ESET Endpoint Security for macOS

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。

Copyright ©2023 by ESET, spol. s r.o.

ESET Endpoint Security for macOS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。

All rights reserved.本ドキュメントのいかなる部分も、作成者の書面による許可がない場合、電子的、機械的、複写、記録、スキャンなど、方法または手段の如何をと遭わず、複製、検索システムへの保存、または転送が禁じられています。

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: 2023年/3月/19日

1 ESET Endpoint Security for macOS 1
1.1 バージョン6の新機能 1
1.2 システム要件 2
2 ESET Security Management Center 経由で接続するユーザー 2
3 インストール 3
3.1 標準インストール 4
3.2 カスタムインストール 5
3.3 リモートインストール 8
4 製品のアクティベーション 9
5 アンインストール 10
6 基本概要 10
6.1 ショートカットキー 11
6.2 システムの動作の確認 11
6.3 プログラムが正しく動作しない場合の解決方法 12
7 コンピューターの保護 12
7.1 ウイルス・スパイウェア対策 12
7.1 全般 13
7.1 除外 13
7.1 スタートアップ保護 14
7.1 リアルタイムファイルシステム保護 14
7.1 詳細設定オプション 15
7.1 リアルタイム保護の設定の変更 15
7.1 リアルタイム保護の確認 15
7.1 リアルタイム保護が機能しない場合の解決方法 16
7.1 コンピューターの検査 17
7.1 検査の種類 17
7.1 Smart検査 18
7.1 カスタム検査 18
7.1 検査の対象 18
7.1 検査プロファイル 18
7.1 ThreatSenseエンジンのパラメーターの設定 19
7.1 検査対象 20
7.1 オプション 20
7.1 駆除 21
7.1 除外 21
7.1 制限 22
7.1 その他 22
7.1 侵入物が検出された 23
7.2 Webとメール保護 23
7.2 Webアクセス保護 24
7.2 ポート 24
7.2 URLリスト 24
7.2 電子メール保護 25
7.2 POP3プロトコルチェック 26
7.2 IMAPプロトコルチェック 26
7.3 アンチフィッシング 26
8 ファイアウォール 27
8.1 フィルタリングモード 27
8.2 ファイアウォールルール 28
8.2 新規ルールの作成 29

8.3 ファイアウォールゾーン 29
8.4 ファイアウォールプロファイル 29
8.5 ファイアウォールログ 30
9 デバイスコントロール 30
9.1 ルールエディタ 31
10 Webコントロール 33
11 ツール 34
11.1 ログファイル 34
11.1 ログの保守 35
11.1 ログのフィルタリング 36
11.2 スケジューラ 36
11.2 新しいタスクの作成 38
11.2 ユーザー定義タスクの作成 39
11.3 LiveGrid® 40
11.3 不審なファイル 41
11.4 隔離 42
11.4 ファイルの隔離 42
11.4 隔離されたファイルの復元 42
11.4 隔離フォルダからのファイルの提出 42
11.5 権限 42
11.6 プレゼンテーションモード 43
11.7 実行中のプロセス 44
12 ユーザーインターフェイス 45
12.1 警告と通知 45
12.1 警告ウィンドウを表示する 46
12.1 保護状態 46
12.2 コンテキストメニュー 46
13 アップデート 47
13.1 アップデートの設定 47
13.1 詳細設定オプション 48
13.2 アップデートタスクの作成方法 49
13.3 システム更新 49
13.4 設定をインポートおよびエクスポートする 50
13.5 プロキシサーバーの設定 51
13.6 共有ローカルキャッシュ 51
14 End User License Agreement 52
15 プライバシーポリシー 58

ESET Endpoint Security for macOS

ESET Endpoint Security for macOS 6では、コンピュータのセキュリティに新しいアプローチで取り組んでいます。最新バージョンのThreatSense®検査エンジンはカスタムファイアウォール と統合され、高速かつ正確に、コンピュータを安全に保ちます。これにより、このインテリジェントシステムは、コンピュータにとって脅威となる可能性のある攻撃と不正ソフトウェアに対して常に警戒態勢を保ちます。

ESET Endpoint Security for macOS 6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。人工知能に基づく高度な技術は、システムのパフォーマンスを低下させたり、コンピュータを中断させることなく、ウイルス、スパイウェア、トロイの木馬、ワーム、アドウェア、ルートキット、およびその他のインターネット経由の攻撃の侵入を強力に阻止します。

本製品は、主に小規模ビジネス/企業環境のワークステーションでの使用を対象に設計されています。ESET Security Management Center 7と接続することにより、ネットワークに接続された任意のコンピュータからクライアントワークステーションをいくつでも簡単に管理し、ポリシーとルールの適用、検出の監視、変更のリモート管理が可能になります。

バージョン6の新機能

ESET Endpoint Security for macOSのグラフィカルユーザーインターフェイスは完全に新しいデザインになり、より高い可視性とより直感的なユーザー経験を実現します。バージョン6で導入されたさまざまな改良の例:

- ESET Enterprise Inspector support - ESET Endpoint Security for macOSバージョン6. 9以降ではESET Endpoint Security for macOSがESET Enterprise Inspectorに接続できますESET Enterprise Inspector (EEI)は、包括的なエンドポイント検出および応答システムであり、インシデント検出、インシデント管理と応答、データ収集、危険検出の指標、特異性の検出、動作検出、ポリシー違反などの機能がありますESET Enterprise Inspectorインストール方法、機能については、ESET Enterprise Inspectorヘルプをご覧ください。
- **64ビットアーキテクチャサポート**
- **ファイアウォール** – ログまたはIDS (Intrusion detection system)通知ウィンドウから直接ファイアウォールルールを作成し、ネットワークインターフェイスにプロファイルを割り当てられるようになりました。
- **Webコントロール** – 不適切または不快な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。
- **Webアクセス保護** - Webブラウザとリモートサーバー間の通信を監視します。
- **電子メール保護** - POP3とIMAPプロトコルで受信したメール通信を制御できます。
- **フィッシング対策保護** – 合法的なサイトを偽装した悪意のあるWebサイトへのアクセスを制限し、パスワードや他の機密情報を取得する試みに対して保護を提供します。
- **デバイスコントロール** – 拡張フィルタ/権限を検査、ブロック、または調整して、外部デバイスへのアクセス方法やその作業方法を定義できます。この機能は、製品バージョン6. 1以降で提供されて

います。

• **プレゼンテーションモード** - ESET Endpoint Security for macOSをバックグラウンドで実行し、ポップアップウィンドウとスケジュールタスクを抑制できます。

• **共有ローカルキャッシュ** – 仮想環境の検査速度を改善できます。

システム要件

ESET Endpoint Security for macOS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
OS	macOS 10.12以降
メモリ	300 MB
空きディスク容量	200 MB

ESET Security Management Center 経由で接続するユーザー

ESET Security Management Center 7は、1つの中央の場所からネットワーク環境にあるESET製品を管理できるアプリケーションです。ESET Security Management Center タスク管理システムでは、ESETセキュリティソリューションをリモートコンピューターにインストールし、新たな問題や脅威に迅速に対応することができます。ESET Security Management Center では、悪意のあるコードに対しての保護は提供せず、各クライアントのESETセキュリティソリューションに依存しています。

ESETセキュリティソリューションは、複数のタイプのプラットフォームを含むネットワークをサポートします。ネットワークは現在のMicrosoft、Linuxベース、Mac OSおよびモバイルデバイス(携帯電話やタブレット)上で実行されるオペレーティングシステムの組み合わせを含めることができます。

ESET Security Management Centerは、前のバージョンのESET Security Management Centerとは大きく異なる、次世代のリモート管理システムです。アーキテクチャが完全に異なるため、ESET Security Management Center 7は、ERA 6と完全には互換せず、ERA 5との後方互換性はありません。ただし、前のバージョンのESETセキュリティとの互換性は残ります。

新しいESET Security Management Centerとともに、ESETは新しいライセンスシステムの次世代セキュリティ製品を開発しました。

ESETセキュリティソリューションポートフォリオの完全な展開を実行するには、次のコンポーネントをインストールする必要があります(WindowsおよびLinuxプラットフォーム)。

- ESET Security Management Centerサーバー
- ESET Security Management Center Webコンソール

- ESET Management Agent

次の付属コンポーネントは任意です。ネットワーク上のアプリケーションの最善のパフォーマンスのためにインストールすることをお勧めします。

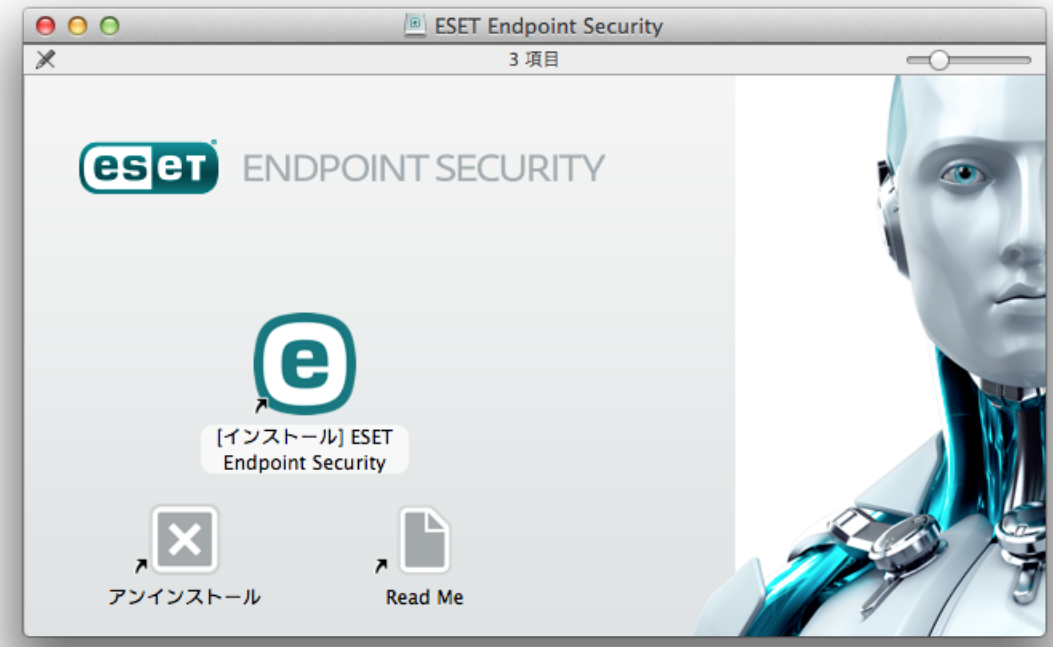
- プロキシ
- RD Sensor
- Apache HTTP Proxy
- モバイルデバイスコネクター

> **ESET Security Management Centerドキュメント**
> 詳細情報については、ESET Security Management Centerオンラインドキュメントを参照してください。

インストール

ESET Endpoint Security for macOSインストーラを実行するには2通りの方法があります。

- インストールCD/DVDからインストールしている場合は、ディスクをCD/DVD-ROMドライブに挿入し、ESET Endpoint Security for macOSインストールアイコンをダブルクリックして、インストールを起動します。
- 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、そのファイルをダブルクリックすると、インストーラーが起動します。



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。



.pkgファイルからのインストール
.pkgファイルからインストールされたmacOS版ESET製品のインストール中および初回起動中にはAppleがESETカーネル拡張の証明を検証できるようにmacでインターネットアクセスが必要です。

使用許諾契約書に同意した後、インストールの種類を以下から選択することができます。

- 標準インストール
- カスタムインストール
- リモートインストール

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。

ESET LiveGrid®

ESET LiveGrid®早期警告システムではESET製品がただちに継続的に新しい侵入を認識し、お客様を迅速に保護できることを保証しますLiveGrid®システムは新しい脅威をESET脅威ラボに送信し、そこで脅威が分析および処理されます。不審なファイルの送信に関する詳細設定を変更するには、**[設定]**をクリックします。詳細については、LiveGrid®を参照してくださいESET LiveGrid®が無効な場合は、ESET Endpoint Security for macOSにセキュリティアラートが表示されます。

望ましくない可能性があるアプリケーション

インストールプロセスの最後のステップでは、**望ましくない可能性があるアプリケーション**の検出を設定します。このようなアプリケーションは、必ずしも悪意があるとは限りませんが、オペレーティングシステムの動作に悪影響を及ぼす可能性があります。望ましくない可能性のあるアプリケーションは、その他のプログラムに組み込まれていることが多く、ダウンロードすることを選択します。インストールプロセス時には気付きにくいことがあります。これらのアプリケーションは通常インストール時に通知を表示しますが、同意なしにインストールできるので、ユーザーが安易にインストールしてしまうこともあります。

ESET Endpoint Security for macOSの最初のインストールの後:

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 Endpoint Security for macOS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 Endpoint Security for macOS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ではESET Endpoint Security for macOS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 Endpoint Security for macOS機能にアクセスするにはESET Endpoint Security for macOS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 Endpoint Security for macOS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 Endpoint Security for macOS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 Endpoint Security for macOS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。

プログラムコンポーネント

ESET Endpoint Security for macOSでは、一部のコアコンポーネントなしで製品をインストールできます(Webとメールメール保護など)。 製品コンポーネントの横のチェックボックスをオフにして、インストールから削除できます。

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するかどうかが不明な場合は、[**システム設定と同じ設定を使用する(推奨)**]を選択すると、現在のシステム設定を使用できます。

権限

次のステップでは、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 LiveGrid®早期警告システムではESET製品がただちに継続的に新しい侵入を認識し、お客様を迅速に保護できることを保証しますLiveGrid®システムは新しい脅威をESET脅威ラボに送信し、そこで脅威が分析および処理されます。不審なファイルの送信に関する詳細設定を変更するには、[**設定**]をクリックします。詳細については、LiveGrid®を参照してくださいESET LiveGrid®が無効な場合は、ESET Endpoint Security for macOSにセキュリティアラートが表示されます。

望ましくない可能性があるアプリケーション

インストールプロセスの次のステップでは、**望ましくない可能性のあるアプリケーション**の検出を設定します。このようなプログラムは、必ずしも悪意があるとは限りませんが、オペレーティングシステムの動作に悪影響を及ぼす可能性があります。これらのアプリケーションは、ダウンロードする他のプログラムにバンドルされていることが多く、インストールされても気付きにくいことがあります。これらのアプリケーションは通常インストール時に通知を表示しますが、同意なしにインストールできるので、ユーザーが安易にインストールしてしまうこともあります。

ネットワーク

ファイアウォールのフィルタリングモードを選択します。 詳細は、フィルタリングモードを参照してください。

ESET Endpoint Security for macOSの最初のインストールの後:

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 Endpoint Security for macOS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 Endpoint Security for macOS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ではESET Endpoint Security for macOS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 Endpoint Security for macOS機能にアクセスするにはESET Endpoint Security for macOS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 Endpoint Security for macOS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 Endpoint Security for macOS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 Endpoint Security for macOS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。

リモートインストール

インストールの前に

macOS 10.13以降にESET Endpoint Security for macOSをインストールする前に、macOS 10.14以降でESETカーネル拡張を許可し、ターゲットコンピューターでのフルディスクアクセスを許可することをお勧めします。インストール後にこれらのオプションを許可するとESETカーネル拡張とフルディスクアクセスが許可されるまで、**システム拡張がブロックされました**および**コンピューターは一部しか保護されていません**という通知がユーザーに表示されます。

ESETカーネル拡張とフルディスクアクセスをリモートで許可するには、コンピューターをJamfなどのMDM (モバイルデバイス管理) サーバーに登録する必要があります。

ESETカーネル拡張を許可する

- カーネル拡張は、ESET Endpoint Security for macOSの初回インストール時にのみ許可する必要があります。デバイスのカーネル拡張をリモートで許可するには、次の手順に従います。

  - MDMとしてJamfを使用している場合は、ナレッジベース記事の手順に従ってください。

  - 別のMDMを使用している場合は、.plist設定プロファイルをダウンロードします。任意のUUID生成ツールを使用して、2つのUUIDを生成します。テキストエディターを使用して、ダウンロードした構成プロファイルで、**ここにUUID 1を挿入**および**ここにUUID 2を挿入**テキストの文字列を置換しますMDMサーバーを使用して.plist設定プロファイルファイルを展開します。設定プロファイルをこれらのコンピューターに展開するには、コンピューターがMDMサーバーに登録されている必要があります。

フルディスクアクセスを許可する

- macOS 10.14では、インストール後に、**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 Endpoint Security for macOSからの通知が表示されます。すべてのESET Endpoint Security for macOS機能を利用し、通知を表示しないようにするには、製品をインストールする前に、ESET Endpoint Security for macOSへの**フルディスクアクセス**を許可する必要があります。リモートで**フルディスクアクセス**を許可するには、次の手順に従います。

  - MDMとしてJamfを使用している場合は、ナレッジベース記事の手順に従ってください。

  - **フルディスクアクセス**をリモートで許可するには、.plist設定ファイルをダウンロードします。 。任意のUUID生成ツールを使用して、2つのUUIDを生成します。テキストエディターを使用して、ダウンロードした構成プロファイルで、**ここにUUID 1を挿入**および**ここにUUID 2を挿入**テキストの文字列を置換しますMDMサーバーを使用して.plist設定プロファイルファイルを展開します。設定プロファイルをこれらのコンピューターに展開するには、コンピューターがMDMサーバーに登録されている必要があります。

インストール

ESET Security Management Centerを使用して ESET Endpoint Security for macOSをWebコンソールからリモートでインストールするには、ソフトウェアのインストールタスクを作成します。

詳細な手順:

- ソフトウェアのインストールタスクERAオンラインヘルプトピック
- ERAを使用してESETエンドポイント製品を展開またはアップグレードするナレッジベース記事
- ソフトウェアのインストールタスクESET Security Management Centerオンラインヘルプトピック

インストール後

ESETカーネル拡張とフルディスクアクセスを許可しなかった場合:

ESETカーネル拡張を許可する

ESET Endpoint Security for macOSの最初のインストールの後:

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**コンピューターが保護されていません**通知がESET Endpoint Security for macOSから送信されます。 すべてのESET Endpoint Security for macOS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。

a.手動で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。

b.デバイスのカーネル拡張をリモートで許可するには、次の手順に従います。

i.MDMとしてJamfを使用している場合は、ナレッジベース記事の手順に従ってください。

ii.別のMDMを使用している場合は、.plist設定プロファイルをダウンロードします。任意のUUID生成ツールを使用して、2つのUUIDを生成します。テキストエディターを使用して、ダウンロードした構成プロファイルで、**ここにUUID 1を挿入**および**ここにUUID 2を挿入**テキストの文字列を置換しますMDMサーバーを使用して.plist設定プロファイルファイルを展開します。設定プロファイルをこれらのコンピューターに展開するには、コンピューターがMDMサーバーに登録されている必要があります。

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 Endpoint Security for macOSからの通知が表示されます。すべてのESET Endpoint Security for macOS機能を利用するにはESET Endpoint Security for macOSへの**フルディスクアクセス**を許可する必要があります。リモートで**フルディスクアクセス**を許可するには、次の手順に従います。

oMDMとしてJamfを使用している場合は、ナレッジベース記事の手順に従ってください。

o**フルディスクアクセス**をリモートで許可するには、.plist設定ファイルをダウンロードします。 。任意のUUID生成ツールを使用して、2つのUUIDを生成します。テキストエディターを使用して、ダウンロードした構成プロファイルで、**ここにUUID 1を挿入**および**ここにUUID 2を挿入**テキストの文

字列を置換しますMDMサーバーを使用して.plist設定プロファイルファイルを展開します。設定プロファイルをこれらのコンピューターに展開するには、コンピューターがMDMサーバーに登録されている必要があります。

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。詳細な手順は、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

インストール完了後、製品のアクティベーションが求められます。 複数のアクティベーション方法を使用できます。 特定のアクティベーション方法を使用できるかどうかは、国、および配布方法(CD/DVD、ESET Webページなど)によって異なります。

プログラムから直接ESET Endpoint Security for macOSのコピーをアクティベートするにはmacOSメニューバー(画面の上部)にあるESET Endpoint Security for macOSアイコンをクリックして、**[製品アクティベーション]**をクリックします。 また、メインメニューから製品をアクティベーションするには、**[ヘルプ]** > **[ライセンスの管理]**または**[保護の状態]** > **[製品のアクティベーション]**を選択します。



ESET Endpoint Security for macOSをアクティベーションするには、次の方法を使用できます。

- **製品認証キーでアクティベート**--一意の文字列XXXX-XXXX-XXXX-XXXX-XXXXの形式。ライセンス所有者を識別し、ライセンスをアクティベートするために使用されます。 製品認証キーは、購入後に受信した電子メールに記載されているか、箱に同梱されているライセンスカードに記載されています。
- **セキュリティ管理者**- 認証情報(電子メールアドレスとパスワード)を使用して、ESET License

Administratorポータルで作成されたアカウント。 この方法では、1つの場所から複数のライセンスを管理できます。

• **オフラインライセンス** – 自動生成されたファイルがESET製品に転送され、ライセンス情報を提供します。オフラインライセンスファイルはESETライセンス管理者ポータルから生成され、アプリケーションがライセンス機関に接続できない環境で使用されます。

コンピューターが管理されたネットワークのメンバーであり、管理者がESET Remote Administratorを使用して製品をアクティベーションする場合は、後からこのクライアントをアクティベーションすることもできます。

サイレントアクティベーション
ESET Remote Administratorは、管理者が使用可能にしたライセンスを使用してバックグラウンドでクライアントコンピュータをアクティベーションできます。

ESET Endpoint Security for macOSバージョン6.3.85.0（以降）ではTerminalを使用して製品をアクティベーションできます。 このためには次のコマンドを使用します。

```
sudo ./esets_daemon --wait-respond --activate key=XXXX-XXXX-XXXX-XXXX-XXXX
```

XXXX-XXXX-XXXX-XXXX-XXXXを、ESET Endpoint Security for macOSのアクティベーションで使用されている製品認証キーまたはESET License Administratorに登録された製品認証キーで置換します。 コマンドがは"OK"状態に戻るか、アクティベーションが失敗した場合はエラーになります。

アンインストール

ESET Endpoint Security for macOSアンインストーラを実行するには複数の方法があります。

• コンピュータにESET Endpoint Security for macOS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 Endpoint Security for macOS 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[**アプリケーション**]フォルダを開き、Ctrlを押しながら**ESET Endpoint Security for macOS**アイコンをクリックして、[**パッケージコンテンツを表示**]オプションを選択します。**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 Endpoint Security for macOS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。

次のセクションは、メインメニューからアクセスできます。

- **保護の状態** – コンピュータ、ファイアウォール、ウェブ、メール保護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** – モジュール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 Endpoint Security for macOS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 Endpoint Security for macOS環境設定を表示します。
- *cmd+O* - ESET Endpoint Security for macOS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 Endpoint Security for macOS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 Endpoint Security for macOSアイコンをクリックすると、開くことができます。
- *cmd+W* - ESET Endpoint Security for macOS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。

システムの動作の確認

保護ステータスを表示するには、メインメニューから[**保護ステータス**]をクリックします。プライマリウィンドウにはESET Endpoint Security for macOS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

モジュールが正しく機能するときには、緑色のチェックマークアイコンが表示されます。モジュールが正しく機能しないときには、赤色のエクスクラメーションマーク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と問題を修正するための解決策の提案が、メインプログラム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。

提案された解決策を使用しても問題を解決できなかった場合、ESETナレッジベースの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ご質問に対してすぐに対応し、ESET Endpoint Security for macOSに関する問題を解決するお手伝いをします。

コンピュータの保護

[コンピュータ]の設定は**[設定]** > **[コンピュータ]**から変更できます。**リアルタイムファイルシステム保護**のステータスが表示されます。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。これにより、コンピュータのセキュリティレベルが低下する可能性があります。各機能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は、必ずしも悪意があるとは限りませんが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があります。通常、このようなアプリケーションをインストールするには同意が必要です。このようなアプリケーションをコンピューターにインストールすると、アプリケーションをインストールする前とは異なる状態でシステムが動作します。最も大きな変化としては、不要なポップアップウィンドウ、隠しプロセスの開始と実行、システムリソースの使用率の増加、検索結果の変更、アプリケーションがリモートサーバーと通信することなどがあります。
- **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。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含め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** – 除外を最後に保存した状態にロールバックします。

[**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設定を変更するには、[**設定...**]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で実行されますThreatSense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。

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 Endpoint Security for macOS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。

実行したファイルに適用するThreatSenseパラメーター –既定では、**アドバンスドヒューリスティック検査**はファイル実行時には使用されません。有効にするときには、スマート最適化とESET LiveGrid®を有効にし、システムパフォーマンスへの影響を低減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上げる – ネットワーク上でファイルにアクセスするときにパフォーマンスを上げます。ネットワークドライブへのアクセス中に速度が低下した場合に有効にしてください。この機能は、OS X 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、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や別のウイルス対策プログラムのリアルタイムスキャナーとの競合がある場合などです。

ESET Endpoint Security for macOS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**])の左下にある[**既定**]ボタンをクリックします。

リアルタイム保護の確認

リアルタイム保護が機能しており、ウイルスを検出することを確認するため、eicar.comのテストファイルを使用します。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。

ESET Security Management Centerを使用せずにリアルタイム保護のステータスを確認するには、**ターミナル**を使用してリモートでクライアントコンピュータに接続します。

```
/Applications/.esets/Contents/MacOS/esets_daemon --status
```

リアルタイム検査のステータスは、`RTPStatus=Enabled`または`RTPStatus=Disabled`として表示されます。

ターミナルBASHの出力には次のステータスも含まれます。

- クライアントコンピュータにインストールされたESET Endpoint Security for macOSのバージョン
- 検出エンジンの日付とバージョン
- 更新サーバーへのパス

注意: ターミナルユーティリティの使用は上級ユーザーにのみ推奨されます。

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。この問題が発生した場合は、ESET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スキャナで検出されなかったマルウェアでも、検出できる場合があります。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、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。

また、選択したファイルおよびフォルダーをデスクトップまたは**Finder**ウィンドウからドラッグし、ESET Endpoint Security for macOSのメイン画面、ドックアイコン、メニューバーアイコンⓔ(画面上部)、またはアプリケーションアイコン(*/Applications*フォルダー内に置かれています)にドロップすることもできます。

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を選択することや、特定の検査対象を選択することができます。

スマート検査

Smart検査を使用すると、コンピューターの検査が開始されて、感染しているファイルからウイルスをユーザー操作無しで駆除できます。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。検出されたウイルスがあれば、自動的に駆除または削除されます。駆除の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」を参照してください。

カスタム検査

カスタム検査では、スキャン対象やスキャン方法などのスキャンパラメータを指定できます。 カスタム検査を実行する利点は、検査パラメータ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。 検査対象をさらに細かく指定するためには、対象にするフォルダ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の検査を実行する方法は、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のみ推奨されます。

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。

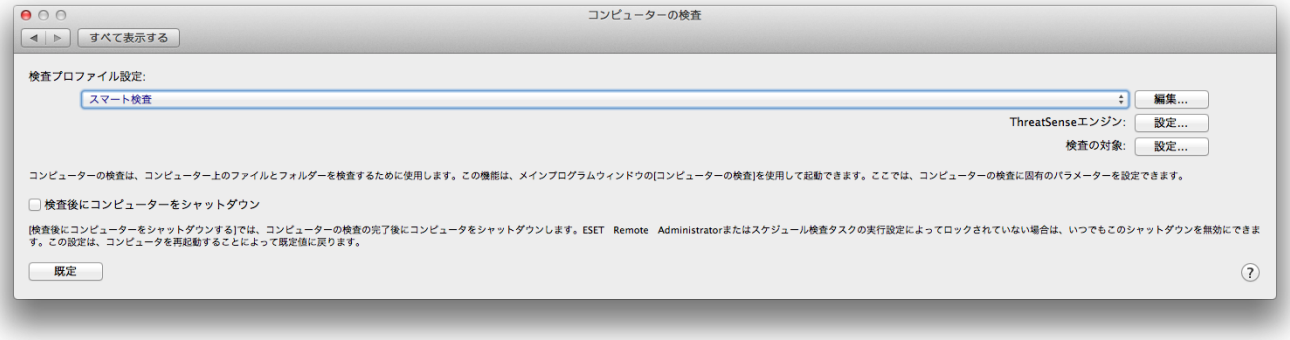
検査の対象をさらに細かく設定するためには、検査の対象に含めるフォルダーまたはファイルのパスを入力します。指定したファイルまたはフォルダに対応するチェックボックスを選択して、コンピュータで使用可能なすべてのフォルダを一覧表示するツリー構造から対象を選択します。

検査プロファイル

検査について目的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。



各自の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」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、ランタイム圧縮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もできます。プロファイルの作成は、［**オンデマンドスキャナ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**］をクリックし、［**OK**］をクリックして確認します。**ThreatSenseエンジン**および**検査の対象**を使用してパラメータを調整し、自分の要件に合わせます。

オンデマンドスキャンの完了後にオペレーティングシステムをオフにして、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。検査エンジンは、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

設定ウィンドウを表示するには、[**設定**] > [**詳細設定を表示する...**](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、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。

- [**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)ファイルへのパスとして解釈され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UPXyodaASPackFGS)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。 その後のアクションとして選択した内容は、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。



標準駆除モード – アーカイブ駆除

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[−]の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、*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。これにより、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。一般的には既定値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。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。
- **最大のファイルサイズ:**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 Endpoint Security for macOS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)

ファイルシステムによって使用される代替データストリーム(リソース/データフォーク)は、通常のスキャン技術では検出できないファイルとフォルダの関連付けです。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CDDVD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、マルウェアを検査する対象を選択します。

ESET Endpoint Security for macOS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。**厳密な駆除**スキャンを実行する際には注意が必要です。厳密な駆除では、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ステータスに関係なく、アーカイブが削除されます。

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。**

検査例外
ESET Endpoint Security for macOS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。
- **Webコントロール** – 不適切または不快な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。

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。

[**許可されたURL**]リストのURLへのアクセスのみを許可するには、[**URLアドレスを制限する**]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する場合は、[**通知**]を選択します。

URLリストを作成するときには、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

電子メール保護ではPOP3とIMAPプロトコルで受信したメール通信を制御できますESET Endpoint Security for macOSで受信メッセージを検査するときにはThreatSenseスキャンエンジンに含まれている詳細なスキャン方法がすべて使用されます。どのような電子メールクライアントを使用していてもPOP3とIMAPプロトコル通信の検査は行われます。

ThreatSenseエンジン:設定 –高度なウィルス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。タグメッセージは排他的に信頼できません。タグは問題があるHTMLメッセージで省略され、一部のウイルスによって偽造される場合があるためです。使用可能なオプションは次のとおりです。

- **何もしない** – 検査通知が追加されません
- **感染電子メールのみ** – 有害なソフトウェアを含むメッセージのみをチェック済みとしてタグ付けします
- **検査した全ての電子メール** - ESET Endpoint Security for macOSは検査した全ての電子メールにタグメッセージを付けます

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ウイルス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 Endpoint Security for macOS)
- %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のセクションでは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 Endpoint Security for macOS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しく動作するには、モジュールが有効になっていることを確認してください。POP3プロトコルチェックは、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のチェックを有効にする – 有効にすると、POP3を使用する全ての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 Endpoint Security for macOS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プロトコルチェックを有効にする – 有効にすると、IMAPを使用する全ての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。

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HTTP、POP3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。

[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]を有効にすると、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ブロックされます。このオプションは、セキュリティ上の重大なリスクの疑いがあってシステムをネットワークから切断する必要がある場合にのみ使用してください。

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 Endpoint Security for macOS 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は、[設定] > **[アプリケーション環境設定...] > [ファイアウォール]**の下にあります。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 – ファイアウォールのカスタム設定を作成できます。通信が検出された時に、既存のルールがその通信には適用されされていない場合、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。このダイアログウィンドウでは、通信を許可するか拒否するかを選択することができます。さらに、許可するか拒否するかというその決定を、ファイアウォールの新しいルールとして保存することもできます。ユーザーが新しいルールを作成するように選択すると、それ以降、その種類の全ての接続がルールに従って許可または拒否されます。



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

ルールは、全てのネットワーク接続をテストするために使用される条件を表し、それらの条件に割り当てられた全てのアクションのセットを決定します。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。

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 – 既定では□Appleが署名したソフトウェアは、自動的にネットワークにアクセスできます。アプリケーションをAppleサービスに接続するか、デバイスにインストールするには、このアプリケーションをAppleが発行した証明書で署名する必要があります。これを無効にするには、このオプションをオフにします□Apple証明書で署名されていないアプリケーションがネットワークにアクセスするには、ユーザーアクションまたはルールが必要です。

このオプションが無効であると□Appleが署名したサービスとのネットワーク通信で、ファイアウォール

ルールで定義されていない場合に、ユーザーの承認が必要になります。

以前のバージョンであるESET Endpoint Security for macOS 6.8以前ではApple証明書を使用したサービスへの受信通信がブロックされていました。現在のバージョンのESET Endpoint Security for macOSでは、受信通知のローカルレシーバーを特定できるため、このオプションが有効であれば、受信通信が許可されます。

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。お使いのコンピューター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、[**全てのアプリケーション**]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。[**ログルール**]を選択して、このルールに関連するすべての通信を記録します。ファイアウォールログを確認する時に、ESET Endpoint Security for macOS 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**]セクションで、アプリケーションが通信するために使用するプロトコルとポートを設定します(TCPまたはUDPプロトコルが選択される場合)。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。与えられたグループ内の各アドレスは、グループ全体に対して一元的に定義された同様のルールが割り当てられています。

これらのゾーンは**追加**ボタンをクリックすることで作成できます。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 Endpoint Security for macOS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 Endpoint Security for macOS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。

デバイスコントロール

ESET Endpoint Security for macOSを使用すると、拡張フィルタ/権限を検査、ブロック、または調整して、ユーザーからの指定デバイスへのアクセス方法やその作業方法を定義できます。この機能は、望ましくないコンテンツを収めたデバイスをユーザーが使用することを防止したいコンピュータ管理者にとって便利です。

サポートされている外部デバイス:

- ディスクストレージ(HDDUSBフラッシュドライブ)
- CD/DVD
- USBプリンタ
- イメージングデバイス
- シリアルポート
- ネットワーク

- ポータブルデバイス

既存のルールでブロックされているデバイスが挿入されると、通知ウィンドウが表示され、デバイスへのアクセス権は付与されません。

デバイスコントロールログは、デバイスコントロールをトリガーするすべてのインシデントを記録します。ログエントリは、ESET Endpoint Security for macOSのメインプログラムウィンドウの[**ツール**] > [**ログファイル**]から表示できます。

ルールエディタ

デバイスコントロール設定オプションは、[**設定**] > [**アプリケーション環境設定の入力...**] > [**デバイスコントロール**]で変更できます。

[**デバイスコントロールを有効にする**]をクリックするとESET Endpoint Security for macOSのデバイスコントロール機能が有効になります。 デバイスコントロールを有効にすると、デバイスコントロールルールを管理および編集できます。 ルール名の横のチェックボックスを選択すると、ルールを有効/無効にします。

+ または − ボタンを使用して、ルールを追加または削除します。 ルールは優先度順に一覧表示されます。最も優先度が高いルールが最上位近くに表示されます。 順序を並べ替えるには、ルールを新しい位置にドラッグアンドドロップするか、⚙をクリックしてオプションのいずれかを選択します。

ESET Endpoint Security for macOSは現在挿入されているデバイスとパラメータをすべて自動的に検出します(デバイスタイプ、ベンダー、モデル、シリアル番号)。 ルールを手動で作成する代わりに、[**入力**]オプションをクリックし、デバイスを選択し、[**続行**]をクリックしてルールを作成します。

特定のデバイスについては、ユーザー単位またはユーザーグループ単位で、および複数の追加パラメータに基づいて許可またはブロックできます。これは、ルール設定で指定できます。 ルール一覧には、名前、デバイスタイプ、ログの重大度、コンピュータにデバイスを接続した後に実行するアクションなどのルールの記述がいくつか示されます。

名前

識別しやすいように、ルールの説明を[**名前**]フィールドに入力します。[**ルールを有効にする**]チェックボックスによって、このルールを無効または有効にすることができます。これは、ルールを完全に削除したくない場合に便利です。

デバイスタイプ

ドロップダウンメニューから外部デバイスタイプを選択します。デバイスタイプ情報はオペレーティングシステムから収集されます。 記憶装置にはUSBまたはFireWireから接続できる外付けハードディスクや標準的なメモリカードリーダーが含まれます。 イメージングデバイスの例としては、スキャナやカメラが挙げられます。 これらのデバイスはアクションに関する情報だけを提供し、ユーザーに関する情報は提供しないため、グローバルにのみブロックできます。

アクション

記憶装置以外へのアクセスは、許可またはブロックのいずれかです。 それに対して、記憶装置のルールについては、次のいずれかの権限設定を選択できます。

読み込み/書き込み – デバイスへの完全アクセスが許可されます。

読み込み専用 – デバイスからの読み込みアクセスだけが許可されます。

拒否 – デバイスへのアクセスはブロックされます。

条件タイプ

デバイスグループまたは**デバイス**を選択します。 追加パラメータは、ルールを微調整したりデバイスに合わせて変更するのに使用できます。

ベンダー – ベンダー名またはIDによるフィルタリング。

モデル – デバイスに付けられている名前。

シリアル – 外部デバイスには通常独自のシリアル番号が付いています CD/DVDの場合は、CD/DVDドライブではなく、そのメディアのシリアル番号があります。



未定義のパラメーター
これらのパラメータが未定義の場合、ルールは照合時にこれらのフィールドを無視します。すべてのテキストフィールドのフィルタリングパラメータは、大文字と小文字が区別されず、ワイルドカード(*、?)はサポートされません。



ヒント
デバイスに関する情報を表示するには、デバイスのタイプのルールを作成し、デバイスをコンピュータに接続します。 デバイスが接続されたら、デバイス詳細がデバイスコントロールログに表示されます。

ログ記録の重大度

常時 – すべてのイベントをログに記録します。

診断 – プログラムを微調整するのに必要な情報をログに記録します。

情報 – 情報メッセージと上記のすべてを記録します。

警告 – 重大な警告、エラー、および警告メッセージを記録します。

なし – ログは記録されません。

ユーザー一覧

ルールを特定のユーザーまたはユーザーグループに限定する場合は、次のようにして該当するユーザーまたはユーザーグループを[ユーザー一覧]に追加します。

編集... - **IDエディタ**が開き、ユーザーまたはグループを選択できます。 ユーザーの一覧を定義するには、左側の[**ユーザー**]一覧からユーザーを選択し、[**追加**]をクリックします。 ユーザーを削除するには、[**選択されたユーザー**]一覧でユーザー名を選択し、[**削除**]をクリックします。 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。 リストが空の場合は、すべてのユーザーが許可されます。

ユーザールール制限
一部のデバイスをユーザールールでフィルタリングできません(たとえば、イメージングデバイスではユーザーに関する情報は提供されず、アクションに関する情報だけが提供されます)。

Webコントロール

Webコントロール機能では、法的責任のリスクから会社を保護する設定を構成できますWebコントロールは、知的財産権に抵触するWebサイトへのアクセスを規制できます。この機能の目的も、作業生産性に悪影響を与える可能性のある不適切または有害なコンテンツやページに従業員がアクセスしないようにすることにあります。企業やシステム管理者は、事前に定義された27以上のカテゴリと140以上のサブカテゴリへのアクセスを禁止できます。

既定ではWebコントロールは無効です。有効にするには、**[設定]** > **[アプリケーション設定を入力する]** > **[Webコントロール]**をクリックして、**[Webコントロールを有効にする]**の横のチェックボックスを選択します。

ルールエディタウィンドウには、既存のURLベースまたはカテゴリベースのルールが表示されます。このルール一覧にはWebコントロールルールおよびログ重大度との突き合わせの結果として、名前、ブロックのタイプ、実行すべきアクションなどのいくつかのルールの説明が示されます。

パラメーターセットを新規作成するには、+ボタンをクリックします。**[名前]**フィールドをダブルクリックし、識別しやすいようにルールの説明を入力します。

[有効]フィールドのチェックボックスはルールを有効/無効にします。これは、後からルールを使用して、完全に削除しない場合に便利です。

タイプ

URLに基づくアクション – 特定のWebサイトへのアクセス。**[URL/分類]**フィールドをダブルクリックして、適切なURLアドレスを入力します。

URLアドレスリストでは、特殊記号の*(アスタリスク)および?(疑問符)は使用できません。複数のTLD (上位レベルドメイン)が含まれるWebページのアドレスは、作成したグループ(*examplepage.com*、*examplepage.sk*など)に入力する必要があります。リストにドメインを追加するときは、このドメインとすべてのサブドメイン(*sub.examplepage.com*など)にあるすべてのコンテンツがURLに基づくアクションに従ってブロックまたは許可されます。

分類に基づくアクション- **[URL/分類]**フィールドをダブルクリックして分類を選択します。

個人情報

ルールが適用されるユーザーを選択できます。

アクセス権

許可- URLアドレス/分類へのアクセスが認可されます。

ブロック - URLアドレス/分類がブロックされます。

重要度(ログファイルのフィルタリング)

常時 – すべてのイベントをログに記録します。

診断 – プログラムを微調整するのに必要な情報をログに記録します。

情報 – 情報メッセージと上記のすべてを記録します。

警告 – 重大な警告、エラー、および警告メッセージを記録します。

なし – ログは作成されません。

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、ウイルスの検出、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 Endpoint Security for macOS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 Endpoint Security for macOS 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** – 侵入の検出に関するイベントの情報。
2. **イベント** – イベントログには ESET Endpoint Security for macOS によって実行されたすべ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** – このウィンドウには、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、特定のコンピュータ検査結果の詳細が表示されます。
4. **デバイスコントロール** – コンピュータに接続されたリムーバブルメディアまたはデバイスの記録が含まれます。個別のデバイスコントロールルールが設定されているデバイスのみがログファイルに記録されます。接続されているデバイスとルールが一致しない場合には、接続されているデバイスのログエントリは作成されません。ここで、デバイスタイプ、シリアル番号、ベンダー名、メディアのサイズ (ある場合) などの詳細情報も確認できます。
5. **ファイアウォール** – ファイアウォールログには、ファイアウォールによって検出された全てのリモート攻撃が表示されます。ファイアウォールログには、システムで検出された攻撃の情報が表示されます。[**イベント**] 列には検出された攻撃が一覧表示されます。[**ソース**] 列には攻撃者の詳細が表示されます。[**プロトコル**] 列には攻撃で使用された通信プロトコルが表示されます。
6. **Web コントロール** – ブロックまたは許可された URL アドレスとその分類方法の詳細が表示されます。
7. **フィルタリングされた Web サイト** – このリストは、 Web アクセス保護 または Web コントロール によってブロックされた Web サイトの一覧を表示する場合に便利です。. 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。

任意のログファイルを右クリックし、[**コピー**] をクリックして、クリップボードにログファイルの内容をコピーします。

ログの保守

ESET Endpoint Security for macOS 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**] > [**アプリケーション設定の入力**] > [**ツール**] > [**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ーが自動的に削除されます。
- **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。

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 (カンマ区切り値ファイル) 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、**[詳細設定]**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。

- 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。
- 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。
- 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。
- デバイスコントロールでブロックされたデバイスについてはdevctllog.txtに記述されています。
- ファイアウォール経由の通信に関連したすべてのイベントはfirewalllog.txtに書き込まれます。
- Webコントロールでブロックされ たWebページについてはwebctllog.txtに記述されています。

[既定のコンピュータ検査ログレコード]のフィルタを設定するには、**[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保存されます。ログのフィルター機能では、特定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。

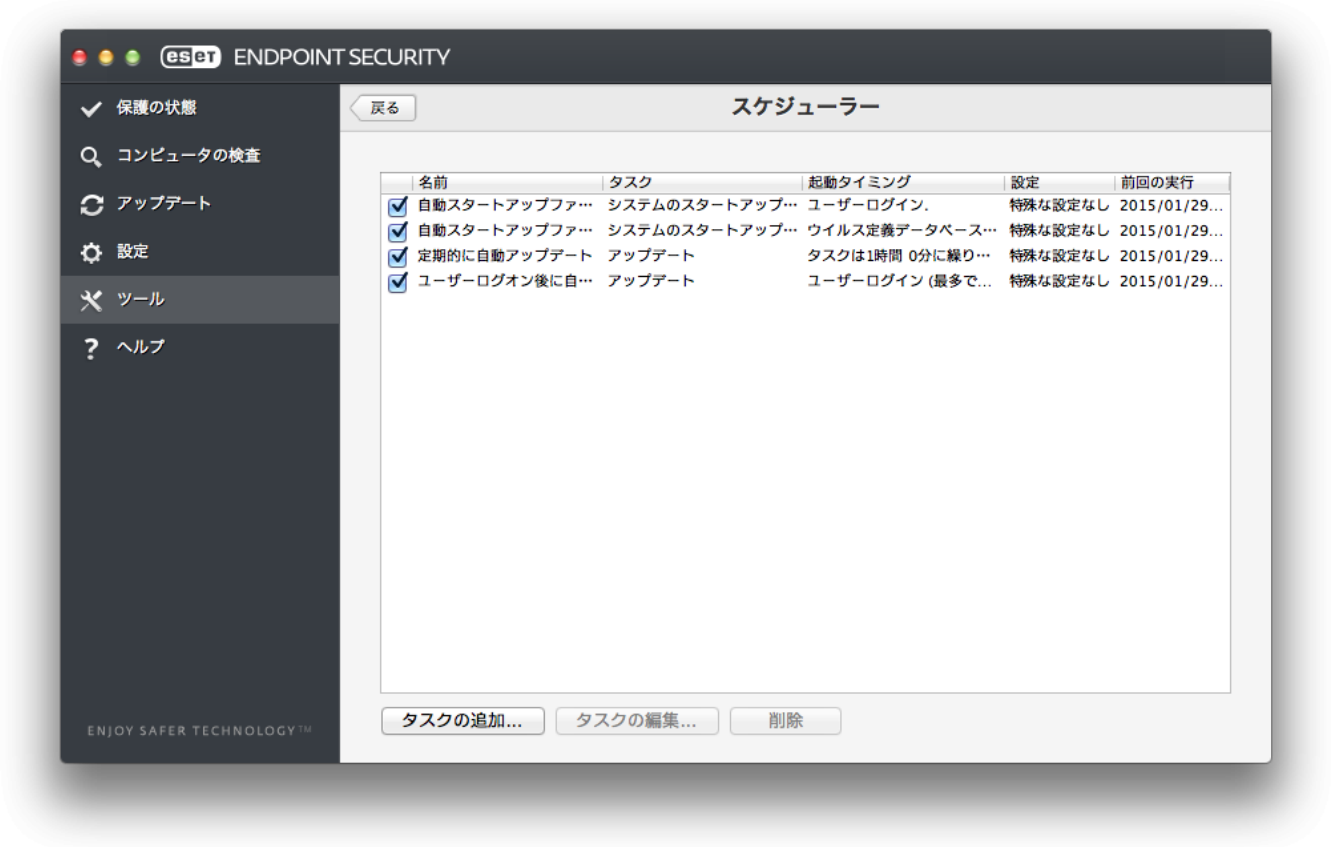
最もよく使用されるログの種類を次に示します。

- **重大な警告** – 致命的なシステムエラー(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 Endpoint Security for macOS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(スケジューラーの設定で[**システムタスクを表示する**]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、[**タスクの追加**]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4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**
- **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**



ユーザー定義のタスク

既定では、アプリケーションは、ESETが作成した、権限が制限された専用ユーザーによって実行されます。 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。



ユーザー名の制限事項

スペースまたは空白文字をユーザー名の前で使うことはできません。 ユーザー名ではスペースを使用することもできません。 空白文字を使用してください。

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 "$VOLUME"` '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' -f /tmp/scan_log "$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 Endpoint Security.app/Contents/MacOS/esets_scan' /tmp

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の代替オプションを選択します。
5.[**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 Endpoint Security for macOS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、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**] > [**アプリケーション設定を入力する...**] > [**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。

ユーザー定義タスクの作成

[タスクの実行]ドロップダウンからタスクタイプとして[ユーザー定義]を選択するときには、定義する必要がある特殊パラメータがいくつかあります。

[**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
```

次の特殊文字がcron式で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。

注意:

ユーザー定義のタスク
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。

LiveGrid®

LiveGrid®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LiveGrid®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、他のユーザーが収集した情報を使用して、検出モジュールを常に最新の状態に保つことです。LiveGrid®の2つのオプションから1つ選択します。

1.LiveGrid®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。ソフトウェアの機能は一切失われませんが、場合によってはESET Endpoint Security for macOSはモジュールアップデートよりも速く新しい脅威に対応できることがあります。

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LiveGrid®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。これらのウイルスを調査することでESETはウイルスのデータベースを最新のものにし、ウイルス検出機能を向上させることができます。

LiveGrid®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LiveGrid®にアクセスするには、[**設定**] > [**アプリケーション設定を入力する**] > [**LiveGrid®**]をクリックします。[**ESET LiveGrid®レピュテーションシステムを有効化する(推奨)**]を選択してLiveGrid®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。

不審なファイル

既定ではESET Endpoint Security for macOSは、疑わしいファイルを詳しく解析するためにESETの脅威ラボに送信するように設定されています。 このようなファイルを自動的に送信しない場合は、**[不審なファイルの提出]** (**[設定]** > **[アプリケーション設定を入力する]** > **[LiveGrid®]** > **[設定]**)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**] > [**分析のためにファイルを提出**]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。

匿名情報と統計情報の提出 - LiveGrid®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。

例: 送信された統計パッケージ

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463[1].zip
```

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きに便利です。 最も一般的なファイルの種類は、既定で除外されます((.doc,.rtfなど)。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。

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 Endpoint Security for macOS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。

なお、任意のファイルを選択して隔離することもできます。これは、ファイルの動作が疑わしいにもかかわらず、ウイルス対策スキャナー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)、隔離理由(ユーザーによって追加など)、および検出された脅威の数を表示するテーブルに表示できます。隔離フォルダ(*/Library/Application Support/Eset/esets/cache/quarantine*)はESET Endpoint Security for macOSのアンインストール後に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 Endpoint Security for macOSのインストール後に再度復元することもできます。

ファイルの隔離

削除されたファイルは、ESET Endpoint Security for macOS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選択解除しなかった場合)。隔離ウィンドウから、[隔離]をクリックして、ファイルを手動で隔離に追加できますCtrlを押しながら任意のタイミングでファイルをクリックして、コンテキストメニューから[サービス] > [ESET Endpoint Security for macOS - ファイルを隔離に追加] をクリックすると、ファイルを隔離に送信できます。

隔離フォルダーからの復元

隔離されたファイルは元の場所に復元できます。このようにするには、隔離されたファイルを選択して、**[復元]**をクリックします。復元はコンテキストメニューから実行できます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。**[復元先を指定]**を使用して、隔離された場所以外の場所にファイルを復元できます。

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。

権限

ESET Endpoint Security for macOS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。このような問題に備えて、プログラム設定を編集する権限を持つユーザーを選択できます。

[設定] > [アプリケーション設定を入力する] > [ユーザー] > [権限]の下で、特権ユーザーを構成できます。

システムの最大限のセキュリティを確保するには、プログラムを正しく設定することが重要です。許可なく変更が行われた場合、重要なデータが失われることがあります。権限ユーザーの一覧を設定するには、左側の[**ユーザー**]一覧からユーザーを選択し、[**追加**]をクリックします。ユーザーを削除するには、右側の[**権限ユーザー**]一覧でユーザー名を選択し、[**削除**]をクリックします。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。

注意: 権限ユーザーの一覧が空の場合、システムの全てのユーザーにプログラムの編集権限があります。

プレゼンテーションモード

プレゼンテーションモードは、ソフトウェアを中断せずに使用し、ポップアップウィンドウを表示せずにCPUの使用量を最小化する必要があるユーザー向けの機能です。プレゼンテーションモードは、ウイルス対策アクティビティによって中断できないプレゼンテーション中に使用することもできます。有効にすると、すべてのポップアップウィンドウが無効になり、スケジュールされたタスクは実行されません。システムの保護は引き続きバックグラウンドで実行されますが、ユーザーの操作は必要ありません。

プレゼンテーションモードを手動で有効にするには、[**設定**] > [**アプリケーション設定を入力する...**] > [**プレゼンテーションモード**] > [**プレゼンテーションモードを有効にする**]をクリックします。

[**全画面でプレゼンテーションモードを自動的に有効にする**]の横のチェックボックスをオンにし、アプリケーションが全画面で実行されたら、プレゼンテーションモードを自動的に起動します。この機能が有効になると、全画面アプリケーションを開始するたびにプレゼンテーションモードが起動し、アプリケーションを終了すると、自動的に終了します。これは特にプレゼンテーションを開始する場合に便利です。

また、[**次の時間が経過した後にプレゼンテーションモードを自動的に無効にする**]を選択し、プレゼンテーションモードが自動的に無効になる時間を分で定義できます。

プレゼンテーションモードを有効にすると、潜在的なセキュリティリスクが発生するためESET Endpoint Security for macOS保護の状態アイコンがオレンジになり、警告が表示されます。

注意: ファイアウォールが対話モードの場合に、プレゼンテーションモードを有効にすると、インターネットとの接続時に問題が発生することがあります。これは、インターネットに接続するアプリケーションを開始するときに問題となります。通常、そのようなときには確認が求められます(通信のルールや例外が定義されてない場合を除く)が、プレゼンテーションモードではユーザーの操作は無効になって

います。これを解決するには、この動作が起こる可能性がある全てのアプリケーションで通信のルールを定義するか、またはファイアウォールで別のフィルタリングモードを使用します。プレゼンテーションモードが有効な場合に、セキュリティ上の潜在的なリスクが存在するWebページまたはアプリケーションにアクセスすると、ブロックされるにもかかわらず、ユーザーとの対話処理が無効なため説明や警告が表示されないことに、注意してください。

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 Endpoint Security for macOSは、ユーザーをESET LiveGrid®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。アクティビティモニター(*/Applications/Utilities*))を使用して、コンピュータで実行中のすべてのプロセスを表示できます。
- **リスクレベル** – ほとんどの場合ESET Endpoint Security for macOSおよびESET LiveGrid®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。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、その後のアップデートファイルにその定義が追加されます。
- **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 LiveGrid®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

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**]>[**アプリケーション設定を入力する...**]>[**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 Endpoint Security for macOS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 Endpoint Security for macOSアイコンを表示し、ESET Endpoint Security for macOS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 Endpoint Security for macOS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**]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。
- カーソルがESET Endpoint Security for macOSの特定のオプションの上に置かれたら、[**ツールヒントを表示する**]を有効にします。
- [**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 Endpoint Security for macOS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 Endpoint Security for macOS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、保護ステータス、およびシステム通知をESET Endpoint Security for macOSでどのように処理するかを設定することができます。

[**警告を表示**]を無効にすると、全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、この章を参照してください。

[**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 Endpoint Security for macOS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 Endpoint Security for macOS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**] > [**アプリケーション設定...**] > [**警告と通知**] > [**アラートの表示:設定...**])は□ESET Endpoint Security for macOS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。各通知を有効化または抑制するには、**ダイアログ名**の左にあるチェックボックスをオンにします。チェックボックスがオンになると、通知は常に表示され、**表示条件**は適用されません。リストの特定のイベントに関する通知を受信しない場合は、このオプションをオフにし、追加で、特定のアクションが実行される**表示条件**を定義できます。

保護状態

ESET Endpoint Security for macOS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 Endpoint Security for macOS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
- 電子メールクライアント保護
- プレゼンテーションモード
- 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

コンテキストメニュー

コンテキストメニューからESET Endpoint Security for macOS機能を使用できるようにするには、[**設定**] > [**アプリケーション設定を入力する**] > [**コンテキストメニュー**]をクリックし、[**コンテキストメニューに統合**]の横のチェックボックスを選択します。ログアウトまたはコンピュータの再起動後に、変更が有効になります。デスクトップの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またはフォルダをクリックすると、[**Finder**]ウィンドウで使用できます。

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 Endpoint Security for macOS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、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、最新のモジュールがある場合は、[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、ライセンスデータ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。この数値インジケーターは、検出エンジンアップデート情報を示すESETのWebページにリンクしています。

アップデートの設定

アップデート設定セクションでは、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、アップデートファイルの送信元の情報を指定します。 既定では、[**アップデートサーバ**]ドロップダウンメニューは自動的に[**自動選択**]に設定され、最もネットワークトラフィックが少ないESETサーバーからアップデートファイルが自動的にダウンロードされます。



使用可能なアップデートサーバーのリストにアクセスするには、[**アップデートサーバ**]ドロップダウンメニューを使用します。 新しいアップデートサーバーを追加するには、**[編集]をクリックし、[アップ**

デートサーバー]入力フィールドに新しいサーバーのアドレスを入力し、[**追加**]をクリックします。

ESET Endpoint Security for macOSでは、代替またはフェイルオーバーのアップデートサーバーを設定できます。 **プライマリ**サーバーは、ミラーサーバーにすることができ、**セカンダリサーバー**は、標準のアップデートサーバーにすることができます。 セカンダリサーバーはプライマリサーバーとは異なっていなければなりません。そうでないと使用できません。 セカンダリアップデートサーバー、ユーザー名、およびパスワードを指定しないと、フェイルオーバーアップデート機能は動作しません。［自動選択］を使用して、該当するフィールドにユーザー名とパスワードを入力し、ESET Endpoint Security for macOSで使用する最適なアップデートサーバーを自動的に選択できます。

プロキシモードでは、プロキシサーバー経由で検出モジュールをアップデートできます(ローカルHTTPプロキシなど)。 サーバーは、接続が必要なすべてのプログラム機能に適用されるグローバルプロキシサーバーと同じまたは別にすることができます。 グローバルプロキシサーバー設定は、インストール中またはプロキシサーバー設定中に定義されている必要があります。

プロキシサーバーからアップデートをダウンロードするようにのみクライアントを構成するには

1. ドロップダウンメニューから[**プロキシサーバを使用して接続する**]を選択します。
2. [**検出**]をクリックし、ESET Endpoint Security for macOSでIPアドレスとポート番号(**3128**が既定)を入力できます
3. プロキシサーバーとの通信で認証が必要な場合は、有効な**ユーザー名**と**パスワード**を該当するフィールドに入力します。

ESET Endpoint Security for macOS はmacOSシステム環境設定からプロキシ設定を検出します。 これらは macOSで、 > **システム環境設定** > **ネットワーク** > **詳細** > **プロキシ**で構成できます。

[**HTTPプロキシが使用できない場合は直接接続を使用する**]を有効にするとESET Endpoint Security for macOSは自動的にプロキシを使用せずにアップデートサーバーに接続しようとします。 このオプションは、MacBooksモバイルユーザーに推奨されます。

検出モジュールアップデートを試行するときに問題が発生した場合は、[**アップデートキャッシュを削除**]**をクリックして、一時アップデートファイルを削除します**

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。

リリース前アップデートを有効にし、最終テストが完了する開発モジュールをダウンロードします。一般的に、リリース前アップデートには、製品の問題に対する修正が含まれます。 延期されたアップデートは、リリース後数時間たってからアップデートをダウンロードし、問題がないことが確認されるまでクライアントがアップデートを受信しないことを保証します。

ESET Endpoint Security for macOS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する]**を有効にしてESET Endpoint Security for macOSでこのような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新規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、アップデートの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。 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。 アップデートの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、[一時停止期間を設定]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すると、標準のアップデートは、手動で復元するまで再開されません。 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] > **[モジュールのアップデート]**をクリックして、検出モジュールアップデートを手動でトリガーします。

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**] > [**スケジューラー**]をクリックしますESET Endpoint Security for macOS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」を参照してください。

システムアップデート

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ESET Endpoint Security for macOSは重要度レベルに従い、見つからないアップデートを通知します。**[オペレーティングシステムアップデート]**の横の**[表示条件]**を使用すると、**[設**

定] > [アプリケーション設定を入力する] > [警告と通知] > [設定]に表示される通知のアップデート重要度を調整できます。

- **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 Endpoint Security for macOS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。

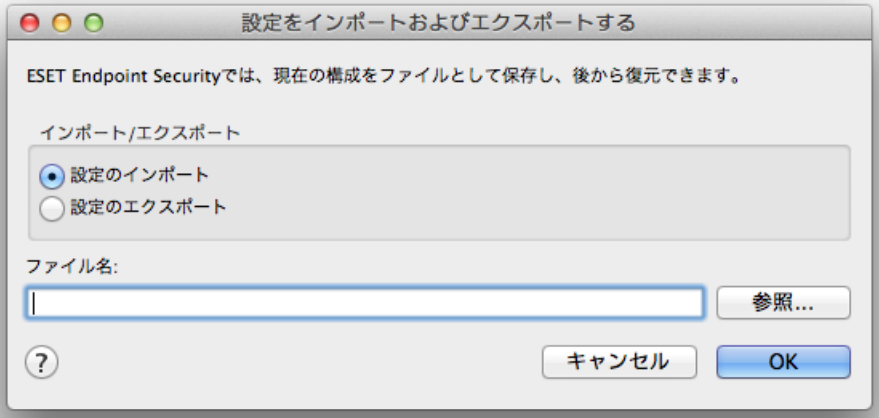
通知ウィンドウにはsoftwareupdateコマンドラインツールで取得された更新が表示されます。このツールで取得された更新は、「ソフトウェア更新」アプリケーションで表示される更新とは異なる場合があります。「未適用のシステムアップデート」ウィンドウで表示されるすべての利用可能な更新をインストールし、「ソフトウェア更新」アプリケーションで表示されない場合は、softwareupdateコマンドラインツールを使用する必要があります。このツールの詳細については、**[ターミナル]**ウィンドウに`man softwareupdate`と入力し、softwareupdateのマニュアルをお読みください。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

設定をインポートおよびエクスポートする

既存の設定またはESET Endpoint Security for macOS設定をインポートするには、**[設定] > [設定をインポート/エクスポートする]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 Endpoint Security for macOS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 Endpoint Security for macOS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、**[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。

プロキシサーバーの設定

プロキシサーバー設定を構成するには、**[設定]** > **[アプリケーション設定を入力する]** > **[プロキシサーバー]**をクリックします。プロキシサーバーをこのレベルで指定すると、ESET Endpoint Security for macOS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 Endpoint Security for macOSは、Basic AccessおよびNTLM (NT LAN Manager)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受け付け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、両方のフィールドを自動的に入力することもできます。

プロキシサーバーとの通信で認証が必要な場合は、有効な**ユーザー名**と**パスワード**を該当するフィールドに入力します。

共有ローカルキャッシュ

共有ローカルキャッシュの使用を有効にするには、[設定] > [アプリケーション設定を入力する] > [共有ローカルキャッシュ]をクリックし、[ESET Shared Local Cacheを使用してキャッシュを有効にする]の横のボックスをオンにします。 この機能を使用すると、ネットワークで重複した検査がなくなり、仮想環境のパフォーマンスが向上します。 これにより、各ファイルが1回だけ検査され、共有キャッシュに保存されます。 有効にすると、ネットワークのファイルとフォルダの検査情報がローカルキャッシュ

に保存されます。 新しい検査を実行する場合は、ESET Endpoint Security for macOSがキャッシュにある検査済みファイルを検索します。 ファイルが一致すると、検査から除外されます。

共有ローカルキャッシュ設定には次の項目があります。

- **サーバーアドレス** – キャッシュがあるコンピュータの名前またはIPアドレス。
- **ポート** – 通信で使用されるポート番号(既定では(3537)
- **パスワード** – 共有ローカルキャッシュのパスワード(任意)

詳細手順
ESET共有ローカルキャッシュのインストールおよび構成方法の詳細については、『ESET共有ローカルキャッシュユーザーガイド』を参照してください。(このガイドは英語でのみ提供されています。)

End User License Agreement

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, 851 01 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, 31 333 535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□I Accept□]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□I Do Not Accept□]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、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、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の他のユーザーのデータ(ランダムまたは謝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の他のユーザーのデータ(ランダムまたは謝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。

データ主題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ー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上またはサードパーティのサーバ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, 851 01 Bratislava, Slovak Republic に送付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: BUS-STANDARD-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:31 333 535) (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

当社の製品に実装されたESETのサービスは、エンドユーザー使用許諾契約(EULA)の条項に従って提供されますが、特定の注意が必要になる項目がある場合があります。当社のサービスの提供に関するデータ収集の詳細について、当社はお客様に提供します。当社は、アップデート/アップグレードサービス Livegrid® データの悪用に対する保護、サポートなど EULAで規定された各種サービスおよび製品文書を提供します。すべてを機能させるには、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。
- 検査されたファイルを、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

較することで、マルウェア対策ソリューションを効率化する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。

• ESETがエンドユーザーのニーズにただちに対応し、最新の脅威への対応力を維持することを可能にするESET LiveGrid®フィードバックシステムの一部としての、世界中の不審なサンプルおよびメタデータ。次の情報の送信はお客様の任意です。

  oウイルスおよび他の悪意のあるプログラムの可能性のサンプルなどの侵入、ならびに実行ファイル、お客様が迷惑メールとして報告または当社の製品で迷惑メールに設定された電子メールメッセージなどの不審、問題、望ましくない可能性、期間な可能性があるオブジェクト

  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クラッシュダンプファイルおよび含まれる情報。

当社はこの範囲外のデータを収集することはしませんが、避けることができない場合があります。誤って収集されたデータは、マルウェア自体(お客様の認識または承認なく収集されている)、あるいはファイル名またはURLの一部として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、請求目的、ライセンスの正当性検証、およびサービス提供の目的で必要です。

• 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、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企業を通して、世界中で事業を展開する企業です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。プライバシーシールドメカニズム、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率する必要があります。

当社は、EULAの下でサービスを提供している間、必要よりも長くデータが保存されないように最善を尽くします。当社の保持期間は、簡単で便利な更新を行うための時間を提供する目的でのみ、ライセンスの有効期間よりも長くなる場合がありますESET LiveGrid®からの最小化された仮名の統計情報が、統計目的でさらに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ています。

データ主体の権利。

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。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

- 不正確な場合、個人データを修正する権利(および不完全な個人データを入力する権利)
- お客様の個人データの消去を要求する権利
- お客様の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
- 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、またはご質問や問題がある場合は、以下の宛先までご連絡ください。

ESET, spol. s r.o.
データ保護責任者
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk