Faronics™
Simplifying Computer Management

Faronics
ANTI-VIRUS™

ADVANCED
System Integrity

ユーザーガイド

www.faronics.com

最新更新日 : 1 月 2023

目次

序文 5
重要な情報 6
Faronicsについて 6
製品マニュアル 6
テクニカル サポート 7
お問い合わせ 7
用語の定義 8

はじめに 11
Faronics Anti-Virus の概要 12
システム要件 13
Faronics Anti-Virus の要件 13
Faronics Coreの要件 13
Deep Freeze の要件 13
Faronics Anti-Virus のライセンス 14

Faronics Anti-Virus のインストール 15
インストール概要 16
Faronics Coreのインストール 16
Faronics Anti-Virus Loadin のインストール 17
Faronics Core によるワークステーションでの Faronics Anti-Virus のインストールまたはアップグレード 20
ワークステーションでの Faronics Anti-Virus の手動インストール 21

Faronics Anti-Virus の使用 23
Faronics Anti-Virus の概要 24
Faronics Core Console による Faronics Anti-Virus の管理 25
Faronics Anti-Virus Client のワークステーションへの配備 25
Faronics Anti-Virus の構成 25
Faronics Anti-Virus のリフレッシュ 27
Faronics Anti-Virus ポリシー 28
Faronics Anti-Virusポリシーの作成 28
Anti-Virusポリシーの適用 47
Anti-Virusポリシーの表示または変更 47
Anti-Virusポリシーの名前変更 47
ポリシーのコピー 48
Anti-Virusポリシーの削除 48
Anti-Virusポリシーのインポート 48
Anti-Virusポリシーのエクスポート 49
Faronics Core Console によるスキャン 50
隔離されたファイルの表示と操作 51

Faronics Core Console による Faronics Anti-Virus の更新 52
Faronics Core Console による Faronics Anti-Virus のスケジュール設定 53
レポートの生成 54
グローバル レポート 54
ワークステーション固有のレポート 54
ワークステーションでの Faronics Anti-Virus の使用 55
Faronics Anti-Virus のワークステーションでの起動 55
ワークステーションのスキャン 56
右クリックによるファイルまたはフォルダのスキャン 57
スキャン履歴の表示 58
検疫済みのファイルの表示と操作 59
ワークステーションでの Anti-Virus 定義の更新 60
ワークステーションでのシステム トレイによる Faronics Anti-Virus の管理 61

コマンドラインコントロール 63
コマンドラインコントロール 64

Faronics Anti-Virus のアンインストール 65
アンインストールの概要 66
Faronics Core Console による Faronics Anti-Virus Client のアンインストール 67
ワークステーションでの [プログラムの追加と削除] による Faronics Anti-Virus Client のアンインストール 68
インストーラによる Faronics Anti-Virus Loadin のアンインストール 69
[プログラムの追加と削除] による Faronics Anti-Virus Loadin のアンインストール 71

序文

本ユーザ ガイドは、Faronics Anti-Virus のインストール方法および使用方法について説明したものです。

トピック

重要な情報
テクニカル サポート
用語の定義

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、業界屈指の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革新的テクノロジーを有効にご利用いただいています。

製品マニュアル

Faronics Anti-Virus 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-Virus 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-Virus 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。

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 : 1-800-943-6422 または 1-604-637-3333

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 : 1-800-943-6422 または 1-604-637-3333
- ファックス : 1-800-943-6488 または 1-604-637-8188
- 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.
  5506 Sunol Blvd, Suite 202
  Pleasanton, CA, 94566
  USA

  Faronics Corporation [カナダおよびその他の国]
  609 Granville Street, Suite 1400
  Vancouver, BC V7Y 1G5
  Canada

  Faronics Corporation [ヨーロッパ]
  8 The Courtyard, Eastern Road,
  Bracknell, Berkshire,
  RG12 2XB, United Kingdom

用語の定義

用語	定義
アクティブ保護	アクティブ保護 [AP] とは、マルウェアをリアルタイムで検出する機能のことです。AP は作業中またはインターネットの閲覧中にバックグラウンドで常駐し、システムに目立った負担をかけることなく実行される [起動される] ファイルを常時監視します。
アドウェア	アドウェアとは、「広告ソフトウェア」とも呼称され、主としてコンテキストまたは行動の傾向に基づいて実行されるソフトウェアのことです。ユーザのウェブ閲覧傾向を追跡し、それに関連付けられたサードパーティ広告を表示します。この広告には、ポップアップ、ポップダウン、バナー、Web ページや一部の Windows インターフェイスに埋め込まれたリンクなど、いくつかの形式が存在します。アプリケーションやサイドバー、検索バー、検索結果に表示されるテキスト形式の広告で構成されるアドウェア広告もあります。
ファイアウォール	ファイアウォールは、受信トラフィックおよび送信トラフィックの両方から、双方向の保護を提供します。ファイアウォールは無許可の侵入からネットワークを保護します。
隔離場所	隔離場所とは、駆除できない可能性があるマルウェアや感染ファイルを保存するために Faronics Anti-Virus が使用する、コンピュータ上の安全な場所のことです。この場所に項目が置かれた後に、コンピュータまたはコンピュータ上のファイルが正常に動作しなくなった場合、リスクの詳細な確認と綿密な調査を実施した上で、当該項目を隔離場所から削除する機会が設けられます。その後、当該項目はコンピュータ上の元の場所に復元されます。当該項目 [リスクの原因] を、隔離場所から永久に削除することもできます。
不正なセキュリティ プログラム	不正なセキュリティ プログラムとは、出所が不明または不確かであるか、価値が疑われるソフトウェアのことです。不正なセキュリティ プログラムは、通常コンピュータがウイルスに感染していると主張し、それをスキャンおよび駆除することを提案してくる押し付けがましい警告として、Web サイトまたはスパム メール上に出現します。こうした警告は、決して信用すべきではありません。著名なアンチウイルス会社またはアンチスパイウェア会社が、このような通知方法を使用することはありません。不正なセキュリティ プログラムは、普通のアンチウイルス プログラムまたはアンチマルウェア プログラムのような見掛けをしていますが、実際にはユーザを欺いたり困らせたりすることによって、そのプログラムを購入するように仕向けます。不正なセキュリティ プログラムには、何の価値ももたらさない怪しげなセールスパーソンのようなものもあれば、マルウェアをインストールしたり、入力した信用情報を盗み出すことによって実害をもたらすものやなりすまし犯罪につながるものもあります。しかし、表示された警告を閉じたり、削除する際には、それらが偽の警告であるとわかっている場合でも、細心の注意を払う必要があります。

用語	定義
ルートキット	ルートキットとは、攻撃者がファイルやデータの存在を隠してそれらの検出を回避し、ユーザに気付かれないようにマシンのコントロールを奪うためのソフトウェアのことです。ルートキットは、ユーザやアンチウイルスおよびアンチスパイウェア アプリケーションなどのマルウェア検出ソフトウェアから発見されないようにするために、通常ウイルス、スパイウェア、トロイの木馬、バックドアといったマルウェアで使用されます。ユーザが好ましくないソフトウェアを削除することがないように、一部のアドウェア アプリケーションおよび DRM [Digital Rights Management: デジタル著作権管理] プログラムで使用されることもあります。
スパイウェア	スパイウェアとは、ユーザに通知することなく、第三者に情報を送信するソフトウェアのことです。別称として、トラックウェア、ハイジャックウェア、スカムウェア、スヌープウェア、スィーフウェアがあります。一部のプライバシー擁護派は、ユーザに通知することなく使用できるという共通点があるため、正当なアクセス コントロールおよびフィルタリング、インターネット モニタリング、パスワード リカバリ、セキュリティ、サーベイランス ソフトウェアさえ、スパイウェアと呼称しています。
トロイの木馬	トロイの木馬は、本物であると偽って、またはそのように見せ掛けて、多くの場合ユーザが十分な情報を得ることなく、同意もしていない状態でインストールされるプログラムのことです。言い換えれば、ユーザにとってまったく害がないように見えても、実際には悪質なコードを含んでいるプログラムのことです。トロイの木馬は、悪意や敵意のある、あるいは有害な機能を備えており、そうした動作をするものがほとんどです。
ウイルス	コンピュータ ウイルスとは、自己複製し、他のプログラムやファイルに侵入し、感染したマシン内で増殖する悪質なコードのことです。ウイルスが増殖する契機は、通常ユーザが感染したファイルを実行したり、感染したメディア、特に CD-ROM やフラッシュ ドライブなどのメディアをロードしたときです。感染した添付ファイルなどによって、電子メールを媒介として増殖する場合もあります。大多数のウイルスには、迷惑なものや混乱を招くものから有害なものや損害を及ぼすものまで、さまざまなペイロードが含まれています。ウイルスはシステム ダメージや重要なデータの損失を引き起こしたり、他のマルウェアをインストールするために使用されることがあります。
ワーム	ワームとは、ユーザの介入なしで自己増殖する悪質なプログラムのことです。自己複製するという点では、ウイルスに類似しています。しかし、他のプログラムやファイルに侵入または感染することなく増殖する点で、ウイルスとは異なります。ワームは、ネットワークに接続されている攻撃を受けやすいマシンのセキュリティ ホールから入り込み、コンピュータ全体に拡がることがあります。また、ユーザのアドレス帳に保存されているすべてのアドレスに、自身のコピーを送信することによって増殖する場合もあります。ワームは、大量のシステム リソースを消費し、システムの動作を著しく遅くしたり、その信頼性を損なうことがあります。感染したマシンのセキュリティを危険にさらし、別の悪質なソフトウェアをダウンロードさせるために使用されるワームもあります。

はじめに

Faronics Anti-Virus は、長いスキャン時間や大きなフットプリントによってコンピュータの処理速度を犠牲にすることなく、セキュリティ脅威からの保護を提供します。Faronics Anti-Virus は、高度に複雑化しているマルウェア脅威からユーザを保護するために、次世代テクノロジーを導入して開発された、強力なアンチウイルス機能およびアンチルートキット機能、アンチスパイウェア機能を 1 つにまとめたソフトウェアであり、Faronics Deep Freeze および Faronics Anti-Executable とのシームレスな統合により、完成された階層化セキュリティ ソリューションを提供します。

トピック

Faronics Anti-Virus の概要
システム要件
Faronics Anti-Virus のライセンス

Faronics Anti-Virus の概要

Faronics Anti-Virus は、以下の脅威からワークステーションを保護します。

- アドウェア
- 不正なセキュリティ プログラム
- ルートキット
- スパイウェア
- トロイの木馬
- ワーム

Faronics Anti-Virus は、Faronics Core から複数のワークステーションに配備できます。Faronics Core については、『Faronics Core ユーザ ガイド』を参照してください。最新のユーザガイドは、http://www.faronics.com/library からダウンロードできます。

Deep Freeze にインストールすると、*Thawed 状態で再起動*したり、*メンテナンス モード*で再起動することなく、Anti-Virus の定義をマネージド ワークステーションで更新することができます。詳細は、『Deep Freeze Enterprise ユーザ ガイド』を参照してください。最新のユーザガイドは、http://www.faronics.com/library からダウンロードできます。

システム要件

Faronics Anti-Virus の要件

Faronics Anti-Virus Loadin には次の環境が必要です。

- Faronics Core 3.7 以降

ワークステーション上の Faronics Anti-Virus Client には次のいずれかのオペレーティングシステムが必要です。

- Windows XP SP3 (32 ビット版) または Windows XP SP2 (64 ビット版)
- Windows 7 (32 ビット版または 64 ビット版)
- Windows 8.1 (32 ビット版または 64 ビット版)
- Windows10 バージョン 22H2 まで (32 ビット版または 64 ビット版)
- Windows11 バージョン 22H2 まで
- Windows Server 2008 R2 (64 ビット版)
- Windows Server 2012 (64 ビット版)
- Windows Server 2016 (64 ビット版)
- Windows Server 2019 (64 ビット版)
- Windows Server 2022 (64 ビット版)

どのコンポーネントのインストールも、Windows の管理者アカウントから行うようにしてください。

Faronics Core の要件

Faronics Core のシステム要件については、『Faronics Core ユーザ ガイド』を参照してください。最新のユーザガイドは、http://www.faronics.com/library からダウンロードできます。

Deep Freeze の要件

Deep Freeze のシステム要件については、『Deep Freeze Enterprise ユーザ ガイド』を参照してください。最新のユーザガイドは、http://www.faronics.com/library からダウンロードできます。

Faronics Anti-Virus を Deep Freeze によって管理されているワークステーションで動作させるには、Deep Freeze Enterprise 7.0 以降が必要です。

Faronics Anti-Virus のライセンス

Faronics Anti-Virus のライセンスは、Faronics Core Console から適用できます。Faronics Anti-Virus のライセンスを適用するには、次の手順を実行します。

1. Faronics Core Console を起動します。
2. [Core Server] を右クリックして、[プロパティ] を選択します。
3. [Anti-Virus] タブをクリックします。[Anti-Virus] タブには、[バージョン] および [ライセンス *キー*] [ライセンス版の場合]、[ライセンス有効期限] が表示されています。
4. [編集] をクリックし、[ライセンス キー] フィールドに *ライセンス キー*を入力します。
5. [適用] をクリックします。[OK] をクリックします。

Faronics Anti-Virus Licensing は、次のような機能があります。

- Core Server (Faronics Core のコンポーネント) は、ライセンス キーを Faronics Anti-Virus Client がインストールされたワークステーションに自動的に転送します (コンピュータがオフラインの場合は、オンラインになるとライセンス キーが適用されます)。

Loadin のインストール中に Faronics Anti-Virus のライセンス キーを入力した場合、[プロパティ] タブに再度入力する必要はありません。

Faronics Anti-Virus のライセンス キーが期限切れの場合、ウイルス定義をダウンロードすることはできません。

Faronics Anti-Virus のインストール

この章では、Faronics Anti-Virus のインストール方法を説明します。

トピック

インストール概要
Faronics Anti-Virus Loadin のインストール
Faronics Core によるワークステーションでの Faronics Anti-Virus のインストールまたはアップグレード
ワークステーションでの Faronics Anti-Virus の手動インストール

インストール概要

Faronics Anti-Virus は、次の 2 つのコンポーネントで構成されています。

- Faronics Anti-Virus Loadin – Faronics Core を備えているコンピュータにインストールします。
- Faronics Anti-Virus Client – Faronics Anti-Virus Loadin によって管理されるワークステーションに配備します。

Faronics Anti-Virus のインストールおよび設定には、次の段階が含まれます。

- Faronics Core のインストール、および Core Agent の生成 / 配備
- Faronics Anti-Virus Loadin のインストール
- Faronics Anti-Virus Client の配備

Faronics Core のインストール

Faronics Core のインストールおよび Core Agent インストーラの作成と配備に関する詳細は、『Faronics Core ユーザガイド』を参照してください。最新のユーザガイドは、http://www.faronics.com/library からダウンロードできます。

Faronics Anti-Virus Loadin のインストール

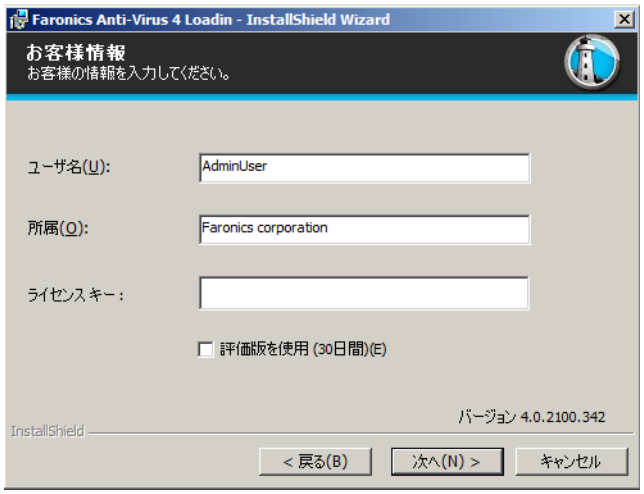
Faronics Anti-Virus Loadin をインストールするには、以下の手順を実行します。

Anti-Virus Loadin を、Faronics Core Console [または Faronics Core Server] がインストールされていないコンピュータにインストールすることはできません。

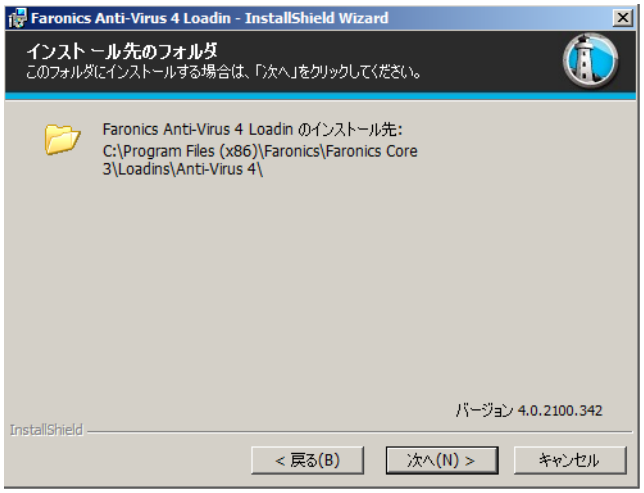
1. Anti-VirusLoadinInstaller.exe をダブルクリックします。[次へ] をクリックします。

2. 使用許諾契約書を読み、同意します。[次へ] をクリックします。

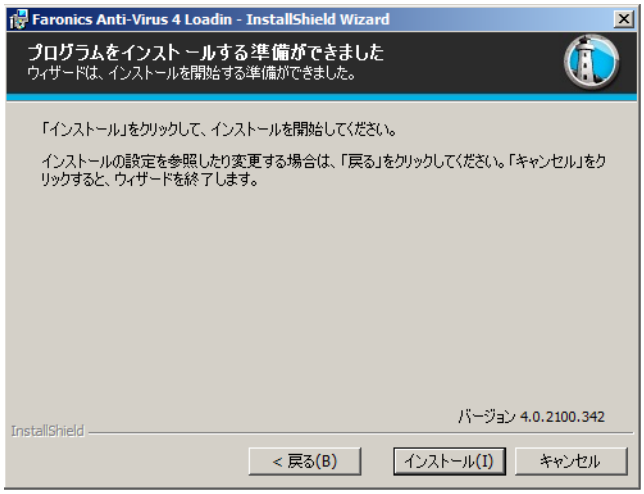
3. ユーザ名、所属、ライセンス キーを入力します。または、[評価版を使用] チェック ボックスを選択します。評価版 Faronics Anti-Virus の有効期間は、30 日です。[次へ] をクリックします。



4. デフォルトのロケーションは、`C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Virus` です。

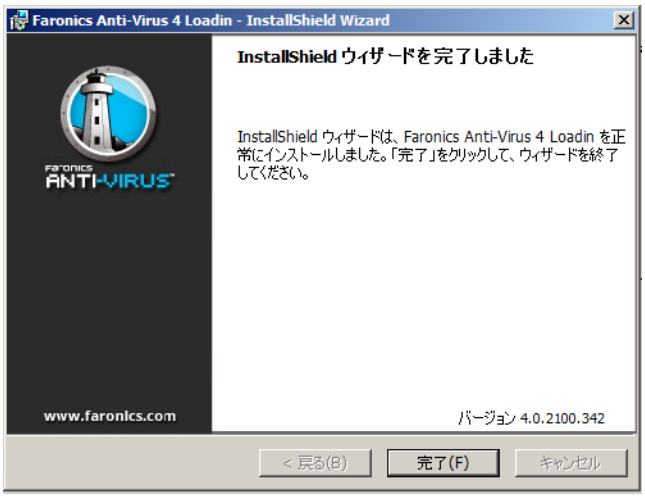


5. [インストール] をクリックして、Faronics Anti-Virus Loadin をインストールします。



6. 次のメッセージが表示されます。Faronics Core Server サービスをすぐに再起動するには、[はい] をクリックします。Faronics Core Server サービスを後で再起動するには、[いいえ] をクリックします。

7. [完了] をクリックして、インストールを終了します。



Faronics Core によるワークステーションでの Faronics Anti-Virus のインストールまたはアップグレード

Faronics Core の一部である Core Agent が、Faronics Anti-Virus によって管理されるワークステーション上にインストールされていなければなりません。Core Agent のインストールに関する情報は、『Faronics Core ユーザガイド』を参照してください。最新のユーザガイドは、http://www.faronics.com/library からダウンロードできます。

Core Agent がインストールされると、ネットワーク上でワークステーションが検出され、Core Console に表示されます。

Faronics Anti-Virus をインストールまたはアップグレードするには、1 台以上のワークステーションを選択して、

1. 右ペインで [ワークステーションの構成] をクリックし、[詳細] > [Faronics Anti-Virus クライアントのインストール / アップグレード] を選択します。
2. 別のアンチウイルスプログラムがインストールされている場合、以下のオプションを選択します。
   > Faronics Anti-Virus Enterprise Workstation をインストールする前に、互換性のないアンチウイルス製品を削除する。
   > 別のアンチウイルス製品がインストールされていたり、その製品を削除できなかった場合でも、Faronics Anti-Virus をインストールする。

インストールまたはアップグレードが正常に終了すると、ワークステーションが再起動します。

1 つ以上の Loadin がインストールされている場合、ワークステーションを右クリックし、[Anti-Virus] を選択し、特定のアクションを選択することで、Faronics Anti-Virus の右クリックコンテキストメニューにアクセスすることができます。

ワークステーションでの Faronics Anti-Virus の手動インストール

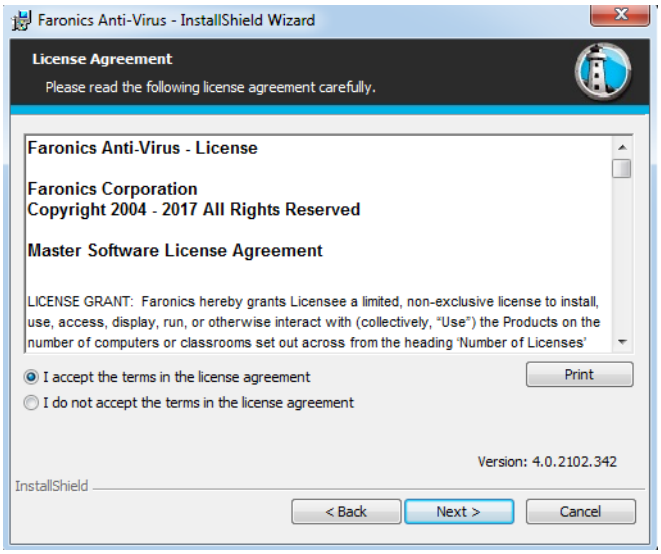
ワークステーションに Faronics Anti-Virus Client をインストールする前に、Anti-Virus Loadin がインストールされたコンピュータの `C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Virus\Wks Installers` というパスにある適切な .msi ファイルを、1 つ以上のワークステーションにコピーします。

Faronics Anti-Virus で保護する各ワークステーションに、同じ手順を繰り返します。

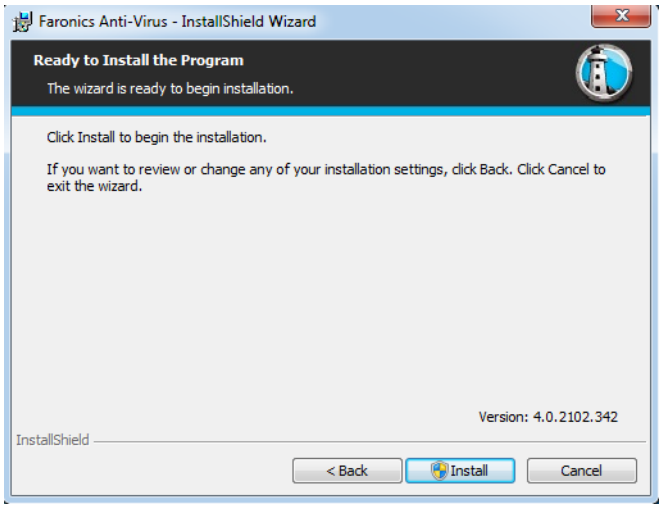
Faronics Anti-Virus をワークステーションにインストールするには、以下の手順を実行します。

1. 32 bit オペレーティング システムの場合は AntiVirus_Ent_32-bit.msi を、64 bit オペレーティング システムの場合は AntiVirus_Ent_64-bit.msi をダブルクリックします。[次へ] をクリックします。

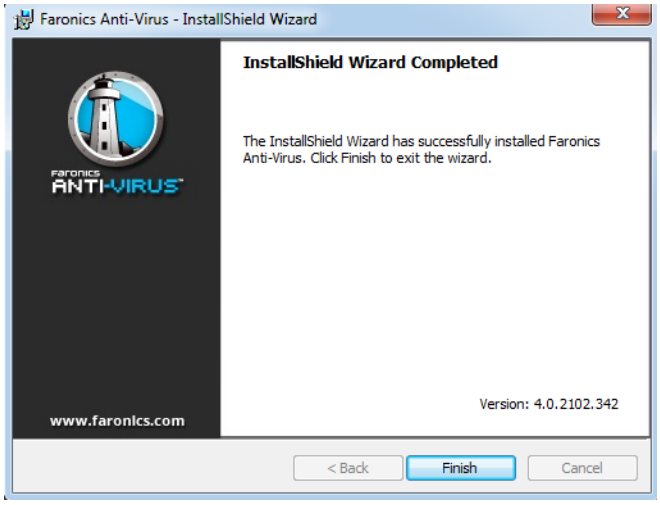
2. 使用許諾契約書を読み、同意します。[次へ] をクリックします。



3. [インストール] をクリックして、Faronics Anti-Virus をインストールします。



4. [完了] をクリックして、インストールを終了します。



ワークステーションに Anti-Virus Client をインストールした直後に、再起動することを推奨します。

Faronics Anti-Virus の使用

この章では、Faronics Anti-Virus の使用方法を説明します。

トピック

Faronics Anti-Virus の概要
Faronics Core Console による Faronics Anti-Virus の管理
Faronics Anti-Virus ポリシー
Faronics Core Console によるスキャン
隔離されたファイルの表示と操作
Faronics Core Console による Faronics Anti-Virus の更新
Faronics Core Console による Faronics Anti-Virus のスケジュール設定
レポートの生成
ワークステーションでの Faronics Anti-Virus の使用
ワークステーションでのシステム トレイによる Faronics Anti-Virus の管理

Faronics Anti-Virus の概要

Faronics Anti-Virus には、次のような使用方法があります。

Faronics Core Console による Faronics Anti-Virus の管理 :

- Faronics Anti-Virus Loadin のインストール [詳細は「Faronics Anti-Virus Loadin のインストール」を参照]
- Faronics Anti-Virus Client のワークステーションへの配備
- Anti-Virus ポリシーの作成、編集、削除、適用
- Faronics Core Console からのワークステーションのスキャン
- ファイアウォールの有効化 / 無効化
- スキャン履歴の表
- 隔離されたファイルの表示と操作
- Faronics Core Console からの Anti-Virus 定義の更新
- レポートの生成
- アクティブ保護の有効化 / 無効化
- ログの表示

ワークステーションでの Faronics Anti-Virus の使用

- Faronics Anti-Virus のワークステーションでの起動
- ワークステーションのスキャン
- ワークステーションでの Anti-Virus 定義の更新
- アクティブ保護の有効化 / 無効化
- ファイアウォールの有効化 / 無効化
- スキャン履歴の表
- 検疫済み

Faronics Core Console による Faronics Anti-Virus の管理

Faronics Anti-Virus Loadin のインストールが完了すると、Faronics Core Console によってワークステーションを管理できるようになります。Faronics Core Console による Faronics Anti-Virus 管理のさまざまな側面については、後続するセクションで説明します。

Faronics Anti-Virus Client のワークステーションへの配備

Faronics Anti-Virus Client をワークステーションに配備するには、以下の手順を実行します。

1. Faronics Core Console を起動します。
2. [コンソール ツリー] ペインで、[Faronics Core Console] > [Core Server の名前] > [ワークステーション] > [マネージド ワークステーション] の順に選択します。
3. 1 つ以上のワークステーションを右クリックして、[ワークステーションの構成] > [詳細] > [Anti-Virus Client のインストール / アップグレード] の順に選択します。

Faronics Anti-Virus Client が各ワークステーションにインストールされます。

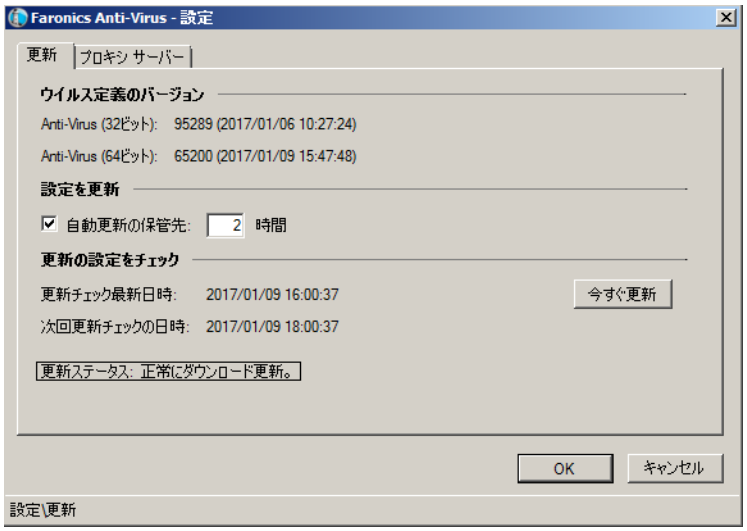
配備が正常に完了したワークステーションには、デフォルト ポリシーと最新のウイルス定義が備わっています。

Faronics Anti-Virus の構成

Faronics Anti-Virus を構成するには、以下の手順を実行します。

1. Faronics Core Console を起動します。
2. [コンソール ツリー] ペインで、[Faronics Core Console] > [Core Server の名前] > [ワークステーション] > [マネージド ワークステーション] > [Anti-Virus] の順に選択します。
3. Anti-Virus を右クリックして、[Anti-Virus の構成] を選択します。
4. [Faronics Anti-Virus の構成] ダイアログの [更新] タブが表示されます。

5. [更新] タブには、[スキャン エンジンのバージョン] と [ウイルス定義のバージョン] が表示されています。次のオプションをそれぞれ指定します。

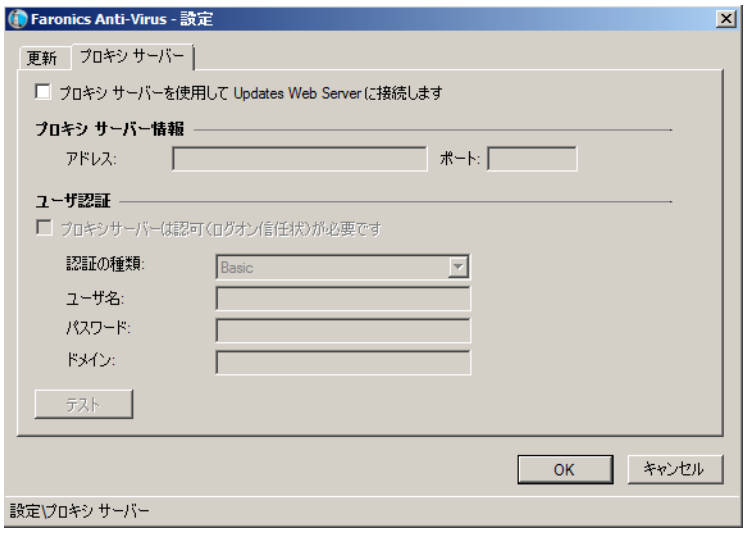


> [自動更新 – 時間を指定] – ウイルス定義を自動的に更新するには、このチェック ボックスを選択します。

> [時間] – 1 から 72 までの値を指定します。

> [今すぐ更新] – このボタンをクリックすると、Anti-Virus の定義が直ちに更新されます。

6. [プロキシ サーバー] タブをクリックして、次のオプションの各値を指定します。



7. [プロキシ サーバーを使用して更新用 Web サーバーと通信する] を選択して、次の情報を指定します。

> [アドレス] – IP アドレスまたは URL を指定します。

> [ポート] – ポートを指定します。

8. [プロキシ サーバーの認証情報 – ログオン証明書] を選択して、次の情報を指定します。
   > 認証タイプ
   > ユーザ名
   > パスワード
   > ドメイン
9. 接続をテストするには、[テスト] をクリックします。プロキシ設定を保存するには、[OK] をクリックします。

Faronics Anti-Virus のリフレッシュ

Faronics Anti-Virus を実行している単一ワークステーションの設定を取得するには、以下の手順を実行します。

1. Faronics Core Console を起動します。
2. [コンソール ツリー] ペインで、[Faronics Core Console] > [Core Server の名前] > [ワークステーション] > [マネージド ワークステーション] の順に選択します。
3. ワークステーションを右クリックして、[Anti-Virus のリフレッシュ] を選択します。
4. Faronics Anti-Virus がリフレッシュされ、次のカラムが更新されます。
   > ポリシー名
   > ステータス
   > スキャン進行度 [%]
   > 定義のバージョン
   > 最終更新日
   > 最終スキャン日
   > 最終脅威検出日
   > バージョン

Faronics Anti-Virus ポリシー

Anti-Virus ポリシーには、Faronics Anti-Virus をワークステーションで実行する方法に関するすべての設定が含まれています。つまり、プログラムによるアクション、スケジュール、プロキシサーバー、エラー報告、およびワークステーション上でユーザに許可された機能が含まれます。次のセクションでは、Anti-Virus ポリシーの作成と適用方法について説明します。

旧バージョンの Anti-Virus を使用している場合は、以下の手順を実行し、Anti-Virus の新バージョンに移行してください。

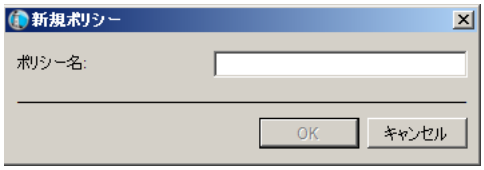
1. マネージドワークステーションから Anti-Virus の旧バージョンをアンインストールします。
2. 新しい Anti-Virus ポリシーを設定します。
3. マネージドワークステーションに新しい Anti-Virus をインストールします。

Faronics Anti-Virus には *デフォルト* のポリシーがあります。デフォルトのポリシーには、Faronics Anti-Virus を管理するための最適な設定が含まれています。

Faronics Anti-Virus ポリシーの作成

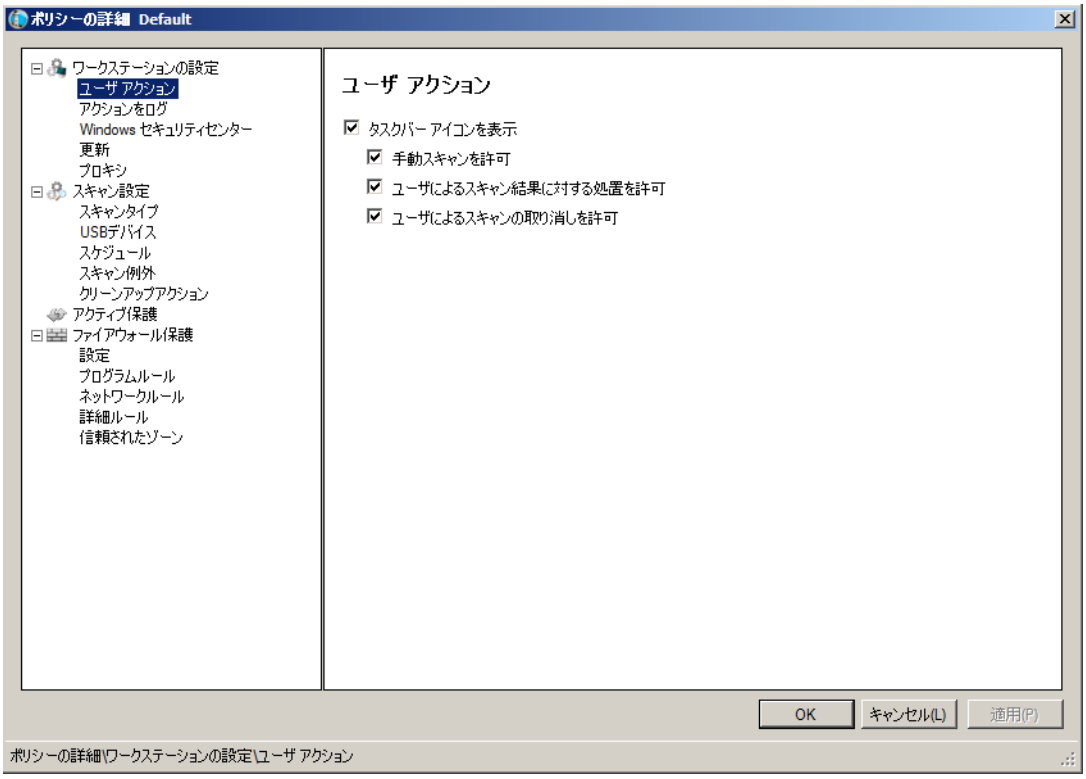
新しい Anti-Virus ポリシーを作成するには、以下の手順を実行します。

1. Faronics Core Console を起動します。
2. [コンソールツリー] ペインで [Faronics Core Console] > [Core Server の名前] > [ワークステーション] > [マネージドワークステーション] > [Anti-Virus] の順に選択します。
3. [Anti-Virus] を右クリックして、[新規ポリシー] を選択します。
4. [新規ポリシー] ダイアログで、ポリシーの名前を指定します。[OK] をクリックします。新しいポリシーが [Anti-Virus] ノードポリシーの下に作成されます。たとえば、新しいポリシーに [新規ポリシー 1] と名前を付けます。



5. [新規ポリシー 1] を右クリックして、[ポリシーの詳細] を選択します。[ポリシーの詳細] ダイアログが表示されます。
6. [ワークステーションの設定] ノードで、次の設定を指定します。

- [ユーザーアクション] ペイン



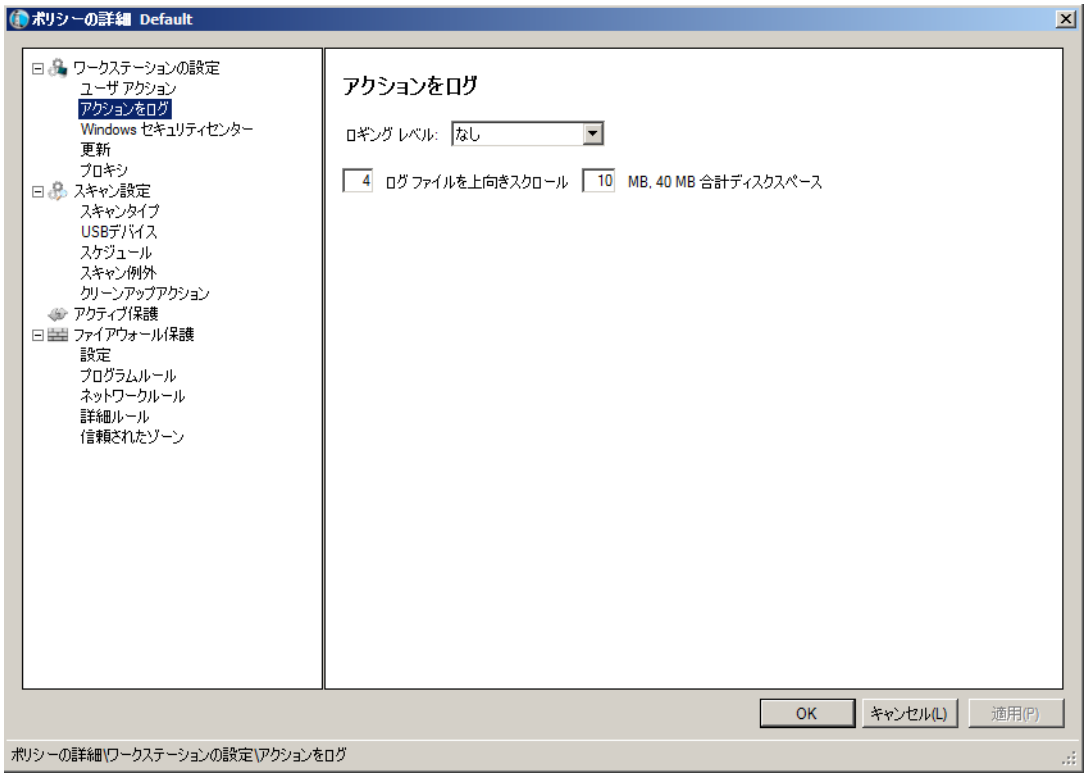
> [タスクバーにアイコンを表示する] – Faronics Anti-Virus アイコンをワークステーションのタスクバーに表示するには、このチェックボックスを選択します。チェックボックスを選択しないと、Faronics Anti-Virus はユーザーに表示されません。

~ [手動スキャンを許可する] – ユーザーがワークステーションで Faronics Anti-Virus のスキャンを手動で開始できるようにするには、このチェックボックスを選択します。

~ [ユーザーによるスキャン結果への対応を許可する] – ユーザーがワークステーションでスキャン結果に応じた行動を取れるようにするには、このチェックボックスを選択します。

~ [ローカルで開始したスキャンのユーザーによる中止を許可する] – ワークステーション上でローカルで開始したスキャンをユーザーが中止できるようにするには、このチェックボックスを選択します。

- [アクションのログ] ペイン

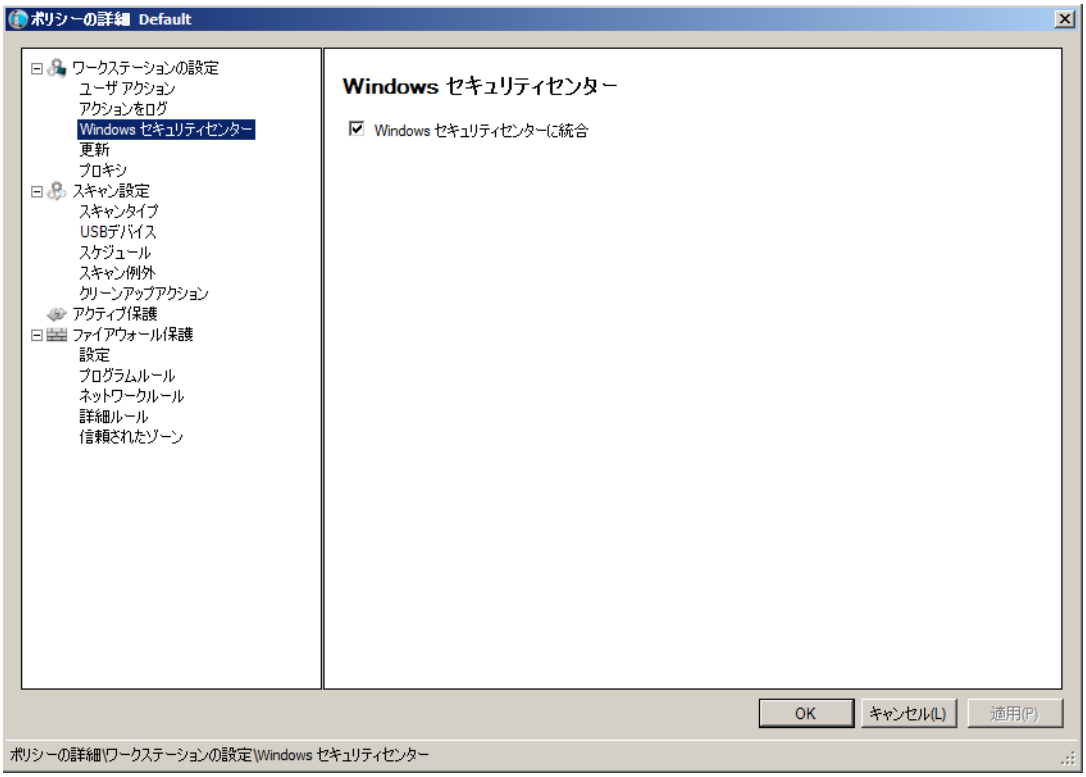


> [ロギングレベル] – ロギングレベルを選択します。ログを行わない場合は、[なし] を選択します。エラーメッセージのログを作成する場合は、[エラー] を選択します。トレースする場合は、[トレース] を選択します。詳細なログを作成する場合は、[詳細] を選択します。

> [ロギングファイルの数] – ロギングファイルの数を指定します。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 の 3 つのファイルがある場合、Faronics Anti-Virus は、まずファイル A にエラーログを書き込みます。ファイル A が満杯になると、ファイル B へ、次にファイル C の順に書き込みを行います。ファイル C が満杯になった場合はファイル A のデータが削除され、新しいロギングデータが書き込まれます。

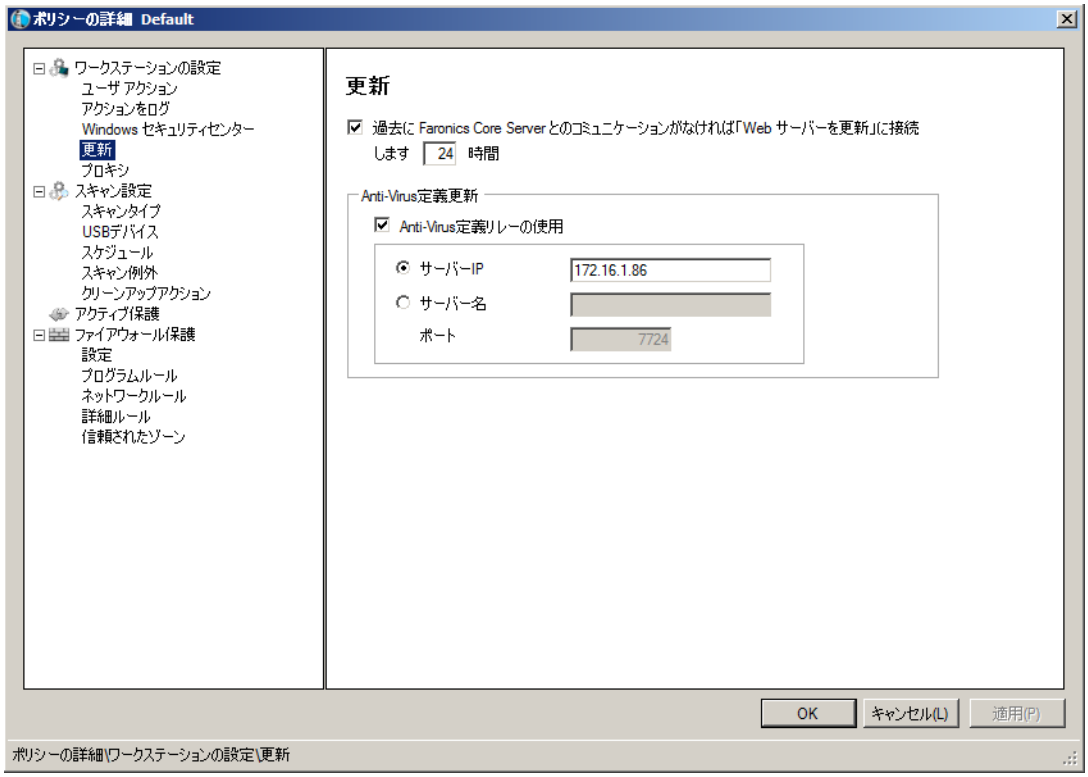
> [ファイルのサイズ] – 各ファイルのサイズを MB で選択します。

- [Windows セキュリティセンター] ペイン



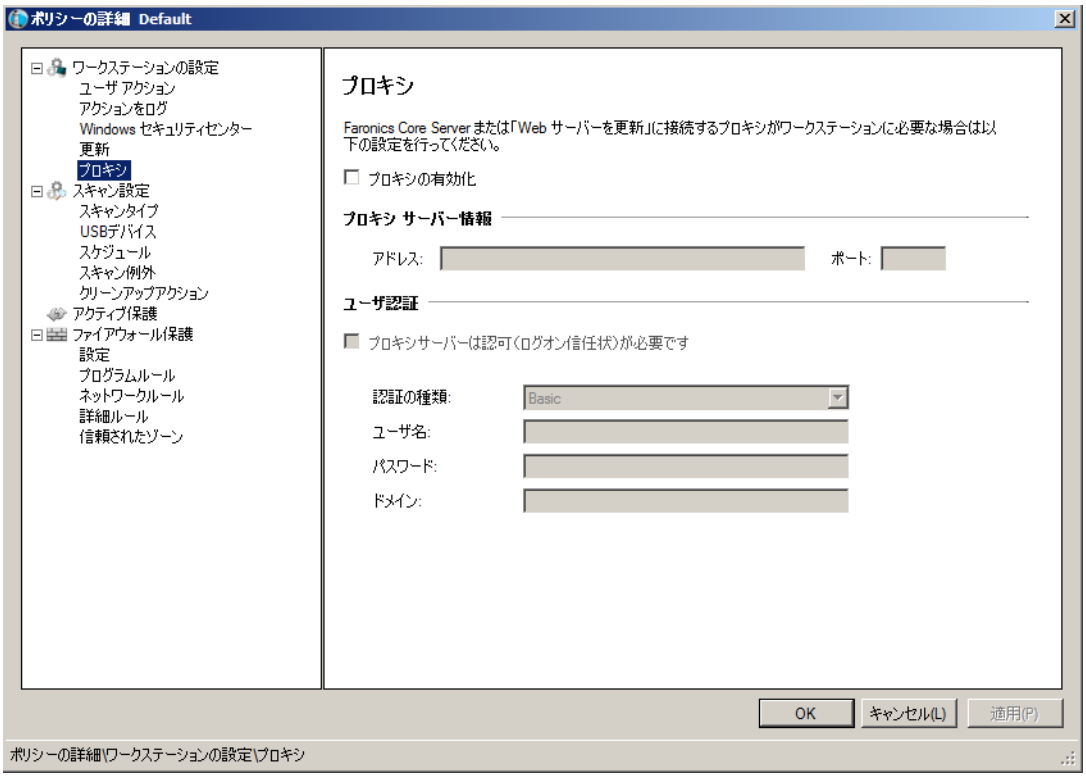
> [Windows セキュリティセンターと統合する] – Faronics Anti-Virus を Windows セキュリティセンターに統合するには、このチェックボックスを選択します。Windows セキュリティセンターは、Faronics Anti-Virus が有効化または無効化されると、システムトレイでそのことを通知します。

- [更新] ペイン



> [過去 X 時間内に Faronics Core Server と通信していない場合は更新用 Web サーバーに接続する] – ワークステーションと Faronics Core Server との通信が途絶えている場合は、このチェックボックスを選択して、更新用 Web サーバーに接続してウイルス定義をダウンロードできるようにします。チェックボックスを選択しないと、ワークステーションと Faronics Core Server との通信が途絶えている限り、ウイルス定義は更新されません。

- [プロキシ] ペイン



> [プロキシの有効化] – ワークステーションが Faronics Core Server または更新用 Web サーバーと通信する際にプロキシが必要な場合、このチェックボックスを選択します。

> [プロキシサーバー情報] – [アドレス] と [ポート] に値を指定します。

> ユーザ認証

[プロキシサーバーは認可 (ログオン信任状) が必要です] – サーバーで認証が必要な場合、次のフィールドに値を指定します。

~ [認証の種類] – 認証タイプを選択します。

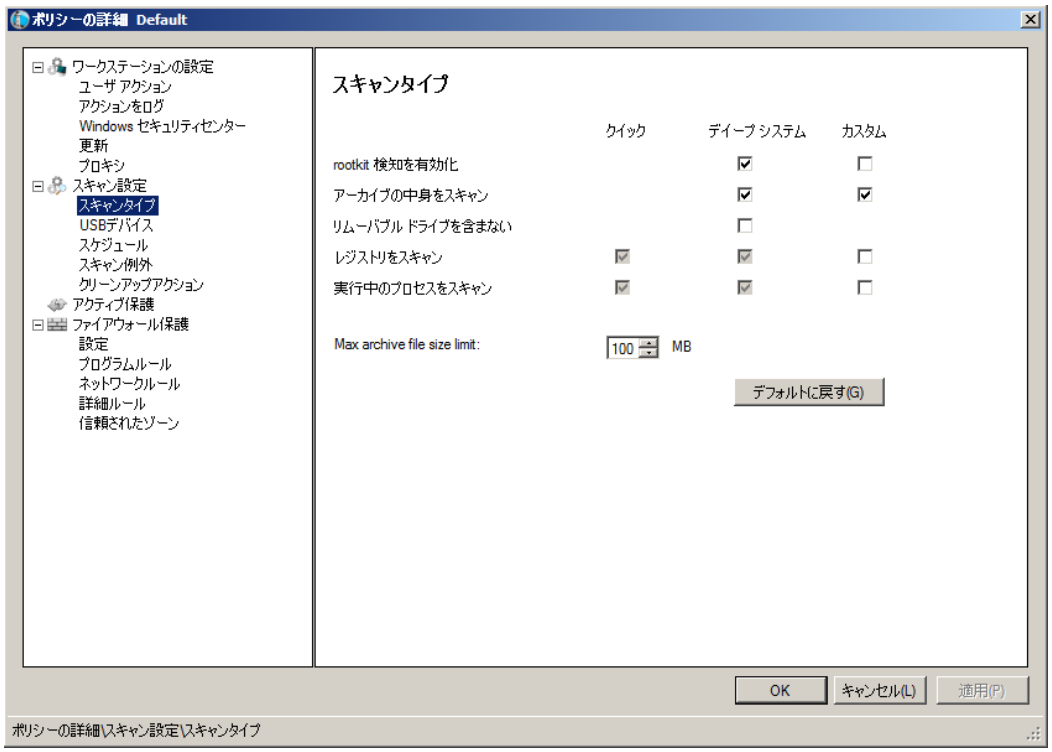
~ [ユーザ名] – ユーザー名を指定します。

~ [パスワード] – パスワードを指定します。

~ [ドメイン] – ドメインを指定します。

7. [スキャン設定] ノードで次の設定を指定します。

- [スキャンタイプ] ペイン



Faronics Anti-Virus では、次の 3 種類のスキャンが利用できます。

> [クイックスキャン] – コンピュータの影響を受けやすい領域をスキャンします。ディープシステムスキャンよりも短い時間でスキャンを完了できます。メモリの使用量もディープスキャンより少なくすみます。

> [ディープシステムスキャン] – コンピュータのすべての領域を詳細にスキャンします。スキャンに要する時間は、ハードドライブのサイズによって異なります。

> [カスタムスキャン] – [ポリシーの詳細] ダイアログでの選択に基づいて、スキャンします。

各タイプのスキャンごとに、次のオプションを選択します (タイプによってはグレーアウトされているオプションもあります)。

> [ルートキット検出を有効化する] – コンピュータがルートキットに感染している場合、それを検出します。

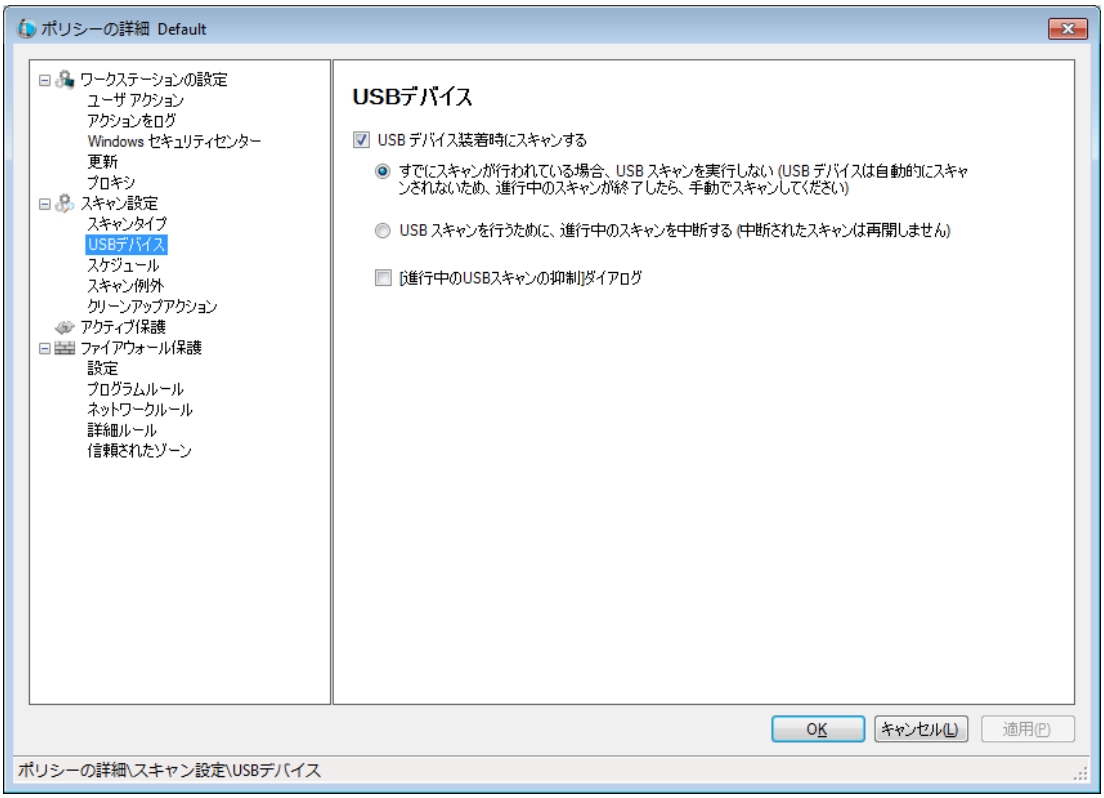
> [アーカイブ内をスキャン] – zip ファイルのコンテンツをスキャンします。スキャンの対象に、.RAR ファイルや .ZIP ファイルなどのアーカイブファイルを含めることができます。.RAR ファイルに感染したファイルが含まれていることがわかった場合、この .RAR は隔離されます。.ZIP ファイルに感染ファイルが含まれていることがわかった場合、感染ファイルは隔離されて .TXT ファイルに置換され、ウイルスへの感染と隔離を示すテキストが表示されます。[ファイルサイズの制限] を指定します。

> [USB などのリムーバブルドライブを除外する]- スキャン対象から、リムーバブルドライブを除外します。外付けのハードディスクや USB ドライブなどが、スキャンされなくなります。

> [レジストリをスキャン] – レジストリをスキャンします。

> [実行中のプロセスをスキャン] – 実行中のすべてのプロセスをスキャンします。

- [USB デバイス] ペイン



[USB デバイスの装着時にスキャンする] – USB デバイスの装着時にスキャンを行うには、チェックボックスを選択し、次のいずれかのオプションを選択します。

> [すでにスキャンが行われている場合、USB スキャンを実行しない] – USB デバイスの装着時に進行中のスキャンが中断されないようにするためには、このオプションを選択します。進行中のスキャンが終了したら、USB デバイスを手動でスキャンする必要があります。

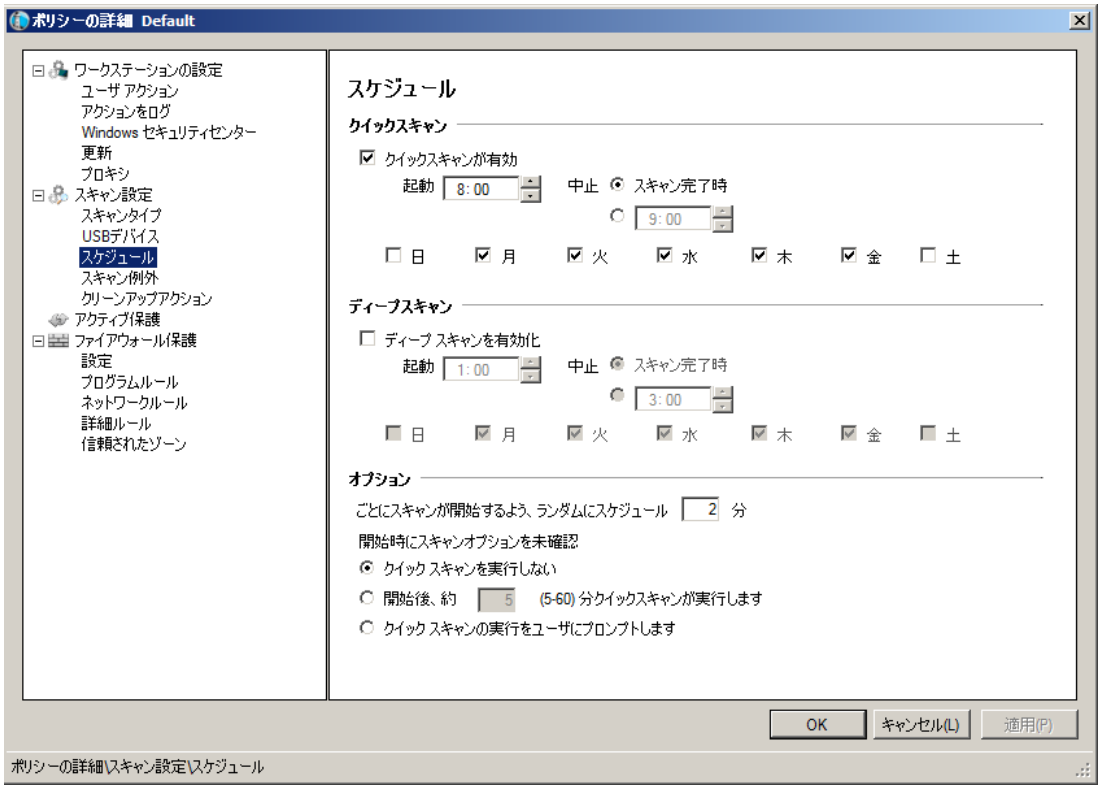
> [USB スキャンを行うために、進行中のスキャンを中断する] – USB デバイスを装着時にスキャンするために進行中のスキャンを中断するには、このオプションを選択します。進行中のスキャンは自動的には再開されないため、手動で再開する必要があります。

> [進行中の USB スキャンを抑制する] – USB デバイスの装着時にウイルス対策ソフトがスキャンを実行していることを表示しないようにするには、このオプションを選択します。ウイルス対策ソフトのインターフェイスはどれも表示されず、システムトレイアイコンもスキャンを進行中であることを示すツールチップを表示しません。ウイルスが検出されるとスキャン終了時にユーザーに通知されますが、検出されなかった場合はスキャンの実行に関する通知は表示されません。

[USB デバイスの装着時にスキャンする] オプションを選択していないと、このオプションは無視されます。

[ワークステーション設定] タブ > [ユーザ アクション] ペインで [手動スキャンを許可] チェックボックスを選択した場合、USB デバイスは自動的にスキャンされます。[手動スキャンを許可] チェックボックスを選択しないと、USB デバイスは自動的にはスキャンされません。

- [スケジュール] ペイン



クイックスキャン：

> [クイックスキャンを有効化する] – クイックスキャンを有効化するには、このチェックボックスを選択します。

> [開始] – 開始時間を指定します。

> [終了] – 終了時間を指定します。*開始*時間から*終了*時間までに設定できる最長時間は *23.59* 時間です。*終了*時間前にすべてのファイルがスキャンされた場合、その時点でスキャンは終了します。*終了*時間前にスキャンが完了しなかった場合、スキャンは*終了*時間に中止されます。スキャンを確実に完了するには、[スキャンが完了した時点] を選択します。

> [曜日] – スケジュール設定したクイックスキャンを実行する曜日を選択します。

ディープスキャン：

> [ディープスキャンを有効化する] – ディープスキャンを有効化するには、このチェックボックスを選択します。

> [開始] – 開始時間を指定します。

> [終了] – 終了時間を指定します。*開始*時間から*終了*時間までに設定できる最長時間は *23.59* 時間です。*終了*時間前にすべてのファイルがスキャンされた場合、その時点でスキャンは終了します。*終了*時間前にスキャンが完了しなかった場合、スキャンは*終了*時間に中止されます。スキャンを確実に完了するには、[スキャンが完了した時点] を選択します。

> [曜日] – スケジュール設定したディープスキャンを実行する曜日を選択します。

オプション：

> [スケジュール設定したスキャンの起動時刻を x 分無作為化する] – 分数を指定します。スケジュール設定したスキャンの開始時間を無作為化することで、ネットワークトラフィックに及ぼす影響を抑制します。スキャンが開始されると、Faronics Anti-Virus が Faronics Core にレポートを送信します。複数のシステムを対象としたスキャンを同時に起動するように設定している場合、この送信によってネットワークトラフィックに悪影響が及ぶ可能性があります。

システム起動時に実行されなかったスキャンのオプション – スケジュール設定した時間にワークステーションが *オン*になっていなかった場合に、次のオプションのいずれかを選択して、どのようなスキャンを行うかを指定します。

> [クイックスキャンを実行しない] – システム起動時にクイックスキャンを実行しないようにするには、このオプションを選択します。

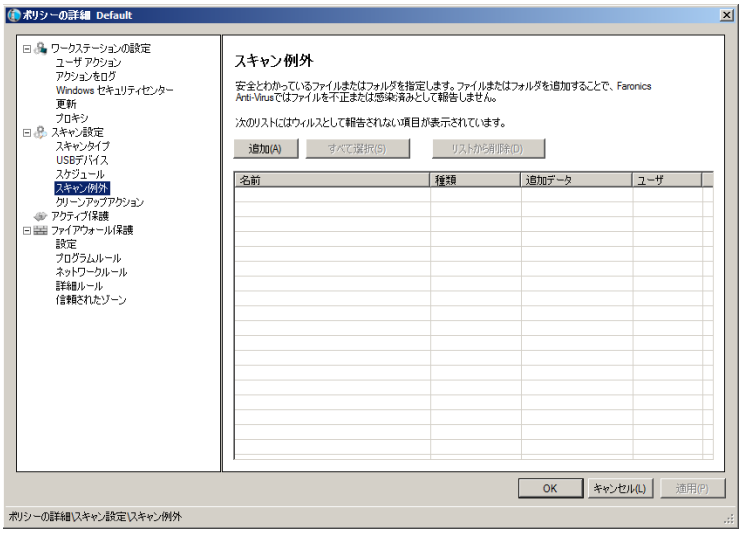
> [システムが起動してから約 x 分後にクイックシステムを実行する] – システムが起動した後に、Faronics Anti-Virus がクイックスキャンを開始するまでの分数を指定します。

> [クイックスキャンを実行するようにユーザーに指示する] – クイックスキャンを実行するようにユーザーに指示するには、このオプションを選択します。

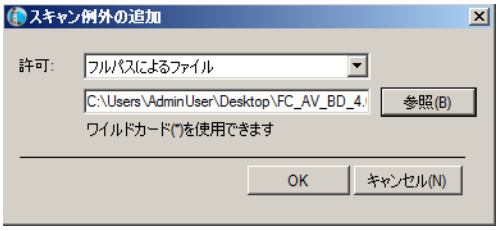
- [スキャン例外] ペイン

  安全で感染していないことがわかっているフォルダまたはファイルは、[スキャン例外] タブに追加できます。[スキャン例外] タブに追加されたファイルは常に Faronics Anti-Virus によりスキャンされますが、それらのファイルは Faronics Anti-Virus により不正または感染ファイルとして報告されません。管理者にとって安全であることがわかっているファイルやフォルダは不正ファイルとして報告されないため、この機能は便利です。

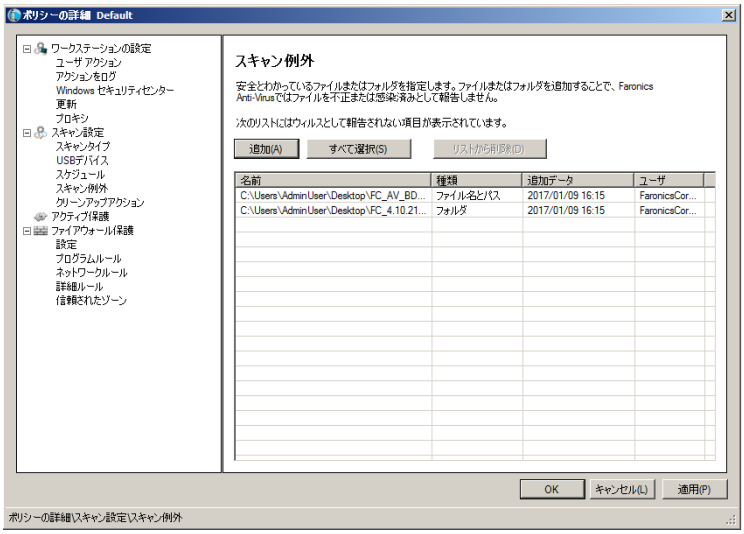
  A. [追加] をクリックします。



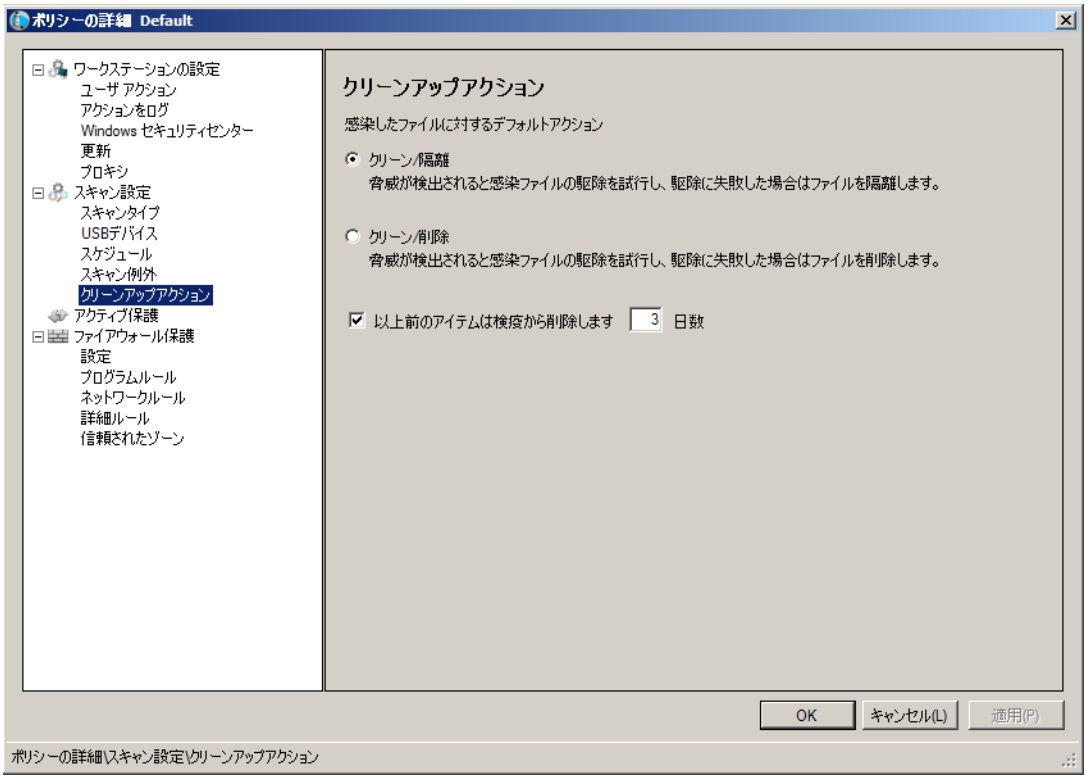
  B. [追加] ダイアログで、[フルパスによるファイル]、[フォルダ全体] のいずれかを選択します。[参照] をクリックしてファイルまたはフォルダを選択し、[OK] をクリックします。



  C. [フルパスによるファイル] が [スキャン例外] ペインに追加されます。



- [クリーンアップアクション] ペイン

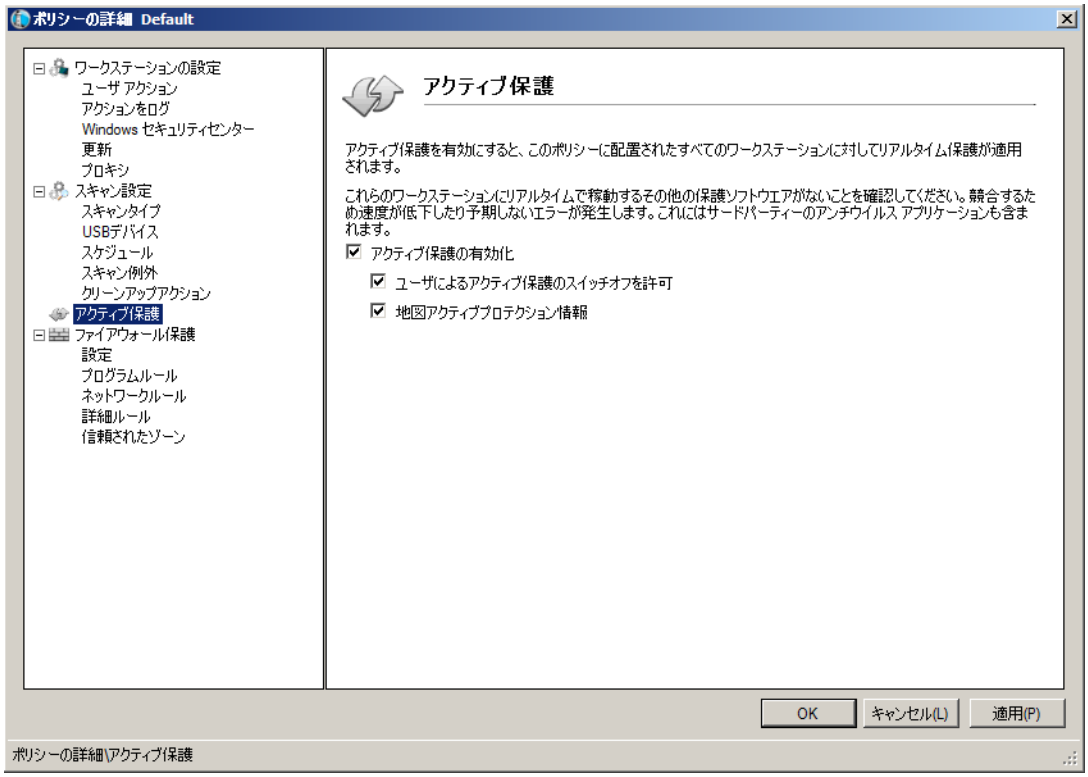


> クリーン / 隔離 – 脅威が検出されると感染ファイルの駆除を試行し、駆除に失敗した場合はファイルを隔離します。

> クリーン / 削除 - 脅威が検出されると感染ファイルの駆除を試行し、駆除に失敗した場合はファイルを削除します。

> [指定した日数を超えて隔離されている項目を隔離場所から削除する] – 隔離場所に項目を保持する日数を指定します。デフォルトは 3 日です。

8. [アクティブ保護] ペインで次の設定を指定します。

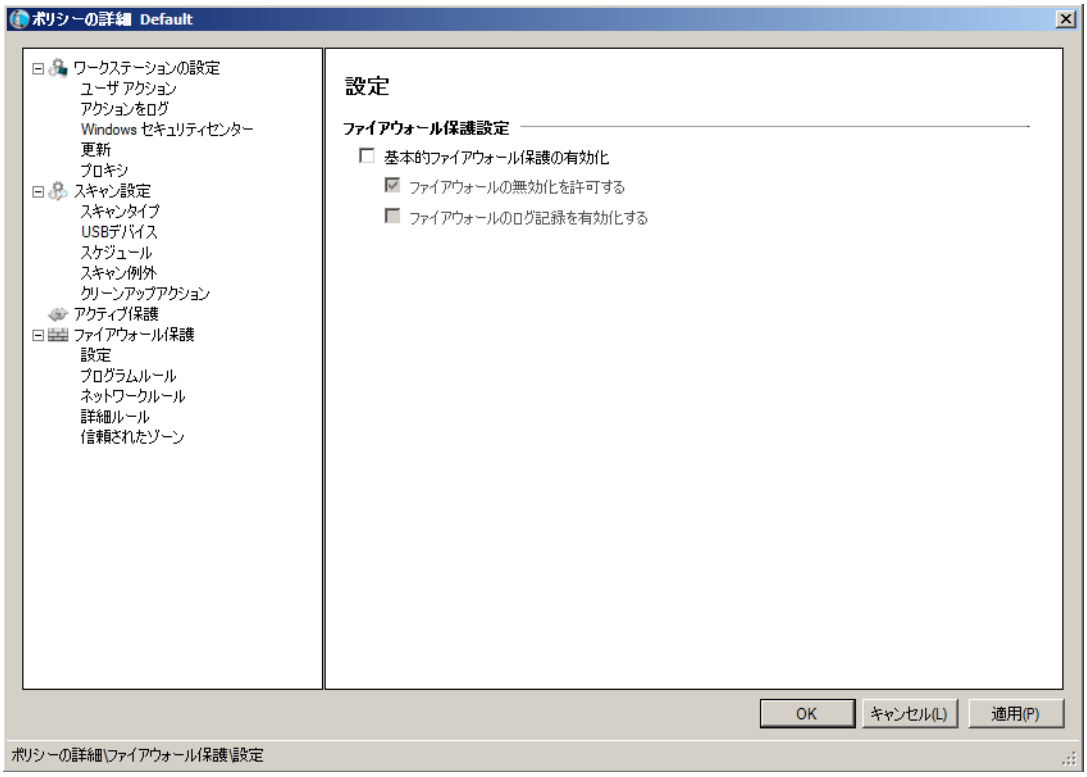


- [アクティブ保護を有効化する] – リアルタイム保護を有効化するには、このオプションを選択します。アクティブ保護は、システムパフォーマンスに影響を及ぼすことなく、Faronics Anti-Virus によって、バックグラウンドで実行されるリアルタイムスキャンです。インターネットからリアルタイムでウイルスに感染するリスクが存在する場合は、このオプションを選択します。
  - > [ユーザーがアクティブ保護をオフにできるようにする] – ユーザーがアクティブ保護をオフにできるようにするには、このオプションを選択します。ウイルスと間違えられる可能性のあるソフトウェアをユーザーがインストールまたは使用する場合 (たとえば Microsoft Office や複雑なバッチファイルで高度なマクロを実行するなど) は、このオプションを選択します。
  - > [アクティブ保護アラートを表示する] – アクティブ保護中に脅威が検出されるとアラートが表示されるようにするには、このオプションを選択します。アラートを表示したくない場合は、このチェックボックスを選択しないでください。

9. [ファイアウォール保護] ノードで次の設定を指定します。

   [ファイアウォール保護] ノードは、受信トラフィックおよび送信トラフィックの両方から、双方向の保護を提供します。ネットワークを保護するために、必要に応じたルールを作成することができます。通信に対し、[許可] または [ブロック] を選択します。

- [設定] ペイン



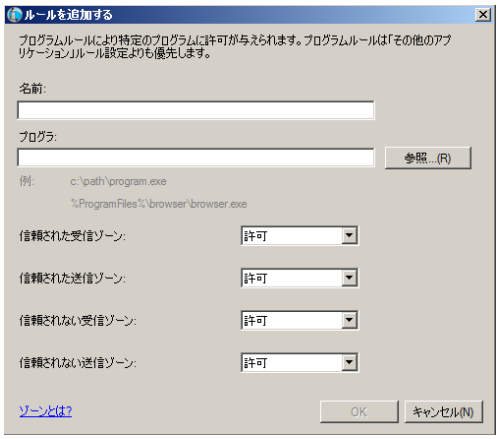
ファイアウォール保護設定

> [基本的ファイアウォール保護の有効化] – ファイアウォール保護を有効化するには、このチェックボックスを選択します。ファイアウォール保護により、ハッカーや悪意のあるソフトウェアがインターネットまたはネットワークを通じてコンピュータにアクセスすることを防ぎます。
>
> ~ [ファイアウォールの無効化を許可する] – ユーザーがコンピュータでファイアウォールを無効化できるようにするには、このオプションを選択します。
>
> ~ [ファイアウォールのログ記録を有効化する] – ファイアウォールに関連するすべてのアクションのログを作成するには、このオプションを選択します。

- [プログラムルール] ペイン

  プログラムルールは、ネットワークアクティビティとアプリケーションの間のファイアウォールのアクションを定義します。プログラムルールはデフォルトのルールよりも優先します。デフォルトのルールは編集できますが、削除はできません。

[追加]をクリックして、新しいプログラムルールを追加します。オプションを指定または選択し、[OK]をクリックします。次のパラメータが表示されます。



> [名前] – ルールの名前。

> [プログラム] – フルパスと拡張子を含む、プログラムの名前。

> [信頼されたゾーン受信] – 信頼されたゾーンのプログラムへの通信に対して取られるアクション ([許可]、[ブロック])。

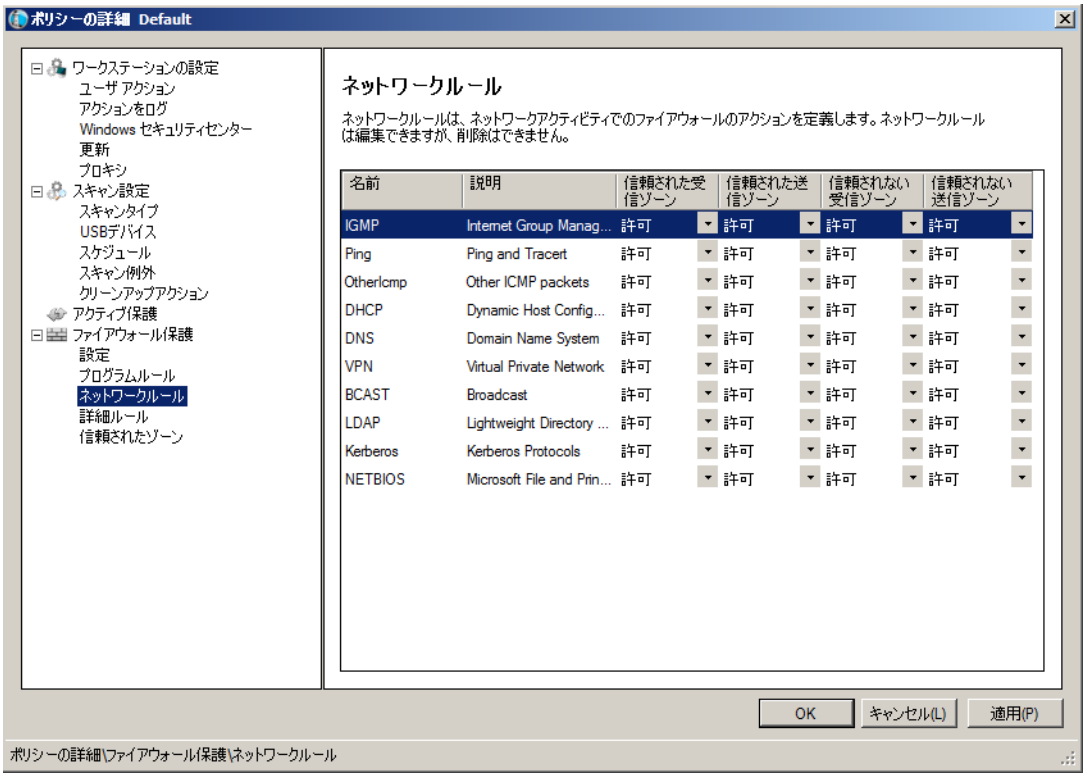
> [信頼されたゾーン送信] – 信頼されたゾーンのプログラムからの通信に対して取られるアクション ([許可]、[ブロック])。

> [信頼されないゾーン受信] – 信頼されないゾーンのプログラムへの通信に対して取られるアクション ([許可]、[ブロック])。

> [信頼されないゾーン送信] – 信頼されないゾーンのプログラムからの通信に対して取られるアクション ([許可]、[ブロック])。

- [ファイアウォール保護] ノード > [ネットワークルール] ペイン

  ネットワークルールは、ネットワークアクティビティでのファイアウォールのアクションを定義します。ネットワークルールは編集できますが、削除はできません。

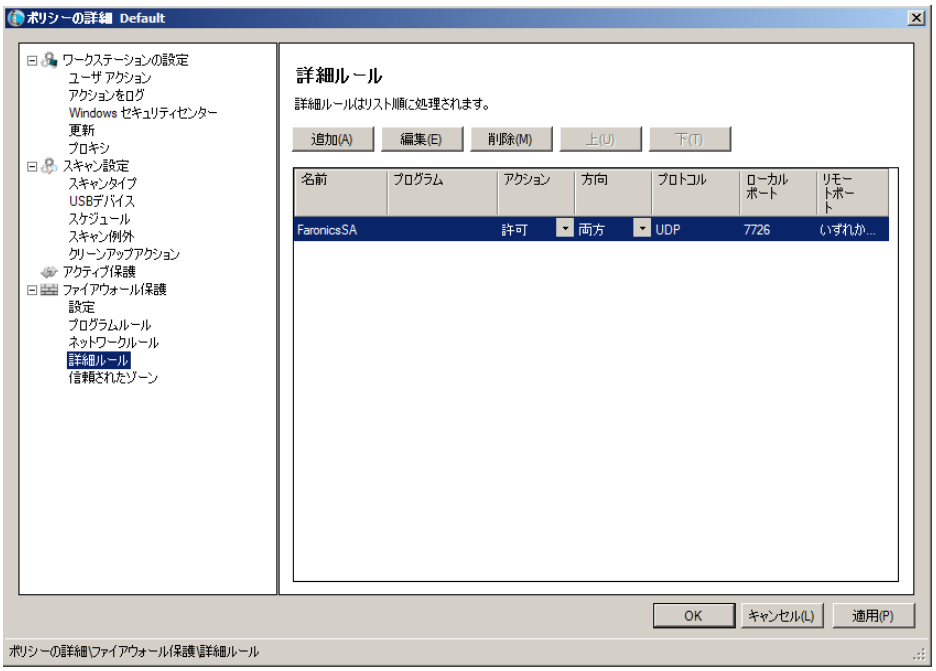


次の項目のネットワークルールを選択します。

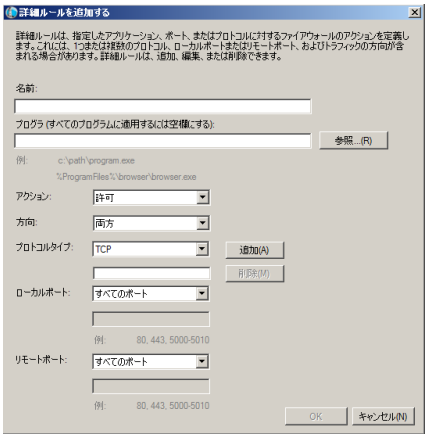
名前	説明	信頼された受信ゾーン	信頼された送信ゾーン	信頼されない受信ゾーン	信頼されない受信ゾーン
IGMP	インターネットグループ管理プロトコル	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択
Ping	Ping および Tracert	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択
OtherIcmp	その他 ICMP パケット	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択
DHCP	動的ホスト構成プロトコル	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択
DNS	ドメインネームシステム	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択
VPN	仮想プライベートネットワーク	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択
BCAST	ブロードキャスト	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択
LDAP	ライトウェイトディレクトリアクセスプロトコル	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択
Kerberos	ケルベロスプロトコル	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択
NETBIOS	Microsoft ファイルおよびプリンタの共有	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択	[許可] または [ブロック] を選択

- [詳細ルール] ペイン

  詳細ルールは、指定したアプリケーション、ポート、またはプロトコルに対するファイアウォールのアクションを定義します。これには、1つまたは複数のプロトコル、ローカルポートまたはリモートポート、およびトラフィックの方向が含まれる場合があります。詳細ルールは、追加、編集、または削除できます。



[追加]をクリックして、新しい詳細ルールを追加します。オプションを指定または選択し、[OK]をクリックします。[詳細ルール]ペインに次のパラメータが表示されます。



> [名前] – ルールの名前。

> [プログラム] – プログラムとパスの名前。

> [アクション] – 指定されたアプリケーション、ポート、またはプロトコルからの通信に対して、ファイアウォールが取るアクション ([許可]、[ブロック])。

> [方向] – 通信の方向 ([双方向]、[受信]、[送信])。

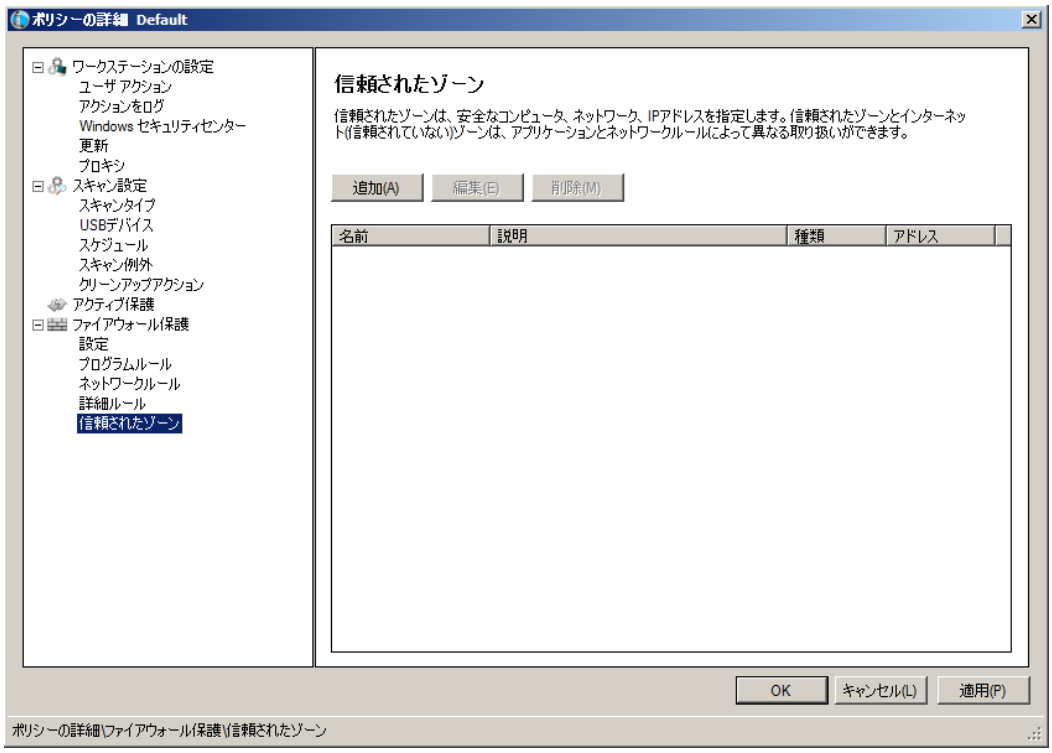
> [プロトコルタイプ] – プロトコルのタイプ（ICMP、IGMP、TCP、UDP）と名前。

> [ローカルポート] – ローカルポートの詳細。

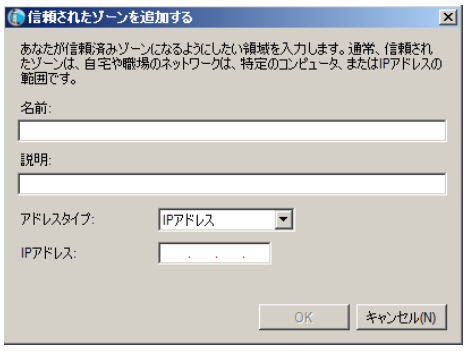
> [リモートポート] – リモートポートの詳細。

- [信頼されたゾーン] ペイン

  信頼されたゾーンは、信頼されたコンピュータ、ネットワーク、IPアドレスを指定します。信頼されたゾーンとインターネット(信頼されていない)ゾーンは、プログラムとネットワークルールによって異なる取り扱いができます。



[追加]をクリックして、新しい信頼されたゾーンを追加します。オプションを指定または選択し、[OK]をクリックします。次のパラメータが表示されます。



> [名前] – 信頼されたゾーンの名前。

> [説明] – 信頼されたゾーンの説明。

> [タイプ] – 信頼されたゾーンのタイプ ([IP アドレス]、[ネットワーク])。

10. [OK] をクリックします。新しいポリシーである「新規ポリシー 1 」が [Anti-Virus] ノードの下に表示されます。

Anti-Virus ポリシーの適用

Anti-Virus ポリシーが作成されたら、Faronics Core Console から 1 台以上のワークステーションに適用することができます。ポリシーを適用するには、次の手順を実行します。

1. 1 台以上のワークステーションを選択します。右クリックをして [ポリシーの再割り当て] を選択します。
2. [ワークステーションのポリシーへの再割り当て] ダイアログが表示されます。[ポリシーの割り当て] ドロップダウンからポリシーを選択し、[OK] をクリックします。
3. 選択したワークステーションにポリシーが適用されます。

Anti-Virus ポリシーの表示または変更

作成した Anti-Virus ポリシーは表示したり、変更することができます。ポリシーを表示または変更するには、次の手順を実行します。

1. Faronics Core Console を起動します。
2. コンソールツリーペインで、[Faronics Core Console] > [コアサーバー] > [マネージドワークステーション] > [Anti-Virus] > [ポリシー名] の順に選択します。
3. ポリシーを右クリックし、[ポリシーの詳細] を選択します。
4. ポリシーを編集するには、Faronics Anti-Virus ポリシーの作成の説明に従い、タブ内で設定を変更します。
5. [OK] をクリックして、変更を適用します。
6. ポリシーに加えた変更は、そのポリシーが管理するワークステーションに自動的に適用されます。

Anti-Virus ポリシーの名前変更

Anti-Virus ポリシーは、作成した後に名前を変更することができます。ポリシーの名前を変更するには、次の手順を実行します。

1. Faronics Core Console を起動します。
2. コンソールツリーペインで、[Faronics Core Console] > [コアサーバー] > [マネージドワークステーション] > [Anti-Virus] > [ポリシー名] の順に選択します。
3. ポリシーを右クリックし、[ポリシーの名前変更] を選択します。[ポリシーの名前変更] ダイアログが表示されます。
4. [新しいポリシー名] を入力し、[OK] をクリックします。

ポリシーのコピー

既存のポリシーは新しいポリシーに簡単にコピーできます。既存ポリシーのデータを別の既存ポリシーにコピーすることも可能です。

ポリシーをコピーするには、次の手順を実行します。

1. Faronics Core Console を起動します。
2. コンソールツリーペインで、[Faronics Core Console] > [コアサーバー] > [マネージドワークステーション] > [Anti-Virus] > [ポリシー名] の順に選択します。
3. ポリシーを右クリックし、[ポリシーのコピー] を選択します。[ポリシーのコピー] ダイアログが表示されます。
4. ドロップダウンから [コピー先ポリシー] を選択するか、[新規] をクリックして新しいポリシーにデータをコピーします。新しいポリシーの名前を指定します。
5. [今すぐポリシー データをコピー] をクリックします。

既存ポリシーにデータがコピーされるか、手順 3 で選択した既存ポリシーのデータから新しいポリシーが作成されます。

Anti-Virus ポリシーの削除

既存ポリシーを削除するには、次の手順を実行します。

1. Faronics Core Console を起動します。
2. コンソールツリーペインで、[Faronics Core Console] > [コアサーバー] > [マネージドワークステーション] > [Anti-Virus] > [ポリシー名] の順に選択します。
3. ポリシーを右クリックし、[ポリシーの削除] を選択します。[ポリシーの削除] ダイアログが表示されます。
4. [はい] を選択してポリシーを削除します。

ワークステーションに割り当てられているポリシーを削除した場合、デフォルトポリシーに置き換えられます。デフォルトポリシーを削除することはできません。

Anti-Virus ポリシーのインポート

あらかじめ設定された Anti-Virus ポリシーは、既存のポリシーにインポートできます。この機能を使うと、ポリシー全体を再設定する必要がないため、時間が節約できます。

既存のポリシーをインポートするには、次の手順を実行します。

1. Faronics Core Console を起動します。
2. コンソールツリーペインで、[Faronics Core Console] > [コアサーバー] > [マネージドワークステーション] > [Anti-Virus] > [ポリシー名] の順に選択します。
3. ポリシーを右クリックし、[ポリシーのインポート] を選択します。既存のポリシーの現在の設定を上書きするには、[はい] をクリックします。
4. 参照して、インポートするポリシーを選択します。XML 形式でエクスポートされているポリシーのみをインポートできます。
5. エクスポート済みのポリシーを選択して、[開く] をクリックします。ポリシーがインポートされます。

Anti-Virus ポリシーのエクスポート

あらかじめ設定された Anti-Virus をエクスポートして、再利用できます。この機能を使うと、ポリシー全体を再設定する必要がないため、時間が節約できます。

既存のポリシーをエクスポートするには、次の手順を実行します。

1. Faronics Core Console を起動します。
2. コンソールツリーペインで、[Faronics Core Console] > [コアサーバー] > [マネージドワークステーション] > [Anti-Virus] > [ポリシー名] の順に選択します。
3. ポリシーを右クリックし、[ポリシーのエクスポート] を選択します。
4. [参照] をクリックして、場所を選択します。
5. [ファイル名] を指定して、[保存] をクリックします。ポリシーが XML 形式でエクスポートされます。

Faronics Core Console によるスキャン

スキャンは、Anti-Virus ポリシーでスケジュール設定することによって、または Faronics Core Console からタスクをスケジュール設定することによって、手動で実行できます。Faronics Core Console からワークステーションを手動でスキャンするには、以下の手順を実行します。

1. Faronics Core Console を起動します。
2. [ワークステーションのリスト] ペインに移動します。
3. 1 つ以上のワークステーションを右クリックして、[スキャン] を選択します。
   > クイック スキャンを実行するには、[スキャン] > [クイック] の順に選択します。
   > ディープ スキャンを実行するには、[スキャン] > [ディープ] の順に選択します。
   > 最新のウィルス定義をダウンロードして、スキャンを実行するには、[今すぐ修正] を選択します。[アクティブ保護] がユーザによって一時的に無効にされている場合は、[今すぐ修正] を選択すると有効になります。

スキャンの進行度 [スキャン進行度 – %] が、Faronics Core Console の [ワークステーションのリスト] ペインに表示されます。

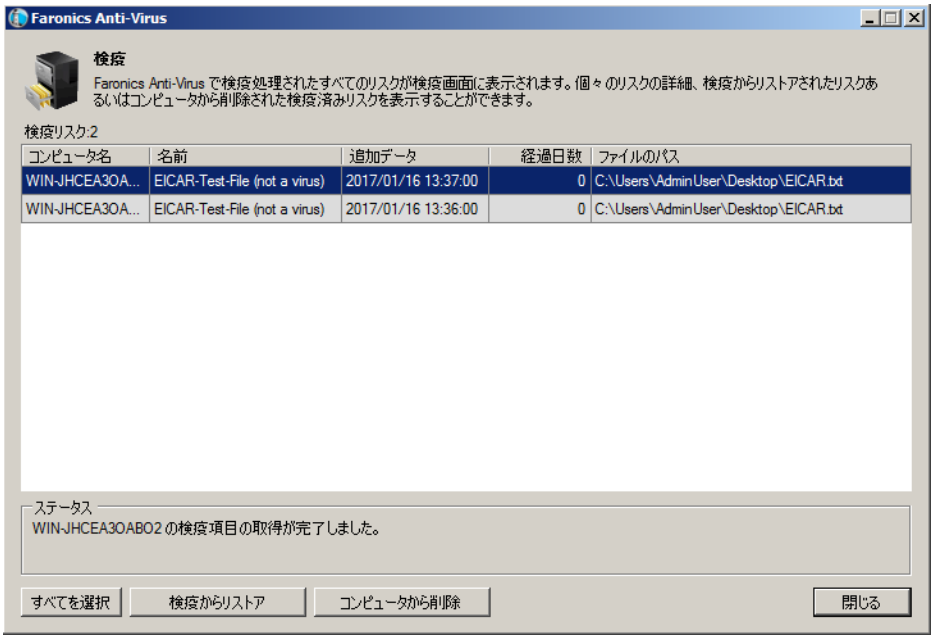
複数の Loadin がインストールされている場合、ワークステーションを右クリックして [Faronics Anti-Virus] を選択し、特定の操作を選択することによって、Faronics Anti-Virus のコンテキスト メニューを使用することができます。

[今すぐ修正] 機能が Faronics Core Console から動作するためには、[アクティブ保護] が有効になっている必要があります。

隔離されたファイルの表示と操作

Faronics Anti-Virus によって検疫されたファイルを表示するには、以下の手順を実行します。

1. Faronics Core Console を起動します。
2. [ワークステーションリスト] ペインを開きます。
3. ワークステーションを選択します。
4. ワークステーションを右クリックして、[検疫を表示] を選択します。検疫されたファイルのリストが表示されます。



5. 感染した各ファイルに関して、以下の情報が表示されます。
   - > リスク名
   - > ファイル名 :
   - > 元のロケーション
   - > 追加データ
   - > 経過日数
6. 以下のオプションを選択します。
   - > 詳細 – 感染ファイルの詳細を表示するには、ファイルを選択して、[詳細] をクリックします。これにより推奨される対処方法も表示されます。
   - > すべて選択 – すべてのファイルを選択できます。
   - > コンピュータから削除 – コンピュータから選択したファイルを削除できます。
   - > 検疫からリストア – コンピュータから選択したファイルを復元できます。
   - > [閉じる] – ダイアログを閉じます。

Faronics Core Console による Faronics Anti-Virus の更新

Faronics Anti-Virus のウイルス定義は、Faronics Core Console を介して、ワークステーション上で更新できます。Faronics Core は、マネージド ワークステーションの Anti-Virus 更新レポジトリの役割を果たします。Anti-Virus の更新は、Faronics Core によって、リモート ワークステーションに自動的に送信されます。また、Faronics Core の管理者は、以下に示すように、ウイルス定義を手動で更新することができます。

Faronics Anti-Virus をワークステーションで更新するには、次の手順を実行します。

1. Faronics Core Console を起動します。
2. [*ワークステーションのリスト*] ペインに移動します。
3. 1 つ以上のワークステーションを右クリックして、[更新] を選択します。
   > [更新] > [差分更新] の順に選択します。これで、Anti-Virus 定義が更新されます。
   > [更新] > [完全更新] の順に選択します。この場合、既存の Anti-Virus 定義が削除され、最新の定義に更新されます。

Faronics Core Console による Faronics Anti-Virus のスケジュール設定

Faronics Anti-Virus と Faronics Core Console は、管理者にとって都合が良い日付および時刻に、1 つ以上のワークステーションでイベントが実行されるようにスケジュール設定することができます。1 つ以上のワークステーションをクリックし、[アクションのスケジュール設定] を選択します。表示されるサブメニューには、以下のような利用可能なアクションリストが含まれます。

Faronics Core Console で管理できるアクション

- シャットダウン
- 再起動
- ウェイク アップ

Faronics Anti-Virus で管理できるアクション

- アクティブ保護 > 有効化
- アクティブ保護 > 無効化
- スキャン > クイック
- スキャン > ディープ
- 更新 > 完全更新
- 更新 > 強制的に完全更新を行う
- 今すぐ修正
- Anti-Virus クライアントのインストール / アップグレード
- Anti-Virus クライアントのアンインストール

アクションを選択すると、[スケジュール] メニューが表示され、管理者は頻度 [1 回限り、毎日、毎週、毎月のいずれか] を指定することができます。頻度に基づいて、特定の時間、曜日、日付、月を選択することができます。

Anti-Virus ポリシーによるタスク スケジュール設定は、Faronics Core Console によるアクション スケジュール設定よりも、常に優先されます。

レポートの生成

Faronics Anti-Virus は、各ワークステーションでの活動を監視するレポートを多数提供します。レポートには、次の 2 つのカテゴリが存在します。

- グローバル レポート – これは、Faronics Anti-Virus によって保護されているすべてのワークステーションに関するレポートです。
- ワークステーション固有のレポート – これは、選択したワークステーション専用のレポートです。

グローバル レポート

グローバル レポートを生成するには、次の手順を実行します。

1. Faronics Core Console を起動します。
2. [コンソール ツリー] ペインで、[Faronics Core Console] > [(Core Server)] > [マネージド ワークステーション] > [Anti-Virus] の順に選択します。
3. [アクション] ペインで、[グローバル レポート] をクリックします。
4. レポートを選択し、表示されたダイアログに日付範囲を入力します。[OK] をクリックします。次のレポートが利用可能です。
   > 検出数別の脅威 – Faronics Anti-Virus によって管理されているすべてのワークステーションで検出された脅威が、検出数別に表示されます。
   > 脅威の重大性のサマリー – 脅威の重大性に関するサマリーが表示されます。
   > 感染数の多い上位 25 のマシン – 感染数の多い上位 25 のコンピュータが表示されます。
5. 選択したレポートは、[コンソール ツリー] ペイン > [レポート] ノードに表示されます。

ワークステーション固有のレポート

ワークステーション固有のレポートを生成するには、次の手順を実行します。

1. Faronics Core Console を起動します。
2. [コンソール ツリー] ペインで、[Faronics Core Console] > [(Core Server)] > [マネージド ワークステーション] の順に選択します。
3. レポートを生成するワークステーションを選択します。
4. ワークステーションを右クリックして、[レポート] を選択します。
5. レポートを選択し、表示されたダイアログに日付範囲を入力します。[OK] をクリックします。次のレポートが利用可能です。
   > ワークステーション詳細
   > 最新スキャン
   > スキャン履歴
   > アクティブ保護履歴
   > 隔離場所
   > 電子メール保護履歴
   > システム イベント メッセージ
6. 選択したレポートは、[コンソール ツリー] ペイン > [レポート] ノードに表示されます。

ワークステーションでの Faronics Anti-Virus の使用

ワークステーションで利用可能な Faronics Anti-Virus の機能は、Anti-Virus ポリシーで選択した設定に、完全に依存します。Anti-Virus ポリシーの詳細については、「Faronics Anti-Virus ポリシー」を参照してください。

Faronics Anti-Virus のワークステーションでの起動

[スタート] > [プログラム] > [Faronics] > [Anti-Virus Enterprise] > [Faronics Anti-Virus Enterprise] の順に選択します。または、システム トレイの Faronics Anti-Virus アイコンをダブルクリックします。

次の各ペインに、重要な情報が表示されます。

- [保護されています] または [保護されていません] – コンピュータが保護されている、または保護されていないことを通知するために表示されます。[保護されていません] が表示されている場合、その下にある [今すぐ修正] ボタンをクリックします。
- [スキャン ステータス] – 最後にスキャンが実行された日時が表示されます。直ちにスキャンするには、[今すぐスキャン] リンクをクリックします。
- [更新ステータス] – 最後に更新が実行された日時が表示されます。ウイルス定義を更新するには、[すべてを今すぐ更新] リンクをクリックします。
- [アクティブ保護] – リアルタイム保護が有効化されているかどうかが表示されます。
- [ファイアウォール保護] - ワークステーションがファイアウォールで保護されているかどうかが表示されます。
- [リスク検出統計] – Faronics Anti-Virus が取ったアクションの統計値が表示されます。数値をゼロにリセットするには、[数のリセット] をクリックします。

ワークステーションのスキャン

ワークステーションをスキャンするには、次の手順を実行します。

1. [スタート] > [プログラム] > [Faronics] > [Anti-Virus Enterprise] > [Faronics Anti-Virus Enterprise] の順に選択します。または、システム トレイの Faronics Anti-Virus アイコンをダブルクリックします。

2. [スキャン ステータス] ペインの [今すぐスキャン] をクリックします。[スキャン] タブが表示されます。または、[スキャン] タブをクリックします。

3. 次の中からオプションを選択してください。
   > [クイック スキャン] – 既知の脅威のみをスキャンします。
   > [ディープ システム スキャン] – ワークステーションのすべてのファイルを詳細にスキャンします。
   > [カスタム スキャン] [次のいずれかひとつを選択します]。
      ~ [実行中のプロセスをスキャンする] – ワークステーションで実行中のプロセスをスキャンします。
      ~ [レジストリをスキャンする] – レジストリをスキャンします。
      ~ [クッキーをスキャンする] – ワークステーションに保存されているクッキーをスキャンします。
      ~ [スキャンするドライブおよびフォルダを指定する] – [参照] をクリックして、フォルダを選択します。
4. [今すぐスキャン] をクリックします。回転しているアイコンは、スキャンが進行中であることを示します。スキャンの結果は、スキャン完了後に表示されます。
5. ファイルを選択します。次のオプションが利用できます。
   > Faronics Anti-Virus によって推奨される動作を設定するには、[駆除アクションの変更] > [推奨されるアクション] の順に選択します。
   > 選択したファイルを隔離または駆除するには、[駆除アクションの変更] > [隔離 / 駆除] の順に選択します。
   > 選択したファイルを削除するには、[駆除アクションの変更] > [削除] の順に選択します。
   > 選択したファイルを許容するには、[駆除アクションの変更] > [許容] の順に選択します。
   > [スキャンの結果] に表示されたすべてのファイルを選択するには、[すべて選択] をクリックします。
   > リスクの詳細を表示するには、[詳細] をクリックします。
   > 何もしないでダイアログを閉じるには、[キャンセル] をクリックします。
   > ファイルを削除し、ダイアログを閉じるには、[駆除] をクリックします。

上記の操作は、Faronics Core Console からも実行できます。詳細は、「隔離されたファイルの表示と操作」を参照してください。

右クリックによるファイルまたはフォルダのスキャン

[1 つまたは複数の] ファイルまたはフォルダを、簡単にウイルス スキャンすることができます。Faronics Anti-Virus がワークステーションにインストールされた時点で、[ウイルス スキャン] オプションが右クリック メニューに追加されます。

コンピュータ上のファイルまたはフォルダをスキャンするには、次の手順を実行します。

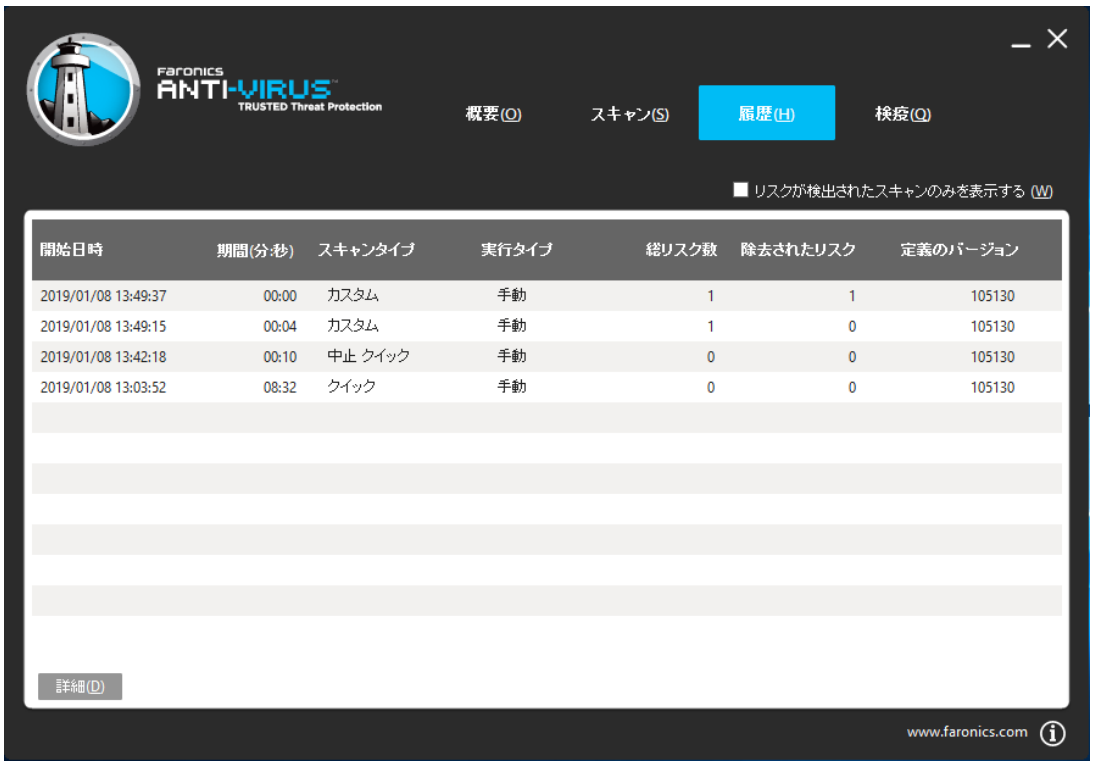
1. ファイルまたはフォルダを右クリックします。
2. [ウイルス スキャン] を選択します。

スキャンが実行され、結果が表示されます。

スキャン履歴の表示

スキャン履歴を表示するには、以下の手順を実行します。

1. [スタート] > [プログラム] > [Faronics] > [Anti-Virus Enterprise] > [Faronics Anti-Virus Enterprise] の順に選択します。または、システムトレイの Faronics Anti-Virus アイコンをクリックすることもできます。
2. [履歴] タブをクリックします。

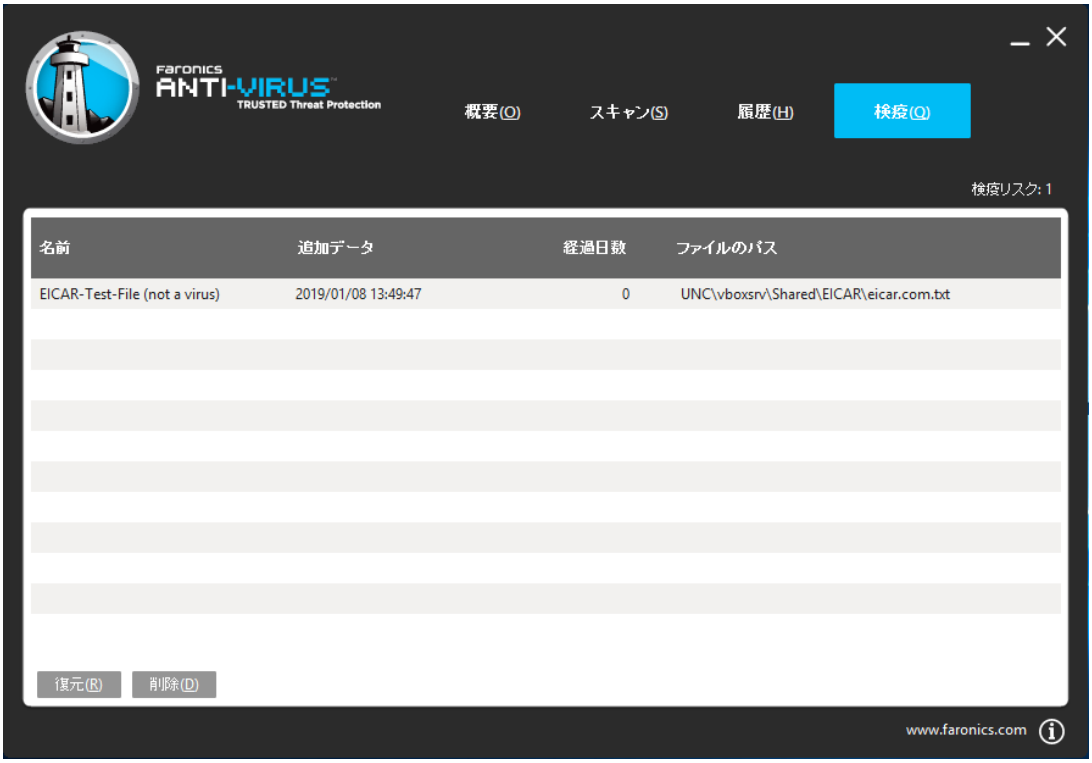


3. 以下のオプションを選択します。
   > リスクが検出されたスキャンのみを表示する – リスクが検出されたスキャンのみを表示するには、このオプションを選択します。
   > 詳細 – スキャンの詳細を表示するには、エントリを選択して、[詳細] を選択します。

検疫済みのファイルの表示と操作

検疫を表示するには、以下の手順を実行します。

1. [スタート] > [プログラム] > [Faronics] > [Anti-Virus Enterprise] > [Faronics Anti-Virus Enterprise] の順に選択します。または、システムトレイの Faronics Anti-Virus アイコンをクリックすることもできます。
2. [検疫] タブをクリックします。



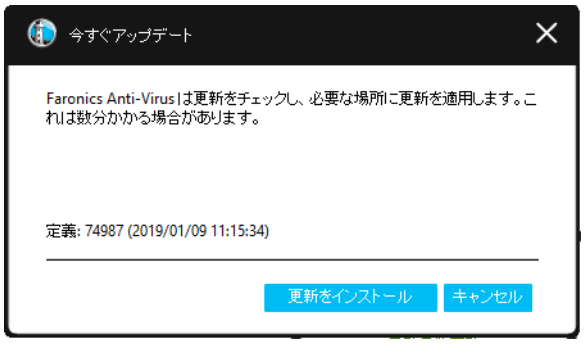
3. [リスクの詳細] をクリックします。感染した各ファイルに関して、以下の情報が表示されます。
   - 名前
   - リスクのカテゴリ
   - 追加データ
   - 経過日数
   - 検疫実行

ワークステーションでの Anti-Virus 定義の更新

Anti-Virus の定義をワークステーションで更新するには、次の手順を実行します。

1. [スタート] > [プログラム] > [Faronics] > [Anti-Virus Enterprise] > [Faronics Anti-Virus Enterprise] の順に選択します。または、システム トレイの Faronics Anti-Virus アイコンをダブルクリックします。

2. [更新ステータス] ペインの [今すぐ更新] をクリックします。[今すぐ更新] ダイアログが表示されます。



3. [更新のインストール] をクリックします。ワークステーションのウイルス定義が更新されます。

ワークステーションでのシステム トレイによる Faronics Anti-Virus の管理

Faronics Anti-Virus は、システム トレイで利用可能なメニューによって、ワークステーションで管理することができます。

システム トレイの Faronics Anti-Virus アイコンを右クリックします。以下のオプションがあ
ります。

- Faronics Anti-Virus を開く – Faronics Anti-Virus をワークステーション上で起動します。
- アクティブ保護
  - > [アクティブ保護] > [アクティブ保護の有効化] – アクティブ保護を有効化します。
  - > [アクティブ保護] > [アクティブ保護の無効化] > [オプションの選択] – アクティブ保護を無効化する時間 [期間] を選択します。5 分、15 分、30 分、1 時間、コンピュータが再起動するまで、永久、のいずれかを選択します。このオプションは、Anti-Virus ポリシーで選択されている場合にのみ表示されます。
- [今すぐスキャン] > [オプションの選択] – [スキャンのキャンセル]、[スキャンの一時停止]、[スキャンの再開]、[クイック スキャン]、[ディープ スキャン] のいずれかを選択します。このオプションは、Anti-Virus ポリシーで選択されている場合にのみ表示されます。
- [ファイアウォール保護]> 有効化または無効化。

上記のオプションは、Anti-Virus ポリシーで指定されている場合にのみ利用できます。詳細は、「Faronics Anti-Virus ポリシーの作成」を参照してください。

コマンドラインコントロール

この章では、Faronics Anti-Virus で利用可能なさまざまなコマンド ライン コントロールについて説明します。

トピック

コマンドラインコントロール

コマンドラインコントロール

Faronics Anti-Virus コマンド ライン コントロールにより、他社製の管理ツールおよび中央管理ソリューションによる制御が可能になり、ネットワーク管理者は Faronics Anti-Virus ワークステーションの管理をより自在に行うことができます。

Faronics Anti-Virus のコマンドを実行するには、以下の手順を実行します。

1. ワークステーションで、コマンド プロンプトから < システム ディレクトリ >:\Program Files\Faronics\Faronics Anti-Virus Enterprise に移動します。
2. AVECLI/[Command]、と入力します。

次のコマンドがあります。

コマンド	定義
definitionversion	ウイルス定義のバージョンを表示します。
scanengineversion	スキャン エンジンのバージョンを表示します。
updatedefs	更新を実行し、ウイルス定義を適用します。
scanquick	クイック スキャンを起動します。
scandeep	ディープ スキャンを起動します。
fixnow	最新のウィルス定義をダウンロードします。アクティブ保護と電子メール保護を有効にします。デフォルトのディープスキャンを実行します。
setlicense[key]	ライセンスキーを適用します。
enableap	アクティブ保護を有効にします。
fixnow /quick	該当する場合は、クイックスキャンを実行します。

構文：

AVECLI/definitionversion

Faronics Anti-Virus のアンインストール

この章では、Faronics Anti-Virus のアンインストール方法を説明します。

トピック

アンインストールの概要
Faronics Core Console による Faronics Anti-Virus Client の アンインストール
ワークステーションでの [プログラムの追加と削除] による Faronics Anti-Virus Client のアンインストール
インストーラによる Faronics Anti-Virus Loadin のアンインストール
[プログラムの追加と削除] による Faronics Anti-Virus Loadin のアンインストール

アンインストールの概要

Faronics Anti-Virus Loadin は、Faronics Core Console [または Faronics Core Server] システムにインストールされています。Faronics Anti-Virus Client は、ワークステーションにインストールされています。

まず、ワークステーションの Faronics Anti-Virus Client を手動で、または Faronics Core Console からアンインストールします。次に、Faronics Anti-Virus Loadin を、Faronics Core Console [または Faronics Core Server] システムからアンインストールします。

アンインストールの具体的な手順については、次のセクションで説明します。

Faronics Core Console による Faronics Anti-Virus Client のアンインストール

Faronics Core Console から Faronics Anti-Virus Client をアンインストールするには、次の手順を実行します。

1. Faronics Core Console を起動します。
2. [コンソール ツリー] ペインで、[Faronics Core Console] > [(Core Server)] > [マネージド ワークステーション] の順に選択します。
3. Faronics Anti-Virus Client をアンインストールするワークステーションを選択します。
4. 右クリックして、[ワークステーションの構成] > [詳細] > [Anti-Virus Client のアンインストール] の順に選択します。

Faronics Anti-Virus Client が、各ワークステーションからアンインストールされます。

ワークステーションでの [プログラムの追加と削除] による Faronics Anti-Virus Client のアンインストール

Windows の [プログラムの追加と削除] を利用して Faronics Anti-Virus をアンインストールするには、次の手順を実行します。

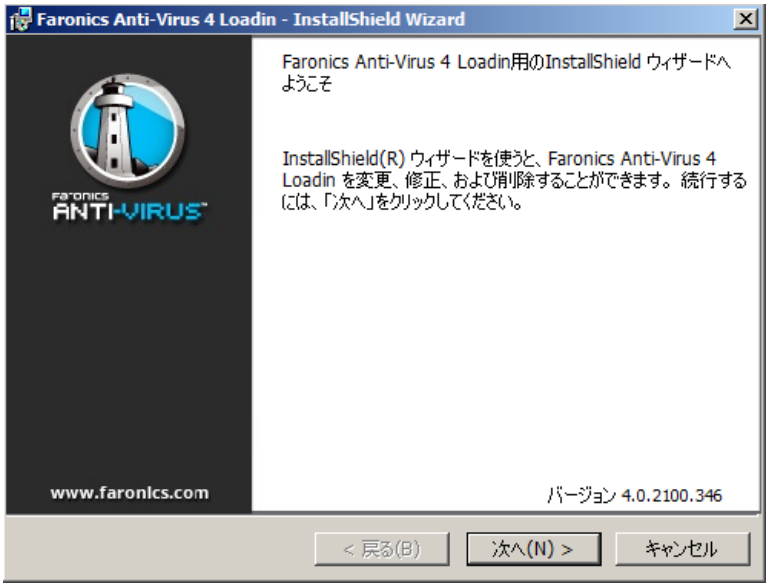
1. [スタート] > [コントロール パネル] > [プログラムの追加と削除] の順にクリックします。
2. [Faronics Anti-Virus Enterprise Workstation] を選択します。
3. [削除] をクリックします。

Faronics Anti-Virus Client が、ワークステーションからアンインストールされます。

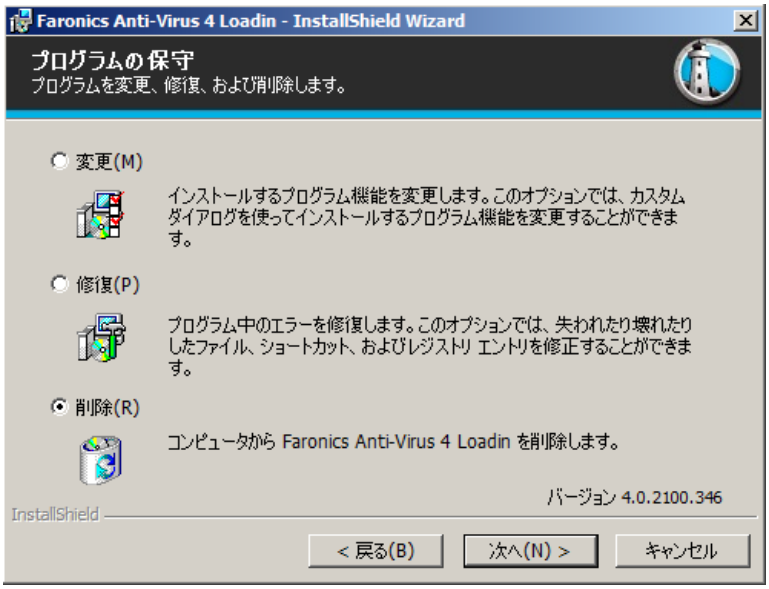
インストーラによる Faronics Anti-Virus Loadin のアンインストール

Faronics Anti-Virus Loadin をアンインストールするには、次の手順を実行します。

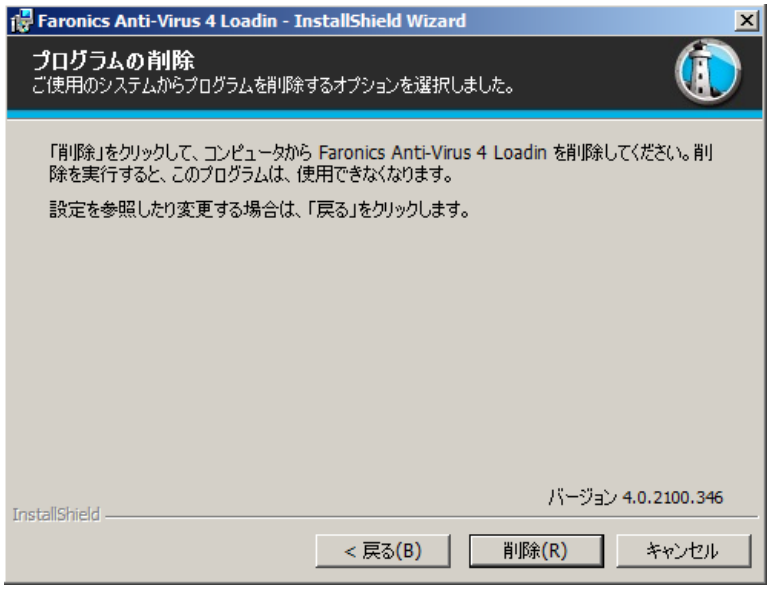
1. Anti-VirusLoadinInstaller.exe をダブルクリックします。[次へ] をクリックします。



2. [削除] を選択します。[次へ] をクリックします。

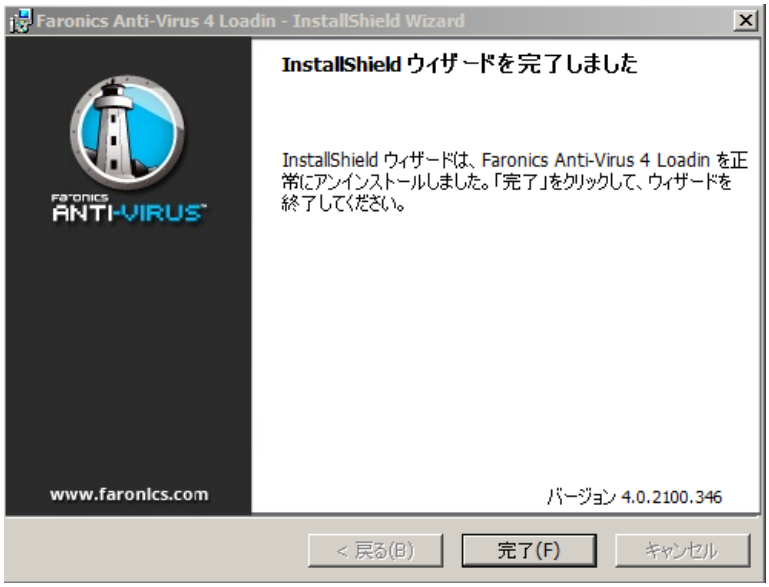


3. [削除] をクリックします。



4. 次のメッセージが表示されます。Faronics Core Server サービスをすぐに再起動する場合は [はい] を、後から手動で再起動する場合は [いいえ] をクリックします。

5. Faronics Anti-Virus Loadin が、コンピュータから削除されます。[完了] をクリックして、アンインストールを終了します。



[プログラムの追加と削除] による Faronics Anti-Virus Loadin のアンインストール

Windows の [プログラムの追加と削除] を利用して Faronics Anti-Virus Loadin をアンインストールするには、次の手順を実行します。

1. [スタート] > [コントロール パネル] > [プログラムの追加と削除] の順にクリックします。
2. [Faronics Anti-Virus Loadin] を選択します。
3. [削除] をクリックします。