

**WithSecure Server Security**

# 目次

<b>第 1 章：製品を使用するには</b> .....	<b>4</b>
1.1 免責事項.....	5
1.2 システム要件.....	5
1.3 製品の設定を変更する.....	6
1.3.1 製品の設定のクイック アクセス.....	7
1.3.2 すべてのセキュリティ機能を無効にする.....	7
1.4 統計情報を確認する.....	8
1.4.1 セキュリティのステータス アイコン.....	8
1.4.2 最近のイベントを表示する.....	9
<b>第 2 章：コンピュータを危険なコンテンツから保護する</b> .....	<b>10</b>
2.1 危険なコンテンツについて.....	11
2.1.1 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.....	11
2.1.2 ワーム.....	11
2.1.3 トロイの木馬.....	12
2.1.4 バックドア.....	13
2.1.5 エクスプロイト.....	13
2.1.6 エクスプロイトキット.....	14
2.2 コンピュータをスキャンする.....	14
2.2.1 リアルタイムスキャンの仕組み.....	14
2.2.2 ファイルを手動でスキャンする.....	15
2.2.3 スケジュール スキャン.....	17
2.3 デープガード.....	17
2.3.1 デ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.....	18
2.3.2 データガードを使用する.....	18
2.3.3 保護するフォルダを追加/削除する.....	19
2.4 データガードアクセス制御の使用.....	20
2.4.1 隔離保存したアイテムを表示する.....	20
2.4.2 隔離保存したアイテムを復元する.....	20
2.4.3 ファイルまたはフォルダをスキャンから除外する.....	21
2.4.4 除外したアプリケーションを表示する.....	21
2.4.5 保護するフォルダを追加/削除する.....	22
2.5 危険なファイルのダウンロードを阻止する.....	22
2.6 AMSI統合を使用したスクリプトベース攻撃を特定する.....	22
<b>第 3 章：Web サイトのアクセスを保護する</b> .....	<b>24</b>
3.1 危険な Web サイトをブロックする.....	25
3.1.1 不審な・禁止されている Web サイトをブロックする.....	25
3.1.2 評価アイコンを使用する.....	25

3.1.3 Web サイトがブロックされた場合.....	26
3.1.4 Web サイトの例外.....	26
3.2 GPOを介したブラウザ保護拡張機能を展開する.....	27
3.2.1 Google ChromeにWithSecureブラウザ保護拡張機能をインストールする方法.....	27
3.2.2 Microsoft Edge ( Chromium ) にWithSecureブラウザ保護拡張機能をインストールする方法.....	28
3.2.3 Mozilla FirefoxにWithSecureブラウザ保護拡張機能をインストールする方法.....	29
3.3 ブラウザの拡張機能が使用中であることを確認する.....	29
<b>第 4 章 : 機密性のあるデータを保護する.....</b>	<b>31</b>
4.1 接続制御を有効にする.....	32
4.2 接続制御を使用する.....	32
<b>第 5 章 : コンテンツ制御を設定する.....</b>	<b>33</b>
5.1 Web コンテンツをブロックする.....	34
5.1.1 コンテンツカテゴリ.....	34
<b>第 6 章 : 検索エンジンのフィルタを使用する.....</b>	<b>36</b>
6.1 検索エンジンのフィルタをオンにする.....	37
<b>第 7 章 : 集中管理.....</b>	<b>38</b>
7.1 Windows イベント ビューワを開く.....	39
<b>第 8 章 : ファイアウォールについて.....</b>	<b>40</b>
8.1 Windows ファイアウォールの設定を変更するには.....	41
8.2 パーソナル ファイアウォールを使用する.....	41
<b>第 9 章 : プログラムを最新の状態にする.....</b>	<b>42</b>
<b>第 10 章 : アップデートの使用方法.....</b>	<b>44</b>
10.1 最新のアップデートを表示する.....	45
10.2 隔離された Server Security ホストでのマルウェア定義の更新.....	45
10.3 接続設定を変更する.....	46
<b>第 11 章 : プライバシー.....</b>	<b>47</b>
11.1 セキュリティデータ.....	48
11.2 製品の改善.....	48
<b>第 12 章 : テクニカル サポート.....</b>	<b>49</b>
12.1 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?.....	50
12.2 サポート ツールを使用する.....	50
12.3 製品の問題をデバッグする.....	50
12.4 電話詐欺と標的にされていると思われる場合の対処方法.....	51

## 製品を使用するには

---

トピック：

- [免責事項](#)
- [システム要件](#)
- [製品の設定を変更する](#)
- [統計情報を確認する](#)

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

## 1.1 免責事項

---

F-Secure ビジネスは、新しいロゴと名前の形に反映された WithSecure™ になりました。

現在、製品のブランド変更を進めています。この期間中、すべての変更が完了するまで、製品とポータルに F-Secure と WithSecure™ が混在して表示される場合があります。

## 1.2 システム要件

---

ここでは、WithSecure Server Securityに関する重要な情報が含まれています。

製品を使用する前に、ドキュメント全体を読むことを強くお勧めします。

### サポートされているOS

注: WithSecure、ベンダーが現在サポートしているオペレーティングシステムのみをサポートします。WithSecureのオペレーティングシステムサポートポリシーの詳細については、「[製品のアップデートとサポート対象バージョン](#)」をご覧ください。ベンダーがサポートを終了したプラットフォームの長期サポートにご興味がある場合は、営業担当者にお問い合わせください。

本製品は次の OS を搭載しているコンピュータにインストールできます。

- Microsoft® Windows Server 2016 Standard
- Microsoft® Windows Server 2016 Essentials
- Microsoft® Windows Server 2016 Datacenter
- Microsoft® Windows Server 2016 Core
- Microsoft® Windows Server 2019 Standard
- Microsoft® Windows Server 2019 Datacenter
- Microsoft® Windows Server 2019 Core
- Microsoft® Windows Server 2022 Standard
- Microsoft® Windows Server 2022 Datacenter
- Microsoft® Windows Server 2022 Core
- Microsoft® Windows Server 2025 Standard
- Microsoft® Windows Server 2025 Datacenter
- Microsoft® Windows Server 2025 Core

注: Windows Server 2016 Nano は対応されていません。

注: ARMはサポートされていません。

以下を除く Microsoft Windows Server editions。

- Itanium プロセッサ向け Windows Server
- Windows HPC editions (特定なハードウェアを対象)
- Windows MultiPoint Server
- Windows Home Server

注: すべてのオペレーティングシステムに最新のサービスパックがインストールされている必要があります。また、OSがMicrosoft Azure Code Signing証明書をサポートしている必要があります。詳細は[こちら](#)をご覧ください。

注: パフォーマンスとセキュリティの理由で本製品は NTFS パーティションにのみインストールできません。

### 対応ターミナル サーバ

WithSecure Server Securityは、次のターミナルサーバプラットフォームをサポートしています。

- Microsoft Windows Terminal/RDP サーバ (上記の Windows Server プラットフォーム上で)
- Citrix® XenApp 5.0
- Citrix® XenApp 6.0
- Citrix® XenApp 6.5

- Citrix®XenApp7.5、7.6、7.14、7.15
- Citrix® Virtual Apps and Desktops 2009

#### ハードウェアおよびシステム要件

製品をインストールする前に、この情報を確認し、ネットワーク、ハードウェア、ソフトウェア、およびその他のシステムコンポーネントが要件を満たしていることを確認することをお勧めします。

注: 同一システム上で複数のサービスを実行する場合、最小限のハードウェア要件では不十分な場合があります。

WithSecure Server Securityをインストールするには、次の最小ハードウェアおよびシステム要件が推奨されます。

- サポートされているOSの要件を満たす任意のコンピュータ。
- 10GB以上のディスク容量を推奨します。
- アップデートの受信やクラウドベースの検出を利用するためには、インターネットへの接続が必要です。
- このServer Securityバージョンをインストールするには、WindowsユニバーサルCランタイム ( <https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows> ) が必要です。

#### セットアップと構成

##### インストール手順:

製品のインストール用JARパッケージをPolicy Manager Consoleにインポートして、選択したホストにリモートで製品を展開します。Policy Manager Consoleでは、製品をインストールするために他の中央管理システム経由で展開できるMSIパッケージをエクスポートすることもできます。

ローカルでインストールを実行するには、WithSecure Policy Manager Consoleのエクスポートツールを使用してMSIパッケージを作成する必要があります。

注: ローカルインストールには、ローカル管理者権限が必要です。

##### 対応言語

サポートされている言語は次のとおりです。英語、中国語(中国、台湾、香港)、チェコ語、デンマーク語、オランダ語、エストニア語、フィンランド語、フランス語、カナダフランス語、ドイツ語、ギリシャ語、ハンガリー語、イタリア語、日本語、韓国語、ノルウェー語、ポーランド語、ポルトガル語、ブラジルポルトガル語、ルーマニア語、ロシア語、スロベニア語、スペイン語、ラテンアメリカスペイン語、スウェーデン語、およびトルコ語。

## 1.3 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: 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 ( 15ページ )

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。

##### データガードアクセス制御の使用 ( 20ページ )

データガードアクセス制御は、不明なアプリケーションがフォルダにアクセスするのを防ぐことで、フォルダをランサムウェア(暗号化による恐喝)から保護します。

##### Windows ファイアウォールの設定を変更するには ( 41ページ )

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 ( 9ページ )

「[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](#) (7ページ)

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。

### 1.3.1 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

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。

1. Windowsの **Start** メニューから [WithSecure Server Security] を開きます。
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
<a href="#">現在のステータスを表示</a>	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。
<a href="#">更新を確認する</a>	最新のアップデートを確認・ダウンロードします。
<a href="#">最近のイベントを表示</a>	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。
<a href="#">設定を開く</a>	製品の設定を開きます。
<a href="#">本製品について</a>	製品のバージョン情報を表示します。

### 1.3.2 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できないように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. Windowsの **Start** メニューから [WithSecure Server Security] を開きます。
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。

## 1.4 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。

### 1.4.1 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。 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。 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。 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。
	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。 対応がすぐに必要で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。 対応が必要な操作 (レピュテーションベースのブラウジング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。 製品を更新しています。

## セキュリティステータスのトレイアイコン

製品に注意やアクションが必要な場合、次の保護ステータスアイコンがシステムトレイに表示されます。


ステータストレイアイコン	ステータス	説明
	注意	コンピュータが保護されていません。  この製品には注意が必要です。たとえば、1つ以上のセキュリティ機能がオフになっているか、アップデートが非常に古いです。
	警告	コンピュータは保護されていません。  サブスクリプションの有効期限が切れているか、重要な機能が故障しているなど、製品には即時の対応が必要です。

### 1.4.2 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. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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

## 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:

- 危険なコンテンツについて
- コンピュータをスキャンする
- ディープガード
- データガードアクセス制御の使用
- 危険なファイルのダウンロードを阻止する
- AMSI統合を使用したスクリプトベース攻撃を特定する

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ーを保護します。

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。

## 2.1 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。

### 2.1.1 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WithSecure製品を設定できます。ブロックされたファイルの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](#) ( 15ページ )

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](#) ( 15ページ )

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。

[データガードアクセス制御の使用](#) ( 20ページ )

データガードアクセス制御は、不明なアプリケーションがフォルダにアクセスするのを防ぐことで、フォルダをランサムウェア (暗号化による恐喝) から保護します。

### 2.1.2 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 \( 15ページ \)](#)

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 \( 15ページ \)](#)

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。

[データガードアクセス制御の使用 \( 20ページ \)](#)

データガードアクセス制御は、不明なアプリケーションがフォルダにアクセスするのを防ぐことで、フォルダをランサムウェア (暗号化による恐喝) から保護します。

## 2.1.3 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思わせ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が、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「罨」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。ユーザがこれらの罨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 \( 15ページ \)](#)

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 \( 15ページ \)](#)

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。

[データガードアクセス制御の使用 \( 20ページ \)](#)

データガードアクセス制御は、不明なアプリケーションがフォルダにアクセスするのを防ぐことで、フォルダをランサムウェア (暗号化による恐喝) から保護します。

## 2.1.4 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 \( 15ページ \)](#)

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 \( 15ページ \)](#)

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。

[データガードアクセス制御の使用 \( 20ページ \)](#)

データガードアクセス制御は、不明なアプリケーションがフォルダにアクセスするのを防ぐことで、フォルダをランサムウェア (暗号化による恐喝) から保護します。

## 2.1.5 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 \( 15ページ \)](#)

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 \( 15ページ \)](#)

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。

[データガードアクセス制御の使用 \(20ページ\)](#)

データガードアクセス制御は、不明なアプリケーションがフォルダにアクセスするのを防ぐことで、フォルダをランサムウェア(暗号化による恐喝)から保護します。

## 2.1.6 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 \(15ページ\)](#)

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 \(15ページ\)](#)

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。

[データガードアクセス制御の使用 \(20ページ\)](#)

データガードアクセス制御は、不明なアプリケーションがフォルダにアクセスするのを防ぐことで、フォルダをランサムウェア(暗号化による恐喝)から保護します。

## 2.2 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。

### 2.2.1 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にアクセスすると、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. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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。

## 2.2.2 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. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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) [**圧縮ファイルのスキャン**] 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。
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。

注：Windows 11 では、[\[他のオプションを表示\]](#) を選択し、[\[マルウェアスキャン\]](#) 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。

## 2.2.3 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行うようになります。

スケジュール スキャンを設定するには

1. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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。
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。

## 2.3 デープガード

デープガードは、未知の脅威に対するプロアクティブで即時の保護を提供します。

デープガードは、アプリケーションを監視し、システムに対する潜在的に有害な変更をリアルタイムで検出し、停止させます。これにより、安全なアプリケーションのみを使用することができます。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: WithSecure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](#)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

デープガードが有効であることを確認するには

1. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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。

注：ディープガードのすべてのルールは、すべてのユーザに表示されます。ルールには、個人情報を含むファイル名とフォルダ名が含まれることがあります。そのため、同じコンピュータの他のユーザは、ディープガードのルールに含まれるパスとファイル名を見ることができることに注意してください。

関連タスク

[セキュリティデータ](#) (48ページ)


このサービスは、潜在的な悪意のあるアクティビティまたは保護されたデバイスに関するクエリを WithSecure **Security Cloud** に送信します。

### 2.3.1 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. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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**」ビューが開きます。

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。

### 2.3.2 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. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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 \(19ページ\)](#)

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。

### 2.3.3 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. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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」ビューが開きます。

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が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ります。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。

## 2.4 データガードアクセス制御の使用

データガードアクセス制御は、不明なアプリケーションがフォルダにアクセスするのを防ぐことで、フォルダをランサムウェア (暗号化による恐喝) から保護します。

注: 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。

[データガードアクセス制御] をオンにするには

1. Windowsの **Start** メニューから [WithSecure Server Security] を開きます。
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. [データガードアクセス制御] をオンにします。

### 2.4.1 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. Windowsの **Start** メニューから [WithSecure Server Security] を開きます。
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」ビューが開きます。


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。

### 2.4.2 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. Windowsの **Start** メニューから [WithSecure Server Security] を開きます。
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」ビューが開きます。

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。

### 2.4.3 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. Windowsの **Start** メニューから [WithSecure Server Security] を開きます。
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」ビューが開きます。

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。

### 2.4.4 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。

また、DeepGuardは特定のSteamゲームをブロックしません。したがって、Steamゲームをスキャンから除外したり、DeepGuardをオフにして実行したりする必要はありません。

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. Windowsの **Start** メニューから [WithSecure Server Security] を開きます。
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」ビューが開きます。
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。

## 2.4.5 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. Windowsの **Start** メニューから [WithSecure Server Security] を開きます。
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」ビューが開きます。

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が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ります。そのため、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。

## 2.5 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. Windowsの **Start** メニューから [WithSecure Server Security] を開きます。
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。

## 2.6 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、2019および2022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. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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。

## Web サイトのアクセスを保護する

---

トピック:

- 危険な Web サイトをブロックする
- GPOを介したブラウザ保護拡張機能を展開する
- 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、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。

## 3.1 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. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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。

### 3.1.1 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. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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。

### 3.1.2 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 (WithSecure 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。

-  このサイトは有害です。このサイトにアクセスしないことをお勧めします。または、管理者がこのサイトをブロックしているため、アクセスすることができません。
-  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。
-  Web サイトのアクセスがブロックされなくなります。

検索結果で評価アイコンを表示するには

1. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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。

### 3.1.3 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、[このコンピューターでWebサイトを許可する] を選択します。ブロックされたWebサイトを許可するには、管理者権限が必要です。  
[許可されたWebサイトの追加] ウィンドウが開き、許可しようとしているアドレスが表示されます。
2. [OK] を選択します。

ブロックされたWebサイトが開きます。また、Webサイトを許可されたWebサイトのリストに追加します。

ブロックされたサイトが安全であり、ブロックされるべきではないと思われる場合は、[ここ](#)からWebサイトの分析を依頼できます。


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。

### 3.1.4 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. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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] または [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。

## 3.2 GPOを介したブラウザ保護拡張機能を展開する

Google Chrome、Microsoft Edge、および Mozilla Firefox に WithSecure ブラウザ保護拡張機能をインストールする方法について説明します。

注: この手順は Elements Endpoint Protection 固有のものであり、管理者ユーザーを対象としています。

WithSecure ブラウザ保護は、インストールされている WithSecure セキュリティ製品に HTTPS プロトコルのサポートを提供する Web ブラウザーの拡張機能です。

注: HTTP サポートは、拡張機能を使用せずに提供されます。

拡張機能は次のものを有効にします。WithSecure HTTPS 使用時の不要な Web コンテンツ、評価アイコン、および検索エンジンのセーフサーチ モードに対するページ サポートをブロックします。管理者は次のことを行うことができます WithSecure ブラウジング保護をオンにし、Windows グループ ポリシーを使用して強制的にオンにします。

### 3.2.1 Google Chrome に WithSecure ブラウザ保護拡張機能をインストールする方法

これらの手順は、Elements Endpoint Protection に固有のものであり、管理者ユーザーを対象としています。

ブラウザ保護拡張機能をインストールして有効にするには

1. 最新の Google Chrome グループポリシー テンプレート ADMX ファイルをダウンロードします。
2. 次の Chrome 管理テンプレート ファイルと、システムで使用されている言語の言語フォルダーを C:\Windows\PolicyDefinitions ディレクトリにコピーします。  
policy\_templates/windows/admx/chrome.admx and google.admx
3. ファイルと、システムで使用されている言語の言語フォルダーを SYSVOL フォルダーにもコピーします。\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions  
例えば: \\example.com\SYSVOL\example.com\Policies\PolicyDefinitions

注: PolicyDefinitions フォルダーがない場合は、作成する必要があります。

4. Windows グループポリシー管理コンソール ( gpmmc.msc ) を開き、新しいグループポリシーを作成するか、既存のポリシーを編集します。

注: 詳細については、「Windows でグループ ポリシー管理テンプレートの中央ストアを作成および管理する」を参照してください。

5. Computer Configuration/Policies/Administrative Templates/Google/Google Chrome/Extensions/Configure the list of Force-Installed apps and extensions に移動し、次のようにポリシーを編集します。

- a) [有効] を選択してポリシーをオンにします。

b) [オプション] で、[表示] を選択し、次の値を入力します。

```
jmjjnhpacphpjmnlnccpfmhkclaaade
```

```
imdndkajeppdomiimjkcblkafeeooghd
```

注：詳細については、「[Chromeブラウザのポリシーを設定する方法](#)」を参照してください。

グループポリシーがアクティブ化されると、WithSecureブラウザ保護がオンになり、強制的にオンになります。

### 3.2.2 Microsoft Edge ( Chromium ) にWithSecureブラウザ保護拡張機能をインストールする方法

これらの手順は、Elements Endpoint Protectionに固有のものであり、管理者ユーザーを対象としています。

注：WithSecureブラウザ拡張機能は、Microsoftグループポリシーオブジェクト（GPO）を通じてGoogleストアからインストールされます。デバイスはMicrosoft Active Directoryドメインのメンバーである必要があります。そうでない場合、このインストールは実行できません。

ブラウザ保護拡張機能をインストールして有効にするには

1. Microsoft Edgeポリシーファイルを使用して、次の操作を行います。

- a) 「[Microsoft Edge \( Chromium \) グループポリシーテンプレートADMXファイル](#)」に移動します。
- b) ブラウザーとオペレーティングシステムのバージョンとビルドの下で「[Windowsポリシーのダウンロード](#)」を選択し、「[同意してダウンロード](#)」を選択します。
- c) ダウンロードしたcabファイルを解凍します。
- d) 抽出したフォルダーから、次のファイルとフォルダーを \\yourdomainhere\sysvol\yourdomainhere\Policies\PolicyDefinitions\フォルダーと SYSVOL フォルダー ( \\yourdomainhere\sysvol\yourdomainhere\Policies\PolicyDefinitions\ ) の両方にコピーします。
  - Microsoft Edge ( Chromium ) 管理テンプレート ファイル : msedge.admxおよび msedgeupdate.admx
  - システムで使用されている言語の言語フォルダー

注：PolicyDefinitionsフォルダーがない場合は、作成する必要があります。

2. Windowsグループポリシー管理コンソール ( gpmmc.msc ) を開き、次のいずれかを実行します。

注：詳細については、「[WindowsでMicrosoft Edgeポリシー設定を構成する](#)」を参照してください。

- 新しいグループポリシーを作成する
- Computer Configuration/Policies/Administrative Templates/Microsoft Edge/Extensions/Control which extensions are installed silentlyに移動し、次のようにポリシーを編集します。
  - a. [有効] を選択してポリシーをオンにします。
  - b. [オプション] で [表示] を選択し、次の値を入力します。

```
cpikpibllpjmpnchjajlibnmmomnnhnm
```

```
aambijcigikmdoehgjhdepcpieghopdl
```

グループポリシーがアクティブ化されると、WithSecureブラウザ保護がオンになり、強制的にオンになります。

### 3.2.3 Mozilla FirefoxにWithSecureブラウザ保護拡張機能をインストールする方法

これらの手順は、Elements Endpoint Protectionに固有のものであり、管理者ユーザーを対象としています。

ブラウザ保護拡張機能をインストールして有効にするには

1. 最新のMozilla FirefoxグループポリシーテンプレートADMXファイルをダウンロードします。
2. cabファイルを抽出し、次のMozilla Firefox管理テンプレートファイルと、システムで使用されている言語の言語フォルダーをC:\Windows\PolicyDefinitionsディレクトリにコピーします。

windows/mozilla.admx and firefox.admx

3. システムで使用されている言語のファイルと言語フォルダーをSYSVOLフォルダーにもコピーします。\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions\  
例：\\example.com\SYSVOL\example.com\Policies\PolicyDefinitions

注：PolicyDefinitionsフォルダーがない場合は、作成する必要があります。

4. Windowsグループポリシー管理コンソール ( gpmmc.msc ) を開き、新しいグループポリシーを作成するか、既存のポリシーを編集します。
5. Computer Configuration/Policies/Administrative Templates/Mozilla/Firefox/Extensions/Extensions to installに移動し、次のようにポリシーを編集します。
  - a) [有効] を選択し、ポリシーをオンにします。
  - b) [オプション] で、[表示] を選択し、次の値を入力します。

```
https://download.sp.f-secure.com/online-safety/fs_firefox_https.xpi
```

```
https://download.withsecure.com/online-safety/ws_firefox_https.xpi
```

6. Computer Configuration/Policies/Administrative Templates/Mozilla/Firefox/Extensions/Prevent extensions from being disabled or removedに移動し、次のようにポリシーを編集します。
  - a) ポリシーをオンにするには、[有効] を選択します。
  - b) [オプション] で、[表示] を選択し、ols@f-secure.comols\_main@withsecure.comを入力します。

グループポリシーがアクティブ化されると、WithSecure Browsing Protectionがオンになり、強制的にオンになります。

## 3.3 ブラウザの拡張機能が使用中であることを確認する

レピュテーションベースのブラウジングには、Web閲覧、オンラインバンキング、ショッピングを保護し、インターネット閲覧中にセキュリティ情報を表示することができるブラウザ拡張機能が必要です。


コンピュータに製品をインストールすると、製品はブラウザ拡張機能を自動的にインストールしようとします。ブラウザを開くと、新しくインストールされた拡張機能に関する通知が表示されるため、有効にする必要がある場合があります。

WithSecureブラウザ保護の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。

通知を見逃した場合は、製品のメインビューに、ブラウザの拡張機能がまだセットアップされていないかどうかが表示されます。ブラウザの拡張機能を設定する最も簡単な方法は、製品のメインビューに表示される通知から [設定] を選択し、画面上の指示に従うことです。

ただし、製品のメインビューに通知が表示されない場合、または通知を見逃した場合は、次の方法でブラウザ拡張機能がインストールされ、有効になっているかどうかを確認できます。

1. WindowsのStartメニューから [WithSecure Server Security] を開きます。

2. メインページで  を選択します。
3. 左下隅のポップアップ画面で、[設定の編集] 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. [はい] を選択して、アプリがデバイスに変更を加えることを許可します。
5. [セキュアブラウジング] を選択します。
6. 使用するWebブラウザに応じて、次のように操作します。
  - **Firefox**を使用している場合は、[**Browser extensions (拡張機能)**] を選択してから、[**Open Firefox Add-ons (Firefox アドオンを開く)**] を選択します。拡張機能が追加され、Firefox で有効になります。
  - **Chrome**を使用している場合は、[**Browser extensions (ブラウザ拡張機能)**] の下にある [Open Chrome Web Store (Chrome Webストアを開く)] を選択します。[**WithSecure ブラウザ保護**] ページがChrome Webストアで開きます。拡張機能がすでにChromeにインストールされているがオフになっている場合は、[**拡張機能**] からオンにします。拡張機能がまだインストールされていない場合は、**Chromeに追加 > 拡張機能を追加** を選択します。拡張機能が追加され、Chrome で有効になります。
  - **Microsoft Edge**を使用している場合は、[**Open Edge Add-ons (Edgeアドオンを開く)**] 下の [Browser extensions (ブラウザ拡張機能)] を選択します。[**WithSecure ブラウザ保護**] ページがEdgeアドオンで開きます。拡張機能がすでにMicrosoft Edgeにインストールされているが無効になっている場合は、[**オン**] を有効にします。拡張機能がまだインストールされていない場合は、[**入手 > 拡張機能の追加**] を選択します。拡張機能が追加され、Microsoft Edgeで有効になります。

注：製品のアップグレードや新しいブラウザのインストール後には、拡張機能の再インストールが必要になる場合があります。

ブラウザで次のテストページを開くと、ブラウザ拡張機能がオンになっていることを確認できます。  
<https://unsafe.fstestdomain.com>。製品ブロックページが開いた場合、ブラウザ拡張機能が使用されています。ブロックページが表示されない場合は、手動でブラウザ拡張機能をオンにする必要があります。

## 機密性のあるデータを保護する

---

トピック：

- 接続制御を有効にする
- 接続制御を使用する

「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に検出して、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。

- Microsoft Edge (Chromium)
- Firefox
- Google Chrome


## 4.1 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. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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。

注：設定を変更するには管理者の権限が必要です。

4. [接続制御] を有効にします。

5. 接続制御の設定を調整するには

- 接続制御がすでに開いている接続を閉じたくない場合は、[信頼できないアプリを切断する] をオフにします。この設定を選択しないままにしておくと、接続制御が有効になったときに、接続しているすべてのインターネット接続が閉じられます。
- 接続制御によってブロックされている外部ツールを使用する必要がある場合は、[コマンドラインおよびスクリプトツールの切断] をオフにしてください。

注：マルウェアの中には、PowerShellなどのWindowsの組み込みコンポーネントを使用して、銀行の認証情報や個人情報にアクセスするものがあるため、絶対に必要な場合を除き、この設定を選択したままにしておくことを推奨します。

- 接続制御がクリップボードにコピーされたデータをどのように処理するかを選択します。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。

接続制御でクリップボードを消去したくない場合、この設定をオフにしてください。

- デフォルトでは、銀行取引中にデバイスへのリモートアクセスはブロックされます。銀行取引は常にプライベートで機密性の高いものであるため、第三者がデバイスにリモートアクセスした場合は、銀行のサイトに決してログインしないでください。


重要：アクセスを要求したユーザとその正確な目的の両方を知っている場合を除き、誰かの要求に応じて[バンキングセッション中のリモートアクセスをブロック]の設定を無効しないでください。

## 4.2 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、**接続制御**インジケータを選択し、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] インジケータをクリックします。
2. 通知の [終了] をクリックします。

## コンテンツ制御を設定する

---

トピック:

- [Web コンテンツをブロックする](#)

不適切なコンテンツのアクセスを制限することでインターネット上の望ましくないコンテンツの閲覧を防ぐことができます。

**重要:** Webコンテンツコントロールが正しく機能するには、Browsing Protection拡張機能が必要です。

インターネットには有益なWebサイトが多くある一方、望ましくない・不適切なコンテンツを多く含むサイトがあります。

コンテンツブロッカー機能を使用すると、コンピュータを使用している各ユーザが不適切・望ましくないコンテンツにさらされることを阻止できます。ユーザがインターネットを使用できる時間も設定できます。また、成人向けコンテンツが検索エンジンで表示されることもブロックできます。


## 5.1 Web コンテンツをブロックする

Webの閲覧中に表示できるコンテンツの種類を制限できます。

不適切なコンテンツを含む Web サイトやページへのアクセスをブロックできます。

**重要:** Webコンテンツコントロールが正しく機能するには、BrowsingProtection拡張機能が必要です。

ブロックする Web コンテンツを選択するには

1. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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. ドロップダウンメニューから、設定を適用するユーザを選択します。
5. [コンテンツフィルタリング] をオンして、すべてのブラウザで選択するコンテンツを制限します。
  - コンテンツタイプでWebページをブロックするには、[Webコンテンツをブロックする]を選択します。次に、ブロックするコンテンツタイプの横にあるチェックボックスを選択します。
  - 特定のWebページへのアクセスのみを許可するには、[選択したWebサイトのみを許可する]を選択します。次に、[許可されたサイトを表示する]を選択して、許可するWebアドレスを入力します。
6. アダルトコンテンツを検索結果から非表示にするには、[検索結果フィルター] をオンにします。

### 5.1.1 コンテンツカテゴリ

さまざまなコンテンツ タイプに対するアクセスをブロックできます。

中絶	中絶、中絶クリニックや中絶センター、中絶全般に関する情報や画像を含むウェブサイト。例えば、プロライフまたはプロチョイスである可能性のあるディスカッションフォーラム。
広告配信	広告を含む様々なFlash、テキスト、ビデオ、画像ファイル、またはその他類似のファイルを指すWebリンク。
アダルト	成人向けなページや性的な要素があるページ。例: アダルトグッズショップや性的描写。
お酒とタバコ	お酒とたばこ製品、および製造者、製造所、ブドウ園、醸造所などを紹介するWebサイト。例: ビールの祭り (ビアガーデンなど) を紹介するサイトやバーやナイトクラブのWebサイトなど。
アノニマイザ	ネットワークのフィルタを回避する方法を説明する Web サイト、Web ベースの翻訳サイトを含む。例: 公開プロキシの一覧を記載しているサイト。
オークション	人々が製品やサービスを売買できるオンライン市場のWebサイト。実際の取引は別の場所で行われるかもしれないが、商品やサービスのリストを提供するサイトも含まれます。
銀行取引	貯蓄銀行、投資銀行、証券取引、外国為替取引サイトなど、銀行やその他の金融機関のWebサイト。
ブログ	個人または機関が情報を公開し、ニュース、ストーリー、ビデオ、写真を共有できるWebログ。それぞれの性質上、ブログで扱われるテーマは多岐にわたり、あらゆるトピックを含めることができます。
チャット	テキスト、音声、ビデオを通じて人々が互いにチャットできるオンラインポータルやメッセージングアプリケーション、チャットサイトなど。
出会い系	出会い系の Web サイト。例: 出会い系サイトや結婚相談所サイト。
麻薬	麻薬の使用を推奨するサイト。例: 違法薬物の購入、栽培、販売に関する情報を提供するサイト。

エンターテインメント	テレビ番組、書籍、コミック、映画、劇場、アートギャラリーなど、エンターテインメント産業に関連するWebサイト。たとえば、テレビやラジオの番組ガイドや音楽、テレビ、映画のレビューサイトなど。
ギャンブル	ユーザが実際にお金や電子マネーなどをインターネットで賭けることができるWebサイト。例: オンラインギャンブル、宝くじサイトやインターネットおよび実世界のギャンブルに関する情報を含むブログ/掲示板。
ゲーム	オンラインゲームのWebサイトや、ゲームをプレイ、ダウンロード、購入できるWebサイト。
ハッキング	利益、挑戦、または楽しみのために、コンピュータシステムやコンピュータネットワークの弱点を探し、それを利用することを促進するWebサイト。たとえば、ハッキングガイドやハッキングツールを含むサイト。
憎悪表現	宗教、人種、国籍、性別、年齢、障害、性的指向などに対して差別を行っているWebサイト。例: 人権侵害、動物虐待などに関する情報や暴行を想起させるサイト。
違法ダウンロード	不正ファイル共有やソフトウェアの違法コピーに用いられるWebサイト。例えば、ソフトウェアへの違法または疑わしいアクセスを提供するサイト、そしてネットワークおよびシステムへ損害を与える可能性のあるプログラムを開発、配布するサイト。
仕事探し	求人サイトなど仕事情報を掲載しているサイト。例: キャリアに特化した検索エンジン、ネットワーキンググループ。
決済サービス	ショッピングサイトと銀行やクレジットカードなどの金融サービスとの間の支払いを処理するWebサイト。一般的な決済に利用できるサイトも含まれます。
詐欺	アンケートに答えたり、クイズに答えたり、同じような行動をとると賞品がもらえるというWebサイト。
買い物物	オンラインショッピング向け商品カタログを掲載しており、ユーザがオンラインで商品やサービスを購入できるWebサイト。もしくはオンラインで注文や購入できる商品の情報を提供しているサイト。
<b>SNS</b>	一般ユーザ同士を結びつけたり、特定のグループのメンバー間の交流、ビジネス交流などを助けるネットワークポータル。例えば、自分の個人的、仕事上の関心事などをシェアするためのメンバープロフィールを作成できるようなサイト。Twitterなどのソーシャルメディアサイトがこれに含まれる。
ソフトウェアのダウンロード	さまざまなソフトウェアをダウンロードするためのオンラインポータル。
スパム	スパムメールから収集されたWebサイト。
ストリーミングメディア	ビデオやオーディオのストリーミングコンテンツを無料またはサブスクリプションモデルで配信するWebサイト。
暴力	暴力を扇動したり、陰惨で暴力的な画像もしくは動画を含むWebサイト。例えば、レイプ、ハラスメント、スナッフ、爆弾、暴行、殺人あるいは自殺についての情報を含むサイト。
武器	人間、もしくは動物に害を与える武器等に使用可能な情報、画像、もしくは動画などを含むWebサイト。これには狩猟や射撃クラブなど、これらの武器の普及を援助している組織が含まれる。またこのカテゴリにはペイントボールガンやBBガンなどのおもちゃの武器も含まれる。
<b>Webメール</b>	Webブラウザを使用してメールアドレスを作成し、アクセスできるようにするウェブサイト。たとえば、Yahoo!メールやGmail、ローカルでISPとリンクしているWebメールサービスなどが含まれます。

## 検索エンジンのフィルタを使用する

---

トピック:

- [検索エンジンのフィルタをオンにする](#)

検索結果フィルターは、Google、Yahoo、Bing、およびYouTubeがSafeSearchの「厳格な」レベルを使用するようにすることで、アダルトコンテンツを非表示にします。


不適切なコンテンツや露骨なコンテンツが検索結果に表示されないようにすることはできませんが、そのようなコンテンツのほとんどを回避することができます。

## 6.1 検索エンジンのフィルタをオンにする

---

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を有効にするには

1. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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サーバーサーチの Web サイト設定が無効になります。

## 集中管理

---

トピック:

- [Windows イベント ビューワを開く](#)

本製品は集中管理モードで実行されます。集中管理モードでは製品の設定がリモートの管理者/エキスパートによって運用されます。

集中管理モードを利用している場合、次が可能になります。

- 製品の設定をリモートから指定できるようになります。
- 設定をロックして、ローカルのユーザが無断で変更できないように指定できます。

[設定 > 集中管理](#) ページには、コンピュータに関する情報が表示されます。製品の設定に問題がある場合、この情報を IT 管理者に提供する必要がありますが、必ずしも必要ありません。

Windows イベントビューワを使用して記録されたエラーを確認します。

## 7.1 Windows イベント ビューワを開く

---

本製品の動作に問題の疑いがある場合、Windows イベント ビューワでエラーが発生したか確認できません。

Windows イベント ビューワからインポートに関するシステム イベントの情報を確認できます。情報の中には、本製品のアクションとエラーが含まれます。

1. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
2. メインページで  を選択します。
3. [集中管理] を選択します。
4. [イベント ビューワを開く] をクリックします。  
Windows イベント ビューワが開きます。
5. 本製品に関するメッセージは [Windows ログ] をクリックして、[アプリケーション] または [システム] を選択します。

注: [ソース] をクリックすると、メッセージをソース順に並び替えられます。

## ファイアウォールについて

---

トピック:

- [Windows ファイアウォールの設定を変更するには](#)
- [パーソナル ファイアウォールを使用する](#)

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アクセスすることを阻止します。

## 8.1 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. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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。

## 8.2 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、WithSecure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、WithSecure の全プロセスを許可するように設定してください。

## プログラムを最新の状態にする

---

製品を使用して、コンピュータにインストールされているソフトウェアを確認し、適用されていないアップデートプログラムをインストールできます。

注：管理者は、管理対象コンピュータへのソフトウェアアップデートプログラムのインストールを制限することがあります。

1. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
2. メインページで  を選択します。  
[ソフトウェアアップデート] ビューには、インストールされていないアップデートが表示されます。
3. [ここをクリックするとアップデートを管理できます] を選択します。

注：適用されていないアップデートをインストールするには管理者権限が必要です。

4. 利用可能な新しいアップデートがあるかどうかを確認する場合、[今すぐチェック] を選択します。
5. インストールするアップデートを選択します。
6. [選択したアップデートをインストール] を選択します。  
[インストール] タブには、選択した各アップデートのステータスと進行状況が表示されます。



# 第 10 章

## アップデートの使用方法

---

トピック:

- [最新のアップデートを表示する](#)
- [隔離された Server Security ホストでのマルウェア定義の更新](#)
- [接続設定を変更する](#)

アップデート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。

## 10.1 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. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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。

## 10.2 隔離された Server Security ホストでのマルウェア定義の更新

ネットワーク接続がないホストに Server Security をインストールした場合は、Policy Manager に付属のツールを使用してマルウェア定義を更新できます。

アップデートをダウンロードするツールは Policy Manager にバンドルされており、提供されたスクリプトを使用して抽出できます。インターネットにアクセスできるマシン上でこのツールを実行すると、最新のアップデートと必要な差分がダウンロードされ、オールインワンアーカイブが生成されます。

デフォルトでは、ツールは data\updates フォルダを使用して、ダウンロードした更新バイナリを保存します。また、最新バージョンへの関連する差分をダウンロードするための参照として使用するために、更新履歴も保存します。

更新バイナリに加えて、準備された更新をインポートするための fsaua-update\_32 ツールも必要です。このツールは、Server Security インストール パッケージに含まれています: C:\Program Files (x86)\F-Secure\Server Security\fsaua-update\_32.exe。

マルウェア定義を更新するには:

1. Policy Manager マシンで次のコマンドを実行して、ツールを準備します。
  - Windows: <F-Secure インストール フォルダ>\Management Server 5\bin\prepare-fspm-definitions-update-tool.bat <保存先フォルダ>
  - Linux: /opt/f-secure/fspms/bin/prepare-fspm-definitions-update-tool <保存先フォルダ>
2. 必要に応じて、準備したバイナリをインターネットにアクセスできるマシンに転送します。
3. 必要に応じて、ツール構成を変更します。
  - conf\channels.json: 更新するチャンネルのリストが含まれています。デフォルトでは、Policy Manager によって管理されるすべてのサポート対象クライアントの更新が含まれているため、環境に必要な Server Security バージョンのみを残すことをお勧めします。
4. ツールを実行します。
  - Windows: fspm-definitions-update-tool.bat
  - Linux: fspm-definitions-update-tool

結果として得られるアーカイブには、最新の定義の完全なセットとこのバージョンとの差分が含まれます。すべてのデータが最新の場合、アーカイブは生成されません。
5. 準備したアーカイブ (デフォルトでは data\f-secure-updates.zip) を、隔離された Server Security ホストの隔離されたホストディレクトリ (C:\Program Files (x86)\F-Secure\Server Security) に転送します。


6. 分離されたホストで更新を起動します。管理者権限で C:\Program Files (x86)\F-Secure\Server Security\fsaua-update\_32.exe 実行します。

## 10.3 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 (ISP) 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. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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。

## プライバシー

---

トピック:

- セキュリティデータ
- 製品の改善

ここでは、SecurityCloud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。

## 11.1 セキュリティデータ

---

このサービスは、潜在的な悪意のあるアクティビティまたは保護されたデバイスに関するクエリを WithSecure **Security Cloud** に送信します。


WithSecure Security Cloud は、WithSecure が運用するサイバー脅威分析用のクラウドベースのシステムです。当社は、お客様がサブスクライブしたセキュリティサービスを提供し、ユーザーに高品質の保護を提供するために、最小限のデータを収集します。

Security Cloud を利用することで、WithSecure は世界の脅威の最新の状況を把握し、新たな脅威が発見された瞬間にお客様を保護することができます。

Security Cloud は、セキュリティ上の理由で WithSecure がブロックしたファイルや Web サイトに関する情報を含む可能性のあるデータのみを収集します。セキュリティデータは、個別のマーケティング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. Windows の **Start** メニューから [WithSecure Server Security] を開きます。
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。

## 11.2 製品の改善

---

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

使用データを提供するには

1. Windows の **Start** メニューから [WithSecure Server Security] を開きます。
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：当社のプライバシーステートメントは [こちら](#) からご覧いただけます。

## テクニカル サポート

---

トピック:

- [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 ツールを使用する](#)
- [製品の問題をデバッグする](#)
- [電話詐欺と標的にされていると思われる場合の対処方法](#)

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。


製品に関する質問や問題がある場合、弊社のカスタマーサポートに連絡する前に、[WithSecureコミュニティ](#)にアクセスし、そこで質問に対する答えが見つかるかどうか確認してください。

## 12.1 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. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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。

## 12.2 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。

セキュリティ製品に技術的な問題が発生した場合、当社のテクニカル サポートがWSDIAGファイルの作成と送信を依頼することがあります。このファイルは、ご使用のコンピュータに固有の技術的な問題を解決するのに役立ちます。

サポートツールを使用してファイルを作成することができます。このツールは、システムおよびその構成に関する情報を収集します。情報には、製品の詳細、オペレーティングシステムのログ、システム設定などが含まれます。なお、情報の一部は機密情報である場合があります。収集された情報は、コンピュータのデスクトップに保存されるファイルに格納されます。

サポート ツールを使用するには

1. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
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.withsecure.com/en/support/contact-support/email-support>で提出できます。

ヒント：製品からサポートツールにアクセスできない場合は、[サポートツールのWebページ](#)にアクセスし、**Windows用サポートツール ( WSDIAG )** で、[ダウンロード]を選択し、wsdiag\_standalone.exeを保存します。次に、ファイルをダブルクリックしてツールを実行します。

## 12.3 製品の問題をデバッグする

---

デバッグログは、カスタマーサポートが製品に問題がある場合はそれを分析して解決するのに役立ちます。


製品の問題点を分析するために、カスタマーサポートに一時的に特定の権限を与えることができます。デバッグログで収集された情報は、機密情報とみなされる場合がありますのでご注意ください。

WebView2は、ネイティブアプリケーションにWebコンテンツを埋め込むために使用されるテクノロジーです。たとえば、アカウントのログインページはWebView2テクノロジーを使用しています。

WebView2コンソールデバッガーは、組み込み型Webビューで問題が発生した場合、当社のカスタマーサポートがWebビューの問題を分析するのに役立ちます。

製品の問題をデバッグするための一時的な許可をサポート担当者を与えるには

注：[デバッグログ]は、カスタマーサポートエージェントから要求された場合にのみオンにします。

1. Windowsの**Start**メニューから [WithSecure Server Security] を開きます。
2. メインページで  を選択します。
3. [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. [ツール] で、トグルスイッチを選択して [デバッグログ] をオンにします。  
デバッグログを有効にすると、[WebView2コンソールデバッガー] オプションが表示されます。
5. [WebView2コンソールデバッガー] をオンにする場合は、トグルスイッチを選択します。  
埋め込みWebビューに入ると、コンソールウィンドウが開きます。
6. カスタマーサポートが問題の分析を完了したらすぐに、トグルスイッチを選択して [デバッグログ] をオフにします。

## 12.4 電話詐欺と標的にされていると思われる場合の対処方法

電話による詐欺は、ソーシャルエンジニアリングを用いて被害者を狙うもので、増加傾向にあります。このトピックでは、このような電話を識別し、最悪の場合（標的にされた場合）、次に何をすべきかについての情報を提供します。

電話詐欺とは何ですか？

電話がかかってくるきっかけは、コールドコールであったり、広告やリンクを使用してパソコンにポップアップが表示されたりします。これらのポップアップは、宣伝されているテクニカルサポート番号に電話するように促します。ポップアップは突然表示されることがあり、取り除くのはそれほど簡単ではありません。

電話詐欺を見分けるにはどうしたらいいですか？

このような電話は、通常、一定のパターンでかかってきます。加害者は、実際には存在しない問題（ウイルスなど）がコンピュータにある問題があることを主張し、存在しないサービスの料金を払わせようとします。不意を突かれて感情を揺さぶられるのです。以下は、一般的なシナリオです。

- 電話詐欺師は、Microsoft、銀行、ネットワークオペレーターなど、有名な会社を名乗ります。評判の良い会社を名乗ることで、ユーザーにより安心感を与えます。また、知識豊富で、専門用語を使うため、正当で信憑性の高い印象を与えます。
- リスクが本当に存在し、コンピューターウイルスの可能性に対して心配するため、ユーザーは加害者にコンピューターへのアクセスを許可します。そして、加害者は、リモートアクセスツールを使用してコンピューターにアクセスするためのアプリケーションをインストールするように説得します。
- 加害者は、お客様のコンピューターにアクセスすると、ウイルスを修正するふりをして、お客様の個人情報を聞き出すこともあります。加害者は問題を解決した後、お客様にオンライン銀行へのログインを求めたり、クレジットカード情報をフォームに記入するよう求めたりします。そして、存在しないサービスに対する料金を請求しますが、結果的にはお客様が考えていたよりもはるかに高額になります。実際のところ、実際にいくら請求しているかを知ることは困難です。

被害に遭ったと思われる場合の対処法

被害に遭っていると思い、上記のようなシナリオに心当たりがある場合は、次のように行動してください。

- すぐに行動してください。
- すぐにクレジットカード会社や銀行に連絡し、詐欺を通報し、銀行口座やクレジットカードを解約してください。迅速に行動すれば、カード会社は不正請求を防いだり、取り消したりすることができるかもしれません。
- 詐欺に遭ったことを適切な機関に通報します。
- 影響を受けたと思われるすべてのWebサイトやサービスのパスワードを変更します。
- 不明な（見覚えのない）サードパーティソフトウェアをアンインストールします。
- コンピューターでフルスキャンを実行します。セキュリティ製品を開き、[ウイルスと脅威] > [完全スキャン]を選択します。

## 迷惑電話に関する注意点

- このような電話を受けた場合、「これを要求したか」と考えてみてください。  
注: 通常、カスタマーサポートから電話がかかってくるのは、すでにお問い合わせいただき、サポートチケットを作成されている場合です。
- テクニカルサポートでは、問題解決を支援する手段として、リモートセッションがよく使われます。  
要確認: 信頼できる人や会社とのリモートセッションのみを許可してください。また、事前にサービスプロバイダーに連絡し、有効なサポートケースがある場合にのみ、リモートセッションを許可してください。他のパスワードを保護する場合と同様に、リモートアクセスデータを保護してください。
- 知らない人にデバイスへのアクセス権を与えてはいけません。詐欺師にリモートアクセスを許可することは、事実上、コンピューターの管理者権限を渡すことになります。ウイルス対策ソフトがインストールされていても、詐欺師がコンピュータを操作するため、ウイルス対策ソフトでは保護できなくなります。
- Microsoftは、ソフトウェアのエラーメッセージや警告メッセージに電話番号を記載することはないとユーザーに伝えています。
- 個人情報やクレジットカードの情報を第三者に簡単に渡してはいけません。
- すぐに通話を終了します。
- このような電話は違法であり、疑わしい場合は、詐欺を扱う関連機関に通報してください。

## セキュリティ製品はどのように役立ちますか？

セキュリティ製品をインストールすることで、コンピュータをウイルス、トロイの木馬、ランサムウェアから保護することができます。また、ブラウザ保護、バンキング保護、リモートアクセスツールの保護機能により、さらに保護が強化され、ブラウジングやオンラインバンキングが安全に行えるようになります。

このような被害に遭い、すでにセキュリティ製品をインストールしている場合は、すぐにコンピュータの完全スキャンを実行し、詐欺師によってインストールされた可能性のあるアプリケーションを検出することができます。これらは潜在的不要アプリケーション (PUA) と呼ばれます。ただし、本製品はこのような電話詐欺の被害からお客様を守ることはできません。

警戒し、安全に過ごしてください。