Trend Micro ServerProtect™ for Linux

管理者ガイド

安心を、ひとつ上のステージへ。

TREND MICRO™

トレンドマイクロへのお客様情報の送信について

ソフトウェアにおいて有害サイトのアクセス規制機能、フィッシング対策機能等を有する場合、お客様が当該機能を有効にした上で、コモンゲートウェイインターフェイスアプリケーションを使用しているサーバで構築されているWebサイトにアクセスし、ID、パスワード等を入力した場合には、お客様がアクセスしたWebページのURLにお客様が入力したID、パスワード等が含まれた状態でトレンドマイクロのサーバに送信される場合があります。この場合、トレンドマイクロでは、お客様がアクセスするWebページの安全性の確認のため、これらのお客様より受領した情報にもとづき、お客様がアクセスするWebページのセキュリティチェックを実施します。

輸出規制について

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

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

2008年4月現在、米国により定められる禁輸国は、キューバ、イラン、北朝鮮、スーダン、シリアが含まれています。

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

著作権について

P/N: SPLXFF-AE0200_R1 (2008/7)

目次

はじめに

Trend Micro ServerProtect for Linux (以下、ServerProtect) 3.0 の管理者ガイドをお読みいただき、ありがとうございます。本書では、ServerProtect の設定オプションについて詳細に説明します。

ServerProtect のインストールに必要となる作業内容および基本的な設定について記載されています。本章の内容は、次のとおりです。

ドキュメント

本バージョンの ServerProtect には、次のようなドキュメントが付属しています。

- **クイックスタートガイド** — このガイドでは、ServerProtect を紹介し、インストール計画とインストール方法を説明しています。また、安全なテスト用ウイルスを使用して、インストール内容をテストする方法も説明しています。
- **管理者ガイド (本書)** — このガイドは、ServerProtect の特長や機能について説明しています。製品の設定や管理についてサポートします。また、有用な付録や用語集なども用意されています。
- **オンラインヘルプ** — オンラインヘルプでは、製品の主要タスクの実行方法、使用上のアドバイス、有効なパラメータ範囲や最適値などの入力フィールド情報を提供しています。オンラインヘルプには、ServerProtect の管理コンソールからアクセスできます。
- **man ページ (マニュアルページ)** — ServerProtect には、splxmain、splx、tmsplx.xml、RemoteInstall、および CMconfig のファイルに関する man ページが用意されています。詳細については、186 ページの「man ページへのアクセス」を参照してください。
- **Readme ファイル** — Readme ファイルには、オンラインドキュメントや印刷版ドキュメントには記載されていない最新の製品情報が記載されています。たとえば、新機能の説明、インストールに関するヒント、既知の問題、リリース履歴などが記載されています。
- **製品 Q&A** — 製品 Q&A は、問題の解決方法やトラブルシューティングの情報が格納されたオンラインデータベースです。製品 Q&A では、製品の既知の問題に関する最新情報が提供されます。製品 Q&A には、次の URL からアクセスできます。

  http://esupport.trendmicro.co.jp/

ヒント： トレンドマイクロでは、最新版ダウンロードサイト (http://www.trendmicro.co.jp/download/) から対応するリンクをクリックして、製品ドキュメントの最新版を入手することをお勧めします。

対象読者

本書の読者は、次の内容を含め、中級から上級レベルの Linux システム管理についての知識を持っていることを前提としています。

- Linux サーバのインストールおよび設定
- Linux サーバでのソフトウェアのインストール
- ネットワークの概要 (IP アドレス、ネットマスク、トポロジー、LAN 設定など)
- さまざまなネットワークトポロジー
- ネットワークデバイスおよびその管理方法
- ネットワーク構成 (VLAN、SNMP、SMTP などの使用)

ドキュメントの表記規則

情報を簡単に検索し、理解できるように、ドキュメントでは、次の表記規則を使用しています。

表記	説明
注意：	設定上の注意
ヒント：	推奨事項
警告：	避けるべき操作や設定についての注意

表 1. 本書で使用している表記規則

第 1 章

製品について

Trend Micro ServerProtect for Linux (以下、ServerProtect) は、Linux OS がインストールされたファイルサーバ上のウイルス、ワーム、トロイの木馬、スパイウェア / グレーウェアを検出できます。ServerProtect を使用すると、プラットフォームに依存しない直感的に操作できる Web ベースのコンソールから、ウイルス / 不正プログラムの検索、パターンファイルのアップデート、イベントのレポート、ウイルス対策の設定などを一元的に実行できます。

本章では、次の内容について説明します。

問題

Linux システムは、セキュリティ上のリスクは比較的低いですが、まったく安全というわけではありません。多くの Linux システムは、Windows システム用のファイルサーバとして使用されています。ウイルスや不正プログラムなどのセキュリティリスクにサーバレベルで対処していないと、Windows のセキュリティ侵害要因が瞬時にネットワーク全体に広がる可能性があります。

また、Linux プラットフォームが普及したことにより、Linux サーバを専門に狙ったウイルスや不正プログラムが増加する傾向にあります。Linux プラットフォームに対するウイルスの攻撃は、頻度と危険性が増大しつつあります。

このような問題に対して、次のような解決方法があります。

- Linux システム内のウイルス / 不正プログラム、ワーム、トロイの木馬、スパイウェア / グレーウェアを検索し、効率よく検出できる。
- ウイルス感染の疑いのあるファイルに対して適切な処理を実行できる。
- 管理者に通知できる。

ServerProtect for Linux のソリューション

ServerProtect は、Linux システム内のデータファイルや実行可能ファイルを検索し、ウイルス / 不正プログラム、ワーム、トロイの木馬、スパイウェア / グレーウェアを検出することでシステムを保護します。

隔離

隔離領域とは、駆除できないファイルを格納するコンピュータやネットワーク上の領域のことです。隔離領域の容量を確保するために、隔離されたファイルは最終的に削除される場合があります。

隔離の重要な使用法の 1 つは、不正プログラムコードが含まれたファイルを一時的に格納することです。隔離ファイルは、削除ファイルと違って、実際のファイル内容が後から必要になった場合は復元できます。したがって管理者は、重要な情報が完全に失われることを心配せずに、隔離を積極的に使用できます。

プラットフォーム、圧縮およびエンコード

トレンドマイクロは、Windows、UNIX、および DOS を含む主要なプラットフォーム用の検索エンジンを開発しました (個別のプラットフォームについては下表を参照)。さらに検索エンジンは、すべてのファイルタイプ、20 以上の圧縮タイプ、主要なエンコードアルゴリズム、Microsoft Office のマクロ、および Web スクリプト言語を認識できます。既知のウイルス / 不正プログラムやネットワークの弱点を攻撃するコードは、すべて検索エンジンによって検出されるとともに、亜種 / 変種のセキュリティ侵害要因からもシステムを保護できます。

エンコード

- MIME
- UUencode
- Bin/Hex

ファイルタイプ

- 実行可能ファイル (.exe、.com、.lnk、.bas、.reg など)
- ライブラリファイル (.dll など)
- その他のファイル (.hlp や .chm など)
- Microsoft Office のファイル (下記の「マクロスクリプト」を参照)

圧縮

- Tar
- Gzip
- Windows のすべての圧縮形式 (一部を除く)

マクロスクリプト

- WordBasic
- VBA (Visual Basic for Applications)
- VBA3

注意： マクロスクリプトを実行できるアプリケーションとしては、Microsoft の Word と Excel などがあります。

スクリプト言語

- JavaScript
- VBScript

パスワード保護ファイル / 暗号化ファイル

ServerProtect は、ファイルを開いてから検索する必要があるため、パスワードで保護されたファイルや暗号化ファイルは検索できません。ServerProtect の検索エンジンは、このようなファイルを「検索不能ファイル」として認識します。管理者は、このようなすべてのファイルが自動隔離されるように設定することも、検索エンジンがこれらのファイルを放置するように選択することもできます。

主要な機能

以下では、ServerProtect の主な機能を説明します。

Control Manager による ServerProtect の管理

トレンドマイクロの中央管理コンソールである Trend Micro Control Manager (以下、Control Manager) を使用して ServerProtect を管理できるようになりました。これは、Control Manager 3.5 で導入された新しい HTTP ベースのプロトコルによって実現しました。Control Manager に登録すると、ServerProtect で Control Manager の次の機能を利用できるようになります。

- Control Manager から参照可能な各種レポート
- 大規模感染予防サービス (ファイルブロック用)。21 ページの「トレンドマイクロ 大規模感染予防サービス」を参照してください。

Control Manager から参照可能な各種レポート

Control Manager から次のレポートを参照できます。

- 上位 10 のウイルス検出ポイントのレポート
- すべてのエンティティのウイルス感染リスト
- 上位 10 のウイルス感染ファイルのレポート
- 上位 10 のウイルスレポート

Control Manager サーバは、ログデータに基づいてこれらのレポートをまとめているため、これらのレポートは、Control Manager から ServerProtect を管理している場合にのみ参照できます。

マルチプロセッサ対応

ServerProtect は、シングルプロセッサとマルチプロセッサのどちらのサーバにもインストールできます。

Web ブラウザからのリモート管理

ブラウザベースのコンソールを使用して ServerProtect を設定できます。このため、どこからでも ServerProtect を管理できます。ブラウザベースのコンソールから ServerProtect を設定する際は、Microsoft Internet Explorer、Mozilla、または Mozilla Firefox を使用できます。

手動検索、リアルタイム検索、および予約検索

手動検索 (「Scan Now」オプション) に加えて、ServerProtect は、ユーザの操作なしでウイルス / 不正プログラムに自動的に対処できます。ファイルを開いたり、コピーするなど、ファイルにアクセスするたびに、リアルタイム検索によってそのファイルがウイルス / 不正プログラムに感染していないかどうか確認されます。予約検索では、ユーザが指定した定期スケジュールに従って、Linux コンピュータ全体にわたってウイルス検索を実行できます。予約検索は、サーバ負荷を考慮して業務時間外に実行することをお勧めします。

実行ファイルに対する検索

ServerProtect のリアルタイム検索では、Linux アプリケーションが実行されている最中は常にアプリケーション内のウイルス / 不正プログラムを検出します。詳細については、73 ページの「除外リスト」を参照してください。

バックアップディレクトリの設定

ServerProtect では、リアルタイム検索、手動検索、または予約検索によってウイルスを駆除する前に、感染ファイルをバックアップできます。この機能は、ウイルスの駆除に失敗し、ファイルが万一破損したときに役立ちます。

詳細で管理しやすく、エクスポート可能なログ

ServerProtect では、システムやウイルス処理の実行状況がログとして記録されます。また、時間の経過に伴って肥大化しないように、ログを自動的に削除することもできます。さらに、システムやウイルス処理の実行状況について詳細なログをエクスポートすることもできます。

ログの手動削除 / 自動削除の選択

ServerProtect のログは、必要に応じて手動で削除することも、スケジュールに従って自動的に削除することもできます。

インターネットを介した手動または自動アップデート

ウイルスパターンファイルと検索エンジンファイルの手動アップデートまたは予約アップデートを実行して、必ず最新のウイルス対策を実施してください。ServerProtect では、トレンドマイクロのアップデートサーバの他に、その他のアップデートサーバを指定することもできます。ユーザ自身のアップデートサーバを設定するには、79 ページの「ダウンロード元をカスタマイズするには」をご確認ください。

ウイルス大規模感染の通知

ServerProtect を実行しているコンピュータで発生したウイルスや不正プログラムの大規模感染などのイベントをメールや Simple Network Management Protocol (SNMP) で通知するように設定できます。

トレンドマイクロ 大規模感染予防サービス

トレンドマイクロ 大規模感染予防サービス (OPS) は、Control Manager の使用時に利用できるトレンドマイクロのサービスです。OPS を使用すると、必要なウイルスパターンファイルが公開される前であっても、新種のウイルス / 不正プログラムに対する事前措置を講じることができます。ウイルスが通知されてからウイルスパターンファイルが配信されるまでの時間的隙間を埋めることによって、ウイルス / 不正プログラムの大規模感染をすばやく阻止し、システムの被害を最少限に抑えて、過度のダウンタイムを回避できます。

ServerProtect を Control Manager に登録すると、ファイルブロック用の OPS を利用できるようになります。

OPS は、トレンドマイクロのエンタープライズ プロテクション ストラテジー (以下、Trend Micro EPS) の主要コンポーネントです。Trend Micro EPS は、被害をもたらす可能性のあるウイルス攻撃を予防または回避するための最適な運用を特定した研究の成果です。この研究は、従来型のセキュリティ対策では CodeRed や Nimda などの新世代ウイルスに通用しないことが明らかになったことを受けて開始されました。

トレンドマイクロは、アウトブレークライフサイクルの各ステージにおける懸念事項に対処するために OPS を開発しました。OPS は、トレンドマイクロの次の 3 つの主要な強みを活用しています。

- 企業環境向けのウイルス対策製品とコンテンツセキュリティ製品
- トレンドマイクロの ISO 認定取得済みウイルス研究 / テクニカルサポートセンターである TrendLabs (トレンドラボ)
- 業界トップクラスのネットワークセキュリティベンダーとのパートナーシップ

そして、これらの強みを Control Manager という単一の強力なインタフェースに集約しています。

OPS を通じて、Control Manager は次の主要なセキュリティ上の疑問に答えます。

- 現在攻撃を受けているか。
- 現在のシステムは攻撃に対処できるか。
- どのように攻撃に対応すべきか。

注意： Trend Micro EPS および OPS の詳細については、トレンドマイクロの Web サイト (http://www.trendmicro.co.jp) を参照してください。

コマンドラインインタフェースのサポート

ServerProtect では、リアルタイム検索、予約検索、手動検索、通知、ログ削除、およびウイルスパターンファイル / 検索エンジンのアップデートを実行する際には、Web ベースの管理コンソールに加えてコマンドラインを使用できます。コマンドラインのオプションについては、付録 A の 226 ページの「splxmain」を参照してください。

詳細なアップデートオプションのサポート

コンポーネントアップデート機能では次のオプションが用意されています。

デジタル署名確認 : ServerProtect は、トレンドマイクロのアップデートサーバからコンポーネントをダウンロードするたびにこの機能を実行できます。この機能は初期設定では無効になっています。

Secure Sockets Layer (SSL) 対応 : ServerProtect は、トレンドマイクロのアップデートサーバ、または社内のアップデートサーバのいずれからでも、安全にコンポーネントをダウンロードできます。

サーバ認証サポート : ServerProtect は、HTTPS のソースからコンポーネントをダウンロードする際は HTTPS 認証をサポートします。

他のプロキシサーバタイプのサポート : ServerProtect は、次のプロキシサーバタイプと認証方式をサポートしています。

- 基本認証の Squid プロキシ (HTTPS と SSL の両方)
- ダイジェスト認証の Squid プロキシ (HTTPS と SSL の両方)

ServerProtect と設定ファイル (tmsplx.xml) 間の整合性確認

ServerProtect は、特定の ServerProtect オプションについて、Web コンソールと設定ファイル (tmsplx.xml) 間の整合性を確認します。vi エディタなどを使用して tmsplx.xml 内でのオプションが手動で変更された場合、次のメッセージが表示されます。

```
The splx configuration file /opt/TrendMicro/SProtectLinux/tmsplx.xml was previously
modified by another program...
```

インテル ハイパー・スレッディング・テクノロジ対応

本バージョンは、インテル ハイパー・スレッディング・テクノロジ搭載のサーバにインストールできます。ハイパー・スレッディング・テクノロジの詳細については、インテル社の Web サイトを参照してください。

トレンドマイクロ オンライン登録システムのサポート

トレンドマイクロの登録 Web サイトで、レジストレーションキーを使用して ServerProtect を登録し、アクティベーションコードを取得します。

https://olr.trendmicro.com/registration/jp/ja/login.aspx

詳細デバッグ用のオプション

ServerProtect では、次のデバッグオプションが用意されています。

カーネルデバッグ: カーネル関連の処理に対するデバッグ

ユーザデバッグ: ユーザ関連の処理に対するデバッグ

Control Manager デバッグ: Control Manager 関連の処理に対するデバッグ

詳細については、105 ページの「デバッグログ」を参照してください。

より安全な設定ファイルの変更

ServerProtect では、設定ファイルの変更内容がエラーチェックされるようになりました。バックアップ用の設定ファイルを使用して、必要に応じて変更前の設定ファイルにロールバックすることで、間違った変更内容を簡単に元に戻すこともできます。

トレンドマイクロの推奨設定と推奨処理

本バージョンの ServerProtect では、次のテクノロジを利用できます。

トレンドマイクロの推奨設定 (IntelliScan): トレンドマイクロの推奨設定は、これまでの検索オプションとは異なる新しい検索対象ファイル選択方法です。トレンドマイクロの推奨設定は、ファイルのヘッダを調べて実際のファイルタイプを判断し、不正プログラムコードが潜んでいる可能性のあるファイルタイプのみを検索することで、セキュリティを最大限に高めます。

トレンドマイクロの推奨処理 (ActiveAction): トレンドマイクロの推奨処理は、ウイルスなどのセキュリティリスクを検出した際に実行する処理を選択する新しい方法です。トレンドマイクロは、ウイルスのタイプに応じて異なる検出時の処理を設定しています。新しい検出時の処理は、トレンドマイクロから新しいパターンファイルをダウンロードしたときにアップデートされます。

アップデートをランダムな間隔で実行する機能

アップデートサーバによるネットワーク帯域幅のピーク使用量を抑制するために、ServerProtect には、予約アップデートの開始日時の経過後に、指定された期間内にアップデートをランダムに実行する機能が用意されています。

複数のダウンロード元のサポート

バックアップのアップデートサーバを設定して、プライマリのアップデートサーバが使用できない場合に、ウイルスパターンファイル / 検索エンジンのアップデート (フェイルオーバーとして) を提供します。

HTTPS (SSL) 対応

HTTPS プロトコルを使用して、ServerProtect の Web ベースのコンソールにアクセスできます。設定の詳細については、34 ページの「ServerProtect Web コンソールにアクセスする」を参照してください。SSL によって、Web ブラウザとホストサーバ間の通信チャネルのセキュリティが確保されます。このプロトコルを利用すると、セキュリティポリシーを損なうことなく ServerProtect を管理できます。

X Window システム用の Quick Access コンソール

Quick Access コンソールを使用して、Konqueror Desktop Environment (KDE) のグラフィカルデスクトップ環境で ServerProtect を管理できます。KDE の Quick Access コンソールを使用すると、次の操作を実行できます。

- 手動検索 (Scan Now) の開始 / 停止
- ServerProtec サービスと ServerProtec 用 HTTPS の開始 / 停止
- Web コンソールの起動
- ログの手動削除
- 手動アップデート (Update Now) の開始
- 予約検索の停止
- システムトレイでの通知アイコンの表示

リモートインストール

新しい RemoteInstall ツールを使用して、1 つまたは複数の ServerProtect インスタンスをリモートコンピュータにインストールできます。

1 つのバイナリパッケージですべてのサポートされている Linux ディストリビューションに対応

以前のバージョンの ServerProtect では、プラットフォームに応じて別々のインストールプロセスが必要でした。インストールが簡易化されて、1 つのインストールパッケージですべてのサポートされているプラットフォームに対応できるようになりました。

除外ディレクトリでのワイルドカードのサポート

リアルタイム検索、予約検索、および手動検索の検索パスと除外パスで、アスタリスク (*) と疑問符 (?) のワイルドカードを使用できるようになりました。アスタリスク (*) は任意の文字列に相当し、疑問符 (?) は任意の 1 文字に相当します。

本リリースの新機能

ServerProtect 3.0 では、以前のバージョンにはなかった以下の新しい機能を利用できます。

64 ビットプロセッサ対応

ServerProtect は、速度も効率も向上した AMD64/Intel 64 プロセッサ搭載機種に対応しました。

注意： このバージョンの ServerProtect は、IA64 ビットプロセッサに対応していません。

新しいプラットフォームのサポート

本リリースでは、サポートされているプラットフォームは Linux カーネル 2.6 をベースにしています。サポートされているプラットフォームは次のとおりです。

- Red Hat Enterprise Linux 4.0 (AS、ES、WS、および Desktop)
- AMD64/Intel 64 対応の Red Hat Enterprise Linux 4.0 (AS、ES、WS、および Desktop)
- Red Hat Enterprise Linux 5.0 (Server* および Desktop)
  *Advanced Platform を含む
- AMD64/Intel 64 対応の Red Hat Enterprise Linux 5.0 (Server* および Desktop)
  *Advanced Platform を含む
- SUSE Linux Enterprise Server 10 (Server および Desktop)
- AMD64/Intel 64 対応の SUSE Linux Enterprise Server 10 (Server および Desktop)
- MIRACLE LINUX V4.0 (Asianux 2.0)
- AMD64/Intel 64 対応の MIRACLE LINUX V4.0 (Asianux 2.0)
- Asianux Server 3
- AMD64/Intel 64 対応の Asianux Server 3

GPL オープンソース KHM

KHM のオープンソース化によってユーザ自身で特定の Linux カーネルに対応した KHM をコンパイルできるようになりました。手順については、Readme、テストスクリプトおよび makefile が用意されています。

ログオンセッション制御

セキュリティを高めるために、Web コンソールセッション制御機能が搭載されています。これにより、ServerProtect Web コンソールは停止から 20 分 (1200 秒) 後に自動的にログアウト (セッションを終了) します。

[Summary] ページ

新しい [Summary] 画面を表示して、Linux システムのウイルス / 不正プログラムへの対処について監視できます。システムステータス、検索結果 / ステータス、アップデートステータスなどの情報を表示できます。

ウイルストラッキングプログラム (WVTP)

トレンドマイクロのウイルストラッキングプログラムにより、世界中の何万という企業や個人のコンピュータシステムからインターネットの脅威となるデータを収集します。

スパイウェア対策

トレンドマイクロのスパイウェア対策テクノロジは、スパイウェア / グレーウェアおよびアドウェア、さらにネットワークに危害を加えるハッキングツールやリモートアクセスツールをブロックするように設計されています。この新たなセキュリティテクノロジにより、侵入者による個人や企業の情報、パスワード、メールアドレスなどのデータの収集を阻止できるようになりました。また、システムリソースと利用可能な帯域幅を解放して、ネットワークのパフォーマンスを向上し、スパイウェア関連のシステム障害を低減します。

通知アイコンとポップアップウイルス情報

Linux システムでグラフィカル KDE を使用すると、ServerProtect Notification アイコンがシステムトレイに自動的に表示され、リアルタイム検索ステータスが表示されます。ウイルス / 不正プログラムが検出されると、通知アイコンが変わります。そのアイコンをダブルクリックすると、ウイルス / 不正プログラムに関する詳細情報がポップアップウィンドウに表示されます。

SMTP 認証

SMTP 認証を有効にして、通知のメールを送信できます。

ローカルログオン時のパスワード入力を省略

ServerProtect をインストールしたサーバ上から Web コンソールにログオンする際のパスワード入力を省略できます。

OpenAFS ネットワークのドライブを検索対象から除外するオプション

場合によっては、ネットワークファイルシステムを検索対象から除外したいことがあります。通常マップされるドライブ形式以外に、OpenAFS でマップされたドライブも手動検索と予約検索から除外できます。

ServerProtect の仕組みについて

ServerProtect を使用すると、Linux サーバ上のウイルスをリアルタイム検索、手動検索、および予約検索できます。ServerProtect は、圧縮ファイルを含むさまざまなファイルに潜むウイルスなどのセキュリティリスクを検出して、エンドユーザに届く前に駆除することで、Samba ファイル共有、HTTP、および FTP 経由でのウイルス感染からユーザを保護します。

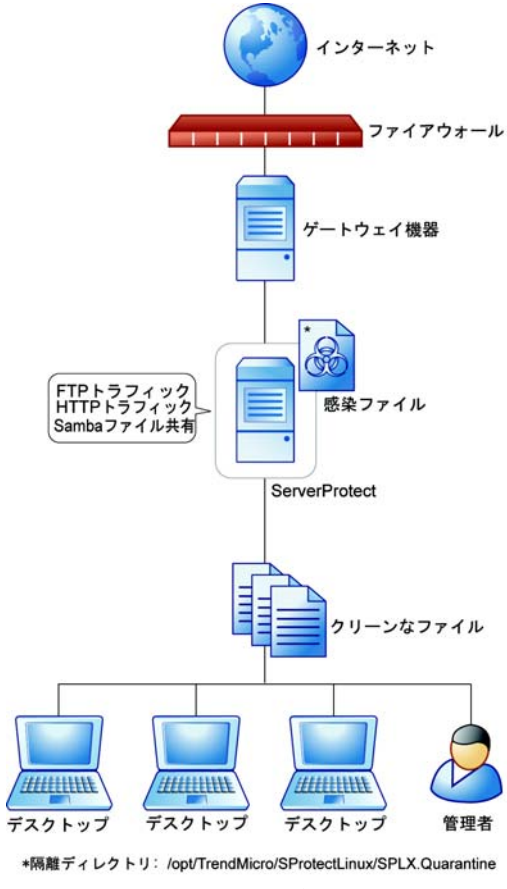


図 1-1.　ServerProtect の仕組み

ServerProtect に付属している Web ベースのコンソールを使用すると、インターネット接続を介してどこからでも簡単に ServerProtect にリモートアクセスできます。
ServerProtect の多くの機能は、コマンドラインからも実行できます。システムイベントや攻撃が発生したときに警告するように通知を設定することもできます。

ServerProtect のさまざまな検索テクノロジ

ServerProtect では、さまざまな形態の不正プログラムを検出するために、パターンマッチング、MacroTrap、ScriptTrap、および圧縮ファイル検出という技術を駆使しています。

パターンマッチング

ServerProtect は、大規模なウイルスパターンデータベースを活用することで、「パターンマッチング」というプロセスを通じてウイルスなどの不正プログラムを識別します。
ServerProtect は、ウイルス感染の疑いのあるファイルの主要な領域に不正プログラムコードの特徴を持つストリングが潜んでいないか調べて、これらの領域をトレンドマイクロが記録している多数のウイルスシグネチャと比較します。

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、ServerProtect の検索エンジンは、ウイルス感染の疑いのあるファイルを保護された場所で実行して解読します。その後でファイル全体を検索し、ミューテーション型ウイルスのコードを見つけ出します。

警告： 非常に多くの新種ウイルス / 不正プログラムが発生しているため、ウイルスパターンファイルを常に最新の状態に保ってください。

MacroTrap

マクロウイルスはアプリケーション固有です。つまり、複数の OS で感染を引き起こします。OS の種類を越えて感染する可能性のあるマクロウイルスは、インターネット利用者の増加、マクロ言語の機能向上に伴って、大きな脅威となっています。トレンドマイクロの MacroTrap は、マクロウイルスからネットワーク環境を守るために開発されました。

MacroTrap の仕組み

MacroTrap は、ルールベース方式によりドキュメント内のすべてのマクロコードを検査します。マクロウイルスコードの多くはテンプレート（通常は見えないファイル）に含まれて、ドキュメントとともに配信されます（たとえば Microsoft Word の場合、.dot テンプレートファイル）。MacroTrap は、ウイルスの活動に似た処理を実行する命令を見つけ出して、テンプレートにマクロウイルス感染の痕跡がないか調べます。マクロウイルスの活動の例としては、テンプレートの一部を他のテンプレートにコピーすること (複製) や、有害なコマンドを実行すること (破壊) などがあります。

圧縮ファイル検索

圧縮ファイル (複数のファイルや圧縮ファイルを含む 1 つのファイル) は、メールやインターネットでのファイル配信で一般的に使用されています。ウイルス対策ソフトウェアが圧縮ファイルの検索に対応していない場合は、ウイルスなどのセキュリティリスクが圧縮ファイルに潜んだ状態でネットワーク内に侵入する可能性があります。

ServerProtect の検索エンジンは圧縮ファイル内を検索できるとともに、多重圧縮ファイル (最大 20 階層) 内でウイルス検索することも可能です (設定が必要)。21 以上の階層は「スキップ」されますが、システムログには記録されます。

トレンドマイクロ検索エンジンは、.zip、.arj、.lzh などの圧縮アルゴリズムに対応しています。詳細なリストについては、オンラインヘルプの [About]→[ServerProtect for Linux]→[How ServerProtect Finds Viruses] トピックを参照してください。

圧縮ファイル検索の制限

ServerProtect では、システムリソースを節約するために、一定のサイズを超える圧縮ファイルはウイルス検索しないように設定できます。検索処理されなかった圧縮ファイルは、システムログに表示されます。サイズの上限を小さくするほど、ウイルス感染の危険性が高くなるのでご注意ください。

注意： 制限により検索されなかった圧縮ファイルは、そのファイルが解凍されるときにリアルタイム検索によって検索されます。

第 2 章

製品の使用

本章では、Trend Micro ServerProtect for Linux (以下、ServerProtect) を使用するための基本的な設定方法と操作手順を説明します。その他の情報については、オンラインヘルプのトピックで検索してください。

本章では、次の内容について説明します。

ServerProtect Web コンソールにアクセスする

ここでは、Web ベースのコンソールを使用して ServerProtect を設定する方法について説明します。ブラウザを使用して、Web コンソールから ServerProtect をローカルおよびリモートで管理、または複数のユーザで管理できます。

注意： ServerProtect を設定する際は、Web コンソールにアクセスするユーザを 1 人に限定することをお勧めします。1 人に限定されていない場合、1 人のユーザによって変更された内容は、同じ Web コンソールにアクセスした別のユーザによって上書きされます。

Web コンソールにアクセスするには、次のいずれかを使用します。

- KDE の Quick Access コンソール
- Trend Micro ServerProtect for Linux のアイコン
- 対応する Web ブラウザ

Web コンソールにアクセスするには

1. root でログオンします。

2. 次のいずれかを実行します。

- KDE で、アプリケーション起動ボタンから、[System (Tools)]→[Trend Micro ServerProtect]→[Launch Web Console] の順にクリックします。
- KDE または GNOME デスクトップで、Trend Micro ServerProtect for Linux アイコンをダブルクリックします。

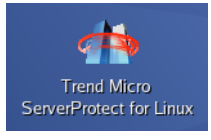


図 2-1. ServerProtect デスクトップアイコン

- 対応する Web ブラウザのアドレスフィールドに、ServerProtect がインストールされたコンピュータの場所とポート番号を次のように入力します。

  http://< ホスト名 >:14942/

  https://< ホスト名 >:14943/

  - **< ホスト名 >** には、ServerProtect がインストールされたサーバのコンピュータ名または IP アドレスを指定します。
  - 14942 は、ServerProtect が使用する初期設定の HTTP ポート番号です。
  - 14943 は、ServerProtect が使用する初期設定の HTTPS ポート番号です。

注意： ポート番号を変更するには、splxmain コマンドを使用します。詳細については、226 ページの「splxmain」を参照してください。
Internet Explorer 7.0 を使用している場合、オンラインヘルプを表示するには、ポップアップブロックを無効にする必要があります。

3. Web コンソールのパスワードを入力して、<Enter> キーを押します。初期設定では、パスワードフィールドは空白です (つまり、初期設定のパスワードはありません)。

ログオンパスワードを設定する

安全のために、はじめてログオンした後で Web コンソールのパスワードを変更することをお勧めします。

ログオンパスワードを設定するには

1. Web コンソールの左のメニューから [Administration]→[Password] の順に選択します。
2. [Current password] フィールドに現在のパスワードを入力します。
3. [New password] フィールドに新しいパスワードを入力します。パスワードは 0 ～ 32 文字で指定します。
4. 確認のために、新しいパスワードを再度入力します。
5. [Save] をクリックします。

注意： Web コンソールは必ずパスワードで保護してください。ServerProtect をインストールしたら、すぐにパスワードを設定して Web コンソールへのアクセスを制限することをお勧めします。

ローカルログオン時のパスワード入力を省略する

ServerProtect をインストールしたサーバにログオンする際に、パスワード確認を無効にできます。

ログオンパスワードの入力を省略するには

1. Web コンソールの左のメニューから [Administration]→[Password] の順に選択します。
2. [Bypass password when logging on] を選択します。

3. [Save] をクリックします。

注意： 他のコンピュータから ServerProtect サーバへログオンする際には、パスワードを入力する必要があります。

Web コンソールからログオフする

コンソールからログオフするには、タイトルバーの 

をクリックします。

Web コンソールに関する注意点

- Web コンソールによって、ServerProtect の機能すべてにアクセスできます。ただし、Web コンソールから ServerProtect を起動したり停止したりできません。起動や停止には、コマンドラインまたは Quick Access コンソールを使用します (39 ページの「ServerProtect を起動および停止する」を参照)。
- Web コンソールの画面を更新するには、ブラウザの更新ボタンを使用します。
- Web コンソールで何も操作を行わないまま 1,200 秒 (20 分) 経過すると、自動的にログアウトします。自動的にログアウトした場合には、パスワードを入力し、[Log On] をクリックして再び Web コンソールにアクセスする必要があります。初期設定のタイムアウトの設定を変更するには、tmsplx.xml ファイル (/opt/TrendMicro/SProtectLinux フォルダ内) の Configuration セクションにある SessionTimeout キーを変更します。

  セッション制御機能は、次の操作には適用しません。

  - パスワードの確認を省略するローカルログオン
  - Control Manager によるシングルサインオン (SSO) を介した ServerProtect Web コンソールへのアクセス

Quick Access コンソールメニューを使用する

ServerProtect コンピュータに KDE バージョン 3.3 以上がインストールしてある場合、インストールプログラムにより [Trend Micro ServerProtect] メニューオプションがデスクトップの次のいずれかの場所に追加されます。

- [System Tools] メニュー (Red Hat)
- [System] メニュー (SUSE)

注意： Quick Access コンソールにアクセスするには、root ユーザとしてログオンする必要があります。

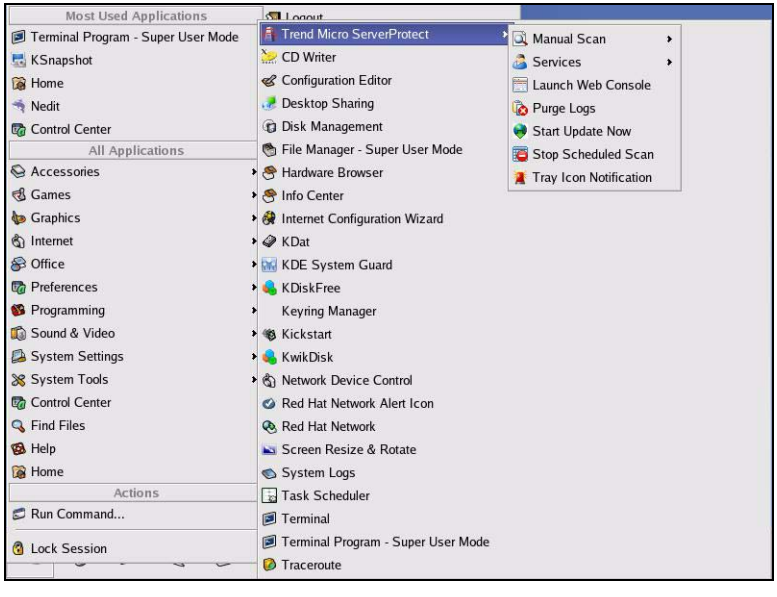


図 2-2.　KDE の Quick Access コンソールのメニュー

使用できるメニュー/ オプションは、次のとおりです。

- Manual Scan メニュー: このメニューにより、手動検索を起動または停止できます。

- Services メニュー: このメニューにより、ServerProtect サービスおよび ServerProtect 用 Apache サービスを起動または停止できます。
- Launch Web Console: このメニューにより、ブラウザで Web コンソールの URL を入力しなくても、デスクトップから Web コンソールを起動できます。
- Purge Logs: このオプションにより、すべての検索ログ、ウイルスログ、スパイウェア / グレーウェアログおよびシステムログを削除します。
- Start Update Now: このオプションにより、アップデート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のダウンロードを開始します。
- Stop Scheduled Scan: このオプションにより、進行中の予約検索を停止します。
- Tray Icon Notification: このオプションにより、システムトレイに ServerProtect の通知アイコンを表示します。

ServerProtect を起動および停止する

ServerProtect を起動または停止する方法には、2 種類あります。

- コマンドラインからの起動または停止
- Quick Access コンソールからの起動または停止

注意： ServerProtect は、インストール先サーバの起動時に自動的に起動するよう初期設定されています。この設定を変更するには、43 ページの「スタートアップを設定する」を参照してください。

ServerProtect を起動する

コマンドラインから ServerProtect を起動するには

1. root でログオンします。

2. ターミナルウィンドウを開き、コマンドラインで「/etc/init.d/splx start」と入力します。次のメッセージが表示されます。

```
[root@localhost ~] # /etc/init.d/splx start
Starting ServerProtect for Linux:
Checking configuration file: [OK]
Starting splxcore:
Starting Entity: [OK]
Loading splx kernel module: [OK]
Starting vsapiapp: [OK]
ServerProtect for Linux core started.
                                        [OK]
Starting splxhttpd:
Starting splxhttpd: [OK]
ServerProtect for Linux httpd started.
                                        [OK]
ServerProtect for Linux started.
[root@localhost ~] #
```

Quick Access コンソールから ServerProtect を起動するには

1. root でログオンします。
2. タスクバーのアプリケーション起動ボタンから、[System (Tools)]→[Trend Micro ServerProtect]→[Services]→[Start SPLX Service] の順にクリックします。

ServerProtect を停止する

コマンドラインから ServerProtect を停止するには

1. root でログオンします。
2. ターミナルウィンドウを開き、コマンドラインで「/etc/init.d/splx stop」と入力します。次のメッセージが表示されます。

```
[root@localhost ~] # /etc/init.d/splx stop
Shutting down ServerProtect for Linux:
Shutting down splxcore:
Shutting down vsapiapp: [OK]
Unloading splx kernel module: [OK]
Shutting down entity: [OK]
ServerProtect for Linux core stopped normally.
                                        [OK]
Shutting down splxhttpd:
Shutting down splxhttpd: [OK]
ServerProtect for Linux httpd stopped normally.
                                        [OK]
ServerProtect for Linux stopped normally.
[root@localhost ~] #
```

Quick Access コンソールから ServerProtect を停止するには

1. root でログオンします。
2. タスクバーのアプリケーション起動ボタンから、[System (Tools)]→[Trend Micro ServerProtect]→[Services]→[Stop SPLX Service] の順にクリックします。

通知アイコン

システムトレイの通知アイコンは、Linux コンピュータの ServerProtect サービスのステータスを示し、ウイルス / スパイウェアが検出されると警告します。

通知アイコンのステータスは、次のとおりです。

アイコン	説明
	ServerProtect は正常に実行中です。
	ServerProtect は実行していません。
	ServerProtect は、Linux コンピュータ上にウイルス / スパイウェアを検出しました。このアイコンをダブルクリックしてウイルス情報画面を表示するまで、ServerProtect サービスが実行を停止しているときも、この警告アイコンはシステムトレイに表示されます。

表 2-1. 通知アイコン

注意： 初期設定では、通知アイコンは root ユーザの KDE システムトレイにのみ表示されます。その他のユーザの KDE システムトレイに通知アイコンを表示するには、/opt/TrendMicro/SProtectLinux/SPLX.tmp ディレクトリおよび /opt/TrendMicro/SProtectLinux/SPLX.vsapiapp 内の virus_catch_monitor ファイルへのアクセス権を設定します。

通知情報の画面

通知情報の画面には、リアルタイムのウイルス / スパイウェア検出情報が表示されます。この画面を表示するには、システムトレイの通知アイコンをダブルクリックします。

検索結果には、次の情報が含まれます。

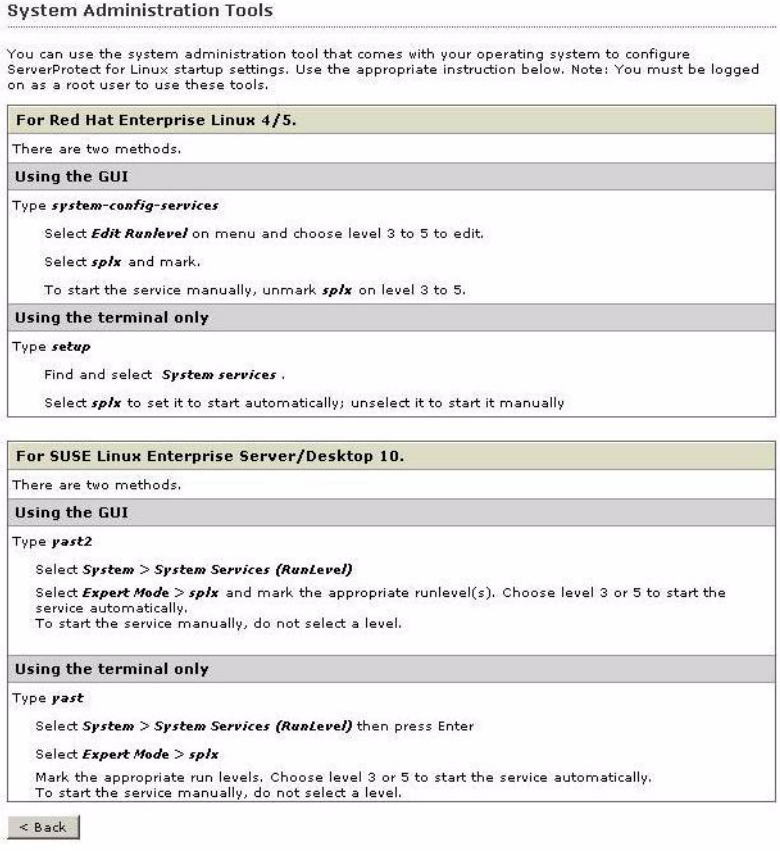
- ウイルス / スパイウェアの名前
- 感染ファイルの名前
- 実行される処理
- 検出日時

注意： 通知情報の画面では、最大 50 件の最新ウイルス / スパイウェアのログが表示されます。通知情報の画面を閉じると、この画面のウイルス / スパイウェアのログは自動的に消去されます。ウイルス / スパイウェアのログを再び表示するには、ServerProtect Web コンソールで該当するログ画面を開きます。

スタートアップを設定する

ServerProtect は、インストール先サーバの起動時に自動的に起動するよう初期設定されています。スタートアップの設定を変更するには、Linux サービス設定ツールを使用します。スタートアップの設定方法は、各 Linux ディストリビューションによって変わります。

ServerProtect の Web コンソールでスタートアップ設定のヘルプを表示するには、[Administration]→[Startup Settings] の順に選択し、[system administration tools] リンクをクリックします。次の画面が表示されます。



System Administration Tools

You can use the system administration tool that comes with your operating system to configure ServerProtect for Linux startup settings. Use the appropriate instruction below. Note: You must be logged on as a root user to use these tools.

For Red Hat Enterprise Linux 4/5.

There are two methods.

Using the GUI

Type ***system-config-services***

Select ***Edit Runlevel*** on menu and choose level 3 to 5 to edit.

Select ***splx*** and mark.

To start the service manually, unmark ***splx*** on level 3 to 5.

Using the terminal only

Type ***setup***

Find and select ***System services*** .

Select ***splx*** to set it to start automatically; unselect it to start it manually

For SUSE Linux Enterprise Server/Desktop 10.

There are two methods.

Using the GUI

Type ***yast2***

Select ***System*** > ***System Services (RunLevel)***

Select ***Expert Mode*** > ***splx*** and mark the appropriate runlevel(s). Choose level 3 or 5 to start the service automatically.
To start the service manually, do not select a level.

Using the terminal only

Type ***yast***

Select ***System*** > ***System Services (RunLevel)*** then press Enter

Select ***Expert Mode*** > ***splx***

Mark the appropriate run levels. Choose level 3 or 5 to start the service automatically.
To start the service manually, do not select a level.

< Back

図 2-3.　Administration:Startup Settings

Red Hat Enterprise Linux 4/5

サービス設定ツールを使用する

1. root でログオンし、コマンドラインで「system-config-services」と入力します。サービス設定ツール画面が表示されます。
2. メニューで [Edit Runlevel] を選択し、レベル 3、4、または 5 を選択して編集します。
3. 画面を下方にスクロールして、[splx] を選択します。

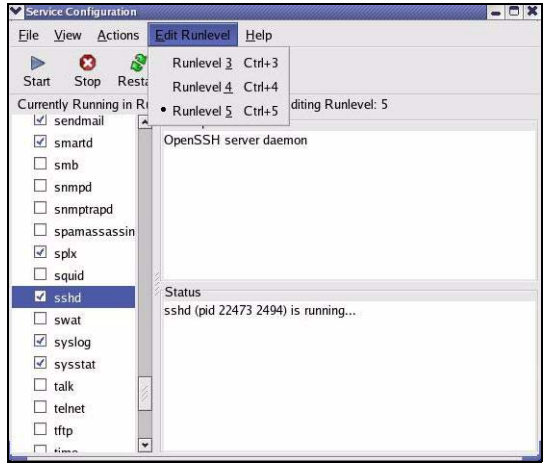


図 2-4. Red Hat: サービス設定ツール

4. サービスを手動で起動する際には、レベル 3、4、または 5 で [splx] を選択しないでください。

テキストモードのセットアップツールを使用する

1. root でログオンし、コマンドラインで「setup」と入力します。テキストモードのセットアップツール画面が表示されます。

2. 矢印キーを押して [System services] を選択し、<Enter> キーを押します。

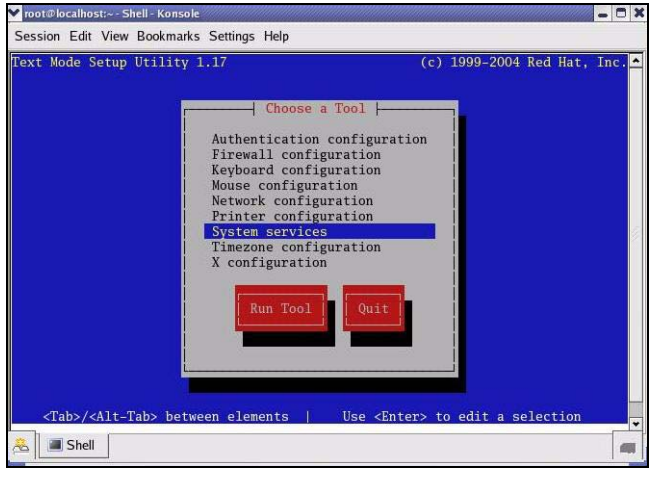


図 2-5. Red Hat: テキストモードのセットアップツール

3. 自動的に起動するには、[splx] をオンにします。手動で起動するには、[splx] をオフにします。

SUSE Linux Enterprise Server/Desktop 10

グラフィカル画面を使用する

1. root でログオンし、コマンドラインで「yast2」と入力します。セットアップツールのユーザインタフェースが表示されます。
2. メニューで [System]→[Runlevel Editor] の順に選択します。
3. [Expert Mode]→[splx] の順に選択し、適切な実行レベルにマークを付けます。
4. サービスを自動的に起動するには、レベル 3、4、または 5 を選択し、手動で起動するには、レベルを選択しません。

ターミナルを使用する

1. root でログオンし、コマンドラインで「yast」と入力します。セットアップツールのユーザインタフェースが表示されます。
2. メニューで [System]→[Runlevel Editor] の順に選択し、<Enter> キーを押します。
3. [Expert Mode]→[splx] の順に選択し、適切な実行レベルにマークを付けます。
4. サービスを自動的に起動するには、レベル 3、4、または 5 を選択し、手動で起動するには、レベルを選択しません。

概要情報を表示する

[Summary] 画面には、現在のシステム情報、ウイルス / スパイウェア検索結果の概要、および既存のウイルス / スパイウェア対策コンポーネントの詳細が表示されます。

[Summary] 画面から実行できる操作は、次のとおりです。

- OS、ハードウェアのバージョンなどのシステム情報の表示
- ウイルス / スパイウェアの検索結果の表示
    - [viruses/spywares detected today] フィールドには、過去 24 時間に検出されたウイルス / スパイウェアの合計数が表示されます。
    - [Today] フィールドには、過去 24 時間に ServerProtect により検出され、特定の処理が実行されたウイルス / スパイウェアの数が表示されます。
    - [Last 7 days] フィールドには、当日を含む過去 7 日間に検出されたウイルス / スパイウェアの合計数が表示されます。

注意： 検出されたウイルス / スパイウェアに対して複数の処理が実行される場合があるので、同じウイルス / スパイウェアが複数の [Summary] フィールドで表示されます。
tmsplx.xml ファイルの MaxRetrieveCount パラメータは、カウンタが表示できる最大数を指定します。詳細については、218 ページの「MaxRetrieveCount」を参照してください。

- 検索ステータスの表示、および [Scan Now] をクリックして手動検索を実行する。
- コンポーネントのステータスの表示、および [Update Now] をクリックして選択したコンポーネントをアップデートする。

Control Manager による ServerProtect の管理

ServerProtect サーバが提供する情報を利用するには、ServerProtect サーバを Control Manager に登録する必要があります。ServerProtect は、Trend Micro Management Communication Protocol (MCP) エージェントを介して Control Manager と通信します。MCP エージェントは、ServerProtect がインストールされるコンピュータにインストールされるので、MCP エージェントをインストールする必要はありません。

ServerProtect を Control Manager に登録するには、次のいずれかの方法を使用します。

- インストールプロセス中に登録する
- ServerProtect Web コンソールで登録する
- CMconfig ツールを使用してコマンドラインにより登録する

Web コンソールを使用して ServerProtect を Control Manager に登録するには

1. Web コンソールにログオンします。

2. [Administration]→[Control Manager Settings] の順にクリックします。[Control Manager Settings] 画面が表示されます。

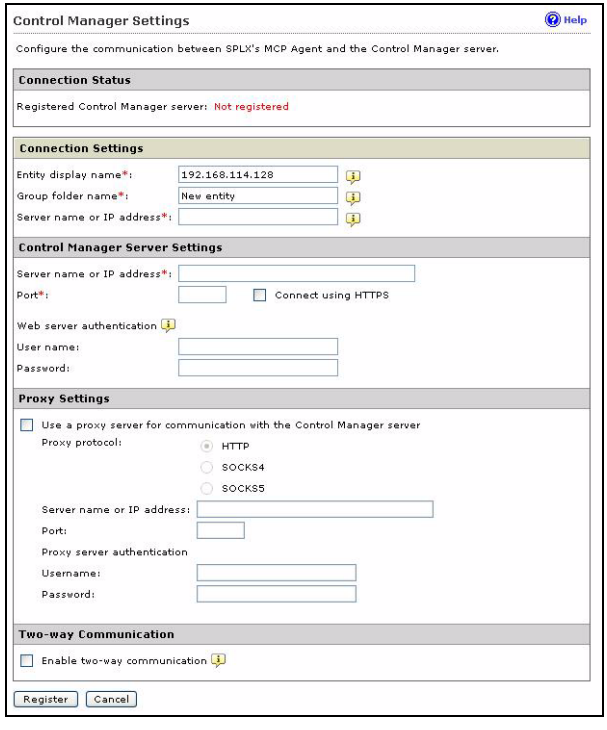


図 2-6. Control Manager

3. [Connection Settings] で次のフィールドを設定します。

- [Entity display name] 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名前を入力します。これが Control Manager サーバの製品ディレクトリに表示され、ServerProtect サーバを識別する名前になるため、慎重に名前を選択します。一意で識別しやすい名前にすると、Control Manager の製品ディレクトリで ServerProtect サーバを迅速に識別できます。
- [Group folder name] フィールドには、Control Manager の製品ツリー内で ServerProtect を識別する意味のある名前を入力します。

- [Server name or IP address] 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 アドレスを入力します。ネットワーク環境で DNS 設定をしている場合には、サーバ名を入力するようお勧めします。

4. [Control Manager Server Settings] で、次の項目を指定します。

   a. Control Manager サーバの IP アドレスまたはホスト名を [Server name or IP address] フィールドに入力します。

   b. MCP エージェントが Control Manager と通信するために使用する、ポート番号を入力します。

   c. Control Manager セキュリティを「中」(Control Manager と管理下の製品の MCP エージェントとの間で HTTPS 通信および HTTP 通信を許可) または「高」(Control Manager と管理下の製品の MCP エージェントの間で HTTPS 通信のみを許可) に設定した場合は、[Connect using HTTPS] を選択します。

   d. ネットワークで認証が必要な場合は、IIS (Internet Information Services) サーバのユーザ名とパスワードを [User name] および [Password] フィールドに入力します。

   注意： IIS サーバの認証を使用すると、Control Manager からコンポーネントをアップデートするように設定できません。[Scheduled Update] 画面または [Manual Update] 画面のダウンロード元としてアップデートサーバ (トレンドマイクロのアップデートサーバまたは各自が設定したサーバ) の URL を指定する必要があります。

   e. インターネットのアクセスにプロキシサーバを使用する場合には、[Proxy Settings] でプロキシサーバの設定を指定する必要があります。

   注意： ServerProtect から Control Manager に NAT デバイスを介して接続する場合、シングルサインオンで Control Manager から ServerProtect Web コンソールにアクセスするには、NAT デバイス側で事前にポート転送を設定する必要があります。詳細については、124 ページの「NAT を使用した通信の手動設定」を参照してください。

5. [Register] をクリックして設定を保存し、ServerProtect コンピュータを Control Manager に登録します。

CMconfig ツールを使用して ServerProtect を Control Manager に登録するには

1. ServerProtect が現在 Control Manager に登録されていないことを確認したら、CMconfig を実行します。/opt/TrendMicro/SProtectLinux/SPLX.util ディレクトリに次のコマンドを入力します。

```
./CMconfig
```

2. 必要なデータの入力を求めるプロンプトが表示され、ServerProtect サーバで使用できる IP アドレスのリストが表示されます。

注意： コマンドオプションについての詳細は、コマンドラインで「./CMconfig -h 」と入力します。
プロキシの種類を指定するには、Agent.ini ファイル (/opt/TrendMicro/SProtectLinux/ フォルダ内) の Proxy_Type パラメータを変更してから、CMconfig コマンドを使用して ServerProtect を Control Manager に登録します。

---

3. SPLX server name or IP address: プロンプトでは、ServerProtect サーバの名前または IP アドレスを入力します。

4. Do you wish to connect to Control Manager server using HTTPS?(y/n) [n] プロンプトでは、「y」を入力し HTTPS で Control Manager に接続します。または、HTTP 接続を使用するよう入力します。

5. Control Manager server name or IP address: プロンプトでは、ServerProtect を管理するために使用する Control Manager サーバの名前または IP アドレスを入力します。

6. Control Manager server port:[80] プロンプトでは、Control Manager にアクセスする際に使用するポートの数を入力するか、<Enter> キーを押して初期設定値の 80 を選択します。

7. Do you access Control Manager through a proxy server?(y/n) [n] プロンプトでは、「y」を入力して <Enter> キーを押すか、<Enter> キーを押して初期設定の「n」を選択します。「n」を選択した場合は、CMconfig により Control Manager の Web コンソールで ServerProtect を識別するための表示名を指定するように要求されます。

ヒント：プロキシサーバを使用して Control Manager に接続する場合、さらに詳しい説明については「クイックスタートガイド」のインストールの章で「プロキシサーバの情報を入力する」を参照してください。

---

8. Please specify the name you would like to display on the Control Manager console:[SPLX server IP address] のプロンプトでは、必要な名前を入力します。Control Manager では、この名前を使用して Control Manager Web コンソールの ServerProtect サーバを識別します。

9. Please specify a folder name for this product (for example:/SPLX) [New entity]: プロンプトでは、前述したフォルダのパスを入力します。入力した情報の概要が表示され、選択内容を確認するように要求されます。

10. Is the above information correct?(y/n) [n] プロンプトでは、表示された選択内容が正しいかどうかを確認します。「n」と入力するか、単に <Enter> キーを押して初期設定の「n」を選択した場合は、ServerProtect サーバの IP アドレスから始まる前述のすべての情報を再入力するためのプロンプトが表示されます。「y」を入力して表示された情報のすべてを確定した場合は、ServerProtect を Control Manager に登録する際にステータスメッセージが出力されます。

自動アップデートの開始

Trend Micro Control Manager (以下、Control Manager) に ServerProtect を登録した後に、Control Manager サーバ上でアップデートを実行する必要があります。管理下の ServerProtect でアップデートを実行する前にこの操作を行ってください。

注意： ServerProtect が Control Manager から自動的にコンポーネントを取得できるようにするには、まず Control Manager サーバでアップデートを実行する必要があります。

自動アップデートを開始するには

1. ServerProtect が Control Manager に正常に登録されていることを確認します。
2. Control Manager の Web コンソールにログオンし、[運用管理]→[アップデート管理] の [手動ダウンロード] または[予約ダウンロード] 画面からコンポーネントのアップデートを実行します。

Control Manager の製品管理の詳細については、119 ページの「Trend Micro Control Manager について」または Control Manager の「管理者ガイド」を参照してください。

ウイルストラッキングプログラム

トレンドマイクロのウイルストラッキングプログラム (WVTP) により、世界中の莫大な数の企業や個人のコンピュータシステムからインターネットの脅威となるデータを収集します。

このプログラムに参加するには、[Administrator]→[World Virus Tracking] の順にクリックして [Yes] を選択します。次に [Save] をクリックして変更内容を確定します。

第 3 章

検索の設定と実行

本章では、次の内容について説明します。

検索の種類

Trend Micro ServerProtect for Linux (以下、ServerProtect) のインストールの際、サーバで使用している Linux のバージョンがセットアッププログラムで自動的に検出されま、適切なカーネルフックモジュール (KHM) がインストールされます。これにより、手動検索、予約検索に加えて、リアルタイム検索も実行できるようになります。

検出された Linux のバージョンがセットアッププログラムでサポートされていない場合には、KHM はインストールされません。つまり、ServerProtect では手動検索と予約検索のみが実行可能となり、リアルタイム検索は実行できません。サポートされていない Linux カーネルバージョンを実行するサーバに KHM をインストールするには、ソースコードから KHM を構築 (コンパイル) する必要があります (詳細については「クイックスタートガイド」の付録を参照)。

ServerProtect で実行できる検索の種類は次の 3 つです。

- リアルタイム検索では、サーバ上の入力ファイル、出力ファイル、実行中のファイルが監視されます。リアルタイム検索を常に有効にしておくことをお勧めします。
- 予約検索によって、サーバを定期的に (週 1 回など) ウイルス検索できます。予約検索では、リアルタイム検索によって常時監視しないディレクトリやファイルタイプを検索対象に含めることができます。予約検索の対象はリアルタイム検索より多くなることがあるため、より多くのコンピューティングリソースが消費される可能性があります。したがって、予約検索は、日曜日の早朝などのピーク外の時間帯に実行することをお勧めします。

- 手動検索では、必要に応じてサーバのウイルス検索を実行できます。たとえば、アウトブレークが発生した場合、この新しいセキュリティ侵害要因が発見されてから、対応するパターンファイルがリリースされるまでの間に無防備な期間が生じます。通常はこのような期間は数時間ですが、その間はサーバは攻撃を受けやすくなります。ServerProtect がアップデートされたパターンファイルをダウンロードした後、手動検索を実行して、無防備だった間にサーバ上に不正プログラムが侵入していないかどうかを確認してください。保守ダウンタイム後にサーバがオンラインに戻ったときにも、手動検索を実行してください。

注意： ServerProtect のウイルス検出方法については、17 ページの「ServerProtect for Linux のソリューション」を参照してください。

次に、各検索の種類を設定する方法を説明します。

リアルタイム検索を設定する

リアルタイム検索を有効にすると、バックグラウンドでウイルス検索が実行され、アクセスされるすべてのファイルが常に検査されます。リアルタイム検索オプションは常に有効にしておくことをお勧めします。

リアルタイム検索では、入力ファイル、出力ファイル、および実行中のファイルからウイルスを検出できます。

- Incoming files: ServerProtect コンピュータに外部から入力してくる検索ファイル。
- Outgoing files: ServerProtect コンピュータから外部へ出力される検索ファイル。
- Running applications: ServerProtect コンピュータ上で実行されている検索ファイル。たとえば、アプリケーションの起動時など。

リアルタイム検索を有効にするには

1. 左のメニューで [Scan Options]→[Real-time Scan] の順にクリックします。
2. [Real-time Scan] 画面で [Enable real-time scan] チェックボックスをオンにします。
3. [Incoming files]、[Outgoing files]、[Running applications] のチェックボックスを必要に応じてオンにします。

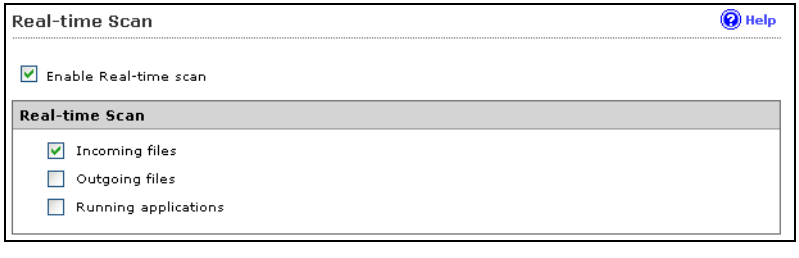


図 3-1.　リアルタイム検索の有効化および設定

4. [Save] をクリックして、設定を適用します。

注意： リアルタイム検索を常に有効にしておくことをお勧めします。インストールイメージに含まれている KHM に対応したカーネルを使用していた場合、リアルタイム検索は初期設定で有効になっています。
その他の検索設定については、64 ページの「検索オプションを設定する」を参照してください。

予約検索を設定する

予約検索では、検索周期や対象ディレクトリ、ファイルタイプをあらかじめ指定して自動的にウイルス検索を実行できます。予約検索では、ユーザが指定した定期スケジュールに従って、Linux コンピュータ全体にわたってウイルス検索を実行できます。予約検索は、サーバ負荷を考慮して業務時間外に実行することをお勧めします。サーバがウイルスなどのセキュリティリスクに感染していないかどうかを定期的に確認するために、予約検索を有効にすることをお勧めします。

予約検索を設定するには

1. 左のメニューから [Scan Options]→[Scheduled Scan] の順にクリックします。
2. [Enable Scheduled Scan] チェックボックスをオンにします。
3. [Save] をクリックして、設定を適用します。

図 3-2. 予約検索の有効化および設定

予約検索の検索周期を設定するには

1. 左のメニューから [Scan Options]→[Scheduled Scan] の順にクリックします。
2. [Scan Frequency] を設定するには、次の情報を入力します。
   - Start time: 検索の開始時間を指定します。
   - Repeat interval: 予約検索を実行する周期を指定します。
3. [Save] をクリックして、設定を適用します。その他の検索設定については、64 ページの「検索オプションを設定する」を参照してください。

予約検索をコマンドラインから実行する

コマンドラインで、「./splxmain」(/opt/TrendMicro/SProtectLinux/SPLxvsapiapp フォルダ内) と入力すると、ただちに予約検索を実行できます。この方法で実行した場合、tmsplx.xml に保存されている予約検索設定が適用されます。

予約検索を実行するには

コマンドラインに次のコマンドを入力します。

```
./splxmain -s
```

予約検索を停止する

Web コンソールで予約検索を無効にすることなく、実行中の予約検索を停止できます。検索は、次回の予約日に再開されます。

注意： 実行中の予約検索の実行を停止しても、次回以降の予約検索はスケジュールどおりに実行されます。
予約検索を停止するには、root でログオンする必要があります。

実行中の予約検索を停止するには、次のいずれかを実行します。

- /opt/TrendMicro/SProtectLinux/SPLX.vsapiapp フォルダの次のコマンドを実行します。

```
./splxmain -t
```

- X Window のタスクバーのアプリケーション起動ボタンから、[System (Tools)]→[Trend Micro ServerProtect]→[Stop Scheduled Scan] の順にクリックします。

手動検索 (Scan Now) を実行する

ウイルス感染をすぐにチェックしたい場合などに手動検索を実行します。手動検索を実行するには、次の 3 つの方法があります。保存済みの設定を使用する方法、設定を変更してから手動検索を実行する方法、コマンドラインを使用する方法です。

その他の検索設定については、64 ページの「検索オプションを設定する」を参照してください。

注意： ServerProtect では、予約検索と手動検索を同時に実行できません。予約検索が既に開始しているときに手動検索を開始しようとすると、警告メッセージ画面が表示されます。予約検索が完了するまで待つか、予約検索を停止してから (./splxmain -t コマンドを使用)、手動検索を開始してください。

保存済みの設定を使用して手動検索を実行するには、次のいずれかを実行してください。

- Web ブラウザで、[Summary] 画面の Scan now をクリックします。
- X Window のタスクバーのアプリケーション起動ボタンから、[System (Tools)]→[Trend Micro ServerProtect]→[Manual Scan]→[Start Scan Now] の順にクリックします。

設定を変更してから手動検索を実行するには

1. 左のメニューから [Scan Options]→[Manual Scan] の順に選択します。[Manual Scan] 画面が表示されます。
2. 必要に応じて、設定内容を変更します。73 ページの「除外リスト」を参照してください。
3. [Save & Scan] をクリックして、設定を適用します。次の確認画面が表示されます。

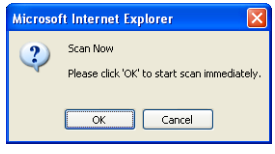


図 3-3.　手動検索の確認画面

4. [OK] をクリックして、検索を開始します。進行状況画面が表示され、検索のステータスが示されます。

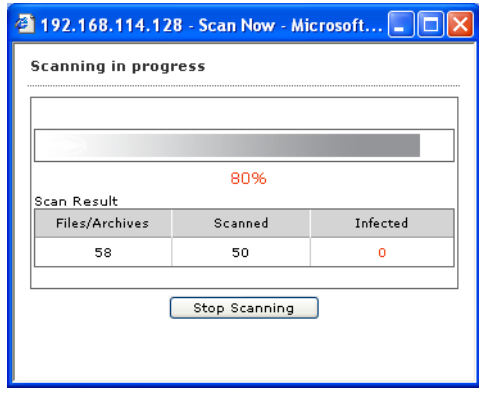


図 3-4. 進行状況画面

注意： 手動検索が完了する時間は、ファイルサイズや検索するファイルの数に応じて異なります。手動検索は、ピーク外の時間帯に実行するか、他のアプリケーションを閉じてから開始することをお勧めします。

コマンドラインから手動検索を実行するには

/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp フォルダの次のコマンドを実行します。

```
./splxmain -m <ディレクトリ>
```

<ディレクトリ> には検索対象のディレクトリのパスを入力します。複数のディレクトリを指定するには、コロン (:) で区切ります。たとえば、/temp1 と /temp2 を検索するには、次のように入力します。

```
./splxmain -m /temp1:/temp2
```

手動検索を停止するには

- 進行状況画面の [Stop Scanning] をクリックします。

- 次のコマンドを実行します。

```
./splxmain -n
```

- X Window のタスクバーのアプリケーション起動ボタンから、[System (Tools)]→[Trend Micro ServerProtect]→[Manual Scan]→[Stop Scan Now] の順にクリックします。

検索オプションを設定する

個々の Web 画面で各検索オプションを設定します。ただし、それらのオプションは次のような複数の共通コンポーネントを共有します。

- 検索するディレクトリ
- 検索するファイルタイプ
- 圧縮ファイルの対処方法
- 感染ファイルの処理
- 除外するディレクトリまたはファイル

次のセクションでは、各コンポーネントについて詳しく説明します。

検索ディレクトリを設定する

検索するディレクトリを指定するには

1. 左のメニューから [Scan Options] を選択して、設定する検索の種類を選択します。

2. [Scan These Locations] セクションで、検索するディレクトリの範囲を選択します。

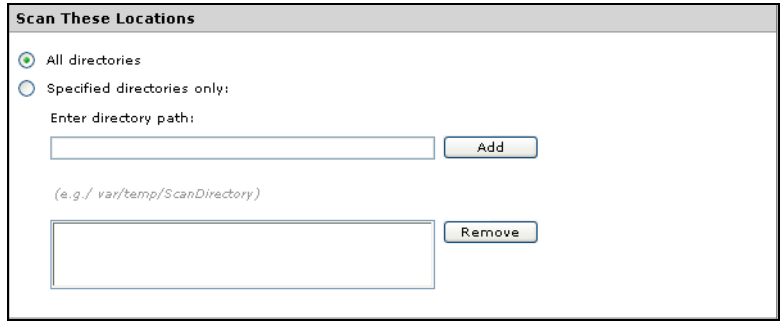


図 3-5. 検索するディレクトリの選択

次のオプションがあります。

- All directories: すべてのディレクトリを検索します (除外リストに含まれるディレクトリは除く)。詳細については、73 ページの「除外リスト」を参照してください。
- Specified directories only: 指定したディレクトリおよびサブディレクトリのみを検索します。指定方法は次のとおりです。

  i. [Enter directory path] に検索対象のディレクトリを入力します。

  例 :/var/temp/ScanDirectory

  注意 : ディレクトリパス名は大文字と小文字が区別されます。

  ii. [Add] をクリックして、入力したパスを [Specified directories only] リストに追加します。

  iii. 他のディレクトリを追加する場合は、上記の手順を繰り返します。

3. [Save] をクリックして、設定を適用します。

注意： 手動検索および予約検索の場合、検索対象のディレクトリを入力する際に、アスタリスク (*) または疑問符 (?) をワイルドカードとして使用できます。リアルタイム検索の場合、ServerProtect ではアスタリスク (*) を使用して同じレベルのすべてのディレクトリに対応させることはできません (/*/home など)。アスタリスク (*) を使用すると、予想しない検索結果が出ることがあります。

検索リストからディレクトリを削除するには

1. 検索リストから削除するディレクトリを選択します。
2. [Remove] をクリックして、検索リストから選択したディレクトリを削除します。
3. [Save] をクリックして、設定を適用します。

検索するファイルタイプを指定する

ウイルスに感染しやすいファイルタイプのみを検索するように設定することにより、検索時間を大幅に短縮できるとともに、システムリソースを節約できます。

検索するファイルタイプを指定するには

1. 左のメニューから [Scan Options] を選択して、設定する検索の種類を選択します。

2. [Scan These Files] で、検索するファイルタイプを指定します。

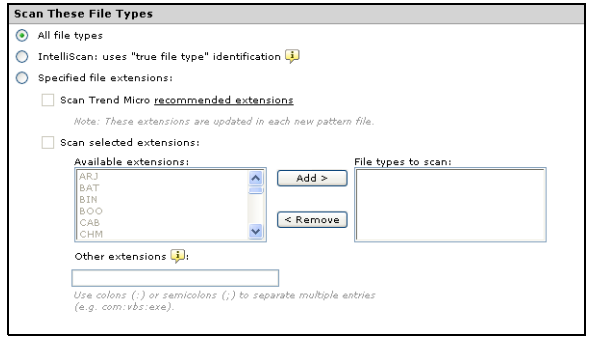
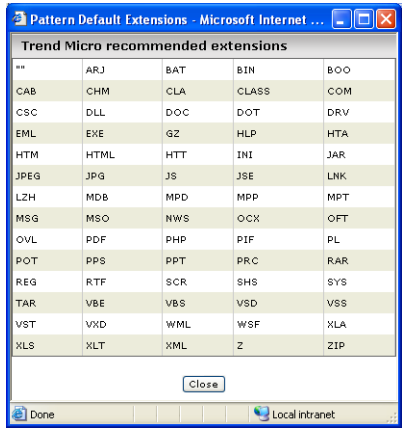


図 3-6. 検索するファイルタイプの選択

次のオプションがあります。

- All file types: 除外リストに含まれるファイルを除いてすべてのファイルを検索します (73 ページの「除外リスト」を参照)。
- IntelliScan: uses "true file type" identification: ファイルのヘッダを検索して、不正プログラムコードが潜んでいる可能性のあるファイルタイプと判断された場合にのみ、ファイルの本体を検索します。ツールチップアイコン ( ) の上にカーソルを合わせると、この機能の詳しい説明が表示されます。
- Specified file extensions: 指定した拡張子を持つファイルのみを検索します。検索対象とするファイルの拡張子は、次のいずれかの方法で指定します。複数の指定方法を組み合わせて指定することもできます。次のオプションがあります。

- Scan Trend Micro recommended extensions : トレンドマイクロの提供するパターンファイルには、検索対象とするファイルの拡張子リストが含まれます。検索対象として推奨されるファイル拡張子の表を表示するには、[recommended extensions] リンクをクリックします。例 :



""	ARJ	BAT	BIN	BOO
CAB	CHM	CLA	CLASS	COM
CSC	DLL	DOC	DOT	DRV
EML	EXE	GZ	HLP	HTA
HTM	HTML	HTT	INI	JAR
JPEG	JPG	JS	JSE	LNK
LZH	MDB	MPD	MPP	MPT
MSG	MSO	NWS	OCX	OFT
OVL	PDF	PHP	PIF	PL
POT	PPS	PPT	PRC	RAR
REG	RTF	SCR	SHS	SYS
TAR	VBE	VBS	VSD	VSS
VST	VXD	WML	WSF	XLA
XLS	XLT	XML	Z	ZIP

図 3-7. ファイル検索の対象としてトレンドマイクロが推奨する拡張子

- Scan selected extensions: このチェックボックスをオンにして、検索対象とする拡張子を指定できます。指定方法は次のとおりです。

  i. [Select extensions...] リストから拡張子を選択します。

  ii. [Add >] をクリックして、検索リストに選択した拡張子を追加します。

  iii. [Save] をクリックします。

- Other extensions: 検索したい拡張子が [Select extensions...] リストに含まれていない場合は、このボックスにその拡張子を入力します。拡張子ごとにセミコロン (;) またはコロン (:) で区切って入力してください。例 :LGL;FIN;ADM または LGL:FIN:ADM

3. [Save] をクリックします。

拡張子を削除するには

1. [File types to scan] リストで、検索対象から除外する拡張子を選択します。
2. [< Remove] をクリックして、選択した拡張子を削除します。
3. [Save] をクリックして、設定を適用します。

圧縮ファイルを検索する

ServerProtect では、圧縮されたファイルのウイルス検索について、一定の制限を設定できます。圧縮ファイルの検索処理では、システムリソースに負荷がかかりますのでご注意ください。

圧縮ファイルの検索を有効にするには

1. 左のメニューから [Scan Options] を選択して、設定する検索の種類を選択します。
2. [Compressed File Scan Settings] で圧縮ファイルの検索を設定します。[Scan compressed files] チェックボックスをオンにして、圧縮ファイル検索を有効にします。

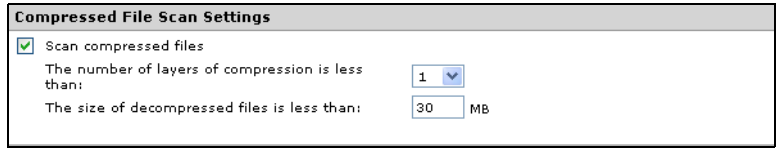


図 3-8.　圧縮ファイル検索

3. 何階層までの多重圧縮ファイルを検索するかを指定します。ServerProtect では、1~20 階層までの多重圧縮ファイルを検索できます。初期設定は、手動検索および予約検索については「5」、リアルタイム検索については「1」です。指定した数字より深い圧縮階層にあるファイルは検索されません。

4. 検索対象とする圧縮ファイルの最大サイズ (圧縮前) を指定します。

   設定できる値は、1MB ～ 2,000MB の値です。初期設定値は、手動検索および予約検索については 60MB、リアルタイム検索については 30MB です。指定したサイズを超えるファイルは検索されませんが、システムログにそれらのファイルに関するエントリが記録されます。

5. [Save] をクリックして、設定を適用します。

感染ファイルの処理を指定する

ウイルス検出時には、ウイルスに対してさまざまな処理を実行できます (下の表を参照)。

処理	説明
Clean (ウイルス駆除)	感染ファイルからウイルスコードを削除します。
Quarantine (隔離)	感染ファイルまたは不正ファイルをアクセスが制限された隔離ディレクトリに隔離します。
Rename (拡張子変更)	感染ファイルの拡張子を変更して、どのプログラムからも開いたり実行したりできないようにします。感染ファイルの拡張子は「vir」に変更されます。
Delete (削除)	感染ファイルや不正ファイルを削除します。
Pass (放置 (手動処理))	感染ファイルや不正ファイルは検索ログに記録されますが、ウイルスに対しては何の処理も実行しません。このオプションはお勧めしません。

表 3-1. 検出したウイルスに対して実行できる処理

感染ファイルの処理を指定するには

1. 左のメニューから [Scan Options] を選択して、設定する検索の種類を選択します。

2. [Actions When Security Risks Found] で、[Back up file containing security risk before action is taken] チェックボックスをオンにして、バックアップコピーを作成してから感染ファイルを駆除します。このオプションを選択するようにお勧めします。不正プログラムの駆除時に万一ファイルが破損したときのために、駆除対象ファイルのバックアップファイルを作成するように設定できます。

3. 検出時の処理を選択します。次のオプションがあります。

   - Use ActiveAction: ウイルスなどの不正プログラムに対して事前設定されている一連の検出時の処理です。ウイルス検出時の推奨処理は、Clean (駆除) です。トロイの木馬およびジョークプログラム検出時の推奨処理は、Quarantine (隔離) です。特定の種類のセキュリティリスクに適した検出時の処理が不明の場合は、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。
   - Use customized scan action: 下の表を使用して、セキュリティリスクの種類 (ジョークプログラム、トロイの木馬、ウイルス、テストウイルス、スパイウェア / グレーウェアなど) ごとに、一次処理を指定します。ウイルス、パッカーなどのセキュリティ侵害要因については、二次処理を選択します。たとえば、ウイルスについては、一次処理として「Clean (駆除)」を選択し、二次処理として「Quarantine (隔離)」を選択するとよいでしょう。

注意： ウイルスなどが検出されたファイルに対して最初の処理も 2 番目の処理も実行不可能な場合、ログエントリでは駆除不能カテゴリで 1 回としてカウントされます。

- Use the same action for all types: これらのフィールドでは、ファイルタイプに関係なく、すべてのファイルに対して同じ処理を選択できます。2 番目の処理は、最初の処理として「Clean (駆除)」が選択されている場合に限り、ウイルス、パッカーなどの脅威に対してのみ適用されます。

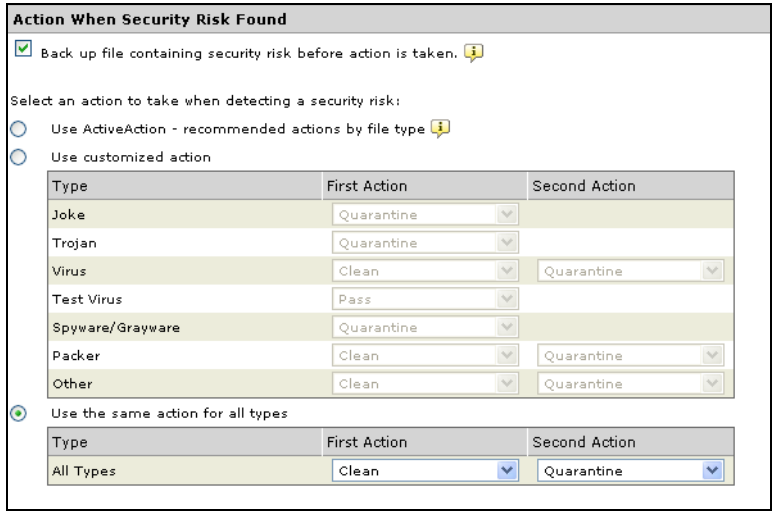


図 3-9.　検出時の処理の指定

注意： 不正プログラムの駆除時に万一ファイルが破損したときのために、駆除対象ファイルのバックアップファイルを作成するように設定できます。[Back up file containing security risk before action is taken] チェックボックスをオンにすると、バックアップファイルが作成されます。

除外リスト

ServerProtect では、特定のファイル、ディレクトリ、およびファイルタイプを検索対象から除外できます。この機能を使用すると、隔離ディレクトリやウイルス感染しない特定ファイルの検索を回避できます。万一、検索エンジンが誤警告を発した場合、誤認されたファイルを一時的にこのリストに含めることができます。

注意： 検索の種類ごとに個別の除外リストがあるため、それぞれの検索の対象を柔軟に制御できます。

除外リストの種類は、次のとおりです。

- Directories to exclude: このリストを使用すると、ディレクトリ全体を検索対象から除外できます。
- Files to exclude: このリストを使用すると、特定のファイルを検索対象から除外できます。
- File types to exclude: このリストでは、指定したファイルタイプを検索対象から除外できます。

警告： 除外するディレクトリのリストが空白の場合、リアルタイム検索は機能しません。

ワイルドカード文字を使用する

手動検索と予約検索では、除外リストでアスタリスク (*) または疑問符 (?) のワイルドカード文字を使用できます。アスタリスク (*) は任意の文字列に相当し、疑問符 (?) は任意の 1 文字に相当します。

注意： リアルタイム検索では、除外リストまたは検索対象とする拡張子のリストでワイルドカードを使用できません。アスタリスク (*) を使用すると、予想しない検索結果が出ることがあります。

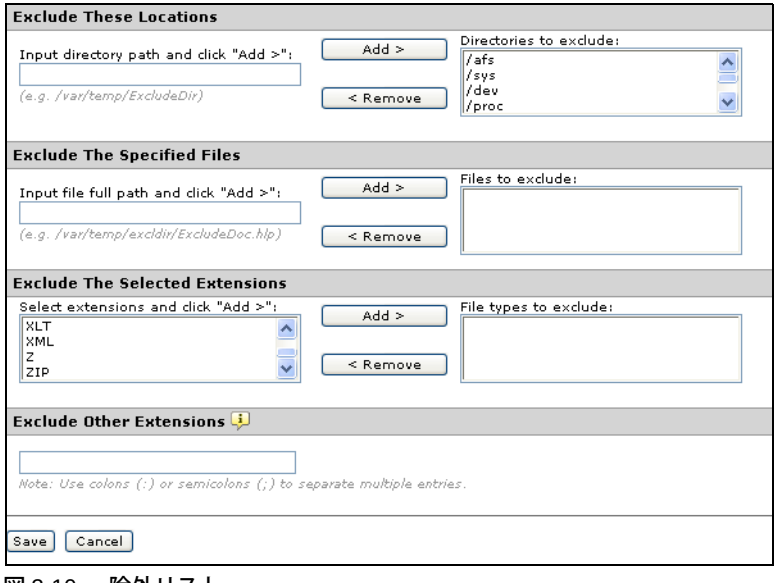


図 3-10.　除外リスト

隔離ディレクトリを指定する

場合によっては、検索エンジンが特定のファイルのウイルスを駆除できないことがあります。また、パスワードで保護されているファイルなど、ウイルスを駆除できないファイルもあります。駆除できないファイルを削除したくない場合は、ServerProtect の隔離ディレクトリにそのファイルを隔離することをお勧めします。初期設定のバックアップディレクトリは次のとおりです。

```
/opt/TrendMicro/SProtectLinux/SPLX.Quarantine
```

警告： 隔離ディレクトリにはウイルス感染の疑いのあるファイルが格納されます。このため、隔離ディレクトリ内のファイルの扱いには注意してください。

隔離ディレクトリを指定するには

1. 左のメニューから [Scan Options]→[Quarantine Directory] の順に選択します。[Quarantine Directory] 画面が表示されます。[Quarantine Directory] 画面が表示されます。
2. [Quarantine directory] フィールドに、隔離ディレクトリのフルパスを入力します。
3. [Save] をクリックします。

注意： 隔離ディレクトリを変更しても、既存の隔離ファイルは変更前のディレクトリ内に残ります。

バックアップディレクトリの場所を指定する

ServerProtect は、リアルタイム検索、手動検索、または予約検索によってウイルスを駆除する前に、感染ファイルをバックアップできます (最初に、希望する検索の種類に対して駆除処理を選択してください)。バックアップディレクトリの場所は、[Backup directory] 画面で必要に応じて変更できます。初期設定のバックアップディレクトリの場所は、次のとおりです。

```
/opt/TrendMicro/SProtectLinux/SPLX.Backup
```

警告： バックアップディレクトリにはウイルス感染の疑いのあるファイルが格納されます。このため、バックアップディレクトリ内のファイルの扱いには注意してください。

バックアップディレクトリの場所を指定するには

1. 左のメニューから [Scan Options]→[Backup Directory] の順に選択します。
2. [Backup Directory] に、新しいバックアップディレクトリのフルパスを入力します。
3. [Save] をクリックします。

注意： このディレクトリを変更しても、既存のバックアップファイルは変更前のディレクトリ内に残ります。新たに作成されるバックアップファイルだけが新しいバックアップディレクトリに保存されます。

第 4 章

アップデート

Trend Micro ServerProtect for Linux (以下、ServerProtect) には、製品開発時点で入手可能な検索エンジンおよびパターンファイルが付属しています。これらのコンポーネントは最新の脅威に対応していない可能性があります。ServerProtect をインストールしたらすぐにアップデートすることをお勧めします。

本章では、次の内容について説明します。

アップデートの概要

アップデートは、多くのトレンドマイクロ製品に共通のサービスです。アップデートでは、トレンドマイクロのアップデートサーバに接続して ServerProtect で使用するパターンファイルと検索エンジンをダウンロードできます。

アップデートを実行しても、ネットワークサービスが妨げられたり、コンピュータを再起動する必要はありません。アップデートは、設定した定期スケジュールに従って利用することも、必要に応じて利用することも可能です。

コンポーネントのアップデート

ServerProtect では、ActiveUpdate (トレンドマイクロのインターネットベースのコンポーネントアップデート機能) を使用して、次のコンポーネントまたはファイルがアップデートされます。

- ウイルス / スパイウェア / グレーウェアのパターンファイル : パターンファイルには、多数のウイルスシグネチャ (ウイルス、トロイの木馬など) が含まれ、有害なファイルを検出する機能が指定されます。トレンドマイクロでは、新種のウイルスに対応するために定期的にパターンファイルをアップデートしています。
- 検索エンジン : 検索エンジンは、ウイルス検索と駆除の働きをするコンポーネントです。検索エンジンは、パターンファイルのシグネチャで比較するパターンマッチング方式を採用しています。検索エンジンは、新種ウイルスに対応した新しい技術の採用など、検索機能を強化するためにアップデートされます。

手動または自動アップデート機能により、コンポーネントのアップデートを実行できます。ServerProtect をインストールしたら、ただちに手動アップデートを実行して、最新のコンポーネントを取得することをお勧めします。

注意 : インターネット接続にプロキシサーバを使用している場合は、あらかじめプロキシを設定しておく必要があります。

ダウンロード元を指定する

ServerProtect が Trend Micro Control Manager (以下、Control Manager) で管理されているかどうかによって、ダウンロード元が変わります。

- Control Manager で管理されていれば、通常のアップデートポリシーに従って自動的にアップデートが実行されるか、大規模感染予防ポリシーが起動されたときに自動的にアップデートが実行されます。Control Manager の初期設定のダウンロード元は、次のとおりです。

  http://xxx.xxx.xxx.xxx/TVCSDownload/ActiveUpdate

  「xxx.xxx.xxx.xxx」は、Control Manager の IP アドレスです。

- Control Manager で管理されていない場合、コンポーネントをアップデートするには Update Now (手動アップデート) 機能または予約ダウンロード機能を使用します。初期設定のダウンロード元は、次のとおりです。

  http://splx3-p.activeupdate.trendmicro.com/activeupdate

ダウンロード元をカスタマイズするには

1. 手動アップデート (83 ページの「手動アップデート」を参照)、または予約アップデート (84 ページの「予約アップデート」を参照) を設定します。
2. 次のいずれかのダウンロード元を選択します。
   - Trend Micro ActiveUpdate server: ServerProtect が Control Manager で管理されていない場合の初期設定のアップデートサーバです。
   - Trend Micro Control Manager update server: ServerProtect が Control Manager で管理されている場合の初期設定のアップデートサーバです。
   - Other Internet source: イントラネットなどの HTTP または HTTPS の Web サイトを指定します。コンポーネントのダウンロードに使用するポート番号も含めます。

     ここで指定するサーバには、最新のコンポーネントが置かれている必要があります。対象サーバのホスト名または IP アドレスと、コンポーネントのあるディレクトリを指定します (例 : https://192.168.10.1:14943/source)。さらに、

複数のバックアップ用のアップデートサーバ / ダウンロード元を設定して、プライマリダウンロード元に障害が発生した場合、自動的にフェイルオーバーするように設定できます。

プロキシサーバを設定する

インターネットへアクセスする際にプロキシサーバを使用している場合、ServerProtect では次の機能に対してプロキシを設定できます。

- ウイルストラッキングプログラム
- ライセンスのアップデート
- コンポーネントのアップデート

ウイルストラッキングプログラムおよびライセンスのアップデートに対してプロキシを設定するには

1. [Update]→[Proxy Settings] をクリックします。[General] 画面が表示されます。
2. [Use a proxy server to access the Internet] チェックボックスをオンにします。
3. [Proxy Protocol] フィールドで [HTTP]、[SOCKS4] または [SOCKS5] を選択します。
4. [Server name or IP address] フィールドに、プロキシサーバの IP アドレスまたはホスト名を入力します。
5. [Port] フィールドに、プロキシサーバの待機ポート番号を入力します。
6. オプションのプロキシ認証のユーザ名とパスワードを使用している場合には、それを [User name] および [Password] に入力します。

7. [Save] をクリックします。

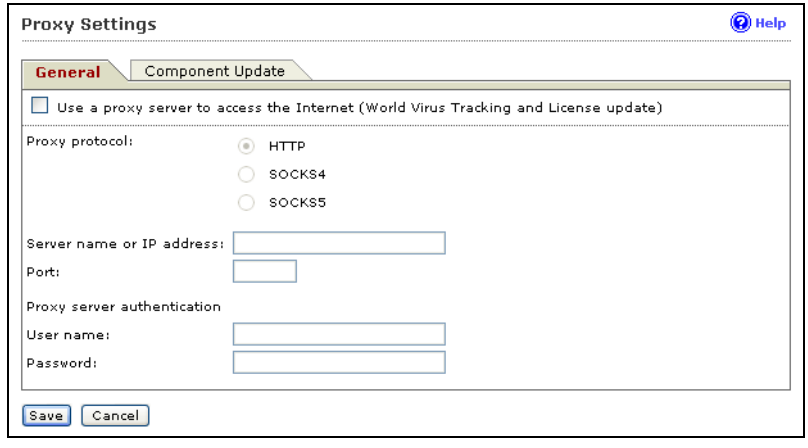


図 4-1. [Proxy Settings General] 画面

ヒント： ServerProtect をインストールしたら、ただちにウイルスパターンファイルおよび検索エンジンをアップデートすることをお勧めします。インターネットへアクセスする際にプロキシサーバを使用する場合には、プロキシサーバを設定してから検索エンジンとパターンファイルをアップデートしてください。

コンポーネントのアップデートにプロキシを設定するには

1. [Update]→[Proxy Settings]→[Component Update] の順にクリックします。[Component Update] 画面が表示されます。

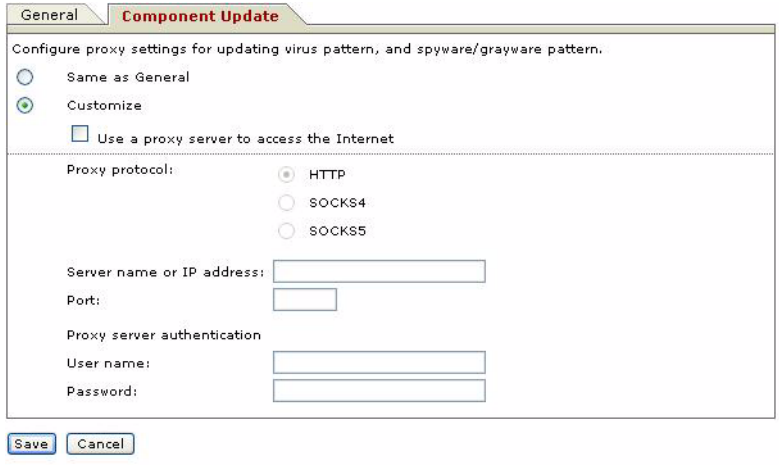


図 4-2. プロキシ設定の [Component Update] 画面

2. [General] 画面で設定したのと同じプロキシサーバを使用するには、[Same as General] を選択します。
3. プロキシを設定するには、[Customize] を選択します。
4. プロキシサーバをコンポーネントのアップデートに使用する場合は、[Use proxy server to access the Internet] をオンにします。そして、手順 5 に進みます。

   プロキシサーバをコンポーネントのアップデートに使用しない場合は、[Use proxy server to access the Internet] をオフにします。たとえば、アップデートサーバが企業のネットワーク内にある場合などです。そして、手順 9 に進みます。
5. [Proxy Protocol] で、[HTTP]、[SOCKS4]、[SOCKS5] を選択します。
6. [Server Name or IP Address] フィールドに、プロキシサーバの IP アドレスまたはホスト名を入力します。
7. [Port] フィールドに、プロキシサーバの待機ポート番号を入力します。

8. オプションのプロキシ認証のユーザ名とパスワードを使用している場合には、それを [User name] および [Password] に入力します。

9. [Save] をクリックします。

注意： コマンドラインでプロキシのパスワードを設定する場合については、226 ページの「splxmain」を参照してください。

手動アップデート

必要なときにただちにアップデート (Update Now) を実行できます。この機能は、ウイルスアウトブレーク発生時などすぐに最新のコンポーネントが必要な場合や、ServerProtect インストール直後に役立ちます。

手動アップデートを実行するには、複数の方法があります。

- [Summary] または [Manual Scan] 画面で [Update Now] をクリックします。
- KDE のメインウインドウで、タスクバーのアプリケーション起動ボタンから [System (Tools)]→[Trend Micro ServerProtect]→[Start Update Now] の順にクリックします。

[Summary] 画面から手動アップデートを実行するには

1. 左のメニューから [Summary] を選択します。
2. [Component Status] セクションで、[Component] チェックボックスですべてのコンポーネントをオンにしてアップデートするか、個々のコンポーネントをオンにしてアップデートします。
3. [Update Now] をクリックします。

[Manual Update] 画面から手動アップデートを実行するには

1. Web コンソールの左のメニューから、[Update]→[Manual Update] の順に選択します。[Manual Update] 画面が表示されます。

2. アップデートするコンポーネントのチェックボックスをオンにします。現在のコンポーネントのバージョンは、各コンポーネントの右に表示されています。[Component] チェックボックスをオンにして、すべてのコンポーネントを選択します。

3. 次に、ダウンロード元を指定します。詳細については、79 ページの「ダウンロード元を指定する」を参照してください。

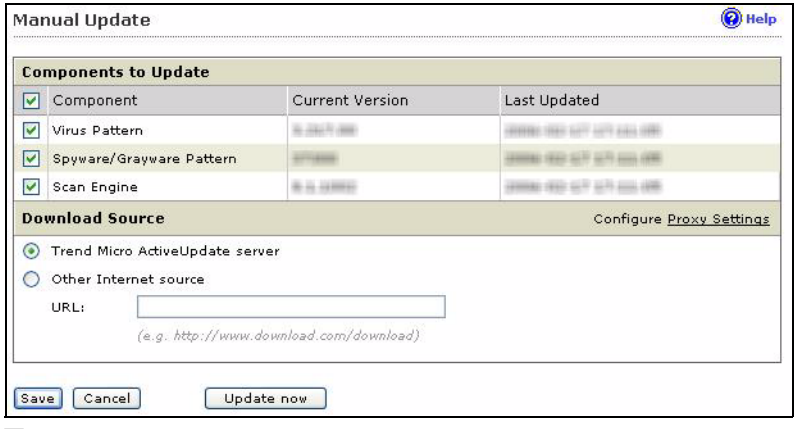


図 4-3. [Manual Update] 画面

4. [Save] をクリックして、設定を保存します。[Update Now] をクリックし、設定内容を保存して手動検索を実行します。

注意： 複数のバックアップのダウンロード元を使用するには、ServerProtect を実行するサーバで新しいプライマリダウンロード元からのアップデートを完了している必要があります。プライマリダウンロード元および追加のバックアップダウンロード元の設定については、トレンドマイクロのテクニカルサポートにお問い合わせください。

予約アップデート

予約アップデートでは、定期的な自動アップデートを設定できます。

予約アップデートを設定するには

1. Web コンソールの左のメニューから、[Update]→[Scheduled Update] の順に選択します。[Scheduled Update] 画面が表示されます。
2. [Enable scheduled update] チェックボックスをオンにします。
3. アップデートするコンポーネントのチェックボックスをオンにします。現在のコンポーネントのバージョンは、各コンポーネントの右に表示されています。[Component] チェックボックスをオンにして、すべてのコンポーネントを選択します。
4. ダウンロード元を選択します。

   プライマリダウンロード元で障害が発生した場合、自動的にフェイルオーバーできるように複数のバックアップのアップデートサーバ / ダウンロード元を設定できます。

   注意： 複数のバックアップのダウンロード元を使用するには、ServerProtect を実行するサーバで新しいプライマリダウンロード元からのアップデートを完了している必要があります。プライマリダウンロード元および追加のバックアップダウンロード元の設定については、トレンドマイクロのテクニカルサポートにお問い合わせください。

5. リストボックスから開始時間を選択します。
6. アップデートの周期を指定します。アップデートの周期は [Hourly（毎時間）]、[Daily（毎日）]、[Weekly（毎週）] から選択します。[Weekly（毎週）] を選択した場合は、曜日 ([Sunday（日曜日）]、[Monday（月曜日）] など) も指定してください。

注意： [Daily] および [Weekly] では、x 時間の期間のアップデートを指定できます。つまり、アップデートは選択した開始時間に従って、x 時間以内に実行されます。この機能により、トレンドマイクロのアップデートサーバではロードバランスが取られます。また、実際の時間を指定することもできます。ツールチップアイコン ( ) 上にカーソルを移動すると、より詳細な機能の説明と例が表示されます。

7. [Proxy Settings] リンクをクリックしてプロキシ設定を行います。詳細については、80 ページの「プロキシサーバを設定する」を参照してください。

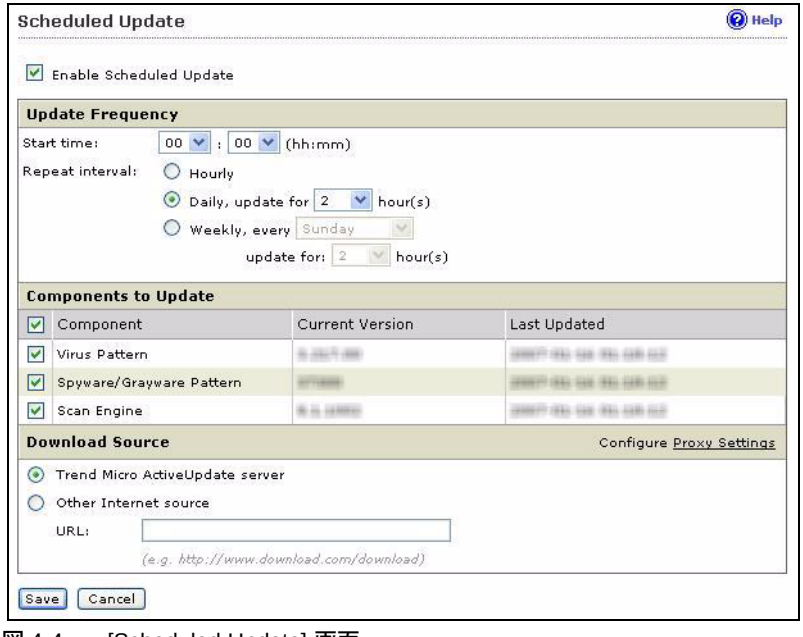


図 4-4. [Scheduled Update] 画面

8. [Save] をクリックします。

第 5 章

ログと通知

本章では、次の内容について説明します。

ログの種類

ServerProtect では、次の 4 種類のログが記録されます。

- Spyware Log (**スパイウェアログ**): スパイウェアログでは、スパイウェア / グレーウェアの検出についてレポートされます。これには、検出日時、セキュリティ侵害要因の名前、検索の種類、実行された処理と結果、スパイウェア / グレーウェアが検出されたファイルの場所などの情報が含まれます。
- Virus Log (**ウイルスログ**): ウイルスログでは、不正プログラムの検出についてレポートされます。これには、検出日時、セキュリティ侵害要因の名前、検索の種類、実行された処理と結果、不正プログラムが検出されたファイルの場所などの情報が含まれます。
- Scan Log (**検索ログ**): 検索ログでは、サーバ上で試行または実行された検索の種類がレポートされます。これには、開始と終了の日時、検索したファイルの数、検出件数などの情報が含まれます。
- System Log (**システムログ**): システムログでは、パターンファイルおよび検索エンジンのアップデートや、各種サービスの有効化および無効化などのシステムイベントがレポートされます。このログには、イベントの日時と理由が記録されます。

検索結果 (ログ) を表示する

検索結果を表示するには、次の 2 つの方法があります。

- 手動検索 (Scan Now) の完了画面で表示 (手動検索の結果のみ)
- Web コンソールのログ画面で表示

手動検索 (Scan Now) の完了画面で表示する

Scan Now の完了画面では、検索したファイルの数、検出した感染ファイルの数などの情報が表示されます。

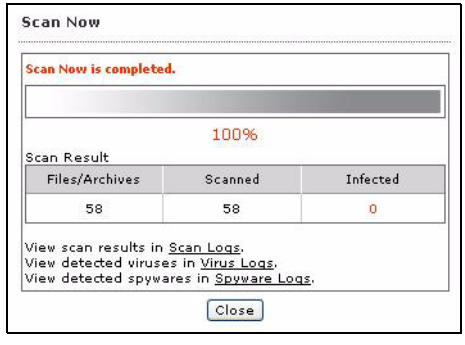


図 5-1.　Scan Now の完了画面

検索の詳細情報を参照するには、[Scan Logs] のリンクをクリックします。感染ファイルや検出ウイルスの詳細情報を参照するには、[Virus Logs] のリンクをクリックします。

Web コンソールのログ画面で表示する

ログを表示するには

1. 左のメニューから [Logs] を選択し、表示したいログの種類を選択します。
2. この画面の [Stored Logs] セクションには、現在ログデータベース内にあるログの数と、保存されているログ (存在する場合) の期間が表示されます。

3. 表示したいログの検索条件を指定します。パラメータは次のとおりです。

- Date Range: 次の一般的な指定期間から選択します。[All dates (すべて)]、[Today (今日)]、[Yesterday (昨日)]、[Past 7 days (7 日前まで)]、または [Past 30 days (30 日前まで)]。この他の期間を指定する場合は、[Specified date range (期間を指定)] を選択して [Start date (開始日)] と [End date (終了日)] を指定します。
- Start date: 表示したいログの中で最も古いログの日付を入力します。この条件を指定するには、[Data Range] で [Specified date range] を選択します。月、日、年の順に入力してください。または、カレンダアイコン () をクリックして、カレンダから日付を選択します。
- End date: 表示したいログの中で最も新しいログの日付を入力します。この条件を指定するには、[Data Range] で [Specified date range] を選択します。月、日、年の順に入力してください。または、カレンダアイコン () をクリックして、カレンダから日付を選択します。
- Sort by: ログのソート順とグループを指定します。グループのオプションは、[Date/Time]、[Virus Name]、[Scan Type]、[Action Result]、および [Source Files] です。ソート順は、[Ascending (昇順)] と [Descending (降順)] のいずれかを選択します。
- Entries per page: ドロップダウンメニューから、1 画面に表示するログの数を選択します。お使いのモニタの解像度に適した設定を選択してください。選択できる値の範囲は 15 ～ 200 であり、初期設定値は 25 です。

注意： 設定ファイルで「検索されるログ」の数を増やすことができます。詳細については、218 ページの「MaxRetrieveCount」を参照してください。

4. [Display Log] をクリックすると、設定した条件でログが表示されます。

検索ログの例については、次の図を参照してください。

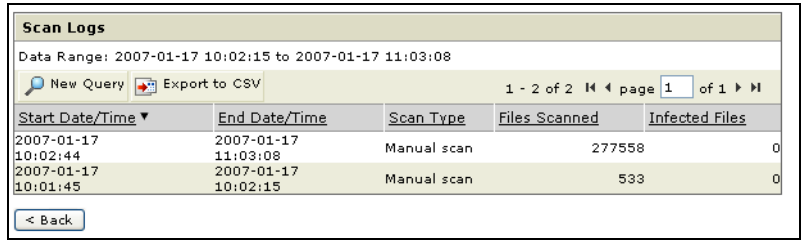


図 5-2. 検索ログの例

ウイルスログの例については、次の図を参照してください。

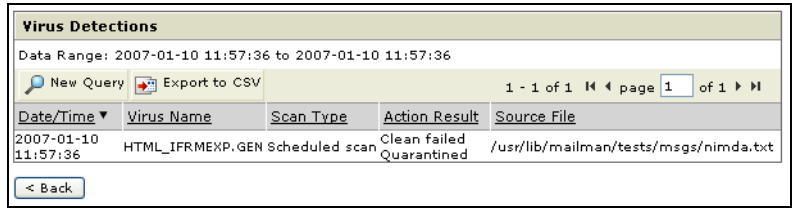


図 5-3. ウイルスログの例

システムログの例については、次の図を参照してください。

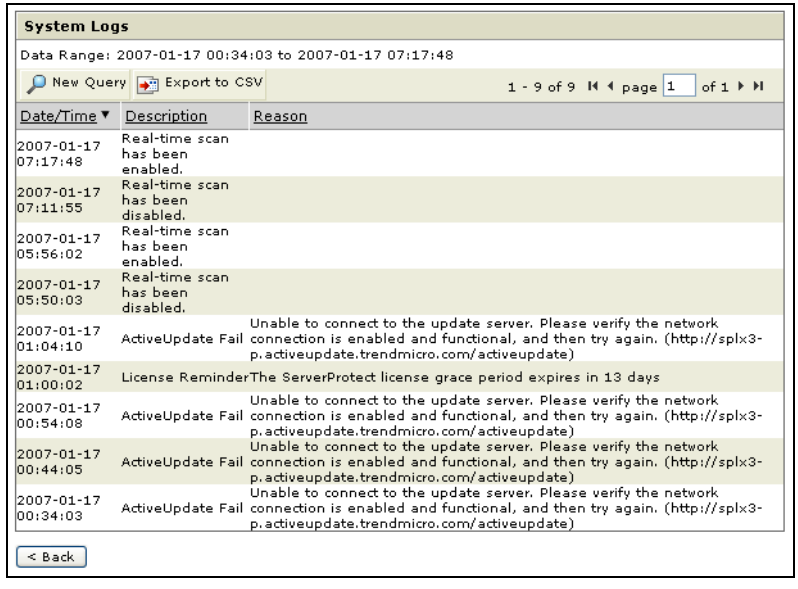


図 5-4.　システムログの例

ログを閉じて新しいログ検索を開始するには、 New Query をクリックします。ログ検索の結果を .csv ファイルに出力するには、 Export to CSV をクリックします。ナビゲーション矢印 (page 1 of 10) をクリックすると、ログ検索結果の最初の画面、前の画面、次の画面、最後の画面に移動できます。データを更新するには、このフレームの Web ブラウザの更新機能を使用します。更新すると、選択したログ検索の種類に応じて、ログ検索画面に新しいデータが追加されることがあります。たとえば、今日のログを数時間前に最初に要求した後でこの画面を更新した場合は、数時間前にログ検索してから更新するまでの間に実行された活動がログ結果に追加されます。

注意： ログを CSV 形式でエクスポートしたファイルは UTF-8 でエンコードされています。CSV 形式のファイル内容を正しく表示するには、システムロケールを UTF-8 に設定する必要があります。

ログディレクトリの場所を指定する

検索ログ、スパイウェアログ、ウイルスログ、およびシステムログは、ログディレクトリに保存されます。初期設定のログディレクトリの場所は次のとおりです。

/var/log/TrendMicro/SProtectLinux

Web コンソールで新しいログディレクトリを指定するには

1. [Logs]→[Log Directory] の順にクリックします。
2. 表示されるフィールドに、新しいログディレクトリのフルパスを入力します。
3. [Save] をクリックします。

注意： このディレクトリを変更しても、既存のログファイルは変更前のディレクトリ内に残ります。

ログを削除する

ログを自動的にまたは手動で削除するように ServerProtect を設定できます。すべてのログを削除するように指定することも、指定した期間より古いログを削除するように指定することもできます。

ログを自動削除する

ログを蓄積してディスク容量を消費しないように、ServerProtect ではログの保存期間が制限されます。初期設定では、ログは 60 日間保存された後自動的に削除されます。

Web コンソールで自動ログ削除を設定するには

1. [Logs]→[Automatic Delete] の順にクリックします。

2. 自動ログ削除を無効にするには、[Keep logs for] チェックボックスをオフにします。この機能を有効にするには、このチェックボックスをオンにして、表示されているフィールドにログの保存日数を入力します。

3. [Save] をクリックして、変更を保存します。

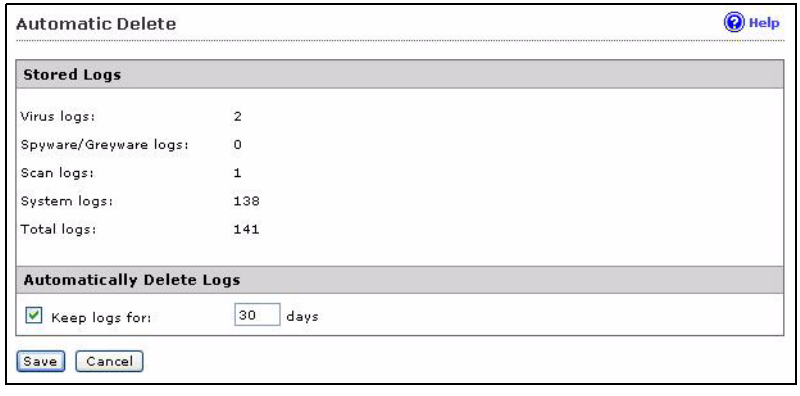


図 5-5. 自動削除

4. ログの保存日数を示す画面が表示されます。[OK] をクリックして、前の画面に戻ります。

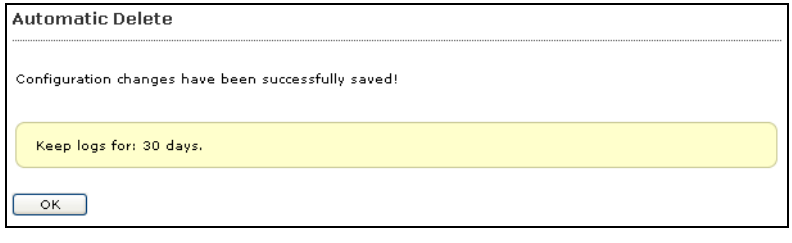


図 5-6. 自動削除設定の保存

ログを手動削除する

指定した日付より前に作成されたログは、いつでも手動で削除できます。これによって、ログが蓄積してディスク容量を消費することが防止されます。

Web コンソールでログを手動削除するには

1. [Logs]→[Manual Delete] の順にクリックします。
2. すべてのログを手動削除するには、[All Logs] を選択します。指定した日付より前に作成されたログを削除するには、[Logs before this date] を選択し、カレンダアイコン ( ) をクリックして日付を選択します。
3. [Delete] をクリックして、変更を保存します。

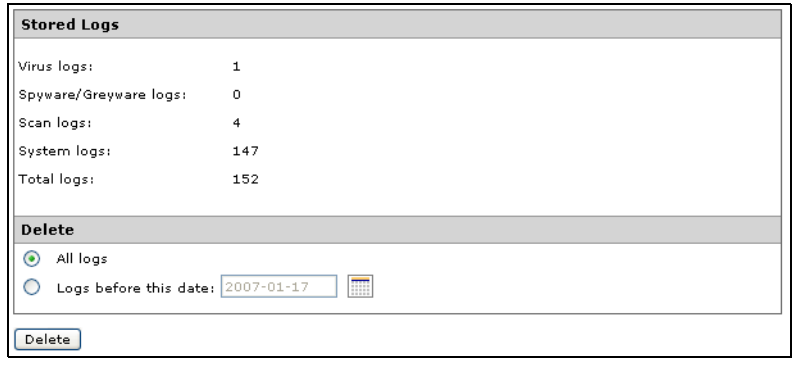


図 5-7. 手動削除

4. 確定を求めるプロンプトが表示されます。[OK] をクリックして、ログを削除します。

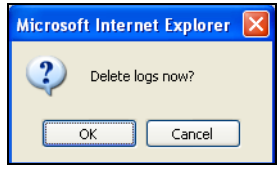


図 5-8. 手動削除の確定

5. 手動削除処理の結果を示す画面が表示されます。[OK] をクリックして、前の画面に戻ります。

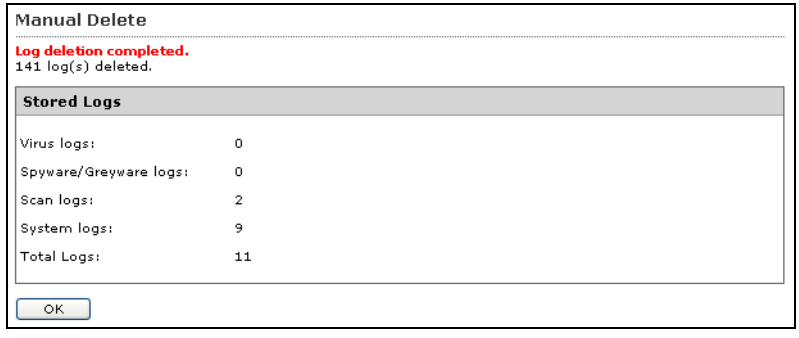


図 5-9. 手動削除の結果

通知を設定する

ServerProtect は、ユーザがネットワークから離れている場合でも、ネットワーク上で発生した特定のイベントをユーザに通知できます。ウイルス大規模感染、感染、およびシステム設定の変更を、さまざまな通知方法でユーザに知らせることができます。

ここでは、通知の対象となる警告イベントを指定する方法や通知方法について説明します。

注意： [Alert Settings] 画面で入力された通知メッセージは UTF-8 でエンコードされます。通知メッセージに非 ASCII 文字を使用する場合は、Web ブラウザのエンコード設定を UTF-8 に設定してください。

警告イベントを設定する

警告イベントおよび各イベントについて ServerProtect から送信されるメッセージを指定できます。ここでは次の手順を説明します。

- 警告の有効化、初期設定の警告通知の確認
- 初期設定の通知を変更してカスタムメッセージを作成

警告設定を確認またはアップデートするには

1. 左のメニューから [Notification]→[Alert Settings] の順に選択します。[Alert Settings] 画面が表示されます。
2. 送信する警告のチェックボックスをオンにします。
   - Send security risk outbreak notification: 指定された期間内に指定された数のウイルスなどの不正プログラムが検出された場合に、通知が送信されます。このオプションを選択した場合は、アウトブレークとして設定する数値も指定します。
   - Send standard security risk infection notification: システム上でセキュリティリスクが検出されるたびに通知が送信されます。
   - Send notification when Real-time Scan configuration was modified: リアルタイム検索の設定が変更されるたびに通知が送信されます。
   - Send notification when ServerProtect starts: ServerProtect サービスが開始されるたびに通知が送信されます。
   - Send notification when ServerProtect stops: ServerProtect サービスが停止されるたびに通知が送信されます。
   - Send notification when pattern files are outdated: 指定された日数を超えてもウイルスパターンファイルがアップデートされなかった場合に通知が送信されます。このオプションを選択した場合は、基準とする期間も指定する必要があります。
   - Send notification when pattern update unsuccessful: パターンファイルのアップデートに失敗した場合に通知が送信されます。
   - Send notification when action performed on malware unsuccessful: 検出された不正プログラムに対して指定された処理を実行できなかった場合に通知が送信されます。

3. 各警告イベントには、初期設定の通知メッセージが用意されています。例については、次の図を参照してください。

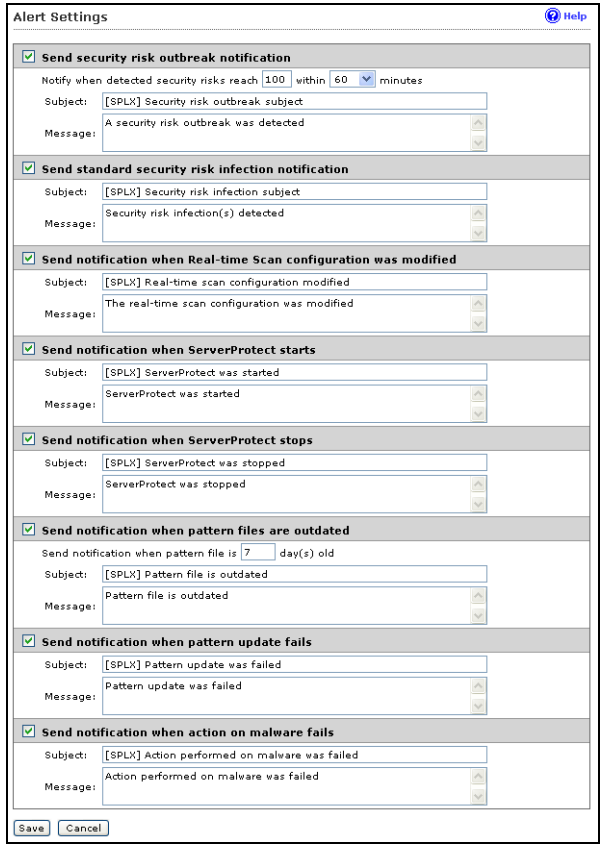


図 5-10.　警告通知メッセージ

カスタム通知メッセージを作成するには

1. [Message] フィールドで、既存のテキストを削除して新しいテキストを入力し、初期設定の通知を変更します。メッセージは 255 文字以内で指定します。
2. [Save] をクリックします。

通知の受信者を指定する

ServerProtect では、メールや SNMP を使用して複数の宛先に通知できます。ここでは、次の手順を説明します。

- SMTP メール通知の設定
- SNMP 通知の設定

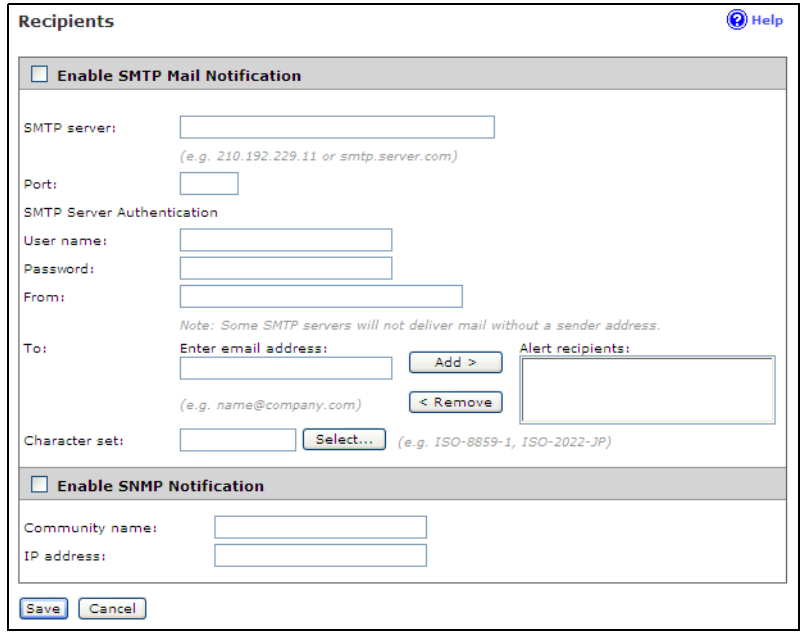


図 5-11.　通知の受信者

SMTP メール通知を設定するには

1. 左のメニューから [Notification]→[Recipients] の順に選択します。
2. [Enable SMTP Mail Notification] チェックボックスをオンにします。

3. [SMTP server] に、SMTP サーバの名前または IP アドレスを入力します。たとえば、次のように入力します。

   smtp.server.com または 192.168.0.0

4. [Port] に、メールサーバの待機ポートを指定します。

5. [User Name] および [Password] フィールドに、メールアカウント情報を入力します。

6. [From] に、メール送信者としたい管理者などのメールアドレスを入力します。

注意： SMTP サーバの種類によっては、送信者のメールアドレスが存在しないとメールが送信できない場合もあります。

7. 受信者のメールアドレスを追加するには、[Enter email address] フィールドに受信者のメールアドレスを入力し、[Add>] をクリックして [Alert Recipients] リストに追加します。

8. 受信者のメールアドレスを削除するには、[Alert Recipient] リストで対象のメールアドレスを選択し、[< Remove] をクリックします。

9. メール通知に使用する文字コードを選択します。[Select ...] をクリックすると、使用可能な文字コードが [Preferred Charset] ウィンドウに表示されます。

注意： システムロケールの文字コードが Preferred Charset のオプションに含まれていない場合、設定ファイル tmsplx.xml の SmtpCharset キーを utf-8 に設定します。これにより、システムロケールに応じてメール通知の文字コードが適切に変換されます。

10. [Save] をクリックします。

SNMP 通知を設定するには

1. 左のメニューから [Notification]→[Recipients] の順に選択します。

2. [SNMP Notification] チェックボックスをオンにします。

3. [Community name] に、メッセージのコミュニティ名を入力します。
4. [IP address] に、SNMP トラップサーバの IP アドレスを入力します。
5. [Save] をクリックします。

第 6 章

トラブルシューティングとテクニカルサポート

本章では、役に立つトラブルシューティングのヒントとテクニカルサポートへの問い合わせに必要な情報について説明します。

本章では、次の内容について説明します。

トラブルシューティング

Trend Micro ServerProtect for Linux（以下、ServerProtect）の使用中に直面する可能性のある問題について、解決方法を説明します。

初期設定のパスワード

ServerProtect の初期設定では、パスワードが設定されていません。ServerProtect のインストール後は、すぐにパスワードを設定するようにしてください。

Web コンソールでパスワードが拒否される

Web コンソールによって、入力したパスワードが拒否される場合があります。これには、次のような理由が考えられます。

- **パスワードの誤り**：パスワードは、大文字と小文字を区別します。「TREND」、「Trend」、「trend」では異なるパスワードになります。
- **ServerProtect 用 Apache サーバが応答していない**：splxhttpd のステータスを確認してください。詳細については、231 ページの「splxhttpd」を参照してください。
- **Java プラグインが正しくインストールされていない**：Mozilla、Mozilla Firefox、または Internet Explorer ブラウザを使用していると、Java プラグインが正しくインストールされない場合があります。サポートが必要な場合は、テクニカルサポートにお問い合わせください。

コンポーネントの自動アップデート

Trend Micro Control Manager (以下、Control Manager) から自動的にコンポーネントを取得できない場合、Control Manager 上でコンポーネントのアップデートを実行してください。これにより Control Manager が ServerProtect の情報を取得し、自動アップデートを実行できるようになります。詳細については、54 ページの「自動アップデートの開始」を参照してください。

ServerProtect に関連したシステムログ

Linux コンピュータで次の ServerProtect システムログが作成される場合があります。これらのログが、ServerProtect またはお使いの Linux コンピュータの、パフォーマンスや動作に影響を与えることはありません。

```
splx_vsapiapp:[MODULE_NAME - CXIpc::connectToServer2] errno=2

some error were found while stopping entity.Force terminating it
```

デバッグログ

ServerProtect では、次のデバッグオプションが用意されています。

- **カーネルデバッグ**: カーネル関連の処理に対するデバッグ
- **ユーザデバッグ**: ユーザ関連の処理に対するデバッグ
- **Control Manager デバッグ**: Control Manager 関連の処理に対するデバッグ

SUSE Linux に syslog-ng を設定する

デバッグログ情報を SUSE Linux Enterprise Desktop/Server 10 で保存できるようにするには、syslog-ng (next-generation) の設定を指定する必要があります。

1. デバッグログファイルのパス /var/log をリアルタイム検索の除外リストに追加します。

2. /etc/syslog-ng/ にある syslog-ng.conf ファイルを開いて、次の行をファイルに追加します。

```
# this is for splx debug log

filter f_splx                          { facility(local3); };

# logs for splx debug

destination splx_debug_log { file("/var/log/splx.debug");
};

log {source(src); filter(f_splx);
destination(splx_debug_log); };
```

3. ターミナルに「/etc/init.d/syslog restart」と入力して、syslog デーモンを再起動します。

4. tmsplx.xml ファイルのデバッグキー (UserDebugLevel) を 5 に設定します。

5. 「service splx restart」と入力して、ServerProtect を再起動します。

この設定を行った後は、ServerProtect では /var/log/ の splx.debug ファイルにデバッグ情報が保存されます。このファイルを開いてデバッグログを確認することができます。

デバッグレベルについて

各デバッグパラメータのデバッグレベルは、tmsplx.xml で定義します。

値	カーネルデバッグ (KernelDebugLevel)	ユーザデバッグ (UserDebugLevel*)	Control Manager デバッグ (ControlManagerDebug †)
0	デバッグ無効 (初期設定)	デバッグ無効	デバッグ無効
1	エラーデバッグ	エラーデバッグ : エラーメッセージを記録します（初期設定）。	エラーデバッグ (初期設定)
2	一般デバッグ	情報デバッグ : エラーメッセージと警告メッセージを記録します。	一般デバッグ
3	詳細デバッグ	一般デバッグ : エラーメッセージ、警告メッセージ、通知メッセージを記録します。	詳細デバッグ
4	n/a	重要デバッグ : エラーメッセージ、警告メッセージ、通知メッセージ、および情報メッセージを記録します。	n/a
5	n/a	詳細デバッグ : エラーメッセージ、警告メッセージ、通知メッセージ、情報メッセージ、およびデバッグメッセージを記録します。	n/a

表 6-1. tmsplx.xml で編集可能なデバッグレベル

*. UserDebugLevel では、スタートアップスクリプトからの出力は制御しません。この出力は、UserDebugLevel の値にかかわらず、常に記録されます。

†. ControlManagerDebug が有効になっている場合、ログは次のログファイルに格納されます。
/opt/TrendMicro/SProtectLinux/EntityMain.log

注意： 詳細デバッグオプションを選択すると、デバッグファイルのファイルサイズが大きくなります。トレンドマイクロでは、問題を記録する直前に詳細デバッグオプションを有効にして、記録が終了したらすぐにこのオプションを無効にすることをお勧めします。また、ログファイルは、ルートパーティション以外の

パーティションに格納することをお勧めします。

デバッグログを有効にする

tmsplx.xml と syslog.conf を編集して、ServerProtect のデバッグログ機能を有効にします。

デバッグログを有効にするには

1. デバッグログファイルのパス /path をリアルタイム検索の除外リストに追加します。
2. vi などのテキストエディタを使用して、次の設定ファイルを編集します。

警告： 設定ファイルに誤った変更を加えると、システムエラーなどの重大な問題が発生する可能性があります。設定ファイルを変更する前に、tmsplx.xml と syslog.conf のバックアップを作成してください。syslog.conf ファイルを変更したら、syslog サービスをすぐに再起動してから処理を続行してください。

   a. 各デバッグパラメータのデバッグレベル (UserDebugLevel と KernelDebugLevel) は、tmsplx.xml で定義します。
   b. デバッグログを保存するディレクトリのパスとファイル名を指定するには、Red Hat Enterprise Linux (以下、RHEL) 4 または RHEL5 プラットフォーム上の /etc/syslog.conf を編集します。SUSE Linux Enterprise Server (以下、SLES) 10 または SUSE Linux Enterprise Desktop (以下、SLED) 10 の場合は、詳細を 105 ページの「SUSE Linux に syslog-ng を設定する」で参照してください。

      例 :

- ServerProtect のすべてのユーザデバッグログを「/path/splxUserDebug.log」に記録するには、syslog.conf に次の行を追加します。

  local3.* /path/splxUserDebug.log

- ServerProtect のカーネルデバッグログを「/path/splxKernDebug.log」に記録するには、syslog.conf に次の行を追加します。

  kern.debug /path/splxKernDebug.log

3. 設定ファイルを保存して閉じます。
4. 次のコマンドで、PID を確認します。

   ps -ef | grep syslogd（RHEL4 または RHEL5）

   ps -ef | grep syslog-ng（SLES10 または SLED10）

5. 次のコマンドで、設定を再度読み込みます。

   kill -HUP <syslogd PID>（RHEL4 または RHEL5）

   kill -HUP <syslog-ng PID>（SLES10 または SLED10）

   注意： Linux ファイル操作エラーが生じないように、ServerProtect サービスを再起動する前に syslog を再起動します。

6. 次のコマンドで ServerProtect のサービスを再起動します。

   /etc/init.d/splx restart

デバッグログを無効にする

tmsplx.xml と syslog.conf を編集して、ServerProtect のデバッグログ機能を無効にします。

デバッグログを無効にするには

1. vi などのテキストエディタを使用して tmsplx.xml を編集し、各デバッグパラメータのデバッグレベルを変更します。

   警告： 設定ファイルに誤った変更を加えると、システムエラーなどの重大な問題が発生する可能性があります。設定ファイルを変更する前に、tmsplx.xml と syslog.conf のバックアップを作成してください。

2. <Esc> キーを押して、「save」と入力し、tmsplx.xml を閉じます。

3. お使いのプラットフォームに応じて、次のファイルのデバッグパスとファイル名を削除するかコメントアウトします。

   ```
   /etc/syslog.conf （RHEL4 または RHEL5）
   /etc/syslog-ng （SLES10 または SLED10）
   ```

4. 次のコマンドで ServerProtect のサービスを再起動します。

   ```
   /etc/init.d/splx restart
   ```

   注意： Linux ファイル操作エラーが生じないように、syslog を再起動する前に ServerProtect サービスを再起動します。

5. 次のコマンドで、PID を確認します。

   ```
   ps -ef | grep syslogd （RHEL4 または RHEL5）
   ps -ef | grep syslog-ng （SLES10 または SLED10）
   ```

6. 次のコマンドで、設定を再度読み込みます。

   ```
   kill -HUP <syslogd PID> （RHEL4 または RHEL5）
   kill -HUP <syslog-ng PID> （SLES10 または SLED10）
   etc/init.d/splx restart
   ```

7. デバッグログを有効にしたときにリアルタイム検索の除外リストに追加したパパス /path を除外リストから削除します。

logrotate を使用する

詳細デバッグオプションを数日または数週間有効にしておきたい場合には、logrotate を使用してログファイルを自動的にローテーションおよび圧縮してください。logrotate の詳細については、logrotate の man ページを参照してください。

logrotate を使用するには

1. vi などのテキストエディタを使用して、/etc/logrotate.d/syslog を開きます。

警告： 設定ファイルに誤った変更を加えると、システムエラーなどの重大な問題が発生する可能性があります。設定ファイルを変更する前に、tmsplx.xml のバックアップを作成してください。

2. 次の行を追加して、ログをローテーションします。

```
/var/log/messages /{path}/{splxlog} {
        sharedscripts
        postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid 2>
        /dev/null` 2> /dev/null || true
        endscript
}
```

3. syslog ファイルを保存して閉じます。

お問い合わせいただく前に

トレンドマイクロのテクニカルサポートにお問い合わせいただく前に、次のいずれかの方法で問題の解決方法が見つかるかどうかお試しいただくことをお勧めします。

- **ServerProtect のドキュメント：**製品付属の「クイックスタートガイド」やオンラインヘルプでは、ServerProtect に関する詳細な情報を提供しています。これらのドキュメントから問題の解決方法が見つかるかどうか確認してください。
- **トレンドマイクロのサポートサイト：**トレンドマイクロのサポートサイト (製品 Q&A) では、トレンドマイクロのすべての製品に関する最新情報を提供しています。また、サポートサイトから、製品に関するよくある質問とその回答を検索できます。

  トレンドマイクロの製品 Q&A サイトには、次の URL からアクセスできます。

  http://esupport.trendmicro.co.jp/

製品サポート情報

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

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

サポートサービスについて

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

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

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

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

製品 Q&A のご案内

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

中小 / 中堅企業のお客さま

http://esupport.trendmicro.co.jp/supportjp/smb/search.do

大企業のお客さま

http://esupport.trendmicro.co.jp/supportjp/enterprise/search.do

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

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

セキュリティ情報

セキュリティ情報の入手先

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

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

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

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

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

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

トレンドマイクロへのウイルス解析依頼

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

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

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

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

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

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

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

ウイルス解析サポートセンター「TrendLabs」

トレンドマイクロのウイルス解析サポートセンター「TrendLabs」(トレンドラボ) は、フィリピンセンターを本部として、米国、日本、台湾、ドイツ、アイルランド、中国の各国センターで構成されています。24 時間体制でウイルスの活動を監視するウイルス解析エンジニアを含む 800 名以上 (2006 年 1 月現在) のスタッフが、セキュリティに関する最新の情報を収集し、高品質なサービスとソリューションを迅速かつ効果的に世界各国のトレンドマイクロのパートナーとお客さまに提供しています。

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

ソフトウェアアップデートについて

製品リリース後に、トレンドマイクロはソフトウェアのアップデートを頻繁に行います。これによって、製品の性能を強化し、新機能を追加し、あるいは既知の問題に対応します。アップデートを発行する理由に応じて、アップデートの種類が異なります。

トレンドマイクロがリリースするアップデートの種類の概要は次のとおりです。

- HotFix：HotFix は、ユーザがレポートした個別の問題に対応する回避方法やソリューションです。HotFix は特定の問題に対応し、すべてのユーザにリリースされるものではありません。Windows の HotFix にはセットアッププログラムが含まれていますが、Windows 以外の HotFix には含まれていません (通常は、プログラムのデーモンを停止して、ファイルをコピーしてインストールディレクトリの該当ファイルを上書きしてから、デーモンを再起動します)。
- Security Patch：Security Patch は、主にセキュリティの問題に対応する HotFix で、すべてのユーザへ配信します。Windows の Security Patch には、セットアッププログラムが含まれていますが、Windows 以外の Patch には一般的にセットアップスクリプトが含まれています。

- Patch：Patch は、HotFix と Security Patch の集まりで、複数のプログラムの問題を解決します。トレンドマイクロは、定期的に利用可能な Patch を作成します。Windows の Patch には、セットアッププログラムが含まれていますが、Windows 以外の Patch には一般的にセットアップスクリプトが含まれています。
- Service Pack：Service Pack は、HotFix、Patch、機能強化が統合されたもので、製品のアップグレードと見なすこともできます。Windows と Windows 以外のどちらの Service Pack にも、セットアッププログラムとセットアップスクリプトが含まれています。

リリースされた HotFix を検索する場合は、トレンドマイクロの製品 Q&A を確認してください。

http://esupport.trendmicro.co.jp/

トレンドマイクロの Web サイトを定期的に調べて、Patch と Service Pack をダウンロードしてください。

http://www.trendmicro.co.jp/download/

すべてのリリースには、製品のインストール、配置、設定に必要な情報が記載されている Readme ファイルが含まれています。HotFix、Patch、Service Pack をインストールする前に、Readme ファイルをよく読んでください。

既知の問題

ServerProtect ソフトウェアの機能には既知の問題があり、一時的に回避方法が必要になる場合があります。既知の問題は、製品に付属の Readme に記載されています。トレンドマイクロ製品の Readme は、トレンドマイクロのアップデートセンターからも入手できます。

http://www.trendmicro.co.jp/download/

既存の問題は、テクニカルサポートの製品 Q&A で検索できます。

http://esupport.trendmicro.co.jp/

注意： Readme テキストを常に確認して、インストールや性能に影響する既知の問題に関する情報、さらに特定のリリースにおける新機能、システム要件、その他のヒントなどを確認することをお勧めします。

Trend Micro Control Manager について

Trend Micro Control Manager（以下、Control Manager）は、トレンドマイクロのゲートウェイ、メールサーバ、ファイルサーバ、デスクトップレベルのウイルス対策製品およびコンテンツセキュリティ製品、およびサードパーティ製品を管理するための集中管理コンソールです。Control Manager の Web ベースの管理コンソールにより、ネットワーク全体のウイルス対策およびコンテンツセキュリティ製品やサービスを 1ヵ所から監視することができます。

Control Manager を通して、システム管理者はウイルス感染やセキュリティ違反といった活動やウイルス検出ポイントを監視し把握することができます。また、アップデートコンポーネントを手動または事前予約によりダウンロードし、ネットワーク全体に配信することで、ウイルス対策を最新で一貫した状態に保つことができます。Control Manager では、製品を個別に、または製品グループ別に柔軟に設定できます。

本章は次の内容で構成されています。

Control Manager の基本機能

Control Manager は、組織のローカルエリアネットワークおよび広域ネットワーク上に配置されているウイルス対策 / コンテンツセキュリティ製品およびサービスを管理するための機能を提供します。

機能	説明
設定の一元化	製品ディレクトリと階層管理構造を通して、単一の管理コンソールからウイルスに対する処理やコンテンツセキュリティ対策を調整できます。 これにより、組織内で一貫したセキュリティポリシーを実施することができます。
大規模感染予防	大規模感染予防サービスにより、ネットワーク上でのウイルスの大規模感染を食い止めるための予防措置を実施します。
安全な通信インフラストラクチャ	Control Manager では、SSL (Secure Socket Layer) プロトコルに基づいた通信技術を採用しています。 指定されているセキュリティレベルに応じて、メッセージを暗号化、または認証付きで暗号化することができます。
設定およびコンポーネントダウンロードの保護	この機能により、管理コンソールへのアクセスとコンポーネントのダウンロードを保護できます。
タスク委任機能	システム管理者は Control Manager 管理コンソールの各ユーザに異なる権限を持つアカウントを与えることができます。 ユーザアカウントにより、ユーザが Control Manager システムで参照および実行できる内容が定義されます。アカウントの利用状況は、アクセスログによって確認することができます。
コマンド追跡	この機能により、実行されたコマンドを Control Manager 管理コンソールから監視することができます。 たとえば、ウイルスパターンファイルの更新や配信など、時間がかかるコマンドが正常に終了されたかどうかを確認したい場合に役立ちます。

表 A-1.　Control Manager には主に次の機能があります。

機能	説明
リアルタイム / オンデマンドでの製品管理	Trend Micro ServerProtect for Linux (以下、ServerProtect) をリアルタイムで管理します。 Control Manager は、管理コンソールで変更された設定を即座に ServerProtect に送信します。システム管理者は管理コンソールから手動検索を実行することができます。このような機能はウイルスの大規模感染発生時には欠かせないものです。
コンポーネントの集中管理	パターンファイル、スパムメール判定ルール、検索エンジン、およびその他のウイルス対策 / コンテンツセキュリティコンポーネントを一括して更新します。
レポートの一元化	包括的なログやレポートを使用して、ウイルス対策およびコンテンツセキュリティ製品のパフォーマンスの概要を調べることができます。 Control Manager を通じて管理下のすべての製品からログを収集できるため、製品別にログをチェックする必要がありません。

表 A-1. Control Manager には主に次の機能があります。

Trend Micro Management Communication Protocol について

Trend Micro Management Communication Protocol (以下、MCP) は、トレンドマイクロが提供する、管理下の製品用の次世代エージェントです。MCP は Trend Micro Management Infrastructure (以下、TMI) の代替として、Control Manager と ServerProtect 間の通信に使用されます。MCP には TMI と比べて、次のような利点があります。

- ネットワーク負荷とパッケージサイズの低減
- NAT およびファイアウォール環境のサポート
- HTTPS サポート
- 一方向および双方向の通信サポート
- シングルサインオン (SSO) サポート

- クラスタノードのサポート

ネットワーク負荷とパッケージサイズの低減

TMI では、XML ベースのアプリケーションプロトコルを使用します。XML は、プロトコルデザインにおいて一定の拡張性と柔軟性を提供しますが、XML を通信プロトコルのデータ形式の標準として使用すると次のような短所があります。

- バイナリ構造体などの他のデータ形式と比べて、XML の解析には、より多くのシステムリソースが必要となります (プログラムが、サーバまたはデバイスのリソースをより多く消費します)。
- XML では、情報の伝送に必要なエージェントの負荷が、他のデータ形式と比べて大幅に大きくなります。
- データが必要とするリソースが大きくなるため、データ処理のパフォーマンスが低下します。
- 他のデータ形式よりも、パケット伝送に時間がかかり、伝送速度が遅くなります。

上記のような問題に対して、MCP のデータ形式では問題解決の工夫が実装されています。MCP のデータ形式は BLOB (バイナリ) ストリームで、各項目は名前 ID、型、長さ、および値によって構成されます。この BLOB 形式には次の利点があります。

- **XML よりもデータ転送サイズが小さい** : データ型を使用することで、情報の格納に使用されるバイト数を制限できます。データ型には、整数型、符号なし整数型、ブール型、浮動小数点型があります。
- **解析速度がより速い** : 固定バイナリ形式を使用して、各データ項目を 1 つずつ簡単に解析できます。解析パフォーマンスは、XML よりも数倍速くなります。
- **設計の柔軟性の強化** : 各項目が名前 ID、型、長さ、および値から構成されることで、設計の柔軟性も考慮に入れられています。項目の順序は任意で、補助項目は必要な場合にのみ通信プロトコルに含めることができます。

MCP では、データ伝送にバイナリストリーム形式が採用されたことに加えて、圧縮 / 非圧縮に関係なく、異なる種類のデータを同一接続上にパックすることができます。このデータ伝送方式によって、ネットワーク帯域幅の節約が可能になると同時に、スケーラビリティが向上します。

NAT およびファイアウォール環境のサポート

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

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

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

NAT を使用した通信の手動設定

一方向または双方向の通信モデルを使用して NAT ネットワークにおける Control Manager の通信に対処するには、Agent.ini ファイルおよび Product.ini ファイルで設定を行い、ポート転送を設定する必要があります。

手順 1: Agent.ini ファイルで、パブリック IP アドレスを設定します。

/opt/TrendMicro/SProtectLinux フォルダの Agent.ini ファイルを開き、IPAddressList パラメータに NAT デバイスのパブリック IP アドレスを指定します。

手順 2: Product.ini ファイルで Control Manager のプロトコル名を設定します。

/opt/TrendMicro/SProtectLinux フォルダの Product.ini ファイルを開き、[ProtocolName] フィールドに、「http」または「https」と入力します。

注意：「https」と入力した場合は、port パラメータを「14943」に設定する必要があります。

手順 3: NAT デバイスにポート転送ルールを設定します。

NAT デバイスのポート 14942 (HTTP) または 14943 (HTTPS) で、トラフィックが NAT デバイスの背後にある ServerProtect サーバに転送されるように、NAT デバイスにポート転送ルールを設定する必要があります。ポート転送ルールは、次のとおりです。
パブリック IP (ポート : 14942/14943) => プライベート IP (ポート : 14942/14943)

HTTPS サポート

MCP 統合プロトコルでは、業界標準の通信プロトコル (HTTP/HTTPS) が採用されています。HTTP/HTTPS には TMI と比べて、次の利点があります。

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

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

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

一方向および双方向通信のサポート

MCP では、一方向および双方向の通信がサポートされます。

一方向通信

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

双方向通信

双方向通信は、一方向通信に代わる方法です。双方向通信では、一方向通信を基本としながら、サーバからの通知を受信するチャネルが追加されています。この追加チャネルも HTTP プロトコルに基づいています。双方向通信では、Control Manager エージェントによるサーバからのコマンド受信とその処理のリアルタイム性が向上します。Control Manager エージェント側には、CGI の要求を処理できる Web サーバまたは CGI 互換のプログラムが必要で、それによって Control Manager サーバからの通知が受信されます。

シングルサインオン (SSO) サポート

シングルサインオン (SSO) 機能を使用することにより、Control Manager にログオンするだけで、各トレンドマイクロ製品にログオンすることなくそれらの製品リソースにアクセスすることができます。

クラスタノードのサポート

さまざまな状況下で、管理者は特定の製品インスタンスを論理ユニットまたはクラスタとしてグループ化する場合があります。たとえば、クラスタ環境でインストールされている製品が、1 つのクラスタグループでインストールされているすべての製品インスタンスを表す場合などです。しかし、Control Manager サーバの観点から言うと、正式な登録プロセスを完了した各製品インスタンスは、独立した管理ユニットと見なされ、各管理ユニットは互いに区別されません。

Control Manager との通信に MCP を使用する製品では、Control Manager でクラスタノードがサポートされるようになりました。

Control Manager エージェント接続ステータス

ServerProtect のステータスを監視するために、Control Manager エージェントはスケジュールに基づいて Control Manager に対してポーリングを実行します。ポーリングは、ServerProtect のステータスを示したり、Control Manager からの ServerProtect へのコマンドを確認したりするために実行されます。ポーリングの実行後に、Control Manager の Web コンソールに ServerProtect のステータスが表示されます。つまり、ServerProtect のステータスは、ネットワークのステータスをリアルタイムに刻一刻と反映したものではありません。Control Manager により、各 ServerProtect コンピュータのステータスがバックグラウンドで順番に確認されます。ServerProtect コンピュータの接続ステータスが確認されないまま一定の時間が経過すると、Control Manager により、ServerProtect のステータスがオフラインに変更されます。

Control Manager による ServerProtect コンピュータのステータス判断の基準となるのは接続ステータスのみではありません。Control Manager では、次に示すことからも ServerProtect のステータスが判断されます。

- Control Manager は ServerProtect からログを受信します。Control Manager が、ServerProtect からいずれかの種類のログを正常に受信したということは、ServerProtect が正常に動作しているということを意味します。
- 双方向の通信モードでは、ServerProtect による保留中のコマンドの取得をトリガするために、Control Manager は積極的に通知メッセージを送信します。サーバが ServerProtect に正常に接続されるということは、ServerProtect が正常に動作していることも表しており、このイベントは 1 つの接続ステータスとみなされます。
- 一方向通信モードでは、Control Manager エージェントから Control Manager に対して定期的にクエリコマンドが送信されます。この定期的なクエリ動作は接続ステータスのような働きをし、Control Manager でも接続ステータスと同様の扱いを受けます。

Control Manager エージェント接続ステータスは、次の方法で実装されます。

- UDP: ServerProtect が UDP を使用してサーバにアクセスできる場合、これは最も単純で高速のソリューションです。ただし、この方法は NAT またはファイアウォール環境では機能しません。また、送信側のクライアントは、サーバが実際に要求を受信しているかどうかを確認できません。

- HTTP/HTTPS: NAT またはファイアウォール環境で機能できるようにするには、複雑な HTTP 接続を使用して、接続ステータスを送信します。

Control Manager は接続ステータスを報告するために、UDP メカニズムと HTTP/HTTPS メカニズムの両方をサポートしています。Control Manager サーバは、登録プロセスで ServerProtect コンピュータがどのモードを適用したかを認識します。モードを判断するために、両者の間で別のプロトコルのハンドシェイクが実行されます。

ServerProtect のステータスを示すために接続ステータスを送信すると同時に、追加データを Control Manager にアップロードすることもできます。通常、追加データには、コンソールに表示される、ServerProtect コンピュータのアクティビティ情報が含まれます。

スケジュールバーの使用

コミュニケータスケジュールを表示、設定するには、[コミュニケータスケジュール設定] 画面のスケジュールバーを使用します。スケジュールバーは 24 個のスロットから構成され、1 つのスロットは 1 時間を表します。

青いスロットは、コミュニケータから Control Manager サーバに情報が送信される稼動中のステータスまたは時間帯を表します。白いスロットは停止中の時間帯を表します。特定のスロットの設定を変更して、稼動中または停止中の時間帯を定義します。

コミュニケータスケジュールでは、最大で 3 つの停止期間を指定できます。

適切な接続ステータス設定について

コミュニケータ接続ステータスの実行間隔を指定するときは、コミュニケータのステータス情報の更新頻度と、システムリソースの消費の抑制の両方を考慮します。初期設定では、一般的な状況を前提にして間隔が設定されていますが、接続ステータス設定をカスタマイズする場合は次の点に注意してください。

接続ステータスの頻度	考慮する点
長い間隔の接続ステータス (60 分以上)	接続ステータスの実行間隔を長く設定すると、Control Manager 管理コンソールにコミュニケータステータスが反映されるまでの期間が長くなり、その間に新たに発生するイベントの数が多くなります。 たとえば、コミュニケータとの接続トラブルが発生して、その後解決された場合でも、ステータスが更新されるまでに時間がかかります。ステータスが「停止中」または「異常」と表示されていたとしても、実際にはコミュニケータとの通信が可能になっている場合があります。
短い間隔の接続ステータス (60 分未満)	接続ステータスの実行間隔を短く設定すると、Control Manager サーバの管理コンソールに、より最新のステータスが表示されるようになります。ただし、コミュニケータとの頻繁な通信によって帯域幅が多く消費されます。

表 A-2.　推奨される接続ステータス

Control Manager への ServerProtect の登録

ServerProtect はスタンドアロン製品であるため、ServerProtect をインストールしたコンピュータの Control Manager への登録は必須ではありません。ただし、Control Manager に登録することにより、この付録で先に説明した機能を利用することができます。ServerProtect の Web コンソールを使用して、すべての機能を管理します。ServerProtect コンピュータを Control Manager サーバに登録する前に、まず ServerProtect コンピュータと Control Manager サーバの両方が同じネットワークセグメントに属していることを確認する必要があります。

インストールプロセス時、または Web コンソールを使用して、ServerProtect コンピュータを Control Manager に登録できます。

Control Manager でステータスを確認するには

1. Control Manager の管理コンソールのメインメニューで [製品] をクリックします。
2. 左端のメニューでリストから [管理下の製品] を選択して [表示] をクリックします。
3. ServerProtect コンピュータが表示されるのを確認します。

Control Manager による ServerProtect コンピュータの管理

管理下の製品とは、製品ディレクトリ内の ServerProtect がインストールされているコンピュータ、ウイルス対策製品、コンテンツセキュリティ製品、またはサードパーティ製品を意味します。管理下の製品は、Control Manager の管理コンソールにアイコンで表示されます。これらのアイコンは、ServerProtect コンピュータ、その他のトレンドマイクロのウイルス対策製品、コンテンツセキュリティ製品、およびサードパーティ製品を表します。

管理下の製品は、製品ディレクトリを通して、製品単位またはグループ単位で管理します。製品ディレクトリ構成をカスタマイズするときには、ディレクトリ管理を使用します。

製品ディレクトリについて

製品ディレクトリは、管理下の製品を論理的にグループ化したものです。次のような影響があるため、製品ディレクトリの構造を慎重に計画する必要があります。

- **ユーザのアクセス権** : ユーザアカウントの作成時に、対象のユーザがアクセスできる製品ディレクトリの項目を指定するよう求められます。ユーザのアクセス権を割り当てることができるのは製品ディレクトリの 1 つの項目 (フォルダまたは製品) に対してのみです。たとえば、root ディレクトリを選択すると、製品ディレクトリ全体へのアクセス権を付与することになります。一方、特定の ServerProtect コンピュータを選択した場合には、その製品へのアクセス権だけが付与されます。
- **配信計画** : Control Manager は、配信計画に基づいて、ウイルス対策製品にパターンファイル、検索エンジン、スパムメール判定ルール、およびプログラムのアップデートを配信します。配信計画は、個々の製品ではなく製品グループに対して配信されます。したがって、製品ディレクトリを適切に構成することで、配信先の指定を簡略化することができます。
- **大規模感染予防ポリシーとダメージクリーンナップテンプレートの配信** : 大規模感染予防ポリシーおよびダメージクリーンナップサービスの配信は、大規模感染予防ポリシーとクリーンナップタスクの効率的な配信のための配信計画によって異なります。

次の製品ディレクトリの例で示すように、管理下の製品では、登録済みのウイルス対策製品とコンテンツセキュリティ製品が識別され、接続ステータスが提供されます。

製品ディレクトリで使用されるアイコン

製品ディレクトリのツリー	アイコン	説明
		[新規エンティティ] フォルダまたはユーザ定義のフォルダの名前
		InterScan eManager
		ウイルスバスター コーポレートエディション
		ServerProtect インフォメーションサーバ
		ServerProtect ドメイン
		ServerProtect for Windows (一般サーバ)
		ServerProtect for NetWare (一般サーバ)
		InterScan Messaging Security Suite
		InterScan Web Security Suite
		InterScan VirusWall for Windows
		InterScan VirusWall for UNIX
		InterScan for Microsoft Exchange
		InterScan for Lotus Notes
		Network VirusWall
		
		
		NetScreen Global PRO ファイアウォール
		管理下の製品接続ステータスのアイコン

表 A-3.　管理下の製品を表すアイコン

ディレクトリ管理機能を使用して、製品ディレクトリを配置します。ServerProtect コンピュータの保護タイプと Control Manager システムの管理モデルに従い、製品の種類を表すフォルダ名を使用して ServerProtect コンピュータをグループ化します。たとえば、ファイルサーバ管理者にアクセス権を付与して、「Server protection」フォルダを設定できるようにします。

ServerProtect の初期設定フォルダへのアクセス

新しく登録された ServerProtect コンピュータは、エージェントのインストール時に指定したユーザアカウントに従って、通常は「新規エンティティ」フォルダに格納されます。Control Manager では、エージェントのインストール時に指定したユーザアカウントの権限によって、ServerProtect コンピュータの初期設定フォルダが指定されます。ただし、TVCS エージェントフォルダの TVCS エージェントによって処理される管理下の製品は別のフォルダに格納されます。

アカウントがアクセス権を持つフォルダ、およびその結果としての管理下の製品の初期設定の配置場所との関係を次に示します。

アカウントがアクセス権を持つフォルダ	管理下の製品の初期設定の配置場所
root フォルダ	新規エンティティ
Server protection フォルダ	Server protection
ウイルスバスター Corp.	新規エンティティ

ユーザアカウントに特定の管理下の製品へのアクセスを設定すると、そのアカウントは新しく登録された管理下の製品にはアクセスできなくなります。

表 A-4.　管理下の製品とユーザのアクセス権の関係

製品ディレクトリへのアクセス

製品ディレクトリを使用して、Control Manager サーバに登録されている ServerProtect コンピュータを管理できます。

注意： 製品ディレクトリのフォルダの表示やフォルダへのアクセスは、管理コンソールへのアクセスに使用するアカウントの種類とフォルダへのアクセス権によって異なります。

製品ディレクトリにアクセスするには

1. 上部のメニューで [製品] を選択します。
2. 左側のメニューでリストから [管理下の製品] を選択し、[表示] をクリックします。

製品ディレクトリによる新規コンポーネントの手動配信

手動配信を使用すると、ServerProtect コンピュータおよびその他の管理下の製品のウイルスパターンファイル、スパムメール判定ルール、および検索エンジンを必要なときに即座にアップデートできます。この機能は、ウイルス感染が急速に拡大している時に特に役立ちます。

特定またはグループ単位の ServerProtect コンピュータまたは管理下の製品にアップデートを配信する前に、新規コンポーネントをダウンロードします。

製品ディレクトリを使用して新規コンポーネントを手動配信するには

1. 上部のメニューで [製品] を選択します。
2. 左側のメニューでリストから [管理下の製品] を選択し、[表示] をクリックします。
3. 左側のメニューで、目的のフォルダまたは ServerProtect を選択します。

4. 右側の画面で [タスク] タブをクリックします。
5. [タスク] リストから実行する処理を選択します。
6. [次へ] をクリックします。
7. [配信開始] をクリックして、新規コンポーネントの手動配信を開始します。
8. [コマンド追跡] を使用して、進行状況を確認してください。
9. [配信開始] タスクの詳細を表示するには、[コマンド詳細] リンクをクリックします。

ServerProtect のステータス概要の表示

[ステータス概要] 画面には、製品ディレクトリツリーにあるすべての ServerProtect およびその他の管理下の製品について、ウイルス対策概要、コンテンツ対策概要、および Web セキュリティ対策概要が表示されます。

ServerProtect のステータス概要を表示するには、次の 2 とおりの方法があります。

- [ホーム] 画面から
- 製品ディレクトリから

ホームページからアクセスするには

- Control Manager 管理コンソールを起動した際の初期画面では、[ホーム] 画面に Control Manager システム全体の概要情報が表示されます。この内容は、製品ディレクトリの root フォルダからアクセスする [製品ステータス] タブの内容と同じです。

製品ディレクトリからアクセスするには

1. 上部のメニューで [製品] を選択します。

2. 左側のメニューで、表示するフォルダまたは ServerProtect を選択します。

   - ServerProtect コンピュータまたは管理下の製品をクリックすると、その ServerProtect コンピュータまたは管理下の製品の概要が [製品ステータス] タブに表示されます。
   - [root] フォルダ、[新規エンティティ] フォルダ、またはその他のユーザ定義フォルダをクリックすると、[製品ステータス] タブにウイルス対策、コンテンツ対策、および Web セキュリティ対策の概要が表示されます。

注意： 初期設定では、最後に問い合わせた日付からさかのぼって 1 週間分の情報がステータス概要に表示されます。この範囲を変更するには、[レポート期間] で [今日]、[過去 7 日間]、[過去 14 日間]、[過去 30 日間] のいずれかを選択します。

ServerProtect と管理下の製品の設定

管理下の製品の種類とエージェントのバージョンによって次のような違いがあります。

- デバイスまたは製品を個別に設定できる場合とフォルダごとにグループで設定できる場合があります。

  グループ設定はフォルダの [設定] タブを使用して実行します。

注意： グループ設定は、1 つのグループに属する ServerProtect コンピュータすべてに同一の設定を適用する場合に実行します。グループ内の一部の製品に同一の設定を適用する場合は、対象のデバイスまたは管理下の製品をショートカットに追加して、その他の管理下の製品の設定が上書きされないようにします。

- [設定] タブには、製品の Web コンソールまたは Control Manager によって生成されたコンソールが表示されます。

管理下の製品を設定するには

1. 上部のメニューで [製品] を選択します。
2. 左側のメニューでリストから [管理下の製品] を選択し、[表示] をクリックします。

3. 左側のメニューで、目的の ServerProtect コンピュータ、管理下の製品または フォルダを選択します。

4. 右側の画面で、[設定] タブをクリックします。

注意： 手順 4 はフォルダの [設定] タブを使用している場合に必要です。

5. [製品] リストボックスから、設定する製品を選択します。

6. [設定] リストボックスから、製品の設定メニューを選択します。

7. [次へ] をクリックします。ServerProtect または管理下の製品の Web ベースの コンソールまたは Control Manager によって生成されたコンソールが表示されます。

ServerProtect と管理下の製品に対するタスクの実行

[タスク] タブを使用すると、グループ単位または特定の ServerProtect コンピュータまたは管理下の製品に対し、有効なタスクを実行できます。ServerProtect コンピュータでは、次のタスクを実行できます。

- 複製の設定
- エンジンの配信
- パターンファイル / クリーンナップテンプレートの配信
- リアルタイム検索の有効化 / 無効化
- 手動検索 (Scan Now) の開始 / 停止
- すべてのコマンドの追跡

最新ではないコンポーネントを使用している ServerProtect には、最新のパターンファイルまたは検索エンジンを配信します。これを適切に実行するには、Control Manager サーバに、トレンドマイクロのアップデートサーバからの最新のコンポーネントが実装されている必要があります。Control Manager サーバに最新のコンポーネントが確実に実装されるようにするには、手動ダウンロードを実行します。

ServerProtect に対してタスクを実行するには

1. 製品ディレクトリにアクセスします。
2. 左側のメニューで、目的の ServerProtect またはフォルダを選択します。
3. 右側の画面で [タスク] タブをクリックします。
4. [タスク] リストからタスクを選択します。
5. [次へ] をクリックします。
6. [コマンド追跡] を使用して、進行状況を確認してください。応答画面で [コマンド詳細] リンクをクリックすると、コマンド情報が表示されます。

ServerProtect コンピュータと管理下の製品ログのクエリと表示

[ログ] タブを使用すると、グループ単位または特定の ServerProtect コンピュータのログにクエリを実行してログを表示できます。

ServerProtect のログにクエリを実行してログを表示するには

1. 製品ディレクトリにアクセスします。
2. 左側のメニューで、目的の ServerProtect またはフォルダを選択します。
3. 右側の画面で [ログ] タブをクリックします。

4. クライアントのログの種類を選択します。

イベントログ

a. 次の検索項目を指定します。

検索項目	説明
重大度	表示可能な情報の重大度を表します。[重大]、[警告]、[情報]、[エラー]、[不明] のオプションがあります。必要な項目のチェックボックスをオンにします。
イベント	イベントを表します。[すべて]、[ウイルス大規模感染]、[モジュールアップデート]、[サービス開始]、[サービス停止]、[セキュリティ違反]、[脆弱性に対する攻撃の兆候] のオプションがあります。
製品	フォルダを選択した場合は、そのフォルダに属する管理下の製品のリストが表示されます。すべての製品に関する情報を表示するには、[すべて] を選択します。そうでない場合は、特定の管理下の製品のログにクエリを実行します。
対象期間	すべてのログを表示するか、特定の期間内に管理下の製品によって生成されたログだけを表示するかを選択します。特定期間内のログだけを表示する場合は、過去 24 時間、今日、過去 7 日間、過去 14 日間、過去 30 日間、または指定する期間のログを指定できます。 [指定する期間] を選択した場合は、[開始日] と [終了日] で適切な年月日を選択します。
ソートの種類	日時、コンピュータ名、製品、イベント、または重大度を基準に結果を並べ替えます。
表示順序	結果を昇順または降順に並べ替えます。

表 A-5. イベントログの検索項目

b. [ログ表示] をクリックして、クエリを開始し、クエリ結果を表示します。

セキュリティログ

a. [すべてのウイルス / スパイウェアログイベント]、または特定のセキュリティログの種類を選択して、[クエリ] をクリックします。

b. 次の検索項目を指定します。

検索項目	説明
対象期間	すべてのログを表示するか、特定の期間内に管理下の製品によって生成されたログだけを表示するかを選択します。特定期間内のログだけを表示する場合は、過去 24 時間、今日、過去 7 日間、過去 14 日間、過去 30 日間、または指定する期間のログを指定できます。 [指定する期間] を選択した場合は、[開始日] と [終了日] で適切な年月日を選択します。
ソートの種類	日時、コンピュータ名、製品、イベント、または重大度を基準に結果を並べ替えます。
表示順序	結果を昇順または降順に並べ替えます。

表 A-6. セキュリティログの検索項目

c. [ログ表示] をクリックして、クエリを開始します。

注意： eManager 製品では、コンテンツセキュリティ違反はウイルスログではなく、セキュリティログに記録されます。

5. [クエリ結果] 画面に結果が表形式で表示されます。
6. 結果の表の [生成日時] 列には、Control Manager サーバの時刻が表示されます。

製品ディレクトリから削除された ServerProtect コンピュータの再登録

Control Manager では、次のような場合に、ServerProtect コンピュータが製品ディレクトリから削除される可能性があります。

- Control Manager サーバを再インストールし、[既存のレコードを削除して、新しいデータベースを作成する] オプションを選択した場合

  このオプションを選択すると、既存のデータベース名を使用して新規のデータベースが作成されます。

- 破損した Control Manager データベースを、同名の別のデータベースで置き換えた場合
- ディレクトリ管理を使用して、ServerProtect コンピュータを誤って削除した場合

ServerProtect コンピュータに関するレコードが Control Manager サーバ側で失われても、登録先サーバの情報はその製品のエージェント側で保持されています。製品のエージェントは、8 時間後またはサービスの再起動時に、自動的にエージェント自身を再登録します。

製品ディレクトリから削除された ServerProtect コンピュータを再登録するには、その ServerProtect コンピュータを再起動します。

ServerProtect コンピュータ、製品ディレクトリフォルダ、またはその他のコンピュータの検索

次の操作は、[検索] ボタンを使用して簡単に実行できます。

- ServerProtect コンピュータを個別またはグループ単位でショートカットに追加
- 製品ディレクトリ内にある特定の ServerProtect コンピュータを検索

フォルダまたは ServerProtect コンピュータを検索するには

1. 製品ディレクトリにアクセスします。
2. 左側のメニューで [検索] をクリックします。
3. 右側の画面で、次の検索項目を指定します。

検索項目	説明
管理下の製品の検索基準	リストボックスから検索対象を選択します。検索は、管理下の製品またはコミュニケータの名前、フォルダ名、またはコンピュータ名に基づいて実行できます。

表 A-7. 検索項目

検索項目	説明
キーワード	検索対象の名前を指定します。 大文字と小文字を区別して検索するには、[大文字と小文字の区別] チェックボックスをオンにします。
管理下の製品ステータス	検索するコミュニケータ、または管理下の製品の適切な接続ステータスを指定します。 [すべて]、[稼動中]、[停止中]、[異常]、[製品稼動中]、および [製品停止中] のオプションがあります。接続ステータスに関係なくすべてのオブジェクトを検索する場合は [すべて] を選択します。
製品	リストから適切な管理下の製品を選択します。すべての製品を検索する場合は [すべて] を選択します。

表 A-7.　検索項目

4. [検索開始] をクリックして検索を開始します。
5. 検索結果が表形式で表示されます。ショートカットサブフォルダを作成し、そこで検索結果をグループ化することもできます。

製品ディレクトリの表示の更新

製品ディレクトリの表示を更新するには

- 製品ディレクトリで、左側のメニューの右上隅にある [更新] アイコンをクリックします。

ディレクトリ管理について

Control Manager に登録すると、ServerProtect はまず製品ディレクトリの初期設定フォルダの下に表示されます。

管理モデルの要件に合わせて製品ディレクトリの構成をカスタマイズするには、ディレクトリ管理を使用します。たとえば、製品の場所で分類したり、メッセージングセキュリティ対策製品、Web セキュリティ対策製品、ファイルサーバ対策製品などの種類別に分類したりできます。

ディレクトリ管理を使用すると、フォルダを作成、変更、削除したり、フォルダ間で ServerProtect コンピュータを移動したりできます。ただし、新規エンティティフォルダの削除と名前変更はできません。

各フォルダに属する ServerProtect コンピュータを慎重に構成します。フォルダと ServerProtect コンピュータの構造を計画して実装する際には、次の点を考慮してください。

- 製品ディレクトリ
- ユーザアカウント
- 配信計画

ServerProtect コンピュータは、配置場所別、管理部門別、製品別などで分類してグループ化します。次の表では、ディレクトリにある ServerProtect コンピュータまたはフォルダへのアクセスに使用される各種アクセス権と組み合わせる場合に、推奨されるグループ化の種類と、その利点と欠点を示しています。

グループ化の種類	長所	短所
配置場所別または管理部門別	構造が明確	同一製品に対するグループ設定がない
製品の種類別	グループ設定とステータスが使用できる	アクセス権が一致しないことがある
上記の組み合わせ	グループ設定とアクセス権の管理が可能	構造が複雑になり、管理が難しいことがある

表 A-8.　管理下の製品のグループ化の比較

ディレクトリ管理のオプションの使用

ディレクトリ管理には、[新規フォルダ]、[削除]、[名前の変更]、[元に戻す]、[やり直し]、[切り取り]、[貼り付け]、および [リセット] の 8 つのオプションが用意されています。

これらのオプションを使用して、Control Manager システム内の ServerProtect を処理して構成します。

ディレクトリ管理でオプションを使用して変更を適用するには

- フォルダまたは ServerProtect コンピュータを右クリックすると、ポップアップメニューが開き、実行可能な処理のリストが表示されます。
- フォルダに属する ServerProtect コンピュータを表示するには、[+] またはそのフォルダをクリックします。
- フォルダの名前を変更する場合は、ポップアップメニューから [名前の変更] をクリックして名前を入力し、<Enter> キーを押すか、任意の場所をクリックします。
- 変更を適用して、ディレクトリ管理の構成を更新するには、[保存] をクリックします。
- まだ保存していない変更を破棄するには、[リセット] をクリックします。

ディレクトリ管理へのアクセス

ディレクトリ管理を使用すると、ServerProtect コンピュータをグループ化できます。

ディレクトリ管理にアクセスするには

1. 製品ディレクトリにアクセスします。
2. 左側のメニューで [ディレクトリ管理] を選択します。

フォルダの作成

Control Manager システムの管理モデルに応じて、ServerProtect コンピュータを異なるフォルダにグループ分けします。

フォルダを作成するには

1. ディレクトリ管理にアクセスします。
2. 右側の画面で、新規フォルダを作成する場所を右クリックします。はじめてサブフォルダを作成する場合は、root フォルダを右クリックします。ポップアップメニューが開きます。
3. ポップアップメニューから [新規フォルダ] を選択します。メインフォルダの下に新規サブフォルダが作成されます。
4. 新規フォルダの名前を入力するか、初期設定の名前を使用して、<Enter> キーを押します。
5. [保存] をクリックします。

フォルダまたは ServerProtect コンピュータの名前変更

フォルダまたは ServerProtect コンピュータの名前を変更するには

1. ディレクトリ管理にアクセスします。
2. 右側の画面で、名前を変更するフォルダまたは ServerProtect コンピュータを右クリックし、ポップアップメニューから [名前の変更] をクリックします。フォルダまたは ServerProtect の名前が編集可能になります。
3. 新規フォルダの名前を入力するか、初期設定の名前を使用して、<Enter> キーを押します。
4. [保存] をクリックします。

注意： ServerProtect コンピュータの名前を変更すると、Control Manager データベース内に保存されている名前だけが変更されます。製品自体に影響はありません。

フォルダまたは ServerProtect コンピュータの移動

フォルダまたは ServerProtect コンピュータを別の場所に移動するには

1. ディレクトリ管理にアクセスします。
2. 右側の画面で、移動するフォルダまたは ServerProtect コンピュータを選択します。
3. 次のいずれかを実行します。
   - フォルダまたは ServerProtect コンピュータを、移動先にドラッグアンドドロップします。
   - フォルダまたは ServerProtect コンピュータを切り取り、移動先に貼り付けます。
4. [保存] をクリックします。

ユーザ定義フォルダの削除

ディレクトリ管理内のユーザ定義フォルダを削除するときは注意が必要です。ServerProtect コンピュータを誤って削除し、ServerProtect サーバからその製品を登録解除してしまう可能性があります。

ユーザ定義フォルダを削除するには

1. ディレクトリ管理にアクセスします。
2. 右側の画面で、削除するフォルダを右クリックし、ポップアップメニューから [削除] をクリックします。
3. [保存] をクリックします。

注意 : 「新規エンティティフォルダ」を削除することはできません。

ショートカットについて

ショートカットには、ServerProtect へのショートカットが作成されます。ショートカットを使用して、製品ディレクトリの構成を変更せずに特定の製品に対する作業を集中的に実行できます。ショートカット機能の最も効果的な利用法として、期限切れのコンポーネントを持つ製品をショートカットに追加し、最新コンポーネントを一括して配信する例があります。

ショートカット機能を使用する際は、次の点に注意してください。

- ServerProtect へのショートカットはすべて、管理コンソールからログオフしたときに Control Manager によって削除されます。
- ショートカットに追加できる ServerProtect は、製品ディレクトリに表示されている ServerProtect だけです。アクセスが許可されていない ServerProtect のショートカットを作成することはできません。

ショートカットとは

ショートカット内の ServerProtect コンピュータは、製品ディレクトリ内の ServerProtect コンピュータと同じように扱うことができます。ショートカット内のフォルダや ServerProtect コンピュータを選択すると、ディレクトリと同様、右側の画面に [ステータス]、[設定]、[タスク]、[ログ] のタブが表示されます。ただし、ServerProtect に対して実行できる処理は、ユーザアカウントのアクセス権に基づいて、Control Manager によって決められます。

ショートカットは次の目的に使用できます。

- フォルダレベルのアクセス権を使用して ServerProtect コンピュータのグループにコマンドを発行します。
- 特定の ServerProtect コンピュータを選択し、アクセス可能な製品ディレクトリのタブを使用して処理を実行します。

ショートカットへのアクセス

ショートカットを使用すると、ServerProtect コンピュータへのアクセスを容易にすることができます。

ショートカットにアクセスするには

1. 製品ディレクトリにアクセスします。
2. 左側のメニューで [ショートカット] をクリックします。

ショートカットへの ServerProtect コンピュータの追加

ショートカットに ServerProtect コンピュータを追加するには、次の 3 つの方法があります。

- 検索結果から追加
- 製品ディレクトリから追加
- [ステータス概要] 画面に基づいて、期限切れのコンポーネントを持つ ServerProtect コンピュータを追加

3 つ目の方法を使用して、複数の ServerProtect コンピュータを一度にショートカットに追加することをお勧めします。[ステータス概要] 画面には、期限切れのコンポーネントを使用している ServerProtect コンピュータに関する情報が表示されます。これにより、異なるフォルダグループに属する複数の ServerProtect コンピュータに対し、まとめて簡単に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を実行できるようになります。

注意： ショートカットに ServerProtect コンピュータを追加する操作では、期限切れのコンポーネントを持つ ServerProtect コンピュータが 1 ヵ所に集められるというだけで、自動配信が開始されるわけではありません。

検索結果から追加するには

1. 上部のメニューで [製品] を選択します。
2. 左側のメニューで [検索] をクリックします。
3. 右側の画面で、ServerProtect コンピュータまたはフォルダを検索します。
4. ServerProtect のショートカットを格納するショートカットサブフォルダの名前を [検索結果用ショートカットサブフォルダ] フィールドに指定します。

注意： 手順 4 は任意です。ショートカットフォルダの下にさらにフォルダ階層を作成するには、[検索結果用ショートカットサブフォルダ] フィールドに「¥{ フォルダ名レベル 1}¥{ サブフォルダ名レベル 2}」の形式で名前を指定します。たとえば、「Pattern(1)¥VB_Corp」と指定した場合、ショートカットフォルダの構造は次のようになります。

---

5. [追加] をクリックします。検索結果から ServerProtect コンピュータがショートカットに追加されます。

製品ディレクトリから追加するには

1. 製品ディレクトリにアクセスします。
2. 左側のメニューで、ショートカットに追加する ServerProtect コンピュータを選択します。
3. キーボードの <+> (プラス) キーを押します。

[ステータス概要] 画面に基づいて、期限切れのコンポーネントを持つ ServerProtect コンピュータを追加するには

1. 製品ディレクトリにアクセスします。
2. 左側のメニューで、目的の製品ディレクトリフォルダを選択します。
3. 右側の画面で、[製品ステータス] タブをクリックします。
4. [コンポーネントのステータス] 表で、期限切れのコンポーネントを使用している ServerProtect コンピュータの数を示す数値のリンクを 1 つクリックします。クリックしたリンクに応じて [パターンファイルのステータス (期限切れ)]、[検索エンジンのステータス (期限切れ)]、または [スパムメール判定ルールのステータス (期限切れ)] 画面が表示され、その画面に、コンピュータ名、製品名、製品バージョン、および期限切れコンポーネントバージョンが表示されます。
5. ステータスの画面で [ショートカットに追加] をクリックします。追加元の画面名と同じ名前のフォルダを使用して、ServerProtect コンピュータがショートカットに配置されます。たとえば、[検索エンジンのステータス (期限切れ)] 画面から追加された ServerProtect コンピュータは、[検索エンジンのステータス (期限切れ)] フォルダに配置されます。

   注意 : [ショートカットに追加] をクリックしたときに追加されるのは、ステータスの画面に表示されている ServerProtect コンピュータだけです。ServerProtect コンピュータのリストが複数ページにわたる場合は、すべてのページで [ショートカットに追加] をクリックして、期限切れコンポーネントを持つ ServerProtect コンピュータをすべて追加してください。

6. [戻る] をクリックして、[ステータス概要] 画面に戻り、次の期限切れコンポーネントに進みます。期限切れのコンポーネントを使用している ServerProtect コンピュータすべてがショートカットに追加されるまで、この操作を繰り返します。

ショートカットからの ServerProtect コンピュータの削除

ショートカットから ServerProtect コンピュータを削除するには

1. 製品ディレクトリにアクセスします。
2. 左側のメニューで [ショートカット] をクリックして展開します。
3. ショートカットリスト内の有効な ServerProtect コンピュータから、削除するフォルダまたは ServerProtect のショートカットを選択します。
4. キーボードの <-> (マイナス) キーを押します。

注意： 管理コンソールからログオフすると、Control Manager によってショートカットにある ServerProtect のショートカットが削除されます。

ショートカットから ServerProtect コンピュータを削除しても、ウイルス対策 / コンテンツセキュリティ製品のサービスが停止したり、Control Manager エージェントが Control Manager サーバからアンインストールされたりすることはありません。

Control Manager からの新しいコンポーネントのダウンロードと配信

アップデート管理は、Control Manager システム上でウイルス対策コンポーネントとコンテンツセキュリティコンポーネントをアップデートするための機能をまとめたものです。トレンドマイクロでは、最新のウイルスおよび不正コードの脅威に対して保護された状態を保てるように、ウイルス対策およびコンテンツセキュリティコンポーネントのアップデートをお勧めしています。初期設定では、Control Manager サーバに管理下の製品が登録されていない場合でも、Control Manager でウイルスパターンファイル、ダメージクリーンナップテンプレート、および脆弱性診断パターンファイルがダウンロードされます。

アップデートできるのは、次のコンポーネントです。ここでは、頻繁にアップデートすることが推奨されるものから記載してあります。

- **パターンファイル** - ウイルスおよびスパイウェア / グレーウェア検索パターンファイル、パターンファイルリリース履歴、ネットワークウイルスおよびスパイウェア / グレーウェアパターンファイル

注意： コンポーネントをアップデートできるのは、製品のアクティベーションが完了している場合だけです。詳細については、Control Manager オンラインヘルプの「製品のアクティベーションについて」を参照してください。

Control Manager システムのトラフィックを最小限に抑えるには、管理下の製品に適用する必要がないコンポーネントのダウンロードを無効にしてください。

アップデート管理について

アップデート管理は、Control Manager のネットワーク上のウイルス対策およびコンテンツセキュリティコンポーネントをアップデートするための機能です。

Control Manager のネットワークのアップデート作業は、次の 2 つの手順に分かれます。

- コンポーネントのダウンロード - 手動または予約によって実行できます。
- コンポーネントの配信 - 手動または予約によって実行します。

手動ダウンロードについて

Control Manager を最初にインストールするとき、ネットワークが攻撃されているとき、または新しいコンポーネントをネットワークに配信する前にテストするときに、最新コンポーネントを手動でダウンロードします。

コンポーネントの手動ダウンロード

トレンドマイクロの推奨する手動ダウンロードの構成方法を、次に説明します。コンポーネントを手動でダウンロードするには、複数の手順を実行する必要があります。

ヒント：配信計画およびプロキシ設定を既に設定してある場合は、手順 1 および 2 は無視してください。

手順 1: コンポーネントの配信計画の設定

手順 2: プロキシの設定 (プロキシサーバを使用する場合)

手順 3: アップデートするコンポーネントの選択

手順 4: ダウンロード方法の設定

手順 5: 自動配信の設定

手順 6: 手動ダウンロードの完了

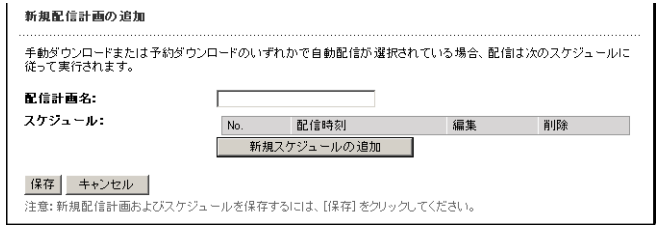
手動でコンポーネントをダウンロードするには

手順 1: コンポーネントの配信計画の設定

1. メインメニューで [運用管理] をクリックします。

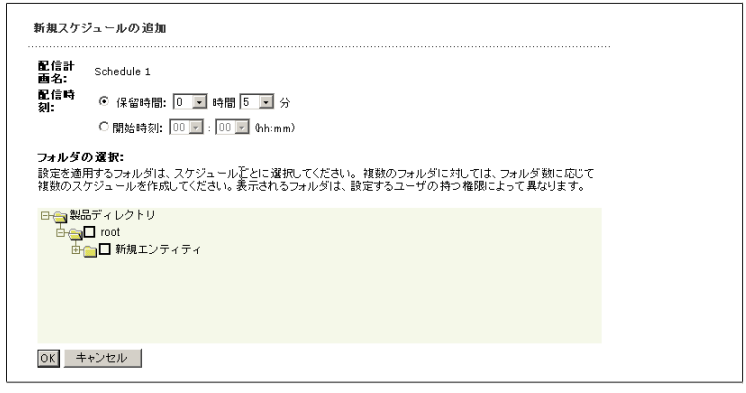
2. 左側のメニューの [アップデート管理] で、[配信計画] をクリックします。[配信計画] 画面が表示されます。

3. 右側の画面で、[新規配信計画の追加] をクリックします。



4. [新規配信計画の追加] 画面で、[配信計画名] フィールドに配信計画名を入力します。

5. [新規スケジュールの追加] をクリックして、配信計画の詳細を入力します。[新規スケジュールの追加] 画面が表示されます。



6. [新規スケジュールの追加] 画面で、次のいずれかのオプションを選択して、配信スケジュールを選びます。

   - **保留時間** — Control Manager で最新コンポーネントをダウンロードした後、指定した間隔に従って、配信を遅らせます。

     メニューを使用して、時間または分単位で保留期間を指定します。

   - **開始時刻** — 指定した時刻に配信を実行します。

     メニューを使用して、時間または分単位で配信時刻を指定します。

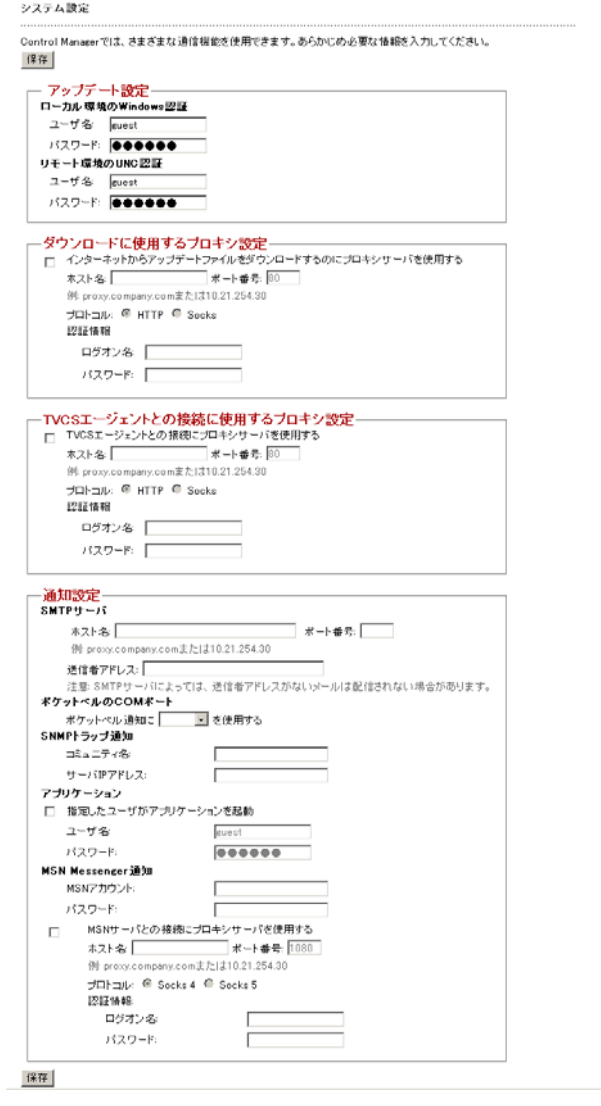
7. スケジュールを適用する製品ディレクトリのフォルダを選択します。選択したフォルダに含まれるすべての製品に対して、スケジュールが適用されます。

8. [OK] をクリックします。

9. [保存] をクリックして、新規配信計画を適用します。

手順 2: プロキシの設定 (プロキシサーバを使用する場合)

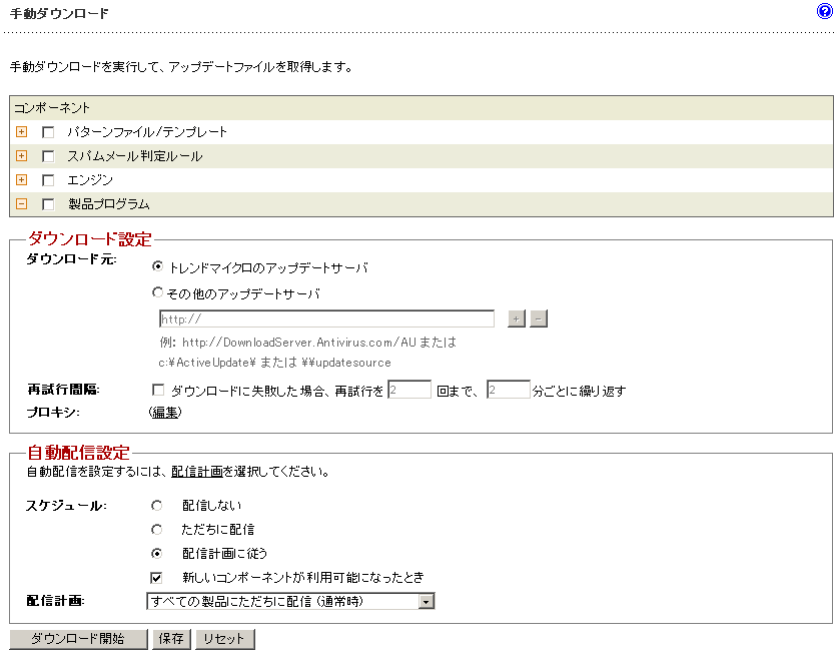
1. [運用管理]→[システム設定] の順に選択します。[システム設定] 画面が表示されます。



2. [ダウンロードに使用するプロキシ設定] で、[インターネットからアップデートファイルをダウンロードするのにプロキシサーバを使用する] チェックボックスをオンにします。
3. [ホスト名] フィールドに、サーバのホスト名または IP アドレスを入力します。
4. [ポート番号] フィールドに、ポート番号を入力します。
5. プロトコルを選択します。
   - HTTPS
   - SOCKS
6. サーバで認証が必要な場合は、ログオン名とパスワードを入力します。
7. [保存] をクリックします。

手順 3: アップデートするコンポーネントの選択

1. [運用管理]→[アップデート管理]→[手動ダウンロード] の順に選択します。[手動ダウンロード] 画面が表示されます。



2. [コンポーネント] で、ダウンロードするコンポーネントを選択します。

   a. 各コンポーネントグループのコンポーネントリストを展開するには [+] アイコンをクリックします。

   b. ダウンロードするコンポーネントを選択します。

手順 4: ダウンロード方法の設定

1. ダウンロード元を選択します。

   - **トレンドマイクロのアップデートサーバ** - トレンドマイクロのアップデートサーバからコンポーネントをダウンロードします。
   - **その他のアップデートサーバ** - 指定のフィールドにダウンロード元の URL を入力します。

     [その他のアップデートサーバ] を選択すると、複数のダウンロード元を指定できます。ダウンロード元を追加するには、[+] アイコンをクリックします。ダウンロード元は 5 つまで設定できます。

2. [再試行間隔] を選択し、コンポーネントのダウンロードを再試行する回数と間隔を指定します。

ヒント： この画面で [編集] または [配信計画] をクリックする前に、[保存] をクリックしてください。[保存] をクリックしないと、設定が失われてしまいます。

---

3. ネットワーク上で HTTP プロキシサーバを使用している場合 (Control Manager サーバがインターネットに直接アクセスできない場合) は、[編集] をクリックして、[システム設定] 画面でプロキシを設定します。

手順 5: 自動配信の設定

1. [スケジュール] で、ダウンロードしたコンポーネントをいつ配信するかを選択します。次のオプションがあります。

   - **配信しない** : コンポーネントは Control Manager にダウンロードされますが、管理下の製品には配信されません。このオプションは次の場合に使用します。
     - 管理下の製品に個々に配信する場合
     - アップデートしたコンポーネントを配信前にテストする場合
   - **ただちに配信** : コンポーネントは Control Manager にダウンロードされ、管理下の製品に配信されます。

- **配信計画に従う**：コンポーネントは Control Manager にダウンロードされますが、選択したスケジュールに基づいて管理下の製品に配信されます。
- **新しいコンポーネントが利用可能になったとき**：管理下の製品に必要なコンポーネントが Control Manager で更新された場合のみ、設定されている計画に基づいて配信されます。

注意： この画面で [編集] または [配信計画] をクリックする前に、[保存] をクリックしてください。[保存] をクリックしないと、設定が失われてしまいます。

2. コンポーネントが Control Manager にダウンロードされたら、[配信計画] リストから配信計画を選択します。
3. [保存] をクリックします。

手順 6: 手動ダウンロードの完了

1. [ダウンロード開始] をクリックし、[OK] をクリックして確認します。ダウンロードの応答画面が表示されます。進捗バーにダウンロードの進行状況が表示されます。
2. [コマンド詳細] をクリックして、[コマンド詳細] 画面にダウンロードの詳細を表示します。
3. [OK] をクリックして [手動ダウンロード] 画面に戻ります。

予約ダウンロードの除外設定

[予約ダウンロードの除外設定] 画面を使用して、予約ダウンロードを実行しない時間帯や曜日を指定できます。

休日や業務時間外に Control Manager でダウンロードが実行されるのを避けたい場合に、この設定が役立ちます。

予約ダウンロードの除外スケジュールを設定するには

1. メインメニューで [運用管理] をクリックします。

2. 左側のメニューの [アップデート管理] で、[予約ダウンロードの除外設定] をクリックします。
3. 次のいずれかを実行します。
   - **曜日の設定** - 予約ダウンロードを実行しない曜日を設定するには、[指定した曜日を除外する] チェックボックスをオンにし、曜日を指定します。
   - **時間の設定** - 予約ダウンロードを実行しない時間帯を設定するには、[指定した時間を除外する] チェックボックスをオンにし、時間を指定します。
4. [保存] をクリックします。

予約ダウンロードについて

コンポーネントの予約ダウンロードを設定して、ネットワークの安全のためにコンポーネントが最新の状態に保たれるようにします。Control Manager では、コンポーネントを細かく分けてダウンロードできます。コンポーネントグループおよび個々のコンポーネントのダウンロードスケジュールを指定できます。すべてのスケジュールは、それぞれ独立して実行されます。コンポーネントグループのダウンロードをスケジュールすると、グループ内のすべてのコンポーネントがダウンロードされます。

現在の Control Manager システムに設定されている、次のコンポーネント情報を入手するときは、[予約ダウンロード] 画面を使用します。

- **実行間隔** : コンポーネントごとに、ダウンロードの実行間隔が表示されます。
- **有効** : 予約ダウンロードが有効であるか無効であるかが表示されます。
- **ダウンロード元** : 最新コンポーネントの場所を示す URL またはパスが表示されます。

コンポーネントの予約ダウンロードを設定するには、複数の手順を実行する必要があります。

手順 1: コンポーネントの配信計画の設定

手順 2: プロキシの設定 (プロキシサーバを使用する場合)

手順 3: アップデートするコンポーネントの選択

手順 4: ダウンロードスケジュールの設定

手順 5: ダウンロード方法の設定

手順 6: 自動配信の設定

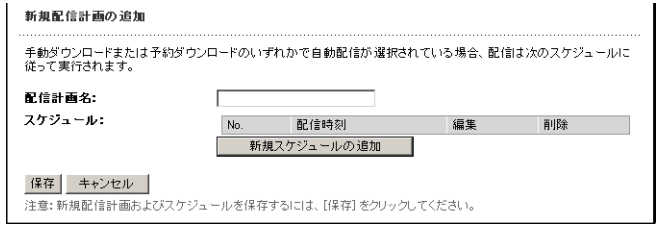
手順 7: スケジュールの有効化と設定の保存

予約ダウンロードの設定とコンポーネントの予約ダウンロードの有効化

手順 1: コンポーネントの配信計画の設定

1. メインメニューで [運用管理] をクリックします。
2. 左側のメニューの [アップデート管理] で、[配信計画] をクリックします。[配信計画] 画面が表示されます。

3. 右側の画面で、[新規配信計画の追加] をクリックします。



4. [新規配信計画の追加] 画面で、[配信計画名] フィールドに配信計画名を入力します。

5. [新規スケジュールの追加] をクリックして、配信計画の詳細を入力します。[新規スケジュールの追加] 画面が表示されます。

6. [新規スケジュールの追加] 画面で、次のいずれかのオプションを選択して、配信スケジュールを選びます。

   - **保留時間** — Control Manager で最新コンポーネントをダウンロードした後、指定した間隔に従って、配信を遅らせます。

     メニューを使用して、時間または分単位で保留期間を指定します。

   - **開始時刻** — 指定した時刻に配信を実行します。

     メニューを使用して、時間または分単位で配信時刻を指定します。

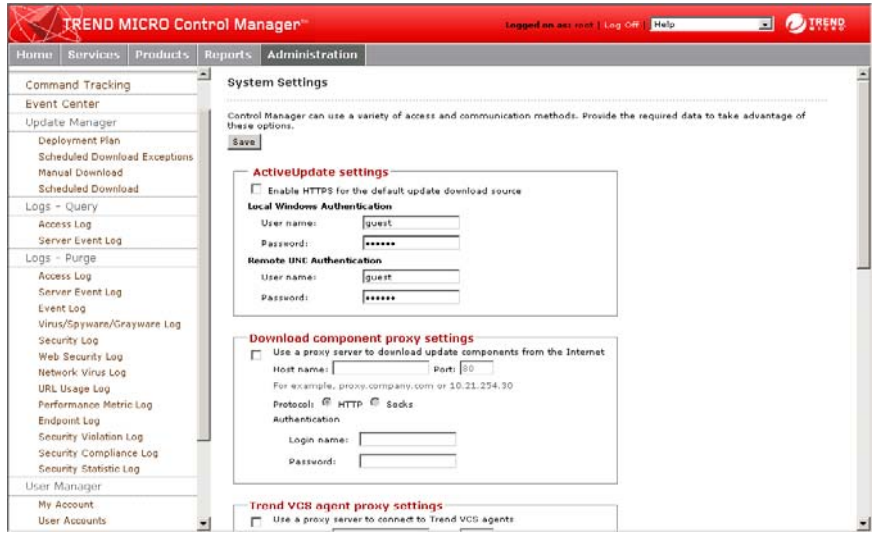
7. スケジュールを適用する製品ディレクトリのフォルダを選択します。選択したフォルダに含まれるすべての製品に対して、スケジュールが適用されます。

8. [OK] をクリックします。

9. [保存] をクリックして、新規配信計画を適用します。

手順 2: プロキシの設定 (プロキシサーバを使用する場合)

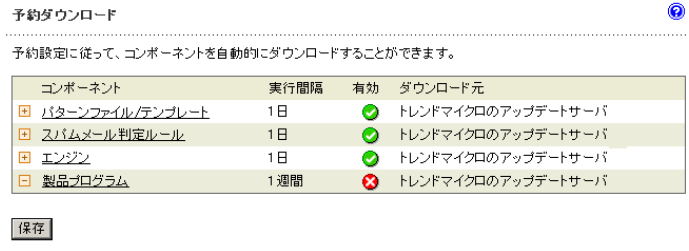
1. [運用管理]→[システム設定] の順に選択します。[システム設定] 画面が表示されます。



2. [ダウンロードに使用するプロキシ設定] で、[インターネットからアップデートファイルをダウンロードするのにプロキシサーバを使用する] チェックボックスをオンにします。
3. [ホスト名] フィールドに、サーバのホスト名または IP アドレスを入力します。
4. [ポート番号] フィールドに、ポート番号を入力します。
5. プロトコルを選択します。
   - HTTPS
   - SOCKS
6. サーバで認証が必要な場合は、ログオン名とパスワードを入力します。
7. [保存] をクリックします。

手順 3: アップデートするコンポーネントの選択

1. [運用管理]→[アップデート管理]→[予約ダウンロード] の順に選択します。[予約ダウンロード] 画面が表示されます。

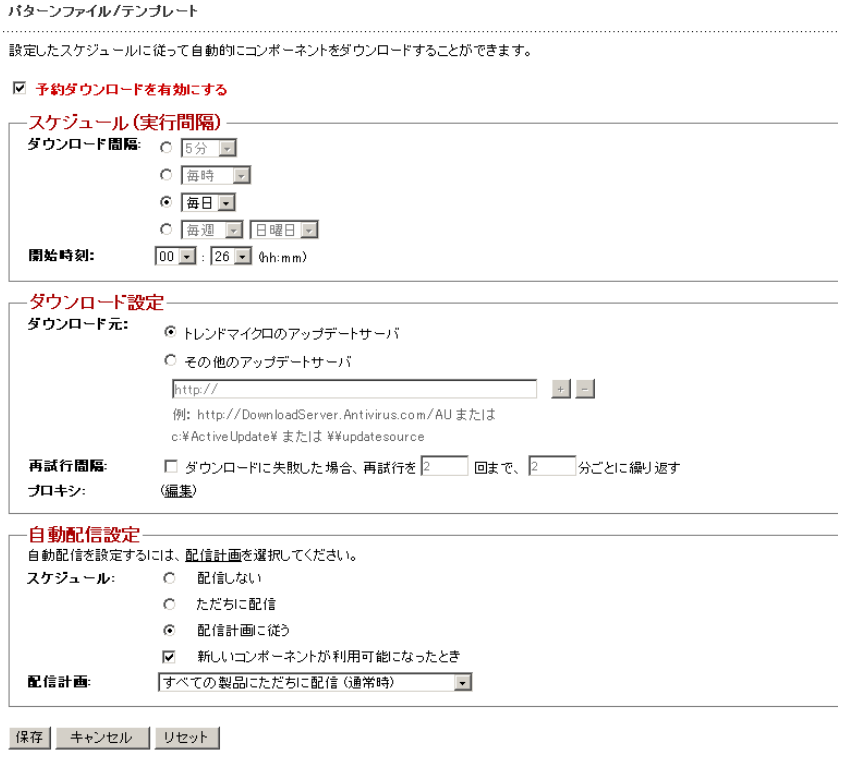


2. [コンポーネント] で、ダウンロードするコンポーネントを選択します。

   a. 各コンポーネントグループのコンポーネントリストを展開するには [+] アイコンをクリックします。

   b. ダウンロードするコンポーネントを選択します。

[< コンポーネント名 >] 画面が表示されます。ここで、< コンポーネント名 > は選択したコンポーネントの名前です。



手順 4: ダウンロードスケジュールの設定

1. [予約ダウンロードを有効にする] チェックボックスをオンにして、コンポーネントの予約ダウンロードを有効にします。
2. ダウンロードのスケジュールを設定します。[ダウンロード間隔] を選択し、該当するリストボックスを使用して、適切なスケジュールを指定します。ダウンロードの実行間隔には、分、時間、日、週のいずれかの時間単位を選択できます。
3. [開始時刻] にて、スケジュールが開始される日付と時刻を指定します。

手順 5: ダウンロード方法の設定

1. ダウンロード元を選択します。

   - **トレンドマイクロのアップデートサーバ** - トレンドマイクロのアップデートサーバからコンポーネントをダウンロードします。
   - **その他のアップデートサーバ** - 指定のフィールドにダウンロード元の URL を入力します。

     [その他のアップデートサーバ] を選択すると、複数のダウンロード元を指定できます。ダウンロード元を追加するには、[+] アイコンをクリックします。ダウンロード元は 5 つまで設定できます。

2. [再試行間隔] を選択し、コンポーネントのダウンロードを再試行する回数と間隔を指定します。

ヒント： この画面で [編集] または [配信計画] をクリックする前に、[保存] をクリックしてください。[保存] をクリックしないと、設定が失われてしまいます。

---

3. ネットワーク上で HTTP プロキシサーバを使用している場合 (Control Manager サーバがインターネットに直接アクセスできない場合) は、[編集] をクリックして、[システム設定] 画面でプロキシを設定します。

手順 6: 自動配信の設定

1. [スケジュール] で、ダウンロードしたコンポーネントをいつ配信するかを選択します。次のオプションがあります。

   - **配信しない** : コンポーネントは Control Manager にダウンロードされますが、管理下の製品には配信されません。このオプションは次の場合に使用します。
     - 管理下の製品に個々に配信する場合
     - アップデートしたコンポーネントを配信前にテストする場合
   - **ただちに配信** : コンポーネントは Control Manager にダウンロードされ、管理下の製品に配信されます。

- **配信計画に従う**：コンポーネントは Control Manager にダウンロードされますが、選択したスケジュールに基づいて管理下の製品に配信されます。
- **新しいコンポーネントが利用可能になったとき**：管理下の製品に必要なコンポーネントが Control Manager で更新された場合のみ、設定されている計画に基づいて配信されます。

ヒント： この画面で [編集] または [配信計画] をクリックする前に、[保存] をクリックしてください。[保存] をクリックしないと、設定が失われてしまいます。

2. コンポーネントが Control Manager にダウンロードされたら、[配信計画] リストから配信計画を選択します。
3. [保存] をクリックします。

手順 7: スケジュールの有効化と設定の保存

1. [有効] 列のステータスボタンをクリックします。
2. [保存] をクリックします。

レポートの使用

Control Manager のレポートは、Control Manager システムで発生したウイルスイベント、スパイウェアイベント、およびコンテンツセキュリティイベントの件数をオンライン集計したものです。Control Manager のエンタープライズ版に、レポート機能が搭載されています。

Control Manager では、次の種類に従ってレポートが分類されます。

- ローカルレポート
- 広域レポート

注意： 上位サーバの管理コンソールからは、[広域レポート] オプションのみを設定できます。

ローカルレポート

ローカルレポートは、上位サーバの管理下の製品に関するレポートです。ローカルレポートには、下位サーバによって作成されたレポートは含まれません。上位サーバに登録されている下位サーバの管理下の製品に関するレポートを表示するときは、[広域レポート] オプションを使用します。

[ローカルレポート] 画面を使用して、利用可能な 1 回限りのローカルレポートおよび予約ローカルレポートを表示できます。

[ローカルレポート] にアクセスするには

1. 上部のメニューで [レポート] を選択します。
2. 左側のメニューで [レポート]→[ローカルレポート] の順に選択します。

注意： 複数のレポートが表示される場合には、[レポートプロファイル] の名前または [前回の作成日時] の日付に基づいてレポートを並べ替えます。

広域レポート

広域レポートは、上位サーバと下位サーバの管理下の製品に関するレポートです。

[広域レポート] 画面を使用して、利用可能な 1 回限りの広域レポートおよび予約広域レポートを表示できます。

[広域レポート] にアクセスするには

1. 上部のメニューで [レポート] を選択します。
2. 左側のメニューで [レポート]→[広域レポート] の順に選択します。
3. 複数のレポートが表示される場合には、[レポートプロファイル] または [作成日時] の日付に基づいてレポートを並べ替えます。

注意 : 広域レポートを表示できるのは、上位サーバだけです。

複数のレポートが表示される場合には、[レポートプロファイル] の名前または [前回の作成日時] の日付に基づいてレポートを並べ替えます。

レポートテンプレートについて

レポートテンプレートを使用することによって、Control Manager レポートの外観と機能を定義できます。特に、レポートテンプレートではレポートに表示される次のセクションが定義されます。

- ヘッダ
- レポート本文
- フッタ

Control Manager 3.5 では、Service Pack 3 以降利用可能な 77 個のレポートテンプレートに、新たに 3 つのレポートテンプレートが追加されています。Service Pack 3 で追加されたレポートは、デスクトップ製品、ファイルサーバ製品、ゲートウェイ製品、メールサーバ製品、ネットワーク製品、および管理下の全製品の 6 つのカテゴリに分類されます。

注意： Control Manager 3.5 では、スパイウェアはウイルスと区別されるようになりました。この変更は、ウイルスに関連する元のすべてのレポートのウイルス数に影響します。

レポートを生成するには、上部のメニューで [レポート] をクリックし、左側のメニューで [ローカルレポート] の下の [レポートプロファイルの作成]、または [広域レポート] の下の [広域レポートの作成] をクリックします。右側の画面に表示される [コンテンツ] タブで、[レポート名]、[レポートタイトル] (任意)、[説明] (任意) を入力できます。レポートの 6 つのカテゴリ (次の表を参照) を表示するには、[レポートのカテゴリ] リストを使用します。チェックボックスをオンにすると、出力されるレポートファイルに、該当するレポートを含めることができます。

Control Manager 3.5 には、このほかに 18 種類のテンプレートが用意されています。これらのテンプレートは、C:¥Program Files¥Trend Micro¥Control Manager¥Reports に、Crystal Reports 9 のファイル (*.rpt) として保存されています (インストール先に応じて異なる場合があります)。これらのテンプレートをローカルレポートおよび広域レポートに適用することができます。

レポートプロファイルについて

プロファイルによって、レポートのコンテンツ (テンプレートと形式)、対象、実行間隔、および受信者がレイアウトされます。次のファイル形式でレポートを表示することができます。

- RTF: リッチテキスト形式。*.RTF レポートを表示するときは、Microsoft Word などのワードプロセッサを使用します。
- PDF: Portable Document Format。*.PDF レポートを表示するときは、Adobe Reader を使用します。

- ActiveX: ActiveX ドキュメント。ActiveX 形式のレポートを表示するときは、Web ブラウザを使用します。

注意： Control Manager では、ActiveX 形式のレポートをメールの添付ファイルとして送信することはできません。

- RPT: Crystal Reports 形式。*.RPT レポートを表示するときは、Crystal Smart Viewer を使用します。

レポートサーバでレポートの作成が完了すると、作成されたレポートのファイル形式に対応する初期設定のビューアが起動します。Crystal Reports 形式のレポートの場合、Crystal Smart Viewer をインストールしておく必要があります。

レポートプロファイルの作成

レポートプロファイルの作成プロセスは、5 段階の手順で構成されます。ローカルレポートと広域レポートでは、作成プロセスが非常に似ています。レポートプロファイルの作成プロセスは、次のとおりです。

手順 1: ローカルレポートと広域レポートのどちらを作成するか選択します。

手順 2: [コンテンツ] タブの設定を指定します。

手順 3: [対象] タブの設定を指定します。

手順 4: [実行間隔] タブの設定を指定します。

手順 5: [受信者] タブの設定を指定します。

ローカルまたは広域レポートプロファイルを作成するには

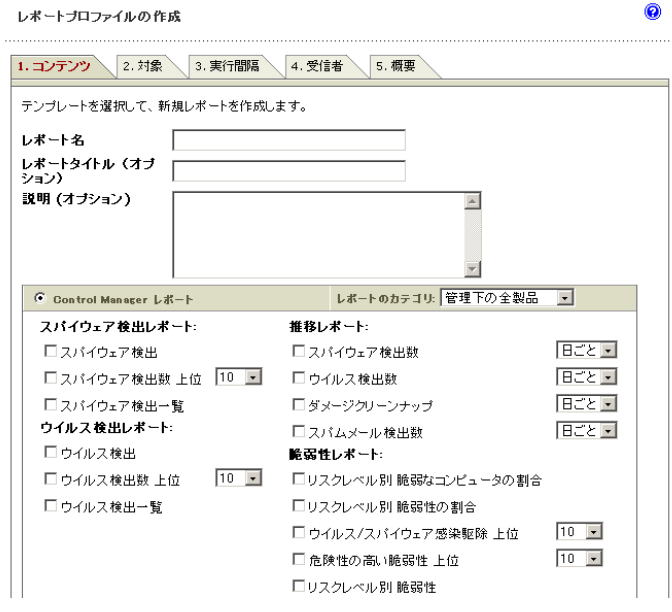
手順 1: ローカルレポートと広域レポートのどちらを作成するか選択します。

1. 上部のメニューで [レポート] を選択します。

2. 次のいずれかの処理を実行します。

   - ローカルレポートプロファイルを作成する場合は、[レポート]→[ローカルレポート] の順に選択します。
   - 広域レポートプロファイルを作成する場合は、[レポート]→[広域レポート] の順に選択します。

3. 左側のメニューで [ローカルレポート] または [広域レポート]→[レポートプロファイルの作成] の順に選択します。



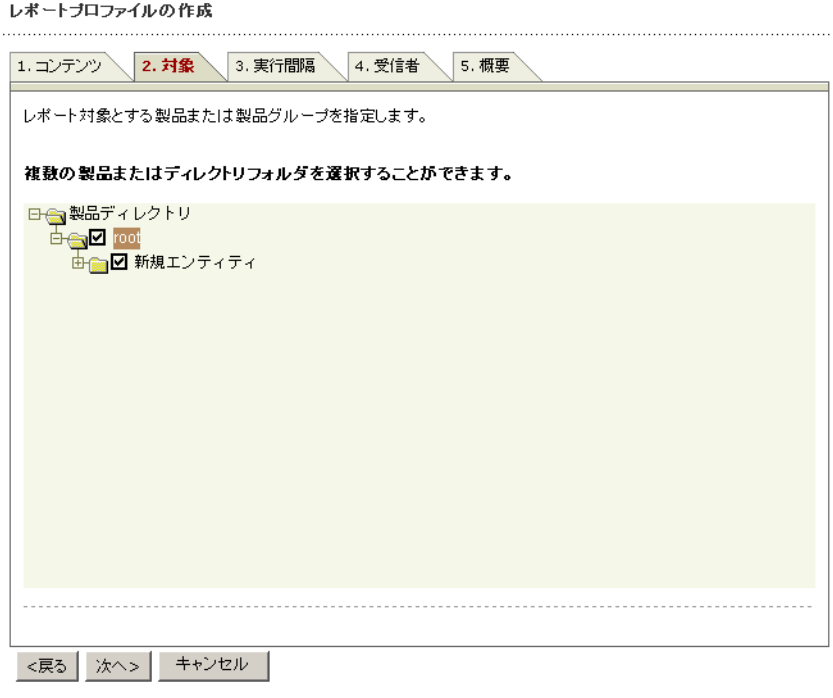
手順 2: [コンテンツ] タブの設定を指定します。

1. 右側の画面の [コンテンツ] タブで、[レポート名] フィールドにレポートの名前を入力します。この名前が、[ローカルレポート] 画面、[広域レポート] 画面のレポートプロファイルに表示されます。
2. [レポートタイトル] フィールドにレポートのタイトルを入力します (任意)。
3. [説明] フィールドにレポートプロファイルの説明を入力します (任意)。

4. [レポートテンプレート] リストボックスから [ネットワーク製品] を選択します。

5. レポートの出力形式を選択します。

6. [次へ >] をクリックして、[対象] タブに進みます。



手順 3: [対象] タブの設定を指定します。

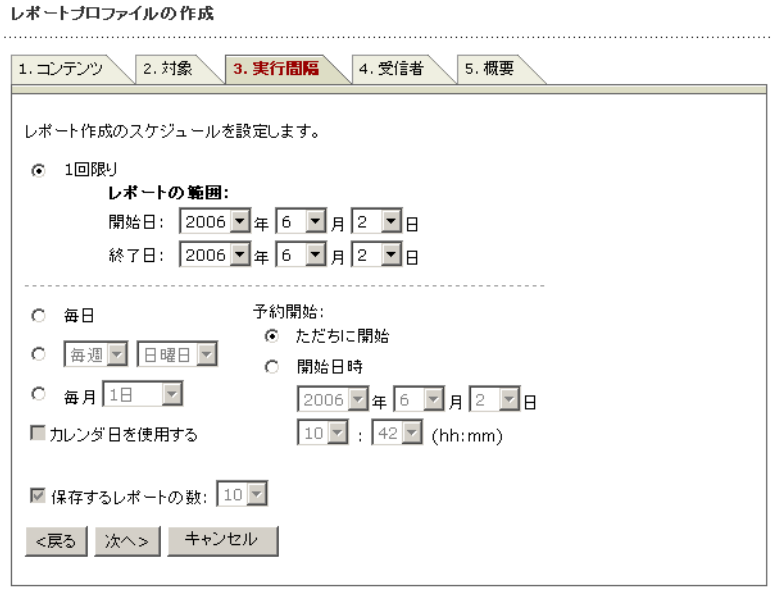
1. 右側の画面の [対象] タブで、ローカルまたは広域レポートプロファイルの対象を選択します。

   - ServerProtect コンピュータまたはフォルダを選択します。プロファイルには、選択した ServerProtect コンピュータまたはフォルダに関する情報だけが含まれます。
   - 下位サーバを選択します。プロファイルには、選択した下位サーバに関する情報だけが含まれます。プロファイルにすべての下位サーバの管理下の製品を含めるときは、上位サーバを選択してください。

2. レポートの対象とするコンピュータを選択します。

   - **すべてのクライアント** : 選択した ServerProtect コンピュータの保護対象のすべてのクライアント
   - **IP 範囲** : レポートの対象とするクライアントの IP 範囲を選択します。
   - **セグメント** : レポートの対象とするクライアントの IP 範囲とセグメントを選択します。

3. [次へ >] をクリックして、[実行間隔] タブに進みます。



手順 4: [実行間隔] タブの設定を指定します。

1. 右側の画面の [実行間隔] タブで、このレポートを作成する間隔を指定します。次のオプションから選択できます。

   - **1 回限り**: 開始日と終了日で指定した情報が含まれます。
   - **毎日**: 作成時 (前日の午前 12 時) から現在の時刻までの情報が含まれます。
   - **毎週または隔週**: 7 日間または 14 日間の情報が含まれます。レポートサーバがレポートの作成を開始する曜日を選択します。
   - **毎月**: 30 日間の情報が含まれます。レポートサーバがレポートの作成を開始する日 (1 日、15 日、または月末日) を選択します。
   - **カレンダ日を使用する**: このチェックボックスをオンにすると、開始時刻は初日の 00:00:00 で、終了時刻は作成日の 00:00:00 になります。

このチェックボックスをオフにすると、開始時刻は初日における作成時刻と同じ時刻で、終了時刻は作成実行日の作成時刻になります。

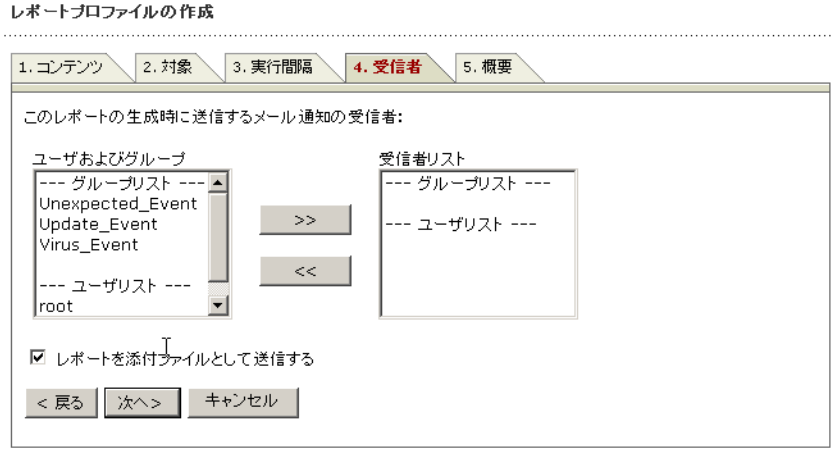
2. [予約開始] で、レポートサーバがこのレポートの情報収集を開始する日時を指定します。次のいずれかを選択します。

   - **ただちに開始**: レポートプロファイルを保存後、ただちに情報が収集されます。
   - **開始日時**: 指定した日時に情報収集が実行されます。

3. 予約レポートの場合は、[保存するレポートの数] をオンにして、サーバ上に保持するレポートの数を指定します。

注意： Control Manager では、予約レポートプロファイルが自動的に有効になります。レポートの作成を一時的に無効にするには、[予約レポート] または [予約広域レポート] 画面に移動し、予約レポートプロファイルの隣にあるチェックボックスをオフにします。

4. [次へ >] をクリックして、[受信者] タブに進みます。



手順 5: [受信者] タブの設定を指定します。

1. 右側の画面の [受信者] タブで、Control Manager のユーザおよびグループから受信者を選択します。

   - >> を使用して、受信者を [ユーザおよびグループ] リストから [受信者] リストに追加します。
   - << を使用して、受信者を [受信者] リストから削除します。

2. レポートを添付ファイルとして送信する場合は、[レポートを添付ファイルとして送信する] をクリックします。添付ファイルの送信を指定しない場合、受信者は、作成されたレポートについてのメール通知のみを受信します。

3. [次へ >] をクリックして、[概要] タブに進みます。

4. 右側の画面の [概要] タブで、プロファイル設定を確認し、[実行] をクリックしてプロファイルを保存します。

レポートプロファイルの設定の確認

プロファイルの設定を確認するには、[プロファイルの概要] 画面を使用します。

[プロファイルの概要] 画面にアクセスしてレポートプロファイルを確認するには

- [ローカルレポート] 画面または [広域レポート] 画面にアクセスします。

  右側の画面の [プロファイル] 列で、[プロファイル表示] をクリックします。

- [予約レポート] 画面または [予約広域レポート] 画面にアクセスします。

  右側の画面の [プロファイル] 列で、[プロファイル表示] をクリックします。

予約レポートプロファイルの有効化

初期設定では、予約プロファイルは Control Manager によって作成時に有効にされます。プロファイルを無効にした場合 (たとえば、データベースまたはエージェントの移行中) は、[予約レポート] 画面または [予約広域レポート] 画面を使用して再度有効にすることができます。

予約レポートプロファイルを有効にするには

1. [予約レポート] 画面または [予約広域レポート] 画面にアクセスします。
2. 右側の画面の [レポートプロファイル] 列で、プロファイルのチェックボックスをオンにします。

   すべてのプロファイルを選択または選択解除するには、[レポートプロファイル] の隣にあるチェックボックスをオンまたはオフにします。
3. [有効] をクリックします。

注意： 実行間隔が「1 回限り」のレポートは 1 度しか生成されないため、これらのレポートプロファイルを有効化、無効化、および編集するオプションは使用できません。

オンデマンド予約レポートの作成

レポートサーバでは、ユーザによって指定された日時に基づいて予約レポートを作成します。予約した作成日時よりも以前にレポートを出力したい場合は、[生成開始] をクリックして、オンデマンドでレポートを作成できます。

オンデマンド予約レポートを作成するには

1. 上部のメニューで [レポート] を選択します。

2. 次のいずれかを実行します。

   - ローカルレポートプロファイルを作成するには、[レポート] の左側のメニューの [ローカルレポート] をクリックします。
   - 広域レポートプロファイルを作成するには、[レポート] の左側のメニューの [広域レポート] をクリックします。

3. 右側の画面の [レポート] 列で、対応する [表示] リンクをクリックします。
4. [開始日] に年、月、日を入力してください。
5. [生成] をクリックします。

レポートのコンテンツによっては、作成に時間がかかることがあります。レポートの作成が終了すると、画面が更新されて、レポートの隣の [レポート表示] リンクが使用できるようになります。

作成されたレポートの表示

レポートをメールの添付ファイルとして送信して表示する以外に、[ローカルレポート] または [広域レポート] 画面を使用して、ローカルレポートまたは広域レポートを表示することもできます。

レポートを表示するには

1. 上部のメニューで [レポート] を選択します。
2. 次のいずれかを実行します。

   - ローカルレポートプロファイルを作成するには、[レポート] の左側のメニューの [ローカルレポート] をクリックします。
   - 広域レポートプロファイルを作成するには、[レポート] の左側のメニューの [広域レポート] をクリックします。

3. 右側の画面の [レポート] 列で、対応する [表示] リンクをクリックします。

   [レポート : { プロファイル名 }] では、[作成要求の送信日時] や [生成完了日時] の順にレポートを並べ替えることができます。

4. [ステータス] 列で、[レポート表示] をクリックします。そのレポートのファイル形式を開くように初期設定で指定されているプログラムが起動します。

設定コマンド

本付録では、コマンドを使用した Trend Micro ServerProtect for Linux (以下、ServerProtect) の設定について解説します。

本付録では、次の内容について説明します。

man ページへのアクセス

ServerProtect では、管理コマンドおよび設定に関する情報を man ページ (マニュアルページ) から参照できます。

ServerProtect では、次の man ページが提供されます。

- tmsplx.xml: ServerProtect 設定パラメータについての説明
- splxmain：splxmain コマンドについての説明
- splx：ServerProtect の起動スクリプトとエラーメッセージに関する説明
- SProtectLinux.bin：ServerProtect インストーラの使用に関する説明
- Cmconfig：このユーティリティの使用方法に関する説明
- RemoteInstall：このユーティリティの使用方法とパラメータに関する説明

man ページを表示するには、次のコマンドを入力します。

```
man 〈コマンド名または設定ファイル名〉
```

例:

```
man tmsplx.xml
```

tmsplx.xml について

ここでは、ServerProtect の設定ファイル「tmsplx.xml」で使用されるパラメータについて説明します。

注意： 設定ファイルに誤った変更を加えると、システムエラーなどの重大な問題が発生する可能性があります。設定ファイルを変更する前に、tmsplx.xml のバックアップを作成してください。

設定ファイル tmsplx.xml は UTF-8 でエンコードされます。tmsplx.xml に非 ASCII 文字を使用する場合はシステムロケールを UTF-8 に設定する必要があります。システムロケールが UTF-8 でない場合、入力した文字が正しくエンコードされず、ServerProtect の動作に問題が発生します。

設定ファイルは次の場所にあります。

```
/opt/TrendMicro/SProtectLinux/tmsplx.xml
```

設定ファイル内の各エントリは、次の形式で定義されています。

```
<P Name="< キー>" Value="< 値 >"/>
```

設定ファイルは、次のグループに分かれています。

- [Scan] グループのキー
- [ActiveUpdate] グループのキー
- [DESTINFO] グループのキー
- [SOURCEINFO] グループのキー

注意： [SOURCEINFO] グループには、アップデートを使用してコンポーネントをダウンロードする際の詳細オプションを有効または無効にするためのパラメータが含まれています。詳細については、オンラインヘルプの [Using ServerProtect]→[Updates]→[Enable/Disable Advanced ActiveUpdate Options] トピックを参照してください。

- [Notification] グループのキー
- [Configuration] グループのキー
- [GUIPassword] グループのキー
- [Logs] グループのキー
- [Registration] グループのキー
- [WVTP] グループのキー

設定ファイルは、次の規則に従って記述する必要があります。

- 各パラメータは「<」で始まり「/>」で終わる
- すべてのキーと値は二重引用符 (" ") で囲まれている
- Value 内の複数の値はコロン (:) で区切られている

  例:

  /var/tmp:/home/samba:/tmp

tmsplx.xml ファイルを変更、保存した後は、ServerProtect を再起動する必要があります。

ServerProtect を再起動するには

コマンドラインで次のように入力します。

```
su root
/etc/init.d/splx restart
```

tmsplx.xml ファイルをカスタマイズしたら、バックアップを作成することをお勧めします。初期設定ファイルのコピーは、tmsplx.xml.tmplate ファイルとして提供されています。ファイルを初期設定に戻すには、このファイルを使用します。tmsplx.xml.tmplate ファイルを設定ファイルのバックアップとして使用してください。

設定ファイルの記述は、ServerProtect ソフトウェアのさまざまなモジュールに対応するサブグループに分かれています。

[Scan] グループのキー

このグループのキーでは、ウイルス検索処理を管理します。リアルタイム検索、予約検索、および手動検索を個々に設定できます。

指定した時間に予約検索を実行する場合、SUSE Linux では cron を使用し、Red Hat では crond を使用します。ServerProtect では、tmsplx.xml ファイルで指定した検索周期と時間が /etc/cron.d/splx の有効なエントリに変換されます。「検索対象」または「検索除外」のいずれかの設定を使用して、ウイルス検索の対象とするファイルをディレクトリまたは拡張子で指定できます。

注意： 検索対象と検索除外の両方が指定されている場合、除外設定が優先されます。

RealtimeScan

このキーでは、リアルタイム検索を有効または無効にします。

有効な値は次のとおりです。

- **0 ：無効**
- **1 ：入力 (書き込み) ファイルを検索 (初期設定)**
- **2 ：出力 (読み取り) ファイルを検索**
- **3 ：入出力ファイルの両方を検索**
- **4 ：実行中のファイルを検索**
- **5 ：実行中のファイルおよび入力 (書き込み) ファイルを検索**
- **6 ：実行中のファイルおよび出力 (読み取り) ファイルを検索**
- **7：実行中のファイル、入力 (書き込み) ファイル、および出力 (読み取り) ファイルを検索**

RealtimeIncludeDirList、ScheduledIncludeDirList、ManualIncludeDirList

これらのキーでは、検索対象のディレクトリを指定します。検索から除外したいディレクトリのフルパスを入力します。複数のディレクトリを指定する場合は、各項目をコロン (:) で区切ります。たとえば、リアルタイム検索の対象に tmp ディレクトリと etc ディレクトリを指定するには、次のように設定します。

```
<P Name="RealtimeIncludeDirList" Value="/tmp:/etc"/>
```

注意： キーの値が null (初期設定) の場合、すべてのディレクトリが検索対象になります。

RealtimeIntelliScan、ScheduledIntelliScan、ManualIntelliScan

設定ファイルでこれらのキーを使用して、トレンドマイクロの推奨設定を有効または無効にします。指定可能な値は次のとおりです。

0 ：トレンドマイクロの推奨設定を無効にする (初期設定)

1 ：トレンドマイクロの推奨設定を有効にする

ScheduledMapDriveExclusion、ManualMapDriveExclusion

設定ファイルでこれらのキーを使用して、割り当てドライブの除外機能を有効または無効にします。指定可能な値は次のとおりです。

0 ：割り当てドライブの除外を無効にする

1 ：割り当てドライブの除外を有効にする

RealtimeIncludeExtList、ScheduledIncludeExtList、ManualIncludeExtList

これらのキーでは、検索対象のファイルタイプを拡張子で指定します。複数の拡張子を指定する場合は、各項目をコロン (:) で区切ります。拡張子の指定では、大文字と小文字は区別されません。たとえば、リアルタイム検索の対象に BIN と RPM の拡張子を指定するには、次のように設定します。

```
<P Name="RealtimeIncludeExtList" Value="BIN:RPM"/>
```

注意： キーの値が null (初期設定) の場合は、すべての拡張子が検索対象になります。

RealtimeIncludeTMExtList、ScheduledIncludeTMExtList、ManualIncludeTMExtList

これらのキーを使用して、すべての種類のファイルを検索するか、トレンドマイクロが推奨する拡張子のファイルを検索するかを選択します。有効な値は次のとおりです。

- 0 ：(初期設定) すべてのファイルを検索する
- 1 ：指定した拡張子のファイルを検索する

RealtimeExcludeDirList、ScheduledExcludeDirList、ManualExcludeDirList

これらのキーでは、特定のディレクトリを検索対象から除外します。検索から除外するディレクトリのフルパスを入力します。複数のディレクトリを指定する場合は、各項目をコロン (:) で区切ります。

注意： キーの値が null の場合、すべてのディレクトリが検索対象になります。

初期設定は次のとおりです。

```
/dev:/proc:/var/spool/mail:/var/mail:/var/spool/mqueue:/var/spool/
mqueue.iscan:/opt/TrendMicro/SProtectLinux/SPLX.Quarantine:/opt/Tr
endMicro/SProtectLinux/SPLX.Backup:
```

RealtimeExcludeFileList、ScheduledExcludeFileList、ManualExcludeFileList

これらのキーでは、検索対象のディレクトリに含まれる個々のファイルを検索対象から除外します。除外したいファイルのフルパスを入力します。複数のファイルを指定する場合は、各項目をコロン (:) で区切ります。たとえば、/etc ディレクトリの example.txt というファイルをリアルタイム検索から除外するには、次のように入力します。

```
<P Name="RealtimeExcludeFileList" Value="/etc/fm.txt"/>
```

注意： キーの値が null (初期設定) の場合は、すべてのファイルが検索対象になります。

RealtimeExcludeExtList、ScheduledExcludeExtList、ManualExcludeExtList

これらのキーでは、拡張子を指定して特定のファイルタイプを検索対象から除外します。複数の拡張子を指定する場合は、各項目をコロン (:) で区切ります。たとえば、リアルタイム検索から BIN と TXT の拡張子を除外するには、次のように入力します。

```
<P Name="RealtimeExcludeExtList" Value="BIN:TXT"/>
```

注意： 拡張子の指定では、大文字と小文字は区別されません。

RealtimeCustomizedAction、ScheduledCustomizedAction、ManualCustomizedAction

これらのキーでは、特定の種類のセキュリティリスクに対して実行するカスタム処理の初期設定を指定します。この設定は、[Real-time Scan] 画面、[Scheduled Scan] 画面、および [Manual Scan] 画面の [Action When Security Risk Found] に表示されます。

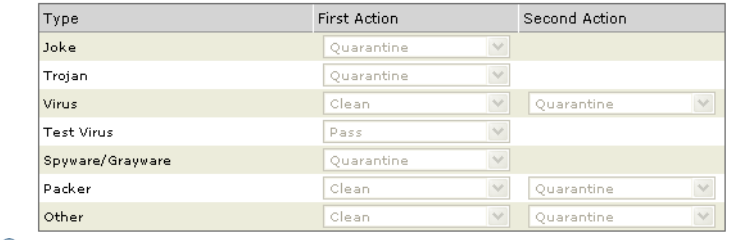


図 B-1.　カスタム検索処理を選択した場合の初期設定

ウイルス、パッカーおよびその他の脅威については、2 番目の処理を指定できます。

有効な値は次のとおりです。

0 ：放置 (何もしません)

1 ：FileExtentionToRename キーで指定した拡張子を追加して、感染ファイルの名前を変更する

2 ：隔離

3 ：ウイルス駆除

4 ：削除

なお、各 AllTypesAction の初期設定値は 3-2 で、無効にする場合は null を設定します。

ジョークプログラム ：2-0

トロイの木馬 ：2-0

ウイルス ：3-2

テストウイルス ：0-0

スパイウェア ：2-0

その他 ：3-2

カスタム処理を無効にする ：0

RealtimeAllTypesAction、ScheduledAllTypesAction、ManualAllTypesAction

これらのキーでは、すべての種類のセキュリティリスクに対して実行する処理の初期設定を指定します。この設定は、[Real-time Scan] 画面、[Scheduled Scan] 画面、および [Manual Scan] 画面の [Action When Security Risk Found] に表示されます。

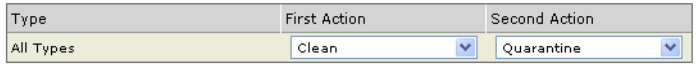


図 B-2. 「すべての種類」検索処理を選択した場合の初期設定 (最初の処理と 2 番目の処理)

ウイルスおよびその他の脅威についてのみ、2 番目の処理を指定できます。

有効な値は次のとおりです。

0 ：放置 (何もしません)

1 ：FileExtentionToRename キーで指定した拡張子を追加して、感染ファイルの名前を変更する

2 ：隔離

3 ：ウイルス駆除

4 ：削除

なお、各 AllTypesAction の初期設定値は 3-2 で、無効にする場合は null を設定します。

すべての種類 ：3-2

すべての種類の処理を無効にする ：0

注意： RealtimeCustomizedAction キー、ScheduledCustomizedAction キー、ManualCustomizedAction キー、RealtimeAllTypesAction キー、ScheduledAllTypesAction キー、および ManualAllTypesAction キーを null に設定した場合、リアルタイム検索、予約検索、および手動検索では、自動的にトレンドマイクロの推奨処理が使用されます。

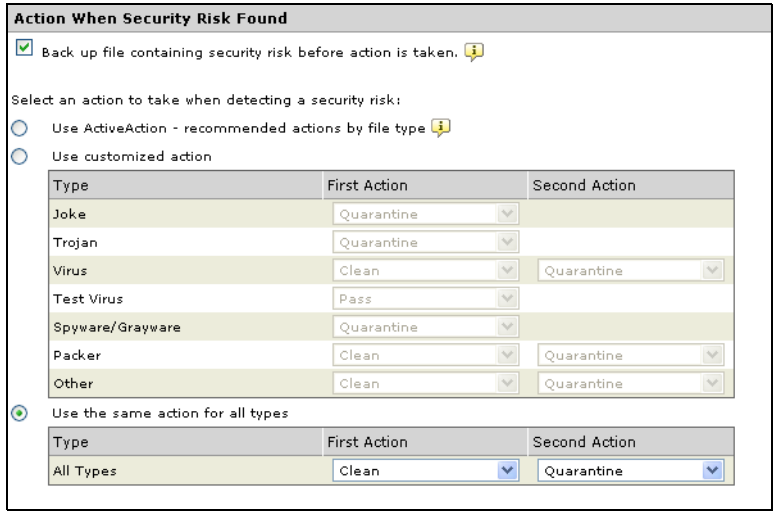


図 B-3.　CustomizedAction と AllTypesAction を null に設定すると、[Use ActiveAction] が選択される

RealTimeScanArchived、ScheduledScanArchived、ManualScanArchived

現在は使用しません。

RealtimeScanCompressed、ScheduledScanCompressed、ManualScanCompressed

これらのキーでは、圧縮ファイルの検索を有効または無効にします。有効な値は次のとおりです。

0 ：圧縮ファイルの検索を無効にする

1 ：圧縮ファイルの検索を有効にする (初期設定)

RealtimeCompressionLayer、ScheduledCompressionLayer、ManualCompressionLayer

これらのキーでは、検索する圧縮ファイルの階層数を指定します。有効な値は 1 ～ 20 です。リアルタイム検索の初期設定は 1、予約検索および手動検索の初期設定は 5 です。

注意： 値を小さく設定すると処理時間が短くなりますが、セキュリティ対策の効果は小さくなります。

RealtimeCompressedFileSize、ScheduledCompressedFileSize、ManualCompressedFileSize

これらのキーでは、検索対象とする圧縮ファイルの最大サイズ (圧縮前) を指定します。値は MB 単位で指定します。最大値は 2000 で、予約検索および手動検索の初期設定は 60 です。リアルタイム検索の初期設定は 30 です。たとえば、RealtimeCompressedFileSize キーの値が 40 の場合、圧縮前のサイズが 40MB 以下の圧縮ファイルのみがリアルタイム検索の対象となります。

```
<P Name="RealtimeCompressedFileSize" Value="40"/>
```

注意： 値を小さく設定すると処理時間が短くなりますが、セキュリティ対策の効果は小さくなります。

RealtimeCleanSave、ScheduledCleanSave、ManualCleanSave

これらのキーでは、ウイルス駆除前のファイルのバックアップを有効または無効にします。有効な値は次のとおりです。

0 ：**ファイルのバックアップを無効にする**

1 ：**ファイルのバックアップを有効にする (初期設定)**

ScheduledNice、ManualNice

これらのキーを使用して、プロセスのスケジュール優先度を設定します。初期設定は null です。有効な値は次のとおりです。

-20 ：優先度が最も高い

19 ：優先度が最も低い

DirToMove

このキーでは、AllTypesAction キーまたは CustomizedAction キーが Quarantine に設定されている場合に、ウイルスが検出された時点でファイルを移動するディレクトリを指定します。初期設定は次のとおりです。

```
/opt/TrendMicro/SProtectLinux/SPLX.Quarantine
```

DirToSave

このキーでは、感染したファイルをウイルス駆除前に保存するディレクトリを指定します。初期設定は次のとおりです。

```
/opt/TrendMicro/SProtectLinux/SPLX.Backup
```

FileExtensionToRename

AllTypesAction または CustomizedAction フィールドが Rename に設定されている場合に、感染ファイルに追加するファイル拡張子です。初期設定は vir。

ActionForTimeout

現在はこのキーを使用しません。

VirusOutbreak

このキーでは、ウイルス大規模感染検出時における通知の送信を有効または無効にします。有効な値は次のとおりです。

0 ：ウイルス大規模感染の通知を送信しない

1 ：ウイルス大規模感染の通知を送信する (初期設定)

注意： 感染ファイルの数が VirusOutbreakCount キーで指定した値に達すると、警告が通知されます。

VirusOutbreakPeriod

このキーでは、大規模感染の通知の周期を分単位で指定します。有効な値は、5、10、30、60、120、および 240 です。初期設定は 60 です。VirusOutbreak キーが無効になっている場合、このキーは機能しません。

VirusOutbreakCount

このキーでは、大規模感染の通知の送信に必要な感染ファイル数を指定します。有効な値は 1 ～ 1000 です。初期設定は 100 です。VirusOutbreak キーが無効になっている場合、このキーは機能しません。

AlertVirusInfection

このキーでは、システム上で感染ファイルが見つかった場合に、警告の通知を送信するかどうかを指定します。有効な値は次のとおりです。

0 ：感染ファイルが見つかったとき、警告の通知を送信しない

1 ：感染ファイルが見つかったとき、警告の通知を送信する (初期設定)

AlertRealtimeConfigChange

このキーでは、リアルタイム検索の設定を変更したときに、警告の通知を送信するかどうかを指定します。有効な値は次のとおりです。

0 ：リアルタイム検索の設定を変更したときに、警告の通知を送信しない

1 ：リアルタイム検索の設定を変更したときに、警告の通知を送信する (初期設定)

AlertServerProtectOn、AlertServerProtectOff

このキーでは、splx サービスを停止または再起動したときに、警告の通知を送信かどうかを指定します。有効な値は次のとおりです。

0 ：splx サービスを停止または再起動したときに、警告の通知を送信しない

1 ：splx サービスを停止または再起動したときに、警告の通知を送信する (初期設定)

AlertPatternOutOfDate

このキーでは、パターンファイルが期限切れになった後、指定の日数が経過した時点で警告の通知を送信するかどうかを指定します。有効な値は次のとおりです。

0 ：パターンファイルの期限が切れた後、指定の日数が経過した時点で警告の通知を送信しない

1 ：パターンファイルの期限が切れた後、指定の日数が経過した時点で警告の通知を送信する (初期設定)

AlertPatternOutOfDatePeriod

このキーでは、パターンファイルが最新かどうかをチェックする周期を日数単位で設定します。有効な値は 1 ～ 1000 です。初期設定は 7 です。たとえば、パターンファイルが最新かどうかを 7 日ごとにチェックする場合は、次のように入力します。

```
<P Name="AlertPatternOutOfDatePeriod" Value="7"/>
```

AlertPatternUpdateFail

このキーでは、パターンファイルのアップデートに失敗したときに、警告の通知を送信するかどうかを指定します。

0 ：パターンファイルのアップデートに失敗したときに、警告の通知を送信しない

1 ：パターンファイルのアップデートに失敗したときに、警告の通知を送信する (初期設定)

AlertActionFail

このキーでは、検出された不正プログラムに対して指定された処理を実行できなかった場合に、警告の通知を送信するかどうかを指定します。

0 ：検出された不正プログラムに対して指定された処理を実行できなかった場合に、警告の通知を送信しない

1 ：検出された不正プログラムに対して指定された処理を実行できなかった場合に、警告の通知を送信する

Schedule

このキーでは、予約検索の実行周期を設定します。有効な値は次のとおりです。

0 ：予約検索ジョブを実行しない (初期設定)

2 ：予約検索ジョブを毎日実行する

3 ：予約検索ジョブを 1 週間ごとに実行する

4 ：予約検索ジョブを 1ヵ月ごとに実行する

ScheduledTime

このキーでは、予約検索の実行時間を 24 時間制で設定します。初期設定は 00:00:00 (午前 0 時) です。

たとえば、予約検索を午後 1 時半に実行するには、次のように入力します。

```
<P Name="ScheduledTime" Value="13:30:00"/>
```

ScheduledWDay

このキーでは、Schedule キーを 3 (1 週間おき) に設定した場合に、予約検索を実行する曜日を設定します。有効な値は、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、Sunday です。初期設定は null です。

ScheduledMDay

このキーでは、Schedule キーを 4 (1ヵ月おき) に設定した場合に、予約検索を実行する日を設定します。有効な値は 1 ～ 31 です。初期設定は null です。

[ActiveUpdate] グループのキー

このグループのキーでは、アップデートサーバに関連するさまざまなオプションを指定します。このグループ内のキーは、ServerProtect の現在のステータスに関する情報を持ちます。

注意： このグループのキーを変更するときは、事前にトレンドマイクロのテクニカルサポートへ問い合わせてください。

EngineType

このキーは変更しないでください。

EngineVersion

このキーは変更しないでください。

EngineLastUpdateTime

このキーは変更しないでください。

PatternType

このキーは変更しないでください。

PatternVersion

このキーは変更しないでください。

PatternDate

このキーは変更しないでください。

PatternLastUpdateTime

このキーは変更しないでください。

SpywarePatternType

このキーは変更しないでください。

SpywarePatternVersion

このキーは変更しないでください。

SpywarePatternDate

このキーは変更しないでください。

SpywarePatternLastUpdateTime

このキーは変更しないでください。

ProductType

このキーは変更しないでください。

ProductVersion

このキーは変更しないでください。

Language

このキーは変更しないでください。

Platform

このキーは変更しないでください。

ManualNOption、ScheduledNOption

このキーでは、ServerProtect で手動アップデートまたは予約アップデートを実行したときにアップデートされるコンポーネントの種類を管理できます。有効な値は次のとおりです。

- **0 ：なし**
- **1 ：ウイルスパターンファイルをアップデートする**
- **2 ：検索エンジンをアップデートする**
- **3 ：ウイルスパターンファイルと検索エンジンの両方をアップデートする**
- **32 ：スパイウェアパターンファイルをアップデートする**
- **33 ：ウイルスパターンファイルとスパイウェアパターンファイルをアップデートする**
- **34 ：スパイウェアパターンファイルと検索エンジンをアップデートする**
- **35 ：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、および検索エンジンをアップデートする (初期設定)**

Option

アップデートのオプションです。このキーは AU_OPTION に設定されており、変更できません。

Schedule

このキーでは、予約アップデートのスケジュールを指定します。有効な値は次のとおりです。

0 ：予約アップデートを実行しない

1 ：1 時間ごとにアップデートする

2 ：1 日ごとにアップデートする (初期設定)

3 ：1 週間ごとにアップデートする

次のキーは、上記の予約アップデートの日時を指定するものです。

ScheduledTime

このキーでは、予約アップデートの時刻を 24 時間制で指定します。Schedule キーの値が 1、2、または 3 の場合に、このキーを使用します。

ScheduledWDay

このキーでは、予約アップデートの曜日を設定します。有効な値は、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、Sunday です。

RandomizedUpdate

このキーでは、アップデートサーバの負荷分散をサポートするため、ランダムアップデート機能を使用することを指定します。この機能は初期設定で有効になっています。初期設定は、指定したアップデート時刻から 2 時間間隔です。値 0 を指定すると、ランダムアップデート機能が無効になります。0 ～ 12 の値を指定できます。

UpdateRetryNum

このキーでは、パターンファイルと検索エンジンのアップデート試行回数を指定します。値 0 を指定すると、ランダムの再試行が無効になります。0 ～ 3 の値を指定できます。初期設定は 3 です。

UpdateRetryInterval

このキーでは、再試行の間隔を分数で指定します。10 ～ 60 を指定できます。初期設定は 10 です。

[SOURCEINFO] グループのキー

このグループのキーでは、パターンファイル、検索エンジン、および大規模感染予防ポリシーのダウンロード元を指定します。

DefaultSource

このキーは、アップデートのダウンロード元 URL を示します。ServerProtect の初期設定は、ServerProtect を Control Manager に登録しているかどうかによって異なります。

ServerProtect を Control Manager に登録している場合、初期設定は次のようになります。

```
http://xxx.xxx.xxx.xxx/TVCSDownload/ActiveUpdate
```

「xxx.xxx.xxx.xxx」は Control Manager の IP アドレスです。
ServerProtect を Control Manager に登録していない場合、初期設定は次のようになります。

```
http://splx3-p.activeupdate.trendmicro.com/activeupdate
```

警告： アップデートの URL が変更されたことをトレンドマイクロから通知されない限り、この値を変更しないでください。

Source

このキーでは、トレンドマイクロのアップデートサーバ以外のダウンロード元を指定します。初期設定は null (ダウンロード元を指定しない) です。このキーの値が null でない場合は、DefaultSource よりもこのダウンロード元が優先されます。Source キーには、URL またはローカルパスを指定できます。

DigSig

このキーでは、ダウンロード元からコンポーネントをダウンロードする際、ServerProtect がデジタル署名を適用するかどうかを指定します。有効な値は次のとおりです。

0 ：デジタル署名ダウンロードを無効にする

1 ：デジタル署名ダウンロードを有効にする

注意： デジタル署名ダウンロードを有効にした場合 (DigSig = 1) に、ダウンロード元が Control Manager サーバであると、Control Manager ではダウンロードにデジタル署名を使用できないため、アップデートが失敗することがあります。

SrvAuth

このキーでは、ダウンロード元が HTTPS の場合に、HTTPS 認証を適用するかどうかを指定します。有効な値は次のとおりです。

0 ：HTTPS 認証ダウンロードを無効にする (初期設定)

1 ：HTTPS 認証ダウンロードを有効にする

Merge

このキーでは、アップデートサーバからアップデートを実行する際に、パターンファイルに対する差分アップデートを許可するかどうかを指定します。有効な値は次のとおりです。

0 ：差分アップデートを無効にする

1 ：差分アップデートを有効にする (初期設定)

ProxyUsername

プロキシサーバで認証が必要な場合、このキーのユーザ名が使用されます。初期設定は null です。

ProxyPassword

プロキシサーバで認証が必要な場合、このキーのパスワードが使用されます。初期設定は null です。Web コンソールまたは splxmain コマンドを使用してこの値を変更できます (splxmain コマンドは、/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp フォルダにあります。226 ページの「splxmain」参照)。

Proxy

このキーでは、プロキシサーバの FQDN または IP アドレスを指定します。初期設定は null です。次に例を示します。

```
proxy.example.com
```

UseProxy

このキーでは、Source キーまたは DefaultSource キーで指定したアップデート URL へのアクセスにプロキシサーバを使用するかどうかを指定します。有効な値は次のとおりです。

0 ：プロキシサーバを使用しない (初期設定)

1 ：プロキシサーバを使用する

UseProxy キーの値を 1 に設定した場合、Proxy キーを使用してプロキシサーバのアドレスを指定する必要があります。また、必要に応じてユーザ名、パスワード、およびポート番号も指定する必要があります。

ProxyPort

このキーでは、プロキシサーバのポート番号を指定します。初期設定は null です。

ProxyType

プロキシサーバの種類を指定します。有効な値は次のとおりです。

0 ：HTTP プロキシ (初期設定)

1 ：Socks4 プロキシ

2 ：Socks5 プロキシ

UseGeneralProxy

このキーでは、ウイルストラッキングプログラム (WVTP) およびライセンスのアップデートの場合と同じ一般プロキシ設定を使用してアップデートサーバから最新コンポーネントをダウンロードするように指定します。有効な値は次のとおりです。

0 ：コンポーネントのアップデートに一般プロキシサーバを使用しない (初期設定)

1 ：コンポーネントのアップデートに一般プロキシサーバを使用する

[DESTINFO] グループのキー

Destination

このキーでは、ServerProtect の初期設定のディレクトリパスを指定します。初期設定は次のとおりです。

```
/opt/TrendMicro/SProtectLinux
```

[Notification] グループのキー

ServerProtect では、さまざまなセキュリティイベントの通知を送信するように設定できます。[Notification] グループのキーでは、通知の内容および受信者を指定します。通知の送信の有効 / 無効を設定するには、[Scan] グループのキーを使用します。

送信者と受信者のメールアドレス、および SMTP または SNMP サーバを指定する必要があります。これらの設定は、あらゆる種類のセキュリティイベントの通知に対して使用されます。

Type

このキーでは、通知の送信方法を指定します。有効な値は次のとおりです。

"" (null)：初期設定

SMTP ：SMTP サーバを使用

SNMP ：SNMP プロトコルを使用

SMTP:SNMP ：両方の送信方法を使用

SmtpServer

このキーでは、SMTP サーバの FQDN または IP アドレスを指定します。次に例を示します。

```
smtp.example.com
```

Type キーの値が SMTP または SMTP:SNMP に設定されている場合は、このキーに値を入力する必要があります。初期設定は null です。

SmtpPort

このキーでは、SMTP サーバのポート番号を指定します。有効な値は 1 ～ 65535 です。初期設定は 25 です。

SmtpUserID

このキーでは、SMTP サーバのユーザアカウント名を指定します。初期設定は null です。

SmtpPassword

このキーでは、SMTP サーバのユーザアカウントのパスワードを指定します。初期設定は null です。

SmtpAuthType

このキーは内部で使用されます。このキーには、SMTP サーバへのログオンに使用された認証方法が記録されます。この認証方法は ServerProtect によって自動的に検出されます。有効な値は次のとおりです。

0 ：認証の必要なし (初期設定)

1 ：LOGIN 認証方法

2 ：PLAIN 認証方法

3 ：CRAM_MD5 認証方法

SmtpFrom

このキーでは、通知メールの送信元となるメールアドレスを指定します。次に例を示します。

```
administrator@example.com
```

初期設定は null です。

注意： SMTP サーバの種類によっては、有効な送信者のメールアドレスがないとメールが送信できない場合があります。

SmtpTo

このキーでは、通知の受信者を指定します。複数の受信者を指定する場合は、各項目をコロン (:) で区切ります。次に例を示します。

```
pd@example.com:fm@example.com
```

注意： このキーの初期設定値は null です。

SmtpTimeout

SMTP タイムアウト値を秒数で指定します。初期設定は 15 です。

SmtpCharset

このキーでは、ServerProtect が通知メールのエンコードに使用する文字コードを指定します。有効な値は次のとおりです。

big5 繁体字中国語

euc-kr 韓国語

gb2312 簡体字中国語

iso-2022-jp 日本語

iso-8859-1 Latin 1 西ヨーロッパ 言語(初期設定)

shift-jis 日本語

us-ascii 英語

SnmpHostname

このキーでは、SNMP サーバの FQDN または IP アドレスを指定します。次に例を示します。

```
snmp.example.com
```

Type キーの値が SNMP または SMTP:SNMP の場合は、このキーに値を入力する必要があります。初期設定は null です。

SnmpCommunity

このキーでは、SNMP のコミュニティ名を指定します。初期設定は public です。Type キーの値が SNMP または SMTP:SNMP の場合は、このキーに値を入力する必要があります。

VirusOutbreakSubject

このキーでは、ウイルス大規模感染の件名を指定します。初期設定は次のとおりです。

```
[SPLX] Security risk outbreak subject
```

VIRUSOUTBREAKMESSAGE

このキーでは、ウイルス大規模感染の通知のメッセージ本文を指定します。初期設定は次のとおりです。

```
A security risk outbreak was detected
```

VirusInfectionSubject

このキーでは、ウイルス感染通知の件名を指定します。初期設定は次のとおりです。

```
[SPLX] Security risk outbreak subject
```

VIRUSINFECTIONMESSAGE

このキーでは、ウイルス感染通知のメッセージ本文を指定します。初期設定は次のとおりです。

```
Security risk infection(s) detected
```

RealtimeConfigChangeSubject

このキーでは、リアルタイム検索設定の変更通知の件名を指定します。初期設定は次のとおりです。

```
[SPLX] Real-time scan configuration modified
```

REALTIMECONFIGCHANGEMESSAGE

このキーでは、リアルタイム検索設定の変更通知のメッセージ本文を指定します。初期設定は次のとおりです。

```
The real-time scan configuration was modified
```

ServerProtectOnSubject

このキーでは、ServerProtect 起動時の通知の件名を指定します。初期設定は次のとおりです。

```
[SPLX] ServerProtect was started
```

ServerProtectOffSubject

このキーでは、ServerProtect 停止時の通知の件名を指定します。初期設定は次のとおりです。

```
[SPLX] ServerProtect was stopped
```

SERVERPROTECTONMESSAGE

このキーでは、ServerProtect 起動時の通知の本文を指定します。初期設定は次のとおりです。

```
ServerProtect was started
```

SERVERPROTECTOFFMESSAGE

このキーでは、ServerProtect 停止時の通知の本文を指定します。初期設定は次のとおりです。

```
ServerProtect was stopped
```

PatternOutOfDateSubject

このキーでは、パターンファイルが指定した日数を経過してもアップデートされない場合に送信される通知の件名を指定します。初期設定は次のとおりです。

```
[SPLX] Virus pattern file is outdated
```

PATTERNOUTOFDATEMESSAGE

このキーでは、パターンファイルが指定した日数を経過してもアップデートされない場合に送信される通知の本文を指定します。初期設定は次のとおりです。

```
Virus pattern file is outdated
```

PatternUpdateFailMessage

このキーでは、パターンファイルのアップデートに失敗した場合に送信される通知の件名を指定します。初期設定は次のとおりです。

```
[SPLX] Pattern update unsuccessful
```

ActionFailMessage

このキーでは、処理が失敗した場合に送信される通知の件名を指定します。初期設定は次のとおりです。

```
[SPLX] Action performed on malware unsuccessful
```

MaxItemNumber

通知キューに格納される通知の最大数です。初期設定は 1000 です。

[Configuration] グループのキー

このグループのキーは、ServerProtect 関連の設定を指定します。

ThreadNumber

このキーは変更しないでください。

UserDebugLevel

ServerProtect のユーザレベル部分に対するデバッグ情報のレポートレベルを指定します。有効な値は次のとおりです。

- 0 ：デバッグ出力なし
- 1 ：ログ関数のエントリおよび関連する名前 / パスのみ (初期設定)
- 2 ：レベル 1 より詳細なプロセス ID に関する情報、関数のリターンコード、およびクラスメンバーの関数とデータメンバーの値に関する詳細を記録する
- 3 ：レベル 2 より詳細な内部データ構造の情報、および、検索エンジン、ウイルスパターンファイル、検索データに関する詳細を記録する

4 ：レベル 3 より詳細な動作フローを記録する

5 ：すべての情報を記録する

一般に、問題を分析する際には、レベル 5 を選択してすべてのデバッグ情報を収集することをお勧めします。

KernelDebugLevel

ServerProtect のカーネルレベル部分に対するデバッグ情報のレポートレベルを指定します。このパラメータを 0 以外の値に設定すると、ServerProtect の動作に関する追加メッセージがシステムの syslog.conf(5)に記録されます。有効な値は次のとおりです。

0 ：デバッグ出力なし (初期設定)

1 ：ログ関数のエントリおよび関連する名前 / パスのみ

2 ：レベル 1 より詳細なプロセス ID に関する情報、関数のリターンコード、およびクラスメンバーの関数とデータメンバーの値に関する詳細を記録する

3 ：すべての情報を記録する

一般に、問題を分析する際には、レベル 3 を選択してすべてのデバッグ情報を収集することをお勧めします。このキーは、syslog.conf ファイル (初期設定では /var/log/messages) に指定されているファイルにシステムロガーによって記録される情報に対してのみ動作します。デバッグのログを有効または無効にするには、105 ページの「デバッグログ」を参照してください。

ControlManagerDebug

値の範囲は 0 ～ 3 です。0 は「無効」を表します。初期設定は 1 です。詳細については、107 ページの表 6-1、「tmsplx.xml で編集可能なデバッグレベル」を参照してください。

MaxCacheItem

このキーは変更しないでください。

MaxListItem

このキーは変更しないでください。

MaxDirItem

このキーは変更しないでください。

MaxExtItem

このキーは変更しないでください。

MaxExcDirItem

このキーは変更しないでください。

MaxExcFilItem

このキーは変更しないでください。

MaxExcExtItem

このキーは変更しないでください。

WaitqTimeout

このキーは変更しないでください。

VsapiTimeout

このキーは変更しないでください。

MaxExcPid

このキーは変更しないでください。

MaxVscPid

このキーは変更しないでください。

MaxPathLen

このキーは変更しないでください。

MaxCmdLen

このキーは変更しないでください。

Lang

このキーは変更しないでください。

SessionTimeout

Web コンソールのセッションタイムアウト値を秒数で指定します。初期設定は、1200 秒 (20 分) です。

[GUIPassword] グループのキー

user1

このキーは変更しないでください。

BypassLocalLogin

このキーでは、ローカルコンピュータにログオンする場合にパスワードの入力なしに管理者ログオンを許可するように設定します。初期設定は 0 です。

0 ：ローカルログオンのパスワード入力を省略しない

1 ：ローカルログオンのパスワード入力を省略する

[Logs] グループのキー

[Logs] グループのキーでは、ServerProtect ログファイルの保存場所およびログファイルの削除の頻度を管理します。ログのサイズが大きくなり過ぎないよう配慮しながら、セキュリティイベントを追跡するために必要な履歴を十分保存できるようにログを管理する必要があります。

ServerProtect では、コマンドラインに「./splxmain -g」と入力することにより指定されるスケジュールに従ってログディレクトリが削除されます (/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp フォルダ内)。Schedule キーの値を 0 に設定すると、ログの自動削除を無効にすることができます。管理者によっては、ログファイルを削除する前に CD やその他のメディアに保存できるよう、手動でログファイルを削除する場合もあります。

注意： ログファイルのサイズは非常に大きくなるため、ディスク領域を圧迫しないよう定期的に削除する必要があります。

splxmain -g コマンドが自動または手動で実行されると、MaxLogDay キーで指定された日数を経過したログが削除されます。

Schedule

このキーでは、ログの自動削除の周期を指定します。有効な値は次のとおりです。

0 ：ログファイルの自動削除を無効にする

1 ：有効にする (初期設定)

ScheduledTime

このキーでは、ログ削除の時刻を 24 時間制で指定します。初期設定は 02:00:00 (午前 2 時) です。

LogDirectory

このキーでは、ServerProtect のすべてのログファイル (検索ログ、ウイルスログ、システムログ) が保存されるディレクトリのフルパスを指定します。初期設定は次のとおりです。

/var/log/TrendMicro/SProtectLinux

MaxLogDay

このキーでは、ログを削除するまで ServerProtect に保存する日数を指定します。有効な値は 1 ～ 1000 です。初期設定は 60 です。

注意： 新規ユーザが誤って履歴を削除してしまわないように、このキーの初期値は大きく設定されています。しかし、ログファイルを 1 週間ごとにバックアップして、MaxLogDay キーの値を小さくすることをお勧めします。

MaxRetrieveCount

このキーを使用して、取得するログエントリの最大数を指定します。ServerProtect リリース 2.5 以前では、Web コンソールの画面に表示できるエントリは 1,000 件のみでした。本リリースでは、tmsplx.xml ファイルでこのパラメータに 200 ～ 65535 の数値を指定することにより、この制限を変更することができます。初期設定は、以前のリリースと同じ 1000 です。

注意： この制限は、Web コンソールからログを参照する場合のみ適用されます。ログが削除されていない限り、ファイルを直接表示すればすべてのエントリを参照できます。
MaxRetrieveCount キーの値が小さすぎると、[Summary] 画面のウイルス / グレーウェアのログの合計数が実際の数よりも少なくなります。

Web コンソールでは、1 ページに表示するログエントリの数も指定できます。有効な値は、15、25、30、50、100、および 200 です。

[Registration] グループのキー

このグループのキーでは、製品の登録とアクティベーションで使用するデータを指定します。

EnableScheduledOnlineUpdateLicense

このキーでは、ライセンスの予約アップデートを ServerProtect でアクティベートするかどうかを指定します。有効な値は次のとおりです。

0 ：ライセンスの予約アップデートを無効にする

1 ：ライセンスの予約アップデートを有効にする (初期設定)

ScheduledTime

このキーでは、ライセンスの予約アップデートの時間 (HH:MM:SS (時 : 分 : 秒)) を設定します。初期設定の時間は 01:30:00 です。

PrServerRegisterURL

このキーでは、アクティベーションコードを取得するための製品登録機能の URL を指定します。このキーは変更しないでください。

PrServerOnlineUpdateURL

このキーでは、オンラインのアップデートに使用する URL を指定します。このキーは変更しないでください。

PrServerRenewInstrURL

このキーでは、製品ライセンスの更新手順にアクセスするための URL を指定します。このキーは変更しないでください。

PrServerUpgradeInstrURL

このキーでは、製品ライセンスのアップグレード手順にアクセスするための URL を指定します。このキーは変更しないでください。

PrServerViewLicenseURL

このキーでは、製品ライセンスの詳細情報にアクセスするための URL を指定します。このキーは変更しないでください。

EnableProxy

このキーでは、Source キーまたは DefaultSource キーで指定したアップデート URL へのアクセスにプロキシサーバを使用するかどうかを指定します。有効な値は次のとおりです。

0 ：プロキシサーバを使用しない (初期設定)

1 ：プロキシサーバを使用する

UseProxy キーの値を 1 に設定した場合、プロキシサーバのアドレスを指定する必要があります。また、必要に応じてユーザ名、パスワード、およびポート番号も指定する必要があります。

ProxyServer

このキーでは、プロキシサーバの FQDN または IP アドレスを指定します。初期設定は null です。次に例を示します。

proxy.example.com

ProxyType

このキーでは、プロキシサーバの種類を設定します。

0 ：HTTP プロキシ (初期設定)

1 ：Socks4 プロキシ

2 ：Socks5 プロキシ

ProxyPort

このキーでは、プロキシサーバのポート番号を指定します。初期設定は null です。

ProxyUserID

プロキシサーバで認証が必要な場合、このキーのユーザ名が使用されます。初期設定は null です。

ProxyPassword

プロキシサーバで認証が必要な場合、このキーのパスワードが使用されます。初期設定は null です。

SessionTimeOut

このキーでは、Web サーバへの接続を終了するまでに待機する秒数を設定します。0 より大きな値を設定する必要があります。初期設定は 10 秒です。

[WVTP] グループのキー

このグループのキーでは、ServerProtect がウイルストラッキングプログラム (WVTP) に使用するデータを指定します。

EnableWVTP

このキーでは、ServerProtect コンピュータがウイルストラッキングプログラムに参加するかどうかを指定します。

- **0 ：無効にする**
- **1 ：有効にする (初期設定)**

CountryCode

このキーは変更しないでください。

ServiceURL

このキーは変更しないでください。

ScheduledTime

このキーは変更しないでください。

設定ファイルをバックアップし、確認する

ServerProtect の設定を変更するときは、設定ファイルのバックアップコピーを作成してください。その際、次の方法でファイルに名前を付けることをお勧めします。

tmsplx.xml － 現在の設定ファイル
tmsplx.xml.bak － 最新のバックアップ (tmsplx.xml の最新アップデートの前)
tmeplx.xml.template －設定ファイルのテンプレート

tmsplx.xml ファイルのキー値が間違っていないことを確認するには、次の手順に従ってください。

コマンドラインで次のように入力します。

```
/opt/TrendMicro/SProtectLinux/SPLX.util/xmlvalidator
```

RemoteInstall.conf

次の表に、RemoteInstall.conf ファイルのキーの概要を示します。各キーの初期設定、および変更可能かどうかも記載しています。

キー	初期設定	説明
DeployOption	1	1 ：ServerProtect パッケージの配信とインストール。 2 ：ServerProtect 設定ファイルの配信。 3 ：KHM モジュールの配信。
Package Name	SProtectLinux-3.0.bin	パッケージ配信用の ServerProtect インストールファイルのパスを指定します。
Activation Code/SerialNumber	(なし)	ServerProtect のインストール時のアクティベーションコード。パッケージを配信するときに使用します。
ConfigFilePath*	config/tmsplx.xml	設定ファイルのパスを指定します。設定ファイルを配信するときに使用します。
XMLvalidatorPath	config/xmlvalidator	XMLvalidator スクリプトパスを指定します。設定ファイルを配信するときに使用します。
XMLdeployerPath	config/xmldeployer	XMLdeployer プログラムのファイルパスを指定します。設定ファイルを配信するときに使用します。
KHMPath	KHM.module/RHEL4/splxmod-2.6.9-22.0.2.ELsmp.o	KHM ファイルのパスを指定します。KHM を配信するときに使用します。一度に配信できる KHM ファイルは 1 つだけです。
ConnectTimeOut	30	ssh サーバに接続する際、初期設定のシステム TCP タイムアウトの代わりに使用するタイムアウト (秒数) を指定します。接続先がダウンしているか、到達不可能な場合のみ使用されます。接続を拒否された場合は使用されません。
ConnectRetry	2	ssh 接続の再試行間隔を指定します。

* この初期設定値を使用することをお勧めします。

表 B-1. RemoteInstall.conf のキー、初期設定、および説明

キー	初期設定	説明
AliveInterval*	30	サーバからデータを受信しない状態が続いた場合に、ssh が暗号化チャネル経由でメッセージを送信し、サーバに応答を要求するまでのタイムアウト時間を秒数で設定します。このオプションはプロトコルバージョン 2 にのみ適用されます ssh_config の man ページをキーワード ServerAliveInterval で参照してください。
AliveCountMax	2	サーバから ssh へメッセージが返送されない場合に送信できる、サーバ生存確認メッセージの数を設定します。サーバ生存確認メッセージは、TCPKeepAlive とまったく異なります。 サーバ生存確認メッセージは暗号化チャネル経由で送信されるので、なりすましの心配がありません接続の可能 / 不可能をサーバまたはクライアントが把握している必要がある場合に、サーバ生存確認機能が役立ちます。 ssh_config の man ページのキーワード ServerAliveCountMax を参照してください。
* この初期設定値を使用することをお勧めします。		

表 B-1.　RemoteInstall.conf のキー、初期設定、および説明

キー	初期設定	説明
ResponseTimeOut	120	クライアントが応答するまでの許容待機時間。
Debug	0	有効な値は 0 (デバッグモードが無効)、および 1 (有効) です。デバッグモードを有効にした場合は、syslog.conf ファイルで以下のエントリを設定してください。 1.syslogd の設定ファイル /etc/syslog.conf で、ServerProtect のエントリを設定します。 #Save boot messages also to boot. loglocal7.* /var/log/boot.log local6.* < デバッグログの出力先 > * この行を追加 2.syslogd (Red Hat) または syslog-ng (SUSE) の PID を確認します。 3. 次のコマンドを実行して、syslogd または syslog-ng の設定を再度読み込みます。 kill -HUP <PID>
StatusFile	splx_remote_status	配信ステータスを格納するファイルの名前を指定します。
FullStatus*	1	詳細な配信ステータスを StatusFile に記録します。
SuccessList	splx_success_list	配信に成功したクライアントのリストを格納するファイル名を指定します。
FailedList	splx_failed_list	配信に失敗したクライアントのリストを格納するファイル名を指定します。
* この初期設定値を使用することをお勧めします。		

表 B-1. RemoteInstall.conf のキー、初期設定、および説明

注意： この初期設定値を使用することをお勧めします。

splxmain

splxmain コマンドを使用して、コマンドラインから ServerProtect を保守管理できます。/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp フォルダでこのコマンドを実行できます。cron(8)または crond(8)で実行するさまざまな ServerProtect 管理タスク、およびコマンドラインから実行できるさまざまな ServerProtect 管理タスクで、splxmain を使用します。splxmain を実行するには root (スーパーユーザ) の権限が必要です。

注意： splxmain コマンドは、Apache サーバを経由せずに ServerProtect を実行する場合のみ使用してください。

splxmain は、ServerProtect で検索、ログ機能、アップデートなどを実行する際のプロセスを制御します。

場所 :

```
/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp/splxmain
```

構文:

```
splxmain [-a |-b |-c |-e |-f |-g < 日付 > |-i |-j |-k |-l < ポート > |-m < ディレクトリ > |-n |-o |-q < アクティベーションコード > |-r |-s |-t |-u |-v |-w < ポート > |-W |-x |-y][-D |-E]
```

注意： -D を除き、一度に指定できる引数は 1 つだけです。

引数:

-a ：すべての vsapiapp プロセス、手動検索プロセス、予約検索プロセスを正規の手順で終了します。これらのプロセスを即座に終了するには、-k オプションを使用します。

-b ：すべての予約ジョブを /etc/cron.d/splx ファイルから削除します。現在実行中のジョブは、そのまま最後まで実行されます。

-c ：/etc/cron.d/splx の予約検索、予約アップデート、および予約ログ削除の設定を tmsplx.xml ファイルの設定に基づいて更新します。

-e ：tmsplx.xml(5) 設定ファイルを読み込み、予約検索、予約アップデート、およびログの自動削除を実行するための /etc/cron.d/splx を設定して、vsapiapp を起動します。-D オプションも指定した場合は、vsapiapp がデーモンとして実行されます。それ以外の場合は通常のプロセスとして実行されます。-D オプションは、このオプションと合わせて使用できます。

注意： -e と共に -D オプションを使用した場合、vsappiapp はデーモンとして実行されます。それ以外の場合は通常のプロセスとして実行されます。

-f ：Web コンソールのパスワードを初期設定 (パスワードなし) に戻します。Web コンソールのパスワードを忘れてしまったときは、このオプションを使用して初期設定に戻した後、-j オプションで新しいパスワードを設定してください。

-g < 日付 > ：ServerProtect のログファイルを削除します。< 日付 > には、削除を実行する日付を YYYY-MM-DD 形式で指定します。次に例を示します。

```
./splxmain -g 2006-04-21 # 2006 年 4 月 21 日より前に
書き込まれたログを削除
```

注意： < 日付 > を省略した場合は、tmsplx.xml ファイルの MaxLogDay キーで指定した値が使用されます。218 ページの「MaxLogDay」参照を参照してください。

-i ：vsapiapp プロセスを再起動します。

-j ：Web コンソールのパスワードを設定します。新しいパスワードを確認のために 2 回入力します。

-k ：SIGKILL シグナルを送信して、vsapiapp プロセス、手動検索プロセス、および予約検索プロセスをただちに終了します。これらのプロセスを正規の手順で終了するには、-a オプションを使用します。

-l < ポート > ：ServerProtect Web コンソールへのアクセス時に使用する ServerProtect HTTP ポートを設定します。
たとえば、./splxmain -l xxxxx のように指定します。

-m < ディレクトリ > ：tmsplx.xml ファイルの手動検索設定に基づいて、手動検索を実行します。複数のディレクトリに対して手動検索を実行するには、ディレク

トリをコロン (:) で区切ります。たとえば、/temp1 と /temp2 を検索する場合は次のように指定します。

```
./splxmain -m /temp1:/temp2
```

注意： 手動検索を実行するために KHM を起動する必要はありません。

-n ：現在実行している手動検索プロセスを終了します。

-o ：/etc/cron.d/splx ファイルから予約検索プロセスを削除します。

-p ：予約アップデートプロセスを開始します。

-q < アクティベーションコード > ：アクティベーションコード / シリアル番号を設定します。

-r ：vsapiapp を再起動せずに、ServerProtect の設定を再ロードします。

-s ：予約検索を今すぐ実行します。通常は、-m オプションを使用して手動検索を実行します。ただし、このオプションを /etc/cron.d/splx で使用すれば、tmsplx.xml ファイルで指定されている予約検索の設定に基づいて手動検索を実行できます。

注意： 予約検索を実行するために KHM を起動する必要はありません。

-t ：cron または crond で実行されている予約検索プロセスを終了します。予約設定は、/etc/cron.d/splx ファイルで確認できます。

-u ：tmsplx.xml に基づいて検索エンジンとウイルスパターンファイルをアップデートし、これらのコンポーネントを再ロードするよう vsapiapp に要求します。

-v ：リアルタイム検索用の子スレッドを生成することによって、リアルタイム検索を有効にします。このオプションは、前に -x オプションを使用してリアルタイム検索を無効にしている場合にのみ使用してください。

注意： このオプションを設定するとリアルタイム検索の設定がリセットされ、ServerProtect はウイルス / 不正プログラムに対して「入力ファイル」のみチェックするようになります。

-w < ポート > ：ServerProtect Web コンソールへのアクセス時に使用する HTTPS ポートを設定します。次に例を示します。

```
./splxmain -w 12345
```

-W ：ウイルストラッキングプログラム (WVTP) を設定します。この機能を有効または無効にするには、「yes」または「no」と入力します。

-x ：リアルタイム検索の子スレッドを終了して、リアルタイム検索を無効にします。

-y ：コンポーネントのダウンロード時に使用するプロキシサーバのユーザ名とパスワードを設定します。

-D ：vsapiapp を強制的にデーモンとして実行します。このオプションは -e と共に使用できます。

-E ：現在のライセンスのステータスに対してクエリを実行します。

この情報は splxmain man ページでも参照できます。splxmain man ページを表示するには、コマンドラインから次のコマンドを実行します。

```
man splxmain
```

splx

splx スクリプトを使用して、ServerProtect を有効または無効にします。

場所:

```
/etc/init.d/
```

構文:

```
splx {start|stop|restart|status}
```

引数:

```
start
```

ServerProtect サービスと ServerProtect Apache サーバを起動します。

```
stop
```

ServerProtect サービスと ServerProtect Apache サーバを停止します。

```
restart
```

ServerProtect サービスと ServerProtect Apache サーバを再起動します。

```
status
```

有効なすべての ServerProtect 本体のサービス、および Control Manager への登録状態が表示されます。

splxcore

ServerProtect 用 Apache サーバ (splxhttpd) を経由しないで ServerProtect を実行するには、splxcore スクリプトを使用します。

注意： splxcore スクリプトの ServerProtect 管理機能はコマンドラインからのみ使用できます。Web コンソールからは使用できません。ServerProtect をインストールした後の製品登録やログ検索など、一部の機能についてはコマンドラインから実行できません。

場所:

```
/etc/init.d/
```

構文:

```
splxcore {start|stop|restart|status}
```

引数:

```
start
```

ServerProtect 本体のサービスを起動します。

```
stop
```

ServerProtect 本体のサービスを停止します。

```
restart
```

ServerProtect 本体のサービスを再起動します。

```
status
```

現在有効な ServerProtect 本体のサービスの稼働状況が表示されます。

splxhttpd

ServerProtect 用 Apache サーバを有効または無効にするには、splxhttpd スクリプトを使用します。

場所:

```
/etc/init.d/
```

構文:

```
splxhttpd {start|stop|restart|status}
```

引数:

```
start
```

ServerProtect 用 Apache サーバを起動します。

```
stop
```

ServerProtect 用 Apache サーバを停止します。

```
restart
```

ServerProtect 用 Apache サーバを再起動します。

```
status
```

現在有効な ServerProtect 用 Apache プロセスが表示されます。

splxcomp

splxcomp は、Trend Micro InterScan VirusWall (以下、InterScan VirusWall)、Trend Micro InterScan Web Security Suite (以下、IWSS)、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS)、および ServerProtect を同じサーバにインストールした場合に、不要な検索が実行されないようにするためのツールです。

splxcomp スクリプトは、/opt/TrendMicro/SProtectLinux/SPLX.util フォルダに配置されています。

splxcomp を使用すると、InterScan VirusWall、IWSS、または InterScan MSS の隔離ディレクトリおよびバックアップディレクトリを特定して、除外リストに追加できます。

注意： InterScan VirusWall、IWSS、または InterScan MSS を ServerProtect コンピュータからアンインストールした場合は、対応する隔離ディレクトリおよびバックアップディレクトリも除外リストから削除する必要があります。これによって、使用されていないディレクトリのウイルス / スパイウェアによる感染を阻止します。

構文:

```
splxcomp {-h} {-v} {-i}
```

引数:

-h ：このツールの引数を一覧表示します。

-v ：バージョン情報を表示します。

-i ：IWSS の重要な設定を取得します。

CMconfig

CMconfig コマンドを使用して、ServerProtect を Control Manager に登録したり、Control Manager から登録を解除したりします。

CMconfig ユーティリティでは、ServerProtect が Control Manager に登録されているかどうかを検出します。ServerProtect が現在 Control Manager に登録されている場合は、CMconfig によって登録が解除されます。そうでない場合は、コマンドラインへの設定情報の入力を求めるプロンプトを表示し、ServerProtect を Control Manager に登録します。

または、ファイルに設定を保存し、-f オプションを使用して CMConfig コマンドが設定情報を取得するファイルの名前を指定することもできます。初期設定のテンプレートファイル tmcm_registration_template.ini には、設定パラメータがすべて含まれています。

場所:

```
/opt/TrendMicro/SProtectLinux/SPLX.util
```

構文:

```
CMconfig [-h] [-f] [-Q] [-P]
```

引数:

-f < **入力ファイル** > ：Control Manager **に登録するための設定を入力ファイルから取得します。**

-Q ：Control Manager **エージェントのステータスに対してクエリを実行します。**

-P ：Control Manager **の** Web **サーバ認証のユーザ名 / パスワードを指定します。**

-h ：**このツールの引数を一覧表示します。**

注意： プロキシの種類を指定するには、Agent.ini ファイル (/opt/TrendMicro/SProtectLinux/ フォルダに配置) の Proxy_Type パラメータを変更してから、CMconfig コマンドを使用して ServerProtect を Control Manager に登録します。

Apache 設定ファイル

ServerProtect では、ServerProtect 用にカスタマイズされた Apache サーバを使用します。そのための設定ファイルは、次の場所にあります。

/opt/TrendMicro/SProtectLinux/SPLX.httpd/conf/splxhttpd.conf

警告： ServerProtect 用の Apache 設定ファイルを変更すると、予期しないエラーが発生する場合があります。このファイルは変更しないことをお勧めします。変更が必要な場合は、splxhttpd.conf のバックアップを作成してください。splxhttpd.conf を編集するときは、詳しい方法をトレンドマイクロテクニカルサポートへお問い合わせください。

Apache ログファイル

ServerProtect Apache サーバのログファイルは、次のディレクトリにあります。

/opt/TrendMicro/SProtectLinux/SPLX.httpd/logs/

用語集

この用語集では、本マニュアルやオンラインヘルプで使用される専門用語について説明しています。

用語	説明
?	検索の対象または対象外にするディレクトリを指定する際に、ワイルドカードとして使用できる文字です。
BIG 5	繁体字中国語をエンコードするために台湾や香港で使用される文字エンコード方式です。詳細については、次の Web サイトを参照してください。 http://ja.wikipedia.org/wiki/BIG5
CMconfig	ServerProtect を Trend Micro Control Manager に登録したり、登録を解除したり、再登録したりできる ServerProtect のコマンドラインユーティリティです。
ELF	Executable and Linkable Format の略であり、UNIX および Linux プラットフォーム用の実行可能ファイル形式です。
EUC-KR	韓国語に使用される 8 ビットの文字エンコード方式です。詳細については、次の Web サイトを参照してください。 http://ja.wikipedia.org/wiki/EUC#.E9.9F.93.E5.9B.BD.E8.AA.9EEUC
EXE ファイル感染ウイルス	ファイル拡張子 .exe を持つ実行可能なプログラムです。
FTP	TCP/IP ネットワークを介してコンピュータ間でファイルを転送するためのクライアント / サーバ型プロトコルです。または、ファイルを転送するためのクライアントプログラムを指すこともあります。

用語	説明
GB 2312	中国本土とシンガポールで簡体字中国語用に使用される文字エンコード方式です。詳細については、次の Web サイトを参照してください。 http://ja.wikipedia.org/wiki/GB_2312
HTML ウイルス	Web ページを作成するための言語である HTML (ハイパーテキストマークアップ言語) を標的にしたウイルスです。このウイルスは Web ページ内に潜んで、ユーザのブラウザを介してダウンロードされます。
HTTPS	Hypertext Transfer Protocol Secure の略であり、トランザクションを安全に処理できるように HTTP を拡張したプロトコルです。
In-the-Wild ウイルス	現在実際に広まっている既知のウイルスのことです。
IP	インターネットプロトコルです。「IP アドレス」を参照してください。
IP アドレス	ネットワーク上のデバイスのインターネットアドレスです。通常は、「192.168.10.1」のようにドットで区切って表記されます。
ISO-2002-JP	日本語用に幅広く使用されている文字エンコード方式です。詳細については、次の Web サイトを参照してください。 http://ja.wikipedia.org/wiki/ISO-2022-JP
ISO-8859-1	単一の 8 ビットコードを使用してアルファベット文字を表す文字エンコード言語です。ISO-8859-1 は、多数のヨーロッパ言語をサポートしています。詳細については、次の Web サイトを参照してください。 http://en.wikipedia.org/wiki/Iso-8859-1

用語	説明
Java Runtime Environment (JRE)	Java プログラミング言語で記述されたアプレットやアプリケーションを実行するのに必要な、Java 仮想マシン、一連のクラスライブラリ、およびその他のコンポーネントです。JRE には、Java プラグインおよび Java Web Start も含まれており、これらによって、Java アプリケーションを複雑なインストール手順を実行せずに起動できます。詳細については、次の Web サイトを参照してください。http://java.sun.com
Konquerer デスクトップ環境 (KDE)	KDE は、UNIX プラットフォーム向けの使いやすい多国語に対応したデスクトップ環境であり、統合されたヘルプシステム、アプリケーションの一貫性のある外観と操作感、統一されたメニューとツールバー、および有用なアプリケーションを提供します。ServerProtect の Quick Access コンソールを使用するには、KDE バージョン 3.2 以上が必要です。KDE の詳細については、次の Web サイトを参照してください。http://www.kde.gr.jp/
Latin-1	ServerProtect で利用可能な 6 種類の文字セットの 1 つです。「ISO-8859-1」も参照してください。
MacroTrap	文書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方式により調べるトレンドマイクロのユーティリティです。通常はマクロウイルスコードは、多くの文書と共に送信される目に見えないテンプレート (Microsoft Word 文書内の .dot ファイルなど) の一部に含まれています。MacroTrap は、ウイルスの活動に似た処理を実行する主要な命令を探し出して、このようなテンプレートにマクロウイルス感染の兆候がないか確認します。たとえば、テンプレートの一部を他のテンプレートにコピー (増殖) する命令や、被害を及ぼす可能性のあるコマンド (破壊) を実行する命令などを探します。
Quick Access コンソール	KDE にインストールされたメニューおよび ServerProtect コマンドラインに相当するものです。

用語	説明
Red Hat Enterprise Linux 4	Red Hat によって開発されているオープンソースの OS です。詳細については、次の Web サイトを参照してください。 http://www.jp.redhat.com/
RemoteInstall	ServerProtect をリモートコンピュータにインストールしたり、リモートコンピュータ上の KHM をアップデートしたり、.CSV 形式の結果ファイルを RemoteInstall.conf 形式に変換したり、リモートコンピュータ上の ServerProtect の設定をアップデートしたりするための ServerProtect の付属ユーティリティです。
RemoteInstall.conf	RemoteInstall ユーティリティの設定ファイルです。
Samba	Samba は、ファイルサービスと印刷サービスを提供するオープンソースのソフトウェアスイートです。これらのサービスにより、Windows 以外のプラットフォームで実行されているホストであっても、Windows のファイルサーバや印刷サーバと同じように、Windows のクライアントやサーバとやり取りできるようになります。詳細については、次の URL を参照してください。 http://us5.samba.org/samba/
Secure Sockets Layer (SSL)	Netscape によって開発されたプロトコルであり、アプリケーションプロトコル (HTTP、Telnet、FTP など) と TCP/IP の間にデータセキュリティの階層を確保します。このセキュリティプロトコルは、データの暗号化、サーバ認証、メッセージの完全性、および TCP/IP 接続時のオプションのクライアント認証を実現します。
SNMP	Simple Network Management Protocol の略であり、ネットワークに接続されたデバイス上で管理者の対処が必要な状態が発生しているかどうかを監視するためのプロトコルです。
SNMP トラップ	トラップとは、コンピュータプログラム内で発生するエラーなどの問題を処理するプログラミングメカニズムのことです。SNMP トラップは、ネットワークデバイスの監視に関連するエラーを処理します。 「SNMP」を参照してください。

用語	説明
Squid	オープンソースのプロキシサーバおよび Web キャッシュサーバです。
SUSE LINUX Enterprise Server 9	Novell によって開発されているオープンソースの OS です。詳細については、次の Web サイトを参照してください。http://www.novell.co.jp/
TCP	Transmission Control Protocol の略。TCP は、通常は IP (インターネットプロトコル) と組み合わせて使用されるネットワークプロトコルであり、コンピュータシステムのインターネット接続を制御します。
Telnet	TCP/IP (Transmission Control Protocol/Internet Protocol) の上位層で動作するリモートログオンのためのインターネット標準プロトコルです。この用語は、リモートログオンセッションの端末エミュレータとして機能するネットワークソフトウェアを指す場合もあります。
US-ASCII	現代英語およびその他の西ヨーロッパ言語で使用される文字エンコード方式です。詳細については、次の Web サイトを参照してください。http://ja.wikipedia.org/wiki/American_Standard_Code_for_Information_Interchange
VBscript ウイルス	VBscript (Microsoft Visual Basic スクリプト言語) は、ブラウザに表示される HTML ページにインタラクティブ機能を追加できる簡単なプログラミング言語です。たとえば、開発者は VBscript を使用して、Web ページに「詳細についてはここをクリック」というボタンを追加できます。 VBscript ウイルスは、HTML コード内のこれらのスクリプトを標的とするウイルスです。このため、このウイルスは Web ページに潜んで、ブラウザを介してダウンロードされることでユーザのデスクトップへ侵入できます。

用語	説明
Zip of Death	圧縮解除時に巨大化 (10 倍など) して展開される zip (またはアーカイブ) ファイルの一種、または多数の添付ファイルが含まれた zip ファイルです。圧縮されたファイルは、検索時に圧縮解除する必要があります。巨大なファイルは、ネットワークの速度を低下させたり機能を停止させたりすることがあります。
アクセス	データをコンピュータやサーバなどの記憶装置から読み取ったり、記憶装置に書き込んだりすることです。
アクセス権	データを読み書きする権限です。ほとんどの OS では、ユーザの職務に応じて異なるレベルのアクセス権を定義できます。
アクティベーション	アクティベーションコードを入力してソフトウェアの機能を有効にすることです。トレンドマイクロ製品は体験版としてインストールされるため、インストール中またはインストール後に管理コンソールの [Product License] 画面でアクティベーションを実行します。
アクティベーションコード	トレンドマイクロ製品をアクティベートするためのハイフンを含めて 37 桁のコードです。アクティベーションコードの例 : 9U-HG53-857B-TD54-MMP8-7754-MPP0 「レジストレーションキー」も参照してください。
アップデート	アップデートは、多くのトレンドマイクロ製品に共通の機能です。トレンドマイクロのアップデート Web サイトと連係したアップデートは、インターネットを通じて、最新のパターンファイル、検索エンジン、およびプログラムファイルを提供します。
イントラネット	組織外のインターネットと類似したサービスを組織内で提供するネットワークのことですが、必ずしもインターネットに接続されていません。

用語	説明
ウイルスのシグニチャ	ウイルスのシグニチャは、特定のウイルスを識別するための一意のビット列です。ウイルスのシグニチャは、トレンドマイクロのウイルスパターンファイルに保存されています。トレンドマイクロの検索エンジンは、メールメッセージの本文や HTTP ダウンロードファイルの内容といった、ファイル内のコードをパターンファイル内のシグニチャと比較します。一致するシグニチャがあれば、ウイルスが検出され、セキュリティポリシーに従って駆除、削除、隔離などの処理が実行されます。
カーネルフックモジュール (KHM	ServerProtect とお使いのバージョンの Linux OS 間をリンクするメカニズムです。
グレーウェア	合法的であるが、不要または有害なソフトウェアのことです。ウイルス、ワーム、トロイの木馬などのセキュリティ侵害要因と異なり、グレーウェアは、データに感染したり、データを複製したり破壊したりしませんが、ユーザのプライバシーを侵害することがあります。グレーウェアの例としては、スパイウェア、アドウェア、リモートアクセスツールなどがあります。
シグニチャ	「ウイルスのシグニチャ」を参照してください。
ジョークプログラム	警告を繰り返し表示するなどしてユーザを邪魔することを目的とした実行可能プログラムです。ウイルスとは異なり、ジョークプログラムは自己増殖せず、システムから削除すれば解決します。
ダメージルーチン	ウイルスコードの破壊的な部分であり、ペイロードとも呼ばれます。
デーモン	直接呼び出されるのではなく、休止状態のまま特定の状態が発生するのを待っているプログラムです。その状態の発生元は、デーモンが潜在的に待機していることを認識する必要はありません。
デジタル署名	公開鍵暗号化と呼ばれる技術を使用して送信者やメッセージデータを識別して認証するための、メッセージに付加された特別なデータです。

用語	説明
トリガ	何らかの処理を実行させる原因となるイベントです。たとえば、お使いのトレンドマイクロ製品がメールメッセージ内でウイルスを検出したとします。この検出イベントは、そのメッセージを隔離して、システム管理者、メッセージ送信者、およびメッセージ受信者に通知を送信する原因となる「トリガ」です。
トレンドマイクロの推奨処理	ウイルス、トロイの木馬、スパイウェア / グレーウェア、ジョークプログラムなどのセキュリティリスクに感染したファイルに対して実行される一連の事前設定された処理 (駆除、削除、隔離など) のことです。
トレンドマイクロの推奨設定	ファイルのヘッダを調べて実際のファイルタイプを判断し、不正プログラムコードが潜んでいる可能性のあるファイルタイプのみを検索することで、パフォーマンスを最大限に高めるトレンドマイクロの検索テクノロジです。実際のファイルタイプを判断することで、無害な拡張子を使用して偽装している不正プログラムコードを発見するのに役立ちます。
トロイの木馬	無害なプログラムを装った不正プログラムです。トロイの木馬は、複製されない実行可能プログラムですが、その代わりに、システムに常駐して侵入者に対してポートを開くといった不正な処理を実行します。
ネットワークウイルス	TCP、FTP、UDP、HTTP などのネットワークプロトコルやメールプロトコルなどを使用して増殖するウイルスです。ネットワークウイルスは、通常は、ハードディスクのブートセクタやシステムファイルを改ざんすることはありません。その代わりに、これらのウイルスはクライアントコンピュータのメモリに感染して、ネットワークトラフィックを強制的に大量発生させることにより、ネットワークの速度を低下させたり機能を完全に停止させたりすることがあります。

用語	説明
パターンファイル (別名「オフィシャルパターンリリース」)	オフィシャルパターンリリース (OPR) とも呼ばれるパターンファイルは、識別されたウイルスの最新パターンをまとめたものです。パターンファイルは、一連の重要なテストに合格したことが保証されているため、最新のウイルス脅威に対する最大限のセキュリティを提供できます。このパターンファイルは、最新の検索エンジンと組み合わせて使用することで最大の効果をもたらします。
ファイル感染型ウイルス	ファイル感染型ウイルスは、実行可能なプログラム (一般に .com や .exe の拡張子を持つファイル) に感染します。このようなウイルスのほとんどは、他のホストプログラムに感染して増殖および拡散しようとするだけですが、場合によっては、オリジナルコードの一部を上書きして感染先のプログラムを意図せずに破壊してしまうこともあります。これらのウイルスのごく一部は非常に破壊的であり、あらかじめ指定された時間にハードドライブをフォーマットしようとしたり、他の不正な処理を実行しようとしたりします。 多くの場合、ファイル感染型ウイルスは感染ファイルから問題なく削除できます。ただし、ウイルスがプログラムコードの一部を上書きしている場合は、元のファイルは修復不能です。
フェイルオーバー	現在使用中のコンポーネントで障害が発生した場合に、予備のサーバ、システム、またはネットワークに自動的に切り替えるプロセスです。フェイルオーバーシステムは、アップデートなどの重要なサービスが継続的に必要になる場合に採用されます。
ヘッダ (ネットワークの定義)	ファイルや送信に関する透過情報が格納されたデータパケットの一部です。
ホスト	ネットワークに接続されたコンピュータです。
ポリモーフィック型ウイルス	さまざまな形態に変化できるウイルスです。

用語	説明
マクロ	アプリケーション内の特定の機能を自動化するためのコマンドです。
マクロウイルス	マクロウイルスは、多くの場合はアプリケーションマクロとしてエンコードされ、文書に組み込まれています。他のウイルスタイプとは異なり、マクロウイルスは OS に固有ではなく、メールの添付ファイル、Web からダウンロードしたファイル、ファイルの転送、連携アプリケーションなどを介して広まることがあります。
マスメール活動	大量のネットワークトラフィックを発生させることで、多大な被害をもたらす可能性のある不正プログラムです。
ライセンス証明書	トレンドマイクロ製品の認可されたユーザであることを証明する文書です。
レジストレーションキー	トレンドマイクロの顧客データベースに登録する際に使用するハイフンを含めて 22 桁のコードのことです。
ログ保管ディレクトリ	ログファイルを保管するためのサーバ上のディレクトリです。
ワーム	自己完結型プログラム (またはプログラムセット) であり、自身またはその一部と同じ機能を持つコピーを別のコンピュータシステムに拡散できます。
ワイルドカード	ディレクトリパスを指定する際に使用される記号であり、アスタリスク (*) は任意の文字列を表します。たとえば、/opt から 2 階層下の任意のディレクトリを指定するには「/opt/*/*」と入力します。この用語はトランプゲームに由来します。「ワイルドカード」と指定された特定のカードは、カードデッキの任意の数字カードまたは組札として使用できます。
隔離	ウイルスに感染した HTTP ダウンロードファイルや FTP ファイルなど、感染データをサーバ上の隔離されたディレクトリ (隔離ディレクトリ) に置くことです。
管理コンソール	トレンドマイクロ製品のユーザインタフェースです。

用語	説明
管理者アカウント	管理者レベルの特権を持つユーザ名とパスワードです。
共有ドライブ	複数のユーザによって使用されるコンピュータの周辺機器です。このため、ウイルス感染の危険性が高まります。
駆除	ファイルやメッセージからウイルスコードを除去することです。
警告	システムのユーザや管理者に、そのシステムの動作状態が変化したことや特定のエラー状態が発生したことを通知するためのメッセージです。
使用許諾契約書 (EULA)	使用許諾契約書 (EULA) は、ソフトウェア発行元とソフトウェアユーザの間で交わされる法的契約です。通常これは、ユーザ側の制限事項の概要を示します。ユーザは、インストール時に「同意する」をクリックしないことにより、この契約を拒否できます。「同意しない」をクリックすると、当然ながらソフトウェア製品のインストールは中止されます。多くのユーザは、特定のフリーソフトウェアをインストールする際に表示される使用許諾契約書のプロンプトで「同意する」をクリックして、そうとは気付かずにスパイウェアやアドウェアのインストールに同意しています。
実際のファイルタイプ	トレンドマイクロの推奨設定で使用されるウイルス検索テクノロジであり、ファイル名の拡張子 (偽装の可能性がある) を無視して、ファイルヘッダを調べることでファイルタイプを特定します。
受信ファイル	サーバに配置されるファイルです。
処理	ウイルスなどの不正プログラムが検出された際に実行される操作です。 処理とは通常、駆除、隔離、削除、放置 (とりあえず送信 / 転送する) を意味します。とりあえず送信 / 転送することはお勧めしません。ウイルスに感染したメッセージを送信したり、ウイルスに感染したファイルを転送したりすると、ネットワークのセキュリティが損なわれることがあります。

用語	説明
送信ファイル	サーバから別の場所へコピーまたは移動されるファイルです。
待機ポート	データ交換のためのクライアント接続要求に使用されるポートです。
中国語 (簡体字)	ServerProtect で利用可能な 6 種類の文字セットの 1 つです。「GB 2312」も参照してください。
中国語 (繁体字)	ServerProtect で利用可能な 6 種類の文字セットの 1 つです。「BIG5」も参照してください。
不正プログラム	ウイルス、ワーム、トロイの木馬など、危害を加える目的で開発されたプログラムやファイルです。
負荷分散	同時実行されるコンピュータ処理の効率を高めるために、これらの処理を複数のプロセッサに割り当てる (または再割り当てする) ことです。
複合感染型ウイルス	システム領域感染型ウイルスとファイル感染型ウイルスの両方の特徴を持つウイルスです。
複合型攻撃	「Nimda」や「Code Red」のように、企業ネットワークの複数の侵入点および脆弱点を利用する複雑な攻撃です。
複製	自己増殖することです。このマニュアルでは、ウイルスやワームが自己増殖できることを意味します。

索引

英数字

あ

か

さ

た

な

は

ま

や

ら