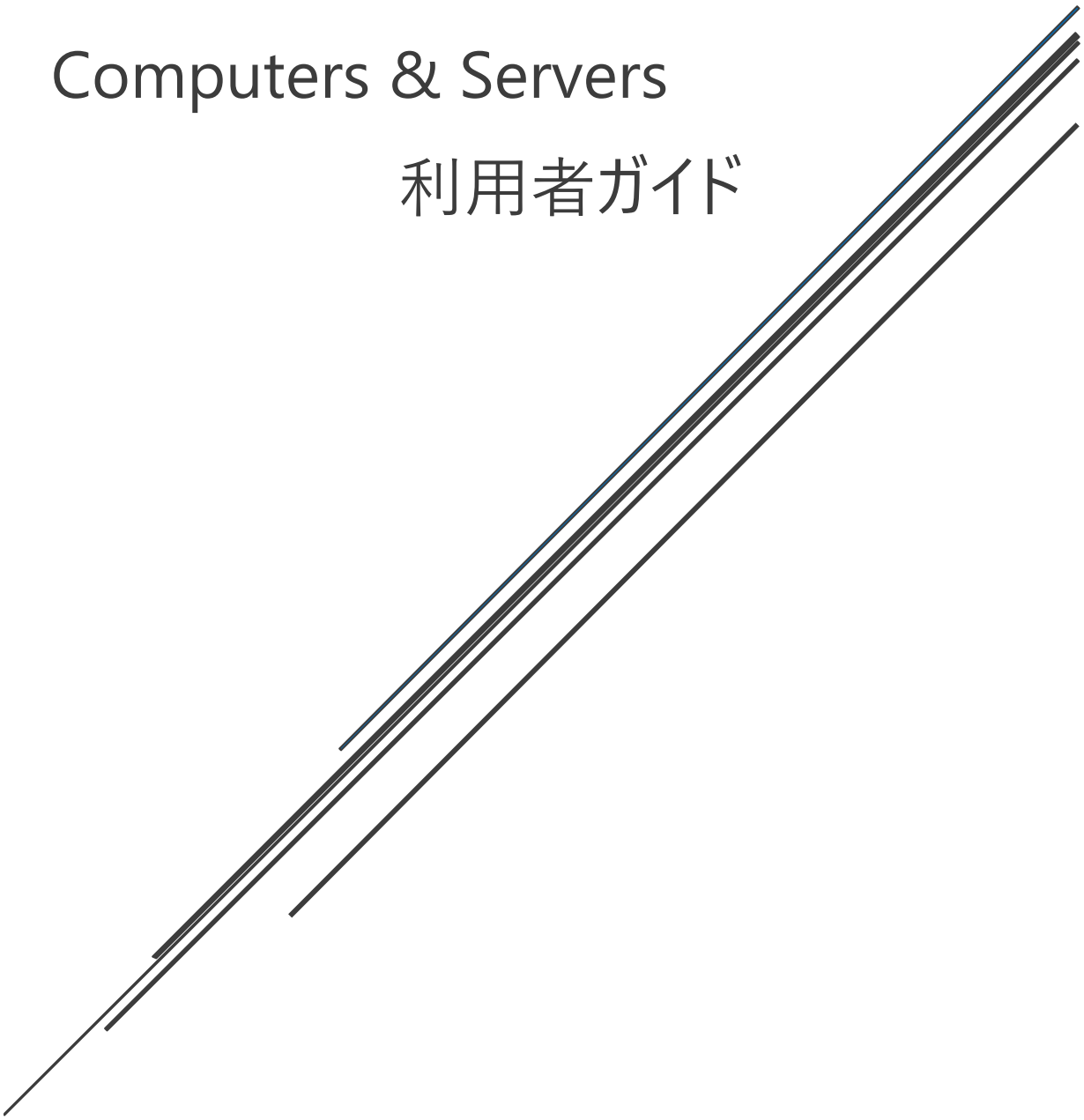
WithSecure™
Elements Endpoint Protection
Computers & Servers
利用者ガイド



WITH secure
ウィズセキュア株式会社

改版履歴

履歴	リビジョン	リリース日
初版	1.0.0	2020/06/28
問い合わせアドレスの変更	1.0.1	2020/07/19

1. はじめに

1.1　適用

この利用者ガイドでは、WithSecure™ Elements Endpoint Protection, Computers Edition（以下 Elements EPP）および WithSecure™ Elements Endpoint Protection, Servers Edition (以下 Elements EPP Servers) の利用者を対象に、インストール方法や使い方について解説しています。WithSecure™ Elements Security Center（以下 Elements Security Center）を利用される管理者は WithSecure™ Elements Security Center ガイドを参照下さい。
なお、本書では Elements EPP の画面を利用して説明していますが、Elements EPP Servers でもインストーラを含めて内容は同じです。
Premium 版でしか利用できない機能には Premium 版であることを明記しています。

1.2　初めてお使い頂く時に

Elements EPP/ Elements EPP Servers の各種機能は、通常のオフィス環境で使用されることを想定したデフォルトのプロフィール設定値に従い動作を開始します。
Elements Security Center から新たなプロフィール設定を受信すると、Elements Security Center で設定された新しいプロフィール設定値に従った動作を開始します。
「ディープガード」機能は未知のマルウェア対策として非常に有効ですので、通常は無効にしないで『有効』のまま使用することを強く推奨します。

1.3　参考ドキュメント

以下のドキュメントも参考にしてください。

Elements EPP (Windows) ガイド
https://help.f-secure.com/data/pdf/fseep_cp_win_manual_jpn.pdf
※表記は旧製品名　F-Secure Computer Protection となっております

F-Secure Elements Endpoint Protection Administrator's Guide
https://help.f-secure.com/data/pdf/fseep_portal_adminguide_jpn.pdf

Elements EPP Release Notes (英文)
https://help.f-secure.com/product.html#business/releasenotes-business/latest/en/fspsb_cp_win-latest-en

1.4　本書で使用される記号

本書で使用される記号について説明します。

記号	意味
	ユーザーアカウント制御：　ボタン押下やリンククリックの際、ユーザーアカウント制御のダイアログが表示される事を表します。続けて操作を行う際は『はい』をクリックします。操作には管理者権限が必要です。 

2.インストールとアンインストール

本章では、Elements EPP / Elements EPP Servers をインストール（ローカルインストール）する手順について説明します。
Elements EPP / Elements EPP Servers 以外のアンチウイルス製品が既に導入されているか、導入されていないかによりインストール手順が変わります。
下記該当項目を参照し、インストール作業を進めて下さい。
なお、インストール後の製品のアップグレードは自動的に行われます。

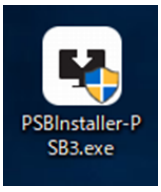
2.1　新規インストール

導入 PC に初めてアンチウイルス製品を導入する場合や、既に以前使用していたアンチウイルス製品を正規手順にて完全に削除している場合が該当します。

【事前確認事項】
①他社製アンチウイルス製品 事前アンインストール徹底のお願い（重要）
初めて WithSecure™ 製品を導入される方は、他社製アンチウイルス製品が含まれていないかを再度確認下さい。

②インストール先
インストール先は C:¥Program Files(x86)¥F-Secure フォルダ下となります。変更はできません。

【手順】
①インストールプログラムの入手と実行
Elements Security Center からインストールプログラムをダウンロードするか、もしくは、指定されたサイトからインストールプログラムを入手してください。
インストールプログラム入手後、導入 PC 上でインストールプログラムをダブルクリックして実行します。インストールプログラムの実行には管理者権限が必要です。

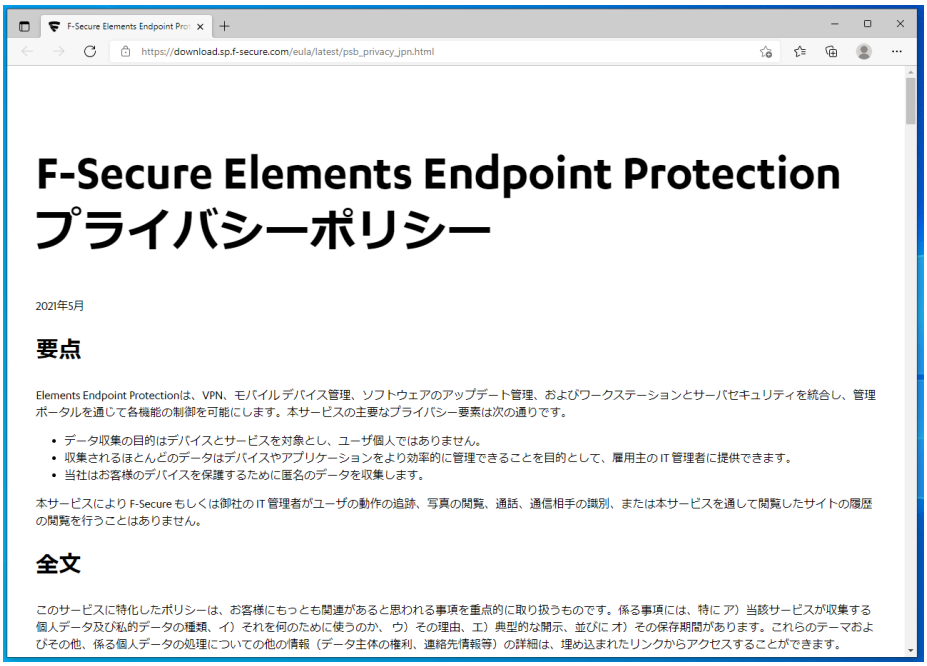


②セットアップ
⚠ダイアログメッセージが表示されます。「はい」を選択してください。

③インストールの確認
「使用許諾契約書」のリンク、及び「データの扱い方」が表示されます。

④使用許諾契約書
「使用許諾契約書」をクリックするとブラウザが起動し「F-SECURE ライセンス約款」のページが表示されます。

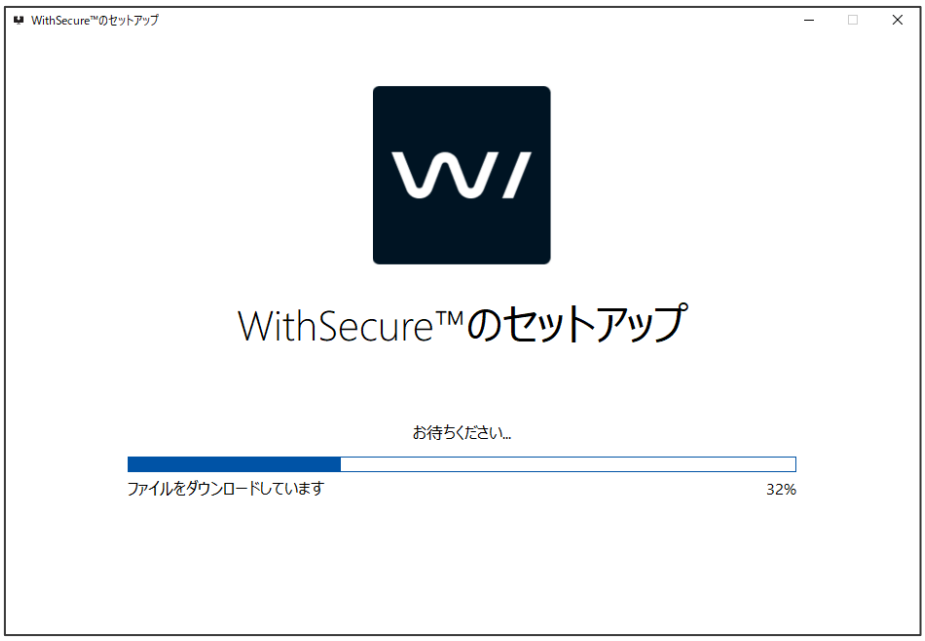
同様に「データの扱い方」をクリックすると、ブラウザが起動し「F-Secure Elements Endpoint Protection プライバシーポリシー」のページが表示されます。



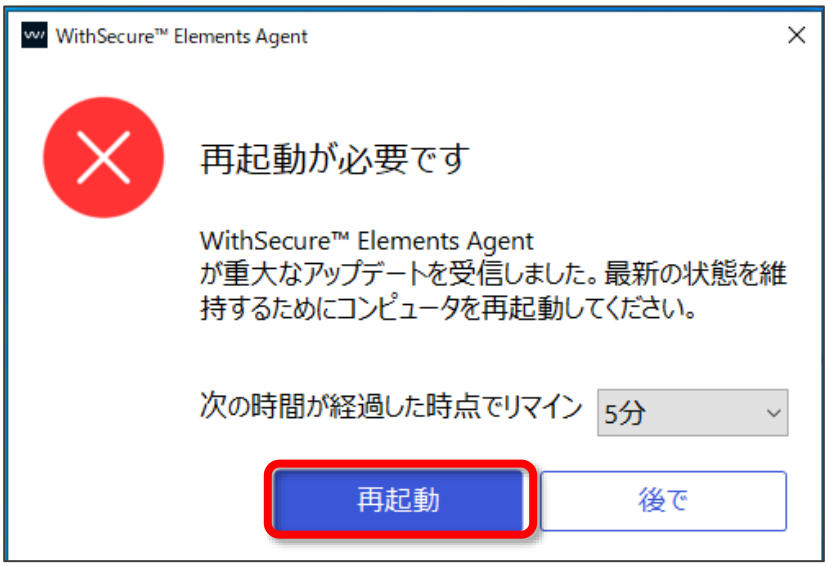
内容を確認し問題なければ、「F-Secure のセットアップ」ダイアログに戻り、「同意して続く」ボタンをクリックします。

※「パーソナライズされていない使用データを F-Secure に送信して製品の改善に貢献できます」に任意でチェックを入れることができます。
これにチェックを入れると、お客様の個人情報を含まない情報が F-Secure に送られ、今後の製品の改善するためのデータとして活用されます。
ここで、チェックを入れた・入れない場合でも、「3.3.8 プライバシー」の設定で、後から追加で設定や設定解除を行うことができます。

⑤インストール処理の開始
インストールが開始されるので、処理完了までしばらく待ちます。



⑥再起動　（必要な場合のみ）
ご利用の PC の設定や状態によっては再起動が必要な場合があります。以下のダイアログが表示された場合、他のアプリケーションを全て終了してから「再起動」をクリックします。
PC の状況によっては再起動が求められないこともあります。実際の表示されるダイアログに従ってください。



⑦ライセンスキーコードの入力（インストールの方法によってはスキップされる場合あり）

（⚠再起動後、）引き続きセットアップが継続されます。ライセンスキーコードの入力が表示されますので、入力欄に指定されたライセンスキーコードを入力し、「次へ」ボタンをクリックします。

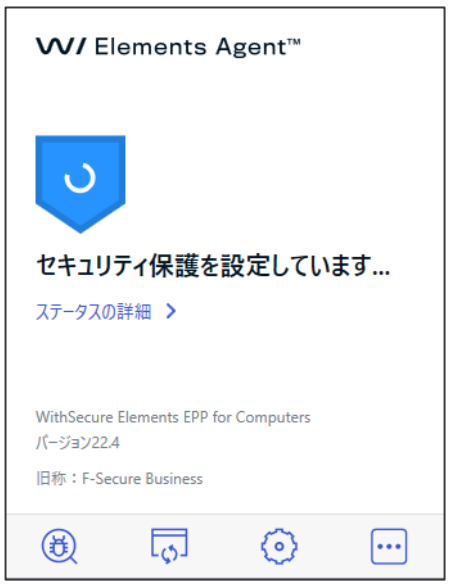
キーコードは、大文字/小文字の区別なく入力できます。

インストールの方法によっては、インストーラにライセンスキーを埋め込む事が可能で、この場合にはこのライセンスキー入力画面が表示されません。

⑧インストールの完了

インストーラは終了しましても、必要な更新を継続して行います。

その間は以下のメイン画面が画面右下に表示され、「セキュリティ保護を設定しています...」メッセージを表示します。



必要な設定が完了すると「コンピュータは保護されています」と表示されます。これで作業としてのインストールは完了です。

【注意】インターネット経由でライセンス認証サーバに接続できない場合は『ライセンスキーコードの認証』を確認する画面が表示されます。
表示された場合は、インターネットの接続を確認し、「認証をもう一度試す」を選択し、「次へ」ボタンを押します。

2.2　他社アンチウイルス製品からの移行方法

既に、他社製アンチウイルス製品をご利用の場合、**必ず既存他社製品を先に確実にアンインストール**し、その後、Elements EPP / Elements EPP Servers をインストールしてください。
もし、他社製品をアンインストールせずに Elements EPP / Elements EPP Servers をインストールした場合、インストールが不完全な状態で終了し、誤動作や動作が重くなるなどの原因となる可能性があります。
Elements EPP / Elements EPP Servers では、主要な他社製品に対して、自動検知と削除の機能（「サイドグレード」と言います）を用意していますが、あくまでもアンインストールし忘れた場合の救済手段であり、サイドグレードにより完全に削除されることを保証するものではありません。

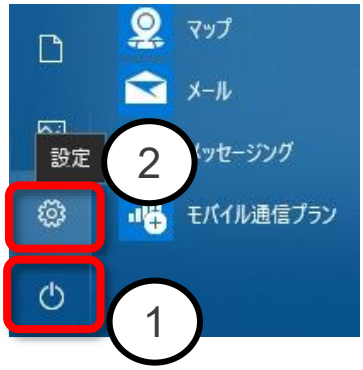
動作上競合する他社品を検出した場合
手順上、⑤インストール処理の開始　の次に競合するアンチウイルス製品をチェックし、うまく登録情報と合致した場合にのみ、インストールの工程の一部として削除作業を挿入します。

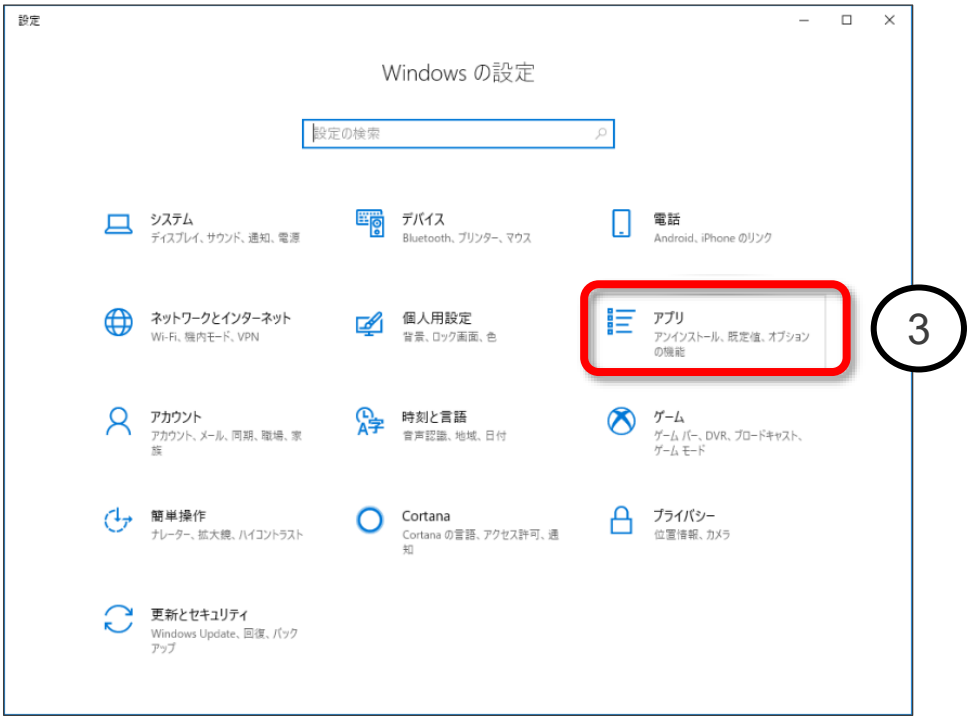
2.3　　アンインストール

⚠ Elements EPP / Elements EPP Servers をアンインストールする場合は、管理者権限のあるユーザにて「アプリと機能」でコンポーネントを削除します。アンインストールには管理者権限が必要です。

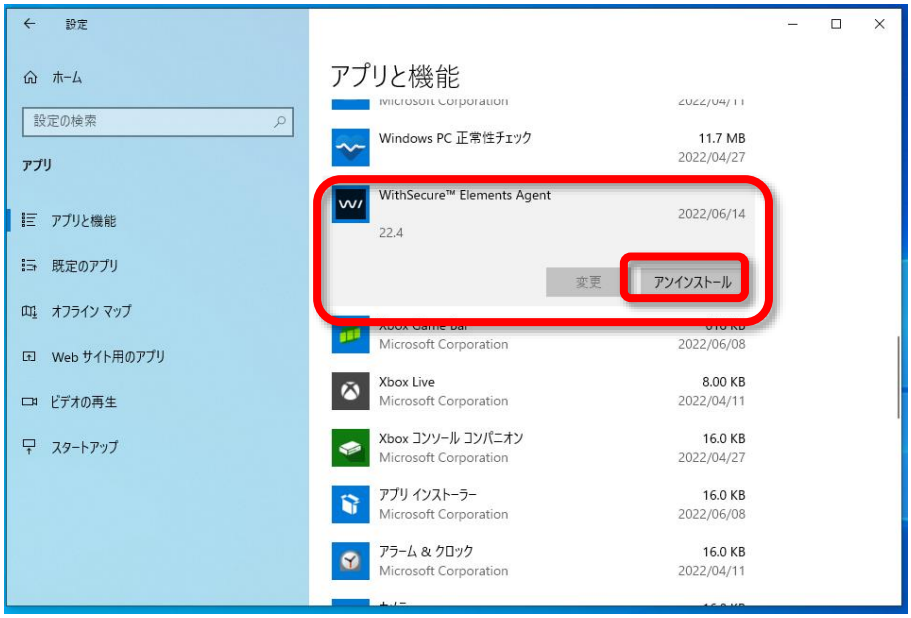
①アプリと機能」の起動
「Windows の設定」画面、「アプリと機能」の起動を起動します。

①「スタート（アイコン）」 ②「設定（アイコン）」 ③「アプリ」 の順で選択します。



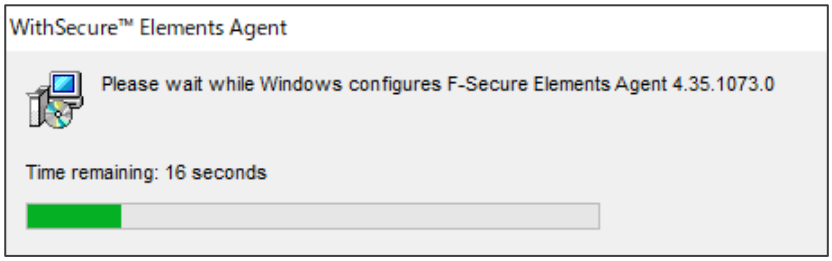


②コンポーネントのアンインストール
「アプリと機能」の欄内にある、「WithSecure™ Elements Agent」を選択し、「アンインストール」をクリックしアンインストールを開始します。



③アンインストールの開始
アンインストールウィザードが表示されます。問題なければ「アンインストール」をクリックします。

処理完了までしばらく待ちます。



④アンインストールの完了
処理が終了するとダイアログが閉じ、アンインストールの完了です。
ここで、システムの再起動を行うことを推奨します。

アンインストール後も「アプリと機能」欄のリストに「WithSecure™ Elements Agent」項目が残っている場合には、画面の再表示を行い、項目がまだ残っているかを確認してください。

レジストリの値やログを含めてきれいに消去し、新規インストール前の状態にしたい場合は、弊社ウェブサイトのサポートツールのページで公開している Elements EPP / Elements EPP Servers 用の「アンインストールツール」をご利用ください。

サポートツール
https://www.withsecure.com/jp-ja/support/support-tools

以上の操作で、Elements EPP / Elements EPP Servers のアンインストールは終了です。

また、Elements Security Center と接続している状態で、クライアントからエージェントをアンインストールした場合、Secuty Center からも当該デバイスが自動的に削除されます。
ネットワーク接続がない場合には、アンインストール後は Elements Security Center から手動で当該デバイスを削除する必要があります。

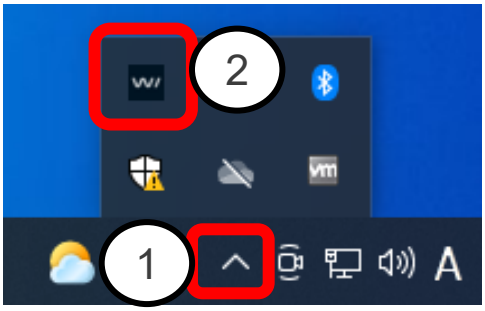
3.　使い方について

「Elements EPP」および「Elements EPP Servers」の「メイン画面」を通じて、使用状況や設定内容の確認、及び設定変更を行うことが出来ます。
但し、Elements Security Center においてロックされたプロフィール設定項目は PC 側でローカルに設定変更は行えません。
このため、ご利用状況により、すべての設定項目が変更できるとは限りません。

3.1　「メイン画面」の表示方法

「メイン画面」を表示するための操作として 以下の方法があります。
(1) タスクトレイから開く（Windows10 の場合）
(2) 「検索」から開く（Windows10 の場合）

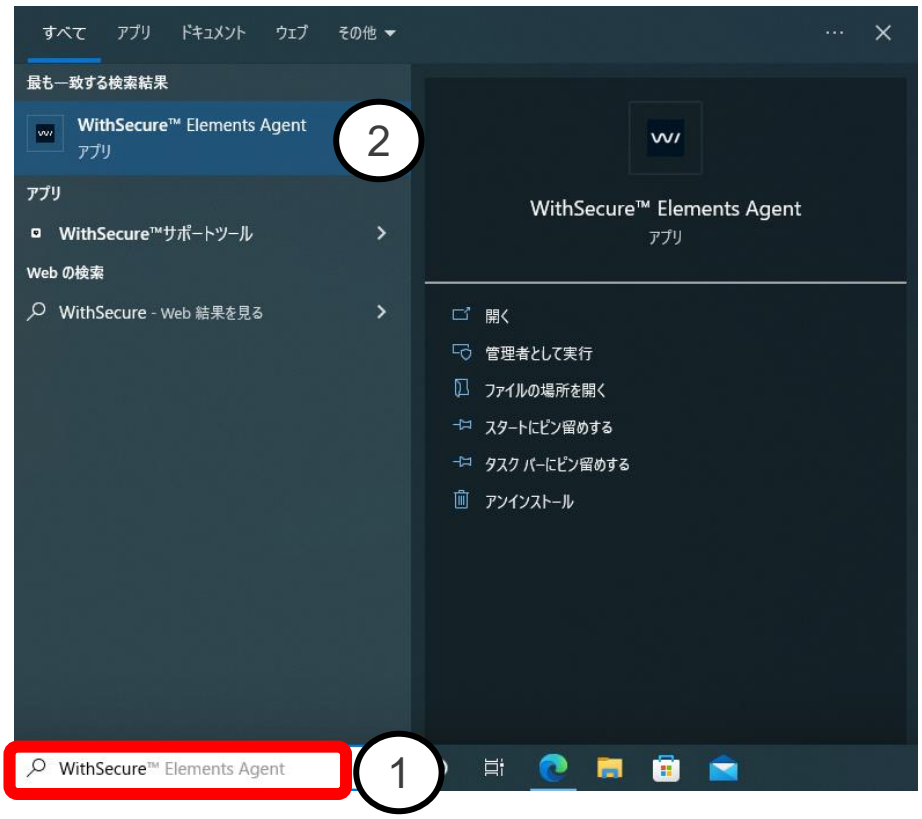
(1) タスクトレイから開く
画面右下の「隠れているインジケータを表示します」ボタンをクリックします。
タスクトレイの「黒の W/マーク」のアイコンをクリックすることで展開します。



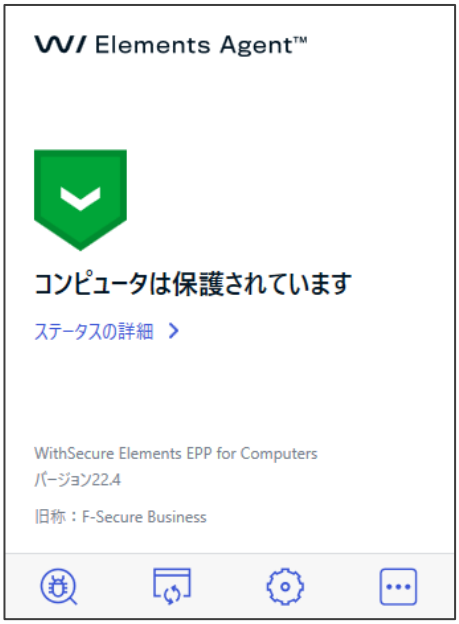
⑵ 「検索」から開く

①表示された検索窓に「WithSecure」と入力します。

②表示されるデスクトップアプリ「WithSecure™ Elements Agent」をクリックすると展開します。

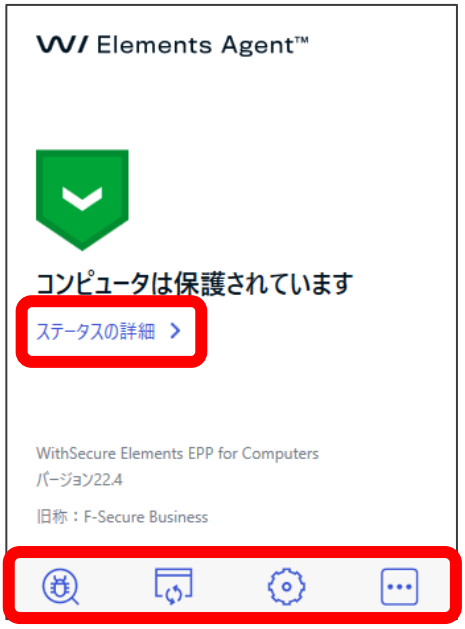


これらの操作を行うことで、「メイン画面」が表示されます。



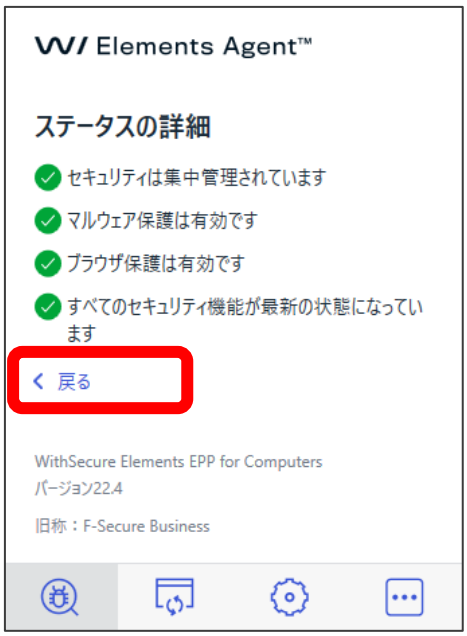
3.2　「メイン画面」の紹介

「メイン画面」はステータスの「詳細」および、「マニュアルスキャン」、「ソフトウェア アップデータ」、「設定」の 3 つのサービスと「追加オプション」が表示されます。
それぞれのサービスおよび操作は以下のような役割を持ちます。



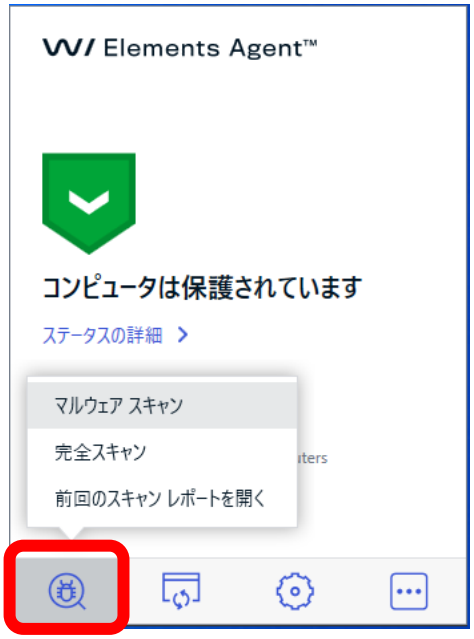
3.2.1　ステータスの詳細

メイン画面の「**詳細**」をクリックすると、ステータスの詳細状態を確認することができます。
正常な場合には以下のように表示されます。
メイン画面に戻る場合は「戻る」をクリックします。

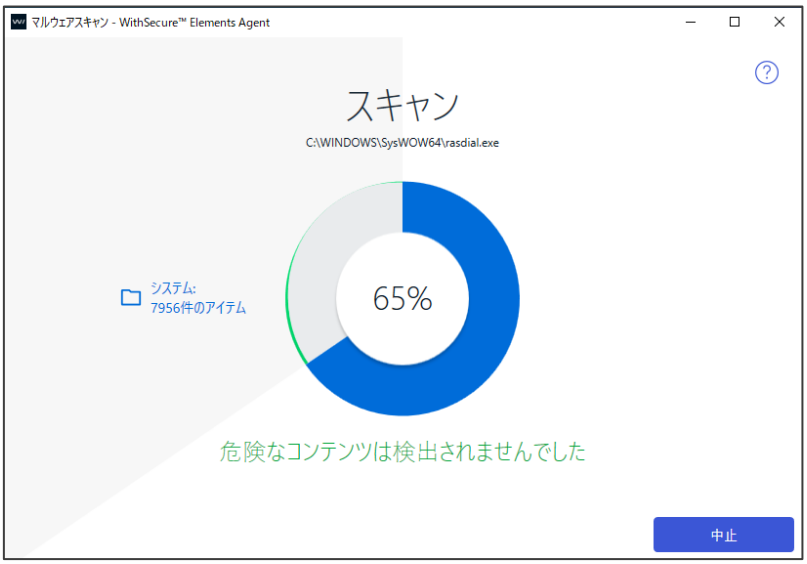


3.2.2　マニュアルスキャン

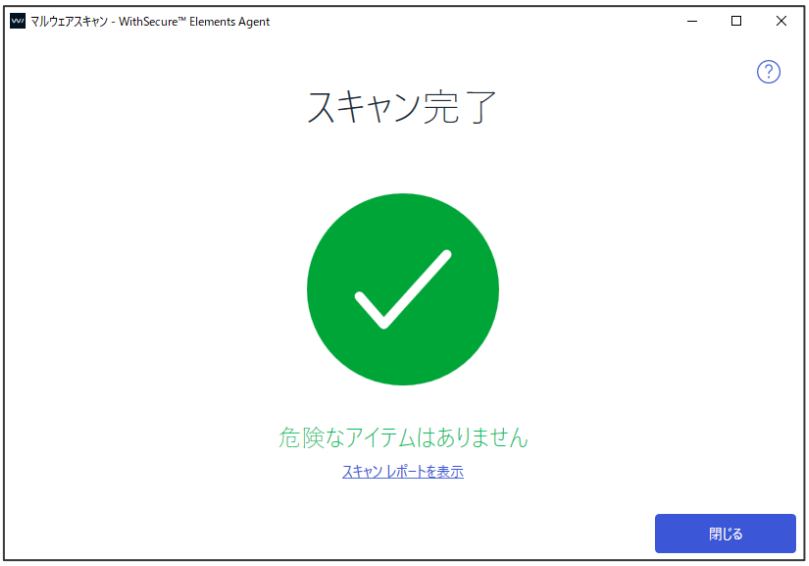
マニュアルスキャンのアイコンをクリックすると、「マルウェアスキャン」、「完全スキャン」、「前回のスキャンレポートを開く」の選択リストが表示されます。
マニュアルスキャンでは、コンピュータに対してウイルスとリスクウェアのスキャンを実行します。



「マルウェアスキャン」は使用中のアプリケーションが含まれるシステムの一部をスキャンします。
必要最小限のスキャンを行うため「完全スキャン」に比べて短時間でスキャンが完了します。
「完全スキャン」は内蔵ハードディスクと外部ハードディスクに対して、マルウェア、スパイウェア、不要な可能性のあるアプリケーションをスキャンします。
ルートキットによって隠蔽されたアイテムも確認します。「マルウェアスキャン」に比べて「完全スキャン」の完了には時間がかかります。
「前回のスキャンレポートを開く」を選択すると最後に実行したマニュアルスキャンのスキャンレポートをブラウザ上で確認することができます。
「マルウェアスキャン」や「完全スキャン」を選択すると次の画面のようにスキャンが開始されます。



100%になると終了です。危険なアイテムが検出されない場合、以下の表示で終了となります。

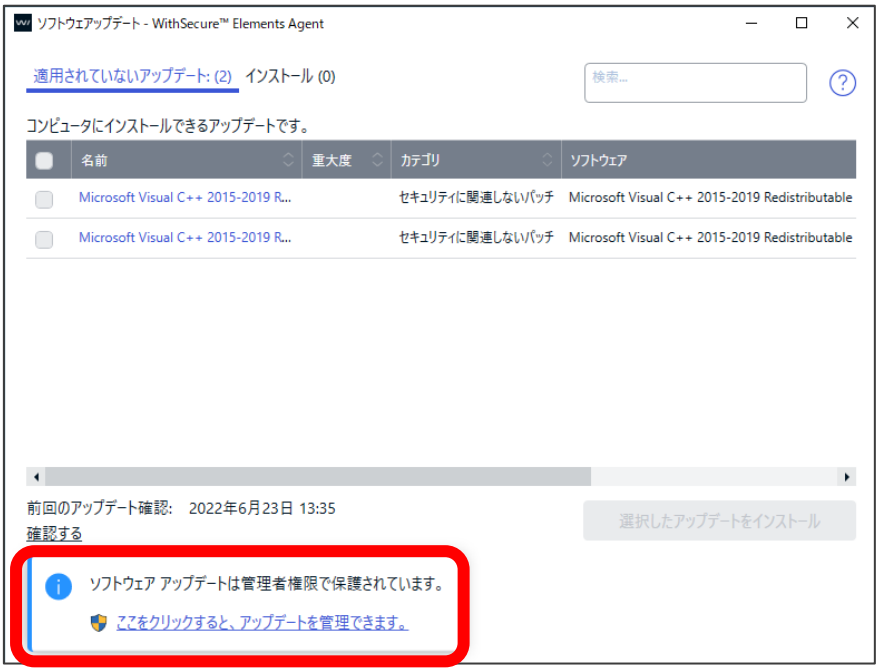


スキャンレポートの例です。

3.2.3　ソフトウェアアップデータ

メイン画面から「ソフトウェアアップデータ」を選択してクリックすると、「ソフトウェアアップデート」画面が表示されます。

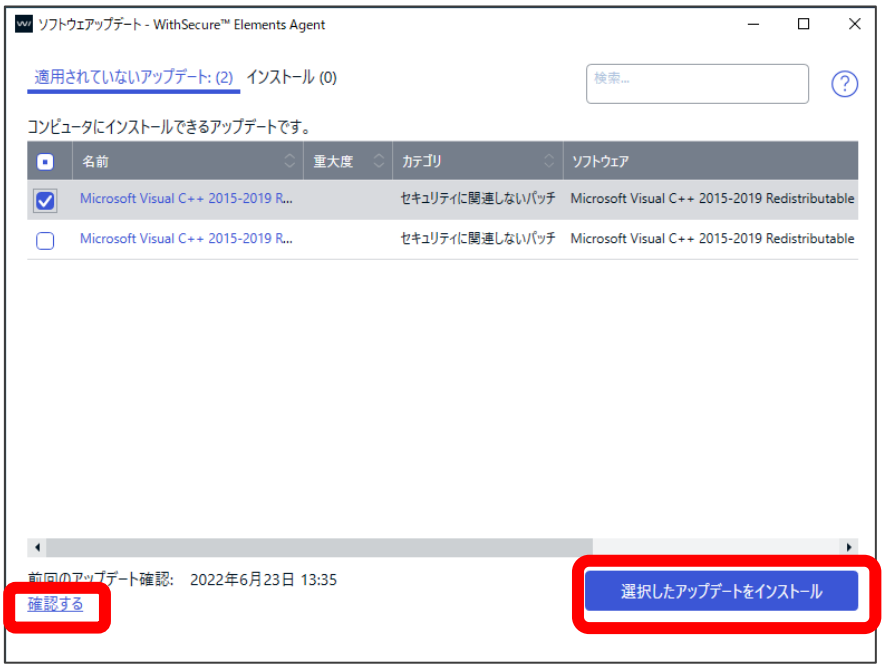
以下がソフトウェアアップデート」画面の例です。



「ソフトウェアアップデート」画面では、その PC に適用可能なアップデートのリストや、既にインストール済のアップデートの一覧をタブ毎に表示可能です。
提要可能なアップデートの一覧においては、個別に適用したいアップデートを選択することや、全てを選択することが可能です。

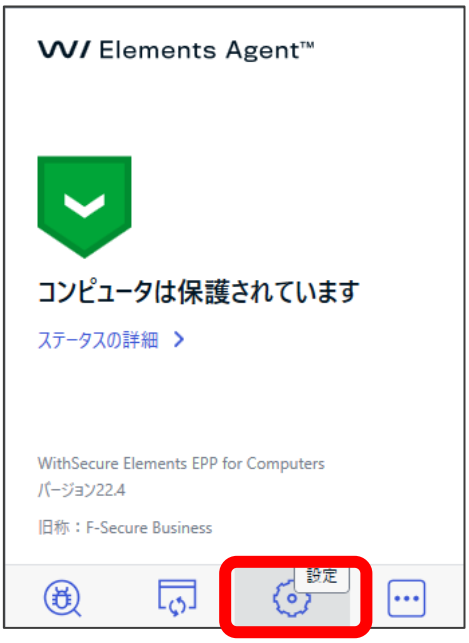
デフォルトでは参照のみですが、「ここをクリックすると、アップデートを管理できます。」をクリックすると、管理者権限に移行し、適切な管理者権限を取得できれば、「選択したアップデートをインストール」ボタンがアクティベートされ、クリック可能となります。

また、「確認する」をクリックすることで、その時点での適用可能なアップデートの有無を確認できます。
通常は PC 起動時に自動的に確認し、Elements Security Center から管理者が指示をする為、お客様自身がこの操作を行う必要はありません。



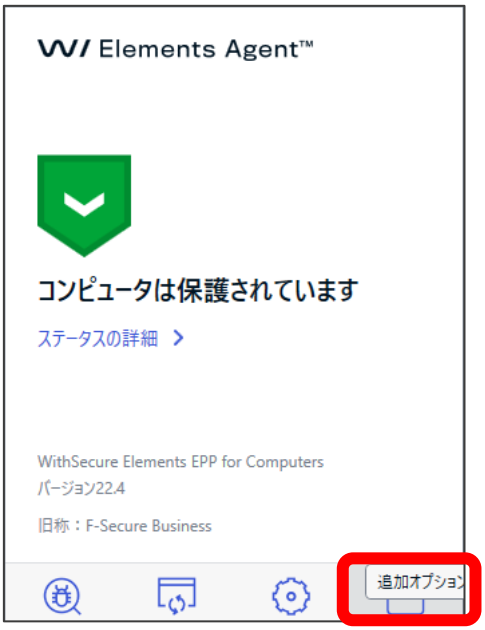
3.2.4　　設定

⚠ Elements EPP / Elements EPP for Servers の「設定」画面を表示します。
各設定項目については『3.3 「設定」画面の紹介』を参照してください。管理者権限が必要です。

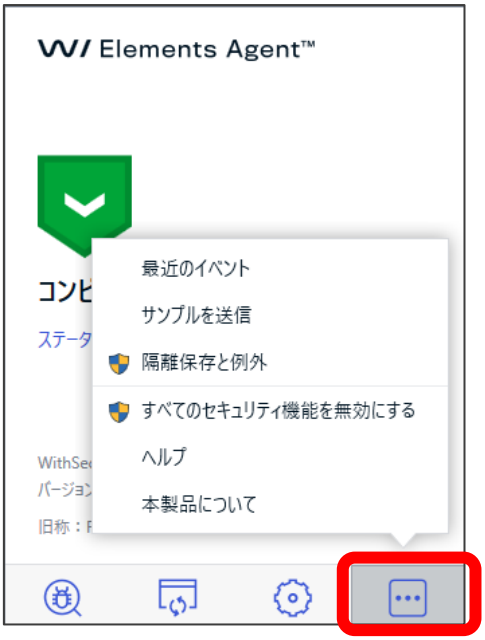


3.2.5　追加オプション

「追加オプション」をクリックすると、Elements EPP / Elements EPP Servers の追加オプション一覧が表示されます。



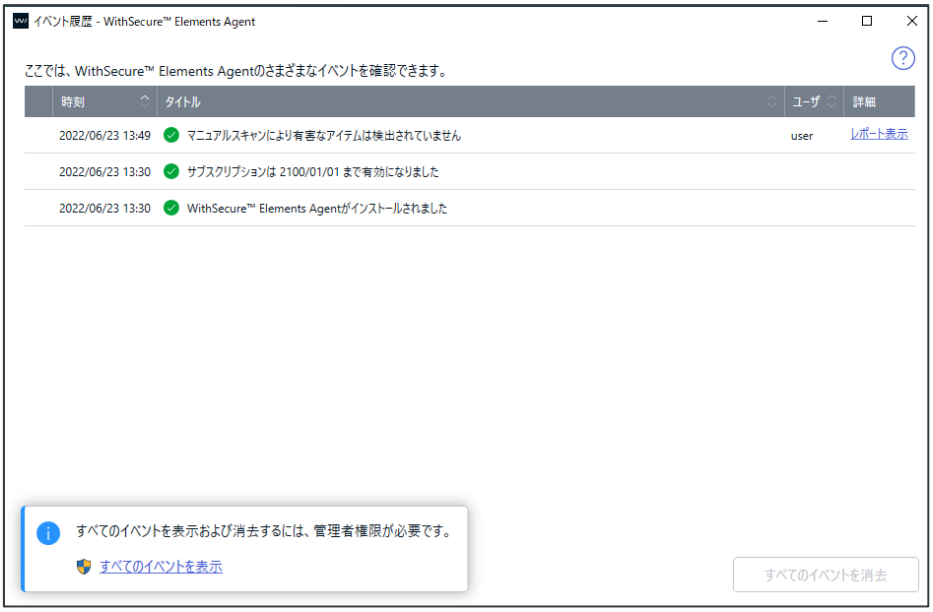
以下が追加オプションの一覧です。



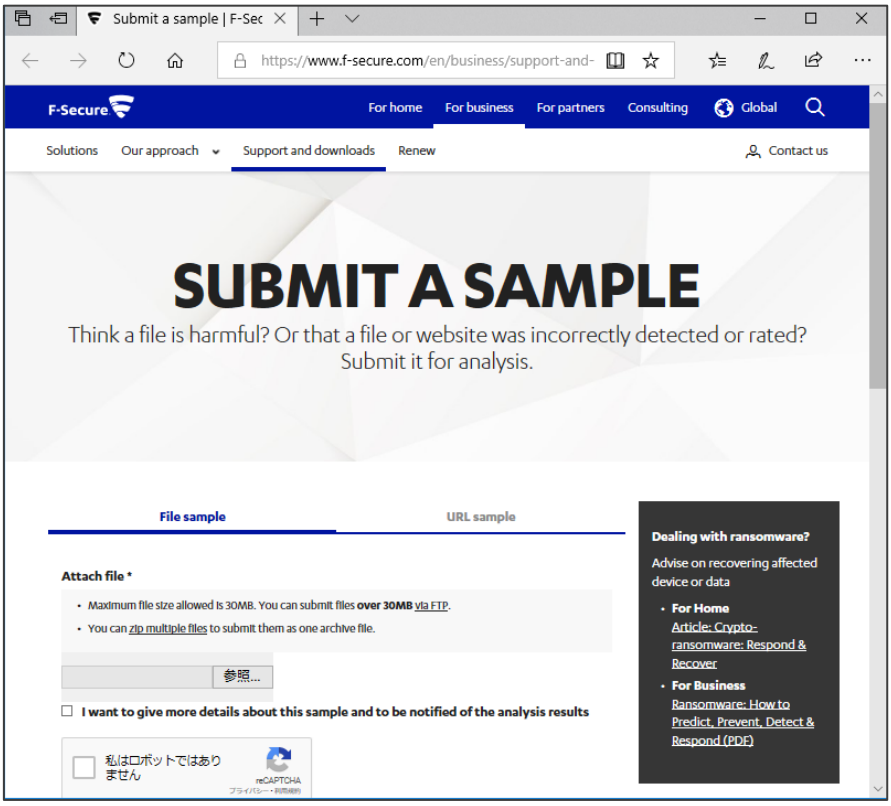
追加オプションの内容

項目名	内容
最近のイベント	製品に関するイベント発生時刻と内容のイベント履歴一覧を表示します。 例 製品のインストール ライセンスキーの有効期限 マニュアルスキャンやリアルタイムスキャンの結果 イベントを「すべて消去」や「すべて表示」させたい場合には管理者権限が必要です。
サンプルを送信	ブラウザにて検体提出ページ(英文)に移動します。
隔離保存と例外 （管理者権限が必要）	「アプリケーション・ファイル制御」画面が開き、「隔離保存済み」、「ブロック済み」、「スッキプ済み」、「保護されています」タブでそれぞれのアイテムを管理できます。 「保護されています」はプレミアム版のみです。
すべてのセキュリティ機能を無効にする （管理者権限が必要）	セキュリティ機能をすべて無効にできます。 コンピュータが脅威にさらされる可能性が上がるのでご注意ください。無効後は再度「有効」にすることができます。 なお、プロフィール設定によっては無効化が禁止されている場合もあります。
ヘルプ	製品のヘルプを参照できます。
本製品について	本製品の商品名やバージョンやコピーライト情報を参照できます。

「最近のイベント」をクリックした場合のイベント履歴の例



「サンプル送信」をクリックした場合のブラウザでのサンプル（検体）送付サイト表示



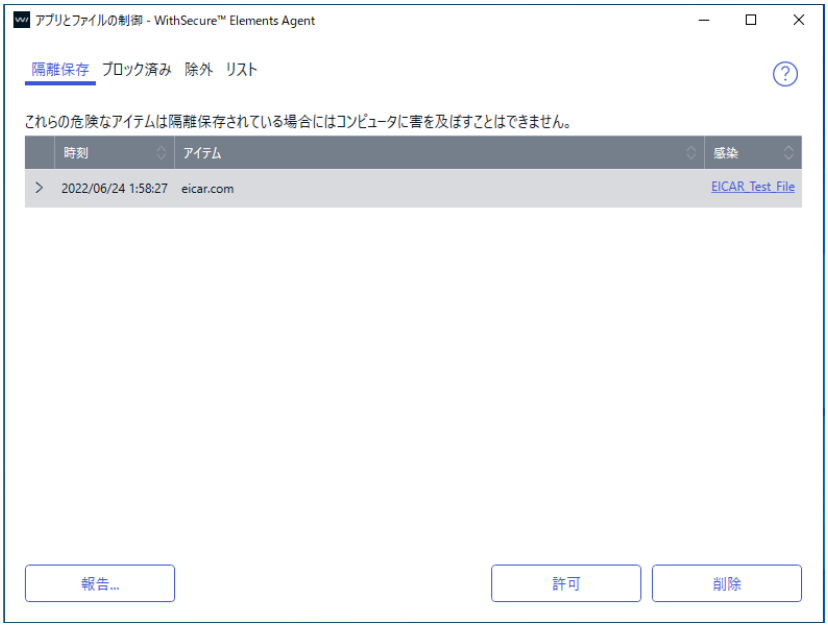
以下の URL となります。
Submit a sample
https://www.f-secure.com/en/business/support-and-downloads/submit-a-sample

検体送付につきましては以下の技術情報（KB）を参考にしてください。

「検体送付手順について教えて下さい。（誤検知/検知漏れ）
https://community.f-secure.com/ja/kb/articles/3045

「隔離保存と例外」をクリックすると、管理者権限の確認が行われます。

ここで「はい」を選択すると、隔離保存の画面が表示されます。



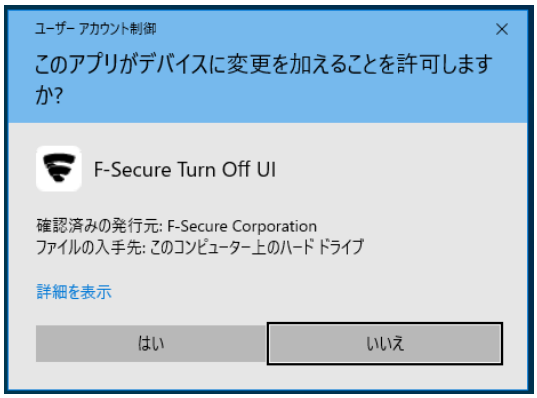
ファイルスキャンにおいて対象アイテムが危険なファイルとして判定された場合、一般ユーザからはアクセスできない隔離保存用フォルダに格納されます。
当該アイテムが安全なファイルと判断される場合は、そのアイテムを選択して「許可」を行うことで、そのアイテムは元の場所に戻されます。
また、「除外」タブの一覧に追加され、以降は検知除外されます。
実際にそのアイテムが危険なファイルの場合には、そのアイテムを選択して「削除」を行うことで実際にファイルが削除されます。

隔離保存されたファイルの検知が誤検知の場合には、そのアイテムを検体としてエフセキュアに誤検知として調査依頼を行うことができます。
この場合、そのアイテムを選択して「報告」を行うことで、以下のダイアログが表示されます

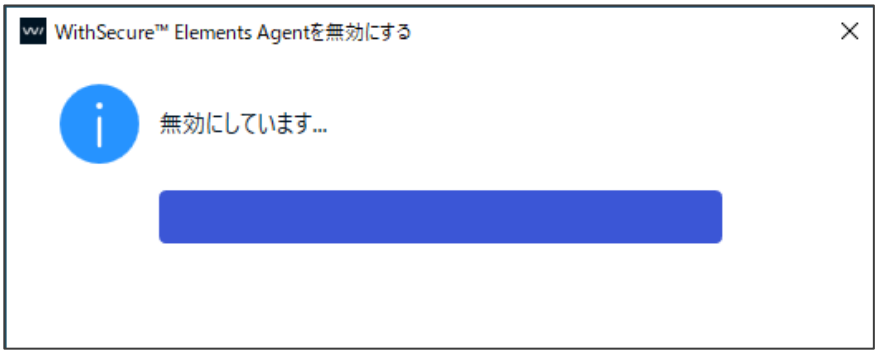
「レポート」を行い、サンプルを送信します。

「ブロック済み」タブはディープガードによりブロックしたアプリケーションの一覧が表示されます。
「リスト」タブはデータガードのプロファイル設定したリストが一覧表示されます。（Premiun 製品）

「すべてのセキュリティ機能を無効にする」をクリックすると、管理者権限の確認が行われます。



ここで「無効」を選択すると、WithSecure™ Elements Agent の機能の無効化が開始されます。

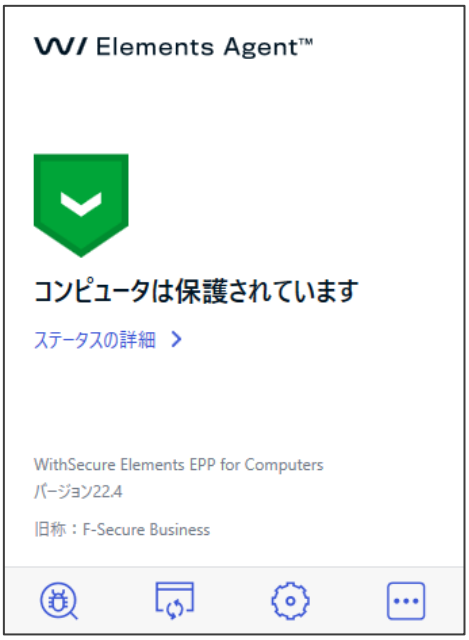


無効化が完了した後のメイン画面は以下のように「コンピュータ保護は無効です」となり、アイコンが変わります。

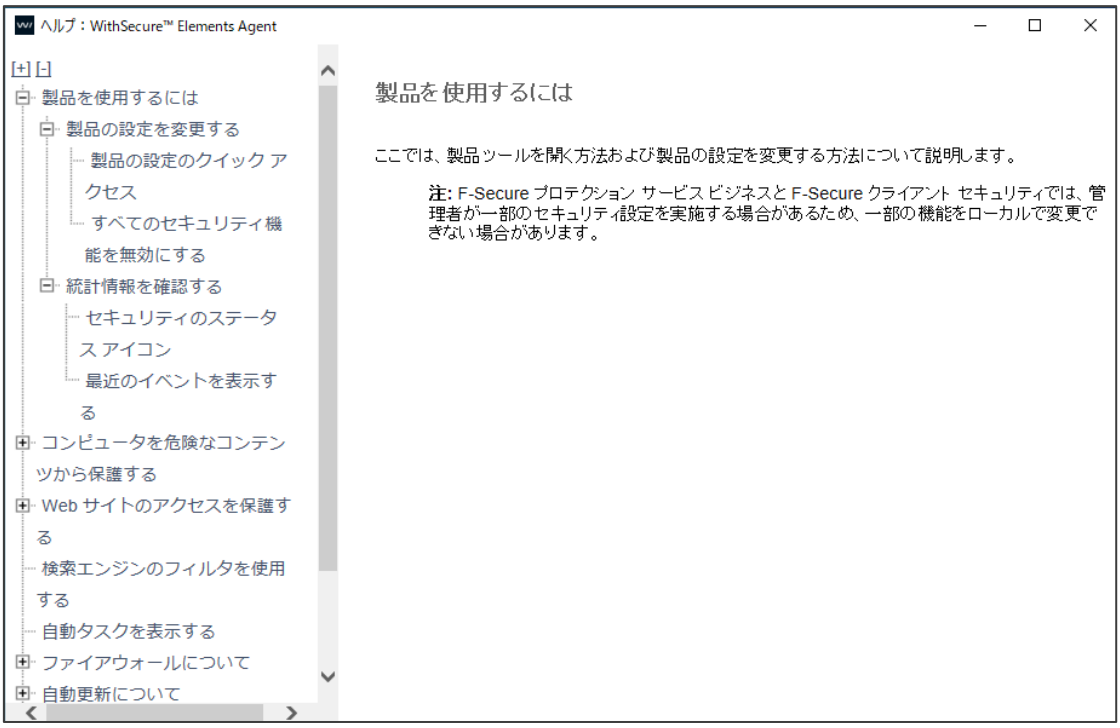
無効化されている場合の「追加オプション」は以下のように「すべてのセキュリティ機能を無効にする」が「有効にする」になります。一部のメニューは機能しません。

ここで「有効にする」をクリックすることで、機能の有効化が開始されます。

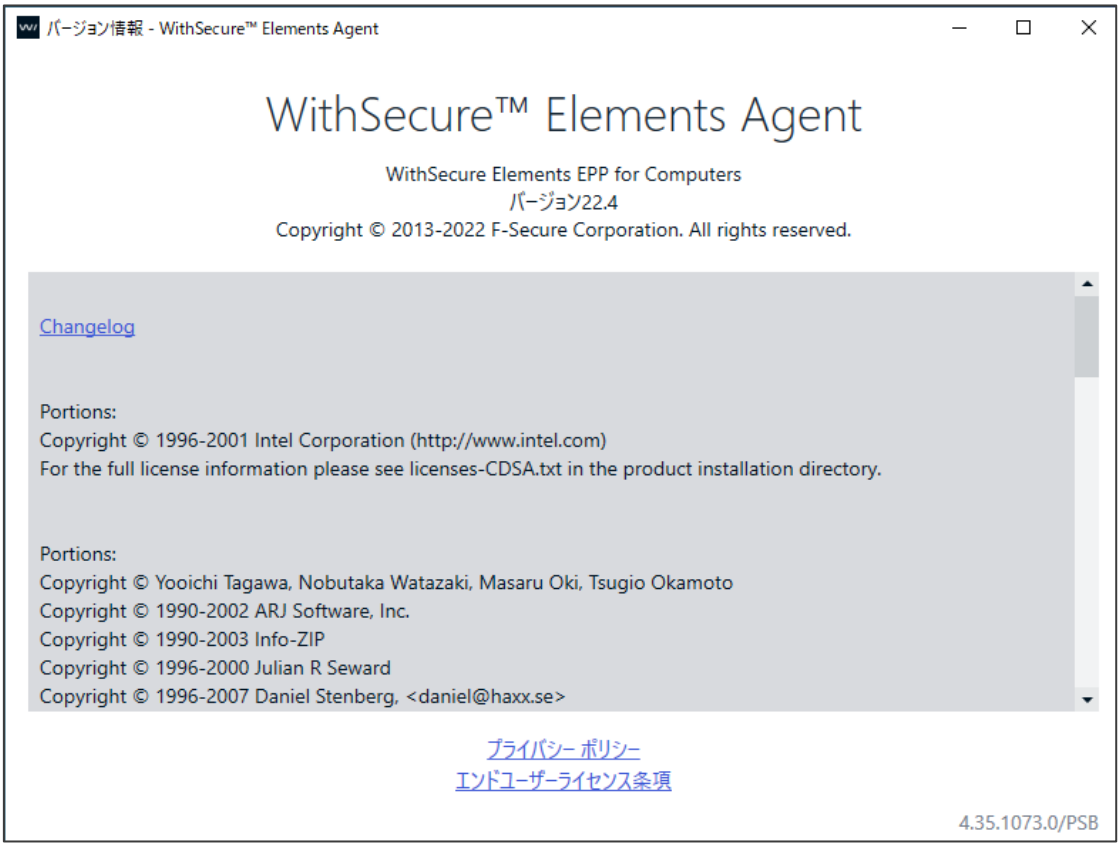
すべて完了すると、メイン画面は元の「コンピュータは保護されています」の状態に戻ります。



「ヘルプ」をクリックすると以下のヘルプ画面となります。

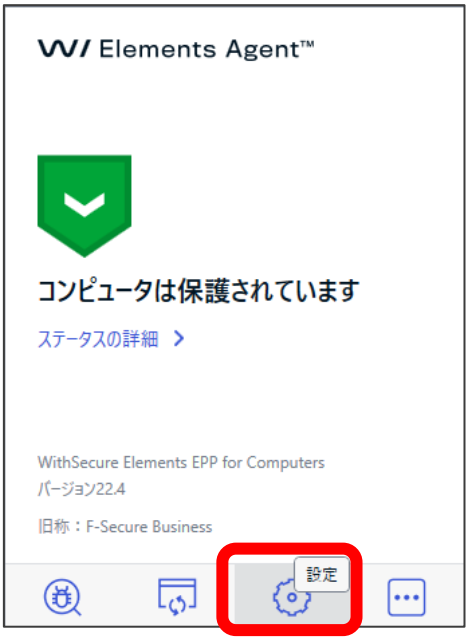


「本製品について」をクリックすると以下のようなバージョン画面が表示されます。



3.3　「設定」画面の紹介

「メイン画面」の「設定」リンクをクリックすると「設定」画面が表示されます。
管理者権限が必要です。



「設定」画面は以下のようになります。

「設定」で行える内容は以下のとおりです。変更には管理者権限が必要です。また、プロフィール設定にて項目がロックされている場合、ローカルでの変更は行なえません。

項目名	内容
マルウェア保護	以下の機能の有効/無効や設定を行えます。 リアルタイムスキャン ディープガード データガード(Premium 版のみ) マルウェア対策スキャンインターフェース（AMSI) 詳細なネットワーク保護（Web スキャン）
スキャン設定	以下の機能の有効/無効や設定を行えます。 マニュアルスキャン スケジュールスキャン USB ストレージデバイス
セキュアブラウジング	以下の機能の有効/無効や設定を行えます。 レピュテーションベースのブラウジング 接続制御 ブラウザ プラグイン
自動化されたタスク	自動化されたタスクの確認が行えます。
ファイアウォール	以下の機能の有効/無効や設定が行なえます。 ファイアウォール
Web コンテンツ制御	以下の機能の有効/無効を行えます。 検索結果のフィルタ
アップデート	以下の機能の設定・確認を行えます。 更新サーバとの状況と手動確認 プロキシの手動設定 アップデート履歴とログ確認
プライバシー	以下の機能の有効/無効を行えます。 Security Cloud 製品の改善
サポート	製品に関する情報の確認とサポートツールの実行を行えます。 ID コード バージョン情報 ツール
一元管理	コンピュータに関する管理情報を確認できます。 製品情報 コンピュータ情報 プロフィール情報 Windows イベント

3.3.1　マルウェア保護

「マルウェア保護」ではマルウェア保護に関する設定を行うことができます。
「マルウェア保護」画面は、「設定」の「マルウェア保護」を選択することで表示されます。

「マルウェア保護」の設定の各設定項目の内容は以下のとおりです。

リアルタイムスキャン項目
リアルタイムスキャンはファイルへのアクセスをトリガに対象ファイルを自動的にスキャンします。

項目名	内容
リアルタイムスキャン 有効 / 無効	リアルタイムスキャン機能の有効/無効の設定を行えます。 リアルタイムスキャンを有効にすると、ファイルアクセス時のスキャンにより、リスクウェアや危険なファイルのシステムへの侵入を阻止します。
リアルタイムスキャンを一時的にオフにする	一定時間、リアルタイムスキャンをオフにすることが可能です。
隔離保存したファイルを表示する	「アプリとファイルの制御」の画面が起動し、「隔離保存」タブにて、隔離保存したアイテムの履歴の一覧を確認することができます。 一覧の各アイテムに対し、「許可」、「削除」と「報告」を行えます。許可したアイテムは「隔離保存「タブの一覧から削除され、元の場所に戻ります。また、以降のスキャンでの検知対象から除外され、そのアイテムは「除外」タブの一覧に追加されます。 削除したアイテムは一覧から削除され、ファイルも削除されます。 報告を選択した場合、そのアイテムはウィズセキュアに送付され、誤検知として報告されます。 「除外」のタブの一覧では「新規追加」と「削除」操作を行えます。 「新規追加」で除外するファイルやフォルダを追加できます。 「削除」すると除外対象から解除され、スキャンの対象に戻ります。 一覧の表示には管理者権限が必要です。

ディープガード項目
ディープガードはプログラムのふるまいを解析して、未知のウイルス、ワーム、およびコンピュータに問題を引き起こす可能性のあるリスクウェアのアクションをブロックします。
各アプリケーションの安全性は、ディープガードにより実行前にクラウドサービスによって検証されます。
安全性が確認できない場合、アプリケーションの実行中はふるまい検知を行い、危険な操作はその実行前にブロックされます。

項目名	内容
ディープガード 有効 / 無効	ディープガードの機能の有効/無効の設定を行えます。 デフォルトは有効です。 未知のマルウェア対策機能となりますので、通常は無効にしないことを強く推奨します。
ディープガードを一時的にオフする	一定時間、ディープガードをオフにすることが可能です。
ブロックしたアプリケーションを表示する	「アプリとファイルの制御」の画面が起動し、「ブロック済み」タブが表示されます。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確認できます。 一覧の各実行をブロックされたアプリケーションに対し、実行を改めて「許可」や、一覧から「削除」をすることができます。 許可をしたアプリケーションは「ブロック済み」タブの一覧から削除され、「除外」タブの一覧に追加されます。以降、ディープガードの監視から除外されます。 一覧の表示には管理者権限が必要です。

データガード項目（Premium 版機能）

データガードは、保護対象のフォルダを監視して、アプリケーション（ランサムウェアなど）による不審なアクティビティをブロックします。

この設定は「Elements EPP / Elements EPP Servers」の Premium 版の場合だけ表示されます。

項目名	内容
フォルダ監視 有効 / 無効	データガードのフォルダ監視の有効/無効の設定を行えます。 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。
データガードアクセス制御 有効 / 無効	データガードのアクセス制御の有効/無効の設定を行えます。 データガードのアクセス制御は未知のアプリケーションがフォルダにアクセスすることを防ぐことで、フォルダを暗号化する有害なソフトウェアから保護します。
保護されているフォルダを表示する	「アプリとファイルの制御」の画面が起動し、「保護されてます」タブが表示されます。データガードの保護対象のフォルダの一覧を確認したり、フォルダを追加や削除することができます。 一覧の表示には管理者権限が必要です。

マルウェア対策スキャンインターフェース（AMSI）項目

Windows 10 が実装するマルウェア対策スキャンインターフェース（AMSI）の統合により、有害なスクリプトやマクロを探すことが可能になります。

項目名	内容
マルウェア対策スキャンインタフェース(AMSI) 有効 / 無効	AMSI の有効/無効の設定を行います。 デフォルトは有効です。

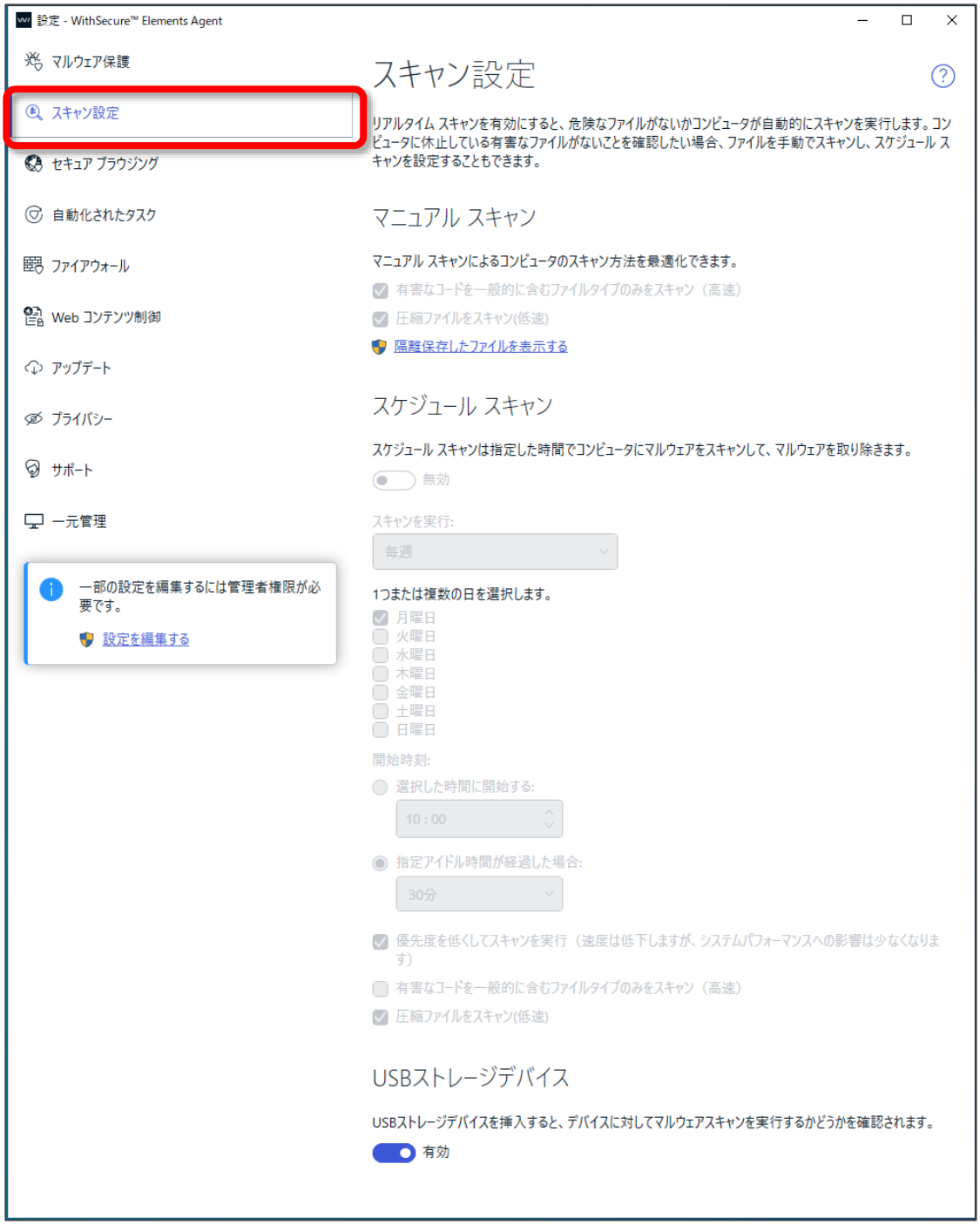
詳細なネットワーク保護項目 (Web トラフィックスキャン：WTS)

アプリケーションが HTTP 経由でのファイルのスキャンを行うかどうかを設定します。これを有効にすると、HTTP 経由で危険なファイルのダウンロードをブロックできます。HTTPS 通信ではスキャンは行いません。

項目名	内容
詳細なネットワーク保護 有効 / 無効	詳細なネットワーク保護の有効/無効の設定を行います。 デフォルトは有効です。

3.3.2　スキャン設定

「スキャン設定」では、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のマニュアルスキャンに関する設定を行えます。
「スキャン設定」画面は、「設定」の「スキャン設定」を選択することで表示されます。



マニュアルスキャン項目
手動によるファイルスキャンの設定内容です。

「マニュアルスキャン」の設定の内容は以下のとおりです。

項目名	内容
有害なコードを一般的に含むファイルタイプのみをスキャン（高速）	既知のファイル タイプのみスキャンします (例: 実行ファイル)。 このオプションを選択すると、スキャン対象のファイル数が限定されるため、全ファイルに対するスキャンより早く完了します。 このオプションを選択しない場合、すべてのファイルがスキャンされます。 デフォルトは有効です。
圧縮ファイルを スキャン（低速）	圧縮ファイルをスキャンします (例: ZIP ファイル)。 このオプションを選択すると、圧縮ファイル内のファイルもスキャンされるのでスキャンの時間が余分にかかります。 このオプションを選択しない場合、圧縮ファイルのスキャンはスキップされるため、スキャンがより早く完了します。 デフォルトは有効です。
隔離保存した ファイルを表示する	「アプリとファイルの制御」の画面が起動し、「隔離保存」タブが表示され、隔離保存したファイルの一覧を確認することができます。 一覧の各アイテムに対し、「許可」、「削除」と「報告」を行えます。 許可したアイテムは「隔離保存」タブの一覧から削除され、以降のスキャンでの検知対象から除外され、そのアイテムは「除外」タブの一覧で確認できます。 削除したアイテムは「隔離保存」タブの一覧から削除され、そのアイテム自身も削除されます。 報告を選択した場合、そのアイテムはエフセキュアに送付され、誤検知として報告されます 「除外」のタブの一覧には「新規追加」と「削除」操作を行えます。 「新規追加」で除外するファイルやフォルダを追加できます。 「削除」すると除外対象から解除され、リアルタイムスキャンの対象に戻ります。 一覧の表示には管理者権限が必要です。

スケジュールスキャン項目
スケジュールスキャンの設定内容です。

コンピュータにマルウェアやリスクウェアがないかどうか定期的に（日単位、週単位、月単位など）スキャンします。スケジュールスキャンの設定は、下図の「スケジュールスキャン」を選択することで表示されます。

「スケジュールスキャン」の設定の内容は以下のとおりです。

項目名	内容
スケジュールスキャン 有効 / 無効	スケジュールスキャンの有効/無効を設定します。 デフォルトは無効です。
スキャンを実行	スケジュールスキャンの動作を以下の単位で、開始時刻に実行します。 日単位 ： 毎日実行します。 毎週 ： 曜日を指定日で指定する。 ４週毎 ： ４週間毎に曜日を指定する。 注意: ローカル設定では「毎月」の設定は行なえません。「毎月」はプロフィールでのみ設定できます。
開始時刻:	スケジュールスキャンを開始する時刻を定義します。「週単位」、「毎月」で定義した場合もここで定義された時間にスケジュールスキャンが実施されます。 以下のいずれかが指定可能です。 選択した時間に開始する 指定したアイドル時間が経過した場合
優先度を低くしてスキャンを実行	コンピュータの他の処理に対してスケジュール スキャンによる性能低下の影響を低くすることができます。 デフォルトは有効です。
有害なコードを一般的に含むファイルタイプのみをスキャン（高速）	既知のファイルタイプのファイルのみスキャンします（例: 実行ファイル)。 このプションを指定すると、特定のファイルのみスキャンするため、スキャン対象のファイル数が少なくなるため、結果的に全数スキャンよりもスキャンがより早く完了します。 オプションを選択しない場合、すべてのファイルがスキャンされます。 デフォルトは無効で、すべてのファイルがスキャン対象です。
圧縮ファイルをスキャン（低速）	圧縮ファイルの中身もスキャンします（例: ZIP ファイル)。 このオプションを選択すると、圧縮ファイル内のファイルもスキャンするのでスキャンに時間がかかります。 オプションを選択しない場合、圧縮ファイルのスキャンはスキップされるので、スキャンがより早く完了します。 デフォルトは有効です。

USB ストレージデバイス項目
USB ストレージデバイスの設定内容です。

USB ストレージデバイスを挿入すると、デバイスに対してマルウェアスキャンを実行するかどうかを確認されます。

項目名	内容
USB ストレージデバイス スキャン 有効 / 無効	USB ストレージデバイス スキャンの有効/無効を設定します。 デフォルトは有効です。

3.3.3　　セキュア ブラウジング

「セキュア ブラウジング」設定では、PC のブラウザで検索サイトの結果をクラウドデータベースで確認する設定や、リンク先のサイトに悪意のあるスクリプトなどが仕込まれていないかを確認することの設定が可能です。
「セキュア ブラウジング」画面は、「設定」の「セキュア ブラウジング」を選択することで表示されます。

レピュテーションベースのブラウジング項目

レピュテーションベースのブラウジング設定の内容は以下のとおりです。

項目名	内容
ブラウザ保護 有効 / 無効	この設定を有効にすると、「危険」と評価されている Web サイトへのアクセスはブロックされます。 デフォルトは有効です。
不審な Web サイトをブロック	この設定を有効にすると、「不審」とカテゴリされているウェブページへのアクセスがブロックされます。 デフォルトは有効です。
禁止されている Web サイトをブロック	この設定を有効にすると、「禁止」とカテゴリされているのウェブページへのアクセスがブロックされます。 デフォルトは有効です。
検索エンジンの結果(Google,Yahoo,Bing,DuckDuckGo)に評価を表示する	検索サイトの検索結果に対し、評価結果のアイコンを表示させることで、サイトの安全性を訪問前に判断できる機能です。 ブラウザのアドオンとして動作します。 デフォルトは有効です。
Web サイトの例外を表示	クリックすると「Web サイトの制限」画面が起動します。 一覧の表示には管理者権限が必要です。

接続制御 項目

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。

また、銀行や金融系サイトのアクセスや取引を行うときに発生する危険な処理からシステムを保護します。

「接続制御」の設定の内容は以下のとおりです。

項目名	内容
接続制御 有効 / 無効	この設定を「有効」にすると、銀行や金融系サイトへのアクセスや、オンライン決済を行なう際、接続制御が有効になります。これにより、取引の安全性を維持するために、同時接続中の他のセッションがブロックされ、機密性のあるデータを保護できます。 デフォルトは有効です。
信頼できないアプリを切断する	信頼できないアプリは接続制御中には使用できなくなります
コマンドラインとスクリプトツールの接続を解除	コマンドラインツールとスクリプトツールのネットワーク接続を解除できます。
クリップボードを消去	プライバシー保護を強化するため、バンキング セッション終了時にクリップボードを消去するかどうか指示します。 デフォルトでは消去し、クリップボードのデータは消去されます。
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する	デバイスへのリモートアクセスをブロックすることができます。たとえば、リモートデスクトップ、TeamViewer、LogMeIn、VNC などのようなツールに対応しています。

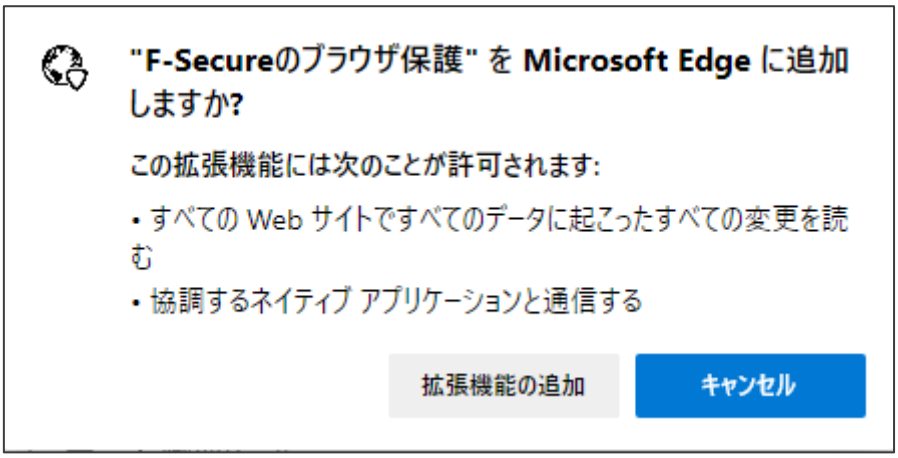
ブラウザ プラグイン項目

ブラウザ プラグイン（ブラウザ拡張機能）は、Web サイトのブラウジングに対するセキュリティを確保するためのプラグイン アプリケーションです。ブラウザ保護を利用するためには、ブラウザ プラグインが必要です。
新しいブラウザのインストールや、新しいブラウザにアップグレードした場合は、プラグインを再インストールする必要がある場合があります。

「ブラウザ プラグイン」の設定の内容は以下のとおりです。

項目名	内容
Firefox の拡張機能をインストール	Firefox の場合のプラグインをインストールします。
Chrome ウェブストアを開く	Google Chrome は、Chrome ウェブストアから拡張機能の再インストールを要求する場合があります。その場合には、Chrome ウェブストアを開き、「Chrome に追加」ボタンをクリックしてください。
Edge の機能拡張を開く	Microsoft Edge は、Edge アドオンから拡張機能の再インストールを要求する場合があります。 その場合には、Edge アドオンから「インストール」ボタンをクリックしてください

例：ブラウザ　プラグインの追加時の表示



3.3.4 自動化されたタスク

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

コンピュータに影響を与える「自動化されたタスク」を確認するには、「設定」の「自動化されたタスク」を選択することで表示されます。

3.3.5　ファイアウォール

「ファイアウォール」設定ではインターネットを通じて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。
また、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。
「ファイアウォール」画面は、「設定」の「ファイアウォール」を選択することで表示されます。

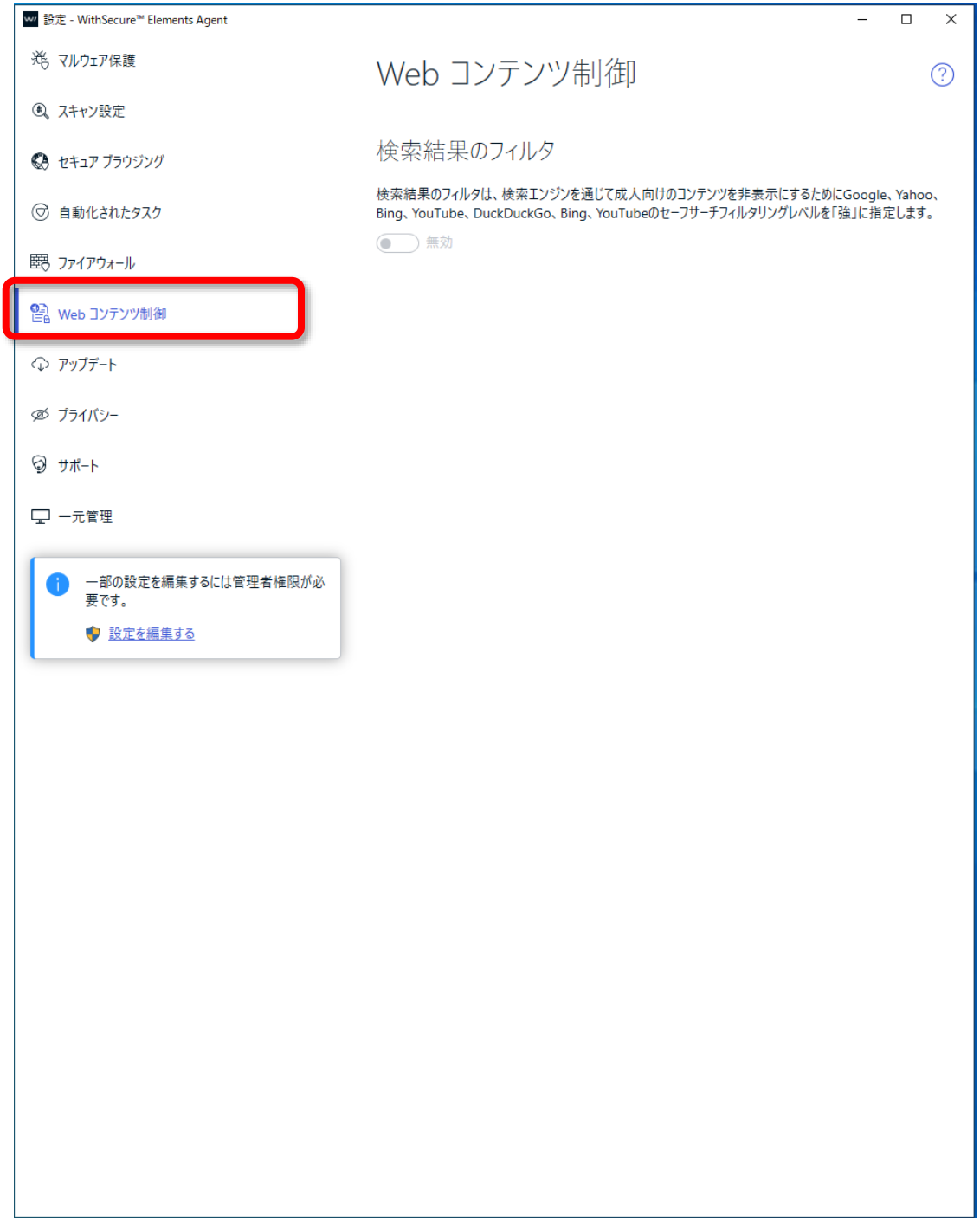
「ファイアウォール」の設定の内容は以下のとおりです。

項目名	内容
有効 / 無効	「有効」でファイアウォールが有効になります。 デフォルトは ON です。
WithSecure™ ファイアウォール プロフィール	適用中の WithSecure™ ファイアウォールのプロフィール名です。表示のみで変更できません。
Windows ファイアウォールの設定を開く	クリックすると Windows のコントロールパネル「Windows ファイアウォールによる PC の保護」画面が起動します。
ログ： ファイアウォールのブロック イベント ログを開く	ファイアウォールでブロックされたイベント情報のログを表示します。

3.3.6　Web コンテンツ制御

「Web コンテンツ制御」設定では、検索エンジンサーチ フィルタを使用して検索結果から不適切なコンテンツをブロックできます。
検索エンジンのフィルタは Google、Yahoo、Bing、YouTube,DuckDuck のセーフモードを有効にし、Google、Yahoo、Bing のセーフサーチ フィルタリング レベルを「強」にすることで成人向けのコンテンツを表示しないようにします、すべての不適切なコンテンツが検索エンジンで表示されないようにすることはできませんが、ほとんどのコンテンツはブロックできます。

「Web コンテンツ制御」画面は、「設定」の「Web コンテンツ制御」項目を選択します。



「Web コンテンツ制御」の設定の内容は以下のとおりです。

項目名	内容
検索結果のフィルタ 有効 / 無効	有効にすると、セーフサーチ フィルタリング レベルを「強」に指定します。 デフォルトは「無効」です。

3.3.7　アップデート

「アップデート」設定では、製品のインターネットの接続方法および最近受信したアップデートを確認できます。
製品のアップデートの確認は自動的に行われる為、手動で確認する必要はありません。
「アップデート」画面は、「設定」の「アップデート」を選択することで表示されます。

「アップデート」の内容は以下のとおりです。

項目名	内容
確認する	最新の更新を手動チェックします。現在の状態が最新でない場合、最新の更新がダウンロードされ適用されます。 前回の確認から 1 時間毎に自動的に更新確認が行われます。
プロキシの手動設定	プロキシが必要なネットワークにおいて、必要に応じて設定します。 使用しない ブラウザの設定を使用 カスタムアドレス/ポート
ログファイルを表示	クリックするとメモ帳が起動し、更新ログファイルの内容が確認できます。

3.3.8　プライバシー

「プライバシー」設定では、Security Cloud への参加や、製品の改善のためにパーソナライズされていないデータを提出するかどうかを指定できます。
「プライバシー」画面は「設定」の「プライバシー」を選択することで表示されます。

項目名	内容
より深い分析を可能にする	チェックを付けると、個人情報を含まないセキュリティデータをエフセキュアの Security Cloud に提供し、Security Cloud 上で詳細な分析を行うことで、最新の脅威に対する保護が強化されます。
パーソナライズされていない使用状況データを送信する	チェックを付けると、個人情報を含まないデバイス情報やサービス情報をエフセキュアに提供し、製品自身や提供サービスの改善に貢献できるようにします。

3.3.9　サポート

「サポート」設定では、製品とサポートツールに関する情報が表示されます。
「サポート」画面は、「設定」の「サポート」を選択することで表示されます。

項目名	内容
ID コード	エフセキュアにお問い合わせする際にご利用できるアカウント ID です。 アカウント ID： アカウント情報です。
バージョン情報	インストールされている製品のバージョン情報です。 製品　　：　製品名 バージョン ： バージョン番号
ツール	コンピュータの環境や構成情報と製品に関する設定やログ情報を収集します。ウィズセキュアに問い合わせする際、この情報は調査のために必要不可欠です。 「サポートツールを実行」をクリックすることで診断情報が作成されます。 管理者権限が必要です。 なお、Elements Security Center 管理者からもリモートで実行させることも可能です。 「接続ツールを実行する」をクリックすることで、WithSecure™のバックエンドシステムに接続できるかどうかの確認ができます。
デバッグログ	有効/無効　カスタマーサポートが問題を分析する際に役立ちます デフォルトは無効

3.3.10　一元管理

「一元管理」設定では、コンピュータ情報などコンピュータに関する組織の管理情報を確認できます。
「一元管理」画面は「設定」の「一元管理」を選択することで表示されます。

項目名	内容
製品情報	サブスクリプション：製品名 製品　　：　インストール製品名 バージョン　　：バージョン番号
コンピュータ情報	Wins 名　：Windows WINS 情報 DNS　　：DNS 情報 IP アドレス　：IP アドレス情報 固有の ID　：固有 ID 情報
プロフィール情報	プロフィール名　：適用中のプロフィール名 プロフィール ID　：適用中のプロフィールの持つ ID 情報 前回の変更　　：適用された日付と時刻 (GMT)
Windows イベント	「イベント ビューアを開く」をクリックすると、イベントビューアが起動されます。

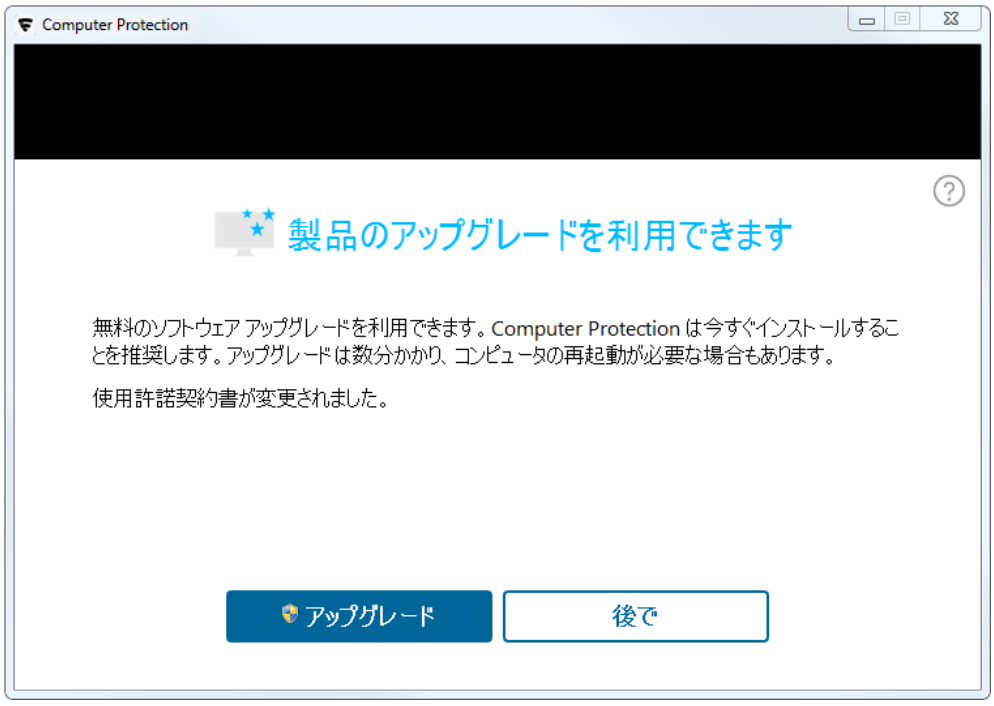
4. 附録

4.1　　アップグレードの通知

Elements EPP / Elements EPP Servers はリブートレスアップグレードを実現しているため、通常はアップグレードの通知は行われず再起動も発生しません。
但し、例外的に使用許諾書（End User License Agreement）の更新においてはアップグレードの通知が行われます。

使用許諾書は、その製品を利用する条件についてユーザと同意を確認するものです。
そのため、この変更が行われた場合には、新たにユーザの同意の確認を得る必要があり、必ずアップデートの通知が行われます。

アップグレードの通知画面のサンプルは、以下の通りです。
通常、このアップグレードの通知では再起動の必要はございませんが、お客様のご利用状況によっては再起動が必要な場合があります。



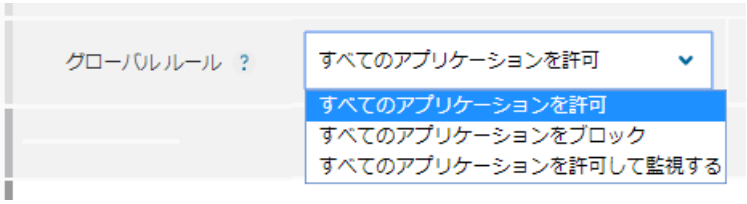
4.2 セキュリティのステータスアイコン

ステータスアイコン	ステータス	説明
	正常	デバイスは保護されています。 セキュリティ保護機能は有効になっており、正常に動作していることを示します。 処置は不要です。
	失効	デバイスは保護されていません。 ライセンスが失効しました。 処置が必要です。
	失効と無効	デバイスは保護されていません。 ライセンスが失効しており、製品も無効になっています。 処置が必要です。
	無効、故障	デバイスは完全もしくは一部保護されていません。 処置が直ちにに必要でがあることを示します（重要な機能が無効、またエラーになっている、または、アップデートが長い間更新されていない場合など）。
	無効	デバイスは保護されていません。 処置が必要な操作（セキュリティ機能が無効など）があることを示します。
	更新中	設定を変更しています。もしくは、製品を更新しています。 処置は不要です。

4.3　アプリケーション制御：除外ルールについて

アプリケーション制御は、Premium 版に搭載されている機能で、アプリケーションやインストーラ、及び。
スクリプトのインストールや起動に対する保護を強化する優れた機能です。
エフセキュアによってあらかじめ定義されたルールでは一般的な攻撃経路の多くをブロックする事が可能です。
また、独自のルールを追加することもできます。

利用する際、まずグローバルルールにて“すべてのアプリケーションを許可”とした上でブロックしたいものをルールに追加する運用と、グローバルルールにて“すべてのアプリケーションをブロック”とした上で許可したいものをルールに追加する運用のどちらで運用されるかをお決めください。



新しいルールを作成する時には、ルールの順序が重要となります。
例えば、一般的なブロックルールの前に特定の許可ルールを作成して、特定のアプリケーションの実行を許可することができます。
プロファイルエディタの矢印を使用してルールの順序を変更できます。

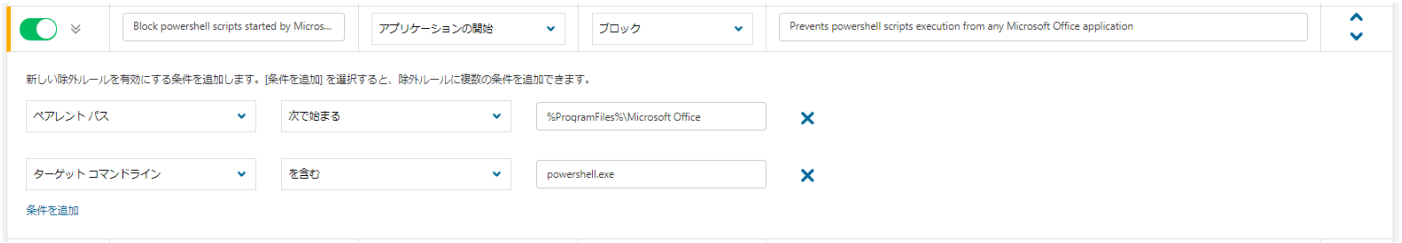
ここでは、一般的なゼロデイ攻撃や標的型攻撃など、アプリケーション制御が攻撃を回避する方法を概説します。
主なシナリオは次の 3 種類です。

・Microsoft Office の脆弱性悪用を防ぐ
・不要なアプリケーションをブロックする
・脆弱なアプリケーションをバージョン別に制限する

4.3.1 Microsoft Office の脆弱性悪用を防ぐ

マルウェアの MS Office の脆弱性を悪用利用した攻撃が増加しており、この種のマルウェアが社内ネットワークに到達するドキュメントを介して拡散されることが、より一般的になっています。
マルウェアが侵入すると、被害者のホストに自分自身を設定し、PowerShell スクリプトエンジンなどの新しいプロセスを起動する可能性もあります。

そのため、管理者として組織のセキュリティを強化したり、Microsoft Office プログラムが他のアプリケーションを起動したりできないようにすることができます。
Microsoft Office アプリケーションは通常他のアプリケーションを起動しないため、この種の制限は通常のユーザの作業には影響しません。



スクリーンショットの設定では、以下の制限を行います。

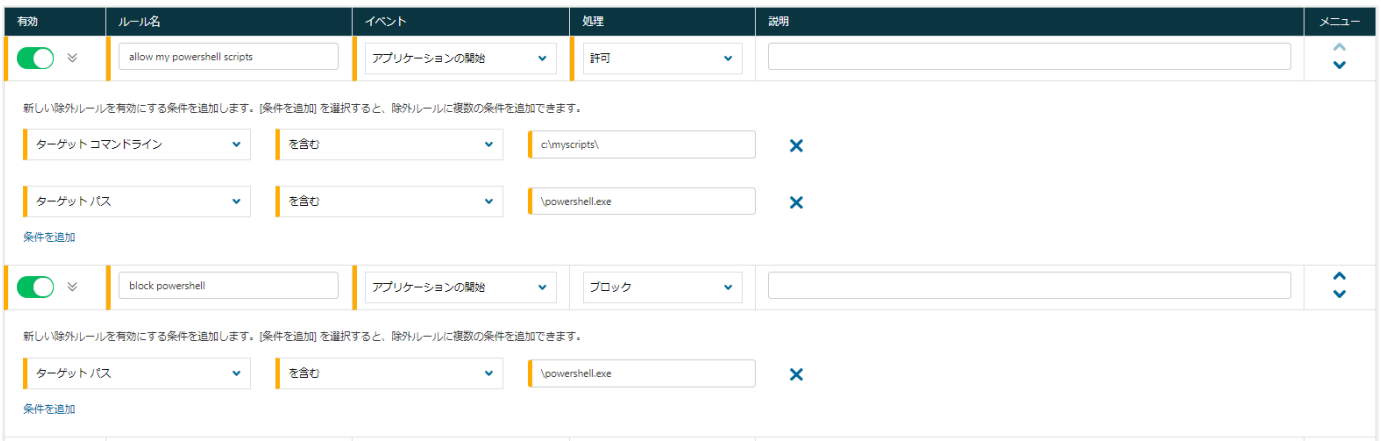
“ペアレントパス” パラメータは、winword.exe などのアプリケーション・ランチャーを参照します。

注： 除外規則では、Microsoft Office はデフォルトの場所にインストールされ、%Program files%環境変数を使用すると想定しています。 アプリケーション制御は、システムとユーザの環境変数をサポートします。

“ターゲットコマンドライン” パラメータは powershell.exe プロセスのみをブロックすることでルールをさらに制限します。

注： MS Office からすべてのアプリケーションを起動しないようにするには、2 番目のパラメータを削除します。

powershell.exe は一般的にワークステーションの設定に使用されるため、必要に応じて powershell.exe の制限を無効にし、自分の個人用スクリプトのみを許可する追加の規則を作成できます。
以下のスクリーンショットでは、管理スクリプトは C:¥myscripts の下に保存されていると仮定しています。



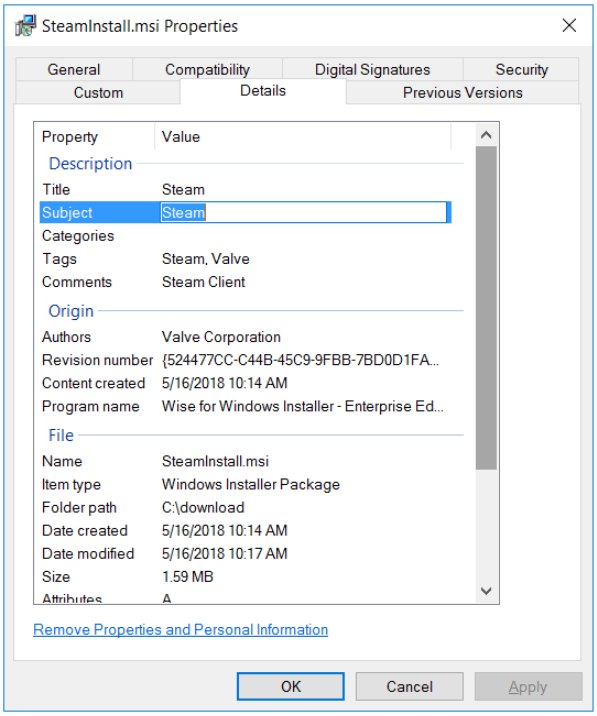
“ターゲットコマンドライン” 条件が C:¥myscripts¥ の場合、除外規則は明示的に powershell.exe の実行を許可します。
例えば、次の powershell コマンドは実行されます。
powershell C:¥myscripts¥login.ps1

注：除外規則ではパスの内容を照合するために "を含む" 条件が使用されます。
しかし、この条件の場合、意図せずに誤って "C:¥powershell.exe¥myprogram.exe" パスとも一致します。
これを回避する別の選択方法として、“に等しい” 規則を使って、次のパス名との完全一致を指定することができます。
"%SystemRoot%¥WindowsPowerShell¥v1.0¥powershell.exe"
（または "次で終わる" 条件を使用してください。）

4.3.2　不要なアプリケーションをブロックする

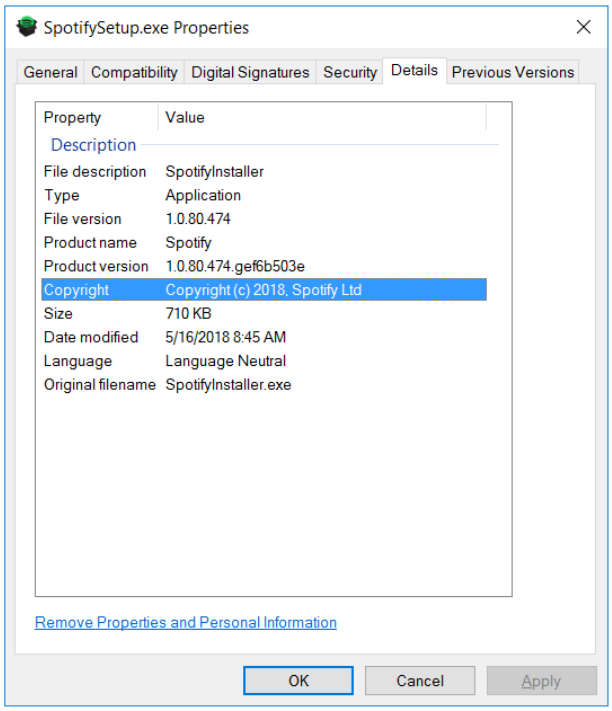
アプリケーション制御は、不要なアプリケーションの実行をブロックするのにも役立ちます。
次の例はゲームの「Steam」のインストールをブロックする方法を示しています。

この規則は、Properties ファイルにある MSI インストーラ、および、ブロックについてはインストーラのサブジェクト別に指定されています。



アプリケーション制御を使用すると、アプリケーションのさまざまなメタプロパティに対するルールを指定できます。
次の例は、著作権で Spotify をブロックする方法を示しています。

このルールは、ファイルがどこにインストールされているかにかかわらず、Spotify の起動をブロックします。 これらのプロパティはファイルの詳細に表示されます。

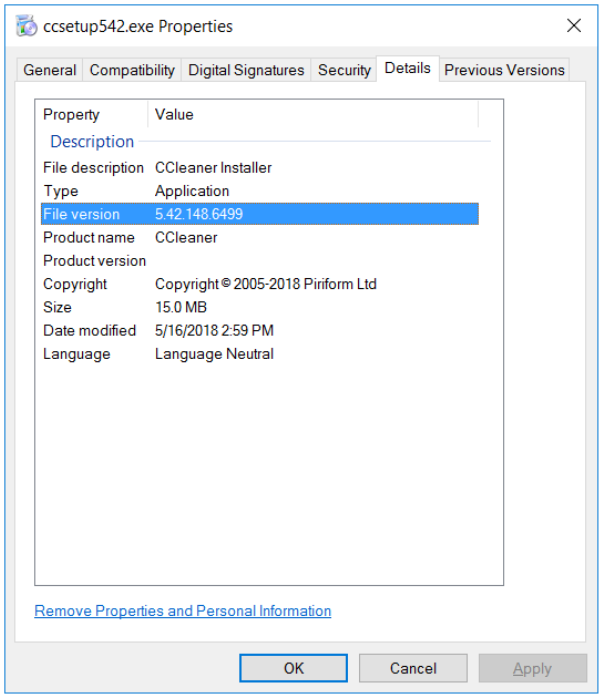

SpotifySetup.exe Properties
General
Compatibility
Digital Signatures
Security
Details
Previous Versions
Property
Value
Description
File description
SpotifyInstaller
Type
Application
File version
1.0.80.474
Product name
Spotify
Product version
1.0.80.474.gef6b503e
Copyright
Copyright (c) 2018, Spotify Ltd
Size
710 KB
Date modified
5/16/2018 8:45 AM
Language
Language Neutral
Original filename
SpotifyInstaller.exe
Remove Properties and Personal Information
OK
Cancel
Apply

4.3.3　脆弱なアプリケーションをバージョン別に制限する

アプリケーション制御は、脆弱性のあるアプリケーションの実行を制限する（たとえば、パッチが適用されていないバージョンをブロックするなど）のに役立ちます。
一例として、CCleaner が最新バージョン 5.42.148.6499 で重大な脆弱性が修正されており、それより古いバージョンはブロックすることができます。

ターゲットファイルバージョンの条件が 5.41.*.*以下である。アスタリスクフィールドは、メジャーフィールドとマイナーフィールドのみが比較に使用されることを示します。
“CCleaner” の記載がターゲットファイルの説明欄にあれば、対象プログラムはファイル名またはその場所に関係なくブロックされます。

ヒント：ファイルのバージョンを確認するには、プロパティファイルを確認してください。



4.3.4 アプリケーション制御の規則で使用される評価と普及率プロパティについて

評価のプロパティ：評価プロパティには、次の値を指定できます。

範囲	タイプ	意味
0-9	クリーン	クリーンなものとして知られておりすべて許可します。
10-79	プロンプト	不審または不要と思われる（PUA)またはリスクウェア。 プロンプトでローカルユーザから操作を促します。
80-89	不要	不要なアプリケーション。 除外オプションで自動検疫します。
90-100	ブロック	悪意のあるものといて知られておりすべての行動をブロックします。
101-999	不明	ローカルで決定します。 応答がない（空の応答）場合もこれがデフォルトです。

普及率プロパティ：普及率プロパティには次の値を指定できます。

Value	Meaning
0	未定義または不明なファイル。 応答がない場合やこのフラグがない場合も、これがデフォルトです。
1	珍しいファイル（3 ヒット以下）
10	非常に稀なファイル（10 ヒット以下）
20	かなり稀なファイル（100 ヒット以下）
30	稀なファイル（1,000 ヒット以下）
40	珍しいファイル（1 万ヒット以下）
50	かなり一般的なファイル（10 万ヒット以下）
60	一般的なファイル（100 万ヒット以下）
70	一般的なファイル（1,000 万ヒット以下）
80	非常に一般的なファイル（1 億ヒット以下）
90	非常に一般的なファイル（10 億ヒット以下）
100	ほとんどのユーザが所有しているファイル（100 億ヒット以下）