ESET Cyber Security

ユーザー ガイド

この文書のオンラインバージョンを表示するにはこちらをクリックしてください。

Digital Security
Progress. Protected.

ESET Cyber SecurityはESET, spol. s r.o.によって開発されています

詳細についてはhttps://www.eset.comをご覧ください。

ESET, spol. s r.o.は、事前の通知なしに、説明されたアプリケーションソフトウェアを変更する権利を有します。

テクニカルサポート: https://support.eset.com

改訂: 2024年/4月/12日

ESET Cyber Security

ESET Cyber Securityは、新しいアプローチにより真に堅牢なコンピューターセキュリティを実現します。最新バージョンのESET LiveGrid®検出エンジンは、速度と精度を使用してコンピューターを安全に保ちます。その結果、インテリジェントシステムは常に警戒態勢を保ち、攻撃や悪意のあるソフトウェアからコンピューターを守ります。

ESET Cyber Security 9は、弊社の長期にわたる取り組みによって保護機能の最大化とシステムフットプリントの最小化を実現した完全なセキュリティソリューションですESET Cyber Securityは人工知能に基づく高度な技術に基づき、システムパフォーマンスを妨害せずに、ウイルス、ワーム、トロイの木馬、スパイウェア、アドウェア、ルートキットによる侵入を積極的に駆除することができます。

バージョン7の新機能

ESET Cyber Securityバージョン6には次のアップデートと改良が導入されています。

- **高パフォーマンスと高い安定性**により、各コンポーネントのアーキテクチャが分離され、必要なときにのみ起動し、エラーが発生した場合にアプリケーション全体がクラッシュから保護します。最適化が向上すると、より迅速かつ効率的な検査が可能になります。
- **ARM互換性**にはARMアーキテクチャに基づくAppleでのネイティブサポートが含まれます。以前のバージョンは、ARMサポートするためにRosetta 2を使用していました。
- **グラフィカルユーザーインターフェースの新しい設計**ダークモードがサポートされます。
- **マルチインストーラー**では、1つのインストールファイルにすべての言語が組み込まれています。
- **自動アップデート**により、アップデートを検索し、新しいバージョンを自動的にダウンロードし、各アップデートについて通知します。
- **アプリケーション環境設定**が再設計され、改善されています。

ESET Cyber Securityの新機能の詳細については、このESETナレッジベース記事をお読みください。

設定の移行

バージョン7.2以降ではESET Cyber Securityバージョン6からの設定が、アップグレードプロセス中に自動的に新しいバージョンに移行されます。

移行処理が完了した後、ESET Cyber Securityのホーム画面に、設定の移行が成功したことを示す次の通知が表示されます。**設定は新しいバージョンに転送されましたS**

既にバージョン6からバージョン7または7.1にESET Cyber Securityをアップグレードしている場合は、新しいバージョンにアップグレードして設定を移行できます。手順については、移行に関するESETナレッジベース記事をご覧ください。

バージョン7.Xで使用可能なすべての設定はバージョン6から移行されますが、次の例外があります。

- 権限設定(バージョン7ではサポートされていません)
- アップデートのカスタムプロキシサーバー(カスタムプロキシはバージョン7でサポートされてい

ません）

- 隔離コンテンツ
- 検査の駆除レベル
- オンデマンド検査の対象プロファイル

次の機能の設定は移行.xmlファイルに保存され、機能が将来のバージョンのESET Cyber Securityにあるときに読み込まれます。

- デバイスコントロール
- ログ
- Webアクセス保護
- プレゼンテーションモード

システム要件

のパフォーマンスを最大化するには、システムは、次のようなハードウェアおよびソフトウェア要件を満たしている必要があります。

	システム要件:
プロセッサーのアーキテクチャー	Intel 64-bit, M1, M2
OS	macOS Big Sur (11.0)以降
メモリ	300 MB
空きディスク容量	600 MB
その他	製品をアクティベーションまたはアップグレードするには、インターネット接続が必要です

ESET Cyber Securityバージョン7は、ARMアーキテクチャでのAppleサポートのネイティブサポートを提供します。

インストール

インストールを開始する前に、すべての開いているコンピュータープログラムを終了しますESET Cyber Securityには、コンピューターにインストールされている他のウイルス対策プログラムと競合する可能性のあるコンポーネントが含まれています。このため、他のすべてのウイルス対策プログラムを削除し、潜在的な問題を防止することを強く推奨します。

インストールウィザードを起動するにはESET Webサイトからダウンロードしたファイルを開き、**インストールESET Cyber Security**アイコンをダブルクリックします。インストールウィザードは、セットアップを案内します。

ESET Cyber Securityインストールファイルも ESET HOMEからダウンロードできます。詳細については、ESETナレッジベース記事を参照してください。

オンボーディング

ESET Cyber Securityのインストール後、**オンボーディングウィザード**が表示されますESET Cyber Securityが完全に機能するための推奨および必須手順を案内する一連の画面が表示されます。

1. **推奨保護設定**を有効にし、優先オプションを選択して、**続行**をクリックします。**ESET LiveGrid®**または**望ましくない可能性のあるアプリケーション**の詳細については、用語集を参照してください。

2. 必須手順:**ESETシステム拡張機能**を有効にする画面の手順に従い、設定を続行します。

3. 必須手順:**プロキシ設定**を許可します。アラートウィンドウで、**許可**を選択します。

4. 必須手順:ESET Cyber Security**フルディスクアクセス**を許可します。画面の手順に従い、フルディスクアクセスを許可します。

5. 次に、ウィザードで**ESET Cyber Securityのアクティベーション**を求めるメッセージが表示されます。アクティベーションの章には複数のアクティベーションオプションがあります。

6. **通知を許可**。通知を許可し、検出された脅威を常にシステムに通知することをお勧めします。

ESET Cyber Securityオンボーディングウィザードをスキップしています。
後で設定をクリックすると、必須設定をスキップできますが、保護は部分的にのみ機能します。

オンボーディングウィザードを再起動しています
Finder > アプリケーションを開く > Controlキーを押しながら**ESET Cyber Security**アイコンをクリック（または右クリック）> ショートカットメニューから**パッケージの内容を表示**を選択 > **Contents**を開く > **Helpers > オンボーディング**を開く。システム拡張機能を許可と、フルディスクアクセスを許可の章に従い、必要なセキュリティ設定を手動で設定することもできます。

ESET Cyber Securityをインストールした後、悪意あるコードを対象としたコンピューターの検査を実行する必要があります。そのために、メインプログラムウィンドウから**検査**をクリックし、**今すぐ検査**をク

リックします。オンデマンドコンピューターの検査の詳細については、オンデマンドコンピューターの検査セクションを参照してください。

システム拡張機能を許可する

初めてESET Cyber Securityをインストールする場合は、**システム拡張機能**をESET Cyber Securityで保護することを許可する必要があります。これは、オンボーディングプロセスの一部として行うことも、以下の手順を使用して手動で**システム拡張機能を許可する**こともできます。

macOS Ventura (13.x)以降を使用している場合は、こちらの手順に従ってください

1. **システム設定**を開きます。
2. 左側のメニューで**プライバシーとセキュリティ**を選択します。
3. **セキュリティ**セクションまでスクロールし、「一部のシステムソフトウェアを使用する前に注意が必要です」というメモの下の**詳細**ボタンをクリックします。

> **「一部のシステムソフトウェアを使用する前に注意が必要です」**が表示され、**詳細**ボタンが使用できない場合、システム拡張機能は以前に許可され、さらなるアクションは必要とされません。

4. **Touch ID**を使用するか、**パスワードを使用**するをクリックして**ユーザー名**と**パスワード**を入力してから、**ロック解除**をクリックします。
5. トグルをクリックすると、**ESETリアルタイムファイルシステム保護**と**ESET Webとメール保護**の両方を有効にできます。
6. **OK**をクリックします。
7. **ESET Webとメール保護**アラートを表示し、**プロキシ設定**を追加するよう指示されます。**許可**]を選択します。アラートが表示されているときにプロキシ設定を許可しない場合は、アラートを開始し、もう一度プロキシ設定を許可するオプションを表示するためには、コンピューターを再起動する必要があります。

詳細な段階的なガイドについては、ナレッジベース記事をご覧ください。言語によって、ナレッジベース記事が提供されていない場合があります。

macOS Monterey (12.x)以前をお使いの場合は、こちらの手順に従ってください

1. **システム環境設定**を開きます。
2. **セキュリティとプライバシー**を選択します。
3. 左下のロックアイコンをクリックすると、設定ウィンドウで変更を行うことができます。
4. **Touch ID**を使用するか、**パスワードを使用**するをクリックしてユーザー名とパスワードを入力してから、**ロック解除**をクリックします。
5. **詳細**をクリックします。
6. すべての**ESET Cyber Security**オプションを選択します。
7. **OK**をクリックします。

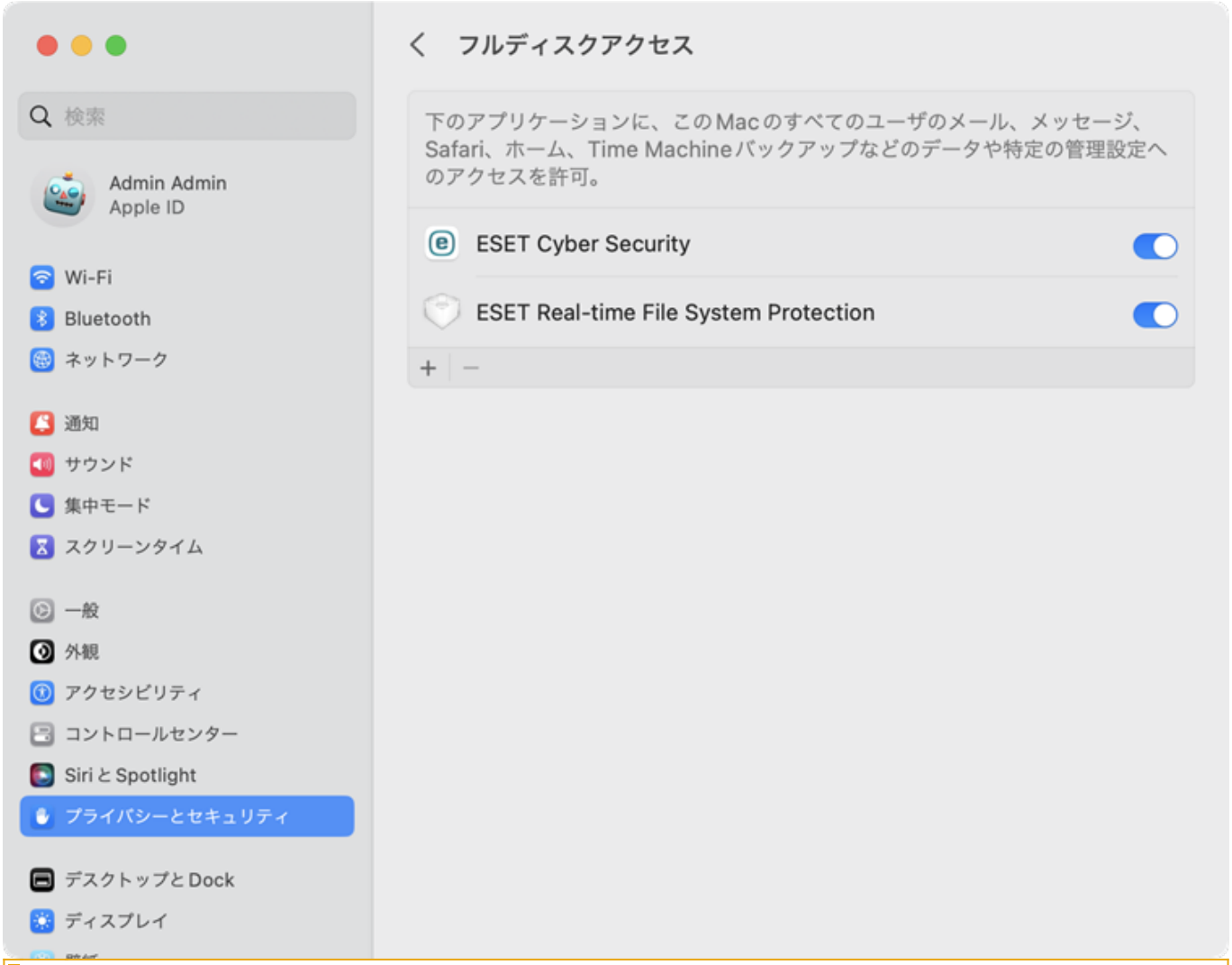
> **オンボーディングウィザードを再起動しています**
> **Finder > アプリケーション**を開く > Controlキーを押しながら**ESET Cyber Security**アイコンをクリック（または右クリック）> ショートカットメニューから**パッケージの内容を表示**を選択 > **Contents**を開く > **Helpers > オンボーディング**を開く。オンボーディングウィザードは、ESET Cyber Securityを完全に保護するために必要な手順を案内します。

フルディスクアクセスを許可

初めてESET Cyber Securityをインストールする場合は、ESET Cyber Security**フルディスクアクセス**を保護することを許可する必要があります。これは、オンボーディングプロセスの一部として行うことも、以下の手順を使用して手動で**フルディスクアクセスを許可する**こともできます。

macOS Ventura (13.x)以降を使用している場合は、こちらの手順に従ってください

1. **システム設定**を開きます。
2. 左側のメニューで**プライバシーとセキュリティ**を選択します。
3. **フルディスクアクセス**オプションをクリックし、ESET Cyber Securityトグルをクリックして有効にします。
4. **Touch ID**を使用するか、**パスワードを使用**するをクリックしてユーザー名とパスワードを入力してから、**ロック解除**をクリックします。
5. ESET Cyber Securityの再起動の確認メッセージが表示される場合は、**後で**をクリックします。
6. **ESETリアルタイムファイルシステム保護**トグルをクリックして有効にします。



リアルタイムファイルシステム保護オプションが使用できない場合は、ESET製品のシステム拡張機能を許可する必要があります。

7. システム拡張機能とフルディスクアクセスを有効にした後、コンピューターを再起動します。詳細については、ナレッジベース記事を参照してください。

macOS Monterey (12.x)以前をお使いの場合は、こちらの手順に従ってください

1. **システム環境設定**を開きます。
2. **プライバシー**タブに移動し、左側のメニューから**フルディスクアクセス**を選択します。
3. 左下のロックアイコンをクリックすると、設定ウィンドウで変更を行うことができます。
4. **Touch ID**を使用するか、**パスワードを使用**するをクリックしてユーザー名とパスワードを入力してから、**ロック解除**をクリックします。
5. リストから**ESET Cyber Security**を選択します。
6. ESET Cyber Securityの再起動通知が表示されます。**後で**クリックします。
7. リストから**ESETリアルタイムファイルシステム保護を**選択します。

リアルタイムファイルシステム保護オプションが使用できない場合は、ESET製品のシステム拡張機能を許可する必要があります。

8. 警告ダイアログウィンドウで**再開**をクリックしてESET Cyber Securityを再起動して変更を反映するか、コンピューターを再起動します。詳細については、ナレッジベース記事を参照してください。

オンボーディングウィザードを再起動しています
Finder > アプリケーションを開く > Controlキーを押しながら**ESET Cyber Security**アイコンをクリック（または右クリック）> ショートカットメニューから**パッケージの内容を表示**を選択 > **Contents**を開く > **Helpers > オンボーディング**を開く。オンボーディングウィザードは、ESET Cyber Securityを完全に保護するために必要な手順を案内します。

製品のアクティベーション

製品のアクティベーションウィンドウは、オンボーディングステップの1つとして表示されます。オンボーディング中に製品のアクティベーションが実行されていない場合は、ESET Cyber Securityアプリケーションでいつでもアクセスできます。アプリケーションを起動するにはmacOSメニューバー（画面の上部）にあるESET Cyber Securityアイコンをクリックし、[ESET Cyber Securityを表示]を選択します。**製品のアクティベーション**アラートは、**概要**セクションに表示されます。アラートには、**アクティベーションダイアログ**へのリンクがあります。アクティベーションダイアログが開きます。次の項目を指定します。

- **製品認証キーでアクティベーションする** – 製品認証キーを入力して、サブスクリプションの所有者を識別し、サブスクリプションをアクティベーションします。製品認証キーはXXXX-XXXX-XXXX-XXXX-XXXXまたはXXXX-XXXXXXXXの形式の一意の文字列です。

- **体験版ライセンス** – 購入前にESET Cyber Securityを評価するには、このオプションを選択します。情報を入力し、**登録**をクリックして、一定の期間ESET Cyber Securityをアクティベーションします。試用ライセンスは、お客様1名に付き1度だけ有効化できます。

- **サブスクリプションの購入** – このオプションをクリックしてサブスクリプションを購入します。これにより、最寄りのESET販売代理店のWebサイトにリダイレクトされます。

- **ESET HOMEアカウントを使用する** - ESET HOMEアカウントにログインし、サブスクリプションを選択して、デバイスでESET製品をアクティベーションします。

- **後でアクティベーション** - 現時点でアクティベーションしない場合は、このオプションをクリックします。

製品認証キーの場所の詳細については、次のESETナレッジベース記事を参照してください。

サブスクリプションを見つける方法

オンラインでサブスクリプションを購入した場合は、製品認証キー(XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)、ライセンスID(xxx-xxx-xxx)、製品名(または製品リスト)、および数量が記載された電子メールがESETから届きます。製品のボックス版を購入した場合、製品認証キーは製品パッケージの内部または裏側に記載されています。

製品認証キーが機能しない場合は、次のESETナレッジベース記事を参照してください。

アンインストール

ESET Cyber Securityを削除するには、次の手順に従います。

1. 起動**Finder**

2. ハードドライブの**Applications**フォルダを開きます。

3. Controlキーを押しながら**ESET Cyber Security**アイコンをクリック(または右クリック)します。

4. ショートカットメニューから**パッケージの内容を表示**を選択します。

5. **Contents** > **Helpers**フォルダを開き、**Uninstaller**アイコンをダブルクリックします。

ESETCyberSecurityインストールファイル(.dmg)を保持している場合は、それを開き、**アンインストールをダブル**クリックします。

ESET Cyber Securityの操作

ESET Cyber Securityのメインウィンドウは、2つのセクションに分かれています。右のプライマリウィンドウには、左のメインメニューで選択したオプションに対応する情報が表示されます。

メインメニューから次のセクションにアクセスできます。

- **概要** - ESET Cyber Securityモジュールの動作状態についての情報の概要を提供します。
- **検査** – すべてのローカルディスクを検査するか、カスタム検査を実行できます。
- **保護** – コンピューターのセキュリティレベルの調整を許可します。
- **アップデート** – 検出エンジンアップデートについての情報を表示します。
- **ツール** - ログファイルと隔離へのアクセスを提供します。
- **ヘルプとサポート**—ヘルプファイル、ESETナレッジベース、サポートリクエストフォームへのアクセスを提供します。

保護の状態の確認

保護の状態を表示するには、メインメニューの**概要**]をクリックします。プライマリウィンドウにはESET Cyber Securityモジュールの動作状態の概要が表示されます。

ヘルプとサポート

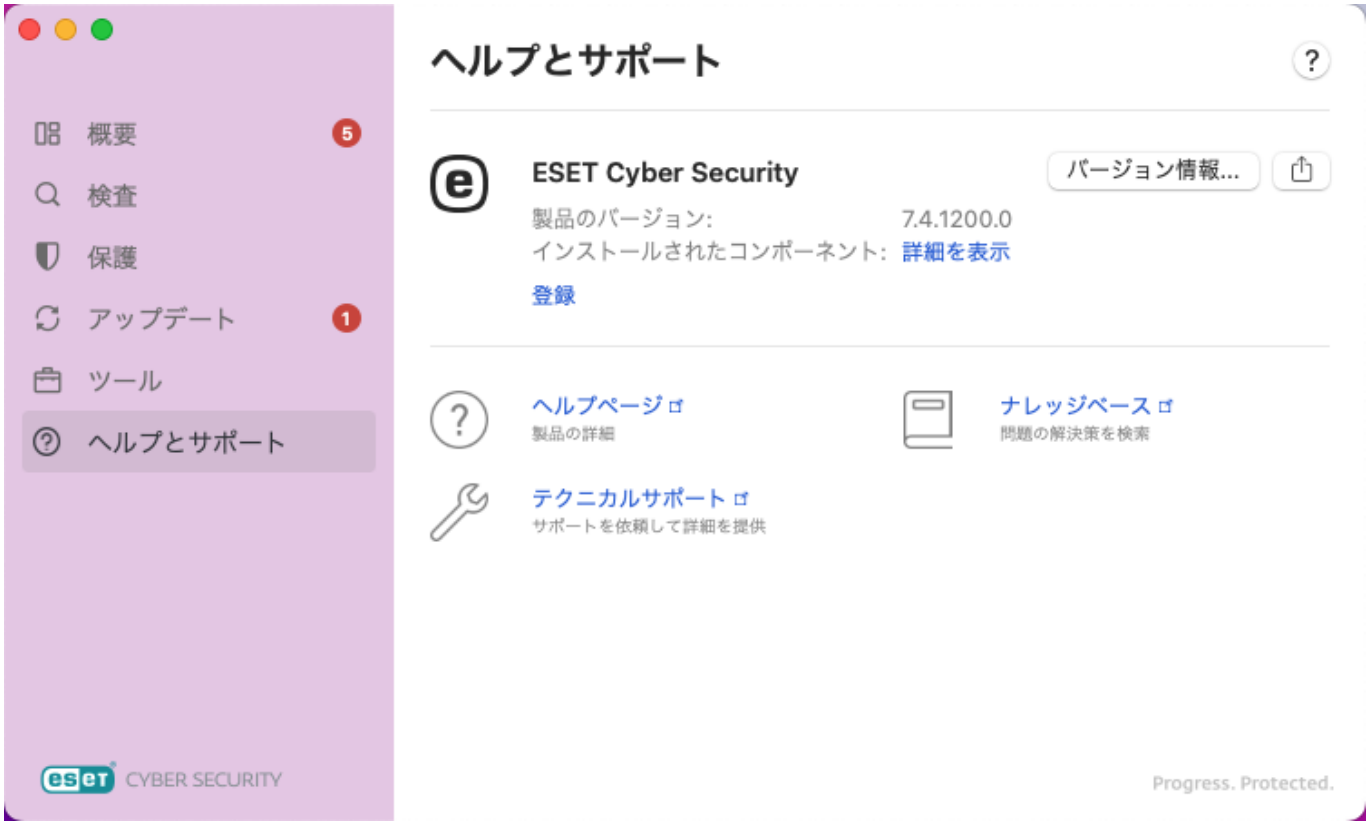
ESET Cyber Securityには、トラブルシューティングツール、および発生する可能性のある問題の解決に役立つサポート情報が含まれます。ヘルプとサポートセクションは、メインアプリケーションウィンドウで確認できます。インストールされたコンポーネントの一覧を表示するには、**インストールされているコンポーネント**の横の**詳細を表示**をクリックします。一覧をクリップボードにコピーするには、[インストールされているコンポーネント]ウィンドウの任意の場所を右クリックし、**すべてコピー**をクリックします。この機能は、トラブルシューティングを行う場合、またはテクニカルサポートに問い合わせる場合に便利です。

ESET Cyber Security製品バージョンと製品サブスクリプションIDが表示されます。サブスクリプションを変更するオプションがあります。このオプションをクリックすると、[アクティベーション]ウィンドウが起動し、製品をアクティベーションします。**バージョン情報**ボタンをクリックするとESET Cyber Securityの詳細が表示されます。

ヘルプページ – このリンクをクリックするとESET Cyber Securityヘルプページが開きます。

テクニカルサポート—ヘルプページで問題を解決できない場合はESETテクニカルサポートまでお問い合わせください。

ナレッジベース - ESETナレッジベース には、最もよくある質問への回答や、さまざまな問題に対する一般的な解決策が登録されていますESETのテクニカルスペシャリストが定期的に更新しているので、このナレッジベースは、さまざまな問題を解決するための最も強力なツールです。



設定のインポート/エクスポート

既存の設定をインポートするかESET Cyber Security設定をエクスポートするにはESET Cyber Securityのメインアプリケーションウィンドウを開き、画面の左上にあるmacOSメニューバーで**ファイル > 設定のインポートまたはエクスポート**をクリックします。

インポートとエクスポートは、後から使用するためにESET Cyber Securityの現在の設定をバックアップする必要がある場合に便利です。[設定のエクスポート]は、ESET Cyber Securityの任意の基本設定を複数のシステムに対して使用する場合にも便利です。設定ファイルをインポートして目的の設定を転送できます。

構成をインポートするには、**設定のインポート**を選択し、インポートする構成ファイルに移動します。エクスポートするには、**[設定のエクスポート]**を選択し、ブラウザーを使用して、構成ファイルを保存するコンピューターの場所を選択します。

ショートカットキー

ESET Cyber Securityで操作を簡単に行うには、次のキーボードショートカットを使用できます。

- cmd+, - ESET Cyber Security環境設定を表示します。
- cmd+Q - ESET Cyber SecurityメインGUIウィンドウを閉じますmacOSメニューバー(画面上部)のESET Cyber Securityアイコンをクリックし、**ESET Cyber Securityを表示**を選択すると、開くことができます。
- cmd+W - ESET Cyber SecurityメインGUIウィンドウを閉じます。

プログラムが正しく動作しない場合の解決方法

すべてのモジュールが正しく機能すると、緑色の**保護されています**ヘッダーが**概要**セクションに表示されます。モジュールが正常に機能しない場合は、赤色の**セキュリティアラート**ヘッダーまたはオレンジ色の**注意が必要です**ヘッダーが表示されますESET Cyber Securityにはモジュールに関する追加情報と、問題を修正するための推奨される解決策が表示されます。各モジュールの状態を変更するには各通知メッセージの下にある青いリンクをクリックします。

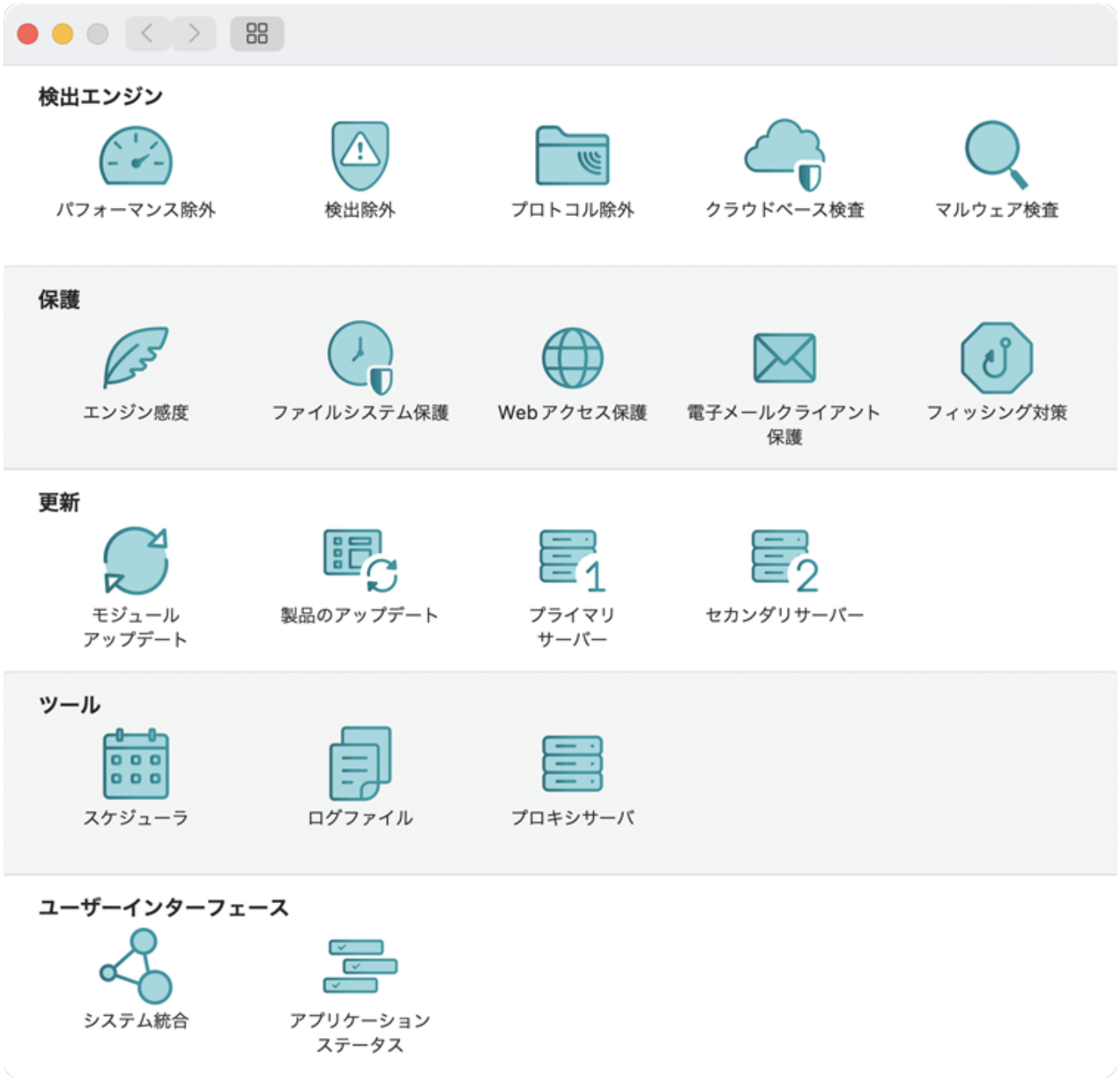
提示された解決策を使用して問題を解決できない場合は、ESETナレッジベースを検索するか、ESETテクニカルサポートにお問い合わせください。

アプリケーション環境設定

ESET Cyber Securityの詳細設定を変更するにはcmd+,を使用して**アプリケーション環境設定**を開くかmacOSメニューバーのESET Cyber Securityをクリックして**環境設定**(設定)を開きます。

次のカテゴリのモジュールの設定を構成できます。

- 検出エンジン
- 保護
- アップデート
- ツール
- ユーザーインターフェース



検出エンジン

検出エンジンは、ファイルを制御することで、悪意のあるシステム攻撃から保護します。たとえば、マルウェアに分類されたオブジェクトが検出された場合、修復が開始します。検出エンジンは、最初にブロックし、その後に駆除、削除、または隔離に移動して、マルウェアを排除できます。

ESET Cyber Security**検出エンジン**の詳細設定を変更するには⍰cmd+,を使用して**アプリケーション環境設定**を開くか⍰macOSメニューバーのESET Cyber Securityをクリックして**環境設定**(設定)を選択します。

パフォーマンス除外

[**パフォーマンス除外**]セクションでは、特定のファイルやフォルダー、アプリケーション、またはIP/IPv6アドレスを検査から除外することができます。パス(フォルダー)を検査から除外することで、ファイルシステムのマルウェア検査に必要な時間を大幅に短縮できます。

- ＋ – 新しい例外を作成します。オブジェクトのパスを入力します。
- － – 選択したエントリーを除去します。

⚠ リアルタイムファイルシステム保護で重大な問題が発生した場合にのみ、ファイルを検査から除外してください。これは、検査からファイルを除外することで全体的な保護が低下するためです。

検出除外

この機能を使用すると、検出名、オブジェクトパス、またはハッシュをフィルタリングして、オブジェクトを駆除から除外できます。

検出除外を設定するときは、具体的な除外基準を指定する必要があります。有効な検出名またはSHA-1ハッシュを指定する必要があります。有効な検出名またはSHA-1ハッシュについては、ログファイルを参照し、ログファイルドロップダウンメニューから検出を選択します。これは、誤検出サンプルがESET Cyber Securityで検出されているときに役立ちます。実際の侵入に対しての除外は非常に危険です。一時的な場合に限って影響を受けるファイルまたはディレクトリのみを除外することを検討してください。除外は、望ましくない可能性があるアプリケーション、安全でない可能性があるアプリケーション、不審なアプリケーションにも適用されます。

次のタイプの**駆除基準**があります。

- **正確なファイル** – ファイルタイプ、場所、名前、拡張子に関係なく、指定されたハッシュSHA-1に基づいて、ファイルを除外します。
- **検出** – 検出名で各ファイルを除外します。
- **パスと検出** – ファイル名(`file:///Users/documentation/Downloads/eicar_com.zip`など)を含む検出名とパスで各ファイルを除外します。

⚠ マルウェアなどの検出で重大な問題が発生した場合にのみ、検出除外を使用してください。これは、マルウェアを検査から除外すると、全体的な保護が低下するためです。

プロトコル除外

除外リストのエントリは製品コンテンツフィルタリングから除外されます。このオプションは信頼できるとわかっているアプリケーションまたはアドレスに対してのみ使用することをお勧めします。

クラウドベース検査

ESET LiveGrid®に参加する(推奨)

ESET LiveGrid®評価システムは、検査済みファイルをクラウドのホワイトリストおよびブラックリスト項目のデータベースと比較し、ESETマルウェア対策ソリューションの効率化を図ります。

ESET LiveGrid®フィードバックシステムを有効にする

詳細分析のため、データはESET Virus Labに送信されます。

サンプルの送信

検出されたサンプルの自動送信：選択したオプションに基づいて、感染したサンプルを分析のためにESET Research Labに送信し、将来の検出を改善できます。

- すべての検出されたサンプル
- 文書を除くすべてのサンプル
- 送信しない

不審なサンプルの自動送信：脅威に似ていたり標準ではない特性や動作を示す不審なサンプルは、分析のためにESET Research Labに送信されます。

- 実行ファイル - .exe.dll.sysなどの実行ファイルが含まれます。
- アーカイブ - .zip..rar..7z..arch..arj..bzip2..gzip..ace..arc..cabなどのアーカイブファイルタイプが含まれます。
- スクリプト - .bat.cmd.hta.js.vbs.ps1などのスクリプトファイルタイプが含まれます。
- 文書 – アクティブなコンテンツが埋め込まれたMicrosoft Office.Libre Office.または他のオフィスツールで作成された文書やPDFが含まれます。
- その他 - .jar.reg.msi.swf.lnkなどのファイルタイプが含まれます。

自動送信除外：除外されたファイルは、不審なコードが含まれる場合でも.ESET Research Labに送信されません。

クラッシュレポートと診断データを送信

クラッシュレポート、モジュールメモリダンプなどのデータを送信します。

匿名の使用状況統計情報を送信し、製品の改善を支援する

脅威名、脅威の日時、検出方法、関連付けられたメタデータ、製品バージョンと設定(システム情報を含む)などの新しく検出された脅威、検査されたファイル(ハッシュ、ファイル名、ファイルの作成元、テレメトリー)、ブロックされたURL.不審なURLに関する匿名情報をESETが収集することを許可します。

連絡先の電子メールアドレス(任意)

連絡先メールアドレスを不審なファイルに含め、分析のためにさらに情報が必要な場合に連絡するために使用されることがあります。詳しい情報が必要でない限り、ESETから連絡することはありません。

マルウェア検査

オンデマンドスキャナーはウイルス対策の重要な部分であり、コンピューター上のファイルやフォルダーのスキャンを実行するために使用されます。セキュリティの観点からは、感染が疑われるときだけコンピューターの検査を実行するのではなく、通常のセキュリティ手段の一環として定期的に実行することが重要です。**マルウェア検査**セクションでは、オンデマンド検査プロファイルのオプションを設定できます。

プロファイルの一覧 –新しいプロファイルを作成するか、既存のプロファイルを削除するには、  または  を選択します。新しいプロファイルを追加するときに、プロファイルの名前を入力し、**[OK]**をクリックします。新しいプロファイルは、既存の検査プロファイルが一覧表示される選択したプロファイルドロップダウンメニューに表示されます。

ThreatSenseパラメーター – 制御するファイルの拡張子、検査するオブジェクト、使用される検出方法などの検査プロファイル設定オプション。

保護

ESET Cyber Securityの詳細**保護**設定を変更するには⍰cmd+,を使用して**アプリケーション環境設定**を開くか⍰macOSメニューバーのESET Cyber Securityをクリックして**環境設定**(設定)を開きます。

エンジン感度

エンジン感度では、すべての保護モジュールの次のカテゴリのレポートおよび保護レベルを設定できます。

- **マルウェア** – コンピューターの既存のファイルの過去である悪意のあるコード

- **望ましくない可能性のあるアプリケーション**– グレイウェアまたは望ましくない可能性があるアプリケーション(PUA)は、ウイルスまたはトロイの木馬などの他のタイプのマルウェアほどはっきりとした意図がない幅広いソフトウェアのカテゴリです。ただし、追加の不審なソフトウェアをインストールし、デジタルデバイスの動作または設定を変更し、ユーザーによって承認または想定されていないアクティビティを実行する可能性があります。この種のアプリケーションの詳細については、「用語集」を参照してください。

- **不審なアプリケーション** – パッカーまたはプロテクターを使用して圧縮されたプログラムなどが挙げられます。この種類の防御は、多くの場合、マルウェアの作成者が検知されるのを逃れるために利用します。パッカーは、数種類のマルウェアを単一のパッケージにロールアップする自己解凍型のランタイム実行可能ファイルです。最も一般的なパッカーは、UPX⍰PE_Compact⍰PKLite⍰およびASPackです。同じマルウェアでも、異なるパッカーを使用して圧縮されると、異なる方法で検出される場合があります。パッカーはまた、時間の経過と共に自身の「シグネチャ」を変化させることで、マルウェアの検出および除去をより一層難しくすることができます。

- **安全ではない可能性があるアプリケーション** – 安全ではない可能性があるアプリケーションとは、そのアプリケーションがインストールされたことをユーザーが知らない場合、攻撃者によって悪用される可能性のある、市販の適正なソフトウェアのことを指します。これには、リモートアクセスツールなどのプログラムが含まれます。このオプションは、既定では無効になっています。

ファイルシステム保護

検査は多種多様なイベントで実行されます⍰ESET LiveGrid®テクノロジを利用し(ThreatSenseエンジンパラメータ設定を参照)、リアルタイムファイルシステム保護は新たに作成されたファイルと既存のファイルとでは異なることがあります。新しく作成されたファイルは、より正確に制御できます。

Real-timeスキャナーから次のタイプのメディアを除外できます。

- **ローカルドライブ** – システムハードドライブ

- **リムーバブルメディア** (USBメディア、Bluetoothデバイスなど)
- **ネットワークメディア** – すべてのマッピングされたドライブ

既定では、**ファイルを開くとき**、**ファイルを作成するとき**に、検査されます。既定の設定ではコンピューターが最大限のレベルでリアルタイムファイルシステム保護が提供されるので、既定の設定を変更しないことをお勧めします。

また、特定のプロセスを検査から除外できます。

既定の設定を使用し、データ転送の速度を大幅に低下させる特定のメディアの検査時などの特定の場合にのみ検査除外を変更することをお勧めします。

Webアクセス保護

Webアクセス保護は、Webブラウザとリモートサーバー間の通信を監視し、HTTP (Hypertext Transfer Protocol)のルールに従います。

Webフィルタリングを実行するにはHTTP通信とURLアドレスのポート番号を定義します。

Webプロトコル

WebプロトコルセクションではHTTPプロトコルのチェックを有効または無効にしHTTP通信で使用されるポート番号を定義できます。既定ではポート番号80、8080および3128が事前定義されています。

URLアドレス管理

このセクションでは、ブロック、許可、またはチェックから除外するHTTPアドレスを指定できます。ブロックされたアドレスのリストにあるWebサイトにはアクセスできません。除外されたアドレスのリストにあるWebサイトは、悪意のあるコードの検査なしでアクセスされます。

許可、ブロック、または除外されたアドレスのリストを有効にするには、アドレスを選択して、**リストアクティブ**オプションを有効にします。現在の一覧からアドレスを入力するときに通知が必要な場合は、**[適用時に通知]**を選択します。

任意のリストで、特殊記号の*(アスタリスク)および?(疑問符)を使用できます。アスタリスクは0文字以上の任意の文字列を、疑問符は任意の1文字をそれぞれ表します。除外するアドレスを指定する際は、特に注意する必要があります。このリストには信頼できる安全なアドレスのみを含める必要があるためです。同様に、このリストでは記号*および?を正しく使用する必要があります。

電子メールクライアント保護

電子メールクライアント保護 - POP3およびIMAPプロトコルを介して受信される電子メール通信を制御します。受信メッセージを検査するときにはESET Cyber SecurityはThreatSense検査エンジンに含まれている詳細な検査方法がすべて使用されますPOP3プロトコルとIMAPプロトコルの通信の検査は、使用されるメールクライアントからは独立しています。使用可能な設定は次のとおりです:

電子メールプロトコル

ここではPOP3とIMAPプロトコル経由で受信された電子メール通信の確認を有効または無効にできます。

POP3プロトコルチェック

POP3プロトコルは、電子メールクライアントアプリケーションでのメールの受信に最もよく使用されているプロトコルですESET Cyber Securityでは、使用される電子メールクライアントに関係なく、このプロトコルに対する保護機能を備えています。

この制御を提供する保護機能はシステム起動時に、自動的に起動され、メモリでアクティブになります。モジュールが正しく動作するにはIMAPプロトコルが有効になっていることを確認してくださいIMAPプロトコル制御は、電子メールクライアントを再構成せずに、自動的に実行されます。既定では、ポート110にある全ての通信が検査されますが、他の通信ポートは必要に応じて追加できます。ポート番号はコンマで区切ります。

POP3プロトコルのチェックオプションを有効にすると、すべてのPOP3トラフィックで悪意のあるソフトウェアが監視されます。

IMAPプロトコルチェック

Internet Message Access Protocol (IMAP)は電子メール取得に使われるもう一つのインタネットプロトコルですIMAPはPOP3よりも優れている点があります。たとえばIMAPでは、複数のクライアントが同時に同じメールボックスに接続して、メッセージが既読か、返信済みか、削除されたかなどの状態の情報を保持できますESET Cyber Securityでは、使用しているメールクライアントに関係なく、このプロトコルを保護できます。

この制御を提供する保護機能はシステム起動時に、自動的に起動され、メモリでアクティブになります。モジュールが正しく動作するにはIMAPプロトコルが有効になっていることを確認してくださいIMAPプロトコル制御は、電子メールクライアントを再構成せずに、自動的に実行されます。既定では、ポート143にある全ての通信が検査されますが、他の通信ポートは必要に応じて追加できます。ポート番号はコンマで区切ります。

IMAPプロトコルのチェックを有効にするとIMAPを通過する全てのトラフィックに悪意のあるソフトウェアが無いか監視されます。

電子メールタグ

電子メールタグを使用すると、電子メールのフットノートにタグメッセージを追加できます。電子メールが検査された後、検査結果を示す通知をメッセージの最後に追加できます。タグメッセージは役立つツールですが、メッセージの安全性を最終的に判断するために使用しないでください。問題のあるHTMLではタグメッセージが省略され、特定の脅威によっては偽装される可能性があります。使用可能なオプションは

- **検出が発生したときに電子メールを受信して読み取る** – マルウェアを含む電子メールのみをチェック済みとしてタグ付けします。
- **検査時のすべての電子メール** –すべての検査された電子メールの最後にはタグメッセージが追加されます。
- **何もしない** – どの電子メールにも検査通知が追加されません

受信メールの件名を更新 – 電子メール保護で感染した電子メールに脅威警告を含める場合は、このチェックボックスをオンにします。この機能では、感染した電子メールの簡易フィルタリングが可能です。また、受信者の信頼を高めることができ、マルウェアが検出された場合、特定の電子メールまたは送信者の脅威レベルについての貴重な情報を得ることができます。

検出された電子メールの件名に追加 – 感染メールの件名のプレフィックス形式を変更する場合はこの

テンプレートを編集します。

ThreatSense パラメータ

詳細検査設定では、検査から除外する検査レベル、検査オプション、およびファイル拡張子を設定できます。

フィッシング対策

フィッシング対策保護は、もう1つの保護レイヤーであり、パスワードやその他の機密情報を取得しようと試みる非合法なWebサイトに対する防御を強化します。既定では、フィッシング対策機能が有効です。常に有効にすることをお勧めします。

アップデート

このセクションでは、アップデートサーバーやそれらのサーバーの認証データなど、アップデート用の設定情報を指定しますESET Cyber Securityの詳細**アップデート**設定を変更するにはcmd+,を使用して**アプリケーション環境設定**を開くかmacOSメニューバーのESET Cyber Securityをクリックして**環境設定**(設定)を開きます。

モジュールと製品のアップデート

モジュールアップデート

アップデートの種類

- **通常アップデート**。これは規定のアップデートの種類です。これにより、検出定義データベースと製品モジュールがESETアップデートサーバーから自動的にアップデートされることが保証されます。

- **リリース前アップデート**には、まもなく公開される予定の最新の不具合修正と検出方法が含まれます。ただし、常に安定しているとは限りません。したがって、本番環境で使用することは推奨されていません。

- **遅延アップデート**では専用のアップデートサーバーからの更新が可能であり、新しいバージョンのウイルスデータベースの提供が少なくともX時間遅れます(つまり、データベースは実際の環境でテストされ、安定しているとみなされます)。

モジュールロールバック

新しい検出エンジンアップデートやプログラムモジュールのアップデートが不安定であったり破損している疑いがある場合、前のバージョンにロールバックし、一時的にアップデートを無効にできます。

モジュールのスナップショットを作成

ESET Cyber Securityは、ロールバック機能を使用するため、検出エンジンとプログラムモジュールのスナップショットを記録します。モジュールデータベースのスナップショットを作成するには、**モジュールのスナップショットを作成**するを有効にしておきます。**モジュールのスナップショットを作成する**を有効にすると、最初のアップデート中に最初のスナップショットが作成されます。次のスナップショットは48時間後に作成されます。**ローカルに保存するスナップショットの数**フィールドにより、保存されて

いる検出エンジンスナップショットの数が定義されます。

最大スナップショット数(例: 3つ)に達すると、最も古いスナップショットが48時間ごとに新しいスナップショットに置換されますmacOSのESET Cyber Securityは検出エンジンとプログラムモジュールのアップデートバージョンを最も古いスナップショットにロールバックします。

製品のアップデート

製品のアップデートにより、常に最新の製品バージョンが使用できるようになります。**自動アップデート**トグルを有効にすると、次回の再起動時に製品のアップデートプログラムが自動的にインストールされ、最新の機能と可能な限り最高の保護に常にアクセスできます。

プライマリサーバーとセカンダリサーバー

プライマリおよびセカンダリアップデートサーバーを自動的に選択するオプションが、規定で有効になっています。自動的に選択するトグルを無効にすると、両方のサーバーを指定できます。

ツール

ESET Cyber Security**ツール**の詳細設定を変更するにはcmd+,を使用して**アプリケーション環境設定**を開くかmacOSメニューバーのESET Cyber Securityをクリックして**環境設定**(設定)を開きます。

スケジューラ

スケジューラを使用すると、指定した時刻に自動的に実行されるオンデマンド検査タスクを設定できます。新しいスケジュールタスクを作成する、もしくは既存のタスクを削除するには、+または−を選択します。また、タスクを繰り返す曜日を定義することもできます。

ログファイル

ログの詳細レベル

ロギング詳細レベルは、ログファイルに含まれる詳細のレベルを定義します。

- **重大な警告** – 重大なエラー(**ウイルス対策保護の起動に失敗した**など)のみが含まれます。
- **エラー** – 重大な警告のほかに、**「ファイルのダウンロードエラー」**といったエラーが記録されます。
- **警告** – 重大なエラー、警告メッセージ、エラーが記録されます。
- **情報レコード** – アップデートの成功メッセージを含むすべての情報メッセージと上記のすべてのレコードを記録します。
- **診断レコード** – プログラムおよび上記のすべてのレコードを微調整するのに必要な情報が記録されます。

ログファイルのクリーニング

次の日数が経過したエントリを自動的に削除 – 指定された日数を経過したログエントリが自動的に削除されます。

ログファイルの最適化

ログファイルを自動的に最適化する – チェックすると、**使用されていないエントリの割合が次の値よりも大きくなったら最適化**フィールドに指定した断片化の割合を超えると、ログファイルは自動的に最適化されます。すべての空のログエントリが削除され、パフォーマンスとログ処理速度が改善します。大量のエントリがログに含まれるときに、この改善が実行されます。

プロキシサーバーの設定

プロキシサーバー設定を指定できます。ここで設定するパラメーターは、インターネットへの接続を必要とするすべてのモジュールで使用されます。

プロキシサーバーを設定するには

1. **プロキシサーバーを使用**を有効にし、プロキシサーバーのアドレスとプロキシサーバーのポート番号をプロキシサーバーフィールドに入力します。

2. プロキシが使用できない場合は**直接接続を使用する**を有効にして、プロキシをバイパスし、直接ESETサーバーと通信します。

3. プロキシサーバーとの通信に認証が必要な場合、**プロキシサーバーは認証が必要**をオンにし、有効な**ユーザー名**と**パスワード**をそれぞれのフィールドに入力します。

ユーザーインターフェース

ESET Cyber Security**ユーザーインターフェース**の詳細設定を変更するには⌘cmd+,を使用して**アプリケーション環境設定**を開くか⌘macOSメニューバーのESET Cyber Securityをクリックして**環境設定**(設定)を開きます。

システム統合

ユーザーインターフェース要素

ユーザーがグラフィカルユーザーインターフェースを開くことを許可 – この設定を無効にすると、ユーザーがGUIにアクセスできません。これは、管理された環境またはシステムリソースを保持する必要がある場合に便利です。

メニューバーにアイコンを表示する – この設定を無効にすると⌘macOSメニューバー(画面上部のメニューバーエクストラ)にESET Cyber Securityアイコンが表示されません。

通知

デスクトップに通知を表示 – デスクトップ通知(アップデートの成功メッセージ、ウイルス検査タスク完了、新しい脅威の検出など)がmacOSメニューバーの横の小さいポップアップウィンドウに表示されます。有効にすると、新しいイベントが発生したときにESET Cyber Securityで通知されます。

アプリケーションステータス

ここではESET Cyber Security製品に表示されるアプリケーションステータスを選択できます。**ステータスを表示**スイッチが無効で、問題が報告された場合ESET Cyber Securityアプリケーションは緑色の**保護されています**ステータスのままになります。

保護

アプリケーションのメインウィンドウの**保護**オプションでは、コンピュータWebメールの保護レベルを調整できます。コンピューター保護とWebとメール保護セクションには、有効または無効にできる保護モジュールが含まれます。すべてのモジュールを有効にしてESET Cyber Securityを最大限に活用し、コンピューターを安全に利用することを強くお勧めします。

コンピュータ保護

コンピューターの保護の設定は**保護 > コンピューター**で確認できます。このウィンドウには、**リアルタイムファイルシステム保護**と**ESET LiveGrid® レピュテーションシステム**モジュールのステータスが表示されます。両方のモジュールを有効にすることをお勧めします。いずれかのモジュールをオフにすると、コンピューターの保護が低下する可能性があります。

トグルをクリックすると、**アップデート**セクションで**自動アップデート**機能を有効または無効にできます。自動アップデートが有効な場合ESET Cyber Securityは最新の製品のアップデートを検出し、自動的にダウンロードします。

Webとメール保護

メインメニューからWebとメール保護にアクセスするには、[**保護**] > [**Webとメール**]をクリックします。各モジュールの詳細設定を管理するにはcmd+,を使用して**アプリケーション環境設定**を開くかmacOSメニューバーでESET Cyber Securityをクリックして**環境設定**(設定)を選択します。次の保護モジュールはWebとメール保護で使用できます。

- **Web** - Webブラウザーとリモートサーバー間のHTTP通信を監視します。
- **フィッシング対策** - Webサイトまたはドメインから発生する潜在的なフィッシング攻撃をブロックします。
- **電子メール** - POP3およびIMAPプロトコルを介して受信される電子メール通信を制御します。

検査例外
ESET Cyber Securityは暗号化されたプロトコルのHTTPS、POP3S、IMAPSを検査しません。

フィッシング対策機能

フィッシングはソーシャルエンジニアリング(機密情報を入手するためにユーザーを操る)を使用する犯罪活動です。フィッシングは、銀行口座番号、クレジットカード番号、PIN番号、ユーザー名、パスワードなどの機密情報を取得するために使用されることがあります。フィッシングの詳細については、ESET用語集を参照してください。

フィッシング対策は有効にしておくことをお勧めします(保護>Webとメール > フィッシング対策機能)。危険なWebサイトまたはドメインからの、フィッシングと考えられる攻撃はすべてブロックされ、攻撃があったことを知らせる警告通知が表示されます。

フィッシング対策機能が機能するかどうかをテストするには、AMTSOテストページを参照してください。

ウイルス・スパイウェア対策

ウイルス・スパイウェア対策は、潜在的な脅威を与えるファイルを修正することによって、悪意のあるシステム攻撃を防御する機能です。悪意のあるコードを含む脅威が検出されると、ウイルス対策機能がブロックし、次に駆除、削除、または移動して隔離することにより、ウイルスを排除できます。

リアルタイムファイルシステム保護

リアルタイムファイルシステム保護では、さまざまなイベントに基づいて、あらゆる種類のメディアを調べ、検査をトリガーします。検査は多種多様なイベントで実行されますESET LiveGrid®テクノロジを利用し(ThreatSenseエンジンパラメータ設定を参照)、リアルタイムファイルシステム保護は新たに作成されたファイルと既存のファイルとでは異なることがあります。新しく作成されたファイルは、より正確に制御できます。

リアルタイムファイルシステム保護の詳細設定を変更するにはcmd+,を使用して**アプリケーション設定**を開くかmacOSメニューバーで**ESET Cyber Security**をクリックし、**環境設定**(設定) > **ファイルシステム保護**を選択します。

既定では、**ファイルを開いてファイルを作成**している間に、すべてのファイルが検査されます。既定の

設定ではコンピューターが最大限のレベルでリアルタイムファイルシステム保護が提供されるので、既定の設定を変更しないことをお勧めします。リアルタイム保護はシステム起動時に起動し、中断されることなく検査が行われます。特殊な場合(別のリアルタイムスキャナーとの競合がある場合など)は、メインプログラムウィンドウからリアルタイム保護を停止できます(**保護 > コンピューター**をクリックし、**リアルタイムファイルシステム保護**をオフにします)。

Real-timeスキャナーから次のタイプのメディアを除外できます。

- **ローカルドライブ** – システムハードドライブ
- **リムーバブルメディア** - CD⍰DVD⍰USBメディア⍰Bluetoothデバイスなど。
- **ネットワークメディア** – すべてのマッピングされたドライブ

また、特定のプロセスを検査から除外できます。

既定の設定を使用し、データ転送の速度を大幅に低下させる特定のメディアの検査時などの特定の場合にのみ検査除外を変更することをお勧めします。

リアルタイムファイルシステム保護の設定の変更

リアルタイムファイルシステム保護は、ESET Cyber Securityで安全なシステムを維持するために必要です。リアルタイム保護パラメーターを変更する場合は、注意が必要です。特定のアプリケーションとの競合がある場合など、特定の場合にのみこれらのパラメーターを変更することをお勧めします。

ESET Cyber Securityのインストール後は、最大レベルのシステムセキュリティをユーザーに提供するように全ての設定が最適化されています。

リアルタイムファイルシステム保護を有効にする

リアルタイム保護が動作し、ウイルスを検出していることを検証するには、eicar.comテストファイルをダウンロードし、ESET Cyber Securityがこのファイルを脅威として特定することを確認します。このテストファイルは、あらゆるウイルス対策プログラムで検出できる特殊な無害のファイルです⍰European Institute for Computer Antivirus Research (EICAR Institute)は、このファイルを作成し、ウイルス対策プログラムの機能をテストしました。

リアルタイム保護が機能しない場合の解決方法

この章では、リアルタイムファイルシステム保護使用時に発生することがあるトラブル、およびその解決方法について説明します。

リアルタイム保護が無効である

ユーザーが不注意にリアルタイムファイルシステム保護を無効にしてしまった場合、保護を再アクティベーションする必要があります。メインメニューからリアルタイムファイルシステム保護を再有効化するには、**リアルタイムファイルシステム保護**トグルをクリックして有効にします。あるいは、アプリケーション設定ウィンドウに移動し、**リアルタイムファイルシステム保護**トグルをクリックして、リアルタイムファイルシステム保護を有効にします。

リアルタイム保護がマルウェアの検出と駆除を行わない

コンピューターに他のウイルス対策プログラムがインストールされていないことを確認します。2つのリアルタイム保護シールドが同時に有効になっていると、互いに競合することがあります。システムから他のウイルス対策プログラム(インストールされている場合)をアンインストールすることをお勧めします。

リアルタイム保護が開始されない

リアルタイムファイルシステム保護がシステム起動時に開始されない場合、他のプログラムと競合している場合があります。リアルタイムファイルシステム保護が開始されない場合は、ESETテクニカルサポートにお問い合わせください。

コンピュータの検査

コンピューターが感染している疑いがある場合(異常な動作をしているため)は、メインアプリケーションウィンドウから**検査**を選択し、**今すぐ検査**をクリックして、コンピューターの侵入を検査します。最大限の保護のために、感染の疑いがあるときにだけではなく、日常のセキュリティ対策の一部として定期的にコンピューターの検査を実行してください。検査を定期的に行うと、ディスクに保存されたときにリアルタイム検査で検出されなかった侵入物でも、検出できます。リアルタイム検査で検出できないケースとは、感染時にリアルタイム検査が無効に設定されていた場合や、検出モジュールが最新でない場合などです。

コンピューターの検査を最低でも月に1回は実行することをお勧めします。

アプリケーション設定の**ツール > スケジューラー**セクションで、スケジュールされたタスクとして、検査を設定できます。

カスタム検査

メインのアプリケーションウィンドウで**スキャン**セクションに移動し、矢印アイコンをクリックして、**カスタム検査**と**サンプルの送信**オプションを表示します。

カスタム検査

カスタム検査は、検査対象や検査方法などの検査パラメータを指定したい場合に最適です。カスタム検査を実行する利点は、パラメータを詳細に設定する機能です。

カスタム検査セクションの**検査**をクリックして、カスタム検査ウィンドウを開きます。検査するファイルをウィンドウ内の指定された領域にドラッグアンドドロップします。**参照**ボタンをクリックして、含めるフォルダーまたはファイルに移動して、**検査対象**を指定することもできます。

メニューアイコンをクリックすると、次の他のオプションが表示されます。**検査プロファイル**と**設定除外**を選択します。

検査プロファイルを選択

ここでは、優先する**検査プロファイル**を選択し、**駆除レベル**を設定できます。

検査プロファイル

スマート検査を使用すると、コンピュータの検査をすぐに開始して、ユーザーが操作しなくても感染しているファイルからウイルスを駆除できます。その主な利点は、詳細検査設定を不要にした簡単な操作です。これにより、すべてのフォルダーでにあるすべてのファイルが検査されます。検出された侵入があれば、自動的に駆除または削除されます。スマート検査プロファイルは、Smart Optimization技術を使用しており、前回の検査で感染していないことが判明したファイルのうち、その検査以降変更されていないファイルを除外します。

詳細検査プロファイルはスマート最適化技術を使用しないため、ファイルは検査から除外されません。

駆除レベル

ここでは、スキャナーが感染したファイルを処理する方法を選択できます。駆除レベルの詳細については、駆除を参照してください。

除外を設定

検査から除外するファイルまたはフォルダーを追加します。除外したいファイルを、表示ウィンドウ内の指定された領域にドラッグします。

カスタム検査でコンピューターの検査を実行するのは、ウイルス対策プログラムを以前に使用した経験のある上級ユーザーにお勧めします。

サンプルの送信

このオプションを使用すると、分析のためにファイルをESET Research Labに送信できます。サンプルファイル送信の詳細については、サンプルの送信を参照してください。

ThreatSenseエンジンのパラメーターの設定

ThreatSenseは、いくつかの複雑な脅威検出方法から構成されるESET独自の技術ですこの技術は事前対応型なので、新しいウイルスが広がる初期の段階でも保護することができます。この技術では、システムのセキュリティを大幅に強化するために連携して動作するさまざまな方法(コード分析、コードエミュレーション、汎用シグネチャなど)の組み合わせが使用されます。スキャンエンジンは、複数のデータストリームを同時に検査して、最大限の効率および検出率を確保することができます。またThreatSense技術によってルートキットを的確に防止することもできます。またThreatSense技術によってルートキットを的確に防止することもできます。

ThreatSense技術の設定オプションを使用すると、ユーザーはさまざまな検査パラメータを指定することができます。

- 検査するファイルの種類および拡張子
- さまざまな検出方法の組み合わせ
- 駆除のレベルなど

アプリケーション環境設定でThreatSense設定を変更できます(cmd+,を使用して開くかmacOSメニューバーのESET Cyber Securityをクリックして、**環境設定**[設定]を選択)。セキュリティシナリオごとに異なる設定が必要になることがあります。これを念頭に、ThreatSenseは、次の保護モジュールについて個々に設定することができます。

- リアルタイムファイルシステム保護
- マルウェア検査
- Webアクセス保護
- 電子メールクライアント保護

ThreatSenseパラメータは機能ごとに固有の最適化がされているので、パラメータを変更すると、システムの動作に大きく影響することがあります。たとえば、常に圧縮された実行形式を検査するように設定を変更したり、リアルタイムファイルシステム保護機能でアドバンスドヒューリスティックを有効にしたりすると、システムの処理速度が低下することがあります。コンピューターの検査を除く全ての機能についてThreatSenseの既定のパラメーターを変更しないことをお勧めします。

検査オプション

検査オプションは、次の保護モジュールのアプリケーション環境設定で設定できます。リアルタイムファイルシステム保護、マルウェア検査Webアクセス保護、電子メールクライアント保護。保護モジュールごとに、システム検査中に使用する方法を選択できます。使用可能なオプションは

- **ヒューリスティック** – ヒューリスティックは、プログラムの(悪意のある)活動を解析するアルゴリズムを使用します。ヒューリスティック検出の主な利点は、以前に存在していなかった新しい悪意のあるソフトウェアを検出できることです。
- **アドバンスドヒューリスティック** – アドバンスドヒューリスティックは、高級プログラミング言語で作成されたコンピュータワームやトロイの木馬の検出に最適の独自のESETに開発されたヒューリスティックアルゴリズムで構成されます。アドバンスドヒューリスティックによって、プログラムの検出能力が大幅に向上します。
- **スマート最適化** – 有効にすると、スマート最適化によって、最も効率的な検査レベルが提供され、同時に最高の検査速度を維持します。多様な保護モジュールがインテリジェントに検査し、特定のファイルタイプにさまざまな検査方法を適用します。

駆除レベル

駆除レベルは、次の保護モジュールのアプリケーション環境設定で設定できます。リアルタイムファイルシステム保護、マルウェア検査Webアクセス保護、電子メールクライアント保護。感染ファイルの駆除方法は、個別のレベルで決まります。使用できる駆除には次のレベルがあります。

- **駆除なし** – 感染しているファイルが自動的に駆除されることはありません。警告ウィンドウが表示され、アクションを選択することができます。
- **標準駆除** – 感染ファイルは自動的に駆除または削除されます。適切なアクションを自動的に選択できなかった場合は、ユーザーがその後のアクションを選択することができます。事前定義されたアクションを完了できない場合にも、フォローアップアクションが表示されます。
- **厳密な駆除** – 全ての感染ファイルが駆除または削除されます(アーカイブも対象)。ただし、シ

ステムファイルは除きます。ファイルを駆除できない場合は、通知が表示され、実行するアクションのタイプを選択する必要があります。

- **完全な駆除** – このモードでは、すべての感染したファイルが自動的に駆除または削除されます。
- **削除** - すべての感染したファイルを削除します。

アーカイブ検査
標準的な駆除モードで、アーカイブファイル全体が削除されるのは、アーカイブ内の全てのファイルが感染している場合のみです。アーカイブに問題がないファイルと感染したファイルが含まれる場合は、削除されません。厳密な駆除モードでは、感染しているアーカイブファイルが検出された場合、感染していないファイルがあっても、アーカイブ全体が削除されます。

除外

拡張子は、ファイル名の一部であり、ピリオドで区切られています。拡張子は、ファイルのタイプとコンテンツを定義します。これらの保護モジュールのアプリケーション環境設定で、検査から除外するファイルのタイプを定義できます。

- リアルタイム検査
- マルウェア検査
- Webアクセス保護
- 電子メールクライアント保護

既定では、拡張子に関係なく、全てのファイルが検査されます。検査から除外するファイルの一覧に任意の拡張子を追加できます。プラス＋およびマイナス－ボタンを使用することで、特定の拡張子の検査を有効にしたり禁止したりできます。

特定のファイルタイプを検査するとプログラムが正しく稼動しなくなる場合のように、場合によっては検査からファイルを除外する必要があります。たとえばlogcfgtmpファイルを除外することをお勧めします。ファイル拡張子を入力する場合の正しい書式は次のとおりです。

- log
- cfg
- tmp

アップデート

最大レベルのセキュリティを維持するためにはESET Cyber Securityを定期的にアップデートする必要があります。アップデート機能では、最新の検出エンジンのダウンロードにより、プログラムを常に最新の状態に保つことができます。

メインメニューの[**アップデート**]をクリックして、前回成功したアップデートの日時、アップデートが必要かどうかなどESET Cyber Securityの現在のアップデートの状態を確認します。新しいアップデートのチェックを開始するには、[**アップデートの確認**]ボタンをクリックします。製品のアップデートが利用可能な場合は、現在のバージョンと利用可能なバージョンに関する情報が、アップデートサイズとリリース日とともに表示されます。**今すぐアップデート**または**再起動後にアップデート**を選択できます。

各製品バージョンの詳細を表示するには、**変更ログを参照してください**リンクをクリックします。

ESET Cyber Securityの新バージョンへの更新

保護の効果を最大限にするためESET Cyber Securityの最新ビルドを使用することが重要です。常に最新バージョンを使用していることを保証するために、**製品の自動アップデート**をオンにすることをお勧めします(メインアプリケーションメニュー > **保護 > コンピューター**)。

ツール

[**ツール**]メニューには、プログラム管理を容易にし、また上級ユーザー向けの追加オプションを備えたモジュールが用意されています。このメニューには、次のツールが含まれています。

- ログファイル
- 隔離

ログファイル

ログファイルには、発生したすべての重要なプログラムイベントに関する情報が格納され、検出されたウイルスの概要が表示されます。ログは、システムの分析、脅威の検出、およびトラブルシューティングで重要なツールとして使用されます。ログへの記録はバックグラウンドでアクティブに実行され、ユーザーの操作を必要としません。情報は、ログの詳細レベルに関する現在の設定に基づいて記録されますESET Cyber Security環境から直接、テキストメッセージとログを表示し、ログをアーカイブすることができます。

ログファイルにアクセスするにはESET Cyber Securityのメインメニューで[**ツール**][**ログファイル**]の順にクリックします。ウィンドウの右上にある[ログ]ドロップダウンメニューを使用して、目的のログの種類を選択します。使用可能なログは次のとおりです。

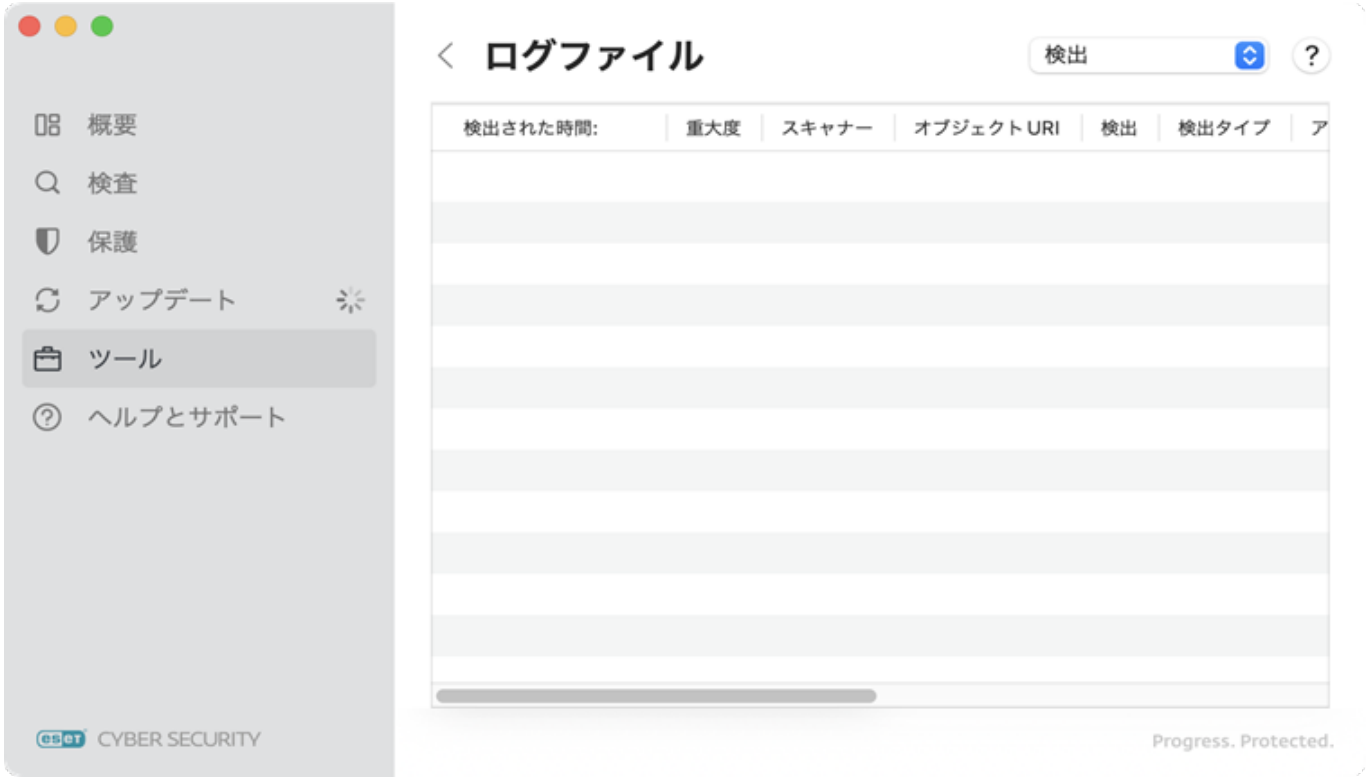
• **検出** – 侵入の検出に関するイベントの情報。

• **コンピューターの検査** – このログには、完了した全ての検査結果が表示されます。エントリーをダブルクリックすると、コンピューターの検査結果の詳細がそれぞれ表示されます。

• **イベント** – システム管理者およびユーザーが問題を解決できます。イベントログにはESET Cyber Securityによって実行された全ての重要なアクションが記録されます。

• **フィルタリングされたWebサイト** – Webアクセス保護によってブロックされたWebサイトの一覧が表示されます。. これらのログでは、特定のWebサイトへの接続を開いた時間URLステータスIPアドレス、ユーザー、およびアプリケーションを確認できます。

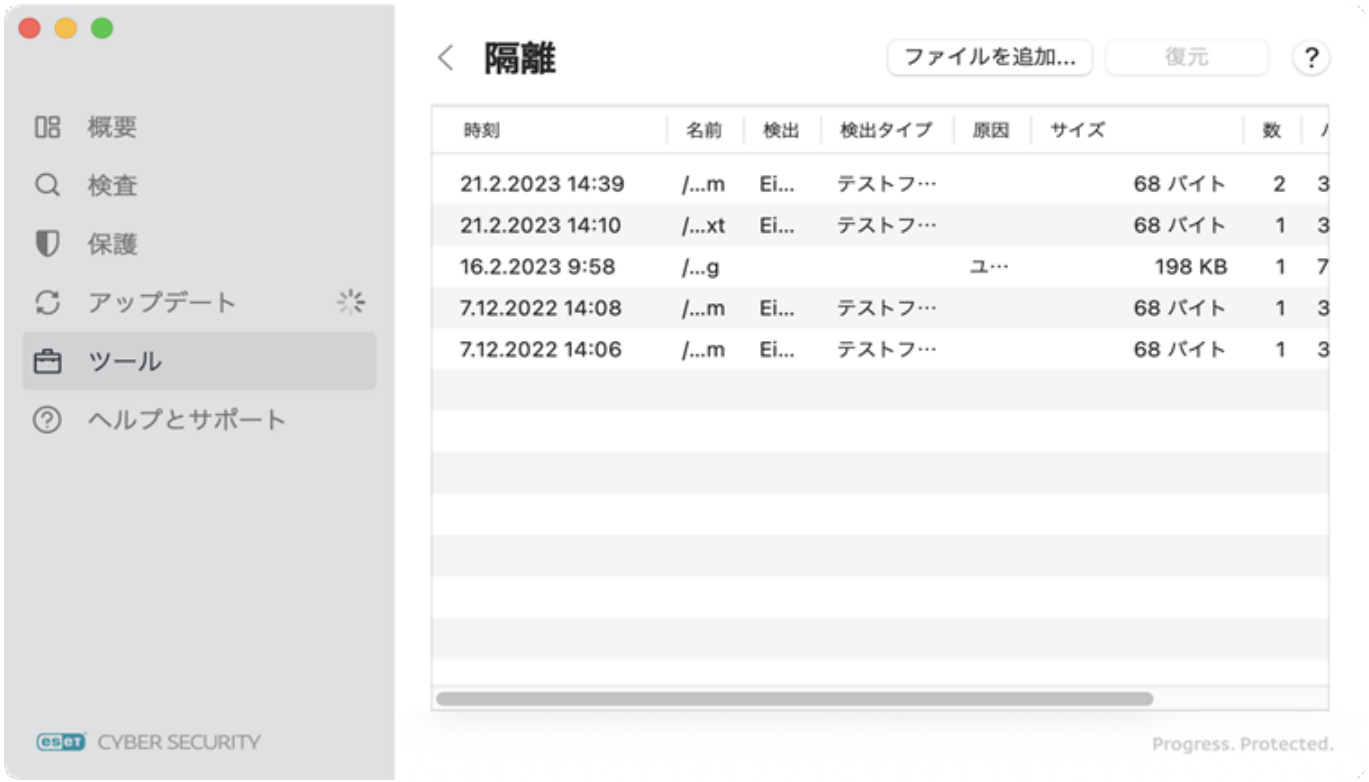
• **送信されたファイル** – 分析に送信されたサンプルのレコードが含まれます。



隔離

隔離の主な役割は、感染ファイルを安全に保存することです。ファイルを駆除できない場合、ファイルの削除が安全でないまたは推奨されない場合、あるいはESET Cyber Securityで誤って検出された場合、ファイルを隔離する必要があります。

隔離フォルダーに保存されているファイルは、隔離の日時、感染ファイルの元の場所のパス、ファイルサイズ(バイト単位)、理由(″ユーザーによって追加されました″など)、およびウイルスの数(複数のマルウェアが紛れ込んだアーカイブの場合など)が表示されるテーブルで参照することができます。隔離されたファイルが格納された隔離フォルダー(*/Library/Application Support/Eset/security/cache/quarantine*)はESET Cyber Securityの削除後もシステムに残ります。隔離されたファイルは暗号化された安全な形式で格納されておりESET Cyber Securityのインストール後に再度復元できます。



ファイルを隔離

ESET Cyber Securityは削除されたファイル(アラートウィンドウでこのオプションをキャンセルしていない場合)を自動的に隔離します。**ファイルの追加**をクリックすると、不審なファイルを手動で隔離します。ファイルまたはフォルダーを手動でドラッグアンドドロップするには、ファイルまたはフォルダーをクリックし、マウスボタンを押しながらマウスポインターをマークした箇所に移動して、ボタンを放します。

隔離フォルダーからの復元

隔離されたファイルを選択し、**復元**をクリックして、元の場所に復元します。この機能は、**隔離**ウィンドウで特定のファイルをControlキーを押しながらクリック(または右クリック)し、**復元**をクリックした場合にも使用できます。コンテキストメニューには、**復元先**オプションもあります。このオプションを使用すると、削除された場所とは別の場所にファイルを復元できます。

隔離フォルダからのファイルの提出

プログラムによって検出されなかった疑わしいファイルを隔離した場合、またはファイルが(コードのヒューリスティック分析などによって)感染していると誤って評価されて隔離された場合は、そのファイルをESETのウイルスラボに送信してください。隔離フォルダからファイルを送信するにはControlキーを押しながらファイルをクリック(または右クリック)し、コンテキストメニューから**サンプルの送信**を選択します。サンプルファイル送信の詳細については、サンプルの送信を参照してください。

分析のためにサンプルを送信

メインのアプリケーションウィンドウで左側メニューの**検査**を選択し、矢印アイコンをクリックして、**サンプルの送信**オプションを表示します。

このオプションを使用すると、コンピューターで見つかった疑わしい動作のファイル、またはオンラインで見つかった疑わしいサイトを選択し、分析のためにESET Research Labに送信できます。

ESETにファイルを提出する前に
提出するサンプルは、次の基準を1つ以上満たしている必要があります。
• このサンプルがESET製品で検出されない
• サンプルが誤ってウイルスとして検出される
• サンプルが個人のファイルではない（ESETは（ESETでのマルウェア検査を希望する）個人のファイルをサンプルとして受け入れず、ESET Research Labはユーザーのためにオンデマンド検査を実行しません

送信をクリックして、分析用に送信するファイルを指定します。**分析のためにサンプルを提出**フォームで次の項目を入力します。

• **送信理由** – コンテキストメニューから選択します。

• **サンプル** – 送信したいファイルへのパスを指定するか、マークされたエリアにファイルをドラッグアンドドロップします。

• **連絡先** - 当社がファイルに関する詳細情報を必要とする場合に、お客様に連絡するための連絡先情報を提供します。[匿名で送信する]トグルを有効にすることで、電子メールの追加を省略できます

次へをクリックすると、最後の手順に進み、観察されたマルウェア感染の兆候や症状、ファイルの出所など、サンプルファイルに関する追加情報を入力します。補足情報をご提供いただくと、サンプルの特定および処理の際に役立ちます。

ESETから連絡することはありません
詳しい情報が必要でない限り、ESETから連絡することはありません。毎日、何千ものファイルがサーバーに送られてくるので、すべての提出に返信することはできません。
サンプルが悪意のあるアプリケーションやWebサイトであることが判明すると、その後のESETアップデートファイルにその検出が追加されます。

エンドユーザーライセンス契約

発効日：2021年10月19日

重要:ダウンロード、インストール、コピー、または使用の前に、製品利用に関する下記契約条件を注意してお読みください。**本製品をダウンロード、インストール、コピー、または使用することにより、お客様はこれらの条件に対する同意を表明し、**プライバシーポリシー**に同意したことになります。

エンドユーザー使用許諾契約

本エンドユーザーライセンス契約（「本契約」）は、Einsteinova 24, 85101 Bratislava, Slovak Republicに所在し、ブラチスラバ第1地方裁判所の有限会社部門District Court Bratislava I. Section Sroにおいて掲載番号3586/B, 31333532として商業登記されているESET, spol. s r. o.（ESETまたは「供給者」）と、自然人または法人であるお客様（「お客様」または「エンドユーザー」）との間で締結され、お客様に本契約の第1条で定義する本ソフトウェアを使用する権利を付与するものです。本契約の第1条で定義する本ソフトウェアは、データ記憶媒体への格納、電子メールでの送付、インターネットからのダウンロード、供給者のサーバーからのダウンロード、または後述の条件および状況下におけるその他の供給者からの取得が行えます。

本契約は購入に関する契約ではなく、エンドユーザーの権利に関する合意事項を定めるものです。供給

者は、本ソフトウェアのコピー、これが商業包装にて供給される物理的媒体、および本契約に基づきエンドユーザーが権利を付与される本ソフトウェアのすべてのコピーの、所有者であり続けます。

本ソフトウェアのインストール時、ダウンロード時、コピー時または使用時に、[同意します]オプションをクリックすることにより、本契約の条件に明示的に同意し、プライバシーポリシーを承諾するものとします。本契約の規定またはプライバシーポリシーに同意しない場合は、直ちに[同意しない]オプションをクリックし、インストールまたはダウンロードを取り消すか、本ソフトウェア、インストールメディア、付属ドキュメント、および購入時の領収書を破棄するかESETまたは本ソフトウェアの供給者にそれを返却してください。

お客様は、本ソフトウェアを使用することにより、お客様が本契約を読了かつ理解し、本契約条項による拘束に同意したことになります。

1.**ソフトウェア。**(i)本契約およびすべてのコンポーネントに付属するコンピュータープログラム(ii)データ媒体、電子メール、またはインターネット経由でのダウンロードで提供される本ソフトウェアのオブジェクトコードの形式を含む、本契約で提供されるディスクCD-ROMDVD電子メール、添付ファイル、その他の媒体のすべての内容(iii)本ソフトウェアに関連する書面の説明資料、その他の文書、特に本ソフトウェア、その仕様のすべての説明、 本ソフトウェアの属性または動作の説明、本ソフトウェアが使用される動作環境の説明、本ソフトウェアの使用またはインストール手順、本ソフトウェアの使用方法の説明(「ドキュメント)(iv)本契約の第3条に従い供給者からお客様にライセンス供与された本ソフトウェアのコピー、本ソフトウェアに不具合があった場合のパッチ、本ソフトウェアへの追加機能、本ソフトウェアの拡張機能、本ソフトウェアの修正バージョン、ソフトウェアコンポーネントのアップデート(該当する場合)を意味します。本ソフトウェアは実行可能なオブジェクトコードの形態でのみ提供されるものとします。

2.**インストール、コンピューター、およびライセンスキー**。データキャリアで供給、電子メールで送信、インターネットからダウンロード、供給者のサーバーからダウンロード、または他のソースから取得されたソフトウェアにはインストールが必要です。お客様は、本ソフトウェアを正しく設定されたコンピューターにインストールし、少なくともドキュメントで規定された要件に準拠する必要があります。インストール方法はドキュメントで説明されています。本ソフトウェアをインストールするコンピューターに、本ソフトウェアに悪影響を及ぼす可能性があるコンピュータープログラムやハードウェアをインストールすることはできません。コンピューターとは、本ソフトウェアがインストールまたは使用される、パーソナルコンピューター、ノートブック、ワークステーション、パームトップコンピューター、スマートフォン、ハンドヘルド電子機器、または本ソフトウェアの対象として設計されている他の電子機器を含む(ただしこれらに限定されない)を意味します。ライセンスキーとは、本契約に準拠して、本ソフトウェア、特定のバージョン、またはライセンス条項の拡張の法的な使用を許可するために、エンドユーザーに提供される一意の連続する記号、文字、数字、または特殊記号を意味します。

3.**ライセンス**。お客様が本契約に同意しており、ライセンス料を支払い期日までに支払い、本契約に定められているすべての契約条項に従うことを前提として、供給者はお客様に対し、以下の権利を付与します（以下「ライセンス」とします）。

a) **インストールおよび使用。**お客様には、コンピューターのハードディスクまたはその他のデータ永久記憶媒体にデータを格納するために本ソフトウェアをインストールし、コンピューターシステムのメモリへ本ソフトウェアをインストールおよび格納し、コンピューターシステム上で本ソフトウェアを実装、格納および表示する、非独占的かつ譲渡禁止の権利が付与されます。

b) **ライセンス数の規定。**本ソフトウェアを使用する権利は、エンドユーザー数によって制限されます。1人のエンドユーザーとは(i)本ソフトウェアがインストールされている1台のコンピューターを意味しますii)ライセンス数がメールボックスを単位として決定される場合、エンドユーザーはメールユーザーエージェント（以下MUAとします）を介して電子メールを受信する1人のコンピューターユーザーを意味します。電子メールがMUAで受信後、複数のユーザーに自動的に配信される場合、エンドユーザーの数は、その電子メールが配信されるユーザーの実際の数によって決まります。メールサーバがメールゲートの役割を果たす場合、エンドユーザーの数は、そのゲートがサービスを提供するメールサーバユーザーの数と同じになります。(エイリアスなどを使用して)1人のユーザーに不特定多数の電子メールア

ドレスが送信され、それらが受け付けられる場合、クライアント側で多数のユーザーにそのメールが自動的に配信されるのでなければ、ライセンスは1台のコンピューターに必要です。同じライセンスは、同時に複数のコンピューターで使用できません。エンドユーザーは、供給者によって付与されたライセンス数に基づく制限に従い、本ソフトウェアを使用する権限が与えられている範囲においてのみ、本ソフトウェアのライセンスキーを入力する資格があります。このライセンスキーは機密情報であると見なされます。本契約または供給者によって許可されている場合を除き、お客様はライセンスを第三者と共有すること、または第三者がライセンスを使用することを許可することが禁止されています。ライセンスキーが危険にさらされた場合は、速やかに供給者に通知してください。

c) **Home/Business Edition**本ソフトウェアのHome Editionバージョンは、家庭および家族での利用に限定された個人または非商業環境でのみ使用されるものとします。本ソフトウェアを商業環境、またはメールサーバー、メール中継、メールゲートウェイ、インターネットゲートウェイで使用する場合は、本ソフトウェアのBusiness Editionバージョンを入手する必要があります。

d) **ライセンス契約の期間。**お客様は、本ソフトウェアを期限付きで使用する権利があります。

e) **OEMソフトウェア。**OEMに分類されたソフトウェアの使用は、それがプリインストールされていたコンピューターに制限されます。別のコンピューターにインストールすることはできません。

f) **NFRまたは試用ソフトウェア。**再販不可品NFRまたは試用版に分類されるソフトウェアは、対価を求めて譲渡することはできず、ソフトウェア機能のデモまたはテスト目的のみで使用されるものとします。

g) **ライセンスの契約解除。**ライセンス契約は，その期間の満了により契約が自動的に解除されます。供給者は、お客様が本契約のいずれかの条項に違反したときは、供給者が持つ他の権利および法的救済手段に影響を与えることなく、本契約を解約することができます。本ライセンスを取り消す場合、お客様は、本ソフトウェアおよびバックアップコピーを直ちにすべて削除、破棄するか、自費でESETまたはソフトウェアの入手元にそれを返却する必要があります。ライセンスの終了時には、供給者は、エンドユーザーが、供給者のサーバーまたはサードパーティのサーバーに接続する必要がある本ソフトウェアの機能を使用する権利を取り消す権利があるものとします。

4.**データ収集機能およびインターネット接続要件。**本ソフトウェアの正常な動作には、インターネット接続が必要であり、プライバシーポリシーに従い、定期的に供給者のサーバーまたは第三者のサーバーおよび該当するデータ収集に定期的に接続する必要があります。インターネットへの接続およびデータ収集は、次のソフトウェア機能で必要です。

a) **ソフトウェアのアップデート。**供給者には、本ソフトウェアのアップデートまたはアップグレード(「アップデート」)を適時発行する権利がありますが、アップデートを提供する義務はありません。この機能は、ソフトウェアの標準の設定から有効にできます。エンドユーザーがアップデートの自動インストールを無効にしていないかぎり、アップデートは自動的にインストールされます。アップデートを提供するために、プライバシーポリシーに準拠し、本ソフトウェアがインストールされているコンピューターまたはプラットフォームに関する情報を含む、ライセンスの正当性を検証する必要があります。

アップデートの提供には、サービス終了ポリシ(EOLポリシー」)が適用される場合があります。https://go.eset.com/eolをご覧ください。本ソフトウェアまたは本ソフトウェアの機能がEOLポリシーで定義されているサービス終了日に達した後は、アップデートが提供されません。

b) **供給者への侵入物および情報の転送**。本ソフトウェアには、コンピューターウイルスおよびその他の悪意のあるプログラム、ファイルURLIPパケット、イーサネットフレームなどの不審、問題、潜在的に望ましくない、または潜在的に危険なオブジェクト(「侵入」)のサンプルを収集する機能が含まれ、インストール処理、コンピューター、ソフトウェアがインストールされているプラットフォームの情報、本ソフトウェアの操作および機能の情報(「情報」)を含む(ただしこれらに限定されない)、これらのオブジェクトを供給者に送信します。情報および侵入には、エンドユーザーまたは本ソフトウェアがインストールされているコンピューターの他のユーザーのデータ(ランダムまたは誤って取得された個人データを含む)、関連付けられたメタデータによる侵入の影響を受けるファイルが含まれる場合があります。

情報および侵入は次のソフトウェア機能によって収集される場合があります。

i.LiveGridレピュテーションシステム機能には、侵入に関する単方向ハッシュの収集と供給者への送信が含まれます。この機能は、ソフトウェアの標準設定で有効です。

ii.LiveGridフィードバックシステム機能には、侵入を収集し、関連付けられたメタデータおよび情報とともに供給者に送信する機能が含まれます。この機能は、本ソフトウェアのインストール処理中に、エンドユーザーがアクティブ化することができます。

供給者は、侵入の分析と研究、ソフトウェアの改良、およびライセンスの正当性の検証の目的でのみ、受け取った情報および侵入を使用するものとし、適切な対策を講じて、受け取った侵入および情報が安全であることを保証するものとします。本機能をアクティブ化することで、プライバシーポリシーの規定に従い、関連する法規制に準拠して、侵入および情報は供給者によって収集および処理される場合があります。この機能はいつでも無効にすることができます。

本契約の目的のために、プライバシーポリシーに従い、供給者がお客様を特定できるようにするデータを収集、処理、および保存する必要があります。お客様は、供給者が独自の手段によって、お客様が本契約の規定に従って本ソフトウェアを使用しているかどうかを確認することに同意します。お客様は、本契約の目的でのみ、本ソフトウェアと供給者のコンピューターシステムまたは供給者の販売およびサポートネットワークの一部としての供給者のビジネスパートナーのコンピューターシステムとの間の通信中に、お客様のデータを転送し、本ソフトウェアの機能および本ソフトウェアの使用許可を保証し、供給者の権利を守る必要があることを承諾します。

本契約の締結後、供給者および供給者の販売およびサポートネットワークの一部としての供給者のビジネスパートナーは、請求目的、本契約の履行、およびお客様のコンピューターでの通知の送信のために、お客様を特定できる基本データを転送、処理、および保管する権利を有するものとします。

データ主体としてのプライバシー、個人データ保護、およびお客様の権利の詳細については、供給者のWebサイトまたはインストール処理で直接アクセスできるプライバシーポリシーを参照してください。お客様は、ソフトウェアのヘルプセクションからアクセスすることもできます。

5.**エンドユーザの権利行使**。お客様は、エンドユーザーの権利を、直接またはお客様の従業員を通じて行使する必要があります。お客様は、自らの活動を確実なものとするためにのみ、およびお客様がライセンスを取得したコンピューターシステムを保護するためにのみ、本ソフトウェアを使用できます。

6.**権利の制限。**お客様は本ソフトウェアのコピー、配布、部品の分離、または派生バージョンの作成を行ってはなりません。本ソフトウェアの使用時には、下記の制限事項に従う必要があります。

a) お客様は、データの永久記憶用媒体上に本ソフトウェアのコピーを1つ、バックアップコピーとして作成できます。ただし、この保管用のバックアップコピーは、他のいかなるコンピュータにもインストールしたり、または使用したりすることができません。これ以外に本ソフトウェアのコピーを作成することは、本契約に対する違反となります。

b) 本契約に規定されている以外のいかなる態様でも、本ソフトウェアまたは本ソフトウェアのコピーの使用、改変、複製、または使用権の譲渡を行ってはなりません。

c) 本ソフトウェアの売却、サブライセンス付与、他人への賃貸もしくは他人からの賃借、借用、または商業サービスの提供目的での本ソフトウェアの使用は禁じられています。

d) 本ソフトウェアのリバースエンジニアリング、逆コンパイル、またはソフトウェアの逆アセンブルを行ったり、ソースコードを取得しようとしたりしてはなりません。ただし、そのような制限を設けることが法律によって明示的に禁止されている範囲内においては、この限りではありません。

e) お客様は、著作権法およびその他の知的財産権から生じる、適用可能な制限など、本ソフトウェアを使用する際の法律におけるすべての適用可能な法的規制に従う態様においてのみ、本ソフトウェアを使用できます。

f) お客様は、本ソフトウェアおよびその機能を、他のエンドユーザーがそれらのサービスにアクセスする可能性を制限しない方法でのみ使用することに同意するものとします。供給者は、可能な限り多くのエンドユーザーがサービスを利用できるようにするために、個別のエンドユーザーに提供されるサービスの範囲を制限する権利を留保します。サービスの範囲を制限することにより、本ソフトウェアのすべての機能を使用することもできなくなり、本ソフトウェアの特定の機能に関連する供給者のサーバー上またはサードパーティのサーバー上のデータおよび情報も削除されることとします。

g) お客様は、本契約の条項に反して、ライセンスキーの使用に関する活動、または何らかの形式での使用済みまたは未使用のライセンスキーの譲渡、不正複製、複製または生成されたライセンスキーの配布、あるいは供給者以外から入手したライセンスキーを使用したソフトウェアの利用など、本ソフトウェアの使用の資格がない個人にライセンスキーを提供する行為を実施しないことに同意します。

7.**著作権**。本ソフトウェア、および所有権や知的所有権を含む一切の権利は、ESETおよび / またはESETのライセンス供給者の財産です。これらは、国際条約の規定と本ソフトウェアが使用される国のその他のすべての準拠法によって保護されます。本ソフトウェアの構造、編成、およびコードは、ESETおよび / またはESETのライセンス供給者の重要な企業秘密であり機密情報です。お客様は、第6条(a)に当てはまる場合を除いて、本ソフトウェアをコピーすることはできません。本契約に基づき、お客様が作成するコピーはすべて、本ソフトウェア上に示されるものと同じ著作権表示および所有権表示を含んでいなければなりません。お客様がリバースエンジニアリング、逆コンパイル、逆アセンブルを行ったり、本契約の規定に違反する方法でソースコードを取得しようとした場合、それによって得られたいかなる情報も、それが発生した瞬間からすべて、本契約の違反に関連する供給者の権利にかかわらず、自動的にかつ取り消しできない形で供給者に譲渡され、供給者の所有であるとみなされます。

8.**権利の留保**。本ソフトウェアに対する権利は、本契約において本ソフトウェアのエンドユーザーとしてお客様に明示的に与えられた権利を除き、すべて供給者自身が留保します。

9.**複数言語対応バージョン、デュアルメディアソフトウェア、複数コピー**。本ソフトウェアが複数のプラットフォームまたは言語をサポートしているか、お客様が本ソフトウェアのコピーを複数入手した場合、お客様はライセンスを取得したバージョンのコンピューターシステム数でのみ本ソフトウェアを使用できます。使用していない本ソフトウェアのバージョンやコピーを、他者に売却、賃貸、賃借、サブライセンス付与、貸与、または譲渡することはできません。

10.**本契約の開始と解除。**本契約は、お客様が本契約に同意した日から有効となります。本契約は、お客様が本契約に同意した日から有効となります。お客様は、供給者またはそのビジネスパートナーから入手した本ソフトウェア、すべてのバックアップコピー、および関連するすべての資料を、永久的に削除、破棄、または自費で返却することにより、本契約を解除することができます。本ソフトウェアおよび本ソフトウェアの機能を使用するお客様の権利にはEOLポリシーが適用される場合があります。本ソフトウェアまたは本ソフトウェアの機能がEOLポリシーで定義されているサービス終了日に達した後は、本ソフトウェアを使用するお客様の権利が失効します。本契約の終了の態様に関係なく、第7条、第8条、第11条、第13条、第19条、および第21条の規定は、無期限に有効であり続けるものとします。

11.**エンドユーザーの表明**。お客様はエンドユーザーとして、明示または暗黙のいかなる種類の保証も伴わず、該当の法律によって許可される範囲において、本ソフトウェアが「現状有姿」のまま提供されていることを認めるものとします。供給者、そのライセンス供給者、関係者、および著作権保有者のいずれも、本ソフトウェアの特定の目的に対する商品性または適合性、および第三者の特許、著作権、商標、またはその他の権利に対する侵害の不存在について、明示または黙示を問わず、一切の表明または保証を行いません。供給者もその他の関係者も、本ソフトウェアに含まれている機能がお客様の要求に沿うこと、または本ソフトウェアが円滑で問題なく動作するということの保証を行いません。お客様は、意図する結果に到達するための本ソフトウェアの選択、および本ソフトウェアのインストール、使用、および本ソフトウェアで達成される結果について、完全に責任とリスクを負います。

12.**さらなる義務の否定**。本契約で具体的に列挙される義務以外に、本契約が供給者およびそのライセンサーに対して課す義務はありません。

13.**責任の制限**。準拠法によって許可される最大限の範囲において、いかなる場合も、供給者、その被雇

用者、ライセンス供給者は、どのような態様で発生したものであろうと、契約、違法行為、怠慢、または責任の発生を定めるその他の事実のいずれに起因するものであるかを問わず、本ソフトウェアのインストール、本ソフトウェアの使用、または本ソフトウェアが使用できないことにより発生した、利益、収益、または売上の損失、データの喪失、補用品またはサービスの購入にかかった費用、物的損害、人的損害、事業の中断、企業情報の喪失、特別損害、直接損害、間接損害、偶発的損害、経済的損害、補填損害、懲罰的損害、特別または派生的損害に対し、一切責任を負わないものとします。これは、たとえ供給者、そのライセンス供給者、または関係者がそのような損害の可能性について通知を受けていた場合であっても同様です。一部の国および法律では、免責を認めず、しかし限定された範囲の責任を負うことは許可しています。その場合、供給者、その被雇用者、ライセンス供給者、または関係者の責任は、お客様がライセンスの対価として支払った金額を限度とします。

14. 本契約に含まれるものは何も、それに反する場合であっても、消費者として取引するすべての当事者の法的権利を損なうものではありません。

15.**テクニカルサポート**。テクニカルサポートは、ESETまたはESETの依頼を受けた第三者の独自の判断により提供され、いかなる種類の保証も表明も伴わないものとします。本ソフトウェアまたは本ソフトウェアの機能がEOLポリシーで定義されているサービス終了日に達した後は、テクニカルサポートが提供されません。エンドユーザーは、テクニカルサポートの提供の前に、存在するすべてのデータ、ソフトウェア、プログラム機能をバックアップする必要があります。ESETおよび / またはESETの依頼を受けた第三者は、テクニカルサポートの提供によりお客様に生じたデータ、資産、ソフトウェアまたはハードウェアの損害または損失、もしくは利益の喪失について、いかなる責任も負いません。ESETおよび / またはESETの依頼を受けた第三者は、問題をテクニカルサポートで解決できないと判断する権利があります。ESETは、独自の判断により、テクニカルサポートの提供を拒否、中断、終了する権利があります。ライセンス情報、情報、およびプライバシーポリシーに準拠した他のデータは、技術サポートを提供するために必要になる場合があります。

16.**ライセンスの譲渡**。本契約の条件に違反しないかぎり、あるコンピューターにインストールされていた本ソフトウェアを別のコンピューターシステムにインストールすることができます。エンドユーザーは、本契約の条件に違反しない場合のみ、供給者の同意の元、本契約から派生するライセンスおよびすべての権利を、別のエンドユーザーに永久に譲渡する権利があります。その場合、(i) 元のエンドユーザーは、ソフトウェアのコピーを保持しておらず、(ii) 元のエンドユーザーから新しいエンドユーザーへ直接権利が譲渡され、(iii) 新しいエンドユーザーが元のエンドユーザーに課せられた本契約に基づくすべての権利および義務を負い、(iv) 元のエンドユーザーが新しいエンドユーザーに、第17条で規定するソフトウェアが正規のものであることを証明するドキュメントを提供するものとします。

17.**正規ソフトウェアの証明。**エンドユーザーのソフトウェアの使用資格は、次のいずれかの方法で証明できます。(i)供給者または供給者が指定した第三者が発行するライセンス証明書、(ii)締結されている場合、書面によるライセンス契約、(iii) アップデートを有効にするライセンスの詳細（ユーザ名およびパスワード）が記載された供給者に送信された電子メールの提出。ライセンス情報およびプライバシーポリシーに準拠したエンドユーザー識別データは、ソフトウェアの純正を検証するために必要になる場合があります。

18.**公共団体および米国政府に対するライセンス**。米国政府を含む公共団体に対する本ソフトウェアのライセンスは、本契約に明記しているライセンス権利および制限に基づいて提供されます。

19.**輸出管理規制**

a)お客様は、直接的または間接的に、ESETまたはESETの持ち株会社、ESETの子会社、持ち株会社の子会社、持ち株会社が管理する事業体による次のような輸出貿易管理法の違反または輸出貿易管理法の下で否定的な結果につながる一切の個人に対して本ソフトウェアを輸出、再輸出、移転、または提供せず、そのような方法でソフトウェアを使用せず、そのような行為に関与したりしないものとします。

i. 米国、シンガポール、英国、欧州連合またはその加盟国、本契約の義務が履行される国、あるいはESETまたはその関連会社が登録または事業を行う国の政府、州、規制当局が発行または採用した、商品、ソフトウェア、技術、サービスの輸出、再輸出、または移転を統制、制限、またはライセンス要件

を課すすべての法律。

ii. 米国、シンガポール、英国、欧州連合またはその加盟国、本契約の義務が履行される国、あるいはESETまたはその関連会社が登録または事業を行う国の政府、州、規制当局が課した経済、金融、貿易、制裁、制限、禁止、輸出入禁止、資金または資産の移転の禁止、サービス提供の禁止、あるいは同等の対策。

(上記第i項および第ii項で参照される法律、ならびに「貿易管理法」)。

b) ESETは、次の場合において、本契約の義務を即時停止または解除する権利を有するものとします。

i.ESETが、合理的な意見において、ユーザーが本契約の第19 a)条の条項に違反したか違反する可能性が高いと判断した

ii. エンドユーザーまたは本ソフトウェアに輸出貿易管理法が適用され、その結果として ESETが、合理的な意見において、本契約の義務の継続的な履行によって ESETまたはその関連会社が輸出貿易管理法に違反するか、輸出貿易管理法の下で否定的な影響を受ける可能性があると判断した

c) いずれの当事者も、適用される輸出貿易管理法に準拠しないか、輸出貿易管理法の下で罰則を受けるか、禁止される行為または不作為(あるいは行為または不作為に同意すること)を勧誘または義務付けられるように、本契約のいずれの条項も意図せず、何もそのように解釈または理解されない

20.**通知**。すべての通知、ならびに本ソフトウェアおよびドキュメントの返却は、本契約の第22条に従い、本契約、プライバシーポリシー EOLポリシー、ドキュメントの変更をお客様に通知するESETの権利を損なうことなく ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic宛てに送付する必要があります ESETは、電子メールや、本ソフトウェア経由でのアプリ内通知を送信したり Webサイトにコミュニケーションを投稿したりする場合があります。お客様は、規約、特別な規約、プライバシーポリシーの変更、契約の提案/承諾、またはキャンペーンへの招待、通知または他の法的な通知に関するコミュニケーションを含め、電子的な形式でESETから法的な通知を受信することに同意します。適用される法律で特に別のコミュニケーションの形態が義務付けられている場合を除き、かかる電子的なコミュニケーションは書面を受け取った場合と同義に見なされるものとします。

21.**準拠法**。本契約は、スロバキア共和国の法律に準拠し、これに従って解釈されるものとします。エンドユーザーおよび供給者は、準拠法および国際物品売買契約に関する国際連合条約の矛盾する規定については、適用されないことに同意するものとします。お客様は、本契約に関するいかなるクレームもしくは供給者との紛争、または本ソフトウェアをお客様が使用することによるいかなる紛争またはクレームも、ブラチスラバ第1地方裁判所で解決し、さらに、ブラチスラバ第1地方裁判所での管轄権の行使に同意し、明示的にこれを承諾するものとします。

22.**一般条項**。本契約の条項のいずれかが無効または履行不能である場合、これが本契約のその他の条項の有効性に影響を及ぼすことはないものとします。これらその他の条項は、本契約に定める条件に基づき、引き続き有効かつ履行可能であるものとします。本契約は英語で締結されました。便宜上またはその他の目的で、本契約書の翻訳が用意されている場合、または本契約の翻訳版の間で不一致がある場合には、英語版が優先されるものとします。

ESETは、(i) 本ソフトウェアまたはESETの事業の方法に関する変更を反映する (ii) 法律、規制、セキュリティの理由から (iii) 悪用または被害を防止するため、関連するドキュメントを更新することで、いつでも、本ソフトウェアを変更し、本契約、付録、補遺、プライバシーポリシー EOLポリシー、ドキュメントまたはその一部を改訂する権利を留保します。これらの条項の改訂は、電子メール、アプリ内通知、または他の電子的な手段で通知されます。お客様が本契約の変更の提案に同意しない場合は、変更の通知を受領してから30日以内にアカウントまたは影響を受ける購入済みのサービスを解約できます。この期限内に本契約を解約しない場合は、提案された変更が承認されたと見なされ、変更の通知を受け取った日時点でお客様側で変更が有効になります。

本契約は、本ソフトウェアに関するお客様および供給者間の合意事項をすべて網羅しており、本ソフト

ウェアに関する従前のいかなる表明、議論、約束、情報交換、または広告にも取って代わります。

EULAID: EULA-PRODUCT-LG; 3537.0

プライバシーポリシー

個人データの保護は、データ管理者としてのESET, spol. s r. o. (登録事業所所在地: Einsteinova 24, 851 01 Bratislava, Slovak Republic商業登記: ブラチスラバ第1地方裁判所、有限会社部門、登録番号3586/B事業登記番号: 31333532) (ESETまたは「当社」)にとって特に重要ですESETは、EU一般データ保護規制(GDPR)の下で法的に規定された透明性要件に準拠します。この目標を達成するためにESETは、データ主体としてのお客様(「エンドユーザー」または「お客様」)に次の個人データ保護事項を通知する目的でのみ、本プライバシーポリシーを発行しています。

- 個人データの処理の法的根拠
- データ共有と機密保持
- データセキュリティ
- データ主体としての権利
- 個人データの処理
- 連絡先情報。

個人データの処理

製品に実装されたESETが提供するサービスは、 エンドユーザーライセンス契約の条項に従って提供されますが、項目によっては特定の注意が必要になる場合がありますESETは、サービスの提供に関連するデータ収集の詳細について、お客様に説明しますESETは、エンドユーザーライセンス契約および製品 ドキュメントをご覧ください。すべてを機能させるためにESETは次の情報を収集する必要があります。

- 製品がインストールされているプラットフォームを含むインストール処理とコンピューターに関する情報、およびオペレーティングシステム、ハードウェア情報、インストールIDライセンスIDIPアドレスMACアドレス、製品の構成設定といった製品の動作と機能に関する情報を含むアップデートおよび統計情報。
- ESET LiveGrid®レピュテーションシステムの一部として侵入に関連する単方向ハッシュ。これは、検査済みファイルをクラウドのホワイトリストおよびブラックリスト項目のデータベースと比較し、ESETマルウェア対策ソリューションの効率化を図ります。
- ESET LiveGrid®フィードバックシステムの一部として世界から収集した不審なサンプルおよびメタデータ。これにようESETは、エンドユーザーのニーズに迅速に対応し、最新の脅威に反応し続けることができますESETはお客様がESETに送信する次の情報を必要としています
    - ウイルスおよび他の悪意のあるプログラム、ならびにお客様によって迷惑メールとして報告されたか、製品によって警告された実行ファイル、電子メールメッセージなどの不審であるか、問題があるか、望ましくない可能性があるか、危険の可能性があるオブジェクトの潜在的なサンプルといった侵入情報
    - デバイスの種類、ベンダー、モデル、名前などのローカルネットワークのデバイスに関する情報
    - IPアドレスおよび地理情報IPパケットURLおよびイーサネットフレームなどのインターネットの使用に関する情報
    - 含まれるクラッシュダンプファイルと情報

当社は、この範囲外でデータを収集する意志はありませんが、場合によってはそれが防止できないことがあります。誤って収集されたデータは、マルウェア自体に含まれる場合があります。当社は、本プライバシーポリシーで規定された目的において、そのようなデータを当社のシステムまたはプロセスに取り込む意図はありません。

- ライセンスIDなどのライセンス情報、および名前、姓、住所、電子メールアドレスなどの個人データは、課金、ライセンスの真正の検証、サービスの提供のために必要です。
- サポート要求に含まれる連絡先情報およびデータは、サポートのサービスで必要になる場合があります。選択した連絡方法に基づき、当社は、電子メールアドレス、電話番号、ライセンス情報、製品詳細、およびサポートケースの説明を収集する場合があります。サポートのサービスを進めるために、他の情報の提供を求められる場合があります。

データ共有と機密保持

ESETがお客様のデータを第三者と共有することはありません。ただしESETは、販売、サービス、およびサポートネットワークの一部として、関連会社またはパートナーを通して、世界中で事業を展開する企業ですESETが処理するライセンス、請求、テクニカルサポート情報は、サービスやサポートの提供といったエンドユーザーライセンス契約の履行の目的で、関連会社またはパートナーとの間で転送される場合があります。

基本的に、ESETは、欧州連合(EU)でデータを処理します。ただし、お客様の居住国(EU外での製品またはサービスの利用)またはお客様が選択するサービスによってはEU外の国にお客様データを転送しなければならない場合があります。たとえばESETは、クラウドコンピューティングに関連してサードパーティサービスを使用しています。このような場合ESETはサービスプロバイダーを厳選し、契約、技術、組織的な対策を導入して、適切なレベルのデータ保護を保証します。原則としてESETは、EUの標準契約条項と補足契約規制(必要な場合)に同意します。

英国やスイスなどのEU外の一部の国についてはEUが既に同等のデータ保護を決定しています。同等のデータ保護が規定されているため、このような国へのデータ転送には特別な認可または同意が必要ありません。

データの主体の権利

すべてのエンドユーザーの権利は重要ですESETは、すべてのエンドユーザ(EU加盟国およびEU非加盟国)が次の権利について保証されていることを通知します。データ主体の権利を行使するには、サポートフォームまたは電子メール(dpo@eset.sk)でお問い合わせください。本人確認目的で、次の情報をご提示ください。お名前、電子メールアドレス、製品認証キー(該当する場合)、お客様番号、会社名。生年月日などの他の個人データは送信しないでください。またESETは、お客様の依頼を処理し、本人確認を行うために、お客様の個人データを処理します。

同意を取り消す権利。同意のみに基づく処理の場合、同意を取り消す権利が適用されますESETがお客様の同意に基づいてお客様の個人データを処理する場合、お客様は、理由を提供せずに、いつでも同意を取り消す権利があります。同意の取り消しは将来に対してのみ有効であり、取り消し前に処理されたデータの合法性には影響しません。

異議を申し立てる権利。同意のみに基づく処理の場合、同意を取り消す権利が適用されますESETが合法的な利益を保護するために、お客様の個人データを処理する場合、データ主体としてのお客様は、いつでもESETが指名した合法的な利益および個人データの処理に対して異議を申し立てる権利があります。異議申し立ては将来に対してのみ有効であり、異議申し立て前に処理されたデータの合法性には影響しませんESETがダイレクトマーケティング目的で個人データを処理している場合、お客様の異議申し立ての理由を提出する必要はありません。これは、このようなダイレクトマーケティングに関連しているかぎり、プロファイリングにも該当します。他のすべての場合において、お客様は、ESETが個人データを処理する正当な利益に対する苦情について簡潔に通知することが求められます。

場合によっては、お客様が同意を取り消したにもかかわらずESETは、契約の履行など、別の法的根拠に基づいて個人データを引き続き処理する資格があります。

アクセスの権利。お客様は、データ主体として、いつでも無料で、ESETによって保存されたデータに関する情報を取得する権利があります。

修正する権利。ESETがお客様に関する誤った個人データを間違って処理した場合、お客様はこれを修正する権利があります。

消去する権利および処理を制限する権利。データ主体として、お客様は、個人データの削除または制限を要求する権利があります。お客様の同意を得た場合などESETがお客様の個人データを処理し、お客様がその同意を取り消し、それ以上の法的根拠(契約など)が存在しない場合ESETはただちにお客様の個人データを削除します。お客様の個人データは、保持期間の終了に指定された目的で必要とされなくなった時点ですみやかに削除されます。

ESETが直接マーケティングの目的でのみお客様の個人データを使用し、お客様が同意を取り消したか、根拠となるESETの合法的な利益に対して異議を申し立てた場合ESETは、未承諾の連絡を回避する目的でお客様の連絡先データを社内ブラックリストに追加する範囲で、お客様の個人データの処理を制限します。そうでない場合、お客様の個人データは削除されます。

ESETは、立法当局または監督当局によって発行された保持義務および期間が終了するまで、お客様のデータを保存することが義務付けられている場合があります。保持義務と期間は、スロバキアの法律によっても生じ得る場合があります。その後、該当するデータは日常的に削除されます。

データ移植性の権利。ESETは、データ主体としてのお客様に対してESETが処理する個人データをxls形式で提供いたします。

苦情を申し立てる権利。データ主体として、お客様は、いつでも監督当局に苦情を申し立てる権利を有しますESETはスロバキア法の規制に準拠し、欧州連合の一部としてデータ保護法によって拘束されます。該当するデータ監督当局は、スロバキア共和国個人データ保護局(Hraničná 12, 82007 Bratislava 27, Slovak Republic)です。

連絡先情報

データ主体として権利を行使する場合、またはご質問や懸念をお持ちの場合は、以下の宛先までご連絡ください。

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk