TREND MICRO

3.0 Trend Micro ServerProtect™ 管理者ガイド

Red Hat Enterprise Linux 9

Endpoint Security

※注意事項

複数年契約について

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

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

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

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

法人向け製品のサポートについて

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

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

商標について

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

P/N: SPEM39609/220921_JP (2022/12)

プライバシーと個人データの収集に関する規定

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

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

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

重要

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

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

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

目次

はじめに

第 1 章：製品について

第 4 章：アップデート

第 5 章：ログと通知

第 6 章：トラブルシューティング

第 7 章：テクニカルサポート

付録 A：設定コマンド

はじめに

Trend Micro ServerProtect for Linux (以下、ServerProtect) 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

本製品には、次のようなドキュメントが付属しています。

- オンラインヘルプ: 製品コンソールからアクセス可能な Web ベースのドキュメントです。

  ServerProtect の機能に関する説明が含まれます。

- man ページ (マニュアルページ): ServerProtect には、`splxmain`、`splx`、`tmsplx.xml`、`RemoteInstall`、および `CMconfig` に関する man ページが用意されています。詳細については、112 ページの「man ページへのアクセス」を参照してください。

- 管理者ガイド (本書): 使用方法および製品の管理について説明している PDF ドキュメントです。

- Readme ファイル: 他の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、機能の説明、インストールに関するヒント、既知の問題、製品のリリース履歴などが記載されています。

- 製品 Q&A: トレンドマイクロの全製品についての最新情報が含まれます。すでに回答済みのその他の質問や、最も多く寄せられる質問の動的なリストも表示されます。

  https://success.trendmicro.com/jp/technical-support

注意

最新のドキュメントおよび Readme ファイルは、次の Web サイトからダウンロードできます。https://www.trendmicro.com/ja_jp/business/products/downloads.html

---

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

情報を簡単に見つけ理解できるように、ServerProtect for Linux のドキュメントでは次の表記規則を使用しています。

表 1. ドキュメントの表記規則

表記規則	説明
 注意	設定に関する注意事項または推奨事項を示します。
 ヒント	ベストプラクティス情報およびトレンドマイクロの推奨事項を示します。
 警告!	ネットワーク上のコンピュータに害を及ぼす可能性のあるアクティビティについて 警告を示します。

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。

主要な機能

以下では、ServerProtect for Linux の主な機能を説明します。

Trend Micro Apex Central または Trend Micro Control Manager からの ServerProtect の管理

Trend Micro Apex Central (以下、Apex Central) (旧称: Trend Micro Control Manager (以下、Control Manager)) は、ServerProtect をはじめとするトレンドマイクロの製品やサービスを管理する中央管理コンソールです。Apex Central/Control Manager に登録すると、ServerProtect で次の機能を利用できるようになります。

- Apex Central/Control Manager から参照可能な各種レポート

注意

このマニュアルで言及している Control Manager のすべての機能と設定は、Apex Central にも適用されます。

ServerProtect では、次のバージョンの Apex Central/Control Manager がサポートされま す。

- Apex Central 2019 以降
- Control Manager 7.0 以降

Apex Central/Control Manager から参照可能な各種レポート

Apex Central/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

Apex Central/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、Apex Central/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、Mozilla Firefox、Microsoft Edge、または Google Chrome 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、62 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、69 ページの「ダウンロード元を指定する」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。

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、149 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、99 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、32 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。

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

本バージョンでの新機能は次のとおりです。

機能	説明
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 5.14 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 9

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。

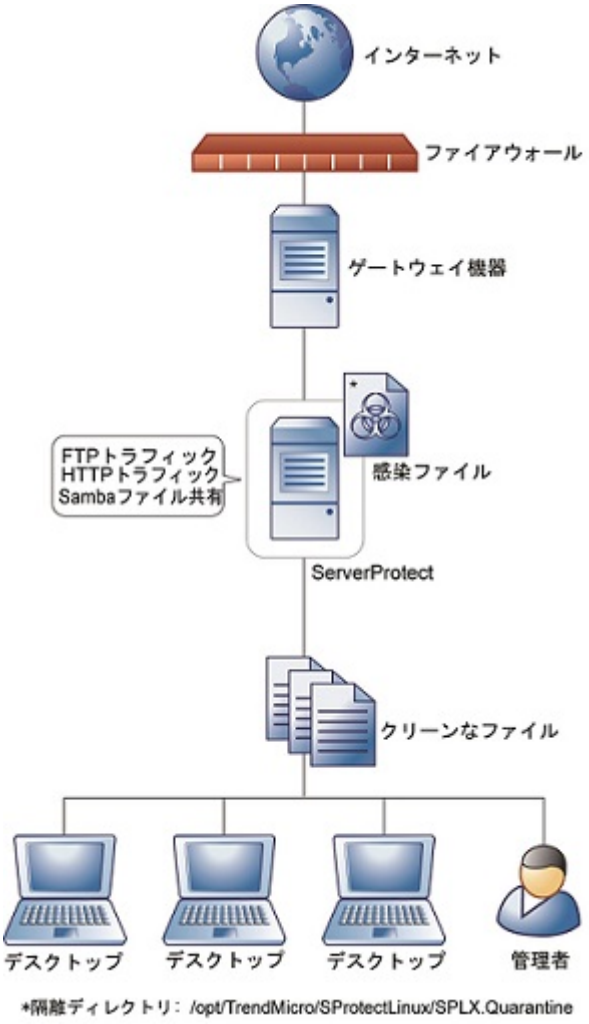


図 1-1. ServerProtect の仕組み

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。

- 対応する Web ブラウザ

手順

1. `root` でログオンします。
2. Web コンソールにアクセスします。
   - 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、149 ページの「splxmain」を参照してください。

Internet Explorer 7.0 以降を使用している場合は、ポップアップウィンドウのブロック機能を無効にして、オンラインヘルプのコンテンツを表示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。

手順

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。

手順

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 [Logout] 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 (35 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
  - Apex Central/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

ServerProtect を起動および停止する

ServerProtect はコマンドラインから起動または停止できます。

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、37 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

タスク	手順

コマンドラインから ServerProtect を起動する	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 ~]#`

ServerProtect を停止する

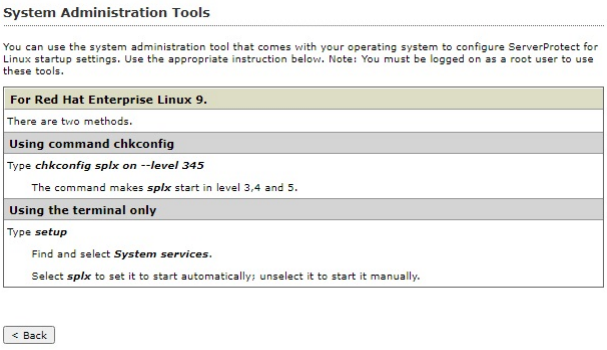
タスク	手順

コマンドラインから ServerProtect を停止する	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 ~]#`

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 9.

There are two methods.

Using command chkconfig

Type ***chkconfig splx on --level 345***

The command makes ***splx*** start in level 3,4 and 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.

< Back

図 2-1. [System Administration Tools] 画面

コマンドラインを使用する

プラットフォーム	設定手順
Red Hat Enterprise Linux 9	コマンド `chkconfig` を使用して、スタートアップ設定を修正します。 1. root でログオンします。 2. コマンドラインで「chkconfig splx on --level 345」と入力します。 **注意** このコマンド例ではレベル 3、4、および 5 の ServerProtect が起動されますが、実際に使用するスタートアップ設定は異なる場合があります。適切なレベルを指定してください。

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、142 ページの「[Logs] グループのキー」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。

Trend Micro Control Manager から ServerProtect を管理する

注意

Trend Micro Control Manager (以下、Control Manager) の名称は Trend Micro Apex Central (以下、Apex Central) に変更されています。このマニュアルで言及している Control Manager のすべての機能と設定は、Apex Central にも適用されます。

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
- 40 ページの「ServerProtect の Web コンソールを使用する」
- 43 ページの「CMconfig ツールを使用する」

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

手順

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。

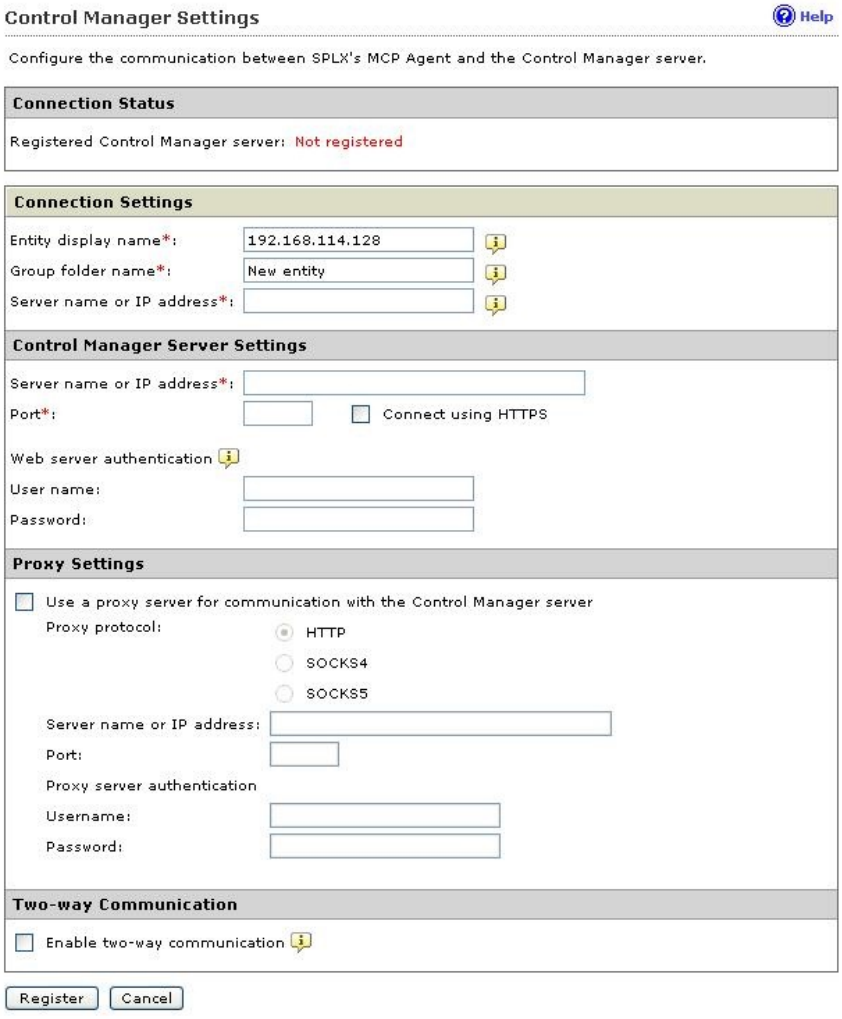


図 2-2. Control Manager

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。

f. NAT デバイスを使用する場合は、[Enable two-way communication] チェックボックスをオフにします。

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

手順

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。

手順

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 Web コンソールにログオンして、[アップデート]→[手動ダウンロード] または [予約ダウンロード] の順にクリックします。
3. [コンポーネントのカテゴリ] セクションで、ServerProtect for Linux で自動アップデートを設定する製品プログラムを選択します。

注意

Control Manager の製品管理の詳細については、Apex Central 2019 のドキュメントを参照してください。

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、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。

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

手順

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。

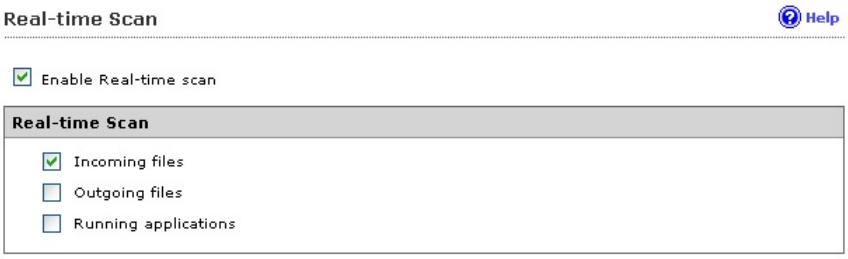


図 3-1. リアルタイム検索の有効化および設定

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、54 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。

手順

1. 予約検索を設定します。

   a. 左のメニューから [Scan Options] > [Scheduled Scan]の順にクリックします。

b. [Enable Scheduled Scan] チェックボックスをオンにします。

c. [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

2. 予約検索の検索周期を設定します。

a. 左のメニューから [Scan Options] > [Scheduled Scan] の順にクリックします。

b. [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。

c. [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、54 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、54 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。

タスク	説明
設定を変更してから手動検索を実行する	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。62 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。確認画面が表示されます。 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。 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。

タスク	説明
コマンドラインから手動検索を実行する	/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	1. 進行状況画面の [Stop Scanning] をクリックします。 2. 次のコマンドを実行します。 ./splxmain -n 3. 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

手順

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。

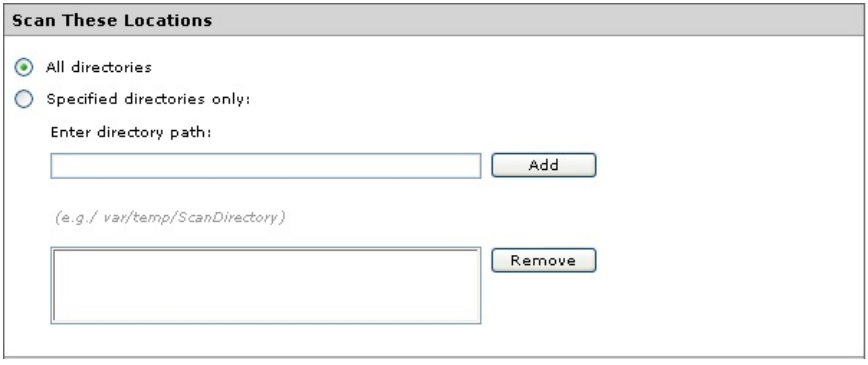


図 3-3. 検索するディレクトリの選択

- 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、62 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。

  a. [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。

  b. [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。

c. 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

リアルタイム検索、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。

検索リストから指定したディレクトリを削除するには、[Scan these directories] リストで削除するディレクトリを選択し、[Remove] をクリックして選択したディレクトリを削除します。[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。

手順

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。

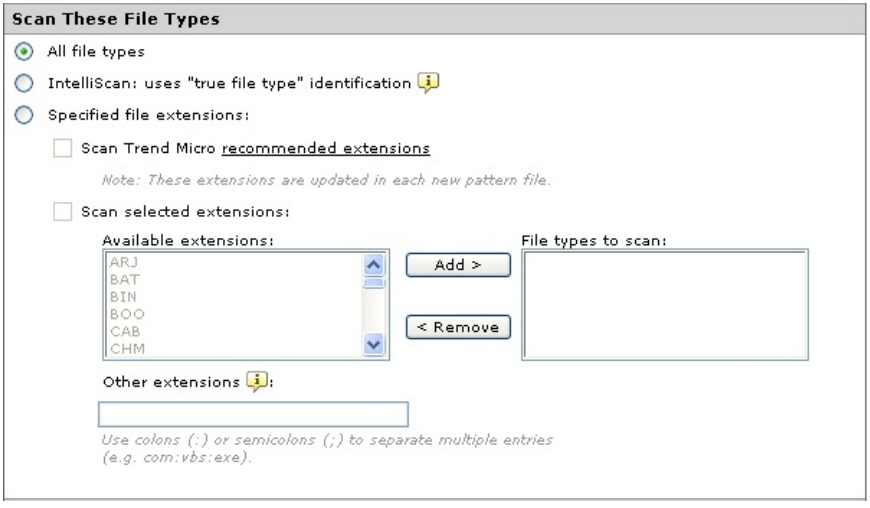


図 3-4. 検索するファイルタイプの選択

- 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 (62 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。
  - 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:

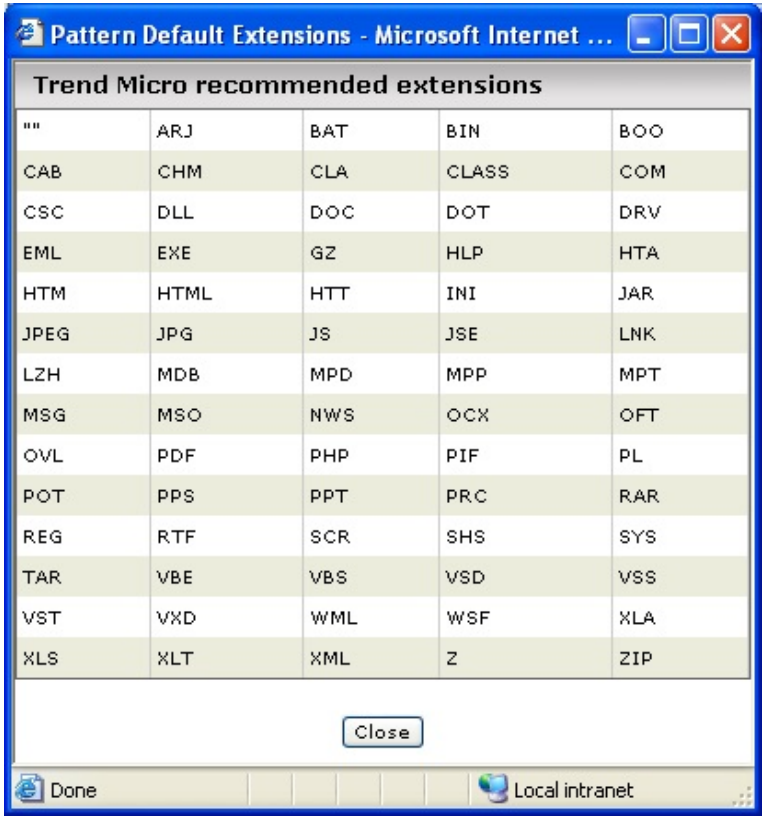


図 3-5. ファイル検索の対象としてトレンドマイクロが推奨する拡張子

- 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。

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

  b. [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。

c. [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。

注意

拡張子を削除するには、[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、[< Remove] をクリックして選択した拡張子を削除し、[Save] をクリックします。

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。

手順

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。

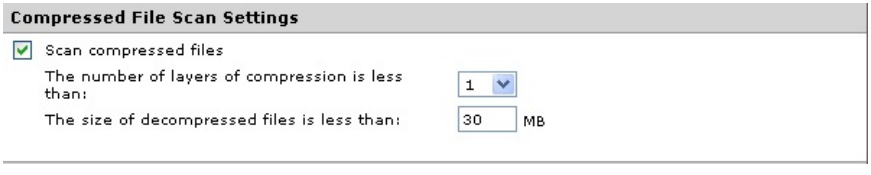


図 3-6. 圧縮ファイル検索

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)。

表 3-1. 検出したウイルスに対して実行できる処理

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。

手順

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 3-7. 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。

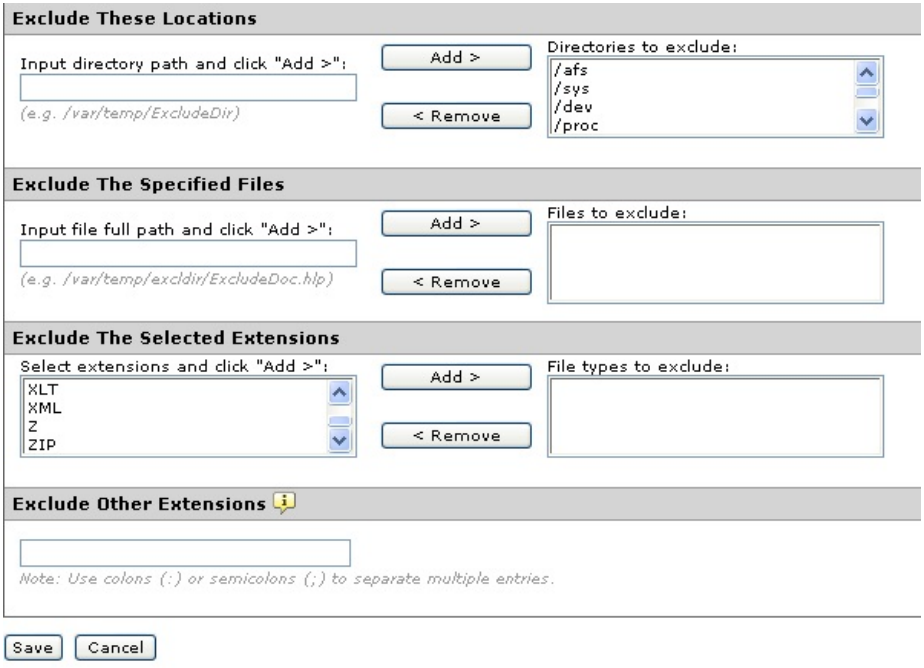


図 3-8. 除外リスト

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。

手順

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。

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。

手順

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`

手順

1. 73 ページの「手動」アップデートまたは 75 ページの「予約」アップデートを設定します。
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 (`https://`

`12.1.123.123:14943/source` など)。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。

機能	参照先
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	詳細については、70 ページの「ウイルストラッキングプログラムとライセンスのアップデート」を参照してください。
コンポーネントのアップデート	詳細については、71 ページの「コンポーネントのアップデート」を参照してください。

ウイルストラッキングプログラムとライセンスのアップデート

手順

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。

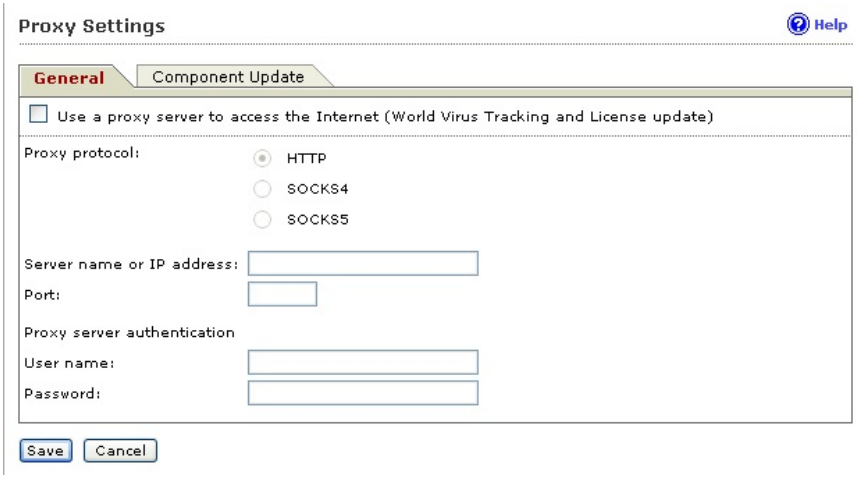


図 4-1. プロキシ設定の [General] 画面

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

手順

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。

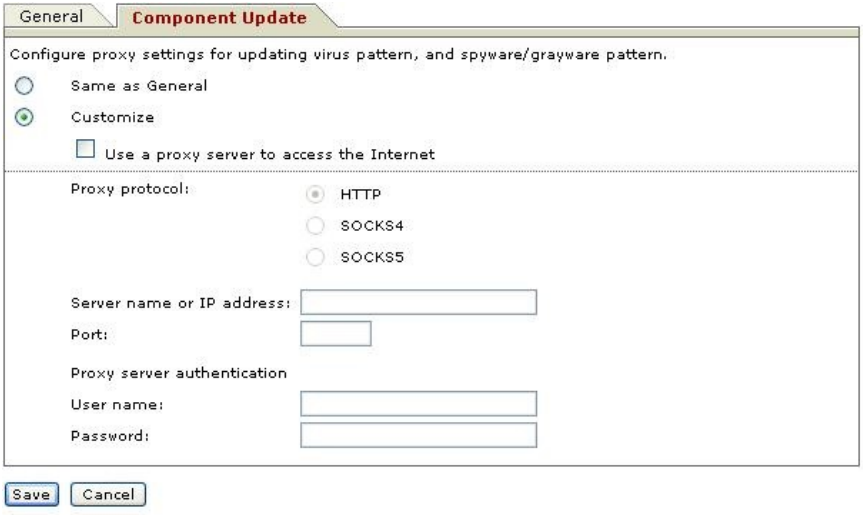


図 4-2. プロキシ設定の [Component Update] 画面

2. 次のいずれかのオプションを選択します。

   - [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。
   - プロキシを設定するには、[Customize] を選択します。

     a. 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 b 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 3 に進みます。

     b. [Proxy Protocol] で、[HTTP]、[SOCKS4]、[SOCKS5] を選択します。

     c. [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。

d. [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。

e. 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。

3. [Save] をクリックします。

ヒント

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、149 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] 画面で [Update Now] をクリックします。詳細については、73 ページの「[Summary] 画面から手動アップデートを実行する」を参照してください。
- [Manual Update] 画面で [Update Now] をクリックします。詳細については、74 ページの「[Manual Update] 画面から手動アップデートを実行する」を参照してください。

[Summary] 画面から手動アップデートを実行する

手順

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

手順

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、69 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。

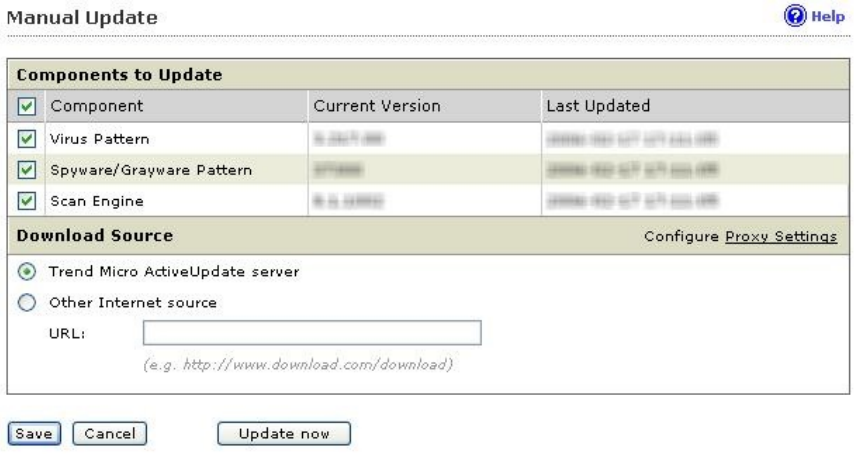


図 4-3. [Manual Update] 画面

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。

手順

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、69 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。

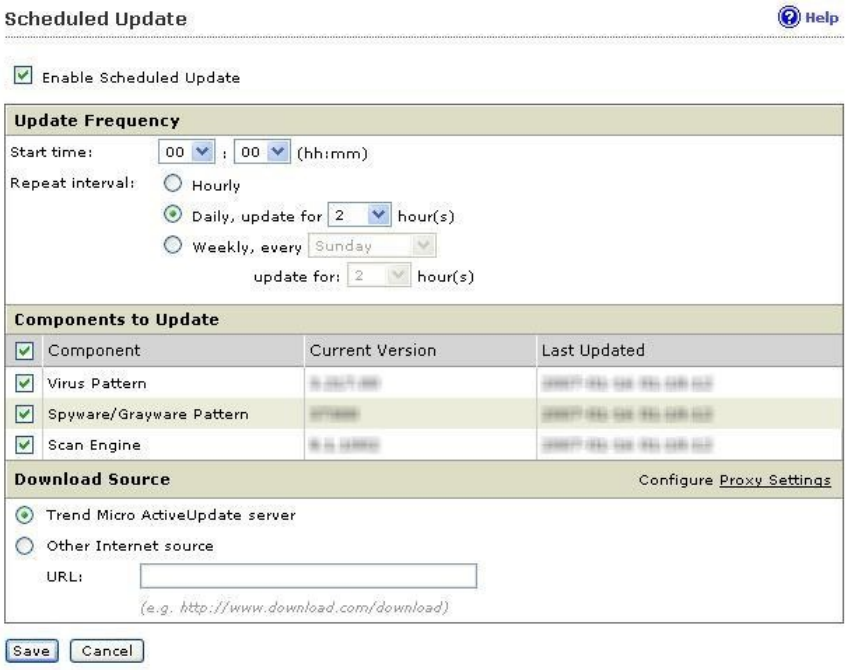


図 4-4. [Scheduled Update] 画面

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。

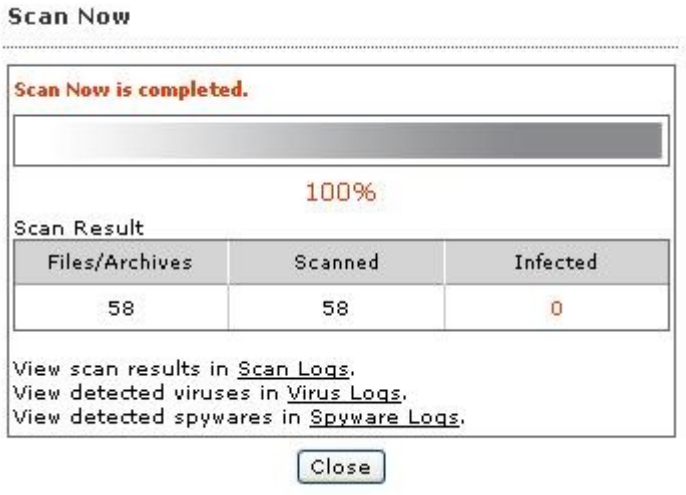


図 5-1. Scan Now の完了画面

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

手順

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。

   - 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、142 ページの「[Logs] グループのキー」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。

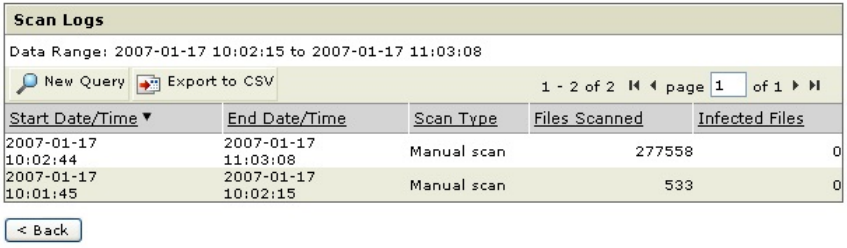


図 5-2. 検索ログの例

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。

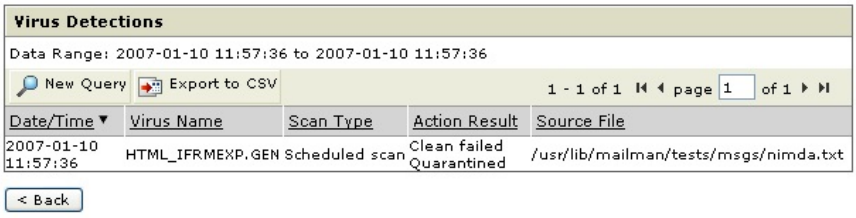


図 5-3. ウイルスログの例

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。

System Logs

Data Range: 2007-01-17 00:34:03 to 2007-01-17 07:17:48

New Query | Export to CSV | 1 - 9 of 9 | page 1 of 1

Date/Time ▼	Description	Reason
2007-01-17 07:17:48	Real-time scan has been enabled.	
2007-01-17 07:11:55	Real-time scan has been disabled.	
2007-01-17 05:56:02	Real-time scan has been enabled.	
2007-01-17 05:50:03	Real-time scan has been disabled.	
2007-01-17 01:04:10	ActiveUpdate Fail	Unable to connect to the update server. Please verify the network connection is enabled and functional, and then try again. (http://splx3-p.activeupdate.trendmicro.com/activeupdate)
2007-01-17 01:00:02	License Reminder	The ServerProtect license grace period expires in 13 days
2007-01-17 00:54:08	ActiveUpdate Fail	Unable to connect to the update server. Please verify the network connection is enabled and functional, and then try again. (http://splx3-p.activeupdate.trendmicro.com/activeupdate)
2007-01-17 00:44:05	ActiveUpdate Fail	Unable to connect to the update server. Please verify the network connection is enabled and functional, and then try again. (http://splx3-p.activeupdate.trendmicro.com/activeupdate)
2007-01-17 00:34:03	ActiveUpdate Fail	Unable to connect to the update server. Please verify the network connection is enabled and functional, and then try again. (http://splx3-p.activeupdate.trendmicro.com/activeupdate)

< Back

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 ( ) 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
```

手順

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。

手順

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。

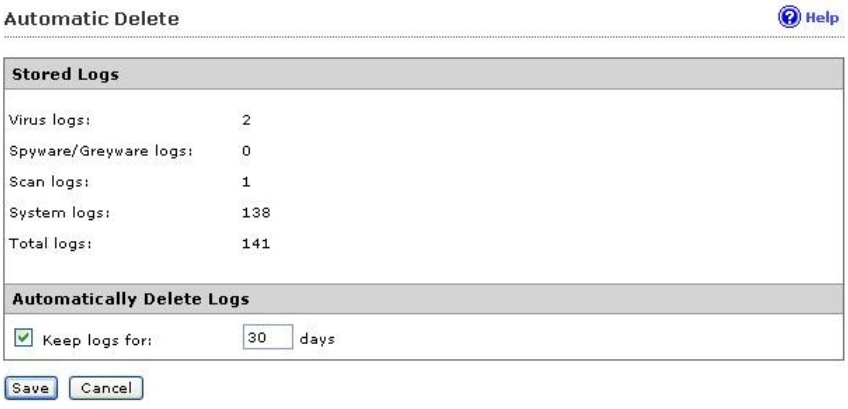


図 5-5. 自動削除

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。

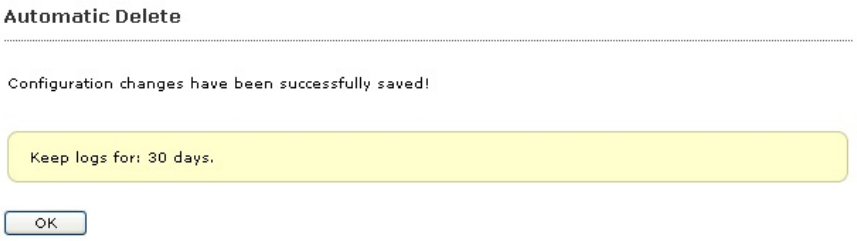


図 5-6. 自動削除設定の保存

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。

手順

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。

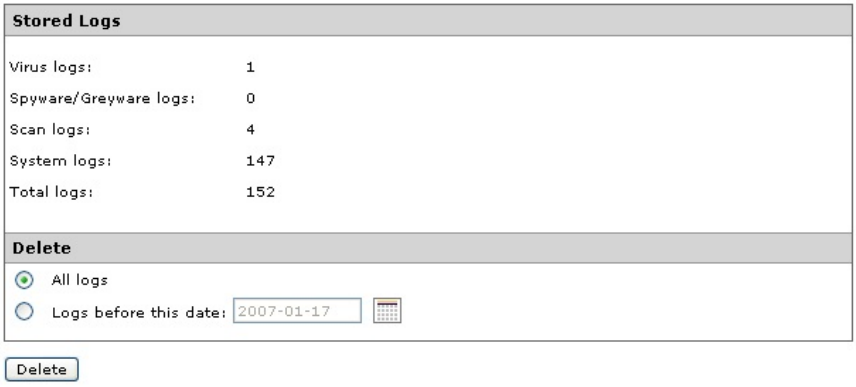


図 5-7. 手動削除

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。

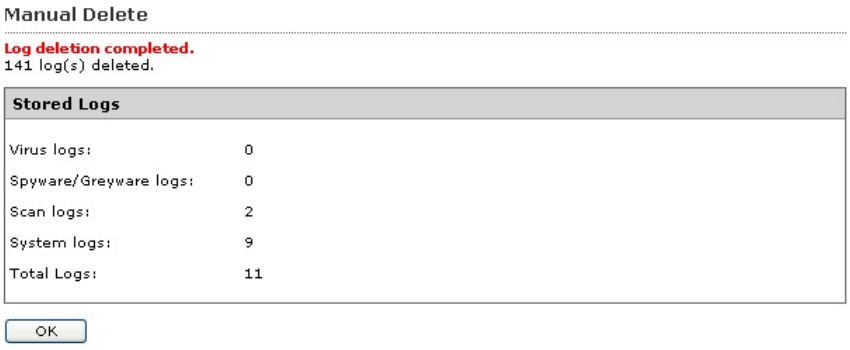


図 5-9. 手動削除の結果

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

警告設定をアップデートする

手順

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。

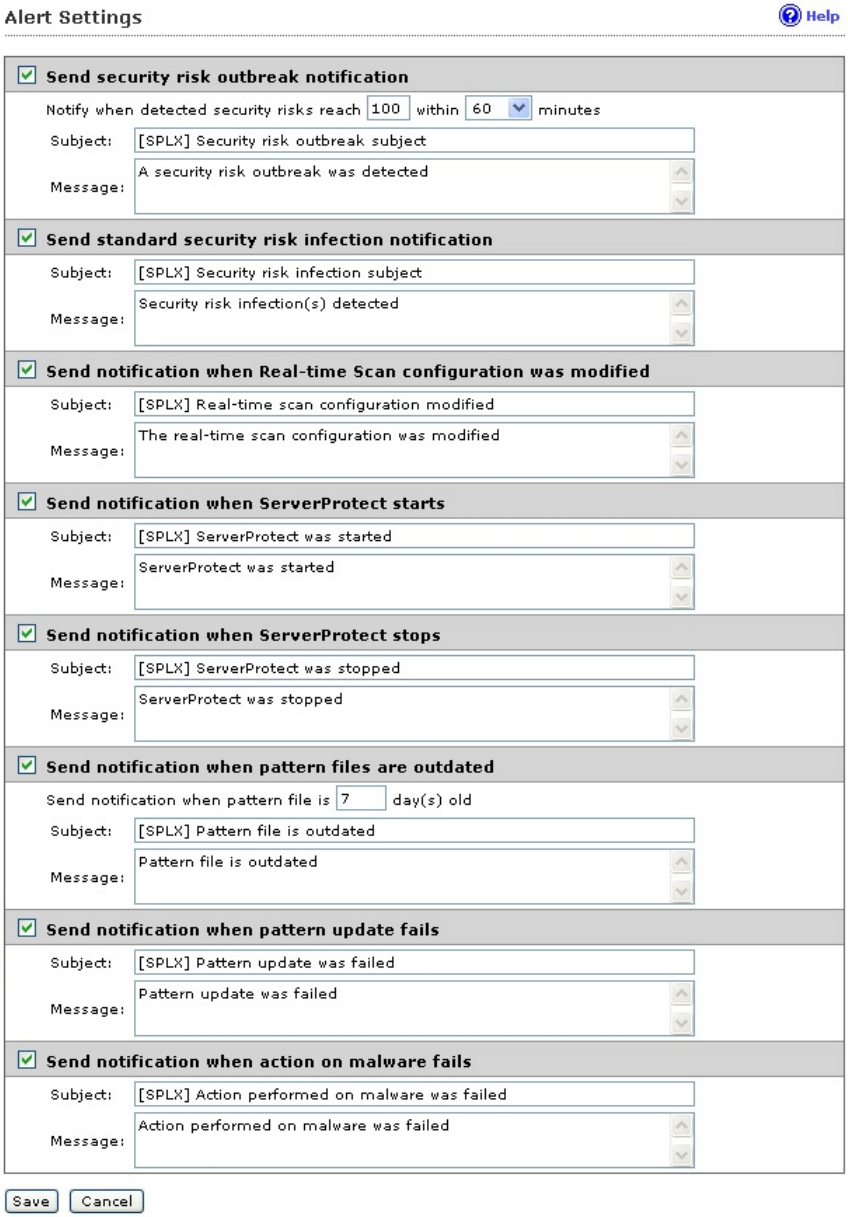


図 5-10. 警告通知メッセージ

カスタム通知を作成する

手順

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

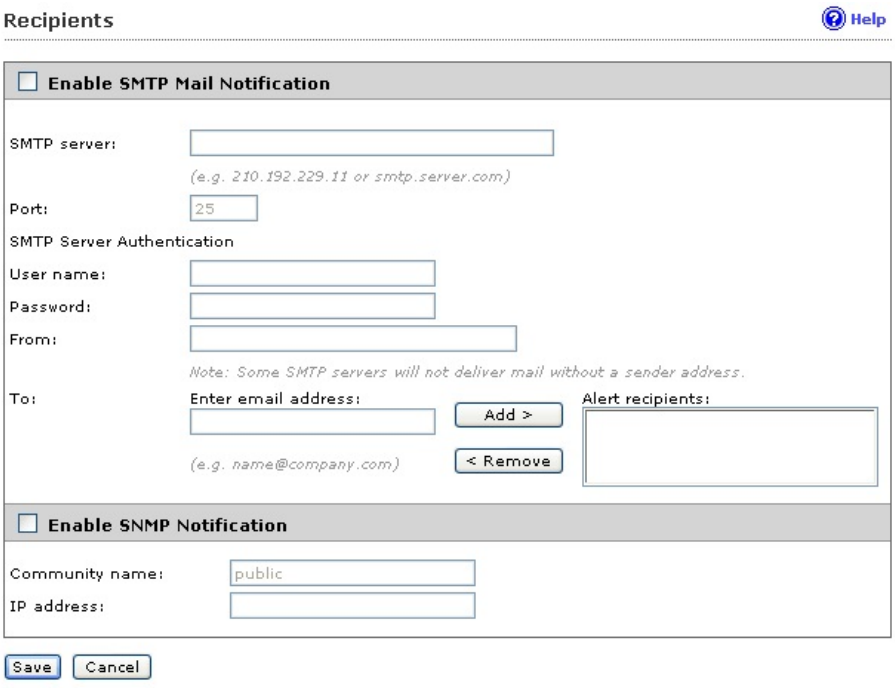


図 5-11. 通知の受信者

SMTP メール通知を設定する

手順

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、次のように SMTP サーバの名前または IP アドレスを入力します。

   `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。

受信者の設定を行う

手順

1. 左のメニューから [Notification] > [Recipients] の順にクリックします。
2. 受信者の設定を行います。
   - 受信者のアドレスを追加するには
     a. [Enter email address] フィールドに受信者のメールアドレスを入力します。たとえば、次のように入力します。

        ```
        yourname@example.com
        ```

     b. [Add >] をクリックして、入力したアドレスを [Alert Recipients] リストに追加します。
     c. [Save] をクリックします。
   - 受信者の設定を変更するには
     a. [Alert Recipients] リストから変更するアドレスを選択します。
     b. 設定項目を必要に応じて変更して、[Save] をクリックします。
   - 受信者のアドレスを削除するには
     a. [Alert Recipients] リストから削除するアドレスを選択します。

b. [< Remove] をクリックして、選択したアドレスを受信者リストから削除します。

c. [Save] をクリックして、変更を適用します。

SNMP 通知を設定するには

手順

1. [SNMP Notification] チェックボックスをオンにします。
2. [Community name] に、メッセージのコミュニティ 名を入力します。
3. [IP address] に、SNMP トラップサーバの IP アドレスを入力します。
4. [Save] をクリックします。

第 6 章

トラブルシューティング

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。

トラブルシューティングのヒント

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、154 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、45 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

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。

表 6-1. tmsplx.xml で編集可能なデバッグレベル

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

- `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 rsyslog.conf を編集して、ServerProtect のデバッグログ機能を有効にします。

手順

1. デバッグログファイルのパス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 rsyslog.conf のバックアップを作成してください。rsyslog.conf ファイルを変更したら、rsyslog 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、/etc/rsyslog.conf を編集します。

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

  ```
  local3.*/path/splxUserDebug.log
  ```

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

手順

1. 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 rsyslog.conf のバックアップを作成してください。

2. <Esc> キーを押し、tmsplx.xml を保存して閉じます。
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/rsyslog.conf
   ```

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、rsyslog を再起動する前に ServerProtect サービスを再起動します。

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。

手順

1. vi などのテキストエディタを使用して、/etc/logrotate.d/rsyslog 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、ファイル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
        /usr/bin/systemctl kill -s HUP rsyslog.service >
/dev/null 2>&1 || true
    endscript
}
```

3. rsyslog ファイルを保存して閉じます。

第 7 章

テクニカルサポート

ここでは、次の項目について説明します。

トラブルシューティングのリソース

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

サポートポータルの利用

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

https://success.trendmicro.com/jp/technical-support

脅威データベース

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

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

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

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

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

サポートサービスについて

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

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

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

注意

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

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出/駆除できない場合などに、感

染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

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

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

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

https://success.trendmicro.com/jp/virus-and-threat-help

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

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

メールレピュテーションについて

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

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

ファイルレピュテーションについて

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

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

Web レピュテーションについて

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

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

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

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

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

注意

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

脅威解析・サポートセンター TrendLabs (トレンドラボ)

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

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

付録 A

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

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 および CentOS 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。

[Scan] グループのキー

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。検索から対象に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 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/TrendMicro/SProtectLinux/SPLX.Backup:sys
```

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。

RealtimeExcludeCommand

このキーでは、特定のコマンドを検索対象から除外します。検索から除外したいプロセスの完全な名前を入力します。複数のプロセスを指定する場合は、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 vsapiapp と splxmain のプロセスを除外するには、次のように入力します。

```
<P Name="RealtimeExcludeCommand" Value="vsapiapp:splxmain"/>
```

RealtimeNotScanSize、OnDemandNotScanSize

これらのキーでは、手動/予約検索およびリアルタイム検索の単一ファイルのサイズの上限 (MB) を設定します。

たとえば、リアルタイム検索の単一ファイルのサイズの上限を設定するには、次のように入力します。

```
<P Name="OnDemandNotScanSize" Value="10"/>
```

このコマンドを実行すると、10MB を超えるすべてのファイルが検索されなくなります。

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。

Type	First Action	Second Action
Joke	Quarantine	
Trojan	Quarantine	
Virus	Clean	Quarantine
Test Virus	Pass	
Spyware/Grayware	Quarantine	
Packer	Clean	Quarantine
Other	Clean	Quarantine

図 A-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 A-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。

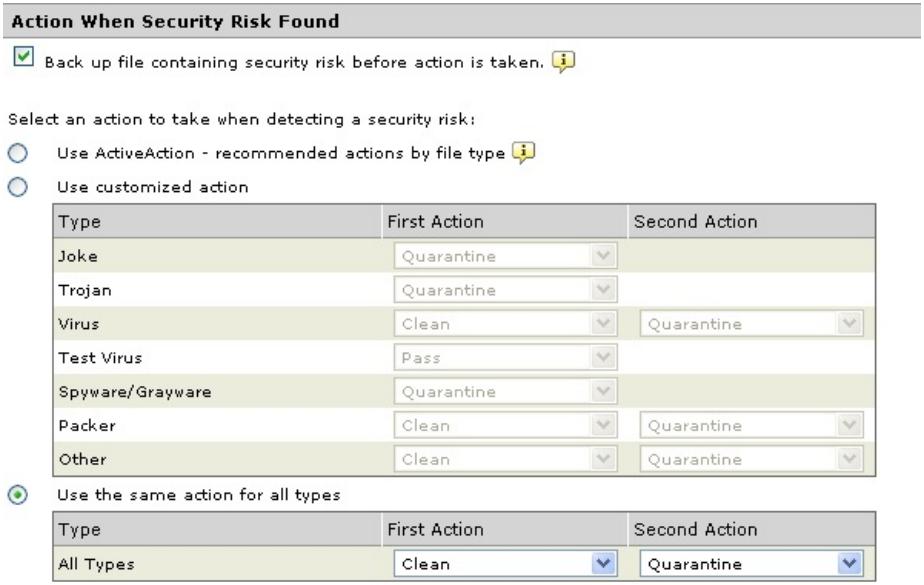


図 A-3. CustomizedAction と AllTypesAction を null に設定すると、[Use ActiveAction] が選択される

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 0 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。

[ActiveUpdate] グループのキー

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、ServerProtect が予約アップデートを実行する場合に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。

[SOURCEINFO] グループのキー設定

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。149 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) と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。

[Notification] グループのキー

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。

[Configuration] グループのキー

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 rsyslog.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、`rsyslog.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、99 ページの「デバッグログ」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、99 ページの「デバッグレベルについて」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。

[Logs] グループのキー

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` キーの値が小さ過ぎると、[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。

[Registration] グループのキー

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、ライセンスのアップデートサーバ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

EnableProxy 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。

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。

表 A-1. `RemoteInstall.conf` のキー、初期設定、および説明

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。

キー	初期設定	説明
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。
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 ページのキーワード ServerAliveInterval を参照してください。
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。

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、rsyslog.conf ファイルで以下のエントリを設定してください。
		1. rsyslogd の設定ファイル/etc/rsyslog.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. `rsyslog` の PID を確認します。
		3. 次のコマンドを実行して、`rsyslogd` 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。

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。142 ページの「[Logs] グループのキー」の「MaxLogDay」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。この機能を有効にするには「yes」、無効にするには「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。テクニカルサポートから指示された場合を除き、splxhttpd.conf の編集はサポートしておりません。

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/
```

付録 B

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。

用語	説明
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。
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。
Red Hat	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。

用語	説明
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。
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	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。

用語	説明
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。
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。

用語	説明
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。
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。

用語	説明
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。
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。
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。

用語	説明
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。
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。

用語	説明
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。
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。

用語	説明
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。