EX AntiMalware v7

クライアントプログラム・ユーザーマニュアル

Revision 2019/2

株式会社フーバーブレイン

Fuva Brain

目次

1. 本製品の特徴

EX AntiMalware v7 は、PC に侵入した各種マルウェア（スパイウェア、ウイルスなど不正プログラム、悪性コードの総称）やグレーツールを検知し隔離/駆除することで、ハッキング、情報漏えい、プライバシーの侵害や悪質なインターネット広告（強制的なブラウザのスタートページ固定やポップアップなど）、ユーザーのリモート制御、ネットワークの機能低下、ウイルスによるシステム破壊などから PC を保護します。

広範囲なマルウェア・グレーツールに対する PC 保護

日本およびアジア圏におけるマルウェア・グレーツールの情報収集/分析に加えて、海外の優れたマルウェア対策ベンダー企業と提携してスパイウェア、悪性アドウェア、ハッキングツール、トロイの木馬、ウイルス、ワーム、ファイル交換ソフト(P2P)など、広範囲なマルウェア・グレーツールを検知します。また、他のアンチウイルス製品など既存セキュリティソフトと共存させることも出来ますので、既存セキュリティソフトでは検知が難しいマルウェア・グレーツールを含む包括的なセキュリティ対策を実現します。

最適化されたスキャンエンジン

誤検知率を最小限に抑え、実行型のファイルだけでなくマルウェア・グレーツールを構成する関連悪性コードまで隔離/駆除します。また、マルウェア・グレーツールが変更したシステム環境なども修復することができます。

リアルタイム監視機能

マルウェア・グレーツールの活動を常時監視し、検知した場合、その活動を中断させ隔離/駆除します。

隔離と除外

マルウェア・グレーツールの活動を遮断し、隔離します。隔離することにより、PC や他のプログラムに影響がある場合は、復旧機能を使って隔離した対象ファイルを復旧させることもできます。また特定のマルウェア・グレーツールを除外（検知対象外）にするための設定機能もあります。

アップデートおよびスキャン

自動/手動/スケジュール化によるマルウェア・グレーツールデータベースやプログラムのアップデート機能、および PC のスキャン機能があります。

利便性

シンプルなユーザーインターフェースにより、どなたにも簡単にご利用いただけます。

1.1. EX AntiMalware v7 Manager による集中管理

専用クライアント管理ツール EX AntiMalware v7 Manager「以下 Manager」から、複数のクライアントに対し利用状況の確認、機能設定、検知したマルウェア・グレーツールの処理、ログの収集・閲覧などの一元管理が可能です。

2. 動作環境

本製品 は、下記オペレーティングシステムをサポートしています。

OS	下記 OS の 32 ビット、64 ビット(x64)をサポートします。 Windows 10, 8.1, 8, 7 Windows Server 2016 / 2012R2 / 2012 / 2008R2 Windows Storage Server 2016 / 2012R2 / 2012 / 2008R2
CPU	クロック周波数 1.5GHz 以上 (推奨 2GHz 以上)
メモリ	2GB 以上 (推奨 4GB 以上) ※リアルタイム監視設定「**標準**」を選択するには、メモリ 4GB 以上を推奨します。4GB 未満の PC は「**軽快モード**」をご使用ください。
HDD 空き容量	インストール時に 1GB 以上

動作環境に関するご注意

1. Windows のサービスパックは、最新の状態でご使用ください。
2. 動作に必要なメモリ空き容量、ディスク空き容量を満たしている場合でも、システム環境によってはパフォーマンスが十分に発揮されない場合があります。
3. プログラムの仕様は、予告なしに変更される場合があります。

2.1. Microsoft .NET Framework

本製品は、Microsoft .NET Framework 4.5.2 以上が必要です。
Microsoft .NET Framework 4.5.2 は、Windows Update により、自動的に導入されるため、通常、手動インストールは必要ありません。

3. インストール

1. インストールは、Windows の管理者権限が必要です。インストール後は制限ユーザーでも使用できます。
   Internet Explorer 11 以降 または Microsoft Edge を起動して、下記 Manager のダウンロードページへ接続し、セットアッププログラムをダウンロードします。

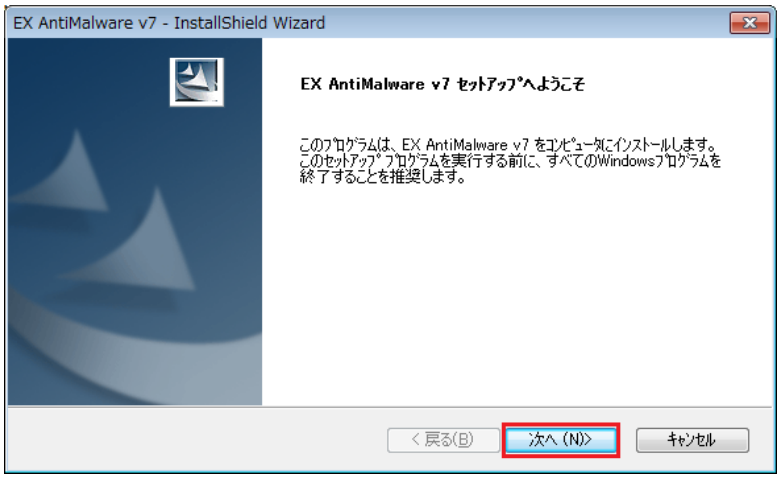
https://exam7.ahkun.jp/akam7/download/

アカウント ID の入力画面が表示されますので、ご契約時にフーバーブレインまたは弊社代理店から提供されたアカウント ID を入力して「**継続**」をクリックします。

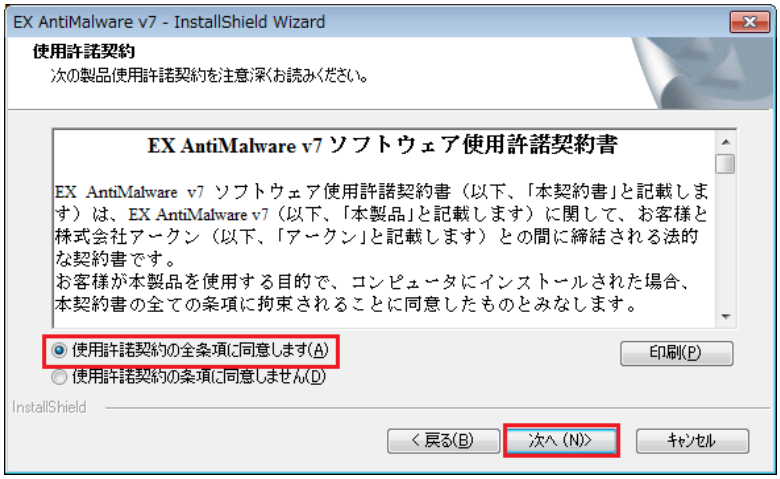
「**アカウント ID が正しくありません**」等のエラーが表示された場合、アカウント ID が正しく入力されているか、ご確認ください。
下記ダウンロードページからセットアッププログラムをダウンロードします。Windows 32 ビット用と 64 ビット用がございますので、インストールする OS に応じたプログラムをダウンロードして実行します。

上記ページから「**Microsoft .NET Framework 4.5.2**」がダウンロードできます。

2. セットアッププログラムを実行すると、ウィザード画面が表示されます。「**次へ(N)**」をクリックします。

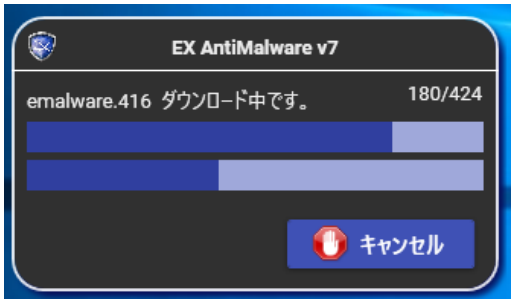


3. 使用許諾書が表示されます。内容を確認のうえ「**同意する(A)**」をチェックし「**次へ(N)**」をクリックします。



表示内容をご確認頂き、セットアップを完了させてください。

4. セットアップが完了すると最新プログラムのダウンロードを開始します。



Microsoft .NET Framework が導入されていないメッセージが表示されるときは・・

Microsoft .NET Framework 4.5.2 以上を適用ください。

最新プログラムのダウンロードが完了したら「**EX AntiMalware v7 設定情報やステータスの確認**」をご覧ください。

4. DVD-ROM からのインストール

DVD-ROM からインストールするには、DVD-ROM に格納された Windows 32 ビット用と 64 ビット用のインストーラを実行し、インストールを完了させてください。

インストールは、Windows の管理者権限が必要です。インストール後は制限ユーザーでも使用できます。

ExAntimalware_x86.exe	32 ビット Windows 用インストーラ
EXAntimalware_x64.exe	64 ビット Windows 用インストーラ

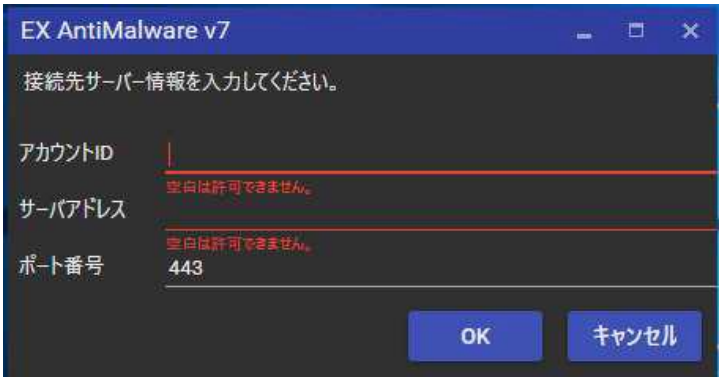
5. アカウント ID, サーバーアドレスの入力画面が表示されるときは

EX AntiMalware v7 インストール後、アカウント ID や接続サーバー設定が必要な場合、下記画面を表示します。正しい値を入力してください。

アカウント ID： 弊社、または弊社代理店から提供されたアカウント ID

サーバーアドレス： exam7.ahkun.jp

ポート番号： 443

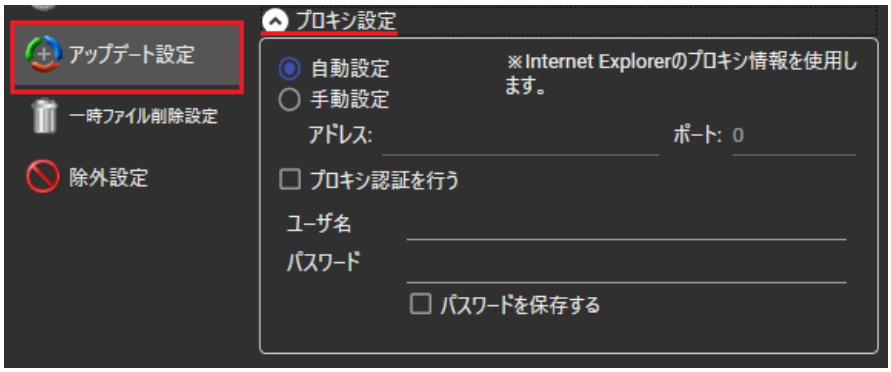


6. 認証プロキシ経由でインターネットに接続している場合

認証プロキシ経由でインターネットに接続している場合、EX AntiMalware v7 がインターネットに接続するため、プロキシ認証情報の入力画面を表示します。正しい値を入力し OK をクリックします。

パスワードを保存するには、**「パスワードを保存する」**をチェックします。

EX AntiMalware v7 メイン画面から、プロキシ情報を設定するには、「環境設定」「アップデート設定」の「プロキシ設定」から行います。

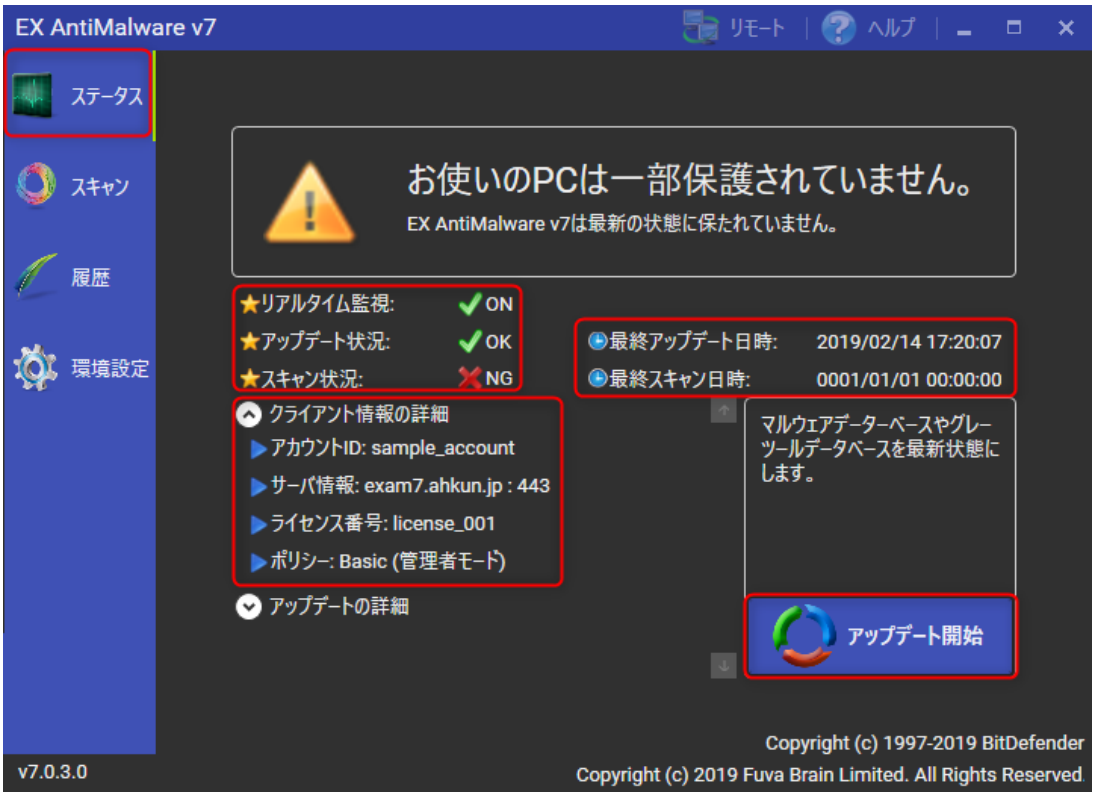


7. EX AntiMalware v7 設定情報やステータスの確認

EX AntiMalware v7 をインストールすると、デスクトップに青い盾のアイコンが作成されます。

同様に Windows タスクトレイ及びスタートメニューにアイコンやメニューを追加します。

アイコンを**ダブルクリック**すると、メイン画面を表示します。



「クライアント情報の詳細」から、アカウント ID、サーバー情報、ライセンス番号、ポリシーが確認できます。

インストール直後は、一度もスキャンをおこなっていないため「スキャン状況」は NG になります。

画面左に表示された「スキャン」から、クイックスキャンを実行すると「スキャン状況」は OK になります。

スキャンを途中でキャンセルした、または Windows シャットダウンなどで、スキャンが最後まで実行できなかった場合、最終スキャン日時は 0001/01/01 00:00:00 になります。

クイックスキャン、またはフルスキャンのどちらかが完了している場合、その日時を表示します。

8. インストールの確認

メイン画面**「ステータス」**右下の**「アップデート開始」**を実行しエラー等発生せず完了するかご確認ください。

また**「スキャン」「クイックスキャン」**を実行し処理が完了するかご確認ください。

9. アンインストール

お使いのシステムから本製品をアンインストールするには、**コントロールパネル** -> **プログラムと機能** から「**EX AntiMalware**」を選択してアンインストールします。

重要

本製品のアンインストールは、システム管理者の許可を得ておこなってください。

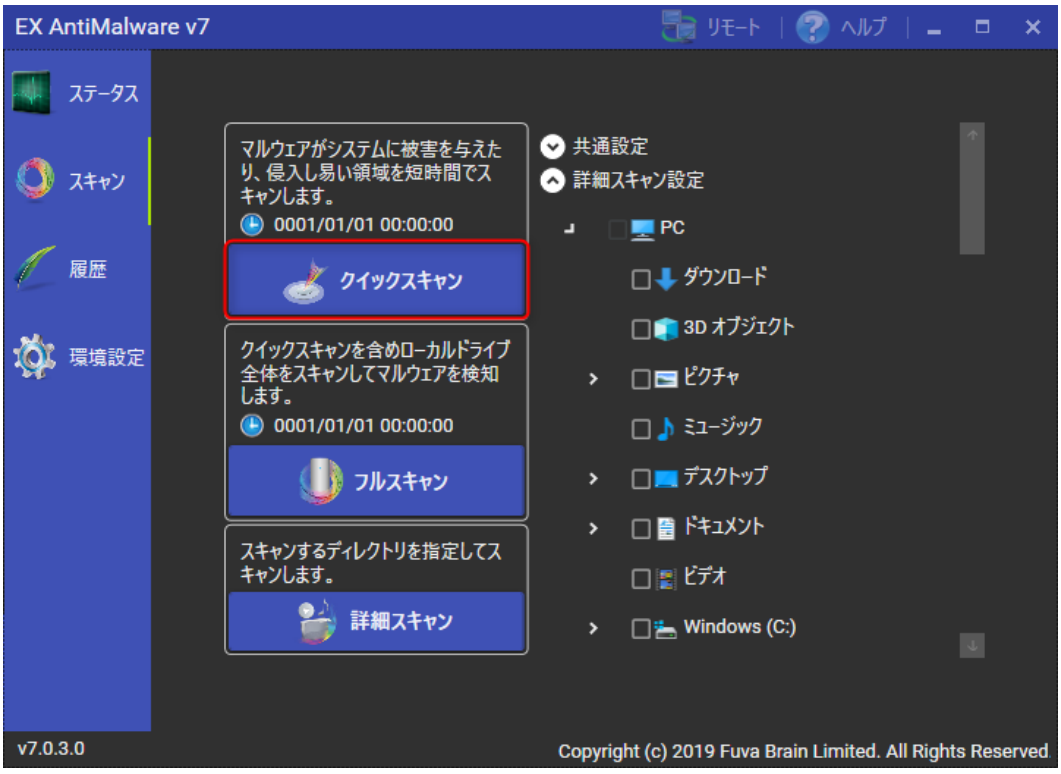
また EX AntiMalware v7 管理者設定によりアンインストールがパスワード保護されている場合があります。

10. マルウェア・グレーツールをスキャンする

スキャンは Manager で設定したポリシーにより、自動で行われます。
クイックスキャンは、毎日、昼 12 時に実行され、フルスキャンは、毎月 8 日の昼 12 時に実行します。
スキャンのスケジュールは、Manager のポリシーにより変更可能です。
スケジュールスキャン時、PC 電源 OFF などにより、スキャンが実行できなかった場合、PC 起動後に実行します。マルウェアのスキャンは、ユーザーの操作により、いつでも実行できます。

10.1. クイックスキャン

クイックスキャンは、PC に最も被害を与える可能性のある領域に対してのみマルウェア/グレーツール/圧縮ファイルが存在しないかスキャンし確認します。そのため、フルスキャンと比べスキャン時間が短縮します。
クイックスキャンを実行するには、EX AntiMalware v7 を起動して「スキャン」から「クイックスキャン」をクリックします。



「クイックスキャン」ボタンの上に表示された日時は、最終スキャン日時です。0001/01/01 00:00:00 の場合、直前のクイックスキャンがユーザーによるキャンセル等で、完了しなかったことを表しています。

スキャン状況の表示

スキャンを開始すると、スキャン時間や、スキャン済ファイル数などの情報を表示します。

スキャンを中止したい場合は、「キャンセル」または「一時停止」をクリックします。「キャンセル」はすべてのスキャンが中止されます。「一時停止」ボタンはスキャンを一時停止します。そのためスキャンを中断した時点からのスキャン再開が可能です。

スキャン結果を参照するには「スキャン結果」をクリックします。

10.2. フルスキャン

C ドライブ等の PC 内蔵 HDD や SSD をスキャンします。ネットワークドライブや、USB メモリ等の取り外し可能なデバイスはスキャン対象外です。ネットワークドライブや、USB メモリ等をスキャンするには、「詳細スキャン」を実行してください。

スキャンを中止したい場合は、「キャンセル」または「一時停止」をクリックします。

スキャン結果を参照するには「スキャン結果」をクリックします。

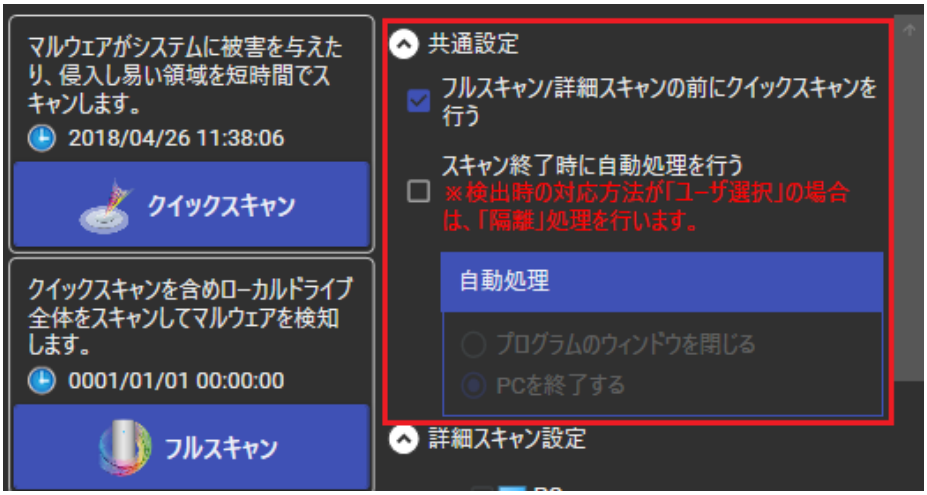
フルスキャンは、**「共通設定」**から以下のオプションが選択できます。

□フルスキャン/詳細スキャンの前にクイックスキャンを行う

選択すると、フルスキャン/詳細スキャンの前にクイックスキャンを行います。

□スキャン終了時に自動処理を行う

選択すると、スキャンが完了した後、プログラムウインドウを閉じたり、Windows シャットダウンを行います。



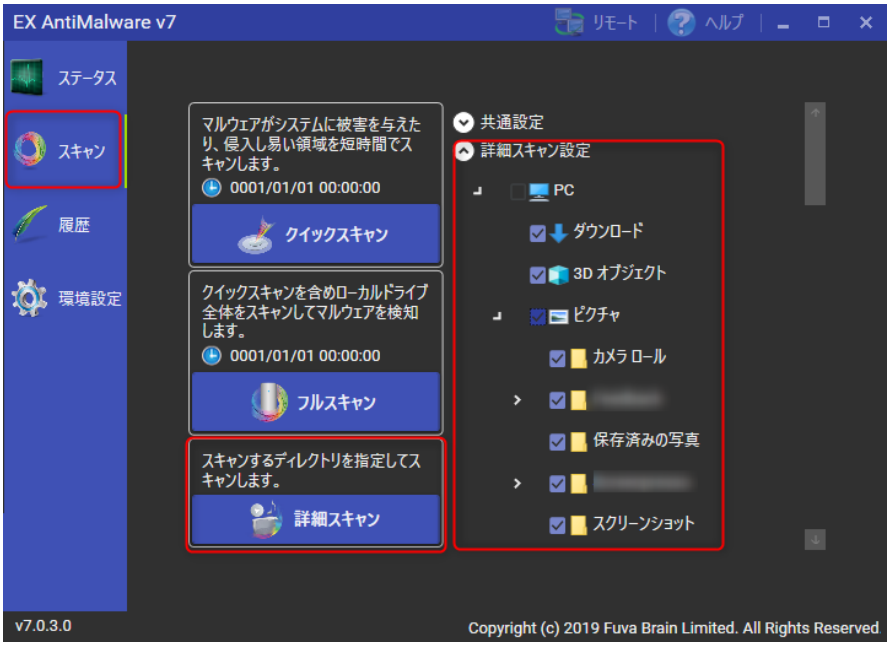
「フルスキャン」ボタンの上に表示された日時は、最終スキャン日時です。0001/01/01 00:00:00 の場合、直前のフルスキャンがユーザーによるキャンセル等で、完了しなかったことを表しています。

10.3. 詳細スキャン

指定した領域に対してマルウェア・グレーツールが存在しないかスキャンし確認します。

詳細スキャンは、ユーザーの任意でファイルやフォルダ、ドライブなどを選択してスキャンすることができます。

詳細スキャンを実行するには、「詳細スキャン設定」からフォルダを指定し「詳細スキャン」をクリックします。



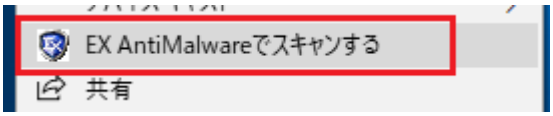
スキャンを中止したい場合は、「キャンセル」または「一時停止」をクリックします。

スキャン結果を参照するには「スキャン結果」をクリックします。

10.4. 右クリックスキャン

右クリックスキャンは、特定のファイルやフォルダに対してマルウェア・グレーツールが存在しないかスキャンします。

右クリックスキャンの実行は、スキャンしたいファイルやフォルダを右クリックしてメニューを表示し「EX AntiMalware でスキャンする」を選択します。

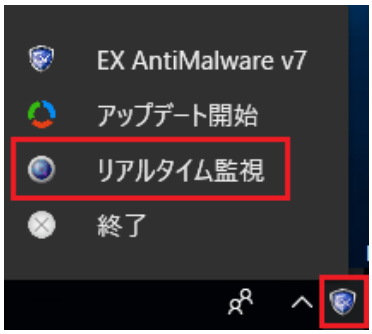


※この機能は、EX AntiMalware v7 の**「環境設定」「スキャン設定」「スキャンオプション」「右クリックメニューにスキャン項目を表示する」**が有効な場合のみ、ご利用いただけます。

10.5. **リアルタイム監視**

マルウェア・グレーツールの活動を常時監視して、PC でマルウェア・グレーツールが実行（侵入）またはコピーされた場合、リアルタイムで検知します。リアルタイム監視機能が有効になっているかを確認するには、タスクトレイの青い盾の EX アイコンを**右クリック**してメニューを表示します。メニューの「リアルタイム監視」アイコンが青く点灯している場合、リアルタイム監視機能は有効です。

※この機能は、**「環境設定」「リアルタイム監視設定」「リアルタイム監視を行う」**が有効な場合、利用いただけます。



10.6. **リアルタイム監視モード「標準」と「軽快」**

リアルタイム監視では「標準（推奨）」と「軽快」の 2 つの監視モードがあります。
デフォルトでは「標準（推奨）」モードが設定されています。

標準(推奨)

フィルタドライバを使用して、監視強度の高いクライアントのリアルタイム監視を実施します。

軽快

ウイルス対策製品の多くは、Windows フィルタドライバという形式で開発されています。複数のウイルス対策のフィルタドライバを重複して導入するとシステムパフォーマンス低下など問題を起こす場合があります。
軽快モードはフィルタドライバを使用せずに、アプリケーションレベルでクライアントのリアルタイム監視を実施します。監視対象は実行中のプロセスと、ファイル作成時に限定されるため、他のドライバとのコンフリクトを回避することができます。また搭載メモリが少ない PC は、軽快モードをご使用ください。

他社のセキュリティ製品または他のアプリケーションとの競合により PC が極端に遅くなった場合、「軽快」に変更することで改善する可能性があります。

10.7. **未知のランサムウェア検知機能**

未知ランサムウェア検知にチェックを入れると、未知のランサムウェア （新型身代金ウイルス） が、データを不正に暗号化したり、変更したりする挙動を検知し、ブロックします。
また、ランサムウェアによる復元ポイントの削除もブロックし、復元ポイントを保護します。
未知ランサムウェア検知機能は、「標準モード」の場合に限り有効にできます。

不正に暗号化する挙動を検知すると、ユーザーに注意を促す警告画面を表示します。未知ランサムウェアを実行した可能性があるため、警告画面をご参照頂きサポートまでご連絡ください。
サポートの調査により、安全が確認できた挙動は、「除外設定」で、今後検知しないよう設定できます。

10.8. **リアルタイム監視を一時的に停止する**

EX AntiMalware v7 導入後、Windows が重くなるなど、システム操作性が低下した場合、原因調査のため、一度、リアルタイム監視を停止し、改善するかご確認ください。
リアルタイム監視の停止は、タスクトレイの青い盾の EX アイコンを**右クリック**してメニューを表示し、メニューの「リアルタイム監視」を選択して、OFF にします。

リアルタイム監視を OFF にすると、マルウェア感染リスクが高くなります。リアルタイム監視は、調査が終わりましたら、元の状態(ON)に戻してください。
※Manager からポリシーを受信すると自動的に Manager の設定(通常リアルタイム監視 ON)になります。

11. マルウェア・グレーツールの検知

マルウェアやグレーツールを検知すると、下記の検知画面を表示します。

※Manager のポリシーで「GUI 非表示」になっている場合は、表示しません。

検知画面が表示された場合、処理方法を選択してください。

隔離

マルウェア・グレーツールを安全な領域に隔離します。対象ファイルを隔離することにより、PC や他のプログラムの動作に影響がある場合は、復旧機能を使って対象ファイルを元の場所に復旧することができます。

除外

検知したマルウェア・グレーツールの対象ファイルを次回からスキャンの対象外として設定します。

除外は、安全なファイルに限り、選択してください。

ログのみ

検知したマルウェア・グレーツールの対象ファイルの情報をログとして記録します。

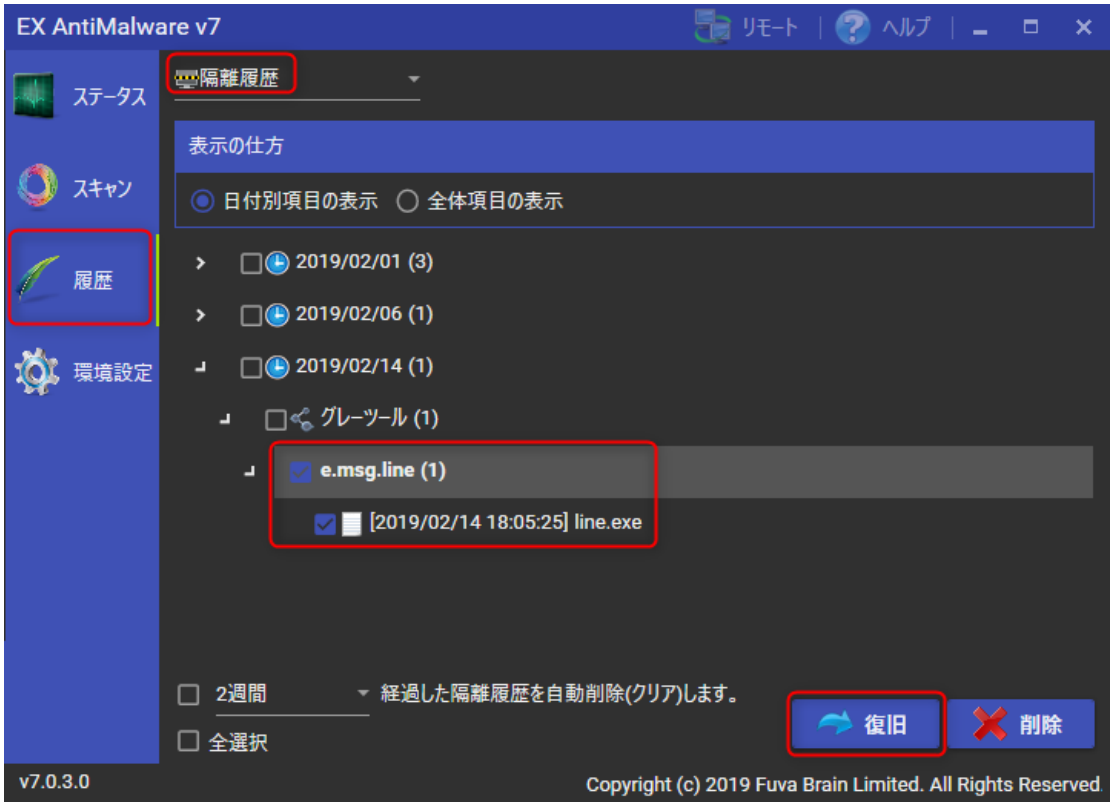
隔離や、除外はしません。ログのみは、安全なファイルに限り、選択してください。

閉じる

隔離や、除外はしません。閉じるは、安全なファイルに限り、選択してください。

11.1. 隔離ファイルの復旧

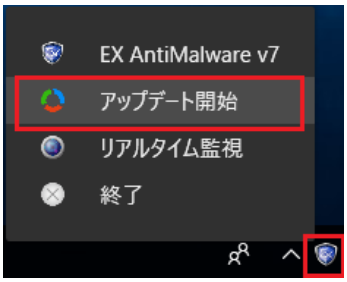
隔離したファイルを元に戻すには、EX AntiMalware v7 メイン画面の「履歴」をクリックし、
「隔離履歴」を選択します。一覧から復旧するファイルを探しチェックを入れ「復旧」をクリックします。



「日付別項目の表示」、または「全体項目の表示」を切り替えると、目的のファイルが見つけやすくなります。
「削除」を選択すると選択した隔離ファイルを削除します。
古い隔離ファイルを一定期間(初期値 2 週間)経過後に、自動削除(クリア)することもできます。
隔離ファイルの自動削除設定は Manager から受信するため、Manager のポリシーを変更してください。

12. データベースの手動アップデート

タスクトレイの青い盾の EX アイコンを右クリックし、「アップデート開始」を実行するとマルウェア/グレーツール・データベース、ポリシー、EX AntiMalware v7 プログラムファイルなどをアップデートします。



アップデートは、バックグラウンドで自動実行されますので、手動でおこなう必要はありませんが、Manager と正常に通信できているか確認することができます。

13. 遠隔サポート(リモート)

サポートでは、正確に問題を解析し早期に解決するため、お客様の PC への遠隔サポートをお願いする場合がございます。メイン画面「リモート」から、簡単に遠隔サポートがご使用できます。
遠隔サポートは、インターネット接続が必要です。

「リモート」をクリックするとブラウザを起動し、弊社遠隔サポート用ツールのダウンロードサイトに接続しますので、「遠隔サポートサービス規定」をご確認の上、遠隔ソフトを実行します。

ご注意事項

サポートは、EX AntiMalware v7 のライセンスおよびソフトウェアサポートをご契約された販売会社様まで、お問い合わせくださいますようお願い致します。
また、弊社では基本的にご購入前のお客様の技術サポートは、お受けしておりません。
製品評価時のご質問につきましては、info_antimalware@fuva-brain.jp または、弊社代理店、または弊社営業担当へお問い合わせください。

14. 環境設定

EX AntiMalware v7 は、Manager からポリシーを自動受信します。

デフォルトは、クライアント PC の設定変更より、Manager から受信したポリシーが優先されます。

メイン画面「環境設定」をクリックすると下記ダイアログが表示されるときは、Manager から設定を変更してください。

Manager のポリシー「管理モード」を変更し、クライアントの設定をクライアントで管理できるように変更できます。この場合、クライアントで設定した内容は Manager に上書きされません。

EX AntiMalware v7 では、動作に影響を与える環境設定が数多く存在します。

設定の詳細は**「EX AntiMalware v7 Manager ユーザガイド」**をご参照ください。

株式会社フーバーブレイン

E-Mail: info_antimalware@fuva-brain.jp URL: https://www.fuva-brain.jp