Trend Micro™ Smart Protection Server 3.3

管理者ガイド

Endpoint Security

Messaging Security

Protected Cloud

Web 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。

http://esupport.trendmicro.com/ja-jp/support-lifecycle/default.aspx

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 InterScan WebManager SCC、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Securing Your Journey to the Cloud、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、および Trend Micro Policy-based Security Orchestration は、トレンドマイクロ株式会社の登録商標です。

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

P/N: APEM37914/170817_JP_R2 (2017/12)

目次

はじめに

第 1 章：Trend Micro Smart Protection Server の概要

第 2 章：Smart Protection Server の使用

第 3 章：Smart Protection Server の監視

第 4 章：Trend Micro Control Manager との統合

第 5 章：サポート情報

はじめに

Smart Protection Server 管理者ガイドへようこそ。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。

http://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 管理者ガイドでは、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

Trend Micro Smart Protection Server の概要

この章では、Trend Micro Smart Protection Server について紹介し、その機能を説明します。

この章の内容は次のとおりです。

Smart Protection Server のしくみ

Smart Protection Server は、クラウドベースの次世代の高度な保護ソリューションです。このソリューションは、クラウドに保存された不正プログラム対策のシグネチャを利用する、高度な検索アーキテクチャを中核に構成されています。

このソリューションでは、セキュリティリスクの検出にファイルレピュテーションおよび Web レピュテーションテクノロジを利用します。このテクノロジにより、これまでエンドポイントに保存されていた大量の不正プログラム対策シグネチャおよびリストが Smart Protection Server に移行されます。

この手法を使用することによって、システムやネットワークに影響を与える、増加し続けるシグネチャアップデートのエンドポイントへのダウンロード量を大幅に削減できます。

新しいソリューションのニーズ

従来のファイルベースの脅威処理方法では、エンドポイントの保護に必要なパターンファイル (または定義) のほとんどの部分が定期的に配信されています。パターンファイルは、トレンドマイクロからエンドポイントにまとめて送信されます。エンドポイント上のウイルス/不正プログラム対策ソフトウェアは、新しいアップデートを受信すると、新しいウイルス/不正プログラムのリスクに対応するために一連のパターン定義をメモリに再度読み込みます。新しいウイルス/不正プログラムのリスクが出現した場合には、保護を継続するために、パターンファイルの一部または全部を再度アップデートして、エンドポイントに読み込むことが必要になります。

長い間に、出現する脅威の絶対数は大幅に増加してきました。脅威の量の増加は、近年、指数級数的な伸びを示しています。この増加のペースは今日の既知のセキュリティリスクの量を大きく上回り、今後は、このセキュリティリスクの量が新種のセキュリティリスクになると予想されます。セキュリティリスクの量は、サーバやワークステーションのパフォーマンス、ネットワーク帯域幅の使用率、また一般に、適切な保護を提供するまでの全体的な時間や「保護にかかる時間」に影響する可能性があります。

トレンドマイクロでは、ユーザがウイルス/不正プログラムなどの増え続ける脅威にも対抗できることを目指した新しい手法を開発しました。この先駆的

な技術で使用されるテクノロジとアーキテクチャには、ウイルス/不正プログラムのシグネチャやパターンファイルの保存をクラウドに移行するテクノロジが採用されています。ウイルス/不正プログラムのシグネチャの保存をクラウドに移行することにより、将来出現する量のセキュリティリスクからユーザを適切に保護できます。

Trend Micro Smart Protection Network ソリューション

クラウドベースのクエリ処理では、次の 2 つのネットワークベースのテクノロジを使用できます。

- Trend Micro Smart Protection Network: 企業ネットワークに直接アクセスできないユーザにサービスを提供する、グローバル規模のインターネットベースインフラストラクチャです。
- Smart Protection Server: Smart Protection Server はローカルネットワーク内に配置して、ローカルの企業ネットワークにアクセス可能なユーザから利用できるようにします。これらのサーバは、効率を最適化するために、処理を企業ネットワーク内で実行するように設計されています。

注意

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。

これら 2 つのネットワークベースソリューションでは、大量のウイルス/不正プログラムパターン定義および Web レピュテーションスコアがホストされています。Smart Protection Network および Smart Protection Server では、潜在的な脅威の確認のためにネットワーク上の他のエンドポイントでこれらの定義を利用できるようにします。クエリが Smart Protection Server に送信されるのは、エンドポイントでファイルまたは URL のリスクを特定できなかった場合のみです。

エンドポイントは、通常のシステム保護処理の一環として、ファイルレピュテーションおよび Web レピュテーションテクノロジを利用して Smart Protection Server にクエリを実行します。このソリューションでは、エージェントから、トレンドマイクロのテクノロジによって判定された識別情報がクエリとして Smart Protection Server へ送信されます。ファイルレピュテーショ

ンテクノロジの使用時は、エージェントからファイル全体が送信されることはありません。ファイルのリスクは、識別情報を使用して判定されます。

パターンファイル

ファイルレピュテーションサービスおよび Web レピュテーションサービスには、Smart Protection のパターンファイルを使用します。トレンドマイクロでは、これらのパターンファイルをトレンドマイクロのアップデートサーバから提供しています。

パターンファイルの種類は次のとおりです。

表 1-1. Smart Protection Server のパターンファイル

レピュテーションサービス	パターンファイル	詳細
ファイルレピュテーションサービス	スマートスキャンパターン	クラウドベースのクエリ処理では、スマートスキャンパターンファイルとリアルタイムクラウドクエリシステムが併用されます。クラウドクエリシステムは、検索処理時に、Smart Protection Server に対してファイル、URL、およびその他のコンポーネントを検証します。Smart Protection Server は、いくつかのアルゴリズムを使用して、ネットワーク帯域幅の使用率を最低限に抑える効率的な処理を実現します。 スマートスキャンパターンファイルは 1 時間ごとに自動的に更新されます。

レピュテーションサービス	パターンファイル	詳細
Web レピュテーションサービス	Web ブロックパターンファイル	Web レピュテーションサービスを使用する製品 (ウイルスバスター Corp.や Deep Security など) では、Smart Protection Server に Web レピュテーションクエリを送信することで、Web ブロックパターンファイルを照会して Web サイトのレピュテーション (評価) を確認します。これらの製品では、Smart Protection ソースから受信したレピュテーションデータをエンドポイントに適用された Web レピュテーションポリシーと照合し、そのポリシーに応じてサイトへのアクセスを許可またはブロックします。 注意 Web レピュテーションサービスを使用する製品の一覧については、「54 ページの「トレンドマイクロ製品およびサービスとの統合」」を参照してください。

パターンファイルのアップデート処理

パターンファイルのアップデートは、セキュリティ上の脅威に対応します。Smart Protection Network および Smart Protection Server は、アップデートサーバからスマートスキャンパターンファイルをダウンロードします。Smart Protection Server をサポートするトレンドマイクロ製品は、アップデートサーバからスマートスキャンエージェントパターンをダウンロードします。

イントラネット内のエンドポイントは、Smart Protection Server をサポートするトレンドマイクロ製品からスマートスキャンエージェントパターンファイルをダウンロードします。外部エンドポイントは、イントラネットの外部にあ

るエンドポイントなので、Smart Protection Server、または Smart Protection Server をサポートするトレンドマイクロ製品に接続できません。

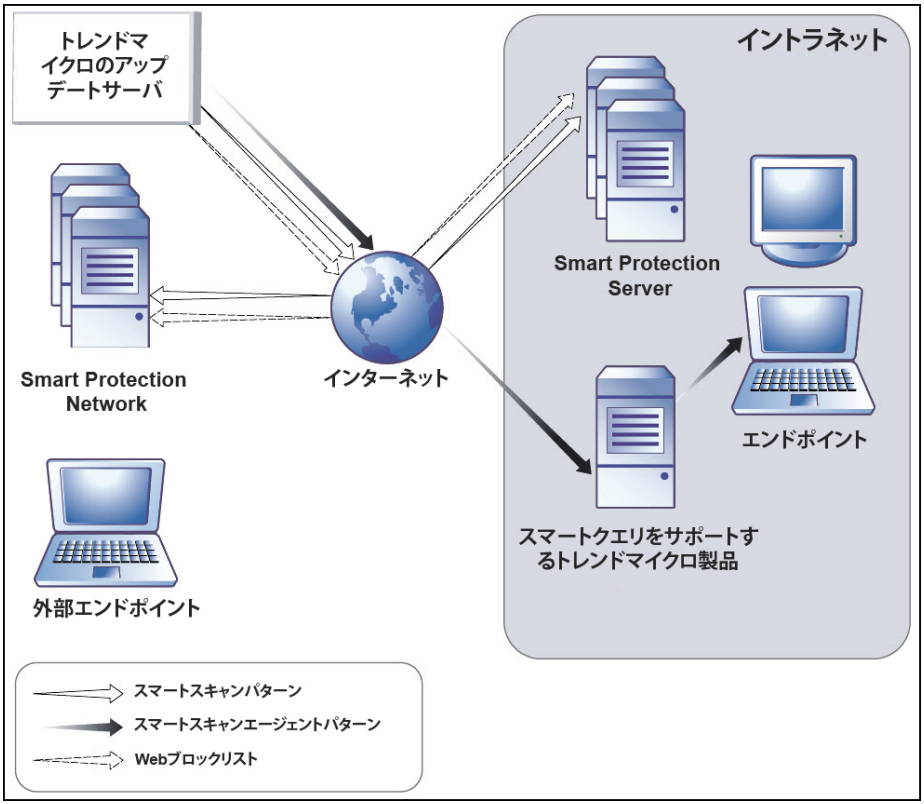


図 1-1. パターンファイルのアップデート処理

クエリ処理

イントラネット内に存在するエンドポイントは、Smart Protection Server を使用してクエリを処理します。イントラネット内に存在しないエンドポイントは、Smart Protection Network に接続してクエリを処理できます。

Smart Protection Server を利用するにはネットワーク接続が必須ですが、ネットワーク接続を利用できないエンドポイントもトレンドマイクロテクノロジを

利用できます。スマートスキャンエージェントパターンおよびエンドポイント内の検索テクノロジは、ネットワーク接続を利用できないエンドポイントを保護します。

エンドポイントにインストールされたエージェントは、最初にエンドポイントで検索を実行します。エージェントがファイルまたは URL のリスクを判定できない場合には、Smart Protection Server にクエリを送信してリスクを検証します。

表 1-2. イントラネットへのアクセスに基づいた保護の動作

場所	パターンファイルおよびクエリの動作
イントラネットへのアクセス	• パターンファイル: エンドポイントは、Smart Protection Server をサポートするトレンドマイクロ製品からスマートスキャンエージェントパターンファイルをダウンロードします。 • クエリ: エンドポイントは、Smart Protection Server に接続してクエリを処理します。
イントラネットへのアクセスなし	• パターンファイル: エンドポイントは、Smart Protection Server をサポートするトレンドマイクロ製品への接続が利用できない限り、最新のスマートスキャンエージェントパターンファイルをダウンロードしません。 • クエリ: エンドポイントは、スマートスキャンエージェントパターンファイルなどのローカルリソースを使用してファイルを検索します。

高度なフィルタリングテクノロジにより、エージェントではクエリの結果を「キャッシュ」できます。これにより、検索パフォーマンスが向上し、同じクエリを Smart Protection Server に何度も送信する必要はなくなります。

特定ファイルのリスクをローカルで確認できないエージェントが、Smart Protection Server への数回の接続試行後も接続できない場合には、そのファイルに検証フラグが付けられ、ファイルへの一時的なアクセスが許可されます。Smart Protection Server への接続が復元されると、フラグが付けられたすべてのファイルが再度検索されます。その後、ネットワークへの脅威として確認されたファイルには適切な検索処理が実行されます。

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。

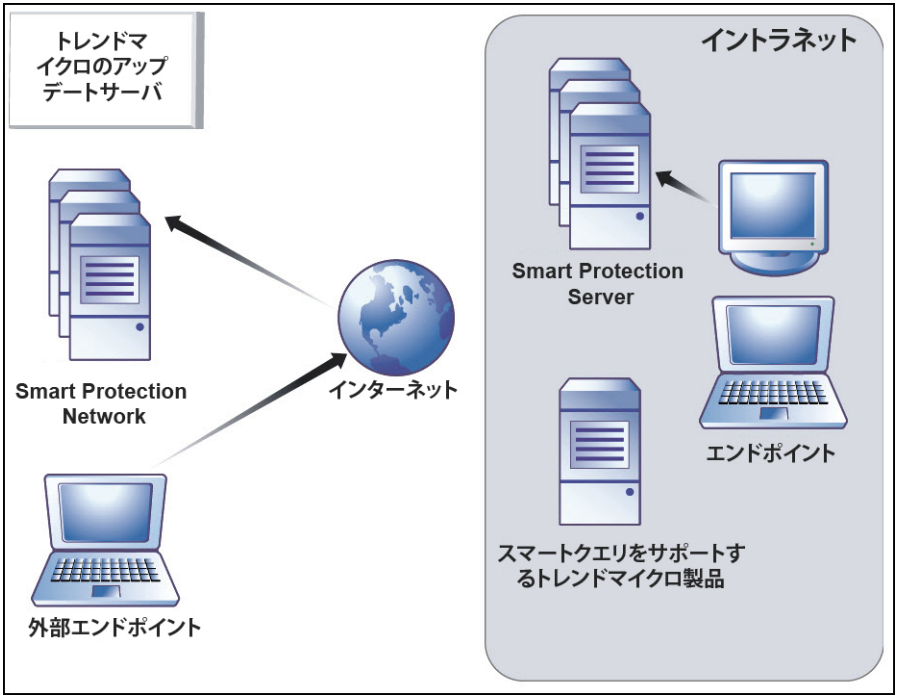


図 1-2. クエリ処理

このリリースの新機能

Smart Protection Server の新機能と強化された機能は次のとおりです。

表 1-3. バージョン 3.3 の新機能

機能	説明
[概要] 画面の改良	Smart Protection Server のダッシュボードが改良され、すべてのウィジェットおよびタブがより合理的に表示されるようになりました。 詳細については、60 ページの「[概要] 画面の使用」を参照してください。
コミュニティドメイン/IP レピュテーションサービスのサポート	Smart Protection Server でコミュニティドメイン/IP レピュテーションサービスのクエリがサポートされるようになりました。 詳細については、54 ページの「トレンドマイクロ製品およびサービスとの統合」を参照してください。
Trend Micro Control Manager 7.0 の統合	Smart Protection Server は、次の機能を通じて Control Manager 7.0 と統合されています。 • Smart Protection Server への Control Manager コンソールからのシングルサインオン (SSO) • 不審オブジェクトリストの自動同期 • Smart Protection Server のステータス情報 (パターンファイルのバージョン、サービスの実行ステータス、サーバのビルドバージョンなど) を Control Manager コンソールに表示 詳細については、82 ページの「サポートされている Control Manager のバージョン」を参照してください。 Control Manager 7.0 は、2017 年 11 月現在、日本においてはリリースされておりません。最新のリリース状況については、最新版ダウンロードページをご参照ください。 http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp
Web レピュテーションでの HTTPS のサポート	このバージョンの Smart Protection Server では、Web レピュテーションサービスで HTTPS 接続がサポートされるようになりました。 詳細については、91 ページのコマンドラインインタフェース (CLI) のコマンドを参照してください。

機能	説明
新しいブラウザのサポート	Smart Protection Server では、Google Chrome がサポートされるようになりました。

主な機能と利点

Smart Protection Server は、次に挙げる機能と利点を提供します。

- ファイルレピュテーションテクノロジ
  - 企業ネットワークで脅威を適切に処理できます。
  - 脅威の発生に対して全体的な「保護までの時間」が大幅に短縮されます。
  - クライアントコンピュータでのカーネルメモリの消費が大幅に削減され、将来の増加量も最小限度に抑えられます。
  - 管理が単純化および合理化されます。大量のパターン定義のアップデートは 1 つのサーバだけで済み、多数のクライアントコンピュータで行う必要はありません。これにより、多くのクライアントコンピュータで、パターンファイルをアップデートすることによる影響がほとんどなくなります。
  - Web ベースの攻撃や複合攻撃に対して保護されます。
  - ウイルス/不正プログラム、トロイの木馬、ワーム、およびこれらのセキュリティリスクの新しい変種を阻止します。
  - スパイウェア/グレーウェア (非表示のルートキットを含む) を検出し、削除します。
- Web レピュテーションテクノロジ
  - Web ベースの攻撃や複合攻撃に対して保護されます。
  - Web レピュテーションクエリでは Trend Micro Smart Protection Network に機密情報を開示する必要がありません。これは、プライバシーの保護を重視するユーザにとって有用です。

- クエリに対する Smart Protection Server の応答時間は、Trend Micro Smart Protection Network へのクエリと比較して短縮されます。
- Smart Protection Server をネットワークにインストールすることで、ゲートウェイの帯域幅の負荷が削減されます。

Trend Micro Smart Protection Network

Smart Protection Network は、ユーザをセキュリティリスクや Web からの脅威から保護するように設計された、次世代のクラウドクライアント型のコンテンツセキュリティ基盤です。このソリューションでは、軽量エージェントを使用し、独自のインターネットクラウドで提供されているメールレピュテーション、Web レピュテーション、ファイルレピュテーションの相関分析テクノロジおよび脅威データベースにアクセスすることで、ローカルソリューションおよびホステッドソリューションの機能を強化して、企業ネットワーク内、自宅、または外出先にいるユーザを保護します。より多くの製品、サービス、およびユーザがネットワークにアクセスすれば、それだけ顧客の保護機能が自動的に更新および強化されることになり、ユーザ自身のリアルタイムな自警システムが構築されていきます。

ファイルレピュテーションサービス

ファイルレピュテーションサービスは、インターネット上のクラウドに格納されている膨大なデータベースを照会して対象ファイルのレピュテーション (評価) を確認します。不正プログラム情報はクラウドに格納されているので、すべてのユーザがただちに使用できます。パフォーマンスに優れたコンテンツ配信ネットワークとローカルのキャッシュサーバによって、確認プロセスで発生する待ち時間は最小限に抑えられます。クラウド-クライアント型のアーキテクチャは、より迅速な保護を実現し、パターンファイル配信の負荷を解消することに加えて、エージェントの全般的なフットプリントを大幅に削減します。

Web レピュテーションサービス

世界最大のドメインレピュテーションデータベースの 1 つを使用するトレンドマイクロの Web レピュテーションテクノロジは、Web サイトの経過日数、

配置場所の変更履歴、および不正プログラムの挙動分析により検出された不審な活動の兆候などの要素に基づいてレピュテーションスコアを割り当てることにより、Web ドメインの信頼性を追跡します。サイトは継続的に検索され、感染サイトへのユーザアクセスがブロックされます。Web レピュテーション機能によって、ユーザがアクセスするページの安全を維持し、Web からの脅威の影響を受けないようにできます。Web からの脅威には、不正プログラム、スパイウェア、フィッシング詐欺などがあり、ユーザをだまして個人情報を入力させるように設計されています。精度を向上させると同時に誤検出を少なくするため、トレンドマイクロの Web レピュテーションテクノロジでは、サイト全体を分類またはブロックするのではなく、サイト内の特定のページまたはリンクにレピュテーションスコアを割り当てています。これは、多くのケースで正規サイトの一部分のみがハッキングされ、時間の経過とともにレピュテーションが動的に変化していることに対応する処理です。

Web レピュテーション機能によって、ユーザがアクセスする Web ページの安全を維持し、Web からの脅威の影響を受けないようにできます。Web からの脅威には、不正プログラム、スパイウェア、フィッシング詐欺などがあり、ユーザをだまして個人情報を入力させるように設計されています。Web レピュテーションは、レピュテーションの評価を基に Web ページをブロックします。Web レピュテーションを有効にすると、ユーザが不正な URL にアクセスするのを阻止することができます。

スマートフィードバック

Trend Micro スマートフィードバックは、トレンドマイクロ製品間、さらに弊社が所有する 24 時間体制の脅威に関する研究センターおよびテクノロジとの間に、継続的な両方向の情報交換を実現します。個々の顧客の定期的なレピュテーションチェックで検出された新しい脅威がトレンドマイクロのすべての脅威データベースに自動的に反映され、その脅威に対する最新の防御情報が世界中のトレンドマイクロ製品に届けられて、すぐに利用可能になります。トレンドマイクロでは、顧客とパートナーの大規模なグローバルネットワークを通じて収集された脅威に関する情報を継続的に処理することにより、最新の脅威に対して自動的なリアルタイムの保護を実現し、「相互の連携が強化された」セキュリティを提供します。これは、地域住民がコミュニティを主体的に保護する自警団のように機能します。情報源のレピュテーションに基づいて脅威情報が収集されるため、顧客の個人情報やビジネス情報のプライバシーは常に保護されます。

第 2 章

Smart Protection Server の使用

この章では、Smart Protection Server の設定情報について説明します。

この章の内容は次のとおりです。

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、インストールガイドの「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。

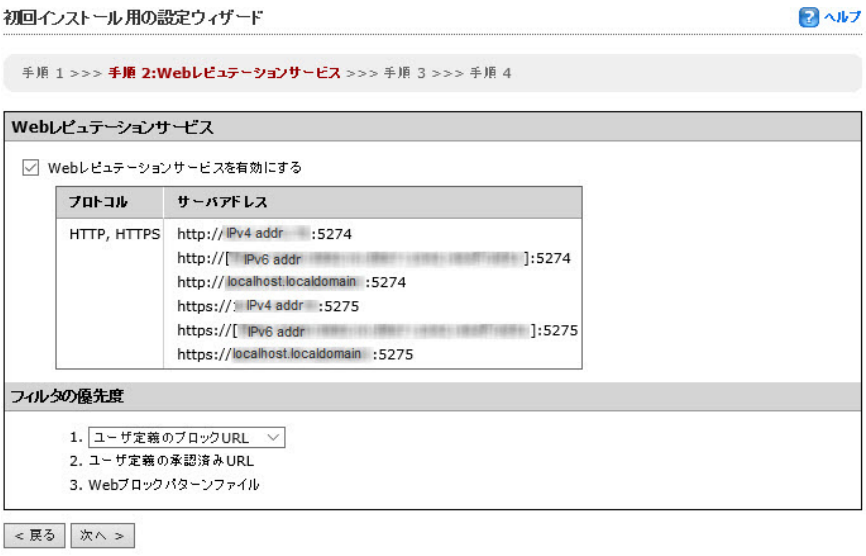
   初回インストール用の設定ウィザードが表示されます。

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。

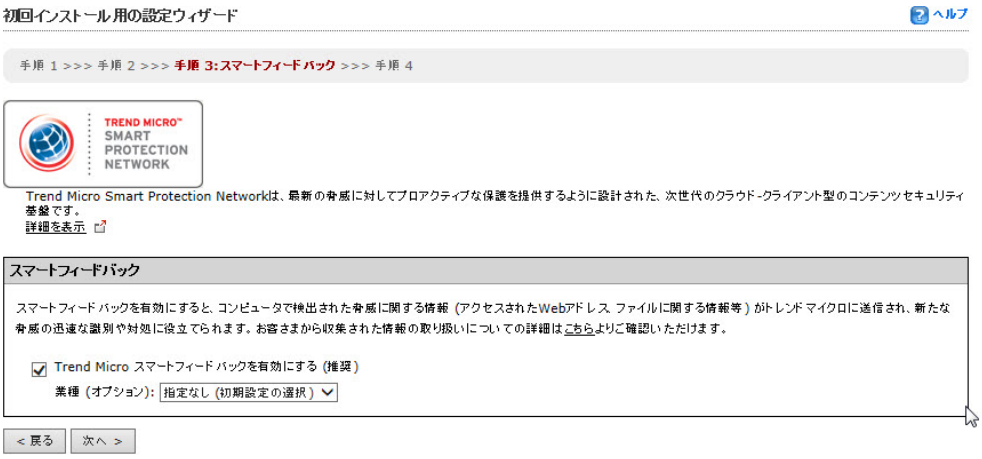
   [Web レピュテーションサービス] 画面が表示されます。

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。

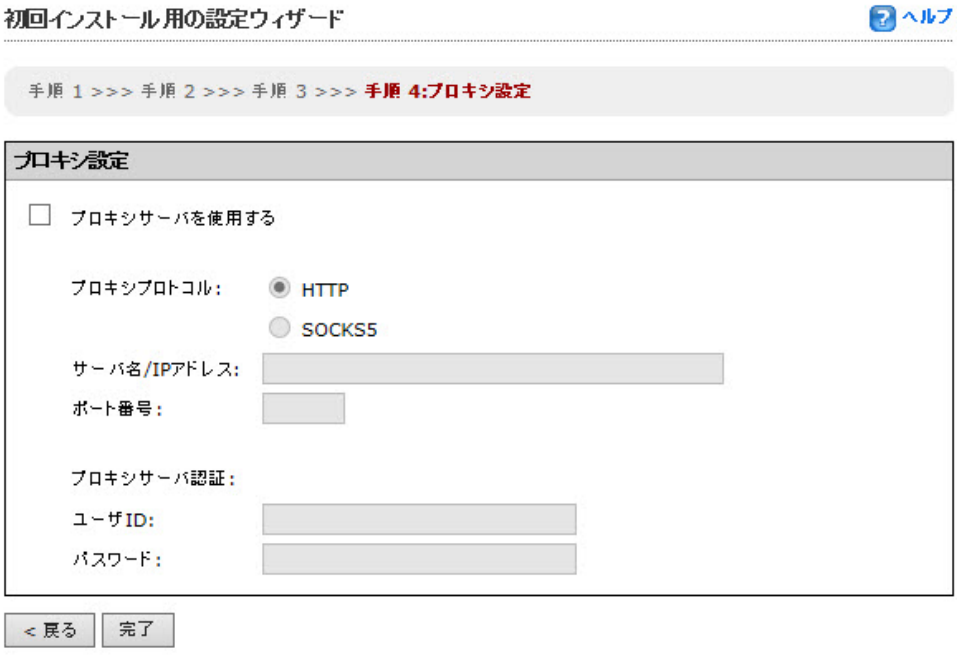
   [スマートフィードバック] 画面が表示されます。



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。

製品コンソールの使用

製品コンソールは、次の要素で構成されています。

- メインメニュー: [概要]、[Smart Protection]、[アップデート]、[ログ]、[管理] 画面へのリンクが表示されます。
- 作業領域: 概要情報とコンポーネントステータスの表示、設定の指定、コンポーネントのアップデート、および管理タスクを実行します。

メニュー	説明
概要	ウィジェットを追加すると、Smart Protection Server、トラフィック、および検出に関するカスタマイズされた情報が表示されます。
Smart Protection	レピュテーションサービス、ユーザ定義の URL、不審オブジェクト、およびスマートフィードバックの設定オプションがあります。
アップデート	予約アップデート、手動のプログラムアップデート、プログラムパッケージのアップロード、およびアップデート元を設定するためのオプションがあります。
ログ	ログのクエリ設定やメンテナンス用のオプションがあります。

メニュー	説明
管理	SNMP サービス、通知、プロキシ設定、およびトラブルシューティングのための診断情報の収集方法を設定するオプションがあります。

製品コンソールへのアクセス

Web コンソールへのログオン後、初期画面に Smart Protection Server のステータス概要が表示されます。

手順

1. Web ブラウザを開いて、インストール後の最初の CLI バナーに表示された URL を入力します。
2. ユーザ名のフィールドに「`admin`」、パスワードのフィールドにインストール時に設定したパスワードを入力します。
3. [ログオン] をクリックします。

Trend Micro Smart Protection の使用

このバージョンの Smart Protection Server には、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が導入されています。

レピュテーションサービスの使用

製品コンソールでレピュテーションサービスを有効にして、他のトレンドマイクロ製品が Smart Protection を使用できるようにします。

ファイルレピュテーションサービスの有効化

ファイルレピュテーションサービスを有効にして、エンドポイントからのクエリをサポートします。

手順

1. [Smart Protection] > [レピュテーションサービス] の順に選択し、[ファイルレピュテーション] タブを選択します。

2. [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。

3. [保存] をクリックします。

   これで、Smart Protection Server をサポートする他のトレンドマイクロ製品からのファイルレピュテーションクエリにサーバアドレスを使用できるようになります。

Web レピュテーションサービスの有効化

Web レピュテーションサービスを有効にして、エンドポイントからのクエリをサポートします。使用可能なオプションについての簡単な説明を次に示します。

- Web レピュテーションサービスを有効にする: エンドポイントからの Web レピュテーションクエリをサポートします。
- サーバアドレス: このオプションは、Web レピュテーションクエリ用として他のトレンドマイクロ製品によって使用されます。
- フィルタの優先度: URL をフィルタ処理するときの優先度を指定します。

手順

1. [Smart Protection] > [レピュテーションサービス] の順に選択し、[Web レピュテーション] タブをクリックします。
2. [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。
3. (オプション) URL をフィルタ処理するときのユーザ定義の承認済み URL/ブロック URL の優先度を指定します。たとえば、ユーザ定義のブロック URL の優先度を 1 にすると、ユーザ定義の承認済み URL の優先度は 2 になります。

4. [保存] をクリックします。

   これで、Smart Protection Server をサポートする他のトレンドマイクロ製品からの Web レピュテーションクエリにサーバアドレスを使用できるようになります。

ユーザ定義の URL の設定

[ユーザ定義の URL] では、承認する URL とブロックする URL を独自に指定できます。これは、Web レピュテーションに使用されます。使用可能なオプションについての簡単な説明を次に示します。

- 検索ルール: ルールのリスト内の文字列を検索します。
- テスト URL: URL がトリガするルールを検索します。URL は、「`http://`」または「`https://`」で始まっている必要があります。

手順

1. [Smart Protection] > [ユーザ定義の URL] の順に選択します。
2. [検索条件] で [追加] をクリックします。

   [ルールの追加] 画面が表示されます。

3. [このルールを有効にする] チェックボックスをオンにします。
4. 次のいずれかの方法を選択します。
   - URL: URL を指定して、その URL のすべてのサブサイトに適用するか、1 つのページだけに適用するかを指定します。
   - URL とキーワード: 文字列を指定し、正規表現を使用します。

   [テスト] をクリックすると、最も多く使用されている 20 件の URL と、Web アクセスログ内の前日の上位 100 件の URL へ、このルールを適用した結果が表示されます。

5. 次のいずれかの方法を選択します。
   - すべてのクライアント: すべてのクライアントに適用します。
   - 範囲の指定: IP アドレス、ドメイン名、およびコンピュータ名を指定します。

   注意
   IPv4 アドレスと IPv6 アドレスの両方がサポートされます。
6. [承認] または [ブロック] を選択します。
7. [保存] をクリックします。

ユーザ定義の URL のインポート

この画面では、別の Smart Protection Server からユーザ定義の URL をインポートできます。使用可能なオプションについての簡単な説明を次に示します。

- 参照: クリックして、コンピュータから .csv ファイルを選択します。
- アップロード: クリックして、選択した .csv ファイルをアップロードします。
- キャンセル: クリックして、前の画面に戻ります。

不審オブジェクトの設定

不審オブジェクトとは、送信されたサンプルで見つかった不正な (あるいは不正と思われる) IP アドレス、ドメイン、URL、SHA-1 値のことです。

Smart Protection Server は、次のソースに登録して不審オブジェクトを同期できます。

表 2-1. Smart Protection Server の不審オブジェクトのソース

ソース	不審オブジェクトの種類	説明
Deep Discovery Analyzer • 仮想アナライザ	URL	仮想アナライザは、不審ファイルを分析するためのクラウドベースの仮想環境です。サンドボックスイメージを使用してネットワーク上のエンドポイントをシミュレートすることで、ネットワークを危険にさらすことなくファイルの挙動を調べることができます。 送信されたサンプルは、管理対象製品の仮想アナライザで追跡および分析され、システムが失われるなどの危険を及ぼす可能性がある不審オブジェクトが見つかるとフラグが付けられます。
Control Manager 集約された不審オブジェクト • Control Manager のユーザ定義の不審オブジェクト • 仮想アナライザの不審オブジェクト	URL	Control Manager は、Deep Discovery Analyzer から不審オブジェクトのリストを受け取ります。 Control Manager の管理者は、仮想アナライザの不審オブジェクトのリストにないオブジェクトが不審であると判断した場合、そのオブジェクトを追加することができます。ユーザ定義の不審オブジェクトは、仮想アナライザの不審オブジェクトよりも優先度が高くなります。 Control Manager は、不審オブジェクトとそれらに対する検索処理を集約し、その情報を Smart Protection Server に配信します。

Smart Protection Server は、登録されている情報を次のように中継します。

- Web レピュテーションクエリを送信するトレンドマイクロ製品 (ウイルスバスター Corp.クライアント、InterScan、Deep Security など) に不審 URL の情報を送信する。
- Web レピュテーションクエリを送信するウイルスバスター Corp.クライアントに不審 URL に対する処理の情報を送信する。

注意

Control Manager による不審オブジェクトの管理方法については、http://docs.trendmicro.com/ja-jp/enterprise/control-manager-60-service-pack-3/whats_new_6sp3/suspicious_object_supported_products.aspx を参照してください。

手順

1. [Smart Protection] > [不審オブジェクト] の順に選択します。
2. 不審オブジェクトのソースの FQDN または IP アドレスを入力します。
3. 不審オブジェクトのソースから入手した API キーを入力します。
4. オプション: サーバ名、IP アドレス、および API キーが有効なことや、ソースに接続できることを確認するには、[接続テスト] をクリックします。
5. [登録] をクリックします。
6. 不審オブジェクトをすぐに同期するには、[不審オブジェクトを同期して有効化] を選択し、[今すぐ同期] をクリックします。

   注意

   このオプションは、Smart Protection Server がソースに接続できた場合にのみ選択できます。

7. [保存] をクリックします。

スマートフィードバックの有効化

スマートフィードバックを使用すると、コンピュータで検出された脅威に関する情報 (アクセスされた Web アドレス、ファイルに関する情報など) がトレンドマイクロに送信され、新たな脅威の迅速な識別や対処に役立てられます。お客さまから収集された情報の取り扱いについての詳細はこちらよりご確認いただけます。

手順

1. [Smart Protection] > [スマートフィードバック] の順に選択します。

   注意

   スマートフィードバックを有効にする前に、Smart Protection Server がインターネットに接続されていることを確認してください。

2. [Trend Micro スマートフィードバックを有効にする] を選択します。

3. 業種を選択します。
4. [保存] をクリックします。

アップデート

Smart Protection Server の効果は、最新のパターンファイルとコンポーネントを使用しているかどうかによって異なります。トレンドマイクロは、スマートスキャンパターンファイルを 1 時間ごとに更新しています。

ヒント

コンポーネントは、インストール後すぐにアップデートすることをお勧めします。

手動アップデートの設定

パターンファイルを手動でアップデートするには

手順

1. [アップデート] を選択します。
2. ドロップダウンメニューで、[パターンファイル] または [プログラム] をクリックします。
3. [アップデート] または [保存してアップデート] をクリックすると、アップデートをただちに適用できます。

予約アップデートの設定

予約アップデートを実行するには

手順

1. [アップデート] を選択します。
2. ドロップダウンメニューで、[パターンファイル] または [プログラム] をクリックします。
3. アップデートスケジュールを指定します。
4. [保存] をクリックします。

パターンファイルのアップデート

パターンファイルをアップデートすることで、最新情報がクエリに適用されます。使用可能なオプションについての簡単な説明を次に示します。

- 予約アップデートを有効にする: 毎時または 15 分ごとに自動アップデートが実行されるように設定します。
- アップデート: すべてのパターンファイルがただちにアップデートされます。

プログラムファイルのアップデート

製品プログラムを最新バージョンにアップデートすることで、製品の強化された機能を使用できます。使用可能なオプションについての簡単な説明を次に示します。

- OS: OS コンポーネントがアップデートされます。
- Smart Protection Server: 製品サーバプログラムファイルがアップデートされます。
- ウィジェットコンポーネント: ウィジェットがアップデートされます。
- 予約アップデートを有効にする: プログラムファイルが毎日指定した時刻に、または毎週アップデートされます。
- ダウンロードのみ: アップデートがダウンロードされ、プログラムファイルのアップデートを求めるメッセージが表示されます。
- ダウンロード後に自動的に適用する: 再実行や再起動が必要かどうかに関係なく、ダウンロード後すべてのアップデートが製品に適用されます。
- 再起動が必要なプログラムを自動的にアップデートしません: すべてのアップデートがダウンロードされ、再実行または再起動を必要としないプログラムのみがインストールされます。
- アップロード: Smart Protection Server 用のプログラムファイルをアップロードおよびアップデートします。
- 参照: プログラムパッケージの場所を参照できます。

- 保存してアップデート: ただちに設定を適用してアップデートを実行します。

プログラムファイルのアップデート方法には、予約アップデート、手動アップデート、およびコンポーネントのアップロードによる手動アップデートの 3 つの方法があります。

予約アップデートの有効化

手順

1. [アップデート] > [プログラム] の順に選択します。
2. [予約アップデートを有効にする] を選択して、アップデートスケジュールを選択します。

3. 次のいずれかのアップデート方法を選択します。
   - ダウンロードのみ: このチェックボックスをオンにすると、プログラムファイルがダウンロードされますが、インストールは実行されません。インストール可能なプログラムファイルのアップデートがある場合、Web 製品コンソールにメッセージが表示されます。
   - ダウンロード後に自動的に適用する: このチェックボックスをオンにすると、更新されたプログラムファイルがダウンロードされたときに自動的にインストールされます。

- 再起動が必要なプログラムを自動的にアップデートしません: このチェックボックスをオンにすると、アップデートで再起動が必要な場合に Web 製品コンソールにメッセージが表示されます。再起動を必要としないプログラムアップデートは自動的にインストールされます。

4. [保存] をクリックします。

手動アップデートの実行

手順

1. [アップデート] > [プログラム] の順に選択します。
2. 次のいずれかのアップデート方法を選択します。
   - ダウンロードのみ: このチェックボックスをオンにすると、プログラムファイルがダウンロードされますが、インストールは実行されません。インストール可能なプログラムファイルのアップデートがある場合、Web 製品コンソールにメッセージが表示されます。
   - ダウンロード後に自動的に適用する: このチェックボックスをオンにすると、更新されたプログラムファイルがダウンロードされたときに自動的にインストールされます。
     - 再起動が必要なプログラムを自動的にアップデートしません: このチェックボックスをオンにすると、アップデートで再起動が必要な場合に Web 製品コンソールにメッセージが表示されます。再起動を必要としないプログラムアップデートは自動的にインストールされます。
3. [保存してアップデート] をクリックします。

コンポーネントのアップロードによる手動アップデート

手順

1. [アップデート] > [プログラム] の順に選択します。

   重要

   処理を進める前に、Smart Protection Server でアップデートが実行されていないことを確認してください。プログラムやコンポーネントをアップデートする必要がある場合は、その前にコンポーネントの予約アップデートを無効にしておきます。

2. [コンポーネントのアップロード] で [参照...] をクリックして、手動プログラムアップデートに使用するプログラムファイルを指定します。

   注意

   トレンドマイクロの Web サイトからダウンロード、またはトレンドマイクロから入手したプログラムファイルを指定します。

3. ファイルを参照して、[開く] をクリックします。
4. [アップロード] をクリックします。

   注意

   プログラムやコンポーネントをアップデートするために予約検索を無効にしていた場合は、アップロードおよびアップデートの完了後に再度有効にします。

アップデート可能なプログラムファイル

この画面では、利用可能なプログラムファイルをアップデートできます。使用可能なオプションについての簡単な説明を次に示します。

- <チェックボックス>: アップデート可能なプログラムのチェックボックスをオンにします。

- アップデート: クリックして、選択したプログラムファイルをアップデートします。

アップデート元の設定

この画面では、ファイルレピュテーションおよび Web レピュテーションのアップデート元を指定できます。初期設定のアップデート元はトレンドマイクロのアップデートサーバです。使用可能なオプションについての簡単な説明を次に示します。

- トレンドマイクロのアップデートサーバ: トレンドマイクロのアップデートサーバからアップデートをダウンロードします。
- その他のアップデート元: Trend Micro Control Manager などのアップデート元を指定できます。

手順

1. [アップデート] > [アップデート元] の順に選択し、[ファイルレピュテーション] タブまたは [Web レピュテーション] タブを選択します。
2. [トレンドマイクロのアップデートサーバ] を選択するか、[その他のアップデート元] を選択して URL を入力します。
3. [保存] をクリックします。

管理タスク

管理タスクでは、SNMP サービス、通知、プロキシサーバの設定や、診断情報のダウンロードなどを実行できます。

SNMP サービス

Smart Protection Server では、製品の監視作業の柔軟性を向上するために SNMP がサポートされています。設定を指定し、[SNMP サービス] 画面で管理情報

ベース (MIB) ファイルをダウンロードします。使用可能なオプションについての簡単な説明を次に示します。

- SNMP サービスを有効にする: SNMP サービスを使用できます。
- コミュニティ名: SNMP コミュニティ名を指定します。
- IP 制限を有効にする: IP アドレスの制限が有効になります。

注意

IP 制限では、Classless Inter-Domain Routing (CIDR) はサポートされません。IP アドレスの制限を有効にすることで、SNMP サービスへの無許可のアクセスを防止できます。

- IP アドレス: システムヘルスステータスを監視するために、SNMP サービスに使用する IP アドレスを指定します。
- サブネットマスク: コンピュータのステータスを監視するために、SNMP サービスに使用する IP アドレス範囲を定義するネットマスクを指定します。
- Smart Protection Server MIB:Smart Protection Server MIB ファイルがダウンロードされます。
- 保存: 設定が保存されます。
- キャンセル: 変更が無視されます。

SNMP サービスの設定

SNMP サービスを設定することで、Smart Protection Server のステータスを SNMP 管理システムから監視できるようになります。

手順

1. [管理] > [SNMP サービス] の順に選択します。

2. [SNMP 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。
3. コミュニティ名を指定します。
4. [IP 制限を有効にする] チェックボックスをオンにすると、SNMP サービスへの無許可のアクセスを防止できます。

> **注意**
> IP 制限では、Classless Inter-Domain Routing (CIDR) はサポートされません。

5. IP アドレスを指定します。
6. サブネットマスクを指定します。
7. [保存] をクリックします。

MIB ファイルのダウンロード

Web コンソールで MIB ファイルをダウンロードして、SNMP サービスで使用します。

手順

1. [管理] > [SNMP サービス] の順に選択します。

2. [Smart Protection Server MIB] をクリックして、MIB ファイルをダウンロードします。確認を求めるメッセージが表示されます。
3. [保存] をクリックします。

   [名前を付けて保存] 画面が表示されます。
4. 保存場所を指定します。
5. [保存] をクリックします。

Smart Protection Server MIB

次の表は、Smart Protection Server MIB の説明を示しています。

オブジェクト名	オブジェクト識別子 (OID)	説明
Trend-MIB:: TBLVersion	1.3.6.1.4.1.6101.1.2.1.1	現在のスマートスキャンパターンのバージョンを返します。
Trend-MIB:: TBLLastSuccessfulUpdate	1.3.6.1.4.1.6101.1.2.1.2	スマートスキャンパターンを正常にアップデートした前回の日時を返します。
Trend-MIB:: LastUpdateError	1.3.6.1.4.1.6101.1.2.1.3	スマートスキャンパターンの前回のアップデートのステータスを返します。 • 0: 前回のパターンファイルのアップデートは成功しています。 • <エラーコード>: 前回のパターンファイルのアップデートは失敗しています。
Trend-MIB:: LastUpdateErrorMessage	1.3.6.1.4.1.6101.1.2.1.4	スマートスキャンパターンの前回のアップデートに失敗している場合に、エラーコードを返します。
Trend-MIB:: WCSVersion	1.3.6.1.4.1.6101.1.2.1.5	現在の Web ブロックパターンファイルのバージョンを返します。

オブジェクト名	オブジェクト識別子 (OID)	説明
Trend-MIB:: WCSLastSuccessfulUpdate	1.3.6.1.4.1.6101.1.2.1.6	Web ブロックパターンファイルを正常にアップデートした前回の日時を返します。
Trend-MIB:: WCSLastUpdateError	1.3.6.1.4.1.6101.1.2.1.7	Web ブロックパターンファイルの前回のアップデートのステータスを返します。 • 0: 前回のパターンファイルのアップデートは成功しています。 • <エラーコード>: 前回のパターンファイルのアップデートは失敗しています。
Trend-MIB:: WCSLastUpdateErrorMessage	1.3.6.1.4.1.6101.1.2.1.8	Web ブロックパターンファイルの前回のアップデートに失敗している場合に、エラーコードを返します。
Trend-MIB:: LastVerifyError	1.3.6.1.4.1.6101.1.2.2.2	ファイルレピュテーションクエリのステータスを返します。 • 0: ファイルレピュテーションクエリは予期されたとおりに動作しています。 • <エラーコード>: ファイルレピュテーションクエリは予期されたとおりに動作していません。
Trend-MIB:: WCSLastVerifyError	1.3.6.1.4.1.6101.1.2.2.3	Web レピュテーションクエリのステータスを返します。 • 0: Web レピュテーションクエリは予期されたとおりに動作しています。 • <エラーコード>: Web レピュテーションクエリは予期されたとおりに動作していません。
Trend-MIB:: LastVerifyErrorMessage	1.3.6.1.4.1.6101.1.2.2.4	ファイルレピュテーションクエリの最新ヘルスステータス確認が失敗している場合に、エラーメッセージを返します。
Trend-MIB:: WCSLastVerifyErrorMessage	1.3.6.1.4.1.6101.1.2.2.5	Web レピュテーションクエリの最新ヘルスステータス確認が失敗している場合に、エラーメッセージを返します。

サポートされる MIB

サポートされるその他の MIB を次の表に示します。

オブジェクト名	オブジェクト識別子 (OID)	説明
SNMP MIB-2 System	1.3.6.1.2.1.1	システムグループには、エンティティが配置されたシステムに関する情報が格納されます。このグループのオブジェクトは、障害の管理や設定の管理に役立ちます。IETF RFC 1213 を参照してください。
SNMP MIB-2 Interfaces	1.3.6.1.2.1.2	インタフェースオブジェクトグループには、ネットワークデバイスの各インタフェースに関する情報が格納されます。このグループの情報は、障害管理、設定管理、パフォーマンス管理、アカウント管理に役立ちます。IETF RFC 2863 を参照してください。

プロキシ設定

ネットワークでプロキシサーバを使用している場合は、プロキシを設定します。使用可能なオプションについての簡単な説明を次に示します。

- プロキシサーバを使用する: ネットワークでプロキシサーバを使用している場合に選択します。
- HTTP: プロキシサーバで、プロキシプロトコルに HTTP を使用している場合に選択します。
- SOCKS5: プロキシサーバで、プロキシプロトコルに SOCKS5 を使用している場合に選択します。
- サーバ名/IP アドレス: プロキシサーバ名または IP アドレスを入力します。
- ポート番号: ポート番号を入力します。
- ユーザ ID: プロキシサーバで認証が必要な場合に、プロキシサーバのユーザ ID を入力します。
- パスワード: プロキシサーバで認証が必要な場合に、プロキシサーバのパスワードを入力します。

プロキシの設定

手順

1. [管理] > [プロキシ設定] の順に選択します。

2. [プロキシサーバを使用する] チェックボックスをオンにします。
3. プロキシプロトコルに [HTTP] または [SOCKS5] を選択します。

> **注意**
>
> SOCKS4 プロキシの設定は Smart Protection Server でサポートされなくなりました。

4. サーバ名または IP アドレスを入力します。
5. ポート番号を入力します。
6. プロキシサーバで資格情報が必要な場合には、[ユーザ ID] と [パスワード] に入力します。
7. [保存] をクリックします。

サポート用システム情報

Web コンソールを使用して、トラブルシューティングやサポート用に診断情報をダウンロードします。

[開始] をクリックすると、診断情報の収集が開始されます。

サポート用システム情報のダウンロード

手順

1. [管理] > [サポート情報] の順に選択します。
2. [開始] をクリックします。

   ダウンロード状況の画面が表示されます。
3. ダウンロードされたファイルについての確認メッセージが表示されたら [保存] をクリックします。
4. 場所とファイル名を指定します。
5. [保存] をクリックします。

製品コンソールのパスワードの変更

製品コンソールのパスワードは、Smart Protection Server を許可されていない変更から保護するための基本的な手段です。環境のセキュリティを向上するため、コンソールのパスワードは定期的に変更し、簡単に思いつかないパスワードを使用してください。admin アカウントのパスワードは、コマンドラインインタフェース (CLI) で変更できます。CLI で「configure password」コマンドを実行し、パスワードを変更します。

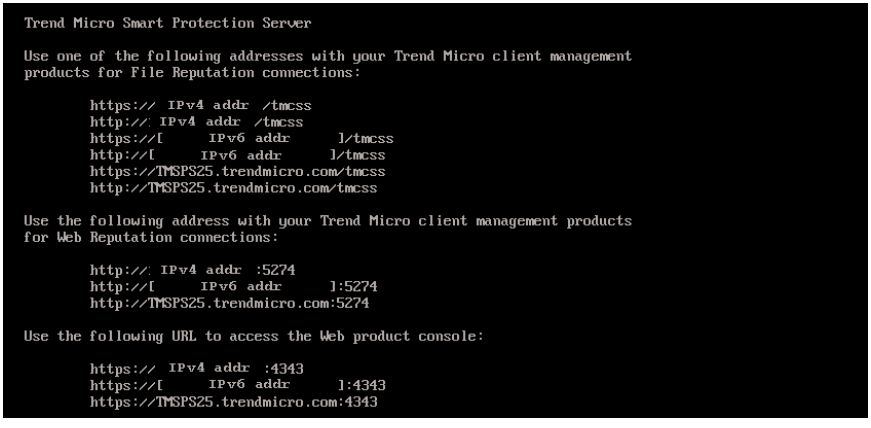
ヒント

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。

手順

1. admin アカウントで CLI コンソールにログオンします。



2. 次のコマンドを入力して管理コマンドを有効にします。

```
enable
```

3. 次のコマンドを入力します。

```
configure password admin
```

4. 新しいパスワードを入力します。
5. パスワードの確認のために再度新しいパスワードを入力します。

証明書のインポート

本バージョンの Smart Protection Server では、安全性およびセキュリティを向上させるために、管理者がサーバ証明書を再生成またはインポートすることができます。

手順

1. [管理]→[証明書] の順に選択します。

   現在の「サーバ証明書情報」が表示されます。
2. [現在の証明書を置き換える] をクリックします。
3. [参照] をクリックして、アップロードする有効な証明書を選択します。証明書は、.pem ファイルである必要があります。
4. [次へ] をクリックします。
5. 新しい証明書の詳細を確認して、[終了] をクリックします。証明書がインポートされるまで数秒間待ちます。

トレンドマイクロ製品およびサービスとの統合

Smart Protection Server は、次の表のトレンドマイクロ製品およびサービスと統合されています。統合の詳細については、対象製品のオンラインヘルプで関連するセクションを参照してください。

表 2-2. ファイルレピュテーションサービス

使用されるコンポーネント	コンポーネントのソース	統合対象製品とサポートされる最小バージョン	最初の Smart Protection Server バージョン
スマートスキャンパターンファイル **注意** スマートスキャンパターンファイルは、統合対象製品にインストールされたスマートスキャンエージェントパターンファイルと連携して動作します。	• トレンドマイクロのアップデートサーバ (初期設定) • その他のアップデート元として HTTP と HTTPS をサポート	• ウイルスバスター Corp. 10 • Core Protection Module 10.5 • Deep Security 7.5 • InterScan Messaging Security Virtual Appliance 9.1 • InterScan Web Security Virtual Appliance 6.5 Service Pack 1 • InterScan for Microsoft Exchange 10 SP1 • PortalProtect 2.1 for SharePoint 2.1 • Trend Micro Threat Mitigator 2.5 • ウイルスバスター ビジネスセキュリティ 6.0	1.0
Smart Protection サービスプロキシ (コミュニティファイルレピュテーションに使用)	なし (組み込み)	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 Service Pack 2 • Deep Discovery Analyzer 5.5 Service Pack 1 • ウイルスバスター Corp. XG	3.0 Patch 2

表 2-3. Web レピュテーションサービス

使用されるコンポーネント	コンポーネントのソース	統合対象製品とサポートされる最小バージョン	最初の Smart Protection Server バージョン
Web ブロックパターンファイル	• トレンドマイクロのアップデートサーバ (初期設定) • その他のアップデート元もサポートされています	• ウイルスバスター Corp. 10.5 • Core Protection Module 10.5 • Deep Discovery Inspector 2.6 • Deep Security 7.5 • InterScan for Microsoft Exchange 10.0 Service Pack 1 • InterScan for Lotus Domino 5.6 • PortalProtect 2.1 • Trend Micro Security (for Mac) 2.0	2.0
承認済み URL/ブロック URL	なし (リストは Smart Protection Server コンソールで直接設定します)		2.0
不審 URL	• Control Manager 6.0 SP2 • Deep Discovery Analyzer 5.0		2.6 Patch 1
不審 URL-拡張版	• Control Manager 6.0 SP3	• ウイルスバスター Corp. 11 SP1	3.0 Patch 1
Smart Protection サービスプロキシ (Web 検査サービスに使用)	なし (組み込み)	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 Service Pack 2 • Deep Discovery Analyzer 5.5 Service Pack 1	3.0 Patch 2

使用されるコンポーネント	コンポーネントのソース	統合対象製品とサポートされる最小バージョン	最初の SMART PROTECTION SERVER バージョン
Smart Protection サービスプロキシ (コミュニティドメイン/IP レピュテーションサービスに使用)	なし (組み込み)	• Deep Discovery Inspector 5.0 • Deep Discovery Analyzer 6.0 Deep Discovery Inspector 5.0、Deep Discovery Analyzer 6.0 および Deep Discovery Email Inspector 3.0 は、2017 年 11 月現在、日本においてはリリースされておりません。最新のリリース状況については、最新版ダウンロードページをご参照ください。http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp	3.3

表 2-4. モバイルアプリレピュテーションサービス

使用されるコンポーネント	コンポーネントのソース	統合対象製品とサポートされる最小バージョン	最初の SMART PROTECTION SERVER バージョン
Smart Protection サービスプロキシ	なし (組み込み)	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 Service Pack 2 • Deep Discovery Analyzer 5.5 Service Pack 1	3.0 Patch 2

表 2-5. ソフトウェア安全性評価サービス

使用されるコンポーネント	コンポーネントのソース	統合対象製品とサポートされる最小バージョン	最初の Smart Protection Server バージョン
Smart Protection サービスプロキシ	なし (組み込み)	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 Service Pack 2 • Deep Discovery Analyzer 5.5 Service Pack 1	3.0 Patch 2

表 2-6. 機械学習型検索

使用されるコンポーネント	コンポーネントのソース	統合対象製品とサポートされる最小バージョン	最初の Smart Protection Server バージョン
Smart Protection サービスプロキシ	なし (組み込み)	• ウイルスバスター Corp. XG • Deep Discovery Inspector 5.0 • Deep Discovery Email Inspector 3.0 • Deep Discovery Analyzer 6.0	3.1

注意

Smart Protection サービスプロキシは、統合対象製品からのクエリ要求を詳しい分析のために Smart Protection Network にリダイレクトします。

第 3 章

Smart Protection Server の監視

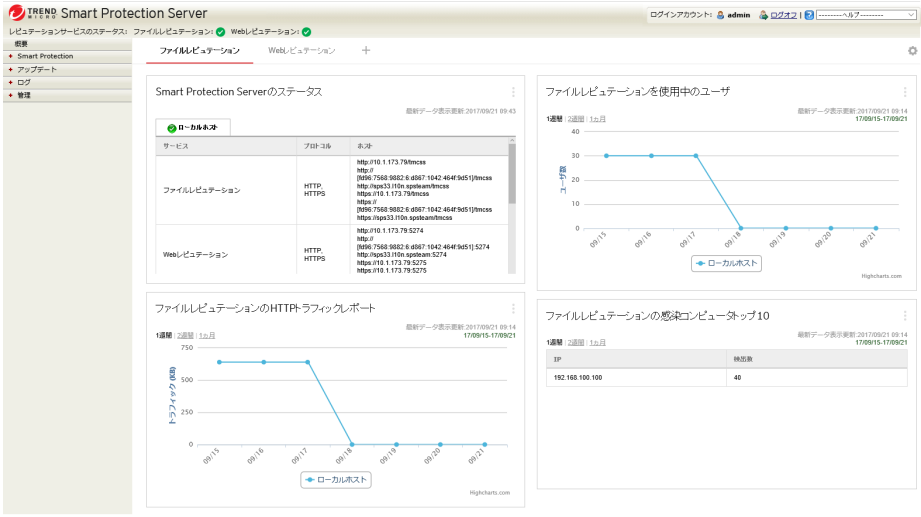
Smart Protection Server は、ログや、[概要] 画面のウィジェットを使用して監視できます。

この章の内容は次のとおりです。

[概要] 画面の使用

[概要] 画面では、Smart Protection Server コンピュータ、トラフィック、および検出に関する情報をカスタマイズして表示できます。

ファイルレピュテーションサービスおよび Web レピュテーションサービスでは、HTTP と HTTPS の両方のプロトコルがサポートされます。HTTPS では接続の安全性が高くなりますが、HTTP では使用する帯域幅が減少します。Smart Protection Server のアドレスは、コマンドラインインタフェース (CLI) コンソールのバナーに表示されます。



歯車アイコン をクリックすると、[概要] 画面の [サーバの可視性] リストにアクセスできます。

図 3-1. サーバの可視性

[サーバの可視性] リストでは、[サーバの可視性] リストにサーバを追加したり、[サーバの可視性] リストのサーバへの接続に使用するプロキシサーバを設定したりできます。サーバ情報の編集方法はすべてのウィジェットで同じです。

注意

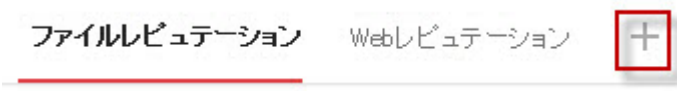
Smart Protection Server のアドレスは、エンドポイントを管理するトレンドマイクロ製品で使用されます。サーバアドレスは、Smart Protection Server コンピュータへのエンドポイントの接続設定に使用されます。

タブの操作

タブの管理作業として、タブの追加、名前の変更、レイアウトの変更、削除、自動切り替えが可能です。

手順

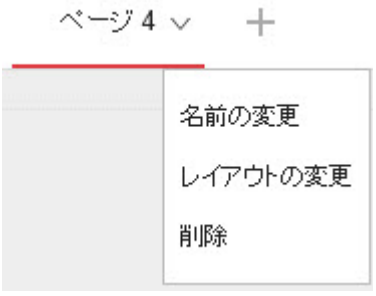
1. [概要] 画面に移動します。
2. 新しいタブを追加するには、次の手順を実行します。
   a. 追加アイコンをクリックします。



b. 新しいタブの名前を入力します。

3. タブの名前を変更するには、次の手順を実行します。

a. タブの名前にカーソルを合わせ、下矢印をクリックします。



b. [名前の変更] をクリックし、タブの新しい名前を入力します。

4. タブのウィジェットのレイアウトを変更するには、次の手順を実行します。

a. タブの名前にカーソルを合わせ、下矢印をクリックします。

b. [レイアウトの変更] をクリックします。

c. 表示される画面で新しいレイアウトを選択します。

d. [保存] をクリックします。

5. タブを削除するには、次の手順を実行します。

a. タブの名前にカーソルを合わせ、下矢印をクリックします。

b. [削除] をクリックし、確認して実行します。

6. タブスライドショーを再生するには、次の手順を実行します。

a. タブの右にある [設定] アイコンをクリックします。

b. [タブスライドショー] コントロールを有効にします。

c. タブの表示を次のタブに切り替えるまでの時間の長さを選択します。

ウィジェットの操作

ウィジェットの管理作業として、項目の追加、移動、サイズ変更、削除が可能です。

手順

1. [概要] 画面に移動します。
2. タブをクリックします。
3. ウィジェットを追加するには、次の手順を実行します。

a. タブの右にある [設定] アイコンをクリックします。

b. [ウィジェットの追加] をクリックします。

c. 追加するウィジェットを選択します。

- ウィジェットの上部にあるドロップダウンで、カテゴリを選択して項目を絞り込むことができます。
- 画面の上部にある検索テキストボックスで、特定のウィジェットを検索できます。

d. [追加] をクリックします。

4. ウィジェットを同じタブ内の別の位置に移動するには、新しい場所にドラッグアンドドロップします。

5. 複数列のタブでウィジェットのサイズを変更するには、ウィジェットの右端にカーソルを合わせ、カーソルを左右に動かします。

6. ウィジェットの名前を変更するには、次の手順を実行します。

a. 設定アイコン (>) をクリックします。

b. 新しいタイトルを入力します。

c. [保存] をクリックします。

7. ウィジェットを削除するには、削除アイコン (>) をクリックします。

使用可能なウィジェット

このリリースで使用可能なウィジェットを以下に示します。

Smart Protection Server のステータス

Smart Protection Server のステータスウィジェットは、Smart Protection Server のステータスを監視するために使用します。

注意

このウィジェットが [概要] 画面に表示されている間は、製品コンソールセッションは期限切れになりません。[コンピュータステータス] が 1 分ごとに更新され、そのたびにサーバに要求が送信されるためです。ただし、表示中のタブにこのウィジェットが含まれていない場合は、セッションの期限切れが発生します。

表 3-1. ウィジェットのデータ

データ	説明
サービス	Smart Protection Server で提供しているサービス。
プロトコル	サービスでサポートされているプロトコル。ファイルレピュテーションサービスおよび Web レピュテーションサービスでは、HTTP プロトコルと HTTPS プロトコルの両方がサポートされます。HTTPS では接続の安全性が高くなりますが、HTTP では使用する帯域幅が減少します。
ホスト	ファイルレピュテーションサービスおよび Web レピュテーションサービスのアドレス。これらのアドレスは、Smart Protection Server コンピュータをサポートするトレンドマイクロ製品で、Smart Protection Server コンピュータへの接続の設定に使用されます。

データ	説明
コンピュータステータス	[ヘルスステータス] には以下の情報が表示されます。 • ファイルレピュテーションクエリ: ファイルレピュテーションが想定どおりに動作しているかどうかが表示されます。 • Web レピュテーションクエリ: Web レピュテーションが想定どおりに動作しているかどうかが表示されます。 • アップデート: アップデートが想定どおりに動作しているかどうかが表示されます。 • 平均 CPU 負荷: カーネルによって生成されたコンピュータの負荷の過去 1 分、5 分、15 分間の平均値が表示されます。 • 空きメモリ: コンピュータの使用可能な物理メモリが表示されます。 • スワップディスク使用率: スワップディスク使用率が表示されます。 • 空き容量: コンピュータの使用可能な空きディスク容量が表示されます。

ファイルレピュテーションを使用中のユーザ

アクティブなユーザウィジェットは、Smart Protection Server に対してファイルレピュテーションクエリを実行したユーザの数を表示します。一意の各クライアントコンピュータがアクティブなユーザと見なされます。

注意

このウィジェットの情報は 2D グラフの形式で表示されます。データは 1 時間に 1 回更新されるほか、更新アイコン ( ) をクリックするといつでも更新することができます。

表 3-2. ウィジェットのデータ

データ	説明
ユーザ数	Smart Protection Server にクエリを送信したユーザの数。
日付	クエリの日付。

ファイルレピュテーションの HTTP トラフィックレポート

HTTP トラフィックレポートウィジェットは、クライアントで生成されたファイルレピュテーションクエリから Smart Protection Server に送信されたネットワークトラフィックの総量 (KB) を表示します。このウィジェットの情報は 1 時間に 1 回更新されます。また、更新アイコン ( ) をクリックするといつでもデータを更新することができます。

表 3-3. ウィジェットのデータ

データ	説明
トラフィック (KB)	クエリによって生成されたネットワークトラフィック。
日付	クエリの日付。

ファイルレピュテーションの感染コンピュータ トップ 10

このウィジェットは、Smart Protection Server がファイルレピュテーションクエリから既知のウイルスを受け取った後に感染コンピュータとして分類された上位 10 個の IP アドレスを表示します。各コンピュータの IP アドレスとそのコンピュータでの検出総数が、表形式で表示されます。データは 1 時間に 1 回更新されるほか、更新アイコン ( ) をクリックするといつでも更新することができます。

このウィジェットは、感染数が多いコンピュータをネットワーク上で上追跡するために使用します。

注意

このウィジェットで複数の Smart Protection Server を有効にした場合、選択した各 Smart Protection Server で検出総数が計算され、それらの Smart Protection Server の中から上位 10 個の感染コンピュータが表示されます。

表 3-4. ウィジェットのデータ

データ	説明
IP	コンピュータの IP アドレス。

データ	説明
検出数	このコンピュータで検出されたセキュリティ上の脅威の数。

Web レピュテーションを使用中のユーザ

アクティブなユーザウィジェットでは、Smart Protection Server に対して Web レピュテーションクエリを実行したユーザの数を表示します。一意の各クライアントコンピュータがアクティブなユーザと見なされます。

注意

このウィジェットの情報は 2D グラフの形式で表示されます。データは 5 分ごとに更新されるほか、更新アイコン ( ) をクリックするといつでも更新することができます。

表 3-5. ウィジェットのデータ

データ	説明
ユーザ数	Smart Protection Server にクエリを送信したユーザの数。
日付	クエリの日付。

Web レピュテーションの HTTP トラフィックレポート

HTTP トラフィックレポートウィジェットは、クライアントで生成された Web レピュテーションクエリから Smart Protection Server に送信されたネットワークトラフィックの総量 (KB) を表示します。このウィジェットの情報は 1 時間に 1 回更新されます。また、更新アイコン ( ) をクリックするといつでもデータを更新することができます。

表 3-6. ウィジェットのデータ

データ	説明
トラフィック (KB)	クエリによって生成されたネットワークトラフィック。
日付	クエリの日付。

Web レピュテーションのブロックされたコンピュータ トップ 10

このウィジェットは、Smart Protection Server が Web レピュテーションクエリの URL を受け取った後にブロックされたコンピュータとして分類された上位 10 個の IP アドレスを表示します。各コンピュータの IP アドレスとそのコンピュータでブロックされた URL の総数が、表形式で表示されます。データは 1 日に 1 回更新されるほか、更新アイコン ( ) をクリックするといつでも更新することができます。

このウィジェットは、ブロックされたサイトへのアクセスが多いコンピュータをネットワーク上で追跡するために使用します。

注意

このウィジェットで複数の Smart Protection Server を有効にした場合、選択した各 Smart Protection Server で検出総数が計算され、それらの Smart Protection Server の中から上位 10 個のブロックされたコンピュータが表示されます。

表 3-7. ウィジェットのデータ

データ	説明
IP	コンピュータの IP アドレス。
検出数	このコンピュータでブロックされた URL の数。

ログ

ログは、Smart Protection Server のステータスを監視するために使用します。ログの情報を表示するには、クエリを実行します。

ブロックされた URL

[ブロックされた URL] 画面には、不正な結果を返す Web レピュテーションクエリの情報が表示されます。

この画面で使用可能なオプションは次のとおりです。

- キーワード: URL の検索時に使用するキーワードを指定します。
- 日付範囲: 日付の範囲を選択します。
- ソース: 該当するログを表示するソースを 1 つ以上選択します。
  - ユーザ定義のブロック URL: Smart Protection Server のユーザ定義のブロック URL と一致する、ブロックされている URL を表示します。
  - Web ブロックパターンファイル: Web ブロックパターンファイルのエントリと一致する、ブロックされている URL を表示します。
  - 以下に一致する C&C URL: 次のソースのエントリと一致する、ブロックされている URL を表示します。
    - Control Manager のユーザ定義の不審オブジェクト: Control Manager のユーザ定義の不審オブジェクトのサブセット
    - 仮想アナライザ: Deep Discovery Advisor、Deep Discovery Analyzer、Control Manager など、仮想アナライザ対応製品の不審オブジェクトのサブセット
    - Web ブロックパターンファイルのグローバルインテリジェンス: Trend Micro Smart Protection Network では、世界中から情報を収集してグローバルインテリジェンスリストを作成し、C&C コールバックアドレスのリスクレベルをテストおよび評価しています。Web レピュテーションサービスでは、そのグローバルインテリジェンスリストを不正 Web サイトのレピュテーションスコアと連携させることで、高度な脅威に対する強化されたセキュリティを提供します。Web レピュテーションのセキュリティレベルに応じて、割り当てられたリスクレベルを基に不正な Web サイトや C&C サーバに対する処理が決まります。

この画面に表示される情報は次のとおりです。

- 日時: ブロックされた URL イベントの日時。
- URL: ブロックされた URL。
- ログを表示: ブロックされた URL のソース情報。
- クライアント GUID: ブロックされた URL にアクセスを試行したコンピュータの GUID。

- サーバ GUID: Smart Protection Server をサポートするトレンドマイクロ製品の GUID。
- クライアント IP: ブロックされた URL にアクセスを試行したコンピュータの IP アドレス。
- コンピュータ名: ブロックされた URL にアクセスを試行したコンピュータ名。
- ドメイン: エンドポイントのドメイン名。

アップデートログ

[アップデートログ] 画面には、パターンファイルまたはプログラムファイルのアップデートに関する情報が表示されます。使用可能なオプションについての簡単な説明を次に示します。

- 日付範囲: アップデートが実行された日付の範囲を選択します。
- 種類: 表示するアップデートの種類を選択します。

ログ詳細:

- 日時: サーバがアップデートされた日時です。
- コンポーネント名: アップデートされたコンポーネントです。
- 結果: 成功または失敗のどちらかになります。
- 説明: アップデートイベントの説明です。
- アップデート方法: 従来型スキャンまたはスマートスキャンのどちらかになります。

レピュテーションサービスログ

[レピュテーションサービスログ] 画面には、Web レピュテーションとファイルレピュテーションのサービスステータス情報が表示されます。使用可能なオプションについての簡単な説明を次に示します。

- サービス: サービスを指定します。
- 結果: 結果の種類を指定します。
- 日付範囲: 日付の範囲を選択します。

ログ詳細:

- 日時: Web レピュテーションやファイルレピュテーションのサービスステータスを確認した日時です。
- サービス: Web レピュテーションまたはファイルレピュテーションのどちらかになります。
- 結果: 成功または失敗のどちらかになります。
- 説明: Web レピュテーションまたはファイルレピュテーションのサービスステータスの説明です。

ログ管理

不要なログを削除するにはログ管理を実行します。使用可能なオプションについての簡単な説明を次に示します。

- パターンファイルのアップデートログ: パターンファイルのアップデートログエントリが削除されます。
- プログラムのアップデートログ: アップデートログエントリが削除されます。
- ブロックされた URL: URL クエリエントリが削除されます。
- レピュテーションサービスログ: レピュテーションサービスイベントエントリが削除されます。
- すべてのログを削除: すべてのログが削除されます。
- 次の日数経過したログを削除: 古いログが削除されます。
- 予約削除を有効にする: 自動削除が予約されます。

手順

1. [ログ] > [ログ管理] の順に選択します。
2. 削除するログの種類を選択します。
3. すべてのログを削除するか、指定した日数よりも古いログを削除するかを指定します。
4. 削除を予約するか、[今すぐ削除] をクリックします。
5. [保存] をクリックします。

通知

Smart Protection Server では、サービスまたはアップデートのステータスに変更があった場合に、メールメッセージや SNMP (Simple Network Management Protocol) トラップ通知を送信するように設定できます。

メール通知

サービスまたはアップデートのステータスに変更があった場合に、メールメッセージを使用して管理者に通知するようメール通知を設定します。使用可能なオプションについての簡単な説明を次に示します。

- SMTP サーバ: SMTP サーバの IP アドレスを入力します。
- ポート番号: SMTP サーバのポート番号を入力します。
- 送信者: メール通知の送信者フィールドのメールアドレスを入力します。
- サービス: ファイルレピュテーション、Web レピュテーション、およびパターンファイルのアップデートにおけるステータスの変更について通知が送信されます。
- 宛先: イベントに対して通知を送信するメールアドレスを入力します (複数入力可)。

- 件名: イベントに対する新しい件名を入力するか、初期設定の件名テキストを使用します。
- メッセージ: イベントに対する新しいメッセージを入力するか、初期設定のメッセージテキストを使用します。
- ファイルレピュテーションのステータスの変更: ステータスの変更について通知を送信したり、この通知の受信者を指定したりできます。
- Web レピュテーションのステータスの変更: ステータスの変更について通知を送信したり、この通知の受信者を指定したりできます。
- パターンファイルアップデートのステータスの変更: ステータスの変更について通知を送信したり、この通知の受信者を指定したりできます。
- アップデート: 通知に関係するすべてのプログラムに対して通知を送信できます。
- プログラムアップデートのダウンロードの失敗: プログラムアップデートのダウンロードに失敗した場合に通知を送信したり、この通知の受信者を指定したりできます。
- プログラムアップデート利用可能: 確認が必要なプログラムアップデートが存在する場合に通知を送信したり、この通知の受信者を指定したりできます。
- プログラムアップデートのステータス: プログラムが更新されたことについて通知を送信したり、この通知の受信者を指定したりできます。
- プログラムアップデートによる Smart Protection Server または関連サービスの再起動: プログラムのアップデートプロセスが Smart Protection Server または関連サービスを再起動した場合に通知を送信したり、この通知の受信者を指定したりできます。
- 初期設定のメッセージ: [件名] と [メッセージ] フィールドが初期設定のテキストに戻ります。

メール通知の設定

手順

1. [管理] > [通知] の順に選択し、[メール] タブを選択します。

   メール通知のタブが表示されます。

2. ステータス変更のメール通知をすべてのサービスについて受け取る場合は、[サービス] チェックボックスをオンにします。特定のサービスについて受け取る場合は、該当するチェックボックスをオンにします。

   - ファイルレピュテーションのステータスの変更: ステータスの変更について通知を送信したり、受信者、件名、およびメッセージを指定したりできます。
   - Web レピュテーションのステータスの変更: ステータスの変更について通知を送信したり、受信者、件名、およびメッセージを指定したりできます。

- パターンファイルアップデートのステータスの変更: ステータスの変更について通知を送信したり、受信者、件名、およびメッセージを指定したりできます。

3. [アップデート] チェックボックスをオンにするか、次のオプションを選択します。

   - プログラムアップデートのダウンロードの失敗: このイベントについて通知を送信したり、受信者、件名、およびメッセージを指定したりできます。
   - プログラムアップデート利用可能: このイベントについて通知を送信したり、受信者、件名、およびメッセージを指定したりできます。
   - プログラムアップデートのステータス: このイベントについて通知を送信したり、受信者、件名、およびメッセージを指定したりできます。
   - プログラムアップデートによる Smart Protection Server または関連サービスの再起動: このイベントについて通知を送信したり、受信者、件名、およびメッセージを指定したりできます。

4. [SMTP サーバ] フィールドに SMTP サーバの IP アドレスを入力します。
5. SMTP ポート番号を入力します。
6. [宛先] フィールドにメールアドレスを入力します。すべてのメール通知で、メールメッセージの [宛先] フィールドにこのアドレスが表示されます。
7. [保存] をクリックします。

SNMP トラップ通知

サービスのステータスに変更があった場合に、SNMP (Simple Network Management Protocol) トラップを使用して管理者に通知するよう SNMP 通知を設定します。使用可能なオプションについての簡単な説明を次に示します。

- サーバ IP アドレス: SNMP トラップ受信者の IP アドレスを指定します。

- コミュニティ名: SNMP コミュニティ名を指定します。
- サービス: ファイルレピュテーション、Web レピュテーション、およびパターンファイルのアップデートにおけるステータスの変更について SNMP 通知が送信されます。
- メッセージ: イベントに対する新しいメッセージを入力するか、初期設定のメッセージテキストを使用します。
- ファイルレピュテーションのステータスの変更: ステータスの変更について通知が送信されます。
- Web レピュテーションのステータスの変更: ステータスの変更について通知が送信されます。
- パターンファイルアップデートのステータスの変更: ステータスの変更について通知が送信されます。
- 初期設定のメッセージ: [メッセージ] フィールドが初期設定のテキストに戻ります。

SNMP トラップ通知の設定

サービスのステータスに変更があった場合に、SNMP (Simple Network Management Protocol) トラップを使用して管理者に通知するよう SNMP 通知を設定します。

手順

1. [管理] > [通知] の順に選択し、[SNMP] タブを選択します。

SNMP トラップ通知のタブが表示されます。

2. [サービス] チェックボックスをオンにするか、次のチェックボックスをオンにします。

   - ファイルレピュテーションのステータスの変更: ステータスの変更について通知を送信したり、受信者、件名、およびメッセージを指定したりできます。
   - Web レピュテーションのステータスの変更: ステータスの変更について通知を送信したり、受信者、件名、およびメッセージを指定したりできます。
   - パターンファイルアップデートのステータスの変更: ステータスの変更について通知を送信したり、受信者、件名、およびメッセージを指定したりできます。

3. SNMP トラップサーバの IP アドレスを入力します。

4. SNMP コミュニティ名を入力します。

5. [保存] をクリックします。

第 4 章

Trend Micro Control Manager との統合

Smart Protection Server と Control Manager の統合

この章の内容は次のとおりです。

Trend Micro Control Manager

Trend Micro Control Manager は、トレンドマイクロ製品およびサービスを、ゲートウェイ、メールサーバ、ファイルサーバ、および企業のデスクトップレベルで一元管理するためのコンソールです。Control Manager の Web ベースの管理コンソールを使用すると、ネットワーク上にある管理対象製品およびサービスを一元的に監視できます。

システム管理者は Control Manager を使用して、感染、セキュリティ違反、ウイルス侵入ポイントなどの活動を監視し、レポートできます。ネットワーク全体にコンポーネントをダウンロードして配置できるため、一貫した最新の保護を実現できます。Control Manager では、手動または予約アップデートを実行できます。また設定や管理は、個別の製品ごとまたはグループ単位で柔軟に行うことができます。

サポートされている Control Manager のバージョン

この Smart Protection Server バージョンは、次の Control Manager のバージョンをサポートしています。

機能	CONTROL MANAGER のバージョン		
	7.0(今後リリースされる日本語版での予定)	6.0 SERVICE PACK 3	6.0 SERVICE PACK 1 以前
不審オブジェクトおよび処理の同期	はい	はい	いいえ
代替アップデート元としての Control Manager の使用	はい	はい	はい

注意

Smart Protection Server は、IPv4 シングルスタックまたはデュアルスタックネットワークの Control Manager にのみ接続します。

この Smart Protection Server リリースにおける Control Manager の統合

この Smart Protection Server リリースには、次の機能が含まれています。

表 4-1. Control Manager との統合

機能	説明
不審オブジェクトおよび処理の同期	1. Control Manager は、不審オブジェクトおよび検索処理を集約し、この情報を Smart Protection Server に中継します。 2. Smart Protection Server は、不審 URL と処理をウイルスバスター Corp.エージェントに中継します。Web レピュテーションクエリを送信する製品 (Portal Protect や Deep Security など) の場合、Smart Protection Server は不審 URL のみを中継します。 **注意** Control Manager による不審オブジェクトの管理方法については、http://downloadcenter.trendmicro.com/index.php?regs=jp&clk=latest&clkval=4312&lang_loc=13 を参照してください。
代替アップデート元としての Control Manager	Smart Protection Server がインターネットに接続していない場合、Control Manager をアップデート元として使用できます。
シングルサインオン (SSO) によるログイン	Control Manager で、Control Manager コンソールからのシングルサインオン(SSO) によるログインが可能になりました。 Control Manager 7.0 は、2017 年 11 月現在、日本においてはリリースされておりません。最新のリリース状況については、最新版ダウンロードページをご参照ください。http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

第 5 章

サポート情報

この章の内容は次のとおりです。

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。

法人カスタマーサービス & サポートの利用

法人カスタマーサービス & サポートでは、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。

手順

1. https://app.trendmicro.co.jp/ecs/default.aspx にアクセスします。
2. キーワードを入力します。
3. 製品またはサービスを該当のドロップダウンリストから選択し、検索します。
4. 解決策が見つからない場合は、次のページで最適なお問い合わせ先を確認し、問い合わせします。 http://esupport.trendmicro.com/ja-jp/contact/ent.aspx

---

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。

セキュリティニュース

トレンドマイクロ「セキュリティニュース」

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

https://www.trendmicro.com/ja_jp/security-intelligence/breaking-news.html

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

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

トレンドマイクロへのウイルス解析依頼

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

ファイルを送信いただく前に、トレンドマイクロの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。

http://esupport.trendmicro.com/ja-jp/contact/ent.aspx

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専門のスタッフが解析し、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。

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

コマンドラインインタフェース (CLI) のコマンド

ここでは、製品内で監視、デバッグ、トラブルシューティング、設定などのタスクに使用できる CLI のコマンドについて説明します。仮想マシンから admin アカウントで CLI にログオンします。CLI コマンドによって、管理者は、設定タスクを実行したり、デバッグやトラブルシューティング機能を実行したりできます。その他に、CLI インタフェースでは、重要なリソースや機能を監視できるコマンドも提供されています。CLI インタフェースにアクセスするには、管理者のアカウントとパスワードが必要です。

コマンド	構文	説明
`certificate regen self-sign`	`certificate regen self-sign <Issued_to> <Issued_by> <Validity>`	自己署名証明書の再生成 <Issued_to>: 証明書の受信者の一般名 (CN) <Issued_by>: 証明書の発行元の一般名 (CN) <Validity>: 証明書の有効期間 (日数)
`certificate update CA`	`certificate update CA`	最新の CA バンドルのダウンロード
`configure date`	`configure date <date> <time>`	日付の設定と CMOS への保存 `date` DATE_FIELD [DATE_FIELD] `time` TIME_FIELD [TIME_FIELD]

コマンド	構文	説明
`configure dns ipv4`	`configure dns ipv4 <dns1> [dns2]`	IPv4 DNS の設定 `dns1` IPv4_ADDR プライマリ DNS サーバ `dns2` IPv4_ADDR セカンダリ DNS サーバ []
`configure dns ipv6`	`configure dns ipv6 <dns1> [dns2]`	IPv6 DNS の設定 `dns1` IPv6_ADDR プライマリ DNS サーバ `dns2` IPv6_ADDR セカンダリ DNS サーバ []
`configure hostname`	`configure hostname <hostname>`	ホスト名の設定 `hostname` HOSTNAME ホスト名または FQDN
`configure ipv4 dhcp`	`configure ipv4 dhcp [vlan]`	初期設定 Ethernet インタフェースで DHCP を使用するための設定 `vlan` VLAN_ID VLan ID [1-4094]、初期設定では VLAN なし: [0]
`configure ipv4 static`	`configure ipv4 static <ip> <mask> <gateway> [vlan]`	初期設定 Ethernet インタフェースで静的 IPv4 アドレスを使用するための設定 `vlan` VLAN_ID VLan ID [1-4094]、初期設定では VLAN なし: [0]
`configure ipv6 auto`	`configure ipv6 auto [vlan]`	初期設定 Ethernet インタフェースで自動ネイバー検出 IPv6 アドレスを使用するための設定 `vlan` VLAN_ID VLan ID [1-4094]、初期設定では VLAN なし: [0]
`configure ipv6 dhcp`	`configure ipv6 dhcp [vlan]`	初期設定 Ethernet インタフェースで動的な IP 設定 (DHCPv6) を使用するための設定 `vlan` VLAN_ID VLan ID [1-4094]、初期設定では VLAN なし: [0]
`configure ipv6 static`	`configure ipv6 static <v6ip> <v6mask> <v6gate> [vlan]`	初期設定 Ethernet インタフェースで静的 IPv6 アドレスを使用するための設定 `vlan` VLAN_ID VLan ID [1-4094]、初期設定では VLAN なし: [0]

コマンド	構文	説明
configure locale de_DE	configure locale de_DE	システムロケールをドイツ語に設定
configure locale en_US	configure locale en_US	システムロケールを英語に設定
configure locale es_ES	configure locale es_ES	システムロケールをスペイン語に設定
configure locale fr_FR	configure locale fr_FR	システムロケールをフランス語に設定
configure locale it_IT	configure locale it_IT	システムロケールをイタリア語に設定
configure locale ja_JP	configure locale ja_JP	システムロケールを日本語に設定
configure locale ko_KR	configure locale ko_KR	システムロケールを韓国語に設定
configure locale ru_RU	configure locale ru_RU	システムロケールをロシア語に設定
configure locale zh_CN	configure locale zh_CN	システムロケールを中国語 (簡体字) に設定
configure locale zh_TW	configure locale zh_TW	システムロケールを中国語 (繁体字) に設定
configure ntp	configure ntp <ip or FQDN>	NTP サーバの設定
configure port	configure port <frs_http_port> <frs_https_port> <wrs_http_port> <wrs_https_port>	ファイルレピュテーションサービスおよび Web レピュテーションサービスのサービスポートの変更

コマンド	構文	説明
`configure password`	`configure password <user>`	アカウントパスワードの設定 `user` USER パスワードの変更対象となるユーザの名前。対象となるユーザには、「admin」、「root」、または Trend Micro Smart Protection Server の Administrator グループ内の任意のユーザを指定できます。
`configure proxy-service`	`configure proxy-service <wis_url> <cfr_url> <grid_url> <mars_url>`	トレンドマイクロのグローバル保護サービス URL の変更 <wis_url>: Web 検査サービス URL <cfr_url>: コミュニティファイルレピュテーション URL <grid_url>: GRID (Goodware Resource and Information Database) URL <mars_url>: モバイルアプリレピュテーションサービス URL
`configure service`	`configure service interface <ifname>`	初期設定のサーバ設定の指定
`configure timezone Africa Cairo`	`configure timezone Africa Cairo`	タイムゾーンをアフリカのカイロ地域に設定
`configure timezone Africa Harare`	`configure timezone Africa Harare`	タイムゾーンをアフリカのハラレ地域に設定
`configure timezone Africa Nairobi`	`configure timezone Africa Nairobi`	タイムゾーンをアフリカのナイロビ地域に設定
`configure timezone America Anchorage`	`configure timezone America Anchorage`	タイムゾーンを米国アンカレッジ地域に設定

コマンド	構文	説明
configure timezone America Bogota	configure timezone America Bogota	タイムゾーンを南米のボゴタ地域に設定
configure timezone America Buenos_Aires	configure timezone America Buenos_Aires	タイムゾーンを南米のブエノスアイレス地域に設定
configure timezone America Caracas	configure timezone America Caracas	タイムゾーンを南米のカラカス地域に設定
configure timezone America Chicago	configure timezone America Chicago	タイムゾーンを米国シカゴ地域に設定
configure timezone America Chihuahua	configure timezone America Chihuahua	タイムゾーンを中央アメリカのチワワ地域に設定
configure timezone America Denver	configure timezone America Denver	タイムゾーンを米国デンバー地域に設定
configure timezone America Godthab	configure timezone America Godthab	タイムゾーンを米国ゴットホープ地域に設定
configure timezone America Lima	configure timezone America Lima	タイムゾーンを南米のリマ地域に設定
configure timezone America Los_Angeles	configure timezone America Los_Angeles	タイムゾーンを米国ロサンゼルス地域に設定

コマンド	構文	説明
configure timezone America Mexico_City	configure timezone America Mexico_City	タイムゾーンを中央アメリカのメキシコシティー地域に設定
configure timezone America New_York	configure timezone America New_York	タイムゾーンを米国ニューヨーク地域に設定
configure timezone America Noronha	configure timezone America Noronha	タイムゾーンを米国ノローニャ地域に設定
configure timezone America Phoenix	configure timezone America Phoenix	タイムゾーンを米国フェニックス地域に設定
configure timezone America Santiago	configure timezone America Santiago	タイムゾーンを米国サンディエゴ地域に設定
configure timezone America St_Johns	configure timezone America St_Johns	タイムゾーンを米国セントジョンズ地域に設定
configure timezone America Tegucigalpa	configure timezone America Tegucigalpa	タイムゾーンを米国テグシガルパ地域に設定
configure timezone Asia Almaty	configure timezone Asia Almaty	タイムゾーンをアジアのアルマティ地域に設定
configure timezone Asia Baghdad	configure timezone Asia Baghdad	タイムゾーンを中近東のバグダッド地域に設定

コマンド	構文	説明
configure timezone Asia Baku	configure timezone Asia Baku	タイムゾーンを中近東のバクー地域に設定
configure timezone Asia Bangkok	configure timezone Asia Bangkok	タイムゾーンをアジアのバンコク地域に設定
configure timezone Asia Calcutta	configure timezone Asia Calcutta	タイムゾーンをアジアのコルカタ地域に設定
configure timezone Asia Colombo	configure timezone Asia Colombo	タイムゾーンをアジアのコロンボ地域に設定
configure timezone Asia Dhaka	configure timezone Asia Dhaka	タイムゾーンをアジアのダッカ地域に設定
configure timezone Asia Hong_Kong	configure timezone Asia Hong_Kong	タイムゾーンをアジアの香港地域に設定
configure timezone Asia Irkutsk	configure timezone Asia Irkutsk	タイムゾーンをアジアのイルクーツク地域に設定
configure timezone Asia Jerusalem	configure timezone Asia Jerusalem	タイムゾーンを中近東のエルサレム地域に設定
configure timezone Asia Kabul	configure timezone Asia Kabul	タイムゾーンを中近東のカブール地域に設定
configure timezone Asia Karachi	configure timezone Asia Karachi	タイムゾーンをアジアのカラチ地域に設定
configure timezone Asia Katmandu	configure timezone Asia Katmandu	タイムゾーンをアジアのカトマンズ地域に設定

コマンド	構文	説明
configure timezone Asia Krasnoyarsk	configure timezone Asia Krasnoyarsk	タイムゾーンをアジアのクラスノヤルスク地域に設定
configure timezone Asia Kuala_Lumpur	configure timezone Asia Kuala_Lumpur	タイムゾーンをアジアのクアラルンプール地域に設定
configure timezone Asia Kuwait	configure timezone Asia Kuwait	タイムゾーンを中近東のクウェート地域に設定
configure timezone Asia Magadan	configure timezone Asia Magadan	タイムゾーンをアジアのマガダン地域に設定
configure timezone Asia Manila	configure timezone Asia Manila	タイムゾーンをアジアのマニラ地域に設定
configure timezone Asia Muscat	configure timezone Asia Muscat	タイムゾーンを中近東のマスカット地域に設定
configure timezone Asia Rangoon	configure timezone Asia Rangoon	タイムゾーンをアジアのラングーン地域に設定
configure timezone Asia Seoul	configure timezone Asia Seoul	タイムゾーンをアジアのソウル地域に設定
configure timezone Asia Shanghai	configure timezone Asia Shanghai	タイムゾーンをアジアの上海地域に設定
configure timezone Asia Singapore	configure timezone Asia Singapore	タイムゾーンをアジアのシンガポール地域に設定
configure timezone Asia Taipei	configure timezone Asia Taipei	タイムゾーンをアジアの台北地域に設定

コマンド	構文	説明
configure timezone Asia Tehran	configure timezone Asia Tehran	タイムゾーンを中近東のテヘラン地域に設定
configure timezone Asia Tokyo	configure timezone Asia Tokyo	タイムゾーンをアジアの東京地域に設定
configure timezone Asia Yakutsk	configure timezone Asia Yakutsk	タイムゾーンをアジアのヤクーツク地域に設定
configure timezone Atlantic Azores	configure timezone Atlantic Azores	タイムゾーンを大西洋アゾレス地域に設定
configure timezone Australia Adelaide	configure timezone Australia Adelaide	タイムゾーンをオーストラリアのアデレード地域に設定
configure timezone Australia Brisbane	configure timezone Australia Brisbane	タイムゾーンをオーストラリアのブリズベン地域に設定
configure timezone Australia Darwin	configure timezone Australia Darwin	タイムゾーンをオーストラリアのダーウィン地域に設定
configure timezone Australia Hobart	configure timezone Australia Hobart	タイムゾーンをオーストラリアのホーバート地域に設定
configure timezone Australia Melbourne	configure timezone Australia Melbourne	タイムゾーンをオーストラリアのメルボルン地域に設定

コマンド	構文	説明
configure timezone Australia Perth	configure timezone Australia Perth	タイムゾーンをオーストラリアのパース地域に設定
configure timezone Europe Amsterdam	configure timezone Europe Amsterdam	タイムゾーンをヨーロッパのアムステルダム地域に設定
configure timezone Europe Athens	configure timezone Europe Athens	タイムゾーンをヨーロッパのアテネ地域に設定
configure timezone Europe Belgrade	configure timezone Europe Belgrade	タイムゾーンをヨーロッパのベオグラード地域に設定
configure timezone Europe Berlin	configure timezone Europe Berlin	タイムゾーンをヨーロッパのベルリン地域に設定
configure timezone Europe Brussels	configure timezone Europe Brussels	タイムゾーンをヨーロッパのブリュッセル地域に設定
configure timezone Europe Bucharest	configure timezone Europe Bucharest	タイムゾーンをヨーロッパのブカレスト地域に設定
configure timezone Europe Dublin	configure timezone Europe Dublin	タイムゾーンをヨーロッパのダブリン地域に設定
configure timezone Europe Moscow	configure timezone Europe Moscow	タイムゾーンをヨーロッパのモスクワ地域に設定

コマンド	構文	説明
configure timezone Europe Paris	configure timezone Europe Paris	タイムゾーンをヨーロッパのパリ地域に設定
configure timezone Pacific Auckland	configure timezone Pacific Auckland	タイムゾーンを太平洋オークランド地域に設定
configure timezone Pacific Fiji	configure timezone Pacific Fiji	タイムゾーンを太平洋フィジー地域に設定
configure timezone Pacific Guam	configure timezone Pacific Guam	タイムゾーンを太平洋グアム地域に設定
configure timezone Pacific Honolulu	configure timezone Pacific Honolulu	タイムゾーンを太平洋ホノルル地域に設定
configure timezone Pacific Kwajalein	configure timezone Pacific Kwajalein	タイムゾーンを太平洋クウェジェリン環礁地域に設定
configure timezone Pacific Midway	configure timezone Pacific Midway	タイムゾーンを太平洋ミッドウェー地域に設定
configure timezone US Alaska	configure timezone US Alaska	タイムゾーンを米国アラスカ地域に設定
configure timezone US Arizona	configure timezone US Arizona	タイムゾーンを米国アリゾナ地域に設定
configure timezone US Central	configure timezone US Central	タイムゾーンを米国中部地域に設定

コマンド	構文	説明
`configure timezone US East-Indiana`	`configure timezone US East-Indiana`	タイムゾーンを米国東インディアナ地域に設定
`configure timezone US Eastern`	`configure timezone US Eastern`	タイムゾーンを米国東部地域に設定
`configure timezone US Hawaii`	`configure timezone US Hawaii`	タイムゾーンを米国ハワイ地域に設定
`configure timezone US Mountain`	`configure timezone US Mountain`	タイムゾーンを米国山岳地域に設定
`configure timezone US Pacific`	`configure timezone US Pacific`	タイムゾーンを米国太平洋岸地域に設定
`disable adhoc-query`	`disable adhoc-query`	Web アクセスログの無効化
`disable ssh`	`disable ssh`	sshd デーモンの無効化
`enable`	`enable`	管理者コマンドの有効化
`enable adhoc-query`	`enable adhoc-query`	Web アクセスログの有効化
`enable ssh`	`enable ssh`	sshd デーモンの有効化
`exit`	`exit`	セッションの終了
`help`	`help`	CLI 構文の概要の表示
`history`	`history [limit]`	現在のセッションのコマンドライン履歴の表示 `[limit]` は表示する CLI コマンドの数を指定します。例: `limit` に「5」を指定すると、5 つの CLI コマンドが表示されます。

コマンド	構文	説明
reboot	reboot [time]	このコンピュータの再起動 (指定時間の経過後かただちに実行) time UNIT このコンピュータを再起動するまでの待ち時間 (分単位) [0]
show date	show date	現在の日時の表示
show hostname	show hostname	ネットワークホスト名の表示
show interfaces	show interfaces	ネットワークインタフェース情報の表示
show ipv4 address	show ipv4 address	ネットワーク IPv4 アドレスの表示
show ipv4 dns	show ipv4 dns	ネットワーク IPv4 DNS サーバの表示
show ipv4 gateway	show ipv4 gateway	ネットワーク IPv4 ゲートウェイの表示
show ipv4 route	show ipv4 route	ネットワーク IPv4 ルーティングテーブルの表示
show ipv4 type	show ipv4 type	ネットワーク IPv4 設定タイプの表示 (dhcp/static)
show ipv6 address	show ipv6 address	ネットワーク IPv6 アドレスの表示
show ipv6 dns	show ipv6 dns	ネットワーク IPv6 DNS サーバの表示
show ipv6 gateway	show ipv6 gateway	ネットワーク IPv6 ゲートウェイの表示
show ipv6 route	show ipv6 route	ネットワーク IPv6 ルーティングテーブルの表示
show ipv6 type	show ipv6 type	ネットワーク IPv6 設定タイプの表示 (auto/dhcp/static)
show timezone	show timezone	ネットワークタイムゾーンの表示
show uptime	show uptime	現在のシステム稼動時間の表示

コマンド	構文	説明
`show url management`	`show url management`	Web コンソール URL の表示
`show url FileReputationService`	`show url FileReputationService`	ファイルレピュテーションサービスのエンドポイント接続アドレスの表示
`show url WebReputationService`	`show url WebReputationService`	Web レピュテーションサービスのエンドポイント接続アドレスの表示
`shutdown`	`shutdown [time]`	このコンピュータのシャットダウン (指定時間の経過後かただちに実行) `time` UNIT このコンピュータをシャットダウンするまでの待ち時間 (分単位) [0]

索引