# Workstation Security for Mac

17-07-19

# 目次

# 製品を使用するには

トピック：

- *コンピュータの保護状況を確認するには*
- *アンインストール*

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 コンピュータの保護状況を確認するには

「ステータス」画面では、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。

「ステータス」画面を開くには

1. メニューバーにある製品アイコンをクリックします。
2. メニューから[を開く]を選択します。
3. 「ステータス」画面は製品を起動したときに開きます。
   「ステータス」画面では次の操作を行えます。
   - 現在のセキュリティ ステータスを確認する
   - すべての機能が最新の状態であるか確認する
   - ライセンスの残り日数を確認する

### 1.1.1 セキュリティのステータス アイコン

「ステータス」画面のアイコンは、製品と機能の全体ステータスを示します。

次のアイコンを通じて製品とセキュリティ機能のステータスを確認できます。

| 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。 |
|  | 情報 | 特別なステータスが発生していることを示します。<br>機能が正常に動作していて、特定の処理(アップデートのダウンロードなど)が進行中であることを示します。 |
|  | 警告 | コンピュータが保護されていないことを示します。<br>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など)があることを示します。<br>ファイアウォールがすべてのトラフィックをブロックしているときにも表示されます。 |
|  | 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。<br>たとえば、重大な機能が無効になっています。 |

| ステータス アイコン | ステータス | 説明 |
| --- | --- | --- |
| | | ファイアウォールが無効になっている可能性もあります。 |
|  | オフ | 機能が無効になっていることを示します。 |

## 1.2 アンインストール

アプリケーションをごみ箱に移動することで本製品はアンインストールできません。製品のアンインストーラを使用する必要があります。

本製品をアンインストールするには、管理者権限のユーザでログインしている必要があります。

次の操作を行います。

1. 本製品をインストールしたフォルダを開きます。デフォルトでは、「アプリケーション」フォルダが使われます。
2. [<Product_Name>のアンインストール] アイコンをダブルクリックします。
   アンインストールを行うプログラムが開きます。
3. [アンインストール] をクリックします。
   本製品をアンインストールするには管理者のパスワードを入力する必要があります。
4. 管理者のユーザ名とパスワードを入力して、[**OK**] をクリックします。

本製品がシステムからアンインストールされます。

# 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。

## 2.1 ウイルスとマルウェアについて

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。

マルウェアは次の様な害を及ぼす可能性があります。

- Web ブラウザの操作
- 検索内容のリダイレクト
- 不要な広告の表示
- アクセスした Web サイトの記録
- 銀行情報などの個人情報の盗難
- ご利用のコンピュータからのスパムの送信
- ご利用のコンピュータからの他のコンピュータの攻撃

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高くなります。

### 2.1.1 ウイルス

ウイルスは、ファイルに感染して繰り返し自己増殖するプログラムです。他のファイルの内容を変更したり置換したりして、コンピュータに害を及ぼします。

ウイルスは、一般に、ユーザの知らないうちにコンピュータにインストールされるプログラムです。インストールされたウイルスは自己増殖を試みます。ウイルスによって、次のような問題が引き起こされます。

- システム リソースの使用
- ウイルスに感染したコンピュータ上のファイルの変更や破損
- ウイルスに感染したコンピュータを利用して別のコンピュータを感染する試み
- 不正目的でのコンピュータの利用

### 2.1.2 スパイウェア

スパイウェアは、キーボード入力・履歴・パスワード・個人情報などの機密情報をインターネットを通じて記録したり送付したりする悪意のあるプログラムです。

スパイウェアは次のような個人情報を収集する可能性があります。

- 閲覧したインターネット サイト
- ご利用のコンピュータ上のメール アドレス
- パスワード
- クレジットカード番号

スパイウェアは、ユーザの明示的な許可なしでインストールされることが多くあります。よくある仕組みで、有用なプログラムと一緒にインストールされるスパイウェアがあります。また、ブラウザのポップアップ ウィンドウのオプションをクリックすることで意図せずにインストールされるものもあります。

### 2.1.3 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、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、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用できる場合、信用できるアプリケーションとし登録できます。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用できる場合、今後のスキャンから除外することができます。

## 2.2 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。

#### 感染レポートを表示する

感染レポートでは、リアルタイム保護で検出され、ごみ箱に移動されたウイルスとスパイウェアを確認できます。

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クリックします。
2. メニューから [感染レポート] を選択します。

👉 注: 感染レポートにはマニュアル スキャンで検出および削除されたマルウェアは表示されません。

### 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。

#### マニュアルスキャンを実行する

ホーム フォルダまたは特定な場所 (フォルダ、パス、ドライブなど) をスキャンすることができます。

この機能は、不審なファイルやフォルダに対して行うと便利です。

マニュアル スキャンを開始するには

1. メニュー バーにある製品アイコンをクリックします。
2. [スキャンするオブジェクトを指定] を選択します。

   👉 ヒント: [ホーム フォルダをスキャン] を選択するとホーム フォルダにあるファイルをすべてスキャンできます。

   スキャンのオプションを指定するウィンドウが開きます。
3. 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。

製品がブロックしたアプリケーションが安全である、またはアプリケーションに危険性がある場合にサンプルを提供できます。

サンプルを分析用に送信するには

1. ユーザ インターフェースで [ツール] を選択します。
2. [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。

3. 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クリックします。
2. メニューから [更新を確認する] を選択します。
   データーベースが最後にインストールされた日付が表示されます。

# 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。すべてのネットワークトラフィックを一時的にブロックしたり、許可したりすることができます。

## 3.1 ネットワーク接続をすべてブロックする

必要に応じて、コンピュータとインターネットに接続されているコンピュータの間のネットワークトラフィックをすべてブロックできます。

すべてのネットワーク接続をブロックするには

1. メニューバーにある製品アイコンをクリックします。
2. メニューから [を開く] を選択します。
3. ユーザインターフェースで [ツール] を選択します。
4. [すべてのトラフィックをブロックする] をクリックします。

## 3.2 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。

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間の接続をすべて接続するには

1. メニューバーにある製品アイコンをクリックします。
2. メニューから [を開く] を選択します。
3. ユーザインターフェースで [ツール] を選択します。
4. [ファイアウォールを無効にする] をクリックします。

# ブラウザ保護

トピック：



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、F-Secure のマルウェア分析、F-Secure のパートナーに基づいて決まります。

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

## 4.1 ブラウザ保護を有効/無効にする

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するには

1. メニュー バーにある製品アイコンをクリックします。
2. [環境設定] をクリックします。
   「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。
4. ブラウザ保護は、ブラウザの拡張機能 (プラグイン) のインストールを必要とします。対象のブラウザにインストールされていない場合、[ブラウザプラグインをインストールする]をクリックします。
   - Safari の場合、ブラウザ拡張機能をダウンロードして個別にインストールする必要があります。[ブラウザ拡張機能をインストール] をクリックすると拡張機能を自動的にダウンロードし、詳細情報を示す Web ページが開きます。
   - 他のブラウザの場合、拡張機能を手動でダウンロードする必要があります。[ブラウザ拡張機能をインストール] をクリックしたあとに追加の操作は必要はありません。

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。

### 4.1.1 ブラウザ保護を Chrome で使用する

ここでは、ブラウザ保護を Google Chrome Web ブラウザで使用するための設定について説明します。

1. 本製品でブラウザ保護が有効になっていること、および Google Chrome の拡張機能 (プラグイン) がインストールされていることを確認します。
2. Google Chrome で「**Chrome**」 メニューを開き、[オプション] を選択します。
3. 左側のペインにある一覧から「拡張機能」 を選択します。
4. [**Browsing protection by F-Secure**] が一覧にあり、有効であることを確認します。

#### ブラウザ プラグインを Google Chrome に再インストールする

Google Chrome のブラウザ保護拡張機能をアンインストールした場合、Chrome の設定を手動で編集する必要があります。

次の方法でブラウザ保護を Google Chrome でもう一度使用できるようになります。

1. Google Chrome で「**Chrome**」 メニューを開き、[設定] を選択します。
2. 左側のペインにある一覧から「拡張機能」 を選択し、Chrome をバックグラウンドで開いた状態にします。
3. [**Dock**] で [**Finder**] をクリックします。
4. [移動] メニューから [フォルダへ移動] を選択します。
5. 次のフォルダを入力します: `/usr/local/f-secure/browsingprotection/chrome/`
6. [移動] をクリックします。
7. `browsing-protection.chromeextension.crx` ファイルを Chrome の「拡張機能」 ウィンドウにドラッグします。
8. [**Browsing protection by F-Secure**] が一覧にあり、有効であることを確認します。

### 4.1.2 ブラウザ保護を Firefox で使用する

ここでは、ブラウザ保護を Firefox Web ブラウザで使用するための設定について説明します。

1. 本製品でブラウザ保護が有効になっていること、および Firefox の拡張機能 (アドオン) がインストールされていることを確認します。
2. Firefox の「ツール」メニューから [アドオン] を選択します。
3. 左側のペインにある一覧から「拡張機能」を選択します。
4. [ブラウザ保護] が一覧にあり、有効であることを確認します。
   拡張機能が有効でない場合、[有効] をクリックします。

### 4.1.3 ブラウザ保護を Safari で使用する

ここでは、ブラウザ保護を Safari Web ブラウザで使用するための設定について説明します。

1. 本製品でブラウザ保護が有効になっていること、および Safari の機能拡張 (プラグイン) がインストールされていることを確認します。
2. Safari の「Safari」メニューを開き、[環境設定] を選択します。
3. 「機能拡張」タブを開きます。
4. 機能拡張の一覧から [ブラウザ保護] を選択します。
5. [ブラウザ保護] が有効であることを確認します。

## 4.2 ブラウザ保護の評価

ブラウザ保護は、検索エンジンにあるリンクに対して評価を表示します。

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。

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

## 4.3 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。

Web サイトは「許可された Web サイト」に追加されます。

2. 許可された Web サイトを表示するには
   a) メニュー バーにある製品アイコンをクリックします。
   b) [環境設定] をクリックします。
      「ブラウザ保護」タブが開いていることを確認します。

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。

# オンライン バンキングを安全に利用する

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。

バンキング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クリックします。
2. [環境設定] をクリックします。
   「ブラウザ保護」タブが開いていることを確認します。
3. [バンキング保護を有効にする] を選択します。