Faronics

ANTI-EXECUTABLE™ STANDARD

実行禁止ファイルから 完全な保護

ユーザーガイド

Faronics™
Intelligent Solutions for ABSOLUTE Control

www.faronics.com

最終更新日 : 2010 年 6 月

目次

はじめに

Anti-Executable は、実行禁止ファイルの実行を防止することによってコンピュータを保護します。

トピック

重要な情報

このセクションにはお客様の Faronics 製品についての重要な情報が記載されています。

Faronics について

Faronics は、複雑な IT 環境の管理を容易にし、セキュリティを確保する、業界をリードするソリューションをお届けしています。Faronics の製品は、システムの可用性を 100 パーセント確保することで、多くの情報技術専門家の日常業務を劇的に改善しました。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御使用頂いています。

製品マニュアル

Faronics Anti-Executable のマニュアルは、次のマニュアルで構成されています :

- Faronics Anti-Executable ユーザガイド — 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 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。

電子メール : support@faronics.com

電話番号 : 800-943-6422 または 604-637-3333

営業時間 : 月曜日～金曜日 午前 7:00 時から午後 5:00 時 (太平洋標準時刻)

お問い合わせ

- 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 7:00 時から午後 5:00 時 (太平洋標準時刻)
- 住所 : Faronics Technologies USA Inc.
  2411 Old Crow Canyon Road, Suite 170
  San Ramon, CA 94583
  USA

  Faronics Corporation
  609 Granville Street, Suite 620
  Vancouver, BC V7Y 1G5
  Canada

  Faronics Corporation（ヨーロッパ）
  Siena Court
  The Broadway Maidenhead
  Berkshire, SL6 1NJ UK

用語の定義

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 の管理者と信頼ユーザーは、アラートのメッセージと表示方法を指定できます。詳細は、「Anti-Executable の構成のエクスポート」を参照してください。
Anti-Executable 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。ホワイトリストとブラックリストの作成および編集、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-Executable Console Loadin	Faronics Core Console の機能を拡張するソフトウェアライブラリで、リモートワークステーションにインストールされた Anti-Executable の構成と操作に対し完全なコントロールを可能にします。
Anti-Executable 信頼ユーザー	信頼ユーザーは、[ステータス] タブ、[ホワイトリスト] タブ、および [ブラックリスト] タブにアクセスできます。ホワイトリストやブラックリストの作成および編集、Anti-Executable 保護の有効化または無効化を行えます。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。
実行許可ファイル	有効なホワイトリストの中の実行ファイル。プログラムを実行することができます。
ブラックフォルダ	ブロックされた実行可能ファイルがあるフォルダおよびそのサブフォルダ。
ブラックリスト	Anti-Executable によってブロックされる実行可能ファイルまたは実行可能ファイルを含むフォルダのリスト。
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。
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いかなるユーザー権限に関係なく、この制限は適用されます。
Faronics Core エージェント	Faronics Core Console との通信を可能にするために、ワークステーション上にインストールされるソフトウェア。
メンテナンスモード	メンテナンスモード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、自動的に有効なホワイトリストに追加されます。
保護	[有効化] に設定すると、Anti-Executable により有効なホワイトリストに応じてワークステーションが保護されます。[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。

用語	定義
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、アラートやスプラッシュ画面が表示されないようにするオプションを利用できます。
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、有効なホワイトリストに存在しないもので、実行できません。
ホワイトフォルダ	すべての実行可能ファイルが実行できるフォルダおよびそのサブフォルダ。
ホワイトリスト	Anti-Executable によって許可される実行可能ファイルまたは実行可能ファイルを含むフォルダのリスト。
ワークステーション	システム要件で指定されたオペレーティングシステムを使用するクライアントまたはリモートコンピュータ。
指紋	それぞれのファイルには、指紋と呼ばれる個別の識別 ID があります。指紋とはファイルの特徴のようなもので、Anti-Executable がファイルを識別するために使用します。
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 は、発行者の名前で発行者が作成したファイルを識別します。

はじめに

Anti-Executable は、実行禁止ファイルの実行を防止することによってコンピュータを保護します。

トピック

Anti-Executable 概要

Anti-Executable について

Anti-Executable では実行禁止ファイルが実行されることを防ぐため、IT 管理者は完全にコンピュータを管理することができます。ホワイトリストと呼ばれるファイルリストにない実行可能ファイルは実行されません。このホワイトリストは、編集、変更、削除などの権限を持つユーザーが完全に管理します。

Anti-Executable は一切迂回できません。実行可能ファイルの名前変更、リムーバブルストレージデバイスやネットワークからの実行はすべてブロックされるため、コンピュータは常に安全に保たれ、時間やコスト、労力が節約できます。

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 Anti-Executable を使用
Standard	非サーバーオペレーティングシステムが搭載されているローカルコンピュータ
Server Standard	サーバーオペレーティングシステムが搭載されているローカルコンピュータ
Enterprise	非サーバーオペレーティングシステムが搭載されているリモートコンピュータ *
Server Enterprise	サーバーオペレーティングシステムが搭載されているリモートコンピュータ *

*Enterprise 版では、Faronics Core Console という中央管理コンソールから複数のコンピュータを保護できます。

Faronics Core Console について

Faronics Core Console は、複数の Faronics 製品を管理するための、軽量で高性能、安全かつ学習し易い、統合されたフレームワークです。これは、表示、管理、インストール、更新、ワークステーションとサーバーの保護を 1 つのコンソールから行う、信頼性が高く一貫性のある方法を提供しています。Faronics 製品の完全な管理ソリューションによって、組織の効率性を高めることができます。

Anti-Executable の Enterprise 版では、Faronics Core Console から複数のワークステーションを保護できます。

システム要件

Anti-Executable は、次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 XP SP3 の 32 ビット版および Windows XP SP2 の 64 ビット版

- Windows Server 2003、Windows Server 2008、Windows Vista、Windows 7 の 32 ビット版および 64 ビット版

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 管理者は、Anti-Executable の [ステータス] タブでライセンス情報を取得できます。評価版を完全版にアップグレードするには、有効なライセンスキーを入力し、[*OK*] をクリックします。

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。

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 は、Windows Server 2003、Windows Server 2008、Windows XP SP3、および Windows Vista の 32bit 版および 64bit 版にインストールできます。

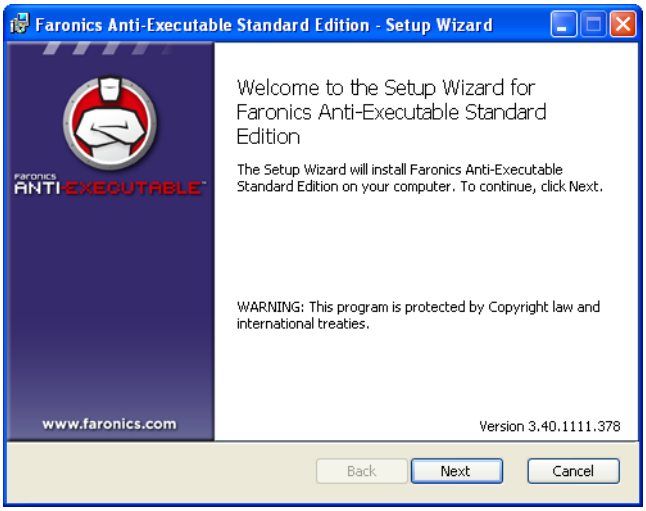
インストールする前に、オペレーティングシステムのバージョンを確認し、以下のリストからインストーラを選択してください。

システム	インストールファイル
Windows XP/Vista (32bit 版)	AEStd_32-bit.msi
Windows XP/Vista (64bit 版)	AEStd_64-bit.msi
Windows Server 2003 および Windows Server 2008 (32bit 版)	AESrvStd_32-bit.msi
Windows Server 2003 および Windows Server 2008 (64bit 版)	AESrvStd_64-bit.msi

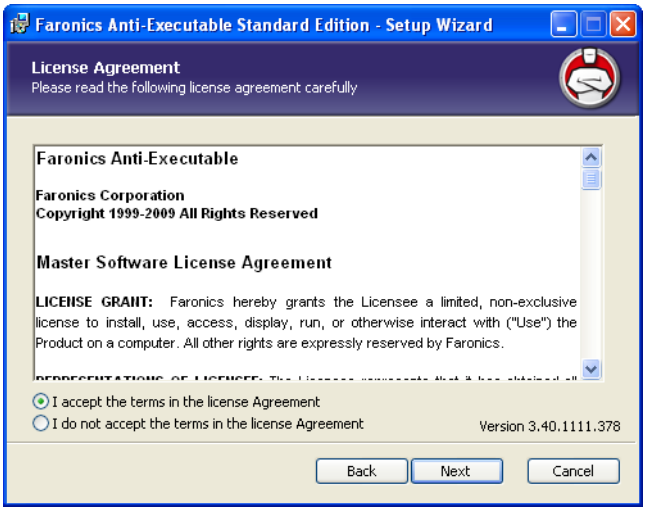
Anti-Executable のインストール

Anti-Executable は、セットアップウィザードを使用してインストールすることができます。Anti-Executable をインストールするには、以下の手順を実行します。

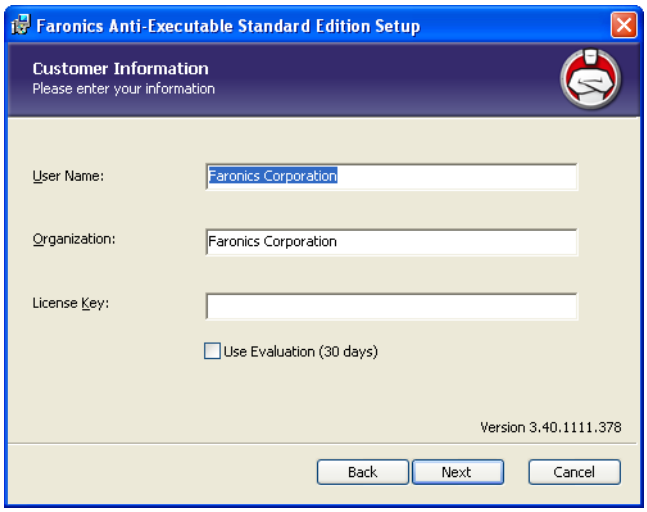
1. CD-ROM ドライブにメディアパッケージの CD-ROM を挿入します。Anti-Executable をインターネット経由でダウンロードした場合は、*AEStd_32-bit_en.msi* (32bit 版オペレーティングシステム) またはを *AEStd_64-bit_en.msi* (64bit 版オペレーティングシステム) をダブルクリックして、インストールプロセスを開始します。[次へ] をクリックして、続行します。



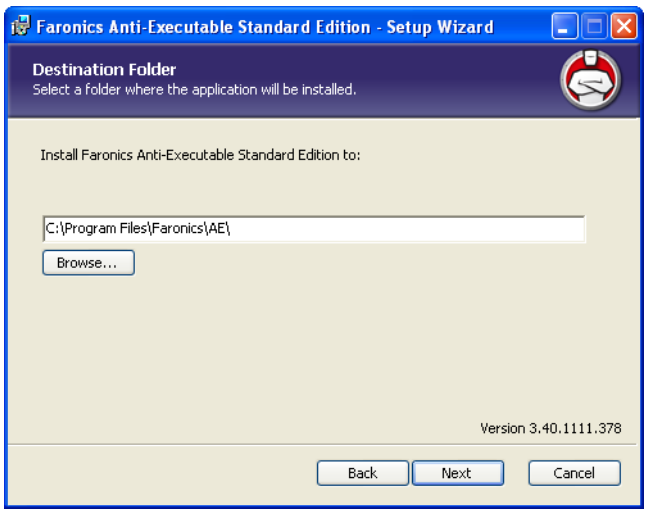
2. 使用許諾契約書を読んで、同意します。[次へ] をクリックして、続行します。



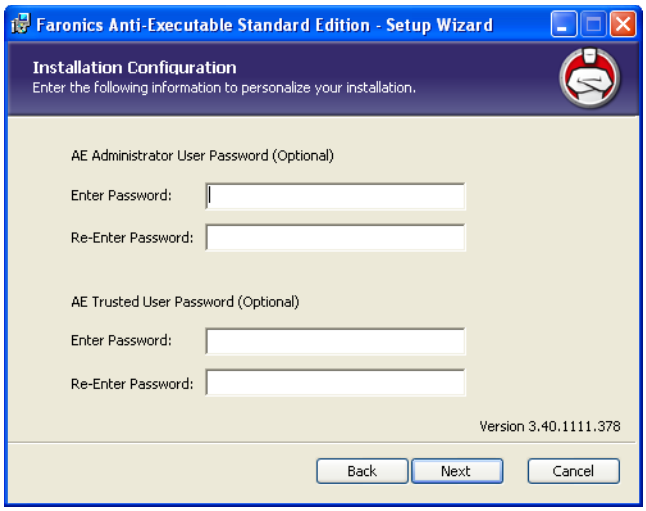
3. ユーザー名と組織を入力します。[評価版を使用] を選択すると、Anti-Executable は評価版としてインストールされ、30 日間有効になります。ライセンスキーを入力していつでも評価版を完全版に変換することができます。[次へ] をクリックして、続行します。



4. インストール場所を指定します。デフォルトは、*C:\Program Files\Faronics\AE* です。[次へ] をクリックして、続行します。



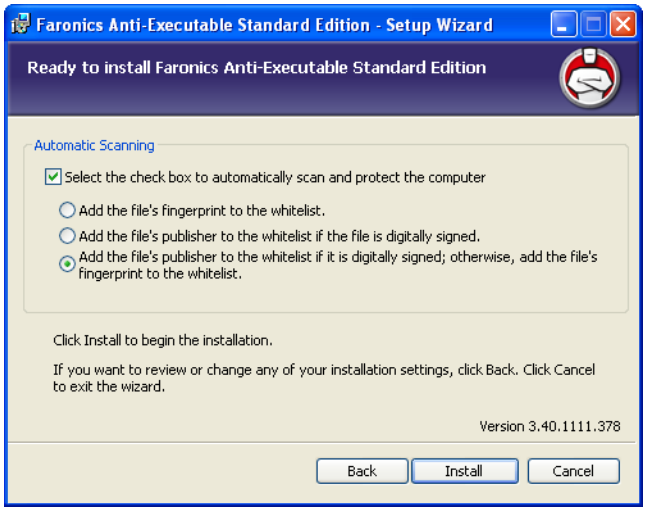
5. この手順は任意です。Anti-Executable 管理者と信頼ユーザーのパスワードを指定します。このパスワードは、インストール後に Anti-Executable の [ユーザー] タブで設定することができます。[次へ] をクリックして、続行します。



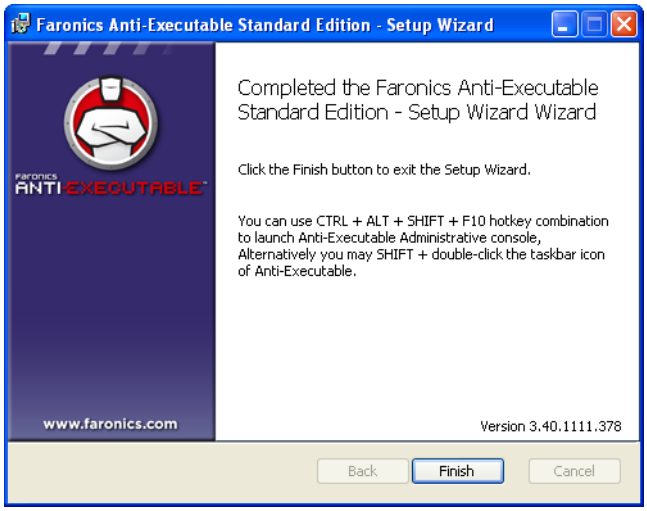
6. [自動スキャン] ダイアログが表示されます。Anti-Executable によりコンピュータのリムーバブル以外のドライブが自動的にスキャンされ、ホワイトリストが作成されるようにするには、チェックボックスを選択します。次のオプションを選択します。

- ファイルの指紋をホワイトリストに追加 - ファイルの個別の識別 ID をホワイトリストに追加します。ホワイトリストに指紋が追加されたファイルは、実行を許可されます。
- デジタル署名したファイルの発行者をホワイトリストに追加 - 発行者をホワイトリストに追加します。ホワイトリストの発行者がデジタル署名したファイルは、実行を許可されます。
- デジタル署名したファイルの発行者をホワイトリストに追加します。または、ファイルの指紋を追加 – デジタル署名したファイルの発行者を追加、またはデジタル署名がない場合は、ファイルの指紋を追加します。

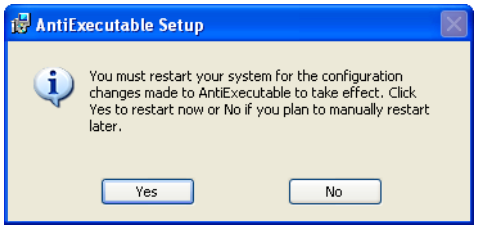
[インストール] をクリックして、Anti-Executable をインストールします。Anti-Executable がインストールされ、ホワイトリストが有効となります。



7. [完了] をクリックして、インストールを終了します。



8. インストールが正常に行われたら、再起動が必要です。すぐに再起動する場合は [はい] をクリックし、後で再起動する場合は [いいえ] をクリックします。



インストール後、すぐに再起動することが推奨されます。

[自動スキャンとホワイトリストの作成] ダイアログで [有効化] チェックボックスが選択されていると、保護が有効になり、コンピュータが再起動したときに有効なホワイトリストが作成されます。

[自動スキャンとホワイトリストの作成] ダイアログで [有効化] チェックボックスが選択されていないと、保護は無効になり、コンピュータが再起動したときに有効なホワイトリストが作成されません。

Anti-Executable の使用

この章では Anti-Executable へのアクセス、構成、使用手順について説明します。

トピック

Anti-Executable へのアクセス

Anti-Executable は、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。アイコンが存在しない場合、*Ctrl* + *Alt* + *Shift* + *F10* ホットキーを使用できます。

管理者は、[ステータス]、[ホワイトリスト]、[ブラックリスト]、[ユーザー]、[セットアップ] 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]、[ホワイトリスト]、[ブラックリスト] 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

インストール後に、Anti-Executable を設定する必要があります。Anti-Executable の管理者は、以下のすべてのタブにアクセスできます。

- ステータス – このタブにはインストールされている Anti-Executable のバージョンおよび新しいバージョンの有無が表示されます。また、構成をインポートおよびエクスポートしたり、Anti-Executable 保護を、[有効化]、[無効化]、または [メンテナンスモード] に設定できます。
- ホワイトリスト – このタブではホワイトリストの作成、編集、適用を行います。
- ブラックリスト – このタブではブラックリストの作成、編集、適用を行います。
- ユーザー – このタブでは、管理者、信頼ユーザー、およびパスワードを追加できます。
- セットアップ – このタブでは、ステルスモードの設定、ログ管理、アラートメッセージ、Deep Freeze と Anti-Executable の互換性の有効化を行います。

インストールを行った Windows 管理者のユーザーアカウントが、最初の Anti-Executable 管理者です。

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、メンテナンスモードの設定、これまで保存されていた構成のインポートまたはエクスポートなどが行えます。Faronics Core Console でワークステーションを 1 台選択し、[*Anti-Executable* の構成] を選択すると、ワークステーションの構成が自動的に取得されます。

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。

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。Faronics に連絡して、ライセンスキーを入手することができます。

Anti-Executable 保護の有効化

インストール中に [自動スキャンとホワイトリスト作成] ダイアログで [有効化] を選択すると、インストール後に、Anti-Executable はデフォルトで有効になります。そうでない場合は、Anti-Executable でコンピュータが保護されません。ホワイトリストでの保護が有効になるように、管理者または信頼ユーザーは、[有効化] を選択する必要があります。

保護が有効になっていても、有効なホワイトリストが空の場合は、基本システム実行可能ファイル (例えばブートアップ、ログイン) だけを実行することができます。Anti-Executable の管理者と信頼ユーザーだけが、ホワイトリストを管理することができます。

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 のメンテナンスモード

メンテナンスモードで Anti-Executable を実行するには、[メンテナンスモード] を選択して、[適用] をクリックします。メンテナンスモード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、自動的に有効なホワイトリストに追加されます。メンテナンスモードを終了するには、[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。

コンピュータがメンテナンスモードで実行されていて、保護が無効になっている場合、メンテナンスモードの間にワークステーションに対して行われた変更は有効なホワイトリストに追加されません。

コンピュータがメンテナンスモード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。

Anti-Executable の構成のエクスポート

Anti-Executable 管理者は、他のコンピュータに適用できる複数の構成を保存することができます。ホワイトリストが有効になっている場合、それも構成のエクスポートに含められます。

Anti-Executable の構成ファイルを保存するには、選択を行った後、[ステータス] タブで [エクスポート] をクリックします。構成ファイルは、不正に変更されるのを防ぐために、専用の形式 (*.aecfg*) で保存されます。以前に定義された構成ファイル (*.aecfg*) を開くには、[開く] をクリックして、構成ファイルを参照します。

XML 形式で設定を保存した場合は、構成を表示することだけが可能になります。XML の構成ファイルは、他のコンピュータには適用できません。

Anti-Executable に加えた変更は、[適用] をクリックするまで有効になりません。

Anti-Executable の構成のインポート

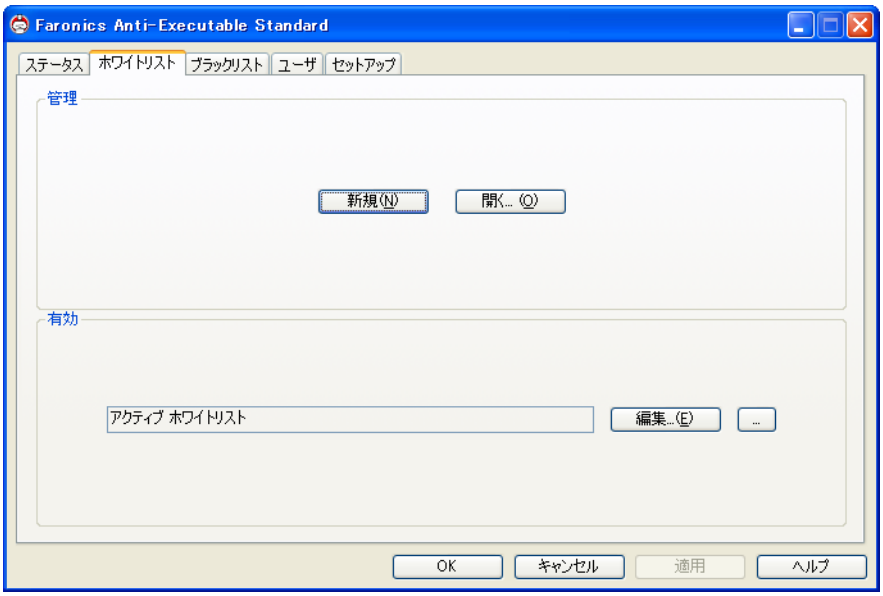
Anti-Executable Administrators および信頼ユーザは、[インポート] をクリックして過去にエクスポートされた Anti-Executable の構成をインポートできます。表示された [インポート オプション] ダイアログから 1 つ以上のインポート オプションを選択します。次のいずれのオプションを選択しなくてもインポートは実行できます。

• アクティブなホワイトリストおよびブラックリストのインポート
• アラート画像のインポート
• Anti-Executable ユーザのインポート
[OK] をクリックして、構成ファイル (.aecfg) を参照します。

ホワイトリストタブ

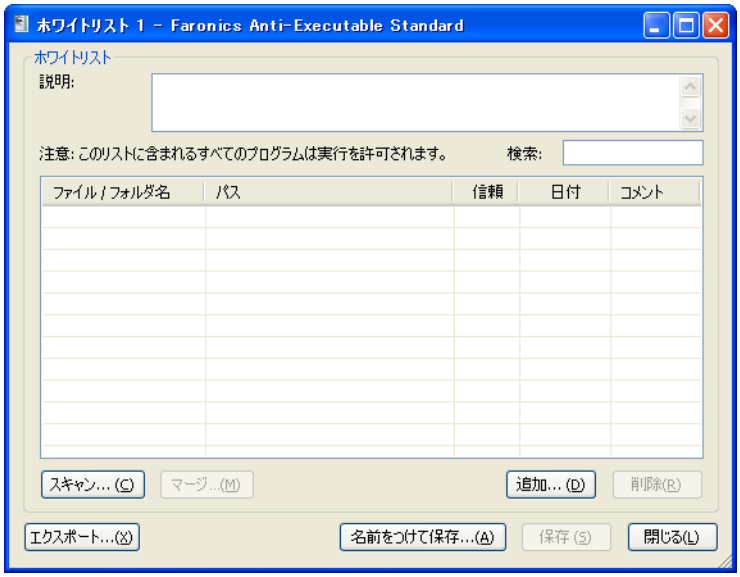
保護が [有効化] に設定されていると、Anti-Executable では、有効なホワイトリストにあるすべての実行可能ファイルの起動が許可されます。また、ホワイトフォルダ (フォルダとそのサブフォルダ) に含まれるすべての実行可能ファイルも起動することができます。

一度に有効にできるホワイトリストは 1 つだけです。最初のホワイトリストを作成するための情報は、「新規ホワイトリストの作成」というタイトルのセクションを参照してください。



ホワイトリストエディタの使用

Anti-Executable のホワイトリストエディタは、[ホワイトリスト] タブをクリックし、[新規]、[開く]、または [編集] のいずれかを選択すると開きます。Windows エクスプローラで、それぞれのホワイトリストファイルを開いたときも、ホワイトリストエディタが開きます。



- 新規 – ホワイトリストエディタが開き、Anti-Executable 管理者と信頼ユーザーは、新規ホワイトリストを作成できます。
- 開く – 既存のホワイトリストを開き、編集できます。
- 編集 – ホワイトリストエディタを開き、有効なホワイトリストに実行可能ファイルやフォルダを追加したり、削除できます。

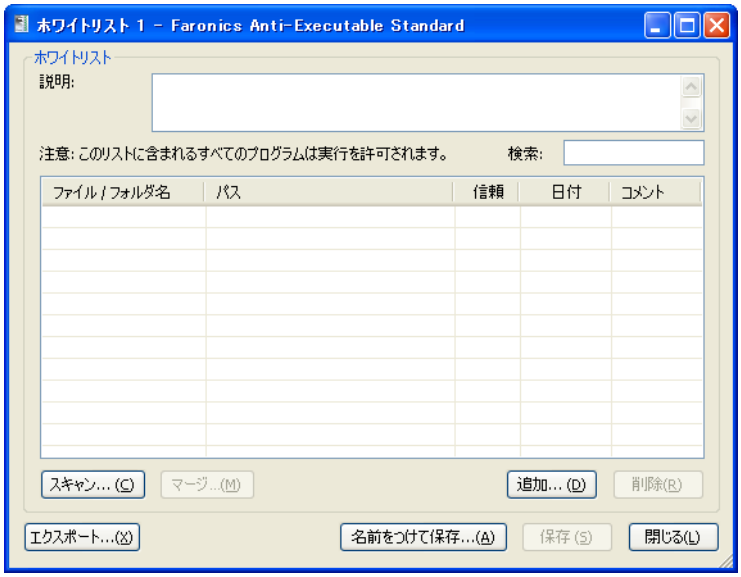
新規ホワイトリストの作成

Anti-Executable 管理者と信頼ユーザーだけが、ホワイトリストエディタにアクセスすることができます。

ホワイトリストを作成するには、クリーンな状態のコンピュータの使用を推奨します。クリーンな状態のコンピュータとは、日常の作業に必要なオペレーティングシステムとその他のアプリケーションがインストールされたシステムをいいます。ユーザーがコンピュータを使いだす前にホワイトリストを作成すると、ホワイトリストにはコンピュータが適切に動作するために必要なファイルのみが含まれます。

新規ホワイトリストを作成するには、以下の手順を実行します。

1. *Shift* キーを押したまま、システムトレイの Anti-Executable アイコンをダブルクリックします。または、*Ctrl* +*Alt* +*Shift* + *F10* ホットキーを押すこともできます。管理者パスワードを入力して、Anti-Executable にログオンします。[ホワイトリスト] タブをクリックします。[新規] をクリックします。ホワイトリストエディタが表示されます。



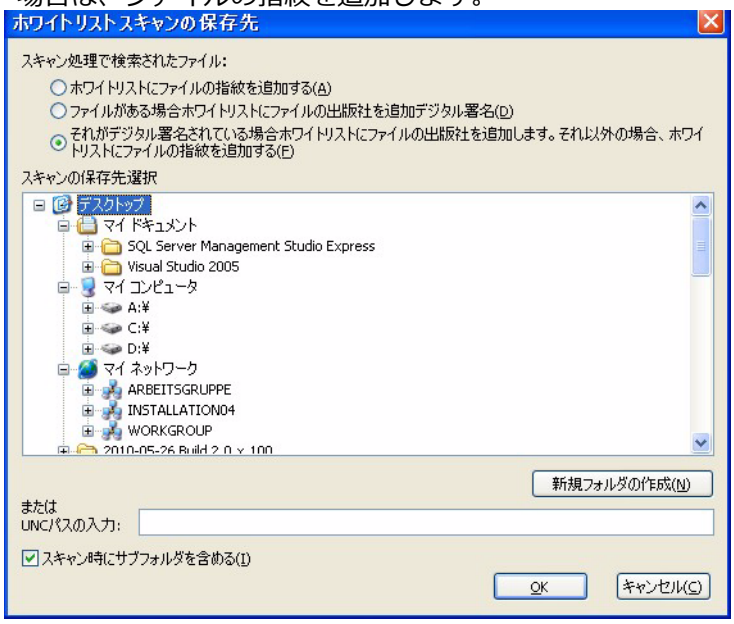
2. ワークステーションをローカルでスキャンするために複数のドライブまたはディレクトリを選択するには、Ctrl キーを押したままクリックするか、Shift キーを押したままクリックします。[マイネットワークプレース] をクリックし、リモートスキャンするリモートのワークステーションを参照して選択します。[UNC パスの入力] フィールドに UNC パスを入力することも可能です。

• 次のオプションを選択します。

– ファイルの指紋をホワイトリストに追加 - ファイルの個別の識別 ID をホワイトリストに追加します。ホワイトリストに指紋が追加されたファイルは、実行を許可されます。

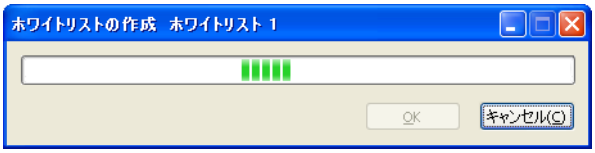
– デジタル署名したファイルの発行者をホワイトリストに追加 - 発行者をホワイトリストに追加します。ホワイトリストの発行者がデジタル署名したファイルは、実行を許可されます。

– デジタル署名したファイルの発行者をホワイトリストに追加します。または、ファイルの指紋を追加 – デジタル署名したファイルの発行者を追加、またはデジタル署名がない場合は、ファイルの指紋を追加します。

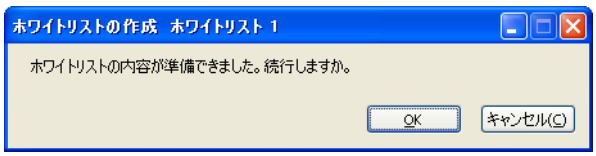


スキャン機能では、選択した場所とそのサブディレクトリのすべての実行可能ファイル (*.scr*、*.jar*、*.bat*、*.com*、または *.exe* の拡張子が付いたファイル) が検索されます。スキャンの時間は、その場所のサイズと、その中で検出された実行可能ファイルの数によって異なります。

3. [*OK*] をクリックします。進行状況を示す [ホワイトリストの作成] ダイアログが表示されます。



4. スキャンが完了したら、続行するかどうかを尋ねられます。[*OK*] をクリックします。

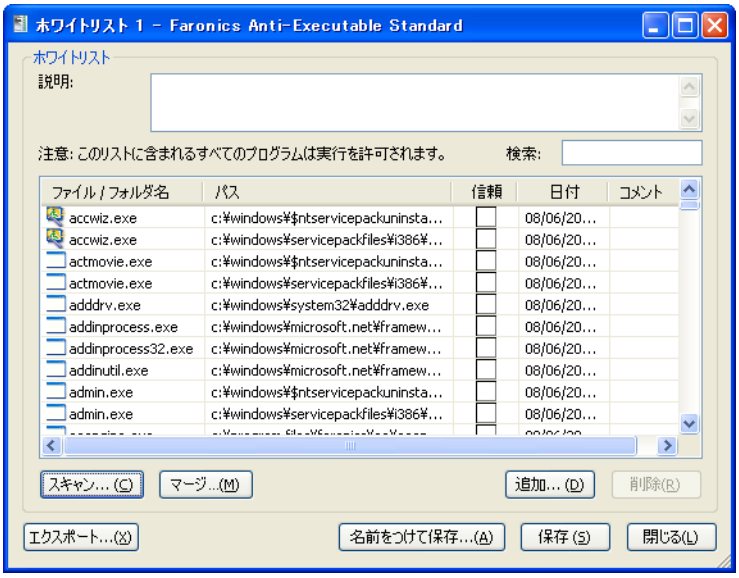


5. 登録されたホワイトリストが表示されます。フォルダと実行可能ファイルは個別に追加することができます。新規ホワイトリストに追加するには、フォルダまたは実行可能ファイルを

選択し、[追加] をクリックします。フォルダを追加すると、フォルダとそのサブフォルダの中の実行可能ファイルは起動を許可されます。

- フォルダまたは実行可能ファイルを削除するには、いずれかを選択して、[削除] をクリックします。これは、フォルダまたは実行可能ファイルをシステムから削除するということではありません。
- 既存のホワイトリストにフォルダまたは実行可能ファイルを統合するには、[マージ] をクリックします。[開く] ダイアログが表示されます。既存のホワイトリストを選択して、[開く] をクリックします。スキャンされたファイルまたは実行可能ファイルのリストは、既存のホワイトリストの内容に統合されます。ホワイトリストを同じ名前で保存するには、[保存] をクリックします。統合したホワイトリストを別の名前で保存するには、[名前を付けて保存] をクリックします。
- 特定のフォルダまたは実行可能ファイルを検索するには、[検索] フィールドにフォルダや実行可能ファイルの名前の 1 文字または数文字を入力します。入力された文字に基づいてリストがフィルターされます。

日付で実行可能ファイルを並べ替えるには、[日付] カラムのタイトルをクリックします。



6. [信頼済み] カラムをクリックし、アプリケーションが信頼済みかどうか定義します。チェックマークが選択されている場合、アプリケーションが信頼済みであり、それらが、自身では実行禁止の他のファイルを起動することができることを示します。
7. [コメント] コラムをクリックして、アプリケーションにコメントを入力します。テキストプロンプトが表示され、追加情報を入力することができます。また、ホワイトリストエディタの上部にあるスペースにリスト全体の説明を入力することもできます。
8. [保存] をクリックして、ホワイトリストを保存します。別の名前で保存するには、[名前を付けて保存] をクリックします。ホワイトリストは、*.aebl* という拡張子が付いた専用の形式で保存されます。ホワイトリストを XML または CSV の形式にエクスポートするには、[エクスポート] をクリックします。XML および CSV 形式のホワイトリストは、Windows エク

スプローラで開き、編集することができます。ただし、有効なホワイトリストとして設定することはできません。

実行可能ファイルに関する詳細は、実行可能ファイルを右クリックして、[*Google* 検索] を選択します。デフォルトのブラウザが起動し、実行可能ファイル名が www.google.com で検索されます。

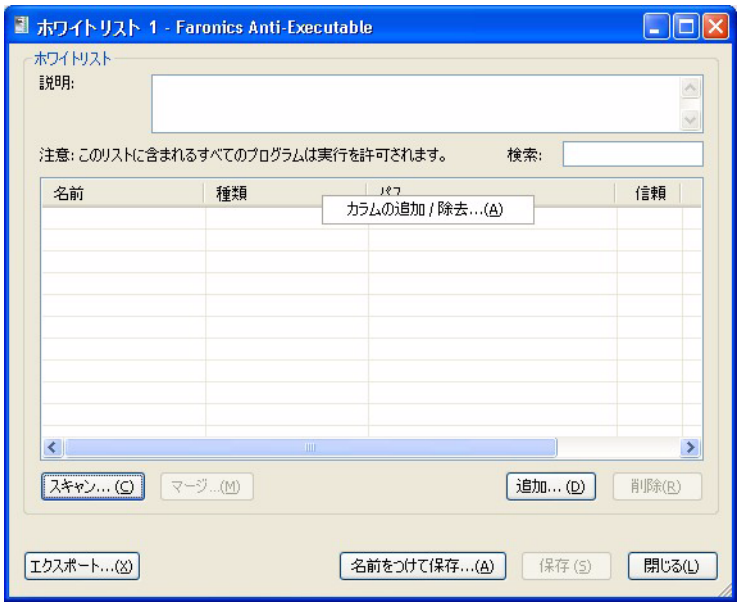
ホワイトリストの有効化

ホワイトリストが作成された後に、[ホワイトリスト] タブの有効なホワイトリストの部分で、[参照] ボタンをクリックすると、有効なホワイトリストに指定できます。[参照] ボタンにより、[開く] ダイアログが起動します。ホワイトリストを参照し、[開く] をクリックします。

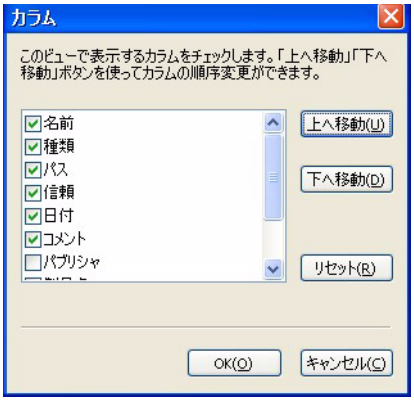
ホワイトリスト エディタのカラムの追加または削除

カラムを追加または削除するには、次の手順を実行します。

1. ホワイトリスト エディタを開きます。
2. カラムのタイトルを右クリックし、[カラムの追加 / 削除] を選択します。



3. 追加するカラムを選択します。削除するカラムはチェックボックスの選択を解除します。また [上に移動または下に移動] をクリックすると、カラムの位置を変更できます。[名前]、[タイプ]、[パス]、[日付]、[コメント] カラムは削除できません。



4. [OK] をクリックします。

既存のホワイトリストへの発行者またはファイル / フォルダの追加

カラムを追加または削除するには、次の手順を実行します。

1. ホワイトリストエディタを開きます。
2. [追加] をクリックします。
3. [ホワイトリストへの追加] ダイアログが表示されます。発行者またはファイル / フォルダを選択します。発行者を追加する場合、その発行者のファイルを検索して選択します。ファイルがデジタル署名されている場合、発行者の名前が表示されます。ファイル / フォルダを追加する場合、ファイルまたはフォルダを検索して選択します。[UNC パスの入力] フィールドに UNC パスを入力することもできます。
4. [OK] をクリックします。発行者またはファイル / フォルダがホワイトリストに追加されます。

既存のホワイトリストへの実行ファイルまたはフォルダの追加

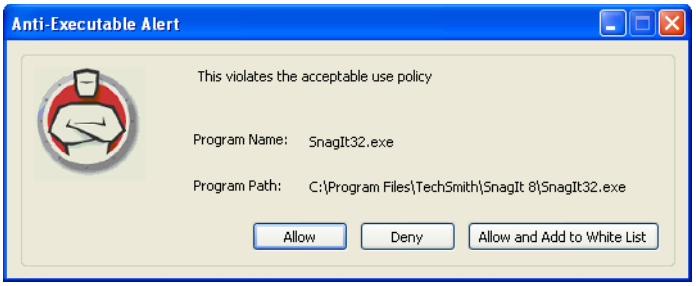
スキャン機能は、新規ホワイトリストに追加する以外に、特定の場所から実行可能ファイルを既存のホワイトリストに追加することができます。この場所はローカル、外部、またはネットワーク上のどこでも可能です。

- [スキャン] をクリックして、[ホワイトリストスキャンの保存先] ダイアログを開きます。これにより選択した場所のすべての実行可能ファイルが検索されます。スキャンが終了すると、結果はホワイトリストに統合されます。
- [追加] をクリックすると、個々のフォルダと実行可能ファイルを追加できます。
- 以前に作成されたホワイトリストを開くには、[開く] をクリックし、ホワイトリストファイルを参照します。[追加]、[削除]、[スキャン]、または [マージ] の各ボタンを使って、必要な変更を加えます。これらのボタンは、ホワイトリストから実行可能ファイルとフォルダを追加 / 削除します。これらは、コンピュータ上の実際のファイルまたはフォルダを変更するわけではありません。
- [ホワイトリストのみ] ボタンをクリックして、ブラックリストから実行可能ファイルを削除し、それらがホワイトリストの一部であることを確認します。

- 同時に、複数のホワイトリストを開き、編集することができます。有効なホワイトリストとして設定できるリストは一度に 1 つだけです。

有効なホワイトリストへの実行可能ファイルの追加

実行可能ファイルは、起動すると、有効なホワイトリストに追加されます。コンピュータが保護状態にあり、実行禁止ファイルが起動された場合、Anti-Executable 管理者または信頼ユーザーは、[許可]、[拒否]、または [許可しホワイトリストに追加する] のいずれかのオプションを選択するよう指示されます。



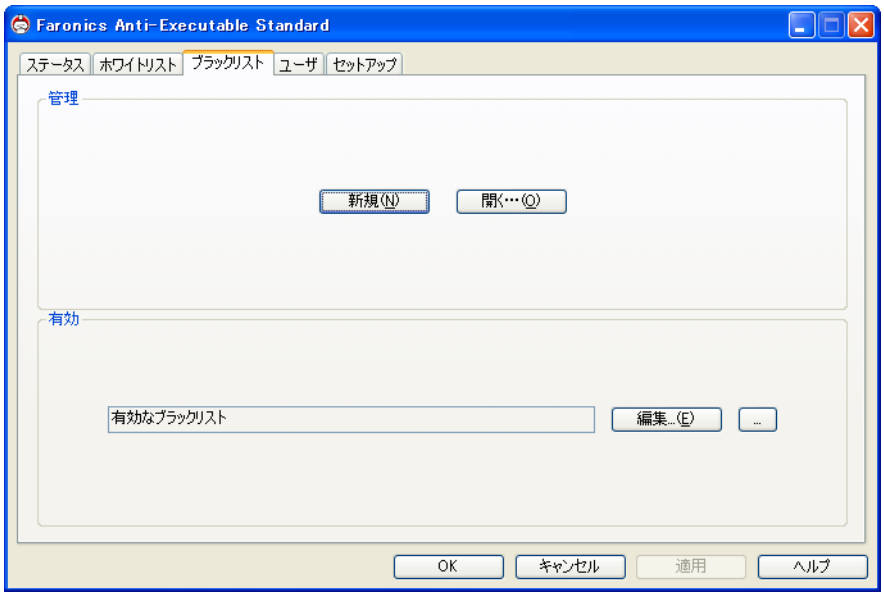
- 許可 – 実行可能ファイルの起動を許可しますが、有効なホワイトリストには追加されません。次回実行可能ファイルを起動すると、再びブロックされます。
- 拒否 – 実行可能ファイルは、有効なホワイトリストに追加されず、実行禁止ファイルのままです。起動は許可されません。
- 許可しホワイトリストに追加する – 実行可能ファイルの起動は許可されます。また、そのファイルは実行許可ファイルとして、有効なホワイトリストに追加されます。

外部のユーザーは、許可するか、拒否するか、または許可しホワイトリストに追加するかを選択するのに必要な権限がありません。有効なホワイトリストにない実行可能ファイルを起動しようと試みた外部のユーザーに、実行可能ファイルがブロックされたことが通知されます。詳細は、「アラートのカスタマイズ」のセクションを参照してください。

ブラックリストタブ

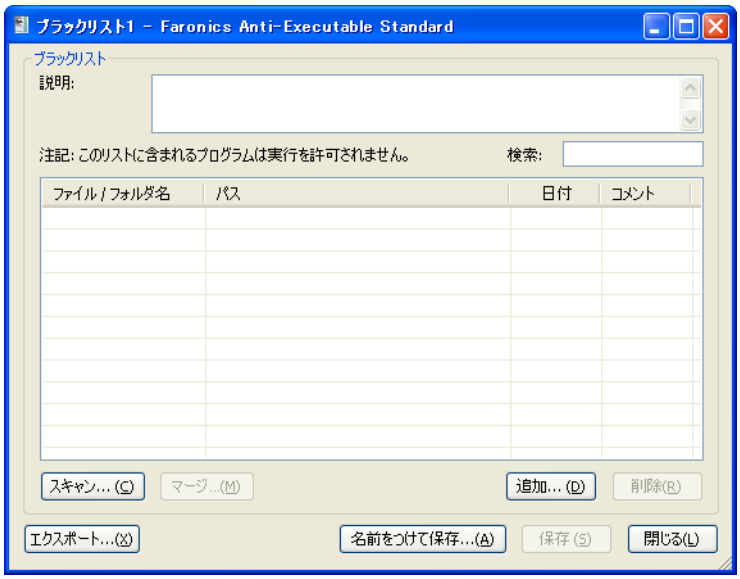
保護が [有効化] に設定されていると、Anti-Executable では、有効なブラックリストにあるすべての実行可能ファイルの起動がブロックされます。また、ブラックフォルダ (フォルダとそのサブフォルダ) に含まれるすべての実行可能ファイルもブロックされます。

一度に有効にできるブラックリストは 1 つだけです。最初のブラックリストを作成するための情報は、「新規ブラックリストの作成」というタイトルのセクションを参照してください。



ブラックリストエディタの使用

Anti-Executable のブラックリストエディタは、[ブラックリスト] タブをクリックし、[新規]、[開く]、または [編集] のいずれかを選択すると開きます。Windows エクスプローラで、ブラックリストファイルを開いても、ブラックトリストエディタが開きます。



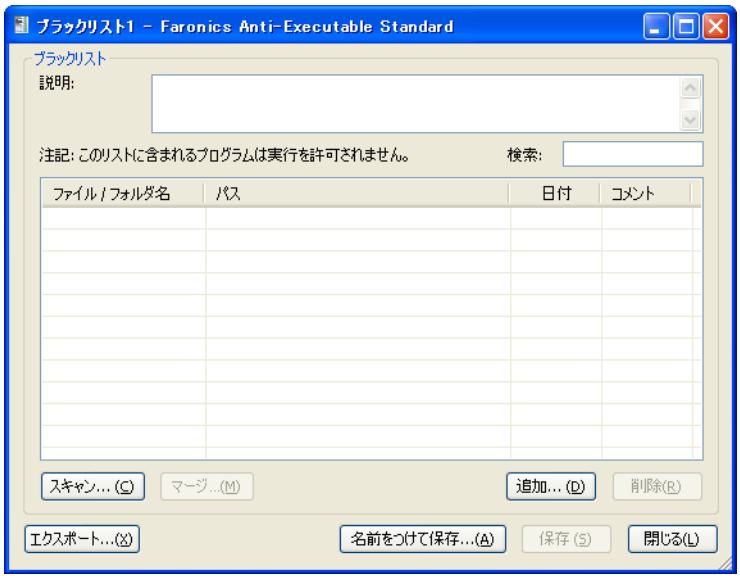
- 新規 – ブラックリストエディタが開き、Anti-Executable 管理者と信頼ユーザーは、新規ブラックリストを作成できます。
- 開く – 既存のブラックリストを開き、編集できます。
- 編集 – ブラックリストエディタを開き、有効なブラックリストに実行可能ファイルやフォルダを追加したり、削除できます。

新規ブラックリストの作成

Anti-Executable 管理者と信頼ユーザーだけが、ブラックリストエディタにアクセスすることができます。

新規ブラックリストを作成するには、以下の手順を実行します。

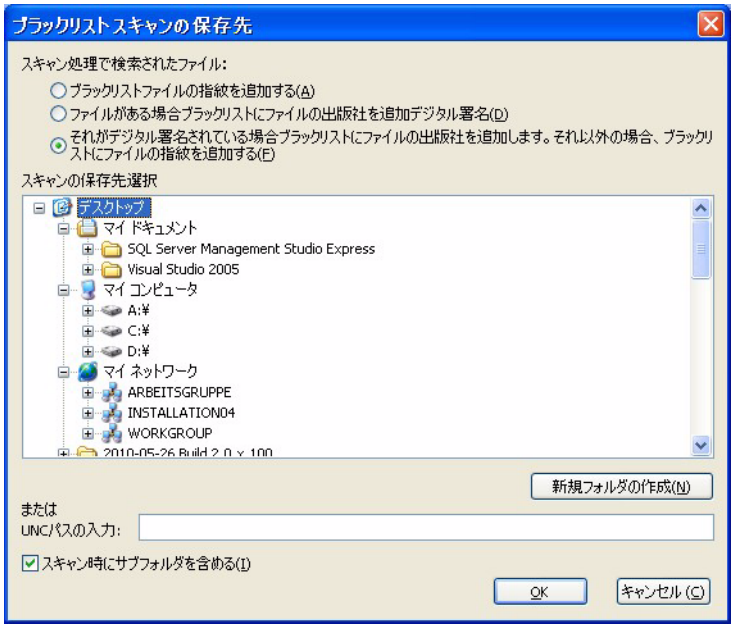
1. *Shift* キーを押したまま、システムトレイの Anti-Executable アイコンをダブルクリックします。または、*Ctrl* +*Alt* +*Shift* + *F10* ホットキーを押すこともできます。管理者パスワードを入力して、Anti-Executable にログオンします。[ブラックリスト] タブをクリックします。[新規] をクリックします。ブラックリストエディタが表示されます。



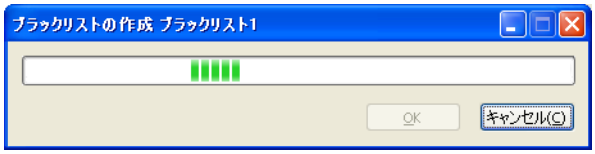
2. 利用可能なアプリケーションをチェックするには、[スキャン] をクリックして、ドライブまたはディレクトリを選択します。複数のドライブまたはディレクトリを選択するには、*Ctrl* キーを押したままクリック、または *Shift* キーを押したままクリックします。または、[マイネットワークプレース] をクリックして参照し、リモートワークステーションを選択することもできます。[*OK*] をクリックします。

次のオプションを選択します。

- ファイルの指紋をブラックリストに追加 - ファイルの個別の識別 ID をブラックリストに追加します。ホワイトリストに指紋が追加されたファイルは、実行を許可されます。
- デジタル署名したファイルの発行者をブラックリストに追加 - 発行者をブラックリストに追加します。ブラックリストの発行者がデジタル署名したファイルは実行を許可されません。
- デジタル署名したファイルの発行者をブラックリストに追加します。または、ファイルの指紋を追加 – デジタル署名したファイルの発行者を追加、またはデジタル署名がない場合は、ファイルの指紋を追加します。

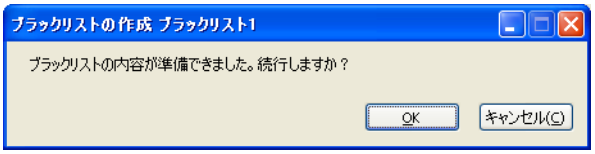


進行状況を示す [ブラックリストの作成] ダイアログが表示されます。



スキャン機能では、選択した場所とそのサブディレクトリのすべての実行可能ファイル (*.scr*、*.jar*、*.bat*、*.com*、または *.exe* の拡張子が付いたファイル) が検索されます。スキャンの時間は、その場所のサイズと、その中で検出された実行可能ファイルの数によって異なります。

3. スキャンが終了すると、その結果を新規ブラックリストに統合するかどうかを尋ねられます。[*OK*] をクリックします。

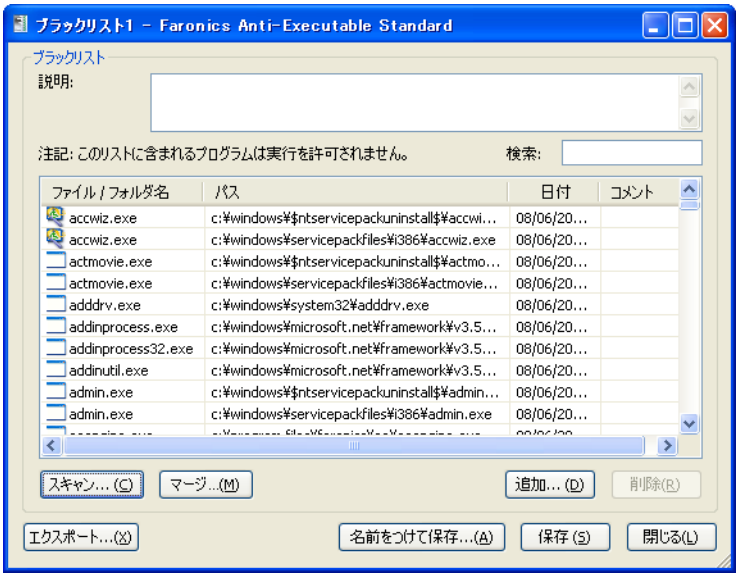


4. 登録されたブラックリストが表示されます。フォルダと実行可能ファイルは個別に追加することができます。新規ブラックリストに追加するには、フォルダまたは実行可能ファイルを

選択し、[追加] をクリックします。フォルダを追加すると、フォルダとそのサブフォルダの中の実行可能ファイルの起動はブロックされます。

- フォルダまたは実行可能ファイルを削除するには、いずれかを選択して、[削除] をクリックします。これは、フォルダまたは実行可能ファイルをシステムから削除するということではありません。
- 既存のブラックリストにフォルダまたは実行可能ファイルを統合するには、[マージ] をクリックします。[開く] ダイアログが表示されます。既存のブラックリストを選択して、[開く] をクリックします。スキャンされたファイルまたは実行可能ファイルのリストは、既存のブラックリストの内容に統合されます。ブラックリストを同じ名前で保存するには、[保存] をクリックします。統合したブラックリストを別の名前で保存するには、[名前を付けて保存] をクリックします。
- 特定のフォルダまたは実行可能ファイルを検索するには、[検索] フィールドにフォルダや実行可能ファイルの名前の 1 文字または数文字を入力します。入力された文字に基づいてリストがフィルターされます。

日付で実行可能ファイルを並べ替えるには、[日付] カラムのタイトルをクリックします。



5. [コメント] カラムをクリックして、アプリケーションにコメントを入力します。テキストプロンプトが表示され、追加情報を入力することができます。また、ブラックリストエディタの上部にあるスペースにリスト全体の説明を入力することもできます。
6. ブラックリストを保存するには、[保存] をクリックします。別の名前で保存するには、[名前を付けて保存] をクリックします。ブラックリストは、*.aebl* という拡張子が付いた専用の形式で保存されます。ブラックリストを XML または CSV の形式にエクスポートするには、[エクスポート] をクリックします。XML および CSV 形式のブラックリストは、Windows エクスプローラで開き、編集することができます。ただし、有効なブラックホワイトリストとして設定することはできません。

実行可能ファイルに関する詳細は、実行可能ファイルを右クリックして、[*Google* 検索] を選択します。デフォルトのブラウザが起動し、実行可能ファイル名が www.google.com で検索されます。

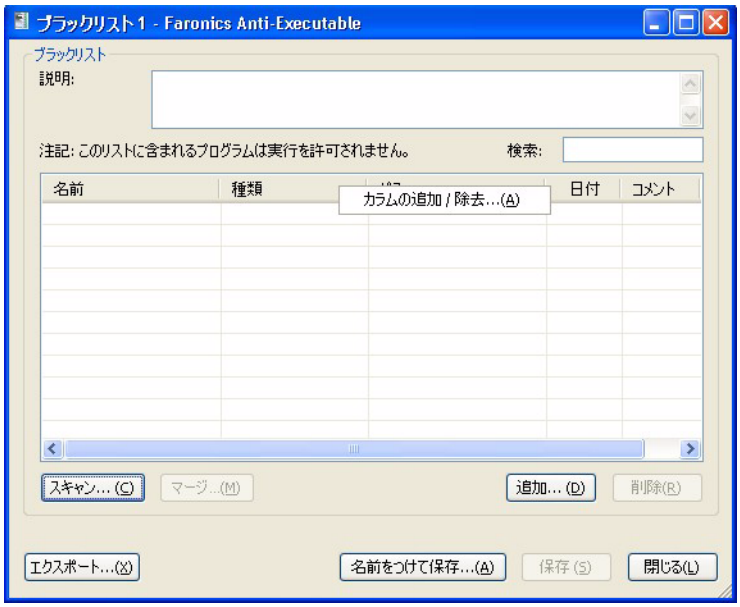
ブラックリストの有効化

ブラックリストが作成された後に、[ブラックリスト] タブの有効なブラックリストの部分で、[参照] ボタンをクリックすると、有効なブラックリストに指定できます。[参照] ボタンにより、[開く] ダイアログが起動します。ブラックリストを参照し、[開く] をクリックします。

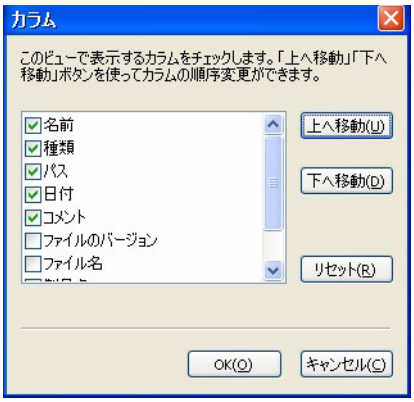
ブラックリストエディタのカラムの追加または削除

カラムを追加または削除するには、次の手順を実行します。

1. ブラックリストエディタを開きます。
2. カラムのタイトルを右クリックし、[カラムの追加 / 削除] を選択します。



3. 追加するカラムを選択します。削除するカラムはチェックボックスの選択を解除します。また [上に移動または下に移動] をクリックすると、カラムの位置を変更できます。[名前]、[タイプ]、[パス]、[日付]、[コメント] カラムは削除できません。

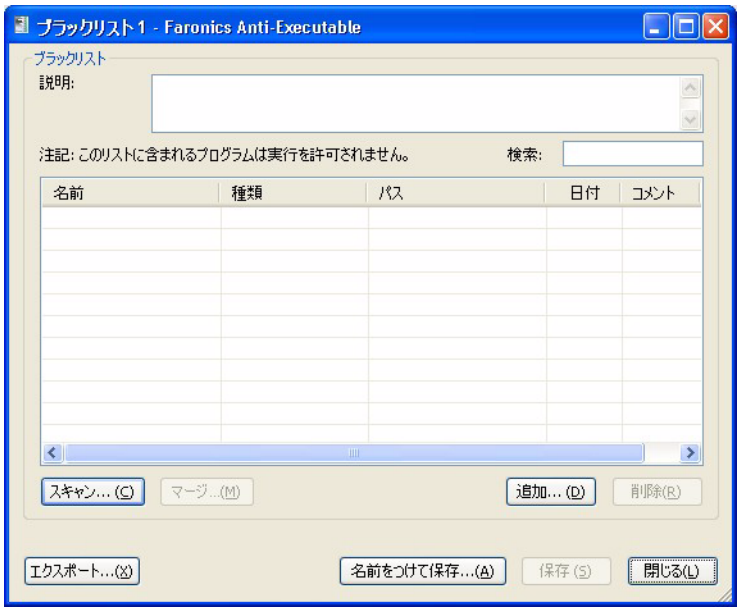


4. [OK] をクリックします。

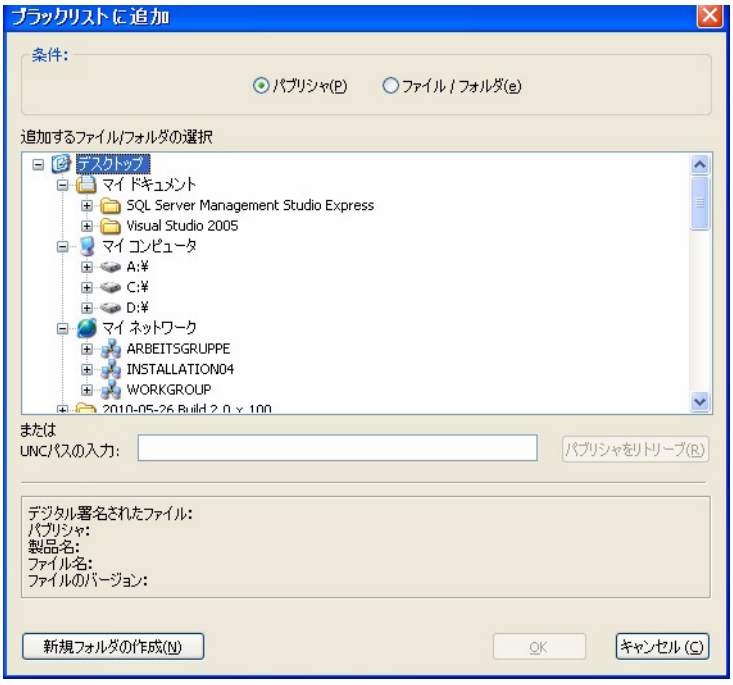
既存のブラックリストへの発行者またはファイル / フォルダの追加

カラムを追加または削除するには、次の手順を実行します。

1. ブラックリストエディタを開きます。
2. [追加] をクリックします。



3. [ブラックリストへの追加] ダイアログが表示されます。発行者またはファイル / フォルダを選択します。発行者を追加する場合、その発行者のファイルを検索して選択します。ファイルがデジタル署名されている場合、発行者の名前が表示されます。ファイル / フォルダを追加する場合、ファイルまたはフォルダを検索して選択します。[UNC パスの入力] フィールドに UNC パスを入力することもできます。



4. [OK] をクリックします。発行者またはファイル / フォルダがブラックリストに追加されます。

ブラックリストエディタを使った、既存のブラックリストへの実行可能ファイルまたはフォルダの追加

スキャン機能は、新規ブラックリストに追加する以外に、特定の場所から実行可能ファイルを既存のブラックリストに追加することができます。この場所はローカル、外部、またはネットワーク上のどこでも可能です。

- [スキャン] をクリックして、[ブラックリストスキャンの保存先] ダイアログを開きます。これにより選択した場所のすべての実行可能ファイルが検索されます。スキャンが終了すると、その結果はブラックリストに統合されます。
- [追加] をクリックすると、個々のフォルダと実行可能ファイルを追加できます。
- 以前に作成されたブラックリストを開くには、[開く] をクリックし、ブラックリストファイルを参照します。[追加]、[削除]、[スキャン]、または [マージ] の各ボタンを使って、必要な変更を加えます。これらのボタンは、ブラックリストから実行可能ファイルとフォルダを追加 / 削除します。これらは、コンピュータ上の実際のファイルまたはフォルダを変更するわけではありません。
- [ブラックリストのみ] ボタンをクリックして、ホワイトリストから実行可能ファイルを削除し、それらがブラックリストの一部であることを確認します。
- 同時に、複数のブラックリストを開き、編集することができます。有効なブラックリストとして設定できるリストは一度に 1 つだけです。

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。2 つのタイプの Anti-Executable ユーザーがあります。

- 管理者ユーザー – ホワイトリスト、ブラックリスト、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 – 有効なホワイトリストまたは有効なブラックリストを作成、構成、設定することができます。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 にリストされていないすべてのユーザーは、有効なホワイトリストによって指定された実行可能ファイル起動制限に従う外部のユーザーです。

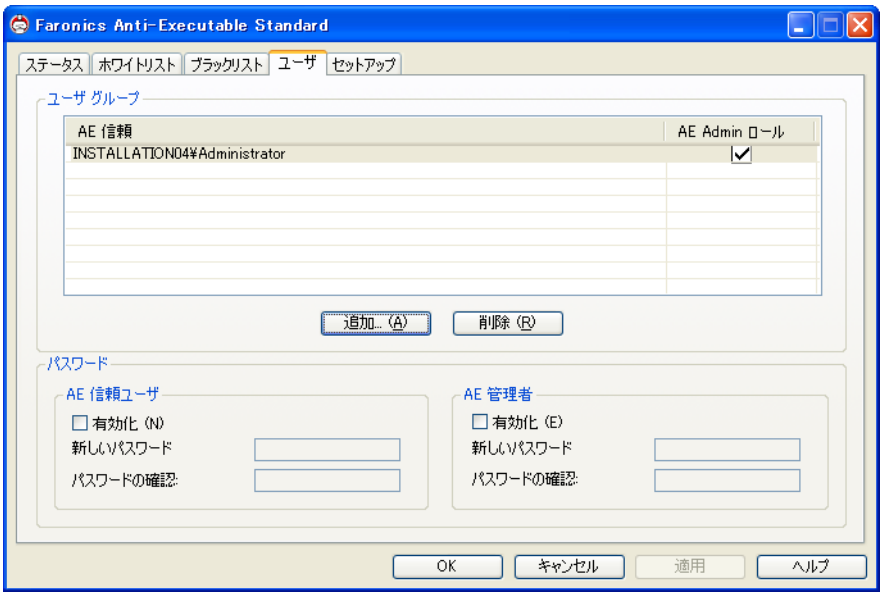
Anti-Executable が有効化されているときに、Anti-Executable 管理者または信頼ユーザーが、実行禁止ファイルを開こうと試みた場合、許可するか、拒否するか、または許可しホワイトリストに追加するかを選択するダイアログが表示されます。

Anti-Executable 管理者または信頼ユーザーの追加

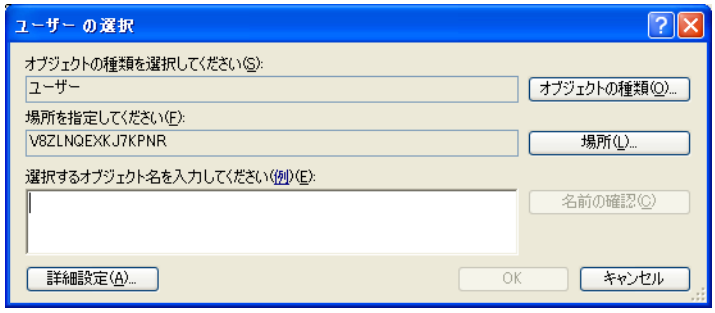
すべての Anti-Executable ユーザーは、既存の Windows ユーザーアカウントです。ただし、すべての Windows ユーザーアカウントが自動的に管理者または信頼ユーザーになるわけではありません。管理者または信頼ユーザーではない Windows ユーザーアカウントは外部ユーザーです。

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。

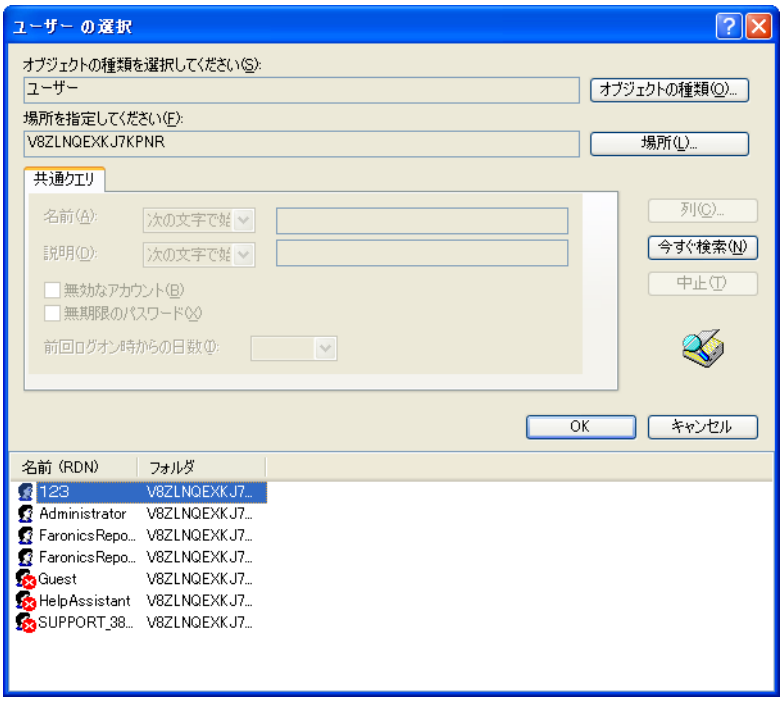
1. Anti-Executable ウインドウの上部の [ユーザー] タブをクリックします。



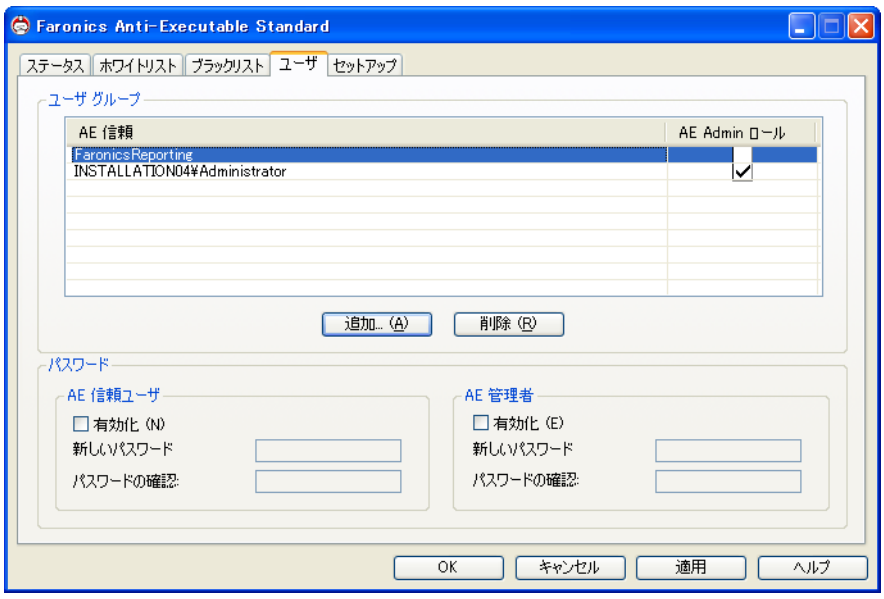
2. [追加] をクリックして、新規ユーザーを追加します。提示されたリストから、ユーザーアイコンを選択します。



3. リストが空の場合、[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。ログインしているドメイン管理者は、他のドメインユーザーを追加することができます。Anti-Executable のリストにユーザーを追加するには、ユーザー名をクリックし、[*OK*] をクリックします。



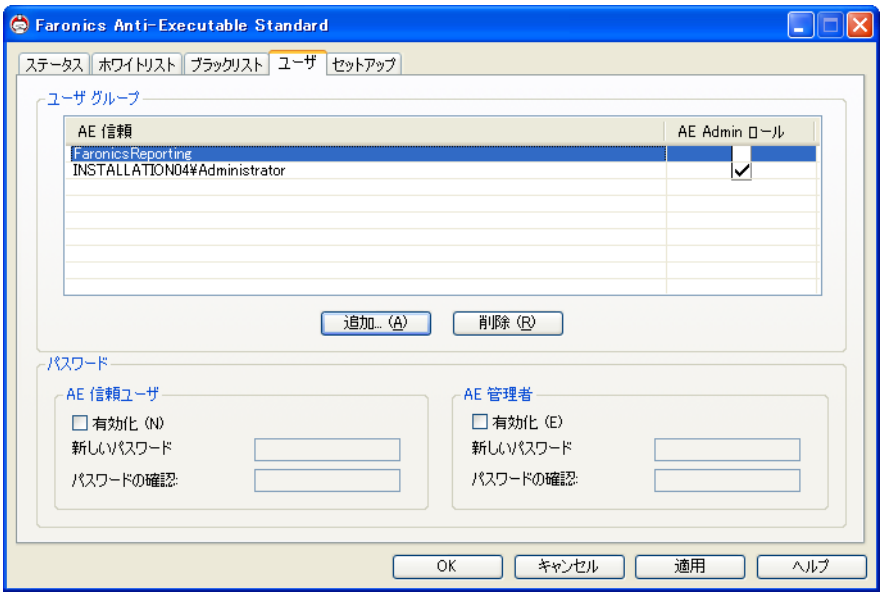
4. デフォルトでは、追加された各ユーザーは Anti-Executable 信頼ユーザーになります。新規ユーザーに管理者権限を与える場合、[*Anti-Executable Admin* ロール] チェックボックスを選択して、Anti-Executable 管理者として指定します。



5. 終了したら、[適用] をクリックします。

Anti-Executable 管理者または信頼ユーザーの削除

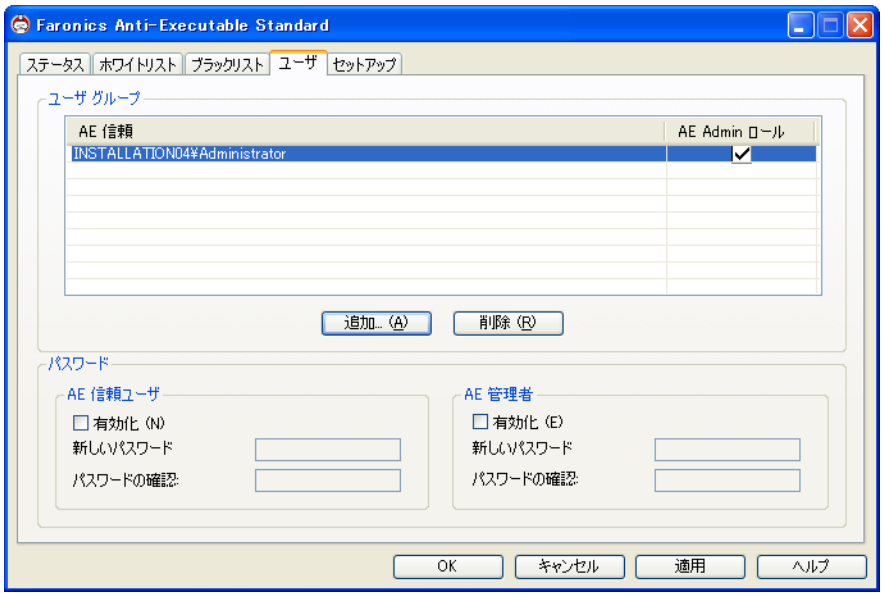
[ユーザー] タブをクリックし、削除するユーザーを選択します。[削除] をクリックします。これによりユーザーの Windows ユーザーアカウントが削除されるわけではありません。これで、ユーザーは外部ユーザーになります。



Anti-Executable パスワードの有効化

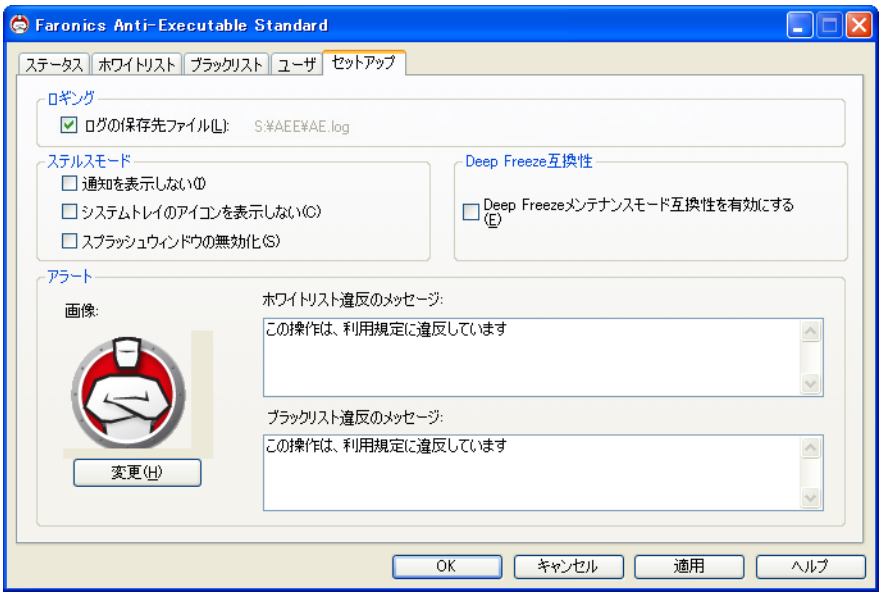
保護の強化として、Anti-Executable では、各ユーザーグループにパスワードを付加することができます。関連づけられたグループのメンバーのみにパスワードは適用されます。

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ます。[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。



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、Deep Freeze 互換性の有効化などができます。



Anti-Executable でのイベントロギングの設定

[ログの作成] を選択して、イベントビューアにイベントのログを作成します。ログファイルはワークステーションの S:/AEE/AE.log に保存されます。

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、アラートやスプラッシュ画面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。
- スプラッシュウィンドウの無効化 – Anti-Executable が起動される前に表示されていた Anti-Executable のスプラッシュウィンドウを無効にします。

Deep Freeze メンテナンス互換性

この機能は、コンピュータに Faronics Deep Freeze と Faronics 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 のメンテナンスモード互換性機能により、管理者は Deep Freeze と Anti-Executable のメンテナンスモードを同期させることができます。[*Deep Freeze* メンテナンスモード互換性を有効にする] チェックボックスを有効にすることで、Deep Freeze がメンテナンスモードになると、Anti-Executable も自動的にメンテナンスモードになります。

Deep-Freeze と Anti-Executable が同時にメンテナンスモード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、有効なホワイトリストに追加されるだけでなく、メンテナンスモード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 のメンテナンスモードが終了する少し前までメンテナンスモードが継続します。Anti-Executable のメンテナンスモードが終了すると、有効なホワイト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 のメンテナンスモードが終了すると、更新されたホワイトリストで保護状態になっているコンピュータが再起動します。

Deep Freeze が保護状態になっていると、[*Deep Freeze* メンテナンスモード互換性を有効にする] チェックボックスを選択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 がメンテナンスモードになると、Anti-Executable は無効の状態が続きます。

Deep Freeze によって開始するメンテナンス期間は、Anti-Executable で設定されているその他のメンテナンス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イメージ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。

- ホワイトリスト違反のメッセージ – ホワイトリストに違反があったときに表示されます。
- ブラックリスト違反のメッセージ – ブラックリストに違反があったときに表示されます。

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、ビットマップイメージを選択します。選択したイメージ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

Anti-Executable のアンインストール

この章では Anti-Executable のアンインストール手順について説明します。

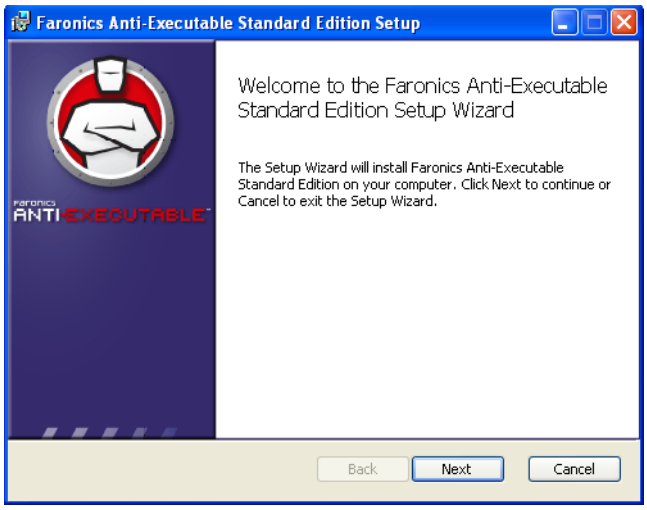
トピック

セットアップウィザードを使用したアンインストール

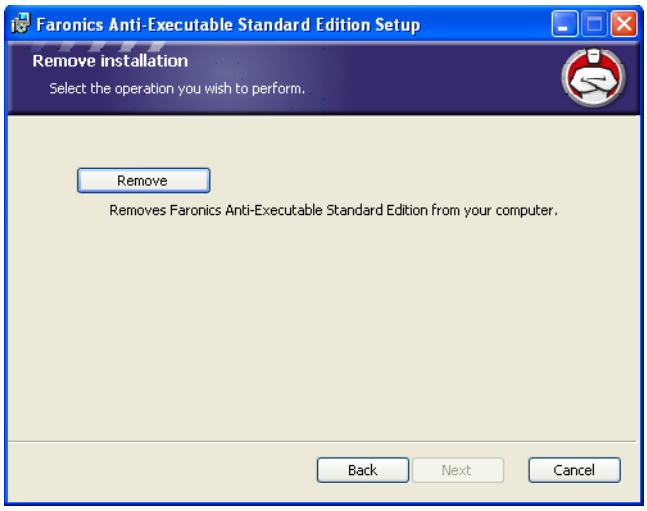
Anti-Executable のアンインストールは、Anti-Executable 管理者権限を持つユーザーとしてログインし、保護が無効に設定されているときにのみ行えます。

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

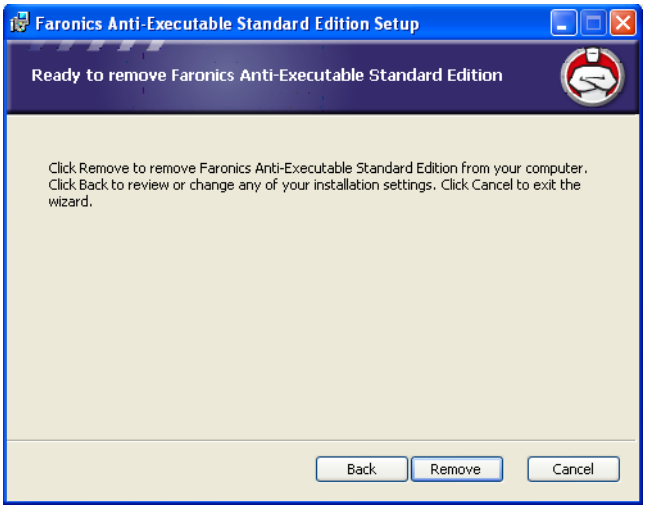
1. *.msi* ファイルをダブルクリックして、アンインストールプロセスを開始します。インストールウィザードが表示されます。



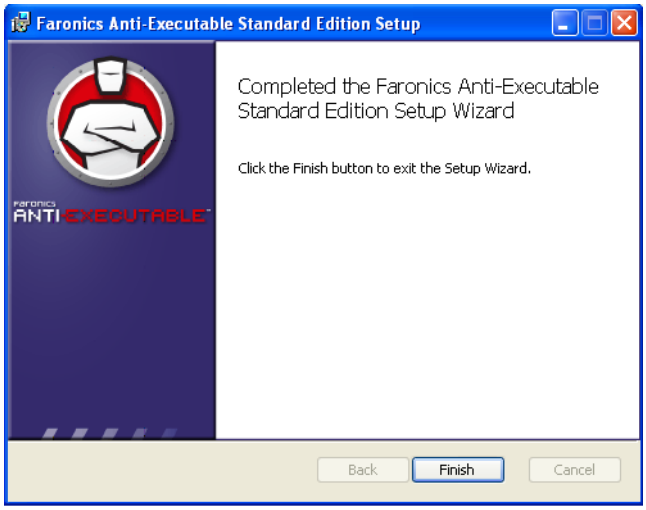
2. [削除] をクリックします。



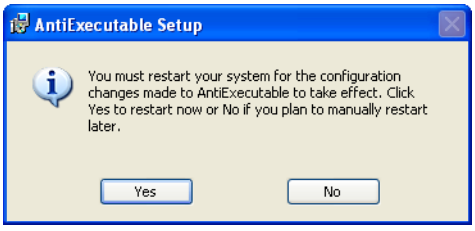
3. [削除] をクリックします。



4. アンインストールが終了したら、[完了] をクリックします。



5. アンインストールが正常に行われたら、再起動が必要になります。すぐに再起動する場合は [はい] をクリックし、後で再起動する場合は [いいえ] をクリックします。



アンインストール後、すぐに再起動することが推奨されます。