

実行禁止ファイルから完全な保護

ザーガイド



www.faronics.com



最新更新日:2023年1月

©1999–2023 Faronics Corporation. All rights reserved. Faronics、Deep Freeze、Deep Freeze Cloud、Faronics Deploy、Faronics Core Console、Faronics Anti-Executable、Faronics Anti-Virus、Faronics Device Filter、Faronics Data Igloo、Faronics Power Save、Faronics Insight、Faronics System Profiler、WINSelect は Faronics Corporation の商標および / または登録商標です。その他すべ ての会社名および製品名はそれぞれの所有者の商標です。



目次

序文	5
重要な情報 Faronicsについて 製品マニュアル	6 6 6
テクニカルサポート お問い合わせ	7 7
用語の定義	8
はじめに	10
Anti-Executable概要 Anti-Executableについて Anti-Executableのエディションについて	11 11 11
$\Delta nti-Fvecutable $ $0 = 7.4 \times 7$	12
	10
Anti-Executableのインストール	15
インストール概要	16
Anti-Executable Standardのインストール	17
Anti-Executable Standardへのアクセス	20
Anti-Executableの使用	21
概要	22
Anti-Executableの設定	23
ステータスタブ 製品情報の確認 Anti-Executable保護の有効化. Anti-ExecutableのMaintenance Mode.	24 24 25 25
実行管理リストタブ	26
ユーザータブ Anti-Executable管理者または信頼ユーザーの追加 Anti-Executable管理者または信頼ユーザーの削除 Anti-Executableパスワードの有効化	27 27 29 29
[一時実行モード]タブーー時実行モードの有効化または無効化	30 31
セットアップタブ Anti-Executableでのイベントログの設定. DLL実行のモニタ. JAR実行のモニタ. VBScript実行のモニタ. PowerShellスクリプト実行のモニタ. Anti-Executableのステルス機能. 互換性オプション. アラートのカスタマイズ.	32 32 33 33 33 33 33 33 33 34 36
Anti Evoquitable O Z V Z L - II	27
Anti-Executableのアンインストール	31
Anti-Executable Standardのアンインストール	38

4 目次





Faronics Anti-Executable は、許可された実行可能ファイルのみをワークステーション やサーバーで実行できるようにすることにより、エンドポイントでのセキュリティを確 実にするソリューションです。

トピック

重要な情報 テクニカルサポート 用語の定義

序文





このセクションには Anti-Executable についての重要な情報を記載しています。

Faronics について

Faronics は、マルチユーザーコンピューティング環境の管理、簡素化、安全保護を支援するソフトウェアを提供します。当社の製品は、ワークステーションの 100% の可用性を保証し、IT 担当者を面倒な技術サポートやソフトウェアの問題から解放してきました。学校施設をはじめ、医療機関、図書館、政府組織、または法人企業でFaronicsの顧客中心の取り組みによるパワフルなテクノロジー改革を有効にご使用いただいています。

製品マニュアル

Faronics Anti-Executable のテクニカルガイドは、以下のマニュアルで構成されています:

- Faronics Anti-Executable ユーザーガイド このマニュアルでは製品の使用方法を 説明します。
- Faronics Anti-Executable リリースノート このドキュメントには新しい機能、既 知の問題、解決された問題が記載されています。
- Faronics Anti-Executable の機能説明書 この説明書には最新の機能が記載されています。
- Faronics Anti-Executable readme.txt このドキュメントではインストールプロセ スを説明します。



テクニカルサポート

当社では、使いやすく、問題のないソフトウェアを設計するためにあらゆる努力を重ねています。万が一、問題が発生した場合は、テクニカルサポートまでご連絡ください。
Web:support.faronics.com
マリーダイヤル(北米):1-800-943-6422
電話番号:1-604-637-3333
営業時間:月曜日~金曜日 午前7時から午後5時(太平洋標準時刻)

お問い合わせ

本社:

Faronics Corporation 609 Granville St., Suite 1400 Vancouver, BC V7Y 1G5, Canada

Web:www.faronics.com

電子メール :sales@faronics.com 電話番号 :800-943-6422 または 604-637-3333 ファックス :800-943-6488 または 604-637-8188 営業時間 : 月曜日~金曜日 午前7時から午後5時(太平洋標準時刻)

Faronics Technologies USA Inc. 5506 Sunol Blvd, Suite 202 Pleasanton, CA, 94566, USA

Faronics EMEA 8, The Courtyard, Eastern Road Bracknell, Berkshire RG12 2XB, United Kingdom

Faronics Pte Ltd 160 Robinson Road #05-05 SBF Center Singapore 068914

用語	定義
アラート	実行禁止ファイルを起動しようとすると、表示される通知ダイアロ グです。Anti-Executable の管理者は、アラートのメッセージと画 像を指定できます。
Anti-Executab le 管理者	Anti-Executable 管理者は、すべての Anti-Executable 設定オプ ションにアクセスできます。Anti-Executable ユーザーの管理、 Anti-Executable 保護の有効化または無効化の設定、 Anti-Executable のアンインストールやアップグレードを行うこと ができます。
Anti-Executab le 信頼ユー ザー	Anti-Executable の保護を「有効」または「無効」に設定できま す。Anti-Executable をアンインストールしたりアップグレードす ることはできません。
実行可能ファイ ル	オペレーティングシステムによって実行できるすべてのファイル。 Anti-Executable によって管理される実行可能ファイルで、.scr、 .jar、.bat、.com、または .exe という拡張子が付いているもの。.dll という拡張子が付いたダイナミックリンクライブラリは、[設定] タブで設定されていれば管理されます。
実行管理リス ト	実行管理リストは、Anti-Executable がファイルまたは発行者を管 理する方法を定義します。この実行管理リストは、ファイルを「許 可」または「ブロック」するかどうかを定義します。
外部ユーザー	Anti-Executable 管理者ユーザーまたは Anti-Executable 信頼ユー ザーのいずれでもないその他すべてのユーザー。 外部ユーザーは、実行許可ファイルのみを実行でき、 Anti-Executable の構成を操作することはできません。オペレー ティングシステムによって指定されたユーザー権限に関係なく、こ の制限は適用されます。
JAR	JAR (Java ARchive) は、多数の Java クラスファイル、関連するメ タデータとリソース (テキスト、画像など)を1つのファイルにま とめたアーカイブファイル形式の1つで、Java プラットフォーム でのアプリケーションソフトウェアまたはライブラリの配布に使用 されます。
Maintenance Mode	Maintenance Mode になっているときに、追加または修正された新 しい実行可能ファイルは、自動的にローカル管理リストに追加され ます。



用語	定義
保護	[有効化]に設定すると、一括管理リストとローカル管理リストに 基づいて、Anti-Executable によりワークステーションが保護され ていることをこの設定が示します。[無効化]に設定すると、あら ゆる実行可能ファイルをワークステーション上で実行することがで きます。
発行者	発行者とはファイルの作成者を指します。発行者はデジタル署名で ファイルを認証します。Anti-Executable では、発行者の名前、製品 のファイル名、バージョンの詳細を使って、発行者が作成したファ イルを識別します。
ステルスモー ド	ステルスモードは、システム上の Anti-Executable の存在を視覚的 に示すアイコンなどを管理する複数のオプションです。ステルス モードでは、管理者は、Windows のシステムトレイで Anti-Executable のアイコンを非表示にしたり、アラートが表示さ れないようにするオプションを利用できます。
—時実行モー ド	ー時実行モードにより、指定期間中、Anti-Executable からの操作 なしで、ユーザーは実行可能ファイルを実行できます。この期間中 は、制限を受けずに、実行可能ファイルを実行することができま す。ブロックされた実行可能ファイルは、実行が許可されません。
信頼実行可能 ファイル	信頼実行可能ファイルでは、実行禁止になっているその他の実行可 能ファイルを実行することができます。
実行禁止ファイ ル	実行禁止ファイルは、実行が許可されていないファイルです。



はじめに

Anti-Executable は、許可されたアプリケーションのみをコンピュータまたはサーバー 上で実行できるようにすることによって、エンドポイントの完全な生産性を保証しま す。プログラムが有害であるか、無許可であるか、または不必要であるかに関わらず、 無許可プログラムの実行は常にブロックされます。

トピック

Anti-Executable 概要 システム要件 Anti-Executable のライセンス



Anti-Executable について

Faronics は、マルチユーザーコンピューティング環境の管理、簡素化、安全保護を支援するソフトウェアを提供します。当社の製品は、ワークステーションの 100% の可用性を保証し、IT 担当者を面倒な技術サポートやソフトウェアの問題から解放してきました。学校施設をはじめ、医療機関、図書館、政府組織、または法人企業で Faronics の顧客中心の取り組みによるパワフルなテクノロジー改革を有効にご使用いただいています。

Anti-Executable のエディションについて

Faronics Anti-Executable には 4 つの異なるエディションがあります。サーバーまたは ワークステーションであろうと、スタンドアロンまたはネットワークの一部であろう と、Anti-Executable は必要とされる保護を提供します。ニーズに最も適した Anti-Executable のエディションを選択してください。

エディション	保護のために使用する Anti-Executable
Standard	非サーバーオペレーティングシステムが稼働している1台のス タンドアロンコンピュータ
Server Standard	サーバーオペレーティングシステムが稼働している1台のスタ ンドアロンコンピュータ
Enterprise	非サーバーオペレーティングシステムが稼働している複数のコ ンピュータ
Server Enterprise	サーバーオペレーティングシステムが稼働している複数のコン ピュータ



システム要件

Anti-Executable は、以下のオペレーティングシステムにインストールできます。

- Windows 7、Windows 8.1、Windows 10 バージョン 22H2 まで、Windows 11 バージョン 22H2 までの 32 ビット版および 64 ビット版
- Windows Server 2008 R2 、Windows Server 2012、Windows Server 2016、 Windows Server 2019、Windows Server 2022



Anti-Executable のライセンス

Anti-Executable には完全版と評価版があります。評価版は無料で Faronics のウェブサ イト (www.faronics.com) からダウンロードできます。評価版をインストールすると 30 日間使用できます。評価版の有効期限が切れると、コンピュータは保護されません。ア ンインストールするか、完全版にアップグレードする必要があります。完全版でコン ピュータを保護するには、有効なライセンスキーが必要です。



Anti-Executable サーバー版は、非サーバーオペレーティングシステムに インストールすることはできません。Anti-Executable サーバー版のライ センスキーは、非サーバー版で使用することはできません。

Anti-Executable 非サーバー版は、サーバーオペレーティングシステムに インストールすることはできません。Anti-Executable 非サーバー版のラ イセンスキーは、サーバー版で使用することはできません。 **14** はじめに





Anti-Executable のインストール

この章では Anti-Executable のインストールプロセスについて説明します。

トピック

インストール概要 Anti-Executable Standard のインストール Anti-Executable Standard へのアクセス



インストール概要

Anti-Executable は、Windows Server 2008 R2、Windows Server 2012、Windows Server 2016、Windows Server 2019、Windows Server 2022、32 ビット版および 64 ビット版の Windows 7、Windows 8.1、Windows 10 バージョン 22H2 まで、Windows 11 バージョン 22H2 までにインストールできます。

システム	インストールファイル
Windows(非サーバー)(32 ビット)	AEStd_32-bit.msi
Windows(非サーバ)(64 ビット)	AEStd_64-bit.msi
Windows Server (32 ビット)	AESrvStd_32-bit.msi
Windows Server (64 ビット)	AESrvStd_64-bit.msi



Anti-Executable Standard のインストール

Anti-Executable Standard をインストールするには、以下の手順を実行します。

1. .msi ファイルをダブルクリックして、インストールプロセスを開始します。[次へ] をクリックして、続行します。



2. 使用許諾契約書に同意します。[次へ]をクリックして、続行します。





3. ユーザー名と組織を入力します。[次へ]をクリックして、続行します。

<u>U</u> ser Name:			
core			
Organization:			
License <u>K</u> ey:		_	
Use Evaluation (30 day	s)		

4. [インストール先フォルダ]を指定します。デフォルトの場所は、C:\Program Files\Faronics\AEです。[次へ]をクリックして、続行します。

岁 Faronics Anti-Executable Standard Edition - Setup Wizard	
Destination Folder Select a folder where the application will be installed.	
Install Faronics Anti-Executable Standard Edition to:	
C: \Program Files \Faronics \AE \	
Browse	
	Version 5.00.1111.513
< Back	Next > Cancel



5. AE Administrator のユーザーパスワードと AE 信頼ユーザーのパスワードを指定します。[次へ]をクリックして、続行します。

stallation Configuration ter the following information to pe	ersonalize your installation.	Ğ
AE Administrator User Passwo	ord (Optional)	
Enter Password:		
Re-Enter Password:		
AE Trusted User Password (O	ptional)	
Enter Password:		
Enter Password:		

- 以下のオプションを選択して、[インストール]をクリックします。
 Anti-Executable によりコンピュータがスキャンされ、すべてのファイルと発行者の リストを含む管理リストが作成されます。
 - > 管理リストの作成時に DLL ファイルを含める DLL を含める場合は、このオプ ションを選択します。

😸 Faronics Anti-Executable Standard Edition - Setup V	Nizard 🗖 🗖 💌
Ready to install program The wizard is ready to begin installation.	
Automatic Scanning	
Click Install to begin the installation. If you want to review or change any of your installati	on settings, dick Back. Click Cancel
to exit the wizard and terminate the installation proce	Version 5.50.1111.655
< <u>B</u> ao	

7. [OK] をクリックして、コンピュータを再起動します。後でコンピュータを再起動す るには、[キャンセル]をクリックします。



8. [完了]をクリックして、インストールを終了します。



Anti-Executable Standard へのアクセス

Anti-Executable は、ワークステーション上で Shift キーを押したまま、Windows のシ ステムトレイの Anti-Executable アイコンをダブルクリックして、アクセスできます。 また、Ctrl+Alt+Shift+F10 ホットキーを使用することもできます。

管理者は、[ステータス]、[実行管理リスト]、[ユーザー]の各タブにアクセスでき ます。信頼ユーザーは、[ステータス]タブと[実行管理リスト]タブのみにアクセス できます。

外部ユーザーは Anti-Executable にアクセスできません。パスワードが設定されている 場合、Anti-Executable 管理者および信頼ユーザーが Anti-Executable にアクセスする には、適切なパスワードを入力する必要があります。



Anti-Executable の使用

この章では Anti-Executable の構成と使用手順について説明します。

トピック

概要 ステータスタブ 実行管理リストタブ ユーザータブ [一時実行モード]タブ セットアップタブ レポートタブ



Anti-Executable は、保護強化のために複数の管理リストを提供します。以下のコン ポーネントがあります。

 実行管理リストは、Anti-Executable がファイルまたは発行者を管理する方法を定 義します。この実行管理リストは、ファイルまたは発行者を「許可」または「ブ ロック」するかどうかを定義します。

Anti-Executable は、一般的に知られているパブリッシャのリストで事前に作成されています。このリストは必要に応じて更新されます。

 ファイルと発行者のローカルリスト(管理リスト)-Anti-Executableをワークス テーションに初めてインストールすると、Anti-Executableによりワークステー ションがスキャンされ、許可されたすべてのファイルと発行者のリストが作成され ます。



Anti-Executable の設定

Anti-Executable には以下のタブがあります。

- ・ ステータス
- 実行管理リスト
- ・ ユーザー
- 一時実行モード
- ・ セットアップ



ステータスタブ

[ステータス]タブにより、Anti-Executable 管理者と信頼ユーザーは、さまざまな設定、保護の有効化、無効化、Maintenance Modeの設定などが行えます。

バージョン情報	
	BLE
製品: Faronics Anti-Executable Standard	
バージョン: 5.20.1111.555	
ライセンスキー: 編	集(E) 有効期限:11月 14, 2012
保護	設定
◎ 有効化(N)	
● 無効化(L)	インポート (1)
メンテナンスモード(T)	
■通知間隔(R) 1 ▼ 分 ▼	エクスポート (X)

製品情報の確認

[バージョン情報]ペインには、インストールされている Anti-Executable のバージョンが表示されます。新しいバージョンがある場合、「新規バージョンが利用可能です」と表示されます。詳細は、[更新]をクリックしてください。

Anti-Executable の評価版がインストールされている場合は、[有効期限]フィールド には、Anti-Executable の有効期限が切れる日付が表示されます。Anti-Executable で は、Windows のシステムトレイに現在のライセンス状況について表示されます。

評価期間の期限が切れると、Anti-Executable でコンピュータが保護されません。 Anti-Executable の有効期限が切れると、以下のアイコンが表示されます。

6

Anti-Executable の評価版を完全版に変換するためには、[編集]をクリックし、[ライ センスキー]フィールドに有効なライセンスキーを入力します。ライセンスキーは Faronics または Faronics パートナーに連絡して入手することができます。



Anti-Executable 保護の有効化

インストール後に、デフォルトで Anti-Executable が有効になります。 保護が無効の場合に、ワークステーション上で Anti-Executable の保護を有効にするように通知させるには、[通知間隔]チェックボックスを使用します。

Anti-Executable の Maintenance Mode

Maintenance Mode で Anti-Executable を実行するには、[Maintenance Mode] を選択 して、[適用]をクリックします。Maintenance Mode になっているときに、追加また は修正された新しい実行可能ファイルは、自動的に実行管理リストに追加されます。 Maintenance Mode を終了するには、[有効化]または[無効化]を選択します。

[有効化] を選択すると、Anti-Executable で変更が記録されます。[無効化] を選択す ると、Anti-Executable で変更は記録されません。



コンピュータが Maintenance Mode で実行されている間は、Windows Updates のために十分な時間を取る必要があります。



コンピュータが Maintenance Mode で実行されていて、保護が無効に なっている場合、Maintenance Mode の間にワークステーションに対し て行われた変更は実行管理リストに追加されません。



実行管理リストタブ

[実行管理リスト]タブにより、一括管理リストにある項目を許可するかブロックするかを指定できます。

2. 前	AETZDSUNY	1壬米百	187
		「生大只	112
adaptertroubleshoo	. 🔮 計門	ファイル	c:¥windows¥system32¥a
addinprocess.exe	◎ 計□]	ファイル	c:¥windows¥microsoft.ne
ddinprocess32.exe	🧭 i千 o J	ファイル	c:¥windows¥microsoft.ne
addinutil.exe	🥝 許可	ファイル	c:¥windows¥microsoft.ne
L aec.exe	🥥 許可	ファイル	c:¥users¥core¥appdata¥
🔝 aeengine.exe	🥝 許可	ファイル	c:¥program files¥faronics
itagent.exe	🤣 許可	ファイル	c:¥windows¥system32¥a
II alg.exe	🥝 許可	ファイル	c:¥windows¥system32¥a
III antiexecutable.exe	🤣 許可	ファイル	c:¥program files¥faronics
appcmd.exe	🥝 許可	ファイル	c:¥windows¥winsxs¥x86
append.exe	🤣 許可	ファイル	c:¥windows¥system32¥a
appidcertstorecheck.	🥥 許可	ファイル	c:¥windows¥system32¥a
	🕗 許可	ファイル	c+¥windows¥system37¥a
•	III		•

Anti-Executable の動作を指定するには、以下の手順を実行します。

1. [ファイルとフォルダの表示]または[発行者の表示]を選択します。

- 2. [ファイルとフォルダの表示]を選択すると、以下の列が表示されます。
 - > 名前
 - > AE アクション
 - > ソース
 - > 信頼
 - > 種類
 - > パス
 - > 追加データ
 - > コメント
- ファイルまたはフォルダを一括管理リストおよび実行管理リストに追加するには、[追加]をクリックします。実行管理リストから削除するには、項目を選択して、[削除]をクリックします。項目を選択して、[許可]または[ブロック]をクリック します。
- 4. [適用]をクリックします。[OK]をクリックします。



ユーザータブ

Anti-Executable では、ユーザーが利用可能な機能を決定するために、Windows のユー ザーアカウントが使用されます。以下の2種類のAnti-Executable ユーザーがありま す。

- 管理者ユーザー 一括管理リスト、ローカル管理リスト、実行管理リスト、ユー ザー、およびセットアップの管理と Anti-Executable のアンインストールができま す。
- 信頼ユーザー Anti-Executable と実行管理リストを設定できます。Anti-Executable のアンインストールは禁止されています。ユーザーまたはセットアップを管理することはできません。

デフォルトでは、Anti-Executable のインストールを行う Windows ユーザーアカウン トが、最初の Anti-Executable 管理者ユーザーになります。その後、この管理者ユー ザーは、既存の Windows ユーザーを、Anti-Executable に追加することができます。

Anti-Executable が有効になっているときに、Anti-Executable 管理者または信頼ユー ザーが無許可のアプリケーションを開こうとすると、[アラート]ダイアログが表示さ れます。

Anti-Executable 管理者または信頼ユーザーの追加

すべての Anti-Executable ユーザーは、既存の Windows ユーザーアカウントです。ただし、すべての Windows ユーザーアカウントが自動的に管理者または信頼ユーザーになるわけではありません。管理者または信頼ユーザーではない Windows ユーザーアカウントは外部ユーザーです。

Anti-Executable にユーザーを追加するには、以下の手順を実行します。

1. Anti-Executable ウインドウの上部の [ユーザー] タブをクリックします。

🖁 core	
	2世70(A) 自归除 (R)
ワード E 信頼ユーザ	2旦70(A)
ワード E 信頼ユーザ]有効化 (N)	2570(A) 創除(R) AE 管理者 同有幼化(E)
ワード E 信頼ユーザ ■ 有効化 (N) 折しいパスワード	2570 (A) 前期除(R) AE 管理者 同有幼化(E) 新し、パスワード



2. [追加]をクリックして、新規ユーザーを追加します。提示されたリストから、 ユーザーアイコンを選択します。

elect Users	8
Select this object type:	
Users	Object Types
From this location:	
WINDOWS	Locations
Enter the object names to select (<u>examples</u>):	
	Check Names

 [詳細]>[検索]をクリックして、利用可能なユーザーのリストを表示します。 Anti-Executable 管理者は、ドメインユーザー(またはグループ)とローカルユー ザー(またはグループ)を追加できます。Anti-Executable のリストにユーザーを追 加するには、ユーザーまたはグループをクリックして、[OK]をクリックします。

Users		Object Types
From this location:		
WINDOWS		Locations
Common Queries		
Name: Starts wi	ith 💌	Columns
Description: Starts wi	ith 💌	Find Now
Disabled accounts		Stop
Horr expiring passive	old	
Days since last logon:	*	<i>~</i>
Days since last logon:	*	OK Cancel
Days since last logon: Gearch results: Lame (RDN) In Fold	der	OK Cancel
Days since last logon: Search results: Lame (RDN) In Fold Administrator WIND	der	OK Cancel
Days since last logon: Search results: Iame (RDN) In Fok Administrator WIND Corre WIND	der der 00WS 00WS	OK Cancel
Days since last logon: Gearch results: Iame (RDN) In Fold Administrator WIND Core WIND Guest WIND	der 10WS 10WS 10WS	OK Cancel
Days since last logon: Gearch results: Lame (RDN) In Fold Administrator WIND Core WIND Guest WIND	der 00WS 00WS 00WS	OK Cancel
Days since last logon: Gearch results: Iame (RDN) In Fold Administrator WIND Core WIND Guest WIND	der 100WS 100WS 100WS	OK Cancel

 デフォルトでは、追加された各ユーザーは Anti-Executable 信頼ユーザーになります。新規ユーザーに管理者権限を与える場合、[Anti-Executable Admin ロール] チェックボックスを選択して、Anti-Executable 管理者として指定します。



Anti-Executable 管理者または信頼ユーザーの削除

[ユーザー]タブをクリックし、削除するユーザーを選択します。[削除]をクリックし ます。これにより Windows ユーザーアカウントは削除されません。これでユーザーは 外部ユーザーになります。

Anti-Executable パスワードの有効化

保護の強化として、Anti-Executable では、各ユーザーグループにパスワードを付加す ることができます。パスワードは関連づけられたグループのメンバーのみに適用されま す。パスワードを指定するには、[有効化]チェックボックスが選択されていることを 確認し、[新しいパスワード]フィールドと[パスワードの確認]フィールドにパス ワードを入力します。変更を保存するには、[適用]をクリックします。

ユーザ	「美口 E 427AT」エーク	
AE	信頼	AE Admin ロール
2	core	
	[追加 (A) 肖耶徐 (R)
-KAD-	- ド ≣≢≣つ+#	AF 管理者
	有効化 (N)	□ 有効化 (E)
2		新しいパスワード
こ 一 新し	んパスワード	and a second sec



[一時実行モード]タブ

ー時実行モードにより、指定期間中、Anti-Executable からの操作なしで、ユーザーは 実行可能ファイルを実行できます。この期間中は、制限を受けずに、実行可能ファイ ルを実行することができます。一時実行モードの期間が終了すると、Anti-Executable が有効になります。[一時実行モード]タブにポリシーの情報が表示されます。[一時 実行モード]タブの設定はワークステーションでは変更できません。

以下のオプションが一時実行モ-	- ドで使用できます。
-----------------	-------------

S Faronics Anti-Executable Standard	
ステータス 実行管理リスト ユーザ 一時実行モード セットアップ レポート	
☑ 次のユーザは一時実行モードにアクセスできます(A) Anti-Executable管理者のみ	•
✓ 一時実行モードのログ制限(L) 4 ローリングログファイル最大 10 MB、40 ME	ディスク総容量
OK キャンセル 適用	

- 次のユーザーは一時実行モードにアクセスできます このチェックボックスを選択 すると、特定のユーザーが各自のシステムで一時実行モードを有効にできます。[すべてのユーザー]、[Anti-Executable ユーザー]、[Anti-Executable 管理者のみ] を選択します。
- 一時実行モードのログ制限 このチェックボックスを選択すると、一時実行モード 中にログファイルが作成されます。
 - > ログファイルの数 ログファイルの数を指定します(最大 10 ファイルまで)。ロ グ情報はファイルに連続的に保存されます。たとえば、A、B、Cという3つの ファイルがある場合、Faronics Anti-Executable では最初にファイルAにエラー ログが書き込まれます。ファイルAが一杯になると、ファイルBに書き込み、 最後にファイルCに書き込みます。ファイルCが一杯になると、ファイルAの データが消去され、新しいログデータがそれに書き込まれます。
 - > ファイルのサイズ 各ファイルのサイズを MB で選択します。それぞれが 10 MB の 10 のログファイル (合計 100 MB)を作成することができます。



一時実行モードの有効化または無効化

- ・ 一時実行モードの有効化:システムトレイで Anti-Executable アイコンを右クリックし、[一時実行モード]> [x 分](最長 60 分、24 時間、または7日のいずれかを選択)の順に選択します。
- 一時実行モードの無効化:システムトレイで Anti-Executable アイコンを右クリックし、[一時実行モード]>[無効]の順に選択します。

[一時実行モード]が有効になると、ワークステーションのシステムトレイに以下のアイコンが表示されます。





-時実行モードが終了する3分前にメッセージがワークステーションに 表示されます。



ー時実行モード中は、Windowsの自動更新は無効になります。



セットアップタブ

Anti-Executable 管理者は、さまざまなユーザーのアクションをログに記録するために ロギングの設定、ステルスモードのさまざまな設定の適用、アラートの設定、互換性 の有効化などができます。

S Faronics Anti-Executable S	tandard		- • •
ステータス 実行管理リスト こ	2ーザ 一時実行モード 1	セットアップ レポート	
- ロギン グ		┌ 高度なコントロール: ヲ	E_夕実行
▼ログの保存先ファイルし	: ログの表示	DLL	VBScript
C:¥Users¥Public¥Documer	nts¥AE.log	<u>]</u> AR	PowerShell Script
ステルスモード		互換性オプション	
■ 通知を表示しない(1)		Deep Freeze互	奥性の有効化(E)
🔲 システムトレイのアイコン	を表示しない(C)		
-75-6			
画像:	実行管理リスト違反のメ	ッセー	
	This action violates the	acceptable use policy	A
	ブロックされた通知:		
	This action violates the	acceptable use policy	*
変更(H)			~
		ок キャンセル	通用 ヘルプ

Anti-Executable でのイベントログの設定

ログファイルにイベントのログを書き込むには、[ファイルへのログの書き込み]を選択します。ログファイルは All Users/Documents ディレクトリにあります。

DLL 実行のモニタ

DLL をモニタするには、[DLL 実行のモニタ] チェックボックスを選択します。この チェックボックスが選択されていないと、実行管理リストに DLL が追加されてもモニ タされません。



[DLL 実行のモニタ] チェックボックスの選択を解除すると、「実行管理 リストのすべての DLL エントリを削除しますか?」というメッセージが 表示されます。すべての DLL エントリを削除するには、[はい]をク リックし、エントリを維持するには、[いいえ]をクリックします。



JAR 実行のモニタ

DLL をモニタするには、[DLL 実行のモニタ] チェックボックスを選択します。この チェックボックスが選択されていないと、実行管理リストに DLL が追加されてもモニ タされません。

VBScript 実行のモニタ

-VBScript ファイルをモニタするには、このオプションを選択します。このチェック ボックスが選択されていないと、管理リストに VBScript ファイルが追加されてもモニ タされません。

PowerShell スクリプト実行のモニタ

PowerShell スクリプトファイルをモニタするには、このオプションを選択します。こ のチェックボックスが選択されていないと、管理リストに PowerShell スクリプトファ イルが追加されてもモニタされません。

Anti-Executable のステルス機能

ステルスモードは、システム上の Anti-Executable の存在を視覚的に示すアイコンなど を管理する複数のオプションです。ステルスモードでは、管理者は、Windows のシス テムトレイで Anti-Executable のアイコンを非表示にしたり、アラートが表示されない ようにするオプションを利用できます。

Anti-Executable がシステムトレイに表示されていない場合、管理者と信頼ユーザーは、 Ctrl+Alt+Shift+F10 ホットキーを使って Anti-Executable を起動できます。

ステルス機能には以下のオプションがあります。

- 通知を表示しない アラートが表示されないようにします。
- システムトレイのアイコンを表示しない システムトレイの Anti-Executable アイ コンを非表示にします。

互換性オプション

Anti-Executable は Deep Freeze と互換性があります。

Deep Freeze 互換性



この機能は、コンピュータに Deep Freeze と Anti-Executable がインス トールされているときにのみ有効になります。

Deep Freeze の互換性機能により、管理者は Deep Freeze と Anti-Executable の Maintenance Mode を同期させることができます。



[Deep Freeze 互換性の有効化] チェックボックスを有効にすることで、Deep Freeze が Maintenance Mode になると (Deep Freeze は、Maintenance Mode のときに Thawed で再起動します)、Anti-Executable も自動的に Maintenance Mode になります。

Deep-Freeze と Anti-Executable が同時に Maintenance Mode になるように設定する ことで、コンピュータに追加された実行可能ファイルは、実行管理リストに追加され るだけでなく、Maintenance Mode の終了後にコンピュータが保護されると、Deep Freeze によって保持されます。

Anti-Executable では、Deep Freeze の Maintenance Mode が終了する少し前まで Maintenance Mode が継続します。Anti-Executable の Maintenance Mode が終了す ると、実行管理リストに新しい実行可能ファイルまたは更新された実行可能ファイル が追加されます。Deep Freeze の Maintenance Mode が終了すると、更新された実行 管理リストで Frozen になっているコンピュータが再起動します。



Deep Freeze 互換性が有効になっており、Deep Freeze が Frozen になっている場合、Anti-Executable を Maintenance Mode に設定することはできません。これはコンピュータに加えられた変更が再起動によって失われるためです。

Anti-Executable が無効になっているときに、Deep Freeze が Maintenance Mode になると、Anti-Executable は無効の状態が続きま す。

Deep Freeze によって開始する Maintenance 期間は、Anti-Executable で設定されているその他の Maintenance 期間よりも優先します。

Deep Freeze の詳細は、http://www.faronics.com/deepfreeze をご覧ください。

アラートのカスタマイズ

Anti-Executable 管理者は、[アラート]ペインを使って、ユーザーが実行禁止ファイ ルを実行しようとしたときに表示されるメッセージと画像を指定することができます。 以下のメッセージを設定できます。

- ・ 実行管理リスト違反のメッセージ:
- ブロックされた通知メッセージ:

メッセージを入力するか、デフォルトのメッセージを使用します。ユーザーが実行禁 止ファイルを実行しようとすると、このテキストがすべてのアラートダイアログに表 示されます。

[変更]をクリックして、ファイルを参照し、ビットマップ画像を選択します。選択した画像はアラートダイアログのテキストとともに表示されます。アラートメッセージには、以下の情報が表示されます。

- 実行可能ファイルの場所
- ・ 実行可能ファイル名
- デフォルトまたはカスタマイズされたイメージ
- デフォルトまたはカスタマイズされたメッセージ



以下はアラートダイアログの例です。

👌 Anti-Executable ア	ラート	×
	This action v	iolates the acceptable use policy
	ファイル名: 場所: 発行者:	remshutdn.exe C:\Users\AdminUser\Desktop\remshutdn.exe 不昭月
	製品名: ファイルのバージ	Remote Shutdown freeware
	種類: サイズ: 修正日: 説明:	アプリケーション 115.52 KB(118300/ドイト) 2008/06/05 17:53:10 Bemote Shutdown
	<u>このファイルのId</u>	lentifile情報を表示する。 表示
オプション		
▼ 実行管理リスト	で記憶する	
□ 関連するDLLを	許可に含める	
詳細		許可 (W) 拒否 (D)



レポートタブ

[レポート]タブにより、選択した期間に関する ¢ 最もブロックされるプログラム £ の レポートを作成できます。

タス 実行管理リスト ユー ポート	・ザ │ →時実行モード │ ・	セットアップ レポート	
最もブロックされるプロ レポート開始日:	コグラム	レポート終了日 <mark>:</mark>	
10/02/2012		11/01/2012	

レポートを作成するには、次の手順を実行します。

- 1. [レポート]タブをクリックします。
- 2. [レポート開始日]に日付を選択します。
- 3. [レポート終了日]に日付を選択します。
- 4. [生成]をクリックします。
- ブラウザが開き、レポートが表示されます。



Anti-Executable のアンインストール

トピック

Anti-Executable Standard のアンインストール



Anti-Executable Standard のアンインストール

Anti-Executable の削除は、.msi ファイルをダブルクリックして行えます。セットアップウィザードが表示されます。

1. [次へ]をクリックして、アンインストールを開始します。



2. [削除]をクリックします。





3. [削除]をクリックします。

📅 Faronics Anti-Executable Standard Edition - Setup Wizard 📃 🔲 💌
Ready to remove program
Click Remove to remove Faronics Anti-Executable Standard Edition from your computer. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Version 5.00.1111.513
< Back Remove Cancel

4. [完了]をクリックします。

