# ESET Endpoint Security 8

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 Endpoint Security 8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: 2025年/2月/27日

# ESET Endpoint Security for macOS

ESET Endpoint Security 8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®検出エンジン、脆弱性とパッチ管理システム、管理されたファイアウォールが連携して速度と精度を活かして、コンピューターを安全に保ちます。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 8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 PROTECT 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ー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8の新機能

ESET Endpoint Security for macOSバージョン8は、新世代の製品です。新機能には次のようなものがあります。

- パフォーマンスと安定性の改善。
- 管理されたファイアウォール
- 脆弱性とパッチ管理(V&PM)
- ライセンスベースの機能
- コンポーネントインストール
- ESET LiveGuard

ESET Endpoint Antivirusは、バージョン8にアップグレードすると、名前がESET Endpoint Securityに変更されます。

# バージョンの比較

| 機能 | バージョン6 | (ESET Endpoint Antivirus) バージョン7.3 & 7.4 | バージョン8 |
|---|---|---|---|
| **アーキテクチャ (Apple Silicon & Intel)** | | | |
| アーキテクチャ | モノリシック | マイクロサービス | マイクロサービス |

| 機能 | バージョン6 | (ESET Endpoint Antivirus) バージョン7.3 & 7.4 | バージョン8 |
|---|---|---|---|
| アーキテクチャセキュリティプロファイル | メインプロセスはrootで実行される<br>(すべての重要な処理はメインプロセスによって実行される) | 各サービスは可能な限り低い権限で実行される<br>可能な攻撃ベクトルを低くする<br>1つのサービスの脆弱性がアプリケーション全体を危険にさらさない<br>1つの製品プロセスがクラッシュまたはハイジャックされた場合、一部の保護が無効になる | バージョン7と同じ |
| アーキテクチャ安定性プロファイル | モノリシックなスキャナーのクラッシュにより、保護が一時的に無効になる<br>クラッシュした場合の自動プロセス再起動 | 重大ではないサービスクラッシュでは保護が一時停止しない<br>特定のタスク向けに最適化されたよりシンプルなサービス<br>クラッシュした場合の自動プロセス再起動 | バージョン7と同じ |
| macOSサポート | 10.12 (Sierra)<br>10.13 (High Sierra)<br>10.14 (Mojave)<br>10.15 (Catalina)<br>11 (Big Sur)<br>12 (Monterey)<br>13 (Ventura)<br>14 (Sonoma) | 10.15 Catalina (バージョン 7.3 のみ)<br>11 (Big Sur)<br>12 (Monterey)<br>13 (Ventura)<br>14 (Sonoma) | 11 (Big Sur)<br>12 (Monterey)<br>13 (Ventura)<br>14 (Sonoma)<br>15 (Sequoia) |
| ネイティブ64ビット検査エンジン | x | x | x |
| ネイティブ64ビットアプリケーション | x | x | x |
| 多言語サポート | 言語固有のインストールパッケージ | 1つのパッケージのすべての言語(システムと同じGUI言語) | 1つのパッケージのすべての言語(システムと同じGUI言語) |
| ネイティブARMサポート | | バージョン7.1.1700.0以降 | x |
| Rosetta ARMサポート | x | x | x |
| **ファイルシステム保護** | | | |
| 望ましくない可能性、安全ではない可能性、不審な可能性があるアプリケーションの検出 | x | x | x |
| パフォーマンス除外 | x | x | x |

| 機能 | バージョン6 | (ESET Endpoint Antivirus) バージョン7.3 & 7.4 | バージョン8 |
|---|---|---|---|
| パス検出による検出、除外 | ESET PROTECT On-Premで検出除外を作成した後(ファイルは検査されますが、問題は無視される)、パフォーマンス除外が作成されます(ファイルは検査されません)。 | x | x |
| 検出による検出除外 | | x | x |
| 正確なファイル(ハッシュ)による検出除外 | | x | x |
| リアルタイムファイルシステム保護 | x | x | x |
| ネットワークボリュームの互換性を上げる | x | 不要 | 不要 |
| ログインユーザーでの検査 | | x | x |
| ローカルドライブの検査 | x | x | x |
| リムーバブルメディアの検査 | x | x | x |
| ネットワークドライブの検査 | x | x | x |
| 開く時、作成時に検査 | x | x | x |
| 実行時の検査 | x | ファイルを開くときに実施 | ファイルを開くときに実施 |
| プロセスの除外 | | x | x |
| クラウドベース保護 | x | x | x |
| ESET LiveGrid®レピュテーションシステム | x | x<br>(拡張) | x<br>(拡張) |
| ESET LiveGrid®フィードバックシステム | x | x | x |
| 送信できる項目の詳細な設定 | | x | x |
| マルウェア検査(オンデマンド) | x | x | x |
| シンボリックリンクの検査 | x | x | x |
| 電子メールファイルの検査 | x | x | x |
| メールボックスの検査 | x | x | x |
| アーカイブの検査 | x | x | x |
| 自己解凍アーカイブの検査 | x | x | x |
| ランタイムパッカーの検査 | x | x | x |
| 代替データストリーム(ADS)を検査 | x | x | x |
| SMART最適化を有効にする | x | x | x |
| システムフォルダを検査から除外する | x | 必要なし | 必要なし |
| 低優先でバックグラウンド検査 | | x | x |
| 最終アクセスのタイムスタンプを保持 | x | x | x |
| 起動時の検査 | x | | |

| 機能 | バージョン6 | (ESET Endpoint Antivirus) バージョン7.3 & 7.4 | バージョン8 |
|---|---|---|---|
| **Webとメール保護** | | | |
| アプリケーション除外 | x | x | x |
| IPアドレス除外 | x | x | x |
| Webアクセス保護(HTTP検査) | x | x | x |
| 電子メールクライアント保護 | x | x | x |
| フィッシング対策機能 | x | x | x |
| **モジュールアップデーター** | | | |
| プライマリ/セカンダリアップデートサーバーのカスタムプロキシサーバー | x | x | x |
| モジュールのロールバック | x | x | x |
| リリース前アップデート | x | x | x |
| 遅延アップデート | x | x | x |
| **その他の主要な機能** | | | |
| デバイスコントロール | x | | |
| ファイアウォール | x | | x |
| Webコントロール | x | | |
| ERMMサポート(リモート監視と管理統合のためのコマンドラインインターフェース) | x | | |
| ESET Enterprise Inspectorサポート | x | x | x |
| **その他の細かい機能** | | | |
| コマンドラインインタフェース | x | x (ESET Endpoint for Linuxと統合) | x (ESET Endpoint for Linuxと統合) |
| 検出ログ | x | x | x |
| イベントログ | x | x | x |
| コンピューターの検査ログ | x | x | x |
| 設定のインポート/エクスポート | x | x | x |
| 隔離 | x | x | x |
| ローカルタスクスケジューラ | x | x | x |
| プロキシサーバー設定 | x | x | x |
| プレゼンテーションモード | x | x (システムネイティブの「おやすみモード」) | x (システムネイティブの「おやすみモード」) |
| **ユーザーインターフェース** | | | |
| ログファイル | x | x | x |
| 検出された脅威 | x | x | x |
| イベント | x | x | x |
| コンピュータの検査 | x | x | x |
| デバイスコントロール | x | | |

| 機能 | バージョン6 | (ESET Endpoint Antivirus) バージョン7.3 & 7.4 | バージョン8 |
|---|---|---|---|
| ファイアウォール | x | | x |
| フィルタリングされたWebサイト | x | x | x |
| Webコントロール | x | | |
| ログのフィルタ | x | x | x |
| 保護統計 | x | x | x |
| スケジューラ | x | x | x |
| 実行中のプロセス | x | | |
| 隔離 | x | x | x |
| 分析のためにファイルを提出 | x | x (7.4) | x |
| 現在の状況 | x | x | x |
| 手動モジュールアップデート | x | x | x |
| ユーザーによるローカル設定/設定 | x | x | x |
| GUIからの設定のインポート/エクスポート | x | x | x |
| ヘルプ | x | x | x |
| 新しいネイティブグラフィカルユーザーインターフェース | | x | x |
| ダークモードのサポート | | x | x |
| 高解像度ディスプレイサポート | x | x | x |
| ユーザーにGUIを無効にする機能 | | x | x |
| ネイティブ通知 | | x | x |
| メニューバー | x | x | x |
| メニューバーアイコンを非表示にする機能 | x | x | x |
| コンテキストメニューの統合 | x | | x |
| GUIに表示/ESET PROTECT On-PremまたはESET PROTECTに報告される保護の状態の詳細制御 | x | x | x |
| システムアップデート通知 | x | x | x |
| **インストール** | | | |
| ローカルGUIベースのインストール | x | x | x |
| コンポーネントベースのインストール | x | | x |
| リモートコンポーネントベースのインストール(コンポーネントインストールには追加手順が必要) | x | | x |
| サイレントインストールサポート(MDM事前承認経由) | x | x | x |
| 再インストールによる製品のアップデート | x | x | x |
| ESET PROTECT On-PremまたはESET PROTECTからの製品のアップデート | x | x | x |
| **製品のアクティベーション** | | | |
| 製品認証キーでアクティベーション | x | x | x |

| 機能 | バージョン6 | (ESET Endpoint Antivirus) バージョン7.3 & 7.4 | バージョン8 |
|---|---|---|---|
| サブスクリプションライセンスサポート | x | x | x |
| ESET PROTECT On-PremまたはESET PROTECT経由でのアクティベーション | x | x | x |
| オフラインライセンスファイルを使用したアクティベーション | x | x | x |
| **ESET管理コンソールとの互換性** | | | |
| ESET PROTECTとの互換性 | x | x | x |
| ESET PROTECT On-Premとの互換性 | x | x | x |

# 変更ログ

# システム要件

ESET Endpoint Security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 | Intel 64-bit, Apple ARM 64-bit |
| OS | macOS Big Sur (11)からmacOS Sequoia (15) |
| メモリ | 300 MB |
| 空きディスク容量 | 600 MB |

ESET Endpoint Securityは、インストール中にインターネットに接続している必要があります。

# インストール/アップグレード/移行

## インストール方法

| インストール方法 | インストールタイプ | 注意 |
|---|---|---|
| GUIインストール | ローカル | インストール.dmgファイルからローカルでESET Endpoint Securityをインストールできます。インストールを開始する前に、すべての開いているコンピュータープログラムを終了します。ESET Endpoint Securityには、コンピューターにインストールされている他のウイルス対策プログラムと競合する可能性のあるコンポーネントが含まれています。このため、他のすべてのウイルス対策プログラムを削除し、潜在的な問題を防止することを強く推奨します。インストール後、オンボーディングウィザードが表示されたら、ここで説明されている手順に従って、コンピューターの保護を確保します。 |

| インストール方法 | インストールタイプ | 注意 |
| --- | --- | --- |
| コマンドラインインストール | ローカル/リモート | インストーラーのGUIを操作せずにESET Endpoint Securityをインストールできます。この方法を使用して、リモートでESET Endpoint Securityをインストールできます。リモートでESET Endpoint Securityをインストールしている場合は、インストール前に、MDM経由でユーザー同意設定を適用することをお勧めします。 |
| ESET PROTECT On-Prem | リモート | ESET PROTECT On-Premでコンピューターが登録されている場合は、インストールタスクを作成し、ターゲットコンピューターにESET Endpoint Securityをインストールできます。 |
| ESET PROTECT | リモート | ESET PROTECTでコンピューターが登録されている場合は、インストールタスクを作成し、ターゲットコンピューターにESET Endpoint Securityをインストールできます。 |

ESET Endpoint Securityが機能するには、ユーザーの同意設定が必要です。これらの設定は、インストール後に手動で適用する必要があります。各コンピューターにユーザー同意設定を追加しないようにするには、デバイスをMDMに登録する必要がありますMDMは構成プロファイルをターゲットコンピューターに配布するために使用されます。インストール前にこれらの設定を適用しない場合、複数のポップアップダイアログがユーザーに表示され、ユーザーは手動でユーザー同意設定を適用する必要がありますESET Endpoint Securityのインストール前に構成プロファイルを配布することをお勧めします。

# オンボーディング

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

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

2.必須手順:**コンポーネントインストール:既定のインストール**、またはインストールするコンポーネントを選択する**カスタムインストール**のいずれかを選択します。

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

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

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

6.必須手順:**ESETネットワークアクセス保護**を許可します。アラートウィンドウで、**許可**を選択します。

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

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

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

> **オンボーディングウィザードを再起動しています**
> Finder > **アプリケーション**を開く > Controlキーを押しながら**ESET Endpoint Security**アイコンをクリック（または右クリック）> ショートカットメニューから**パッケージの内容を表示**を選択 > Contents を開く > Helpers > **オンボーディング**を開く。必須のセキュリティ設定は、手動オンボーディングの章に従って手動で設定することもできます。

ESET Endpoint Securityをインストールした後、悪意あるコードを対象としたコンピューターの検査を実行する必要があります。そのために、メインプログラムウィンドウから**検査**をクリックし、**今すぐ検査**をクリックします。オンデマンドコンピューターの検査の詳細については、オンデマンドコンピューターの検査の章を参照してください。

# システム拡張機能を許可する

初めてESET Endpoint Securityをインストールする場合は、**システム拡張機能**を完全に保護することを許可する必要があります。

> システム拡張を許可する手順を実行する前に、ESET Endpoint Securityがアクティベーションされていることを確認してください。

macOS Sequoia (15)

1. **システム設定**を開きます。
2. 左メニューの**一般**を選択します。
3. **ログイン項目&拡張機能**を選択し、**拡張機能**まで下にスクロールします。
4. **エンドポイントセキュリティ拡張機能**の横にある情報記号ⓘをクリックし、トグルを使用して**ESETリアルタイムファイルシステム保護**をオンにします。**Touch ID**を使用するか、**パスワードを使用**をクリックし、**パスワード**を入力して**OK**をクリックします。**完了**をクリックします。
5. **ネットワーク拡張機能**の横にある情報記号ⓘをクリックし、トグルを使用して**ESET Webとメール保護**をオンにします。**Touch ID**を使用するか、**パスワードを使用**をクリックし、**パスワード**を入力して**OK**をクリックします。
6. **ESET Endpoint Security**アラートが表示され、**他のアプリからのデータアクセス**をリクエストされたら、**許可**をクリックします。
7. **ESET Webとメール保護**アラートを表示し、**プロキシ設定**を追加するよう指示されます。**許可**]を選択します。
8. トグルを使用して、**ESETネットワークアクセス保護**をオンにします。**Touch ID**を使用するか、**パスワードを使用**をクリックし、**パスワード**を入力して**OK**をクリックします。
9. ESET Endpoint Securityは**ネットワークコンテンツをフィルタリングしようとしています**という通知が表示されたら、**許可**をクリックします。そうしないと、ファイアウォールが機能しません。
10. **デバイスが新しいネットワークに接続しています**というアラートウィンドウが表示された場合は、接続しているネットワークが**プライベート**か**パブリック**かを指定します。
11. **完了**をクリックします。

macOS Ventura (13)またはmacOS Sonoma (14)

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

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

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

macOS Monterey (12)以前

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

# フルディスクアクセスを許可

初めてESET Endpoint Securityをインストールする場合は、**フルディスクアクセス**を完全に保護することを許可する必要があります。

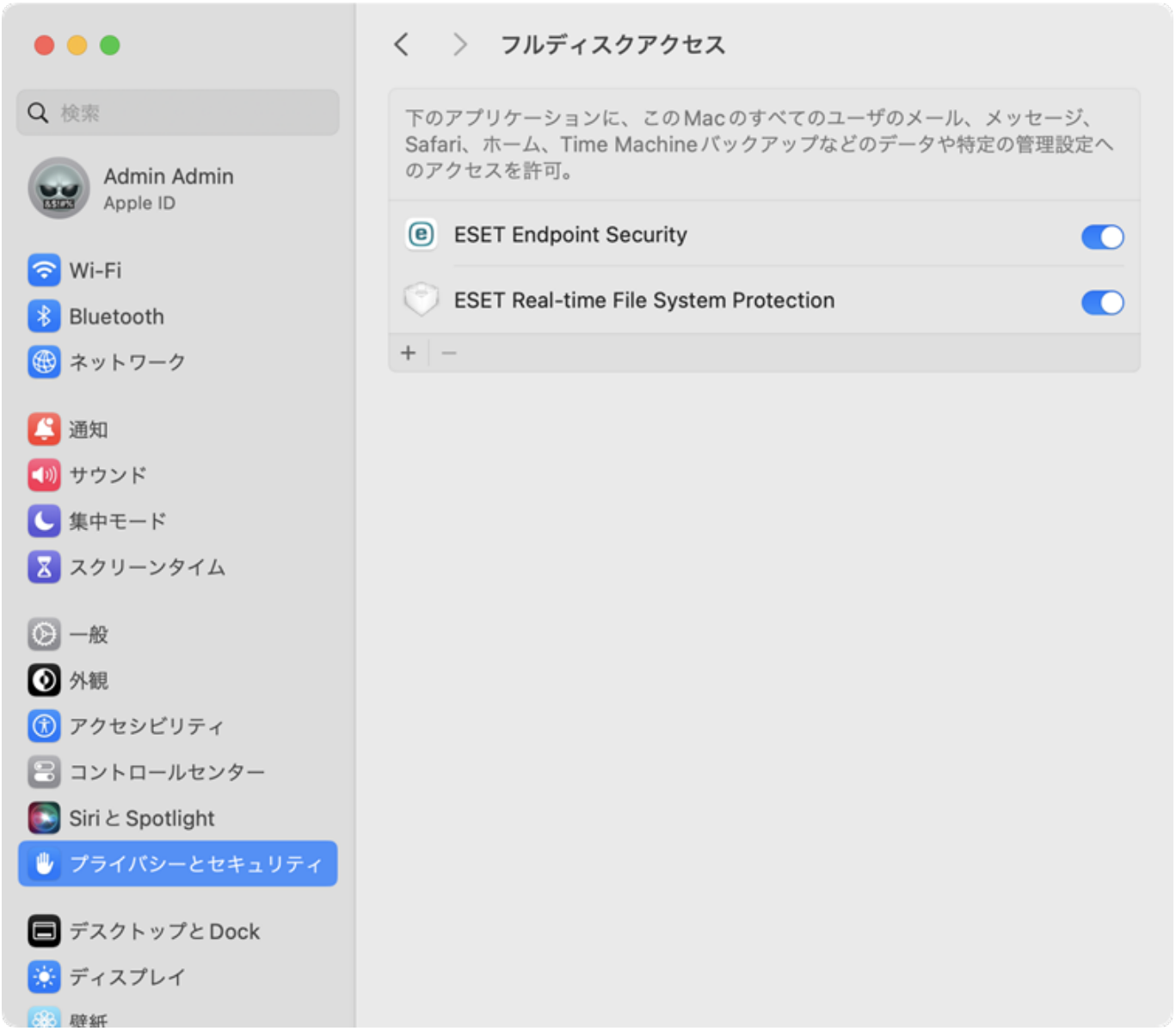
> フルディスクアクセスを許可する手順を実行する前に、ESET Endpoint Securityがアクティベーションされていることを確認してください。

macOS Sequoia (15)

1. **システム設定**を開きます。
2. 左側のメニューで**プライバシーとセキュリティ**を選択します。
3. **フルディスクアクセス**を選択します。
4. トグルを使用して**ESET Endpoint Security**にフルディスクアクセスを付与します。**Touch ID**を使用するか、**パスワードを使用**をクリックし、**パスワード**を入力して**設定の変更**をクリックします。
5. トグルを使用して、**ESETリアルタイムファイルシステム保護**にフルディスクアクセスを付与します。

macOS Ventura (13)またはmacOS Sonoma (14)

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




[macOS Monterey (12)以前]

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

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

8. 警告ダイアログウィンドウで**再開**をクリックしてESET Endpoint Securityを再起動して変更を確認するか、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。

# コマンドラインインストール

コマンドライン経由でESET Endpoint SecurityをインストールしてGUIインストールをスキップします。コンピューターがMDMに登録されていない場合は、システム設定で手動でESET Endpoint Securityのユーザーアクセス権を許可する必要があります。

> コマンドラインインストールを使用してリモートでESET Endpoint Securityをインストールする場合は、ESET Endpoint Securityのインストール前に、MDM経由でユーザー同意設定の構成プロファイルを配布することをお勧めします。構成プロファイル設定は、インストール前設定のトピックを参照してください。

1. ダウンロードESET Endpoint Security

2. ダウンロードした.dmgファイルをマウントするには、ファイルをダブルクリックするか、次のコマンドラインプロセスを使用します。

   a.ターミナルでファイルの場所に移動します。ターミナルでファイルの場所に移動します。`cd ~/Downloads`と入力します。
   `Downloads`をダウンロードしたファイルの場所に置換します。

   b.`hdiutil attach ees_osx_mlp_0.dmg`と入力します。
   `ees_osx_mlp_0`をファイル名に置き換えてください。

3. ターミナルで`sudo installer -pkg /Volumes/ESET\ Endpoint\ Antivirus/.resources/Installer.pkg -target /`と入力します。
   Installer.pkgへのパスは自分のInstaller.pkgの場所に置換する必要がある場合があります。

4. インストール後、完全な保護を許可するには、手動オンボーディングでESET Endpoint Securityのユーザーの同意設定を許可する必要があります。

# リモートインストール

## インストールの前に

ESET Endpoint Securityでは、デバイスをMDMに登録せずにリモートで完全にインストールすることを防止する権限設定が必要です。デバイスがMDMに登録されている場合は、MDMを使用して、設定プロファイル経由でこれらの設定を配布できます。デバイスがMDMに登録されていない場合は、これらの権限設定を各コンピューターで手動で許可する必要があります。

Jamfを使用している場合は、Jamf固有のガイドもご確認ください。

# ESET Endpoint Securityの構成プロファイルの設定

ESET Endpoint Securityをインストールする前に、ターゲットコンピューターで次の設定を有効にする必要があります。

- **ESETシステム拡張機能**
  インストール前にESETシステム拡張機能が有効ではない場合、ESETシステム拡張機能が有効になるまで、ユーザーは**システム拡張機能がブロックされた**という通知を受信します。

- **フルディスクアクセス**
  インストール前にフルディスクアクセスが有効ではない場合、フルディスクアクセスが有効になるまで、ユーザーは**コンピューターの一部が保護されている**という通知を受信します。

- **ネットワーク**
  ファイアウォールが機能するには、ファイアウォール設定をシステム設定に追加する必要があります。
  ESET Endpoint Securityインストール後にファイアウォール設定が不足している場合、「ESET Endpoint Security」**がネットワークコンテンツをフィルタリングしようとしている**というメッセージが表示されます。この通知を受信したときには、**許可**をクリックします。**許可しない**をクリックすると、ファイアウォールが動作しません。

- **Webとメール保護**
  Webとメール保護が機能するには、Webとメール保護設定をシステム設定に追加する必要があります。
  ESET Endpoint Securityインストール後にWebとメール保護設定が不足している場合、「ESET Endpoint Security」**がネットワークコンテンツをフィルタリングしようとしている**というメッセージが表示されます。この通知を受信したときには、**許可**をクリックします。**許可しない**をクリックすると、Webとメール保護が動作しません。

上記のESET設定をリモートで有効にするには、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。

必要なインストール前設定をすべて有効にするには、ESET Endpoint Securityバージョン8用の.plistペイロードファイルをダウンロードし、それを使用してMDMに設定プロファイルを作成します。コンポーネントのインストールによってプログラムコンポーネントを無効にする場合は、それらのコンポーネントをMDM設定プロファイルからも削除する必要があります。

## ESETシステム拡張機能を有効にする

デバイスのシステム機能拡張をリモートで有効にするには、インストール前にMDMで設定プロファイルを作成します。次の設定を使用します。

| | |
|---|---|
| Team ID (TeamID) | P8DQRXPVLP |
| バンドルID (BundleID) | com.eset.endpoint<br>com.eset.network<br>com.eset.firewall |

## フルディスクアクセスを有効にする

フルディスクアクセスをリモートで有効にするには、インストール前に次の手順のいずれかを実行します。

• デバイスがESET PROTECT On-PremまたはESET PROTECTで管理されている場合、ESET Management Agentのフルディスクアクセスも有効にする必要があります。ESET Management Agentの.plistペイロードファイルをダウンロードします。

• 次の設定を使用して、構成プロファイルを作成します。

**ESET Endpoint Security**

| | |
|---|---|
| ID | com.eset.ees.g2 |
| IDタイプ | bundleID |
| コード要件 | identifier "com.eset.ees.g2" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| アプリまたはサービス | SystemPolicyAllFiles |
| アクセス | 許可 |

| | |
|---|---|
| ID | com.eset.endpoint |
| IDタイプ | bundleID |
| コード要件 | identifier "com.eset.endpoint" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| アプリまたはサービス | SystemPolicyAllFiles |
| アクセス | 許可 |

**ESET Endpoint Securityバージョン8の追加設定**

| | |
|---|---|
| ID | com.eset.network |
| IDタイプ | bundleID |
| コード要件 | identifier "com.eset.network" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| アプリまたはサービス | SystemPolicyAllFiles |
| アクセス | 許可 |

| | |
|---|---|
| ID | com.eset.firewall |
| IDタイプ | bundleID |
| コード要件 | identifier "com.eset.firewall" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| アプリまたはサービス | SystemPolicyAllFiles |
| アクセス | 許可 |

**macOS 12 Montereyの以降**

| | |
|---|---|
| ID | com.eset.app.Uninstaller |
| IDタイプ | bundleID |
| コード要件 | identifier "com.eset.app.Uninstaller" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| アプリまたはサービス | SystemPolicyAllFiles |
| アクセス | 許可 |

**ESET Management Agent**

| | |
|---|---|
| ID | com.eset.remoteadministrator.agent |
| IDタイプ | bundleID |
| コード要件 | identifier "com.eset.remoteadministrator.agent" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| アプリまたはサービス | SystemPolicyAllFiles |
| アクセス | 許可 |

フルディスクアクセスとシステム拡張機能をリモートで許可した後、システム設定>プライバシーとセキュリティでこれらの設定が無効として表示される場合があります。ESET Endpoint Securityに警告が表示されない場合は、システム設定>プライバシーとセキュリティのステータスに関係なく、フルディスクアクセスとシステム拡張機能が許可されます。

## ファイアウォール

ファイアウォール設定をシステム設定にリモートで追加するには、インストール/アップグレードの前にファイアウォールのコンテンツフィルター設定プロファイルを作成します。次の設定を使用します。

| | |
|---|---|
| ID | com.eset.firewall.manager |
| フィルター順序 | Firewall |
| ソケットフィルター | com.eset.firewall |
| ソケットフィルター指定要件 | identifier "com.eset.firewall" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |

## Webとメール保護

Webとメール保護の設定をシステム設定にリモートで追加するには、インストール前にVPNタイプの設定プロファイルを作成します。次の設定を使用します。

| | |
|---|---|
| VPNタイプ | VPN |
| 接続タイプ | Custom SSL |

| | |
|---|---|
| カスタムSSL VPN ID | com.eset.network.manager |
| サーバー | localhost |
| プロバイダーバンドルID | com.eset.network |
| ユーザー認証 | 証明書 |
| プロバイダータイプ | App-proxy |
| プロバイダー指定要件 | identifier "com.eset.network" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| アイドルタイマー | 切断しない |
| プロキシ設定 | なし |

Webとメール保護設定は、ESET Endpoint Securityのアンインストール後に削除されます。ESET Endpoint Securityをアンインストールしてインストールする必要がある場合は、アンインストール後にWebとメール保護設定をターゲットコンピューターに展開する必要があります。

# Jamfインストール前設定

必要なインストール前設定をすべて有効にするには、ESET Endpoint Securityバージョン8用の.plistペイロードファイルをダウンロードし、それを使用してMDMに設定プロファイルを作成します。コンポーネントのインストールによってプログラムコンポーネントを無効にする場合は、それらのコンポーネントをMDM設定プロファイルからも削除する必要があります。

## ESET Endpoint Securityの設定プロファイルを手動で設定する

Jamfメインウィンドウで、**コンピューター > 構成プロファイル**をクリックします。

## Webとメール保護

Webとメール保護が機能するには、Webとメール保護設定をシステム設定に追加する必要があります。ESET Endpoint Securityインストール後にWebとメール保護設定が不足している場合、ESET Endpoint Securityがネットワークコンテンツをフィルタリングしようとしているというメッセージが表示されます。

> Webアクセス保護設定は、ESET Endpoint Securityのアンインストール後に削除されます。ESET Endpoint Securityをアンインストールして再インストールする必要がある場合は、Webとメール保護設定をターゲットコンピューターに再展開する必要があります。

**一般**セクションで次の項目を入力します。

| | |
|---|---|
| 名前 | ESET Webとメール保護など |
| レベル | コンピューターレベル |
| 配布方法 | 通常:自動的にインストール |

**VPN**セクションで次の項目を入力します。

| | |
|---|---|
| VPNタイプ | VPN |

| | |
|---|---|
| 接続タイプ | カスタムSSL |
| ID | com.eset.network.manager |
| サーバー | localhost |
| プロバイダーバンドルID | com.eset.network |
| ユーザー認証 | 証明書 |
| プロバイダータイプ | アプリプロキシ |
| プロバイダー指定要件 | identifier "com.eset.network" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| ID証明書 | なし |
| アイドルタイマー | 切断しない |
| プロキシ設定 | なし |

---

## ESETシステム拡張機能を有効にする

**一般**セクションで次の項目を入力します。

| | |
|---|---|
| 名前 | ESET SEXTなど |
| レベル | コンピューターレベル |
| 配布方法 | 通常、自動的にインストール |

**システム拡張機能**セクションで次の項目を入力します。

| | |
|---|---|
| 表示名 | ESET SEXTなど |
| システム拡張機能タイプ | 許可されたシステム拡張機能 |
| Team ID | P8DQRXPVLP |
| 許可されたシステム拡張機能 | com.eset.endpoint<br>com.eset.network<br>com.eset.firewall<br>com.eset.devices |

---

## フルディスクアクセスを有効にする

**一般**セクションで次の項目を入力します。

| | |
|---|---|
| 名前 | ESET Full disk accessなど |
| レベル | コンピューターレベル |
| 配布方法 | 通常、自動的にインストール |

**プライバシー設定ポリシー制御**セクションで次の項目を入力します。

| | |
|---|---|
| ID | com.eset.endpoint |
| IDタイプ | bundle ID |
| コード要件 | identifier "com.eset.endpoint" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| アプリまたはサービス | SystemPolicyAllFiles |
| アクセス | 許可 |

| | |
|---|---|
| ID | com.eset.ees.g2 |
| IDタイプ | bundle ID |
| コード要件 | identifier "com.eset.ees.g2" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| アプリまたはサービス | SystemPolicyAllFiles |
| アクセス | 許可 |

| | |
|---|---|
| ID | com.eset.network |
| IDタイプ | bundle ID |
| コード要件 | identifier "com.eset.network" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| アプリまたはサービス | SystemPolicyAllFiles |
| アクセス | 許可 |

| | |
|---|---|
| ID | com.eset.firewall |
| IDタイプ | bundle ID |
| コード要件 | identifier "com.eset.firewall" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| アプリまたはサービス | SystemPolicyAllFiles |
| アクセス | 許可 |

| | |
|---|---|
| ID | com.eset.app.Uninstaller |
| IDタイプ | bundle ID |
| コード要件 | identifier "com.eset.app.Uninstaller" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |

| | |
|---|---|
| アプリまたはサービス | SystemPolicyAllFiles |
| アクセス | 許可 |

フルディスクアクセスとシステム拡張機能をリモートで許可した後、システム設定>プライバシーとセキュリティでこれらの設定が無効として表示される場合があります。ESET Endpoint Securityに警告が表示されない場合は、システム設定>プライバシーとセキュリティのステータスに関係なく、フルディスクアクセスとシステム拡張機能が許可されます。

### ファイアウォール

ファイアウォール設定をシステム設定にリモートで追加するには、インストール/アップグレードの前にファイアウォールのコンテンツフィルター設定プロファイルを作成します。次の設定を使用します。

| | |
|---|---|
| ID | com.eset.firewall.manager |
| フィルター順序 | Firewall |
| ソケットフィルター | com.eset.firewall |
| ソケットフィルター指定要件 | identifier "com.eset.firewall" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |

# リモートコンポーネントインストール

設定ファイルを作成し、どのESET Endpoint Securityコンポーネントをアクティブにし、どのコンポーネントを無効にするかを定義することで、選択したコンポーネントのリモートインストールが可能です。

## 設定ファイルの作成

設定ファイルはJSON形式で、**コンポーネントインストールユーティリティ**で作成できます。ESET Endpoint Securityのコンポーネントはすべてファイル内に含まれており、それぞれをオンまたはオフに切り替えることができます。

このファイルは、インストーラーが自動的に認識できるように、以下の場所に保存する必要があります。

```
/Library/Application Support/ESET/Security/ComponentInstallation/comp_install.json
```

`owner:group`を`root:wheel`に設定し、`640` (-rw-r-----)のアクセス権を持つようにファイルを設定する必要があります。

上記のように、**コンポーネントインストールユーティリティ**を使用して設定ファイルを出力できます。あるいは、 `./compinst --print`オプションを使用してアプリケーションバンドルに含めてから、設定を変更します。以下に示すように形式を定義して手動で作成することもできます。

```
{
  "antiphishing":1,
  "email_access":1,
```

```
  "network_access":1,
  "vapm":1,
  "web_protection":1
}
```

ESET Endpoint Securityのコンポーネントの完全なリストについては、**コンポーネントインストールユーティリティ**の出力オプションを使用してください。

# ESET管理コンソールによる展開

ESET Endpoint Securityでは、デバイスをMDMに登録せずにリモートで完全にインストールすることを防止する権限設定が必要です。デバイスがMDMに登録されている場合は、MDMを使用して、設定プロファイル経由でこれらの設定を配布できます。デバイスがMDMに登録されていない場合は、これらの権限設定を各コンピューターで手動で許可する必要があります。

## ESET PROTECT On-Prem

ESET PROTECT On-Prem経由でESET Endpoint Securityを展開する前に、ESET Management Agentをターゲットコンピューターに配布する必要があります。

1.ESET Management Agentをインストールするには、エージェントライブインストーラーを作成します。

2.macOSエージェントライブインストーラーをダウンロードします。

3.ダウンロードした.tar.gzアーカイブから.shスクリプトを抽出します。

4.ターゲットコンピューターで. shスクリプトを展開して実行し、エージェントをインストールしますMDMとしてJamfを使用する場合は、Jamfを使用してスクリプトを展開および実行できます。

5.エージェントがターゲットコンピューターにインストールされた後、ESET PROTECT On-Premでコンピューターが表示されます。

ESET Endpoint Securityをインストールするには、ESET PROTECT On-Premでソフトウェアインストールタスクを作成して実行します。

---

## ESET PROTECT

ESET PROTECTとESET Management Agentを同時に使用してESET Endpoint Securityをインストールするには、ライブインストーラーを作成します。

ESET PROTECT On-PremまたはESET PROTECTに接続されたライセンスを所有している場合は、ライセンスが自動的にインストールパッケージに追加されESET Endpoint Securityが自動的にアクティベーションされます。

# ESET Endpoint Securityをバージョン8へアップグレードする

ESET Endpoint AntivirusまたはESET Endpoint Securityバージョン6をバージョン8にアップグレードした後、ESET Endpoint Securityは既定の設定に戻ります。つまり、カスタマイズされた設定またはポリシーは既定値にリセットされます。

## アップグレード方法

- ローカルアップグレード(ローカルコンピューターで直接アップグレードを実行できます。)
- コマンドラインによるアップグレード(コマンドラインの指示を使用してアップグレードします。)
- ESET管理コンソールによるアップグレード(複数のエンドポイントを管理している場合、この一元化されたコンソールを使用すると、ネットワーク全体で効率的にアップグレードできます。)
- 設定の移行(アップグレードプロセス中に既存の設定が正しく移行されるようにします)。

## ローカルアップグレード

1. 最新のESET Endpoint Securityインストールファイル(.dmg)をダウンロードします。

2. インストールファイル(.dmg)を開きます。

3. **ESET Endpoint Securityのインストール**アイコン  をダブルクリックします。

4.他のセキュリティアプリケーションがインストールされていない場合は、**続行**をクリックします。別のウイルス対策アプリケーションがインストールされている場合は、インストールが失敗する可能性があります。

5. **続行**をクリックして、システム要件を確認します。

6. **同意**をクリックして、エンドユーザーライセンス契約およびプライバシーポリシーに同意します。

7. インストール先フォルダーを変更するか、すべてのユーザーがESET Endpoint Securityにアクセスできる場合は、**インストール先の変更**をクリックします。インストールを開始するには、**インストール**をクリックします。

インストール先を変更

インストール先を選択します。コンピューターのすべてのユーザーまたは現在のユーザーのみのどちらに対してESET Endpoint Securityをインストールするのかを選択しますESET Endpoint Securityインストールする特定のフォルダーを選択することもできます。オプションを選択し、**続ける**をクリックして、**インストールの種類**手順に戻ります。

8. インストールの開始時に管理者パスワードを入力するように指示される場合があります。

9. **閉じる**をクリックすると、インストールが完了します。

10. インストール後、オンボーディングウィザードが表示されたら、ここで説明されている手順に

従って、コンピューターの保護を確保します。

---

## コマンドライン経由でのアップグレード

コマンドラインを使用してESET Endpoint Securityをバージョン8にアップグレードするには

1.ESET Endpoint Securityバージョン8をダウンロードします。

2..dmgファイルをターゲットコンピューターに配布します。

3.コマンドラインインストールトピックの説明に従い、インストールを実行します。

---

## ESET PROTECT On-PremまたはESET PROTECT経由でのESET Endpoint Securityのアップグレード

ESET Endpoint Antivirusは、バージョン8にアップグレードすると、名前がESET Endpoint Securityに変更されます。
ESET Endpoint AntivirusまたはESET Endpoint Securityバージョン6からアップグレードする場合は、新しい設定プロファイルを使用することをお勧めします。ダウンロードするESET Endpoint Securityバージョン8の新しい設定プロファイルについては、インストール前設定トピックを参照してください。新しい設定プロファイルを展開した後は、バージョン6の設定プロファイルを削除し、ESET管理コンソール経由の展開トピックでインストールを続行します。

アップグレード前に、MDMの設定プロファイルで次の変更を行う必要があります。

**フルディスクアクセス**設定プロファイル

| **バージョン6 (ESET Endpoint Security)** | | **バージョン8 (ESET Endpoint Security)** | |
|---|---|---|---|
| ID | com.eset.ees.6 | ID | com.eset.ees.g2 |

| **バージョン6 (ESET Endpoint Antivirus)** | | **バージョン8 (ESET Endpoint Security)** | |
|---|---|---|---|
| ID | com.eset.eea.6 | ID | com.eset.ees.g2 |

| **バージョン7 (ESET Endpoint Antivirus)** | | **バージョン8 (ESET Endpoint Security)** | |
|---|---|---|---|
| ID | com.eset.eea.g2 | ID | com.eset.ees.g2 |

macOS 12以降にESET Endpoint Securityをインストールする場合は、Uninstaller.appのフルディスクアクセスを追加する必要があります。これは、システムからバージョン6を削除し、将来バージョン8をリモートでアンインストールするために必要です。フルディスクアクセス設定プロファイルに次の情報を追加します。

| macOS 12 MontereyのESET Endpoint Security | |
|---|---|
| ID | com.eset.app.Uninstaller |
| IDタイプ | bundleID |
| コード要件 | identifier "com.eset.app.Uninstaller" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |
| アプリまたはサービス | SystemPolicyAllFiles |
| アクセス | Allow |

**Webとメール保護**設定プロファイル

| バージョン6 | | バージョン8 | |
|---|---|---|---|
| カスタムSSL VPN ID | com.eset.sysext.manager | カスタムSSL VPN ID | com.eset.network.manager |

### ファイアウォール

ファイアウォール設定をシステム設定にリモートで追加するには、インストール/アップグレードの前にファイアウォールのコンテンツフィルター設定プロファイルを作成します。次の設定を使用します。

| ID | com.eset.firewall.manager |
|---|---|
| フィルター順序 | Firewall |
| ソケットフィルター | com.eset.firewall |
| ソケットフィルター指定要件 | identifier "com.eset.firewall" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP |

バージョン8にアップグレードする前にバージョン6の設定を削除すると、設定が適用されていない場合のように、ユーザーに通知が表示されます。ESET Endpoint Securityバージョン8の新しい設定プロファイルを作成し、設定プロファイルをターゲットコンピューターに展開して、ESET Endpoint Securityをアップグレードし、バージョン6の設定プロファイルを削除することをお勧めします。また、1つのデバイスにESET Endpoint Securityのインストールポリシーが1つだけであることを確認することをお勧めします。ESET PROTECT On-PremとJamf両方を使用する場合は、それぞれのインストールポリシーが1つだけであることを確認してください。

# 設定の移行

## 移行プロセス

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

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

ESET Endpoint Securityバージョン6に存在するすべての機能がバージョン8に存在するわけではないため、ESET PROTECT On-PremとESET PROTECTのポリシーは自動的には移行されません。バージョン8にアップグレードした後、既存のポリシーを確認し、バージョン8の機能に基づいて新しいポリシーを作成する必要があります。ポリシーを作成または削除する方法の詳細については、「ポリシー」トピックを参照してください。

- ESET PROTECT On-Premのポリシー
- ESET PROTECTのポリシー

ESET Endpoint Securityバージョン6およびバージョン8のESET PROTECT On-PremおよびESET PROTECTのポリシーは同時にアクティブにできます。

既にバージョン6からバージョン8にESET Endpoint Securityをアップグレードしている場合でも、新しいバージョンにアップグレードして設定を移行できます。手順については、ESETナレッジベースの移行に関する記事を参照してください。

バージョン8.Xで使用可能なすべての設定はバージョン6から移行されますが、次の例外があります。

- 権限設定(バージョン8ではサポートされていません)
- アップデートのカスタムプロキシサーバー(カスタムプロキシはバージョン8でサポートされていません)
- 隔離コンテンツ
- 検査の駆除レベル
- オンデマンド検査の対象プロファイル

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

- デバイスコントロール
- Webコントロール

### その他のアプリケーションの問題

- カスタム検査プロファイルは移行されESET PROTECT On-PremESET PROTECTまたはアプリケーション環境設定で管理できます。

# ライセンスを見つける方法

ライセンスを購入した場合は、ESETから2件の電子メールが届きます。最初の電子メールにはESET Business Accountポータルに関する情報が記載されています。2番目の電子メールには、製品認証キー(XXXXX-XXXXX-XXXXX-XXXXX)ライセンスID (xxx-xxx-xxx)製品名(または製品のリスト)、および数量の詳細情報が記載されています。

ESET Endpoint Security機能は、購入したライセンスの種類によって利用できるようになります。ライセンスにすべてのセキュリティ機能が含まれていない場合は、**メインアプリケーションメニュー** > **概要**にアラートが表示され、**ライセンスをアップグレードすると完全な保護を受ける**ことができます。

# ローカルアクティベーション

1.ESET Endpoint Securityを開く

2.製品のアクティベーションセキュリティアラートで、**アクティベーションダイアログ**をクリックします。


3.アクティベーションダイアログウィンドウが開きます。製品認証キーを入力して、続行をクリックします。

4.**完了**をクリックします。

ESET Endpoint Security機能は、購入したライセンスの種類によって利用できるようになります。ライセンスにすべてのセキュリティ機能が含まれていない場合は、**メインアプリケーションメニュー** > **概要**にアラートが表示され、**ライセンスをアップグレードすると完全な保護を受ける**ことができます。

# ターミナル経由でのアクティベーション

特権ユーザーでsudo /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/licユーティリティを使用して、ターミナルウィンドウからESET Endpoint Securityをアクティベーションします。

構文: sudo /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/lic [OPTIONS]

## 例

```
sudo /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/lic -k XXXX-XXXX-XXXX-XXXX-XXXX

sudo /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/lic --key XXXX-XXXX-XXXX-XXXX-XXXX
```

1. 実行

```
sudo /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/lic -u your@username
```

ここでyour@usernameはEBAまたはEMAアカウントのユーザー名を表しています。パスワードを入力し、Enterキーを押します。使用可能なEESライセンスIDとサイト(ライセンスプール)のリストが表示されます。1つ目のライセンスIDはpool_IDで、2つ目がpublic_IDです。

2. 以下のようにコマンドの後にEBAまたはEMAアカウントのユーザー名を入力し、さらにpublic_ID(-p XXX-XXX-XXX)またはpool_ID(-i XXXXXXXX-XXXX-XXXX-XXXXXXXXXXXX).のいずれかを入力します。

```
sudo /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/lic -u your@username -p XXX-XXX-XXX

sudo /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/lic -u your@username -i XXXXXXXX-XXXX-XXXX-XXXXXXXXXXXX
```

3. パスワードをもう一度入力し、**Enter**キーを押して、「**アクティベーションが正常に完了しました**」というメッセージが表示されるまで待ちます。

```
sudo /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/lic -f ofline_license.lf

sudo /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/lic --file=offline.license.lf
```

# リモートアクティベーション

ESET PROTECT On-PremまたはESET PROTECT経由でESET Endpoint Securityをインストールしていて、ESET PROTECT On-PremまたはESET PROTECTに接続されたライセンスを所有している場合は、ライセンスが自動的にインストールパッケージに追加され、ESET Endpoint Securityが自動的にアクティベーションされます。

## ESET PROTECTを使用してリモートでESET Endpoint Securityをアクティベーションする

後でESET PROTECT On-PremまたはESET PROTECT経由でESET Endpoint Securityをアクティベーションするには、ESET PROTECT Webコンソールにログインし、製品のアクティベーションクライアントタスクを使用します。

# リモート管理されたエンドポイントのドキュメント

ESET Endpoint Securityバージョン8は、ESET PROTECTまたはESET PROTECT On-Premによってリモートで管理できます。ESETリモート管理ツールを使用すると、1つの集中管理された場所から、ESETソリューションの展開、タスクの管理、セキュリティポリシーの施行、システムステータスの監視、およびリモートコ

ンピューターでの問題や脅威に対する迅速な対応が可能です。

## ESETリモート管理ツール

ESET Endpoint Securityは、ESET管理コンソールによってリモートで管理できます。

- ESET PROTECT On-Premの概要
- ESET PROTECTの概要

## モバイルデバイス管理(MDM)

リモートでESET Endpoint Securityをインストールするには、デバイスがMDMに登録されている必要があります。デバイスがMDMに登録されていない場合は、各デバイスに物理的にアクセスしてESET Endpoint Securityをインストールする必要があります。

モバイルデバイス管理(MDM)ソリューションにより、管理者は組織および設定ポリシーの展開、デバイスの監視、アプリケーションのインストールまたはアンインストールができます。一部のMDMソリューションはAppleデバイスをサポートしていません。MDMソリューションの選択を支援するためにAppleはMDMソリューションの選定ガイドを作成しています。

MDMの詳細については、Appleドキュメントと MDMベンダー固有のドキュメントを参照してください。

MDM経由で実行する必要があるESET Endpoint Security設定には、MDMで設定プロファイルを作成するために使用できる汎用ダウンロード可能なペイロードが含まれます。MDMとしてJamfを使用する場合は、Jamf固有のガイドも使用できます。

# ESET PROTECTの製品設定

ESET Endpoint Securityをリモートで設定するには:

1. ESET PROTECTで**ポリシー** > **新しいポリシー**をクリックし、ポリシーの名前を入力します。

**ESET Endpoint for macOS (V7+)**の既存のポリシーの設定を調整するには、ポリシーのリストで変更するポリシーをクリックし、**設定の編集** > **設定**をクリックします。

2. **設定**をクリックして、ドロップダウンメニューから**ESET Endpoint for macOS (V7+)**を選択します。
3. 任意の設定を調整します。
4. **続行** > 割り当てをクリックし、該当するコンピューターのグループを選択します。
5. **完了**をクリックします。

ESET Endpoint Securityをローカルで設定するには、アプリケーション環境設定を参照してください。

# 検出エンジン

検出エンジンは、ファイルを制御することで、悪意のあるシステム攻撃から保護します。たとえば、マルウェアに分類されたオブジェクトが検出された場合、修復が開始します。検出エンジンは、最初にブ

ロックし、その後に駆除、削除、または隔離に移動して、マルウェアを排除できます。

ESET Endpoint Securityをリモートで設定するには:

1. ESET PROTECTで**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。

**ESET Endpoint for macOS (V7+)**の既存のポリシーの設定を調整するには、ポリシーのリストで変更するポリシーをクリックし、**設定の編集 > 設定**をクリックします。

2. **設定**をクリックして、ドロップダウンメニューから**ESET Endpoint for macOS (V7+)**を選択します。

3. 任意の設定を調整します。

4. **続行** > 割り当てをクリックし、該当するコンピューターのグループを選択します。

5. **完了**をクリックします。

ESET Endpoint Securityをローカルで設定するには、アプリケーション環境設定を参照してください。

## 除外

パフォーマンス除外 – パス(フォルダー)を検査から除外することで、ファイルシステムのマルウェア検査に必要な時間を大幅に短縮できます。

除外を作成するには

1. パフォーマンス除外の横の編集をクリックします。

2. 追加をクリックし、スキャナーでスキップされるパスを定義します。任意で、情報用のコメントを追加します。

3. OK > 保存をクリックし、除外を作成してダイアログを閉じます。

# クラウドベース保護

ESET LiveGrid®は複数のクラウド技術から構成される高度な早期警告システムです。評価に基づいて新たな脅威を検出し、ホワイトリストによって検査パフォーマンスを改善します。

既定では ESET Endpoint Securityは、不審なファイルを分析するためにESET Research Labに送信するように設定されています .docまたは.xlsなど、特定の拡張子の付いたファイルは、常に除外されます。お客様やお客様の組織で送信したくない特定のファイルがあれば、他の拡張子を追加することもできます。

ESET Endpoint Securityをリモートで設定するには:

1. ESET PROTECTで**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。

**ESET Endpoint for macOS (V7+)**の既存のポリシーの設定を調整するには、ポリシーのリストで変更するポリシーをクリックし、**設定の編集 > 設定**をクリックします。

2. **設定**をクリックして、ドロップダウンメニューから**ESET Endpoint for macOS (V7+)**を選択します。

3. 任意の設定を調整します。

4. **続行** > 割り当てをクリックし、該当するコンピューターのグループを選択します。

5. **完了**をクリックします。

ESET Endpoint Securityをローカルで設定するには、アプリケーション環境設定を参照してください。

検出エンジン > クラウドベース保護では次の設定を構成できます。

# クラウドベース保護

**ESET LiveGrid®に参加する(推奨)**

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

**ESET LiveGrid®フィードバックシステムを有効にする**

詳細分析のため、データはESET Virus Labに送信されます。

**クラッシュレポートと診断データを送信**

クラッシュレポート、モジュールメモリダンプなどのデータを送信します。

**匿名の使用状況統計情報を送信し、製品の改善を支援する**

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

**連絡先の電子メールアドレス(任意)**

不審なファイルに連絡先の電子メールアドレスを添付することができます。このメールアドレスは、分析のために詳しい情報が必要な場合にユーザーに連絡するために使用されることがあります。詳しい情報が必要でない限り、ESETからユーザーに連絡することはありません。

# サンプルの送信

## 検出されたサンプルの自動送信

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

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

## 不審なサンプルの自動送信

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

**実行ファイル** – .exe, .dll, .sysなどの実行ファイルが含まれます。

**アーカイブ** – 次のアーカイブファイルタイプが含まれます.zip.rar.7z.arch.arj.bzip2.gzip.ace.arc.cab

**スクリプト** – 次のスクリプトファイルタイプが含まれます.bat.cmd.hta.js.vbs..ps1

**その他** – 次のファイルタイプが含まれます.jar.reg.msi.swf.lnk

**実行ファイル、アーカイブ、スクリプト、その他のサンプルをESETのサーバーから削除する** – 既定値は**「しない」に設定されています**

### 除外

**除外**の横の**編集**をクリックし、特定のファイルまたはフォルダーを送信から除外します。除外されたファイルは、不審なコードが含まれる場合でもESET Research Labに送信されません。

**サンプルの最大サイズ(MB)**

サンプルの最大サイズを定義します(1-64 MB)

## ESET LiveGuard

ESET LiveGuardは、特に、新しい脅威を軽減するために設計された、クラウドベース保護の層を追加する機能です。有効にすると、マルウェアであることがまだ確認されてなかったり、マルウェアが隠されている可能性がある不審なサンプルが自動的にESETcloudに送信されます。送信されたサンプルはサンドボックスで実行されESETの高度なマルウェア検出エンジンによって評価されます。

### ESET LiveGuardを有効にする

ESET LiveGuardを有効にすると、クラウドベースのテクノロジーを利用して新しいタイプの脅威を分析および検出できるので、セキュリティが強化されますESET LiveGrid®が有効になっている場合にのみESET LiveGuardを有効にできます。

### 検出しきい値

選択したしきい値以上の値を持つ結果が脅威として検出されます。しきい値は、**不審**な脅威、**非常に不審**な脅威、**悪意**のある脅威に設定できます。

### 検出後のアクション

脅威が検出された後のアクションを選択します。**実行中の処理を停止して駆除**または**次回アクセス時に駆除**から選べます。

### プロアクティブ保護

**実行をただちに許可する**または**分析結果を受信するまで実行をブロックする**モードを利用できます。ブロックモードでのプロアクティブ保護は、コンピューターの保護の強化に役立ちます。リムーバブルメディア上に配置されたか、アーカイブから抽出されたファイルが、サポートされているWebブラウザーまたは電子メールクライアントを使用して、ダウンロードされた場合、実行前にファイルを評価します。

### 分析結果の最大待機時間

この設定を調整する前に、平均分析時間を考慮します。この時間が経過すると、ユーザーは分析結果に関係なくサンプルを実行することができます。

### 不審なサンプルの自動送信

**文書** – アクティブなコンテンツが埋め込まれたMicrosoft Office、Libre Office、または他のオフィスツールで作成された文書やPDFが含まれます。

**ESETのサーバーから文書を削除する** – この値は、**しない**、**30日後**または**分析後即時**のいずれかに設定できます。

# マルウェア検査

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

ESET Endpoint Securityをリモートで設定するには：

1. ESET PROTECTで**ポリシー** > **新しいポリシー**をクリックし、ポリシーの名前を入力します。

**ESET Endpoint for macOS (V7+)**の既存のポリシーの設定を調整するには、ポリシーのリストで変更するポリシーをクリックし、**設定の編集** > **設定**をクリックします。

2. **設定**をクリックして、ドロップダウンメニューから**ESET Endpoint for macOS (V7+)**を選択します。

3. 任意の設定を調整します。

4. **続行** > 割り当てをクリックし、該当するコンピューターのグループを選択します。

5. **完了**をクリックします。

ESET Endpoint Securityをローカルで設定するには、アプリケーション環境設定を参照してください。

検出エンジン > マルウェア検査では、オンデマンド検査プロファイルのオプションを設定できます。

選択されたプロファイル – 編集するプロファイルを選択します。

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

ThreatSenseパラメーター – 制御するファイルの拡張子、検査するオブジェクト、使用される検出方法などの検査プロファイル設定オプション。詳細については、ThreatSenseパラメーターを参照してください。

# ThreatSense パラメータ

ThreatSenseは、ウイルスを検出する多数の複雑な方法から構成される技術です。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コード分析、コードエミュレーション、汎用シグネチャ、ウイルスシグネチャを組み合わせて使用します。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

てルートキットを除去することもできます。

ThreatSenseエンジン設定オプションを使用すると、さまざまな検査パラメータを指定できます。

- 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

セキュリティシナリオごとに異なる設定が必要になることがあります。これを念頭に、ThreatSenseは、次の保護モジュールについて個々に設定することができます。

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

ThreatSenseのパラメーターは機能ごとに高度に最適化されているので。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、常にランタイム圧縮形式をスキャンするようにパラメーターを変更するか、リアルタイムファイル保護機能のアドバンスドヒューリスティックを有効にすると、システムの処理速度が低下することがあります(通常は、新しく作成されたファイルのみがこれらの方法を使用してスキャンされます)。

# 検査するオブジェクト

このセクションでは、感染を検査するコンピュータのコンポーネントおよびファイルを定義できます。

電子メールファイル – プログラムは以下の拡張子をサポートします:DBX (Outlook Express)およびEML:

アーカイブ – プログラムは以下の拡張子をサポートします:ARJ:BZ2:CAB:CHM:DBX:GZIP:ISO/BIN/NRG:LHA:MIME:NSIS:RAR:SIS:TAR:TNEF:UUE:WISE:ZIP:ACE:およびその他多数。

自己解凍アーカイブ – 自己解凍アーカイブ(SFX)は自分自身を展開できるアーカイブです。

圧縮された実行形式 – 圧縮された実行形式(標準の解凍形式とは異なる)は、実行後メモリー内で解凍されます。スキャナーでは、コードのエミュレーションによって、標準の静的圧縮形式(例: UPX:yoda:ASPack:FSGなど)のほかにも他の多数の圧縮形式を認識できます。

# 検査オプション

システムの侵入を検査するときに使用する方法を選択します。使用可能なオプションは

ヒューリスティック – ヒューリスティックは、悪意のあるプログラムの活動を分析するアルゴリズムです。アドバンスドヒューリスティックを使用すると:ESET製品の脅威検出機能が大幅に高まります。シグネチャは確実にウイルスを検出し、特定することができます。欠点は、非常に少ないとはいえ、誤検出の可能性がある点です。

アドバンスドヒューリスティック/DNAシグネチャ – アドバンスドヒューリスティックは、ESETが開発した独自のヒューリスティックアルゴリズムで構成されます。このアルゴリズムは、コンピューターワームやトロイの木馬を検出するために最適化され、高度なプログラミング言語で記述されています。アド

バンスドヒューリスティックを使用するとESET製品の脅威検出機能が大幅に高まります。シグネチャは確実にウイルスを検出し、特定することができます。自動アップデートシステムを利用することにより、新しいシグネチャを使用するためのウイルス検出時間を短縮できます。シグネチャの欠点は、既知のウイルス(またはこれらのウイルスの多少の変更が加えられたバージョン)しか検出しない点です。

## 駆除

ThreatSenseパラメーターには次の駆除レベルがあります。

| 駆除レベル | 説明 |
|---|---|
| 駆除なし | エンドユーザーは、オブジェクトの駆除中に対話型ウィンドウが表示され、アクション(削除または無視など)を選択する必要があります。このレベルは、検出された場合に実行する手順を理解している上級ユーザー向けに設計されています。 |
| 標準駆除 | オブジェクトの駆除中に検出の駆除を試みます。ユーザー操作はありません。一部の場合(システムファイルや、感染していないファイルと感染したファイルの両方を含むアーカイブなど)で、検出を駆除できない場合は、報告されたオブジェクトは元の場所に残されます。 |
| 厳密な駆除 | オブジェクトの駆除中に検出の駆除を試みます。ユーザー操作はありません。ごく一部の場合(システムファイルなど)で、検出を駆除できない場合は、報告されたオブジェクトは元の場所に残されます。 |
| 完全な駆除 | オブジェクトの駆除中に検出の駆除を試みます。一部の場合で、アクションを実行できない場合は、エンドユーザーにインタラクティブアラートが表示され、エンドユーザーが駆除アクション(削除または無視など)を選択する必要があります。ほとんどの場合、この設定が推奨されます。 |
| 削除 | エンドユーザーの操作を必要とせずに、すべての感染ファイルの削除を試行します。 |

## 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。

## その他

オンデマンドコンピューターの検査でThreatSenseエンジンパラメータを設定する場合は、[その他]セクションの次のオプションも設定できます。

代替データストリーム(ADS)を検査-NTFS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は、通常の検査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。

低優先でバックグラウンドで検査 – 検査が行われるたびに、一定の量のシステムリソースが使用されます。システムリソースにかなりの負荷がかかるプログラムを使用している場合、優先度が低い検査をバックグラウンドで実行することによって、アプリケーションのためにリソースを節約することができます。

スマート最適化を有効にする – スマート最適化を有効にすると、スキャンの速度を最高に保ちながら最も効率的なスキャンレベルが確保されるように、最適な設定が使用されます。さまざまな保護モジュールで高度に検査を行い、それぞれで異なる検査方法を使用して、それらを特定のファイルタイプに適用します。スマート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検査の実行時に適用されます。

最終アクセスのタイムスタンプを保持 – データバックアップシステムでの利用などを考慮して、検査済みファイルへのアクセス日時を更新せずに元のまま保持するには、このオプションを選択します。

### 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。

### オブジェクトの設定

既定のオブジェクト設定の横のスライダーバーを無効にし、次のオプションを設定します。

オブジェクトの最大サイズ – 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。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。既定値は無制限です。

オブジェクトの最長検査時間(秒) – オブジェクトの検査の最長時間の値を定義します。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。既定値:無制限

### アーカイブ検査の設定

既定のアーカイブ検査設定の横のスライダーバーを無効にし、次のオプションを設定します。

スキャン対象の下限ネストレベル – アーカイブの検査の最大レベルを指定します。既定値:10.

スキャン対象ファイルの最大サイズ – このオプションでは、検査対象のアーカイブ(抽出された場合)に含まれているファイルの最大サイズを指定できます。既定値は無制限です。

一般的な環境で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。

## 追加のThreatSenseパラメータ

これらの設定は、リアルタイムファイルシステム保護でのみ使用できます。

新しく作成または修正されたファイルの感染の可能性は、既存のファイルよりも比較的高くなります。この理由により、プログラムはこれらのファイルを追加の検査パラメーターで確認しますESET Endpoint Securityは検出エンジンの更新がリリースされる前に、定義ベースの検査方法と組み合わせてアドバンスドヒューリスティックを使用し、新しい脅威を検出します。

新規に作成したファイル以外に、自己解凍アーカイブのファイル(SFX)および圧縮された実行形式(内部圧縮された実行可能ファイル)も検査されます。既定では、アーカイブは10番目の入れ子レベルまで検査され、実際のサイズに関わらずチェックされます。アーカイブ検査設定を変更するには、既定のアーカイブ検査の設定オプションを選択解除します。

## 駆除レベル

| 駆除レベル | 説明 |
| --- | --- |
| 駆除なし | エンドユーザーは、オブジェクトの駆除中に対話型ウィンドウが表示され、アクション(削除または無視など)を選択する必要があります。このレベルは、検出された場合に実行する手順を理解している上級ユーザー向けに設計されています。 |
| 標準駆除 | オブジェクトの駆除中に検出の駆除を試みます。ユーザー操作はありません。一部の場合(システムファイルや、感染していないファイルと感染したファイルの両方を含むアーカイブなど)で、検出を駆除できない場合は、報告されたオブジェクトは元の場所に残されます。 |
| 厳密な駆除 | オブジェクトの駆除中に検出の駆除を試みます。ユーザー操作はありません。ごく一部の場合(システムファイルなど)で、検出を駆除できない場合は、報告されたオブジェクトは元の場所に残されます。 |
| 完全な駆除 | オブジェクトの駆除中に検出の駆除を試みます。一部の場合で、アクションを実行できない場合は、エンドユーザーにインタラクティブアラートが表示され、エンドユーザーが駆除アクション(削除または無視など)を選択する必要があります。ほとんどの場合、この設定が推奨されます。 |
| 削除 | エンドユーザーの操作を必要とせずに、すべての感染ファイルの削除を試行します。 |

# アップデート

このセクションでは、アップデートサーバーやそれらのサーバーの認証データなど、アップデート用の設定情報を指定します。

ESET Endpoint Securityをリモートで設定するには:

1. ESET PROTECTで**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。

**ESET Endpoint for macOS (V7+)**の既存のポリシーの設定を調整するには、ポリシーのリストで変更するポリシーをクリックし、**設定の編集 > 設定**をクリックします。

2. **設定**をクリックして、ドロップダウンメニューから**ESET Endpoint for macOS (V7+)**を選択します。

3. 任意の設定を調整します。

4. **続行** > 割り当てをクリックし、該当するコンピューターのグループを選択します。

5. **完了**をクリックします。

ESET Endpoint Securityをローカルで設定するには、アプリケーション環境設定を参照してください。

アップデートでは、次の設定を構成できます。

## 基本

既定では、アップデートの種類は定期アップデートです。これにより、検出定義データベースと製品モジュールが ESETアップデートサーバーから自動的にアップデートされることが保証されます。

リリース前アップデートには、まもなく公開される予定の最新の不具合修正と検出方法が含まれます。ただし、これらは必ずしも安定しているとは限らないため、本番環境での使用は推奨されません。

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

安定しているとみなされます)。

### モジュールロールバック

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

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

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

### 製品のアップデート

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

**カスタムサーバー**セクションでは、アップデートを保存する場所として使用するHTTP(S)サーバー、ローカルドライブ、またはリムーバブルドライブを指定できますESET Endpoint Securityのサーバーまたはドライブにアクセスできるようにするには、該当する**ユーザー名**と**パスワード**を入力します。

# アップデートミラー(カスタムアップデートサーバー)

「ミラーサーバーの作成」の使用 - LAN環境でアップデートファイルのコピーを作成すると、ベンダのアップデートサーバーからワークステーションごとに繰り返しアップデートファイルをダウンロードしなくて済むので便利です。アップデートがローカルのミラーサーバーにダウンロードされ、すべてのワークステーションに配信されるため、ネットワークトラフィックが過負荷状態になる危険性を回避することができます。ミラーからクライアントワークステーションをアップデートすると、ネットワークの負荷分散が最適化されると共に、インターネット接続の帯域幅が節約されます。

ESET Endpoint Securityをリモートで設定するには:

1. ESET PROTECTで**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。

**ESET Endpoint for macOS (V7+)**の既存のポリシーの設定を調整するには、ポリシーのリストで変更するポリシーをクリックし、**設定の編集 > 設定**をクリックします。

2. **設定**をクリックして、ドロップダウンメニューから**ESET Endpoint for macOS (V7+)**を選択します。

3. 任意の設定を調整します。

4. **続行** > 割り当てをクリックし、該当するコンピューターのグループを選択します。

5. **完了**をクリックします。

ESET Endpoint Securityをローカルで設定するには、アプリケーション環境設定を参照してください。

アップデート>プライマリサーバーまたはセカンダリサーバーでは、アップデートミラー(カスタムアップデートサーバー)を使用するようにESET Endpoint Securityを設定できます。

1. 基本セクションで、自動選択の横のスライダーバーを無効にします。

2. アップデートサーバーフィールドに、次の形式のいずれかを使用して、ミラーサーバーのURLアドレスを入力します。

http://<IP>:<port>

http://<hostname>:<port>

アップデートをインストールするには、次のサーバーを使用する必要があります:http://update.eset.com/eset_upd/businessmac/

3. **ミラーからのアップデート**セクションで、該当するユーザー名とパスワードを入力します。

ネットワークで使用可能なその他のミラーサーバーがある場合は、上記の手順を繰り返して、セカンダリサーバーを設定します。

# 保護

**エンジン感度**は、保護設定の一部として定義されます。侵入のカテゴリごとに、**レポート**と**保護**のレベルを**最大**から**標準**/**最小**の範囲で設定できます。または、検出を完全に**オフ**にすることもできます。検出応答を変更できる侵入のタイプを以下に示します。

## マルウェア検出

マルウェア – コンピューターの既存のファイルに含まれる悪意のあるコード。

## 望ましくない可能性が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マルウェアタイプ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。

## 疑わしい可能性があるアプリケーション

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。このようなプロテクターは、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。

## 安全ではない可能性があるアプリケーション

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

# 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、システムで発生する、ウイルスが関係するイベントを全て検査します。ファイルは全て、コンピューター上で開くとき、作成するとき、または実行するときに、悪意のあるコードがないか検査されます。既定では、リアルタイムファイルシステム保護はシステム起動時に起動し、中断なしに検査を行います。

ESET Endpoint Securityをリモートで設定するには:

1. ESET PROTECTで**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。

**ESET Endpoint for macOS (V7+)**の既存のポリシーの設定を調整するには、ポリシーのリストで変更するポリシーをクリックし、**設定の編集 > 設定**をクリックします。

2. **設定**をクリックして、ドロップダウンメニューから**ESET Endpoint for macOS (V7+)**を選択します。

3. 任意の設定を調整します。

4. **続行** > 割り当てをクリックし、該当するコンピューターのグループを選択します。

5. **完了**をクリックします。

ESET Endpoint Securityをローカルで設定するには、アプリケーション環境設定を参照してください。

検出エンジン > リアルタイムファイルシステム保護では次の設定を構成できます。

## リアルタイムファイルシステム保護

既定では、リアルタイムファイルシステム保護はシステム起動時に起動し、中断なしに検査を行います。特殊な場合(別のリアルタイムスキャナーと競合する場合など)は、リアルタイムファイルシステム保護を有効にするの横のスライダーバーをクリックして、リアルタイムファイルシステム保護を無効にできます。

### 検査するメディア

既定では、あらゆる種類のメディアに対して潜在的な脅威が検査されます。

- ローカルドライブ – システムハードディスクをすべて検査します。
- リムーバブルメディア - CD/DVD、USB記憶装置、Bluetoothデバイスなどを検査します。
- ネットワークドライブ – マッピングされたドライブをすべて検査します。

既定の設定を使用し、あるメディアの検査によりデータ転送が極端に遅くなるときなど、特別な場合にかぎり既定の設定を変更することをお勧めします。

### 検査のタイミング

既定では、ファイルを開いたり、作成したり、実行したりするときに、すべてのファイルが検査されます。既定の設定ではコンピュータ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。

- ファイルのオープン – 開いたファイルの検査を有効または無効にします。
- ファイルの作成 – 作成するファイルの検査を有効または無効にします。
- リムーバブルメディアのアクセス – コンピューターに接続するときにリムーバブルメディアの自動検査を有効または無効にします。

### プロセスの除外

検査から除外するプロセス – プロセスを検査から除外することで、システムのマルウェア検査に必要な時間を大幅に短縮できます。

除外を作成するには

1. 検査対象外とするプロセスの横の編集をクリックします。
2. 追加をクリックして、実行ファイルへのパスを定義します。
3. 保存 > 保存をクリックし、除外を作成してダイアログを閉じます。

## ThreatSense パラメータ

リアルタイムファイルシステム保護は、ファイルアクセスなど、さまざまなシステムイベントごとにトリガされ、すべての種類のメディアを確認します。リアルタイムファイルシステム保護は、ThreatSense テクノロジの検出方法(「ThreatSenseエンジンのパラメーターの設定」セクションに説明があります)を使用しており、新しく作成されたファイルを既存のファイルと異なる方法で扱うように設定できます。たとえば、新しく作成されたファイルを今までよりも細かく監視するように、リアルタイムファイルシステム保護を設定できます。

# ネットワークアクセス保護

## ネットワーク接続プロファイルの割り当て

ネットワーク接続プロファイルは自動的に割り当てられます。

## ネットワーク接続プロファイル

ネットワーク接続プロファイルにより、ネットワーク接続の特定のカテゴリにファイアウォールルールを適用できます。ネットワーク接続は、信頼などのプロファイルのプロパティも継承します。組み込みのプロファイルを使用することも、カスタムプロファイルを作成することもできますが、どちらもネットワーク接続に自動的に割り当てられます。ネットワーク接続でプロファイルがアクティブな場合、グローバルルール(プロファイルの指定がないルール)と選択したプロファイルに割り当てられているルールのみが適用されます。ネットワーク接続に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。

### プライベートネットワーク接続プロファイル

信頼できるホームネットワークまたはオフィスネットワーク用のプロファイルで、デバイス間でファイルとリソースを共有し、よりシームレスでコラボレーション可能なネットワークエクスペリエンスを提供します。

### パブリックネットワーク接続プロファイル

セキュリティを優先し、ネットワーク上の他のデバイスとのファイルやリソースの共有を制限する、パブリックまたは信頼できないネットワーク環境用のプロファイル。

## ネットワーク接続プロファイルを追加または編集する

**編集**をクリックして、ネットワーク接続プロファイルを設定できます。既存のプロファイルを**編集**、**削除**、または**コピー**するか、**追加**をクリックし、以下のすべてのフィールドを指定して、新しいプロファイルを作成します。

**名前** – プロファイルのカスタム名。

**説明** – プロファイルの識別に役立つプロファイルの説明。

**追加の信頼できるアドレス** – ここで定義したアドレスは、このプロファイルが適用されるネットワーク接続の信頼ゾーンに追加されます(ネットワークの保護の種類に関係なく)。

**信頼できる接続** – コンピューターとコンピューターに保存された共有ファイルは他のネットワークユーザーに表示され、ネットワーク上の他のユーザーがシステムリソースにアクセスできます(共有ファイルとプリンターへのアクセスは有効、受信RPC通信は有効、リモートデスクトップ共有は利用可能)。セキュリティで保護されたローカルネットワーク接続のプロファイルを作成する場合は、この設定を使用することをお勧めします。直接接続されたネットワークサブネットもすべて信頼済みと見なされます。例えば、ネットワークアダプタがIPアドレス192.168.1.5とサブネットマスク255.255.255.0を使用してこのネットワークに接続する場合、サブネット192.168.1.0/24がネットワーク接続の信頼ゾーンに追加されます。アダプターに他にもアドレス/サブネットがある場合は、それらすべてが信頼されます。

アクティベートユーザー – ネットワーク接続プロファイルをネットワーク接続に割り当てるために満たす必要があるカスタム条件です。接続されたネットワークが、接続されたネットワークプロファイルのアクティベートユーザーで定義されているものと同じ属性を持つ場合、プロファイルはそのネットワークに適用されます。ネットワーク接続プロファイルには、1つまたは複数のアクティベートユーザーが含まれていることがあります。複数のアクティベートユーザーが含まれている場合は、ORロジックが適用されます(1つ以上の条件を満たす必要があります)。

カスタムネットワーク接続プロファイルの作成は、経験豊富なユーザーが行う必要があります。

## IPセット

IPセットは、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集合を表します。**編集**をクリックしてIPセットを設定できます。

### 事前定義されたIPセット:

- 信頼ゾーン—実際の信頼ゾーンは、これらのアドレスの他に、信頼できるネットワークで指定されたアドレスから計算されます。
- IDSの対象外とするアドレス。

- TCP/UDPポート表示ゾーン—利用できないTCP/UDPポートに関する通知を送信するアドレス。
- DNSサーバー。
- ローカルアドレス。
- ローカルサブネット。
- プライベートアドレス。
- 信頼できるリバースプロキシ—製品がX-Forwarded-Forヘッダーから送信元IPを取得できるプロキシのリスト。
- ローカル仮想マシン—内部仮想スイッチに接続された仮想アダプターに割り当てられたサブネット。

### ファイアウォール

この機能については、別の章のファイアウォールで説明します。

# アクティベートユーザー

**アクティベートユーザー**は、**ネットワーク接続プロファイル**を**ネットワーク接続**に割り当てるために満たす必要があるカスタム条件です。接続されたネットワークが、接続されたネットワークプロファイルのアクティベートユーザーで定義されているものと同じ属性を持つ場合、プロファイルはそのネットワークに適用されます。ネットワーク接続プロファイルには、1つまたは複数のアクティベートユーザーが含まれていることがあります。複数のアクティベートユーザーが含まれている場合は、ORロジックが適用されます(1つ以上の条件を満たす必要があります)。アクティベートユーザーは、ネットワーク接続プロファイルエディターで定義できます。カスタムネットワーク接続プロファイルの作成は、経験豊富なユーザーが行う必要があります。

次の**アクティベートユーザー**を使用できます(現在のネットワークの詳細を知りたい場合は、ネットワーク接続を参照してください)。

## アダプタ

**アダプタタイプ** – 選択したアダプタタイプでネットワーク接続が確立されている場合にプロファイルを適用します。

**アダプタ名** – ネットワークアダプタ名が一致する場合にプロファイルを適用します。

**アダプタIP** – ネットワークアダプターのIPアドレスまたはIPアドレスの範囲が一致する場合にプロファイルを適用します。

## DNS

**DNSサフィックス** – ドメイン名が一致する場合にプロファイルを適用します。

**DNS IP** - DNSサーバーのIPアドレスまたはIPアドレスの範囲が一致する場合にプロファイルを適用します。

### WINS

Windowsインターネットネームサービス(WINS)にマップされたIPアドレスが一致する場合にプロファイルを適用します。

### DHCP

**DHCP IP** - DHCP サーバーのIPアドレスと一致する場合。

### デフォルトゲートウェイ

**IP** – 既定のゲートウェイIPアドレスまたはIPアドレスの範囲が一致する場合にプロファイルを適用します。

**MACアドレス** – 既定のゲートウェイMACアドレスが一致する場合にプロファイルを適用します。

### Wi-Fi

**SSID** - SSID (Wi-Fiの名前) が一致する場合にプロファイルを適用します。

### Windowsプロファイル

Windowsプロファイル設定の場合は**任意**を選択します。

### 認証

ネットワーク認証によってネットワーク内の特定のサーバーが検索され、非対称暗号化(RSA)を使用してそのサーバーが認証されます。認証されるネットワーク名は、認証サーバー設定で設定した名前と一致する必要があります。名前は大文字と小文字を区別します。サーバー名は、IPアドレス、DNS、またはNetBIOS名として入力できます。

## ファイアウォール

ファイアウォールは、システムとの間のすべてのネットワークトラフィックを制御します。これは、指定されたフィルタリングルールに基づいて個々のネットワーク接続を許可または拒否することによって実現されます。リモートコンピューターからの攻撃に対して保護を提供し、一部のサービスをブロックできるようにします。

### ファイアウォールを有効にする

システムを保護するために、この機能を有効にしておくことをお勧めします。ファイアウォールを有効にすると、ネットワークトラフィックは両方向で検査されます。

### ルール

**ファイアウォールルール**は、すべてのネットワーク接続を効果的にテストするために使用される条件およびそれらの条件に割り当てられたすべてのアクションのセットを表します。ファイアウォールルールを使用すると、各種ネットワーク接続が確立されるときに実行されるアクションを定義できます。ルールは上から下へと評価され、最初の列に優先度が表示されます。評価中の各ネットワーク接続に対して、最初に一致するルールのアクションが使用されます。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。受信者側が送信を要求していない接続、安全でない接続、または不明な接続は、システムにセキュリティ上のリスクをもたらします。このような接続が確立された場合は、コンピューターに接続しようとしているリモートデバイスおよびアプリケーションに注意することをお勧めします。個人データを取得して送信しようとしたり、他の悪意のあるアプリケーションをホストワークステーションにダウンロードしようとしたりするマルウェアが多数あります。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。

[ルールの設定]では、信頼済みゾーンおよびインターネット内で個々のアプリケーションによって生成されるトラフィックに適用されたすべてのルールを表示することができます。ルールフィルタリング設定にアクセスするには**編集**をクリックします。ファイアウォールルールが多数ある場合は、フィルターを使用して特定のルールのみを表示できます。ファイアウォールルールをフィルター処理するには、ファイアウォールルールリストの上にある**その他のフィルター**をクリックします。次の条件に基づいてルールをフィルタリングできます。

- 元
- 方向
- アクション
- 可用性

既定では、定義済みのファイアウォールルールは非表示になっています。すべての定義済みルールを表示するには、**ビルトイン(定義済み)ルールを非表示**の横にあるトグルを無効にします。これらのルールを無効にできますが、定義済みルールは削除できません。

右上の拡大鏡アイコンをクリックしてルールを検索します。

## 列

**優先度** – ルールは上から下へと評価され、最初の列に優先度が表示されます。

**有効** – ルールが有効か無効かを示します。ルールを有効にするには、対応するチェックボックスを選択する必要があります。

**アプリケーション** – ルールの適用先のアプリケーション。

**方向** – 通信の方向(内向き/外向き/双方向)。

**アクション** – 通信のステータス(拒否/許可/確認)を表示します。

**名前** – ルールの名前ESETアイコンは、定義済みのルールを表します。

**適用回数** – ルールが適用された合計回数。

展開アイコンをクリックして、ルールの詳細を表示します。

## コントロール要素

**追加** - 新しいルールを作成します

**編集** - 既存のルールを変更します

**削除** – 既存のルールを削除します。

**コピー** – 選択したルールのコピーを作成します。

 最上位/上/下/最下位 – ルールの優先度レベルを調整できます(ルールは最上位から最下位へと実行されます)。

## フィルタリングモード

1.**自動モード** – このモードが既定のモードです。このモードは、ルールを定義する必要なく、ファイアウォールを容易かつ簡便に使用したいユーザーに適しています。自動モードでは、特定のシステムに対して標準の送信トラフィックが許可され、ネットワーク側から開始されていないすべての接続がブロックされます。また、ユーザー定義のカスタムルールを追加することもできます。

2.**ポリシーベースモード** – 接続を許可する特定のルールによって定義されていない全ての接続がブロックされます。経験豊富なユーザーは、ポリシーベースモードを使用することで、必要かつ安全な接続のみを許可するルールを定義することができます。

# ファイアウォールルールの追加または編集

ファイアウォールルールは、全てのネットワーク接続を効果的にテストするために使用される条件およびそれらの条件に割り当てられたアクションを表します。ネットワーク設定が変更(リモート側のネットワークアドレスやポート番号など)が変更された場合、ルールの影響を受けるアプリケーションが正しく動作していることを確認するには、ファイアウォールルールの編集または追加が必要な場合があります。カスタムファイアウォールルールの作成は、経験豊富なユーザーが行ってください。

ファイアウォールルールは、**保護 > ネットワークアクセス保護 > ファイアウォール > ルール > 編集**で追加または編集できます。ファイアウォールルールウィンドウで、**追加**または**編集**をクリックします。

**名前** – ルールの名前を入力します。

**有効** – トグルをクリックしてルールをアクティベーションします。

ファイアウォールルールのアクションと条件を追加します。

## アクション

**アクション** – このルールで定義された条件に一致する通信を**許可/ブロック**するか、通信が確立されるたびにESET Security Ultimateで**確認**するかを選択します。

**ログルール** – ルールが適用されると、ログファイルに記録されます。

**ログ記録の重大度** – このルールのログ記録の重大度を選択します。

[**ユーザーに通知**]を選択すると、ルールが適用されたときに通知が表示されます。

## OS

オペレーティングシステムを選択します。

## アプリケーション

このルールを適用するアプリケーションを指定します。

**アプリケーションパス** – アプリケーションのフルパスを指定します。アプリケーションの名前のみを入力しないでください。

**アプリケーション署名** – アプリケーション署名(公開者の名前)に基づいてルールをアプリケーションに適用できます。**有効な署名**を持つアプリケーション、または**特定の署名者によって署名**されたアプリケーションにルールを適用する場合に、ドロップダウンメニューから選択します。**特定の署名者によって署名**されたアプリケーションを選択する場合は、署名者の名前フィールドで署名者を定義する必要があります。

**App Storeアプリケーション** – ドロップダウンメニューでApp Storeからインストールされたアプリケーションを選択します。

**サービス** – アプリケーションの代わりにシステムサービスを選択できます。

**子プロセスに適用** – 一部のアプリケーションでは、アプリケーションウィンドウが1つしか表示されないのに、複数のプロセスが実行される場合があります。トグルをクリックして、指定したアプリケーションのすべてのプロセスに対してルールを有効にします。

# 方向

このルールの通信方向を選択します。

**双方向** – 内向きおよび外向きの通信

**内向き** – 内向きの通信のみ

**外向き** – 外向きの通信のみ

## IPプロトコル

このルールを特定のプロトコルにのみ適用する場合は、ドロップダウンメニューからプロトコルを選択します。

## ローカルホスト

このルールが適用されるローカルアドレス、アドレス範囲、またはサブネット。アドレスが指定されていない場合、ルールはローカルホストとのすべての通信に適用されますIPアドレス、アドレス範囲、またはサブネットをIPテキストフィールドに直接追加するかIPセットの横にある**編集**をクリックして既存のIPセットから選択できます。

## ローカルポート

ローカルポート番号。番号が指定されていない場合、ルールはすべてのポートに適用されます。1つの通信ポートまたは通信ポートの範囲を追加できます。

## リモートホスト

このルールが適用されるリモートアドレス、アドレス範囲、またはサブネット。アドレスが指定されていない場合、ルールはリモートホストとのすべての通信に適用されますIPアドレス、アドレス範囲、またはサブネットをIPテキストフィールドに直接追加するかIPセットの横にある**編集**をクリックして既存のIPセットから選択できます。

## リモートポート

リモートポート番号。番号が指定されていない場合、ルールはすべてのポートに適用されます。1つの通信ポートまたは通信ポートの範囲を追加できます。

## プロファイル

ファイアウォールルールは、特定のネットワーク接続プロファイルに適用できます。

**すべて** – ルールは、使用されているプロファイルに関係なく、すべてのネットワーク接続に適用されます。

**選択** – 選択したプロファイルに基づいて、特定のネットワーク接続にルールが適用されます。選択したいプロファイルの横にあるチェックボックスをオンにします。

# 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。

ESET Endpoint Securityをリモートで設定するには:

1. ESET PROTECTで**ポリシー** > **新しいポリシー**をクリックし、ポリシーの名前を入力します。

**ESET Endpoint for macOS (V7+)**の既存のポリシーの設定を調整するには、ポリシーのリストで変更するポリシーをクリックし、**設定の編集** > **設定**をクリックします。

2. **設定**をクリックして、ドロップダウンメニューから**ESET Endpoint for macOS (V7+)**を選択します。

3. 任意の設定を調整します。

4. **続行** > 割り当てをクリックし、該当するコンピューターのグループを選択します。

5. **完了**をクリックします。

ESET Endpoint Securityをローカルで設定するには、アプリケーション環境設定を参照してください。

Webとメール > Webアクセス保護では、次の設定を構成できます。

## 基本

Web保護を有効にする - Webブラウザーとリモートサーバー間のHTTP通信を監視します。

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

## Webプロトコル

HTTPプロトコルのチェックを有効にする – 任意のアプリケーションで使用されるHTTP通信を検査します。

HTTPプロトコルが使用するポートで定義されたポート上のトラフィックだけを検査します。必要に応じて、他の通信ポートを追加できます。複数のポート番号は、コンマで区切る必要があります。

## URLアドレス管理

URLアドレス管理を使用すると、ブロックに対するHTTPアドレスを指定して、検査からブロック、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。検出されたマルウェアは無視されますアドレスのリストにあるWebサイトは、悪意のあるコードを検査せずにアクセスされます。

許可アドレスリストの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の横のスライダーバーを有効にします。

リストを有効にするには、特定のリスト名のアクティブのリストの横のスライダーバーをオンにします。特定のリストからアドレスを入力するときに通知を受信するには、適用時に通知の横のスライダーバーをオンにします。

アドレス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0文字以上の任意の文字列を、疑問符は任意の1文字をそれぞれ表します。

除外するアドレスを指定する際は、特に注意する必要があります。このリストには信頼できる安全なアドレスのみを含める必要があるためです。同様に、このリストでは記号*および?を正しく使用する必要があります。

## プロトコルフィルタリング

プロトコルフィルタリングではThreatSense検査テクノロジを利用してPOP3IMAPおよびHTTPアプリケーションプロトコル経由で転送されるデータをフィルタリングできます。

**対象外のアプリケーション** – リスト内のアプリケーションの通信は、プロトコルコンテンツフィルタリングから除外されます。

**対象外のIPアドレス** – リスト中のエントリは製品コンテンツフィルタリングから除外されます。選択したIPアドレスとの通信は検査されません。このオプションは信頼できるとわかっているアドレスに対してのみ使用することをお勧めします。

**プロトコルフィルタリング詳細ログを有効にする** – すべてのイベントを記録して、問題の診断および解決を可能にします。

## ThreatSense パラメータ

ThreatSenseパラメーターを使用すると、検査するオブジェクト、使用される検出方法などのWebアクセス保護の設定オプションを指定できます。詳細については、ThreatSenseパラメーターを参照してください。

# 電子メールクライアント保護

電子メールクライアント保護 - POP3およびIMAPプロトコルを介して受信される電子メール通信を制御します。

ESET Endpoint Securityをリモートで設定するには:

1. ESET PROTECTで**ポリシー** > **新しいポリシー**をクリックし、ポリシーの名前を入力します。

**ESET Endpoint for macOS (V7+)**の既存のポリシーの設定を調整するには、ポリシーのリストで変更するポリシーをクリックし、**設定の編集** > **設定**をクリックします。

2. **設定**をクリックして、ドロップダウンメニューから**ESET Endpoint for macOS (V7+)**を選択します。

3. 任意の設定を調整します。

4. **続行** > 割り当てをクリックし、該当するコンピューターのグループを選択します。

5. **完了**をクリックします。

ESET Endpoint Securityをローカルで設定するには、アプリケーション環境設定を参照してください。

Webとメール > 電子メールクライアント保護では次の設定を構成できます。

# 基本

ESET Endpoint Securityをメールクライアントと統合すると、メールメッセージにおいて悪意のあるコードから積極的に保護するレベルが向上します。電子メール保護を有効にするをオンにすることをお勧めします。

# 電子メールプロトコル

IMAPとPOP3プロトコルは、メールクライアントアプリケーションでの電子メール通信の受信に最もよく使用されているプロトコルですIMAP(インターネットメッセージアクセスプロトコル)はメール受信のためのもう1つのプロトコルです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。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。

ESET Endpoint Securityでは、使用される電子メールクライアントに関係なく、さらに電子メールクライアントを再設定せずに、これらのプロトコルを保護します。IMAP/POP3プロトコルで使用されるポートで定義されたポート上のトラフィックだけが検査されます。必要に応じて、他の通信ポートを追加できます。複数のポート番号は、コンマで区切る必要があります。

## ThreatSense パラメータ

ThreatSenseパラメーターを使用すると、検査するオブジェクト、使用される検出方法などの電子メールクライアント保護の設定オプションを指定できます。詳細については、ThreatSenseパラメーターを参照してください。

# 電子メールタグ

電子メールが検査された後、スキャン結果を記載した通知をメールに追加することができます。受信電子メールと既読電子メールにタグメッセージを追加を選択できます。問題のあるHTMLメッセージの場合やメッセージがマルウェアによって偽造された場合は、タグメッセージが存在しないことがあることに注意してください。タグメッセージは、受信/既読電子メールに追加することができます。使用可能なオプションは次のとおりです。

- 追加しない – 検査通知は追加されません。
- 検出が発生したとき – 悪意のあるソフトウェアをもった検査通知のみに検査済みのマークが付

けられます(既定)。

- 検査時にすべての電子メール – 検査された全てのメールに検査通知が追加されます。

受信メールと既読メールの件名を更新 – 電子メールの保護で、感染しているメールの件名にウイルス警告を追加しない場合は無効にします。この機能は、感染している電子メールを件名に基づいて単純にフィルタリングする場合に有効です(電子メールプログラムでサポートされている場合)。また、受信者の信頼を高めることができ、マルウェアが検出された場合、特定の電子メールまたは送信者の脅威レベルについての貴重な情報を得ることができます。

検出された電子メールの件名に追加するテキスト – 感染メールの件名のプレフィックス形式を変更する場合はこのテンプレートを編集します。この機能を実行すると、メッセージの件名"Hello"が、"[occurred detection %VIRUSNAME%] Hello"で置き換えられます。変数の%VIRUSNAME%は検出を表します。

## プロトコルフィルタリング

プロトコルフィルタリングではThreatSense検査テクノロジを利用してPOP3IMAPおよびHTTPアプリケーションプロトコル経由で転送されるデータをフィルタリングできます。

**対象外のアプリケーション** – リスト内のアプリケーションの通信は、プロトコルコンテンツフィルタリングから除外されます。

**対象外のIPアドレス** – リスト中のエントリは製品コンテンツフィルタリングから除外されます。選択したIPアドレスとの通信は検査されません。このオプションは信頼できるとわかっているアドレスに対してのみ使用することをお勧めします。

**プロトコルフィルタリング詳細ログを有効にする** – すべてのイベントを記録して、問題の診断および解決を可能にします。

# ツール

ESET Endpoint Securityをリモートで設定するには:

1. ESET PROTECTで**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。

> **ESET Endpoint for macOS (V7+)**の既存のポリシーの設定を調整するには、ポリシーのリストで変更するポリシーをクリックし、**設定の編集 > 設定**をクリックします。

2. **設定**をクリックして、ドロップダウンメニューから**ESET Endpoint for macOS (V7+)**を選択します。
3. 任意の設定を調整します。
4. **続行** > 割り当てをクリックし、該当するコンピューターのグループを選択します。
5. **完了**をクリックします。

> ESET Endpoint Securityをローカルで設定するには、アプリケーション環境設定を参照してください。

ツールでは、次の設定を構成できます。

## スケジューラ

スケジューラでは、スケジュールされたオンデマンド検査タスクが、あらかじめ定義された設定やプロパティとともに管理され、開始されます。

タスクの横の編集をクリックすると、すべてのスケジュールされたタスクと設定プロパティの一覧が表示されます。

既存のスケジュールされたタスクの設定を編集するには、修正するタスクを選択して、編集をクリックします。タスクを削除するには、タスクを選択して、削除をクリックします。

新しいタスクを追加するには

1. リストの一番下にある追加をクリックします。

2. タスクの名前を入力し、タスク実行の時刻を設定します。

3. タスクが繰り返し実行される日を選択します。次へをクリックします。

4. スケジュールされた検査で使用する検査プロファイルを選択します。検査プロファイルを表示および編集するには、マルウェア検査を参照してください。

5. 検査対象を定義し、検出された項目が駆除されるかどうか、検査プロファイル設定で設定した除外もスケジュールされた検査で検査するかどうかを選択します。

6. 終了 > 保存をクリックします。

# プロキシサーバ

大規模なLANネットワークでは、コンピュータがプロキシサーバを介してインターネットと通信している場合があります。この構成を使用する場合は、次の設定を定義する必要があります。定義しなかった場合、プログラムは自動的にアップデートされません。

ESET Endpoint Securityをリモートで設定するには：

1. ESET PROTECTで**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。

**ESET Endpoint for macOS (V7+)**の既存のポリシーの設定を調整するには、ポリシーのリストで変更するポリシーをクリックし、**設定の編集 > 設定**をクリックします。

2. **設定**をクリックして、ドロップダウンメニューから**ESET Endpoint for macOS (V7+)**を選択します。

3. 任意の設定を調整します。

4. **続行** > 割り当てをクリックし、該当するコンピューターのグループを選択します。

5. **完了**をクリックします。

ESET Endpoint Securityをローカルで設定するには、アプリケーション環境設定を参照してください。

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

プロキシサーバーを設定するには

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

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

3. 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、プロキシに到達できない場合は、プロキシをバイパスし、直接ESETサーバーと通信します。

# ログファイル

ESET Endpoint Securityのログの設定を変更します。ESET PROTECT On-Premを使用してログファイルを表示できます。

ESET Endpoint Securityをリモートで設定するには:

1. ESET PROTECTで**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。

**ESET Endpoint for macOS (V7+)**の既存のポリシーの設定を調整するには、ポリシーのリストで変更するポリシーをクリックし、**設定の編集 > 設定**をクリックします。

2. **設定**をクリックして、ドロップダウンメニューから**ESET Endpoint for macOS (V7+)**を選択します。

3. 任意の設定を調整します。

4. **続行** > 割り当てをクリックし、該当するコンピューターのグループを選択します。

5. **完了**をクリックします。

ESET Endpoint Securityをローカルで設定するには、アプリケーション環境設定を参照してください。

ツール > ログファイルでは、次の設定を構成できます。

ログに記録する最低レベル

ログの詳細レベルは、ログファイルに含まれる詳細のレベルを定義します。

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

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

除されます。

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

Syslogファシリティ

Syslogファシリティは、類似したログメッセージをグループ化するために使用されるsyslogログパラメーターです。たとえば、デーモンログ(syslogファシリティデーモン経由でログを収集する)は~/log/daemon.logに移動できます(設定されている場合)。最近のsystemdおよびジャーナルへの切り替えにより、syslogファシリティの重要は低くなっていますが、ログのフィルタリングで使用できます。

# ユーザーインターフェース

ESET Endpoint Securityをリモートで設定するには:

1. ESET PROTECTで**ポリシー**>**新しいポリシー**をクリックし、ポリシーの名前を入力します。

**ESET Endpoint for macOS (V7+)**の既存のポリシーの設定を調整するには、ポリシーのリストで変更するポリシーをクリックし、**設定の編集**>**設定**をクリックします。

2. **設定**をクリックして、ドロップダウンメニューから**ESET Endpoint for macOS (V7+)**を選択します。

3. 任意の設定を調整します。

4. **続行** > 割り当てをクリックし、該当するコンピューターのグループを選択します。

5. **完了**をクリックします。

ESET Endpoint Securityをローカルで設定するには、アプリケーション環境設定を参照してください。

ユーザーインターフェースでは、次の設定を構成できます。

## ユーザーインターフェース要素

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

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

### 通知

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

ステータス

アプリケーションステータス - 編集をクリックすると、保護の状態ウィンドウに通知が表示されるアプリケーションステータスと、ESET PROTECT Webコンソールに報告されるアプリケーションステータスを設定できます。

# 脆弱性とパッチ管理

## 脆弱性とパッチ管理

### 脆弱性とパッチ管理を有効にする

有効にすると、脆弱性管理システムはデバイスを検査して、セキュリティリスクに対して脆弱な可能性のあるインストール済みソフトウェアを検出します。パッチ管理は、自動ソフトウェアアップデートによりこれらのリスクを修復し、デバイスのセキュリティ強化に役立ちます。

### アプリケーションの自動パッチ管理を有効にする

有効にすると、自動パッチ管理により、サポートされているインストール済みソフトウェアが最新バージョンに自動的に更新されます。作業の中断を避けるため、ソフトウェアは通常の勤務時間後(午後5時から午前8時の間)に更新されます。

### コンピューターの再起動オプション

特定のソフトウェアを更新するには、正常に完了するためにシステムの再起動が必要になる場合があります。作業を中断したり、不都合な状況が発生しないように、再起動が必要であることをエンドユーザーに通知する方法と時間をカスタマイズできます。

### 脆弱性とパッチ管理スケジューラ

この設定により、定期的な脆弱性検査を実行し、許可されたアプリケーションを更新する期間を選択できます。

### パッチ管理に必要な最小ディスク容量

ここで、パッチ管理が正しく機能するために必要なディスク容量を設定できます(2GBから4096 TBまでの範囲)。

# パッチ管理のカスタマイズ

## アプリケーションの自動パッチ管理カスタマイズ

### 自動パッチ戦略

**許可されたアプリケーションにのみパッチを適用**オプションでは、**許可されたアプリケーション**リストのアプリケーションのみがアップデートされます。

**除外されたアプリケーションを除くすべてにパッチを適用**は、**除外されたアプリケーション**リストのアプリケーションを除くすべてのアプリケーションをアップデートします。

### 許可されたアプリケーション

ここで、自動的に更新しても安全なアプリケーションを指定できます。

### 対象外のアプリケーション

ここで、自動的に更新するには重要すぎるアプリケーションを指定できます。

# ESET PROTECTの概要

ESET PROTECTではESET PROTECT On-PremやESET Security Management Centerなどの物理または仮想サーバーを必要とせずに、ネットワーク環境におけるワークステーションおよびサーバー上のESET製品を、集中管理された1つの場所から管理できますESET PROTECT Webコンソールを使用すればESETソリューションの展開、タスクの管理、セキュリティポリシーの施行、システムステータスの監視、リモートコンピューターでの問題や脅威への迅速な対応が可能です。

- ESET PROTECTオンラインユーザーガイドをお読みください

# ESET PROTECT On-Premの概要

ESET PROTECT On-Premで、ネットワーク接続環境におけるワークステーションおよびサーバー上のESET製品を1つの集中管理された場所から管理できます。

ESET PROTECT Webコンソールを使用するとESETソリューションの展開、タスクの管理、セキュリティポリシーの施行、システムステータスの監視、リモートコンピューターでの問題や検出への迅速な対応ができます。ESET PROTECT On-Premアーキテクチャおよびインフラストラクチャ要素の概要ESET PROTECT Webコンソールの基本操作サポートされているデスクトッププロビジョニング環境を参照してください。

ESET PROTECT On-Premは次のコンポーネントで構成されています。

- ESET PROTECT サーバー - ESET PROTECTサーバーはWindowsとLinuxにインストールでき、仮想アプライアンスとして付属しています。エージェントとの通信を処理し、アプリケーションデータを収集し、データベースに保存します。

- ESET PROTECT Webコンソール - ESET PROTECT Webコンソールは、環境内のクライアントコンピューターを管理できるメインのインターフェースです。ネットワーク上のクライアントについてステータスの概要を表示し、管理対象外のコンピューターにリモートでESETソリューションを展開できますWebサーバーをインターネット上で公開すると、インターネットに接続されているすべての場所とデバイスからESET PROTECTを使用できますWebサーバーをインターネット上で公開すると、インターネットに接続されているすべての場所とデバイスからESET PROTECT On-Premを使用できます。

- ESET Managementエージェント - ESET Managementエージェントは、ESET PROTECTサーバーとクライアントコンピューターの間の通信を容易にします。コンピューターとESET PROTECTサーバーの間の通信を確立するには、エージェントをクライアントコンピューターにインストールする必要があります。そうすれば、クライアントコンピューター上のESET Managementエージェントを使用することになって複数のセキュリティシナリオを保存できるため、新しい検出への対応時間が大幅に短くなりますESET PROTECTWebコンソールを使用するとActive DirectoryまたはESET RD Sensorで特定された管理対象外のコンピューターに、ESET Managementエージェントを展開できます。また、必要に応じて、クライアントコンピューターに、ESET Managementエージェントを手動でインストールできます。

- Rogue Detection Sensor - ESET PROTECT On-Prem Rogue Detection (RD) Sensorは、ネットワークに存在する管理されていないコンピュータを検出し、その情報をESET PROTECTサーバーに送信します。これにより、新しいクライアントコンピュータを保護されたネットワークに容易に追加できますRD Sensorは検出されたコンピュータを記憶し、同じ情報を2回送信しません。

- ESET Bridge - ESET PROTECT On-Premと組み合わせて使用できるサービスで、

  oクライアントコンピュータにアップデートを配布し、ESET Managementエージェントにインストールパッケージを配布します。

  oESET Managementエージェントから ESET PROTECTサーバーに通信を転送します。

- ESET PROTECT仮想アプライアンス - ESET PROTECT On-Prem VAは、仮想環境でESET PROTECT On-Premを実行したいユーザを対象にしています。

- ミラーツール – ミラーツールは、オフラインモジュールアップデートで必要です。クライアントコンピュータがインターネットに接続しない場合、ミラーツールを使用してESETアップデートサーバーからアップデートファイルをダウンロードし、ローカルに保存できます。

- ESET Remote Deployment Tool – このツールではESET PROTECT Webコンソールで作成されたオールインワンパッケージを展開できます。ネットワーク上のコンピュータでESET Managementエージェントとと ESET製品を配布するための便利な方法です。

- ESET Business Account - ESETビジネス製品向けの新しいライセンスポータルでは、ライセンスを管理できますESET Business Accountの使用方法の詳細についてはESET Business Accountユーザーガイドを参照してください。

- ESET Enterprise Inspector – 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 PROTECT Webコンソールを使用してESETソリューションの展開、タスクの管理、セキュリティポリシーの施行、システムステータスの監視、リモートコンピューターでの問題や脅威に対する迅速な対応ができます。

詳細については、ESET PROTECT On-Premオンラインユーザーガイドをご覧ください。

# MDM経由で通知を無効にする

ESET Endpoint Security通知はESET管理コンソールに表示されますESET管理コンソールでESET 製品を管理する場合は、ESET Endpoint Security通知を受信する必要がありません。

MDM経由で通知を無効にできます。

.plistペイロードファイルをダウンロードします。

ほとんどのMDMでは.plistペイロードを添付するか、設定プロファイルのファイル内容をコピーして貼り付けることができます。

## Jamfユーザー

1. Jamfメインウィンドウで、**コンピューター** > **構成プロファイル**をクリックします。

2. **一般**セクションで次の項目を入力します。

| 設定 | 値 |
|---|---|
| 名前 | 例: ESET通知 |
| レベル | コンピューターレベル |
| 配布方法 | 通常、自動的にインストール |

3. **通知**セクションで、**追加**+をクリックし、以下を入力します。

| 設定 | 値 |
|---|---|
| アプリ名 | ESET Endpoint Security |
| バンドルID | com.eset.ees.agent |
| 重大な通知 | 無効 |
| 通知 | 無効 |

# ESET Endpoint Securityを使用する

メインプログラムウィンドウを開くにはmacOSメニューバー(画面の上部)に表示されているESET Endpoint Securityアイコンをクリックし、ESET Endpoint Securityを表示をクリックします。

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


メインメニューでは次のオプションを使用できます。

- 概要
- 検査
- 保護
- アップデート
- ツール
- ヘルプとサポート

ESET Endpoint Securityの詳細設定を変更するには⍰cmd+,を使用して**アプリケーション環境設定**を開くか⍰macOSメニューバーのESET Endpoint Securityをクリックして**環境設定**(設定)を開きます⍰ESET Endpoint Securityが管理対象の場合、ESET PROTECT On-PremまたはESET PROTECTを使用して、ESET Endpoint Security設定を構成できます。

# 概要

メインプログラムウィンドウで概要をクリックすると、コンピューターの現在の保護レベルに関する情報が表示されます。


概要ウィンドウには、前回成功したアップデートの日時を含む、現在のアップデートの状態も表示されます。

ESET Endpoint Securityには、次の保護の状態のいずれかが表示されます。

- **緑のヘッダー**の保護されています状態 – 最大の保護が保証されます
- **オレンジ色のヘッダー**の注意が必要です状態 - ESET Endpoint Securityで重大ではない問題に関する注意が必要です
- 赤のヘッダーの**セキュリティアラート** – 重大な問題が存在し、最大の保護が保証されません

保護の状態が**注意が必要です**または**セキュリティアラート**の場合、保護の状態ウィンドウに追加情報と推奨される解決策が表示されます。

提示された解決策を使用して問題を解決できない場合は、ESETナレッジベースを検索できます。問題が解決されない場合は、ESETテクニカルサポート要求を送信してください。

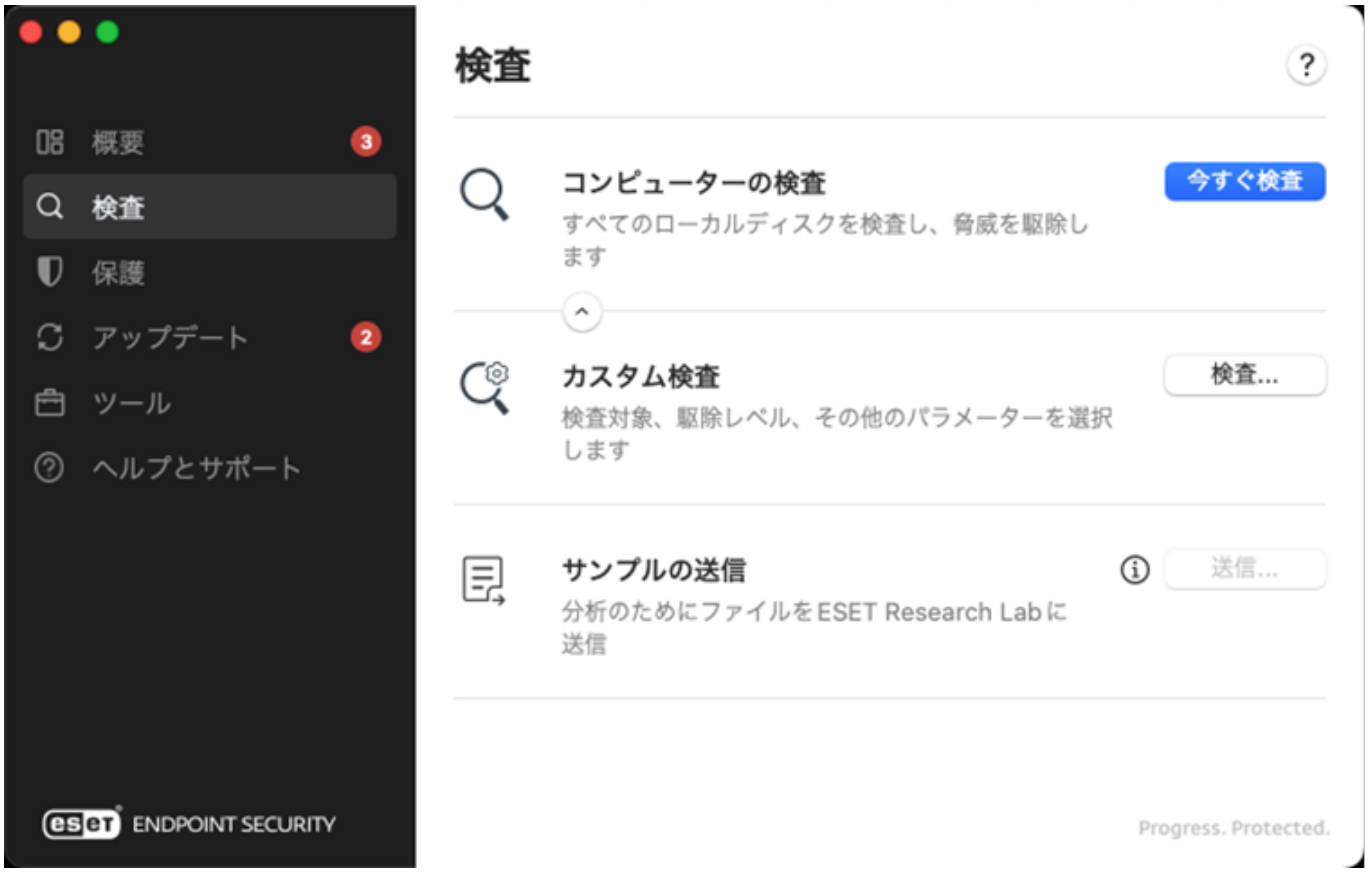
# 検査

メインプログラムウィンドウで**検査**をクリックして、コンピューターでファイルとフォルダの検査を実行します。

オンデマンド検査はウイルス対策ソリューションの重要な部分であり、コンピューター上のファイルやフォルダーの検査を実行するために使用されます。セキュリティの観点からは、感染が疑われるときだけコンピューターの検査を実行するのではなく、通常のセキュリティ手段の一環として定期的に実行することが重要です。

定期的にシステムの詳細検査を実行し、リアルタイムファイルシステム保護では検出されないウイルス

を検出することをお勧めします。これは、リアルタイムファイルシステム保護が特定の時点で無効であった場合、検出エンジンが古い場合、またはファイルがディスクに保存されたときにウイルスとして検出されなかった場合に発生することがあります。




## コンピューターの検査

今すぐ検査をクリックすると、すばやくコンピューターの検査を起動でき、ユーザーの手を煩わせることなく感染したファイルを駆除できます。コンピューターの検査は、操作が簡単で、詳細な検査設定は必要ありません。これにより、ローカルドライブにあるすべ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。

矢印アイコンをクリックすると、**カスタム検査**オプションと**サンプルの送信**オプションが表示されます。

## カスタム検査

検査をクリックすると、カスタム検査ウィンドウが開きます。

**カスタム検査**では、検査対象、検査プロファイル、駆除レベル、除外などの検査パラメーターを指定できます。


カスタム検査対象を追加するには

- ファイルまたはフォルダを手動でドラッグアンドドロップするには、ファイルまたはフォルダをクリックし、マウスボタンを押しながらマウスポインターをマークした箇所に移動して、ボタンを放します
- **参照**をクリックすると、検査するファイルまたはフォルダーを選択できます。

メニューアイコン⋯をクリックすると、詳細検査オプションが表示されます。

**検査プロファイルを選択** – カスタム検査の**検査プロファイル**と駆除レベルを選択します。

ESET PROTECT On-PremまたはESET PROTECTを使用するか、アプリケーション環境設定で、検査プロファイルを編集できます。

**除外の設定** – 検査から除外するファイルまたはフォルダーを追加します。

odscanユーティリティを使用してターミナルからオンデマンド検査を実行するには、ターミナル経由でのオンデマンド検査のトピックを参照してください。

## サンプルの送信

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

**送信**をクリックして、分析用に送信するファイルを指定します。まず、送信の理由を選択してから、ファイルを選択します。ファイルまたはフォルダを手動でドラッグアンドドロップするには、ファイルまたはフォルダをクリックし、マウスボタンを押しながらマウスポインターをマークした箇所に移動して、ボタンを放します。あなたのメールアドレスを含めるオプションがあり、詳細情報が必要な場合にこちらから連絡できます。**匿名で送信する**トグルを有効にしている場合は、メールアドレスを含める必要はありません。

提出するサンプルは、次の基準を1つ以上満たしている必要があります。

- このサンプルがESET製品で検出されない
- サンプルが誤ってウイルスとして検出される

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

> ESETは（マルウェア検査を希望する）個人のファイルをサンプルとして受け入れません。ESET Research Labは、ユーザーのためにオンデマンド検査を実行しません。

# カスタム検査

**カスタム検査**では、検査対象、検査プロファイル、駆除レベル、除外などの検査パラメーターを指定できます。


カスタム検査対象を追加するには

- ファイルまたはフォルダを手動でドラッグアンドドロップするには、ファイルまたはフォルダをクリックし、マウスボタンを押しながらマウスポインターをマークした箇所に移動して、ボタンを放します
- **参照**をクリックすると、検査するファイルまたはフォルダーを選択できます。

メニューアイコン⋯をクリックすると、詳細検査オプションが表示されます。

**検査プロファイルを選択** – カスタム検査の**検査プロファイル**と駆除レベルを選択します。

> ESET PROTECT On-PremまたはESET PROTECTを使用するか、アプリケーション環境設定で、検査プロファイルを編集できます。

**除外の設定** – 検査から除外するファイルまたはフォルダーを追加します。

# 「見つかった脅威」警告が表示された場合の対処方法

ESET Endpoint Securityによる侵入または脅威への対処方法の一般的な例として、既定の駆除レベルを使用してリアルタイムファイルシステム監視によって侵入が検出されたものとします。リアルタイムファイルシステム保護は、ファイルを駆除または削除しようとします。検出された脅威を自動的に駆除できなかった場合、または駆除レベルが**駆除なし**に事前定義されている場合は、警告ウィンドウでオプションを選択するように求められます。**「見つかった脅威」**警告ウィンドウは、オンデマンドのコンピューター検査の結果として表示されることもあります。

## 「見つかった脅威」警告のオプション

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、感染したファイルが感染状態のままになるため、推奨されていません。このオプションは、そのファイルが「無害なのに誤って感染が検出された」と確信できる場合を対象としています。

## ファイルを駆除するとは

ファイルがウイルスの攻撃を受け、悪意のあるコードがファイルに添付された場合に、駆除を行います。この場合、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でのみ構成されている場合には、全体が削除されます。

# サンプルの送信

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

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

**送信**をクリックして、分析用に送信するファイルを指定します。まず、送信の理由を選択してから、ファイルを選択します。ファイルまたはフォルダを手動でドラッグアンドドロップするには、ファイルまたはフォルダをクリックし、マウスボタンを押しながらマウスポインターをマークした箇所に移動して、ボタンを放します。あなたのメールアドレスを含めるオプションがあり、詳細情報が必要な場合にこちらから連絡できます。**匿名で送信する**トグルを有効にしている場合は、メールアドレスを含める必要はありません。

提出するサンプルは、次の基準を1つ以上満たしている必要があります。

- このサンプルがESET製品で検出されない
- サンプルが誤ってウイルスとして検出される

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

> ESETは（マルウェア検査を希望する）個人のファイルをサンプルとして受け入れません。ESET Research Labは、ユーザーのためにオンデマンド検査を実行しません。

# 保護

保護は、ファイル、メール、およびインターネット通信を制御することにより、悪意のあるシステム攻撃から守ります。アプリケーションのメインウィンドウの**保護**オプションを使用して、コンピューター、ネットワークアクセス、Webとメールの保護レベルを調整できます。コンピューター、ネットワークアクセス、Webとメールセクションには、有効または無効にできる保護モジュールが含まれます。すべてのモジュールを有効にして、ESET Endpoint Securityを最大限に活用し、コンピューターを安全に保つことを強くお勧めします。

# コンピューター

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


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

# ネットワークアクセス保護

ネットワークアクセス保護設定には**ファイアウォール**が含まれており、この保護は、個々のネットワーク接続を許可または拒否することで、システムとのすべてのネットワークトラフィックを制御します。

ファイアウォールを有効または無効にすることができ、設定はESET PROTECT On-PremまたはESET PROTECT経由でリモートで管理されているエンドポイントでのみ使用できます。ESET PROTECTで設定されていないファイアウォールは、既定の設定で製品の定義済みルールセットを使用します。

# Webとメール

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

- **Web保護** - Webブラウザーとリモートサーバー間のHTTP通信を監視します。
- **フィッシング対策保護** - 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。
- **電子メール保護** - 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。

# アップデート

メインプログラムウィンドウのアップデートをクリックすると、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表示できます。

コンピューターの最大レベルのセキュリティを確保するためにはESET Endpoint Securityを定期的にアップデートするのが最善の方法です。自動アップデートは、プログラムモジュールおよびシステムのコンポーネントが常に必ず最新情報であることを保証します。自動アップデートのほかに、アップデートの確認をクリックすると、手動アップデートをトリガーできます。製品のアップデートが利用可能な場合は、現在のバージョンと利用可能なバージョンに関する情報が、アップデートサイズとリリース日とともに表示されます。製品のアップデートを続行するには、**エンドユーザーライセンス契約**に同意し、**プライバシーポリシー**に同意する必要があります。**同意して今すぐアップデート**または**同意して、再起動後にアップデート**を選べます。各製品バージョンの詳細を表示するには、**変更ログを参照してください**リンクをクリックします。

前回の成功したアップデート – 最終成功更新日です。最近の日付が表示されない場合、製品モジュールは最新でない可能性があります。

アップデートの前回確認 – 成功アップデートを確認した最終日を記載します。

ESET Endpoint Securityの詳細**アップデート**設定を変更するにはcmd+,を使用して**アプリケーション環境設定**を開くかmacOSメニューバーのESET Endpoint Securityをクリックして**環境設定**(設定)を開きますESET Endpoint Securityが管理対象の場合は、ESET PROTECT On-PremまたはESET PROTECTを使用してリモートで詳細アップデート設定を構成できます。

updユーティリティを使用してターミナルから検出モジュールをアップデートするには、ターミナル経由の検出モジュールのアップデートのトピックを参照してください。

# ツール

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

-

ログファイル

隔離

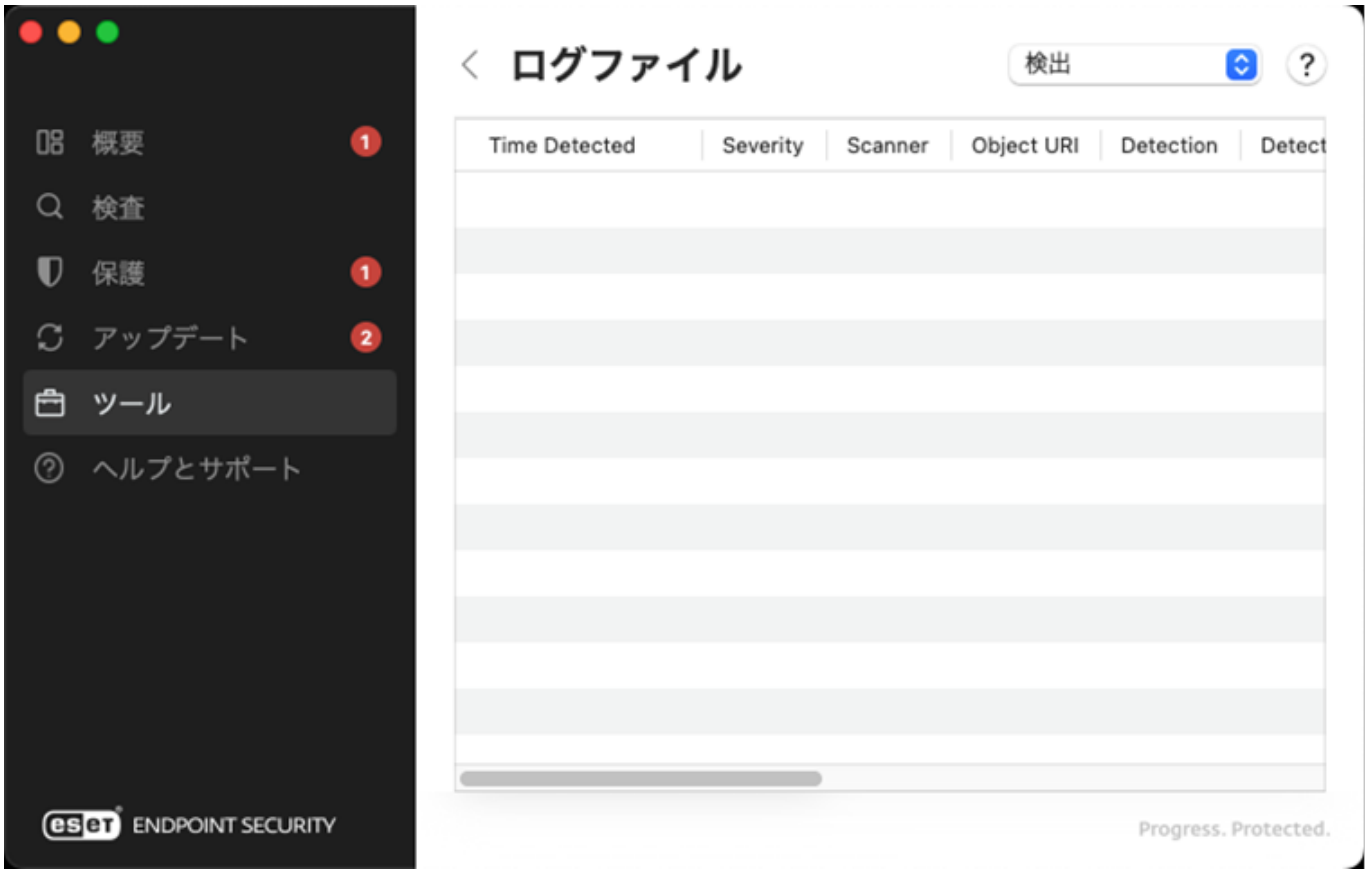
# ログファイル

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

ESET Endpoint Security環境から直接、テキストメッセージとログを表示し、ログをアーカイブできます。

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

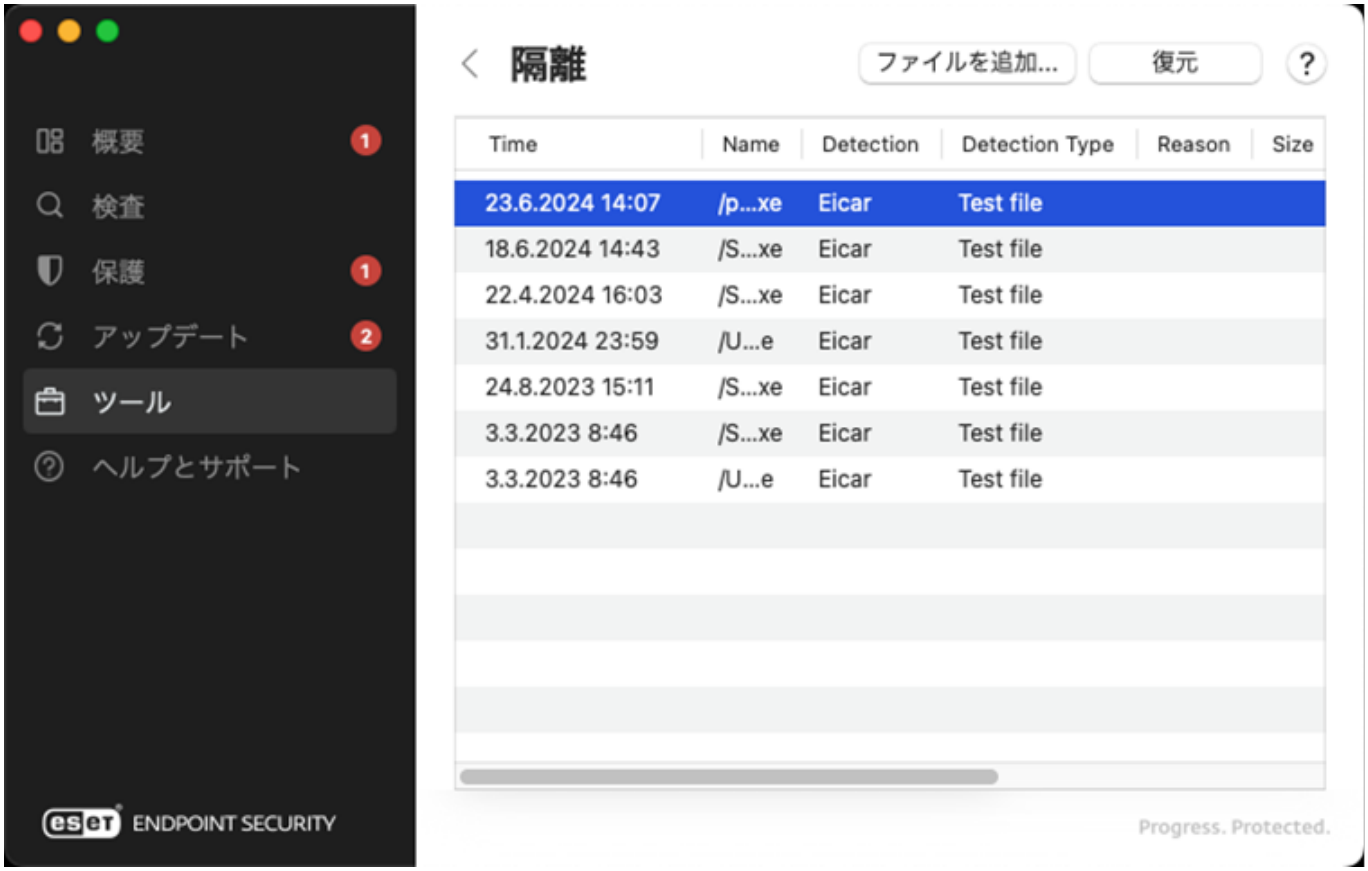
- **検出** – 侵入の検出に関するイベントの情報がすべて表示されます
- **コンピューターの検査** – 完了した全ての検査結果が表示されます。エントリーをダブルクリックすると、各オンデマンドコンピューター検査の詳細が表示されます
- **イベント** – システム管理者およびユーザーが問題を解決するために使用します。イベントログにはESET Endpoint Securityによって実行されたすべての重要なアクションが記録されます
- **ブロックされたファイル** - ESET Inspectによって設定されたブロックされたファイル(ブロックされたハッシュ)のリストに基づいて、検査中にブロックされたファイルのレコードが含まれます。
- **フィルタリングされたWebサイト** – Webアクセス保護によってブロックされたWebサイトの一覧が表示されます。これらのログでは、特定のWebサイトへの接続を開いた時間URLステータスIPアドレス、ユーザー、およびアプリケーションを確認できます。
- **送信されたファイル** – 分析に送信されたサンプルのレコードが含まれます。




# 隔離

隔離は、感染ファイルを安全に保存します。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で誤って検出された場合、ファイルを隔離する必要があります。

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




## ファイルを隔離

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

## 隔離からの復元

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

## 隔離フォルダからのファイルの提出

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

# ヘルプとサポート

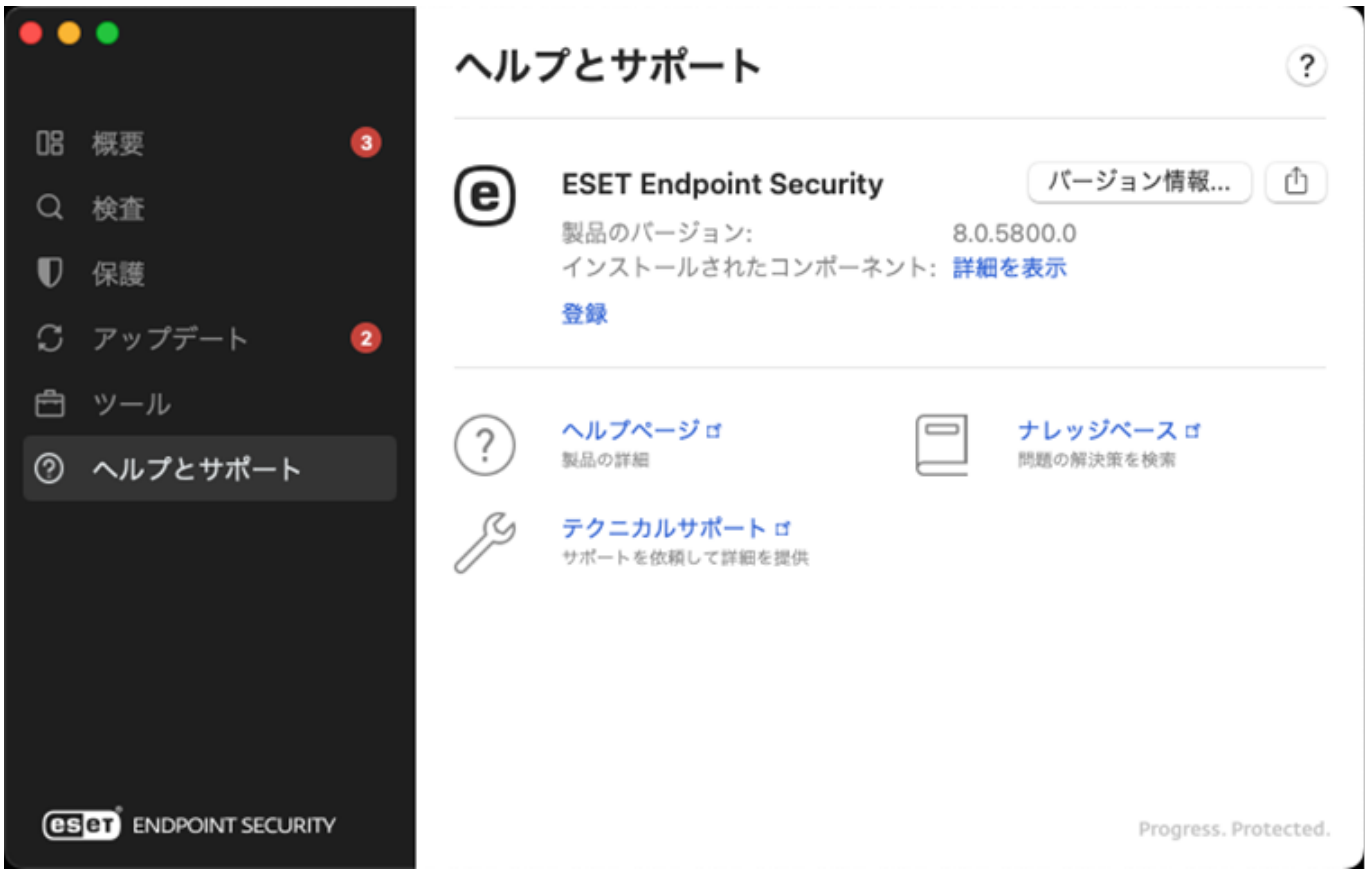
ESET Endpoint Securityには、トラブルシューティングツール、および発生する可能性のある問題の解決に役立つサポート情報が含まれます。ヘルプとサポートセクションは、メインアプリケーションウィンドウで確認できます。インストールされたコンポーネントの一覧を表示するには、**インストールされたコンポーネント**の横の**詳細を表示**をクリックします。一覧をクリップボードにコピーするには、[インストールされたコンポーネント]ウィンドウの任意の場所を右クリックし、**すべてコピー**をクリックします。この機能は、トラブルシューティングを行う場合、またはテクニカルサポートに問い合わせる場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

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

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

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

**ナレッジベース** - ESETナレッジベースにアクセスして、よくある質問への回答や、さまざまな問題の推奨解決策をご覧ください。ESETのテクニカルスペシャリストが定期的に更新しているので、このナレッジベースは、さまざまな問題を解決するための最も強力なツールです。




# ターミナルユーティリティとデーモン

## コマンドラインユーティリティ

- ./ lslog – ログリストユーティリティは、ESET Endpoint Securityによって生成されたログを表示します。
- ./ odscan – ターミナルウィンドウからオンデマンド検査を実行するために使用できるオンデマンドスキャナー。
- ./ cfg - ESET Endpoint Security設定をインポートおよびエクスポートするために使用できる構成ユーティリティ。
- ./ mdm-info - MDM経由でプリインストール設定を完了するために必要な設定プロファイルの作成で必要な情報を表示するMDM情報ユーティリティ。
- ./ lic – ライセンスユーティリティ。購入した製品認証キーでESET Endpoint Securityをアクティベーションするか、アクティベーションステータスとライセンスの有効期間を確認するために使用します。
- ./ upd – モジュールのアップデートユーティリティ。モジュールアップデートの管理またはアップデート設定の修正に使用します。
- ./ quar – 隔離管理ユーティリティ。隔離された項目を管理するために使用します。

# 隔離

隔離は、感染ファイルを安全に保存します。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、ウイルス対策スキャナーによって検出されない場合にお勧めします。分析のために隔離したファイルをESET Virus Labに送信することができます。

## ターミナルを使用した隔離された項目の管理

構文: /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/quar [OPTIONS]

| オプション – 短い形式 | オプション – 長い形式 | 説明 |
|---|---|---|
| -i | --import | ファイルを隔離フォルダーにインポートする |
| -l | --list | 隔離のファイルのリストを表示する |
| -r | --restore=id | IDで指定された隔離された項目を--restore-pathで定義されたパスに復元する |
| -e | --restore-exclude=id | IDで指定され、除外可能列で「x」が設定されている隔離された項目を復元する |
| -d | --delete=id | IDで指定された隔離された項目を削除する |
| | --restore-path=path | 隔離された項目を復元する新しいパス |
| -h | --help | ヘルプの表示 |
| -v | --version | バージョン情報の表示と終了を実行します |

復元
コマンドが特権ユーザーとして実行されない場合は、復元を使用できません。

## 例

ID 0123456789の隔離された項目を削除:

```
/Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/quar -d 0123456789
```

または

```
/Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/quar --
delete=0123456789
```

IDが「9876543210 Downloadの隔離された項目をログインユーザーのフォルダーに復元し、名前をrestoredFile.testに変更する:

```
/Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/quar -r 9876543210 --
restore-path=/Users/$USER/Desktop/restoredFile.test
```

または

```
/Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/quar --
restore=9876543210 --restore-path=/Users/$USER/Desktop/restoredFile.test
```

ID 9876543210 **除外可能**列**x**の隔離された項目をDownloadフォルダーに復元する:

```
/Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/quar -e 9876543210 --
restore-path=/Users/$USER/Downloads/restoredFile.test
```

または

```
/Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/quar --restore-
exclude=9876543210 --restore-path=/Users/$USER/Downloads/restoredFile.test
```

## ターミナルを使用して隔離フォルダーからファイルを復元する

1. 隔離された項目を一覧表示します。
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar -l

2. 復元する隔離済みオブジェクトのIDと名前を検索し、次のコマンドを実行します。
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar --restore=ID_OF_OBJECT_TO_RESTORE --restore-

# 設定

```
/Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/cfg --export-xml=/tmp/export.xml
```

### 設定のインポート

```
/Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/cfg --import-xml=/tmp/export.xml
```

### 使用可能なオプション

| 短い形式 | 長い形式 | 説明 |
|---|---|---|
| | --import-xml | 設定のインポート |
| | --export-xml | 設定のエクスポート |
| -h | --help | ヘルプの表示 |
| -v | --version | バージョン情報の表示 |

# イベント

ESET Endpoint SecurityのWebインターフェイスで実行される重要なアクション（Webインターフェースへのログインの失敗、ターミナルから実行されるESET Endpoint Securityに関連するコマンド、および一部のその他の情報は**イベント**画面に出力されます。

各記録されるアクションには、イベントが発生した時刻、コンポーネント(ある場合)、イベント、ユーザーがあります。

## ターミナルからイベントを表示する

ターミナルウィンドウから**イベント**画面の内容を表示するには（lslogコマンドラインツールを使用します。

構文: /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/lslog [OPTIONS]

| オプション – 短い形式 | オプション – 長い形式 | 説明 |
|---|---|---|
| -f | --follow | 新しいログを待って出力の最後に追加します。 |
| -o | --optimize | ログを最適化します。 |
| -c | --csv | CSV形式でログを表示します。 |
| -e | --events | イベントログを一覧表示します。 |
| -u | --urls | URLログレコードを一覧表示します。 |
| -n | --sent-files | 分析のために送信されたファイルのリストを表示します。 |
| -s | --scans | コンピューター検査ログを一覧表示します。 |
| | --with-log-name | ログ名列も表示します。 |
| | --ods-details=log-name | ログ名で指定されたオンデマンド検査の詳細を表示します。 |

| オプション – 短い形式 | オプション – 長い形式 | 説明 |
|---|---|---|
| | --ods-events=log-name | ログ名で指定された特定のオンデマンド検査中に検査されていない、見つかった検出とファイルを印刷します。 |
| | --ods-detections=log-name | ログ名で指定されたオンデマンド検査の検出を表示します。 |
| | --ods-notscanned=log-name | ログ名で指定されたオンデマンド検査の検査されていない項目を表示します。 |
| -d | --detections | 検出ログレコードを一覧表示します。 |
| -b | --blocked-files | ブロックされたファイルログを一覧表示します。 |
| -t | --network | ネットワークアクセス保護のログレコードを一覧表示します。 |
| | --va-scans | 脆弱性評価の検査ログを一覧表示します |

## 例

すべてのイベントログを表示する

```
/Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/lslog -e
```

すべてのイベントログをCSV形式で、現在のユーザーのドキュメントディレクトリのファイルに保存します。

```
/Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/lslog -
ec > /Users/$USER/Desktop/eventlogs.csv
```

# ターミナル経由の検出モジュールのアップデート

## ターミナル経由のモジュールのアップデート

ターミナルウィンドウからすべての製品モジュールをアップデートするには、次のコマンドを実行します。

```
/Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/upd -u
```

## ターミナル経由のアップデートとロールバック

| オプション – 短い形式 | オプション – 長い形式 | 説明 |
|---|---|---|
| -u | --update | Module aktualisieren |
| -c | --cancel | モジュールのダウンロードをキャンセルする |
| -e | --resume | アップデートのブロックを解除する |
| -r | --rollback=VALUE | スキャナモジュールを最も古いスナップショットにロールバックし、値に設定した時間すべてのアップデートをブロックします。 |
| -l | --list-modules | 製品モジュールのリストを表示 |

| オプション – 短い形式 | オプション – 長い形式 | 説明 |
|---|---|---|
| | --check-app-update | リポジトリの新しい製品バージョンの利用可能状況を確認する |
| | --perform-app-update | 利用可能な場合は新しい製品バージョンをダウンロードしてインストールする |
| | --accept-license | ライセンスの変更を許可 |

**updの制限**
updユーティリティを使用して、製品構成を変更することはできません。

アップデートを48時間停止し、スキャナーモジュールの最も古いスナップショットにロールバックするには、特権ユーザーで次のコマンドを実行します。
```
sudo /opt/eset/efs/bin/upd --rollback=48
/Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/upd --rollback=48
```
スキャナーモジュールの自動アップデートを再開するには、特権ユーザーとして次のコマンドを実行します。
```
sudo /opt/eset/efs/bin/upd --resume
/Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/upd --rollback=48
```
IPアドレス「192.168.1.2」とポート「2221」で使用可能なミラーサーバーからアップデートするには、特権ユーザーで次のコマンドを実行します。
```
sudo /opt/eset/efs/bin/upd --update --server=192.168.1.2:2221
/Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/upd --rollback=48
```

# ターミナル経由のオンデマンド検査

構文: /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/odscan [OPTIONS..]

| オプション – 短い形式 | オプション – 長い形式 | 説明 |
|---|---|---|
| -l | --list | 現在実行中の検査を表示する |
| | --list-profiles | すべての使用可能な検査プロファイルを表示 |
| | --all | 他のユーザーが実行した検査も表示(ルート権限が必要) |
| -r | --resume=session_id | session_idで指定された一時停止中の検査を再開 |
| -p | --pause=session_id | session_idで指定された検査を一時停止 |
| -t | --stop=session_id | session_idで指定された検査を停止 |
| -s | --scan | 検査の開始 |
| | --show-scan-info | 開始した検査に関する基本情報(log_nameを含む)を表示 |
| | --profile=PROFILE | 選択されたプロファイル名で検査 |
| | --profile-priority=優先度 | タスクは、指定された優先度で実行されます。<br>優先度は、normal□lower□lowest□idleです。 |
| | --readonly | 駆除せずに検査する |
| | --local | ローカルドライブの検査 |
| | --network | ネットワークドライブの検査 |
| | --removable | リムーバブルメディアの検査 |
| | --exclude=FILE | 選択されたファイルまたはディレクトリーをスキップする |
| | --ignore-exclusions | 除外されたパスと拡張子も検査 |

| オプション – 短い形式 | オプション – 長い形式 | 説明 |
|---|---|---|
| | --boot-local | ローカルドライブのブートセクター |
| | --boot-removable | リムーバブルメディアのブートセクター |
| | --boot-main | メインブートセクター |

odscanユーティリティは検査の完了後、終了コードで終了します。検査が完了した後に、ターミナルウィンドウで`echo $?`を実行すると、終了コードが表示されます。

**終了コード**

| 終了コード | 意味 |
|---|---|
| 0 | マルウェアは検出されませんでした |
| 1 | マルウェアが検出され、駆除されました |
| 10 | 一部のファイルはスキャンできません(マルウェアの可能性あり) |
| 50 | 脅威が検出されました |
| 100 | エラー |

# 例

バックグラウンドプロセスとして@Smart scan検査プロファイルを使用して、再帰的に*/root/*ディレクトリのオンデマンド検査を実行します。

```
  /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/odscan --scan --
profile="@Smart scan" / &
```

複数の宛先に関して@Smart scan検査プロファイルを使用して、再帰的にオンデマンド検査を実行します。

```
  /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/odscan --scan --
profile="@Smart scan" /Application/ /tmp/ /home/
```

すべての実行中の検査のリストを表示する

```
  /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/odscan -l
```

session-id "15"の検査を一時停止します。検査を開始すると、各検査の一意のsession-idが生成されます。

```
  /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/odscan -p 15
```

session-id "15"の検査を停止します。検査を開始すると、各検査の一意のsession-idが生成されます。

```
  /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/odscan -t 15
```

ディレクトリ/exc_dirと除外されたファイル/eicar.comを使用して、オンデマンド検査を実行します。

```
  /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/odscan --scan --
profile="@In-depth scan" --exclude=/exc_dir/ --exclude=/eicar.com /
```

リムーバブルデバイスのブートセクターを検査します。以下のコマンドを特権ユーザーとして実行します。

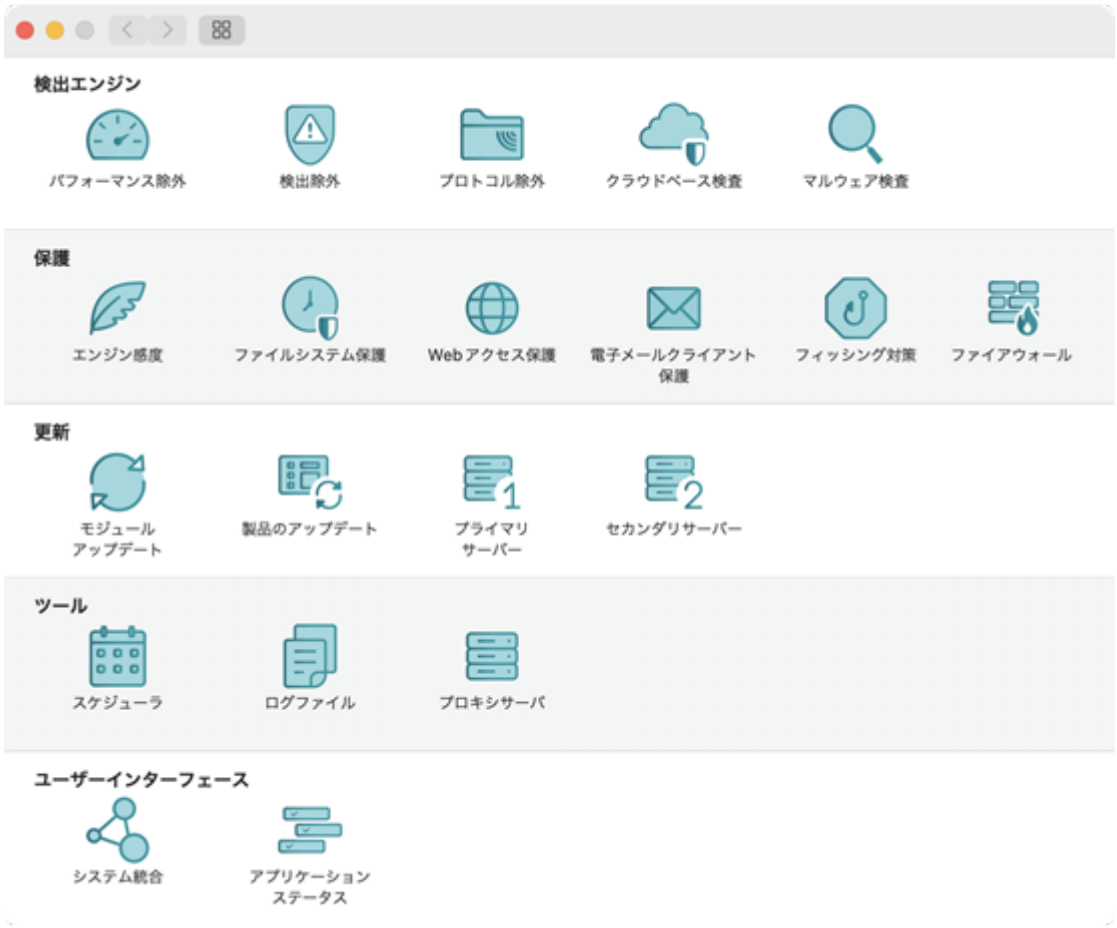
```
  sudo /Applications/ESET\ Endpoint\ Security.app/Contents/MacOS/odscan --scan --
profile="@In-depth scan" --boot-removable
```

# アプリケーション環境設定

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

次のカテゴリのモジュール設定を構成できます。

- 検出エンジン
- 保護
- 更新
- ツール
- ユーザーインターフェース




# 検出エンジン

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

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

# パフォーマンス除外

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

- **+** – 新しい例外を作成します。ドラッグアンドドロップを使用して新しい除外を追加するか、オブジェクトまたはフォルダーへのパスを入力します(例: `/Users/username/Downloads`)
- **−** – 選択したエントリーを除去します。

⚠ リアルタイムファイルシステム保護で重大な問題が発生した場合にのみ、ファイルを検査から除外してください。これは、検査からファイルを除外することで全体的な保護が低下するためです。一部の電子メールサーバー、バックアップソフトウェアなどのファイルレベルの検査が異常なシステム動作を引き起こしている場合は、パフォーマンス除外リストにファイルを追加すると、解決につながる可能性があります。

# 検出除外

検出除外では、検出名、オブジェクトパス、またはハッシュをフィルタリングして、オブジェクトを駆除から除外できます。ドラッグアンドドロップを使用して新しい検出除外を追加するには、ファイルまたはフォルダーをクリックし、マウスボタンを押しながらマウスポインターをマークした箇所に移動して、ボタンを放します。

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

次のタイプの駆除基準があります。

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

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

# プロトコル除外

除外リストのエントリは製品コンテンツフィルタリングから除外されます。選択した**IPアドレス**との通信、または選択した**アプリケーション**による通信は、プロトコルフィルタリング(HTTP、POP3、IMAP)によって検査されません。このオプションは信頼できるとわかっているアドレスまたはアプリケーションに対してのみ使用することをお勧めします。

- [+] – 新しい例外を作成します。ドラッグアンドドロップを使用して新しい除外を追加するか、オブジェクトまたはフォルダーへのパスを入力します(例: `/System/Applications/Calculator.app`)
- [−] – 選択したエントリーを除去します。

# ネットワークプロファイル

ネットワークプロファイルを使用すると、ファイアウォールで認識されるネットワークの信頼レベルを設定できます。安全で信頼できることがわかっているネットワークに、信頼済みステータスを割り当てることをお勧めします。コンピューターが新しいネットワークに接続すると、ダイアログウィンドウが表示されます。このウィンドウで、ネットワークの種類を**プライベート**または**パブリック**に設定できます。ダイアログウィンドウを無視する場合は、ネットワークをパブリックとしてマークする方が安全です。

ネットワーク接続プロファイルを設定し、ネットワーク接続の特定のカテゴリにファイアウォールルールを適用するには、ネットワークアクセス保護のトピックに従ってください。ネットワーク接続プロファイルの設定は、リモートで管理されているエンドポイントでのみ使用できます。

## ネットワークタイプ

### プライベート

プライベートネットワークは信頼できると見なされます。信頼できる(プライベート)ネットワークからの受信接続は、特別なファイアウォールルールによって許可される場合があります。

### パブリックまたはゲスト

パブリックネットワークとは、あなたがゲストとして参加している、信頼できない可能性があるネットワークのことです。こうした種類のネットワークには、さらに厳しいファイアウォールルールが適用されます。

ネットワークプロファイルにネットワークを追加できるのはESET Endpoint Securityファイアウォールによって検出されたネットワークに最初に接続したときだけです。ネットワークプロファイルに既に保存されているネットワークに接続した場合、ネットワークオプションを含むダイアログウィンドウは表示されません。また、このダイアログウィンドウは、ESET Endpoint Securityのリモート管理バージョンを使用している場合には表示されません。

# クラウドベース検査

## ESET LiveGrid®に参加する(推奨)

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

## ESET LiveGrid®フィードバックシステムを有効にする

詳細分析のため、データはESET Virus Labに送信されます。

## サンプルの送信

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

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

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

- 実行可能ファイル – ファイルのタイプ: .exe□.dll□.sys
- アーカイブ – ファイルのタイプ: .zip□□.rar□□.7z□□.arch□□.arj□□.bzip2□□.gzip□□.ace□□.arc□□.cab□

- スクリプト – ファイルのタイプ: .bat、.cmd、.hta、.js、.vbs、.ps1
- ドキュメント – アクティブなコンテンツを含むMicrosoft Office、Libre Office、または他のオフィスツールで作成されたドキュメントやPDFが含まれます。
- その他 – ファイルのタイプ: .jar、.reg、.msi、.swf、.lnk

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

### クラッシュレポートと診断データを送信

クラッシュレポート、モジュールメモリダンプなどのデータを送信します。

### 匿名の使用状況統計情報を送信し、製品の改善を支援する

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

### 連絡先の電子メールアドレス(任意)

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

## マルウェア検査

オンデマンドスキャナーはコンピューター上のファイルやフォルダの検査を実行するため、ウイルス対策の重要な部分です。セキュリティの観点から、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。**マルウェア検査**セクションでは、オンデマンド検査プロファイルのオプションを設定できます。

**プロファイルの一覧** –新しいプロファイルの一覧を作成するか、既存のプロファイル一覧を削除するには、+または−を選択します。新しいプロファイルの一覧を追加するときに、プロファイルの名前を入力し、**OK**をクリックします。新しいプロファイルは、既存の検査プロファイルが一覧表示される選択したプロファイルドロップダウンメニューに表示されます。

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

## 保護

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

## エンジン感度

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

• **マルウェア** – コンピューターの既存のファイルに含まれる悪意のあるコード。

• **望ましくない可能性のあるアプリケーション** – グレイウェアまたは望ましくない可能性があるアプリケーション(PUA)は、ウイルスまたはトロイの木馬などの他のマルウェアタイプ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。これらのアプリケーションの詳細については、用語集を参照してください。

• **不審なアプリケーション** – パッカーまたはプロテクターを使用して圧縮されたプログラムなどが挙げられます。このようなプロテクターは、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。

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

# ファイルシステム保護

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

## 検査するメディア

Real-timeスキャナーから次のメディアを除外できます。

• **ローカルドライブ** – システムハードドライブ

• **リムーバブルメディア** (USBメディアBluetoothデバイスなど)

• **ネットワークメディア** – すべてのマッピングされたドライブ

## 検査のタイミング

既定では、**ファイルを開いてファイルを作成**している間に、すべてのファイルが検査されます。既定の設定では最大限のリアルタイムファイルシステム保護が確保されているので、既定の設定を変更しないことをお勧めします。

## プロセスの除外

また、特定のプロセスを検査から除外できます。特定のプロセスを除外するには、プロセスバイナリへの完全パスを指定する必要があります。アプリケーションバンドルを使用するだけでは不十分です。ワイルドカードはサポートされていません。たとえばSafariを除外するには、プロセスパスとして「`/Applications/Safari.app/Contents/MacOS/Safari`」を使用してプロセス除外を作成します。

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

### ThreatSense パラメータ

これらは検出エンジンの詳細設定であり、経験豊富なユーザーのみが変更するようにしてください。最適な保護とパフォーマンスを得るために、既定値を変更しないでください。

# Webアクセス保護

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

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

### Webプロトコル

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

### URLアドレス管理

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

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

特殊記号の*（アスタリスク）および?（疑問符）を使用できます。アスタリスクは0文字以上の任意の文字列を、疑問符は任意の1文字をそれぞれ表します。除外するアドレスを指定する際は、注意する必要があります。この一覧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、記号*および?を正しく使用する必要があります。

# 電子メールクライアント保護

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

### 電子メールプロトコル

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

#### POP3プロトコルのチェック

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

ロトコルを保護します。

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□POP3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□POP3プロトコル制御は、電子メールクライアントを再構成せずに、自動的に実行されます。既定では、ポート110にある全ての通信が検査されますが、他の通信ポートは必要に応じて追加できます。ポート番号はコンマで区切ります。

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

### IMAPプロトコルのチェック

IMAP(インターネットメッセージアクセスプロトコル)はメール受信のためのもう1つのインターネットプロトコルで、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します。

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。ポート番号はカンマで区切る必要があります。

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

## 電子メールタグ

電子メールタグを使用すると、電子メールのフットノートにタグメッセージを追加できます。電子メールが検査された後、検査結果を示す通知を追加できます。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判断するために使用しないでください。問題のあるHTMLメッセージではタグメッセージが省略され、特定の脅威によって偽装される可能性があります。使用可能なオプションは次のとおりです。

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

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

**検出された電子メールの件名に追加** – 感染メールの件名のプレフィックス形式を変更する場合はこのテンプレートを編集します。

### ThreatSense パラメータ

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

# フィッシング対策機能

フィッシング対策保護は、もう1つの保護レイヤーであり、パスワードやその他の機密情報を取得しようと試みる非合法なWebサイトに対する防御を強化します。フィッシング対策機能は既定で有効になっています。これは有効にしておくことをお勧めします。

# ファイアウォール

ファイアウォールは、システムとの間のすべてのネットワークトラフィックを制御します。これは、指定されたフィルタリングルールに基づいて個々のネットワーク接続を許可または拒否することによって実現されます。リモートコンピューターからの攻撃に対して保護を提供し、一部のサービスをブロックできるようにします。

ファイアウォール設定は、ESET PROTECT On-PremまたはESET PROTECTを使用してリモートで管理されているエンドポイントに対してのみ使用可能です。

# アップデート

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

# モジュールと製品のアップデート

## モジュールのアップデート

### アップデートの種類

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

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

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

### モジュールロールバック

新しい検出エンジンアップデートやプログラムモジュールのアップデートが不安定であったり破損して

いる疑いがある場合、前のバージョンにロールバックし、一時的にアップデートを無効にできます。

### モジュールのスナップショットを作成

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

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

## 製品のアップデート

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

## プライマリサーバーとセカンダリサーバー

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

# ツール

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

# スケジューラ

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

# ログファイル

## ログの詳細レベル

ログの詳細レベルは、ログファイルに含まれる詳細レベルを定義します。

- **重大な警告** – 重大なエラー(**ウイルス対策保護の起動に失敗した**など)のみが含まれます
- **エラー** – 重大な警告に加えて、**ファイルのダウンロードエラー**などのエラーを記録します
- **警告** – 重大なエラー、エラー、および警告メッセージを記録します。
- **情報レコード** – アップデートの成功メッセージを含むすべての情報メッセージと上記のすべて

のレコードを記録します。

• **診断レコード** – プログラムおよび上記のすべてのレコードを微調整するのに必要な情報が記録されます。

### ログファイルのクリーニング

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

### ログファイルの最適化

**ログファイルを自動的に最適化する** – チェックすると、**使用されていないエントリの割合(%)が次の値よりも大きくなったら最適化**フィールドで指定した断片化の割合を超えると、ログファイルは自動的に最適化されます。すべての空のログエントリが削除され、パフォーマンスとログ処理速度が改善します。ログに多数のエントリが含まれている場合に、この改善が見られます。

## プロキシサーバーの設定

プロキシサーバー設定を指定できます。定義されたパラメータは、インターネット接続を必要とするすべてのモジュールで使用されます。

プロキシサーバーを設定するには

1.**プロキシサーバーを使用**を有効にし、プロキシサーバーのアドレスを**プロキシサーバーアドレス**フィールドに入力し、さらにプロキシサーバーの**ポート**番号を入力します。

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

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

## ユーザーインターフェース

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

## システム統合

**ユーザーインターフェース要素**

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

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

## 通知

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

# アプリケーションステータス

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

# アンインストール

## ローカルアンインストール

ESET Endpoint Securityアイコンをアプリケーションフォルダーからごみ箱にドラッグしてもESET EndpointSecurityを完全にアンインストールすることはできません。システム拡張はコンピューターにインストールされたままでUninstaller.appは後から削除できません。
ユーザーがESET Endpoint Securityをアンインストールできないように、修正不可フラグをESET Endpoint Securityに追加することをお勧めします。修正不可フラグを追加するには、ターゲットコンピューターで次のコマンドを実行します。

```
sudo chflags -Rf schg /Applications/ESET\ Endpoint\ Security\.app
```

ESET Endpoint Securityをアンインストールする前に、修正不可フラグを削除する必要があります。修正フラグを削除するには、ターゲットコンピューターで次のコマンドを実行します。

```
sudo chflags -Rf noschg /Applications/ESET\ Endpoint\ Security\.app
```

ESET Endpoint Securityをアンインストールするには

ESET PROTECT On-PremまたはESET PROTECTを使用してESET Endpoint Securityを管理している場合は、クライアントタスクを作成および実行し、リモートでESET Endpoint Securityをアンインストールできます。

- ESET PROTECT On-Premでソフトウェアアンインストールタスクを作成して実行します。
- ESET PROTECTでソフトウェアアンインストールタスクを作成して実行します。

1. ESET Endpoint Securityアンインストーラーを起動しますESET Endpoint Securityアンインストーラーを実行するには複数の方法があります。

   - ESET Endpoint Security インストールファイル((.dmg))を開き、Uninstallerをダブルクリックします。

   - Finderを起動し、ハードドライブのアプリケーションフォルダを開き、**ESET Endpoint Security**アイコンをControlキーを押しながらクリック(右クリック) > ショートカットメニューから**パッケージの内容を表示**を選択します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。

2. **アンインストール**をクリックすると、アンインストール処理が開始します。管理者パスワードを入力する必要があります。

システム拡張機能の削除の問題がある場合は、アンインストール処理中に管理者パスワードを入力する必要がある場合があります。

3. macOS 12 MontereyでESET Endpoint Securityをアンインストールしている場合は、Uninstaller.appがESET Endpoint Securityによって作成されたユーザーを管理することを許可するように指示されます。次のダイアログが表示されます。
“Uninstaller.app”がコンピュータを管理することを要求しています。管理にはパスワード、ネットワーク、およびシステム設定の変更が含まれます。
OKをクリックします。許可しないをクリックするとESET Endpoint Securityが完全にアンインストールされません。

4. 閉じるをクリックすると、アンインストーラーを終了します。

5. コンピューターを再起動します。

---

## コマンドライン経由でのアンインストール

アンインストールスクリプトを実行して、**ターミナル**からESET Endpoint Securityをアンインストールできます。既定の場所にESET Endpoint Securityをインストールした場合は、次のコマンドを実行します。

```
sudo /Applications/ESET\ Endpoint\
Antivirus.app/Contents/Helpers/Uninstaller.app/Contents/Scripts/uninstall.sh
```

# テクニカルサポート

## テクニカルサポートに問い合わせる

問題の回答が見つからない場合はESETのWebサイトにあるこのフォームを使用してESETテクニカルサポート部門に簡単に問い合わせることができます。

## テクニカルサポート情報

問題を迅速かつ正常に解決するために、サポートチケットを作成するときには、次の手順を実行することをお勧めします。

- ライセンス詳細、製品名、製品バージョン、オペレーティングシステムなどの情報を含める。
- 問題を詳細に説明する。
- 問題のスクリーンショットまたは動画を添付する。
- ESET LogCollectorのログを添付する。

### ESET LogCollector

ESET LogColletorは、ESET Endpoint Securityの使用で発生した問題をサポートと開発者が特定するうえで役に立つ重要な情報が記録されたログを作成します。

詳細については、ESETナレッジベースのESET LogCollectorを参照してください。言語によっては、記事が提供されていない場合があります。

ESET LogCollectorでログを作成する

1. ダウンロードESET LogCollector

2. eset_logcollector.dmgファイルを開き、LogCollectorアプリを実行します。

3. 画面の手順に従い、ログを作成します。

> **ESET LogCollectorの使用上のヒント**
> • ESETサポート用の詳細ログを作成するには、**レプリケーション**セクションで、歯車アイコンをクリックして、詳細オプションを開きます。
> • 問題と手順を再現する準備をする前に、レプリケーションを開始しないでください。

ログファイルが作成された後、デスクトップにcustomer_info.zipというログファイルが作成されます。このファイルをサポート依頼に添付します。

# エンドユーザーライセンス契約

発効日：2021年10月19日

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

エンドユーザー使用許諾契約

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

本契約は購入に関する契約ではなく、エンドユーザーの権利に関する合意事項を定めるものです。供給者は、本ソフトウェアのコピー、これが商業包装にて供給される物理的媒体、および本契約に基づきエンドユーザーが権利を付与される本ソフトウェアのすべてのコピーの、所有者であり続けます。

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

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

1.**ソフトウェア。**(i)本契約およびすべてのコンポーネントに付属するコンピュータープログラム(ii)データ媒体、電子メール、またはインターネット経由でのダウンロードで提供される本ソフトウェアのオブジェクトコードの形式を含む、本契約で提供されるディスクCD-ROMDVD電子メール、添付ファイル、その他の媒体のすべての内容(iii)本ソフトウェアに関連する書面の説明資料、その他の文書、特に本ソ

フトウェア、その仕様のすべての説明、 本ソフトウェアの属性または動作の説明、本ソフトウェアが使用される動作環境の説明、本ソフトウェアの使用またはインストール手順、本ソフトウェアの使用方法の説明(「ドキュメント」)(iv)本契約の第3条に従い供給者からお客様にライセンス供与された本ソフトウェアのコピー、本ソフトウェアに不具合があった場合のパッチ、本ソフトウェアへの追加機能、本ソフトウェアの拡張機能、本ソフトウェアの修正バージョン、ソフトウェアコンポーネントのアップデート(該当する場合)を意味します。本ソフトウェアは実行可能なオブジェクトコードの形態でのみ提供されるものとします。

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

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

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

b) **ライセンス数の規定。**本ソフトウェアを使用する権利は、エンドユーザー数によって制限されます。1人のエンドユーザーとは(i) 本ソフトウェアがインストールされている1台のコンピューターを意味します(ii)ライセンス数がメールボックスを単位として決定される場合、エンドユーザーはメールユーザーエージェント（以下「MUA」とします）を介して電子メールを受信する1人のコンピューターユーザーを意味します。電子メールがMUAで受信後、複数のユーザーに自動的に配信される場合、エンドユーザーの数は、その電子メールが配信されるユーザーの実際の数によって決まります。メールサーバがメールゲートの役割を果たす場合、エンドユーザーの数は、そのゲートがサービスを提供するメールサーバユーザーの数と同じになります。(エイリアスなどを使用して)1人のユーザーに不特定多数の電子メールアドレスが送信され、それらが受け付けられる場合、クライアント側で多数のユーザーにそのメールが自動的に配信されるのでなければ、ライセンスは1台のコンピューターに必要です。同じライセンスは、同時に複数のコンピューターで使用できません。エンドユーザーは、供給者によって付与されたライセンス数に基づく制限に従い、本ソフトウェアを使用する権限が与えられている範囲においてのみ、本ソフトウェアのライセンスキーを入力する資格があります。このライセンスキーは機密情報であると見なされます。本契約または供給者によって許可されている場合を除き、お客様はライセンスを第三者と共有すること、または第三者がライセンスを使用することを許可することが禁止されています。ライセンスキーが危険にさらされた場合は、速やかに供給者に通知してください。

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

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

e) **OEMソフトウェア。**OEMに分類されたソフトウェアの使用は、それがプリインストールされていたコ

ンピューターに制限されます。別のコンピューターにインストールすることはできません。

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

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

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

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

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

b) **供給者への侵入物および情報の転送**。本ソフトウェアには、コンピューターウイルスおよびその他の悪意のあるプログラム、ファイル、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。

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

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

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

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

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

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

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

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

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

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

7.**著作権**。本ソフトウェア、および所有権や知的所有権を含む一切の権利は、ESETおよび / またはESETのライセンス供給者の財産です。これらは、国際条約の規定と本ソフトウェアが使用される国のその他のすべての準拠法によって保護されます。本ソフトウェアの構造、編成、およびコードは、ESETおよび

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

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

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

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

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

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

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

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

15.**テクニカルサポート**。テクニカルサポートは、ESETまたはESETの依頼を受けた第三者の独自の判断に

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

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

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

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

19.**輸出管理規制**

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

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

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

（上記第i項および第ii項で参照される法律、ならびに「貿易管理法」）。

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

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

ii. エンドユーザーまたは本ソフトウェアに輸出貿易管理法が適用され、その結果としてESETが、合理的

な意見において、本契約の義務の継続的な履行によってESETまたはその関連会社が輸出貿易管理法に違反するか、輸出貿易管理法の下で否定的な影響を受ける可能性があると判断した

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

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

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

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

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

本契約は、本ソフトウェアに関するお客様および供給者間の合意事項をすべて網羅しており、本ソフトウェアに関する従前のいかなる表明、議論、約束、情報交換、または広告にも取って代わります。

EULAID: EULA-PRODUCT-LG-MAC; 3537.0

# 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