Yarai
Home and Business Edition
操作ガイド

Version 1.4.2

FFRI Security, Inc.

目次

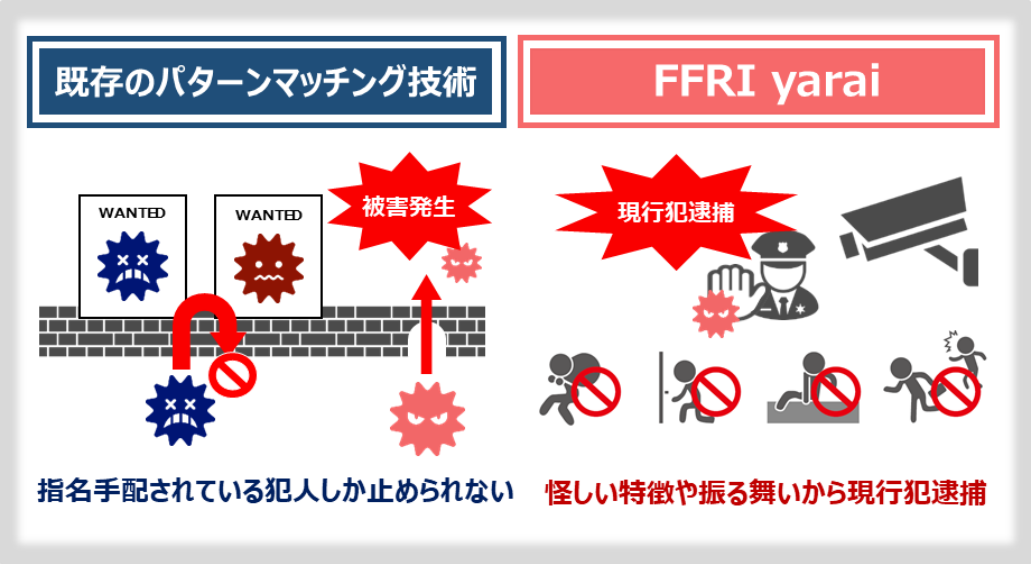
1 FFRI yarai のコンセプト

1.1 今までにないセキュリティ

FFRI yarai および FFRI yarai Home and Business Edition は、未知の脅威に特化した、日本発の次世代エンドポイントセキュリティです。

一般的なウイルス対策ソフトは出回ったマルウェアの定義ファイルを用いるパターンマッチング技術により防御を行っています。

FFRI yarai は定義ファイルに依存せず、マルウェアの振る舞いを見て防御する仕組みです。



FFRI yarai の防御イメージ図

※未知の脅威 …… セキュリティベンダーに発見されていない脆弱性（OS やアプリケーションなどに存在する、保安上の欠陥・弱点）を突いた攻撃やマルウェアのこと。これらは OS のアップデートや、パターンマッチングをベースとしたウイルス対策ソフトだけでは防ぐことができない。近年のサイバー攻撃は、未知の脅威を用いるケースが多く見受けられ、新たな対策を講じる必要がある。

※マルウェア …… コンピューター・ウイルス、スパイウェアなど、悪意のある目的を持ったソフトやプログラムのこと。

1.2 FFRI yarai の特徴

純国産セキュリティ製品

国内で開発からサポートを実施。FFRI yarai (※1)は政府官公庁、金融機関、大手企業での導入実績も多数。

未知マルウェアを検知

既存のパターンマッチング技術では守ることのできないランサムウェアをはじめとする未知のマルウェアを現行犯逮捕。

他社ソフトと同居可能

一般的なウイルス対策ソフトと同居が可能。同居することでより強固なセキュリティ対策を行うことが可能。(※2)

定期スキャン不要で軽い

パターンファイルの更新や定期スキャンが一切不要。PCへの負担が少なくインストール後も快適。

導入実績が豊富

FFRI yaraiの契約ライセンス数はエンドポイント型標的型攻撃対策分野で販売本数・売上ともに、6年連続No.1(※3)を獲得。

防御実績を公開中

ニュースで話題になったサイバー攻撃も事件発生前にリリースしたエンジンで検知

(※1) FFRI yarai は官公庁、大手～中小企業を対象とした法人向け製品。FFRI yarai Home and Business Edition は FFRI yarai と同じエンジンを搭載した個人・小規模事業者向け製品。

(※2) 同居可能なウイルス対策ソフト：https://www.ffri.jp/products/yaraihb/requirement.htm

(※3) 出典：ミック経済研究所「情報セキュリティソリューション市場の現状と将来展望 2017【外部攻撃防御型ソリューション編】」

防御実績　https://www.ffri.jp/products/yarai/defense_achievements.htm

1.3 防御の仕組み～「先読み防御」技術～

マルウェアの感染前、活動開始時など、静的・動的に保護する 5 つの防御エンジンを搭載しています。

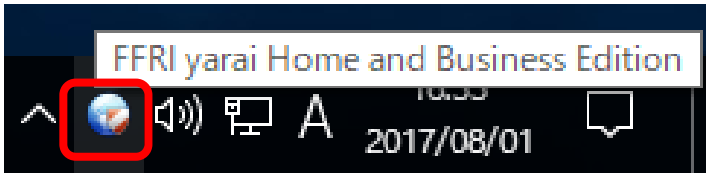
1.4 マルウェア検出後の駆除機能

FFRI yarai Home and Business Edition（以降、yarai HB と呼称）では独自のマルウェア駆除機能を搭載しているため、万が一マルウェアの攻撃が検出されてしまった場合でも、安全に駆除することが可能です。

2 yarai HB のアイコンとメインウインドウ

2.1 タスクトレイのアイコン表示

yarai HB をインストールすると、デスクトップ右下のタスクトレイ内に yarai HB アイコンが表示されます。



アイコンの表示で yarai HB の動作状態を確認できます。

アイコン	内容
	通常のアイコン表示です。システムは安全な状態で動作しています。
	yarai HB のサービスが停止しています。

yarai HB アイコンをクリックすると、メインウインドウが表示されます。

2.2 メインウインドウ

yarai HB メインウインドウの各フィールドについて紹介します。

【メインウインドウ】

1 機能選択タブ： タブをクリックして機能を選択します。選択したタブごとに、メインページに詳細情報や設定項目が表示されます。

項目	内容
ステータス	システムのセキュリティ状態、稼動中のエンジン、yarai HB のバージョン、ライセンスの有効期限を表示します。
スキャン	PC 内のファイルを検査します。 クイックスキャン、フルスキャン、カスタマイズスキャンから選択し、検査対象を指定してファイルを検査できます。
マルウェア管理	検出されたマルウェアを駆除します。 また、過検出かどうかの判定の問い合わせにも利用できます。
ログ管理	マルウェアを検出した日時、マルウェアの存在場所などのイベントを一覧表示します。
設定	稼動するエンジンの選択や、監視対象外リストの登録、ネットワーク設定、サポートに利用します。

❷ メインページ：　タブで選択された機能の詳細ページです。動作状態や設定項目が表示されます。各ページの機能については「各画面の機能」を参照してください。

3 各画面の機能

メインウインドウ上部のタブをクリックして、機能を選択します。

ここでは、各画面でできる動作状態の確認や設定項目について紹介します。

- ステータス
- スキャン
- マルウェア管理
- ログ管理
- 設定

3.1 ステータス

「ステータス」タブを選択したときの画面表示です。
稼動中の検出エンジン、アップデート情報、ライセンスの有効期限が表示されます。

【ステータスタブ】

❶ エンジンステータス： 各検出エンジンの監視状態が表示されます。

アイコン	内容
✔	検出エンジンが監視動作中です。
✖	検出エンジンが稼動していません。

「設定」画面で、検出エンジンごとに有効／無効の切り替えができます。詳しくは「設定」を参照してください。初期設定では、すべての検出エンジンが有効になっています。

❷ アップデート：　インストールされているプログラムのバージョン情報やステータスが表示されます。

項目	内容
製品バージョン	yarai HB 本体のバージョン情報が表示されます。
ステータス	「最新バージョンにアップデートして下さい」と表示されている場合は、アップデートを行い、最新バージョンに更新してご利用ください。 「再起動が必要です」と表示されている場合は、アップデートのために一度コンピューターの再起動を行ってください。 「アップデートサーバへのリクエスト送信に失敗しました。」と表示されている場合は、インターネットへ接続されているか確認してください。

❸ ライセンス：　ライセンスの有効期限が表示されます。有効期限が切れると、すべての機能が利用できなくなります。
ライセンスの購入をクリックすると、新しいライセンスキー（シリアル番号）を購入することができます。

3.2 スキャン

「スキャン」タブを選択したときの画面表示です。

【スキャンタブ】

❶ スキャンの種類：　ドロップダウンリストでスキャンの種類を選択します。

項目	内容
クイックスキャン	重要なフォルダーのみ検査します。
フルスキャン	すべてのドライブ（CD/DVD ドライブ等を除く）を検査します。リムーバブルディスク、ネットワークドライブは画面下部に出現するチェックボックスにより、任意で追加できます。
カスタムスキャン	ドライブやフォルダーを指定して検査します。❷に表示されるツリー表示でドライブやフォルダーにチェックを入れ、検査対象を選択します。「実行」ボタンをクリックすると、チェックを入れたフォルダーの配下にあるすべてのファイルに対し、ファイル検査が実行されます。

❷ スキャン対象：　選択したスキャンの種類により、検査対象となるドライブやフォルダーが表示されます。「カスタムスキャン」を選択した場合は、検査対象のドライブやフォルダーにチェックを入れて指定してください。

❸ 操作ボタン

項目	内容
「実行」ボタン 「終了」ボタン	選択したスキャンを開始します。スキャンのステータスに検査状況が表示されます。スキャン終了時に「終了」ボタンに変化します。
「一時停止」ボタン	実行中のスキャンを一時停止します。「実行」ボタンをクリックすると、一時停止中のスキャンを再開します。
「停止」ボタン	実行中のスキャンを途中で終了します。

【スキャンタブ － スキャン中】

4 スキャンのステータス：実行中の検査状況が表示されます。

項目	内容
ファイル	スキャン中のファイルの存在場所を表示します。
スキャン	スキャンが完了したファイル数と、スキャン対象の総ファイル数を表示します。 ※スキャン中に一時ファイルが削除された場合など、総数が一致しないことがあります。
検出	検出されたマルウェアの数を表示します。検出したマルウェアの詳細は、「マルウェア管理」画面や「ログ管理」画面に表示されます。
エラー	スキャンに失敗したファイルの数を表示します。
経過時間	スキャン開始からの経過時間を表示します。
状況	準備中、スキャン中、完了などスキャン状況を表示します。スキャンの進捗状況はプログレスバーで確認してください。

スキャンの実行結果は、「ログ管理」画面のログに「オンデマンドスキャン」として記録されます。

3.3 マルウェア管理

「マルウェア管理」タブを選択したときの画面表示です。

「マルウェア一覧」に yarai HB が検出したマルウェアの一覧が表示されます。

【マルウェア管理タブ】

1 マルウェア一覧： 検出したマルウェアが一覧表示されます。

アイコン	内容
	マルウェア検出アイコンです。 マルウェアが検出された場合に表示されます。「駆除」ボタンまたは「監視対象外リストに入れる」ボタンで処理を進めてください。

❷ 操作ボタン

項目	内容
「お問い合わせ」	過検出判定の問い合わせやマルウェアのアップロードを行います。  「過検出判定のお問い合わせ」では、検知されたファイルを zip ファイルに圧縮します。 お問い合わせフォームが開きますので、zip ファイルを添付の上お問い合わせください。 「製品向上の為にＦＦＲＩセキュリティに提供」では、検知されたファイルをＦＦＲＩセキュリティのクラウドに送信します。 検出率の向上や過検出の低減に役立たせて頂きます。
「駆除」	駆除したいマルウェア（ファイル）を選択し、「駆除」ボタンをクリックしてコンピューターから取り除きます。 駆除を行うと、マルウェア（ファイル）は復元できませんので、ご注意ください。 駆除しても良いものか不明な場合は、過検出判定をご依頼ください。
「監視対象外リストに入れる」	「マルウェア一覧」で選択したファイルを、「監視対象外リスト」に登録します。 たとえば、自作のアプリケーションや、配布元が確認できて実行しても問題ないとわかっているプログラムなど、マルウェアではないファイルが「マルウェア一覧」に含まれていた場合は、「監視対象外リストに入れる」ボタンをクリックし、「設定」画面の「監視対象外リスト」に追加できます。「監視対象外リスト」に登録されたファイルはマルウェアとして判断されません。

3.4 ログ管理

「ログ管理」タブを選択したときの画面表示です。

スキャンの実行結果と検出したマルウェアの情報が一覧表示されます。

【ログ管理タブ】

※イベントログが約 7500 行を超えた場合、約 3500 行の過去ログが自動的に削除されます。

※Windows Defender の一部のログも表示されます。

❶ イベントログ： スキャンの実行結果と検出したマルウェアの情報が一覧表示されます。イベントログのリスト上で右クリックすると、ログのエクスポート（CSV 形式で出力）とログの消去のメニューを選択できます。Windows Defender のログをダブルクリックすると Windows Defender を起動します。

項目	内容
日時	イベントが発生した日時を表示します。
履歴	スキャンの実行結果、または、検出結果を表示します。
プロセス	スキャンイベントでは、スキャンの種別（オンデマンドスキャン）を表示します。マルウェア検出イベントでは、検出したマルウェアのプロセス（ファイル名）を表示します。 Windows Defender のイベントでは、Windows Defender と表示します。
詳細	スキャンイベントでは、スキャンファイル数を表示します。 マルウェア検出イベントでは、検出結果や yarai HB が行った対処を表示します。 Windows Defender のイベントでは、スキャンイベントはその種別（クイックスキャン等）を表示します。その他のイベントでは Windows Defender が行った対処を表示します。
ファイルの場所	検出したマルウェアのフルパスやスキャンした場所を表示します。 Windows Defender のイベントでは、検出したマルウェアのフルパスや、更新された定義のバージョンを表示します。

❷ 詳細表示フィールド： イベントログのリストで選択しているイベントの詳細情報を表示します。

履歴のエクスポート

【ログ管理タブ － 履歴のエクスポート】

「❶イベントログ」のリスト画面を右クリックすると、メニューが表示されます。「名前を付けてログを保存」をクリックするとファイル選択ダイアログが表示されます。保存するファイルを指定すると、イベントログがファイルへエクスポートされます（CSV 形式）。

また、「すべてのログを消去」を選択すると、イベントログが削除されます。

Windows Defender の GUI 起動

【ログ管理タブ – Windows Defender の GUI 起動】

「❶イベントログ」の Windows Defender のログをダブルクリックすると、Windows Defender の GUI が起動されます。

※Windows 10 April 2018 Update 以前から、Windows 10 October 2018 Update 以降にアップデートした環境において、ダブルクリックしても Windows Defender の GUI が起動しない場合があります。

3.5 設定

「設定」タブを選択したときの画面表示です。

検出エンジンやネットワークの設定、監視対象外リストの登録を行います。

検出エンジン

【設定タブ － 検出エンジン】

※検出エンジンの操作は「Administrator」または「コンピューターの管理者」の権限を持つユーザーのみ設定を変更できます。

❶エンジン設定：　有効にする検出エンジンのチェックボックスにチェックを入れ、監視機能を稼動させます。

項目	内容
スタティック分析	ウイルス定義ファイルに依存せずに未知のマルウェアを検出するスタティック分析エンジンを利用します。プログラムのコード部とデータ部を汎用性の高い検出ロジックで分析し、マルウェアを検出します。
サンドボックス	仮想環境でプロセスを命令単位で実行することで、未知のマルウェアを検出するサンドボックスエンジンを利用します。
HIPS	PC で稼動中のアプリケーションの挙動を監視してマルウェアを検出する HIPS エンジンです。マルウェア独特の動きなど不審な挙動を検知すると、マルウェアと判断してブロックします。
機械学習	機械学習による判定の結果、実行中のアプリケーションがマルウェアである可能性が疑われる場合、アプリケーションを停止させます。
リアルタイムスキャンの対象	通常は全てのディスク/ドライブが対象となりますが、通信速度の遅い回線を利用したネットワークドライブを利用するときなど、ネットワークドライブを監視から除外することでパフォーマンスを改善できることがあります。 ※ リアルタイムスキャンとは、ファイルのコピーや実行時に行われる、スタティック分析エンジン及びサンドボックスエンジンによるスキャンを指します。
脆弱性攻撃防御	0-day 攻撃など OS やアプリケーションの脆弱性を突いた攻撃を防ぐ ZDP エンジンを利用します。Web ブラウザ、ワープロソフト、メーラーなど、攻撃に利用されやすいデスクトップ・アプリケーションの脆弱性を悪用した攻撃を防ぎます。
Windows Defender	Windows Defender のリアルタイム保護を利用します。

❷ 操作ボタン

項目	内容
「詳細設定」	P. 26 の「検出エンジンの詳細設定」を開きます。
「適用」	チェックボックスの変更をエンジンに適用します。
「キャンセル」	チェックボックスの変更を元に戻します。

注意

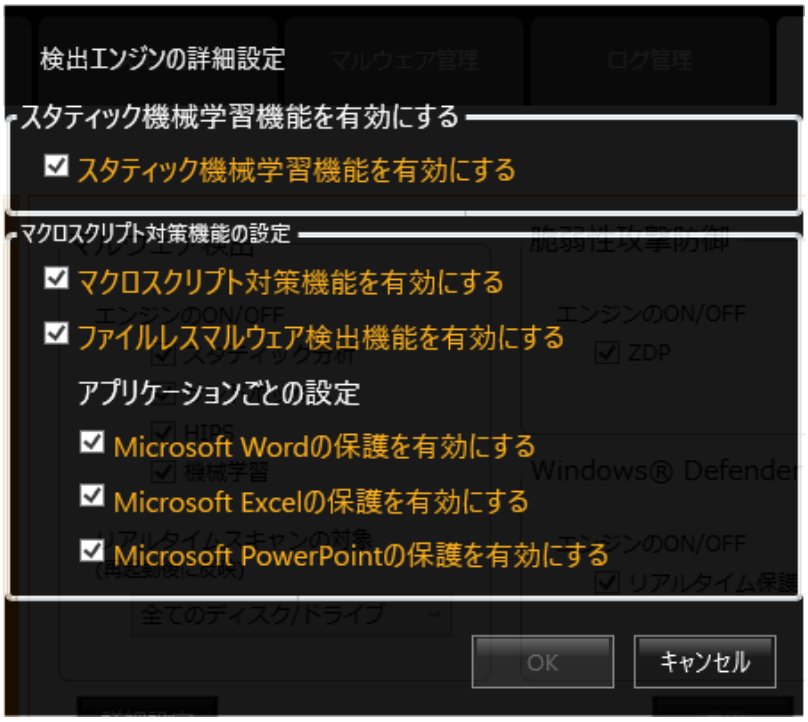
- 通常はすべての検出エンジンを有効にしてご利用ください。

■ **エンジンの依存関係**

各エンジンには依存関係があるため、自動的に設定が行われる項目がありますので、ご注意ください。

項目	内容
スタティック分析	このエンジンを無効にすると、サンドボックス、HIPS も含めたマルウェア検出機能は全て無効となります。
サンドボックス	このエンジンを利用するには、スタティック分析エンジンを有効にする必要があります。
HIPS	このエンジンを利用するには、スタティック分析エンジンを有効にする必要があります。
機械学習	このエンジンを利用するには、HIPS エンジンを有効にする必要があります。

■ **検出エンジンの詳細設定**



□ **スタティック機械学習機能を有効にする**

チェックボックスにチェックを入れると、Static 分析エンジンの機能の一つである、スタティック機械学習機能が有効になります。

□ **マクロスクリプト対策機能を有効にする**

チェックボックスにチェックを入れると、HIPS エンジンの機能の一つである、マクロスクリプト対策機能が有効になります。

□ **ファイルレスマルウェア検出機能を有効にする**

チェックボックスにチェックを入れると、マクロスクリプト対策機能の内部機能の一つである、ファイルレスマルウェア検出機能が有効になります。

□ **アプリケーションごとの設定**

チェックボックスにチェックを入れると、マクロスクリプト対策機能で、それぞれのチェックボックスの項目に対応するアプリケーションの保護が有効になります。

監視対象外リスト

【設定タブ － 監視対象外リスト】

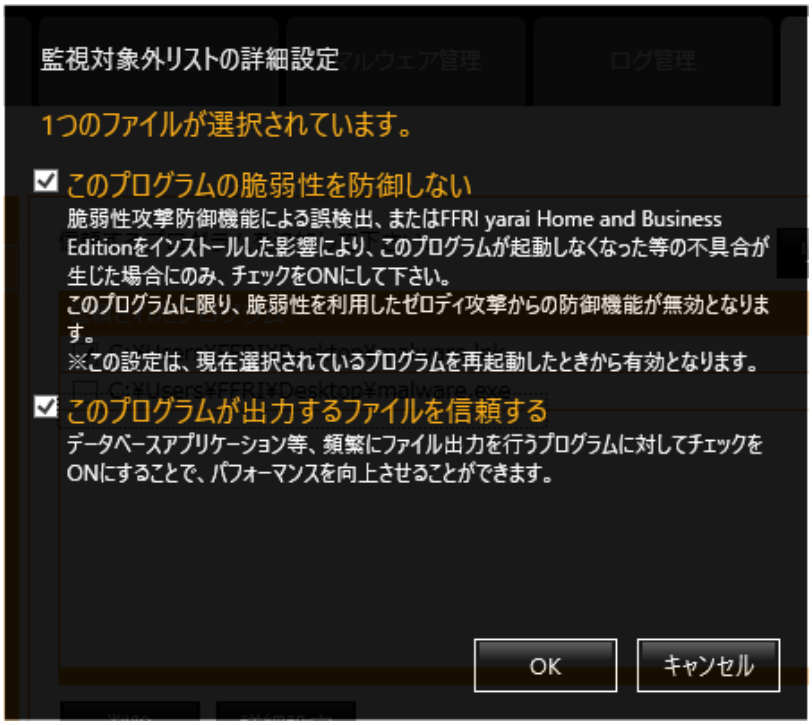
配布元が確認できている等、実行しても問題ないプログラムや自作のアプリケーションがマルウェアと判断されてしまった場合、監視対象外として登録します。

また、データベースアプリケーション等、ファイル操作を頻繁に行うアプリケーションを登録しておくことで、パフォーマンスの低下を防ぐ目的としても利用できます。

項目	内容
1 「リストの管理」	信頼するファイルリストを「監視対象外リスト」に一括で登録します。 「インポート」ボタンをクリックすると、ファイル選択ダイアログが表示されます。登録したいリストファイルを指定し、監視対象外リストに追加します。 また、「エクスポート」ボタンをクリックすると、ファイル選択ダイアログが表示されます。今登録されている「監視対象外リスト」の全てをファイルに出力します。
2 「削除」	登録されたファイルを監視対象外リストから削除します。

❸「詳細設定」	登録されたファイルに対して、オプションで詳細な設定を行うことができます。 脆弱性攻撃防御機能による過検出対策や、パフォーマンスの向上を目的としています。
❹「追加」	指定のファイルやフォルダーを「監視対象外リスト」に登録します。 「ファイル」ボタンをクリックすると、ファイル選択ダイアログが表示されます。リストに登録したいファイルを指定し、追加します。 また、「フォルダー」ボタンをクリックすると、フォルダー選択ダイアログが表示されます。リストに登録したいフォルダーを指定し、追加します。

■ **監視対象外リストの詳細設定**



□ **このプログラムの脆弱性を防御しない**

脆弱性攻撃防御機能によって過検出されてしまうアプリケーションや、誤動作を引き起こすアプリケーションがある場合、リストに登録した上でこのチェックを ON にすることで症状が改善されます。

□ **このプログラムが出力するファイルを信頼する**

このチェックを ON にすると yarai HB のリアルタイムスキャンの監視から除外することができます。ファイル出力を大量に行うプログラムを登録することで、パフォーマンスを向上させることができます。

他に、開発環境など実行ファイルを自ら生成するようなプログラムと競合が発生した場合にも、リストに登録した上でこのチェックを ON にすることにより、多くの場合症状が改善されます。

ネットワーク環境の設定

プロキシ(※)を利用していないユーザーは設定の必要はありません。

インターネット接続にプロキシをご利用の場合は、本設定を行うことにより

yarai HB のアップデートやライセンス認証時、お知らせ機能のインターネット接続にプロキシを利用できます。

※プロキシ・・・企業や組織などの内部ネットワークとインターネットの間に設置し、内部のコンピューターの代理としてインターネットとの接続を行うコンピューターのこと。

【設定タブ － ネットワーク】

項目	内容
プロキシを有効にする	チェックボックスを ON にすると、以降で設定する内容が有効になります。
インターネットオプションの設定を使用する	ホスト名とポート番号を自動的にインターネットオプションの設定から取得します。 初期状態ではこの設定が有効になっています。
プロキシサーバー	プロキシサーバーのホスト名、もしくは IP アドレスを入力します。
ポート番号	プロキシサーバーへの接続に利用するポート番号を入力します。
ユーザー名	認証が必要なプロキシを利用している場合は、ユーザー名を入力する必要があります。
パスワード	認証に必要なパスワードを設定します。

※コンピューターの管理者の権限を持つユーザーが設定を行うと、共通設定にもプロキシの設定が反映され、そのコンピューターの全てのユーザーが設定されたプロキシを利用できるようになります。
ユーザー毎に異なるプロキシを設定したい場合は、そのユーザーでログオンした後、改めて設定を行ってください。

※認証が必要なプロキシに関しては、BASIC 認証による動作確認を行っております。

※ダイレクトに接続を行う場合は、全てのチェックボックスが OFF になるよう設定を行ってください。

※プロキシを設定するには管理者ユーザーとしてログオンしている必要があります。

サポート

製品に関するお問い合わせや、ライセンスキー(シリアル番号)の確認、ライセンス解除を行うことが可能です。

【設定タブ － サポート 1】

【設定タブ － サポート 2】

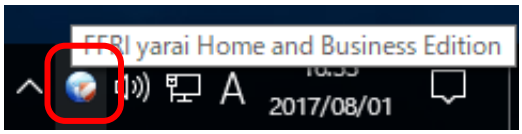
【設定タブ － サポート 3】

項目	内容
❶「マルウェア管理を閲覧する」	マルウェア管理タブを開きます。
❷「お問い合わせ用のログを収集する」	お問い合わせ用のシステム情報を ZIP に圧縮し、任意の場所に保存できます。
❸「シリアルナンバー」	現在使用中のライセンスキー(シリアル番号)を確認できます。
❹「ディアクティベーションする」	現在使用中のライセンスを解除できます。ライセンス解除については 6.1 ライセンス解除を参照して下さい。

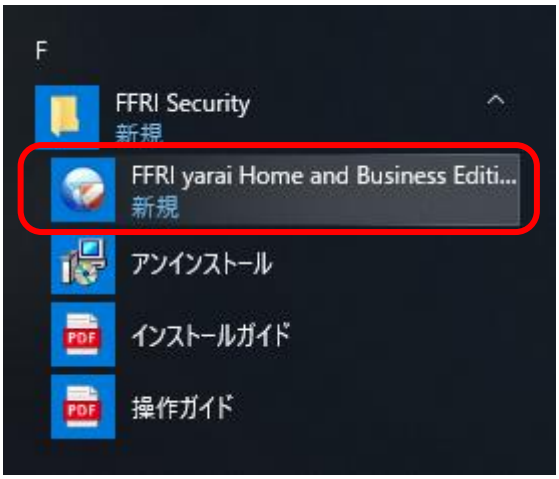
4 yarai HB の使い方

タスクトレイの yarai HB アイコンをクリック、または、「スタート」＞「FFRI Security」＞「FFRI yarai Home and Business Edition」を選択すると、メインウインドウが表示されます。このメインウインドウで機能タブをクリックし、各機能をご利用ください。

- 手動スキャン（フォルダーやファイルを指定して検査したいときに検査を実行します）
- マルウェアの検出
- 監視対象外リストの設定（指定のファイルがマルウェアとして判断されないように登録します）
- マルウェアの駆除（検出されたマルウェアを PC から取り除きます）
- 検出したファイルのアップロード
- お知らせ機能



【タスクトレイ】



【スタート ＞ FFRI Security】

4.1 手動スキャン

任意のフォルダーやファイルに対し、手動でファイル検査を実行できます。

メインウインドウの「スキャン」画面からフォルダーを指定してスキャンする

メインウインドウの「スキャン」画面で検査対象のフォルダーを指定してスキャンする方法です。

1 **タスクトレイの yarai HB アイコンをクリックし、メインウインドウを表示します。**

2 **「スキャン」タブをクリックします。**

3 **ドロップダウンリストでスキャンの種類を選択し、スキャン対象を指定します。**

- **クイックスキャン**
  重要なフォルダーのみ検査します。
- **フルスキャン**
  すべてのドライブ（CD/DVD ドライブ等を除く）を検査します。
  リムーバブルディスク、ネットワークドライブは画面下部に出現するチェックボックスにより、任意で追加できます。
- **カスタムスキャン**
  ドライブやフォルダーを指定して検査します。
  ツリー表示でドライブやフォルダーにチェックを入れ、検査対象を指定します。
  チェックを入れたフォルダー／ドライブの配下にあるすべてのファイルが検査対象となります。

4 **「実行」ボタンをクリックします。**

選択したフォルダー内のファイルに対し、スキャンが開始されます。スキャン実行中の検査状況がスキャンのステータス画面に表示されます。

スキャン実行中

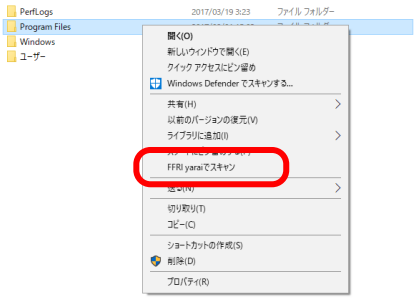
- **「一時停止」ボタン**
  実行中のスキャンを一時停止します。「実行」ボタンをクリックすると、一時停止中のスキャンを再開します。
- **「停止」ボタン**
  実行中のスキャンを途中で終了します。

エクスプローラー画面でフォルダーを右クリックしてスキャンする

エクスプローラー画面で検査対象のフォルダーやファイルを選択してスキャンする方法です。

1 **エクスプローラー画面を開きます。**

2 **検査対象のフォルダーまたはファイルを右クリックし、メニューから「FFRI yarai でスキャン」を選択します。**



エクスプローラー画面で右クリック

3 **選択したフォルダー内のファイルまたは選択したファイルに対し、スキャンが開始されます。スキャン実行中の検査状況がスキャンのステータス画面に表示されます。**

スキャン実行中

- 「一時停止」ボタン：
  実行中のスキャンを一時停止します。「実行」ボタンをクリックすると、一時停止中のスキャンを再開します。
- 「停止」ボタン：
  実行中のスキャンを途中で終了します。

注意

- 手動スキャンを既に実行中の場合、右クリックからのスキャン機能はご利用できません。
- 32 ビット OS のみでご利用になれます。

4.2 マルウェアの検出

yarai HB はマルウェアを検出すると、警告画面が表示されます。

マルウェアを検出した場合

デスクトップの画面右下に警告ダイアログが表示されます。

【警告ダイアログ】

「詳細を表示する」をクリックするとログ管理画面が表示されます。

脆弱性攻撃を検出した場合

デスクトップの画面中央に警告ダイアログが表示されます。

【警告ダイアログ】

「詳細を表示する」をクリックするとログ管理画面が表示されます。

この画面が表示された場合、利用中の正常なアプリケーション(この画面では iexplore.exe というマルウェアではない通常のアプリケーション)が攻撃を受けている可能性があります。

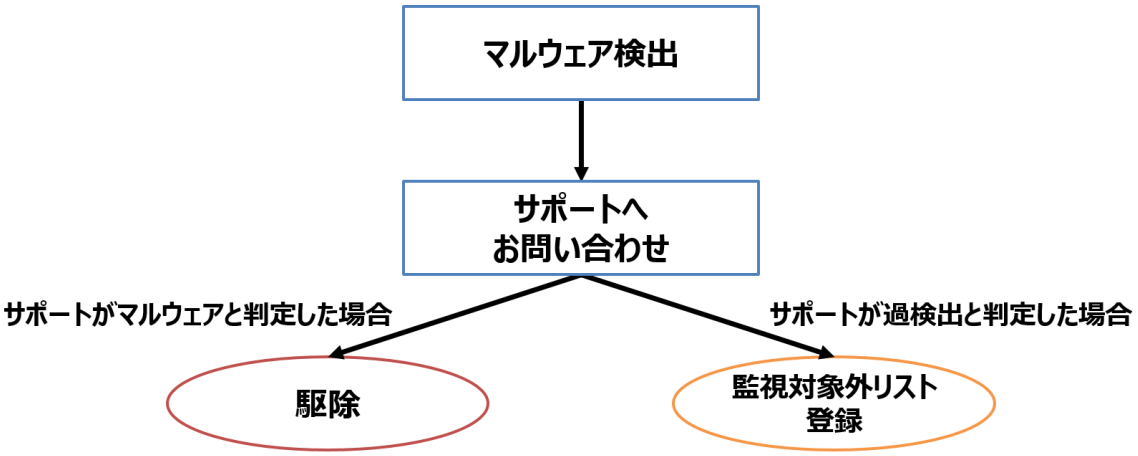
終了ボタンをクリックすることで、利用中のアプリケーションを直ちに終了し、攻撃を止めることができます。

4.3 マルウェア検出後の対応について

検出したファイルは、すぐに駆除は行わず、必ずサポートへお問い合わせください。

本製品は、一般的なウイルス対策ソフトとは異なり、ヒューリスティック検出技術（プログラムの挙動・振る舞いを見て悪意を判断する）を用いてマルウェアの検出を行う製品です。

そのため、マルウェアと類似した動きを行う、正常なプログラム（アプリケーションソフト）を過検出する場合があります。サポートの回答でマルウェアと判明したファイルは駆除を、過検出と判明したファイルは監視対象外リストへの登録をお願いいたします。



【マルウェア検出後の流れ】

4.4 マルウェア検出後のお問い合わせ方法について

検出されたファイルが本当にマルウェアかどうかお問い合わせする

検出されたマルウェアは「マルウェア管理」画面の「マルウェア一覧」に アイコンで表示されます。ファイルを選択して、処理を進めてください。

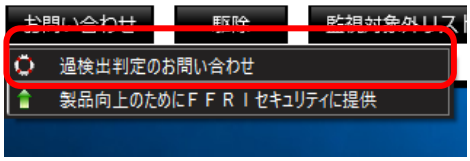
1 **タスクトレイの yarai HB アイコンをクリックし、メインウインドウを表示します。**

2 **マルウェア管理タブの「マルウェア一覧」でアップロードするファイルを指定します。**

対象ファイルの左側にあるチェックボックスをチェックして個別にファイルを選択、または、最上部のチェックボックスをチェックして表示されているすべてのファイルを選択してください。

マルウェア一覧

3 **「お問い合わせ」ボタンをクリックし「過検出判定のお問い合わせ」を選択します。**



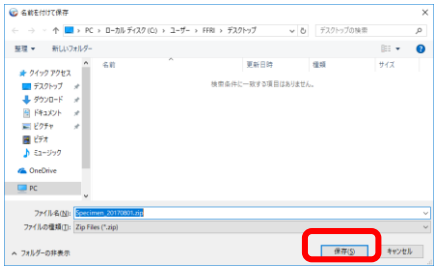
4 **「マルウェア過検出判定お問い合わせ用ファイル作成」のメニューが表示されますので、「保存先の指定」ボタンをクリックします。**

ZIP ファイルにシステム情報を含める場合は、「システム情報を含めて ZIP ファイルを作成する」チェックボックスにチェックを入れて下さい。
システム情報があると、分析がより正確に行えますのでチェックを入れていただくことを推奨します。

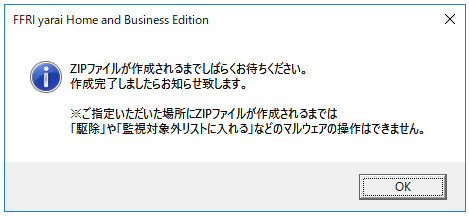
注意

- 判定に必要なファイルが不足している場合など、システム情報が必須となる事があります。

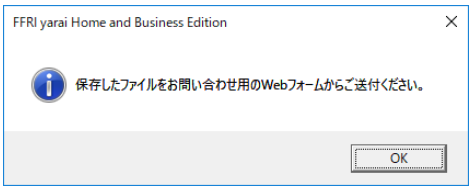
5 **ファイル保存ダイアログが表示されますので、任意の場所を選択し保存をクリックします。**



6 **以下のメッセージが表示されますので、OK をクリックしてお待ちください。**



7 **以下のメッセージが表示されますので、OK をクリックしてください。**



8 **お問い合わせフォームが開きますので、必要事項をご記入の上、送信してください。**

“■ファイルのアップロード” では、先ほど **5** で保存したファイルを選択してください。

※サポートの混雑状況によってはすぐに回答ができない場合がございます。
※判定はベストエフォート対応となります。数が多い場合やファイルサイズが大きい場合を含め、当社にて判定が困難な場合など、 お断りさせて頂くことがございます。
※お問い合わせ受付メールが送られてこない場合は下記をご確認ください。
・メールが迷惑メールフォルダー、ごみ箱に移動されていないか。

4.5 監視対象外リストの設定

配布元が確認できて実行しても問題ないアプリケーションや自作のアプリケーションがマルウェアと判断されないように、「監視対象外リスト」に登録する機能です。指定のプログラムを「信頼されたプログラム」として追加できます。

監視対象外リストにプログラムを追加する

1 **タスクトレイの yarai HB アイコンをクリックし、メインウインドウを表示します。**

2 **「設定」タブをクリックします。**

3 **「監視対象外リスト」フィールドの「追加」ボタンをクリックします。**

「設定」画面

4 **「ファイル」と「フォルダー」のメニューが表示されます。**

ファイルを一つ追加する場合は「ファイル」を、フォルダー内の全てのファイルを指定する場合は「フォルダー」をクリックしてください。

5 **「ファイル」をクリックした場合「ファイルを開く」ダイアログが表示されます。**

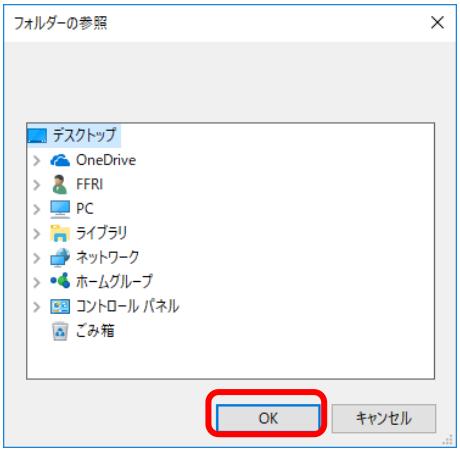
監視対象外リストに登録するファイルを選択し、「開く」ボタンをクリックしてください。

「ファイルを開く」ダイアログ

ステップ 7 へ

6 **「フォルダー」をクリックした場合「フォルダーの参照」ダイアログが表示されます。**

監視対象外リストに登録するフォルダーを選択し、「ＯＫ」ボタンをクリックしてください。



「フォルダーの参照」ダイアログ

7 **指定したプログラムが監視対象外リストに表示されているか確認してください。**

フォルダーを追加した場合パスの最後が「¥*」となります。

監視対象外リスト

注意

- フォルダーを登録すると、サブフォルダーも含めてフォルダー内の全てのファイルが監視対象外となります。あまり広範囲に指定しますと、マルウェアの侵入を許すことになりかねないため、慎重に選択してください。

監視対象外リストにプログラムを一括で追加する

1 **タスクトレイの yarai HB アイコンをクリックし、メインウインドウを表示します。**

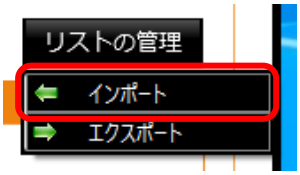
2 **「設定」タブをクリックします。**

3 **「監視対象外リスト」フィールドの「リストの管理」ボタンをクリックします。**

「設定」画面

4 **「インポート」と「エクスポート」のメニューが表示されます。**

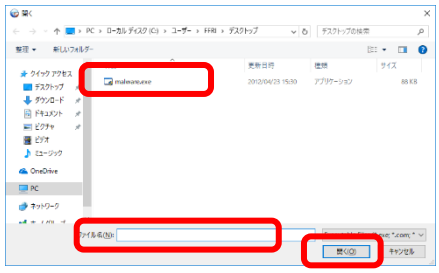
ファイルから取り込む場合は「インポート」を、監視対象外リストを保存する場合は「エクスポート」をクリックしてください。



「リストの管理」メニュー
(インポート選択時)

5 **「インポート」をクリックした場合「ファイルを開く」ダイアログが表示されます。**

監視対象外リストファイルを選択し、「開く」ボタンをクリックしてください。



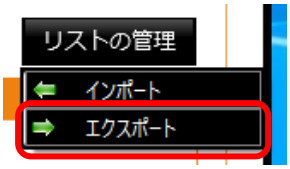
「ファイルを開く」ダイアログ

6 **指定したプログラムが監視対象外リストに表示されているか確認してください。**

フォルダーを追加した場合パスの最後が「¥*」となります。

監視対象外リスト

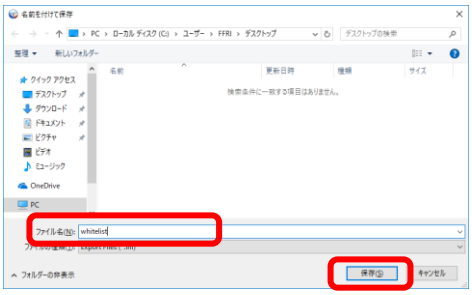
7 「エクスポート」をクリックした場合



「リストの管理」メニュー
(エクスポート選択時)

「名前を付けて保存」ダイアログが表示されます。

監視対象外リストファイルを選択、またはファイル名を指定し、「保存」ボタンをクリックしてください。



「名前を付けて保存」ダイアログ

検出されたマルウェアを監視対象外リストに登録する

1 タスクトレイの yarai HB アイコンをクリックし、メインウインドウを表示します。

2 「マルウェア管理」タブをクリックします。

3 「マルウェア一覧」で アイコンが表示されているプログラムを選択し、「監視対象外リストに入れる」ボタンをクリックします。

「マルウェア管理」画面

4 メインウインドウの「設定」タブをクリックします。「監視対象外リスト」フィールドを表示し、指定したプログラムが監視対象外リストに登録されているか確認してください。

監視対象外リスト

登録済みのプログラムを監視対象外リストから削除する

1 タスクトレイの yarai HB アイコンをクリックし、メインウインドウを表示します。

2 「設定」タブをクリックします。

3 「監視対象外リスト」フィールドの信頼されたプログラム一覧で、削除したいプログラムをチェックボックスで選択し、「削除」ボタンをクリックします。

監視対象外リスト

4 選択したプログラムが監視対象外リストに表示されていないことを確認してください。

検出理由ごとの監視対象外リストの登録方法

① マルウェアを検出した場合

検出されたファイル自体を監視対象外リストに追加してください。検出されたファイルは「マルウェア管理」タブの「マルウェア一覧」から「監視対象外リストに入れる」ことによって追加することもできます。

② 脆弱性攻撃を検出した場合

「脆弱性攻撃を検出」という履歴で検出されたファイルを監視対象外リストに追加してください。また、詳細設定で「このプログラムの脆弱性を防御しない」にチェックを入れてください。

※同時刻に「マルウェアを検出」という履歴がある場合、②の手順は実施せずに、③の手順で監視対象外リストに追加してください。

③ 脆弱性攻撃、マルウェアを同時に検出した場合

「マルウェアを検出」という履歴で検出されたファイルを監視対象外リストに追加してください。検出されたファイルは「マルウェア管理」タブの「マルウェア一覧」から「監視対象外リストに入れる」ことによって追加することができます。

【監視対象外リストの登録】

4.6 マルウェアの駆除

検出されたマルウェアを駆除する

検出されたマルウェアは「マルウェア管理」画面の「マルウェア一覧」に アイコンで表示されます。ファイルを選択して、駆除処理を進めてください。

1 **タスクトレイの yarai HB アイコンをクリックし、メインウインドウを表示します。**

2 **マルウェア管理タブの「マルウェア一覧」で駆除するファイルを指定します。**

対象ファイルの左側にあるチェックボックスをチェックして個別にファイルを選択、または、最上部のチェックボックスをチェックして表示されているすべてのファイルを選択してください。

マルウェア一覧

3 **「駆除」ボタンをクリックし、駆除処理を実行します。**

ステップ 3 で選択したファイルが「マルウェア一覧」に表示されていないことを確認してください。

注意

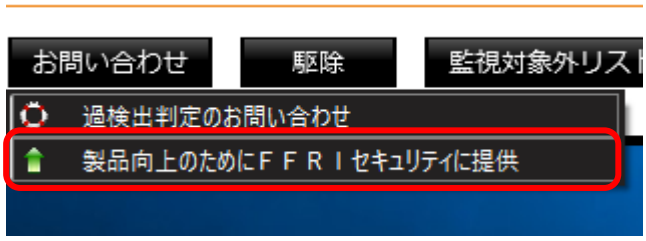
- 駆除したファイルは元に戻す事はできません。重要なファイルであった場合は、過検出判定を依頼の上、駆除を行ってください。

4.7 検出したファイルのアップロード

検知精度向上のため、検出されたファイルをＦＦＲＩセキュリティの専用サーバーへアップロードすることができます。

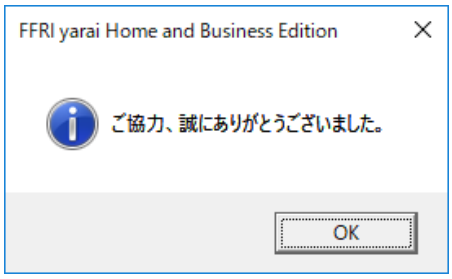
製品の検出率や過検出低減のためにＦＦＲＩセキュリティにファイルを提供する

検出されたファイルをアップロードすることで、yarai HB の性能向上に役立てる事ができます。



1 **お問い合わせと同じ要領で「お問い合わせ」ボタンをクリックし「製品向上の為にＦＦＲＩセキュリティに提供」を選択します。**

2 **以下のメッセージが表示されたら、OK ボタンをクリックしてください。**



※インターネットに接続できない場合など、アップロードができない場合があります。

4.8 お知らせ機能

ＦＦＲＩセキュリティから yarai HB ご利用ユーザーに対して、お知らせがある場合にデスクトップ右下に通知する機能です。

【お知らせダイアログ】

- 「今後同じメッセージは表示しない。」チェックボックス
  - チェックを有効にして、「閉じる」ボタンは押下した場合、新たなお知らせに更新されるまでお知らせは再度表示されません。
- 「閉じる」ボタン
  - お知らせポップアップを閉じます。「今後同じメッセージは表示しない。」チェックボックスを有効にしていない場合、一定時間、再度お知らせが表示されます。
- 「詳細を表示する」ボタン
  - ブラウザが起動し、ＦＦＲＩセキュリティのお知らせ一覧ページが表示されます。再度、お知らせは通知されません。

以下の URL でも過去のお知らせをご確認できます。

https://www.ffri.jp/info/index.htm

5 ライセンス認証（更新時）

注意

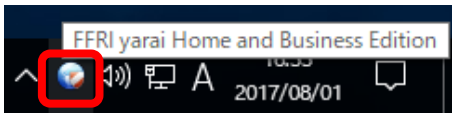
- ライセンスの更新を行う場合は、ライセンス認証された状態で手続きを行う必要があります。
- ライセンス解除した状態や再インストールした状態で、新しいライセンスキー（シリアル番号）を用いてライセンス認証を行うと、元のライセンスの残期間が引き継がれません。
- 必ずインターネットに接続された状態で実施してください。

メモ

- 期間終了時も引き続きご利用頂くには、ライセンスキー（シリアル番号）の登録が必要です。
- ライセンスは FFRI オンラインショップからご購入が可能です。
- ライセンス有効期間終了後でなくても、新たなライセンスキー（シリアル番号）を入力しますと、残期間に新たなライセンスの有効期限が加算されます。
- ステータスタブの「ライセンス」から、ライセンスの有効期限が確認できます。こちらで残期間が引き継がれているかご確認ください。

メインウインドウ

1 タスクトレイの yarai HB をクリックし、メインウインドウを表示します。



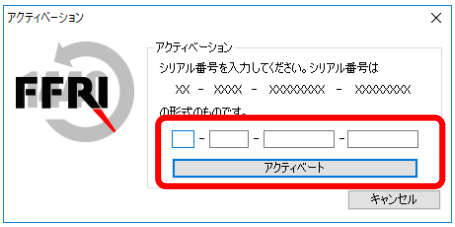
タスクトレイにアイコン表示

2 ステータスタブの「ライセンス認証・更新」をクリックします。

メインウインドウ

3

アクティベーションダイアログが表示されます。
新しいライセンスキー（シリアル番号）を入力し、「アクティベート」ボタンをクリックしてください。



アクティベーションダイアログ

6 ライセンス解除とアンインストール

6.1 ライセンス解除

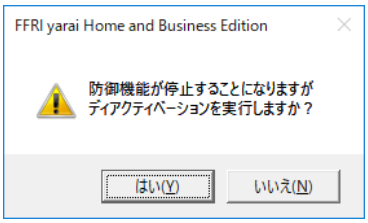
一度ライセンス認証を行ったライセンスキー（シリアルナンバー）を解除することができます。

ライセンスを他の PC に移したり、マザーボードを交換したりする際に利用します。

【ライセンス解除】

1 「設定」タブ内のサポート画面を表示します。

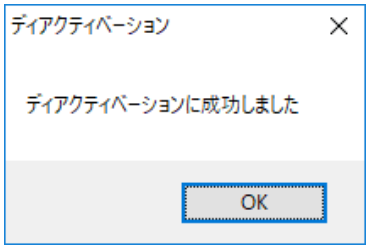
2 「ディアクティベーションする」をクリックすると、警告メッセージが表示されます。



3 「はい」をクリックすると、ライセンスが解除されます。

4 「ユーザーアカウント制御」の確認メッセージが表示されたら「はい」をクリックします。

5 成功すると以下のメッセージが表示されます。



注意

- 必ずインターネットに接続された状態で実施してください。
- ディアクティベート期間中もライセンスの有効日数は消費されますのでご注意ください。

6.2 アンインストール

メモ

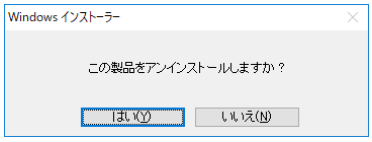
- お使いのパソコンから yarai HB を削除する際の作業です。
- 「Administrator」又は「コンピューターの管理者」の権限を持つユーザーとして Windows にログオンしてからアンインストールを行ってください。
- ユーザー権限の確認方法については、インストールガイドを参照してください。

注意

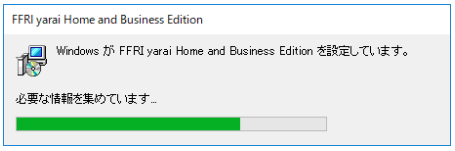
- ライセンスを他のパソコンに移したり、マザーボードを交換したりする際は、P. 55 でご説明したライセンス解除を行った後にアンインストールしてください。

1 **スタートメニューから「FFRI Security」>「アンインストール」をクリックします。**

2 **確認画面で「はい」をクリックします。**

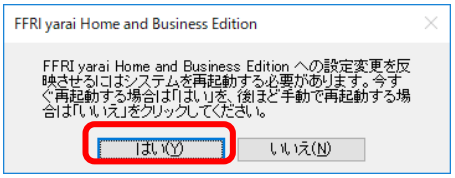


3 **アンインストールが進行します。**



ユーザーアカウント制御の確認画面が表示されたら、「はい」をクリックします。

4 **「はい」をクリックして、Windows を再起動すると、アンインストールが完了します。**



7 マニュアル・FAQ

設定タブには、製品サポートに関する機能があります。

製品マニュアルや FAQ（WEB サイト）へのリンクが用意されています。

不明な点があれば、まずはこちらを確認してください。

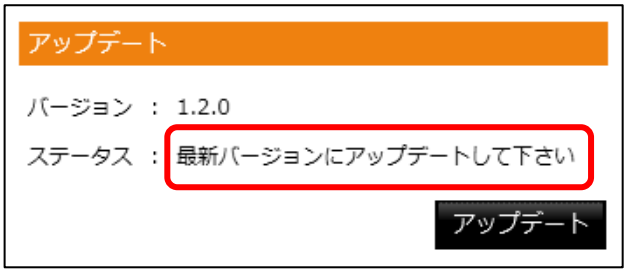
【設定タブ － サポート】

お問い合わせ用の Web フォームへのリンクも用意されています。

マニュアルや FAQ で解決しない場合には、こちらの Web フォーム（**https://regist.ffri.jp/Inquiry/**）よりお問い合わせください。

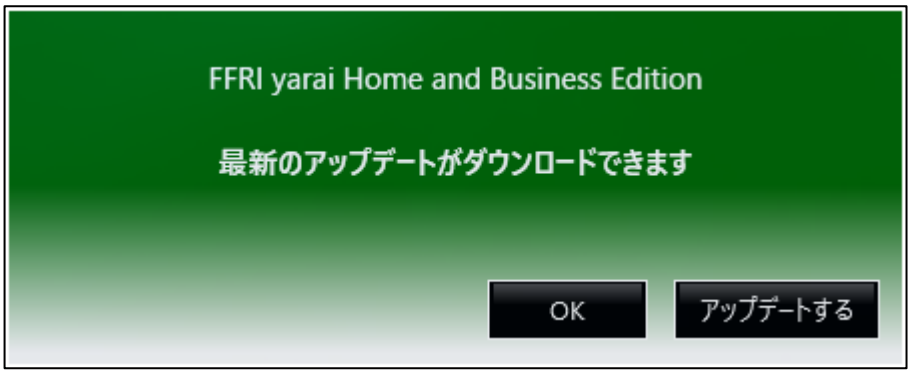
8 アップデート

「ステータス」画面の「アップデート」フィールドに、「最新バージョンにアップデートして下さい」と表示されている場合、お使いの yarai HB は最新の状態に更新されていません。アップデートを実行し、最新バージョンに更新してお使いいただけます。



【アップデートのステータス表示】

また、デスクトップの画面右下にアップデート通知のダイアログが表示されます。



【アップデートの通知】

メモ

- 「Administrator」または「コンピューターの管理者」の権限を持つユーザーとして Windows にログオンしてからアップデートを行ってください。
- ユーザー権限の確認方法については、インストールガイドを参照してください。

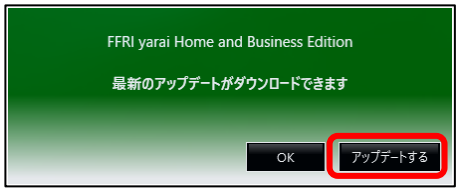
注意

- アップデートを行う際、スキャンを実施しているとスキャンが強制終了されることがあります。

1 **「ステータス」画面の「アップデート」から「アップデート」ボタンをクリックします。**

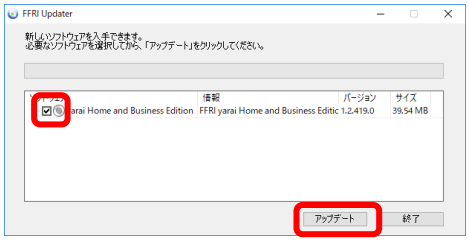
「ステータス」画面

あるいは、アップデート通知の「アップデートする」をクリックします。

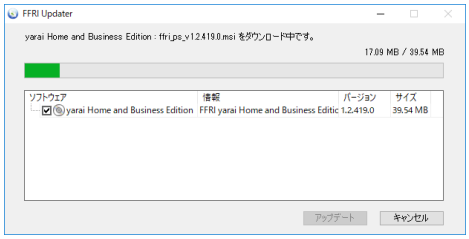


アップデートの通知

2 **アップデート情報が表示されます。yarai HB のチェックボックスにチェックを入れ、「アップデート」ボタンをクリックしてください。**



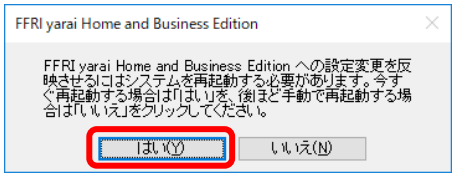
アップデート情報



アップデート中

以降、表示される指示に従ってアップデートを進めてください。

3 **「はい」ボタンをクリックし、コンピューターを再起動すると、アップデートは完了です。**



再起動メッセージ

9 トラブルシューティング

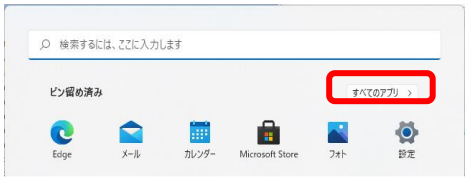
9.1 こんなときは

Q タスクトレイの yarai HB アイコンに「Scan Engine Service あるいは Inject Service のいずれかが停止しています」の通知バルーンが表示される

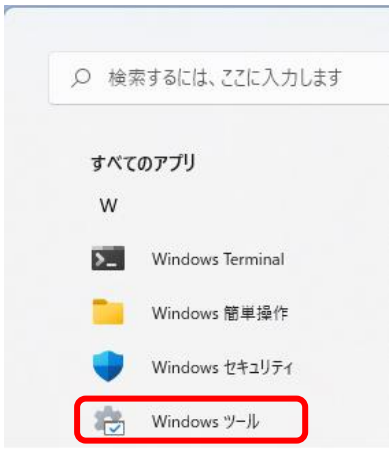
A Scan Engine Service と Inject Service は yarai HB のプログラムです。通常の運用中に停止することはありませんが、システムの状況により、サービスが停止することがあります。自動的にサービスの再起動は実施されますが、上記の通知バルーンが表示された場合は、サービスマネージャから Scan Engine Service または Inject Service の確認を行い停止していた時は起動してください。

■ **Windows 11 の場合**

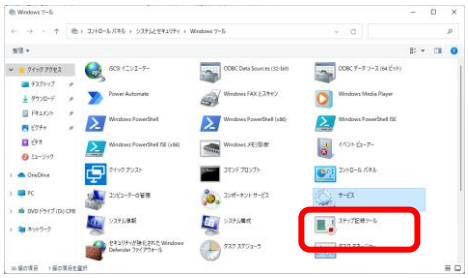
1 「スタートメニュー」から「すべてのアプリ」をクリックします。



2 「Windows ツール」をクリックします。



3 「サービス」をダブルクリックします。



4 FFRI Scan Engine Service (FFRI Inject Service)の上で右クリックし、メニューから「開始」を選択します。

5 タスクトレイのyarai HBアイコンが通常の状態に戻り、通知バルーンが表示されていないことを確認してください。

■ Windows 10 の場合

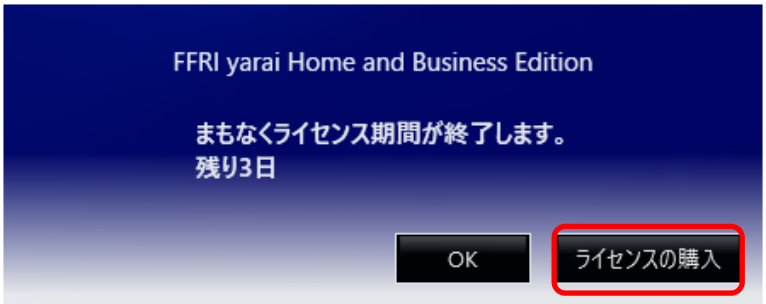
1 スタートメニューから「Windows管理ツール」＞「サービス」をクリックします。

2 FFRI Scan Engine Service (FFRI Inject Service)の上で右クリックし、メニューから「開始」を選択します。

3 タスクトレイのyarai HBアイコンが通常の状態に戻り、通知バルーンが表示されていないことを確認してください。

Q タスクトレイの yarai HB アイコンに「まもなくライセンス期間が終了します。」の通知バルーンが表示される

A yarai HB のライセンスが間もなく切れることを表します。ライセンスが切れると、yarai HB が利用できなくなります。引き続きご利用頂くには、ライセンスを更新して頂く必要がございます。

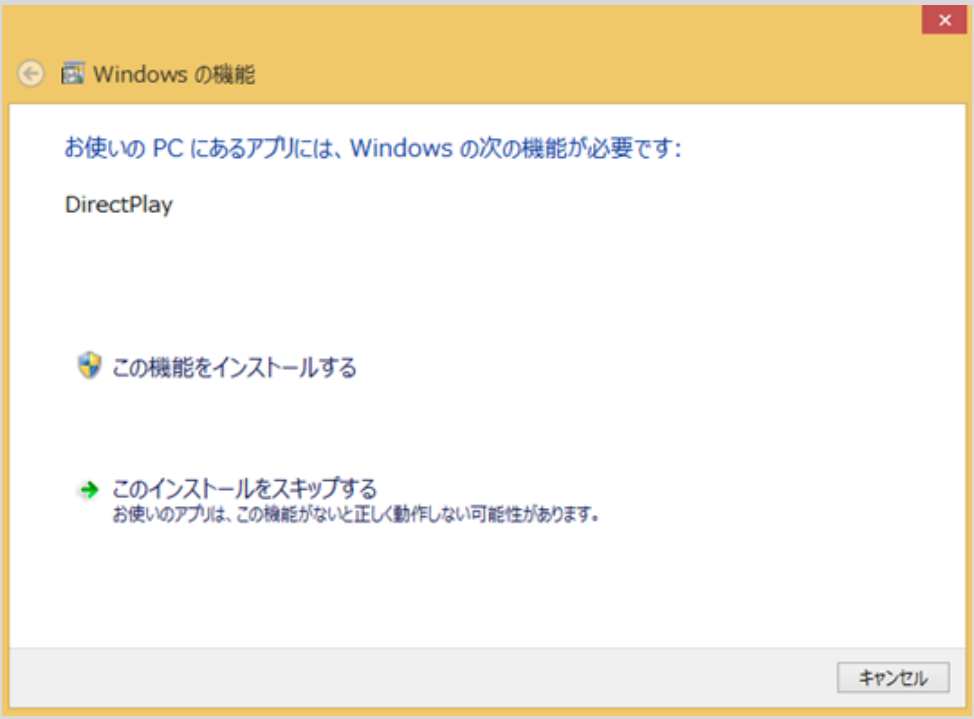


上記ポップアップ画面内の「ライセンスの購入」ボタンをクリックすると、ブラウザで FFRI オンラインショップを開きます。

Q スキャンが途中で終了してしまった

A スキャン中にコンピューターがスリープ状態に入ると、スキャンが停止することがあります。
フルスキャンを行う場合などは、スキャン終了までスリープ状態とならないよう、ご注意ください。

Q スキャン中に「Windows の機能」画面が表示された



A 上記は Windows 8 以降に搭載された「オンデマンド機能」によるものです。yarai HB によるスキャン中などに意図せずに上記画面が表示された場合は、キャンセルボタンを押して画面を閉じてください。

Q スキャン終了後にスキャン結果でエラーが表示されているのですがどうすればいいですか？

A エラーとはスキャンに失敗したファイルの数を示します。
yarai HB は指定した方法（フルスキャン、クイックスキャン、カスタムスキャン）でスキャンを行いますが、各アプリケーションがファイルをロックしている場合スキャンに失敗する場合がございます。
実行ファイル形式でない場合（動画ファイルなど）、スキャンに失敗しても問題はございません。

Q アンインストール中にエラーが発生し、アンインストールができなくなった

A FFRI yarai 削除ツールを利用し、コンピューター内から本製品に関係するファイルを削除することで yarai HB インストール前の状態に戻すことができます。削除ツールの詳細につきましては、サポートまでお問い合わせください。

10 お問い合わせ先

製品に関するご質問は、下記サポートまでお問い合わせください。

10.1 サポート受付・対応時間

平日・土日・祝日 / 10:00～19:00（年中無休）

10.2 電話からのお問い合わせ

0570-004-044（ナビダイヤル）

※ 電話番号のお掛け間違いにご注意ください。

10.3 Web フォームからのお問い合わせ

https://regist.ffri.jp/Inquiry/

10.4 お問い合わせ方法

お問い合わせをいただく前に以下の情報が必要となりますので、事前にご用意をお願いいたします。

- 検出されたファイル（検出されたものについてのお問い合わせの場合）
- ログ
- 詳細な症状および状況（どのような操作をしていたか等）
- （ライセンス認証の場合）ライセンスキー（シリアル番号）

※検出されたファイルとログは「マルウェア管理」タブのアップロードボタンで収集できます。

※ お問い合わせの際に発生する通話料金等はお客様のご負担となります。

※ お問い合わせの内容によっては、回答までにお時間をいただく場合や回答を差し控えさせていただく場合があります。

10.5 ご注意

本マニュアルは作成時の情報に基づき作成されています。製品のバージョンアップなどにより、記載内容と機能が異なる場合がございます。また、本マニュアルは予告なく変更されることがあります。

株式会社ＦＦＲＩセキュリティ

〒100-0005 東京都千代田区丸の内３丁目３番１号 新東京ビル２階