# F-Secure Server Protection

# 目次

# 第 章
# 1

## はじめに

本ガイドでは、製品に関する一般的な情報を提供し、使用方法について説明します。

F-Secure Server Protection は、最新のツールを含め、Windows サーバに強力なセキュリティ機能を提供します。データガードやアプリケーション制御などの高度なセキュリティ機能を組み込んだPremiumバージョンが含まれています。Rapid Detection and Response はライセンスタイプを変更することでもアクティベートできます。

本製品は以下のサブスクリプションを利用してインストールすることができます。

- Server Protection
- Server Protection Premium
- Server Protection Premium + Rapid Detection & Response

第章
2

# 製品を使用するには

**トピック：**



ここでは、製品ツールを開く方法および製品の設定を変更する方法について説明します。

**注：** F-Secure Elements Endpoint ProtectionとF-Secure Client Securityでは、管理者が一部のセキュリティ設定を実施する場合があるため、一部の機能をローカルで変更できない場合があります。

## 2.1 製品の設定を変更する

製品の動作は設定から変更できます。

製品の設定を変更するには管理者権限が必要です。一部の設定はトレイ アイコンのコンテキスト メニューからアクセスできます。

**注:** F-Secure Elements Endpoint ProtectionとF-Secure Client Securityでは、管理者が一部のセキュリティ設定を実施する場合があるため、一部の機能をローカルで変更できない場合があります。

**関連タスク**

マルウェア スキャンを実行するページ16
危険なファイルや不要なアプリケーションが存在していないことを確認するためにコンピュータ全体をスキャンできます。

アプリとファイル制御を使用するページ20
「**アプリとファイル制御**」ビューでは製品がブロックしたアプリケーションとファイルを確認・管理できます。

Windows ファイアウォールの設定を変更するにはページ35
ファイアウォールを有効にすると、コンピュータのアクセスが制限されます。

最近のイベントを表示するページ9
「**イベント履歴**」画面では、本製品が行った処理を確認することができます。

すべてのセキュリティ機能を無効にするページ8
セキュリティ機能を無効にすると、コンピュータのシステム メモリを開放できます。

### 2.1.1 製品の設定のクイック アクセス

トレイ アイコンのコンテキスト メニューから一部の製品の設定をアクセスできます。

トレイ アイコンのコンテキスト メニューを開くには

1. Windows タスクバーにある製品のアイコンを右クリックします。

   

   **注:** 製品のアイコンが隠されている場合、タスクバーにある [**非表示アイコンを表示**] の矢印をまずクリックします。

2. コンテキスト メニューから次のオプションを選択できます。

| オプション | 説明 |
|---|---|
| **現在のステータスを表示** | コンピュータの現在のセキュリティ ステータスを表示します。 |
| **更新を確認する** | 最新のアップデートを確認・ダウンロードします。 |
| **メッセージを表示** | 本製品に関連する重要な通知を表示します。 |
| **最近のイベントを表示** | 本製品がコンピュータやを保護するために行った処理を表示します。 |
| **設定を開く** | 製品の設定を開きます。 |

| オプション | 説明 |
| --- | --- |
| **本製品について** | 製品のバージョン情報を表示します。 |

### 2.1.2 すべてのセキュリティ機能を無効にする

セキュリティ機能を無効にすると、コンピュータのシステム メモリを開放できます。

**注:** 管理者がセキュリティ機能をオフにすることをブロックするポリシーを設定している可能性があります。

**注:** セキュリティ機能を無効にすると、コンピュータは完全に保護されていない状態になります。

1. 製品を Windows **Start** メニューから開きます。
2. メインページで を選択します。
3. [**すべてのセキュリティ機能を無効にする]** を選択します。

コンピュータを次回再起動するときにセキュリティ機能が自動で有効になります。また、製品のメインビューから手動で有効にすることもできます。

## 2.2 統計情報を確認する

セキュリティ ステータスのアイコンは製品が実行中であることを示し、セキュリティの統計情報は製品がコンピュータをどのように保護したかを示します。

### 2.2.1 セキュリティのステータス アイコン

セキュリティ ステータス アイコンは、製品の全体的なステータスとその機能を表示します。

セキュリティのステータス アイコン:

| ステータス アイコン | ステータス | 説明 |
| --- | --- | --- |
| | OK | コンピュータが保護はされています。<br>機能が有効になっており、正常に動作していることを示します。 |
| | 失効 | コンピュータは保護されていません。<br>サブスクリプションが失効しました。 |
| | 失効および無効 | コンピュータは保護されていません。<br>サブスクリプションが失効しており、製品が無効になっていることを示します。 |

| ステータス アイコン | ステータス | 説明 |
|---|---|---|
|  | 無効、故障 | コンピュータが完全または一部保護されていません。<br>対応がすぐに必要でがあることを示します (重大な機能が無効またエラーになっている、アップデートが長い間更新されていない場合など)。 |
|  | 無効 | コンピュータが保護されていません。<br>対応が必要な操作 (セキュリティ機能が無効など) があることを示します。 |
|  | アップデート中 | セキュリティを設定しています。<br>製品を更新しています。 |

表示されるステータス メッセージの例

- **Google Chrome のブラウザ拡張機能が使用されていません**
- **Mozilla Firefox のブラウザ拡張機能が使用されていません**
- **Microsoft Edgeのブラウザ拡張機能は使用されていません**

## 2.2.2 最近のイベントを表示する

「**イベント履歴**」画面では、本製品が行った処理を確認することができます。

イベント履歴には、インストールされた製品に関連するイベントおよび製品が実行したセキュリティ対策の詳細が表示されます。たとえば、検出され、駆除/隔離されたすべての有害なアイテムを表示します。

製品のイベント履歴全体を表示するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで を選択します。
3. [**最近のイベント**] を選択します。
   「**イベント履歴**」画面が開きます。

イベント履歴には、各イベントの時間と説明が表示されます。イベントの種類に応じて、イベントをクリックして詳細を表示できます。たとえば、有害なファイルの場合、次の情報が表示されます。

- マルウェア (危険なファイル) が検出された日時
- マルウェアの名前とコンピュータで検出された場所/パス
- 実行されたアクション

# 第 章
# 3

## コンピュータを危険なコンテンツから保護する

**トピック：**



コンピュータの破壊、個人情報の盗難、コンピュータの不正使用といった問題を引き起こす可能性のあるプログラムからユーザを保護します。

デフォルトでは、マルウェアは検出時にすぐに処理され、コンピュータに害を及ぼせないようになります。

デフォルトでは、ローカルのハードディスク、リムーバブル メディア (ポータブル ドライブや DVD など)、およびダウンロードされたコンテンツを自動的にスキャンします。

本製品は、危険ファイルの存在を示す可能性のある変更がないかコンピュータを常に監視します。重要なシステム プロセスを変更するシステム設定やその試みなど、問題を引き起こす可能性のあるシステムの変更を検出した場合、危険性があるため、ディープガードによってアプリケーションの実行が停止されます。

**注：** 管理者が一部のセキュリティ設定を実施する場合があるため、一部の機能をローカルで変更できない場合があります。

## 3.1 危険なコンテンツについて

危険なアプリケーションとファイルはデータを破壊したり、コンピュータへの無断なアクセスを入手して個人情報を盗み取ろうとします。

### 3.1.1 不要な可能性があるアプリケーションと不要なアプリケーション

「不要な可能性があるアプリケーション」には、不快な、または望ましくないと思われる動作や特性があります。「不要なアプリケーション」は、デバイスやデータに深刻な影響を与えることができます。

次の条件がある場合、アプリケーションは不要である可能性があります。

- **プライバシーや生産性に影響を与えます** - たとえば、個人情報の漏洩や、不正な操作を行います。
- **デバイスのリソースに過度の負担をかけます** - たとえば、過剰にストレージやメモリの容量を使用します。
- **デバイスのセキュリティやそのデバイスに保存されている情報を侵害します** - たとえば、予期しないコンテンツやアプリケーションにさらされます。

これらの動作や特性がデバイスやデータに与える影響はさまざまです。しかし、このアプリケーションをマルウェアとして分類するほど有害なわけではありません。

より深刻な動作または特性を示すアプリケーションは、「不要なアプリケーション」とみなされます。このようなアプリケーションはより注意深く扱われます。

本製品は、PUA か UA かによってアプリケーションを異なる方法で処理します。

- **不要な可能性があるアプリケーション** - 製品がアプリケーションの実行を自動的にブロックします。アプリケーションを確実に信頼できる場合、スキャンから除外するように F-Secure 製品を設定できます。ブロックされたファイルをスキャンから除外するには管理者権限が必要です。
- **不要なアプリケーション** - 製品がアプリケーションの実行を自動的にブロックします。

**関連タスク**

リアルタイム スキャンを有効にするにはページ15
リアルタイムスキャンを有効にすると、コンピュータに害を与える前に危険なファイルを削除することができます。

マルウェア スキャンを実行するページ16
危険なファイルや不要なアプリケーションが存在していないことを確認するためにコンピュータ全体をスキャンできます。

アプリとファイル制御を使用するページ20
「**アプリとファイル制御**」ビューでは製品がブロックしたアプリケーションとファイルを確認・管理できます。

### 3.1.2 ワーム

「ワーム」は、ネットワーク上にあるデバイスから別のデバイスに、自分自身のコピーを送信するプログラムです。一部のワームは、影響を受けたデバイス上で有害な動作も実行します。

多くのワームは、ユーザに魅力的に見えるように設計されています。画像、動画、アプリケーション、その他の有用なプログラムやファイルのように思うかもしれません。この偽装の目的は、ユーザを引き付け、ワームをインストールさせることです。他のワームは完全なステルス設計で、ユーザに気付かれることすらなく、ワーム自体をインストールするデバイス (またはそれにインストールされたプログラム) の脆弱性を悪用できます。

ワームは、一度インストールされると、デバイスの物理リソースを使用して自身のコピーを作成し、それらのコピーをネットワーク経由で届く範囲の他のデバイスに送信します。大量のワームのコピーが送

信されると、デバイスのパフォーマンスが低下する可能性があります。ネットワーク上の多くのデバイスが影響を受け、ワームのコピーを送信すると、ネットワーク自体が混乱する可能性があります。一部のワームは、影響を受けたデバイスに保存されているファイルを変更したり、他の有害なアプリケーションをインストールしたり、データを盗むなど、直接害を与えることもできます。

ほとんどのワームは、一種類のネットワークにのみ感染します。比較的まれですが、2種類以上のネットワークに拡散できるものもあります。通常、ワームは、次のネットワークに拡散しようと試みます(これ以外にアクセスが低いものを標的にするものもあります)。

- ローカル ネットワーク
- メール ネットワーク
- ソーシャル メディア サイト
- Peer-to-peer (P2P) 接続
- SMS/MMS メッセージ

**関連タスク**

リアルタイム スキャンを有効にするにはページ15
リアルタイムスキャンを有効にすると、コンピュータに害を与える前に危険なファイルを削除することができます。

マルウェア スキャンを実行するページ16
危険なファイルや不要なアプリケーションが存在していないことを確認するためにコンピュータ全体をスキャンできます。

アプリとファイル制御を使用するページ20
「**アプリとファイル制御**」ビューでは製品がブロックしたアプリケーションとファイルを確認・管理できます。

### 3.1.3 トロイの木馬

「トロイの木馬」は、魅力的な機能や特徴を提供している、あるいは提供していると見せかけるプログラムですが、バックグラウンドで静かに有害な動作を行います。

ギリシャの伝説のトロイの木馬にちなんで名付けられたトロイの木馬は、ユーザに魅力的に見えるように設計されています。ゲーム、スクリーンセーバー、アプリケーションのアップデート、その他の有用なプログラムやファイルのように見えるかもしれません。一部のトロイの木馬は、人気のあるプログラムや有名なプログラムを模倣あるいはそのままコピーし、より信頼性を高く見せています。この偽装の目的は、ユーザがトロイの木馬をインストールするよう誘導することです。

インストールされると、トロイの木馬は「罠」を使用し、正当であるという錯覚を維持することもできます。たとえば、スクリーンセーバーアプリケーションや文書ファイルに偽装されたトロイの木馬は、画像または文書を表示します。ユーザがこれらの罠に気を取られている時に、トロイの木馬は、バックグラウンドで他の動作を静かに実行します。

トロイの木馬は、通常、デバイスに有害な変更(ファイルの削除や暗号化、プログラム設定の変更など)を行ったり、そこに保存されている秘密データを盗み出したりします。トロイの木馬は、実行する動作によって区別できます。

- **Trojan-downloader (ダウンローダー型トロイの木馬)**: リモート サイトに接続して他のプログラムをダウンロードしてインストールします。
- **Trojan-dropper (埋め込み型トロイの木馬)**: 1つまたは複数の追加プログラムが含まれており、それをインストールします。
- **Trojan-pws (パスワード窃盗型トロイの木馬)**: デバイスに保存されたパスワードや Webブラウザに入力されたパスワードを盗み出します。
    - **Banking-trojan (バンキング型トロイの木馬)**: オンライン バンキング ポータルのユーザ名とパスワードを特定する特殊なトロイの木馬です。

- **Trojan-spy (スパイ型トロイの木馬)**: デバイスのアクティビティを監視し、詳細情報をリモート サイトに転送します。

**関連タスク**

リアルタイム スキャンを有効にするにはページ15
リアルタイムスキャンを有効にすると、コンピュータに害を与える前に危険なファイルを削除することができます。

マルウェア スキャンを実行するページ16
危険なファイルや不要なアプリケーションが存在していないことを確認するためにコンピュータ全体をスキャンできます。

アプリとファイル制御を使用するページ20
「**アプリとファイル制御**」ビューでは製品がブロックしたアプリケーションとファイルを確認・管理できます。

### 3.1.4 バックドア

「バックドア」は、プログラム、デバイス、ポータルまたはサービスのセキュリティ機能を回避するために使用できる機能またはプログラムです。

プログラム、デバイス、ポータル、またはサービスの機能は、その設計や実装がセキュリティリスクをもたらす場合、バックドアと見なすことができます。たとえば、オンラインポータルへのハードコードされた管理者アクセスは、バックドアとして使用できます。

バックドアは、通常、プログラム、デバイス、ポータル、またはサービスのコードの欠陥を利用します。欠陥は、バグ、脆弱性、または文書化されていない機能である可能性があります。

アタッカーは、バックドアを使用して、不正アクセスを取得したり、アクセス制限、認証、暗号化などのセキュリティ機能を回避するための有害なアクションを実行できます。

**関連タスク**

リアルタイム スキャンを有効にするにはページ15
リアルタイムスキャンを有効にすると、コンピュータに害を与える前に危険なファイルを削除することができます。

マルウェア スキャンを実行するページ16
危険なファイルや不要なアプリケーションが存在していないことを確認するためにコンピュータ全体をスキャンできます。

アプリとファイル制御を使用するページ20
「**アプリとファイル制御**」ビューでは製品がブロックしたアプリケーションとファイルを確認・管理できます。

### 3.1.5 エクスプロイト

「エクスプロイト」(脆弱性を利用したソースコード)とは、プログラムの欠陥を利用して予期せぬ動作を実行するオブジェクトまたはメソッドであり、アタッカーが有害な行為を行える条件を生み出します。

エクスプロイトは、オブジェクトまたはメソッドのいずれかになります。たとえば、巧妙に細工されたプログラム、コードや文字列はすべてオブジェクトです。コマンドの特定のシーケンスがメソッドです。

エクスプロイトは、プログラムの欠陥または抜け穴(脆弱性とも呼ばれます)を悪用するために使用されます。すべてのプログラムが異なるため、各エクスプロイトはその特定のプログラムに合わせて慎重に調整する必要があります。

アタッカーがエクスプロイトを配信してコンピュータやデバイスに影響を与える方法はいくつかあります。

- **ハッキングされた、または巧妙に細工されたプログラムに埋め込む** - プログラムをインストールして起動すると、脆弱性を利用した攻撃が開始されます。
- **メールに添付された文書ファイルに埋め込む** - 添付ファイルを開くと、攻撃が開始されます。
- **ハッキングされた Web サイトや有害な Web サイトに忍ばせる** - サイトにアクセスすると、その脆弱性と利用した攻撃が開始されます。

エクスプロイトを起動すると、強制的にクラッシュしたり、システムのストレージやメモリを改ざんしたりするなど、予期しない動作が発生します。これにより、アタッカーがデータを盗んだり、OS の制限された部分にアクセスするなど、他の有害な措置を実行できるような条件が生じる可能性があります。

**関連タスク**

リアルタイム スキャンを有効にするにはページ15
リアルタイムスキャンを有効にすると、コンピュータに害を与える前に危険なファイルを削除することができます。

マルウェア スキャンを実行するページ16
危険なファイルや不要なアプリケーションが存在していないことを確認するためにコンピュータ全体をスキャンできます。

アプリとファイル制御を使用するページ20
「**アプリとファイル制御**」ビューでは製品がブロックしたアプリケーションとファイルを確認・管理できます。

## 3.1.6 エクスプロイト キット

「エクスプロイトキット」は脆弱性を管理して、脆弱性のあるコンピュータまたはデバイスに危険なプログラムを送り込むためのツールキットです。

エクスプロイトキットには、エクスプロイトが複数含まれおり、それぞれが、プログラム、コンピュータ、またはデバイスの欠陥(脆弱性)を悪用します。キット自体は、通常、有害なサイトやハッキングされたサイトでに配置されているため、サイトを訪れるコンピュータやデバイスがその影響を受けることがあります。

新しいコンピュータやデバイスが仕掛けられたサイトに接続すると、エクスプロイトキットは、キット内のエクスプロイトの攻撃から影響を受ける可能性のある脆弱性を探索します。検出された場合、キットはその脆弱性を利用するためにエクスプロイトを起動します。

コンピュータやデバイスに侵入した後、エクスプロイトキットはペイロードをそのコンピュータに送り込むことができます。これは通常、コンピュータまたはデバイスにインストールされて起動される別の有害なプログラムで、次々に他の不正な操作を実行します。

エクスプロイトキットは、モジュールとして設計され使いやすいため、不正操作者はツールキットにエクスプロイトやペイロードを簡単にに追加・削除できます。

**関連タスク**

リアルタイム スキャンを有効にするにはページ15
リアルタイムスキャンを有効にすると、コンピュータに害を与える前に危険なファイルを削除することができます。

マルウェア スキャンを実行するページ16
危険なファイルや不要なアプリケーションが存在していないことを確認するためにコンピュータ全体をスキャンできます。

アプリとファイル制御を使用するページ20

「**アプリとファイル制御**」ビューでは製品がブロックしたアプリケーションとファイルを確認・管理できます。

## 3.2 コンピュータをスキャンする

*マルウェア保護*はコンピュータに対して危険なファイルのスキャンを自動で行います。

本製品の*マルウェア保護*を常に有効にすることを推奨します。必要に応じてマニュアルスキャンで危険なファイルがないことを確認したり、リアルタイムスキャンから除外したファイルをスキャンしたりできます。また、スケジュールスキャンを設定して特定の日時にコンピュータを定期的にスキャンすることも可能です。

### 3.2.1 リアルタイムスキャンの仕組み

リアルタイムスキャンは、ファイルにアクセスされたときにスキャンを実行し、*マルウェア*を含むファイルが検出された場合、そのファイルへのアクセスをブロックしてコンピュータを保護します。

コンピュータがファイルをアクセスすると、リアルタイムスキャンがファイルのアクセスを許可する前にマルウェアのスキャンを実行します。

リアルタイムスキャンが危険なコンテンツを検出した場合、ファイルが脅威をさらせないように隔離保存されます。

#### リアルタイム スキャンとシステムの処理速度

通常、スキャンは短時間で終わり、使用するシステムリソースも少ないため、ユーザがその処理を意識することはありません。リアルタイムスキャンに必要な時間とシステムの負荷は、ファイルの内容、場所、種類などによって異なります。

CD、DVD、USB ドライブなどのリムーバブル ドライブにあるファイルのスキャンはより長くかかります。

**注：** ZIP ファイルなどの圧縮ファイルは、リアルタイム スキャンではスキャンされません。

次のような場合、リアルタイム スキャンはコンピュータの動作を低下する可能性があります。

- コンピュータがシステム要件に満たない場合
- 多数のファイルを同時にアクセスする場合。たとえば、スキャン対象のファイルが多く格納されているディレクトリを開いた場合など。

#### リアルタイム スキャンを有効にするには

リアルタイムスキャンを有効にすると、コンピュータに害を与える前に危険なファイルを削除することができます。

リアルタイム スキャンが有効であることを確認するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで ⚙ を選択します。
3. **マルウェア保護** > **設定を編集する** を選択します。

   **注：** 設定を変更するには管理者の権限が必要です。
4. [**リアルタイム スキャン**] を有効にします。

## 3.2.2 ファイルを手動でスキャンする

危険なファイルや不要なアプリケーションが存在していないことを確認するためにコンピュータ全体をスキャンできます。

完全スキャンは内部および外部ハードドライブに対してウイルス、スパイウェア、不要な可能性があるアプリケーションをスキャンします。また、ルートキットによって隠されているアイテムも確認します。完全スキャンは完了するまで時間がかかる場合があります。コンピュータの一部(危険なアプリケーションが一般的にインストールされているフォルダなど)をスキャンして不要なアプリケーションや危険なアイテムを効率的に取り除くことも可能です。

### ファイルとフォルダをスキャンする

コンピュータで不審なファイルがある場合、対象のファイル・フォルダのみスキャンできます。このようなスキャンは完全スキャンより早く完了します。たとえば、外部ハードドライブやUSBデバイスを接続した時に効率的にスキャンできます。

### マルウェア スキャンを実行する

危険なファイルや不要なアプリケーションが存在していないことを確認するためにコンピュータ全体をスキャンできます。

コンピュータをスキャンするには

1. 製品を Windows **Start** メニューから開きます。
2. マニュアル スキャンがどのようにコンピュータをスキャンするか最適化を行う場合、メインページから を選択し、[**スキャンの設定**] を選択します。
   a) すべてのファイルをスキャンしたくない場合、[**一般的に有害なコードを含むファイルタイプのみをスキャンする (高速)**] を選択します。
   次のファイル形式は、このオプションを選択したときにスキャンされるファイルタイプの例です: com、doc、dot、exe、htm、ini、jar、pdf、scr、wma、xml、zip。
   b) [**圧縮ファイルをスキャン**] を選択すると、圧縮されたアーカイブ ファイルをスキャンできます (例: ZIP ファイル)。このオプションを選択すると、スキャンの速度が遅くなります。オプションを選択しない場合、アーカイブファイル自体はスキャンされますが、アーカイブの中にあるファイルはスキャンされません。
3. メインページで を選択します。
4. [**マルウェア スキャン**] または [**完全スキャン**] を選択します。
   - **マルウェアスキャン**は、コンピュータのアクティブメモリをスキャンすることから始まり、その後、ドキュメントフォルダを含むマルウェアが一般的に検出された場所をスキャンします。コンピュータ上の不要なアプリケーションや有害なアイテムを短時間で検出し、削除することができます。
   - [**完全スキャン**] は内部および外部ハード ドライブに対してウイルス、スパイウェア、不要な可能性があるアプリケーションをスキャンします。また、ルートキットによって隠されているアイテムも確認します。完全スキャンは完了するまで時間がかかる場合があります。

   ウイルス スキャンが開始します。
5. スキャンで危険なアイテムが検出された場合、危険なアイテムが表示されます。
6. 検出したアイテムをクリックすると処理方法を選択できます。

| オプション | 説明 |
|---|---|
| **駆除** | ファイルを自動的にクリーンします。クリーンできないファイルは隔離保存されます。 |

| オプション | 説明 |
|---|---|
| **隔離保存** | ファイルを安全な場所に移し、コンピュータに害を与えないようにします。 |
| **削除** | コンピュータからファイルを完全に削除します。 |
| **省略** | ファイルをコンピュータに残します。 |
| **除外** | アプリケーションを許可して今後スキャンから除外します。 |

**注：** 危険なアイテムによっては特定のオプションが選択できない場合もあります。

7. [**すべて処理**] を選択するとクリーンアップ処理が開始されます。
8. マルウェア スキャンが結果を表示し、クリーンアップした危険なアイテムの数を確認できます。

**注：** マルウェア スキャンを完了するためにコンピュータの再起動が必要となる場合もあります。その場合、[**再起動**] を選択することで危険なアイテムのクリーンアップを完了し、コンピュータを再起動します。

[**前回のスキャン レポートを開く**] を選択すると、最新のウイルス スキャンの結果を確認できます。

### Windows Explorer でスキャンを実行する

Windows エクスプローラからディスク、フォルダ、およびファイルに対して、危険なファイルおよび不要な可能性があるアプリケーションのスキャンを実行することができます。

コンピュータで不審なファイルがある場合、対象のファイル・フォルダのみスキャンできます。このようなスキャンは完全スキャンより早く完了します。たとえば、外部ハードドライブやUSBデバイスを接続した時に効率的にスキャンできます。

ディスク、フォルダ、またはファイルをスキャンするには

1. スキャン対象のディスク、フォルダ、またはファイルを右クリックします。
2. 右クリック メニューから [**マルウェアをスキャン**] を選択します。
   ウイルス スキャンが開始し、選択したディスク、フォルダ、ファイルをスキャンします。

スキャン中に危険なファイルまたは不要なアプリケーションが検出された場合、ウイルススキャンは処理に対する確認を表示します。

## 3.2.3 スケジュール スキャン

スケジュールスキャンを設定すると、コンピュータを使用していない時間にスキャンが自動的に開始するようにしたり、特定の時間にスキャンを定期的に実行できるようになります。

スケジュール スキャンを設定するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで  を選択します。
3. [**スキャン設定**] を選択します。
4. [**スケジュール スキャン**] を有効にします。
5. [**スキャンを実行**] でコンピュータを自動的にスキャンする頻度を選択します。

| オプション | 説明 |
|---|---|
| **日単位** | スキャンを毎日実行します。 |

| オプション | 説明 |
| --- | --- |
| **毎週** | スキャンを毎週指定の曜日に実行します。リストから曜日を選択します。 |
| **4週間ごとに** | 選択した平日に4週間間隔でコンピュータをスキャンします。リストから平日を選択します。スキャンは、選択された平日から開始されます。 |

6. [**開始時間**] でスケジュール スキャンを開始する日時を選択します。
7. [**低優先度でスキャンを実行**] を選択すると、コンピュータの他の処理に対してスケジュール スキャンの干渉を低くすることができます。
8. すべてのファイルをスキャンしたくない場合、[**一般的に有害なコードを含むファイルタイプのみをスキャンする (高速)**] を選択します。

   次のファイル形式は、このオプションを選択したときにスキャンされるファイル タイプの例です: com、doc、dot、exe、htm、ini、jar、pdf、scr、wma、xml、zip。
9. [**圧縮ファイルをスキャン**] を選択すると、圧縮されたアーカイブ ファイルをスキャンできます (例: ZIPファイル)。このオプションを選択すると、スキャンの速度が遅くなります。オプションを選択しない場合、アーカイブファイル自体はスキャンされますが、アーカイブの中にあるファイルはスキャンされません。

**注:** スケジュール スキャンはプレゼンテーション モードが有効の際にはキャンセルされます。*プレゼンテーションモード*を無効にしたらスケジュールスキャンは自動的に有効になり、スキャンがスケジュール通りに実行されます。

## 3.3 ディープガード

ディープガードは危険性のあるシステム変更を検出するためにアプリケーションを監視します。

ディープガードは使用しているアプリケーションの安全性を確認します。アプリケーションの安全性は信頼性の高いクラウドサービスにより検証されます。安全性を確認できない場合、ディープガードがアプリケーションの動作を監視します。

**ヒント:** F-Secureがアプリケーションを許可されたアプリケーションのリストに追加することを希望する場合は、ここでからアプリケーションの分析を依頼してください。プログラムを解析した後、連絡先の詳細をお知らせいただければ、分析結果をお知らせします。

ディープガードは、*トロイの木馬*、*ワーム*、*エクスプロイト*および他の危険なアプリケーションの検出とブロックを行い、不審なアプリケーションがインターネットに接続することを阻止します。

ディープガードは次のようなシステムの変更を検出できます。

- システム設定 (Windows レジストリ) の変更
- 重要なシステム プログラム (本製品のようなセキュリティ プログラムなど) を無効にしようとする試み
- 重要なシステム ファイルを編集しようとする試み

ディープガードが有効であることを確認するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで ⚙ を選択します。
3. **マルウェア保護** > **設定を編集する** を選択します。

**注:** 設定を変更するには管理者の権限が必要です。

4. [**設定を編集する**] を選択します。

   **注：** 設定を変更するには管理者の権限が必要です。

5. [**ディープガード**] を有効にします。

ディープガードは有効の際にシステムを変更する可能性があるアプリケーションを自動的にブロックします。

**関連タスク**

Security Cloudページ39

Security Cloud (旧「ディープガード ネットワーク」) は、未知のアプリケーションや Web サイト、悪意のあるアプリケーションや Web サイトのエクスプロイト (悪用) に関するセキュリティ データを収集します。

## 3.3.1 データガードを使用する

データガードは、一連のフォルダを監視し、ランサムウェアやその他の有害なソフトウェアによる潜在的で危険な変更を監視します。

「ランサムウェア」は、コンピュータ上の重要なファイルを暗号化してアクセスすることを妨げる有害なソフトウェアです。犯罪者はファイルを復元するために身代金を要求しますが、支払いを選択したとしても、個人データが帰ってくることについては保証はありません。

データガードは、保護しているフォルダのアクセスを安全なアプリケーションに限定します。安全でないアプリケーションが保護しているフォルダにアクセスしようとすると、製品が通知します。特定のアプリケーションを認識/信頼している場合、そのアプリケーションが対象のフォルダにアクセスできるように設定できます。データーガードは、ディープガードが保護しているフォルダのリストを使用して、追加のセキュリティ保護も提供できます。

ランサムウェアなど、破壊的なソフトウェアに対する追加のセキュリティ保護が必要なフォルダを選択できます。

**注:** データガードを使用するには、ディープガードをオンにする必要があります。データガードは、プレミアムバージョンでのみ使用できます。

保護されているフォルダを管理するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで を選択します。
3. **マルウェア保護** > **設定を編集する** を選択します。

   **注：** 設定を変更するには管理者の権限が必要です。

4. [**データガード**] を有効にします。
5. [**保護されているフォルダを表示する**] を選択します。
6. 「**保護**」タブを選択します。
   保護されているすべてのフォルダの一覧が表示されます。
7. 必要に応じてフォルダを追加/削除します。
   新しいフォルダを保護するには
   a) [**追加**] をクリックします。
   b) 保護するフォルダを選択します。
   c) [**フォルダの選択**] をクリックします。
   フォルダを削除するには

a) 一覧からフォルダを選択します。
b) [**削除**] をクリックします。

**ヒント:** 製品をインストールしてから保護されたフォルダの一覧に行った変更を取り消す場合、[**デフォルトに戻す**] をクリックします。

**関連タスク**

保護するフォルダを追加/削除するページ23
ランサムウェアなど、破壊的なソフトウェアに対する追加のセキュリティ保護が必要なフォルダを選択できます。

## 3.4 アプリとファイル制御を使用する

「**アプリとファイル制御**」ビューでは製品がブロックしたアプリケーションとファイルを確認・管理できます。

アクセスするには **アプリとファイルの制御**見る

1. 製品を Windows **Start** メニューから開きます。
2. [**ウイルスと脅威**] を選択します。
3. [**アプリとファイル制御**] を選択します。

NS **アプリとファイルの制御**4つの個別のタブを含むビューが開きます。

**隔離保存** 「隔離保存」は危険なファイルが脅威をさらすことができない場所にあることを示します。本製品は危険なアイテムおよび望ましくないアプリケーションを隔離保存できます。アプリケーションやファイルは必要に応じて後から復元できます。隔離保存したアイテムは必要でない場合には削除することが可能です。隔離保存したアイテムを削除すると、アイテムがコンピュータから完全に削除されます。

**ブロック** このタブはディープガードがブロックしたアプリケーションを表示します。ディープガードは監視しているアプリケーションの中で不審な動作またはインターネットの接続試行を行なっているものをブロックします。

**除外** このタブはスキャンから除外されているアプリケーション、ファイル、フォルダを表示します。ディープガードは除外したアプリケーションの実行をブロックせず、製品は除外したパスに対して危険なアイテムのスキャンを実行しません。フォルダとファイルを除外できます。

**保護** このタブには、破壊的なソフトウェア (ランサムウェアなど) から保護されているフォルダが表示されます。本製品は、危険なアプリケーションがこれらのフォルダに格納されているファイルを変更することをブロックします。

**注:** このタブは、プレミアムバージョンでのみ使用できます。

### 3.4.1 隔離保存したアイテムを表示する

隔離保存したアイテムの詳細を確認できます。

「隔離保存」は危険なファイルが脅威をさらすことができない場所にあることを示します。本製品は危険なアイテムおよび望ましくないアプリケーションを隔離保存できます。アプリケーションやファイルは必要に応じて後から復元できます。隔離保存したアイテムは必要でない場合には削除することが可能です。隔離保存したアイテムを削除すると、アイテムがコンピュータから完全に削除されます。

隔離保存したアイテムの詳細を表示するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで ⋯ を選択します。
3. [**隔離保存と例外**] を選択します。

   **注：** 設定を変更するには管理者の権限が必要です。

   「**アプリとファイル制御**」が開きます。
4. 「**隔離保存**」タブを選択します。
   この一覧では、隔離保存したアイテムの名前、検出日、感染タイプが表示されます。
5. 詳細を表示するには、隔離保存したアイテムをダブルクリックします。
   単一のアイテムの場合、隔離保存したアイテムの元の場所 (パス) が表示されます。

## 3.4.2 隔離保存したアイテムを復元する

隔離保存したアイテムを復元することができます。

必要に応じて、隔離保存フォルダからアプリケーションやファイルを復元することができます。隔離保存フォルダからアイテムを復元するとアイテムに対する保護は無効になりますので、注意が必要です。復元したアイテムはコンピュータ上の元の場所に戻ります。

隔離保存したアイテムを復元するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで ⋯ を選択します。
3. [**隔離保存と例外**] を選択します。

   **注：** 設定を変更するには管理者の権限が必要です。

   「**アプリとファイル制御**」が開きます。
4. 「**隔離保存**」タブを選択します。
5. 復元する隔離保存アイテムを選択します。
6. [**許可**] をクリックします。
7. [**はい**] をクリックして、隔離保存アイテムの復元を確定します。

選択したアイテムが元の場所へ自動的に復元されます。感染の種類によって、アイテムが今後のスキャンから除外されます。

**注:** 除外されているファイルとアプリケーションを表示するには、「**除外**」タブの[**アプリとファイル制御**] ビューを選択します。

## 3.4.3 ファイルまたはフォルダをスキャンから除外する

スキャンから除外されたファイルまたはフォルダに対して有害なコンテンツはスキャンされません。

ファイルまたはフォルダをスキャンから除外するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで ⋯ を選択します。
3. [**隔離保存と例外**] を選択します。

   **注：** 設定を変更するには管理者の権限が必要です。

   「**アプリとファイル制御**」が開きます。
4. 「**除外**」タブを選択します。

このビューには、除外されたファイルとフォルダのリストが表示されます。

5. [**新規追加**] を選択します。
6. スキャンから除外するファイル/フォルダを選択します。
7. [**OK**] を選択します。

指定したドライブ/フォルダがスキャンから除外されます。

### 3.4.4 除外したアプリケーションを表示する

スキャンの対象から除外したアプリケーションを除外リストから削除することで、スキャンの対象に含むことができます。

不要な可能性のあるアプリケーションまたはスパイウェアとして識別されたアプリケーションを安全と断定できる場合、そのアプリケーションをスキャンから除外することができます。

**注:** ウイルスまたは危険なアプリケーションとして動作するアプリケーションを除外することはできません。

スキャンの対象から除外されているアプリケーションを表示するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで を選択します。
3. [**隔離保存と例外**] を選択します。

   **注:** 設定を変更するには管理者の権限が必要です。

   「**アプリとファイル制御**」が開きます。
4. 「**除外**」タブを選択します。
   このビューには、除外されたファイルとフォルダのリストが表示されます。
5. 除外したアプリケーションをもう一度スキャンしたい場合
   a) スキャンの対象に含むアプリケーションを選択します。
   b) [**削除**] をクリックします。

新しいアプリケーションは、スキャン中に除外した場合に除外リストに表示されるようになります。除外リストに直接追加することはできません。

### 3.4.5 ディープガードがブロックしたアプリケーションを許可する

ディープガードが許可/ブロックするアプリケーションを設定できます。

ディープガードはまれに安全なアプリケーションの動作をブロックすることもあります。これは、アプリケーションがシステムを変更する可能性があり、危険性があると判断されることで起こります。また、ディープガードのポップアップが表示されたときに、ユーザがアプリケーションを誤ってブロックした可能性もあります。

ディープガードがブロックしたアプリケーションを許可するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで を選択します。
3. [**隔離保存と例外**] を選択します。

   **注:** 設定を変更するには管理者の権限が必要です。

   「**アプリとファイル制御**」が開きます。
4. 「**ブロック**」タブを選択します。

ディープガードがブロックしたアプリケーションの一覧を表示します。

5. 許可するアプリケーションを選択して、[**許可**] を選択します。
6. [**はい**] を選択して、アプリケーションの許可を確定します。

選択したアプリケーションが「**除外**」リストに追加され、ディープガードがシステムの変更をアプリケーションに許可します。

### 3.4.6 保護するフォルダを追加/削除する

ランサムウェアなど、破壊的なソフトウェアに対する追加のセキュリティ保護が必要なフォルダを選択できます。

データガードは、保護されたフォルダに対する危険なアクセスをブロックします。

1. 製品を Windows **Start** メニューから開きます。
2. メインページで ⋯ を選択します。
3. [**隔離保存と例外**] を選択します。

   **注：** 設定を変更するには管理者の権限が必要です。

   「**アプリとファイル制御**」が開きます。
4. 「**保護**」タブを選択します。
   保護されているすべてのフォルダの一覧が表示されます。
5. 必要に応じてフォルダを追加/削除します。

   新しいフォルダを保護するには

   a) [**追加**] をクリックします。
   b) 保護するフォルダを選択します。
   c) [**フォルダの選択**] をクリックします。

   **ヒント：** 保護されたフォルダにアクセスする必要のあるすべてのアプリケーションを個別に許可する必要があるため、インストールされているゲームやアプリケーションを含むフォルダ (例: Steam Library Folders) を追加しないことを推奨します。追加した場合、アプリケーションが正しく動作しなくなる可能性があります。

   フォルダを削除するには

   a) 一覧からフォルダを選択します。
   b) [**削除**] をクリックします。

**ヒント：** 製品をインストールしてから保護されたフォルダの一覧に行った変更を取り消す場合、[**デフォルトに戻す**] をクリックします。

## 3.5 危険なファイルのダウンロードを阻止する

危険なファイルのダウンロードを阻止することができます。

Web サイトの中には脆弱性や危険なファイルが含まれているものがあります。詳細なネットワーク保護を設定することでアプリケーションが危険なファイルをダウンロードすることを阻止できます。

危険なファイルのダウンロードをブロックする

1. 製品を Windows **Start** メニューから開きます。
2. [**設定を編集する**] を選択します。

   **注：** 設定を変更するには管理者の権限が必要です。

3. メインページで を選択します。
4. **マルウェア保護** > **設定を編集する** を選択します。

   **注：** 設定を変更するには管理者の権限が必要です。

5. [**詳細なネットワーク保護**] を有効にします。

   **注：** この設定はファイアウォールを無効にしても有効です。

## 3.6 AMSI統合を使用したスクリプトベース攻撃を特定する

マルウェア対策スキャンインターフェース AMSI は、組み込まれているスクリプトサービスに対する詳細なスキャンを可能にするMicrosoft Windowsのコンポーネントです。

**注：** AMSI統合は、 Windows Server 2016および2019でのみ使用できます。

高度なマルウェアは、従来のスキャン方法を回避するために、偽装または暗号化されたスクリプトを使用します。このようなマルウェアは多くの場合、メモリに直接読み込まれるため、デバイス上のファイルを使用しません。

AMSIは、Windows上で動作しているアプリケーションやサービスが、コンピュータにインストールされているマルウェア対策製品にスキャン要求を送信するために使用できるインターフェースです。これにより、PowerShellやOffice365などのWindowsのコアコンポーネントや他のアプリケーション上でスクリプトやマクロを使用して検出を回避する有害なソフトウェアに対する追加の保護を提供できます。

製品でAMSI統合をオンにするには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで を選択します。
3. **マルウェア保護** > **設定を編集する** を選択します。

   **注：** 設定を変更するには管理者の権限が必要です。

4. [**マルウェア対策スキャンインターフェース AMSI** ] を有効にします。
   本製品は、AMSIが検出した有害な内容を通知し、検出した内容をイベント履歴に記録するようになりました。

第章

4

# Web サイトのアクセスを保護する

**トピック：**



ブラウザ保護は、Web サイトの安全性評価をブラウザに表示し、危険な Web サイトのアクセスをブロックすることでブラウザの Web アクセスを保護します。

## 4.1 危険な Web サイトをブロックする

ブラウザ保護は有効時に危険な Web サイトのアクセスをブロックします。

ブラウザ保護が有効であることを確認するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで を選択します。
3. [**セキュア ブラウジング**] を選択します。
4. [**設定を編集する**] を選択します。

   **注：** 設定を変更するには管理者の権限が必要です。
5. [**ブラウザ保護**] を有効にします。
6. ブラウザが開いている場合、変更を適用するためにブラウザを再起動してください。

**注：** ブラウザ保護は、使用するWebブラウザでブラウザ保護の拡張機能がオンになっている必要があります。

### 4.1.1 不審な・禁止されている Web サイトをブロックする

ブラウザ保護は信用できないまたは禁止コンテンツが含まれているWebサイトに対する意図していないアクセスを阻止できます。

ときには不審・侵害・不正なコンテンツを含むWebサイトにアクセスすることがあります。偽装されている Web サイト、スパム サイト、望ましくないプログラムが含まれている可能性のあるサイト、地域に関係なく不正・不法なコンテンツを含むサイトなどがあります。

ブラウザ保護を使用すると、このようなWebサイトに対する無意識なアクセスを防ぐことができます。

1. 製品を Windows **Start** メニューから開きます。
2. メインページで を選択します。
3. [**セキュア ブラウジング**] を選択します。
4. [**設定を編集する**] を選択します。

   **注：** 設定を変更するには管理者の権限が必要です。
5. 「**ブラウザ保護**」が有効であることを確認します。
6. 「不審」および「危険」として評価されたWebサイトをブロックする場合、[**不審なWebサイトをブロック**] を選択します。
7. 禁止コンテンツを含む Web サイトをブロックする場合、[**禁止されている Web サイトをブロック**] を選択します。
8. ブラウザが開いている場合、変更を適用するためにブラウザを再起動してください。

**注：** ブラウザ保護は、使用するWebブラウザでブラウザ保護の拡張機能がオンになっている必要があります。

### 4.1.2 評価アイコンを使用する

ブラウザ保護で Google、Bing、YahooまたはDuckDuckGoを使用すると、検索結果ページに Web サイトの安全性評価が表示されます。

サイトに関する評価は色つきで表示されます。検索エンジンの検索結果に関する評価も同じようなアイコンで表示されます。アイコンは次のように分けられています。

| | |
|---|---|
|  | サイトが安全である (F-Secure の分かる範囲で) ことを示します。Web サイトに不審なコンテンツは検出されていません。 |
|  | サイトに不審なコンテンツがあることを示し、アクセスする際には注意が必要です。サイトでのファイル ダウンロードや個人情報の提供を避けてください。 |
|  | サイトが危険であることを示します。サイトのアクセスを避けることを推奨します。 |
|  | 分析されていないページで、情報が不明であることを示します。 |
|  | 管理者が Web サイトのアクセスを許可しています。 |
|  | 管理者がこのサイトをブロックしています。サイトにアクセスできません。 |

**ヒント：** ファイルまたはURLが誤って検出されたと思われる場合、サンプルをF-Secure Labs https://www.f-secure.com/en/business/support-and-downloads/submit-a-sample に送信できます。複数のURLやIPアドレスをテキストファイルにまとめてファイルとして送信することができます。

検索結果で評価アイコンを表示するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで  を選択します。
3. [**セキュア ブラウジング**] を選択します。
4. [**設定を編集する**] を選択します。

   

   **注：** 設定を変更するには管理者の権限が必要です。
5. 「**ブラウザ保護**」が有効であることを確認します。
6. [**検索エンジンの結果に評価を表示する**] を選択します。
7. ブラウザが開いている場合、変更を適用するためにブラウザを再起動してください。

**注：** ブラウザ保護は、使用するWebブラウザでブラウザ保護の拡張機能がオンになっている必要があります。

### 4.1.3 Web サイトがブロックされた場合

「危険」として評価されている Web サイトにアクセスすると、ブラウザ保護のブロック ページが表示されます。

ブラウザ保護のブロック ページが表示した場合

1. Web サイトにアクセスする場合、[**Web サイトを許可する**] をクリックしてください。
   Windows *ユーザー アカウント制御* (UAC) が操作の確認を尋ねます。
2. 必要に応じて管理者アカウントの情報を入力し、変更を確認します。

ブロックしたサイトが安全と思われる、[**Web サイトを通知**] をクリックします。Web サイトの分析を依頼するために必要な情報を入力するページが開きます。ページが開かない場合は、ここからサイトの分析を送信してください。

**注：** ブロックページが表示されない場合は、使用しているWebブラウザでブラウザ保護の拡張機能がオンになっていることを確認してください。

### 4.1.4 Web サイトの例外

Web サイトの例外リストには許可またはブロックしている Web サイトが表示されます。

**注：** 管理者が特定の Web サイトをブロックした場合、あるいは禁止コンテンツを含む Web サイトの場合、**許可した**リストに追加されていてもそのサイトに対するアクセスはブロックされます。

Web サイトの例外を表示・変更するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで を選択します。
3. **セキュア ブラウジング** > **設定を編集する** を選択します。
4. [**Web サイトの例外を表示する**] を選択します。

   許可/拒否された Web サイト リストにある Web サイトを許可/ブロックするには

   a) 編集したい Web サイトが含まれているタブ ([**許可**] また [**拒否**] ) を選択します。
   b) Web サイトを右クリックして、[**許可**] または [**拒否**] を選択します。

   Web サイトが許可/拒否された Web サイト リストに含まれていない場合

   a) Web サイトを許可する場合、「**許可**」タブを選択します。Web サイトをブロックする場合、「**拒否**」タブをクリックします。
   b) [**追加**] を選択すると Web サイトがリストに追加されます。
   c) 追加する Web ページのアドレスを入力して [**OK**] を選択します。
   d) 「**Web サイトの例外**」ウィンドウで [**閉じる**] を選択します。
5. [**OK**] を選択するメインページに戻ります。

許可/ブロックした Web サイトを右クリックして [**編集**] を選択すると、Web サイトのアドレスを変更できます。

許可/ブロックしたWebサイトを選択して[**削除**]を選択すると、Webサイトをリストから削除できます。

## 4.2 機密性のあるデータを保護する

「*接続制御*」は、機密性のある取引をハッカーからブロックしてセキュリティを強化します。たとえば、銀行サイトのアクセスやオンラインの取引を行うときにシステムを保護します。

*接続制御*はインターネットの銀行Webサイトに対するセキュアな接続を自動的を検出して、意図していないサイトのアクセスに対する接続をブロックします。銀行のWebサイトをアクセスする時には、安全とみなされる接続は許可されます。

取引を完了するためにブロックされている Web サイトのアクセスが必要な場合、ブロックした Web サイトのアクセスを一時的に許可することができます。また、*接続制御*のセッションを終了してWebサイトにアクセスすることもできます。

*接続制御*は次のブラウザに対応しています。

- Internet Explorer 9 以降
- Microsoft Edge (Chromium)

- Firefox
- Google Chrome

### 4.2.1 接続制御を有効にする

*接続制御*を有効にすると、セキュリティが強化されます。

*接続制御*は有効時に安全ではない接続をブロックします。たとえば、銀行のWebサイトのアクセス時またはオンライン決済を行う際に*接続制御*は有効になり、オンラインバンキングに不要な接続はすべてブロックされることで機密性のある取引は保護されます。

*接続制御*を有効にするには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで を選択します。
3. **セキュア ブラウジング** > **設定を編集する** を選択します。
4. [**接続制御**] を有効にします。
5. 有効なインターネット接続を閉じたくない場合、[**有効なインターネット接続を中断しない**] を選択します。

   この設定を選択しない場合、*接続制御*は有効時にアクティブなインターネット接続をすべて閉じます。
6. クリップボードにコピーされたデータを*接続制御*でどのように処理するか選択します。

   デフォルトでは、*接続制御*は、プライバシーを保護するために*接続制御*のセッションが終了したときにクリップボードからすべてのデータを消去します。

   クリップボードを消去したくない場合、[**クリップボードを消去しない**] を選択します。

### 4.2.2 接続制御を使用する

*接続制御*を有効にすると、銀行サイトのアクセスが自動的に検出されます。

オンライン バンキングの Web サイトを開くと、「*接続制御*」の通知が画面の上に表示されます。バンキング保護のセッションが開いている時には他の接続はブロックされます。

**ヒント:** *接続制御*の有効時に他の接続を中断したくない場合、設定の変更を防ぐために、**続制御**インジケーターを選択し、接続制御通知の右上隅にある を選択します。

*接続制御*のセッションを終了して他の接続を復元するには

1. 画面上部の [**接続制御**] インジケーターをクリックします。
2. 通知の [**終了**] をクリックします。

## 4.3 ブラウザの拡張機能が使用中であることを確認する

ブラウザ保護は、ブラウザ拡張機能を使用して、暗号化されたブラウジングを保護し、インターネットのブラウジング中にセキュリティ情報を表示します。

製品の「**アンチウイルス**」画面ではデフォルトブラウザで拡張機能(プラグイン)が有効になっているか表示されます。

**ヒント:** Firefox、Chrome、Microsoft Edge の場合、「**アンチウイルス**」ページで [**今すぐ設定**] をクリックして、ブラウザで拡張機能を有効にするためのページを開くことができます。

製品にブラウザの拡張機能がインストールされていない、または無効になっているという警告が表示された場合

1. ブラウザを開いて、ブラウザの拡張機能が有効になっているか確認します。

   Firefox の場合

   a) メニューから [**アドオン**] を選択し、[**拡張機能**] をクリックします。
   b) そこにブラウザ保護の拡張機能/プラグインが表示されている場合、その横にある[**有効**]をクリックします

   Chrome の場合

   a) メニューから **その他のツール** > **拡張機能**の順に選択します。
   b) ブラウザ保護の拡張機能のトグル スイッチをクリックして有効にします。

   Microsoft Edge の場合

   a) メニューから [**拡張機能**] を選択します。
   b) ブラウザ保護の拡張機能のトグル スイッチをクリックして有効にします。

   👉 **注：** Microsoft Edge では、ブラウザ保護の拡張機能を使用するために他の Web ストアの拡張機能がを許可する必要があります。

   Internet Explorer の場合

   a) **ツール** > **アドオンの管理**を選択します。
   b) 拡張機能の選択し、[**有効**] をクリックします。

2. 拡張機能がブラウザに表示されていない場合、手動で拡張機能を再インストールする必要があります。

   👉 **注：** 設定を変更するには管理者の権限が必要です。

   a) 製品を Windows **Start** メニューから開きます。
   b) メインページで ⚙ を選択します。
   c) [**セキュア ブラウジング**] を選択します。

      Firefoxを使用している場合、[**拡張機能**] で[**Firefoxの拡張機能をインストール**]をクリックします。

      Chrome または Microsoft Edge を使用している場合、**[拡張機能**] で [**Chrome Web ストアを開く**] をクリックしてブラウザ保護の拡張機能ページにアクセスし、[**Chromeに追加**] をクリックします。

3. ブラウザで次のテスト ページを開き、拡張機能が有効になっていることを確認します: https://unsafe.fstestdomain.com。
   製品のブロック ページが開く場合、ブラウザの拡張機能は有効です。

# 第 5 章

# 検索エンジンのフィルタを使用する

検索エンジンサーチ フィルタを使用して検索結果から不適切なコンテンツをブロックできます。

検索エンジンのフィルタは Google、Yahoo、Bing のセーフモードを有効にし、Google、Yahoo、Bing、YouTube のセーフサーチ フィルタリング レベルを「強」にすることで成人向けのコンテンツを表示しないようにします。すべての不適切なコンテンツが検索エンジンで表示されないにできませんが、ほとんどのコンテンツはブロックできます。

検索エンジンのフィルタを有効にするには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで を選択します。
3. [**Web コンテンツ制御**] を選択します。
4. [**検索結果のフィルタ**] を有効にします。

検索エンジンのフィルタを有効にすると、ログインしている Windows ユーザ アカウントに対してセーフサーチの Web サイト設定が無効になります。

# 第 章
# 6

## 自動タスクを表示する

管理者は、スケジュールタスクを設定して、コンピュータを自動的にスキャンし、適用されていない更新プログラムをチェックし、セキュリティ更新プログラムをインストールすることができます。

コンピュータに影響を与える自動タスクの詳細を確認するには、以下の手順に従います。

1. 製品を Windows **Start** メニューから開きます。
2. メインページで を選択します。
3. [**自動タスク**] を選択します。

このページには、管理者が各タスクに設定した説明とスケジュールが表示されます。また、各タスクが最後に実行された日時と次回の実行予定日時も表示されます。

次の表は、タスクに対して表示されるスケジュールの例をいくつか示しています。

| スケジュール | 説明 |
|---|---|
| @daily | タスクは毎日ランダムな時間に実行されます。 |
| @weekdays | タスクは平日の毎日のランダムな時間に実行されます。 |
| @weekly | タスクは毎週特定の日のランダムな時間に実行されます。 |
| @monthly | タスクは毎月特定の日のランダムな時間に実行されます。 |

| スケジュール | 説明 |
| --- | --- |
| * * 12 ? 5 | タスクは、指定されたCRON式に応じて実行されます。この例では、毎週土曜日の12:00から13:00の間のランダムな時間に実行されます。<br><br>CRON式は、以下の一般的な形式に従ってスペースで区切られた6つのフィールドで構成される文字列です。<br><br><seconds> <minutes> <hours> <days of the month> <months> <days of the week><br><br>各フィールドは通常、数値または特殊文字を含み、たとえばランダム化された値を示すことができます。 |

# 第 章
# 7

## ファイアウォールについて

**トピック：**



*ファイアウォール*は、インターネットを通じて侵入者と危険なアプリケーションがコンピュータに入ってくることを阻止します。

ファイアウォールは、コンピュータが安全なインターネット接続のみ許可し、不正な侵入者がインターネットからコンピュータにをアクセスすることを阻止します。

## 7.1 Windows ファイアウォールの設定を変更するには

ファイアウォールを有効にすると、コンピュータのアクセスが制限されます。

本製品は、Windows ファイアウォールを使用してコンピュータを保護します。

Windows ファイアウォールの設定を変更するには

1. 製品を Windows **Start** メニューから開きます。
2. メイン ビューで、[**ウイルスと脅威**] を選択します。
3. [**Windows Firewall の設定**] を選択します。

Windows Firewall の詳細について、Microsoft Windows の説明書を参照してください。

## 7.2 パーソナル ファイアウォールを使用する

本製品はWindows Firewall と動作します。他のパーソナルファイアウォールを使用する場合、追加の設定が必要です。

本製品はファイアウォールの基本的な機能の面(着信ネットワークトラフィックの制御、内部ネットワークとインターネットの区別など) で Windows Firewall を使用します。ディープガードはインストールされているアプリケーションの監視、および不審なアプリケーションに対する無断アクセスの阻止を行います。

Windows Firewall の代わりにパーソナル ファイアウォールを使用している場合、F-Secure の全プロセスに対する着信および発信ネットワーク トラフィック許可されていることを確認してください。



**ヒント :** パーソナル ファイアウォールが手動のフィルタ モードを搭載している場合、F-Secure の全プロセスを許可するように設定してください。

第章

8

# 自動更新について

**トピック：**



自動更新はコンピュータを最新の脅威から守ります。

本製品は、コンピュータがインターネットに接続している際に最新の更新をダウンロードします。回線が遅いネットワークでも、インターネット回線の帯域を圧迫することなく最新の更新を受信することが可能です。

## 8.1 最新のアップデートを表示する

更新を最後に受信した日付と時間を確認できます。

自動更新が有効の場合、本製品はコンピュータがインターネットに接続しているときに最新の更新をダウンロードします。

インストールされている製品に関する最新のアップデートを確認するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで を選択します。
3. [**アップデート**] を選択します。
4. [**接続**] で最新のアップデートに関する情報が表示されます。
5. [アップデート] で [**今すぐ更新**] を選択すると、最新のアップデートを手動で確認できます。
   アップデートを利用できる場合、製品が最新のアップデートを自動的にインストールします。

   **注：** アップデートの確認を行うにはインターネットの接続が必要です。

## 8.2 接続設定を変更する

ここでは、コンピュータがインターネットに接続する方法を指定し、モバイルネットワークを使用しているときのアップデート処理方法について説明します。

インターネット サービス プロバイダはプロキシの使用を提供することや要求することがあります。プロキシは、コンピュータとインターネットの間の仲介役として機能します。インターネットへのすべての要求を遮断して、キャッシュを使用して要求を満たすことができるか確認します。プロキシは、セキュリティの向上、パフォーマンスの向上、要求のフィルタリング、およびインターネットに対するコンピュータの匿名化に使用されます。

1. 製品を Windows **Start** メニューから開きます。
2. メインページで を選択します。
3. **アップデート** > **設定を編集** を選択します。

   **注：** 設定を変更するには管理者の権限が必要です。

4. [**手動プロキシの設定**] でコンピュータがプロキシ サーバを使用してインターネットに接続するか選択します。
   - コンピュータがインターネットに直接接続している場合、[**使用しない**] を選択します。
   - [**ブラウザの設定を使用**] を選択したら Web ブラウザの HTTP プロキシ設定が適用されます
   - [**カスタム アドレス**] を選択し、HTTP プロキシを手動で設定するためにプロキシ アドレスと [**ポート**] 番号をを追加します。

第章
9

# プライバシー

**トピック：**



ここでは、Security Cloud と匿名データの提供方法および製品の改善に貢献できる方法について説明します。

## 9.1 Security Cloud

Security Cloud (旧「ディープガード ネットワーク」) は、未知のアプリケーションや Web サイト、悪意のあるアプリケーションや Web サイトのエクスプロイト (悪用) に関するセキュリティ データを収集します。

当社はユーザが購入したライセンスの対象となるセキュリティ サービスおよび当社の他のサービスを改善するためにセキュリティ データを収集します。収集されるセキュリティ データには不明なファイル、不審なデバイスの動作、アクセスした URL が含まれます。このデータは当社のサービスが動作するために不可欠です。このように収集されたオブジェクトは、限られた時間のみ保持され、一定の期間が過ぎた時点で削除されます。

Security Cloud は、Web の行動 (アクセスしたサイトなど) を記録しません。また、すでに分析された Web サイトおよびコンピュータにインストールされている安全なアプリケーションに関する情報を収集しません。セキュリティ データは個人を対象とした広告の目的には使用されません。

データを提供する

Security Cloud にセキュリティ データを提供すると、最新の脅威に対する保護が強化されます。このように収集されたオブジェクトは、限られた時間のみ保持され、一定の期間が過ぎた時点で削除されます。

1. 製品を Windows **Start** メニューから開きます。
2. メインページで ⚙ を選択します。
3. [**プライバシー**] 設定ページに移動します。
4. [**設定を編集する**] を選択します。

   **注:** 設定を変更するには管理者の権限が必要です。
5. [**Security Cloud**] で [**詳細分析を許可する**] を選択します。

   **注:** F-Secure の個人情報保護方針はここからご覧になれます:
   http://download.sp.f-secure.com/eula/latest/security_cloud_jpn.html

## 9.2 製品の改善

F-Secure に使用データをご提供いただくと、製品の改善に貢献にすることになります。

使用データを提供するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで ⚙ を選択します。
3. [**プライバシー**] 設定ページに移動します。
4. [**設定を編集する**] を選択します。

   **注:** 設定を変更するには管理者の権限が必要です。
5. [**製品の改善**] で [**個人データ以外のデータを提供する**] を選択します。

   **注:** F-Secure の個人情報保護方針はここからご覧になれます:
   http://download.sp.f-secure.com/eula/latest/privacy_jpn.html

第 章
10

# テクニカル サポート

**トピック：**



ここでは、技術的な問題を解決するための情報を見つけられます。

## 10.1 アカウント ID はどこで確認できますか?

サポートにお問い合わせする場合、ID コードが必要になることがあります。

ID コードを表示するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで ⚙ を選択します。
3. [**サポート**] を選択します。
4. [**識別コード**] で [**アカウント ID**] を見つけます。

## 10.2 製品のバージョン情報を確認するにはどうすれば良いですか?

サポートにお問い合わせする場合、製品のバージョンが必要になることがあります。

製品のバージョン情報を確認するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで ⚙ を選択します。
3. [**サポート**] を選択します。
4. [**バージョン情報**] でインストールされている製品に関する情報を確認できます。

## 10.3 サポート ツールを使用する

サポートにお問い合わせする前に、サポート ツールを実行してハードウェア、OS、ネットワークの構成およびインストールされているソフトウェアに関する基本的な情報を収集してください。

サポート ツールを使用するには

1. 製品を Windows **Start** メニューから開きます。
2. メインページで ⚙ を選択します。
3. [**サポート**] を選択します。
4. [**設定を編集する**] を選択します。

   **注:** 設定を変更するには管理者の権限が必要です。
5. [**サポートツールを実行する**] を選択します。
6. 「**サポート ツール**」ウィンドウで [**診断ツールを実行**] を選択します。
   サポート ツールが起動し、データ収集の進捗を示すウィンドウが表示されます。

ツールの実行が終了すると、収集したデータがデスクトップ上のアーカイブに保存されます。収集したデータ 診断ファイル は、https://www.f-secure.com/en/business/support-and-downloads/support-request で提出できます。

**注:** 管理者は、サポート ツールの診断をリモートで要求できます。製品がこの通知を表示し、ユーザに要求を [**許可**] または [**拒否**] するように求めます。