Trend Micro™ Smart Protection Server 3.3

インストールガイド

※注意事項

複数年契約について

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

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

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

https://success.trendmicro.com/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

P/N: APEM37915/170817_JP_R1 (2022/06)

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。

Smart Protection Server 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。Smart Protection Server 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

付録 A：設定の移行

索引

はじめに

はじめに

Smart Protection Server インストールガイドへようこそ。このドキュメントには、製品の設定に関する情報が記載されています。

この章の内容は次のとおりです。

トレンドマイクロについて

トレンドマイクロは、ウイルス対策、スパム対策、コンテンツフィルタなど、セキュリティ関連のソフトウェアとサービスを提供し、世界中のユーザのコンピュータを不正コードによる侵害から保護しています。

製品ドキュメント

Smart Protection Server には、次のドキュメントが付属しています。

ドキュメント	説明
インストールガイド	インストール、アップグレード、および配信の計画について説明しています。
管理者ガイド	製品のすべての設定について説明しています。
オンラインヘルプ	各フィールドの詳細な入力手順と、ユーザインタフェースを使用したすべての機能の設定方法について説明します。
Readme ファイル	他のドキュメントには記載されていない可能性のある最新の製品情報が記載されています。機能の説明、インストールのヒント、既知の制限事項、製品リリース履歴などのトピックがあります。

ドキュメントは、次の URL から入手できます。

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

対象読者

Smart Protection Server のドキュメントは IT 管理者を対象としており、読者にコンピュータネットワークについての深い知識があることを前提としています。

このドキュメントでは、読者にウイルス/不正プログラム対策やスパムメール対策のテクノロジに関する知識があることは前提としていません。

ドキュメントの表記規則

Smart Protection Server ユーザ用ガイドでは、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	説明
ナビゲーション > パス	特定の画面へのナビゲーションパス たとえば、[ファイル] > [保存] と記載されている場合、画面の [ファイル] をクリックしてから [保存] をクリックすることを意味します。
 注意	設定上の注意
 ヒント	推奨事項
 警告!	重要な処理や設定オプション

第 1 章

Smart Protection Server のインストールとアップグレードの計画

この章では、Smart Protection Server の新規インストールまたはアップグレードの計画について説明します。

この章の内容は次のとおりです。

システム要件

システム要件のリストについては、次の Web サイトを参照してください。

https://www.go-tm.jp/sps/req

注意

Smart Protection Server には、パフォーマンスの強化および調整が行われた専用の 64 ビット Linux OS が付属しています。

配信を計画する

ここでは、ローカル Smart Protection Server のインストール時に設定する環境の決定方法について説明します。

ベストプラクティス

- 手動検索と予約検索を同時に実行しないようにします。グループで検索が重ならないように調整します。
- すべてのクライアントで ScanNow が同時に実行されないように設定します([アップデート後、Scan Now を実行する] オプションなど)。
- 複数の Smart Protection Server をインストールすることで、特定の Smart Protection Server への接続が不通になった場合にも保護を継続できます。
- `ptngrowth.ini` ファイルに変更を加えることで、低速のネットワーク接続 (約 512Kbps) 用に Smart Protection Server をカスタマイズします。

`ptngrowth.ini` ファイルを設定する

手順

1. `/var/tmcss/conf/`の `ptngrowth.ini` ファイルを開きます。

2. 次の推奨値を使用して ptngrowth.ini ファイルを変更します。

```
[COOLDOWN]
ENABLE=1
MAX_UPDATE_CONNECTION=1
UPDATE_WAIT_SECOND=360
```

3. ptngrowth.ini ファイルを保存します。

4. コマンドラインインタフェース (CLI) から次のコマンドを入力して、lighttpd サービスを再起動します。

```
systemctl restart lighttpd
```

配信のガイドライン

ローカル Smart Protection Server を設定する場合は、次の点を考慮します。

- Smart Protection Server は CPU バウンドアプリケーションです。つまり、CPU リソースが増えると、処理される同時要求数も増加します。
- ネットワークインフラストラクチャや同時アップデート要求数または接続数によっては、ネットワーク帯域幅がボトルネックになることがあります。
- Smart Protection Server コンピュータとエンドポイントとの間の同時接続数が多い場合、追加のメモリが必要になることがあります。

インストールを準備する

Smart Protection Server のインストールプロセスでは、既存のシステムがプログラムのインストール用にフォーマットされます。VMware または Hyper-V でインストールする場合、インストールの前に仮想マシンを作成する必要があります。ネットワークで使用する Smart Protection Server コンピュータの数を決定したら、インストールプロセスを開始できます。

ヒント

複数の Smart Protection Server をインストールすることで、特定の Smart Protection Server への接続が不通になった場合にも保護を継続できます。

インストールには、次の情報が必要です。

- プロキシサーバ情報
- ネットワークの要件を満たす仮想マシンサーバ

第 2 章

Smart Protection Server のインストール

この章では、Smart Protection Server のアップグレードとインストールについて説明します。

この章の内容は次のとおりです。

新規インストールを実行する

インストールの要件を整えた後、インストールプログラムを実行してインストールを開始します。

Smart Protection Server のインストール

ここでは、Smart Protection Server をインストールするプロセスについて説明します。

注意

Smart Protection Server 3.1 を使用している場合は、コマンドラインの移行ツールを使用して既存の設定を Smart Protection Server 3.3 に転送できます。

移行を開始するための前提条件については、40 ページの「設定を移行する際の前提条件」を参照してください。詳細については、40 ページの「Smart Protection Server 3.1 から設定を移行する」を参照してください。

手順

1. VMware または Hyper-V サーバ上に仮想マシンを作成し、Smart Protection Server ISO イメージから起動するように仮想マシンを指定します。
2. 仮想マシンを起動します。

[Smart Protection Server へようこそ] 画面が表示されます。

3. Smart Protection Server のインストールに使用する言語を選択します。
4. [続行] をクリックします。

[Trend Micro Smart Protection Server 使用許諾契約書] 画面が表示されます。

5. [同意する] をクリックして、使用条件に同意します。

[インストールの概要] 画面が表示されます。

6. [日付と時刻] をクリックして、日時の設定を確認します。

   a. 日時をカスタマイズするには、[地域] と [都市] をドロップダウンリストから選択するか、地図上で地域をクリックします。

   b. [完了] をクリックします。

7. [ネットワークとホスト名] をクリックして、ネットワークアダプタの設定を確認します。

注意

ブート時に有効にするデバイスをインストール後に変更するには、コマンドラインインタフェース (CLI) にログオンしてください。

ネットワークデバイスが複数ある場合は、すべてのデバイスの設定を指定します。

---

a. 高度なネットワーク設定が必要な場合は、[設定...] をクリックします。

注意

[設定...] ボタンを使用すると、IPv4 設定と IPv6 設定を指定できます。IPv4 の初期設定は [動的な IP 設定 (DHCP)] です。IPv6 の初期設定は [自動ネイバー検出] です。

b. [完了] をクリックします。

8. [インストール先] をクリックして、インストール先のディスクを選択します。

   a. [ローカルの標準ディスク] で仮想ディスクを選択します。

   b. [完了] をクリックします。

9. [root パスワード] をクリックして、次のパスワードを作成します。

   - root パスワード: root アカウントのパスワードを作成します。

     root アカウントは OS シェルへのアクセスに使用するアカウントで、サーバに対するすべての権限を持ちます。このアカウントには最も多くの権限があります。

   - 管理者パスワード: 管理者アカウントのパスワードを作成します。

     管理者アカウントは初期設定の管理アカウントで、Smart Protection Server の Web および CLI 製品コンソールへのアクセスに使用します。このアカウントには、Smart Protection Server アプリケーションに対するすべての権限がありますが、OS シェルへのアクセス権はありません。

注意

パスワードは 6～32 文字で指定してください。安全なパスワードを設定するためには、次の点を考慮してください。

- 文字と数字の両方を含めます。
- (あらゆる言語の) 辞書に含まれている単語の使用を避けます。
- 意図的に間違ったスペルを使用します。
- 単語を結合した語句を使用します。
- 大文字と小文字を組み合わせて使用します。
- 記号を使用します。

a. [完了] をクリックします。

10. [インストールの開始] をクリックします。

警告!

インストールを続行すると、必要なディスク領域のフォーマットとパーティション分割が実行され、OS とアプリケーションがインストールされます。消去できないデータがハードディスク上にある場合は、インストールをキャンセルし、そのデータをバックアップしてから続行してください。

インストールが開始されます。インストールが完了すると、システムが再起動します。

注意

インストールのログファイルは次の場所で確認できます。

`/root/install.log`

11. Smart Protection Server 3.1 を使用している場合は、コマンドラインの移行ツールを使用して既存の設定を Smart Protection Server 3.3 に転送します。

注意

詳細については、40 ページの「Smart Protection Server 3.1 から設定を移行する」を参照してください。

12. Smart Protection Server Web コンソールにログオンし、プロキシ設定の指定など、インストール後のタスクを実行します。その他の設定、トラブルシューティング、または管理タスクを実行する必要がある場合は、Smart Protection Server CLI シェルにログオンします。

    注意

    root アカウントを使用して、すべての権限がある状態で OS シェルにログオンしてください。

13. インストール後のタスクを実行します。

    注意

    詳細については、27 ページのインストール後のタスクを参照してください。

アップグレード

Smart Protection Server 3.2 から Smart Protection Server 3.3 にアップグレードします。

表 2-1. バージョンアップグレードの詳細

バージョン	要件
Smart Protection Server 3.3 へのアップグレード	• インストールの前に、システム要件が満たされていることを確認してください。14 ページの「システム要件」を参照してください。 • Smart Protection Server 3.2 • Web コンソールにログオンする前に、ブラウザのインターネット一時ファイルを削除してください。

アップグレードプロセス中、Web サービスが約 5 分間無効になります。この間は、エンドポイントから Smart Protection Server にクエリを送信できません。アップグレード時は別の Smart Protection Server にエンドポイントをリダイレクトすることをお勧めします。ネットワークにインストールされている Smart Protection Server が 1 つしかない場合は、ピーク外の時間帯にアッ

プグレードすることをお勧めします。Smart Protection Server への接続が復元されると、不審なファイルのログへの記録および検索がただちに実行されます。

注意

SOCKS4 プロキシの設定は Smart Protection Server から削除されています。以前のバージョンで SOCKS4 プロキシを設定していた場合は、本バージョンへのアップグレード後、プロキシを再設定する必要があります。

Smart Protection Server のアップグレード

手順

1. Web コンソールにログオンします。
2. メインメニューの [アップデート] をクリックします。

   ドロップダウンメニューが表示されます。
3. [プログラム] をクリックします。

   プログラム画面が表示されます。
4. [コンポーネントのアップロード] で、[参照] をクリックします。

   [アップロードするファイルの選択] 画面が表示されます。
5. [アップロードするファイルの選択] 画面でアップグレードファイルを選択します。
6. [開く] をクリックします。

   [アップロードするファイルの選択] 画面が閉じて、[プログラムパッケージのアップロード] ボックスにファイル名が表示されます。
7. [アップデート] をクリックします。
8. インストール後のタスクを実行します。

   27 ページのインストール後のタスク を参照してください。

第 3 章

インストール後のタスク

この章では、Smart Protection Server のインストール後のタスクについて説明します。

この章の内容は次のとおりです。

インストール後

次のインストール後のタスクを実行することをお勧めします。

- 最小システム要件でインストールした場合は、admin アカウントを使用してコマンドラインインタフェース (CLI) から次を入力して、ブロックされた Web アクセスログを無効にします。

```
enable
disable adhoc-query
```

- 初期設定を実行します。28 ページの「初期設定」を参照してください。
- スマートスキャンソリューションをサポートする他のトレンドマイクロ製品に、Smart Protection Server 設定を指定します。

注意

[Smart Protection Server のステータス] ウィジェットおよび Smart Protection Server の CLI コンソールに、Smart Protection Server のアドレスが表示されます。

Smart Protection Server をインストールした場合、VMWare Tools をインストールする必要はありません。サーバのカーネルモジュールには、Smart Protection Server に必要な VMWare Tools モジュール (vmxnet3) が含まれています。

初期設定

インストール後、次のタスクを実行します。

重要

Smart Protection Server 3.1 からの移行の場合は、処理を進める前に、Smart Protection Server 移行ツール (Migration.py) を実行して、設定を Smart Protection Server 3.3 に転送します。

詳細については、「40 ページの「Smart Protection Server 3.1 から設定を移行する」」を参照してください。

手順

1. Web コンソールにログオンします。

   ようこそ画面が表示されます。

2. [初回インストールの設定] をクリックします。

   初回インストール用の設定ウィザードが表示されます。

3. [ファイルレピュテーションサービスを有効にする] チェックボックスをオンにします。

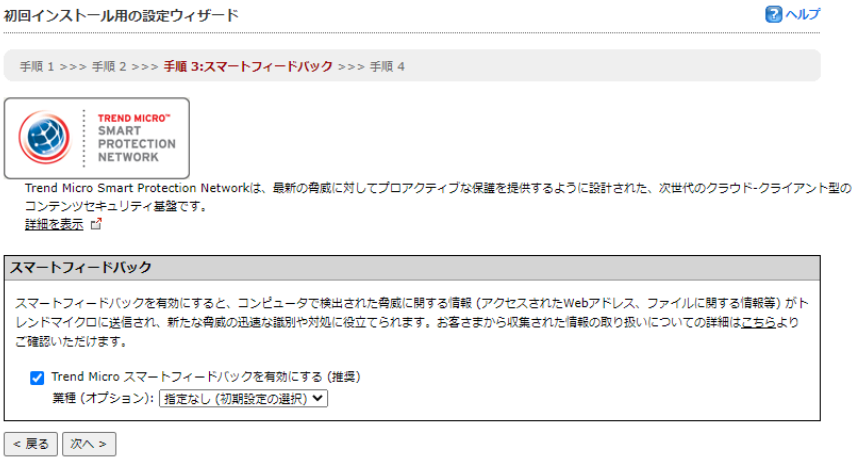
4. [次へ] をクリックします。

   [Web レピュテーションサービス] 画面が表示されます。

5. [Web レピュテーションサービスを有効にする] チェックボックスをオンにします。

6. (オプション) フィルタの優先度を設定すると、URL クエリのフィルタ順を指定できます。
7. [次へ] をクリックします。

[スマートフィードバック] 画面が表示されます。



8. スマートフィードバックを有効にします。ユーザからの支援によって、トレンドマイクロは新しい脅威に対してより迅速にソリューションを提供できるようになります。

9. [次へ] をクリックします。

[プロキシ設定] 画面が表示されます。

10. ネットワークでプロキシサーバを使用する場合は、プロキシ設定を指定します。
11. [完了] をクリックして、Smart Protection Server の初期設定を終了します。

    Web コンソールの [概要] 画面が表示されます。

注意

Smart Protection Server は、初期設定の後、自動的にパターンファイルをアップデートします。

第 4 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

設定の移行

この章では、移行ツールを使用して Smart Protection Server 3.x から設定を移行する方法について説明します。

この章の内容は次のとおりです。

設定を移行する際の前提条件

Smart Protection Server には、既存の設定を Smart Protection Server 3.1 から最新バージョンに転送できるコマンドラインの移行ツールが用意されています。

重要

Smart Protection Server の以前のバージョンから設定を移行できるのは、Smart Protection Server 3.3 の初期設定を行う前に限られます。Smart Protection Server 3.3 の初期設定後は、サーバをアンインストールして再インストールしない限り、設定を移行することはできなくなります。

移行を開始するための前提条件は次のとおりです。

要件	説明
仮想マシン	• Smart Protection Server 3.3 には、移行元のコンピュータと同等以上の仕様の仮想マシンインスタンスが必要です。 • ツールを実行する前に、仮想マシンインスタンスに Smart Protection Server 3.3 ISO をインストールしておく必要があります。
SSH	移行元の Smart Protection Server で SSH が有効になっている必要があります。 詳細については、オンラインヘルプまたは管理者ガイドを参照してください。
不審オブジェクトの同期	不審オブジェクトの同期が有効になっている場合は、新しい仮想マシンと不審オブジェクトのソースの間で接続が確立されていることを確認してください。

Smart Protection Server 3.1 から設定を移行する

Smart Protection Server には、既存の設定を Smart Protection Server 3.1 から最新バージョンに転送できるコマンドラインの移行ツールが用意されています。

重要

Smart Protection Server の以前のバージョンから設定を移行できるのは、Smart Protection Server 3.3 の初期設定を行う前に限られます。Smart Protection Server 3.3 の初期設定後は、サーバをアンインストールして再インストールしない限り、設定を移行することはできなくなります。

移行を開始するための前提条件については、40 ページの「設定を移行する際の前提条件」を参照してください。

手順

1. Smart Protection Server 3.3 の仮想マシンで、root アカウントの資格情報を使用してコマンドラインを開きます。
2. 作業ディレクトリを`/usr/tmcss/bin/MigrationTool` に変更します。
3. 次のコマンドを使用して、移行ツールを実行します。

   ```
   #>./Migration.py
   ```

   サーバ情報の入力を求められます。
4. [Server location] に以前のサーバ (設定の移行元) の Smart Protection Server の場所を入力します。

   注意

   場所は IP アドレスまたは FQDN の形式で指定でき、SSH 接続を使用して指定した場所が確認されます。
5. 以前のサーバから設定を取得するには、root アカウントとパスワードを入力します。

   以前のサーバからの設定移行プロセスが開始されます。データベースのサイズによっては、移行プロセスが完了するまでに時間がかかることがあります。移行プロセスが完了すると、Smart Protection Server 3.3 が自動的に再起動し、移行した設定が適用されます。

重要

移行プロセスで問題が発生した場合、Smart Protection Server は再起動せず、エラーメッセージのリストが表示されます。移行時のエラーログファイルは次の場所で確認できます。

```
/var/tmcss/debuglogs/SPSMigration.log
```

6. 管理者アカウントで Smart Protection Server 3.3 のコンソールを開き、移行した設定を確認します。

   - ファイルレピュテーションサービスと Web レピュテーションサービスのパターンファイルのステータスを確認します。

     a. [アップデート] > [パターンファイル] の順に選択します。

     b. [ファイルレピュテーション] と [Web レピュテーション] の設定が正しいことを確認します。

     c. パターンファイルが誤って無効になっている場合は、[アップデート] をクリックして最新のパターンファイルを取得します。

     注意

     アップデートが失敗する場合は、インターネットにアクセスできること、およびプロキシ設定 ([管理] > [プロキシ設定]) が正しいことを確認してください。

   - [Smart Protection] > [不審オブジェクト] の順に選択し、[不審オブジェクトを同期して有効化] が正しく設定されていることを確認します。

     注意

     [不審オブジェクトを同期して有効化] が無効になっている場合は、仮想アナライザの [ソース] と [API キー] の情報を確認し、[登録] をクリックします。

   - Smart Protection Server Web コンソールで、その他のすべての設定を確認します。

7. 以前の Smart Protection Server 3.1 で証明書が必要だった場合は、証明書を再インポートする必要があります。

注意

詳細については、「*Smart Protection Server* ***管理者ガイド***」を参照してください。

8. Smart Protection Server 3.3 コンソールで以前のバージョンの Smart Protection Server と同じ IP アドレスを引き続き使用する場合は、以前のバージョンの Smart Protection Server をシャットダウンします。

索引