# ESET Endpoint Antivirus

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

詳細についてはhttps://www.eset.comをご覧ください。



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

テクニカルサポート: https://support.eset.com

改訂: 2024年/4月/12日

# ESET Endpoint Antivirus

ESET Endpoint Antivirusは、新しいアプローチにより真に堅牢なコンピューターセキュリティを実現します。最新バージョンのESETLiveGrid®検査エンジンは、ご使用中のコンピューターを高い速度と精度をもって安全に保ちます。 その結果、このシステムでは、コンピュータにとって脅威となる攻撃とマルウェアを常に警戒します。

ESET Endpoint Antivirus 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。

ESET Endpoint Antivirus は主に小規模事業環境のワークステーションで使用するために設計されています。

インストールセクションでは、ダウンロード⍰インストール⍰アクティベーションなど、ヘルプトピックが複数の章と節に分類され、位置付けやコンテキストがわかりやすくなっています。

エンタープライズ環境でESET Endpoint AntivirusをESET PROTECTとともに使用することにより、ネットワークに接続されたのどのコンピュータからクライアントワークステーションをいくつでも簡単に管理し、ポリシーとルールの適用、検出の監視、クライアントのリモート設定が可能になります。

よくある質問の章では、よくある質問と問題をいくつか説明します。

---

## 機能と利点

| | |
|---|---|
| **ユーザーインターフェイスの再設計** | このバージョンでは、ユーザーインターフェイスが大幅に再設計され、ユーザビリティテストの結果に基づいて簡略化されています。すべての GUI 用語と通知は慎重にレビューされ、インターフェースは現在ヘブライ語やアラビア語など右から左に記述する言語もサポートしています。オンラインヘルプはESET Endpoint Antivirusに統合され、ダイナミックにアップデートされたサポートコンテンツを提供します。 |
| **ダークモード** | 画面をダークテーマにすばやく切り替えることができる拡張機能。ユーザーインタフェース要素で好みの配色を選択できます。 |
| **ウイルス・スパイウェア対策** | 従来よりもさらに多くの既知および未知のウイルス、ワーム⍰トロイの木馬、そしてルートキットを早期に検出し駆除します。アドバンスドヒューリスティックにより、これまで見られなかったようなマルウェアも検出して未知の脅威からユーザーを保護し、損害をもたらす前にそれらを無効化します⍰[Webアクセス保護]と[フィッシング対策]は、Webブラウザとリモートサーバー間の通信(SSLを含む)を監視することで保護します。[電子メールクライアント保護]では⍰POP3(S)とIMAP(S)プロトコルで受信したメール通信を検査します。 |
| **通常アップデート** | 検出エンジン(以前はウィルス定義データベースという名称)とプログラムモジュールを定期的にアップデートすることは、コンピューターのセキュリティを最大限に確保するのに最良の方法です。 |
| **ESET LiveGrid®(クラウドによる評価)** | ユーザーは、ESET Endpoint Antivirusから、稼働中のプロセスやファイルの評価を直接チェックできます。 |

| | |
|---|---|
| **リモート管理** | ESET PROTECTで、ネットワーク接続環境におけるワークステーション、サーバー、モバイルデバイス上の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(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。 |
| **ネットワーク攻撃保護** | ネットワークトラフィックの内容を分析し、ネットワーク攻撃から保護します。有害だと見なされるすべてのトラフィックがブロックされます。 |
| **Webコントロール(ESET Endpoint Securityのみ)** | Webコントロールを使用すると、不快な内容を掲載していると考えられるWebページをブロックできます。さらに、企業やシステム管理者は、事前に定義された27以上のカテゴリと140以上のサブカテゴリへのアクセスを禁止できます。 |

# 新機能

## ESET Endpoint Antivirusバージョン10. 1の新機能

### Intel® Threat Detection Technology

ランサムウェアがメモリでの検出を回避しようとしたときにランサムウェアを見つけるハードウェアベースの技術。この統合により、ランサムウェア保護が強化され、高い全体的なシステムパフォーマンスも実現できます。サポートされているプロセッサーを参照してください。

### ダークモードとUIの再設計

このバージョンのグラフィカルユーザーインターフェース(GUI)は再設計され、最新のバージョンです。ダークモードを追加すると、ユーザーインターフェース要素でESET Endpoint Antivirus GUIを明るい配色にするか暗い配色にするかを選択できます。

### 再設計された詳細設定

詳細設定が再設計され、ユーザーエクスペリエンス向上のために設定がグループ化されました。

### さまざまなバグ修正とパフォーマンスの改善

# システム要件

ESET Endpoint Antivirusをシームレスに動作させるために、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(既定の製品設定)。

## サポート対象のプロセッサ

IntelまたはAMDのSSE2命令セットの32ビット(x86)プロセッサーまたは64ビット(x64)プロセッサ1 GHz以上
ARM64ベースのプロセッサ1GHz以上

## OS

Microsoft® Windows® 11

Microsoft® Windows® 10

サポートされているMicrosoft® Windows® 10とMicrosoft® Windows® 11バージョンの詳細については、Windowsオペレーティングシステムサポートポリシーを参照してください。

常にオペレーティングシステムを最新の状態に保つようにしてください。

2023年7月以降にリリースされたESET製品をインストールまたはアップグレードするには、すべてのWindowsオペレーティングシステムにAzure Code Signingのサポートをインストールする必要があります。詳細情報

## ESET Endpoint Antivirus機能要件

次の表の特定のESET Endpoint Antivirus機能に関するシステム要件を参照してください。

| 機能 | 要件 |
|---|---|
| Intel® Threat Detection Technology | サポートされているプロセッサーを参照してください。 |
| 専用駆除アプリケーション | 非ARM64ベースのプロセッサー。 |
| エクスプロイトブロッカー | 非ARM64ベースのプロセッサー。 |
| 詳細動作検査 | 非ARM64ベースのプロセッサー。 |

ESET PROTECTで作成されたESET Endpoint Antivirusインストーラーは、Windows 10 Enterprise for Virtual DesktopsおよびWindows 10マルチセッションモードをサポートします。

## その他

- コンピューターにインストールされているオペレーティングシステムと他のソフトウェアのシステム要件が満たされていること
- 0.3 GBの空きシステムメモリ(注記1を参照)
- 1 GBの空きディスク領域(注記2を参照)
- 最低ディスプレイ解像度1024 x 768
- 製品アップデートのソース(注記3を参照)へのインターネット接続またはローカルエリアネットワーク接続
- 1台のデバイスで同時に実行されている2つのウイルス対策プログラムにより、システムの速度が低下して動作不能になるなど、必然的にシステムリソースの競合が発生します。

これらの要件を満たしていないシステムでも製品をインストールおよび実行できる場合がありますが、パフォーマンス要件に基づく事前の使用可能性のテストを推奨しています。

**(1)**: 感染による損傷が多いコンピューターでメモリが使用されない場合、または大量のデータリストが製品にインポートされているとき(URLホワイトリストなど)には、製品は追加のメモリを使用する可能性があります。
**(2)** インストーラーをダウンロード、製品をインストール、ロールバック機能をサポートするためにプログラムデータのインストールパッケージと製品アップデートのバックアップのコピーを保存するために必要なディスク領域。別の設定が使用される(追加の製品アップデートバックアップバージョンが保存されるときにメモリダンプまたは大量のログレコードのリストが保持されるなど)場合、または感染したコンピューター(隔離機能のため)では、追加のディスク領域が使用される場合があります。オペレーティングシステムとESET製品のアップデートをサポートするために、十分な空きディスク領域を確保することをお勧めします。
**(3)** 製品はリムーバブルメディアから手動でアップデートできます(非推奨)。

# サポートされている言語

ESET Endpoint Antivirusは、次の言語でインストールおよびダウンロードできます。

| 言語 | 言語コード | LCID |
|---|---|---|
| 英語(米国) | en-US | 1033 |
| アラビア語(エジプト) | ar-EG | 3073 |
| ブルガリア語 | bg-BG | 1026 |
| 簡体中国語 | zh-CN | 2052 |
| 繁体中国語 | zh-TW | 1028 |
| クロアチア語 | hr-HR | 1050 |
| チェコ語 | cs-CZ | 1029 |
| エストニア語 | et-EE | 1061 |
| フィンランド語 | fi-FI | 1035 |
| フランス語(フランス) | fr-FR | 1036 |
| フランス語(カナダ) | fr-CA | 3084 |
| ドイツ語(ドイツ) | de-DE | 1031 |
| ギリシャ語 | el-GR | 1032 |
| *ヘブライ語 | he-IL | 1037 |
| ハンガリー語 | hu-HU | 1038 |
| *インドネシア語 | id-ID | 1057 |
| イタリア語 | it-IT | 1040 |
| 日本語 | ja-JP | 1041 |
| カザフスタン語 | kk-KZ | 1087 |
| 韓国語 | ko-KR | 1042 |
| *ラトビア語 | lv-LV | 1062 |
| リトアニア語 | lt-LT | 1063 |
| オランダ語 | nl-NL | 1043 |
| ノルウェー語 | nb-NO | 1044 |
| ポーランド゛語 | pl-PL | 1045 |
| ポルトガル語(ブラジル) | pt-BR | 1046 |
| ルーマニア語 | ro-RO | 1048 |
| ロシア語 | ru-RU | 1049 |
| スペイン語(チリ) | es-CL | 13322 |
| スペイン語(スペイン) | es-ES | 3082 |
| スウェーデン語(スウェーデン) | sv-SE | 1053 |
| スロバキア語 | sk-SK | 1051 |
| スロヴェニア語 | sl-SI | 1060 |
| タイ語 | th-TH | 1054 |
| トルコ語 | tr-TR | 1055 |

| 言語 | 言語コード | LCID |
| --- | --- | --- |
| ウクライナ語(ウクライナ) | uk-UA | 1058 |
| *ベトナム語 | vi-VN | 1066 |

* ESET Endpoint Antivirusはこの言語で提供されていますが、オンラインユーザーガイドは提供されていません(英語版にリダイレクトされます)。

このオンラインユーザーガイドの言語を変更するには、(右上隅にある)言語選択ボックスを確認してください。

# 変更ログ

# セキュリティの考え方

コンピューターを使用するとき、特にインターネットを利用する場合には、検出とリモート攻撃の危険を完全に排除できるウイルス対策システムは存在しないということを忘れないでください。最大限の保護と利便性を提供するには、ウイルス対策ソリューションを正しく試用し、複数の役立つルールに従うことが重要です。

## 定期的にアップデートする

ESET LiveGrid®の統計データによると、既存のセキュリティ手段をすり抜けマルウェアの作成者に利益をもたらすために、毎日数千種類のマルウェアが新たに作成されています。この利益は、他のユーザーの犠牲の上に成り立っています。ESET Virus Labの担当者は、ユーザーの保護レベルを改善するために、これらの脅威を毎日解析し、更新ファイルを作成してリリースしています。最大限の効果を保証するには、システムでアップデートを正しく設定する必要があります。アップデートの設定方法の詳細は、「アップデートの設定」の章を参照してください。

## セキュリティパッチをダウンロードする

多くの場合、悪意のあるソフトウェアの作成者はシステムの脆弱性を悪用します。それは、悪意のあるコードを効率的に蔓延させるためです。これを念頭に、ソフトウェアベンダ各社は、アプリケーションの脆弱性が表面化しないかどうかを注意深く見守り、潜在的な脅威を排除するためにセキュリティ更新ファイル(セキュリティパッチ)を定期的にリリースします。これらのセキュリティ更新ファイルは、リリースされたらすぐにダウンロードすることが重要です。例えばMicrosoft WindowsやMicrosoft EdgeなどのWebブラウザは、アップデートファイルが定期的にリリースされています。

## 重要なデータをバックアップする

マルウェアの作成者がユーザーのニーズに配慮することは、ほとんどありません。悪意のあるプログラムが、オペレーティングシステムの誤作動を引き起こし、重要なデータの損失を招くことがよくあります。DVDや外付けハードディスクなどの外部メディアに、データを定期的にバックアップする必要があります。これにより、システム障害が発生したときでもデータを簡単にすばやく復旧できます。

## コンピュータにウイルスがいないか定期的にスキャンする

既知や未知のウイルス、ワーム、トロイの木馬、およびルートキットの検出は、リアルタイムファイルシステム保護モジュールによって処理されます。これにより、ファイルにアクセスするかファイルを開くたびに、マルウェアの活動を検査します。ただし、マルウェアのシグネチャは変化することがあり、

検出エンジンは毎日更新されるため、少なくとも1か月に1回はコンピュータの完全な検査を実行することをお勧めします。

## 基本的なセキュリティルールに従う

常に用心することこそ、あらゆるルールの中で最も有益で効果的なルールです。今日の多くのマルウェアは、ユーザーが操作しないと、実行されず蔓延しません。新しいファイルを開くときに注意すれば、感染した場合にマルウェアを駆除するために多大な時間と労力を費やさずに済みます。次に、いくつかの有益なガイドラインを示します。

- ポップアップや点滅する広告がいくつも表示される、怪しいWebサイトにはアクセスしない。
- フリーウェアやコーデックパックのインストール時には注意する。安全なプログラムだけ使用し、安全なWebサイトにだけアクセスする。
- メールの添付ファイルを開くときに注意する。特に、大量に送信されたメッセージや知らない送信者からのメッセージの添付ファイルに注意する。
- 日々の作業では、コンピュータの管理者アカウントを使用しない。

# ヘルプページ

ESET Endpoint Antivirusユーザーガイドをご利用いただき、誠にありがとうございます。ここに示された情報を参照することで、製品の理解を深めることができ、コンピューターの安全性を高めることができます。

## はじめに

ESET Endpoint Antivirusの使用を開始する前に、ESET PROTECTを使用して製品をリモートで管理できることに注意してください。また、コンピューターの使用時に発生する可能性がある、さまざまなタイプの侵入とリモート攻撃について、十分に理解することをお勧めします。

このバージョンのESET Endpoint Antivirusに導入された機能の詳細については、「新機能」を参照してください。ESET Endpoint Antivirusの基本設定とカスタマイズに便利なガイドもご用意しました。

## ESET Endpoint Antivirusヘルプページの使用方法

ヘルプトピックは、位置付けやコンテキストをわかりやすくするために、複数の章と節に分割されています。関連する情報は、ヘルプページ構造を見るだけで見つけることができます。

プログラムで表示されるウィンドウについての説明を見るには、**F1**キーを押してください。現在表示しているウィンドウに関連するヘルプページが表示されます。

ヘルプページを検索するには、キーワードを使用するか、単語またはフレーズを入力します。キーワード検索では、その特定のキーワードが本文中に出てこないヘルプページでも、論理的に関連付けられている場合表示されます。語句による検索では、すべてのページの内容が検索され、その語句が出てくるページだけが表示されます。

一貫性と混乱を防止するため、このガイドで使用される用語はESET Endpoint Antivirusパラメーター名に基づいています。また、統一された記号を使用して、特定の関心または重要性があるトピックを強調しています。

> 簡単な説明です。省略できますが、特定の機能や一部の関連トピックへのリンクといった有益な情報が含まれていることがあります。

目を通すことが推奨される注意が必要な項目です。通常は、重大ではないものの、重要な情報が記載されています。

一層の注意が必要な情報です。特に、有害な間違いを防止するために警告が書かれています。警告の括弧内にある文を読んで理解してください。十分な注意が必要なシステム設定やリスクがある設定について説明されています。

これは使用例または実際の例であり、特定の機能を使用する方法を理解できるようにすることを目的としています。

| 表記規則 | 意味 |
|---|---|
| **太字** | ボックスやオプションボタンなどのインターフェイス項目の名前。 |
| 斜体 | ユーザーが入力する情報のプレースホルダー。たとえば、ファイル名やパスは、ユーザーが実際のパスまたはファイル名を入力することを意味します。 |
| `Courier New` | コードサンプルまたはコマンド。 |
| ハイパーリンク | 相互参照されたトピックまたは外部Webサイトへのすばやく簡単なアクセスを提供します。ハイパーリンクは青字でハイライトされ、下線も付いている場合があります。 |
| *%ProgramFiles%* | Windowsにインストールされたプログラムが保存されるWindowsシステムディレクトリ。 |

**オンラインヘルプ**はヘルプコンテンツの主なソースです。インターネットに接続している場合には、最新バージョンのオンラインヘルプが自動的に表示されます。

# リモート管理されたエンドポイントのドキュメント

ESETビジネス製品およびESET Endpoint Antivirusは、1つの集中管理された場所から、ネットワーク接続環境におけるクライアントワークステーション、サーバー、およびモバイルデバイスで、リモート管理できます。10台以上のクライアントワークステーションを管理するシステム管理者は、ESETリモート管理ツールのいずれかを展開すると、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 Antivirusは、ESET PROTECTまたはESET PROTECT Cloudでリモート管理できます。

- ESET PROTECTの概要
- ESET PROTECT Cloudの概要

- ESET HUB - ESET PROTECT統合セキュリティプラットフォームへの中央ゲートウェイ。すべてのESETプラットフォームモジュールのIDサブスクリプション、およびユーザー管理を一元的に行うことができます。製品をアクティベーションする手順については、ESET PROTECTライセンス管理を参照してくださいESET Business AccountとESET MSP Administratorは完全にESET HUBに置き換わります。

- ESET Business Account - ESET Business Accountのライセンス管理ポータル。製品をアクティベーションする手順については、ESET PROTECTライセンス管理を参照してくださいESET Business Accountの使用に関する詳細については、ESET Business Accountオンラインヘルプを参照してください。すでにESETが発行したユーザー名とパスワードがあり、製品認証キーに変換する場合には、レガシーライセンス資格情報の変換」セクションを参照してください。

## その他のセキュリティ製品

- ESET Inspect – 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 Endpoint Encryption – 保存中および転送中のデータを保護するよう設計された包括的なセキュリティアプリケーションです。ESET Endpoint Encryptionを使用すると、ファイル、フォルダー、電子メールの暗号化、暗号化された仮想ディスクの作成、アーカイブの圧縮、安全にファイルを削除するデスクトップシュレッダーの追加といったことができます。

## サードパーティーのリモート管理ツール

- リモート監視と管理 (RMM)

## ベストプラクティス

- ESET Endpoint Antivirusを使用してすべてのエンドポイントをESET PROTECTに接続する
- 接続されたクライアントコンピューターで、詳細設定を保護し、不正な修正を防止する
- 推奨されたポリシーを適用して、使用可能なセキュリティ機能を施行する
- ユーザーインターフェースを最小化する。ユーザーによるESET Endpoint Antivirusの操作を制限する。

## ガイド

- 上書きモードを使用する方法
- GPOまたはSCCMを使用してESET Endpoint Antivirusを展開する方法

# ESET PROTECTの概要

ESET PROTECTで、ネットワーク接続環境におけるワークステーション、サーバー、モバイルデバイス上の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。ESET PROTECT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、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 – 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。
- ESET PROTECT Webコンソール - 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のステータス概要を表示し、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ESET PROTECTサーバーをインストールすればWebブラウザーを使用してWebコンソールにアクセスできます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。
- ESET Managementエージェント - 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ESETManagement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。

- ESET Rogue Detection Sensor – 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、手動で検索および追加せずにESET PROTECTで新しいクライアントコンピューターを管理できますRogue Detection 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と組み合わせて使用できるサービスで、
    - 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。
    - ESET ManagementエージェントからESET PROTECTサーバーに通信を転送します。
- モバイルデバイスコネクター - ESET PROTECTでモバイルデバイス管理を可能にするコンポーネントであり、モバイルデバイス(AndroidおよびiOS)を管理し、ESET Endpoint Security for Androidを管理できます。
- ESET PROTECT仮想アプライアンス – 仮想環境でESET PROTECTを実行したいユーザを対象にしています。
- ESET PROTECT Virtual Agent Host– エージェントレス仮想コンピューターを管理するエージェントエンティティを仮想化するESET PROTECTのコンポーネント。このソリューションにより、自動化、動的グループの利用、物理コンピューターのESET Managementエージェントと同じレベルのタスク管理が可能になります。仮想エージェントは仮想マシンから情報を収集し、ESET PROTECTサーバーに送信します。
- ミラーツール – 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 - <%PRODUCT%> 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します。ネットワーク上のコンピュータでESET Managementエージェントと ESET製品を配布するための便利な方法です。

詳細情報については、ESET PROTECTオンラインヘルプを参照してください。

# ESET PROTECT Cloudの概要

ESET PROTECT CloudではESET PROTECTや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 Cloud 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 Cloudは次のコンポーネントで構成されています。

- ESET PROTECT Cloudインスタンス – 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 Cloud Webコンソール - 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のステータス概要を表示し、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。インターネットに接続されている場所やデバイスからESET PROTECT Cloudを使用できます。
- ESET Managementエージェント - ESET PROTECT Cloudとクライアントコンピューター間の通信を容易にします。コンピューターとESET PROTECT Cloud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 PROTECT CloudWebコンソールを使用すると、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。

- ESET Bridge - ESET PROTECT Cloudと組み合わせて使用できるサービスで、
  - 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。
  - ESET ManagementエージェントからESET PROTECT Cloudに通信を転送します。
- モバイルデバイス管理 - ESET PROTECT Cloudでモバイルデバイス管理を可能にするコンポーネントであり、モバイルデバイス(AndroidおよびiOS)を管理し、ESET Endpoint Security for Androidを管理できます。
- 脆弱性およびパッチ管理 – ワークステーションを定期的に検査して、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する機能。ESET PROTECT Cloudで利用できます。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。

詳細情報については、ESET PROTECT Cloudオンラインヘルプを参照してください。

# 設定をパスワードで保護する

システムのセキュリティを最大化するには、ESET Endpoint Antivirusを正しく設定する必要があります。適正ではない変更や設定は、クライアントセキュリティや保護レベルの低下につながるおそれがあります。詳細設定へのユーザーアクセスを制限するために、管理者は、設定をパスワードで保護することができます。

管理者は、接続されたクライアントコンピューターのESET Endpoint Antivirusの詳細設定をパスワードで保護するためのポリシーを作成できます。新しいポリシーを作成するには、次の手順に従います。

1. ESET PROTECT Webコンソールで、左側のメインメニューで**ポリシー**をクリックします。
2. **新しいポリシー**をクリックします。
3. 新しいポリシーの名前を指定し、任意で簡単な説明を指定します。**続行**ボタンをクリックします。
4. 製品のリストから、**ESET Endpoint for Windows**を選択します。
5. 設定リストの**ユーザーインターフェース**をクリックし、**アクセス設定**を展開します。
6. ESET Endpoint Antivirusのバージョンに従い、サイドバーをクリックして、**設定を保護するパスワード**を有効にします。ESET Endpoint製品バージョン7では、保護が強化されています。バージョン7とバージョン6 の両方のEndpoint製品をネットワークで使用している場合は、各バージョンに別のパスワードを使用して2つの別のポリシーを作成することをお勧めします。
7. 通知ウィンドウで、新しいパスワードを作成し、確認して、**OK**をクリックします。**続行**をクリックします。
8. ポリシーをクライアントに割り当てます。**割り当て**をクリックし、パスワードで保護するコンピュータまたはコンピュータのグループを選択します。**OK**をクリックして確認します。
9. すべての目的のクライアントコンピュータがターゲットリストにあることを確認し、**続行**をクリックします。
10. サマリーでポリシー設定を確認し、**完了**をクリックして、新しいポリシーを保存します。

# ポリシーの概要

管理者は、ESET PROTECT Webコンソールまたは Webコンソールから、ポリシーを使用して、クライアントコンピューターで実行されるESET製品に特定の設定をプッシュすることができます。ポリシーは、直接個別のコンピューターやコンピューターのグループに適用できます。また、複数のポリシーをコンピューターまたはグループに割り当てることができます。

ユーザーが新しいポリシーを作成するには、次の権限が必要です。**読み取り**権限は、ポリシーのリストを読み取ります。**使用**権限は、ポリシーをターゲットコンピュータに割り当てます。**書き込み**権限は、ポリシーを作成、修正、または編集します。

ポリシーは静的グループの順序で適用されます。動的グループの場合、ポリシーが最初に子動的グループに適用されます。これにより、影響度がより大きいポリシーをグループツリーの最上位に適用し、個別性の高いポリシーをサブグループに適用できます。フラグを使用すると、ツリーの上位にあるグループにアクセスできるESET Endpoint Antivirusユーザーは、下位のグループのポリシーを上書きできます。このアルゴリズムについては、ESET PROTECTオンラインヘルプを参照してください。

> グループツリーの上位にあるグループには、より汎用的なポリシー(アップデートサーバーポリシーなど)を割り当てることをお勧めします。より特定のポリシー(デバイスコントロール設定など)はグループツリーの下位に割り当てられます。通常、マージ時に下位のポリシーが上位の設定を上書きします(ポリシーフラグで定義されている場合を除く)。

# ポリシーのマージ

通常、クライアントに適用されたポリシーは、複数のポリシーが1つの最終ポリシーにマージされたものです。ポリシーは1つずつマージされます。ポリシーをマージするときの原則は、後のポリシーによって、前のポリシーで構成された設定が必ず置換されるということです。この動作を変更するには、ポリシーフラグ(各設定で使用可能)を使用できます。

ポリシーを作成するときには、一部の設定には設定できる追加ルール(置換/後に追加/前に追加)があります。

- **置換** – リスト全体が置換され、新しい値が追加されて、すべての以前の値が削除されます。
- **後に追加** – 項目は現在適用されているリストの最後に追加されます(別のポリシーである必要があります。ローカルリストは常に上書きされます)。
- **前に追加** – 項目はリストの先頭に追加されます(ローカルリストは上書きされます)。

ESET Endpoint Antivirusは、新しい方法でリモートポリシーとローカル設定のマージをサポートします。設定がリスト(ブロックされたWebサイトのリストなど)で、ポリシーが既存のローカル設定と競合している場合、リモートポリシーが優先されます。ローカルリストとリモートリストを結合する方法を選択するには、別のマージルールを選択します。

- リモートポリシーの設定のマージ。
- リモートおよびローカルポリシーのマージ – ローカル設定を結果のリモートポリシーでマージ。

ポリシーのマージの詳細については、ESET PROTECTオンラインユーザーガイドに従い、例を参照してください。

# フラグの仕組み

通常、クライアントコンピュータに適用されるポリシーは、1つの最終ポリシーにマージされる複数のポリシーの結果です。ポリシーをマージするときには、適用されるポリシーの順序のため、ポリシーフラグを使用して、最終ポリシーの想定される動作を調整できます。フラグは、ポリシーが特定の設定を処理する方法を定義します。

各設定に対して、次のフラグのいずれかを選択できます。

| | |
|---|---|
| **未適用** | このフラグの設定はポリシーによって設定されていません。設定はポリシーによって設定されていないため、後から適用される他のポリシーで変更できます。 |
| **適用** | **適用**フラグが付いた設定は、クライアントコンピューターに適用されます。ただし、ポリシーをマージするときには、後から適用される他のポリシーによって上書きされることがあります。このフラグが付いた設定を含むクライアントコンピューターにポリシーが送信されるときには、これらの設定により、クライアントコンピューターのローカル設定が変更されます。設定は強制ではないため、後から適用される他のポリシーによって変更されることがあります。 |
| **強制** | **強制**フラグが付いた設定は優先度があり、(**強制**フラグがある場合でも)後から適用されるどのポリシーによっても上書きされることはありません。これにより、後から適用される他のポリシーがマージ中にこの設定を変更できないことが保証されます。このフラグが付いた設定を含むクライアントコンピューターにポリシーが送信されるときには、これらの設定により、クライアントコンピューターのローカル設定が変更されます。 |

**シナリオ**:管理者はユーザー*John*がホームグループのポリシーを作成または編集し、 強制フラグが付いたポリシーを含む、管理者が作成したすべてのポリシーを表示できるようにします。管理者は、*John*がすべてのポリシーを表示できるようにしますが、管理者が作成した既存のポリシーの編集は許可しません。*John*は、ホームグループSan Diego内でのみ、ポリシーを作成または編集できます。
解決策:管理者は次の手順に従います。
**カスタム静的グループと権限設定の作成**
1. 新しい静的グループの*San Diego*を作成します。
2. 静的グループすべてへのアクセスと**ポリシー**の**読み取り**権限がある新しい権限設定の*Policy - All John*を作成します。
3. 静的グループ*San Diego*へのアクセスと**グループとコンピュータ**と**ポリシー**の**書き込み**権限がある新しい権限設定の*Policy John*を作成します。この権限設定により、*John*は、ホームグループ*San Diego*でポリシーを作成または編集できます。
4. 新しいユーザー*John*を作成し、 **権限**設定セクションで、*Policy - All John*と*Policy John*を選択します。
**ポリシーの作成**
5. 新しいポリシー*All- Enable Firewall*を作成し、 **設定**セクションを展開し、**ESET Endpoint for Windows**を選択して、**パーソナル ファイアウォール > 基本**に移動して、 強制フラグですべての設定を適用します。**割り当て**セクションを展開し、静的グループ*All*を選択します。
6. 新しいポリシー*John Group- Enable Firewall*を作成し、**設定**セクションを展開し、**ESET Endpoint for Windows**を選択して、**パーソナルファイアウォール > 基本**に移動して、 適用フラグですべての設定を適用します。**割り当て**セクションを展開し、静的グループ*San Diego*を選択します。
**結果**
**強制**フラグがポリシー設定に適用されたため、管理者が作成したポリシーは最初に適用されます。強制フラグが適用された設定は優先度があり、後から適用される別のポリシーで上書きできません。ユーザー*John*が作成したポリシーは、管理者が作成したポリシーの後に適用されます。最終ポリシー順序を確認するには、**詳細 > グループ > San Diego**に移動します。コンピュータを選択して、**詳細の表**示を選択します。**設定**セクションで、**適用されたポリシー**をクリックします。

# インストール

ESET PROTECTまたはESET PROTECT Cloud経由で、ESET Endpoint Antivirusをリモートでクライアントワークステーションに展開する場合を除き、クライアントワークステーションでは、複数のESET Endpoint Antivirusのインストール方法があります。

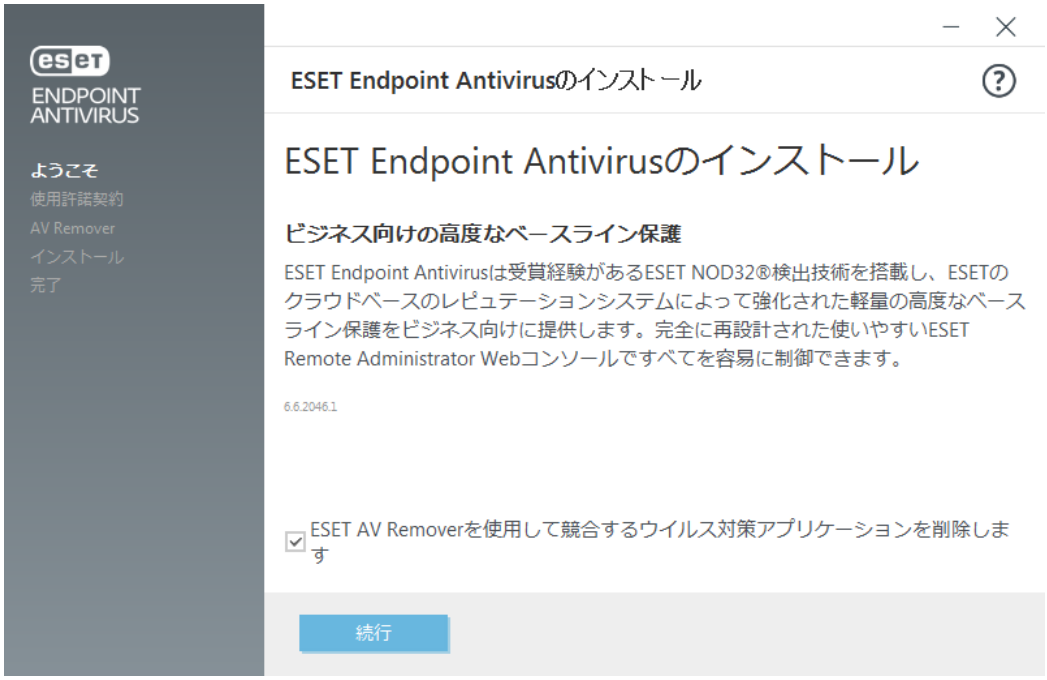
ESET Endpoint AntivirusからESET Endpoint Securityにアップグレードするには、ESET Endpoint Antivirusをインストール済みの状態でESET Endpoint Securityインストーラーを実行します。ただし、同じバージョンまたはそれ以降のバージョンをインストールする必要があります。

| 検査方法 | 目的 | ダウンロードリンク |
| --- | --- | --- |
| ESET AV Removerでインストール | ESET AV Removerヘルプツールを使用すると、インストールを続行する前に、以前にシステムにインストールしたほぼすべてのウイルス対策ソフトウェアを削除できます。 | 64ビット版のダウンロード<br>32ビット版のダウンロード |
| *** インストール (.exe) | ESET AV Removerを使用しないインストール処理 | 64ビット版のダウンロード<br>32ビット版のダウンロード |
| インストール (.msi) | ビジネス環境では.msiインストーラーが推奨されるインストールパッケージです。これは、主に、オフラインおよびリモート展開がESET PROTECTなどのさまざまなツールを使用するためです。 | 64ビット版のダウンロード<br>32ビット版のダウンロード |
| コマンドラインインストール | ESET Endpoint Antivirusは、コマンドラインでローカルにインストールするかESET PROTECTからのクライアントタスクを使用してリモートでインストールできます。 | N/A |
| GPOまたはSCCMを使用した展開 | GPOやSCCMなどの管理ツールを使用してESET Management AgentおよびESET Endpoint Antivirusをクライアントワークステーションに展開します。 | N/A |
| RMMツールを使用した展開 | Remote Management and Monitoring (RMM)ツール向けのESET DEMプラグインではESET Endpoint Antivirusをクライアントワークステーションに展開できます。 | N/A |

ESET Endpoint Antivirusは30種類以上の言語で提供されています。

# ESET AV Removerでインストール

インストール処理を続行する前に、コンピュータ上の既存のセキュリティアプリケーションをアンインストールすることが重要です。**ESET AV Removerを使用して不要なセキュリティ製品をアンインストールする**の横のチェックボックスを選択し、ESETAVRemoverでシステムを検査し、サポートされているセキュリティアプリケーションを削除します。チェックボックスをオフにして、**続行**をクリックするとESET AV Removerを実行せずにESET Endpoint Antivirusをインストールします。



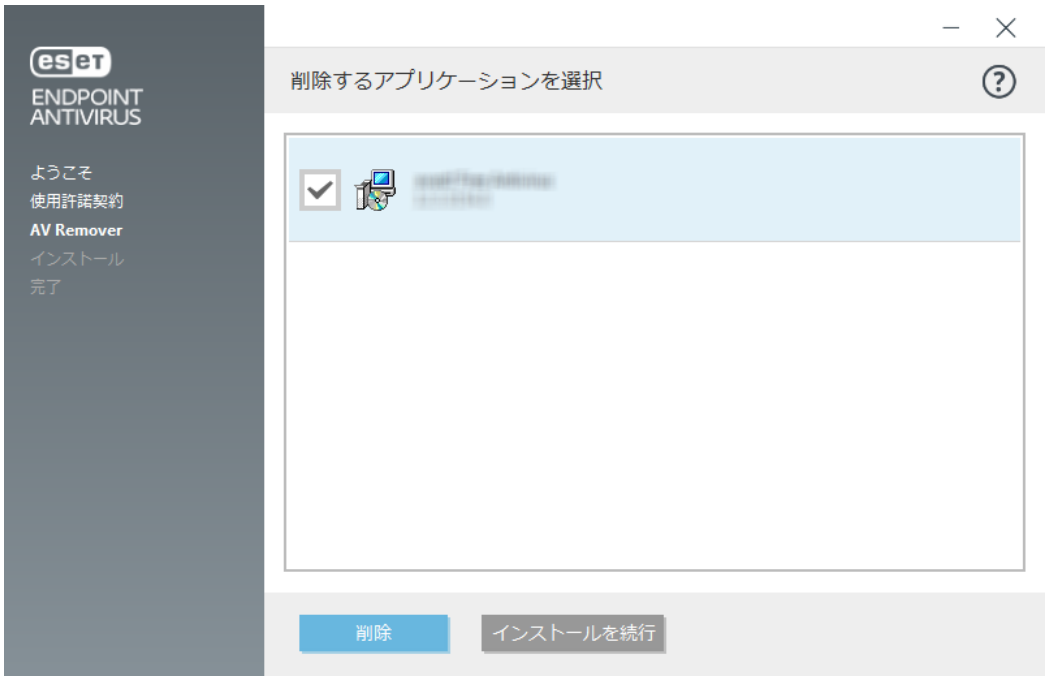

# ESET AV Remover

ESET AV Removerツールを使用すると、以前にシステムにインストールしたほぼすべてのウイルス対策ソフトウェアを削除できます。次の手順に従い、ESET AV Removerを使用して既存のウイルス対策プログラムを削除します。

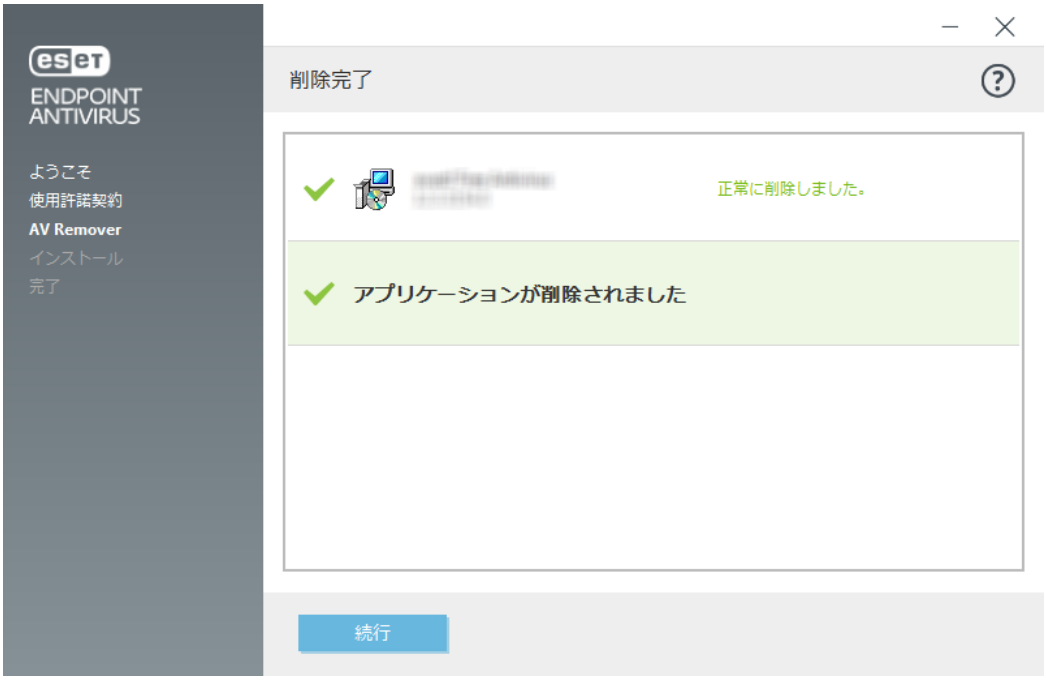
1. ESET AV Removerで削除できるウイルス対策ソフトウェアの一覧については、ESETナレッジベース記事を参照してください。
2. エンドユーザーライセンス契約を読んで[**同意する**]をクリックし、承諾することを確認します。[**同意しない**]をクリックすると、コンピュータ上の既存のセキュリティアプリケーションを削除せずにESET Endpoint Antivirusのインストールを続行します。


2. ESET AV Removerがシステムのウイルス対策ソフトウェアを検索し始めます。

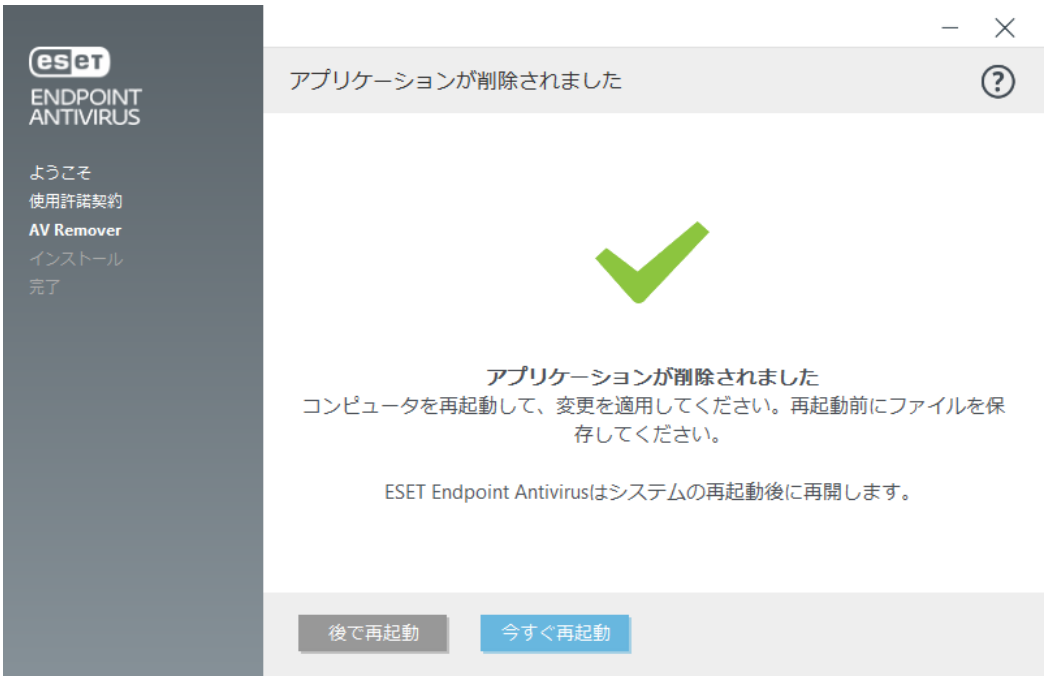

2. 一覧のウイルス対策アプリケーションを選択し、[**削除**]をクリックします。削除にはしばらくかかる場合があります。




2. 削除が成功したら、[**続行**]をクリックします。




6. コンピュータを再起動して変更を適用し、ESET Endpoint Antivirusのインストールを続行します。アンインストールが失敗した場合は、このガイドの「ESET AV Removerによるアンインストールがエラーで終了した場合」を参照してください。




# ESET AV Removerによるアンインストールがエラーで終了した場合

ESET AV Removerを使用してウイルス対策プログラムを削除できない場合は、削除しようとしているアプリケーションがESET AV Removerによってサポートされていない可能性があるという通知が表示されます。ESETナレッジベースのサポートされている製品の一覧または一般的なWindowsウイルス対策ソフトウェアのアンインストーラを参照して、この特定のプログラムを削除できるかどうかを確認してください。

セキュリティ製品のアンインストールが失敗した場合や、コンポーネントの一部が部分的にアンインストールされなかった場合は、**再起動して再検査**するように指示されます。起動後にUACを確認し、検査

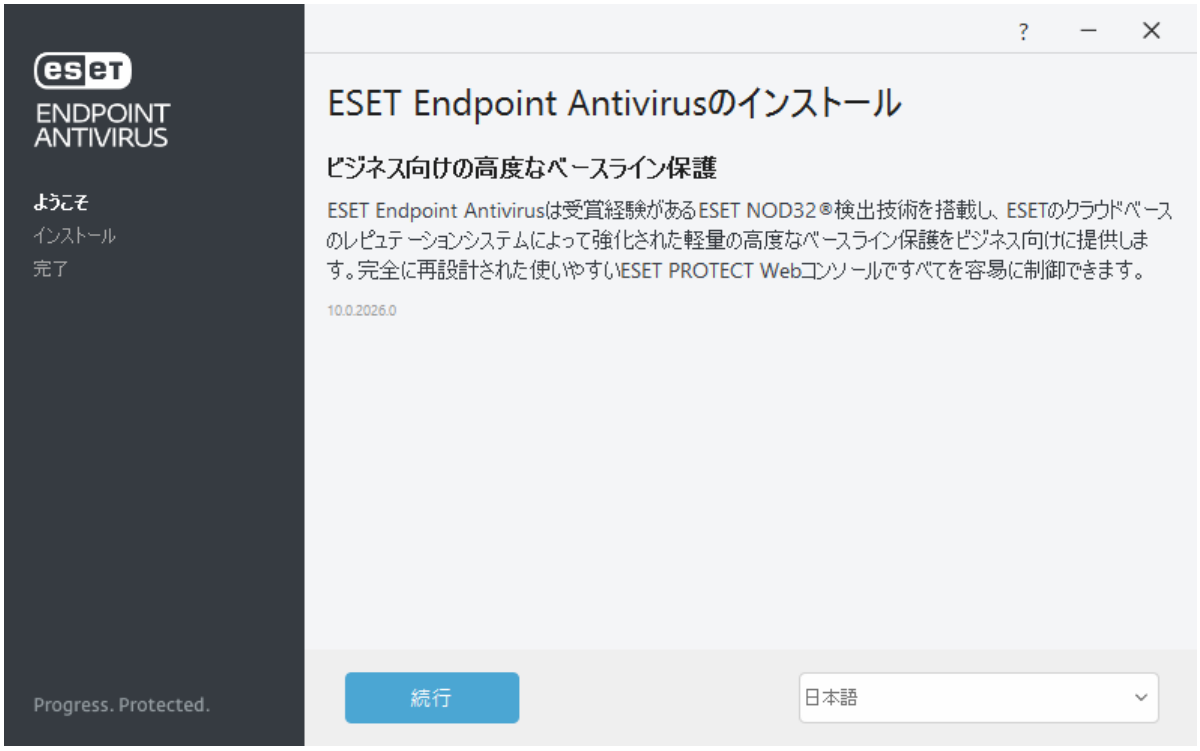
とアンインストール処理を続行します。

必要に応じて、ESETテクニカルサポートに連絡してサポート申請を行い、**AppRemover.log**ファイルを提出してESET技術者を支援します。**AppRemover.log**ファイルは**eset**フォルダにあります。Windowsエクスプローラで*%TEMP%*を参照し、このフォルダにアクセスします。ESETテクニカルサポートはできるかぎり速やかに対応し、問題の解決をお手伝いします。

# インストール (.exe)

インストーラーを起動すると.exeインストールウィザードが表示されるので、その案内に従ってインストール処理を行ってください。

コンピュータに他のウイルス対策プログラムがインストールされていないことを確認します。2つ以上のウイルス対策プログラムが1台のコンピュータにインストールされている場合、互いに競合する場合があります。システムから他のウイルス対策プログラムをアンインストールすることをお勧めします。一般的なウイルス対策ソフトウェアのアンインストーラツール(英語および他のいくつかの各国語のもの)のリストは、ナレッジベースの記事を参照してください。




1. 次の機能の設定を選択し、エンドユーザーライセンス契約とプライバシーポリシーを読み、**続行**をクリックするか、**すべて許可して続行**をクリックしてすべての機能を有効にします。

- ESET LiveGrid®フィードバックシステム
- 望ましくない可能性のあるアプリケーション検出

**続行**または**すべて許可して続行**をクリックして、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を確認します。ESET Endpoint Antivirusを特定のフォルダーにインストールするには、インストールフォルダーの変更をクリックします。


2. インストールが完了した後、ESET Endpoint Antivirusをアクティベーションするように指示されます。

# インストールフォルダの変更(.exe)

インストール中**にインストールフォルダを変更**できますESET Endpoint Antivirusインストールの場所を選択します。既定では、プログラムは以下のディレクトリにインストールされます。

*C:\Program Files\ESET\ESET Security*

プログラムモジュールとデータの場所を指定できます。既定では、プログラムは以下のディレクトリにそれぞれインストールされます。

*C:\Program Files\ESET\ESET Security\Modules*
*C:\ProgramData\ESET\ESET Security*

場所を変更するには、[**参照**]をクリックします(推奨しません)。

**戻る**をクリックし、インストール処理を続行します。

# インストール (.msi)

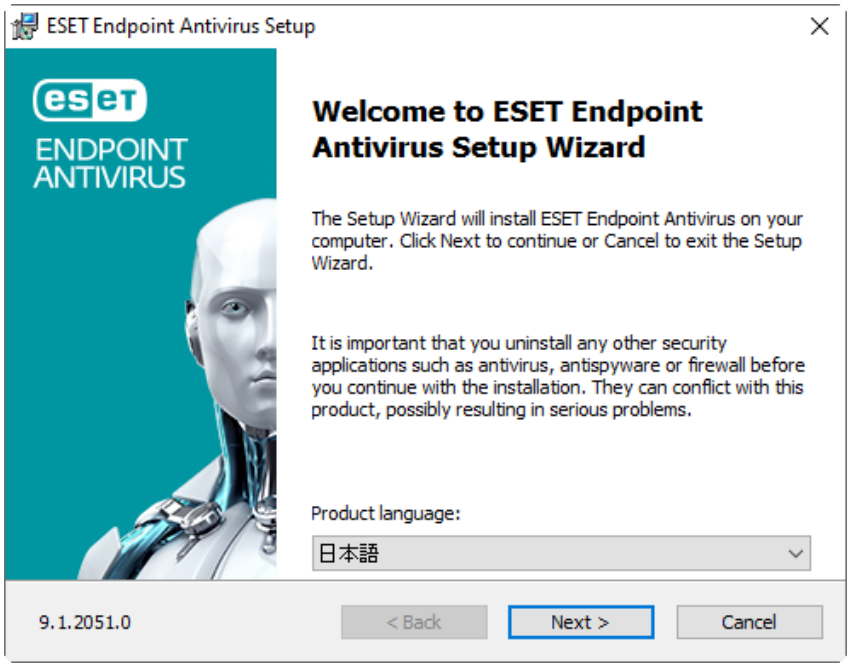
.msiインストーラーを起動すると、インストールウィザードが表示されるので、その案内に従ってインストール処理を行ってください。

ビジネス環境では.msiインストーラーが推奨されるインストールパッケージです。これは、主に、オフラインおよびリモート展開がESET PROTECTなどのさまざまなツールを使用するためです。

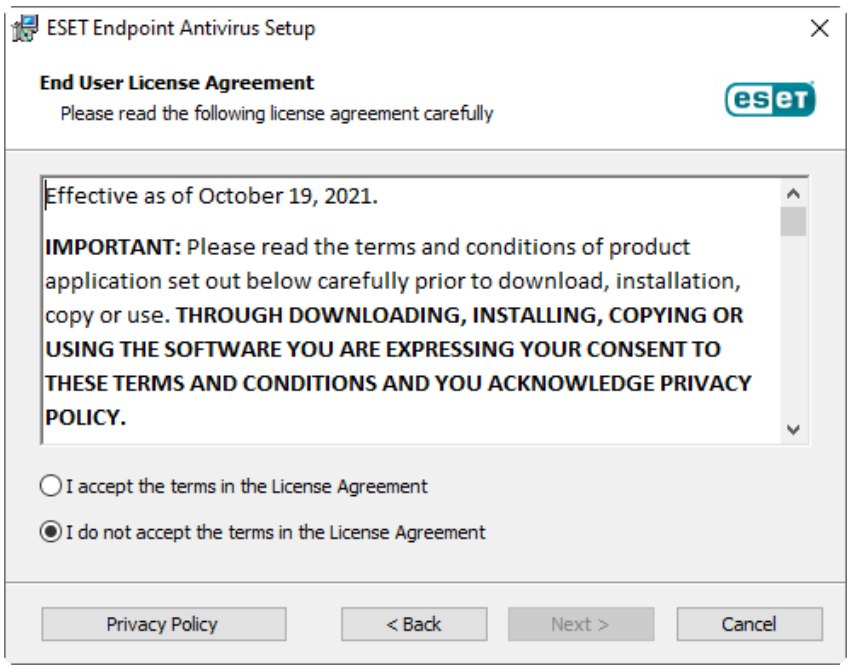
コンピュータに他のウイルス対策プログラムがインストールされていないことを確認します。2つ以上のウイルス対策プログラムが1台のコンピュータにインストールされている場合、互いに競合する場合があります。システムから他のウイルス対策プログラムをアンインストールすることをお勧めします。一般的なウイルス対策ソフトウェアのアンインストーラツール(英語および他のいくつかの各国語のもの)のリストは、ナレッジベースの記事を参照してください。

ESET PROTECTで作成されたESET Endpoint Antivirusインストーラーは、Windows 10 Enterprise for Virtual DesktopsおよびWindows 10マルチセッションモードをサポートします。

1. 任意の言語を選択し、**次へ**をクリックします。

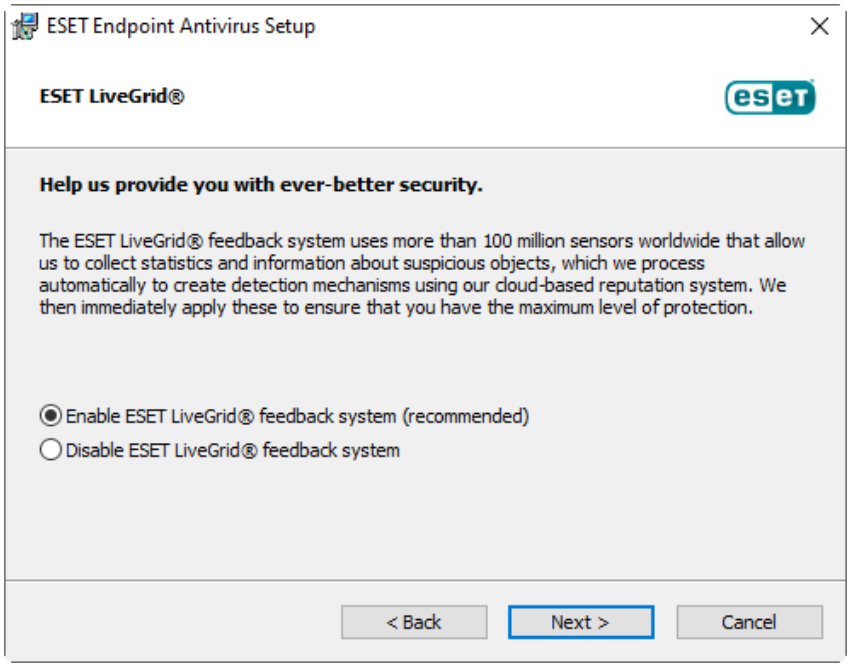



2. エンドユーザーライセンス契約を読み、[**ライセンス契約条項を受諾します**]をクリックし、エンドユーザーライセンス契約を承諾することを確認します。契約に同意したら[**次へ**]をクリックし、インストールを続行します。




3. ESET LiveGrid®フィードバックシステムの設定を選択しますESET LiveGrid®は、ESETが新しい侵入情報について継続的に即時通知を受け、保護が強化されることを保証します。これによって、ユーザーの保護を強化できますESETウイルスラボに新しい脅威を提出するようにし、そこでこれらが

解析および処理され、検出エンジンに追加されます。**詳細設定**をクリックして、追加のインストールパラメータを設定します。




4. 最後の手順では、[**インストール**]をクリックしてインストールを確認します。インストールが完了した後、ESET Endpoint Antivirusをアクティベーションするように指示されます。

# 詳細インストール (.msi)

詳細インストールでは、標準インストールでは使用できないインストールパラメータをカスタマイズできます。

1. インストール中に**インストールフォルダを変更**できますESET Endpoint Antivirusインストールの場所を選択します。既定では、プログラムは以下のディレクトリにインストールされます。

*C:\Program Files\ESET\ESET Security*

プログラムモジュールとデータの場所を指定できます。既定では、プログラムは以下のディレクトリにそれぞれインストールされます。

*C:\Program Files\ESET\ESET Security\Modules*
*C:\ProgramData\ESET\ESET Security*

場所を変更するには、[**参照**]をクリックします(推奨しません)。

2. インストールされる製品コンポーネントを選択します。コンピューターの検査と利用可能なすべての保護の設定を選択できます。アップデートミラーコンポーネントは、ネットワークの他のコンピューターをアップデートするために使用できます。リモート監視および管理(RMM)は、管理サービスプロバイダーによってアクセスできるローカルでインストールされたエージェントを使用して、ソフトウェアシステムを監視および制御するプロセスです。

3. [**インストール**]をクリックすると、インストールプロセスが始まります。

# 最小モジュールインストール

インストーラーのサイズに関連するネットワークトラフィックを削減し、リソースを節約するためにESETには最小モジュールインストーラーが付属しています。インストーラーには必須モジュールのみが含まれています。他のすべてのモジュールは、製品のアクティベーション後の最初のモジュールのアップデート中にダウンロードされます。主な利点は、大幅に小さいインストーラーを使用し、製品認証キーで製品をアクティベーションするときに、最新のアプリケーションモジュールのみをESET Endpoint Antivirusダウンロードすることです。

最小モジュールインストーラーには次のモジュールが含まれています。

- ローダー
- Direct Cloud通信
- 翻訳サポート
- 設定
- SSL

製品のアクティベーション後には、機能の初期化に関する通知が表示される**保護の初期化**状態が表示されます。

モジュールダウンロードの問題がある場合(プロキシ設定、ネットワークに未接続など)は、警告アプリケーションステータスの**注意が必要です**が表示されます。メインプログラムウィンドウで**アップデート > アップデートの確認**をクリックすると、処理が再開します。

何回か失敗すると、赤色のアプリケーションステータスの**保護設定が失敗しました**が表示されます。[再試行]をクリックすると、保護の設定が再開します。初期化処理が失敗し、モジュールをダウンロードできない場合は、完全なMSIインストーラーをダウンロードします。

クライアントコンピューターがインターネットに接続していない場合や、オフラインで、アップデートが必要な場合は、次の方法を使用して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ます。
- ミラーからのアップデート
- ミラーツールの使用

# コマンドラインインストール

コマンドラインを使用してローカルでESET Endpoint Antivirusをインストールするか、ESET PROTECTからクライアントタスクを使用してリモートでインストールできます。

## サポートされているパラメータ

### APPDIR= <path>

- path - 有効なディレクトリパス
- アプリケーションインストールディレクトリ。

### APPDATADIR= <path>

- path - 有効なディレクトリパス
- アプリケーションデータインストールディレクトリ。

### MODULEDIR= <path>

- path - 有効なディレクトリパス
- モジュールインストールディレクトリ。

### ADDLOCAL= <list>

- コンポーネントインストール – ローカルでインストールされる必須以外の機能のリスト。
- ESET .msiパッケージでの使用方法: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- **ADDLOCAL**プロパティの詳細については、http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspxを参照してください。

### ADDEXCLUDE= <list>

- ADDEXCLUDEリストは、インストールされないすべての機能名のカンマ区切りのリストであり、古いREMOVEに代わるものです。
- インストールしない機能を選択するときには、パス全体(すべてのサブ機能など)と関連する非表示の機能を明示的にリストに含める必要があります。
- ESET .msiパッケージでの使用方法: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

**ADDEXCLUDE**は**ADDLOCAL**とともに使用できません。

適切なコマンドラインスイッチで使用される**msiexec**バージョンについては、ドキュメントを参照してください。

## ルール

- **ADDLOCAL**リストは、インストールされるすべての機能名のカンマ区切り値リストです。
- インストールする機能を選択するときには、パス全体(すべての親機能)が明示的にリストに含まれる必要があります。
- 正しい使用方法については、追加ルールを参照してください。

# コンポーネントと機能

ADDLOCAL/ADDEXCLUDEパラメーターを使用したコンポーネントインストールは、ESET Endpoint Antivirusで動作しません。

機能は4つのカテゴリに分類されます。

- **必須** – 機能は常にインストールされます。
- **オプション** – 機能の選択を解除して、インストールされないようにすることができます。
- **非表示** – 他の機能が正常に動作するために必要な論理機能。
- **プレースホルダ** – 製品には影響がない機能。ただし、サブ機能とともにリストに含まれます。

ESET Endpoint Antivirusの機能セットは次とおりです。

| 説明 | 機能名 | 機能親 | 存在 |
|---|---|---|---|
| 基本プログラムコンポーネント | Computer | | プレースホルダ |
| 検出エンジン | Antivirus | Computer | 必須 |
| 検出エンジン/マルウェア検査 | Scan | Computer | 必須 |

| 説明 | 機能名 | 機能親 | 存在 |
| --- | --- | --- | --- |
| 検出エンジン/リアルタイムファイルシステム保護 | RealtimeProtection | Computer | 必須 |
| 検出エンジン/マルウェア検査/ドキュメント保護 | DocumentProtection | Antivirus | 任意 |
| デバイスコントロール | DeviceControl | Computer | 任意 |
| ネットワーク保護 | Network | | プレースホルダ |
| ネットワーク保護/ファイアウォール | Firewall | Network | 任意 |
| ネットワーク保護/ネットワーク攻撃保護/... | IdsAndBotnetProtection | Network | 任意 |
| 安全なブラウザー | OnlinePaymentProtection | WebAndEmail | 任意 |
| Webとメール | WebAndEmail | | プレースホルダ |
| Webとメール/プロトコルフィルタリング | ProtocolFiltering | WebAndEmail | 非表示 |
| Webとメール/Webアクセス保護 | WebAccessProtection | WebAndEmail | 任意 |
| Webとメール/電子メールクライアント保護 | EmailClientProtection | WebAndEmail | 任意 |
| Webとメール/電子メールクライアント保護/電子メールクライアント | MailPlugins | EmailClientProtection | 非表示 |
| Webとメール/電子メールクライアント保護/電子メールクライアント迷惑メール対策 | Antispam | EmailClientProtection | 任意 |
| Webとメール/Webコントロール | WebControl | WebAndEmail | 任意 |
| ツール/ESET RMM | Rmm | | 任意 |
| アップデート/プロファイル/アップデートミラー | UpdateMirror | | 任意 |
| ESET Inspectプラグイン | EnterpriseInspector | | 非表示 |

グループ機能セット:

| 説明 | 機能名 | 機能の存在 |
| --- | --- | --- |
| すべての必須機能 | _Base | 非表示 |
| すべての使用可能な機能 | ALL | 非表示 |

### 追加ルール

- **WebAndEmail**機能がインストールに選択されている場合、非表示の**ProtocolFiltering**機能をリストに含める必要があります。
- すべての機能の名前は大文字と小文字を区別します。たとえばUpdateMirrorはUPDATEMIRRORと同じではありません。

## 構成プロパティのリスト

| プロパティ | 値 | 機能 |
| --- | --- | --- |
| CFG_POTENTIALLYUNWANTED_ENABLED= | 0 – 無効<br>1 – 有効 | PUA検出 |
| CFG_LIVEGRID_ENABLED= | 以下を参照 | 以下のLiveGridプロパティを参照 |
| FIRSTSCAN_ENABLE= | 0 – 無効<br>1 – 有効 | インストール後にコンピューターの検査をスケジュールして実行 |
| CFG_PROXY_ENABLED= | 0 – 無効<br>1 – 有効 | プロキシサーバーの設定 |
| CFG_PROXY_ADDRESS= | <ip> | プロキシサーバのIPアドレス |
| CFG_PROXY_PORT= | <port> | プロキシサーバーポート番号 |
| CFG_PROXY_USERNAME= | <username> | 認証のユーザー名。 |
| CFG_PROXY_PASSWORD= | <password> | 認証のパスワード。 |
| ACTIVATION_DATA= | 以下を参照 | 製品のアクティベーション、製品認証キー、またはオフラインライセンスファイル |
| ACTIVATION_DLG_SUPPRESS= | 0 – 無効<br>1 – 有効 | 「1」に設定すると、製品のアクティベーションダイアログが最初の起動後に表示されません |
| ADMINCFG= | <path> | エクスポートされたXML構成へのパス<br>(既定値*cfg.xml*) |

## LiveGrid®プロパティ

ESET Endpoint AntivirusとCFG_LIVEGRID_ENABLEDをインストールすると、インストール後の製品の動作は次のようになります。

| 機能 | CFG_LIVEGRID_ENABLED=0 | CFG_LIVEGRID_ENABLED=1 |
| --- | --- | --- |
| **ESET LiveGrid®レピュテーションシステム** | オン | オン |
| **ESET LiveGrid®フィードバックシステム** | オフ | オン |
| **匿名で統計情報を送付する** | オフ | オン |

## ACTIVATION_DATAプロパティ

| 書式 | 検査方法 |
| --- | --- |
| ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE | ESET製品認証キーを使用したアクティベーション(インターネット接続が必要) |
| ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf | 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 |

## 言語プロパティ

ESET Endpoint Antivirus言語(両方のプロパティを指定する必要があります)

| プロパティ | 値 |
| --- | --- |
| PRODUCT_LANG= | LCID10進数(ロケールID)例: 1033は英語(米国)。言語コードの一覧を参照してください。 |

| プロパティ | 値 |
| --- | --- |
| PRODUCT_LANG_CODE= | 小文字のLCID文字列(言語カルチャー名)。例: en-usは英語 – 米国。言語コードの一覧を参照してください。 |

### 再起動プロパティ

インストール後にコンピューターを再起動するには、次のパラメーターを指定します。

| プロパティ | 値 | 機能 |
| --- | --- | --- |
| REBOOT_WHEN_NEEDED= | 0 – 無効<br>1 – 有効 | 有効にすると、インストール後に、コンピューターが再起動します。 |
| REBOOT_CANCELABLE= | 0 – 無効<br>1 – 有効 | 有効にすると、ユーザーはコンピューターの再起動をキャンセルできます。 |
| REBOOT_POSTPONE= | 値(秒) | ユーザーがコンピューターの再起動を延期する最大時間(秒)。 |

REBOOT_CANCELABLEが有効になっているREBOOT_POSTPONE場合にのみREBOOT_WHEN_NEEDED使用できます。

## コマンドラインインストールの例

インストールを実行する前に、エンドユーザーライセンス契約を読んで、管理者権限があることを確認してください。

**NetworkProtection**セクションをインストールから除外する(すべての子機能を指定する必要があります):
```
msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection
```

インストール後にESET Endpoint Antivirusを自動的に設定する場合は、インストールコマンド内で基本設定パラメーターを指定できます。
ESET LiveGrid®を有効にしてESET Endpoint Antivirusをインストールする:
```
msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1
```

既定以外のアプリケーションインストールディレクトリにインストールします。
```
msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\
```

ESET製品認証キーを使用してESET Endpoint Antivirusをインストールしてアクティベーションします。
```
msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE
```

詳細ロギング(トラブルシューティングで有用)でサイレントインストール、必須のコンポーネントでのみRMM:
```
msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm
```

指定された言語でサイレント完全インストールを強制する。
```
msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us
```

## インストール後のコマンドラインオプション

- ESETCMD –.xml設定ファイルをインポートするか、セキュリティ機能をオン/オフにします
- コマンドラインスキャナー – コマンドラインからコンピューターの検査を実行します

# GPOまたはSCCMを使用した展開

クライアントワークステーションに直接ESET Endpoint Antivirusをインストールする他に、グループポリシーオブジェクト(GPO)ソフトウェアセンター構成マネージャ(SCCM)Symantec AltirisまたはPuppetなどの管理ツールを使用してインストールすることもできます。

## 管理対象(推奨)

管理されたコンピューターの場合、最初にESET Managementエージェントをインストールしてから、ESET PROTECT経由でESET Endpoint Antivirusを展開します。ESET PROTECTはネットワークにインストールする必要があります。

1. ESET Managementエージェント向けのスタンドアロンインストーラーをダウンロードします。
2. GPO/SCCMリモート展開スクリプトを準備します。
3. GPOまたはSCCMを使用して、ESET Managementエージェントを展開します。
4. クライアントコンピューターがESET PROTECTに追加されたことを確認します。
5. ESET Endpoint Antivirusをコンピューターに展開してアクティベーションします。

次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
- SCCMまたはGPO経由でESET Management Agentを展開する
- グループポリシーオブジェクト(GPO)を使用してESET Management Agentを展開する

---

## 管理対象外

管理対象外のコンピューターの場合、直接クライアントワークステーションにESET Endpoint Antivirusを展開できます。この方法では、ワークステーションのすべてのESETエンドポイント製品のポリシーを監視して施行することができないため、推奨されていません。

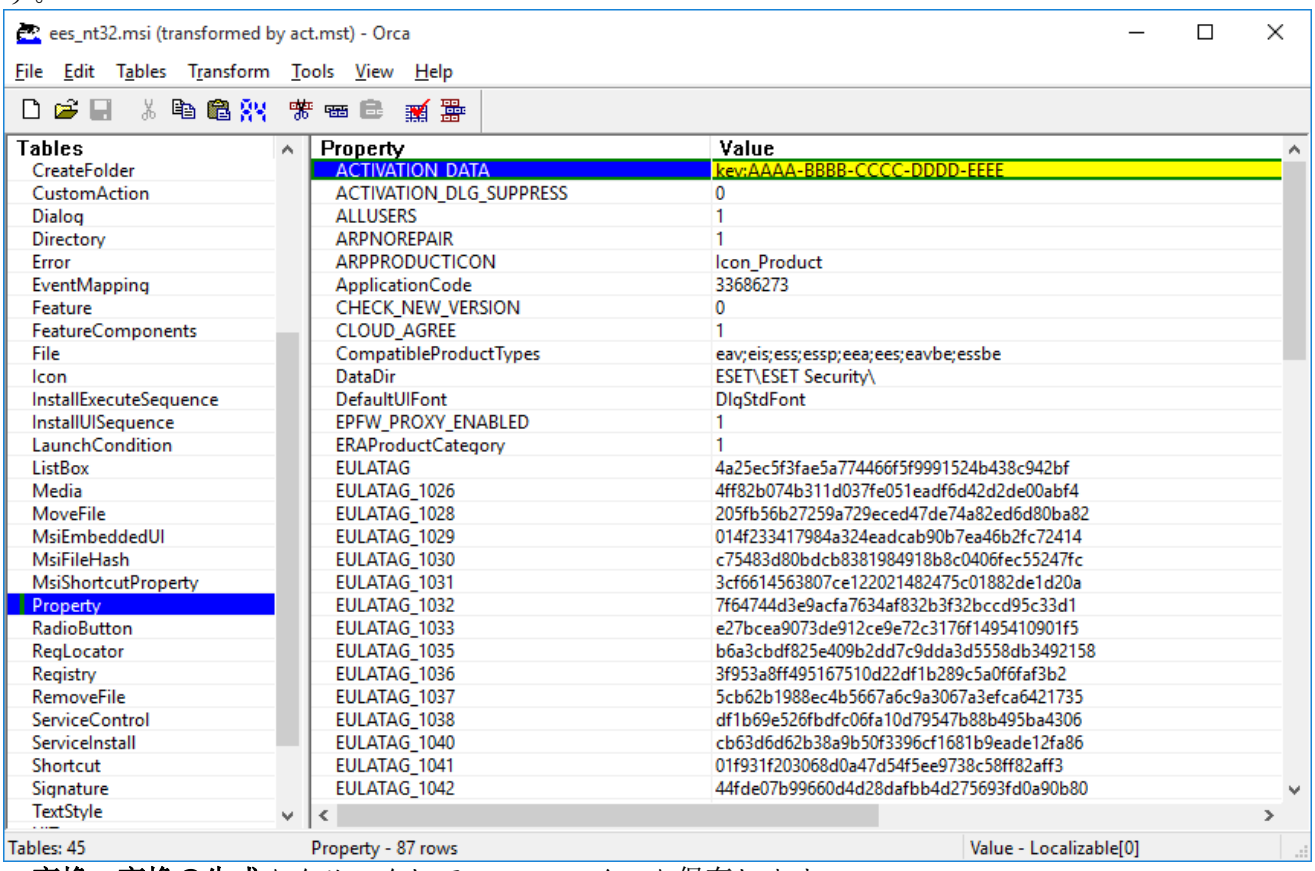
既定では、ESET Endpoint Antivirusはインストール後にアクティベーションされないため、機能しません。

### オプション1(ソフトウェアインストール)

1. ESET Endpoint Antivirus向けの.msiインストーラーをダウンロードします。
2. .msiファイルから.mst変換パッケージを作成(例: Orca.msiエディターを使用)して、製品のアクティベーションプロパティ(コマンドラインインストールの`ACTIVATION_DATA`を参照)を含めます。

Orcaで. mstを作成する手順を表示

1. Orcaを開く
2. **File > Open**をクリックして.msiインストーラーを読み込みます。
3. **Transform > New Transform**をクリックします。
4. **Tables**セクションで**Property**をクリックしてから、メニューで**Tables > Add row**をクリックします。
5. **Add Row**ウィンドウで、**Property**にACTIVATION_DATAを入力し、**Value**にライセンス情報を入力します。




6. **変換 > 変換の生成**をクリックして.mstファイルを保存します。

1. オプション：カスタマイズされたESET Endpoint Antivirus.xml設定ファイル（たとえばRMMを有効にするか、プロキシサーバー設定を設定する）をインポートするには.msiインストーラーと同じ場所にcfg.xmlファイルを置きます。
2. GPO（ソフトウェアインストール経由）またはSCCMを使用して.msiインストーラーと.mstファイルをリモートで展開します。

## オプション2（スケジュールされたタスクを使用）

1. ESET Endpoint Antivirus向けの.msiインストーラーをダウンロードします
2. コマンドラインインストールスクリプトを準備して、製品のアクティベーションプロパティを含めます（ACTIVATION_DATAを参照）。
3. すべてのワークステーション.msiインストーラーと、.cmdスクリプトにネットワークでアクセスできるようにします。
4. オプション：カスタマイズされたESET Endpoint Antivirus.xml設定ファイル（たとえばRMMを有効にするか、プロキシサーバー設定を設定する）をインポートするには.msiインストーラーと同じ場所にcfg.xmlファイルを置きます。
5. GPOまたはSCCMを使用して、準備されたコマンドラインインストールスクリプトを適用します。
    - GPOの場合、グループポリシー設定 > グループポリシースケジュールタスク > 即時タスクを使用します。

ESET PROTECTを使用して□ESETエンドポイント製品をリモート管理しない場合は、ESET Endpoint AntivirusにRMM向けのESETプラグインが含まれます。これによって、管理サービスプロバイダーがアクセスできる、ローカルインストールされたエージェントを使用して、ソフトウェアシステムを監視および制御できます。詳細情報

# 最新バージョンへのアップグレード

プログラムモジュールの自動更新では解決できない問題の修正や改良を行うために□ESET Endpoint Antivirusの新バージョンが提供されています。

最新バージョンへのアップグレードには、いくつかの方法があります。

1. ESET PROTECT, またはESET PROTECT Cloudを使用して自動的に実行します。
2. 自動的にアップグレードします。GPOまたはSCCMを使用します。
3. 自動的に、プログラムアップデートを使用します。
   プログラムのアップデートはすべてのユーザーに配布されますが、システム設定によっては影響を受ける可能性があります。従って、考えられるどのようなシステム設定でも確実に動作するように、長期間のテストを経て発行されます。リリース直後の新バージョンにアップグレードする必要がある場合、以下の方法の1つを使用します。
   **詳細設定** > アップデート > **プロファイル** > **製品のアップデート**で**アップデートモード**を有効にしたことを確認してください。
4. 手動で、最新バージョンをダウンロードおよびインストールし、以前のバージョンに上書きインストールします。

## 推奨アップグレードシナリオ

### ESET 製品をリモートで管理する、管理したい

10台を超えるESET Endpoint製品を管理する場合は、ESET PROTECT□ESET PROTECT Cloudを使用してアップグレードを処理することを検討してください。次のドキュメントを参照してください。

- ESET PROTECT | クライアントタスクを使用してESETソフトウェアをアップグレードする
- ESET PROTECT | 最大250のWindows ESET エンドポイント製品を管理する小規模から中規模の企業向けガイド
- ESET PROTECT Cloudの概要

### クライアントコンピューターで手動によりアップグレードする

個別のクライアントワークステーションで手動によりESET Endpoint Antivirusをアップグレードする

1. 現在インストールされているバージョンがサポートされていることを確認します。
2. オペレーティングシステムがサポートされていることを確認します。

2. 最新バージョンをダウンロードし、以前のバージョンにインストールします。

「サポート終了」サポートレベルのバージョンでは、前のバージョンの上に最新バージョンを正常にインストールされることは保証されません□ESET Endpoint Antivirusのサポートレベルを確認するには、サポート終了ポリシーを参照してください。
サポートされていないバージョンからアップグレードするには、最初にESET Endpoint Antivirusをアンインストールします。クライアントワークステーションでのESETEndpointAntivirusのアップグレードの詳細については、次のESETナレッジベース記事をお読みください。

# レガシー製品自動アップグレード

ESET製品バージョンはサポートされておらず、製品は最新バージョンにアップグレードされました。

一般的なインストールの問題

ESET製品の新しいバージョンごとに、多くのバグ修正と改良が行われます。ESET製品の有効なライセンスをお持ちのお客様は、同じ製品の最新バージョンに無料でアップグレードできます。

インストールを完了するには:

1. **同意して続行**をクリックして、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を確認します。エンドユーザーライセンス契約に同意しない場合は、**アンインストール**をクリックします。前のバージョンに戻すことはできません。
2. **すべて許可して続行**をクリックして、ESET LiveGrid®フィードバックシステムを許可するか、参加しない場合は**続行**をクリックします。
3. 製品認証キーを使用して新しいESET製品をアクティベーションすると、ホームページが表示されます。ライセンス情報が見つからない場合は、新しい試用ライセンスで続行します。前の製品で使用されているライセンスが無効な場合は、ESET製品をアクティベーションしてください。
4. インストールを完了するには、デバイスの再起動が必要です。

# セキュリティと安定性のアップデート

悪意のあるコードに対する完全な保護を維持するための基本的な作業としてESET Endpoint Antivirusのアップデートが必要です。各新しいバージョンのESET Endpoint Antivirusには、多数の改良やバグ修正が導入されていますESET Endpoint Antivirusを定期的にアップデートして、セキュリティの脆弱性や脅威を防止することを強くお勧めしますESET Endpoint Antivirusは、他のESET製品のように製品ライフサイクルの特定の段階に適合します。

詳細については次の項目をお読みください。
サポート終了ポリシー(ビジネス製品)
製品のアップデート
セキュリティと安定性のホットフィックス
ESET Endpoint Antivirusの変更の詳細については、次のESETナレッジベース記事をお読みください。

自動アップデートは、製品の最大限のセキュリティと安定性を保証します。セキュリティアップデートと安定性アップデートを無効にすることはできません。

# 製品のアクティベーション

インストール完了後、製品のアクティベーションが求められます。

製品のアクティベーションには、いくつかの方法があります。[アクティベーション]ウィンドウ内の特定のアクティベーションシナリオを使用できるかどうかは、国、および配布方法(ESET Webページ、インストーラータイプ .msi または .exe など)によって異なります。

プログラムのメインウィンドウ > **ヘルプとサポート** > **製品のアクティベーション**または**保護の状態** > **製品のアクティベーション**でESET Endpoint Antivirusをアクティベーションできます。

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

- **購入した製品認証キーを使用** - XXXX-XXXX-XXXX-XXXX-XXXXの形式の一意の文字列。ライセンス所有者を識別し、ライセンスをアクティベーションするために使用されます。
- **ESET HUB** – 作成する必要があるESET HUBアカウントESET HUBは、ESET PROTECT統合セキュリティプラットフォームへの中央ゲートウェイです。すべてのESETプラットフォームモジュールのIDサブスクリプション、およびユーザー管理を一元的に行うことができます。このオプションを使用して、古いライセンス管理ツール(ESET Business AccountまたはESET MSP Administrator)でもESET Endpoint Antivirusをアクティベーションできます。
- **オフラインライセンス** – 自動生成されたファイルESET製品に転送され、ライセンス情報を提供します。ライセンスによってオフラインライセンスファイル(.lf)をダウンロードできる場合は、このファイルを使用してオフラインアクティベーションを実行できます。オフラインライセンス数は、使用可能な合計ライセンス数から減算されます。オフラインファイルの生成の詳細については、ESET Business Accountユーザーガイドを参照してください。

コンピュータが管理対象ネットワークのメンバーで、管理者がESETPROTECT経由でリモートアクティベーションを実行する場合は、**[後からアクティベーション]**をクリックします。後からこのクライアントをアクティベートする場合は、このオプションを使用することもできます。

ユーザー名とパスワードが前のESET製品のアクティベーションで使用されている場合は、レガシー資格情報を製品認証キーに変換します。

製品ライセンスは、プログラムのメインウィンドウ**>ヘルプとサポート>ライセンスの変更**でいつでも変更できますESETサポートへのライセンスを識別するための公開ライセンスIDが表示されます。

> ESET PROTECTは、管理者が使用可能にしたライセンスを使用してバックグラウンドでクライアントコンピュータをアクティベーションできます。手順については、ESET PROTECTオンラインヘルプを参照してください。

製品のアクティベーションが失敗した場合

# アクティベーション中の製品認証キーの入力

自動アップデートはセキュリティのために重要ですESET Endpoint Antivirusは、**ライセンスキー**を使用してアクティベーションが完了した後にのみアップデートを受信します。

インストール後に製品認証キーを入力していない場合は、製品がアクティベーションされません。メインプログラムウィンドウでライセンスを変更できます。このためには、**ヘルプとサポート>ライセンスのアクティベーション**をクリックし、受け取ったESETセキュリティ製品のライセンスデータを[製品のアクティベーション]ウィンドウに入力します。

**[製品認証キー]**は、書かれている通りに入力する必要があります。

- ライセンスキーは、XXXX-XXXX-XXXX-XXXX-XXXXの形式の一意の文字列です。ライセンス所有者を識別し、ライセンスをアクティベーションするために使用されます。

正確性を保つためにも、登録メールからコピーしてペーストすることを強くお勧めします。

# ESET HUBアカウント

ESET HUBは、ESET PROTECT統合セキュリティプラットフォームへの中央ゲートウェイです。すべてのESETプラットフォームモジュールのIDサブスクリプション、およびユーザー管理を一元的に行うことができますESET HUBを使用すると、次のことができます。

- セキュリティサブスクリプションの概要を取得する
- サブスクライブしたサービスの使用状況とステータスを確認する
- 各ESETプラットフォームへの細かいアクセスを割り当て、制御する
- すべてのリンクされた、アクセス可能なESETプラットフォームに対するシングルサインイン

このアクティベーションオプションを使用して、古いライセンス管理ツール(ESET Business Accountまたは ESET MSP Administrator)でもESET Endpoint Antivirusをアクティベーションできます。

ESET HUBアカウントを作成し、**メールアドレス**と**パスワード**でログインできます。

パスワードを忘れた場合は、**パスワードを忘れた場合**をクリックするとESET HUBに移動します。電子メールアドレスを入力し、**サインイン**をクリックして確認します。次に、パスワードリセット手順が記載されたメッセージが届きます。

# レガシーライセンス資格情報を使用してESETエンドポイント製品をアクティベーションする方法

ユーザー名とパスワードがあり、ライセンスキーを受け取りたい場合は、ESET Business Accountポータルにアクセスし、認証情報を新しいライセンスキーに変換できます。

# アクティベーションに失敗

ESET Endpoint Antivirusのアクティベーションが成功しない場合、最も一般的なシナリオは次のとおりです。

- 製品認証キーが既に使用されている
- 無効な製品認証キーを入力しました。
- アクティベーションフォームの情報が不足しているか無効です。
- アクティベーションサーバーとの通信に失敗しました。
- ESETアクティベーションサーバーへの接続がないか無効です

正しい製品認証キーを入力したか、オフラインライセンスを添付したことを確認して、アクティベーションを再試行してください。

アクティベーションできない場合は、ウェルカムパッケージがアクティベーションとライセンスに関する一般的な質問、エラー、問題について説明します(英語および複数の他の言語で提供されています)。

- ESET製品のアクティベーションのトラブルシューティングを開始

# 登録

登録フォームのフィールドを入力し、[**続行**]をクリックして、ライセンスを登録してください。括弧で必須に設定されているフィールドは必ず入力する必要があります。この情報はESETライセンスに関する問題でだけ使用されます。

# アクティベーションの進行状況

ESET Endpoint Antivirusをアクティベーションしています。しばらくお待ちください。

# アクティベーションは正常に実行されました

アクティベーションは正常に実行されESET Endpoint Antivirusが有効になりました。これでESET Endpoint Antivirusは定期アップデートを受信して、最新の脅威を特定し、コンピュータを安全に保ち続けることができます。製品のアクティベーションを完了するには、[**完了**]をクリックします。

# 一般的なインストールの問題

インストール中に問題が発生した場合、インストールウィザードは、可能な場合に、問題を解決するトラブルシューティングツールを提供します。

**トラブルシューティングツールの実行**をクリックすると、トラブルシューティングツールを開始します。トラブルシューティングツールが完了したら、推奨される解決策に従います。

問題が解決しない場合は、一般的なインストールエラーと解決策の一覧を参照してください。

# 初心者向けガイド

この章ではESET Endpoint Antivirusの概要とその基本設定について説明します。

# システムトレイアイコン

最も重要な設定オプションと機能の一部は、システムトレイアイコンを右クリックすると使用できます。

> システムトレイ(Windows通知領域)アイコンメニューにアクセスするには、ユーザーインターフェース要素の起動モードが完全に設定されていることを確認してください。

**保護を一時停止する** – ファイルWebおよびメール通信を制御することによって攻撃から保護する、検出エンジンを無効にするための確認ダイアログボックスを表示します。**間隔**ドロップダウンメニューでは、保護を無効にする時間を指定できます。

**詳細設定** - ESET Endpoint Antivirus詳細設定を開きますプログラムのメインウィンドウから詳細設定を開くには、キーボードのF5キーを押すか、**設定 > 詳細設定**をクリックします。

ログファイル – ログファイル には、発生した重要なプログラムイベントに関する情報が格納され、検出の概要が表示されます。

**ESET Endpoint Antivirus**を開く – トレイ(Windows通知領域)アイコンからESET Endpoint Antivirusメインプログラムウィンドウを開きます。

**ウィンドウレイアウトのリセット** - ESET Endpoint Antivirusのウィンドウを既定のサイズと画面上の位置にリセットします。

**色モード** – グラフィカルユーザーインタフェースの色を変更できるユーザーインターフェース設定を開きます。

**アップデートのチェック...** – モジュールまたは製品のアップデートを開始し、保護を保証しますESET Endpoint Antivirusは、1日に数回自動的にアップデートを確認します。

バージョン情報 – システム情報、インストールされているESET Endpoint Antivirusのバージョンに関する詳細、インストールされているプログラムモジュール、オペレーティングシステムおよびシステムリソースについての情報が表示されます。

# ショートカットキー

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

| キーボードショートカット | アクション |
|---|---|
| F1 | ヘルプページを開きます |
| F5 | 詳細設定を開きます |
| 上矢印/下矢印 | ドロップダウンメニュー項目のナビゲーション |
| TAB | ウィンドウの次のGUI要素に移動 |
| Shift+TAB | ウィンドウの前のGUI要素に移動 |
| ESC | アクティブなダイアログウィンドウを閉じます |
| Ctrl+U | ESETライセンスとコンピューターの情報を表示します(テクニカルサポート詳細) |
| Ctrl+R | 製品ウィンドウを既定のサイズ・既定の位置に戻します |
| ALT +左矢印 | 戻る |
| ALT +右矢印 | 進む |
| ALT+Home | ホームに戻る |

マウスボタンを使用して前後に移動することもできます。

# プロファイル

プロファイルマネージャは、ESETEndpointAntivirus内の2ヶ所、つまり**オンデマンド検査**セクションと**アップデート**セクションで使用します。

## コンピュータの検査

ESET Endpoint Antivirusには、次の4つの定義済み検査プロファイルがあります。

- **スマート検査**: これは既定の詳細検査プロファイルです。スマート検査プロファイルは、スマート最適化技術を使用しており、前回の検査で感染していないことが判明したファイルのうち、その検査以降変更されていないファイルを除外します。これにより、検査時間を短縮でき、システムセキュリティへの影響を最小限に抑えることができます。
- **コンテキストメニューの検査**: コンテキストメニューから、任意のファイルのオンデマンド検査を開始できます。コンテキストメニューの検査プロファイルでは、この方法で検査をトリガーするときに使用される検査構成を定義できます。
- **詳細検査**: 既定では、詳細検査プロファイルはスマート最適化を使用しないため、このプロファイルを使用して検査から除外されるファイルはありません。
- **コンピューターの検査**：これは標準コンピューターの検査で使用される既定のプロファイルです。

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

新しいプロファイルを作成するには、詳細設定 > **検出エンジン** > **マルウェア検査** > **オンデマンド検査** > **プロファイルのリスト** > **編集**を開きます。**オンデマンド検査**ウィンドウには、既存の検査プロファイルと、新しいプロパティを作成するためのオプションを表示する**選択されたプロファイル**ドロップダウンメニューがあります。各自のニーズに合った検査プロファイルを作成するための参考情報として、ThreatSenseにある検査設定の各パラメーターの説明を参照してください。

既にある**コンピューターの検査**の設定は部分的にしか自分のニーズを満たさないので、独自の検査プロファイルを作成する必要があると仮定します。**プロファイルマネージャ**ウィンドウで新しいプロファイルの名前を入力し、[追加]。をクリックします **選択されたプロファイル**ドロップダウンメニューから新しいプロファイルを選択し、要件に合わせて残りのパラメータを調整し、**[OK]**をクリックして新しいプロファイルを保存します。

## アップデート

アップデート設定のプロファイルエディターを使用すると、新しいプロファイルを作成できます。ユーザー独自のカスタムプロファイル(つまり、既定の**マイプロファイル**以外)を作成して使用するのは、コンピュータからアップデートサーバーへの接続方法が複数ある場合だけにしてください。

例えば、通常はローカルネットワーク内のローカルサーバー、つまりミラーに接続しますが、出張などでこのローカルネットワークに接続していないときには、更新ファイルをESETのアップデートサーバから直接ダウンロードします。これによりノートPCは、2つのプロファイルを使用することができます。1つ目のプロファイルではローカルサーバに接続し、2つ目ではESETのサーバに接続します。1つ目のプロファイルではローカルサーバに接続し、2つ目ではESETのサーバに接続します。プロファイルを設定したら、**ツール** > **スケジューラ**に移動し、アップデートタスクのパラメーターを編集します。一方のプロファイルをプライマリ、他方をセカンダリに指定します。

**編集するプロファイルを選択** – 現在使用されている更新プロファイル。変更するには、ドロップダウンメニューからプロファイルを選択します。

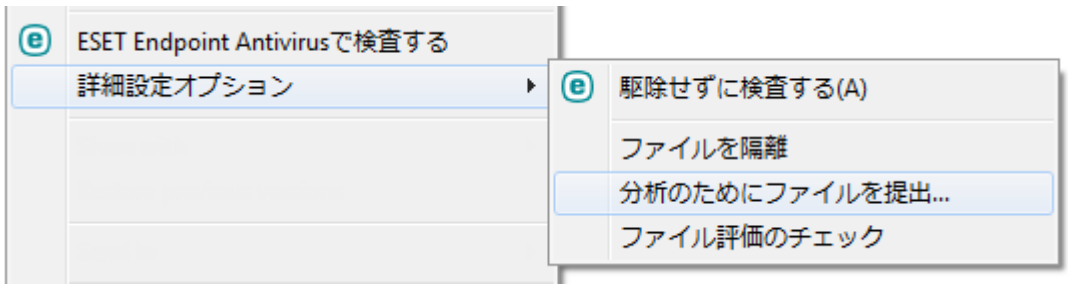
**プロファイルのリスト** – 新しいアップデートプロファイルを作成するか、既存のアップデートプロファイルを削除します。

# コンテキストメニュー

オブジェクト(ファイル)を右クリックすると、コンテキストメニューが表示されます。このメニューには、オブジェクトに対して実行できるすべてのアクションが一覧表示されます。

ESET Endpoint Antivirusのコントロール要素をコンテキストメニューに統合できます。詳細設定 > **ユーザーインターフェース** > **ユーザーインターフェース要素**に、この機能に対する設定オプションがあります。

**コンテキストメニューに統合する** - ESET Endpoint Antivirusのコントロール要素をコンテキストメニューに統合します。

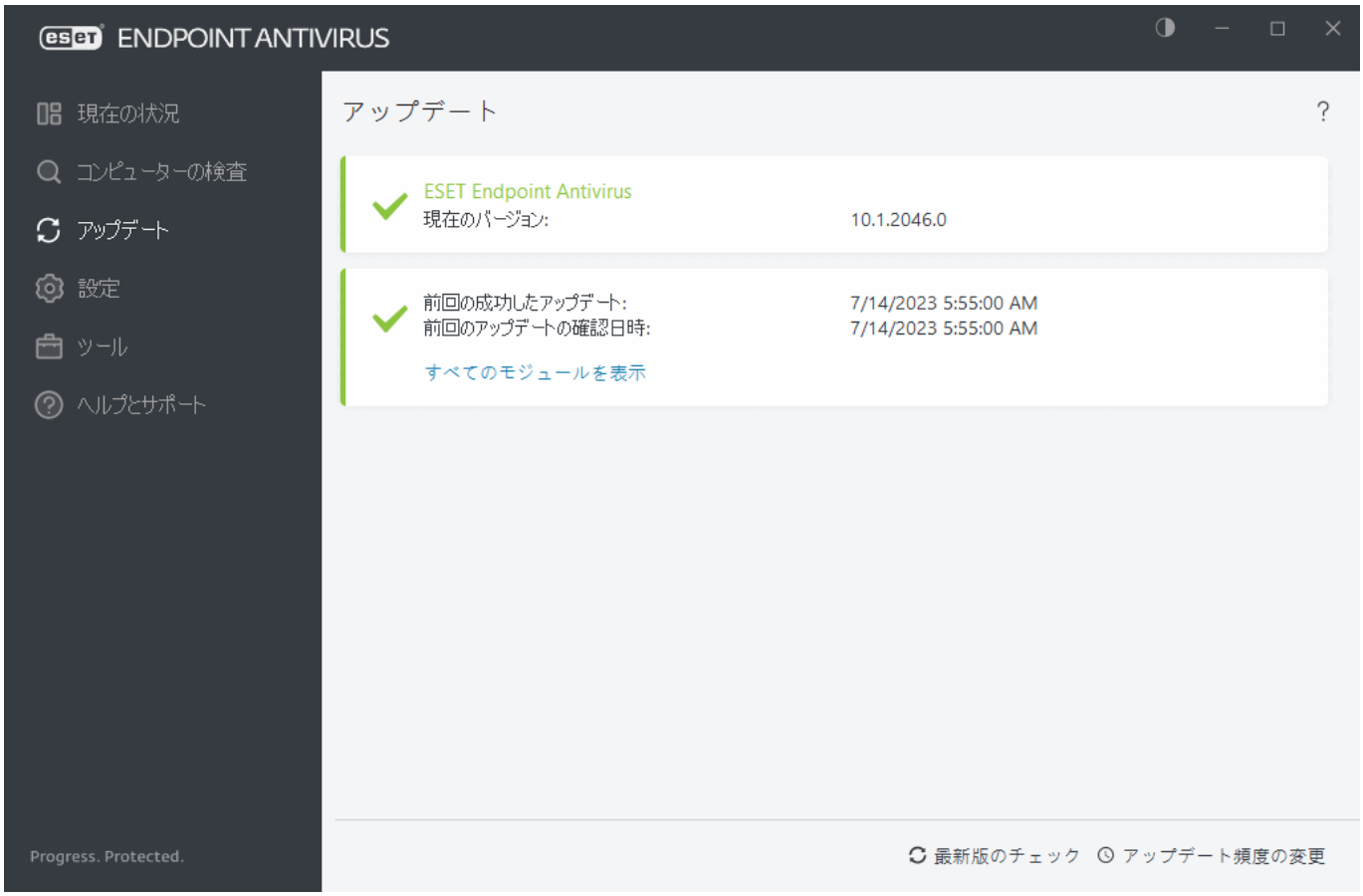


# アップデートの設定

コンピューターのセキュリティを最大化するためにはESET Endpoint Antivirusを定期的にアップデートするのが最善の方法です。[アップデート]モジュール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ようにします。

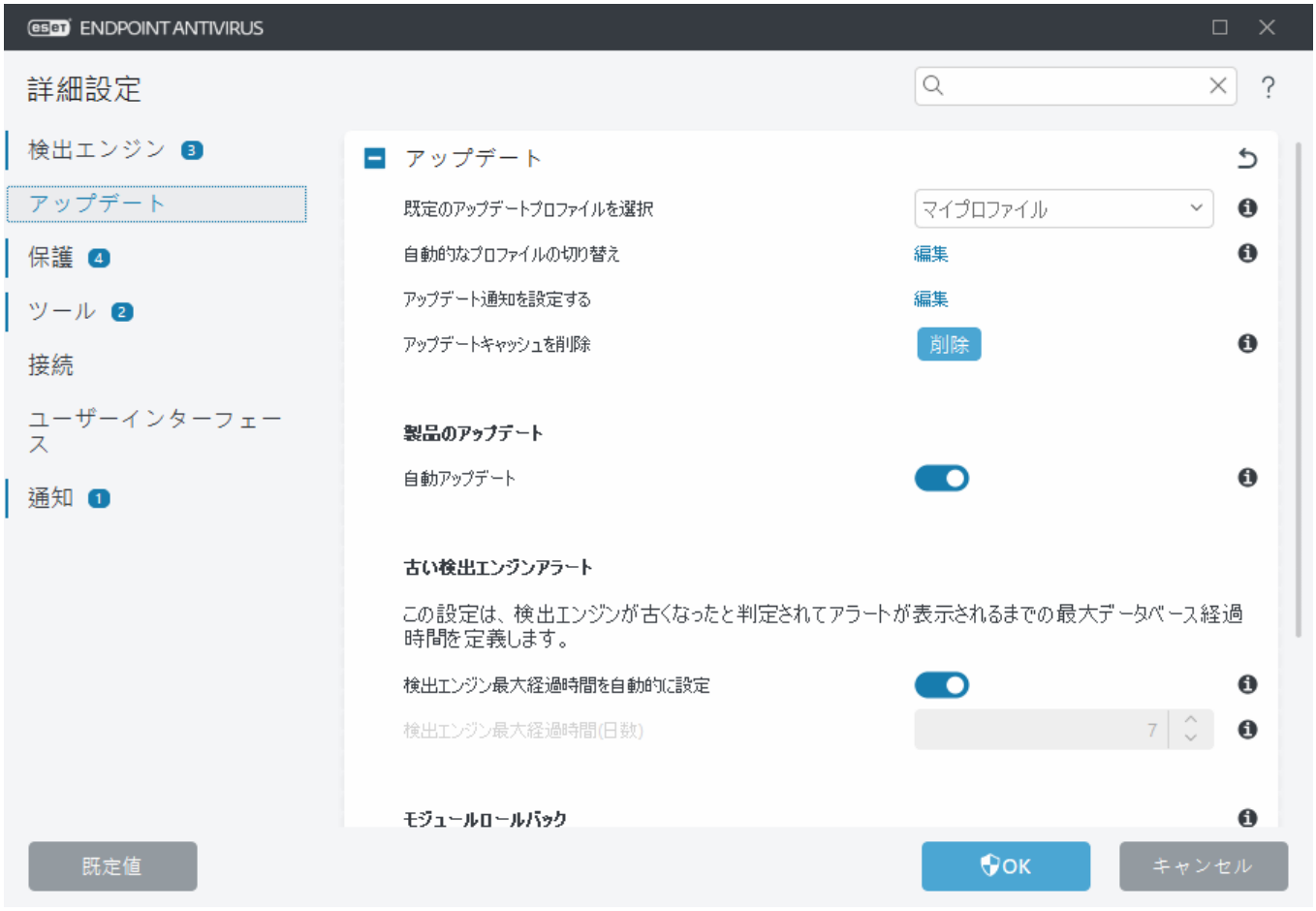
メインプログラムウィンドウの[**アップデート**]をクリックすると、前回成功したアップデートの日時、アップデートが必要かどうかなど、現在のアップデートの状態を表示できます。

自動アップデートの他に、**最新版のチェック**をクリックして手動アップデートをトリガーできます。




詳細設定 > **アップデート**には、アップデートモード、プロキシサーバーアクセスLAN接続などのその他のアップデートオプションが含まれています。

アップデートで問題が発生した場合は、**削除**をクリックして、アップデートキャッシュをクリアします。それでもプログラムモジュールを更新できない場合は、「モジュールのアップデートが失敗しました」メッセージのトラブルシューティングを参照してください。




詳細設定 > **アップデート** > **プロファイル** > **アップデート** > **モジュールのアップデート**の**自動選択**オプションは、既定で有効になっています。ESETアップデートサーバーを使用してアップデートを受信する場合、これをそのままにすることをお勧めします。

最適な機能を実現するには、プログラムを自動的にアップデートする必要があります。**ヘルプとサポート** > **製品のアクティベーション**から正しい製品認証キーを入力した場合にのみ、自動アップデートが可能です。インストール後にライセンスキーを入力していない場合は、いつでも入力できます。アクティベーションの詳細については、ESET Endpoint Antivirusをアクティベーションする方法を参照してください。

# ネットワーク保護の設定

既定では、ESET Endpoint Antivirusは、新しいネットワーク接続が検出されたときのWindows設定を使用します。新しいネットワークが検出されたときにダイアログウィンドウを表示するには、ネットワーク保護プロファイルの割り当てを**確認**に変更します。コンピューターが新しいネットワークに接続されるたびに、ネットワーク保護設定がが表示されます。


次のネットワーク接続プロファイルから選択できます。

**自動** - ESET Endpoint Antivirusは各プロファイルに設定されたアクティベートユーザーに基づいて、プロファイルを自動的に選択します。

**プライベート** – 信頼できるネットワーク(自宅または職場ネットワーク)の場合。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)。安全なローカルネットワークにアクセスするときにはこの設定を使用することをお勧めします。このプロファイルは、Windowsでドメインまたはプライベートネットワークとして設定されている場合、ネットワーク接続に自動的に割り当てられます。

**パブリック** – 信頼できないネットワーク(パブリックネットワーク)の場合。システムのファイルとフォルダーはネットワーク上の他のユーザーと共有したり、表示したりできません。システムリソースの共有が無効になります。無線ネットワークにアクセスするときにはこの設定を使用することをお勧めします。このプロファイルは、Windowsでドメインまたはプライベートネットワークとして設定されていないネットワーク接続に自動的に割り当てられます。

**ユーザー定義プロファイル** – ドロップダウンメニューから作成したプロファイルを選択できます。このオプションは、1つ以上のカスタムプロファイルを作成した場合にのみ使用できます。

ネットワーク設定が正しくないと、コンピューターにセキュリティ上のリスクが生じることがあります。

# ブロックされたハッシュ

環境でESET Inspectを使用すると、管理者はハッシュに基づいて指定された実行可能ファイルへのアクセスをブロックできます。管理者が実行可能ファイルへのアクセスをブロックし、ユーザーがその実行可能ファイルにアクセスしようとするとESET Endpoint Antivirusによって次の通知が表示されます。

**ファイルアクセスがブロックされました** – アプリケーション(アプリケーションの名前が表示されます)が、管理者によって許可されていないファイルにアクセスしようとしました。

管理者が通知で指定されたアプリケーションへのアクセスを許可する場合は、ESET Inspectオンラインヘルプのブロックされたハッシュを参照してください。ユーザーがアプリケーションの動作を変更する場合は、管理者に問い合わせてください。

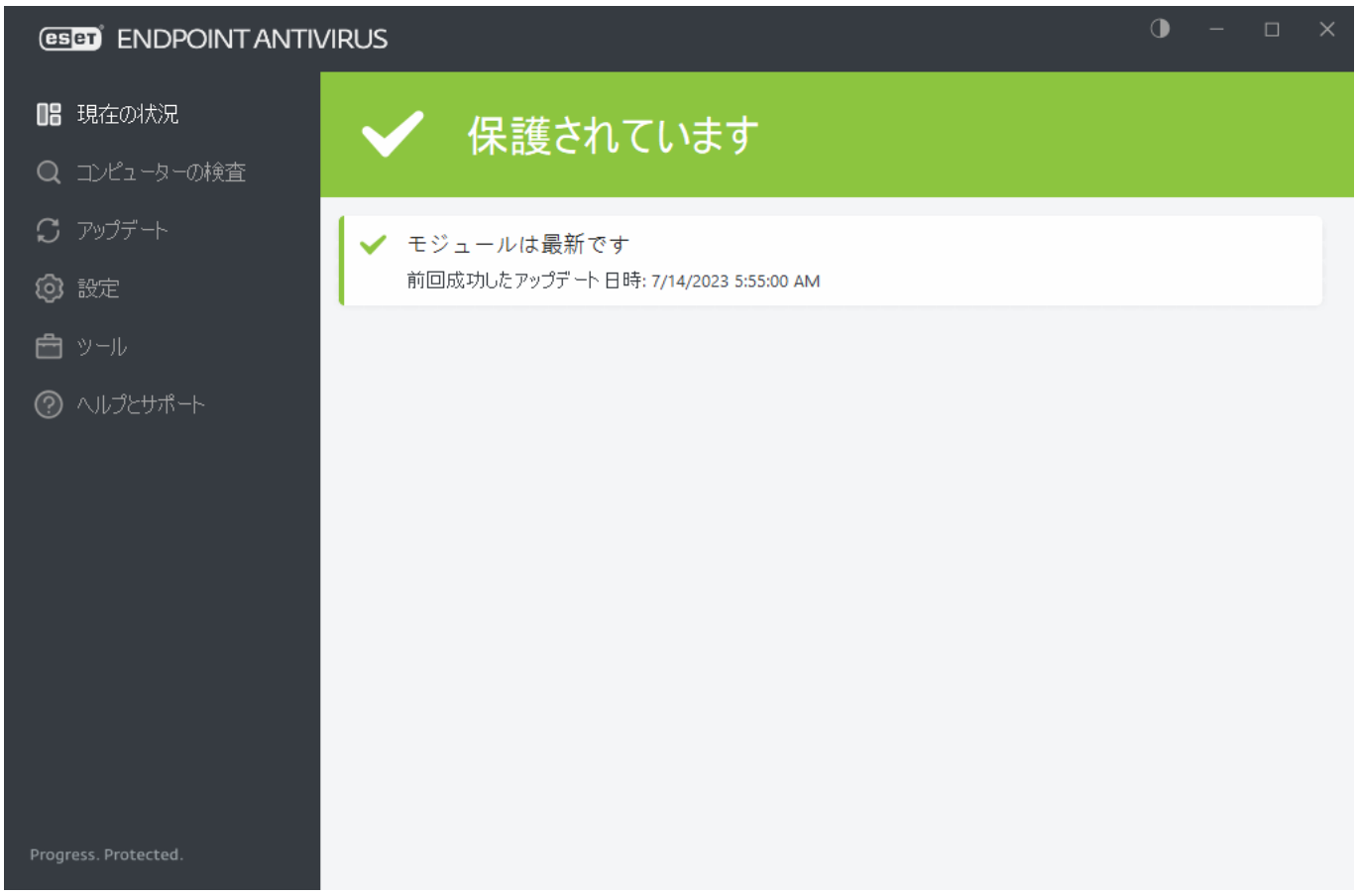
# ESET Endpoint Antivirusの操作

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

> **図解手順**
> 英語および他の複数の言語で提供されている図解手順については、ESET Windows製品のメインプログラムウィンドウを開くを参照してください。

メインプログラムウィンドウの右上のESET Endpoint Antivirus GUIの配色を選択できます。**最小化**アイコンの横にある**配色**アイコン(現在選択されている配色に基づいてアイコンが変更されます)をクリックし、ドロップダウンメニューから配色を選択します。

- **システム色と同じ** – オペレーティングシステム設定に基づいてESET Endpoint Antivirusの配色を設定します。
- **ダークモード** - ESET Endpoint Antivirusには暗い配色(ダークモード)があります。
- **ライトモード** - ESET Endpoint Antivirusには標準の明るい配色があります。




メインメニューオプション:

現在の状況 - ESET Endpoint Antivirusの保護の状態に関する情報が表示されます。

コンピューターの検査 – コンピュータの検査を設定および起動、またはカスタムスキャンを作成しま

す。

アップデート – モジュールおよび検出エンジンアップデートに関する情報を表示します。

ツール – 機能により、プログラム管理が容易になり、上級ユーザー用の追加オプションも利用できるようになります。

設定 - ESET Endpoint Antivirus保護機能の設定オプションと詳細設定へのアクセスを提供します。

ヘルプとサポート – ライセンス、インストールされているESET製品の情報、およびオンラインヘルプ、ESETナレッジベーステクニカルサポートへのリンクを表示します。

# 保護の状態

**保護の状態**ウィンドウには、コンピューターの現在の保護と前回のアップデートに関する情報が表示されます。緑の保護の状態アイコンは、**最も高い保護**の状態が確保されていることを示します。

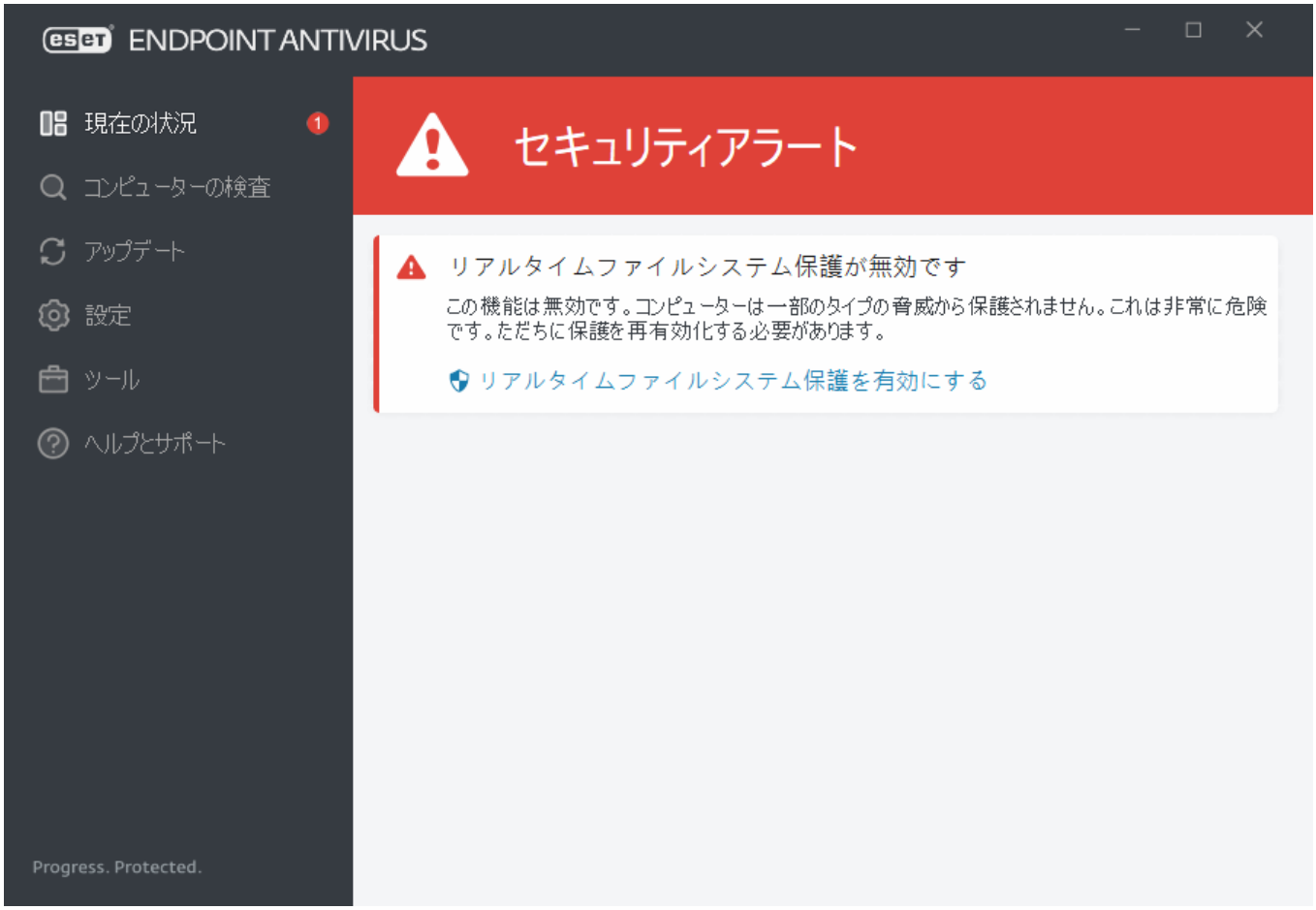
**保護の状態**ウィンドウには、通知とそれに関する詳細情報と推奨解決策が表示されESET Endpoint Antivirusのセキュリティを改善したり、追加機能をオンにしたり、最大限の保護を保証したりできます。


緑のアイコンと緑の**保護中**状態は、最高の保護が確保されていることを示します。

## プログラムが正しく動作しない場合の解決方法

緑色のチェックマークは、完全に機能するすべてのプログラムモジュールの横に表示されます。赤の「！」マークやオレンジの通知アイコンは、モジュールに注意する必要がある場合に表示されます。完全な機能を復元する方法に関する推奨事項を含む、モジュールに関する追加情報がウィンドウの上部に

表示されます。モジュールのステータスを変更するには、メインメニューの[**設定**]をクリックし、必要なモジュールをクリックします。




赤い感嘆符(!)アイコンはコンピューターの最大の保護が保証されていないことを示します。このタイプの通知は次のシナリオで表示される場合があります。

- **ウイルス・スパイウェア対策は一時停止しています** - [**すべてのウイルス対策をスパイウェア対策モジュールを起動**]をクリックすると、メインプログラムウィンドウの[**現在の状況**]ペインまたは[**設定**]ペインの[**ウイルス対策とスパイウェア対策保護を有効にする**]でウイルス対策とスパイウェア対策保護を再有効化します。
- ウイルス対策機能が機能していません – ウィルススキャナーの初期化が失敗しました。ほとんどのESET Endpoint Antivirusモジュールは正常に機能しません。
- **フィッシング対策機能が機能していません**– この機能は機能していません。他の必要なプログラムモジュールがアクティブではありません。
- **検出エンジンが最新ではありません** – このエラーは、検出エンジン(旧称「ウイルス定義データベース」)をアップデートしようとして何回か失敗すると表示されます。アップデートの設定をチェックすることをお勧めします。このエラーが起こる原因として最も多いのは、認証データが正しく入力されていない、または 接続設定が適切ではないことです。
- **製品がアクティベーションされていません**または**ライセンスは有効期限切れです** – 赤色の保護の状態アイコンで示されます。ライセンスの期限が過ぎると、このプログラムではアップデートできなくなります。ライセンスを更新するには、警告ウィンドウの指示に従ってください。
- **ホスト侵入防止システム(HIPS)が無効です** – この問題は、HIPSが無効にされたときに発生します。コンピューターは一部のタイプの脅威から保護されていません。保護を再有効化するには、[**HIPSを有効にする**]をクリックしてください。
- **定期アップデートがスケジュールされていません** – アップデートタスクをスケジュールしないとESET Endpoint Antivirusは重要なアップデートを確認または受信しません。
- **ネットワークアクセスがブロックされました** – ESET PROTECTからのこのワークステーションのコ

**ンピューターをネットワークから隔離する**クライアントタスクがトリガーされたときに表示されます。詳細については、システム管理者に連絡してください。
- **リアルタイムファイルシステム保護が一時停止しています** – リアルタイム保護はユーザーによって無効にされました。コンピューターは脅威から保護されていません。[リアルタイム保護を有効にする]をクリックし、この機能を再有効化します。


オレンジの「i」は、緊急ではない問題に関する注意が必要であることを示します。理由はいくつか考えられます。

- **Webアクセス保護は無効になっています** - Webアクセス保護を再有効化するには、セキュリティ通知をクリックしてから、**[Webアクセス保護を有効にする]**をクリックします。
- **ライセンスの有効期限がまもなく切れます/ライセンスの有効期限が本日切れます** – これは「!」を表示する保護の状態アイコンで示されます。ライセンスの期限が切れたら、プログラムの更新はできなくなり、保護の状態アイコンは赤に変わります。
- **電子メールクライアント迷惑メール対策が一時停止しています** - **電子メールクライアント迷惑メール対策を有効にする**をクリックして、この機能を再度有効にします。
- **Webコントロールが一時停止しています** - **[Webコントロール有効にする]をクリックし、この機能を再有効化します。**
- **ポリシー上書きアクティブ** – おそらくトラブルシューティングが完了するまで、ポリシーによる設定は一時的に上書きされます。許可されたユーザーのみがポリシー設定を上書きできます。詳細情報については、上書きモードを使用する方法を参照してください。
- **デバイスコントロールが一時停止しています** - **[デバイスコントロール有効にする]**をクリックし、この機能を再有効化します。

ESET Endpoint Antivirusの最初のウィンドウで表示の製品内ステータスを調整するには、アプリケーションステータスを参照してください。

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、**[ヘルプとサポート]**をクリックしてヘルプにアクセスするか、あるいはESETナレッジベースを検索してください。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。いただいたご質問にはESETテクニカルサポートが迅速に対応し、解決のお手伝いをいたします。

ステータスがESET PROTECTポリシーによってブロックされる機能に属する場合、リンクをクリックできません。

# コンピュータの検査

オンデマンドスキャナはESET Endpoint Antivirusの重要な部分です。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のスキャン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。システムの詳細検査を定期的に実行(1か月に1回など)し、リアルタイムファイルシステム保護で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。


2種類の**コンピューターの検査**が利用できます。**コンピューターの検査検査**では、検査パラメータを追加で設定することなく、簡単にシステムを検査します。**カスタム検査**では、あらかじめ定義した検査プロファイルの選択や、特定の検査対象を定義できます。

検査プロセスの詳細については、「検査の進行状況」を参照してください。

## コンピューターの検査

**コンピューターの検査**では、すばやくコンピューターのスキャンを起動でき、ユーザーの手を煩わせることなく感染したファイルをクリーンナップできます。**コンピューターの検査**の利点は、操作が簡単で、詳細な検査設定を必要としないことにあります。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。駆除のレベルは自動的に既定値に設定されます。駆除の種類の詳細については、「駆除」を参照してください。

また[**ドラッグアンドドロップ機能**]を使ってファイルまたはフォルダーをクリックすると、マウスボタンを押したままマウスポインターをマークした箇所に移動してからリリースしながら、そのファイルやフォルダーを手動で検査します。その後、アプリケーションが前面に移動します。

**詳細検査**では、次の検査オプションが使用可能です。

## カスタム検査

***カスタム検査***では、検査対象や検査方法などの検査パラメーターを指定できます。***カスタム検査***には、パラメーターを詳細に設定できるという利点があります。これは、同じパラメーターで検査を繰り返し実行する場合に便利です。

## リムーバブルメディア検査

**コンピューター検査**と同じように、現在コンピュータに接続されているリムーバブルメディア(CD/DVD/USBなど)の検査をすばやく開始します。これはUSBフラッシュドライブをコンピュータに接続し、マルウェアや他の潜在的な脅威についてそのコンテンツを検査する場合に便利です。

このタイプの検査は、[**カスタム検査**]をクリックし、[**検査の対象**]ドロップダウンメニューから[**リムーバブルメディア**]を選択して、[**検査**]をクリックして開始することもできます。

## 前回の検査の再実行

前回実行した検査と同じ設定を使用して、すばやく起動します。

**検査後のアクション**ドロップダウンメニューでは、検査の完了後に自動的に実行されるアクションを設定できます。

- **アクションなし** – 検査が完了しても、アクションは実行されません。
- **シャットダウン** – 検査完了後にコンピュータがオフになります。
- **必要に応じて再起動** – 検出された脅威の駆除を完了するために必要な場合にのみ、コンピューターを再起動します。
- **再起動** – 検査完了後に、開いているプログラムをすべて終了し、コンピュータを再起動します。
- **必要に応じて強制再起動** – 検出された脅威の駆除を完了するために必要な場合にのみ、コンピューターを再起動します。
- **強制再起動** – ユーザー操作を待機せずにすべての開いているプログラムを強制的に閉じ、検査が完了した後にコンピューターを再起動します。
- **スリープ** – セッションを保存し、コンピュータを低電力モードにするため、作業を迅速に再開できます。
- **休止** - RAMで実行中のものをすべて取り込み、ハードディスクの特定のファイルに移動します。コンピュータはシャットダウンしますが、次回の起動時に元の状態から再開されます。

> **スリープ**または**休止**アクションは、オペレーティングシステムのコンピューターの電源およびスリープ設定またはコンピューター/ノートブック機能に基づいて使用できます。コンピュータをスリープにしても、コンピュータは動作しています。基本機能は実行され続け、コンピュータがバッテリで動作している場合は、電力を使用します。バッテリの持続時間を長くするために、オフィス外での移動中などには、休止オプションを使用することをお勧めします。

選択したアクションは、実行中のすべての検査が完了した後に開始します。**シャットダウン**または**再起動**を選択すると、確認ダイアログウィンドウに30秒のカウントダウンが表示されます(**キャンセル**をクリックすると、要求されたアクションが無効になります)。

> コンピュータの検査を最低でも月に1回は実行することをお勧めします。[**ツール**] > [**スケジューラ**]で、検査をスケジュールされたタスクとして設定できます。週次コンピュータ検査をスケジュールする方法

# カスタム検査起動ツール

カスタム検査を使用すると、システム全体ではなく、オペレーティングメモリ、ネットワーク、ディスクの特定の部分を検査できます。それには、**詳細検査** > **カスタム検査**をクリックし、フォルダーツリー構造から個別の対象を選択します。

特定の対象の検査時に使用するプロファイルを、**プロファイル**ドロップダウンメニューから選択できます。既定のプロファイルは**スマート検査**です。さらに、**詳細検査**および**コンテキストメニューの検査**お

よび**コンピューターの検査**という3つの事前定義された検査プロファイルがあります。これらの検査プロファイルでは、さまざまなThreatSenseパラメーターを使用します。使用可能なオプションについては、詳細設定 > **検出エンジン** > **マルウェア検査** > **オンデマンド検査** > ThreatSenseで説明されています。

フォルダー(ツリー)構造には、特定の検査対象も含まれています。

- **システムメモリ** – 現在オペレーティングメモリで使用されているすべてのプロセスとデータを検査します。
- **ブートセクター/UEFI** – ブートセクターとUEFIにマルウェアが存在するかどうかを検査します。用語集のUEFIスキャナーの詳細をお読みください。
- **WMIデータベース**– Windows Management Instrumentation WMIデータベース全体、すべての名前空間、すべてのクラスインスタンス、およびすべてのプロパティを検査します。データとして埋め込まれた感染ファイルまたはマルウェアへの参照を検索します。
- **システムレジストリ** – システムレジストリ全体、すべてのキー、およびサブキーを検査します。データとして埋め込まれた感染ファイルまたはマルウェアへの参照を検索します。検出を駆除するときには、重要なデータが失われないように、レジストリに参照が残ります。

検査対象(ファイルまたはフォルダー)にすばやく移動するには、ツリー構造の下のテキストフィールドにパスを入力しますパスは大文字と小文字を区別します。検査に対象を含めるには、ツリー構造のチェックボックスを選択します。

> **週次コンピューター検査をスケジュールする方法**
> 定期的なタスクをスケジュールするには、週次コンピューター検査をスケジュールする方法を参照してください。


詳細設定 > **検出エンジン** > **マルウェア検査** > **オンデマンド検査** > **ThreatSense** > **駆除**で、検査の駆除パラメータを設定できます。駆除アクションなしで検査を実行するには、**詳細設定**をクリックし、**駆除せずに検査する**を選択します。スキャンに関する情報は、スキャンログに保存されます。

**除外を無視**を選択すると、以前に除外された拡張子のファイルも、例外なく検査されます。

設定したカスタムパラメータを使用して検査を実行するには、[**検査**]をクリックします。

[**管理者として検査**]を使用すると、管理者アカウントで検査を実行できます。現在のユーザーに検査対象のファイルにアクセスするための権限がない場合は、これを使用します。現在ログインしているユーザーが管理者としてユーザーアカウント制御を呼び出せない場合、このボタンは使用できません。

[ログを表示]をクリックすると、検査が完了したときにコンピューター検査ログを表示できます。

# 検査の進行状況

検査の進行状況ウィンドウには、検査の現状および悪意のあるコードが含むファイルの数に関する情報が表示されます。

パスワード保護されたファイルやシステム専用ファイル(一般的な例としては、*pagefile.sys*や特定のログファイル)など一部のファイルは、検査できなくても正常です。詳細については、ナレッジベース記事をご覧ください。

### 週次コンピューター検査をスケジュールする方法

定期的なタスクをスケジュールするには、週次コンピューター検査をスケジュールする方法を参照してください。

**検査の進行状況** – 進行状況バーに実行中の検査のステータスが表示されます。

**対象** – 現在検査されている対象の名前と場所。

**検出されました** – 検査中に検査されたファイルと、見つかった脅威と、駆除された脅威の総数を表示します。

詳細をクリックすると、次の情報が表示されます。

- **ユーザー** – 検査を開始したユーザーアカウントの名前。
- **検査されたオブジェクト** – すでに検査されたオブジェクトの数。
- **期間** – 経過時間。

一時停止アイコン – 検査を一時停止します。

再開アイコン – このオプションは、検査を中断した場合に表示されます。アイコンをクリックすると、検査が続行されます。

停止アイコン – 検査を終了します。

**検査ウィンドウを開く**をクリックして、検査の詳細を含むコンピューターの検査ログを開きます。

**ログをスクロールする** – オンにすると、新しいエントリーが追加されるときに検査ログが自動的にスクロールされて、最新のエントリーが表示されます。

現在実行中の検査に関する詳細情報を表示するには、拡大鏡または矢印をクリックします。**コンピューターの検査**または**詳細検査 > カスタム検査**をクリックすると、並行して別の検査を実行できます。


**検査後のアクション**ドロップダウンメニューでは、検査の完了後に自動的に実行されるアクションを設定できます。

- **アクションなし** – 検査が完了しても、アクションは実行されません。
- **シャットダウン** – 検査完了後にコンピュータがオフになります。
- **必要に応じて再起動** – 検出された脅威の駆除を完了するために必要な場合にのみ、コンピューターを再起動します。
- **再起動** – 検査完了後に、開いているプログラムをすべて終了し、コンピュータを再起動します。
- **必要に応じて強制再起動** – 検出された脅威の駆除を完了するために必要な場合にのみ、コンピューターを再起動します。
- **強制再起動** – ユーザー操作を待機せずにすべての開いているプログラムを強制的に閉じ、検査が完了した後にコンピューターを再起動します。
- **スリープ** – セッションを保存し、コンピュータを低電力モードにするため、作業を迅速に再開できます。
- **休止** - RAMで実行中のものをすべて取り込み、ハードディスクの特定のファイルに移動します。コンピュータはシャットダウンしますが、次回の起動時に元の状態から再開されます。

**スリープ**または**休止**アクションは、オペレーティングシステムのコンピューターの電源およびスリープ設定またはコンピューター/ノートブック機能に基づいて使用できます。コンピュータをスリープにしても、コンピュータは動作しています。基本機能は実行され続け、コンピュータがバッテリで動作している場合は、電力を使用します。バッテリの持続時間を長くするために、オフィス外での移動中などには、休止オプションを使用することをお勧めします。

選択したアクションは、実行中のすべての検査が完了した後に開始します。**シャットダウン**または**再起動**を選択すると、確認ダイアログウィンドウに30秒のカウントダウンが表示されます(**キャンセル**をクリックすると、要求されたアクションが無効になります)。

# コンピューターの検査ログ

特定の検査に関連する詳細情報は、ログファイルで確認できます。検査ログには、以下の情報が含まれます。

- 検出エンジンのバージョン
- 開始日時
- 検査したディスク、フォルダー、ファイルのリスト
- スケジュールされた検査名(スケジュールされた検査のみ)
- 検査を開始したユーザー。
- 検査状況
- 検査したファイルの数
- 見つかった検出数
- 完了時間
- 検査に要した時間

以前に実行された同じスケジュールされたタスクがまだ実行中の場合は、スケジュールされたコンピューターの検査タスクの新規開始がスキップされます。スキップされたスケジュールされた検査タスクは、検査済みオブジェクト0件、**以前の検査がまだ実行中のため、検査が開始しませんでした**ステータスとしてコンピューターの検査ログを作成します。

以前の検査ログを見つけるには、メインプログラムウィンドウで**ツール > ログファイル**を選択します。ドロップダウンメニューで**コンピューターの検査**を選択し、任意のレコードをダブルクリックします。


「レコードを開けない」、「レコードを開くときのエラー」、または「破損したレコードのアーカイブ」の詳細については、ESETナレッジベース記事を参照してください。

スイッチアイコン **フィルタリング**をクリックすると、ログフィルタリングウィンドウが開き、カスタム条件を定義して検索を絞り込むことができます。コンテキストメニューを表示するには、特定のログエントリを右クリックします。

| アクション | 使用状況 |
|---|---|
| 同じレコードをフィルタ | ログフィルタリングを有効にします。ログには、選択したタイプと同じタイプのレコードのみが表示されます。 |
| フィルタ | このオプションを使用すると、ログフィルタリングウィンドウが開き、特定のログエントリの条件を定義できます。ショートカット: Ctrl+Shift+F |
| フィルタをクリア | フィルター設定を有効にします。初めてフィルターを有効にするときには、設定を定義する必要があります。ログフィルタリングウィンドウが開きます。 |
| フィルタをクリア | フィルターをオフにします(下部にあるスイッチをクリックするのと同じ)。 |
| コピー | ハイライトされたレコードをクリップボードにコピーします。ショートカット: Ctrl+C |
| すべてコピー | ウィンドウのすべてのレコードをコピーします。 |
| エクスポート | クリップボードでハイライトされたレコードををXMLファイルにエクスポートします。 |
| すべてエクスポート | ウィンドウのすべてのレコードがXMLファイルにエクスポートされます。 |
| 検出の説明 | ハイライトされた侵入の危険と兆候に関する情報を含むESETの脅威に関する情報へのリンクです。 |

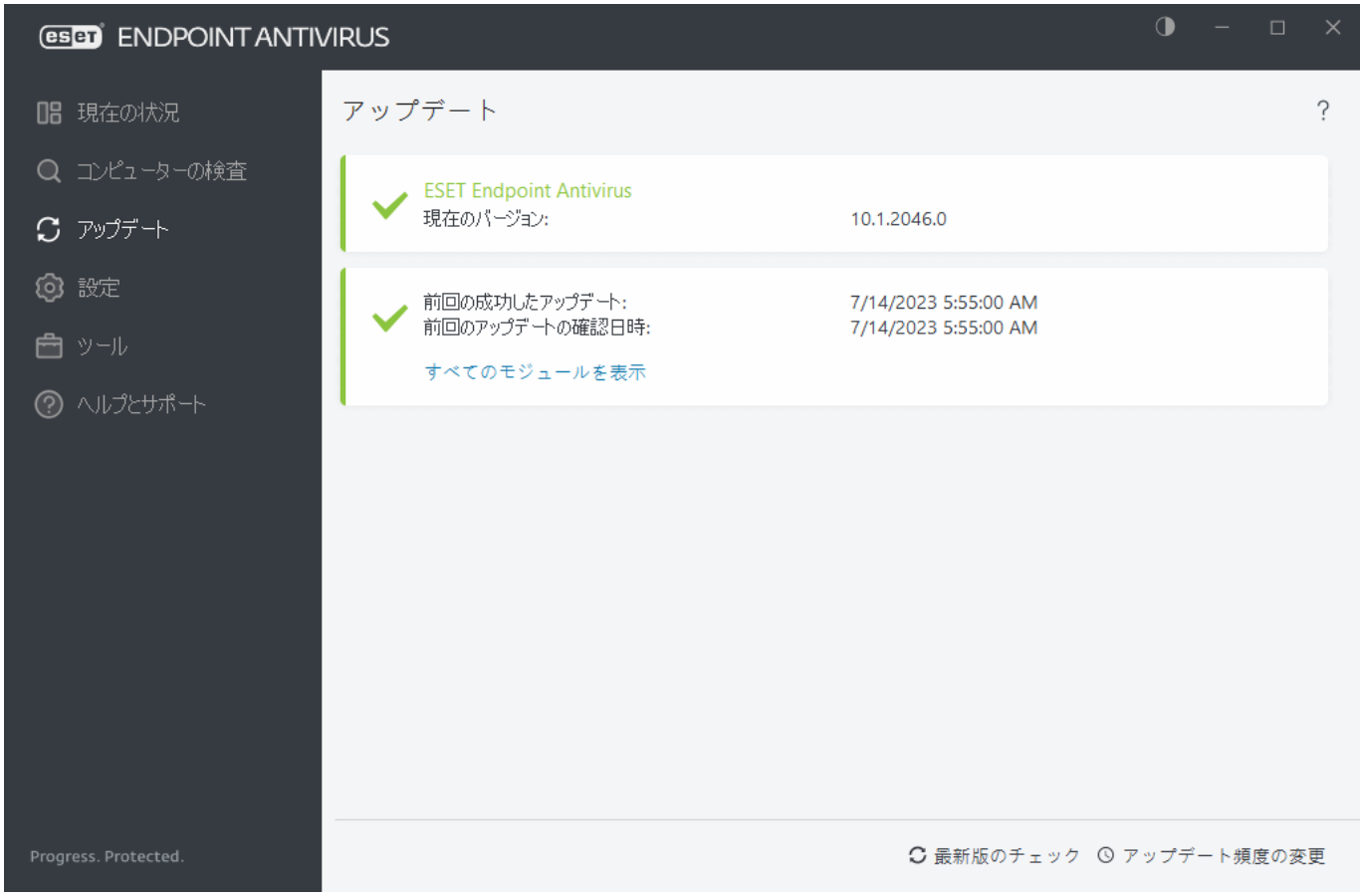
# アップデート

コンピュータのセキュリティを最大限確保するためにはESET Endpoint Antivirusを定期的にアップデートするのが最善の方法です。[アップデート]モジュール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ようにします。

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。

自動アップデートの他に、**アップデートの確認**をクリックして手動アップデートをトリガーできます。プログラムモジュールとコンポーネントの定期アップデートは、悪意のあるコードから完全な保護を管理するうえで重要な部分です。製品モジュール設定や操作には注意してください。アップデートを受信するには、製品認証キーを使用して、製品をアクティベーションする必要があります。インストール中に入力しなかった場合は、ESETのアップデートサーバーにアクセスする際にESET Endpoint Antivirusをアクティベーションする必要がありますESET Endpoint Antivirusの購入後、製品認証キーは電子メールでESETから送信されます。

ユーザー名とパスワードを使用せずに、オフラインライセンスファイルを使用してESET Endpoint Antivirusをアクティベーションする場合は、赤色の情報**モジュールアップデートが失敗しました**が表示され、ミラーからのみアップデートをダウンロードできることを示します。




**現在のバージョン** - ESET Endpoint Antivirusのビルド番号。

**最終成功アップデート** – 最終成功アップデートの日時です。検出エンジンが最新、つまり最近の日付になっていることを確認します。

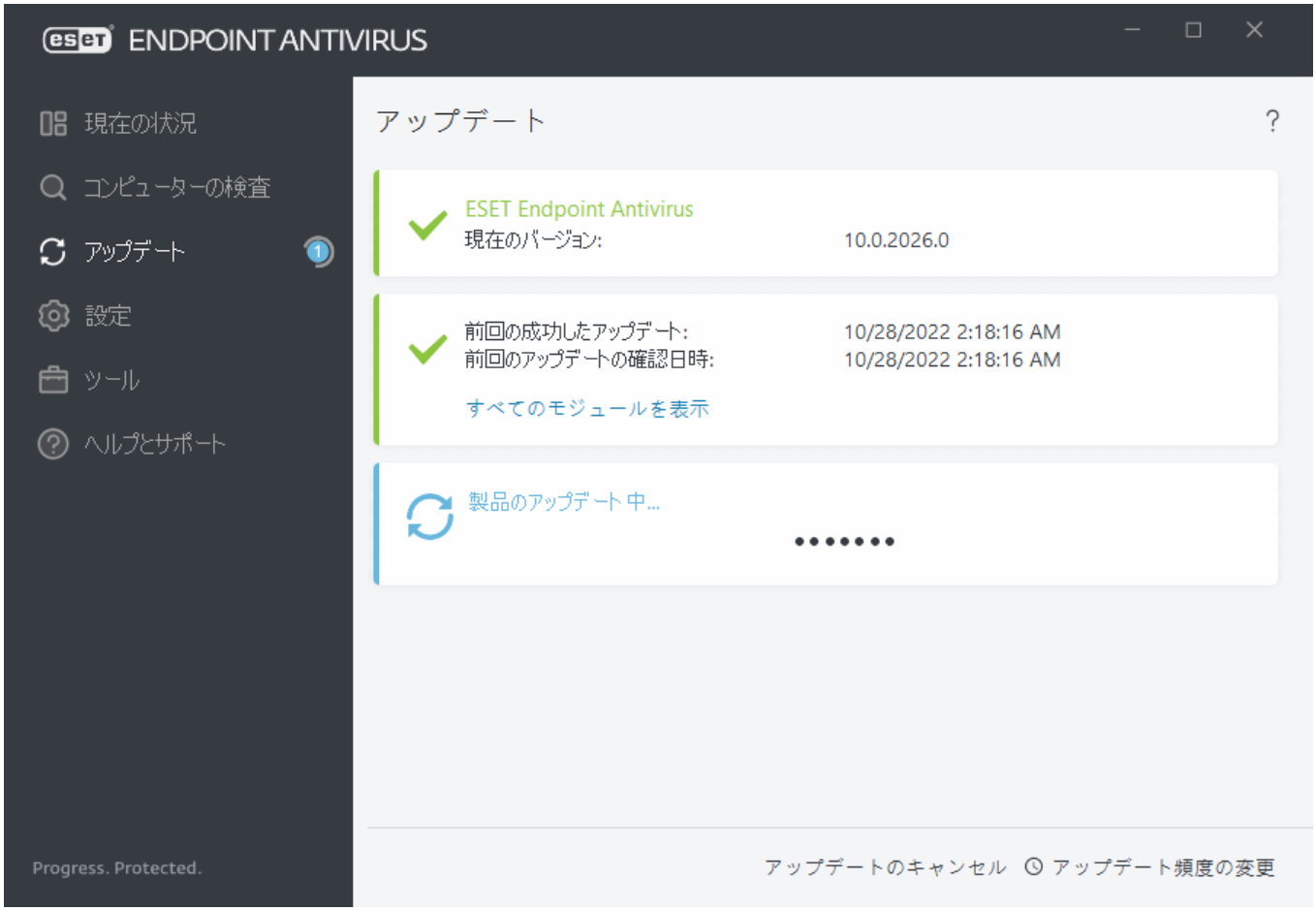
**アップデートの最終成功チェック** – モジュールのアップデートを最後に試行して成功した日時。

**すべてのモジュールを表示** – クリックすると、インストールされたモジュールのリストを開き、モジュールのバージョンと最後のアップデートを確認します。

---

# アップデートプロセス

[**アップデートの確認**]をクリックすると、ダウンロードが始まります。ダウンロードの進行状況バーとダウンロードにかかる残り時間が表示されます。アップデートを中断するには、[**アップデートのキャンセル**]をクリックします。




正常な状況では、［**アップデート**］ウィンドウに緑色のチェックマークが表示され、プログラムが最新であることを示します。表示されないということは、プログラムが古くなっており、感染しやすくなっているということです。プログラムモジュールをすぐにアップデートしてください。

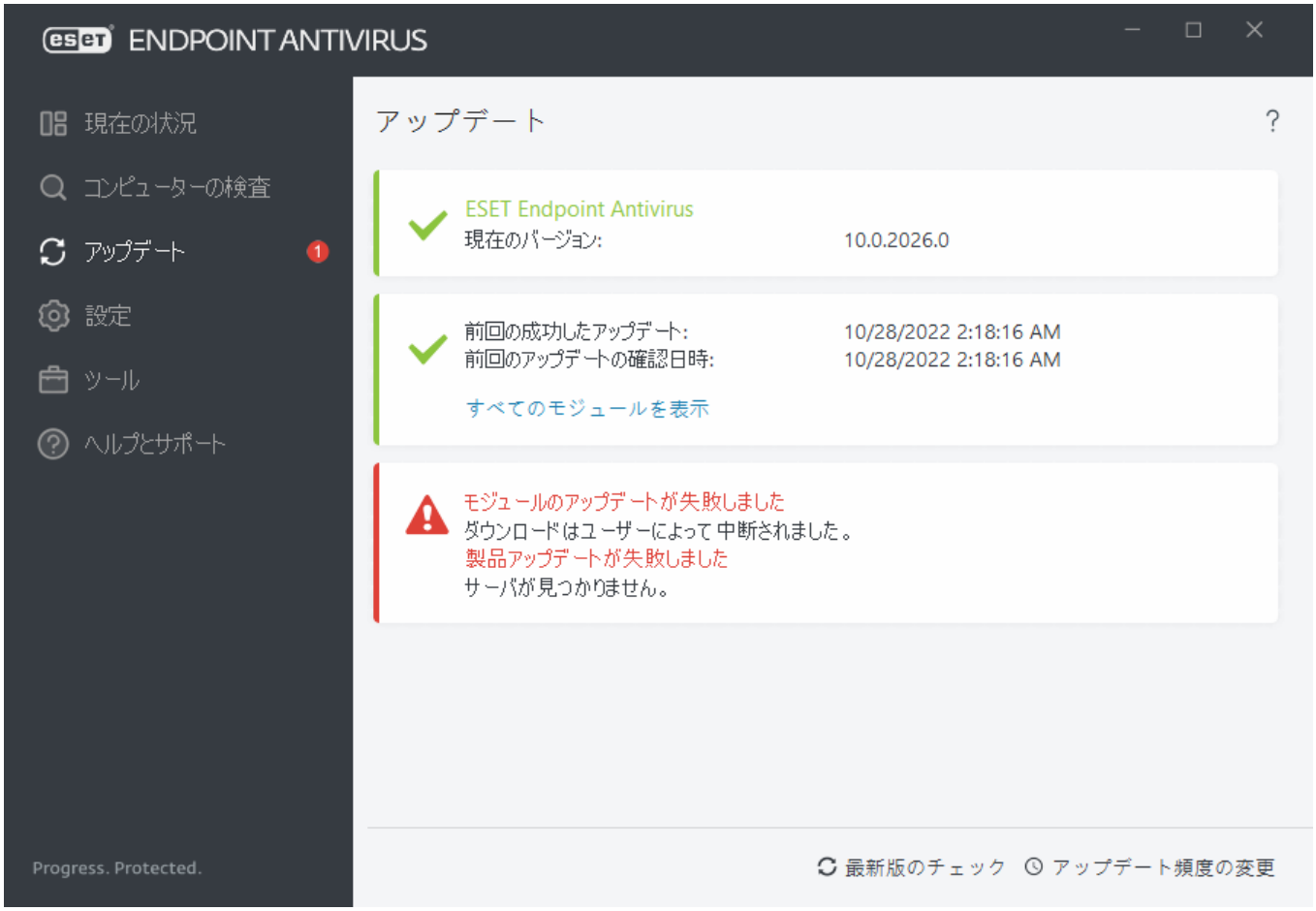
---

# 失敗したアップデート

**検出エンジンは最新ではありません** – このエラーは、モジュールをアップデートしようとして何回か失敗すると表示されます。アップデートの設定をチェックすることをお勧めします。このエラーが起こる原因として最も多いのは、認証データが正しく入力されていない、または 接続設定が適切ではないことです。

上記の通知は、アップデートの失敗に関する次の2つのメッセージ(**モジュールのアップデートが失敗しました**)に関連します。

1. **無効なライセンス** – ライセンスがアクティブではありません。認証データを確認することをお勧めします。メインメニューで**[ヘルプとサポート]** > **[ライセンスの変更]**をクリックして、新しい製品認証キーを入力します。
2. **アップデートファイルのダウンロード中にエラーが発生しました** – このエラーはインターネット接続の設定が正しくないことが原因のことがあります。インターネット接続を確認することをお勧めします(Webブラウザーで任意のWebサイトを開いてみます)。Webサイトが開かない場合、インターネット接続が確立されていないか、コンピューターの接続に問題がある可能性があります。インターネットサービスプロバイダ(ISP)からアクティブなインターネット接続が接続されていることを確認してください。




詳細については、ESETナレッジベース記事を参照してください。

# アップデートタスクの作成方法

アップデートを手動で開始するには、メインメニューの[**アップデート**]をクリックした後で、[**最新版のチェック**]をクリックします。

アップデートはスケジュールされたタスクとしても実行できます。スケジュールされたタスクを設定するには、[**ツール**] > [**スケジューラ**]をクリックします。既定では、次のアップデートタスクがESET Endpoint Antivirusでアクティベーションされます。

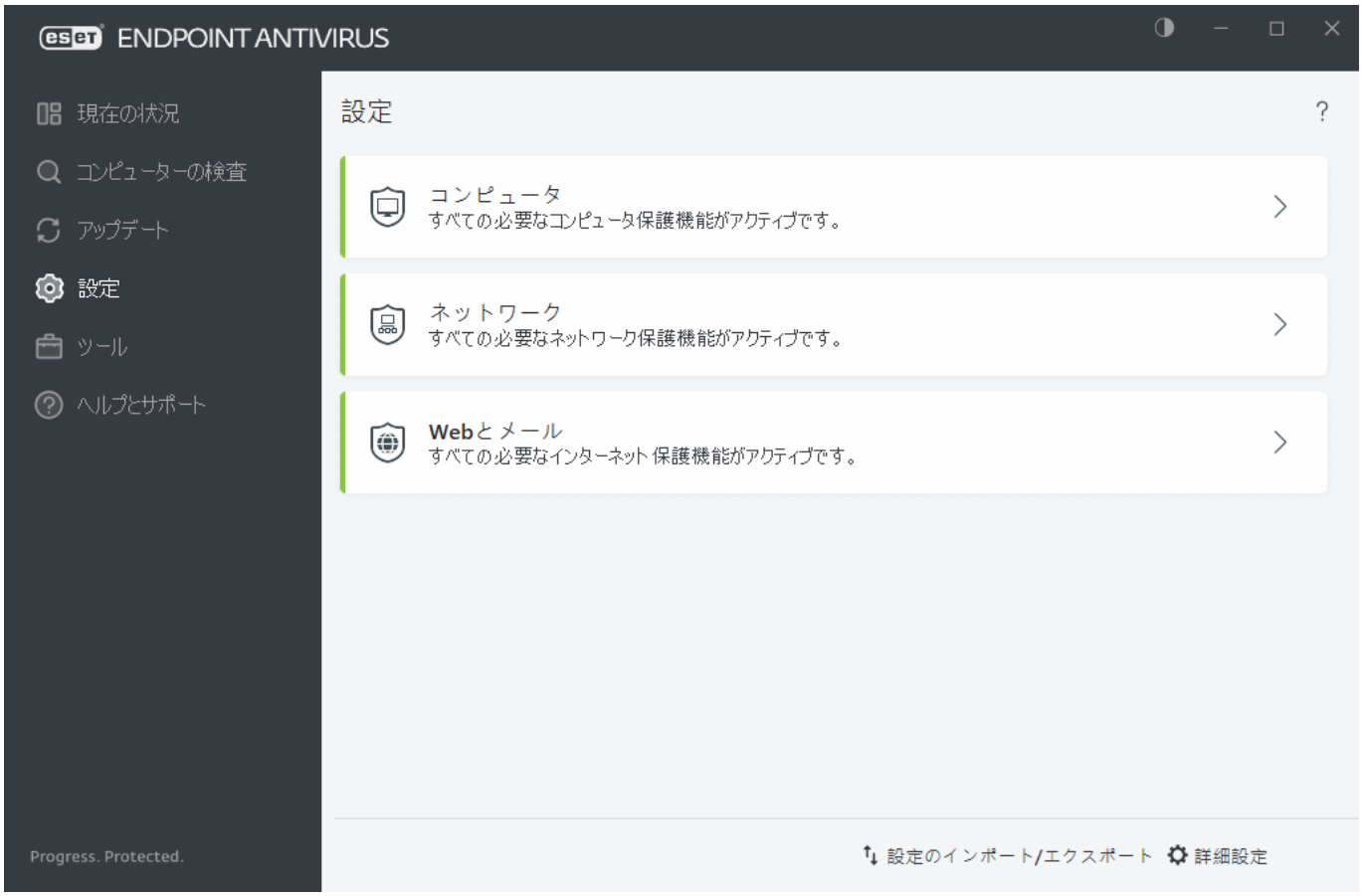
- **定期的に自動アップデート**
- **ユーザーログオン後に自動アップデート**

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

# 設定

使用可能な保護機能のグループは、プログラムのメインウィンドウ > **設定**にあります。

ESET PROTECT Webコンソールからポリシーを作成するときには、各設定のフラグを選択できます。強制フラグの設定には優先度があり、後のポリシーに強制フラグがある場合でも、後のポリシーによって上書きすることはできません。こうすると、この設定が変更されない(たとえばユーザーによって、またはマージ中に後のポリシーによって)ことが保証されます。詳細情報については、ESET PROTECTオンラインヘルプのフラグを参照してください。




[**設定**]メニューには次のセクションがあります。

コンピュータ

ネットワーク

Webとメール

ESET PROTECTポリシーが適用されるときには、特定のコンポーネントの横にロックアイコンが表示されますESET PROTECTによって適用されたポリシーは、ログインユーザー(管理者など)による認証の後にローカルで上書きできます。詳細情報については、ESET PROTECTオンラインヘルプを参照してください。

この方法で無効にされたすべての保護対策は、コンピュータの再起動後に再有効化されます。

設定ウィンドウの下部に追加オプションがあります。詳細設定をクリックして、それぞれのモジュールの詳細パラメーターを設定します。***.xml設定ファイルを使用して設定パラメーターをロードしたり、現在の設定パラメーターを設定ファイルに保存したりするには、[設定のインポートおよびエクスポート]を使用します。

# コンピュータ

プログラムのメインウィンドウ > **設定**の**コンピューター**をクリックし、すべての保護モジュールの概要を表示します。


**コンピューター**セクションでは、次のコンポーネントを有効または無効にできます。

- リアルタイムファイルシステム保護 – 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。リアルタイムファイルシステム保護の横の歯車アイコンをクリックし、除外の編集をクリックして除外設定ウィンドウを開くと、ファイルとフォルダーを検査対象外にできます。リアルタイムファイルシステム保護詳細設定を開くには、設定をクリックします。
- デバイスコントロール – 自動デバイスコントロール(CD/DVD/USBなど)を備えています。このモジュールを使用すると、拡張フィルタ/権限をブロック、または調整して、ユーザーからの指定デバイスへのアクセス方法やその作業方法を定義できます。
- Host Intrusion Prevention System (HIPS) - HIPSは、オペレーティングシステム内のイベントを監視し、カスタマイズされた一連のルールに従って動作します。
- **詳細メモリ検査**はエクスプロイトブロックとともに動作し、難読化または暗号化を使用することで、マルウェア対策製品の検出を回避するように設計されたマルウェアに対する保護を強化します。既定では、詳細メモリ検査が有効です。この保護の詳細については、「用語集」を参照してください。
- **エクスプロイトブロック** - Webブラウザ、PDFリーダー、電子メールクライアント、MS Officeコンポーネントなどの一般的に利用されるアプリケーションタイプの保護を強化するための機能です。既定では、エクスプロイトブロックが有効です。この保護の詳細については、「用語集」を参照してください。
- **ランサムウェア保護**- HIPS機能の一部として動作する保護の別のレイヤーです。ランサムウェア保護を実行するにはESET LiveGrid®レピュテーションシステムを有効にする必要があります。この保護の詳細を参照してください
- プレゼンテーションモード – ソフトウェアを中断せずに使用し、通知を表示せずCPUの使用量を最小化する必要があるユーザー向けの機能です。警告メッセージ(潜在的なセキュリティリス

ク)を受け取った後、プレゼンテーションモードを有効にするとメインプログラムウィンドウがオレンジに変わります。

**ウイルス・スパイウェア対策保護を一時停止する** – ウイルス・スパイウェア対策保護を一時的に無効にする場合は、ドロップダウンメニューを使用して、選択したコンポーネントを無効にする時間を選択してから、**[適用]**をクリックすると、セキュリティコンポーネントを無効にできます。保護を再有効化するには、**[ウイルス・スパイウェア対策を有効にする]**をクリックします。

個別の保護モジュールを一時停止または無効にするには、トグルアイコンをクリックします。

⚠ 保護モジュールをオフすると、コンピューターの保護レベルが低下する可能性があります。

# 脅威が検出されました

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

## 標準的な動作

ESET Endpoint Antivirusは、一般的に以下を使用してマルウェアを検出して処理します。

- リアルタイムファイルシステム保護
- Webアクセス保護
- 電子メールクライアント保護
- コンピュータの検査

各機能は、標準的な駆除レベルを使用し、ファイルを駆除して、隔離に移動するか、接続を終了しようとします。通知ウィンドウは、画面の右下にある通知領域に表示されます。検出/駆除されたオブジェクトの詳細については、「ログファイル」を参照してください。駆除レベルと動作の詳細については、「駆除」を参照してください。


## 駆除と削除

リアルタイムファイルシステム保護にあらかじめ指定されたアクションがない場合は、警告ウィンドウが表示され、オプションを選択するよう求められます。選択できるオプションは通常、**[駆除]**、**[削除]**、および**[脅威を無視]**のいずれかです。**[脅威を無視]**を選択すると、感染ファイルが駆除されないまま残されるので、推奨されません。唯一の例外は、そのファイルが「無害なのに誤って感染が検出された」と確信できる場合です。


ウイルスの攻撃によって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。

感染しているファイルが、システムプロセスによって"ロック"または使用されている場合、通常は開放後でなければ削除できません(通常は再起動後)。

## 隔離フォルダーからの復元

隔離にはESET Endpoint Antivirusのメインプログラムウィンドウから**ツール > 隔離**をクリックしてアクセスできます。

隔離されたファイルは元の場所に復元することもできます。

- この目的のために**復元**機能を使用するには、隔離内の特定のファイルを右クリックして、コンテキストメニューを使用します。
- ファイルが望ましくない可能性があるアプリケーションに設定されている場合、**復元および検査時に除外**オプションが有効になります。「除外」も参照してください。
- コンテキストメニューには、**復元先を指定**オプションもあります。このオプションを使用すると、削除される前の場所とは異なる場所にファイルを復元することができます。
- 復元機能は、読み取り専用のネットワーク共有上にあるファイルなど、使用できない場合があります。

## 複数の脅威

コンピュータの検査中に駆除されなかった感染ファイルがある場合(または駆除レベルが[**駆除なし**]に設定されていた場合)、警告ウィンドウが開き、これらのファイルに対するアクションを選択するよう求められます。

## アーカイブのファイルの削除

既定の駆除モードでは、アーカイブファイルに感染ファイルしか含まれていない場合にのみ、アーカイブファイル全体が削除されます。つまり、感染していない無害なファイルも含まれている場合には、アーカイブは削除されません。厳密な駆除スキャンを実行する際には注意が必要です。厳密な駆除を有効に

した状態では、アーカイブに感染ファイルが1つでも含まれていれば、アーカイブ内の他のファイルの状態に関係なく、そのアーカイブは削除されます。

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

- ESET Endpoint Antivirusを開き、[コンピュータの検査]をクリックする
- [**スマート検査**]をクリックする(詳細については、「コンピュータ検査」を参照)
- スキャン終了後、ログでスキャン済みファイル、感染ファイル、および駆除済みファイルの件数をそれぞれ確認する

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

# ネットワーク

ネットワーク保護設定を設定するか、ネットワーク通信のトラブルシューティングを行うには、プログラムのメインウィンドウ > **設定** > **ネットワーク**を開きます。

個別の保護モジュールを一時停止または無効にするには、トグルアイコンをクリックします。

保護モジュールをオフすると、コンピューターの保護レベルが低下する可能性があります。

保護モジュールの横の歯車アイコンをクリックし、詳細設定にアクセスします。

ネットワーク攻撃保護(IDS)を有効にする– ネットワークトラフィックの内容を分析し、ネットワーク攻撃から保護します。有害であると見なされるすべてのトラフィックはブロックされます。ESET Endpoint Antivirusは、保護されていないワイヤレスネットワークまたは保護が弱いネットワークに接続するときに通知します。

**ボットネット保護** – システム上のマルウェアを迅速かつ正確に特定します。

**ブロックされた通信の解決** - ESETファイアウォールが原因の接続の問題を解決できます。詳細については、トラブルシューティングウィザードを参照してください。

**一時的にブロックされたIPアドレスを解決** – 攻撃の元であると検出され、一定の時間、接続をブロックするためにブラックリストに追加されたIPアドレスの一覧を表示します。

**ログを表示** - ネットワーク保護ログファイルを開きます。


# ネットワークアクセストラブルシューティング

トラブルシューティングウィザードでは、ファイアウォールが原因の接続の問題を解決できます。**ネットワークアクセスのトラブルシューティング**は、プログラムのメインウィンドウ > **設定** > **ネットワーク** > **ブロックされた通信の解決**にあります。

**ローカルアプリケーション**に対してブロックされた通信、または**リモートデバイス**からのブロックされた通信を表示するかを選択します。

ドロップダウンメニューから、通信がブロックされた期間を選択します。最近ブロックされた通信のリストで、アプリケーションやデバイスの種類、評判とその期間中にブロックされたアプリケーションとデバイスの合計数についての概要の説明を確認できます。ブロックされた通信の詳細については、**詳細**をクリックします。次のステップは、接続の問題が発生したアプリケーションやデバイスのブロックの解除です。

**[ブロック解除]**をクリックすると以前ブロックされた通信が許可されます。それ以降もアプリケーションで問題が発生する場合、またはデバイスが期待どおりに動作しない場合は、**別のルールを作成**をクリックすると、以前にそのデバイスでブロックされたすべての通信が許可されます。問題が解決しない場合は、コンピューターを再起動します。

次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
- トラブルシューティングウィザードを使用した例外の追加

ルールを作成できない場合は、エラーメッセージが表示されます。**再試行**をクリックし、このプロセスを繰り返して通信のブロックを解除するか、ブロックされた通信のリストから別のルールを作成します。

# 一時IPアドレスブラックリスト

攻撃の元であると検出されたIPアドレスを表示するには、一定の時間、接続をブロックするためにブラックリストに追加されます。ESET Endpoint Antivirusから、**設定 > ネットワーク > 一時IPアドレスブラックリスト**に移動します。一時的にブロックされたIPアドレスは1時間ブロックされます。

## 列

**IPアドレス** – ブロックされているIPアドレスを示します。

**ブロックの理由** – このアドレスで防御された攻撃の種類(TCPポートスキャニング攻撃など)示します。

**タイムアウト** – アドレスがブラックリストから有効期限切れになる日時を示します。

## コントロール要素

**削除** – クリックすると、有効期限切れになる前にアドレスがブラックリストから削除されます。

**すべて削除** – クリックすると、すべてのアドレスがただちにブラックリストから削除されます。

**例外の追加** – クリックするとIDSフィルタリングにファイアウォール例外が追加されます。

# ネットワーク保護ログ

ESET Endpoint Antivirusネットワーク保護はすべての重要なイベントをログファイルに保存します。ログファイルを表示するには、プログラムのメインウィンドウ > **設定 > ネットワーク > ログを表示**を開きます。

ログファイルは、エラーを検知し、システムへの侵入を明らかにするために使用できます。ネットワーク保護のログには以下のデータが含まれます:

- イベントの日時
- イベントの名前
- ソース
- 対象ネットワークのIPアドレス
- ネットワーク通信プロトコル
- 適用されたルール、ワームの名前(特定された場合)
- アプリケーションパスと名前
- ハッシュ
- ユーザー
- アプリケーションの署名者(発行者)
- パッケージ名
- サービスの名前

このデータを詳しく分析することで、システムのセキュリティを侵害しようとする行為を検出することができます。 その他にも、不明な場所からの頻繁な接続、接続を確立しようとする多数の試行、不明なアプリケーションの通信、通常と異なるポート番号の使用など、多くの要素は潜在的なセキュリティリスクがあることを示唆しており、その影響を最小限にとどめることができます。

セキュリティ脆弱性の悪用

実際の悪用が発生する前に、悪用の試みが検出され、ネットワークレベルでブロックされているため、特定の脆弱性が既に修正されている場合でも、セキュリティ脆弱性の悪用のメッセージをログに記録します。

# ESETネットワーク保護の問題の解決

ESET Endpoint Antivirusがインストールされた状態で接続の問題がある場合は、複数の方法で、ESETネットワーク保護が原因になっているかどうかを判断できます。さらにESETネットワーク保護を使用すると、接続の問題を解決するための新しいルールまたは例外を作成できます。

ESETネットワーク保護の問題を解決するには、次のトピックを参照してください。

- ネットワークアクセストラブルシューティング
- ロギングとログからのルールまたは例外の作成
- ネットワーク保護詳細ログ
- ネットワークトラフィックスキャナーの問題を解決する

# ロギングとログからのルールまたは例外の作成

既定ではESETファイアウォールは、ブロックされたすべての接続を記録するわけではありません。ネットワーク保護でブロックされた項目を確認する場合は、詳細設定 > **ツール** > **診断** > **詳細ログ**を開き、**ネットワーク保護詳細ログを有効にする**を有効にします。ログに記録されている項目をファイアウォールでブロックしたくない場合は、項目を右クリックして、**今後、同様のイベントをブロックしない**を選択すると、ルールまたはIDSルールを作成できます。ブロックされたすべての接続のログには、多数の項目が含まれることがあり、このログで特定の接続が見つかりにくい可能性があります。問題が解決したら、ロギングをオフにできます。

ログの詳細については、「ログファイル」を参照してください。

ロギングをしようして、ネットワーク保護が特定の接続をブロックする順序を確認できます。さらに、ログからルールを作成すると、目的のルールを正確に作成できます。

# ログからルールを作成

新しいバージョンのESET Endpoint Antivirusでは、ログからルールを作成できます。メインメニューで、**ツール** > **ログファイル**をクリックします。ドロップダウンメニューから**ネットワーク保護**を選択し、目的のログエントリを右クリックして、コンテキストメニューから[**同様のイベントを今後ブロックしない**]を選択します。通知ウィンドウに新しいルールが表示されます。

ログから新しいルールを作成するには、次の設定でESET Endpoint Antivirusを構成する必要があります。

1. **詳細設定** > ツール > **ログファイル**で、ログに記録する最低レベルを**診断**に設定します。
2. 詳細設定 > **保護** > **ネットワークアクセス保護** > **ネットワーク攻撃保護** > **詳細オプション** > **侵入検出**で、**セキュリティホールに対する受信攻撃を通知**を有効にします。

# ネットワーク保護詳細ログ

この機能は、ESETテクニカルサポートにより複雑なログファイルを提供するためのものです。ESETテクニカルサポートから要請があった場合にのみこの機能を使用してください。大量のログファイルが生成され、コンピューターの速度が低下するおそれがあります。

1. 詳細設定 > **ツール > 診断** > 詳細ログに移動し、**ネットワーク保護詳細ログを有効にする**を有効にします。
2. 発生している問題を再現してみます。
3. ネットワーク保護詳細ログを無効にします。
4. ネットワーク保護詳細ログで作成されるPCAPログファイルは、診断メモリダンプが生成されるディレクトリにあります：*C:\ProgramData\ESET\ESET Security\Diagnostics*

# ネットワークトラフィックスキャナーの問題を解決する

ブラウザーまたは電子メールクライアントで問題が発生した場合は、まず、ネットワークトラフィックスキャナーに問題がないかを確認します。このためには、詳細設定 > **検出エンジン > ネットワークトラフィックスキャナー**で一時的にネットワークトラフィックスキャナーを無効にします(完了したら必ずオンに戻してください。そうでないと、ブラウザーとメールクライアントが保護されなくなります)。オフにして問題が解決したら、次の一般的な問題の一覧を確認して、問題を解決してください。

## アップデートまたは安全な接続の問題

アプリケーションで更新できない場合や、通信チャネルが安全ではないというエラーが表示される場合:

- SSL/TLSが有効な場合、一時的にオフにしてください。これで問題が解決する場合は、問題がある通信を除外するとSSL/TLSを使用し続け、アップデートを動作させることができます。
  無効化 SSL/TLSアップデートに戻ります。暗号化されたネットワークトラフィックについて通知するダイアログが表示されます。このアプリケーションが問題を解決したアプリケーションと一致し、証明書がアップデート元のサーバーから発行されていることを確認します。次に、この証明書のアクションを保存することを選択し、[無視]をクリックします。これ以上ダイアログが表示されない場合は、フィルタリングモードを自動に戻すことができます。問題は解決されます。
- 問題のアプリケーションがブラウザーまたは電子メールクライアントではない場合、Webアクセス保護から完全に除外できます(ブラウザーまたは電子メールクライアントでこの操作を実行すると、危険にさらされます)。過去に通信をフィルタリングしたアプリケーションは、例外を追加したときに既にリストに登録されています。このため、手動で追加する必要はありません。

## ネットワーク上のデバイスにアクセスする問題

ネットワーク上のデバイスの機能を使用できない場合(WebカメラのWebページを開けない、ホームメディアプレイヤーで動画を再生できない場合など)はIPv4およびIPv6アドレスを除外されたアドレスのリストに追加します。

## 特定のWebサイトの問題

URLアドレス管理を使用すると、Webアクセス保護から特定のWebサイトを除外できます。例えば、https://www.gmail.com/intl/en/mail/help/about.htmlにアクセスできない場合は、除外されたアドレス

のリストに*gmail.com*を追加します。

### エラー「ルート証明書をインポートできない一部のアプリケーションがまだ実行中です」

SSL/TLSを有効にするとESET Endpoint Antivirusは、証明書ストアに証明書をインポートしてSSLプロトコルをフィルタリングする方法をインストールされたアプリケーションが信頼するようにします。一部のアプリケーションは、証明書をインポートするために再起動が必要な場合があります。これにはFirefoxOperaがあります。これらのいずれも実行中ではないことを確認(最も簡単な方法では、タスクマネージャを開き、[プロセス]タブにfirefox.exeopera.exeが表示されていないことを確認)し、再試行をクリックします。

### 信頼できない発行元または無効なシグネチャに関するエラー

一般的に、前述のインポートが失敗したことを意味します。まず、前述のアプリケーションのいずれも実行されていないことを確認します。次に、SSL/TLSを無効にしてから再度有効にします。これでインポートが再実行されます。

## ネットワークの脅威がブロックされました

この状況は、コンピューターのアプリケーションがネットワーク上の別のデバイスに悪意のあるトラフィックを送信し、セキュリティホールを利用しようとしている場合やポート検査の試行が検出された場合に発生することがあります。

脅威のタイプと関連するデバイスIPアドレスは通知で確認できます。**この脅威の処理を変更**をクリックし、次のオプションを表示します。

**ブロックを続ける**– 検出された脅威をブロックします。特定のリモートアドレスからのこのタイプの脅威に関する通知の受信を停止する場合は、**通知しない**の横のラジオボタンを選択してから、**ブロックを続行**をクリックします。次の設定の侵入検出サービス(IDS)ルールが作成されます。**ブロック** – 既定、**通知** – いいえ、**ログ** – いいえ。

**許可** - 侵入検出サービス(IDS)ルールを作成し、検出された脅威を許可します。**許可**をクリックしてルール設定を指定する前に、次のオプションから1つ選択します。

- **この脅威がブロックされた場合にのみ通知** – ルール設定:**ブロック** – いいえ、**通知** – いいえ、**ログ** – いいえ。
- **この脅威が発生するたびに通知** – ルール設定:**ブロック** – いいえ、**通知** – 既定、**ログ** – 既定。
- **通知しない** – ルール設定:**ブロック** – いいえ、**通知** – いいえ、**ログ** – いいえ。

検出された脅威のタイプによっては、通知ウィンドウに表示される情報が異なる場合があります。脅威と他の関連用語の詳細については、リモート攻撃のタイプまたは検出のタイプを参照してください。
**ネットワークで重複するIPアドレス**イベントを解決するには、ESETナレッジベース記事を参照してください。

## Webとメール

インターネット接続はパーソナルコンピューターの標準機能ですが、悪意のあるコードを転送するための主要な方法にもなっています。プログラムのメインウィンドウ > **設定** > **Webとメール**を開いて、インターネット保護を強化するESET Endpoint Antivirus機能を設定します。

個別の保護モジュールを一時停止または無効にするには、トグルアイコンをクリックします。

保護モジュールをオフすると、コンピューターの保護レベルが低下する可能性があります。


保護モジュールの横の歯車アイコンをクリックし、そのモジュールの詳細設定にアクセスします。

Webアクセス保護は、HTTP/HTTPS通信を検査してマルウェアやフィッシングを検出しますWebアクセス保護をオフにするのは、トラブルシューティングの場合のみにしてください。

[フィッシング対策機能]では、フィッシングコンテンツを配布していることが判明しているWebページをブロックできます。フィッシング対策は有効にしたままにすることを強くお勧めします。

**フィッシングサイトを報告する** – 分析のためにフィッシング/悪意のあるWebサイトをESETに報告します。

ESETにWebサイトを提出する前に、次の基準の1つ以上を満たしていることを確認してください。
- Webサイトがまったく検出されない。
- Webサイトが誤ってウイルスとして検出される この場合は誤ってブロックされたページを報告できます。

[電子メールクライアント保護]ではPOP3(S)とIMAP(S)プロトコルで受信したメール通信が検査されますESET Endpoint Antivirusでは、メールクライアントのプラグインプログラムを使用して、メールクライアントからのすべての通信を検査できるようにしています。

# フィッシング対策機能

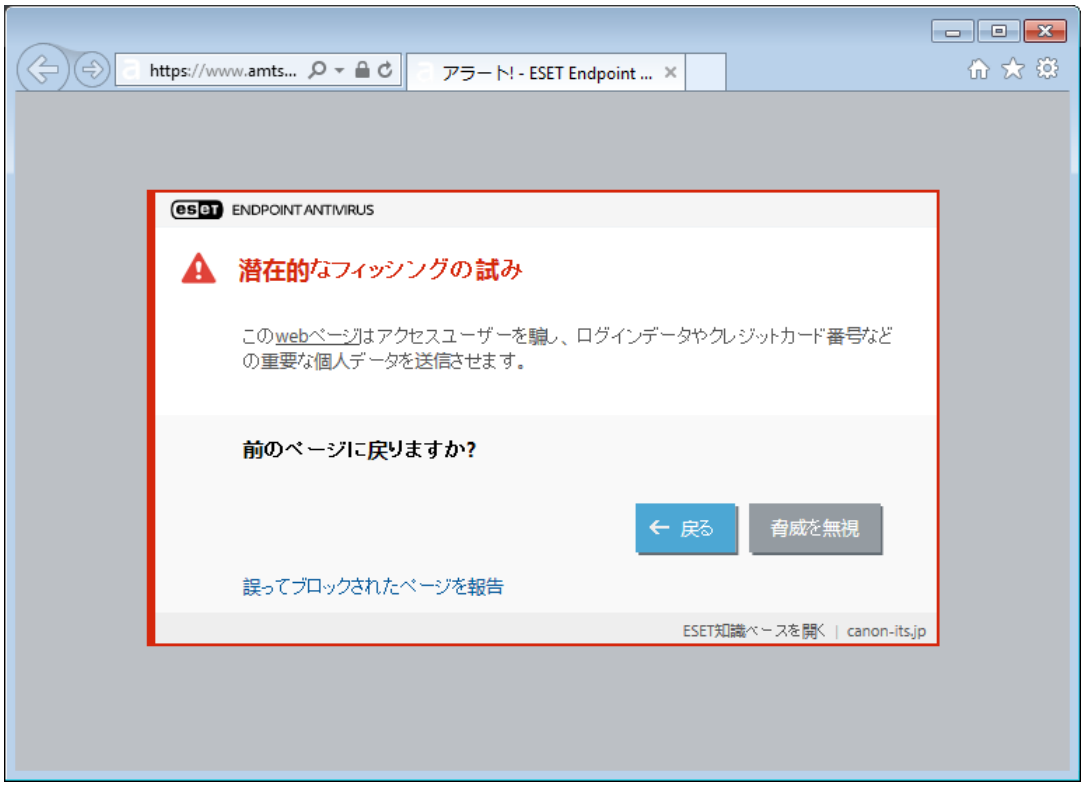
フィッシングはソーシャルエンジニアリング(機密情報を入手するためにユーザーを操る)を使用する犯罪活動です。フィッシングは、銀行の口座番号やPINなどの機密データにアクセスするために使用されます。詳細については、用語集を参照してください。ESET Endpoint Antivirusはフィッシング対策機能を提供し、このようなコンテンツを配布することが知られているWebページをブロックできます。

フィッシング対策機能は既定で有効です。この設定は、詳細設定 > **保護** > **Webアクセス保護**で設定できます。

ESET Endpoint Antivirusのフィッシング対策保護の詳細については、ナレッジベース記事を参照してください。

## フィッシングWebサイトにアクセスする

認識されているフィッシングWebサイトにアクセスすると、Webブラウザーに次のダイアログが表示されます。それでもWebサイトにアクセスする場合は、**[脅威を無視]**(推奨されません)をクリックします。




ホワイトリストに入れられた潜在的なフィッシングWebサイトは、既定では数時間後に有効期限が切れます。Webサイトを永続的に許可するには、URLアドレス管理ツールを使用します。詳細設定 > **保護** > **Webアクセス保護** > **URLアドレス管理** > **アドレスリスト** > **編集**で、編集するWebサイトをリストに追加します。

## フィッシングサイトを報告する

**誤ってブロックされたページを報告する**リンクを使用すると、誤って脅威として検出されたWebサイトを報告できます。

また、メールでWebサイトを提出することもできます。メールはsamples@eset.comに送信してください。わかりやすい件名にし、Webサイトに関する情報(参照元のWebサイト、このWebサイトを知った経緯な

ど)をできるだけ多く記載してください。

# 設定のインポート/エクスポート

**設定**メニューから、カスタマイズしたESET Endpoint Antivirus.xml設定ファイルをインポートまたはエクスポートできます。

> **図解手順**
> 英語および他の複数の言語で提供されている図解手順については、.xmlファイルを使用したESET構成設定のインポートまたはエクスポートを参照してください。

設定ファイルのインポートとエクスポートは、後で使用するためにESET Endpoint Antivirusの現在の設定をバックアップする必要がある場合に便利です。エクスポート設定オプションは、好みの基本設定を複数のシステムに対して使用する場合にも便利です。.xmlファイルをインポートして、設定を転送できます。

設定をインポートするには、メインプログラムウィンドウで**設定** > **設定のインポート/エクスポート**をクリックし、**設定のインポート**を選択します。設定ファイルのファイル名を入力するか、**...**ボタンをクリックして、インポートする設定ファイルを参照します。

設定をエクスポートするには、メインプログラムウィンドウで**設定** > **設定のインポート/エクスポート**をクリックします。**設定のエクスポート**を選択し、ファイル名を含むファイルの完全パスを入力します。**...**をクリックしてコンピューターの場所を参照し、設定ファイルを保存します。

> エクスポートしたファイルを指定したディレクトリに書き込むための十分な権限を持たない場合、設定のエクスポート中に、エラーが表示されることがあります。


# ツール

[**ツール**]メニューには、プログラム管理を容易にし、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。

- ログファイル
- 実行中のプロセス (ESET Endpoint AntivirusでESET LiveGrid®が有効になっている場合)
- セキュリティレポート (管理されていないエンドポイントの場合)
- ESET SysInspector
- スケジューラ
- 分析のためにサンプルを提出 – 分析のために不審なファイルをESET Research Labに提出します(ESET LiveGrid®の設定によっては使用できない場合があります)
- 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、ウイルスの検出、およびトラブルシューティングで重要なツールとして使用されます。ログへの記録はバックグラウンドでアクティブに実行され、ユーザーの操作を必要としません。情報は、ログの詳細レベルに関する現在の設定に基づいて記録されますESET Endpoint Antivirus環境から直接、テキストメッセージとログを表示することができます。ログファイルのアーカイブもできます。

ログファイルにアクセスするには、メインプログラムウィンドウで[**ツール**] > [**ログファイル**]をクリックします。[**ログ**]ドロップダウンメニューから目的のログタイプを選択します。使用可能なログは次のとおりです。

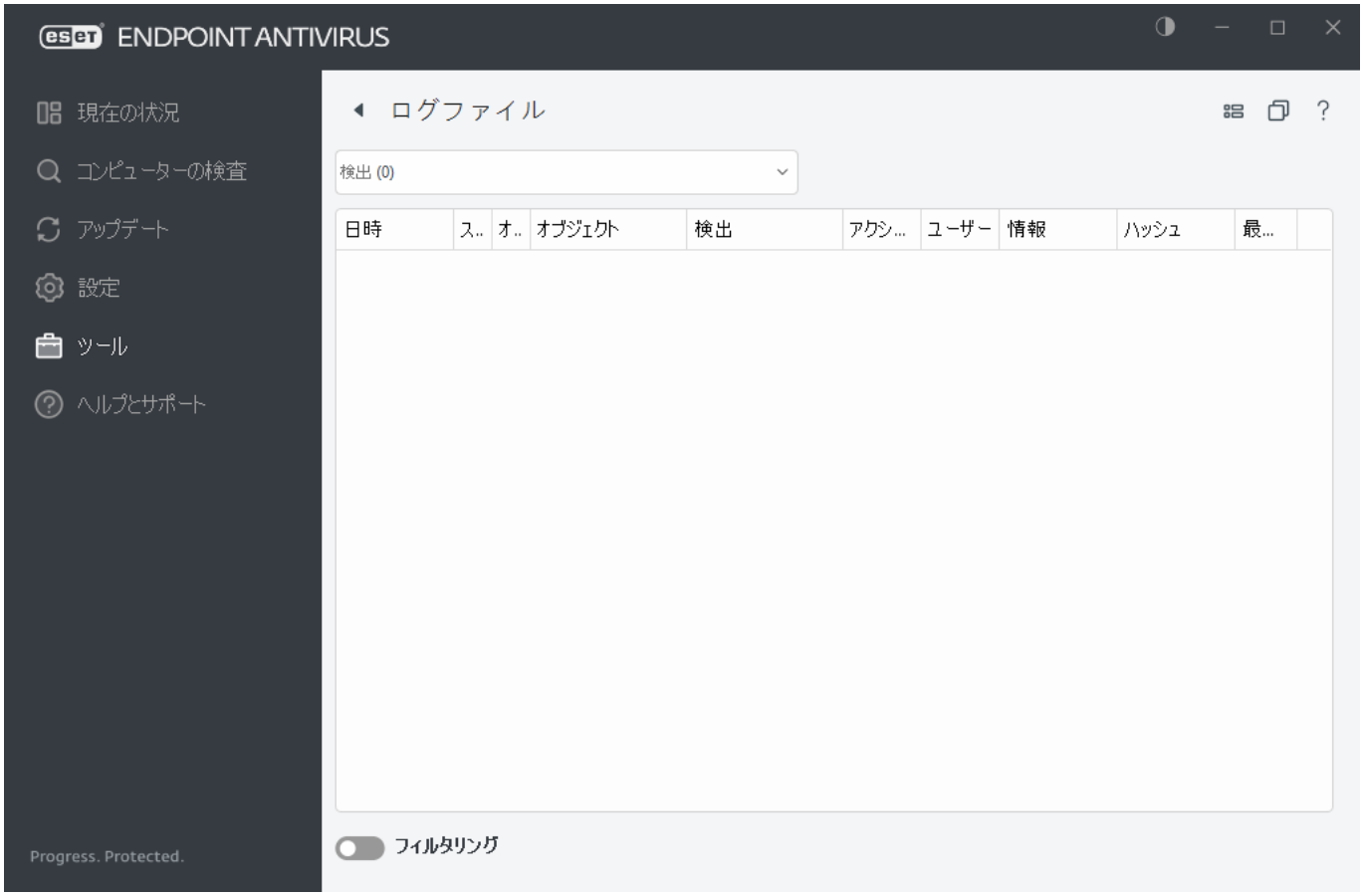
- **検出** – このログにはESET Endpoint Antivirusにより検知された検出と侵入についての詳細情報が記録されています。ログ情報には、検出時刻、検出の名前、場所、実行されたアクション、マルウェアの検出時にログインしていたユーザーの名前が含まれます。ログエントリーをダブルクリックすると、その詳細が別のウィンドウに表示されます。駆除されていない侵入は、常に、明るい赤色の背景に赤色のテキストで表示されます。駆除された侵入は、白色の背景に黄色のテキストで表示されます。駆除されていないPUAまたは安全でない可能性があるアプリケーションは、白

色の背景に黄色のテキストで表示されます。

- **イベント** – イベントログにはESET Endpoint Antivirus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。イベントログには、プログラムで発生したイベントやエラーに関する情報が格納されます。システム管理者およびユーザーが問題を解決するように設計されています。多くの場合、ここで見つかる情報は、プログラムで発生した問題の解決法の検出に役立ちます。
- **コンピューターの検査** – すべての検査結果はこのウィンドウに表示されます。各行は、個々のコンピューター制御に対応します。エントリーをダブルクリックすると、それぞれの検査結果の詳細が表示されます。
- **ブロックされたファイル** – ESET Enterprise Inspectorに接続したときに、ブロックされ、アクセスできなかったファイルのレコードを含みます。プロトコルはファイルをブロックした理由とソースモジュール、ファイルを実行したアプリケーションとユーザーを示します。詳細については、ESET Enterprise Inspectorオンラインユーザーガイドをご覧ください。
- **送信されたファイル** - ESET LiveGrid®またはESET LiveGuardに分析のために送信されたファイルのレコード。
- **監査ログ** – 各ログには、変更が実行された日時、変更のタイプ、説明、ソース、およびユーザーの情報が含まれます。詳細については、監査ログを参照してください。
- **HIPS** – 記録対象としてマークされた特定のルールのレコードが示されます。このプロトコルは、操作を呼び出したアプリケーション、結果(ルールが許可されたのか禁止されたのか)、および作成されたルール名を表示します。
- **ネットワーク保護** – ファイアウォールログには、ネットワーク攻撃保護(IDS)によって検出されたすべてのリモート攻撃が表示されます。 ここでは、コンピューターに対するすべての攻撃についての情報が見つかります。[イベント]列には検出された攻撃が表示されます。[ソース]列には、攻撃者の詳細が表示されます。[プロトコル]列には、攻撃に使用された通信プロトコルが表示されます。ファイアウォールのログを解析することにより、システムへ侵入しようとする試みを検知し、不正なアクセスの防止に役立つ場合があります。ネットワーク攻撃の詳細については、IDSおよび詳細オプションを参照してください。

- **フィルタリングされたWebサイト** – このリストは、Webアクセス保護によってブロックされたWebサイトのリストを表示する場合に便利です。 これらのログでは、特定のWebサイトへの接続を開いた時間URLユーザー、およびアプリケーションを確認できます。

- **デバイスコントロール** – コンピュータに接続されたリムーバブルメディアまたはデバイスの記録が含まれます。個別のデバイスコントロールルールが設定されているデバイスのみがログファイルに記録されます。接続されているデバイスとルールが一致しない場合には、接続されているデバイスのログエントリは作成されません。ここで、デバイスタイプ、シリアル番号、ベンダー名、メディアのサイズ(ある場合)などの詳細情報も確認できます。




ログの内容を選択し、`Ctrl + C`**を押してクリップボードにコピーします。**`Ctrl + Shift`を押して、複数のエントリを選択できます。

**フィルタリング**をクリックすると、フィルタリング条件を定義することができる ログフィルタリング ウィンドウが開きます。

特定のレコードを右クリックすると、コンテキストメニューが開きます。以下のオプションがコンテキストメニューに用意されています。

- **表示** – 新しいウィンドウで選択したログに関する詳細を表示します。
- **同じレコードをフィルタ表示** – このフィルターをアクティブにすると、同じタイプのレコード(診断、警告、など)だけが表示されます。
- **フィルタ** – このオプションをクリックすると、ログフィルタリングウィンドウで、特定のログエントリのフィルタリング条件を定義できます。
- **フィルタを有効にする** – フィルタ設定を有効にします。
- **フィルターを無効にする** – フィルターのすべての設定(上記)をクリアします。
- **コピー/すべてコピー** – ウィンドウにあるすべてのレコードに関する情報をコピーします。
- **セルをコピー** – 右クリックしたセルの内容をコピーします。
- **削除/すべて削除** – 選択されたレコードまたは表示されているすべてのレコードを削除します。このアクションには、管理者権限が必要です。
- **エクスポート** – レコードに関する情報をXML形式でエクスポートします。
- **すべてエクスポート** – レコードに関する情報をXML形式でエクスポートします。
- **検索/次を検索/前を検索** – このオプションをクリックした後、フィルタリング条件を定義し、ログフィルタリングウィンドウを使用して特定のエントリをハイライトすることができます。
- **除外の作成** – ウィザードを使用して新しい検出除外を作成します(マルウェア検出では使用できません)。

# ログのフィルタリング

ツール > **ログファイル**で **フィルタリング**をクリックして、フィルタリング条件を定義します。

ログフィルタリング機能では、特に、多数のレコードがあるときに、検索している情報を見つけることができます。特定のイベントのタイプ、ステータス、期間を検索する場合などに、ログレコードを絞り込むことができます。ログレコードをフィルタリングするには、特定の検索オプションを指定します。検索オプションに従って、関連するレコードのみがログファイルウィンドウに表示されます。

**テキスト検索**フィールドに検索するキーワードを入力します。**列を検索**ドロップダウンメニューを使用して、検索を絞り込みます。**レコードの種類**ドロップダウンメニューから、1つ以上のレコードを選択します。結果を表示する**期間**を定義します。**完全一致のみ**または**大文字と小文字を区別する**などの詳細検索オプションも使用できます。

## テキスト検索

文字列(単語、特定の単語)を入力します。この文字列を含むレコードのみが表示されます。他のレコードは省略されます。

## 列を検索

検索時に考慮される列を選択します。検索で使用する列を1つ以上チェックできます。

## レコードの種類

ドロップダウンメニューからログレコードの種類を1つ以上選択します。

- **診断** – 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をログに記録します。
- **情報** – 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。
- **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。
- **エラー** – 「ファイルのダウンロード中にエラーが発生しました」といったエラーや重大なエラーを記録します。
- **重大** – 重大なエラー(ウイルス対策保護の開始エラー)

## 期間

結果を表示する期間を指定します:

- **未指定**(既定) – 期間で検索せず、ログ全体を検索します。
- **昨日**
- **先週**
- **先月**
- **期間** – 正確な期間(開始日と終了日)を指定して、特定の期間のレコードのみをフィルタリングできます。

## 完全一致のみ

より正確な結果を得るために完全一致のみで検索する場合に、このチェックボックスをオンにします。

## 大文字と小文字を区別する

フィルタリング時に大文字または小文字を使用することが重要な場合、このオプションを**有効**にします。フィルタリング/検索オプションを設定した後、**OK**をクリックして、フィルタリングされたログレコードを表示するか、検索で検索を開始します。ログファイルは、現在の位置(ハイライトされたレコード)から、上から下に検索されます。最初の一致するレコードが見つかると、検索が停止します。**F3**を押すと、次のレコードを検索します。右クリックして**検索**を選択すると、検索オプションを絞り込みます。

# 監査ログ

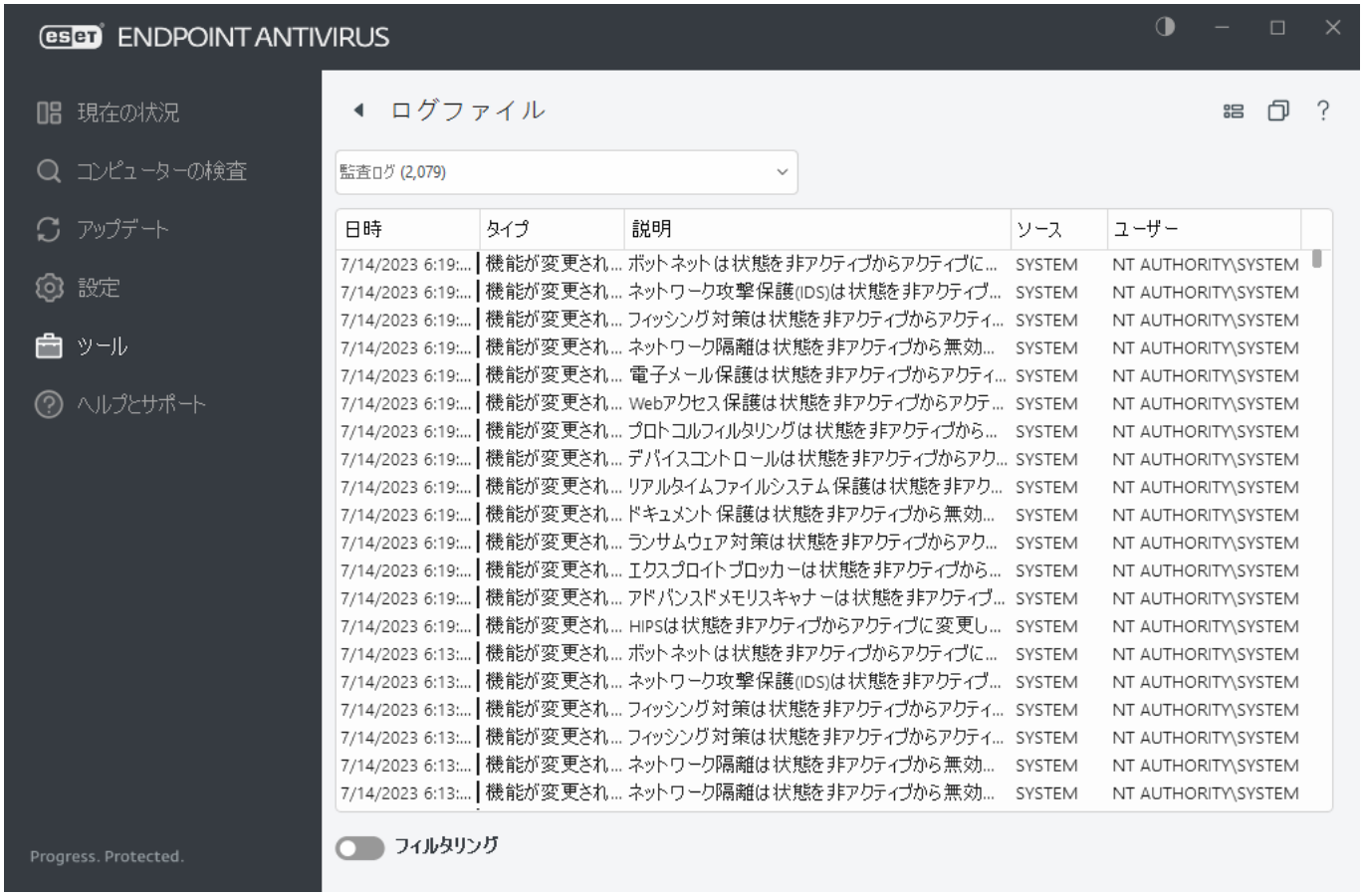
エンタープライズ環境では、通常、エンドポイントを設定するためのアクセス権が定義された複数のユーザーが存在します。製品設定の修正は製品の動作方法に大きく影響する可能性があるため、管理者がユーザーが行った変更を追跡し、問題をすばやく特定および解決し、詳細に同じまたは同様の問題が発生することを防止できるようにすることが重要です。

監査ログは、新しいタイプのログであり、問題の根本を特定するのに役立ちます。監査ログは、設定または保護状態の変更を追跡し、後から参照するためにスナップショットを記録します。

**監査ログ**を表示するには、メインメニューで**ツール**をクリックしてから、**ログファイル**をクリックして、ドロップダウンメニューから**監査ログ**を選択します。

監査ログには次の情報が含まれます。

- 時間– 変更が実行された日時
- タイプ – 変更された設定または機能の種類
- 説明 – 正確な変更の内容、変更された設定の部分、および変更された設定の数
- ソース – 変更の場所
- ユーザー – 変更を行ったユーザー




ログファイルウィンドウで監査ログの**設定変更**タイプを右クリックし、コンテキストメニューから**変更を表示**を選択して、実行された変更に関する詳細情報を表示します。さらに、コンテキストメニューから**復元**をクリックすると、設定変更を復元できます(ESET PROTECTで管理されている製品では使用不可)。コンテキストメニューから**すべて削除**を選択すると、このアクションに関する情報のログが作成されます。

**詳細設定** > ツール > **ログファイル**で**自動的にログファイルを最適化**を有効にする場合、監査ログは自動的に他のログとして分断されます。

**詳細設定** > ツール > **ログファイル次の日数が経過したエントリを自動的に削除**を有効にすると、指定された日数を経過したログエントリは自動的に削除されます。

# 実行中のプロセス

実行中のプロセスは、コンピューター上で実行中のプログラムまたはプロセスを表示し、新規のウイルスを即座にESETに通知し、その通知を継続しますESET Endpoint Antivirusは実行中のプロセスについて詳細な情報を提供し、ESET LiveGrid®技術を有効にしてユーザーを保護します。


**レピュテーション** – 多くの場合、ESET Endpoint AntivirusおよびESET LiveGrid®技術では、各オブジェクトの特性を検証して悪意のあるアクティビティである可能性に重み付けする一連のヒューリスティックルールを使用して、オブジェクト(ファイル、プロセス、レジストリキーなど)に危険レベルが割り当てられます。これらのヒューリスティックに基づいて、オブジェクトに9 – 良好(緑)、0 – 危険(赤)のリスクレベルが割り当てられます。

**プロセス** – コンピューターで現在実行中のプログラムまたはプロセスのイメージ名。Windowsタスクマネージャを使用して、コンピューターで動作中のプロセスすべてを表示することもできます。タスクマネージャを開くには、タスクバーの何もない領域で右クリックしてから[タスクマネージャ]をクリックするか、またはキーボードで**Ctrl+Shift+Esc**を押します。

**PID** - Windowsオペレーティングシステムで実行中のプロセスのID

緑のマークの付いた既知のアプリケーションは、感染していないことが判明しており(ホワイトリストに記載)、検査から除外されます。これは、コンピューターでの[コンピュータの検査]または[リアルタイムファイルシステム保護]の検査速度を向上させるための仕組みです。

**ユーザー数** – 指定されたアプリケーションを使用するユーザーの数。この情報は、ESET LiveGrid®技術によって収集されます。

**初回発見日** - ESET LiveGrid®技術によってアプリケーションが検出された日付。

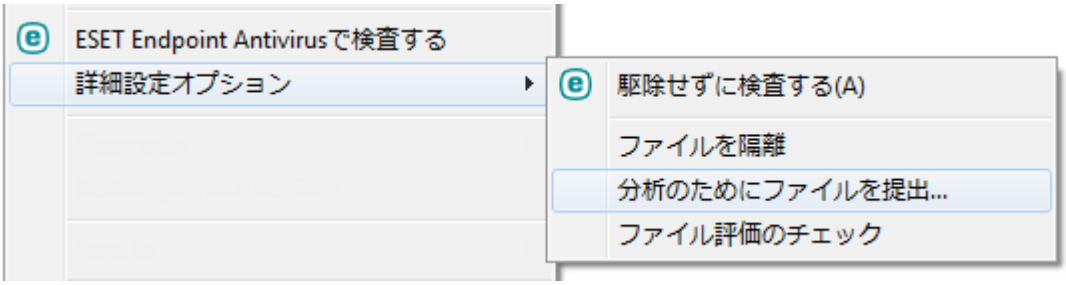
アプリケーションが不明(オレンジ)のセキュリティレベルのマークを付けられていても、必ずしも悪意のあるソフトウェアというわけではありません。通常は、単に新しいアプリケーションというだけです。ファイルについて不明点がある場合は、分析のためにファイルを提出機能を使用してESETのウイルスラボにファイルを送信できます。そのファイルが悪意のあるアプリケーションであることが判明すると、それ以降のいずれかの検出エンジンアップデートファイルにその検出が追加されます。

**アプリケーション名** – プログラムまたはプロセスの特定の名前。

下部の特定のアプリケーションをクリックすることにより、次の情報がウィンドウ下部に表示されます。

- **パス** – コンピューター上のアプリケーションの場所。
- **サイズ** – ファイルサイズがKB(キロバイト単位)またはMB(メガバイト単位)のいずれか。
- **説明** – オペレーティングシステムからの情報に基づくファイル特性。
- **会社** – ベンダーまたはアプリケーションプロセスの名前。
- **バージョン** – アプリケーション発行元からの情報。
- **製品** – アプリケーション名および/または商号。
- **作成日** – アプリケーションが作成された日時。
- **変更日** – アプリケーションが最後に変更された日時。

評価は、実行中のプログラム/プロセスとして動作しないファイルに対してもチェックできます – チェックするファイルをマークして右クリックし、コンテキストメニューから[**詳細オプション**] > [**ESET LiveGrid®を使用したファイル評価のチェック**]を選択します。




# セキュリティレポート

この機能は、次のカテゴリの統計情報の概要を示します。

- **ブロックされたWebページ** – ブロックされたWebページ数を表示します(PUA、フィッシング、ハッキングされたルータ、IPまたは証明書のブラックリストに登録されたURL)。
- **検出された感染した電子メールオブジェクト** – 検出された感染した電子メールオブジェクト数を表示します。
- **検出されたPUA** – 検出された望ましくない可能性のあるアプリケーション(PUA)数を表示します。
- **検査されたドキュメント** – 検査された文書オブジェクト数を表示します。
- **検査されたアプリ** – 検査された実行可能なオブジェクト数を表示します。
- **検査された他のオブジェクト** – 他の検査されたオブジェクト数を表示します。
- **検査されたWebページオブジェクト** – 検査されたWebページオブジェクト数を表示します。
- **検査された電子メールオブジェクト** – 検査された電子メールオブジェクト数を表示します。

これらのカテゴリは、降順の数値に基づいています。ゼロ値のカテゴリは表示されません。[**詳細表示...**]をクリックすると、非表示のカテゴリを展開して表示します。

右上端で歯車⚙をクリックすると、**セキュリティレポート通知を有効/無効にする**か、過去30日間のデータが表示されるか、製品がアクティベーションされた時点以降のデータが表示されるかどうかを選択します。ESET Endpoint Antivirusのインストール期間が30日未満の場合、インストール日数のみを選択できます。30日間の期間は既定で設定されます。


**データのリセット**は、すべての統計情報をクリアし、セキュリティレポートの既存のデータを削除します。**詳細設定** > ユーザーインターフェース > **通知** > **対話アラート**で**統計情報をリセットする前に確認する**オプションをオフにした場合を除き、このアクションを確認する必要があります。

# ESET SysInspector

ESET SysInspectorは、コンピューターを徹底的に検査し、ドライバーやアプリケーション、ネットワーク接続、重要なレジストリーエントリーなどのシステムコンポーネントについて詳細な情報を収集し、コンポーネントごとのリスクレベルを評価するアプリケーションです。この情報で、ソフトウェアやハードウェアの互換性の問題やマルウェア感染が原因と思われる疑わしいシステム動作を判別することができます。ESET SysInspectorの使用方法については、ESET SysInspectorオンラインヘルプを参照してください。

ESET SysInspectorウィンドウには、ログに関する次の情報が表示されます。

- **日時** – ログ作成時刻。
- **コメント** – 短いコメント。
- **ユーザー** – ログを作成したユーザーの名前。
- **状態** – ログ作成の状態。

使用できるアクションは次のとおりです。

- **表示** – 選択したログをESET SysInspectorで開きます。また、特定のログファイルを右クリックして、メニューから[**表示**]を選択できます。
- **作成** – 新しいログを作成します。ログにアクセスを試行する前に、ESET SysInspectorが生成される(**作成済み**ステータス)まで待機します。ログはC:\ProgramData\ESET\ESET Security\SysInspectorに保存されます。
- **削除** – 選択したログをリストから削除します。

次の項目は、1つ以上のログファイルが選択されたときに、コンテキストメニューから使用できます。

- **表示** - ESET SysInspectorで選択したログを開きます(ログをダブルクリックするのと同じ機能)。
- **作成** – 新しいログを作成します。ログにアクセスを試行する前に、ESET SysInspectorが生成される(**作成済み**ステータス)まで待機します。
- **削除** – 選択したログをリストから削除します。
- **すべて削除** – すべてのログを削除します。
- **エクスポート** - .xmlファイルまたは圧縮された.xmlにログをエクスポートします。

# スケジューラ

スケジューラーでは、スケジュールされたタスクが、あらかじめ定義された設定やプロパティと共に管理され、開始されます。

スケジューラーにはESET Endpoint Antivirusのメインプログラムウィンドウから[**ツール**] > [**スケジューラ**]をクリックしてアクセスできます。**スケジューラー**には、スケジュール済みのすべてのタスクと設定プロパティ(あらかじめ定義した日付、時刻、使用する検査プロファイルなど)の一覧が表示されます。

スケジューラーは次のタスクのスケジュールを行います。検出エンジンアップデート、検査タスク、システムの起動時におけるファイルの検査、およびログの保守。スケジューラーのメインウィンドウから直接、タスクの追加または削除を行うことができます(下部にある[**タスクの追加**]または[**削除**]をクリックします)。[スケジューラ]ウィンドウ内で右クリックすると、次のアクションを実行できます。 詳細情報の表示、タスクの即時実行、新しいタスクの追加、および既存のタスクの削除。タスクをアクティブ/非アクティブにするには、各エントリーの最初にあるチェックボックスを使用します。

既定では、次のスケジュールされたタスクが**スケジューラ**に表示されます。

- **ログの保守**
- **定期的に自動アップデート**
- **ダイヤルアップ接続後に自動アップデート**
- **ユーザーログオン後に自動アップデート**
- **自動スタートアップファイルのチェック**(ユーザーのログオン後)
- **自動スタートアップファイルのチェック**(モジュールの正常なアップデート後)

ESET PROTECTでは、特に大型ネットワークの場合には、タスクの実行時のサーバー負荷を軽減できます。このオプションを使用して、ネットワーク全体のすべてのワークステーションでタスクを同時に実行するのとは対照的に、ネットワーク全体でタスクを実行する時間範囲を定義できます。タスクの実行時には、設定された時間値がランダムにセグメント化されて、ネットワーク上の各ワークステーションごとにそれぞれ独自のタスク実行時間が割り振られます。これにより、サーバーの過負荷やその関連問題(たとえば、ネットワーク全体を通してワークステーション上で全体アップデートを同時に実行するときにDoS攻撃が報告される場合があります)。

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


# 新しいタスクの追加

1. ウィンドウの一番下にある[**タスクの追加**]をクリックします。
2. タスク名を入力します。
3. ドロップダウンメニューから目的のタスクを選択します。

- **外部アプリケーションの実行** – 外部アプリケーションの実行をスケジュールします。
- **ログの保守** –ログファイルには削除されたレコードの痕跡も収められています。このタスクは、効率的に運用するためにログファイル内のレコードを定期的に最適化します。
- **システムのスタートアップファイルのチェック** – システムの起動時またはログインに実行されるファイルを検査します。
- **コンピュータの状態のスナップショットを作成する** – ドライバーやアプリケーションなどのシステムコンポーネントについての情報を収集し、各コンポーネントのリスクレベルを評価するESET SysInspectorコンピュータスナップショットを作成します。
- **オンデマンドコンピュータの検査** – コンピュータ上のファイルやフォルダに関するコンピュータの検査を実行します。
- **アップデート**– 検出エンジンおよびプログラムモジュールをアップデートすることにより、アップデートタスクをスケジュールします。

4. タスクを有効にする場合(スケジュールされたタスクのリストでチェックボックスをオン/オフにして後から操作できます)は、[**有効**]をオンにし、[**次へ**]をクリックして、タイミングオプションのいずれかを選択します。

- **1回** – あらかじめ定義した日時にタスクが実行されます。
- **繰り返し** – 指定した間隔でタスクが実行されます。
- **毎日** – 毎日、指定した時刻に繰り返しタスクが実行されます。
- **毎週** – 選択した曜日と時刻にタスクが実行されます。
- **イベントごと** – 指定したイベントの発生時にタスクが実行されます。

5. [**コンピューターがバッテリーで動作している場合は実行しない**]を選択すると、ノートブックコンピュータのバッテリ電源での実行中に、システムリソースを最小化できます。タスクは、**タスクの実行**フィールドで指定された日時に実行されます。あらかじめ定義した時刻にタスクが実行されなかった場合、タスクを再度実行する時期を指定することができます。

- **次のスケジュール設定日時まで待機**
- **実行可能になり次第実行する**
- **すぐに、前回の実行からの時間が指定した値を超えた場合は (前回実行からの時間** スクロールボックスを使用して間隔を定義できます)

スケジュールされたタスクを確認するには、タスクを右クリックして**タスクの詳細を表示**をクリックします。

# スケジュールされた検査オプション

このウィンドウで、スケジュールしたコンピューターの検査タスクの詳細オプションを指定できます。

駆除アクションなしで検査を実行するには、**詳細設定**をクリックし、**駆除せずに検査する**を選択します。スキャンに関する情報は、スキャンログに保存されます。

**除外を無視**を選択すると、以前スキャンから除外された拡張子を持つファイルも、例外なくスキャンされます。

ドロップダウンメニューを使用して、検査の完了後に自動的に実行されるアクションを設定できます。

- **アクションなし** – 検査が完了しても、アクションは実行されません。
- **シャットダウン** – 検査完了後にコンピュータがオフになります。
- **再起動** – 検査完了後に、開いているプログラムをすべて終了し、コンピュータを再起動します。
- **必要に応じて再起動** – 検出された脅威の駆除を完了するために必要な場合にのみ、コンピューターを再起動します。
- **強制的に再起動** – ユーザー操作を待機せずにすべての開いているプログラムを強制的に閉じ、検査が完了した後にコンピューターを再起動します。
- **必要に応じて強制再起動** – 検出された脅威の駆除を完了するために必要な場合にのみ、コンピューターを再起動します。
- **スリープ** – セッションを保存し、コンピュータを低電力モードにするため、作業を迅速に再開できます。
- **休止** - RAMで実行中のものをすべて取り込み、ハードディスクの特定のファイルに移動します。コンピュータはシャットダウンしますが、次回の起動時に元の状態から再開されます。

> **スリープ**または**休止**アクションは、オペレーティングシステムのコンピューターの電源およびスリープ設定またはコンピューター/ノートブック機能に基づいて使用できます。コンピュータをスリープにしても、コンピュータは動作しています。基本機能は実行され続け、コンピュータがバッテリで動作している場合は、電力を使用します。バッテリの持続時間を長くするために、オフィス外での移動中などには、休止オプションを使用することをお勧めします。

**検査をキャンセルできない**を選択すると、権限がないユーザーは、検査後に実行されたアクションを停止できません。

一部のユーザーが指定した期間にコンピュータ検査を一時停止できるようにする場合は、**ユーザーによる検査一時停止可能時間**オプションを選択します。

検査の進行状況も参照してください。

# スケジュールタスクの概要

カスタムタスクをダブルクリックするか、カスタムスケジューラタスクを右クリックして**[タスクの詳細を表示]**をクリックすると、このダイアログウィンドウには、選択したスケジュールタスクに関する詳細情報が表示されます。

# タスク詳細

**タスク名**を入力し、**タスクの種類**のいずれかを選択して、**次へ**をクリックします。

- **外部アプリケーションの実行** – 外部アプリケーションの実行をスケジュールします。
- **ログの保守** –ログファイルには削除されたレコードの痕跡も収められています。このタスクは、効率的に運用するためにログファイル内のレコードを定期的に最適化します。
- **システムのスタートアップファイルのチェック** – システムの起動時またはログインに実行されるファイルを検査します。
- **コンピュータの状態のスナップショットを作成する** – ドライバーやアプリケーションなどのシステムコンポーネントについての情報を収集し、各コンポーネントのリスクレベルを評価するESET SysInspectorコンピュータスナップショットを作成します。
- **オンデマンドコンピュータの検査** – コンピュータ上のファイルやフォルダに関するコンピュータの検査を実行します。
- **アップデート**– モジュールをアップデートすることにより、アップデートタスクをスケジュールします。

# タスクタイミング

指定した間隔でタスクが繰り返し実行されます。タイミングオプションのいずれかを選択します。

- **1回** – 事前定義した日時にタスクを1回だけ実行します。
- **繰り返し** – 指定した間隔(時間単位)でタスクが実行されます。
- **毎日** – 毎日、指定した時刻にタスクが実行されます。
- **毎週** – 1週間に1回以上、選択した曜日と時刻にタスクが実行されます。
- **イベントごと** – 指定したイベントが発生すると、タスクが実行されます。

**コンピューターがバッテリーで動作している場合は実行しない** – タスクの実行時にコンピュータがバッテリで動作している場合は、タスクが開始されません。これは、コンピュータがUPSで動作している場合にも当てはまります。

# タスクのタイミング – 1回

**タスクの実行** – 指定したタスクは、指定した日時に1回だけ実行されます。

# タスクのタイミング – 毎日

毎日、指定した時刻にタスクが実行されます。

# タスクのタイミング – 毎週

毎週選択した日時にタスクが繰り返し実行されます。

# タスクのタイミング – イベントのトリガー

次のイベントのいずれかによってタスクが開始されます。

- **コンピュータの起動時**
- **一日の最初のコンピュータ起動時**
- **インターネット/VPNへのダイヤルアップ接続**
- **モジュールアップデートが成功しました。**
- **製品アップデート成功**
- **ユーザのログオン**
- **ウイルスの検出**

イベントによって開始されるタスクをスケジュールする際には、タスクを実行する最短間隔を指定することができます。たとえば、1日に複数回、コンピュータにログオンする場合、その日および翌日の初回ログオン時にのみタスクを実行するには、24時間を選択します。

# タスクが実行されなかった場合

タスクは、コンピューターの電源がオフか、バッテリで動作している場合はスキップできます。これらのオプションのいずれかからスキップされたタスクを実行する時間を選択し、**次へ**をクリックします。

- **次のスケジュール設定日時まで待機** – 次回のスケジュールされた日時にコンピューターがオンになっている場合は、タスクが実行されます。
- **実行可能になり次第実行する** – コンピューターがオンのときにタスクが実行されます。
- **前回のスケジュール実行以降の時間(時間)を超えた場合は即時** – タスクの最初にスキップされた実行から経過した時間を表します。この時間を超えると、タスクがただちに実行されます。

## 前回のスケジュール実行以降の時間(時間)を超えた場合は即時 – 例

例のタスクは、1時間ごとに繰り返し実行される設定です。**前回のスケジュール実行以降の時間(時間)を超えた場合は即時**オプションが選択され、経過時間が2時間に設定されています。タスクは13:00に実行され、完了するとコンピューターはスリープ状態になります。

- コンピューターは15:30にウェイクアップします。最初にスキップされたタスクの実行は14:00です。14:00から1時間半しか経過していないため、タスクは16:00に実行されます。
- コンピューターは16:30にウェイクアップします。最初にスキップされたタスクの実行は14:00です。14:00から2時間半経過したため、タスクはただちに実行されます。

# タスクの詳細 – アップデート

2つのアップデートサーバからプログラムをアップデートする場合、2つの異なるアップデートプロファイルを作成する必要があります。最初のサーバでアップデートファイルのダウンロードに失敗すると、自動的に次のサーバに切り替えられます。これは、通常はローカルLANのアップデートサーバーからアップデートを行っているが、別のネットワークからインターネットに接続することも多いノートパソコンなどに最適です。その場合、最初のプロファイルが失敗すると、次のプロファイルが自動的にESETの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ます。

# タスクの詳細 – アプリケーションの実行

このタスクでは、外部アプリケーションの実行をスケジュールすることができます。

**実行可能ファイル** - **...**オプションをクリックするか手動でパスを入力して、ディレクトリツリーから実行可能ファイルを選択します。

**作業フォルダ** – 外部アプリケーションの作業ディレクトリを指定します。選択した**実行可能ファイル**のすべての一時的なファイルは、このディレクトリに作成されます。

**パラメーター** – アプリケーションのコマンドラインパラメーター(任意)。

[**完了**]をクリックすると、タスクが適用されます。

# 分析用サンプルの提出

コンピューター上の疑わしいファイル、またはインターネット上の疑わしいサイト見つかった場合は、ESETのリサーチラボに提出して解析を受けることができます(ESET LiveGrid®の構成によっては使用できない場合があります)。

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

サンプル送信では、次の方法のいずれかを使用して、分析のためにファイルまたはサイトをESETに送信できます。

1. サンプル送信の使用は、**ツール > 分析のためにサンプルを提出**にあります。
2. また、メールでファイルを提出することもできます。この方法を希望する場合は、WinRAR/ZIPを使用してファイルを圧縮し、アーカイブを"infected"というパスワードで保護し、samples@eset.comに送信してください。
3. 迷惑メールまたは迷惑メールの誤検知を報告するには、ESETナレッジベース記事を参照してください。

**分析のためのサンプルを選択**を開き、以下の**サンプル提出の理由**ドロップダウンメニューから、お客様が伝えたい内容に最も近いものを選択します。

- 不審なファイル
- 不審なウェブサイト(何らかのマルウェアに感染しているWebサイト)
- 誤検出ファイル(感染と検出されたが未感染であるファイル)
- 誤検出サイト
- その他

**ファイル/サイト** – 提出するファイルその他Webサイトへのパスを入力します。

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

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。毎日、何万ものファイルがサーバーに送られてくるので、すべての提出に返信することはできません。
サンプルが悪意のあるアプリケーションやWebサイトであることが判明すると、その後のESETアップデートファイルにその検出が追加されます。

# 分析のためにサンプルを提出 – 不審なファイル

**観察されたマルウェア感染の兆候および症状** – コンピューター上にある不審なファイルの動作の説明を入力します。

**ファイルの入手元(URLアドレスまたはベンダ)** – ファイルの入手元(ソース)と、このファイルを入手方法のメモを入力してください。

**備考および補足情報** – ここには、不審なファイルの判別処理の助けとなる追加情報または説明を入力します。

1つ目のパラメーターである[**観察されたマルウェア感染の兆候および症状**]は必須ですが、補足情報もご提供いただくと、研究所でのサンプルの特定および処理に非常に役立ちます。

# 分析のためにサンプルを提出 – 不審なウェブサイト

[**サイトの問題点**]ドロップダウンメニューで以下のうち1つを選択してください。

- **感染** – ウイルス、またはさまざまな方法で配布される他のマルウェアが含まれるWebサイト。
- [**フィッシング**] – 銀行の口座番号やPINコードなどの機密データを入手するためによく使用されます。この攻撃の詳細については、「用語集」を参照してください。
- [**詐欺**] – 簡単にお金を手に入れることを主な目的とした、詐欺または偽装Webサイト。
- 送信するサイトに上記のオプションが該当しない場合は、[**その他**]を選択します。

[**備考および補足情報**] – ここには、不審なWebサイトを分析するときの助けとなる追加情報または説明を入力します。

# 分析のためにサンプルを提出 – 誤検出ファイル

感染していると検出され、実際には感染していないファイルは、ウイルス対策およびフィッシング対策のエンジンの向上と他のお客様の保護のために、送信してくださるようお願いします。ファイルのパターンが検出エンジンのパターンと一致する場合、誤検出(FP)が発生する場合があります。

**アプリケーション名およびバージョン** – プログラム名とバージョン(番号、エイリアスまたはコード名など)。

**ファイルの入手元(URLアドレスまたはベンダ)** – ファイルの入手元(ソース)と、このファイルの入手方法のメモを入力してください。

**アプリケーションの目的** – アプリケーションの概要、アプリケーションの種類(ブラウザ、メディアプレーヤなど)、その機能などを入力します。

**備考および補足情報** – ここには、不審なファイルを処理する際に役立つ追加情報または説明を入力できます。

3つのパラメーターは、アプリケーションが正当なものであるかどうかを識別し、悪意のあるコードと区別するために必要です。補足情報をご提供いただくと、研究所でのサンプルの特定および処理の際に大いに役立ちます。

# 分析のためにサンプルを提出 – 誤検出サイト

感染、詐欺、またはフィッシングと検出され、実際には感染していないサイトは、送信してくださるようお願いします。ファイルのパターンが検出エンジンのパターンと一致する場合、誤検出(FP)が発生する場合があります。ウイルス対策およびフィッシング対策のエンジンの向上と他のお客様の保護のために、そのようなWebサイトはご報告ください。

**備考および補足情報** – ここには、不審なWebサイトを処理する際に役立つ追加情報または説明を入力できます。

# 分析のためにサンプルを提出 – その他

ファイルを**不審なファイル**または**誤検出**に分類できない場合は、このフォームを使用します。

**ファイル提出の理由** – ファイル送信に関する詳細な説明と送信理由を入力します。

# 隔離

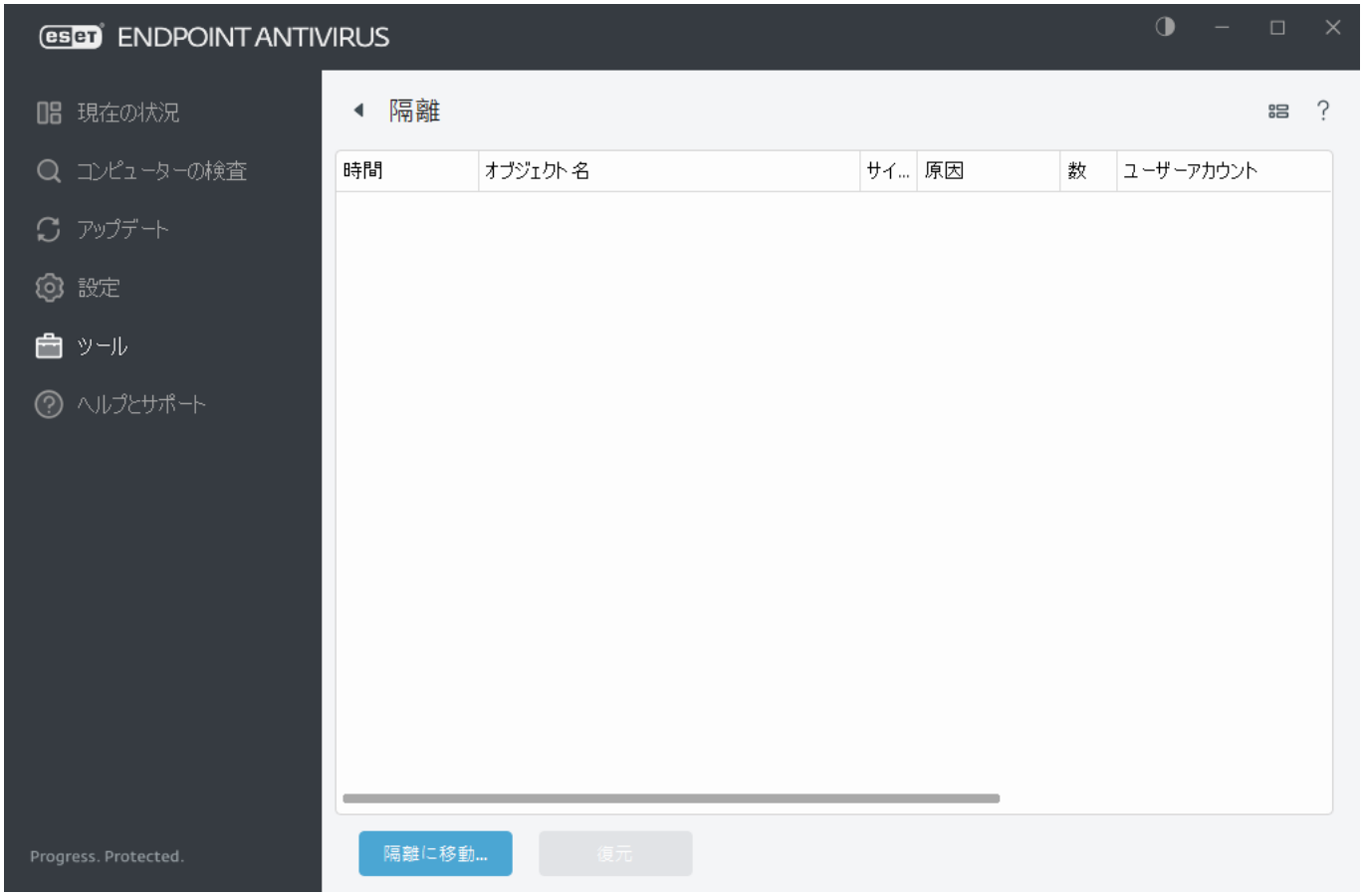
隔離の主な機能は、報告されたオブジェクト(マルウェア、感染したファイル、望ましくない可能性のあるアプリケーションなど)を安全な方法で保存することです。

隔離にはESET Endpoint Antivirusのメインプログラムウィンドウから**ツール > 隔離**をクリックしてアクセスできます。

隔離フォルダーに保存されているファイルについては、表形式で次の情報が表示されます。

- 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(ユーザーが追加したオブジェクトなど)、
- 検出数(同じファイルの重複した検出、複数の侵入を含むアーカイブの場合)。

リモートでクライアントワークステーションの隔離を管理する




# ファイルの隔離

ESET Endpoint Antivirus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。

次の場合は、追加のファイルを隔離することをお勧めします。

- 駆除できない
- 安全でないか、削除することが推奨される
- ESET Endpoint Antivirusによって誤って検出された場合
- ファイルが不審な動作をしているが、スキャナーで検出されない

ファイルを隔離するには、次の複数のオプションがあります。

- ドラッグアンドドロップ機能を使って、ファイルをクリックすると、マウスボタンを押したままマウスポインターをマークした箇所に移動してからマウスボタンを放すと、そのファイルやフォルダーを手動で隔離します。その後、アプリケーションが前面に移動します。
- メイン プログラムウィンドウで**隔離に移動...**をクリックします。
- この操作にはコンテキストメニューも使用することができます。**隔離**ウィンドウ内で右クリックし、**隔離**を選択します。

# 隔離フォルダーからの復元

隔離されたファイルは元の場所に復元することもできます。

- この目的のために**復元**機能を使用するには、隔離内の特定のファイルを右クリックして、コンテキストメニューを使用します。
- ファイルが望ましくない可能性があるアプリケーションに設定されている場合、**復元および検査時に除外**オプションが有効になります。「除外」も参照してください。

- コンテキストメニューには、**復元先を指定**オプションもあります。このオプションを使用すると、削除される前の場所とは異なる場所にファイルを復元することができます。
- 復元機能は、読み取り専用のネットワーク共有上にあるファイルなど、使用できない場合があります。

## 隔離から削除する

特定の項目を右クリックし、**隔離フォルダからの削除**を選択するか、削除する項目を選択し、キーボードの**Delete**を押します。複数の項目を選択して、一度に削除することもできます。削除された項目は完全にデバイスと隔離から削除されます。

## 隔離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や、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、分析するためサンプルをESET研究所に送信してください。ファイルを提出するには、ファイルを右クリックし、コンテキストメニューから**分析のために提出**を選択します。

次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
- ESET PROTECT で隔離を管理する
- ESET製品で検出が通知されました。何をすればよいですか。

# ヘルプとサポート

プログラムのメインウィンドウの**ヘルプとサポート**をクリックすると、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とトラブルシューティングツールが表示されます。

**インストールされている製品**

- ESET Endpoint Antivirus について - ESET Endpoint Antivirusに関する情報が表示されます。
- 製品のトラブルシューティング – 最もよくある問題の解決策を見つけるには、このリンクをクリックします。
- ライセンスのトラブルシューティング – このリンクをクリックすると、アクティベーションまたはライセンス変更の問題の解決策を検索します。
- ライセンスの変更 – 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。

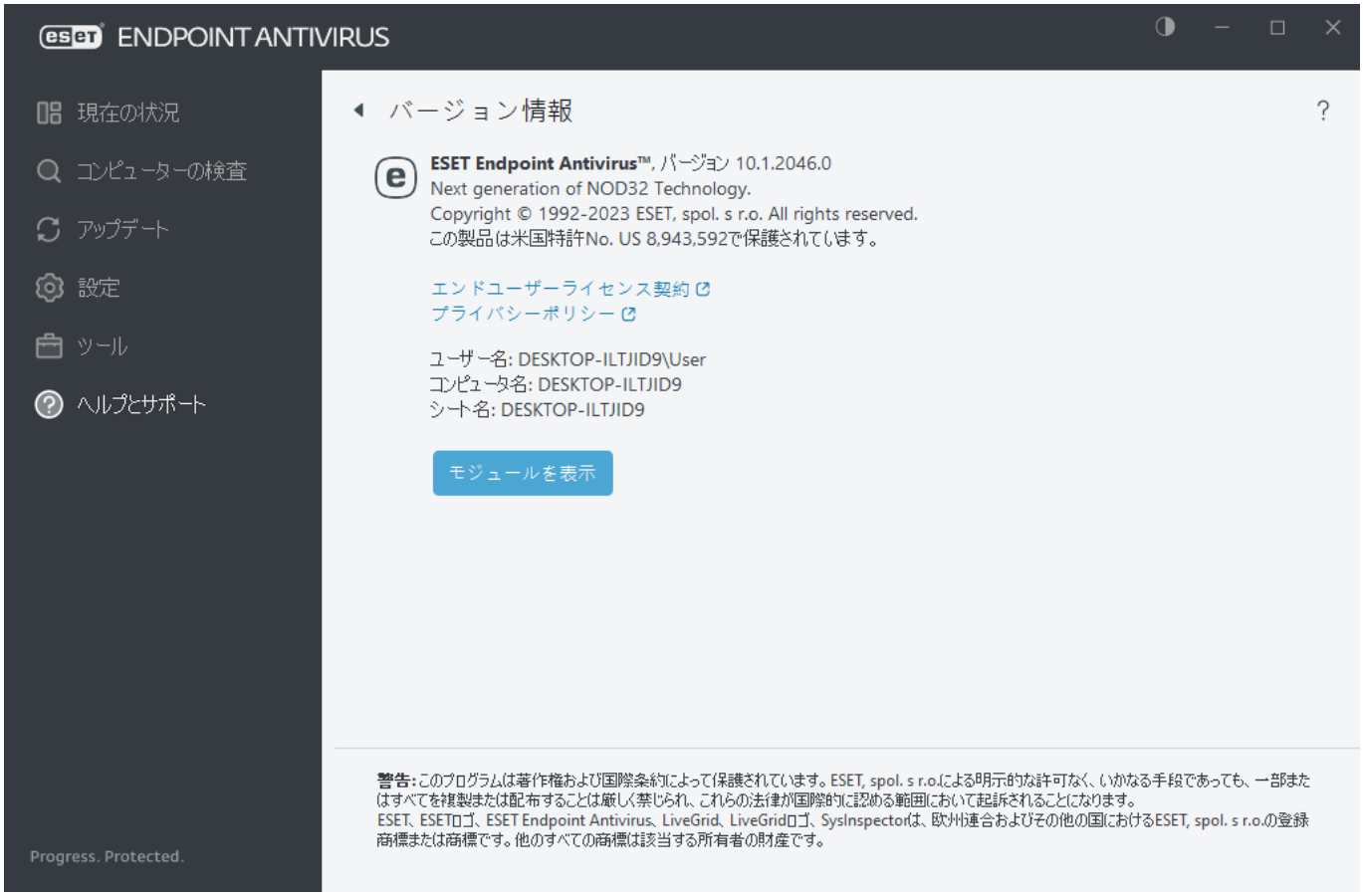
**ヘルプページ** – このリンクをクリックするとESET Endpoint Antivirusヘルプページが開きます。

テクニカルサポート

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

# ESET Endpoint Antivirusの概要

このウィンドウには、インストールされたESET Endpoint Antivirusのバージョンとコンピューターの詳細情報が表示されます。




**モジュールを表示**をクリックすると、読み込まれたプログラムモジュールの一覧が表示されます。

- [**コピー**]をクリックして、モジュールに関する情報をクリップボードにコピーできます。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。
- モジュールウィンドウで**検出エンジン**をクリックし、ESETウイルスレーダーを開きます。ここにはESET検出エンジンの各バージョンに関する情報が表示されます。

# システム構成データの送信

できるかぎり迅速かつ正確にサポートを提供するためにESETは、ESET Endpoint Antivirus構成、詳細なシステム情報、実行中のプロセス(ESET SysInspectorログファイル)、およびレジストリデータに関する情報を必要としていますESETはお客様に技術支援を提供するためにのみこのデータを使用します。

Webフォームを送信すると、システム設定データもESETに送信されます。この処理を記憶する場合は、**常に送信**を選択します。Webフォームをデータを送信せずに提出するには、**データを送信しない**をクリックして続行します。

システム設定データの送信は、詳細設定 > **ツール** > **診断** > テクニカルサポートで設定できます。

システム設定データを送信する場合は、Webフォームに入力して送信する必要があります。そうでないと、チケットは作成されず、システム設定データは失われます。システム設定データを送信できない場合は、Webフォームに入力し、テクニカルサポートからの指示を待ちます。

# テクニカルサポート

メインプログラムウィンドウで、**ヘルプとサポート > テクニカルサポート**をクリックします。

## テクニカルサポートに問い合わせる

**サポートを依頼** – 問題の回答が見つからない場合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Web フォームを入力する前に、設定に基づいて、システム構成データの送信ウィンドウが表示されます。

## テクニカルサポート情報

**テクニカルサポート詳細** – メッセージが表示された場合、情報をコピーして ESETテクニカルサポートに送信できます（ライセンス詳細情報、製品名、製品バージョン、オペレーティングシステム、コンピューター情報など）。

**ESET Log Collector** - ESETナレッジベース記事へのリンク。問題をより迅速に解決するためにコンピュータから情報とログを自動的に収集するアプリケーションである ESET Log Collector ユーティリティをダウンロードできます。詳細については、ESET Log Collectorオンラインユーザーガイドをご覧ください。

詳細ログを有効にすると、開発者が問題を診断および解決するために、すべての使用可能な機能の詳細ログを作成できます。最小ログ詳細レベルは、**診断**に設定されています。**詳細ログの停止**をクリックして停止しない場合、詳細ログは、2時間後に自動的に無効にされます。すべてのログが作成されるときには、通知ウィンドウが表示され、診断フォルダーと作成されたログに直接アクセスできます。

# 詳細設定

詳細設定を使用すると、ニーズに合わせて詳細なESET Endpoint Antivirus設定を設定できます。

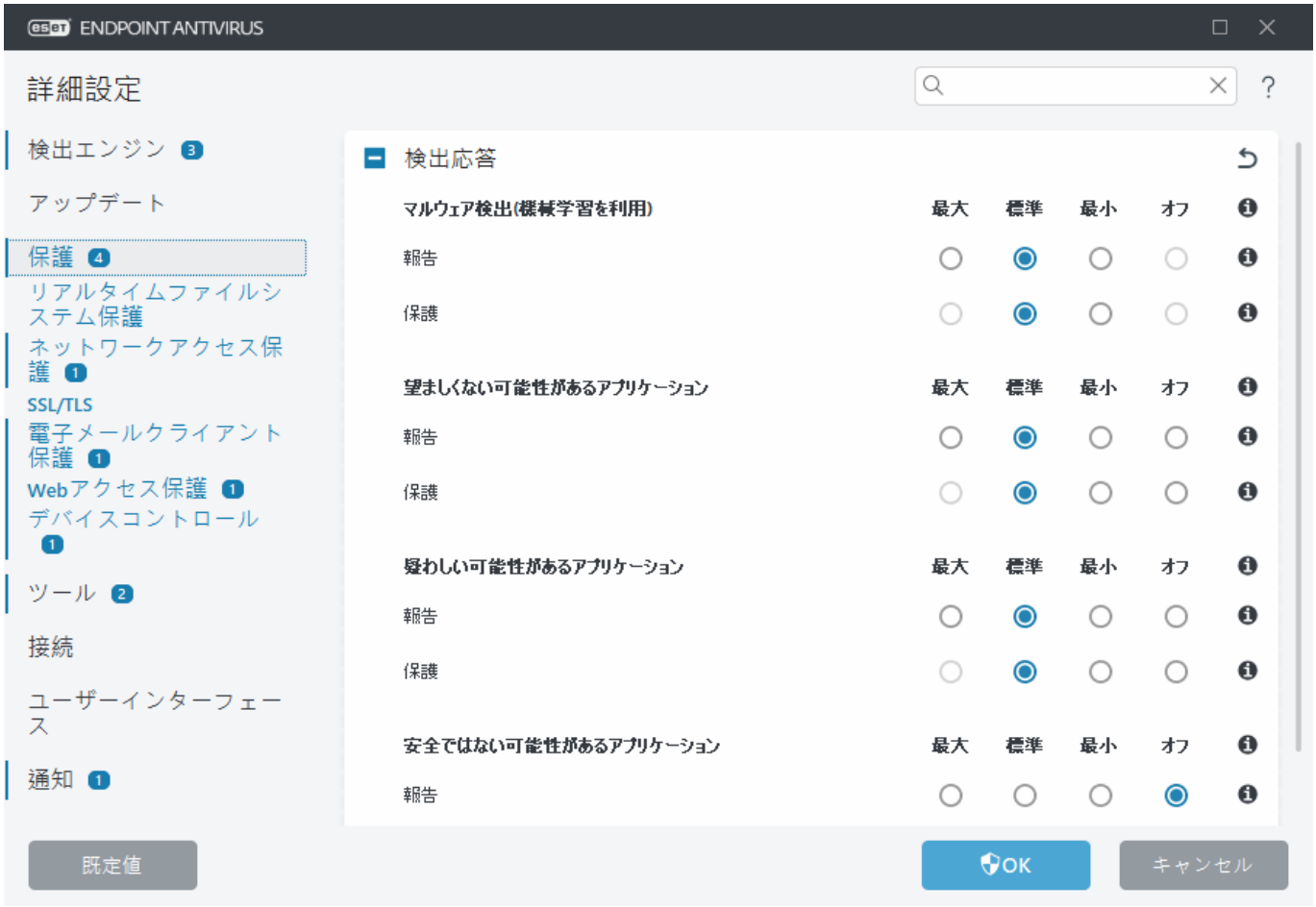
詳細設定を開くには、プログラムのメインウィンドウを開き、キーボードの**F5**キーを押すか、**設定 > 詳細設定**をクリックします。

ESET PROTECT Webコンソールからポリシーを作成するときには、各設定のフラグを選択できます。強制フラグの設定には優先度があり、後のポリシーに強制フラグがある場合でも、後のポリシーによって上書きすることはできません。こうすると、この設定が変更されない（たとえばユーザーによって、またはマージ中に後のポリシーによって）ことが保証されます。詳細情報については、ESET PROTECTオンラインヘルプのフラグを参照してください。

アクセス設定によっては、詳細設定を開くためのパスワードの入力を求められる場合があります。

詳細設定では、次の設定を設定できます。

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




# 検出エンジン

詳細設定 > **検出エンジン**で、次のオプションを設定できます。

- 除外
- 詳細設定オプション
- ネットワークトラフィックスキャナー

# 除外

**除外**では、オブジェクトを検出エンジンから除外することができます。すべての対象で検査されるように、絶対に必要な場合を除いては、除外を作成しないことをお勧めします。対象を除外する必要がある場合もあります。たとえば、検査中にコンピューターの速度を低下させる恐れのある大きなデータベースエントリーや、検査と競合するソフトウェアなどです。

パフォーマンス除外 – ファイルとフォルダーを検査から除外できます。パフォーマンス除外は、ファイルレベルでのゲームアプリケーションの検査を除外したり、異常なシステム動作やパフォーマンスが増加したときに便利です。

検出除外では、検出名、パス、またはハッシュを使用して、オブジェクトを駆除から除外します。検出除外は、パフォーマンス除外と違い、ファイルとフォルダーを検査から除外しません。検出除外は、検出エンジンで検出され、適切なルールが除外リストにあるときにのみ、オブジェクトを除外します。

他の種類の除外と混同しないでください。

- プロセス除外 – 除外されたすべてのアプリケーションプロセスに関連するすべてのファイル操

作が検査から除外されます(バックアップ速度とサービスの可用性を向上させるために必要になる場合があります)。
- 除外されたファイル拡張子
- HIPS除外
- クラウドベース保護の除外フィルター

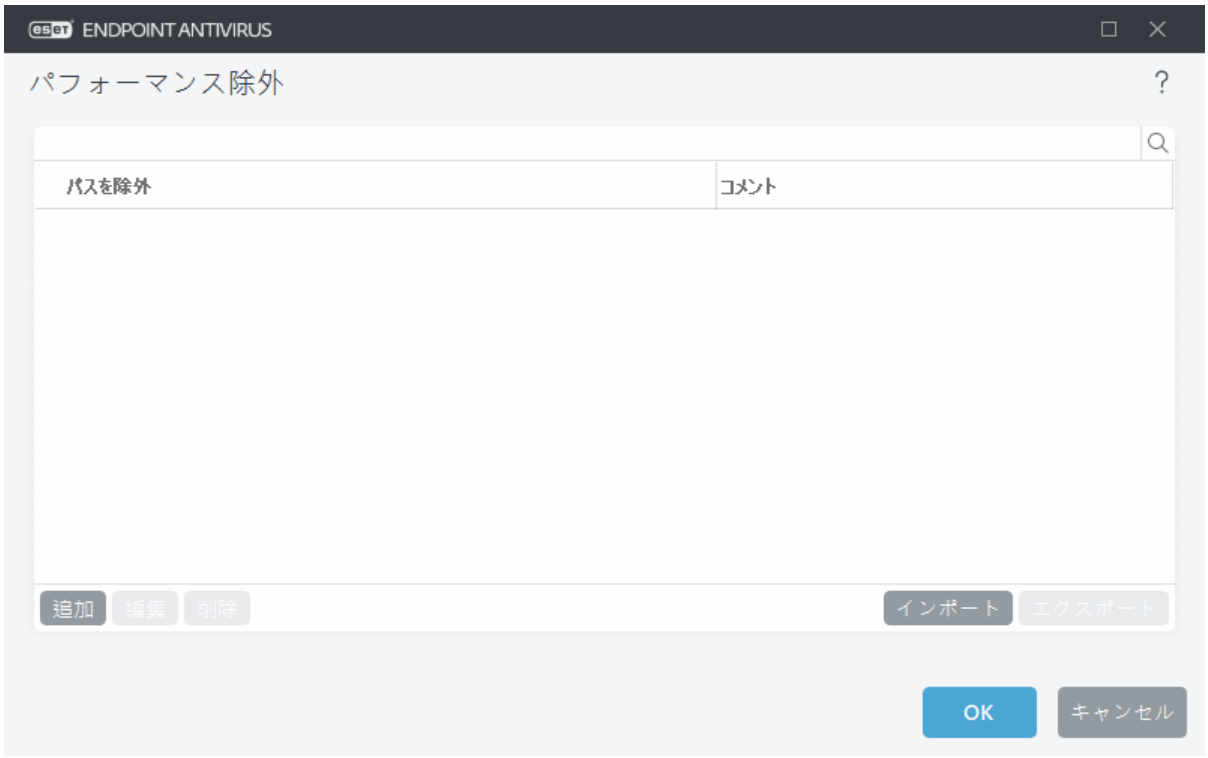
# パフォーマンス除外

パフォーマンス除外では、ファイルとフォルダーを検査から除外できます。

すべての対象で脅威が検査されるように、絶対に必要な場合を除いては、除外を作成しないことをお勧めします。しかし、対象を除外する必要がある場合もあります。たとえば、検査中にコンピューターの速度を低下させる恐れのある大きなデータベースエントリーや、検査と競合するソフトウェアなどです。

詳細設定 > **検出エンジン** > **除外** > **パフォーマンス除外** > **追加**で、検査から除外するファイルとフォルダーを除外のリストに追加できます。

オブジェクト(パス：ファイルまたはフォルダ)を検査から除外するには、**追加**をクリックして、アプリケーションパスを入力するか、ツリー構造でパスを選択します。




ファイルがスキャンからの除外基準に適合すると、**リアルタイムファイルシステム保護**モジュールまたは**コンピューターの検査**モジュールはファイル内の脅威を検出しません。

## コントロール要素

- **追加** – オブジェクトを検査から除外する新しいエントリを追加します。
- **編集** – 選択したエントリーを編集します。
- **削除** – 選択したエントリを削除します(CTRLを押しながらクリックすると、複数のエントリを選択できます)。
- **インポート/エクスポート** – パフォーマンス除外のインポートとエクスポートは、後で使用する

ためにの現在の除外をバックアップする必要がある場合に便利です。エクスポート設定オプションは、管理サーバで管理されていない環境で任意の除外設定を複数のシステムに対して適用する場合にも便利です。.txtファイルを簡単にインポートして、設定を展開できます。

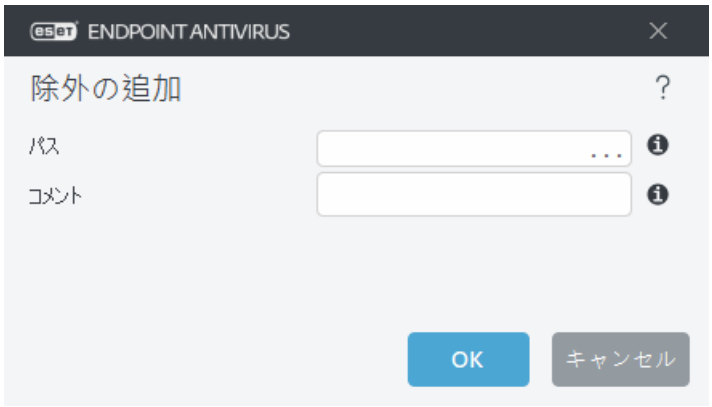
インポート/エクスポートファイル形式の例を表示する

```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.PerformanceExclusions","columns":["Path","Description"]}

C:\Backup\*,custom comment

C:\pagefile.sys
```

# パフォーマンス除外の追加または編集

このダイアログウィンドウは、このコンピューターの特定のパス(ファイルまたはディレクトリ)を除外します。

該当するパスを選択するには、**パス**フィールドで**...**をクリックします。手動で入力するときには、以下の除外形式の例を参照してください。




---

ワイルドカードを使用すると、複数のファイルを除外することができます。疑問符(*?*)は1つの文字を表し、アスタリスク(*)は0文字以上の文字列を表します。

- フォルダー内のすべてのファイルとサブフォルダーを除外する場合は、フォルダーのパスを入力し、*のようにワイルドカードを使用します。
- docファイルのみを除外する場合は、マスク**.doc*のようにワイルドカードを使用します。
- 実行可能ファイルの名前に特定数の文字が使用されており(それぞれの文字は異なります)、最初の文字(たとえば"D")のみが明らかな場合は、次の形式を使用します。
*D????.exe*(疑問符は、不足している文字または不明な文字の代わりに使用されます)

例:

- *C:\Tools** – パスの最後にはバックスラッシュ(\)とアスタリスク(*)を指定して、フォルダーとフォルダーの内容すべて(ファイルとサブフォルダー)が除外されることを示す必要があります。
- *C:\Tools*.* - C:\Tools**と同じ動作
- *C:\Tools* – *Tools*フォルダーは除外されません。スキャナーの観点から、*Tools*をファイル名にすることもできます。
- *C:\Tools*.dat* – これは、*Tools*フォルダーの.datファイルを除外します。
- *C:\Tools\sg.dat* – 正確なパスにあるこの特定のファイルを除外します

*%PROGRAMFILES%*などのシステム変数を使用して、検査除外を定義できます。
• このシステム変数を使用してProgram Filesフォルダーを除外するには、除外に追加するときに、パス*%PROGRAMFILES%**(必ずパスの最後にバックスラッシュとアスタリスクを追加すること)を使用します。
• *%PROGRAMFILES%*サブディレクトリのすべてのファイルとフォルダーを除外するには、パス*%PROGRAMFILES%\Excluded_Directory**を使用します。

サポートされるシステム変数のリストを展開する

次の変数は、パス除外形式で使用できます。
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*

ユーザー固有のシステム変数(*%TEMP%*または*%USERPROFILE%*など)、あるいは環境変数(*%PATH%*など)はサポートされていません。

パフォーマンス除外で正式にサポートされていないため、パスの中間でワイルドカードを使用する(例: *C:\Tools*\Data\file.dat*)と、正常に動作しない場合があります。詳細については、次のナレッジベース記事を参照してください。
検出除外を使用するときには、パスの中央でワイルドカードを使用することに関する制限はありません。

除外の順序:
• 上下ボタンを使用して、除外の優先度レベルを調整するオプションはありません。。
• スキャナーによって最初に適用されるルールが一致すると、2番目に適用されるルールは評価されません。
• ルールが少ないほど、検査のパフォーマンスが向上します。
• 同時ルールの作成を避ける。

# パス除外形式

ワイルドカードを使用すると、複数のファイルを除外することができます。疑問符(*?*)は1つの文字を表し、アスタリスク(*)は0文字以上の文字列を表します。

• フォルダー内のすべてのファイルとサブフォルダーを除外する場合は、フォルダーのパスを入力し、*のようにワイルドカードを使用します。
• docファイルのみを除外する場合は、マスク**.doc*のようにワイルドカードを使用します。
• 実行可能ファイルの名前に特定数の文字が使用されており(それぞれの文字は異なります)、最初の文字(たとえば"D")のみが明らかな場合は、次の形式を使用します。
*D????.exe*(疑問符は、不足している文字または不明な文字の代わりに使用されます)
例:
• *C:\Tools** – パスの最後にはバックスラッシュ(\)とアスタリスク(*)を指定して、フォルダーとフォルダーの内容すべて(ファイルとサブフォルダー)が除外されることを示す必要があります。
• *C:\Tools*.*- C:\Tools**と同じ動作
• *C:\Tools* – *Tools*フォルダーは除外されません。スキャナーの観点から、*Tools*をファイル名にすることもできます。
• *C:\Tools*.dat* – これは、*Tools*フォルダーの. datファイルを除外します。
• *C:\Tools\sg.dat* – 正確なパスにあるこの特定のファイルを除外します

*%PROGRAMFILES%*などのシステム変数を使用して、検査除外を定義できます。
• このシステム変数を使用してProgram Filesフォルダーを除外するには、除外に追加するときに、パス*%PROGRAMFILES%**(必ずパスの最後にバックスラッシュとアスタリスクを追加すること)を使用します。
• *%PROGRAMFILES%*サブディレクトリのすべてのファイルとフォルダーを除外するには、パス*%PROGRAMFILES%\Excluded_Directory**を使用します。

サポートされるシステム変数のリストを展開する

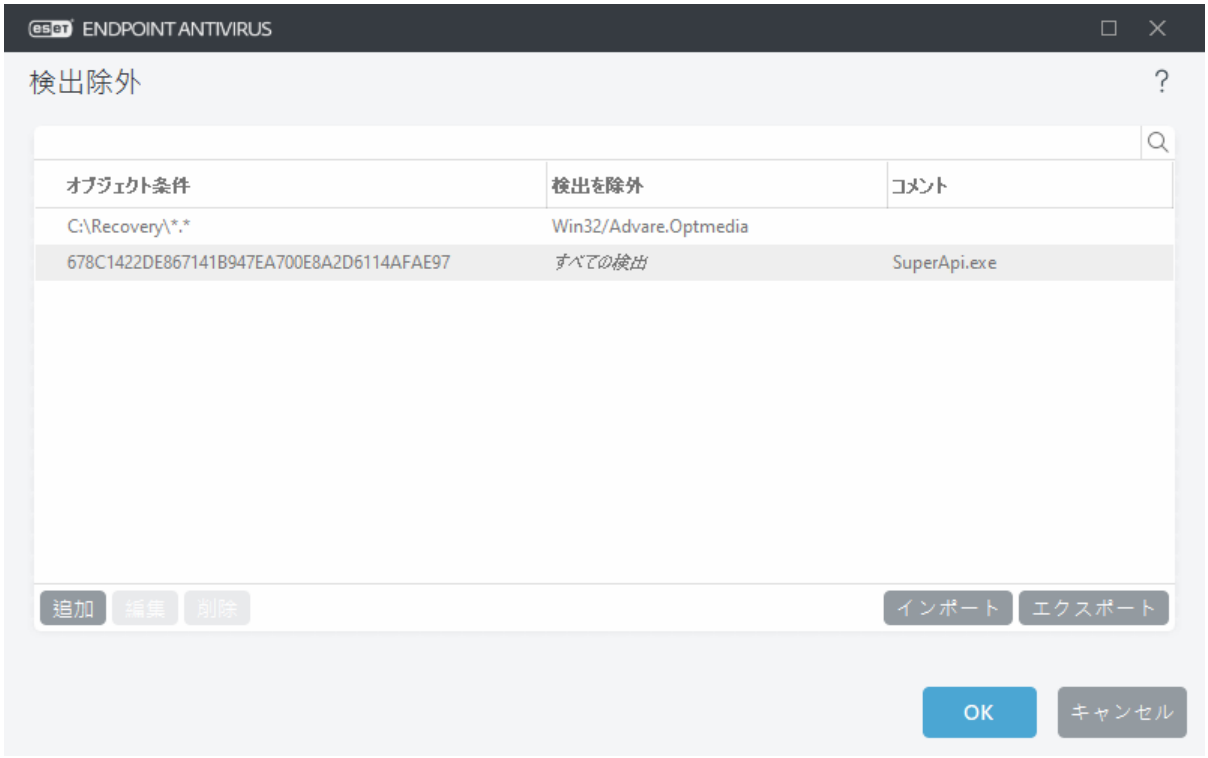
次の変数は、パス除外形式で使用できます。
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*

ユーザー固有のシステム変数(*%TEMP%*または*%USERPROFILE%*など)、あるいは環境変数(*%PATH%*など)はサポートされていません。

# 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。

検出除外は、パフォーマンス除外と違い、ファイルとフォルダーを検査から除外しません。検出除外は、検出エンジンで検出され、適切なルールが除外リストにあるときにのみ、オブジェクトを除外します。
たとえば(以下の画像の最初の行を参照)、オブジェクトがWin32/Adware.Optmediaとして検出され、検出されたファイルが*C:\Recovery\file.exe*のときです。2番目の行では、適切なSHA-1ハッシュがある各ファイルは、検出名に関係なく、常に除外されます。




すべての脅威を確実に検出するために、絶対に必要なときにのみ検出除外を作成することをお勧めします。

ファイルとフォルダを除外リストに追加するには、詳細設定 > **検出エンジン** > **除外** > **検出除外** > **編集**を開きます。

駆除から(検出名またはハッシュで)オブジェクトを除外するには、**追加**をクリックします。

望ましくない可能性があるアプリケーションと安全でない可能性があるアプリケーションの場合、次の方法で、検出名による除外も作成できます。

- 検出を報告するアラートウィンドウで**詳細オプションを表示**をクリックし、**検出から除外を選択**します。
- 検出除外の作成ウィザードを使用するログファイルコンテキストメニュー。
- **ツール** > **隔離**をクリックし、隔離されたファイルを右クリックし、コンテキストメニューから**復元および検査時に除外**を選択して作成できます。

## 検出除外オブジェクト条件

- **パス** – 指定されたパス(またはすべて)の検出除外を制限します。
- **検出名** – 除外されるファイルの横に検出の名前がある場合、ファイルは特定の検出に対してのみ除外され、完全には除外されません。このファイルが後で他のマルウェアに感染した場合は検出されます。
- **ハッシュ** – 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。

## コントロール要素

- **追加** – オブジェクトを駆除から除外する新しいエントリを追加します。
- **編集** – 選択したエントリーを編集します。

- **削除** – 選択したエントリを削除します(CTRLを押しながらクリックすると、複数のエントリを選択できます)。
- **インポート/エクスポート** – 検出除外のインポートとエクスポートは、後で使用するための現在の除外をバックアップする必要がある場合に便利です。エクスポート設定オプションは、管理サーバで管理されていない環境で任意の除外設定を複数のシステムに対して適用する場合にも便利です。.txtファイルを簡単にインポートして、設定を展開できます。

  インポート/エクスポートファイル形式の例を表示する

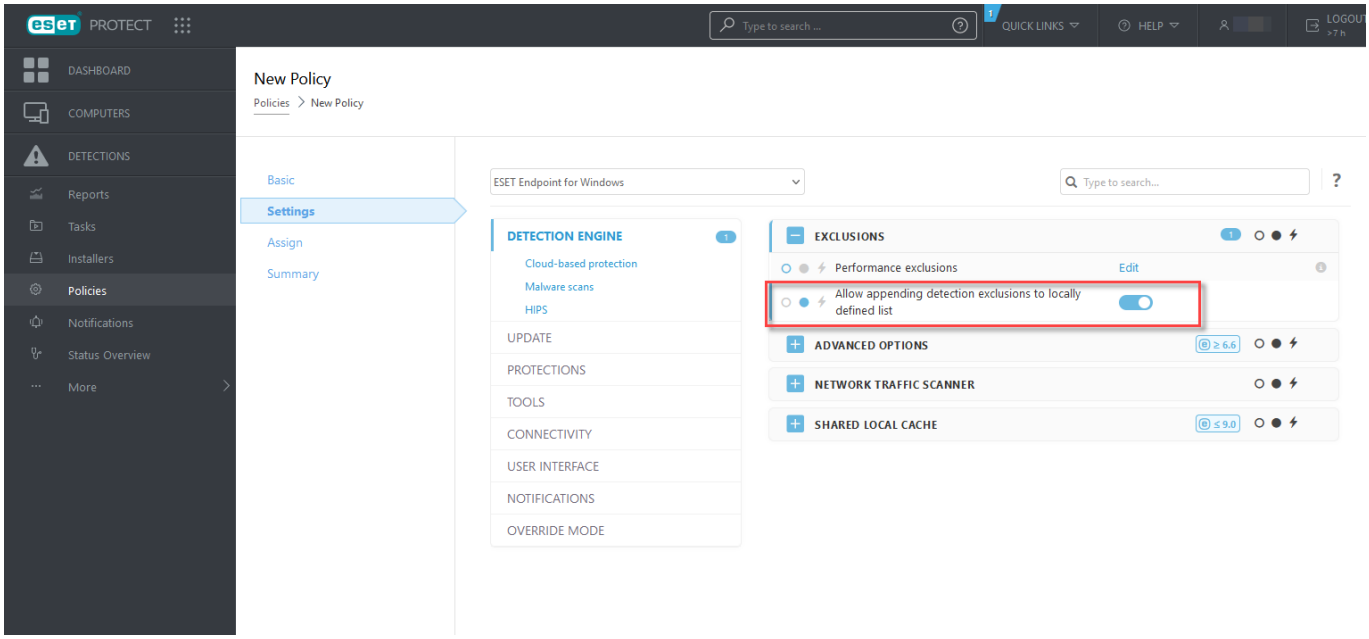
```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","FileHash"]}

4c59cd02-357c-4b20-a0ac-ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF

2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,
```

## ESET PROTECTでの検出除外設定

ESET PROTECT検出除外管理ウィザード – 検出除外を作成し、別のコンピューターまたはグループに適用できます。

### ESET PROTECTから検出除外が上書きされる可能性

検出除外ローカルリストが既に存在しているときには、管理者は、**検出除外をローカル定義リストの最後に追加することを許可**によってポリシーを適用する必要があります。その後に、想定どおりESET PROTECTから検出除外を最後に追加できるようになります。

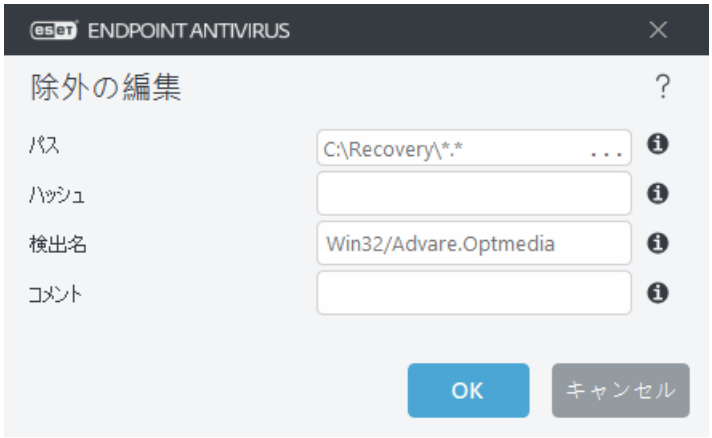



# 検出除外の追加または編集

## 検出を除外

有効なESET検出名を指定してください。有効な検出名については、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 Antivirus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。**パスマスク**フィールドで**...**をクリックして、影響を受けるファイル/ディレクトリのみを除外するか、一時的な場合に限って除外することを検討してください。除外は、望ましくない可能性があるアプリケーション、安全でない可能性があるアプリケーション、不審なアプリケーションにも適用されます。

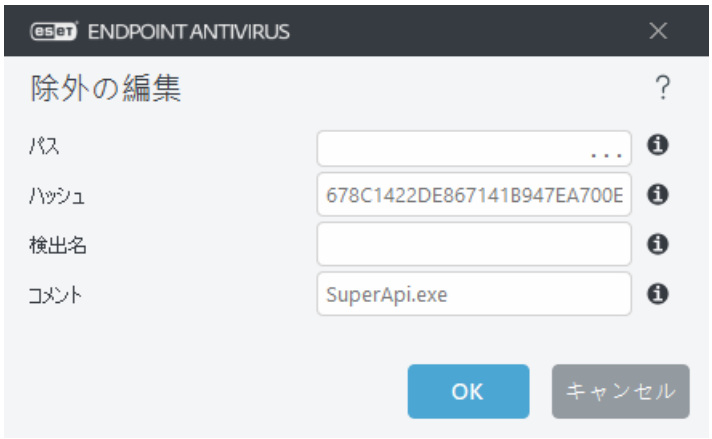
パス除外形式を参照してください。




以下の検出除外の例を参照してください。

## ハッシュを除外

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。




特定の検出を名前で除外する場合は、有効な検出名を入力します。
*Win32/Adware.Optmedia*
ESET Endpoint Antivirusアラートウィンドウから検出を除外するときには、次の形式を使用することもできます。
*@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt*
*@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan*
*@NAME=Win32/Bagle.D@TYPE=worm*

### コントロール要素

- **追加** – オブジェクトを検出対象外にします。
- **編集** – 選択したエントリーを編集します。
- **削除** – 選択したエントリを削除します(CTRLを押しながらクリックすると、複数のエントリを選択できます)。

# 検出除外の作成ウィザード

検出除外は、ログファイルコンテキストメニューからも作成できます(マルウェア検出では使用できません)。

1. メインプログラムウィンドウで、**ツール > ログファイル**をクリックします。
2. **検出ログ**で検出を右クリックします。
3. **除外の作成**をクリックします。

**除外条件**に基づいて1つ以上の検出を除外するには、**条件の変更**をクリックします。

- **正確なファイル** – SHA-1ハッシュで各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 + 検出** – ファイル名(*file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*など)を含む検出名とパスで各ファイルを除外します。

推奨オプションは、検出タイプに基づいてあらかじめ選択されています。

任意で、**除外の作成**をクリックする前に、**コメント**を追加できます。

# 検出エンジンの詳細オプション

**AMSIによる詳細検査を有効にする**は、Microsoft Antimalware Scan Interfaceツールでは□PowerShellスクリプト□Windows Script Hostによって実行されるスクリプト、およびAMSI SDKを使用して検査されたデータの検査を許可します。

# ネットワークトラフィックスキャナー

ネットワークトラフィックスキャナーは、複数の高度なマルウェア検査テクニックを統合した、アプリケーションプロトコルのマルウェア保護を提供します。ネットワークトラフィックスキャナーは、インターネットブラウザーや電子メールクライアントに関係なく□HTTP(S)□POP3(S)□およびIMAP(S)プロトコルを自動的に検査します。ネットワークトラフィックスキャナーは、詳細設定 > **検出エンジン > ネットワークトラフィックスキャナー**で有効/無効にできます。

**ネットワークトラフィックスキャナーを有効にする** – このオプションを無効にすると□HTTP(S)□POP3(S)□およびIMAP(S)プロトコルは検査されません。次のESET Endpoint Antivirus機能を使用するには、ネットワークトラフィックスキャナーを有効にする必要があります。

- Webアクセス保護
- SSL/TLS
- フィッシング対策機能
- 電子メールクライアント保護

# クラウドベース保護

ESET LiveGrid®高度早期警告システム上に構築されたESETThreatSense.Netは ESETユーザーが世界中で提出したデータを収集し、ESETのリサーチラボに送信します。世界中の不審なサンプルとメタデータを提供することでESET LiveGrid®によって、お客様のニーズに即時に対応し、最新の脅威に対するESETの対応力を確保できます。

使用可能なオプションは

## オプション1:ESET LiveGrid®レピュテーションシステムを有効にする

ESETLiveGrid®に参加する（推奨）は、クラウドベースのホワイトリストとブラックリストを提供します。

直接的にはこのプログラムのインタフェースやコンテキストメニューを用いるか、あるいはESET LiveGrid®に用意されている追加情報を読んで、実行中のプロセスやファイルの評価をチェックします。

## オプション2:ESET LiveGrid®フィードバックシステムを有効にする

ESET LiveGrid®レピュテーションシステムとESET LiveGrid®フィードバックシステムは、新しく検出された脅威に関連して、コンピューターに関する情報を収集します。この情報には、ウイルスが検出されたファイルのサンプルまたはコピー、そのファイルのパス、ファイル名、日時、ウイルスがコンピューターに侵入したプロセス、およびコンピューターのオペレーティングシステムについての情報が含まれます。

既定ではESET Endpoint Antivirusは、疑わしいファイルを詳しく解析するためにESETのウイルスラボ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。

## オプション3:ESET LiveGrid®を有効にしないことを選択する

ソフトウェアの機能は一切失われませんが、場合によってはESET LiveGrid® が有効になっている場合ESET Endpoint Antivirusは検出エンジンアップデートよりも速く新しい脅威に対応できることがあります。

> 用語集でESET LiveGrid®を参照してください。
> ESET Endpoint AntivirusでESET LiveGrid®を有効または無効にする方法については、英語および他の複数の言語で提供されている図解手順を参照してください。

---

## 詳細設定でクラウドベース保護を設定する

ESET LiveGrid®設定にアクセスするには、詳細設定 > **検出エンジン** > **クラウドベース保護**を開きます。

**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。

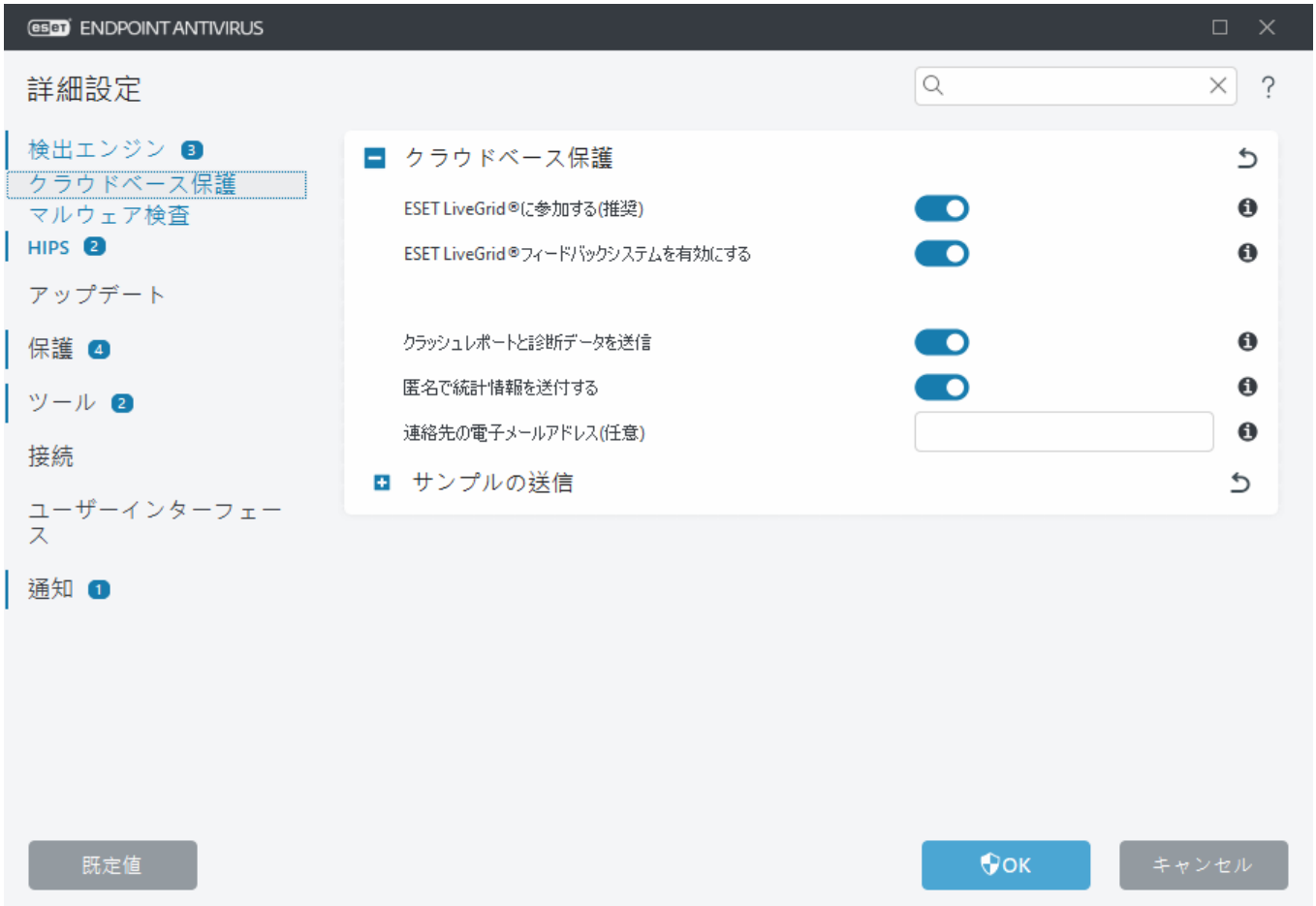
**ESET LiveGrid®フィードバックシステムを有効にする** – 関連する送信データ（以下の**サンプルの送信**セクションを参照）、クラッシュレポート、統計情報をさらに分析するためESET研究所に送信します。

**ESET LiveGuardを有効にする**(ESET LiveGuardはESETが販売する追加機能で、既定では利用できません) - ESET LiveGuardはESETが提供する有料サービスです。その目的は、発生中の新しい脅威を軽減するために特別に設計された保護層を追加することです。不審なファイルは自動的にESETクラウドに送信されます。クラウドでは、脅威が高度なマルウェア検出エンジンによって分析されます。サンプルを提供したユーザーは、観察されたサンプルの動作の概要を示す動作レポートを受け取ります。

**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やモジュールメモリダンプなどのESET LiveGrid®関連の診断データを送信します。このオプションを有効にしESETによる問題の診断、製品の改善、確実なエンドユーザー保護の強化を支援することをお勧めします

**匿名の統計情報を送信** – 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)** – 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。この電子メールアドレスは、分析のために詳しい情報が必要な場合の連絡先として使用されます。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。




## サンプルの送信

**サンプルの手動送信** – このオプションを有効にすると、コンテキストメニューの隔離またはツールから手動でサンプルをESETに送信します。

**検出されたサンプルの自動送信**

分析および将来の検出を改善する目的で、ESETに送信されるサンプルの種類を選択します。使用可能なオプションは

- **すべての検出されたサンプル – 検出エンジン**によって検出されたすべての検出された**オブジェクト**(スキャナー設定で有効になっている場合は望ましくない可能性のあるアプリケーションを含む)。
- **文書を除くすべてのサンプル – 文書**を除くすべての検出されたオブジェクト(以下を参照)。
- **送信しない** – 検出されたオブジェクトはESETに送信されません。

**不審なサンプルの自動送信**

検出エンジンで検出されなかった場合にも、これらのサンプルがESETに送信されます。たとえば、検出されなかったサンプルや、ESET Endpoint Antivirus**保護モジュール**のいずれかが不審であると見なしたサンプル、不明瞭な動作のサンプルなどです。

- **実行ファイル** - .exe, .dll, .sysなどのファイルが含まれます。
- **アーカイブ** - .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cabなどのファイルタイプが含まれます。
- **スクリプト** - .bat, .cmd, .hta, .js, .vbs, .ps1などのファイルタイプが含まれます。
- **その他** - .jar, .reg, .msi, .sfw, .lnkなどのファイルタイプを含みます。
- **考えられる迷惑メール** – これにより、詳細な分析のため、添付ファイル付きの迷惑メールの可能性があるメールの一部または全部をESETに送信できます。このオプションを有効にすると、将来の迷惑メール検出の改良などの迷惑メールのグローバル検出が改善されます。
- **文書** – アクティブなコンテンツの有無に関係なくMicrosoft OfficeまたはPDF文書が含まれます。

  すべての含まれる文書ファイルタイプの一覧を展開する

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

**除外**

**除外フィルタ**を使用すると、特定のファイルまたはフォルダを送信から除外できます(例: ドキュメントやスプレッドシートなど、機密情報が含まれる可能性があるファイルを除外する場合に便利なことがあります)。このリスト内のファイルは、疑わしいコードを含んでいても、解析のためにESETのラボに送信されることはありません。最も一般的なファイルの種類は、既定で除外されます(.docなど)。必要に応じて、除外するファイルは追加できます。

download.domain.comからダウンロードされたファイルを除外するには、**詳細設定** > **クラウドベース保護** > **サンプル除外の送信** > **除外**に移動して、*download.domain.com*の除外を追加します。

**サンプルの最大サイズ(MB)** – 自動的に送信されるサンプルの最大サイズを定義します(1-64 MB)

## ESET LiveGuard

ESET LiveGuard Webコンソールを使用してクライアントコンピューターでESET PROTECTサービスを有効にするには**ESET Endpoint AntivirusのESET LiveGuard構成を**参照してください。

以前にESETLiveGrid®を使用したことがあり、その後で無効にした場合、送信するデータパッケージが残っていることがあります。無効にした後でも、このようなパッケージはESETに送信されます。すべての最新情報が送信されると、パッケージはこれ以上作成されません。

# クラウドベース保護の除外フィルター

除外フィルターを使用すると、特定のファイルやフォルダーをサンプル提出から除外することができます。このリスト内のファイルは、疑わしいコードを含んでいても、解析のためにESETのラボに送信されることはありません。既定では、一般的なファイルタイプ(.docなど)が除外されます。

ドキュメントやスプレッドシートなど、機密情報が含まれているファイルを除外すると便利です。

download.domain.comからダウンロードされたファイルを除外するには、詳細設定 > **検出エンジン** > **クラウドベース保護** > **サンプルの送信** > **除外**を開いて、*download.domain.com*の除外を追加します。

# マルウェア検査

**マルウェア検査**セクションは、詳細設定 > **検出エンジン** > **マルウェア検査**からアクセスでき、検査プロファイルの検査パラメータを設定できます。

## オンデマンド検査

**選択されたプロファイル** – オンデマンドスキャナーによって使用される特定のパラメーターのセット。新しいプロファイルを作成するには、**[プロファイルのリスト]**の横の**[編集]**をクリックします。詳細については、検査プロファイルを参照してください。

検査プロファイルを選択したら、以下のオプションを設定できます。

**検査対象** – 特定の対象のみ、または対象のグループを検査する場合は、**検査の対象**の横の**編集**をクリックし、フォルダ(ツリー)構造からオプションを選択します。詳細については、検査対象を参照してください。

**オンデマンド保護および機械学習保護** – 検査プロファイルごとにレポートと保護レベルを設定できます。既定では、検査プロファイルはリアルタイムファイルシステム保護で定義されているものと同じ設定を使用します。**リアルタイムファイルシステム保護設定を使用**の横にあるトグルを無効にすると、カスタムレポートと保護レベルを設定できます。レポートと保護レベルの詳細な説明については、保護を参照してください。

**ThreatSense** – コントロールするファイル拡張子や使用される検出方法などの詳細設定オプション。詳細については、ThreatSenseを参照してください。

# 検査プロファイル

ESET Endpoint Antivirusには、次の4つの定義済み検査プロファイルがあります。

- **スマート検査**: これは既定の詳細検査プロファイルです。スマート検査プロファイルは、スマート最適化技術を使用しており、前回の検査で感染していないことが判明したファイルのうち、その検査以降変更されていないファイルを除外します。これにより、検査時間を短縮でき、システムセキュリティへの影響を最小限に抑えることができます。
- **コンテキストメニューの検査**: コンテキストメニューから、任意のファイルのオンデマンド検査を開始できます。コンテキストメニューの検査プロファイルでは、この方法で検査をトリガーするときに使用される検査構成を定義できます。
- **詳細検査**: 既定では、詳細検査プロファイルはスマート最適化を使用しないため、このプロファイルを使用して検査から除外されるファイルはありません。

- **コンピューターの検査**：これは標準コンピューターの検査で使用される既定のプロファイルです。

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

新しいプロファイルを作成するには、詳細設定 > **検出エンジン** > **マルウェア検査** > **オンデマンド検査** > **プロファイルのリスト** > **編集**を開きます。**オンデマンド検査**ウィンドウには、既存の検査プロファイルと、新しいプロパティを作成するためのオプションを表示する**選択されたプロファイル**ドロップダウンメニューがあります。各自のニーズに合った検査プロファイルを作成するための参考情報として、ThreatSenseにある検査設定の各パラメーターの説明を参照してください。

既にある**コンピューターの検査**の設定は部分的にしか自分のニーズを満たさないので、独自の検査プロファイルを作成する必要があると仮定します。**プロファイルマネージャ**ウィンドウで新しいプロファイルの名前を入力し、[**追加**]。をクリックします **選択されたプロファイル**ドロップダウンメニューから新しいプロファイルを選択し、要件に合わせて残りのパラメータを調整し、**[OK]**をクリックして新しいプロファイルを保存します。

# 検査対象

**検査の対象**ドロップダウンメニューでは、事前定義されている次の検査対象を選択できます。

- **プロファイル設定に依存**– 選択された検査プロファイルに設定されている対象を選択します。
- **リムーバブルメディア** – フロッピーディスク、USB記憶装置、CD/DVDを選択します。
- **ローカルドライブ** – システムハードディスクをすべて選択します。
- **ネットワークドライブ** – マッピングされたネットワークドライブをすべて選択します。
- **カスタム選択** – 以前の選択をすべてキャンセルします。

フォルダー(ツリー)構造には、特定の検査対象も含まれています。

- **システムメモリ** – 現在オペレーティングメモリで使用されているすべてのプロセスとデータを検査します。
- **ブートセクタ/UEFI** – ブートセクターとUEFIにマルウェアが存在するかどうかを検査します。用語集のUEFIスキャナーの詳細をお読みください。
- **WMIデータベース**– Windows Management Instrumentation WMIデータベース全体、すべての名前空間、すべてのクラスインスタンス、およびすべてのプロパティを検査します。データとして埋め込まれた感染ファイルまたはマルウェアへの参照を検索します。
- **システムレジストリ** – システムレジストリ全体、すべてのキー、およびサブキーを検査します。データとして埋め込まれた感染ファイルまたはマルウェアへの参照を検索します。検出を駆除するときには、重要なデータが失われないように、レジストリに参照が残ります。

検査対象(ファイルまたはフォルダー)にすばやく移動するには、ツリー構造の下のテキストフィールドにパスを入力しますパスは大文字と小文字を区別します。検査に対象を含めるには、ツリー構造のチェックボックスを選択します。

# アイドル状態検査

詳細設定 > **検出エンジン** > **マルウェア検査** > **アイドル状態検査**でアイドル状態検査を有効にできます。

## アイドル状態検査

**アイドル状態検査を有効にする**の横のトグルをオンにすると、この機能が有効になります。コンピュータがアイドル状態になると、すべてのローカルドライブでコンピュータの検査がサイレントに実行されます。

既定では、アイドル状態検出はコンピュータ(ノートパソコン)がバッテリー電源で動作しているときは実行されません。この設定を変更するには、詳細設定で**コンピューターがバッテリー電源で作動している場合にも実行する**の横のスライダーバーをオンにします。

詳細設定の**ログを有効にする**の横のスライダバーをオンにして、ログファイルセクションでコンピューターの検査出力を記録します(プログラムのメインウィンドウで**ツール > ログファイル**をクリックし、**ログ**ドロップダウンメニューから**コンピューターの検査**を選択します)。

## アイドル状態検知

アイドル状態スキャナーをトリガーするために満たす必要がある条件の一覧については、アイドル状態検出トリガーを参照してください。

**ThreatSense** – コントロールするファイル拡張子や使用される検出方法などの詳細設定オプション。詳細については、ThreatSenseを参照してください。

# アイドル状態検知

アイドル状態検知設定は、詳細設定 > **検出エンジン > マルウェア検査 > アイドル状態検査 > アイドル状態検知**で設定できます。この設定により、次の場合にアイドル状態検査のトリガが指定されます。

- **ディスプレイの電源を切るもしくはスクリーンセーバー**
- **コンピュータのロック**
- **ユーザーのログオフ**

それぞれの状態についてチェックボックスを使用して、アイドル状態の検出トリガを有効または無効にします。

# スタートアップ検査の設定

既定では、システムの起動時および検出エンジンのアップデート時に自動起動ファイルの検査が実行されます。この検査は、スケジューラの設定およびタスクに依存します。

スタートアップ検査の設定は、[**システムのスタートアップファイルのチェック**]のスケジューラタスクに含まれます。設定を修正するには、**ツール > スケジューラ**と移動し、**自動スタートアップファイルのチェック**▯**編集**の順にクリックします。最後のステップでは、自動スタートアップファイルのチェックウィンドウが表示されます。スケジューラタスクの作成と管理の詳細については、「新しいタスクの作成」を参照してください。

**ThreatSense** – コントロールするファイル拡張子や使用される検出方法などの詳細設定オプション。詳細については、ThreatSenseを参照してください。

# 自動スタートアップファイルのチェック

システム起動時のファイルチェックスケジュールタスクを作成するときに、次のパラメータを調整するいくつかのオプションがあります。

**検査の対象**ドロップダウンメニューでは、高度なアルゴリズムに基づくシステムの起動時のファイルの検査レベルを指定します。ファイルは次の基準に従って降順で整理されます。

- **すべての登録されたファイル**（検査対象のファイル数は最多）
- **使用頻度が低いファイル**
- **一般的に使用されるファイル**
- **使用頻度が高いファイル**
- **最も多く使用されるファイルのみ**（検査対象のファイル数は最小）

次の2つの検査レベルグループも含まれます。

- **ユーザーのログオン前に実行されるファイル** – ユーザーがログオンしていない状態でアクセスできる場所のファイルが含まれます(サービス、ブラウザヘルパーオブジェクト、Winlogon通知、Windowsスケジューラのエントリ、既知のdllといったスタートアップの場所にあるすべてのファイル)。
- **ユーザーのログオン後に実行されるファイル** – ユーザーがログオンした後にのみアクセスできる場所にあるファイル(特定のユーザーだけが実行するファイル、通常は*HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*にあるファイル)が含まれます。

検査されるファイルのリストは、上記の各グループで固定されます。システム起動時に実行されるファイルの検査レベルを低く選択すると、検査されていないファイルは、開くときまたは実行時に検査されます。

**検査の優先度** – 以下のとおりの、検査をいつ開始するかを決定するために使用する優先度レベル。

- **アイドル時** – システムのアイドル時にのみタスクが実行されます。
- **最低** – システム負荷が可能なかぎり低い場合
- **低** – システム負荷は低い
- **通常** – システム負荷は平均的

# リムーバブルメディア

ESET Endpoint Antivirusには、リムーバブルメディア(CD/DVD/USBなど)をコンピューターに挿入したときに自動的に検査する機能があります。この機能は、ユーザーが求めたものでないコンテンツを収めたリムーバブルメディアのユーザーによる使用を防止したいコンピュータ管理者にとって便利です。

リムーバブルメディアを挿入し、詳細設定 > **検出エンジン** > **マルウェア検査** > **リムーバブルメディア**で**検査オプションを表示**が設定されると、次のダイアログが表示されます。

このダイアログのオプション:

- **今すぐ検査** – リムーバブルメディアのスキャンを開始します。
- **検査しない** – リムーバブルメディアは検査されません。
- **設定** - 詳細設定を開きます。
- **選択したオプションを常に使用する** – これを選択すると、リムーバブルメディアが別の時間に挿入されたときに同じアクションが実行されます。

また、ESET Endpoint Antivirusは、所定のコンピューター上で外部デバイスを使用するためのルールを定義することができるデバイスコントロール機能の役割も果たします。デバイスコントロールの詳細については、「デバイスコントロール」セクションで参照することができます。

---

リムーバブルメディア検査の設定を表示するには、詳細設定 > **検出エンジン** > **マルウェア検査** > **リムーバブルメディア**を開きます。

**リムーバブルメディアの挿入後に行うアクション** – コンピューターにリムーバブルメディアデバイス(CD、DVD、USB)が挿入されたときに実行する既定のアクションを選択します。リムーバブルメディアをコンピューターに挿入したときに実行するアクションを選択します。

- **検査しない** – アクションは実行されず、**新規デバイスの検出**ウィンドウは開きません。
- **自動デバイス検査** – 挿入したリムーバブルメディアに対してコンピューターの検査が実行されます。
- **強制デバイス検査** – 挿入したリムーバブルメディアに対するコンピューターの検査が実行され、キャンセルできません。
- **検査オプションの表示** - **新規デバイスの検出**ウィンドウが開きます。

# ドキュメント保護

ドキュメントの保護機能によりMicrosoft Officeドキュメントの検査(開く前に実行)、およびInternet Explorerにより自動的にダウンロードされたファイル(Microsoft ActiveX要素など)の検査が行われます。ドキュメントの保護により、リアルタイムファイルシステム保護に加えてさらに別段の保護が提供されますが、大量のMicrosoft Officeドキュメントを扱わないシステムでは、パフォーマンスを向上させるためにこれを無効にすることができます。

ドキュメント保護を有効にするには、詳細設定 () > **検出エンジン** > **マルウェア検査** > **ドキュメント保護**を開き、**ドキュメント保護を有効にする**の横のスライダーバーをクリックします。

**ThreatSense** – コントロールするファイル拡張子や使用される検出方法などの詳細設定オプション。詳細については、ThreatSenseを参照してください。

> この機能は、Microsoft Antivirus API (Microsoft Office 2000 以上、Microsoft Internet Explorer 5.0以上など)を使用するアプリケーションでアクティベーションされます。

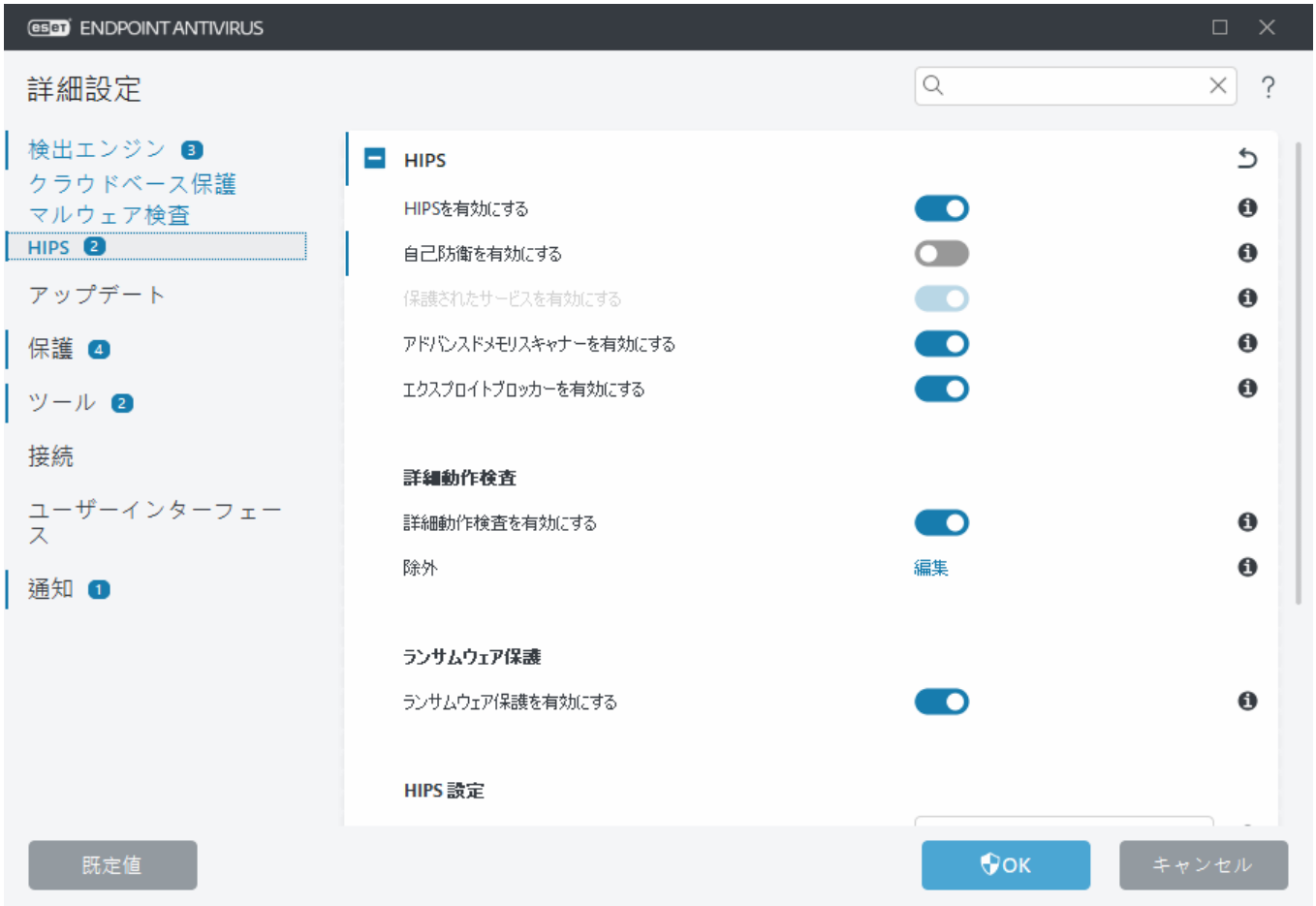
# HIPS - ホストベースの侵入防止システム)

> HIPS設定の変更は、経験豊富なユーザーだけが行ってください。HIPSの設定が正しくないと、システムが不安定になる可能性があります。

**ホストベースの侵入防止システム(HIPS)**により、コンピュータのセキュリティに悪影響を与えようとす

る望ましくない活動およびマルウェアからシステムが保護されますHIPSは、高度な動作分析とネットワークフィルタリングの検出機能を連携して、実行中のプロセス、ファイル、およびレジストリキーを監視しますHIPSはリアルタイムファイルシステム保護とは異なります。

HIPS設定は、詳細設定 > **検出エンジン** > **HIPS** > **ホスト侵入防止システム**で設定できますHIPSの状態(有効/無効)は、ESET Endpoint Antivirusのプログラムのメインウィンドウ > **設定** > **コンピューター**に表示されます。




## HIPS

**HIPSを有効にする** - ESET Endpoint Antivirusでは既定でHIPSが有効ですHIPSをオフにすると、エクスプロイトブロッカーなどのHIPS関連機能が無効になります。

**自己防衛を有効にする** - ESET Endpoint Antivirusには、悪意のあるソフトウェアによってウイルス・スパイウェア対策の保護機能が破損されたり無効化されたりしないようにするHIPSの一部として、**自己防衛**技術が組み込まれています。自己防衛は、重要なシステムおよびESETのプロセス、レジストリキー、およびファイルを改ざんから防止します。インストール時にはESET Managementエージェントも保護されます。

**保護されたサービスを有効にする** – ESET Service (ekrn.exe)の保護を有効にします。有効にすると、サービスは保護されたWindowsプロセスとして起動し、マルウェアによる攻撃を防御します。このオプションは、Windows 8.1およびWindows 10で使用できます。

**詳細メモリ検査を有効にする**はエクスプロイトブロックとともに動作し、難読化または暗号化を使用することで、マルウェア対策製品の検出を回避するように設計されたマルウェアに対する保護を強化します。既定では、詳細メモリ検査が有効です。この保護の詳細については、「用語集」を参照してください。

**エクスプロイトブロックを有効にする** - Webブラウザ、PDFリーダー、電子メールクライアント、MS Officeコンポーネントなどの一般的に利用されるアプリケーションタイプの保護を強化するための機能です。既定では、エクスプロイトブロックが有効です。この保護の詳細については、「用語集」を参照してください。

## 詳細動作検査

**詳細動作検査を有効にする**は、HIPS機能の一部として動作する別のレイヤーの保護です。このHIPSの拡張は、コンピューターで実行中のすべてのプログラムの動作を分析し、プロセスの動作に悪意がある場合はユーザーに警告します。

詳細動作検査のHIPS除外では、プロセスをスキャンから除外することができます。すべてのプロセスで脅威の可能性がスキャンされるように、絶対に必要な場合を除いては、除外を作成しないことをお勧めします。

## ランサムウェア保護

**ランサムウェアシールドを有効にする** - HIPS機能の一部として動作する保護の別のレイヤーです。ランサムウェア保護を実行するにはESET LiveGrid®レピュテーションシステムを有効にする必要があります。この保護の詳細を参照してください

**Intel® Threat Detection Technology**を有効にする – 固有のIntel CPUテレメトリを使用して、ランサムウェア攻撃を検出し、検出効率を高め、誤検知アラートを減らし、詳細な回避技術を検出する可視性を高めます。サポートされているプロセッサーを参照してください。

**監査モードを有効にする** – ランサムウェア保護で検出されたすべての項目は自動的にブロックされませんが、重要度警告でログに出力され、「監査モード」フラグ付きで管理コンソールに送信されます。管理者は、このような検出を除外して、さらなる検出を防止するか、有効な状態を保つ(監査モードが終了した後にブロックされ、削除されます)かどうかを決定できます。監査モードを有効//無効にするとESET Endpoint Antivirusのログに記録されます。このオプションは、ESET PROTECTポリシー設定エディターでのみ使用できます。

## HIPS 設定

**フィルタリングモード**は、次のモードのいずれかで実行できます。

| フィルタリングモード | 説明 |
|---|---|
| **ルール付き自動モード** | 操作は、システムを保護する事前定義ルールでブロックされる操作を除いて有効です。 |
| **スマートモード** | 非常に不審なイベントに関する通知だけが表示されます。 |
| **対話モード** | ユーザーは操作を確定するよう要求されます。 |
| **ポリシーベースモード** | 許可する特定のルールで定義されていない、すべての処理をブロックします。 |

| フィルタリングモード | 説明 |
| --- | --- |
| **学習モード** | 操作は有効で、各操作の後にルールが作成されます。このモードで作成されたルールは、**HIPSルール**エディターで表示できますが、手動で作成したルールや、自動モードで作成されるルールより優先度は低くなります。**フィルタリングモード**ドロップダウンメニューで**学習モード**を選択すると、**学習モードが終了**設定が使用できるようになります。学習モードを有効にする期間を選択します。最大期間は14日です。指定した期間が過ぎると、学習モード中にHIPSで作成されたルールを編集するように指示されます。別のフィルタリングモードを選択するか、決定を延期し、学習モードを使用し続けることもできます。 |

**学習モードの期限切れの後に設定されるモード** – 学習モードの期限が終了した後に使用されるフィルタリングモードを選択します。期限切れの後に**ユーザーに確認**するオプションでHIPSフィルタリングモードを変更するには、管理者権限が必要です。

HIPSシステムはオペレーティングシステム内部のイベントを監視し、ファイアウォールで使用されるルールに似たルールに基づいて対応します。**ルール**の横の[**編集**]をクリックして、**HIPSルール**エディターを開きますHIPSルールウィンドウでは、ルールを選択、追加、編集、または削除できます。ルール作成およびHIPS操作の詳細については、HIPS ルールの編集を参照してください。

# HIPS除外

除外によって、プロセスをHIPS詳細動作検査から除外できます。

HIPS除外を編集するには、詳細設定 > **検出エンジン** > **HIPS** > **ホスト侵入防止システム** > **除外** > **編集**を開きます。

> 除外されたファイル拡張子検出除外パフォーマンス除外、またはプロセス除外と混同しないでください。

オブジェクトを除外するには、**追加**をクリックして、オブジェクトのパスを入力するか、あるいは下のツリー構造でパスを選択します。選択したエントリを編集または削除することもできます。

# HIPS詳細設定

次のオプションは、アプリケーションの動作をデバッグおよび分析するときに役立ちます。

使用するデバイスドライバー – ユーザールールで明示的にブロックされないかぎり、設定されたフィルタリングモードに関係なく、選択したドライバは常にロードされます。

**ブロックされた操作をすべて記録** – ブロックされたすべての操作がHIPSログに書き込まれます。トラブルシューティング時またはESETテクニカルサポートから要求された場合にのみこの機能を使用してください。

**スタートアップアプリケーションに変更があったとき通知する** – アプリケーションがシステムスタートアップに追加、またはスタートアップから削除されるたびに、デスクトップ通知を表示します。

# ドライバは常にロードできます

明示的にユーザールールでブロックされている場合を除き、このリストに表示されるドライバは、HIPSフィルタリングモードに関係なく、常にロードできます。

**追加** – 新しいドライバを追加します。

**編集** – 選択したドライバを編集します。

**削除** – ドライバをリストから削除します。

**リセット** – システムドライバのセットをリロードします。

手動で追加したドライバを含める場合は、[**リセット**]をクリックします。これは、複数のドライバを追加し、手動でリストから削除できない場合に有効です。

インストール後、ドライバの一覧が空です。時間の経過に伴い、ESET Endpoint Antivirusのリストが自動的に入力されます。

常に読み込みが許可されているドライバーはデバイスごとに固有であり、ESET PROTECTポリシーを使用して編集することはできません。インストール後、ドライバの一覧が空です。時間の経過に伴い、ESET Endpoint Antivirusのリストが自動的に入力されます。

# HIPSインタラクティブウィンドウ

HIPS通知ウィンドウでは、HIPSが検出する新しいアクションに基づいてルールを作成し、そのアクションを許可または拒否する条件を定義できます。

通知ウィンドウで作成したルールは手動で作成したルールと同等であるとみなされます。通知ウィンドウから作成したルールは、そのダイアログウィンドウをトリガしたルールより汎用的にすることができます。つまり、そのようなルールを作成した場合、同じ操作で同じウィンドウをトリガできます。詳細については、HIPSルールの優先度を参照してください。

ルールの既定のアクションを**毎回確認**に設定した場合、ルールがトリガーされるたびにダイアログウィンドウが表示されます。操作を[**遮断**]または[**許可**]することもできます。指定された時間内にアクションを選択しなかった場合は、ルールに基づいて新しいアクションが選択されます。

**アプリケーションが終了するまで記憶**では、ルールまたはフィルタリングモードの変更、HIPSモジュールの更新、またはシステムの再起動まで、アクション(**許可/拒否**)が使用されます。これら3つのアクションのいずれかが実行された後は、一時的なルールは削除されます。

**ルールを作成し、永久に記憶**オプションは、HIPSルール管理セクション(管理者権限が必要)で後から変更できる、新しいHIPSルールを作成します。

下部で**詳細**をクリックすると、処理をトリガーするアプリケーション、ファイルのレピュテーション、または許可または拒否するように求められる操作の種類を確認します。

詳細ルールパラメーターの設定は、**詳細オプション**をクリックして、アクセスできます。以下のオプションは、**ルールを作成し、永久に記憶**を選択した場合にアクセスできます。

- **このアプリケーションでのみ有効なルールを作成する** – このチェックボックスをオフにすると、すべてのソースアプリケーションのルールが作成されます。
- **処理のみ** – ルールファイル/アプリケーション/レジストリ処理を選択します。すべてのHIPS処理

の説明をご参照ください。

- **ターゲットのみ** – ルールファイル/アプリケーション/レジストリターゲットを選択します。

通知の表示を停止するには、**詳細設定** > 検出エンジン > **HIPS** > **基本**で、フィルタリングモードを**ルール付き自動モード**に変更します。


# 潜在的なランサムウェア動作の検出

このインタラクティブウィンドウは、潜在的なランサムウェア動作が検出されたときに表示されます。操作を[**遮断**]または[**許可**]することもできます。


**詳細**をクリックすると、特定の検出パラメーターが表示されます。このダイアログウィンドウでは、**分析のために送信**するか、**検出から除外**することができます。

ランサムウェア保護が正しく動作するにはESET LiveGrid®を有効にする必要があります。

# HIPSルール管理

これはHIPSで、ユーザーが定義したルールと自動追加されたルールのリストです。ルール作成とHIPS処理の詳細については、HIPSルール設定の章を参照してください。HIPSの一般原理も参照してください。

## 列

**ルール** – ユーザーが定義したか、または自動選択されたルール名。

**有効** – ルールをリスト内に置いたまま、使用しない場合にこのオプションをオフにします。

**アクション** – ルールは、条件が一致した場合に実行する必要のあるアクション、つまり[**許可**]または[**ブロック**]、または[**確認**]を指定します。

**ソース** – ルールは、このアプリケーションによってイベントが起動された場合のみ使用されます。

**ターゲット**– 操作が特定のファイル、アプリケーション、レジストリエントリに関連付けられている場合にのみ、このルールが使用されます。

**ログ記録の重大度** – このオプションをオンにすると、このルールに関する情報がHIPSログに書き込まれます。

**通知** – イベントが起動された場合に通知が右下隅に表示されます。

## コントロール要素

**追加** – 新しいルールを作成します。

**編集** – 選択したエントリーを編集します。

**削除** – 選択したエントリーを削除します。

## HIPSルールの優先度

上下ボタンを使用してHIPSルールの優先度レベルを調整するオプションはありません。。

- 作成するすべてのルールの優先度は同じです
- ルールが具体的になるほど、優先度が上がります(たとえば、特定のアプリケーションのルールはすべてのアプリケーションを対象としたルールよりも優先度が高くなります)
- 内部的にはHIPSには、ユーザーがアクセスできない高優先度ルールが実装されています(たとえば、自己防衛が定義したルールは上書きできません)
- オペレーティングシステムをフリーズさせる可能性があるルールを作成した場合は、適用されません(優先度が最低になります)

# HIPSルール設定

HIPSルール管理を参照してください。

**ルール名** – ユーザーが定義したか、または自動選択されたルール名。

**アクション** – ルールは、条件が一致した場合に実行する必要のあるアクション、つまり[**許可**]/[**ブロック**]、または[**確認**]を指定します。

**動作影響** – ルールが適用される処理のタイプを選択する必要があります。ルールは、選択された[ターゲット]に対するこのタイプの操作に限り使用されます。

**有効** – ルールをリスト内に置いたまま適用しない場合、このトグルをオフにします。

**ログ記録の重大度** – このオプションをオンにすると、このルールに関する情報がHIPSログに書き込まれます。

**ユーザーに通知** – イベントが起動された場合に通知が右下隅に表示されます。

ルールは、このルールの使用をトリガする条件を記述した部分で構成されます。

**ソースアプリケーション** – ルールは、このアプリケーションによってイベントが起動された場合のみ使用されます。ドロップダウンメニューから**特定のアプリケーション**を選択し、[**追加**]をクリックして、新しいファイルを選択します。あるいは、ドロップダウンメニューから**すべてのアプリケーション**を選択してすべてのアプリケーションを追加します。

**ターゲットファイル**– ルールは、操作がこのターゲットと関連する場合に限り使用されます。ドロップダウンメニューから**特定のファイル**を選択し、[**追加**]をクリックして、新しいファイルまたはフォルダを選択します。あるいは、ドロップダウンメニューから**すべてのファイル**を選択してすべてのファイルを追加します。

**ターゲットファイル**– ルールは、操作がこのターゲットと関連する場合に限り使用されます。ドロップダウンメニューから**特定のアプリケーション**を選択し、[**追加**]をクリックして、新しいファイルまたはフォルダを選択します。あるいは、ドロップダウンメニューから**すべてのアプリケーション**を選択してすべてのアプリケーションを追加します。

**レジストリエントリ**– ルールは、操作がこのターゲットと関連する場合に限り使用されます。ドロップダウンメニューから**特定のエントリ**を選択し、[**追加**]をクリックして、新しいファイルまたはフォルダを選択します。あるいは、ドロップダウンメニューから**すべてのエントリ**を選択してすべてのエントリを追加します。

HIPSで事前定義された特定のルールの操作にはブロックできないものがあり、既定で許可されています。さらに、システムの動作すべてがHIPSにより監視されているわけではありません/HIPSは、危険性があると考えられる動作を監視しています。

パスを指定すると/C:\exampleはフォルダー自体のアクションに影響し、C:\example*.*はフォルダーのファイルに影響します。

# アプリケーション動作

- **別のアプリケーションのデバッグ** – デバッガをプロセスにアタッチします。アプリケーションのデバッグ中にそのアプリケーションの動作のさまざまな詳細を表示して変更し、そのデータにアクセスできます。
- **別のアプリケーションからのイベントの取得** – ソースアプリケーションは、特定のアプリケーションを対象としたイベントを取得しようとします(キーロガーがブラウザのイベントのキャプチャを試みるなど)。
- **別のアプリケーションの終了/中断** – プロセスの中断、再開、終了(Process Explorerまたは Processesペインから直接アクセス可能)。
- **新規アプリケーションの開始** – 新しいアプリケーションまたはプロセスの開始。
- **別のアプリケーションの状態を変更** – ソースアプリケーションは、ターゲットアプリケーションのメモリに書き込もうとしているか、または代行でコードを実行しようとしています。この機能

は、この動作の使用をブロックするルール中で、重要なアプリケーションをターゲットアプリケーションとして設定することによって保護するのに役立ちます。

## レジストリの操作

- **スタートアップ設定の変更** – 設定(Windows起動時に実行するアプリケーションの定義)の変更。これらは、たとえばWindowsレジストリのRunのキーを検索することによって見つけられます。
- **レジストリからの削除** – レジストリキーまたはその値の削除。
- **レジストリキー名の変更** – レジストリキーの名前の変更。
- **レジストリの変更** – レジストリキーの新しい値の作成、既存の値の変更、データベース ツリー内のデータの移動、またはレジストリキーのユーザー権限またはグループ権限の設定。

**ルールでのワイルドカードの使用**
ルールのアスタリスクは、ように、特定のキーを代入する目的でのみ使用できますHKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start他のワイルドカードの使用方法はサポートされていません。

**HKEY_CURRENT_USERキーを対象にしたルールの作成**
このキーは、SID (セキュアID)で識別されたユーザー固有のHKEY_USERSの適切なサブキーへのリンクにすぎません。現在のユーザーのルールのみを作成するにはHKEY_CURRENT_USERへのパスを使用する代わりにHKEY_USERS\%SID%を参照するパスを使用します。アスタリスクをSIDとして使用し、ルールをすべてのユーザーに適用することができます。

非常に一般的なルールを作成すると、このタイプのルールに関する警告が表示されます。

次の例では、特定のアプリケーションの不要な動作を制限する方法を説明します。

1. ルールに名前を付けて、[**アクション**]ドロップダウンメニューから[**ブロック**](後から選択する場合)**確認**を選択します。
2. [**ユーザーに通知**]チェックボックスをチェックすると、ルールが適用されたときはいつでも通知が表示されます。
3. ルールが適用される1つ以上の処理を、**影響する処理**セクションで選択します。
4. **次へ**をクリックします。
5. **ソースアプリケーション**ウィンドウで、ドロップダウンメニューから**特定のアプリケーション**を選択し、指定したアプリケーションに対して選択したアプリケーション処理のいずれかを実行しようとするすべてのアプリケーションに、新しいルールを適用します。
6. **追加**をクリックして、**...**をクリックし、特定のアプリケーションへのパスを選択してから、**OK**を押します。必要に応じて、その他のアプリケーションを追加します。
   例: *C:\Program Files (x86)\Untrusted application\application.exe*
7. **ファイルへの書き込み**処理を選択します。
8. ドロップダウンメニューから**すべてのファイル**を選択します。これにより、前の手順で選択したアプリケーションがファイルに書き込む試みをブロックします。
9. [**終了**]をクリックして新規ルールを保存します。


# HIPSのアプリケーション/レジストリパスの追加

[...]オプションをクリックして、ファイルアプリケーションのパスを選択します。フォルダを選択すると、その場所にあるすべてのアプリケーションが組み込まれます。

[**レジストリエディタを開く**]オプションをクリックするとWindowsのレジストリ エディタ(regedit)が開始されます。レジストリパスを追加するときは、正しい場所を[**値**]フィールドに入力してください。

ファイルまたはレジストリのパスの例

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

# アップデート

アップデートの設定オプションは、詳細設定>**アップデート**で使用できます。このセクションでは、アップデートサーバやそれらのサーバの認証データなど、アップデート用の設定情報を指定します。

アップデートファイルを正しくダウンロードするには、全てのアップデートパラメータを正しく入力することが重要です。ファイアウォールを使用している場合は、ESETプログラムがインターネットとの通信(HTTPS通信)を許可されていることを確認してください。

## アップデート

現在使用中のアップデートプロファイルは、**既定のアップデートプロファイルを選択**ドロップダウンメニューに表示されます。

新しいプロファイルを作成するには、アップデートプロファイルセクションを参照してください。

**アップデート通知を設定する** – 編集をクリックすると、表示されるアプリケーション通知を選択でき

ます。通知がデスクトップに表示されるか、電子メールで送信されるかどうかを選択できます。

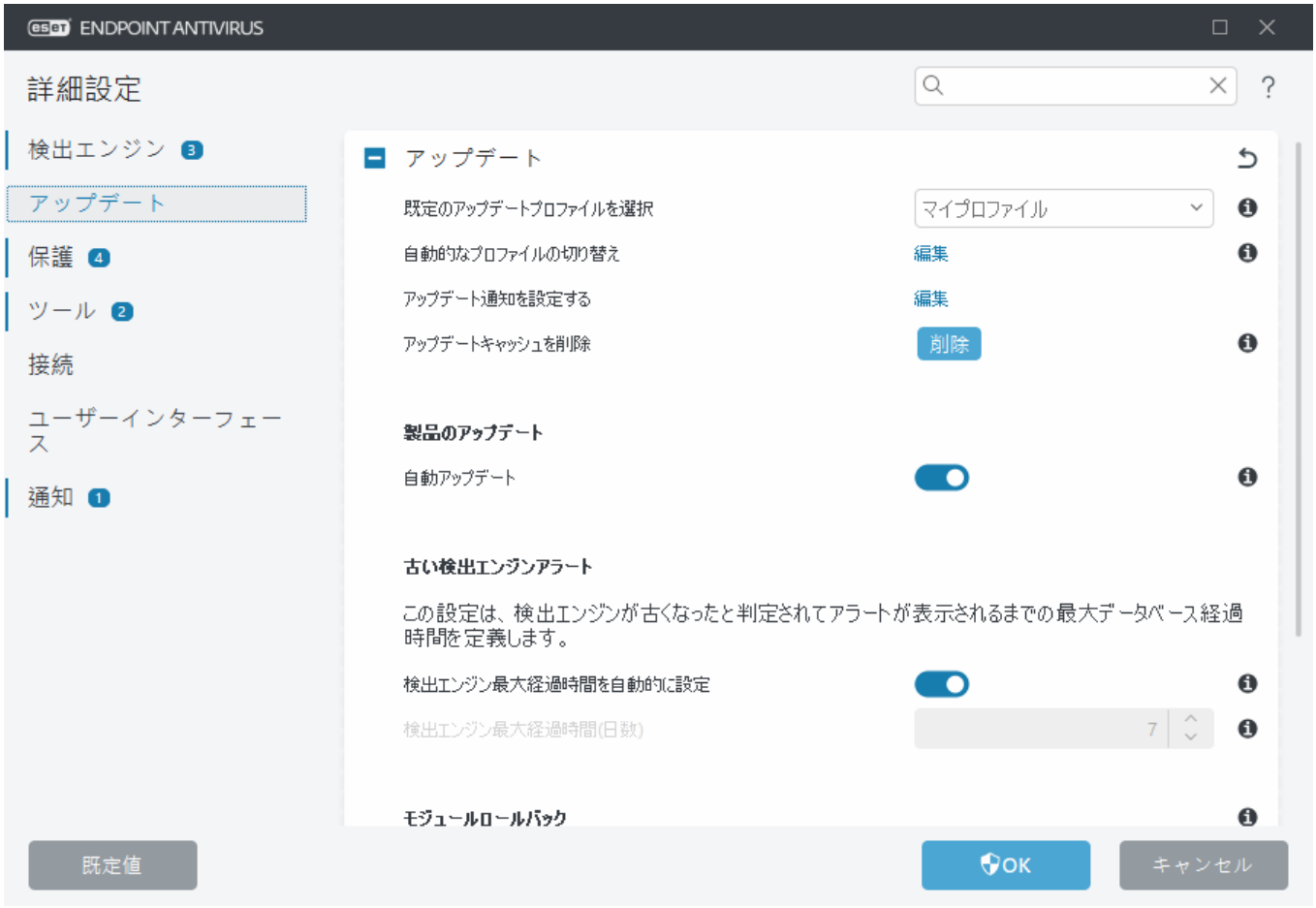
モジュールアップデートを試行するときに問題が発生した場合は、**アップデートキャッシュをクリア**の横の**クリア**をクリックして、一時アップデートファイルとキャッシュを消去します。

## 古い検出エンジンアラート

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

## モジュールロールバック

検出エンジン/プログラムモジュールの新規アップデートが不安定であったり破損している疑いのある場合、前のバージョンにロールバックし、設定した期間中のアップデートを無効にできます。




## プロファイル

さまざまなアップデートの設定用およびアップデートタスク用のアップデート プロファイルを作成できます。アップデートプロファイルを作成することは、常時変わるインターネット接続のプロパティに合わせて代替プロファイルが必要なモバイルユーザーにとって特に便利です。

[**編集するプロファイルを選択**]ドロップダウンメニューには、現在選択されているプロファイルが表示されます。これは、既定では[**マイプロファイル**]に設定されます。

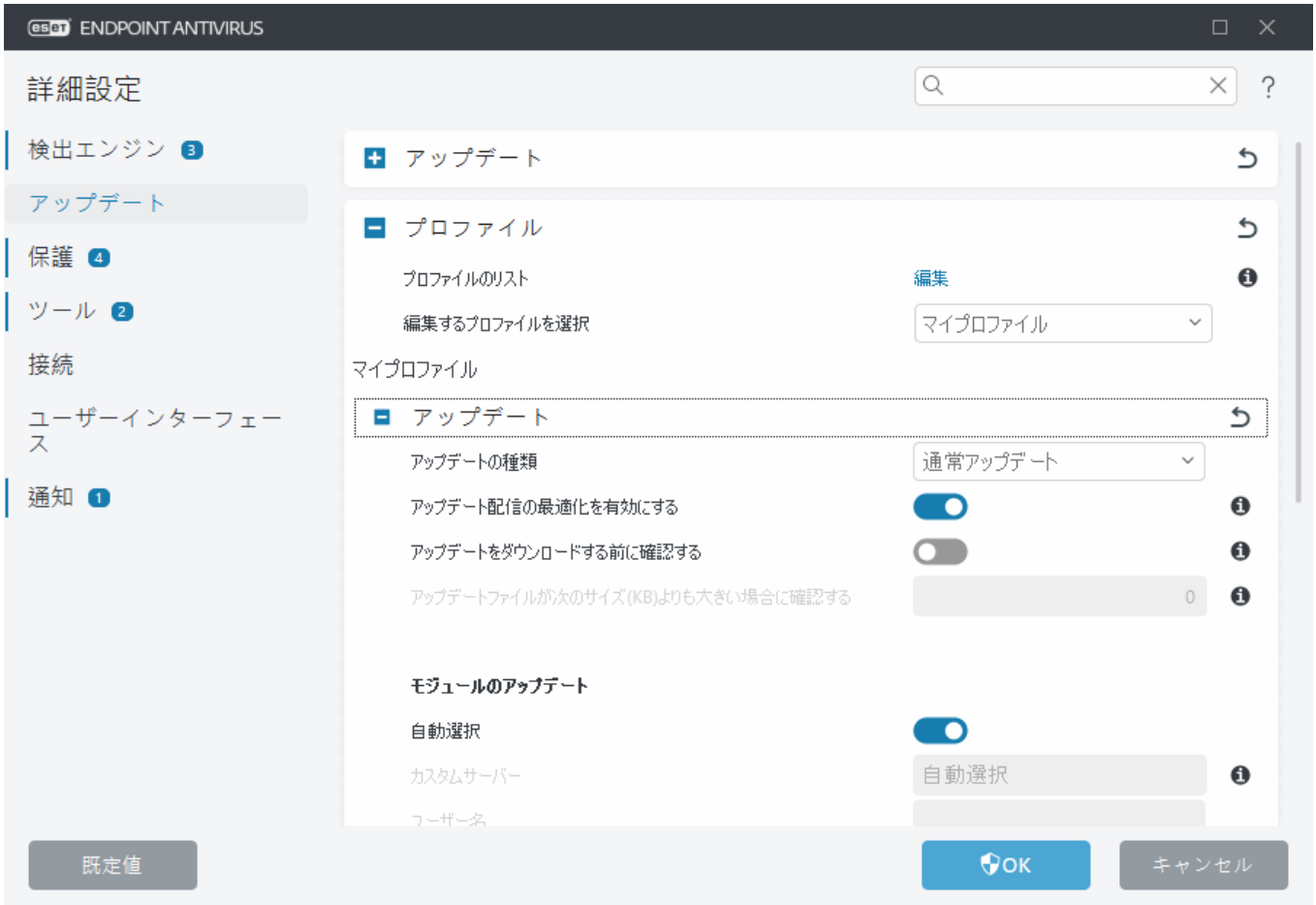
新しいプロファイルを作成するには、[**プロファイルのリスト**]の横の[**編集**]をクリックし、[**プロファイル名**]フィールドに自分の名前を入力して、[**追加**]をクリックします。

# 更新

既定では、**[アップデートの種類]**が**[通常アップデート]**に設定され、最低限のネットワークトラフィックでアップデートファイルがESETサーバーから自動的にダウンロードされます。テストモードのアップデート(**[リリース前アップデート]**オプション)は、徹底的な内部テストを経てリリースされ、近いうちに一般に公開されるアップデートです。テストモードを有効にすることで、最新の保護機能や修正プログラムを利用することができます。ただし、テストモードは常に安定しているとは限りません。最大限の可用性と安定性が必要な実働サーバーやワークステーションでは決して使用しないでください。[遅延アップデート]を使用すると、12時間以上の遅延のある最新バージョンのウイルスデータベース(つまり、実際の環境でテスト済みであって、そのため安定しているとみなされるデータベース)を提供する特別なサーバーからアップデートできます。

**アップデート配信最適化を有効にする** – 有効にするとCDN(コンテンツ配信ネットワーク)からアップデートファイルをダウンロードできます。この設定を無効にすると、専用ESETアップデートサーバーが過負荷状態になったときに、ダウンロードが中断され、速度が低下する場合があります。ファイアウォールによってESETアップデートサーバIPアドレスへのアクセスのみに制限されているときやCDNサービスへの接続が動作していないときに無効にすると役立ちます。

**アップデートをダウンロードする前に確認する** – アップデートファイルのダウンロードを確認または拒否できる通知が表示されます。アップデートファイルのサイズがアップデートファイルが次のサイズより大きい場合確認する(kB)フィールドに指定した値より大きい場合、確認ダイアログが表示されます。アップデートファイルのサイズが0 KBの場合は、常に確認ダイアログが表示されます。




## モジュールアップデート

**自動選択**オプションが既定で有効です。**カスタムサーバー**オプションは、アップデートファイルが保存される場所でESETアップデートサーバーを使用するときには、既定のオプションを選択することをお勧めします。

**検出定義のより頻繁なアップデートを有効にする** – 検出定義のアップデート間隔が短くなります。この設定を無効にすると、検出率に悪影響を及ぼす場合があります。

**リムーバブルメディアからモジュールのアップデートを許可する** – 作成されたミラーが含まれる場合は、リムーバブルメディアからアップデートできます。[自動]が選択されている場合、アップデートはバックグラウンドで実行されます。アップデートダイアログを表示する場合は、[常に確認する]を選択します。

ローカルのHTTPサーバー、つまりミラーを使用する場合は、アップデートサーバーを*http://*コンピューター名または*IP*アドレス:2221

SSLを使用するローカルのHTTPサーバーを使用する場合は、アップデートサーバーを*https://*コンピューター名または*IP*アドレス:2221

ローカル共有フォルダを使用する場合は、アップデートサーバーを次のように設定してください。\\コンピューター名または*IP*アドレス\共有フォルダー

> 上記の例で指定されたHTTPサーバーポート番号は、HTTP/HTTPSサーバーがリスニングするポートによって異なります。

### 製品のアップデート

製品のアップデートを参照してください。

### 接続オプション

接続オプションを参照してください。

## 配布用アップデート

アップデートミラーを参照してください。

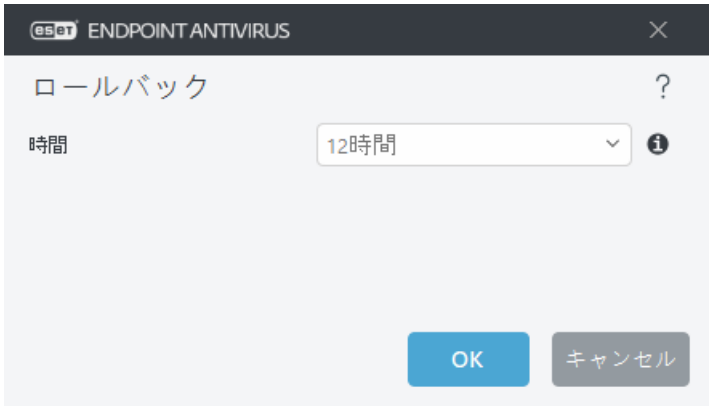
# アップデートのロールバック

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。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 Antivirus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。ウイルス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**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**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。

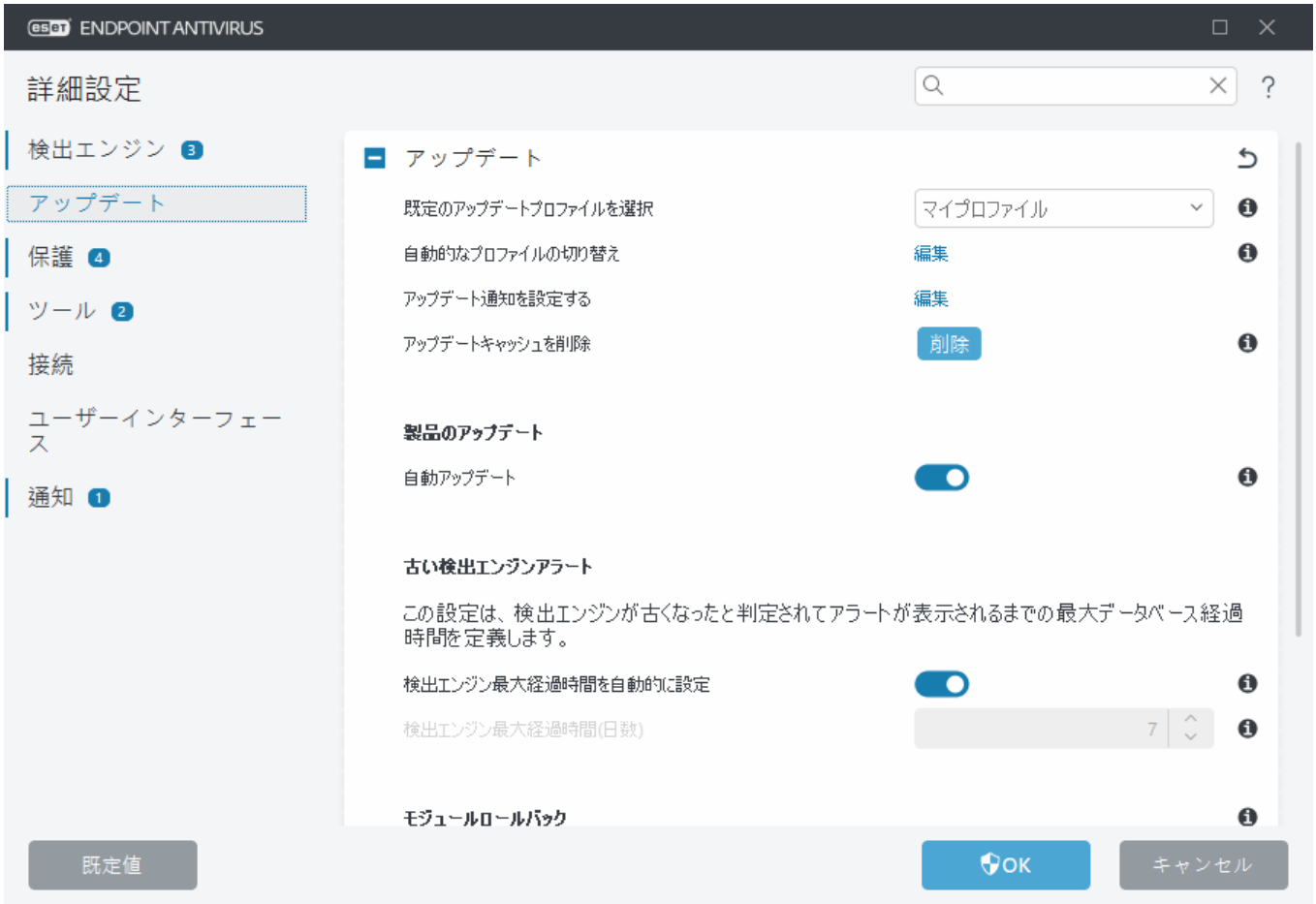
> 最大スナップショット数(例: 3つ)に達すると、最も古いスナップショットが48時間ごとに新しいスナップショットに置換されます。ESET Endpoint Antivirusは検出エンジンとプログラムモジュールのアップデートバージョンを最も古いスナップショットにロールバックします。

詳細設定 > **アップデート** > **アップデート** > **モジュールロールバック** > **ロールバック**を開き、**時間**ドロップダウンメニューから時間間隔を選択します。




アップデート機能を手動で復元するまで、定期アップデートを無期限に延期するには、[**取り消しまで**]を選択します。これには潜在的なセキュリティリスクがあるため、このオプションの選択はお勧めしません。

ロールバックを実行すると、**ロールバック**ボタンは**アップデートを許可**に変わります。[**時間**]ドロップダウンメニューで選択した期間中は、アップデートは許可されません。検出エンジンのバージョンは最も古いものにダウングレードされて、ローカルのコンピューターファイルシステムにスナップショットとして保存されます。



検出エンジンの最新のバージョンが22700であると仮定します。検出エンジンのスナップショットとして、22698と22696が保存されているとします。22697は利用できません。この例では、22697のアップデート中にコンピューターがオフになっていて、22697がダウンロードされるよりも前により新しいアップデートが利用できるようになっています。**ローカルに保存するスナップショットの数**フィールドを2に設定して、**ロールバック**をクリックすると、検出エンジン(プログラムモジュールを含む)はバージョン番号22696に復元されます。このプロセスには少々時間がかかることがあります。アップデートセクションで検出エンジンのバージョンがダウングレードされたかどうかを確認してください。

# 製品のアップデート

**製品のアップデート**セクションには、製品のアップデートに関連するオプションがあります。このプログラムでは、新しい製品のアップデートが使用可能になったときの動作を事前に定義することができます。

製品のアップデートによって、新しい機能が提供されたり、これまでのバージョンの既存の機能が変更されたりします。ユーザーが操作を行わずに自動的にアップデートが実行されるようにすることも、アップデートするかどうかをユーザーが決定できるようにすることもできます。製品のアップデートをインストールした後、コンピューターの再起動が必要になることがあります。

**自動アップデート** – 特定のアップデートプロファイルの自動アップデートを一時停止すると、他のネットワークまたは測定された接続を使用してインターネットに接続している間に、自動製品アップデートが一時的に無効になります。最新の機能と可能なかぎり最高レベルの保護に常にアクセスするために、この設定を常に有効にしてください。自動アップデートの詳細については、自動アップデートFAQを参照してください。

既定では、製品のアップデートはESETリポジトリサーバーからダウンロードされます。大規模な環境やオフライン環境では、トラフィックを分散し、製品ファイルの内部キャッシュを有効にすることができます。

プログラムコンポーネントのアップデートのカスタムサーバーの定義

1. **カスタムサーバー**フィールドで製品のアップデートへのパスを定義します。
HTTP(S)リンク、SMBネットワーク共有パス、ローカルディスクドライブ、またはリムーバブルメディアパスにすることができます。ネットワークドライブの場合、マッピングされたドライブ文字の代わりにUNCパスを使用できます。
2. 必要ではない場合、**ユーザー名**と**パスワード**を空欄にします。
必要に応じて、カスタムWebサーバーのHTTP認証について、該当する資格情報をここで定義します。
3. 変更を確認し、標準のESET Endpoint Antivirusアップデートを使用して、製品のアップデートの存在をテストします。

最適なオプションの選択方法は、設定が適用されるワークステーションによって異なります。ワークステーションとサーバーとでは異なる点に注意してください。たとえば、製品のアップデート後にサーバーを自動的に再起動すると、企業に重大な損害が生じることがあります。

# 接続オプション

特定のアップデートプロファイルのプロキシサーバー設定オプションにアクセスするには、詳細設定 > **アップデート** > **プロファイル** > **アップデート** > **接続オプション**を開きます。

## プロキシサーバー

[**プロキシモード**]ドロップダウンメニューをクリックし、次の3つのオプションのいずれかを選択します。

- プロキシサーバを使用しない
- プロキシサーバを使用して接続する
- グローバルプロキシサーバ設定を使用する

**グローバルプロキシサーバー設定を使用する**を選択すると、詳細設定 > **接続** > **プロキシサーバー**で既に指定されているプロキシサーバー設定が使用されます。

[**プロキシサーバを使用しない**]を選択するとESET Endpoint Antivirusのアップデートにプロキシサーバーを使用しないように指定されます。

[**プロキシサーバを使用して接続する**]オプションは、次の場合に選択する必要があります。

- [**ツール**] > [**プロキシサーバー**]で定義されている以外のプロキシサーバーはESET Endpoint Antivirusをアップデートするために使用されます。この設定では、必要に応じて、[**プロキシサーバー**]の下で、そのプロキシサーバーのアドレス、**ポート**(既定は3128)、**ユーザー名**と**パスワード**を指定する必要があります。
- プロキシサーバー設定はグローバルには設定されませんがESET Endpoint Antivirusはアップデートを取得するためにプロキシサーバーに接続する場合。
- コンピュータがプロキシサーバーを介してインターネットに接続される場合。設定はプログラムのインストール時にブラウザーから取得されますが、変更されている(ISPを変更するなど)場合、このウィンドウから一覧のプロキシ設定が正しいことを確認します。しなかった場合、プログラムはアップデートサーバーに接続できません。

プロキシサーバーの既定の設定は、[**グローバルプロキシサーバ設定を使用する**]です。

**プロキシが使用できない場合は直接接続を使用する** –接続できない場合はアップデート中にプロキシをバイパスします。

## Windows共有

Windows NTオペレーティングシステムのバージョンでローカルサーバーからアップデートする場合は、既定で、ネットワーク接続ごとに認証が必要です。

このようなアカウントを構成するには、ドロップダウンメニューから**LANに接続するアカウント**を選択します。

- **システムアカウント(既定)**
- **現在のユーザー**
- **指定したユーザー**

システムアカウントを認証に使用するには、[**システムアカウント(既定)**]を選択します。一般に、アップデートの設定のメインセクションで認証データが指定されていない場合、認証プロセスは実行されません。

現在ログインしているユーザーアカウントを使用して認証が行われるようにするには、[**現在のユーザー**]を選択します。この方法の欠点は、ログインしているユーザーがいない場合、プログラムがアップデートサーバーに接続できない点です。

特定のユーザーアカウントが認証に使用されるようにするには、[**指定されたユーザー**]を選択します。この方法は、既定のシステムアカウント接続に失敗した場合に使用してください。指定されたユーザーのアカウントは、ローカルサーバー上のアップデートファイルディレクトリーにアクセスできなければなりません。アクセスできない場合は、接続を確立して、アップデートファイルをダウンロードすることができません。

**ユーザー名**と**パスワード**は任意です。

[**現在のユーザー**]または[**指定されたユーザー**]オプションが有効になっている場合、プログラムのIDを目的のユーザーに変更すると、エラーが発生することがあります。そのため、アップデートの設定のメインセクションでLANの認証データを入力することをお勧めします。このアップデート設定セクションでは、認証データは次のように入力する必要があります。*domain_name\user*(これがワークグループの場合は*workgroup_name\name*と入力します)およびパスワード。ローカルサーバーのHTTPミラーからアップデートする場合、認証は不要です。

アップデートファイルのダウンロード後もサーバーとの接続がアクティブなままになる場合は、[アップデート終了後にサーバから**切断**する]を選択して強制的に切断します。

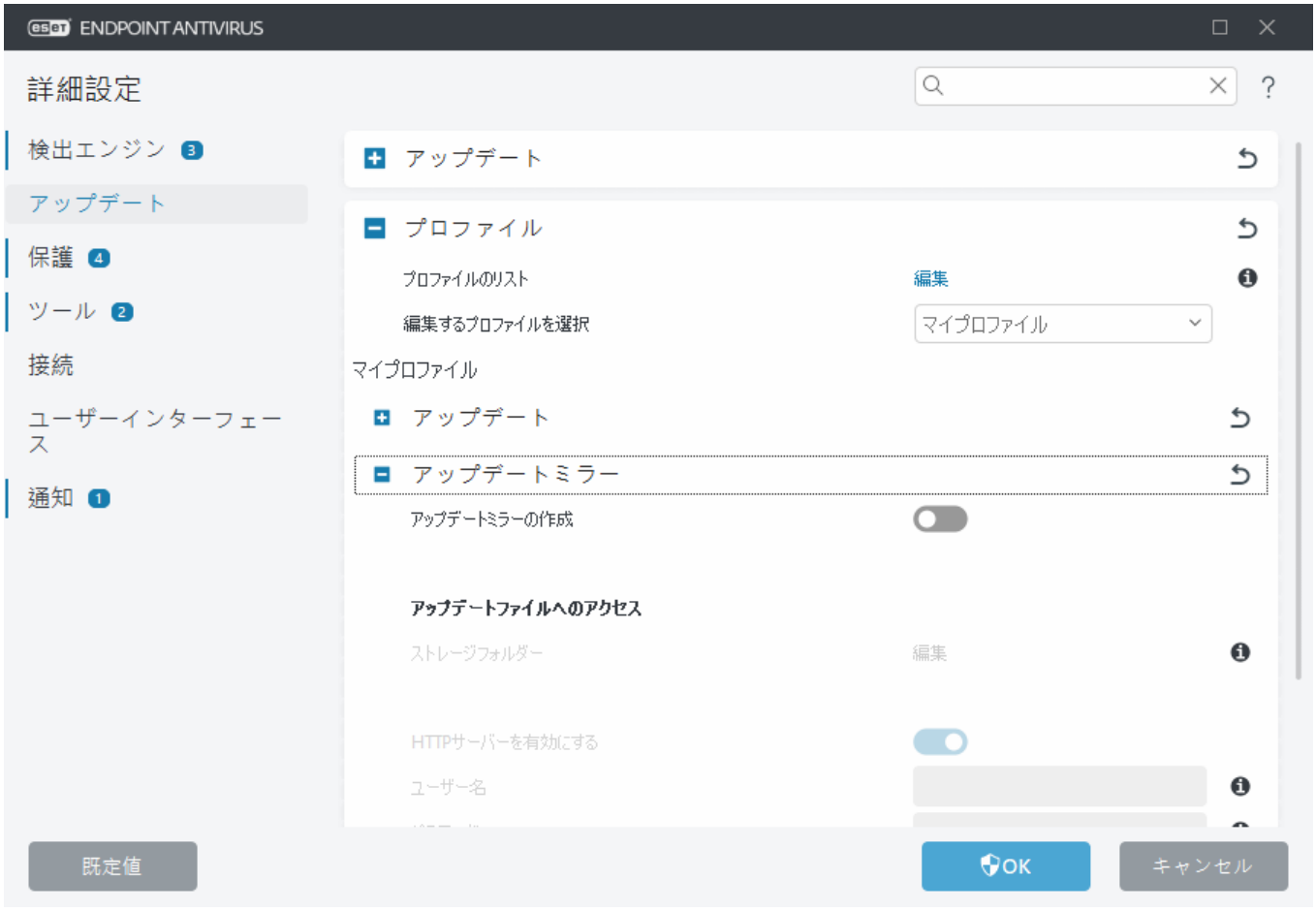
# 配布用アップデート

ESET Endpoint Antivirusでは、ネットワーク内の他のワークステーションをアップデートするために使用できるアップデートファイルのコピーを作成することができます。「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。

アップデートミラーは、同じ世代のESET Endpoint Antivirus for Windowsを実行するワークステーションをアップデートするために使用できるアップデートファイルのコピーを作成します。(たとえばESET Endpoint Antivirus for Windowsバージョン10.xはバージョン10.x (ESET Endpoint Antivirus for WindowsとESET Endpoint Security for Windows)のアップデートファイルのみを作成します)

多数のクライアントを管理するためにESET PROTECTが使用されるネットワークのインターネットトラフィックを最小化するために、クライアントをミラーとして設定するのではなくESET Bridgeを使用することをお勧めしますESET Bridgeは、オールインワンインストーラーを使用してESET PROTECTと一緒にインストールするか、スタンドアロンコンポーネントとしてインストールできますESET Bridge, Apache HTTPプロキシ、ミラーツール、および直接接続の詳細と違いについては、ESET PROTECTオンラインヘルプページを参照してください。

詳細設定 > **アップデート** > **プロファイル** > **アップデートミラー**で、ローカルミラーサーバーの設定オプションを使用できます。




クライアントワークステーションでミラーを作成するには、[**アップデートミラーを作成**]を有効にします。このチェックボックスをチェックすると、アップデートファイルへのアクセス方法やミラー化されたファイルへのパスなど、他のミラー設定オプションがアクティブになります。

## アップデートファイルへのアクセス

**HTTPサーバーを有効にする** – このチェックボックスをチェックすると、HTTP経由でアップデートファイルにアクセスすることができます。認証情報は必要ありません。

ミラーサーバーへのアクセス方法の詳細については、「ミラーからのアップデート」を参照してください。ミラーにアクセスする基本的な方法は2つあります。アップデートファイルを含むフォルダが共有ネットワークフォルダとして表示するか、クライアントがHTTPサーバー上にあるミラーにアクセスする方法です。

ミラーのアップデートファイルを保存するために使用するフォルダーは、[**ストレージフォルダ**]で定義します。別のフォルダーを選択するには、[**クリア**]をクリックして、定義済みフォルダーの*C:\ProgramData\ESET\ESET Endpoint Antivirus\mirror*を削除し、[**編集**]をクリックして、ローカルフォルダーまたは共有ネットワークフォルダーのフォルダーを参照します。指定したフォルダの認証が必要な場合は、[**ユーザー名**]フィールドと[**パスワード**]フィールドで認証データを指定する必要があります。選択した保存先フォルダーが、Windows NT/2000/XPオペレーティングシステムを実行するネットワークディスクにある場合、選択したフォルダーに対する書き込み権限があるユーザー名とパスワードを指定する必要があります。ユーザー名は、ドメイン/ユーザーまたはワークグループ/ユーザーという形式で入力する必要があります。対応するパスワードを必ず指定してください。

# ミラーのHTTPサーバーとSSL

**ミラー**タブの**HTTPサーバー**セクションで、HTTPサーバーがリスニングする**サーバーポート**、およびHTTPサーバーで使用される**認証**のタイプを指定できます。既定では、サーバーポートは**2221**に設定されています。

[**認証**] – アップデートファイルにアクセスするために使用される認証方法を定義します。使用可能なオプションは[**なし**]、[**基本**]、[**NTLM**]。基本のユーザー名およびパスワード認証でbase64エンコードを使用する場合は、[**基本**]を選択してください。[**NTLM**]を選択すると、安全なエンコード方法でエンコードされます。認証については、アップデートファイルを共有するワークステーション上で作成されたユーザーが使用されます。既定の設定は[**なし**]で、認証なしでアップデートファイルにアクセスすることができます。

**ユーザー名**と**パスワード**が必要な場合のみ入力してください。ミラーHTTPサーバーへのアクセスにのみ使用されます。

HTTPS (SSL)サポートを使ったHTTPサーバーを実行する場合、[**証明書チェーンファイル**]を追加するか、自己署名証明書を生成します。以下の**証明書タイプ**を使用できますASN、PEM、PFXセキュリティの強化のためHTTPSプロトコルを使用してアップデートファイルをダウンロードできます。このプロトコルを使用してデータ転送やログイン資格情報を追跡するのはほぼ不可能です。**秘密鍵タイプ**オプションは、既定で**統合**に設定されています。このため、**秘密鍵ファイル**オプションは既定で無効です。つまり、秘密鍵は選択した証明書チェーンファイルの一部です。

**HTTPSミラーの自己署名証明書**
HTTPSミラーサーバーを使用している場合は、その証明書をすべてのクライアントコンピューターの信頼できるルートストアにインポートする必要がありますWindowsでの信頼できるルート証明書のインストールを参照してください。

# ミラーからのアップデート

ミラーを構成するには、2つの基本方法があります。ミラーは、基本的に、クライアントがアップデートファイルをダウンロードできるリポジトリです。アップデートファイルがあるフォルダは、共有ネットワークフォルダまたはHTTPサーバーとして表示されます。

アップデートミラーは、同じ世代のESET Endpoint Antivirus for Windowsを実行するワークステーションをアップデートするために使用できるアップデートファイルのコピーを作成します。(たとえばESET Endpoint Antivirus for Windowsバージョン10.xはバージョン10.x (ESET Endpoint Antivirus for WindowsとESET Endpoint Security for Windows)のアップデートファイルのみを作成します)

## 内蔵のHTTPサーバーを使用したミラーへのアクセス

これは、事前定義されたプログラム設定で指定される、既定の設定ですHTTPサーバを使用してミラーにアクセスできるようにするには、[詳細設定] > [**アップデート**] > [**プロファイル**] > [**アップデートミラー**]タブ)に移動して、[**更新ミラーの作成**]オプションを選択します。

**ミラー**タブの**HTTPサーバー**セクションで、HTTPサーバーがリスニングする**サーバーポート**、およびHTTPサーバーで使用される**認証**のタイプを指定できます。既定では、サーバーポートは**2221**に設定されています。

[**認証**] – アップデートファイルにアクセスするために使用される認証方法を定義します。使用可能なオ

プションは[**なし**]⍰[**基本**]⍰[**NTLM**]。基本のユーザー名およびパスワード認証でbase64エンコードを使用する場合は、[**基本**]を選択してください。[**NTLM**]を選択すると、安全なエンコード方法でエンコードされます。認証については、アップデートファイルを共有するワークステーション上で作成されたユーザーが使用されます。既定の設定は[**なし**]で、認証なしでアップデートファイルにアクセスすることができます。

HTTPサーバー経由によるアップデートファイルへのアクセスを許可する場合、ミラーフォルダーは、ミラーフォルダーを作成するESET Endpoint Antivirusのインスタンスと同じコンピューターに置かれている必要があります。

ミラーからのアップデートが数回失敗すると、メインメニューの[アップデート]ペインに、**無効なユーザー名またはパスワード**エラーが表示されます。詳細設定>**アップデート**>**プロファイル** > **アップデートミラー**に移動し、ユーザー名とパスワードを確認することをお勧めします。このエラーの最も一般的な原因は、入力した認証データが正しくないことです。

ミラーサーバーの設定後、クライアントワークステーション上に新しいアップデートサーバーを追加する必要があります。手順は次のとおりです。

- 詳細設定を開き、**アップデート** > **プロファイル** > **アップデート** > **モジュールのアップデート**をクリックします。
- **自動選択**をオフにし、次のいずれかの形式で、**アップデートサーバー**フィールドに新しいサーバーを追加します。
  *http://*<サーバの*IP*アドレス>:2221
  *https://*<サーバーの*IP*アドレス>:2221 (SSLを使用する場合)

## システム共有を使用したミラーへのアクセス

まず、ローカルデバイスまたはネットワークデバイスに共有フォルダーを作成する必要があります。ミラーのフォルダーを作成する際には、フォルダーにアップデートファイルを保存するユーザーに"書き込み"アクセス権を与え、ミラーフォルダーからESET Endpoint Antivirusをアップデートするすべてのユーザーに"読み取り"アクセス権を与える必要があります。

次に、詳細設定 > **アップデート** > **プロファイル** > **アップデートミラー**タブで、**HTTPサーバーを有効にする**チェックボックスのチェックを外して、ミラーへのアクセスを設定します。プログラムのインストールパッケージでは、このチェックボックスは既定でチェックされています。

共有フォルダーがネットワーク内の別のコンピューターにある場合は、そのコンピューターへのアクセスに使用する認証データを入力する必要があります。認証データを入力するには、の詳細設定を開いて、**アップデート** > **プロファイル** > **アップデート** > **接続オプション** > **Windows共有** > **アップデートサーバーへの接続に使用するユーザーアカウント**。この設定は、「アップデートサーバーへの接続に使用するユーザーアカウント」セクションで説明されているアップデートの設定と同じです。

ミラーフォルダにアクセスするには、ミラーが作成されたコンピュータにログインするために使用されたアカウントでこの操作を実行する必要があります。コンピュータがドメインの場合、「ドメイン\ユーザー」ユーザー名を使用してください。コンピュータがドメインにない場合は、「サーバーのIPアドレス\ユーザー」または「ホスト名\ユーザー」を使用してください。

ミラーの設定が完了したら、次の手順で、クライアントワークステーションで、アップデートサーバーとして*\\UNC\PATH*を設定します。

1. [詳細設定]を開き、[**アップデート**]> [**プロファイル**] > [**アップデート**]をクリックします。
2. **モジュールのアップデート**の横の**自動選択**をオフにし、**アップデートサーバー**フィールドに新しいサーバーを追加します(*\\UNC\PATH*形式)。

アップデートが正しく動作するには、ミラーフォルダのパスをUNCパスとして指定する必要があります。マップされたドライブからのアップデートは動作しない場合があります。

**ミラーツールを使用したミラーの作成**
ミラーツールは、Endpointミラーが作成するフォルダーとは別のフォルダー構造を作成します。各フォルダーには、製品のグループのアップデートファイルが格納されます。ミラーを使用する製品のアップデート設定で、正しいフォルダーへの完全パスを指定する必要があります。
たとえば、ミラーからESET PROTECTをアップデートするには、アップデートサーバーを(HTTPサーバーのルートの場所に応じて)次のように設定します。
`http://your_server_address/mirror/eset_upd/ep10`

最後のセクションでは、プログラムコンポーネント(PCU)を制御します。既定では、ダウンロードされたプログラムコンポーネントは、ローカルのミラーにコピーできるようになっています。**製品のアップデート**が選択されている場合、ファイルが使用可能な状態になると、自動的にローカルミラーにコピーされるため、**アップデート**をクリックする必要はありません。製品のアップデートの詳細については、アップデートモードを参照してください。

# ミラーアップデートの問題のトラブルシューティング

一般的に、ミラーサーバーからのアップデート中の問題は、次の1つ以上の原因が該当します。ミラーフォルダオプションの指定が正しくない、ミラーフォルダへの認証データが正しくない、ミラーからアップデートファイルのダウンロードを試行するローカルワークステーションの設定が正しくない、これらの理由の組み合わせ。以下に、ミラーからのアップデート時に発生する可能性のあるよくある問題の概要を紹介します。

**ESET Endpoint Antivirusミラーサーバへの接続エラーが報告される** – 原因として、ローカルワークステーションが更新をダウンロードするアップデートサーバー(ミラーフォルダーのネットワークパス)が正しく指定されていないことが考えられます。フォルダーを確認するにはWindowsの[**スタート**]ボタンをクリックし、[**ファイル名を指定して実行**]をクリックします。次に、フォルダー名を入力し、[**OK**]をクリックします。フォルダーの内容が表示されます。

**ESET Endpoint Antivirusでユーザー名とパスワードが要求される** – 原因として、アップデートセクションで認証データ(ユーザー名とパスワード)が正しく入力されていないことが考えられます。ユーザー名とパスワードは、プログラムが自身を更新するアップデートサーバーへのアクセスを許可するために使用されます。認証データが適切な形式で正しく入力されていることを確認してください。たとえば、<ドメイン>/<ユーザー名>または<ワークグループ>/<ユーザー名>とそれに対応するパスワードを入力します。"全てのユーザー"がミラーサーバにアクセス可能であっても、全てのユーザーがアクセスを許可されているわけではありません。"全てのユーザー"とは、全ての認証されていないユーザーを意味するのではなく、全てのドメインユーザーがフォルダにアクセスできることを意味します。つまり、"全てのユーザー"がフォルダにアクセス可能な場合でも、アップデートの設定セクションでドメインユーザー名とパスワードを入力する必要があります。

**ESET Endpoint Antivirusミラーサーバーへの接続エラーが報告される** – ミラーのHTTPサーバーへのアクセスについて定義されているポート上の通信がブロックされています。

**ESET Endpoint Antivirusがアップデートファイルのダウンロード中にエラーを報告する** – 原因として、ローカルワークステーションのアップデートファイルのダウンロード元であるアップデートサーバー(ミラーフォルダーのネットワークパス)が正しく指定されていないことが考えられます。

# 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。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、修復が開始されます。保護は、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。

保護を細かく設定するには、詳細設定 > **保護**を開きます。

保護の変更は、経験豊富なユーザーだけが行ってください。設定が正しくないと、システムの保護レベルが低下する可能性があります。

このセクションの内容:



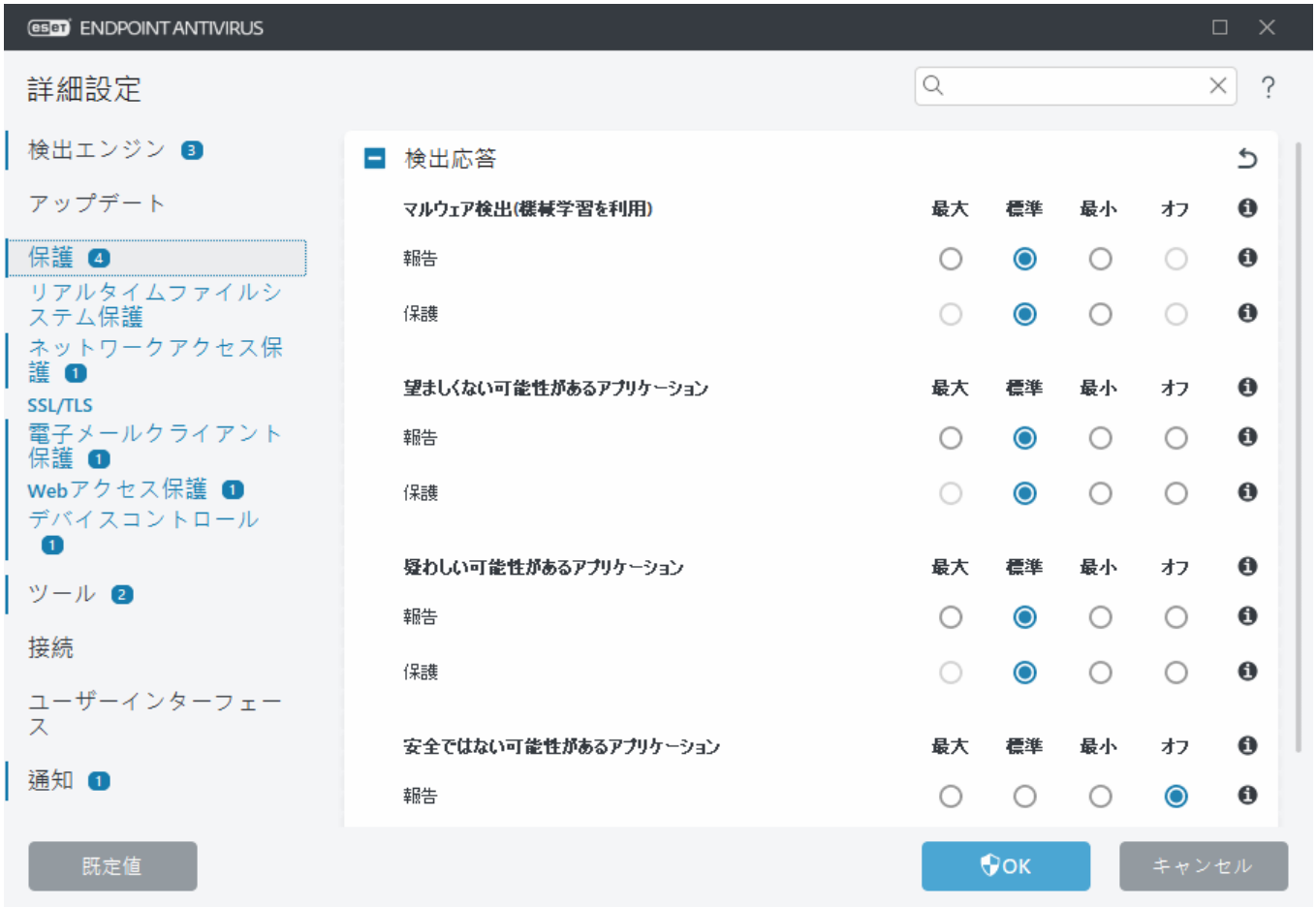
---

## 検出応答

検出応答を使用すると、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。

- **マルウェア検出(機械学習を利用)** – コンピューターウイルスは、コンピューターの既存のファイルの前後に追加される悪意のあるコードです。ただし、「ウイルス」という用語は、よく間違って使用されます。「マルウェア」(悪意のあるソフトウェア)がより正確な用語です。マルウェアの検出は、検出エンジンモジュールと機械学習コンポーネントを組み合わせて実行されます。この種のアプリケーションの詳細については、「用語集」を参照してください。

- **望ましくない可能性のあるアプリケーション**– グレイウェアまたは望ましくない可能性があるアプリケーション(PUA)は、ウイルスまたはトロイの木馬などの他のタイプのマルウェアほどはっきりとした意図がない幅広いソフトウェアのカテゴリです。ただし、追加の不審なソフトウェアをインストールし、デジタルデバイスの動作または設定を変更し、ユーザーによって承認または想定されていないアクティビティを実行する可能性があります。この種のアプリケーションの詳細については、「用語集」を参照してください。
- **疑わしい可能性があるアプリケーション**には、パッカーまたはプロテクターで圧縮されたプログラムが含まれています。この種類の防御は、多くの場合、マルウェアの作成者が検知されるのを逃れるために利用します。
- **安全ではない可能性があるアプリケーション**は、不正な目的で悪用される可能性のある、市販の適正なソフトウェアです。安全ではない可能性のあるアプリケーション(PUA)の例には、リモートアクセスツール、パスワード解析アプリケーション、キーロガー(ユーザーが入力した各キーストロークを記録するプログラム)が含まれます。この種のアプリケーションの詳細については、「用語集」を参照してください。




**改善された保護**

高度な機械学習は、機械学習に基いた検出を取込んだ高度な保護レイヤーとして、保護の一部になりました。このタイプの保護の詳細については、用語集をお読みください。

---

# 報告設定

検出が発生するとき(例: 脅威が見つかり、マルウェアとして分類される)に、情報が検出ログに記録され、ESET Endpoint Antivirusで設定されている場合はデスクトップ通知が発生します。

報告しきい値は、カテゴリごとに設定されます。

1. マルウェア検出
2. 望ましくない可能性があるアプリケーション
3. 安全ではない可能性があるアプリケーション
4. 疑わしい可能性があるアプリケーション

機械学習コンポーネントを含む検出エンジンでレポートが実行されます。現在の保護しきい値よりも高い報告しきい値を設定できます。これらのレポート設定は、オブジェクトのブロック、駆除、または削除に影響しません。

カテゴリの報告のしきい値(またはレベル)を修正する前に、次の点をお読みください。

| しきい値 | 説明 |
|---|---|
| **最大** | カテゴリの報告は最大感度に設定されています。より多くの検出が報告されます。**最大**設定では、オブジェクトが誤ってカテゴリとして特定される場合があります。 |
| **標準** | カテゴリの報告は標準に設定されています。この設定は、検出率のパフォーマンスおよび精度と、誤った報告されるオブジェクト数の間でバランスを保つように最適化されています。 |
| **最小** | カテゴリの報告は、誤って特定されるオブジェクトの数を最小限に抑えながら、効率的なレベルの保護を維持するように設定されています。確率が明らかであり、カテゴリの動作と一致するときにのみ、オブジェクトが報告されます。 |
| **オフ** | カテゴリの報告は有効ではありません。このタイプの検出は見つからないか、報告されないか、駆除されません。このため、この設定では、この検出タイプからの保護が無効になります。マルウェア報告ではオフを使用できません。これは、安全でない可能性があるアプリケーションの既定値です。 |

### ESET Endpoint Antivirus保護モジュールの使用可否

選択したカテゴリしきい値の保護モジュールの使用可否(有効または無効)は次のとおりです。

| | 最大 | 標準 | 最小 | オフ* |
|---|---|---|---|---|
| 高度な機械学習モジュール | ✓ (強モード) | ✓ (低モード) | X | X |
| 検出エンジンモジュール | ✔ | ✔ | ✔ | X |
| 他の保護モジュール | ✔ | ✔ | ✔ | X |

* 非推奨。

### 製品バージョン、プログラムモジュール、ビルド日を確認します

1. **ヘルプとサポート** > **ESET Endpoint Antivirusについて**をクリックします。
2. **バージョン情報**画面で、テキストの最初の行にはESET製品のバージョン番号が表示されます。
3. **モジュールを表示**をクリックすると、特定のモジュールに関する情報が表示されます。

## 基本事項

環境に適切なしきい値を設定するときの複数の基本事項:

- **標準**しきい値は、ほとんどの設定で推奨されます。
- **注意**しきい値は、セキュリティソフトウェアにオブジェクトの誤検出を最小化することが優先される環境で推奨されます。
- 報告しきい値が高いほど、検出率が上がりますが、オブジェクトの誤検出の確率も上がります。
- 実際の観点からは、100%の検出率の保証はなく、マルウェアとしてのクリーンなオブジェクトの誤った分類を回避する可能性は0%です。
- ESET Endpoint Antivirusとモジュールを最新に保つことで、パフォーマンスと検出率の正確性、および誤検出のオブジェクト数の間でバランスを最大化します。

---

# 保護設定

カテゴリに分類されたオブジェクトが報告されると、そのオブジェクトがブロックされ、その後に駆除、削除、または隔離に移動されます。

カテゴリ保護のしきい値(またはレベル)を修正する前に、次の点をお読みください。

| しきい値 | 説明 |
| --- | --- |
| **最大** | 報告されたアグレッシブ(以下)レベルの検出はブロックされ、自動修復(たとえば駆除)が開始します。すべてのエンドポイントがアグレッシブ設定で検査され、誤って報告されたオブジェクトが検出除外に追加されたときには、この設定が推奨されます。 |
| **標準** | 報告されたバランス(以下)レベルの検出はブロックされます。自動修復(駆除)が開始します。 |
| **最小** | 報告された注意レベルの検出はブロックされます。自動修復(駆除)が開始します。 |
| **オフ** | 誤って報告されたオブジェクトを特定して除外する際に便利です。<br>マルウェア保護ではオフを使用できません。これは、安全でない可能性があるアプリケーションの既定値です。 |

---

# ベストプラクティス

## 管理対象外(個別のクライアントワークステーション)

既定の推奨値をそのまま使用してください。

## 管理された環境

通常、これらの設定は、ポリシー経由でワークステーションに適用されます。

## 1. 初期フェーズ

このフェーズは最大で1週間かかる場合があります。

- すべての**報告**しきい値を**標準**に設定します。
  注記:必要に応じて、**最大**に設定します。
- マルウェアの**保護**を**標準**に設定するか、保持します。
- 他のCATEGORIESの**保護**を**最小**に設定します。
  **備考:**このフェーズでは、**保護**しきい値を**最大**に設定することは推奨されません。誤検出を含むすべての検出が修復されるためです。
- 検出ログから誤検出のオブジェクトを特定し、まず検出除外に追加します。

## 2. 移行フェーズ

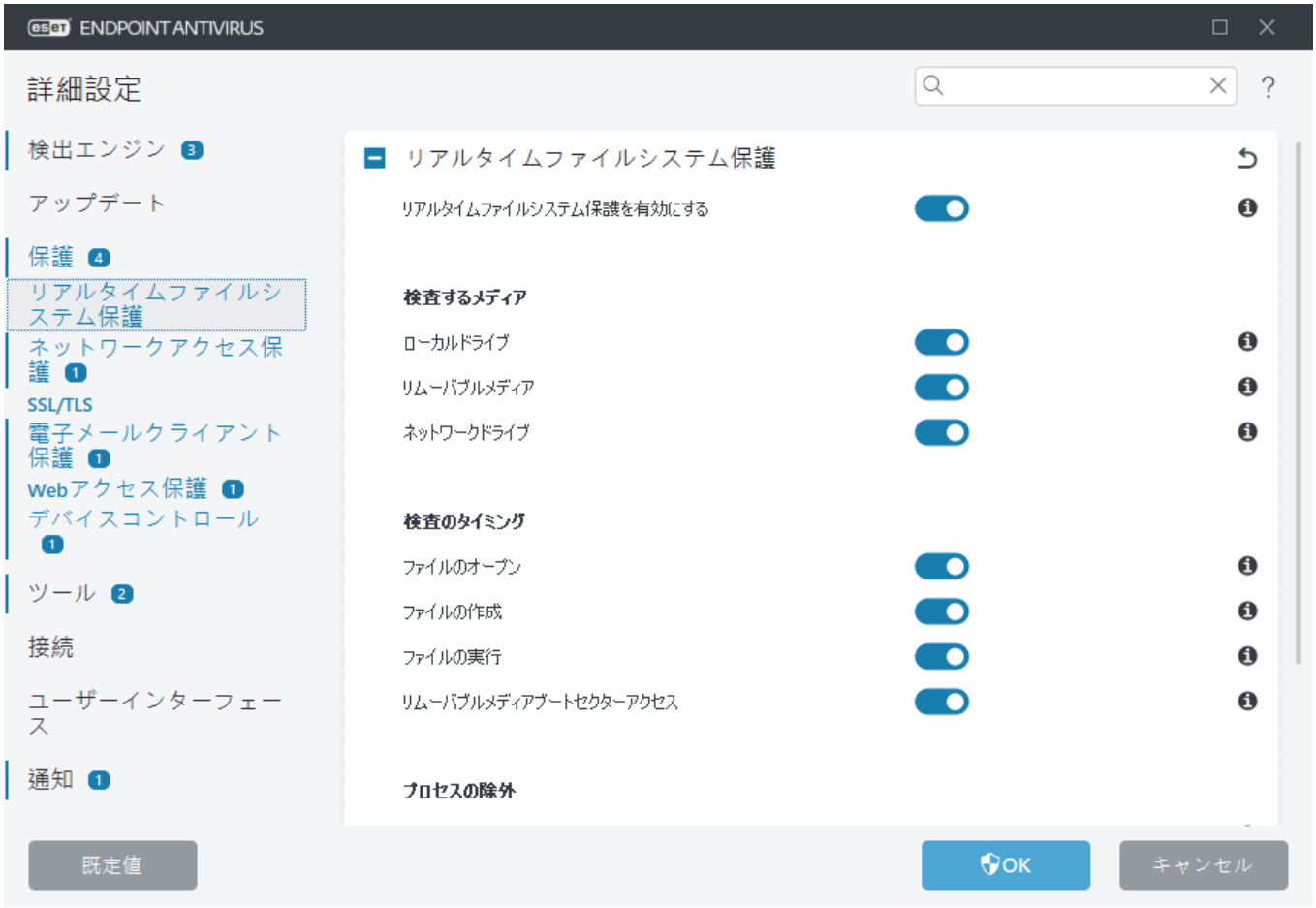
- 「本番フェーズ」をテストとして一部のワークステーションに実装します(ネットワークのすべてのワークステーションではない)。

## 3. 本番フェーズ

- すべての**保護**しきい値を**標準**に設定します。
- リモートで管理するときにはESET Endpoint Antivirusの該当するウイルス対策定義済みポリシーを使用します。
- **最大**保護しきい値は、最高の検出率が必要で、オブジェクトの誤検出が許容される場合に設定できます。
- 検出ログまたはESET PROTECTレポートに見つかっていない検出があるかどうかを確認してください。

# リアルタイムファイルシステム保護

リアルタイムファイルシステム保護は、ファイルを開く、作成、実行操作が行われたときに、システムのすべてのファイルを悪意のあるコードから保護します。




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。詳細設定 > **保護** > **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**リアルタイムファイルシステム保護を有効にする**を無効にしないことをお勧めします。

## 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** – すべてのシステムと固定ハードドライブを検査します(例: *C:*、*D:*)。
- **リムーバブルメディア** – CD/DVD、USBストレージ、メモリカードなどを検査します。
- **ネットワークドライブ** – すべてのマッピングされたネットワークドライブ(例: *\\store04*としての*H:*)または直接アクセスネットワークドライブ(例: *\\store08*)を検査します。

既定の設定を変更するのは、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、特別な場合だけにすることをお勧めします。

## 検査のタイミング

既定では、ファイルを開く、作成、実行するときに、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** – ファイルを開くときに検査します。
- **ファイルの作成** – 作成または修正されたファイルを検査します。
- **ファイルの実行** – **ファイルを実行するときに検査します。**
- **リムーバブルメディアブートセクターアクセス** – ブートセクタを含むリムーバブルメディアがデバイスに挿入されると、ブートセクターがただちに検査されます。このオプションでは、リムーバブルメディアファイル検査は有効になりません。リムーバブルメディアファイル検査は、**[マルウェア検査] > [リムーバブルメディア]**にあります。**リムーバブルメディアブートセクターアクセス**が正常に動作するには□ThreatSenseで**ブートセクタ□/UEFI**を有効にしたままにする必要があります。

## プロセスの除外

プロセスの除外を参照してください。

## ThreatSense

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**技術の検出方法(ThreatSense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。

システムの使用領域を最小化するために、リアルタイム保護の使用時、すでに検査されたファイルは(変更がない限り)繰り返し検査されません。各検出エンジンがアップデートされると、直ちにファイルが再検査されます。この動作は[**スマート最適化**]を使用して設定します。この**スマート最適化**が無効の場合、すべてのファイルがアクセスのたびに検査されます。この設定を変更するには、詳細設定 > **保護 > リアルタイムファイルシステム保護**を開きます。**ThreatSense > その他**をクリックし、**スマート最適化を有効にする**を選択または選択解除します。

リアルタイムファイルシステム保護では、追加のThreatSenseパラメータを設定することもできます。

# プロセスの除外

プロセス除外機能では、リアルタイムファイルシステム保護からアプリケーションプロセスを除外できます。バックアップ速度、プロセス整合性、サービス可用性を改善するために、5レベルのマルウェア保護と競合することが確認されている一部の技術がバックアップ中に使用されます。両方の状況を回避するための効率的な方法は、マルウェア対策ソフトウェアを無効にすることだけです。特定のプロセス(バックアップソリューションなど)を除外すると、このような除外されたプロセスに関連するすべてのファイル処理が無視され、安全であると見なされるため、バックアッププロセスへの干渉が最小化されます。除外を作成するときには、注意することをお勧めします。除外されたバックアップツールは、除外された権限がリアルタイム保護モジュールでのみ許可された拡張権限である、アラートをトリガーせずに、感染したファイルにアクセスできます。

> 除外されたファイル拡張子□HIPS除外□検出除外、またはパフォーマンス除外と混同しないでください。

プロセス除外は、潜在的な競合のリスクを最小化し、除外されたアプリケーションのパフォーマンスを改善します。これにより、オペレーティングシステムの全体的なパフォーマンスと安定性に好ましい影響を及ぼします。プロセス/アプリケーションの除外は、実行ファイルの除外です(*.exe*)□

実行ファイルは、詳細設定 > **保護 > 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 > プロセスの除外**で除外プロセスのリストに追加できます。

この機能は、バックアップツールを除外するために設計されています。バックアップツールのプロセスを検査から除外すると、システムの安定を保証するだけではなく、実行中にバックアップ速度が低下しないため、バックアップパフォーマンスにも影響しません。

**編集**をクリックして、**プロセス除外**管理ウィンドウを開きます。ここでは、除外を追加し、検査から除外される実行ファイル(*Backup-tool.exe*など)を参照できます。
*.exe*ファイルが除外に追加されるとすぐに、このプロセスのアクティビティがESET Endpoint Antivirusによって監視され、このプロセスで実行されるすべてのファイル処理で検査が実行されません。

プロセス実行ファイルを選択するときに参照機能を使用しない場合は、実行ファイルの完全パスを手動で入力する必要があります。そうしないと、除外が正常に動作せず、HIPSがエラーを報告する場合があります。

既存のプロセスを**編集**するか、除外から**削除**することもできます。

Webアクセス保護は、この除外を考慮しません。このためWebブラウザーの実行ファイルを除外する場合、ダウンロードされたファイルがまだ検査されます。このようにして、侵入を検出できます。このシナリオは、例ですWebブラウザーの除外は作成しないことをお勧めします。

# プロセス除外の追加または編集

このダイアログウィンドウでは、検出エンジンから除外されるプロセスを**追加**できます。プロセス除外は、潜在的な競合のリスクを最小化し、除外されたアプリケーションのパフォーマンスを改善します。これにより、オペレーティングシステムの全体的なパフォーマンスと安定性に好ましい影響を及ぼします。プロセス/アプリケーションの除外は、実行ファイルの除外です(*.exe*)

...(*C:\Program Files\Firefox\Firefox.exe*など)をクリックして、想定されたアプリケーションのファイルパスを選択します。アプリケーションの名前は入力しないでください。
*.exe*ファイルが除外に追加されるとすぐに、このプロセスのアクティビティがESET Endpoint Antivirusによって監視され、このプロセスで実行されるすべてのファイル処理で検査が実行されません。

プロセス実行ファイルを選択するときに参照機能を使用しない場合は、実行ファイルの完全パスを手動で入力する必要があります。そうしないと、除外が正常に動作せず、HIPSがエラーを報告する場合があります。

既存のプロセスを**編集**するか、除外から**削除**することもできます。

# リアルタイム保護の設定の変更

リアルタイム保護は、安全なシステムを維持するために最も必要不可欠な要素です。パラメーターを変更する際には注意してください。特定の状況に限ってパラメーターを変更することをお勧めします。

ESET Endpoint Antivirusのインストール後は、最大レベルのシステムセキュリティをユーザーに提供するように全ての設定が最適化されています。既定の設定に戻すには、詳細設定 > **保護** > **検出応答**の横にあるをクリックします。

# リアルタイム保護の確認

リアルタイムファイルシステム保護が機能していてウイルスが検出されることを確認するには□eicar.comのテストファイルを使用します。このテストファイルは、あらゆるウイルス対策プログラムが検出できる無害のファイルです。このファイルは、EICAR(European Institute for Computer Antivirus Research)が、ウイルス対策プログラムの機能をテストする目的で作成しました。

このファイルはhttp://www.eicar.org/download/eicar.comでダウンロードできます。
ブラウザーにこのURLを入力した後、脅威が削除されたというメッセージが表示されます。

# リアルタイム保護が機能しない場合の解決方法

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

## リアルタイム保護が無効である

ユーザーが不注意にリアルタイムファイルシステム保護を無効にしてしまった場合、機能を再アクティベーションする必要があります。リアルタイムファイルシステム保護を再開するには、メインプログラムウィンドウの**設定**に移動し、[**コンピューター**] > [**リアルタイムファイルシステム保護**]を有効にします。

リアルタイムファイルシステム保護がシステムの起動時に開始しない場合は[**リアルタイムファイルシステム保護を有効にする**]が無効になっている場合が考えられます。このオプションが有効になっていることを確認するには、詳細設定 > **保護** > **リアルタイムファイルシステム保護**を開きます。

## リアルタイム保護がマルウェアの検出と駆除を行わない場合

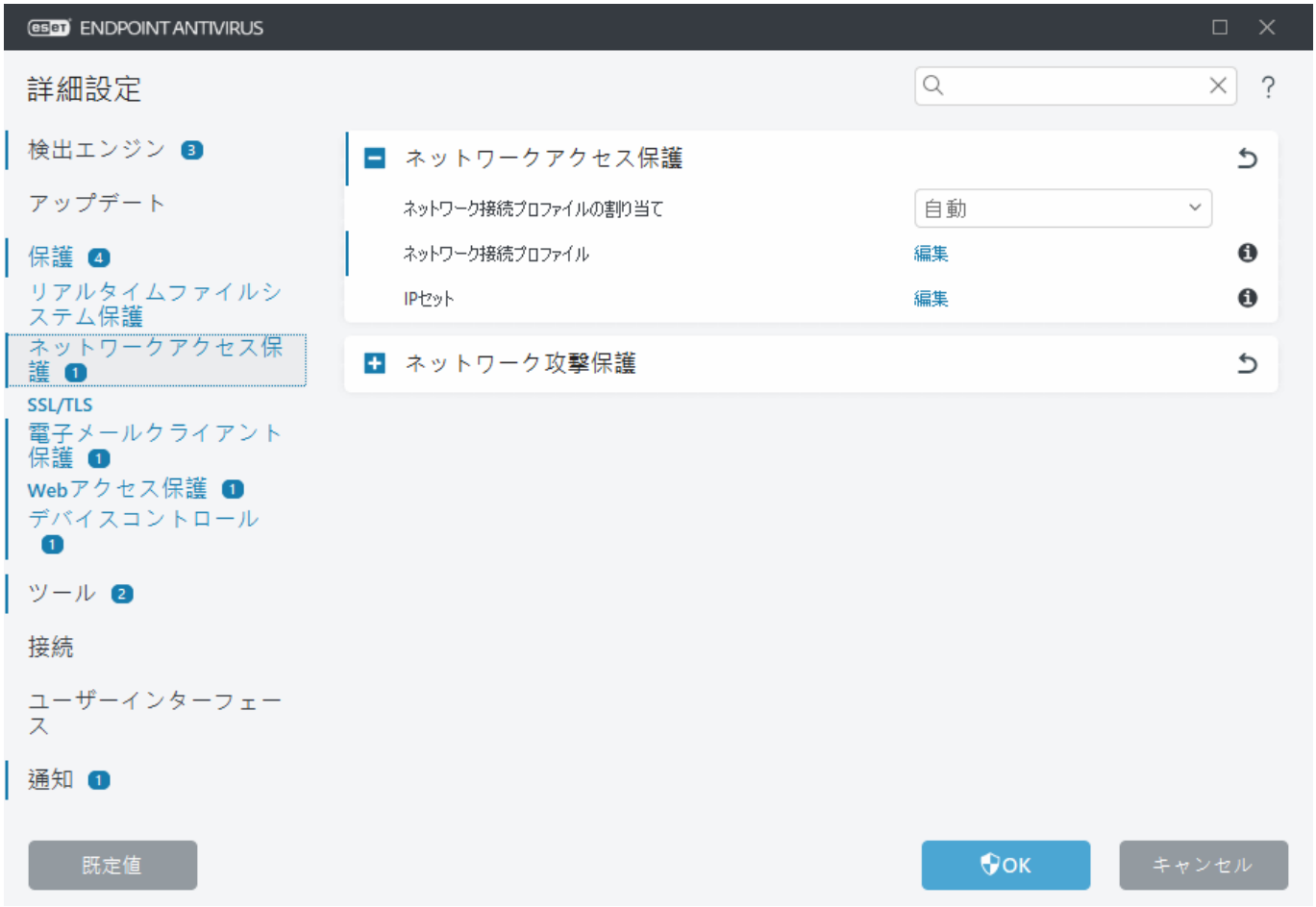
コンピュータに他のウイルス対策プログラムがインストールされていないことを確認します。2つのウィルス対策ソフトが同時にインストールされていると、互いに競合することがあります□ESETをインストールする前に、システムから他のウイルス対策プログラムをアンインストールすることをお勧めします。

## リアルタイム保護が開始されない

**リアルタイムファイルシステム保護を有効にする**が有効であるにもかかわらず、リアルタイムファイルシステム保護がシステム起動時に開始しない場合、他のプログラムとの競合が原因である可能性があります。この問題を解決するには、ESET SysInspectorログを作成して、分析のためにESETテクニカルサポートに送信してください。

# ネットワークアクセス保護

ネットワークアクセス保護を使用すると、すべてのネットワーク接続を設定できます。既定で、ESET Endpoint Antivirusではセキュリティを最大限に高めるために、ネットワークアクセス保護が事前に設定されています。ただし、特定の環境ではカスタム設定が必要になる場合があります。既定の設定の変更は、経験豊富なユーザーのみが行ってください。




詳細設定 > **保護** > **ネットワークアクセス保護**で次の設定を設定できます(各ネットワークアクセス保護オプションの詳細な説明については、以下のリンクをクリックしてください)。

## 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 – プロファイルを使用して、特定のネットワーク接続のネットワークアクセス保護を制御できます。

IPセット – 1つの論理IPアドレスグループを作成するIPアドレスコレクションを定義でき、信頼ゾーンとして追加したり、ネットワーク攻撃保護(IDS)から除外したりできます。

ネットワーク攻撃保護

# ネットワーク接続プロファイル

プロファイルを使用して、特定のネットワーク接続に対してESET Endpoint Antivirusネットワークアクセス保護の動作を制御できます。IDSルール総当たり攻撃保護ルールを作成または編集するときに、特定のプロファイルに割り当てることも、すべてのプロファイルに適用することもできます。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。

ネットワーク接続プロファイルと割り当ては、詳細設定 > **保護** > **ネットワークアクセス保護** > **ネットワークアクセス保護**で設定できます。

**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で設定されたアクティベートユーザーに基づいて、新しく検出されたネットワーク接続に事前定義されたプロファイルまたはカスタムプロファイルを自動的に割り当てるか(ドロップダウンメニューから**自動**を選択)、新しいネットワー

ク接続が検出されるたびにネットワーク保護を設定し、プロファイルを手動で割り当てるよう確認を求められるか(ドロップダウンメニューから**確認**を選択)を選択できます。

プログラムのメインウィンドウ > **設定** > **ネットワーク** > **ネットワーク接続**で、特定のネットワーク接続プロファイルを手動で割り当てることもできます。特定のネットワーク接続にカーソルを合わせ、メニューアイコン > **編集**をクリックしてネットワーク保護の設定ウィンドウを開き、プロファイルを選択します。

**ネットワーク接続プロファイル** - **編集**をクリックして、ネットワーク接続プロファイルを追加または編集します。

次のプロファイルは事前に定義されており、編集/削除できません。

**プライベート** – 信頼できるネットワーク(自宅または職場ネットワーク)の場合。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)。安全なローカルネットワークにアクセスするときにはこの設定を使用することをお勧めします。このプロファイルは、Windowsでドメインまたはプライベートネットワークとして設定されている場合、ネットワーク接続に自動的に割り当てられます。

**パブリック** – 信頼できないネットワーク(パブリックネットワーク)の場合。システムのファイルとフォルダーはネットワーク上の他のユーザーと共有したり、表示したりできません。システムリソースの共有が無効になります。無線ネットワークにアクセスするときにはこの設定を使用することをお勧めします。このプロファイルは、Windowsでドメインまたはプライベートネットワークとして設定されていないネットワーク接続に自動的に割り当てられます。

ネットワーク接続が他のプロファイルに切り替わった場合、画面の右下に通知が表示されます。

# ネットワーク接続プロファイルを追加または編集する

ネットワーク接続プロファイルは、詳細設定 > **保護** > **ネットワークアクセス保護** > **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** > **編集**で追加または編集できます。プロファイルを編集するには、**ネットワーク接続プロファイル**ウィンドウのリストから選択する必要があります。

次のプロファイルは事前に定義されており、編集/削除できません。

**プライベート** – 信頼できるネットワーク(自宅または職場ネットワーク)の場合。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)。安全なローカルネットワークにアクセスするときにはこの設定を使用することをお勧めします。このプロファイルは、Windowsでドメインまたはプライベートネットワークとして設定されている場合、ネットワーク接続に自動的に割り当てられます。

**パブリック** – 信頼できないネットワーク(パブリックネットワーク)の場合。システムのファイルとフォルダーはネットワーク上の他のユーザーと共有したり、表示したりできません。システムリソースの共有が無効になります。無線ネットワークにアクセスするときにはこの設定を使用することをお勧めします。このプロファイルは、Windowsでドメインまたはプライベートネットワークとして設定されていないネットワーク接続に自動的に割り当てられます。

**トップ/アップ/ダウン/ボトム** – ネットワーク接続プロファイルの優先度レベルを調

整できます(ネットワーク接続プロファイルは優先度によって評価および適用されます。最初にマッチしたプロファイルが常に適用されます)。

## プロファイルを追加または編集する

カスタムネットワーク接続プロファイルを使用すると、総当たり攻撃保護ルールを適用し、特定のネットワーク接続の追加設定を定義できます。カスタムプロファイルを割り当てるネットワーク接続は、アクティベートユーザーセクションで指定します。

プロファイルエディターを開くには、**ネットワーク接続プロファイル**ウィンドウで

- [**追加**]をクリックします。
- 既存のプロファイルの1つを選択し、**編集**をクリックします。
- 既存のプロファイルの1つを選択し、**コピー**をクリックします。

**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。

**弱いWi-Fi暗号化を報告** – ESET Endpoint Antivirusは、保護されていないワイヤレスネットワークまたは保護が弱いネットワークに接続するときにデスクトップ通知を表示します。

**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。詳細については、アクティベートユーザーを参照してください。

# 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。

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の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。

## 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アドレスが一致する場合にプロファイルを適用します。

## WINS

Windows Internet Name Service (WINS)のマッピングされた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。
**プロファイル名** - Wi-Fiプロファイル名が一致する場合にプロファイルを適用します。
**セキュリティタイプ** – セキュリティタイプがドロップダウンメニューから選択したものと一致する場合にプロファイルを適用します。(複数と一致させる場合は、別のアクティベートユーザーを作成します)。
**暗号化タイプ** – 暗号化タイプがドロップダウンメニューから選択したものと一致する場合にプロファイルを適用します。(複数と一致させる場合は、別のアクティベートユーザーを作成します)。
**ネットワークセキュリティ** – ネットワークが**オープン**または**保護されている**場合にプロファイルを適用します。

## Windowsプロファイル

Windowsでネットワークが**ドメイン/プライベート/パブリック**として設定されている場合にプロファイルを適用します。

## 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。
ESET認証サーバーをダウンロード
公開鍵は、次のいずれかの種類のファイルを使用してインポートできます。
• PEM暗号化公開鍵(.pem)で、ESET認証サーバーを使用して生成できます
• 暗号化公開鍵
• パブリックキー証明書(.crt)
[テスト]をクリックして設定をテストします。認証が成功すると、サーバーの認証に成功しましたが表示されます。認証が正常に設定されないと、次のいずれかのエラーメッセージが表示されます:
サーバーの認証に失敗しました。署名が無効であるか、一致しません。
サーバー署名が入力された公開鍵と一致しません。
サーバーの認証に失敗しました。ネットワーク名が一致しません。
設定されているネットワーク名が、認証サーバーゾーン名と一致していません。両方の名前を確認し、同じであることを確かめてください。
サーバーの認証に失敗しました。サーバーからの応答が無効か、応答がありません。
サーバーが実行中ではないか、アクセスできない場合、応答を受信しません。別のHTTPサーバーが指定されたアドレスで実行されていると、無効な応答が受信される場合があります。
無効な公開鍵が入力されました。
入力された公開鍵ファイルが破損していないことを確認します。

# IPセット

IPセットは、IPアドレスの1つの論理グループを作成するIPアドレスのコレクションであり、複数の総当たり攻撃保護ルールで同じアドレスセットを再利用する場合に役立ちます。またESET Endpoint Antivirusには内部ルールが適用される事前定義されたIPセットも含まれています。このようなグループの一例として、**信頼ゾーン**があります。信頼ゾーンはネットワークアドレスのグループを表し、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。

IPセットを追加する手順は次のとおりです。

1. 詳細設定 > **保護** > **ネットワークアクセス保護** > **IPセット** > **編集**を開きます。
2. **追加**をクリックし、ゾーンの**名前**と**説明**を入力し、**リモートコンピューターアドレス(IPv4/IPv6、範囲、マスク)**を入力します。
3. **OK**をクリックします。

詳細については、IPセットの編集を参照してください。

# IPセットの編集

IPセットについて詳しくは、IPセットを参照してください。

## 列

**名前** – リモートコンピューターのグループの名前。

**説明** – グループの一般的な説明。

**IPアドレス** - IPセットに属するリモートIPアドレス。

## コントロール要素

IPセットを**追加**または**編集**する場合、次のフィールドを使用できます。

**名前** – リモートコンピューターのグループの名前。

**説明** – グループの一般的な説明。

**リモートコンピュータアドレス(IPv4IPv6範囲、マスク)** – リモートアドレス、アドレス範囲、またはサブネットを追加します。

**削除** – リストからゾーンを削除します。

定義済みのIPセットは削除できません。

IPアドレスの例
IPv4アドレスの追加:
**単一のアドレス** – 各コンピューターのIPアドレス(*192.168.0.10*など)を追加します。
**アドレス範囲** – 最初と最後のIPアドレスを入力して、*192.168.0.1*-*192.168.0.99*など、複数のコンピューターのIP範囲を指定します。
**サブネット** – サブネット(コンピューターのグループ)は、IPアドレスとマスクによって定義されます。たとえば、255.255.255.0は192.168.1.0サブネットのネットワークマスクです。*192.168.1.0/24*でサブネットタイプ全体を除外します。
IPv6アドレスの追加:
**単一のアドレス** - *2001:718:1c01:16:214:22ff:fec9:ca5*など、各コンピューターのIPアドレスを追加します。
**サブネット** – サブネット(コンピューターのグループ)は、IPアドレスとマスクによって定義されます(例: *2002:c0a8:6301:1::1/64*)

# ネットワーク攻撃保護(IDS)

ネットワーク攻撃保護(IDS)は、既知の脆弱性の悪用の検出を改善します。ネットワーク攻撃保護の詳細については、用語集をお読みください。ネットワーク攻撃保護を設定するには、詳細設定 > **保護** > **ネットワークアクセス保護** > **ネットワーク攻撃保護**を開きます。

**ネットワーク攻撃保護(IDS)を有効にする** – ネットワークトラフィックの内容を分析し、ネットワーク攻撃から保護します。有害だと見なされるすべてのトラフィックがブロックされます。

**ボットネット保護を有効にする**– コンピュータが感染した場合や、ボットが通信を試みているときに、一般的なパターンに基づいて、悪意のあるコマンドとの通信およびコントロールサーバーを検出してブロックします。用語集のボットネット保護をお読みください。

IDSルール – このオプションでは、コンピューターに害をもたらす可能性があるさまざまな攻撃およびエクスプロイトタイプを検出する、詳細なフィルタオプションを設定できます。

ネットワーク保護によって検出されたすべての重要なイベントがログファイルに保存されます。詳細については、ネットワーク保護ログを参照してください。

# IDSルール

一部の状況では、Intrusion Detection Service (IDS)によって、ルーターまたは他の内部ネットワークデバイスとの間の通信が攻撃の可能性として検出される場合があります。たとえば、確認済みの安全なアドレスをIDSゾーンから除外されたアドレスに追加してIDSによる検出を回避することができます。

次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
- クライアントワークステーションでESET Endpoint AntivirusのIDSルールを作成する
- クライアントワークステーションでESET PROTECTのIDSルールを作成

## IDSルールの管理

- **追加** – クリックすると、新しいIDSルールを作成します。
- **編集** – クリックすると、既存のIDSルールを編集します。
- **削除** - IDSルールのリストから既存の例外を削除する場合は、選択してクリックします。
- **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(例外は最上位から最下位へと評価されます)。


管理者がESET PROTECT Webコンソールで IDS除外を作成する場合は、タブ**除外**が表示されますIDS除外には許可ルールのみが含まれIDSルールの前に評価されます。

## ルールエディタ

**検出** – 検出のタイプ。

**脅威名** – 使用可能な一部の検出に対して脅威名を指定できます。

**アプリケーション** - ...(*C:\Program Files\Firefox\Firefox.exe*など)をクリックして、想定されたアプリケーションのファイルパスを選択します。アプリケーションの名前は入力しないでください。

**リモートIPアドレス** – リモートIPv4またはIPv6アドレス/範囲/サブネットのリスト。複数のアドレスはカンマで区切る必要があります。

**プロファイル** – このルールを適用するネットワーク接続プロファイルを選択できます。

## アクション

**ブロック** – すべてのシステムプロセスには独自の既定の動作があり、アクション(ブロックまたは許可)が割り当てられています。ESET Endpoint Antivirusの既定の動作を無効にするには、ドロップダウンメニューを使用して、動作をブロックするか許可するかどうかを選択できます。

**通知** – はいを選択すると、コンピューターでデスクトップ通知を表示します。デスクトップ通知を表示しない場合は、いいえを選択します。既定/はい/いいえの値を使用できます。

**ログ – はい**を選択すると、 ESET Endpoint Antivirusログファイルにイベントを記録します。イベントを記録しない場合は、**いいえ**を選択します。**既定/はい/いいえ**の値を使用できます。


イベントが発生するたびに、通知を表示して、ログを記録する。
1. **追加**をクリックして、新しいIDSルールを追加します。
2. **検出**ドロップダウンメニューから特定のアラートを選択します。
3. **...**をクリックし、通知を適用する特定のアプリケーションのファイルパスを入力します。
4. **ブロック**ドロップダウンメニューで**既定**を選択したままにします。ESET Endpoint Antivirusで適用された既定のアクションが継承されます。
5. **通知**と**ログ**ドロップダウンメニューを、**はい**に設定します。
6. **OK**をクリックしてこの通知を保存します。

脅威と見なさない検出のタイプに関する繰り返し通知を削除する。
1. **追加**をクリックして、新しいIDS例外を追加します。
2.**検出**ドロップダウンメニューから特定のアラート(たとえば、**セキュリティ拡張なしSMBセッション**)を選択します。
3. 受信通信の場合は、ドロップダウンメニューで**受信**を選択します。
4. **通知**ドロップダウンメニューを**いいえ**に設定します。
5. **ログ**ドロップダウンメニューを**はい**に設定します。
6. **アプリケーション**を空白のままにします。
7. 通信から特定のIPからではない場合、**リモートIPアドレス**を空白にします。
8. **OK**をクリックしてこの通知を保存します。

# 総当たり攻撃保護

総当たり攻撃保護は、RDPおよびSMBサービスに対するパスワード推測攻撃をブロックします。総当たり攻撃とは、文字、数字、および記号のあらゆる組み合わせを系統的に試して、狙ったパスワードを発見する方法です。総当たり攻撃保護を設定するには、詳細設定 > **保護** > **ネットワークアクセス保護** > **ネットワーク攻撃保護** > **総当たり攻撃保護**を開きます。

**総当たり攻撃保護を有効にする** - ESET Endpoint Antivirusでは、ネットワークトラフィックの内容を検査し、パスワード推測攻撃の試みをブロックします。

**ルール** – 送受信ネットワーク接続のルールを作成、編集、表示できます。詳細については、ルールを参照してください。

**除外** - IPアドレス別またはアプリケーションパスで定義された除外された検出のリスト。除外は、ESET PROTECTで作成および編集できます。詳細については、除外を参照してください。

# ルール

総当たり攻撃保護ルールを使用すると、受信および送信ネットワーク接続のルールを作成、編集、表示できます。あらかじめ定義されたルールは編集または削除できません。

## 総当たり攻撃保護ルールの管理

- **追加** – クリックすると、新しい総当たり攻撃保護ルールを作成します。
- **編集** – クリックすると、既存の総当たり攻撃保護ルールを編集します。
- **削除** - IDSルールのリストから既存の例外を削除する場合は、選択してクリックします。
-  **最上位/上/下/最下位** – ルールの優先度レベルを調整します。


可能なかぎり高い保護を保証するために、複数のブロックルールが検出条件と一致するときに、最も低い**最大試行回数**値のブロックルールは、ルールがルールリストの下位に位置する場合でも適用されます。

## ルールエディタ

**名前** – ルールの名前。

**有効** – ルールをリスト内に置いたまま適用しない場合、このトグルをオフにします。

**アクション** – ルール設定が満たされた場合に、接続を**拒否**するか、**許可**するかどうかを選択します。

**プロトコル** – このルールが検査する通信プロトコル。

**プロファイル** – このルールを適用するネットワーク接続プロファイルを選択できます。

**最大試行回数** – この回数まで反復攻撃の試行が許可されます。この回数を超えるとIPアドレスがブロックされ、ブラックリストに追加されます。

**ブラックリスト保持期間(分)** – ブラックリストのアドレスが有効期限切れになる時間を設定します。

**送信元IP** - IPアドレス/範囲/サブネットのリスト。複数のアドレスはカンマで区切る必要があります。

**送信元IPセット** - IPセットですでに定義したIPアドレスのセット。


# 除外

総当たり攻撃の除外を使用すると、特定の条件の総当たり攻撃の検出を抑制することができます。これらの除外は、総当たり攻撃の検出に基づいてESET PROTECTから作成されます。

## 列

- **検出** – 検出のタイプ。
- **アプリケーション** - ...(*C:\Program Files\Firefox\Firefox.exe*など)をクリックして、想定されたアプリケーションのファイルパスを選択します。アプリケーションの名前は入力しないでください。
- **リモートIP** – リモートIPv4またはIPv6アドレス/範囲/サブネットのリスト。複数のアドレスはカンマで区切る必要があります。

## 除外の管理

管理者がESET PROTECT Webコンソールで総当たり攻撃の除外を作成する場合は、タブ除外が表示されます。総当たり攻撃の除外には許可ルールのみが含まれ、IDSルールの前に評価されます。

# 詳細設定オプション

詳細設定 > **保護** > **ネットワークアクセス保護** > **ネットワーク攻撃保護** > **詳細オプション**では、コンピューターに損害を与える可能性のあるさまざまな種類の攻撃やエクスプロイトの検出を有効または無効にできます。

ブロックされた通信についての脅威の通知を受け取らないことがあります。ファイアウォールログでブロックされたすべての通信を表示する手順については、「ロギングとログからのルールまたは例外の作成」を参照してください。

このウィンドウで特定のオプションを使用できるかどうかはESET製品とファイアウォールモジュールの種類とバージョンおよびオペレーティングシステムのバージョンによって異なる場合があります。

## 侵入検出

- **[プロトコル SMB]**- SMBプロトコルのさまざまなセキュリティの問題を検出してブロックします。
- **不正サーバーチャレンジ攻撃認証を検出** – 認証の際にユーザー認証を取得しようとして不正なチャレンジを使用する攻撃から保護します。
- **名前付きパイプを開くときのIDS回避を検出** - SMBプロトコルでMSRPC名前付きパイプを開くために使用される既知の回避方法を検出します。
- **CVE検出** (Common Vulnerabilities and Exposures) - SMBプロトコルでのさまざまな攻撃、フォーム、セキュリティホール、悪用に関する実装済みの検出方法です。CVE識別子(CVEs)に関する詳細については、cve.mitre.orgのCVE Webサイトを参照してください。
- **プロトコルRPC** - 分散コンピューティング環境(DCE)のために開発されたリモートプロシージャコールシステムでのCVEを検出してブロックします。
- **プロトコルRDP** - RDPプロトコルでさまざまなCVEを検出してブロックします(前記を参照)。
- **攻撃の検出後に安全ではないアドレスをブロック** – 攻撃の元であると検出されたIPアドレスは、一定の時間、接続を遮断するためにブラックリストに追加されます。**ブラックリスト保持期間**を定義し、攻撃の検出後にアドレスがブロックされる期間を設定できます。
- **攻撃の検出について通知** – 画面の右下にあるWindows通知領域がオンになります。
- **セキュリティホールに対する受信攻撃を通知** – セキュリティホールに対する攻撃が検出された場合や、脅威によってこの方法でシステムに侵入する試みが行われた場合に通知します。

## パケットのチェック

- **SMBプロトコルでの管理用共有への内向き接続を許可** – 管理用共有は、既定のネットワーク共有で、システム内のハードドライブのパーティション(*C$*、*D$*、...)をシステムフォルダ(*ADMIN$*)と共有します。管理用要求への接続を無効にすると、多くのセキュリティリスクが低下します。たとえばConfickerワームは管理用共有に接続するためにディクショナリアタックを行います。
- **古い(サポート対象外) SMBダイアレクトを遮断** - IDSによってサポートされていない古いSMBダイアレクトを使用するSMBセッションを遮断します。最近のWindowsオペレーティングシステム

は、Windows 95などの古いオペレーティングシステムとの後方互換性を確保するために、古いSMBダイアレクトをサポートしています。攻撃者は、SMBセッションで古いダイアレクトで使用することにより、トラフィック検査を逃れることができます。お使いのコンピュータで古いバージョンのWindowsを搭載したコンピュータとファイルを共有する必要がない場合は(または通常のSMB通信を使用)、古いSMBダイアレクトを遮断してください。

- **拡張セキュリティのないSMBセキュリティを遮断** - SMBセッションネゴシエーションの際、LAN Managerチャレンジ/レスポンス(LM)認証よりも安全な認証メカニズムを提供するために、拡張セキュリティを使用できます。LMスキームは、脆弱であると考えられ、使用は推奨されません。
- **セキュリティアカウントマネージャ(SAM)サービスとの通信を許可** – このサービスの詳細については、[MS-SAMR]を参照してください。
- **ローカルセキュリティ機関(LSA)サービスとの通信を許可** – このサービスの詳細については、[MS-LSAD]と[MS-LSAT]を参照してください。
- **リモートレジストリサービスとの通信を許可** – このサービスの詳細については、[MS-RRP]を参照してください。
- **サービスコントロールマネージャサービスとの通信を許可** – このサービスの詳細については、[MS-SCMR]を参照してください。
- **サーバーサービスとの通信を許可** – このサービスの詳細については、[MS-SRVS]を参照してください。
- **他のサービスとの通信を許可** – 他のMSRPCサービス。MSRPCは、MicrosoftによるDCE RPCメカニズムの実装です。また。MSRPCでは、転送(ncacn_np転送)のためにSMB(ネットワークファイル共有)プロトコルで名前付きパイプを使用できます。MSRPCサービスには。Windowsシステムをリモートからアクセスして管理するためのインタフェースが用意されています。Windows MSRPCシステムに関しては、いくつかのセキュリティ上の脆弱性が発見、悪用されてきました(Conficker。ワーム。Sasserワームなど)。多くのセキュリティリスク(リモートコード実行、サービス拒否攻撃など)低下させるために、提供する必要がないMSRPCサービスとの通信は無効にしてください。

# SSL/TLS

ESET Endpoint Antivirusは、SSLプロトコルを使用する通信の脅威を検査できます。SSLで保護された通信には、信頼できる証明書、不明な証明書。SSLで保護された通信の検査対象から除外された証明書を使用する、さまざまなフィルタリングモードがあります。SSL/TLS設定を編集するには、詳細設定 > **保護** > **SSL/TLS**を開きます。


**SSL/TLSを有効にする** – これを無効にするとESET Endpoint AntivirusはSSL/TLSを介した通信を検査しません。

**SSL/TLSモード**は次のオプションで使用できます。

| フィルタリングモード | 説明 |
|---|---|
| **自動** | 既定モードではWebブラウザまたは電子メールクライアントとなど適切なアプリケーションのみをスキャンします。通信が検査されるアプリケーションを選択することで上書きできます。 |
| **対話モード** | 新しいSSLで保護されたサイト(不明な証明書を使用)にアクセスする場合、アクション選択ダイアログが表示されます。このモードでは、検査から除外するSSL証明書/アプリケーションのリストを作成できます。 |
| **ポリシーベース** | 検査対象から除外された証明書に保護されている通信以外のSSLで保護された全通信を検査するには、このオプションを選択します。不明な署名付き証明書を使用した新しい通信が確立された場合、ユーザに通知されず、通信は自動的にフィルタリングされます。信頼しているとマークされている(信頼できる証明書リストに追加済み)信頼されない証明書を使用してサーバーにアクセスすると、そのサーバーへの通信は許可され、通信チャネルコンテンツがフィルタリングされます。 |

**アプリケーション検査ルール** – 特定のアプリケーションに対するESET Endpoint Antivirusの動作をカスタマイズできます。

**証明書ルール** – 特定のSSL証明書に対するESET Endpoint Antivirusの動作をカスタマイズできます。

**ESETによって信頼されたドメインのトラフィックを検査しない** – これを有効にすると、信頼されたド

メインとの通信は検査から除外されますESETが管理する組み込みのホワイトリストによって、ドメインの信頼性を判断します。

**ESETルート証明書をサポートされているアプリケーションに統合** – ブラウザーや電子メールクライアントでSSL通信を正しく機能させるにはESETのルート証明書を既知のルート証明書(発行元)のリストに追加する必要があります。このオプションを選択するとESET Endpoint AntivirusではESET SSL Filter CA証明書が既知のブラウザ(Operaなど)に自動的に追加されます。システム認証ストアを使用するブラウザには、証明書が自動的に追加されます。たとえばFirefoxは自動的にシステム認証ストアのルート認証局を信頼するように設定されています。

サポートされないブラウザーに証明書を適用するには、[**証明書の表示**] > [**詳細**] > [**ファイルにコピー**]をクリックして、証明書をブラウザーに手動でインポートします。

**証明書の信頼を確立できない場合のアクション** - Trusted Root Certification Authorities (TRCA)ストアを使用してWebサイト証明書を検証できない場合があります(期限切れの証明書、信頼できない証明書、特定のドメインに対して無効な証明書、解析できるが証明書に正しく署名されていない署名など)。合法的なWebサイトは常に信頼できる証明書を使用します。信頼できる証明書を提供していない場合、攻撃者があなたの通信を復号化しているかWebサイトが技術的な問題を抱えていることを意味していることがあります。

**証明書の有効性を確認する**が選択されていると(既定で選択済み)、暗号化通信の確立時にアクションを選ぶよう求められます。アクションを選択するダイアログが表示され、ユーザーはその証明書を信頼するか除外するかマークできます。証明書がTRCAリストに含まれていない場合、ウィンドウは赤になります。証明書がTRCAリストに含まれている場合、ウィンドウは緑になります。

**証明書を使用する通信をブロックする**を選択して、信頼できない証明書を使用するサイトとの暗号化通信をいつでも切断できます。

**古いSSL2で暗号化されたトラフィックをブロック** – 以前のバージョンのSSLプロトコルを使用する通信は自動的にブロックされます。

**破損した証明書に対するアクション** – 破損した証明書とは、証明書がESET Endpoint Antivirusによって認識されない形式を使用しているか、破損している(たとえば、ランダムデータで上書きされているなど)ことを意味します。この場合は、**証明書を使用する通信をブロックする**を選択したままにすることをお勧めします。**証明書の有効性を確認する**を選択した場合は、暗号化された通信が確立されたときにアクションを選択するよう求められます。

次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
- ESET製品の証明書通知
- Webページにアクセスすると、「暗号化されたネットワークトラフィック:信頼できない証明書」が表示されます

# アプリケーション検査ルール

**アプリケーション検査ルール**を使用すると、特定のアプリケーションに対するESET Endpoint Antivirusの動作をカスタマイズし、**SSL/TLSモード**が**対話モード**のときに選択されたアクションを記憶できます。このリストは、詳細設定 > **保護** > **SSL/TLS** > **アプリケーション検査ルール** > **編集**で表示および編集できます。

**アプリケーション検査ルール**ウィンドウは、次の項目で構成されています。

## 列

**アプリケーション - ...** オプションをクリックするか手動でパスを入力して、ディレクトリツリーから実行可能ファイルを選択します。

**検査アクション - 検査の対象** または **無視**を選択して通信をスキャンまたは無視します。**自動**を選択すると、自動モードでは検査し、対話モードでは確認します。**確認**を選択すると、常に処理方法をユーザーに確認します。

## コントロール要素

**追加** – フィルタリングされたアプリケーションを追加。

**編集** – 設定するアプリケーションを選択し、[**編集**]をクリックします。

**削除** – 削除するアプリケーションを選択し、[**削除**]をクリックします。

**インポート/エクスポート** – ファイルからアプリケーションをインポートするか、現在のアプリケーションのリストをファイルに保存します。

**OK/キャンセル** – 変更を保存する場合は[**OK**]をクリックします。保存せずに終了する場合は[**キャンセル**]をクリックします。

# 証明書ルール

**証明書ルール**を使用すると、特定のSSL証明書に対するESET Endpoint Antivirusの動作をカスタマイズし、**SSL/TLSモード**が**対話モード**のときに選択されたアクションを記憶できます。このリストは、詳細設定 > **保護** > **SSL/TLS** > **証明書ルール** > **編集**で表示および編集できます。

**証明書ルール**ウィンドウは、次の項目で構成されます。

## 列

**名前** – 証明書の名前。

**証明書の発行者** – 証明書の作成者名。

**証明書の表題** – 件名フィールドは、件名パブリックキーフィールドに保存されたパブリックキーに関連付けられたエンティティを指定します。

**アクセス** - **許可**または**拒否**を**アクセスアクション**として指定し、信頼性に関係なく、この証明書で保護された通信を許可またはブロックします。**自動**を選択すると、信頼できる証明書を許可し、信頼できない証明書については確認します。**確認する**を選択すると、常に処理方法をユーザーに確認します。

**検査** - **検査**または**無視**を**検査アクション**として選択すると、この証明書で保護された通信を検査または無視します。**自動**を選択すると、自動モードでは検査し、対話モードでは確認します。**確認**を選択すると、常に処理方法をユーザーに確認します。

## コントロール要素

**追加** – 新しい証明書を追加し、アクセスと検査オプションの設定を調整します。

**編集** – 設定する証明書を選択し、[**編集**]をクリックします。

**削除** – 削除する証明書を選択し、[**削除**]をクリックします。

**OK/キャンセル** – 変更を保存する場合は[**OK**]をクリックします。保存せずに終了する場合は[**キャンセル**]をクリックします。

# 暗号化されたネットワークトラフィック

SSL/TLS検査を使用するようにシステムが設定されている場合、次の2つの状況でアクションを選択するように指示するダイアログウィンドウが表示されます。

まずWebサイトが検証不可能または無効な証明書を使用し、このような場合にESET Endpoint Antivirusがユーザーに確認するように設定されている(検証不可能な証明書の既定は[はい]、無効な証明書の既定は[いいえ])場合、接続を**許可**するか**拒否**するかを確認するダイアログボックスが表示されます。証明書がTrusted Root Certification Authorities store (TRCA)にない場合、信頼できないと見なされます。

次に、**SSL/TLSモード**が**対話モード**に設定されている場合、各Webサイトのダイアログボックスが表示され、トラフィックを**検査**するか**無視**するかどうかを確認します。一部のアプリケーションは、SSLトラフィックが誰かによって修正または検査されていないことを確認します。このような場合ESET Endpoint Antivirusはトラフィックを**無視**し、アプリケーションを動作させ続ける必要があります。

> **図解例**
> 次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
> • ESET Windows製品の証明書通知
> • Webページにアクセスすると、「暗号化されたネットワークトラフィック:信頼できない証明書」が表示されます

いずれの場合も、ユーザーは選択したアクションを記憶するように選択できます。保存されたアクションは、証明書ルールに保存されます。

# 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を設定するには、詳細設定 > **保護** > **電子メールクライアント保護**を開き、次の設定オプションから選択します。

- メール転送保護
- メールボックス保護
- ThreatSense

# メール転送保護

IMA(S)PとPOP3(S)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 Antivirusでは、使用される電子メールクライアントに関係なく、このプロトコルに対する保護機能を備えています。電子メールクライアントの再設定は不要です。既定では、既定のPOP3/IMAPポート番号に関係なくPOP3およびIMAPプロトコルのすべての通信が検査されます。

MAPIプロトコルは検査されません。ただしMicrosoft Exchangeサーバーとの通信は、Microsoft Outlookなどの電子メールクライアントの統合モジュールによって検査できます。

ESET Endpoint AntivirusではIMAPS (585, 993)およびPOP3S (995)プロトコルの検査もサポートします。この場合、暗号化チャンネルを使用して、サーバーとクライアント間で情報を送受信しますESET Endpoint Antivirusは、SSL (Secure Socket Layer)およびTLS (Transport Layer Security)プロトコルを使用して通信を検査します。
暗号化された通信は、既定で検査されます。スキャナーの設定を表示するには、詳細設定 > **保護** > SSL/TLSを開きます。

メール転送保護を設定するには、詳細設定 > **保護** > **電子メールクライアント保護** > **メール転送保護**を開きます。

**メール転送保護を有効にする** – 有効にするとESET Endpoint Antivirusがメール転送通信を検査します。

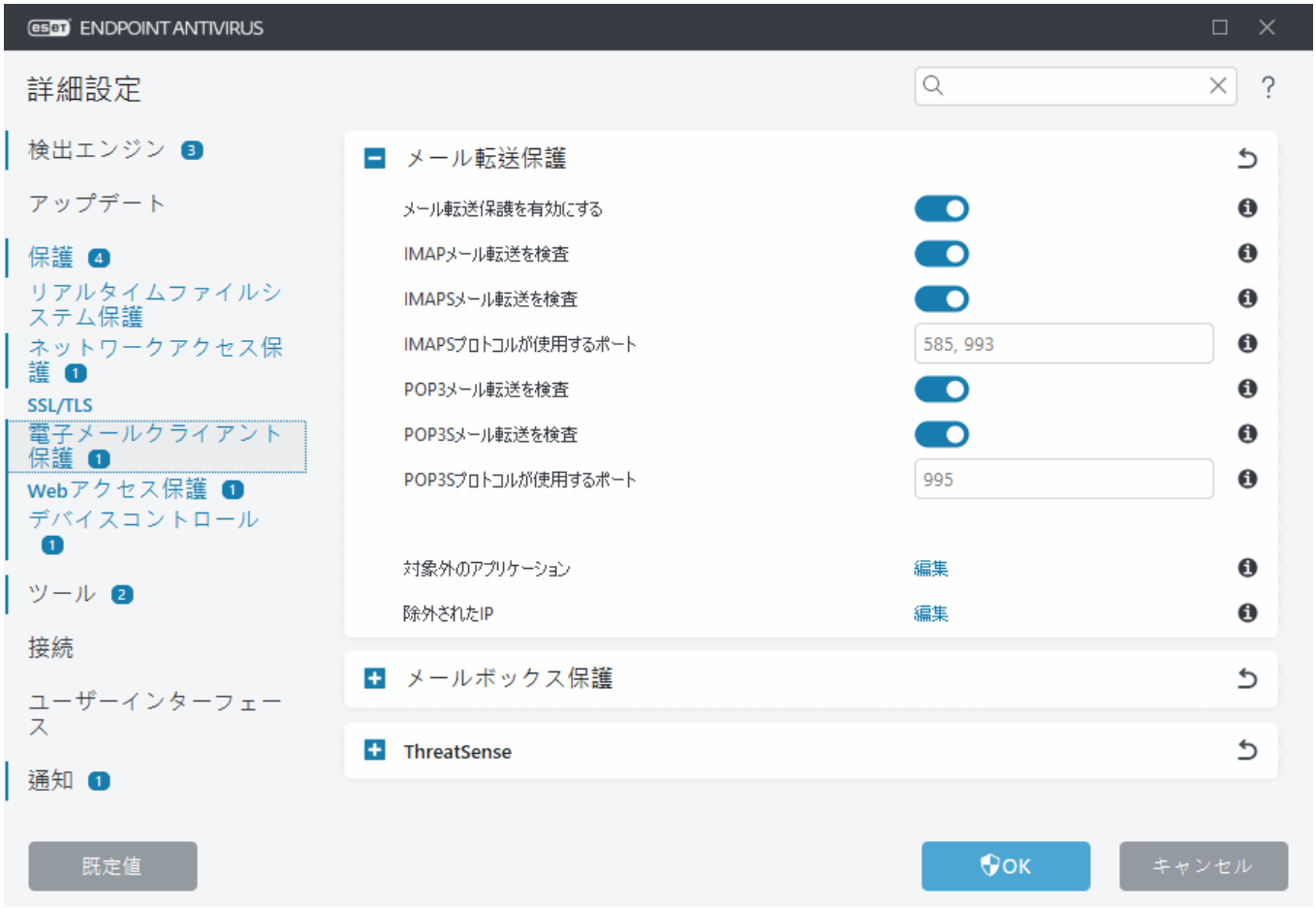
次のオプションの横にあるトグルをクリックして、検査するメール転送プロトコルを選択できます(既定では、すべてのプロトコルの検査が有効になっています)。

- **IMAPメール転送を検査**
- **IMAPSメール転送を検査**
- **POP3メール転送を検査**
- **POP3Sメール転送を検査**

既定ではESET Endpoint Antivirusは標準ポートでIMAPSおよびPOP3S通信を検査しますIMAPSおよびPOP3Sプロトコルのカスタムポートを追加するには、**IMAPSプロトコルが使用するポート**または**POP3Sプロトコルが使用するポート**の横のテキストフィールドに追加します。複数のポート番号は、コンマで区切る必要があります。

対象外のアプリケーション – 特定のアプリケーションをメール転送保護による検査対象から除外できますWebアクセス保護によって互換性の問題が発生した場合に便利です。

除外されたIP – 特定のリモートアドレスをメール転送保護による検査対象から除外できますWebアクセス保護によって互換性の問題が発生した場合に便利です。



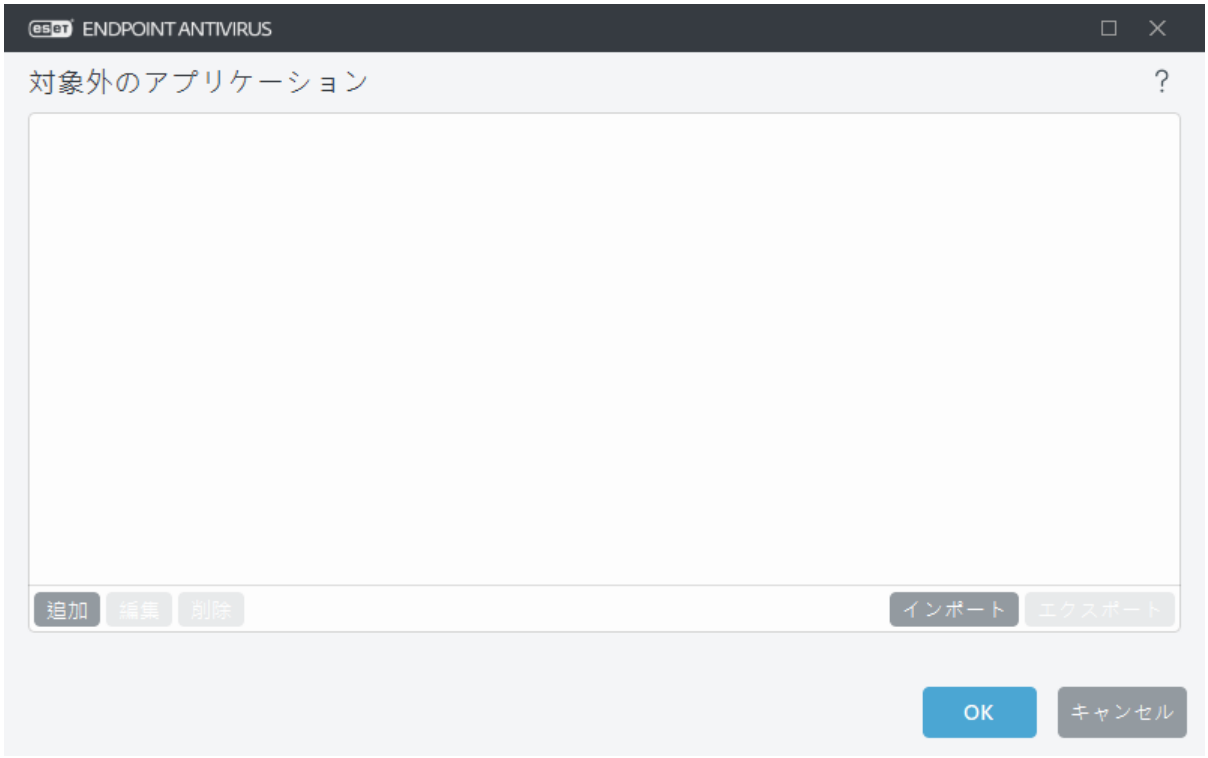

# 対象外のアプリケーション

特定のアプリケーションの通信の検査対象から除外するには、そのアプリケーションをリストに追加します。選択したアプリケーションのHTTP(S)/POP3(S)/IMAP(S)通信のマルウェアは検査されません。通信を検査すると正常に機能しないアプリケーションに限って、この機能を使用することをお勧めします。

**追加**をクリックすると、実行中のアプリケーションとサービスはここから自動的に利用できるようになります。**...**をクリックし、アプリケーションに移動して手動で除外を追加します。

**編集** – リストから選択したエントリを編集します。

**削除** – 選択したエントリーをリストから削除します。



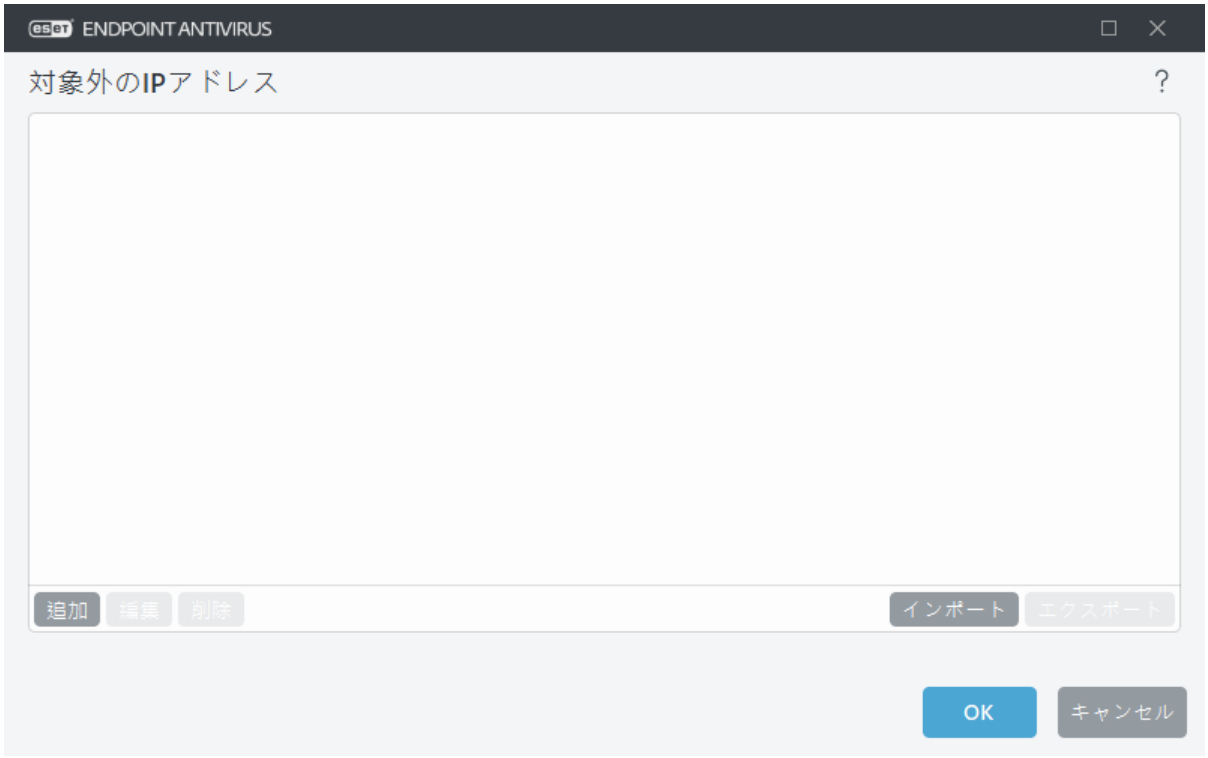

# 除外されたIP

リスト中のエントリは検査から除外されます。選択したアドレスに対する送受信のHTTP(S)/POP3(S)/IMAP(S)通信のマルウェアは検査されません。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。

**追加** – クリックすると、ルールが適用されるリモートポイントのIPアドレス/アドレス範囲/サブネットを追加することができます。

**編集** – リストから選択したエントリを編集します。

**削除** – 選択したエントリーをリストから削除します。




### IPアドレスの例

IPv4アドレスの追加:

**単一のアドレス** – 各コンピューターのIPアドレス(*192.168.0.10*など)を追加します。

**アドレス範囲** – 最初と最後のIPアドレスを入力して、*192.168.0.1*–*192.168.0.99*など、複数のコンピューターのIP範囲を指定します。

**サブネット** – サブネット(コンピューターのグループ)は、IPアドレスとマスクによって定義されます。たとえば、255.255.255.0は192.168.1.0サブネットのネットワークマスクです。*192.168.1.0/24*でサブネットタイプ全体を除外します。

IPv6アドレスの追加:

**単一のアドレス** - *2001:718:1c01:16:214:22ff:fec9:ca5*など、各コンピューターのIPアドレスを追加します。

**サブネット** – サブネット(コンピューターのグループ)は、IPアドレスとマスクによって定義されます(例: *2002:c0a8:6301:1::1/64*)

# メールボックス保護

ESET Endpoint Antivirusをメールボックスと統合すると、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。

メールボックス保護を設定するには、詳細設定 > **保護** > **電子メールクライアント保護** > **メールボックス保護**を開きます。

**クライアントプラグインによって電子メール保護を有効にする** – 無効にすると電子メールクライアントプラグインによる保護がオフなります。

検査する電子メールを選択:

- **受信メール**
- **送信メール**
- **既読メール**
- **変更された電子メール**

**クライアントプラグインによって電子メール保護を有効にする**を有効にすることをお勧めします。統合が無効である場合や機能していない場合でも、電子メール通信がメール転送保護(IMAP/IMAPSおよびPOP3/POP3S)で保護されます。

**統合** – メールボックス保護を電子メールクライアントに統合できます。詳細については、統合を参照してください。

**応答** – 迷惑メールメッセージの処理をカスタマイズできます。詳細については、応答を参照してください。

# 統合

ESET Endpoint Antivirus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。電子メールクライアントがサポートされている場合は、ESET Endpoint Antivirusで統合を有効にできます。統合が有効な場合ESET Endpoint Antivirusツールバーが直接電子メールクライアントに挿入され、電子メール保護を効率化できます。統合設定を編集するには、詳細設定 > **保護** > **電子メールクライアント保護** > **メールボックス保護** > **統合**を開きます。

**Microsoft Outlookに統合する** – 現在、Microsoft Outlookはサポートされている唯一の電子メールクライアントです。電子メール保護はプラグインとして機能します。プラグインの主な利点は、使用されるプロトコルに依存しない点です。暗号化されたメールをメールクライアントが受信した場合、メールは解読されてウイルススキャナーに送信されます。サポートされているMicrosoft Outlookバージョンの一覧については、このESETナレッジベース記事を参照してください。

**詳細電子メールクライアント処理** – 追加のOutlook Messaging API (MAPI)イベントのオブジェクト変更(`fnevObjectModified`)およびオブジェクト作成(`fnevObjectCreated`)を処理します。電子メールクライアントの使用時にシステムの速度が低下する場合は、このオプションを無効にしてください。

# Microsoft Outlookツールバー

Microsoft Outlookの保護機能はプラグインとして動作しますESET Endpoint Antivirusがインストールされると、ウイルス対策保護オプションを含むこのツールバーがMicrosoft Outlookに追加されます。

**ESET Endpoint Antivirus** – アイコンをダブルクリックするとESET Endpoint Antivirusのメインウィンドウが開きます。

**メッセージの再検査** – 電子メールのチェックを手動で開始できます。チェックするメッセージを指定して、受信メールの再検査を有効にできます。詳細については、メールボックス保護を参照してください。

**スキャナーの設定** - メールボックス保護の設定オプションを表示します。

# 確認ダイアログ

この通知は、選択したアクションの実行を確認する意味で表示されるので、誤った操作を防止する効果があります。

一方、ダイアログにはこの確認を行わないオプションも用意されています。

# メッセージの再検査

メールクライアントに組み込まれたESET Endpoint Antivirusのツールバーでは、メール検査に関するオプションをいくつか指定できます。[**メッセージの再検査**]オプションでは次の2つのスキャンモードを選択できます。

**現在のフォルダ内にあるすべてのメッセージ** – 現在表示されているフォルダ内にあるメッセージを検査します。

**選択したメッセージのみ** – ユーザーがマークしたメッセージのみを検査します。

[**検査済みのメッセージも含む**]チェックボックスをオンにすると、事前に検査されているメッセージを再度検査できます。

# 応答

メッセージ検査の結果に基づいてESET Endpoint Antivirusは検査したメッセージを移動したり、件名にカスタムテキストを追加したりできます。これらの設定は、詳細設定 > **保護** > **電子メールクライアント保護** > **メールボックス保護** > **応答**で設定できます。

検出を含むメッセージがある場合、既定ではESET Endpoint Antivirusはメッセージの駆除を試行します。メッセージを駆除できない場合は、**駆除できない場合に実行するアクション**を選択できます。

- **何もしない** – これを有効にすると、感染している添付ファイルは特定されますが、メールに対してはいずれのアクションも実行されずそのまま残ります。
- **メールの削除** – 侵入がユーザーに通知され、メールは削除されます。
- **メールをゴミ箱に移動する** – 感染しているメールを自動的に[削除済み]フォルダに移動します。
- **メールを次のフォルダに移動**(既定のアクション) – 感染しているメールを自動的に指定したフォルダに移動します。

**移動先のファイル** – 検出に感染した電子メールを移動するカスタムフォルダを指定します。

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。**受信メールと既読メールに検査メッセージを追加**または**送信メールに検査メッセージを追加**を選択できます。まれに、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/既読メールまたは送信メール(あるいはその両方)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** – タグメッセージが追加されません。
- **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 / 送信メールの件名を更新** – このオプションを有効にすると、以下で指定したカスタムテキストがメッセージに追加されます。

**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、"[detection %DETECTIONNAME%] Hello"で置き換えられます。変数の%DETECTIONNAME%は検出を表します。

# ThreatSense

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

設定ウィンドウにアクセスするにはThreatSense技術を使用する任意のモジュール(下記を参照)の詳細設定にある**ThreatSense**をクリックします。セキュリティシナリオごとに異なる設定が必要になることがあります。これを念頭に、ThreatSenseは、次の保護モジュールについて個々に設定することができます。

- リアルタイム検査
- アイドル状態検査
- スタートアップ検査の設定
- ドキュメント保護
- 電子メールクライアント保護
- Webアクセス保護
- コンピューターの検査

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、パラメーターを変更すると、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)。コンピューターの検査を除く全ての機能についてThreatSenseの既定のパラメーターを変更しないことをお勧めします。

## 検査するオブジェクト

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。

**システムメモリ** – システムメモリーを攻撃対象とするマルウェアを検査します。

**ブートセクタ/UEFI** – ブートセクターのマスターブートレコードにおけるマルウェアの存在を検査します。用語集のUEFIの詳細をお読みください

**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** – 拡張子ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACEなどがサポートされます。

**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(UPX, yoda, ASPack, FSGなど)のほかにも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次のとおりです。

**ヒューリスティック** – ヒューリスティックは、悪意のあるプログラムの活動を分析するアルゴリズムです。この技術の主な利点は、前には存在しなかったり、これまでの検出エンジンのバージョンで特定されていなかったりした悪意のあるソフトウェアを特定できる点です。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署名** – 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

駆除設定は、オブジェクト駆除中のESET Endpoint Antivirusの動作を決定します。

## 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。このThreatSense設定のセクションでは、検査するファイルの種類を指定します。

## その他

オンデマンドコンピューターの検査でThreatSenseエンジン設定を設定する場合は、**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。

**すべてのオブジェクトをログに記録する** – 検査ログには、自己解凍アーカイブで、感染していないファイルも含め、すべての検査されたファイルが表示されます(大量の検査ログデータが生成され、検査ログファイルのサイズが大きくなることがあります)。

**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

**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。

**オブジェクトの最大検査時間(秒)** – コンテナーオブジェクト(RAR/ZIPアーカイブや複数の添付ファイルを含む電子メールなど)のファイルを検査する最大時間の値を定義します。この設定は、スタンドアロンファイルには適用されません。ユーザー定義の値が入力され、その時間が経過すると、コンテナーオブジェクトの各ファイルの検査が完了したかどうかに関係なく、検査が可能な限りすぐに停止します。大きなファイルを含むアーカイブの場合、検査はアーカイブからファイルが展開された後すぐに停止します(たとえば、ユーザー定義変数が3秒で、ファイルの展開には5秒かかる場合)。アーカイブの残りのファイルは、その時間が経過した後は検査されません。大きなアーカイブを含む検査時間を制限するには、**最大オブジェクトサイズ**と**アーカイブのファイルの最大サイズ**を使用します(セキュリティ上のリスクの可能性があるため推奨されません)。既定値は無制限です。

### アーカイブ検査の設定

**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.

**アーカイブの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。最大値は3 GB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。

# Webアクセス保護

Webアクセス保護では、インターネット保護モジュールの詳細設定を設定できます。次のオプションは、詳細設定 > **保護** > **Webアクセス保護** > **Webアクセス保護**で使用できます。

**Webアクセス保護を有効にする** – この機能が無効になるとWebアクセス保護とフィッシング対策機能は実行されません。

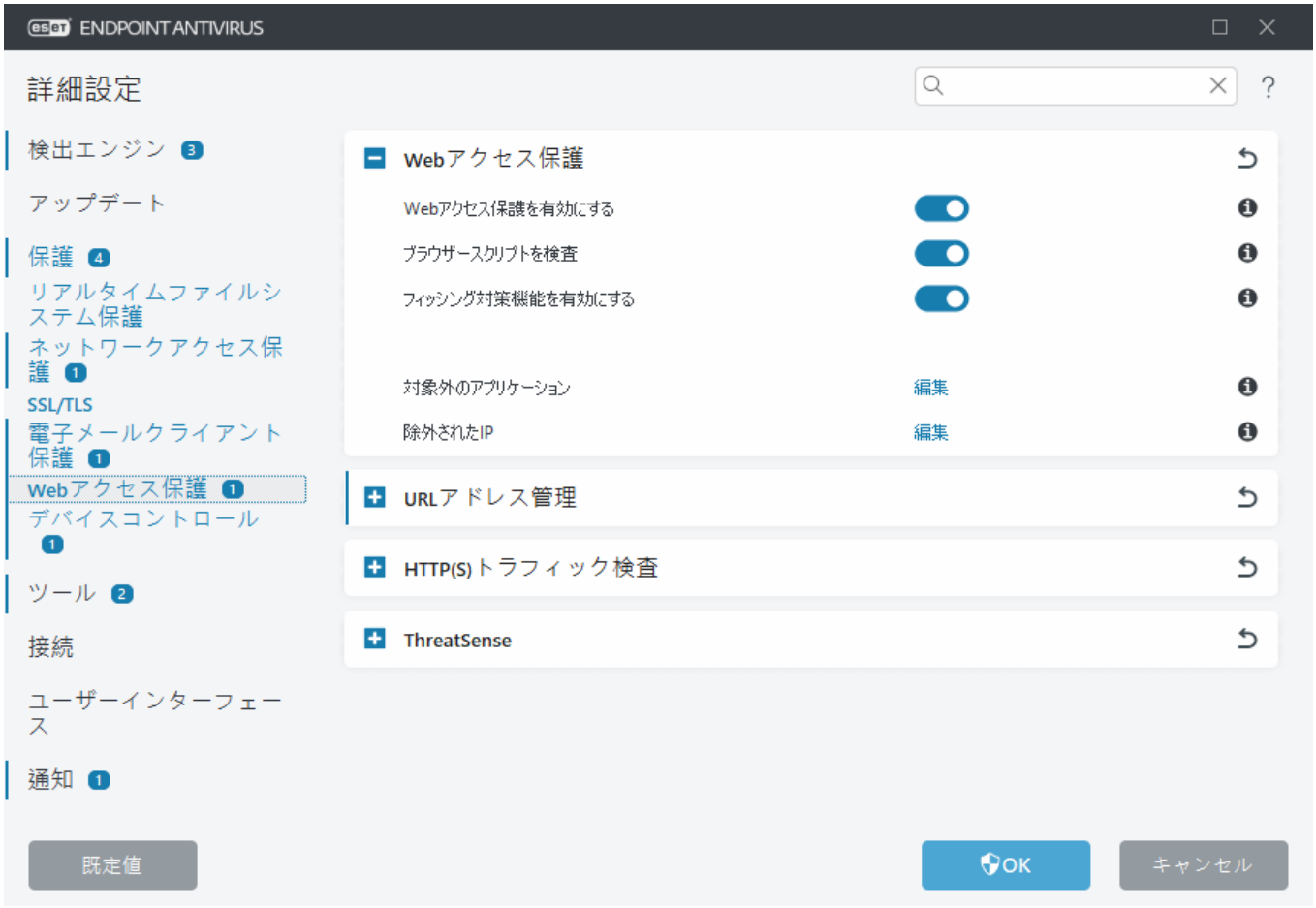
> 既定のままWebアクセス保護を有効にしておき、アプリケーションやIPアドレスを除外しないことを強くお勧めします。

**ブラウザースクリプトを検査** – 有効にすると、検出エンジンはWebブラウザーによって実行されるすべてのJavaScriptプログラムをチェックします。

**フィッシング対策機能を有効にする** – 有効にすると、フィッシングWebページがブロックされます。詳細については、「フィッシング対策保護」を参照してください。

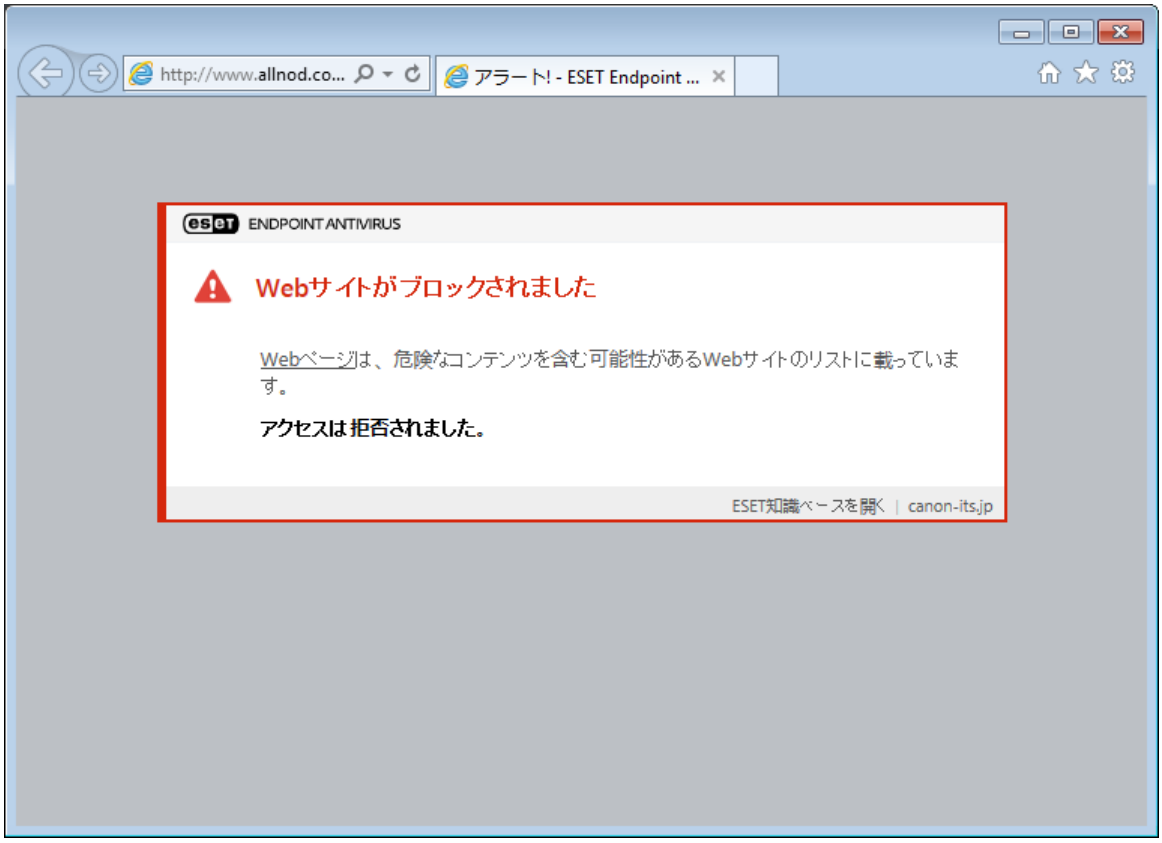
対象外のアプリケーション – 特定のアプリケーションをWebアクセス保護による検査対象から除外できますWebアクセス保護によって互換性の問題が発生した場合に便利です。

除外されたIP – 特定のリモートアドレスをWebアクセス保護による検査対象から除外できますWebアクセス保護によって互換性の問題が発生した場合に便利です。




---

Webアクセス保護は、Webサイトがブロックされたときに、ブラウザーに次のメッセージが表示されます。




次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
• ESET Endpoint Antivirusで個別のワークステーションの安全なWebサイトをブロック解除する

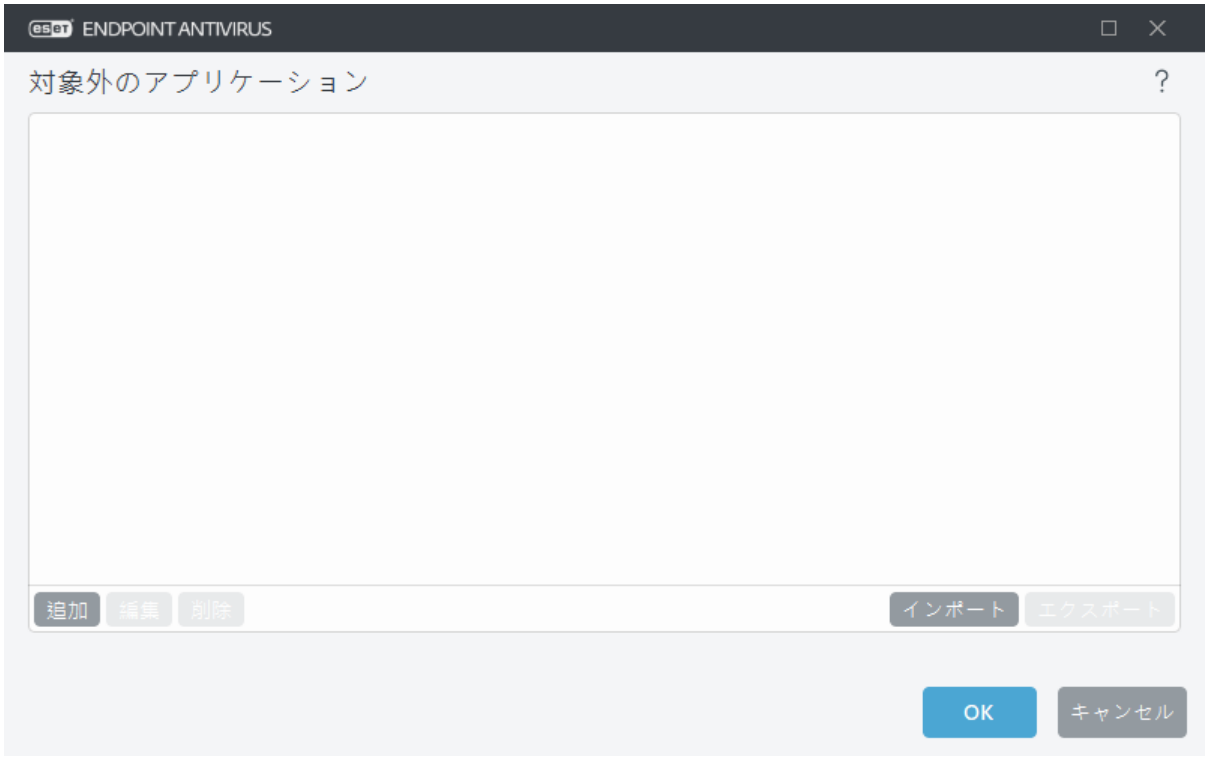
# 対象外のアプリケーション

特定のアプリケーションの通信の検査対象から除外するには、そのアプリケーションをリストに追加します。選択したアプリケーションのHTTP(S)/POP3(S)/IMAP(S)通信のマルウェアは検査されません。通信を検査すると正常に機能しないアプリケーションに限って、この機能を使用することをお勧めします。

**追加**をクリックすると、実行中のアプリケーションとサービスはここから自動的に利用できるようになります。**...**をクリックし、アプリケーションに移動して手動で除外を追加します。

**編集** – リストから選択したエントリを編集します。

**削除** – 選択したエントリーをリストから削除します。



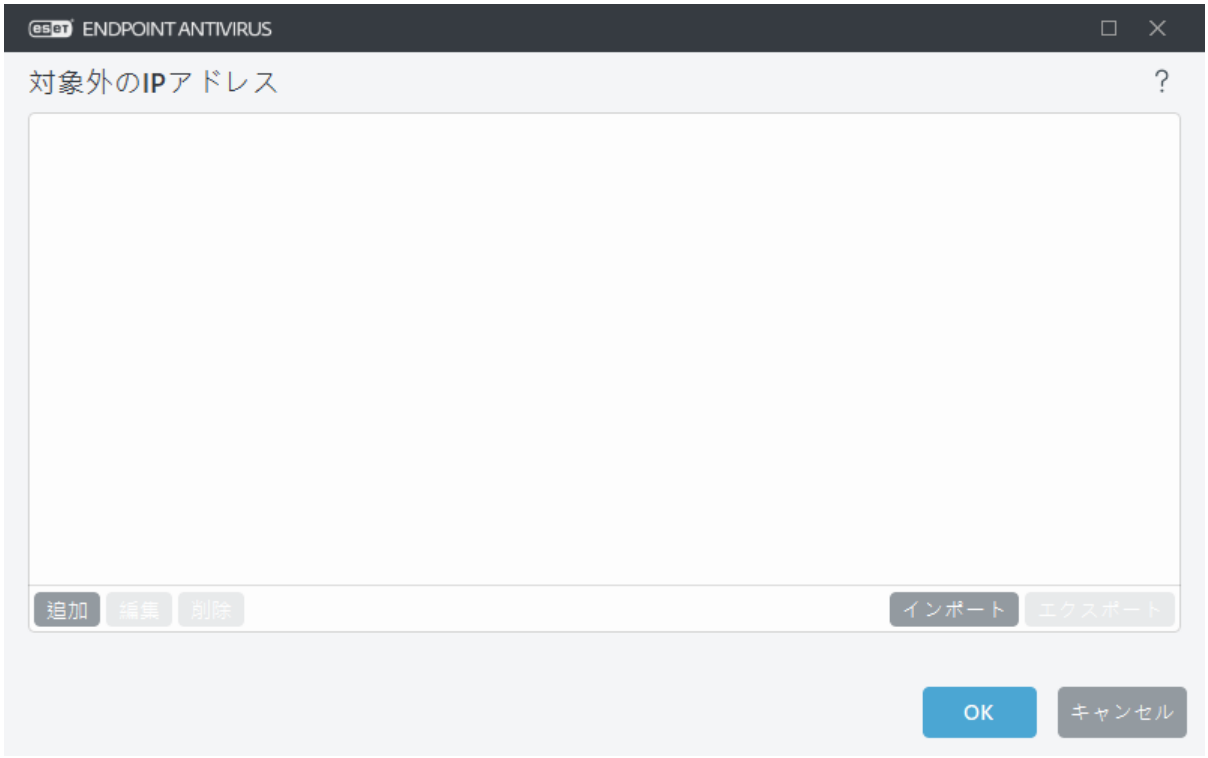

# 除外されたIP

リスト中のエントリは検査から除外されます。選択したアドレスに対する送受信のHTTP(S)/POP3(S)/IMAP(S)通信のマルウェアは検査されません。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。

**追加** – クリックすると、ルールが適用されるリモートポイントのIPアドレス/アドレス範囲/サブネットを追加することができます。

**編集** – リストから選択したエントリを編集します。

**削除** – 選択したエントリーをリストから削除します。




**IPアドレスの例**

IPv4アドレスの追加:

**単一のアドレス** – 各コンピューターのIPアドレス(*192.168.0.10*など)を追加します。

**アドレス範囲** – 最初と最後のIPアドレスを入力して、*192.168.0.1*–*192.168.0.99*など、複数のコンピューターのIP範囲を指定します。

**サブネット** – サブネット(コンピューターのグループ)は、IPアドレスとマスクによって定義されます。たとえば、255.255.255.0は192.168.1.0サブネットのネットワークマスクです。*192.168.1.0/24*でサブネットタイプ全体を除外します。

IPv6アドレスの追加:

**単一のアドレス** - *2001:718:1c01:16:214:22ff:fec9:ca5*など、各コンピューターのIPアドレスを追加します。

**サブネット** – サブネット(コンピューターのグループ)は、IPアドレスとマスクによって定義されます(例: *2002:c0a8:6301:1::1/64*)

# URLアドレス管理

詳細設定 > **保護** > **Webアクセス保護**の**URLアドレス管理**で、ブロック、許可、またはコンテンツ検査から除外するHTTPアドレスを指定できます。

HTTPに加えてHTTPSアドレスをフィルタリングする場合は、SSL/TLSを有効にする必要があります。そうしないとアクセスしたHTTPSサイトのドメインのみが追加され、完全なURLは追加されません。

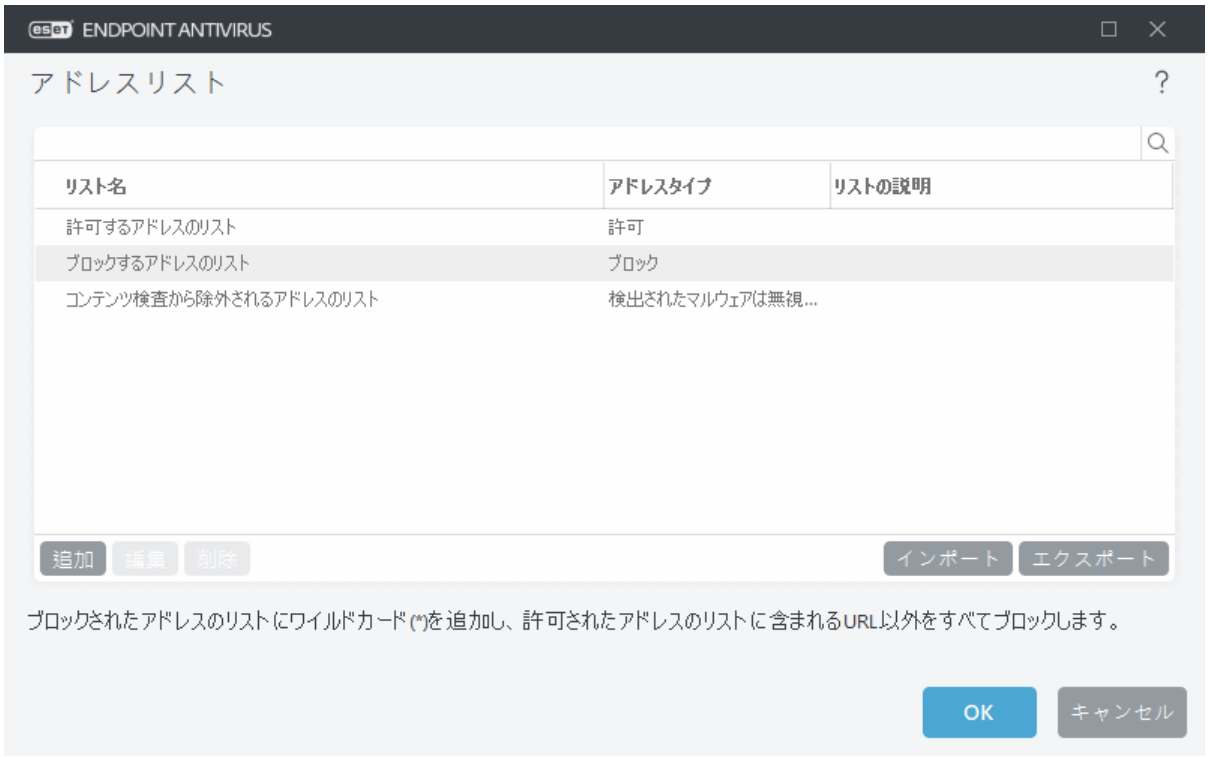
**ブロックするアドレスのリスト**のWebサイトは、**許可するアドレスのリスト**にも重複して登録されている場合を除いて、アクセスできません。**コンテンツ検査から除外されるアドレスのリスト**のWebサイトは、アクセス時に悪意のあるコードがあるかどうかの検査が行われません。

アクティブな**許可するアドレスのリスト**にあるアドレスを除き、すべてのHTTPアドレスをブロックする場合は、アクティブな**ブロックするアドレスのリスト**に*を追加します。

特殊記号の*(アスタリスク)および?(疑問符)も各アドレスリストで使用できます。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、記号の*および?を各アドレスリスト内で正しく使用してください。すべてのサブドメインを含むドメイン全体が安全に照合される方法については、「HTTPアドレス/ドメインのマスクの追加」を参照してください。アドレスリストを有効にするには、**[アクティブのリスト]**をクリックします。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。

> **ESETによって信頼されたアドレス**
>
> SSL/TLSで**ESETによって信頼されたドメインのトラフィックを検査しない**が有効になっている場合、ESETによって管理されるホワイトリスト上のドメインは、URLアドレス管理設定の影響を受けません。




## コントロール要素

**追加** – 定義済みのリストの他に、新しいリストを作成します。さまざまなグループのアドレスを論理的に分割する場合に便利です。例えば、ブロックされたアドレスの1つのリストには、一部の外部パブリックブラックリストのアドレスを登録し、もう1つのブロックされたアドレスのリストには独自のブラックリストを登録できます。これにより自分のブラックリストを修正せずに、外部リストを簡単に更新できます。

**編集** – 既存のリストを修正します。これを使用して、アドレスを追加・削除します。

**削除** – 既存のリストを削除します。追加で作成したリストのみを削除できます。**追加**で作成したリストのみを削除できます。既定は削除できません。

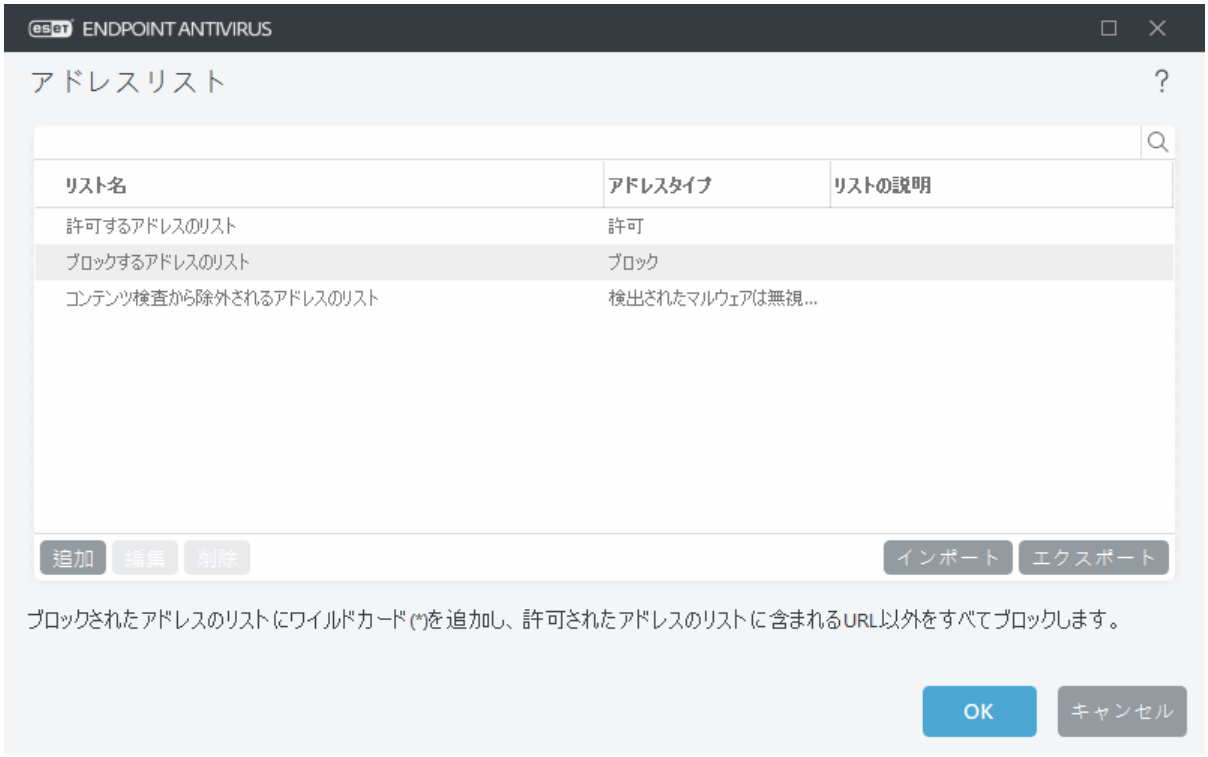
# アドレスリスト

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(S)アドレスのリストを指定できます。

既定では、次の3つのリストを使用できます。

- **コンテンツ検査から除外されるアドレスのリスト** – アドレスをリストに追加すると、悪意のあるコードのチェックは実行されません。
- **許可するアドレスのリスト** – [許可されたアドレスのリスト内のHTTPアドレスのみにアクセスを許可する]が有効で、ブロックされたアドレスのリストに*(すべてと一致)が含まれる場合、ユーザーはこのリストで指定されたアドレスのみにアクセスできます。このリストのアドレスは、ブロックされたアドレスのリストに含まれる場合にでも、許可されます。
- **ブロックするアドレスのリスト** – 許可するアドレスのリストにも重複して登録されている場合を除いて、ユーザーは、このリストで指定されたアドレスにはアクセスできません。

新しいリストを作成するには、[**追加**]をクリックします。選択したリストを削除するには、[**削除**]をクリックします。




次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
- ESET Endpoint Antivirusで個別のワークステーションの安全なWebサイトをブロック解除する

詳細については、「URLアドレス管理」を参照してください。

# 新しいアドレスリストの作成

このダイアログウィンドウでは、ブロック、許可、またはチェックから除外するURLアドレス/マスクの新しいリストを設定できます。

次のオプションを設定できます。

**アドレスリストのタイプ** – 3種類のリストがあります。

- **検出されたマルウェアは無視されます** – アドレスをリストに追加すると、悪意のあるコードのチェックは実行されません。
- **ブロック** –このリストで指定されたアドレスへのアクセスはブロックされます。
- **許可** –このリストで指定されたアドレスへのアクセスは許可されます。このリストのアドレスは、ブロックされたアドレスのリストと一致する場合でも、許可されます。

**リスト名** – リストの名前を指定します。このフィールドは、定義済みリストのいずれかを編集するときには使用できません。

**リストの説明** – リストの短い説明を入力します(オプション)。定義済みリストのいずれかを編集するときには使用できません。

リストを有効にするには、リストの横の**アクティブのリスト**をクリックしますWebサイトにアクセスし、特定のリストが使用されたときに通知を表示する場合は、**適用時に通知**を選択します。たとえば、ブロックされた許可されたアドレスのリストにあるWebサイトがブロックまたは許可された場合、通知が発行されます。通知には、リストの名前があります。

**ログの重要度** – ドロップダウンメニューから重要度を選択します。警告詳細レベルのレコードは、ESET PROTECTによって収集できます。

情報と警告ロギングの詳細レベルは、ドメイン内にワイルドカードを使用せずに2つ以上のコンポーネントを含むルールでのみ使用できます。例:
- *.domain.com/*
- *www.domain.com/*

## コントロール要素

**追加** – 新しいURLアドレスをリストに追加します(複数の値は区切り文字を使用して入力)。

**編集** – リストの既存のアドレスを修正します。**追加**を使用して作成されたアドレスでのみ使用できます。

**削除** – リストの既存のアドレスを削除します。**追加**を使用して作成されたアドレスでのみ使用できます。

**インポート** - URLアドレスを含むファイルをインポートします(たとえば、エンコードUTF-8を使用した*.txtなど、値を改行で区切ります)。

詳細については、URLマスクの追加方法の章を参照してください。

# URLマスクを追加する方法

希望のアドレス/ドメインマスクを入力する前に、このダイアログの指示を確認してください。

ESET Endpoint Antivirusでは、指定したWebサイトへのアクセスを遮断して、インターネットブラウザにそのコンテンツを表示させないようにすることができます。さらに、検査から除外するアドレスを指定することもできます。リモートサーバの完全な名前が不明であるか、またはリモートサーバのグループ全体を指定する場合には、いわゆるマスクを使用して、そのようなグループを特定できます。マスクには、記号の"?"と"*"があります。

- 記号1つを表すには、"?"を使用します。
- 文字列1つを表すには、"*"を使用します。

たとえば、*.c?mは最後の部分がcで始まってmで終わり、その間に任意の記号が1つ入るアドレス全て(.comや. camなど)を表します。

たとえば、マスク*x?は最後の2文字前の文字がであるアドレスを示します。ドメイン全体と一致させるには、*.domain.com/*の形式で入力します。マスクでプロトコルプレフィックスhttp://https://を指定

することは任意です。省略する場合、マスクはすべてのプロトコルと一致します。先頭の「*.」シーケンスは、ドメイン名の先頭で使用されると、特殊な方法で処理されます。まず、この場合、*ワイルドカードはスラッシュ文字(「/」)とは一致しません。これによりマスクの迂回を回避します。たとえば、マスク*.domain.comは http://anydomain.com/anypath#.domain.comと一致しません(このようなサフィックスはダウンロードに影響せずにURLの最後に付加できます)。次に、この特殊な場合では、「*.」は空の文字列にも一致します。これは、1つのマスクを使用したサブドメインを含むドメイン全体と一致できるようにするためです。たとえば、マスク*.domain.comは http://domain.comにも一致します。*domain.comの使用は http://anotherdomain.comにも一致するため、正しくありません。

情報と警告ロギングの詳細レベルは、ドメイン内にワイルドカードを使用せずに2つ以上のコンポーネントを含むルールでのみ使用できます。例:
- *.domain.com/*
- *www.domain.com/*

# HTTP(S)トラフィック検査

既定で、ESET Endpoint Antivirusはインターネットブラウザーやその他のアプリケーションで使用されるHTTPおよびHTTPSトラフィックを検査するように設定されています。サードパーティのソフトウェアで問題が発生していて、問題の原因がESET Endpoint Antivirusなのか確認したい場合のみ、トラフィック検査を無効にしてください。

**HTTPトラフィック検査を有効にする** – HTTPトラフィックは、すべてのアプリケーションのすべてのポートで常に監視されます。

**HTTPSトラフィック検査を有効にする** -HTTPSトラフィックでは、暗号化チャンネルを使用して、サーバーとクライアント間で情報を送受信しますESET Endpoint Antivirusは、SSL (Secure Socket Layer)およびTLS (Transport Layer Security)プロトコルを使用した通信を検査します。このプログラムは、オペレーティングシステムのバージョンに関係なく、**HTTPS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を検査します(事前に定義された443と0-65535にポートを追加できます)。

# ThreatSense

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

設定ウィンドウにアクセスするにはThreatSense技術を使用する任意のモジュール(下記を参照)の詳細設定にある**ThreatSense**をクリックします。セキュリティシナリオごとに異なる設定が必要になることがあります。これを念頭に、ThreatSenseは、次の保護モジュールについて個々に設定することができます。

- リアルタイム検査
- アイドル状態検査

- スタートアップ検査の設定
- ドキュメント保護
- 電子メールクライアント保護
- Webアクセス保護
- コンピューターの検査

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、パラメーターを変更すると、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)。コンピューターの検査を除く全ての機能について□ThreatSenseの既定のパラメーターを変更しないことをお勧めします。

# 検査するオブジェクト

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。

**システムメモリ** – システムメモリーを攻撃対象とするマルウェアを検査します。

**ブートセクタ□/UEFI** – ブートセクターのマスターブートレコードにおけるマルウェアの存在を検査します。用語集のUEFIの詳細をお読みください□

**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** – 拡張子ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACEなどがサポートされます。

**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(UPX, yoda, ASPack, FSGなど)のほかにも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次のとおりです。

**ヒューリスティック** – ヒューリスティックは、悪意のあるプログラムの活動を分析するアルゴリズムです。この技術の主な利点は、前には存在しなかったり、これまでの検出エンジンのバージョンで特定されていなかったりした悪意のあるソフトウェアを特定できる点です。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署名** – 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

駆除設定は、オブジェクト駆除中のESET Endpoint Antivirusの動作を決定します。

## 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。このThreatSense設定のセクションでは、検査するファイルの種類を指定します。

## その他

オンデマンドコンピューターの検査でThreatSenseエンジン設定を設定する場合は、**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。

**すべてのオブジェクトをログに記録する** – 検査ログには、自己解凍アーカイブで、感染していないファイルも含め、すべての検査されたファイルが表示されます(大量の検査ログデータが生成され、検査ログファイルのサイズが大きくなることがあります)。

**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

**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。

**オブジェクトの最大検査時間(秒)** – コンテナーオブジェクト(RAR/ZIPアーカイブや複数の添付ファイルを含む電子メールなど)のファイルを検査する最大時間の値を定義します。この設定は、スタンドアロンファイルには適用されません。ユーザー定義の値が入力され、その時間が経過すると、コンテナーオブジェクトの各ファイルの検査が完了したかどうかに関係なく、検査が可能な限りすぐに停止します。大きなファイルを含むアーカイブの場合、検査はアーカイブからファイルが展開された後すぐに停止します(たとえば、ユーザー定義変数が3秒で、ファイルの展開には5秒かかる場合)。アーカイブの残りのファイルは、その時間が経過した後は検査されません。大きなアーカイブを含む検査時間を制限するには、**最大オブジェクトサイズ**と**アーカイブのファイルの最大サイズ**を使用します(セキュリティ上のリスクの可能性があるため推奨されません)。既定値は無制限です。

## アーカイブ検査の設定

**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.

**アーカイブの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。最大値は3 GB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。

# デバイスコントロール

ESET Endpoint Antivirusは、デバイス(CD/DVD/USBなど)の自動コントロールを提供します。このモジュールを使用すると、拡張フィルタ/権限をブロック、または調整して、ユーザーからの指定デバイスへのアクセス方法やその作業方法を定義できます。この機能は、望ましくないコンテンツを収めたデバイスをユーザーが使用することを防止したいコンピューター管理者に便利です。

## サポートされている外部デバイス:

- ディスクストレージ(HDD、USBリムーバブルディスク)
- CD/DVD
- USBプリンター
- FireWireストレージ
- Bluetoothデバイス
- スマートカードリーダー
- イメージングデバイス
- モデム
- LPT/COMポート
- ポータブルデバイス(メディアプレイヤー、スマートフォン、プラグアンドプレイデバイスなどのバッテリ電源のデバイス)
- すべてのデバイスタイプ

デバイスコントロール設定オプションは、[詳細設定] > **保護** > [**デバイスコントロール**]で変更できます。

**デバイスコントロールを有効にする**トグルをクリックしてESET Endpoint Antivirusのデバイスコントロール機能を有効にします。この変更を有効にするには、コンピューターを再起動する必要があります。デバイスコントロールを有効にした後、ルールエディタウィンドウで**ルール**を定義できます。

> スケジューラを使用して、ルールを含むデバイスコントロールグループをXMLファイルからインポートできます。詳細と段階的なガイドについては、ESETナレッジベース記事を参照してください。

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

# デバイスコントロールルールエディタ

**デバイスコントロールルールエディタ**ウィンドウには既存のルールが表示されます。このウィンドウを使用すると、ユーザーがコンピューターに接続する外付けデバイスを細かくコントロールすることができます。デバイスコントロールルールの追加も参照してください。

次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
ESETエンドポイント製品を使用してデバイスコントロールルールを追加および変更する


特定のデバイスについては、ユーザー単位またはユーザーグループ単位で、および複数の追加パラメータに基づいて許可またはブロックできます。これは、ルール設定で指定できます。ルールのリストには、名前、デバイスタイプ、デバイスがコンピューターに接続された際に行われるアクション、ログ記録の重大度といった複数の説明を含みます。

[**追加**]または[**編集**]をクリックしてルールを管理します。ルールの横の**有効**チェックボックスをオフにすると、今後使用するときまで無効になります。1つ以上のルールを選択し、[**削除**]をクリックすると、ルールが完全に削除されます。

**コピー** – 別の選択済みルールで使用されている事前定義オプションを備えた新しいルールを作成します。

コンピュータに接続されているデバイスのリムーバブルメディアデバイスパラメータを自動的に入力するには、[**入力**]をクリックします。

ルールは優先度順に一覧表示されます。最も優先度が高いルールが最上位近くに表示されます。
最上位/上/下/最下位**をクリックすると、ルールを移動し、個別またはグループで移動できます。**

デバイスコントロールログは、デバイスコントロールがトリガーされるすべての状況を記録します。ログエントリは、ESET Endpoint Antivirusのメインプログラムウィンドウの[**ツール**] > [ログファイル]から表示できます。

# 検出されたデバイス

[**入力**]ボタンを使用すると、現在接続されているすべてのデバイスの概要が表示されます。この情報には、デバイスタイプ、デバイスの製造元、モデル、シリアル番号(ある場合)などがあります。

検出されたデバイスのリストからデバイスを選択し、**OK**をクリックして、定義済み情報のデバイスコン

トロールルールを追加します(すべての設定は調整できます)。

低電力(スリープ)モードのデバイスには警告アイコンが表示されます。**OK**ボタンを有効にして、このデバイスのルールを追加するには、次の手順を実行します。

- デバイスを再接続します。
- デバイスを使用します(たとえばWindowsでカメラアプリを起動し、Webカメラをウェイクアップします)。

# デバイスコントロールルールの追加

デバイスコントロールルールでは、ルール基準に適合するデバイスがコンピューターに接続されたときに実行されるアクションを定義します。


特定しやすいように、ルールの説明を**名前**フィールドに入力します。**ルール有効**の横のスライドバーを選択すると、このルールは無効または有効になります。これは、ルールを完全に削除したくない場合に便利です。

**適用期間** - 特定の期間に作成されたルールを適用できます。ドロップダウンメニューから、時間スロットを選択します。時間スロットの詳細を参照してください。

## デバイスのタイプ

外部デバイスタイプをドロップダウンメニュー(ディスクストレージ/ポータブルデバイス/Bluetooth/FireWire/...)から選択します。デバイスタイプ情報は、オペレーティングシステムから収集されます。デバイスタイプは、デバイスがコンピューターに接続されていれば、そのシステムのデバイスマネージャで確認できます。記憶装置にはUSBまたはFireWireから接続できる外付けハードディスク

や標準的なメモリカードリーダーが含まれます。スマートカードリーダーとはSIMカード、認証カードなど、集積回路が埋め込まれているスマートカードを読み取るリーダーのことです。イメージングデバイスの例としては、スキャナやカメラが挙げられます。これらのデバイスはアクションに関する情報だけを提供し、ユーザーに関する情報は提供しないため、グローバルにのみブロックできます。

ユーザー一覧機能はモデムデバイスタイプで使用できません。ルールはすべてのユーザーに適用され、現在のユーザー一覧は削除されます。

## アクション

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

- **許可** – デバイスへの完全アクセスが許可されます。
- **ブロック** – デバイスへのアクセスはブロックされます。
- **書き込みブロック** – デバイスからの読み込みアクセスだけが許可されます。
- **警告** – デバイスに接続するたびに、許可またはブロックするかが通知され、ログエントリが作成されます。デバイスは記憶されません。同じデバイスに後から接続する場合にも、通知が表示されます。

デバイスのタイプによっては、適用されないアクション(権限)もあります。記憶装置タイプのデバイスの場合、4つのアクションすべてを使用できます。記憶装置以外のデバイスでは、これらのうち3つだけが適用可能です(たとえばBluetoothの場合、[**書き込みブロック**]アクションは適用できないので、許可かブロックだけになります)。

## 条件タイプ

**デバイスグループ**または**デバイス**を選択します。

次の追加パラメーターは、さまざまなデバイスに合わせてルールを微調整するのに使用できます。すべてのパラメーターは大文字と小文字を区別し、ワイルドカード(*、?)をサポートします。

- **ベンダー** – ベンダー名またはIDによるフィルタリング。
- **モデル** – デバイスに付けられている名前。
- **シリアル番号** – 外部デバイスには通常独自のシリアル番号が付いていますCD/DVDの場合は、CDドライブではなく、そのメディアのシリアル番号があります。

これらのパラメータが未定義の場合、ルールは照合時にこれらのフィールドを無視します。すべてのフィールドのフィルタリングパラメーターは大文字と小文字を区別し、ワイルドカード(疑問符(?)は1つの文字を表し、アスタリスク(*)は0文字以上の文字列を表します)をサポートします。

デバイス情報を表示するには、デバイスのタイプのルールを作成し、デバイスをコンピュータに接続してから、デバイスコントロールログでデバイス詳細を確認します。

## ログ記録の重大度

- **常に** – すべてのイベントをログに記録します。
- **診断** – プログラムを微調整するのに必要な情報をログに記録します。
- **情報** – 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。
- **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、ERA Serverに送信します。
- **なし** – ログは記録されません。

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

- **追加**-[**オブジェクトの種類:ユーザーまたはグループ**]ダイアログウィンドウを開きます。このウィンドウで目的のユーザーを選択できます。
- **削除** – 選択されたユーザーをフィルタから削除します。

> **ユーザーリストの制限**
> 特定のデバイスタイプのルールには、ユーザーリストを定義できません。
> • USBプリンタ
> • Bluetoothデバイス
> • スマートカードリーダー
> • イメージングデバイス
> • モデム
> • LPT/COMポート

**ユーザーに通知** – 既存のルールでブロックされているデバイスが挿入されると、通知ウィンドウが表示されます。

# デバイスグループ

> ⚠ コンピュータに接続されたデバイスは、セキュリティリスクになる可能性があります。

デバイスグループウィンドウは、2つの部分に分かれます。ウィンドウの右側には、該当するグループに属するデバイスが一覧表示されます。ウィンドウの左側には、作成されたグループが表示されます。デバイスを右側のペインに表示するグループを選択します。

デバイスグループウィンドウを開き、グループを選択すると、一覧からデバイスを追加または削除します。また、ファイルからインポートして、グループにデバイスを追加することもできます。あるいは、[**入力**]ボタンをクリックすると、コンピュータに接続されたすべてのデバイスが[**検出されたデバイス**]ウィンドウに一覧表示されます。入力されたリストからデバイスを選択し、**OK**をクリックしてグループに追加します。

## コントロール要素

**追加** – ボタンをクリックしたウィンドウの部分に応じて、名前またはデバイスを既存のグループに入力して、グループを追加できます。

**編集** – 選択したグループまたはデバイスのパラメータ(ベンダー、モデル、シリアル番号)の名前を変更できます。

**削除** – ボタンをクリックしたウィンドウの部分によって、選択したグループまたはデバイスを削除します。

**インポート** – テキストファイルからデバイスのリストをインポートします。テキストファイルからデバイスをインポートするには、正しい形式でなければなりません。

- 1行に1つのデバイスを記述します。
- 各デバイスの**ベンダー□モデル□シリアル番号**は必須であり、カンマで区切る必要があります。

> ✓ テキストファイルの内容の例を次に示します。
> ```
> Kingston,DT 101 G2,001CCE0DGRFC0371
> 04081-0009432,USB2.0 HD WebCam,20090101
> ```

**エクスポート** – デバイスのリストをファイルにエクスポートします。

[入力]ボタンを使用すると、現在接続されているすべてのデバイスの概要が表示されます。この情報には、デバイスタイプ、デバイスの製造元、モデル、シリアル番号(ある場合)などがあります。

スケジューラを使用して、ルールを含むデバイスコントロールグループをXMLファイルからインポートできます。詳細と段階的なガイドについては、ESETナレッジベース記事を参照してください。

## デバイスの追加

右側のウィンドウで追加をクリックし、デバイスを既存のグループに追加します。次の追加パラメーターは、さまざまなデバイスに合わせてルールを微調整するのに使用できます。すべてのパラメーターは大文字と小文字を区別し、ワイルドカード(*、?)をサポートします。

- **ベンダー** – ベンダー名またはIDによるフィルタリング。
- **モデル** – デバイスに付けられている名前。
- **シリアル番号** – 外部デバイスには通常独自のシリアル番号が付いています。CD/DVDの場合は、CDドライブではなく、そのメディアのシリアル番号があります。
- **説明** – 整理しやすくするためのデバイスの説明。

これらのパラメータが未定義の場合、ルールは照合時にこれらのフィールドを無視します。すべてのフィールドのフィルタリングパラメーターは大文字と小文字を区別し、ワイルドカード(疑問符(?)は1つの文字を表し、アスタリスク(*)は0文字以上の文字列を表します)をサポートします。

**OK**をクリックして変更を保存します。変更を保存せずに[**デバイスグループ**]を終了する場合は、[**キャンセル**]をクリックします。

デバイスグループを作成した後には、作成されたデバイスグループの新しいデバイスコントロールルールを追加し、実行するアクションを選択する必要があります。

デバイスのタイプによっては、適用されないアクション(権限)もあります。記憶装置タイプのデバイスの場合、4つのアクションすべてを使用できます。記憶装置以外のデバイスでは、これらのうち3つだけが適用可能です(たとえばBluetoothの場合、[**書き込みブロック**]アクションは適用できないので、許可かブロックだけになります)。

# ThreatSense

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

設定ウィンドウにアクセスするにはThreatSense技術を使用する任意のモジュール(下記を参照)の詳細

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

- リアルタイム検査
- アイドル状態検査
- スタートアップ検査の設定
- ドキュメント保護
- 電子メールクライアント保護
- Webアクセス保護
- コンピューターの検査

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、パラメーターを変更すると、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)。コンピューターの検査を除く全ての機能についてThreatSenseの既定のパラメーターを変更しないことをお勧めします。

# 検査するオブジェクト

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。

**システムメモリ** – システムメモリーを攻撃対象とするマルウェアを検査します。

**ブートセクタ/UEFI** – ブートセクターのマスターブートレコードにおけるマルウェアの存在を検査します。用語集のUEFIの詳細をお読みください

**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** – 拡張子ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACEなどがサポートされます。

**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(UPX, yoda, ASPack, FSGなど)のほかにも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次のとおりです。

**ヒューリスティック** – ヒューリスティックは、悪意のあるプログラムの活動を分析するアルゴリズムです。この技術の主な利点は、前には存在しなかったり、これまでの検出エンジンのバージョンで特定されていなかったりした悪意のあるソフトウェアを特定できる点です。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署名** – 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

駆除設定は、オブジェクト駆除中のESET Endpoint Antivirusの動作を決定します。

## 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。このThreatSense設定のセクションでは、検査するファイルの種類を指定します。

## その他

オンデマンドコンピューターの検査でThreatSenseエンジン設定を設定する場合は、**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。

**すべてのオブジェクトをログに記録する** – 検査ログには、自己解凍アーカイブで、感染していないファイルも含め、すべての検査されたファイルが表示されます(大量の検査ログデータが生成され、検査ログファイルのサイズが大きくなることがあります)。

**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

**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。

**オブジェクトの最大検査時間(秒)** – コンテナーオブジェクト(RAR/ZIPアーカイブや複数の添付ファイルを含む電子メールなど)のファイルを検査する最大時間の値を定義します。この設定は、スタンドアロンファイルには適用されません。ユーザー定義の値が入力され、その時間が経過すると、コンテナーオブジェクトの各ファイルの検査が完了したかどうかに関係なく、検査が可能な限りすぐに停止します。大きなファイルを含むアーカイブの場合、検査はアーカイブからファイルが展開された後すぐに停止します(たとえば、ユーザー定義変数が3秒で、ファイルの展開には5秒かかる場合)。アーカイブの残りの

ファイルは、その時間が経過した後は検査されません。大きなアーカイブを含む検査時間を制限するには、**最大オブジェクトサイズ**と**アーカイブのファイルの最大サイズ**を使用します(セキュリティ上のリスクの可能性があるため推奨されません)。既定値は無制限です。

### アーカイブ検査の設定

**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.

**アーカイブの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。最大値は3 GB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。

## 駆除レベル

目的の保護モジュールの駆除レベル設定を変更するには、**ThreatSense**(たとえば、**リアルタイムファイルシステム保護**)を展開し、ドロップダウンメニューから**駆除レベル**を選択します。

ThreatSenseには、次の修復(駆除など)レベルがあります。

### ESET Endpoint Antivirusでの修復

| 駆除レベル | 説明 |
|---|---|
| **常に検出を修正する** | ユーザー操作なしで、オブジェクトの駆除中に検出の修復を試みます。ごく一部の場合(システムファイルなど)で、検出を修正できない場合は、報告されたオブジェクトは元の場所に残されます。**常に検出を修正する**は、管理された環境で推奨される既定の設定です。 |
| **安全な場合は検出を修正する、そうでない場合は保持する** | ユーザー操作なしで、オブジェクトの駆除中に検出の修復を試みます。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、検出を修正できない場合は、報告されたオブジェクトは元の場所に残されます。 |
| **安全な場合は検出を修正する、そうでない場合は確認する** | オブジェクトの駆除中に検出の修復を試みます。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、エンドユーザーが修復アクション(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。 |
| **常にエンドユーザーに確認する** | 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、修復アクション(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。 |

## 検査対象外とするファイル拡張子

除外されたファイル拡張子はThreatSenseの一部です。除外されたファイル拡張子を設定するには、ThreatSense技術を使用するモジュールの詳細設定で**ThreatSense**をクリックします。

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。このThreatSense設定のセクションでは、検査するファイルの種類を指定します。

プロセス除外、HIPS除外、またはパフォーマンス除外と混同しないでください。

既定では、すべてのファイルが検査されます。スキャンから除外するファイルの一覧には、どの拡張子でも追加できます。

特定の種類のファイルをスキャンすると、特定の拡張子を使用するプログラムが適切に動作しなくなる場合は、ファイルの除外が必要になることがあります。たとえばMS Exchange Serverを使用しているときには、拡張子.edb.eml、および.tmpを除外すると良いでしょう。

新しい拡張子をリストに追加するには、**追加**をクリックします。空のフィールドに拡張子を(tmpなど)を入力して、**[OK]**をクリックします。[**複数の値を入力**]を選択すると、改行、カンマ、セミコロンで区切られた複数のファイル拡張子を追加できます(たとえば、区切り文字として、ドロップダウンから**セミコロン**を選択し、edb;eml;tmpを入力します)。
特殊記号?(疑問符)を使用できます。疑問符は任意の記号を表します(たとえば、?db)

Windowsオペレーティングシステムのファイルの正確な拡張子(該当する場合)を表示するには、**Windowsエクスプローラー** > **表示**(タブ)で**ファイル名の拡張子**チェックボックスをオンにします。

# 追加のTHREATSENSEパラメータ

これらの設定を編集するには、詳細設定 > **保護** > **リアルタイムファイルシステム保護** > **追加のThreatSenseパラメータ**を開きます。

## 新しく作成および変更されたファイルに適用する追加のThreatSenseパラメータ

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 Antivirus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。

## 実行したファイルに適用する追加のThreatSenseパラメータ

**ファイル実行時のアドバンスドヒューリスティック** – 既定では アドバンスドヒューリスティック はファイルの実行時に使用されます。有効にするときには、スマート最適化とESET LiveGrid®を有効にし、システムパフォーマンスへの影響を低減することを強くお勧めします。

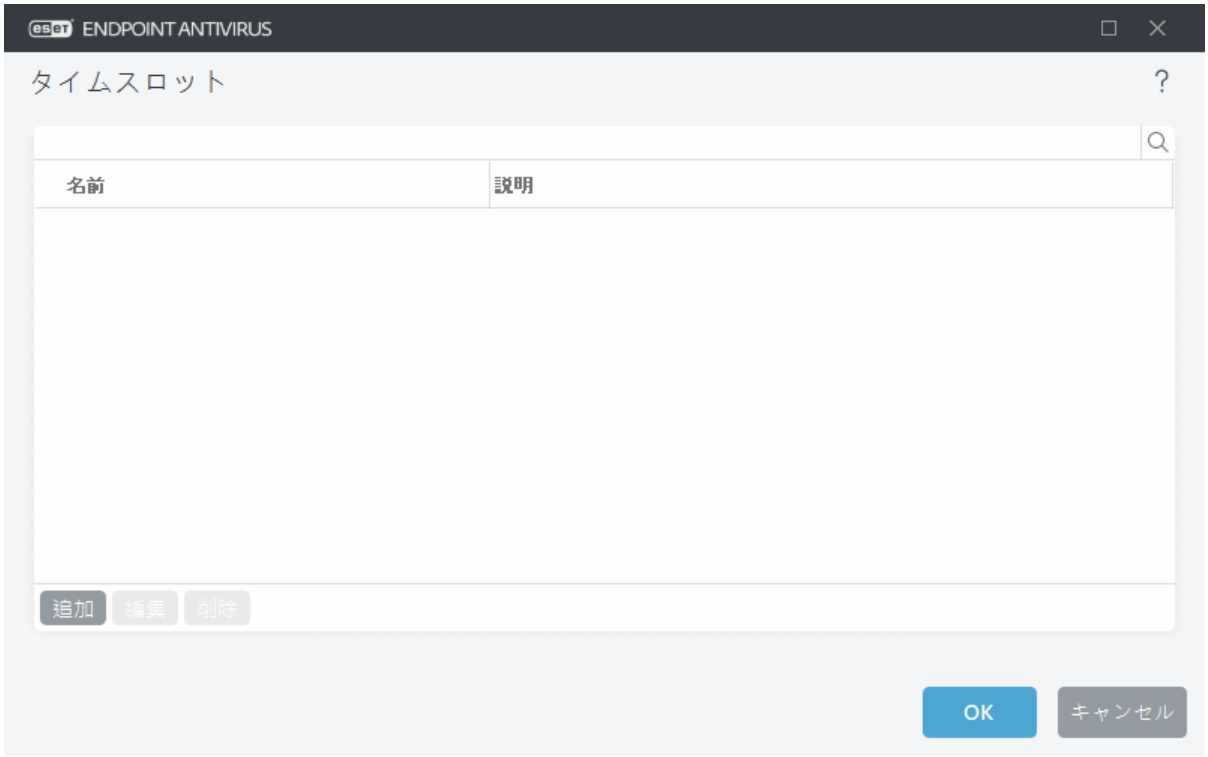
**リムーバブルメディアからのファイルの実行時のアドバンスドヒューリスティック** – コードがリムーバブルメディアから実行されることを許可する前に、高度なヒューリスティックが仮想環境でコードを列挙し、その動作を評価します。

# ツール

セキュリティを強化し、ESET Endpoint Antivirus管理を簡素化するのに役立つ機能の詳細設定は、詳細設定 > **ツール**で設定できます。

# タイムスロット

タイムスロットを作成し、**デバイスコントロール**に対してルールを割り当てることができます。**タイムスロット**設定は、詳細設定 > **ツール**にあります。これにより、一般的に使用されるタイムスロット(例:作業時間、週末など)を定義し、すべてのルールの時間範囲を再定義せずに、簡単に再利用できます。タイムスロットは、時間ベースの制御をサポートするルールの関連するタイプに適用できます。




タイムスロットを作成するには、次の手順を実行します。

1. **編集** > **追加**をクリックします。
2. タイムスロットの名前と**説明**を入力し、**追加**をクリックします。
3. タイムスロットの曜日と開始/終了時刻を指定するか、**終日**を選択します。
4. **OK**をクリックして確認します。

1つのタイムスロットは、曜日と時刻に基づいて、1つ以上の時間範囲とともに定義できます。タイムスロットが作成されると、デバイスコントロールルールエディタウィンドウの**適用期間**ドロップダウンメニューに表示されます。

# Microsoft Windows Update

Windowsアップデート機能は、悪意のあるソフトウェアからユーザーを保護する重要なコンポーネントです。そのためMicrosoft Windowsアップデートが使用可能になったら即座にインストールすることが欠かせませんESET Endpoint Antivirusは、指定されたレベルに従って、欠落したアップデートがあるとユーザーにそれを通知します。使用可能なレベルは次のとおりです。

- **アップデートしない** – 提示されるシステムアップデートはありません。
- **オプションのアップデート** – 低優先度以上とマークされているアップデートがダウンロード用として提示されます。
- **推奨アップデート** – 通常優先度以上とマークされているアップデートがダウンロード用として提示されます。
- **重要なアップデート** – 重要優先度以上とマークされているアップデートがダウンロード用として提示されます。
- **緊急のアップデート** – 緊急のアップデートのみがダウンロード用として提示されます。

変更内容を保存するには、[**OK**]をクリックします。アップデートサーバーでステータスの検証を行った後、システムのアップデートウィンドウが表示されます。そのため、システムアップデートの情報は、変更を保存した後、即座に使用できない場合があります。

# ダイアログウィンドウ - OSのアップデート

オペレーティングシステムのアップデートが利用可能な場合は、ESET Endpoint Antivirus Homeウィンドウに通知が表示されます。**詳細**をクリックし、システムアップデートウィンドウを開きます。

[システムアップデート]ウィンドウには、ダウンロードおよびインストールが可能なアップデートのリストが表示されます。アップデートタイプは、アップデートの名前の横に表示されます。

アップデート行をダブルクリックすると、アップデート情報ウィンドウと追加情報が表示されます。

**システムアップデートの実行**をクリックすると、すべての一覧のOSのアップデートをダウンロードしてインストールします。

# アップデート情報

[システムアップデート]ウィンドウには、ダウンロードおよびインストールが可能なアップデートのリストが表示されます。アップデートの優先レベルは、アップデートの名前の横に表示されます。

[**システムアップデートの実行**]をクリックして、オペレーティングシステムのアップデートのダウンロードおよびインストールを開始します。

任意のアップデート行を右クリックし、**情報の表示**をクリックすると、追加情報を含む新しいウィンドウが表示されます。

# ESET CMD

これは高度なecmdコマンドを有効にする機能です。コマンドライン(ecmd.exe)を使用して、設定をインポートおよびエクスポートできます。これまでは、GUIのみを使用して設定をエクスポート及びインポートすることが可能でしたESET Endpoint Antivirus設定を. *xml*ファイルにエクスポートできます。

ESET CMDを有効にすると、2つの認証方法を使用できます。

- **なし** – 認証なし。潜在的なリスクとなる未署名の設定のインポートが許可されるため、この方法は推奨されません。
- **[詳細設定パスワード]**-*.xml*ファイルから設定をインポートするときには、パスワードが必要です。このファイルを署名する必要があります(*.xml*設定ファイルの署名を参照してください)。アクセス設定で指定されたパスワードを、新しい設定をインポートする前に指定する必要があります。アクセス設定パスワードが有効ではないか、パスワードが一致しないか、*.xml*設定ファイルが署名されていない場合は、設定はインポートされません。

ESET CMDを有効にするとESET Endpoint Antivirus設定のエクスポート/インポートでコマンドラインを使用できます。手動で実行するか、自動化用のスクリプトを作成できます。

高度なecmdコマンドを使用するには、管理者権限で実行するか、**管理者として実行**を使用してWindowsコマンドプロンプト(cmd)を開く必要があります。さもなければ、「**Error executing command**」というメッセージが表示されます。また、設定のインポート時には、インポート先フォルダーが存在する必要があります。エクスポートコマンドは、ESET CMD設定がオフでも動作します。

高度なecmdコマンドはローカルでのみ実行できますecmdコマンドの一時停止は、ESET PROTECTを使用してクライアントタスクの**コマンドの実行**を使用した場合にのみ実行できます。

設定のエクスポートコマンド:
```
ecmd /getcfg c:\config\settings.xml
```
設定のインポートコマンド:
```
ecmd /setcfg c:\config\settings.xml
```

*.xml*設定ファイルの署名:

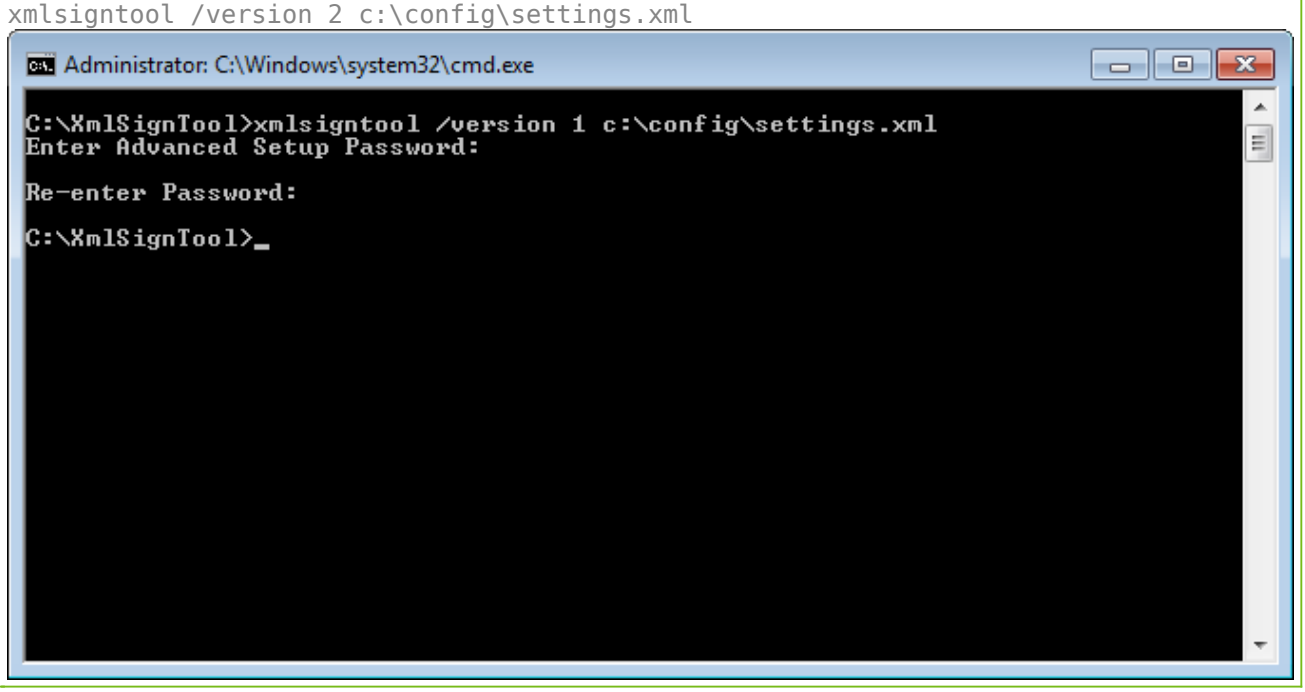
1. XmlSignTool実行ファイルをダウンロードします。
2. **管理者として実行**を使用してWindowsコマンドプロンプト(cmd)を開きます。
3. `xmlsigntool.exe`の保存場所に移動します。
4. コマンドを実行し、*.xml*設定ファイルに署名します。使用方法: `xmlsigntool /version 1|2 <xml_file_path>`

`/version`パラメーターの値は、ESET Endpoint Antivirusのバージョンによって異なります。バージョン7以降では、`/version 2`を使用します。

5. XmlSignToolで要求されたら、詳細設定 パスワードを入力します。*.xml*設定ファイルが署名されます。パスワード認証方法によってESET CMDを使用してESET Endpoint Antivirusの別のインスタンスでインポートするために使用できます。

エクスポートされた設定ファイルの署名コマンド:

```
xmlsigntool /version 2 c:\config\settings.xml
```




アクセス設定パスワードを変更し、古いパスワードで以前に署名された設定ファイルをインポートする場合は、現在のパスワードで.*xml*設定ファイルをもう一度署名する必要があります。これにより、インポート前にESET Endpoint Antivirusを実行する他のコンピューターでエクスポートせずに、古い設定ファイルを使用できます。

認証なしでESET CMDを有効にすることは推奨されません。これにより、署名されていない設定のインポートが可能になります。[詳細設定] > [**ユーザーインターフェイス**] > [**アクセス設定**]でパスワードを設定し、ユーザーによる無許可の修正を防止します。

**ecmdコマンドのリスト**

個別のセキュリティ機能は、ESET PROTECTクライアントタスク実行コマンドで有効にしたり、一時的に無効にしたりできます。コマンドはポリシー設定を上書きせず、一時停止した設定は、コマンドの実行後またはデバイスの再起動後に元の状態に戻されます。この機能を利用するには、同じ名前のフィールドで実行するコマンドラインを指定します。

以下の各セキュリティ機能のコマンドのリストを確認してください。

| セキュリティ機能 | Temporary Pauseコマンド | Enableコマンド |
|---|---|---|
| リアルタイムファイルシステム保護 | ecmd /setfeature onaccess pause | ecmd /setfeature onaccess enable |
| ドキュメント保護 | ecmd /setfeature document pause | ecmd /setfeature document enable |
| デバイスコントロール | ecmd /setfeature devcontrol pause | ecmd /setfeature devcontrol enable |
| プレゼンテーションモード | ecmd /setfeature presentation pause | ecmd /setfeature presentation enable |
| パーソナルファイアウォール | ecmd /setfeature firewall pause | ecmd /setfeature firewall enable |
| ネットワーク攻撃保護(IDS) | ecmd /setfeature ids pause | ecmd /setfeature ids enable |
| ボットネット保護 | ecmd /setfeature botnet pause | ecmd /setfeature botnet enable |
| Webコントロール | ecmd /setfeature webcontrol pause | ecmd /setfeature webcontrol enable |
| Webアクセス保護 | ecmd /setfeature webaccess pause | ecmd /setfeature webaccess enable |
| 電子メールクライアント保護 | ecmd /setfeature email pause | ecmd /setfeature email enable |

| セキュリティ機能 | Temporary Pauseコマンド | Enableコマンド |
|---|---|---|
| 電子メールクライアント迷惑メール対策 | ecmd /setfeature antispam pause | ecmd /setfeature antispam enable |
| フィッシング対策機能 | ecmd /setfeature antiphishing pause | ecmd /setfeature antiphishing enable |

# リモート監視と管理

リモート監視と管理(RMM)は、管理サービスプロバイダーがアクセスできるローカルにインストールされたエージェントを使用して、ソフトウェアシステムを監視および制御するプロセスです。

## ERMM - RMM向けのESETプラグイン

- 既定のESET Endpoint Antivirusインストールには、次のディレクトリ内のEndpointアプリケーションにある`ermm.exe`ファイルが含まれます。
  *C:\Program Files\ESET\ESET Security\ermm.exe*
- `ermm.exe`は、エンドポイント製品の管理とRMMプラグインとの通信を容易にするために設計されたコマンドラインユーティリティです。
- `ermm.exe`はRMMプラグインとデータを交換します。これはRMMサーバーにリンクされたRMMエージェントと通信します。既定ではESET RMMツールは無効です。

### その他のリソース

- ERMMコマンドライン
- ERMM JSONコマンドのリスト

- リモート監視と管理をアクティブ化する方法ESET Endpoint Antivirus

## サードパーティRMMソリューション向けのESET Direct Endpoint Managementプラグイン

サードパーティーのサーバーではRMMサーバーはサービスとして実行されています。詳細については、次のESET Direct Endpoint Managementオンラインユーザーガイドを参照してください。

- ESET Direct Endpoint Managementプラグイン(ConnectWise Automate版)
- ESET Direct Endpoint Managementプラグイン(DattoRMM版)
- ESET Direct Endpoint Managementプラグイン(Solarwinds N-Central版)
- ESET Direct Endpoint Management (NinjaRMM版)

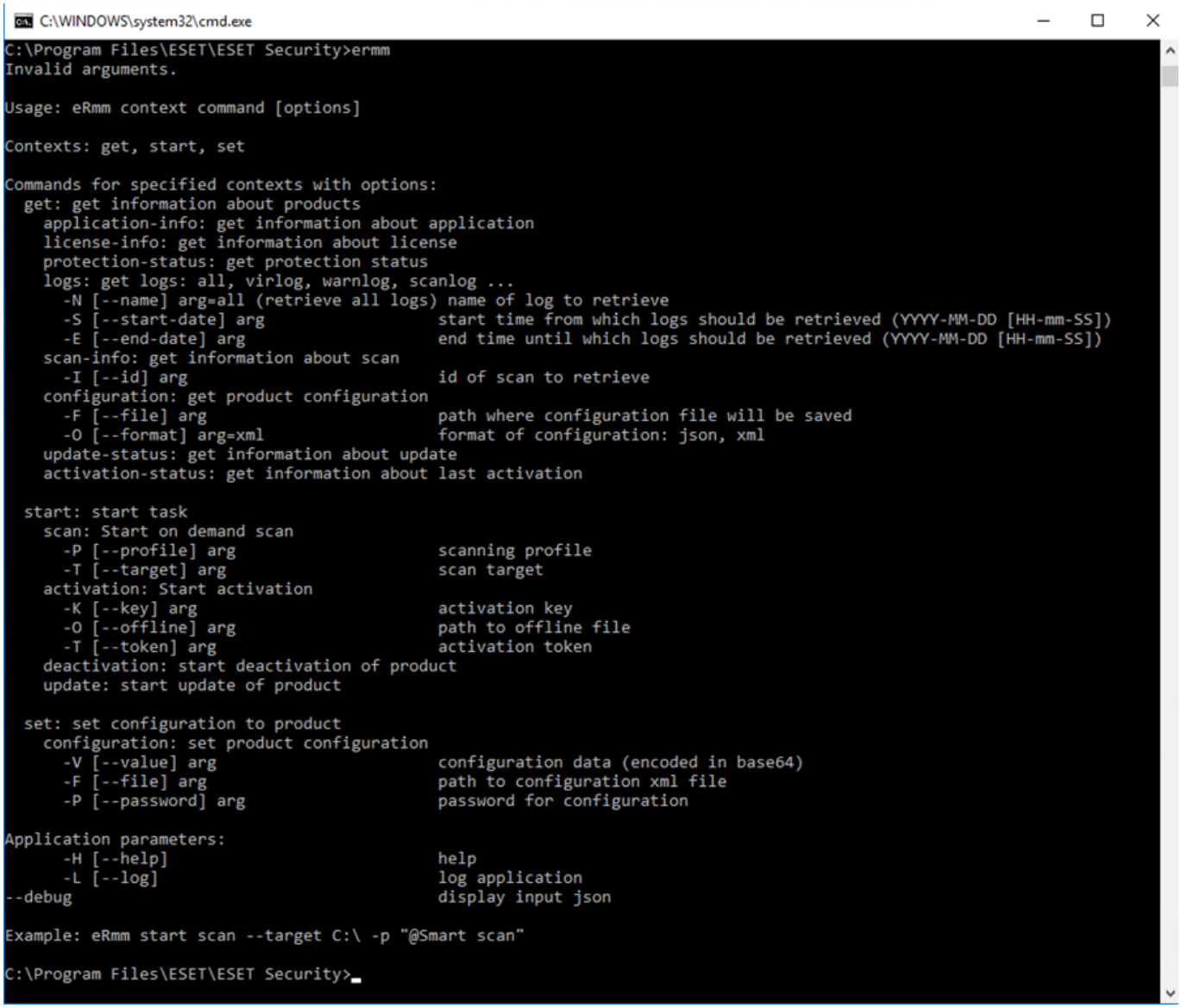
# ERMMコマンドライン

リモート監視管理はコマンドラインインターフェースを使用して実行されます。既定のESET Endpoint Antivirusインストールでは、*c:\Program Files\ESET\ESET Security*ディレクトリ内のエンドポイントアプリケーションにermm.exeファイルが含まれます。

管理者としてコマンドプロンプト(cmd.exe)を実行し、上記のパスに移動します(コマンドプロンプトを開き、キーボードのWindowsボタン+ Rを押し、実行ウィンドウにcmdと入力し、Enterを押します)。

コマンド構文は次のとおりです。`ermm context command [options]`

ログパラメーターは大文字と小文字を区別します。




ermm.exeは次の3つの基本コンテキストを使用します。取得、開始、設定。以下の表では、コマンド構文の例を示します。コマンド列のリンクをクリックすると、詳細オプション、パラメーター、および使用方法の例が表示されます。コマンドの実行が成功した後、出力部(結果)が表示されます。入力部分を表示するには、コマンドに`--debug`パラメータを追加します。

| コンテキスト | コマンド | 説明 |
|---|---|---|
| **get** | | **製品情報の取得** |
| | application-info | 製品情報の取得 |
| | license-info | ライセンス情報の取得 |
| | protection-status | 保護の状態の取得 |
| | logs | ログの取得 |
| | scan-info | 実行中の検査に関する情報の取得 |
| | configuration | 製品設定の取得 |
| | update-status | アップデートに関する情報の取得 |
| | activation-status | 前回のアクティベーションに関する情報の取得 |
| **start** | | **タスクの開始** |

| コンテキスト | コマンド | 説明 |
|---|---|---|
| | scan | オンデマンド検査を開始 |
| | activation | 製品のアクティベーションを開始 |
| | deactivation | 製品のアクティベーション解除を開始 |
| | update | 製品のアップデートを開始 |
| **set** | | **製品のオプションを設定** |
| | configuration | 構成を製品に設定 |

すべてのコマンドの出力結果では、表示される最初の情報は結果IDです。結果情報の詳細な説明については、以下のIDの表を確認してください。

| エラーID | エラー | 説明 |
|---|---|---|
| **0** | Success | |
| **1** | Command node not present | 「コマンド」ノードが入力jsonに存在しない |
| **2** | Command not supported | このコマンドはサポートされていません |
| **3** | General error executing the command | コマンドの実行エラー |
| **4** | Task already running | 要求されたタスクはすでに実行中であり、開始されています |
| **5** | Invalid parameter for command | 不正なユーザー入力 |
| **6** | Command not executed because it's disabled | RMMは詳細設定で有効ではないか、管理者として起動します |

# ERMM JSONコマンドのリスト

- get protection-status
- get application-info
- get license-info
- get logs
- get activation-status
- get scan-info
- get configuration
- get update-status
- start scan
- start activation
- start deactivation
- start update
- set configuration

# get protection-status

Get the list of application statuses and the global application status

### コマンドライン

```
ermm.exe get protection-status
```

### パラメータ

None

### 例

**call**

```
{
"command":"get_protection_status",
"id":1,
"version":"1"
}
```

**result**

```
{
"id":1,
"result":{
"statuses":[{
"id":"EkrnNotActivated",
"status":2,
"priority":768,
"description":"Product not activated"
}],
"status":2,
"description":"Security alert"
},
"error":null
}
```

## get application-info

Get information about the installed application

### コマンドライン

```
ermm.exe get application-info
```

### パラメータ

None

### 例

**call**

```
{
"command":"get_application_info",
"id":1,
"version":"1"
}
```

**result**

```
{
"id":1,
"result":{
"description":"ESET Endpoint Antivirus",
"version":"6.6.2018.0",
"product":"eea",
"lang_id":1033,
"modules":[{
"id":"SCANNER32",
"description":"Detection engine",
"version":"15117",
"date":"2017-03-20"
},{
"id":"PEGASUS32",
"description":"Rapid Response module",
"version":"9734",
"date":"2017-03-20"
},{
"id":"LOADER32",
"description":"Update module",
"version":"1009",
"date":"2016-12-05"
},{
"id":"PERSEUS32",
"description":"Antivirus and antispyware scanner module",
"version":"1513",
"date":"2017-03-06"
},{
"id":"ADVHEUR32",
"description":"Advanced heuristics module",
"version":"1176",
"date":"2017-01-16"
},{
"id":"ARCHIVER32",
"description":"Archive support module",
"version":"1261",
"date":"2017-02-22"
},{
"id":"CLEANER32",
"description":"Cleaner module",
"version":"1132",
"date":"2017-03-15"
},{
"id":"SYSTEMSTATUS32",
"description":"ESET SysInspector module",
"version":"1266",
"date":"2016-12-22"
},{
"id":"TRANSLATOR32",
"description":"Translation support module",
"version":"1588B",
"date":"2017-03-01"
},{
"id":"HIPS32",
"description":"HIPS support module",
"version":"1267",
"date":"2017-02-16"
},{
"id":"PROTOSCAN32",
"description":"Internet protection module",
"version":"1300",
"date":"2017-03-03"
},{
"id":"DBLITE32",
"description":"Database module",
"version":"1088",
"date":"2017-01-05"
},{
"id":"CONFENG32",
"description":"Configuration module (33)",
"version":"1496B",
"date":"2017-03-17"
},{
"id":"IRIS32",
"description":"LiveGrid communication module",
"version":"1022",
"date":"2016-04-01"
},{
"id":"SAURON32",
"description":"Rootkit detection and cleaning module",
"version":"1006",
"date":"2016-07-15"
},{
"id":"SSL32",
"description":"Cryptographic protocol support module",
"version":"1009",
"date":"2016-12-02"
}
},
"error":null
}
}
```

# get license-info

Get information about the license of the product

## コマンドライン

```
ermm.exe get license-info
```

## パラメータ

None

## 例

**call**

```
{
"command":"get_license_info",
"id":1,
"version":"1"
}
```

**result**

```
{
"id":1,
"result":{
"type":"NFR",
"expiration_date":"2020-12-31",
"expiration_state":"ok",
"public_id":"3XX-7ED-7XF",
"seat_id":"6f726793-ae95-4e04-8ac3-e6a20bc620bf",
"seat_name":"M"
},
"error":null
}
```

# get logs

Get logs of the product

## コマンドライン

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-
date "2017-04-04 12-00-00"
```

## パラメータ

| Name | Value |
|---|---|
| **name** | { all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve |
| start-date | start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS]) |
| end-date | end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS]) |

## 例

**call**

```
{
"command":"get_logs",
"id":1,
"version":"1",
"params":{
"name":"warnlog",
"start_date":"2017-04-04 06-00-00",
"end_date":"2017-04-04 12-00-00"
}
}
```

**result**

```
{
"id":1,
"result":{
"warnlog":{
"display_name":"Events",
"logs":[{
"Time":"2017-04-04 06-05-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15198 (20170404).",
"UserData":""
},{
"Time":"2017-04-04 11-12-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15199 (20170404).",
"UserData":""
}]
}
},
"error":null
}
```

# get activation-status

Get information about the last activation. Result of status can be { success, running, failure }

## コマンドライン

```
ermm.exe get activation-status
```

## パラメータ

None

## 例

**call**

```
{
"command":"get_activation_status",
"id":1,
"version":"1"
}
```

**result**

```
{
"id":1,
"result":{
"status":"success"
},
"error":null
}
```

# get scan-info

実行中の検査に関する情報を取得します。

## コマンドライン

```
ermm.exe get scan-info
```

## パラメータ

なし

## 例

**call**

```
{
"command":"get_scan_info",
"id":1,
"version":"1"
}
```

**結果**

```
{
"id":1,
"result":{
"scan-info":{
"scans":[{
"scan_id":65536,
"timestamp":272,
"state":"finished",
"pause_scheduled_allowed":false,
"pause_time_remain":0,
"start_time":"2017-06-20T12:20:33Z",
"elapsed_tickcount":328,
"exit_code":0,
"progress_filename":"Operating memory",
"progress_arch_filename":"",
"total_object_count":268,
"infected_object_count":0,
"cleaned_object_count":0,
"log_timestamp":268,
"log_count":0,
"log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
"username":"test-PC\\test",
"process_id":3616,
"thread_id":3992,
"task_type":2
}],
"pause_scheduled_active":false
}
},
"error":null
}
```


# get configuration

Get the product configuration. Result of status may be { success, error }

## コマンドライン

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

## パラメータ

| Name | Value |
|---|---|
| file | the path where the configuration file will be saved |
| format | format of configuration: json, xml. Default format is xml |

## 例

| call |
|---|

```
{
"command":"get_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml"
}
}
```

**result**

```
{
"id":1,
"result":{
"configuration":"PD94bWwgdmVyc2lvbj0iMS4w=="
},
"error":null
}
```

# get update-status

Get information about the update. Result of status may be { success, error }

## コマンドライン

```
ermm.exe get update-status
```

## パラメータ

None

## 例

**call**

```
{
"command":"get_update_status",
"id":1,
"version":"1"
}
```

**result**

```
{
"id":1,
"result":{
"last_update_time":"2017-06-20 13-21-37",
"last_update_result":"error",
"last_successful_update_time":"2017-06-20 11-21-45"
},
"error":null
}
```

# start scan

Start scan with the product

## コマンドライン

```
ermm.exe start scan --profile "profile name" --target "path"
```

## パラメータ

| Name | Value |
|---|---|
| profile | Profile name of On-demand computer scan defined in product |
| target | Path to be scanned |

## 例

**call**

```
{
"command":"start_scan",
"id":1,
"version":"1",
"params":{
"profile":"Smart scan",
"target":"c:\\"
}
}
```

**result**

```
{
"id":1,
"result":{
"task_id":458752
},
"error":null
}
```

# start activation

Start activation of product

## コマンドライン

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

## パラメータ

| Name | Value |
|---|---|
| key | Activation key |
| offline | Path to offline file |

## 例

**call**

```
{
"command":"start_activation"
"id":1,
"version":"1",
"params":{
"key":"XXXX-XXXX-XXXX-XXXX-XXXX"
}
}
```

**result**

```
{
"id":1,
"result":{
},
"error":null
}
```

# start deactivation

Start deactivation of the product

## コマンドライン

```
ermm.exe start deactivation
```

## パラメータ

None

## 例

**call**

```
{
"command":"start_deactivation",
"id":1,
"version":"1"
}
```

**result**

```
{
"id":1,
"result":{
},
"error":null
}
```

# start update

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

## コマンドライン

```
ermm.exe start update
```

## パラメータ

None

## 例

**call**

```
{
"command":"start_update",
"id":1,
"version":"1"
}
```

**result**

```
{
"id":1,
"result":{
},
"error":{
"id":4,
"text":"Task already running."
}
}
```

# set configuration

Set configuration to the product. Result of status may be { success, error }

## コマンドライン

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

## パラメータ

| Name | Value |
|---|---|
| file | the path where the configuration file will be saved |
| password | password for configuration |
| value | configuration data from the argument (encoded in base64) |

## 例

**call**

```
{
"command":"set_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml",
"password": "pass"
}
}
```

**result**

```
{
"id":1,
"result":{
},
"error":null
}
```

# ライセンス間隔チェック

ESET Endpoint Antivirusは自動的にESETライセンスサーバーに接続する必要があります。ESETライセンスサーバーへの接続数は、詳細設定 > **ツール** > **ライセンス**で制限できます。既定では、**間隔チェック**は**自動**に設定され、接続は1時間ごとに数回確立されます。ネットワークトラフィックが増大した場合には、**間隔チェック**を**制限**に変更すると、負荷が低減されます。**制限**が選択されると、ESET Endpoint Antivirusは1日に1回またはコンピューターが再起動するときにのみライセンスサーバーを確認します。

**間隔チェック**設定が**制限**に設定されている場合は、ESET HUB/ESET MSP Administrator経由で実行されたすべてのライセンス関連の変更がESET Endpoint Antivirusに適用されるまでに最大で1日かかる場合があります。

# ログファイル

ESET Endpoint Antivirusのログ設定は、詳細設定 > **ツール** > **ログファイル**でアクセスできます。[ログ]セクションでは、ログの管理方法を定義することができます。ハードディスクの容量を節約するために、古いログは自動的に削除されます。ログファイルの次のオプションを指定することができます。

**ログに記録する最小レベル** – ログに記録するイベントの最低詳細レベルを指定します。

- **診断** – 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をログに記録します。
- **情報** – 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。
- **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。
- **エラー** – 「ファイルのダウンロード中にエラーが発生しました」といったエラーや重大なエラーを記録します。
- **重大** – 重大なエラー(ウイルス対策保護の開始エラーなど)のみが表示されます。

**診断**の詳細レベルを選択すると、すべてのブロックされた接続が記録されます。

[**次よりも古いレコードを削除(日数)**]フィールドに指定された日数を経過したログエントリは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。

[**最適化**]をクリックすると、ログファイルの最適化が開始します。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。

**テキスト方式を有効にする**をオンにすると、ログファイルとは別のファイル形式でログを保存できます。

- **保存先のフォルダ** – ログファイルが保存されるディレクトリを選択します(テキスト/CSVのみ)。パスをコピーするか、[**クリア**]をクリックして別のディレクトリを選択します。各ログセクションには定義済みのファイル名を使用した独自のファイル(例: プレーンテキストファイル形式でログを保存する場合は、ログファイルの**検出された脅威**セクションは*virlog.txt*)があります。
- **タイプ - テキスト**ファイル形式を選択する場合は、ログがテキストファイルに保存されます。データはタブ区切りです。同じことがカンマ区切りの**CSV**ファイル形式にも当てはまります。**イベント**を選択すると、ファイルではなくWindowsイベントログに、ログが保存されます(コントロールパネルのイベントビューアで表示できます)。
- **全てのログファイルを削除 - [タイプ]**ドロップダウンメニューで現在選択されているすべての保存済みログが消去されます。ログ削除の成功に関する通知が表示されます。

**監査ログでの構成変更の追跡を有効にする** – 各構成変更について通知します。詳細については、監査ログを参照してください。

> 問題をより迅速に解決できるように、コンピューターからログを提供するように依頼される場合があります。ESET Log Collectorを使用すると、必要な情報を簡単に収集できます。ESET Log Collectorの詳細については、ESETナレッジベース記事を参照してください。

# プレゼンテーションモード

プレゼンテーションモードは、ソフトウェアを中断せずに使用し、ポップアップウィンドウを表示せず、CPUの使用量を最小化する必要があるユーザー向けの機能です。プレゼンテーションモードは、ウイルス対策アクティビティによって中断されてはならないプレゼンテーション中に使用することもできます。この機能を有効にすると、すべてのポップアップウィンドウが無効になり、スケジューラーの活動は完全に停止されます。システムの保護は引き続きバックグラウンドで実行されますが、ユーザーの操作を必要としません。

プログラムのメインウィンドウの**設定 > コンピューター**で  をクリックするか、**プレゼンテーションモード**の横の  をクリックして、プレゼンテーションモードを有効または無効にできます。プレゼンテーションモードを有効にすると、潜在的なセキュリティリスクが発生するため、タスクバーの保護の状態アイコンがオレンジになり、警告が表示されます。この警告はメインプログラムウィンドウでも確認でき、**プレゼンテーションモードがアクティブです**がオレンジで表示されます。

詳細設定 > **ツール > プレゼンテーションモード**で**アプリケーションを全画面モードで実行中の場合自動的にプレゼンテーションモードを有効にする**をアクティベーションすると、アプリケーションを全画面モードで起動するたびに、プレゼンテーションモードが開始され、アプリケーションが終了すると停止します。

**次の時間が経過した後にプレゼンテーションモードを自動的に無効にする**をアクティベーションし、プレゼンテーションモードが自動的に無効になる時間を定義します。

# 診断

診断はESETプロセスのアプリケーションクラッシュダンプ(ekrnなど)を提供します。アプリケーションがクラッシュすると、ダンプが生成されます。これを使用して、開発者は各種ESET Endpoint Antivirusの問題をデバッグおよび修正できます。

**ダンプの種類**の横のドロップダウンメニューをクリックし、3つの使用可能なオプションのいずれかを選択します。

- **メモリダンプを生成しない**をクリックすると、この機能を無効にします。
- **ミニダンプ**（既定）– アプリケーションが不意にクラッシュした理由を特定するのに役立つ最低限の有用な情報を記録します。この種類のダンプファイルは、領域が限られているときに便利です。ただし、含まれる情報が限られるため、問題の発生時に実行されていたスレッドがエラーの直接の原因ではない場合、ファイルを解析しても原因を判別できない場合があります。
- **完全** – アプリケーションが不意に停止した場合に、システムメモリの全内容が記録されます。完全なメモリーダンプには、メモリーダンプが収集されたときに実行されていたプロセスのデータが含まれます。

**保存先のフォルダー** – クラッシュ時、ダンプが作成されるディレクトリーです。

**ダンプファイルの保存フォルダを開く** – このディレクトリーを新しい *Windows Explorer* ウィンドウで開く場合は、[**開く**]をクリックします。

**診断ダンプの作成** - [**作成**]をクリックすると、[**ターゲットディレクトリ**]に診断ダンプを作成します。

## 詳細ログ

**コンピュータースキャナー詳細ログを有効にする** – コンピューターの検査またはリアルタイムファイルシステム保護によるファイルとフォルダーの検査中に発生するすべてのイベントを記録します。

**デバイスコントロール詳細ロギングを有効にする** – デバイスコントロールで発生するすべてのイベントを記録します。これにより、開発者はデバイスコントロールに関連する問題を診断および修正できます。

**Direct Cloud詳細ログを有効にする** – 製品とDirect Cloudサーバー間のすべての製品通信を記録します。

**ドキュメント保護詳細ログを有効にする** – ドキュメント保護で発生するすべてのイベントを記録し、診断と問題解決ができます。

**電子メールクライアント保護詳細ログを有効にする** – 電子メールクライアント保護と電子メールクライアントプラグインで発生するすべてのイベントを記録し、診断と問題解決ができます。

**カーネル詳細ロギングを有効にする**-ESETカーネルサービス(ekrn)で発生するすべてのイベントを記録し、問題の診断と解決を許可します。

**ライセンス詳細ロギングを有効にする** – ESETアクティベーションおよびライセンスサーバーとのすべての製品の通信を記録します。

**メモリ追跡を有効にする** – 開発者がメモリリークを診断できるようにすべてのイベントを記録します。

**ネットワーク保護詳細ロギングを有効にする**- PCAP形式でファイアウォール経由のすべてのネットワークデータ転送を記録します。これによって、開発者はファイアウォール関連の問題を診断および修正できます。

**ネットワークトラフィックスキャナー詳細ログを有効にする** – ネットワークトラフィックスキャナーを通過するすべてのデータを、PCAP形式で記録するので、開発者がネットワークトラフィックスキャナーに関連する問題を診断および修正するのに役立ちます。

**オペレーティングシステム詳細ログを有効にする** – 実行中のプロセス、CPUアクティビティ、ディスク処理などのオペレーティングシステムに関する追加情報が収集されます。これにより、開発者は、オペレーティングシステムで実行中のESET製品に関連する問題を診断および修正できます。

**プッシュメッセージング詳細ログを有効にする** – プッシュメッセージング中に発生するすべてのイベントを記録し、診断と問題解決を許可します。

**リアルタイムファイルシステム保護詳細ログを有効にする** – リアルタイムファイルシステム保護で発生するすべてのイベントを記録し、診断と問題解決ができます。

**アップデートエンジン詳細ロギングを有効にする** – アップデート処理中に発生するすべてのイベントを記録します。これにより、開発者はアップデートエンジンに関連する問題を診断および修正できます。

**脆弱性およびパッチ管理の詳細ログを有効にする** - 脆弱性およびパッチ管理ですべてのイベントを記録します。この設定は、脆弱性およびパッチ管理がお使いの環境で有効になっている(ESET PROTECT Cloudで有効になっている)場合にのみ表示されます。

ログファイルは*C:\ProgramData\ESET\ESET Security\Diagnostics*にあります。

# テクニカルサポート

ESET Endpoint AntivirusからESETテクニカルサポートに問い合わせるときには、システム構成データを送信できます。**システム構成データの送信**ドロップダウンから**常に送信**を選択するか、**送信する前に確認**を選択してデータを送信する前に確認するようにします。

# 接続

特定のネットワークでは、コンピューター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。プロキシサーバーを使用している場合は、次の設定を定義する必要があります。定義しない場合、ESET Endpoint Antivirusとそのモジュールは自動的に更新されません。ESET Endpoint Antivirusでは、詳細設定の2つの異なるセクションにプロキシサーバー設定があります。

グローバルプロキシサーバー設定は、詳細設定 > **接続** > **プロキシサーバー**から設定できます。プロキシサーバーをこのレベルで指定すると、ESET Endpoint Antivirusの全ての全体的なプロキシサーバー設定が指定されることになります。ここで設定するパラメータは、インターネットへの接続を必要とする全てのモジュールで使用されます。

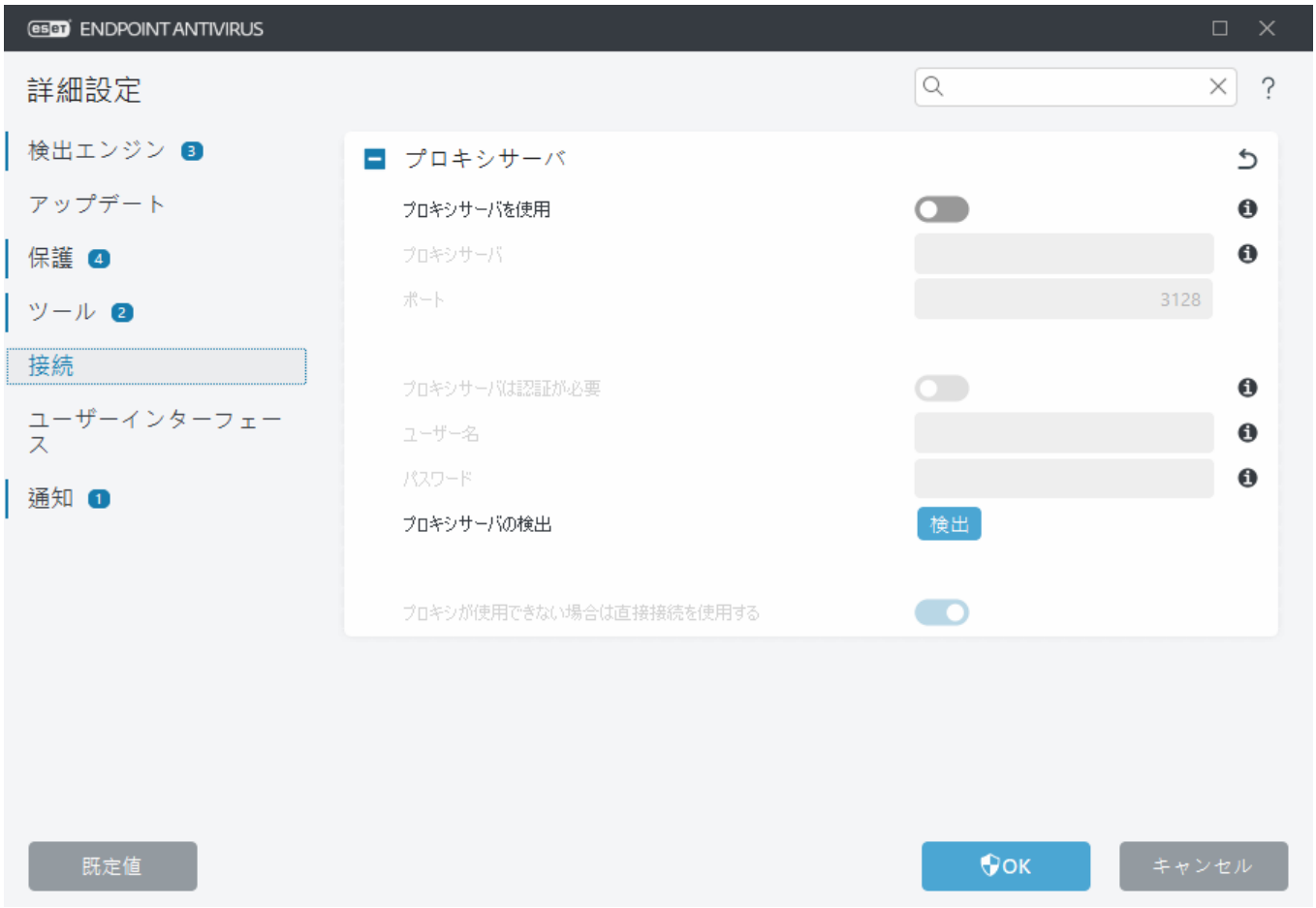
グローバルプロキシサーバー設定を指定するには、**プロキシサーバーを使用する**を有効にし、**プロキシサーバー**のアドレスとプロキシサーバーの**ポート**番号を入力します。

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**を該当のフィールドに入力します。**プロキシサーバの検出**をクリックすると、自動的にプロキシサーバー設定が検出されて取り込まれます。オペレーティングシステムのプロキシ設定を見つけるには、**Windows + I**ショートカットキーを押して、**ネットワークとインターネット** > **プロキシ**をクリックします。ESET Endpoint AntivirusはInternet ExplorerまたはGoogle Chromeのインターネットオプションで指定されたパラメーターをコピーします。

**プロキシサーバー**設定には、手動でユーザー名とパスワードを入力する必要があります。

**プロキシが使用できない場合は直接接続を使用する** - ESET Endpoint Antivirusがプロキシを使用して接続するように設定され、プロキシに接続できない場合は、ESET Endpoint Antivirusはプロキシをバイパスし、直接ESETサーバーと通信します。

プロキシサーバー設定は、詳細設定 > **アップデート** > **プロファイル** > **アップデート** > **接続オプション**で、**プロキシモード**ドロップダウンメニューから**グローバルプロキシサーバーを使用して接続する**を選択しても設定できます。この設定はアップデートにのみ適用されます。リモートロケーションからモジュールアップデートを受信するノート型コンピューターにお勧めします。詳細については、アップデートの詳細設定を参照してください。




# ユーザーインターフェイス

プログラムのグラフィカルユーザーインターフェース(GUI)の動作を設定するには、詳細設定 > **ユーザーインターフェース**を開きます。

ユーザーインタフェース要素詳細設定画面では、プログラムの表示状態やエフェクトを調整できます。

セキュリティソフトウェアのセキュリティを最大限に高めるには、アクセス設定ツールを使用してパスワードによる設定の保護を実現し、アンインストールや不正な変更を防止します。

システム通知、検出アラート、およびアプリケーションステータスの動作を設定するには、通知セクションを参照してください。

アプリケーションでの作業中に、ポップアップウィンドウ、スケジュールされたタスク、およびプロセッサやRAMに負荷を与えるコンポーネントなどによって中断されたくないユーザーにとっては、プレゼンテーションモードが便利です。

ESET Endpoint Antivirusユーザーインターフェースを最小化する方法も参照してください(管理された環境で有用です)。

# ユーザーインタフェース要素

ESET Endpoint Antivirusのユーザーインターフェースの設定オプションを使用すると、各自のニーズに合わせて作業環境を調整することができます。これらの設定オプションには、**[詳細設定]** (F5) > **[ユーザーインタフェース]** > **[ユーザーインタフェース要素]**ブランチからアクセスします。

**[ユーザーインタフェース要素]**セクションでは、作業環境を調整できます。**[起動モード]**ドロップダウンメニューを使用して、次のGUI起動モードを選択します。

**完全メモリダンプ** – 完全なGUIが表示されます。

**最低** - GUIが実行中ですが、通知のみがユーザーに表示されます。

**手動** – GUIはログオン時に自動的に起動しません。ユーザーは手動で起動できます。

**サイレント** – 通知またはアラートは表示されません。GUIは管理者のみが起動できます。このモードは、管理された環境またはシステムリソースを節約する必要がある場合に有効です。

> 最低GUI起動モードを選択してコンピューターが再起動すると、通知が表示されますがGUIは表示されません。完全GUIモードに戻すには、管理者としてスタートメニューの**[すべてのプログラム]** > **[ESET]** > ESET Endpoint Antivirusの下にあるGUIを実行するか、ポリシーを使用してESET PROTECT経由で実行します。

**色モード** – ドロップダウンメニューからESET Endpoint Antivirus GUIの配色を選択します。

- **システム色と同じ** – オペレーティングシステム設定に基づいてESET Endpoint Antivirusの配色を設定します。
- **暗い** - ESET Endpoint Antivirusには暗い配色(ダークモード)があります。
- **明るい** - ESET Endpoint Antivirusには標準の明るい配色があります。

> メインプログラムウィンドウの右上のESET Endpoint Antivirus GUIの配色を選択することもできます。

ESET Endpoint Antivirusのスプラッシュウィンドウが表示されないようにするには、[**起動時にスプラッシュウィンドウを表示する**]のチェックを外します。

スキャン中に脅威が発見されたりスキャンが終了したなどの重要なイベントが発生したときESET Endpoint Antivirusがサウンドを再生するようにするには、[**サウンドシグナルを使用する**]を選択します。

**コンテキストメニューに統合する** - ESET Endpoint Antivirusのコントロール要素をコンテキストメニューに統合します。

## ライセンス情報

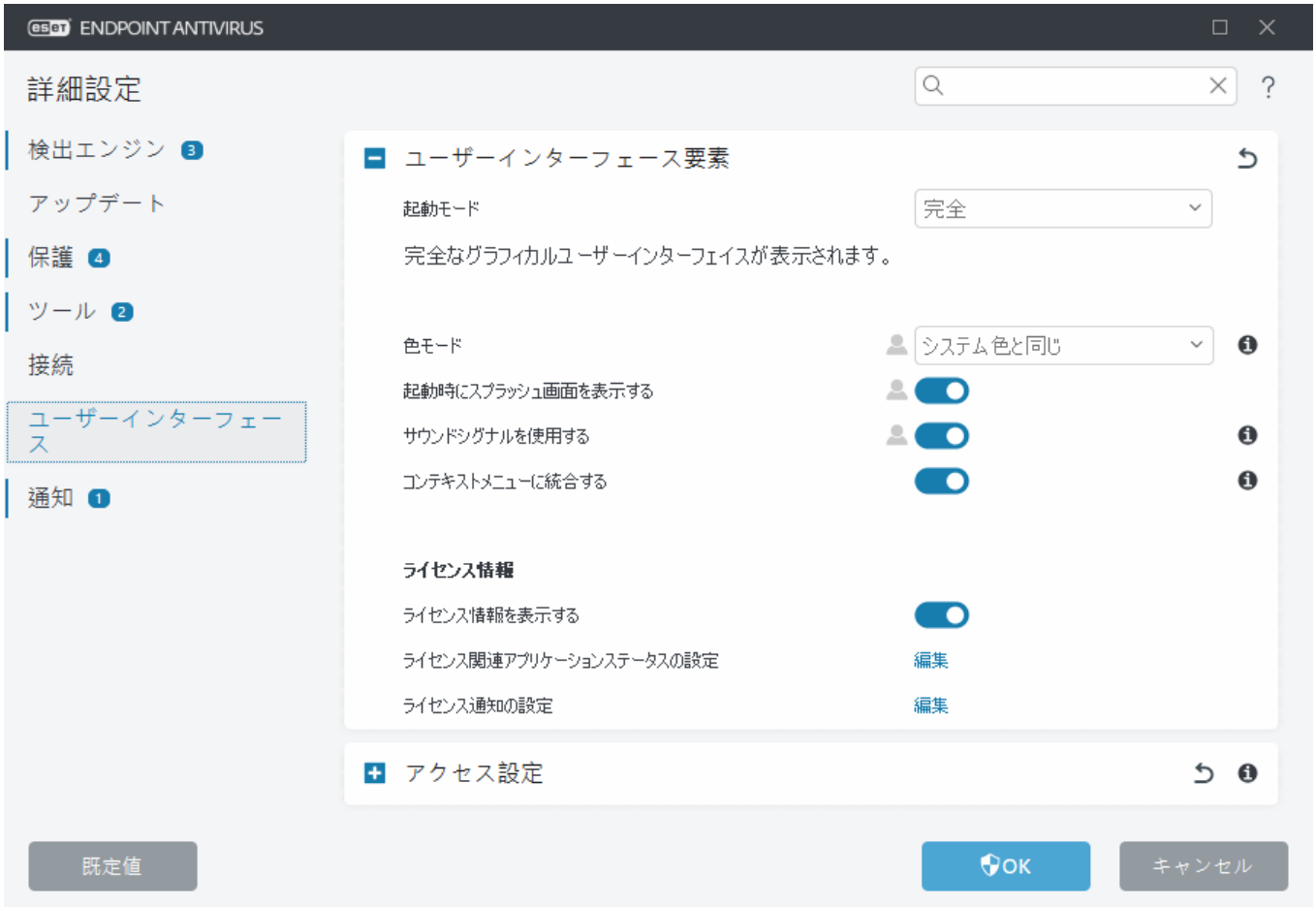
**ライセンス情報を表示する**– 無効にすると、**[保護ステータス]**および**[ヘルプとサポート]**画面のライセンス有効期限が非表示になります。

**ライセンス関連のアプリケーションステータスの設定** – ライセンス関連のアプリケーションステータスの一覧が開きます。

**ライセンスメッセージと通知を表示する** – 無効にすると、ライセンスが期限切れの場合にのみ、通知

とメッセージが表示されます。

ライセンス情報設定は適用されますがMSPライセンスでアクティベーションされたESET Endpoint Antivirusでのみアクセスできます。




# アクセス設定

ESET Endpoint Antivirusの設定はセキュリティポリシーの非常に重要な部分です。許可なく変更が行われた場合は、システムの安定性と保護が危険にさらされる可能性があります。認証されていないユーザーによる変更を防ぐためにESET Endpoint Antivirusの設定パラメーターおよびアンインストールをパスワードで保護することができます。アクセス設定は、詳細設定 > **ユーザーインターフェース** > **アクセス設定**で設定できます。

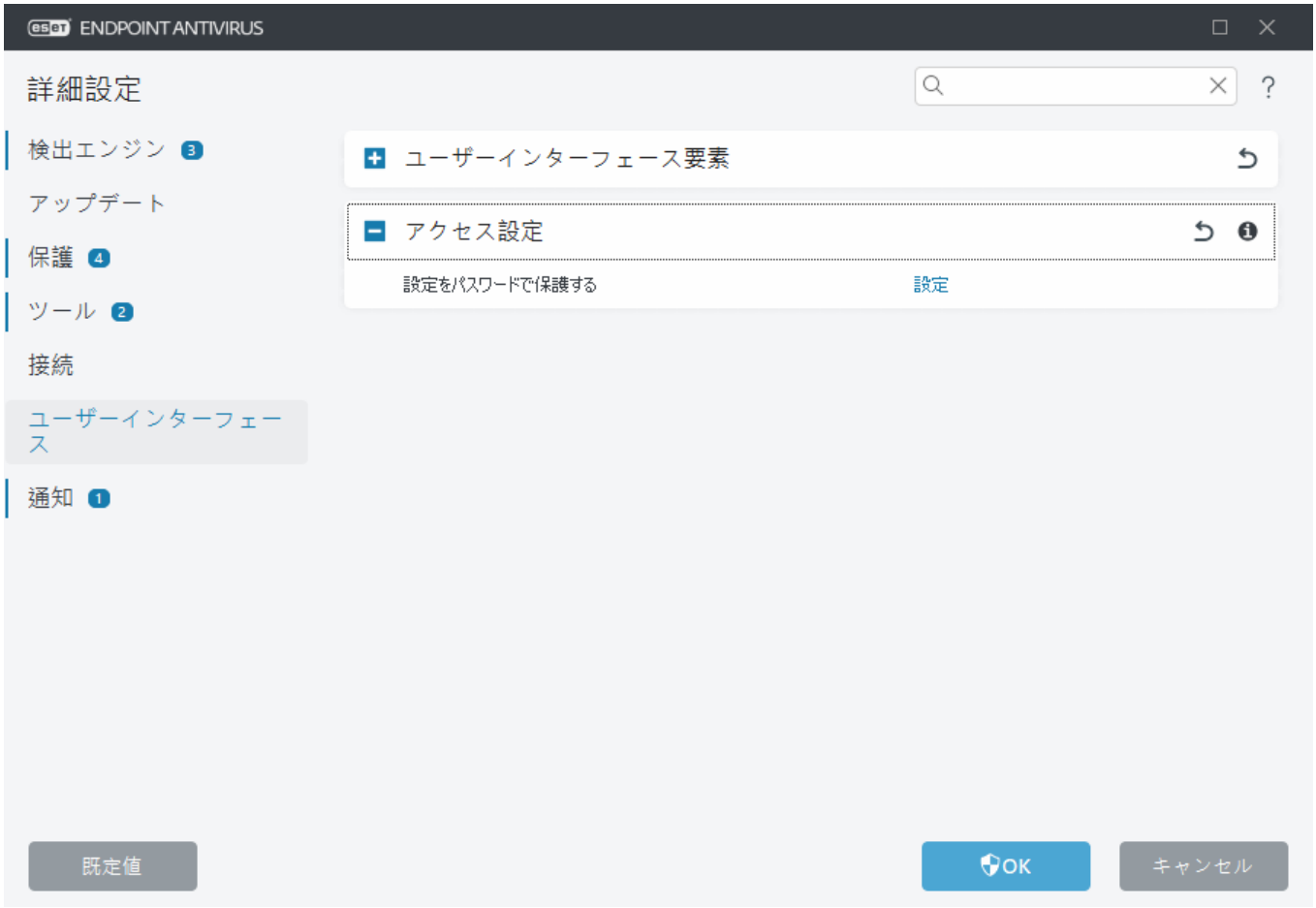
パスワードを設定してESET Endpoint Antivirusの設定パラメーターとアンインストールを保護するには、**設定をパスワードで保護する**の横の**設定**をクリックします。

パスワードを変更するには、**設定をパスワードで保護する**の横の**パスワードの変更**をクリックします。

パスワードを削除するには、**設定をパスワードで保護する**の横の**削除**をクリックします。

## 管理された環境

管理者は、接続されたクライアントコンピューターのESET Endpoint Antivirusの設定をパスワードで保護するためのポリシーを作成できます。新しいポリシーを作成するには、パスワード保護設定を参照してください。




# 詳細設定のパスワード

ESET Endpoint Antivirus詳細設定を保護し、許可されてない修正を回避するには、**新しいパスワード**と**新しいパスワードの確認**に新しいパスワードを入力します。**OK**をクリックします。

## 管理された環境

管理者は、接続されたクライアントコンピューターのESET Endpoint Antivirusの設定をパスワードで保護するためのポリシーを作成できます。新しいポリシーを作成するには、パスワード保護設定を参照してください。

## 管理対象外

既存のパスワードを変更したいとき:

1. **パスワードの変更**をクリックします。
2. **新しいパスワード**と**新しいパスワードの確認**に新しいパスワードを入力します。
3. **OK**をクリックします。

ESET Endpoint Antivirusを将来修正するには、このパスワードが必要です。

パスワードを忘れた場合は、ESETエンドポイント製品で設定パスワードのロックを解除するを参照してください。

ESET製品認証キー、ライセンスの有効期限、またはESET Endpoint Antivirusの他のライセンス情報を忘れた場合に回復するには、ユーザー名とパスワード/製品認証キーをなくしましたを参照してください。

# パスワード

認証されていないユーザーによる変更を防ぐためにESETEndpointAntivirusの設定パラメーターをパスワードで保護することができます。

# セーフモード

ESET Endpoint Antivirusのグラフィカルインタフェースをセーフモードで起動すると、これはセーフモードで実行されることを示すダイアログウインドウが表示されます。セーフモードでは、あらゆるプログラムの動作が制限されるのでESET Endpoint Antivirusのグラフィカルインタフェースを標準モードのように開くことはできません。

表示されたウィンドウで、コンピューターの検査を実行できます。悪意のあるコードが、コンピュータに潜んでいないかどうかを検査する場合は、[**はい**]をクリックします。

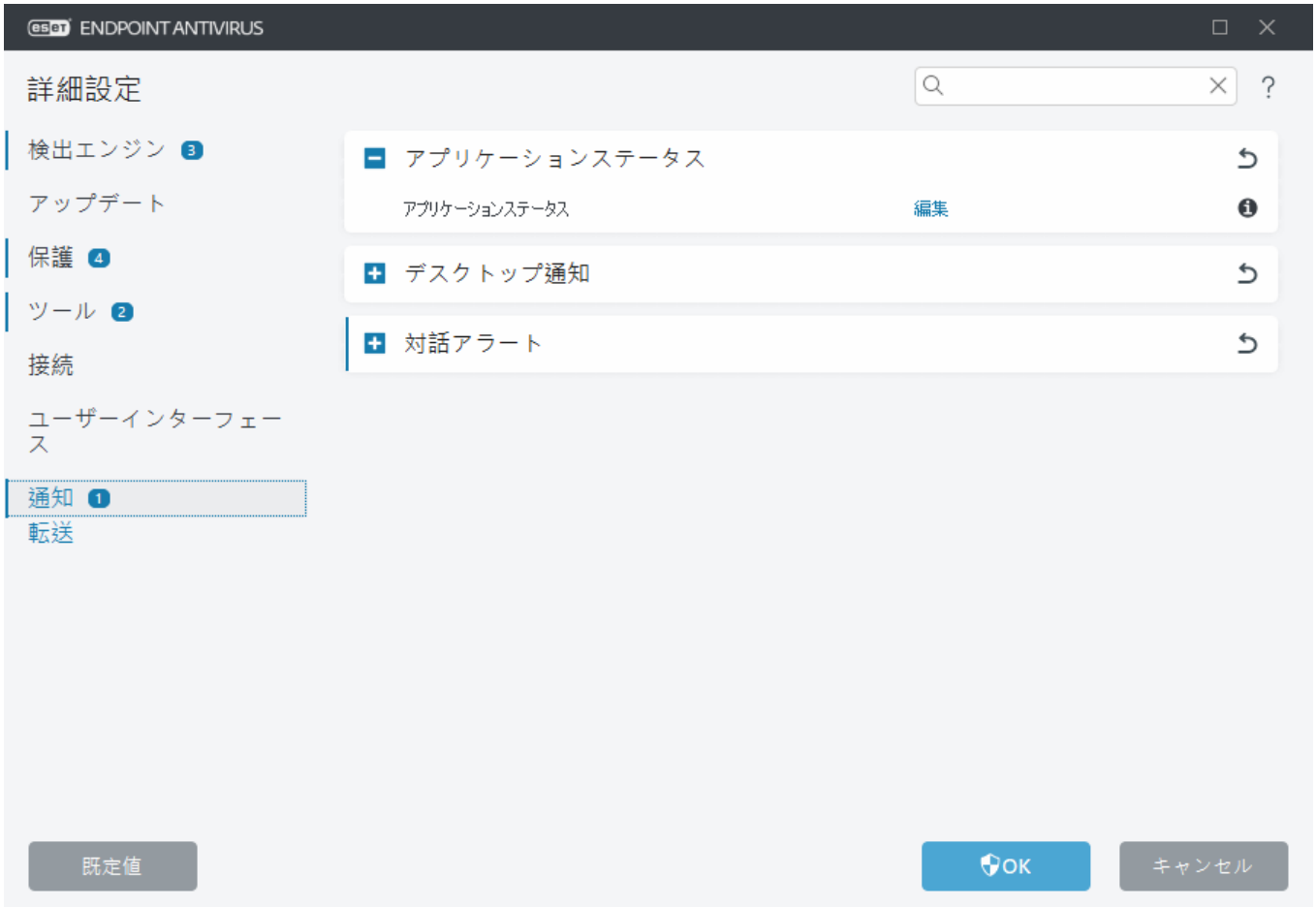
そうすると、ウィンドウがもう 1 つ表示されて、スキャンが開始されます。このスキャンではESET Endpoint Antivirusのインストール時に設定されたコンピュータスキャンの既定プロファイルと同じパラメーターが使用されます。

ダイアログウィンドウを閉じるには[**いいえ**]オプションを選択しますESET Endpoint Antivirusはアクションを何も行いません。

# 通知

ESET Endpoint Antivirus通知を管理するには、詳細設定 > **通知**を開きます。次のタイプの通知を設定できます。

- アプリケーションステータス – メインプログラムウィンドウのホームセクションに表示される通知。
- デスクトップ通知 – システムタスクバーの横の小さい通知ウィンドウ。
- 対話アラート – ユーザーの操作が必要なアラートウィンドウとメッセージボックス。
- 転送（電子メール通知）– 電子メール通知は指定された電子メールアドレスに送信されます。
- 通知のカスタマイズ – デスクトップ通知などにカスタム通知を追加します。




## アプリケーションステータス

**アプリケーションステータス** - **編集**をクリックすると、メインプログラムウィンドウのホームセクション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。

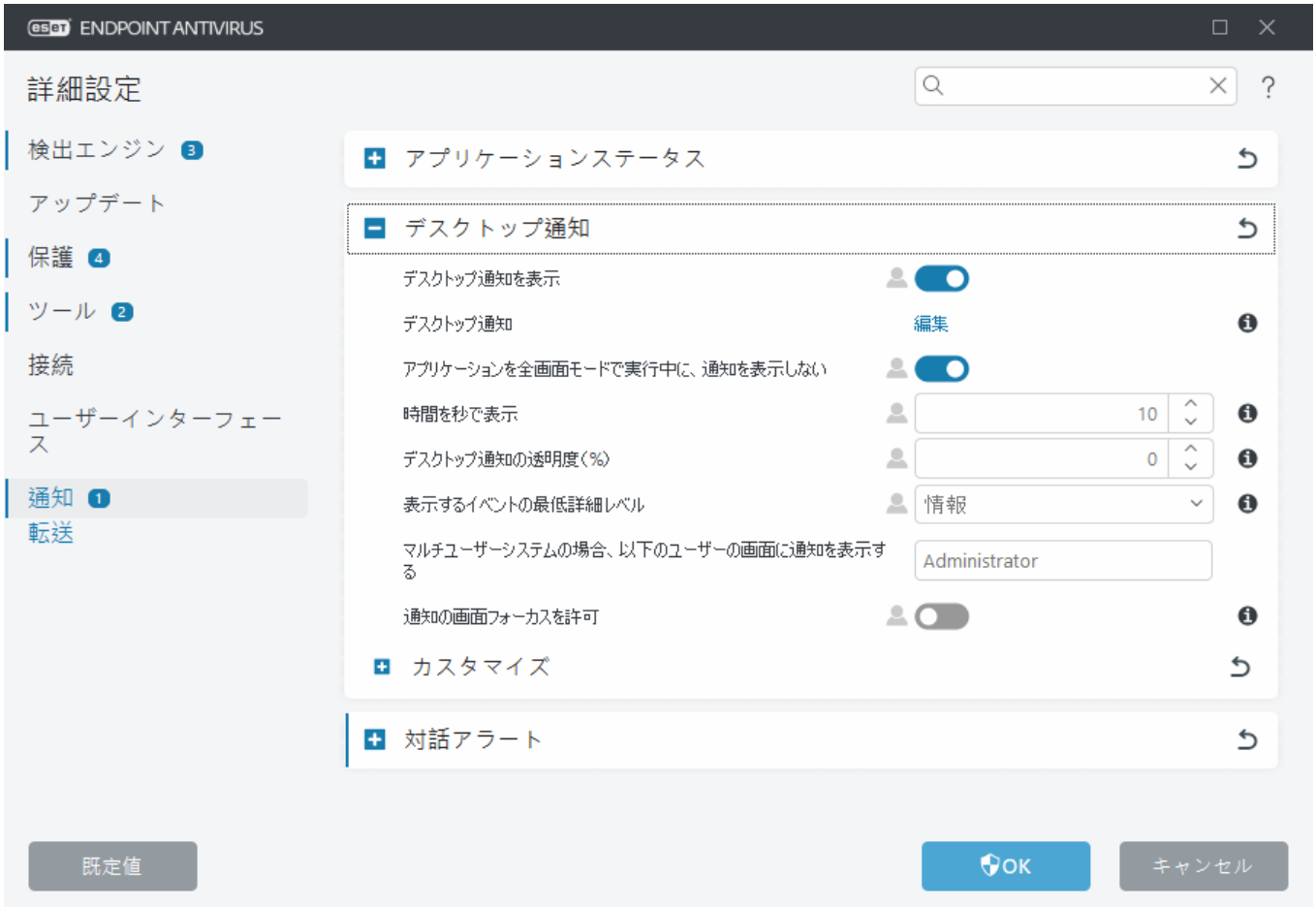
# アプリケーションステータス

表示されるアプリケーションステータスを設定する(ウイルス・スパイウェア対策保護を一時停止したり、プレゼンテーションモードを有効にしたりした場合など)には、詳細設定 > **通知**を開き、**アプリケーションステータス**の横の**編集**をクリックします。

また、製品がアクティベーションされていない場合や、ライセンスが有効期限切れの場合にも、アプリケーションステータスが表示されます。この設定は、ESET PROTECTポリシーから変更できます。


# デスクトップ通知

デスクトップ通知はシステムタスクバーの横の小さい通知ウィンドウで表示されます。既定では、10秒間表示され、ゆっくりと消えるように設定されています。これはESET Endpoint Antivirusが製品のアップデートの成功、新しい接続されたデバイス、ウイルス検査タスクの完了、または新しい脅威の検出についてユーザーに通知する主な手段です。




**デスクトップ通知を表示** – このオプションは有効にし、新しいイベントが発生するときに製品が通知を送信することをお勧めします。

**デスクトップ通知 – 編集**をクリックすると、特定のデスクトップ通知を有効または無効にできます。

**アプリケーションを全画面モードで実行中に、通知を表示しない** – 全画面モードでアプリケーションを実行しているときに、すべての非対話型通知を非表示にします。

**時間を秒で表示** – 通知の表示期間を設定します。値は3~30秒である必要があります。

**デスクトップ通知の透明度(%)** – 通知の透明度を割合で設定します。サポートされている範囲は0(透明ではない)から80(非常に高い透明度)です。

**表示するイベントの最低詳細レベル** – 表示する通知の最低重要度を設定します。ドロップダウンメニューから次のオプションのいずれかを選択します。

- **診断** – 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をログに記録します。
- **情報** – 標準以外のネットワークイベントなどの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。
- **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(例: アップデートの失敗)。
- **エラー** – エラー(ドキュメント保護が起動していません)や重大なエラーを記録します。
- **重大** – 重大なエラー(ウイルス対策保護の開始エラーや感染したシステム)のみを記録します。

**マルチユーザーシステムで、このユーザーの画面に通知を表示する** – 選択したアカウントでデスクトップ通知を受信できます。たとえば、管理者アカウントを使用しない場合は、完全なアカウント名を入力すると、指定したアカウントのデスクトップ通知が表示されます。1つのユーザーアカウントのみがデスクトップ通知を受信できます。

**通知の画面フォーカスを許可** – 通知は画面にフォーカスし、Alt+Tabからアクセスできます。

# 通知のカスタマイズ

このウィンドウでは、通知で使用されるメッセージをカスタマイズできます。

**既定の通知メッセージ**– 通知のフッターに表示される既定のメッセージ。

## 検出

**[検出通知を自動的に閉じない]**を有効にすると、手動で閉じるまでマルウェア通知が画面に表示されます。

**既定の通知メッセージ**を無効にし、**検出の通知メッセージ**フィールドに独自のメッセージを入力すると、カスタム通知メッセージが使用されます。

# ダイアログウィンドウ – デスクトップ通知

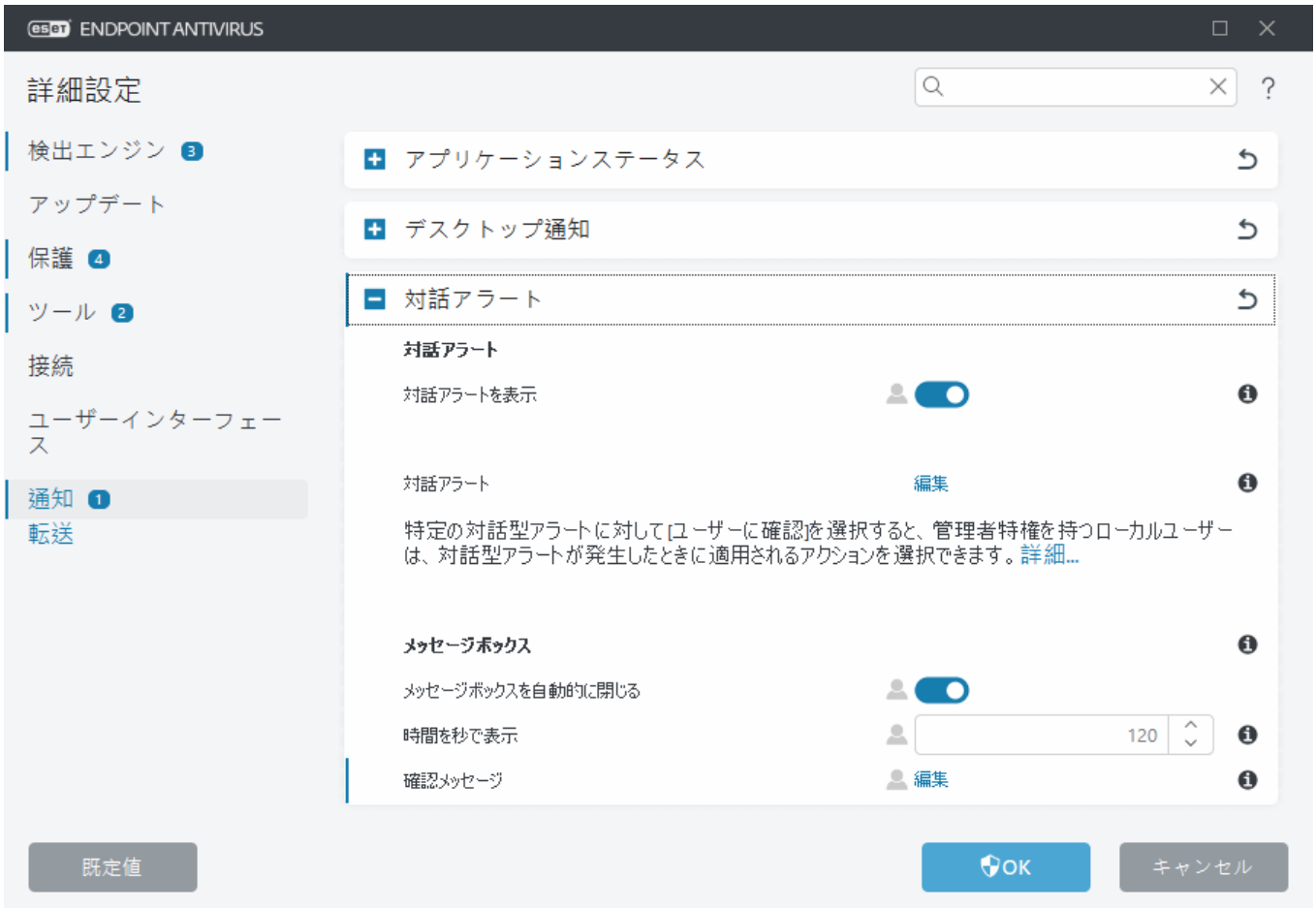
デスクトップ通知(画面右下に表示)の表示を調整するには、詳細設定 > **通知** > **デスクトップ通知**に移動します。**デスクトップ通知**の横の**編集**をクリックし、該当する**デスクトップに表示**チェックボックスを選択します。


ESET LiveGuardの使用中に**ファイルが分析されました**および**ファイルが分析されていません**通知を設定する場合は、プロアクティブ保護を**分析結果を受信するまで実行をブロックする**に設定する必要があります。

# 対話アラート

共通のアラートと通知に関する情報
- マルウェアが検出されました
- アドレスがブロックされました
- アクティベーションされていません
- アップデートを利用できます
- アップデート情報に矛盾があります。
- 「モジュールアップデート失敗」メッセージのトラブルシューティング
- 「ファイルが破損しています」または「ファイルの名前を変更できませんでした」
- Webサイト証明書が取り消されました
- ネットワークの脅威がブロックされました
- 分析のためファイルがブロックされましたブロックされた

**詳細設定** > 通知の**対話アラート**セクションでは、ユーザーが決定する必要がある検出のメッセージボックスと対話アラート(潜在的なフィッシングWebサイトなど)をESET Endpoint Antivirusで処理する方法を設定できます。




## 対話アラート

**対話アラートを表示する**をオフにすると、すべての警告ウィンドウとブラウザー内ダイアログが表示されなくなります。この設定が適しているのは、特定の限られた状況のみです。

- 管理者権限のないユーザーの場合、このオプションは既定の設定のまま(有効)にすることをお勧めします。
- 管理者権限のあるユーザーの場合、この設定を有効にし、対話アラートのリストでユーザーの定

義済みアクションを選択します。

**対話アラート—編集**をクリックし、表示される対話アラートを選択します。

## メッセージボックス

特定の時間が経過した後で自動的にメッセージウィンドウを閉じるには、**メッセージボックスを自動的に閉じる**を選択します。警告ウィンドウを手動で閉じない場合、指定した時間が経過すると、ウィンドウは自動的に閉じられます。

**時間を秒で表示** – 通知アラートの表示期間を設定します。値は10~999秒である必要があります。

**確認メッセージ - 編集**をクリックすると、表示または非表示にする確認メッセージを選択できるリストが表示されます。

# 対話アラートのリスト

このセクションでは、アクションが実行される前に、ESET Endpoint Antivirusで表示される複数の対話アラートウィンドウについて説明します。

設定可能な対話アラートの動作を調整するには、詳細設定 > **通知** > **インタラクティブアラート**に移動し、**対話アラート**の横の**編集**をクリックします。

管理者が幾つもの「**ユーザーに確認**」を選択解除したり、対話アラートウィンドウが表示された時に適用される定義済みのアクションを選択しておけるので、管理された環境で役立ちます。


特定の対話アラートウィンドウについては、他のヘルプセクションを確認してください。

## リムーバブルメディア

- 新しいデバイスが選択されました

### ネットワーク保護

- ネットワークアクセスがブロックされましたは、ESET PROTECTからのこのワークステーションの**コンピューターをネットワークから隔離する**クライアントタスクがトリガーされたときに表示されます。
- ネットワーク通信がブロックされました
- ネットワークの脅威がブロックされました

### Webブラウザーアラート

- 望ましくない可能性があるコンテンツが見つかりました
- フィッシングのためWebサイトがブロックされました

### コンピュータ

これらのアラートが発生していると、ユーザーインターフェースの色が変わります。

- コンピューターを再起動する(必須)
- コンピューターを再起動する(推奨)

対話アラートには、検出エンジンHIPSファイアウォールの対話ウィンドウは含まれません。これらの動作は、特定の機能で個別に設定することができます。

## 確認メッセージ

確認メッセージを調整するには、詳細設定 > **通知** > **対話アラート**に移動し、**確認メッセージ**の横の**編集**をクリックします。


このダイアログウィンドウには、アクションが実行される前に、ESET Endpoint Antivirusで表示される確認メッセージが表示されます。各確認メッセージの横のチェックボックスをオンまたはオフにすると、

メッセージを許可または無効にします。

確認メッセージに関連した特定の機能の詳細:

- ESET SysInspectorログを削除する前に確認する
- すべてのESET SysInspectorログを削除する前に確認する
- 隔離フォルダのオブジェクトを削除する前に確認する
- 詳細設定の設定を破棄する前に確認する
- すべての検出された脅威を駆除せずにアラートウィンドウから移動する前に確認する
- ログからレコードを削除する前に確認する
- スケジューラのスケジュールタスクを削除する前に確認する
- すべてのログレコードを削除する前に確認する
- 統計をリセットする前に確認する
- 隔離フォルダからオブジェクトを復元する前に確認する
- 隔離フォルダからオブジェクトを復元して検査から除外する前に確認する
- スケジューラのスケジュールタスクを実行する前に確認する
- Outlook ExpressとWindows Mail電子メールクライアントで製品確認ダイアログを表示する
- Windows Live Mailで製品確認ダイアログを表示する
- Outlook電子メールクライアントで製品確認ダイアログを表示する

# 詳細設定競合エラー

このエラーは、何らかのコンポーネント(HIPS)とユーザーが同時にインタラクティブまたは学習モードでルールを作成した場合に発生することがあります。

独自のルールを作成する場合は、フィルタリングモードを既定の**自動モード**に変更することをお勧めします。 詳細については、HIPSおよびHIPSフィルタリングモードをお読みください。

# 再起動する必要があります

ESET Endpoint Antivirusを新しいバージョンにアップグレードした後、または脆弱性およびパッチ管理を介してアプリケーションにパッチを適用した後は、コンピューターの再起動が必要です。プログラムモジュールの自動更新では解決できない改善の導入や問題の修正を行うためにESET Endpoint Antivirusの新バージョンが提供されています。

**今すぐ再起動**をクリックしてコンピューターを再起動します。後でコンピューターを再起動する場合は、**後で通知する**をクリックします。後から、メインプログラムウィンドウの**保護の状態**セクションから手動でコンピューターを再起動できます。

「再起動が必要」または「再起動推奨」アラートを無効にするには、次の手順に従います。

1. **詳細設定**(F5) > **通知** > **対話アラート**を開きます。
2. **対話アラート**の横の**編集**をクリックします。**コンピューター**セクションで、**コンピューターを再起動する(必須)**と**コンピューターを再起動する(推奨)**の横のチェックボックスをオフにします。
3. **OK**をクリックすると、両方の開いているウィンドウで変更を保存できます。
4. アラートは、エンドポイントコンピューターに表示されません。
5. (任意)ESET Endpoint Antivirusのメインプログラムウィンドウでアプリケーションステータスを無効にするには、アプリケーションステータスウィンドウで、**コンピューターの再起動が必要です**と**コンピューターの再起動が推奨されます**の横のチェックボックスをオフにします。

# 再起動が推奨されます

ESET Endpoint Antivirusを新しいバージョンにアップデートした後に、コンピューターの再起動が必要です。プログラムモジュールの自動更新では解決できない改善の導入や問題の修正を行うためにESET Endpoint Antivirusの新バージョンが提供されています。

**今すぐ再起動**をクリックしてコンピューターを再起動します。後でコンピューターを再起動する場合は、**後で通知する**をクリックします。後から、メインプログラムウィンドウの**保護の状態**セクションから手動でコンピューターを再起動できます。

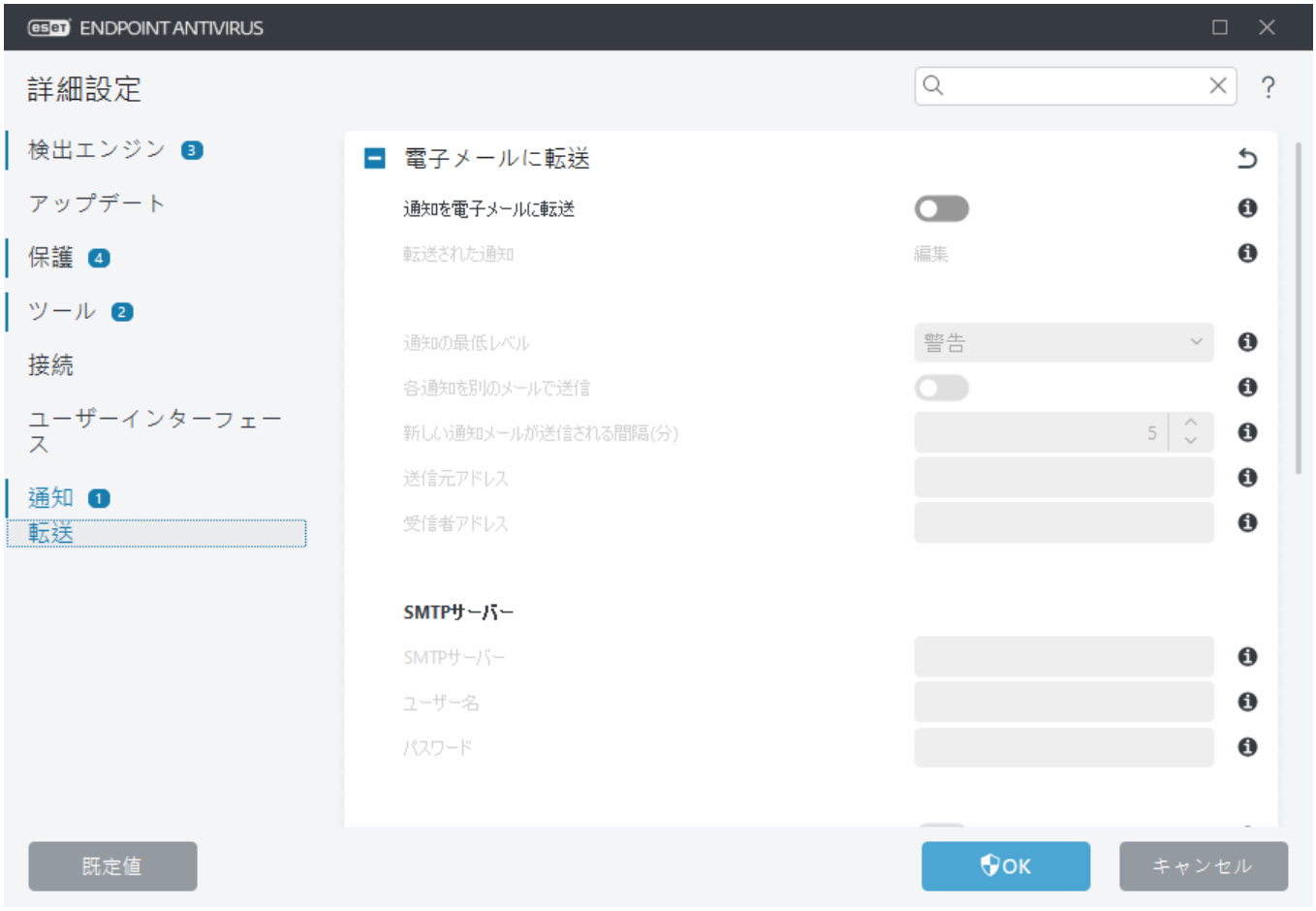
「再起動が必要」または「再起動推奨」アラートを無効にするには、次の手順に従います。

1. **詳細設定**(F5) > **通知** > **対話アラート**を開きます。
2. **対話アラート**の横の**編集**をクリックします。**コンピューター**セクションで、**コンピューターを再起動する(必須)**と**コンピューターを再起動する(推奨)**の横のチェックボックスをオフにします。
3. **OK**をクリックすると、両方の開いているウィンドウで変更を保存できます。
4. アラートは、エンドポイントコンピューターに表示されません。
5. (任意)ESET Endpoint Antivirusのメインプログラムウィンドウでアプリケーションステータスを無効にするには、アプリケーションステータスウィンドウで、**コンピューターの再起動が必要です**と**コンピューターの再起動が推奨されます**の横のチェックボックスをオフにします。

# 転送

ESET Endpoint Antivirusは、選択されている詳細レベルのイベントの発生時に、自動的に通知メールを送信できます。詳細設定 > **通知** > **転送** > **電子メールに転送**セクションで、**通知を電子メールに転送**を有効にして、電子メール通知を有効にします。

**転送される通知** – 電子メールに転送されるデスクトップ通知を選択します。




**通知の最低レベル**ドロップダウンメニューで、送信する通知の開始重要度を選択できます。

- **診断** – 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をログに記録します。
- **情報** – 標準以外のネットワークイベントなどの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。
- **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(例: アップデートの失敗)。
- **エラー** – エラー(ドキュメント保護が起動していません)や重大なエラーを記録します。
- **重大** – 重大なエラー(ウイルス対策保護の起動エラーや脅威の検出など)のみを記録します。

**各通知を別のメールで送信**– 有効にすると、受信者は、各通知に関する新しい電子メールを受信します。このため、短期間で大量の電子メールを受信する場合があります。

**新しい通知メールが送信される間隔(分)**– 新しい通知が電子メールに送信されるまでの間隔(分)。この値を0に設定すると、通知がただちに送信されます。

**送信元アドレス** – 通知メールのヘッダーに表示される送信者アドレスを定義します。

**受信者アドレス** – 通知電子メールのヘッダーに表示される受信者アドレスを定義します。複数の値がサポートされます。区切り文字にはセミコロンを使用してください。

## SMTPサーバー

**SMTPサーバー** – 通知を送信するために使用されるSMTPサーバー(例: *smtp.provider.com:587*、事前定義されたポートは25)。

TLS暗号化機能を備えたSMTPサーバーは、ESET Endpoint Antivirusでサポートされます。

**ユーザー名とパスワード** - SMTPサーバで認証を要求する場合、有効なユーザー名とパスワードをフィールドに入力してSMTPサーバへのアクセスを許可する必要があります。

**送信者アドレス** – 通知メールのヘッダーに表示される送信者アドレスをこのフィールドに指定します。

**受信者アドレス** – 通知メールのヘッダーに表示される受信者アドレスをこのフィールドに指定します。セミコロン「;」を使用して、複数の電子メールアドレスを区切ります。

**TLSを有効にする** - TLS暗号化でサポートされる警告と通知メッセージの送信を有効にします。

## メッセージの書式

プログラムとリモートユーザーまたはシステム管理者間の通信は、メールまたはLANメッセージ(Windowsメッセージングサービスを使用)によって行われます。警告メッセージおよび通知の既定のフォーマットは、ほとんどの状況に適しています。ただし、場合によっては、イベントメッセージのフォーマットを変更しなければならないことがあります。

**イベントメッセージの書式** – リモートコンピュータで表示されるイベントメッセージの形式。

**脅威警告メッセージの書式** – 脅威警告と通知メッセージには定義済みの既定の形式があります。この書式は変更しないようお勧めします。ただし、状況によっては(自動メール処理システムを使用している場合など)、メッセージの書式を変更しなければならないことがあります。

**文字セット** – Windows地域設定(windows-1250Unicode (UTF-8)ACSII 7-bit日本語(ISO-2022-JP)など)に基づいて、電子メールメッセージをANSI文字エンコーディングに変換します。結果としてÁ"á"は˝a"に変換され、不明な記号は˝?˝に変換されます。

**Quoted-printableエンコーディングを使用** – 電子メールメッセージのソースはQuoted-printable (QP)書式でエンコードされます。この書式は、ASCII文字を使用し、特殊な各国語文字を8ビット書式(áéíóú)の電子メールで正確に送信できます。

メッセージでは、指定されている実際の情報でキーワード(%記号で区切られた文字列)が置き換えられます。使用可能なキーワードは次のとおりです。

- **%TimeStamp%**– イベントの日時
- **%Scanner%**– 関連するモジュール
- **%ComputerName%**– 警告が発生したコンピュータの名前
- **%ProgramName%**– 警告を生成したプログラム
- **%InfectedObject%**– 感染しているファイルやメールなどの名前
- **%VirusName%**– ウイルスのID
- **%Action%** – 侵入に対する処理
- **%ErrorDescription%** – ウイルス以外のイベントの説明

キーワード**%InfectedObject%**および**%VirusName%**はマルウェア警告メッセージのみで使用され、**%ErrorDescription%**はイベントメッセージのみで使用されます。

# すべての設定を既定値に戻す

**詳細設定**で既定値をクリックすると、すべてのモジュールのすべてのプログラム設定を元に戻します。これで、すべてのモジュールのすべてのプログラム設定が新規インストール時の状態にリセットされます。

設定をインポートおよびエクスポートするを参照してください。

# 現在のセクションのすべての設定を元に戻す

カーブした矢印↩をクリックすると、現在のセクションのすべての設定がESETで定義した既定の設定に戻ります。

**既定に戻す**をクリックすると、行われたすべての変更が失われます。

**テーブルの内容を戻す** – 有効にすると、手動または自動で追加されたルール、タスク、プロファイルが失われます。

設定をインポートおよびエクスポートするを参照してください。

# 設定の保存中のエラー

このエラーメッセージは、エラーが発生したため設定が正しく保存されなかったことを示しています。

通常、これは、プログラムパラメーターを修正しようとしたユーザーが次の状態であることを意味します。

- アクセス権が不十分であるか、設定ファイルとシステムレジストリを修正するために必要なオペレーティングシステム権限がないことを意味します。
  > 目的の修正を実行するには、システム管理者がログインする必要があります。
- 最近HIPSまたはファイアウォールで学習モードを有効にし、詳細設定を変更しようとしました。
  > 設定を保存し、設定の競合を回避するには、保存せずに詳細設定を閉じ、目的の変更をもう一度試してください。

2番目に一般的な原因としては、プログラムが壊れて正しく動作しなくなり、再インストールが必要になったことが考えられます。

# コマンドラインスキャナー

ESET Endpoint Antivirusの保護モジュールは、コマンドラインから手動で起動することも("ecls"コマンドを使用します)、バッチ("bat")ファイルを使用して起動することもできます。ecls.exeは、既定値では[C:\Prog]に格納されています。

ESETコマンドラインスキャナーの使用方法:

```
ecls [OPTIONS..] FILES..
```

コマンドラインからオンデマンドスキャナーを実行する際には、次のパラメーターおよびスイッチを使用することができます。

## オプション

| | |
|---|---|
| /base-dir=移動先のフォルダ | FOLDERからモジュールをロードします |
| /quar-dir=移動先のフォルダ | FOLDERを隔離します |
| /exclude=MASK | MASKと一致するファイルをスキャン対象から除外します |
| /subdir | サブフォルダーを検査します(既定) |
| /no-subdir | サブフォルダーを検査しません |
| /max-subdir-level=LEVEL | スキャン対象に含めるサブフォルダー階層の下限レベル |

| | |
|---|---|
| /symlink | シンボリックリンクを辿ります(既定) |
| /no-symlink | シンボリックリンクをスキップします |
| /ads | ADSを検査します(既定) |
| /no-ads | ADSを検査しません |
| /log-file=ファイル | ログをFILEに出力します |
| /log-rewrite | 出力ファイルを上書きします(既定 - append) |
| /log-console | ログをコンソールに出力します(既定) |
| /no-log-console | ログをコンソールに出力しません |
| /log-all | 感染していないファイルも記録します |
| /no-log-all | 感染していないファイルは記録しません(既定) |
| /aind | アクティビティインジケーターを表示します |
| /auto | すべてのローカルディスクを検査し、自動的に駆除します |

## スキャナーオプション

| | |
|---|---|
| /files | ファイルを検査します(既定) |
| /no-files | ファイルを検査しません |
| /memory | メモリーを検査します |
| /boots | ブートセクターを検査します |
| /no-boots | ブートセクターを検査しません(既定) |
| /arch | アーカイブを検査します(既定) |
| /no-arch | アーカイブを検査しません |
| /max-obj-size=SIZE | SIZEメガバイト未満のファイルのみスキャンします(既定0 = 制限なし) |
| /max-arch-level=LEVEL | スキャン対象に含めるアーカイブ内の上限ネストレベル |
| /scan-timeout=LIMIT | 最大でLIMIT秒間アーカイブを検査します |
| /max-arch-size=SIZE | アーカイブのうち?SIZE未満のファイルのみスキャンします(既定0 = 制限なし) |
| /max-sfx-size=SIZE | 自己解凍アーカイブのうち?SIZEメガバイト未満のファイルのみスキャンします(既定0 = 制限なし) |
| /mail | 電子メールファイルをスキャンします(既定) |
| /no-mail | 電子メールファイルをスキャンしません |
| /mailbox | 受信箱を検査します(既定)。 |
| /no-mailbox | 受信箱を検査しません |
| /sfx | 自己解凍アーカイブを検査します(既定) |
| /no-sfx | 自己解凍アーカイブを検査しません |
| /rtp | ランタイム圧縮形式を検査します(既定) |
| /no-rtp | ランタイム圧縮形式を検査しません |
| /unsafe | 安全でない可能性があるアプリケーションを検査します |
| /no-unsafe | 安全でない可能性があるアプリケーションを検査しません(既定) |
| /unwanted | 潜在的に不要なアプリケーションを検査します |
| /no-unwanted | 潜在的に不要なアプリケーションを検査しません(既定) |

| | |
|---|---|
| /suspicious | 不審なアプリケーションを検査する(既定) |
| /no-suspicious | 不審なアプリケーションを検査しない |
| /pattern | シグネチャーを使用します(既定) |
| /no-pattern | シグネチャーを使用しません |
| /heur | ヒューリスティックを有効にします(既定) |
| /no-heur | ヒューリスティックを無効にします |
| /adv-heur | アドバンスドヒューリスティックを有効にします(既定) |
| /no-adv-heur | アドバンスドヒューリスティックを無効にします |
| /ext-exclude=EXTENSIONS | コロンで区切られたEXTENSIONSファイルを検査対象から除外します |
| /clean-mode=MODE | 感染したオブジェクトに対して駆除モードを使用します。<br><br>使用可能なオプションは<br>• none（既定）– 自動駆除を実行しません。<br>• standard - ecls.exeは感染したファイルを自動的に駆除または削除しようとします。<br>• strict – ecls.exeはユーザー操作を要求せずに感染したファイルを自動的に駆除または削除しようとします(ファイルが駆除される前の確認メッセージは表示されません)。<br>• rigorous – ファイルの内容に関係なくecls.exeは駆除を試行せずにファイルを削除します。<br>• delete - ecls.exeは駆除を試行せずにファイルを削除しますがWindowsシステムファイルなどの重要なファイルは削除しません。 |
| /quarantine | 感染ファイルを隔離フォルダーにコピーします<br>(駆除中に実行したアクションの補足) |
| /no-quarantine | 感染ファイルを隔離フォルダーにコピーしません |

## 一般的なオプション

| | |
|---|---|
| /help | ヘルプの表示と終了を実行します |
| /version | バージョン情報の表示と終了を実行します |
| /preserve-time | 最終アクセスのタイムスタンプを保持 |

## 終了コード

| | |
|---|---|
| 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 | 一部のファイルを検査できませんでした(脅威の可能性があります) |
| 50 | マルウェアが検出されました |
| 100 | エラー |

100を超える終了コードは、ファイルがスキャンされなかったため、感染している可能性があることを意味します。

# よくある質問

この章では、よくある質問と問題をいくつか説明します。問題の解決方法を調べるには、該当するトピックをクリックしてください。

- ESET Endpoint Antivirusをアップデートする方法
- ESET Endpoint Antivirusをアクティベートする方法
- ESET Endpoint Antivirusが脅威を検出した
- PCからウイルスを取り除く方法
- スケジューラで新しいタスクを作成する方法
- 週次コンピューター検査をスケジュールする方法
- 通知と対話型アラートを管理する方法
- 製品をESET PROTECTに接続する方法
  上書きモードを使用する方法
  - ESET Endpoint Antivirusの推奨されたポリシーを適用する方法
- ミラーを構成する方法
- ESET Endpoint Antivirusがインストールされた状態でWindows 10にアップグレードする方法
- リモート監視と管理をアクティブ化する方法
- インターネットから特定のファイルタイプのダウンロードをブロックする方法
- ESET Endpoint Antivirusユーザーインターフェースを最小化する方法

上記ヘルプページのリストに含まれていない問題の場合は、問題をよく表現しているキーワードまたは語句を使用してESET Endpoint Antivirusヘルプページ内を検索してみてください。

ヘルプページで問題や疑問への解決策が見つからない場合は、ESETナレッジベースにアクセスし、一般的な問題や質問への回答を検索します。

- ESET Endpoint Antivirusのアンインストール方法
- ファイルコーダー(ランサムウェア)マルウェアから保護するためのベストプラクティス
- ESET Endpoint SecurityおよびESET Endpoint Antivirus FAQ
- ESET製品の完全な機能を許可するためには、他社製のファイアウォールでどのアドレスとポートを開く必要がありますか。

必要に応じて、問題/質問について当社のオンラインテクニカルサポートセンターまでお問い合わせいただくこともできます。オンラインお問い合わせフォームへのリンクは、メインプログラムウィンドウの**[ヘルプとサポート]**ページにあります。

# 自動アップデートのFAQ

ESET Endpoint Antivirusの製品のアップデートの詳細については、次のESETナレッジベース記事をお読みください。
- ESET製品のアップデートとリリースタイプ

## コンピューターは自動的にアップデートされますか。再起動の前または後にアップデートがダウンロードされますか。

ダウンロードは再起動する前に実行され、アップデートされたファイルもこの段階で準備されます。再起動後、アップデートされたファイルはまだ準備状態で、使用はできません。現在インストールされているバージョンでは中断されずに保護されます。次回のESET Endpoint Antivirusの起動後に、変更が適用されます。

## 約3000台のコンピューターを使用しています。すべてのコンピューターが同時にアップデートをダウンロードしますか。このような多数のコンピューターの自動アップデートではプロキシを使用できますか。

ESETは大規模なネットワーク向けにミラーツールとプロキシソリューションを提供します。このため、アップデートはインターネットから1回だけダウンロードされ、ローカルで配布されます。アップデートは小さく、一般的には5~10MBです。ESETは、最初の数週間の提供期間中にアップデートを調整します。このため、一部のクライアントは、直接ESETサーバーに接続するときに、同時にダウンロードを開始しません。

## 自動的にアップデートされるコンピューター数とコンピューター数を決定できますか。1時間に10台以上のコンピューターをダウンロードしないようにするか、今は10台のコンピューターだけアップデートし、数日後に別のコンピューターをアップデートするようにしたいと考えています。

管理された環境には自動アップデートポリシーがあります。ここで、最新の任意のバージョンを指定できます。ワイルドカード(9.0.2032.*など)もサポートされます。詳細については、ESET PROTECTまたはESET PROTECT Cloudのオンラインヘルプの「自動アップデート」の章をご覧ください。残念ながら、現在、自動アップデートを制限する他のオプションはありません。複数のグループに対して複数のポリシーを割り当てることができます。

## 自動アップデートはポリシー経由でのみ設定されますかESET製品をアップデートしない場合は、ポリシーを無効にできますか。

ESETエンドポイント製品のセキュリティと安定性ホットフィックスがある場合は、該当するエンドユーザーライセンス契約で規定された条項に従い、自動アップデートが無効な場合でも、製品がアップデートされますESETはセキュリティと安定性ホットフィックスを使用して、重要な問題に対処し、ESET製品のセキュリティと安定性を最大限に確保します。

自動アップデートポリシーは、現在の自動アップデート設定に関係なく、任意のグループのエンドポイントに割り当てることができます。管理されていない環境ではESETエンドポイント製品の詳細設定画面で、ローカルで自動アップデートを設定できます。

## 最も古い使用可能なバージョンを使用するポリシーを設定する場合はどうすれば良いですか。その場合でもESETは製品をアップデートしますか。

ホットフィックスと重要なホットフィックス(セキュリティと安定性のアップデート)は、アップデートカテゴリが少し異なります。ユーザー設定が許可されているときには、標準ホットフィックスは、ユーザー設定で許可されているときに、標準優先度の自動アップデートに割り当てられます。重要なホットフィックスは、ユーザー設定に関係なく、最高優先度が適用されます。

## オフラインシナリオではどのようにアップデートが機能しますか。

## ユーザーはいつオフラインリポジトリを使用するのですか。

オフラインリポジトリには.dupファイルと.fupファイルも含まれます。リポジトリセクションはモジュールのアップデートではなく、ミラーツールによってダウンロードする必要があります。詳細については ESET PROTECTのオンラインヘルプのオフラインリポジトリトピックを参照してください。

## アップデートが必要なことをどのようにESET製品で確認していますか。リポジトリからですか。サーバーに送信されるデータがありますかESETがバージョンリリースの1か月後にアップデートする予定の場合ESETサーバーは世界中のリリースに対応できますか。

ESET製品はリポジトリから自動アップデートをダウンロードします。緊急のアップデートのサイズがわずか数KBのときには、サーバーはそれに対応していますESETはリポジトリサーバーで緊急のアップデートを調整しません。ただし、自動アップデートが大きい場合は、サーバーアップデートを調整するオプションがあります。以下の表は、差分自動アップデートの場合の、ホットフィックスサイズの例を示します。

| 前のバージョン | 新しいバージョン | サイズ |
|---|---|---|
| 9.0.2032.2 | 9.0.2032.6 | 420 KB |
| 8.1.2037.2 | 9.0.2032.2 | 6.5 MB |
| 8.0.2028.0 | 9.0.2032.2 | 11.5 MB |

差分自動アップデートが失敗するとESET製品が完全アップデートを開始する場合があります。これは機能保証のある自動アップデートですが.dupファイルの代わりに、大きい.fupがダウンロードされます。バージョン9.0.2032.2では27MBです。ただし、このようなシナリオはまれにしか発生しません。

## ESETEndpointAntivirusアップデートは調整されてリリースされますか。リリース後にアップデートが調整される時間はどのくらいですか。

ESETは、新しいバージョンがリリースされた後の最初の数週間にアップデートを調整し、サーバーの負荷を削減し、新しいバージョンを均等に配布します。

## 自動アップデートはアップグレードの主な方法の1つになります。どのように詳細に機能しますか。

自動アップデートの目的は、できる限り多くの顧客を自動アップデートでアップデートすることです。多数の以前のバージョンが利用可能になっていると、サポートが困難です。自動アップデート機能はシンプルな方法で動作します。最初のモジュールのアップデートチェック中に.dupファイルがダウンロードされます。アップデート手順中には、製品が完全に機能し、コンピューターを保護します。再起動後に新しいバージョンがアクティベーションされますESET PROTECT (サーバー側)では、ポリシーを使用して、アップデートする最新バージョンを指定できます。詳細については、ESET PROTECTまたはESET PROTECT Cloudのオンラインヘルプの「自動アップデート」の章をご覧ください。

## 1/10で自動アップデートが動作するというのは正しい認識ですか。現在ESET Endpoint Security 8.0.2028.1を使用しています。自動アップ

### デートが実行される場合、どのバージョンにアップデートされますか。

リポジトリサーバーの調整のため、自動アップデートを使用した製品のアップデートが遅延する場合があります。製品のアップデートが調整でリリースされた場合、自動アップデートチェックでただちに受信されない場合があります。アップデートが安全で安定であると見なされた場合、調整が完全に削減または削除され、すべての残りのクライアントがアップデートを受信できます。

調整では、アップデートごとにかかる時間が異なる場合があります。これは、アップデートを要求するクライアント数、サーバーのトラフィック、および他の要因によって異なります。この手順は常に進化し、変更は常に発生します。

### 8:45 a.mにコンピューターを起動し、5:00 p.mにシャットダウンすると、いつ自動アップデートが開始しますか。

自動アップデートは、次のスケジュールされたモジュールのアップデートが成功した時点で開始され、24時間ごとに最大1回実行されます。

### 自動アップデートの実行中にコンピューターがシャットダウンされた場合、いつ次のアップデートが実行されますか。

アップデートは次のスケジュールされたアップデートウィンドウで実行されます。自動アップデート(以前はuPCU)手順には堅牢なフェールセーフメカニズムがあります。アップデートをダウンロードしてコンピューターを再起動した後も、アップデートされたファイルは準備状態であり、まだ使用できません。現在インストールされているバージョンの保護は中断されずに保護されます。変更は、次回のESETエンドポイント製品の起動後に適用されます。

### 24時間に1回、定期接続を待機せずにすぐに自動アップデートを実行するにはどのようにすることができますか。他にアップデートの確認をクリックする方法はありますか。

現在、メインプログラムウィンドウを開き、**アップデート** > **アップデートの確認**をクリックした場合にのみ手動で自動アップデート手順を開始できます。モジュールアップデートを修正する他のすべての方法は、24時間自動アップデートスケジューラポリシーを反映します。現在、自動アップデートダウンロードはリモートで開始できません。ESETは今後この機能を追加します。

## ESET Endpoint Antivirusをアップデートする方法

ESET Endpoint Antivirusは、手動または自動で更新できます。更新を開始するには、メインプログラムウィンドウの**アップデート**をクリックしてから、**最新版のチェック**をクリックします。

既定のインストール設定では、1時間ごとに実行される自動更新タスクが作成されます。間隔を変更するには、**ツール** > スケジューラに移動します。

## PCからウイルスを取り除く方法

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

1. プログラムのメインウィンドウで、[**コンピュータの検査**]をクリックします。
2. [**スマート検査**]をクリックし、システムの検査を開始します。
3. スキャンが完了したら、スキャンされたファイル、感染しているファイル、および駆除されたファイルの数をログで確認します。
4. ディスクの一部のみをスキャンするには、[**カスタム検査**]をクリックし、ウイルスをスキャンする対象を選択します。

詳細については、定期的に更新されるESETナレッジベース記事を参照してください。

# スケジューラで新しいタスクを作成する方法

[**ツール**]>[**スケジューラ**]で新しいタスクを作成するには、[**追加...**]をクリックするか、または右クリックしてコンテキストメニューから[**追加**]を選択します。次の5種類のスケジュールされたタスクが使用可能です。

- **外部アプリケーションの実行** – 外部アプリケーションの実行をスケジュールします。
- **ログの保守** –ログファイルには削除されたレコードの痕跡も収められています。このタスクは、効率的に運用するためにログファイル内のレコードを定期的に最適化します。
- **システムのスタートアップファイルのチェック** – システムの起動時またはログインに実行されるファイルを検査します。
- **コンピュータの状態のスナップショットを作成する** – ドライバーやアプリケーションなどのシステムコンポーネントについての情報を収集し、各コンポーネントのリスクレベルを評価するESET SysInspectorコンピュータスナップショットを作成します。
- **オンデマンドコンピュータの検査** – コンピュータ上のファイルやフォルダに関するコンピュータの検査を実行します。
- **アップデート**– モジュールをアップデートすることにより、アップデートタスクをスケジュールします。

スケジュールされたタスクの中で**アップデート**が最もよく使用されるので、新しいアップデートタスクを追加する方法を説明します。

**タスクの種類**ドロップダウンメニューから**アップデート**を選択します。**タスク名**フィールドにタスクの名前を入力し、[**次へ**]をクリックします。タスクの頻度を選択します。使用可能なオプションは**1回**、**繰り返し**、**毎日**、**毎週**、**イベントごとです。コンピューターがバッテリーで動作している場合は実行しない**を選択すると、ノートブックコンピュータのバッテリ電源での実行中に、システムリソースを最小化できます。タスクは、**タスクの実行**フィールドで指定された日時に実行されます。次に、スケジュールされた時刻にタスクを実行できない場合や完了できない場合に実行するアクションを定義します。使用可能なオプションは次のとおりです。

- **次のスケジュール設定日時まで待機**
- **実行可能になり次第実行する**
- **前回実行されてから次の時間が経過した場合は直ちに実行する(前回実行からの時間**スクロールボックスを使用して間隔を定義できます)

次のステップでは、現在のスケジュールされたタスクに関する情報が含まれる概要ウィンドウが表示されます。変更が完了したら、[**終了**]をクリックします。

ダイアログウィンドウが表示され、スケジュールされたタスクに使用するプロファイルを選択することができます。ここでは、プライマリプロファイルと代替プロファイルを設定できます。プライマリプロファイルを使用してタスクを完了できない場合は、代替プロファイルが使用されます。[**終了**]をクリックして確認し、新しくスケジュールされたタスクが、現在スケジュールされているタスクのリストに追加されます。

# 週次コンピューター検査をスケジュールする方法

定期的なタスクをスケジュールするには、プログラムのメインウィンドウを開き、**ツール**>**その他のツール** > スケジューラをクリックします。タスクをスケジュールする手順は次のとおりです。このタスクによって、ローカルドライブの検査が毎週実行されます。詳細な説明については、ナレッジベース記事を参照してください。

スキャンタスクをスケジュールするには:

1. スケジューラのメイン画面で**タスクの追加**をクリックします。
2. ドロップダウンメニューから[**コンピュータの検査**]を選択します。
3. タスクの名前を入力し**タスクの頻度に**[**毎週**]を選択します。
4. タスクを実行する日時を設定します。
5. スケジュールされたタスクの実行が何らかの理由で実行しない場合(コンピューターがオフの場合など)は、[**実行可能になりしだい実行する**]を選択して、後からタスクを実行します。
6. スケジュールされたタスクの概要を確認し、[**次へ**]をクリックします。
7. ドロップダウンメニューから**ローカルドライブ**を選択します。
8. [**終了**]をクリックすると、タスクが適用されます。

# ESET Endpoint AntivirusをESET PROTECTに接続する方法

コンピューターにESET Endpoint Antivirusをインストールし、ESET PROTECT経由で接続するときには、必ず、クライアントワークステーション上にESET Managementエージェントもインストールしたことを確認してください。これはESET PROTECTサーバーと通信するすべてのクライアントソリューションの不可欠の要素です。

- クライアントワークステーションにESET Managementエージェントをインストールまたは展開する

参照:

- リモート管理されたエンドポイントのドキュメント
- 上書きモードを使用する方法
- ESET Endpoint Antivirusの推奨されたポリシーを適用する方法

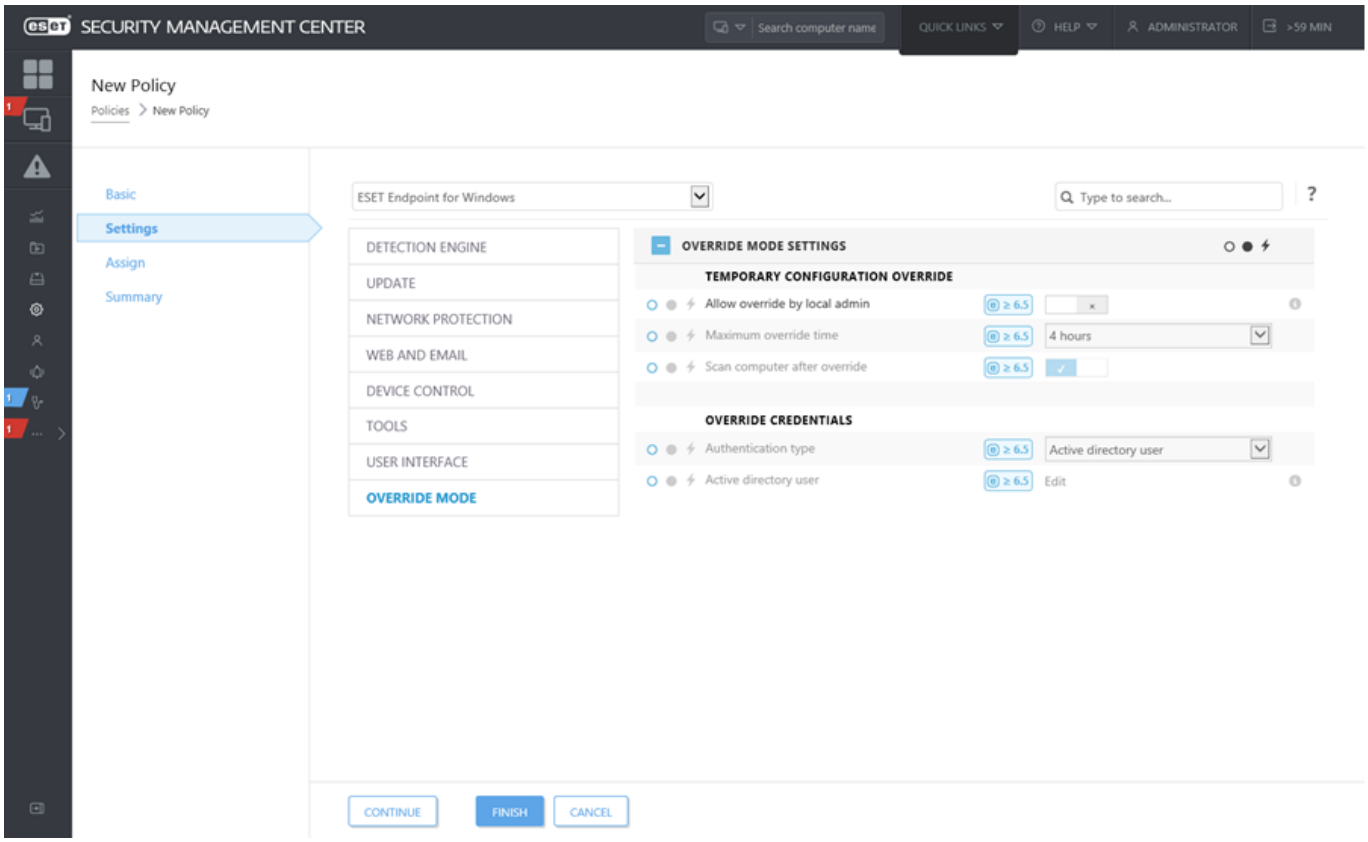
# 上書きモードを使用する方法

ESET Endpoint製品 for Windowsバージョン6.5以上)がコンピューターにインストールされている場合は、上書き機能を使用できます。上書きモードでは、設定が適用されたポリシーがある場合でも、クライアントコンピューターレベルで、インストールされたESET製品の設定を変更できます。上書きモードは、特定のADユーザーで有効にするか、パスワードで保護できます。この機能は、1回で4時間を超えると有効にできません。

上書きモードを1度有効にするとESET PROTECT Webコンソールから停止できます。上書き期間が終了すると、上書きモードは自動的に無効化されます。クライアントコンピューターでオフにすることもできます。
上書きモードを使用しているユーザーも、Windows管理者権限が必要です。それ以外の場合、ユーザーはESET Endpoint Antivirusの設定で変更を保存できません。
Active Directoryグループ認証がサポートされます。

**上書きモード**を設定するには

1. **ポリシー** > **新しいポリシー**に移動します。
2. [**基本**]セクションに、このポリシーの**名前**と**説明**を入力します。
3. [**設定**]画面で、**[ESET Endpoint for Windows]**を選択します。
4. [**上書きモード**]をクリックし、上書きモードのルールを設定します。
5. [**割り当て**]セクションで、このポリシーが適用されるコンピューターまたはコンピューターのグループを選択します。
6. [**サマリー**]セクションで、[**完了**]をクリックしてポリシーを適用します。



*John*のエンドポイント設定に問題があり、一部の重要な機能またはWebアクセスがコンピューターでブロックされる場合、管理者は*John*が既存のエンドポイントポリシーを上書きし、コンピューターで手動で設定を調整できるようにすることができます。後から、これらの新しい設定はESET PROTECTで要求されるため、管理者はそこから新しいポリシーを作成できます。
手順は次のとおりです。
1. **ポリシー > 新しいポリシー**に移動します。
2. **名前**および**説明**フィールドを入力します。[**設定**]画面で、**[ESET Endpoint for Windows]**を選択します。
3. [**上書きモード**]をクリックし、1時間上書きモードを有効にしADユーザーとして*John*を選択します。
4. *John*のコンピューターにポリシーを割り当て、[**完了**]をクリックしてポリシーを保存します。
5. *John*はESETエンドポイントで**上書きモード**を有効にし、コンピューターで手動で設定を変更する必要があります。
6. ESET PROTECT Webコンソールで、[**コンピューター**]に移動し、 *John*のコンピューターをクリックして、[**詳細を表示**]をクリックします。
7. [**設定**]セクションで、[**設定の要求**]をクリックして、クライアントタスクをスケジュールして、クライアントから設定をすぐに取得します。
8. 少したった後、新しい設定が表示されます。設定を保存する製品をクリックし、[**設定を開く**]をクリックします。
9. 設定を確認し、[**ポリシーに変換**]をクリックできます。
10. **名前**および**説明**フィールドを入力します。
11. [**設定**]セクションでは、必要に応じて設定を変更できます。
12. [**割り当て**]セクションで、このポリシーを*John*のコンピューター(またはその他)に割り当てることができます。
13. [**完了**]をクリックして設定保存します。
14. 必ず、必要がなくなった時点で、上書きポリシーを削除してください。

# ESET Endpoint Antivirusの推奨されたポリシーを適用する方法

ESET Endpoint AntivirusをESET PROTECTに接続した後のベストプラクティスは、推奨されたポリシーを適用するか、カスタムポリシーを適用することです。

ESET Endpoint Antivirusには複数の定義済みポリシーがあります。

| ポリシー | 説明 |
|---|---|
| ウイルス対策 – バランス重視 | ほとんどの設定に推奨されるセキュリティ設定。 |
| ウイルス対策 – 最大限のセキュリティ | 機械学習、詳細動作検査SSLフィルタリングを活用します。安全ではない可能性があるアプリケーション、望ましくない可能性があるアプリケーション、不審な可能性があるアプリケーションの検出に影響します。 |
| クラウドベースのレピュテーションおよびフィードバックシステム | ESET LiveGrid®クラウドベースのレピュテーションおよびフィードバックシステムは、最新の脅威の検出を向上し、悪意あるまたは未知の脅威を分析するのに役立ちます。 |
| デバイスコントロール – 最大限のセキュリティ | すべてのデバイスがブロックされます。デバイスを接続する場合は、管理者によって許可される必要があります。 |
| デバイスコントロール – 読み取り専用 | すべてのデバイスが読み取り専用です。書き込みはできません。 |

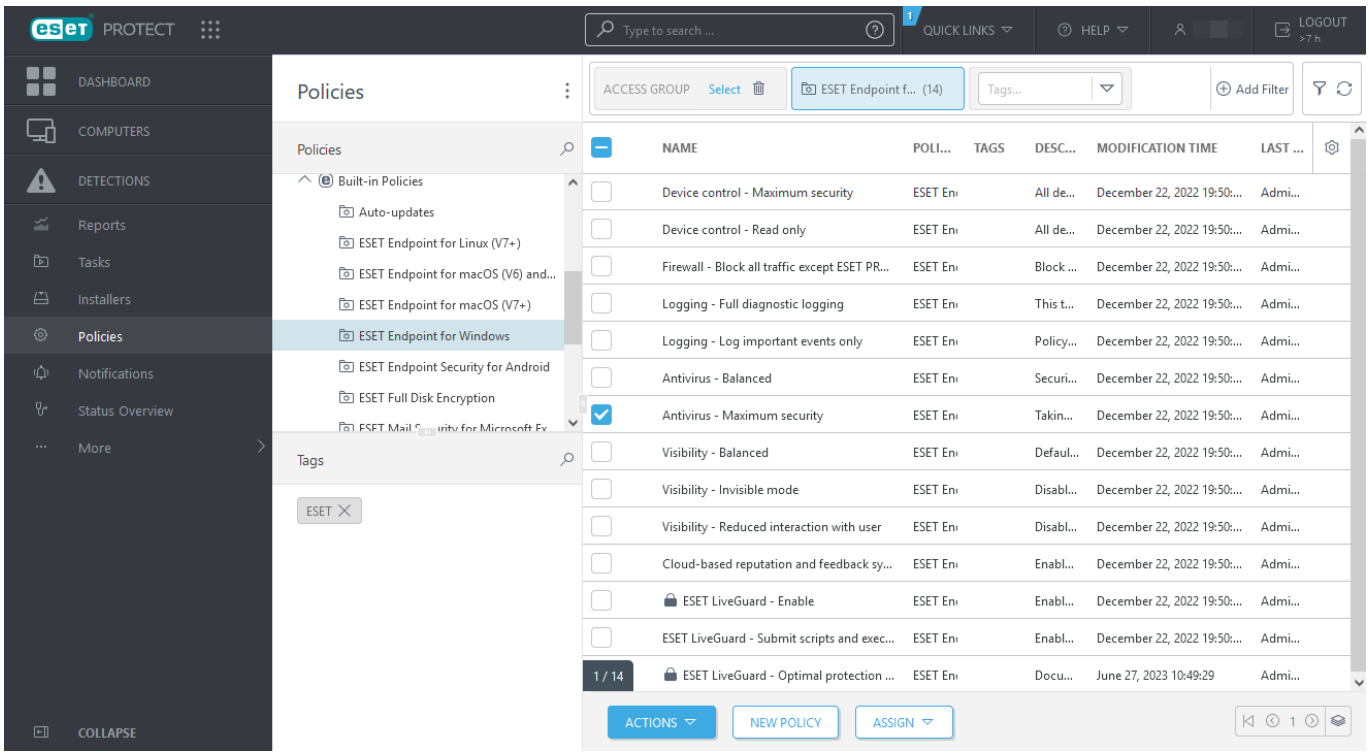
| ポリシー | 説明 |
| --- | --- |
| ファイアウォール - ESET PROTECT & ESET Inspect接続を除くすべてのトラフィックをブロック | ESET PROTECTおよびESET Inspect Server (ESET Endpoint Securityのみ)への接続を除くすべてのトラフィックをブロックします。 |
| ログ – 完全診断ログ | このテンプレートは、必要な場合に、管理者が使用可能なすべてのログを取得できることを保証します。HIPSとThreatSenseパラメーター、ファイアウォールを含む最小の詳細レベルからすべてが記録されます。ログは90日を経過すると自動的に削除されます。 |
| ログ – 重要なイベントのみを出力 | ポリシーは、警告、エラー、重大なイベントが記録されることを保証します。ログは90日を経過すると自動的に削除されます。 |
| 表示 – バランス重視 | 詳細レベルの既定の設定。ステータスと通知が無効です。 |
| 表示 – 非表示モード | 通知、アラート、GUIのコンテキストメニューとの統合が無効です。egui.exeは実行されません。ESET PROTECT Cloudのみからの管理に適しています。 |
| 表示 – ユーザーの操作を減らす | ステータスと通知が無効で、GUIは表示されます。 |

---

ワークステーションにインストールされたESET Endpoint Antivirus向けに51個以上の推奨設定を施行する**ウイルス対策 – 最大限のセキュリティ**のポリシーを設定するには、次の手順に従います。

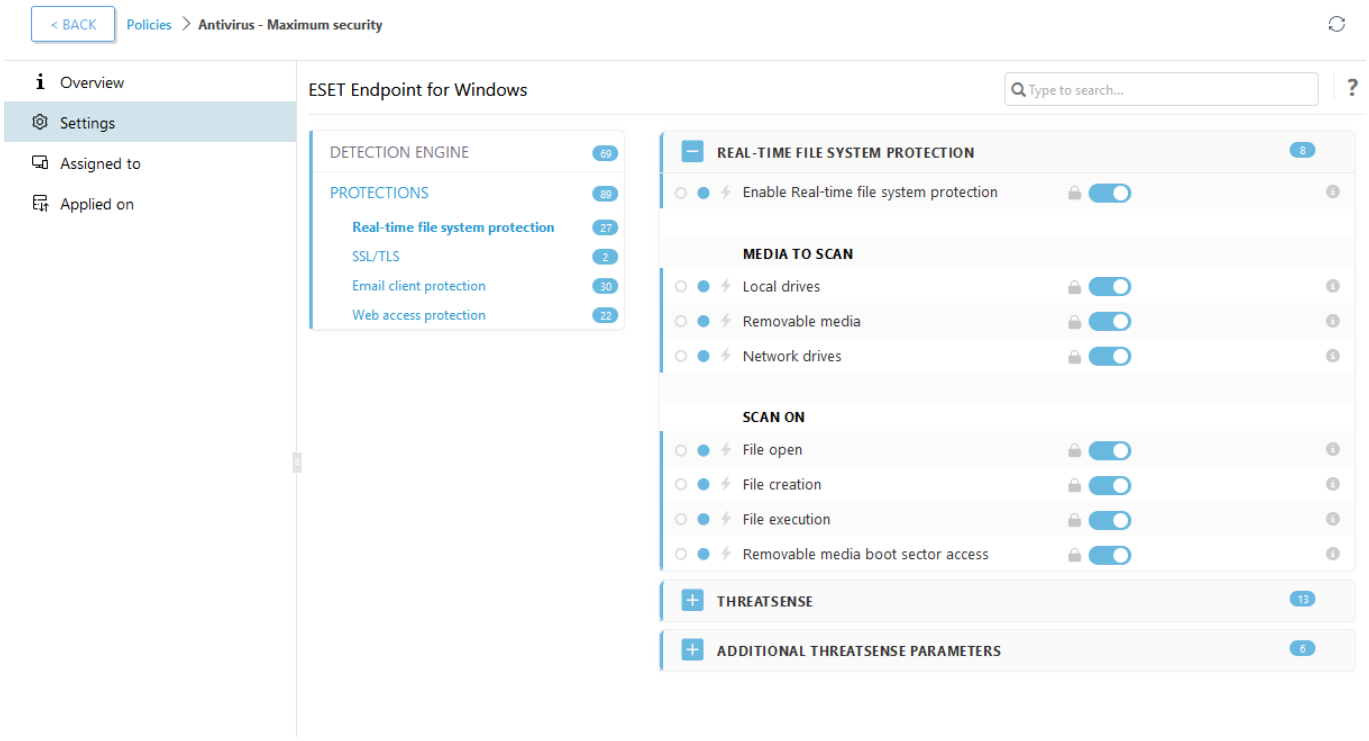
次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
ESET PROTECTを使用して ESET Endpoint Antivirusの推奨または定義済みポリシーを適用する

1. ESET PROTECT Webコンソールを開きます。
2. **ポリシー**に移動して、**ビルトインポリシー > ESET Endpoint for Windows**を展開します。
3. **ウイルス対策 – 最大限のセキュリティ – 推奨**をクリックします。
4. **割り当て先**タブで、**クライアントの割り当て**または**グループの割り当て**をクリックし、このポリシーを適用する適切なコンピューターを選択します。



このポリシーに適用される設定を確認するには、**設定**タブをクリックして、詳細設定ツリーを展開します。

- 青色の点は、このポリシーの変更された設定を表します。
- 青色の枠の中の数字は、このポリシーによって変更された設定数を表します。
- ESET PROTECTポリシーの詳細




# ミラーを構成する方法

ESET Endpoint Antivirusは検出エンジンアップデートファイルのコピーを保存し、ESET Endpoint AntivirusまたはESET Endpoint Securityを実行している他のワークステーションにアップデートを配布するように設定できます。

アップデートミラーは、同じ世代のESET Endpoint Antivirus for Windowsを実行するワークステーションをアップデートするために使用できるアップデートファイルのコピーを作成します。(たとえばESET Endpoint Antivirus for Windowsバージョン10.xはバージョン10.x (ESET Endpoint Antivirus for WindowsとESET Endpoint Security for Windows)のアップデートファイルのみを作成します)

## ESET Endpoint Antivirusをミラーとして構成し、内部HTTPサーバー経由でアップデートを配布する

1. **F5**を押して、詳細設定にアクセスし、**アップデート > プロファイル > アップデートミラー**を展開します。
2. **アップデート**を展開し、**モジュールアップデート**の**自動的に選択**オプションが有効になっていることを確認します。
3. **アップデートミラー**を展開し、**アップデートミラーを作成する**と**HTTPサーバーを有効にする**を有効にします。

詳細については、次の項目を参照してください。
- 配布用アップデート
- ミラーからのアップデート

## 共有ネットワークフォルダ経由でアップデートを配布するようにミラーサーバーを構成する

1. ローカルまたはネットワークドライブで共有フォルダを作成します。このフォルダはESETセキュリティソリューションを実行するすべてのユーザーによって読み取られ、ローカルSYSTEMアカウントから書き込み可能でなければなりません。
2. **詳細設定** > **アップデート** > **プロファイル** > **アップデートミラー**の下で、**アップデートミラーを作成する**を有効にします。
3. **クリア**⍰**編集**の順にクリックして、該当する**保存フォルダー**を選択します。作成された共有フォルダーを選択します。

内部HTTPサーバー経由でモジュールのアップデートを提供しない場合は、**HTTPサーバーを有効にする**を無効にします。

# ESET Endpoint Antivirusがインストールされた状態でWindows 10にアップグレードする方法

最新バージョンのESET製品にアップグレードしてから、最新のモジュールアップデートをダウンロードした後に、Windows 10にアップグレードすることを強くお勧めします。これにより、最大の保護が保証されⓇWindows 10へのアップグレード中にプログラム設定とライセンス情報が保持されます。

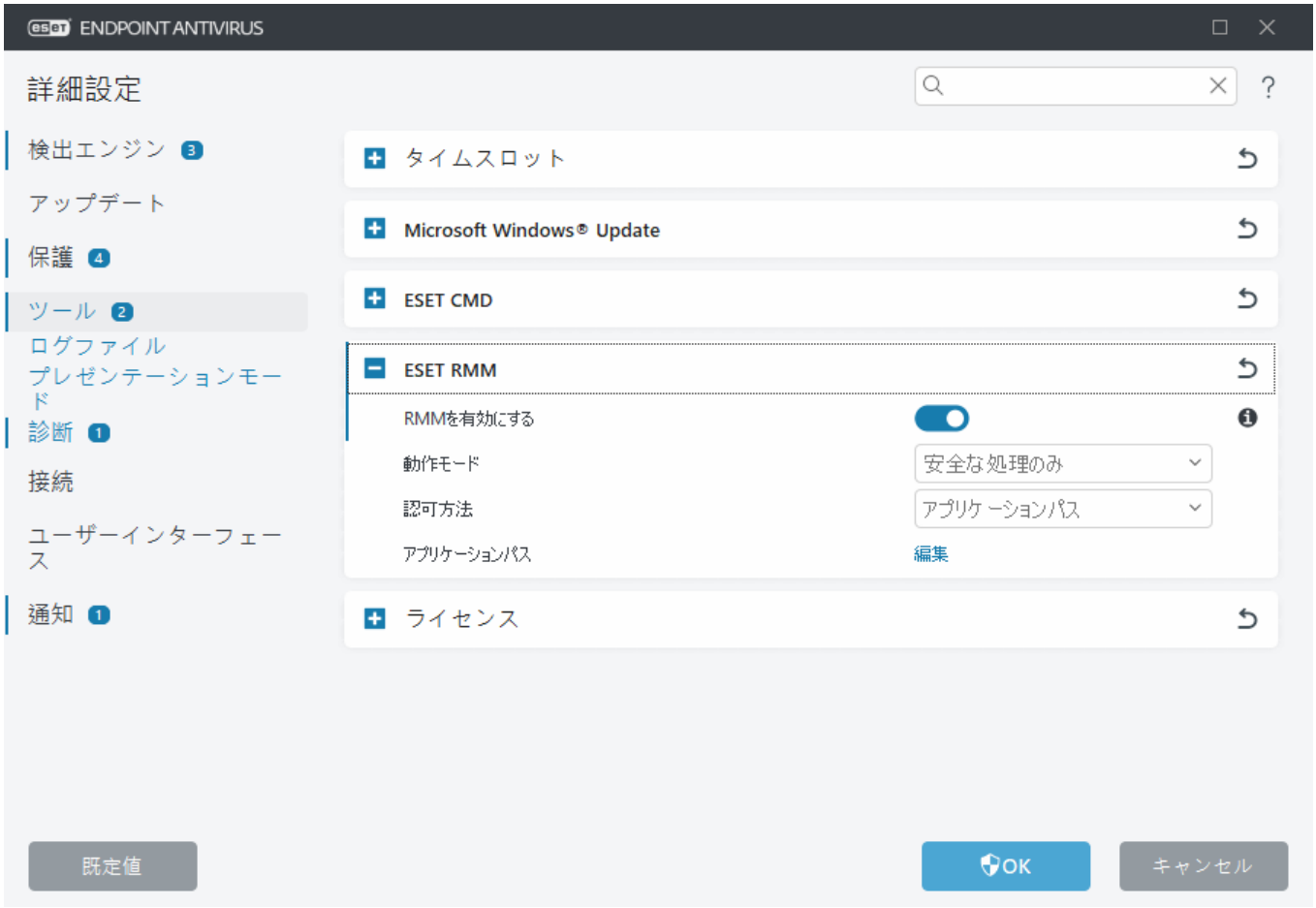
## その他の言語バージョン:

別の言語バージョンのESETエンドポイント製品を探している場合は、ESETのダウンロードページをご覧くださいⓇ

ESETビジネス製品とWindows 10の互換性に関する情報Ⓡ

# リモート監視と管理をアクティブ化する方法

リモート監視と管理(RMM)は、管理サービスプロバイダーがアクセスできるローカルにインストールされたエージェントを使用して、ソフトウェアシステム(デスクトップ、サーバー、モバイルデバイスにインストールされたシステムなど)を監視および制御するプロセスですⓇESET Endpoint Antivirusは、バージョン6. 6. 2028. 0からRMMで管理できます。




既定では□ESET RMMは無効です□ESET RMMを有効にするには、詳細設定 > **ツール** > **ESET RMM**を開き、**RMMを有効にする**の横にあるトグルを有効にします。

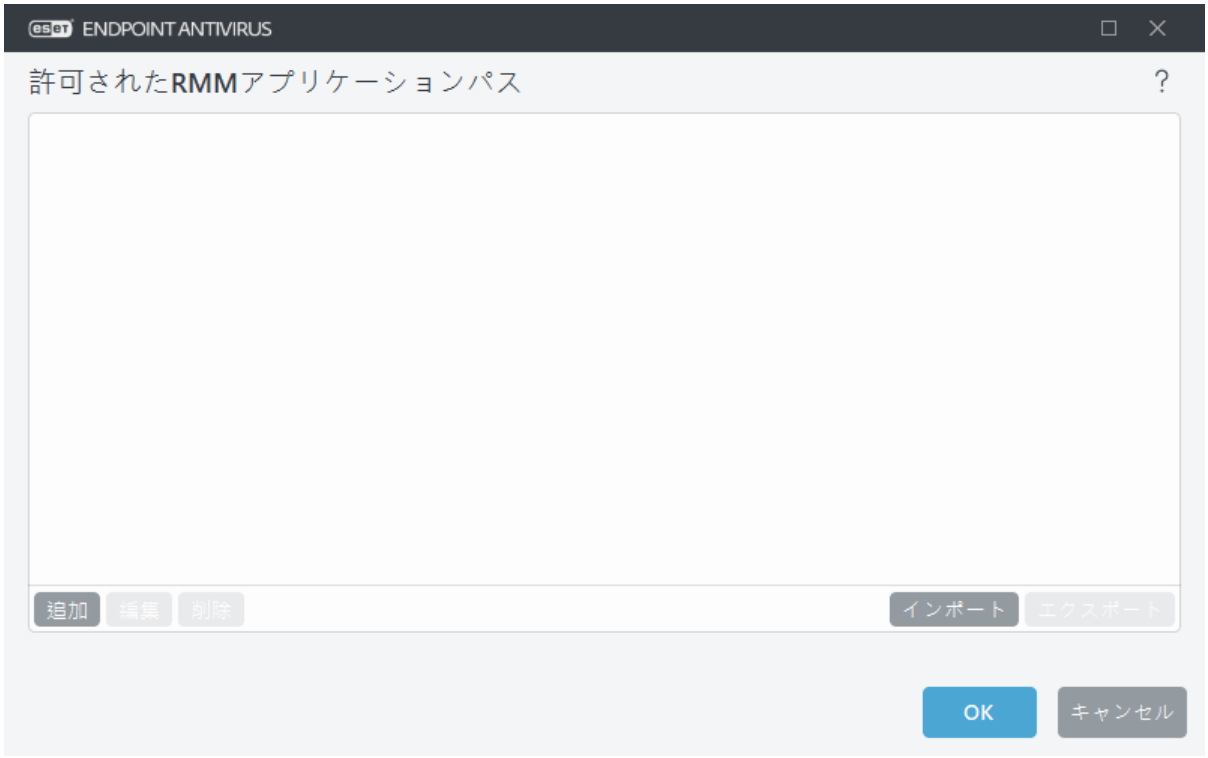
**動作モード** – 安全な読み取り専用操作用にRMMインターフェースを有効にする場合は、**安全な操作のみ**を選択します。すべての操作でRMMインターフェースを有効にする場合は、**すべての操作**を選択します。

| 処理 | モード安全な操作のみ | モードすべての操作 |
|---|---|---|
| アプリケーション情報の取得 | ✔ | ✔ |
| 設定の取得 | ✔ | ✔ |
| ライセンス情報の取得 | ✔ | ✔ |
| ログの取得 | ✔ | ✔ |
| 保護の状態の取得 | ✔ | ✔ |
| アップデート状態の取得 | ✔ | ✔ |
| 構成の設定 | | ✔ |
| アクティベーションの開始 | | ✔ |
| 検査の開始 | ✔ | ✔ |
| アップデートの開始 | ✔ | ✔ |

**認証方法**–RMM認証方法を設定します。認証を使用するには、ドロップダウンメニューから[**アプリケーションパス**]を選択するか、[**なし**]を選択します。

RMMは常に認証を使用し、悪意のあるソフトウェアがESETエンドポイント保護を無効化または回避できないようにする必要があります。

**アプリケーションパス** – RMMを実行できる特定のアプリケーション。認証方法として**アプリケーションパス**を選択した場合は、**編集**をクリックして、**許可されたRMMアプリケーションパス**設定ウィンドウを開きます。




**追加** – 新しい許可されたRMMアプリケーションパスを作成します。パスを入力するか、**...**ボタンをクリックして実行ファイルを選択します。

**[編集]** – 既存の許可されたパスを変更します。実行ファイルの場所が別のフォルダーに変更された場合は、**[編集]**を使用します。

**[削除]** – 既存の許可されたパスを削除します。

既定のESET Endpoint Antivirusインストールには、Endpointアプリケーションディレクトリ(既定のパス*C:\Program Files\ESET\ESET Security*)にあるermm.exeファイルがあります。ermm.exeはRMMエージェントと通信し、RMMサーバーにリンクされたRMMプラグインとデータを交換します。

- ermm.exe – ESETによって開発されたコマンドラインユーティリティで、Endpoint製品の管理とRMMプラグインとの通信ができます。
- RMMプラグインはEndpoint Windowsシステムでローカルで実行される他社のアプリケーションです。このプラグインは、特定のRMMエージェント(Kaseyaのみなど)とermm.exeと通信するために設計されました。
- RMMエージェントはEndpoint Windowsシステムでローカルで実行される他社のアプリケーションです。エージェントはRMMプラグインとRMMサーバーと通信します。

# インターネットから特定のファイルタイプのダウンロードをブロックする方法

インターネットから特定のファイルタイプ(exe、pdf、zipなど)のダウンロードを許可しない場合は、URLアドレス管理とワイルドカードを組み合わせて使用します。F5キーを押して、**詳細設定**にアクセスします。**[Webとメール] > [Webアクセス保護]**をクリックし、**[URLアドレス管理]**を展開します。**アドレスリ**

ストの横の[**編集**]をクリックします。

**アドレスリスト**ウィンドウで、**ブロックされたアドレスのリスト**を選択し、**編集**をクリックするか、**追加**をクリックして、リストを作成または編集します。新しいウィンドウが開きます。新しいリストを作成している場合は、**アドレスリストタイプ**ドロップダウンメニューから**ブロック**を選択し、リスト名を指定します。現在のリストからファイルタイプにアクセスするときに通知する場合は、**適用するときに通知**サイドバーを有効にします。ドロップダウンメニューから**ログの重要度**を選択しますESET PROTECTは**警告**詳細レベルのレコードを集めることができます。

情報と警告ロギングの詳細レベルは、ドメイン内にワイルドカードを使用せずに2つ以上のコンポーネントを含むルールでのみ使用できます。例:
- *.domain.com/*
- *www.domain.com/*


[**追加**]をクリックすると、ダウンロードをブロックするファイルタイプを指定するマスクを入力できます。特定のWebサイトからの特定のファイルのダウンロードをブロックする場合は、完全なURL (例: *http://example.com/file.exe*) を入力します。ワイルドカードを使用すると、複数のファイルを指定することができます。疑問符 (?) は1つの可変文字を表し、アスタリスク (*) は0文字以上の可変文字列を表します。たとえば、マスク **/*.zip*はすべての圧縮されたzipファイルのダウンロードをブロックします。

ファイル拡張子がファイルURLの一部であるときに、この方法を使用して、特定のファイルタイプのダ

ウンロードのみをブロックできます。Webページでファイルダウンロードを使用する場合(例: *www.example.com/download.php?fileid=42*)、このリンクにあるすべてのファイルは、拡張子をブロックした場合でも、ダウンロードされます。

# ESET Endpoint Antivirusユーザーインターフェースを最小化する方法

リモートで管理するときには、「表示」定義済みポリシーを適用できます。

そうでない場合は、手動で次の手順を実行します。

1. **F5**キーを押して詳細設定を開き、**ユーザーインターフェース > ユーザーインターフェース要素**を展開します。
2. **起動モード**を必要な値に設定します。起動モードの詳細について
3. **起動時にスプラッシュ画面を表示**と**サウンド信号を使用**を無効にします。
4. 通知を設定します。
5. アプリケーションステータスを設定します。
6. 確認メッセージを設定します。
7. アラートとメッセージボックスを設定します。

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

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

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

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

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

c) **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□□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□□EOLポリシー、ドキュメントまたはその一部を改訂する権利を留保します。これらの条項の改訂は、電子メール、アプリ内通知、または他の電子的な手段で通知されます。お客様が本契約の変更の提案に同意しない場合は、変更の通知を受領してから30日以内にアカウントまたは影響を受ける購入済みのサービスを解約できます。この期限内に本契約を解約しない場合は、提案された変更が承認されたと見なされ、変更の通知を受け取った日時点でお客様側で変更が有効になります。

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

EULAID: EULA-PRODUCT-LG; 3537.0

# プライバシーポリシー

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。

ESETは、処理するすべての情報が重要であり、お客様へのサービスおよび製品の提供という正当な利益のために必要であると考えています。

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