TREND MICRO | txOne networks

2.0 TXOne StellarProtect
インストール & 管理者ガイド

※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: APEM29618_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 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 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

この管理者ガイドでは、TXOne Networks StellarProtect について紹介するとともに、製品管理のあらゆる側面について説明します。

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 Networks StellarProtect 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 Networks StellarProtect のドキュメントは、エージェントのインストールを含めた StellarProtect 管理担当者を対象としています。

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

この章では、産業グレード次世代ウィルス対策を資産に対して提供する TXOne StellarProtect について紹介し、その機能を概説します。

TXOne Stellar および StellarProtect について

TXOne Stellar は、業界初の OT エンドポイント保護プラットフォームであり、次の各製品で構成されています。

- StellarProtect: モダナイズされた OT/ICS エンドポイント向けの、産業グレード次世代ウィルス対策およびアプリケーション制御のエンドポイントセキュリティ配信機能を備えた統合エージェント
- StellarProtect (Legacy Model): 旧来の特定用途の OT/ICS エンドポイントに対する、手動のウイルス検索機能を備えた信頼リストベースのアプリケーション制御を提供
- StellarOne: モダナイズされたシステム向けの StellarProtect とレガシーシステム向けの StellarProtect (Legacy Model) の両方の管理を効率化するように設計された集中管理コンソール

TXOne StellarProtect は、OT/ICS 互換の高性能かつゼロタッチのエンドポイント保護ソリューションです。

新機能

TXOne StellarProtect 2.0 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 2.0 の新機能

機能	説明
アプリケーション制御	この機能は、アプリケーションリストで定義されているファイルをロックダウンすることにより、不正プログラムによる攻撃を阻止し、保護レベルを引き上げます。
不正プログラムのリアルタイム検索	メンテナンスモードを設定するためのグラフィカルユーザインタフェースを提供します。また、[メンテナンスモード] オプションの下に [リアルタイムの不正プログラム検索] スイッチが追加され、メンテナンス期間中も検索機能を有効にするようユーザを促します。

エージェントの機能と特徴

StellarProtect には、次の機能と特徴があります。

機能	特徴
アプリケーション制御	アプリケーションリストに追加されたファイルをロックダウンし、未承認のファイルからエンドポイントを保護することにより、不正プログラムによる攻撃を阻止し、保護レベルを引き上げます。
産業グレード次世代ウィルス対策	OT/ICS の信頼の基点と高度な脅威検索で、操作を中断することなく OT 資産を保護します。
オペレーション振る舞い検知	オペレーションを監視することでファイルレス攻撃を検知、ブロックします。
OT アプリケーション保護	OT アプリケーションを検出し、OT アプリケーションの改ざんなどから保護します。
デバイスコントロール	USB デバイスなどの外部接続デバイスが端末に接続する際、許可されたデバイスのみ接続を許可することで外部デバイス経由の感染を防ぎます。
メンテナンスモード	エンドポイントでファイルのアップデートを実行するには、メンテナンスモードを設定します。これにより、StellarProtect がすべてのファイルの実行を許可し、作成、実行、または変更されたすべてのファイルを許可リストに追加する期間を定義できます。
Trend Micro Portable Security 2 および 3 との互換性	StellarProtect は Trend Micro Portable Security 製品と互換性があります。

第 2 章

インストール

この章では、TXOne StellarProtect エージェントのインストール方法について説明します。StellarProtect エージェントには、ローカルインストールとサイレントインストールという 2 つのインストールの種類があります。

この章の内容は次のとおりです。

システム要件

最新の情報については、次の Web サイトを参照してください。

https://www.trendmicro.com/ja_jp/business/products/iot/industrial-endpoint-security/txone-stellar-protect.html

注意

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

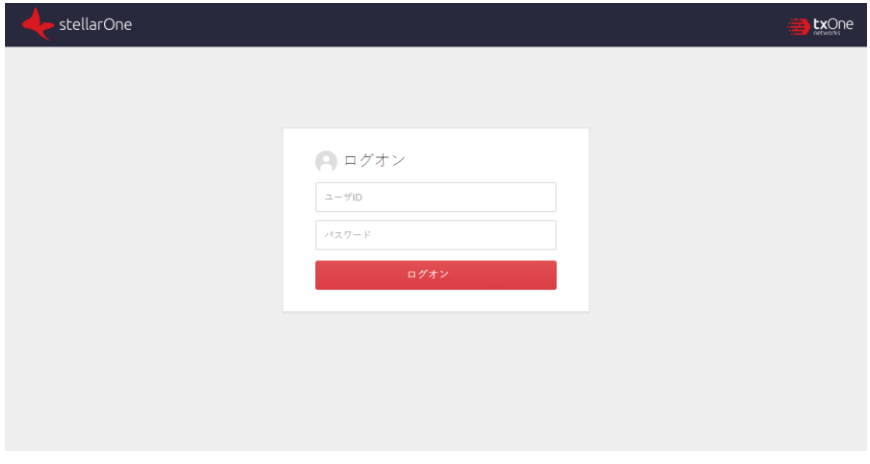
ローカルインストール

ここでは主に、StellarOne からのインストールファイルのダウンロード、インストーラの実行、および設定の実行など、StellarProtect のインストール手順について説明します。

StellarProtect エージェントパッケージの入手

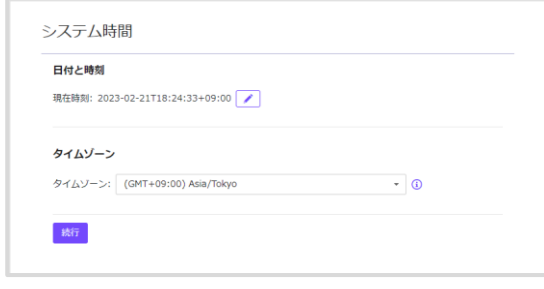
手順

1. まず、StellarOne にログインします (初期設定の ID とパスワードは admin/txone)。アカウントのセキュリティを確保するため、パスワードを変更するように求められます。



2. 管理者パスワードを変更します。新しいログイン名 (ID) の強度がチェックされ、確認のためにパスワードを 2 回入力するように求められます。

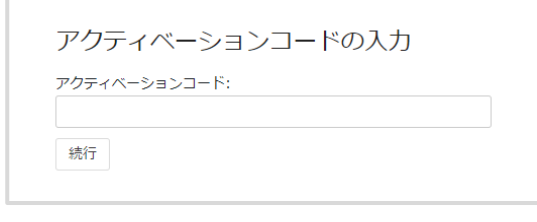
3. パスワードの変更後、日付と時刻を設定するための画面が表示されます。



4. StellarOne のサービスをアクティベートするため、アクティベーションコード (AC) を入力するように求められます。

注意

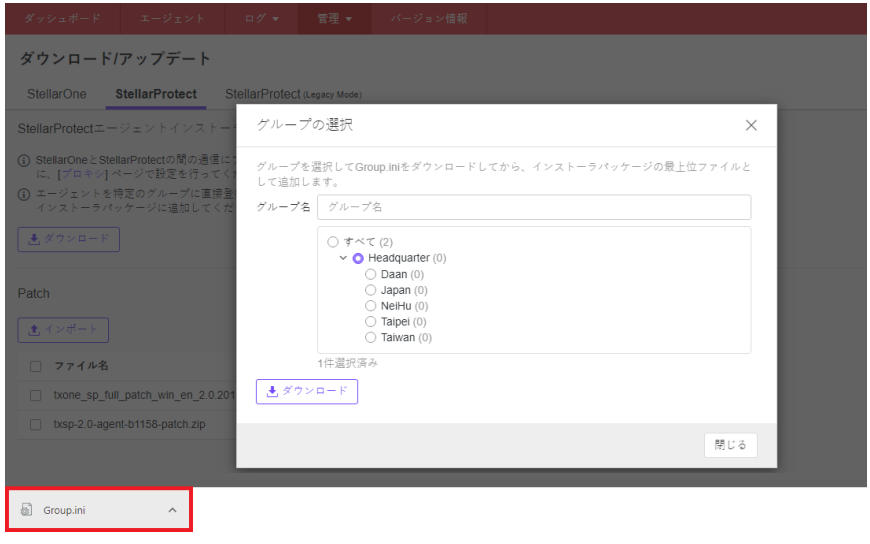
AC は、トレンドマイクロまたはその他の認定代理店から入手できます。



5. StellarOne の管理サーバ画面からインストールパッケージをダウンロードします。[管理]→[ダウンロード/アップデート] の順に選択して、StellarProtect のインストールパッケージをダウンロードできます。ダウンロードしたパッケージは StellarOne によりパックされており、すべてのエージェントでインストールできます。

6. (オプション) StellarProtect エージェントをグループに登録するには、[管理]→[ダウンロード/アップデート] の順に選択して、`Group.ini` ファイルをダウンロードします。

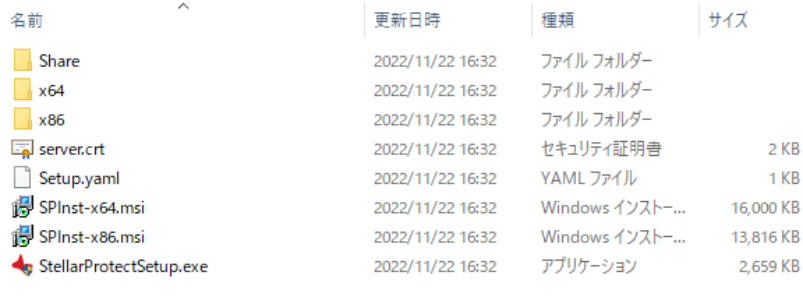
7. (オプション) StellarProtect エージェントのグループを選択し、[ダウンロード] をクリックします。Group.ini という名前のファイルがダウンロードされます。この `Group.ini` ファイルを、エージェントのインストーラパッケージの最上位ファイルとして追加します。



StellarProtect エージェントのインストール

手順

1. インストーラ StellarProtectSetup.exe を起動します。



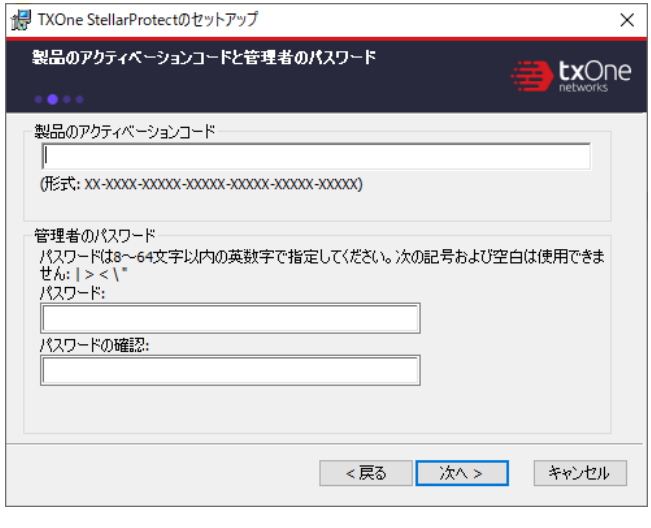
注意

1. StellarOne の管理サーバ画面を介して StellarProtect エージェントを特定グループに登録するには、StellarOne の管理サーバ画面に `Group.ini` ファイルをダウンロードした後、StellarProtect エージェントのインストーラパッケージに追加する必要があります。

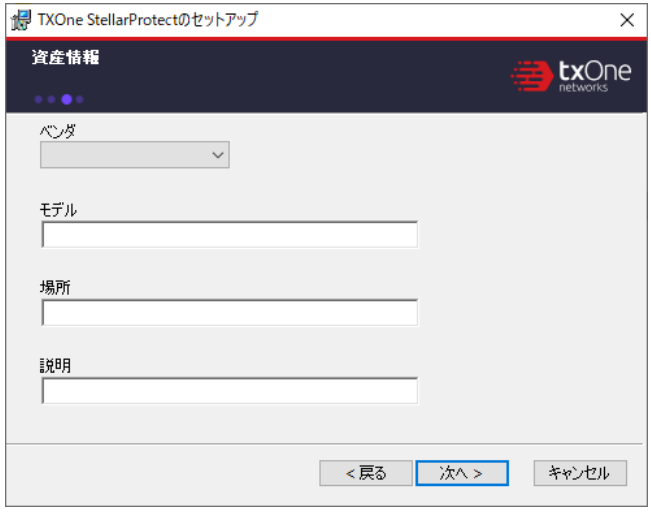
2. [次へ] をクリックして、インストールを開始します。

3. エンドユーザ使用許諾契約 (EULA) が表示されます。内容を読み、[使用許諾契約に同意します] チェックボックスをオンにして [次へ] をクリックします。

4. 製品のアクティベーションコードを入力し、管理者パスワードを選択します。8～64 文字の英数字から構成される強力な管理者パスワードを使用してください。



5. インストールされるデバイスの資産情報を入力します。ベンダ名、モデル、場所、説明など、ICS 関連の正しい情報を入力してください。



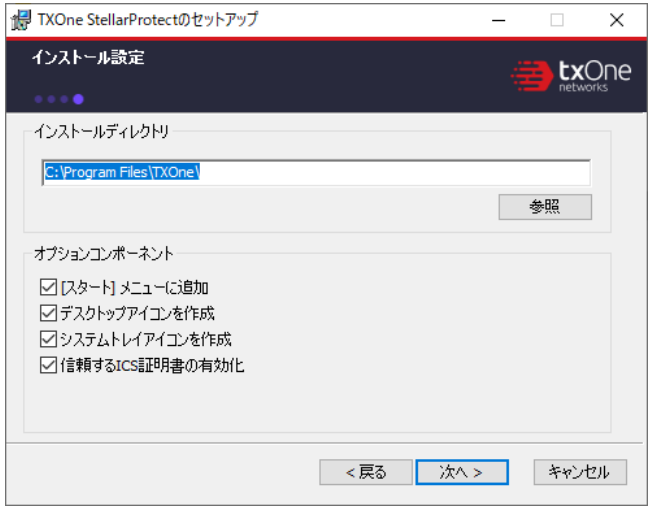
6. インストールディレクトリやオプションコンポーネントの設定など、インストール設定を確認します。

注意

[スタート] メニューへのアイコンの追加、デスクトップアイコンの作成、およびシステムトレイアイコンの作成を行うかどうかを選択できます。

重要

[信頼する ICS 証明書の有効化] チェックボックスもオンにすることをお勧めします。この機能により、StellarProtect で信頼する ICS 証明書が同期され、ICS アプリケーションが強化され、インストーラが常に StellarProtect によって認識されるようになります。

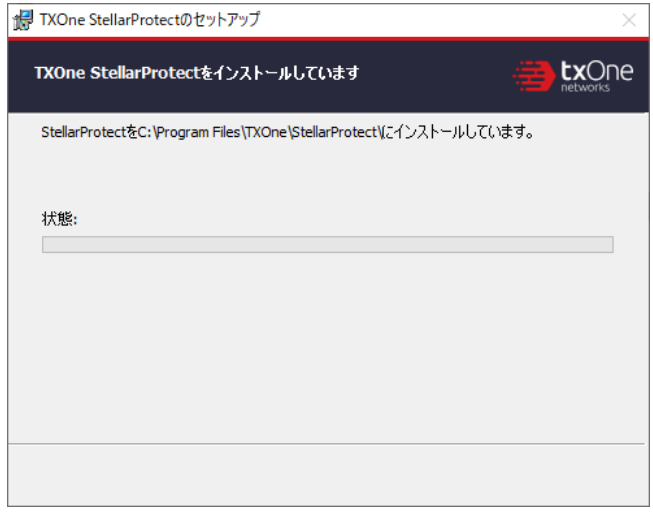


7. StellarProtect により互換性のないソフトウェアがシステム上で検出されると、次に示すメッセージが表示されます。検出されなかった場合、このメッセージは表示されません。

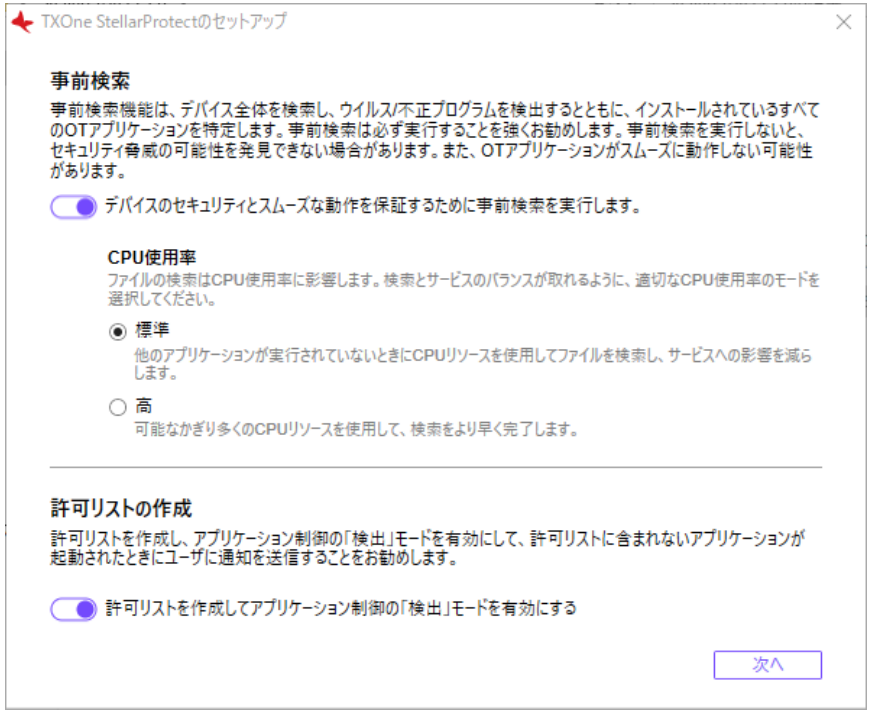
注意

互換性のないソフトウェアとは、ウイルスバスター コーポレートエディションシリーズ、ApexOne、ウイルスバスター ビジネスセキュリティ、ウイルスバスター ビジネスセキュリティサービスなどの一部のトレンドマイクロ製品を指します。互換性の問題を防ぐため、これらのソフトウェアをアンインストールするように求められます。

8. インストール中は、進行状況バーにステータスが表示されます。



9. [検索] ボタンをクリックして、事前検索を開始します。この手順は非常に重要です。インストールされている ICS アプリケーションを StellarProtect が把握できるように、ICS デバイスの検索を許可してください。



重要

事前検索を実行しないと、StellarProtect は稼働を再開する前に ICS アプリケーションを認識することができず、初めて実行された場合と同様にアプリケーションを学習しなければならなくなります。また、これにより ICS アプリケーションで遅延が発生する場合もあるため、StellarProtect がインストールされているアプリケーションを事前に学習できるように、[検索] をクリックすることを強くお勧めします。

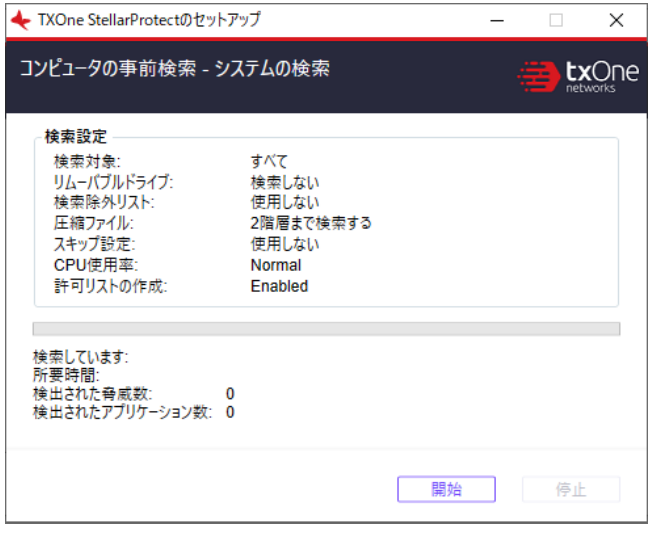
StellarProtect には、さらに効率的な [高] オプションがあります。[高] オプションでは検索時間が大幅に短縮されますが、より多くの CPU リソースを消費します。システム上で他の重要なアプリケーションを実行していない場合は、[高] オプションを選択することで検索時間をさらに短縮できます。

10. 既存の問題を検出するため、コンピュータの事前検索を実行してください。検索設定を確認し、[開始] ボタンをクリックして、StellarProtect のコンピュータの事前検索タスクを起動できます。

注意

事前検索を開始する前に、選択した設定に基づいてコンポーネントのアップデートが実行されます。スタンドアロンエージェントのインストーラパッケージについては、アップデートの実行にはトレンドマイクロのアップデートサーバへの接続が必要であり、インターネットアクセスが必要になります。

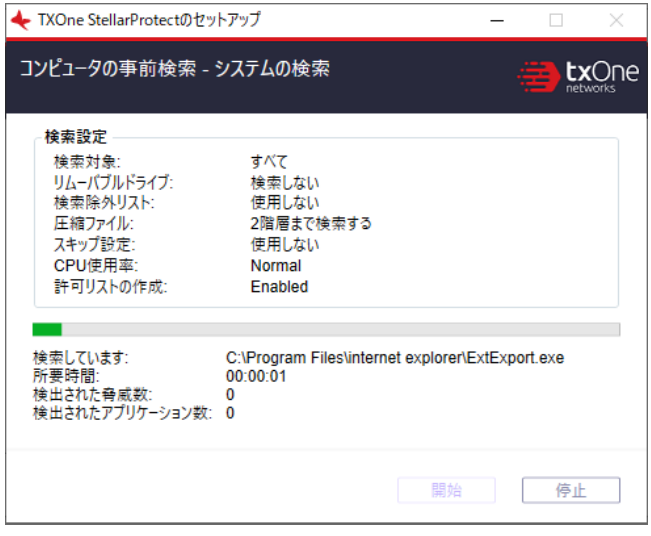
アップデートプロセスでは次のメッセージが表示されます。この画面は表示されても問題ありません。



検索設定の説明を次に示します。

- **検索対象:** テンプレートに基づいた初期設定のウイルス検索です。
- **リムーバブルドライブ:** 選択したリムーバブルドライブが検索されます。
- **検索除外リスト:** 指定したファイルまたはフォルダが検索から除外されます。
- **圧縮ファイル:** 20階層までの圧縮ファイルを検索します。
- **スキップ設定:** 指定したファイルがスキップされます。
- **CPU使用率:** 事前検索で使用されるCPUリソース。
- **許可リストの作成:** 許可リストの作成が有効になっているかどうか。

進行状況バーに事前検索のステータスが表示されます。

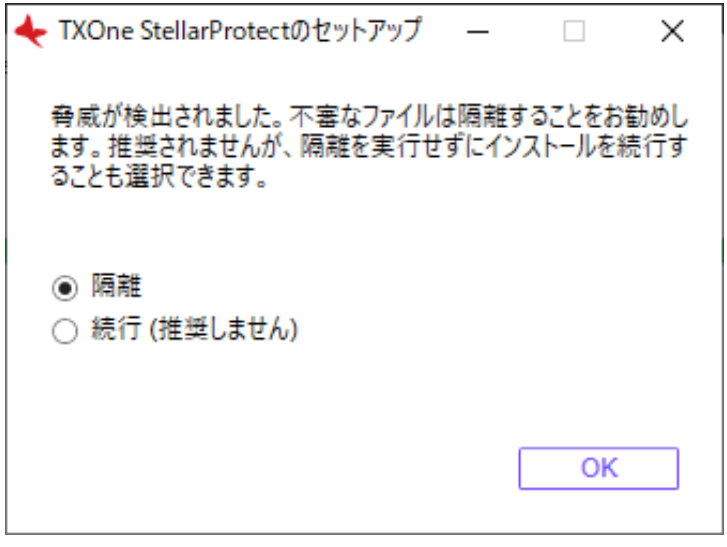


11. 事前検索が完了すると、確認のために結果が表示されます。

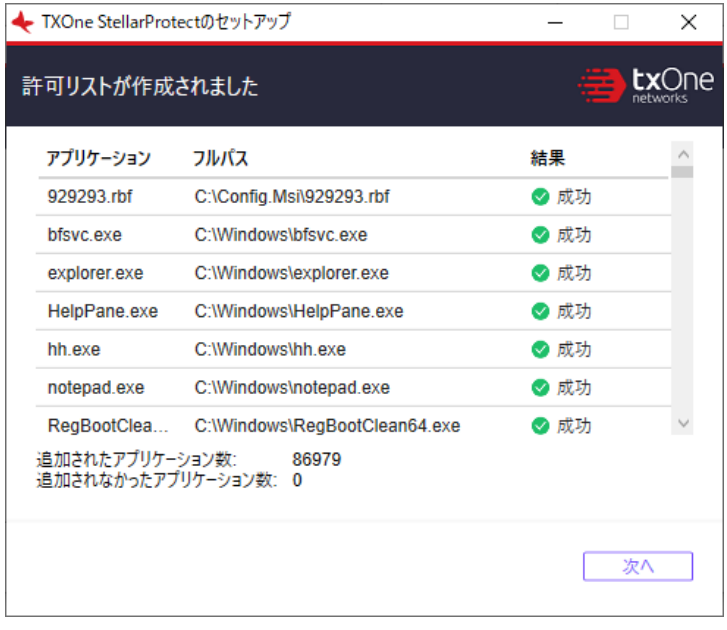
12. 脅威が検出された場合は、次の 2 つのオプションから選択できます。

    a. **隔離:** 脅威を隔離します。

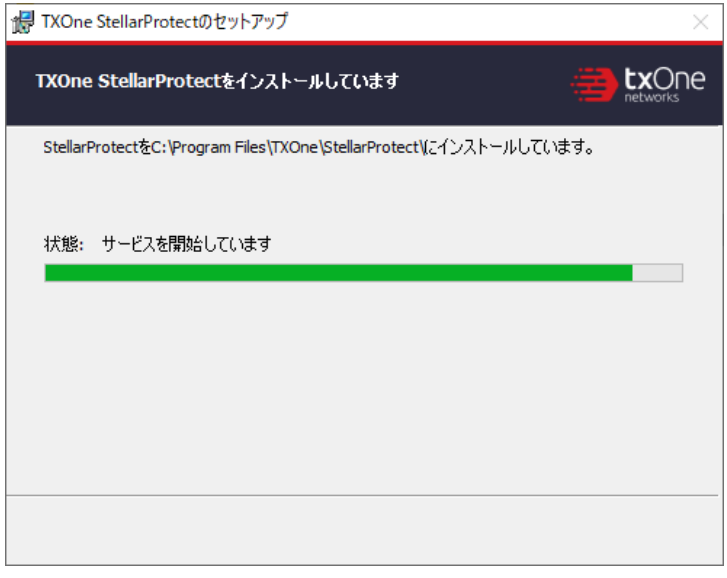
    b. **続行:** 今回は何も処理を実行しません。



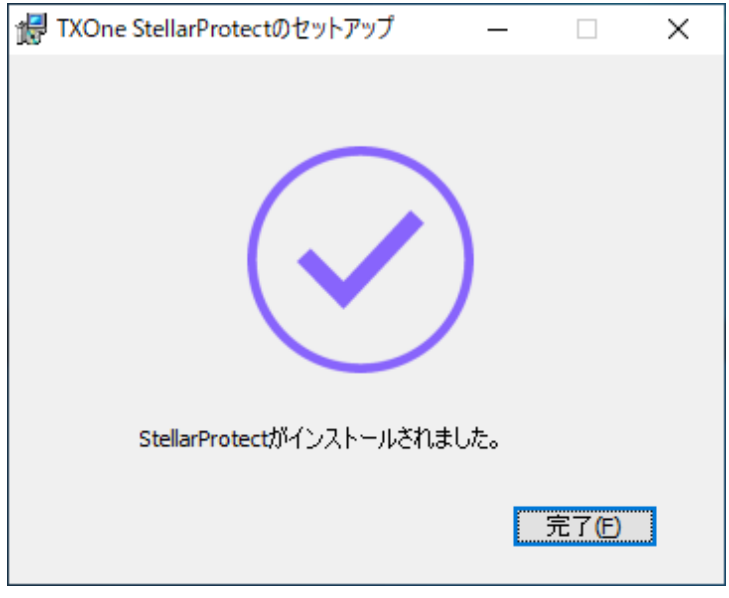
13. 許可リストへのアプリケーションの追加の結果が、確認のために表示されます。



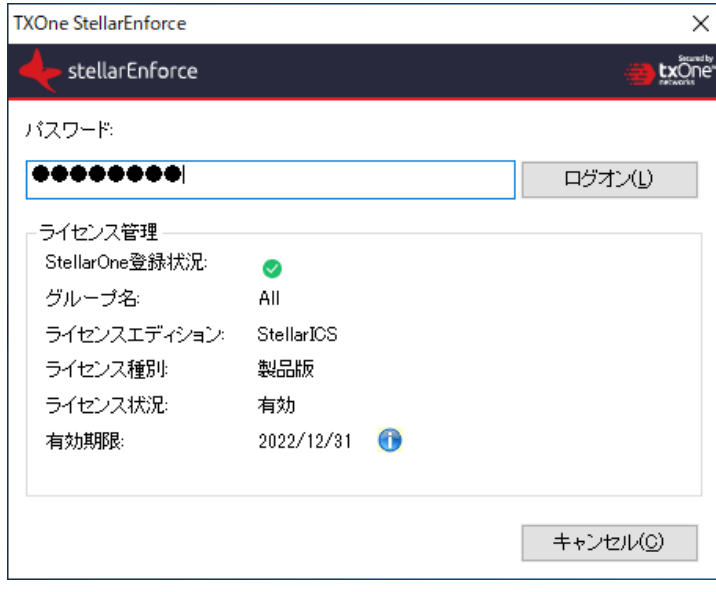
14. 事前検索と許可リストの作成が完了すると、StellarProtect アプリケーションがインストールされます。



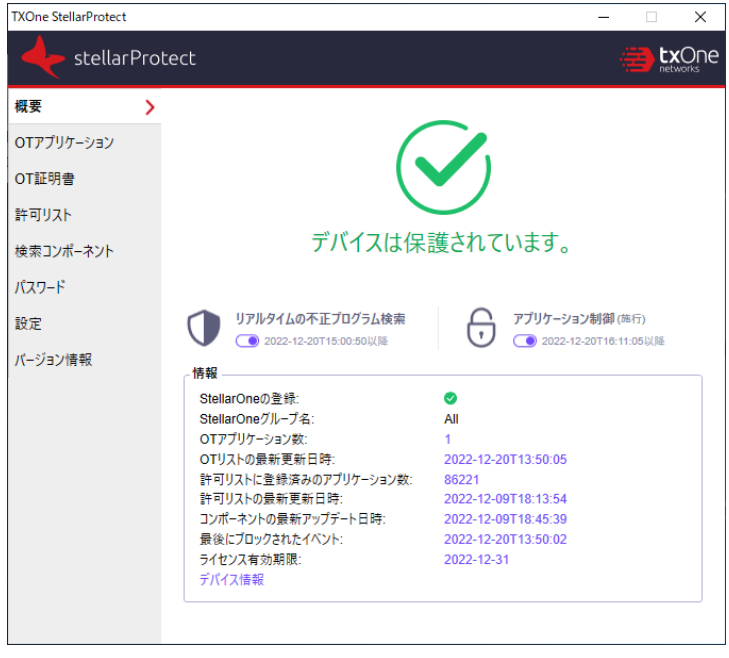
15. インストールが完了すると、次の画面が表示されます。



16. TXOne StellarProtect を実行し、自分のパスワードを使用してログインします。



17. StellarProtect へのログインに成功すると、次の画面が表示されます。



サイレントインストール

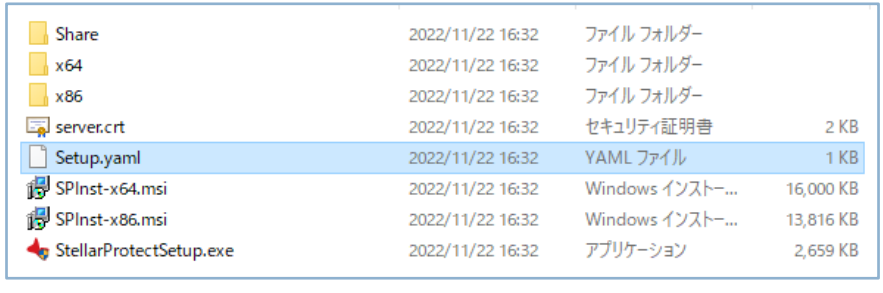
StellarProtect では、事前指定の設定ファイルに基づいてサイレントインストールを実行できます。設定セッションを使用して Setup.yaml に基づくサイレントインストールを有効にしてから、サイレントモードで StellarProtectSetup.exe を実行します。

サイレントインストールの設定

インストール用のセットアップ設定を事前に指定できます。セットアップファイル名は Setup.yaml に固定されています。

ランチャーにより実行時に Setup.yaml が解析されます。

次に示すように、Setup.yaml はインストールフォルダ内にあります。



- Client:
  - import_source: <IMPORT_SOURCE>
- install:
  - activation_code: <ACTIVATION_CODE>
  - asset_description: <ASSET_DESCRIPTION>
  - asset_location: <ASSET_LOCATION>
  - asset_model: <ASSET_MODEL>
  - asset_vendor: <ASSERT_VENDOR>
  - enable_desktop_icon: <ENABLE_DESKTOP_ICON>

    - enable_lockdown_al_building: <ENABLE_LOCKDOWN_AL_BUILDING>
    - enable_lockdown_detection: <ENABLE_LOCKDOWN_DETECTION>
    - enable_prescan: <ENABLE_PRESCAN>
    - enable_silent_install: <ENABLE_SILENT_INSTALL>
    - enable_start_menu: <ENABLE_START_MENU>
    - enable_systray_icon: <ENABLE_SYSTRAY_ICON>
    - enable_trusted_ics_cert: <ENABLE_TRUSTED_ICS_CERT>
    - install_location: <INSTALL_PATH>
    - password: <PASSWORD>

- prescan:
    - action: <PRESCAN_ACTION>
    - cpu_usage_mode: <PRESCAN_CPU_MODE>
- proxy:
    - default:
        - host: <DEFAULT_PROXY_SERVER_HOST>
        - password: < DEFAULT_PROXY_SERVER_PASSWORD>
        - port: < DEFAULT_PROXY_SERVER_PORT>
        - username: < DEFAULT_PROXY_SERVER_USERNAME>
- server:
    - cert: <SERVER_CERT>
    - host: <SERVER_HOST>
    - listen: <LISTEN_PORT>
    - port: <SERVER_PORT>

注意

次の隠しパラメータの詳細については、以下の表を参照してください。

- `bypass_windefend_check: <BYPASS_WINDEFEND_CHECK>`

次の表に、`Setup.yaml` のパラメータとその用途の詳細を示します。

パラメータ	タイプ	初期設定値	説明
`IMPORT_SOURCE`	string	空の文字列	インポートする設定を含むフォルダのパス。
`ACTIVATION_CODE`	string	空の文字列	ライセンスのアクティベーションに使用する StellarProtect のアクティベーションコード (AC)。
`ASSET_DESCRIPTION`	string	空の文字列	StellarProtect をインストールするデバイスの説明
`ASSET_LOCATION`	string	空の文字列	StellarProtect をインストールするデバイスの設置場所
`ASSET_MODEL`	string	空の文字列	StellarProtect をインストールするデバイスのモデル名
`ASSET_VENDOR`	string	空の文字列	StellarProtect をインストールするデバイスのメーカー名
`ENABLE_DESKTOP_ICON`	boolean	true	StellarProtect アイコンのデスクトップへの配置を有効にします。
`ENABLE_LOCKDOWN_AL_BUILDING`	boolean	true	アプリケーション制御用の許可リストの作成を有効にします。

パラメータ	タイプ	初期設定値	説明
ENABLE_LOCKDOWN_DETECTION	boolean	true	アプリケーション制御の検出モードを有効にします。
ENABLE_PRESCAN	boolean	true	インストール中のウイルス検索を有効にします。
ENABLE_SILENT_INSTALL	boolean	false	インストール画面を非表示にします。 サイレントインストール中に ACTIVATION_CODE と PASSWORD を指定する必要があります。
ENABLE_START_MENU	boolean	true	Windows の [スタート] メニューへの StellarProtect の追加を有効にします。
ENABLE_SYSTRAY_ICON	boolean	true	Windows のシステムトレイへの StellarProtect アイコンの追加を有効にします。
ENABLE_TRUSTED_ICS_CERT	boolean	true	インストーラがインストール中に ICS コードサイニング証明書をインストールすることを許可します。
INSTALL_PATH	string	空の文字列→初期設定のインストールパス C:\Program Files\TXOne (初期設定のインストールパスはインストーラで指定済み)	StellarProtect のインストールパス。

パラメータ	タイプ	初期設定値	説明
PASSWORD	string	空の文字列	管理者のパスワード。 パスワードは、アンインストール、コマンドライン、サポートツールなどの特定の機能で必要になります。
PRESCAN_ACTION	int	1	0: なし 1: 隔離
PRESCAN_CPU_MODE	int	0	0: 標準 (シングルスレッド検索) 1: 高 (マルチスレッド検索)
DEFAULT_PROXY_SERVER_HOST	string	empty string	イントラネットプロキシサーバの FQDN、ホスト名、または IP アドレス
DEFAULT_PROXY_SERVER_PASSWORD	string	empty string	イントラネットプロキシサーバのパスワード。プロキシサーバがユーザ名とパスワードで認証するように設定されている場合にのみ必要です。
DEFAULT_PROXY_SERVER_PORT	int	-1	イントラネットプロキシサーバのポート番号
DEFAULT_PROXY_SERVER_USERNAME	string	空の文字列	イントラネットプロキシサーバのユーザ名。プロキシサーバがユーザ名とパスワードで認証するように設定されている場合にのみ必要です。
SERVER_CERT	string	server.crt	StellarOne と通信するための証明書のファイル名

パラメータ	タイプ	初期設定値	説明
SERVER_HOST	string	空の文字列	StellarOne のホスト名または IP
LISTEN_PORT	int	14336	StellarOne のクライアント待機ポート
SERVER_PORT	int	9443	クライアントに接続するための StellarOne のポート
BYPASS_WINDEFEND_CHECK	boolean	false	Windows Defender のチェックのバイパスのステータス

注意

1. ENABLE_PRESCAN が false に設定されている場合、ENABLE_LOCKDOWN_AL_BUILDING と ENABLE_LOCKDOWN_DETECTION は自動的に false に設定されます。
2. BYPASS_WINDEFEND_CHECK は Setup.yaml の隠しパラメータで、StellarProtect のインストールにおいて Windows Defender を無効にする必要がある Windows 7 および Windows Server 2016 以降のプラットフォーム用に設計されたものです。パラメータの値を true に設定すると、Windows Defender を無効にせずに StellarProtect をインストールするため、Windows Defender のチェックがバイパスされます。使用法については、以降の説明を参照してください。

StellarProtect エージェントのサイレントインストール

手順

1. アクティベーションコードとパスワードを入力し、設定ファイルで `enable_silent_install` の値を `true` に変更してサイレントインストールを有効にします。StellarOne を使用してエージェントを管理する場合は、server セクションのホストの値にサーバの IP アドレスを設定します。

   サイレントインストールの設定ファイルの例については、次を参照してください。

```
client:
    import_source: C:\txsp_config
install:
    activation_code:  TE-XXXXX-SAMPL-EXXXX-CODES-XXXXX-TXONESP
    asset_description: This is a machine
    asset_location: Factory1 North Area
    asset_model: ABB-1X2Y
    asset_vendor: ABB
    enable_desktop_icon: true
    enable_lockdown_al_building: true
    enable_lockdown_detection: true
    enable_prescan: true
    enable_silent_install: true
    enable_start_menu: true
    enable_systray_icon: true
    enable_trusted_ics_cert: true
    install_location: C:\test
    password: 11111111
prescan:
    action:  1
    cpu_usage_mode: 0
```

```
proxy:
    default:
        host:
        password:
        port:
        username:
server:
    cert: server.crt
    host: 10.1.195.100
    listen:  14336
    port:  9443
```

注意

(オプション) install セクションの下に行を挿入し、次のように入力します。

```
bypass_windefend_check: true
```

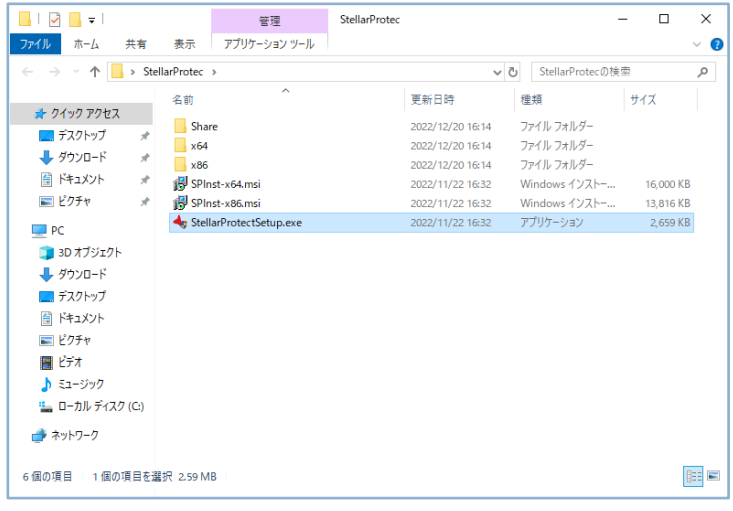
Windows Defender を無効にせずに StellarProtect をインストールするため、Windows Defender のチェックがバイパスされます。

2. インストーラ `StellarProtectSetup.exe` をダブルクリックします。

注意

サイレントインストールを開始するには、次の 2 つの方法があります。

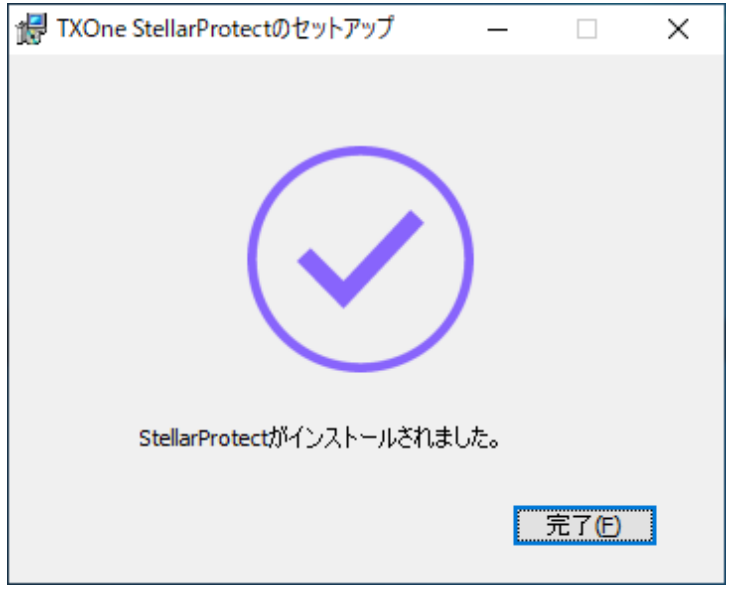
- GUI を使用してサイレントインストールを実行するには、インストーラ `StellarProtectSetup.exe` をダブルクリックします。



- GUI なしでサイレントインストールを実行するには、手順 2 で実行可能ファイルをダブルクリックする代わりに、コマンドプロンプトを使用し、引数-s を指定して `StellarProtectSetup.exe` を実行します。この方法では、次の手順に示すポップアップ画面が表示されないことに注意してください。インストールに関連する情報を表示するには、**C:\Windows\Temp\StellarProtect** の下のログファイルを確認します。

```
C:\package>StellarProtectSetup.exe -s
```

3. インストールが完了すると、このメッセージボックスが表示されます。



4. StellarProtect を実行し、設定したパスワードを使用してログインします。
5. StellarProtect にログインすると、[概要] 画面が表示されます。

インストール設定の暗号化 (Setup.yaml)

StellarProtect では、機密データの漏えいを防ぐために、インストール用の設定ファイルを暗号化できます。暗号化された設定ファイルの名前は Setup.bin に固定されています。

手順

1. 33 ページの「サイレントインストール」の説明に従って、Setup.yaml を準備します。
2. コマンドプロンプトで `StellarProtectSetup.exe -e <設定ファイル>` を実行して、`Setup.yaml` を暗号化します。パラメータ`-e` は、設定ファイルを暗号化し、作業ディレクトリに `Setup.bin` ファイルを生成することを指定します。
3. `Setup.bin` ファイルが生成されたら、インストーラパッケージに追加します。
4. 暗号化された設定でインストールを実行できるようになります。

第 3 章

StellarProtect のアンインストール

注意

エンドポイントから StellarProtect をアンインストールするには、StellarProtect の管理者パスワードが必要です。

重要

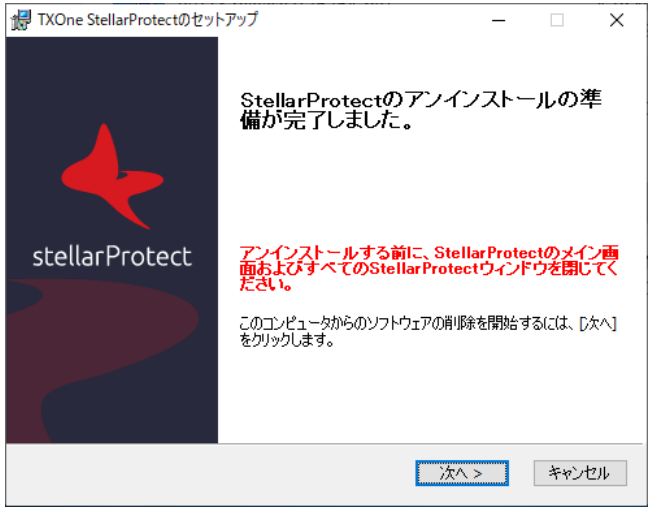
StellarProtect のメイン画面が開いていないことを確認してください。

手順

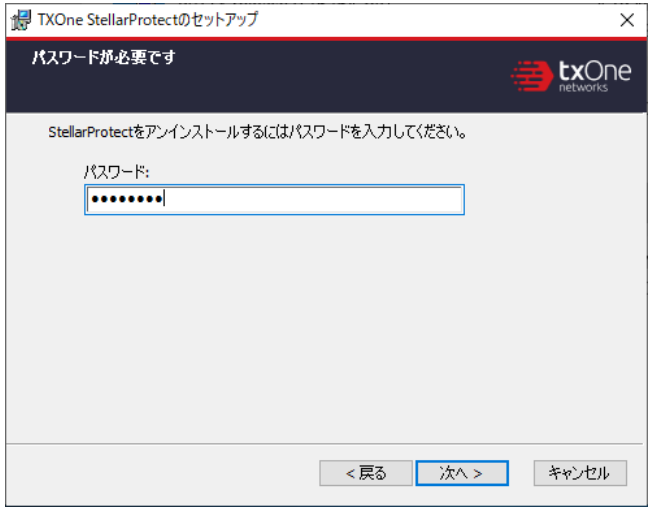
1. StellarProtect エージェントがインストールされたエンドポイントで、StellarProtect のセットアップを起動します。
2. お使いの OS に応じた手順を実行します。

OS	手順
• Windows 10 Enterprise • Windows 10 IoT Enterprise • Windows 10 Professional • Windows 10 Fall Creators Update (Redstone 3) • Windows 10 April 2018 Update (Redstone 4) • Windows 10 October 2018 Update (Redstone 5) • Windows 11 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 [StellarProtect] をクリックします。 e. [アンインストール] をクリックします。
• Windows Server 2022 • Windows Server 2016 • Windows Server 2012 • Windows Storage Server 2016 • Windows 8 • Windows 7	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] をダブルクリックします。

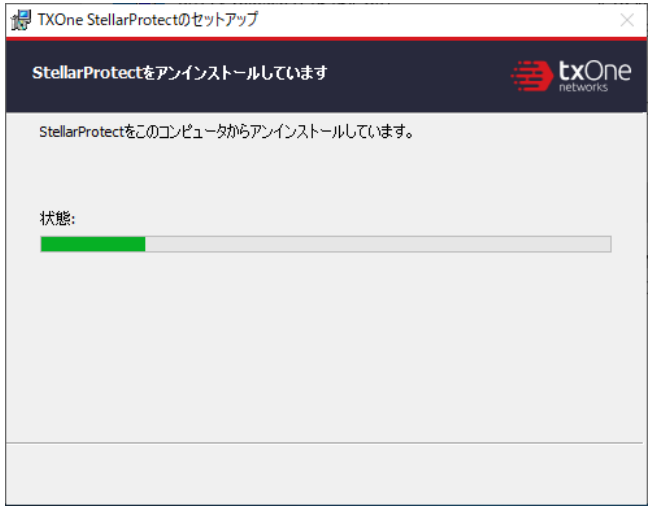
3. StellarProtect のセットアップが開いたら、[次へ] をクリックします。



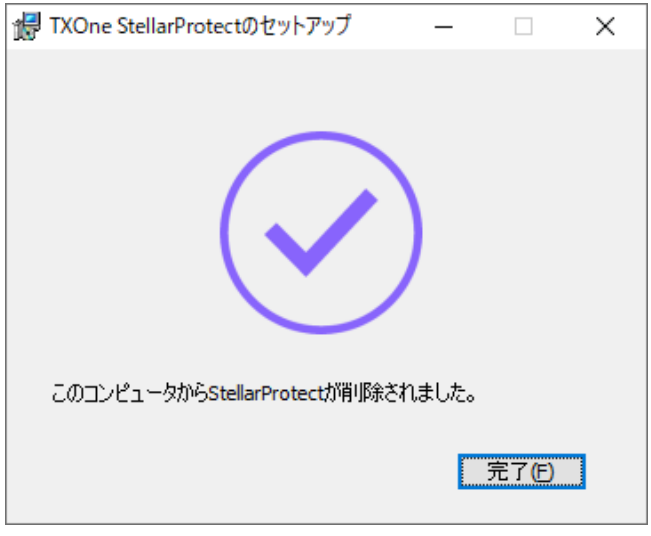
4. StellarProtect の管理者パスワードを入力して、[次へ] をクリックします。



5. [OK] をクリックする前に、StellarProtect のメイン画面が完全に閉じていることを確認します。



6. StellarProtect 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。



重要

Windows 7 および Windows Server 2016 以降のプラットフォームに StellarProtect をインストールするには、先に Windows Defender を無効にする必要があります。StellarProtect をアンインストールしたら、セキュリティ上の理由から、Windows Defender を手動で有効にすることをお勧めします。

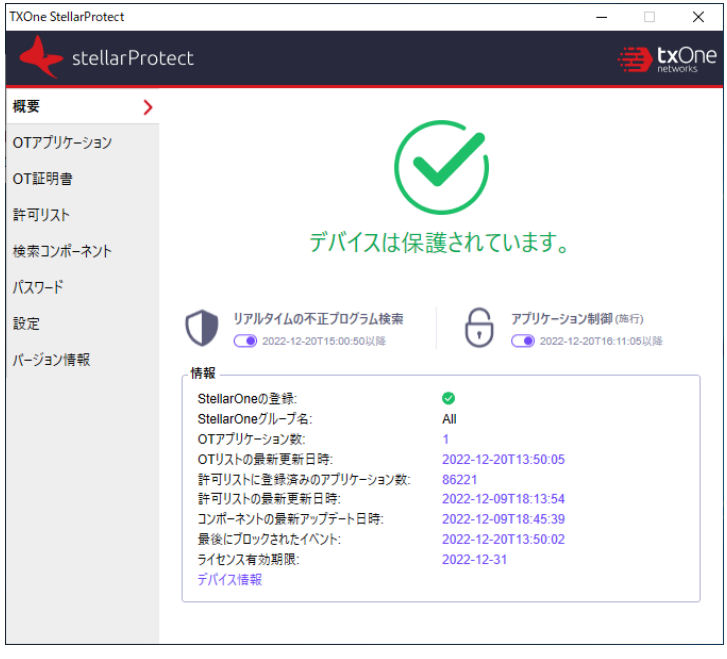
第 4 章

エージェントのメイン画面の使用

この章では、エンドポイントでエージェントのメイン画面を使用して TXOne StellarProtect のさまざまな機能を操作する方法について説明します。

この章の内容は次のとおりです。

概要



[概要] には、StellarProtect システムの現在のステータスの説明が表示されます。
緑のチェックマークはエンドポイントがリアルタイムの不正プログラム検索またはアプリケーション制御あるいはその両方により保護されていることを示し、赤いバツ印はエンドポイントが危険にさらされていることを示します。

Stellar Standard ライセンスの StellarProtect エージェントでは、緑のチェックマークまたは赤いバツ印の下には、左側に盾の形のアイコンとエンドポイントが StellarProtect のリアルタイムの不正プログラム検索で現在保護されているかどうかを示すスイッチが表示され、右側に錠前の形のアイコンとアプリケーション制御機能が有効になっているかどうかを示すスイッチが表示されます。

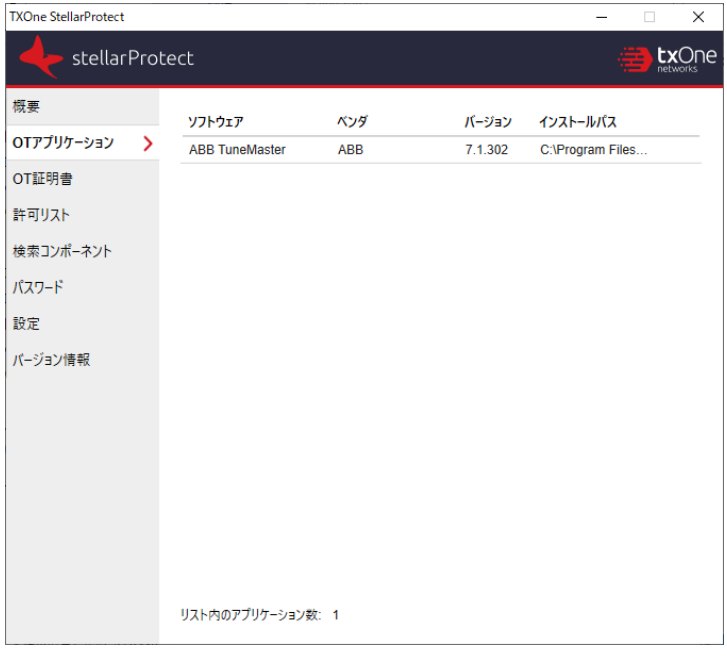
Stellar Lite ライセンスの StellarProtect エージェントでは、緑のチェックマークまたは赤いバツ印の下には、盾の形のアイコンとエンドポイントが StellarProtect のリアルタイムの不正プログラム検索で現在保護されているかどうかを示すスイッチが表示されます。

Stellar Lockdown 無期限版の StellarProtect エージェントでは、緑のチェックマークまたは赤いバツ印の下には、錠前の形のアイコンとアプリケーション制御機能が有効になっているかどうかを示すスイッチが表示されます。

エンドポイント保護に関する、以下の現在の情報が表示されます。

- **StellarOne の登録:** 緑のチェックマークは StellarProtect エージェントが指定したグループに StellarOne の管理サーバ画面を介して登録されたことを示し、赤いバツ印は特定グループへの登録に失敗したことを示します。
- **StellarOne グループ名:** エージェントが属するグループ名を示します。グループ名の上にマウスを重ねると、グループ名に関する情報、グループ ID、およびポリシーバージョンが表示されます。
- **OT アプリケーション数:** エンドポイント上にある OT アプリケーションの数を示します。
- **OT リストの最新更新日時:** このエンドポイント上で OT アプリケーションリストが最後に更新された日時を示します。
- **許可リストに登録済みのアプリケーション数:** このエンドポイント上で許可リストに登録されているアプリケーションの数を示します。
- **許可リストの最新更新日時:** 許可リストが最後に更新された日時を示します。
- **コンポーネントの最新アップデート日時:** コンポーネントが最後にアップデートされた日時を示します。
- **最後にブロックされたイベント:** このリンクをクリックすると、最近ブロックされたイベント 1000 件が表示されます。
- **ライセンス有効期限:** StellarProtect の現在のライセンスの有効期限を示します。
- **デバイス情報:** このリンクをクリックすると、ベンダ、モデル、場所、コメントなどのエンドポイントのデバイス情報が表示されます。

OT アプリケーション

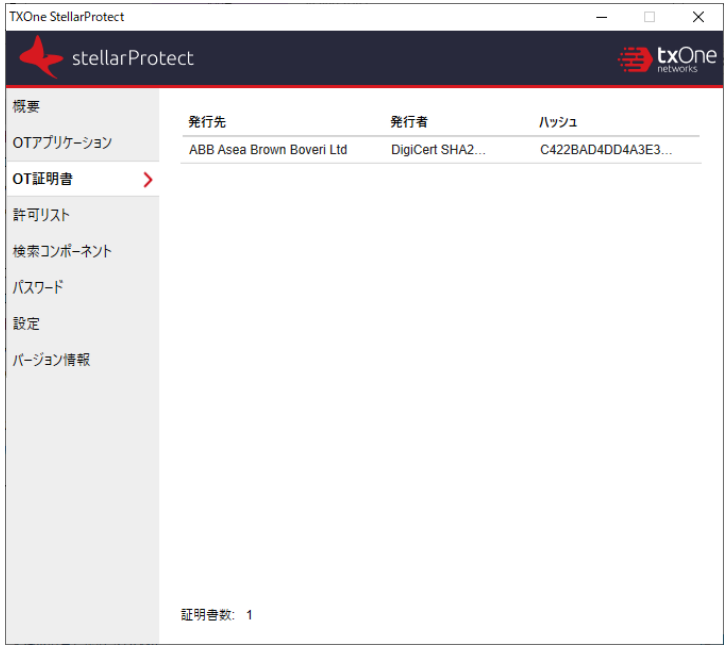


この機能は、このエンドポイント上で StellarProtect により認識されている各 OT/ICS アプリケーションシステムのソフトウェア名、ベンダ名、製品バージョン、およびインストールパスを表示します。

StellarProtect が認識する OT/ICS アプリケーションシステムの数は、OT/ICS アプリケーションリストのアップデートとともに増え続けます。このリストは、OT/ICS の製品分析に基づき、TXOne の研究所によって維持されています。

デバイス管理のため、この情報は StellarOne のバックエンドと同期されます。

OT 証明書

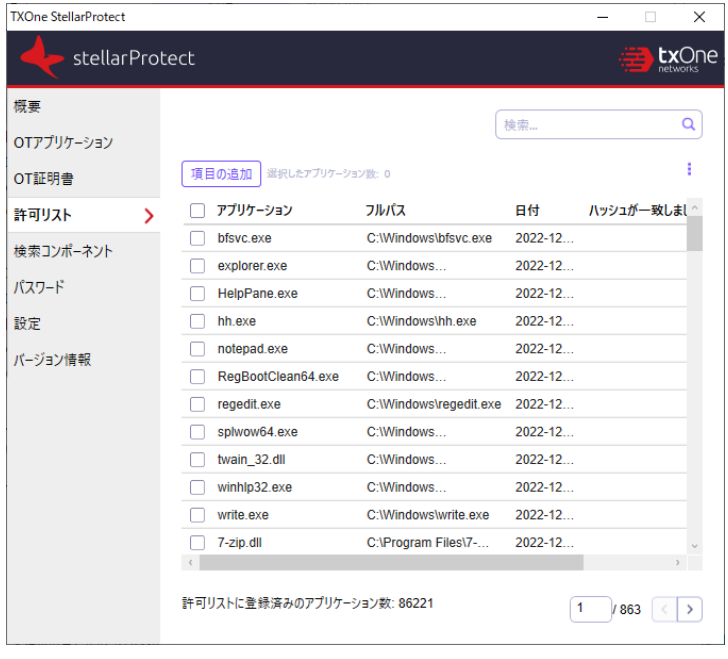


デジタル署名は現在最も安全なソフトウェア製品識別技術です。この技術により、署名されたソフトウェアコンポーネントが不正に修正されていないことを確認し、ソフトウェアが正規メーカーにより提供されたものであることを識別できます。

StellarProtect が認識する OT/ICS 証明書の数は、OT/ICS アプリケーションリストのアップデートとともに増え続けます。このリストは、OT/ICS の製品分析に基づき、TXOne の研究所によって作成されています。

管理のため、この情報は StellarOne のバックエンドと同期されます。

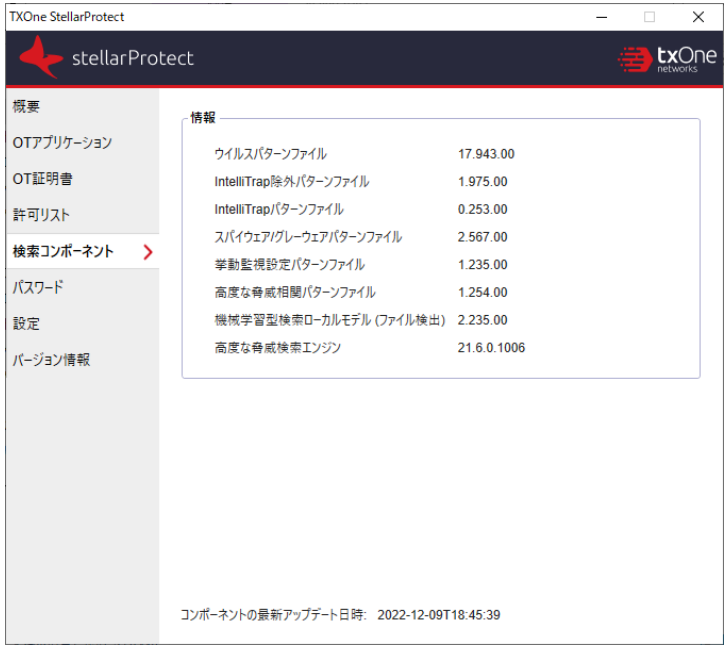
許可リスト



事前検索で検出されたアプリケーションは許可リストに追加されます。この画面でアプリケーションの追加や検索を行えます。[⋮]のドロップダウンメニューをクリックして、信頼するハッシュをインポートまたはエクスポートすることもできます。

検索コンポーネント

すべての重要な検索エンジンとパターンファイルが、StellarProtect で使用されているバージョンとともに表示されます。

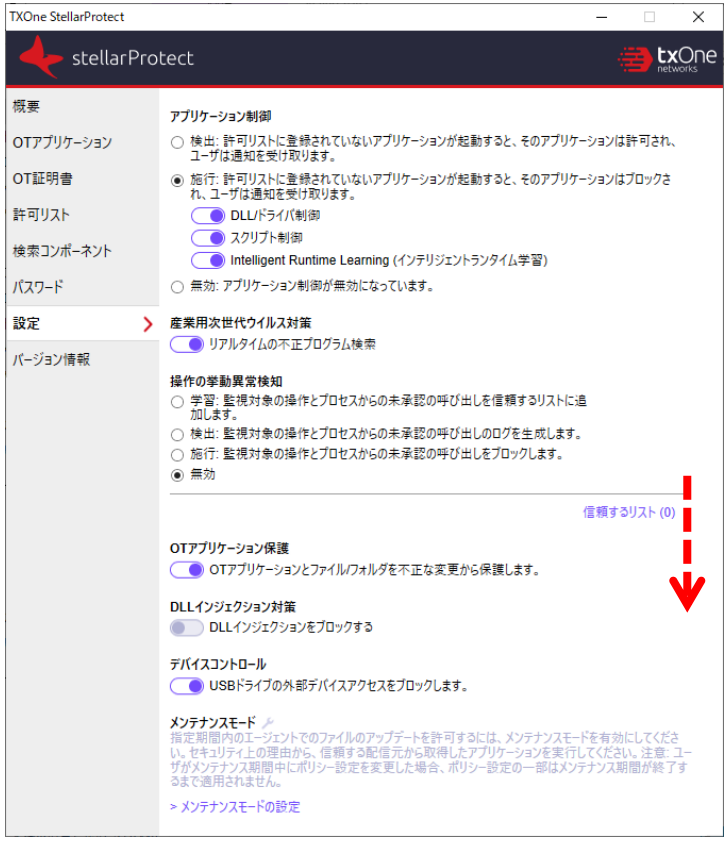


パスワード

StellarProtect の管理者パスワードを変更する機能です。パスワードを変更するには、現在のパスワードを正しく入力し、新しいパスワードを 2 回入力し、新しいパスワードの長さが条件を満たしていることを確認して、[保存] をクリックする必要があります。

設定

主に StellarProtect の設定が表示されます。7 つの主要な保護機能については、この後、詳しく説明します。各機能にはオンとオフを切り替えるためのスイッチがあります。



アプリケーション制御

この機能は、アプリケーションリストで定義されているファイルを制御することにより、不正プログラムによる攻撃を阻止し、保護レベルを引き上げます。検出、施行、および無効の 3 つのモードから選択できます。

検出: 許可リストに登録されていないアプリケーションの実行は許可され、ユーザは通知を受け取ります。

施行: 許可リストに登録されていないアプリケーションの実行はブロックされ、ユーザは通知を受け取ります。

[検出] または [施行] 機能を有効にすると、さらに次の 3 つの保護オプションが使用可能になります。

1. DLL/ドライバ制御: DLL/ドライバファイルの制御を行います。DLL/ドライバ制御が有効な場合は、許可リストに含まれる DLL、ドライバファイルのみがロードされます。
2. スクリプト制御: スクリプトファイルの制御を行います。スクリプト制御が有効な場合は、許可リストに含まれるスクリプトファイルのみがインタープリタアプリケーションに読み込まれます。
3. Intelligent Runtime Learning (インテリジェントランタイム学習): 操作が途切れないように、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可能ファイルを許可します。

無効: ユーザが必要としている場合はアプリケーション制御モードを無効にすることもできますが、この機能は有効にすることをお勧めします。

産業グレード次世代ウィルス対策

産業グレード次世代ウィルス対策 (リアルタイムの不正プログラム検索) は、StellarProtect の中核となる保護機能です。署名ベースと AI ベースのウイルス対策ソフトウェアを統合することによって、あらゆるファイルやプロセスのアクティビティのリアルタイム検索を実行します。

StellarProtect には OT/ICS アプリケーションシステムの認識技術が組み込まれており、誤警報の発生を大幅に削減できます。

この機能は、スイッチをクリックしてオンとオフを切り替えられます。

オペレーション振る舞い検知

異常な操作は、高度な攻撃 (ファイルレス攻撃など) により引き起こされている可能性があります。StellarProtect では、このような脅威の挙動を検知し、将来の分析のためにログに記録できます。

この機能により、主に `wscript.exe`、`cscript.exe`、`mshta.exe`、`powershell.exe`、および `psexec.exe` などのリスクの高い特定のアプリケーションを監視し、正規のプログラムの悪用を阻止します。StellarOne の管理サーバ画面で、その他の監視対象プロセスを追加することもできます。

この機能には次の 4 つのモードがあります。

- **学習モード**

  未承認のプログラムの呼び出しを監視し、それらを信頼するリストに追加して、OT/ICS関連プログラムの呼び出しの挙動について詳しく学習します。

- **検出モード**

  未承認のプログラムの呼び出しを監視し、それらを将来の分析のためにログに記録します。

- **施行モード**

  未承認のプログラムの呼び出しを監視し、それらをブロックしてエンドポイントを保護します。

- **無効モード**

  保護がオフになります。

検出または施行モードでは、[アグレッシブモード] オプションを選択して、ウイルス対策セキュリティをさらに強化することもできます。この機能は、プロセスパラメータを認識することで保護を有効にします。

監視タスクにパラメータの識別を追加することにより、操作プロセスと、それに付随する監視対象パラメータの変更をチェックすることができます。

OT アプリケーション保護

OT/ICS アプリケーションの Patch や HotFix により、ウイルス対策で誤警報が発生し、ブロックされる可能性があります。StellarProtect は、OT/ICS アプリケーションリストの技術を使用して OT/ICS アプリケーションに対する正規のアップデートを確認し、ブロックやアラートを発生させることなく、認識された OT/ICS アプリケーションを最新の状態に保つことができます。

この機能は、OT/ICS アプリケーションテクノロジーを識別し、OT/ICS アプリケーションシステムのアップデートに合致した保護を提供することにより StellarProtect をサポートします。

[OT アプリケーションとファイル/フォルダを不正な変更から保護します。] を有効にすると、ICS アプリケーションの実行可能ファイルはユーザの指定なしに自動的に保護されるようになります。一方、StellarOne の管理サーバ画面でユーザにより指定されたファイルやフォルダは、StellarProtect により監視および保護されます。

DLL インジェクション対策

DLL インジェクションは OT/ICS 分野におけるリスクの高い攻撃であり、この機能を有効にすることで、この種の攻撃を防ぐことができます。

注意

DLL インジェクション対策は、32 ビットの Windows OS でのみ有効にできます。

デバイスコントロール

デバイスコントロールは、許可された USB デバイスのみを StellarProtect で保護されたエンドポイントで使用できるよう、外部 USB ストレージデバイスを制御する StellarProtect の機能です。

この機能は主に、外部 USB ストレージデバイスの識別とそれに対する保護を提供します。USB デバイスのベンダ ID (VID)、製品 ID (PID)、およびシリアル番号 (SN) を使用して、デバイスが信頼する USB ストレージデバイスであるかどうかを判断します。

デバイスコントロールには、管理者による認証後に USB ストレージへのアクセスを承認するための、1 回限りの許可機能があります。未許可の USB ストレージデバイスがエンドポイントに初め

て挿入されると、ユーザは管理者パスワードを入力するように求められます。ユーザの利便性を高めるために、これは 1 回限りの許可機能として設定されています。

その間に、StellarProtect はブロックされたイベントの通知を StellarOne に送信し、管理者は StellarOne の管理サーバ画面でブロックされたイベントを確認し、ブロックを継続するのか、アクセスを承認するのかを決定できます。

デバイスコントロールの使用例を次に示します。

1. USB を挿入します。
2. デバイスコントロールが有効で、デバイスが信頼されていない場合、USB はブロックされます。
3. 管理者のパスワードを入力するように求めるポップアップメッセージが表示されます。
4. 取り外すまで、この USB デバイスへのアクセスが許可されます。

この機能は、スイッチをクリックしてオンとオフを切り替えられます。

メンテナンスモード

エンドポイントでファイルのアップデートを実行するには、メンテナンスモードを設定します。これにより、StellarProtect がすべてのファイルの実行を許可し、作成、実行、または変更されたすべてのファイルを許可リストに追加する期間を定義できます。

メンテナンス期間中は、一貫したセキュリティを維持するため、リアルタイムのウイルス検索を実行しながら新しく追加されたすべてのファイルをアップデートできます。(Stellar Standard / Standard Lite のみ)
これにより、新しく追加されたアプリケーションが StellarProtect によって認識され、保護下で実行されるようになります。

注意

メンテナンス期間中にアプリケーション制御、OT アプリケーション保護、リアルタイムの不正プログラム検索 (産業グレード次世代ウィルス対策) のポリシー設定が変更された場合、そのポリシー設定はメンテナンス期間が終了するまで適用されません。

バージョン情報

StellarProtect の製品情報、バージョンとビルド番号、サードパーティライセンス情報などが表示されます。

プロキシ

StellarProtect は、StellarOne との通信および検索コンポーネントのアップデートにプロキシを使用できます。

プロキシは、インストール前に `Setup.yaml` を使用して、またインストール後にコマンドラインを使用して設定できます。

- インストール前に `Setup.yaml` を使用してプロキシを設定する方法については、33 ページの「サイレントインストールの設定」を参照してください。
- インストール後にコマンドラインを使用してプロキシを設定する方法については、66 ページの「全コマンドのリスト」を参照してください。

第 5 章

エージェントのコマンドラインの使用

この章では、コマンドラインを使用した TXOne StellarProtect の設定と使用方法について説明します。

この章の内容は次のとおりです。

コマンドラインでの OPCmd の使用

管理者は、**OPCmd.exe** プログラムを使用して、コマンドラインから直接 TXOne StellarProtect を操作できます。

手順

1. Windows の管理者権限を使用して、コマンドプロンプトウィンドウを開きます。
2. **cd** コマンドを使用して、TXOne StellarProtect のインストールフォルダに移動します。

   たとえば、次のコマンドを入力すると初期設定の場所に移動します。

   ```
   cd /d "c:\Program Files\TXOne\StellarProtect\"
   ```
3. **OPCmd.exe** と入力します。

概要

このプログラムでは、POSIX スタイルのコマンドラインを使用できます。一般的な使用法は次のとおりです。

```
C:> opcmd.exe [グローバルオプション] [コマンド [オプション]]
```

グローバルオプションはすべてのコマンドに影響するオプションであり、コマンドの前に指定する必要があります。コマンドは、1 つまたは複数の単語と、それに続くそのコマンド固有のオプションから構成されます。オプションに引数が必要な場合は、次のいずれかの構文で指定できます。

オプション

```
--option=<引数>
```

ロング形式のオプションと引数を等号で区切ります。

```
-o<引数>
```

引数をオプション文字の直後に指定します。

`-o <引数>`

引数の指定が任意ではない場合は、オプションと引数をスペースで区切ることもできます。

重要

グローバルオプションとコマンド固有のオプションを含め、すべてのオプションの指定は任意です。以降に説明するコマンドで引数が必須と記載されている場合は、オプションの指定時に引数が必要ということを意味しています。

ショート形式のオプションを使用する場合、引数を指定するオプションが最後にあれば、複数のオプション文字を 1 つの単語として組み合わせることができます。たとえば、次のコマンドはすべて同じ内容を指しています。

- `opcmd.exe foo -a -b 15 -c`
- `opcmd.exe foo -ac -b15`
- `opcmd.exe foo -cab 15`
- `opcmd.exe foo -acb15`

グローバルオプション

- グローバルオプション: `-h`、`--help`

  説明: 単独で使用する場合、コマンドラインの使用方法についての概要が表示されます。コマンドと一緒に使用する場合、そのコマンドに対するヘルプテキストが表示されます。

  引数: なし

- グローバルオプション: `-p`、`--password [<パスワード>]`

  説明: 保護コマンドを実行するための管理者パスワードを指定します。-pオプションは保護コマンドについては必須です。このオプションを使用して管理者パスワードを指定しないと、保護コマンドを実行する前にパスワードの入力を求められ、パスワードが正しくない場合はコマンドが実行されません。バッチファイルから保護コマンドを実行する必要がある場合は、-pを使用してパスワードを指定し、権限のあるユーザのみがバッチファイルを読めるようにします。

> **注意**
>
> 管理者パスワードが誤って漏えいすることを防ぐには、シェル (cmd.exe) によってパスワードがコマンド履歴に記録されないように、引数なしで-p を使用します。

引数: 任意。プレーンテキストのパスワード。

- グローバルオプション: `-v`、`--version`

  説明: コマンドラインプログラムのバージョンを表示します。

  引数: なし

全コマンドのリスト

コマンド	説明	オプション
`opcmd.exe about components`	GUIプログラムでコンポーネントのバージョンを確認するか、このコマンドを使用してYAML形式のリストを取得できます。	なし
`opcmd.exe -p appinv make`	予約したメンテナンスモードが終了すると、インストールされている OT/ICS アプリケーションが StellarProtect サービスにより再検出されます。また、このコマンドを使用していつでも手動で検出を実行できます。	なし
`opcmd.exe appinv list`	GUI プログラムで検出された OT/ICS アプリケーションのリストを確認するか、このコマンドを使用して YAML 形式のリストを取得できます。	なし

コマンド	説明	オプション
opcmd.exe -p config decrypt [-i INPUTFILE] [-o OUTPUT-FILE]	暗号化された設定ファイルを復号し、復号されたプレーンテキストを出力します。 このコマンドのデータセキュリティは、設定ファイルの保護用に設計されていることに注意してください。個人的なプライバシーデータの保護にこのコマンドを使用しないでください。	-i、--input 入力ファイル: 必須の引数。入力ファイルのファイル名を指定します。省略した場合、標準入力から読み込みます。 -o、--output 出力ファイル: 必須の引数。出力ファイルのファイル名を指定します。省略した場合、標準出力に書き出します。
opcmd.exe -p config encrypt [-i INPUTFILE] [-o OUTPUT-FILE]	プレーンテキストの設定ファイルを暗号化し、暗号化されたデータを出力します。 このコマンドのデータセキュリティは、設定ファイルの保護用に設計されていることに注意してください。個人的なプライバシーデータの保護にこのコマンドを使用しないでください。	-i、--input 入力ファイル: 必須の引数。入力ファイルのファイル名を指定します。ファイル名を省略した場合、標準入力から読み込みます。 -o、--output 出力ファイル: 必須の引数。出力ファイルのファイル名を指定します。省略した場合、標準出力に書き出します。
opcmd.exe -p config export OUTPUT-FOLDER	製品設定を指定したフォルダにエクスポートします。	なし
opcmd.exe -p config import INPUT-FOLDER	製品設定を指定したフォルダからインポートします。	-n、--no_ptn パターンファイルをインポートしません。
opcmd.exe -p dip disable	DLL インジェクション対策機能を無効にします。	なし
opcmd.exe -p dip enable	DLL インジェクション対策機能を有効にします。	なし
opcmd.exe -p lock appinv disable	OT/ICS アプリケーションリストの保護を無効にします。	なし
opcmd.exe -p lock appinv enable	OT/ICS アプリケーションリストの保護を有効にします。	なし

コマンド	説明	オプション
opcmd.exe -p lock disable [-d DURATION] [-s START-TIME]	保護対象ファイルでファイルを変更できるように、変更制御モジュールを無効にします。ファイルの変更および自動的な保護の有効化が可能なメンテナンスモードを予約する期間と開始時刻も指定できます。 -d を指定しない場合、変更制御モジュールは有効にするまで無効となります。 -s を指定しない場合、変更制御モジュールはただちに無効になります。一度に予約できるのは 1 つのメンテナンスモードのみであり、コマンドラインまたはポリシー設定からの新しい設定によって常に以前の設定が上書きされます。	-d、--duration 期間: 必須の引数。メンテナンスモードの期間を指定します。この期間の経過後、変更制御モジュールは現在の設定に戻されます。期間は時間、分、またはその両方で指定できます。(例: -d 30m、-d 2h、-d 2h30m) 期間を分のみで指定する場合、'm' は省略できます。 -s、--start 開始時刻: 必須の引数。メンテナンスモードの開始時刻を指定します。開始時刻は、タイムゾーンなしの ISO8601 形式で指定します。(例: -s 2021-04-14T18:00:00)
opcmd.exe -p lockdown approvedlist info	アプリケーション制御の許可リストの情報を表示します。	なし
opcmd.exe -p lockdown approvedlist init [--overwrite]	アプリケーション制御の許可リストを初期化します。	-o、--overwrite: 既存のアプリケーション制御の許可リストを上書きします。 -o を指定しない場合、検出されたアプリケーションは、既存のアプリケーション制御の許可リストに追加されます。
opcmd.exe -p lockdown approvedlist add -p PATH [--recursive]	指定したファイルをアプリケーション制御の許可リストに追加します。	-p、--path パス: 指定したファイルをアプリケーション制御の許可リストに追加します。 -r、--recursive: 指定したフォルダおよび関連するサブフォルダを含めます。

コマンド	説明	オプション
`opcmd.exe -p lockdown enable -m MODE`	アプリケーション制御を有効にします。	`-m`、`--mode` モード: 有効モード (detect、enforce) を指定します。
`opcmd.exe -p lockdown disable`	アプリケーション制御を無効にします。	なし
`opcmd.exe -p lockdown exceptionpath -t TYPE -p PATH (--add|--remove)`	アプリケーション制御の除外パスを追加または削除します。	`-t`、`--type` タイプ: 除外パスのタイプ (file、folder、folder_and_subfolder、ecmascript_regexp) を指定します。 `-p`、`--path` パス: 除外パスまたは正規表現を指定します。
`opcmd.exe -p lockdown info`	アプリケーション制御の情報を表示します。	なし
`opcmd.exe -p lockdown script info`	アプリケーション制御のすべてのスクリプトルールを表示します。	なし
`opcmd.exe -p lockdown script add -e EXTENSION -p INTERPRETER [-p INTERPRETER2] ...`	指定したスクリプト拡張と、スクリプトの実行に必要なインタープリタを追加します。	`-e`、`--ext` 拡張: スクリプト拡張を指定します。 `-p`、`--proc` インタープリタ: スクリプトインタープリタの名前を指定します。
`opcmd.exe -p lockdown script remove -e EXTENSION [-p INTERPRETER] ...`	指定したスクリプト拡張と、スクリプトの実行に必要なインタープリタを削除します。	`-e`、`--ext` 拡張: スクリプト拡張を指定します。 `-p`、`--proc` インタープリタ: スクリプトインタープリタの名前を指定します。
`opcmd.exe -p lockdown subfeature -f SUBFEATURE (--enable|--disable)`	アプリケーション制御のサブ機能を切り替えます。	`-f`、`--feature` サブ機能: サブ機能を指定します (dll_driver、script、intelligent_runtime_learning)。
`opcmd.exe -p lockdown trustedhash -h HASH (--add|--remove)`	アプリケーション制御の信頼するハッシュを追加または削除します。	`-h`、`--hash` ハッシュ: 信頼するハッシュを指定します。

コマンド	説明	オプション
		SHA-256 のみサポートされています。
`opcmd.exe -p lock enable`	保護対象ファイルでファイルを変更できないように、変更制御モジュールを有効にします。予約したメンテナンスモードにより変更制御モジュールが無効になっている場合、このコマンドによってメンテナンスモードがただちに終了します。	なし
`opcmd.exe -p maintenance start`	メンテナンスモードを開始または予約します。ファイルの変更および自動的な保護の復元が可能なメンテナンスモードを予約する期間と開始時刻を指定できます。	`-d、--duration` 期間: メンテナンスモードの期間を指定します。分、時間、またはその両方で指定できます (例: `-d30`、`-d2h`、`-d2h30m`)。期間を分のみで指定する場合、'm' は省略できます。 `-s、--start` 開始時刻: メンテナンスモードの開始時刻を指定します。開始時刻は、タイムゾーンなしの ISO8601 形式で指定します (例: `-s 2021-04-14T18:00:00`)。 `-r、--activate-rts` リアルタイム検索の有効化: メンテナンスモード中のリアルタイム検索を有効にします。
`opcmd.exe -p maintenance stop`	メンテナンスモードの実行を停止するか、予約メンテナンスモードをキャンセルします。	なし
`opcmd.exe -p maintenance info`	メンテナンスモードの情報を表示します。	なし

コマンド	説明	オプション
opcmd.exe -p oad disable	オペレーション振る舞い検知を無効にします。	なし
opcmd.exe -p oad enable -m MODE [-l LEVEL]	オペレーション振る舞い検知を有効にします。	-m、--mode モード：必須の引数。特定のモード (learn、detect、enforce) でのオペレーション振る舞い検知を有効にします。 -l、--level レベル：必須の引数。検索レベルを normal または aggressive に設定します。
opcmd.exe -p oad info	オペレーション振る舞い検知の情報を表示します。	なし
opcmd.exe -p oad remove -i ID	オペレーション振る舞い検知から許可済みの操作を削除します。	-i、--id ID：必須の引数。整数の操作 ID。
opcmd.exe password	管理者がコマンドラインから管理者のパスワードを変更することを可能にします。新しいパスワードを設定するには、現在のパスワードを入力する必要があります。	なし
opcmd.exe -p proxy get	プロキシサーバ設定を表示します。	なし
opcmd.exe -p proxy set [-h HOST -p PORT [-u USERNAME] [-P PASSWORD]]	プロキシサーバ設定を指定します。 プロキシの使用を無効にするには、オプションを指定せずにこのコマンドを使用します。	-h、--host ホスト：必須の引数。プロキシサーバの FQDN、ホスト名、または IP アドレスを指定します。 -p、--port ポート：必須の引数。プロキシサーバのポート番号を指定します。 -u、--username ユーザ名：必須の引数。プロキシサーバ

コマンド	説明	オプション
		認証のユーザ名を指定します。 `-P、--password` パスワード：必須の引数。プロキシサーバ認証のパスワードを指定します。
`opcmd.exe -p regexp test -s STRING -p PATTERN`	正規表現が文字列と一致するかどうかを確認します。	なし
`opcmd.exe -p scan-task -s START-TIME -daily --weekly --monthly`	指定した開始時刻で、繰り返し検索タスクを予約します。	`-s、--start` 開始時刻：必須の引数。予約検索の開始時刻を指定します。開始時刻は、タイムゾーンなしの ISO8601 形式で指定します。（例：`-s 2021-04-14T18:00:00`） `--daily`：予約検索を毎日実行することを指定します。 `--weekly`：予約検索を毎週実行することを指定します。 `--monthly`：予約検索を毎月実行することを指定します。 `--remove`：予約検索を削除します。
`opcmd.exe -p service start`	インストール後、システムの電源がオンになると、StellarProtect サービスは自動的に起動します。StellarProtect サービスが何らかの理由で停止した場合は、このコマンドを使用して手動で StellarProtect サービスを起動できます。	なし
`opcmd.exe -p service stop`	システムの電源がオフになるまで StellarProtect サービスを	なし

コマンド	説明	オプション
	停止します。StellarProtect サービスを停止する必要がある場合は、このコマンドを使用して手動で StellarProtect サービスを停止できます。	
`opcmd.exe update [-s SOURCE]`	製品コンポーネントをアップデートします。	`-s、--source`: 必須の引数。SOURCE アップデート元の URL を指定します。例: `-s http://tmut.contoso.com/ iau_server`
`opcmd.exe -p update stop`	現在実行中のアップデートを停止します。	なし
`opcmd.exe -p usb add [- v VID -p PID -s SN] [- o]`	信頼する USB デバイスを追加します。	`-v、--vid VID`: 必須の引数。ベンダ ID を 16 進文字列で指定します。 `-p、--pid PID`: 必須の引数。製品 ID を 16 進文字列で指定します。 `-s --sn SN`: 必須の引数。シリアル番号を指定します。 `-o、--onetime`: USB デバイスに対する 1 回限りのアクセスを許可します。
`opcmd.exe -p usb enable`	USB チャネル制御を有効にします。	なし
`opcmd.exe -p usb disable`	USB チャネル制御を無効にします。	なし
`opcmd.exe -p usb info -d DRIVE`	指定したドライブに対する USB 情報を表示します。	`-d、--drive` ドライブ: 必須の引数。ドライブのパスを指定します (例 `E:`)。
`opcmd.exe -p usb list`	信頼する USB デバイスのリストを表示します。	なし
`opcmd.exe -p usb remove [-v VID -p PID -s SN]`	信頼する USB デバイスを削除します。	`-v、--vid VID`: 必須の引数。ベンダ ID を 16 進文字列で指定します。

コマンド	説明	オプション
		-p、--pid PID: 必須の引数。製品 ID を 16 進文字列で指定します。 -s --sn SN: 必須の引数。シリアル番号を指定します。
opcmd.exe -p usb status	USB チャネル制御のステータスを表示します。	なし
opcmd.exe -p quarantine show	隔離ファイルのリストを表示します。	なし
opcmd.exe -p quarantine restore [QUARANTINENAME]	指定した隔離ファイルを復元します。	なし
opcmd.exe -p udso list	ユーザ指定不審オブジェクトのリストを表示します。	-a、--all: すべてのタイプの不審オブジェクトのリストを表示します。 -p、--file-path: ファイルパスで指定した不審オブジェクトのリストを表示します。 -h、--file-sha1: ファイルの SHA1 ダイジェストで指定した不審オブジェクトのリストを表示します。 -H、--file-sha2: ファイルの SHA2 ダイジェストで指定した不審オブジェクトのリストを表示します。
opcmd.exe -p udso scan	ユーザ指定不審オブジェクトについて、既存のプロセスを検索します。	これらの不審なプロセスを終了する前に確認メッセージが表示されます。
opcmd.exe -p update-task	指定した時刻に繰り返しアップデートを予約します。	--time 開始時刻: 予約アップデートの開始時刻 (HH:MM) を指定します。 --daily: 予約アップデートを毎日実行することを指定します。

コマンド	説明	オプション
		`--weekly` 曜日: 予約アップデートを毎週特定の曜日に実行することを指定します。Sunday、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday のみ有効です。 `--monthly` 日付: 予約アップデートを毎月特定の日付 (1〜31) に実行することを指定します。月の最終日に実行するには、-1 と指定します。 `--remove`: 予約アップデートを削除します。

第 6 章

イベント

この章では、TXOne StellarProtect エージェント内で記録されるイベントについて説明します。

この章の内容は次のとおりです。

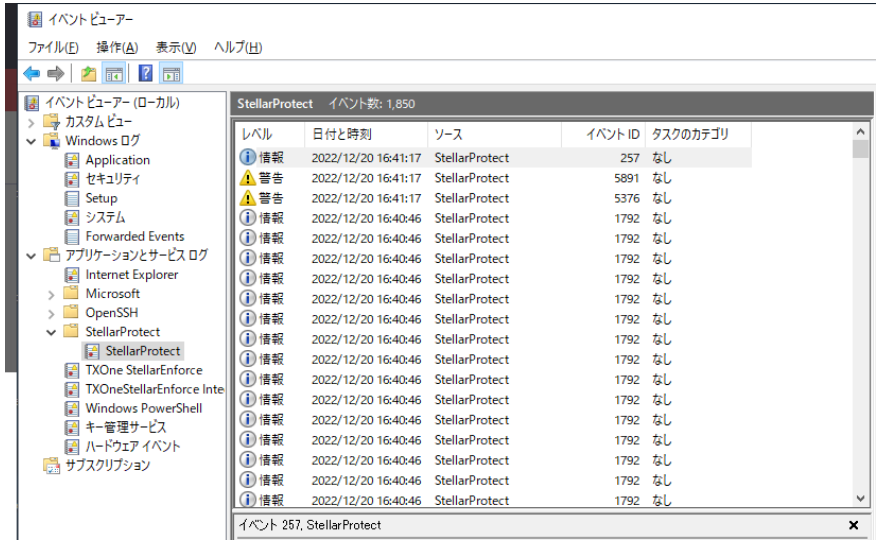
StellarProtect のイベントの概要

StellarProtect エージェントでは、イベントは次の 3 つの分類で記録されます。

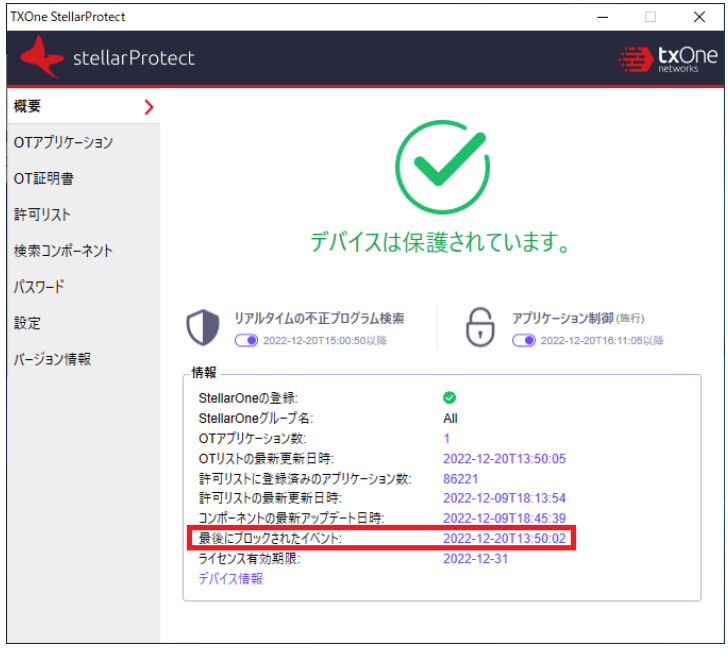
- **レベル 0: 情報**では、重要なタスクが記録されます。
- **レベル 1: 警告**では、インシデントが記録されます。
- **レベル 2: 重大**では、重要な機能がオンまたはオフになったことが記録されます。

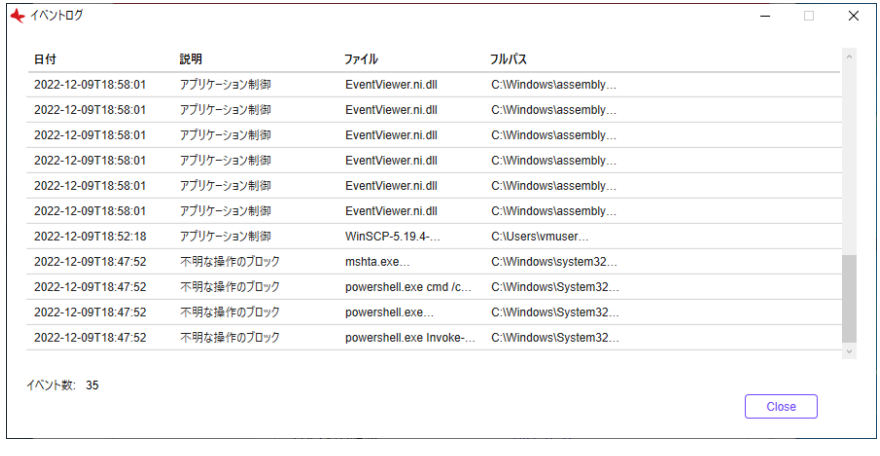
エージェントのイベントログの説明

StellarProtect では、Windows イベントビューアーを使用してすべての StellarProtect イベントログを表示できます。イベントビューアーにアクセスするには、[スタート]→[コントロール パネル]→[管理ツール]→[イベントビューアー] の順にクリックします。



StellarProtect エージェントのメイン画面でも、StellarProtect のブロックされたイベントログを確認できます。エージェントのブロックされたイベントにアクセスするには、StellarProtect を実行して、[概要] 画面の [情報] で [最後にブロックされたイベント] をクリックします。


TXOne StellarProtect
stellarProtect
概要
OTアプリケーション
OT証明書
許可リスト
検索コンポーネント
パスワード
設定
バージョン情報
デバイスは保護されています。
リアルタイムの不正プログラム検索
2022-12-20T15:00:50以降
アプリケーション制御 (施行)
2022-12-20T16:11:05以降
情報
StellarOneの登録:
StellarOneグループ名: All
OTアプリケーション数: 1
OTリストの最新更新日時: 2022-12-20T13:50:05
許可リストに登録済みのアプリケーション数: 86221
許可リストの最新更新日時: 2022-12-09T18:13:54
コンポーネントの最新アップデート日時: 2022-12-09T18:45:39
最後にブロックされたイベント: 2022-12-20T13:50:02
ライセンス有効期限: 2022-12-31
デバイス情報


イベントログ
日付 説明 ファイル フルパス
2022-12-09T18:58:01 アプリケーション制御 EventViewer.ni.dll C:\Windows\assembly...
2022-12-09T18:58:01 アプリケーション制御 EventViewer.ni.dll C:\Windows\assembly...
2022-12-09T18:58:01 アプリケーション制御 EventViewer.ni.dll C:\Windows\assembly...
2022-12-09T18:58:01 アプリケーション制御 EventViewer.ni.dll C:\Windows\assembly...
2022-12-09T18:58:01 アプリケーション制御 EventViewer.ni.dll C:\Windows\assembly...
2022-12-09T18:58:01 アプリケーション制御 EventViewer.ni.dll C:\Windows\assembly...
2022-12-09T18:52:18 アプリケーション制御 WinSCP-5.19.4-... C:\Users\vmuser...
2022-12-09T18:47:52 不明な操作のブロック mshta.exe... C:\Windows\system32...
2022-12-09T18:47:52 不明な操作のブロック powershell.exe cmd /c... C:\Windows\System32...
2022-12-09T18:47:52 不明な操作のブロック powershell.exe... C:\Windows\System32...
2022-12-09T18:47:52 不明な操作のブロック powershell.exe Invoke-... C:\Windows\System32...
イベント数: 35
Close

エージェントイベントのリスト

イベント ID	レベル	イベントの内容	詳細情報
256	情報	サービスが開始されました	サービスが開始されました。
257	情報	ポリシーが適用されました (バージョン: %version%)	ポリシーが適用されました。
258	情報	Patch が適用されました。ファイル名: %file_name%	Patch が適用されました。
259	情報	Patch を適用中	Patch を適用中です。 先に適用された Patch が完了すると、この Patch (%deferred_file_name%) が自動的に適用されます。
513	情報	ICS アプリケーションのリストがアップデートされました	ICS アプリケーションのリストがアップデートされました。
514	情報	リアルタイム検索が有効になりました	リアルタイム検索が有効になりました。
515	情報	予約検索の開始	予約検索が開始されました。
516	情報	予約検索の終了	予約検索が終了しました。
517	情報	手動検索の開始	手動検索が開始されました。
518	情報	手動検索の終了	手動検索が終了しました。
519	情報	予約検索が有効になりました	予約検索が有効になりました。 次回の検索は%NextScan%に実行されます。
520	情報	予約検索が無効になりました	予約検索が無効になりました。
768	情報	オペレーション振る舞い検知が有効になりました	モード: %Mode% レベル: %Level%

イベント ID	レベル	イベントの内容	詳細情報
769	情報	オペレーション振る舞い検知における許可済みの操作を追加しました	アクセスユーザ: %USERNAME% Id: %ID% 対象プロセス: %PATH% %ARGUMENT% 親プロセス 1: %PATH% %ARGUMENT% 親プロセス 2: %PATH% %ARGUMENT% 親プロセス 3: %PATH% %ARGUMENT% 親プロセス 4: %PATH% %ARGUMENT%
770	情報	オペレーション振る舞い検知における許可済みの操作を削除しました	Id: %ID% 対象プロセス: %PATH% %ARGUMENT% 親プロセス 1: %PATH% %ARGUMENT% 親プロセス 2: %PATH% %ARGUMENT% 親プロセス 3: %PATH% %ARGUMENT% 親プロセス 4: %PATH% %ARGUMENT%
784	情報	DLL インジェクション対策が有効になりました	DLL インジェクション対策が有効になりました。
1280	情報	デバイスコントロールが有効になりました	デバイスコントロールが有効になりました。
1281	情報	信頼する USB デバイスが追加されました	ベンダ ID: %HEX% 製品 ID: %HEX% シリアル番号: %STRING% タイプ:永続的または 1 回限り

イベント ID	レベル	イベントの内容	詳細情報
1282	情報	信頼する USB デバイスが削除されました	ベンダ ID: %HEX% 製品 ID: %HEX% シリアル番号: %STRING%
1792	情報	ファイルのアクセスが許可されました: %PATH%	パス: %PATH% アクセスユーザ: %USERNAME% モード: %MODE% リスト: %LIST%
1793	情報	メンテナンスモードで許可リストに追加されました	パス: %PATH% ハッシュ: %SHA256_HEXSTR%
1794	情報	メンテナンスモードで許可リストがアップデートされました。	パス: %PATH% ハッシュ: %SHA256_HEXSTR%
1795	情報	許可リストの初期化を開始しました	許可リストの初期化を開始しました。
1796	情報	許可リストの初期化が完了しました	許可リストの初期化が完了しました。 数: %COUNT%
1797	情報	アプリケーション制御有効	アプリケーション制御が有効になりました。 モード: %MODE%
1798	情報	DLL/ドライバ制御が有効になりました	DLL/ドライバ制御が有効になりました。
1799	情報	スクリプト制御が有効になりました	スクリプト制御が有効になりました。
1800	情報	Intelligent Runtime Learning (インテリジェントランタイム学習) が有効になりました	Intelligent Runtime Learning (インテリジェントランタイム学習) が有効になりました。
2048	情報	コンポーネントのアップデートを開始しました。	コンポーネントのアップデートを開始しました。
2049	情報	コンポーネントのアップデートが終了しました。	コンポーネントのアップデートが終了しました。

イベントID	レベル	イベントの内容	詳細情報
2050	情報	コンポーネントの予約アップデートが有効になっています。次回のアップデートは%NEXT_UPDATE_LOCAL_TIME_STR%に実行されます (エージェントのローカルシステム時間)。	コンポーネントの予約アップデートが有効になっています。次回のアップデートは%NEXT_UPDATE_LOCAL_TIME_STR%に実行されます (エージェントのローカルシステム時間)。
2051	情報	コンポーネントの予約アップデートが無効になっています。	コンポーネントの予約アップデートが無効になっています。
4352	警告	サービスが停止されました	サービスが停止されました。
4353	警告	ポリシーを適用できません (バージョン: %version%)	ポリシーを適用できません。
4354	警告	ファイルをアップデートできません: %dst_path%	ファイルをアップデートできません。 アップデート元のパス: %src_path% アップデート先のパス: %dst_path% エラーコード: %err_code%
4355	警告	Patch を適用できません。ファイル名: %file_name%	Patch を適用できません。 ファイル名: %file_name% エラーコード: %err_code%
4609	警告	受信ファイルが検索されました。ウイルス対策により実行された処理: %PATH%	ウイルス対策によって受信ファイルが検索されました。設定に従って処理が実行されました。 ファイルパス: %PATH% ファイルハッシュ: %STRING% 脅威の種類: %STRING% 脅威の名前: %STRING% 処理の結果: %INTEGER% 隔離パス: %PATH%

イベント ID	レベル	イベントの内容	詳細情報
4610	警告	受信ファイルが検索されました。次世代ウイルス対策により実行された処理: %PATH%	次世代ウイルス対策によって受信ファイルが検索されました。 設定に従って処理が実行されました。 ファイルパス: %PATH% ファイルハッシュ: %STRING% 脅威の種類: %STRING% 脅威の名前: %STRING% 処理の結果: %INTEGER% 隔離パス: %PATH%
4611	警告	ローカルファイルが検索されました。ウイルス対策により実行された処理: %PATH%	ウイルス対策によってローカルファイルが検索されました。 設定に従って処理が実行されました。 ファイルパス: %PATH% ファイルハッシュ: %STRING% 脅威の種類: %STRING% 脅威の名前: %STRING% 処理の結果: %INTEGER% 隔離パス: %PATH%
4612	警告	ローカルファイルが検索されました。次世代ウイルス対策により実行された処理: %PATH%	次世代ウイルス対策によってローカルファイルが検索されました。 設定に従って処理が実行されました。 ファイルパス: %PATH% ファイルハッシュ: %STRING% 脅威の種類: %STRING% 脅威の名前: %STRING% 処理の結果: %INTEGER% 隔離パス: %PATH%

イベント ID	レベル	イベントの内容	詳細情報
4613	警告	不審なプログラムの実行がブロックされました: %PATH%	不審なプログラムの実行がブロックされました。 ファイルパス: %PATH% ファイルハッシュ: %STRING%
4614	警告	不審なプログラムが実行されています: %PATH%	不審なプログラムが実行されています。 プロセス ID: %PID% ファイルパス: %PATH% ファイルハッシュ: %STRING% ファイルの信頼性: %STRING%
4615	警告	ウイルス対策によってアプリケーションの実行がブロックされました: %PATH%	ウイルス対策によってアプリケーションの実行がブロックされました。 対象プロセス: %PATH% ファイルハッシュ: %STRING% 脅威の種類: %STRING% 脅威の名前: %STRING%
4617	警告	次世代ウイルス対策によってアプリケーションの実行がブロックされました: %PATH%	次世代ウイルス対策によってアプリケーションの実行がブロックされました。 対象プロセス: %PATH% ファイルハッシュ: %STRING% 脅威の種類: %STRING% 脅威の名前: %STRING%
4864	警告	オペレーション振る舞い検知が無効になりました	オペレーション振る舞い検知が無効になりました。

イベント ID	レベル	イベントの内容	詳細情報
4865	警告	オペレーション振る舞い検知によりプロセスが許可されました: %PATH% %ARGUMENT%	アクセスユーザ: %USERNAME% 親プロセス 1: %PATH% %ARGUMENT% 親プロセス 2: %PATH% %ARGUMENT% 親プロセス 3: %PATH% %ARGUMENT% 親プロセス 4: %PATH% %ARGUMENT% モード: %Mode%
4866	警告	オペレーション振る舞い検知によりプロセスがブロックされました: %PATH% %ARGUMENT%	アクセスユーザ: %USERNAME% 親プロセス 1: %PATH% %ARGUMENT% 親プロセス 2: %PATH% %ARGUMENT% 親プロセス 3: %PATH% %ARGUMENT% 親プロセス 4: %PATH% %ARGUMENT% モード: %Mode%
4880	警告	DLL インジェクション対策が無効になりました	DLL インジェクション対策が無効になりました。
5120	警告	Safeguard により ICS ファイルの変更がブロックされました: %PATH%	Safeguard により ICS ファイルに対する変更がブロックされました。 ブロックされたプロセス: %PATH% 対象ファイル: %PATH%
5121	警告	Safeguard により ICS プロセスの操作がブロックされました: %PATH%	Safeguard により ICS プロセスの操作がブロックされました。 ブロックされたプロセス: %PATH% 対象プロセス: %PATH%
5376	警告	デバイスコントロールが無効になりました	デバイスコントロールが無効になりました。

イベント ID	レベル	イベントの内容	詳細情報
5377	警告	USB のアクセスがブロックされました: %PATH%	パス: %PATH% アクセスユーザ: %USERNAME% ベンダ ID: %HEX% 製品 ID: %HEX% シリアル番号: %STRING%
5888	警告	ファイルのアクセスが許可されました: %PATH%	パス: %PATH% アクセスユーザ: %USERNAME% モード: %MODE% 理由: %ALLOWED_REASON% ファイルのハッシュが許可されました: %SHA256_HEXSTR% %THROTTLING_INFO_MSG%
5889	警告	ファイルのアクセスがブロックされました: %PATH%	パス: %PATH% アクセスユーザ: %USERNAME% モード: %MODE% 理由: %BLOCKED_REASON% ブロックされたファイルのハッシュ: %SHA256_HEXSTR%%THROTTLING_INFO_MSG%
5890	警告	許可リストに対して追加またはアップデートを実行できませんでした: %PATH%	許可リストに対して追加またはアップデートを実行できませんでした: %PATH%
5891	警告	アプリケーション制御が無効になりました	アプリケーション制御が無効になりました。
5892	警告	DLL/ドライバ制御が無効になりました	DLL/ドライバ制御が無効になりました。
5893	警告	スクリプト制御が無効になりました	スクリプト制御が無効になりました。
5894	警告	Intelligent Runtime Learning (インテリジェントランタイム学習) が無効になりました	Intelligent Runtime Learning (インテリジェントランタイム学習) が無効になりました。

イベント ID	レベル	イベントの内容	詳細情報
5895	警告	許可リストの初期化がキャンセルされました	許可リストの初期化がキャンセルされました。
8706	重大	リアルタイム検索が無効になりました	リアルタイム検索が無効になりました。
9216	重大	メンテナンスモード開始	メンテナンスモードを開始しました。
9217	重大	メンテナンスモード終了	メンテナンスモードが終了しました。

第 7 章

製品サポート情報

TXOne Networks 製品のサポートは、TXOne Networks とトレンドマイクロが相互に行います。すべての製品サポート情報は、TXOne と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: APEM29618_JP2303