ESET Cyber Security Pro

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 Pro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 Pro

ESET Cyber Security Proは真の意味で統合されたコンピューターセキュリティへの新しいアプローチを示します。 最新バージョンのThreatSense®検査エンジンは電子メールクライアント保護、ファイアウォール、ペアレンタルコントロールを統合し、あなたのコンピューターの安全を維持する動作速度と精度を活用します。 その結果、攻撃や悪意のあるソフトウェアを常に警戒し、コンピュータを防御するインテリジェントシステムが開発されました。

ESET Cyber Security Proは最大の保護と最小のシステムフットプリントを合わせようとする長期間の取り組みから生まれた完璧なセキュリティソリューションです。ESET Cyber Security Pro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6の新機能

ESET Cyber Security Pro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。

- **64ビットアーキテクチャーサポート**
- **フィッシング詐欺対策** – 信頼できるWebサイトに偽装された偽のWebサイトが個人情報を取得できないように防止します。
- **システムアップデート** - ESET Cyber Security Proバージョン6には、オペレーティングシステムアップデートの通知など、さまざまな修正と改良が導入されています。 詳細については、システム更新セクションを参照してください。
- **保護ステータス** – 保護ステータス画面の通知(例: 電子メール保護が無効ですまたはコンピューターの再起動が必要です)を非表示にします。
- **検査するメディア** – 特定のタイプのメディアをリアルタイムスキャナーから除外できます(ローカルドライブ、リムーバブルメディア、ネットワークメディア)。
- **ネットワーク接続** – コンピューターのネットワーク接続を表示し、これらの接続のルールを作成できます。

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

システム要件

ESET Cyber Security Pro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 10.12以降
メモリ	300 MB
空きディスク容量	200 MB

既存のIntelサポートに加えてESET Cyber Security Proバージョン 6.10.900.0以降は、Rosetta 2を使用してApple M1およびM2チップをサポートします。

インストール

インストール処理を開始する前に、コンピューター上に開いているすべてのプログラムを閉じてください。ESET Cyber Security Proには、すでにコンピューターにインストールされているその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。問題が生じる可能性をなくすため、他のウイルス対策プログラムを削除することを強くお勧めします。

インストールウィザードを起動するには、次のいずれかを実行します。

- ESETウエブサイトからダウンロードしたファイルを使用してインストールする場合は、ダウンロードしたファイルを開き、[**インストール**]アイコンをダブルクリックします。
- インストールCD/DVDからインストールしている場合は、コンピュータに挿入し、デスクトップまたは**Finder**から開き、**インストール**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、基本セットアップを実行します。インストールの初期段階中に、インストーラーは自動的に最新の製品バージョンを自動的にオンラインで確認します。新しいバージョンが見つかった場合は、インストール処理を続行する前に、最新のバージョンをダウンロードするオプションが表示されます。

使用許諾契約書に同意した後、インストールのモードを以下から選択するように指示されます。

- 標準インストール
- カスタムインストール

標準インストール

標準インストールモードには、ほとんどのユーザーに適した設定オプションが用意されています。この設定は、最大限のセキュリティと優れたシステムパフォーマンスの組み合わせを実現します。標準インストールは既定のオプションで、固有の設定に対して特定の要件を必要としない限り推奨されます。

1.**ESET LiveGrid**ウィンドウで、任意のオプションを選択して、**続行**をクリックします。後からこの設定を変更する場合は、**LiveGrid設定**を使用して実行できます。ESET Live Gridの詳細については、用語集を参照してください。
2.**望ましくない可能性のあるアプリケーション**ウィンドウで、任意のオプションを選択(「望ましくない可能性のあるアプリケーション」を参照)して、**続行**をクリックします。後からこの設定を変更する場合は、**詳細設定**を使用します。
3.**インストール**をクリックします。macOSパスワードを入力するように指示されたら、入力して、**ソフトウェアのインストール**をクリックします。

ESET Cyber Security Proをインストールした後に次の手順を実行します。

macOS Big Sur (11)

1.システム拡張機能を許可します。

2.フルディスクアクセスを許可する。

3.ESETがプロキシ設定を追加することを許可します。次の通知が表示されます。「ESET Cyber Security Pro」**はプロキシプロキシ設定を追加しようとしています**。この通知が表示された場合は、**許可**をクリックします。**許可しない**をクリックすると、Webアクセス保護は動作しません。

- **macOS 10.15以前**

  1.macOS 10.13以降では、システムから**システム拡張がブロックされました**通知とESET Cyber Security Proから**コンピューターが保護されていません**通知が送信されます。 すべてのESET Cyber Security Pro機能にアクセスにするには、デバイスでカーネル拡張を許可する必要があります。 デバイスでカーネル拡張を許可するには、**システム環境設定 > セキュリティとプライバシー**に移動し、**許可**をクリックして、開発者**ESET, spol. s.r.o.**からのシステムソフトウェアを許可します。詳細については、ナレッジベース記事をご覧ください。

  2.macOS 10.14以降では「ESET Cyber Security Proから**コンピューターの一部が保護されています**通知が送信されます。すべてのESET Cyber Security Pro機能にアクセスするには「ESET Cyber Security Pro」への**フルディスクアクセス**を許可する必要があります。**システム設定を開く > セキュリティとプライバシー**をクリックします。**プライバシー**タブに移動し、**フルディスクアクセス**オプションを選択します。ロックアイコンをクリックすると、編集が有効になります。プラスアイコンをクリックして「ESET Cyber Security Proアプリケーションを選択します。コンピューターには、コンピューターを再起動するように指示する通知が表示されます。**後で再起動**をクリックします。ここでコンピューターを再起動しないでください。「ESET Cyber Security Pro」通知ウィンドウで**再開**をクリックするか、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ご覧ください。

ESET Cyber Security Pro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[**コンピューターの検査**]をクリックし、[**スマート検査**]をクリックします。 コンピューターの検査の詳細については、「コンピューターの検査」セクションを参照してください。

カスタムインストール

カスタムインストールモードは、経験豊富なユーザーがインストールプロセス中に詳細な設定を変更できるように設計されています。

- **プロキシサーバー**

プロキシサーバーを使用している場合は、[**プロキシサーバーを使用する**]を選択することによって、

パラメーターを定義できます。 次のウィンドウで、[**アドレス**]フィールドにプロキシサーバーのIPアドレスまたはURLを入力します。[**ポート**]フィールドには、プロキシサーバーが接続を受け付けるポートを指定します(既定では3128です)。 プロキシサーバーで認証が要求される場合は、有効な[**ユーザー名**]と[**パスワード**]を入力して、プロキシサーバーへのアクセスを可能にする必要があります。 プロキシサーバーを使用しない場合は、**[プロキシサーバーを使用しない]**を選択します。 プロキシサーバーを使用しているか不明な場合は、**システム設定を使用(推奨)**を選択し、現在のシステム設定を使用します。

• **権限**
プログラム設定を編集できる権限ユーザーまたはグループを定義できます。 左側のユーザー一覧からユーザーを選択し、[**追加**]をクリックして[**権限ユーザー**]の一覧に追加します。 全てのシステムユーザーを表示するには、[**全ユーザーを表示**]を選択します。 [権限ユーザー]の一覧を空のままにすると、すべてのユーザーに権限があると判断されます。

• **ESET LiveGrid®**
ESET Live Gridの詳細については、用語集を参照してください。

• **望ましくない可能性があるアプリケーション**
望ましくない可能性が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。

• **ファイアウォール**
フィルタリングモードを選択できます。 詳細は、「フィルタリングモード」トピックを参照してください。ESET Cyber Security Proをインストールした後に次の手順を実行します。

macOS Big Sur (11)

1.システム拡張機能を許可します。

2.フルディスクアクセスを許可する

3.ESETがプロキシ設定を追加することを許可します。次の通知が表示されます。「ESET Cyber Security Pro」**はプロキシプロキシ設定を追加しようとしています**。この通知が表示された場合は、**許可**をクリックします。**許可しない**をクリックするとWebアクセス保護は動作しません。

macOS 10.15以前

1.macOS 10.13以降では、システムから**システム拡張がブロックされました**通知とESET Cyber Security Proから**コンピューターが保護されていません**通知が送信されます。 すべてのESET Cyber Security Pro機能にアクセスにするには、デバイスでカーネル拡張を許可する必要があります。 デバイスでカーネル拡張を許可するには、**システム環境設定 > セキュリティとプライバシー**に移動し、**許可**をクリックして、開発者**ESET, spol. s.r.o.**からのシステムソフトウェアを許可します。詳細については、ナレッジベース記事をご覧ください。

2.macOS 10.14以降ではESET Cyber Security Proから**コンピューターの一部が保護されています**通知が送信されます。すべてのESET Cyber Security Pro機能にアクセスするにはESET Cyber Security Proへの**フルディスクアクセス**を許可する必要があります。**システム設定を開く > セキュリティとプライバシー**をクリックします。**プライバシー**タブに移動し、**フルディスクアクセス**オプションを選択します。ロックアイコンをクリックすると、編集が有効になります。プラスアイコンをクリックしてESET Cyber Security Proアプリケーションを選択します。コンピューターには、コンピューターを再起動するように指示する通知が表示されます。**後で再起動**をクリックします。ここでコンピューターを再起動しないでくださいESET Cyber Security Pro通知ウィンドウで**再開**をクリックするか、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ご覧ください。

ESET Cyber Security Pro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**コンピューターの検査**をクリックし、**スマート検査**をクリックします。 コンピューターの検査の詳細については、「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

MacOS 11 (Big Sur)では、カーネル拡張機能がシステム拡張機能によって置き換えられました。このため、新しいサードパーティのシステム拡張機能を読み込む前に、ユーザーが承認する必要があります。

macOS Big Sur (11)以降のESET Cyber Security Proをインストールした後、システムからの「システム拡張機能がブロックされました」通知と、ESET Cyber Security Proからの「コンピューターが保護されていません」通知が表示されます。すべてのESET Cyber Security Pro機能にアクセスにするには、デバイスでシステム拡張機能を許可する必要があります。

前のmacOSからBig Surにアップグレードします。
既にESET Cyber Security Proをインストールし、macOS Big Surにアップグレードする場合は、アップグレード後に手動でESETカーネル拡張機能を許可する必要があります。クライアントコンピューターへの物理アクセスが必要です。リモートアクセス時には、[許可]ボタンが無効になります。

macOS Big Sur以降にESET製品をインストールしている場合は、手動でESETカーネル拡張機能を許可する必要があります。クライアントコンピューターへの物理アクセスが必要です。リモートアクセス時には、このオプションが無効になります。

システム拡張機能を手動で許可する

1. **システム設定を開く**をクリックするか、いずれかの警告ダイアログボックスで**セキュリティ設定を開く**をクリックます。
2. 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。
3. 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。
4. **詳細**をクリックします。
5. ESET Cyber Security Pro**.app**オプションを両方クリックします。
6. **OK**をクリックします。

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(ナレッジベース記事は一部の言語では提供されていません)。

フルディスクアクセスを許可する

macOS 10.14では、**コンピューターは一部しか保護されていません**というESET Cyber Security Proからの通知が表示されます。すべてのESET Cyber Security Pro機能を利用するにはESET Cyber Security Proへの**フルディスクアクセス**を許可する必要があります。

1. 警告ダイアログウィンドウで**システム設定を開く**をクリックします。
2. 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。
3. 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。

4.リストからESET Cyber Security Pro**.app**を選択します。

5.ESET Cyber Security Proの再起動通知が表示されます。後でクリックします。

6.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。

> **ESETリアルタイムファイルシステム保護が存在しません**
> **リアルタイムファイルシステム保護**オプションがリストに表示されない場合は、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.ESET Cyber Security Proの警告ダイアログウィンドウで[再開]をクリックするか、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。

製品のアクティベーション

インストール後、[製品アクティベーション]ウィンドウが自動的に表示されます。任意の時点で製品アクティベーションダイアログを表示するにはmacOSメニューバー（画面の上部）にある ESET Cyber Security Pro アイコン をクリックし、**[製品のアクティベーション...]**をクリックします。

- **製品認証キー** - XXXX-XXXX-XXXX-XXXX-XXXXまたはXXXX-XXXXXXXXという形式の一意野文字列。ライセンス所有者の識別またはライセンスのアクティベーションで使用されます。製品のリテールパッケージ版を購入する場合、 製品認証キー を使用して製品をアクティベートします。アクティベーションキーは通常、製品パッケージの背面またはパッケージ内に同梱されています。
- **ユーザー名とパスワード** – ユーザー名とパスワードがありESET Cyber Security Proのアクティベーション方法がわからない場合は、**[ユーザー名とパスワードをお持ちのお客様]**をクリックしますmy.eset.comに移動し、資格情報を製品認証キーに変換できます。
- **無料試用版ライセンス** – 購入する前にESET Cyber Security Proを評価する場合はこのオプションを選択します。メールアドレスを入力してESET Cyber Security Proを一定の期間内のみアクティベーションします。試用ライセンスはメールで送信されます。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。
- **ライセンスの購入** – ライセンスがなく、購入する場合は、[ライセンスの購入]をクリックします。このオプションを選択すると、お客様の地域のESET販売元のWebページが表示されます。
- **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。

アンインストール

ESET Cyber Security Proをアンインストールするには、次のいずれかの手順を実行します。

- コンピューターにESET Cyber Security ProインストールCD/DVDを挿入し、これをデスクトップまたは[**Finder**]ウィンドウから開き、[**アンインストール**]をダブルクリックします。
- ESET Cyber Security Pro インストールファイル（*.dmg*）を開き、[**アンインストール**]をダブルクリックします。
- [**Finder**]を起動し、ハードドライブにある**Applications**フォルダを開き、Ctrlを押しながら**ESET Cyber Security Pro**アイコンをクリックして、[**パッケージコンテンツを表示**]を選択します。**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。

基本概要

ESET Cyber Security Proのメインウィンドウは、2つのメイン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。

次のセクションにはメインメニューからアクセスできます。

- [**ホーム**] – コンピューター、ネットワーク（ファイアウォール）、ウェブ、メール保護とペアレンタルコントロールの保護状態についての情報を提供します。
- [**コンピューターの検査**] –このセクションを使用すると、コンピューターの検査の設定や起動を行うことができます。
- **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。
- [**設定**] – このセクションを選択するとコンピューターのセキュリティレベルを調整することができます。
- [**ツール**] - ログファイル、スケジューラ、隔離フォルダー、実行中のプロセスとその他のプログラム機能へのアクセスを提供します。
- [**ヘルプ**] – ヘルプファイル、インターネットナレッジベース、サポートリクエストフォームへのアクセスを表示します。

ショートカットキー

ESET Cyber Security Proで使用できるショートカットキーは、次のとおりです。

- cmd+, - ESET Cyber Security Pro環境設定を表示します。
- cmd+O - ESET Cyber Security ProのメインGUIウィンドウを既定のサイズに変更し、画面の中央に移動します
- cmd+Q - ESET Cyber Security ProメインGUIウィンドウを非表示にします。macOSメニューバー(画面上部)のESET Cyber Security Proアイコンをクリックすると、開くことができます。
- cmd+W - ESET Cyber Security ProメインGUIウィンドウを閉じます。

次のキーボードショートカットは、[**設定**]>[**アプリケーション環境設定の入力...**]の下の[**標準メニューを使用する**]が有効な場合にのみ動作します。> **インターフェイス**:

- cmd+alt+L – [ログファイル]セクションを開きます
- cmd+alt+S – [スケジューラー]セクションを開きます
- cmd+alt+Q – [隔離]セクションを開きます。

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[**ホーム**]をクリックします。プライマリウィンドウにはESET Cyber Security Proモジュールの動作状態の概要が表示されます。

プログラムが正しく動作しない場合の解決方法

モジュールが正常に機能している場合は、緑色のアイコンが表示されます。モジュールが正常に機能していない場合は、赤色の感嘆符またはオレンジ色の通知アイコンが表示されます。モジュールに関する詳細情報がウィンドウの上部に表示されます。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。

推奨される解決策を使用しても問題を解決できない場合は、ESETナレッジベースで解決策を検索するか、ESETカスタマーサポートまでお問い合わせください。カスタマーサポートはESET Cyber Security Proに関するご質問に迅速に対応し、問題の解決をサポートします。

コンピューターの保護

[コンピューター]の設定は[設定]-[コンピューター]から変更できます。[コンピューター]の設定には、[リアルタイムファイルシステム保護]と[リムーバブルメディアのブロック]があります。各機能を無効にする場合は、該当する機能を[無効]に切り替えてください。これはあなたのコンピューターの保護レベルを下げる可能性があることご注意ください。各モジュールの詳細設定にアクセスするには[**設定...**]をクリックします。

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。

全般

[**全般**]セクション([**設定**] > [**詳細設定を表示する...**]> [**全般**])で、以下のタイプのアプリケーションを検出するように設定できます。

- **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。これらのタイプのアプリケーションの詳細については、用語集をご覧ください。
- **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。そのため、既定ではこのオプションは無効に設定されています。
- **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。この種のプロテクターは、検出を回避するためにマルウェアの作成者によって使用されることがよくあります。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。

ファイルシステムまたはWebとメールの除外を設定するには、[**設定...**]ボタンをクリックします。

除外

[**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。

[**ファイルシステム**]タブに表示されているファイルとフォルダーは、すべての検査(起動時、リアルタイム、およびオンデマンド)から除外されます。

- **パス** – 除外されるファイルやフォルダーのパスです。
- **脅威** – 除外されるファイルの横に脅威の名前がある場合、ファイルは特定の脅威に対してのみ除外され、完全には除外されません。このファイルが後で他のマルウェアに感染した場合は、ウイルス対策機能によって検出されます。
-  – 新しい例外を作成します。対象のパスを入力するか(ワイルドカード*および?を使用できます)、あるいはツリー構造でフォルダーまたはファイルを選択します。
-  – 選択したエントリーを除去します。
- **既定** – 全ての除外対象を取り消します。

[**Webとメール**]タブでは、特定の[**アプリケーション**]または[**IP/IPv6アドレス**]をプロトコルの検査から除外できます。

スタートアップ保護

スタートアップファイルのチェックでは、システムの起動時にファイルを自動的に検査します。既定では、この検査はスケジュール設定されたタスクとして、ユーザーのログオン後または検出モジュールの更新に成功した後、定期的に実行されます。起動時の検査に適用できるThreatSenseエンジンパラメーター設定を変更するには、[**設定**]ボタンをクリックしますThreatSenseエンジン設定の詳細については、このセクションを参照してください。

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、あらゆる種類のメディアを調べます。検査は多種多様なイベントによってトリガーされますThreatSenseテクノロジーを利用し(ThreatSenseエンジンパラメーター設定を参照)、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。

既定では、**ファイルを開くときファイルを作成するとき**、または**ファイルを実行するとき**に検査されます。既定の設定によりコンピューターが最大限のレベルでリアルタイムに保護されるので、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。他のリアルタイムスキャナーと競合する場合などの特殊な場合は、メニューバー(画面最上部)のESET Cyber Security Proアイコンをクリックし、[**リアルタイムファイルシステム保護を無効にする**]を選択して、リアルタイム保護を終了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は、メインプログラムウィンドウ([**設定**] > [**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[**無効**]に切り替える)からも無効にできます。

次のタイプのメディアはReal-timeスキャナーから除外できます。

- **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** - CDDVDUSB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詳細設定を変更するには、[**設定**] > [**詳細設定を表示する...**]（または*cmd+,*を押す）> [**リアルタイム保護**]に移動し、[**詳細オプション**]の横の[**設定**]をクリックします(詳細検査オプションを参照)。

詳細設定オプション

このウィンドウではThreatSenseエンジンで検査されるオブジェクトタイプを定義できます。**自己展開アーカイブランタイムパッカー高度なヒューリスティック**の詳細については、ThreatSenseエンジンパラメーター設定を参照してください。

アーカイブネストの値を大きくするとシステムのパフォーマンスが低下する場合があるため、特定の問題を解決するために必要でない場合を除き、[**既定のアーカイブ設定**]セクションで変更しないことをお勧めします。

実行されたファイルのThreatSenseパラメーター – 既定では、ファイルの実行時に**高度なヒューリスティック**が使用されます。スマート最適化とESET Live Gridを有効にし、システムパフォーマンスへの影響を緩和することを強くお勧めします。

ネットワークボリュームの互換性を高める – ネットワークでファイルにアクセスするときにこのオプションを使用すると、パフォーマンスが上がります。ネットワークドライブへのアクアセス中に速度が低下した場合は、有効にしてください。この機能は、macOS 10.10以降でシステムファイルコーディネーターを使用します。一部のアプリケーションはファイルコーディネーターをサポートしません。たとえばMicrosoft Word 2011はサポートしませんがWord 2016はサポートします。

リアルタイム保護の設定の変更

リアルタイム保護は、ESET Cyber Security Proで安全なシステムを維持するために最も必要不可欠な要素です。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。特定の状況に限ってパラメーターを変更することをお勧めします。たとえば、特定のアプリケーションと競合する状況があります。

ESET Cyber Security Pro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すべての設定が最適化されています。既定の設定に戻すには、[**リアルタイム保護**]ウィンドウ([**設定**] > [**アプリケーションの設定を入力する...**]>[**リアルタイム保護**])の左下の[**既定**]をクリックします。

リアルタイム保護の確認

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 Pro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。このファイルは、EICAR (European Institute for Computer Antivirus Research)が、ウイルス対策プログラムの機能をテストする目的で作成しました。

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保護を無効にしてしまった場合は、再開する必要があります。リアルタイム保護を再開するには、メインメニューから[**設定**] >[**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[**有効**]に切り替えます。あるいは、アプリケーション設定ウィンドウの[**リアルタイム保護**]で、[**リアルタイムファイルシステム保護を有効にする**]を選択して、リアルタイムファイルシステム保護を有効にすることもできます。

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、他のプログラムとの競合が原因であることがあります。この場合にはESETのカスタマーサポートまでお問い合わせください。

コンピューターの検査

コンピューターの動作が異常で感染していると思われる場合には、[**Smart検査**]を実行して、コンピューターにマルウェアがいないかどうかを調べます。保護機能の効果を最大化するため、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必要があります。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。[**ツール**] > [**スケジューラ**]で、検査をスケジュールされたタスクとして設定できます。

検査の種類

コンピューターの検査には次の2種類があります。[**Smart検査**]では、検査パラメーターを追加で設定することなく、簡単にシステムを検査します。[**カスタム検査**]では、あらかじめ定義した検査プロファイルの選択や、特定の検査の対象の選択を行うことができます。

Smart検査

Smart検査を使用すると、コンピューター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。主な利点は、スキャンを詳細に設定しなくても簡単に操作できることにありますSmart検査では、全てのフォルダーにある全てのファイルが検査されます。検出されたマルウェアがあれば、自動的に駆除または削除されます。駆除レベルは自動的に既定値に設定されます。駆除の種類の詳細については、「駆除」のセクションを参照してください。

カスタム検査

カスタム検査は、検査の対象やスキャン方法などの検査パラメーターを自分で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、パラメーターを詳細に設定できることです。 さまざまな設定をユーザー定義の検査プロファイルとして保存できます。これは、同じパラメータで検査を繰り返し実行する場合に便利です。

検査の対象を選択するには、[**コンピューターの検査**] > [**カスタム検査**]を選択し、ツリー構造から特定の**検査の対象**を選択します。 検査の対象をさらに細かく指定することもできます。そのためには、対象にするフォルダーまたはファイルのパスを入力します。 システムの検査で追加の駆除アクションを実行する必要がない場合は、[**駆除せずに検査する**]を選択します。 さらに、[**設定...**] > [**駆除**]をクリックして、3種類の駆除レベルから選択できます。

> **カスタム検査**
> 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。

検査の対象

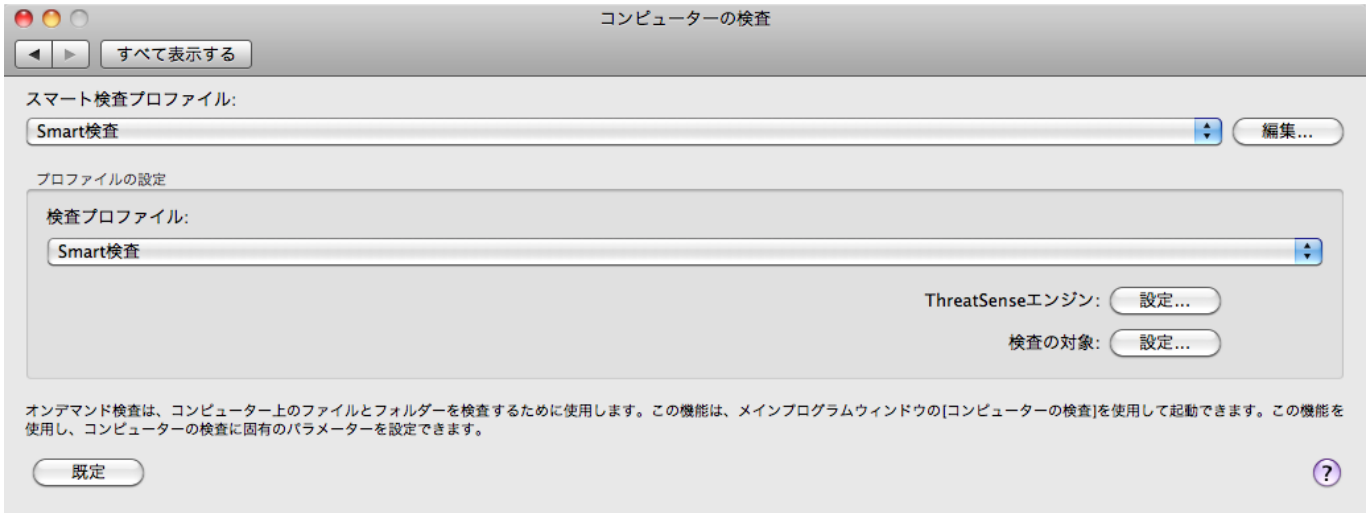
[検査の対象]ツリー構造を使用すると、ウイルスを検査するファイルおよびフォルダーを選択できます。フォルダーはプロファイルの設定に従って選択することもできます。

検査の対象をさらに細かく定義することもできます。そのためには、検査の対象に含めるフォルダーまたはファイルのパスを入力します。特定のファイルまたはフォルダに対応するチェックボックスをオンにし、コンピュータで使用可能なすべてのフォルダの一覧を示すツリー構造から対象を選択します。

検査プロファイル

検査について好みの基本設定を保存して、後で検査を行う際に使用できます。さまざまな検査の対象、検査方法、およびその他のパラメーターについて、定期的に行う検査ごとにプロファイルを作成することをお勧めします。

新しいプロファイルを作成するには、メインメニューから[**設定**] > [**詳細設定を表示する ...**]（または*cmd+,*を押す）> [**コンピューター検査**]をクリックし、現在のプロファイルのリストの横の[**編集...**]をクリックします。



ニーズに合った検査プロファイルを作成するための参考情報として、「ThreatSenseエンジンのパラメーターの設定」セクションにある検査設定の各パラメーターの説明を参照してください。

例:既にあるSmart検査の設定は部分的にしか自分のニーズを満たさないので、独自の検査プロファイルを作成する必要があるとします。そこで、圧縮された実行形式と安全でない可能性があるアプリケーションを検査しないよう設定します。また、厳密な駆除を適用することにします。[**オンデマンド検査プロファイルリスト**]ウィンドウで、プロファイル名を入力して[**追加**]ボタンをクリックし、[**OK**]をクリックして確認します。次に、[**ThreatSenseエンジン**]および[**検査の対象**]を設定してパラメーターを調整し、自分の要件に合わせます。

オンデマンド検査の完了後にオペレーティングシステムをオフにし、コンピュータをシャットダウンする場合は、**検査後にコンピュータをシャットダウン**オプションを使用します。

ThreatSenseエンジンのパラメータ設定

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、新しい脅威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。

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

セットアップウィンドウを開くには、**セットアップ > アプリケーション環境設定の入力**(または*cmd+,*を押す)をクリックし、ThreatSenseエンジンの[**設定**]ボタンをクリックします。このボタンは、[**スタートアップ保護**]、[**リアルタイム保護**]、および[**コンピューターの検査**]モジュール(いずれも以下に示すThreatSense技術を使用)にあります。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、以下の保護モジュールごとにThreatSenseを個々に設定できます。

- [**スタートアップ保護**]－[自動起動ファイルの検査]
- [**リアルタイム保護**]ー[リアルタイムファイルシステム保護]
- [**コンピュータの検査**]－[オンデマンドコンピュータ検査]
- **Webアクセス保護**
- **電子メール保護**

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。そのため、コンピュータ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を変更しないことをお勧めします。

オブジェクト

[**検査対象**]セクションでは、侵入物を検査するファイルを指定できます。

- **シンボリックリンク** – (コンピュータの検査のみ)オペレーティングシステムによって別のファイルまたはディレクトリへのパスとして解釈され、たどることができるテキスト文字列を含むファイルを検査します。
- **電子メールファイル** – (リアルタイム保護では使用できません)電子メールファイルを検査します。
- **メールボックス** – (リアルタイム保護では使用できません)システム内のユーザーのメールボックスを検査します。このオプションを正しく使用しない場合、電子メールクライアントとの競合が発生することがあります。このオプションの利点と欠点の詳細については、次のナレッジベースベースの記事を参照してください。
- **アーカイブ** – (リアルタイム保護では使用できません)アーカイブ内の圧縮されたファイル(.rar□.zip□.arj□.tarなど)を検査します。
- **自己解凍形式** – (リアルタイム保護では使用できません)自己解凍形式のアーカイブファイルに含まれているファイルを検査します。
- **圧縮された実行形式** – 標準のアーカイブ形式とは異なり、ランタイム圧縮形式はメモリに展開されます。このオプションを選択すると、標準的な静的圧縮形式(たとえば□UPX□yoda□ASPack□FGS)も検査されます。

オプション

[**オプション**]セクションでは、システムの検査時に使用される方法を選択できます。次のオプションは使用可能です。

- **ヒューリスティック** – ヒューリスティックは、悪意のあるプログラムの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。

駆除

駆除設定により、感染ファイルからウイルスを駆除するときのスキャナの動作が決まります。 駆除には、3つ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。
- **標準的な駆除** – 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。 あらかじめ指定したアクションを完了できなかった場合にも、その後のアクションの選択が表示されます。
- **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。

アーカイブファイル

既定の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。

アーカイブ検査

既定の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、ファイルの種類と内容を規定しますThreatSenseパラメータ設定のこのセクションでは、検査から除外するファイルの種類を指定できます。

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。 + および − ボタンを使用することで、目的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、*log cfg tmp*ファイルを除外するとよい場合があります。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

制限

[**制限**]セクションでは、検査対象のオブジェクトの最大サイズおよびネストされたアーカイブのレベルを指定できます。

- **最大サイズ:**検査対象のオブジェクトの最大サイズを定義します。最大サイズが定義されると、ウイルス対策機能では、指定した値より小さいサイズのオブジェクトのみが検査されます。上級ユーザーが大きいオブジェクトを検査から除外する必要がある場合のみ、このオプションを変更してください。
- **最長検査タイム:**オブジェクトの検査に割り当てられた最長時間を定義します。ここでユーザー定義の値が入力されていると、検査が終わっているかどうかにかかわらず、その時間が経過するとウイルス対策機能は検査を停止します。
- **最大ネストレベル:**アーカイブの検査の最大レベルを指定します。一般的な環境では既定値10を変更する理由はないので、その値を変更しないことをお勧めします。ネストされたアーカイブ数が原因で検査が途中で終了した場合、アーカイブは未チェックのままになります。
- **最大ファイルサイズ:**このオプションを使用すると、検査対象のアーカイブ(抽出された場合)に含ま

れるファイルの最大ファイルサイズを指定できます。この制限により検査が途中で終了した場合、アーカイブは未チェックのままになります。

その他

SMART最適化を有効にする

スマート最適化を有効にすると、スキャンの速度を犠牲にすることなく最も効率的なスキャンレベルが確保されるように、設定が最適化されます。さまざまな保護モジュールで高度にスキャンを行い、異なるスキャン方法を使用します。SMART最適化は製品内で厳密に定義されているものではありません。ESET開発チームは新しい変更点を継続的に実装し、通常のアップデートでお使いのESET Cyber Security Proに組み込みます。SMART最適化を無効にすると、特定のモジュールのThreatSenseコアのユーザー定義設定のみがスキャンの実行時に適用されます。

[**代替データストリームを検査する**]（オンデマンド検査のみ）

代替データストリーム　は、ファイルシステムによって使用され、通常のスキャン技術では検出できないファイルおよびフォルダーの関連付けです。多くのマルウェアが、自らを代替データストリームに見せかけることによって、検出を逃れようとします。

侵入物が検出された

侵入物がシステムに侵入する経路は、Webページ、共有フォルダー、電子メールや、コンピューターのリムーバブルデバイス(USB、外付けハードディスク、CD、DVDなど)など、さまざまです。

使用しているコンピューターが、マルウェアに感染している兆候(処理速度が遅くなる、頻繁にフリーズするなど)を示している場合は、次の処置を取ることをお勧めします。

1. [**コンピュータの検査**]をクリックします。
2. [**Smart検査**]をクリックします(詳細については、「Smart検査」を参照してください)。
3. 検査終了後、ログで検査済みファイル、感染ファイル、および駆除済みファイルの件数をそれぞれ確認します。

ディスクの特定の部分だけを検査するには、[**カスタム検査**]をクリックし、ウイルスを検査する対象を選択します。

ESET Cyber Security Proでのマルウェアの一般的な処理例として、リアルタイムのファイルシステムモニターにより既定の駆除レベルを使用してマルウェアが検出された場合を説明します。リアルタイム保護によって、ファイルからのウイルスの駆除、またはファイル自体の削除が試みられます。リアルタイム保護モジュールで使用できるあらかじめ指定されたアクションがない場合は、警告ウィンドウが表示され、オプションを選択するよう求められます。選択できるオプションは通常、[**駆除**]、[**削除**]、および[**何もしない**]のいずれかです。[**何もしない**]はお勧めできません。感染しているファイルが、そのままにされるからです。このオプションは、ファイルが「無害なのに誤って感染が検出された」と確信できる場合に使用します。

駆除と削除
ウイルスが悪意のあるコードをファイルに添付して攻撃している場合に、駆除を行います。この場合、ファイルを元の状態に戻すため、まず感染しているファイルからのウイルスの駆除を試みます。ファイルが悪意のあるコードのみで構成されている場合には、ファイル全体が削除されます。

アーカイブのファイルの削除
既定の駆除モードでは、アーカイブファイルに感染ファイルしか含まれていない場合にのみ、アーカイブファイル全体が削除されます。つまり、感染していない無害なファイルも含まれている場合には、アーカイブは削除されません。ただし、**厳密な駆除**スキャンを実行する際には注意が必要です。厳格な駆除では、アーカイブに感染ファイルが1つでも含まれていれば、アーカイブ内の他のファイルの状態に関係なく、アーカイブが削除されます。

リムーバブルメディアの検査と遮断

ESET Cyber Security Proでは、挿入されたリムーバブルメモリデバイス(CD、DVD、USBなど)のオンデマンド検査を実行できます。macOS 10.15では、ESET Cyber Security Proは他の外部メディアデバイスも検査できます。

macOS 11以降でのリムーバブルメディア検査
ESET Cyber Security ProがmacOS 11以降にインストールされている場合は、メモリデバイスのみを検査します。

リムーバブルメディア(に悪意のあるコードが入っていると、コンピュータを危険にさらす可能性があります。リムーバブルメディアをブロックするには、**[メディアブロックの設定]**(上記の画像を参照)をクリックするか、メインプログラムウィンドウのメインメニューで[**設定**]>[**アプリケーション設定を入力する...**]>[**メディア**]をクリックし、[**リムーバブルメディアのブロックを有効にする**]を選択します。特定のタイプのメディアへのアクセスを許可するには、必要なメディアボリュームの選択を解除します。

CD-ROMアクセス
USBケーブルによってコンピューターに接続された外部CD-ROMドライブへのアクセスを許可するには、[**CD-ROM**]オプションの選択を解除します。

Anti-Phishing

フィッシングとは、ソーシャルエンジニアリング(機密情報を入手するためのユーザーの不正操作)を使用する犯罪活動を意味します。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。

[**設定**] > [**詳細設定を表示する ...**] > [**アンチフィッシング保護**]を有効にしておくことをお勧めします。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。

ファイアウォール

ファイアウォールは、指定されたフィルタリングルールに基づいて個別のネットワーク接続を許可または遮断し、システムに対するすべての送受信ネットワークトラフィックを制御します。それはリモートのコンピューターからの攻撃に対して保護を提供しサービスの一部をブロックできるようにします。それはまたHTTPPOP3及び IMAP プロトコルにウイルス・スパイウェア対策を提供します。

検査例外
ESET Cyber Security Proは暗号化されたプロトコルのHTTPSPOP3SIMAPSを検査しません。

[ファイアウォール]の設定は[**設定**] >[**ファイアウォール**]から変更できます。ここではフィルタリングモード、ルールや詳細な設定を調整することができます。また、ここからプログラムの詳細設定にアクセスできます。

[**すべてのネットワーク通信を遮断**]を[**有効**に切り替えると、すべてのインバウンドおよびアウトバウンドの通信は、ファイアウォールによって遮断されます。ネットワークからシステムからの切断を必要とする重大なセキュリティ上のリスクが疑われる場合にのみ、このオプションを使用します。

フィルタリングモード

三種類のフィルタリングモードが ESET Cyber Security Pro ファイアウォールに適用できます。フィルタリングモード設定は ESET Cyber Security Pro 設定(*cmd+,*を押します) > **ファイアウォール**において見つけられます。選択したモードに基づいてファイアウォールのふるまいが変化します。フィルタリングモードが必要なユーザーインターアクションのレベルに影響を与えます。

すべての通信をブロック – すべてのインバウンドとアウトバウンドの接続が遮断されます。

自動モード – 既定のモード。このモードでは、ルールを定義することなく、ファイアウォールの簡単で便利な使用を好むユーザーに適しています。自動モードでは、特定のシステムの標準アウトバウンドトラフィックを許可し、ネットワーク側から開始されなかったすべての接続を遮断します。また、カスタムやユーザー定義ルールを追加することができます。

対話モード – ファイアウォールのカスタム設定を作成できます。通信が検出された際、その通信に適用されるルールがなければ、不明な接続を報告するダイアログウィンドウが表示されます。ダイアログウィンドウは通信を許可または拒否するオプションを提供し、許可または拒否するかどうかの決定は、

ファイアウォールの新しいルールとして保存することができます。以降はそのルールに基づき、該当する接続は規則に従って許可またはブロックされます。

遮断された接続の詳細をログファイルに記録するには、**ブロックされた接続をすべて記録**オプションを選びます。ファイアウォールログファイルを確認するには、メインメニューから[**ツール**] > [**ログ**]をクリックし、[**ログ**]ドロップダウンメニューから[**ファイアウォール**]を選択します。

ファイアウォールルール

ファイアウォールルールは、全てのネットワーク接続をテストするための条件であり、それらの条件に適切なアクションを決定します。ファイアウォールルールを使用すると、ルールで定義された接続が確立された場合に取るアクションのタイプを定義することができます。

内向き通信とは、リモートコンピュータがローカルコンピュータとの接続を確立しようとする通信です。外向き通信は、その逆向きの通信です。

新しい未知の通信が検出された場合、慎重にそれを許可または拒否するかどうかを検討する必要があります。保護されていない、または未知の接続は、システムにセキュリティリスクをもたらします。そのような接続が確立されている場合は、お使いのコンピュータに接続しようとするリモートコンピュータとアプリケーションに特に注意を払うことをお勧めします。多くの攻撃は、プライベートデータを取得し、送信しようとするか、ホストのワークステーションに、他の悪意のあるアプリケーションをダウンロードします。ファイアウォールを使用すると、ユーザーはこのような接続を検出し、切断することができます。

既定ではAppleが署名したソフトウェアが自動的にネットワークにアクセスできます。これを無効にするには、**[Appleが署名したソフトウェアが自動的にネットワークにアクセスすることを許可する]**をオフにします。

新規ルールの作成

[**ルール**]タブは個々のアプリケーションによって生成されたトラフィックに適用されているルールが含まれています。ルールは新しい通信に対するユーザーの反応に従って自動的に追加されます。

1.新しいルールを作成するために、[**追加**]をクリックし、このルール名を入力し、アプリケーションのアイコンを空白のフィールドにドラッグアンドドロップし、[**参照**]をクリックし、*/Applications*フォルダにあるプログラムを探します。コンピュータにインストールされているすべてのアプリケーションにルールを適用するには、**[すべてのアプリケーション]**オプションを選びます。

2.次のウィンドウで、**アクション**(選択したアプリケーションとネットワーク間の通信を許可また

は拒否)と通信の**方向**(内向き、外向き、またはその両方)を指定します。このルールに関連するすべての通信をログファイルに記録できます。このためには、**ログルール**オプションを選択します。ログを確認する時に、ESET Cyber Security Proのメインメニューから **ツール > ログ** をクリックし、**ログ** ドロップダウンメニューから **ファイアウォール** を選びます。

3.**プロトコル/ポート** セクションにおいて、アプリケーションの通信に使用するプロトコルとポート番号を選択します(TCPまたはUDPプロトコルが選択されている場合)。トランスポートプロトコルレイヤによって、セキュアで効率的なデータ転送が実現します。

4.最後に、ルールの**宛先**条件(IPアドレス、範囲、サブネット、イーサネット、またはインターネット)を指定します。

ファイアウォールゾーン

ゾーンでは、1つの論理グループを作成するネットワークアドレスのコレクションを表します。特定のグループ内の各アドレスには、グループ全体について集中的に定義された同様なルールが割り当てられています。

これらのゾーンは **追加...** をクリックと作成できます。このゾーンの **名前** と **説明**、このゾーンの所属するプロファイルを選んでIPv4/IPv6アドレス、アドレス範囲、サブネットWiFiネットワークまたはあるインターフェイスを選びます。

ファイアウォールプロファイル

プロファイルはESET Cyber Security Proファイアウォールの制御を認めます。ファイアウォールルールを作成または編集するときは、そのルールを特定のプロファイルに割り当てることができます。あるプロファイルを選ぶ時に、目標ルール(指定されたプロフィルが付いてません)と適用されたプロファイルに割り当てられたルールだけです。それぞれ異なるルールが割り当てられた複数のプロファイルを作成することで、ファイアウォールの動作を容易に変更できます。

ファイアウォールログ

ESET Cyber Security Proファイアウォールはすべての重要なイベントをログファイルに保存します。ファイアウォールログにアクセスするには、メインメニューから[**ツール**] > [**ログ**]をクリックし、[**ログ**]ドロップダウンメニューから[**ファイアウォール**]を選択します。

ログファイルはエラーの検出やお使いのシステムへの侵入を明らかにする上、とても役に立ちますESETファイアウォールのログには以下のデータが含まれます。

- イベントの日時
- イベントの名前
- ソース
- 対象ネットワークのIPアドレス
- ネットワーク通信プロトコル
- ルールの適用
- 関係するアプリケーション
- ユーザー

このデータの徹底的な分析は、システムのセキュリティを侵害しようとする試みを検出するのに役立ちます。不明な場所からの頻繁な接続、接続を確立する複数回の試み、不明なアプリケーション通信、一般的ではないポート番号など、他の多くの要因が潜在的なセキュリティリスクを示しており、パーソナルファイアウォールを使用するとこれらを防ぐことができます。

Webとメールの保護

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、[**設定**] > [**Webとメール**]をクリックします。ここから、[**設定**]をクリックして、各モジュールの詳細設定にアクセスすることもできます。

- **Webアクセス保護** - Webブラウザとリモートサーバー間のHTTP通信を監視します。
- **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。
- **フィッシング対策保護** - 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。

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

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通信のポート番号またはURL アドレスを定義します。

ポート

[**ポート**]タブで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リスト

URLリストセクションを使用すると、ブロックに対するHTTPアドレスを指定して、チェックからブロック、許可または除外することができます。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。

[**許可するURL**]リストに表示されているURLアドレスのみにアクセスを許可する場合は、[**URLアドレスを制限する**]オプションを選択します。

リストを有効にするには、リスト名の横の[**有効**]を選択します。リストのURLにアクセスされたときに通知してほしい場合は、[**通知**]を選択します。

すべてのリストには、特殊記号*（アスタリスク）および?（クエスチョンマーク）を使用できます。アスタリスクは任意の文字列を置き換え、クエスチョンマークは任意のシンボルを置き換えます。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ではPOP3プロトコルおよびIMAPプロトコルで受信したメール通信が検査されます。 受信メッセージを検査するときにはESET Cyber Security Pro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。

ThreatSenseエンジン：設定 -高度な検査設定により検査対象、検査方法等の設定が出来ます。[**設定**]をクリックし詳細検査設定ウィンドウを表示して下さい。

メールのフットノートへ検査メッセージを追加 - 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、

- **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
- **感染メールのみ** - 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
- **すべての検査済み電子メール** - すべての検査済み電子メールの最後にはタグメッセージが追加されます

感染メールの件名にタグを追加 - 電子メール保護で感染した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、受信者の信頼レベルを上げます。侵入が検出された場合は、指定された電子メールまたは送信者の脅威レベルに関する重要な情報が提供されます。

[**感染メールの件名に追加する目印のテンプレート**] - 感染メールの件名プレフィックス形式を修正するには、このテンプレートを編集します。

- %avstatus% - 電子メール感染状態を追加します(例：未感染、感染...)
- %virus% - 脅威名を追加します
- %aspmstatus% - 迷惑メール対策検査の結果に基づいて件名を変更します
- %product% - ESET製品名を追加します(この場合はESET Cyber Security Pro)
- %product_url% - ESET Webサイトリンクを追加します(www.eset.com)

このウィンドウの下部では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。 詳細については、次のトピックを参照してください。

- POP3プロトコルチェック
- IMAPプロトコルチェック

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 Pro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。プロトコルフィルタリングが正常に動作するには、モジュールが有効なことを確認してくださいPOP3プロトコル確認は、電子メールクライアントを構成せずに、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を有効にする**]オプションが選択されている場合、すべてのPOP3トラフィックに悪意のあるソフトウェアがないか監視されます。

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 Pro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。モジュールが正常に動作するにはIMAPプロトコル確認が有効な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**]がオンになっている場合、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。

ペアレンタルコントロール

ペアレンタルコントロールセクションでは、保護者が子どもを保護するための自動ツールを提供するペアレンタルコントロールの設定ができます。 この機能により、不適切または有害なコンテンツを含むページへのアクセスから子供や若者を守ることができます。 [ペアレンタルコントロール]セクションでは、対象ユーザーに対して適切でない内容を掲載していると考えられるWebページをブロックします。さらに、両親が最大で27の事前定義されたサイトカテゴリへのアクセスを禁止することができます。

あなたのユーザーアカウントは次の場所にリストアップされています: **ペアレンタルコントロール** ウィンドウ(**セットアップ > 詳細設定を表示する ... >> ペアレンタルコントロール**)。 ペアレンタルコントロールで使用するユーザーアカウントを選択します。 選定されたアカウントへの保護レベルを指定するために、**設定**をクリックします。 新規アカウントを作成するには、[**追加**]をクリックします。 これでmacOSシステムアカウントウィンドウへリダイレクトします。

ペアレンタルコントロール セットアップ ウィンドウにおいて、 **設定プロファイル** ドロップダウンメニューから事前定義されたプロファイルをひとつ選ぶか、または他のユーザーアカウントからペアレンタルセットアップをコピーします。 各プロファイルには、許可されたカテゴリの修正済みリストがあります。 カテゴリにチェックマークが付いていたら、それは許可されています。 カテゴリの上にマウスを移動すると、そのカテゴリの説明が表示されます。

[**許可するWebページとブロックするWebページ**]のリストを修正するには、ウィンドウ下部にある[**設定...**]をクリックし、ドメイン名を任意のリストに追加します。 *http://*と入力しないでください。 ワイルドカード(*)の入力は不要です。http://やワイルドカード(*)の入力は不要です。 たとえば、*google.com*を[**許可されたWebページのリスト**]に追加した場合、すべてのサブドメイン(*mail.google.com*、*news.google.com*、*maps.google.com*など)が許可されます。

> **ルール**
> 特定のWebページをブロックするか許可するほうが、1つの分類のWebページ全体をブロックまたは許可するより、精度が高くなることがあります。

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 Pro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 Proの現在のアップデートの状態を確認します。アップデートプロセスを手動で開始するには、 **モジュールのアップデート**をクリックします。

通常の状況では、更新ファイルが正常にダウンロードされると、[アップデート]ウィンドウに[**アップデートは必要ありません – インストールされているモジュールは最新です。**]というメッセージが表示されます。モジュールをアップデートできない場合は、アップデートの設定を確認することをお勧めします。このエラーの最も多い原因に、認証データ(ユーザー名とパスワード)の入力が正しくない、または接続設定の誤りがあります。

アップデートウィンドウには、検出エンジンのバージョンも表示されます。バージョン番号は、検出エンジンアップデート情報を一覧で示すESETのWebページにリンクしています。

アップデートの設定

一時的に保存されたアップデートデータを全て削除するには、[**アップデートキャッシュを削除**]の横にある[**削除**]クリックします。アップデート中に問題が発生した場合はこのオプションを使用してください。

詳細設定オプション

アップデートに成功するごとに表示される通知を無効にするには、[**成功したアップデートについての通知を表示しない**]を選択します。

最終テスト段階の開発モジュールをダウンロードするには、**リリース前アップデート**を有効にします。通常、リリース前アップデートは製品の問題の修正が含まれます。**遅延アップデート**は、リリースの数時間後にアップデートをダウンロードするため、問題がないことが確認されるまでアップデートを受信しません。

ESET Cyber Security Proは、[**アップデートロールバック**]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。**[アップデートファイルのスナップショットを作成]**をオンにしておくとESET Cyber Security Proはこれらのスナップショットを自動的に記録します。新しい検出モジュール/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のある場合、ロールバック機能を使用すると、前のバージョンにロールバックし、設定した期間中のアップデートを無効にできます。アップデートを履歴の最も古いバージョンに戻すには、**ロールバック**をクリックします。あるいは、無期限に延期した場合、前に無効にしたアップデートを有効にすることもできます。アップデートロールバック機能を使用して前のアップデートに戻すときには、**一時停止期間の設定**ドロップダウンメニューを使用して、アップデートを一時停止する期間を指定します。**[取り消しまで]**を選択した場合は、手動で復元するまで、通常のアップデートが再開されません。手動でアップデートを復元するには、**許可**をクリックします。アップデートを一時停止する期間を設定するときには注意してください。

最大検出エンジン経過時間を自動的に設定 – 検出モジュールが期限切れに設定されるまでの最大時間(日数)を設定できます。 既定値は7日です。

アップデートタスクの作成方法

アップデートはメインメニューの[**アップデート**]▯[**モジュールのアップデート**]の順にクリックして、手動でトリガーできます。

アップデートはスケジュールされたタスクとしても実行できます。スケジュールされたタスクを設定するには、[**ツール**] > [**スケジューラ**]をクリックします▯ESET Cyber Security Proでは、次のタスクが既定で有効になっています。

- **定期的に自動アップデート**
- **ユーザーログオン後に自動アップデート**

アップデートタスクはそれぞれ、ユーザーのニーズに合わせて変更することができます。ユーザーは、既定のアップデートタスクとは別に、ユーザー定義の設定で新しいアップデートタスクを作成することができます。アップデートタスクの作成と設定の詳細については、「スケジューラ」セクションを参照してください。

ESET Cyber Security Pro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 Proの最新ビルドを使用することが重要です。新しいバージョンの有無を確認するには、メインメニューで[**ホーム**]をクリックします。新しいビルドが入手可能な場合、メッセージが表示されます。[**詳細を見る...**]をクリックすると、新たなウィンドウに新ビルドのバージョン番号と変更内容が表示されます。

[**はい**]をクリックして最新ビルドをダウンロードするか、[**後で**]をクリックしてウィンドウを閉じ、後でアップグレードをダウンロードします。

[**はい**]をクリックした場合、ファイルはdownloadsフォルダー(またはブラウザーが設定する既定のフォルダー)にダウンロードされます。ファイルのダウンロードが完了したら、そのファイルを実行し、表示されるインストール手順に従ってください。ユーザー名とパスワードは、新しくインストールされたバージョンに自動的に引継がれます。アップグレードの有無は定期的に確認してください▯CDまたはDVDからESET Cyber Security Proをインストールした場合は特に、定期的に確認することをお勧めします。

システム更新

macOSシステムアップデート機能は、悪意のあるソフトウェアからユーザーを保護するための重要なコンポーネントです。最大限のセキュリティのために、更新が利用可能になった時点でただちにインストールすることをお勧めします。更新通知の利用可能状況を調整するには、[**設定**] > [**詳細設定を表示する...**](または*cmd+,*を押す) > [**警告と通知** > **設定...**]で、[**未適用のアップデート**]の横の[**表示条件**]をクリックします。

- **すべてのアップデートを表示** – システム更新が見つからない場合は、必ず通知が表示されます。
- **推奨のみを表示** – 推奨更新のみが通知されます。

見つからない更新の通知を表示しない場合は、[**未適用のアップデート**]の横のチェックボックスをオフにします。

通知ウィンドウには▯macOSオペレーティングシステムで利用可能な更新の概要と、macOSネイティブツールのソフトウェア更新で更新されたアプリケーションが表示されます。通知ウィンドウまたは[**未適用**

のアップデート］をクリックして□ESET Cyber Security Proの［**Home**］セクションから直接更新を実行できます。

通知ウィンドウには、アプリケーション名、バージョン、サイズ、プロパティ(フラグ)、および利用可能な更新の詳細が表示されます。［フラグ］列には、以下の情報が含まれます。

- ［**推奨**］－オペレーティングシステムの製造元は、システムのセキュリティと安定性を高めるために、この更新をインストールすることを推奨しています。
- ［**再起動**］－インストール後にコンピューターの再起動が必要です。
- ［**シャットダウン**］－インストール後にコンピューターをシャットダウンし、電源を入れ直す必要があります。

通知ウィンドウには□□softwareupdate□コマンドラインツールで取得された更新が表示されます。このツールで取得された更新は、「ソフトウェア更新」アプリケーションで表示される更新とは異なる場合があります。「未適用のシステムアップデート」ウィンドウで表示されるすべての利用可能な更新をインストールし、「ソフトウェア更新」アプリケーションで表示されない場合は、□softwareupdate□コマンドラインツールを使用する必要があります。このツールの詳細については、［ターミナル］ウィンドウにman softwareupdateと入力し、□softwareupdate□のマニュアルをお読みください。これは上級ユーザーにのみ推奨されます。

ツール

[**ツール**］メニューには、プログラム管理を容易にし、上級ユーザー用の追加オプションを提供する機能を含みます。

ログファイル

ログファイルには、発生した全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、検出された脅威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 Pro環境から直接、ログをアーカイブするだけでなく、テキストメッセージとログを表示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 Pro のメインメニューで［ **ツール**]□[**ログ**］の順にクリックします。ウィンドウの最上部にある［**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。

1. **検出された脅威** － このオプションを選択すると、マルウェアの検出に関連するイベントに関する全ての情報が表示されます。
2. **イベント** － このオプションは、システム管理者およびユーザーが問題を解決するために使用します。イベントログには□ESET Cyber Security Pro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。
3. **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。
4. **ペアレンタルコントロール** － ペアレンタルコントロールにブロックされたWebページのリスト。
5. **パーソナルファイアウォール** － このログには、ネットワーク関連のイベントの結果が含まれます。
6. **フィルタリングされたWebサイト** - Webアクセス保護でブロックされたWebサイトのリストを表示する場合は、このリストが便利です。これらのログでは、特定のWebサイトへの接続が開かれた時刻□

URL□ステータス□IPアドレス、ユーザー、アプリケーションが表示されます。

各セクションで、エントリーを選択し、[**コピー**]ボタンをクリックすると、表示されている情報をクリップボードに直接コピーすることができます。

ログの保守

ESET Cyber Security Proのログの設定には、プログラムのメインウィンドウからアクセスすることができます。[**設定**] > [**詳細設定を表示する**]（または*cmd+,*を押す）> [**ログファイル**]をクリックします。ログファイルの次のオプションを指定することができます。

- **古いログレコードを自動的に削除する** – 指定した日数より古いログエントリが自動的に削除されます（既定は90日）。
- **ログファイルを自動的に最適化する** – 未使用のレコードが指定した割合を超えると、ログファイルが自動的に最適化されます（既定は25%）。

グラフィカルユーザーインターフェイスに表示されるすべての関連情報、脅威、およびイベントメッセージは、プレーンテキストやCSV(Comma-separated values)などの人間が読み取れるテキスト形式で保存できます。これらのファイルをサードパーティ製のツールを使用して処理できるようにするには、[**テキストファイルへのログ記録を有効化する**]の横のチェックボックスをオンにします。

ログファイルの保存先フォルダを定義するには、[**詳細オプション**]の横の[**設定**]をクリックします。

[**テキストログファイル:編集**]の下で選択したオプションに基づいて、次の書き込まれた情報とともにログを保存できます。

- o無効なユーザー名とパスワード□モジュールを更新できませんなどのイベントは、eventslog.txtファイルに書き込まれます。
- o起動時検査、リアルタイム保護、またはコンピュータ検査によって検出された脅威はthreatslog.txtファイルに保存されます。
- oすべての完了した検査の結果は、scanlog.番号.txtの形式で保存されます。
- oファイアウォール経由の通信に関連するすべてのイベントはfirewalllog.txtに書き込まれます。

[**既定のコンピューター検査ログレコード**]のフィルターを設定するには、[**編集**]をクリックし、必要に応じてログの種類を選択または選択解除します。これらのログタイプの詳細については、ログフィルタリングを参照してください。

ログのフィルタリング

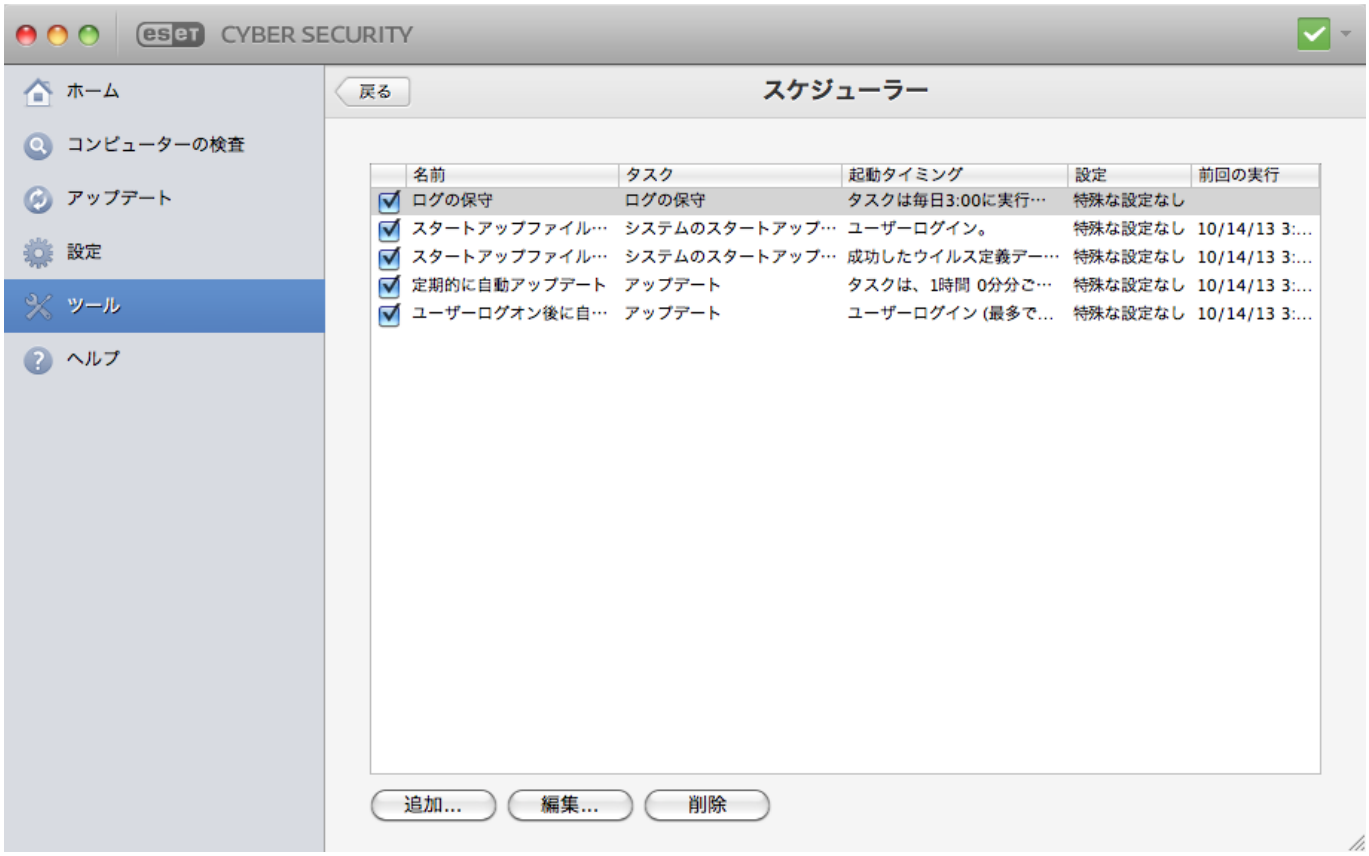
ログには、重要なシステムイベントに関する情報が格納されています。ログフィルタリング機能では、特定の種類のイベントに関するレコードを表示することができます。

最も頻繁に使用されるログの種類は以下のとおりです。

- **重大な警告** – 重大なシステムエラー（ウイルス・スパイウェア対策の起動に失敗したなど）。
- **エラー** - "ファイルのダウンロードエラー"などのエラーメッセージと重大なエラー。
- **警告** – 警告メッセージ。
- **情報レコード** – アップデートの正常完了や警告などの通知情報。
- **診断レコード** – プログラムの微調整に必要な情報および上記の全てのレコード。

スケジューラ

[**スケジューラ**]はESET Cyber Security Proのメインメニューの[**ツール**]にあります。**スケジューラ**には、スケジュール済みの全てのタスクと設定プロパティ(あらかじめ定義した日付、時刻、使用する検査プロファイルなど)の一覧が表示されます。



スケジューラでは、スケジュールされたタスクが、あらかじめ定義された設定やプロパティと共に管理され、開始されます。設定およびプロパティには、日時のほか、タスクの実行時に使用される所定のプロファイルなどの情報が含まれます。

既定では、次のスケジュールされたタスクがスケジューラに表示されます。

- ログの保守(スケジューラの設定で[**システムタスクを表示する**]オプションを有効にした後)
- 起動ファイルの検査(ユーザーのログオン後)
- スタートアップファイルのチェック (検出エンジンの正常なアップデート後)
- 定期的に自動アップデート
- ユーザーログオン後に自動アップデート

既存のスケジュールされたタスク(既定のタスクおよびユーザー定義のタスク)の設定を編集するにはCtrlキーを押して、変更するタスクをクリックし、[**編集**]を選択するか、あるいはタスクを選択して[**タスクの編集...**]ボタンをクリックします。

新しいタスクの作成

スケジューラで新しいタスクを作成するには、[**追加**]ボタンをクリックするか、またはCtrlキーを押してブランクのフィールド内をクリックし、コンテキストメニューから[**追加...**]を選択します。 次の5

種類のスケジュールされたタスクが使用可能です。

- **アプリケーションの実行**
- **アップデート**
- **ログの保守**
- **コンピュータの検査**
- **システムのスタートアップファイルのチェック**

アプリケーションの実行

[**Run application**]を選択すると□□nobody□システムユーザーとしてプログラムを実行できます。 スケジューラーでアプリケーションを実行するための権限は、macOSで定義されます。既定のユーザーから変更するには、ユーザー名、コロン(:)、コマンドの順に入力します。この機能では、**root**ユーザーを使用することもできます。

例: ユーザーとしてタスクを実行

この例では、電卓アプリをスケジュールし、選択した時刻にユーザー**UserOne**として起動するようにします。

1.**スケジューラー**で**タスクの追加**を選択します。
2.タスク名を入力します。 **スケジュールされたタスク**として**アプリケーションの実行**を選択します。 **タスクの実行**ウィンドウで、**1回**を選択して、このタスクを1回実行します。[**次へ**]をクリックします。
3.[参照]をクリックし、電卓アプリを選択します。
4.アプリケーションパスの前に**UserOne:**を入力(UserOne:'/Applications/Calculator.app/Contents/MacOs/Calculator')し、**次へ**をクリックします。
5.タスクを実行する時刻を選択し、**次へ**をクリックします。
6.タスクを実行できない場合は、代替オプションを選択し、**次へ**をクリックします。
7.[**完了**]をクリックします。
8.ESETスケジューラーにより、選択した時刻に電卓アプリが起動します。

例: 更新タスク

この例では、指定された時刻に実行される更新タスクを作成します。

1.[**スケジュールタスク**]ドロップダウンメニューから[**アップデート**]を選択します。
2.[**タスク名**]フィールドにタスクの名前を入力します。
3.[**実行タスク**]ドロップダウンメニューからタスクの頻度を選択します。 選択された頻度に基づいて、さまざまなアップデートパラメーターを指定するように指示されます。[**ユーザー定義**]を選択すると□cronフォーマットで日付/時刻を指定するためのプロンプトが表示されます(詳細については「ユーザー定義タスクの作成」セクションを参照してください)。
4.次のステップで、スケジュールされた時刻にタスクを実行できない場合や完了できない場合に実行するアクションを定義します。
5.最後のステップでは、現在のスケジュールされたタスクに関する情報の概要のウィンドウが表示されます。 [**完了**]をクリックします。 新しくスケジュールされたタスクが、現在スケジュールされているタスクのリストに追加されます。

既定では□ESET Cyber Security Proには、製品を正常に機能させるため、いくつかの重要なタスクがあらかじめスケジュール設定されています。 これらのタスクは、不用意に変更されないように既定では非表示にされています。 これらのタスクを表示するには、メインメニューから[**設定**] > [**詳細設定を表示する ...**](または*cmd+,*を押す) > [**スケジューラ**]をクリックし、[**システムタスクを表示する**]を選択します。

ディレクトリ所有者として検査

次のディレクトリの所有者として、ディレクトリを検査できます。

```
root:for VOLUME in /Volumes/*; do sudo -u \#`stat -
f %u "$VOLUME"` '/Applications/ESET Cyber Security.app/Contents/MacOS/esets_scan' -
f /tmp/scan_log "$VOLUME"; done
```

また、現在のログインユーザーとして、 `/tmp` フォルダーを検査することもできます。

```
root:sudo -u \#`stat -
f %u /dev/console` '/Applications/ESET Cyber Security.app/Contents/MacOS/esets_scan'
 /tmp
```

ユーザー定義タスクの作成

[**ユーザー定義タスク**]の日付および時刻は、4桁の西暦でのcronフォーマット(スペース区切りの6つのフィールドで構成される文字列)で入力する必要があります。

分(0-59)時(0-23)日(1-31)月（1-12)年(1970-2099)曜日(0-7)(日曜 = 0 または 7)

例:

```
30 6 22 3 2012 4
```

cron表現では、以下の特殊文字がサポートされています:

- アスタリスク(*) - 表現はフィールドのすべての値に一致します。例：3つ目のフィールド(日)にアスタリスクがある場合、毎日となります
- ハイフン(-) - 範囲を指定します。例：`3-9`
- カンマ(,)- リストの項目を区切ります。例：`1,3,7,8`
- スラッシュ(/) - 範囲の増分を定義します。例：`3-28/5`。3つ目のフィールド(日にち)では、月の第3日、その後5日ごととなります。

曜日名 (Monday-Sunday) と月名 (January-December) はサポートされていません。

> **コマンドの実行**
> 日および曜日の両方を定義すると、コマンドは両フィールドが一致するときのみに実行されます。

隔離

隔離の主な目的は、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 Pro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。

任意のファイルを選択して隔離することができます。これは、ファイルの動作が疑わしいにもかかわらず、ウイルス対策機能によって検出されない場合にお勧めします。隔離したファイルは、ESETのウイルスラボに提出して分析を受けることができます。

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(複数のマルウェアを含むアーカイブかどうかなど)を表示するテーブルで見ることができます。隔離ファイルを収容した隔離フォルダー（）はアンインストールした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 Proのインストール後に再度復元できます。

ファイルの隔離

削除されたファイルは、ESET Cyber Security Proにより自動的に隔離されます(警告ウィンドウでユーザーがこのオプションをオフにしなかった場合)。**[隔離...]**をクリックすると、不審なファイルを手動で隔離できます。. この操作にはコンテキストメニューも使用することができます。Ctrlキーを押し、空欄のフィールド内をクリックし、[**隔離**]を選択してから、隔離するファイルを選択し、[**開く**]をクリックします。

隔離フォルダーからの復元

隔離されたファイルを元のファイルに復元するには、隔離されたファイルを選択し、**[復元]**をクリックします。コンテキストメニューからも復元を実行できます。CTRLキーを押しながら、[隔離]ウィンドウの特定のファイルをクリックし、**[復元]**をクリックします。コンテキストメニューには、[**復元先を指定...**]オプションもあります。このオプションを使用すると、隔離される前の場所とは異なる場所にファイルを復元することができます。

隔離フォルダー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脅威ラボに送信してください。隔離フォルダからファイルを提出するにはCTRLキーを押しながらファイルをクリックし、コンテキストメニューから[**分析のためにファイルを提出**]を選択します。

実行中のプロセス

[**実行中のプロセス**]の一覧には、コンピューターで実行中のプロセスが表示されます。ESET Cyber Security Proは、ユーザーをESET Live Grid技術で保護するために、実行中のプロセスに関する詳細情報を提供します。

- **プロセス** – 現在コンピューターで実行中のプロセスの名前。実行中のすべてのプロセスを表示するには、アクティビティ監視機能(*/Applications/Utilities*で見つかります)を使用することもできます。
- **リスクレベル** – ほとんどの場合、ESET Cyber Security ProおよびESET Live Grid技術では、各オブジェクトの特性を検査してから悪意のあるアクティビティの可能性を判定する一連のヒューリスティックルールを使用して、オブジェクト(ファイル、プロセスなど)にリスクレベルを割り当てます。これらのヒューリスティックにより、オブジェクトにはリスクレベルが割り当てられます。緑でマークされた既知のアプリケーションはクリーン(ホワイトリストに入っている)であり、検査から除外されます。これにより、オンデマンドおよびリアルタイムの検査の速度が向上します。不明(黄色)とマークされたアプリケーションは、必ずしも悪意を持ったソフトウェアであるとは限りません。通常、これは単に新しいアプリケーションです。ファイルについて不明な場合は、分析のためにESET脅威ラボに送信

できます。ファイルが悪意のあるアプリケーションであるとわかった場合は、シグネチャがその後のアップデートのいずれかに追加されます。

- **ユーザー数** – 特定のアプリケーションを使用するユーザーの数。この情報はESET Live Grid技術によって収集されます。
- **動作期間** – アプリケーションがESET LiveGrid®技術によって発見されてからの時間。
- **アプリケーションバンドルID** – ベンダーまたはアプリケーションプロセスの名前。

特定のプロセスをクリックすると、次の情報がウィンドウの下部に表示されます。

- **ファイル** – コンピュータ上のアプリケーションの場所
- **ファイルサイズ** – ディスク上のファイルの物理サイズ
- **ファイルの説明** – オペレーティングシステムからの説明に基づくファイルの特性
- **アプリケーションバンドルID** – ベンダーまたはアプリケーションプロセスの名前
- **ファイルのバージョン** – アプリケーション発行元からの情報
- **製品名** – アプリケーション名またはビジネス名

ネットワーク接続

ネットワーク接続は、コンピューター内のアクティブなネットワーク接続のリストですESET Cyber Security Proは、各接続に関する詳細情報を示し、これらの接続をブロックするルールを作成できるようにします。

この接続のブロックルールを作成する

ESET Cyber Security Proでは、**ネットワーク接続**マネージャーの各接続に対してブロックルールを作成できます。 ブロックルールを作成するには、接続を右クリックし、**この接続のブロックルールを作成**を選択します。

1.ルールに作成する接続**プロファイル**を選択し、ルールの名前を入力します。 ルールが適用されるアプリケーションを選択するか、チェックボックスを選択して、ルールがすべてのアプリケーションに適用されるようにします。

2.接続のアクションを選択します。接続を拒否(ブロック)するか、許可します。 ルールが適用される通信の方向を選択します。 ルールのログファイルを作成するには、**ログルール**をクリックします。

3.接続プロトコルとポートタイプを選択します。 サービスのポートを選択するか、開始ポートと終了ポートの形式を使用してポート範囲を指定します。

4.宛先を選択し、宛先に応じて必須フィールドに情報を入力します。

Live Grid

Live Grid早期警告システムは、新しいマルウェアについての情報を即座に継続的にESETに提供し続けます。双方向のLive Grid早期警告システムの目的は、ESETが提供する保護を改善することです。新しい脅威が出現したらただちに確実に確認するための最善の方法は、できる限り多くのユーザーとつながり、脅威スカウトとしてユーザーを使用することです。2つのオプションがあります。

1.Live Grid早期警告システムを無効にするように決めることができます。この場合でも、ソフトウェ

アにおけるどのような機能も失わずに、当社が提供する最良の保護を受けることができます。

2.脅威を与える新たなコードが含まれる新しい脅威についての匿名情報を提出するようにLive Grid早期警告システムを設定することができます。この情報は詳細分析のためにESETに送信されます。これらの脅威について検討することはESETが検出エンジンを更新し、プログラムの脅威検出能力を向上させるのに役立ちます。

Live Grid早期警告システムは、新たに検出された脅威に関連する情報を収集します。この情報には、ウイルスが検出されたファイルのサンプルまたはコピー、そのファイルのパス、ファイル名、日時、ウイルスがコンピューターに侵入したプロセス、およびコンピューターのオペレーティングシステムについての情報が含まれます。

この結果、ユーザーやコンピューターに関する情報（マルウェアが検出された箇所のファイルパスなど）がESETのウイルスラボに提出されますが、これらの情報が新しいウイルスに迅速に対応するため以外の目的で使用されることはありません。

メインメニューからLive Gridにアクセスするには、[**設定**] > [**詳細設定を表示する ...**]（または*cmd+,*を押す）> [**Live Grid**]をクリックします。[**Live Grid早期警告システムを有効化する**]を選択してLive Gridを有効化し、次に[**詳細設定オプション**]の横の[**設定...**]をクリックします。

Live Gridの設定

既定では、不審なファイルは詳細な分析を受けるためにESET脅威ラボに提出するようにESET Cyber Security Proが設定されます。これらのファイルを自動的に提出しない場合は、[**ファイルの提出**]をオフにします。

不審なファイルがある場合は、ESETのウイルスラボに提出して分析を受けることができます。そのためには、メインプログラムウィンドウから[**ツール**] > [**分析のためにサンプルを提出**]をクリックします。そのファイルが悪意のあるアプリケーションであることが判明すると、次のアップデートにその検出が追加されます。

匿名統計情報の提出 - Live Grid早期警告システムは、新しく検出された脅威に関係するコンピューターの情報を匿名で収集します。この情報には、マルウェアの名前、マルウェアが検出された日時ESETセキュリティ製品のバージョン、オペレーティングシステムのバージョン、およびローカル設定が含まれます。統計は通常、1日1回または2回、ESETのサーバーに配信されます。

除外フィルタ – このオプションを使用すると、特定のファイルの種類を提出から除外することができます。たとえば、ドキュメントやスプレッドシートなど、機密情報が含まれている可能性があるファイルを除外すると便利です。なお、最も一般的なファイルの種類(.doc.rtfなど)は、既定で除外されます。除外するファイルの一覧にファイルの種類を追加できます。

連絡先の電子メールアドレス(任意) – 分析用に追加情報が必要な場合は、お客様の電子メールアドレスを使用することがあります。詳細情報が不要な場合は、ESETから応答を受信することはありません。

分析のためにサンプルを提出

コンピューター上の疑わしいファイルが見つかった場合は、ESETのリサーチラボに提出して解析を受けることができます。

ESETにファイルを提出する前に

次の条件の1つ以上を満たさないかぎり、サンプルを送信しないでください。
- このサンプルがESET製品でまったく検出されない
- サンプルが誤ってウイルスとして検出される
- (ESETでのマルウェア検査を希望する)個人のファイルはサンプルとして許可されません(ESETリサーチラボはユーザーのオンデマンド検査を実行しません)
- わかりやすい件名にし、ファイルに関する情報(ダウンロード元のスクリーンショットやWebサイトなど)をできるだけ多く記載してください。

サンプルを送信するには、製品のサンプル送信フォームを使用します。**ツール > 分析のためにサンプルを提出**にあります。

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。

ファイル – 提出するファイルへのパスを入力します。

コメント –ファイルを提出する理由を説明します。

連絡先のメールアドレス – 不審なファイルと共に連絡先のメールアドレスをESETに送信します。解析のために詳しい情報が必要な場合、このメールアドレスに連絡がある場合があります。メールアドレスの入力は任意です。

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、何万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。

ユーザーインターフェイス

ユーザーインターフェイスの設定オプションを使用すると、各自のニーズに合わせて作業環境を調整することができます。これらのオプションは[**設定**] > [**詳細設定を表示する ...**](または*cmd+,*を押す) > [**インターフェイス**]をクリックし、メインメニューからアクセスできます。

- システムの起動時にESET Cyber Security Proスプラッシュウィンドウ機能を表示するには、[**起動時にスプラッシュウィンドウを表示する**]を選択します。
- [**アプリケーションをドックに表示する**]を使用すると、 *cmd+tab*を押してmacOS DockでのESET Cyber Security Proアイコンを表示し、ESET Cyber Security Proとその他の動作アプリケーションの間で切り替えを行うことができます。変更点はESET Cyber Security Proの再起動(通常はコンピューターの再起動によって行います)後に有効になります。
- [**標準メニューを使用**]オプションを使用すると、特定のショートカットキーを使用し(ショートカットキーを参照)、(画面の上部にある)Mac OSメニューバーに標準メニュー項目([ユーザーインターフェイス]、[設定]、および[ツール])が表示されます。
- ESET Cyber Security Proの特定のオプションに対するツールヒントを有効にするには、[**ツールヒントの表示**]を選択します。
- [**隠しファイルを表示する**]を選択すると、[**コンピューターの検査**]の[**検査の対象**]設定で隠しファイルを表示して選択することができます。
- 既定ではESET Cyber Security Proアイコンが、macOSメニューバー(画面上部)の右に表示されるメ

ニューバ⍰Extrasに表示されます。これを無効にするには、[**メニューバーにアイコンを表示する**]をオフにします。変更点はESET Cyber Security Proの再起動（通常はコンピューターの再起動によって行います）後に有効になります。

警告と通知

[**警告と通知**]セクションでは、脅威の警告やシステム通知をESET Cyber Security Proでどのように処理するかを設定することができます。

[**警告ウィンドウを表示**]を無効にすると、すべての警告ウィンドウが表示されなくなります。この設定が推奨されるのは、特定の限られた状況のみです。ほとんどのユーザーには、既定の設定のままにすることをお勧めします(チェックボックスをオンにします)。詳細オプションは、この章で説明します。

[**デスクトップに通知を表示する**]を選択すると、ユーザーの操作が不要な警告ウィンドウをデスクトップに表示できます(既定では画面の右上端)。通知の表示時間を定義するには、[**次の後に通知を自動的に閉じる**] X [**秒**]の値を調整します(既定は5秒)。

ESET Cyber Security Proバージョン6. 2以降では、特定の**保護ステータス**をプログラムのメイン画面(**保護ステータス**ウィンドウ)に表示しないようにできます。詳細については、保護ステータスを参照してください。

警告ウィンドウを表示する

ESET Cyber Security Proは、 新しいプログラムバージョン、オペレーティングシステムアップデート、特定プログラムコンポーネントの無効、ログの削除などについてユーザーに通知する警告ダイアログウィンドウを表示します。[**今後このダイアログを表示しない**]を選択して、それぞれの通知が行われないようにすることができます。

[**ダイアログの一覧**] ([**設定**] > [**詳細設定を表示する...**] > [**警告と通知**] > [**設定...**])は⍰ESET Cyber Security Proによって起動されるすべての警告ダイアログを表示します。各通知を有効または無効にするには、[**ダイアログ名**]の左のチェックボックスをオンにします。また、新しいプログラムバージョンとオペレーティングシステムアップデートの通知が表示される[**表示条件**]を定義することができます。

保護状態

ESET Cyber Security Proの現在の保護ステータスを変更するには、[**設定**] > [**アプリケーション環境設定の入力...**]> [**アラートと通知**] > [**保護ステータス画面に表示:設定**]を有効または無効にします。さまざまなプログラム機能のステータスは、ESET Cyber Security Proメイン画面(**保護ステータス**ウィンドウ)で表示または非表示になります。

次のプログラム機能の保護ステータスを非表示にできます。

- ファイアウォール
- フィッシング対策
- Webアクセス保護
- 迷惑メール対策機能
- オペレーティングシステムアップデート
- ライセンスの期限が切れました!

- コンピュータの再起動が必要

権限

ESET Cyber Security Proの設定は組織のセキュリティポリシーにとって非常に重要です。 許可なく変更が行われた場合は、システムの安定性と保護が危険にさらされる可能性があります。 このため、プログラム設定を編集する権限を持つユーザーを定義できます。

特権ユーザーを指定するには、[**設定**] > [**詳細設定を表示する...**]（または*cmd+,*を押す）> [**権限**]をクリックします。 左のリストからユーザーまたはグループを選択し、[**追加**]をクリックします。 全てのシステムユーザー/グループを表示するには、[**全ユーザー/グループを表示**]を選択します。 ユーザーを削除するには、右側の[**選択したユーザー**]一覧でユーザー名を選択し、[**削除**]をクリックします。

アップグレード
[選択したユーザー]の一覧を空のままにすると、すべてのユーザーに権限があると判断されます。

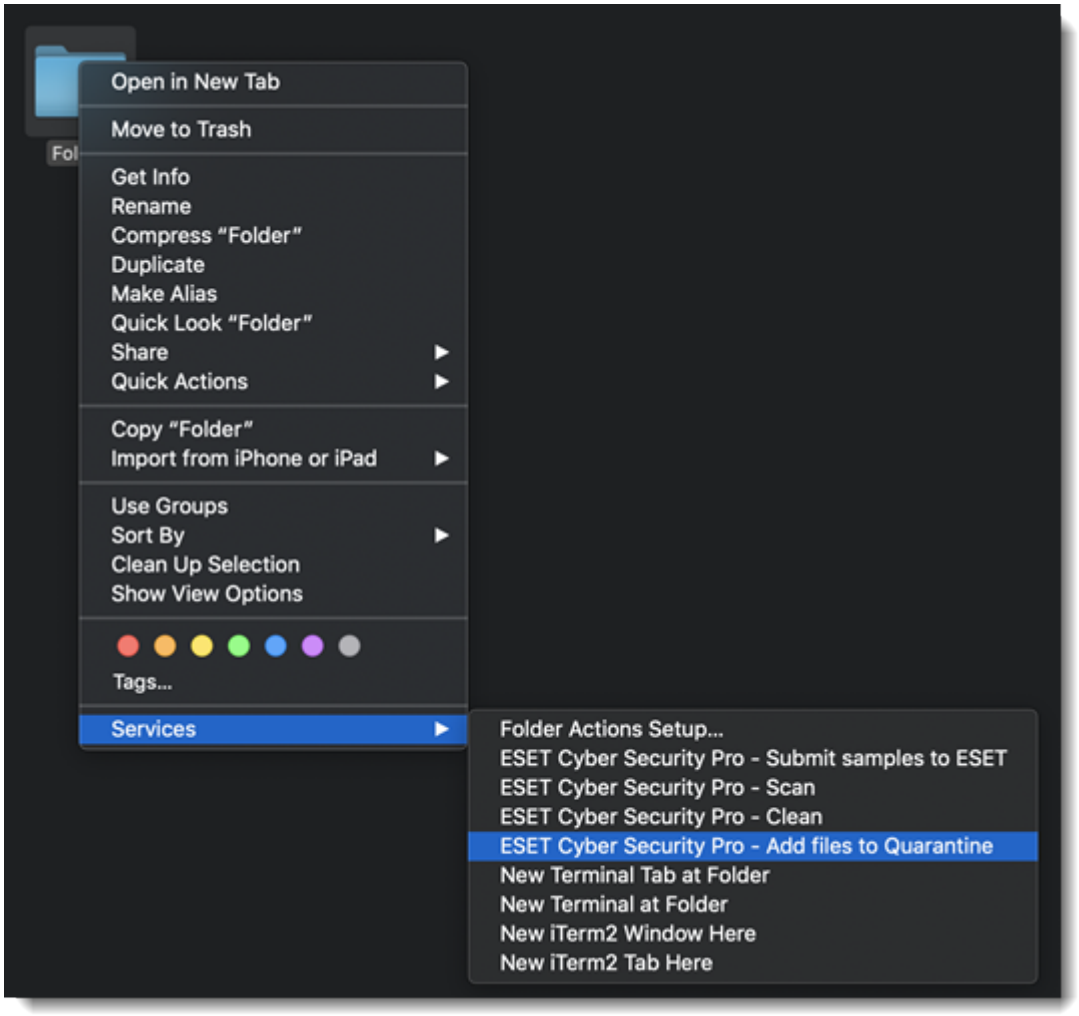
コンテキストメニュー

コンテキストメニューの統合を有効にするには、[**コンテキストメニューに統合**]を選択し、[**設定**] > [**詳細設定を表示する ...**]（または*cmd+,*を押す）> [**コンテキストメニュー**]をクリックします。 変更を有効にするには、ログアウトするか、コンピューターを再起動する必要があります。 コンテキストメニューのオプションは、Ctrlキーを押しながら任意のファイルをクリックすると、[**Finder**]ウィンドウで使用できます。

コンテキストメニューに表示されるオプションを選択できます。**検査のみ**オプションを表示できます。これは、選択したファイルを検査できます。**駆除のみ**オプションは、選択たファイルをコンテキストメニューから駆除できます。ウイルスが悪意のあるコードをファイルに添付して攻撃している場合に、駆除を行います。この場合、ファイルを元の状態に戻すため、まず感染しているファイルからのウイルスの駆除を試みます。ファイルが悪意のあるコードのみで構成されている場合には、ファイル全体が削除されます。

すべてオプションを選択すると、コンテキストメニューから次のタスクを実行できます。

- ESETにサンプルを提出
- 検査
- 感染していません
- ファイルを隔離フォルダに追加する



設定をインポートおよびエクスポートする

既存の構成をインポートするか、ESET Cyber Security Pro構成をエクスポートするには、**[設定]** > **[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、後日使用するためにESET Cyber Security Pro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 Proの好み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、**[参照]**をクリックして、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]**をクリックし、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上の場所を選択します。

プロキシサーバーの設定

プロキシサーバの設定は[**設定**]>[**アプリケーション設定を入力する ...**](*cmd+,*を押すか）>[**プロキシサーバー**]で行えます。プロキシサーバをこのレベルで指定すると□ESET Cyber Security Proのすべての機能に対するプロキシサーバーのグローバル設定が指定されることになります。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□ESET Cyber Security Proは、Basic AccessおよびNTLM (NT LAN Manager)タイプの認証をサポートします。

プロキシサーバー設定をこのレベルで指定するには、[**プロキシサーバーを使用する**]を選択し、プロキシサーバーのIPアドレスまたはURLを[**プロキシサーバー**]フィールドに入力します。[ポート]フィールドには、プロキシサーバーが接続を許可するポートを指定します(既定では3128です)。**[検出]**をクリックして、プログラムによって両方のフィールドを入力することもできます。

プロキシサーバーとの通信に認証が必要な場合は、有効な**ユーザー名**と**パスワード**を入力します。

エンドユーザーライセンス契約

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、次の項目に同意したことになります**プライバシーポリシー□

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（以下「本契約」とします）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.□またはESETグループ内の別企業（以下□ESET□または「供給者」とします）と、自然人または法人であるお客様（以下「お客様」または「エンドユーザー」とします）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するものとします。本契約の規定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入手元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-ROM□DVD□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) **Business Edition**本ソフトウェアをメールサーバー、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（以下「アップデート」とします）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。

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 URL IP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。お客様は、マーケティング情報を含む(ただしこれに限定されない)通知およびメッセージを受信することに同意します。

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、本ソフトウェアを使用したことにより、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。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(「関連会社」)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(「輸出貿易管理法」)。

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(「制裁法」)。

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、返却される本ソフトウェアおよび本件ドキュメントは、スロバキア共和国, ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic

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。本契約に対するいかなる修正も、書面によってしか行うことができず、当該修正は、供給者の正式な代表者か、委任状の条項でこの役割を果たすことが明示的に認められた代理人によって署名されなければなりません。

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。

EULA ID: HOM-ECS-20-01

プライバシーポリシー

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: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」)は、お客様の個人データとプライバシーの処理に関して透明でありたいと考えています。この目標を達成するために、当社は、お客様(「エンドユーザー」または「お客様」)に次の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、
- データの機密保持、
- データの主体の権利。

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(EULA)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、アップデート/アップグレードサービス ESET LiveGrid® データの悪用に対する保護、サポートなど、エンドユーザーライセンス契約および製品資料に記載されているさまざまなサービスを提供します。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ID IP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。これにより 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
  - o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

o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

oIP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

o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。

データの機密保持

ESETは、販売、サービス、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経由で、世界中で事業を展開している会社ですESETによって処理された情報は、サービスの提供、サポート、または請求などのEULAの履行のため、関連会社またはパートナー企業との間で転送される場合があります。選択した位置情報およびサービスに基づき、欧州委員会の適切な決定権がない国にお客様のデータを転送する必要がある場合があります。この場合でも、情報を転送するたびに、データ保護法の規制が適用され、必要な場合にのみ実行されます。標準契約条項、拘束的企業準則、または他の適切な安全保護対策を例外なく確立する必要があります。

ESETは、エンドユーザーライセンス契約に従って、サービスを提供している間、必要最低限の期間にのみデータが保存されるように最善の努力を講じますESETの保持期間は、お客様が簡単かつスムーズな更新が行える時間的余裕を用意するために、ライセンスの有効期間よりも少し長くなる場合がありますESET LiveGrid®からの最小化および仮名化された統計情報および他のデータが統計目的で処理される場合があります。

ESETは、適切な技術的および組織的な対策を導入し、潜在的なリスクに適したレベルのセキュリティを保証します。当社は最善を尽くし、処理システムおよびサービスに関する、継続中の機密性、完全性、可用性、および障害回復力を保証します。ただし、お客様の権利と自由を脅かす結果になるデータ違反の場合には、すぐに監督当局とデータ主体に通知します。データ主体として、お客様は、監督当局に苦情を申し立てる権利を有します。

データの主体の権利

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。適用されるデータ保護法で規定された条件が適用されます。お客様は、データ主体として、次の権利を有しています。

- ESETに対してお客様の個人データへのアクセスを要求する権利、
- 不正確な個人データを修正する権利(不完全な個人データを完全にする権利もあります)
- 個人データの消去を要求する権利、

- 個人データの処理の制限を要求する権利
- 処理に異議を申し立てる権利
- 苦情を申し立てる権利および
- データ移植性の権利。

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