ふるまい検知オプション 日本語 OS への導入時の同居可能なウイルス対策ソフト

2024 年 2 月 7 日

同居する際には後述の【推奨設定】をご確認ください。

ベンダー	製品	注意点	ふるまい検知エージェント 3.4.x
Microsoft	Microsoft Defender (旧称 Windows Defender) (Windows 10 以降)		○
	Microsoft Defender for Endpoint (プラン 1 及びプラン 2 の両方に対応)	・FFRI yarai 2 系との同居はサポート対象外です	v3.4.6 以降のみ
	Microsoft Defender for Business		-
TrendMicro	Apex One （最新の検証済バージョンは「14.0.10101」）	・同居する際の注意点あり	○
	Apex One + Apex One Endpoint Sensor 最新の検証済バージョンは Apex One「14.0.11564」、Apex One Endpoint Sensor「3.0.1672;1.7.1078」）	・同居する際の注意点あり	○
	ウイルスバスタークラウド 17.7 （最新の検証済バージョンは「17.7.1634」	・同居する際の注意点あり	-
	Trend Micro ServerProtect 5.8 （最新の検証済バージョンは「5.8.0.1576」）	・同居する際の注意点あり	○
	ウイルスバスタービジネスセキュリティ 10.0 （最新の検証済バージョンは「10.0.2436」）	・同居する際の注意点あり	○
	ウイルスバスタービジネスセキュリティサービス 5.6	・同居する際の注意点あり	○
	ウイルスバスタービジネスセキュリティサービス 5.8	・同居する際の注意点あり	○
	ウイルスバスタービジネスセキュリティサービス 6.0 (最新の検証済バージョンは「6.0.1208」）	・同居する際の注意点あり	○
	ウイルスバスタービジネスセキュリティサービス 6.1 (最新の検証済バージョンは「6.1.1226」）	・同居する際の注意点あり	○
	ウイルスバスタービジネスセキュリティサービス 6.2 （最新の検証済バージョンは「6.2.1220」）	・同居する際の注意点あり	○
	ウイルスバスタービジネスセキュリティサービス 6.3 （最新の検証済バージョンは「6.3.1386」）	・同居する際の注意点あり	○
	ウイルスバスタービジネスセキュリティサービス 6.5 （最新の検証済バージョンは「6.5.1386」）	・同居する際の注意点あり	○

ふるまい検知オプション 同居可能なウイルス対策ソフト一覧

ベンダー	製品	注意点	ふるまい検知エージェント 3.4.x
TrendMicro	ウイルスバスタービジネスセキュリティサービス 6.6 （最新の検証済バージョンは「6.6.1386」）	・同居する際の注意点あり	◯
	ウイルスバスタービジネスセキュリティサービス 6.7 （最新の検証済バージョンは「6.7.3075」）	・同居する際の注意点あり	◯
Broadcom	Symantec Endpoint Protection 14 (最新の検証済バージョンは「14.3.9681.7000」)	・同居する際の注意点あり ・注意点あり　※注 1	◯
Trellix	Trellix Endpoint Security（McAfee Endpoint Security）10(最新の検証済バージョンは「10.7.0.5162」)	・Trellix 側のエクスプロイト防止を無効にする必要あり	◯
WithSecure	WithSecure Client Security (F-Secure Client Security) 15 (最新の検証済バージョンは「15.30.3961」)	・WithSecure 側のディープガード機能を無効にする必要あり	◯
	WithSecure Server Security (F-Secure Server Security) 15 (最新の検証済バージョンは「15.30.3894」)	・WithSecure 側のディープガード機能を無効にする必要あり	◯
ESET	ESET Endpoint アンチウイルス 8.1 (最新の検証済バージョンは「8.1.2050.1」)		-
	ESET Endpoint アンチウイルス 9.1 (最新の検証済バージョンは「9.1.2060.1」)		-
	ESET Endpoint アンチウイルス 10.0 (最新の検証済バージョンは「10.0.2034.1」)		-
	ESET NOD32 アンチウイルス 16 (最新の検証済バージョンは「16.0.24.0」)	・同居する際の注意点あり	-
	ESET Internet Security 16 (最新の検証済バージョンは「16.0.24.0」)	・同居する際の注意点あり	-
ESET	ESET Endpoint Security 8.1 (最新の検証済バージョンは「8.1.2050.1」)		-
	ESET Endpoint Security 9.1 (最新の検証済バージョンは「9.1.2060.1」)		-
	ESET Endpoint Security 10.0 (最新の検証済バージョンは「10.0.2034.1」)		-
	ESET File Security for Microsoft Windows Server 7.3 (最新の検証済バージョンは「7.3.12005.1」)		v3.4.6 以降のみ
	ESET Server Security for Microsoft Windows Server 8.0 (最新の検証済バージョンは「8.0.12013.1」)		-
	ESET Server Security for Microsoft Windows Server 9.0 (最新の検証済バージョンは「9.0.12013.1」)		-
Sophos	Sophos Central Intercept X Advanced (最新の検証済の製品バージョンは「Sophos Intercept X 2022.1.3.3」)	・同居する際の注意点あり	◯
	Sophos Central Intercept X Advanced for Server (最新の検証済の製品バージョンは「Server Intercept X 2022.1.3.3」)	・同居する際の注意点あり	◯

ふるまい検知オプション 英語 OS への導入時の同居可能なウイルス対策ソフト

ベンダー	製品	注意点	ふるまい検知エージェント 3.4.x
Microsoft	Microsoft Defender (旧称 Windows Defender) (Windows 8.1 以降)		◯
	Microsoft Defender for Endpoint (プラン 1 及びプラン 2 の両方に対応)	・FFRI yarai 2 系との同居はサポート対象外です	v3.4.6 以降のみ
	Microsoft Defender for Business		-
Broadcom	Symantec Endpoint Protection 14 (最新の検証済バージョンは「14.3.9681.7000」)	・同居する際の注意点あり ・注意点あり ※注 1	◯
Trellix	Trellix Endpoint Security（McAfee Endpoint Security）10 (最新の検証済バージョンは「10.7.0.5162」)	・Trellix 側のエクスプロイト防止を無効にする必要あり	◯
WithSecure	WithSecure Server Security (F-Secure Server Security) 15 (最新の検証済バージョンは「15.30.3961」)	・WithSecure 側のディープガード機能を無効にする必要あり	◯
Sophos	Sophos Central Intercept X Advanced (最新の検証済の製品バージョンは「Sophos Intercept X 2022.1.3.3」)	・FFRI yarai 2 系との同居はサポート対象外です ・同居する際の注意点あり	◯
	Sophos Central Intercept X Advanced for Server (最新の検証済の製品バージョンは「Server Intercept X 2022.1.3.3」)	・同居する際の注意点あり	◯

※注 1：Symantec Endpoint Protection Small Business Edition はサポート対象外となります。

ふるまい検知エージェント 日本語 OS / ふるまい検知エージェント 英語 OS への導入時の同居可能な上記の製品は、各ベンダーの製品サポート期間終了時にふるまい検知エージェントのサポート対象外となります。

ふるまい検知エージェント日本語 OS / ふるまい検知エージェント英語 OS への導入時の同居可能な上記の製品として記載のないエンドポイント型のウイルス対策ソフトと同居した環境については、 ふるまい検知エージェントのサポート対象外となります。

ふるまい検知オプション 同居可能なウイルス対策ソフト一覧

【同居可能なウイルス対策ソフトのクラウド（SaaS）版や英語版のサポートに関して】
弊社側で同居検証済みのウイルス対策ソフトと、同一製品・同一機能・同一バージョンであれば、提供形態自体がクラウド（SaaS）版や英語版の場合であっても、サポート対象外とはしておりません。
なお、弊社ふるまい検知エージェントと同居可能なクライアント側のウイルス対策ソフトについては、システム要件に別途環境や言語の記載が無い限り、日本語版ふるまい検知エージェントはオンプレミス版(クラウド版のみの提供のものを除く)/日本語版の他社製ウイルス対策ソフトで、英語版ふるまい検知エージェントはオンプレミス版(クラウド版のみの提供のものを除く)/英語版のウイルス対策ソフトで同居検証しております。

【推奨設定】
ウイルス対策ソフトと同居させる場合、ふるまい検知エージェントの継続的な安定動作（ウイルス対策ソフト側の定義ファイルの更新等に伴う、検出機能の干渉や動作の競合が発生する可能性を防止）のために、ウイルス対策ソフト側でふるまい検知エージェントを監視対象外として設定することをお願いします。

yarai のデフォルトのインストールフォルダー
- 64 ビット版 OS の場合「C:¥Program Files (x86)¥FFR¥yarai」
- 32 ビット版 OS の場合「C:¥Program Files¥FFR¥yarai」

なお、yarai 3.x をご利用で管理されたクライアントとしてインストールしている場合は以下のフォルダも追加してください。
- 64 ビット版 OS の場合「C:¥Program Files (x86)¥FFRI」
- 32 ビット版 OS の場合「C:¥Program Files¥FFRI」

上記に加え、以下のフォルダとファイルをすべて追加してください。
- 「C:¥ProgramData¥FFR¥yarai」
- 「C:¥Windows¥System32¥drivers¥」内の以下の名称ではじまるファイル
  - FFRFileScan
  - FFRFileTracer
  - FFRFramework
  - FFRINetIsolator
  - FFRRegistry
  - FFRZDPInjector

※ウイルス対策ソフトでふるまい検知エージェント関連のモジュールが処理されてしまった場合、ウイルス対策ソフト側で復元を行ってください。

ふるまい検知エージェントが正常に動作しない場合は、ふるまい検知エージェントの再インストールをお願いします。

【 ふるまい検知オプション 日本語 OS、英語 OS への導入時の同居可能なウイルス対策ソフトの注意点】

- 上記の製品は、各メーカーの製品サポート期間終了時に ふるまい検知エージェント のサポート対象外となります。

【Microsoft】

- Windows Defender との連携機能における制限事項
  - Windows 8.1、Windows 10、Windows Server 2016 以降が対象となります。
  - 他社製品のアンチウイルスソフトとの併用時には動作保証しておりません。
  - Windows Defender 側の問題についてはサポート対象外となります。以下、サポート対象外となる例を示します。
    - Windows Defender による検出に対するお問い合わせ
    - Windows Defender のエラー、不具合についてのお問い合わせ
      - Windows Defender が検出しない
      - Windows Defender で検出したにも関わらずふるまい検知エージェントのログに表示されない
      - Windows Defender の定義ファイル更新に失敗
      - Windows Defender のスキャンに失敗
      - その他 Windows Defender に起因する問題
  - 管理コンソールから Windows Defender のリアルタイム保護を無効にするポリシーを配信しても、PC を再起動すると Windows の仕様によりリアルタイム保護が有効になります。
  - Windows Defender で検出した場合、マルウェア一覧には表示されません。また、検体収集機能を有効にしていても検体は収集されません。
- Windows 10 Fall Creators Update、Windows 11 以降の OS 環境下で、ふるまい検知エージェントと Windows Defender を同居し「コントロールされたフォルダーアクセス」機能を有効にして利用する場合、Windows Defender の設定を変更する必要があります。
  設定変更を行わないで本製品を利用する場合、Internet Explorer の脆弱性攻撃を検知しても、検知メッセージがふるまい検知エージェントに通知されません。（Windows Defender と ふるまい検知エージェント の検知機能自体は問題なく動作します）Windows Defender 側で下記設定変更が必要です。
  - Windows Defender セキュリティセンター ＞ ウイルスと脅威の防止 ＞ ウイルスと脅威の防止の設定 ＞ コントロールされたフォルダーアクセス ＞ アプリをコントロールされたフォルダーアクセスで許可する ＞ [+]許可されたアプリを追加する ＞ScanEngine.exe を選択（Windows 10 April Update 適用前の場合）
  - Windows Defender セキュリティセンター ＞ ウイルスと脅威の防止 ＞ ランサムウェアの防止 ＞ コントロールされたフォルダーアクセス ＞ アプリをコントロールされたフォルダーアクセスで許可する ＞ [+]許可されたアプリを追加する ＞ScanEngine.exe を選択（Windows 10 April Update 以降の場合）

    ScanEngine.exe は、ふるまい検知エージェントのインストールディレクトリ内に存在します。初期設定のイ

ンストールディレクトリは 32 ビット OS では「C:￥Program Files￥FFRI￥yarai」、64 ビット OS では「C:￥Program Files(x86)￥FFRI￥yarai」です。

- Windows 10 November 2019 Update 以降の OS 環境下で、Windows Defender を ふるまい検知 GUI から無効化する、もしくは管理コンソールから無効化するポリシーを配信する場合、Windows Defender 側で下記設定変更が必要です。
  - Windows セキュリティ＞ウイルスと脅威の防止＞ウイルスと脅威の防止の設定＞改ざん防止 をオフ

【Trend Micro】

- トレンドマイクロ製品と同居する場合、ふるまい検知エージェントのモジュールである MHHub.dll をトレンドマイクロ製品の除外設定に指定する必要があります。
  MHHub.dll の初期設定のインストールディレクトリは 32 ビット OS では「C:¥Program Files¥FFR¥yarai」、64 ビット OS では「C:¥Program Files (x86)¥FFR¥yarai」です。
- ウイルスバスターXG と ふるまい検知エージェント の同居環境で ふるまい検知エージェントをアンインストールすると一部フォルダが残存する場合があります。この事象は、AMC 配下の管理されたクライアントのみで発生します。ウイルスバスターXG 側の信頼済みプログラムに、ffriamcc.exe と ffriamcun.exe を追加することで事象の回避が可能です。
  ffriamcc.exe と ffriamcun.exe の初期設定のインストールディレクトリは 32 ビット OS では「C:¥Program Files¥FFRI¥AMC¥Client」、64 ビット OS では「C:¥Program Files (x86)¥FFRI¥AMC¥Client」です。
- ウイルスバスタービジネスセキュリティサービスにおいて、同製品の仕様により当社で同居検証が行われていないバージョンへ自動的にアップデートされる場合があり、それによって同居に関する問題が発生した際には当社から回避策や修正モジュールの提供に時間が掛かる可能性がありますのでご了承ください。
- トレンドマイクロ製品と同居する場合、ご利用の環境によっては ふるまい検知エージェントのハンティング機能と競合し、パフォーマンスが低下する場合があります。ふるまい検知エージェントのハンティング機能をご利用の場合は、トレンドマイクロ製品の下記インストールフォルダーをハッシュ計算例外リストへご登録いただくことを推奨します。
  - C:¥Program Files (x86)¥Trend Micro

【Broadcom】

- Symantec Endpoint Protection 12.x と共存させた際、Symantec 側の改変対策機能のメッセージ表示を有効にしますと、改変対策機能がふるまい検知エージェントを検出しポップアップを表示することがあります。この現象を回避するためには、ふるまい検知エージェントの例外リストに Symantec Endpoint Protection 12 のフォルダを追加し、詳細設定のオプション 2 つを有効にする必要があります。
- Symantec Endpoint Protection 12.1.671.4971 と共存させた場合、ZDP エンジンの一部防御機能が動作しない事が判っています。この問題を回避するには、Symantec Endpoint Protection 12.1.1000.157 RU1 以降にアップデートして頂くか、v2.4 以降にアップデートして頂く必要があります。
- 64 ビット環境において、Symantec Endpoint Protection 12.1.1000 以降と共存させた際、ZDP エンジンの防御機能が動作しない事が判っています。この問題を回避するには、v2.2 以降にアップデートして頂く必要があります。

- Windows Vista 以降の環境において、Symantec Endpoint Protection 12 と同居している環境の場合、ふるまい検知エージェントのメール送信機能が動作しない可能性があります。動作させるためには、Symantec 側に以下の設定が必要です。
  - ウイルスとスパイウェア対策の設定
    - インターネット電子メール Auto-Protect のタブにて「インターネット電子メール Auto-Protect を有効にする」のチェックボックスを外す。
- Symantec Endpoint Protection 14 以降アンチウイルス製品側で下記設定変更が必要です。※各言語版にて共通
  - Symantec Endpoint Protection 14 側の設定で「汎用悪用機能/メモリエクスプロイト緩和機能」を無効にする必要があります
  - Symantec Endpoint Protection 14 の GUI を起動後、[状態] 画面にて [ネットワークとホスト悪用防止] の横にある [オプション] を押下し、「汎用悪用機能を無効にする/メモリエクスプロイト緩和機能を無効にする」を選択する。
- Symantec Endpoint Protection 14 以降 と ふるまい検知エージェント 3.x.x を同居している環境で AMC からクライアントのアップデート配布命令を実行した場合、ふるまい検知エージェントのアップデート自体は正常に完了しますが、完了通知が送信されず、AMC のクライアント管理画面のアップデート配布状況が「配布中」のままになる事象が確認されています。
  完了通知を送信するためには、Symantec 側で下記設定変更が必要です。
  - 「ネットワークとホストのエクスプロイト緩和機能」-「ネットワークアプリケーション監視を有効にする」を OFF にして、AMC からアップデートを配布する

【McAfee】

- McAfee Virus Scan Enterprise と併用する場合、McAfee 側の以下の機能を無効にして下さい。
  - バッファオーバーフロー保護
  - Anti-Virus 最大プロテクト（ウイルス対策最大保護）
    - McAfee のバージョンによって呼称が異なります。
    - [ブロック]と[レポート]の両方のチェックを外し無効化する必要があります。
  - 一般最大プロテクト
    - [ブロック]と[レポート]の両方のチェックを外し無効化する必要があります。
- McAfee Virus Scan Enterprise 8.8 Patch 4 以降、64bit OS と Windows 8 以降の 32bit OS にてバッファオーバーフロー保護の設定が存在しない環境があることを確認いたしました。
  設定がない環境につきましては、設定をせずともサポートさせていただきます。
  - 設定がある場合はバッファオーバーフロー保護を無効にしていただく必要がございます。
  - 設定がない環境につきましては、デフォルトでバッファオーバーフロー保護が無効となっており、有効に変更できないことを確認しております。
- McAfee VirusScan Enterprise(8.8) と同居している環境の場合、ふるまい検知エージェントのメール送信機能が動作しない可能性があります。動作させるためには、McAfee 側に以下のいずれかの設定が必要です。
  - 「アクセス保護」を無効にする

- 「アクセス保護」の中の「大量メール配信型ワームにメールを送信させない」のチェックを外す
  - [ブロック]と[レポート]の両方のチェックがありますが、[ブロック]のみチェックを外し無効化する必要があります。
- 「大量メール配信型ワームにメールを送信させない」の中の除外するプロセスに「cscript.exe」を追加する

- McAfee Endpoint Security 10 以降アンチウイルス製品側で下記設定変更が必要です。McAfee Endpoint Security 10 の GUI を起動し、[設定] - [脅威対策] -[エクスプロイト防止]にて「エクスプロイト防止を有効にする」のチェックを外し、右上の適用から設定を適用する。
- McAfee Virus Scan Enterprise のインストール時に「標準の保護」を選択する必要があります。

【ESET】

- ESET NOD32 アンチウイルス、ESET Internet Security と ふるまい検知エージェントの同居環境でネットワークフォルダにアクセスするとアクセスできなくなる場合や、BSOD になる場合があります。事象を解消するには ESET 側で以下の設定が必要です。
  - ［設定］→［詳細設定］をクリックして、設定ウインドウを開く
    - ［検出エンジン］→［リアルタイムファイルシステム保護］→［基本］を展開し、［検査するメディア］の［ネットワークドライブ］を［×］印（無効）に変更して［OK］ボタンを押下する

【F-Secure】

- F-Secure Client Security 13 以降 または、F-Secure Server Security 12 とふるまい検知エージェントの同居時にディープガードを無効にする必要があります。
  - F-Secure Client Security の GUI を起動し、[設定] - [コンピュータ] - [ウイルスとスパイウェアスキャン]にて[ディープガードを有効にする] のチェックを外し、右下の[OK]から設定を適用する。
  - F-Secure Server Security の Web コンソールにログイン後、ホーム画面の左ペインから[サーバ保護] - [リアルタイムスキャン] - [ディープガード]にて[ディープガード]を OFF にし、下部の[保存して適用]から設定を適用する。
- WithSecure Server Security(F-Secure Server Security) 15 以降とふるまい検知エージェントの同居時にディープガードを無効にする必要があります。
  - WithSecure Server Security の GUI を起動し、[設定] - [マルウェア保護] にてディープガードの [有効] のチェックを外す。

【Sophos】

- Sophos Central Intercept X Advanced または、 Sophos Central Intercept X Advanced for Server とふるまい検知エージェントの同居時に、 Sophos 側の「脆弱なアプリケーションにおけるエクスプロイトを防止する」機能を無効化する必要があります。
  1. Sophos Central にサインインする
  2. 使用している製品を選択する
  3. 「ポリシー」を押下する
  4. 「ポリシーの追加」を押下する
  5. ドロップダウンリストから「脅威対策」を選択する
  6. ポリシー配布の種類として「ユーザー」または「デバイス」を選択する(サーバープロテクションの場合はこの手順は存在しません)
  7. ユーザーの場合は配布予定のユーザーを選択して「＞」を押下して、割り当て済みサーバーに追加する(サーバープロテクションの場合はユーザーではなくデバイスを選択してください)
  8. 設定タブに遷移する
  9. ポリシー名を入力して「推奨設定を使用する」のチェックを外す(サーバープロテクションの場合はこの手順は存在しません)
  10. 「脆弱なアプリケーションにおけるエクスプロイトを防止する」を無効化する
  11. 「保存」を押下する
  12. 配布先の環境を再起動してポリシーを反映させる