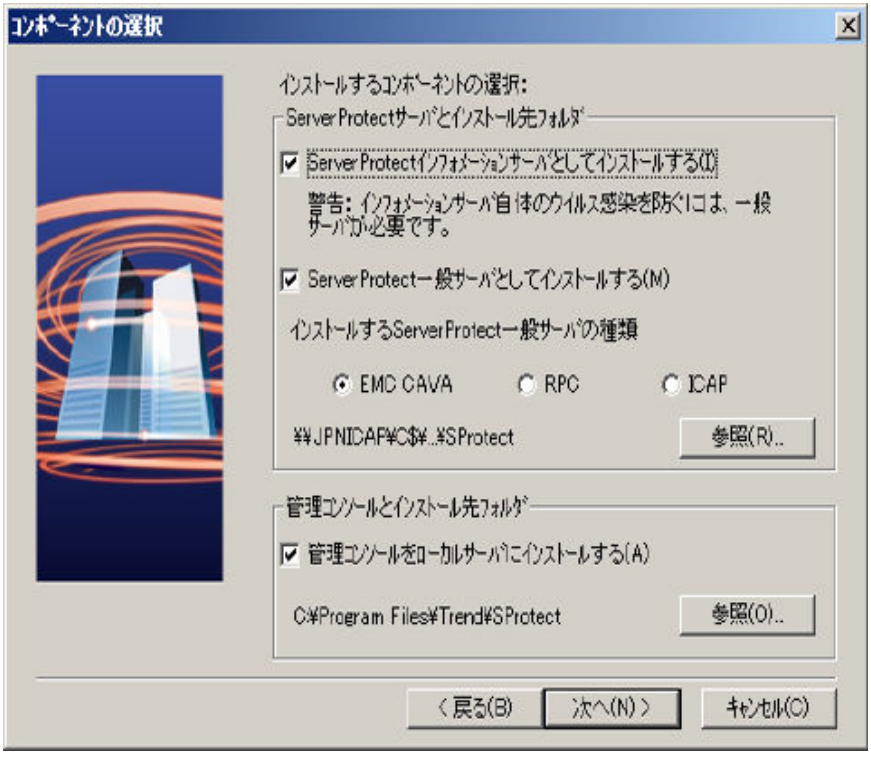


図 2-5. コンポーネントの選択

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選択してください。

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。

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。

Huawei OceanStor Storage を保護したい場合は、[EMC CAVA]を選択してください。

詳細については、68 ページの「EMC CAVA スキャナーを使用した ServerProtect for Storage のインストール」を参照してください。

目的のセットアップに対してコンポーネントの選択が適切であることを確認してください。[C$]や[D$]などの隠し共有ストレージデバイスを宛先フォルダーとして選択できます。

初期設定のインストールパスは次のとおりです。

```
<drive>:¥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 [◯] 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. [次へ]をクリックします。通常サーバまたは情報サーバのいずれかをインストールすることを選択した場合、[ログオン情報の入力]画面が表示されます。[ログオン情報]の下に、[ドメイン名]、[ユーザ名]、[パスワード]、[パスワードの確認入力]フィールドに適切なデータを入力します。続行するには[次へ]をクリックします。

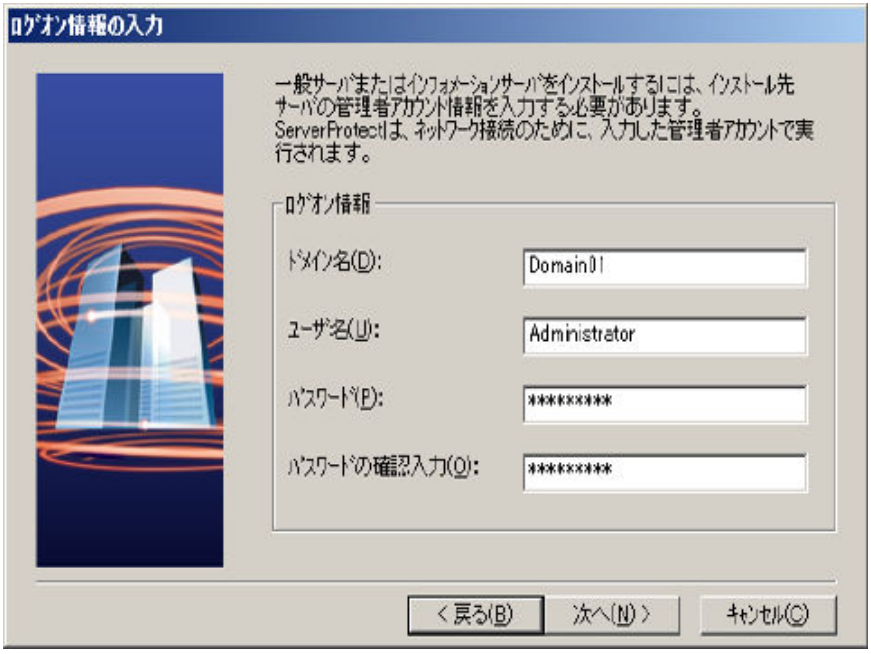


図 2-6. ログオン情報の入力

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。

手順

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選択します。49 ページの ServerProtect コンポーネント選択画面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] 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。

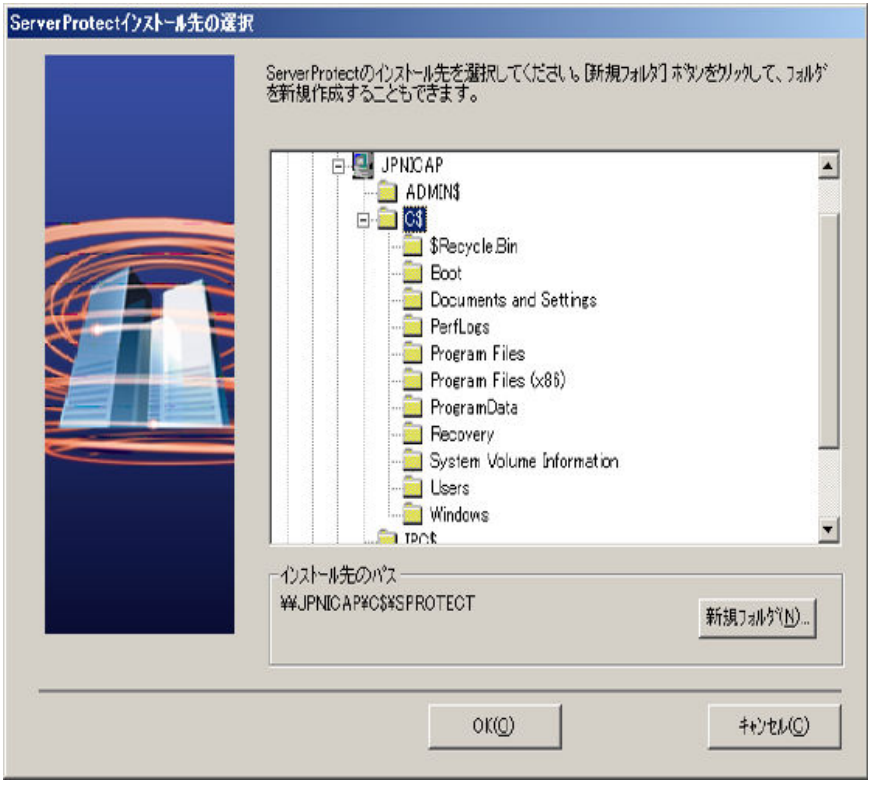


図 2-7. ServerProtect インストール先の選択

4. ターゲットサーバをダブルクリックし、ServerProtect Information Server ファイルのインストールパスを選択します。インストールを新しいフォルダに行う必要がある場合は、[新しいフォルダ]をクリックします。[コンポーネントの選択]画面に戻るには[OK]をクリックします。49 ページの ServerProtect コンポーネント選択画面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]の下で、[ドメイン名]、[ユーザ名]、[パスワード]、[パスワ

ードの確認入力]のフィールドに有効なデータを入力し、[次へ]をクリックします。[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。

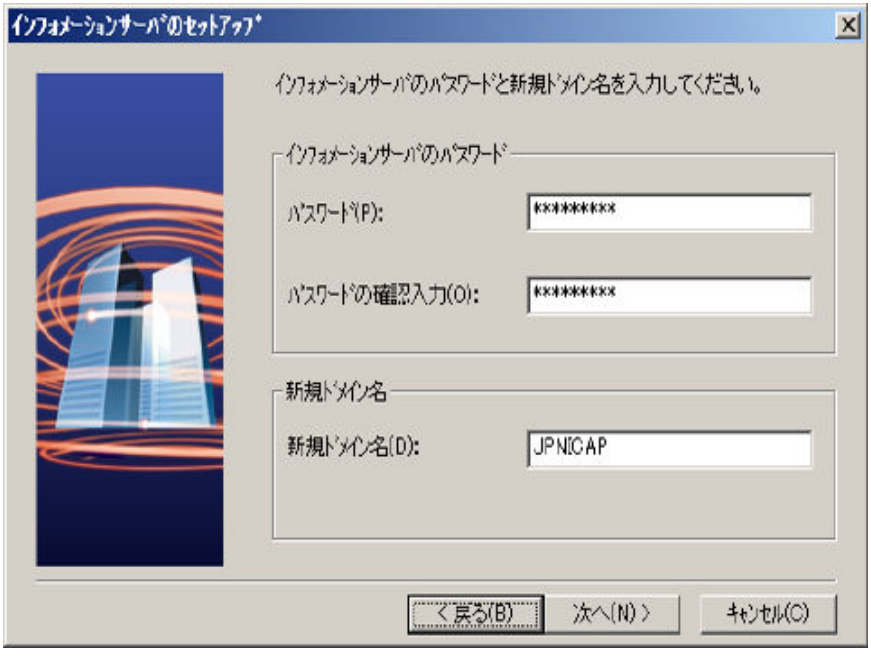


図 2-8. インフォメーションサーバのセットアップ

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]ウィンドウが表示されます。画面に表示されている情報を確認してください。

8. [次へ] をクリックしてセットアッププログラムを続行します。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。

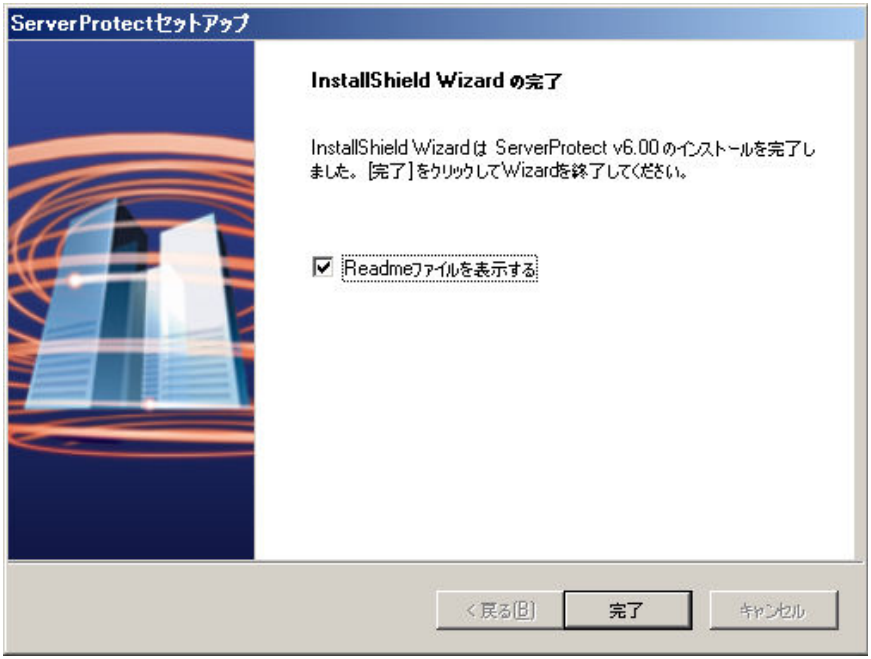


図 2-9. セットアップの完了

9. [完了] をクリックします。

管理コンソールのインストール

管理者は、管理コンソールを使用して ServerProtect ノーマルサーバーをリモートで管理できます。管理コンソールは、ユーザーが操作する ServerProtect コンポーネントです。情報サーバーおよびノーマルサーバーと同じコンピュータにインストールすることも、別のコンピュータにインストールすることもできます。

手順

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、[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選択します。[参照]をクリックして

ローカルインストールパスを変更できます。管理コンソールは Windows Storage サーバ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. [次へ]をクリックします。[プログラムフォルダを選択]画面が表示されます。
5. 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] 画面が表示されます。
6. [次へ] をクリックしてセットアッププログラムを続行します。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。

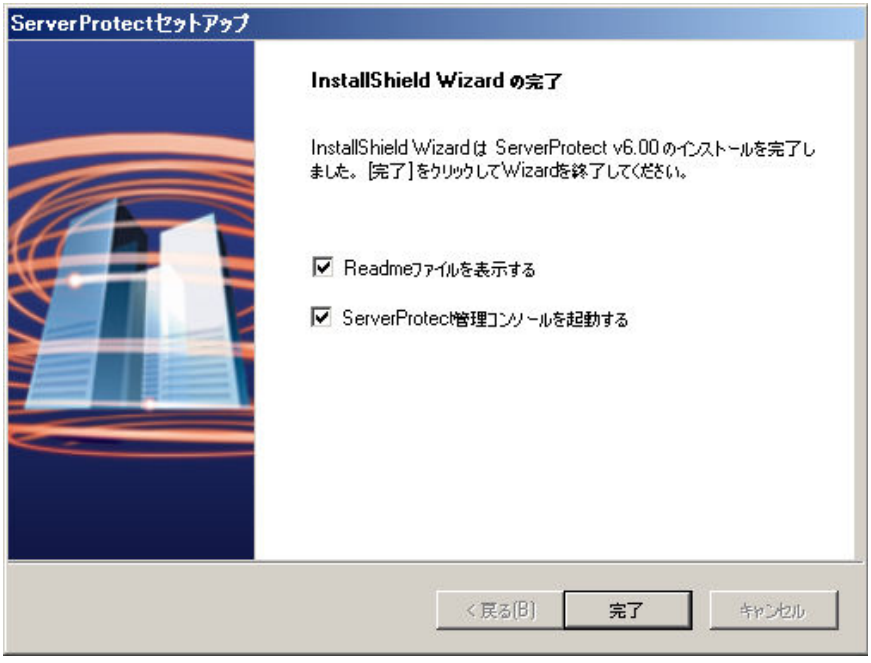


図 2-10. セットアップの完了

7. [完了]をクリックします。[インフォメーションサーバを選択する]ウィンドウが表示されます。

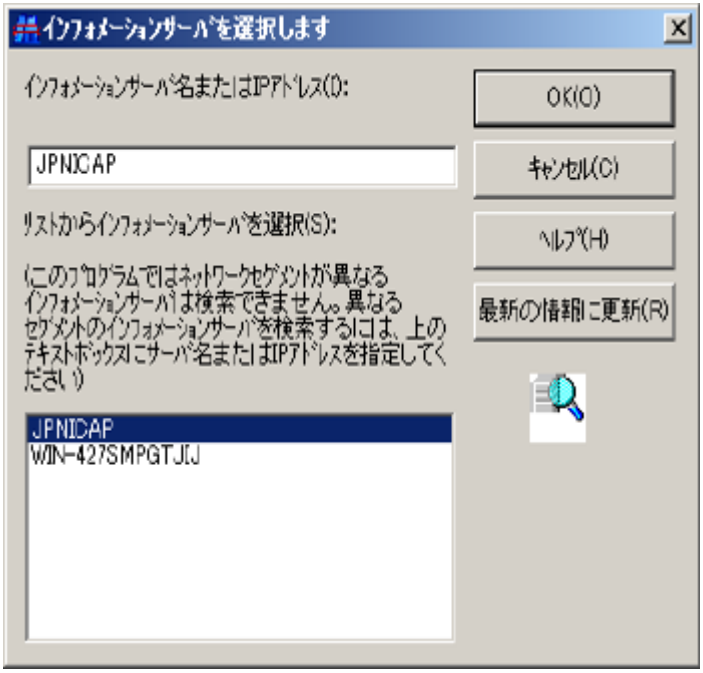


図 2-11. インフォメーションサーバ選択

8. 次のいずれかの操作を実行して管理コンソールが制御する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。

9. [OK]をクリックして変更を保存するか、[キャンセル]をクリックして保存せずにウィンドウを閉じます。

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。

手順

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. [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 [コンポーネントの選択] 画面で選択し、インストールしたいスキャナーの種類を選択します。49 ページの ServerProtect コンポーネントの選択画面 を参照してください。[参照] をクリックして、ノーマルサーバをインストールしたいターゲットサーバとフォルダを指定します。
[ServerProtect インストール先の選択] 画面が表示されます。

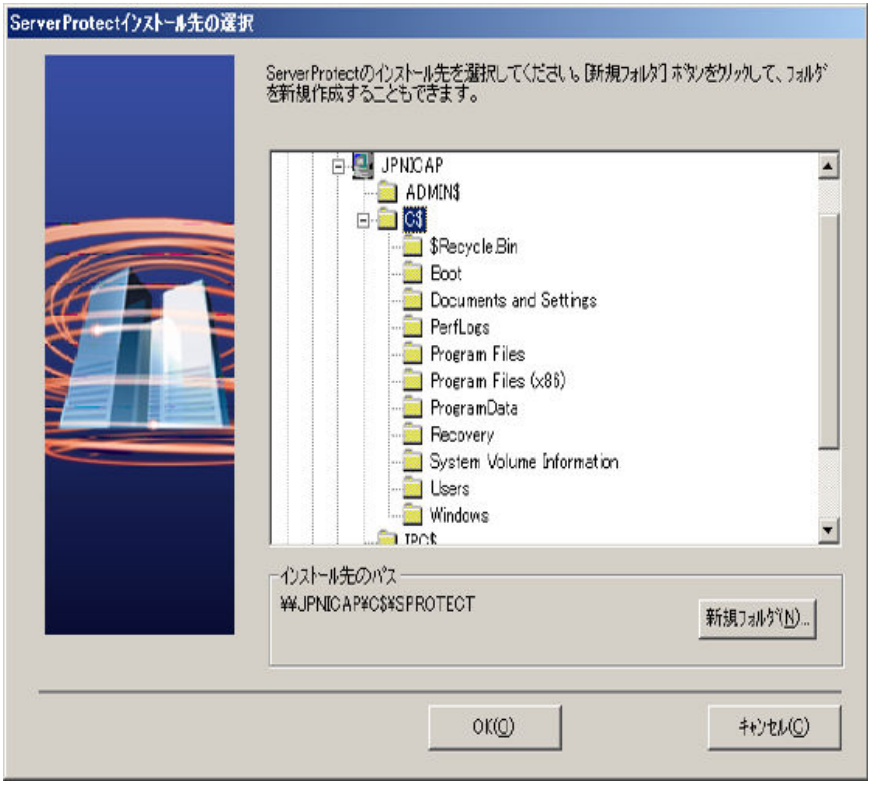


図 2-12. Windows Server でのインストール先の選択

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. ターゲットサーバをダブルクリックします。次に表示される[パスワードを入力してください]画面で、管理者ユーザ名とパスワードを入力し、[OK]をクリックします。ターゲットサーバのローカルドライブがツリーに表示されます。

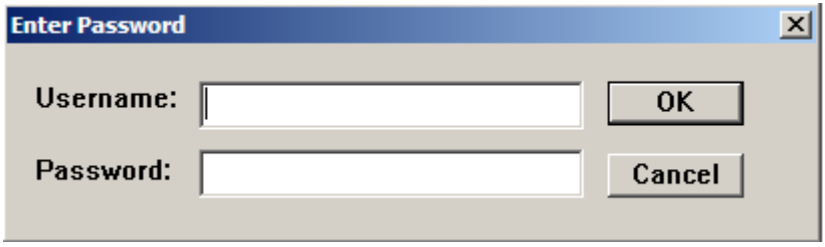


図 2-13. ターゲットサーバのログオン

5. 一般サーバのインストールパスを指定します。インストールを新しいフォルダにする必要がある場合は、[新しいフォルダ] をクリックします。続行するには、[OK] をクリックします。
6. [コンポーネントの選択]画面で[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。
7. [ログオン情報]の下で、[ドメイン名]、[ユーザ名]、[パスワード]、[パスワードの確認入力]フィールドの横に適切なデータを入力してください。
8. [次へ]をクリックすると、[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 2-14. [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。

10. 新しい ServerProtect ドメインが通常のサーバをホストするために必要な場合は、[新規ドメイン]をクリックしてください。

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、[インフォメーションサーバ]フィールドにサーバ名または IP アドレスを入力してください。

---

11. 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。

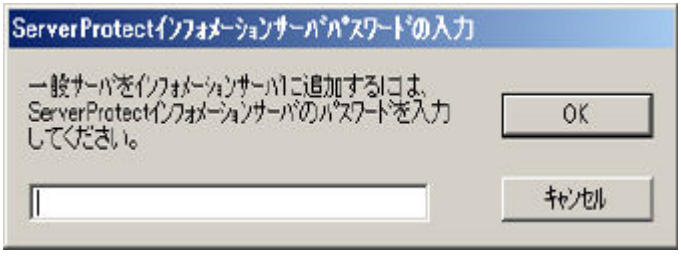


図 2-15. ServerProtect インフォメーションサーバパスワードの入力

[次へ]をクリックします。[ファイルコピーの開始]ダイアログが表示されます。画面に表示されている情報を確認してください。

12. [次へ] をクリックしてセットアッププログラムを続行します。 ServerProtect 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、[セットアップ完了] 画面が表示されます。

13. [完了]をクリックします。アイコン ( ) が Windows タスクバーに追加され、スキャナーがオンであることを通知します。

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。例えば、Windows ストレージサーバには、実行元として Windows ストレージタイプのサーバが必要です。システムは、ドメイン内に存在する場合、デフォルトの実行元サーバとして同じ種類の一般サーバを選択します。

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。

手順

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]を選択してください。
   - 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。

   [実行元サーバを選択]ウィンドウが開きます。
2. 既存の Windows 標準サーバの選択およびインストールするスキャナの種類リストボックスから[OK] 。確認画面が表示されます。クリック[OK]を起動します[サーバをドメインに追加]ウィンドウ。
3. 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]にサーバ名を入力してください。

   [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。

4. 手順 3 を繰り返し、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続けます。 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、[追加と削除] をクリックします。 右のリストボックスに表示されているすべてのサーバを削除するには、[すべて削除] をクリックします。

5. [OK]をクリックして変更を保存するか、[キャンセル]をクリックしてサーバを追加せずにウィンドウを閉じます。

サイレントモードで ServerProtect をインストールする

インストール中 ServerProtect サイレントモードは、Microsoft Windows 環境に通常のサーバをリモートインストールする場合に非常に便利です。

手順

1. 情報サーバをインストールします。51 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。

   一般サーバとしてインストールしたいサーバからこのフォルダにアクセスできることを確認してください。 複数のサイレントインストールを実行する場合、インストール先のサーバに SMS フォルダをマッピングします。

3. インストール先のサーバで、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. ターゲット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にマッピングされたドライブに移動し、次のコマンドを入力します: `<drive>:\setup -SMS -s -m"SPFS"`

   例:

   a. インストール先サーバで、SMS フォルダをドライブ「M」にマップします。

   b. コマンドプロンプトを開きます。

   c. `M:`と入力してドライブ M:に移動します。

   d. 次の内容を入力してください: `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、対象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。

a. SMS フォルダで Setup.ini ファイルを探します。

b. 次の行を追加します。

```
[CommonSection]
```

```
ServerTargetUNCPath=D$\Utility\AntiVirus\SProtect
```

説明:

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

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

```
[CommonSection]
```

```
ServerTargetSN=XXXX-XXXX-XXXX-XXXX-XXXX
```

説明:

XXXX-XXXX-XXXX-XXXX-XXXX: 有効なシリアル番号

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

a. SMS フォルダで Setup.ini ファイルを探します。

b. 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 のインストールプロセスについて説明します。

手順

1. 情報サーバをインストールしてください。51 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. 通常のサーバをインストールします。58 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。54 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 サーバーまたはデスクトップ システム コンピュータに、管理コンソールを追加インストールすることもできます。

   注意

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

4. ServerProtect パターンと検索エンジンファイルを更新してください。110 ページの「アップデートファイルのダウンロード」と 105 ページの「アップデートの設定」を参照してください。
5. 追加の ServerProtect ドメインを作成して、通常のサーバーを管理します。83 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残りの通常サーバーをインストールします。62 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 スキャナーを使用した 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 スキャナーを使用した ServerProtect for Storage をインストールする前に

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。

ServerProtect for Storage で EMC CAVA 検索サービスを実行する場合:

1. AV ユーザアカウントと Antivirus 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 Celerra Event Enabler Technical Note* 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 Celerra Event Enabler Technical Note* を参照してください。

Huawei OceanStor ストレージの場合:

1. AV ユーザアカウントと Antivirus 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、*Huawei OceanStor Storage Technical Note* を参照してください。
2. ServerProtect の通常サーバがインストールされる各サーバに Huawei Antivirus エージェントをインストールしてください。詳細な手順については *Huawei OceanStor Storage Technical Note* を参照してください。
3. Huawei OceanStor Storage を設定してウイルス対策機能を有効にします。詳細な手順については *Huawei OceanStor Storage Technical Note* を参照してください。

EMC CAVA スキャナーを使用した ServerProtect for Storage のインストール

EMC CAVA スキャナーを使用するストレージの場合、ServerProtect 一般サーバをインストールする Windows サーバ上に 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。

Huawei OceanStor Storage 用に、ServerProtect 一般サーバをインストールする Windows サーバ上に Huawei ウイルス対策エージェント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、Huawei ウイルス対策システムの一部です。

手順

1. 情報サーバをインストールしてください。51 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. 通常のサーバをインストールします。58 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。54 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 サーバーまたはデスクトップ システム コンピュータに、管理コンソールを追加インストールすることもできます。

   注意

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

   ---

4. ServerProtect パターンと検索エンジンファイルを更新します。110 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。
5. 追加の ServerProtect ドメインを作成して、通常サーバーを管理します。83 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残りの通常サーバーをインストールします。62 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

ServerProtect の 3 つのコンポーネントは、一緒にまたは個別に削除することができます。個別の削除については、以下のセクションで説明します。

一般サーバの削除

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削除するには

1. 管理コンソールから、削除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 をアンインストールします]をナビゲートします。

一般サーバをローカルで削除するには

1. Windows デスクトップの[コントロールパネル] > [プログラムと機能]から移動します。
2. アンインストールする一般サーバを選択し、[追加と削除] 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。

手順

1. [スタート] > [コントロールパネル] > [プログラムと機能]をクリックします。
2. [ServerProtect インフォメーションサーバ]をクリックし、次に[追加と削除]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。

手順

1. [スタート] > [コントロールパネル] > [プログラムと機能]をクリックします。
2. [ServerProtect 管理コンソール]をクリックし、次に[追加と削除]をクリックします。

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。

- 75 ページの「管理コンソールとは」
- 82 ページの「管理する ServerProtect ドメイン」
- 86 ページの「インフォメーションサーバの管理」
- 88 ページの「一般サーバの管理」
- 105 ページの「アップデートの設定」
- 118 ページの「アップデートファイルの配信」
- 124 ページの「タスクの管理」
- 138 ページの「通知メッセージの設定」
- 145 ページの「一般サーバのウイルス検索」
- 155 ページの「リアルタイム検索」
- 159 ページの「手動検索 (ScanNow)」
- 165 ページの「予約検索 (タスク検索)」

- 180 ページの「検索対象ファイルの種類 (拡張子) の選択」

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 ネットワーク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。

管理コンソールを開く

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。

手順

1. [スタート] > [Trend Micro ServerProtect Management Console]をクリックします。システムは選択した情報サーバへのログオンのために管理者パスワードを求めます。

図 3-1. トレンドマイクロ ServerProtect 管理コンソールログオンウィンドウ

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] をクリックして続行します。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。

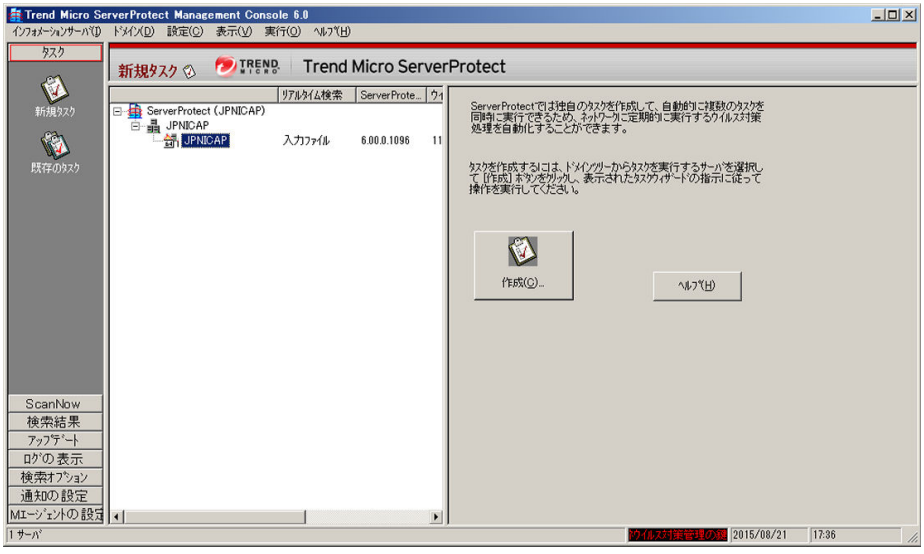


図 3-2. 管理コンソールのメイン画面構成

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]の右側で[メインメニュー]の下に位置しています。ツリービューは ServerProtect の構成を示し、[インフォメーションサーバ]、[ドメイン要素]、[一般サーバ]を含みます
- [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] : ビュー ServerProtect ログファイル、検索結果、およびトレンドマイクロウイルス百科事典。
- [実行]:
  - [タスクの作成] / [既存のタスク]: タスクの作成または変更
  - [ScanNow]: オンデマンドスキャンを実行
  - [アップデート] / [ロールバック]: さまざまな ServerProtect アンチウイルス要素を更新またはロールバック
  - [Control Manager (CM) エージェント設定]: Trend Micro Control Manager の登録、登録解除、および設定
  - [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]: IS パスワードを変更する
  - [ドメインの検索]: ドメインまたはサーバーを検索

- [STOP サインでサーバに接続]: 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[停止]が表示されている場合に使用します
- [ファイルを送信]: 不審ファイルまたはクリーンできないファイルをトレンドマイクロのウイルスドクターに無料で送信してください。ウイルスドクターがファイルをクリーンし、E メールで返送します
- [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
- [機能リクエストを送信]: ServerProtect に追加してほしい新機能のリクエストを送信するために使用します

- [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]: 新しいタスクを作成する
  - [既存のタスクリスト]: 既存のタスクを表示、実行、変更、または削除する
- [[検索] グループ]
  - [ScanNow]: 手動ウイルス検索を設定するには
- [[検索結果] グループ]
  - [リアルタイム検索]: リアルタイム検索と EMC CAVA スキャナーの結果を表示するには
  - [ストレージ検索サービス]: RPC 検索と ICAP 検索の結果を表示するには

- [ScanNow]: 手動検索の結果を表示するには
- [タスク検索]: タスクによって実行されたスキャン結果を表示する

- [[アップデート] グループ]
  - [アップデート]: ネットワーク上の通常サーバーに更新をダウンロードして展開する
  - [ロールバック]: ネットワークで実行された以前の展開アクションにロールバックするため
- [[ログの表示] グループ]
  - [ログの表示]: ネットワーク上で発生したウイルス対策イベントの履歴情報を表示する
- [[検索オプション] グループ]
  - [リアルタイム検索]: ネットワークでリアルタイムウイルス検索を設定する
  - [ストレージ検索サービス]: ストレージスキャナーウイルス検索を設定するには
  - [検索除外リスト]: ServerProtect ウイルススキャンエンジンによって無視されるファイル、ディレクトリ、またはウイルスを定義するため
  - [書込み禁止リスト]: 特定のファイルやディレクトリの変更を防ぐため
- [[通知の設定] グループ]
  - [標準通知]: サーバでデフォルトの条件が検出されたときに標準アラートを設定する
  - [アウトブレイク通知]: 比較的短期間に多くのウイルスイベントが発生した場合にウイルスアウトブレークアラートを設定する
  - [CM エージェント設定]: Trend Micro Control Manager 設定の登録、登録解除、構成を行う

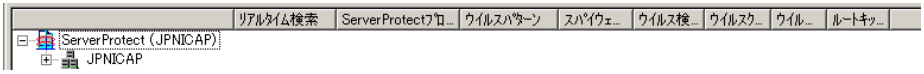
ドメインブラウザツリー

ドメインブラウザツリーには、ソフトウェア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。



ツリーのアイコンを右クリックします。ServerProtect コンソールをクリックして、選択したコンポーネントの設定を変更します。ドメインブラウザツリーを含むフレームは、サイズを変更できます。

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。さらに、インフォメーションサーバはドメインを相互にリンクします。

情報サーバ

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 ドメインとは異なります。

- ServerProtect ドメイン
- 感染した通常サーバを含む 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 サーバタイプの通常のサーバ
- 64 ビット Microsoft Windows サーバタイプの通常のサーバ
- 32 ビット Microsoft Windows サーバタイプの感染した通常のサーバ
- 感染した 64 ビット Microsoft Windows サーバタイプの通常サーバ
- 切断されたかサービスが無効化された通常のサーバ

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。

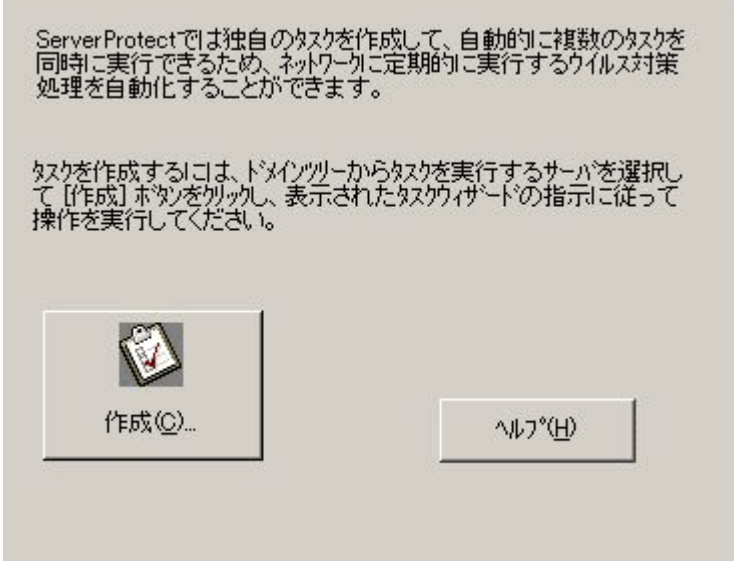


図 3-3. 設定データ領域

管理する 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。

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、感染したサーバのアイコンに炎が表示されます。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。感染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、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。

手順

1. 次のいずれかの操作を実行します。
   - ドメインを追加したい情報サーバを選択してください。メインメニューから移動します[ドメイン] > [新規ドメインの追加]。
   - 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]ウィンドウが表示されます。

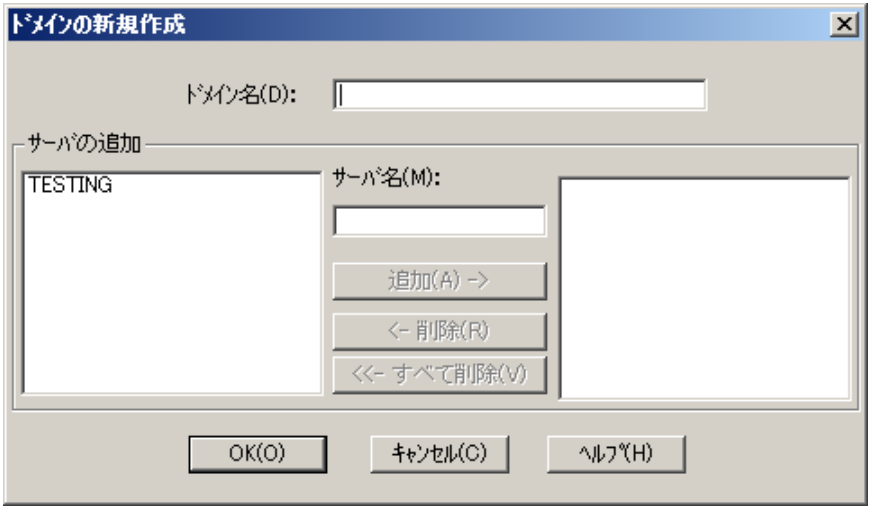


図 3-4. [ドメインの新規作成] ウィンドウ

2. [ドメイン名]フィールドに名前を入力してください。
3. ドメインに追加するサーバを識別します。次のいずれかを実行します。
   - 画面の左のリストからサーバを選択します。
   - [サーバ名を入力してください]フィールドにサーバ名を入力してください。
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、[追加と削除] をクリックします。 右のリストからすべてのサーバを削除するには、[すべて削除] をクリックします。
6. [OK] ボタンをクリックして変更内容を保存します。 または、[キャンセル] ボタンをクリックして新しいドメインを作成せずにウィンドウを閉じます。

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。

手順

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ます。
   - 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。
   - メインメニューで[ドメイン] > [ドメインのリネーム]を選択します。
   - キーボードの[F2]キーを押してください。

   [ドメイン名の変更]ウィンドウが表示されます。

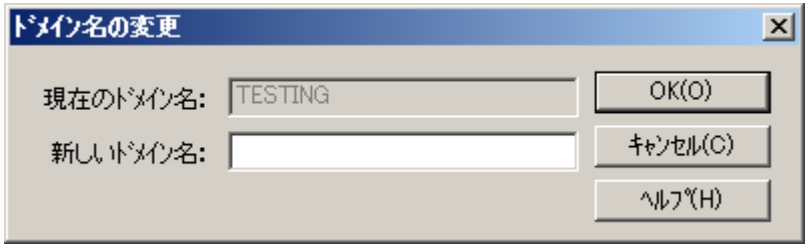


図 3-5. [ドメイン名の変更] ウィンドウ

3. []テキストボックスに新規ドメイン名を入力し、[OK]をクリックします。保存せずにウィンドウを閉じるには[キャンセル]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。

手順

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ます。
   - 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。
   - メインメニューで[ドメイン] > [ドメインの削除]をクリックします。
   - キーボードの[削除]キーを押してください。

注意

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。

また、ServerProtect ドメインを作成する際に通常のサーバを移動することもできます。83 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。

手順

1. メインメニューで[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]をクリックします。

   [インフォメーションサーバの選択]ウィンドウが表示されます。

2. 次のいずれかの操作を実行します。

   - インフォメーションサーバとして使用するサーバの名前または IP アドレスを入力します。
   - リストからインフォメーションサーバを選択します。

   コンピュータに複数のネットワークインタフェースカード (NIC) がインストールされている場合、プライマリ NIC に接続されているインフォメーションサーバのみがリストボックスウィンドウに表示されます。 リストのサーバ表示を更新するには、[最新の情報に更新] ボタンをクリックします。

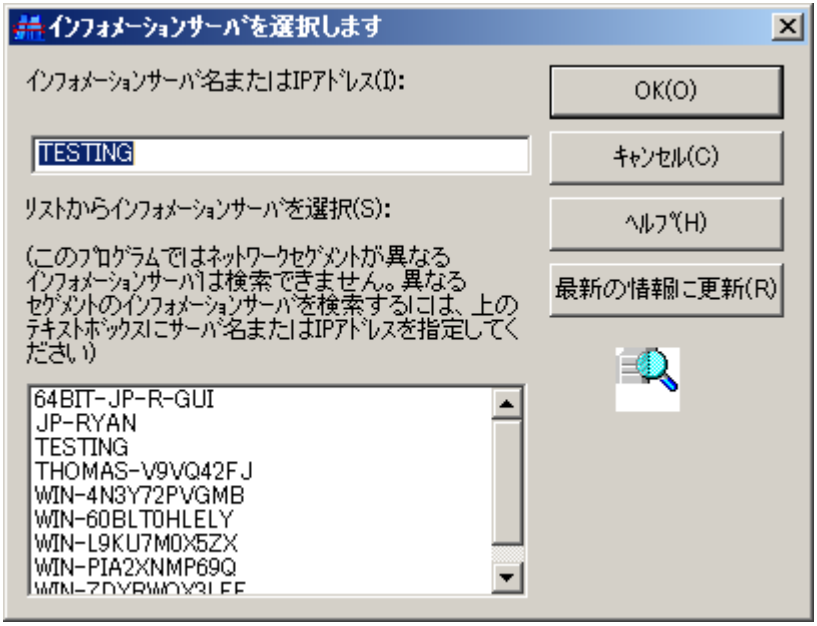


図 3-6. トレンドマイクロ ServerProtect 管理コンソールウィンドウ

3. [OK]をクリックして変更を保存するか、[キャンセル]をクリックして保存せずにウィンドウを閉じます。

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。このセクションでは、一般サーバの管理方法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。

一般サーバの移動

ServerProtect 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。

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、古い通常のサーバを ServerProtect6.0 情報サーバに移動することはできません。

手順

1. 次のいずれかの操作を実行します。
   - 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。
   - 移動したい通常のサーバを選択し、メインメニューで[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]をクリックします。[実行先インフォメーションサーバの選択]ウィンドウが表示されます。
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]/[パスワード]]フィールドまたは[GUID]のフィールドに適切な値を入力してください。[OK]ボタンをクリックしてダイアログボックスを送信します。

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検索サーバにより、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 を検索サーバに追加します。

また、複数の検索サーバーを個々の NetApp デバイスに割り当てて負荷分散を行うこともできます。94 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。

NetApp 7-Mode デバイスを追加中

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

- 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

手順

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。

[デバイスを追加]画面が表示されます。

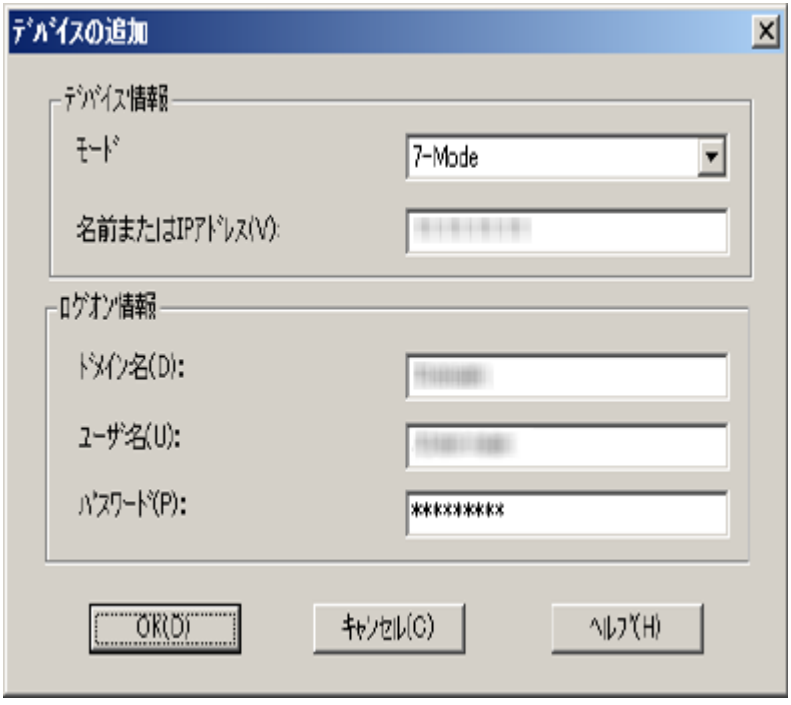


図 3-7. [デバイスの追加] 画面 (1)

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ボックスから[7-Mode デバイス]を選択してください。
   - [デバイス名または 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。

Cluster-Mode AV Connector の追加

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

手順

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[デバイス一覧]を選択します。

   [デバイス一覧]画面が表示されます。

2. [追加] をクリックします。

[デバイスを追加]画面が表示されます。

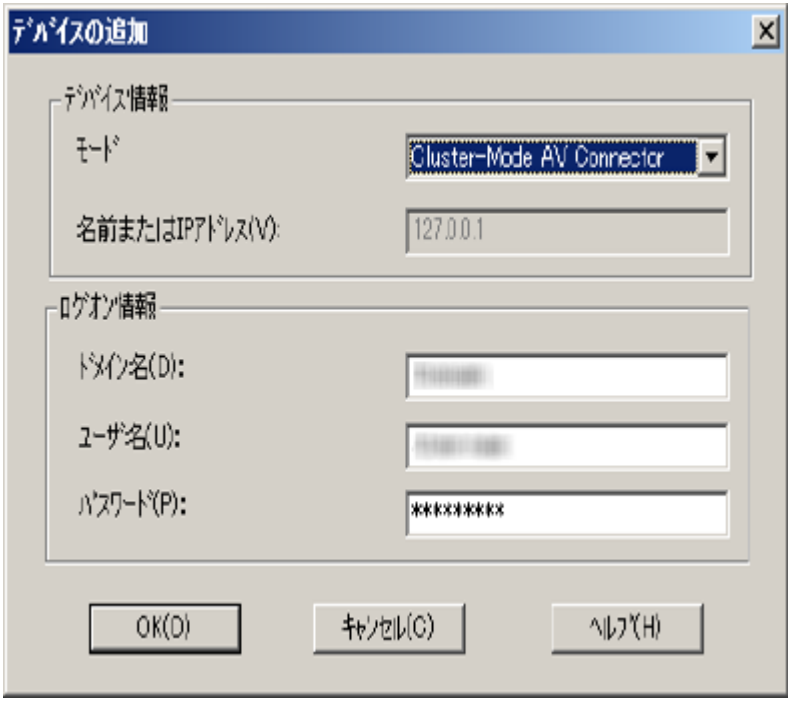


図 3-8. [デバイスの追加] 画面 (2)

3. 次の手順に従ってください。
   - [デバイスモード]のドロップダウンリストボックスから[Cluster-Mode AV Connector]を選択してください。
   - [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 Microsoft Windows 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)。

複数のスキャンサーバが 1 台の NetApp デバイスに対して動作していることを確認する手順は次のとおりです。

手順

1. 確認対象となるストレージ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、次を入力します。

   ```
   netapp> vscan scanners
   ```

   ストレージ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。

手順

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. [追加と削除]をクリックします。[デバイスを削除]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 の情報の更新

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、ServerProtect で Storage with RPC Scanner の 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 Storage で、ServerProtect における 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

手順

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]をクリックしてください。

   [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。

   - [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。

- [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 で Storage の 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 のシステム情報を更新する手順は、NetApp 7-Mode デバイスのシステム情報を更新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場合、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されます。

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
- 受信と送信

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[受信と送信]に設定してください。 ただし、コンピュータを検索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。

次の手順では、リアルタイム検索を受信および送信に設定する方法について説明します。

手順

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ます。
   - サイドバーで[[検索オプション]] > [リアルタイム検索]をクリックします
   - メインメニューで[設定] > [検索オプション] > [リアルタイム検索]をクリックしてください

[リアルタイム検索の設定]画面が表示されます。

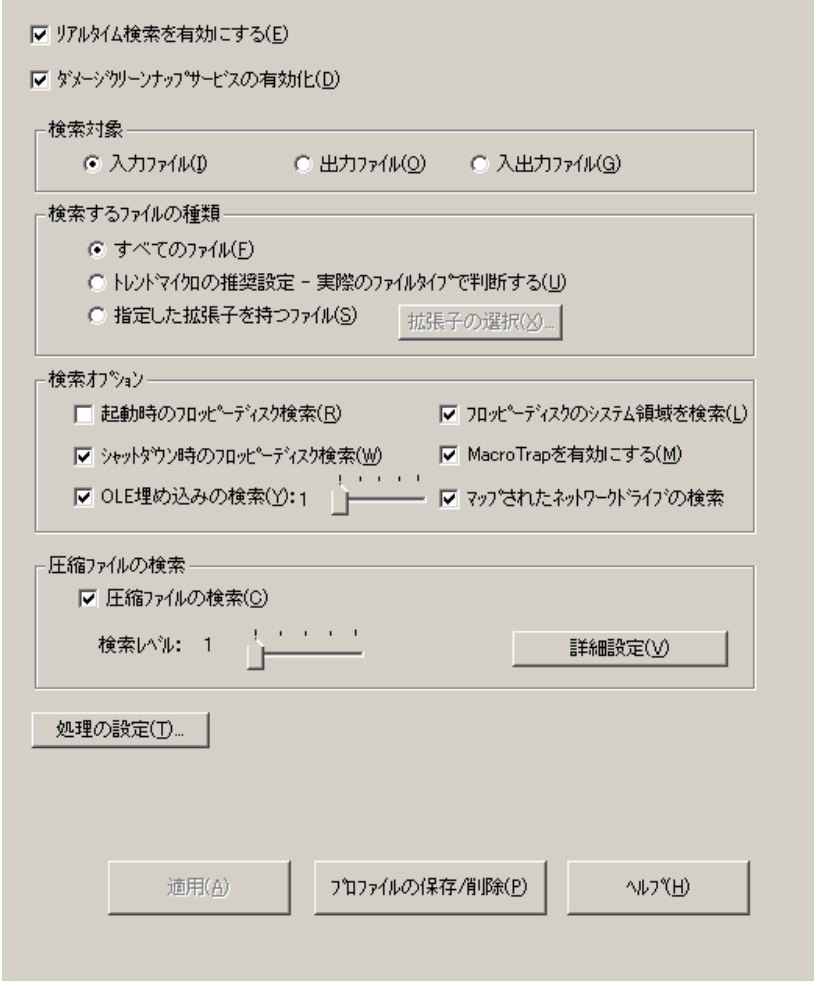


図 3-9. [リアルタイム検索設定] 画面

3. [検索方向]の下で、[受信と送信]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、155 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。

手順

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]を選択してください。
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

手順

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]の[デバイス名]、[ステータス]、[Mode]フィールドを確認して NetApp デバイスのステータスを検証します。

   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]または[オフライン]が表示されます。

NetApp デバイスの 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。

手順

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ます。
   - メインメニューから[設定] > [通知] > [一般の警告]を選択してください。
   - サイドバーで[通知の設定]をクリックし、次に[一般の警告]をクリックします。
3. [デバイスの RPC 接続の成功/失敗]を選択します。

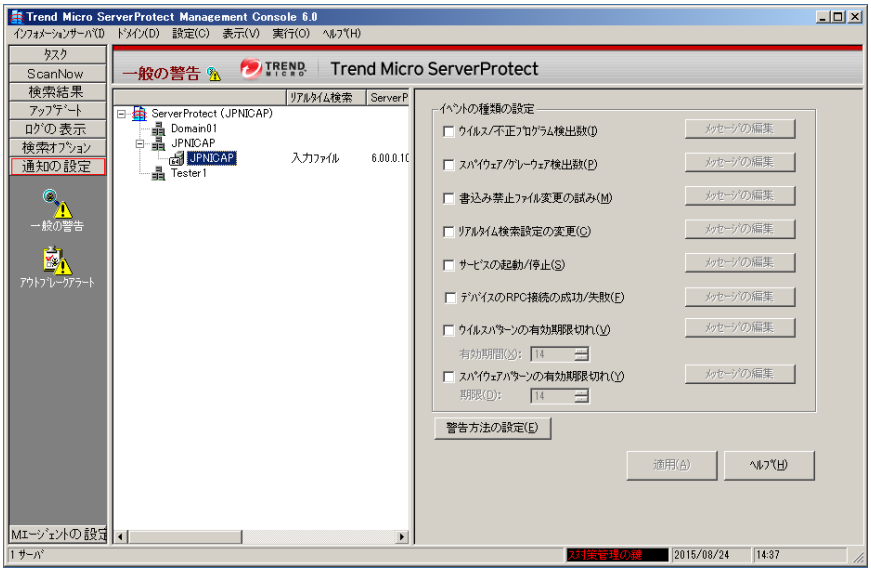


図 3-12. 一般の警告の設定

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。

   詳細については、138 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。その後、各 NetApp デバイスは、アップデートサーバから新しいアップデートが届くまで、以前検索したファイルのキャッシュを再構築し始めます。

更新のダウンロードに関する詳細については、110 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。

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。

ICAP クライアントからの検索リクエストを受け入れる

以下の手順では、すべての ICAP クライアントまたは ICAP クライアントリストに存在する ICAP クライアントからの検索リクエストを受け入れる方法について説明します。

手順

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。

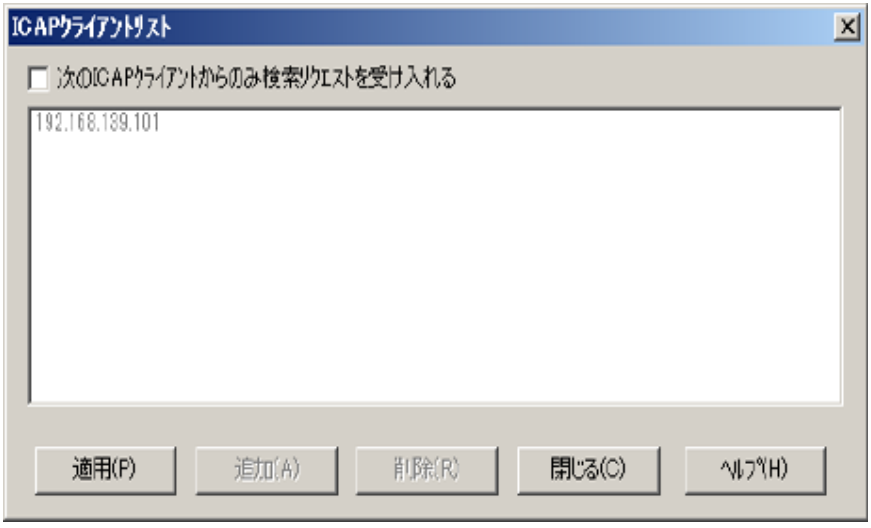


図 3-13. ICAP クライアントリスト

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 クライアントの ICAP クライアントリストへの追加

手順

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/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

手順

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。アップデートプロセスは、ダウンロードと配信で構成されます。

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、実際にウイルスを検出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 用)]: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

次の図は、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 の処理の流れを示しています。

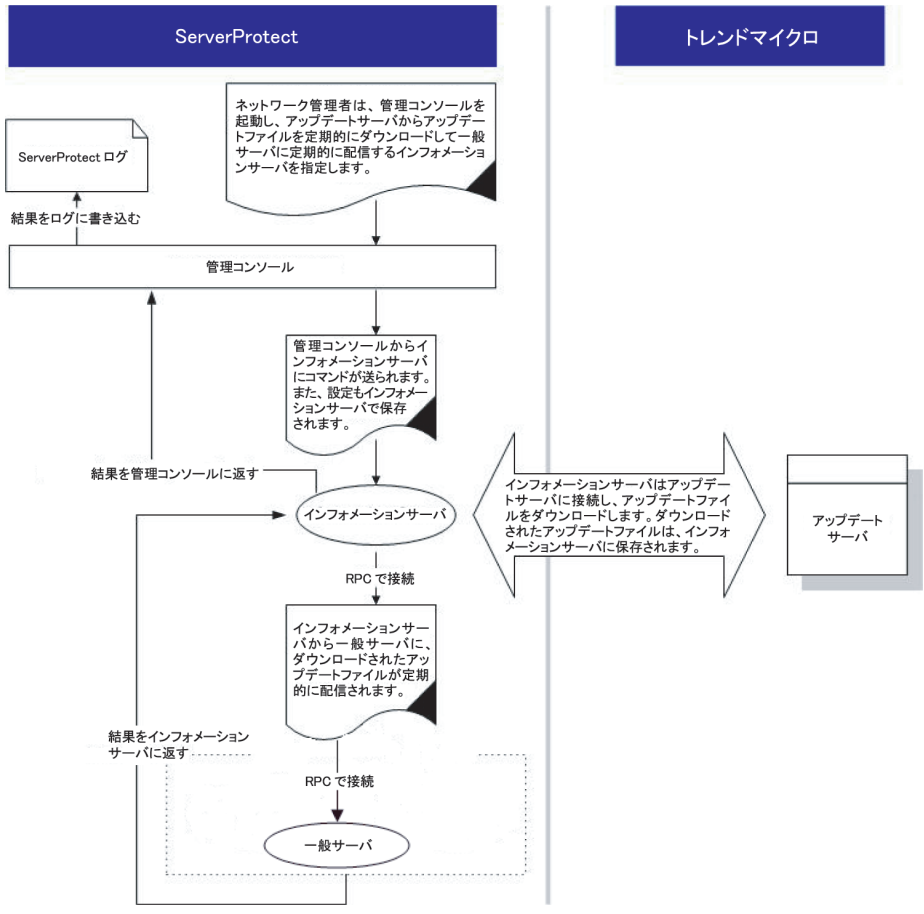


図 3-14. ダウンロードと配信の流れ

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とスキャンエンジンを確認できます。

次のいずれかの操作を実行してください。

- サイドバーで[アップデート] > [アップデート]をクリックします。
- メインメニューで[実行] > [アップデート]をクリックします。

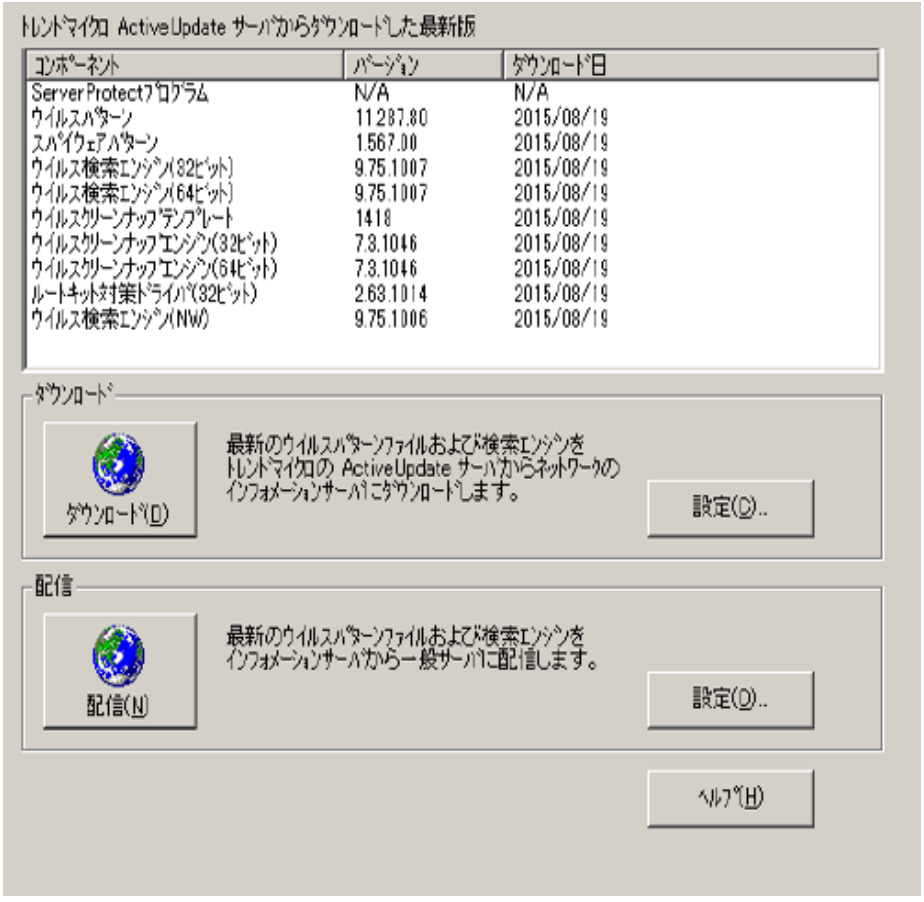


図 3-15. トレンドマイクロ ServerProtect [アップデート] メイン画面

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
- 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/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 /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)

初めて ServerProtect をインストールした後、バージョンフィールドが表示されます。[ダウンロードの設定]をクリックしてトレンドマイクロ更新サーバから最新の更新をダウンロードし、正常に更新を行うと、更新された情報が表示されます。

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毎週数回リリースしています。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、重複したダウンロードを避けることができます。

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。

ダウンロード元の設定

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。

トレンドマイクロのアップデートサーバをダウンロードソースとして設定する

手順

1. 次のいずれかの操作を実行します。
   - サイドバーで[アップデート] > [アップデート]をクリックしてください。
   - メインメニューから[実行] > [アップデート]をクリックします。
2. [ダウンロード]グループで[設定]をクリックして、[ダウンロードオプション]ウィンドウを開きます。
3. [インターネット] オプションを選択し、次の URL を指定して トレンドマイクロ アップデートサーバからファイルをダウンロードします。

   `http://spfs60-p.activeupdate.trendmicro.com/activeupdate`
4. [OK] をクリックします。 ダウンロードされたファイルは、インフォメーションサーバの次のディレクトリに保存されます。

   `¥ProgramFiles¥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として設定

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。 詳細については、112 ページの「ダウンロード元フォルダの作成」を参照してください。

手順

1. 次のいずれかの操作を実行します。
   - サイドバーで[アップデート] > [アップデート]をクリックしてください。

- メインメニューから[実行] > [アップデート]をクリックします。

2. [ダウンロード]の下で、[設定]をクリックします。

   [ダウンロードオプション]ウィンドウが表示されます。

3. [ローカルまたはネットワークドライブ]をクリックしてください。

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。

   次に例を示します。

   ```
   ¥¥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ための情報を指定します。 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。

ダウンロード元フォルダの作成

手順

1. [ダウンロードの設定] 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ます。

   - <drive>:¥ProgramFiles¥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。

注意

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。

手順

1. 次のいずれかの操作を実行します。
   - サイドバーで[アップデート] > [アップデート]をクリックします。
   - メインメニューから[実行] > [アップデート]をクリックします。
2. [アップデート]メイン画面で[ダウンロードの設定]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[ダウンロードの設定]を使用する場合は、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[ダウンロードの設定]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、115 ページの「ダウンロードオプションの設定」を参照してください。

ServerProtect では、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

ServerProtect の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ダウンロードすることができます。

手順

1. 次のいずれかの操作を実行します。
   - サイドバーで[アップデート] > [アップデート]をクリックします。
   - メインメニューから[実行] > [アップデート]をクリックします。
2. [ダウンロード]の下で、[設定]をクリックします。

   [ダウンロードオプション] ウィンドウが表示されます。
3. [予約設定] タブをクリックします。

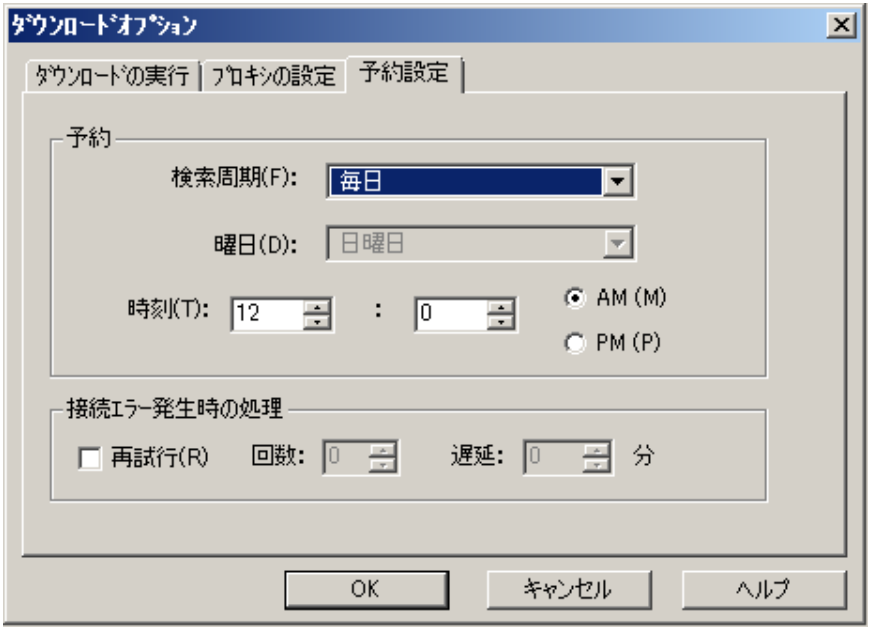


図 3-16. [ダウンロードオプション] - [予約設定]ウィンドウ

4. [検索周期]リストの[スケジュール]の下で、ダウンロード頻度をクリックします。[なし]、[毎時間]、[毎日]、または[週 1 回]を選択できます。ダウンロードをスケジュールしたくない場合は、[なし]をクリックします。[週 1 回]をクリックした場合は、[曜日]リストで日をクリックします。
5. [時刻] ボックスに、コンポーネントを更新したい時間を入力または選択し、[午前] または [午後] をクリックします。
6. [再試行]チェックボックスをオンにして、ServerProtect に初回のダウンロード操作が失敗した場合にダウンロードサーバに再接続を試みるよう指示します。[回数]および[遅延]ボックスに、再試行する回数と各再試行の間の遅延を入力または選択します。
7. [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。

   ¥Trend¥SProtect¥SpntShare

ダウンロードオプションの設定

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。

ダウンロードの設定を構成する

手順

1. 次のいずれかの操作を実行します。
   - サイドバーで[アップデート] > [アップデート]をクリックします。
   - メインメニューから[実行] > [アップデート]をクリックします。
2. [アップデート]画面で[設定]をクリックして、ダウンロード設定を変更します。

[ダウンロードオプション]ウィンドウが表示されます。

図 3-17. ダウンロードオプションウィンドウ

プロキシサーバ設定

インターネットに接続している場合は、ServerProtect をプロキシサーバの設定を使用するように構成できます。

手順

1. 次のいずれかの操作を実行します。
   - サイドバーで[アップデート] > [アップデート]をクリックします。
   - メインメニューから[実行] > [アップデート]をクリックします。

2. [ダウンロード]の下で、[設定]をクリックします。

   [ダウンロードオプション]ウィンドウが表示されます。

3. [プロキシ設定]タブをクリックしてください。

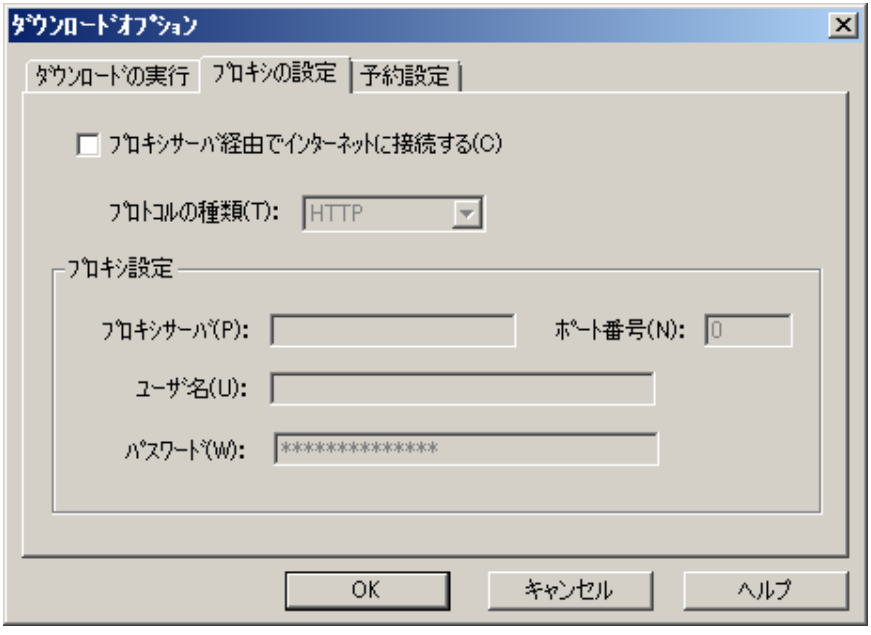


図 3-18. [ダウンロードオプション] - [プロキシの設定]ウィンドウ

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選択します。

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]の下で次の操作を行います。

   - [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情報を入力します。

7. [OK] をクリックします。

アップデートファイルの配信

情報サーバが通常サーバに更新を展開する際、各通常サーバにコマンドを送信し、更新のコピーを取得するよう要求します。ServerProtect は接続と展開プロセスの両方をログファイルに記録します。

配信の設定

[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。

手順

1. 次のいずれかの操作を実行します。
   - サイドバーで[アップデート] > [アップデート]をクリックします。
   - メインメニューから[実行] > [アップデート]をクリックします。
2. [配信]をクリックします。確認ウィンドウが表示されます。手動更新の展開を続行するには[◯]をクリックします。

[配信]ウィンドウが表示されます。

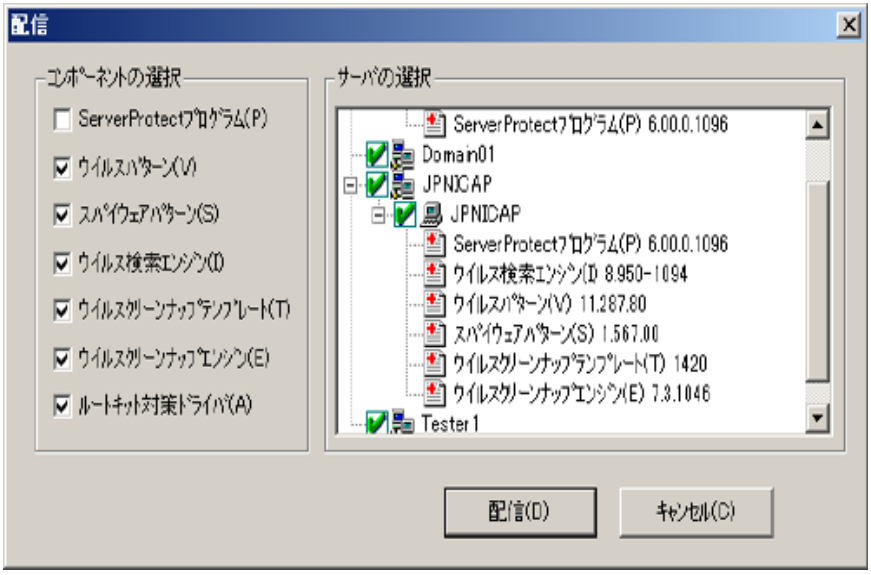


図 3-19. デプロイウィンドウ

[コンポーネントを選択]グループ内の複数のチェックボックスは、通常のサーバに展開するためのコンポーネントを示します。[ウイルスパターンファイル]、[スパイウェア]、[ウイルスクリーンナップテンプレート]のチェックボックスは、アプリケーションの初期段階でデフォルト設定の一部として選択されています。[サーバの選択]ペインでは、ダウンロードされた ServerProtect アンチウイルス要素のバージョン情報がツリービュー UI 要素に表示されます。64 ビット Windows サーバの場合、[コンポーネントを選択]グループに表示されるチェックボックスは、[サーバ保護プログラム]、[ウイルスパターンファイル]、[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 Windows サーバの場合、64 ビット Windows 用に説明された 6 つの要素に加えて、[ルートキット対策ドライバ]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、[コンポーネントを選択] 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 UI 要素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。

4. [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 はデフォルトでデプロイタスクを作成します。125 ページの「初期設定のタスク」を参照してください。

スケジュールされたタスクの設定方法についての詳細は、126 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。

手順

1. 次のいずれかの操作を実行します。
   - サイドバーで[アップデート] > [アップデート]をクリックします。
   - メインメニューから[実行] > [アップデート]をクリックします。
2. [配信]セクションで[設定]をクリックします。

[配信オプション]ウィンドウが表示されます。

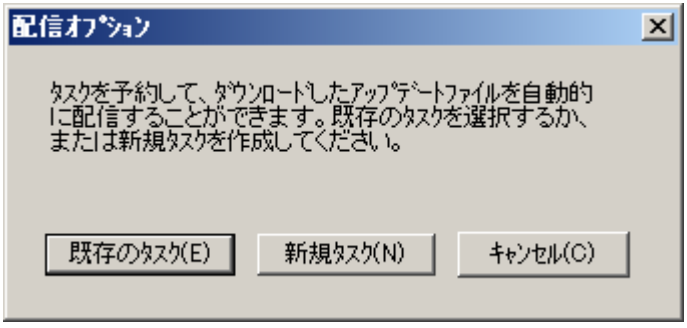


図 3-20. デプロイオプションウィンドウ

3. 次のいずれかの操作を実行します。
   - [新規タスク]をクリックして、タスクを作成します。
   - [既存のタスク]をクリックして、タスクを編集します。

   タスクの作成または編集方法については、126 ページの「新規タスクの作成」および 133 ページの「既存タスクの変更」を参照してください。

以前の配信処理のロールバック

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。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する必要があります。

手順

1. 次のいずれかの操作を実行します。

- サイドバーで[アップデート] > [ロールバック]をクリックします。
- メインメニューから[実行] > [ロールバック]をクリックします。

[ロールバック]画面が表示されます。

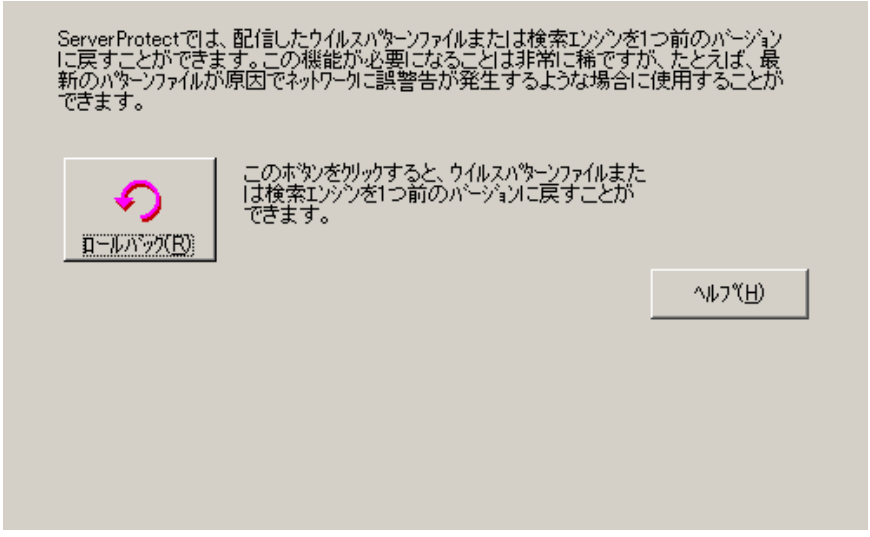


図 3-21. ロールバックの設定ウィンドウ

2. [ロールバック] をクリックします。

ServerProtect[ロールバック]ウィンドウが表示されます。

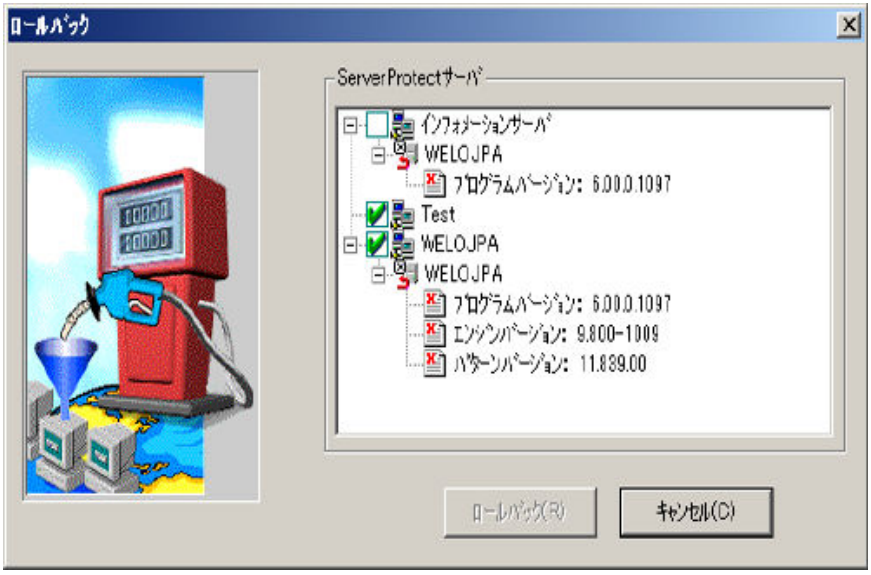


図 3-22. ロールバックウィンドウ

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。 バージョンとビルド番号も表示されます。

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]: 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。たとえば、ネットワークのパフォーマンスが正常なときにのみ受信ファイルをスキャンします
- [ScanNow]: サーバがウイルスに感染していないかを確認します
- [ログの削除]: データベースから削除するログの種類を定義します。 あらかじめ設定した期間より古いウイルスログを自動削除することができます。
- [ログのファイル出力]: 他のアプリケーションで使用できるように CSV ファイルでログを出力します
- [ログの印刷]: 特定の条件に一致したログを印刷するネットワークプリンタを選択します
- [統計の実行]: サーバ上のウイルス検索に関する統計を収集し表示します
- [配信]: ウイルスパターンファイルと検索エンジンのアップデートファイルを他の ServerProtect サーバに配信する予約を設定します

図 3-23. タスクウィザードウィンドウ

初期設定のタスク

デフォルトタスクは、通常のサーバインストールごとに ServerProtect によって作成されます。初めて ServerProtect をインストールすると、すぐに 3 つのデフォルトタスク (検索、統計、および展開) が用意されます。デフォルトタ

スクを編集することはできますが、タスク名やタスク所有者を変更することはできません。

新規タスクの作成

タスクは、保守、設定手順を自動化する 1 つの方法です。

タスクを作成します

手順

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ます。
   - メインメニューで[実行] > [タスクの作成]をクリックします。
   - サイドバーで[タスク] > [新規タスク]をクリックします。
3. [作成] をクリックします。

   [新しいタスクを作成]ウィンドウが表示されます。

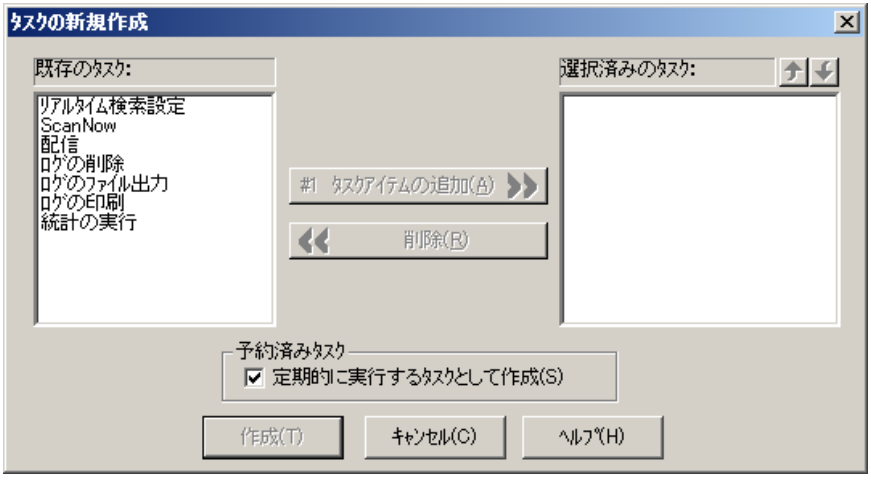


図 3-24. [タスクの新規作成] ウィンドウ

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] をクリックして、選択した機能を [選択済みのタスク] リストに追加します。さらに機能を追加することも、既に選択した機能を削除することもできます。

ヒント

[選択済みのタスク] の横にある上下の矢印アイコンをクリックして、機能の実行順序を変更できます。 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. このタスクを指定されたスケジュールに従って実行したい場合は、[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選択してください。タスクは毎時実行するようにスケジュールできます。
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、[新規作成] ウィンドウが閉じます。

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。

手順

1. 126 ページの「タスクを作成します」の手順 1 から 6 に従ってください。[予約済みタスク]の下にある[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必ず選択してください。

   [タスクウィザード]ウィンドウが表示されます。
2. [次へ] をクリックします。

[予約設定]ウィンドウが表示されます。

図 3-25. スケジュール設定ウィンドウ

3. [検索周期]リストの[スケジュールされた時間]の下で、ダウンロード頻度をクリックします。[月 1 回]、[週 1 回]、[毎日]、または[毎時間]を選択できます。[週 1 回]を選択した場合は、[曜日]リストで日をクリックします。あるいは、[月 1 回]を選択した場合は、[月の日]リストで日をクリックします。

4. [時刻] ボックスに、コンポーネントを更新したい時間を入力または選択し、[AM] または [午後] をクリックします。
5. [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。後者のオプションでは、ネットワーク上の別のドライブを検索することも可能です。

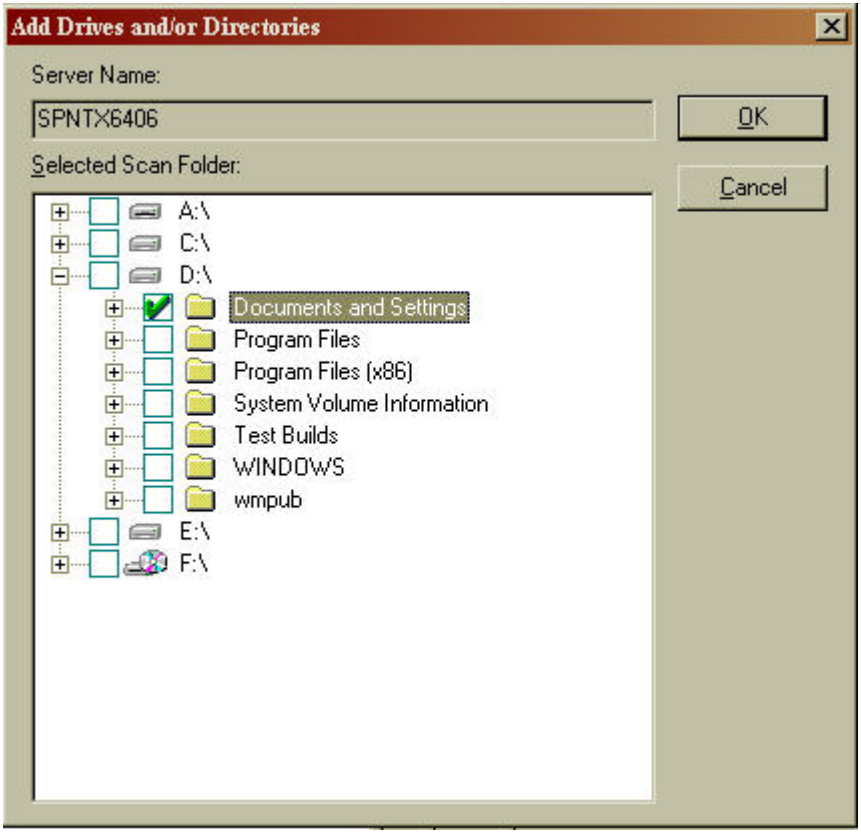


図 3-26. ドライブ/ディレクトリの追加ウィンドウ

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。

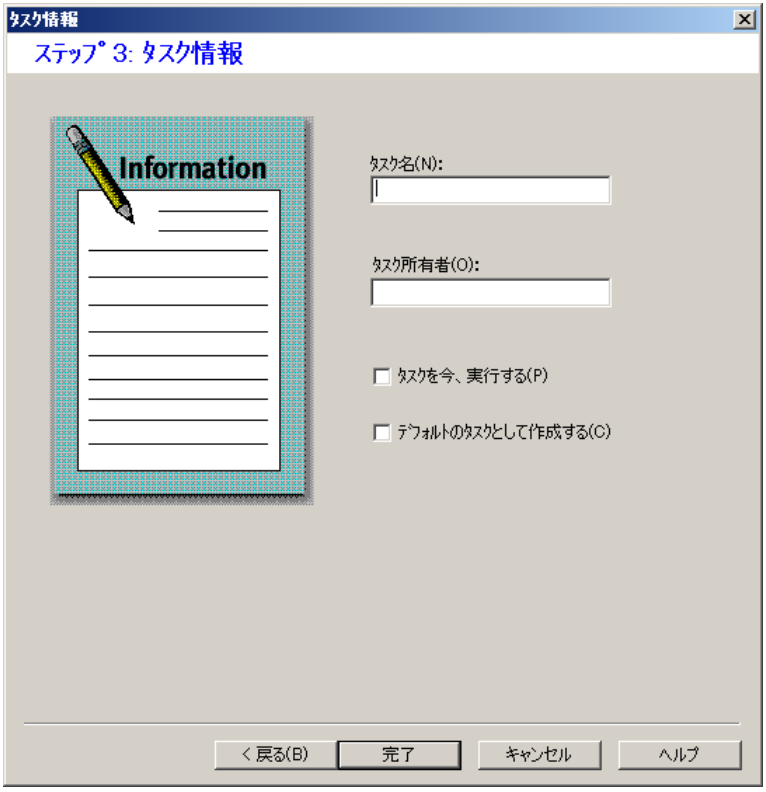


図 3-27. タスク情報ウィンドウ

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、既に作成されたタスクに関する情報が表示されます。 [既存のタスク]リストを使用して、タスクの定義を実行、修正、削除、または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。

- サイドバーで[タスク] > [既存のタスク]をクリックしてください。

- メインメニューで[実行] > [既存のタスク]をクリックします。

[既存のタスク] リスト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[既存のタスク] リストを使ってタスクを実行できます。

手順

1. 次のいずれかの操作を実行します。
   - サイドバーで[タスク] > [既存のタスク]をクリックします。
   - メインメニューで[実行] > [既存のタスク]をクリックします。

   [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、[今すぐ実行] 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。

既存タスクの変更

手順

1. 次のいずれかの操作を実行します。
   - サイドバーで[タスク] > [既存のタスク]をクリックします。
   - メインメニューで[実行] > [既存のタスク]をクリックします。

   [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]ウィンドウが表示されます。

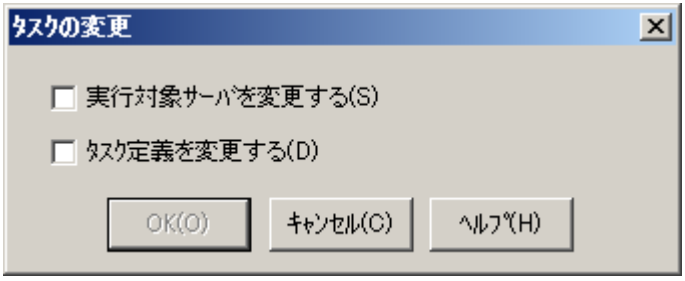


図 3-29. タスクの変更ウィンドウ

4. 次のいずれかの操作を実行します。
   - [実行対象サーバを変更する] チェックボックスをオンにすると、タスクの実行先サーバを変更できます。
   - [タスク定義を変更する]チェックボックスをオンにすると、既存タスクの定義内容を変更できます。
5. [OK] をクリックします。

既存のタスクの実行対象サーバを変更する

手順

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。

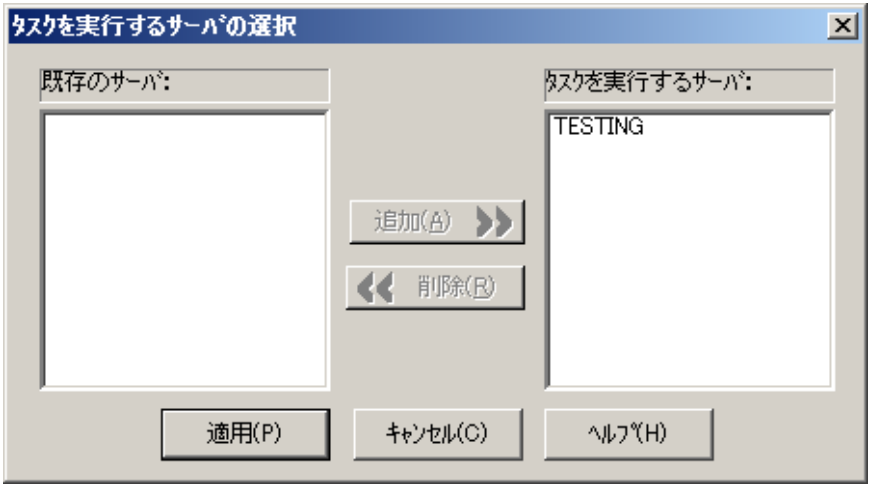


図 3-30. タスクを実行するサーバの選択ウィンドウ

3. [適用]をクリックします。変更を保存せずにウィンドウを閉じるには、[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

手順

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。

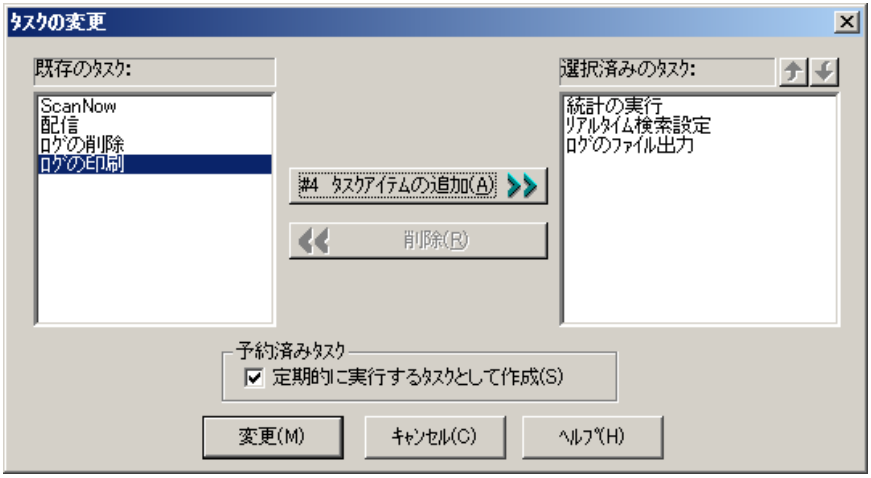


図 3-31. タスクウィンドウの変更

2. [#n タスクアイテムの追加]をクリックして、選択した機能を[選択済みのタスク]リストに追加します。

   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

[選択済みのタスク] の横にある上下の矢印アイコンをクリックして、機能の実行順序を変更できます。 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] 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、[新しいタスクを作成] ウィンドウが閉じます。

既存タスクの表示

既存タスクの属性は [既存のタスク] ウィンドウに表示され、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。

手順

1. 次のいずれかの操作を実行します。
   - メインメニューで[実行] > [既存のタスク]をクリックします。
   - サイドバーで[タスク] > [既存のタスク]をクリックしてください。
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. 構成エリアの下部にある[表示]をクリックします。あるいは、[既存のタスク]テーブル内のタスクのレコードエントリをダブルクリックすることもできます。[タスク情報を表示]ウィンドウが表示されます。

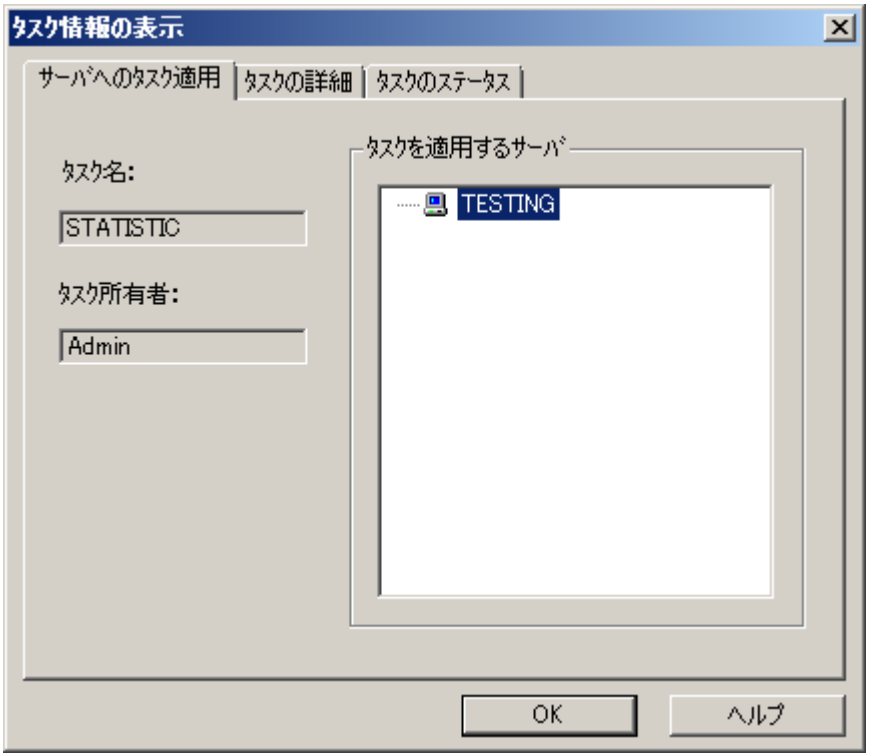


図 3-32. タスクウィンドウを表示

この画面には、[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]というラベルの付いた 3 つのタブセクションが含まれています。

- [サーバへのタスク適用]: [タスク名]と[所有者]はタブの左側に表示されます。[対象サーバ]はタスクが実行されるネットワーク上のすべてのサーバーを表示します。
- [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。[タスク順序] リストの機能をクリックすると、右のタスク定義テーブル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]は、タスクが実行されるネットワーク上のすべてのサーバーを表示します。[ステータス]、[前回の実行日時]、および[次回の実行予定]フィールドは、タスクのステータスと最後に実行された時間を表示します。

4. [OK]をクリックして[タスク情報を表示]ウィンドウを閉じます。

既存のタスクの削除

は[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に関する情報が表示されます。次を使用できます。[既存のタスク]リストをクリックしてタスク定義を削除します。

手順

1. 次のいずれかの操作を実行します。
   - メインメニューで[実行] > [既存のタスク]をクリックします。
   - サイドバーで[タスク] > [既存のタスク]をクリックします。
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] 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 通知には標準アラートとアウトブレイクアラートが含まれます。アラートは様々な方法で配信されます。すべての配信オプションについては 143 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/グレーウェア検出]: サーバ上のスパイウェア感染ファイルの検出
- [書込み禁止ファイル変更の試み]: 書き込み保護された設定を変更しようとする試み
- [リアルタイム設定の変更]: リアルタイム検索の設定変更
- [サービスの起動/停止]: ServerProtect を停止/開始する
- [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
- [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

一般の警告の設定

手順

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ます。
   - メインメニューで[設定] > [通知] > [一般の警告]をクリックします。
   - サイドバーで[通知の設定] > [一般の警告]をクリックします。

   [一般の警告]画面が表示されます。

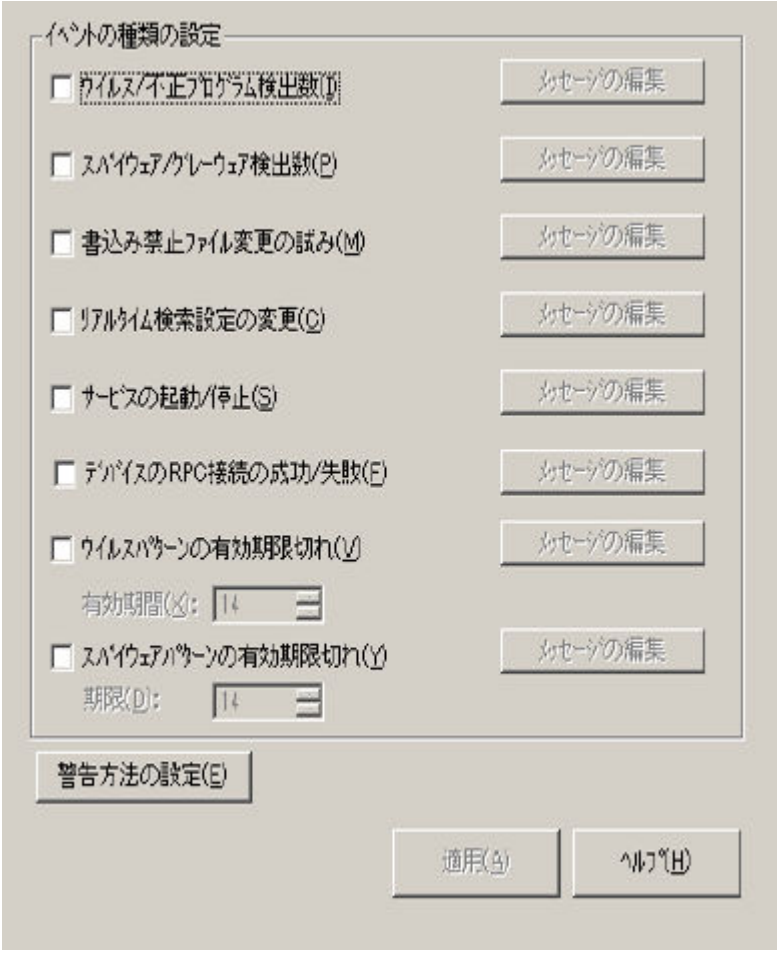


図 3-33. ServerProtect 一般の警告の設定

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. 各選択イベントに対して[メッセージの編集]をクリックしてください。

   [警告メッセージの編集]ウィンドウが表示されます。
5. 警告メッセージの内容を入力したら、[OK] をクリックしてウィンドウを閉じます。(日本語での入力も可能です。)
6. [警告方法の設定]をクリックして通知方法を選択してください。詳細については 143 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の設定

手順

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ます。
   - サイドバーで[通知の設定] > [ウイルスアウトブレークアラート]をクリックします。

- メインメニューで[設定] > [通知] > [ウイルスアウトブレークアラート]をクリックします。

[ウイルスアウトブレークアラート]画面が表示されます。

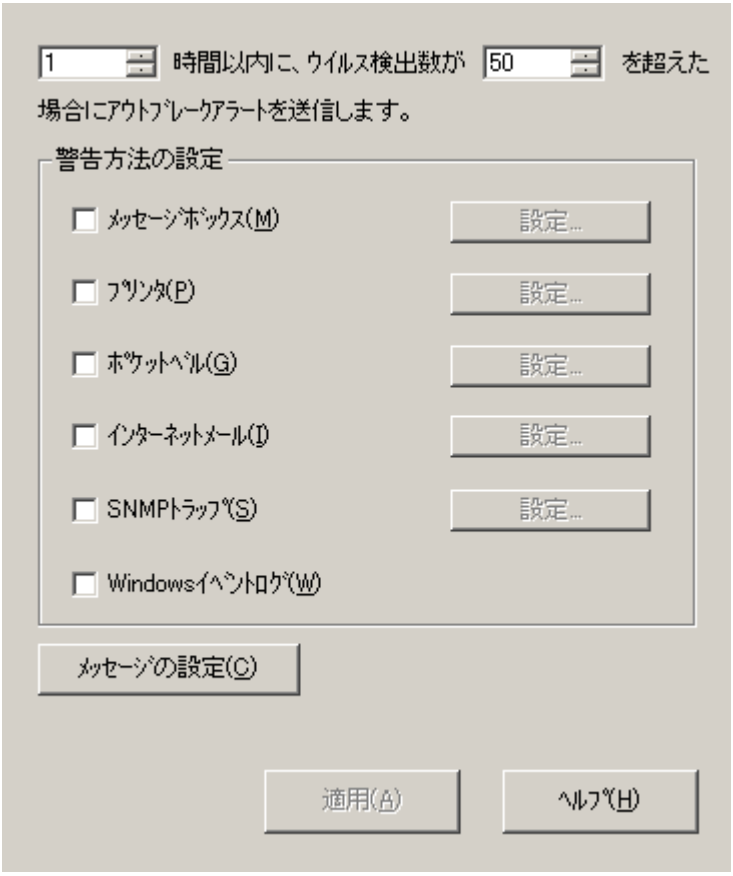


図 3-34. ServerProtect アウトブレークアラートの設定

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] 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、143 ページの「警告方法の設定」 を参照してください。

6. [警告メッセージ] の下で、[メッセージの編集] をクリックし、ウイルスのアウトブレークが発生した場合に表示するメッセージを設定することができます。

7. [適用]をクリックして設定を保存します。

警告方法の設定

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

- [メッセージボックス]: 管理者のコンピュータに、標準的な Windows ポップアップメッセージボックスが表示されます。
- [プリンタ]: メッセージがローカルまたはネットワークプリンタに送信されます。
- [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、トレンドマイクロ ServerProtect が動作しているサーバにモデムが接続されている必要があります。
- [インターネットメール]: ウイルス検出時にメールメッセージが送信されます。
- [SNMP トラップ]: SNMP によってネットワーク管理者にアラートメッセージが送信されます。これは、会社内で導入されている他の SNMP 互換の管理ツールと統合されます。
- [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。

複数の通知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、このドキュメントで説明します。他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) 警告を送信するための設定

手順

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ます。
   - アウトブレークアラートを設定するには
     - サイドバーで[通知の設定] > [ウイルスアウトブレークアラート]をクリックします。
     - メインメニューで[設定] > [通知]をクリックし、次に[ウイルスアウトブレークアラート]をクリックします。
   - 一般の警告を設定するには
     - メインメニューで[設定] > [通知] > [一般の警告]をクリックし、次に[警告方法の設定]をクリックします。
     - サイドバーで[通知の設定] > [一般の警告]をクリックし、次に[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選択し、[設定]をクリックします。

   [インターネットメールを設定]ウィンドウが表示されます。

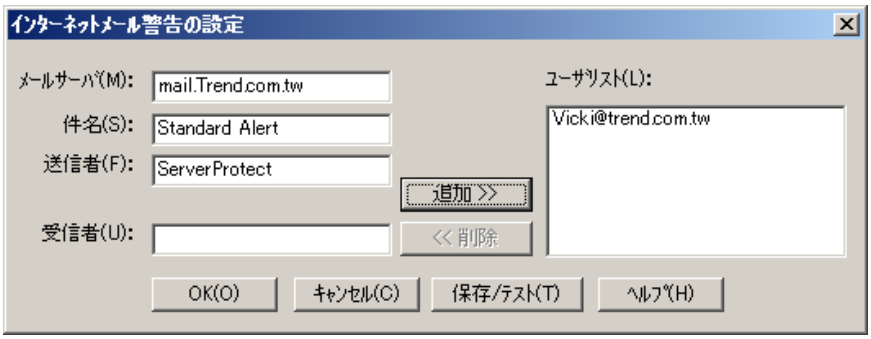


図 3-35. インターネットメール警告ウィンドウの設定

4. 次の手順に従ってください。

   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. [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 [ユーザへ] 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 [追加と削除] 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、[保存/テスト]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. [OK]をクリックして設定変更を保存し、[警告方法の設定]ウィンドウに戻ります。

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 のウイルス検出には、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、選択した 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[検索結果の表示]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。

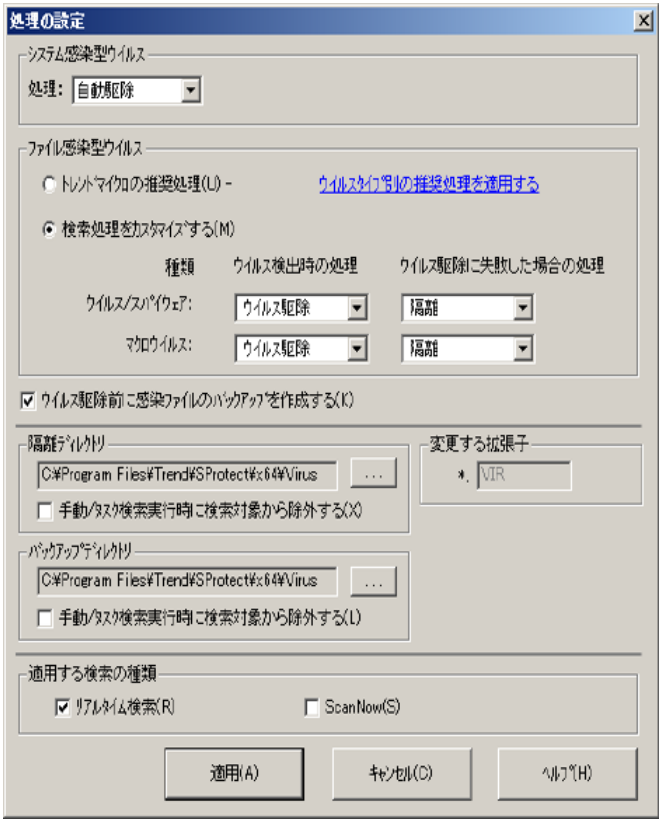


図 3-36. ウイルスアクション設定ウィンドウ

手順

1. [ScanNow]または[リアルタイム検索]の設定エリアから[処理の設定]をクリックします。ウイルスアクション設定ウィンドウが表示されます。

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. 未満[システム感染型ウイルス]で[処理]リストで、必要なウイルス対策をクリックします。ServerProtect ブートウイルスが検出されたときに取得します。選択できます[自動駆除]または[放置] 。

3. [ファイル感染型ウイルス]の下で、次のいずれかを行います。

   - [トレンドマイクロの推奨処理]をクリックして、トレンドマイクロ推奨ウイルス対策を設定します。スパイウェア感染に対して取れるアクションは[放置]に限られており、スパイウェア感染を処理するための[ウイルス駆除]アクションはサポートされていません。スパイウェアに感染したファイルに[ウイルス駆除]アクションを適用すると、ファイルが削除されます。

     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]をクリックして、[処理]および[ウイルス駆除に失敗した場合の処理]リスト内のファイルおよびマクロウイルスに対して適切なアクションを選択します。23 ページの「ウイルスを検出した場合」を参照してください。ActiveAction の詳細については、31 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] チェックボックスを選択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と隔離ディレクトリの両方を検索から除外する必要があります。詳細については、オンラインヘルプの[ディレクトリ除外リスト]トピックを参照してください。選択された検索の種類は[適用する検索の種類]の下に表示されます。

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ストレージデバイスを保護します。 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。詳細については、オンラインヘルプの[スキャンプロファイルの選択]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。133 ページの「既存タスクの変更」を参照してください。

スキャンプロファイルの保存

手順

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。

   156 ページの「リアルタイム検索の設定」と 160 ページの「ScanNow 検索の設定」を参照してください。

2. [保存として/プロファイルの削除]をクリックします。

[プロファイルの保存/削除]ウィンドウが表示されます。

図 3-37. [プロファイルの保存/削除] ウィンドウ

3. [プロファイル名]テキストボックスにプロファイル名を入力してください。
4. [保存]をクリックして新しいプロファイルを保存します。あるいは、[閉じる]をクリックして保存せずにウィンドウを閉じます。

スキャンプロファイルの削除

手順

1. 次のいずれかの操作を実行します。
   - サイドバーで[ScanNow] > [ScanNow]をクリックします。
   - メインメニューで[実行] > [ScanNow]をクリックします。
   - サイドバーで[[検索オプション] を設定] > [リアルタイム検索]をクリックします。
2. [プロファイルの保存として/削除]をクリックします。

   [プロファイルの保存/削除]ウィンドウが表示されます。

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]をクリックしてプロファイルを削除します。削除せずにウィンドウを閉じるには、[閉じる]をクリックしてください。

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。

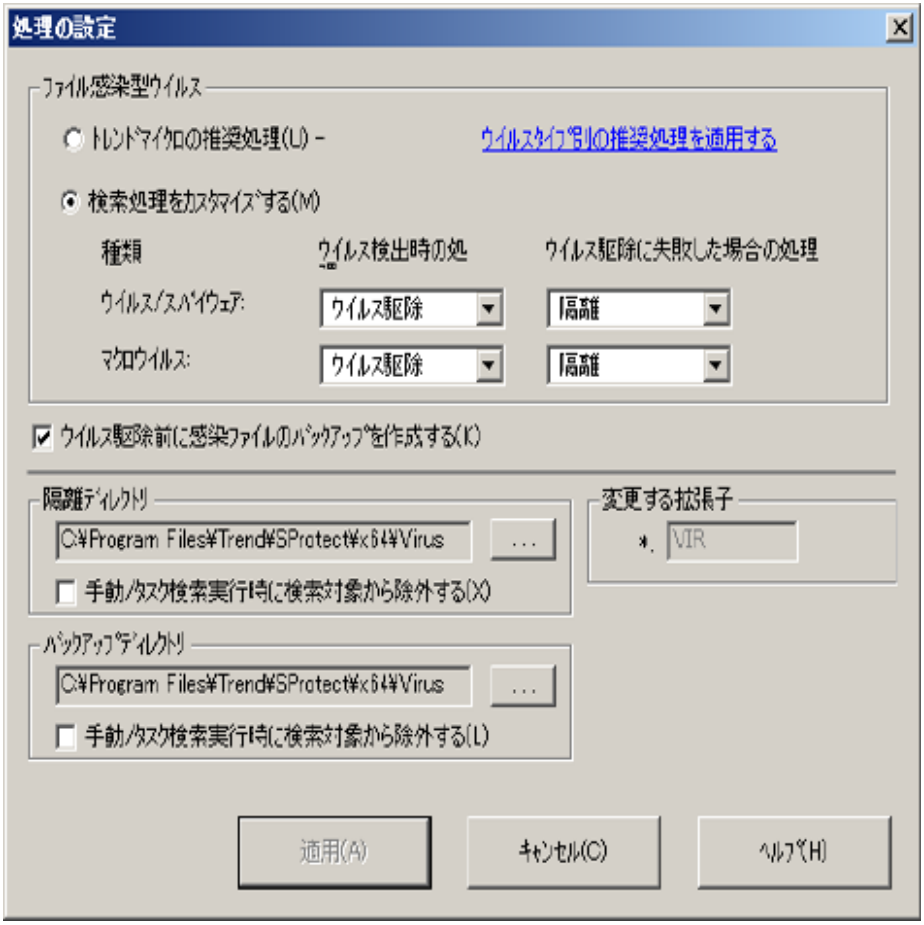


図 3-38. [処理の設定] ダイアログボックス

手順

1. [ストレージ検索サービス]設定エリアから[処理の設定]をクリックします。[処理の設定]ダイアログが表示されます。
2. [ファイル感染型ウイルス]の下で、次のいずれかを実行してください。
   - [トレンドマイクロの推奨処理を使用]をクリックして、トレンドマイクロ推奨のウイルス対策を設定します。スパイウェア感染に対して取れるアクションは[放置]に限られており、スパイウェア感染に対して[ウイルス駆除]アクションはサポートされていません。スパイウェアに感染したファイルに[ウイルス駆除]アクションを適用すると、ファイルが削除されます。
   - [検索処理をカスタマイズする]をクリックして、[処理]および[ウイルス駆除に失敗した場合の処理]リスト内のファイルおよびマクロウイルスに対して適切なアクションを選択します。23 ページの「ウイルスを検出した場合」を参照してください。ActiveAction の詳細については、31 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、トレンドマイクロ 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] チェックボックスを選択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は[適用する検索の種類]の下に表示されます。
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ストレージデバイスを保護します。 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。

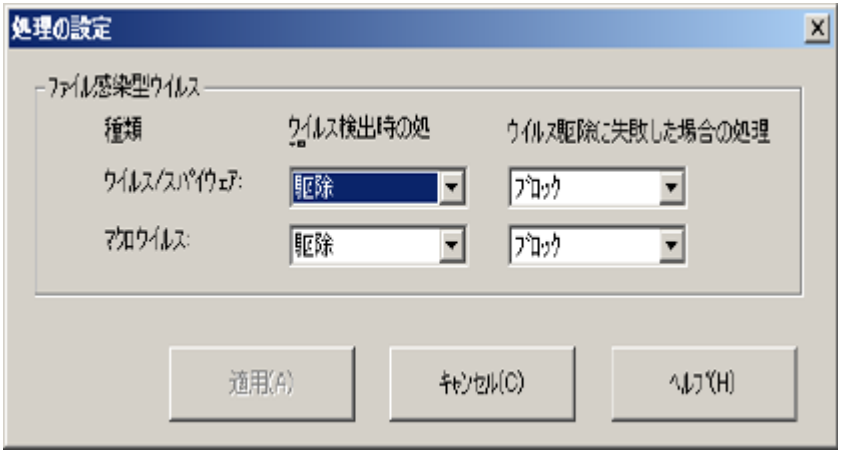


図 3-39. [処理の設定] ダイアログボックス

手順

1. [ストレージ検索サービス]設定エリアから[処理の設定]をクリックします。[処理の設定]ダイアログが表示されます。
2. [ファイル感染型ウイルス]の下で、[処理]および[ウイルス駆除に失敗した場合の処理]リスト内のファイルウイルスとマクロウイルスに対して取るべき適切なアクションを選択します。詳細は 23 ページの「ウイルスを検出した場合」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。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。

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 には、特許取得済みの MacroTrap™技術が含まれており、Microsoft™ Office ファイルおよびテンプレートにおける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]: このオプションは埋め込みファイルを検索します。OLE レイヤー検索は 5 層の保護を提供します。詳細は 30 ページの「OLE 埋め込みの検索」を参照してください。
- [マップされたネットワークドライブの検索]: ServerProtect では、ネットワークドライブを検索対象に選択することができます (あらかじめネットワークドライブを割り当てておく必要があります)。

リアルタイム検索の設定

手順

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ます。
   - サイドバーで[[検索オプション]] > [リアルタイム検索]をクリックします。
   - メインメニューで[設定] > [検索オプション] > [リアルタイム検索]をクリックします。

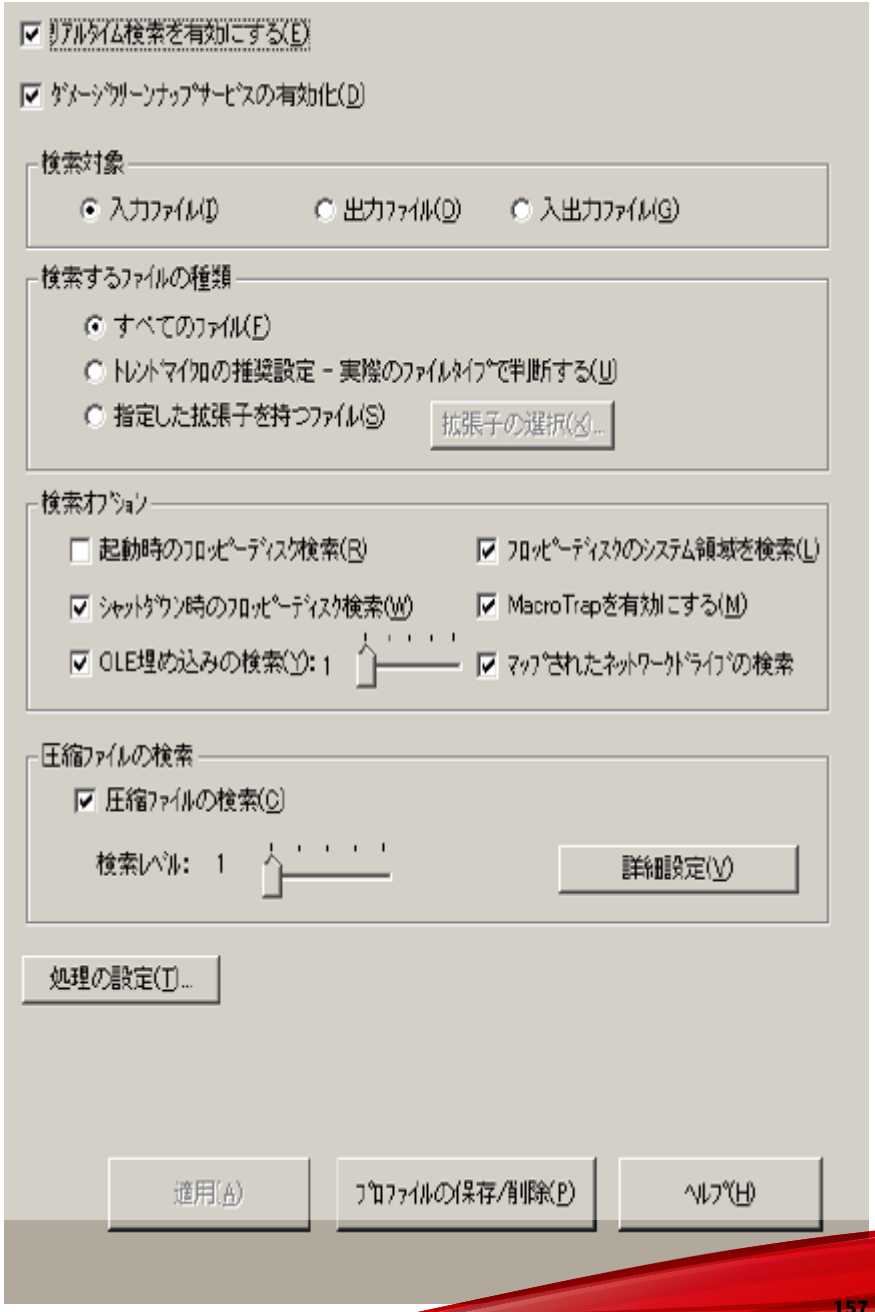


図 3-40 リアルタイム検索の設定

3. [リアルタイム検索を有効にする]チェックボックスを選択します。
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 ビットプラットフォームをサポートしています。 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. [検索方向] グループで次のオプションを選択します。
   - [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]: サーバからコピーされるファイルを検索します
   - [入出力]: 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]: すべてのファイルタイプをスキャン
   - [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

     31 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]: 指定されたファイルのみをスキャン

     [指定した拡張子を持つファイル]を選択した場合、検索したいファイルタイプを定義するには[拡張子の選択]をクリックしてください。180 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、155 ページの「リアルタイム検索」を参照してください。

8. 圧縮ファイルを検索する場合は、[圧縮ファイルを検索] 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設定します。詳細設定については、オンラインヘルプの [圧縮ファイルの検索] トピック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]をクリックして、ServerProtect が感染ファイルに対してどのように動作するかを設定します。147 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]をクリックして設定を保存するか、または[プロファイルとして保存]をクリックして、設定を適用せずに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ストレージデバイスを保護します。 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
- 処理の設定

ScanNow 検索の設定

手順

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) の設定画面を表示します。
   - サイドバーで[ScanNow] > [ScanNow]をクリックします。
   - メインメニューから[実行] > [ScanNow]をクリックします。

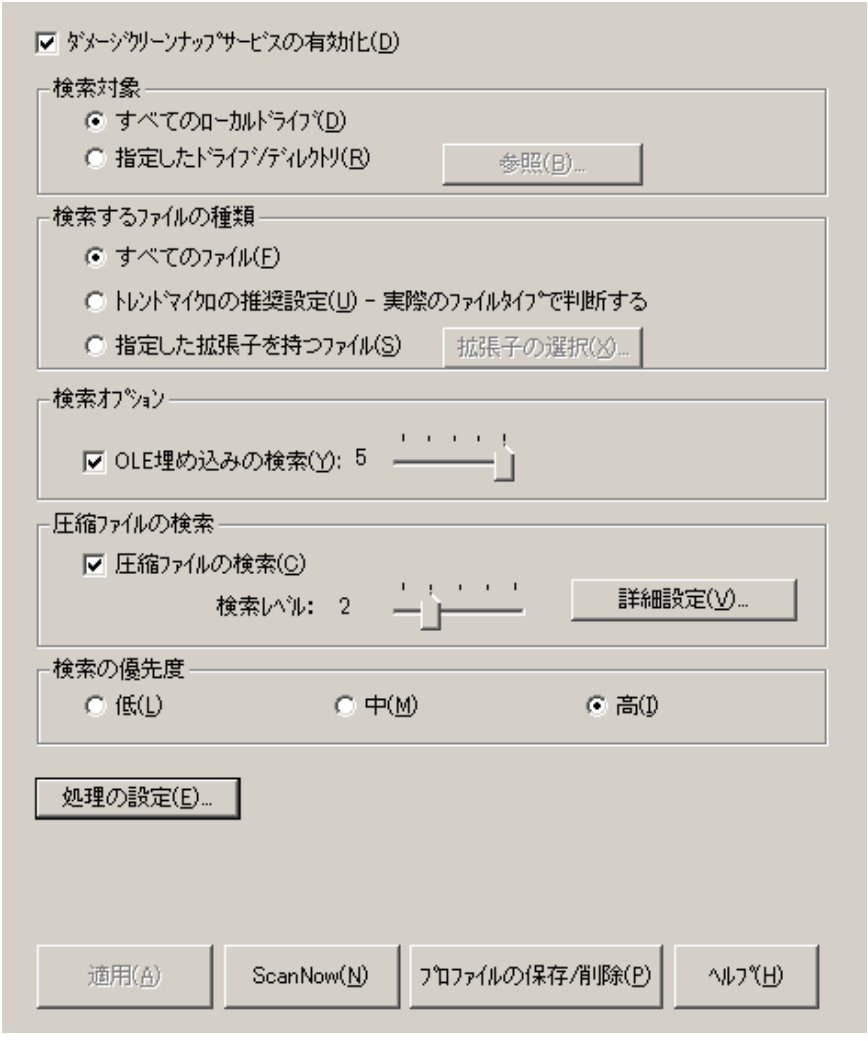


図 3-41. 手動検索の設定ウィンドウ

3. [ダメージクリーンナップサービスを有効化] 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]: サーバ内のすべてのドライブをスキャンします
   - [選択したドライブ/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]をクリックします。[ドライブ/ディレクトリの追加]ウィンドウが表示されます。検索したいドライブまたはディレクトリのチェックボックスを選択し、[OK]をクリックしてウィンドウを閉じます。

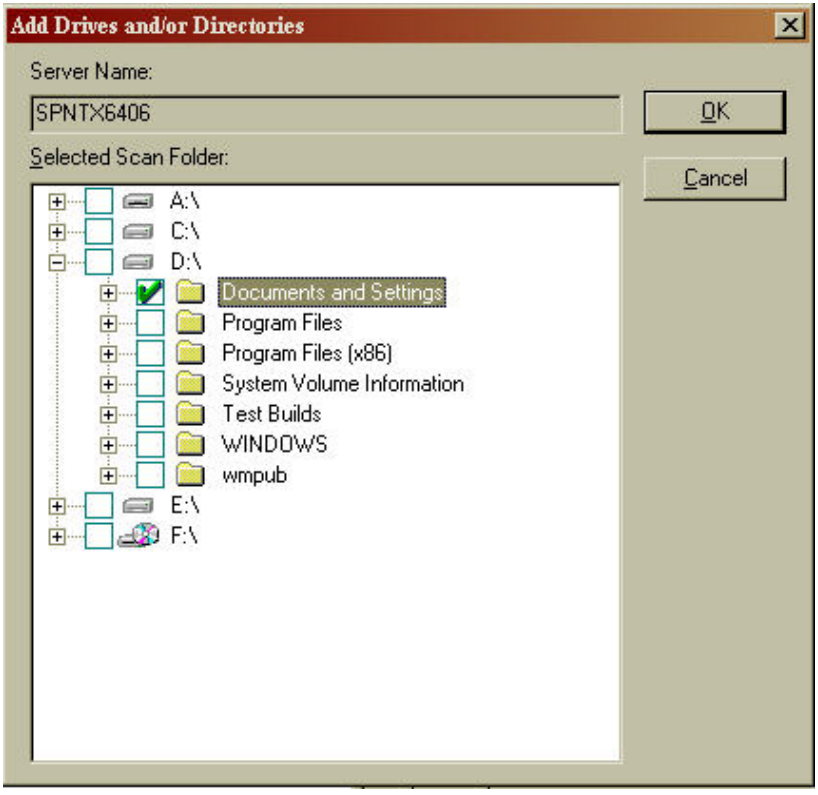


図 3-42. ドライブ/ディレクトリの追加ウィンドウ

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]: すべてのファイルタイプをスキャン
- [[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

  31 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]: 指定されたファイルのみをスキャン

  [拡張子の選択]をクリックして、検索したいファイルタイプを定義します。180 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. [検索オプション]の下で[OLE 埋め込みの検索]を選択します。[OLE 埋め込みの検索]スライダーを動かして OLE 層の数を設定します。ServerProtect は最大 5 層まで検索できます。
7. [圧縮ファイルの検索] の [圧縮ファイルを検索] チェックボックスを選択します。 [検索レベル] スライダを調整して、検索レベル (階層数) を指定します。 詳細設定については、**圧縮ファイル検索** のトピックをオンラインヘルプで参照してください。

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. [検索の優先度]の下で、[低]、[中]、または[高]をクリックします。高検索優先度はより多くの CPU リソースを消費しますが、検索ジョブをより速く完了できます。
9. [処理の設定]をクリックして、ServerProtect が感染ファイルに対してどのように動作するかを設定します。147 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内容を保存するか、または [プロファイルとして保存] ボタンをクリックして、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検索の検索対象、検索するファイルの種類などの設定で検索が実行されます。

ScanNow ツールを実行する

手順

1. 通常のサーバで[スタート] > [すべてのプログラム] > [アクセサリ] > [エクスプローラー]をクリックします。

   [エクスプローラー]ウィンドウが表示されます。

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 ツールを停止する

手順

1. 通常のサーバで[スタート] > [ファイル名を指定して実行]をクリックします。実行ウィンドウが表示されます。

2. [参照]をクリックして、ScanNow.EXE ファイルを見つけてください。

   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

ファイル名と停止スイッチの間にスペースを入れる必要があります。

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ファイルが検索されます。これにより、一般サーバの定期的な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、126 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、ServerProtect が自動的にサーバに検索タスクを適用します。デフォルトの検索タスクは、毎週金曜日にすべてのローカルディレクトリを検索するように設定されています。

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 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

手順

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。
   - サイドバーで[[検索オプション]] > [ストレージ検索サービス]をクリックします。
   - メインメニューで[実行] > [ストレージ検索サービス]をクリックします。

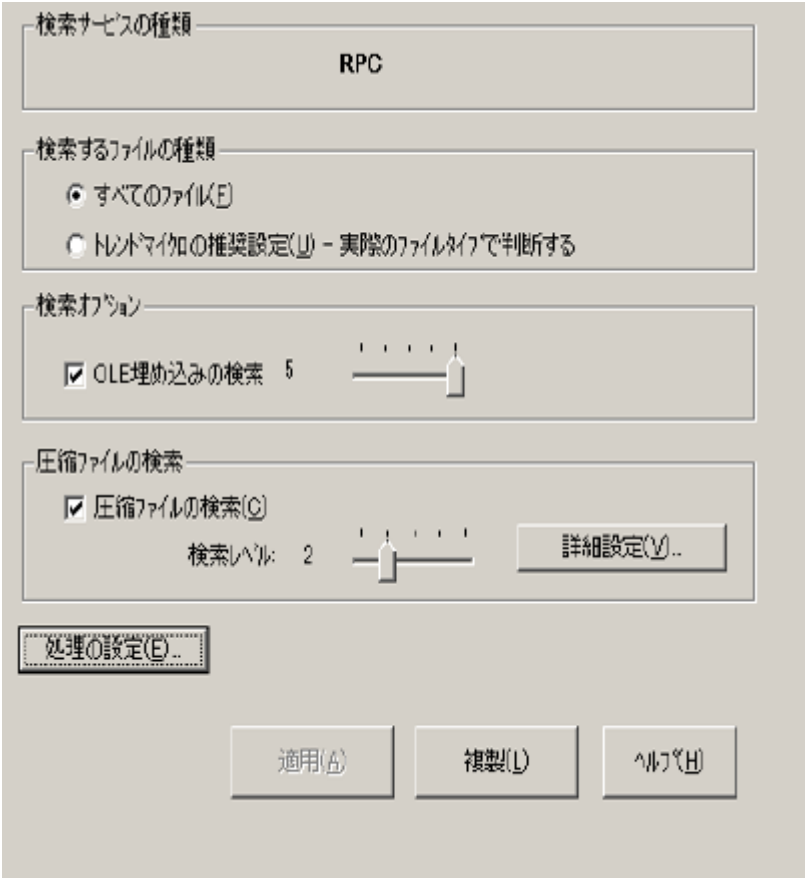


図 3-43. RPC 検索サービスの設定

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スキャン
   - [IntelliScan を使用]: 真のファイルタイプ識別を使用してファイルをスキャンします。31 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. [検索オプション]の下で[OLE 埋め込みの検索]を選択します。[OLE 埋め込みの検索]スライダーを動かして OLE 層の数を設定します。ServerProtect は最大 5 層まで検索できます。
5. [圧縮ファイルの検索] の下で、[圧縮ファイルを検索] チェックボックスを選択します。[検索レベル] スライダを調整して、検索レベル (階層数) を指定します。詳細設定については、**圧縮ファイル検索** トピックをオンラインヘルプで参照してください。
6. [処理の設定]をクリックして、ServerProtect が感染ファイルに対してどのように動作するかを設定します。152 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の複製

手順

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。
   - サイドバーで[[検索オプション]] > [ストレージ検索サービス]をクリックします。
   - メインメニューで[実行] > [ストレージ検索サービス]をクリックします。
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。

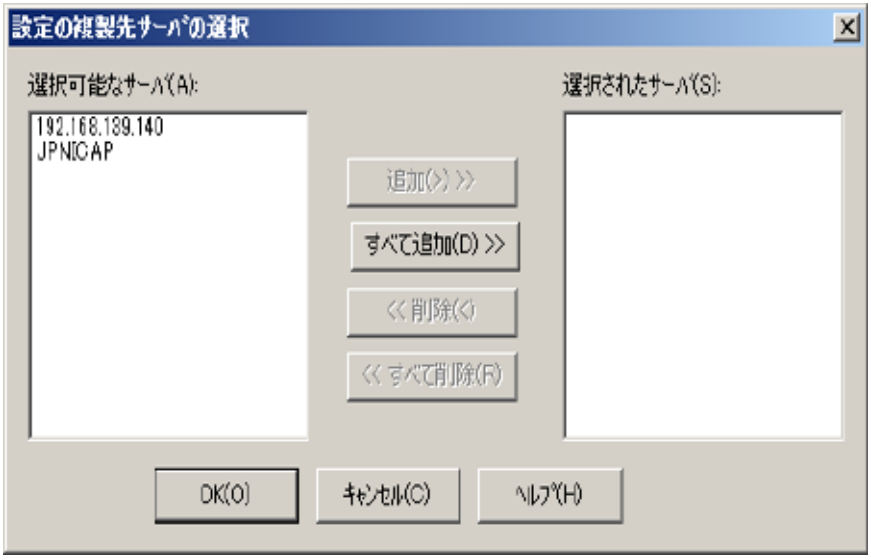


図 3-44. 設定の複製

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、選択した通常サーバを[選択されたサーバ]に追加します。
   - [すべて追加]をクリックして、[選択可能なサーバ]内のすべての通常サーバを[選択されたサーバ]に追加します。
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

ストレージが EMC CAVA をサポートしている場合は EMC CAVA スキャナーを使用し、ウイルススキャンには Huawei Antivirus エージェントを使用してください。EMC CAVA/Huawei Antivirus エージェントは、ストレージデバイスから以下のイベントを受信するとリアルタイム検索を開始します。

- ストレージデバイス上のファイル名が変更されました。
- ファイルがストレージデバイスにコピーまたは保存されました。
- ストレージデバイス上のファイルが変更され、閉じられました。

リアルタイム検索をトリガーするためのより厳しい条件を定義したい場合は、ストレージデバイスのドキュメントを参照してください。

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。

- リアルタイム検索の有効化
- ダメージクリーンナップサービスの有効化
- 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
- 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ストレージデバイスを保護します。 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。

手順

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。
   - サイドバーで[[検索オプション]] > [ストレージ検索サービス]をクリックしてください。
   - メインメニューで[実行] > [ストレージ検索サービス]をクリックします。

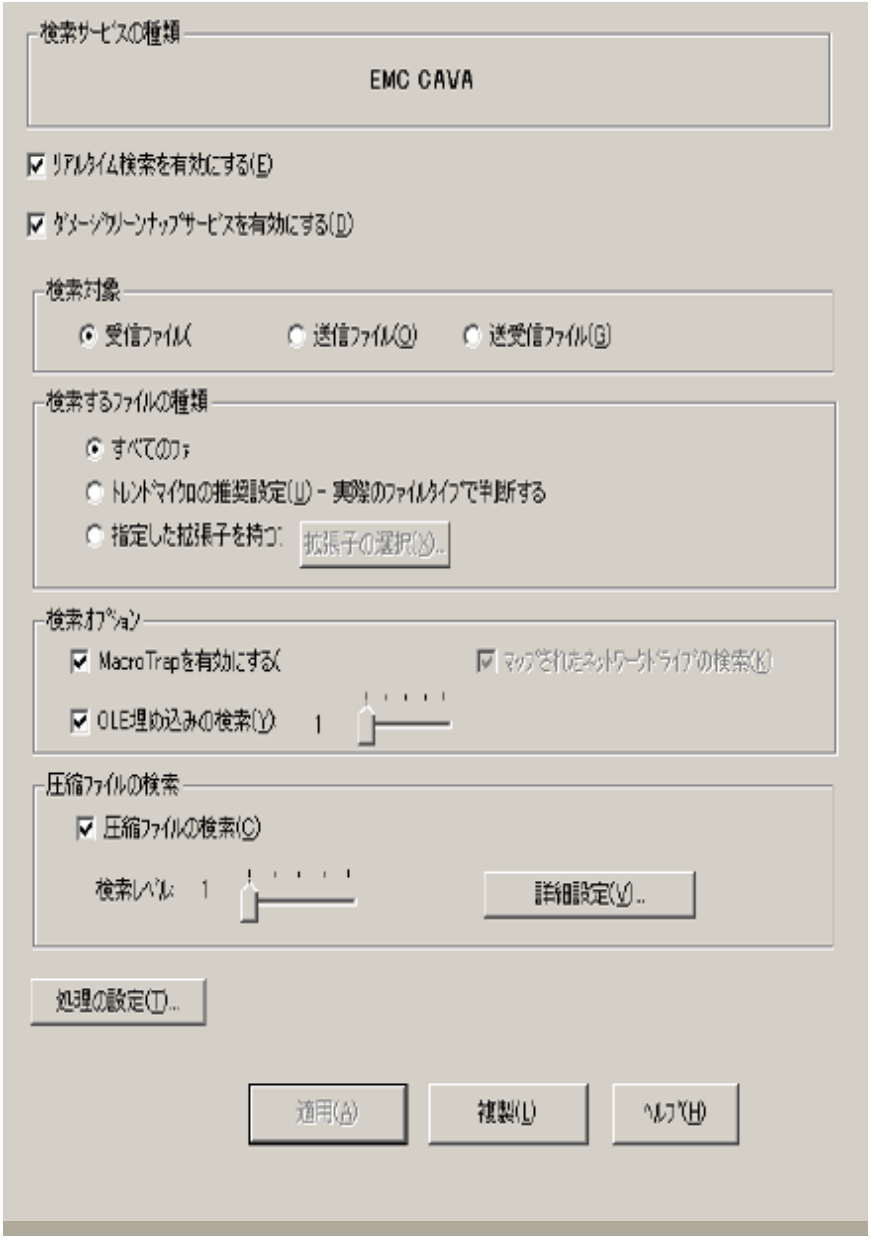


図 3-45. EMC CAVA 検索サービスの設定

3. [リアルタイム検索を有効にする]チェックボックスを選択してください。
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 ビットプラットフォームをサポートしています。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] で、検索するファイルの方向を選択します。
   - [出力]: サーバからコピーされるファイルを検索します
   - [入出力]: サーバ上の入力、出力、両方向のファイルを検索します

   注意

   [入力ファイル]オプションは EMC CAVA/Huawei Antivirus エージェントではサポートされていません。トレンドマイクロは、双方向でファイルをスキャンする[入出力]を選択することを推奨します。
6. [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]: すべてのファイルタイプをスキャン
   - [トレンドマイクロの推奨設定]: 真のファイルタイプ識別を使用してファイルをスキャンします。31 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]: 指定されたファイルのみをスキャン

     [指定した拡張子を持つファイル]を選択した場合は、[拡張子の選択]をクリックして、検索したいファイルタイプを定義してください。180 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、155 ページの「リアルタイム検索」を参照してください。

8. 圧縮ファイルを検索する場合は、[圧縮ファイルを検索] 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選択します。 詳細設定については、オンラインヘルプの**圧縮ファイルの検索**トピック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]をクリックして、ServerProtect が感染ファイルに対してどのように動作するかを設定します。152 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の複製

手順

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。
   - サイドバーで[[検索オプション]] > [ストレージ検索サービス]をクリックします。
   - メインメニューで[実行] > [ストレージ検索サービス]をクリックします。
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。

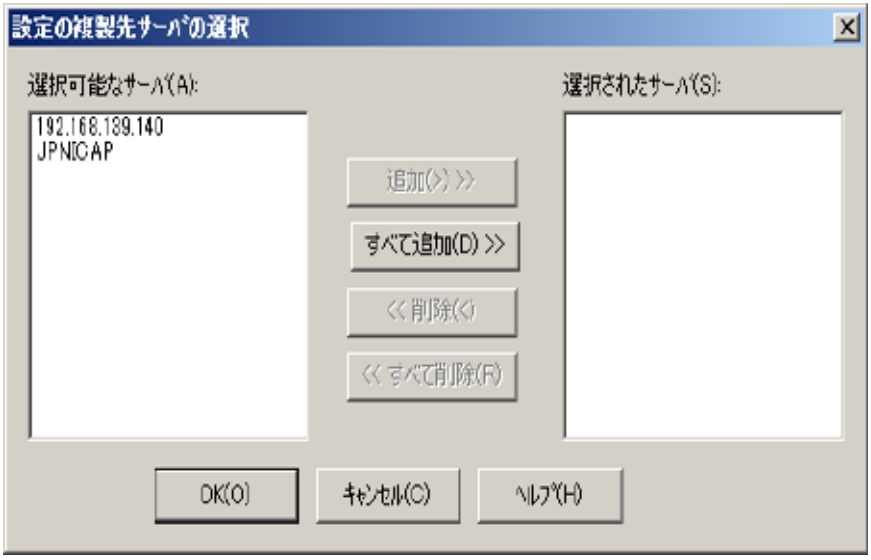


図 3-46. 設定の複製

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、選択した通常サーバを[選択されたサーバ]に追加します。
   - [すべて追加]をクリックして、[選択可能なサーバ]のすべての通常サーバを[選択されたサーバ]に追加します。
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

手順

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。
   - サイドバーで[[検索オプション]] > [ストレージ検索サービス]をクリックします。
   - メインメニューで[実行] > [ストレージ検索サービス]をクリックします。

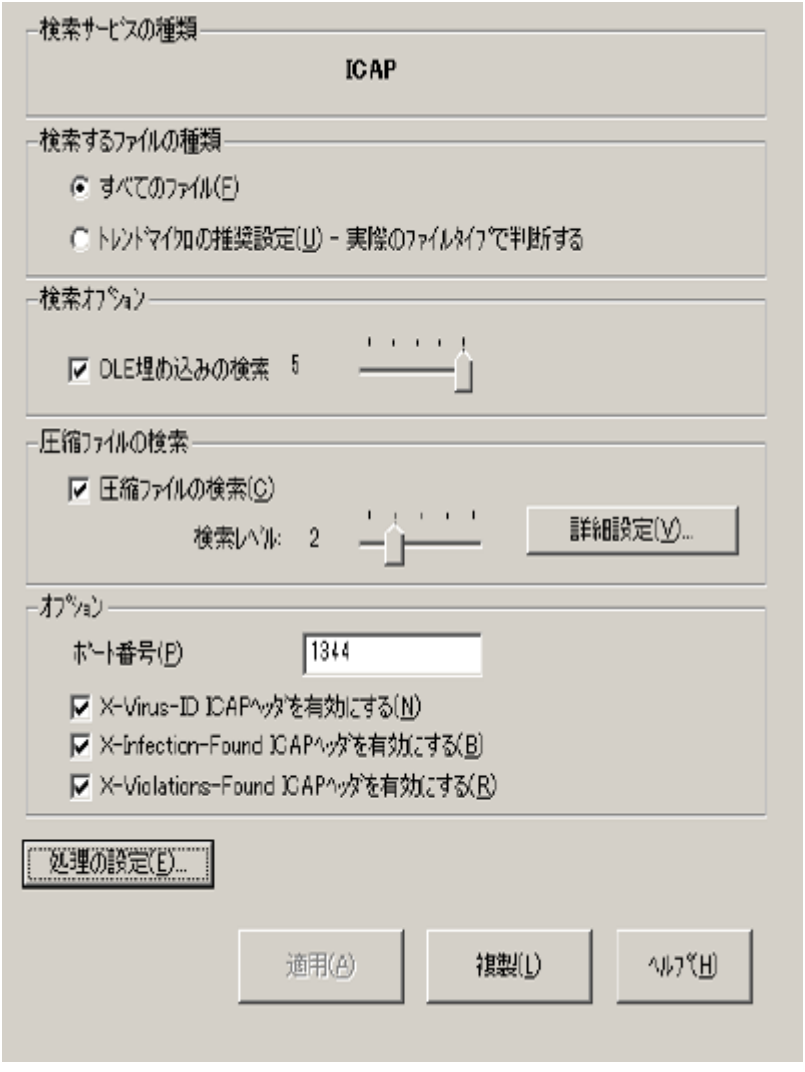


図 3-47. ICAP 検索サービスの設定

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]: すべてのファイルタイプをスキャン

- [トレンドマイクロの推奨設定]: 真のファイルタイプ識別を使用してファイルをスキャンします。31 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. [検索オプション]の下で[OLE 埋め込みの検索]を選択します。[OLE 埋め込みの検索]スライダーを動かして OLE レイヤーの数を設定します。ServerProtect は最大 5 層まで検索できます。

5. [圧縮ファイルの検索] で [圧縮ファイルを検索] チェックボックスを選択します。 [検索レベル] スライダを調整して、検索レベル (階層数) を指定します。 詳細設定については、**圧縮ファイル検索** のトピックをオンラインヘルプで参照してください。

6. [オプション]の下で、次の操作を行ってください。

   - [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]を選択します。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]を選択します。ウイルスが検出されると、ICAP 応答に[X-感染が見つかりました] 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]を選択します。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]をクリックして、ServerProtect が感染ファイルに対してどのように動作するかを設定します。154 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の複製

手順

1. ドメインブラウザツリーで、CAP 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。
   - サイドバーで[[検索オプション]] > [ストレージ検索サービス]をクリックします。
   - メインメニューで[実行] > [ストレージ検索サービス]をクリックします。
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。

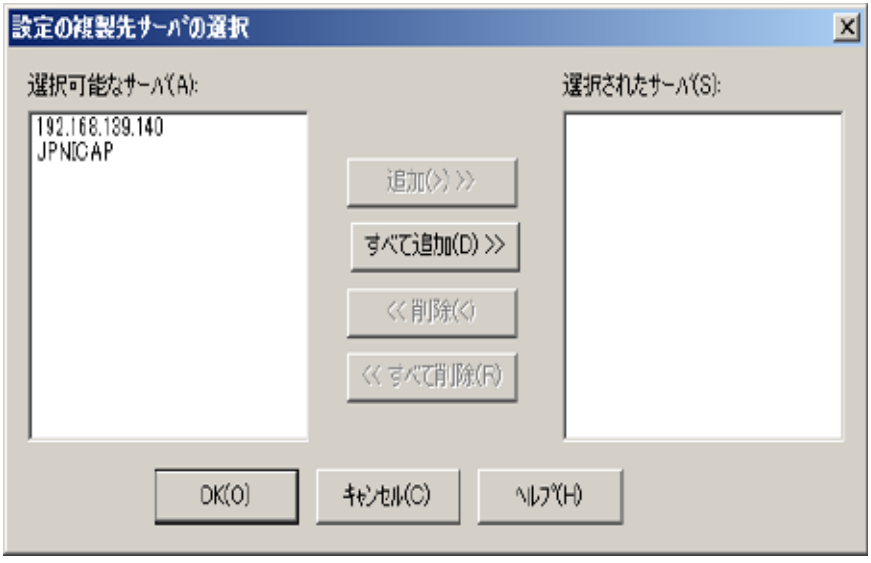


図 3-48. 設定の複製

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、選択した通常サーバを[選択されたサーバ]に追加します。
   - [すべて追加]をクリックして、[選択可能なサーバ]のすべての通常サーバを[選択されたサーバ]に追加します。
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。

手順

1. [リアルタイム検索]または[ScanNow]の設定エリアで、[検索するファイルの種類]の下にある[指定した拡張子を持つファイル]をクリックし、次に[拡張子の選択]をクリックして検索したいファイルタイプを定義します。

次に[検索対象ファイルの選択]ウィンドウが表示されます。

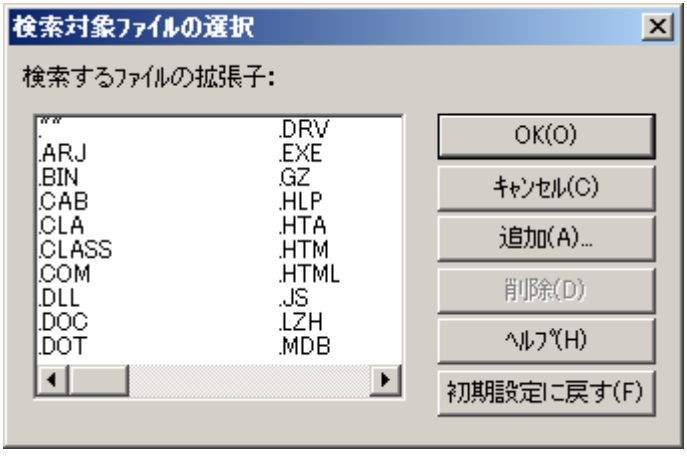


図 3-49. 検索対象ファイルの選択ウィンドウ

2. 次のいずれかの操作を実行します。

   • [追加]をクリックします。[ファイル拡張子の追加]ウィンドウが表示されます。

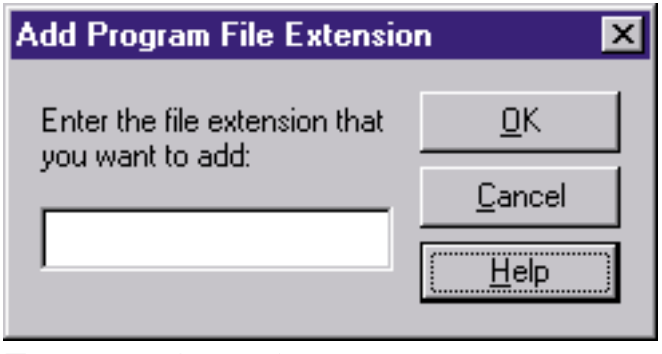


図 3-50. ファイル拡張子の追加ウィンドウ

追加したいファイル拡張子をテキストボックスに入力し、[OK]をクリックしてリストに拡張子を追加します。または、[キャンセル]をクリックして変更を保存せずにウィンドウを閉じます。最後に、[OK]

をクリックして[スキャン対象ファイルの選択]ウィンドウを閉じます。

- [初期設定に戻す]をクリックしてすべてのデフォルトのファイル拡張子を追加し、[OK]をクリックして[スキャン対象ファイルの選択]ウィンドウを閉じます。カスタマイズされた拡張子は失われます。

  デフォルト設定はほとんどの環境に対して十分な保護を提供します。詳細については、182 ページの「スキャン対応ファイル拡張子」を参照してください。

- 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。

スキャン対応ファイル拡張子

ServerProtect はスキャンのために次のデフォルトのファイル拡張子をサポートしています。

- .ARJ
- .CLASS
- .DOT
- .HLP
- .JS
- .MPT
- .OVL
- .PPT
- .SHS
- .VSD
- .XLT
- .BIN
- .COM

- .DRV
- .HTA
- .LZH
- .MSG
- .PIF
- .RAR
- .SYS
- .VST
- .Z
- .CAB
- .DLL
- .EXE
- .HTM
- .MDB
- .OCX
- .POT
- .RTF
- .TAR
- .XLA
- .ZIP
- .CLA
- .DOC
- .GZ
- .HTML
- .MPP

- .OFT
- .PPS
- .SCR
- .VBS
- .XLS

ファイル拡張子を検索対象から除外する

手順

1. 左サイドバーから[[検索オプション]][検索除外リスト]を選択します。
2. メインメニューで[設定] > [検索オプション] > [検索除外リスト]をクリックします。
3. [検索対象から除外するファイル拡張子]の下で、[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。

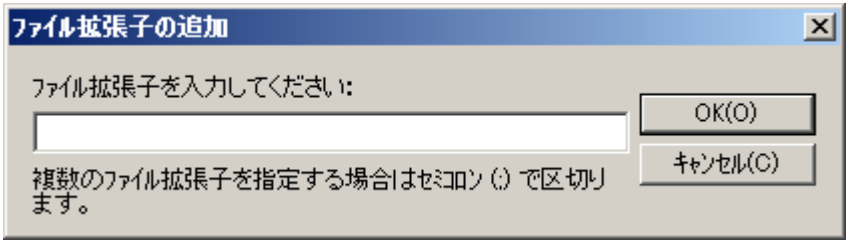


図 3-51. [ファイル拡張子の追加] ダイアログボックス

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 [追加と削除] をクリックします。
7. [適用] をクリックします。

第 4 章

既存の ServerProtect のアップグレード

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

バージョン 6.0 インストールプログラムは、通常のサーバ、情報サーバ、管理コンソールを含む ServerProtect コンポーネントの存在を検出できます。アップグレードと移行機能は ServerProtect インストールプログラムの重要な部分です。この章では、主要な概念を紹介し、ユーザに機能の使用方法を説明します。

さらに本章では、ServerProtect for Storage のトラブルシューティングについても紹介します。

本章で説明する内容には、次の項目が含まれます。

- 187 ページの「ServerProtect アップグレード機能の概要」
- 188 ページの「インストールパッケージを使用した、ServerProtect のローカルアップグレード」
- 190 ページの「インストールパッケージを使用した、ServerProtect のリモートアップグレード」
- 191 ページの「サイレントモードインストールの実行による一般サーバのアップグレード」
- 195 ページの「ServerProtect 体験版のアップグレード」

- 195 ページの「の RPC スキャナーを使用した ServerProtect のトラブルシューティング」

ServerProtect アップグレード機能の概要

多くの ServerProtect のユーザは、ネットワークサーバシステムに以前のバージョンの製品をすでにインストールしています。例えば、ServerProtect5.8 です。ServerProtect6.0 に統合されたアップグレード機能は、ユーザが目的に最も効果的なものを選択できるように、いくつかのアップグレードオプションを提供します。この概要では、各オプションを説明し、関連する重要な概念を紹介します。

1. ServerProtect6.0 のインフォメーションサーバでは、ServerProtect5.8 一般サーバを管理できます。 これにより、インフォメーションサーバをアップグレードした後も、古い一般サーバを引き続き管理できるようになります。

   注意

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

2. ServerProtect のインストールを開始し、最新バージョンである ServerProtect6.0 のインフォメーションサーバがインストールされるよう正しい選択を行います。 既存のインフォメーションサーバをアップグレードするには、インストール時に同じインストール先サーバを選択するだけで済みます。詳細については、188 ページの「インストールパッケージを使用した、ServerProtect のローカルアップグレード」を参照してください。

3. 最新バージョンの管理コンソールがインストールされていない場合は、管理コンソールコンポーネントをインストールします。詳細については、188 ページの「インストールパッケージを使用した、ServerProtect のローカルアップグレード」を参照してください。

4. この時点では、管理コンソールとインフォメーションサーバの準備はできています。 一般サーバは、次の方法でアップグレードできます。

   - インストールパッケージを使用して、ローカルにアップグレードを実行する。
   - インストールパッケージを使用して、ネットワーク経由でリモートにアップグレードを実行する。

- サイレントモードインストールを使用してアップグレードを実行してください。サイレントモードインストールは、一般サーバのみがインストールされているコンピュータのアップグレードに使用してください。他のコンポーネントがインストールされていることが検出されると、サイレントインストーラは終了し、何も実行しません。一般サーバをアップグレードするときはこの方法を使用することをお勧めします。この方法を使用すると、リモートの実行先コンピュータでインフォメーションサーバが誤ってアップグレードされることを回避できます。

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

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

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

ローカルアップグレードセッションを開始するには、インストールパッケージを使用してローカルコンピュータでインストールセッションを起動します。詳細については、45 ページの「ServerProtect のインストール」を参照し

てください。インストールプログラムはユーザを全手順にわたって案内します。次のように[ServerProtect の [コンポーネントの選択]]ウィンドウで:

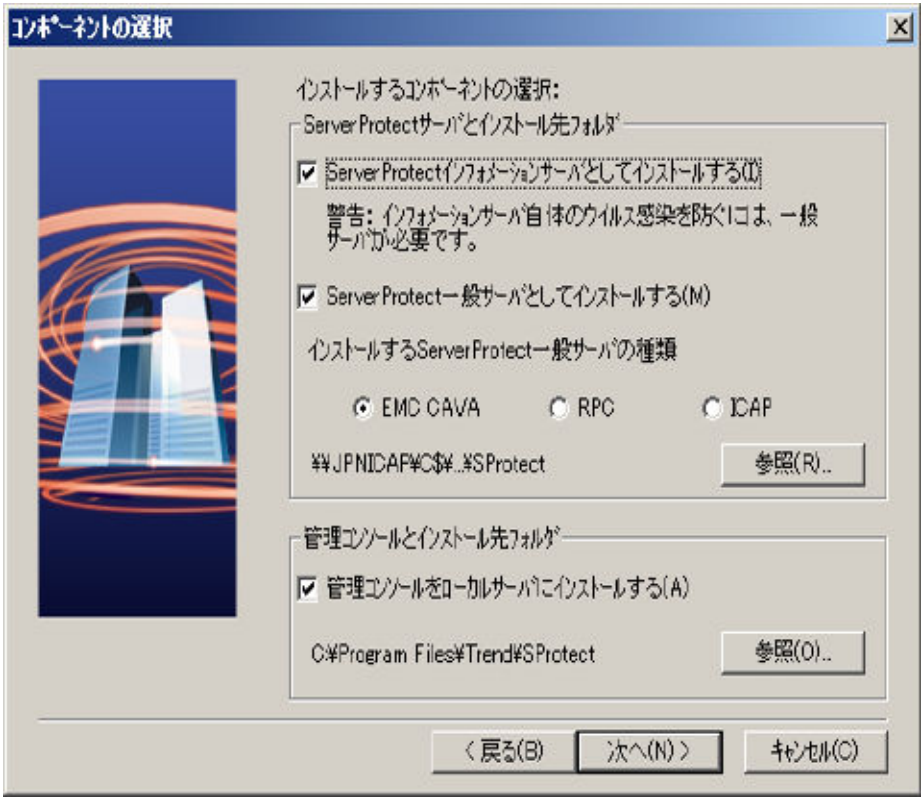


図 4-1. ServerProtect の [コンポーネントの選択] 画面

注意

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

アップグレードが必要なオプションに対応するチェックボックスを設定し、[参照...]をクリックして[ServerProtect インストールパスの選択]ウィンドウを表示します。51 ページの「インフォメーションサーバのインストール」の手

順 3 を参照してください。ローカルコンピュータ上でアップグレードが必要な対象フォルダに移動します。インストールプログラムは、プログラムファイルをコピーし、関連するすべてのサービスを開始した後にアップグレードを完了します。

注意

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

注意

トレンドマイクロ Control Manager エージェントがインストールされている場合、Information サーバがインストールされた後にアップグレードする必要があります。

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

ServerProtect をリモートでアップグレードする方法は、ローカルで行う方法とあまり変わりません。ServerProtect インストールプログラムが起動したら、契約条件に同意し、正しいシリアル番号を入力します。すると、ServerProtect の [コンポーネントの選択] ウィンドウが表示されます。アップグレードの候補として一般サーバを選択し、[ブラウザー...] ボタンを使用して実行先のサーバを指定します。ユーザは、接続されているサーバネットワークシステムに移動し、アップグレード対象の一般サーバまたはインフォメーションサーバを検索することができます。そして、ローカルアップグレードのときと同じアップグレード操作を実行します。詳細については、45 ページの「ServerProtect のインストール」 を参照してください。

注意

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

サイレントモードインストールの実行による一般サーバのアップグレード

Microsoft Windows 環境では、DOS コマンドラインウィンドウでプログラムを実行すると、一定のメリットがあることはよく知られています。Windows シェルは、スクリプトファイル内のコマンドを解釈することが可能であるので、特定のタスクを自動化するためのスクリプトファイルを作成できます。ServerProtect6.0 では、インストールプログラムをサイレントモードで起動できるので、ユーザはこの利点を活用できます。

注意

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

サイレントモードでのインストール

手順

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

   注意

   読み取り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。

   一般サーバとしてインストールしたいサーバからこのフォルダにアクセスできることを確認してください。 複数のサイレントインストールを実行する場合、インストール先のサーバに SMS フォルダをマッピングします。

3. インストール先のサーバで、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 NetApp 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。

   ```
   <drive>:\setup -SMS -s -m"SPFS"
   ```

   例:

   a. インストール先サーバで、SMS フォルダをドライブ"M"に割り当てます。

   b. コマンドプロンプトを開きます。

   c. 「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、対象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。

a. ソースフォルダで Setup.ini ファイルを探します。

b. 次の行を追加します。

```
[CommonSection]
```

```
ServerTargetUNCPath=D$\Utility\AntiVirus\SProtect
```

説明:

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

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

```
[CommonSection]
```

```
ServerTargetSN=XXXX-XXXX-XXXX-XXXX-XXXX
```

説明:

XXXX-XXXX-XXXX-XXXX-XXXX: 有効なシリアル番号

インフォメーションサーバでドメインコントローラが使用されているため、「SMS」ドメインに一般サーバを登録できない場合があります。 この

問題を解決するには、サイレントインストールを実行する前に、IP アドレスを設定します。

IP アドレス指定してインストールするには

a. SMS フォルダで `Setup.ini` ファイルを探します。

b. `AgentName` の横にあるホスト名をその IP アドレスで置き換えて、ファイルを保存します。

注意

アップグレードをサイレントモードで実行する際は、アップグレードする必要のあるすべてのインストール先サーバが含まれるように、SMS フォルダの共有について注意を払ってください。 この強力なツールの使用に関する詳細については、64 ページの「サイレントモードで ServerProtect をインストールする」を参照してください。

ServerProtect for NetApp または EMC Celerra のアップグレード

古いバージョンの ServerProtect for NetApp または EMC Celerra を使用している場合、新しいバージョンにアップグレードできます。 ServerProtect for NetApp および EMC Celerra のアップグレード手順は、Windows 版の ServerProtect と同じです。

注意

NetApp または EMC Celerra 用の ServerProtect から本バージョンにアップグレードしても、以前のインストールの設定オプションはすべてそのまま維持されます。

古いバージョンの ServerProtect for NetApp または EMC Celerra をアップグレードするには、次の手順を実行してください。

1. この新バージョン用のシステム要件を確認します。
2. 187 ページの「ServerProtect アップグレード機能の概要」を参照してください。

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、Storage の登録バージョンの ServerProtect にアップグレードしてください。 体験版 ServerProtect を製品版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。

の RPC スキャナーを使用した ServerProtect 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 NetApp 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 NetApp 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:

のネットアップデバイスでサイズの大きいファイルを検索する場合 ServerProtect の RPC スキャナを使用したストレージの場合、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¥Current
   Version¥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、検索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 NetApp 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。

```
device> 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。

```
device> vscan extensions add vbs
```

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

ServerProtect を Trend Micro Control Manager で管理する

注意

Trend Micro Control Manager は Trend Micro Apex Central に名前が変更されました。このドキュメントで言及されているすべての Control Manager の機能と設定は Apex Central に適用されます。

ServerProtect サーバが提供できる情報を活用するには、ServerProtect サーバを Control Manager に登録してください。ServerProtect は、情報サーバサービスと共に同じコンピュータにインストールされたトレンドマイクロ管理通信プロトコル (MCP) エージェントを通じて Control Manager と通信します。

本章で説明する内容には、次の項目が含まれます。

- 200 ページの「Control Manager 統合サマリー」
- 201 ページの「Trend Micro Control Manager に登録する」
- 204 ページの「Control Manager での ServerProtect ステータスの確認」
- 204 ページの「Control Manager からの登録解除」

Control Manager 統合サマリー

このトピックでは、Control Manager 7.0 とこの ServerProtect バージョンの統合の程度について説明します。

以下の表に記載されている機能と機能の詳細については、Control Manager ドキュメントを参照してください。

表 5-1. 統合概要

統合機能	関数の詳細
登録	MCP エージェントを介して ServerProtect 管理コンソールから
シングルサインオン	サポートされません。
ライセンス管理	サポートされません。
コマンド追跡	サポート対象
Control Manager から展開されたコンポーネント	すべてのコンポーネント
Control Manager から管理および展開されたポリシー	なし
ユーザ/エンドポイントディレクトリに表示される情報	なし
ログクエリ	ログクエリを実行して製品情報およびログを表示するときに、次のデータビューのいずれかを選択します。 • 製品のステータス情報 • 製品のイベント情報 • ウイルス/不正プログラム情報 • スパイウェア/グレーウェア情報
製品に固有のダッシュボードウィジェット	なし
他の管理下の製品と共有されているダッシュボードウィジェット	なし
静的レポートテンプレート	なし

統合機能	関数の詳細
カスタムレポートテンプレート (事前定義済み)	• TM-管理下の製品の接続/コンポーネントステータス • TM-脅威の概要 (全体) • TM-スパムメール検出の概要 • TM-スパイウェア/グレーウェア検出の概要 • TM-脅威の兆候検出の概要 • TM-ウイルス/不正コード検出の概要
イベント通知	なし
情報漏えい対策 (DLP) インシデントの管理	該当なし
不審オブジェクトと IOC ファイルの管理	該当なし

Trend Micro Control Manager に登録する

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。

手順

1. [スタート] > [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ます。
   - サイドバーで[Control Manager エージェントの設定]をクリックしてください。
   - メインメニューで[実行] > []をクリックします。

[Control Manager エージェントの設定]画面が表示されます。サーバ[登録ステータス]は[Control Manager に未登録]です。

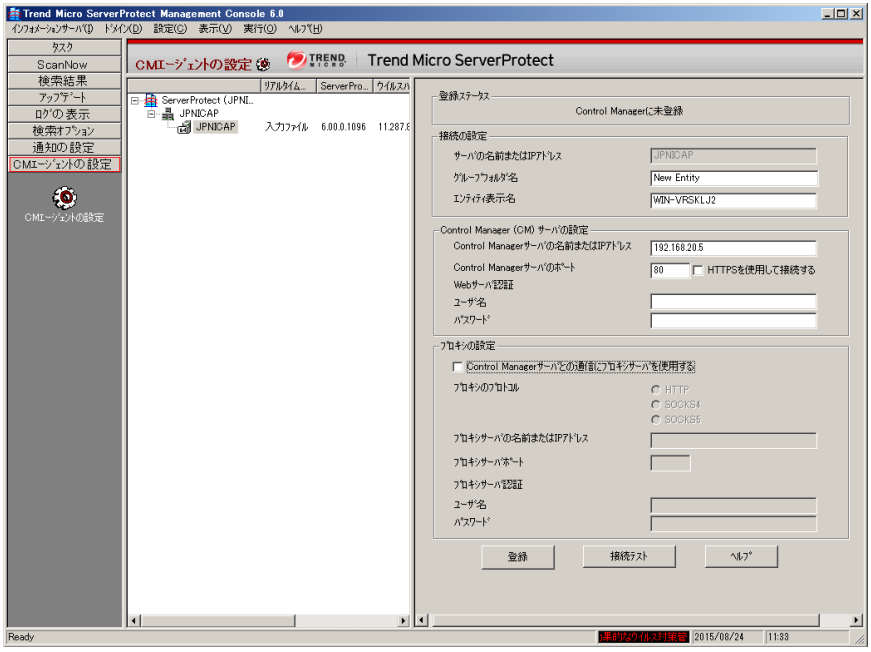


図 5-1. [Control Manager エージェントの設定] 画面

3. 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 情報サーバの名前を入力してください。この名前は Control Manager サーバの製品ディレクトリに表示され、ServerProtect 情報サーバを識別するために使用されるため、慎重に選択してください。ユニークで意味のある名前は、Control Manager の製品ディレクトリで ServerProtect サーバを迅速に識別するのに役立ちます。エンティティ表示名の最大長は 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。

4. [Control Manager (CM) サーバの設定]セクションで、以下を指定してください。

   - [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 アドレスをこのフィールドに入力します。
   - [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 (Control Manager と管理下の製品の MCP エージェントとの間で HTTPS および HTTP 通信が可能) または高 (Control Manager と管理下の製品の MCP エージェントとの間で HTTPS 通信のみ可能) の場合は、[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 ActiveUpdate 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。

5. 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]: プロキシプロトコルを選択してください。

- [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てください。
- [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。

6. [接続テスト]をクリックして、ServerProtect が提供された情報を使用して Control Manager サーバに接続できることを確認します。
ServerProtect が Control Manager サーバに接続できない場合は、提供された設定を確認してください。また、ServerProtect コンピュータと Control Manager サーバの接続を確認してください。
7. [Register]をクリックして設定を保存し、ServerProtect を登録します。

Control Manager での ServerProtect ステータスの確認

手順

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 を Control Manager に登録した際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

別の Control Manager サーバに切り替えたい場合は、まず現在の Control Manager サーバから ServerProtect の登録を解除し、新しいサーバに登録してください。

手順

1. [スタート] > [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ます。
   - 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。
   - メインメニューで[実行] > []をクリックします。

     [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 6 章

テクニカルサポート

ここでは、次の項目について説明します。

- 208 ページの「トラブルシューティングのリソース」
- 208 ページの「製品サポート情報」
- 209 ページの「トレンドマイクロへのウイルス解析依頼」
- 211 ページの「その他のリソース」

トラブルシューティングのリソース

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

サポートポータルの利用

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

https://success.trendmicro.com/dcx/s/?language=ja

脅威データベース

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

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

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

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

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

サポートサービスについて

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

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

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

注意

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

トレンドマイクロへのウイルス解析依頼

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

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

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

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

https://success.trendmicro.com/dcx/s/threat?language=ja

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

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

メールレピュテーションについて

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

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

ファイルレピュテーションについて

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

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

Web レピュテーションについて

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

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

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

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

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

注意

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

付録 A

ServerProtect 製品版へのアップグレード

ServerProtect はシリアル番号を入力しないでインストールした場合、30 日体験版としてインストールされます。このバージョンは完全に機能しますが、30 日後にはウイルススキャンが無効になります。その後は、製品を購入するか、プログラムを削除する必要があります。

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。

- 214 ページの「[ソフトウェア体験版] ダイアログボックス」
- 214 ページの「シリアル番号リストの確認」
- 216 ページの「シリアル番号の入力」
- 217 ページの「よくある質問」

[ソフトウェア体験版] ダイアログボックス

ServerProtect の体験版を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]ウィンドウが表示されます。[ソフトウェア体験版]ウィンドウには、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と、期限が切れるまでの日数が表示されます。

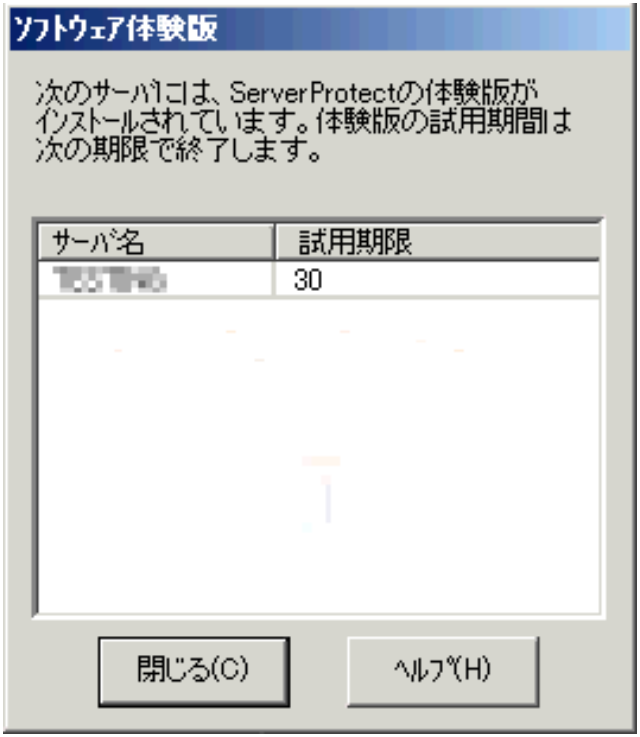


図 A-1. 体験版

シリアル番号リストの確認

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

手順

1. メインメニューで[ヘルプ] > [バージョン情報]をクリックします。

   [ServerProtect 管理コンソールのバージョン情報]ウィンドウが表示されます。

図 A-2. ServerProtect 管理コンソールウィンドウのバージョン情報

2. [シリアル番号]をクリックしてください。

[シリアル番号リスト] ウィンドウが表示されます。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。

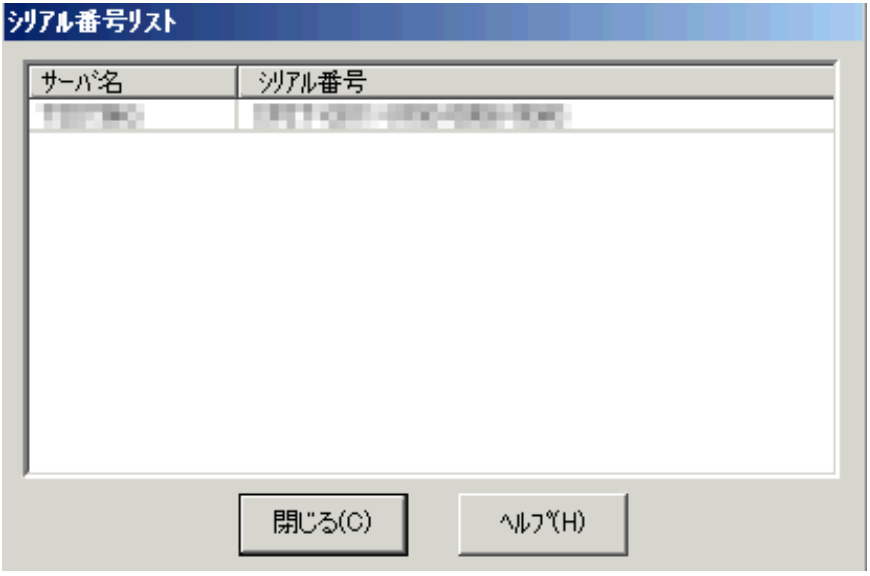


図 A-3. シリアル番号リスト

3. [閉じる]をクリックして[シリアル番号リスト]ウィンドウを閉じ、[OK]をクリックして[ServerProtect 管理コンソールのバージョン情報]ウィンドウを閉じます。

シリアル番号の入力

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。

手順

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. メインメニューで[実行] > [製品版へのアップグレード]をクリックします。

   [新しいシリアル番号の入力]ウィンドウが表示されます。

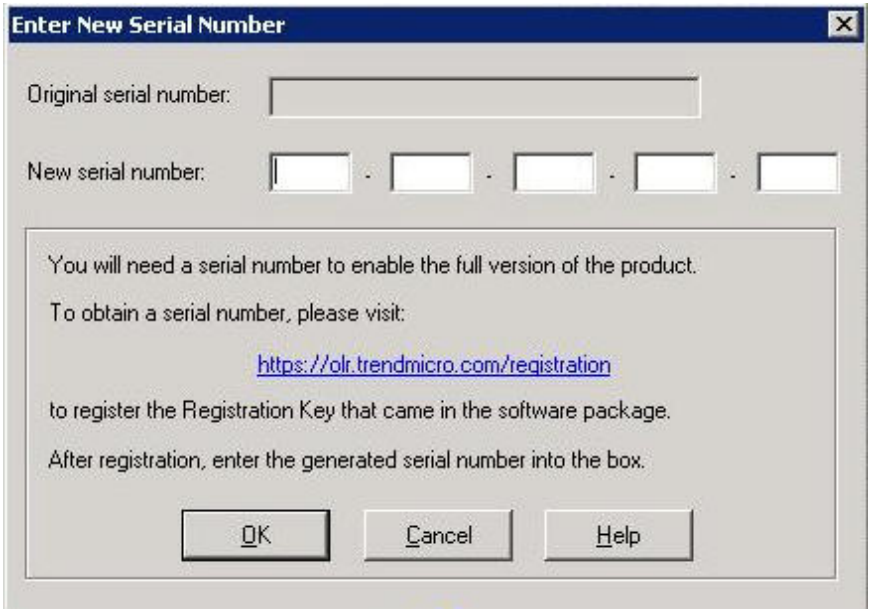


図 A-4. 新しいシリアル番号ウィンドウの入力

3. [新しいシリアル番号] テキストボックスに新しいシリアル番号を入力します。

4. [OK]をクリックしてください。それ以外の場合は、[キャンセル]をクリックしてウィンドウを閉じてください。

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。

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 [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、ServerProtect が既存のすべてのログを Control Manager サーバに送信します。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。

- なぜ Admin.ini で"ExcludeUNCPath"を有効にしても除外リストに単語を登録できないのですか?

  設定された内容は、`Admin.ini` で `ExcludeUNCPath` が有効になっていても、ユーザアクセス制御 (UAC) が有効な場合、管理コンソールに反映されない可能性があります。

- なぜ ServerProtect は Windows ログインパスワードが空白の場合にログイン失敗エラーを表示するのですか?

  Microsoft Windows にはユーザアカウント制限があるため、リモートログインにはパスワードが必要です。そのため、パスワードが設定されていない場合、ServerProtect にログイン失敗エラーが表示されます。

索引