



# 2.0 TXOne StellarOne

## 管理者ガイド

### for StellarProtect (Legacy Mode)



#### ※注意事項

##### 複数年契約について

- お客様が複数年契約（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。

##### 著作権について

本ドキュメントに関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が事前に承諾している場合を除き、形態および手段を問わず、本ドキュメントまたはその一部を複製することは禁じられています。本ドキュメントの作成にあたっては細心の注意を払っていますが、本ドキュメントの記述に誤りや欠落があつてもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本ドキュメントおよびその記述内容は予告なしに変更される場合があります。

##### 商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDI オプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポートプレミアム、Air サポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、Smart Check、Trend Micro XDR、Trend Micro Managed XDR、OT Defense Console、Edge IPS、Trend Micro Cloud One、スマスキヤ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック！、Trend Micro Security Master、およびTrend Micro Service One は、トレンドマイクロ株式会社の登録商標です。

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

Copyright © 2023 Trend Micro Incorporated. All rights reserved.

P/N: APEM29595\_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、お客様の製品の利用状況や検出にかか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、お客様が関連機能を無効にする必要があります。

TXOne StellarOne for StellarProtect (Legacy Mode) により収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次の Web サイトを参照してください。

<https://www.go-tm.jp/data-collection-disclosure>

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



### 重要

データ収集の無効化やデータの削除により、製品、サービス、または機能の利用に影響が発生する場合があります。TXOne StellarOne for StellarProtect (Legacy Mode) における無効化の影響をご確認の上、無効化はお客様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、お客様のデータを取り扱います。

[https://www.trendmicro.com/ja\\_jp/about/legal/privacy-policy-product.html](https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html)

## 目次

<b>第1 章: 本製品の概要</b> .....	<b>12</b>
<b>概要</b> .....	<b>12</b>
TXOne StellarOne について .....	13
サーバの機能と特徴.....	13
新機能 .....	14
<b>第2 章: エージェント/グループ管理</b> .....	<b>15</b>
<b>StellarProtect (Legacy Mode) エージェントの管理</b> .....	<b>15</b>
<b>[エージェント] 画面について</b> .....	<b>16</b>
エージェントツリーを管理する .....	17
グループを追加する .....	17
グループ名を変更する .....	18
グループを削除する/エージェントを登録解除する .....	18
エージェント/グループを検索する .....	19
<b>第3 章: ポリシー管理</b> .....	<b>21</b>
<b>グループ/エージェントポリシーを管理する</b> .....	<b>21</b>
アプリケーション制御を設定する .....	22
Intelligent Runtime Learning (インテリジェントランタイム学習) を設定する .....	23
ロックダウン除外を設定する .....	24
信頼するハッシュ値の設定 .....	24
ハッシュ値を計算する .....	24
信頼するハッシュ値を追加する .....	25
信頼するハッシュ値をインポートする .....	26
信頼するハッシュ値を編集する .....	26

信頼するハッシュ値を削除する	27
信頼するデジタル証明書の設定	28
信頼するデジタル証明書をインポートする	28
信頼するデジタル証明書を削除する	29
除外パスの設定	30
ファイル、フォルダ、または正規表現を除外パスとして追加する	30
除外パスを編集する	30
除外パスを削除する	31
書き込み制御の設定	31
書き込み制御にファイル、フォルダ、レジストリキー、またはレジストリ値を追加する	31
書き込み制御を編集する	32
書き込み制御を削除する	32
除外をインポートする	33
除外をエクスポートする	34
<b>予約検索を設定する</b>	<b>34</b>
予約検索	35
コンポーネントアップデート	35
検索対象ファイル	36
検出時の処理	37
検索除外	38
<b>デバイスコントロールを設定する</b>	<b>38</b>
デバイス情報を取得する	39
信頼する USB デバイスのコマンド	39
信頼する USB デバイスを追加する	40

信頼する USB デバイスを編集する	41
ポリシーの設定により、信頼する USB デバイスを削除する	42
設定のインポートにより、信頼する USB デバイスを削除する	42
<b>ユーザ指定不審オブジェクトを設定する</b>	<b>43</b>
ユーザ指定不審オブジェクトを追加する	44
ユーザ指定不審オブジェクトを削除する	44
エージェントのパスワードを設定する	45
Patch を設定する	46
<b>第4 章: エージェントの保護とアップデート</b>	<b>47</b>
メンテナنسモードを設定する	47
許可リストをアップデートする	51
検索開始を設定する	52
検索開始を実行する	53
エージェントコンポーネントのアップデート	54
エージェントに Patch を配信する	55
接続を確認する	57
イベントログを収集する	58
<b>第5 章: エージェントの設定のインポート/エクスポート</b>	<b>60</b>
エージェントの設定をエクスポートする	61
エージェントの設定をエクスポートする	61
許可リストをエクスポートする	62
エージェントの設定をインポートする	64
エージェントの設定をインポートする	64
許可リストをインポートする	65
エージェントの処理	67

タグを編集する .....	67
移動する .....	68
削除する .....	69
<b>第6 章: StellarProtect (Legacy Mode) の監視 .....</b>	<b>70</b>
<b>StellarProtect (Legacy Mode) の監視 .....</b>	<b>70</b>
ダッシュボードについて .....	70
ブロックされたイベントの履歴 .....	71
ブロック件数が上位のエージェント .....	72
ブロックされた件数が上位のファイル .....	73
CPU 使用率 .....	73
メモリ使用率 .....	74
ディスク使用率 .....	74
ウィジェットを追加する .....	75
ウィジェットを使用する .....	76
[エージェントイベント] 画面について .....	78
エージェントイベントログをクエリする .....	79
エージェントイベントをエクスポートする .....	80
[サーバイベント] 画面について .....	81
サーバイベントログをクエリする .....	82
サーバイベントログをエクスポートする .....	83
[システムログ] 画面について .....	83
サーバログをクエリする .....	83
システムログをエクスポートする .....	84
[監査ログ] 画面について .....	85
監査ログをクエリする .....	85

監査ログをエクスポートする	87
<b>第7 章: 管理設定</b>	<b>88</b>
<b>[アカウント管理] 画面について</b>	<b>89</b>
<b>サーバアカウントの概要</b>	<b>90</b>
アカウントを追加する	92
アカウントを編集する	94
アカウントを削除する	95
<b>API キーの生成</b>	<b>96</b>
<b>シングルサインオン</b>	<b>97</b>
シングルサインオンの問題の解決	98
<b>システム時間</b>	<b>100</b>
日付と時刻	100
タイムゾーン	101
<b>Syslog 転送</b>	<b>101</b>
Syslog 形式	102
<b>ログの削除設定</b>	<b>104</b>
今すぐ削除	104
自動削除	105
<b>予約レポートの設定</b>	<b>106</b>
<b>通知設定</b>	<b>108</b>
警告レベルのエージェントイベント	109
大規模感染	110
<b>SMTP 設定</b>	<b>111</b>
<b>プロキシ設定</b>	<b>112</b>
<b>ダウンロード/アップデート設定</b>	<b>114</b>

グループのマッピング .....	115
ファームウェア .....	117
SSL 証明書 .....	118
ライセンス管理 .....	119
アクティベーションコードを変更する .....	120
<b>第8章: ログの説明の参照情報 .....</b>	<b>122</b>
エージェントのイベントログの説明 .....	122
エージェントのエラーコードの説明 .....	147
サーバのイベントログの説明 .....	150
<b>第9章: テクニカルサポート .....</b>	<b>155</b>
トラブルシューティングのリソース .....	155
サポートポータルの利用 .....	156
脅威データベース .....	156
製品サポート情報 .....	157
サポートサービスについて .....	157
トレンドマイクロへのウイルス解析依頼 .....	158
メールレビューションについて .....	158
ファイルレビューションについて .....	158
Web レビューションについて .....	158
その他のリソース .....	159
最新版ダウンロード .....	159
脅威解析・サポートセンターTrendLabs (トレンドラボ) .....	159

# 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。

## 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

次の表は、TXOne StellarOne のドキュメントで使用されている表記規則を示しています。

表 1. ドキュメントの表記規則

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

## 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 のサーバプログラムです。
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 (Legacy Mode) クライアントプログラムを実行しているホストです。
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 (Legacy Mode) 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。
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ーフェースです。
CLI	コマンドラインインターフェース
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。
エージェントの インストールフォルダ	StellarProtect (Legacy Mode) エージェントのファイルが含まれるホスト上のフォルダです。インストール時に初期設定を使用すると、インストールフォルダは次の場所になります。 "C:\Program Files\TXOne\StellarProtect (Legacy Mode)"

## 第 1 章

# 本製品の概要

## 概要

TXOne StellarOne は、レガシーシステム向けの TXOne StellarProtect (Legacy Mode) とモダナイズされたシステム向けの TXOne StellarProtect 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です。このマニュアルでは、主に TXOne StellarProtect (Legacy Mode) を管理する方法について説明します。シンプルかつメンテナンス不要なソリューションである TXOne StellarProtect (Legacy Mode) は、特定用途向けのコンピュータをロックダウンして保護することにより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。

## TXOne StellarOne について

TXOne StellarOne は、StellarProtect (Legacy Mode) エージェントのインストール、ステータス、およびイベントの集中管理を実現します。たとえば管理者は、エージェントの許可リストを作成したりアプリケーション制御を変更したりできます。

## サーバの機能と特徴

TXOne StellarOne には、次の機能と特徴があります。

機能	特徴
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 StellarProtect (Legacy Mode) 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 StellarProtect (Legacy Mode) 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 StellarProtect (Legacy Mode) 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。
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。 <ul style="list-style-type: none"> <li>StellarProtect (Legacy Mode) エージェントステータスの監視</li> <li>接続ステータスの確認</li> <li>設定の表示</li> <li>手動またはポリシーによるエージェントログの収集</li> <li>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</li> <li>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</li> <li>エージェントのメンテナンスモードの設定</li> <li>エージェントコンポーネントのアップデート</li> <li>許可リストの初期化</li> <li>エージェントへの Patch の配信</li> <li>信頼するファイルおよび USB デバイスの追加</li> </ul>
イベントの集中管理	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。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。

機能	特徴
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できます。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 for StellarProtect (Legacy Mode) 2.0 には、次の新機能および機能強化が含まれています。

機能	説明
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。
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

# エージェント/グループ管理

### **StellarProtect (Legacy Mode) エージェントの管理**

この章では、エージェント管理を行う管理サーバ画面の概要について説明します。

## [エージェント] 画面について

[エージェント] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。この画面では、StellarOne の管理サーバ画面で管理されているエージェントのリストが表示され、設定タスクを実行できます。



### 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。  アイコンはグループを、  アイコンはエージェントを示します。



The screenshot shows the StellarOne management interface with the following details:

- Header:** stellarOne, admin (Admin), txOne networks
- Navigation:** ダッシュボード, エージェント (highlighted), ログ, 管理, バージョン情報
- Page Title:** エージェント すべて (2)
- Search and Filter:** 検索 (Search) icon, 前 (Previous) icon, 次 (Next) icon, リセット (Reset) icon, ページ数 (Page 1 of 1), 検索条件 (Search Conditions) icon.
- Buttons:** + グループの新規作成, フィルタ, 保護, アップデート, インポート/エクスポート
- Table:** Displays a list of 2 agents with the following columns: 名前 (Name), IPアドレス (IP Address), 保護 (Protection), ポリシーの継承 (Policy Inheritance), 許可リスト (Allow List), エージェントバージョン (Agent Version), 前回の接続 (Last Connection), 機能タイプ (Function Type), and 处理 (Action). The table shows two entries:

名前	IPアドレス	保護	ポリシーの継承	許可リスト	エージェントバージョン	前回の接続	機能タイプ	処理
TXSP-WIN10...	192.168.0.102	🔒 🔔	● 継承済み	86802	1.3.1028	2022-12-21T19...	StellarProtect (Legacy Mode)	⋮
TXSP-WIN10...	192.168.0.101	✖	● 継承済み	-	1.3.1029	2022-12-21T19...	StellarProtect (Legacy Mode)	⋮
Headquarter (0)	-	-	継承済み	-	-	-	-	⋮

## エージェントツリーを管理する

StellarOne では、エージェントツリーを編成して StellarProtect (Legacy Mode) エージェントの情報を持続的に監視できます。

タスク	詳細
エージェントグループの追加	複数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します。
エージェントグループの再編成	グループを再編成します。
エージェントグループ名の変更	グループの名前を変更します。
エージェントグループの削除/エージェントの登録解除	StellarOne の管理サーバ画面から、グループを削除するかエージェントを登録解除します。
エージェントまたはグループの検索	検索条件を追加してエージェント/グループを検索します。

## グループを追加する

### 手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。[エージェント] 画面が表示されます。
2. [エージェント] ビューの [すべて] グループから開始します。
3. グループ名をクリックして目的の親グループに移動し、新しいグループを作成します。
4. 上部のコントロール領域で  ボタンをクリックします。
5. [グループの新規作成] 画面が表示されます。
6. グループ名を入力し、[確認] を選択します。



### 注意

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

## グループ名を変更する

### 手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。[エージェント] 画面が表示されます。
2. 名前を変更するグループを選択します。
3. [処理] の縦 3 点リーダーのアイコン (⋮) をクリックし、[名前の変更] をクリックします。
4. [エージェントグループ名の変更] 画面が表示されます。
5. 新しい名前を入力し、[確認] をクリックします。



### 注意

同一レベルで同じグループ名を指定することはできません。

## グループを削除する/エージェントを登録解除する

### 手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。[エージェント] 画面が表示されます。
2. 削除するグループまたは登録解除するエージェントを選択します。
3. [処理] の縦 3 点リーダーのアイコン (⋮) をクリックし、[削除] をクリックします。

4. [項目の削除] 確認画面が表示されます。
5. [確認] をクリックして、グループの削除またはエージェントの登録解除を行います。



### 注意

空でない(グループまたは資産がある)グループは削除できません。

## エージェント/グループを検索する

### 手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。[エージェント] 画面が表示されます。
2. 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。

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	ポリシーの継承モード。[継承済み] または [カスタマイズ済み] を選択します。
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	前回の接続時間。初期設定の期間を選択するか、[カスタム]を選択して時間範囲を独自に指定します。初期設定の期間は次のとおりです。 <ul style="list-style-type: none"> <li>1 時間以内</li> <li>24 時間以内</li> <li>過去 7 日間</li> <li>過去 30 日間</li> </ul>
製品	[StellarProtect (Legacy Mode)] または [StellarProtect] を選択します。
OS	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。

## 第3章

# ポリシー管理

## グループ/エージェントポリシーを管理する

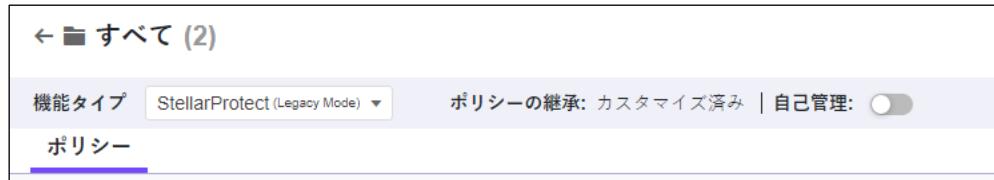
- グループをエージェントとともに追加して、親グループからグループポリシーを継承することも、独自のグループポリシーをカスタマイズすることもできます。
- エージェントは、親グループからポリシーを継承する代わりに、カスタマイズした独自のエージェントポリシーを持つこともできます。



The screenshot shows the StellarOne management interface with the following details:

- Header:** StellarOne, admin (Admin), txOne networks
- Top Navigation:** ダッシュボード, エージェント, ログ, 管理, バージョン情報
- Sub-Header:** エージェント すべて (2) ▾
- Toolbar:** グループの新規作成, フィルタ, リスト, リソース, アップデート, インポート/エクスポート
- Table Headers:** 許可リスト, エージェントバージョン, 前回の接続, 機能タイプ, 操作 (処理)
- Table Data:** TXSP-WIN10, 192.168.0.102, 66802, 1.3.1028, 2022-12-21T19:..., StellarProtect (Legacy Mode)
- Table Data:** TXSP-WIN10, 192.168.0.101, -, 1.3.1029, 2022-12-21T19:..., StellarProtect (Legacy Mode)
- Table Data:** Headquarter (0), -, -, -, -
- Annotations:** A red box highlights the "Inheritance Status" column in the table, which shows "Inherited" for the first two rows and "Not Inherited" for the last row. Another red box highlights the "Actions" column, which contains three vertical ellipsis icons for each row.

- エージェントを含むグループは、[製品] (StellarProtect または StellarProtect (Legacy Mode)) を切り替えると、それぞれの [ポリシー] を表示できます。



← ■ すべて (2)

機能タイプ StellarProtect (Legacy Mode) ポリシーの継承: カスタマイズ済み | 自己管理:

ポリシー

- エージェントは、タブを切り替えると、それぞれの [一般情報] と [ポリシー] を表示できます。



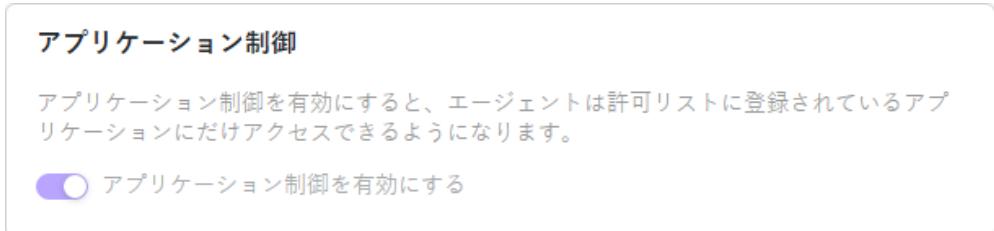
← □ TXSP-WIN10-A01

StellarProtect (Legacy Mode) ポリシーの継承:  親グループから継承:すべて | 自己管理:

一般情報 ポリシー

## 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。許可リストの設定は [ロックダウン除外] で行います (詳細は以降のセクションを参照)。



### アプリケーション制御

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。

アプリケーション制御を有効にする

## 手順

- [エージェント] ビューで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。
- 次のいずれかの方法で [ポリシー] ビューを表示します。
  - [ポリシーの継承] リンクをクリックします。

- [処理] のポリシーアイコン (🛡) をクリックします。
- 3. [ポリシー] ビューで [アプリケーション制御] ペインに移動します。
- 4. スイッチを切り替えて、[親グループから継承] を無効にします。
- 5. スイッチを切り替えて、アプリケーション制御を有効または無効にします。



#### 注意

StellarProtect (Legacy Mode) エージェントの管理者は、StellarProtect (Legacy Mode) エージェントのメイン画面からアプリケーション制御のステータスを変更することもできます。

## Intelligent Runtime Learning (インテリジェントランタイム学習) を設定する

Intelligent Runtime Learning (インテリジェントランタイム学習) が有効な場合、エージェントでは、信頼リストに含まれるアプリケーションによって生成されたランタイム実行ファイルが許可されます。

### Intelligent Runtime Learning (インテリジェントランタイム学習)

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。

Intelligent Runtime Learning (インテリジェントランタイム学習) の有効化

### 手順

1. [エージェント] ビューで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。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
  - [ポリシーの継承] リンクをクリックします。
  - [処理] のポリシーアイコン (🛡) をクリックします。

3. [ポリシー] ビューで [Intelligent Runtime Learning (インテリジェントランタイム学習)] ペインに移動します。
4. スイッチを切り替えて、[親グループから継承] を無効にします。
5. スイッチを切り替えて、Intelligent Runtime Learning (インテリジェントランタイム学習) を有効または無効にします。

## ロックダウン除外を設定する

[ロックダウン除外] を使用すると、アプリケーション制御からの除外を設定できます。つまり、ブロックするよう指定されたアプリケーションのユーザ指定の設定です。ここで設定する許可リストには、[ポリシー] ビューの [ロックダウン除外] ペインにある [信頼するハッシュ値]、[信頼するデジタル証明書]、[除外パス]、および [書き込み制御] の設定が含まれます。

## 信頼するハッシュ値の設定

ハッシュ値を使用して、管理対象資産のアプリケーションやファイルの実行をリモートで許可できます。

## ハッシュ値を計算する

信頼するハッシュ値を追加する前に、**ファイルハッシュ生成ツール**を使用してハッシュ値を計算します。

### 手順

1. [信頼するハッシュ値] 領域からファイルハッシュ生成ツールをダウンロードします。
2. ダウンロードしたフォルダから **WKFileHashGen.exe** を実行します。[ファイルハッシュ生成ツール] 画面が表示されます。
3. 次のいずれかの方法を使用してファイルを選択し、ハッシュ値を計算します。
  - フォルダまたはファイルを [ファイルハッシュ生成ツール] 画面にドラッグアンドドロップします。
  - ドロップダウンボタンをクリックし、[ファイルの追加] をクリックして、追加するファイルを選択します。

- ドロップダウンボタンをクリックし、[フォルダの追加]をクリックして、選択したフォルダのすべてのファイルを追加します。
- [ファイルハッシュ (SHA-1)] 列にハッシュ値が表示されます。
4. ファイルが 1 つの場合は、項目を右クリックして [ハッシュ値のコピー] を選択します。ファイルが複数の場合は、[すべてエクスポート] をクリックしてハッシュ値のリストを生成します。



#### 注意

すべての必要なファイルでハッシュ値を計算するには、対象アプリケーションのルートフォルダをファイルハッシュ生成ツールに追加することをお勧めします。

[フォルダの追加] ボタンでは、インストーラファイル、スクリプトファイル、および PE (ポータブル実行可能) 形式のファイルのみが計算対象となることに注意してください。

## 信頼するハッシュ値を追加する

### 手順

- [エージェント] ビューで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。
- 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
  - [ポリシーの継承] リンクをクリックします。
  - [処理] のポリシーアイコン (🛡) をクリックします。
- [ポリシー] ビューの [ロックダウン除外] ペインにある [信頼するハッシュ値] に移動します。
- ハッシュ値とメモを入力します。
- 信頼するインストールパッケージによって作成または変更されたファイルが自動的に許可リストに追加されるようにするには、スイッチを切り替えてインストーラを有効にします。
- [追加] ボタンをクリックして、单一のハッシュ値と以前保存した設定を追加します。



### 注意

信頼するインストールパッケージによって作成または変更されたファイルが自動的に許可リストに追加されるようにするには、[インストーラ] 列でアプリケーションインストーラを選択します。

## 信頼するハッシュ値をインポートする

### 手順

1. [ポリシー] ビューの [ロックダウン除外] ペインにある [信頼するハッシュ値] に移動します。
2. [インポート] ボタンをクリックして、ハッシュ値をまとめて追加します。
3. 許可済みのインストーラによって作成または変更されたすべてのファイルを [許可リスト] に自動的に追加するように、[インストーラ] スイッチを切り替えて有効にします。



### 注意

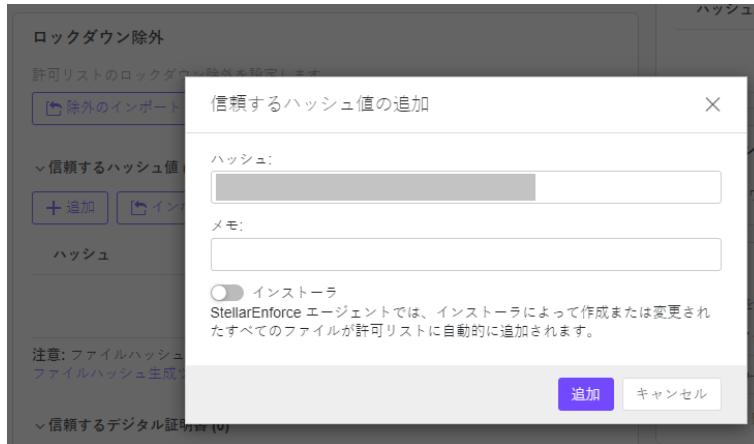
StellarOne は、インストーラフラグがマークされた信頼するハッシュ値のリストを含む.txt ファイルの一括インポート/エクスポートをサポートします。ただし、インポート/エクスポート処理により、[メモ] に含まれるタブ文字が (信頼するハッシュの配信画面で表示されるように) 空白に自動的に変換されます。

## 信頼するハッシュ値を編集する

### 手順

1. [ポリシー] ビューの [ロックダウン除外] ペインにある [信頼するハッシュ値] に移動します。
2. 編集するハッシュ値を選択します。
3. [追加] ボタンをクリックすると、[信頼するハッシュ値の追加] 画面が表示されます。

4. 編集後、[追加] ボタンをクリックして設定を保存します。



## 信赖するハッシュ値を削除する

### 手順

1. [ポリシー] ビューの [ロックダウン除外] ペインにある [信赖するハッシュ値] に移動します。
2. 削除するハッシュ値を選択します。
3. [削除] ボタンをクリックすると、確認画面が表示されます。

4. [確認] ボタンをクリックして、選択したエントリを削除します。



## 信頼するデジタル証明書の設定

ハッシュ値と同様に、アプリケーションベンダや組織によって作成される信頼するデジタル証明書は、StellarProtect (Legacy Mode) が信頼できるアプリケーションを識別するのに役立ちます。

## 信頼するデジタル証明書をインポートする

### 手順

1. [エージェント] ビューで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。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
  - [ポリシーの継承] リンクをクリックします。
  - [処理] のポリシーアイコン (⚙️) をクリックします。
3. [ポリシー] ビューの [ロックダウン除外] ペインにある [信頼するデジタル証明書] に移動します。
4. [ファイルの選択] ボタンをクリックし、追加する証明書を見つけてクリックします。
5. 許可済みのインストーラによって作成または変更されたすべてのファイルを [許可リスト] に自動的に追加するように、[インストーラ] スイッチを切り替えて有効にします。

- [インポート] ボタンをクリックして信頼するデジタル証明書を追加し、設定を保存します。



## 信頼するデジタル証明書を削除する

### 手順

- [ポリシー] ビューの [ロックダウン除外] ペインにある [信頼するデジタル証明書] に移動します。
- 削除する信頼するデジタル証明書を選択します。
- [削除] ボタンをクリックすると、[信頼するデジタル証明書の削除] 画面が表示されます。
- [確認] ボタンをクリックして、選択したエントリを削除します。



## 除外パスの設定

除外パスは、ファイルまたはファイルフォルダを直接指定して、ファイルの実行を許可するためには使用されます。

## ファイル、フォルダ、または正規表現を除外パスとして追加する

### 手順

1. [エージェント] ビューで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。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
  - [ポリシーの継承] リンクをクリックします。
  - [処理] のポリシーアイコン (💡) をクリックします。
3. [ポリシー] ビューの [ロックダウン除外] ペインにある [除外パス] に移動します。
4. [追加] ボタンをクリックすると、[除外パスの追加] 画面が表示されます。
5. 除外のタイプとして、**ファイル、フォルダ、または正規表現**を選択します。
6. 除外対象のファイルシステムパスを入力します。
7. [追加] ボタンをクリックして单一の除外パスを追加し、設定を保存します。

## 除外パスを編集する

### 手順

1. 編集する除外パスを選択します。
2. [編集] ボタンをクリックすると、[除外パスの編集] 画面が表示されます。
3. 単一の除外パスを変更したら、[編集] ボタンをクリックして設定を保存します。

## 除外パスを削除する

### 手順

1. 削除する除外パスを選択します。
2. [削除] ボタンをクリックすると、[除外パスの削除] 画面が表示されます。
3. [確認] ボタンをクリックして、選択したエントリを削除します。

## 書き込み制御の設定

書き込み制御により、特定のファイルまたはフォルダの内容を、不正なユーザやアプリケーションによる変更から保護できます。

## 書き込み制御にファイル、フォルダ、レジストリキー、またはレジストリ値を追加する

### 手順

1. [エージェント] ビューで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。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
  - [ポリシーの継承] リンクをクリックします。
  - [処理] のポリシーアイコン (P) をクリックします。
3. [ポリシー] ビューの [ロックダウン除外] ペインにある [書き込み制御] に移動します。
4. [追加] ボタンをクリックすると、[書き込み制御の追加] 画面が表示されます。
5. 制御のタイプとして、ファイル、フォルダ、レジストリキー、またはレジストリ値を選択します。
6. 書き込み制御の対象とするオブジェクトのパスを入力します。
7. [除外プロセスタイプ] を設定します。
  - すべてのユーザおよびアプリケーションからの書き込みを制限する

- すべてのユーザおよびアプリケーションからの書き込みを許可する
  - 書き込み可能なアプリケーションを指定する
8. [追加] ボタンをクリックして設定を保存します。

## 書き込み制御を編集する

### 手順

- [ポリシー] ビューの [ロックダウン除外] ペインにある [書き込み制御] に移動します。
- 編集する制御のタイプを選択します。
- [編集] ボタンをクリックして設定を保存します。

書き込み制御の追加

×

保護タイプ:  ファイル  フォルダ  レジストリキー  レジストリキー/レジストリ値

パス:

除外プロセスタイプ:  すべてのユーザおよびアプリケーションからの書き込みを制限する  すべてのユーザおよびアプリケーションからの書き込みを許可する  書き込み可能なアプリケーションを指定する

**追加** **キャンセル**

## 書き込み制御を削除する

### 手順

- [ポリシー] ビューの [ロックダウン除外] ペインにある [書き込み制御] に移動します。
- 削除する制御のタイプを選択します。
- [削除] ボタンをクリックすると、[書き込み制御の削除] 画面が表示されます。
- [確認] ボタンをクリックして、選択したエントリを削除します。

## 除外をインポートする

除外をインポートすることにより、ハッシュ値、信頼するデジタル証明書、除外パス、および書き込み制御の設定をグループ間で移動できます。

### ロックダウン除外

許可リストのロックダウン除外を設定します。

 除外のインポート

 除外のエクスポート

### 手順

- [エージェント] ビューで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。
- 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
  - [ポリシーの継承] リンクをクリックします。
  - [処理] のポリシーアイコン (🛡) をクリックします。
- [ポリシー] ビューの [ロックダウン除外] ペインにある [除外のインポート] ボタンに移動します。
- [除外のインポート] ボタンをクリックすると、[除外のインポート] 画面が表示されます。
- [ファイルの選択] ボタンをクリックし、エクスポートした設定を含むファイル (例: **exclusion.xml**) を選択します。
- [インポート] ボタンをクリックします。



## 除外をエクスポートする

### 手順

1. [ポリシー] ビューの [ロックダウン除外] ペインにある [除外のエクスポート] に移動します。
2. [除外のエクスポート] ボタンをクリックすると、除外設定がブラウザからダウンロードされます。

## 予約検索を設定する

[予約検索の設定] ペインから、検索の実行間隔、検索前のコンポーネントアップデートの設定、検索対象ファイル、検索時に実行する処理、および検索から除外するファイルを設定できます。



### 注意

検索機能は、Stellar 無期限版では利用できません。

予約検索の設定

予約検索  予約

[詳細設定](#)

予約

×

更新間隔:  日次  
 週次、毎週

開始時刻:  :

## 予約検索

### 手順

1. [エージェント] ビューで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。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
  - [ポリシーの継承] リンクをクリックします。
  - [処理] のポリシーアイコン (🛡) をクリックします。
3. [ポリシー] ビューの [予約検索の設定] ペインにある [予約] ボタンに移動します。
4. [実行間隔] ([日次]、[週次]、または[月次]) と [開始時刻] を設定します。
5. [確認] ボタンをクリックします。

## コンポーネントアップデート

### 手順

1. [ポリシー] ビューの [予約検索の設定] ペインにある [詳細設定] に移動します。
2. [コンポーネントアップデート] に移動します。
3. コンポーネントアップデートに失敗した場合でも検索を継続するには、該当するチェックボックスをオンにします。



### 注意

チェックボックスをオフにすると、検索が実行されないためコンポーネントをアップデートできません。

#### コンポーネントアップデート

検索を開始する前に、エージェントは最新コンポーネントのダウンロードを自動的に試行します。

コンポーネントアップデートに失敗した場合でも検索を継続する

## 検索対象ファイル

### 手順

1. [ポリシー] ビューの [予約検索の設定] ペインにある [詳細設定] に移動します。
2. [検索対象ファイル] に移動します。
3. [すべてのローカルフォルダ] または [初期設定のフォルダ (クイック検索)] を選択するか、[特定のフォルダ] を選択して検索するフォルダのパスを入力します。
4. すべてのリムーバブルドライブを検索するには、[リムーバブルドライブを検索する] の横にあるチェックボックスをオンにします。
5. すべての圧縮ファイルを検索するには、[圧縮ファイルを検索する] の横にあるチェックボックスをオンにします。



#### 注意

このチェックボックスの下で、圧縮ファイル内の検索する階層数を選択できます。

---

6. 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する] チェックボックスをオンにし、ファイルサイズを **1~9999MB** の間で入力します。

検索対象ファイル

すべてのローカルフォルダ  
 初期設定のフォルダ (クイック検索)  
 特定のフォルダ

リムーバブルドライブを検索する  
 圧縮ファイルを検索する。 最大階層:

30 MBを超えるファイルをスキップする (1 - 9999)

## 検出時の処理

### 手順

1. [ポリシー] ビューの [予約検索の設定] ペインにある [詳細設定] に移動します。
2. [検出時の処理] に移動します。

#### 検出時の処理

- トレンドマイクロの推奨処理を使用する [\(i\)](#)
- 処理しない
- 駆除する、駆除処理に失敗した場合は削除する
- 駆除する、駆除処理に失敗した場合は隔離する
- 駆除する、駆除処理に失敗した場合は無視する

- 事前に設定された検出時の処理を使用するには、[トレンドマイクロの推奨処理を使用する] を選択します。これは検出時の処理に詳しくない場合、または適切な処理がわからない場合に適しています。
- 結果を読み出すだけで、検出されたファイルに処理を実行しない場合は、[処理しない] を選択します。
- 対象ファイルを復元できない場合に、初期設定でそのファイルを削除するには、[駆除する、駆除処理に失敗した場合は削除する] を選択します。
- 対象ファイルを復元できない場合に、初期設定でそのファイルを隔離するには、[駆除する、駆除処理に失敗した場合は隔離する] を選択します。
- 対象ファイルを復元できない場合に、初期設定でそのファイルを無視するには、[駆除する、駆除処理に失敗した場合は無視する] を選択します。

## 検索除外

### 手順

1. [ポリシー] ビューの [予約検索の設定] ペインにある [検索除外] に移動します。
2. 検索から除外するファイル、フォルダ、または拡張子を指定します。
  - **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:** 検索から除外するファイルのタイプをファイル拡張子で指定します。

## デバイスコントロールを設定する

USB ドライブ、CD/DVD ドライブ、フロッピーディスクドライブやネットワークドライブなどの外部デバイスのアクセスを許可またはブロックします。除外を設定して、信頼する USB デバイスからのアクセスを許可することもできます。

**デバイスコントロール (0)**

USB ドライブ、CD/DVD ドライブ、フロッピーディスクドライブやネットワークドライブなどの外部デバイスのアクセスをブロックします。除外を設定して、次の信頼する USB デバイスからのアクセスを許可することができます。

**+ 追加**

ベンダID	製品ID	シリアル番号	処理
表示するデータがありません			

## デバイス情報を取得する

次のいずれかの方法で、エージェントに接続されているデバイスの情報を取得します。

- エージェントで**デバイスマネージャ**を開きます。
- エージェントで、次の項に示すコマンドを指定して **SLCmd.exe** を実行します。
- StellarOne の管理サーバ画面で [エージェントイベント] 画面に移動し、**エージェントイベント ID 5001** のリムーバブルデバイスの [詳細情報の表示] をクリックします。

## 信頼する USB デバイスのコマンド

StellarProtect (Legacy Mode) エージェントで、コマンドラインインターフェースに次の形式でコマンドを入力して、信頼する USB デバイスリストを設定します。

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

次の表は、使用可能なパラメータの省略表記一覧を示しています。

パラメータ	省略表記	用法
trustedusbdevice	tud	信頼する USB デバイスリストを管理します

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

コマンド	パラメータ	説明
show usbinfo	<drive_letter>	USB ストレージデバイスの識別子 (VID/PID/SN) を表示します たとえば、USB ストレージデバイスが D ドライブにある場合は、次のように入力します。 SLCmd.exe -p <admin_password> show usbinfo d
show trustedusbdevice		すべての信頼する USB ストレージデバイスを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show trustedusbdevice

コマンド	パラメータ	説明
add trustedusbdevice	[-vid <VID>] [-pid <PID>] [-sn <SN>]	<p>指定した識別子を持つ、信頼する USB ストレージデバイスを追加します。識別子は 1 つ以上指定する必要があります。</p> <p>たとえば、次のように入力します。</p> <p>SLCmd.exe -p &lt;admin_password&gt; add trustedusbdevice -sn 123456</p>
remove trustedusbdevice	[-vid <VID>] [-pid <PID>] [-sn <SN>]	<p>指定した識別子を持つ、信頼する USB ストレージデバイスを削除します。</p> <p>識別子は 1 つ以上指定する必要があります。</p> <p>たとえば、次のように入力します。</p> <p>SLCmd.exe -p &lt;admin_password&gt; remove trustedusbdevice -sn 123456</p>

## 信頼する USB デバイスを追加する

デバイス情報に基づいて、管理下のエージェントへのアクセスを許可する USB ストレージデバイスを指定できます。

### 手順

1. [エージェント] リストで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。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
  - [ポリシーの継承] リンクをクリックします。
  - [処理] のポリシーアイコン (🛡) をクリックします。
3. [ポリシー] ビューで [デバイスコントロール] ペインに移動します。
4. スイッチを切り替えて、[ベンダ ID、シリアル番号、および製品 ID によって信頼する USB デバイスのみを許可する] を有効にします。[信頼する USB デバイスリスト] が表示されます。
5. [追加] ボタンをクリックすると、[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、[OK] ボタンをクリックします。
  - **ベンダ ID**
  - **製品 ID**

- シリアル番号

信頼するUSBデバイスの追加

信頼するUSBデバイスについて、次の情報を1つ以上指定してください。

ベンダID:

製品ID:

シリアル番号:

注意: エージェントに接続されているデバイスの情報を取得するには、対象エージェントで次のいずれかを実行してください。  
(1) [デバイス管理] を開く  
(2) SLCmd.exe show usbinfo <drive\_letter>コマンドを使用する

OK キャンセル



#### 注意

エージェントにある信頼する USB デバイスのリストを表示するには、エージェントの設定をエクスポートします。エージェントにある信頼する USB デバイスのリストを手動で設定するには、SLCmd コマンドを使用してエージェントの設定をエクスポートするか、変更を行うか、アップデートした設定ファイルをインポートします。

## 信頼する USB デバイスを編集する

### 手順

- [ポリシー] ビューで [デバイスコントロール] ペインに移動します。
- スイッチを切り替えて、[ベンダ ID、シリアル番号、および製品 ID によって信頼する USB デバイスのみを許可する] を有効にします。[信頼する USB デバイスリスト] が表示されます。
- 編集する信頼する USB デバイスを選択します。
- [編集] ボタンをクリックすると、確認画面が表示されます。
- [OK] ボタンをクリックして設定を保存します。

## ポリシーの設定により、信頼する USB デバイスを削除する

### 手順

1. [ポリシー] ビューで [デバイスコントロール] ペインに移動します。
2. スイッチを切り替えて、[ベンダ ID、シリアル番号、および製品 ID によって信頼する USB デバイスのみを許可する] を有効にします。[信頼する USB デバイスリスト] が表示されます。
3. 削除する信頼する USB デバイスを選択します。
4. [削除] ボタンをクリックすると、[通知] 画面が表示されます。
5. [確認] ボタンをクリックして設定を保存します。

## 設定のインポートにより、信頼する USB デバイスを削除する

### 手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。[エージェント] 画面が表示されます。
2. 1つ以上のエージェントを選択します。
3. [インポート/エクスポート] → [エージェントの設定のエクスポート] の順にクリックします。
4. [ステータス] で [ダウンロード] リンクをクリックし、エージェント設定ファイルをコンピュータにダウンロードします。
5. エージェント設定ファイルをテキストエディタで開き、<DeviceException> セクションを見つけます。

信頼する USB デバイスが追加されていない場合、空の <DeviceException> セクションが次のように表示されます。

```
<StorageDeviceBlocking Enable="no" ActionMode="1">
    <DeviceException>
        <DeviceGroup name="UserDefined"/>
    </DeviceException>
</StorageDeviceBlocking>
```

信頼する USB デバイスの 2 つのエントリが追加されている場合、<DeviceException> セクションは次のように表示されます。

```
<StorageDeviceBlocking Enable="no" ActionMode="1">
<DeviceException>
    <DeviceGroup name="UserDefined">
        <Device vid="781" pid="5151" sn="2444130A5442A4F5"/>
        <Device vid="951" pid="1666"
            sn="E03F49AEC0DDF351E913003F"/>
    </DeviceGroup>
</DeviceException>
</StorageDeviceBlocking>
```

6. 目的の信頼する USB デバイスのエントリを削除し、エージェント設定ファイルを保存します。
7. 更新したエージェント設定ファイルをインポートします。

## ユーザ指定不審オブジェクトを設定する

ユーザ指定不審オブジェクトを設定すると、TXOne の研究者により発見された不正プログラムからシステムを保護することができます。

**ユーザ指定不審オブジェクト (0)**

新しい脅威情報に更新して、ネットワーク上のまだ識別されていない不審オブジェクトから保護します。

**+** 追加

ハッシュ/ファイルパス	タイプ	メモ	処理
表示するデータがありません			

## ユーザ指定不審オブジェクトを追加する

### 手順

1. [エージェント] リストで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。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
  - [ポリシーの継承] リンクをクリックします。
  - [処理] のポリシーアイコン (🛡) をクリックします。
3. [ポリシー] ビューで [ユーザ指定不審オブジェクト] ペインに移動します。
4. [追加] ボタンをクリックすると、[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。
5. 変更後、[OK] ボタンをクリックして設定を保存します。



## ユーザ指定不審オブジェクトを削除する

### 手順

1. [ポリシー] ビューで [ユーザ指定不審オブジェクト] ペインに移動します。
2. 削除するハッシュ/ファイルパスを選択します。
3. [削除] ボタンをクリックすると、確認画面が表示されます。

4. [確認] ボタンをクリックして、選択した項目を削除します。

## エージェントのパスワードを設定する

StellarOne の管理サーバ画面を使用して、StellarProtect (Legacy Mode) エージェントのパスワードをリモートで更新します。新しいパスワードの作成に古いエージェントのパスワードは必要ありません。

### 手順

1. [エージェント] リストで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。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
  - [ポリシーの継承] リンクをクリックします。
  - [処理] のポリシーアイコン (🛡) をクリックします。
3. [ポリシー] ビューで [エージェントのパスワード] ペインに移動します。
4. [新しいパスワード] と [パスワードの確認] を入力します。
5. [保存] ボタンをクリックして設定を保存します。

エージェントのパスワード

新しいパスワード\* .....

パスワードの確認\* .....

パスワードポリシー

パスワードは8~64文字以内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: | > " : < \



### 注意

この機能を利用できるのは、管理者またはオペレータの権限を持つユーザだけです。管理者またはオペレータの権限を持つユーザは、エージェント管理者のパスワードをリモートで変更できます。

# Patch を設定する

## 手順

1. [エージェント] リストで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。
2. 次のいずれかの方法を使用して [ポリシー] ビューを表示します。
  - [ポリシーの継承] リンクをクリックします。
  - [処理] のポリシーアイコン (🛡) をクリックします。
3. [ポリシー] ビューで [Patch] ペインに移動します。
4. 適用する Patch の横にあるチェックボックスをオンにします (複数可)。
5. [アップデート] リンクをクリックして、新しい Patch をインポートします。
6. リンクをクリックして、[ダウンロード/アップデート] 画面に移動します。
7. [確認] ボタンをクリックして設定を保存します。



### 注意

Patch のバージョンが現在のエージェントのバージョンよりも低い場合は、その Patch を適用しないでください。ステータスは非同期のままとなり、他のポリシーも配信されません。20 分待てば、他のポリシーがエージェントに適用可能になります。

## 第4章

# エージェントの保護と アップデート

## メンテナンスモードを設定する

エージェントで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 (Legacy Mode) 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。

たとえば、Mozilla Firefox をインストールまたはアップデートする必要がある場合は、メンテナンスモードを有効にしてインストールまたはアップデートを許可し、さらに処理中に作成または修正されたファイルを許可リストに追加します。

セキュリティ強化のため、メンテナンス期間後は**ファイルの検索**を有効にして**検出時の処理**を選択できます。



### 重要

メンテナنسモードを使用する前に、必要なアップデートを次のサポート対象プラットフォームに適用してください。

- Windows 2000 Service Pack 4 の場合、Microsoft Update カタログの Web サイトから更新プログラム KB891861 を適用します。
- Windows XP SP1 の場合、Windows XP SP2 にアップグレードします。

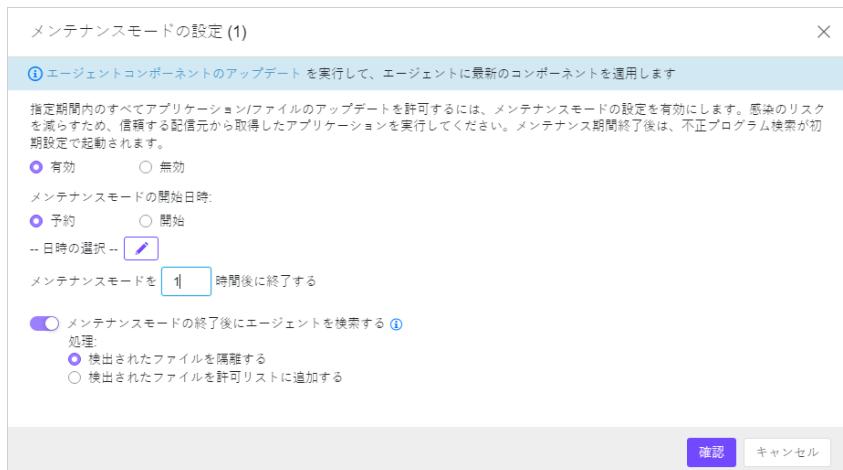
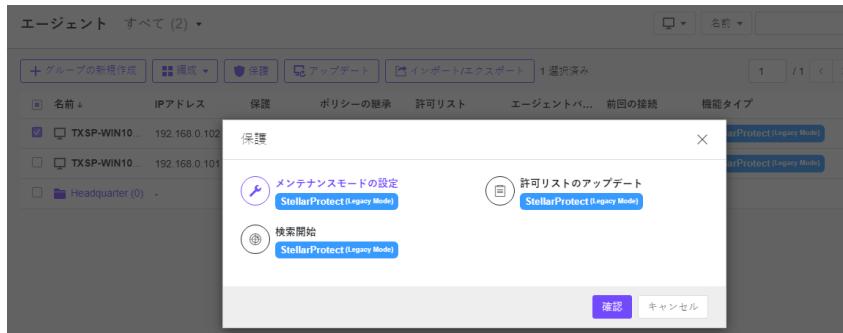


### 注意

- 感染のリスクを減らすため、メンテナنس期間中は、信頼する配信元から取得したアプリケーションのみをエージェント上で実行してください。
- エージェントでは、一度に 1 つの予約されたメンテナنس期間を開始できます。新しいメンテナنس期間を設定すると、まだ開始されていない既存のメンテナنسの予約が上書きされます。
- メンテナنسモードを終了しようとしているときにエージェントを再起動すると、StellarProtect (Legacy Mode) がキュー内のファイルを許可リストに追加できなくなります。
- メンテナنس期間中、エージェントの Patch のアップデートは実行できません。
- メンテナنسモードが有効な場合、StellarProtect (Legacy Mode) では、メンテナنس期間中にエージェントの再起動を必要とする Windows Update がサポートされません。
- メンテナنس期間中にネットワークフォルダにファイルを配信するインストーラを実行するには、StellarProtect (Legacy Mode) にネットワークフォルダに対するアクセス権限が必要です。
- メンテナنسモードでは Microsoft Windows Visual Studio デバッガはサポートされないことに注意してください。

## 手順

- [エージェント] ビューで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。
- 横にあるチェックボックスをオンにして、エージェント (またはグループ) を 1 つ以上選択します。
- [エージェント] 画面の上部にあるツールバーで  ボタンをクリックします。
- [メンテナンスマードの設定] オプションをクリックし、さらに [保護] メニュー画面の [確認] ボタンをクリックします。設定画面が表示されます。



5. [有効] または [無効] を選択します。
  - メンテナスマードの設定を開始するには、[有効] をクリックします。
  - メンテナスマードを終了するか、予約されたメンテナス期間を中止するには、[無効] をクリックします。
6. [予約] または [開始] を選択します。
  - [予約] を選択した場合は、メンテナス期間を指定する必要があります。
  - [メンテナスマードの終了後にエージェントを検索する] を選択すると、StellarProtect (Legacy Mode) はメンテナス期間終了後にエージェントで脅威を検索します。
7. 目的の処理を選択します。
  - 検出されたファイルを隔離する
  - 検出されたファイルを許可リストに追加する



### 注意

StellarProtect (Legacy Mode) は、メンテナス期間中にエージェントで作成、実行、または変更されたファイルを検索します。

8. [確認] ボタンをクリックして、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。
9. [コマンド配信] 画面に配信ステータスが表示されます。この画面は、[閉じる] ボタンをクリックして閉じることができます。

コマンド配信 ×

日付と時刻	2022-12-21T18:37:57+08:00		
イベント	メンテナスマードの設定		
すべてのステータス (1) ▾			
エージェント	IPアドレス	グループ	ステータス
WIN-8M4GLJBMP6Z	192.168.250.102	All	<input type="radio"/> 配信しています...

閉じる

## 許可リストをアップデートする

アプリケーション制御が有効な場合は、実行したいアプリケーションを新規インストールした後、StellarProtect (Legacy Mode) エージェントの許可リストを定期的にアップデートしてください。許可リストのアップデートを実行すると、選択したエージェントの許可リストが再作成され、新たに検出されたアプリケーションがグローバルな許可リストに追加されます。

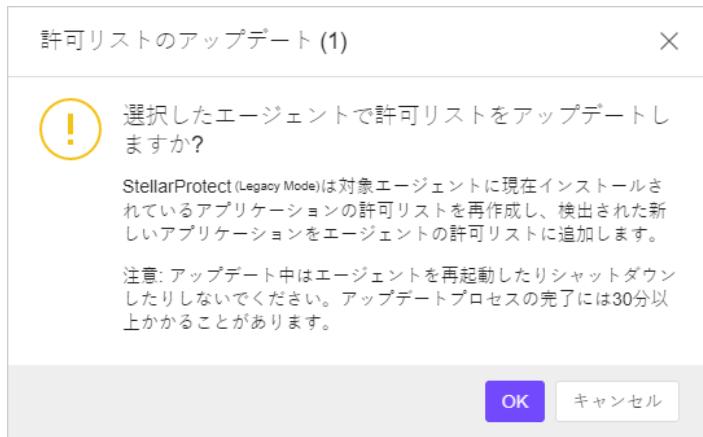
StellarProtect (Legacy Mode) でエージェントの保護を開始するには、最初に、エージェントをチェックしてシステムの正常な実行に必要なアプリケーションとファイルを確認する必要があります。StellarProtect (Legacy Mode) のアプリケーション制御が有効な場合は、許可リストに含まれるアプリケーションのみを実行できます。

許可リストを設定した後は、メンテナンスマードを有効にすることで新しいプログラムも追加できるようになり、新しいファイルまたは変更済みのファイルが許可リストに追加されます。



### 手順

- [エージェント] リストで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。
- 横にあるチェックボックスをオンにして、エージェント (またはグループ) を 1 つ以上選択します。
- [エージェント] 画面の上部にあるツールバーで  ボタンをクリックします。
- [許可リストのアップデート] オプションをクリックし、さらに [保護] メニュー画面の [確認] ボタンをクリックします。確認画面が表示されます。
- [OK] ボタンをクリックして許可リストをアップデートします。

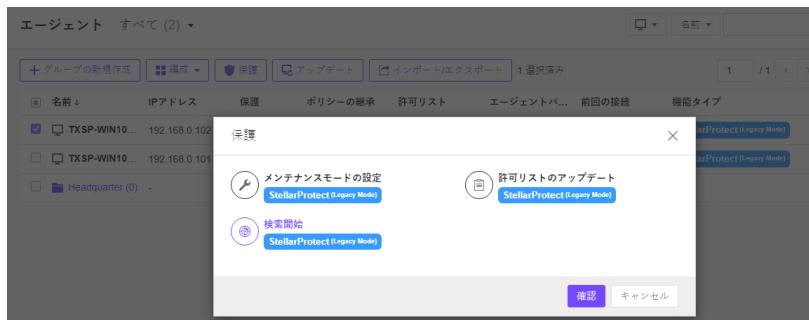


### 注意

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。

## 検索開始を設定する

選択したエージェントで手動検索を開始し、検索を設定して、1 つまたは複数の StellarProtect (Legacy Mode) の対象エージェントに配信できます。



## 検索開始を実行する

感染が疑われる 1 つ以上のエージェントに対して検索開始を実行できます。

### 手順

1. [エージェント] リストで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。
2. 横にあるチェックボックスをオンにして、エージェント (またはグループ) を 1 つ以上選択します。
3. [エージェント] 画面の上部にあるツールバーで  ボタンをクリックします。
4. [検索開始] オプションをクリックし、さらに [保護] メニュー画面の [確認] ボタンをクリックします。確認画面が表示されます。
5. 検索の設定後、[OK] ボタンをクリックして検索開始を実行します。

サーバから選択した StellarProtect (Legacy Mode) エージェントに通知が送信されます。検索のステータスについてログを確認できます。

コマンド配信

日付と時刻 2022-12-21T18:46:20+08:00

イベント 検索開始

すべてのステータス (1) ▾

エージェント	IPアドレス	グループ	ステータス
WIN-8M4GLJBMP6Z	192.168.250.102	All	2022-12-06T16:48:34+08:...

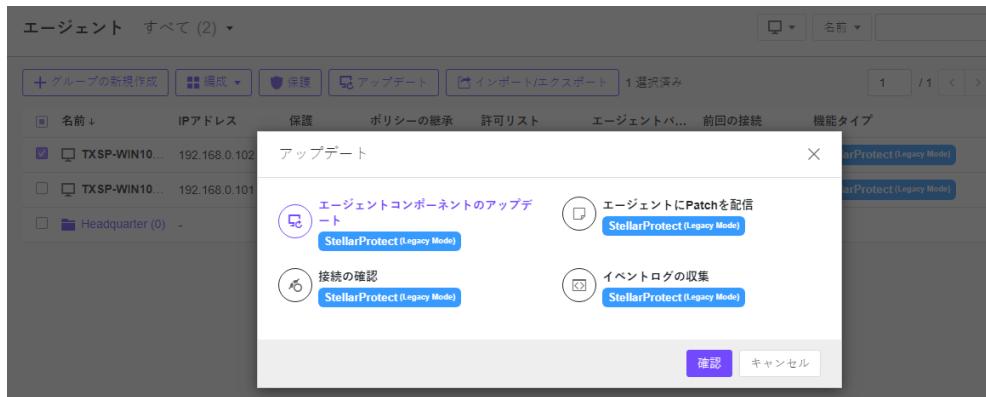
閉じる

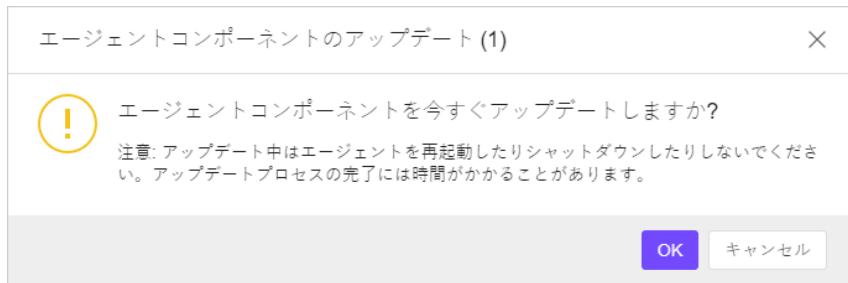
## エージェントコンポーネントのアップデート

選択したエージェントに対して、StellarOne からエージェントコンポーネントのアップデートプロセスを開始できます。エージェントは、最新のコンポーネントアップデートをダウンロードします。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で、最新のセキュリティリスクからエージェントを保護できます。

### 手順

1. [エージェント] 表で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。
2. 横にあるチェックボックスをオンにして、エージェント（またはグループ）を 1 つ以上選択します。
3. [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。
4. [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、さらに [アップデート] メニュー画面の [確認] ボタンをクリックします。確認画面が表示されます。
5. [OK] ボタンをクリックしてエージェントコンポーネントをアップデートします。





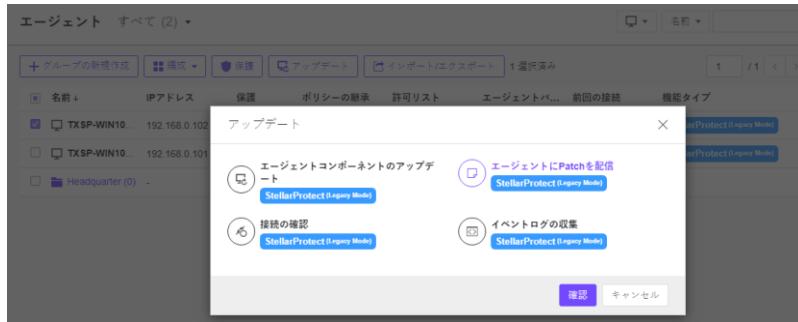
## エージェントに Patch を配信する

StellarOne を使用して、アップロードした Patch ファイルを選択した StellarProtect (Legacy Mode) エージェントに配信することで、管理サーバ画面からリモートでエージェントをアップグレードできます。

### 手順

1. [エージェント] リストで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。
2. 横にあるチェックボックスをオンにして、エージェント (またはグループ) を 1 つ以上選択します。
3. [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。
4. [エージェントに Patch を配信] オプションをクリックし、さらに [アップデート] メニュー画面の [確認] ボタンをクリックします。確認画面が表示されます。

5. 設定後、[OK] ボタンをクリックします。



アップロードプロセスの完了を待ちます。StellarOne でファイルの有効性が検証されると、選択したエージェントに Patch ファイルが配信されます。



### 注意

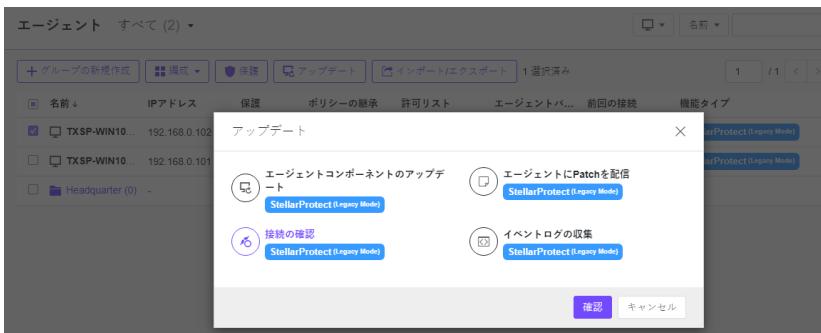
Windows 7 SP1 以前のバージョンでは、StellarProtect (Legacy Mode) 1.0 エージェントへの Patch のリモート配信はサポートされません。

# 接続を確認する

選択した StellarProtect (Legacy Mode) エージェントの接続ステータスを確認します。

## 手順

1. [エージェント] リストで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。
2. 横にあるチェックボックスをオンにして、エージェント (またはグループ) を 1 つ以上選択します。
3. [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。
4. [接続の確認] オプションをクリックし、さらに [確認] ボタンをクリックします。画面が表示されます。
5. [ステータス] または [製品] の基準を選択して、接続ステータスを確認します。



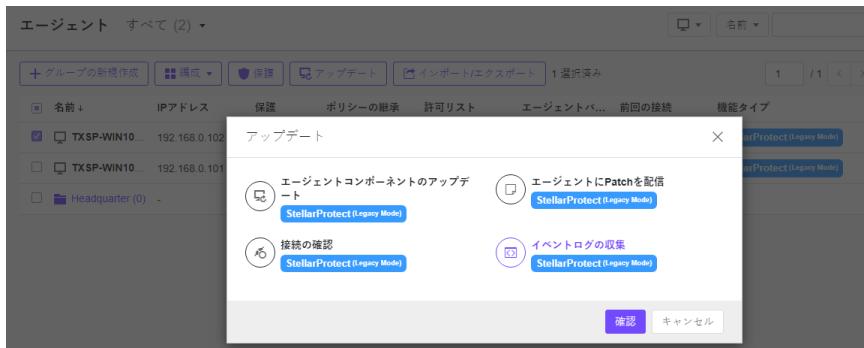


### 注意

- StellarOne サーバに接続できないエージェントを特定したら、接続されていないエージェントのネットワーク接続を確認することをお勧めします。
- 初期設定では、エージェントは StellarOne の管理サーバ画面と **20** 分ごとに自動同期されます。

## イベントログを収集する

ログにはエージェントのアクティビティに関する情報が含まれています。イベントログを収集することで、StellarOne のデータベースを更新し、選択したエージェント情報を最新の状態にすることができます。



### 手順

- [エージェント] リストで対象のエージェントに移動します。
- 横にあるチェックボックスをオンにして、エージェントを 1 つ以上選択します。
- [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。
- [イベントログの収集] オプションをクリックし、さらに [確認] ボタンをクリックします。

ログとステータスが StellarProtect (Legacy Mode) エージェントから StellarOne に正常に送信されると、[前回の接続] 列に表示される日付と時刻が更新されます。



### 注意

ユーザは次のログの情報レベル (Setup.ini) を有効にして、エージェントのアクティビティに関する情報を含める必要があります。

```
[EventLog]
Enable = 1
Level_WarningLog = 1
Level_InformationLog = 1
```

---

## 第 5 章

# エージェントの設定の インポート/エクスポート

以下の機能はエージェントレベル専用です。ユーザがリストから任意のグループを選択する際、この機能は無効化されています。

## エージェントの設定をエクスポートする

StellarOne の管理サーバ画面からエージェントの設定と許可リストをエクスポートしてダウンロードすることにより、それらをリモートで取得できます。

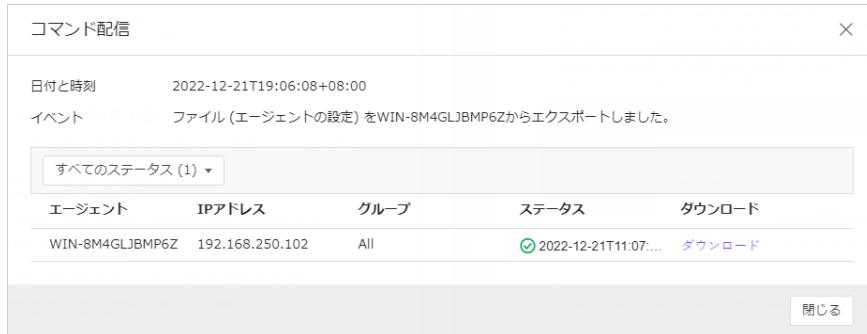


## エージェントの設定をエクスポートする

### 手順

1. [エージェント] リストで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。
2. 横にあるチェックボックスをオンにして、対象のエージェントを選択します。
3. [エージェント] 画面の上部にあるツールバーで **[Import/Export]** ボタンをクリックします。
4. [エージェントの設定のエクスポート] オプションをクリックし、さらに [Import/Export] メニュー画面の [確認] ボタンをクリックします。画面が表示されます。

5. [ダウンロード] リンクをクリックして、エージェントの設定ファイルをダウンロードします。  
[詳細] ポップアップ画面で進行状況を確認できます。



エージェント	IPアドレス	グループ	ステータス	ダウンロード
WIN-8M4GLJBMP6Z	192.168.250.102	All	2022-12-21T11:07:....	<a href="#">ダウンロード</a>

## 許可リストをエクスポートする

### 手順

- [エージェント] リストで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。
- 横にあるチェックボックスをオンにして、対象のエージェントを選択します。
- [エージェント] 画面の上部にあるツールバーで  ボタンをクリックします。

4. [許可リストのエクスポート] オプションをクリックし、さらに [インポート/エクスポート] メニュー画面の [確認] ボタンをクリックします。画面が表示されます。



5. [ダウンロード] リンクをクリックして、許可リストファイルをダウンロードします。[詳細] ポップアップ画面で進行状況を確認できます。



## エージェントの設定をインポートする

StellarOne の管理サーバ画面から、新しいエージェントの設定をリモートで適用できます。この機能により次のことが可能になります。

- エージェントの設定をリモートで上書きする
- 許可リストをリモートで上書きする

カスタマイズしたエージェントの設定ファイルまたは許可リストを必ず最初に準備してください。

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

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

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

## エージェントの設定をインポートする

### 手順

1. [エージェント] リストで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。
2. 横にあるチェックボックスをオンにして、対象のエージェントを選択します。
3. [エージェント] 画面の上部にあるツールバーで **【インポート/エクスポート】** ボタンをクリックします。

4. [エージェントの設定のインポート] オプションをクリックし、さらに [インポート/エクスポート] メニュー画面の [確認] ボタンをクリックします。画面が表示されます。



5. [ファイルの選択] をクリックしてファイルを選択し、[OK] ボタンをクリックして設定のインポートを開始します。



## 許可リストをインポートする

### 手順

- [エージェント] リストで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。
- 横にあるチェックボックスをオンにして、対象のエージェントを選択します。
- [エージェント] 画面の上部にあるツールバーで  インポート/エクスポート ボタンをクリックします。

4. [許可リストのインポート] オプションをクリックし、さらに [インポート/エクスポート] メニュー画面の [確認] ボタンをクリックします。画面が表示されます。



5. [ファイルの選択] をクリックしてファイルを選択し、[OK] ボタンをクリックして許可リストのインポートを開始します。



### 注意

[既存アプリケーションの信頼するハッシュ値を更新します。] スイッチは、(許可リスト内の) 既存の信頼するハッシュ値を上書きする場合に使用します。

# エージェントの処理

## タグを編集する

エージェントの識別と検索に役立つタグを編集できます。タグを編集するには、次の手順に従います。

- 各エージェントの [処理] メニューから
- [編成] ボタンの [タグの編集] から

### 手順

- [エージェント] 画面に移動します。
- 横にあるチェックボックスをオンにして、エージェントを1つ以上選択します。
- [処理] にある [さらに処理を表示] アイコンをクリックします。
- [タグの編集] をクリックし、内容を入力または変更します。
- [確認] ボタンをクリックします。



This screenshot shows the 'Agents' list screen. The 'Edit Tags' button is highlighted in the context menu for selected agents. The table displays agent details such as name, IP address, protection status, policy inheritance, permission list, agent version, last connection, function type, and processing status.



This screenshot shows the 'Agents' list screen with the 'Edit Tags' button highlighted in the context menu. The 'Edit Tags' option is expanded, showing sub-options: '保護' (Protection), 'ポリシーの継承' (Policy Inheritance), '許可リスト' (Permission List), 'エージェントバージョン' (Agent Version), '前回の接続' (Last Connection), '機能タイプ' (Function Type), and '処理' (Processing). The table structure is identical to the previous screenshot.

## 移動する

複数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エージェントをグループ化します。

- 各エージェントの [処理] メニューから
- [編成] ボタンの [タグの編集] から

### 手順

- [エージェント] 画面に移動します。
- 横にあるチェックボックスをオンにして、エージェントを1つ以上選択します。
- [処理] にある [さらに処理を表示] アイコンをクリックします。
- [移動] をクリックし、対象のグループ名を選択します。

エージェントを別のグループに移動

×

グループ名

すべて (2)  
 Daan (0)  
 Japan (0)  
 MuZha (0)  
 NeiHu (0)  
 StellarProtect-G1 (0)  
 Taipei (0)  
 Taiwan (0)  
 Xinyi (0)

確認 キャンセル

- [確認] ボタンをクリックします。

## 削除する

StellarOne サーバからエージェントを削除します。

エージェントの StellarOne からの削除は、エージェントのアンインストール時に試行されます。ただし、StellarProtect (Legacy Mode) が StellarOne に接続されていなければエージェントを削除することはできません。

エージェントを環境から削除する前にアンインストールできない場合、そのエージェントが [エージェント] 画面に表示されたままになることがあります。今後 StellarOne で管理しないエージェントを監視対象エージェントのリストから削除するには、[削除] 機能を使用します。

### 手順

1. [エージェント] 画面に移動します。
2. 横にあるチェックボックスをオンにして、エージェントを 1 つ以上選択します。
3. [処理] にある [さらに処理を表示] アイコンをクリックします。
4. [削除] をクリックし、対象のグループ名を選択します。
5. [確認] ボタンをクリックして、選択した項目を削除します。リストからエージェントが削除されます。



#### 注意

監視対象エージェントのリストからエージェントを削除しても、既存のエージェントイベントログは削除されません。

---

## 第 6 章

# StellarProtect (Legacy Mode) の監視

## StellarProtect (Legacy Mode) の監視

この章では、StellarOne の管理サーバ画面の監視方法の概要について説明します。

### ダッシュボードについて

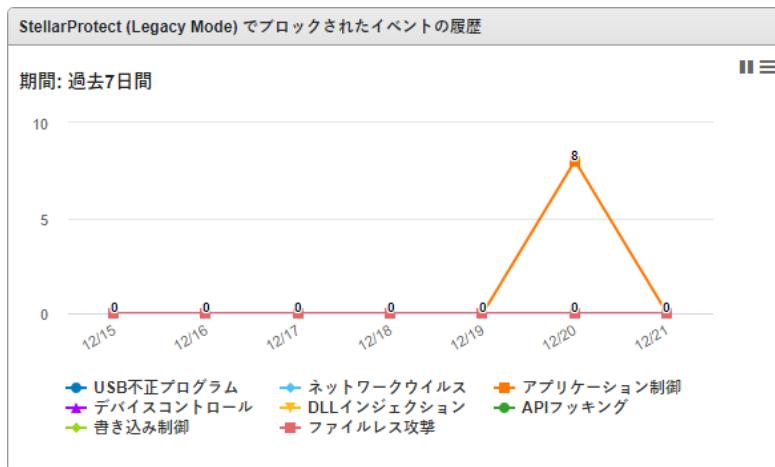
[ダッシュボード] では、[概要] タブに表示される情報を使用してイベントを監視します。このタブは、ユーザ指定のタブがない場合に初期設定で [ダッシュボード] に追加されます。

[概要] タブと [システム] タブに含まれる初期設定のウィジェットには、[ロックされたイベントの履歴]、[イベントをロックしたエージェントの上位]、[CPU 使用率]、[メモリ使用率]、および [ディスク使用率] があります。

## ロックされたイベントの履歴

このウィジェットには、指定した期間内にロックされたイベントの概要が表示されます。初期設定で、このウィジェットは [ダッシュボード] の [イベントの概要] タブに表示されます。表示アイコンをクリックすると、データが円グラフまたは折れ線グラフで表示されます。

- 指定した期間内のイベントデータのみを表示するには、[期間] のドロップダウンを使用します。
- グラフ下に並ぶカテゴリをクリックすると、そのイベントのデータが表示または非表示になります。
- グラフの値をクリックすると、ロックされたイベントの詳細が表示されます。



## ブロック件数が上位のエージェント

このウィジェットには、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 [イベントの概要] タブに表示されます。

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

イベントをブロックした StellarProtect (Legacy Mode) エージェントの上位			
期間: 過去7日間	エージェント名	説明	IP アドレス
	TXSP-WIN10-A01	-	192.168.0.101
	TXSP-WIN10-A01	-	192.168.0.102

[ブロックされたイベント] 列の値をクリックすると、そのイベントの詳細が表示されます。指定した期間内のイベントデータのみを表示するには、[期間] のドロップダウンを使用します。表示するイベント数を指定するには、[ウィジェット設定] ダイアログを開き、[表示するイベント] の値を選択します。

## ロックされた件数が上位のファイル

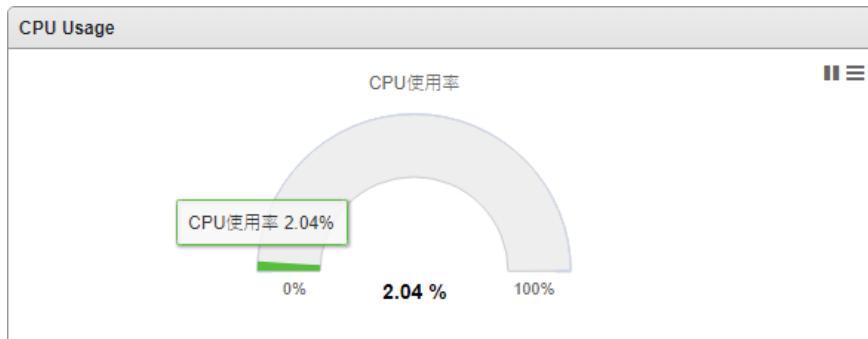
このウィジェットには、ロック件数が上位のファイルのリストが表示されます。初期設定ではダッシュボードに表示されません。

列	説明
ファイル名	ロックされたファイルの名前
ファイルハッシュ	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数
ロックされたイベント	当該ファイルについて報告されたブロックイベントの合計数

StellarProtect (Legacy Mode) でロックされたファイルの上位			
期間: 過去7日間	ファイル名	ファイルハッシュ	エージェント
	_PSScriptPolicyTe	1aaf53cec2717f47c	1
	_PSScriptPolicyTe	6c7e616bd9980501	1
	adksetup.exe	f0b63c943fcf9daf5c	1
	sdksetup.exe	4540251f0ca62da5	1

## CPU 使用率

このウィジェットには、CPU の使用率情報が表示されます。



## メモリ使用率

このウィジェットには、メモリの使用率情報が表示されます。



## ディスク使用率

このウィジェットには、ディスクの使用率情報が表示されます。



## 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、タブのレイアウトに応じて異なります。

タブ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. [ウィジェットの追加] をクリックして画面を表示します。

ダッシュボード



ダッシュボード

ダッシュボード エージェント ログ ▾ 管理 ▾ バージョン情報

ダッシュボード

資産 (5)  
システム (3)

イベントをブロックしたStellarProtect (Legacy Mode) エージェントの上位  
イベントのブロック数が最も多い上位エージェントを表示します。

StellarProtect (Legacy Mode) でブロックされたイベントの履歴  
指定した期間内にブロックされたイベントを表示します。

StellarProtect (Legacy Mode) でブロックされたファイルの上位  
最もブロックされたファイルを表示します。

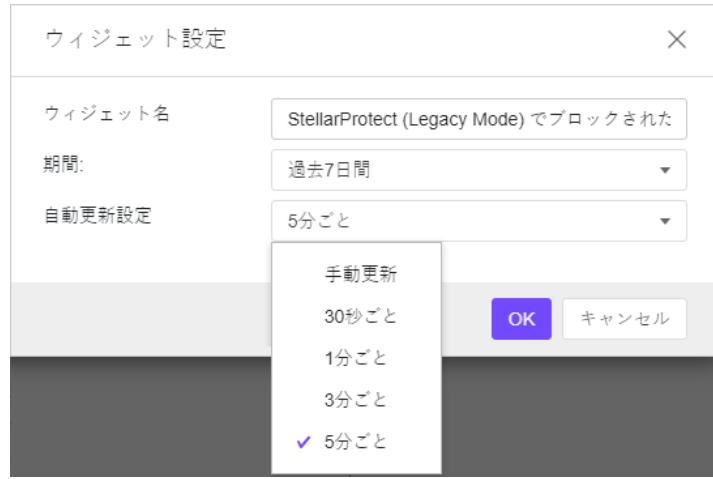
追加 キャンセル このタブで現在選択されているウィジェットです (10/10)。

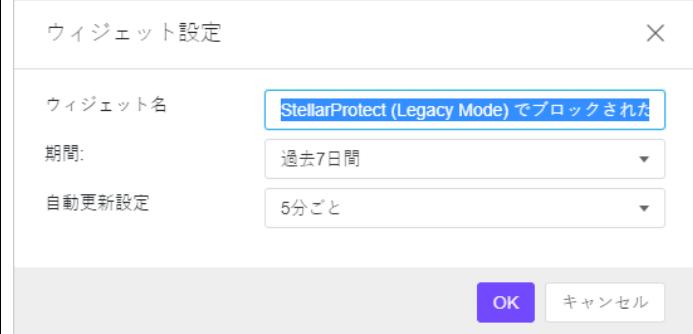
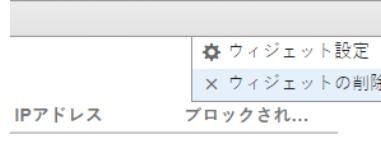
This screenshot shows the txOne dashboard interface. At the top, there are tabs for 'Summary' and 'System'. Below the tabs, there are buttons for 'タブ設定' (Tab Settings), 'ウィジェットの追加' (Add Widget) with a red box around it, and '削除' (Delete). The main content area is titled 'ダッシュボード' and shows three widget cards. Each card has a checkbox and a description: '資産 (5)' and 'システム (3)'. The first card is for 'StellarProtect (Legacy Mode) でブロックされたイベントの上位' (Top blocked events), the second for 'StellarProtect (Legacy Mode) でブロックされたイベントの履歴' (Event history), and the third for 'StellarProtect (Legacy Mode) でブロックされたファイルの上位' (Top blocked files). At the bottom, there are '追加' (Add) and 'キャンセル' (Cancel) buttons, and a message stating 'このタブで現在選択されているウィジェットです (10/10)' (This tab contains 10 selected widgets).

4. 現在のタブに追加するウィジェットを1つ以上選択し、[追加] をクリックします。

## ウィジェットを使用する

各ウィジェットで次のタスクを実行します。

タスク	手順
ウィジェットの移動	ウィジェット上部のタイトルバーをクリックしたままドラッグして、タブ内の任意の場所に移動します。
ウィジェットのサイズ変更	ウィジェットの端をドラッグしてサイズを変更します。
ウィジェットデータの表示更新	最初は[ウィジェット設定]で[自動更新設定]を指定します(初期設定値は[5分ごと])。
	
ウィジェット名の変更	<ol style="list-style-type: none"> <li>1. ウィジェットの上部にある[他のオプション]アイコンをクリックします。</li> <li>2. [ウィジェット設定]を選択します。[ウィジェット設定]画面が表示されます。</li> <li>3. わかりやすいウィジェット名を入力します。</li> </ol>

タスク	手順
	
ウィジェットを閉じる	<ol style="list-style-type: none"> <li>1. ウィジェットの上部にある [他のオプション] アイコンをクリックします。</li> <li>2. [ウィジェットの削除] を選択します。</li> </ol> 
期間の設定	<p>指定した期間のデータを表示します (初期設定値は [過去 7 日間])。</p> 

## [エージェントイベント]画面について

[エージェントイベント]画面を表示するには、管理サーバ画面の上部にあるナビゲーションで、[ログ]→[エージェントイベント]の順に選択します。この画面には、StellarOne の管理下のエージェントの許可リストにないアプリケーションに関するイベントのリストが表示されます。

StellarProtect (Legacy Mode) は、「機能の状態」に基づいて、次の表のイベントに対応した処理を行い、ログを生成します。イベントログには、許可リストにないファイルと実行された処理に関する、管理下のエージェントからの情報が含まれます。

イベント	機能の状態	StellarProtect (Legacy Mode) の処理
エージェントの許可リストにないファイルが動作しようとしたり、エージェントに変更を加えようとする	ロックダウンが無効	ファイルの動作を許可します
	ロックダウンが有効	ファイルをロックし、ユーザ処理を求めるプロンプトを表示します
ストレージデバイス (CD/DVD ドライブ、フロッピーディスク、または USB デバイス) がエージェントにアクセスしようとする	デバイスコントロールが無効	デバイスのアクセスを許可します
	デバイスコントロールが有効	(デバイスの種類がリムーバルデバイスの場合) デバイスのアクセスを拒否し、ユーザ処理を求めるプロンプトを表示します

次の表は、イベントに対するユーザ処理を示しています。

ユーザ処理	説明
許可リストに追加	検出されたタイミングではファイルの実行を防いだり USB デバイスのエンドポイントへのアクセスを拒否したりしますが、ファイルまたは USB デバイスをエージェントの許可リストに追加します。これにより、以降の検出についてファイルの実行または USB デバイスのアクセスが許可されるようになります。
無視	ファイルの実行は防ぎますが、ファイルの移動や変更は行いません。
隔離	ファイルの実行を防ぎ、後で分析するためにファイルを隔離します。
削除	ファイルの実行を防ぎ、ファイルを削除します。

## エージェントイベントログをクエリする

クエリを実行すると、表示されるエージェントイベントログのリストが更新されます。

### 手順

1. 管理サーバ画面の上部にあるナビゲーションで [ログ]→[エージェントイベント] の順に選択します。[エージェントイベント] 画面が表示されます。
2. 期間でフィルタするには、初期設定が [過去 30 日間] である [期間] のドロップダウンをクリックして、期間を選択します。次のいずれかを実行します。
  - リストされる期間をクリックします。
  - [カスタム] をクリックし、期間を指定して [検索] をクリックします。
3. [エージェント名]、[エージェントグループ]、[IP アドレス]、[IP アドレスの範囲]、[タグ]、[イベントのタイプ]、[重大度]、[変更監視]、[ロックされたファイル]、または [不正プログラム検出] でフィルタするには、検索バーの左側にあるドロップダウンをクリックして条件を指定します。
  - エージェント名: 探しているエージェントの名前を指定します。
  - エージェントグループ: 探しているグループの名前を指定します。
  - IP アドレス: 探しているエージェントのIP アドレスを指定します。
  - IP アドレスの範囲: エージェントを検索するIP アドレスの範囲を指定します。
  - タグ: エージェントに割り当てられたタグを指定します。
  - イベントのタイプ: 特定のイベントを選択し、[適用] をクリックします。
  - 重大度: イベントレベルとして [情報] または [警告] を選択します。
  - 変更監視: [ファイルまたはフォルダ] または [レジストリキーまたはレジストリ値] を選択し、[検索] をクリックします。[ファイルまたはフォルダ] 検索では、文字列の部分一致がサポートされます。
  - ロックされたファイル: [ファイル名] または [ファイルハッシュ (SHA-1)] を選択し、[検索] をクリックします。[ファイル名] 検索では、文字列の部分一致がサポートされます。
  - 不正プログラム検出: [すべての検出]、[失敗した処理]、[駆除されました]、[隔離されました]、[削除されました]、[無視されました]、または [ロールバックされました] を選択します。

- 選択したフィルタに一致するエントリのみが表に表示されます。

## エージェントイベントをエクスポートする

選択したエージェントのイベントログエントリに関するデータを **CSV** ファイル形式で保存します。



選択内容のエクスポート (4)	レベル	イベント	エージェント	処理
すべてエクスポート	● 警告	2509 ファイルのアクセスがブロックされました。ファイルが許可リストに存在しません	TXSP-WIN10-A01	
<input checked="" type="checkbox"/> 2022-12-21T04:38:38+...	● 警告	2509 ファイルのアクセスがブロックされました。ファイルが許可リストに存在しません	TXSP-WIN10-A01	
<input checked="" type="checkbox"/> 2022-12-21T04:38:38+...	● 警告	2509 ファイルのアクセスがブロックされました。ファイルが許可リストに存在しません	TXSP-WIN10-A01	
<input checked="" type="checkbox"/> 2022-12-21T04:26:52+...	● 警告	2509 ファイルのアクセスがブロックされました。ファイルが許可リストに存在しません	TXSP-WIN10-A01	

### 手順

- 管理サーバ画面の上部にあるナビゲーションで [ログ]→[エージェントイベント] の順に選択します。[エージェントイベント] 画面が表示されます。
- 情報をエクスポートするエージェントログエントリをリストから選択します。
  - すべてのエントリをエクスポートするには、右上にある [すべてエクスポート] をクリックします。
  - 選択したエントリのみをエクスポートするには、エクスポートするエントリを選択し、左上にある [選択内容のエクスポート] ボタンをクリックします。
- ファイルを保存します。

## [サーバイベント] 画面について

[サーバイベント] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで、[ログ]→[サーバイベント] の順に選択します。



The screenshot shows the 'Server Event' log interface. At the top, there are tabs for 'StellarProtect', 'StellarProtect (Legacy Mode)' (which is selected), and 'StellarOne'. Below the tabs is a search bar with fields for 'ユーザID' and '検索' (Search), and dropdowns for '最新の1,000レコード' (Latest 1,000 records) and '過去30日間' (Past 30 days). The main area displays a table of events with columns: '時間' (Time), 'ユーザID' (User ID), 'イベント' (Event), 'エージェント/[グループ]' (Agent/[Group]), and 'ステータス' (Status). The table contains five entries, all from '2022-12-21T11:07:27+0...' and 'admin', with event codes 5601 and status TXSP-WIN10-A01. The last two entries are marked as '許可リスト' (Allow List).

時間	ユーザID	イベント	エージェント/[グループ]	ステータス
2022-12-21T11:07:27+0...	admin	5601 ファイル (エージェントの設定) をTXSP-WIN10-A01からエクスポートし...	TXSP-WIN10-A01	
2022-12-21T11:07:17+0...	admin	5601 ファイル (エージェントの設定) をTXSP-WIN10-A01からエクスポートし...	TXSP-WIN10-A01	
2022-12-21T11:03:40+0...	admin	5601 ファイル (許可リスト) をTXSP-WIN10-A01からエクスポートしました。	TXSP-WIN10-A01	
2022-12-21T11:01:30+0...	admin	5601 ファイル (許可リスト) をTXSP-WIN10-A01からエクスポートしました。	TXSP-WIN10-A01	
2022-12-21T11:00:34+0...	admin	5601 ファイル (エージェントの設定) をTXSP-WIN10-A01からエクスポートし...	TXSP-WIN10-A01	

この画面には、StellarProtect、StellarProtect (Legacy Mode)、および StellarOne の監査対象 StellarOne ユーザアカウントのアクティビティのログが表示されます。



### 注意

サーバイベントログには、StellarOne のユーザアカウントとポリシーにより実行された処理について収集された情報が含まれます。

## サーバイベントログをクエリする

クエリを実行すると、表示されるサーバイベントログのリストが更新されます。

### 手順

1. 管理サーバ画面の上部にあるナビゲーションで、[ログ]→[サーバイベント] の順に選択します。  
[サーバイベント] 画面が表示されます。
2. [サーバイベント] のドロップダウンリストをクリックします。検索条件のリストが表示されます。
3. 目的の検索条件を選択します。選択した条件に応じた検索フィールドが表示されます。
4. 選択した条件に応じた手順を実行します。

オプション	説明
期間	次のいずれかを実行します。 <ul style="list-style-type: none"><li>リストから期間を選択します。</li><li>期間をカスタマイズして指定します。<ol style="list-style-type: none"><li>リストの [カスタム範囲] を選択します。</li><li>カスタマイズする期間を指定します。</li><li>[適用] をクリックします。</li></ol></li></ul>
ユーザID	特定のユーザによりログに記録されたすべてのイベントを表示します。
エージェント名	エージェントのホスト名 (最初の数文字またはすべて) を入力し、[検索] をクリックします。
グループ名	特定のグループによりログに記録されたすべてのイベントを表示します。
イベントのタイプ	特定のイベントを選択します。

サーバイベントログのリストに検索結果が表示されます。

## サーバイベントログをエクスポートする

選択したサーバのイベントログエントリに関するデータを CSV ファイル形式で保存します。

### 手順

1. 管理サーバ画面の上部にあるナビゲーションで、[ログ]→[サーバイベント] の順に選択します。  
[サーバイベント] 画面が表示されます。
2. 情報をエクスポートするサーバログエントリをリストから選択します。
  - すべてのエントリをエクスポートするには、[すべてエクスポート] アイコンをクリックします。
  - 選択したエントリのみをエクスポートするには、エクスポートするエントリを選択し、[選択内容のエクスポート] をクリックします。
3. ファイルを保存します。

## [システムログ] 画面について

[システムログ] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで、[ログ]→[システムログ] の順に選択します。この画面には、調整可能な StellarOne の管理サーバ画面の設定のログが表示されます。

## サーバログをクエリする

クエリを実行すると、表示されるサーバイベントログのリストが更新されます。

### 手順

1. 管理サーバ画面の上部にあるナビゲーションで、[ログ]→[システムログ] の順に選択します。  
[システムログ] 画面が表示されます。
2. 目的の検索条件を選択します。選択した条件に応じた検索フィールドが表示されます。
3. 選択した条件に応じた手順を実行します。

オプション	説明
期間	次のいずれかを実行します。 <ul style="list-style-type: none"> <li>リストから期間を選択します。</li> <li>期間をカスタマイズして指定します。</li> </ul> a. リストの [カスタム] を選択します。 <ul style="list-style-type: none"> <li>カスタマイズする期間を指定します。</li> <li>[検索] をクリックします。</li> </ul>
重大度	次のいずれかの条件を選択して、[検索] をクリックします。 <ul style="list-style-type: none"> <li>緊急</li> <li>アラート</li> <li>重大</li> <li>エラー</li> <li>警告</li> <li>注意</li> <li>情報</li> <li>デバッグ</li> </ul>

システムログのリストに検索結果が表示されます。

## システムログをエクスポートする

選択したサーバのイベントログエントリに関するデータを CSV ファイル形式で保存します。

### 手順

- 管理サーバ画面の上部にあるナビゲーションで、[ログ]→[システムログ] の順に選択します。[システムログ] 画面が表示されます。
- 情報をエクスポートするシステムログエントリをリストから選択します。
  - すべてのエントリをエクスポートするには、[すべてエクスポート] アイコンをクリックします。
  - 選択したエントリのみをエクスポートするには、エクスポートするエントリを選択し、[選択内容のエクスポート] をクリックします。

## [監査ログ] 画面について

[監査ログ] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで、[ログ]→[監査ログ] の順に選択します。この画面には、StellarOne の監査ログが表示されます。

## 監査ログをクエリする

クエリを実行すると、表示されるサーバイベントログのリストが更新されます。



日時	重大度	ユーザーID	クライアントIP	ライアントIP	メッセージ
2022-12-21T13:12:42+08:00	注意	admin	192.168.0.1		ユーザ (admin) がログインしました
2022-12-21T12:06:30+08:00	注意	admin	192.168.0.1		ユーザ (admin) がタイムアウトしました、ログアウトを強制します
2022-12-21T10:59:29+08:00	注意	admin	192.168.0.1		ユーザ (admin) がログインしました
2022-12-21T10:59:22+08:00	警告	admin	192.168.0.1		ユーザ (admin) がログインに失敗しました

### 手順

1. 管理サーバ画面の上部にあるナビゲーションで、[ログ]→[監査ログ] の順に選択します。[監査ログ] 画面が表示されます。
2. 目的の検索条件を選択します。選択した条件に応じた検索フィールドが表示されます。
3. 選択した条件に応じた手順を実行します。



オプション	説明
期間	<input style="width: 150px; height: 20px; border: 1px solid #ccc; margin-right: 10px;" type="text" value="ユーザーID"/> <input style="width: 30px; height: 20px; border: 1px solid #ccc; margin-right: 10px;" type="button" value="検索"/> <input style="width: 100px; height: 20px; border: 1px solid #ccc; margin-right: 10px;" type="button" value="最新の1,000レコード"/> <input style="width: 100px; height: 20px; border: 1px solid #ccc;" type="button" value="過去30日間"/> <div style="border: 1px solid #ccc; padding: 5px; display: inline-block; width: 150px; height: 150px; margin-top: 10px;">         1時間以内          3時間以内          12時間以内          24時間以内          過去3日間          過去7日間  <b>過去30日間</b>          過去90日間          カスタム範囲       </div>

オプション	説明																																																												
	<p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> <li>リストから期間を選択します。</li> <li>期間をカスタマイズして指定します。</li> </ul> <ol style="list-style-type: none"> <li>リストの [カスタム] を選択します。</li> <li>カスタマイズする期間を指定します。</li> <li>[検索] をクリックします。</li> </ol>																																																												
ユーザ ID	ユーザ ID を入力し、[検索] をクリックします。																																																												
クライアント IP	クライアント IP 番号を入力し、[検索] をクリックします。																																																												
重大度	<p>次のいずれかの条件を選択して、[検索] をクリックします。</p> <div style="border: 1px solid #ccc; padding: 5px; width: 300px;"> <p>監査ログ</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="4">監査ログ</th> <th>重大度</th> <th>検索</th> </tr> <tr> <th colspan="4"></th> <th>緊急</th> <th></th> </tr> </thead> <tbody> <tr> <td colspan="4"></td> <td>アラート</td> <td></td> </tr> <tr> <td colspan="4"></td> <td>重大</td> <td></td> </tr> <tr> <td colspan="4"></td> <td>エラー</td> <td></td> </tr> <tr> <td>□</td> <td>日時</td> <td>重大度</td> <td>ユーザ</td> <td>エラー</td> <td></td> </tr> <tr> <td>□</td> <td>2022-12-21T20:53:34+08:00</td> <td>注意</td> <td>admin</td> <td>警告</td> <td></td> </tr> <tr> <td>□</td> <td>2022-12-21T20:48:04+08:00</td> <td>注意</td> <td>admin</td> <td>注意</td> <td></td> </tr> <tr> <td>□</td> <td>2022-12-21T17:05:38+08:00</td> <td>注意</td> <td>admin</td> <td>情報</td> <td>192.168.0.1 ユーザ (admin) がログインしました</td> </tr> <tr> <td>□</td> <td>2022-12-21T17:05:33+08:00</td> <td>情報</td> <td>admin</td> <td></td> <td>192.168.0.1 ユーザ (admin) がログアウト</td> </tr> </tbody> </table> </div> <ul style="list-style-type: none"> <li>緊急</li> <li>アラート</li> <li>重大</li> <li>エラー</li> <li>警告</li> <li>注意</li> <li>情報</li> <li>デバッグ</li> </ul>	監査ログ				重大度	検索					緊急						アラート						重大						エラー		□	日時	重大度	ユーザ	エラー		□	2022-12-21T20:53:34+08:00	注意	admin	警告		□	2022-12-21T20:48:04+08:00	注意	admin	注意		□	2022-12-21T17:05:38+08:00	注意	admin	情報	192.168.0.1 ユーザ (admin) がログインしました	□	2022-12-21T17:05:33+08:00	情報	admin		192.168.0.1 ユーザ (admin) がログアウト
監査ログ				重大度	検索																																																								
				緊急																																																									
				アラート																																																									
				重大																																																									
				エラー																																																									
□	日時	重大度	ユーザ	エラー																																																									
□	2022-12-21T20:53:34+08:00	注意	admin	警告																																																									
□	2022-12-21T20:48:04+08:00	注意	admin	注意																																																									
□	2022-12-21T17:05:38+08:00	注意	admin	情報	192.168.0.1 ユーザ (admin) がログインしました																																																								
□	2022-12-21T17:05:33+08:00	情報	admin		192.168.0.1 ユーザ (admin) がログアウト																																																								

監査ログのリストに検索結果が表示されます。

## 監査ログをエクスポートする

選択したサーバのイベントログエントリに関するデータを CSV ファイル形式で保存します。



The screenshot shows the StellarOne management interface. At the top, there are navigation tabs: ダッシュボード, エージェント, ログ (selected), 管理, and バージョン情報. On the right, there is a user dropdown (admin (Admin)) and the txOne networks logo. Below the tabs, the page title is "監査ログ" (Audit Log). There are filters for "重大度" (Severity) and search fields for "最新の1,000レコード" (Latest 1,000 records) and "過去30日間" (Past 30 days). The main content area displays a table of audit log entries. The table has columns: "選択内容のエクスポート (3)" (Export Selection (3)), "重大度" (Severity), "ユーザID" (User ID), "クライアントIP" (Client IP), and "メッセージ" (Message). The "重大度" column shows 00 (注意 - Notice) for all entries. The "メッセージ" column shows messages like "ユーザー (admin) がログインしました" (User (admin) logged in) and "ユーザー (admin) がログアウトを強制しました" (User (admin) forced logout). The table shows three entries with checkboxes, where the first two are checked. The last two entries are not checked. The table has a header row and three data rows.

### 手順

1. 管理サーバ画面の上部にあるナビゲーションで、[ログ]→[監査ログ] の順に選択します。[監査ログ] 画面が表示されます。
2. 情報をエクスポートするシステムログエントリをリストから選択します。
  - すべてのエントリをエクスポートするには、[すべてエクスポート] をクリックします。
  - 選択したエントリのみをエクスポートするには、エクスポートするエントリを選択し、[選択内容のエクスポート] をクリックします。

## 第 7 章

# 管理設定

この章では、TXOne StellarOne の管理設定の概要について説明します。

## [アカウント管理] 画面について

[アカウント管理] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで [管理] → [アカウント管理] の順に選択します。

この画面は、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管理に使用します。 TXOne StellarOne の管理サーバ画面にアクセスするためのアカウントには、次の権限があります。

アカウントの種類	権限
管理者 (フルコントロール)	<ul style="list-style-type: none"> <li>a. StellarOne 管理: システム設定を行うための権限です。</li> <li>b. 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。</li> <li>c. 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。</li> <li>d. 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。</li> </ul>
オペレータ (資産コントロール)	<ul style="list-style-type: none"> <li>a. 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。</li> <li>b. 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。</li> </ul>
閲覧者 (読み取りのみ)	<ul style="list-style-type: none"> <li>a. [ダッシュボード]、[ポリシー設定]、[エージェントイベント] の読み取りのみです。</li> <li>b. エージェントインストーラパッケージをダウンロードできます。</li> <li>c. 自身のアカウントのパスワードを変更します。</li> </ul>

## サーバーアカウントの概要

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 (Legacy Mode) エージェントを監視または管理できます。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。

タスク	許可される権限		
	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	✓	✓	
メンテナンスマードの設定	✓	✓	
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	✓	✓	✓
サーバイベントログの監視	✓	✓	

タスク	許可される権限		
	管理者	オペレータ	閲覧者
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	✓	✓	
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	✓		
SSL 証明書	✓		
ライセンス管理	✓	✓	

## アカウントを追加する

### 手順

- 管理者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。(ここに入力する情報は、大文字と小文字が区別されることに注意してください)
- 管理サーバ画面の上部にあるナビゲーションで [管理]→[アカウント管理] の順に選択します。[アカウント管理] 画面が表示されます。
- [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。
- [認証ソース] を指定します ([ローカル] または [SAML ID プロバイダ])。
  - ローカルユーザを追加するには、[ID] と [名前] を指定します (ここに入力する情報は、大文字と小文字が区別されることに注意してください)。
  - 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 (ここに入力する情報は、大文字と小文字が区別されることに注意してください)。

ユーザアカウントの追加

認証ソース	SAML IDプロバイダ
シングルサインオンの設定	
ロール	閲覧者
SAMLアカウントのマッピング用 メール*	認証サーバのアカウントと同じ大文字/小文字を使用して入力してください。
名前*	
グループコントロール*	<input type="checkbox"/> すべて (2) ▾ <input type="checkbox"/> Taiwan (0) <input checked="" type="checkbox"/> Taipei (0) <input checked="" type="checkbox"/> Daan (0) <input type="checkbox"/> Muzha (0) <input type="checkbox"/> Xinyi (0)
説明	
<input type="button" value="確認"/> <input type="button" value="キャンセル"/>	

5. [ロール] にアカウントの権限として [管理者]、[オペレータ]、または [閲覧者] (初期設定) を指定します。

ユーザアカウントの追加

認証ソース	ローカル
ロール	閲覧者
ID*	管理者
名前*	オペレータ
ローカルパスワード*	閲覧者
	*****

アカウント管理

ユーザ	ロール
管理者	ユーザアカウント管理と資産の設定
オペレータ	資産の設定のみ
閲覧者	読み取りのみ

- a. ローカルユーザの場合、[ローカルパスワード] を指定し、再入力します。
6. [グループコントロール] に、対象アカウントがアクセスするグループコントロールを指定します。

グループコントロール*	<input type="checkbox"/> すべて (2) ▾ <input type="checkbox"/> Taiwan (0) <input checked="" type="checkbox"/> Taipei (0) <input checked="" type="checkbox"/> Daan (0) <input type="checkbox"/> Muzha (0) <input type="checkbox"/> Xinyi (0)
-------------	---

7. 必要に応じて、アカウントの [説明] を入力します。
8. [確認] ボタンをクリックすると、対象のユーザアカウントが作成されます。

## アカウントを編集する

### 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 (ここに入力する情報は、大文字と小文字が区別されることに注意してください)。
2. 管理サーバ画面の上部にあるナビゲーションで [管理]→[アカウント管理] の順に選択します。[アカウント管理] 画面が表示されます。
3. [処理] の**編集**アイコンをクリックすると、[ユーザアカウントの編集] 画面が表示されます。
  - ローカルユーザの場合、アカウントの [ロール]、[名前]、[ローカルパスワード]、[グループコントロール]、[説明] を指定できます。
  - **SAML IDプロバイダ**ユーザの場合、アカウントの [ロール]、[名前]、[グループコントロール]、[説明] を指定できます。
4. [確認] をクリックします。

ユーザアカウントの編集

認証ソース	SAML IDプロバイダ
シングルサインオンの設定	
ロール	オペレータ
SAMLアカウントのマッピング用メール*	eason_huang@trendmicro.com 認証サーバのアカウントと同じ大文字/小文字を使用して入力してください。
名前*	Operator-01
グループコントロール*	<input type="checkbox"/> すべて (2) <input type="checkbox"/> Taiwan (0) <input checked="" type="checkbox"/> Taipei (0) <input checked="" type="checkbox"/> Daan (0) <input type="checkbox"/> Muzha (0) <input type="checkbox"/> Xinyi (0)
説明	
<input type="button" value="確認"/> <input type="button" value="キャンセル"/>	

## アカウントを削除する

### 手順

- 管理者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。(ここに入力する情報は、大文字と小文字が区別されることに注意してください)
- 管理サーバ画面の上部にあるナビゲーションで [管理]→[アカウント管理] の順に選択します。[アカウント管理] 画面が表示されます。
- 削除するアカウントを選択します。(初期設定の **admin** だけは削除できません)



ダッシュボード エージェント ログ メニュー バージョン情報

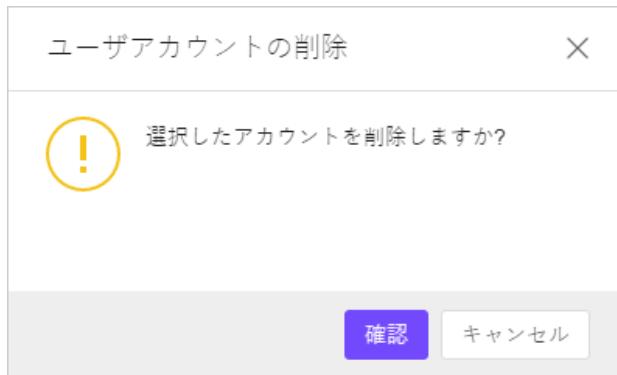
アカウント管理

ユーザ ロール

+ ユーザの追加 削除 フィルタ

ID	名前	ロール	認証ソース	グループコントロール	APIキーの有効期限	説明	処理
admin	Admin	マスター管理者	ローカル	すべて, Daan, Headqua...	-	初期設定のトレーニ...	<span style="border: 1px solid red; padding: 2px;">編集</span>
<input checked="" type="checkbox"/> eason_huang@tre...	Operator-01	オペレータ	SAML ID プロバイダ	Headquarter	-	-	<span style="border: 1px solid red; padding: 2px;">APIキーの生成</span> <span style="border: 1px solid red; padding: 2px;">ユーザの削除</span>

- 削除アイコンをクリックすると、[ユーザアカウントの削除] 画面が表示されます。



- [確認] ボタンをクリックすると、対象のユーザアカウントがリストから削除されます。

## API キーの生成

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。各ユーザー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。(ここに入力する情報は、大文字と小文字が区別されることに注意してください)
2. 管理サーバ画面の上部にあるナビゲーションで [管理]→[アカウント管理] の順に選択します。[アカウント管理] 画面が表示されます。
3. [ユーザ] タブで、変更するユーザ ID を見つけ、画面右側の [操作] の下にある三点リーダーメニューに移動します。
4. 三点リーダーをクリックし、[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。

# シングルサインオン

## 手順

- 管理者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。(ここに入力する情報は、大文字と小文字が区別されることに注意してください)
- 管理サーバ画面の上部にあるナビゲーションで [管理]→[シングルサインオン] の順に選択します。
- [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。
- StellarOne の 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。
- [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。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。

③ IdPのメタデータXMLファイルのアップロード  
 IdPのメタデータXMLファイルをアップロードして、SAML 2.0 のシングルサインオン設定を完了します。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。

IdPの表示名: SAMLtestIdP  
 プロトコル: SAML 2.0/SAML 1.1  
 IdPのシングルサインオンURL:  
 マッピング属性: メールアドレス

- 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。
- [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。

ダッシュボード エージェント ログ ▾ 管理 ▾ バージョン情報

シングルサインオン ✓ IdPの接続テストに成功しました。 ×

SAML設定

① StellarOneのメタデータXMLファイルのダウンロード  
 StellarOneのXMLファイルをIdPにアップロードする



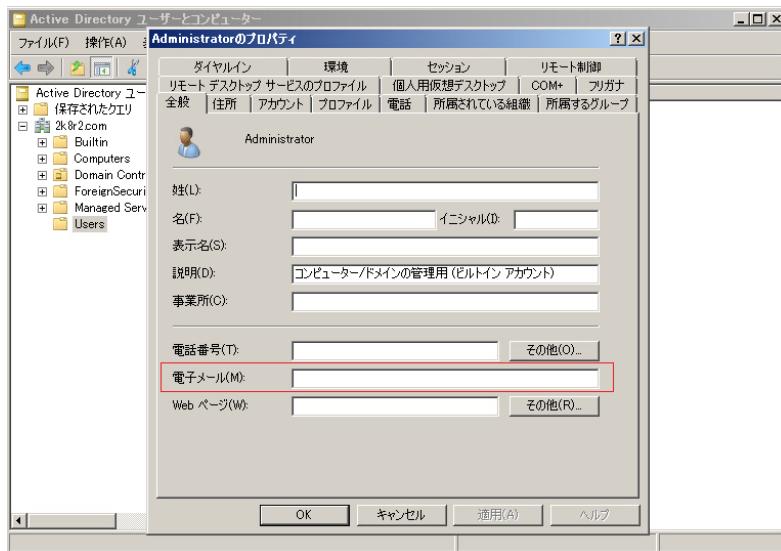
### 注意

SAML 設定の完了後、無効なログオンを示すエラーメッセージが表示されることがあります。シングルサインオンの問題の解決を参照して、IdP サーバでのメールアドレスの設定、および IdP サーバと StellarOne サーバのシステム時間の同期について確認してください。

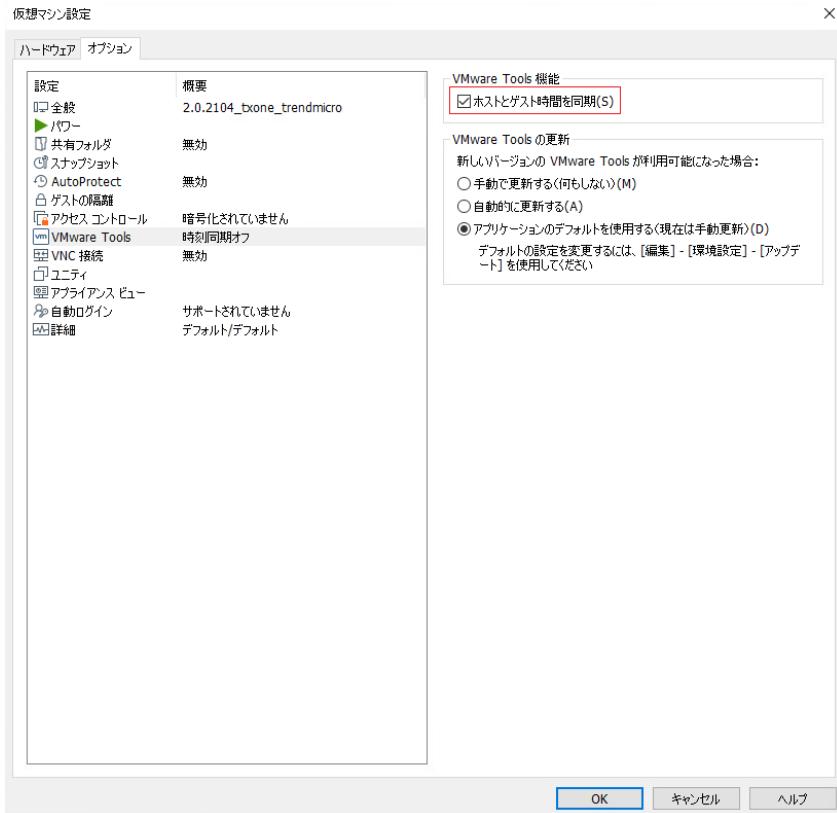
## シングルサインオンの問題の解決

### 手順

1. IdP サーバの [Active Directory ユーザーとコンピューター] 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ーアカウントを右クリックし、[プロパティ]→[全般] の順に移動します。
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。



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。
- 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。
  - 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。
  - [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。



## システム時間

システム時間設定を変更するには、[管理]→[システム時間] の順に選択します。

### 日付と時刻

[期間] ドロップダウンボタンを使用し、特定のシステム時間を選択します。

ダッシュボード エージェント ログ ▾ 管理 ▾ バージョン情報

#### システム時間

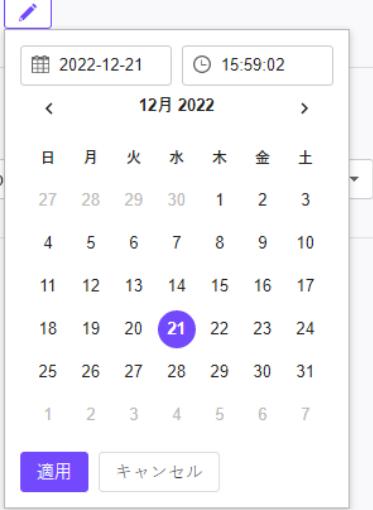
日付と時刻

現在時刻: 2022-12-21T15:59:05+08:00 

タイムゾーン

タイムゾーン: (GMT+08:00) Asia/Taipei



2022-12-21 15:59:02

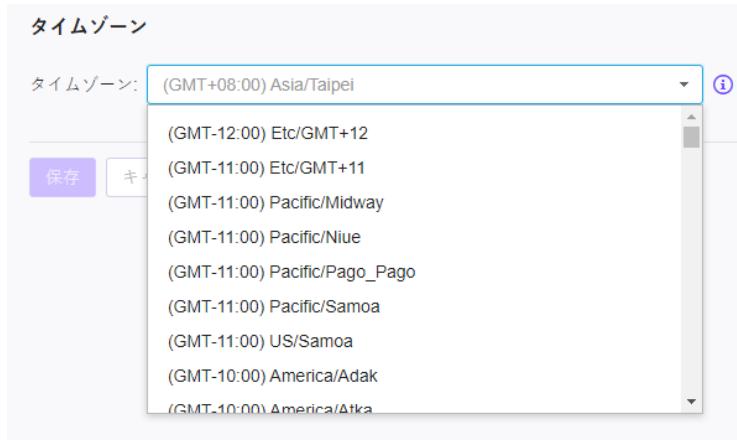
12月 2022

日	月	火	水	木	金	土
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

## タイムゾーン

ドロップダウンを使用し、特定のシステムタイムゾーンを選択します。



## Syslog 転送

サーバとエージェントのイベントログを外部 syslog サーバに転送することで、他のデバイスでの管理および監視が可能になります。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)] を有効にします。

3. Syslog サーバのプロトコル、サーバアドレス、およびポート番号を指定します。

ダッシュボード エージェント ログ ▾ 管理 ▾ バージョン情報

### Syslog転送

ログをSyslogサーバに転送する (CEFのみ)

サーバアドレス\*

ポート番号\*  ⓘ

プロトコル  TCP  UDP

保存 キャンセル

## Syslog 形式

CEF キー	説明	値
Header (logVer)	CEF 形式のバージョン	CEF: 0
Header (vendor)	デバイスのベンダ	例: TXOne Networks
Header (pname)	デバイスの製品	例: StellarOne、StellarProtect (Legacy Mode)
Header (pver)	デバイスのバージョン	例: 1.2.0171
Header (eventid)	デバイスのイベントクラス ID	例: 2509、6005
Header (eventName)	名前	例: エージェントイベント、サーバイベント、管理サーバ画面ログ
Header (severity)	重大度	例: 4
rt	ログに記録された日時	例: Apr 02 2022 13:31:51 GMT+00:00

CEF キー	説明	値
msg	イベント ID のマッピングされたメッセージ	例: ファイルのアクセスがブロックされました。ファイルが許可リストに存在しません
dvchost	コンピュータ名	例: ローカルホスト
dvc	IP アドレス	例: 192.168.154.137
cs1Label	詳細なイベントメッセージ	詳細なイベントメッセージ
cs1	イベント ID のマッピングされた詳細なメッセージ	例: ファイルのアクセスがブロックされました: C:\Documents and Settings\Administrator\Local Settings\Temp\is-D5V0T.tmp\is-H7K40.tmp 不正プログラムが検出されました: 隔離。ファイルパス: C:\eicar\EICAR_TEST_FILE.exe
cs2Label	クライアント OS	クライアント OS
cs2	OS の説明	例: Microsoft Windows 7 Enterprise Edition Service Pack 1 build 7601, 64-bit
cs3Label	クライアントの説明	クライアントの説明
cs3	説明	-
suser	ログインユーザ	例: PC1688\Administrator
act	処理の種類	例: ACTION_TYPE_BLOCKED
fileHash	SHA1	例: 2201589AA3ED709B3665E4FF979E10C6AD5137FC
filePath	ファイルパス	例: C:\Documents and Settings\Administrator\Local Settings\Temp\is-D5V0T.tmp\is-H7K40.tmp
fileCreateTime	ファイル作成日時	例: 04 02 2022 14:00:21

CEF キー	説明	値
fileModificationTime	ファイル変更日時	例: 04 02 2022 14:00:21
logGuid	ログの GUID	例: F43500BB-1F8A-4589-A292-144A9DA343AA, {56B7345A-B6D3-4BBB-A515-4AFFAE04092F}
ServerIP	サーバの IP アドレス	例: 10.8.145.157

#### 例:

メッセージ: CEF:0|TXOne Networks|StellarProtect (Legacy Mode)|1.2.0171|2509|エージェントイベント|4|rt=Apr 02 2022 14:09:29 GMT+00:00 msg=ファイルのアクセスがブロックされました。  
 ファイルが許可リストに存在しません dvchost=PC1688 dvc=192.168.154.137  
 logGuid={CEFD0E54-7693-4B3F-9DDA-3E6F40A9384E} cs1Label=詳細なイベントメッセージ cs1=ファイルのアクセスがブロックされました: C:\\eicar\\EICAR\_TEST\_FILE.gz.vbs cs2Label=クライアント OS cs2=Windows XP Professional Service Pack 3 build 2600, 32-bit cs3Label=クライアントの説明 cs3=suser=PC1688\\Administrator act=ACTION\_TYPE\_BLOCKED  
 fileHash=7dd27fab1f11084e984b631a614a5120c8e25598  
 filePath=C:\\eicar\\EICAR\_TEST\_FILE.gz.vbs fileCreateTime=09 13 2007 23:57:52  
 fileModificationTime=09 13 2007 23:57:52

## ログの削除設定

古いログを削除して、StellarOne で使用しているデータベースのサイズを削減します。

### 今すぐ削除

#### 手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理]→[ログの削除] の順に選択します。[ログの削除] 画面が表示されます。
2. 削除するログの種類を指定します。
  - すべてのログ

- ・ システムログ、監査ログ、エージェントイベント、またはサーバイベント
3. 経過期間にイベントログエントリを保持する最長期間を指定します。
    - ・ 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
  4. 最大保持数に保持するイベントエントリの最大件数を指定します。
    - ・ 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
  5. [今すぐ削除] ボタンをクリックすると、イベントログが削除されます。



## 自動削除

1 日に 1 回の自動削除を設定するには、次の設定を使用します。

### 手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理]→[ログの削除] の順に選択します。[ログの削除] 画面が表示されます。
2. 削除するログの種類を指定します。
  - ・ システムログ
  - ・ 監査ログ
  - ・ エージェントイベント
  - ・ サーバイベント

3. 経過期間にイベントログエントリを保持する最長期間を指定します。
  - 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
4. 最大保持数に保持するイベントエントリの最大件数を指定します。
  - 10,000件
  - 50,000件
  - 100,000件
  - 500,000件
  - 1,000,000件
  - 5,000,000件
  - 10,000,000件
5. [保存] ボタンをクリックします。

自動削除

次の期間を経過した エージェントイベント	を削除する	制限なし	最大	1,000,000件のエントリ...
次の期間を経過した サーバイベント	を削除する	制限なし	最大	1,000,000件のエントリ...
次の期間を経過した システムログ	を削除する	制限なし	最大	10,000,000件のエントリ...
次の期間を経過した 監査ログ	を削除する	制限なし	最大	10,000,000件のエントリ...

## 予約レポートの設定

[管理]→[予約レポート] にある [予約レポート] 画面には、ユーザ指定のスケジュールで自動的に生成されるすべてのレポートのリストが表示されます。この画面を使用して、これまでに設定した予約レポートや受信者に関する基本情報を表示したり、予約レポートを有効および無効にしたりすることができます。

次の表は、[予約レポート] 画面で実行できるタスクを示しています。

タスク	説明
予約レポートの送信	[予約レポートの送信] チェックボックスをオンにして、予約レポートを有効にします (初期設定は無効)。
レポート内容	<p>イベントのタイプ:</p> <ul style="list-style-type: none"> <li>StellarProtect (Legacy Mode) でブロックされたイベントの履歴</li> <li>イベントをブロックした StellarProtect (Legacy Mode) エージェントの上位 10 件</li> <li>StellarProtect (Legacy Mode) でブロックされたファイルの上位 10 件</li> </ul> <p>期間:</p> <ul style="list-style-type: none"> <li>過去 7 日間</li> <li>過去 14 日間</li> <li>過去 30 日間</li> <li>過去 3 か月</li> <li>過去 6 か月</li> </ul>
予約	<p>予約レポートの頻度と開始時刻を日、週、または月単位で設定します。</p> <div style="border: 1px solid #ccc; padding: 10px; margin-bottom: 10px;"> <p>予約</p> <p>更新間隔:</p> <p><input checked="" type="radio"/> 日次  <input type="radio"/> 週次、毎週 <input type="button" value="日曜日 ▾"/>  <input type="radio"/> 月次、日 <input type="button" value="01 ▾"/></p> <p>開始時刻: <input type="button" value="18 ▾"/> : <input type="button" value="30 ▾"/></p> </div> <hr/> <p> <b>注意</b></p> <p>指定した日付が存在しない月は予約タスクがスキップされます。タスクを定期的に実行するには、29 日、30 日、または 31 日を指定しないことをお勧めします。</p>
受信者	レポートの受信者を指定するには有効なメールアドレスが必要です。


**TXOne StellarOneレポート**

レポートが生成され、このメッセージに添付されています。

**StellarEnforce Top 10 Endpoints with Blocked Events**

Endpoint Name	Description	IP Address	Blocked Events
JP123あいうえお		172.16.122.30	129544
DESKTOP-KU5803S		172.16.122.64	6336
DESKTOP-FLOHVPU		172.16.122.30	1563
DESKTOP-KU5803S	cc	172.16.122.64	41

**StellarEnforce Block Event History**

Date	Network Virus	Application Lockdown	Device Control	USB Malware
2022-04-05~2022-04-11	0	11	0	0
2022-04-05~2022-04-11	0	13	1	0
2022-04-05~2022-04-11	0	23	17	0
2022-04-05~2022-04-11	0	129532	0	0
2022-04-05~2022-04-11	0	1554	0	0
2022-04-05~2022-04-11	0	6390	0	0
2022-04-05~2022-04-11	0	8	0	0

Date	DLL Injection	API Hooking	Write Protection	Fileless Attack
2022-04-05~2022-04-11	0	0	0	0
2022-04-05~2022-04-11	0	0	0	0
2022-04-05~2022-04-11	0	0	0	0
2022-04-05~2022-04-11	0	0	0	0
2022-04-05~2022-04-11	0	0	5	0
2022-04-05~2022-04-11	0	0	0	0
2022-04-05~2022-04-11	0	0	0	0

**StellarEnforce Top 10 Blocked Files**

File Name	File Hash	Endpoints	Blocked Events
InputSwitch.dll	acc4a727ba0cc45f47f225eed55493b75dcc7b4d	1	127612
mscorlib.ni.dll	d2b37b1c4ba74dcff26544d492b8faea97ae9755	1	4104
mscorlib.ni.dll	a1b824f78c227d69899eecc55e2af2fd17a123f65f	1	1918
policymanager.dll	19c7704e2d3757052e46d4ef9d803cd67132a39	1	538
TextShaping.dll	f802186a955c4bdbf4246f2e246f6f08c907d87e	1	210
windows.storage.dll	23fc00b1da661158d3b2c2fe4d6a70425b919	1	201
TextInputHost.exe	13819310f37471f14158451f0e092edddc79ac8e	1	159
uxtheme.dll	36e592e6e7b0dc8cef09217a565eeeea71dd7078	1	114
gpapi.dll	4f743bdf9116ea6e7da01a094bb94d28390f0e3	1	98
AppxDeploymentClient.dll	414799473d1629565aaea6b276877a830da9a492	1	76

## 通知設定

[メール通知] にメールを入力します。画面を保存する際、他の設定と一緒にメールも保存されます。

1. 最初に [管理]→[SMTP 設定] の順に選択して、SMTP サーバの設定を指定します。
2. 通知設定を変更するには、[管理]→[通知] の順に選択します。
3. [通知] には次のセクションがあります。
  - 警告レベルのエージェントイベント (初期設定は無効)
  - 大規模感染 (初期設定は無効)
  - メール通知

## 警告レベルのエージェントイベント

[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。

## 大規模感染

[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。



The screenshot shows an email from StellarOne titled "StellarOne: 大規模感染通知". The message content is as follows:

StellarOne

2022-04-28 00:12:17.122801023 +0000 UTC m=+328260.700159656に大規模感染を検出しました。1分間に1件を超える警告イベントが発生しました。  
詳細については、[https://\[REDACTED\]/signin?%7B%22redir%22%3A%22%2Flog%2Fagent\\_events%22%2C%22type%22%3A%22SIEf%22%7D](https://[REDACTED]/signin?%7B%22redir%22%3A%22%2Flog%2Fagent_events%22%2C%22type%22%3A%22SIEf%22%7D) にあるStellarOneの管理サーバー画面を確認してください。

大規模感染が発生したと見なす監視するイベント数 (1~20,000) と、その数を計測する期間 (1~60分) を設定できます。



The screenshot shows the "Large-scale infection" configuration settings:

大規模感染通知を送信する

監視する警告イベント数:  (1~20,000)

監視する期間:  (1~60分)

## SMTP 設定

この画面には、通知や予約レポートを送信するための SMTP サーバの設定を指定できます。

### 手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理]→[SMTP 設定] の順に選択します。  
[SMTP 設定] 画面が表示されます。
2. [サーバアドレス]、[ポート]、および [送信者] を指定します。
3. SMTP サーバで認証が必要な場合は、[SMTP サーバの認証を設定する] を選択します。
4. StellarOne からテストメールを送信するには、[テストメールの送信] ボタンをクリックします。
5. [保存] ボタンをクリックします。



### SMTP設定

サーバアドレス:*	<input type="text"/>
ポート:*	<input type="text"/>
送信者:*	<input type="text"/>
<input checked="" type="checkbox"/> SMTPサーバの認証を設定する	
ユーザ名*	<input type="text"/>
パスワード*	<input type="text"/>

## 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. 管理サーバ画面の上部にあるナビゲーションで [管理]→[プロキシ] の順に選択します。
2. 次のプロキシ設定を指定します。
  - 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。
  - (1) 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、StellarProtect (Legacy Mode) 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。

---

- (2) [サーバアドレス] で、プロキシサーバの IPv4 アドレスか FQDN を指定します。
- (3) [ポート] を指定します。
- (4) プロキシサーバで認証が必要な場合は、[プロキシサーバ認証] を選択して資格情報を指定します。
- (5) [保存] をクリックします。

## プロキシ

### StellarOneのインターネットプロキシ設定

StellarOneのインターネットプロキシ設定

HTTPS  HTTP

サーバアドレス\*

ポート番号\*

プロキシサーバの認証を設定する

ユーザ名\*

パスワード\*

### StellarOneからエージェントへの通信プロキシ設定

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

エージェントからStellarOneへの通信プロキシ設定



## ヒント

StellarProtect (Legacy Mode) 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。

### StellarOne からエージェントへの通信プロキシ設定:

エージェントインストーラパッケージで使用する設定ファイルにプロキシ情報を追加します。プロキシ設定を保存します。これにより、エージェント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。

### エージェントから StellarOne への通信プロキシ設定:

StellarProtect (Legacy Mode) の管理者ガイドを参照し、ローカルの StellarProtect (Legacy Mode) エージェントで **SLCmd.exe** コマンドラインインターフェースツールを使用します。

## ダウンロード/アップデート設定

StellarOne および StellarProtect (Legacy Mode) のダウンロード/アップデートを管理するには、管理サーバ画面の上部にあるナビゲーションで [管理]→[ダウンロード/アップデート] の順に選択します。

ここには [StellarOne] と [StellarProtect (Legacy Mode)] の 2 つのタブがあります。

次の表は、この画面の [StellarOne] タブで実行するタスクを示しています。

機能	説明
検索コンポーネント	[アップデート] をクリックすると、最新のコンポーネントをダウンロードできます。ここにはパターンファイルとエンジンのすべてのバージョンがリストされています。
検索コンポーネントのアップデートスケジュール	コンポーネントの予約アップデートの頻度と時刻を [日次]、[週次]、または [月次] のいずれかに設定し、その曜日または日付と [開始時刻] を指定します。
検索コンポーネントのアップデート元 (StellarOne)	アップデートサーバを指定するか、トレンドマイクロのアップデートサーバから直接アップデートをダウンロードします。
検索コンポーネントのアップデート元 (エージェント)	アップデートサーバを指定することも、StellarOne から直接ダウンロードすることもできます。

次の表は、この画面の [StellarProtect (Legacy Mode)] タブで実行するタスクを示しています。

機能	説明
StellarProtect (Legacy Mode) エージェントインストーラパッケージの準備	<ul style="list-style-type: none"> <li>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します。エージェントコンポーネントのアップデート元やプロキシ設定を変更したり、最新のコンポーネントにアップデートしたりすることもできます。</li> <li>Group.ini ファイルをダウンロードしてインストーラパッケージに追加します。これにより、StellarOne の管理サーバ画面を介して StellarProtect (Legacy Mode) エージェントを特定グループに直接登録できるようになります。詳細については、<a href="#">グループのマッピング</a>を参照してください。</li> </ul>
Patch	ここでは、[インポート] ボタンをクリックして Patch を手動でインポートするか、[削除] をクリックして StellarProtect (Legacy Mode) の Patch を削除できます。

## グループのマッピング

### 手順

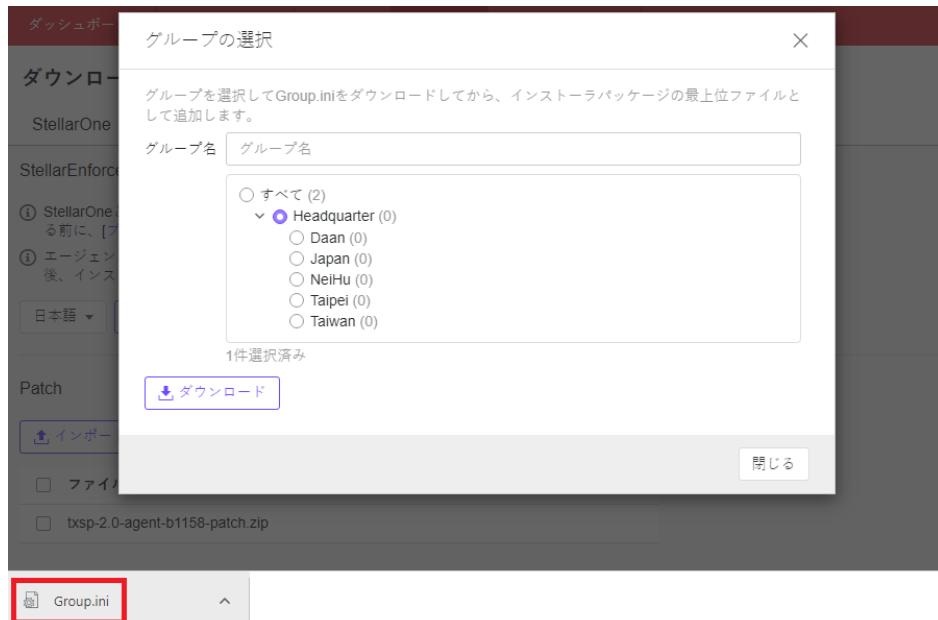
1. 管理サーバ画面の上部にあるナビゲーションで [管理]→[ダウンロード/アップデート] の順に選択します。
2. [StellarProtect (Legacy Mode)] タブを選択します。
3. インストーラパッケージをダウンロードした後、[Group.ini のダウンロード] をクリックします。



The screenshot shows the StellarOne management interface. The top navigation bar includes links for 'ダッシュボード', 'エージェント', 'ログ', '管理', and 'バージョン情報'. The '管理' tab is currently selected. Below this, a sub-navigation bar has tabs for 'StellarOne', 'StellarProtect', and 'StellarProtect (Legacy Mode)', with the latter being the active tab. The main content area is titled 'ダウンロード/アップデート' and contains a sub-section for 'StellarProtect (Legacy Mode) エージェントインストーラパッケージの準備'. It includes two numbered steps: ① 'StellarOne と StellarProtect (Legacy Mode) の間の通信にプロキシを使用する場合は、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] ページで設定を行ってください。' and ② 'エージェントを特定のグループに直接登録するには、グループIDと名前: [Group.ini のダウンロード] を実行した後、インストーラパッケージに追加してください。'. At the bottom of this section are language selection buttons for '日本語' and 'ダウンロード', with the 'ダウンロード' button highlighted by a red box.

4. StellarProtect (Legacy Mode) 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配置します。

5. 対象のエージェントでインストールを実行します。インストール時、エージェントが StellarOne の管理サーバ画面に接続されていることを確認してください。



6. StellarOne の管理サーバ画面と StellarProtect (Legacy Mode) のメイン画面で、エージェントが登録されたことを確認できます。

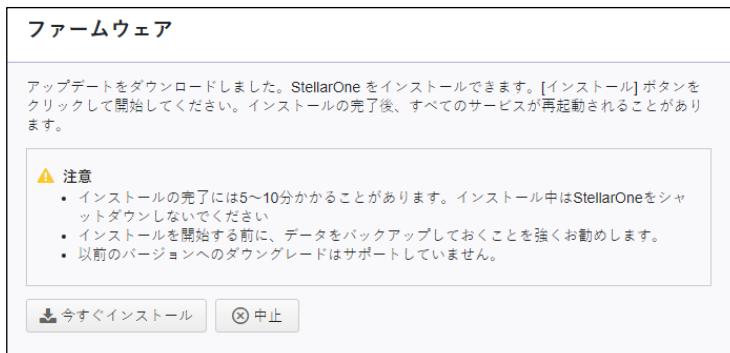
# ファームウェア

## 手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理]→[ファームウェア] の順に選択します。
2. [インポート] をクリックして、ファームウェアの Patch ファイルを指定します (例: `acus.fw_2.0.1137.acf`)。
  - [バージョン] に、StellarOneの現在のビルドバージョンが表示されます。
  - [公開日] と [説明] には、StellarOneのPatchファイルの現在の情報が表示されます。



3. [ファームウェアのアップデート] 画面が表示されたら、[適用] をクリックして、Patch を StellarOne に適用します。
4. 通知の説明を確認します。
5. [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。



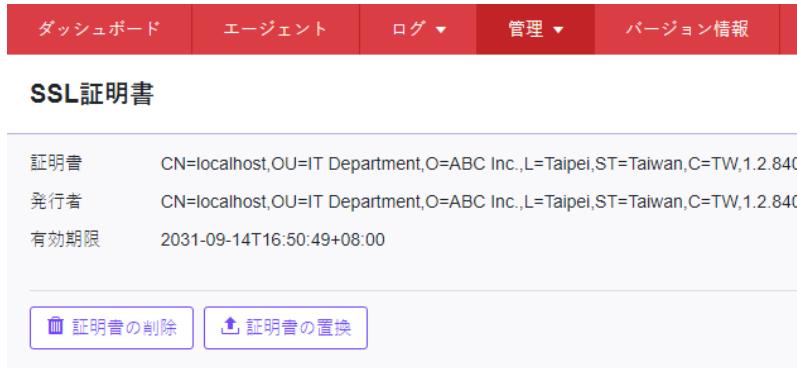
## SSL 証明書

### 手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理]→[SSL 証明書] の順に選択します。
2. 目的の [証明書のインポート] を選択します。
3. 証明書をインポートするには、仮想インスタンスを再起動する必要があります。
  - (1) [証明書] の横にある [ファイルの選択...] ドロップダウンを使用して、インポートする証明書を選択します。
  - (2) [秘密鍵] の横にある [ファイルの選択...] ドロップダウンを使用して、目的の秘密鍵を選択します。
  - (3) [パスフレーズ] を指定します (任意)。



4. [インポートして再起動] をクリックします (StellarOne の管理サーバ画面が再ロードされます)。



証明書 CN=localhost,OU=IT Department,O=ABC Inc.,L=Taipei,ST=Taiwan,C=TW,1.2.840  
 発行者 CN=localhost,OU=IT Department,O=ABC Inc.,L=Taipei,ST=Taiwan,C=TW,1.2.840  
 有効期限 2031-09-14T16:50:49+08:00

証明書の削除 証明書の置換

## ライセンス管理

[ライセンス管理] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで [管理]→[ライセンス] の順に選択します。この画面には、次の詳細事項が表示されます。

項目	説明
ライセンスエディション	StellarProtect (Legacy Mode) および StellarProtect の現在のライセンスエディションを表示します。
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: 永久使用可能で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。

項目	説明
ステータス	<p>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。</p> <hr/> <p> <b>注意</b></p> <p>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。</p>
有効期限	StellarOne と StellarProtect (Legacy Mode) エージェントの機能が利用できる期限の日付が表示されます。(製品サポートは StellarEnforce のサポート終了期限まで提供します。)
アクティベーションコード	アクティベーションコードが表示されます
最終更新日	アクティベーションコードの前回の更新日が表示されます
詳細	リンクをクリックすると、ライセンスの詳細についてオンラインヘルプが表示されます。

## アクティベーションコードを変更する

### ライセンス

アクティベーションコードの入力

**StellarICs**

StellarProtect ライセンスエディション:	オールインワンエディション
StellarProtect (Legacy Mode) ライセンスエディション:	AVエディション
ライセンス種別:	製品版
シート数:	2/10
ステータス:	有効
有効期限:	2022-12-31
アクティベーションコード:	
最終更新日:	2022-11-25T17:44:43+08:00

## 手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理]→[ライセンス] の順に選択します。[ライセンス管理] 画面が表示されます。
2. [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て、StellarOne の管理サーバ画面で更新を実行します。



### 注意

[ライセンスの更新] ボタンをクリックして、製品ライセンスを更新します。TXOne の製品ライセンスサーバへの接続が必要になります。

---

## 第 8 章

# ログの説明の参照情報

この章では、管理に関する追加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。

- StellarProtect (Legacy Mode) エージェントのイベントログの説明
- StellarProtect (Legacy Mode) エージェントのエラーコードの説明
- StellarOneサーバのイベントログの説明

## エージェントのイベントログの説明



The screenshot shows a web-based event log interface for the StellarProtect (Legacy Mode) agent. The top navigation bar includes links for 'ダッシュボード', 'エージェント', 'ログ', '管理', and 'バージョン情報'. The 'ログ' link is currently selected, indicated by a blue underline. Below the navigation is a search bar with a dropdown for 'エージェント名' and a search button. There are also filters for '最新の1,000レコード' and '過去30日間'. The main content area displays a table of event logs. The table has columns for '時間' (Time), 'レベル' (Level), 'イベント' (Event), 'エージェント' (Agent), and '処理' (Action). The table shows three entries:

時間	レベル	イベント	エージェント	処理
2022-12-21T17:04:09+0...	警告	1102 ストレージデバイスのブロックが無効になりました	TXSP-WIN10-A01	
2022-12-21T17:04:09+0...	警告	1114 Intelligent Runtime Learning (インテリジェントランタイム学習) の無効化	TXSP-WIN10-A01	
2022-12-21T17:02:20+0...	警告	1001 サービスが停止されました	TXSP-WIN10-A01	

イベント ID	タスクカテゴリ	レベル	ログの説明
1000	システム	情報	サービスが開始されました。
1001	システム	警告	サービスが停止されました。
1002	システム	情報	アプリケーション制御が有効になりました。
1003	システム	警告	アプリケーション制御が無効になりました。
1004	システム	情報	無効化されました。
1005	システム	情報	管理者パスワードが変更されました。
1006	システム	情報	制限付きユーザのパスワードが変更されました。
1007	システム	情報	制限付きユーザのアカウントが有効になりました。
1008	システム	情報	制限付きユーザのアカウントが無効になりました。
1009	システム	情報	製品が有効になりました。
1010	システム	情報	製品が無効になりました。
1011	システム	警告	ライセンスの有効期限が終了しています。猶予期間が有効になりました。
1012	システム	警告	ライセンスの有効期限が終了しています。猶予期間が終了しました。
1013	システム	情報	製品の設定のインポートを開始しました: %path%
1014	システム	情報	製品の設定のインポートが完了しました: %path%
1015	システム	情報	製品の設定のエクスポート先: %path%
1016	システム	情報	USB 不正プログラム対策が [許可] に設定されました。
1017	システム	情報	USB 不正プログラム対策が [ブロック] に設定されました。
1018	システム	情報	USB 不正プログラム対策が有効になりました。
1019	システム	警告	USB 不正プログラム対策が無効になりました。
1020	システム	情報	ネットワークウイルス対策が [許可] に設定されました。

イベント ID	タスクカテゴリ	レベル	ログの説明
1021	システム	情報	ネットワークウイルス対策が[ブロック]に設定されました。
1022	システム	情報	ネットワークウイルス対策が有効になりました。
1023	システム	警告	ネットワークウイルス対策が無効になりました。
1025	システム	情報	メモリのランダム化が有効になりました。
1026	システム	警告	メモリのランダム化が無効になりました。
1027	システム	情報	API フッキング対策が[許可]に設定されました。
1028	システム	情報	API フッキング対策が[ブロック]に設定されました。
1029	システム	情報	API フッキング対策が有効になりました。
1030	システム	警告	API フッキング対策が無効になりました。
1031	システム	情報	DLL インジェクション対策が[許可]に設定されました。
1032	システム	情報	DLL インジェクション対策が[ブロック]に設定されました。
1033	システム	情報	DLL インジェクション対策が有効になりました。
1034	システム	警告	DLL インジェクション対策が無効になりました。
1035	システム	情報	事前指定による許可リスト自動更新が有効になりました。
1036	システム	情報	事前指定による許可リスト自動更新が無効になりました。
1037	システム	情報	DLL/ドライバ制御が有効になりました。
1038	システム	警告	DLL/ドライバ制御が無効になりました。
1039	システム	情報	スクリプト制御が有効になりました。
1040	システム	警告	スクリプト制御が無効になりました。
1041	システム	情報	スクリプトが追加されました。 [詳細] ファイル拡張子: %extension% インタープリタ: %interpreter%

イベント ID	タスクカテゴリ	レベル	ログの説明
1042	システム	情報	スクリプトが削除されました。 <a href="#">[詳細]</a> ファイル拡張子: %extension% インタープリタ: %interpreter%
1044	システム	情報	除外パスが有効になりました。
1045	システム	情報	除外パスが無効になりました。
1047	システム	情報	信頼するデジタル証明書が有効になりました。
1048	システム	情報	信頼するデジタル証明書が無効になりました。
1049	システム	情報	書き込み制御が有効になりました。
1050	システム	警告	書き込み制御が無効になりました。
1051	システム	情報	書き込み制御が [許可] に設定されました。
1052	システム	情報	書き込み制御が [ブロック] に設定されました。
1055	システム	情報	書き込み制御リストに追加されたファイル。 パス: %path%
1056	システム	情報	書き込み制御リストから削除されたファイル。 パス: %path%
1057	システム	情報	書き込み制御の除外リストに追加されたファイル。 パス: %path% プロセス: %process%
1058	システム	情報	書き込み制御の除外リストから削除されたファイル。 パス: %path% プロセス: %process%
1059	システム	情報	書き込み制御リストに追加されたフォルダ。 パス: %path% 範囲: %scope%
1060	システム	情報	書き込み制御リストから削除されたフォルダ。 パス: %path% 範囲: %scope%

イベント ID	タスクカテゴリ	レベル	ログの説明
1061	システム	情報	書き込み制御の除外リストに追加されたフォルダ。 パス: %path% 範囲: %scope% プロセス: %process%
1062	システム	情報	書き込み制御の除外リストから削除されたフォルダ。 パス: %path% 範囲: %scope% プロセス: %process%
1063	システム	情報	書き込み制御リストに追加されたレジストリ値。 レジストリキー: %regkey% レジストリ値の名前: %regvalue%
1064	システム	情報	書き込み制御リストから削除されたレジストリ値。 レジストリキー: %regkey% レジストリ値の名前: %regvalue%
1065	システム	情報	書き込み制御の除外リストに追加されたレジストリ値。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% プロセス: %process%
1066	システム	情報	書き込み制御の除外リストから削除されたレジストリ値。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% プロセス: %process%
1067	システム	情報	書き込み制御リストに追加されたレジストリキー。 パス: %regkey% 範囲: %scope%
1068	システム	情報	書き込み制御リストから削除されたレジストリキー。 パス: %regkey% 範囲: %scope%
1069	システム	情報	書き込み制御の除外リストに追加されたレジストリキー。 パス: %regkey% 範囲: %scope% プロセス: %process%

イベント ID	タスクカテゴリ	レベル	ログの説明
1070	システム	情報	書き込み制御の除外リストから削除されたレジストリキー。 パス: %regkey% 範囲: %scope% プロセス: %process%
1071	システム	情報	カスタム処理が [無視] に設定されました。
1072	システム	情報	カスタム処理が [隔離] に設定されました。
1073	システム	情報	カスタム処理が [Intelligent Manager で確認する] に設定されました
1074	システム	情報	隔離ファイルが復元されました。 [詳細] 元の場所: %path% ソース: %source%
1075	システム	情報	隔離ファイルは削除されました。 [詳細] 元の場所: %path% ソース: %source%
1076	システム	情報	変更監視が有効になりました。
1077	システム	情報	変更監視が無効になりました。
1078	システム	情報	Root Cause Analysis レポートに失敗しました。 [詳細] パス: %path%
1079	システム	情報	管理サーバの証明書のインポート先: %path%
1080	システム	情報	管理サーバの証明書のエクスポート先: %path%
1081	システム	情報	集中管理モードの設定のインポート先: %path%
1082	システム	情報	集中管理モードの設定のエクスポート先: %path%
1083	システム	情報	集中管理モードが有効になりました。
1084	システム	情報	集中管理モードが無効になりました。
1085	システム	情報	書き込み制御が有効の場合、書き込み制御リストと許可リストが対象に含まれます。

イベント ID	タスクカテゴリ	レベル	ログの説明
1086	システム	警告	書き込み制御が有効の場合、書き込み制御リストのみが対象になります。
1088	システム	情報	Windows Update サポートが有効になりました。
1089	システム	情報	Windows Update サポートが無効になりました。
1094	システム	情報	TXOne StellarProtect (Legacy Mode) がアップデートされました。 適用されたファイル: %file_name%
1096	システム	情報	信頼するハッシュリストが有効になりました。
1097	システム	情報	信頼するハッシュリストが無効になりました。
1099	システム	情報	ストレージデバイスのアクセスが [許可] に設定されました
1100	システム	情報	ストレージデバイスのアクセスが [ブロック] に設定されました
1101	システム	情報	ストレージデバイスのブロックが有効になりました
1102	システム	警告	ストレージデバイスのブロックが無効になりました
1103	システム	情報	イベントログの設定が変更されました。 [詳細] Windows イベントログ: %ON off% レベル: 警告ログ: %ON off% 情報ログ: %ON off% システムログ: %ON off% 除外パスログ: %ON off% 書き込み制御ログ: %ON off% リストログ: %ON off% 許可されたアクセスのログ: DLL ドライバログ: %ON off% アップデートプログラムのログ: %ON off% 除外パスログ: %ON off% 信頼するデジタル証明書のログ: %ON off% 信頼するハッシュのログ: %ON off% 書き込み制御ログ: %ON off% ブロックされたアクセスのログ: %ON off% USB 不正プログラム対策ログ: %ON off% 実行防止対策のログ: %ON off% ネットワークウイルス対策のログ: %ON off%

イベント ID	タスクカテゴリ	レベル	ログの説明
			変更監視ログ ファイル作成ログ: %ON off% ファイル変更ログ: %ON off% ファイル削除ログ: %ON off% ファイル名変更ログ: %ON off% RegValue 変更ログ: %ON off% RegValue 削除ログ: %ON off% RegKey 作成ログ: %ON off% RegKey 削除ログ: %ON off% RegKey 名前変更ログ: %ON off% デバイスコントロールのログ: %ON off% デバッグログ: %ON off%
1104	システム	警告	このバージョンの Windows ではメモリのランダム化は使用できません。
1105	システム	情報	ファイルのブロック通知が有効になりました。
1106	システム	情報	ファイルのブロック通知が無効になりました。
1107	システム	情報	管理者パスワードがリモートで変更されました。
1111	システム	情報	ファイルレス攻撃対策が有効になりました。
1112	システム	警告	ファイルレス攻撃対策が無効になりました。
1500	リスト	情報	許可リスト自動更新が開始されました。
1501	リスト	情報	許可リスト自動更新が停止されました。
1502	リスト	情報	許可リストのインポートを開始しました: %path%
1503	リスト	情報	許可リストのインポートが完了しました: %path%
1504	リスト	情報	許可リストのエクスポート先: %path%
1505	リスト	情報	許可リストに追加されました: %path%
1506	リスト	情報	許可済みインストーラまたはアップデートプログラムのリストに追加されました: %path%
1507	リスト	情報	許可リストから削除されました: %path%
1508	リスト	情報	許可済みインストーラまたはアップデートプログラムのリストから削除されました: %path%
1509	リスト	情報	許可リストがアップデートされました: %path%

イベント ID	タスクカテゴリ	レベル	ログの説明
1510	リスト	情報	許可済みインストーラまたはアップデートプログラムのリストがアップデートされました: %path%
1511	リスト	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%
1512	リスト	警告	許可済みインストーラまたはアップデートプログラムの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%
1513	システム	情報	除外パスリストに追加されました。 [詳細] 種類: %exceptionpath% パス: %exceptionpath%
1514	システム	情報	除外パスリストから削除されました。 [詳細] 種類: %exceptionpath% パス: %exceptionpath%
1515	システム	情報	信頼するデジタル証明書リストに追加されました。 [詳細] ラベル: %label% ハッシュ: %hashvalue% 種類: %type% 件名: %subject% 発行者: %issuer%
1516	システム	情報	信頼するデジタル証明書リストから削除されました。 [詳細] ラベル: %label% ハッシュ: %hashvalue% 種類: %type% 件名: %subject% 発行者: %issuer%

イベント ID	タスクカテゴリ	レベル	ログの説明
1517	システム	情報	信頼するハッシュリストに追加されました。%n [詳細] ラベル: %label% ハッシュ: %hashvalue% 種類: %type% 許可リストに追加: %yes no% パス: %path% メモ: %note%
1518	システム	情報	信頼するハッシュリストから削除されました。%n [詳細] ラベル: %label% ハッシュ: %hashvalue% 種類: %type% 許可リストに追加: %yes no% パス: %path% メモ: %note%
1519	リスト	情報	許可リストからリモートで削除されました: %path%
1520	リスト	警告	%1 でファイルの列挙中に予期しないエラーが発生したため、許可リストを作成できません。%n エラーコード: %2 %n
1521	システム	情報	ファイルレス攻撃対策の除外を追加しました。 [詳細] ラベル: %label% 対象プロセス: %process_name% 引数: %arguments% %regex_flag% 親プロセス 1 のパス: %path% 親プロセス 2 のパス: %path% 親プロセス 3 のパス: %path% 親プロセス 4 のパス: %path%
1522	システム	情報	ファイルレス攻撃対策の除外を削除しました。 [詳細] ラベル: %label% 対象プロセス: %process_name% 引数: %arguments% %regex_flag% 親プロセス 1 のパス: %path% 親プロセス 2 のパス: %path% 親プロセス 3 のパス: %path% 親プロセス 4 のパス: %path%

イベント ID	タスクカテゴリ	レベル	ログの説明
1523	システム	情報	メンテナンスマードを開始しました
1524	システム	情報	メンテナンスマードを終了しています
1525	システム	情報	メンテナンスマードを終了しました
1526	リスト	情報	メンテナンスマードで許可リストに追加されました。 パス: %1 ハッシュ: %2
1527	リスト	情報	メンテナンスマードで許可リストがアップデートされました。 パス: %1 ハッシュ: %2
2000	許可されたアクセス	情報	ファイルのアクセスが許可されました: %path% [詳細] パス: %path% アクセスユーザー: %username% モード: %mode% リスト: %list%
2001	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% [詳細] パス: %path% アクセスユーザー: %username% モード: %mode% ファイルハッシュが許可されました: %hash%
2002	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% 許可リストの確認中にファイルパスを取得できません。 [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%
2003	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% 許可リストの確認中にハッシュを計算できません。 [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%

イベント ID	タスクカテゴリ	レベル	ログの説明
2004	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% プロセスを監視するための通知を取得できません。
2005	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% プロセスを例外リスト以外に追加できません。
2006	許可されたアクセス	情報	ファイルのアクセスが許可されました: %path% [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%
2007	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% 除外パスリストの確認中にエラーが発生しました。 [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%
2008	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% 信頼するデジタル証明書リストの確認中にエラーが発生しました。 [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%
2011	許可されたアクセス	情報	レジストリのアクセスが許可されました。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%
2012	許可されたアクセス	情報	レジストリのアクセスが許可されました。 レジストリキー: %regkey% [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%

イベント ID	タスクカテゴリ	レベル	ログの説明
2013	許可されたアクセス	情報	除外リストによってファイル/フォルダの変更が許可されました: %path% [詳細] パス: アクセスユーザー: %username% モード: %mode%
2015	許可されたアクセス	情報	除外リストによってレジストリ値の変更が許可されました。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%
2016	許可されたアクセス	情報	除外リストによってレジストリキーの変更が許可されました。 レジストリキー: %regkey% [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%
2017	許可されたアクセス	警告	ファイル/フォルダの変更が許可されました: %path% [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%
2019	許可されたアクセス	警告	レジストリ値の変更が許可されました。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%

イベント ID	タスクカテゴリ	レベル	ログの説明
2020	許可されたアクセス	警告	レジストリキーの変更が許可されました。 レジストリキー: %regkey% [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%
2021	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% 信頼するハッシュリストの確認中にエラーが発生しました。 [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%
2022	許可されたアクセス	警告	ファイルレス攻撃対策によりプロセスが許可されました: %path% %argument% [詳細] アクセスユーザー: %username% 親プロセス 1 のパス: %path% 親プロセス 2 のパス: %path% 親プロセス 3 のパス: %path% 親プロセス 4 のパス: %path% モード: アプリケーション制御が無効の状態 理由: %reason%
2503	ブロックされたアクセス	警告	ファイル/フォルダの変更がブロックされました: %path% [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%
2505	ブロックされたアクセス	警告	レジストリ値の変更がブロックされました。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%

イベント ID	タスクカテゴリ	レベル	ログの説明
2506	ブロックされたアクセス	警告	レジストリキーの変更がブロックされました。 レジストリキー: %regkey% [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%
2507	ブロックされたアクセス	情報	指定した処理が実行されました: %path% [詳細] 操作: %action% ソース: %source%
2508	ブロックされたアクセス	警告	指定された処理の実行に失敗しました: %path% [詳細] 操作: %action% ソース: %source%
2509	ブロックされたアクセス	警告	ファイルのアクセスがブロックされました: %path% [詳細] パス: %path% アクセスユーザー: %username% モード: %mode% 理由: 許可リスト内に存在しません。 ファイルハッシュがブロックされました: %hash%
2510	ブロックされたアクセス	警告	ファイルのアクセスがブロックされました: %path% [詳細] パス: %path% アクセスユーザー: %username% モード: %mode% 理由: 計算されたハッシュ値が、保存されている値と一致しません。 ファイルハッシュがブロックされました: %hash%
2511	ブロックされたアクセス	情報	ファイル/フォルダの変更がブロックされました: %path% [詳細] パス: %path% アクセスユーザー: %username% モード: %mode%

イベント ID	タスクカテゴリ	レベル	ログの説明
2512	ブロックされたアクセス	警告	<p>レジストリ値の変更がブロックされました。</p> <p>レジストリキー: %regkey%</p> <p>レジストリ値の名前: %regvalue%</p> <p>[詳細]</p> <p>パス: %path%</p> <p>アクセスユーザー: %username%</p> <p>注意</p> <p>イベント ID 2512 は、サービス作成対策機能を有効にすることに起因します。</p>
2513	ブロックされたアクセス	警告	<p>ファイルレス攻撃対策によりプロセスがブロックされました: %path% %argument%</p> <p>[詳細]</p> <p>アクセスユーザー: %username%</p> <p>親プロセス 1 のパス: %path%</p> <p>親プロセス 2 のパス: %path%</p> <p>親プロセス 3 のパス: %path%</p> <p>親プロセス 4 のパス: %path%</p> <p>モード: アプリケーション制御が有効の状態</p> <p>理由: %reason%</p>
2514	ブロックされたアクセス	警告	<p>ファイルのアクセスがブロックされました: %BLOCKED_FILE_PATH%</p> <p>[詳細]</p> <p>パス: %PARENT_PROCESS_PATH%</p> <p>アクセスユーザー: %USER_NAME%</p> <p>理由: ブロックされたファイルは、大文字と小文字を区別する属性が有効になっているフォルダ内にあります。</p>
3000	USB 不正プログラム対策	警告	<p>デバイスのアクセスが許可されました: %path%</p> <p>[詳細]</p> <p>パス: %path%</p> <p>アクセスユーザー: %username%</p> <p>デバイスタイプ: %type%</p>
3001	USB 不正プログラム対策	警告	<p>デバイスのアクセスがブロックされました: %path%</p> <p>[詳細]</p> <p>パス: %path%</p> <p>アクセスユーザー: %username%</p> <p>デバイスタイプ: %type%</p>

イベント ID	タスクカテゴリ	レベル	ログの説明
3500	ネットワーク ウイルス対策	警告	ネットワークウイルスが許可されました: %name% [詳細] プロトコル: TCP 送信元 IP アドレス: %ip_address% 送信元ポート: %port% 送信先 IP アドレス: %ip_address% 送信先ポート: 80
3501	ネットワーク ウイルス対策	警告	ネットワークウイルスがブロックされました: %name% [詳細] プロトコル: TCP 送信元 IP アドレス: %ip_address% 送信元ポート: %port% 送信先 IP アドレス: %ip_address% 送信先ポート: 80
4000	プロセス保護 イベント	警告	API フッキング/DLL インジェクションが許可されました: %path% [詳細] パス: %path% ユーザ: %username%
4001	プロセス保護 イベント	警告	API フッキング/DLL インジェクションがブロックされました: %path% [詳細] パス: %path% ユーザ: %username%
4002	プロセス保護 イベント	警告	API フッキング対策が許可されました: %path% [詳細] パス: %path% ユーザ: %username%
4003	プロセス保護 イベント	警告	API フッキング対策がブロックされました: %path% [詳細] パス: %path% ユーザ: %username%
4004	プロセス保護 イベント	警告	DLL インジェクションが許可されました: %path% [詳細] パス: %path% ユーザ: %username%

イベント ID	タスクカテゴリ	レベル	ログの説明
4005	プロセス保護 イベント	警告	DLL インジェクションがブロックされました: %path% [詳細] パス: %path% ユーザ: %username%
4500	システム内の 変更	情報	作成されたファイル/フォルダ: %path% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4501	システム内の 変更	情報	変更されたファイル: %path% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4502	システム内の 変更	情報	削除されたファイル/フォルダ: %path% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4503	システム内の 変更	情報	名前が変更されたファイル/フォルダ: %path% 新しいパス: %path% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4504	システム内の 変更	情報	変更されたレジストリ値: レジストリキー: %regkey% レジストリ値の名前: %regvalue% レジストリ値の種類: %regvaluetype% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%

イベント ID	タスクカテゴリ	レベル	ログの説明
4505	システム内の変更	情報	削除されたレジストリ値: レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザー: %username%
4506	システム内の変更	情報	作成されたレジストリキー: レジストリキー: %regkey% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザー: %username%
4507	システム内の変更	情報	削除されたレジストリキー: レジストリキー: %regkey% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザー: %username%
4508	システム内の変更	情報	名前が変更されたレジストリキー: レジストリキー: %regkey% 新しいレジストリキー: %regkey% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザー: %username%
5000	デバイスコントロール	警告	ストレージデバイスのアクセスが許可されました: %PATH% [詳細] パス: %PATH% アクセスユーザー: %USERNAME% デバイスタイプ: %TYPE% %DEVICEINFO%
5001	デバイスコントロール	警告	ストレージデバイスのアクセスがブロックされました: %PATH% [詳細] パス: %PATH% アクセスユーザー: %USERNAME% デバイスタイプ: %TYPE% %DEVICEINFO%

イベント ID	タスクカテゴリ	レベル	ログの説明
6000	システム	情報	<p>%Result%</p> <p>[詳細]</p> <p>アップデート元: %SERVER%</p> <p>[元のバージョン]</p> <p>ウイルスパターンファイル: %VERSION%</p> <p>スパイウェアパターンファイル: %VERSION%</p> <p>デジタル署名パターンファイル: %VERSION%</p> <p>プログラム検査パターンファイル: %VERSION%</p> <p>ダメージクリーンナップテンプレート: %VERSION%</p> <p>ダメージクリーンナップエンジン設定: %VERSION%</p> <p>ウイルス検索エンジン: %VERSION%</p> <p>ダメージクリーンナップエンジン: %VERSION%</p> <p>検索サービス: %VERSION%</p> <p>[最新バージョン]</p> <p>ウイルスパターンファイル: %VERSION%</p> <p>スパイウェアパターンファイル: %VERSION%</p> <p>デジタル署名パターンファイル: %VERSION%</p> <p>プログラム検査パターンファイル: %VERSION%</p> <p>ダメージクリーンナップ</p> <p>テンプレート: %VERSION%</p> <p>ダメージクリーンナップエンジン設定: %VERSION%</p> <p>ウイルス検索エンジン: %VERSION%</p> <p>ダメージクリーンナップエンジン: %VERSION%</p> <p>検索サービス: %VERSION%</p>
6001	システム	警告	<p>アップデートに失敗しました: %ERROR_MSG%</p> <p>(%ERROR_CODE%)</p> <p>[詳細]</p> <p>アップデート元: %SERVER%</p> <p>[元のバージョン]</p> <p>ウイルスパターンファイル: %VERSION%</p> <p>スパイウェアパターンファイル: %VERSION%</p> <p>デジタル署名パターンファイル: %VERSION%</p> <p>プログラム検査パターンファイル: %VERSION%</p> <p>ダメージクリーンナップテンプレート: %VERSION%</p> <p>ダメージクリーンナップエンジン設定: %VERSION%</p> <p>ウイルス検索エンジン: %VERSION%</p> <p>ダメージクリーンナップエンジン: %VERSION%</p> <p>検索サービス: %VERSION%</p> <p>[最新バージョン]</p> <p>ウイルスパターンファイル: %VERSION%</p>

イベント ID	タスクカテゴリ	レベル	ログの説明
			スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップテンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION%
6002	システム	情報	不正プログラム検索を開始しました: %SCAN_TYPE% [詳細] 検索するファイル: %SCAN_FOLDER_TYPE% 検索されたフォルダ: %PATHS% 除外されたパス: %PATHS% 除外されたファイル: %PATHS% 除外された拡張子: %PATHS% [コンポーネント] ウイルスパターンファイル: %VERSION% スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップテンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION%
6003	システム	情報	不正プログラム検索が完了しました: %SCAN_TYPE% 感染ファイル数: %NUM% [詳細] 検索するファイル: %SCAN_FOLDER_TYPE% 検索されたフォルダ: %PATHS% 除外されたパス: %PATHS% 除外されたファイル: %PATHS% 除外された拡張子: %PATHS% 開始日時: %DATE_TIME% 終了日時: %DATE_TIME% 検索ファイル数: %NUM% 感染ファイル数: %NUM% 駆除されたファイル数: %NUM% 再起動後に駆除されたファイル数: %NUM%

イベント ID	タスクカテゴリ	レベル	ログの説明
			<p>[コンポーネント]    ウイルスパターンファイル: %VERSION%    スパイウェアパターンファイル: %VERSION%    デジタル署名パターンファイル: %VERSION%    プログラム検査パターンファイル: %VERSION%    ダメージクリーンナップテンプレート: %VERSION%    ダメージクリーンナップエンジン設定: %VERSION%    ウイルス検索エンジン: %VERSION%    ダメージクリーンナップエンジン: %VERSION%    検索サービス: %VERSION%</p>
6004	システム	警告	<p>不正プログラム検索は完了していません: %SCAN_TYPE%    %ERROR%    [詳細]    検索するファイル: %SCAN_FOLDER_TYPE%    検索されたフォルダ: %PATHS%    除外されたパス: %PATHS%    除外されたファイル: %PATHS%    除外された拡張子: %PATHS%    開始日時: %DATE_TIME%    終了日時: %DATE_TIME%    検索ファイル数: %NUM%    感染ファイル数: %NUM%    駆除されたファイル数: %NUM%    再起動後に駆除されたファイル数: %NUM%    [コンポーネント]    ウイルスパターンファイル: %VERSION%    スパイウェアパターンファイル: %VERSION%    デジタル署名パターンファイル: %VERSION%    プログラム検査パターンファイル: %VERSION%    ダメージクリーンナップテンプレート: %VERSION%    ダメージクリーンナップエンジン設定: %VERSION%    ウイルス検索エンジン: %VERSION%    ダメージクリーンナップエンジン: %VERSION%    検索サービス: %VERSION%</p>

イベント ID	タスクカテゴリ	レベル	ログの説明
6005	システム	情報	<p>不正プログラムが検出されました: %ACTION%</p> <p>ファイルパス: %PATH%</p> <p>[詳細]</p> <p>再起動が必要: %NEED_REBOOT%</p> <p>[検索結果]</p> <p>脅威の種類: %TYPE%</p> <p>脅威の名前: %NAME%</p> <p>[コンポーネント]</p> <p>ウイルスパターンファイル: %VERSION%</p> <p>スパイウェアパターンファイル: %VERSION%</p> <p>デジタル署名パターンファイル: %VERSION%</p> <p>プログラム検査パターンファイル: %VERSION%</p> <p>ダメージクリーンナップテンプレート: %VERSION%</p> <p>ダメージクリーンナップエンジン設定: %VERSION%</p> <p>ウイルス検索エンジン: %VERSION%</p> <p>ダメージクリーンナップエンジン: %VERSION%</p> <p>検索サービス: %VERSION%</p>
6006	システム	警告	<p>不正プログラムが検出されました。検出時の処理を実行できません: %PATH%</p> <p>[詳細]</p> <p>1 次処理: %1ST_ACTION%</p> <p>2 次処理: %2ND_ACTION%</p> <p>脅威の種類: %TYPE%</p> <p>脅威の名前: %NAME%</p> <p>[コンポーネント]</p> <p>ウイルスパターンファイル: %VERSION%</p> <p>スパイウェアパターンファイル: %VERSION%</p> <p>デジタル署名パターンファイル: %VERSION%</p> <p>プログラム検査パターンファイル: %VERSION%</p> <p>ダメージクリーンナップテンプレート: %VERSION%</p> <p>ダメージクリーンナップエンジン設定: %VERSION%</p> <p>ウイルス検索エンジン: %VERSION%</p> <p>ダメージクリーンナップエンジン: %VERSION%</p> <p>検索サービス: %VERSION%</p>

イベント ID	タスクカテゴリ	レベル	ログの説明
6007	メンテナンスマード	警告	<p>メンテナンスマードで不正プログラムが検出されました(ファイルの隔離に成功): %PATH%</p> <p>[詳細]</p> <p>コンポーネントのバージョン: ウイルスパターンファイル: %VERSION% スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップテンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION%</p>
6008	メンテナンスマード	警告	<p>メンテナンスマードで不正プログラムが検出されました(ファイルの隔離に失敗): %PATH%</p> <p>[詳細]</p> <p>コンポーネントのバージョン: ウイルスパターンファイル: %VERSION% スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップテンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION%</p>
6009	メンテナンスマード	警告	<p>メンテナンスマードで不正プログラムが検出されました: %PATH%</p> <p>[詳細]</p> <p>コンポーネントのバージョン: ウイルスパターンファイル: %VERSION% スパイウェアパターンファイル: %VERSION% デジタル署名パターンファイル: %VERSION% プログラム検査パターンファイル: %VERSION% ダメージクリーンナップテンプレート: %VERSION% ダメージクリーンナップエンジン設定: %VERSION% ウイルス検索エンジン: %VERSION% ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION%</p>

イベント ID	タスクカテゴリ	レベル	ログの説明
7000	システム	情報	<p>グループポリシーが適用されました</p> <p>[詳細]</p> <p>古いグループ名: %GROUP NAME%</p> <p>古いポリシーバージョン: %VERSION%</p> <p>新しいグループ名: %GROUP NAME%</p> <p>新しいポリシーバージョン: %VERSION%</p>
7001	システム	警告	<p>グループポリシーを同期できません</p> <p>[詳細]</p> <p>古いグループ名: %GROUP NAME%</p> <p>古いポリシーバージョン: %VERSION%</p> <p>新しいグループ名: %GROUP NAME%</p> <p>新しいポリシーバージョン: %VERSION%</p> <p>理由: %Reason%</p>

## エージェントのエラーコードの説明

このリストでは、TXOne StellarProtect (Legacy Mode) エージェントで使用されるさまざまなエラーコードについて説明します。

### エラーコードの説明 (StellarProtect (Legacy Mode))

コード	説明
0x00040200	操作に成功しました。
0x80040201	操作に失敗しました。
0x80040202	操作に失敗しました。
0x00040202	一部のみ操作に成功しました。
0x00040203	要求された機能はインストールされていません。
0x80040203	要求された機能はサポートされていません。
0x80040204	無効な引数です。
0x80040205	無効なステータスです。
0x80040206	メモリが不足しています。
0x80040207	ビジー状態です。要求は無視されました。
0x00040208	やりなおしてください。(通常はタスクの実行時間が長すぎる場合に出力されます)
0x80040208	システムにより予約済み。(未使用)
0x80040209	ファイルパスが長すぎます。
0x0004020a	システムにより予約済み。(未使用)
0x8004020b	システムにより予約済み。(未使用)
0x0004020c	システムにより予約済み。(未使用)
0x0004020d	システムにより予約済み。(未使用)
0x8004020d	システムにより予約済み。(未使用)
0x0004020e	再起動が必要です。

コード	説明
0x8004020e	予期しないエラーのため再起動が必要です。
0x0004020f	タスクの実行が許可されました。
0x8004020f	許可が拒否されました。
0x00040210	システムにより予約済み。(未使用)
0x80040210	無効または予期しないサービスモードです。
0x00040211	システムにより予約済み。(未使用)
0x80040211	要求されたタスクは現在のステータスでは許可されていません。ライセンスを確認してください。
0x00040212	システムにより予約済み。(未使用)
0x00040213	システムにより予約済み。(未使用)
0x80040213	パスワードが一致しません。
0x00040214	システムにより予約済み。(未使用)
0x80040214	システムにより予約済み。(未使用)
0x00040215	見つかりません。
0x80040215	「必要ですが見つかりません。」
0x80040216	認証がロックされています。
0x80040217	パスワードの長さが無効です。
0x80040218	パスワードに無効な文字が含まれています。
0x00040219	パスワードが重複しています。管理者と制限付きユーザのパスワードは同一にできません。
0x80040220	システムにより予約済み。(未使用)
0x80040221	システムにより予約済み。(未使用)
0x80040222	システムにより予約済み。(未使用)
0x80040223	ファイルが見つかりません(予想どおりでエラーではありません)。
0x80040224	システムにより予約済み。(未使用)
0x80040225	システムにより予約済み。(未使用)

コード	説明
0x80040240	ライブラリが見つかりません。
0x80040241	ライブラリ関数で無効なライブラリステータスまたは予期しないエラーが発生しました。
0x80040260	システムにより予約済み。(未使用)
0x80040261	システムにより予約済み。(未使用)
0x80040262	システムにより予約済み。(未使用)
0x80040263	システムにより予約済み。(未使用)
0x80040264	システムにより予約済み。(未使用)
0x00040265	システムにより予約済み。(未使用)
0x80040265	システムにより予約済み。(未使用)
0x80040270	システムにより予約済み。(未使用)
0x80040271	システムにより予約済み。(未使用)
0x80040272	システムにより予約済み。(未使用)
0x80040273	システムにより予約済み。(未使用)
0x80040274	システムにより予約済み。(未使用)
0x80040275	システムにより予約済み。(未使用)
0x80040280	アクティベーションコードが無効です。
0x80040281	アクティベーションコードの形式が正しくありません。

## サーバのイベントログの説明

[サーバイベント] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで、[ログ]→[サーバイベント] の順に選択します。



時間	ユーザID	イベント	エージェント [グループ]	ステータス
2022-12-21T11:07:27+0...	admin	5601 ファイル (エージェントの設定) をTXSP-WIN10-A01からエクスポートしま...	TXSP-WIN10-A01	
2022-12-21T11:07:17+0...	admin	5601 ファイル (エージェントの設定) をTXSP-WIN10-A01からエクスポートしま...	TXSP-WIN10-A01	
2022-12-21T11:03:40+0...	admin	5601 ファイル (許可リスト) をTXSP-WIN10-A01からエクスポートしました。	TXSP-WIN10-A01	
2022-12-21T11:01:30+0...	admin	5601 ファイル (許可リスト) をTXSP-WIN10-A01からエクスポートしました。	TXSP-WIN10-A01	

### サーバのイベントログの説明 (StellarProtect (Legacy Mode))

イベント ID	サーバイベント	説明
1001	コンソールにログオン	管理サーバ画面にログオンしました。
1002	コンソールからログオフ	管理サーバ画面からログオフしました。
1003	セッションタイムアウト	管理サーバ画面のセッションがタイムアウトしました。アカウント「%user_name%」は自動的にログオフしました。
1011	レポートを送信できません	予約レポートを%email_address%に送信できません。
1012	通知を送信できません	通知を%email_address%に送信できません。
2001	アカウントの作成	Intelligent Manager アカウント「%user_name%」を作成しました。
2002	アカウントの削除	Intelligent Manager アカウント「%user_name%」を削除しました。
2003	アカウントの変更	Intelligent Manager アカウント「%user_name%」%field_name%を変更しました。

イベント ID	サーバイベント	説明
3001	エージェントイベントログの削除 -自動	エージェントイベントログの自動削除。
3002	エージェントイベントログの削除 -手動	エージェントイベントログの手動削除。
3003	エージェントイベントログのバックアップ	エージェントイベントログの自動バックアップ。 パス: %filepath%
3004	サーバイベントログの削除 -自動	サーバイベントログの自動削除。
3005	サーバイベントログの削除 -手動	サーバイベントログの手動削除。
3006	サーバイベントログのバックアップ	サーバイベントログの自動バックアップ。 パス: %filepath%
4001	許可されていない ブロックされた ファイルの処理	エージェントに要求を送信しました(ブロックされたファイルを許可リストに追加する)。 ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1) エージェントに要求を送信しました(ブロックされたファイルを削除する)。 ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1) エージェントに要求を送信しました(ブロックされたファイルを無視する)。 ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1) エージェントに要求を送信しました(ファイルを隔離する)。 ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1) エージェントに要求を送信しました(隔離されたファイルを復元する)。 ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1)

イベント ID	サーバイベント	説明
4004	隔離された 不正ファイルの解除	エージェントに要求を送信しました(隔離された ファイルを復元する)。 ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1)
4005	隔離された 不正ファイルの削除	エージェントに要求を送信しました(隔離された ファイルを削除する)。 ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1)
4006	許可されていない ファイルレス攻撃の処理	エージェントに要求を送信しました(ブロックさ れたプロセスチェーンとコマンド引数の組み合 わせを追加する)。 プロセスチェーン: %process_name% コマンド引数: %parameter% エージェントに要求を送信しました(ブロックさ れたプロセスチェーンとコマンド引数の組み合 わせを無視する)。 プロセスチェーン: %process_name% コマンド引数: %parameter%
5001	アプリケーション制御を 有効化	エージェントのアプリケーション制御を有効化 しました。
5002	アプリケーション制御を 無効化	エージェントのアプリケーション制御を無効化 しました。
5011	信頼するファイルの ハッシュを追加しました	エージェントに信頼するファイルのハッシュを 1個追加しました。エージェントに信頼する ファイルのハッシュを%num%個追加しました。
5013	許可されたファイルの 削除	指定された項目をエージェントの許可リストか ら SLtasks.exe を使用して削除しました。
5021	ストレージデバイスの アクセスをブロック	エージェントでストレージデバイスのアクセス をブロックしました。
5023	ストレージデバイスの アクセスを許可	エージェントでストレージデバイスのアクセス を許可しました。
5025	信頼する USB デバイスの 追加	選択したエージェントに信頼する USB デバイス を追加しました
5601	エージェントの設定の エクスポート	ファイル (%file_desc%) を%endpoint_name%か らエクスポートしました。

イベント ID	サーバイベント	説明
5602	エージェントの設定のインポート	ファイル (%file_desc%) をエージェントにインポートしました。
5800	エージェントの管理者パスワードの変更	エージェントのパスワードを変更しました。
5700	不正プログラムの検索	エージェントで不正プログラム検索を実行しました。
5701	エージェントコンポーネントのアップデート	エージェントコンポーネントをアップデートしました。
5900	エージェントの許可リストの更新	エージェントの許可リストを更新しました。
6001	エージェントにPatchを配信	エージェントに Patch を配信します。 Patch 名: %patch_name%
6101	エージェントの移動	エージェントが新しい Intelligent Manager サーバに移動されました
6201	メンテナンスマードを有効にしました	エージェントのメンテナンスマードを有効にしました。
6202	メンテナンスマードを無効にしました	エージェントのメンテナンスマードを無効にしました。
6301	グループポリシーの配信	グループポリシーを配信します。 バージョン: %version%
6302	ODC サーバに接続できません	ODC サーバに接続できません。
6401	Intelligent Runtime Learning (インテリジェントランタイム学習) の設定	Intelligent Runtime Learning (インテリジェントランタイム学習) を設定します。 バージョン: %policy_version%
6402	エージェントのパスワードの設定	エージェントのパスワードを設定します。 バージョン: %policy_version%
6403	予約検索の設定	予約検索を設定します。 バージョン: %policy_version%
6404	ユーザ指定不審オブジェクトの設定	ユーザ指定不審オブジェクトを設定します。 バージョン: %policy_version%

イベント ID	サーバイベント	説明
6405	エージェントの Patch の設定	エージェントの Patch を設定します。 バージョン: %policy_version%

## サーバのイベントログの説明 (StellarOne)

サーバイベント				
StellarProtect	StellarProtect (Legacy Mode)	StellarOne		
<input type="checkbox"/> 時間	ユーザID	イベント	エージェント[グループ]	ステータス
2022-12-20T14:57:41+0...	System	45325 スキャンコンポーネント [protect] を更新できませんでした。エラー <TmuError_...	-	失敗
2022-12-20T14:56:51+0...	System	45325 スキャンコンポーネント [enforce] を更新できませんでした。エラー <TmuError_...	-	失敗
2022-12-20T14:56:01+0...	System	45314 スキャンコンポーネント [protect] の更新が開始されました	-	成功
2022-12-20T14:56:01+0...	System	45314 スキャンコンポーネント [enforce] の更新が開始されました	-	成功

イベント ID	説明
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] のアップデートジョブが開始されました
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

## 第9章

# テクニカルサポート

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。

この章では、トラブルシューティング、TXOne およびトレンドマイクロへの問い合わせ、不審コンテンツの送信、およびその他のリソース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、お客様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。

## メールレビューションについて

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](https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html)

## ファイルレビューションについて

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](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](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](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: APEM29595\_JP2303