

Version 1.5.0

FFR

(c) FFRI Security, Inc., 2015-2025 / Author: FFRI Security, Inc.



FFRI Security, Inc.

目次

1	FFRI yarai のコンセプト	5
1.1	L 今までにないセキュリティ	5
1.2	2 FFRI yarai の特徴	6
1.3	3 防御の仕組み~「先読み防御」技術~	7
1.4	1 マルウェア検出後の駆除機能	7
2	yarai HB のアイコンとメインウインドウ	8
2.1	L タスクトレイのアイコン表示	
2.2	2 メインウインドウ	9
3	各画面の機能	11
3.1	L ステータス	
3.2	2 スキャン	
3.3	3 マルウェア管理	17
3.4	4 ログ管理	
	履歴のエクスポート	21
1	Microsoft Defenderの GUI 起動	22
3.5	5 設定	
:	検出エンジン	23
	監視対象外リスト	29
	ネットワーク環境の設定	32
	サポート	34
4	yarai HB の使い方	36



4.1 手動スキャン
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37 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
4.2 マルウェアの検出39
マルウェアを検出した場合39 脆弱性攻撃を検出した場合40
4.3 マルウェア検出後の対応について

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	42

4.5	監視対象外リストの設定	44
臣	監視対象外リストにプログラムを追加する	.44
Ē	監視対象外リストにプログラムを一括で追加する	.46
桥	検出されたマルウェアを監視対象外リストに登録する	.48
	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	.49
杉	食出理由ごとの監視対象外リストの登録方法	.50
4.6	マルウェアの駆除	51
杉	食出されたマルウェアを駆除する	.51
4.7	検出したファイルのアップロード	52
4.7	検出したファイルのアップロード	52 . 52

5 ライセンス認証(更新時)54

ライセンス解除とアンインストール......56 6



7	マニュアル・FAQ59
8	アップデート60
9	トラブルシューティング62
9	.1 こんなときは 62
10	お問い合わせ先67
1	0.1 サポート受付・対応時間67
1	0.2 電話からのお問い合わせ 67
1	0.3 Web フォームからのお問い合わせ 67
1	0.4 お問い合わせ方法
1	0.5ご注意



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/yaraihb_requirement
- (※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/products_yarai/defense_achievements



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。



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。





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。

ステータス	スキャン	マルウェア管理	ログ管理	設定
ステータス				
エンジンステータス		アップデ	- ト	
マルウェア検出		バージョン	2 : 1.5.0	
🥩 スタティック分析	🤣 HIPS	ステータス	ス : 最新バージョンがイン	ストールされています
父 サンドボックス	❤️ 機械学習			アップデート
脆弱性攻擊防御				
🤣 ZDP		ライセン	ス	
クラウド連携 ―――		有効期限	: 2025/09/30 (残り 36	5 日間) ライセンスの購
🧼 利用可能			ラ	イセンス認証・更新
Microsoft Defender -				
💜 リアルタイム保護				

【メインウインドウ】

一機能選択タブ: 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。
2	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。



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	スキャン	マルウェア管理	ログ管理	設定	
ステータス					
エンジンステータス		アップデー	k		
マルウェア検出		バージョン	: 1.5.0		
🤣 スタティック分析	💞 HIPS	ステータス	: 最新バージョンがイン	ストールされています	
父 サンドボックス	❤️ 機械学習	2		アップデート	
脆弱性攻擊防御					
🞸 ZDP	1	ライセンス			
クラウド連携 ―――		有効期限	: 2025/09/30 (残り 36	5日間)	
▲ 利田可能		3		<u>ライゼンスの購入</u>	
			7	イゼンス認証・更新	
Microsoft Defender -					
🧼 リアルタイム保護					

【ステータスタブ】

1 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。		
	クラウド連携機能の連携モードが OFF の状態です。		

「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。



2 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。

③ 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。

YARA	lome and Busi	ness Edition		? _ 🗆 ×
ステータス	スキャン	マルウェア管理	ログ管理	設定
スキャン			スキャンの種類とス キャン 1 ク・	ン対象を選択して下さい イックスキャン v
	rname¥De⇔iments			
C:¥Users¥use		al¥Microsoft¥Windows¥	INetCache	
C:¥Users¥use	rname¥AppData¥Loc	al¥Temp	Intecount	
C:¥ProgramD	ata			
🔽 🚽 C:¥Users¥use	rname¥Downloads			
C:¥Users¥use	rname¥AppData¥Roa	aming		
		8	実行	亭止 停止

【スキャンタブ】

	1
--	---

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。 こ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。

2 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。

🔒 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。

Yara	۰ ۱ Hor	ne and Bu	siness Edition			?_□×
ステータス		スキャン	マルウェア管理	ログ管	理	設定
スキャン 4				スキャンの種類	とスキャン対象を フルスキャ	E選択して下さい 7ン 、
ファイル	: C:¥Prog	gram Files¥Inte	rnet Explorer¥ielowuti	l.exe		
スキャン	: 452/1	5387				
検出	: 0					
エラー	: 0					
経過時間	: 00:00::	LO				
状況	: スキャン	/中				
				実行	一時停止	停止

【スキャンタブ - スキャン中】

🙆 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。

Yara	Home and Busin	ess Edition			?_ 🗆 X
ステータス	スキャン	マルウェア管理	ログ	管理	設定
マルウェア一覧					
C:¥Users¥u	isername¥Desktop¥malw	are.exe			
0					
	2	お問い合わせ	駆除	監視対象外	リストに入れる
	_				

【マルウェア管理タブ】

⑦ マルウェアー覧: 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。

2 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。 お問い合わせ 駆除 監視対象外リス ● 過検出判定のお問い合わせ ● 過検出判定のお問い合わせ ● 裂品向上のためにFFRIセキュリティに提供 「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。

人ナータ人	スキャン	マルウェア管理	ログ管理 設定
イベントログ			
日時	履歴	プロセス	詳細
2024/09/30 20	:54 マルウェアを検出	malware.js	不審なファイルが検出されました。
2024/09/30 20	:53 駆除成功	malware.exe	説明: マルウェアの駆除に成功しました。
2024/09/30 20	:53 <mark>駆除成功</mark>	malware.lnk	説明: マルウェアの駆除に成功しました。
2024/09/30 20	:53 <mark>.</mark> 駆除成功	malware.cpl	説明:マルウェアの駆除に成功しました。
2024/09/30 20	:53 駆除成功	malware.vbs	説明:マルウェアの駆除に成功しました。
2024/09/30 20	:52 マルウェアを検出	malware.vbs	不審なファイルが検出されました。
2024/09/30 20	:51 マルウェアを検出	malware.cpl	不審なファイルが検出されました。
2024/09/30 20	:51 マルウェアを検出	malware.cpl	不審なファイルが検出されました。
2024/09/30 20	:50 マルウェアを検出	malware.lnk	不審なファイルが検出されました。
🙆 2024/09/30 20	:50 マルウェアを検出	malware.lnk	不審なファイルが検出されました。
2024/09/30 20	:42 スキャンが完了しました	= オンデマンドスキャン	ファイル数: 1310, スキャン済: 1310, 桃
🙆 2024/09/30 20	:40 マルウェアを検出	malware.exe	不審なファイルが検出されました。
2024/09/30 20	:35 スキャンが完了しました	オンデマンドスキャン	ファイル数: 236205, スキャン済: 1526
2024/09/30 18	:30 定義更新	Microsoft Defender	スパイウェア対策が更新されました。
A 2024/00/20 10	:29 定義更新	Microsoft Defender	ウィルス対策が更新されました。

【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。 ※Microsoft Defender の一部のログも表示されます。

 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。
 Microsoft Defender のログをダブルクリックすると Microsoft 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。 Microsoft Defender のイベントでは、Microsoft 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。 Microsoft 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 Microsoft 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。 Microsoft 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。

2 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。

ステータス	スキャン	マルウェア管理	口グ管理	設定
イベントログ				
日時	履歴	プロセス	詳細	
2024/09/30 20:	54 マルウェアを検出	malware.js	不審なファイルが検出さ	れました。
2024/09/30 20:	53 <mark>駆除成功</mark>	malware.exe	説明:マルウェアの駆除	に成功しました。
2024/09/30 20:	53 🕸 🚓 nyun	imalware.ink	説明: マルウェアの駆除(に成功しました。
2024/09/30 20:	53 🖡 除 💾 名前を付け	てログを保存	説明: マルウェアの駆除	に成功しました。
2024/09/30 20:	53 馬 🞼 🚫 すべてのログ	を消去	説明:マルウェアの駆除	に成功しました。
2024/09/30 20:	52 マルウェアを検出	malware.vbs	不審なファイルが検出さ	れました。
2024/09/30 20:	51 マルウェアを検出	malware.cpl	不審なファイルが検出さ	れました。
2024/09/30 20:	51 マルウェアを検出	malware.cpl	不審なファイルが検出さ	れました。
2024/09/30 20:	50 マルウェアを検出	malware.lnk	不審なファイルが検出さ	れました。
2024/09/30 20:	50 マルウェアを検出	malware.lnk	不審なファイルが検出さ	れました。
2024/09/30 20:	42 スキャンが完了しまし;	た オンデマンドスキャン	ファイル数: 1310, スキ	ャン済: 1310, ;
2024/09/30 20:	40 マルウェアを検出	malware.exe	不審なファイルが検出さ	れました。
2024/09/30 20:	35 スキャンが完了しまし;	た オンデマンドスキャン	ファイル数: 236205, ス	キャン済: 1520
2024/09/30 18:	30 定義更新	Microsoft Defender	スパイウェア対策が更新	されました。
2024/09/30 18:	29 定義更新	Microsoft Defender	ウィルス対策が更新され	ました。

【ログ管理タブ - 履歴のエクスポート】

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。

履歴のエクスポート

Microsoft Defender の GUI 起動

ステータス	スキャン	マルウェア管理	ログ管理 設定
ベントログ			
侍	履歴	プロセス	詳細
2024/09/30 20:54	マルウェアを検出	malware.js	不審なファイルが検出されました。
2024/09/30 20:53	3 駆除成功	malware.exe	説明: マルウェアの駆除に成功しました。
2024/09/30 20:53	3 駆除成功	malware.lnk	説明: マルウェアの駆除に成功しました。
2024/09/30 20:53	3 駆除成功	malware.cpl	説明: マルウェアの駆除に成功しました。
2024/09/30 20:53	3 駆除成功	malware.vbs	説明: マルウェアの駆除に成功しました。
2024/09/30 20:52	2 マルウェアを検出	malware.vbs	不審なファイルが検出されました。
2024/09/30 20:5	マルウェアを検出	malware.cpl	不審なファイルが検出されました。
2024/09/30 20:5	レマルウェアを検出	malware.cpl	不審なファイルが検出されました。
2024/09/30 20:50) マルウェアを検出	malware.lnk	不審なファイルが検出されました。
2024/09/30 20:50	マルウェアを検出	malware.lnk	不審なファイルが検出されました。
2024/09/30 20:42	2 スキャンが完了しました	オンデマンドスキャン	ファイル数: 1310, スキャン済: 1310, 検出
2024/09/30 20:40) マルウェアを検出	malware.exe	不審なファイルが検出されました。
2021/09/30 20.3	スキャンが完了しました	オンデマンドスキャン	ファイル数: 236205, スキャン済: 15267, 1
2024/09/30 18:30)定義更新	Microsoft Defender	スパイウェア対策が更新されました。
2024/09/30 18:25	上药更新	Microsoft Defender	ウィルス対策が更新されました。

【ログ管理タブ - Microsoft Defenderの GUI 起動】

「1 イベントログ」の Microsoft Defender のログをダブルクリックすると、Microsoft 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 Microsoft 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

Yara	Home and Business Edition		? _ 🗆 X
ステータス	スキャンマルウェア管理	ログ管理	設定
設定			
検出エンジン 監視対象外リスト	マルウェア検出	クラウド連携 ―――	
ネットワーク サポート	エンジンのON/OFF 「 スタティック分析 「 サンドボックス	連携モード クラウド連携	~
	 ✓ HIPS ✓ 機械学習 リアルタイムスキャンの対象 (再起動後に反映) 全てのディスク/ドライブ ~ 	Microsoft Defender エンジンのON/OFF ロリアルタイム保護	
	脆弱性攻撃防御 エンジンのON/OFF ☑ ZDP	詳細設定 適用 キャンセル	

【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。

①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。

項目	内容	
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。	
クラウド連携	 クラウド連携機能によって、FFRIセキュリティのクラウド連携サーバーに問い合わせを行い、最新のデータベースによって実行しようとしているプログラムがマルウェアでないかを判定します。 本機能を利用するためには、インターネットへの接続が必要となります。 設定可能な連携モードには下記の3種類があります。 OFF: クラウド連携サーバーとの連携を行わないモードで、以下のようなケースを想定しています。 クラウド連携サーバーとのインターネット接続が行えない環境 クラウド連携サーバーとの通信を行いたくないユーザー ホワイトリスト連携: yarai HB にてマルウェアを検出した場合のみ、クラウド連携サーバー上のデータベースと照合し、逆検出を低減します。 「クラウド連携」よりもネットワークトラフィックへの影響が軽微 クラウド連携: 「ホワイトリスト連携」に加え、ファイルが実行される際にクラウドサーバー上の脅威情報と照合し、一致する場合に起動をブロックします。 デフォルトモード 	
Microsoft Defender	Microsoft Defender のリアルタイム保護を利用します。	

2 操作ボタン

項目	内容
「詳細設定」	P. 27 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。
- クラウド連携機能のうち、クラウド連携モードはアプリケーションの初回実行時 などに、クラウド連携サーバーへの通信が発生する関係上、アプリケーションの 実行に時間がかかることがあります。

下記のように利用不可の状態か、インターネットへの通信を発生させない場合には「設定」タブからクラウド連携の連携モードを「OFF」に設定ください。

? _ ロ ×			? _ 🗆 X
ステータス スキャン	マルウェア管理	ログ管理	設定
ステータス			
エンジンステータス	アップデート	×	
マルウェア検出	バージョン:	: 1.5.0	
 ✓ スタティック分析	ステータス	: アップデートサーバー/ 失敗しました。	ヽのリクエスト送信に
脆弱性攻撃防御 ✓ ZDP	574222		/////-F
クラウド連携	有効期限	: 2025/09/30 (残り 364	4日間)
💥 利用不可		=	<u>ライセンスの購入</u> イヤンス認証・更新
Microsoft Defender			
🤣 リアルタイム保護			

■ 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、機械学習、クラ ウド連携を含めたマルウェア検出機能が無効となります。
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、スタティック分析エンジンとサンドボック スエンジンを有効にする必要があります。
脆弱性攻撃防御	ZDP エンジンは、独立したエンジンのため、依存関係はありません。
クラウド連携	この機能を使用するには、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。

■ 検出エンジンの詳細設定

□ スタティック機械学習機能

チェックボックスにチェックを入れると、スタティック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。

□ オンデマンドスキャンでのディープマクロ分析機能

チェックボックスにチェックを入れると、オンデマンドスキャン時に、スタティック分析 エンジンの機能の一つである、ディープマクロ分析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、それぞれのチェックボックスの項目のファイル に対する、オンデマンドスキャン時のディープマクロ分析機能が有効になります。

□ マクロスクリプト対策機能

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

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。

□ ディープマクロ分析機能

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、ディープマクロ分析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。

● 「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。
🕢 「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。

Yara	Home and Busir	ness Edition		?_□×
ステータス	スキャン	マルウェア管理	ログ管理	設定
設定				
検出エンジン 監視対象外リスト	プロキシサーバー	の設定		
オットワーク サポート	 ✓ プロキシを有効 プロキシサーバー ボート番号 ユーザー名 パスワード 	hにする	 	 インターネット オプションの 設定を使用する

【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。

<u> サポート</u>

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】

項目	内容
①「マルウェア管理を閲	マルウェア管理タブを開きます。
覧する」	
2 「お問い合わせ用の口	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
グを収集する」	¢, à ø
③「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。
④「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。

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】

[X - h > FFRI Security]

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。

- 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。

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。

YAR	21	Home and Bu	siness Edition		? _ 🗆 ×
ステータス		スキャン	マルウェア管理	口グ管理	設定
スキャン				スキャンの種類とスキャン カス	対象を選択して下さい (タムスキャン ジ
ファイル	: c	:¥Users¥All Users¥Mi	crosoft¥Windows Defen	der¥Definition Updates¥Bi	ackup¥mpasbasi
スキャン	: 33	33 / 6610			
検出	: 0				
エラー	: 0				
经通时部	: 0	0:00:05			
状况	: 7	キャン中			
	_				
				東行 一時(it (it

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。

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。

	FFRI y	arai Home	and Busine	ess Ed	ition
		マルウェア	を検出しまし	た	
C:¥Use	rs¥FFRI¥De	sktop¥mal	ware.exe		
			ОК	:	詳細を表示する

【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。

た険な このアン	FFRI yarai Home and Business Edition 動作を検出しました。 プリケーションは攻撃されている可能性があります。
パス	: C:¥Program Files¥Internet Explorer ¥iexplore.exe
プロセスID	: 2068
スレッドID	: 3096
	終了 詳細を表示する

【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。

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。

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。

😨 名教を付けて保	存							×
$\in \rightarrow - \uparrow$	🔲 > PC	» ローカル・ディス	₹7(C) > ユーザー	> FFRI > デスク	リトップ	✓ ð 7201-570	快景	P
整理 ▼ 新し	いフォルター						(iii •	0
クイック アクキ ラスクトップ	ez 🔒	68	^	枝南条件。	東新日時 	推明 6月ません。	97X	
 ダウンロード ドキュメント ビクチャ ビクティ ConeDrive 	* * *							
PC								
7ヶイル名(N: Specin	ven_20170801.zi	ip.					~
ファイルの種類	(): Zip File	ıs (*.zip)					_	~
へ フォルダーの非妻	1.00					便存(5	4177	5.JL

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。

FFRI yarai Hor	ne and Business Edition	×
TIP (†)	ワァイルが作成されるまでしばらくお待ちください。 戎完了しましたらお知らせ致します。	
ж; Г <u>Б</u>	ご指定いただいた場所にZIPファイルが作成されるまでは 「除」や「監視対象外リストに入れる」などのマルウェアの操作はできま	きせん。
		ОК

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。

88	い合わせ	
お問	別い合わせ	
ご利用	用の製品	FFRI yarai Home and Business Edition
Ť	己の事項をご入り	いたきい
シリテ ※ 水準	アルナンバー	(ハイマン区切り)
注文	番号	(ハイフン区切り)
お問。 × あ押	い合わせ区分	選択してください。
製品。 ※此課	バージョン	灌択してください。▼
使用	06 ×老师	選択してください。 ▼
″ 🔳	ファィ	イルのアップロード" では、先
ほと		5 で保存したファイルを選
択し	ってく	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。

「ファイルを開く」ダイアログ ステップ7へ

「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 ×

デスクトップ		
> 🝊 OneDrive		
> 🤱 FFRI		
> 💻 PC		
> 🀂 ライブラリ		
> 💣 ネットワーク		
> 🔩 ホームグループ		
> 🖭 コントロール パネル		
🔯 ごみ箱		
	ОК	キャンセル

「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。

ステータス		マルウェア管理	ログ管理	設定
设定				
検出エンジン	信頼するプログラムを	達加して下さい。		リストの管理
ネットワーク	信頼されたプログラ	4		
サポート	C:¥Users¥user	name¥Desktop¥*		

監視対象外リスト

1 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。

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。

「マルウェア管理」 タブをクリック します。

「マルウェアー覧」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

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。

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。

「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

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。

$\left(\right)$	ara	Home and Busin	ess Edition		? _ □ ×
	ステータス	スキャン	マルウェア管理	ログ管理	設定
-	マルウェア一覧				
	☑ ☑ 🙆 C:¥Users¥us	ername¥Documents¥ma	alware.js		
L			お問い合わせ	駆除 監視対象	めりノストに入れる

【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<u>◎</u>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。

FFRI yarai Home and Business Edition
新しいお知らせがあります。
■test■
これはテスト用のテキストファイルです。 This is a test text file.
○ 今後同じメッセージは表示しない。
閉じる詳細を表示する

【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://product-notify.ffri.jp/ja/yaraihb/info/

ライセンス認証(更新時)

- 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。

间 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。

ステータスタブの「ライセンス認

メインウインドウ

2

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		×
FFR	アクティベーション シリアル番号を入力してください。シリアル番号は ンベ - XXXX - XXXXXX - XXXXXXXX の形にされられです。 	
	キャンセル	
アクテ	ィベーションダイアログ	

6

ライセンス解除とフ	マンイン	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。

Yarai	Home and Busin	ess Edition		?_□×
ステータス	スキャン	マルウェア管理	ログ管理	設定
設定				
検出エンジン 監視対象外リスト ネットワーク サポート	お問い合わせ 保存したファ <u>Webお問い合</u> ■シリアルナンバー	セ用のログを収集する イルをWebお問い合れ わせ窓口	つせ窓口からご送付くた	<i>ೆ</i> ರು.
	■ディアクティベー: ディアクティベー	ション ションする		
			FFI	
	[=	ライセンス解除	}]	
としていた。 します)サポート画面	を表	FFRI yarai Ho	me and Business Edition

「はい」をクリックすると、ライセ

ンスが解除されます。

1

3

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。

ディアクティベーション	×
ディアクティベーションに成功しました	
ОК	

● 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。

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。

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. 56
 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 Sec	タートメニューから「FFRI curity」>「アンインストール」	3	アンインストールが進行します。
をク	フリックします。		FFRI yarai Home and Business Edition
			Windows か FFRI yarai Home and Business Edition を語れ起しています。
F			必要な情報を集めています
	FFRI Security		フーザーアカウント制御の確認画面が
	FFRI varai Home and Business Editi		表示されたら、「はい」をクリックし
			ます。
			ユーザーアカウント制御 ×
	🚾 インストールガイド		このアプリがテバイスに変更を加えることを許可します か?
	2017年1月1日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日		FFRI yarai Home and Business Edition
			確認済みの発行元: FFRI.Inc. ファイルの入手先: このコンピューター上のハード ドライブ
			詳細を表示
2 2 す。	『画面で「はい」をクリックしま		はい いいえ
	Windows インストーラー ×		
	この製品をアンインストールしますか?	4	「はい」をクリックして、Windows
	[JUXY] UU12(N)	4	を再起動すると、アンインストール
L			が完了します。
			FFRI yarai Home and Business Edition $\qquad \qquad \qquad$
			FFRI yarai Home and Business Edition への設定変更を反 映えせるコゴシフテムを再起動する必要があります。今す ぐ再起動する場合は「しは、」を、後まど手動で再起動する場 合はしていえ」をクリックして代きてい。

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。

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】

チモ

- 「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。

「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

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。

) FFRI U	pdater				-		×
新しい 必要な	いフトウェアを入手できま シソフトウェアを選択してか	さす。 NG、「アップデート」	」をクリックしてください。				
ſ	arai Home and	Business Edition	情報 FFRI yarai Home and	/(– Business Editic 1.2.4	ジョン 19.0	サイズ 39.54 MB	
				Twittink		該 7	
				- F973 - F		96. T	
							_
		アッ	プデート	·情報			
FFRI U	pdater	アッ	プデート	·情報	_		>
FFRI U yarai I	pdater Home and Business E	アッ	プデート 124190.msi をダウンロート	·情報 ^{sepcs} 。	-		>
FFRI U yarai I	pdater Home and Business E	アッ idition : ffri.ps_v	プデート 12.419.0msi をダウンロート	· 情報	17.09	□ MB / 39.54	мв
FFRI U yarai l	pdater Home and Business E	アッ、 idition : ffri.ps_v	プデート 12419.0msiをダウンロート 情報	·情報 *******	- 17.09 797	ロ MB / 39.54 サイズ	мв
FFRI U yarai I Y7h	pdater Home and Business E 기가 연() yarai Home and	アッ、 idition : ffri_ps_v Business Edition	プデート 12.419.0 msi をダウンロート 12.419.0 msi をダウンロート	小青報 やです。 Business Editic 1.2.4	ー 17.09 I ジョン 19.0	mB / 39.54 サイズ 39.54 MB	мв
FFRI U yarai I У7ト	pdater Home and Business E 217 21®yarai Home and	アッ dition : ffri_ps_v Business Edition	プデート 124180.msi を対ウンロート 124180.msi を対ウンロート 124180.msi を対ウンロート	r 情報 ☆です。 Business Editic 1.2.4	ー 17.09 I ジョン 19.0	mB / 39,54 サイズ 39,54 MB	мв
FFRI U yarai I y7h	pdater Home and Business E 217 2∭yarai Home and	アツ. idition : ffri.ps_v	プデート 124190 <i>m</i> siをがソロート 体税 1 FFRI yarai Home and	· 信報 ☆中です。 Business Editic 1.2.4	ー 17.09 I ジョン 19.0	ー MB / 39.54 サイズ 39.54 MB	MB
FFRI U yarai I Y7F	pdater Home and Business E 717 717 3 (5) yarai Home and	アツ、 idition : ffri.ps.yv	プデート 124190 <i>m</i> siをがンロート 124190 <i>m</i> siをがンロート 124190 <i>m</i> siをがい ート	小吉報 やです。 Business Editic 1.2.4	ー 17.09 ジョン 19.0	ロ MB / 39.54 サイズ 39.54 MB	MB

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。
	FFRI yarai Home and Business Edition $\qquad \qquad \qquad$
	FFRI yarai Home and Business Edition への設定変更を反 映させるロネンステム改善時起動する必要があります。今す ぐ再起動する場合は1よいを、役まど手動で再起動する場 合は1、いえ」をフリックしてください。
	[]]] I. X (Y) I. N. 17. (N)

再起動メッセージ

トラブルシューティング

9.1 こんなときは

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。

「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。	「サービス」をダブルクリックし ます。
	← → + + + + 2)10-1/(15 + 525221357+)Wednet7-5 - C D
	81* Ex Ex I
2 「Windows ツール」をクリック 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。
すべてのアプリ	《 FFRI Inject Ser FFR 開始 自動 FFRI Scan Engin FFR ERE FINITION Discov 開始(S)
W	G Function Discov つ時停止(U)
Vindows Terminal	Group Folicy Clin 再開(M) 再起動(E)
Windows 簡単操作	Given and the second s
Windows セキュリティ	Q Interactive Ser プロパティ(R)
Windows ツール	G. Internet Connec G. Internet Explor ET 手動 G. IP Helper 接続 開始 自動

- 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。

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。

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。

AAM				
🖏 FFRI Inject Service	FFRI I	実行中	自動	Loca
🐘 FFRI Scan Engine Service	FFRI	88.44	(0)	
Service File History Service	ユーザ	開始	(5)	53
Sunction Discovery Provider	FDR	停止	(O)	soq
Sunction Discovery Resourc	このコ	一時	停止(U)	bca
Ceolocation Service	このサ	再開	(M)	bCa
🆏 Group Policy Client	管理	再起	動(E)	soc
🆏 HomeGroup Listener	口-力			500
🆏 HomeGroup Provider	木-ム		(のタスク(K)	soc <
🖏 Human Interface Device Ser	キーボ	最新	の情報に更新(F)	500
🥋 Hyper-V Data Exchange Ser	仮想			soc
🖏 Hyper-V Guest Service Interf	仮想	プロハ	(ティ(R)	soc
🖏 Hyper-V Guest Shutdown S	この	AILT	Ĵ(H)	500
🏟 Hyper-V Heartbeat Service	定期		7 50 (1 272 1507H)	5062
Apper-V PowerShell Direct S	仮想		手動 (トリガー開始)	Loca

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。

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。

各検出エンジンで監視するためアプリケーションの起動までに時間がかかる 可能性があります。

「3.5 設定」の検出エンジンを参照してエンジン設定を見直してください。

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。

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?

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。

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

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。

本マニュアルの著作権は株式会社FFRIセキュリティに帰属します。

本マニュアルの一部または全てを無断で転写、複製、改変することはその形態を問わず、 禁じます。

「FFRI yarai」、「FFRI yarai Home and Business Edition」は、株式会社 F F R I セキュリティの登録商標です。 その他すべての社名、製品・サービス名は、各社の商標または登録商標です。

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

(c) FFRI Security, Inc., 2015-2025 / Author: FFRI Security, Inc.