



# Faronics ANTI-VIRUS

# **ADVANCED** System Integrity



www.faronics.com



最新更新日:1月2023

© 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
重要な情報6
Faronicsについて
製品マニュアル
テクニカル サポート
お問い合わせ
用語の定義8
はじめに
Faronics Anti-Virus の概要
システム要件
Faronics Anti-Virus の要件
Faronics Coreの要件
Deep Freeze の要件
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
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
ワークステーションでの Faronics Anti-Virus の手動インストール
Faronics Anti-Virus の使用
Faronics Anti-Virus の概要
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
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
Faronics Anti-Virusポリシーの作成28
Anti-Virusポリシーの適用
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
Anti-Virusポリシーの削除
Anti-Virusポリシーのインポート
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



Faronics Core Console による Faronics Anti-Virus の更新	52 53 54 54 54
「ケークステーションでのFaronics Anti-Virus の使用5 Faronics Anti-Virus のワークステーションでの起動5	55 55
ワークステーションのスキャン5	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5	58
検疫済みのファイルの表示と操作5	59
ワークステーションでの Anti-Virus 定義の更新6	50
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6	51
<b>コマンドラインコントロール</b>	<b>53</b>
Faronics Anti-Virus のアンインストール	<b>5</b> 5
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	57
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	38
インストーラによる Faronics Anti-Virus Loadin のアンインストール	39
[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  $[\exists - \Box \forall \gamma \uparrow]$ 8 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom



# 用語の定義

田田田	
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。

**10** 序文





# 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。
- [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。

🚏 Faronics Anti-Virus 4 Loadin - InstallShield Wizard	×
使用許諾契約 次の使用注語契約書を注意深くお読みください。	
Faronics Anti-Virus Enterprise - ライセンス	<b>_</b>
Faronics Corporation Copyright 2004 – 2017 All Rights Reserved	
マスター ソフトウェア ライセンス契約	
ライセンスの許諾: Faronicsは本契约の祭項に基づいて、上記の「ライセンス数」の 数のコンピュータまたは教室で本製品をインストール、使用、アクセス、表示、実行 する似下総称して、「使用」別定的かつ非独占なライセンスをライセンシーに許諾	D項で規定された f、またはやり取り fします。いかなる 💌
<ul> <li>         ・         ・         ・</li></ul>	EU胎(b)
バージ:	a) 4.0.2100.342
< 戻る(B)	キャンセル



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。

🙀 Faronics Anti-Viru	s 4 Loadin - InstallShield Wizard	×
お客様情報 お客様の情報を入力し	してください。	
ユーザ名( <u>U</u> ):	AdminUser	
所属(0).	Faronics corporation	
77144 <u>(0</u> 7)	<u> </u>	
ライセンスキー:		
	□ 評価版を使用 (30日間)(E)	
TestallChield	バージョン 4.0.2	100.342
มารนสเอากอเนิ	< 戻る(B) 次へ(N) > キ	ャンセル

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。

<b>得 Faronics</b> インスト このフォル!	i Anti-Virus 4 Loadin - InstallShield Wizard  マル先のフォルダ がにインストールする場合は、「次へ」をクリックしてください。
Þ	Faronics Anti-Virus 4 Loadin のインストール先: C:\Program Files (x86)\Faronics\Faronics Core 3\Loadins\Anti-Virus 4\
InstallShield	バージョン 4.0.2100.342 < 戻る(B) / 次へ(N) > キャンセル

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。

🚏 Faronics Anti-Virus 4 Loadin - InstallShield Wizard 🔀
<b>プログラムをインストールする準備ができました</b> ウィザードは、インストールを開始する準備ができました。
「インストール」をクリックして、インストールを開始してください。
インストールの設定を参照したり変更する場合は、「戻る」をクリックしてください。「キャンセル」をク リックすると、ウィザードを終了します。
バージョン 4.0.2100.342 InstallShield
< 戻る(B) インストール(I) キャンセル



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 Anti-Virus 4 Loa	din - InstallShield Wizard
Paronics Anti-Virus 4 Load	InstallShield ウィザードを完了しました InstallShield ウィザードは、Faronics Anti-Virus 4 Loadin を正常にインストールしました。「完了」をクリックして、ウィザードを終了してください。
www.faronics.com	バージョン 4.0.2100.342 < 戻る(B) <b>完了(F)</b> キャンセル



# 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

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。

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。

😸 Faronics Anti-Virus - InstallShield Wiz	ard		×
License Agreement			
Please read the following license agreem	ent carefully.		
Faronics Anti-Virus - License			<b>^</b>
Faronics Corporation Copyright 2004 - 2017 All Rights F	Reserved		
Master Software License Agreem	ient		
LICENSE GRANT: Faronics hereby grants use, access, display, run, or otherwise into number of computers or classrooms set ou	Licensee a limited, non eract with (collectively, it across from the head	-exclusive licen , "Use") the Pro ding 'Number of	se to install, ducts on the Licenses' <del>•</del>
<ul> <li>I accept the terms in the license agreement</li> </ul>	ent		Print
$\bigcirc$ I do not accept the terms in the license a	greement		
InstallShield	< Back	Version: Next >	4.0.2102.342



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。

📸 Faronics Anti-Virus - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back Sack Cancel
完了」をクリックして、インストールを終了しま
B Faronics Anti-Virus - InstallShield Wizard
InstallShield Wizard Completed





4.

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。
- [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。
- [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。

④ Faronics Anti-Virus - 設定	×
更新 プロキシ サーバー	_,
ウイルス定義のバージョン ――――	
Anti-Virus (32ピット): 95289 (2017/01/06 10:27:24)	
Anti-Virus (64ビット): 65200 (2017/01/09 15:47:48)	
設定を更新	
▶ 自動更新の保管先: 2 時間	
更新の設定をチェック	
更新チェック最新日時: 2017/01/09 16:00:37 今すぐ更新	
次回更新チェックの日時: 2017/01/09 18:00:37	
更新ステータス: 正常にダウンロード更新。	
  OKキャンセル	,
設定\更新	

- > [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。

() Faronics Anti-Virus - 設定	×
更新 プロキシサーバー	
🔲 プロキシ サーバーを使用して Updates Web Server に接続します	
プロキシ サーバー情報 ――――	
<u> </u> ምドレス: ポート:	
ユーザ認証	
□ プロキシサーバー(は認可くログオン/信任状)が必要です	
認証の種類: Basic V	
ユーザ名:	
パスワード:	
КУ47):	
テスト	
OK ++>t/	
設定 プロキシ サーバー	

- 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。
- [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。
- [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。

🌘 新規ポリシー		X
ポリシー名:	Γ	
		0K ++>1211

- 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1	ペイ	ン
	/ / / -	· 」		-

🚺 ポリシーの詳細 Default			×
<ul> <li>□ ● ワークステーションの設定</li> <li>□ ● ワークステーションの設定</li> <li>アクションを口グ</li> <li>アクションを口グ</li> <li>アクションを口グ</li> <li>アクキシ</li> <li>マ スキャン長定</li> <li>スキャン長定</li> <li>スキャン長定</li> <li>スキャン人プ</li> <li>US6デバイス</li> <li>スケジュール</li> <li>スキャン例外</li> <li>クリーンアジアクション</li> <li>アクティブ保護</li> <li>ロ= アイアウォール(保護</li> <li>設定</li> <li>プログラムルール</li> <li>ネットワークルール</li> <li>詳細ルール</li> <li>信頼されたゾーン</li> </ul>	<ul> <li>ユーザ アクション</li> <li>Øスカバーアイコンを表示</li> <li>☑ 手動スキャンを許可</li> <li>☑ ユーザによるスキャン結果に対する処置を許可</li> <li>☑ ユーザによるスキャンの取り消しを許可</li> </ul>		
	N_N.	OK キャンセル(L) 適用(P)	

- > [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 @ポリシーの詳細 Default	ン		x
<ul> <li>□ ● ワークステーションの設定</li> <li>ユーザ アクション</li> <li>アンコンをロジ</li> <li>Windows セキュリティセンター 更新 プロキシ</li> <li>□ ● スキャン設定 スキャンタイプ</li> <li>USBデドイス スケジュール</li> <li>スキャン/例外 クリーンアップアクション</li> <li>アクティブ(保護</li> <li>□ ■ ファイアウォール(保護</li> <li>副定定 プログラムルール</li> <li>ネットワークルール</li> <li>詳細ルール</li> <li>信頼されたゾーン</li> </ul>	<b>アクションをログ</b> ロギングレベル: なし ④ ログ ファイルを上向きスクロール 10 MB. 40 MB 合計ディスクスペース		
ポリシーの詳細(ワークステーションの設定、アクションを(	<u>ок</u>	<b>キャンセル(L)</b> 道用(P)	

- > [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

🚯 ボリシーの詳細 Default		×
<ul> <li>□ ● ワークステーションの設定 ユーザアクション アクションをログ</li> <li>● ジョンをログ</li> <li>● 夏新 プロキシ</li> <li>□ ● スキャン感定 スキャン感定</li> <li>□ ● スキャン感定</li> <li>□ ● スキャン感定</li> <li>□ ● スキャンのイブ</li> <li>□ SBデバイス</li> <li>スケジュール</li> <li>スキャンタイブ</li> <li>□ ● ファイアウォール(保護</li> <li>■ 設定</li> <li>□ プログラムルール</li> <li>ネットワークルール</li> <li>■ 詳細ルール</li> <li>(言頼されたゾーン</li> </ul>	Windows セキュリティセンターに統合  Windows セキュリティセンターに統合	
ポリシーの詳細\ワークステーションの設定\Windows t	レベ キャンセルに 迎用(?) ビキュリティセンター	 .::

 > [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。 •



<ul> <li>□ ● クークステーションの設定 ユーザアクションをログ アクションをログ Windows セキュリティセンター 更新 プロキシ</li> <li>□ ● スキャン設定 スキャンタイプ USBデバイス スケジュール スキャン/例外 クリーンアップアクション</li> <li>● アクティブ(保護 設定 プログラムルール 素ットワークルール 詳細ルール (言頼されたゾーン</li> </ul>	史がには、「「「」」」」」では、「「」」」」」では、「「」」」」」     「「」」」」     「「」」」     「「」」」     「「」」」     「「」     「「」     「「」」     「「」     「「」     「「」     「「」     「「」     「「」     「「」     「「」     「「」     「」     「「」     「「」     「「」     「「」     「「」     「「」     「「」     「「」     「「」     「「」     「「」     「「」     「「」     「「」     「「」     「「」      「」      「「」      「「」      「      「」      「      「      「      「」      「      「      「」      「      「      「      「」      「」      「      「      「      「」      「」      「」      「      「      「      「      「」      「        「	
--	---	--

> [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

)ポリシーの詳細 Default		×
□       ワークステーションの設定         □・ザ アクションをログ         アクションをログ         Windows セキュリティセンター         更新         ブロギジ         スキャン最定         スキャン最定         スキャンのイブ         USBデバイス         スケジョール         スキャンタイブ         USBデバイス         フケジール         スキャンタイブ         USBデバイス         スケジョール         スキャンタイブ         USBデバイス         スケジョール         スキャンタイブ         B支ご         プログラムルール         ネッドワークルール         詳細ルール         信頼されたゾーン	プロキシ         Faronica Core Server または「Web サーバーを更新」に接続するプロキシがワークステーションに必要な場合は以下の設定を行ってください。         プロキシの有効化         プロキシ サーバー情報         アドレス:       ポート:         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         認証の種類:       Dasic         ユーザ名:       パスワード:         ドメイン:       ・	
() () () () () () () () () () () () () (	OK きゃンセル(L) 」 道用(P)	

- > [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。
- [スキャンタィプ]ペイン

🚯 ボリシーの詳細 Default					×
<ul> <li>() オリシーの詳細 Default</li> <li>□ ○ ワークステーションの設定 ユーザ アウション アウションをログ Windows セキュリティセンター 更新 プロキシ</li> <li>□ ○ スキャン設定</li> <li>スキャン設定</li> <li>スキャン設定</li> <li>スキャンジョール スキャン例外 クリーンアップアウション</li> <li>アクライブ代表表</li> <li>□ 逆 フィイアウォール(保護 設定 プログラムルール ネットワークルール 詳細ルール (言頼されたゾーン</li> </ul>	<b>スキャンタイプ</b> rootkit 検知を有効化 アーカイブの中身をスキャン リムーバブル ドライブを含まない レジストリをスキャン 実行中のプロセスをスキャン Max archive file size limit:	ウイック マ 100 単 ME	デイーブシステム ▼ □ ▼ デフォルドにま	カスタム 「 「 「 、 、 実す(G)	×
			ОК	キャンセル(L) 道用	∃(P)

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

🕼 ポリシーの詳細 Default	
<ul> <li>□ ● ワークステーションの設定 ユーザアグション アクジョンをログ Windows セキュリティセンター 更新 プロキシ</li> <li>□ ● スキャン設定 スキャンタイプ</li> <li>□ ○ アイアイマ スケジュール スキャン(例外 クリーンアップアグション</li> <li>◆ アクティブ(保護 設定 プログラムルール ネットワークルール 詳細ルール</li> <li>(言頼されたゾーン</li> </ul>	<ul> <li>USBデバイス装着時にスキャンする</li> <li>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 デバイスは自動的にスキャンされないため、進行中のスキャンを実行したら、手動でスキャンしてください)</li> <li>USB スキャンを行うために、進行中のスキャンを中断する(中断されたスキャンは再開しません)</li> <li>貸進行中のUSBスキャンの抑制」ダイアログ</li> </ul>
ポリシーの詳細\スキャン設定\USBデバイス	<u>OK</u> キャンセルし) 適用P 

[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。

	1
<ul> <li>□ - クノステーションの設定 <ul> <li>□ - ザ アクションをログ アクションをログ Windows セキュリティセンター 更新 プロキシ スキャン設定 スキャン設定 スキャン設定 スキャンの引力 USBデバイス スケジュール スキャン例外 クリーンアップアクション ジアグライブ保護 ジェアクウォール/保護 設定 プログラムルール ネットワークルール 詳細ルール 信律順どれたゾーン         </li> </ul> </li> </ul>	スケジュール         クイックスキャンが有効         起物 ⑧:00 ●       中止 ◎ スキャン完了時         ○ ⑨:00 ●         □ 日 ○ 月 ○ 火 ○ 水 ○ 木 ○ 金 □ ±         ディーブスキャンを有効化         起物 1:00 ●       中止 ◎ スキャン完了時         ○ ③:00 ●         □ 日 ○ 月 ○ 火 ○ 水 ○ 木 ○ 金 □ ±         ガジュン         □ 日 ○ 月 ○ 火 ○ 水 ○ 木 ○ 金 □ ±         オブション         ごとにスキャンが開始するよう、ランダムにスケジュール □ 分         開始に強にスキャンオブションを未確認         ○ ケック スキャンの実行もユーザにプロンプトします

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。

<ul> <li>□ ふ ワークステーションの設定</li> <li>ユーザ アジョン アジョンセルブ</li> <li>Windows セキュリティセンター 更新 プロキシ</li> <li>□ ネトマンタイプ</li> <li>USBF/ドイス</li> </ul>	スキャン例外 安全にわかっているファイルを対けフォルダを指 Anti-Muasではファイルを不正または恋味であ 法のリストにはウィルスとして報告されない項目 適切(A) でてご道社(S)	定します。ファイルま として報告しません。 目が表示されています リストから別	をはフォルダを追加すること す。 「昨(D)	C., Faronics
スケジュール スモンダが パーンアップアウション ◎ アラティ(学校 つ アジィ(学校 10 <sup>7</sup> 5L/Nール お花 ガログシL/Nール ネッドワーンルール 詳細ルール (含様されたゾーン	<u>名前</u>		道加データ   道加データ	2-4

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。

() X+v	ン例外の追加
許可:	フルパスによるファイル
	C:\Users\AdminUser\Desktop\FC_AV_BD_4. 参照(B)
	ワイルドカード(*)を使用できます
	OKキャンセル(N)

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。

<ul> <li>□ ● ワークステーションの設定</li> <li>□ ーザ アグション</li> <li>アグションを力グ</li> <li>Windows セキュリティセンター 更新 プロキシ</li> <li>□ ● スキャン表定 スキャンあ定</li> <li>スキャン表定</li> <li>USBF/F/A ス</li> </ul>	スキャン例外 安全にかっているファイルまたはフォルダを指定 Ans-Muaではファイルを不正または感染液みと 次のリストにはウッルスとして解告されない項目が i動のAi すべて選択(S)	します。ファイルまたは て報告しません。 「表示されています。 リストから削り余	:フォルダを注意加することで、1 (D)	aronics
スケジュール	名前	種類	追加データ	ユーザ
スキャン1999↑ クリーンアップアクション	C:\Users\AdminUser\Desktop\FC_AV_BD	ファイル名とパス	2017/01/09 16:15	FaronicsCor
設定 プログラムルール ネットワークルーフル 詳細ルール 音欄されたゾーン				
			0K ++>	セル(L) 適用(



• [クリーンアップアクション]ペイン

🌘 ポリシーの詳細 Default		×
<ul> <li>□ ● ワークステーションの設定 ユーザアグション アクションをログ Windows セキュリティセンター 更新 プロキシ</li> <li>□ ● スキャン設定 スキャン処定 スキャン処プ USBデバイス スケジュール スキャン例外 DI ● アクティブ(保護</li> <li>□ ■ ファイアウオール(保護 設定 プログラムルール ネットワークルール 詳細ルール (言頼されたゾーン</li> </ul>	クリーンアップアクション 感染したファイルに対するデフォルトアクション ● クリーン/電離 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/間除 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。 ■ 以上前のアイテムは検疫から削除します ■ 日数	
ポリシーの詳細はキャン設定とリーンアップアクション	OK         キャンセル(L)         適用(P)	

- > 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

<ul> <li>□ ◆ ワークステーションの設定 ユーザアクション アクションをログ Windows セキュリティセンター 更新 プロキシ</li> <li>□ ◆ スキャン設定 スキャンタイプ USBデドイス スケジュール スキャン例外 クリーンアップアクション ● プロデブイス</li> <li>○ オャンタイプ</li> <li>● 本 フィアウォール スキャン例外</li> <li>クーンア・ファブアクション</li> <li>● アクティブ(保護 設定 プログラムルール ネットワークルール 詳細ルール 信頼されたゾーン</li> </ul>	設定 ファイアウォール保護の有効化 受力イアウォールの無効化を許可する ファイアウォールの回び記録を有効化する
ポリシューの話が知って、イアウィュール(兄弟)語や学	

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。

<ul> <li>□ (-) (-) (-) (-) (-) (-) (-) (-) (-) (-)</li></ul>	プログラムル プログラムルールは ログラムルールはテ 追加(A)	ーー <b>ル</b> た、ネットワークアクティビテ 「フォルトのルールよりも優 編集(E) 所服	ィとアプリケーショ  先します。 デフォ  (M)	ンの間のファイ ・ルトのルールは	戸ウォ	⊢ールのアクシ: 見できますが、	記り	を定義します。 記できません。	9	
スキャンダイン USBデバイス	名前	プログラム	信頼された受	信頼された	Ĕ	信頼されない	3	信頼されない		
スケジュール コという/別の	Faronics Event	%PROGRAMFILES	許可	許可	-	東国ノーノ	-	許可	-	
スイヤンIngjr クリーンアップアクション	Faronics Core	%PROGRAMFILES	許可・	・許可	-	許可	-	許可	-	
● アクティブ保護 マロン マクティブ保護	Faronics Anti-Vi	%INSTALL_DIR%\	許可,	1 許可	•	許可	•	許可	•	
	Faronics Anti-Vi	%INSTALL_DIR%\	許可	* 許可	•	許可	•	許可	•	
プログラムルール	Faronics Anti-Vi	%INSTALL_DIR%\	許可·	• 許可	•	許可	•	許可	•	
ネットワークルール 詳細山ー山	Faronics Core	%PROGRAMFILES	許可	* 許可	•	許可	•	許可	•	
信頼されたゾーン	Faronics Enterp	%PROGRAMFILES	許可・	• 許可	•	許可	•	許可	•	
	Internet Explorer	%PROGRAMFILES	許可・	・許可	-	ブロック	•	許可	•	
	lsass.exe	%WINDIR%\system	ブロック・	「 許可	•	ブロック	•	許可	•	
	services.exe	%WINDIR%\system	ブロック・	・ 許可	•	ブロック	•	許可	•	
	winlogon.exe	%WINDIR%\system	ブロック・	・ 許可	•	ブロック	•	許可	•	
	svchost.exe	%WINDIR%\system	ブロック・	* 許可	•	許可	•	許可	•	
	Deep Freeze S	%PROGRAMFILES	許可・	・ 許可	•	許可	•	許可	•	
	Deep Freeze A	%PROGRAMFILES	許可	・ 許可	•	許可	•	許可	•	
	Deep Freeze C	%PROGRAMFILES	許可 、	* 許可	•	許可	•	許可	-	

[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。

🗊 ルールを追加する		>
プログラムルールにより特定のプログラムに許 リケーション」ルール設定よりも優先します。	可が与えられます。プログラムルーノ	レは「その他のアプ
名前:		1
1 プログラ:		
		参照(R)
例: c:\path\program.exe		
%ProgramFiles%\browser\brows	er.exe	
信頼された受信ゾーン:	許可	
信頼された送信ゾーン:	許可	
信頼されない受信ゾーン:	<b>許可</b>	
信頼されない送信ゾーン:	許可	
<u> ゾーンとは?</u>	OK	キャンセル(N)

- > [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。

🚺 ボリシーの詳細 Default							×
<ul> <li>□ ふ ワークステーションの設定</li> <li>ユーザアクション</li> <li>アクションをログ</li> <li>アクションをログ</li> <li>Windows セキュリティセンター</li> <li>更新</li> <li>プロキジ</li> <li>□ ふ えたべき設定</li> <li>□ この かく?</li> </ul>	ネットワーク ネットワークルー、 は編集できます; 名前	<b>リルール</b> いは、ネットワークアクティビティ) が、育成家はできません。 説明	でのファイアウォー 信頼された受 信 ゾーン	-ルのアクションを   信頼されたう   信ゾーン	を定義します。ネッ き 信頼されない 受信ゾーン	トワークルール ) 信頼されない 送信ゾーン	3
スキャンタリン US5デバイス スケジュール スキャン例外 クリーンアップアウション ● アウティブ保護 回転 フログラムルール ネットワークルール 詳細ルール 信頼されたゾーン	IGMP Ping Otherlemp DHCP DNS VPN BCAST LDAP Kerberos NETBIOS	Internet Group Manag Ping and Tracert Other ICMP packets Dynamic Host Config Domain Name System Virtual Private Network Broadcast Lightweight Directory Kerberos Protocols Microsoft File and Prin	許可     、       許可     、	<ul> <li>許可</li> <li>許可</li> <li>許許許許許許許許許許許許</li> <li>가許可</li> <li>가許可</li> <li>가許可</li> <li>가許可</li> <li>가</li> </ul>	<ul> <li>許可</li> </ul>	<ul> <li>許可</li> </ul>	
OK キャンセル(L) 適用(P)							
ポリシーの詳細、ファイアウォールイ保護、ネットワークル	-JL						



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
Otherlcmp	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。

<ul> <li>□ ● ワークステーションの設定 ユーザ アグジョンをDづ Whodows ビキュリティビンター 更新 ブロキジ</li> <li>□ ● スキャン設定 スキャンかイブ いSBFプドイス スキャンの州外 ウリーンアウブアウジョン</li> <li>● ● アグライパ経過 ● ● フィイグウォール/保護 香油 「ログラムルール ネキャンの川 (音報されたジーン)</li> <li>○ ● マンビルル</li> </ul>	♪ボリシーの詳細 Default		×
OK     キャンセル(L)     適用(P)	<ul> <li>オリシーの詳細 Default</li> <li>□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □</li></ul>	詳細ルール         詳細ルールはリスト順に処理されます。         適加(A)       編集(E)       削除(M)       上(U)       下(T)         名前       プログラム       アクション       方向       プロトコル       ローカル         名前       プログラム       アクション       方向       プロトコル       ローカル       リモー・ トポート         FaronicsSA       詳可       面方       UDP       7726       いずれか	
uno, la Férencia (l'India, la Verte) Férencia a		OK キャンセル(L) 適用(P)	

[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。

🌘 詳細ルールを追	加する		×
詳細ルールは、指) ます。これには、1つ まれる場合がありま	定したアプリケーション、ボート、または、 または雑数のプロトコル、ローカルボー ます。詳細ルールは、道加、編集、また	クロトコルに対するファイアウ トまたはリモートボート、お とは削取象できます。	フォールのアクションを定義し よびトラフィックの方向が含
名前:			
ブログラ はべてのつ	カガラム(ご適用する(こけ空間)にする)・		
			参照(R)
例: c:\path	n \program.exe		
%Progra	amFiles%\browser\browser.exe		
アクション:	iii可 💌		
方向:	両方		
プロトコルタイプ:	TCP	18力D(A)	
		前(耶余(M)	
ローカルボート:	すべてのポート		
	例: 80, 443, 5000-5010		
リモートボート:	すべてのボート		
	例: 80, 443, 5000-5010		OK キャンセル(N)

- > [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。

信頼されたゾーン 信頼されたゾーンは、安全なコンピュータ、ネットワーク、 ト(信頼されていない)ゾーンは、アプリケーションとネットワ 追加(A) 編集(E) 削除(M) 名前 説明	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 ワークルールによって異なる取り扱いができます。 種類 アドレス
	信頼されたゾーン 信頼されたゾーンは、安全なコンピュータ、ネットワーク、 ト(信頼されていない)ゾーンは、アプリケーションとネット 追加(A) 編集(日 削防(M)           追加(A) 編集(日 削防(M)           名前

[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。

●信頼されたゾーンを追加する 🛛 📉							
ー あなたが信頼済みゾーンになるようにしたい領域を入力します。通常、信頼され たゾーンは、自宅や職場のネットワークは、特定のコンピュータ、また(IPPドレスの 範囲です。							
名前:							
1997:							
アドレスタイプ: IPアドレス 💌							
IPアドレス:							
OK +++>+UN							

- > [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。
- [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。
- 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。
- 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。
- 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。
- 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。
- 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。

(	Faronics Anti-Vir	rus				×
	検疫 Faronics るいはコン	Anti-Virus で検疫処理されたす/ パュータから削除された検疫済。	べてのリスクが検疫画面にま みリスクを表示することがで	長示されます。個 きます。	々のリスクの詳細、検疫からリストアされたリスクあ	
	検疫リスク:2					
	コンピュータ名	名前	追加データ	経過日数	ファイルのパス	
	WIN-JHCEA3OA	EICAR-Test-File (not a virus)	2017/01/16 13:37:00	0	C:\Users\AdminUser\Desktop\EICAR.txt	
	WIN-JHCEA3OA	EICAR-Test-File (not a virus)	2017/01/16 13:36:00	0	C:\Users\AdminUser\Desktop\EICAR.txt	
	- 7 <del>-</del> - b7					
	WIN-JHCEA3OABC	02の検疫項目の取得が完了し	ました。			
	すべてを選択	検疫からリストア	コンピュータから削除		閉じる	

- 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。
- 3. 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
- 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。

	スキャン(5) 履歴(出)	_ × <sub>検疫(0)</sub>
保護されている		世史
すべての保護設定が有効になり、最新	アクティブ保護	ファイアウォール保護
の状態になります	<sub>有効</sub>	<sup>有効</sup>
リスク検出統計	く	く
スキャン完了: 3	更新ステータス	スキャン ステータス
スキャンによりリスク除去済み: 1	自動更新有効	最後のスキャン:
アクティブ保護によりリスクブロック済み: 0	スキャンエンジン: v3.0.5.370	2019/01/08 13:49:48
ファイアウォールによりブロック済み: 317	定義: v105130	次回のスキャン:
除去またはまブロックされたリスク総数: 318	2019/01/08 10:39:36	2019/01/09 8:00:00
リセット数(R)	今すぐ更新(L)	今すぐスキャン(N)

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。



[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。

	概要(0)	スキャン(S)	履歴(出)	検疫(0)	_ ×
既知のリスクのみチェック(K)     既知のリスクのみチェック					
デイーブ システム スキャン(D) コンピュータにあるすべてのファイルをチェック		<i></i>	<b>イック ス</b> ピ 今すぐスキャン	キャン	
スキャンをカスタム(C) 既知のリスクのみチェック					
				www.faro	nics.com (j)



- 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。

- [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。

		S" eat Protection	概要(0)	スキャン(S)	履歴(出) ■ リスクが検出され	_ × 検疫(Q) たスキャンのみを表示する (W)
開始日時	期間(分:秒)	スキャンタイプ	実行タイプ	総リスク数	除去されたリスク	定義のバージョン
2019/01/08 13:49:37	00:00	カスタム	手動	1	1	105130
2019/01/08 13:49:15	00:04	カスタム	手動	1	0	105130
2019/01/08 13:42:18	00:10	中止 クイック	手動	0	0	105130
2019/01/08 13:03:52	08:32	クイック	手動	0	0	105130
言羊組( <u>D</u> )						
						www.faronics.com (j

- 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。

	URUS USTED Threat Protection	概要①	スキャン(S)	履歴(出)	<u> 検疫(Q)</u>	_ ×
						検疫リスク:1
名前	追加データ		経過日数	ファイルのバス		
EICAR-Test-File (not a virus)	2019/01/08 13:49:47		0	UNC\vboxsrv\Shared\	EICAR\eicar.com.txt	
						_
						_
						_
復元( <u>R</u> ) 削除( <u>D</u> )						
					www.far	onics.com (j

- 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。



管理

## 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

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]、[スキャンのー時停止]、[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。

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。
- 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。

Faronics Anti-Virus 4 Loadin - InstallShield Wizard プログラムの削除 ご使用のシステムからプログラムを削除するオプションを選択しました。	×
「削除」をクリックして、コンピュータから Faronics Anti-Virus 4 Loadin を削除してくた 除を実行すると、このプログラムは、使用できなくなります。	ざい。削
設定を参照したり変更する場合は、「戻る」をクリックします。	
バージョン 4.0	.2100.346
Instalishield < 戻る(B) 削除(R)	キャンセル

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。

🙀 Faronics Anti-Virus 4 Loadin - InstallShield Wizard						
1	インストールを正常に終了する(とは、Faronics Core Serverサー ビスを再起動する必要があります。					
	Faronics Core Serverサービスを再起動すると、有効なセッショ ンの接続がすべて切断されます。今これを行いますか?					
	Faronics Core Serverサービスを今再起動するには、はいを選択します。					
	Faronics Core Serverサービスを後で手動で再起動するには、 いいえを選択します。					
InstallShield						

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。

