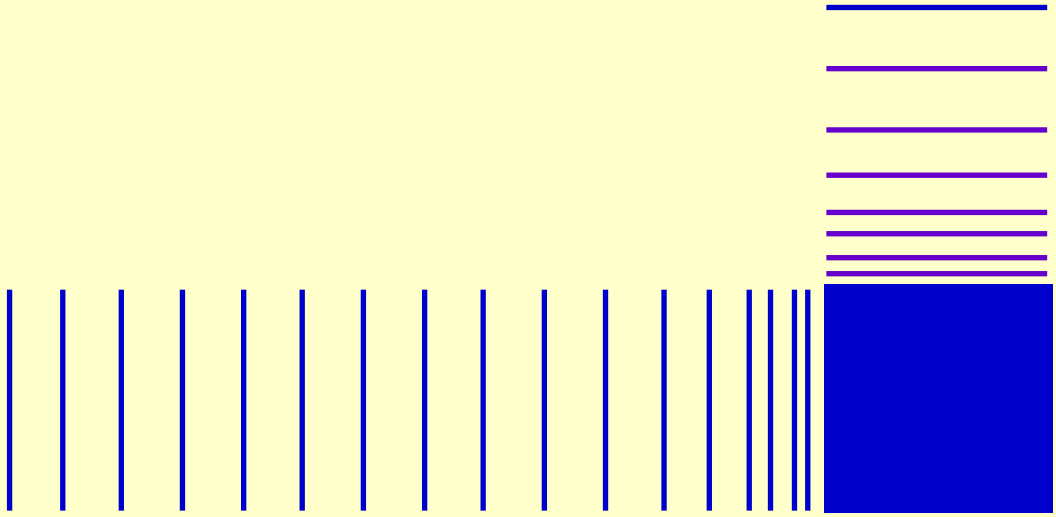
HITACHI

セキュリティソフトウェア

RunProtector™

ユーザーズガイド



RP-UG-JP-01-01

株式会社 日立インダストリアルプロダクツ

この製品を輸出される場合には、外国為替および外国貿易法
の規制並びに米国輸出管理規則など外国の輸出関連法規を
ご確認の上、必要な手続きをお取りください。
なお、不明な場合は、弊社担当営業にお問合わせください。

２０２６年 ９月（第１版）ＲＰ－ＵＧ－ＪＰ－０１－０１

● このマニュアルの一部または全部を無断で転写したり複写することは、
固くお断りいたします。
● このマニュアルの内容を、改良のため予告なしに変更することがあります。

All Rights Reserved, Copyright © 2026 Hitachi Industrial Products, Ltd.

ご注意

（1） このソフトウェアをご使用になる前に、このマニュアルの記載内容をよく読み、書かれている指示や注意を十分理解してください。

（2） このマニュアルの記載内容について理解できない内容、疑問点または不明点がございましたら、最寄りの当社営業までお知らせください。

（3） 当社提供ソフトウェアを改変して使用した場合には、発生した事故や損害につきましては、当社は責任を負いかねますのでご了承下さい。

（4） 当社提供以外のソフトウェアを使用した場合の信頼性については、当社は責任を負いかねますのでご了承下さい。

（5） このソフトウェアが万一故障したり、誤動作やプログラムに欠陥があった場合でも、ご使用されるシステムの安全が十分に確保されるよう、保護・安全回路は外部に設け、人身事故・重大な災害に対する安全対策などが十分確保できるようなシステム設計としてください。

はじめに

このマニュアルは RunProtector™ ついて記述したものです。このソフトウェアをご使用になる前に、このマニュアルをよくお読みください。

＜マニュアルの構成＞

このマニュアルは、次のような構成となっています。

第 1 章 RunProtector™ とは
第 2 章 RunProtector™ のインストール
第 3 章 Trellix Embedded Control の使用方法
第 4 章 Trellix Embedded Control 動作上の特記事項
第 5 章 保守・障害解析関連
第 6 章 RunProtector™ のアンインストール

＜商標について＞

- Microsoft®, Windows®, Windows Server®は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- Trellix®は、米国 Musarubra US LLC.の米国およびその他の国における登録商標または商標です。
- 上記以外にこのマニュアル記載されている他社製品名（ソフトウェア）は、各社の登録商標、商標、または製品です。

目次

はじめに 1
目次 2
表目次 4
第 1 章 RunProtector™ とは 5
第 2 章 RunProtector™ のインストール 7
2.1. インストールする前に 7
2.1.1. システム要件 7
2.1.2. 事前の準備 8
2.2. RunProtector™ をインストールする 9
2.3. インストール中に出力されるエラーメッセージについて 10
第 3 章 Trellix Embedded Control の使用方法 11
3.1. ステータス確認 11
3.2. アローリストの作成／削除 12
3.2.1. アローリストの作成手順 12
3.2.2. アローリストからの削除手順 15
3.2.3. アローリストへの登録／未登録ファイルの確認手順 15
3.3. Trellix Embedded Control の有効化／無効化 16
3.3.1. Trellix Embedded Control の有効化手順 16
3.3.2. Trellix Embedded Control の無効化手順 17
3.4. パスワード設定 18
3.5. 手動更新方法（Update モード） 19
3.6. 自動更新方法（アップデータ） 21
3.6.1. アップデータの登録手順 21
3.6.2. アップデータの削除手順 23
3.6.3. アップデータリストの表示方法 24
3.7. Finetune ユーティリティによるアップデータ登録 25
第 4 章 Trellix Embedded Control 動作上の特記事項 28
4.1. Trellix Embedded Control 保護有効中のイベントログ記録について 28
4.2. Trellix Embedded Control 保護有効中のファイルコピーについて 28

第 5 章 保守・障害解析関連 29
5.1. Trellix Embedded Control ログ確認方法 29
5.1.1. イベントログ出力先の設定 29
5.1.2. イベントログメッセージ 31
5.1.3. イベント出力例 35
5.1.4. イベントキャッシュサイズ設定 36
5.1.5. ログファイルサイズの設定 37
5.1.6. ログファイル数の設定 37
5.1.7. 拡張設定パラメータの確認 38
5.2. トラブルシューティング 39
5.2.1. GatherInfo ツール 39
5.2.2. GatherInfo ログ取得方法 39
第 6 章 RunProtector™ のアンインストール 41
6.1. アンインストールする前に 41
6.1.1. 事前の準備 41
6.2. RunProtector™ をアンインストールする 42
6.3. アンインストール中に出力されるエラーメッセージについて 43

表目次

表 2-1 インストール中のエラーメッセージ一覧.....10
表 4-1 TEC 保護有効中のエラーログ.....28
表 5-1 TEC が記録するイベントログ一覧.....31
表 6-1 アンインストール中のエラーメッセージ一覧.....43

第1章 RunProtector™ とは

RunProtector™ は、米国 Trellix 社(旧 McAfee 社)が開発したアローリスト型のセキュリティ対策ソフト「Trellix® Embedded Control」（以下、TEC と略す）を適用することにより、デナイリスト方式に比べて堅牢性が高く、スタンドアロン環境でも利用可能な産業機器に適したセキュリティ機能を提供します。

TEC は、ファイルシステムのフィルタードライバとして動作し、以下の機能を有しています。

（１）アローリスト登録されたファイルのみ実行許可、アローリスト未登録のファイルは全て実行阻止、未知のマルウェア（ゼロデイ攻撃）に対応

TEC は、ローカルドライブ（= FPD/DVD/USB 等を除く）に存在する exe、dll、sys、 ocx、bat、vbs 等の実行形式ファイルとスクリプトの一覧を「アローリスト」として自動作成し、アローリストに未登録のファイルの実行は拒否します。(ネットワークや可搬媒体等でシステム内へモジュールを新規コピーすることは可能ですが、実行は拒否します。)

なお、既存のウィルス対策ソフトは、ウィルスを「デナイリスト」としてパターンファイルに登録する方式であるため、以下の問題がありました。

①エンジン／パターンファイルの更新作業が頻繁に必要となる。

②ウィルススキャンの実行には、相当なシステム負荷と時間が必要となる。

③パターンファイルの肥大化に起因する性能劣化が生じることがある。

④パターンファイルに存在しない、未知のウィルスに対する防御（ゼロデイ攻撃の防御）ができない。

これに対して、TEC は、実行を許可するファイルを「アローリスト」に登録する方式をとるため、更新作業は不要で未知のマルウェアに対する防御も可能となります。

（２）システム登録された実行形式ファイル、スクリプトを更新する機能

「アローリスト」に登録された実行形式ファイルやスクリプトは、予め定義した「更新権限プロセス」(「アップデータ」)以外のプロセス/スクリプトによる変更、削除、上書き、リネームは拒否されます。

「更新権限プロセス」には、以下の機能があります。

・アローリストに記載のないローカルドライブ、CD-DVD、USB ドライブ、ネットワークドライブ上のファイルを実行出来ます。

・「更新権限プロセス」が、他の実行形式ファイル、スクリプトを実行する場合、アローリストを参照せず、直ちに実行出来ます。

・「更新権限プロセス」機能は、子、孫、プロセスにも引き継がれるため、親プロセスのみを「更新権限プロセス」に登録すれば、子、孫、プロセスも本機能を有します。
また、親プロセスが消滅しても、子、孫、プロセスの「更新権限プロセス」機能は有効です。

（３）保護対象ファイルの不正変更の試みを履歴として残す機能

アローリスト登録済みファイルの変更の試みやリード／ライト保護されたファイルの参照、変更の試み等を、履歴としてイベントログ(アプリケーション)等にリアルタイムで記録します。また、保護されたファイルに対して、変更などを実施する場合は、更新権限プロセスで行うことが可能です。

（４）メモリー保護機能

アローリストチェックを通過しメモリー上で実行状態のコードに脆弱性があった場合、脆弱なネットワーク環境では、その脆弱性を利用してネットワーク経由でメモリー上に不正コードを直接注入され、実行を試みられる場合があります。

TEC は「メモリー保護機能」で、非コード領域からのシェルコード実行の阻止や実行コードやデータのメモリー上の配置をランダム化するなどの対策を実施しています。

（５）ファイルレスマルウェア対策

「ファイルレスマルウェア」はディスク上に実行ファイルとして保存されず、メモリーや OS 標準の正規ツール（PowerShell 等）を悪用して動作するマルウェアです。

ファイルが存在しないため、従来のウィルス対策ソフトによる検知が難しいという特徴があります。「ファイルレスマルウェア」は、アローリストでは防御できないため、その振る舞いや特性から実行を阻止する必要があります。

TEC では「ファイルレスマルウェア」対策として、「実行制御ルール」による対策を実施しています。

例えば、「実行制御ルール」に従って、特定 APL から PowerShell.exe や cmd.exe を呼び出そうとした場合に、アローリストに登録がある PowerShell.exe、cmd.exe の実行阻止やバッチファイル内で PowerShell コマンドを実行しようとした場合に実行阻止します。

【補足】

Trellix® Embedded Control に関する製品ガイド・リリースノードは下記サイトより閲覧ください。

https://docs.trellix.com/ja-JP/bundle/application-change-control-landing/page/UUID-52a27749-32a8-9db0-c79a-0e1e75772485.html

第2章 RunProtector™ のインストール

2.1. インストールする前に

この節では、RunProtector™ のインストールに際して、動作環境に関する各種確認について説明します。なお、以降の作業はコンピューターの管理者アカウントでサインインして行なってください。

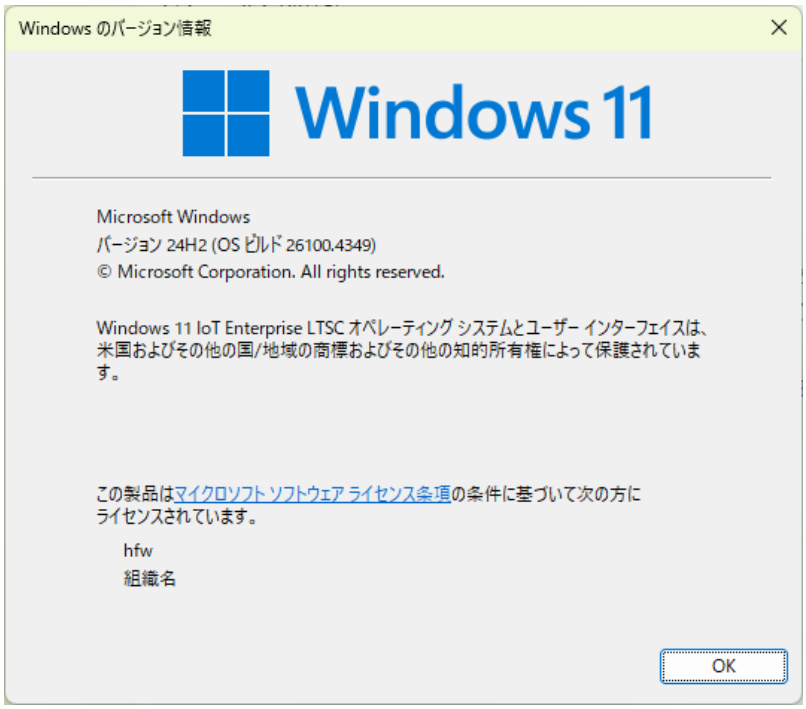
2.1.1. システム要件

RunProtector™ は、Windows® 11/Windows® Server2025 に対してインストールすることができます。ご使用の OS を確認する際は以下の手順を行ってください。

① 「ファイル名を指定して実行」ウィンドウを開きます。
「スタート」ボタンを右クリックし、表示されたメニューより「ファイル名を指定して実行」をクリックします。

② 名称ボックスに「winver」と入力し、[Enter]キーを押します。

③ 表示された「Windows のバージョン情報」ウィンドウを参照し、OS の種類を確認します。



2.1.2. 事前の準備

RunProtector™ のインストールを開始する前に、ご使用の OS に応じて以下のインストール/アンインストール DVD を準備してください。

OS の種別	準備するインストール/アンインストール DVD
クライアント向け OS	RunProtector for Devices(S-763A-A2P)
サーバー向け OS	RunProtector for Servers(S-763A-A3P)

2.2. RunProtector™ をインストールする

この節では、RunProtector™ のインストール方法について説明します。なお、インストールはコンピューターの管理者アカウントでサインインして行なってください。

① DVD ドライブに RunProtector™ のインストール/アンインストール DVD をセットします。
② 「スタート」ボタンをクリックします。
③ 「すべて」―「Windows ツール」―「コマンドプロンプト」を右クリックし、「管理者として実行」を選択します。
④ インストーラーを起動します。
・コマンドラインに以下を入力して[Enter]キーを押します。
D:¥RunProtectorInstaller.exe

※ ここでは、DVD メディアでのインストール手順として、DVD ドライブのドライブ文字を D ドライブと仮定したパスを指定しています。下線部のパスはセットアッププログラムが格納されている場所に応じて変更してください。

⑤ 「Would you like to proceed with the installation of the RunProtector?」のダイアログが表示されたら「はい」を押下するとインストールが開始されます。
※ インストール処理はすべて自動で行われます。
インストールが完了するまで 5 分程度かかります。
⑥ インストール完了後、「Installation complete.」のダイアログが表示されますので「OK」ボタンを押下してインストーラーを終了します。
⑦ 以下の項目の確認をしてください。
・デスクトップに"Trellix Solidifier コマンドライン"のショートカットが作成されていること。
・[設定]-[アプリ]-[インストールされているアプリ]に、「Trellix Solidifier」が追加されていること。

以上で RunProtector™ のインストールは完了です。

留意事項

RunProtector™ のインストール時に、TEC に対して自動的に以下の設定が行われます。
HF-W の動作が不安定となりますので、これらの設定は変更しないでください。
・非コード領域から実行されるシェルコードを無効にするメモリー保護機能(mp-casp)を有効に設定しています。
・アローリストにファイルを登録する際、大文字/小文字の区別を無効にしています。
この設定にて、大文字と小文字の区別を無効に設定しています。

2.3. インストール中に出力されるエラーメッセージについて

インストール中にエラーが発生すると、エラーを示すポップアップメッセージが出力されます。
その原因について以下に示します。
エラーを示すポップアップメッセージが出力された場合、OK ボタンを押下すると、
インストーラーは処理を中断して終了します。

表 2-1 インストール中のエラーメッセージ一覧

No.	出力エラーメッセージ	原因
1	Not the product to be installed.	稼働中の OS が、RunProtector™ をインストールするための条件を満たしていません。
2	Installation was not completed.	RunProtector™ の設定中にエラーが発生しました。

第3章 Trellix Embedded Control の使用方法

正常にインストールが完了すると、デスクトップに“Trellix Solidifier コマンドライン”アイコンが表示されます。Trellix Embedded Control の状態の確認や設定の変更はこのアイコンから起動するプロンプトから実行します。

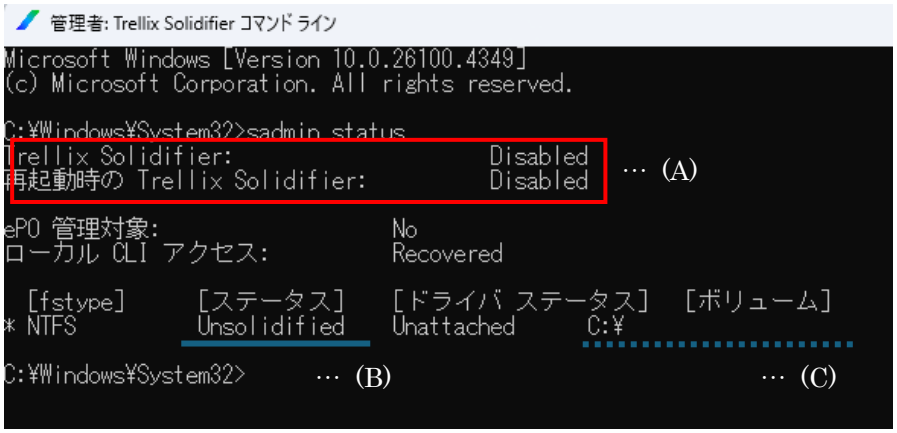
なお、プロンプトを起動する際は管理者として実行してください。



3.1. ステータス確認

TEC の現在の状態を確認するには次のコマンドを実行します。

> sadmin status



(A) TEC の有効・無効の状態を表示します。

- Disabled : TEC による保護が無効な状態です。(無効モード)
- Enabled : TEC による保護が有効な状態です。(有効モード)
- Update : ソフトウェアの更新やインストールを行う状態です。(Update モード)

※インストール直後は、無効モード状態(Disabled)となります。

(B) アローリストによる保護の実行状態を表示します。

- Unsolidified : 対象ボリュームのアローリストが作成されていない状態です。
- Solidified : 対象ボリュームのアローリストが作成されている状態です。

※インストール直後は、Unsolidified となります。

(C) 保護対象ボリュームを表示します。

対象のボリュームが複数ある場合は、ボリューム毎に表示されます。

3.2. アローリストの作成／削除

3.2.1. アローリストの作成手順

留意事項

- アローリストを作成する際は、実施前にウイルスチェックのフルスキャンを実施するなど
  システムをクリーンな状態にしてから行ってください。

システム上の全てのローカルドライブを対象として、アローリストを作成する場合は次のコマンドを使用してください。

> sadmin solidify

または、次の省略形式でも使用できます。

> sadmin so



留意事項

- アローリストを作成するためのプロセスの所要時間は、システムのスペック、システム内の
  ファイル数やファイルサイズなどで異なり、数分から数時間かかることがあります。

アローリストの作成が完了すると、以下のメッセージが表示されます。
ボリュームが複数ある場合は、ボリューム毎にメッセージが表示されます。

```
インストール済製品を列挙しています。
ボリューム C:¥を固定化しています。
00:15:21:スキャンされたファイルの合計  190745、固定化されたファイルの合計  51587
```

特定のボリュームを個別にアローリストへ登録することもできます。
例えば、ボリューム C の全てのプログラムファイルをアローリストへ追加する場合には、次のコマンドを実行してください。

> sadmin so c:

※システムボリュームは、アローリストに登録する必要があります。

特定のフォルダを個別にアローリストへ登録する場合、次のコマンドを使用してください。

> sadmin so “DirectoryName”

複数のフォルダを指定する場合は以下のコマンドを使用してください。

> sadmin so “DirectoryName1” “DirectoryName2”

特定のファイルを個別にアローリストへ登録する場合、次のコマンドを使用してください。

> sadmin so “pathname”

複数のフォルダを指定する場合は以下のコマンドを使用してください。

> sadmin so “pathname1” “pathname2”

コマンドには、以下の引数を指定できます

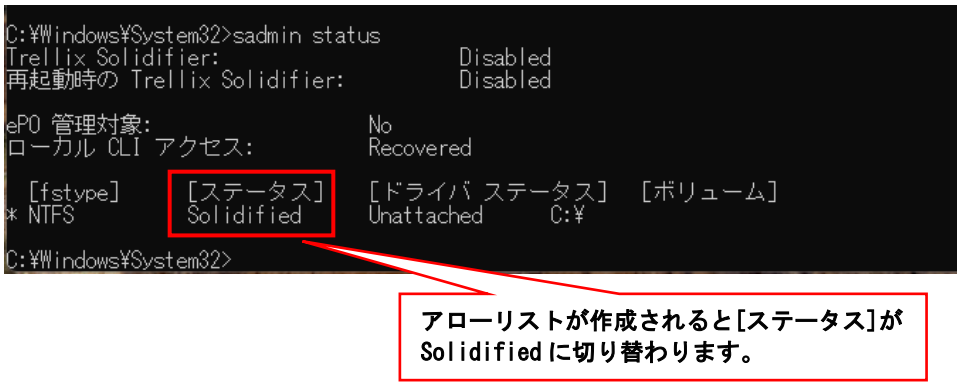
-q：エラーメッセージのみが画面に表示されます。
その他のメッセージは全て Solidcore ログに書き込まれます。

-v：全てのメッセージが画面に表示されると同時に、Solidcore ログに書き込まれます。

※どちらの引数も指定しなかった場合には、メッセージは Solidcore ログにのみ書き込まれます。

アローリスト作成後、“sadmin status”にて状態確認を行います。

[ステータス]が“Unsolidified” → “Solidified”に切替わったことを確認します。
※ボリュームが複数ある場合には、ボリューム毎に**[ステータス]**を確認します。



アローリストに登録されるファイルとして、以下の種類があります。

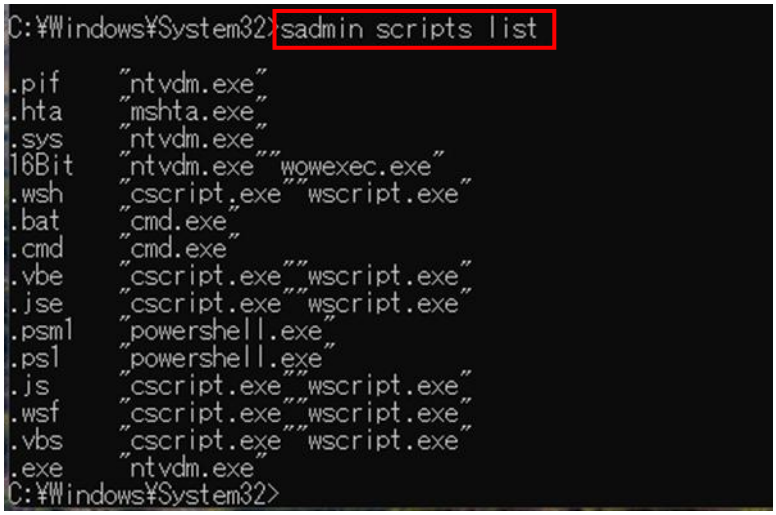
１．実行形式のバイナリ

２．登録されているスクリプト

“１”に関しては、バイナリファイル内のPEヘッダの情報を基にアローリストに登録されるため、どのような拡張子であっても“sadmin so”コマンドでスキャンする際にアローリストへ登録されます。

“２”に関しては、以下のコマンドを実行することで登録対象とするスクリプトのリストが表示されます。

> sadmin scripts list



スクリプトのリストに登録がない拡張子をアローリストとして管理したい場合、以下のコマンドで追加することができます。

> sadmin scripts add “拡張子” “実行するモジュール”

例：java の.jar ファイルをアローリストに登録する場合

> sadmin scripts add .jar java.exe

次のコマンドにて“.jar”が追加されていることを確認してください。

> sadmin scripts list

3.2.2. アローリストからの削除手順

システム上でアローリストに登録しているファイルを、アローリストから削除する場合は、次のコマンドを実行してください。

> sadmin unsolidify “pathname / directoryname / volume”

または、次の省略形式でも使用できます。

> sadmin unso “pathname / directoryname / volume”

3.2.3. アローリストへの登録／未登録ファイルの確認手順

アローリストに登録されているファイルを確認する場合は、次のコマンドを実行します。

> sadmin list-solidified

または、次の省略形式でも使用できます。

> sadmin ls

ファイル、ディレクトリ、ボリュームを指定して確認する場合は、次のコマンドを実行してください。

> sadmin ls “file / directory / volume”

テキストベースでリストを出力する場合は、次のコマンドを実行してください。

> sadmin ls > XXX.txt (任意の名前)

コマンドには、以下の引数を指定できます

-l : アローリストの詳細が表示されます。

アローリストに登録されていないファイルを確認する場合は、次のコマンドを実行してください。

> sadmin list-unsolidified

または、次の省略形式でも使用できます。

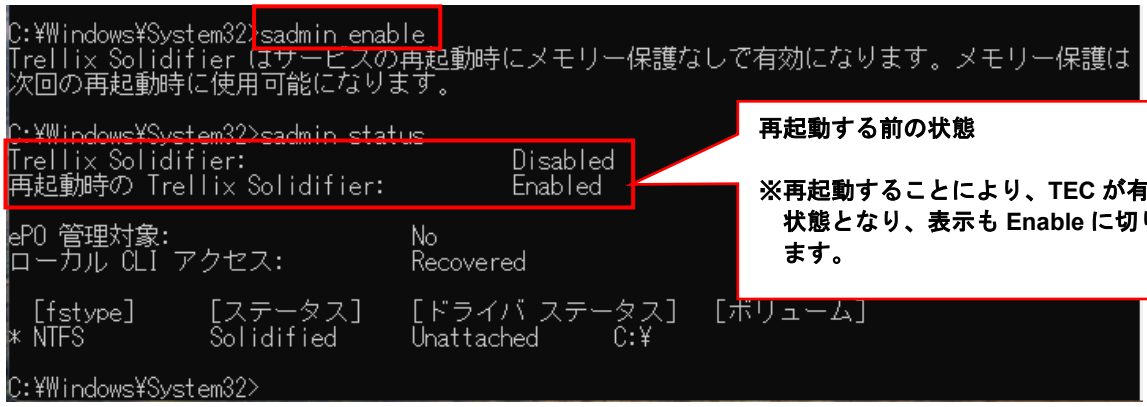
> sadmin lu

3.3. Trellix Embedded Control の有効化／無効化

3.3.1. Trellix Embedded Control の有効化手順

アローリストにシステム上のファイルを登録した後、TEC を有効化するには次のコマンドを使用してください。

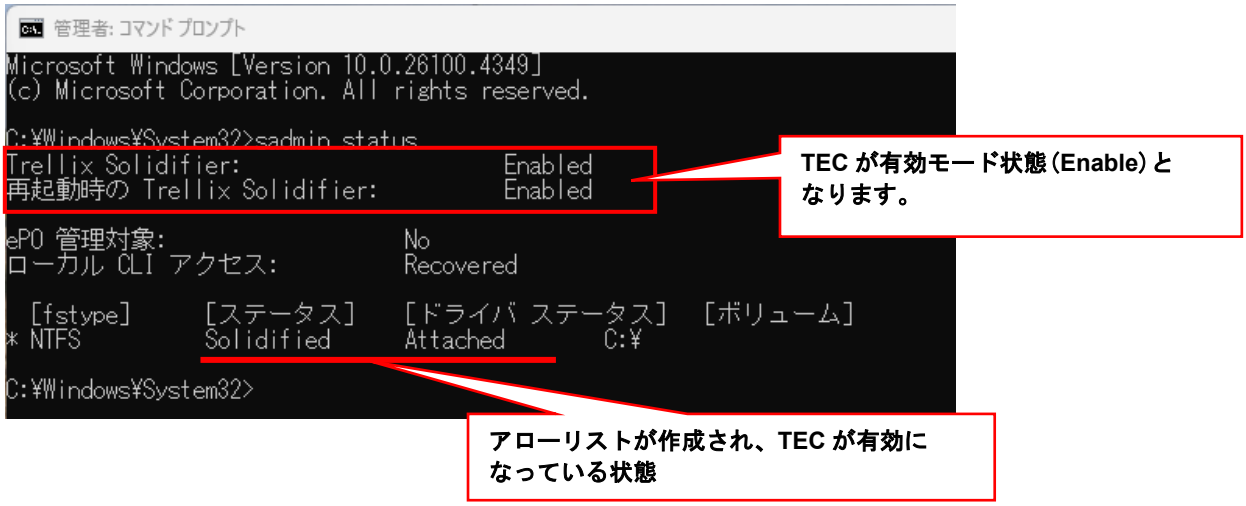
> sadmin enable



留意事項

- コマンド実行後にメモリー保護機能を動作させない場合、TEC のサービス(scsrvc)を再スタートしてください。
- コマンド実行後にメモリー保護機能を動作させる場合、システムの再起動が必要になります。
- TEC が実際に有効(Enable)になるのは、サービまたはシステムの再起動後になります。

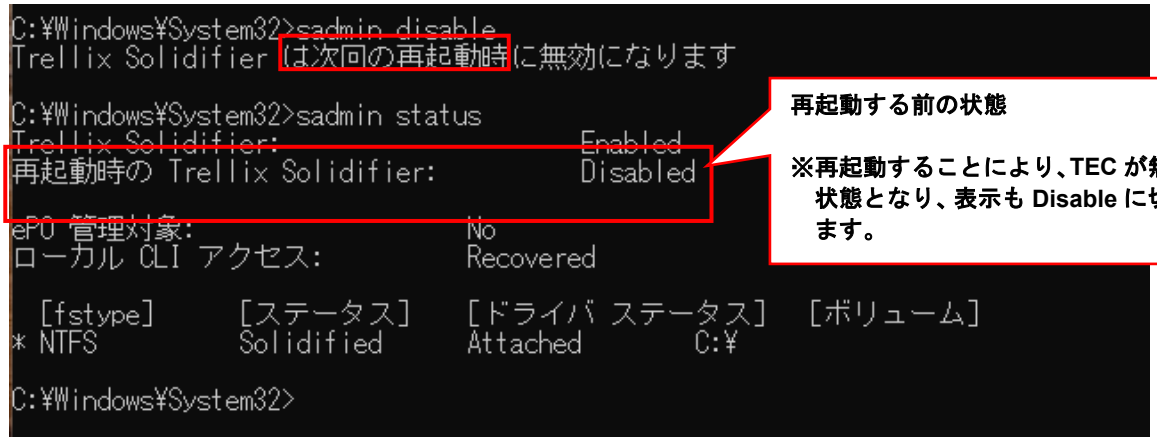
以下、再起動後の状態となります。



3.3.2. Trellix Embedded Control の無効化手順

TEC を無効化するには次のコマンドを使用してください。

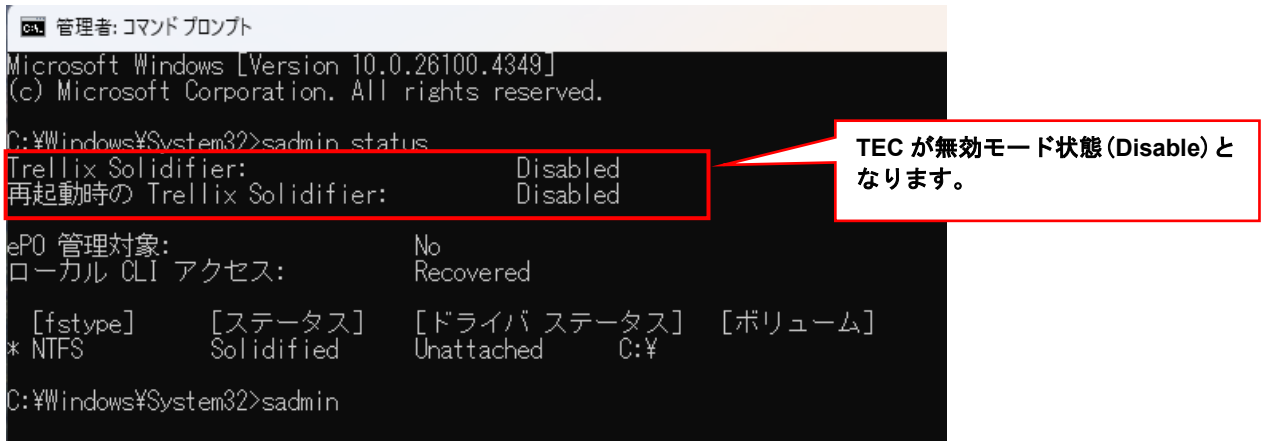
> sadmin disable



留意事項

- コマンド実行後はシステムの再起動が必要になります。
- TEC が実際に無効(Disable)になるのは、サービまたはシステムの再起動後になります。

以下、再起動後の状態となります。



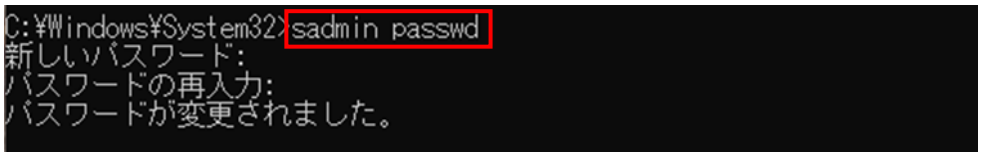
3.4. パスワード設定

パスワード保護機能は、個人によるクリティカルな sadmin コマンドの使用を sadmin 管理者のみに限定することができます。パスワードが一旦設定されると、パスワード保護が有効化されます。クリティカルなコマンドは、すべてパスワードで保護され、パスワードを入力しないとアクセスできなくなります。

パスワード保護は、次のコマンドを使用して設定されます。

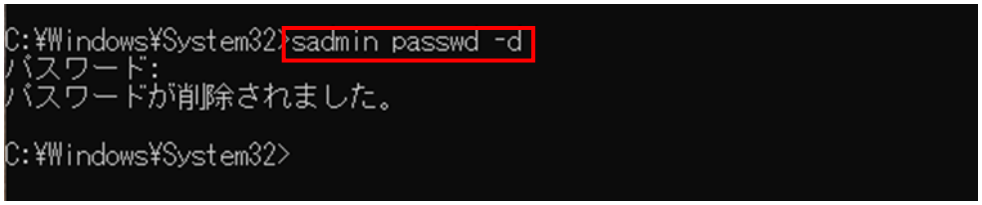
> sadmin passwd

このコマンドは、（パスワードが設定されていれば）古いパスワードを入力するよう指示し、次に新しいパスワードを確認のため 2 回入力するよう指示します。



既存のパスワードは、次のコマンドを使用して削除できます。

> sadmin passwd –d



3.5. 手動更新方法（Update モード）

Update モードでは、システム上のソフトウェアの追加、削除、変更など全ての更新操作を処理できます。また、アローリストへ自動更新する機能を備えており、Update モード中に追加または変更された実行ファイルのみが、操作完了後にアローリストへ登録されます。これにより、新規または変更されたソフトウェアは、Enable モードにシステムが戻ると、Update モード時に更新されたファイルの実行が可能になります。

Update モードでソフトウェアの更新を行う場合には、以下の手順を実行してください。

①“sadmin status”コマンドを実行して現在の状態を確認します。

> sadmin status

TEC の有効化モードであることを確認します。

Trellix Solidifier:　　Enabled

再起動時の Trellix Solidifier:　　Enabled

②以下のコマンドを実行して Update モードを開始します。

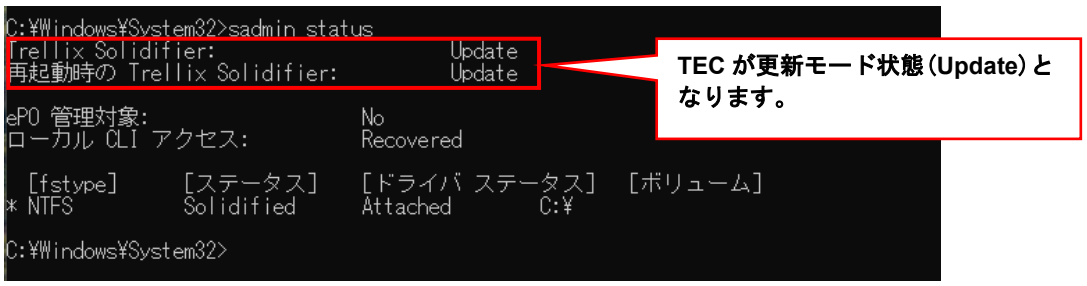
> sadmin begin-update

または、次の省略形式でも使用できます。

> sadmin bu



③“sadmin status”コマンドを実行して、Update モードに切り替わったことを確認します。



Update モードを終了する場合には、以下の手順を実行してください。

①以下のコマンドを実行して Update モードを開始します。

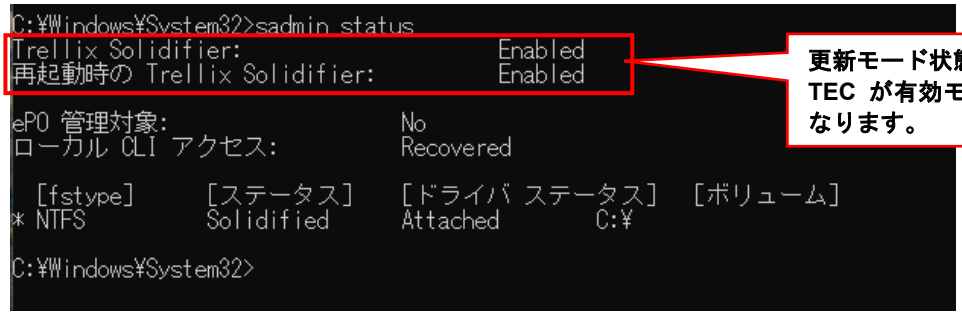
> sadmin end-update

または、次の省略形式でも使用できます。

> sadmin eu



②“sadmin status”コマンドを実行して、Update モードが終了したことを確認します。



更新モード状態(Update)が終了し、TEC が有効モード状態(Enable)となります。

3.6. 自動更新方法（アップデータ）

アップデータの登録を行うことで、Trellix Embedded Control は、Update モードに切り替えることなく、ファイルの変更および削除を行うことが可能になります。

また、MSI ベースのインストーラーをアップデータに登録することで、インストールすることが可能です。

3.6.1. アップデータの登録手順

指定した実行ファイルをアップデータリストに登録するには、次のコマンドを実行してください。

> sadmin updaters add xxx.exe

※保護されたファイルまたはレジストリキーに対して、更新処理を承認します。

MSI ファイルをアップデータリストに登録する場合は、次のコマンドを実行してください。

> sadmin updaters add xxx.msi

※MSI ファイル xxx.msi 対応の Windows インストーラーが保護されたファイルまたはレジストリキーに対して、変更を行うことを承認します。
新規ファイルはシステムに置かれ、アローリストへ登録されます。

アップデータ登録として、条件付きのアップデータ登録をすることができます。
以下、設定例となります。

例１：

実行ファイル AAA.exe が実行ファイル BBB.exe を親として起動された場合のみ、アップデータとして設定するには次のコマンドを実行してください。

> sadmin updaters add -p BBB.exe AAA.exe

-p：指定した親が起動されている場合のみ適応できます。

例２：

実行ファイル AAA.exe がライブラリ BBB.dll をロードする場合のみ、アップデータとして設定するには次のコマンドを実行してください。

> sadmin updaters add -l BBB.dll AAA.exe

-l：指定したライブラリがロードされた場合のみ適応できます。

例３：

実行ファイル AAA.exe をアップデータとして設定するが、子プロセスはアップデータのルールに含めない場合は次のコマンドを実行してください。

> sadmin updaters add -d AAA.exe

-d：子プロセスは使用できません。

イベントログへ表示する機能およびログ機能を無効化する機能として、アップデータ登録することができます。

以下、設定例となります。

例１：

実行ファイル AAA.exe をアップデータとして設定します。

また、アップデータルールによって処理された全てのファイルについて、タグ rule-id がイベントに表示されるようにするには次のコマンドを実行してください。

> sadmin updaters add -t rule-id AAA.exe

-t：rule-id、指定されている場合、イベントログにこのルールにより処理された全てのファイルが表示されます。

例２：

実行ファイル AAA.exe をアップデータとして設定します。

また、また、ログ機能が無効にするには次のコマンドを実行してください。

> sadmin updaters add -n AAA.exe

-n：ログを中止します。

変更等を許可するために、信頼があるユーザーをアップデータ登録することができます。ユーザー設定するには、次のコマンドを実行します。

> sadmin updaters add -u USERNAME

-u：ユーザーがアップデータとして処理されるように指定します。

留意事項

- USERNAME としては、単純な名前(hitachi)、ユーザーのドメイン名(hitachi@xxx.co.jp)、階層的なドメイン名(MYDOMAIN¥hitachi)を指定できます。
- ユーザーとしてアップデータ登録する場合は、-l、-p、-d、-n の引数は使用できません。

3.6.2. アップデータの削除手順

承認されたアップデータを削除する場合には、次のコマンドを使用して、アップデータリストから削除できます。

> sadmin updaters remove “pathname”

※pathname には、承認されたアップデータリストから削除する必要がある保護されたプログラムへのパスを入力します。

同様に、条件付きの保護されたファイルを削除する場合には、次のコマンドを使用して、アップデータリストから削除できます。

> sadmin updaters remove -p “pathname”

> sadmin updaters remove -l “pathname”

> sadmin updaters remove -u “USERNAME”

承認されたアップデータリストを全て削除（フラッシュ）するには、次のコマンドを実行します。

> sadmin updaters flush

3.6.3. アップデータリストの表示方法

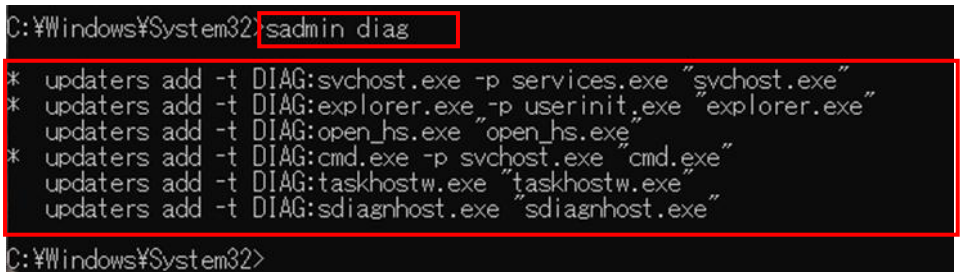
承認されたアップデータリストの一覧表示は、次のコマンドを使用して表示できます。

> sadmin updaters list

また、TEC では、参考情報としてシステム上でファイルの追加/削除/変更等を処理しているプロセスに対して、一覧を表示する機能があります。

以下のコマンドを実行することで、リストを表示することができます。アップデータに追加する際は、十分検討した上でアップデータへ登録してください。

> sadmin diag



“*”があるリストは、OS 内部の動作になるため、動作に問題ない限りアップデータへ追加する必要はありません。

3.7. Finetune ユーティリティによるアップデータ登録

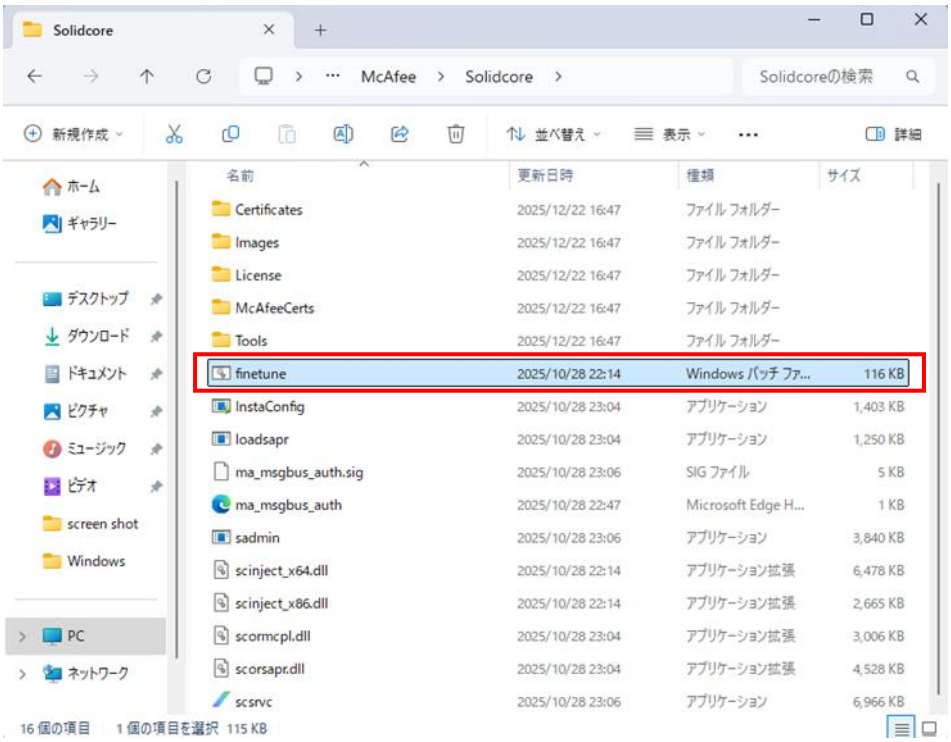
Finetune ユーティリティは、デフォルトのシステム設定に商用アプリケーションを実行するために必要な設定をデフォルトのアップデータとして追加できます。

Trellix Embedded Control のインストールフォルダにインストールされているバッチファイル(finetune.bat)を実行することにより、自動的にアローリストに反映されます。

このユーティリティを使用して、設定を追加したり削除したりすることができます。

＜Finetune バッチ格納先＞

C:¥Profram Files¥McAfee¥Solidcore



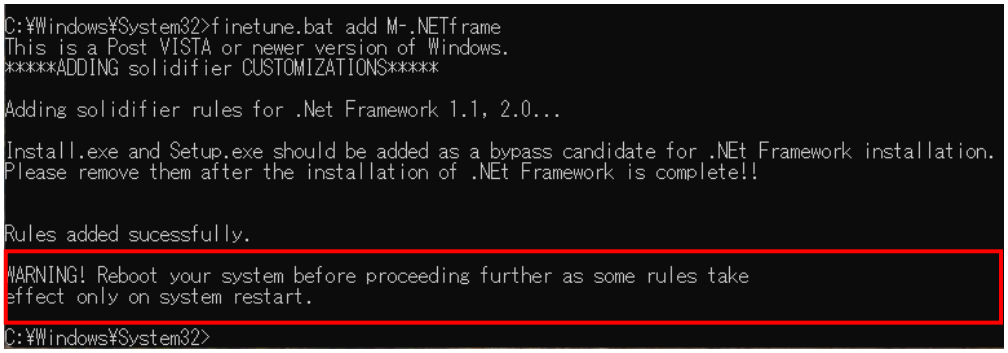
アプリケーションをデフォルトのアップデータ設定に追加する場合には、次のコマンドを実行します。

> finetune.bat add X-XXX

例えば、.NET を使用している場合、finetune を実行することでデフォルトアップデータ設定が行えます。追加する場合には、次のコマンドを実行します。

> finetune.bat add M-.NETframe

上記コマンドを実行すると、次のメッセージが表示されます。適応するにはシステムの再起動が必要になります。



アプリケーションをアップデータ設定から削除する場合には、次のコマンドを実行します。

> finetune.bat remove X-XXX

NET のデフォルトアップデータ設定を削除する場合には、次のコマンドを実行します。

> finetune.bat remove M-.NETframe

Finetune がサポートするヘルプを参照する場合には、次のコマンドを実行します。

（Finetune ユーティリティに定義されているアプリケーションを確認することができます。）

> finetune.bat help

```
C:¥Windows¥System32>finetune.bat help
This is a Post VISTA or newer version of Windows.
Finetune.bat (Fine tunes solidifier for a Windows system)
Copyright 2023 Musarubra US, LLC. All Rights Reserved

Add or remove solidifier customizations for a particular application

finetune.bat add/remove APPLICATION

add                 adds solidifier rules
remove              removes solidifier rules
APPLICATION         application for which you can add/remove
                    solidifier rules.

Specify the application indentifier from the list given below.


ANTI VIRUS
==========
A-Trellix            Trellix (8.0,9.0), Trellix virusscan (7.1,10.0),
                    Trellix Enterprise 8.0,Trellix Total Protection 4.7
A-Etrust            Etrust Version 7.0, Etrust Version 7.1,
                    Etrust Version 6.0, Etrust PestPatrol Anti-Spyware
A-NAV               2005, NAV Corporate Editon (8.1, 10.1,10.2,9.0),
                    NAV 2004,Norton Removal Tool, Norton 2008
A-SPC            Symantec PcAnywhere (11.5, 12.1)
A-MSE            Symantec Mail Security
A-SMSMSE                 Symantec Mail Security for Exchange
A-SEP            Symantec Endpoint Protection
A-Sophos            Sophos Version 5.1.3
A-Avast             Avast Virus Cleaner
A-AVG               AVG Version 7.0
A-Fsecure           Fsecure2006, 2007, 2008, 2009 Anti Virus
A-NOD32             NOD32 Anti Virus version 2.5
A-TrendMicro        Trend Micro IMSSS, Client server security Agent,
                    OfficeScan, Trend Micro Server Protect
A-GDATA             GDATA version
A-ZoneAlarm         Zone Alarm 6.1
A-AVK               AVK version
A-BTD               BitDefender 9 prof plus, BitDefender 8,BitDefenderAVPlus10 Final
A-FProt          F-Prot AV 3.16f
A-MCGroupShield  Trellix Group shield for Exchange
A-QHeal          Quick Heal Total Security 2007
A-QHealPlus      Quick Heal Plus 2007
A-Ksky           Kaspersky Internet Security 7.0
A-Panda          Panda antivirus 2009
A-InstNAV2011    Install Norton 2011

BACKUP/RESTORE
==============
B-Veritas           Veritas Backup 10, Veritas Storage Cental
B-Brightstor        BrightstorARCServe 9.0/11.5 BackupServer
B-Symantec          Symantec Backup Exec 11d

続行するには何かキーを押してください . . .
```

第4章 Trellix Embedded Control 動作上の特記事項

4.1. Trellix Embedded Control 保護有効中のイベントログ記録について

TEC 保護有効中に以下のイベントログが記録されることがありますが、システムの動作に影響ありません。

表 4-1 TEC 保護有効中のエラーログ

ソース	イベント ID	種類
Trellix Solidfier	144	エラー

4.2. Trellix Embedded Control 保護有効中のファイルコピーについて

TEC の保護有効中にアローリストに加えられていないファイルのコピーを失敗する場合があります。具体的な例を以下に示します。

- コマンドプロンプトより、拡張子が bat であるファイルのコピー
- Powershell より、拡張子が ps1 であるファイルのコピー

本事象を回避するには、コピー対象のファイルをアローリストへ加える必要があります。

第5章 保守・障害解析関連

5.1. Trellix Embedded Control ログ確認方法

Trellix Embedded Control は、システムの変更を追跡し、オペレーティングシステムログにその変更を全てイベントとして記録します。イベントごとに、変更の発生が記録されます。記録されるイベントは、イベントシンクと呼ばれる 1 つまたは複数の場所に保存されますので、お客様の設定によりログの出力される場所が決まります。

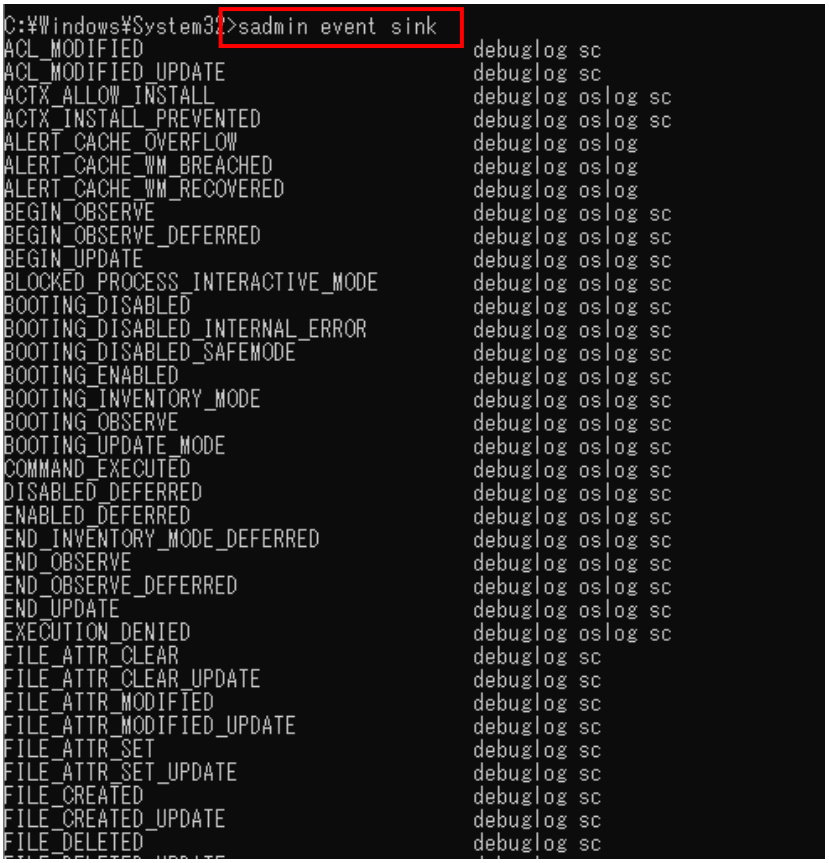
サポートされるイベントシンクは、以下となります。

- オペレーティングシステムログ（oslog）
- System Controller (sc)
- デバック出力（debuglog）

5.1.1. イベントログ出力先の設定

イベントとそのシンク設定の一覧を表示する場合には、次のコマンドを実行します。

> sadmin event sink

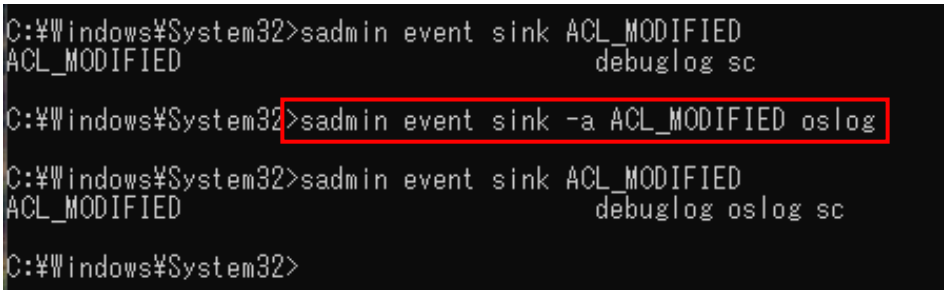


指定されたイベントに特定のシンクを追加する場合には、次のコマンドを実行します。

> sadmin event sink -a EventName sc　または

> sadmin event sink -a EventName debuglog　または

> sadmin event sink -a EventName oslog

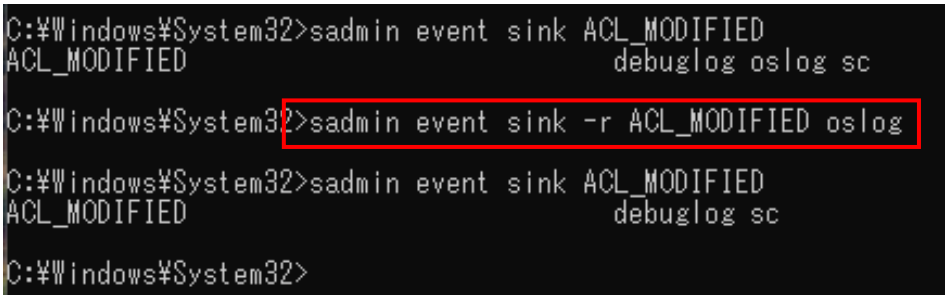


指定されたイベントから特定のシンクを削除する場合には、次のコマンドを実行します。

> sadmin event sink -r EventName sc　または

> sadmin event sink -r EventName debuglog　または

> sadmin event sink -r EventName oslog



5.1.2. イベントログメッセージ

この節では、TEC が記録するイベントログの一覧について記載します。

表 5-1 TEC が記録するイベントログ一覧 (1/4)

イベント ID	イベント名	レベル	説明
19	PROCESS_TERMINATED	エラー	Trellix Solidifier が、API '<string>' の不正呼び出しによるプロセス <string> (プロセス ID: <string>、ユーザー: <string>) のハイジャックを阻止しました。プロセスは終了しました
20	WRITE_DENIED	エラー	Trellix Solidifier がファイル <string> に対する変更を阻止しました。変更を試みたプロセス / スクリプトは <string> (sha1: <string> 、 md5: <string>、sha256: <string>) (プロセス ID: <string>、ユーザー: <string>)
21	EXECUTION_DENIED	エラー	Trellix Solidifier が '<string>' (sha1: <string> 、 md5: <string> 、 sha256: <string>、ファイル タイプ: <string>) の未承認の実行を阻止しました。実行を試みたプロセスは <string> (プロセス ID:<string>、ユーザー: <string>)、親プロセス <string>、deny_reason: <string> (拒否理由コード: <string>)、レピュテーション スコア: <string>
29	PROCESS_TERMINATED_UNAUTH_SYSCALL	エラー	Trellix Solidifier が、<string> によって開始されたプロセス <string> による不正な syscall %d (戻りアドレス %d) を阻止しました。プロセスは終了しました
30	PROCESS_TERMINATED_UNAUTH_API	エラー	Trellix Solidifier が、<string> によって開始されたプロセス <string> による API <string> の不正アクセス (戻りアドレス <string>) を阻止しました。プロセスは終了しました
49	REG_VALUE_WRITE_DENIED	エラー	Trellix Solidifier が、プロセス <string> (プロセス ID: <string>、ユーザー: <string>) によるレジストリ キー '<string>' (値: '<string>') の変更を阻止しました
50	REG_KEY_WRITE_DENIED	エラー	Trellix Solidifier が、プロセス <string> (プロセス ID: <string>、ユーザー: <string>) によるレジストリ キー '<string>' の変更を阻止しました
51	REG_KEY_CREATED_UPDATE	情報	Trellix Solidifier が、プログラム <string> (ユーザー: <string>、ワークフロー ID: <string>) によるレジストリ キー '<string>' の作成を検出しました

表 5-2 TEC が記録するイベントログ一覧 (2/4)

イベント ID	イベント名	レベル	説明
52	REG_KEY_DELETED_UPDATE	情報	Trellix Solidifier が、プログラム <string> (ユーザー: <string>、ワークフロー ID: <string>) によるレジストリキー '<string>' の削除を検出しました
54	REG_VALUE_DELETED_UPDATE	情報	Trellix Solidifier が、プログラム <string> (ユーザー: <string>、ワークフロー ID: <string>) によるレジストリ (値 '<string>'、キー '<string>') の削除を検出しました
57	OWNER_MODIFIED_UPDATE	情報	Trellix Solidifier が、プログラム <string> (ユーザー: <string>、ワークフロー ID: <string>) による '<string>' 所有者の変更を検出しました
61	PROCESS_HIJACKED	エラー	Trellix Solidifier がプロセス <string> (sha1: <string> 、 md5: <string> 、 sha256: <string>) に対する攻撃を検出しました。攻撃元のアドレス <string>
62	INVENTORY_CORRUPT	重大	Trellix Solidifier がボリューム <string> の内部インベントリの破損を検出しました
75	FILE_CREATED_UPDATE	情報	Trellix Solidifier が、プログラム <string> (ユーザー: <string>、元のユーザー: <string>、ワークフロー ID: <string>) による '<string>' の作成を検出しました
76	FILE_DELETED_UPDATE	情報	Trellix Solidifier が、プログラム <string> (ユーザー: <string>、元のユーザー: <string>、ワークフロー ID: <string>) による '<string>' の削除を検出しました
77	FILE_MODIFIED_UPDATE	情報	Trellix Solidifier が、プログラム <string> (ユーザー: <string>、元のユーザー: <string>、ワークフロー ID: <string>) による '<string>' の変更を検出しました
79	FILE_RENAMED_UPDATE	情報	Trellix Solidifier が、プログラム <string> (ユーザー: <string>、元のユーザー: <string>、ワークフロー ID: <string>) による名前変更 ('<string>' から '<string>') を検出しました
80	FILE_SOLIDIFIED	情報	<string>' は固定化されています。プログラム <string>(ユーザー: <string>、ワークフロー ID: <string>) によって作成されました
82	FILE_UNSOLIDIFIED	情報	<string>' は固定化が解除されています。プログラム <string> (ユーザー: <string>、ワークフロー ID: <string>) によって削除されました
89	READ_DENIED	エラー	Trellix Solidifier が、プロセス <string> (プロセス ID: <string>、ユーザー: <string>) によるファイル '<string>' の読み取りを阻止しました

表 5-3 TEC が記録するイベントログ一覧 (3/4)

イベント ID	イベント名	レベル	説明
96	PKG_MODIFICATION_PREVENTED	重大	Trellix Solidifier がパッケージの変更を阻止しました。変更を試みたプロセス '<string>'(sha1: <string>、md5: <string>、sha256: <string>)、ユーザー: '<string>'
97	PKG_MODIFICATION_ALLOWED_UPDATE	情報	Trellix Solidifier がパッケージの変更を許可しました。変更を試みたプロセス <string>'(sha1: <string>、md5: <string>、sha256: <string>)、ユーザー: '<string>'。(ワークフロー ID: <string>)
98	PKG_MODIFICATION_PREVENTED_2	重大	Trellix Solidifier が、'<string>' (ユーザー: '<string>') によるパッケージの変更を阻止しました
99	NX_VIOLATION_DETECTED	重大	Trellix Solidifier がプロセス '<string>' (プロセス ID: '<string>'、SHA1: <string>、MD5: <string>、SHA256: <string>、ユーザー: '<string>') の乗っ取りを防ぎました。コードページ領域外にあるアドレスからのコードの実行を阻止しました。障害アドレス '<string>'。プロセスは終了しました
101	REG_VALUE_MODIFIED_UPDATE	情報	Trellix Solidifier が、プログラム '<string>' (ユーザー: <string>、ワークフロー ID: <string>) によるデータ (<string>) を使用したレジストリ (値 '<string>'、タイプ '<string>'、キー '<string>') の変更を検出しました
103	FILE_READ_UPDATE	情報	Trellix Solidifier が、プログラム <string> (ユーザー: <string>、元のユーザー: <string>、ワークフロー ID: <string>) による '<string>' の読み取りを検出しました
124	INITIAL_SCAN_TASK_COMPLETED	情報	Trellix Solidifier 初期スキャン タスクが完了し、システムで Application Control が施行されています
126	ACTX_ALLOW_INSTALL	情報	Trellix Solidifier が、ActiveX <string> のインストールを許可しました (ワークフロー ID: <string>、ユーザー <string>)
127	ACTX_INSTALL_PREVENTED	エラー	Trellix Solidifier が、ActiveX <string> のインストールを阻止しました (ワークフロー ID: <string>、ユーザー <string>)
129	VASR_VIOLATION_DETECTED	重大	Trellix Solidifier がプロセス '<string>' (プロセス ID: '<string>'、sha1: <string>、md5: <string>、sha256: <string>、ユーザー: <string>') の乗っ取りを阻止しました。再配置不能な DLL '<string>' からの実行を阻止しました。障害アドレス <string>。ターゲット アドレス '<string>'

表 5-4 TEC が記録するイベントログ一覧 (4/4)

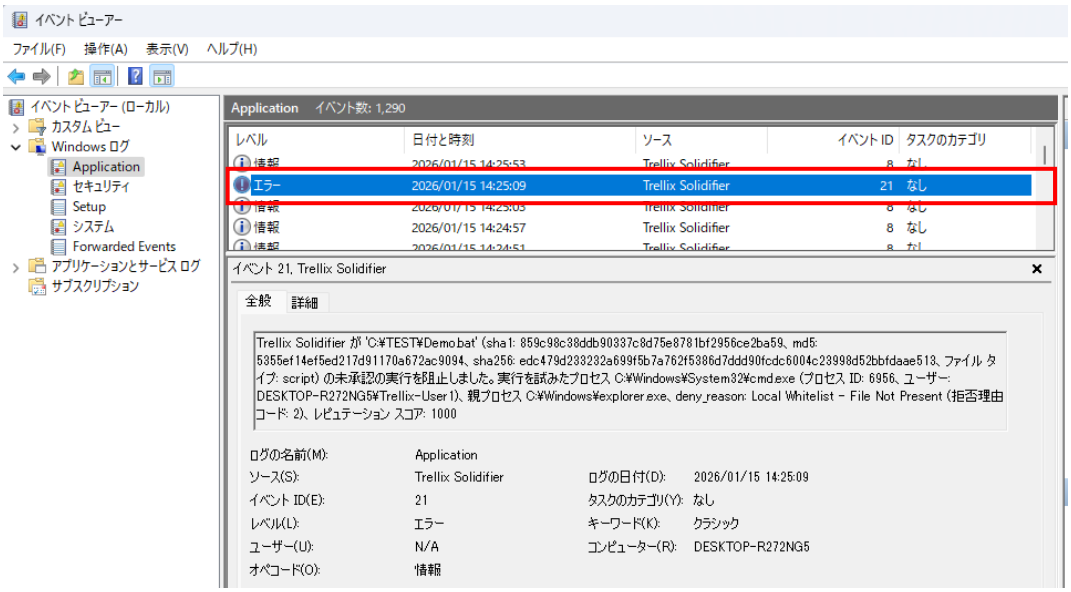
イベント ID	イベント名	レベル	説明
133	LOCAL_CLI_ACCESS_DISABLED	エラー	間違ったパスワードが入力されたため、ローカル CLI が無効になりました。<string> 分後に復旧できます
134	LOCAL_CLI_RECOVER_SUCCESS	情報	ローカル CLI が正常に復旧しました
135	LOCAL_CLI_RECOVER_FAILED	情報	ローカル CLI の復旧に失敗しました
136	OBSERVED_FILE_EXECUTION	情報	Trellix Solidifier が '<string>'(プロセス ID: <string>、sha1: <string>、md5: <string>、sha256: <string>、ユーザー: <string>、ワークフロー ID: <mode>: AUTO_2、original_procname: <string>、 parent_name = <string>) の開始を確認しました。コマンドライン: '<string>'
137	PREVENTED_FILE_EXECUTION	エラー	Trellix Solidifier が '<string>' (プロセス ID: <string>、sha1: <string>、md5: <string>、sha256: <string>、ユーザー: <string>、original_procname: <string>、parent_name = <string>) の開始をブロックしました。コマンドライン: '<string>'
138	INVENTORY_RECOVERED	重大	Trellix Solidifier が、ボリューム <文字列> でインベントリの破損を検出しました。<string> 付けのバックアップが読み込まれました
139	INVENTORY_RECOVER_FAILED	重大	Trellix Solidifier が、ボリューム〈文字列〉でインベントリの破損を検出しました。バックアップの読み込みができません。システムを確認してソリディフィケーションを実行し、許可リストを作成してください
140	BLOCKED_PROCESS_INTERACTIVE_MODE	重大	Trellix Solidifier が対話モードのプロセス <string> をブロックしました。(プロセス ID: <string>、sha1: <string>、md5: <string>、sha256: <string>、ユーザー: <string>、original_procname: <string>、parent_name = <string>)

管理対象外の環境でのイベントのリスト：

https://docs.trellix.com/ja-JP/bundle/application-change-control-8.4.x-product-guide-windows/page/UUID-bdb1805d-23bd-079c-9ace-bf28df029da6.html

5.1.3. イベント出力例

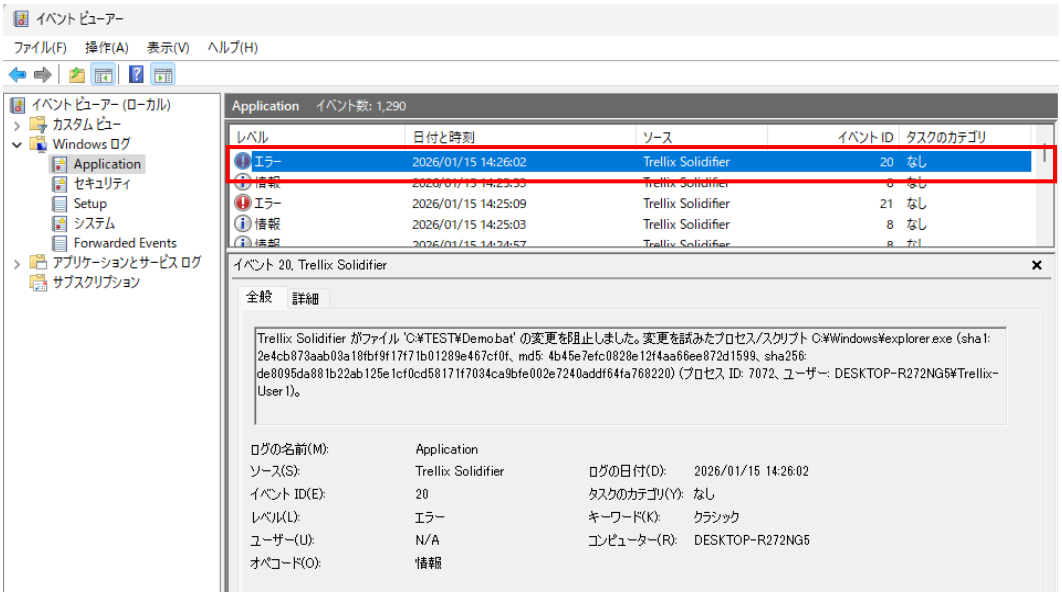
アローリストに登録されていないファイルを実行した場合、以下のエラーが出力されます。



… (A)

(A) 実行が阻止された場合、イベント ID:21 が出力されます。

アローリストに登録されているファイルを変更や削除しようとした場合に、以下のエラーが出力されます。



… (B)

(B) 変更が阻止された場合に、イベント ID:20 が出力されます。

5.1.4. イベントキャッシュサイズ設定

変更イベントは、ネットワークの攻撃などに対処するために、Trellix Embedded Control は、イベントをバッファに保存します。デフォルトで、このバッファサイズは、2MB に設定されています。

バッファサイズが閾値に近づくと、キャッシュがオーバーフローしそうであることが警告され、イベントはシステムログに記録されます。バッファの制限を超えると、バッファ内のイベント数がその高水位標を下回るまで新しいイベントは破棄されます。この上限を定義する高水位標を設定できます。同様に、低水位標を設定すると、キャッシュがオーバーフローから回復したことが示されます。

高水位標および低水位標は、それぞれ EventCacheWMHigh および EventCacheWMLow パラメータで設定できます。

・EventCacheWMHigh パラメータ入力値：50～100 の範囲（デフォルト値：90）

・EventCacheWMLow パラメータ入力値：20 以上（デフォルト値：70）

留意事項

- これらのパラメータを設定する際は、低水位標（EventCacheWMLow）の値が必ず高水位標（EventCacheWMHigh）より小さいことを確認してください。

イベントキャッシュサイズの値を設定する場合には、次のコマンドを実行します。

> sadmin config set EventCacheSize=< value >

高水位標を設定する場合には、次のコマンドを実行します。

> sadmin config set EventCacheWMHigh=<value>

低水位標を設定する場合には、次のコマンドを実行します。

> sadmin config set EventCacheWMLow=< value >

5.1.5. ログファイルサイズの設定

Trellix Embedded Control によって作成されたログファイル(solidcore.log)サイズは、LogFileSize パラメータを使用して設定できます。デフォルトサイズは、2048KB です。

このパラメータを 0 に設定すると、デフォルト値が適応されます。

また、ファイルサイズが 2048KB に到達すると、このログファイルは solidcore.log.1 にリネームされ、新しいログファイル solidcore.log が生成されます。

ログファイルのサイズを設定する場合には、次のコマンドを実行します。

> sadmin config set LogFileSize=<size>

※パラメータ LogFileSize は、ファイルサイズを KB 単位で保存します。

5.1.6. ログファイル数の設定

作成されるログファイル(solidcore.log)の数は、LogFileNum パラメータを使用して設定できます。このパラメータのデフォルト値 4 です。

これは、solidcore.log ファイルから solidcore.log.4 ファイルまでの最大 5 つのログファイルが作成されます。システム内に作成するログファイルの最大数に制限はありません。

このパラメータを 0 に設定すると、デフォルト値である 4 が適応されます。

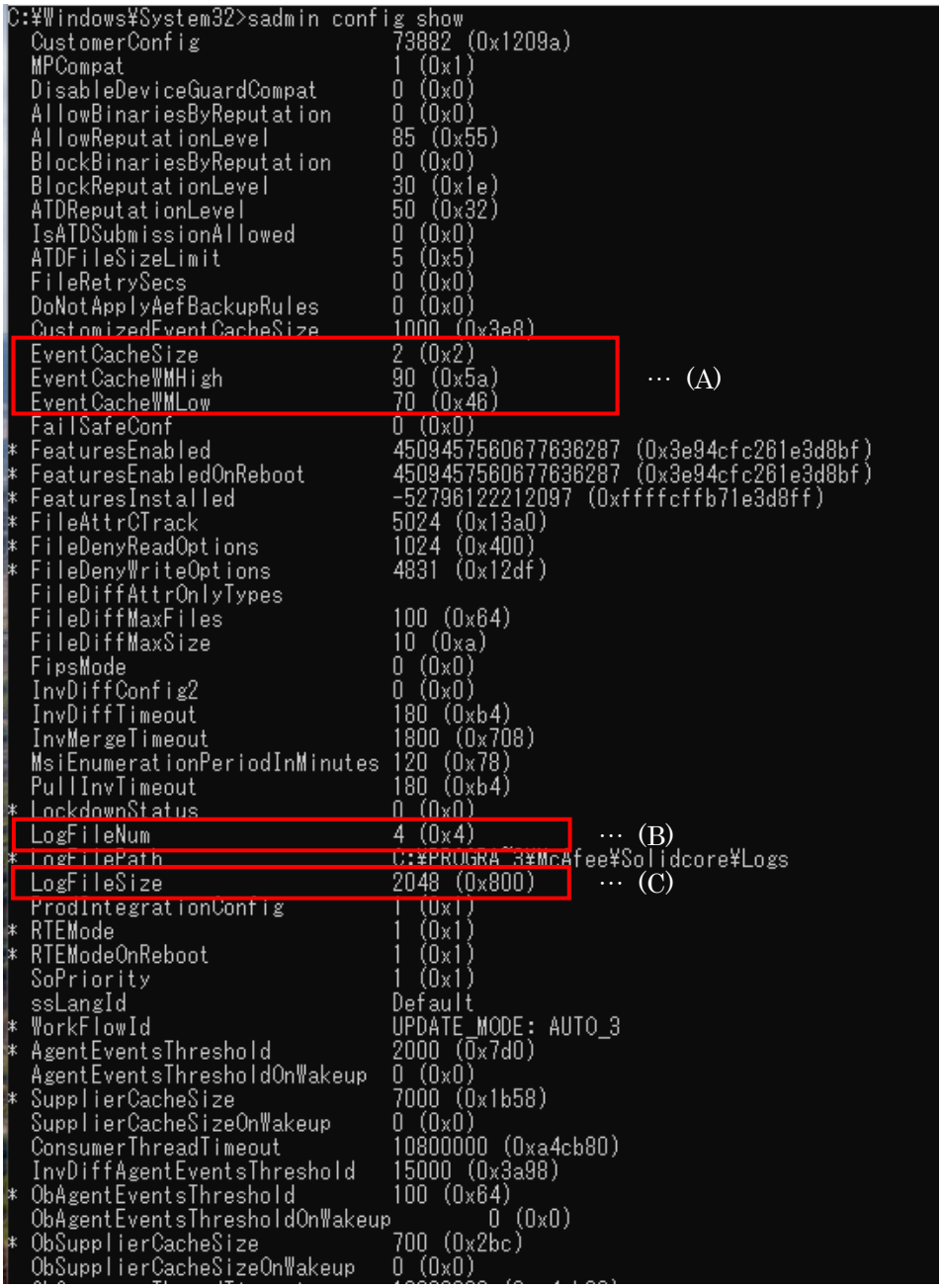
ログファイルの数を設定する場合には、次のコマンドを実行します。

> sadmin config set LogFileNum=<no>

5.1.7. 拡張設定パラメータの確認

次のコマンドを実行することで、設定パラメータアイテムリストを出力します。
各パラメータの設定値を確認できます。

> sadmin config show



(A) イベントキャッシュサイズのデフォルト値

(B) ログファイル数のデフォルト値

(C) ログファイルサイズのデフォルト値

5.2. トラブルシューティング

Trellix Embedded Control が動作している環境で問題が発生した場合、障害解析のためにシステム内の情報や Trellix Embedded Control の動作ログを収集する必要があります。

この節では、トラブルシューティングのための情報収集ツールとその使い方について説明します。

5.2.1. GatherInfo ツール

GatherInfo ツールは、トラブルシューティングで必要となるログファイル、インベントリ、バージョン、システム情報などに関連した情報が収集されます。

本ツールは以下のディレクトリにインストールされます。

デフォルトの場所：C:¥Program Files¥McAfee¥Solidcore¥Tool¥GatherInfo

5.2.2. GatherInfo ログ取得方法

このツールによりログデータを取得する場合、以下の手順を実行してください。

① Trellix Solidifier コマンドラインにて、次のコマンドを実行します。

> gatherinfo



以下のパラメータをこのコマンドに使用できます。

-h：GatherInfo のヘルプを表示します。

-v：GatherInfo のバージョンを表示します。

-q：クワイエットモードでログを収集します。

-x：セキュリティログを除外してログを取集します。

② GatherInfo ツール実行結果にエラーの記録がないことを確認してください。

```
C:¥Windows¥System32>gatherinfo

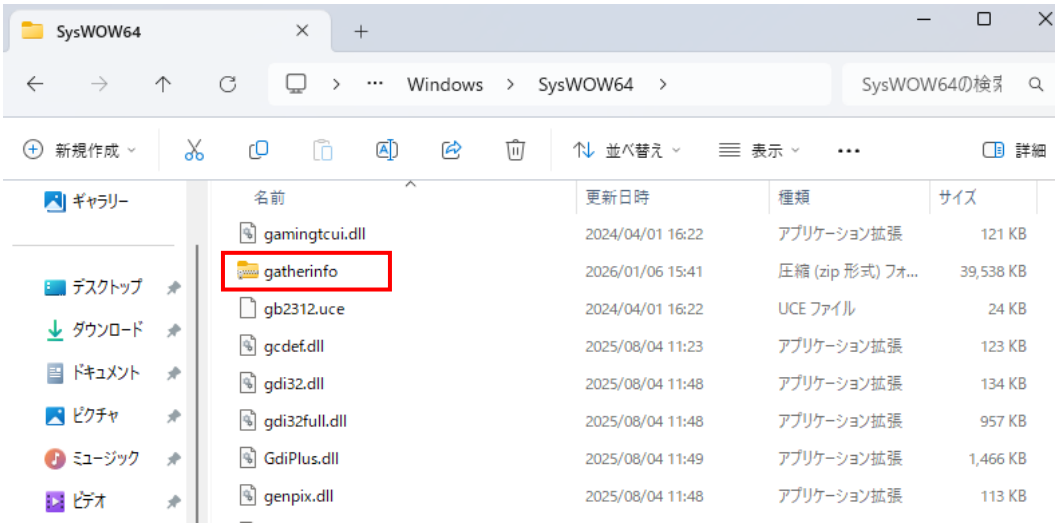
C:¥Windows¥System32>REM Copyright (C) 2024 Musarubra US, LLC.  All rights reserved.
gatherinfo version - 8.4.4
Deleting old Directory...
Creating new Directory...
Copying the event files...
Taking Application Event Log Dump...
Taking System Event Log Dump...
Retrieving msinfo32 log file...
Taking HostName file...
Retrieving Solidifier Installer log file...
Collecting DEP status...
Retrieving Solidifier log files...
Retrieving McAfee scanalyzer data...
Scanalyzer data "C:¥Windows¥System32¥data"
C:¥Windows¥System32¥data¥scan_DESKTOP-R272NG5_06Jan2026_154040.txt
        1 個のファイルを移動しました。
Scanalyzer previous data "C:¥PROGRA~1¥McAfee¥SOLIDC~1¥Tools¥GATHER~1¥¥..¥scanalyzer¥data"
C:¥PROGRA~1¥McAfee¥SOLIDC~1¥Tools¥GATHER~1¥¥..¥scanalyzer¥data¥scan_DESKTOP-R272NG5_22Dec2025_164813.txt
        1 個のファイルをコピーしました。
アクセスが拒否されました。
        0 個のファイルをコピーしました。
Retrieving the Product info ...
Retrieving solidcore folder on each drive...
Retrieving Registry...
Zipping Files...
Deleting data directory ...
ディレクトリが空ではありません。
C:¥Windows¥System32>
```

… (A)

(A) 出力内容にエラー記録がないことを確認します。

③ コマンドが正常に完了すると、以下の保存場所に gatherinfo.zip ファイルが作成されます。

保存場所：C:¥Windows¥SysWOW64



第6章 RunProtector™ のアンインストール

6.1. アンインストールする前に

この節では、RunProtector™ のアンインストールに際して、事前準備について説明します。

6.1.1. 事前の準備

RunProtector™ のアンインストールを開始する前に、ご使用の OS に応じて以下のインストール/アンインストール DVD を準備してください。

OS の種別	準備するインストール/アンインストール DVD
クライアント向け OS	RunProtector for Devices (S-763A-A2P)
サーバー向け OS	RunProtector for Servers (S-763A-A3P)

6.2. RunProtector™ をアンインストールする

この節では、RunProtector™ のアンインストール方法について説明します。なお、アンインストールはコンピューターの管理者アカウントでサインインして行ってください。

① TEC を無効化します。
TEC を無効化する手順については、「3.3. Trellix Embedded Control の有効化／無効化」を参照してください。
② DVD ドライブに RunProtector™ のインストール/アンインストール DVD をセットします。
③ 「スタート」ボタンをクリックします。
④ 「すべて」―「Windows ツール」―「コマンドプロンプト」を右クリックし、
「管理者として実行」を選択します。
⑤ アンインストーラーを起動します。
コマンドラインに以下を入力して[Enter]キーを押します。

D:¥RunProtectorUninstaller.exe

※ ここでは、DVD メディアでのアンインストール手順として、DVD ドライブのドライブ文字を D ドライブと仮定したパスを指定しています。下線部のパスはセットアッププログラムが格納されている場所に応じて変更してください。

⑥ 「Would you like to proceed with the uninstallation of the RunProtector?」のダイアログが表示されたら「はい」を押下するとアンインストールが開始されます。
※ アンインストール処理はすべて自動で行われます。
アンインストールが完了するまで 1 分程度かかります。
⑦ アンインストール完了後、「Uninstallation complete.」のダイアログが表示されますので「OK」ボタンを押下してアンインストーラーを終了します。
⑧ システムを再起動します。
⑨ 以下の項目の確認をしてください。
・デスクトップに"Trellix Solidifier コマンドライン"のショートカットが存在しないこと。
・[設定]-[アプリ]-[インストールされているアプリ]に、「Trellix Solidifier」が存在しないこと。

以上で RunProtector™ のアンインストールは完了です。

6.3. アンインストール中に出力されるエラーメッセージについて

アンインストール中にエラーが発生すると、エラーを示すポップアップメッセージが出力されます。その原因について以下に示します。

エラーを示すポップアップメッセージが出力された場合、OK ボタンを押下するとアンインストーラーは処理を中断して終了します。

表 6-1 アンインストール中のエラーメッセージ一覧

No.	出力メッセージ	原因
1	Not the product to be installed.	稼働中の OS が、RunProtector™ をアンインストールするための条件を満たしていません。