WithSecure Elements Endpoint Protection for Computers (Mac)

目次

1: 製品を使用するには....4

1.1 免責事項....5
1.2 システム要件....5
1.3 サブスクリプションに関する情報の表示....6
1.4 製品の設定を変更する....6
1.4.1 製品の設定のクイック アクセス....6
1.4.2 ツールを表示する....7
1.5 コンピュータの保護状況を確認するには....7
1.5.1 セキュリティのステータス アイコン....7

2: コンピュータを危険なコンテンツから保護する....9

2.1 危険なコンテンツについて....10
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....10
2.1.2 ワーム....10
2.1.3 トロイの木馬....11
2.1.4 バックドア....11
2.1.5 エクスプロイト....12
2.1.6 エクスプロイト キット....12
2.2 コンピュータをスキャンする....12
2.2.1 ファイルを自動的にスキャンする....12
2.2.2 ファイルを手動でスキャンする....13
2.3 サンプルを送る....14
2.4 自動更新について....14
2.4.1 更新ステータスを確認する....14
2.5 WithSecure XFenceとは?....14

3: Web サイトのアクセスを保護する....16

3.1 危険な Web サイトをブロックする....17
3.1.1 特定の Web サイトを許可/ブロックする....17
3.1.2 Web サイトがブロックされた場合....17
3.1.3 ブラウザ保護の評価....18
3.2 安全なオンライン バンキング....18
3.2.1 バンキング保護を有効にする....19
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....19
3.3.1 Safariのブラウザ拡張機能を有効にする....19
3.3.2 Chromeのブラウザ拡張機能をインストールして有効にする....20
3.3.3 Firefoxのブラウザ拡張機能をインストールして有効にする....20

4: ファイアウォールについて.....21

4.1 コンピュータに対してすべての接続を許可する.....22

付録 A: テクニカル サポート.....23

A.1 アカウント ID はどこで確認できますか?.....24
A.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?.....24
A.3 サポート ツールを使用する.....24
A.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.....24

第 章
1

製品を使用するには

トピック :

- 免責事項
- システム要件
- サブスクリプションに関する情報の表示
- 製品の設定を変更する
- コンピュータの保護状況を確認するには

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。

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

このセクションには、WithSecure Elements Agent for Mac (旧 F-Secure PSB Computer Protection & RDR for Mac)。製品の使用を開始する前に、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オペレーティング システム

Elements Agent for Macは、次のオペレーティング システムのバージョンをサポートしています。

- macOS13「ベンチュラ」
- macOS 12「モントレー」
- macOS 11 Big Sur

システム要件

推奨されるシステム要件は次のとおりです。

- Intel または Apple Silicon Mac
- 500 MB の空きディスク容量
- 1GB以上のメモリ
- インターネット接続: サブスクリプションを検証してアップデートを受信するには、インターネット接続が必要です

対応ブラウザ

- Safari
- Chrome
- Firefox

サポートされている言語

サポートされている言語は、英語、ブルガリア語、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、フランス語(カナダ)、ドイツ語、ギリシャ語、ハンガリー語、イタリア語、日本語、リトアニア語、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、ロシア語です。、スロベニア語、スペイン語、スペイン語(メキシコ)、スウェーデン語、トルコ語、ベトナム語、繁体字中国語 (香港)、繁体字中国語 (台湾)、簡体字中国語。

既知の制限

ブラウジング保護:

- 「セキュリティ クラウド」が利用できない場合、ウェブサイトはブロック ページをバイパスします。

  「Security Cloud」が利用できない場合、ユーザーは設定に関係なく、おそらくどの Web サイトにもアクセスできます。

- プロキシとの接続の問題。

  ソフトウェアの実行中にプロキシが変更された場合、製品が新しいプロキシを使用できるようにするには、コンピュータを再起動する必要がある場合があります。

- Chrome シークレット モードでは、ブラウザ保護とバンキング保護はデフォルトで有効になっていません。

ユーザーは、Chrome シークレット モードの機能を有効にすることができます。[クロム] > [環境設定] > [拡張機能]「WithSecureによるブラウジング保護」拡張機能の「シークレットモードで許可」オプションをチェックします。

- すべての銀行サイトは、まだ銀行として分類されていません。

  バンキング通知が届くはずだったのに表示されない場合は、次の URL からバンキング URL を送信してください。https://www.withsecure.com/en/support/contact-support/submit-a-sample

既知の問題点

ウイルス対策:

- Time Capsule ディスクのアンマウント中にコンピュータが一時的にハングアップすることがあります。

  Time Capsule ディスクのアンマウント中に、リアルタイム スキャンによってコンピュータの速度が低下したり、ハングしたりすることがあります。コンピュータを再起動すると、問題が解決します。

Rapid Detection & Responseスタンドアロン モード:

- ブラウザ保護の Safari 拡張機能は表示されますが、Safari で動作しません。Rapid Detection & Responseスタンドアロン モード

  ブラウザ保護は動作していません Rapid Detection & Responseこれは予想される動作です。

1.3 サブスクリプションに関する情報の表示

このセクションでは、サブスクリプションに関連する情報を提供します。

サブスクリプションに関する情報を表示するには

1. メニューバーの製品アイコンから製品を開きます。
2. 製品メニューから、[サブスクリプション] を選択します。
   [サブスクリプション] ビューが開きます。

ビューでは、現在のサブスクリプションとそのステータスに関する情報を確認できます。

必要に応じて、このビューからオンライン管理ポータルにアクセスすることもできます。

必要に応じて、アクセスすることもできます My F-Secureこの観点から。

1.4 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。アプリメニューまたはメニューバーの製品アイコンから、製品設定にすばやくアクセスできます。

注: 管理者がセキュリティ設定を強制している場合があり、ローカルで一部の機能を変更できない場合があります。

1.4.1 製品の設定のクイック アクセス

製品の設定は、アプリメニューおよびメニューバーの製品アイコンからアクセスできます。

製品の設定をすぐに変更したい場合は、メニューバーの製品アイコンを選択し、ドロップダウンメニューから [環境設定] を選択すると、製品の環境設定にアクセスできます。

[環境設定] の他に、製品アイコンメニューには次のオプションが含まれています。

オプション	説明
[<product name> を開く]	製品を開きます。
[環境設定...]	製品の設定を変更できる設定画面を開きます。
[ウイルスとスパイウェアのスキャン]	システム内のアクセス可能なすべてのファイルをスキャンして、完全なウイルス対策チェックを行います。
スキャンするオブジェクトを指定...	システム内の特定のフォルダをスキャンすることができます。
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。
感染レポート...	システムで検出されたすべての感染を一覧表示するウィンドウを開きます。

メニューには、コンピュータの保護ステータス、製品バージョン、および最新のデータベース更新に関する情報も表示されます。

1.4.2 ツールを表示する

コンピュータを保護するために使用できるツールにアクセスするには、[ウイルスと脅威] と [安全なブラウジングとバンキング] セクションを使用できます。

1.5 コンピュータの保護状況を確認するには

製品のメインビューでは、現在のセキュリティステータスと製品に関する重要な情報が表示されます。

メインビューの右上隅に、サブスクリプションのステータスが表示されます。

メニューバーの製品アイコンにマウスを置くと、ウイルス保護とブラウザ保護がアクティブであるかどうか、およびすべてのセキュリティ機能が最新であるかどうかを示す通知が表示されます。

最新のアップデートがインストールされていることを確認するには

1. メニュー バーにある製品アイコンを選択します。
2. [アップデートを確認する] を選択します。
   製品は最新のアップデートをすぐに取得します。

1.5.1 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のアイコンは、製品と機能の全体ステータスを示します。

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	コンピュータは保護されてます。 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。
	警告	コンピュータが保護されていないことを示します。 対応が必要な操作 (アップデートが長い間行われていない、セキュリティ機能がオフの場合など) があることを示します。
	エラー	コンピュータが保護されていないことを示します。 対応がすぐに必要でがあることを示します (重要な機能が無効になっている、サブスクリプションが失効した場合など)。

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**
- [**Safariブラウザ拡張機能は使用されていません**]
- **サブスクリプションが失効しました**

第 章
2

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
- サンプルを送る
- 自動更新について
- WithSecure XFenceとは?

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。

ディープガードは、セキュリティを強化して、有害なアプリケーションによる個人データの削除、改ざん、または盗難から保護します。

2.1 危険なコンテンツについて

マルウェアは、コンピュータの破壊、悪用、情報の搾取を目的とするプログラムです。

マルウェアは次のことを実行できます。

- Webブラウザを制御する
- 検索内容をリダイレクトする
- 不要な広告を表示する
- アクセスしたWebサイトを記録する
- 銀行情報などの個人情報を盗む
- コンピュータを使用してスパムを送信する
- コンピュータを利用して他のコンピュータを攻撃する

また、コンピュータの動作を遅くしたり不安定にすることもあります。コンピュータの動作が急に遅くなったり、頻繁にクラッシュするようになった場合、コンピュータがマルウェアに感染している可能性があります。

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」には、デバイスやデータに深刻な影響を与える動作や特性があります。

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、多くの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危険にさらします**-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、軽いものから重大なものまでさまざまです。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。

アプリケーションに、重大な影響を与える動作または特性がある場合、その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。

「不要な可能性がある」アプリケーションや「不要な」アプリケーションを信頼して使用するかどうかの判断はユーザが選択することができます。

- **不要な可能性があるアプリケーション**-アプリケーションが普通に実行される前に警告メッセージが表示されます。アプリケーションを信頼できる場合、製品の実行を許可できます。また、アプリケーションをブロックすることもできます。
- **不要なアプリケーション**-アプリケーションをブロックおよび隔離保存します。アプリケーションを信頼できる場合、今後のスキャンから除外することができます。

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

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。

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。

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。

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。

2.2 コンピュータをスキャンする

マルウェアに対して、リアルタイム、またはマニュアル⊠手動⊠スキャンを実行することができます。

2.2.1 ファイルを自動的にスキャンする

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ごみ箱に移動されます。

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。

次のようなファイルはスキャンが通常より長くかかります。

- 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。
- 圧縮ファイル (***.zip*** など)。

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。

感染レポートの表示

感染レポートには、リアルタイム保護が検出してゴミ箱に移動したウイルスとスパイウェアが表示されます。

感染レポートを表示するには

1. メニュー バーにある製品アイコンを選択します。
2. 選択する [**感染レポート...**]メニューから。
   NS **感染症**レポートが開きます。
3. 検出された感染をスキャンの除外に追加する場合は、レポートからアイテムを選択してから、[**除外に追加**]。
   このアイテムは、今後のスキャンでウイルスや有害なコンテンツがないかスキャンまたはブロックされることはありません。

注: 感染レポートには、手動スキャン中に検出および削除されたマルウェアはリストされていません。

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 (アプリケーションが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。

手動でスキャンする対象を選択する

システム内の特定のファイルまたはフォルダをスキャンできます。

ファイルやフォルダにマルウェアが含まれている可能性がある場合、手動でスキャンすることができます。

ファイルまたはフォルダを手動でスキャンするには

1. メニュー バーにある製品アイコンを選択します。
2. [**スキャンするオブジェクトを指定...**] を選択します。
   スキャンする対象を指定するウィンドウが開きます。
3. スキャンするファイルまたはフォルダを選択してから、[**開く**] を選択します。

スキャンが開始されます。スキャンが完了すると、スキャンウィンドウにスキャン結果が表示されます。

スキャン中にマルウェアが検出されると、マルウェアの名前とパスが表示され、感染したファイルが自動的にごみ箱へ移動されます。

ヒント：感染したファイルを完全に削除するためにごみ箱を空にしてください。

2.3 サンプルを送る

不審なアプリケーションを分析用にF-Secureに提供することでF-Secureの検出精度の改善に貢献できます。

製品がセキュリティのリスクのあるアプリケーションをブロックした場合、アプリケーションのサンプルを分析用に F-Secure に送信することができます。

ファイルが脅威として誤ってマークされていると思われる場合、または悪意があると思われる場合は、分析のために匿名でファイルを送信できます。

サンプルを分析用に送信するには

1. メニューバーの製品アイコンから製品を開きます。
2. メイン ビューで、[ウイルスと脅威] を選択します。
3. [サンプルを送信] を選択します。
   デフォルトの Web ブラウザで新しい Web ページが開きます。
4. サンプルを提出するために Web ページのフォームを入力します。

2.4 自動更新について

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自動的に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。

2.4.1 更新ステータスを確認する

更新を最後に受信した日付と時間を確認できます。

通常、更新を手動で確認する必要はありません。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。

最新の更新を受信しているかどうか確認するには

1. メニュー バーにある製品アイコンを選択します。
2. [アップデートを確認する] を選択します。
   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。
3. 最新のデータベースがインストールされている日付を確認するには、製品のアイコンを選択します。
   最新のデータベースに関する情報は、メニューの下部に表示されます。

2.5 WithSecure XFenceとは?

WithSecure XFenceは、セキュリティを強化して、マルウェアによる個人データの削除、改ざん、または盗難から保護します。

アプリケーションがファイルへの書き込みまたはファイルの削除を試みると、XFenceはWithSecureのSecurity Cloudからアプリケーションの評価をチェックします。アプリケーションが信頼されている場合、操作は許可され、アプリケーションが疑わしい、または有害であることが判明している場合、アプリケーションがブロックされます。利用可能な情報がない場合、XFenceは、アプリケーションを拒否または許可するように求める許可ダイアログを表示します。

ファイルの評価を確認することにより、XFenceはシステム侵害の検出を改善します。また、プライバシーを尊重しないアプリケーションがWebカメラを使用したり、新しいスタートアッププログラムをインストールしたり、他のプログラムを制御したり、インターネット接続を盗聴したり、プライバシーに影響を与える可能性のあるその他のアクティビティを防ぐことができます。

第 章
3

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
- 安全なオンライン バンキング
- 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 サイトの安全性をユーザに示し、危険性のある Web サイトにアクセスすることを阻止します。

ブラウザ保護は検索エンジンで紹介される Web サイトの安全性に関する評価を表示する機能です。危険性のある Web サイト (マルウェアなどが埋め込まれているサイトなど) を識別することによって、ブラウザ保護は最新および未知の脅威に対する保護を提供します。

安全性評価は、WithSecureマルウェアアナリストやWithSecureパートナーなど、複数の情報源からの情報に基づいています。

ブラウザ保護は Safari、Firefox、Chrome の Web ブラウザに対応しています。

関連タスク

ブラウザの拡張機能が使用中であることを確認するページ19
ブラウザ保護には、ウェブ閲覧、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。

3.1 危険な Web サイトをブロックする

ブラウザ保護を有効にしたら、本製品が危険な Web サイトのアクセスを阻止します。

ブラウザ保護を有効にしたら、検索エンジンで表示される各リンクに対して安全性評価が示され、危険な Web サイトのアクセスがブロックされます。

ブラウザ保護を有効にするには

1. メニュー バーにある製品アイコンを選択します。
2. [**環境設定**] を選択します。
   「**ブラウザ保護**」タブが開いていることを確認します。
3. [**ブラウザ保護 を有効にする**] を選択します。

注: ブラウザ保護では、使用するWebブラウザにブラウザ拡張機能がインストールされ、オンになっている必要があります。製品は通常、Safariに拡張機能を自動的にインストールしますが、機能する前にブラウザで拡張機能を有効にする必要があります。本製品はFirefoxとChromeにも対応していますが、手動でインストールして有効にする必要があります。

関連タスク

ブラウザの拡張機能が使用中であることを確認するページ19

ブラウザ保護には、ウェブ閲覧、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。

3.1.1 特定の Web サイトを許可/ブロックする

ブラウザ保護は、有害と評価されたWebサイトへのアクセスを自動的にブロックし、個人情報を盗もうとする可能性があります。

有害と思われる特定のWebサイトを手動でブロックするか、安全であると確信できる場合は自動的にブロックされたWebサイトを許可することができます。

Web サイトを許可するには

1. メニューバーの製品アイコンから製品を開きます。
2. メイン ビューで、[**セキュアブラウジングとバンキング**] を選択します。
3. [**セキュアブラウジングとバンキング**]ビューで、[**ブロックおよび許可されたWebサイトの管理**]を選択します。
4. 左下隅にある鍵のアイコンを選択します。
   設定を変更するには管理者の権限が必要です。
5. [**セキュアブラウジング**] タブで [**Webサイトの例外**] を選択します。
   [**Webサイトの例外**] ウィンドウが開きます。
6. [**+**] を選択して、許可するWebサイトのアドレスを入力して [Enter] を押します。
   Webサイトは、Webサイトの例外のリストに追加されます。

3.1.2 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** > **許可**をクリックしてください。
2. 管理者パスワードを入力して、[**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、許可されたWebサイトのリストにWebサイトが追加されます。

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、Webサイトをここから分析用に送信することができます。

関連タスク

特定の Web サイトを許可/ブロックするページ17

ブラウザ保護は、有害と評価されたWebサイトへのアクセスを自動的にブロックし、個人情報を盗もうとする可能性があります。

3.1.3 ブラウザ保護の評価

ブラウザ保護は、検索エンジンの検索結果にWebサイトの安全性評価を表示します。

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。
	Web サイトのアクセスがブロックされなくなります。
	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。

ブラウザ保護の評価は次の検索サイトで利用できます。

- Google
- Bing
- Yahoo
- DuckDuckGo

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.withsecure.com/en/support/contact-support/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。

3.2 安全なオンライン バンキング

「バンキング保護」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。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。

バンキング保護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。

バンキング保護は次のブラウザに対応しています。

- Safari
- Firefox
- Google Chrome

3.2.1 バンキング保護を有効にする

バンキング保護は、銀行サイトのアクセスや取引を行うときに発生する可能性がある危険な処理からシステムを保護します。

バンキング保護は安全な銀行サイトに対する接続の安全性を識別し、そのようなサイトにアクセスするときにユーザを通知します。

デフォルトでは、バンキング保護は有効になっています。有効になっていない場合は、次の方法でバンキング保護をオンにします。

1. メニュー バーにある製品アイコンを選択します。
2. [**環境設定**] をメニューから選択します。
3. [**セキュア ブラウジング**] タブを選択します。
4. 左下隅にある鍵のアイコンを選択します。
   設定を変更するには管理者の権限が必要です。
5. [**バンキング保護を有効にする**] を選択します。

注 : バンキング保護は、ブラウザ拡張機能が使用されていることを必要とします。

関連タスク

ブラウザの拡張機能が使用中であることを確認するページ19
ブラウザ保護には、ウェブ閲覧、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。

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

ブラウザ保護には、ウェブ閲覧、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。

本製品をコンピュータにインストールした後、使用するWebブラウザ用の拡張機能をインストールして有効にする必要があります。

この製品はSafari用のブラウザ拡張機能を自動的にインストールします。必要なのは、拡張機能がオンになっていることを確認することだけです。

ChromeとFirefoxの場合、インターネットを安全に閲覧するためには、ブラウザの拡張機能をインストールして有効にする必要があります。また、拡張機能のインストールには、閲覧したWebアドレスの情報にアクセスするための許可が必要です。より詳しい情報は、関連情報をご覧ください。

3.3.1 Safariのブラウザ拡張機能を有効にする

ブラウザを安全に使用できるようにするには、Safariのブラウザ拡張機能を有効にする必要があります。

この製品はブラウザ拡張機能を自動的にインストールします。必要なのは、拡張機能がオンになっていることを確認することだけです。

Safariのブラウザ拡張機能がオンになっていることを確認するには

1. メニュー バーにある製品アイコンを選択します。
2. [**環境設定**] をメニューから選択します。
3. [**セキュア ブラウジング**] タブを開きます。
4. [**ブラウザ プラグインをインストールする**] を選択します。
   [**ブラウザ保護のインストール**] ウィンドウが開きます。
5. ドロップダウンから [**Safari**] > [**今すぐ有効にする**] を選択します。
6. [**拡張機能**] ダイアログで、[**ブラウザ保護**] が選択されていることを確認します。

Safariを使用してインターネットを安全に閲覧できるようになります。

ブラウザ拡張機能が正しく動作していることを確認するために次のページをブラウザで開きます: https://unsafe.fstestdomain.com。製品のブロック ページが表示されるはずです。

3.3.2 Chromeのブラウザ拡張機能をインストールして有効にする

Chromeブラウザを安全に使用するには、Chromeのブラウザ拡張機能をインストールして有効にする必要があります。

Chromeのブラウザ拡張機能を設定するには

1. メニュー バーにある製品アイコンを選択します。
2. [**環境設定**] をメニューから選択します。
3. [**セキュア ブラウジング**] タブを開きます。
4. [**ブラウザ プラグインをインストールする**] を選択します。
   [**ブラウザ保護のインストール**] ウィンドウが開きます。
5. ドロップダウンから [**Chrome**] > [**今すぐインストール**] を選択します。
6. **Chromeに追加** > **拡張機能を追加する**を選択します。
   拡張機能がインストールされると、ユーザの同意ダイアログが開きます。ブラウザ拡張機能は、アクセスしたWebアドレスに関する情報にアクセスするための許可を必要とします。
7. [**同意する**] を選択します。

   👉 **注 :** 許可しない場合、拡張機能を使用できなくなり、ブラウザ保護は有害なWebサイトをブロックしたり、検索結果の評価を表示したりすることはできません。また、拡張機能はブラウザから削除されます。

8. 拡張機能の設定を完了するには、[**OK**] を選択します。

Chromeを使用してインターネットを安全に閲覧できるようになります。

ブラウザ拡張機能が正しく動作していることを確認するために次のページをブラウザで開きます: https://unsafe.fstestdomain.com。製品のブロック ページが表示されるはずです。

3.3.3 Firefoxのブラウザ拡張機能をインストールして有効にする

Firefoxブラウザを安全に使用するには、Firefoxのブラウザ拡張機能をインストールして有効にする必要があります。

Firefoxのブラウザ拡張機能を設定するには

1. メニュー バーにある製品アイコンを選択します。
2. [**環境設定**] をメニューから選択します。
3. [**セキュア ブラウジング**] タブを開きます。
4. [**ブラウザ プラグインをインストールする**] を選択します。
   [**ブラウザ保護のインストール**] ウィンドウが開きます。
5. ドロップダウンから、を選択します [**Firefox**]その後 [**今すぐインストール**]。
6. [**追加**] を選択します。
   拡張機能がインストールされると、ユーザの同意ダイアログが開きます。ブラウザ拡張機能は、アクセスしたWebアドレスに関する情報にアクセスするための許可を必要とします。
7. [**同意する**] を選択します。

   👉 **注 :** 許可しない場合、拡張機能を使用できなくなり、ブラウザ保護は有害なWebサイトをブロックしたり、検索結果の評価を表示したりすることはできません。また、拡張機能はブラウザから削除されます。

8. 拡張機能の設定を完了するには、[**OK**] を選択します。

Firefoxを使用してインターネットを安全に閲覧できるようになります。

ブラウザ拡張機能が正しく動作していることを確認するために次のページをブラウザで開きます: https://unsafe.fstestdomain.com。製品のブロック ページが表示されるはずです。

第 章

4

ファイアウォールについて

トピック :

- コンピュータに対してすべての接続を許可する

*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侵入することを阻止します。

ファイアウォールは、コンピュータとインターネットに接続されている他のコンピュータの接続を制御します。すべての接続を一時的に許可することができます。

4.1 コンピュータに対してすべての接続を許可する

必要に応じてファイアウォールを完全に無効にできます。

お使いのコンピューターとインターネット上の他のコンピューター間のすべての接続を許可するには

1. メニューバーの製品アイコンから製品を開きます。
2. メイン ビューで、[**ウイルスと脅威**] を選択します。
3. に **ウイルスと脅威**表示、選択 [**macOSファイアウォールの設定**]。

   注： システム環境設定を変更するには、管理者権限が必要です。

4. に **ファイアウォール**のタブ **セキュリティとプライバシー**設定では、最初に左下隅にある鍵のアイコンを選択し、管理者パスワードを入力してから、[**ロックを解除する**]。
5. 選択する [**ファイアウォールをオフにする**]。

これで、コンピューターのファイアウォールがオフになります。このコンピューターへのすべての着信接続が許可されます。

注： コンピューターのファイアウォール設定に他の変更を加える場合は、[**ファイアウォールオプション...**]。

付録 A

テクニカル サポート

トピック :

- アカウント ID はどこで確認できますか?
- 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
- 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。

A.1 アカウント ID はどこで確認できますか?

カスタマーサポートに連絡する際に、お客様のアカウントIDをお尋ねることがあります。

アカウントIDを確認するには

1. メニューバーの製品アイコンから製品を開きます。
2. メインビューで、右上隅にある を選択します。
3. [**バージョン情報**] を選択します。
   アカウントIDは、製品のバージョン情報の下に表示されています。

A.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. メニューバーの製品アイコンから製品を開きます。
2. メインビューで、右上隅にある を選択します。
3. [**バージョン情報**] を選択します。
   [**バージョン情報**] ウィンドウには、バージョン情報以外に、アカウントIDや最新のデータベースバージョンなどの情報が表示されます。

A.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. [**アプリケーション**] の下の製品フォルダに移動し、[**サポートツール**] アプリケーションを実行します。
2. 「**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。

   注: ツールを実行するには管理者の権限が必要です。

3. コンピュータ管理者パスワードを入力します。

   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。

4. データ収集が完了したら、結果が含まれている`tar.gz`アーカイブを保存する場所を選択し、[**保存**] を選択します。
   サポートツールで保存されたファイルを示す [**Finder**] ウィンドウが開きます。
5. ファイルを求められたらカスタマーサポートに送信します。

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。

A.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

残念ながら、電話詐欺は増加傾向にあり、詐欺師はソーシャルエンジニアリングを使用して被害者を標的にしています。

このトピックは、これらの呼び出しを特定するのに役立ち、最悪の場合⊠ターゲットにされている場合⊠、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、マイクロソフト、銀行、さらにはネットワーク事業者などの有名な会社の出身であると主張しています。彼らは評判の良い名前を使用しているので、これはあなたをより安心させます。また、知識が豊富で専門用語を使用しているため、正当で信頼できるように見えます。
- 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する（セキュリティ製品を開き、[**[ウイルスと脅威]** > **[フルコンピュータースキャン]**。

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に連絡してサポートチケットを作成している場合は、カスタマーサポートから電話があります。

- 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： 知っている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。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。また、他のパスワードを保護するのと同じように、リモートアクセスデータを保護します。

- 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ということは、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と、コンピュータはウイルス、トロイの木馬、ランサムウェアから保護されます。ブラウジング保護およびバンキング保護機能は、保護のもう1つの層を追加し、オンラインバンキングを安全に参照および実行できるようにします。

標的にされ、すでにセキュリティ製品がインストールされている場合は、すぐに完全なコンピュータスキャンを実行して、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できます。これらは、潜在的に不要なアプリケーション（PUA）と呼ばれます。ただし、この製品では、これらのタイプの電話詐欺からユーザーを保護することはできません。

警戒し、安全に過ごしてください。