TREND MICRO | txOne networks

2.0 TXOne StellarOne
管理者ガイド
for StellarProtect

※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: APEM29594_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 Networks 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 StellarOne 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 StellarOne 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 StellarOne 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 StellarEnforce のドキュメント

ドキュメント	説明
Readme ファイル	既知の制限事項および基本的なインストール手順に関する説明
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	StellarOne エージェントのインストール、製品の概要、設定、およびサーバとエージェントを管理するために必要な詳細情報の説明

対象読者

TXOne StellarOne 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 StellarOne 管理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

用語

次の表は、TXOne StellarOne のドキュメントで使用されている用語を示しています。

用語	説明
サーバ	StellarOne の管理サーバ画面プログラムです。
サーバコンピュータ	StellarOne サーバがインストールされているホストです。
エージェント	StellarProtect クライアントプログラムを実行しているホストです。
NAT エージェント	ネットワークアドレス変換 (NAT) 機能が有効なルータの下に構成されたエージェントです。
管理対象エージェント 管理下のエージェント	StellarOne サーバプログラムが認識している、StellarProtect クライアントプログラムを実行しているホストです。
対象エージェント	StellarOne の管理対象エージェントをインストールするホストです。
管理者 (または StellarOne 管理者)	StellarOne サーバを管理している人物です。
StellarOne の 管理サーバ画面	StellarOne の設定や管理対象エージェントを設定して管理するユーザインタフェースです。
CLI	コマンドラインインタフェース
ライセンスの アクティベーション	StellarOne サーバのインストールの種類と、アプリケーションの使用許諾期間が含まれます。

第 1 章

本製品の概要

この章では、TXOne StellarOne について紹介するとともに、産業用次世代ウイルス対策およびアプリケーション制御による保護を資産に対して提供するエージェントを StellarOne で管理する方法について説明します。ここでは管理機能の概要を取り上げます。このマニュアルでは、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ある TXOne StellarProtect を管理する方法について主に説明します。

この章の内容は次のとおりです。

TXOne Stellar 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。

- 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
- StellarProtect: モダナイズされた OT/ICS エンドポイント向けの、産業用次世代ウイ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

TXOne Stellar では、これらの製品が連携することで、共存する新旧システムの保護を同じ管理サーバ画面から調整および維持することができ、セキュリティ上の脅威から企業を守り、高い生産性を実現します。

主な機能と特徴

StellarOne の管理サーバ画面には、次の機能と特徴があります。

表 1-1. 機能と特徴

機能	説明
ダッシュボード	管理サーバ画面のダッシュボードには、監視下のエージェントについての概要情報が表示されます。 インストール済みのエージェントのステータスを簡単に確認でき、指定された期間内のエージェントのアクティビティについてセキュリティレポートを生成できます (Legacy Mode のみ)。
エージェントの集中管理	TXOne StellarOne では、管理者は次のタスクを実行できます。 • StellarProtect/StellarProtect (Legacy Mode) エージェントのステータスの監視 • 接続ステータスの確認 • 設定の表示

機能	説明
	• 手動またはポリシーによるエージェントログの収集 (Legacy Mode のみ) • エージェントのアプリケーション制御の有効化または無効化 • エージェントのデバイスコントロールの有効化または無効化 • エージェントのメンテナンスモードの設定 • エージェントコンポーネントのアップデート • 許可リストの初期化 • エージェントへの Patch の配信 • 信頼するファイルおよび USB デバイスの追加
イベントの集中管理	StellarProtect/StellarProtect (Legacy Mode) エージェントで保護されたコンピュータでは、管理者がステータスやイベントを監視し、ファイルの実行がブロックされた場合はそれに対処できます。TXOne StellarOne にはイベント管理機能があり、管理者はこれを使用して、ブロックされたファイルイベントを迅速に把握して処理を実行できます。
監査	StellarOne の管理サーバ画面にアクセスするためのアカウントで実行された操作を監査することが可能です。StellarOne では各アカウントの操作をログに記録して、ログインしたユーザ、設定を変更したユーザ、イベントログを削除したユーザなどを追跡できます。

新機能

TXOne StellarOne 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 1-2. TXOne StellarOne 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。次の 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。 • 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。
エージェントコンポーネントのスケジュールアップデート	StellarOne の管理サーバ画面にある既存のコンポーネントのスケジュールアップデート機能に加え、エージェントに対するコンポーネントのスケジュールアップデートも設定できるようになりました (StellarProtect)。コンポーネントのアップデートは指定された時間間隔で自動的に実行されます。
自己管理グループポリシー	この新しく追加されたグループポリシーにより、現場のオペレータがエージェントのポリシー設定を独自に指定できるようになります。自己管理ステータスに切り替わったローカルエージェントは、StellarOne の管理サーバ画面のポリシー管理から外されます。
メンテナンスモードでのリアルタイムの不正プログラム検索	[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、シームレスな保護のためにメンテナンス期間中もリアルタイムの不正プログラム検索を有効にするようユーザを促します。
オープン API	エージェントのデータをクエリするためのオープン API が提供されています。API キーを生成して、アカウント管理のために各ユーザアカウントに対して有効期限を設定することもできます。

第 2 章

管理サーバ画面

この章では、StellarOne の Web ベースの管理サーバ画面にアクセスして設定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。

管理サーバ画面について

TXOne StellarOne は、ユーザが Web ブラウザからアクセス可能な Web GUI を備えた管理サーバ画面です。StellarOne は、Open Virtual Appliance (OVA) または Virtual Hard Disk v2 (VHDX) 形式でパッケージ化されています。OVA ファイルでは VMware ESXi および VMware Workstation システムが、VHDX ファイルでは Windows Hyper-V マネージャーWindows システムがサポートされています。

注意

サポートされるブラウザ:

- Google Chrome 87 以降のバージョン
- Microsoft Edge 79 以降のバージョン
- Mozilla Firefox 78 以降のバージョン

StellarOne にはじめてログオンする場合は、17 ページの「StellarOne の管理サーバ画面を開く」を参照してください。

StellarOne のインストールの詳細については、「StellarOne インストールガイド」を参照してください。

StellarOne の管理サーバ画面を開く

手順

1. Web ブラウザから次の形式で StellarOne のアドレスを入力します。`https://`<対象サーバの `IP` アドレス>ログオン画面が表示されます。
2. 資格情報 (ユーザ名とパスワード) を入力します。

   初回ログオン時には、次の初期設定の管理者資格情報を入力します。

   - ユーザ名: `admin`
   - パスワード: `txone`

3. [ログオン] をクリックします。
4. StellarOne の管理サーバ画面をはじめて使用する場合は、次の手順で初期設定を実行します。
   a. [ログイン情報の設定] 画面が表示され、パスワードを変更するように求められます。次の手順でパスワードの設定を確認します。
      - [新しいパスワード] に新しいパスワードを入力します。
      - [パスワードの確認] にパスワードを再度入力します。
   b. [確認] をクリックします。自動的にログアウトされます。[ログオン] 画面が再度表示されます。
   c. 新しい資格情報を使用して、再度ログオンします。
   d. 最初のアクティベーションコードを入力して、[続行] をクリックします。別の製品のアクティベーションコードを入力する場合は、[続行] の代わりに [別のコードを入力してください] をクリックします。
   e. [エンドユーザ使用許諾契約および TXOne OT Intelligent Trust への同意] 画面が表示されます。リンクをクリックしてドキュメントを読み、「同意する」ボタンを押して次の手順に進みます。

注意

セキュリティの配信を強化するために、TXOne OT Intelligent Trust は有効にすることをお勧めします。詳細については、114 ページの「OT Intelligent Trust」を参照してください。

f. [日付と時刻] や [タイムゾーン] などの時間設定を指定して、[続行] をクリックします。

g. StellarOne の管理サーバ画面が使用可能になります。

5. 初期設定が完了すると、さまざまなユーザアカウントで Web ブラウザを使用して、リモートから StellarOne にログオンできるようになります。

6. (オプション) 画面の右上角の ID アイコンをクリックし、[パスワードの変更] をクリックすることでパスワードを変更できます。

7. (オプション) セキュリティ上の理由から必要な場合は、画面の右上角の ID アイコンをクリックし、[ログオフ] をクリックすることにより手動でログオフできます。

注意

30 分間操作が行われないと、ユーザは自動的に管理サーバ画面からログオフされます。

第 3 章

ダッシュボード

この章では、StellarOne の管理サーバ画面のダッシュボードの概要を説明し、その設定の指定方法について紹介します。

この章の内容は次のとおりです。

[ダッシュボード] 画面について

ダッシュボードには、管理対象エージェントのイベントの概要と、StellarOne の管理サーバ画面のシステムステータスが表示されます。管理サーバ画面の上部にあるナビゲーションバーで [ダッシュボード] タブをクリックすると、[概要] と [システム] の 2 つのタブを含む [ダッシュボード] 画面が表示されます。

図 3-1.　[ダッシュボード] 画面

表 3-1.　[ダッシュボード] 画面について

機能	説明
概要	許可リストとポリシー配信のプロセスフローが強化され、システム操作の効率性が向上します。 • **イベントをブロックしたエージェントの上位** • **ブロックされた件数が上位のファイル** 詳細については、22 ページの「StellarProtect の監視用ウィジェット」および 25 ページの「ウィジェットを追加する」を参照してください。 **注意** 初期設定では、[概要] タブページが**ダッシュボード**のランディングページとして設定されています。

機能	説明
システム	このタブでは、次に関連する StellarOne の管理サーバ画面のシステムステータスを確認できます。 • CPU 使用率 • メモリ使用率 • ディスク使用率
タブ設定	このボタンを使用して、タブ名をカスタマイズできます。ボタンをクリックし、[タブ名] に名前を入力し、[OK] をクリックすることで簡単にタブ名を変更できます。
ウィジェットの追加	このボタンを使用して、必要なウィジェットを [ダッシュボード] 画面に追加できます。詳細については、25 ページの「ウィジェットを追加する」を参照してください。
印刷	このボタンを使用して、現在の [概要] または [システム] ページを印刷できます。

StellarProtect の監視用ウィジェット

[ダッシュボード] 画面の [概要] タブには、StellarProtect エージェントのイベントを監視するための 2 つのウィジェットを追加できます。

- **イベントをブロックしたエージェントの上位:** このウィジェットには、イベントのブロック件数が上位のエージェントが表示されます。初期設定で、このウィジェットは [ダッシュボード] の [概要] タブに表示されます。

  表 3-2. ウィジェット: イベントをブロックしたエージェントの上位

列	説明
エージェント名	エージェントの名前
説明	エージェントに割り当てられたタグ
IP アドレス	エージェントの IP アドレス
ブロックされたイベント	エージェントでブロックされたイベントの合計数

- **ブロックされた件数が上位のファイル:** このウィジェットには、ブロック件数が上位のファイルのリストが表示されます。

表 3-3.　ウィジェット: ブロックされた件数が上位のファイル

列	説明
ファイル名	ブロックされたファイルの名前
ファイルハッシュ	ブロックされたファイルの SHA-1 ハッシュ
エージェント	当該ファイルのブロックイベントを報告したエージェントの合計数
ブロックされたイベント	当該ファイルに対するブロックイベントの合計数

ヒント

- 自動更新を開始するには、再生ボタンをクリックします。自動更新を停止するには、一時停止ボタンをクリックします。
- ドロップダウンメニューボタンをクリックすると、次の 2 つの機能が表示されます。
  - **ウィジェット設定:**
    - **ウィジェット名:** ウィジェットの名前を編集できます。
    - **期間:** 特定の期間を選択できます。この期間により、表示されるブロックされたイベントまたはファイルの数が決まります (初期設定値は [過去 7 日間])。
    - **自動更新設定:** 設定を手動更新に変更するか、自動更新頻度 (初期設定値は [5 分ごと]) を指定できます。
  - **ウィジェットの削除:** [ダッシュボード] 画面からウィジェットを削除できます。
- ウィジェットを移動するには、ウィジェットのタイトルバーをクリックしたまま、タブページ上の任意の位置にドラッグします。
- ウィジェットのサイズを変更するには、ウィジェットの端にマウスを重ねます。斜めのサイズ変更ポインタが表示されたら、ドラッグしてウィジェットのサイズを変更します。

ウィジェットを追加する

タブに追加できるウィジェットの数は、タブページのレイアウトに応じて異なります。タブページに含まれるウィジェットが最大数に達した場合は、ウィジェットをタブページから削除するか、追加するウィジェットに対して新しいタブを作成する必要があります。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [ダッシュボード] を選択します。
2. ダッシュボードで、ウィジェットを追加するタブ ([概要] または [システム]) を選択します。
3. 右側の [ウィジェットの追加] ボタンをクリックすると、ウィジェットを追加する画面が表示されます。
4. 追加するウィジェット名の横にあるチェックボックスをオンにして、1 つ以上のウィジェットを現在のタブに追加します。
5. [追加] ボタンをクリックして、タスクを完了します。

第 4 章

エージェント管理

この章では、StellarOne の管理サーバ画面から StellarProtect エージェントを管理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。

[エージェント] 画面について

StellarOne の管理サーバ画面では、エージェントをさまざまなグループにまとめ、グループを階層化して (子グループの上に親グループ) エージェント/グループのツリー構造を作成できるため、エージェントの管理が容易になります。

StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。[エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示され、設定タスクを実行できるようになります。設定タスクは、即座に処理が実行される 1 回限りのコマンドです。

注意

- 初期設定では、[すべて] グループにすべてのエージェントが表示されます。
- 画面は 5 分ごとに自動更新されます。

図 4-1. [エージェント] 画面 - ツールバー

表 4-1.　ツールバー

ツール	説明
+グループの新規作成	複数のエージェントの管理を容易にするため、場所、種類、または目的に応じてグループを作成できます。詳細については、31 ページの「グループを追加する」を参照してください。
編成	エージェント説明の編集や別グループへの移動、または、エージェント/グループを削除できます。詳細については、32 ページの「エージェントの説明を編集する」および 32 ページの「エージェント/グループを編成する」を参照してください。
保護	メンテナンスモードを設定し、アプリケーション制御機能が有効な場合は許可リストをアップデートし、ファイルの検索設定をカスタマイズできます。詳細については、37 ページの「メンテナンスモードを設定する」、39 ページの「許可リストをアップデートする」、および 40 ページの「検索開始を設定する」を参照してください。
アップデート	コンポーネントをアップデートし、エージェントに Patch を配信できます。詳細については、42 ページの「エージェントコンポーネントをアップデートする」および 43 ページの「エージェントに Patch を配信する」を参照してください。
インポート/エクスポート	現在 StellarProtect では [インポート/エクスポート] ツールはサポートされていません。このツールは、StellarProtect (Legacy Mode) エージェントの管理に使用します。

図 4-2.　[エージェント] 画面 - 表の列見出し

表 4-2.　表の列見出し

列見出し	説明
名前	• : エージェントを示します。 • : グループを示します。 • : エージェントのライセンスの有効期限が切れており、更新が必要であることを示します。
IP アドレス	エージェントの IP アドレスを示します (1 つの IP アドレスが 1 つのエージェントに対応)。
保護	• : エージェントのアプリケーション制御機能が有効になっていることを示します。 • : エージェントが保護されていることを示します。 • : エージェントがメンテナンスモード中であることを示します。 • : エージェントが保護されておらず、セキュリティ脅威にさらされていることを示します。
ポリシーの継承	• **継承済み:** エージェント/グループのポリシー設定が親グループから継承されていることを示します。 • **カスタマイズ済み:** エージェント/グループのポリシー設定がユーザによりカスタマイズされていることを示します。 • **自己管理対象:** エージェント/グループが StellarOne の管理サーバ画面のポリシー管理から外れており、自身のポリシー設定を自己管理できることを示します。 • : 緑のライトは、エージェントのポリシー設定が StellarOne の管理サーバ画面と同期されることを示します。 • : グレーのライトは、エージェントのポリシー設定が StellarOne の管理サーバ画面と同期されないことを示します。 • : エージェント/グループが StellarOne の管理サーバ画面のポリシー管理から外れており、自身のポリシー設定を現場で指定できることを示します。
許可リスト	許可リストに追加されたアプリケーションの合計数を示します。エージェントで許可リストを作成中の場合は、代わりに進行状況バーが表示されます。
エージェントバージョン	エージェントのファームウェアバージョンを示します。
前回の接続	エージェントが StellarOne の管理サーバ画面に最後に接続された日時を示します。

列見出し	説明
機能タイプ	StellarProtect が次のいずれの機能タイプであるかを示します。 • StellarProtect: Windows 7 以降のバージョンのデバイス用。 • StellarProtect (Legacy Mode): Windows XP/2000 などのレガシープラットフォームのデバイス用。
処理	この列では次の操作を実行できます。 • [一般情報] ポリシーページを表示するには、ポリシーアイコン をクリックします。 • エージェントを編成し、グループを名前変更または削除するには、縦三点リーダーメニューのアイコンをクリックします。詳細については、32 ページの「エージェントの説明を編集する」および 32 ページの「エージェント/グループを編成する」を参照してください。

図 4-3.　[エージェント] 画面 - その他のツール

表 4-3.　その他のツール

ツール	説明
フィルタ	 : 並べ替えと検索により、エージェント/グループをすばやく見つけることができます。詳細については、35 ページの「エージェント/グループのフィルタオプション」を参照してください。
表の表示設定	 : 次の方法で表の表示設定をカスタマイズできます。 • 表示ページ間を移動する。 • [表をカスタマイズ] 設定で、ページごとに表示するエージェント/グループの数を選択し、特定の内容のみ表示することを指定する。 • 表を手動で更新して、最新の出力を表示する。

グループを追加する

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. ツールバーの [+グループの新規作成] ボタンをクリックします。
4. [新しいエージェントグループの追加] 画面が表示されます。テキストフィールドにグループ名を入力します。

注意

- グループ名は 50 文字以内で入力してください。
- グループレベルの最大数は 15 です。

5. [確認] をクリックしてグループを追加します。

エージェントの説明を編集する

ローカルエージェントのメイン画面に表示されるエージェントの説明を編集するには、次の手順を実行します。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. エージェントの説明は、次の 2 つの方法で編集できます。
   - 複数のエージェントの説明を同時に編集するには、対象エージェントまたはグループの横にあるチェックボックスにチェックを入れツールバーの [編成] ツールをクリックします。
   - 1 つのエージェントの説明を編集するには、対象エージェントの [処理] 見出しの下にある縦三点リーダーメニューのアイコンをクリックします。
4. ドロップダウンメニューが表示されます。最初のオプションである [タグの編集] をクリックすると、別の画面が表示されます。
5. テキストフィールドにエージェントの説明を入力します。
6. [確認] をクリックしてタスクを完了します。

エージェント/グループを編成する

次の方法でエージェント/グループを編成することができます。

- グループ名を変更する。
- グループを削除する。
- グループからエージェントを削除 (登録解除) する。
- エージェントを別のグループに移動する。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. グループの名前を変更するには、対象グループの [処理] 見出しの下にある縦三点リーダーメニューのアイコンをクリックします。ドロップダウンメニューが表示されます。[名前の変更] ボタンを選択すると、ポップアップ画面が表示されます。古いグループ名を削除し、新しい名前で置き換えます。[確認] をクリックしてタスクを完了します。

注意

同じレベルのグループに同じグループ名を付けることはできません。

4. グループまたはエージェントを削除するには、次の 2 つの方法があります。

   - 複数のエージェントまたはグループを同時に削除するには、対象エージェントまたはグループの横にあるチェックボックスにチェックを入れます。ツールバーの [編成] ツールをクリックし、[削除] を選択します。[確認] をクリックしてエージェント/グループを削除します。

     重要

     - エージェントを削除すると、エージェントのサーバへの登録が解除されます。
     - グループを削除すると、グループおよびその設定が削除されます。

   - 1 つのエージェントまたはグループを削除するには、対象エージェント/グループの [処理] 見出しの下にある縦三点リーダーメニューのアイコンをクリックします。ドロップダウンメニューが表示されます。[削除] ボタンを選択してエージェント/グループを削除します。

重要

子グループ/エージェントを持つグループを削除するには、先に対象グループから子グループ/エージェントを削除する必要があります。

5. エージェントを別のグループに移動するには、次の 2 つの方法があります。

   - 複数のエージェントを同時に別のグループに移動するには、対象エージェントの横にあるチェックボックスにチェックを入れます。ツールバーの [編成] ツールをクリックします。
   - 1 つのエージェントを別のグループに移動するには、対象エージェントの [処理] 見出しの下にある縦三点リーダーメニューのアイコンをクリックします。

   ドロップダウンメニューが表示されます。[移動] ボタンを選択すると、ポップアップ画面が表示されます。グループを選択し、[確認] をクリックしてタスクを完了します。

エージェント/グループを検索する

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. 画面の右上角にあるドロップダウンリストから条件を選択し、必要に応じて検索条件を追加して、特定のエージェントを検索します。

エージェント/グループのフィルタオプション

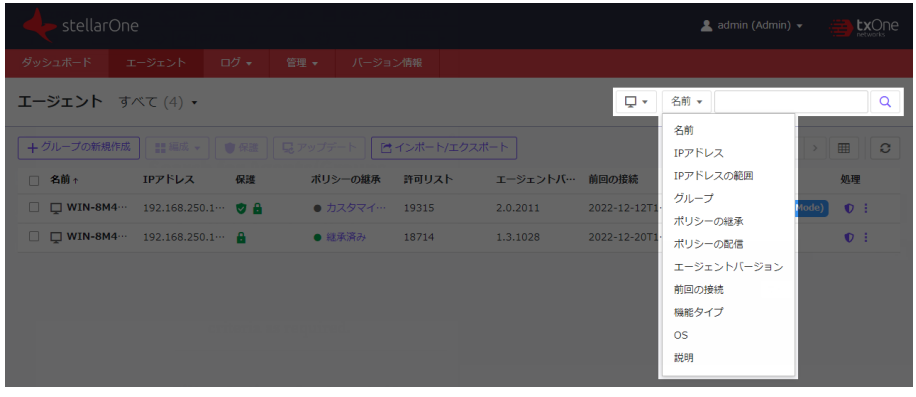


図 4-4.　フィルタオプション

表 4-4.　エージェント/グループのフィルタオプション

オプション	説明
名前	エージェントの名前。特定のエージェントを指定するには、エージェントの完全なホスト名またはホスト名の一部を入力します。
IP アドレス	IPv4 アドレスを入力します。
IP アドレスの範囲	IPv4 アドレスの範囲を入力します。
グループ	グループの名前。選択可能なグループを選択します。
ポリシーの継承	[継承済み]、[カスタマイズ済み]、および [自己管理対象] の 3 つの種類から選択できます。
ポリシーの配信	StellarOne からエージェントへのポリシー配信ステータス。[完了] または [実行中] を選択します。
エージェント バージョン	エージェントバージョンを入力します。

オプション	説明
前回の接続	エージェントが StellarOne に最後に接続された時間。初期設定の期間を選択するか、[カスタム] を選択して期間を指定します。初期設定の期間は次のとおりです。 • 1 時間以内 • 24 時間以内 • 過去 7 日間 • 過去 30 日間
機能タイプ	[StellarProtect] または [StellarProtect (Legacy Mode)] を選択します。
OS	対象エージェントの OS を選択します。
説明	特定のエージェントをクエリするには、完全な説明または説明の一部を入力します。

エージェントの保護

[保護] ツールは、即座に処理を実行する 1 回限りのコマンドをエージェントに送信します。このツールを使用して、メンテナンスモードを設定し、アプリケーション制御機能が有効な場合は許可リストをアップデートし、ファイルの検索設定をカスタマイズできます。

この節の内容は次のとおりです。

- 37 ページの「メンテナンスモードを設定する」
- 39 ページの「許可リストをアップデートする」
- 40 ページの「検索開始を設定する」

メンテナンスモードを設定する

エージェ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。利用するライセンスによっては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。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。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. チェックボックスにチェックを入れエージェント (またはグループ) を 1 つ以上選択します。
4. [エージェント] 画面の上部にあるツールバーで、[保護] ボタンをクリックします。
5. ポップアップ画面が表示されます。[メンテナンスモードの設定] オプションをクリックします。
6. [確認] をクリックします。
7. 設定画面が表示されます。注意事項を読み、[有効] または [無効] ラジオボタンをクリックします。
   - メンテナンスモードの設定を開始するには、[有効] をクリックします。手順 8 に進みます。
   - メンテナンスモードを終了するには、[無効]→[OK] の順にクリックします。これにより、エージェント上で予約されているメンテナンス期間がキャンセルされます。

a. 警告メッセージが表示されます。メッセージを読んでから、次の手順に進みます。

重要

メンテナンスモードが終了すると、OT アプリケーション保護により認識されないファイルの実行はブロックされるようになります。

b. [OK] をクリックして、メンテナンスモードを終了します。エージェントでのメンテナンスモード終了の配信ステータスを示すポップアップ画面が表示されます。

8. 予約設定画面が表示されます。メンテナンスモードを予約するには、次のいずれかの手順を実行します。

   - [予約] ラジオボタンをクリックしてから、編集アイコンをクリックし、メンテナンスモードの開始日時を指定します。続いて、[メンテナンスモードの残り時間] でメンテナンスモードの期間を指定します。
   - [開始] ラジオボタンをクリックしてから、[メンテナンスモードの残り時間] でメンテナンスモードの期間を指定します。

9. [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の有効/無効を切り替えるスイッチが追加されています。初期設定はオンです。

注意

- ポリシー設定でリアルタイムの不正プログラム検索を無効にしている場合、シームレスな保護のために、メンテナンス期間中はここで [リアルタイムの不正プログラム検索] スイッチをオンにすることをお勧めします。メンテナンス期間が終了すると、元のポリシー設定 (リアルタイムの不正プログラム検索は無効) に戻ります。
- この機能の詳細については、54 ページの「リアルタイムの不正プログラム検索」を参照してください。

10. [OK] をクリックして、選択したエージェントまたはグループに設定を配信します。

11. 配信ステータスを示す [コマンド配信] 画面が表示されます。[閉じる] ボタンをクリックして画面を閉じます。

許可リストをアップデートする

この機能では、数回クリックするだけで、選択したエージェント/グループ上の許可リストをアップデートできます。アプリケーション制御機能が有効な場合、新たに追加されたアプリケーションもエージェント上で実行できるように、許可リストは定期的にアップデートする必要があります。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. チェックボックスにチェックを入れエージェント (またはグループ) を 1 つ以上選択します。
4. [エージェント] 画面の上部にあるツールバーで、[保護] ボタンをクリックします。
5. ポップアップ画面が表示されます。[許可リストのアップデート] オプションをクリックします。
6. [確認] をクリックします。
7. [許可リストのアップデート] ポップアップ画面が表示されます。[OK] をクリックして、許可リストのアップデートプロセスを開始します。

警告!

アップデート中はエージェントを再起動したりシャットダウンしたりしないでください。アップデートプロセスの完了には 30 分以上かかることがあります。

8. アップデートステータスを示す [許可リストのアップデート] 画面が表示されます。[閉じる] ボタンをクリックして画面を閉じます。

検索開始を設定する

選択した 1 つまたは複数の対象エージェントに検索設定を配信し、選択したエージェントに対する検索を手動で開始できます。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. チェックボックスにチェックを入れエージェント (またはグループ) を 1 つ以上選択します。
4. [エージェント] 画面の上部にあるツールバーで、[保護] ボタンをクリックします。
5. ポップアップ画面が表示されます。[検索開始] オプションをクリックします。
6. [確認] をクリックします。
7. 設定画面が表示されます。
8. この設定画面は、[検索対象ファイル]、[検出時の処理]、および [検索除外] の 3 つのセクションから構成されています。
   a. [検索対象ファイル] セクションでは、すべてのファイルを詳細に検索するには [すべてのローカルフォルダ] を、全般的な検索を実行するには [初期設定のフォルダ (クイック検索)] を、検索対象のフォルダのパスを指定するには [特定のフォルダ] をクリックします。

> **ヒント**
>
> [特定のフォルダ] オプションでは、[+] または [-] アイコンをクリックして、特定のフォルダへのパスを追加または削除します。

   - (オプション) [圧縮ファイルを検索] チェックボックスをオンにし、圧縮ファイルの [最大階層] を 1～20 の間で指定します。

- (オプション) 特定のサイズを超えるファイルをスキップするには、[(任意の値) MB を超えるファイルをスキップ] チェックボックスをオンにし、ファイルサイズを 1〜9999MB の間で指定します。指定したファイルサイズを超えるファイルは検索されません。
- (オプション) 既存の信頼するリスト内のファイルも検索するには、[アグレッシブ検索 (すべての OT アプリケーションと CA ファイルを含む)] チェックボックスをオンにします。

b. [検出時の処理] セクションでは、検索プロセスで脅威が検出された場合の処理を事前に指定します。検出された疑わしいファイルまたは感染したファイルを隔離フォルダに移動してさらにチェックするには、[隔離] を選択します。結果を読み出すだけで、疑わしいファイルに対して処理を実行しない場合は、[処理しない] を選択します。

c. (オプション) [検索除外] セクションでは、特定のフォルダ、ファイル、またはファイル拡張子を検索の対象から除外することを選択できます。

- **フォルダ:** 検索から除外するフォルダのパスを指定します。
- **ファイル:** 検索から除外するファイルのパスを指定します。
- **ファイル拡張子:** 検索から除外する特定ファイルの拡張子を指定します。

注意

- [検索除外] ではローカルパスのみがサポートされます。URL や\\[ホスト名] などのリモートパスはサポートされません。
- ファイル拡張子の前に「.」や「*.」を追加する必要はありません。

ヒント

特定のフォルダ/ファイルのパス、または特定のファイルタイプのファイル拡張子を追加または削除するには、[+] または [-] アイコンをクリックします。

9. [OK] をクリックして、選択したエージェントに設定を配信します。
10. 配信ステータスを示す [コマンド配信] 画面が表示されます。[閉じる] ボタンをクリックして画面を閉じます。

エージェントのアップデート

この節では、StellarOne の管理サーバ画面から StellarProtect エージェントの検索コンポーネントをアップデートし、Patch を配信する方法について説明します。

この節の内容は次のとおりです。

エージェントコンポーネントをアップデートする

StellarOne の管理サーバ画面を使用して、選択したエンドポイント上の StellarProtect エージェントコンポーネントをアップデートできます。最新のセキュリティ脅威からエージェントを保護するために、エージェントコンポーネントを定期的にアップデートすることをお勧めします。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. チェックボックスにチェックを入れエージェント (またはグループ) を 1 つ以上選択します。
4. [エージェント] 画面の上部にあるツールバーで、[アップデート] ボタンをクリックします。
5. ポップアップ画面が表示されます。[エージェントコンポーネントのアップデート] オプションをクリックします。
6. [確認] をクリックします。
7. [エージェントコンポーネントのアップデート] 画面が表示されます。[OK] をクリックしてアップデートを開始します。

重要

アップデート中はエージェントを再起動したりシャットダウンしたりしないでください。アップデートプロセスの完了にはしばらくかかることがあります。

8. アップデートステータスを示す [コマンド配信] 画面が表示されます。[閉じる] ボタンをクリックして画面を閉じます。

エージェントに Patch を配信する

StellarOne の管理サーバ画面を使用して、選択したエンドポイント上の StellarProtect エージェントに Patch ファイルを配信できます。最新のセキュリティ脅威からエージェントを保護するために、エージェントの Patch を定期的にアップデートすることをお勧めします。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. チェックボックスにチェックを入れエージェント (またはグループ) を 1 つ以上選択します。
4. [エージェント] 画面の上部にあるツールバーで、[保護] ボタンをクリックします。
5. ポップアップ画面が表示されます。[エージェントに Patch を配信] オプションをクリックします。
6. [確認] をクリックします。
7. [エージェントに Patch を配信] ポップアップ画面が Patch のリストとともに表示されます。配信する Patch のチェックボックスにチェックを入れ選択します。

図 4-5.　Patch のバージョンの選択

注意

[アップデート] リンクをクリックすると、エージェントの新しい Patch をインポートするための [ダウンロード/アップデート] ページ (103 ページ) が表示されます。

8. [OK] をクリックして、エージェントの Patch 配信プロセスを開始します。[閉じる] ボタンをクリックして画面を閉じます。

第 5 章

ポリシー設定

[エージェント] 画面で提供される設定 (即座に処理が実行される 1 回限りのコマンド) と異なり、**ポリシー**設定ではエージェントへの長期的な配信について指定します。

エージェントをさまざまなグループにまとめ、グループを階層化したら (子グループの上に親グループ)、最上位グループに対してポリシーを設定し、次の方法でその**ポリシー**設定を各レベルに適用できます。

- ポリシーの**継承:** グループのポリシーが親グループから継承されます。
- ポリシーの**カスタマイズ:** StellarOne の管理サーバ画面を使用して、グループのポリシーを特定のエージェント/グループに対してカスタマイズできます。
- ポリシーの**自己管理:** グループのポリシーがローカルエージェント/グループにより自己管理されます。ローカルエージェント/グループは StellarOne の管理サーバ画面のポリシー管理から外され、現場のオペレータがポリシー設定を独自に指定できるようになります。

この章の内容は次のとおりです。

[ポリシー] 画面について

StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。[すべて] グループをクリックすると、StellarOne で管理されている 2 番目のレベルのグループ/エージェントが表示されます。対象エージェントまたはグループに移動し、対応する [ポリシーの継承] ([継承済み]、[カスタマイズ済み]、または [自己管理対象]) をクリックします。[ポリシー] 画面が表示されます。

図 5-1.　[ポリシー] 画面へのアクセス

注意

[すべて] グループの対応する [ポリシーの継承] リンクをクリックして、そのポリシー設定を確認することもできます。

図 5-2.　[ポリシー] 画面のスイッチオプション

表 5-1. [ポリシー] 画面のスイッチオプション

オプション	説明
製品	[製品] の横にあるドロップダウンボタンを使用して、[StellarProtect] と [StellarProtect (Legacy Mode)] を切り替えることができます。
ポリシーの継承	このスイッチボタンでは、親グループからのポリシーの継承を有効または無効にできます。
自己管理	このスイッチボタンでは、エージェントの自己管理を有効または無効にできます。有効にすると、エージェントは StellarOne の管理サーバ画面のポリシー管理から外されます。
一般情報/ポリシー	このタブでは、一般情報とポリシー設定の表示を切り替えることができます。

図 5-3.　[ポリシー] 画面の機能

表 5-2.　[ポリシー] 画面の機能

機能	説明
アプリケーション制御	許可リストに登録されているアプリケーションへのアクセスのみを許可することにより、保護を提供します。詳細については、51 ページの「アプリケーション制御を設定する」を参照してください。
産業用次世代ウイルス対策	産業用次世代ウイルス対策のリアルタイム検索および予約検索を設定できます。詳細については、54 ページの「産業用次世代ウイルス対策」を参照してください。
エージェントコンポーネントのアップデートスケジュール	エージェントコンポーネントのアップデートを予約できます。詳細については、60 ページの「エージェントコンポーネントのアップデートスケジュール」を参照してください。
操作の挙動異常検知	ファイルレス攻撃に対する保護を提供します。詳細については、61 ページの「操作の挙動異常検知」を参照してください。
OT アプリケーション保護	StellarProtect が認識している OT アプリケーションをブロックや制限されることなくアップデートすることによって、継続的な操作を可能にします。詳細については、65 ページの「OT アプリケーション保護」を参照してください。
DLL インジェクション対策	DLL ハイジャック攻撃に対する保護を提供します。詳細については、67 ページの「DLL インジェクション対策」を参照してください。
デバイスコントロール	USB デバイスへの不正なアクセスに対する保護を提供します。詳細については、68 ページの「デバイスコントロール」を参照してください。
ユーザ指定不審オブジェクト	疑わしいファイルによるエージェントの感染を防ぐため、ファイルのハッシュやパスを手動で追加できます。詳細については、69 ページの「ユーザ指定不審オブジェクト」を参照してください。
エージェントのパスワード	管理者は、接続しているすべてのエージェントの StellarProtect 管理者パスワードを StellarOne の管理サーバ画面から変更できます。詳細については、70 ページの「エージェントのパスワード」を参照してください。

機能	説明
Patch	管理者は、同じグループポリシー下のすべてのエージェントに Patch ファイルを配信できます。詳細については、71 ページの「Patch」を参照してください。
信頼するデジタル証明書	管理者は、ポリシー設定に新しい信頼するデジタル証明書を追加できます。詳細については、72 ページの「信頼するデジタル証明書」を参照してください。

アプリケーション制御を設定する

アプリケーション制御を有効にすると、エージェントは許可リストに登録されているアプリケーションにだけアクセスできるようになります。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. 対象エージェントまたはグループに移動し、[ポリシーの継承] リンクをクリックします。
4. [アプリケーション制御] セクションに移動します。
5. 次の 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が起動すると、そのアプリケーションは許可され、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が起動すると、そのアプリケーションはブロックされ、ユーザは通知を受け取ります。
   - 無効: アプリケーション制御は無効になります。

注意

許可リストの除外の設定方法については、52 ページの「除外パスを設定する」を参照してください。

除外パスを設定する

アプリケーション制御を有効すると、エージェントは許可リストに登録されているアプリケーションにだけアクセスできるようになります。ただし、**除外パス**を使用すれば、許可リストに対する制御の除外を設定することができます。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. 対象のエージェントまたはエージェントグループに移動します。
4. 次のいずれかの方法で、[ポリシー] ページに移動します。
   - [ポリシーの継承] リンクをクリックします。
   - [処理] 見出しの下にあるポリシーアイコンをクリックしてから、[ポリシー] タブをクリックします。
5. [アプリケーション制御] 機能の下にある [除外パス] をクリックします。
   - 除外パスを追加する場合:
     a. [+追加] ボタンをクリックすると、ポップアップ画面が表示されます。
     b. [フォルダ]、[ファイル]、または [正規表現] を選択し、対応するテキストフィールドに必要な情報を入力します。

注意

実際のパスまたはハードリンクパスのみがサポートされています。

c. [追加] をクリックして、許可リストに対する除外パスの追加を完了します。

- 既存の除外パスを編集する場合:
  a. 編集する除外パスを選択し、[処理] 見出しの下にある対応する編集アイコンをクリックします。
  b. ポップアップ画面が表示されます。[フォルダ]、[ファイル]、または [正規表現] を選択し、対応するテキストフィールドを編集します。
  c. [保存] をクリックして、許可リストに対する除外パスの編集を完了します。
- 複数の既存の除外パスを削除する場合:
  a. 既存の除外パスの横にあるチェックボックスをオンにします。
  b. [+追加] ボタンの横にある [削除] ボタンをクリックします。
  c. 警告メッセージ画面が表示されます。[確認] をクリックして、選択した項目を削除します。
- 1 つの既存の除外パスを削除する場合:
  a. 削除する除外パスを選択し、[処理] 見出しの下にある対応する削除アイコンをクリックします。
  b. 警告メッセージ画面が表示されます。[確認] をクリックして、選択した項目を削除します。

産業用次世代ウイルス対策

産業用次世代ウイルス対策は、ICS の信頼の基点と高度な脅威検索を提供して、操作を中断することなくエンドポイントを保護します。関連する設定は次のとおりです。

- 54 ページの「リアルタイムの不正プログラム検索」
- 55 ページの「予約検索」

リアルタイムの不正プログラム検索

リアルタイムの不正プログラム検索では、エンドポイントで継続的なファイル検索が実行されます。ファイルを受信、ダウンロード、コピー、または変更したり開いたりするたびにセキュリティ評価のための検索が行われ、セキュリティ脅威が検出されなかったファイルはアクセスが可能になります。一方、セキュリティリスクまたはウイルス/不正プログラムの可能性が検出された場合には、感染したファイルおよび具体的なセキュリティリスクを示す通知メッセージが表示されます。

さらに、検索のキャッシュが継続的に保持され、**リアルタイムの不正プログラム検索**が実行されるたびに再ロードされます。**リアルタイムの不正プログラム検索**では、この機能が無効になってファイルが検索のキャッシュからアンロードおよび削除されるまで、ファイルやフォルダに対して行われたすべての変更が追跡されます。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. 対象のエージェントまたはエージェントグループに移動し、[ポリシーの継承] リンクをクリックします。
4. [産業用次世代ウイルス対策] セクションの [リアルタイムの不正プログラム検索] に移動します。
5. スイッチをクリックしてオンにすることにより、[リアルタイムの不正プログラム検索] を有効にします。

注意

検索するファイルタイプ、セキュリティリスクの可能性の検出後の処理、および検索除外リストの設定については、57 ページの「詳細設定」を参照してください。

機械学習型検索

機械学習型検索は、インテリジェントな機械学習テクノロジを使用して脅威情報を相関するとともに、デジタル DNA フィンガープリンティングや API マッピングなどのファイルプロパティを利用した詳細なファイル分析を実行して、新たに出現した未知のセキュリティリスクを検出します。また、未知のプロセスやあまり広まっていないプロセスに対して挙動分析を行い、新たに出現した未知の脅威がネットワークを侵害しようとしていないか確認します。**機械学習型検索**は、未知の脅威やゼロデイ攻撃から資産やネットワーク環境を保護するのに役立つ強力なツールです。

[機械学習型検索] 機能を有効にするには、[リアルタイムの不正プログラム検索] を有効にした後、このチェックボックスにチェックをオンにします。

予約検索

ウイルス対策の定期的な検索予約をカスタマイズすることで、技術オペレータの負荷を減らすことができます。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. 対象のエージェントまたはエージェントグループに移動し、[ポリシーの継承] リンクをクリックします。
4. [産業用次世代ウイルス対策] セクションの [予約検索] に移動します。
5. スイッチをクリックしてオンにすることにより、[予約検索] 機能を有効にします。
6. カレンダーアイコンをクリックします。[予約] 画面が表示されます。

7. 次のいずれかのラジオボタンを選択して、検索の実行間隔を指定します。

   - **日次:** 検索を毎日実行します。
   - **週次:** 検索を毎週実行します (初期設定は毎週日曜日)。
   - **月次:** 検索を毎月実行します (初期設定は 1 日)。

重要

すべての月に 29、30、31 日があるわけではない (たとえば 2 月は 28 日、うるう年には 29 日しかない) ため、月次のアップデートには 29、30、31 日を選択しないことをお勧めします。これにより、29、30、31 日のない月もアップデートが行われるようになります。

8. [開始時刻] に検索の開始時刻を指定します (初期設定は 00:00)。
9. [確認] をクリックして設定を完了します。

注意

検索するファイルタイプ、セキュリティリスクの可能性の検出後の処理、および検索除外リストの設定については、57 ページの「詳細設定」を参照してください。

詳細設定

[リアルタイムの不正プログラム検索] および [予約検索] の [詳細設定] では、検索するファイルタイプ、セキュリティリスクの可能性の検出後の処理、および検索除外リストに関する追加の設定を指定できます。

リアルタイムの不正プログラム検索の詳細設定

手順

1. [エージェント]→[ポリシー]→[産業用次世代ウイルス対策] の順に選択します。
2. [リアルタイムの不正プログラム検索] セクションで [詳細設定] をクリックします。
3. [詳細設定] 画面が表示されます。
4. この設定画面は、[検索対象ファイル]、[検出時の処理]、および [検索除外] の 3 つのセクションから構成されています。
5. [検索対象ファイル] セクションで、次の設定を行います。
   - [圧縮ファイルを検索] チェックボックスをオンにし、圧縮ファイルの [最大階層] を 1〜20 の間で指定します。
   - 特定のサイズを超えるファイルをスキップするには、[(任意の値) MB を超えるファイルをスキップ] チェックボックスをオンにし、ファイルサイズを 1〜9999MB の間で指定します。指定したファイルサイズを超えるファイルは検索されません。
6. [検出時の処理] セクションでは、検索プロセスで脅威が検出された場合の処理を事前に指定します。検出された疑わしいファイルを隔離フォルダに移動してさらにチェックするには、[隔離] を選択します。結果を読み出すだけで、疑わしいファイルに対して処理を実行しない場合は、[処理しない] を選択します。
7. [検索除外] セクションでは、特定のフォルダ、ファイル、またはファイル拡張子を検索の対象から除外することを選択できます。
   - **フォルダ:** 検索から除外するフォルダのパスを指定します。
   - **ファイル:** 検索から除外するファイルのパスを指定します。
   - **ファイル拡張子:** 検索から除外する特定ファイルの拡張子を指定します。

注意

- [検索除外] ではローカルパスのみがサポートされます。URL や\\[ホスト名] などのリモートパスはサポートされません。
- ファイル拡張子の前に「.」や「*.」を追加する必要はありません。

ヒント

フォルダ/ファイルのパスまたはファイル拡張子を追加または削除するには、[+] または [-] アイコンをクリックします。

8. [確認] をクリックして、リアルタイムの不正プログラム検索の詳細設定を完了します。

予約検索の詳細設定

手順

1. [エージェント]→[ポリシー]→[産業用次世代ウイルス対策] の順に選択します。
2. [予約検索] セクションで [詳細設定] をクリックします。
3. [詳細設定] 画面が表示されます。
4. この設定画面は、[検索対象ファイル]、[検出時の処理]、および [検索除外] の 3 つのセクションから構成されています。
5. [検索対象ファイル] セクションでは、すべてのファイルを詳細に検索するには [すべてのローカルフォルダ] を、全般的な検索を実行するには [初期設定のフォルダ (クイック検索)] を、検索対象のフォルダのパスを指定するには [特定のフォルダ] をクリックします。

ヒント

[特定のフォルダ] オプションでは、[+] または [-] アイコンをクリックして、特定のフォルダへのパスを追加または削除します。

- (オプション) [圧縮ファイルを検索] チェックボックスをオンにし、圧縮ファイルの [最大階層] を 1〜20 の間で指定します。
- (オプション) 特定のサイズを超えるファイルをスキップするには、[(任意の値) MB を超えるファイルをスキップ] チェックボックスをオンにし、ファイルサイズを 1〜9999MB の間で指定します。指定したファイルサイズを超えるファイルは検索されません。

6. [検出時の処理] セクションでは、検索プロセスで脅威が検出された場合の処理を事前に指定します。検出された疑わしいファイルを隔離フォルダに移動してさらにチェックするには、[隔離] を選択します。結果を読み出すだけで、疑わしいファイルに対して処理を実行しない場合は、[処理しない] を選択します。

7. (オプション) [検索除外] セクションでは、特定のフォルダ、ファイル、またはファイル拡張子を検索の対象から除外することを選択できます。

   - **フォルダ:** 検索から除外するフォルダのパスを指定します。
   - **ファイル:** 検索から除外するファイルのパスを指定します。
   - **ファイル拡張子:** 検索から除外する特定ファイルの拡張子を指定します。

   注意

   - [検索除外] ではローカルパスのみがサポートされます。URL や\\[ホスト名] などのリモートパスはサポートされません。
   - ファイル拡張子の前に「.」や「*.」を追加する必要はありません。

   ヒント

   特定のフォルダ/ファイルのパス、または特定のファイルタイプのファイル拡張子を追加または削除するには、[+] または [-] アイコンをクリックします。

8. [確認] をクリックして、予約検索の詳細設定を完了します。

エージェントコンポーネントのアップデートスケジュール

StellarOne の管理サーバ画面を使用して、StellarProtect エージェントコンポーネントのアップデートスケジュールを設定できます。コンポーネントのアップデートは指定された時間間隔で自動的に実行されます。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. 対象のエージェントまたはグループに移動し、対応する [ポリシーの継承] リンクをクリックします。
4. [ポリシー] タブページの [エージェントコンポーネントのアップデートスケジュール] セクションで、[予約アップデート] をオンにします。

ヒント

先に StellarOne の管理サーバ画面でコンポーネントのアップデートスケジュール設定を確認してから、エージェントコンポーネントのアップデートスケジュールを設定することをお勧めします。

5. (オプション) [StellarOne 検索コンポーネントのアップデートスケジュールに移動] をクリックし、StellarOne のコンポーネントのアップデートスケジュールに対する現在の設定を確認します。

注意

StellarOne のコンポーネントのアップデートスケジュールを編集できるのは、管理者またはオペレータアカウントでログインしているユーザのみです。

6. [予約アップデート] をオンにすると、[実行間隔] と [開始時刻] を設定するためのラジオボタンが表示され、エージェントコンポーネントのアップデートを予約することができます。

   - **週次**のアップデートの初期設定は**毎週日曜日**です。
   - **月次**のアップデートの初期設定は **1 日**です。
   - **開始時刻**の初期設定は 20:00 です。

重要

すべての月に 29、30、31 日があるわけではない (たとえば 2 月は 28 日、うるう年には 29 日しかない) ため、月次のアップデートには [月の最後の日] を選択することをお勧めします。これにより、29、30、31 日のない月もアップデートが行われるようになります。

操作の挙動異常検知

StellarProtect では、**操作の挙動異常検知**によりファイルレス攻撃からエージェントを保護します。

StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。[エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。対象エージェントまたはグループに移動し、[ポリシーの継承] リンクをクリックします。

下にスクロールし、[操作の挙動異常検知] セクションに移動します。基本的には、[操作の挙動異常検知] には次の 4 つのモードがあります。

- **学習:** 未承認のプログラムの呼び出しを監視し、それらを信頼する操作リストに追加します。これにより、エージェントは OT 関連プログラムの呼び出しの挙動について継続的に詳しく学習します。
- **検出:** 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:** 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ージェントを保護します。

- **無効:** [操作の挙動異常検知] は無効になり、ファイルレス攻撃に対する保護がオフになります。

注意

- **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、ウイルス対策をさらに強化することができます。詳細については、62 ページの「アグレッシブモード」を参照してください。
- 操作やプロセスで使用されている、悪用されることの多いアプリケーションを**ウォッチリスト**に手動で追加することで、セキュリティ監視を強化できます。詳細については、64 ページの「ウォッチリスト」を参照してください。

アグレッシブモード

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、ウイルス対策をさらに強化することができます。この機能は、監視タスクにパラメータの識別を追加し、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のチェックを可能にすることで保護を強化します。

注意

アグレッシブモードでは、監視対象の操作プロセスからの識別されたパラメータを持つ承認された呼び出しのみを許可することにより、最大限のセキュリティを確保するための厳密なルールが実行されます。

アグレッシブモードのしくみの例を示します。

1. [操作の挙動異常検知] で [学習] モードを選択し、次のプロセスが学習されたとします。
   - `explorer.exe → cmd.exe → powershell.exe → script.ps1 argument1`

2. [検出] または [施行] モードに切り替えた場合、[アグレッシブモード] が無効であれば、識別されないパラメータを持っていても承認されたプログラムの呼び出しはブロックされないため、次のプロセスは許可されます。

   - `explorer.exe → cmd.exe → powershell.exe → script.ps1 argument2`

   注意

   `argument2` はプロセスに渡される新しいデータであり、プロセスのパラメータを変更しますが、[アグレッシブモード] が無効な場合はプロセスの未承認のアプリケーションとはみなされません。

3. [アグレッシブモード] が有効な場合は、[検出] または [施行] モードであっても次のプロセスは許可されません。

   - `explorer.exe → cmd.exe → powershell.exe → script.ps1 argument2`

   注意

   [アグレッシブモード] が有効な場合、`argument2` はブロックする必要がある未承認のパラメータとして検出されます。

4. つまり、[アグレッシブモード] が有効な場合は、厳密に同じ (手順 1 で学習した) 次のプロセスのみが許可されます。

   - `explorer.exe → cmd.exe → powershell.exe → script.ps1 argument1`

ウォッチリスト

操作やプロセスで使用されている、悪用されることの多いアプリケーションを**ウォッチリスト**に手動で追加することで、セキュリティ監視を強化できます。[操作の挙動異常検知] が有効な場合、初期設定では、`Powershell.exe`、`wscript.exe`、`cscript.exe`、`mshta.exe`、`psexec.exe` が監視されます。

手順

1. [エージェント]→[ポリシーの継承] の順にクリックし、下にスクロールして [操作の挙動異常検知] セクションに移動します。[学習]、[検出]、または [施行] を選択して、[操作の挙動異常検知] を有効にします。

   注意

   [操作の挙動異常検知] の初期設定は [無効] です。[操作の挙動異常検知] を有効にしないと、プロセスの監視は有効になりません。

2. StellarProtect で監視する初期設定のアプリケーションのほかに、他のアプリケーションを監視対象として追加する必要がある場合は、[ウォッチリスト] リンクをクリックします。
3. [ウォッチリスト] 画面が表示されます。[+追加] をクリックして、監視するアプリケーションを指定します。
4. [追加] をクリックすると、追加したアプリケーションが [監視対象アプリケーション] リストに表示されます。
5. [閉じる] をクリックして画面を閉じます。

   注意

   追加したアプリケーションを削除するには、[処理] の下にあるごみ箱アイコンをクリックします。

6. エージェントイベントログを表示して、異常な操作やプロセスが検出されているかどうか確認できます。詳細については、74 ページの「エージェントイベント」を参照してください。

OT アプリケーション保護

OT アプリケーション保護は、産業ベースの変更管理保護です。この機能は、StellarProtect により認識されている OT アプリケーションをブロックも制限もなしにアップデートすることを可能にします。また、OT アプリケーション保護を有効にして、認識されている OT アプリケーションの実行可能バイナリファイルをセキュリティで保護することもできます。

注意

StellarProtect は起動時に、現在インストールされている OT アプリケーションを自動検出して保護します。認識されている OT アプリケーションは、[一般情報] タブページに表示されます。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. 対象のエージェントまたはエージェントグループに移動し、[処理] 見出しの下にあるポリシーアイコンをクリックします。
4. [一般情報] 画面が表示されます。StellarProtect エージェントにより自動的に認識された OT アプリケーションを確認します。

注意

新しい OT アプリケーションをインストールする前に、必ず**メンテナンスモード**を有効にしてください。インストールプロセスの終了後、**メンテナンスモード**を無効にすると、新たに追加された OT アプリケーションが自動的に再検索されます。検出された新しいアプリケーションは、OT アプリケーション保護リストに追加されます。この機能を有効にする方法については、37 ページの「メンテナンスモードを設定する」を参照してください。

5. アプリケーションのインストールパスを手動で保護リストに追加することもできます。

   a. [ポリシー] タブをクリックし、下にスクロールして、画面左側の [OT アプリケーション保護] セクションに移動します。

   b. [OT アプリケーション保護] のスイッチがオンになっていることを確認します。

   c. [ファイル/フォルダ] をクリックすると、ポップアップ画面が表示されます。

   d. [+追加] ボタンをクリックしてから [フォルダ] または [ファイル] を選択し、対応するテキストフィールドにフォルダまたはファイルのパスを指定します。

   注意

   初期設定では、選択したフォルダおよびそのサブフォルダ内の PE ファイル (`.exe` および `.dll`) のみが保護されます。

   e. (オプション) 選択したフォルダ内のすべてのファイルを保護するには、[実行可能ファイルのみ] チェックボックスをオフにします。

   ヒント

   [実行可能ファイルのみ] チェックボックスをオフにすることにより、選択したフォルダ内にある機密ファイルや設定などのファイルが変更されることを防ぐことができます。

   f. [追加] をクリックして設定を完了します。

6. ユーザ指定のプロセスを追加することもできます。

   a. [ポリシー]→[OT アプリケーション保護] に移動し、[承認プロセス] オプションをクリックします。

   b. ポップアップ画面が表示されます。[+追加] ボタンをクリックし、対応するテキストフィールドに承認プロセスを指定します。

重要

承認プロセスを追加することで、他のアプリケーションを信頼するアプリケーションとして設定したり、これまでに指定した保護対象ファイル/フォルダや、エージェントにより検出された OT アプリケーションの PE ファイルを変更したりすることができます。承認プロセスとして悪意のあるファイルが設定されている場合、このファイルによる OT アプリケーションの変更を阻止することはできないことに注意してください。これは、そのファイルが StellarProtect の監視プロセスからすでに除外されているためです。ユーザ指定の承認プロセスを追加する前に、そのプロセスが安全であることを確認してください。

c. [追加] をクリックして設定を完了します。

DLL インジェクション対策

DLL インジェクション対策は、DLL ハイジャック攻撃に対する保護を提供します。

注意

DLL インジェクション対策は x86 プラットフォームでのみサポートされています。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。
3. StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。対象のエージェントまたはグループに移動し、対応する [ポリシーの継承] リンクをクリックします。
4. 下にスクロールして、画面左側の [DLL インジェクション対策] セクションに移動します。
5. [DLL インジェクションをブロックする] スイッチをクリックして有効にします。

デバイスコントロール

StellarProtect エージェントでは、現場での 1 回限りの USB アクセス権限がサポートされています。一方、StellarOne の管理サーバ画面では、リモート設定を介した永続的な USB アクセス権限が提供されます。ローカルエージェントでは、USB デバイスコントロールが有効になっている場合、ユーザが USB デバイスを挿入するたびに、USB デバイスのアクセスが許可されているかどうかを確認するメッセージが表示されます。これに加え、管理者またはオペレータのロールを持つ StellarOne ユーザは、信頼する USB デバイスを**デバイスコントロールリスト**に追加することで、指定したデバイスのさらなるチェックなしでのアクセスを許可して、信頼する USB デバイスのアクセスを永続的に容易にすることができます。

手順

1. [エージェント] 画面に移動します。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. 対象のエージェントまたはグループに移動し、[ポリシーの継承] 見出しの下にある対応するリンクをクリックします。
4. [デバイスコントロール] のスイッチがオンになっていることを確認します。
5. [追加] をクリックします。[信頼する USB デバイスの追加] 画面が表示されます。
6. 信頼する USB デバイスについて、次の情報を 1 つ以上指定します。
   - **ベンダ ID**
   - **製品 ID**
   - **シリアル番号**
7. [OK] をクリックして設定を完了します。
8. USB デバイスがデバイスコントロールリストに追加されていることを確認します。
9. (オプション) USB デバイス情報を編集するには、USB デバイスを選択し、[処理] 見出しの下にある編集アイコンをクリックします。ポップアップ画面が表示されます。関連するテキストフィールドで USB デバイス情報を編集し、[OK] をクリックします。

10. (オプション) 信頼するリストから USB デバイスを削除するには、次のいずれかの手順を実行します。

    - 複数の USB デバイスを同時に削除するには、該当する USB デバイスを選択し、[+追加] ボタンの横にある [削除] ボタンをクリックします。
    - 1 つの USB デバイスのみを削除するには、[処理] 見出しの下にある編集アイコンをクリックします。

    [通知] ポップアップ画面が表示されます。[確認] をクリックして USB デバイスを削除します。

ユーザ指定不審オブジェクト

ユーザ指定不審オブジェクト機能では、新しい IOC (セキュリティ侵害インジケータ) のファイルハッシュ (SHA-1 または SHA-2) やパスをブロックするファイルのリストに手動で追加することによって、管理下のエージェントが悪意のあるファイルにより感染するのを防ぐことができます。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. 対象のエージェントまたはグループに移動し、対応する [ポリシーの継承] リンクをクリックします。
4. 下にスクロールして、画面右側の [ユーザ指定不審オブジェクト] セクションに移動します。
5. [追加] をクリックします。[ユーザ指定不審オブジェクトに項目を追加] 画面が表示されます。
6. 不審なファイルタイプとして、[ハッシュ] または [ファイルパス] を選択します。
7. 対応するテキストフィールドにファイルハッシュまたはパスを指定します。
8. (オプション) [メモ] テキストフィールドにメモを入力します。
9. [OK] をクリックしてタスクを完了します。

エージェントのパスワード

この機能を使用すると、OT 管理者は、接続しているすべてのエージェントの StellarProtect 管理者パスワードを StellarOne の管理サーバ画面から変更できます。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。対象のエージェントまたはグループに移動し、対応する [ポリシーの継承] リンクをクリックします。
2. 下にスクロールして、画面右側の [エージェントのパスワード] セクションに移動します。
3. 新しいパスワードを 2 回入力し、[保存] をクリックしてポリシー設定を完了します。

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。次の記号および空白は使用できません。| > " : < \

Patch

Patch 機能を使用すると、管理者は、同じグループポリシー下のすべてのエージェントに Patch ファイルアップグレードを配信できます。Patch 適用処理はポリシー同期を使用してリモートかつ自動的に実施されます。各グループポリシーでは、一度に 1 つの Patch ファイル (エージェントバージョン) のみをアップグレードできます。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。対象のエージェントまたはグループに移動し、対応する [ポリシーの継承] リンクをクリックします。
2. 下にスクロールして、画面右下の [Patch] セクションに移動します。
3. 配信する Patch ファイルのバージョンの横にあるチェックボックスをオンにします。

> **注意**
>
> エージェントに対する新しい Patch は、[ダウンロード/アップデート] ページ (103 ページ) でインポートできます。

4. 選択した Patch ファイルが、同じグループポリシー下のエージェントに配信されます。

> **注意**
>
> 複数のデバイスに Patch を適用する際、StellarProtect ではすべてのエージェントを対象としたグローバルポリシーとグループ所有のマシンを対象としたグループポリシーを使用できるため、エージェントバージョンを選択する場合は次の点に注意してください。
>
> - エージェントの初期設定のポリシーはグローバルポリシーです。他のグループに移動する前のすべてのエージェントにはこのポリシーが適用されます。
> - Patch を配信するエージェントバージョンを設定しない場合は、[Patch] セクションで、エージェントバージョンの Patch ファイルの横にあるすべてのチェックボックスをオフにしてください。

信頼するデジタル証明書

信頼するデジタル証明書は、新しい信頼するデジタル証明書を管理者が追加できる重要な機能を提供します。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[エージェント] タブをクリックします。
2. [エージェント] 画面で [すべて] グループをクリックします。StellarOne で管理されているエージェントのリストが [エージェント] 画面に表示されます。
3. 対象のエージェントまたはグループに移動し、[ポリシーの継承] 見出しの下にある対応するリンクをクリックします。
4. [ポリシー]→[信頼するデジタル証明書] に移動します。
5. [インポート] をクリックして、選択した信頼するデジタル証明書ファイルをインポートします。
6. 信頼するデジタル証明書を削除するには、次のいずれかの手順を実行します。
   - 複数の信頼するデジタル証明書を同時に削除するには、該当する証明書を選択し、[+追加] ボタンの横にある [削除] ボタンをクリックします。
   - 1 つの証明書のみを削除するには、[処理] 見出しの下にある編集アイコンをクリックします。

   [通知] ポップアップ画面が表示されます。[確認] をクリックして、選択した証明書を削除します。

第 6 章

ログ

この章では、StellarOne で生成されたログや StellarProtect エージェントに関連するログにアクセスする方法、および高度な管理のためのログの詳細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。

エージェントイベント

StellarOne はエージェントのアクティビティを収集し、エージェントイベントログに記録します。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[ログ] タブにマウスを重ねます。[エージェントイベント] オプションをクリックします。
2. [StellarProtect] タブをクリックして、StellarProtect のエージェントイベントログを表示します。
3. トラブルシューティングや分析に関連するログメッセージの検索方法については、76 ページの「エージェントイベントログのフィルタリング」を参照してください。

注意

イベント ID や対応するログ情報の詳細については、付録の 122 ページの「StellarProtect のエージェントイベントログの説明」を参照してください。

[エージェントイベント] 画面について

図 6-1. StellarProtect のエージェントイベントログ

表 6-1. [エージェントイベント] 画面について

項目	説明
(1) エクスポート	[エクスポート] ボタンをクリックすることにより、ログリストを .csv ファイルとしてエクスポートできます。次の項目を含むドロップダウンメニューが表示されます。 • **選択内容のエクスポート:** エクスポートするログの横にあるチェックボックスをオンにすると、このボタンが有効になります。 • **すべてエクスポート:** このボタンは常に有効であり、すべてのログをエクスポートします。
(2) フィルタ	トラブルシューティングや分析に関連するログメッセージを検索できます。詳細については、76 ページの「エージェントイベントログのフィルタリング」を参照してください。
(3) ログの表示設定	次のいずれかを指定して、表示するログの数をカスタマイズできます。 • 最新のログレコードの数 • 特定の期間内に生成されたログ
(4) 画面の表示設定	このボタンをクリックすると、次の方法で画面の表示をカスタマイズできます。 • 1 ページに表示するログの数を選択する。 • [表をカスタマイズ] 画面で、[日時]、[重大度]、[ユーザ ID]、[クライアント IP]、または [メッセージ] チェックボックスをオフにして、特定の内容を非表示にする。
(5) 表示の更新	画面の表示を手動で更新して、最新のログ出力を表示できます。
(6) 処理	イベント情報やエージェント情報など、イベントの詳細を表示して印刷できます。

エージェントイベントログのフィルタリング

ここでは、**エージェントイベント**ログをフィルタリングして、最も関連するログメッセージを見つける方法について説明します。

手順

1. [ログ]→[エージェントイベント]→[StellarProtect] の順に選択します。検索バーの横にある [エージェント名] をクリックして、ドロップダウンメニューを表示します。
2. ドロップダウンメニューから、2 種類のログフィルタリングを実行できます。必要に応じて、次のいずれかの方法を選択します。
   - [エージェント名]、[IP アドレス]、[IP アドレスの範囲]、または [説明] を選択してから、検索フィールドに検索文字列を入力します。
   - [エージェントグループ]、[イベントのタイプ]、または [重大度] を選択して、下向き矢印付きの検索ボックスを表示します。この矢印をタップすると、各カテゴリのオプションが表示されます。
     - **エージェントグループ:** [グループの選択] 画面が表示されます。1 つのグループを選択し、[確認] をクリックして、そのログレコードを表示します。
     - **イベントのタイプ:** イベントタイプオプションを含むドロップダウンメニューが表示されます。いずれかのタイプを選択して、関連するログレコードを表示します。

       注意

       さまざまなイベントタイプの詳細については、122 ページの「StellarProtect のエージェントイベントログの説明」を参照してください。

     - **重大度:** [警告]、[重大]、および [情報] の各オプションを含むドロップダウンメニューが表示されます。いずれかのオプションを選択して、レベルごとのログレコードを表示します。
3. 検索バーの横にある検索アイコンをクリックして、検索結果を画面に表示します。
4. 検索条件をクリアするには、[エクスポート] ボタンの上に表示されているフィルタリング条件を閉じます。

サーバイベント

StellarOne サーバ上のアクティビティ、および StellarOne から StellarProtect エージェントに配信された設定がログに記録され、[サーバイベント] 画面に表示されます。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[ログ] タブにマウスを重ねます。[サーバイベント] オプションをクリックします。
2. [StellarProtect] タブをクリックすると、StellarOne から StellarProtect エージェントに配信された設定イベントが表示されます。
3. [StellarOne] タブをクリックすると、StellarOne のサーバイベントログが表示されます。

[サーバイベント] 画面について

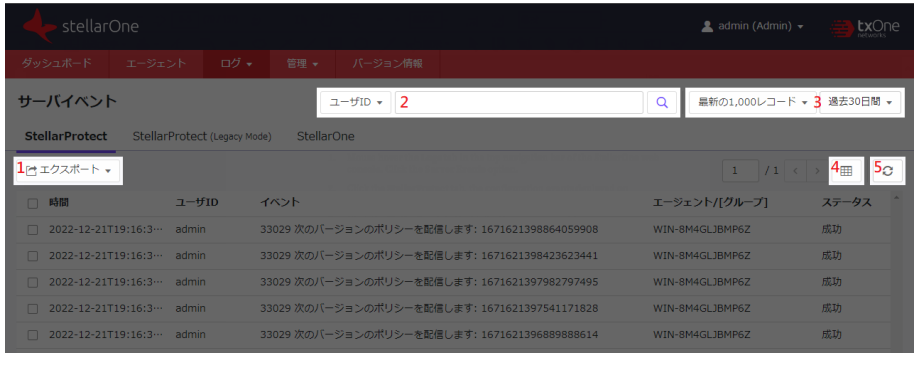


図 6-2.　SterllarProtect のサーバイベントログ

表 6-2. StellarProtect の [サーバイベント] 画面について

項目	説明
(1) エクスポート	[エクスポート] ボタンをクリックすることにより、ログリストを .csv ファイルとしてエクスポートできます。次の項目を含むドロップダウンメニューが表示されます。 • **選択内容のエクスポート:** エクスポートするログの横にあるチェックボックスをオンにすると、このボタンが有効になります。 • **すべてエクスポート:** このボタンは常に有効であり、すべてのログをエクスポートします。
(2) フィルタ	トラブルシューティングや分析に関連するログメッセージを検索できます。手順については、79 ページの「サーバイベントログのフィルタリング」を参照してください。
(3) ログの表示設定	次のいずれかを指定して、表示するログの数をカスタマイズできます。 • 最新のログレコードの数 • 特定の期間内に生成されたログ
(4) 画面の表示設定	このボタンをクリックすると、次の方法で画面の表示をカスタマイズできます。 • 1 ページに表示するログの数を選択する。 • [表をカスタマイズ] 画面で、[日時]、[重大度]、[ユーザ ID]、[クライアント IP]、または [メッセージ] チェックボックスをオフにして、特定の内容を非表示にする。
(5) 表示の更新	画面の表示を手動で更新して、最新のログ出力を表示できます。

サーバイベントログのフィルタリング

ここでは、**サーバイベントログ**をフィルタリングして、最も関連するログメッセージを見つける方法について説明します。

手順

1. [ログ]→[サーバイベント]→[StellarProtect] の順に選択します。検索バーの横にある [ユーザ ID] をクリックして、ドロップダウンメニューを表示します。
2. ドロップダウンメニューから、2 種類のログフィルタリングを実行できます。必要に応じて、次のいずれかの方法を選択します。
   - [ユーザ ID] または [エージェント名] を選択してから、検索フィールドに検索文字列を入力します。
   - [グループ名] または [イベントのタイプ] を選択して、下向き矢印付きの検索ボックスを表示します。この矢印をタップすると、各カテゴリのオプションが表示されます。
   - **グループ名:** [グループの選択] 画面が表示されます。1 つのグループを選択し、[確認] をクリックして、そのログレコードを表示します。
   - **イベントのタイプ:** イベントタイプオプションを含むドロップダウンメニューが表示されます。いずれかのタイプを選択して、関連するログレコードを表示します。

   注意

   さまざまなイベントタイプの詳細については、135 ページの「StellarProtect のサーバイベントログの説明」を参照してください。
3. 検索バーの横にある検索アイコンをクリックして、検索結果を画面に表示します。
4. 検索条件をクリアするには、[エクスポート] ボタンの上に表示されているフィルタリング条件を閉じます。

注意

イベント ID や対応するログ情報の詳細については、付録の 135 ページの「StellarProtect のサーバイベントログの説明」および 137 ページの「StellarOne のサーバイベントログの説明」を参照してください。

システムログ

StellarOne サーバにより生成された内部システムプロセスがログに記録され、[システムログ] 画面に表示されます。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[ログ] タブにマウスを重ねます。
2. [システムログ] オプションをクリックします。
3. [システムログ] 画面が表示されます。

[システムログ] 画面について

図 6-4. [システムログ] 画面

表 6-4. [システムログ] 画面について

項目	説明
エクスポート	[エクスポート] ボタンをクリックすることにより、ログリストを.csv ファイルとしてエクスポートできます。次の項目を含むドロップダウンメニューが表示されます。 • **選択内容のエクスポート:** エクスポートするログの横にあるチェックボックスをオンにすると、このボタンが有効になります。 • **すべてエクスポート:** このボタンは常に有効であり、すべてのログをエクスポートします。
フィルタ	検索バーで特定の重大度レベルを選択するか直接指定することにより、ログをフィルタリングできます。重大度レベルは次のとおりです。 • 警告 • 注意 • 情報 • デバッグ • 緊急 • アラート • 重大 • エラー 検索条件を設定して検索ボタンをクリックすると、検索結果が表示されます。フィルタリング条件は [エクスポート] ボタンの上に表示されています。検索条件をクリアして元の画面に戻るには、フィルタリング条件を閉じます。
ログの表示設定	次のいずれかを指定して、表示するログの数をカスタマイズできます。 • 最新のログレコードの数 • 特定の期間内に生成されたログ
画面の表示設定	このボタンをクリックすると、次の方法で画面の表示をカスタマイズできます。 • 1 ページに表示するログの数を選択する。 • [表をカスタマイズ] 画面で、[日時]、[重大度]、または • [メッセージ] チェックボックスをオフにして、特定の内容を非表示にする。
表示の更新	画面の表示を手動で更新して、最新のログ出力を表示できます。

監査ログ

[監査ログ] 画面には、ログイン、ログアウト、アカウントの作成/削除などのユーザアクティビティが表示されます。

手順

1. StellarOne の管理サーバ画面の上部にあるナビゲーションバーで、[ログ] タブにマウスを重ねます。
2. [監査ログ] オプションをクリックします。
3. [監査ログ] 画面が表示されます。

[監査ログ] 画面について

図 6-5.　[監査ログ] 画面

表 6-5. [監査ログ] 画面について

項目	説明
(1) エクスポート	[エクスポート] ボタンをクリックすることにより、ログリストを.csv ファイルとしてエクスポートできます。次の項目を含むドロップダウンメニューが表示されます。 • **選択内容のエクスポート:** エクスポートするログの横にあるチェックボックスをオンにすると、このボタンが有効になります。 • **すべてエクスポート:** このボタンは常に有効であり、すべてのログをエクスポートします。
(2) フィルタ	トラブルシューティングや分析に関連するログメッセージを検索できます。詳細については、84 ページの「監査ログのフィルタリング」を参照してください。
(3) ログの表示設定	次のいずれかを指定して、表示するログの数をカスタマイズできます。 • 最新のログレコードの数 • 特定の期間内に生成されたログ
(4) 画面の表示設定	このボタンをクリックすると、次の方法で画面の表示をカスタマイズできます。 • 1 ページに表示するログの数を選択する。 • [表をカスタマイズ] 画面で、[日時]、[重大度]、[ユーザ ID]、[クライアント IP]、または [メッセージ] チェックボックスをオフにして、特定の内容を非表示にする。
(5) 表示の更新	画面の表示を手動で更新して、最新のログ出力を表示できます。

監査ログのフィルタリング

ここでは、**監査ログ**をフィルタリングして、最も関連するログメッセージを見つける方法について説明します。

手順

1. [ログ]→[監査ログ] の順に選択します。検索バーの横にある [重大度] をクリックして、ドロップダウンメニューを表示します。
2. ドロップダウンメニューから、2 種類のログフィルタリングを実行できます。必要に応じて、次のいずれかの方法を選択します。
   - [ユーザ ID] または [クライアント IP] を選択してから検索フィールドに検索文字列を入力すると、特定のユーザアカウントまたは IP アドレスに関連するログが表示されます。
   - [重大度] を選択して、下向き矢印付きの検索ボックスを表示します。この矢印をタップすると、次のオプションが表示されます。いずれかのオプションを選択して、レベルごとのログレコードを表示します。
     - 警告
     - 注意
     - 情報
     - デバッグ
     - 緊急
     - アラート
     - 重大
     - エラー
3. 検索バーの横にある検索アイコンをクリックして、検索結果を画面に表示します。
4. 検索条件をクリアするには、[エクスポート] ボタンの上に表示されているフィルタリング条件を閉じます。

第 7 章

管理

この章では、StellarOne の管理サーバ画面の管理設定について説明します。

この章の内容は次のとおりです。

アカウント管理

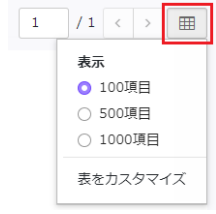
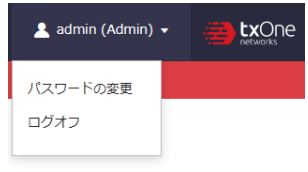
[管理]→[アカウント管理] の順に選択して、StellarOne の管理サーバ画面にアクセスするユーザアカウントを管理できます。

[アカウント管理] 画面には、[ユーザ] と [ロール] の 2 つのタブがあります。[ユーザ] タブではアカウントを管理でき、[ロール] タブでは各アカウントのさまざまな権限に関する情報を確認できます。

図 7-1.　[アカウント管理] 画面

表 7-1.　[アカウント管理] 画面 - ユーザ

項目	説明
(1) **+ユーザの追加**	StellarOne の管理サーバ画面にアクセスするためのアカウントを追加できます。手順については、91 ページの「アカウントを追加する」を参照してください。
(2) **削除**	アカウントを削除できます。手順については、93 ページの「アカウントを削除する」を参照してください。
(3) **処理**	アカウントを編集または削除できます。手順については、92 ページの「アカウントを編集する」を参照してください。

項目	説明
(4) **画面の表示設定**	 このボタンをクリックすると、次の方法で画面の表示をカスタマイズできます。 • 1 ページに表示する項目の数を選択する。 • [表をカスタマイズ] 画面で、タイトルに関連する項目のチェックボックスをオフにして、特定の内容を非表示にする。
(5) **アカウントアイコン**	 画面右上のアカウントアイコンをクリックすると、パスワードの変更またはログオフを行えます。

[ロール] タブページの詳細については、88 ページの「アカウントの種類」を参照してください。

アカウントの種類

StellarOne のユーザアカウントは、次の 3 つの種類に分類されます。

表 7-2.　StellarOne のアカウントの種類

アカウントの種類	アクセス権	権限
管理者	フルコントロール	• StellarOne 管理: システム設定を行うための権限です。 • アカウント管理: StellarOne アカウントを管理するための権限です。 • グループ管理: グループを作成、移動、または削除するための権限です。 • ポリシー設定: USB コントロールや Intelligent Runtime Learning (インテリジェントランタイム学習) など、エージェントのポリシーを定義するための権限です。
オペレータ	資産コントロール	• グループ管理: グループを作成、移動、または削除するための権限です。 • ポリシー設定: USB コントロールや Intelligent Runtime Learning (インテリジェントランタイム学習) など、エージェントのポリシーを定義するための権限です。
閲覧者	読み取りのみ	• ダッシュボード、エージェントイベントログ、エージェントのポリシー/予約レポート/通知の設定、および StellarOne の検索コンポーネント情報の読み取りのみ可能です。 • エージェントのインストーラパッケージと `Group.ini` ファイルをダウンロードできます。 • 自身のアカウントパスワードを変更できます。

サーバアカウントの概要

TXOne StellarOne では、管理サーバ画面にアクセスするためのアカウントにいくつかの権限と制限を適用できます。これらのアカウントを使用して StellarOne を設定し、StellarProtect エージェントを監視または管理します。次の表は、一般的な StellarOne のタスクと、その実行に必要なアカウントの権限を示しています。

表 7-3. StellarOne のアカウントの種類

タスク	許可されるアカウント権限		
	管理者	オペレータ	閲覧者
ダッシュボード	√	√	√
アプリケーション制御の設定	√	√	
メンテナンスモードの設定	√	√	
デバイスコントロールの設定	√	√	
信頼するファイルの追加	√	√	
信頼する USB デバイスの追加	√	√	
検索開始	√	√	
許可リストのアップデート	√	√	
エージェントコンポーネントのアップデート	√	√	
エージェントに Patch を配信	√	√	
接続の確認	√	√	
イベントログの収集	√	√	
インポート/エクスポート (許可リスト/エージェントの設定)	√	√	
編成 (タグの編集/移動/削除)	√	√	
グループポリシーの設定	√	√	
グローバルポリシーの設定	√	√	
エージェントイベントログの監視	√	√	√

タスク	許可されるアカウント権限		
	管理者	オペレータ	閲覧者
サーバイベントログの監視	√	√	
システムログの監視	√	√	
監査ログの監視	√	√	
アカウント管理	√		
シングルサインオン	√		
システム時間設定	√	√	
Syslog 転送	√	√	
ログの削除	√	√	
レポートの予約	√	√	√
通知設定	√	√	√
SMTP 設定	√	√	
プロキシ設定	√	√	
ダウンロード/アップデート	√	√	√
ファームウェアのアップデート	√		
SSL 証明書	√		
ライセンス管理	√	√	

アカウントを追加する

ここでは、StellarOne の管理サーバ画面にアクセスするためのユーザアカウントを追加する方法について説明します。

手順

1. **管理者**ロールを持つアカウントを使用して、管理サーバ画面にログオンします。

   注意

   - ここに入力するログオン資格情報では、大文字と小文字が区別されます。
   - ユーザアカウントを管理できるのは、**管理者**ロールを持つアカウントのみです。

2. [管理]→[アカウント管理] の順に選択します。
3. [ユーザの追加] ボタンをクリックすると、[ユーザアカウントの追加] 画面が表示されます。
4. [認証ソース] ([ローカル] または [SMAL ID プロバイダ]) を指定します。
   - **ローカル**ユーザを追加するには、[ID] と [名前] を指定します。
   - **SAML ID プロバイダ**ユーザを追加するには、[SAML アカウントのマッピング用メール] と [名前] を指定します。

     注意

     SAML ID プロバイダユーザがシングルサインオン (SSO) を使用してログインできるようにするには、[シングルサインオンの設定] リンクをクリックします。手順については、95 ページの「シングルサインオン」を参照してください。

   注意

   ここに入力する [ID]、[名前]、[SAML アカウントのマッピング用メール] では、大文字と小文字が区別されます。

5. **ロール:** アカウントのロールとして、[管理者]、[オペレータ]、または [閲覧者] (初期設定) を選択します。アカウント権限の詳細については、88 ページの「アカウントの種類」を参照してください。
   - **ローカル**ユーザについては、[ローカルパスワード] を指定し、確認のために再入力します。
6. **グループコントロール:** 対象のアカウントがアクセスまたは閲覧できるグループを選択します。
7. [確認] をクリックして、ユーザアカウントの作成を完了します。

アカウントを編集する

ここでは、作成したユーザアカウントを編集する方法について説明します。

手順

1. **管理者**ロールを持つアカウントを使用して、管理サーバ画面にログオンします。

注意

- ここに入力するログオン資格情報では、大文字と小文字が区別されます。
- ユーザアカウントを管理できるのは、**管理者**ロールを持つアカウントのみです。

2. [管理]→[アカウント管理] の順に選択します。
3. [処理] 列で、対象のユーザアカウントに対する編集アイコンをクリックします。
4. [ユーザアカウントの編集] 画面が表示されます。
   - **ローカル**ユーザについては、アカウントの [ロール]、[名前]、[パスワード]、[グループコントロール]、および [説明] を編集できます。
   - **SAML ID プロバイダ**ユーザについては、アカウントの [ロール]、[名前]、[グループコントロール]、および [説明] を編集できます。

注意

SAML ID プロバイダユーザがシングルサインオン (SSO) を使用してログインできるようにするには、[シングルサインオンの設定] リンクをクリックします。手順については、95 ページの「シングルサインオン」を参照してください。

5. [確認] をクリックして、ユーザアカウントの編集を完了します。

アカウントを削除する

ここでは、不要になったユーザアカウントを削除する方法について説明します。

手順

1. **管理者**ロールを持つアカウントを使用して、管理サーバ画面にログオンします。

注意

- ここに入力するログオン資格情報では、大文字と小文字が区別されます。
- ユーザアカウントを管理できるのは、**管理者**ロールでログオンしているユーザのみです。

2. [管理]→[アカウント管理] の順に選択します。
3. ユーザアカウントは次の 2 つの方法で削除できます。
   - 一度に 1 つのユーザアカウントのみを削除するには、[処理] 列で、対象のユーザアカウントに対するごみ箱アイコンをクリックします。
   - 複数のユーザアカウントを同時に削除するには、削除するユーザアカウントの横にあるチェックボックスをオンにし、[ユーザの追加] ボタンの横にある [削除] ボタンをクリックします。
4. [ユーザアカウントの削除] 画面が表示されます。
5. [確認] をクリックして、ユーザアカウントの削除を完了します。

API キーを生成する

API キーを生成し、オープン API を使用してエージェントのデータをクエリできます。各ユーザアカウントに対して API キーの有効期限を設定することで、アカウント管理の効率性が向上します。

手順

1. **管理者**ロールを持つアカウントを使用して、管理サーバ画面にログオンします。

   注意

   - ここに入力するログオン資格情報では、大文字と小文字が区別されます。

2. [管理]→[アカウント管理] の順に選択します。
3. [ユーザ] タブで、変更するユーザ ID を見つけ、画面右側の [処理] の下にある縦三点リーダーメニューのアイコンをクリックします。
4. 表示されるメニューから、[API キーの生成] オプションを選択します。
5. [API キーの生成] 画面が表示されます。日付選択機能をクリックし、表示されるカレンダーで有効期限を選択します。[確認] をクリックします。
6. API キーが生成されます。クリップボードをクリックし、生成された API キーをコピーします。

   重要

   次の手順へ進む前に、コピーした API キーのバックアップを必ず作成してください。セキュリティ上の理由から、この API キーは再度表示されません。

7. [OK] をクリックします。
8. [API の有効期限] の下の結果を確認するか、ユーザアカウントの縦三点リーダーメニューのアイコンにマウスを重ねて API キーの有効期限を表示します。

シングルサインオン

SAML ID プロバイダユーザアカウントでログオンする場合、シングルサインオンを設定できます。シングルサインオンを使用すると、1 つのログオン資格情報で複数のアプリケーションやサービスにアクセスすることができます。

手順

1. **管理者**ロールを持つアカウントを使用して、管理サーバ画面にログオンします。

注意

- ここに入力するログオン資格情報では、大文字と小文字が区別されます。

2. [管理]→[シングルサインオン] の順に選択します。
3. [ダウンロード] ボタンをクリックして、StellarOne のメタデータ XML ファイルをダウンロードします。
4. StellarOne のメタデータ XML ファイルを IdP にアップロードしてから、IdP のメタデータ XML ファイルをダウンロードします。
5. [アップロード] ボタンをクリックして IdP のメタデータ XML ファイルを StellarOne の管理サーバ画面にアップロードし、SAML 2.0 のシングルサインオン設定を完了します。

重要

IdP の設定に変更がある場合は、IdP のメタデータ XML ファイルを再度アップロードする必要があります。

6. IdP のメタデータ XML ファイルがアップロードされると、[テスト接続] ボタンが表示されます。
7. [テスト接続] ボタンをクリックして、StellarOne への接続をテストします。

注意

SAML 設定の完了後に、無効なログオンというエラーメッセージが表示されることがあります。IdP サーバのメール設定および IdP と StellarOne サーバとのシステム時間の同期を確認するには、96 ページの「シングルサインオンの問題を解決する」を参照してください。

シングルサインオンの問題を解決する

手順

1. IdP サーバの [Active Directory ユーザとコンピュータ] で [Users] フォルダを開きます。
2. シングルサインオンに使用するユーザアカウントを右クリックし、[プロパティ]→[全般] の順に選択します。
3. [電子メール] を確認します。ここに入力されているメールアドレスが、StellarOne の管理サーバ画面にアクセスするためのアカウントのメールアドレスと一致することを確認します。

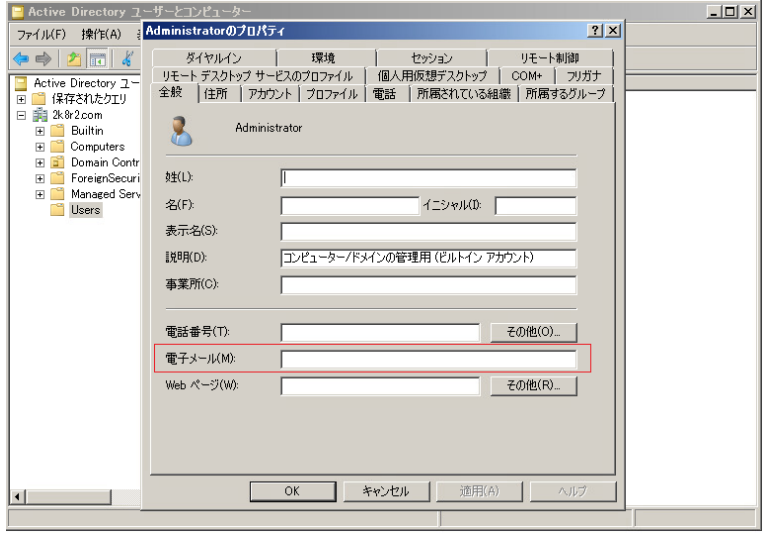


図 7-2.　シングルサインオンの問題の解決 - メールアドレスの確認

4. IdP サーバと StellarOne サーバのシステム時間が同期することを確認します。時間を同期するための推奨される設定手順は次のとおりです。

   a. IdP サーバの時間が StellarOne 仮想マシンを実行するホスト PC と同期するようにします。

   b. StellarOne の仮想マシン設定を開きます。[オプション]→[VMware Tools] の順に移動します。

   c. [ホストとゲスト時間を同期] チェックボックスをオンにして、[OK] をクリックします。

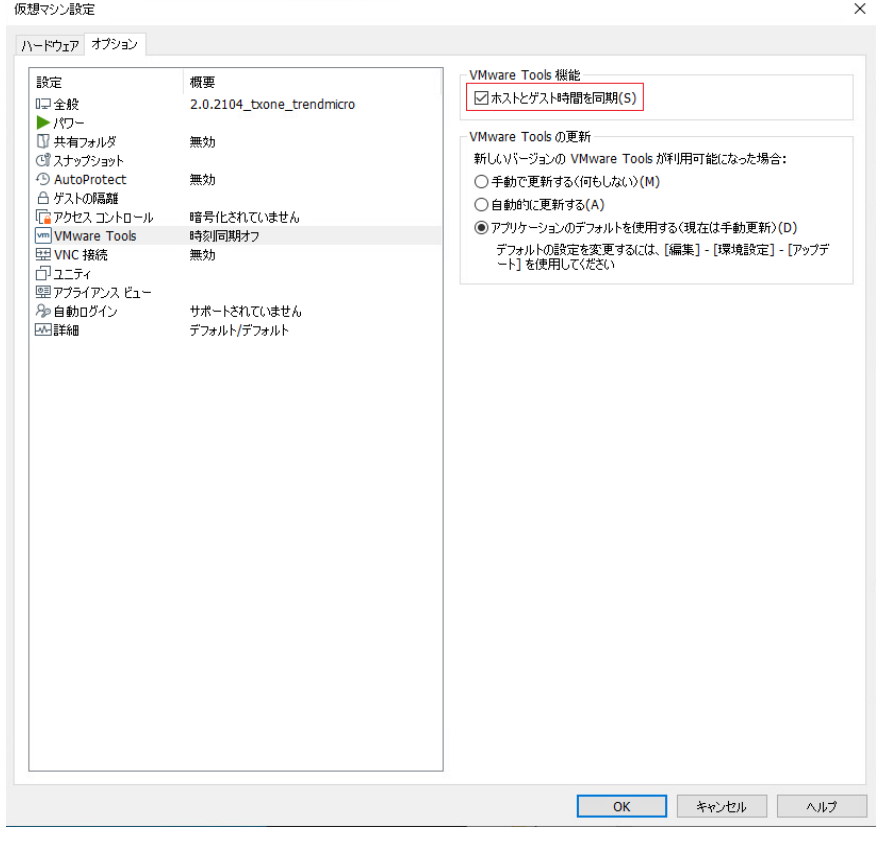


図 7-3.　仮想マシンの設定 - 時間の同期

システム時間

StellarOne の管理サーバ画面のシステム時間を設定できます。

手順

1. [管理]→[システム時間] の順に選択します。
2. [日付と時刻] セクションで、編集アイコンをクリックして日付と時間を選択します。
3. [適用] をクリックします。
4. [タイムゾーン] セクションで、空のバー内の下向き矢印をクリックします。グローバルタイムゾーンを含むドロップダウンメニューが表示されます。
5. システムに適切なタイムゾーンを選択し、[保存] をクリックして設定を完了します。

Syslog 転送

サーバイベントとエージェントイベントのログを外部 Syslog サーバに転送することで、監視および管理機能を拡張することが可能になります。TXOne StellarOne の管理サーバ画面では、ログが Common Event Format (CEF) 形式で転送されます。お使いの Syslog サーバが Common Event Format (CEF) 形式をサポートしていることを確認してください。

手順

1. [管理]→[Syslog 転送] の順に選択します。
2. [ログを Syslog サーバに転送する (CEF のみ)] スイッチをクリックして、この機能を有効にします。
3. Syslog サーバの [サーバアドレス]、[ポート]、および [プロトコル] を指定します。
4. [保存] をクリックして設定を完了します。

   Common Event Format (CEF) 形式で転送されるログの詳細については、付録の139ページの「エージェントイベントの形式」、142ページの「StellarProtectのサーバイベントの形式」、または143ページの「StellarOneのサーバイベントの形式」を参照してください。

ログの削除

この機能では、ログファイルの量を管理して、StellarOne のディスク容量の使用率を最適化できます。

手順

1. [管理]→[ログの削除] の順に選択します。
2. ログの削除設定には 2 つの方法があります。次のいずれかの方法を選択できます。
   - **今すぐ削除:**

     ログをただちに削除するにはこの設定を使用します。

     a. [次の期間を経過した] タイトルの横にあるドロップダウンメニューをクリックし、削除するログタイプを選択します。
        - すべてのログ
        - システムログ、監査ログ、サーバイベント、またはエージェントイベント

     b. [を削除する] タイトルの横にあるドロップダウンメニューをクリックし、期間を選択します。この期間を過ぎたファイルは削除されます。
        - 無期限
        - 1 か月、2 か月、3 か月、6 か月、12 か月、18 か月、24 か月、36 か月、48 か月、60 か月

     c. [最大] タイトルの横にあるドロップダウンメニューをクリックし、保持するログエントリの最大数を選択します。
        - 0 件
        - 10,000 件、50,000 件、100,000 件、500,000 件、1,000,000 件、5,000,000 件、10,000,000 件

     d. [今すぐ削除] ボタンをクリックすると、イベントログがただちに削除されます。
   - **自動削除:**

     1日に1回の自動削除を設定するには、この設定を使用します。

     a. 削除するログタイプとして、[システムログ]、[監査ログ]、[サーバイベント]、または [エージェントイベント] を指定します。

b. [を削除する] タイトルの横にあるドロップダウンメニューをクリックし、期間を選択します。この期間を過ぎたファイルは削除されます。

- 無期限
- 1 か月、2 か月、3 か月、6 か月、12 か月、18 か月、24 か月、36 か月、48 か月、60 か月

c. [最大] タイトルの横にあるドロップダウンメニューをクリックし、保持するログエントリの最大数を選択します。

- 0 件
- 10,000 件、50,000 件、100,000 件、500,000 件、1,000,000 件、5,000,000 件、10,000,000 件

d. [保存] ボタンをクリックすると、イベントログが 1 日に 1 回自動的に削除されるようになります。

通知と SMTP 設定

警告や大規模感染に関する通知をメールで受信するように設定できます。

手順

1. [管理]→[SMTP 設定] の順に選択して、通知の送信に必要な SMTP サーバを設定します。
2. [サーバアドレス]、[ポート]、および [送信者] を指定します。
3. (オプション) SMTP サーバに認証が必要な場合は、[SMTP サーバの認証を設定する] チェックボックスをオンにします。SMTP サーバへの認証用の資格情報として、[ユーザ名] と [パスワード] を指定します。
4. [テストメールの送信] ボタンをクリックして、StellarOne からテストメールを送信します (これは手順 12 のために必要です)。
5. [保存] をクリックして SMTP 設定を完了します。
6. [管理]→[通知] の順に選択して、通知条件とメール設定を指定します。
7. [警告レベルのエージェントイベント] の下にある [警告レベルのエージェントイベントを送信する] スイッチをクリックしてオンにします。

注意

[警告レベルのエージェントイベント] の下にあるスイッチがオンの場合、「**警告**」を引き起こすイベントが発生するとメールで通知が送信されます。

8. [大規模感染] の下にある [大規模感染通知を送信する] スイッチをクリックしてオンにします。

注意

[大規模感染] の下にあるスイッチがオンの場合、指定した期間内に指定した数を超える未処理の警告メッセージが発生すると、メールで通知が送信されます。

9. 検出数と検出期間を指定して、大規模感染を定義します。
   - [監視する警告イベント数] に、イベントの発生回数 (1～20000) を指定します。
   - [監視する期間] に、イベントが発生した期間 (1～60 分) を指定します。
10. [メール通知] の下にある [送信先] に、通知を受信するメールアドレスを指定します。
11. [保存] をクリックして設定を完了します。
12. 指定したメールボックスに移動し、StellarOne から送信されたテストメール (手順 4 を参照) を受信したかどうか確認します。

プロキシ設定

[StellarOne のインターネットプロキシ設定]、[StellarOne からエージェントへの通信プロキシ設定]、および [エージェントから StellarOne への通信プロキシ設定] の 3 つのプロキシ設定があります。

手順

1. [管理]→[プロキシ] の順に選択します。
2. [プロキシ設定...] スイッチをオンにして、次の設定を有効にします。
   - **StellarOne のインターネットプロキシ設定**
   - **StellarOne からエージェントへの通信プロキシ設定**
   - **エージェントから StellarOne への通信プロキシ設定**
3. アップデートのためのプロキシ設定を行うには、次の手順を実行します。
   a. プロトコルとして [HTTPS] または [HTTP] を選択します。

   注意

   [エージェントから StellarOne への通信プロキシ設定] については、StellarProtect では現在 HTTPS プロキシがサポートされていないため、接続先が HTTPS サーバの場合は、接続に HTTP プロキシを使用してください。

   b. [サーバアドレス] で、プロキシサーバの IPv4 アドレスまたは FQDN を指定します。
   c. [ポート] を指定します。
   d. プロキシサーバで認証が必要な場合は、[プロキシサーバの認証を設定する] を選択し、資格情報を入力します。
   e. [保存] をクリックします。

ヒント

StellarProtect にリクエストを送信するために StellarOne で使用するプロキシ設定を行うには、次の手順を実行します。

- **インストール前:** エージェントのインストーラパッケージ内の設定ファイルにプロキシ情報を追加し、プロキシ設定を保存します。これにより、エージェントのインストーラパッケージを再パックする際に、保存した設定が含まれるようになります。
- **インストール後:** ローカルの StellarProtect エージェントで `opcmd.exe` コマンドラインインタフェースツールを使用します。

ダウンロード/アップデート

[ダウンロード/アップデート] ページでは、StellarOne の検索コンポーネントの設定、エージェントインストーラパッケージのダウンロード、StellarProtect 用 Patch ファイルのインポートまたは削除、および StellarOne を使用して StellarProtect エージェントを特定のグループに登録するための Group.ini ファイルのダウンロードを行うことができます。

手順

1. [管理]→[ダウンロード/アップデート] の順に選択します。
2. [StellarOne] タブで次の手順を実行します。
   - StellarOne のコンポーネントアップデートをただちに開始するには、[検索コンポーネント] セクションの [アップデート] ボタンをクリックします。

注意

- [アップデート] をクリックすると、最新のコンポーネントがダウンロードされてアップデートされます。使用可能なすべてのパターンファイルとエンジンのバージョンが、[アップデート] ボタンの下に表示されます。
- 検索コンポーネントが最後にアップデートされた日時は、[アップデート] ボタンの横にある [最終更新日] で確認できます。

- コンポーネントのアップデートを予約するには、[検索コンポーネントのアップデートスケジュール] の下にある [予約アップデート] スイッチをクリックして、この機能を有効にします。
  - [更新間隔] の下にあるラジオボタンをクリックして、更新間隔を [日次]、[週次]、または [月次] で指定します。

    重要

    すべての月に 29、30、31 日があるわけではない (たとえば 2 月は 28 日、うるう年には 29 日しかない) ため、月次のアップデートには [月の最後の日] を選択することをお勧めします。これにより、29、30、31 日のない月もアップデートが行われるようになります。

  - [開始時刻] をクリックして、検索コンポーネントの予約アップデートを開始する時刻を指定します。
- StellarOne のダウンロード元を指定するには、[検索コンポーネントのアップデート元 (StellarOne)] の下にあるいずれかのラジオボタンをクリックします。[アップデートサーバ] を選択すると、コンポーネントアップデートがアップデートサーバから直接ダウンロードされます。StellarOne サーバがアップデートサーバに接続できない場合、またはアップデートサーバを内部ネットワークでホストしている場合は、[その他のアップデート元] を選択し、テキストフィールドにアドレスを指定します。
- StellarProtect エージェントのダウンロード元を指定するには、[検索コンポーネントのアップデート元 (エージェント)] の下にあるいずれかのラジオボタンをクリックします。コンポーネントアップデートは StellarOne サーバから直接ダウンロードするか、[その他のアップデート元] を選択し、テキストフィールドにアドレスを指定することでダウンロードできます。

3. [StellarProtect] タブで次の手順を実行します。

   - StellarProtect の最新のエージェントインストーラパッケージをダウンロードするには、[ダウンロード] ボタンをクリックします。

     注意

     StellarOne と StellarProtect 間の通信にプロキシを使用している場合は、インストーラパッケージをダウンロードする前に、[プロキシ] リンクをクリックするか [管理]→[プロキシ] の順に選択して、プロキシ設定を行います。詳細な手順については、102 ページの「プロキシ設定」を参照してください。

   - StellarOne の管理サーバ画面を使用して StellarProtect エージェントを特定のグループに直接登録するには、[Group.ini のダウンロード] リンクをクリックして、Group.ini ファイルをインストーラパッケージに追加します。詳細な手順については、105 ページの「グループのマッピング」を参照してください。
   - StellarProtect の Patch ファイルをインポートするには、[インポート] ボタンをクリックして、手動で Patch をインポートします。
   - StellarProtect の Patch ファイルを削除するには、Patch ファイル名の横にあるチェックボックスをオンにします。[インポート] ボタンの横に [削除] ボタンが表示されます。[削除] ボタンをクリックして、選択したエントリを削除します。

グループのマッピング

この機能では、StellarOne の管理サーバ画面を使用して、エージェントを特定のグループに直接登録できます。

手順

1. [管理]→[ダウンロード/アップデート] の順に選択します。
2. 対象エージェントのタイプに応じて、[StellarProtect] または [StellarProtect (Legacy Mode)] タブを選択します。
3. [ダウンロード] をクリックして、インストーラパッケージをダウンロードします。
4. [Group.ini のダウンロード] リンクをクリックします。

5. [グループの選択] 画面が表示されます。
6. 対象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。[閉じる] ボタンをクリックして画面を閉じます。
7. `Group.ini` という名前のファイルがダウンロードされています。`Group.ini` ファイルを、対象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。
8. 対象エージェントでインストールを実行します。インストールプロセス中は、エージェントが StellarOne の管理サーバ画面に接続されている必要があります。
9. StellarOne の管理サーバ画面および現場の対象エージェントで、エージェントが登録されているかどうか確認できます。

ファームウェアと SSL 証明書のインポート

ここでは、StellarOne の管理サーバ画面にファームウェアと SSL 証明書をインポートする方法について説明します。

ファームウェアをインポートする

手順

1. [管理]→[ファームウェア] の順に選択します。
2. [インポート] ボタンをクリックして、ファームウェアの Patch ファイル (acus.fw_2.0.xxxx.acf など) を StellarOne にインポートします。
3. [ファームウェアのアップデート] 画面が表示されます。[バージョン] に StellarOne の現在のビルドバージョン、[公開日] と [説明] に StellarOne の Patch ファイルの情報が表示されます。
4. [適用] をクリックして、Patch を StellarOne に適用します。
5. アップグレードの注意を読みます。
6. [今すぐインストール] をクリックしてアップデートを実行するか、[中止] をクリックしてアップデートを停止します。

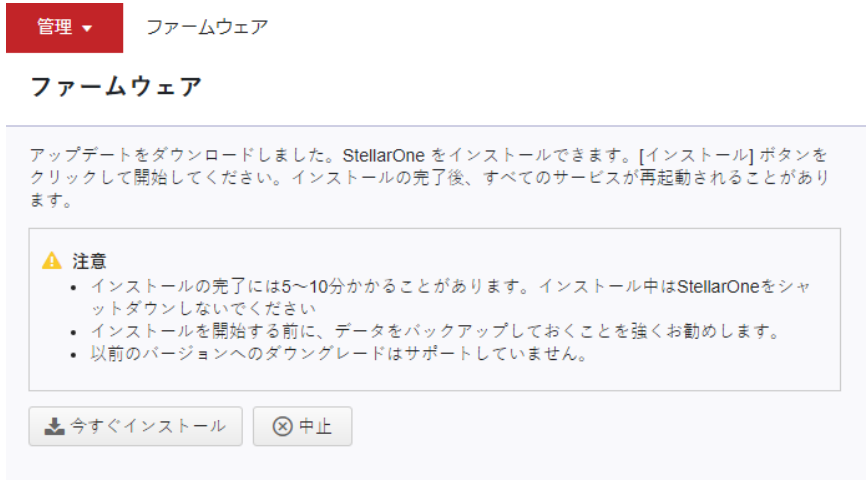


図 7-4.　ファームウェアのアップデートに関する注意

SSL 証明書をインポートする

手順

1. [管理]→[SSL 証明書] の順に選択します。
2. [証明書のインポート] をクリックすると、[証明書のインポート] 画面が表示されます。
   - [証明書] オプションの横にある [ファイルの選択...] をクリックして、対象の証明書を選択します。
   - [秘密鍵] オプションの横にある [ファイルの選択...] をクリックして、対象の秘密鍵を選択します。
   - (オプション) [パスフレーズ] テキストフィールドにパスフレーズを入力します。
3. [インポートして再起動] をクリックして、対象の証明書のインポートを開始します。

注意

証明書をインポートするには、StellarOne の管理サーバ画面を再起動する必要があります。

ライセンス管理

[管理]→[ライセンス] の順に選択して、Stellar 製品のライセンスを追加または更新できます。次の表に、[ライセンス] ページの詳細を示します。

図 7-5.　[ライセンス] ページ

表 7-4.　ライセンス情報

項目	説明
アクティベーションコードの入力	新しいアクティベーションコードを追加するためのボタン
ライセンスの更新	新しいアクティベーションコードの追加後にライセンスを更新するためのボタン。
ライセンスエディション	StellarProtect および StellarProtect (Legacy Mode) の現在のライセンスエディションが表示されます。詳細については、112 ページの「ライセンスエディション」を参照してください。
ライセンス種別	• 製品版: 正式に承認されたバージョン。 • 体験版: 使用機能が制限されたバージョン。 • 無期限: 永続使用可能でトレンドマイクロによる製品サポート終了までテクニカルサポートを提供。
シート数	StellarOne に現在登録されているエージェント数と、StellarOne に登録可能なエージェントの合計数を指定します。たとえば、「シート数: 2/10」は次のことを意味します。 • 2 つのエージェントが登録済み • 10 個までのエージェントを登録可能
ステータス	• 有効: 既存のライセンスは有効です。 • 有効期限終了: 既存のライセンスは古くなっています。 **注意** ウイルスの脅威からデバイスを保護するため、ただちにライセンスを更新することをお勧めします。詳細については、110 ページの「ライセンスのアクティベーションと更新」を参照してください。
有効期限	既存のライセンスの有効期限が表示されます。
アクティベーションコード	StellarOne をアクティベートするために必要なコード。
最終更新日	アクティベーションコードの前回の更新日時が表示されます。

ライセンスのアクティベーションと更新

StellarOne をはじめてインストールする場合は、最初のライセンスのアクティベーションについて、「StellarOne インストールガイド」を参照してください。ライセンスを更新する場合は、次の手順を実行します。

手順

1. [管理]→[ライセンス] の順に選択します。
2. 新しいアクティベーションコードを入力する場合は、[アクティベーションコードの入力] ボタンをクリックします。
   a. [アクティベーションコードの入力] 画面が表示されます。新しいアクティベーションコードを入力して、StellarOne の管理サーバ画面のライセンスを更新します。
   b. [保存] をクリックします。
   c. 更新に成功したことを示すメッセージが表示されます。

   注意

   更新に失敗した場合は、StellarOne サーバが TXOne の製品ライセンスサーバに外部接続できるかどうか確認します。

3. 既存のアクティベーションコードに対するライセンスを更新する場合は、[ライセンスの更新] ボタンをクリックします。
4. ライセンスの更新のため、StellarOne が TXOne の製品ライセンスサーバに接続します。

アクティベーションコードを変更する

アクティベーションコードを変更する必要がある場合は、次の手順を実行します。

手順

1. アクティベーションコードの変更について、トレンドマイクロの販売代理店に問い合わせます。
2. 新しいアクティベーションコードを受け取ったら、[管理]→[ライセンス] の順に選択し、[アクティベーションコードの入力] ボタンをクリックします。
3. 新しいアクティベーションコードを入力し、[保存] をクリックします。
4. [ライセンスの更新] をクリックして、製品ライセンスを更新します。

> **注意**
>
> StellarOne の管理サーバ画面が TXOne の製品ライセンスサーバに接続するには、[ライセンスの更新] ボタンをクリックする必要があります。

5. 「ライセンスが更新されました」というメッセージが表示されます。[最終更新日] にライセンスが更新された日時が表示されます。

ライセンスを更新する

同じアクティベーションコードでライセンスを更新する必要がある場合は、次の手順を実行します。

手順

1. ライセンスの更新リクエストについて、トレンドマイクロのの販売代理店に問い合わせます。
2. ライセンスの更新を確認したら、[管理]→[ライセンス] の順に選択し、[ライセンスの更新] ボタンをクリックします。
3. 「ライセンスが更新されました」というメッセージが表示されます。[最終更新日] にライセンスが更新された日時が表示されます。

ライセンスエディション

ここでは、TXOne Stellar バージョン 2.0 の 3 種類のライセンスエディションについて説明します。StellarProtect では Windows 7 以降のバージョン、StellarProtect (Legacy Mode) では Windows XP/2000 などのレガシープラットフォームがサポートされています。

表 7-5. ライセンスエディション

エディション	主な機能	期間
Stellar Standard	StellarProtect エージェント: • ウイルス対策 (リアルタイムの不正プログラム検索) • アプリケーション制御	1 年
	StellarProtect (Legacy Mode) エージェント: • アプリケーション制御 (手動検索を含む)	
Stellar Lite	StellarProtect エージェント: • ウイルス対策 (リアルタイムの不正プログラム検索)	1 年
	StellarProtect (Legacy Mode) エージェント: • アプリケーション制御 (手動検索を含む)	
Stellar Lockdown 無期限版	StellarProtect エージェント: • アプリケーション制御	無期限 **注意** Stellar Lockdown 無期限版では、TXOne Stellar が永続使用可能であり、トレンドマイクロによる製品サポート終了までテクニカルサポートが提供されます。
	StellarProtect (Legacy Mode) エージェント: • アプリケーション制御	

各ライセンスエディションの機能

Stellar Standard、Stellar Lite、Stellar Lockdown 無期限版の各ライセンスエディションでは異なる機能が提供されており、さまざまな業界のユーザが特定のニーズに応じて選択することが可能です。

表 7-6.　各ライセンスエディションの機能

機能	Stellar Standard	Stellar Lite	Stellar Lockdown 無期限版
次世代ウイルス対策 (NGAV)	√	√	-
操作/アプリケーション制御	√	Windows XP/2000 のみ	√
操作の挙動異常検知	√	√	√
産業用アプリケーションと証明書のリポジトリ	√	-	√
OT アプリケーション保護	√	-	√
Intelligent Runtime Learning (インテリジェントランタイム学習 - 機械学習型検索)	√	-	√
信頼する USB デバイスコントロール	√	√	√
レガシーシステムとの互換性	√	√	√

OT Intelligent Trust

TXOne OT Intelligent Trust を有効にすると、匿名の脅威情報が Smart Protection Network と共有され、新たな脅威を迅速に特定して対処できるようになります。

TXOne OT Intelligent Trust は、管理サーバ画面からいつでも無効にできます。

手順

1. [管理]→[OT Intelligent Trust] の順に選択します。
2. [詳細] をクリックして、TXOne の OT 脅威調査 Web サイトにアクセスします。
3. [TXOne OT Intelligent Trust を有効にする (推奨)] スイッチをクリックしてオンにし、TXOne OT Intelligent Trust を有効にします。

第 8 章

テクニカルサポート

TXOne Networks 製品のサポートは、TXOne 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。

付録 A

ログの説明

この付録では、各ログについて説明します。この付録の内容は次のとおりです。

StellarProtect のエージェントイベントログの説明

この表は、StellarProtect に対する Windows イベントログの説明を示しています。

イベント ID	レベル	カテゴリ	イベントの内容	イベントの詳細
256	情報	System	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	System	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	System	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	System	Patch を適用中	Patch を適用中です。先に適用された Patch の更新が完了すると、この Patch (%deferred_file_name%) が自動的に適用されます。
513	情報	intelli_av	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	intelli_av	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	intelli_av	予約検索の開始	予約検索が開始されました。
516	情報	intelli_av	予約検索の終了	予約検索が終了しました。

イベント ID	レベル	カテゴリ	イベントの内容	イベントの詳細
517	情報	intelli_av	手動検索の開始	手動検索が開始されました。
518	情報	intelli_av	手動検索の終了	手動検索が終了しました。
519	情報	intelli_av	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	intelli_av	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	anomaly_detect	操作の挙動異常検知が有効になりました	モード: %Mode% レベル: %Level%
769	情報	anomaly_detect	操作の挙動異常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%

イベント ID	レベル	カテゴリ	イベントの内容	イベントの詳細
770	情報	anomaly_detect	操作の挙動異常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	anomaly_detect	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	device_control	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	device_control	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	カテゴリ	イベントの内容	イベントの詳細
1282	情報	device_control	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	lockdown	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	lockdown	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	lockdown	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	lockdown	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	lockdown	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	lockdown	アプリケーション制御が有効になりました	アプリケーション制御が有効になりました。 モード: %MODE%

イベント ID	レベル	カテゴリ	イベントの内容	イベントの詳細
1798	情報	lockdown	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	lockdown	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	lockdown	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	update	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	update	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。
2050	情報	update	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	update	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。

イベント ID	レベル	カテゴリ	イベントの内容	イベントの詳細
4352	警告	system	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	system	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	system	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	system	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	intelli_av	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%

イベント ID	レベル	カテゴリ	イベントの内容	イベントの詳細
				脅威の種類: %STRING% 脅威の名前: %STRING% 処理の結果: %INTEGER% 隔離パス: %PATH%
4610	警告	intelli_av	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	intelli_av	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。

イベント ID	レベル	カテゴリ	イベントの内容	イベントの詳細
				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	intelli_av	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	カテゴリ	イベントの内容	イベントの詳細
4613	警告	intelli_av	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	intelli_av	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	intelli_av	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%

イベント ID	レベル	カテゴリ	イベントの内容	イベントの詳細
				脅威の名前: %STRING%
4617	警告	intelli_av	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	anomaly_detect	操作の挙動異常検知が無効になりました	操作の挙動異常検知が無効になりました。
4865	警告	anomaly_detect	操作の挙動異常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%

イベント ID	レベル	カテゴリ	イベントの内容	イベントの詳細
4866	警告	anomaly_detect	操作の挙動異常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	anomaly_detect	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	change_control	Safeguard により ICS ファイルの変更がブロックされました: %PATH%	Safeguard により実行可能ファイルに対する ICS ファイルの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	change_control	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。

イベント ID	レベル	カテゴリ	イベントの内容	イベントの詳細
				ブロックされたプロセス: %PATH% 対象プロセス: %PATH%
5376	警告	device_control	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。
5377	警告	device_control	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	lockdown	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%

イベント ID	レベル	カテゴリ	イベントの内容	イベントの詳細
5889	警告	lockdown	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	lockdown	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: %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: %PATH%
5891	警告	lockdown	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	lockdown	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	lockdown	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	lockdown	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	カテゴリ	イベントの内容	イベントの詳細
5895	警告	lockdown	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	intelli_av	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	change_control	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	change_control	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。

StellarProtect のサーバイベントログの説明

この表は、StellarProtect に対するサーバイベントログの説明を示しています。

ID	内容
33027	エージェント (%s) のポリシーモードへの切り替え
33028	エージェント (%s) の個別のモードへの切り替え
33029	バージョン%s でポリシーを配信
33041	慣用 (DLL インジェクション対策、デバイスコントロール、OT アプリケーション保護、OBAD) 設定の変更、対象グループポリシー: [%s] (バージョン: %s)
33042	リアルタイム検索の設定の変更、対象グループポリシー: [%s] (バージョン: %s)
33043	予約検索の設定の変更、対象グループポリシー: [%s] (バージョン: %s)
33044	デバイスコントロールリストの維持、対象グループポリシー: [%s] (バージョン: %s)
33045	ユーザ指定不審オブジェクトリストの維持、対象グループポリシー: [%s] (バージョン: %s)

ID	内容
33046	操作の挙動異常検知ウォッチリストの維持、対象グループポリシー: [%s] (バージョン: %s)
33047	信頼するデジタル証明書リストの維持、対象グループポリシー: [%s] (バージョン: %s)
33048	OT アプリケーション保護リストの維持、対象グループポリシー: [%s] (バージョン: %s)
33049	エージェントパスワードの変更、対象グループポリシー: [%s] (バージョン: %s)
33056	使用可能な Patch の設定の変更、対象グループポリシー: [%s] (バージョン: %s)
33057	承認プロセスの維持、対象グループポリシー: [%s] (バージョン: %s)
33058	パターンファイルの予約アップデートの変更 予約アップデートの設定の変更、対象グループポリシー: [%s] (バージョン: %s)
33059	制御設定の変更、対象グループポリシー: [%s] (バージョン: %s)
33105	個別のコマンドをエージェント (%s) に送信
33106	保護コマンド <変更画面の設定> をエージェントに送信
33107	保護コマンド <検索開始> をエージェントに送信
33108	保護コマンド <コンポーネントのアップデート> をエージェントに送信
33109	保護コマンド <パッチの適用> をエージェントに送信
33110	保護コマンド <制御の許可リストの初期化> をエージェントに送信
33121	イベントの処理をエージェント (%AGENT_NAME%) に適用
33122	イベントの処理 <%ACTION_TYPE%> をエージェントに適用
37122	ポリシーバージョン%s でアクティベーションコードを設定
37123	アクティブなエージェント
37124	非アクティブなエージェント

StellarOne のサーバイベントログの説明

この表は、StellarOne に対するサーバイベントログの説明を示しています。

ID	内容
45313	検索コンポーネントのアップデート開始
45314	検索コンポーネント [%s] のアップデートタスクが開始されました
45315	検索コンポーネントの予約アップデートを有効にする
45316	検索コンポーネントの予約アップデートを無効にする
45317	StellarOne の検索コンポーネントのアップデート元を変更する
45318	エージェントの検索コンポーネントのアップデート元を変更する
45319	検索コンポーネント [%s] のアップデートに成功しました
45320	検索コンポーネント [%s] のアップデートに成功しましたが複製は必要ありませんでした
45321	内部エラーにより検索コンポーネント [%s] のアップデートに失敗しました
45322	ネットワークに接続できなかったため検索コンポーネント [%s] のアップデートに失敗しました
45323	ポリシーのカスタマイズ
45324	[%s] からのポリシーの継承

付録 B

Syslog コンテンツ - CEF

この付録では、StellarOne のログ出力と CEF Syslog タイプとの対応を示します。

この付録の内容は次のとおりです。

エージェントイベントの形式

Common Event Format (CEF) 形式での StellarProtect のエージェントイベントについては、次の表を参照してください。

表 B-1.　エージェントイベントの形式

CEF フィールド名	説明	値の例
Header		
CEF:Version	CEF 形式のバージョン	CEF:0
Device Vendor	デバイスのベンダ	TXOne Networks
Device Product	デバイスの製品	StellarProtect
Device Version	デバイスのバージョン	2.0
Device Event Class ID	イベント ID	{}
Name	イベントのカテゴリ	Agent Event
Severity	LOG_CRIT: 2 LOG_WARNING: 4 LOG_INFO: 6	{2, 4, 6}
Extension		
eventTime	StellarProtect の形式	Jan 02 2006 15:04:05 GMT +00:00
msg	<string>	
category	OPTION: 0 SYSTEM: 1 INTELLI_AV: 2 ANOMALY_DETECT: 3 CHANGE_CONTROL: 4 DEVICE_CONTROL: 5 MISC: 15	
agentEndpoint	<string>	
agentIp	<string>	

CEF フィールド名	説明	値の例
agentLocation	<string>	
agentVendor	<string>	
agentModel	<string>	
agentOS	<string>	
policyVersion	<string>	
detailMsg	<string>	
targetProcess	<string>	
fileHash	<string>	
threatType	<string>	
threatName	<string>	
filePath	<string>	
actionResult	<int>	
quarantinePath	<string>	
obadMode	<string>	
obadLevel	<string>	
accessUser	<string>	
processId	<string>	
parentProcess1	<string>	
parentProcess2	<string>	
parentProcess3	<string>	
parentProcess4	<string>	
targetArguments	<string>	
parentArguments1	<string>	
parentArguments2	<string>	
parentArguments3	<string>	

CEF フィールド名	説明	値の例
parentArguments4	<string>	
blockedProcess	<string>	
targetFile	<string>	
vid	<int>	
pid	<int>	
sn	<string>	
accessImagePath	<string>	
srcPath	<string>	
dstPath	<string>	
errCode	<int>	
patchFileName	<string>	
filePath	<string>	
type	<string>	

StellarProtect のサーバイベントの形式

Common Event Format (CEF) 形式での StellarProtect のサーバイベントについては、次の表を参照してください。

表 B-2.　StellarProtect のサーバイベントの形式

CEF フィールド名	説明	値の例
Header		
CEF:Version	CEF 形式のバージョン	CEF:0
Device Vendor	デバイスのベンダ	TXOne Networks
Device Product	デバイスの製品	StellarProtect
Device Version	デバイスのバージョン	2.0
Device Event Class ID	イベント ID	{}
Name	イベントのカテゴリ	Server Event
Severity	LOG_INFO: 6	{6}
Extension		
eventTime	StellarProtect の形式	Jan 02 2006 15:04:05 GMT +00:00
msg	<string>	
userName	<string>	
userRole	<string>	
clientIp	<string>	

StellarOne のサーバイベントの形式

Common Event Format (CEF) 形式での StellarOne のサーバイベントについては、次の表を参照してください。

表 B-3.　StellarOne のサーバイベントの形式

CEF フィールド名	説明	値の例
Header		
CEF:Version	CEF 形式のバージョン	CEF:0
Device Vendor	デバイスのベンダ	TXOne Networks
Device Product	デバイスの製品	StellarOne
Device Version	デバイスのバージョン	2.0
Device Event Class ID	イベント ID	{}
Name	イベントのカテゴリ	Console Log
Severity	LOG_INFO: 6	{6}
Extension		
eventTime	StellarOne の形式	Jan 02 2006 15:04:05 GMT +00:00
msg	<string>	
userName	<string>	
userRole	<string>	
clientIp	<string>	
status	UNSPECIFIED: 0 AU_SUCCESS: 1 AU_FAIL: 2	{0, 1, 2}
product	<string>	{protect}

文書番号: APEM29594_JP2303