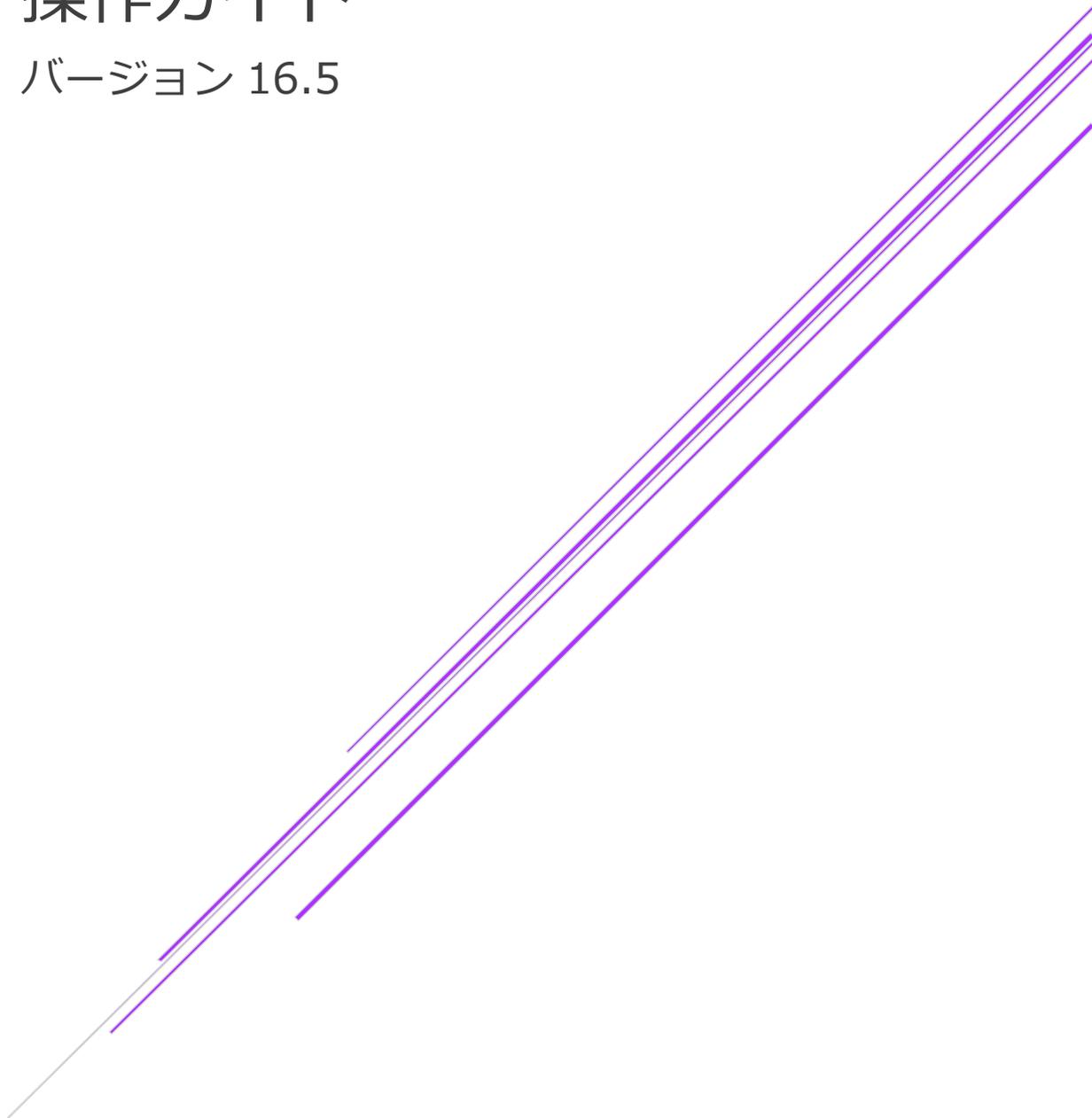


PC プロテクションプラス 操作ガイド

バージョン 16.5



エフセキュア株式会社

改版履歴

履歴	リビジョン	リリース日
初版	1.0.0	2016/3/16
改訂第2版	5.0.0	2017/1/26

● 免責事項

本書は本書執筆／更新時点の情報を基に記述されており、特に断りのない限り、本書内の記述は、本書記載時のバージョンの製品を元にしております。例の中で使用されている会社、名前およびデータは、別途記載のない限り架空のものとなります。

エフセキュア株式会社（以下、弊社）は、本書の情報の正確さに万全を期していますが、本書に記載されている情報の誤り、脱落、または、本書の情報に基づいた運用の結果につきまして、弊社は、如何なる責任も負わないことといたします。本書に記載されている仕様は、予告なく変更することがあります。

● 商標

F-Secure および三角形の記号はエフセキュア株式会社の登録商標です。また、弊社の製品名および記号／ロゴは、いずれも弊社の商標です。本書に記載されている全ての製品名は、該当各社の商標または登録商標です。弊社では、自社に属さない商標および商標名に関する、いかなる所有上の利益も放棄します。

● 複製の禁止

本書の著作権は弊社が保有しており、弊社による許諾無く、本書の一部または全てを複製することはできません。また、譲渡もできません。

目次

はじめに.....	4
1. 動作環境.....	4
1.1 対応 OS.....	4
1.2 対応ハードウェア.....	4
2. 製品.....	5
2.1 「Computer Security」.....	6
2.2 「Online Safety」.....	23
2.3 「サポートサービスのご案内」.....	30

はじめに

本書では、「PC プロテクションプラス」を利用する際の操作方法や機能等について説明します。

1. 動作環境

以下では、本製品の動作要件について説明いたします。

1.1 対応 OS

Windows Vista(32bit/64bit) 全エディション

Windows 7 (32bit/64bit) 全エディション

Windows 8/8.1(32bit/64bit) 全エディション(ARM CPU は未対応)

Windows 10(32bit/64bit) 全エディション(ARM CPU は未対応)

※ 各 OS は、最新のサービスパックの適用をお願いします。

1.2 対応ハードウェア

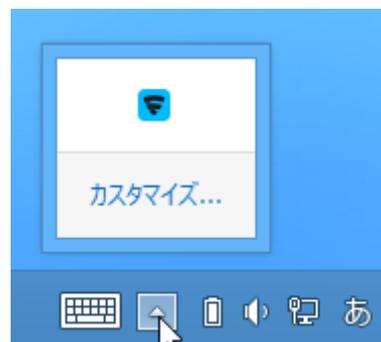
プロセッサ	Intel Pentium4 2GHz 以上
メモリ	1GB 以上(2GB 以上推奨)
ディスク	1.2GB 以上の空き容量

2. 製品

1) 製品機能

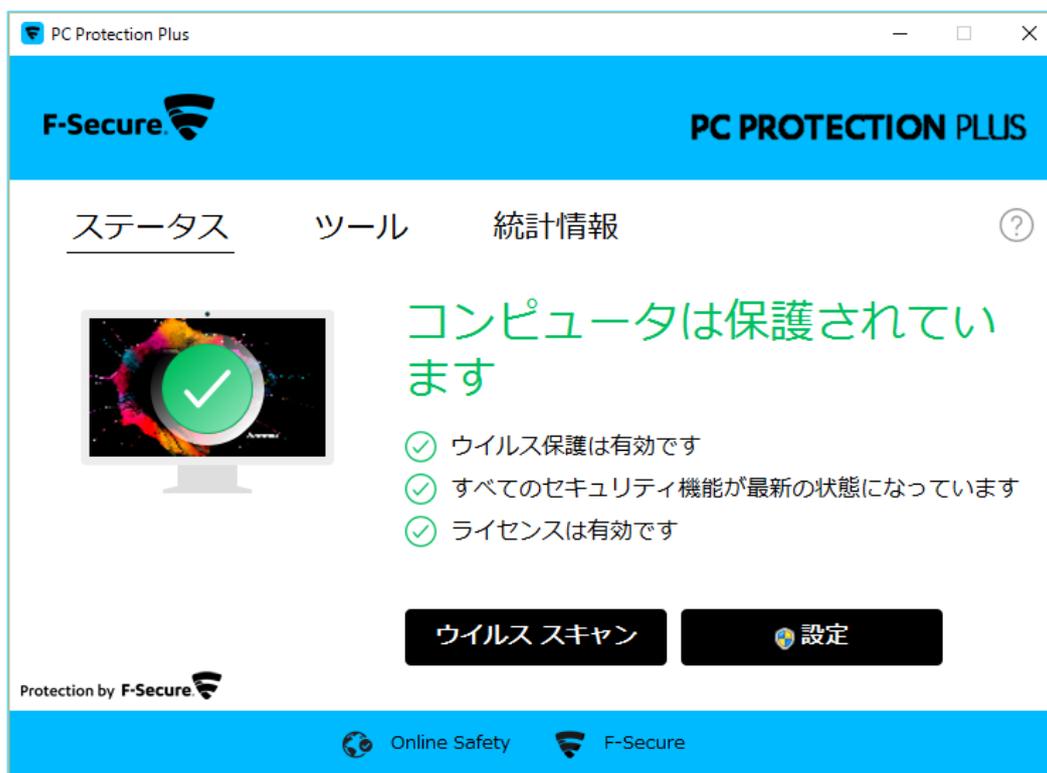
基本的にはインストール後、そのまま有効な製品となっており、特に設定等をして頂く必要はありません。自動的にパターンファイルが更新され、ウイルスから保護されます。

設定メニューやツールをご利用頂く場合は、タスクトレイの F-Secure アイコンかデスクトップのアイコンをクリックします。



2) 製品管理画面

- リアルタイムスキャン等のアンチウイルス機能を管理する「Computer Security」メニューと「Online Safety」メニューの二つで構成されます。

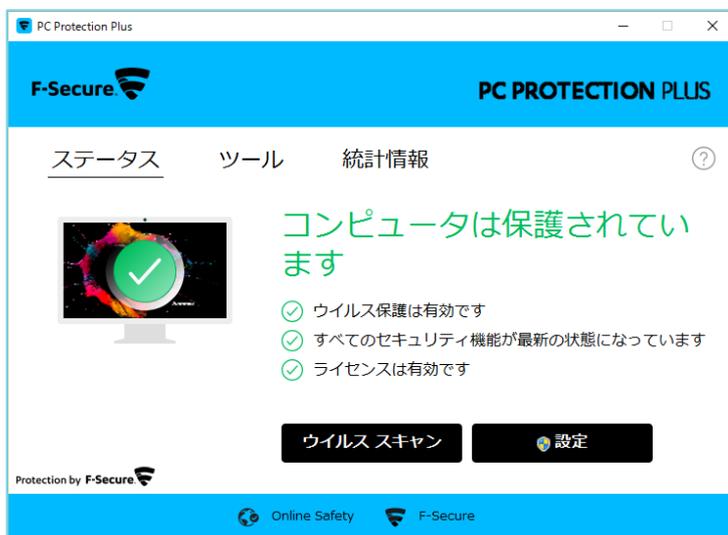


2.1 「Computer Security」

1) 「Computer Security」メイン画面

「ステータス」：製品のトップ画面です。

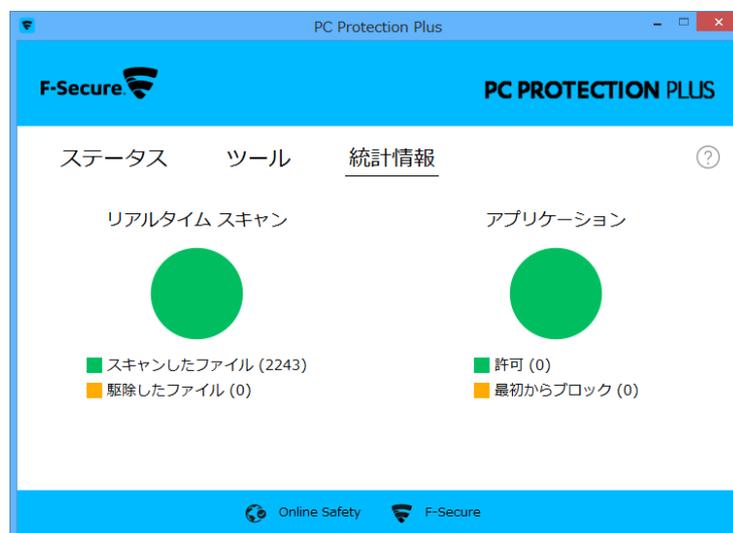
「設定」ボタンから詳細設定画面が開けますが、通常は利用しません。



- 「ツール」：各ツール類の利用画面となっており、通常はこちらを利用します。



- 「統計情報」：ウイルス検知数等がグラフで閲覧できます。



2) 「ツール」メニュー

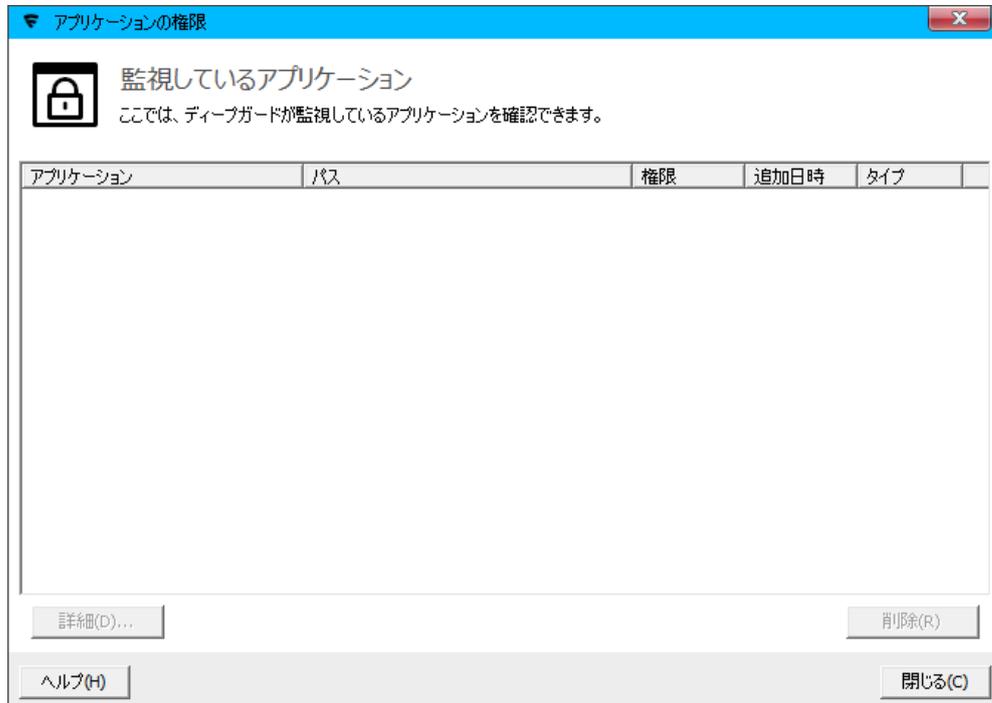


3) 「ツール」メニュー - 詳細スキャン



4) 「ツール」メニュー:アプリケーションの権限

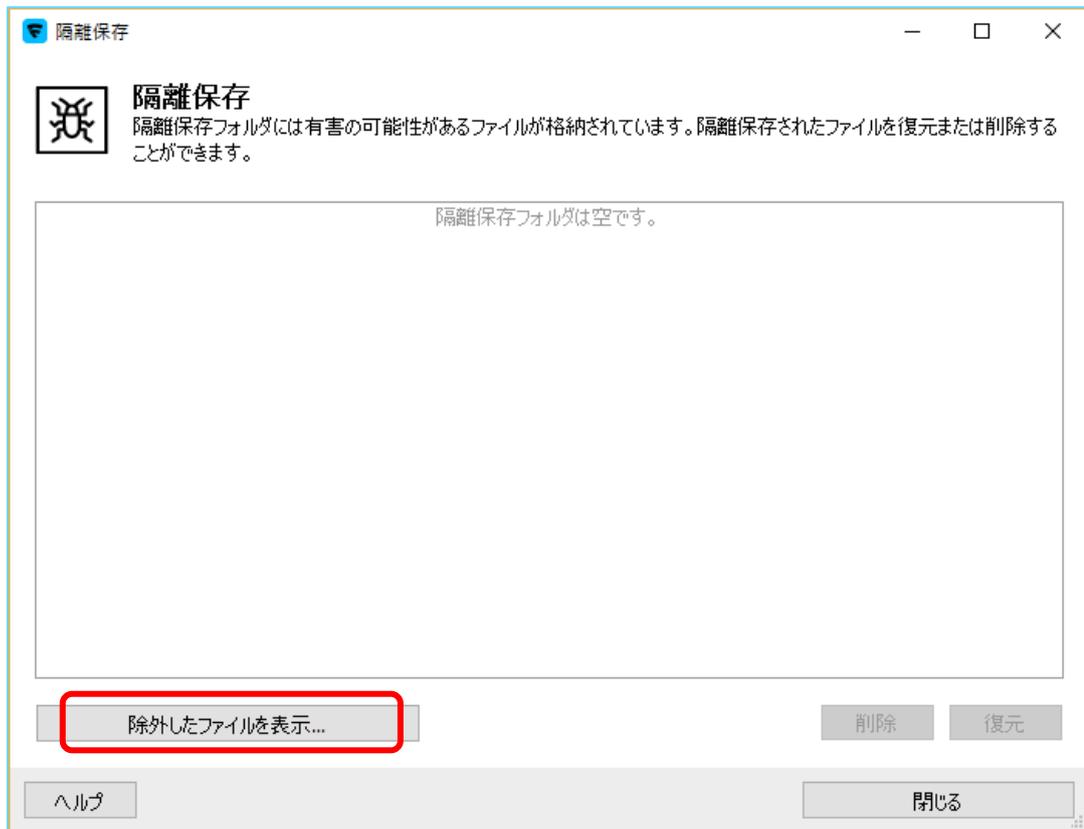
ディープガードで分析されたアプリケーションの一覧が表示されます。
同画面から、誤ってブロックに登録してしまったアプリケーションを削除することができます。



5) 「ツール」メニュー：隔離保存

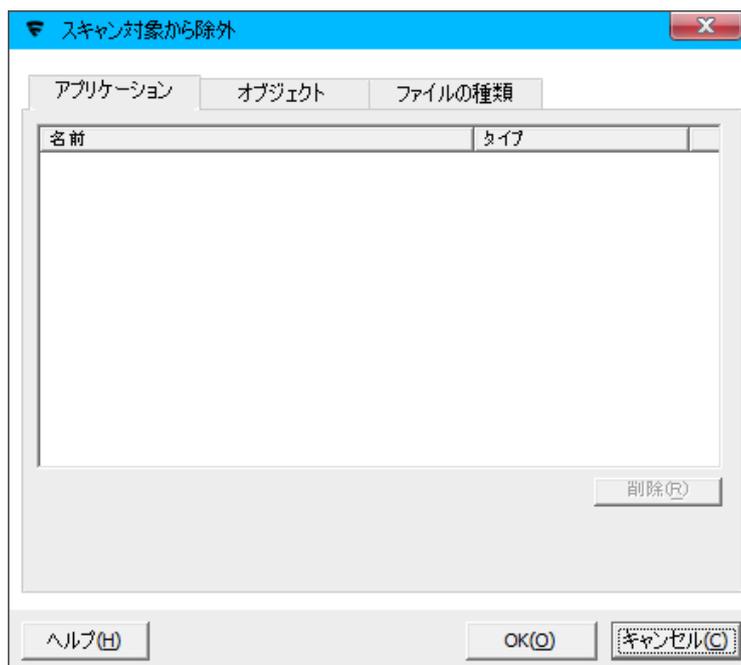
ウイルスの検知後、隔離保存されたものが一覧で表示されます。

「復元」ボタンから元の状態に復元することができます。



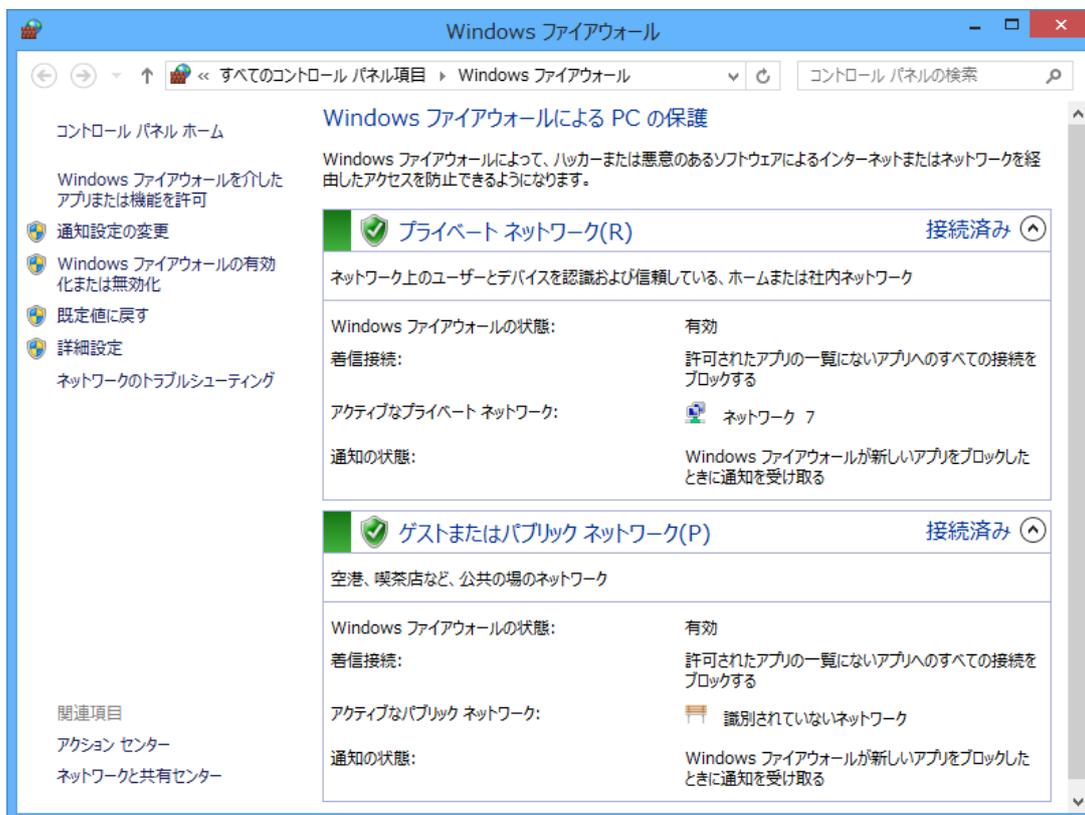
リアルタイムスキャン、マニュアルスキャンの対象から除外したファイルを表示。

除外から対象に戻したい場合は、選択し、削除をクリックします



6) 「ツール」メニュー：Windows ファイアウォールの設定

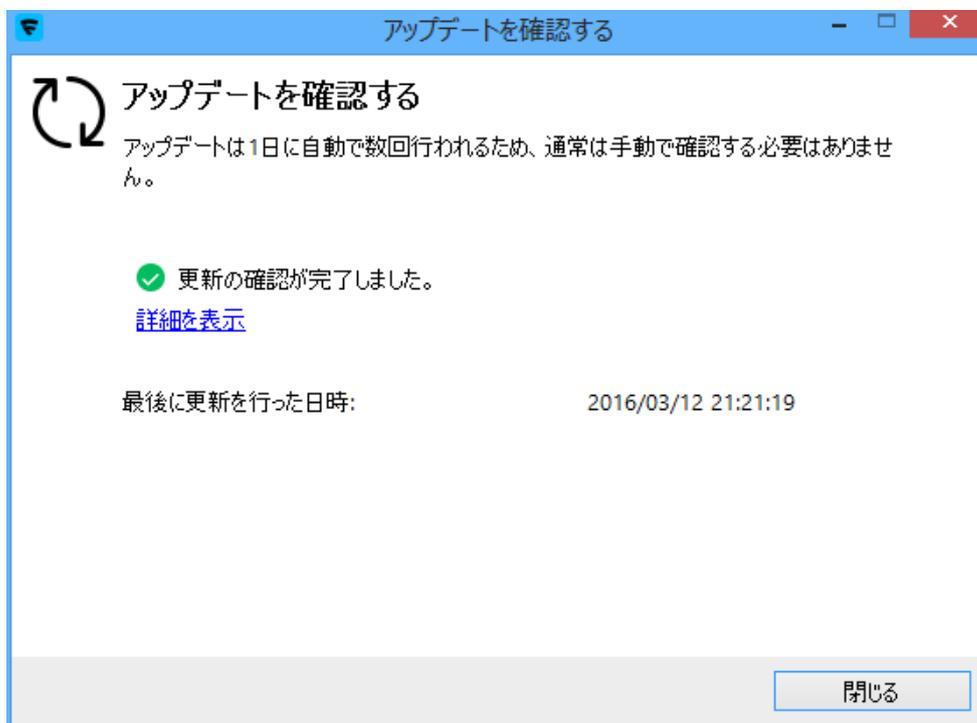
Windows OS 標準のファイアウォール設定画面が開いて、OS 側のファイアウォールの設定を利用します。



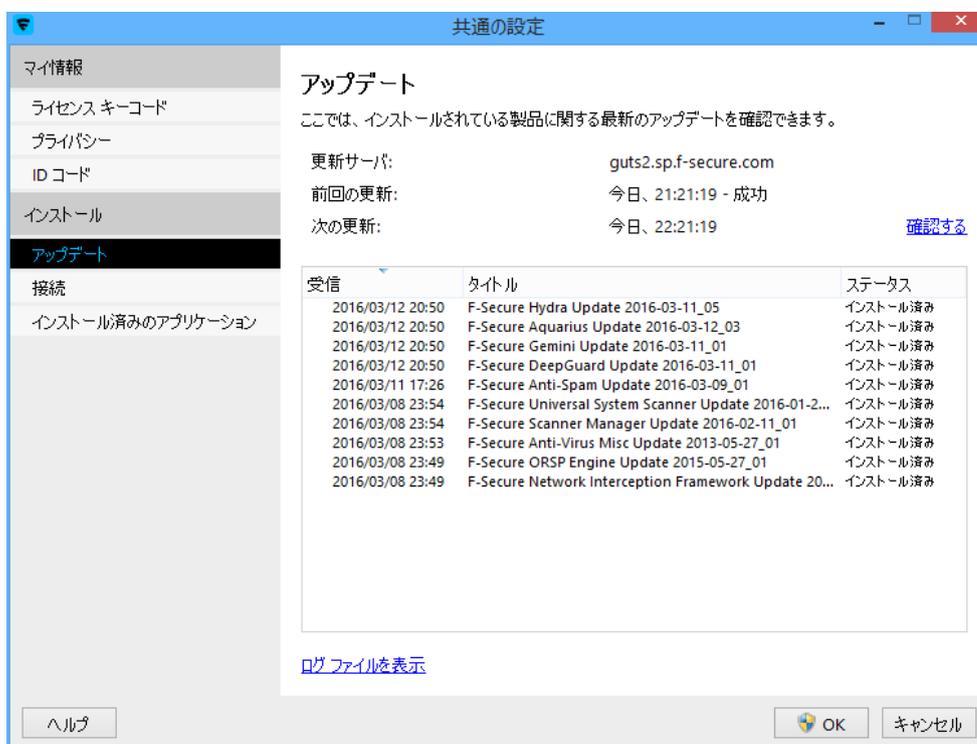
7) 「ツール」メニュー：更新

パターンファイルの更新を実行できます。

通常は自動で更新されるので、この機能を利用する必要はありませんが、パターンファイルの更新ができない場合等の切り分けにご利用頂けます。

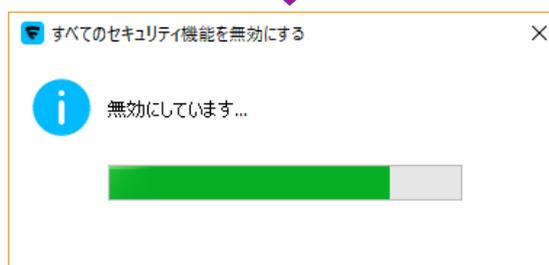
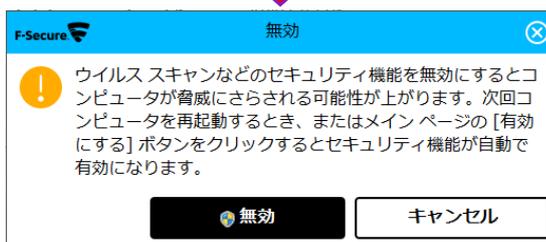


[詳細を表示]をクリックすると下記情報が表示されます。



8) 「ツール」メニュー：すべてのセキュリティ機能を無効にする

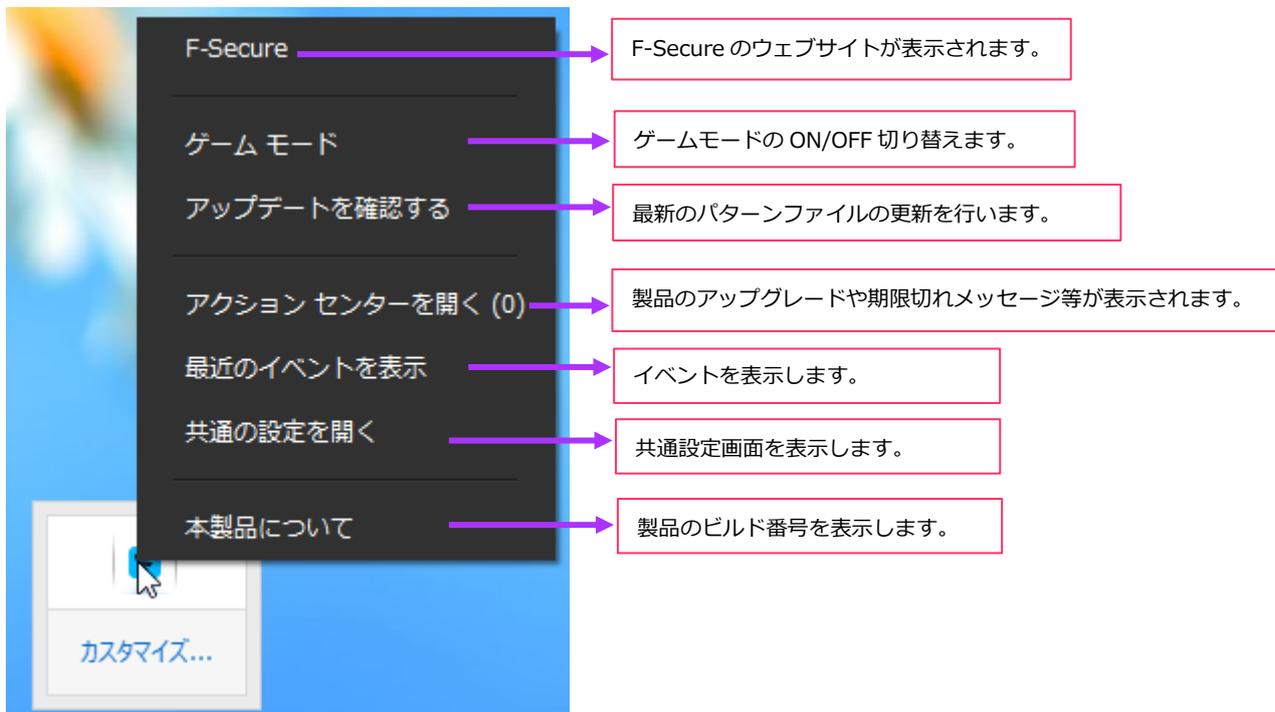
トラブルシューティング時の切り分けの為に、一時的にすべてのセキュリティ機能を無効にすることができます。アンロードとも言います。



「有効にする」をクリックすると有効化されます。

9) 「F-Secure」メニュー

システムトレイのアイコンを右クリックするとメニューが表示されます。

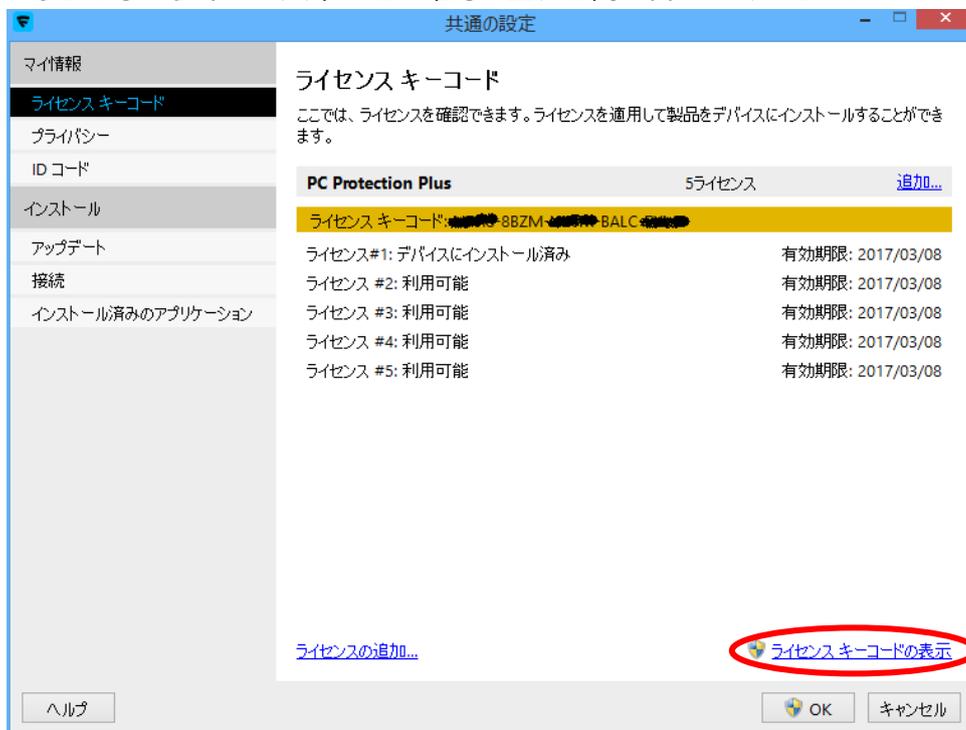


各メイン画面の[?]をクリックするとメニューが表示されます。



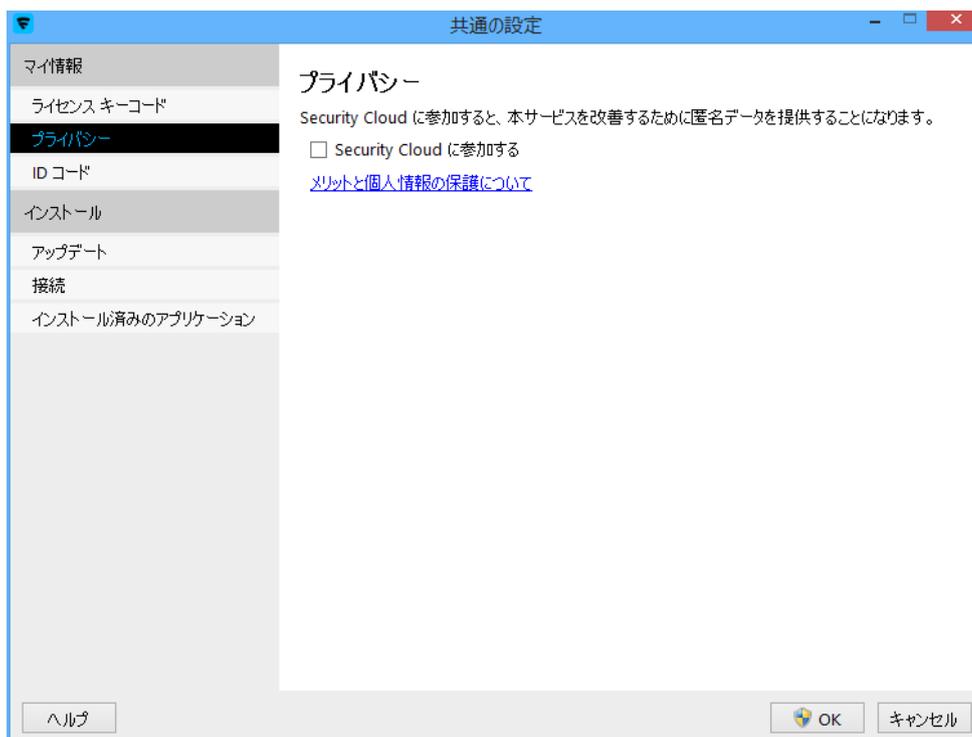
10) 「F-Secure」メニュー：共通の設定 - ライセンスキーコード

「ライセンスキーコード」をクリックすると製品で使用されているライセンスキーが表示されます。ライセンス認証がうまくいかない等の問題をお問い合わせ頂く場合には、あらかじめライセンスキーをご確認の上、お問い合わせください。



11) 「F-Secure」メニュー：共通の設定 - プライバシー

「プライバシー」をクリックすると、Security Cloud への匿名データ提供についての許可/拒否の設定が変更できます。Security Cloud に参加した場合も、個人が特定される情報は送付されることはありません。



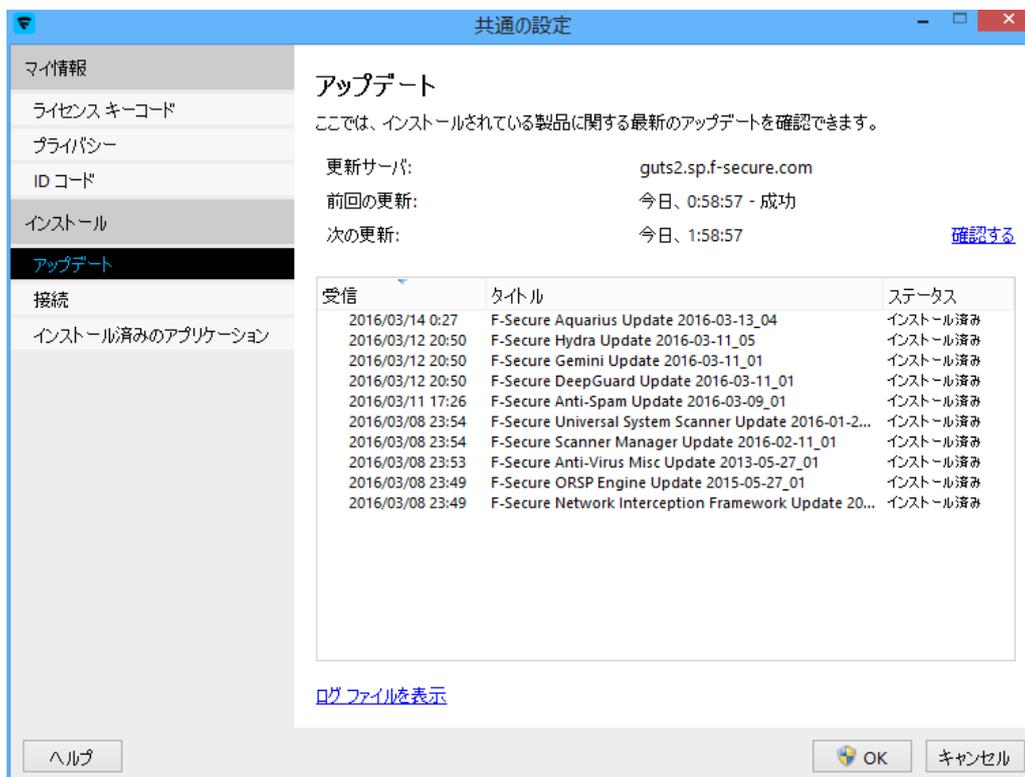
12) 「F-Secure」メニュー：共通の設定 - ID コード

お客様に付与されたアカウント ID と、ご利用のデバイスのデバイス ID が表示されます。サポートセンターにお問い合わせ頂く際にご連絡ください。



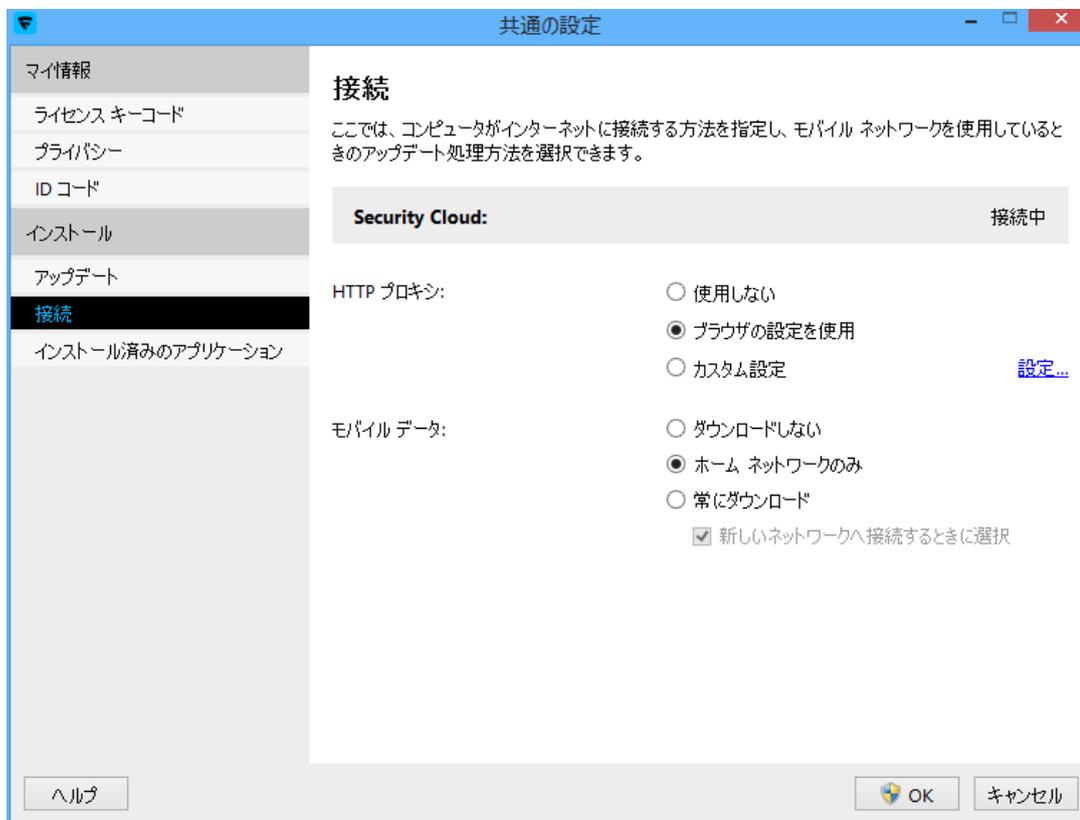
13) 「F-Secure」メニュー：共通の設定 - アップデート

インストール製品のアップデート状況が確認できます。

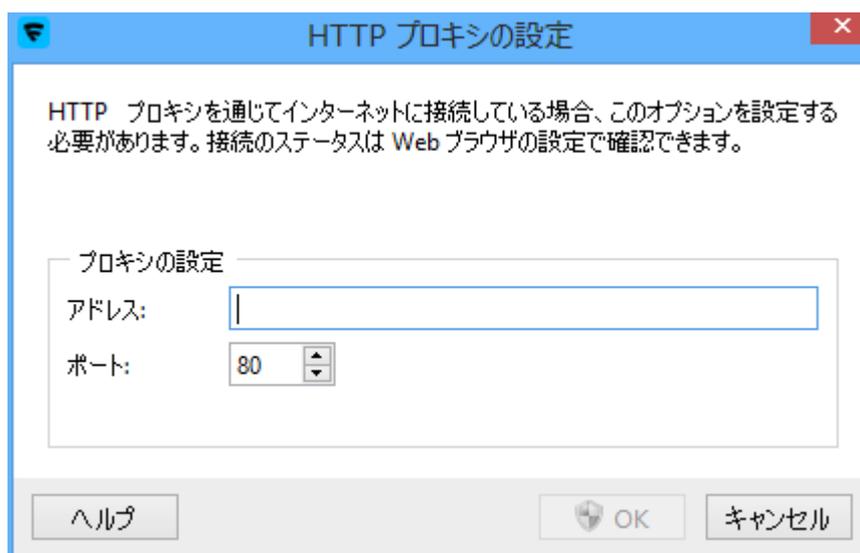


14) 「F-Secure」メニュー：共通の設定 - 接続

インターネットへの接続方法を設定できます。常時接続環境であれば特に設定変更の必要はありません。プロキシを利用する必要がある場合も、基本的にはブラウザの設定を参照する設定（デフォルト設定）で問題ありません。

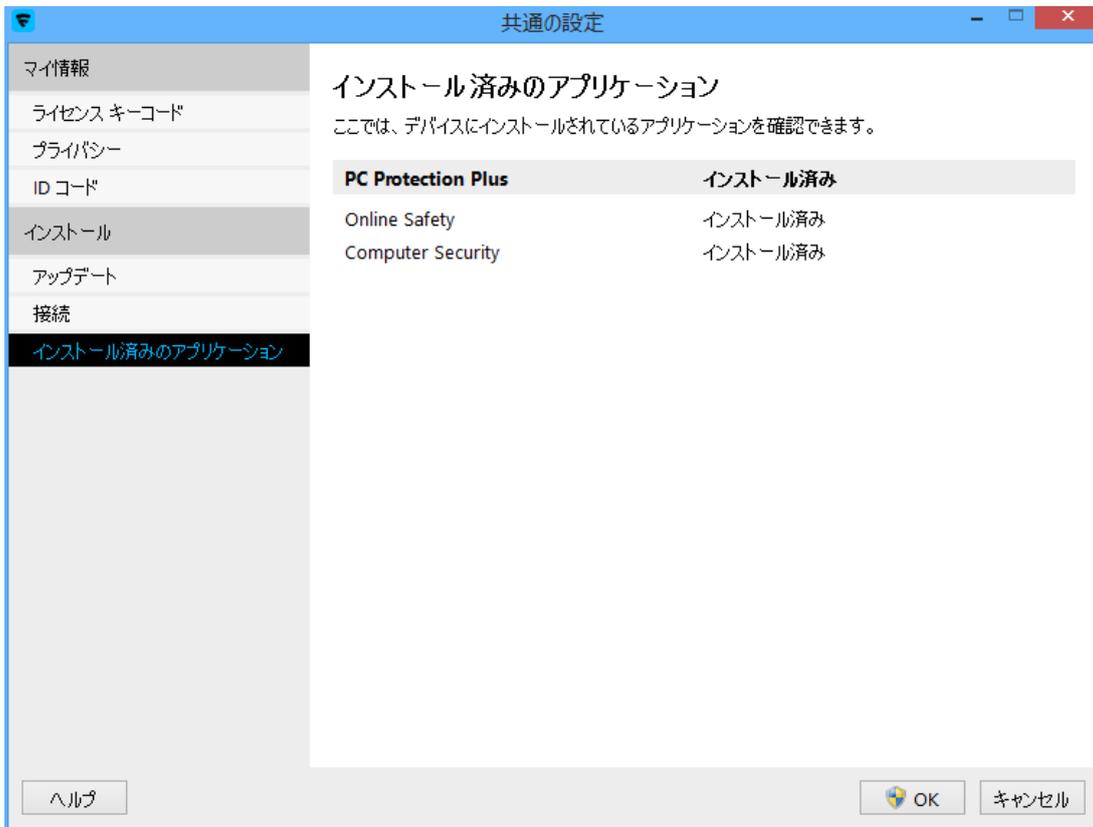


[設定]をクリックすると、HTTP プロキシの設定を行うことができます。



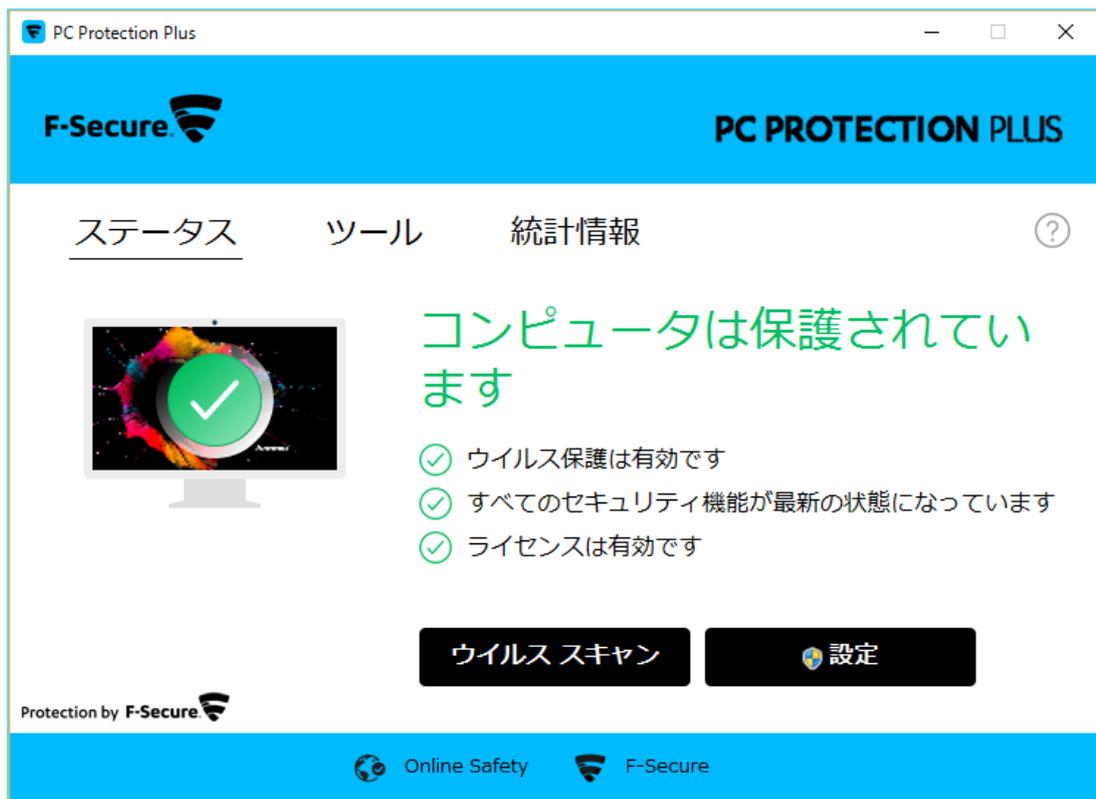
15) 「F-Secure」メニュー：共通の設定 - インストール済みのアプリケーション

デバイスにインストールされているアプリケーションを確認できます。



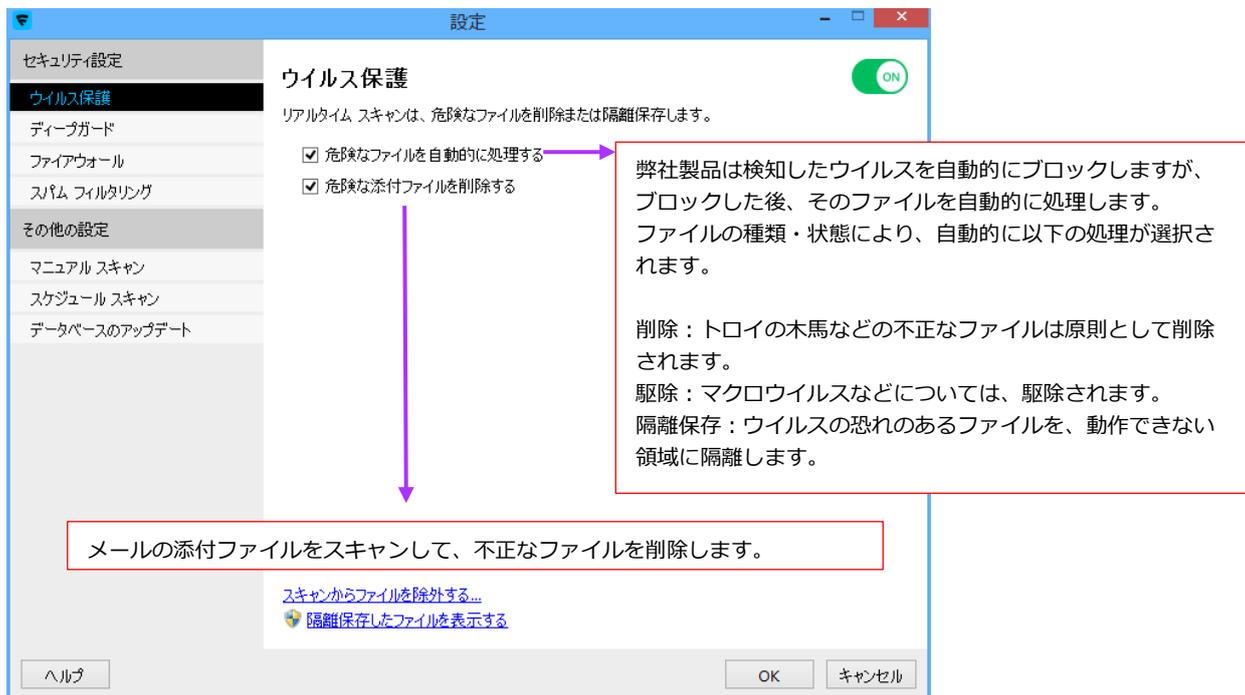
16)メイン画面の設定

同画面は上級者用のメニューとなっており、通常、使用する必要はありません。基本的には、特定の環境での使用や、アプリケーションとの競合を避ける目的で、幾つかの機能を無効化したり、トラブルシューティング時に切り分けに用いられったりするものと理解ください。[設定]をクリックすると詳細設定画面が表示されます。



17)設定 : ウイルス保護

リアルタイムスキャンの設定を行えます。



設定

セキュリティ設定

ウイルス保護 ON

リアルタイム スキャンは、危険なファイルを削除または隔離保存します。

危険なファイルを自動的に処理する

危険な添付ファイルを削除する

弊社製品は検知したウイルスを自動的にブロックしますが、ブロックした後、そのファイルを自動的に処理します。ファイルの種類・状態により、自動的に以下の処理が選択されます。

削除：トロイの木馬などの不正なファイルは原則として削除されます。

駆除：マクロウイルスなどについては、駆除されます。

隔離保存：ウイルスの恐れのあるファイルを、動作できない領域に隔離します。

メールの添付ファイルをスキャンして、不正なファイルを削除します。

[スキャンからファイルを除外する...](#)

[隔離保存したファイルを表示する](#)

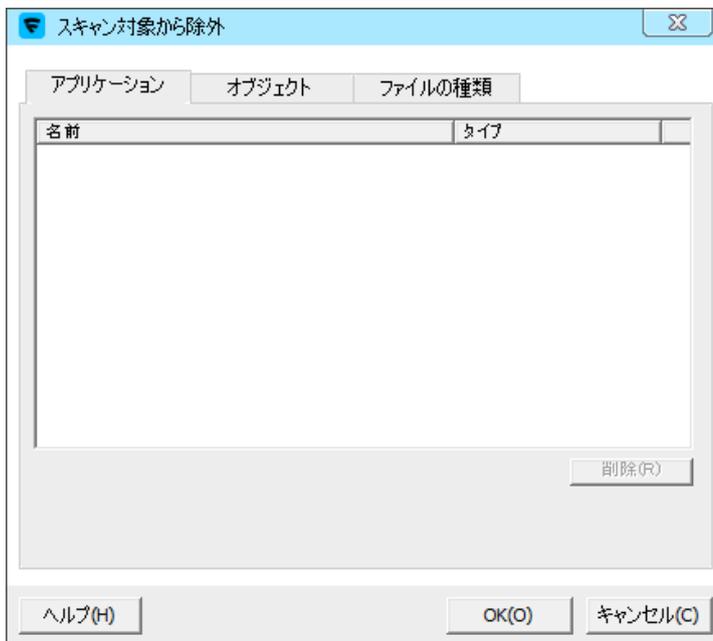
ヘルプ OK キャンセル

18)設定 : ウイルス保護 - スキャンからファイルを除外する

ウイルススキャンの対象から特定のファイルやフォルダを除外することができます。

スキャンからファイルを除外する

[隔離保存したファイルを表示する](#)



スキャン対象から除外

アプリケーション オブジェクト ファイルの種類

名前	タイプ

削除(R)

ヘルプ(H) OK(O) キャンセル(C)

19)設定：リアルタイムスキャン - 隔離保存したファイルを表示する

ウイルスの検知後、隔離保存されたものが一覧で表示されます。「復元」ボタンから元の状態に復元することができます。

スキャンからファイルを除外する...
 隔離保存したファイルを表示する



20)設定：ディープガード

未知のウイルス対策機能である、ディープガードの設定を変更できます。

有効にすると、特定のアプリケーションに対する常時監視を解除します。

ふるまい検知によりプログラムの不審な動作が検出されると、警告メッセージを表示します。

エクスプロイト(脆弱性を悪用した攻撃)が検出されると、警告メッセージが表示されます。

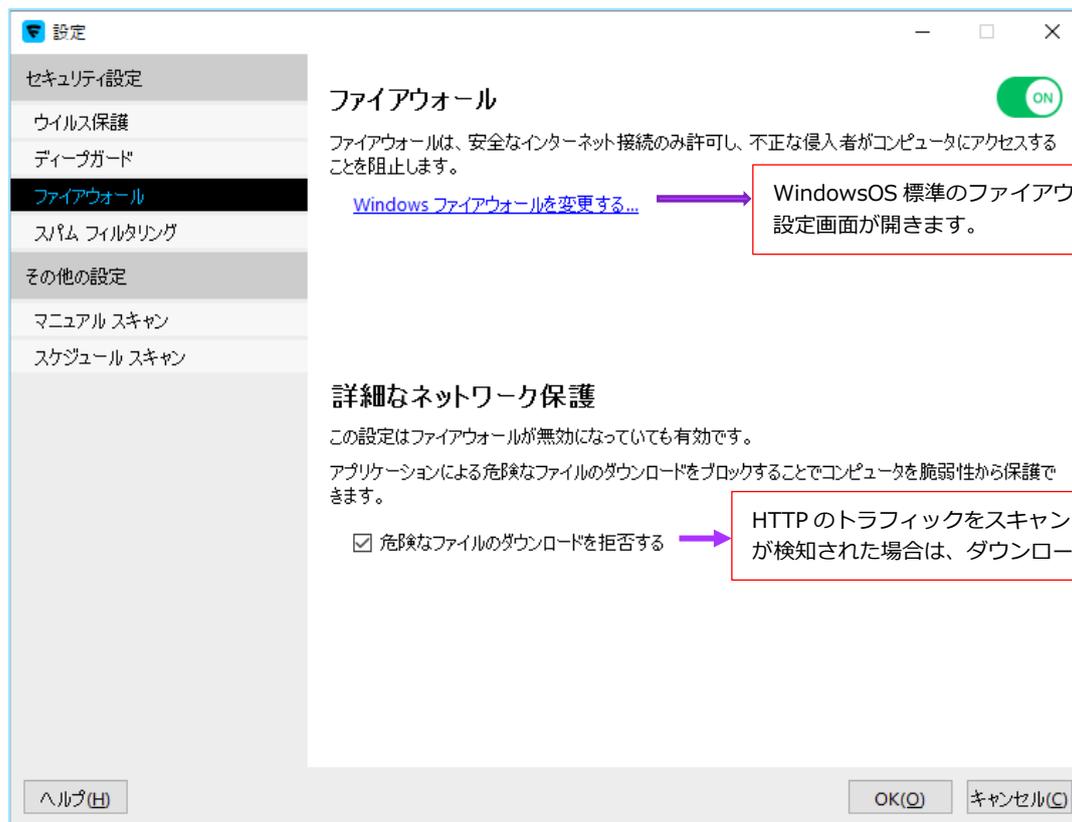
不正なプログラムが、外部と通信しようとしている恐れがある場合に警告メッセージを表示します。

アプリケーションの権限を変更する...

ディープガードで監視、検出されたプログラムの一覧を表示します。

21)設定 : ファイアウォール

ファイアウォールの設定を変更できます。



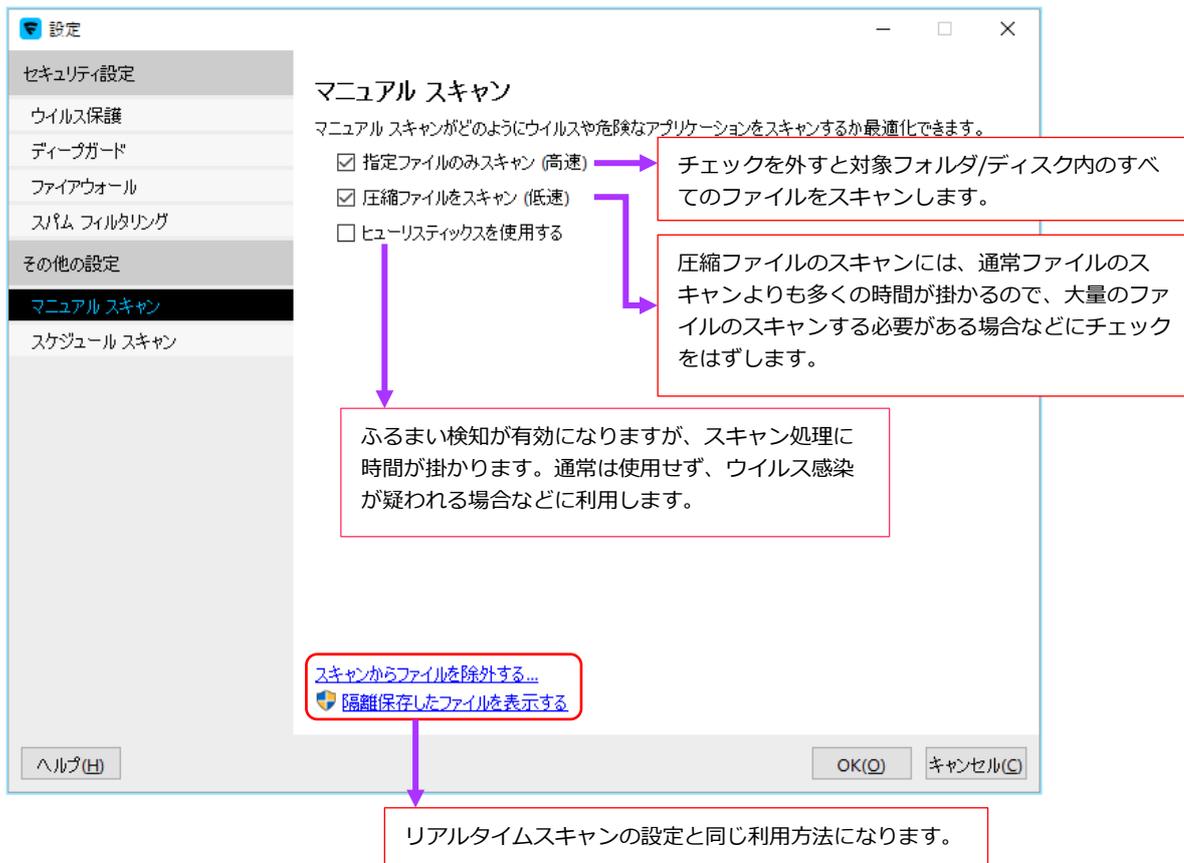
22)設定 : スпамフィルタリング

スパム/フィッシングフィルタリングと検出されたメールの件名に[SPAM]を追加します



23)設定 : マニュアルスキャン

マニュアルスキャンの設定を変更できます。



マニュアル スキャン
 マニュアル スキャンがどのようにウイルスや危険なアプリケーションをスキャンするか最適化できます。

- 指定ファイルのみスキャン (高速) → チェックを外すと対象フォルダ/ディスク内のすべてのファイルのスキャンします。
- 圧縮ファイルをスキャン (低速) → 圧縮ファイルのスキャンには、通常ファイルのスキャンよりも多くの時間が掛かるので、大量のファイルのスキャンする必要がある場合などにチェックをはずします。
- ヒューリスティックスを使用する → ふるまい検知が有効になりますが、スキャン処理に時間が掛かります。通常は使用せず、ウイルス感染が疑われる場合などに利用します。

ヘルプ(H) OK(O) キャンセル(C)

スキャンからファイルを除外する...
 隔離保存したファイルを表示する

リアルタイムスキャンの設定と同じ利用方法になります。

24)設定 : スケジュールスキャン

日時を指定して、マニュアルスキャンを実行することができます。



スケジュール スキャン ON

スケジュール スキャンは指定の時間でウイルスと危険なアプリケーションに対するスキャンを行います:

<input type="radio"/> 日単位	<input type="checkbox"/> 月曜日	<input type="checkbox"/> 土曜日
<input checked="" type="radio"/> 週単位	<input type="checkbox"/> 火曜日	<input type="checkbox"/> 日曜日
<input type="radio"/> 月単位	<input type="checkbox"/> 水曜日	
	<input type="checkbox"/> 木曜日	
	<input checked="" type="checkbox"/> 金曜日	

開始時刻: 0:00
 指定アイドル時間が経過した場合: 5分

ヘルプ(H) OK(O) キャンセル(C)

スケジュール スキャンは、圧縮ファイルのスキャンと危険なファイルの自動駆除を除き、マニュアル スキャンと同じ設定を使用します。

2.2 「Online Safety」

「Online Safety」メニュー

1) 「Online Safety」設定画面

メイン画面から[Online Safety]をクリックします。



初めて[Online Safety]を立ち上げた時には下記画面が表示されます。「今後、このダイアログを表示しない」にチェックを入れると、次回から表示されなくなります。

[閉じる]をクリックします。

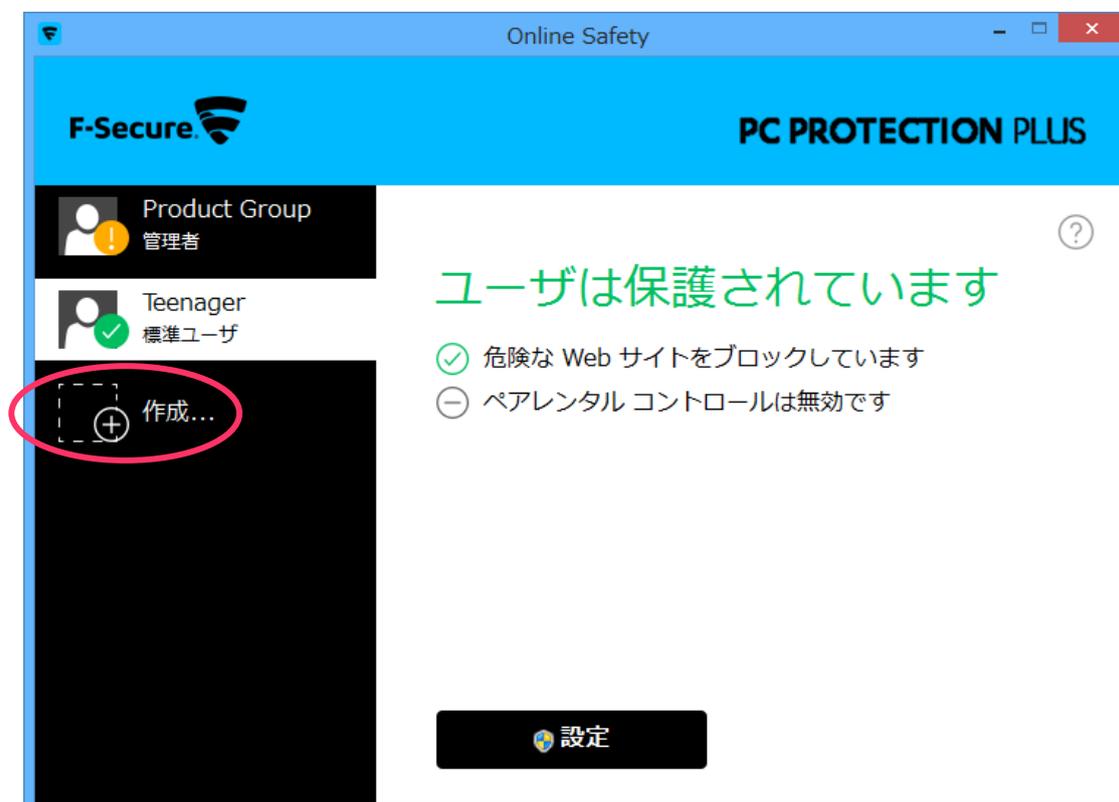


Online Safety の設定画面が表示されます。設定を行うユーザを選択し、[設定]をクリックすることで、詳細設定を行います。



2) 「Online Safety」：アカウントの追加

Windows OS 標準のアカウント管理より新しいアカウントを追加できます。



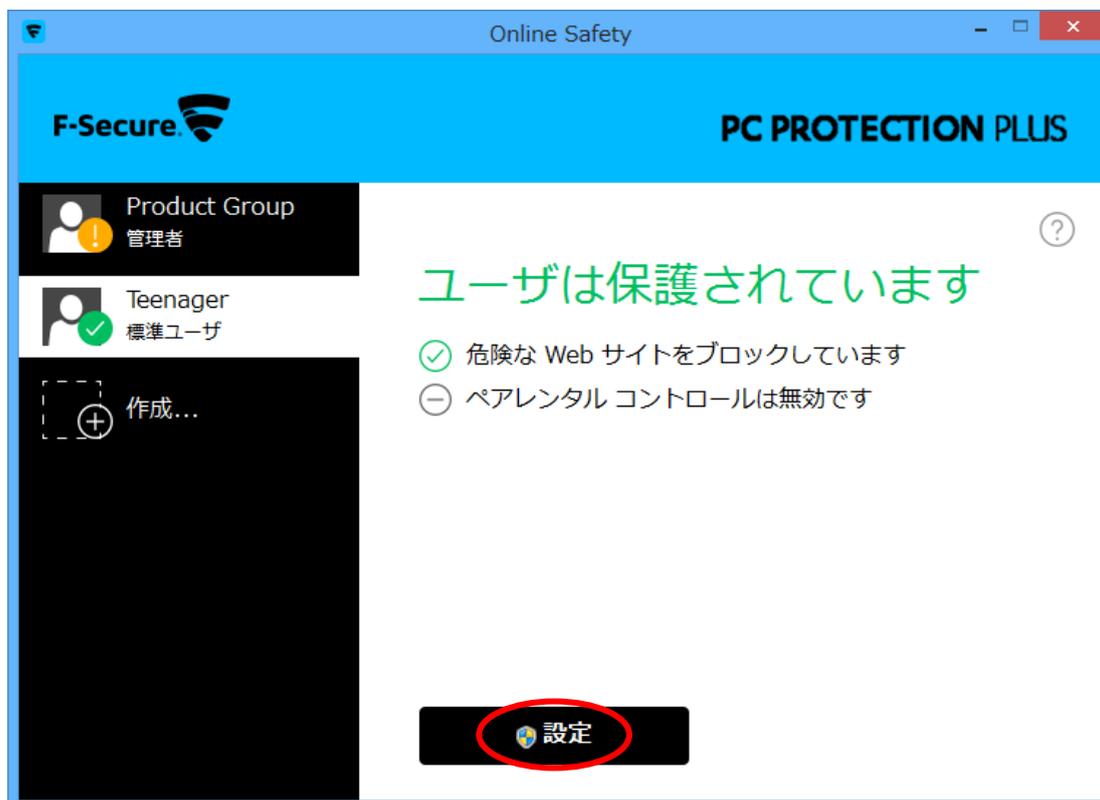
[作成]をクリックすると、下記 Windows OS 標準のアカウント管理画面が表示されますので、新しいアカウントを追加してください。



3) 「Online Safety」：設定

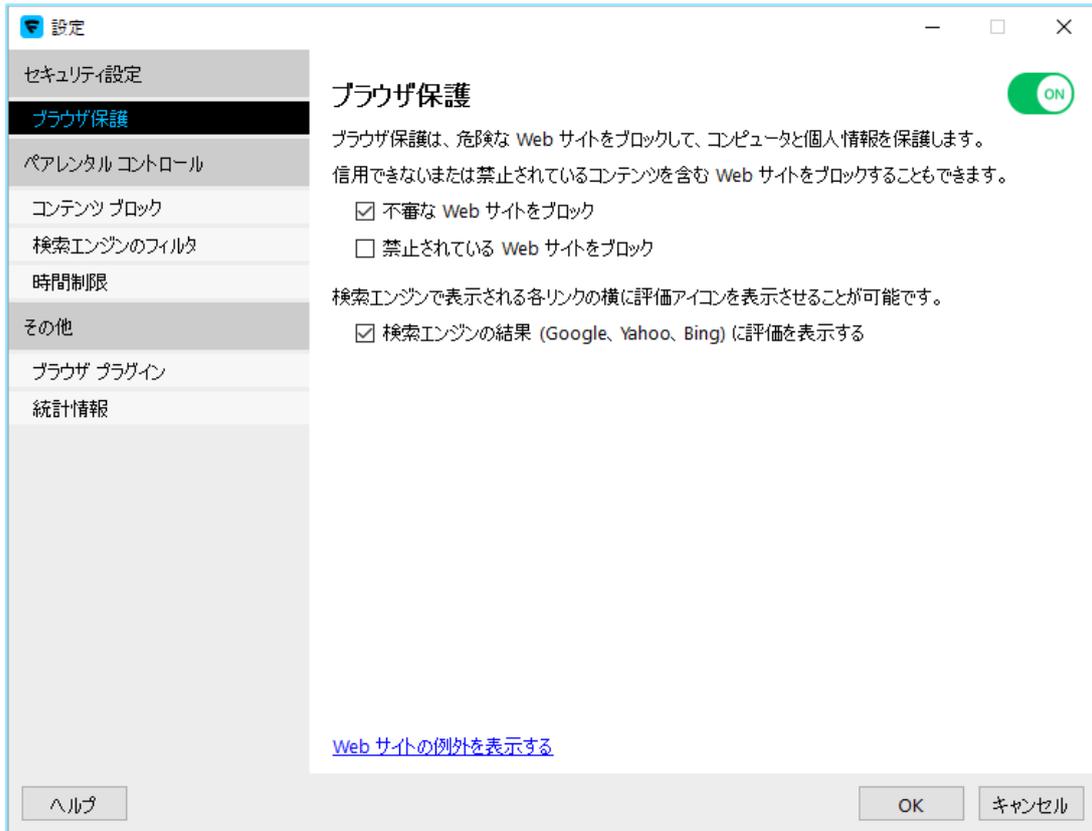
「ブラウザ保護」や「コンテンツブロック」を設定します。

ここではユーザ「Teenager」を選択し、[設定]をクリックします。



4) 「Online Safety」 : ブラウザ保護

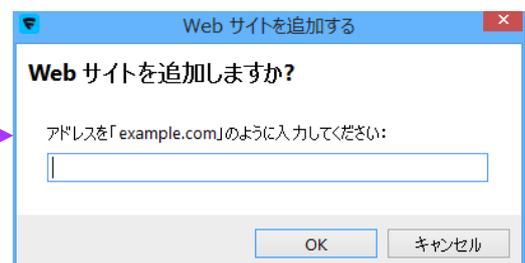
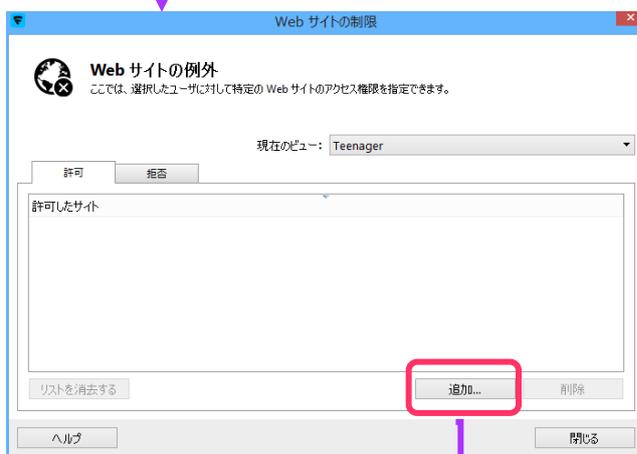
Web サイトの安全性に関する評価表示をユーザに表示します。
[ON]にすることで有効になります。



5) 「Online Safety」 : ブラウザ保護 - Web サイトの例外を表示する

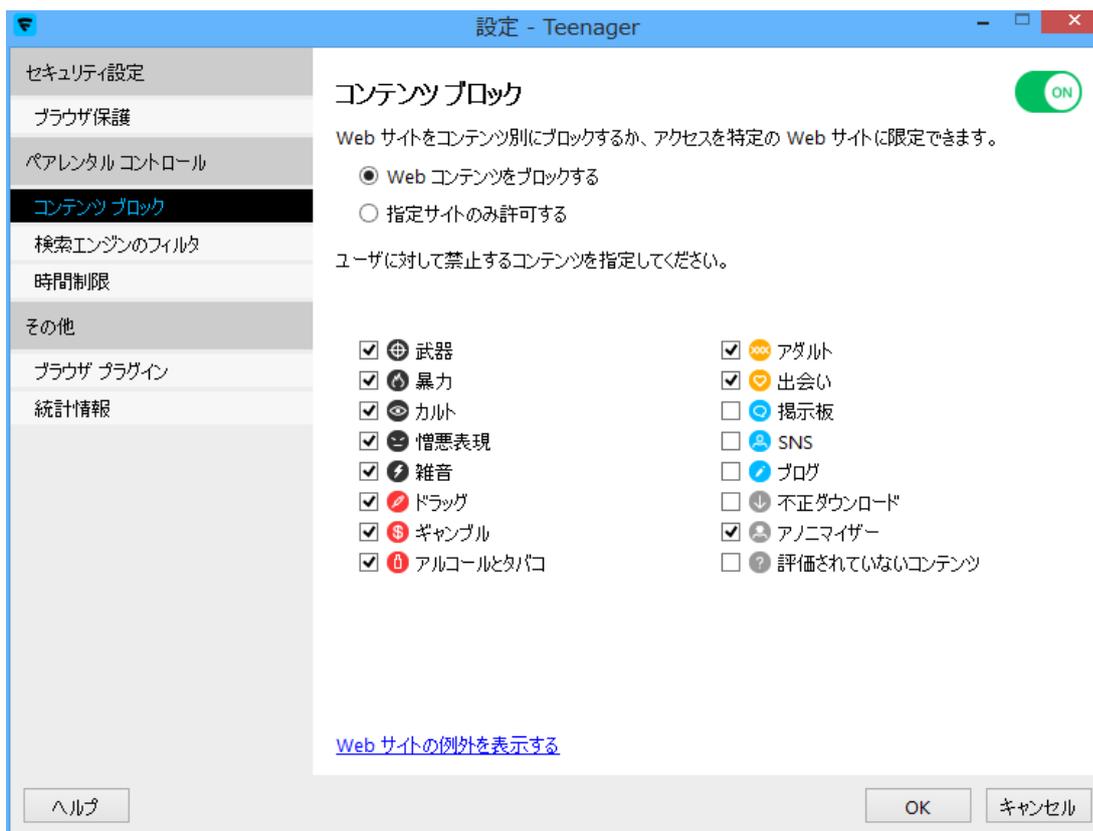
ユーザ毎に対して、閲覧を許可する web サイトのリストや閲覧を禁止する web サイトのリストを作成できます。

[Web サイトの例外を表示する](#)



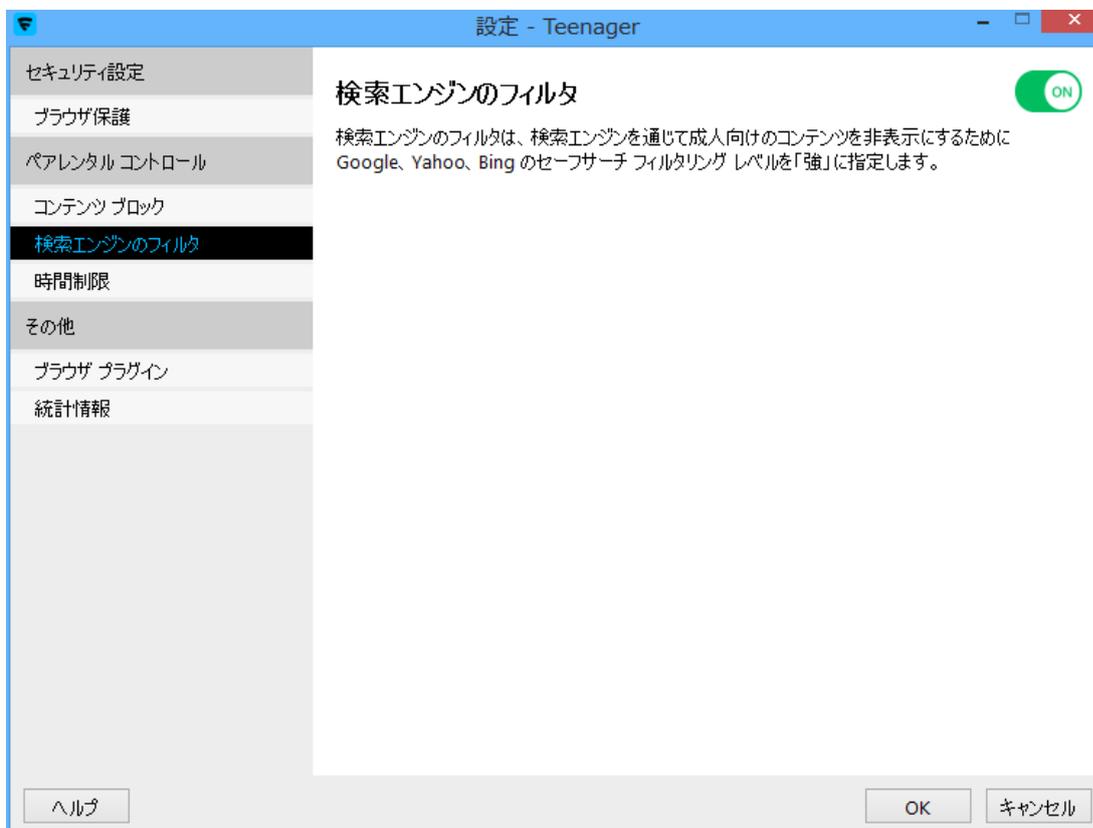
6) 「Online Safety」：コンテンツブロック

選択した Web コンテンツを含む Web ページのアクセスをブロックできます。



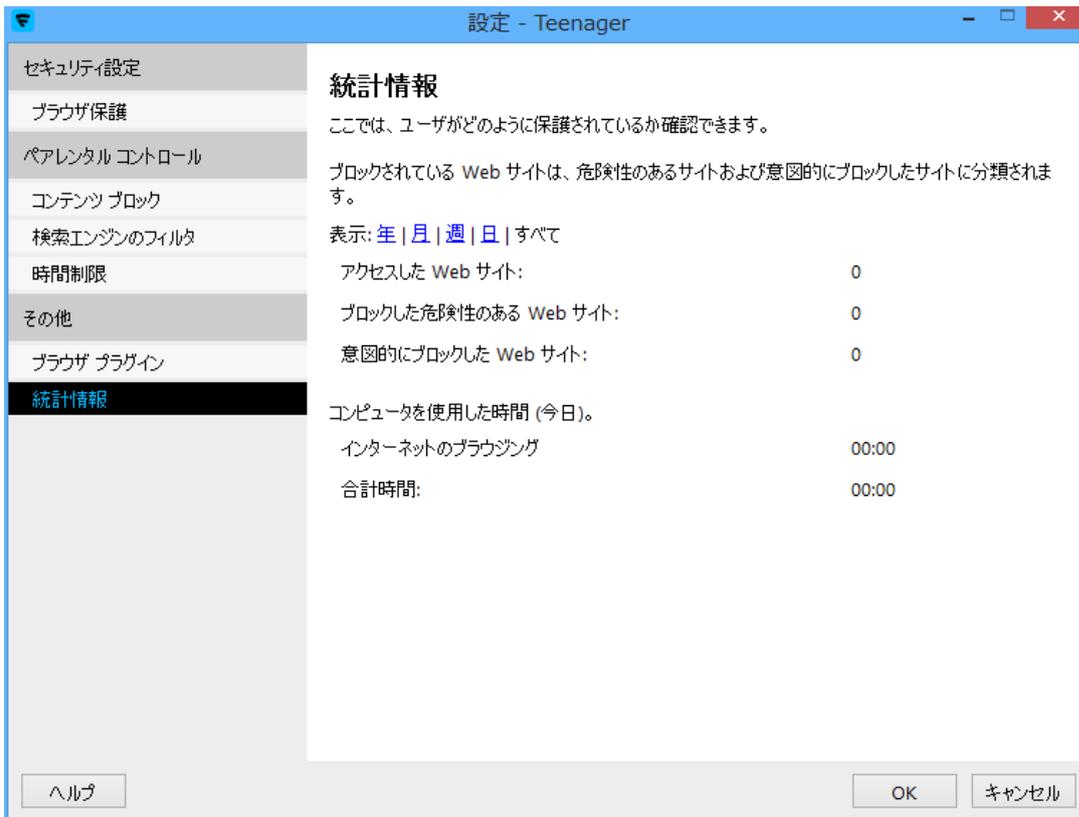
7) 「Online Safety」：検索エンジンのフィルタ

検索エンジンサーチフィルタを使用して検索結果に不適切なコンテンツを表示しないようにします。



10) 「Online Safety」：統計情報

ユーザーごとにアクセス/ブロックした Web サイトの情報を表示します。



統計情報

ここでは、ユーザーがどのように保護されているか確認できます。

ブロックされている Web サイトは、危険性のあるサイトおよび意図的にブロックしたサイトに分類されます。

表示: 年 | 月 | 週 | 日 | すべて

アクセスした Web サイト:	0
ブロックした危険性のある Web サイト:	0
意図的にブロックした Web サイト:	0

コンピュータを使用した時間 (今日)。

インターネットのブラウジング	00:00
合計時間:	00:00

ヘルプ OK キャンセル

2.3 「サポートサービスのご案内」

■製品サポートページ

http://www.catv-web.jp/pscs_faq/

「FAQ」に直接アクセスできます。

FAQ には、よくある質問とその解決策が項目別にまとめられています。

「エフセキュア PCプロテクション」を使っていて困ったときは、まずはFAQをご覧ください。

■サポートサービス

「製品サポートページ」や「オンラインヘルプ」で問題を解決できない場合は、電話またはメールで、ご契約のインターネットサービスプロバイダーまでお問い合わせください。

■メールでのお問合せ

「エフセキュア PCプロテクション」をご使用中、なんらかのトラブルがあった場合は、トラブルの内容を記載したメールに「診断情報 (fsdiag)」を添付して、サポートセンターへ送信してください。

「診断情報 (fsdiag)」は、以下の手順で自動作成できます。

- ① Windows の[スタート]ボタンから、[全てのプログラム (アプリ)] → [F-Secure] → [F-Secure サポートツール] クリック。
- ② 「診断ツールを実行」をクリックします。(処理に時間がやや掛かります)
- ③ 終了メッセージで [閉じる] ボタンをクリックします。
- ④ デスクトップに「診断情報 (fsdiag)」が作成されます。

トラブルの内容を記載したメールに「fsdiag」を添付してサポートセンターへ送信してください。