1.3 TXOne StellarProtect (Legacy Mode) 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。

P/N: APEM139597_JP2303

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および TXOne Netwoks 社に送信します。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。

TXOne StellarProtect (Legacy Mode) 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

https://www.txone.com/privacy-policy

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。TXOne StellarProtect (Legacy Mode) 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

このインストールガイドでは、TXOne StellarProtect (Legacy Mode) の概要を説明し、さらに管理者がインストールおよび管理するための手順を説明します。

この章の内容は次のとおりです。

ドキュメントについて

本製品には、次のドキュメントが付属しています。

表 1.　TXOne StellarProtect (Legacy Mode) のドキュメント

ドキュメント	説明
インストールガイド	製品の概要、インストール計画、インストール、設定の説明
管理者ガイド	製品の概要、設定、および製品環境を管理するために必要な詳細情報の説明
Readme ファイル	既知の制限事項に関する説明

マニュアルは、弊社の「最新版ダウンロード」サイトから入手することも可能です。

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

対象読者

TXOne StellarProtect (Legacy Mode) のドキュメントは、StellarProtect (Legacy Mode) の管理やエージェントをインストールする担当者を対象としています。これらのユーザがネットワークとサーバ管理に関する高度な知識を備えていることを前提としています。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 2.　ドキュメントの表記規則

表記	説明
 注意	設定上の注意
 ヒント	推奨事項
 重要	避けるべき操作や設定についての注意
 警告!	使用上の重要事項

第 1 章

本製品の概要

TXOne StellarProtect (Legacy Mode) は、システムを特定用途化 (ロックダウン) することにより、不正プログラムの侵入や実行を防止します。また、使いやすいユーザインタフェースや製品連携機能を有しているため、迅速な導入と高い運用性を実現します。

この章の内容は次のとおりです。

TXOne StellarProtect (Legacy Mode) について

TXOne StellarProtect (Legacy Mode) は、産業用制御システム (ICS)、POS (Point of Sale) 端末、キオスク端末、ATM 機器のような特定用途のコンピュータを不正なソフトウェアや不正使用から保護します。本製品は使用するリソースの量が少なく、パフォーマンスへの影響やダウンタイムを最小限に抑えながら、特定用途のコンピュータを保護します。

新機能

TXOne StellarProtect (Legacy Mode) 1.3 には、次の新機能および機能強化が含まれています。

表 1-1. TXOne StellarProtect (Legacy Mode) 1.3 の新機能

機能	説明
イベント処理の強化	許可リストとポリシー配信処理が強化され、システム操作の効率性が向上します。
エージェント/サーバ間の通信の強化	エージェント/サーバ間の通信が強化され、コマンドラインインタフェースを使用して接続を確認したり、集中管理機能を設定したりできるようになります。

エージェントの機能と特徴

StellarProtect (Legacy Mode) には、次の機能と特徴があります。

アプリケーション (プログラム、DLL ファイル、ドライバ、およびスクリプト) の制御

StellarProtect (Legacy Mode) で、アプリケーションの制御時にアプリケーションの許可リスト (アプリケーションの信頼リスト) に登録されていないプログラム、DLL ファイル、ドライバ、およびスクリプトの実行を許可しません。これにより、不正なソフトウェアの実行をブロックし、プログラムの予期しない使用を防ぐことで、生産性とシステムの整合性が向上します。制御対象とするスクリプトファイルはユーザが個別に指定することができます。

また、書き込み制御によりファイル/フォルダ/レジストリの変更や削除を防止します。

脆弱性攻撃対策

新しい脅威や未知の脅威だけでなく、Downad や Stuxnet などの既知の標的型攻撃の脅威は ICS やキオスクのコンピュータにおける重大なリスクです。最新の OS アップデートが行われていないシステムは、標的型攻撃に対して特に脆弱です。

StellarProtect (Legacy Mode) は、不正侵入対策によってエージェントへの脅威の蔓延を防止し、実行防止対策によってエージェントでの脅威を防止します。

許可リストの管理

ソフトウェアのインストールまたはアップデートが必要な場合は、次のいずれかの方法を使用することで、エージェントに加えた変更を許可リストに自動的に追加できます。これらの機能では、ロック解除の操作を実施する必要はありません。

- メンテナンスモード
- 許可リスト自動更新
- 事前指定による許可リスト自動更新リスト
- コマンドラインインタフェース (CLI):
  - 信頼するハッシュ
  - 信頼する証明書

スモールフットプリント

大容量のパターンファイルを絶えずアップデートしなければならない他のエンドポイントセキュリティソリューションと比較すると、アプリケーションの制御で使用するメモリやディスク容量は少なく、パターンファイルなどをダウンロードする必要もありません。

権限設定

管理者アカウントと制限付きユーザアカウントの 2 種類が用意されており、制限付きユーザアカウントが利用できる機能を制限することが可能です。

インタフェース

CLI (コマンドラインインタフェース) だけでなく、操作性や視認性の良い GUI (グラフィカルインタフェース) を提供します。

セルフプロテクション

セルフプロテクション機能を使用すると、TXOne StellarProtect (Legacy Mode) が正常に機能するために必要なプロセスおよびその他のリソースを保護できます。この機能は、アプリケーションや実際のユーザが TXOne StellarProtect (Legacy Mode) を無効化しようとする試みをブロックします。

セルフプロテクション機能は、以下のサービスを停止しようとするすべての試みをブロックします。

- Trend Micro 不正変更防止サービス (`TMBMSRV.exe`)
- Trend Micro パーソナルファイアウォール (`TmPfw.exe`)
- TXOne StellarProtect (Legacy Mode) サービス (`WkSrv.exe`)

システム要件

システム要件については、次の Web サイトを参照してください。

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

エージェントがサポートする OS

システム要件については、次の Web サイトを参照してください。

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

エージェント利用時の概要

TXOne StellarProtect (Legacy Mode) は信頼リストベースのソリューションです。コンピュータをロックダウンして、許可リストに登録されていないプログラムが実行されないようにします。StellarProtect (Legacy Mode) は、グラフィカルユーザインタフェース (GUI) を使用したエージェントのメイン画面か、コマンドラインを使用して設定および管理できます。システムのアップデートは、メンテナンスモード、信頼するハッシュ、信頼するデジタル証明書、事前指定による許可リスト自動更新リスト、または許可リスト自動更新を使用して、エージェントでアプリケーション制御を解除せずに適用できます。

一般的な使用例は次のとおりです。

1. 許可リストを設定し、エージェントでアプリケーション制御を有効にして、未登録のアプリケーションの起動をブロックします。
2. メンテナンスモード、信頼するハッシュ、信頼するデジタル証明書、事前指定による許可リスト自動更新リスト、または許可リスト自動更新を使用して、ソフトウェアをアップデートまたはインストールします。
3. 後でメンテナンスするために、制限付きユーザアカウントを設定して有効にします。

   許可リストに登録されていないプログラムをユーザが実行しようとした場合、TXOne StellarProtect (Legacy Mode) はそのプログラムの実行をブロックしますが、画面上にメッセージを表示することはありません。ただし、プログラムを実行した元のプログラムによって以下のようなメッセージが表示される場合があります。

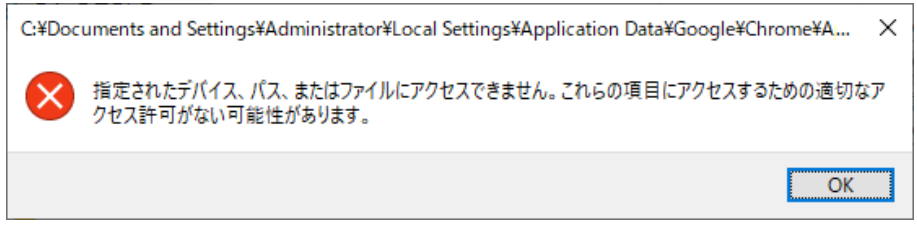


図 1-1. TXOne StellarProtect (Legacy Mode) ブロックメッセージ

第 2 章

ローカルエージェントのインストール

この章では、ローカルの TXOne StellarProtect (Legacy Mode) エージェントのインストールとセットアップの手順について説明します。

この章の内容は次のとおりです。

ローカルインストールの概要

手順

1. コンピュータが TXOne StellarProtect (Legacy Mode) のシステム要件を満たしていることを確認します。

   詳細については、11 ページの「システム要件」を参照してください。

2. 任意のインストール方法で、TXOne StellarProtect (Legacy Mode) をインストールします。

   TXOne StellarProtect (Legacy Mode) は、Windows インストーラ、またはコマンドラインからインストーラを実行してインストールできます。

表 2-1. StellarProtect (Legacy Mode) のローカルインストールの方法

インストール方法	メリット
Windows インストーラ	Windows インストーラは、初回または単一のインストール向けに簡易化されたインストールウィザードを提供します。 詳細については、16 ページの「Windows インストーラを使用したインストール」を参照してください。
コマンドライン	コマンドラインからインストールを実行する方法は、サイレントインストールや、大規模に展開するためのバッチファイル作成に適しています。 詳細については、26 ページの「コマンドラインを使用したインストール」を参照してください。

注意

1. Windows インストーラ、コマンドラインインタフェースのどちらでも、`setup.ini` ファイルを変更することで TXOne StellarProtect (Legacy Mode) エージェントの設定をカスタマイズできます。
2. StellarOne の管理サーバを介して StellarProtect (Legacy Mode) エージェントを特定グループに登録するには、StellarOne の管理サーバから Group.ini ファイルをダウンロードした後、StellarProtect (Legacy Mode) エージェントのインストーラパッケージフォルダに Group.ini ファイルを追加する必要があります。

詳細については、29 ページの「インストールパラメータをカスタマイズする」を参照してください。

3. インストールしたエージェントを設定します。
   a. TXOne StellarProtect (Legacy Mode) のメイン画面を開き、許可リストを設定します。

      TXOne StellarProtect (Legacy Mode) によるエージェントの保護を開始するには、最初に、システムの正常な実行に必要な既存のアプリケーションおよびファイルを、エージェントの許可リストに追加する必要があります。

      詳細については、23 ページの「許可リストの設定」を参照してください。

   b. TXOne StellarProtect (Legacy Mode) の設定を変更します。

   c. (オプション) アップデートされた設定を複数のエージェントに配信します。

      複数の TXOne StellarProtect (Legacy Mode) エージェントに設定を配信するには、エージェント設定ファイルを使用します。

Windows インストーラを使用したインストール

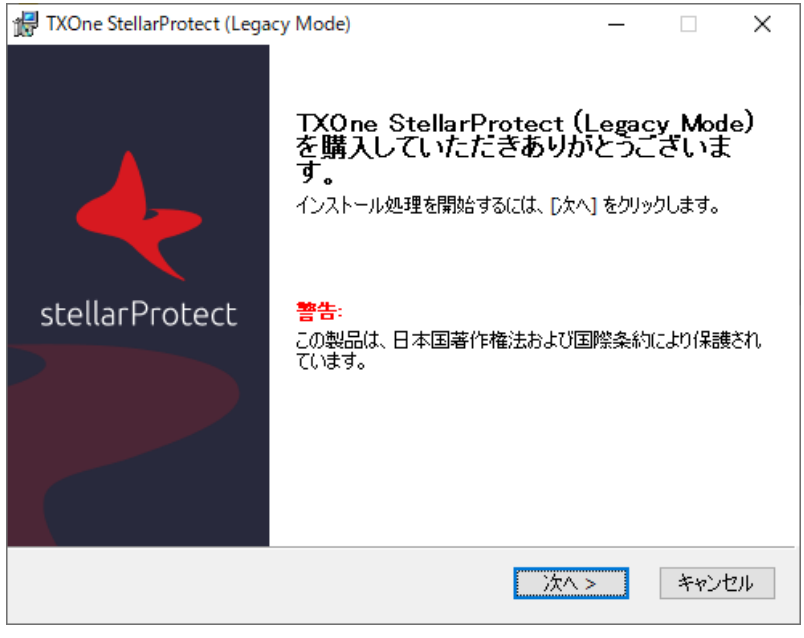
TXOne StellarProtect (Legacy Mode) をインストールするには、管理者権限のあるアカウントでログインする必要があります。

手順

1. `SL_Install.exe` をダブルクリックします。

   Windows の [ユーザーアカウント制御] の警告が表示される場合は、[はい] をクリックします。

2. インストールウィザードが表示されたら、[次へ] をクリックします。



注意

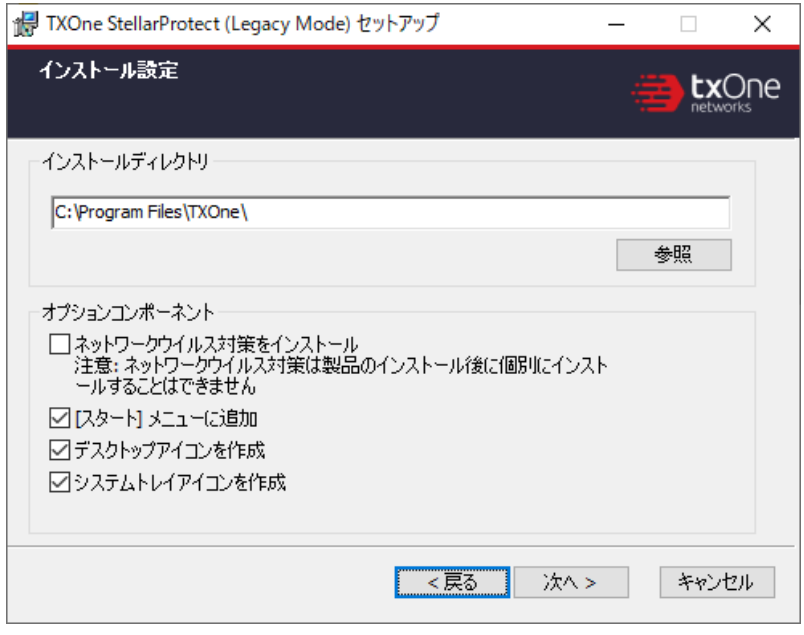
コンピュータ上に別のバージョンの StellarProtect (Legacy Mode) が存在する場合、インストーラはそれを削除してから最新バージョンをインストールします。

3. 使用許諾契約書を読み、[使用許諾契約書に同意します] を選択して [次へ] をクリックします。

4. インストールオプションを必要に応じて変更して、[次へ] をクリックします。

重要

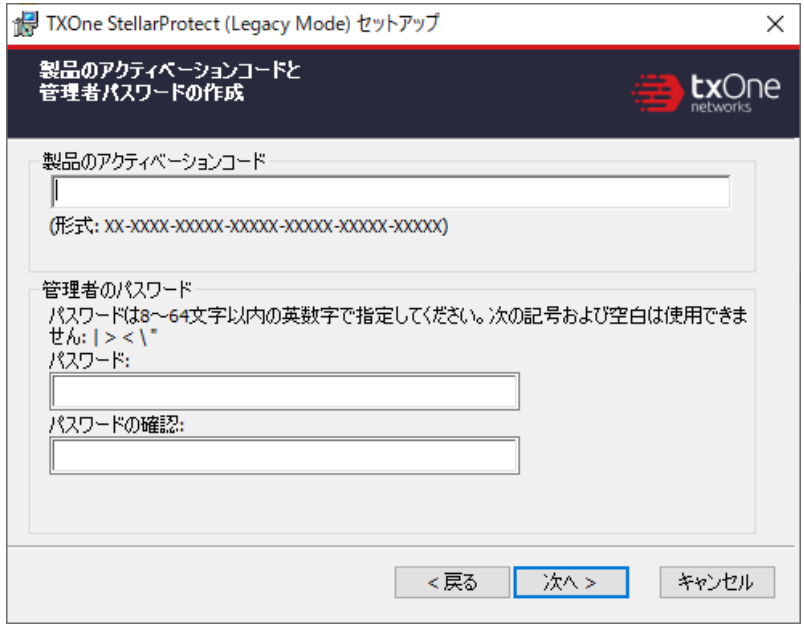
ネットワークウイルス対策をインストールできるのは初回のプログラムインストール時のみですが、必要に応じて後から無効にすることもできます。詳細については、管理者ガイドの「脆弱性攻撃対策の設定」を参照してください。



5. TXOne StellarProtect (Legacy Mode) のアクティベーションコードと管理者のパスワードを入力します。

注意

パスワードは 8～64 文字の英数字で指定してください。|><\"の記号および空白は使用できません。StellarProtect (Legacy Mode) 管理者のパスワードは、Windows 管理者のパスワードとは別に設定されます。

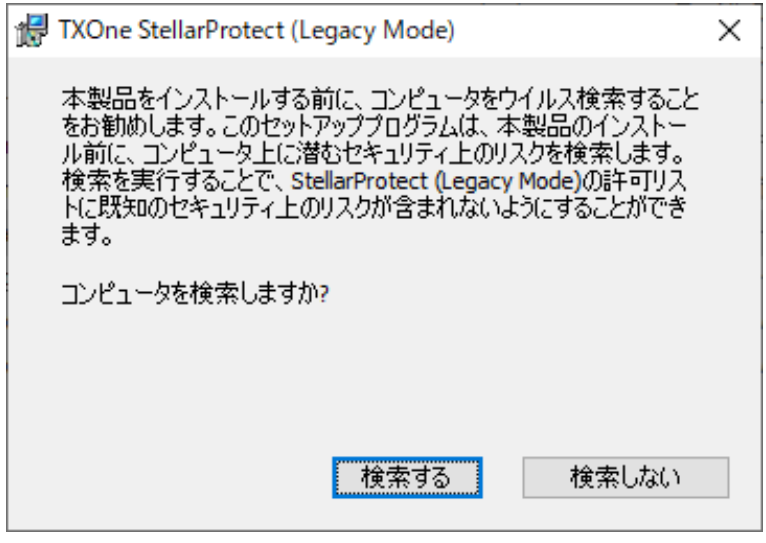


警告!

StellarProtect (Legacy Mode) 管理者のパスワードは安全に保管し、忘れないようにしてください。StellarProtect (Legacy Mode) 管理者のパスワードを忘れた場合は、トレンドマイクロのテクニカルサポートにお問い合わせください。

6. [次へ] をクリックします。

   インストールを続行する前に、コンピュータで事前に脅威を検索するかどうかを確認するメッセージが表示されます。



7. (オプション) インストールを続行する前にコンピュータで脅威の事前検索を実行します。この検索は実行することをお勧めします。

   - コンピュータで脅威を検索するには、[検索する] をクリックします。

     a. [コンピュータの事前検索] 画面が表示されます。

     b. 検索設定をカスタマイズするには、[検索設定の編集] をクリックします。

     c. [検索開始] をクリックします。

        コンピュータの事前検索でセキュリティリスクが検出された場合は、インストールをキャンセルすることをお勧めします。コンピュータの脅威を削除してから、再度実行してください。重要なプログラムが脅威として検出された場合は、コンピュータが安全であることと、インストール済みのプログラムのバージョンに脅威が含まれていないことを確認します。検出結果が誤検出であることが明らかな場合のみ、検出された脅威を無視します。

注意

Setup.ini ファイルに PRESCANCLEANUP および FORCE_PRESCAN オプションを設定している場合、検索プロセスは停止できません。

詳細については、52 ページの「Prescan セクション」を参照してください。

ヒント

エージェントから脅威を検出して削除するには、手動検索を実行します。詳細については、管理者ガイドで「手動検索のコマンド」を参照してください。

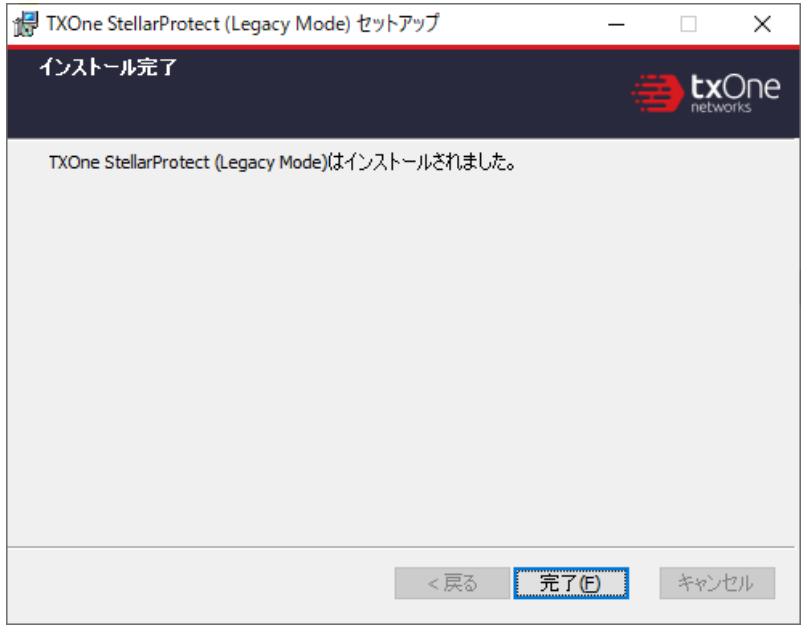
- 検索を省略するには、[検索しない] をクリックします。

注意

Setup.ini ファイルに PRESCANCLEANUP および FORCE_PRESCAN オプションを設定している場合、[検索しない] ボタンと [閉じる] ボタンは使用できません。

詳細については、52 ページの「Prescan セクション」を参照してください。

8. [インストール完了] 画面が表示されたら、[完了] をクリックします。



注意

Address Space Layout Randomization (ASLR) がサポートされていない、またはサポートが制限されている Windows XP や Windows Server 2003 などの以前の OS 対して、オプションでメモリのランダム化を有効にします。詳細については、管理者ガイドの「脆弱性攻撃対策の設定」を参照してください。

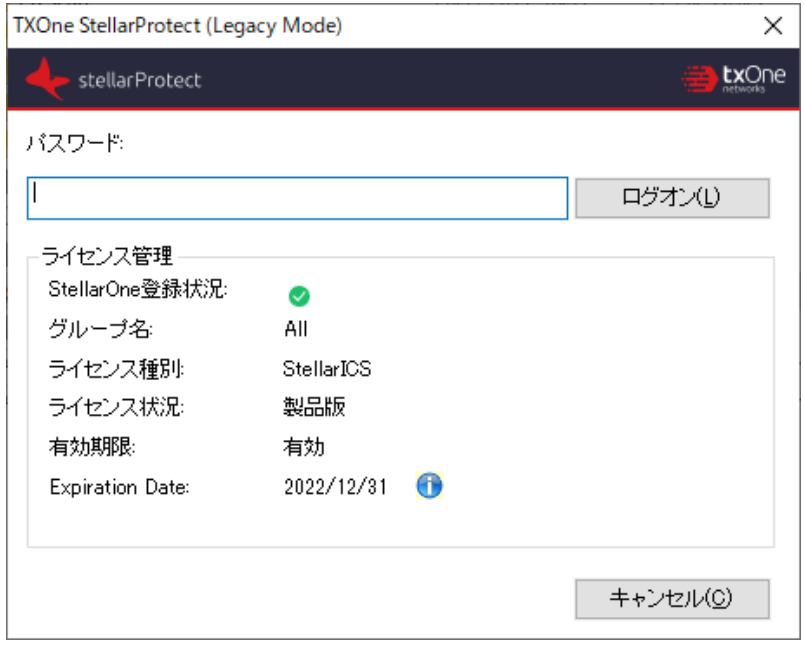
許可リストの設定

TXOne StellarProtect (Legacy Mode) でエージェントの保護を開始するには、最初に、エージェントをチェックしてシステムの正常な実行に必要なアプリケーションとファイルを確認する必要があります。

手順

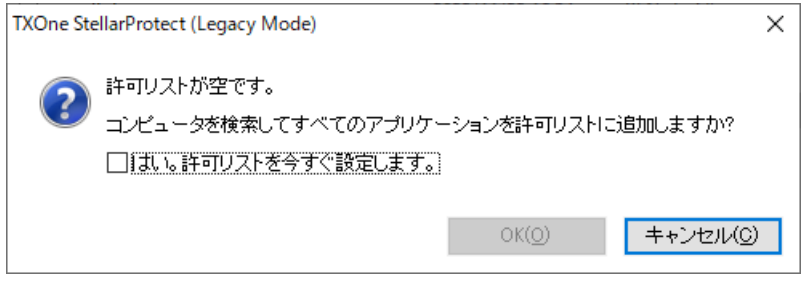
1. StellarProtect (Legacy Mode) のメイン画面を開きます。

   StellarProtect (Legacy Mode) のログイン画面が表示されます。



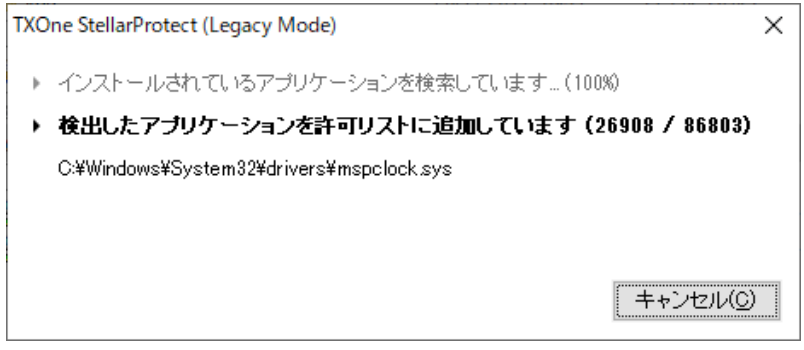
2. パスワードを入力して [ログオン] をクリックします。

   許可リストを今すぐ設定するかどうかを確認するメッセージが表示されます。

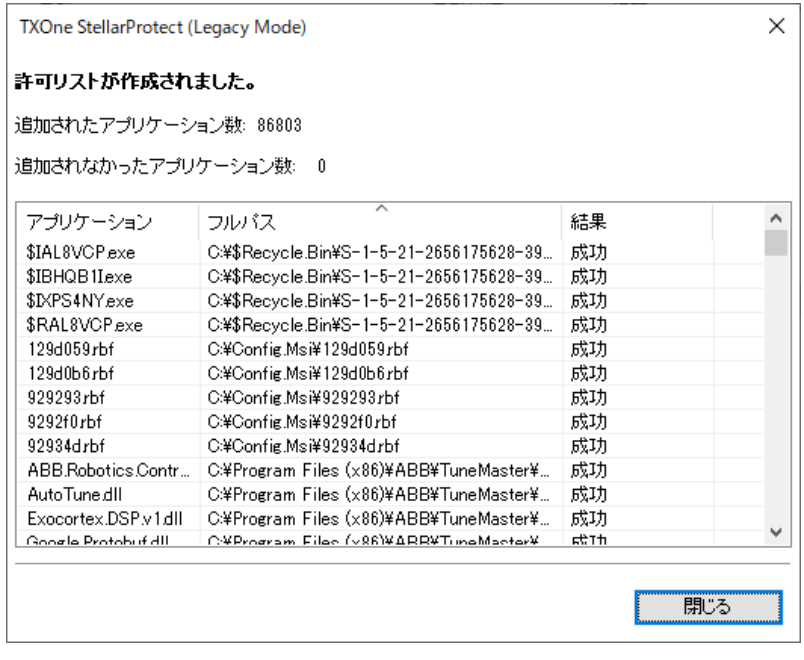


3. 通知ウィンドウで、[はい。許可リストを今すぐ設定します。] を選択して [OK] をクリックします。

   エージェントが検索され、すべてのアプリケーションが許可リストに追加されます。



許可リストの設定結果が表示されます。



注意

TXOne StellarProtect (Legacy Mode) のアプリケーション制御が有効な場合は、許可リストに含まれるアプリケーションのみを実行できます。

4. [閉じる] をクリックします。

コマンドラインを使用したインストール

管理者は、サイレントインストールおよび大規模な展開を考慮して、コマンドラインから、またはバッチファイルを使用して StellarProtect (Legacy Mode) をインストールできます。

大規模な展開の場合、カスタマイズされたインストールでは設定ファイルと許可リストが必要となることがあるため、最初に試験的にエージェントに StellarProtect (Legacy Mode) をインストールすることを推奨します。許可リストと設定ファイルの詳細については、「TXOne StellarProtect (Legacy Mode) 管理者ガイド」を参照してください。

警告!

- StellarProtect (Legacy Mode) 管理者のパスワードは慎重に保管してください。StellarProtect (Legacy Mode) 管理者のパスワードを忘れた場合は、トレンドマイクロのテクニカルサポートにお問い合わせください。
- Address Space Layout Randomization (ASLR) がサポートされていない、またはサポートが制限されている Windows XP や Windows Server 2003 などの以前の OS に対して、必ずメモリのランダム化を有効にしてください。詳細については、管理者ガイドの「脆弱性攻撃対策の設定」を参照してください。

重要

ネットワークウイルス対策をインストールできるのは初回のプログラムインストール時のみですが、必要に応じて後から無効にすることもできます。詳細については、管理者ガイドの「脆弱性攻撃対策の設定」を参照してください。

注意

パスワードは 8〜64 文字の英数字で指定してください。|><\"の記号および空白は使用できません。StellarProtect (Legacy Mode) 管理者のパスワードは、Windows 管理者のパスワードとは別に設定されます。

インストーラのコマンドラインインタフェースのパラメータ

次の表は、SL_Install.exe で使用可能なコマンド一覧を示しています。

表 2-2. StellarProtect (Legacy Mode) インストーラのコマンドラインオプション

パラメータ	値	説明
-q		サイレントモードでインストールします **注意** インストールの実行中、C:\windows\temp フォルダにある次のログファイルを表示して、事前検索プロセスや最初の許可されたプロセスのステータスを確認することができます。 • 事前検索プロセス: YYYYMMDDHHMMSS_wk_PreScanProgress.log • 最初の許可されたプロセス: YYYYMMDDHHMMSS_wk_InitListProgress.log
-p	<administrator_password>	管理者パスワードを指定します
-d	<path>	インストールパスを指定します
-ac	<activation_code>	アクティベーションコードを指定します
-nd		デスクトップショートカットを作成しません

パラメータ	値	説明
-fw		ネットワークウイルス対策を有効にします
-ns		[スタート] メニューにショートカットを追加しません
-ni		タスクトレイアイコンを非表示にします
-cp	<path>	StellarProtect (Legacy Mode) 設定ファイルを指定します **注意** 設定ファイルは StellarProtect (Legacy Mode) のインストール後にエクスポートできます。
-lp	<path>	許可リストを指定します **注意** 許可リストは、StellarProtect (Legacy Mode) をインストールして許可リストを作成した後にエクスポートできます。
-qp	<path>	カスタム処理が「隔離」モードに設定されている場合に隔離ファイルのフォルダパスを指定します
-nps		事前検索を実行しないようにします
-ips		事前検索によって脅威が検出されてもインストールを中止しません

コマンドラインインストールの例は、次のようになります。

```
SL_Install.exe -q -ac XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX -p
P@ssW0Rd -nd
```

重要

インストールを続行するには、管理者のパスワードとアクティベーションコードを入力する必要があります。

インストールパラメータをカスタマイズする

注意

インストーラは指定された引数を次の順序で適用します。

- 暗号化された `setup.bin`
- コマンドラインインタフェース (CLI)
- `setup.ini`

`setup.bin` が存在する場合、インストーラは `setup.bin` の設定を優先して適用し、CLI や `setup.ini` ファイルの設定を無視します。

Setup.ini ファイルを使用して初期設定のインストールパラメータを変更するには、次の手順に従います。

手順

1. インストールフォルダで Setup.ini ファイルを見つけます。
2. 必要に応じてインストールパラメータをカスタマイズします。

   インストールパラメータと設定可能な値の詳細については、30 ページの「インストールのカスタマイズ」を参照してください。
3. 重要な設定への無許可でのアクセスを防ぐため、必要に応じて、Setup.ini ファイルを暗号化します。
   a. インストールフォルダから、Setup.ini ファイルと WKSupportTool.exe ファイルをデスクトップにコピーします。
   b. コマンドプロンプトウィンドウを管理者として実行します。
   c. デスクトップに移動し、「`WKSupportTool.exe encryptsetupini Setup.ini Setup.bin`」と入力して Setup.ini ファイルを暗号化し、暗号化したファイルに「Setup.bin」という名前を付けます。
   d. Setup.bin ファイルをインストールフォルダに保存し、Setup.ini ファイルを削除します。

インストールのカスタマイズ

注意

インストーラは指定された引数を次の順序で適用します。

- 暗号化された `setup.bin`
- コマンドラインインタフェース (CLI)
- `setup.ini`

`setup.bin` が存在する場合、インストーラは `setup.bin` の設定を優先して適用し、CLI や `setup.ini` ファイルの設定を無視します。

初期設定のインストールパラメータを変更するには、`SL_Install.exe` と同じフォルダに `setup.ini` という名前のテキストファイルを編集します。次の表は、`setup.ini` (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

注意

コマンドラインで指定した引数はセットアップファイルより優先されます。セットアップファイルは初期設定値より優先されます。たとえば、`SL_Install.exe` にスイッチ `-nd` が追加され、`setup.ini` に `NO_DESKTOP=0` が含まれる場合は、スイッチが優先され、StellarProtect (Legacy Mode) のデスクトップショートカットは作成されません。

Property セクション

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-3. Setup.ini ファイルの [Property] セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
ACTIVATION_CODE	アクティベーションコード	<activation_code>	<空白>	なし
NO_DESKTOP	デスクトップにショートカットを作成します	• 0:ショートカットを作成します • 1:ショートカットを作成しません	0	なし
NO_STARTMENU	[スタート] メニューにショートカットを作成します	• 0:ショートカットを作成します • 1:ショートカットを作成しません	0	なし
NO_SYSTRAY	システムトレイアイコンと Windows 通知を表示します	• 0:システムトレイにアイコンを作成します • 1:システムトレイにアイコンを作成しません	0	なし
NO_NSC	ネットワークウイルス対策のファイアウォールをインストールします	• 0:ファイアウォールを作成します • 1:ファイアウォールを作成しません	1	なし
CONFIG_PATH	設定ファイルのパス	• <path>	<空白>	なし
LIST_PATH	インポートする許可リストのパスです	• <path>	<空白>	なし

KEY	説明	使用可能な値	初期設定値	暗号化
APPLICATION FOLDER	エージェントプログラムのインストールパスです	• <path>	<空白>	なし
PASSWORD	**SLCmd.exe** と StellarProtect (Legacy Mode) のメイン画面で使用するパスワード	• <password>	<空白>	なし
CUSTOM_ACTION	ブロックしたイベントに対するカスタム処理です	• 0:無視 • 1:隔離 • 2:サーバに確認	0	なし
QUARANTINE_FOLDER_PATH	エージェントプログラムの隔離パスです	• <path>	<空白>	なし
INTEGRITY_MONITOR	変更監視を有効にします	• 0:無効 • 1:有効	0	なし
PREDEFINED_TRUSTED_UPDATER	事前指定による許可リスト自動更新を有効にします	• 0:無効 • 1:有効	0	なし
WINDOWS_UPDATE_SUPPORT	Windows Update サポートを有効にします	• 0:無効 • 1:有効	0	なし
PRESCAN	StellarProtect (Legacy Mode) をインストールする前に対象コンピュータを事前検索します	• 0:コンピュータを事前検索しません • 1:コンピュータを事前検索します	1	なし
MAX_EVENT_DB_SIZE	データベースファイルの最大サイズ (MB)	正の整数	1024	なし

KEY	説明	使用可能な値	初期設定値	暗号化
WEL_SIZE	Windows イベントログのサイズ (KB)	正の整数 **注意** インストールしたエージェントの初期設定値です。 StellarProtect (Legacy Mode) をバージョンアップしても、以前のインストールで設定されたユーザ指定の WEL_SIZE 値は変更されません。	10240	なし
WEL_RETENTION	イベントログのサイズが [Windows イベントログ] の最大値に達したときの [Windows イベントログ] のオプションです	Windows XP 以前のプラットフォームの場合: • 0:必要に応じてイベントを上書きします • 1〜365:指定した日数 (1〜365 日) よりも古いイベントを上書きします • -1:イベントを上書きしません (ログは手動で消去します)	0	なし

KEY	説明	使用可能な値	初期設定値	暗号化
		Windows Vista 以降のプラットフォームの場合: • 0:必要に応じてイベントを上書きします (最も古いイベントから) • 1:ログがいっぱいになったらアーカイブし、イベントを上書きしません • -1:イベントを上書きしません (ログは手動で消去します)		
WEL_IN_SIZE	変更監視イベントの Windows イベントログのサイズ (KB)	正の整数	10240	なし
WEL_IN_RETENTION	変更監視イベントのイベントログのサイズが [Windows イベントログ] の最大値に達したときの [Windows イベントログ] のオプションです	Windows XP 以前のプラットフォームの場合: • 0:必要に応じてイベントを上書きします • 1〜365:指定した日数 (1〜365 日) よりも古いイベントを上書きします • -1:イベントを上書きしません (ログは手動で消去します)	0	なし

KEY	説明	使用可能な値	初期設定値	暗号化
		Windows Vista 以降のプラットフォームの場合: • 0:必要に応じてイベントを上書きします (最も古いイベントから) • 1:ログがいっぱいになったらアーカイブし、イベントを上書きしません • -1:イベントを上書きしません (ログは手動で消去します)		
USR_DEBUGLOG_ENABLE	ユーザセッションのデバッグログを有効にします	• 0:ログに記録しません • 1:ログに記録します	0	なし
USR_DEBUGLOGLEVEL	ユーザセッションに許可されたデバッグログエントリの数です	256	256	なし
SRV_DEBUGLOG_ENABLE	サービスセッションのデバッグログを有効にします	• 0:ログに記録しません • 1:ログに記録します	0	なし
SRV_DEBUGLOGLEVEL	サービスセッションに許可されたデバッグログエントリの数です	256	256	なし

KEY	説明	使用可能な値	初期設定値	暗号化
SILENT_INSTALL	サイレントモードでインストールを実行します	• 0:サイレントモードを使用しません • 1:サイレントモードを使用します	0	なし
	重要 サイレントモードを使用するには、ACTIVATION_CODE および PASSWORD のキーと値も指定する必要があります。例: [PROPERTY] ACTIVATION_CODE=XX-XXXXX-XXXXX-XXXXX-XXXXX PASSWORD=P@ssW0Rd SILENT_INSTALL=1			
STORAGE_DEVICE_BLOCKING	管理下のエージェントへの CD/DVD ドライブ、フロッピーディスクドライブや USB デバイスなどのストレージデバイスによるアクセスをブロックします	• 0:ストレージデバイスのアクセスを許可します • 1:ストレージデバイスのアクセスをブロックします	0	なし

KEY	説明	使用可能な値	初期設定値	暗号化
INIT_LIST	インストール時に許可リストを初期化します	• 0:インストール時に許可リストを初期化しません • 1:インストール時に許可リストを初期化します	0	なし
	注意 LIST_PATH は INIT_LIST より優先されます。 例: [PROPERTY] LIST_PATH=liststore.dbINIT_LIST=1 この場合、liststore.db はインポートされますが、INIT_LIST は無視されます。			
INIT_LIST_PATH	許可リストの初期化で横断するフォルダパスです 空白の場合は各ローカルディスクのルートディレクトリを横断します	<フォルダパス>	<空白>	なし

KEY	説明	使用可能な値	初期設定値	暗号化
INIT_LIST_PATH_OPTIONAL	許可リストの初期化で横断するフォルダパスです 空白の場合は各ローカルディスクのルートディレクトリを横断します	<フォルダパス>	<空白>	なし
INIT_LIST_EXCLUDED_FOLDER	許可リストの初期化時にファイルの自動列挙から除外するフォルダの絶対パスです この設定は許可リストの最初の初期化とそれ以降のすべての許可リストのアップデートに適用されます 複数のフォルダを指定する場合は、INIT_LIST_EXCLUDED_FOLDER から始まる名前で新しいエントリを作成します。各エントリの名前は一意にします。次に例を示します INIT_LIST_EXCLUDED_FOLDER=c:\folder1	<フォルダパス> **注意** • 最大 260 文字まで指定できます。 • 存在しないフォルダパスを指定することもできます。 • 除外はサブフォルダに適用されます。	<空白>	なし

KEY	説明	使用可能な値	初期設定値	暗号化
	INIT_LIST_EXCLUDED_FOLDER2=c:\folder2 INIT_LIST_EXCLUDED_FOLDER3=c:\folder3			
INIT_LIST_EXCLUDED_EXTENSION	許可リストの初期化時にファイルの自動列挙から除外するファイルの拡張子です この設定は許可リストの最初の初期化とそれ以降のすべての許可リストのアップデートに適用されます 複数の拡張子を指定する場合は、INIT_LIST_EXCLUDED_EXTENSION から始まる一意の名前で新しいエントリを作成します。次に例を示します INIT_LIST_EXCLUDED_EXTENSION=bmp INIT_LIST_EXCLUDED_EXTENSION2=png	<ファイル拡張子>  **注意** 実行可能ファイルのファイル拡張子(例:exe、dll、sys)を指定すると、アプリケーション制御で問題が発生する場合があります。	INIT_LIST_EXCLUDED_EXTENSION1=log INIT_LIST_EXCLUDED_EXTENSION2=txt INIT_LIST_EXCLUDED_EXTENSION3=ini	なし

KEY	説明	使用可能な値	初期設定値	暗号化
LOCKDOWN	インストール後にアプリケーション制御を有効にします	• 0:アプリケーション制御を無効にします • 1:アプリケーション制御を有効にします	0	なし
FILELESS_ATTACK_PREVENTION	ファイルレス攻撃対策機能を有効にします	• 0:機能を無効にします • 1:機能を有効にします	0	なし
SERVICE_CREATION_PREVENTION	サービス作成対策機能を有効にします	• 0:機能を無効にします • 1:機能を有効にします	0	なし

注意

StellarProtect (Legacy Mode) は、次の場合にサービス作成対策機能を一時的に無効にします。

- 許可リスト自動更新によって許可されたインストーラを使用して、新しいアプリケーションをアップデートまたはインストールする場合許可リスト自動更新のプロセス完了後、自動的に本機能が再度有効になります
- Windows Update サポートを有効にしている場合

  Windows Update サポートを無効にすると、自動的に本機能が再度有効になります

KEY	説明	使用可能な値	初期設定値	暗号化
USR_DEBUGLOG_ENABLE	ユーザセッションのデバッグログを有効にします	• 0:デバッグログを無効にします • 1:デバッグログを有効にします	0	なし
USR_DEBUGLOGLEVEL	ユーザセッションのデバッグレベル	273	273	なし
SRV_DEBUGLOG_ENABLE	サービスセッションのデバッグログを有効にします	• 0:デバッグログを無効にします • 1:デバッグログを有効にします	0	なし
SRV_DEBUGLOGLEVEL	サービスセッションのデバッグレベル	273	273	なし
FW_USR_DEBUGLOG	ファイアウォールのユーザセッションのデバッグログを有効にします	• 0:デバッグログを無効にします • 1:デバッグログを有効にします	0	なし
FW_USR_DEBUGLOG_LEVEL	ファイアウォールのユーザセッションのデバッグレベル	数値	273	なし
FW_SRV_DEBUGLOG_ENABLE	ファイアウォールのサービスセッションのデバッグログを有効にします	• 0:デバッグログを無効にします • 1:デバッグログを有効にします	0	なし
FW_SRV_DEBUGLOG_LEVEL	ファイアウォールのサービスセッションのデバッグレベル	数値	273	なし

KEY	説明	使用可能な値	初期設定値	暗号化
BM_SRV_DEBUGLOG_ENABLE	挙動監視コアサービスのデバッグログを有効にします	• 0:デバッグログを無効にします • 1:デバッグログを有効にします	0	なし
BM_SRV_DEBUGLOG_LEVEL	挙動監視コアサービスのデバッグレベル	51	51	なし
INTELLIGENT_RUNTIME_LEARNING	許可リスト内のアプリケーションによって生成されたランタイム実行ファイルがエージェントで許可されます	• 0:無効 • 1:有効	0	なし
ACTIVEUPDATE_SOURCE	アップデート元を指定するために使用されます	https://txse-p.activeupdate.trendmicro.com/activeupdate (初期設定)	<空白>	なし
ALLOW_NON_MASS_STORAGE_USB_DEVICE	タッチスクリーン/赤外線センサ/Android スマホなどのハードウェアデバイスが接続され、ストレージデバイスのブロックが有効な場合に、対象ドライバのロードが許可されます。	• 0:無効 (初期設定) • 1:有効	<空白>	なし

EventLog セクション

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-4. Setup.ini ファイルの [Eventlog] セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
ENABLE	StellarProtect (Legacy Mode) のイベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
LEVEL_WARNINGLOG	StellarProtect (Legacy Mode) の警告レベルのイベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
LEVEL_INFORMATIONLOG	StellarProtect (Legacy Mode) の情報レベルのイベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	0	なし
BLOCKEDACCESSLOG	StellarProtect (Legacy Mode) でブロックされたファイルをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
APPROVEDACCESSLOG	StellarProtect (Legacy Mode) で許可されたファイルをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
APPROVEDACCESSLOG_TRUSTEDUPDATER	許可リスト自動更新で許可されたアクセスをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし

KEY	説明	使用可能な値	初期設定値	暗号化
APPROVEDACCESSLOG_TRUSTEDHASH	信頼するハッシュで許可されたアクセスをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
APPROVEDACCESSLOG_DLLDRIVER	DLL/ドライバ制御で許可されたアクセスをログに記録します	• 1:ログに記録します • 0:ログに記録しません	0	なし
APPROVEDACCESSLOG_EXCEPTIONPATH	アプリケーション制御除外パスで許可されたアクセスをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
APPROVEDACCESSLOG_TRUSTEDCERT	信頼するデジタル証明書で許可されたアクセスをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
APPROVEDACCESSLOG_WRITEPROTECTION	書き込み制御で許可されたアクセスをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
SYSTEMEVENTLOG	StellarProtect (Legacy Mode) のシステムに関連するイベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
SYSTEMEVENTLOG_EXCEPTIONPATH	アプリケーション制御の機能に関連するイベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし

KEY	説明	使用可能な値	初期設定値	暗号化
SYSTEMEVENTLOG_WRITEPROTECTION	書き込み制御の機能に関連するイベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
LISTLOG	許可リストに関連するイベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
USBMALWAREPROTECTIONLOG	USB 不正プログラム対策を作動させるイベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
EXECUTIONPREVENTIONLOG	実行防止対策を作動させるイベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
NETWORKVIRUSPROTECTIONLOG	ネットワークウイルス対策を作動させるイベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
INTEGRITYMONITORINGLOG_FILECREATED	変更監視のファイルおよびフォルダ作成イベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
INTEGRITYMONITORINGLOG_FILEMODIFIED	変更監視のファイル変更イベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし

KEY	説明	使用可能な値	初期設定値	暗号化
INTEGRITYMONITORINGLOG_FILEDELETED	変更監視のファイルおよびフォルダ削除イベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
INTEGRITYMONITORINGLOG_FILERENAMED	変更監視のファイル名およびフォルダ名変更イベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
INTEGRITYMONITORINGLOG_REGVALUEMODIFIED	変更監視のレジストリ値変更イベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
INTEGRITYMONITORINGLOG_REGVALUEDELETED	変更監視のレジストリ値削除イベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
INTEGRITYMONITORINGLOG_REGKEYCREATED	変更監視のレジストリキー作成イベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
INTEGRITYMONITORINGLOG_REGKEYDELETED	変更監視のレジストリキー削除イベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし
INTEGRITYMONITORINGLOG_REGKEYRENAMED	変更監視のレジストリキー名変更イベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし

KEY	説明	使用可能な値	初期設定値	暗号化
DEVICECONTROLLOG	デバイスアクセスコントロールに関連するイベントをログに記録します	• 1:ログに記録します • 0:ログに記録しません	1	なし

Server セクション

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-5. Setup.ini ファイルの [Server] セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
HOSTNAME	サーバのホスト名	<host_name>	<空白>	なし
PORT_FAST	高速接続用のサーバの待機ポート	1 - 65535	<空白>	なし
CERT	証明書ファイル名	<certificate_file_name>	<空白>	なし

Agent セクション

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-6. Setup.ini ファイルの [Agent] セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
PORT	エージェントの待機ポート	1 - 65535	<空白>	なし
FIXED_IP	StellarProtect (Legacy Mode) サーバと通信するエージェントの IP アドレスを設定します	• A.B.C.D/E • A,B,C,D: 0~255 • E: 1~32	<空白>	なし

Maintenance Mode セクション

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-7. Setup.ini ファイルの [Maintenance Mode] セクションの引数

キー	説明	使用可能な値	初期設定値	暗号化
ENABLE_DURATION	インストールプロセスの終了後、この期間のメンテナンスモードをただちに開始します	0 - 999 単位:時間	0	なし
SCAN	メンテナンス期間後のファイルの検索を有効にします	• 0:検索しない (初期設定) • 1:隔離 StellarProtect (Legacy Mode) は、メンテナンス期間中に作成、実	0	なし

キー	説明	使用可能な値	初期設定値	暗号化
		行、または変更されたファイルを検索し、検出されたファイルを隔離します • 2:al StellarProtect (Legacy Mode) は、メンテナンス期間中に作成、実行、または変更されたファイルを検索し、不正として検出されたファイルを含めて許可リストに追加します		

Message セクション

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-8. Setup.ini ファイルの [Message] セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
INITIAL_RETRY_INTERVAL	StellarOne にイベントの再送信を試行する間隔 (秒) の初期設定値です この間隔は、MAX_RETRY_INTERVAL 値に達するまで、試行が失敗するたびに倍増します	• 0 ～ 2147483647	120	なし

KEY	説明	使用可能な値	初期設定値	暗号化
MAX_RETRY_INTERVAL	StellarOne にイベントの再送信を試行する間隔 (秒) の最大値です	• 0 ～ 2147483647	7680	なし

MessageRandomization セクション

注意

StellarProtect (Legacy Mode) エージェントは、可能なかぎり速やかに StellarOne からの要求に応答します。詳細については、StellarProtect (Legacy Mode) 管理者ガイドの「メッセージタイムグループを適用する」を参照してください。

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-9. Setup.ini ファイルの [MessageRandomization] セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
TOTAL_GROUP_NUM	サーバコントロールで制御されるグループ数	0-2147483646	0	なし
OWN_GROUP_INDEX	このエージェントが所属するグループのインデックス	0-2147483646	0	なし
TIME_PERIOD	エージェントがデータをアップロードする最長時間 (秒単位)	0-2147483647	0	なし

Proxy セクション

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-10. Setup.ini ファイルの [PROXY] セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
MODE	プロキシのモード	• 0:プロキシを使用しません • 1:手動設定でプロキシを使用します • 2:Internet Explorer から自動的に取得された設定でプロキシを使用します	0	なし
HOSTNAME	プロキシホスト名	<host_name>	<空白>	なし
PORT	プロキシポート番号	1-65535	<空白>	なし
USERNAME	プロキシユーザ名	<user_name>	<空白>	なし
PASSWORD	プロキシのパスワード	<password>	<空白>	なし

Prescan セクション

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-11. Setup.ini ファイルの[PRESCAN]セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
IGNORE_THREAT	事前検索中に不正プログラムを検出したらインストールを取り消します	• 0:キャンセル • 1:事前検索中に不正プログラムを検出してもインストールを続行します • 2:不正プログラムが検出されない場合、または検出されたすべての不正プログラムが駆除、削除、または隔離された後、システムを再起動せずにインストールを続行します	2	なし
REPORT_FOLDER	事前検索の結果レポートを保存するフォルダの絶対パスです	• <folder_path> • <空白>:初期設定は%windir%\temp\prescan\log です	<空白>	なし

KEY	説明	使用可能な値	初期設定値	暗号化

SCAN_TYPE	サイレントインストール中に実行する検索の種類です
	
	注意
	選択した値は UI インストールの初期設定値として使用されます。
		• Full:コンピュータのすべてのフォルダを検索します
		• Quick:次のフォルダを検索します
		  • 固定ルートドライブ
		  例:
		  C:\
		  d:\
		  • システムのルートフォルダ
		  例:
		  c:\Windows
		  • システムフォルダ
		  例:
		  c:\Windows\System
		  • System32 フォルダ
		  例:
		  c:\Windows\System32
		  • ドライバフォルダ
		  例:
		  c:\Windows\System32\Drivers
			Full	なし

KEY	説明	使用可能な値	初期設定値	暗号化
		• 一時フォルダ 例: c:\Users\Trend\AppData\Local\Temp • デスクトップフォルダ (サブフォルダとファイルを含む) 例: c:\Users\Trend\Desktop • Specific:SPECIFIC_FOLDER エントリで指定したフォルダを検索します		
COMPRESS_LAYER	圧縮ファイルを検索する際の圧縮階層数です	• 0:圧縮ファイルは検索しません • 1 - 20:指定された階層数まで圧縮ファイルを検索します	2	なし
MAX_FILE_SIZE	検索可能な最大ファイルサイズです	• 0:すべてのサイズのファイルを検索します • 1 - 9999:指定したサイズ (MB)以下のファイルのみを検索します	0	なし

KEY	説明	使用可能な値	初期設定値	暗号化
SCAN_REMOVABLE_DRIVE	リムーバブルドライブを検索する	• 0:リムーバブルドライブを検索しない • 1:リムーバブルドライブを検索する	0	なし
SPECIFIC_FOLDER	検索の種類が [Specific] の場合に検索するフォルダの絶対パスです	<folder_path> SPECIFIC_FOLDER で始まる名前の新しいエントリを作成することにより複数のフォルダを指定できます 各エントリ名は一意である必要があります 例: SPECIFIC_FOLDER=c:\folder1 SPECIFIC_FOLDER2=c:\folder2 SPECIFIC_FOLDER3=c:\folder3	<空白>	なし
EXCLUDED_FILE	検索から除外するファイルの絶対パスです	<file_path> EXCLUDED_FILE で始まる名前の新しいエントリを作成することにより複数のファイルを指定できます 各エントリ名は一意である必要があります 例: EXCLUDED_FILE=c:\file1.exe EXCLUDED_FILE2=c:\file2.exe EXCLUDED_FILE3=c:\file3.exe	<空白>	なし

KEY	説明	使用可能な値	初期設定値	暗号化
EXCLUDED_FOLDER	検索から除外するフォルダの絶対パスです	<folder_path> EXCLUDED_FOLDER で始まる名前の新しいエントリを作成することにより複数のフォルダを指定できます 各エントリ名は一意である必要があります 例: EXCLUDED_FOLDER=c:\file1 EXCLUDED_FOLDER2=c:\file2 EXCLUDED_FOLDER3=c:\file3	<空白>	なし
EXCLUDED_EXTENSION	検索から除外するファイル拡張子です	<file_extension> EXCLUDED_EXTENSION で始まる名前の新しいエントリを作成することにより複数の拡張子を指定できます 各エントリ名は一意である必要があります 例: EXCLUDED_EXTENSION=bmp EXCLUDED_EXTENSION2=png	<空白>	なし

KEY	説明	使用可能な値	初期設定値	暗号化
PRESCANCLEANUP	事前検索中に検出されたファイルの駆除を試行します	• 0:処理は行われません • 1:駆除します。駆除処理に失敗した場合は削除します • 2:駆除します。駆除処理に失敗した場合は隔離します • 3:駆除します。駆除処理に失敗した場合は無視します	2	なし
FORCE_PRESCAN	インストール前に事前検索を実行します	• 0:無効 • 1:有効	0	なし

BlockNotification セクション

次の表は、setup.ini (セットアップファイル) で使用可能な通知コマンドを示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

詳細については、31 ページの「Property セクション」を参照してください。

重要

この機能を有効にする場合は、必ず、システムトレイアイコンと通知の表示も有効にしてください。詳細については、この表の「NO_SYSTRAY」を参照してください。

表 2-12. Setup.ini ファイルの[BlockNotification]セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
ENABLE	StellarProtect (Legacy Mode) が許可されていないファイルをブロックしたときに管理下のエージェントに通知を表示します	• 0:無効 • 1:有効	0	なし
ALWAYS_ON_TOP	開かれている画面の上部にポップアップ通知を表示します	• 0:無効 • 1:有効	1	なし
SHOW_DETAILS	通知にファイル名、ファイルパス、およびイベント時間を表示します	• 0:無効 • 1:有効	1	なし
AUTHENTICATE	通知を閉じるときに管理者パスワードを要求して、ユーザを認証します	• 0:無効 • 1:有効	1	なし
TITLE	通知のタイトル	<notification_title>	<空白>	なし
MESSAGE	通知内容	<notification_content>	<空白>	なし

第 3 章

エージェント設定ファイルの配信

この章では、エージェント設定ファイルを使用して複数の TXOne StellarProtect (Legacy Mode) エージェントに設定を配信する方法について説明します。

スタンドアロンエージェントへの配信

スタンドアロンモードでインストールされたエージェントは TXOne StellarProtect (Legacy Mode) 管理コンソールサーバによって管理されません。単一の設定を複数のスタンドアロンエージェントに手動で配信するには、エージェント設定ファイルを使用します。

設定ファイルをエクスポートまたはインポートする

注意

TXOne StellarProtect (Legacy Mode) では、エクスポート前に設定ファイルを暗号化します。ユーザは、設定ファイルを復号してから内容を変更する必要があります。

手順

1. TXOne StellarProtect (Legacy Mode) のデスクトップアイコン、または [スタート] メニューから [すべてのプログラム]→[TXOne StellarProtect (Legacy Mode)] をクリックして、管理サーバ画面を開きます。
2. パスワードを指定して [ログオン] をクリックします。
3. [設定] メニュー項目をクリックして [設定のエクスポート/インポート] セクションにアクセスします。

   設定ファイルをエクスポートするには

   a. [設定のエクスポート] をクリックして、ファイルの保存場所を選択します。

   b. ファイル名を指定して、[保存] をクリックします。

   設定ファイルをインポートするには

   a. [設定のインポート] をクリックして、設定ファイルを指定します。

   b. ファイルを選択して、[開く] をクリックします。

   TXOne StellarProtect (Legacy Mode) の既存の設定が、設定ファイルの内容で上書きされます。

StellarOne を使用した配信

集中管理モードでインストールされたエージェントは StellarOne サーバによって管理されており、サーバからすべての管理対象エージェントにリモートでコマンドを発行できます。複数の管理対象エージェントにエージェントの設定を配信するには、StellarOne の管理サーバ画面を起動して、[エージェント管理] 画面にある [コマンドの送信] メニューを使用します。

エージェントの設定をリモートでエクスポートする

StellarOne からエージェントの設定と許可リストをエクスポートしダウンロードすることで、それらをリモートで取得できます。

手順

1. StellarOne で [エージェント]→[StellarProtect (Legacy Mode)] の順にクリックします。

   [エージェント管理] 画面が表示されます。

2. 対象のエージェントを選択します。

3. [インポート/エクスポート] をクリックして、次のいずれかを選択します。

   - 許可リストのインポート
   - エージェントの設定のインポート

   StellarOne からコマンドが発行されます。[詳細] ポップアップウィンドウで進行状況を確認できます。

4. 設定をエクスポートするには、前述の手順を繰り返し、手順 3 で [許可リストのエクスポート] または [エージェントの設定のエクスポート] のいずれかを選択します。

エクスポートが完了すると、画面上部に次のメッセージが表示されます。

5. [ダウンロード] をクリックして、エクスポートされた設定をダウンロードします。

エージェントの設定をリモートでインポートする

StellarOne からエージェントに新しい設定をリモートで適用できます。この機能により次のことが可能になります。

- エージェントの設定をリモートで上書きする
- 許可リストをリモートで上書きする
- 許可する項目を許可リストにリモートで追加する

手順

1. カスタマイズするエージェントの設定ファイルまたは許可リストを準備します。
   a. エージェントの設定ファイルまたは許可リストをエクスポートしてダウンロードします。
   b. ダウンロードしたファイルをカスタマイズします。

注意

正常にインポートするため、インポートするファイルが次の要件を満たしていることを確認します。

- CSV 形式で UTF-8 エンコーディングを使用している
- 許可リストの場合、サポートされるファイルの最大サイズは 20MB
- エージェントの設定ファイルの場合、サポートされるファイルの最大サイズは 1MB

2. StellarOne の管理サーバ画面で [エージェント] をクリックします。

   [エージェント管理] 画面が表示されます。

3. カスタマイズしたファイルをエージェントにインポートするには、次の手順を実行します。

   a. エージェント列でエージェントを 1 つ以上選択します。

   b. [インポート/エクスポート] をクリックします。

   c. [許可リストのインポート] または [エージェントの設定のインポート] を選択します。

      インポートダイアログが表示されます。

4. カスタマイズしたファイルをエージェントグループにインポートするには、次の手順を実行します。

   a. 左のパネルでエージェントグループを選択し、[インポート/エクスポート] を選択します。

   b. [許可リストのインポート] または [エージェントの設定のインポート] を選択します。

      インポートダイアログが表示されます。

5. 初期設定で、StellarOne では以下が実行されます。

   - **許可リスト:**カスタマイズした許可リストから対象の許可リストに項目が累積されます。対象の許可リストをカスタマイズした許可リストで置き換えるには、[既存アプリケーションの信頼するハッシュ値を更新します。] をオンにします。
   - **エージェントの設定:**カスタマイズした許可リストで対象の許可リストが上書きされます。

6. [ファイルの選択] をクリックして、カスタマイズしたファイルを選択します。
7. [OK] をクリックします。

第 4 章

ローカルエージェントのアンインストール

この章では、TXOne StellarProtect (Legacy Mode) エージェントのアンインストール手順について説明します。

この章の内容は次のとおりです。

エージェントを Windows からアンインストールする

注意

エージェントから StellarProtect (Legacy Mode) をアンインストールするには、管理者パスワードが必要です。

手順

1. StellarProtect (Legacy Mode) エージェントがインストールされたエージェントで、TXOne StellarProtect (Legacy Mode) のセットアップを起動します。

   お使いの OS に応じて、次のいずれかを実行します。

オプション	説明
次のいずれかの OS を使用している場合: • Windows 10 Enterprise • Windows 10 IoT Enterprise • Windows 10 Professional	a. [スタート]→[設定] の順に選択します。 b. Windows 10 のバージョンに応じて、次のいずれかのカテゴリから [アプリと機能] セクションを見つけます。 • システム • アプリ c. 左側のペインで [アプリと機能] をクリックします。 d. 表示されるリストで [TXOne StellarProtect (Legacy Mode)] を選択します。 e. [アンインストール] をクリックします。
次のいずれかの OS を使用している場合: • Windows 7 • Windows 8 • Windows Vista • Windows Server 2008 • Windows Server 2012 • Windows Server 2016 • Windows Storage Server 2016	a. [スタート]→[コントロールパネル]→[プログラムと機能] の順に選択します。 b. 表示されるリストで [TXOne StellarProtect (Legacy Mode)] をダブルクリックします。

オプション	説明
• Windows Server 2019	
次のいずれかの OS を使用している場合: • Windows Server 2003 • Windows XP • Windows 2000	a. [スタート]→[コントロール パネル]→[プログラムの追加と削除] の順に選択します。 b. 表示されるリストで [TXOne StellarProtect (Legacy Mode)] を選択します。 c. [削除] をクリックします。

StellarProtect (Legacy Mode) のセットアップがアンインストーラモードで開きます。

2. StellarProtect (Legacy Mode) のセットアップが開いたら、[次へ] をクリックします。
3. StellarProtect (Legacy Mode) 管理者パスワードを指定して、[次へ] をクリックします。
4. StellarProtect (Legacy Mode) のアンインストールが完了したら、[完了] をクリックします。

第 5 章

製品サポート情報

TXOne Networks は、トレンドマイクロと Moxa 社の合弁企業であり、TXOne Networks 製品のサポートはトレンドマイクロが行います。すべての製品サポート情報は、トレンドマイクロのエンジニアを介して提供されます。

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。

文書番号: APEM139597_JP2303