1.3 TXOne StellarEnforce
管理者ガイド

※注意事項

複数年契約について

- お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。
- 複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。
- 各製品のサポート提供期間は以下の Web サイトからご確認いただけます。
  https://success.trendmicro.com/jp/solution/000207383

法人向け製品のサポートについて

- 法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。
- 法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

P/N: APEM139622_JP2303

プライバシーと個人データの収集に関する規定

トレンドマイクロ製品の一部の機能は、お客さまの製品の利用状況や検出にかかわる情報を収集してトレンドマイクロおよび TXOne Networks 社に送信します。この情報は一定の管轄区域内および特定の法令等において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客さまが関連機能を無効にする必要があります。

TXOne StellarEnforce 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 StellarEnforce における無効化の影響をご確認の上、無効化はお客さまの責任で行っていただくようお願いいたします。

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシー (Global Privacy Notice) に従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

目次

はじめに

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

この章の内容は次のとおりです。

ドキュメントについて

本製品には、次のドキュメントが付属しています。

表 1.　TXOne StellarEnforce のドキュメント

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

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

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

対象読者

TXOne StellarEnforce のドキュメントは、StellarEnforce の管理やエージェントをインストールする担当者を対象としています。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 2.　ドキュメントの表記規則

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

第 1 章

本製品の概要

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

この章の内容は次のとおりです。

TXOne StellarEnforce について

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

新機能

TXOne StellarEnforce 1.3 には、次の新機能および機能強化が含まれています。

表 1-1. TXOne StellarEnforce 1.3 の新機能

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

エージェントの機能と特徴

StellarEnforce には、次の機能と特徴があります。

脆弱性攻撃対策の設定

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

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

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

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

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

許可リストの管理

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

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

スモールフットプリント

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

権限設定

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

インタフェース

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

セルフプロテクション

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

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

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

システム要件

システム要件については、次の Web サイトを参照してください。

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

エージェントがサポートする OS

システム要件については、次の Web サイトを参照してください。

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

エージェントバージョンアップの準備

このバージョンの StellarEnforce では、次のバージョンからのバージョンアップがサポートされます。

- StellarEnforce 1.0

- StellarEnforce 1.1
- StellarEnforce 1.2

注意

バージョンアップする前に、WKSupportTool 画面と StellarEnforce エージェントのメイン画面を閉じてください。

警告!

バージョンアップする前に、選択したインストール方法およびインストールされている StellarEnforce エージェントのバージョンに応じて、次に示す適切な処理を実行してください。

アップデートの最新版は、StellarEnforce ソフトウェアのダウンロードセンター (https://downloadcenter.trendmicro.com/index.php?_clk=left_nav&clkval=all_download&regs=jp) からダウンロードできます。

表 1-2. StellarEnforce エージェントの新規インストール

インストール方法	インストールされているエージェントのバージョン	必要な処理	維持される設定
Windows インストーラを使用したローカルインストール	StellarEnforce 1.0/1.1/1.2	使用する前にインストールファイル (SL_Install.exe) を信頼するハッシュリストに手動で追加する必要があります。	なし
コマンドラインインタフェースインストーラを使用したローカルインストール	StellarEnforce 1.0/1.1/1.2	使用する前にインストールファイル (SL_Install.exe) を信頼するハッシュリストに手動で追加する必要があります。	なし

表 1-3.　インストール後のエージェントバージョンアップ (レガシーOS - SHA1 をサポート)

インストール方法	インストールされているエージェントのバージョン	必要な処理	維持される設定
`stellar_enforce_patch.exe` の実行によるパッチの適用 サイレントインストールを実行するには、管理者としてコマンドプロンプトを開いて次のコマンドを入力します。 `> stellar_enforce_patch.exe-s-a-s/g`	StellarEnforce 1.0/1.1/1.2	準備不要	互換性のある設定
リモートインストール	StellarEnforce 1.1/1.2 注意: StellarEnforce 1.0 ではローカルインストールのみサポートされます。	準備不要	互換性のある設定

表 1-4.　インストール後のエージェントバージョンアップ (最新 OS - SHA2 をサポート)

インストール方法	インストールされているエージェントのバージョン	必要な処理	維持される設定
`stellar_enforce_patch.exe` の実行によるパッチの適用 サイレントインストールを実行するには、管理者としてコマンドプロンプトを開いて次のコマンドを入力します。 `> stellar_enforce_patch.exe-s-a-s/g`	注意: 1.2 Patch 1より前のバージョンのエージェントでは、スタンドアロンのStellarEnforceエージェントのローカルバージョンアップはサポートされません。次のいずれかの方法を使用してください。 - StellarOneの管理サーバ画面からStellarEnforceエージェントをリモートでバージョンアップする - Patchファイルのハッシュを信頼するハッシュとして追加してから、ローカルバージョンアップを実行する	準備不要	互換性のある設定
リモートインストール	StellarEnforce 1.0/1.1/1.2	準備不要	互換性のある設定

エージェント利用時の概要

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

一般的な使用例は次のとおりです。

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

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

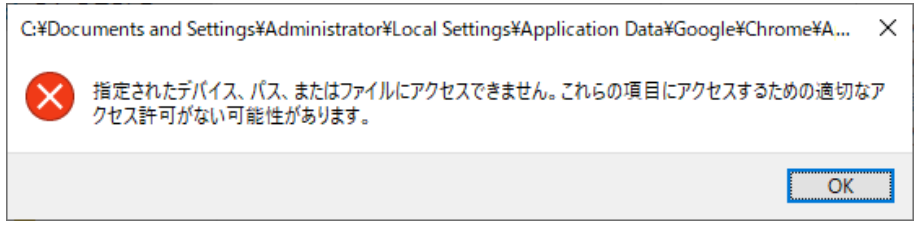


図 1-1. TXOne StellarEnforce ブロックメッセージ

第 2 章

エージェントのメイン画面の使用

この章では、エージェントのメイン画面を使用して TXOne StellarEnforce を設定する方法について説明します。

この章の内容は次のとおりです。

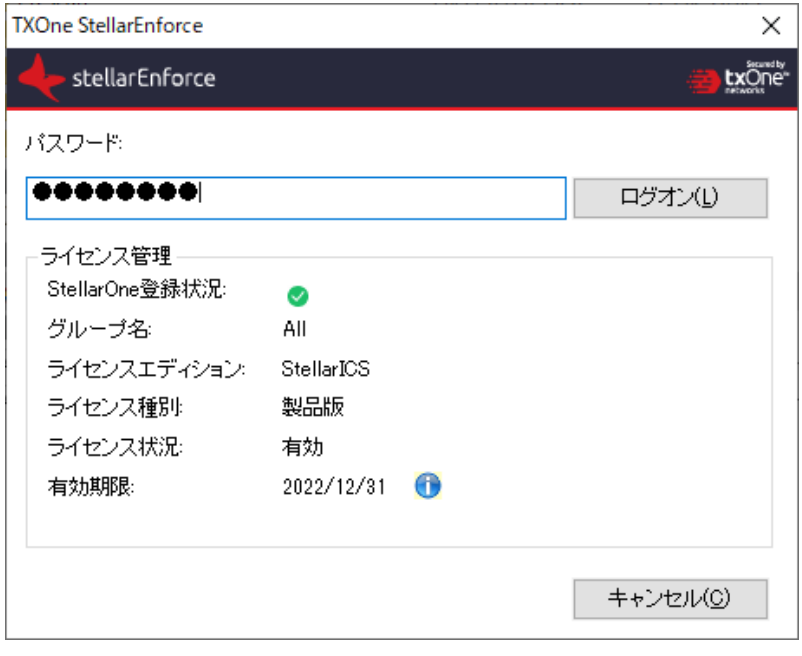
許可リストの設定

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

手順

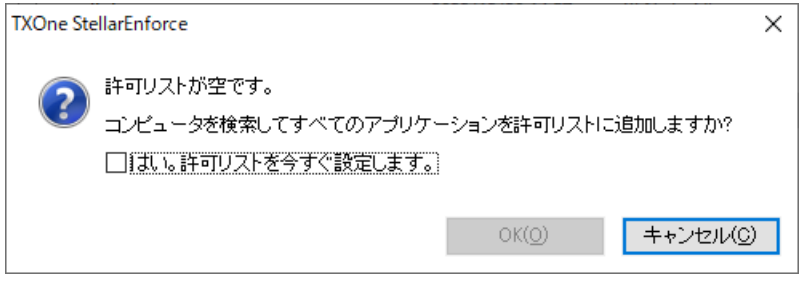
1. StellarEnforce のメイン画面を開きます。

   StellarEnforceのログイン画面が表示されます。



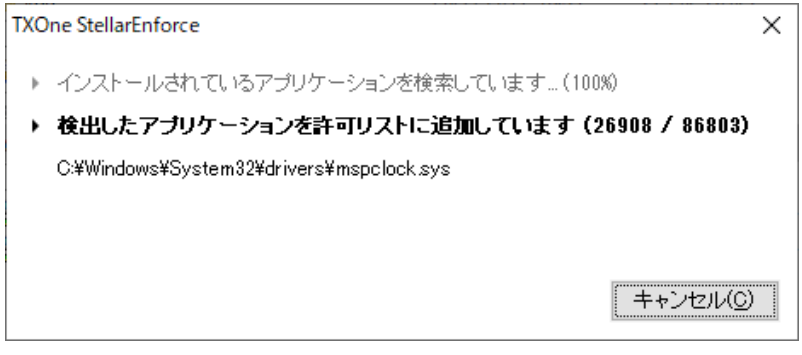
2. パスワードを入力して [ログオン] をクリックします。

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

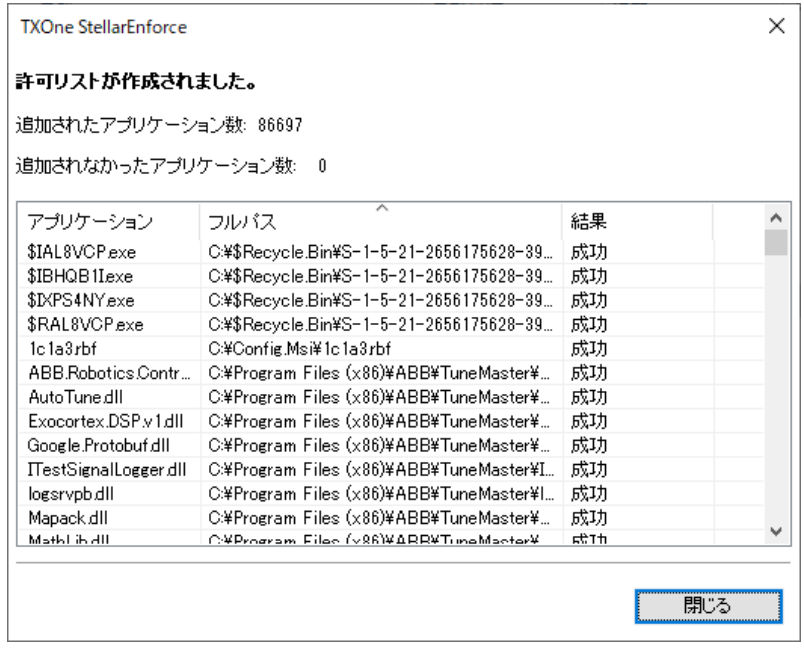


3. 通知ウィンドウで、[はい。許可リストを今すぐ設定します。] を選択して [OK] をクリックします。

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



   許可リストの設定結果が表示されます。



注意

1. TXOne StellarEnforce 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。
2. 許可リストを作成中またはアップデート中のエージェントにはポリシー設定を配信できません。

4. [閉じる] をクリックします。

ブロックされたファイルのポップアップ通知を設定する

許可されていないファイルの実行やエージェントへの変更を StellarEnforce がブロックしたときに管理下のエージェントに表示する通知を設定できます。この通知はあらゆるブロックイベントの管理者に送信され、ブロックされたファイルの詳細情報を提供します。

注意

- この機能は初期設定で無効になっています。
- StellarEnforce では、エージェントの Setup.ini や設定ファイルを使用した機能のカスタマイズのみがサポートされます。

表 2-1. ブロックされたファイルのポップアップ通知を設定する

設定	初期設定	設定場所	
		エージェント配信前	エージェント配信後
通知	無効	エージェントの Setup.ini ファイルの `[BlockNotification]` セクションをカスタマイズします。	エージェントのコマンドラインインタフェースに `blockedfilenotification` コマンドを入力します。
通知を閉じるときに管理者パスワードを要求する	有効 (通知機能が有効な場合)		エージェントのコマンドラインインタフェースに `blockedfilenotification` コマンドを入力します。
イベントの詳細を表示する (ファイル名、ファイルパス、イベント時間)			エージェントのコマンドラインインタフェースに `blockedfilenotification` コマンドを入力します。

設定	初期設定	設定場所	
		エージェント配信前	エージェント配信後
通知のタイトルとメッセージをカスタマイズする	• タイトル: アプリケーションがブロックされました • メッセージ: プログラムがブロックされました。ヘルプデスクまたは管理者に問い合わせてください。		エージェントのコマンドラインインタフェースに `blockedfilenotification` コマンドを入力します。

エージェントのメイン画面について

エージェントのメイン画面を使用すると、TXOne StellarEnforce でよく使用する機能に簡単にアクセスできます。

図 2-1.　StellarEnforce のメイン画面

次の表は、メイン画面で使用できる機能を示しています。

表 2-2.　メイン画面の機能の説明

#	項目	説明
1	概要	StellarEnforce のステータスを表示します
	許可リスト	実行が許可されているアプリケーションを表示し、ユーザがリストを管理できるようにします

#	項目	説明
	パスワード	StellarEnforce 管理者と制限付きユーザのパスワードを変更します (管理者のみ可能)
	設定	脆弱性攻撃対策の設定の有効化または無効化とシステム設定のエクスポートまたはインポートを行います
	バージョン情報	製品およびコンポーネントのバージョンを表示します
2	ステータス情報	StellarEnforce の現在のステータスを表示します
3	アプリケーション制御を有効にする	システムをロックダウンし、許可リストにないアプリケーションの実行をブロックします
	アプリケーション制御を無効にする	システムのロックダウンを解除し、許可リストにないアプリケーションの実行を許可します **注意** アプリケーション制御を無効にすると StellarEnforce が「監視」モードに切り替わります。StellarEnforce ではアプリケーションの実行がブロックされなくなりますが、許可リストにないアプリケーションが実行されるとログに記録されます。これらのログを使用して、エージェントで必要なアプリケーションがすべて許可リストに含まれているかどうかを判断できます。
4	アプリケーション制御が有効になった日時	アプリケーション制御が前回有効になった日付と時刻を表示します
	アプリケーション制御が無効になった日時	アプリケーション制御が前回無効になった日付と時刻を表示します
5	脆弱性攻撃対策	有効: すべての脆弱性攻撃対策機能が有効化されます ステータスをクリックすると、設定画面が開きます。
		有効 (一部): 脆弱性攻撃対策機能の一部が有効化されます ステータスをクリックすると、設定画面が開きます。
		無効: 脆弱性攻撃対策機能が有効化されません ステータスをクリックすると、設定画面が開きます。

#	項目	説明
6	許可リストステータス	許可リストの項目数または許可リストの更新日時をクリックすると、許可リストが表示されます。 前回のアプリケーションブロック日時をクリックすると、ブロックされたアプリケーションのログが表示されます。
7	ライセンス有効期限	StellarEnforce の有効期限を表示します 日付をクリックすると、新しいアクティベーションコードを入力できます。
8	StellarOne 登録状況 グループ名	StellarOne 登録状況: 緑のチェックマークは StellarEnforce エージェントが指定したグループに登録されたことを示し、赤いバツ印は特定グループへの登録に失敗したことを示します。 グループ名: エージェントが属するグループ名を表示します。グループ名の上にマウスを重ねると、グループ名に関する情報、グループ ID、およびポリシーバージョンが表示されます。

StellarEnforce のステータスを表示する

StellarEnforce のステータスは、システムトレイアイコンで以下のように表示されます。

注意

インストール時にシステムトレイアイコンを無効にしている場合は表示されません。

表 2-3.　ステータスアイコンの説明

メイン画面アイコン	システムトレイアイコン	ステータス	説明
		ロック	システムがロックダウンされています。許可リストに登録されていないアプリケーションは実行できません。
		ロック解除	システムのロックダウンが解除されています。許可リストに登録されていないアプリケーションも実行可能です。
		ロックおよびメンテナンスモード	システムがロックダウンされているメンテナンスモードです。許可リストに登録されているすべてのアプリケーションが実行可能です。
		ロック解除およびメンテナンスモード	システムのロックダウンが解除されているメンテナンスモードです。すべてのアプリケーションが実行可能です。
該当なし		有効期限終了	StellarEnforce のサポート契約の有効期限が終了していると、システムをロックできません。メイン画面から有効期限をクリックしてアクティベーションコードを入力します。
該当なし		ブロック	StellarEnforce はブロックされており、許可されていないアプリケーションを実行したり、管理下のエージェントに変更を加えたりすることはできません。

許可リストについて

StellarEnforce で実行を許可するファイルを追加/表示するには、許可リストを使用します。

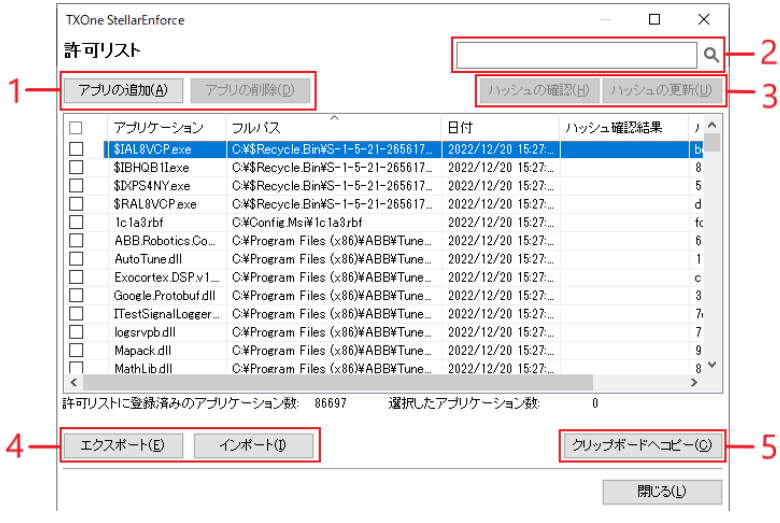


図 2-2.　StellarEnforce の許可リスト

次の表は、許可リストの画面で使用できる機能を示しています。

表 2-4.　許可リストの項目の説明

#	項目	説明
1	アプリの追加/ アプリの削除	選択した項目を許可リストに追加または許可リストから削除します。
2	検索バー	[アプリケーション] 列および [ファイルパス] 列を検索します。
3	ハッシュの確認/ ハッシュの更新	許可リストのアプリケーションに対するハッシュ値を確認または更新します。
4	エクスポート/ インポート	許可リストをエクスポートまたはインポートします。

#	項目	説明
5	クリップボードへコピー	CSV 形式 (カンマ区切りのテキスト) で許可リストをクリップボードにコピーします。リストを確認したりレポートを作成するのが容易になります。

ハッシュについて

StellarEnforce では、許可リスト内の各ファイルについて一意のハッシュ値が計算されます。ハッシュ値はファイル変更が行われるたびに変わるため、この値を使用してファイルに加えられた変更を検出できます。現在のハッシュ値を以前の値と比較することで、ファイルに対して変更が行われたかどうかを確認できます。

次の表は、ハッシュを確認するためのステータスアイコンを示しています。

表 2-5. ハッシュを確認するためのステータスアイコン

アイコン	説明
	計算されたハッシュ値は、保存されている値と一致しています。
	計算されたハッシュ値は、保存されている値と一致していません。
	ハッシュ値の計算でエラーが発生しました。

許可リスト自動更新を使用せずにファイルを移動または上書きすると、ハッシュ値が一致しなくなることがありますが、ハッシュ値の不一致は、他のアプリケーション (不正プログラムを含む) によって既存ファイルが変更または上書きされた結果である可能性もあります。ハッシュ値の不一致が発生した原因が不明な場合は、エージェントのウイルス検索などを行って脅威が存在しないかどうか確認してください。

ハッシュを確認または更新する

許可リスト内のファイルのハッシュ値を確認すると、実行を許可されているファイルの整合性を確認できます。

手順

1. TXOne StellarEnforce のデスクトップアイコン、または [スタート] メニューから [すべてのプログラム] > [TXOne StellarEnforce] をクリックして、メイン画面を開きます。
2. パスワードを指定して [ログイン] をクリックします。
3. [許可リスト] メニュー項目をクリックしてリストを開きます。

   ファイルのハッシュ値を確認するには

   a. 確認するファイルを選択します。すべてのファイルを確認するには、許可リストの上部にあるチェックボックスをオンにします。

   b. [ハッシュの確認] をクリックします。

   ファイルのハッシュ値を更新するには

   a. 更新するファイルを選択します。

   b. [ハッシュを更新] をクリックします。

重要

ハッシュ値の不一致が発生した原因が不明な場合は、エージェントのウイルス検索などを行って脅威が存在しないかどうか確認してください。

許可リストの設定

許可リストの設定後、ユーザは [アプリの追加] をクリックして新しいプログラムを追加できます。クリックすると、次の表に示すオプションが表示されます。

表 2-6.　許可リストにアプリケーションを追加する方法

オプション	使用する場面
手動で参照しファイルを選択する	対象ソフトウェアがすでにエージェント上に存在し、それが最新の状態である場合は、このオプションを選択します。 ファイルを追加すると、そのファイルの起動が可能になりますが、そのファイルやシステムは変更されません。 たとえば、初期設定の後に Windows Media Player (`wmplayer.exe`) が許可リストに含まれていない場合、ユーザは画面から許可リストにそれを追加できます。
選択したアプリケーションインストーラによって作成または修正されたファイルを自動的に追加する (許可リスト自動更新)	TXOne StellarEnforce をロック解除せずに管理下のエージェントに対して新規アプリケーションの追加やアップデートを実行する必要がある場合は、このオプションを選択します。 TXOne StellarEnforce によって新規または修正されたファイルが許可リストに追加されます。 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、このオプションを選択してインストールまたはアップデートを許可し、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。

ファイルを追加または削除する

手順

1. TXOne StellarEnforce のデスクトップアイコン、または [スタート] メニューから [すべてのプログラム] > [TXOne StellarEnforce] をクリックして、メイン画面を開きます。
2. パスワードを指定して [ログイン] をクリックします。
3. [許可リスト] メニュー項目をクリックしてリストを開きます。

   項目を追加するには

   a. [アプリの追加] をクリックし、[手動で参照しファイルを選択する] を選択して、[次へ] をクリックします。

   b. 表示されるウィンドウで、[特定のアプリケーション]、[選択したフォルダ内のすべてのアプリケーション]、または [指定したパス以下のすべてのアプリケーション] をドロップダウンリストから選択します。

   c. 選択画面が開いたら、追加するアプリケーションまたはフォルダを選択して、[開く] または [OK] をクリックします。

   d. [OK] をクリックします。追加する項目を確認して、[許可(A)] をクリックします。

   e. 必要な項目を許可リストに追加したら、[閉じる] をクリックします。

   項目を削除するには

   a. 削除するアプリケーションを許可リストから検索します。

   b. 削除するファイル名の横にあるチェックボックスをオンにして、[アプリの削除] をクリックします。

   c. 項目を削除するかどうか確認する画面で、[OK] をクリックします。

   d. もう一度 [OK] をクリックして、確認ウィンドウを閉じます。

許可リスト自動更新を使用して、アップデートまたはインストールする

TXOne StellarEnforce では、許可リスト自動更新によってアプリケーションが追加または変更されると、そのアプリケーションが許可リストに自動的に追加されます。

手順

1. TXOne StellarEnforce のデスクトップアイコン、または [スタート] メニューから [すべてのプログラム] > [TXOne StellarEnforce] をクリックして、メイン画面を開きます。
2. パスワードを指定して [ログイン] をクリックします。
3. [許可リスト] メニュー項目をクリックしてリストを開きます。
4. アプリケーションをインストールまたはアップデートするには、許可リスト自動更新によって一時的に実行を許可するインストーラを選択します。
   a. [アプリの追加] をクリックし、[選択したアプリケーションインストーラによって作成または修正されたファイルを自動的に追加する] を選択して、[次へ] をクリックします。
   b. 表示されるウィンドウで、[特定のインストーラ]、[フォルダ/サブフォルダ内のすべてのインストーラ]、または [フォルダ内のすべてのインストーラ] をドロップダウンリストから選択します。
   c. 追加するインストールパッケージまたはフォルダを選択して、[開く] をクリックします。

   注意
   許可リスト自動更新に追加できるのは、既存の EXE、MSI、BAT、および CMD ファイルのみです。

   d. 期待する項目がリストに表示されていることを確認して、[開始] をクリックします。

進捗を表すアニメーションが表示されます。

図 2-3.　進捗を表すアニメーション

5. プログラムを通常どおりインストールまたはアップデートします。完了したら、進捗を表すアニメーションで [停止] をクリックします。
6. 期待する項目が許可リストに表示されていることを確認し、[許可] をクリックしてから、[閉じる] をクリックします。

許可リストをエクスポートまたはインポートする

許可リストをデータベース形式 (.db) のファイルとしてエクスポートまたはインポートし、大規模な展開を行う場合に再利用できます。[クリップボードへコピー] を使用すると、Windows のクリップボードに CSV バージョンのリストが作成されます。

警告!

TXOne StellarEnforce は OS の実行ファイルも制御対象として制御します。許可リストをインポートする際には、エクスポートしたシステムと OS ファイルレベルで同じことを確認してからインポートしてください。

エンドポイント上の OS ファイルに何らかの差異がある場合、インポート後に OS の誤動作やシステムロックアウトを引き起こす可能性があります。

手順

1. TXOne StellarEnforce のデスクトップアイコン、または [スタート] メニューから [すべてのプログラム] > [TXOne StellarEnforce] をクリックして、メイン画面を開きます。
2. パスワードを指定して [ログイン] をクリックします。
3. [許可リスト] メニュー項目をクリックしてリストを開きます。

   許可リストをエクスポートするには

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

   b. ファイル名を指定して、[保存] をクリックします。

      エクスポートしたファイルには次の情報が含まれます。

      - ファイルのフルパス
      - ファイルハッシュ値
      - 追加のメモ
      - 最新の更新時刻

   前回のアップデート日時許可リストをインポートするには

   a. [インポート] をクリックして、許可リストを探します。

   b. ファイルを選択して、[開く] をクリックします。

アカウントの種類

TXOne StellarEnforce の権限設定により、管理者はメイン画面の特定機能へのアクセス権をユーザに付与できます。設定ファイルを使用して、制限付きユーザアカウントで使用可能な機能を指定できます。

表 2-7.　StellarEnforce のアカウント

アカウント	詳細
管理者	• 初期設定のアカウント • StellarEnforce の機能へのフルアクセス • メイン画面とコマンドラインの両方を使用可能
制限付きユーザ	• メンテナンス用セカンダリアカウント • StellarEnforce の機能への制限付きアクセス • メイン画面のみ使用可能

制限付きユーザアカウントを有効にするには、36 ページの「パスワードの設定」を参照してください。特定のアカウントでログインするには、そのアカウントのパスワードを指定します。

パスワードの設定

StellarEnforce 管理者と制限付きユーザのパスワードはメイン画面を使用して変更できますが、パスワードを変更できるのは管理者のみです。管理者アカウントでメイン画面にログインするには、メイン画面の起動時に管理者パスワードを入力します。

重要

StellarEnforce 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。

手順

1. TXOne StellarEnforce のデスクトップアイコン、または [スタート] メニューから [すべてのプログラム] > [TXOne StellarEnforce] をクリックして、メイン画面を開きます。
2. StellarEnforce 管理者パスワードを指定して、[ログオン] をクリックします。
3. [パスワード] メニュー項目をクリックして管理者パスワードページを表示します。

   StellarEnforce 管理者パスワードを変更するには

   a. 現在のパスワードを入力し、新しいパスワードを指定して確認し、[保存] をクリックします。

   警告!

   StellarEnforce 管理者のパスワードは慎重に保管してください。パスワードを忘れた場合は、トレンドマイクロのテクニカルサポートにお問い合わせください。

   制限付きユーザのパスワードを作成するには

   a. タブをクリックして、[制限付きユーザ] 画面に切り替えます。

   b. [制限付きユーザを有効にする] チェックボックスをオンにします。

   c. パスワードを指定して確認し、[保存] をクリックします。

   既存の制限付きユーザのパスワードを変更するには

   a. 新しいパスワードを指定して確認し、[保存] をクリックします。

機能の設定について

StellarEnforce では、以下の保護機能を提供します。

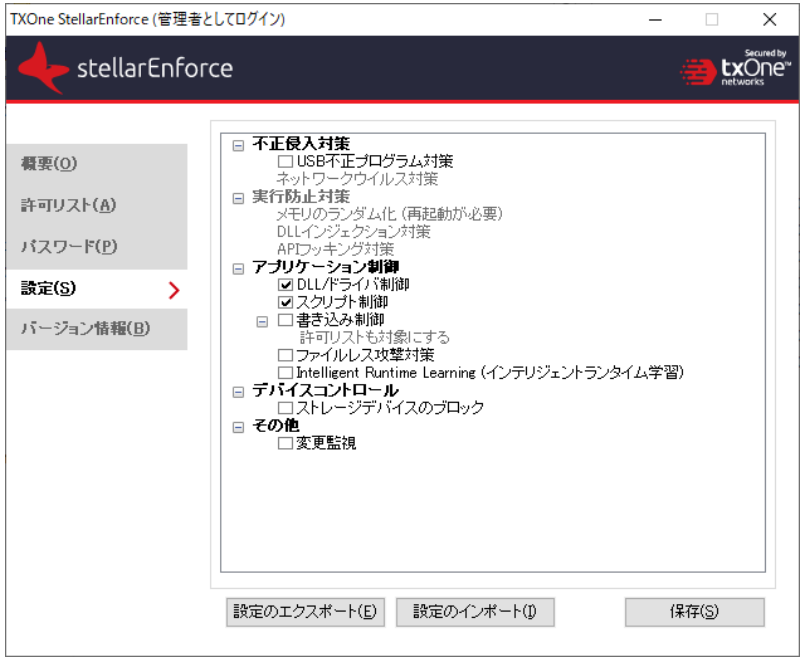


図 2-4.　StellarEnforce の設定画面

表 2-8.　不正侵入対策

設定	説明
USB 不正プログラム対策	USB 不正プログラム対策を使用すると、USB デバイスからエージェントへのウイルスの感染を防ぐことができます。ドライブの内容を表示するだけでも、ウイルスが感染する場合があります。 この機能を有効にすると、USB デバイス上のファイルからエージェントにウイルスが自動感染することを防止できます。
ネットワークウイルス対策	ネットワークトラフィックの送受信を検索して、ネットワーク上のコンピュータまたはその他のデバイスに脅威が感染しないようブロックします。 この機能を有効にすると、ネットワーク上の脅威がエージェントに感染することを防止できます。

表 2-9.　実行防止対策

設定	説明
メモリのランダム化 (再起動が必要)	Address Space Layout Randomization (ASLR: アドレス空間配置のランダム化) は、重要な機能に対するメモリの場所をランダムに割り当てることで、攻撃者が特定のプロセスのメモリの場所を強引に推測して行うシェルコードインジェクションを防止します。 Address Space Layout Randomization がサポートされていない、またはサポートが制限されている Windows XP や Windows Server 2003 などの以前のオペレーティングシステムに対して、この機能を有効にしてください。 **注意** メモリのランダム化を有効または無効にするには、エージェントを再起動する必要があります。
DLL インジェクション対策	DLL インジェクション対策は、不正なソフトウェアなどで使用される API コールの動作を検出してブロックします。これらの脅威をブロックすることで、不正なプロセスの実行を防止できます。 システムをさまざまな種類の重大な脅威から保護するために、トラブルシューティングを目的とする場合を除き、この機能は無効にしないでください。

設定	説明
API フッキング対策	API フッキング対策は、オペレーティングシステム内の重要なプロセスで使用されるメッセージの遮断や改変を実行しようとする不正なソフトウェアを検出してブロックします。 システムをさまざまな種類の重大な脅威から保護するために、トラブルシューティングを目的とする場合を除き、この機能は無効にしないでください。

表 2-10. アプリケーション制御

設定	説明	
DLL/ドライバ制御	DLL/ドライバファイルの制御を行います。DLL/ドライバファイル制御が有効な場合は、許可リストに含まれる DLL、ドライバファイルのみがロードされます。	**重要** DLL/ドライバ制御、スクリプト制御、書き込み制御、またはファイルレス攻撃対策を有効にするには、管理下のエージェントでアプリケーション制御が有効であることを確認してください。
スクリプト制御	スクリプトファイルの制御を行います。スクリプト制御が有効な場合は、許可リストに含まれるスクリプトファイルのみがインタープリタアプリケーションに読み込まれます。	
書き込み制御	書き込み制御リストに登録されたオブジェクト (ファイル、フォルダ、レジストリエントリ) への書き込みアクセスを防止し、オプションで、許可リストに登録されたファイルへの書き込みアクセスを防止します。	
ファイルレス攻撃対策	ファイルレス攻撃イベントにつながる可能性のある、許可されていないプロセスチェーンおよび引数の組み合わせを検出してブロックします。	
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。	

表 2-11. デバイスコントロール

設定	説明
ストレージデバイスのブロック	管理下のエージェントへの 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ストレージデバイスによるアクセスをブロックします。

表 2-12. その他

設定	説明
変更監視	変更監視では、管理下のエージェントのファイル、フォルダおよびレジストリの変更に関連するイベントを記録します。 **注意** 管理下のエージェントの変更監視ログを表示するには、[スタート] > [コントロール パネル] > [管理ツール] の順に選択し、[イベント ビューア] にアクセスします。

機能の設定を有効または無効にする

注意

1. TXOne StellarEnforce では、初期設定で脆弱性攻撃対策の [アプリケーション制御] にある [DLL/ドライバ制御] および [スクリプト制御] 機能が有効になっています。
2. 初期インストール時、[ネットワークウイルス対策をインストール] チェックボックスをオンにする必要があります。オンにしないと、ネットワークウイルス対策機能を選択できません。ネットワークウイルス対策を有効にしたい場合は、TXOne StellarEnforce をアンインストールしてから再インストールする必要があります。その際に必ず [ネットワークウイルス対策をインストール] チェックボックスをオンにしてください。詳細については、インストールガイドを参照してください。

手順

1. TXOne StellarEnforce のデスクトップアイコン、または [スタート] メニューから [すべてのプログラム] > [TXOne StellarEnforce] をクリックして、メイン画面を開きます。
2. パスワードを指定して [ログオン] をクリックします。
3. [設定] メニュー項目をクリックして、脆弱性攻撃対策の設定を行います。
4. 該当する機能を有効または無効にします。
5. [保存] をクリックします。

第 3 章

エージェントのコマンドラインの使用

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

この章の内容は次のとおりです。

コマンドラインで SLCmd を使用する

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

手順

1. Windows の管理者権限を使用して、コマンドプロンプトウィンドウを開きます。
2. cd コマンドを使用して、TXOne StellarEnforce のインストールフォルダに移動します。
3. たとえば、次のコマンドを入力すると初期設定の場所に移動します。

   ```
   cd /d "c:\Program Files\TXOne\StellarEnforce\"
   ```

4. 「SLCmd.exe」と入力します。

SLCmd プログラムとメイン画面の機能の比較

次の表は、SLCmd プログラムと StellarEnforce のメイン画面プログラムで使用できる TXOne StellarEnforce の機能を一覧表示しています。

表 3-1. コマンドラインでの SLCmd プログラムとメイン画面の機能の比較

機能	コマンドラインでの SLCmd プログラム	メイン画面
アカウントの管理	あり	あり
エージェントイベントの集約	なし	なし
許可リストの管理	あり	あり
設定ファイルの暗号化/復号	あり	なし
ブロックされたアプリケーションのログの表示	あり	あり
許可リストのエクスポート/インポート	あり	あり
設定のエクスポート/インポート	あり	あり
グループポリシー/グローバルポリシー	なし	なし

機能	コマンドラインでの SLCmd プログラム	メイン画面
インストール	あり	あり
Intelligent Runtime Learning (インテリジェントランタイム学習)	あり	あり
Windows Update サポート	あり	なし
アプリケーション制御	あり	あり
書き込み制御	あり	あり
書き込み制御の除外	あり	なし
変更監視	あり	あり
除外パス	あり	なし
ライセンス管理	あり	あり
管理者パスワード	あり	あり
アプリケーション制御の有効化/無効化	あり	あり
ブロックされたファイルのポップアップ通知の有効化/無効化	あり	なし
許可リスト自動更新の有効化/無効化	あり	あり
信頼するハッシュリスト	あり	なし
サービスの開始/停止	あり	なし
アンインストール	なし	なし
ストレージデバイスコントロール	あり	あり
ファイルレス攻撃対策	あり	あり
信頼する USB デバイスの追加	あり	なし
メンテナンスモードの設定	あり	なし

コマンドラインまたはメイン画面ですべての設定を行えるわけではありません。システム設定の変更の詳細については、120 ページの「エージェント設定ファイルの操作」を参照してください。

SLCmd プログラムのコマンド

次の表は、コマンドラインで SLCmd プログラムとともに使用できる主なコマンドを一覧表示しています。SLCmd プログラムを使用するには、SLCmd および目的のコマンドを入力します。「SLCmd」と入力して <Enter> キーを押し、使用可能なコマンドのリストを表示します。

注意

SLCmd をコマンドラインで使用できるのは、Windows の管理者権限を持つ StellarEnforce の管理者のみです。SLCmd では、コマンドを実行する前に管理者のパスワードを求めるプロンプトが表示されます。

SLCmd プログラムとともに使用できるコマンドの詳細なリストは次のとおりです。

汎用コマンド

コマンドラインインタフェースを使用して一般的な処理を実行します。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。

表 3-2.　省略表記と用法

パラメータ	省略表記	用法
adminpassword	ap	StellarEnforce の管理者パスワードを管理します
lock	lo	アプリケーション制御のステータスを管理します
blockedlog	bl	StellarEnforce でブロックされたアプリケーションを管理します
license	lc	StellarEnforce のライセンスを管理します
settings	set	StellarEnforce の設定を管理します
service	srv	StellarEnforce サービスを管理します

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。

表 3-3.　汎用コマンド

コマンド	パラメータ	説明
help		このヘルプファイルを表示します たとえば、次のように入力します。 SLCmd.exe help
activate	<activation_code>	本製品をアクティベートします たとえば、次のように入力します。 SLCmd.exe activate XX-XXXX-XXXXX-XXXXX- XXXXX-XXXXX-XXXXX
set adminpassword		管理者のパスワードを設定します 確認のためのパスワードの再入力が必要です たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set adminpassword
	<new_password>	管理者のパスワードを設定します 確認のためのパスワードの再入力は不要です たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set adminpassword P@ssW0Rd
set lock		現在のアプリケーション制御のステータスを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set lock **注意** 初期ステータスは disable です。
	enable	アプリケーション制御を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set lock enable

コマンド	パラメータ	説明
	disable	アプリケーション制御を無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set lockdisable
set blockedfilenotification		現在の通知設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set blockedfilenotification **注意** 初期設定は disable です。
	enable	StellarEnforce がファイルをブロックしたときに管理下のエージェントに通知を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set blockedfilenotification enable
	disable	StellarEnforce がファイルをブロックしても通知を表示しません たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set blockedfilenotification disable
show blockedlog		ブロックされたアプリケーションログを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show blockedlog
show license		ライセンス情報を表示します たとえば、次のように入力します。 SLCmd.exe show license

コマンド	パラメータ	説明
`show settings`		現在の設定を表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> show settings`
`start service`		StellarEnforce サービスを起動します たとえば、次のように入力します。 `SLCmd.exe start service`
`status`		現在の StellarEnforce のステータスを表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> status`
`stop service`		StellarEnforce サービスを停止します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> stop service`
`version`		バージョン情報を表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> version`

集中管理コマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、集中管理機能を設定します。

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

たとえば、エージェント/サーバ間の接続をテストするには、次のように入力します。

```
SLCmd.exe -p <password> test mm
```

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。

表 3-4.　省略表記と用法

パラメータ	省略表記	用法
managedmodeconfiguration	mmc	設定ファイルを管理します
servercertification	sc	サーバ証明書ファイルを管理します
managedmode	mm	エージェントの「集中管理モード」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。

表 3-5.　集中管理コマンド

コマンド	パラメータ	説明
decrypt managedmodeconfig uration	<path_of_encrypted_ file> <path_of_decrypted_ output_file>	集中管理モードの設定ファイルを復号します
encrypt managedmodeconfig uration	<path_of_file> <path_of_encrypted_ output_file>	集中管理モードの設定ファイルを暗号化します
export managedmodeconfig uration	<path_of_encrypted_ output>	指定したファイルに集中管理モードの設定をエクスポートします
export servercertification	<path_of_certification_file>	指定したファイルに管理サーバの証明書ファイルをエクスポートします
import managedmodeconfig uration	<path_of_encrypted_ input>	指定した集中管理モードの設定ファイルをインポートします
import servercertification	<path_of_certification _file>	管理サーバの証明書ファイルをインポートします

コマンド	パラメータ	説明
set managedmode	enable [-cfg <path_of_encrypted_file>] [-sc <path_of_certification_file]	集中管理モードを有効にします **注意** 初期ステータスは disable です。 次のオプションのパラメータを使用できます。 • -cfg <path_of_encrypted_file> 設定ファイルのパスを指定できます • -sc <path_of_certification_file> 証明書ファイルのパスを指定できます
set managedmode		現在の集中管理モードを表示します
show managedmodeconfig uration		集中管理モードの設定を表示します
test managedmode		管理サーバにテスト接続します

オプション機能コマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、オプションのセキュリティ機能を設定します。

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。

表 3-6.　省略表記と用法

パラメータ	省略表記	用法
apihookingprevention	api	API フッキング対策を管理します
customaction	ca	StellarEnforce で特定の種類のイベントがブロックされたときの処理を管理します

パラメータ	省略表記	用法
dlldriverlockdown	dd	DLL/ドライバ制御を管理します
dllinjectionprevention	dll	DLL インジェクション対策を管理します
exceptionpath	ep	アプリケーション制御の除外対象を管理します
integritymonitoring	in	変更監視を管理します
memoryrandomization	mr	メモリのランダム化を管理します
networkvirusprotection	net	ネットワークウイルス対策を管理します
script	scr	スクリプト制御を管理します
storagedeviceblocking	sto	管理下のエージェントへのストレージデバイス (CD/DVD ドライブ、フロッピーディスクドライブ、およびネットワークドライブ) によるアクセスを許可またはブロックします。
usbmalwareprotection	usb	USB 不正プログラム対策を管理します
writeprotection	wp	書き込み制御を管理します
writeprotection-includes-approvedlist	wpal	許可リストを含めた書き込み制御を管理します

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。

表 3-7.　オプション機能コマンド

コマンド	パラメータ	説明
set apihookingprevention	enable	API フッキング対策を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set apihookingprevention enable

コマンド	パラメータ	説明
		 **注意** 初期ステータスは `Disabled` です。
	`disable`	API フッキング対策を無効にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set apihookingprevention disable`
		API フッキング対策の設定を表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set apihookingprevention`
`set customaction`		カスタムイベント処理の設定を表示します  **注意** 初期設定は `Ask` です。
	`ignore`	カスタムイベント処理を「無視」にします アプリケーションがブロックされた後にアプリケーションに対して追加の処理を行いません たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set customaction ignore`
	`quarantine`	カスタムイベント処理を「隔離」にします アプリケーションがブロックされた後にアプリケーションに対して隔離処理を行います Windows 2000 や Windows XP などの環境では設定できません たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set customaction qurantine`

コマンド	パラメータ	説明
		注意 StellarEnforce は、Windows (Standard) XPEmbedded SP1 に対して「隔離」のカスタム処理をサポートしていません。
	ask	カスタムイベント処理を「確認」にします アプリケーションがブロックされた後にアプリケーションに対する処理を管理者がサーバで確認できるようにします 集中管理モードでのみ有効です たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set customaction ask`
`set dlldriverlockdown`		DLL/ドライバ制御の設定を表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set dlldriverlockdown` **注意** 初期ステータスは `Enabled` です。
	`enable`	DLL/ドライバ制御を有効にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set dlldriverlockdown enable`
	`disable`	DLL/ドライバ制御を無効にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set dlldriverlockdown disable`

コマンド	パラメータ	説明
set dllinjectionprevention		DLL インジェクション対策の設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set dllinjectionprevention **注意** 初期ステータスは Disabled です。
	enable	DLL インジェクション対策を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set dllinjectionprevention enable
	disable	DLL インジェクション対策を無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set dllinjectionprevention disable
set exceptionpath		アプリケーション制御の除外パス設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set exceptionpath **注意** 初期設定は Disabled です。
	enable	アプリケーション制御の除外パス設定を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set exceptionpath enable

コマンド	パラメータ	説明
	disable	アプリケーション制御の除外パス設定を無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set exceptionpath disable
set integritymonitoring		変更監視機能の設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set integritymonitoring  **注意** 初期ステータスは Disabled です。
	enable	変更監視機能を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set integritymonitoring enable
	disable	変更監視機能を無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set integritymonitoring disable
set memoryrandomization		メモリのランダム化の設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set memoryrandomization  **注意** 初期ステータスは Disabled です。

コマンド	パラメータ	説明
	enable	メモリのランダム化を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set memoryrandomization enable
	disable	メモリのランダム化を無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set memoryrandomization disable
set networkvirusprotection		ネットワークウイルス対策の設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set networkvirusprotection **注意** 初期ステータスは Enabled です。
	enable	ネットワークウイルス対策を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set networkvirusprotection enable
	disable	ネットワークウイルス対策を無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set networkvirusprotection disable
set script		スクリプト制御の設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set script **注意** 初期ステータスは Enabled です。

コマンド	パラメータ	説明
	enable	スクリプト制御を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set script enable
	disable	スクリプト制御を無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set script disable
set storagedeviceblocking		ストレージデバイスのブロックの設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set storagedeviceblocking **注意** 初期ステータスは Disabled です。
	enable	ストレージデバイスのブロックを有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set storagedeviceblocking enable
	disable	ストレージデバイスのブロックを無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set storagedeviceblocking disable

コマンド	パラメータ	説明
set usbmalwareprotection		USB 不正プログラム対策の設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set usbmalwareprotection **注意** 初期ステータスは Disabled です。
	enable	USB 不正プログラム対策を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set usbmalwareprotection enable
	disable	USB 不正プログラム対策を無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set usbmalwareprotection disable
set writeprotection		書き込み制御機能の設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set writeprotection **注意** 初期ステータスは Disabled です。
	enable	書き込み制御機能を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set writeprotection enable
	disable	書き込み制御機能を無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set writeprotection disable

コマンド	パラメータ	説明
`set writeprotection-includes-approvedlist`		書き込み制御のオプション設定を表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set writeprotection-includes-approvedlist` **注意** 初期ステータスは `Disabled` です。ただし、書き込み制御が有効になると、ステータスは `Enabled` に変更されます。
	`enable`	書き込み制御有効時に許可リストを書き込み制御の保護対象にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set writeprotection-includes-approvedlist enable`
	`disable`	許可リストを書き込み制御の保護対象から外します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set writeprotection-includes-approvedlist disable`

制限付きユーザアカウントのコマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、制限付きユーザアカウントを設定します。

`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。

表 3-8.　省略表記と用法

パラメータ	省略表記	用法
`user`	`us`	制限付きユーザアカウントを管理します
`userpassword`	`up`	制限付きユーザのパスワードを管理します

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。

表 3-9.　制限付きユーザアカウントのコマンド

コマンド	パラメータ	説明
`set user`		制限付きユーザのアカウントの設定を表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set user` **注意** 初期ステータスは `Disabled` です。
	`enable`	制限付きユーザのアカウントを有効にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set user enable`
	`disable`	制限付きユーザのアカウントを無効にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set user disable`

コマンド	パラメータ	説明
set userpassword		制限付きユーザのアカウントパスワードを設定します 確認のためのパスワードの再入力が必要です たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set userpassword
	<new_password>	制限付きユーザのアカウントパスワードを設定します 確認のためのパスワードの再入力は不要です たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set userpassword P@ssW0Rd

スクリプトコマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、スクリプトを配信します。

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。

表 3-10. 省略表記と用法

パラメータ	省略表記	用法
script	scr	スクリプトコマンドを管理します

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。

表 3-11. スクリプトコマンド

コマンド	パラメータ	説明
`add script`	<extension><interpreter1> [interpreter2] ...	指定したファイル拡張子とスクリプトインタープリタをスクリプト制御のルールとして追加します たとえば、スクリプトの拡張子 `JSP` とインタープリタファイル `jscript.js` を追加するには、次のように入力します。 `SLCmd.exe -p <admin_password> add script jsp C:\Scripts\jscript.js`
`remove script`	<extension> [interpreter1] [interpreter2] ...	指定したファイル拡張子とスクリプトインタープリタをスクリプト制御のルールから削除します たとえば、スクリプトの拡張子 `JSP` とインタープリタファイル `jscript.js` を削除するには、次のように入力します。 `SLCmd.exe -p <admin_password> remove script jsp C:\Scripts\jscript.js` **注意** インタープリタを指定しない場合は、スクリプトの拡張子に関連するすべてのインタープリタが削除されます。インタープリタを指定すると、指定したインタープリタのみがスクリプト拡張子ルールから削除されます。
`show script`		スクリプト制御のルールを表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> show script`

注意

StellarEnforce では次の初期設定のスクリプト制御のルールを使用します。

- bat <cmd.exe>
- cmd <cmd.exe>
- com <ntvdm.exe>
- dll <ntvdm.exe>
- drv <ntvdm.exe>
- exe <ntvdm.exe>
- js <cscript.exe>,<wscript.exe>
- msi <msiexec.exe>
- pif <ntvdm.exe>
- ps1 <powershell.exe>
- sys <ntvdm.exe>
- vbe <cscript.exe>,<wscript.exe>
- vbs <cscript.exe>,<wscript.exe>

許可リストコマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、許可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。

表 3-12. 省略表記と用法

パラメータ	省略表記	用法
approvedlist	al	許可リストのファイルを管理します
list	li	許可リストのインポート/エクスポート機能を管理します

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。

表 3-13. 許可リストコマンド

コマンド	パラメータ	説明
`add approvedlist`	`[-r]` <file_or_folder_path>	ファイルを許可リストに追加します たとえば、すべての Microsoft Office ファイルを許可リストに追加するには、次のように入力します。 `SLCmd.exe -p <admin_password> add approvedlist -r "C:\Program Files \Microsoft Office"` **注意** `-r` パラメータを使用すると、指定したフォルダのすべてのサブフォルダとファイルが含まれます。
`remove approvedlist`	<file_path>	指定したファイルを許可リストから削除します たとえば、`notepad.exe` を許可リストから削除するには、次のように入力します。 `SLCmd.exe -p <admin_password> remove approvedlist C:\Windows\notepad.exe`
`show approvedlist`		許可リストのファイルを一覧表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> show approvedlist`
`check approvedlist`	`-f`	許可リストのファイルをチェックしてハッシュの不一致を修復します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> check approvedlist -f`

コマンド	パラメータ	説明
	-q	許可リストのファイルをチェックして確認結果を一覧表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> check approvedlist -q
	-v	許可リストのファイルをチェックして詳細な確認結果を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> check approvedlist -v
export list	<output_file>	指定したファイルに許可リストをエクスポートします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> export list c:\approvedlist\ap.db **注意** 出力ファイルのタイプは DB 形式である必要があります。
import list	[-o] <input_file>	指定したファイルから許可リストをインポートして既存のリストに追加します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> import list c:\approvedlist\ap.db **注意** 入力ファイルのタイプは DB 形式である必要があります。 必要に応じて-o 値を使用して、既存のリストを上書きします。

アプリケーション制御関連のコマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、アプリケーション制御に関連する処理を実行します。

`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。

StellarEnforce では、拡張正規表現 (ERE) がサポートされます。詳細については、https://pubs.opengroup.org/onlinepubs/7908799/xbd/re.html#tag_007_004 を参照してください。

表 3-14. 省略表記と用法

パラメータ	省略表記	用法
quarantinedfile	qf	隔離ファイルを管理します
exceptionpath	ep	アプリケーション制御の除外対象を管理します

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。

表 3-15. アプリケーション制御関連のコマンド

コマンド	パラメータ	説明
show quarantinedfile		隔離ファイルの一覧を表示します
restore quarantinedfile	<id> [-al] [-f]	指定した隔離ファイルを復元します -al: オプションで復元したファイルを許可リストに追加します -f: オプションで強制的にファイルを復元します
remove quarantinedfile	<id>	指定した隔離ファイルを削除します
show exceptionpath		アプリケーション制御の除外パスを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show exceptionpath

コマンド	パラメータ	説明
add exceptionpath	-e <file_path>-t file	指定したファイルをアプリケーション制御の除外パスリストに追加します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add exceptionpath -e c:\sample.bat -t file
	-e <folder_path>-t folder	指定したフォルダをアプリケーション制御の除外パスリストに追加します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add exceptionpath -e c:\folder -t folder
	-e <folder_path>-t folderandsub	指定したフォルダおよびサブフォルダをアプリケーション制御の除外パスリストに追加します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add exceptionpath -e c:\folder -t folderandsub
	-e <regular_expression> -t regexp	正規表現を使用して除外を追加します たとえば、次のように入力します。 • SLCmd.exe -p <admin_password> add exceptionpath -e c:\\folder\\.* -t regexp • SLCmd.exe -p <admin_password> add exceptionpath -e \\\\computer\\folder\\.*\\file\.exe -t regexp
remove exceptionpath	-e <file_path>-t file	指定したファイルをアプリケーション制御の除外パスリストから削除します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> remove exceptionpath -e c:\sample.bat -t file

コマンド	パラメータ	説明
		 **注意** 対応する add コマンドで最初に指定した、正確な <file_path> を指定してください。
	-e <folder_path>-t folder	指定したフォルダをアプリケーション制御の除外パスリストから削除します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> remove exceptionpath -e c:\folder -t folder`  **注意** 対応する add コマンドで最初に指定した、正確な <folder_path> を指定してください。
	-e <folder_path>-t folderandsub	指定したフォルダおよびサブフォルダをアプリケーション制御の除外パスリストから削除します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> remove exceptionpath -e c:\folder -t folderandsub`  **注意** 対応する add コマンドで最初に指定した、正確な <folder_path> を指定してください。
	-e <regular_expression> -t regexp	正規表現を使用して除外を削除します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password>`

コマンド	パラメータ	説明
		`remove exceptionpath -e c:\\test\\.* -t regexp` **注意** 対応する add コマンドで最初に指定した、正確な <regular_expression> を指定してください。
`test exceptionpath`	<regular_expression> <string> `-t regexp`	正規表現が文字列に一致するかどうか確認します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> test exceptionpath C:\\test\\.* C:\test\sample.exe -t regexp`

書き込み制御コマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、書き込み制御リストと書き込み制御の除外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。

表 3-16. 省略表記と用法

パラメータ	省略表記	用法
`writeprotection`	`wp`	書き込み制御機能を管理します
`writeprotection-file`	`wpfi`	書き込み制御リストのファイルを管理します
`writeprotection-folder`	`wpfo`	書き込み制御リストのフォルダを管理します

パラメータ	省略表記	用法
writeprotection-regvalue	wprv	書き込み制御リストのレジストリ値と、関連するレジストリキーを管理します
writeprotection-regkey	wprk	書き込み制御リストのレジストリキーを管理します
writeprotection-file-exception	wpfie	書き込み制御の除外リストのファイルを管理します
writeprotection-folder-exception	wpfoe	書き込み制御の除外リストのフォルダを管理します
writeprotection-regvalue-exception	wprve	書き込み制御の除外リストのレジストリ値と、関連するレジストリキーを管理します
writeprotection-regkey-exception	wprke	書き込み制御の除外リストのレジストリキーを管理します

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。

表 3-17. 書き込み制御リストの「File」コマンド

コマンド	パラメータ	値	説明
show	writeprotection		書き込み制御リストを表示します
	writeprotection-file		ファイルに関連する書き込み制御リストを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show writeprotection-file
	writeprotection-file-exception		ファイルに関連する書き込み制御除外リストを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show

コマンド	パラメータ	値	説明
			writeprotection-file-exception
	writeprotection-folder		フォルダに関連する書き込み制御リストを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show writeprotection-folder
	writeprotection-folder-exception		フォルダに関連する書き込み制御除外リストを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show writeprotection-folder-exception
add	writeprotection-file	<file_path>	指定したファイルを書き込み制御リストに追加します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add writeprotection-file archive.txt **注意** パスの最後から前方に向かって <file_path> 値のパターンマッチングが行われます。たとえば、userfile.txt を指定すると、c:\Windows\userf

コマンド	パラメータ	値	説明
			ile.txt および c:\Temp\userfile .txt に一致します。
	writeprotection-file-exception	-t <file_path> -p <process_path>	指定したファイルに対する指定したプロセスからの書き込みを許可するルールを書き込み制御除外リストに追加します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add writeprotection-file-exception -t userfile.txt -p notepad.exe **注意** パスの最後から前方に向かって-p -t 値のパターンマッチングが行われます。たとえば、userfile.txt を指定すると、c:\Windows\userfile.txt および c:\Temp\userfile.txt に一致します。

コマンド	パラメータ	値	説明
		-t <file_path>	指定したファイルに対する書き込みを許可するルールを書き込み制御除外リストに追加します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add writeprotection-file-exception -t userfile.txt **注意** パスの最後から前方に向かって-t 値のパターンマッチングが行われます。たとえば、userfile.txt を指定すると、c:\Windows\userfile.txt および c:\Temp\userfile.txt に一致します。
		-p <process_path>	指定したプロセスからのファイルへの書き込みを許可するルールを書き込み制御除外リストに追加します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add writeprotection-file-exception -p notepad.exe

コマンド	パラメータ	値	説明
			注意 プロセスパスの最後から前方に向かって `-p` 値のパターンマッチングが行われます。たとえば、`notepad.exe` を指定すると、`c:\Windows\notepad.exe` および `c:\Temp\notepad.exe` に一致します。
	`writeprotection-folder`	`[-r] <folder_path>`	指定したフォルダを書き込み制御リストに追加します `-r` オプションでサブフォルダも追加できます たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> add writeprotection-folder -r c:\Windows\` **注意** 必要に応じて`-r` 値を使用して、指定したフォルダと関連するサブフォルダを含めます。 パスの最後から前方に向かって <folder_path> 値のパターンマッチングが行われます。たとえば、`userfile.txt`

コマンド	パラメータ	値	説明
			を指定すると、c:\Windows\userfolder および c:\Temp\userfolder に一致します。
	writeprotection-folder-exception	[-r] -t <folder_path> -p <process_path>	指定したフォルダに対する指定したプロセスからの書き込みを許可するルールを書き込み制御除外リストに追加します -r: オプションでサブフォルダを含みます たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add writeprotection-folder-exception -r -t c:\Windows\System32\Temp\ -p c:\Windows\notepad.exe **注意** 必要に応じて-r 値を使用して、指定したフォルダと関連するサブフォルダを含めます。 パスの最後から前方に向かって-p -t 値のパターンマッチングが行われます。たとえば、userfile.txt を指定すると、c:\Windows\userf

コマンド	パラメータ	値	説明
			ile.txt および c:\Temp\userfile.txt に一致します。
		[-r] -t <folder_path>	指定したフォルダに対する書き込みを許可するルールを書き込み制御除外リストに追加します -r: オプションでサブフォルダを含みます たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add writeprotection-folder-exception -r -t c:\Users\ **注意** 必要に応じて-r 値を使用して、指定したフォルダと関連するサブフォルダを含めます。 フォルダパスの最後の部分から前方に向かって-t 値のパターンマッチングが行われます。たとえば、userfolder を指定すると、c:\Windows\userfolder および c:\Temp\userfolder に一致します。

コマンド	パラメータ	値	説明
		-p <process_path>	指定したプロセスからのフォルダへの書き込みを許可するルールを書き込み制御除外リストに追加します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> add writeprotection-folder-exception -p c:\Windows\System32\` **注意** プロセスパスの最後からパスの前方に向かって`-p` 値のパターンマッチングが行われます。たとえば、`notepad.exe` と指定すると、`c:\Windows\notepad.exe` と `c:\Temp\notepad.exe` に一致します。
`remove`	`writeprotection-file`	<file_path>	指定したファイルを書き込み制御リストから削除します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> remove writeprotection-file archive.txt`

コマンド	パラメータ	値	説明
			 **注意** 対応する add コマンドで最初に指定した、正確な <file_path> を指定してください。
	`writeprotection-file-exception`	`-t` <file_path> `-p` <process_path>	指定したファイルに対する指定したプロセスからの書き込みを許可するルールを書き込み制御除外リストから削除します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> remove writeprotection-file-exception -t userfile.txt -p notepad.exe`  **注意** 対応する add コマンドで最初に指定した、正確な <file_path> および <process_path> を指定してください。

コマンド	パラメータ	値	説明
		-t <file_path>	指定したファイルに対する書き込みを許可するルールを書き込み制御除外リストから削除します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> remove writeprotection-file-exception -t userfile.txt **注意** パスの最後から前方に向かって-t 値のパターンマッチングが行われます。たとえば、userfile.txt を指定すると、c:\Windows\userfile.txt および c:\Temp\userfile.txt に一致します。
		-p <process_path>	指定したプロセスからのファイルへの書き込みを許可するルールを書き込み制御除外リストから削除します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> remove writeprotection-file-exception -p notepad.exe

コマンド	パラメータ	値	説明
			 **注意** プロセスパスの最後からパスの前方に向かって`-p` 値のパターンマッチングが行われます。たとえば、`notepad.exe` と指定すると、`c:\Windows\notepad.exe` と `c:\Temp\notepad.exe` に一致します。
	`writeprotection-folder`	`[-r] <folder_path>`	指定したフォルダを書き込み制御リストから削除します `-r`:オプションでサブフォルダを含みます たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> remove writeprotection-folder -r c:\Windows\`  **注意** 必要に応じて`-r` 値を使用して、指定したフォルダと関連するサブフォルダを含めます。 対応する add コマンドで最初に指定した、正確な <folder_path> および

コマンド	パラメータ	値	説明
			-r 値を指定してください。
	writeprotection-folder-exception	[-r] -t <folder_path> -p <process_path>	指定したフォルダに対する指定したプロセスからの書き込みを許可するルールを書き込み制御除外リストから削除します -r: オプションでサブフォルダを含みます たとえば、次のように入力します。 SLCmd.exe -p <admin_password> remove writeprotection-folder-exception -r -t c:\Windows\System32\Temp\ -p c:\Windows\notepad.exe **注意** 必要に応じて-r 値を使用して、指定したフォルダと関連するサブフォルダを含めます。 対応する add コマンドで最初に指定した、正確な <folder_path>、<process_path>、および-r 値を指定してください。

コマンド	パラメータ	値	説明
		[-r] -t <folder_path>	指定したフォルダに対する書き込みを許可するルールを書き込み制御除外リストから削除します -r:オプションでサブフォルダを含みます たとえば、次のように入力します。 SLCmd.exe -p <admin_password> remove writeprotection-folder-exception -r -t c:\Users\ **注意** 必要に応じて-r 値を使用して、指定したフォルダと関連するサブフォルダを含めます。 フォルダパスの最後の部分から前方に向かって-t 値のパターンマッチングが行われます。たとえば、userfolder を指定すると、c:\Windows\userfolder および c:\Temp\userfolder に一致します。

コマンド	パラメータ	値	説明
		-p <process_path>	指定したプロセスからのフォルダへの書き込みを許可するルールを書き込み制御除外リストから削除します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> remove writeprotection-folder-exception -p c:\Windows\System32\` **注意** プロセスパスの最後から前方に向かって `-p` 値のパターンマッチングが行われます。たとえば、`notepad.exe` を指定すると、`c:\Windows\notepad.exe` および `c:\Temp\notepad.exe` に一致します。

表 3-18. 書き込み制御リストの「Registry」コマンド

コマンド	パラメータ	値	説明
show	writeprotection		書き込み制御リストを表示します
	writeprotection-regvalue		レジストリ値に関連する書き込み制御リストを表示します
	writeprotection-regvalue-exception		レジストリ値に関連する書き込み制御除外リストを表示します

コマンド	パラメータ	値	説明
	writeprotection-regkey		レジストリキーに関連する書き込み制御リストを表示します
	writeprotection-regkey-exception		レジストリキーに関連する書き込み制御除外リストを表示します
add	writeprotection-regvalue	<path_of_registry_key> <registry_value>	指定したレジストリ値を書き込み制御リストに追加します レジストリキーの指定が必要です たとえば、「HKEY\test\」レジストリキーのレジストリ値「testvalue」を書き込み制御リストに追加するには、次のように入力します。 SLCmd.exe -p <admin_password> add writeprotection-regvalue HKEY\test testvalue
	writeprotection-regvalue-exception	-t <path_of_registry_key> <registry_value> -p <process_path>	指定したレジストリ値に対する指定したプロセスからの書き込みを許可するルールを書き込み制御除外リストに追加します レジストリキーの指定が必要です **注意** このコマンドにより、指定したプロセスによる指定したレジストリ値への書き込みアクセスが可能になります。 プロセスパスの最後から前方に向かって-p 値のパターンマッチングが行われます。

コマンド	パラメータ	値	説明
		-t <path_of_registry_key> <registry_value>	指定したレジストリ値に対する書き込みを許可するルールを書き込み制御除外リストに追加します レジストリキーの指定が必要です **注意** このコマンドにより、任意のプロセスによる指定したレジストリ値への書き込みアクセスが可能になります。
		-p <process_path>	指定したプロセスからのレジストリ値への書き込みを許可するルールを書き込み制御除外リストに追加します **注意** このコマンドにより、指定したプロセスによる任意のレジストリ値への書き込みアクセスが可能になります。 プロセスパスの最後から前方に向かって-p 値のパターンマッチングが行われます。
	writeprotection-regkey	[-r] <path_of_registry_key>	指定したレジストリキーを書き込み制御リストに追加します -r:オプションでサブキーを含みます

コマンド	パラメータ	値	説明
			 **注意** 必要に応じて`-r` 値を使用して、指定したフォルダと関連するサブフォルダを含めます。
	`writeprotection-regkey-exception`	[`-r`] `-t` <path_of_registry_key> `-p` <process_path>	指定したレジストリキーに対する指定したプロセスからの書き込みを許可するルールを書き込み制御除外リストに追加します `-r`: オプションでサブキーを含みます  **注意** このコマンドにより、指定したプロセスによる指定したレジストリキーへの書き込みアクセスが可能になります。 必要に応じて`-r` 値を使用して、指定したフォルダと関連するサブフォルダを含めます。 プロセスパスの最後から前方に向かって`-p` 値のパターンマッチングが行われます。
		[`-r`] `-t` <path_of_registry_key>	指定したレジストリキーに対する書き込みを許可するルールを書き込み制御除外リストに追加します `-r`: オプションでサブキーを含みます

コマンド	パラメータ	値	説明
			 **注意** このコマンドにより、任意のプロセスによる指定したレジストリキーへの書き込みアクセスが可能になります。 プロセスパスの最後から前方に向かって`-p` 値のパターンマッチングが行われます。
		`-p <process_path>`	指定したプロセスからのレジストリキーへの書き込みを許可するルールを書き込み制御除外リストに追加します  **注意** このコマンドにより、指定したプロセスによる任意のレジストリキーへの書き込みアクセスが可能になります。 プロセスパスの最後から前方に向かって`-p` 値のパターンマッチングが行われます。

コマンド	パラメータ	値	説明
remove	writeprotection-regvalue	<path_of_registry_key> <registry_value>	指定したレジストリ値を書き込み制御リストから削除します レジストリキーの指定が必要です **注意** 対応する add コマンドで最初に指定した、正確な <path_of_registry_key> および <registry_value> を指定してください。
	writeprotection-regvalue-exception	-t <path_of_registry_key> <registry_value> -p <process_path>	指定したレジストリ値に対する指定したプロセスからの書き込みを許可するルールを書き込み制御除外リストから削除します レジストリキーの指定が必要です **注意** 対応する add コマンドで最初に指定した、正確な <path_of_registry_key>、<registry_value>、および <process_path> を指定してください。 パスの最後から前方に向かって-p 値のパターンマッチングが行われます。
		-t <path_of_registry_key> <registry_value>	指定したレジストリ値に対する書き込みを許可するルールを書き込み制御除外リストから削除します レジストリキーの指定が必要です

コマンド	パラメータ	値	説明
		-p <process_path>	指定したプロセスからのレジストリ値への書き込みを許可するルールを書き込み制御除外リストから削除します  **注意** パスの最後から前方に向かって-p 値のパターンマッチングが行われます。
	writeprotection-regkey	[-r] <path_of_registry_key>	指定したレジストリキーに対する指定したプロセスからの書き込みを許可するルールを書き込み制御除外リストから削除します -r:オプションでサブキーを含みます  **注意** 対応する add コマンドで最初に指定した、正確な <path_of_registry_key> および-r 値を指定してください。 必要に応じて-r 値を使用して、指定したフォルダと関連するサブフォルダを含めます。
	writeprotection-regkey-exception	[-r] -t <path_of_registry_key> -p <process_path>	指定したレジストリキーに対する書き込みを許可するルールを書き込み制御除外リストから削除します -r:オプションでサブキーを含みます

コマンド	パラメータ	値	説明
			 **注意** 対応する add コマンドで最初に指定した、正確な <path_of_registry_key>、<process_path>、および-r 値を指定してください。 必要に応じて-r 値を使用して、指定したフォルダと関連するサブフォルダを含めます。 パスの最後から前方に向かって-p 値のパターンマッチングが行われます。
		[-r] -t <path_of_registry_key>	指定したレジストリキーに対する書き込みを許可するルールを書き込み制御除外リストから削除します -r: オプションでサブキーを含みます  **注意** 必要に応じて-r 値を使用して、指定したフォルダと関連するサブフォルダを含めます。
		-p <process_path>	指定したプロセスからのレジストリキーへの書き込みを許可するルールを書き込み制御除外リストから削除します

コマンド	パラメータ	値	説明
			注意 パスの最後から前方に向かって-p 値のパターンマッチングが行われます。

信頼するデジタル証明書コマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、信頼するデジタル証明書を設定します。

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。

表 3-19. 省略表記と用法

パラメータ	省略表記	用法
trustedcertification	tc	信頼するデジタル証明書の管理

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。

表 3-20. 信頼するデジタル証明書コマンド

コマンド	パラメータ	説明
set trustedcertification		信頼するデジタル証明書の設定を表示します **注意** 初期設定は Enabled です。
	enable	信頼するデジタル証明書の設定を有効にします
	disable	信頼するデジタル証明書の設定を無効にします
show trustedcertification	[-v]	信頼するデジタル証明書のリストを表示します -v: オプションで詳細情報を表示します

コマンド	パラメータ	説明
`add trustedcertification`	`-c` <file_path> [`-l` <label>] [`-u`]	指定したファイルを信頼するデジタル証明書リストに追加します `-l`: オプションで一意のラベルを指定できます `-u`: オプションで指定したデジタル証明書ファイルで署名されたファイルを許可リストの自動更新監視対象にします
`remove trustedcertification`	`-l` <label>	信頼するデジタル証明書リストから指定されたラベルのルールを削除します

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

コマンドラインインタフェースに次の形式でコマンドを入力して、Intelligent Runtime Learning (インテリジェントランタイム学習) を設定します。

表 3-21. 省略表記と用法

パラメータ	省略表記	用法
`intelligentruntimelearning`	`irl`	許可リスト内のアプリケーションによって生成されたランタイム実行ファイルがエージェントで許可されます

表 3-22. Intelligent Runtime Learning (インテリジェントランタイム学習) のコマンド

コマンド	パラメータ	説明
`set intelligentruntimelearning`		Intelligent Runtime Learning (インテリジェントランタイム学習) を使用するための現在の設定を表示します
	`enable`	Intelligent Runtime Learning (インテリジェントランタイム学習) の使用を有効にします
	`disable`	Intelligent Runtime Learning (インテリジェントランタイム学習) の使用を無効にします

信頼するハッシュリストのコマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、信頼するハッシュ値を設定します。

`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。

表 3-23. 省略表記と用法

パラメータ	省略表記	用法
`trustedhash`	`th`	StellarEnforce 管理者が追加した信頼するハッシュ値 (ファイル) 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。

表 3-24. 信頼するハッシュリストのコマンド

コマンド	パラメータ	説明
`set trustedhash`		信頼するハッシュリストの設定を表示します **注意** 初期設定は `Disabled` です。
	`enable`	信頼するハッシュリストの使用を有効にします
	`disable`	信頼するハッシュリストの使用を無効にします
`show trustedhash`		信頼するハッシュリストのハッシュ値を表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> show trustedhash`
`add trustedhash`	`-v <hash> [-l <label>] [-u][-al] [-t<file_path>][-n<note>]`	指定したハッシュ値を信頼するハッシュリストに追加します ハッシュ値 `xxx` を含む信頼するファイルを信頼するハッシュリストに追加するには、次のように入力します。

コマンド	パラメータ	説明
		SLCmd.exe -p <admin_password> add trustedhash -v xxx -l：オプションでこのハッシュに対する一意のラベルを指定できます -u：オプションでこのハッシュに一致するファイルを許可リストの自動更新の監視対象にできます  **注意** -u オプションを使用する場合は、事前指定による許可リスト自動更新が有効である必要があります。 -al：オプションでファイルへの最初のアクセス時、このハッシュ値に一致するファイルを許可リストに追加できます -t：オプションでハッシュの確認対象となるファイルのパスを指定できます  **注意** パスの最後から前方に向かって-t 値のパターンマッチングが行われます。たとえば、userfile.txt を指定すると、c:\Windows\userfile.txt および c:\Temp\userfile.txt に一致します。 -n：オプションでメモを指定できます
remove trustedhash	-l <label>	指定したラベルのファイルを信頼するハッシュリストから削除します
remove trustedhash	-a	信頼するハッシュリストのハッシュ値をすべて削除します

許可リスト自動更新コマンド

エージェントの許可リストに指定されていないインストーラやファイルを実行するには、次の形式でコマンドを入力して許可リスト自動更新を設定します。

`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。

表 3-25. 省略表記と用法

パラメータ	省略表記	用法
`trustedupdater`	`tu`	事前指定による許可リスト自動更新のツールプロセスを管理します

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。

表 3-26. 許可リスト自動更新コマンド

コマンド	パラメータ	説明
`start trustedupdater`	[-r] <path_of_installer>	許可リスト自動更新を開始して、指定するフォルダ内のインストールパッケージ (`EXE` および `MSI` ファイル形式) を許可リストに追加します **注意** `-r`: オプションでサブフォルダを含みます たとえば、`C:\Installers` フォルダとそのサブフォルダのすべてのインストールパッケージを含めるには、次のように入力します。 `SLCmd.exe -p <admin_password> start trustedupdater -r C:\Installers`

コマンド	パラメータ	説明
`stop trustedupdater`	`[-f]`	許可リスト自動更新を無効にして、許可リストへの新規または更新済みファイルの追加を停止します **注意** `-f`: オプションで新規/更新ファイルを自動で許可リストに追加します たとえば、許可リスト自動更新を停止し、プロンプトが表示された後、指定したすべてのインストーラ (停止コマンドを受信する前に指定したもの) を許可リストに追加するには、次のように入力します。 `SLCmd.exe -p <admin_password> stop trustedupdater -f`

信頼する USB デバイスのコマンド

コマンドラインインタ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。

表 3-27. 省略表記と用法

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。

表 3-28. 信頼する USB デバイスのコマンド

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`
`add trustedusbdevice`	`[-vid <VID>] [-pid <PID>] [-sn <SN>]`	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 たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> add trustedusbdevice -sn 123456`
`remove trustedusbdevice`	`[-vid <VID>] [-pid <PID>] [-sn <SN>]`	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。識別子は 1 つ以上指定する必要があります たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> remove trustedusbdevice -sn 123456`

事前指定による許可リスト自動更新コマンド

重要

事前指定による許可リスト自動更新にファイルを追加するための add コマンドは、事前指定による許可リスト自動更新のコマンド一覧に指定された汎用コマンドとは別の形式に準拠します。事前指定による許可リスト自動更新へのファイルの追加の詳細については、102 ページの「事前指定による許可リスト自動更新の「追加」コマンド」を参照してください。

コマンドラインインタフェースに次の形式でコマンドを入力して、事前指定による許可リスト自動更新を設定します。

`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。

表 3-29. 省略表記と用法

パラメータ	省略表記	用法
predefinedtrustedupdater	ptu	事前指定による許可リスト自動更新のファイルを管理します

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。

表 3-30. 事前指定による許可リスト自動更新コマンド

コマンド	パラメータ	説明
`add predefinedtrustedupdater`	`-e` <folder_or_file_exception>	指定したファイル/フォルダを事前指定による許可リスト自動更新の除外リストに追加します このオプションは`-u`、`-t` オプションと同時に指定することはできません **重要** 事前指定による許可リスト自動更新にファイルを追加するための `add` コマンドは、このリストに指定されたその他のコマンドとは別の形式に準拠します。事前指定による許可リスト自動更新の除外リストではなく、事前指定による許可リスト自動更新へのファイルの追加の詳細については、102 ページの「事前指定による許可リスト自動更新の「追加」コマンド」を参照してください。 たとえば、`notepad.exe` を事前指定による許可リスト自動更新の除外リストに追加するには、次のように入力します。 `SLCmd.exe -p <admin_password> add predefinedtrustedupdater -e C:\Windows\notepad.exe`

コマンド	パラメータ	説明
`decrypt predefinedtrustedupdater`	<path_of_encrypted_file> <path_of_decrypted_output_file>	指定した事前指定による許可リスト自動更新の設定ファイルを指定した場所に復号します たとえば、`C:\Notepad.xen` を `C:\Editors\notepad.xml` に復号するには、次のように入力します。 `SLCmd.exe -p <admin_password> decrypt predefinedtrustedupdater C:\Notepad.xen C:\Editors\notepad.xml`
`encrypt predefinedtrustedupdater`	<path_of_file> <path_of_encrypted_output_file>	指定した事前指定による許可リスト自動更新の設定ファイルを指定した場所に暗号化します たとえば、`C:\notepad.xml` を `C:\Editors\Notepad.xen` に暗号化するには、次のように入力します。 `SLCmd.exe -p <admin_password> encrypt predefinedtrustedupdater C:\Editors\notepad.xml C:\Notepad.xen`
`export predefinedtrustedupdater`	<path_of_encrypted_output t>	指定した場所に事前指定による許可リスト自動更新の設定ファイルをエクスポートします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> export predefinedtrustedupdater C:\Lists\ptu_list.xen`

コマンド	パラメータ	説明
`import predefinedtrustedupdater`	<path_of_encrypted_input>	指定した場所の事前指定による許可リスト自動更新の設定ファイルをインポートします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> import predefinedtrustedupdater C:\Lists\ptu_list.xen`
`remove predefinedtrustedupdater`	`-l` <label_name>	事前指定による許可リスト自動更新設定から指定されたラベルのルールを削除します たとえば、「Notepad」ルールを削除するには、次のように入力します。 `SLCmd.exe -p <admin_password> remove predefinedtrustedupdater -l Notepad`
	`-e` <folder_or_file_exception>	指定したファイル/フォルダを事前指定による許可リスト自動更新の除外リストから削除します たとえば、`notepad.exe` の除外を削除するには、次のように入力します。 `SLCmd.exe -p <admin_password> remove predefinedtrustedupdater -e C:\Windows\notepad.exe`
`set predefinedtrustedupdater`		事前指定による許可リスト自動更新のステータスを表示します **注意** 初期ステータスは `Disabled` です。

コマンド	パラメータ	説明
	Enable	事前指定による許可リスト自動更新を有効にします
	disable	事前指定による許可リスト自動更新を無効にします
show predefinedtrustedupdater		事前指定による許可リスト自動更新のルールを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show predefinedtrustedupdater
	-e	事前指定による許可リスト自動更新の除外リストを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show predefinedtrustedupdater -e

事前指定による許可リスト自動更新の「追加」コマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、事前指定による許可リスト自動更新にプロセス、ファイル、またはフォルダを追加します。

SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u <folder_or_file> -t <type_of_object> [<optional_values>]

次の表は、コマンド、パラメータ、および基本の値の一覧を示しています。

表 3-31. 前指定による許可リスト自動更新の「Add」コマンド

コマンド	パラメータ	値	説明
add	predefinedtrusteedupdater	<folder_or_file>	指定したファイルまたはフォルダを事前指定による許可リスト自動更新に追加します たとえば、notepad.exe を事前指定による許可リスト自動更新の除外リストに追加するには、次のように入力します。

			SLCmd.exe -p <admin_password> add predefinedtrustedupdater -e C:\Windows \notepad.exe

コマンドの末尾に次の値を追加します。

表 3-32. 事前指定による許可リスト自動更新の「Add」コマンドの追加値

値	必須/任意	説明		使用例
-u <folder_or_file>	必須	事前指定による許可リスト自動更新リストに追加するファイル/フォルダを指定します 指定したファイル/フォルダの種類を -t オプションで指定する必要があります		該当なし  **注意** このパラメータには、-t <type_of_object> の値を使用する必要があります。
-t <type_of_object>	必須	-u オプションで指定したファイルの種類を指定します 以下のオブジェクト名が指定できます:		SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows \notepad.exe -t process
		process	EXE などの実行形式ファイル	
		file	MSI や BAT ファイルなどのファイル	
		folder	EXE、MSI や BAT ファイルを含むフォルダ	
		folderandsub	EXE、MSI や BAT ファイルを含むフォルダとサブフォルダ	

値	必須/任意	説明	使用例
-p <parent_process>	任意	親プロセスのファイルパスを指定できます	SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -p C:\batch files\note.bat
-l <label_name>	任意	許可リストの自動更新ルールに一意のラベルを指定できます **注意** 指定しない場合、任意のラベルが設定されます	SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -l EDITOR
-al Enable	任意	-u オプションで指定したファイルが実行されるときまたは指定したフォルダに含まれるファイルが実行されるときに、許可リストのハッシュ値と実行されるファイルの比較を行います **注意** 何も指定しない場合はこのオプションが有効になりハッシュのチェックが行われます	SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -al enable

値	必須/任意	説明	使用例
-al Disable	任意	-u オプションで指定したファイルが実行されるときまたは指定したフォルダに含まれるファイルが実行されるときに、許可リストのハッシュ値と実行されるファイルの比較を行わずに処理を継続させます	SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -al disable

Windows Update サポート

コマンドラインインタフェースに次の形式でコマンドを入力して、Windows Update サポートを設定します。

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。

表 3-33. 省略表記と用法

パラメータ	省略表記	用法
windowsupdatesupport	wus	アプリケーション制御が有効なエージェントでの Windows Update の実行を許可します

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。

表 3-34. Windows Update サポートのコマンド

コマンド	パラメータ	説明
set windowsupdatesupport		Windows Update サポートの現在の設定を表示します **注意** 初期設定は Disabled です。
	enable	Windows Update サポートを有効にします

コマンド	パラメータ	説明
	disable	Windows Update サポートを無効にします

ファイルのブロック通知コマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、ファイルのブロック通知を有効または無効にします。

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。

表 3-35. 省略表記と用法

パラメータ	省略表記	用法
blockedfilenotification	bfn	StellarEnforce がアプリケーションの実行やエージェントへの変更をブロックしたときに管理下のエージェントに通知を表示します

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。

表 3-36. ファイルのブロック通知コマンド

コマンド	パラメータ	説明
set blockedfilenotification		現在の通知設定を表示します **注意** 初期設定は Disabled です。
	enable	ポップアップ通知を有効にします
	disable	ポップアップ通知を無効にします

設定ファイルコマンド

コマンドラインインタフェースに次のコマンドを入力して、設定ファイルに対して処理を実行します。

`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。

表 3-37. 省略表記と用法

パラメータ	省略表記	用法
`configuration`	`con`	設定ファイルを管理します

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。

表 3-38. 設定ファイルコマンド

コマンド	パラメータ	説明
`decrypt configuration`	<path_of_encrypted_file> <path_of_decrypted_output_file>	設定ファイルを復号します たとえば、`C:\config.xen` を `C:\config.xml` に復号する場合は、次のように入力します。 `SLCmd.exe -p <admin_password> decrypt configuration C:\config.xen C:\config.xml`
`encrypt configuration`	<path_of_file> <path_of_encrypted_output_file>	設定ファイルを暗号化します たとえば、`C:\config.xml` を `C:\config.xen` に暗号化する場合は、次のように入力します。 `SLCmd.exe -p <admin_password> encrypt configuration C:\config.xml C:\config.xen`
`export configuration`	<path_of_encrypted_output>	指定したファイルに設定をエクスポートします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> export configuration C:\config.xen`

コマンド	パラメータ	説明
import configuration	<path_of_encrypted_input>	指定したファイルから設定をインポートします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> import configuration C:\config.xen

ファイルレス攻撃対策のコマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、ファイルレス攻撃対策機能を設定します。

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。

表 3-39. 省略表記と用法

パラメータ	省略表記	用法
filelessattackprevention	flp	ファイルレス攻撃対策を管理します
filelessattackprevention-process	flpp	ファイルレス攻撃対策のプロセスを管理します
filelessattackprevention-exception	flpe	ファイルレス攻撃対策の除外を管理します

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。

表 3-40. ファイルレス攻撃対策のコマンド

コマンド	パラメータ	説明
set filelessattackprevention		ファイルレス攻撃対策の現在のステータスを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set filelessattackprevention

コマンド	パラメータ	説明
	enable	ファイルレス攻撃対策を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set filelessattackprevention enable
	disable	ファイルレス攻撃対策を無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set filelessattackprevention disable
show filelessattackprevention-process		監視対象プロセスのリストを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show filelessattackprevention-process
add filelessattackprevention-exception	<monitored_process> <Parentprocess1> <Parentprocess2> <Parentprocess3> <Parentprocess4> -a <arguments> -regex -l <label>	ファイルレス攻撃対策の除外を追加します 次の除外の場合: • 監視対象プロセス: cscript.exe • 親プロセス 1: a.exe • 親プロセス 2: • 親プロセス 3: c.exe • 親プロセス 4: • 引数: -abc -def • 引数のユーザ正規表現: No 除外を追加するには、次のように入力します。 SLCmd.exe -p <admin_password> add flpe cscript.exe a.exe "" c.exe "" -a "-abc -def"
remove filelessattackprevention-exception	-l <label>	ファイルレス攻撃対策の除外を削除します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> remove filelessattackprevention-exception -l <label>

注意

- 監視対象プロセスが StellarEnforce の起動前に開始された場合、StellarEnforce はそのプロセスを検出およびブロックできません。
- Windows Vista x86 システム (Service Pack のインストールなし) では、ファイルレス攻撃対策機能でプロセスチェーンのチェックを実行できますが、コマンドライン引数のチェックを実行することはできません。プロセスチェーンのチェックをパスすると、コマンドライン引数のチェックはスキップされます。

メンテナンスモードのコマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、メンテナンスモードに関連する処理を実行します。

```
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。

表 3-41. 省略表記と用法

パラメータ	省略表記	用法
approvedlist	al	メンテナンスモードで許可リストを管理します
maintenancemode	mtm	メンテナンスモードを管理します
maintenancemodeschedule	mtms	メンテナンスモードの予約を管理します

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。

表 3-42. メンテナンスモードのコマンド

コマンド	パラメータ	説明
start maintenancemode		メンテナンスモードを開始します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> start maintenancemode

コマンド	パラメータ	説明
	-duration	メンテナンスモードの終了後に実行する処理と、メンテナンスモードの期間を時間単位 (1～999) で設定します たとえば、次のように入力します。`SLCmd start maintenancemode -scan al -duration 3`
	`-scan quarantine`	メンテナンスモードを開始し、メンテナンス期間後のファイルの検索を有効にします StellarEnforce は、メンテナンス期間中に作成/実行/変更されたファイルを検索し、検出されたファイルを隔離して、不正として検出されなかったファイルは許可リストに追加します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> start maintenancemode -scan quarantine`
	`-scan al`	メンテナンスモードを開始し、メンテナンス期間後のファイルの検索を有効にします。StellarEnforce は、メンテナンス期間中に作成/実行/変更されたファイルを検索し、不正として検出されたファイルを含めて許可リストに追加します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> start maintenancemode -scan al`
`stop maintenancemode`		メンテナンスモードを終了します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> stop maintenancemode` **注意** エージェントがメンテナンスモードを終了中の場合、メンテナンスモードは終了できません。

コマンド	パラメータ	説明
	-discard	メンテナンスモードを終了し、ファイルキュー内のファイルを許可リストに追加しません たとえば、次のように入力します。 SLCmd.exe -p <admin_password> stop maintenancemode discard **注意** エージェントがメンテナンスモードを終了中の場合、メンテナンスモードは終了できません。
set maintenancemodeschedule	-start YYYY-MM-DDTHH:MM:SS -end YYYY-MM-DDTHH:MM:SS	メンテナンスモードの予約を設定します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set maintenancemodeschedule -start 2019-04-07T01:00:00 -end 2019-04-07T05:00:00 **注意** • エージェントがすでにメンテナンスモードになっているか、メンテナンスモードを終了中 の場合、メンテナンスモードの予約は設定できません。 • 現在の時間よりも前にメンテナンスモードの予約を開始するように設定している場合、設定を保存後、ただちにメンテナンス期間が開始されます。

コマンド	パラメータ	説明
	`-start` YYYY-MM-DDTHH:MM:SS `-end` YYYY-MM-DDTHH:MM:SS `-scan quarantine`	次を設定します。 • メンテナンスモードの予約を設定します • メンテナンス期間後のファイルの検索を有効にします: StellarEnforce は、メンテナンス期間中に作成/実行/変更されたファイルを検索し、検出された脅威を隔離して、不正として検出されなかったファイルは許可リストに追加します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set maintenancemodeschedule -start 2019-04-07T01:00:00 -end 2019-04-07T05:00:00 -scan quarantine`  **注意** • エージェントがすでにメンテナンスモードになっているか、メンテナンスモードを終了中の場合、メンテナンスモードの予約は設定できません。 • 現在の時間よりも前にメンテナンスモードの予約を開始するように設定している場合、設定を保存後、ただちにメンテナンス期間が開始されます。

コマンド	パラメータ	説明
	`-start` YYYY-MM-DDTHH:MM:SS `-end` YYYY-MM-DDTHH:MM:SS `-scan al`	次を設定します。 • メンテナンスモードの予約を設定します • メンテナンス期間後のファイルの検索を有効にします: StellarEnforce は、メンテナンス期間中に作成/実行/変更されたファイルを検索し、不正として検出されたファイルを含めて許可リストに追加します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set maintenancemodeschedule -start 2019-04-07T01:00:00 -end 2019-04-07T05:00:00 -scan al`  **注意** • エージェントがすでにメンテナンスモードになっているか、メンテナンスモードを終了中の場合、メンテナンスモードの予約は設定できません。 • 現在の時間よりも前にメンテナンスモードの予約を開始するように設定している場合、設定を保存後、ただちにメンテナンス期間が開始されます。

コマンド	パラメータ	説明
`remove maintenancemodeschedule`		メンテナンスモードの予約設定を取り消します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> remove maintenancemodeschedule` **注意** エージェントがすでにメンテナンスモードになっているか、メンテナンスモードを終了中の場合、予約設定は削除できません。
`show maintenancemode`		メンテナンスモードのステータスを表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> show maintenancemode`
`show maintenancemodeschedule`		メンテナンスモードの予約設定を表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> show maintenancemodeschedule`

重要

メンテナンス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、メンテナンス期間中は、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。
- エージェントは、一度に 1 つの予約されたメンテナンス期間を開始します。新しいメンテナンス期間を設定すると、まだ開始されていない既存のメンテナンスの予約が上書きされます。
- メンテナンスモードを終了しようとしているときにエージェントコンピュータを再起動すると、StellarEnforce 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。
- メンテナンス期間中、エージェントの Patch のアップデートは実行できません。
- メンテナンスモードが有効な場合、StellarEnforce では、メンテナンス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。
- メンテナンス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、StellarEnforce 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。
- メンテナンスモードでは、Windows Visual Studio デバッガはサポートされません。

手動検索のコマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、エージェントの手動検索に関連する処理を実行します。

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

注意

- 手動検索のコマンドを使用するには、別途ライセンスが必要になります。正しいアクティベーションコードがあることを確認してから使用してください。アクティベーションコードの取得方法の詳細については、販売代理店にお問い合わせください。
- エージェントコンポーネントのアップデートでは、StellarEnforce エージェントがプロキシサーバを使用せずにアップデート元に接続できることを確認してください。
- アップデートの完了後、コンポーネントは以前のバージョンにロールバックできません。

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。

表 3-43. 手動検索のコマンド

コマンド	パラメータ	説明
`start scan`	`[-action <action>]`	エージェントで手動検索を実行します `-action` オプションには、異常が検出された場合に実行する処理を指定します 指定可能な処理は次のとおりです。 • 0: 処理は行われません • 1: 駆除します。駆除処理に失敗した場合は削除します • 2: 駆除します。駆除処理に失敗した場合は隔離します。これが初期設定です • 3: 駆除します。駆除処理に失敗した場合は無視します

コマンド	パラメータ	説明

		たとえば、次のように入力します。
		`SLCmd.exe -p <admin_password> start scan -action 1`
		
		注意
		• 手動検索ごとに、StellarEnforce は検索結果を `C:\Program Files\TXOne\StellarEnforce\Scan\log` のログファイル (ファイル名: `ScanResult_YYYYMMDDHHMMSS.log`) に保存します。
		• 管理者権限を使用して次のコマンドを実行すると、隔離ファイルを復元できます。
		`WKSupportTool.exe RestorePrescan <QuarantinedFilePath> <FilePathToRestore>`
		`<QuarantinedFilePath>` には隔離ファイルのファイルパスを、`<FilePathToRestore>` にはファイルを復元するフォルダの場所を指定します。
		隔離ファイルの詳細については、検索ログを参照してください。

`start update`		StellarEnforce エージェントコンポーネント (パターンファイルと検索エンジン) をアップデートします
`set update`	`-source <source>`	コンポーネントアップデートのアップデート元を設定します
`show update`	`-source <source>`	現在のアップデート元を表示します

第 4 章

エージェント設定ファイルの操作

この章では、設定ファイルを使用して TXOne StellarEnforce を設定する方法について説明します。

この章の内容は次のとおりです。

エージェント設定ファイルの操作

設定ファイル管理者は設定ファイルを使用して、複数のコンピュータに同じ設定を適用できます。

詳細については、121 ページの「設定ファイルをエクスポートまたはインポートする」を参照してください。

詳細設定を変更する

一部の設定の変更は、コマンドラインを利用して設定ファイルを介してのみ可能です。詳細については、43 ページの「コマンドラインで SLCmd を使用する」を参照してください。

手順

1. 設定ファイルをエクスポートします。
2. SLcmd を利用し、設定ファイルを復号します。
3. Windows のメモ帳またはその他のテキストエディタで設定ファイルを編集します。

重要

設定ファイルでは UTF-8 エンコードのみがサポートされます。

ヒント

変更した設定のみをインポートして、複数エージェントの共有設定をアップデートできます。

4. SLcmd を利用し、編集した設定ファイルを暗号化します。
5. 編集した設定ファイルをインポートします。

設定ファイルをエクスポートまたはインポートする

注意

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

手順

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

   データベースファイル (.xen) として設定ファイルをエクスポートするには

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

   b. ファイル名を指定して、[保存] をクリックします。

   データベースファイル (.xen) として設定ファイルをインポートするには

   a. [インポート] をクリックして、設定ファイルを指定します。

   b. ファイルを選択して、[開く] をクリックします。

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

設定ファイルの構文

設定ファイルでは、XML 形式を使用して、StellarEnforce で使用するパラメータを指定します。

重要

設定ファイルでは UTF-8 エンコードのみがサポートされます。

設定ファイルの例を次に示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<Configurations  version="1.00.000"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-i
    <Configuration>
        <AccountGroup>
            <Account Id="{24335D7C-1204-43d1-9CBB-332D688C85B6}"
            Enable="no">
                <Password/>
            </Account>
        </AccountGroup>
        <UI>
            <SystemTaskTrayIcon Enable="yes">
                <BlockNotification Enable="no" AlwaysOnTop="yes"
                ShowDetails="ye
                    <Title/>
                    <Message/>
                </BlockNotification>
            </SystemTaskTrayIcon>
        </UI>
        <Feature>
            <ApplicationLockDown LockDownMode="2">
                <TrustList RecentHistoryUnapprovedFilesLimit="50">
                    <ExclusionList/>
                            </TrustList>
                <ScriptLockdown Enable="yes">
                    <Extension Id="bat">
                        <Interpreter>cmd.exe</Interpreter>
                    </Extension>
                    <Extension Id="cmd">
                        <Interpreter>cmd.exe</Interpreter>
                    </Extension>
```

```
                <Extension Id="com">
                    <Interpreter>ntvdm.exe</Interpreter>
                </Extension>
                <Extension Id="dll">
                    <Interpreter>ntvdm.exe</Interpreter>
                </Extension>
                <Extension Id="drv">
                    <Interpreter>ntvdm.exe</Interpreter>
                </Extension>
                <Extension Id="exe">
                    <Interpreter>ntvdm.exe</Interpreter>
                </Extension>
                <Extension Id="js">
                    <Interpreter>cscript.exe</Interpreter>
                    <Interpreter>wscript.exe</Interpreter>
                </Extension>
                <Extension Id="msi">
                    <Interpreter>msiexec.exe</Interpreter>
                </Extension>
                <Extension Id="pif">
                    <Interpreter>ntvdm.exe</Interpreter>
                </Extension>
                <Extension Id="ps1">
                    <Interpreter>powershell.exe</Interpreter>
                </Extension>
                <Extension Id="sys">
                    <Interpreter>ntvdm.exe</Interpreter>
                </Extension>
                <Extension Id="vbe">
                    <Interpreter>cscript.exe</Interpreter>
                    <Interpreter>wscript.exe</Interpreter>
                </Extension>
                <Extension Id="vbs">
                    <Interpreter>cscript.exe</Interpreter>
                    <Interpreter>wscript.exe</Interpreter>
                </Extension>
            </ScriptLockdown>
            <TrustedUpdater>
                <PredefinedTrustedUpdater Enable="no">
                    <RuleSet/>
                </PredefinedTrustedUpdater>
                <WindowsUpdateSupport Enable="no"/>
            </TrustedUpdater>
            <DllDriverLockDown Enable="yes"/>
            <ExceptionPath Enable="no">
                <ExceptionPathList/>
```

```
            </ExceptionPath>
            <TrustedCertification Enable="yes"/>
            <TrustedHash Enable="no"/>
            <WriteProtection Enable="no" ActionMode="1"
            ProtectApprov
            <CustomAction ActionMode="0"/>
            <FilelessAttackPrevention Enable="no">
                <ExceptionList/>
            </FilelessAttackPrevention>
            <IntelligentRuntimeLearning Enable="no"/>
        </ApplicationLockDown>
        <UsbMalwareProtection Enable="no" ActionMode="1"/>
        <DllInjectionPrevention Enable="no" ActionMode="1"/>
        <ApiHookingPrevention Enable="no" ActionMode="1"/>
        <IntegrityMonitoring Enable="no"/>
        <StorageDeviceBlocking Enable="no" ActionMode="1"
        AllowNonMassStorageUSBDevice="no">
            <DeviceException>
                <DeviceGroup name="UserDefined"/>
            </DeviceException>
        </StorageDeviceBlocking>
        <Log>
            <EventLog Enable="yes">
                <Level>
                    <WarningLog Enable="yes"/>
                    <InformationLog Enable="no"/>
                </Level>
                <BlockedAccessLog Enable="yes"/>
                <ApprovedAccessLog Enable="yes">
                    <TrustedUpdaterLog Enable="yes"/>
                    <DllDriverLog Enable="no"/>
                    <ExceptionPathLog Enable="yes"/>
                    <TrustedCertLog Enable="yes"/>
                    <TrustedHashLog Enable="yes"/>
                    <WriteProtectionLog Enable="yes"/>
                </ApprovedAccessLog>
                <SystemEventLog Enable="yes">
                    <ExceptionPathLog Enable="yes"/>
                    <WriteProtectionLog Enable="yes"/>
                </SystemEventLog>
                <ListLog Enable="yes"/>
                <UsbMalwareProtectionLog Enable="yes"/>
                <ExecutionPreventionLog Enable="yes"/>
                <NetworkVirusProtectionLog Enable="yes"/>
                <IntegrityMonitoringLog>
                    <FileCreatedLog Enable="yes"/>
```

```
                        <FileModifiedLog Enable="yes"/>
                        <FileDeletedLog Enable="yes"/>
                        <FileRenamedLog Enable="yes"/>
                        <RegValueModifiedLog Enable="yes"/>
                        <RegValueDeletedLog Enable="yes"/>
                        <RegKeyCreatedLog Enable="yes"/>
                        <RegKeyDeletedLog Enable="yes"/>
                        <RegKeyRenamedLog Enable="yes"/>
                    </IntegrityMonitoringLog>
                    <DeviceControlLog Enable="yes"/>
                </EventLog>
                <DebugLog Enable="yes"/>
            </Log>
        </Feature>
        <ManagedMode Enable="no">
            <Agent>
                <Port/>
                <FixedIp/>
            </Agent>
            <Server>
                <HostName/>
                <FastPort/>
            </Server>
            <Message InitialRetryInterval="120"
            MaxRetryInterval="7680">
            </Message>
            <MessageRandomization TotalGroupNum="1" OwnGroupIndex="0"
            <Proxy Mode="0">
                <HostName/>
                <Port/>
                <UserName/>
                <Password/>
            </Proxy>
            <GroupPolicy>
                <SyncInterval>20</SyncInterval>
            </GroupPolicy>
        </ManagedMode>
    </Configuration>
    <Permission>
        <AccountRef  Id="{24335D7C-1204-43d1-9CBB-332D688C85B6}">
            <UIControl Id="DetailSetting" State="no"/>
            <UIControl Id="LockUnlock" State="yes"/>
            <UIControl Id="LaunchUpdater" State="yes"/>
            <UIControl Id="RecentHistoryUnapprovedFiles" State="yes"/>
            <UIControl Id="ImportExportList" State="yes"/>
            <UIControl Id="ListManagement" State="yes"/>
```

```
                <UIControl Id="SupportToolUninstall" State="no"/>
            </AccountRef>
        </Permission>
    </Configurations>
```

設定ファイルのパラメータ

設定ファイルには、StellarEnforce で使用するパラメータを指定するセクションが含まれています。

表 4-1. 設定ファイルのセクションと説明

セクション			説明	追加情報
Configuration			<Configuration> セクションのコンテナ	
	AccountGroup		制限付きユーザアカウントを設定するパラメータ	128 ページの「<AccountGroup> セクション」を参照してください。 35 ページの「アカウントの種類」を参照してください。
	UI		システムトレイアイコンの表示を設定するパラメータ	129 ページの「<UI> セクション」を参照してください。
	Feature		<Feature> セクションのコンテナ	
		ApplicationLockDown	StellarEnforce の機能を設定するパラメータ	130 ページの「<Feature> セクション」を参照してください。
		UsbMalwareProtection		
		DllInjectionPrevention		
		ApiHookingPrevention		
		MemoryRandomization		

セクション			説明	追加情報
		NetworkVirusProtection		
		IntegrityMonitoring		
		StorageDeviceBlocking	ストレージデバイスによる管理下のエージェントへのアクセスを制御するパラメータ	
		Log	各種のログを設定するパラメータ	145 ページの「<Log> セクション」を参照してください。 179 ページの「エージェントのイベントログの説明」を参照してください。
	ManagedMode		集中管理機能を設定するパラメータ	150 ページの「<ManagedMode> セクション」を参照してください。
Permission			<Permission> セクションのコンテナ	
	AccountRef		制限付きユーザアカウントで使用できる StellarEnforce のメイン画面のコントロールを設定するパラメータ	153 ページの「<AccountRef> セクション」を参照してください。 35 ページの「アカウントの種類」を参照してください。

<AccountGroup> セクション

制限付きユーザアカウントを設定するパラメータ

35 ページの「アカウントの種類」を参照してください。

表 4-2. <AccountGroup> セクションのパラメータ

パラメータ			設定	値	説明
Configuration					<Configuration> セクションのコンテナ
	AccountGroup				<AccountGroup> セクションのコンテナ
		Account	ID	<GUID>	制限付きユーザアカウントの GUID
			Enable	yes	制限付きユーザアカウントを有効にします
				no	制限付きユーザアカウントを無効にします
			Password	<admin_password>	メイン画面にアクセスするための、制限付きユーザアカウントのパスワード **注意** StellarEnforce 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。

<UI> セクション

システムトレイアイコンの表示を設定するパラメータ

表 4-3. <UI> セクションのパラメータ

パラメータ				設定	値	説明
Configuration						<Configuration> セクションのコンテナ
	UI					<UI> セクションのコンテナ
		SystemTaskTrayIcon		Enable	yes	システムトレイアイコンと Windows 通知を表示します
					no	システムトレイアイコンと Windows 通知を非表示にします
			BlockNotification	Enable	yes	エージェントの許可リストに指定されていないファイルをブロックしたときに管理下のエージェントに通知を表示します
					no	エージェントの許可リストに指定されていないファイルをブロックしたときに管理下のエージェントに通知を表示しません
				Authenticate	yes	通知を閉じるときに管理者パスワードの入力を求めるプロンプトを表示します
					no	通知を閉じるときにパスワードは求められません
				ShowDetails	yes	ブロックされたファイルのファイルパスとイベント時間を表示します
					no	イベントの詳細情報を表示しません
				AlwaysOnTop	yes	通知の最前面表示を維持します
					no	他の画面を通知の前面に表示できます

パラメータ				設定	値	説明
				Title	<Title>	通知のタイトルを指定します
				Message	<Message>	通知のメッセージを指定します

<Feature> セクション

StellarEnforce の機能を設定するパラメータ

37 ページの「機能の設定について」を参照してください。

表 4-4. <Feature> セクションのパラメータ

パラメータ				設定	値	説明
Configuration						<Configuration> セクションのコンテナ
	Feature					<Feature> セクションのコンテナ
		ApplicationLockDown		LockDownMode	1	アプリケーション制御を有効にします
					2	アプリケーション制御を無効にします
			IntelligentRuntimeLearning		Enable	Intelligent Runtime Learning (インテリジェントランタイム学習) の使用を有効にします
					Disable	Intelligent Runtime Learning (インテリジェントランタイム学習) の使用を無効にします
			TrustList	RecentHistoryUnapprovedFilesLimit	0 - 65535	ブロックされたファイルのログエントリの最大数

パラメータ	設定	値	説明
ExclusionList			許可リスト初期化時の除外セクションのコンテナ
	Folder	<folder_path>	除外するフォルダパス
	Extension	<file_extension>	除外するファイル拡張子
ScriptLockDown	Enable	yes	スクリプト制御を有効にします
		no	スクリプト制御を無効にします
Extension	ID	<file_extension>	スクリプト制御でブロックするファイル拡張子 たとえば、MSI の値を指定すると .msi ファイルがブロックされます
Interpreter		<file_name>	指定したファイル拡張子のインタープリタ たとえば、msiexec.exe を .msi ファイルのインタープリタとして指定します
TrustedUpdater			<TrustedUpdater> セクションのコンテナ
PredefinedTrustedUpdater	Enable	yes	許可リスト自動更新を有効にします

パラメータ							設定	値	説明
								no	許可リスト自動更新を無効にします
				RuleSet					<RuleSet> 条件のコンテナ
					Condition		ID	<unique_ruleset_name>	ルールセットの一意の名前
						ApprovedListCheck	Enable	yes	許可リスト自動更新を使用して実行されたプログラムのハッシュの確認を有効にします
								no	許可リスト自動更新を使用して実行されたプログラムのハッシュの確認を無効にします
						ParentProcess	Path	<process_path>	許可リスト自動更新のリストに追加する親プロセスのパス
					Exception		Path	<process_path>	許可リスト自動更新のリストから除外するパス
					Rule		Label	<unique_rule_name>	このルールの一意の名前
						Updater	Type	process	指定された EXE ファイルを使用します
								file	指定された MSI または BAT ファイルを使用します

パラメータ	設定	値	説明
		folder	指定されたフォルダの EXE、MSI、または BAT ファイルを使用します
		folderandsub	指定されたフォルダとそのサブフォルダの EXE、MSI、または BAT ファイルを使用します
	Path	<updater_path>	アップデートプログラムのパス
	ConditionRef	<condition_ID>	許可リスト自動更新の詳細なルールを提供するための条件 ID
WindowsUpdateSupport	Enable	yes	ロックダウンされている管理下のエージェントでの Windows Update の実行を許可します
		no	ロックダウンされている管理下のエージェントでの Windows Update をブロックします
DLLDriverLockdown	Enable	yes	DLL/ドライバ制御を有効にします
		no	DLL/ドライバ制御を無効にします
ExceptionPath	Enable	yes	除外パスを有効にします
		no	除外パスを無効にします

パラメータ					設定	値	説明
				ExceptionPathList			除外リストのコンテナ
				ExceptionPath	Path	<exception_path>	除外パス
					Type	file	指定されたファイルのみを使用します
						folder	指定されたフォルダのファイルを使用します
						folderandsub	指定されたフォルダとそのサブフォルダのファイルを使用します
						regexp	正規表現を使用して除外を使用します
			TrustedCertification		Enable	yes	信頼するデジタル証明書の使用を有効にします
						no	信頼するデジタル証明書の使用を無効にします
				PredefinedTrustedCertification	Type	updater	この証明書で署名されたファイルはアップデートプログラムとみなされます
						lockdown	この証明書で署名されたファイルはアップデートプログラムとみなされません
					Hash	<SHA-1_hash_value>	このデジタル証明書の SHA1 ハッシュ値です

パラメータ					設定	値	説明
					Label	<label>	このデジタル証明書の説明です
					Subject	<subject>	このデジタル証明書の発行先です
					Issuer	<issuer>	このデジタル証明書の発行者です
			TrustedHash		Enable	yes	信頼するハッシュリストの使用を有効にします
						no	信頼するハッシュリストの使用を無効にします
				PredefinedTrustedHash	Type	updater	このハッシュ値に一致したファイルはアップデートプログラムとみなされます
						lockdown	このハッシュ値に一致したファイルはアップデートプログラムとみなされません
					Hash	<SHA-1_hash_value>	このファイルの SHA-1 ハッシュ値です
					Label	<label>	このファイルの説明です
					AddToApprovedList	yes	初回アクセス時にこのハッシュ値に一致したファイルを許可リストに追加します
						no	このハッシュ値に一致したファイルを許可リストに追加しません

パラメータ	設定	値	説明
	Path	<file_path>	ファイルパス
	Note	<note>	このハッシュ値に一致したファイルのメモを追加します
WriteProtection	Enable	yes	書き込み制御を有効にします
		no	書き込み制御を無効にします
	ActionMode	0	編集、名前の変更、削除などの処理を許可します
		1	編集、名前の変更、削除などの処理をブロックします
	ProtectApprovedList	yes	書き込み制御が有効な場合に、書き込み制御リストとともに許可リストの保護を有効にします
		no	書き込み制御が有効な場合に、書き込み制御リストとともに許可リストの保護を無効にします
List			書き込み制御リストのコンテナ
File	Path	<file_path>	ファイルパス
Folder	Path	<folder_path>	フォルダパス
	IncludeSubfolder	yes	指定されたフォルダとそのサブフォルダ

パラメータ						設定	値	説明
								のファイルを使用します
							no	指定されたフォルダのファイルを使用します
					RegistryKey	Key	<reg_key>	レジストリキー <reg_key> は、次に示すように省略形を使用することも、省略せずに記述することもできます。 • HKEY_LOCAL_MACH INE\test HKLM\test • HKEY_CURRENT_CO NFIG\test HKCC\test • HKEY_CLASSES_RO OT\test HKCR\test • HKEY_CURRENT_US ER\test HKCU\test • HKEY_USERS\test HKU\test
						IncludeSubkey	yes	サブキーをすべて含めます
							no	サブキーを含めません
					RegistryValue	Key	<reg_key>	レジストリキー <reg_key> は、次に示すように省略形を使用することも、省略せずに記述することもできます。

パラメータ						設定	値	説明
								• HKEY_LOCAL_MACH INE\test HKLM\test • HKEY_CURRENT_CO NFIG\test HKCC\test • HKEY_CLASSES_RO OT\test HKCR\test • HKEY_CURRENT_US ER\test HKCU\test • HKEY_USERS\test HKU\test
						Name	<reg_value_name>	レジストリ値の名前
				ExceptionList				書き込み制御の除外リストのコンテナ
					Process	Path	<process_path>	プロセスのパス
					File	Path	<file_path>	ファイルパス
					Folder	Path	<folder_path>	フォルダパス
						IncludeSubfolder	yes	指定されたフォルダとそのサブフォルダのファイルを使用します
							no	指定されたフォルダのファイルを使用します

パラメータ						設定	値	説明
					RegistryKey	Key	<reg_key>	レジストリキー <reg_key> は、次に示すように省略形を使用することも、省略せずに記述することもできます。 • HKEY_LOCAL_MACH INE\test HKLM\test • HKEY_CURRENT_CO NFIG\test HKCC\test • HKEY_CLASSES_RO OT\test HKCR\test • HKEY_CURRENT_US ER\test HKCU\test • HKEY_USERS\test HKU\test
						IncludeSubkey	yes	サブキーをすべて含めます
							no	サブキーを含めません
					RegistryValue	Key	<reg_key>	レジストリキー <reg_key> は、次に示すように省略形を使用することも、省略せずに記述することもできます。 • HKEY_LOCAL_MACH INE\test HKLM\test • HKEY_CURRENT_CO NFIG\test HKCC\test

パラメータ	設定	値	説明
			• HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test • HKEY_USERS\test HKU\test
	Name	<reg_value_name>	レジストリ値の名前
CustomAction	ActionMode	0	アプリケーション制御で次のいずれかのイベントがブロックされた場合に、ブロックされたファイルまたはプロセスを無視します • プロセスの起動 • DLL の読み込み • スクリプトファイルのアクセス
		1	アプリケーション制御で次のいずれかのイベントがブロックされた場合に、ブロックされたファイルまたはプロセスを隔離します • プロセスの起動 • DLL の読み込み • スクリプトファイルのアクセス
		2	アプリケーション制御で次のいずれかのイベントがブロック

パラメータ	設定	値	説明
			された場合に、ブロックされたファイルまたはプロセスに対する処理を確認します • プロセスの起動 • DLL の読み込み • スクリプトファイルのアクセス
UsbMalwareProtection	Enable	yes	USB 不正プログラム対策を有効にします
		no	USB 不正プログラム対策を無効にします
	ActionMode	0	検出された不正プログラムによって処理を許可します
		1	検出された不正プログラムによって処理をブロックします
DllInjectionPrevention	Enable	yes	DLL インジェクション対策を有効にします
		no	DLL インジェクション対策を無効にします
	ActionMode	0	DLL インジェクションを許可します
		1	DLL インジェクションをブロックします
ApiHookingPrevention	Enable	yes	API フッキング対策を有効にします
		no	API フッキング対策を無効にします
	ActionMode	0	API フッキングを許可します

パラメータ	設定	値	説明
		1	API フッキングをブロックします
MemoryRandomization	Enable	yes	メモリのランダム化を有効にします
		no	メモリのランダム化を無効にします
NetworkVirusProtection	Enable	yes	ネットワークウイルス対策を有効にします
		no	ネットワークウイルス対策を無効にします
	ActionMode	0	検出されたネットワークウイルスによって処理を許可します
		1	検出されたネットワークウイルスによって処理をブロックします
IntegrityMonitoring	Enable	yes	変更監視を有効にします
		no	変更監視を無効にします
StorageDeviceBlocking	Enable	yes	管理下のエージェントへのストレージデバイス (CD/DVD ドライブ、フロッピーディスクおよび USB デバイス) によるアクセスをブロックします
	Disable	no	管理下のエージェントへのストレージデ

パラメータ				設定	値	説明
						バイス (CD/DVD ドライブ、フロッピーディスクおよび USB デバイス) によるアクセスを許可します
				ActionMode	0	編集、名前の変更、削除などの処理を許可します
					1	編集、名前の変更、削除などの処理をブロックします
				AllowNonMassStorageUSBDevice	yes	タッチスクリーン/赤外線センサ/Android スマホなどのハードウェアデバイスが接続され、ストレージデバイスのブロックが有効な場合に、対象ドライバのロードを許可します。
					no	タッチスクリーン/赤外線センサ/Android スマホなどのハードウェアデバイスが接続され、ストレージデバイスのブロックが有効な場合に、対象ドライバのロードをブロックします。
			DeviceException			ストレージデバイスのブロックのデバイス除外リストのコンテナ
				DeviceGroup		ストレージデバイスのブロックのデバイスリストのコンテナ

パラメータ				設定	値	説明
				name		デバイスリストの一意の名前
			Device	vid		デバイスのベンダ ID
				pid		デバイスの製品 ID
				sn		デバイスのシリアル番号
		Log				ログ設定のコンテナ 145 ページの「<Log> セクション」を参照してください。
	FilelessAttackPrevention			Enable	yes	ファイルレス攻撃対策を有効にします
					no	ファイルレス攻撃対策を無効にします
		ExceptionList				ファイルレス攻撃対策の除外リストのコンテナ
			Exception	Target	<monitored process>	powershell.exe、wscript.exe、CScript.exe、または mshta.exe を指定します
				Label	<label>	この除外の一意の名前
			Arguments		<arguments>	許可される引数
				Regex	yes	引数に正規表現が含まれる場合は yes を指定します
					no	引数に正規表現が含まれない場合は no を指定します

パラメータ	設定	値	説明
Parent1		<parent process>	監視対象プロセスの親プロセス
Parent2		<grandparent process>	監視対象プロセスの祖父母プロセス
Parent3		<greatgrandparent process>	監視対象プロセスの曾祖父母プロセス
Parent4		<greatgreatgrandparent process>	監視対象プロセスの高祖父母プロセス

<Log> セクション

各種のログを設定するパラメータ

179 ページの「エージェントのイベントログの説明」を参照してください。

表 4-5. ログ設定のパラメータ

パラメータ	設定	値	説明
Configuration			<Configuration> セクションのコンテナ
Feature			<Feature> セクションのコンテナ
Log			ログ設定のコンテナ
EventLog	Enable	yes	次の要素に指定された StellarEnforce イベントをログに記録します

パラメータ	設定	値	説明
		no	次の要素に指定された StellarEnforce イベントをログに記録しません
Level			ログレベル設定のコンテナ
WarningLog	Enable	yes	警告レベルのイベントをログに記録します
		no	警告レベルのイベントをログに記録しません
InformationLog	Enable	yes	情報レベルのイベントをログに記録します
		no	情報レベルのイベントをログに記録しません
BlockedAccessLog	Enable	yes	StellarEnforce でブロックされたファイルをログに記録します
		no	StellarEnforce でブロックされたファイルをログに記録しません
ApprovedAccessLog	Enable	yes	StellarEnforce で許可されたファイルをログに記録します
		no	StellarEnforce で許可されたファイルをログに記録しません
TrustedUpdaterLog	Enable	yes	許可リスト自動更新で許可されたアクセスのログを有効にします
		no	許可リスト自動更新で許可されたアクセスのログを無効にします
DLLDriverLog	Enable	yes	DLL/ドライバの許可されたアクセスのログを有効にします
		no	DLL/ドライバの許可されたアクセスのログを無効にします
ExceptionPathLog	Enable	yes	アプリケーション制御除外パスの許可されたアクセスのログを有効にします

パラメータ		設定	値	説明
			no	アプリケーション制御除外パスの許可されたアクセスのログを無効にします
	TrustedCertLog	Enable	yes	信頼するデジタル証明書の許可されたアクセスのログを有効にします
			no	信頼するデジタル証明書の許可されたアクセスのログを無効にします
	WriteProtectionLog	Enable	yes	書き込み制御の許可されたアクセスのログを有効にします
			no	書き込み制御の許可されたアクセスのログを無効にします
SystemEventLog		Enable	yes	システムに関連するイベントをログに記録します
			no	システムに関連するイベントをログに記録しません
	ExceptionPathLog	Enable	yes	アプリケーション制御からの除外を有効にします
			no	アプリケーション制御からの除外を無効にします
	WriteProtectionLog	Enable	yes	書き込み制御のシステムログを有効にします
			no	書き込み制御のシステムログを無効にします
ListLog		Enable	yes	許可リストに関連するイベントをログに記録します
			no	許可リストに関連するイベントをログに記録しません
USBMalwareProtectionLog		Enable	yes	USB 不正プログラム対策を作動させるイベントをログに記録します

パラメータ	設定	値	説明
		no	USB 不正プログラム対策を作動させるイベントをログに記録しません
ExecutionPreventionLog	Enable	yes	実行防止対策を作動させるイベントをログに記録します
		no	実行防止対策を作動させるイベントをログに記録しません
NetworkVirusProtectionLog	Enable	yes	ネットワークウイルス対策を作動させるイベントをログに記録します
		no	ネットワークウイルス対策を作動させるイベントをログに記録しません
IntegrityMonitoringLog			変更監視ログの設定のコンテナ
FileCreatedLog	Enable	yes	ファイルおよびフォルダ作成イベントをログに記録します
		no	ファイルおよびフォルダ作成イベントをログに記録しません
FileModifiedLog	Enable	yes	ファイル変更イベントをログに記録します
		no	ファイル変更イベントをログに記録しません
FileDeletedLog	Enable	yes	ファイルおよびフォルダ削除イベントをログに記録します
		no	ファイルおよびフォルダ削除イベントをログに記録しません
FileRenamedLog	Enable	yes	ファイルおよびフォルダ名変更イベントをログに記録します
		no	ファイルおよびフォルダ名変更イベントをログに記録しません

パラメータ						設定	値	説明
					RegValueModifiedLog	Enable	yes	レジストリ値変更イベントをログに記録します
							no	レジストリ値変更イベントをログに記録しません
					RegValueDeletedLog	Enable	yes	レジストリ値削除イベントをログに記録します
							no	レジストリ値削除イベントをログに記録しません
					RegKeyCreatedLog	Enable	yes	レジストリキー作成イベントをログに記録します
							no	レジストリキー作成イベントをログに記録しません
					RegKeyDeletedLog	Enable	yes	レジストリキー削除イベントをログに記録します
							no	レジストリキー削除イベントをログに記録しません
					RegKeyRenamedLog	Enable	yes	レジストリキー名変更イベントをログに記録します
							no	レジストリキー名変更イベントをログに記録しません
				DeviceControlLog		Enable	yes	ストレージデバイスコントロールイベントをログに記録します
							no	ストレージデバイスコントロールイベントをログに記録しません
				DebugLog		Enable	yes	デバッグ情報をログに記録します
							no	デバッグ情報をログに記録しません

<ManagedMode> セクション

集中管理機能を設定するパラメータ

表 4-6. <ManagedMode> セクションのパラメータ

パラメータ	設定	値	説明
Configuration			<Configuration> セクションのコンテナ
GroupPolicy			グループポリシーを StellarOne に設定するためのコンテナです
SyncInterval		0 ～ 2147483647 単位: 分	この同期期間に従ってエージェント情報が定期的にアップデートされます
Agent			StellarEnforce エージェントの設定のコンテナ
Port		<server_messages_port>	サーバ通信用のセキュアポート番号を指定します (従来の呼称はエージェントの待機ポート)
FixedIp		• A.B.C.D/E • A,B,C,D: 0~255 • E: 1~32	StellarEnforce サーバと通信するエージェントの IP アドレス (CIDR (Classless Inter-Domain Routing) 形式) を指定します
Server			StellarOne の設定のコンテナ
HostName		<hostname>	StellarOne のホスト名を指定します

パラメータ				設定	値	説明
			FastPort		<logs_port>	ログとステータスを収集するためのセキュアポート番号を指定します (従来の呼称は高速接続)
		Message				StellarOne 宛自動送信メッセージの設定のコンテナ
			InitialRetryInterval		0 ～ 2147483647 単位: 秒	StellarOne にイベントの再送信を試行する間隔 (秒) の初期設定値です この間隔は、MaxRetryInterval 値に達するまで、試行が失敗するたびに倍増します
			MaxRetryInterval		0 ～ 2147483647 単位: 秒	StellarOne にイベントの再送信を試行する間隔の最大値です
			RegularStatusUpdate		0 1	0: この同期期間中、エージェント情報は定期的にアップデートされません 1: この同期期間中、エージェント情報は定期的にアップデートされます

パラメータ	設定	値	説明
MessageRandomization **注意** StellarEnforce エージェントは、可能なかぎり速やかに StellarEnforce 管理コンソールからの要求に応答します。詳細については、Trend Micro StellarEnforce 管理者ガイドの「メッセージタイムグループを適用する」を参照してください。			
	TotalGroupNum	正の整数 (>= 1)	メッセージタイムグループの合計数を指定します
	OwnGroupIndex	ゼロまたは正の整数、< TotalGroupNum	この StellarEnforce エージェントのメッセージタイムグループ ID 番号を指定します
	TimePeriod	ゼロまたは正の整数	このメッセージタイムグループのメッセージ送信サイクルがアクティブな場合に、このグループの ID 番号で StellarOne に自動送信メッセージを送信する時間を秒単位で指定します **注意** メッセージタイムグループは、この時間がゼロ (0) に設定されている場合はアクティブになりません。

パラメータ				設定	値	説明
		Proxy		Mode	0	プロキシを使用しません (直接アクセス)
					1	プロキシを使用します (手動設定)
					2	プロキシ設定を Internet Explorer と同期します
			HostName		<proxy_hostname>	プロキシホスト名を指定します
			Port		<proxy_port>	プロキシポート番号を指定します
			UserName		<proxy_user_name>	プロキシユーザ名を指定します
			Password		<proxy_password>	プロキシパスワードを指定します

<AccountRef> セクション

制限付きユーザアカウントで使用できる StellarEnforce のメイン画面のコントロールを設定するパラメータ

35 ページの「アカウントの種類」を参照してください。

表 4-7. <AccountRef> セクションのパラメータ

パラメータ			設定	値	説明
Configuration					<Configuration> セクションのコンテナ
	Permission				<Permission> セクションのコンテナ
		AccountRef			<AccountRef> セクションのコンテナ
			UIControl	ID	DetailSetting	StellarEnforce のメイン画面の [設定] ページの機能にアクセスします

パラメータ	設定	値	説明
			注意 制限付きユーザのアカウントでは [パスワード(P)] ページは使用できません。
		LockUnlock	[概要] 画面のアプリケーション制御の設定にアクセスします
		LaunchUpdater	制限付きユーザが [許可リスト] 画面の [アプリの追加] をクリックした場合の、[選択したアプリケーションインストーラによって作成または修正されたファイルを自動的に追加する] オプションにアクセスします。
		RecentHistoryUnapprovedFIles	制限付きユーザが [概要] 画面の [前回のアプリケーションブロック日時] をクリックした場合の、ブロックログにアクセスします
		ImportExportList	[リストのインポート] ボタンと [リストのエクスポート] ボタンにアクセスします
		ListManagement	[許可リスト] 画面の次の項目にアクセスします • [アプリの削除] ボタン • [ハッシュを更新] ボタン • [アプリの追加] > [既存ファイルとフォルダの追加] メニュー
	State	yes	ID で指定された権限を有効にします
		no	ID で指定された権限を無効にします

第 5 章

トラブルシューティング

この章では、TXOne StellarEnforce に関するトラブルシューティングの方法とよくある質問について説明します。

この章の内容は次のとおりです。

よくある質問 (FAQ)

エージェントがウイルスに感染した場合の対処方法

次のいずれかを実行して、エージェントからウイルスを削除します。

- エージェントで手動検索を実行します。

  詳細については、117ページの「手動検索のコマンド」を参照してください。

- TXOne StellarEnforce 管理コンソールにアクセスし、検索コマンドを送信して、エージェントの不正プログラム検索を実行します。

TXOne StellarEnforce に関する詳細情報の入手先

最新情報およびサポート情報については、次のトレンドマイクロのサポート

Web サイトで入手できます。

https://success.trendmicro.com/jp/technical-support

StellarEnforce のトラブルシューティング

TXOne StellarEnforce サポートツールを使用して、次のような診断機能を実行できます。

- デバッグログの作成、収集、削除
- セルフプロテクション機能の有効化または無効化

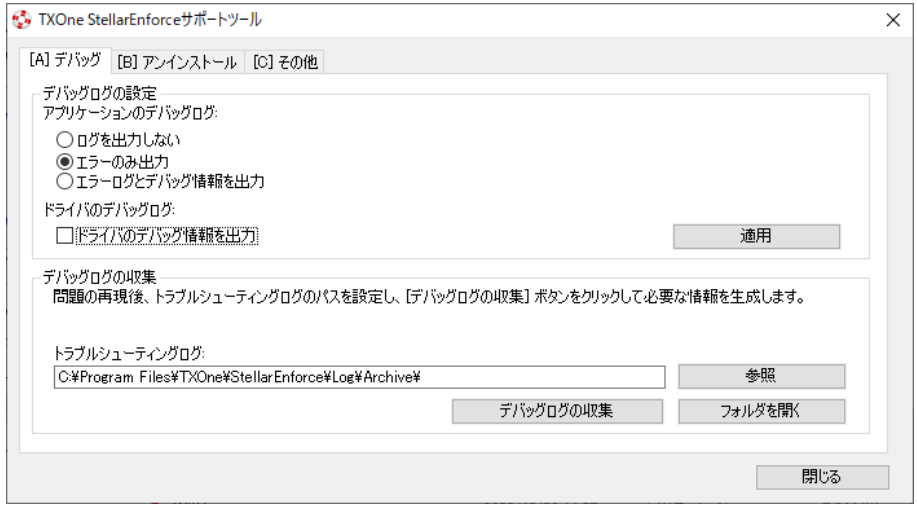


図 5-1.　TXOne StellarEnforce サポートツールの [デバッグ] タブ

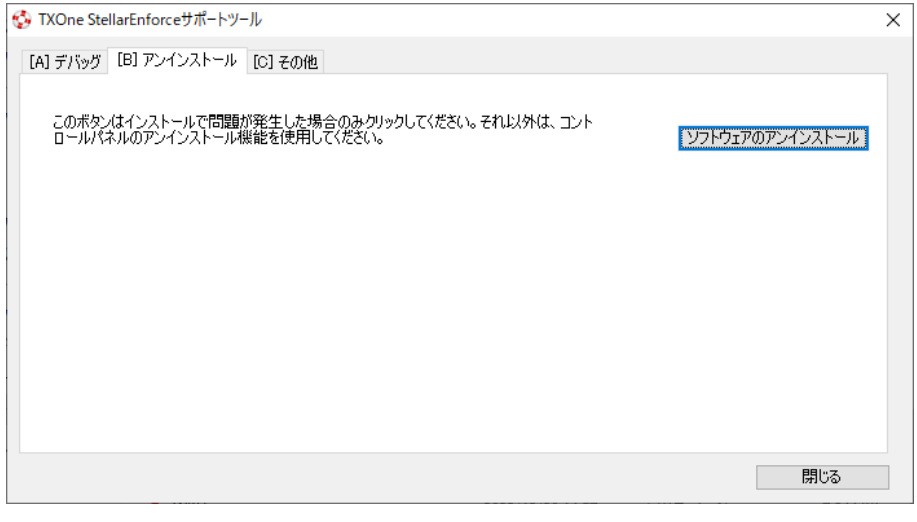


図 5-2.　TXOne StellarEnforce サポートツールの [アンインストール] タブ

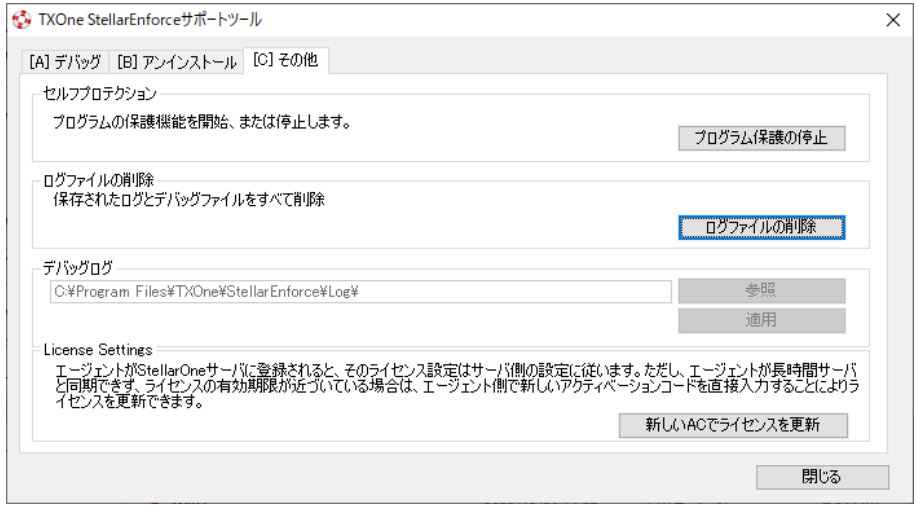


図 5-3.　TXOne StellarEnforce サポートツールの [その他] タブ

サポートツールの使用

TXOne StellarEnforce で問題が発生した場合は、アプリケーションとドライバのデバッグログを分析用に生成して、トレンドマイクロのテクニカルサポートに送信します。StellarEnforce の管理者アカウントと制限付きユーザアカウントの両方がこのログを収集できます。

手順

1. サポートツールを開いてデバッグログ機能を有効にします。

   a. TXOne StellarEnforce インストールフォルダを開いて `WKSupportTool.exe` を実行します。

> **注意**
>
> 初期設定のインストール場所は `c:\Program Files\TXOne \StellarEnforce\` です。

b. StellarEnforce の管理者または制限付きユーザのパスワードを入力し、[OK] をクリックします。

c. [[A] デバッグ] タブで [エラーログとデバッグ情報を出力] と [ドライバのデバッグログ情報を出力] を選択して、[適用] をクリックします。

2. 問題を再現します。

3. デバッグログを収集します。

a. サポートツールをもう一度開きます。

b. [[A] デバッグ] タブで [参照] をクリックして、TXOne StellarEnforce のログの保存場所を選択します。

注意

保存済みログの初期設定の場所は `c:\Program Files\TXOne \StellarEnforce\Log\Archive\` です。

c. 完了したら [閉じる] をクリックします。

d. [デバッグログの収集] をクリックします。

e. デバッグログが収集されたら、[フォルダを開く] をクリックして圧縮されたログファイルにアクセスし、内容を確認するか、トレンドマイクロのテクニカルサポートにメールで送信してください。

サポートツールのコマンド

次の表は、サポートツール WKSupportTool.exe を使用して利用できるコマンドを一覧表示しています。

注意

サポートツールのコマンドを使用できるのは StellarEnforce の管理者のみです。WKSupportTool.exe では、コマンドを実行する前に管理者のパスワードを求めるプロンプトが表示されます。

表 5-1. サポートツールのコマンド

コマンド	説明
-p <パスワード>	コマンドを実行できるようにユーザを認証します。
debug [on|off] [verbose|normal] [-drv on] [-drv off]	デバッグログをオンまたはオフにし、ログの詳細レベル、およびドライバログを含めるかどうかを指定します。
collect [path]	デバッグ情報を収集し、指定されたパスに zip ファイルを作成します。パスが指定されていない場合、初期設定のログの場所 <インストールディレクトリ>\Log\Archive が使用されます。
selfprotection [on|off]	StellarEnforce セルフプロテクションをオンまたはオフにします。
deletelogs	StellarEnforce のすべてのログを削除します。
uninstall	TXOne StellarEnforce をアンインストールします。
changelogpath [path]	デバッグログの出力フォルダを変更します。
EncryptSetupIni Setup.ini Setup.bin	Setup.ini ファイルを暗号化します。

StellarEnforce のデバッグログを収集する

失敗したインストールのデバッグログを収集する

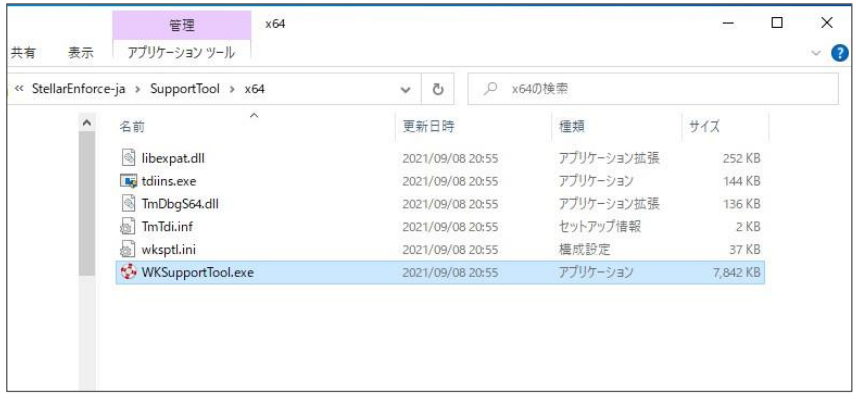
手順

1. `setup.ini` を次のように調整します。

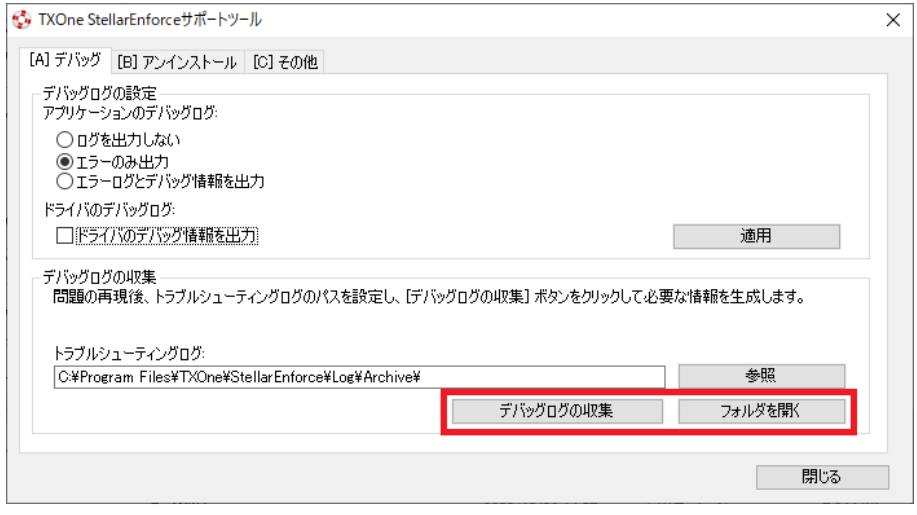
2. インストーラ `SL_Install.exe` を起動して、問題を再現します。
3. インストーラパッケージに含まれる `WKSupportTool` を実行します。

注意

- x86 プラットフォームの場合、`install_package\Supporttool\x86` にあるツールを使用してください。
- x64 プラットフォームの場合、`install_package\Supporttool\x64` にあるツールを使用してください。



4. [デバッグログの収集] をクリックします。
5. [フォルダを開く] をクリックして、圧縮された zip ファイルを取得します。

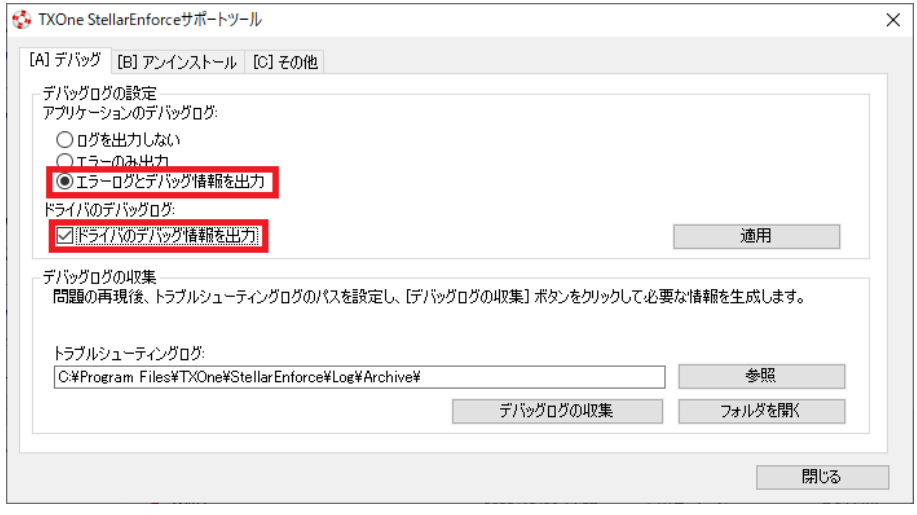


インストール後にデバッグログを収集する

StellarEnforce のインストール後に異常な動作または問題が見つかった場合は、次の手順を使用して、StellarEnforce と Microsoft Windows の Process Monitor の両方からログを収集してください。

手順

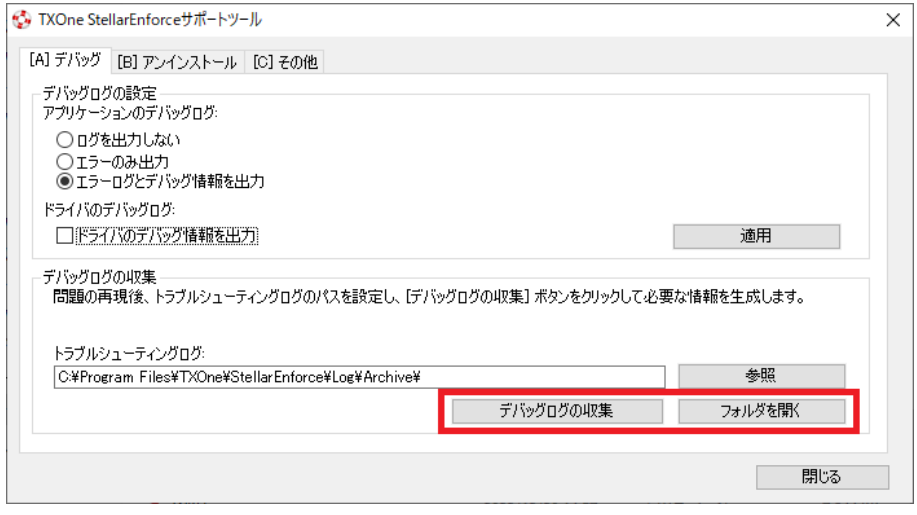
1. `WKSupportTool` でデバッグ情報を有効にします。



2. Process Monitor を起動してシステムを監視します。
3. 問題を再現します。
4. Process Monitor のログ (PML) を保存します。

> **重要**
>
> フィルタリングされていないすべてのイベントが必要です。PML を表示用に使用する場合はフィルタリングを使用できますが、トレンドマイクロに送付するログにはフィルタリングは使用しないでください。

5. `WKSupportTool` で [デバッグログの収集] をクリックして、ログを収集します。
6. [フォルダを開く] をクリックして、圧縮された zip ファイルを取得します。
7. 分析のために両方のログファイルをトレンドマイクロに送付してください。その際、ログの中で問題を再現した時刻および関連するアプリケーションの名前を明記してください。



パフォーマンスの問題のデバッグログを収集する

パフォーマンスの問題が発生した場合は、次のログを提供してください。

1. StellarEnforce のパフォーマンスレポート
2. Windows パフォーマンス レコーダー
3. トレンドマイクロパフォーマンス調整ツール (挙動監視に含まれる)

StellarEnforce でパフォーマンスレポートを生成する

手順

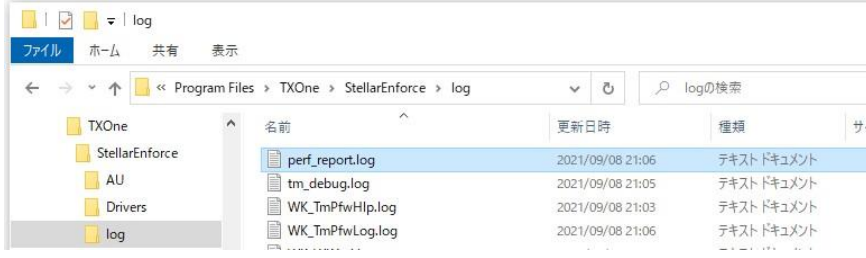
1. StellarEnforce サービスを停止します。(`Slcmd.exe stop service`)
2. 次に示すレジストリ値を作成します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\SafeLock\2\DebugLog
```

```
"EnableProfiling"=dword:00000001
```

3. StellarEnforce サービスを開始します。(`Slcmd.exe start service`)

4. 問題に関連したタスクをいくつか実行します。
5. StellarEnforce サービスを停止します。(`Slcmd.exe stop service`)
6. `<wk_installed_folder>\log` で `perf_report.log` ファイルを探します。



注意

このレポートを生成するためにデバッグログを有効にする必要はありません。実際、パフォーマンスの測定中はデバッグログを無効にするように推奨されます。

Windows パフォーマンス レコーダーを設定してログを生成する

- マイクロソフトは、Windows 上のすべてのアクティビティを記録するために、Windows パフォーマンス レコーダー (WPR) というツールを提供しています。
- このツールを含む Windows パフォーマンス ツールキットは、Windows アセスメント&デプロイメント キットに含まれています。
- 64 ビット OS を実行している場合は、次のレジストリ設定を追加してから再起動します。

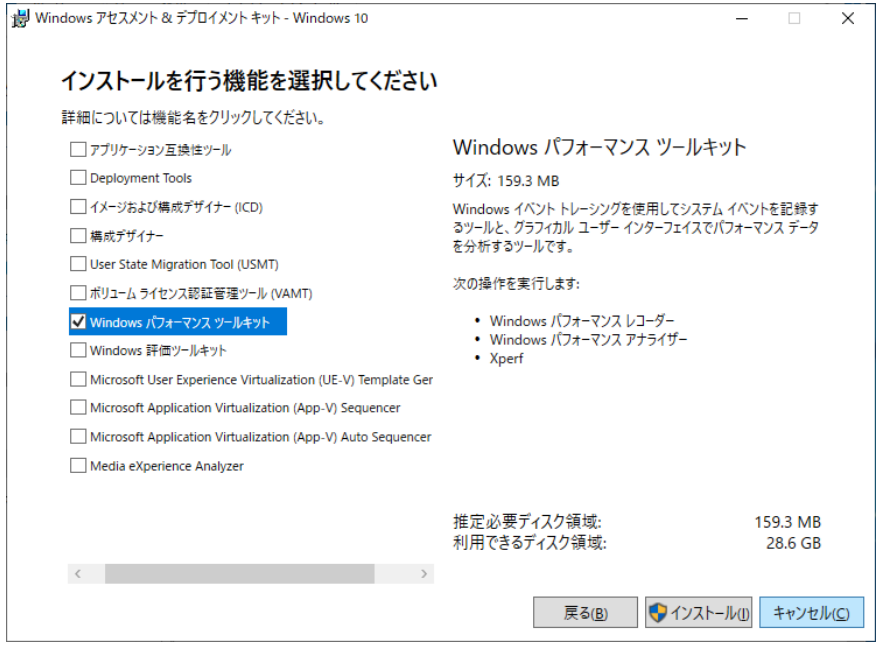
```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\Memory
```

```
"DisablePagingExecutive"=DWORD:1
```

Windows パフォーマンス レコーダーを設定する: Windows 8 以降

手順

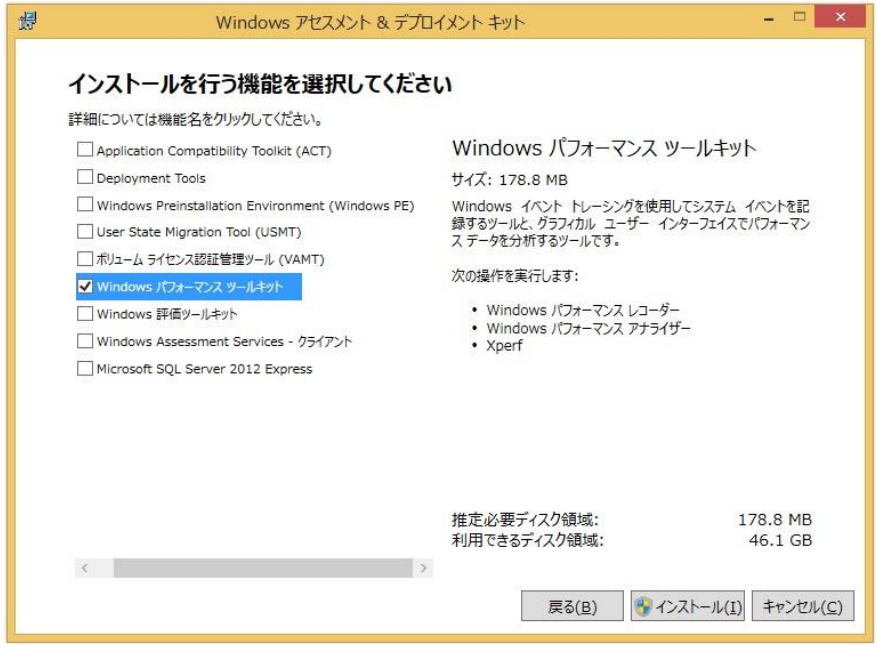
1. Windows ADK for Windows 10 をダウンロードします。
2. インストール時は [Windows パフォーマンス ツールキット] のみを選択します。



Windows パフォーマンス レコーダーを設定する: Windows 7 および 2008 R2

手順

1. Windows ADK for Windows 8 をダウンロードします。
2. インストール時は [Windows パフォーマンス ツールキット] のみを選択します。



Windows パフォーマンス レコーダーを設定する: Windows Vista、Windows 2008、Windows 2003 SP1、および Windows XP SP2

手順

1. Windows パフォーマンス ツールキット 4.x を使用します。Windows パフォーマンス ツールキット 4.x の使用ガイドラインを参照してください。

Windows パフォーマンス レコーダーでログを生成する

手順

1. [スタート] メニューから [Windows パフォーマンス レコーダー] を起動します。
2. [その他のオプション] の下で次の項目を選択します。
   - [CPU使用率]
   - [ディスクI/O処理]
   - [ファイルI/O処理]
   - [レジストリI/O処理]
   - [ネットワークI/O処理]
   - [ヒープ使用量]
   - [プール使用量]
3. [ログ モード] を [ファイル] に変更します。
4. [開始] をクリックします。
5. 再現する問題に関連したアプリケーションまたはタスクを実行します。
6. 問題が再現されたら、[保存] をクリックします。
7. [参照] をクリックしてログの保存先を指定し、[保存] をクリックします。
8. [フォルダを開く] をクリックして ETL ファイルにアクセスし、圧縮してトレンドマイクロに送付してください。

第 6 章

製品サポート情報

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

ここでは、次の項目について説明します。

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

https://success.trendmicro.com/jp/technical-support

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2 つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/をご覧ください。

- 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- Web 攻撃およびオンラインのトレンド情報
- 不正プログラムの週次レポート

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている

「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話またはお問い合わせ Web フォームをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポートサービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービス継続を希望される場合は契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意

サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

トレンドマイクロへのウイルス解析依頼

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

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

https://success.trendmicro.com/jp/virus-and-threat-help

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

メールレピュテーションについて

スパムメールやフィッシングメールなどの送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

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

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

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

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

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

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

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

注意

サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

脅威解析・サポートセンターTrendLabs (トレンドラボ)

TrendLabs (トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 か所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

第 7 章

付録: 参照

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

この章の内容は次のとおりです。

ローカル管理者アカウントを有効にする

Windows NT 6.x (Windows Vista、Windows 7、Windows 8、Windows 8.1、Windows Server 2008、Windows Server 2012) および Windows NT 10.x (Windows 10、Windows Server 2016) では、ローカル Windows 管理者アカウントを使用できるようにするための特別な手順が必要です。

手順

1. [コンピュータの管理] を開きます。
   a. [スタート] メニューを開きます。
   b. [コンピュータ] を右クリックします。
   c. [管理] を選択します。

      [コンピュータの管理] 画面が表示されます。
2. 左側のリストで、[コンピュータの管理] > [システム ツール] > [ローカルユーザーとグループ] > [ユーザー] の順に選択します。

   ローカル Windows ユーザアカウントのリストが表示されます。
3. ユーザアカウントのリストで [Administrator] を右クリックし、[プロパティ] を選択します。

   [Administrator のプロパティ] 画面が表示されます。
4. [全般] タブで、[アカウントを無効にする] をオフにします。
5. [OK] をクリックします。

   [コンピュータの管理] 画面が再び表示され、ローカル Windows ユーザアカウントのリストが表示されます。
6. [Administrator] を右クリックして、[パスワードの設定...] を選択します。

   パスワード設定の手順を示すメッセージが表示されます。
7. パスワードを設定します。
8. [コンピュータの管理] を終了します。

ローカルアカウントの初期設定の共有を有効にする

Windows NT Version 6.x、Windows Vista、Windows 7、Windows 8、Windows 8.1、Windows 10、Windows Server 2008、および Windows Server 2012 では、ローカル Windows 管理者アカウントを使用して初期設定の共有 (初期設定の共有された admin$など) にアクセスできるようにするための特別な手順が必要です。

ヒント

手順は Windows のバージョンによって異なります。お使いの Windows のバージョンに合わせた手順およびヘルプが必要な場合は、https:// msdn.microsoft.com/ja-jp/default.aspx でマイクロソフトのサポート技術情報を参照してください。

手順

1. [レジストリ エディター] (regedit.exe) を開きます。
   a. [スタート] > [ファイル名を指定して実行] の順に選択します。
   b. 「regedit」と入力して <Enter> キーを押します。
2. 次のレジストリサブキーを探してクリックします。

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
3. レジストリエントリ LocalAccountTokenFilterPolicy を探します。このレジストリエントリがない場合は、次の手順を実行します。
   a. [編集] > [新規] の順に選択します。
   b. [DWORD 値] を選択します。
   c. 「LocalAccountTokenFilterPolicy」と入力して <Enter> キーを押します。
4. LocalAccountTokenFilterPolicy を右クリックして、[修正] を選択します。
5. [値のデータ] に「1」と入力します。
6. [OK] をクリックします。
7. [レジストリ エディター] を終了します。

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できます。

- エージェントコンピュータでデバイスマネージャを開きます。
- エージェントコンピュータで `SLCmd.exe show USBinfo` コマンドを使用します。詳細については、96 ページの「信頼する USB デバイスのコマンド」を参照してください。
- メイン画面で [エージェントイベント] 画面に移動し、イベント ID5001 のリムーバルデバイスの [詳細情報の表示] をクリックします。

エージェントのイベントログの説明

TXOne StellarEnforce では、StellarEnforce イベントログを表示するために Windows イベントビューアを使用します。イベントビューアにアクセスするには、[スタート] > [コントロール パネル] > [管理ツール] > [イベントビューア] の順にクリックします。

ヒント

イベントログへの出力内容は、setup.ini もしくは設定ファイルにて変更することができます。

詳しくは 120 ページの「エージェント設定ファイルの操作」を参照してください

表 7-1. Windows イベントログの説明

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。

イベント ID	タスクカテゴリ	レベル	ログの説明
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。

イベントID	タスクカテゴリ	レベル	ログの説明
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%
1042	システム	情報	スクリプトが削除されました。 [詳細] 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%

イベントID	タスクカテゴリ	レベル	ログの説明
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%
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%

イベントID	タスクカテゴリ	レベル	ログの説明
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%
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%

イベントID	タスクカテゴリ	レベル	ログの説明
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	実行する処理を管理コンソールで確認するようにカスタム処理が設定されました。
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。
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	エージェントに Patch が適用されました。 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:

イベント ID	タスクカテゴリ	レベル	ログの説明
			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% 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。

イベントID	タスクカテゴリ	レベル	ログの説明
1113	システム	警告	Intelligent Runtime Learning (インテリジェントランタイム学習) を有効にします。
1114	システム	警告	Intelligent Runtime Learning (インテリジェントランタイム学習) を無効にします。
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%
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: %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%

イベントID	タスクカテゴリ	レベル	ログの説明
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: %exceptionpathtype% 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: %exceptionpathtype% 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

イベントID	タスクカテゴリ	レベル	ログの説明
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%
1523	システム	情報	メンテナンスモードを開始しました
1524	システム	情報	メンテナンスモードを終了しています
1525	システム	情報	メンテナンスモードを終了しました
1526	リスト	情報	メンテナンスモードで許可リストに追加されました。 パス: %1 ハッシュ: %2

イベントID	タスクカテゴリ	レベル	ログの説明
1527	リスト	情報	メンテナンスモードで許可リストがアップデートされました。 パス: %1 ハッシュ: %2
1528	システム	情報	メンテナンスモードの概要 許可リストに追加されたファイル数: %1 許可リストに追加できなかったファイル数: %2 検出時の処理: %3 処理が実行されたファイル数: %4 処理を実行できなかったファイル数: %5
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: %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: %username% モード: %mode% ファイルハッシュが許可されました: %hash%

イベントID	タスクカテゴリ	レベル	ログの説明
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: %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: %username% モード: %mode%
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: %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
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: %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: %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: %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: %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: %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: %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: %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: %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
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: %username% モード: %mode%
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: %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: %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: %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%

イベントID	タスクカテゴリ	レベル	ログの説明
			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: %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: %username% モード: %mode%
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: %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%

イベントID	タスクカテゴリ	レベル	ログの説明
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: %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: %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%

イベント ID	タスクカテゴリ	レベル	ログの説明
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: %username% モード: %mode%
2512	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: %username% **注意** 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。
2513	ブロックされたアクセス	警告	ファイルレス攻撃対策によりプロセスがブロックされました: %path% %argument% [詳細] アクセスユーザ: %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有効の状態 理由: %reason%

イベント ID	タスクカテゴリ	レベル	ログの説明
2514	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: %BLOCKED_FILE_PATH% [詳細] パス: %PARENT_PROCESS_PATH% アクセスユーザ: %USER_NAME% 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。
3000	USB 不正プログラム対策	警告	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: %username% デバイスタイプ: %type%
3001	USB 不正プログラム対策	警告	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: %username% デバイスタイプ: %type%
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

イベント ID	タスクカテゴリ	レベル	ログの説明
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%

イベント ID	タスクカテゴリ	レベル	ログの説明
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%
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%

イベント ID	タスクカテゴリ	レベル	ログの説明
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%
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: %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: %username%

イベントID	タスクカテゴリ	レベル	ログの説明
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: %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: %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: %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: %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	%Result% [詳細] アップデート元: %SERVER% [元のバージョン] 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% [最新バージョン] 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%

イベントID	タスクカテゴリ	レベル	ログの説明
			ダメージクリーンナップエンジン: %VERSION% 検索サービス: %VERSION%
6001	システム	警告	アップデートに失敗しました: %ERROR_MSG% (%ERROR_CODE%) [詳細] アップデート元: %SERVER% [元のバージョン] 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% [最新バージョン] 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%

イベントID	タスクカテゴリ	レベル	ログの説明
			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%

イベントID	タスクカテゴリ	レベル	ログの説明
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% [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%

イベントID	タスクカテゴリ	レベル	ログの説明
6004	システム	警告	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%

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	不正プログラムが検出されました: %ACTION% ファイルパス: %PATH% [詳細] 再起動が必要: %NEED_REBOOT% [検索結果] 脅威の種類: %TYPE% 脅威の名前: %NAME% [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%
6006	システム	警告	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% [詳細] 1 次処理: %1ST_ACTION% 2 次処理: %2ND_ACTION% 脅威の種類: %TYPE%

イベントID	タスクカテゴリ	レベル	ログの説明
			脅威の名前: %NAME% [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%
6007	メンテナンスモード	警告	メンテナンスモ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% [詳細] 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%

イベントID	タスクカテゴリ	レベル	ログの説明
			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%
6008	メンテナンスモード	警告	メンテナンスモ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% [詳細] 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%
6009	メンテナンスモード	警告	メンテナンスモードで不正プログラムが検出されました: %PATH% [詳細] 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%

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

エージェントのエラーコードの説明

このリストでは、TXOne StellarEnforce 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。

表 7-2. TXOne StellarEnforce のエラーコードの説明

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。
0x8004020e	予期しないエラーのため再起動が必要です。

コード	説明
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)
0x80040240	ライブラリが見つかりません。

コード	説明
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。

文書番号: APEM139622_JP2303