Trend Micro™

ServerProtect™ 3.0

クイックスタートガイド

Red Hat Enterprise Linux 10

※注意事項

複数年契約について

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

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

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

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

法人向け製品のサポートについて

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

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

商標について

P/N: SPEM310011/250715_JP (2025/11)SPEM310010/250715_JP (2025/11)

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

はじめに v
ドキュメント v
対象読者 vi
ドキュメントの表記規則 vi

第 1 章：インストールの準備

システム要件 2
ServerProtect のインストールに必要な情報 2
インターネットのアップデート用プロキシ 2
Apex Central/Control Manager サーバ情報 2
アクティベーションコード 2
ローカルまたはリモートインストール 3

第 2 章：インストール

ServerProtect インストーラオプション 6
ローカルインストールの手順 6
インストールプログラムを実行する 7
トレンドマイクロのエンドユーザ使用許諾契約書に同意する 9
ServerProtect を Control Manager に登録する 9
プロキシサーバの情報 11
インストール時にアクティベートする 12
リモートインストール 13
RemoteInstall の機能 13
RemoteInstall を ServerProtect のバイナリから抽出する 14
リモート配信で設定ファイルを使用する 15
CSV 形式のファイルを RemoteInstall.conf 形式に変換する 16
リモート配信先のクライアントを指定する 16

RemoteInstall ツールを実行する 18
RemoteInstall ツールのオプション 19
カーネルフックモジュール 20
カーネルフックモジュールをインストールする 21
カーネルフックモジュールをリモート配信する 22
インストールを確認する 23
ServerProtect をアンインストールする 23

第 3 章：インストール後の設定

ServerProtect Web コンソールにログオンする 26
管理者パスワードを設定する 28
プロキシサーバを設定する 28
一般的なプロキシ設定 28
コンポーネントアップデートでのプロキシの設定 30
ServerProtect を登録する 31
アクティベーションを実行する 32
製品版にアップグレードする 33
コンポーネントをアップデートする 35
自動アップデートの開始 35
EICAR テストウイルスを使用して ServerProtect をテストする 36
EICAR テストファイルを取得する 37
Linux に rsyslog を設定する 37

付録 A：カーネルフックモジュールの構築とインストール

はじめに 40
要件 40
インストール 40
Linux カーネルのバージョンとアーキテクチャを調べる .. 40
カーネルソースを準備する 41

カーネルソースを設定する 43
KHM を構築する 44
KHM をテストする 45
KHM をインストールする 46
ServerProtect を再起動する 46

付録 B：トラブルシューティング

Linux 内で、依存ライブラリがないことに関連する問題 48
KHM の構築とインストール 48
初期設定のパスワード 50
Web コンソールでパスワードが拒否される 50
デバッグログ 51

付録 C：テクニカルサポート

トラブルシューティングのリソース 54
サポートポータルの利用 54
脅威データベース 54
製品サポート情報 54
サポートサービスについて 55
トレンドマイクロへのウイルス解析依頼 55
メールレピュテーションについて 56
ファイルレピュテーションについて 56
Web レピュテーションについて 56
その他のリソース 57
最新版ダウンロード 57
脅威解析・サポートセンター TrendLabs (トレンドラボ) .. 57

索引

索引 59

はじめに

Trend Micro ServerProtect for Linux (以下、ServerProtect) クイックスタート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。本章では、次の内容について説明します。

- v ページの「ドキュメント」
- vi ページの「対象読者」
- vi ページの「ドキュメントの表記規則」

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。

- 製品の設定や管理についてサポートします。また、有用な付録や用語集なども用意されています。
- オンラインヘルプ: 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。
- 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/ja-JP/

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。

表記規則	説明
 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

インストールの準備

注意

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

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

本章では、Trend Micro ServerProtect for Linux (以下、ServerProtect) の Linux サーバへのインストール前の情報収集の段階について説明します。

本章では、次の内容について説明します。

- 2 ページの「システム要件」
- 2 ページの「ServerProtect のインストールに必要な情報」

システム要件

最新の情報については、次の Web サイトを参照してください。

http://www.go-tm.jp/splx/req

注意

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

ServerProtect のインストールに必要な情報

ServerProtect のセットアッププログラムでは、インストールプロセス時に選択したオプションに応じて、必要な情報を入力するようにポップアップが表示されます。

インターネットのアップデート用プロキシ

ServerProtect サーバとインターネット間にプロキシがある場合、プロキシのホスト名または IP アドレス、ユーザ名、およびパスワードを入力します。

Apex Central/Control Manager サーバ情報

ServerProtect を既存の Trend Micro Apex Central(以下、Apex Central)/Trend Micro Control Manager (以下、Control Manager) サーバに登録する場合、そのサーバのホスト名または IP アドレス、およびログオン名が必要です。

注意

ServerProtect をお使いのネットワーク上の Apex Central/Control Manager サーバに登録するには、Apex Central または Control Manager サーバ 7.0 以上が必要です。

アクティベーションコード

製品の登録時に、レジストレーションキーと引き換えにアクティベーションコード/シリアル番号を取得し、プログラムの「ロックを解除」します。次の

トレンドマイクロのオンライン登録 Web サイトにアクセスして、インストール前にアクティベーションコードを登録し、取得できます。

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

注意

すでにアクティベーションコードをお持ちの場合には、オンライン登録の必要はありません。アクティベーションコードの詳細については、販売代理店にお問い合わせください。

ローカルまたはリモートインストール

本バージョンの ServerProtect は、ローカルサーバまたはリモートサーバのいずれにもインストールできます。また、1 台でも、複数のリモートサーバでもインストールできます。

第 2 章

インストール

本章では、Linux サーバへの Trend Micro ServerProtect for Linux (以下、ServerProtect) のインストールを説明します。本章では、次の内容について説明します。

- 6 ページの「ServerProtect インストーラオプション」
- 6 ページの「ローカルインストールの手順」
- 13 ページの「リモートインストール」
- 20 ページの「カーネルフックモジュール」
- 23 ページの「インストールを確認する」
- 23 ページの「ServerProtect をアンインストールする」

ServerProtect インストーラオプション

インストーラで使用できるパラメータの詳細を表示するには、次のコマンドを実行してください。

```
./SProtectLinux-3.0-1715.bin -h
```

次の表では、パラメータについて説明します。

オプション	説明
-f	ServerProtect を強制的にインストールします。
-h	このバイナリ (現在表示している出力) で使用可能なパラメータのリストを表示します。
-n	ServerProtect をインストールした後に、ServerProtect サービスを開始しません。
-r	リモートインストールツールを抽出します。
-s	使用許諾契約書を表示しません。
-S { アクティベーションコード}	アクティベーションコードを入力して、ServerProtect をアクティベートします。
-x	ServerProtect の rpm ファイルを抽出します。
-X	ServerProtect のバイナリファイルを抽出します。

ローカルインストールの手順

次のリストでは、ローカルの Linux サーバでの ServerProtect のインストール手順を示します。それに続くセクションでは、この手順について詳細に説明します。

手順 1: 7 ページの「インストールプログラムを実行する」

手順 2: 9 ページの「トレンドマイクロのエンドユーザ使用許諾契約書に同意する」

手順 3: 9 ページの「ServerProtect を Control Manager に登録する」

手順 4: 12 ページの「インストール時にアクティベートする」

手順 5: 21 ページの「カーネルフックモジュールをインストールする」 (必要に応じて)

インストールプログラムを実行する

ServerProtect をインストールする前に、お使いの Linux のディストリビューションとカーネルがこのリリースでサポートされていることを確認してください。カーネルに対応するカーネルフックモジュール (以下、KHM) は、英語サイト (http://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=latest&clkval=111&lang_loc=1) から確認、ダウンロードできます。お使いのカーネルがシステム要件に記載されていない場合は、21 ページの「カーネルフックモジュールをインストールする」セクションの手順に従って、Linux システムに対応した KHM を入手していただく必要があります。

注意

Linux コンピュータに ServerProtect をインストールする前に、次の依存ライブラリ (64 ビット版) がインストールされていることを確認します。

-glibc

-libgcc

-zlib

-bzip2

-libuuid

- libstdc++ (Red Hat および CentOS のみ)

- nss-softokn-freebl (Red Hat および CentOS のみ)

- perl-Sys-Syslog (Red Hat および CentOS のみ)

chkconfig (Red Hat 9 および Red Hat 10 のみ)

ライブラリのバージョンについては、OS イメージにバンドルされている初期設定のライブラリを使用できます。

ServerProtect インストールを開始するには

手順

1. ServerProtect のインストールファイルをダウンロードまたはコピーします。
2. `root` でログオンします。
3. ServerProtect のインストールファイルが含まれるディレクトリで、次のコマンドを実行します。

   ```
   SProtectLinux-3.0-1715.bin
   ```

   このコマンドを実行すると、必要なファイルが適切な場所に抽出されます。
4. インストール中はリアルタイム検索を無効にします。
   a. `-n` オプションを使用して、インストールを開始します。たとえば、`SProtectLinux-3.0-1715.bin` のコマンドを実行します。
   b. インストールが完了したら、`tmsplx.xml` 設定ファイルの `RealtimeScan` パラメータの値を「`0`」に設定します。
   c. ServerProtect サービスを再起動します。

注意

KHM がお使いの Linux カーネルをサポートしていないという警告メッセージが表示された場合、KHM を構築してインストールします。KHM のインストールが完了しても、ServerProtect サービスを起動、または再起動しないでください。次に、上記の手順 b および c を実行します。

警告!

`-n` オプションを使用して ServerProtect をインストールする場合、システムスタートアップで実行するには、ServerProtect サービスを手動で設定する必要があります。そのためには、`/opt/TrendMicro/SProtectLinux/SPLX.util` フォルダで `./add_splx_service` を実行します。

トレンドマイクロのエンドユーザ使用許諾契約書に同意する

ServerProtect のインストールを開始する前に、製品に同梱されている使用許諾契約書を読んでください。

注意

製品の使用にあたってはインストール時に表示される英語の許諾契約書は適用されず、製品に同梱されている日本語の許諾契約書が適用されます。

スペースキーを押して、使用許諾契約書をスクロールします。最後に「`yes`」と入力してください(「`yes`」を入力しない場合は、インストールを続行できません)。

```
NOTICE: Trend Micro licenses its products in accordance with cer-
tain terms and conditions. By breaking the seal on the CD jacket
in the Software package or installing a serial number, registra-
tion key or activation code, You already accepted a Trend Micro
license agreement. A courtesy copy of a representative Trend Micro
License Agreement is included for reference below. The language
and terms of the actual Trend Micro license agreement that you
accepted may vary. By accepting the License Agreement below, or
using the Software, You confirm Your agreement to the terms and
conditions of the original Trend Micro license agreement you
accepted.

Trend Micro License Agreement
(Package Version 0403Nov03E021004)

-----------------------[SNIP] -------------------------

SPLX version 3.0 Released June, 2015

Do you agree to the above license terms? (yes or no)
```

図 2-1. インストール時に表示される使用許諾契約書画面 (表示例)

ServerProtect を Control Manager に登録する

Control Manager を使用して ServerProtect を管理する場合は、インストール時に ServerProtect を Control Manager に登録できます。

ServerProtect を Control Manager に登録するには

手順

1. 7 ページの「インストールプログラムを実行する」の手順に従って、ServerProtect のインストールを開始します。
2. 「Do you wish to connect this SPLX server to Trend Micro Control Manager?」というメッセージが表示されたら、「y」と入力して <Enter> キーを押します (または単に<Enter>キーを押して初期設定の「y」を選択します)。

   ユーザから必要なデータを収集することを通知するメッセージが表示されて、ServerProtect サーバ用に使用できる IP アドレスのリストが表示されます。

   

   注意

   Control Manager を使用して ServerProtect を管理しない場合は、「n」と入力して<Enter>キーを押します。「Activate ServerProtect to continue scanning and security updates.」というメッセージが表示され、アクティベーションコードの入力のためのプロンプトが表示されます。このプロセスの詳細については、12 ページの「インストール時にアクティベートする」を参照してください。
3. 「SPLX server name or IP address」プロンプトで、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、HTTPS を使用して Control Manager に接続する場合には「y」を、HTTP 接続を使用する場合には「n」を入力します。
5. 「Control Manager server name or IP address:」プロンプトで、ServerProtect を管理するための Control Manager サーバのサーバ名または IP アドレスを入力します。
6. 「Control Manager server port: [80]」プロンプトで、Control Manager にアクセスするためのポートの番号を入力するか、単に <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、「y」を入力するか (yes の場合)、単に<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、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。プロキシサーバを使用して Control Manager に接続する場合は、11 ページの「プロキシサーバの情報」を参照してこのプロセスの詳細を確認してください。

8. 「Please specify the name you would like to display on the Control Manager console: [SPLX server name or IP address]」プロンプトで、適切な名前を入力します。Control Manager は、この名前を使用して Control Manager の Web コンソール上で 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、ServerProtect を登録する Control Manager の製品ディレクトリ上のフォルダパスを入力します (この入力を省略して <Enter> キーを押した場合、「新規エンティティ」フォルダに登録されます)。

   ユーザが入力した情報が一覧表示されて、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、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」と入力してすべての表示された情報を確定した場合は、「Saving information to the configuration file done」というメッセージが表示されて、アクティベーションコードを入力するかどうか尋ねられます。このプロセスの詳細については、12 ページの「インストール時にアクティベートする」を参照してください。

プロキシサーバの情報

プロキシサーバを使用して Control Manager に接続する場合は、インストール時にプロキシサーバの情報を入力して、ServerProtect が Control Manager と正しく通信できるようにしてください。

インストール時にプロキシサーバの情報を指定するには

以下のプロンプトで該当する情報を入力してください。

- Proxy Server name or IP address:(プロキシサーバの名前または IP アドレス)
- Proxy Server port: [80](プロキシサーバのポート番号)
- Does your proxy server require user authentication? (y/n) [n](プロキシサーバでユーザ認証が必要かどうか)

  (認証が必要な場合)

  - Proxy user name:(プロキシのユーザ名)
  - Proxy password:(プロキシのパスワード)
  - Retype proxy password:(プロキシのパスワードの確認入力)

インストール時にアクティベートする

アクティベートした場合は、製品版の製品がインストールされます。これを省略すると、ServerProtect はアクティベートされず、検索機能およびコンポーネントのアップデート機能は有効になりません。アップデートは、ServerProtect をアクティベートするまで再開されません。

手順

1. ServerProtect を登録するためのプロンプトが表示されます。アクティベーションコードをすでに取得している場合は手順 2 に進んでください。

```
Step 1. Register
Use the Registration Key that came with your product
to register online
(https://olr.trendmicro.com/redirect/product_register.aspx)
(Skip this step if the product is already registered.)

Step 2. Activate
Type the Activation Code received after registration
to activate ServerProtect.
(Press [Ctrl+D] to abort activation.)
```

   a. 今すぐ登録するには、次の URL にアクセスします。

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

b. 31 ページの「ServerProtect を登録する」に示された手順に従います。

2. 次に、ServerProtect をアクティベートするためのプロンプトが表示されます。この時点でアクティベートすることも、この手順を省略して後でアクティベートすることもできます。この手順を省略する場合は、<Ctrl>+<D> キーを押します。

   ServerProtect をアクティベートするには、アクティベーションコードをプロンプトに入力して、<Enter>キーを押します。

   インストール時に登録またはアクティベーションを実行しなかった場合の ServerProtect の登録手順は、31 ページの「ServerProtect を登録する」を参照。

リモートインストール

集中管理された分散環境に ServerProtect をインストールして管理できるようにするために、リモートインストールツール(RemoteInstall) を提供しています。

RemoteInstall の機能

RemoteInstall には次の機能があります。

- ServerProtect をリモートコンピュータにインストールします。
- 設定ファイルにはクライアントコンピュータのアカウント情報が保持されます。
- ServerProtect のインストール後に、ServerProtect の設定データを対象コンピュータに配信します。
- ServerProtect のインストール後に、カーネルフックモジュール (KHM) を対象コンピュータに配信します。
- クライアント環境に関する特定の情報を収集します (実行している Linux ディストリビューションや Linux カーネル番号など)。
- 設定情報を.csv 形式でエクスポートできます。これにより RemoteInstall は、初回の配信が失敗したコンピュータのリストをそれ以降の配信で再利用します。

リモートインストールの実行手順は、次のとおりです。

- RemoteInstall の抽出
- RemoteInstall 設定ファイルの編集
- RemoteInstall の実行

RemoteInstall を ServerProtect のバイナリから抽出する

-r パラメータを使用して、RemoteInstall を単一パッケージから、または特定の Linux カーネルバージョン用のバイナリファイルから抽出できます。たとえば、次のコマンドを実行すると、ServerProtect のバイナリファイルからリモートインストールツールが抽出されます。

```
SProtectLinux-3.0-1715.bin
```

使用許諾契約書に同意して、リモートインストールプログラム (RemoteInstall) を抽出した後で、上記のコマンドを実行すると、作業ディレクトリの下に `remote.install.splx` サブディレクトリが作成されます。このサブディレクトリに含まれるファイルとディレクトリのリストについては、次の表を参照してください。

表 2-1. RemoteInstall のディレクトリ

ファイルまたはディレクトリ	説明
`config/`	ServerProtect の設定ファイルの配信用のディレクトリ。次の 4 つのファイルが含まれます。 • `tmsplx.xml` — ServerProtect の設定ファイル。このファイルを配信用に変更できます。 • `tmsplx.xml.template` — 上記設定ファイル (`tmsplx.xml`) のテンプレートファイル。`tmsplx.xml` が壊れた場合は、このテンプレートを使用してこのファイルを復元できます。 • `xmldeployer` — 設定ファイル配信用のスクリプト。 • `xmlvalidator` — `tmsplx.xml` 内のすべてのキーの値を検証するためのツール。
`KHM.module`	KHM ファイル配信用のディレクトリ

ファイルまたはディレクトリ	説明
RemoteInstall	リモートインストールツール
RemoteInstall.conf	配信用の設定ファイル
RemoteInstall.csv	.CSV 形式のファイルを .conf 形式に変換するためのテンプレート

リモート配信で設定ファイルを使用する

RemoteInstall で使用される初期設定の設定ファイルは、RemoteInstall.conf です。抽出時に、このファイルは remote.install.splx ディレクトリに配置されています。RemoteInstall.conf は、多くのキーが含まれた複雑な設定ファイルです。この設定ファイルは、次の 3 種類の配信で使用できます。

- ServerProtect パッケージの配信とインストール
- ServerProtect の設定のアップデート
- カーネルフックモジュール (KHM) の配信

次の表では最も重要な設定可能キーのみを示しています。キーの詳細については、「管理者ガイド」を参照してください。

表 2-2. 最もよく使用される RemoteInstall.conf の設定可能キー

キー	説明
DeployOption	実行する配信の種類を指定します。 • 1: ServerProtect パッケージの配信とインストール • 2: ServerProtect の設定ファイルのアップデート • 3: KHM の配信
PackageName	パッケージ配信用の ServerProtect インストールパスを指定します
Activation Code	パッケージ配信で使用されます。インストール用の ServerProtect のアクティベーションコードを指定します
ConfigFilePath	設定ファイルの配信で使用されます。設定ファイルのパスを指定します

CSV 形式のファイルを RemoteInstall.conf 形式に変換する

設定ファイルを簡単に変更できるように、RemoteInstall には、ファイルを CSV 形式でインポートするためのオプションが用意されています。設定ファイルの情報を表計算プログラム (OpenOffice に含まれるものなど) で変更する場合は、次の手順に従ってください。

手順

1. `RemoteInstall.csv` ファイルを表計算プログラムにインポートして編集します。ファイルを別のファイル名で保存します。
2. この新しいファイルを ServerProtect の `remote.install.splx` ディレクトリにコピーします。
3. RemoteInstall を実行する際には、次の例のように`-p` オプションの後ろに変更後の CSV ファイルの名前を指定します。

   ```
   ./RemoteInstall -p my_conf_file.csv
   ```

   RemoteInstall は、次の命名規則に従って CSV ファイルを `RemoteInstall.conf` 形式に変換します。`RemoteInstall_yyyy-mm-dd_hhmmss.conf`

リモート配信先のクライアントを指定する

`RemoteInstall.conf` の「Client assignment」セクションの情報を変更して、リモート配信先のクライアントを指定します。このセクションには、配信先のリモートコンピュータを指定するための 2 つのサブセクションがあります。RemoteInstall の配信先となる 1 台のコンピュータの設定を入力するには、「`#single deploy`」セクションを編集します。1 つ以上のクライアントグループの設定を入力するには、「`#group deploy`」セクションを編集します。1 回の配信で両方のセクションを使用することもできます。

以下では、正しく配信するために入力する必要のある設定データを一覧表記しています。

- シングル配信

  `RemoteInstall.conf` の「`Client assignment`」セクションの「`#single deploy`」には、正しく配信するために RemoteInstall が認識する必要のある 13 個の設定項目があります。

表 2-3. 設定ファイル内のクライアント割り当てキー (シングル配信)

行	説明
1. [x.x.x.x]	クライアントの IP アドレス
2. RootPassword	クライアントの root パスワード
3. ConnectCM	1 (初期設定): Control Manager サーバに登録します。 0: Control Manager サーバに登録しません。
4. CMServerIP	Control Manager サーバの IP アドレス
5. CMServerPort	Control Manager サーバの接続ポート (初期設定=80)
6. UseProxyAccessCM	1: プロキシサーバを使用して Control Manager サーバに接続します。 0 (初期設定): プロキシを使用しません。
7. ProxyServerIP	プロキシサーバの IP アドレス
8. ProxyServerPort	プロキシサーバの接続ポート (初期設定=80)
9. ProxyAuthentication	1: プロキシ認証を使用します。 0 (初期設定): プロキシ認証を使用しません。
10. ProxyUserName	プロキシ認証のユーザ名
11. ProxyPassword	プロキシ認証のパスワード
12. CMClientName	Control Manager コンソールに表示されるクライアントコンピュータ名 初期設定= クライアントの IP アドレス
13. CMProductDirectoryName	Control Manager コンソールに表示されるディレクトリ名。ディレクトリを使用してクライアントがグループ分けされます。 初期設定=「New Entity」

- グループ配信

グループ配信の場合は、次の表以外のすべての行は「#single deploy 」と同じです。

表 2-4. 設定ファイル内のクライアント割り当てキー (グループ配信)

行	説明
1.[Group1]	1 台のコンピュータの IP アドレスのキーの代わりに、最初のキーでは配信先クライアントのグループを指定します。
14. Machine1=x.x.x.x	この行 (およびこの後に必要なだけ記述される行) では、RemoteInstall が ServerProtect を配信する各コンピュータの IP アドレスを列記します。
15. Machine2=x.x.x.x	(同上)
(必要なだけ記述)	(同上)

ヒント

参照しやすいように、すべてのグループ名は、営業、研究開発のように分かりやすい語を先頭に付けることをお勧めします。同様にコンピュータ名も、*Server1*、*Server2* のように指定することをお勧めします。

RemoteInstall ツールを実行する

下記の主要な手順に従って RemoteInstall プログラムを実行してください。

手順

1. ServerProtect のすべてのバイナリファイルを配信サーバに配置します。
2. RemoteInstall を ServerProtect のバイナリから抽出します(詳細については、14 ページの「RemoteInstall を ServerProtect のバイナリから抽出する」を参照してください)。
3. ServerProtect を複数のコンピュータに配信するには、RemoteInstall.conf を配信用に設定します。(`RemoteInstall.conf` ファイルの詳細については、16 ページの「リモート配信先のクライアントを指定する」を参照してください)。

4. 次のコマンドをコマンドラインから実行します。

   ```
   ./RemoteInstall
   ```

   RemoteInstall は、ServerProtect 対象コンピュータに配信して、進行状況メッセージを出力します。この配信によって、次の表に示す 5 つの結果ファイルが作成されます。

   表 2-5. RemoteInstall によって作成される結果ファイル

結果ファイル	説明
splx_failed_list_yyyy-mm-dd_hhmmss.conf	設定ファイル形式の失敗リスト
splx_failed_list_yyyy-mm-dd_hhmmss.csv	.CSV ファイル形式の失敗リスト
splx_success_list_yyyy-mm-dd_hhmmss.conf	設定ファイル形式の成功リスト
splx_success_list_yyyy-mm-dd_hhmmss.csv	.CSV ファイル形式の成功リスト
splx_remote_status_yyyy-mm-dd_hhmmss.txt	配信ステータス

RemoteInstall ツールのオプション

RemoteInstall ツールのオプションの使用法を表示するには、次のように-h パラメータを使用してください。

```
./RemoteInstall -h
```

表 2-6. RemoteInstall スクリプトで使用できるパラメータ

パラメータ	説明
-c	クライアント情報をチェックします。

パラメータ	説明
-f {代替設定ファイル}	リモートインストールの設定ファイルを指定します。このオプションは、RemoteInstall.conf 以外の設定ファイルを使用して RemoteInstall を実行する場合に使用します (代替設定ファイルを使用できるのは、この代替ファイルに RemoteInstall.conf と同じキー/値ペアが含まれている場合のみです。15 ページの「リモート配信で設定ファイルを使用する」を参照してください)。
-h	使用法を表示します。
-n	使用許諾書を表示しません。
-p {CSV ファイル}	指定した CSV ファイルを RemoteInstall で使用する設定ファイルに変換します (このオプションの詳細については、16 ページの「CSV 形式のファイルを RemoteInstall.conf 形式に変換する」を参照してください)。
-v	バージョンを表示します。

カーネルフックモジュール

このバージョンの ServerProtect には、サポートされている各カーネル用のカーネルフックモジュール (KHM) が付属しています。KHM のソースコードも、インストールパッケージに含まれています。

ServerProtect でリアルタイム検索を実行するには、KHM をインストールする必要があります。お使いの Linux カーネルが、対応ディストリビューションおよびカーネルのリスト (http://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=111&regs=NABU&lang_loc=1) にある場合、ServerProtect セットアッププログラムにより、ServerProtect パッケージに付属する適切な KHM が自動的にインストールされています。

お使いの Linux カーネルがリストにない場合、次を実行します。

- お使いの Linux カーネルに適した KHM を、次のトレンドマイクロ Web サイトからダウンロードします。

  http://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=111&regs=NABU&lang_loc=1

- お使いの Linux カーネルに適した KHM が使用できない場合、Linux システム上で KHM を構築します。構築手順は、39 ページの「カーネルフックモジュールの構築とインストール」を参照してください

注意

Linux カーネルをアップグレードする際には、KHM を ServerProtect のインストール先ディレクトリにコピーする必要があります。

カーネルフックモジュールをインストールする

本セクションでは、トレンドマイクロ Web サイトからダウンロードした KHM パッケージのインストール方法を説明します。また、ServerProtect のインストール後、最新の KHM をインストールすることもできます。

注意

インストール中に、インストールを続行するには依存パッケージのインストールが必要であるというエラーメッセージが表示された場合は、お使いの Linux システムに対応した KHM を上記のトレンドマイクロ Web サイトから入手してください。

手順

1. root でログオンします。
2. お使いのカーネルが最新バージョンの ServerProtect でサポートされていることを確認するには、次の URL にアクセスします。

   http://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=111&regs=NABU&lang_loc=1

3. KHM の名前は、対応するカーネルバージョンに応じて付けられます。お使いの Linux カーネルに適した KHM パッケージをダウンロードして、次のディレクトリにコピーします。

   ```
   /opt/TrendMicro/SProtectLinux/SPLX.module/
   ```

4. 上記のディレクトリに移動して、次のコマンドを実行して KHM パッケージを抽出します。

```
tar xzvf {SPLX バージョンとカーネルバージョン}.tar.gz
```

次のファイルがパッケージから抽出されます。

- {カーネルバージョン}.md5
- splxmod-{カーネルバージョン}.o

ヒント

MD5 チェックサムを調べて、ファイルが完全な状態でダウンロードされて抽出されたことを確認することを強くお勧めします。

5. 次のコマンドを実行して ServerProtect サービスを再起動します。

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

6. インストール後、次の URL から ServerProtect Web コンソールにアクセスできます。

   `http://<ホストサーバ>:14942`

   または

   `https://<ホストサーバ>:14943`

   お使いの Linux システムのポート 14942 または 14943 が開いていて、ServerProtect にアクセスできることを確認します。

カーネルフックモジュールをリモート配信する

RemoteInstall を使用して、KHM を複数のコンピュータにリモート配信できます。

手順

1. 最新の KHM を次のトレンドマイクロ Web サイトからダウンロードします。

   http://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=111&regs=NABU&lang_loc=1

2. この KHM を配信サーバ上の対応するディレクトリにコピーします。

3. RemoteInstall を実行します。

ヒント

ネットワーク全体に配信する前に、少数のコンピュータを対象にして配信をテストすることをお勧めします。

インストールを確認する

インストールが完了したら、ServerProtect が正常に動作していることを確認してください。

手順

1. 次のコマンドをコマンドラインから実行します。

   ```
   /etc/init.d/splx status
   ```

2. 次の例のように、すべての実行中プロセスが表示されます。

   ```
   splxmod module is running...
   vsapiapp (pid 3854) is running...
   entity (pid 3845 3844) is running...
   ServerProtect for Linux core is running...
   splxhttpd (pid 3869 3868 3867 3866 3865 3864) is running...
   ServerProtect for Linux httpd is running...
   ServerProtect for Linux manual scan is stopped
   ServerProtect for Linux scheduled scan is stopped
   ServerProtect for Linux Control Manager agent is not
   registered to Trend Micro Control Manager server
   ```

ServerProtect をアンインストールする

ServerProtect を削除するには、`root` でログオンしている必要があります。ターミナルウィンドウで、「`rpm -e SProtectLinux`」と入力して、ServerProtect サービスを停止し、アプリケーションを削除します。

第 3 章

インストール後の設定

本章では、Trend Micro ServerProtect for Linux (以下、ServerProtect) の Web コンソールへのアクセス方法とインストール後の設定タスクについて説明します。本章は次の内容で構成されています。

- 26 ページの「ServerProtect Web コンソールにログオンする」
- 28 ページの「管理者パスワードを設定する」
- 28 ページの「プロキシサーバを設定する」
- 31 ページの「ServerProtect を登録する」
- 32 ページの「アクティベーションを実行する」
- 33 ページの「製品版にアップグレードする」
- 35 ページの「コンポーネントをアップデートする」
- 36 ページの「EICAR テストウイルスを使用して ServerProtect をテストする」
- 37 ページの「Linux に rsyslog を設定する」

ServerProtect Web コンソールにログオンする

Web コンソールを開くには、ブラウザウィンドウの URL アドレスフィールドに次のいずれかを入力して <Enter> キーを押します。

`http://{ホストサーバの IP アドレス}:14942`

`https://{ホストサーバの IP アドレス}:14943`

ログオン画面がブラウザウィンドウに表示されます。

注意

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。ログアウトした場合には、パスワードを入力して [Log On] をクリックすると、Web コンソールに再びアクセスできます。タイムアウトの初期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 グループにある `SessionTimeout` キーを変更します。詳細については、「**管理者ガイド**」を参照してください。

インストール後にはじめてログオンするときは、ServerProtect にアクセスするのにパスワードは不要です。[Log On] をクリックします。

図 3-1. ServerProtect Web コンソールのログオン画面

[Summary] 画面が表示されます。この画面は、Web コンソールを開いたときの初期設定表示です。ServerProtect の登録とアクティベーションを行っていない場合、この画面には、ServerProtect がまだアクティベートされていないことを示すメッセージが表示されます。

左側のメニューから選択して、ユーザインタフェース内を移動してください。

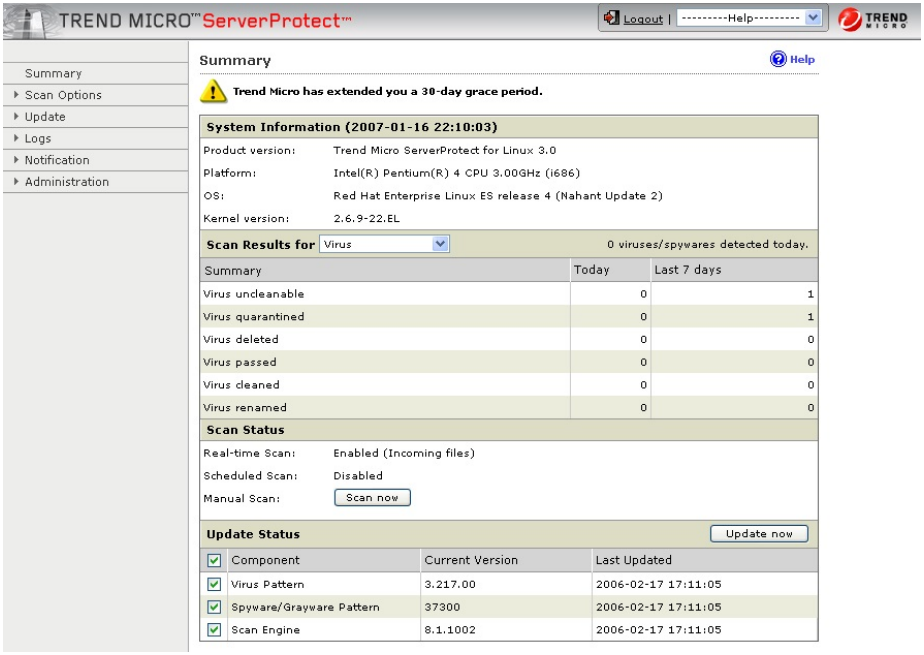

図 3-2. ログオン後の Web コンソールの初期設定表示

注意

リアルタイム検索は初期設定で有効になっています。

Web コンソールからログオフする前に、パスワード付きの管理者アカウントをセットアップすることをお勧めします。

管理者パスワードを設定する

左側のメニューから [Administrator] > [Password] の順に選択すると、[Password] 画面が表示されます。現在のパスワードの入力、および新しいパスワードの入力と確認入力のためのフィールドが表示されます。パスワードは、32 文字以内で、アルファベット、数字 (A〜Z、a〜z、0〜9)、およびハイフン (-) が使用できます。

はじめてログオンしたら、[Current password] フィールドを空白のままにし、[New password] フィールドと [Confirm password] フィールドに同じ情報を入力します。また、後からこの画面でパスワードを変更できます。

インストール後に ServerProtect Web コンソールにログオンする際は、パスワードは空白です(初期設定のパスワードはありません)。

パスワードをコマンドラインからリセットする方法については、「**管理者ガイド**」で `splxmain` コマンドの`-f` オプションに関する説明を参照してください。

プロキシサーバを設定する

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、ServerProtect で次の機能におけるプロキシを設定します。

- ライセンスアップデート
- コンポーネントアップデート

一般的なプロキシ設定

ライセンスアップデート機能でのプロキシの設定手順は次のとおりです。

手順

1. [Administration] > [Proxy Settings] の順に選択します。

   [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] フィールドと [Password] フィールドにこれらの情報を入力します。
7. [Save] をクリックします。

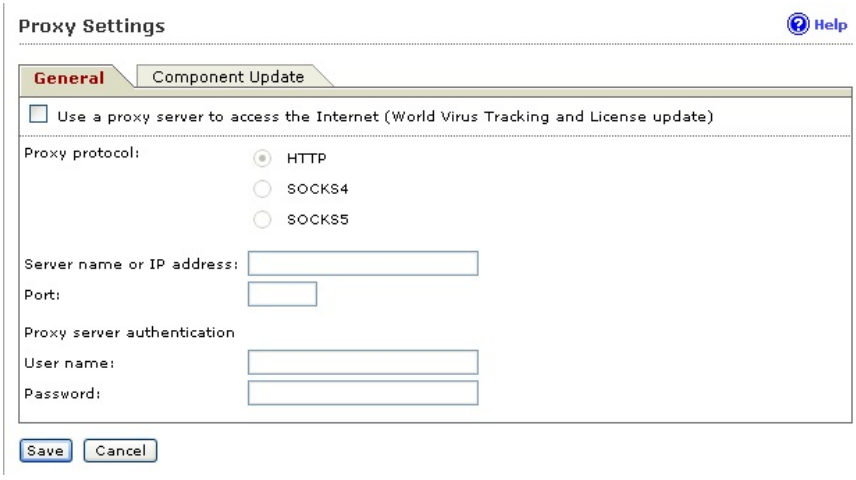

図 3-3. プロキシ設定の [General] 画面

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。

コンポーネントアップデートでのプロキシの設定

検索エンジンとパターンファイルのアップデートに必要なプロキシサーバの設定手順は次のとおりです。

手順

1. [Administration] > [Proxy Settings] > [Component Update] の順に選択します。

   [Component Update] 画面が表示されます。

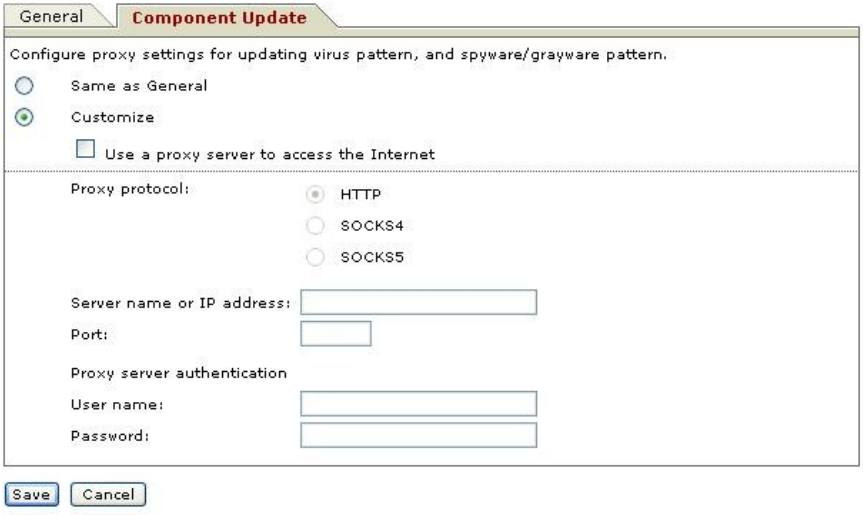

図 3-4. プロキシ設定の [Component Update] 画面

2. 次のいずれかのオプションを選択します。

   - [General] 画面で指定したプロキシサーバの設定と同じ設定を使用するには、[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. コンポーネントのアップデートにプロキシサーバを使用する場合は、[Use a proxy server to access the Internet] を選択します。その後、手順 b に進みます。

コンポーネントのアップデートにプロキシサーバを使用しない場合は、[Use a proxy server to access the Internet] の選択を解除します。これは、たとえば、アップデートサーバが自社のネットワーク内に存在する場合です。その後、手順 3 に進みます。

b. [Proxy Protocol] フィールドで [HTTP]、[SOCKS4] または [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は、[User name] フィールドと [Password] フィールドにこれらの情報を入力します。

3. [Save] をクリックします。

ServerProtect を登録する

トレンドマイクロでは、アクティベーションコードに定められた期間内、すべての登録ユーザの皆さまに、テクニカルサポート、ウイルスパターンファイルのダウンロード、プログラムアップデートの各サービスを提供しています。期間終了後もこれらのサービスを継続してご利用になるには、サポート契約を更新していただく必要があります。ServerProtect を登録して、最新のセキュリティアップデート、その他の製品のサービス、およびメンテナンスサービスが受けられるようにします。ServerProtect の登録は、インストール時でも、インストール後でもできます。

ServerProtect の購入時に、トレンドマイクロまたは販売代理店より、レジストレーションキーまたはシリアル番号/アクティベーションコードを発行します。

レジストレーションキーの形式

レジストレーションキーは、次のような形式で表示されます。

XX-XXXX-XXXX-XXXX-XXXX

アクティベーションコード/シリアル番号の形式

アクティベーションコード/シリアル番号は、次のような形式で表示されます。

XX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

注意

すでにアクティベーションコードをお持ちの場合、オンライン登録の必要はありません。

ServerProtect のアクティベーションコードをすでにお持ちの場合は、32 ページの「アクティベーションを実行する」で説明している手順に従って ServerProtect をアクティベートしてください。

アクティベーションを実行する

ServerProtect のアクティベーションは、次のいずれかの方法で実行できます。

- インストールプロセスで実行する
- Web コンソールから [Product Registration] 画面にアクセスする
- `/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp` フォルダで次のコマンドを入力する

  ```
  ./splxmain -q
  ```

  ServerProtect のアクティベーションはインストール時に実行することをお勧めします。

方法	手順
[Product Registration] 画面で	1. ServerProtect Web コンソールの左側のメニューから、[Administration] > [Product Registration] の順に選択します。 2. [Activation Code] フィールドに ServerProtect のアクティベーションコードを入力します。 3. [Register] をクリックします。ServerProtect がアクティベートされます。

方法	手順

コマンドプロンプトから	1. 次のディレクトリに移動します。
	`/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp`
	2. 次のコマンドを実行すると、ServerProtect がアクティベートされます。
	`./splxmain -q <アクティベーションコード>`

製品版にアップグレードする

インストール時に <Ctrl>+<D> キーを押して登録/アクティベーションの手順を省略した場合、ウイルス/スパイウェアの検索、コンポーネントのアップデートなど、ServerProtect のほとんどの機能は無効になります。インストールされた製品のステータス (アクティベートされているかどうか) は、[Product Registration] 画面で確認できます。次の画面例では、ServerProtect はアクティベートされていません。

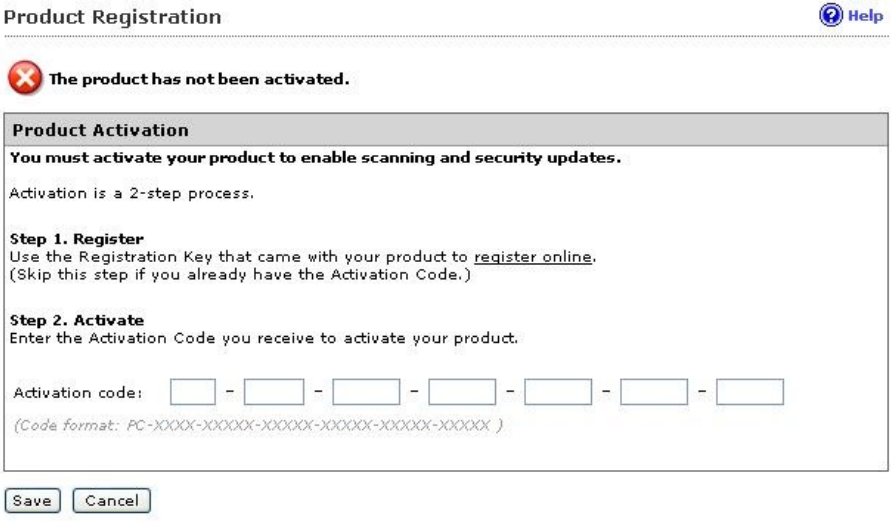

図 3-5. [Product Registration] 画面: アクティベートされていない場合

一定の期間中、ServerProtect のすべての機能を有効にする体験版アクティベーションコードを使用している場合、[Product Registration] 画面の [Version] フィールドに「Trial」と表示されます。次はその画面例です。

図 3-6. [Product Registration] 画面: 体験版

ServerProtect を製品版にアップグレードするには、ServerProtect の登録とアクティベーションを実行します。ServerProtect パッケージに含まれているレジストレーションキーを使用するか、またはトレンドマイクロの販売代理店からレジストレーションキーを購入し、で説明する手順に従って、トレンドマイクロのオンライン登録からアクティベーションコード/シリアル番号を取得します。

次は、製品版 ServerProtect の画面例です。

図 3-7. [Product Registration] 画面: 製品版

コンポーネントをアップデートする

最新のウイルス/不正プログラムやスパイウェアへの対応を確実にするため、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ファイルを手動または自動でアップデートしてください。

手順

1. [Updata] > [Manual Update] の順に選択して [Manual Update] 画面を表示するか、または[Update] > [Scheduled Update] の順に選択して [Scheduled Update] 画面を表示します。
2. [Component] チェックボックスをオンにします。
3. [Save] をクリックします。

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。

EICAR テストウイルスを使用して ServerProtect をテストする

ServerProtect のインストール後、アプリケーションが正常に機能することを確認してください。

EICAR (European Institute for Computer Antivirus Research) は、ウイルス対策ソフトウェアをテストするためのテストウイルスを開発しました。このスクリプトは不活性テキストファイルです。このバイナリパターンは、ほとんどのウイルス対策ベンダーのウイルスパターンファイルに組み込まれています。

テストウイルスは実際のウイルスではないため、プログラムコードが含まれておらず、無害で、自己複製しません。

警告!

ウイルス対策機能のテストでは、実際のウイルスを使用しないでください。

EICAR テストファイルを取得する

EICAR テストファイルは次の Web サイトからダウンロードできます。

http://www.eicar.org/anti_virus_test_file.htm

または、次の文字をテキストファイルに入力またはコピーし、拡張子が com のファイル (virus.com など) として保存します。

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

ファイルをダウンロードする前に、HTTP 検索を無効にする必要があります。ネットワークに Trend Micro InterScan VirusWall がインストールされている場合、テストファイルを、メールに添付して SMTP 検索のテストや FTP/HTTP ファイル転送の確認に使用します。

どちらを選択しても、テストファイルを単にダウンロードするか作成するだけで、リアルタイム検索によってウイルスと同様に検出されます。

Linux に rsyslog を設定する

デバッグログ情報を保存できるようにするには、rsyslog の設定を指定する必要があります。

手順

1. `/etc/rsyslog.conf` を開いて次の手順を実行します。
   a. 次の行をファイルに追加します。

      ```
      # this is for splx debug log
      local3.* /var/log/splx_usr.log
      ```

   b. `#$ModLoad imklog` を探して、テキストから`#`を削除します。
   c. 次の行をファイルに追加します。

      ```
      # this is for KHM debug log
      ```

```
if $msg contains "SPLXMOD" and not($msg contains
"systemd-journal") then {
action(type="omfile" file="/var/log/splx_kern.log")
}
```

2. ターミナルに「service rsyslog restart」と入力して、rsyslog デーモンを再起動します。
3. tmsplx.xml ファイルのデバッグパラメータ (UserDebugLevel) を 5 に設定します。
4. tmsplx.xml ファイルのデバッグパラメータ (KernelDebugLevel) を 3 に設定します。
5. 「service splx restart」と入力して、ServerProtect を再起動します。

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

付録 A

カーネルフックモジュールの構築とインストール

本付録では、RedHat でのカーネルフックモジュール (以下、KHM) の構築およびインストール方法について説明します。

- 40 ページの「はじめに」
- 40 ページの「要件」
- 40 ページの「インストール」

はじめに

KHM は、Trend Micro ServerProtect for Linux (以下、ServerProtect) 用のカーネルモジュールであり、リアルタイム検索機能をサポートします。カーネルモジュール構築の通常の手順と同じ手順に従って、Linux システム上に KHM を構築できます。本書には、コマンドラインの例を記載しています。

このプロセスの概要は次のとおりです。

手順 1: 40 ページの「Linux カーネルのバージョンとアーキテクチャを調べる」

手順 2: 41 ページの「カーネルソースを準備する」

手順 3: 43 ページの「カーネルソースを設定する」

手順 4: 44 ページの「KHM を構築する」

手順 5: 45 ページの「KHM をテストする」

手順 6: 46 ページの「KHM をインストールする」

手順 7: 46 ページの「ServerProtect を再起動する」

要件

KHM を正常に構築するのに必要なものは、次のとおりです。

- Linux システムへの root アクセス権
- GCC
- GNU Make
- 実行カーネルに対応するカーネルソースと設定ファイル
- elfutils-libelf-devel

インストール

Linux カーネルのバージョンとアーキテクチャを調べる

お使いの Linux システムのカーネルのバージョンを調べるには、次のコマンドを使用します。

```
uname -r
```

このコマンドは、文字列 (「4.18.080.el8」など) を返します。本書では、「<カーネルバージョン>」をこの文字列に置き換えます。

お使いの Linux システムのカーネルのアーキテクチャを調べるには、次のコマンドを使用します。

```
uname -m
```

このコマンドは文字列 (通常、「x86_64」) を返します。本書内では、「<アーキテクチャ>」をこの文字列に置き換えます。

注意

ServerProtect Web コンソールの [Summary] 画面でも、同じ情報を確認できます。

カーネルソースを準備する

お使いの Linux システムで設定済みのカーネルソースが利用できるかどうかを確認します。このセクションでは、次の Linux システムのカーネルソースの準備方法について説明します。

- Red Hat Enterprise Linux 10
- カスタム構築した Linux システム

どの Linux ディストリビューションを使用しているか調べるには、ServerProtect Web コンソールの [Summary] 画面をチェックするか、次のコマンドを入力します。

```
uname -a
```

Red Hat Enterprise Linux 10 を使用している場合

次の RPM パッケージがインストールされているかどうかを確認します。

- kernel-devel
- kernel
- kernel-core

- kernel-modules
- kernel-modules-core

注意

これらのパッケージの 1 つがすでにインストールされているかどうか確認する方法については、トラブルシューティングの#1 を参照してください。

RPM パッケージをインストールするには、次のコマンドを入力します。インストールするパッケージは、実行カーネルのバージョンによって決まります。

```
rpm -ivh <rpm package name>
```

例:

実行カーネルのバージョンが「4.18.080.el8」で、アーキテクチャが「x86_64」の場合は、次のように入力します。

```
rpm -ivh kernel-devel-4.18.0-80.el8.x86_64.rpm
```

コマンドラインを使用する他に、次のいずれかを使用してパッケージをインストールすることもできます。

- Linux デスクトップ環境 (たとえば GNOME などで、[Application] > [System Settings] > [Add/Remove Program] の順に選択)
- up2date プログラム

自分で構築したカスタムのカーネルを使用している場合

実行カーネルのバージョンに合わせて、カーネルソースが正しく設定され、準備されているかどうか確認します。

通常、確認するには、次のように入力して、/boot ディレクトリからカーネルソースディレクトリ (/usr/src/linux-<*Kernel Version*>など) に設定ファイルをコピーし、make oldconfig コマンドと make modules_prepare コマンドを実行します。

```
cp /boot/config-<Kernel Version> /usr/src/linux-<Kernel
Version>/.config
```

```
cd /usr/src/linux-<Kernel Version>
```

```
make oldconfig

make modules_prepare
```

カーネルソースを設定する

コンパイル後の KHM のサイズを小さくするため、カーネルの設定の [Kernel Hacking] メニューで [Compile the kernel with debug info] オプションの選択を解除することをお勧めします。

カーネルソースは次のディレクトリにあります。

```
cd /lib/modules/<カーネルバージョン>/build
```

次に、カーネルソースディレクトリで次のコマンドを入力して、設定ユーザインタフェースを表示します。

```
make menuconfig
```

[Kernel Hacking] メニューで [Compile the kernel with debug info] オプションを確認します。この項目の前にアスタリスクが表示されている場合は、キーボードの「N」を入力してアスタリスクを消去します。その後、設定ユーザインタフェースを終了して、設定を保存します。

警告!

設定ユーザインタフェースでは、[Compile the kernel with debug info] オプションのみ、選択解除します。他のオプションは変更しないでください。変更すると、KHM の使用中にカーネルパニックが発生する可能性があります。

注意

「make menuconfig」コマンドの使用中に問題が発生した場合は、使用している Linux システムに「ncurses」パッケージがインストールされていない可能性があります。次のいずれかを実行してください。

- - パッケージをインストールする。Linux インストール CD からパッケージを取得するか、Linux ベンダーの Web サイトからパッケージをダウンロードします。
- - カーネルソースディレクトリにある.config ファイルを変更する。ファイル内の CONFIG_DEBUG_INFO=y を CONFIG_DEBUG_INFO=n に変更します。

設定後、次のコマンドを入力して、カーネルモジュールのコンパイルに使用するソースを準備します。

```
make modules_prepare
```

KHM を構築する

注意

実行カーネルのアーキテクチャが x86_64 の場合、構築プロセスが正常に終了しないときの対処法については、トラブルシューティングの 47 ページのトラブルシューティング#6 を参照してください。

KHM ソースが保存されているディレクトリ (初期設定の位置は/opt/TrendMicro/SProtectLinux/SPLX.module/src/module) に移動します。

make コマンドを使用して新しい KHM を生成します。

```
cd /opt/TrendMicro/SProtectLinux/SPLX.module/src/module

make
```

構築プロセス中に表示される警告メッセージは無視してかまいません。構築プロセスが正常に終了すると、splxmod-<カーネルバージョン>.<アーキテクチャ>.o というファイル名の KHM が bin ディレクトリに生成されます。

KHM をテストする

注意

コンピュータに KHM をインストールする前に、この KHM テストを実行することをお勧めします。このテストにより、動作しない KHM を Linux コンピュータに誤ってインストールしてしまうのを回避できます。このような KHM をインストールすると、システムを再起動するたびにコンピュータがハングアップします。

KHM テストの実行前に、次のように入力して ServerProtect のサービスを停止します。

```
/etc/init.d/splx stop
```

次のコマンドを入力して、構築した KHM の基本機能のテストを実行します。通常、このテストは 5 秒以内に終了します。このテストが 5 秒以上かかる場合は、システムが応答していない可能性があります。

```
make test
```

警告!

このテストスクリプトでは、KHM が動作可能かどうかを確認する基本テストのみが実行されます。テストが正常に終了しても、その KHM がどのような状況でも正常に動作することが保証されたわけではありません。KHM テスト中には、システムがハングアップしたり、カーネルパニックが発生したりすることがあります。そのため、このテストは、テストコンピュータで実行することをお勧めします。

次の場合の対処法については、を参照してください。

- KHM テスト中に Linux コンピュータが応答しなくなった
- KHM テストに失敗した (この場合は、その KHM をインストールしないでください)

KHM をインストールする

コンパイル済み KHM のテストが正常に終了した場合は、次のインストールスクリプトを入力することによって、KHM をインストールできます。

```
make install
```

このコマンドにより、コンパイル済み KHM が/opt/TrendMicro/SProtectLinux/SPLX.module ディレクトリにコピーされます。このディレクトリに同名の KHM がすでに存在する場合は、元のファイルの名前の末尾に.bak が自動的に付加されます。

システムの再起動後、Linux コンピュータが応答しなくなった場合は、トラブルシューティングの#8 を参照してください。

ServerProtect を再起動する

新たにインストールした KHM が使用されるように、ServerProtect を再起動します。

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

付録 B

トラブルシューティング

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

- 48 ページの「Linux 内で、依存ライブラリがないことに関連する問題」
- 48 ページの「KHM の構築とインストール」
- 50 ページの「初期設定のパスワード」
- 50 ページの「Web コンソールでパスワードが拒否される」
- 51 ページの「デバッグログ」

Linux 内で、依存ライブラリがないことに関連する問題

Linux コンピュータに ServerProtect をインストールする前に、次の依存パッケージ (64 ビット版) がインストールされていることを確認します。

- glibc
- libgcc
- zlib
- bzip2
- libuuid
- libstdc++ (Red Hat および CentOS のみ)
- nss-softokn-freebl (Red Hat および CentOS のみ)
- perl-Sys-Syslog (Red Hat および CentOS のみ)
- chkconfig (Red Hat 9 および Red Hat 10 のみ)

KHM の構築とインストール

make プログラムで、カーネルソースパッケージまたはカーネルオブジェクトパッケージをインストールするように求めるプロンプトが表示されたら、どうしたらいいですか。

41 ページの「カーネルソースを準備する」の作業が必ず正常に終了していなければなりません。必要な RPM パッケージがすでにインストールされているかどうか確認するには、次のコマンドを入力します。

```
rpm -q <rpm パッケージ名>
```

必要なパッケージがインストールされていない場合は、Linux ベンダーの Web サイトまたはインストールソース (CD-ROM など) からパッケージを取得して、インストールします。

カスタム構築したカーネルを使用しています。カーネルソースは準備してありますが、「make」コマンドを入力すると、まだ「Unable to locate source package」というメッセージが表示されます。

/usr/src/linux-<カーネルバージョン>ディレクトリにカーネルソースをコピーするか、またはカーネルソースのシンボリックリンクを作成してから、make コマンドを再実行してみてください。

テストプログラムに「Cannot find ... symbol in System.map」というメッセージが表示されます。

KHM が正常に動作するためには、/boot/System.map-<カーネルバージョン> ファイルから特定のシンボルアドレスを取得する必要があります。このファイルがないと、KHM は正常に動作しません。このファイルが存在しなければ、Linux カーネルを再構築してこのファイルを取得しなければならない場合があります。

KHM 構築プロセスが正常に終了しない場合はどうしたらいいですか。

まず、トレンドマイクロの Web サイトにアクセスして、お使いの Linux システムに適した KHM が入手可能かどうか確認します。入手可能な場合は、その KHM をダウンロードして使用します。

トレンドマイクロでの KHM ソースコードの更新状況は、トレンドマイクロの Web サイトで確認できます。Linux カーネルは定期的に更新されているため、トレンドマイクロでも、新しい Linux カーネルに適合するように、それぞれのカーネルに対応する KHM ソースコードを定期的に更新しています。

KHM コードは GPL ベースで発行されているため、このソースコードを変更して、独自の問題解決を試みることもできます。

テストプログラムがクラッシュまたはハングアップした場合や、「Cannot remove KHM from kernel」というメッセージが表示された場合は、どうしたらいいですか。

まず、システムを再起動した後、トレンドマイクロの Web サイトにアクセスして、お使いの Linux システムの KHM が入手可能かどうか確認します。入手可能な場合は、その KHM をダウンロードして使用します。

トレンドマイクロでの KHM ソースコードの更新状況は、トレンドマイクロの Web サイトで確認できます。Linux カーネルは定期的に更新されているた

め、トレンドマイクロでも、新しい Linux カーネルに適合するように、それぞれのカーネルに対応する KHM ソースコードを定期的に更新しています。

KHM コードは GPL ベースで発行されているため、このソースコードを変更して、独自の問題解決を試みることもできます。

KHM をインストールした後、システムの再起動後に Linux コンピュータがハングアップします。

この問題は、Linux コンピュータで正常に動作するかどうかの検証テストを行わずにインストールした KHM に原因がある可能性があります。この問題を解決するには、次の手順に従ってください。

1. Linux コンピュータを再起動して「init 1」モードを開始します (そのためには、GRUB などのブートローダでカーネルのブートパラメータを変更します)。
2. 次のコマンドを入力して、`/opt/TrendMicro/SProtectLinux/SPLX.module` ディレクトリから KHM を削除します。

   ```
   rm /opt/TrendMicro/SProtectLinux/SPLX.module/splxmod-‘uname -r‘. ‘uname -m‘.o
   ```

3. コンピュータを再起動します。今度は、正常に Linux システムが起動するはずです。ただし、KHM はインストールされていないため、ServerProtect のリアルタイム検索は有効ではありません。リアルタイム検索を有効にするには、KHM を再構築します。

この問題を回避するため、新たに構築した KHM をインストールする場合は、事前に「make test」を実行することをお勧めします。

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

  パスワードでは大文字と小文字が区別されます。「TREND」、「Trend」、「trend」では異なるパスワードになります。

- ServerProtect 用にカスタマイズされた 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、「管理者ガイド」を参照してください。

デバッグログ

デバッグログの詳細については、「管理者ガイド」を参照してください。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: Trend Micro Control Manager 関連の処理に対するデ バッグ

付録 C

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。

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

トラブルシューティングのリソース

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

サポートポータルの利用

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

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

脅威データベース

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

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

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

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

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

サポートサービスについて

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

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

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

注意

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

トレンドマイクロへのウイルス解析依頼

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

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

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

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

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

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

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

メールレピュテーションについて

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

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

ファイルレピュテーションについて

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

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

Web レピュテーションについて

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

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

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

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

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

注意

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

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。

索引