ESET Security Ultimate

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 Security Ultimate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 Security Ultimate

ESETSecurityUltimateは、新しいアプローチにより真に堅牢なコンピューターセキュリティを実現します。最新バージョンのESET LiveGrid®検査エンジンは、ファイアウォールおよび迷惑メール対策機能を備え、ご使用中のコンピューターを高い精度と速度をもって安全に保ちます。 これにより、このインテリジェントシステムは、コンピュータにとって脅威となる可能性のある攻撃と不正ソフトウェアに対して常に警戒態勢を保ちます。

ESETSecurityUltimateは、最大の保護機能と最小のメモリ使用率を兼ね備えた究極の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、コンピューター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、その他の脅威の侵入を阻止します。

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 Security Ultimate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機能は、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 Security Ultimate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。
デバイスコントロール	すべてのUSBフラッシュドライブ、メモリカード、およびCD/DVDを自動的に検査します。またメディアの種類、メーカー、サイズなどの属性に基づいて、リムーバブルメディアをブロックできます。
HIPSの機能	システムの動作を詳細にカスタマイズできます。システムレジストリやアクティブなプロセスとプログラムのルールを指定し、セキュリティ設定を微調整できます。
ゲームモード	ゲームなど全画面モード中に、すべてのポップアップウィンドウ、更新、およびその他のシステムの集中的な活動を延期し、システムリソースの最小化を行います。

ESET Security Ultimateの機能

バンキングとブラウジング保護	すべてのオンライン取引が信頼できる、安全な環境の中で確実に行われるよう、バンキングとブラウジング保護はオンラインバンキングとオンライン決済ゲートウェイにアクセスする時に保護されたブラウザーを提供します。

ネットワークシグネチャのサポート	ネットワークシグネチャは、ボットやエクスプロイトキットに関連したユーザーデバイスからくる悪意あるトラフィックをすばやく特定し、ブロックを可能にするものです。この機能はボットネット保護の拡張機能とお考えください。
インテリジェントファイアウォール	認証されていないユーザーがコンピューターにアクセスして個人データを利用することを防ぎます。
電子メールクライアント迷惑メール対策	迷惑メールは全メール通信の実に50%も占めています。電子メールクライアント迷惑メール対策は、この問題から保護します。
アンチセフト	アンチセフトは、コンピューターの紛失、盗難の際のセキュリティを拡張するものです。ESET Security Ultimateとアンチセフトをインストールすると、ユーザーのデバイスがWebインターフェースに表示されます。Webインタフェースを使用して、ユーザーはデバイスでアンチセフトの設定を管理し、アンチセフトの機能を管理できます。
ペアレンタルコントロール	さまざまな分類のWebサイトをブロックし、不適切と考えられるWebコンテンツから家族を保護します。
Password Manager	Password Managerは、パスワードと個人データを保護して保存します。
Secure Data	Secure Dataでは、コンピューターおよびリムーバブルドライブのデータを暗号化し、個人情報や機密情報の悪用を防止します。
ESET LiveGuard	未知の脅威を検出し、阻止し、将来の検出のために情報を処理します。
VPN	データを安全に保ち、不要な追跡を回避し、匿名IPアドレスでセキュリティを強化してオンラインのプライバシーを高めます。
ESET Identity Protection	個人情報、信用情報、財務情報を保護します。ESET Identity Protectionは継続的な監視を提供することにより、個人情報の違法な販売を検出します。

ESET Security Ultimateの機能を動作させるには、サブスクリプションがアクティブである必要があります。ESET Security Ultimateのサブスクリプションの有効期限が切れる数週間前にサブスクリプションを更新することをお勧めします。

新機能

ESET Security Ultimate17.1の新機能

- ネットワーク検査の小規模な改善
- バンキングとブラウジング保護の小規模な改善
- ESET LiveGuard- ドキュメントの送信が既定で有効になりました
- その他の軽微なバグ修正と改善

新機能の通知を無効にするには：
1. 詳細設定 > **通知** > **デスクトップ通知**を開きます。
2. **デスクトップ通知**の横にある**編集**をクリックします。
3. **新機能の通知を表示する**チェックボックスをオフにして、**OK**をクリックします。
通知の詳細については、通知セクションを参照してください。

ESET Security Ultimateの変更点の詳細なリストについては、ESET Security Ultimate変更ログを参照してください。

使用している製品の見分け方

強力で高速なウイルス対策ソリューションから、システム負荷を最小限に抑えたオールインワンセキュリティソリューションまで、新しい製品には複数のレイヤーのセキュリティがあります。

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**
- **ESET Security Ultimate**

インストールされた製品を確認するには、メインプログラムウィンドウを開きます。ウィンドウの上部に製品名が表示されます(ナレッジベース記事を参照)。

以下の表は、各製品で提供されている詳細な機能を示します。

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
検出エンジン	✔	✔	✔	✔
高度な機械学習	✔	✔	✔	✔
エクスプロイトブロッカー	✔	✔	✔	✔
スクリプトに基づく攻撃保護	✔	✔	✔	✔
フィッシング対策	✔	✔	✔	✔
Webアクセス保護	✔	✔	✔	✔
HIPS（ランサムウェア保護を含む）	✔	✔	✔	✔
迷惑メール対策		✔	✔	✔
ファイアウォール		✔	✔	✔
ネットワーク検査		✔	✔	✔
Webカメラ保護		✔	✔	✔
ネットワーク攻撃保護		✔	✔	✔
ボットネット保護		✔	✔	✔
バンキングとブラウジング保護		✔	✔	✔
ブラウザーのプライバシーおよびセキュリティ		✔	✔	✔
ペアレンタルコントロール		✔	✔	✔
アンチセフト		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

上記の製品の一部については、お客様の言語または地域で使用できないことがあります。

システム要件

ESET Security Ultimateを最適に実行するには、システムで次のハードウェアおよびソフトウェア要件を満たす必要があります。

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

サポートされているオペレーティングシステム

Microsoft® Windows® 11

Microsoft® Windows® 10

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

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。

ESET Security Ultimate機能要件

次の表の特定のESET Security Ultimate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。
バンキングとブラウジング保護	サポートされているWebブラウザを参照してください。
透明の背景	Windows 10バージョンRS4以降。
専用駆除アプリケーション	非ARM64ベースのプロセッサー。
システムクリーナー	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。

その他

アクティベーションとESET Security Ultimateアップデートの正常な機能には、インターネット接続が必要です。

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。

古いバージョンのMicrosoft Windows

問題

- Windows 7、Windows 8 (8.1)またはWindows Home Server 2011が動作しているコンピューターで最新バージョンのESET Security Ultimateをインストールする
- インストール中に、ESET Security Ultimateで**古いオペレーティングシステム**のエラーが表示される

詳細

最新バージョンのESET Security Ultimateでは、Windows 10またはWindows 11オペレーティングシステムが必要です。

解決策

使用可能な解決策は次のとおりです。

Windows 10またはWindows 11にアップグレードする

アップグレードプロセスは比較的簡単です。多くの場合、ファイルが消去される心配なく実行できます。Windows 10にアップグレードする前に、次の手順を実行します。

1. 重要なデータをバックアップする
2. MicrosoftのWindows 10へのアップグレードFAQまたはWindows 11 FAQへのアップグレードを読み、Windowsオペレーティングシステムを更新してください。

ESET Security Ultimateバージョン 16.0のインストール

Windowsをアップグレードできない場合は、バージョンESET Security Ultimate 16.0をインストールします。詳細については、ESET Security Ultimateバージョン16.0オンラインヘルプを参照してください。

セキュリティの考え方

コンピュータを使用するとき、特にインターネットを利用する場合には、攻撃や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使用し、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のリサーチラボの担当者は、ユーザーの保護レベルを改善するために、これらのウイルスを毎日解析し、更新ファイルを作成してリリースしています。これらの最新版の効果を最大限生かすためには、システムのアップデートを正しく設定することが重要です。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さまざまな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Internet ExplorerなどのWebブラウザは、更新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、重要なデータを喪失させることがよくあります。重要なデータや機密データは、DVDや外付けハードディスクなどの外部メディアに定期的にバックアップすることが重要です。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は、リアルタイムファイルシステム保護機能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 Security Ultimate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 Security Ultimateを使用する前に、コンピューターの使用中に発生することが考えられるさまざまな検出の種類とリモート攻撃について読むことができます。またESET Security Ultimateで導入された新機

能の一覧も用意されています。

まず、ESET Security Ultimateをインストールします。既にESET Security Ultimateがインストールされている場合は、ESET Security Ultimateの操作を参照してください。

ESET Security Ultimateヘルプページの使用方法

オンラインヘルプは複数の章とサブ章に分かれています。ESET Security UltimateでF1を押すと、現在開いているウィンドウに関する情報が表示されます。

このプログラムでは、ヘルプトピックをキーワードで検索したり、語句を入力して内容を検索したりできます。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、その語句が本文中に実際に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 Security Ultimateユーザーインターフェースに基づいています。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、重大ではないが重要な情報が表示されます。

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。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。

インストール

コンピュータにESET Security Ultimateをインストールするには、いくつかの方法があります。インストール方法は、国、および配布方法によって異なります。

- ライブインストーラーは、ESET WebサイトまたはCD/DVDからダウンロード可能です。インストー

ルパッケージは、すべての言語で共通です(該当する言語を選択してください)。ライブインストーラー自体は小さなファイルです。ESET Security Ultimateのインストールに必要な追加ファイルは、自動的にダウンロードされます。

- オフラインインストール – ライブインストーラーファイルよりも大きい.exeファイルを使用します。インストールを完了するためにインターネット接続または追加ファイルが必要はありません。

ESET Security Ultimateをインストールする前に、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て下さい。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、ESETナレッジベースの記事を参照してください。

ライブインストーラー

ライブインストーラーインストールパッケージをダウンロードする場合は、インストールファイルをダブルクリックして、インストールウィザードの手順に従います。

このタイプのインストールでは、インターネットに接続する必要があります。

1. 該当する言語をドロップダウンメニューから選択し、**続行**をクリックします。

パスワードで保護された設定を使用して、前のバージョンよりも新しいバージョンをインストールしている場合は、パスワードを入力します。アクセス設定では設定パスワードを構成できます。

2. 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があるアプリケーション
- カスタマーエクスペリエンス改善プログラム

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。

3. ESET HOMEを使用して、デバイスのセキュリティをアクティベーション、管理、表示するには、デバイスをESET HOMEアカウントに接続します。**ログインのスキップ**をクリックするとESET HOMEに接続せずに続行します。後からデバイスをESET HOMEアカウントに接続できます。

4. ESET HOMEに接続せずに続行する場合は、アクティベーションオプションを選択します。前のバージョンの上に新しいバージョンをインストールしている場合は、**製品認証キー**が自動的に入力されます。

5. インストールウィザードは、サブスクリプションに基づいて、インストールされるESET製品を決定します。セキュリティ機能が最も充実しているバージョンが常にあらかじめ選択されています。別のバージョンのESET製品をインストールする場合は、**製品を選択**をクリックします。**続行**をクリックすると、インストール処理が開始します。これにはしばらく時間がかかる場合があります。

過去にアンインストールされたESET製品の残り(ファイルまたはフォルダー)がある場合は、削除を許可するようにプロンプトで表示されます。**インストール**をクリックして続行します。

6. **完了**をクリックすると、インストールウィザードが終了します。

インストールのトラブルシューティングツール

製品がインストールおよびアクティベーションされた後、モジュールのダウンロードが開始します。保護が初期化されます。ダウンロードが完了していない場合は、一部の機能が完全に機能しない場合があります。

オフラインインストール

以下のオフラインインストーラ(.exe)を使用してESETWindowsホーム製品をダウンロードしてインストールします。ダウンロードするESETホーム製品のバージョンを選択します(32ビット、64ビット、またはARM)

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
64ビットダウンロード 32ビットダウンロード ARMダウンロード	64ビットダウンロード 32ビットダウンロード ARMダウンロード	64ビットダウンロード 32ビットダウンロード ARMダウンロード	64ビットダウンロード 32ビットダウンロード ARMダウンロード

アクティブなインターネット接続がある場合は、ライブインストーラーを使用してESET製品をインストールします

オフラインインストーラ(.exe)を起動すると、インストールウィザードが表示され、セットアップ処理を案内します。

1. 該当する言語をドロップダウンメニューから選択し、**続行**をクリックします。

パスワードで保護された設定を使用して、前のバージョンよりも新しいバージョンをインストールしている場合は、パスワードを入力します。アクセス設定では設定パスワードを構成できます。

2. 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があるアプリケーション
- カスタマーエクスペリエンス改善プログラム

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。

3. **ログインのスキップ**をクリックします。インターネットに接続すると、デバイスをESET HOMEアカウントに接続できます。

4. **アクティベーションのスキップ**をクリックしますESET Security Ultimateが完全に機能するには、インストール後にアクティベーションする必要があります。製品のアクティベーションには、アクティブなインターネット接続が必要です。

5.インストールウィザードは、ダウンロードされたオフラインインストーラーに基づいて、インストールされるESET製品を表示します。**続行**をクリックすると、インストール処理が開始します。これにはしばらく時間がかかる場合があります。

過去にアンインストールされたESET製品の残り(ファイルまたはフォルダー)がある場合は、削除を許可するようにプロンプトで表示されます。**インストール**をクリックして続行します。

6. **完了**をクリックすると、インストールウィザードが終了します。

インストールのトラブルシューティングツール

サブスクリプションアップグレード

この通知ウィンドウは、ESET製品をアクティベーションするために使用されているサブスクリプションが変更されたときに表示されます。変更されたサブスクリプションにより、セキュリティ機能が多い製品をアクティベーションできます。変更が実行されていない場合ESETSecurityUltimateは1回アラートウィンドウを表示し、**機能が充実した製品への変更**を確認します。

はい（推奨） – セキュリティ機能が追加された製品が自動的にインストールされます。

いいえ – 変更は行われず、通知は完全に消去されます。

後から製品を変更するには、ESETナレッジベース記事を参照してくださいESETサブスクリプションの詳細については、サブスクリプションFAQを参照してください。

以下の表は、各製品で提供されている詳細な機能を示します。

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
検出エンジン	✔	✔	✔	✔
高度な機械学習	✔	✔	✔	✔
エクスプロイトブロッカー	✔	✔	✔	✔
スクリプトに基づく攻撃保護	✔	✔	✔	✔
フィッシング対策	✔	✔	✔	✔
Webアクセス保護	✔	✔	✔	✔
HIPSランサムウェア保護を含む）	✔	✔	✔	✔
迷惑メール対策		✔	✔	✔
ファイアウォール		✔	✔	✔
ネットワーク検査		✔	✔	✔
Webカメラ保護		✔	✔	✔
ネットワーク攻撃保護		✔	✔	✔
ボットネット保護		✔	✔	✔
バンキングとブラウジング保護		✔	✔	✔
ブラウザーのプライバシーおよびセキュリティ		✔	✔	✔
ペアレンタルコントロール		✔	✔	✔
アンチセフト		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

製品のアップグレード

既定のインストーラーをダウンロードし、アクティベーションする製品を変更することを決定したか、インストールされている製品をセキュリティ機能が多い製品に変更しようとしています。

インストール中に製品を変更します

以下の表は、各製品で提供されている詳細な機能を示します。

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
検出エンジン	✔	✔	✔	✔
高度な機械学習	✔	✔	✔	✔
エクスプロイトブロッカー	✔	✔	✔	✔
スクリプトに基づく攻撃保護	✔	✔	✔	✔
フィッシング対策	✔	✔	✔	✔
Webアクセス保護	✔	✔	✔	✔
HIPSランサムウェア保護を含む）	✔	✔	✔	✔
迷惑メール対策		✔	✔	✔
ファイアウォール		✔	✔	✔
ネットワーク検査		✔	✔	✔
Webカメラ保護		✔	✔	✔
ネットワーク攻撃保護		✔	✔	✔
ボットネット保護		✔	✔	✔
バンキングとブラウジング保護		✔	✔	✔
ブラウザーのプライバシーおよびセキュリティ		✔	✔	✔
ペアレンタルコントロール		✔	✔	✔
アンチセフト		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

サブスクリプションダウングレード

このダイアログは、ESET製品をアクティベーションするために使用されているサブスクリプションが変更されたときに表示されます。変更されたサブスクリプションは、セキュリティ機能が少ない、別のESET製品でのみ使用できます。製品は、保護が失われないように、自動的に変更されました。

ESETサブスクリプションの詳細については、サブスクリプションFAQを参照してください。

以下の表は、各製品で提供されている詳細な機能を示します。

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
検出エンジン	✔	✔	✔	✔
高度な機械学習	✔	✔	✔	✔
エクスプロイトブロッカー	✔	✔	✔	✔
スクリプトに基づく攻撃保護	✔	✔	✔	✔
フィッシング対策	✔	✔	✔	✔
Webアクセス保護	✔	✔	✔	✔
HIPS（ランサムウェア保護を含む）	✔	✔	✔	✔
迷惑メール対策		✔	✔	✔
ファイアウォール		✔	✔	✔
ネットワーク検査		✔	✔	✔
Webカメラ保護		✔	✔	✔
ネットワーク攻撃保護		✔	✔	✔
ボットネット保護		✔	✔	✔
バンキングとブラウジング保護		✔	✔	✔
ブラウザーのプライバシーおよびセキュリティ		✔	✔	✔
ペアレンタルコントロール		✔	✔	✔
アンチセフト		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

製品のダウングレード

現在インストールされている製品には、アクティベーションしようとしている製品よりも多くのセキュリティ機能があります（VPN、ID保護、Secure Data、Password Managerはこの製品では利用できません。暗号化されたファイルを作成できません。

以下の表は、各製品で提供されている詳細な機能を示します。

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
検出エンジン	✔	✔	✔	✔
高度な機械学習	✔	✔	✔	✔
エクスプロイトブロッカー	✔	✔	✔	✔
スクリプトに基づく攻撃保護	✔	✔	✔	✔
フィッシング対策	✔	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Webアクセス保護	✔	✔	✔	✔
HIPS（ランサムウェア保護を含む）	✔	✔	✔	✔
迷惑メール対策		✔	✔	✔
ファイアウォール		✔	✔	✔
ネットワーク検査		✔	✔	✔
Webカメラ保護		✔	✔	✔
ネットワーク攻撃保護		✔	✔	✔
ボットネット保護		✔	✔	✔
バンキングとブラウジング保護		✔	✔	✔
ブラウザーのプライバシーおよびセキュリティ		✔	✔	✔
ペアレンタルコントロール		✔	✔	✔
アンチセフト		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

インストールのトラブルシューティングツール

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。

インストール後の最初の検査

ESET Security Ultimateをインストールすると、最初のアップデートが成功した後に、コンピュータは悪意のあるコードをチェックするために自動的に検査を開始します。

コンピューターの検査は、プログラムのメインウィンドウで**[コンピューターの検査]** > **[コンピューターの検査]**をクリックして手動で開始することもできます。コンピュータの検査の詳細は、「コンピュータの検査」セクションを参照してください。

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 Security Ultimateの新バージョンが提供されています。新しい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. 自動で、プログラムアップデートを利用する方法。
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** > **アップデート**で、**アプリケーション機能アップデート**を有効にしたことを確認してください。

2. 手動で、メインプログラムウィンドウで、**アップデート**セクションの**最新版のチェック**をクリックします。

3. 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。

詳細と図解による手順については、次を参照してください。

- ESET製品のアップデート—最新の製品モジュールの確認
- ESET製品のアップデートとリリースタイプ

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製品の有効なサブスクリプション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とカスタマーエクスペリエンス改善プログラムの両方を許可するか、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、概要ページが表示されます。サブスクリプション情報が見つからない場合は、無料体験版を続行してください。前の製品で使用されているサブスクリプションが無効な場合は、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。

ESET Security Ultimateがインストールされます

このダイアログウィンドウは次のときに表示できます。

- インストール処理中 – **続行**をクリックしてESET Security Ultimateをインストールします。
- ESET Security Ultimateでサブスクリプションを変更する場合—**アクティベーション**をクリックして、サブスクリプションを変更し、ESET Security Ultimateをアクティベーションします。

製品の変更オプションでは、お持ちのESETサブスクリプションに応じてESETホーム製品を切り替えることができます。詳細については、使用している製品の見分け方を参照してください。

別の製品ラインに変更

お持ちのESETサブスクリプションに応じて、各種ESETWindowsホーム製品を切り替えることができます。詳細については、使用している製品の見分け方を参照してください。

登録

登録フォームのフィールドを入力し、**アクティベーション**をクリックして、サブスクリプション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サブスクリプション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

アクティベーションプロセスが完了するまで数秒お待ちください(インターネット接続速度とコンピューターにより必要な時間が異なります)。

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プロセスは完了しました。インストール後ウィザードに従ってESET Security Ultimateの設定を完了します。

モジュールのアップデートが数秒後に開始しますESET Security Ultimate製品の定期アップデートがすぐに行われます。

モジュールのアップデートから即時、最初の検査が自動的に開始します。

アクティベーションプロセスは、オファリングがESET HOMEに関連付けられていない場合に中断できますESET HOMEにログインするか、アカウントを作成します。

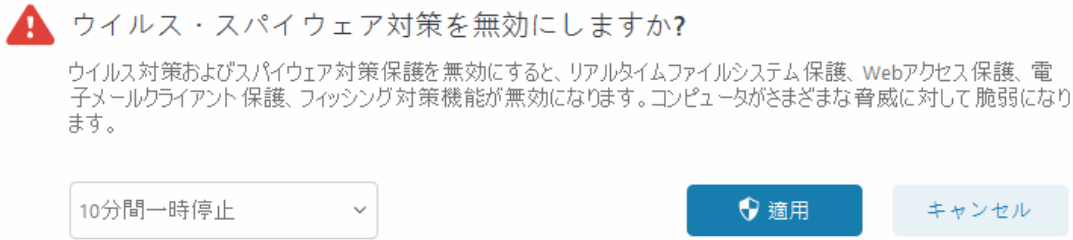
初心者向けガイド

この章ではESET Security Ultimate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。

保護を一時停止 – ファイルWebおよび電子メール通信を制御することによって悪意のあるシステム攻撃から保護する、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。



ファイアウォールの一時停止(すべてのトラフィックを許可) – ファイアウォールを無効状態に切り替えます。詳細については、「ネットワーク」を参照してください。

すべてのネットワークトラフィックをブロック – すべてのネットワークトラフィックをブロックします。再有効化するには、**すべてのネットワークトラフィックのブロックを停止**をクリックします。

詳細設定 - ESET Security Ultimate詳細設定を開きます製品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 Security Ultimateを開く – ESET Security Ultimateの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 Security Ultimate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 - GUI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 Security Ultimate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 Security Ultimate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 Security Ultimate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サブスクリプション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、ESET Security Ultimate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 Security Ultimate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。

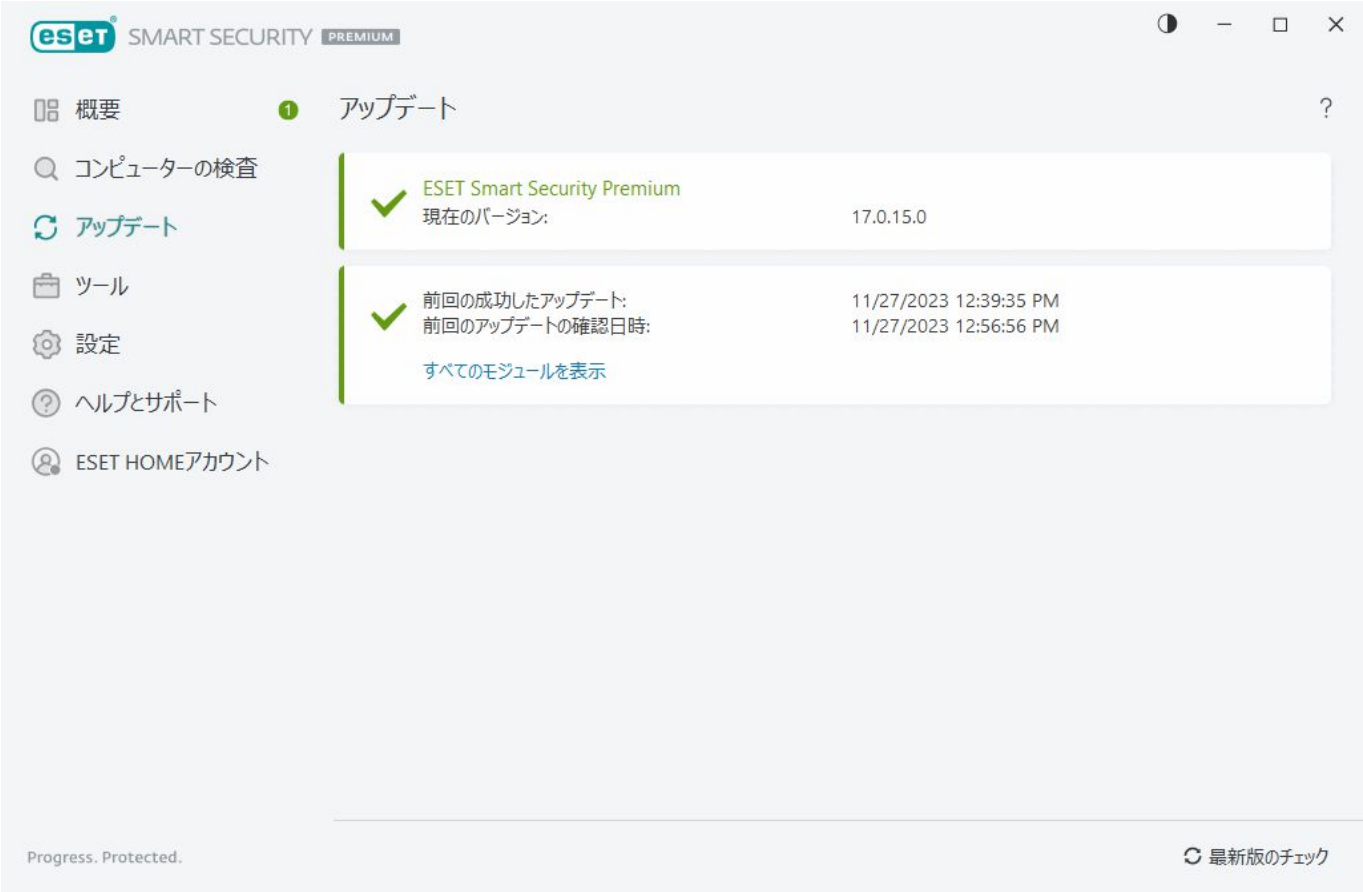
更新

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 Security Ultimate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。

ネットワーク保護の設定

既定ではESET Security Ultimateは、新しいネットワーク接続が検出されたときに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 Security Ultimate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。

アンチセフトを有効にする

自宅から職場への毎日の通勤や他の公共の場所への外出時には、パーソナルデバイスが常に紛失や盗難のリスクにさらされています。アンチセフトは、デバイスの紛失・盗難に備えて、ユーザーレベルのセキュリティを強化する機能です。アンチセフトでは、デバイスの使用を監視したり、ESET HOMEでIPアドレスによる位置検出機能を使用して紛失中のデバイスを追跡したりできるので、デバイスの回収と個人データの保護に役立ちます。

IPアドレスによる位置検出Webカメラによる写真撮影、ユーザーアカウント保護、デバイス監視を備えているアンチセフトは紛失・盗難にあったコンピューターやデバイスが、今どこに有るかを調べる際に、個人ユーザーおよび法執行機関を支援します。ESET HOMEでは、コンピューターまたはデバイスで実行されるアクティビティを確認できます。

ESET HOMEでアンチセフトの詳細を確認するには、ESET HOMEオンラインヘルプを参照してください。

ユーザーアカウント管理の制限により、ドメインのコンピューターではアンチセフトが正常に動作しない場合があります。

アンチセフトを有効にし、紛失または盗難の際にデバイスを保護するには、次のオプションのいずれかを選択します。

- プログラムのメインウィンドウ > **概要**で、**アンチセフト**の横にある**設定**をクリックします。
- メインプログラムウィンドウ > **概要**画面で[Anti-Theftを使用できます]メッセージが表示されている場合は、**アンチセフトを有効にする**をクリックします。
- メインプログラムウィンドウで、**設定** > **セキュリティツール**をクリックします。トグル **アンチセフト**を有効にして、画面の指示に従います。

デバイスがESET HOMEに接続されていない場合は、次の手順を実行する必要があります。
1. アンチセフトを有効にするときにESET HOMEアカウントにログインします。
2. デバイス名を設定

アンチセフトはMicrosoft Windows Home Serverをサポートしていません。

アンチセフトを有効にした後、メインプログラムウィンドウ > **設定** > **セキュリティツール** > **アンチセフト**でデバイスのセキュリティを最適化できます

ペアレンタルコントロール

既にESET Security Ultimateでペアレンタルコントロールを有効化してある場合は、すべての関連するユーザーアカウントのペアレンタルコントロールを設定する必要があります。

ペアレンタルコントロールがアクティブで、ユーザーアカウントが設定されていない場合、**概要**画面で[ペアレンタルコントロールは設定されていません]という通知がESETSecurityUltimateに表示されます。詳細については、ペアレンタルコントロールセクションを参照してください。

製品のアクティベーション

製品をアクティベーションするには、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、国や配布方法(CD/DVD、ESET Webページなど)によって異なります。

- 小売りバージョンの製品を購入された場合、または電子メールでサブスクリプション詳細情報を受け取った場合は、**購入した製品認証キーを使用**をクリックして製品をアクティベーションします。アクティベーションを正常に行うには、製品認証キーを記載どおりに入力する必要があります。製品認証キー - XXXX-XXXX-XXXX-XXXX-XXXXの形式の一意の文字列。サブスクリプション所有者を識別し、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。製品認証キーは通常、製品パッケージの背面またはパッケージ内に同梱されています。

- [ESET HOMEアカウントを使用]を選択した後、ESET HOMEアカウントにログインするように指示されます。

- サブスクリプションを所有しておらず、製品を購入したい場合は、**サブスクリプションを購入**を選択してください。このオプションを選択すると、お客様の地域のESET販売元のWebページが表示されますESET Windowsホーム製品のサブスクリプションは無料ではありません

製品サブスクリプションはいつでも変更できます。変更するには、メインプログラムウィンドウで[**ヘルプとサポート**] > [**サブスクリプションの変更**]をクリックしますESETサポートへのサブスクリプションを識別するための公開IDが表示されます。

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時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 Security Ultimateは、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。

[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。製品認証キーは、XXXX-XXXX-XXXX-XXXX-XXXXの形式の一意の文字列です。サブスクリプション所有者を識別し、サブスクリプションをアクティベーションするために使用されます。

正確性を保つためにも、製品認証キーを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。

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 > **ヘルプとサポート** > **サブスクリプションをアクティベーション**でESET Security Ultimateをアクティベーションできます。

ESET Windowsホーム製品のサブスクリプションは無料ではありません。

ESET HOMEアカウントの使用

デバイスをESET HOMEに接続して、すべてのアクティベーションされたESETサブスクリプションとデバイスを表示して管理します。サブスクリプションを更新、アップグレード、または拡張し、重要なサブスクリプション詳細情報を表示できます。ESET HOME管理ポータルまたはモバイルアプリでは、別のサブスクリプションを追加したり、製品をデバイスにダウンロードしたり、製品セキュリティステータスを確認したり、電子メールでサブスクリプションを共有したりできます。詳細については、ESET HOMEオンラインヘルプをご覧ください。

アクティベーション方法として**ESET HOMEアカウントを使用**を選択した後、またはインストール中にESET HOMEアカウントに接続するときは、次の手順を実行します。

1. ESET HOMEアカウントにログインします。

ESET HOMEアカウントをお持ちではない場合は、**アカウントの作成**をクリックして登録するか、ESET HOMEオンラインヘルプの手順を参照してください。
パスワードを忘れた場合は、**パスワードを忘れた場合**をクリックし、画面の手順に従うか、ESET HOMEオンラインヘルプの手順を参照してください。

2. すべてのESET HOMEサービスで使用される**デバイス名**を設定し、**続行**をクリックします。

3. アクティブ化するサブスクリプションを選択するか、新しいサブスクリプションを追加します。**続行**をクリックするとESET Security Ultimateをアクティベーションします。

無料のESET製品認証キー

ESET Security Ultimateのサブスクリプションは無料ではありません。

ESET製品認証キーは、エンドユーザーライセンス契約に準拠したESET Security Ultimateの法的な利用を許可するためにESETが提供するダッシュで区切られた一意の連続する文字および数字です。すべてのエンドユーザーは、ESETが付与したライセンス数に基づいてESET Security Ultimateを使用する権利を有する範囲においてのみ製品認証キーを使用する資格があります。製品認証キーは機密情報と見なされ、共有することはできません。ただし、ESET HOMEを使用してサブスクリプションを共有することはできます。

インターネット上には「無償」のESET製品認証キーを提供するソースがありますが、次の点に留意してください。

• 「無償のESETサブスクリプション」という広告をクリックすると、コンピューターやデバイスが危険にさらされ、マルウェアに感染するおそれがあります。マルウェアは、非公式のWebコンテンツ(動画など)やWebサイトに隠されていることがあり、アクセスなどに基づいて金銭を得るための広告を表示します。通常、これは罠です。

• ESETは海賊版サブスクリプションを無効にすることができます。

• 海賊版の製品認証キーは、ESET Security Ultimateをインストールするために同意する必要があるエンドユーザーライセンス契約に準拠していません。

• www.eset.comなどの公式チャネルまたはESETの代理店、またはリセラーからのみESETサブスクリプションを購入してください(eBayなどの非公式のサードパーティWebサイトからのサブスクリプションや、サードパーティーからの共有サブスクリプションを購入しないこと)。

• ESET Security Ultimateのダウンロードは無償ですが、インストール中のアクティベーションには有効なESET製品認証キーが必要です(ダウンロードしてインストールできますが、アクティベーションは動作しません)。

• インターネットまたはソーシャルメディアでサブスクリプションを共有しないでください(拡散する可能性があります)。

海賊版のESETサブスクリプションを特定して報告するには、ナレッジベース記事の手順をご覧ください。

ESETセキュリティ製品の購入について不明な点がある場合は、検討中に試用バージョンを使用できます。

1. 無料体験版を使用してESET Security Ultimateをアクティベーションする

2. ESET評価版プログラムに参加する

3. Androidモバイルデバイスを使用している場合は、ESET Mobile Securityをインストールします。これは無償です。

ライセンスの割引を取得する/ライセンスを延長するには、ESETを更新してください。

アクティベーションの失敗 – 一般的なシナリオ

ESETSecurityUltimate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、インターネット接続がアクティブであることを確認しますESET Security Ultimateの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ESET HOMEアカウントを使用している場合は、ESET HOMEサブスクリプションとサブスクリプション管理 – オンラインヘルプを参照してください。

特定のエラー(一時停止されたサブスクリプションの中断や使用超過のサブスクリプションなど)が表示された場合は、サブスクリプションステータスの指示に従ってください。

アクティベーションできない場合は、ESET製品アクティベーショントラブルシューティング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)。

サブスクリプションステータス

サブスクリプションにはさまざまなステータスがあります。サブスクリプションのステータスは、ESET HOMEで確認できます。サブスクリプションをESET HOMEアカウントに追加するには、サブスクリプションの追加を参照してください。

ESET HOMEアカウントをお持ちではない場合は、新しいESET HOMEアカウントを作成できます。

サブスクリプションステータスが**アクティブ**以外の場合は、アクティベーション中のエラーまたはメインプログラムウィンドウの通知が表示されます。

サブスクリプションステータス通知を無効にするには、詳細設定 > **通知** > **アプリケーションステータス**を開きます。**アプリケーションステータス**の横の**編集**をクリックし、**ライセンス**を展開して、無効にする通知の横のチェックボックスをオフにします。通知を無効にしても、この問題は解決しません。

次の表で、異なるサブスクリプションステータスの説明と推奨されるソリューションを参照してください。

サブスクリプションステータス	説明	解決策
アクティブ	サブスクリプションは有効です。操作する必要はありません。ESET Security Ultimateをアクティベーションできます。サブスクリプション詳細は、メインプログラムウィンドウ > **ヘルプとサポート**で確認できます。	
使用超過	許可されているよりも多くのデバイスでこのサブスクリプションが使用されています。アクティベーションエラーが表示されます。	詳細については、使用超過サブスクリプションのため、アクティベーションが失敗しましたを参照してください。

サブスクリプションステータス	説明	解決策
停止中	決済の問題のため、サブスクリプションが一時停止されました。サブスクリプションを使用するには、ESET HOMEで決済詳細情報が最新であることを確認するか、サブスクリプションのリセラーにお問い合わせください。アクティベーション中またはメインプログラムウィンドウでこのエラーが発生する場合があります。	インストールされている製品 - ESET HOMEアカウントがある場合は、メインプログラムウィンドウに表示される通知で、**ESET HOMEでサブスクリプションを管理**をクリックして、決済詳細情報を確認します。それ以外の場合は、サブスクリプションのリセラーにお問い合わせください。 アクティベーションエラー - ESET HOMEアカウントがある場合は、アクティベーションエラーウィンドウで**ESET HOMEを開く**をクリックして、決済詳細を確認します。それ以外の場合は、サブスクリプションのリセラーにお問い合わせください。
有効期限切れ	サブスクリプションは有効期限切れです。このサブスクリプションを使用してESET Security Ultimateをアクティベーションすることはできません。アクティベーション中またはメインプログラムウィンドウでこのエラーが発生する場合がありますESET Security Ultimateが既にインストールされている場合、コンピューターは保護されておらず、アップデートされません。	インストールされている製品 — メインプログラムウィンドウに表示される通知で、**サブスクリプションの更新**をクリックして、サブスクリプションを更新する方法の手順に従うか、**製品のアクティベーション**をクリックして、アクティベーション方法を選択します。 アクティベーションエラー – アクティベーションエラーウィンドウで、**サブスクリプションの更新**をクリックして、サブスクリプションを更新する方法の手順に従います。あるいは、新しいまたは更新された製品認証キーを入力して、**サブスクリプションの更新**をクリックします。
キャンセル済み	サブスクリプションは、ESETまたはサブスクリプションのリセラーによってキャンセルされました。	ライセンスが正常に機能するはずなのに、メインプログラムウィンドウまたはアクティベーション中にサブスクリプションをキャンセルしました。サブスクリプションが正常に機能する場合は、サブスクリプションのリセラーにお問い合わせください。

使用超過サブスクリプションのため、アクティベーションが失敗しました

問題

- サブスクリプションが使用超過または悪用されている可能性があります
- 使用超過サブスクリプションのため、アクティベーションが失敗しました

解決策

サブスクリプションは、許可されているよりも多くのデバイスで使用されています。海賊版ソフトウェアや偽造ソフトウェアの被害に遭っている可能性があります。このサブスクリプションを使用して他のESET製品をアクティベーションすることはできませんESET HOMEアカウントでサブスクリプションを管理できる場合、または合法的な販売者からサブスクリプションを購入した場合は、直接この問題を解決することができます。アカウントをお持ちでない場合は、作成することができます。

サブスクリプション所有者であり、電子メールアドレスの入力を求められない場合:

1. ESETサブスクリプションを管理するにはWebブラウザーを開き、https://my.eset.comにアクセスしますESET License Managerにアクセスし、シートを削除またはアクティベーション解除します。詳細については、「使用超過サブスクリプションの場合の対応」を参照してください。

2. 海賊版のESETサブスクリプションを特定して報告するには、海賊版ESETサブスクリプションを特定して報告する記事の手順をご覧ください。

3. 不明な場合は、**[戻る]**をクリックして、ESETテクニカルサポートまで電子メールでお問い合わせください。

サブスクリプション所有者ではない場合、サブスクリプションの使用数が超過したためESET製品をアクティベーションできないという情報を、このサブスクリプションの所有者に通知してください。所有者はESET HOMEポータルでこの問題を解決できます。

電子メールアドレスを確認するように指示された場合(複数の場合のみ)はESET Security Ultimateを購入またはアクティベーションするときに最初に使用した電子メールアドレスを入力します。

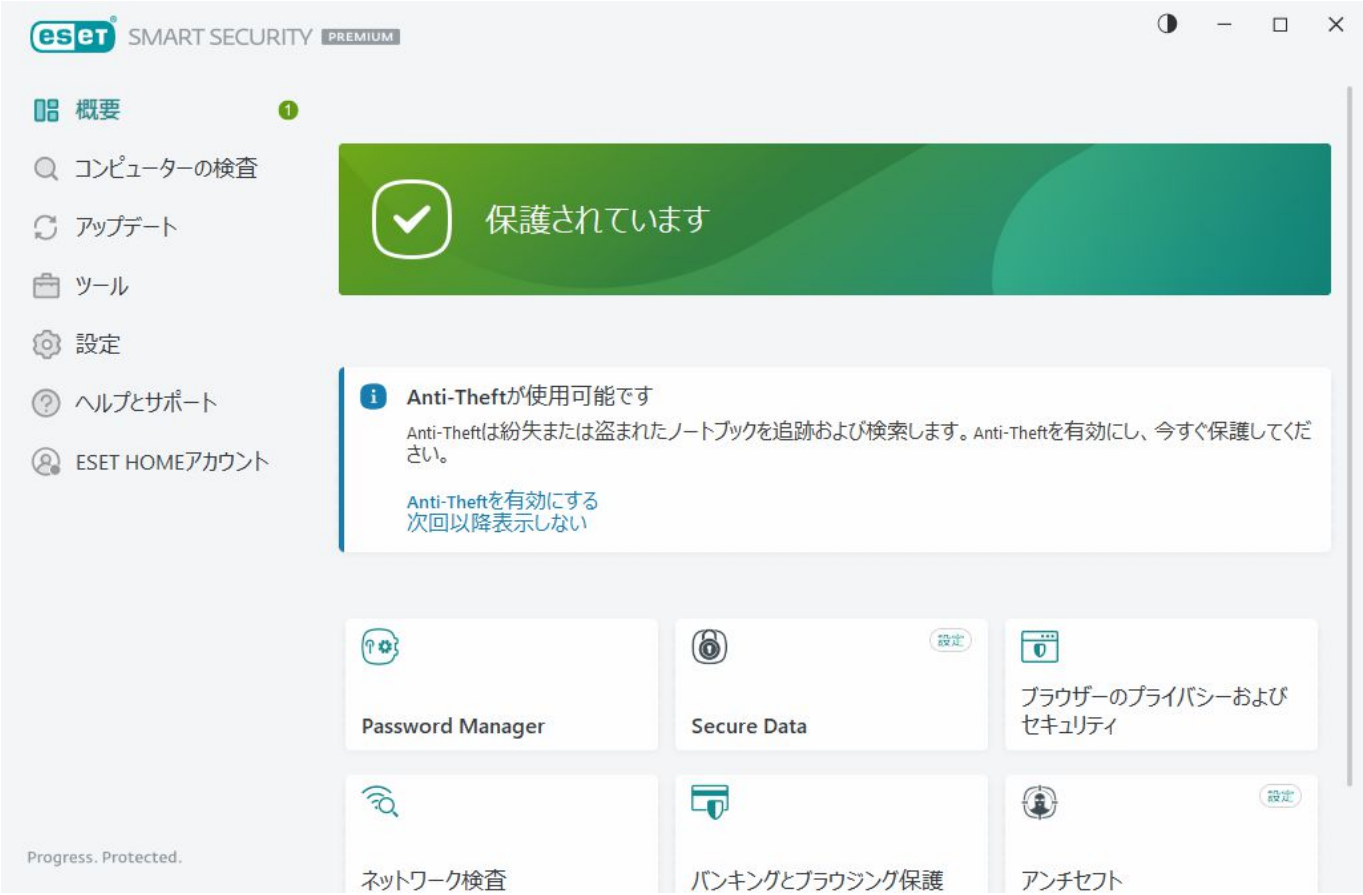
ESET Security Ultimateの操作

ESET Security Ultimate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 Security Ultimate 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 Security Ultimateの配色を設定します。
- **ダークモード** - ESET Security Ultimateには暗い配色(ダークモード)があります。
- **ライトモード** - ESET Security Ultimate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:

概要 - ESET Security Ultimate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 - ネットワーク検査と、プログラム管理が容易になるその他の機能にアクセスでき、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 Security Ultimate保護機能(コンピューター保護、ネットワーク保護、およびセキュリティツール)の設定オプションを提供し、詳細設定へアクセスできます。

ヘルプとサポート – サブスクリプション、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。

ESET HOMEアカウント–デバイスをESET HOMEに接続するか、ESET HOMEアカウント接続ステータスを確認します。ESET HOMEを使用して、アンチセフト設定とアクティベーションされたESETサブスクリプションとデバイスを表示および管理します。

概要

概要ウィンドウには、コンピューターの現在の保護に関する情報と、ESETSecurityUltimateのセキュリティ機能へのクイックリンクが表示されます。

概要ウィンドウには、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 Security Ultimate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。その他の通知がある場合は、**その他のX件の通知**をクリックしてすべて展開します。

Password Manager — Password Managerの設定方法の手順が開きます。

ネットワーク検査 – ネットワークのセキュリティを確認

Secure Data - セキュリティツールを開きます。**Secure Data**の横のトグルアイコンをクリックして有効にしますSecure Dataが既に有効な場合は、クイックリンクでSecure Dataページが開きます。

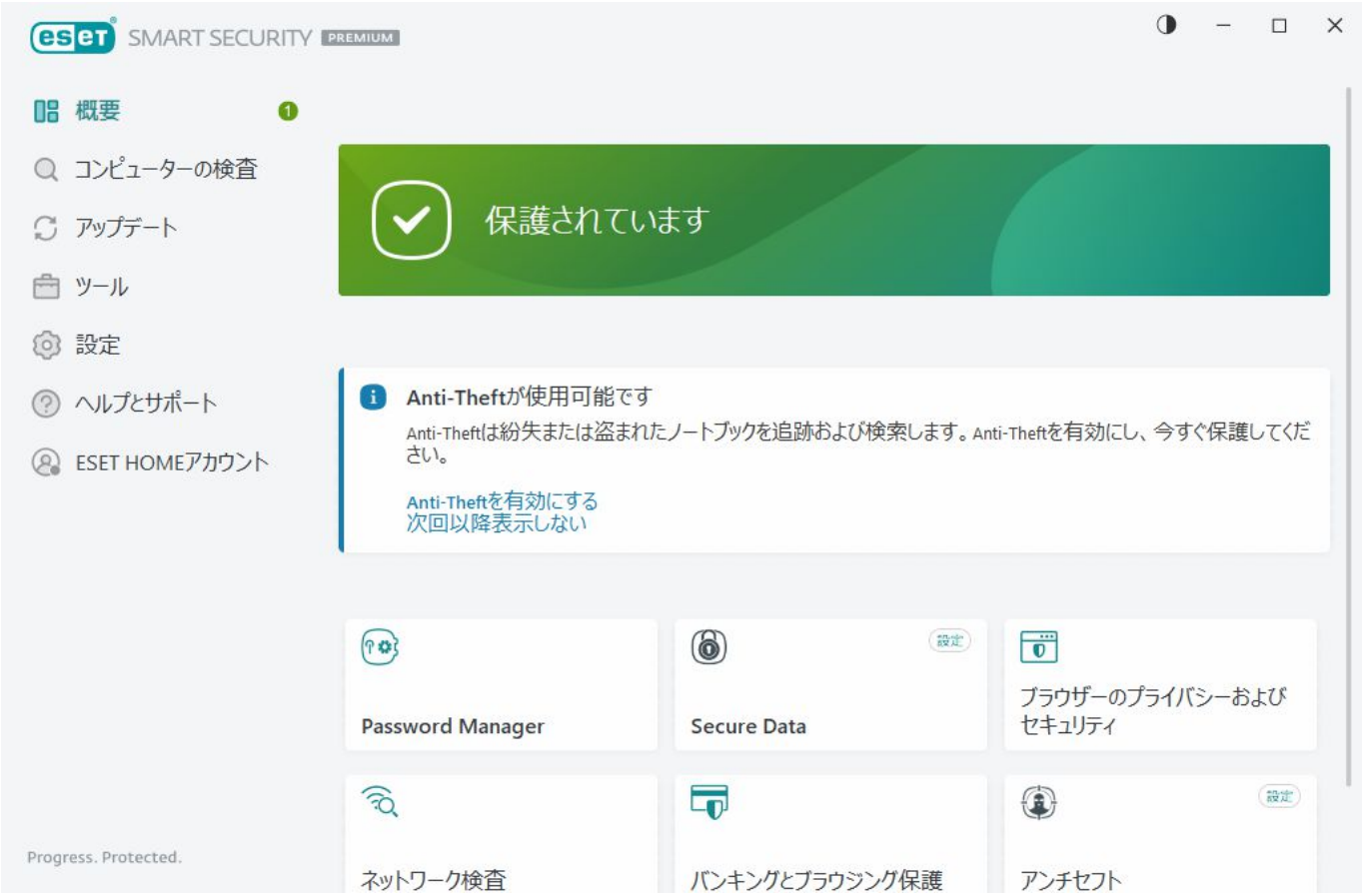
バンキングとブラウジング保護 - Windowsの既定の設定でセキュアモードでブラウザーを起動します。

ブラウザーのプライバシーおよびセキュリティ - ESETによって保護されたブラウザーへのインストールを許可する拡張機能を選択できます。

アンチセフト - アンチセフトセットアップを開始します。アンチセフトがセットアップされている場合は、クイックリンクでアンチセフトページが開きます。

VPN – データを安全に保ち、不要な追跡を回避し、匿名IPアドレスの追加セキュリティでプライバシーを強化します

Identity Protection—個人情報、信用情報、財務情報を保護しますIdentity Protectionは継続的な監視を提供することにより、個人情報の違法な販売を検出します。



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

有効になっている保護モジュールが正しく動作している場合、保護の状態アイコンは緑になります。赤の「！」マークやオレンジの通知アイコンは、リスクがあることを示します。各モジュールの保護の状態に関する詳細情報と、完全な保護を復元するために推奨される解決策が**概要**ウィンドウに通知として表示されます。各モジュールの状態を変更するには、[**設定**]をクリックして目的のモジュールを選択します。

赤いアイコンと赤い**セキュリティアラート**の状態は、重大な問題があることを示しています。この状態が表示される原因はいくつか考えられます。以下に例を示します。

- **製品がアクティベーションされていません**または**サブスクリプションは期限切れです** – 赤色の保護の状態アイコンで示されています。サブスクリプションの期限が過ぎると、このプログラムではアップデートできなくなります。サブスクリプションを更新するには、警告ウィンドウの指示に従ってください。
- **検出エンジンは最新ではありません** – このエラーは、検出エンジン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。
- **リアルタイムファイルシステム保護が無効です** – 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。**リアルタイムファイルシステム保護を有効にする**をクリックして、この機能を再有効化してください。
- **ウイルス対策・スパイウェア対策による保護は無効です** – ウイルス対策・スパイウェア対策機能モジュールをすべて再度有効にするには[**ウイルス・スパイウェア対策の保護機能を有効にする**]をクリックします。
- **ESETファイアウォールが無効になっています** – この問題もデスクトップの**ネットワーク**ア

イテムの横のセキュリティ通知で確認できます。[**ファイアウォールを有効にする**]をクリックして、ネットワークの保護を再度有効にできます。

オレンジ色のアイコンは保護が制限されていることを意味します。たとえば、プログラムのアップデートで問題が発生した場合や、サブスクリプションの有効期限が近付いている場合などが考えられます。

この状態が表示される原因はいくつか考えられます。以下に例を示します。

- **アンチセフト最適化警告** – このデバイスは アンチセフト 用に最適化されていません。たとえば、架空アカウント（デバイスを紛失中としてマークすると、自動的にトリガされるセキュリティ機能）はコンピューター上では作成できない場合があります。必要に応じて、アンチセフトのWebインタフェースの最適化機能を使って架空アカウントを作成してください。
- **ゲームモードが有効です** -ゲームモードを有効にすると、セキュリティリスクが発生します。この機能を有効にすると、すべての通知/アラートウィンドウが無効となり、スケジュールされたタスクをすべて停止します。
- **サブスクリプションの有効期限がまもなく切れます/サブスクリプションの有効期限が本日切れます** – これは保護の状態アイコンで示され、システム時計の横に「！」が表示されます。サブスクリプションの期限が切れたら、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。

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、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。

コンピューターの検査

オンデマンドスキャナーはウイルス対策の重要な部分であり。コンピューター上のファイルやフォルダーのスキャンを実行するために使用されます。セキュリティの観点からは、感染が疑われるときだけコンピュータ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。定期的にシステムの詳細検査を実行し、ディスクに書き込まれるときに、リアルタイムファイルシステム保護では検出されないウィ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**では、スキャンパラメーターを指定することなく、すばやくシステムをスキャンできます。**カスタム検査**(詳細検査の下)では、特定の検査場所を対象にあらかじめ定義した検査プロファイルの選択や、特定の検査対象の選択を行うことができます。

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。

既定ではESET Security Ultimateはコンピューターの検査中に検出された検出を自動的に駆除または削除しようとします。一部の場合で、アクションを実行できない場合は、インタラクティブアラートが表示され、駆除アクション(削除または無視など)を選択する必要があります。駆除レベルを変更する方法および詳細については、駆除を参照してください。前回の検査を確認するには、ログファイル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。カスタム検査の利点は、パラメーターを詳細に設定できることです。**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)。

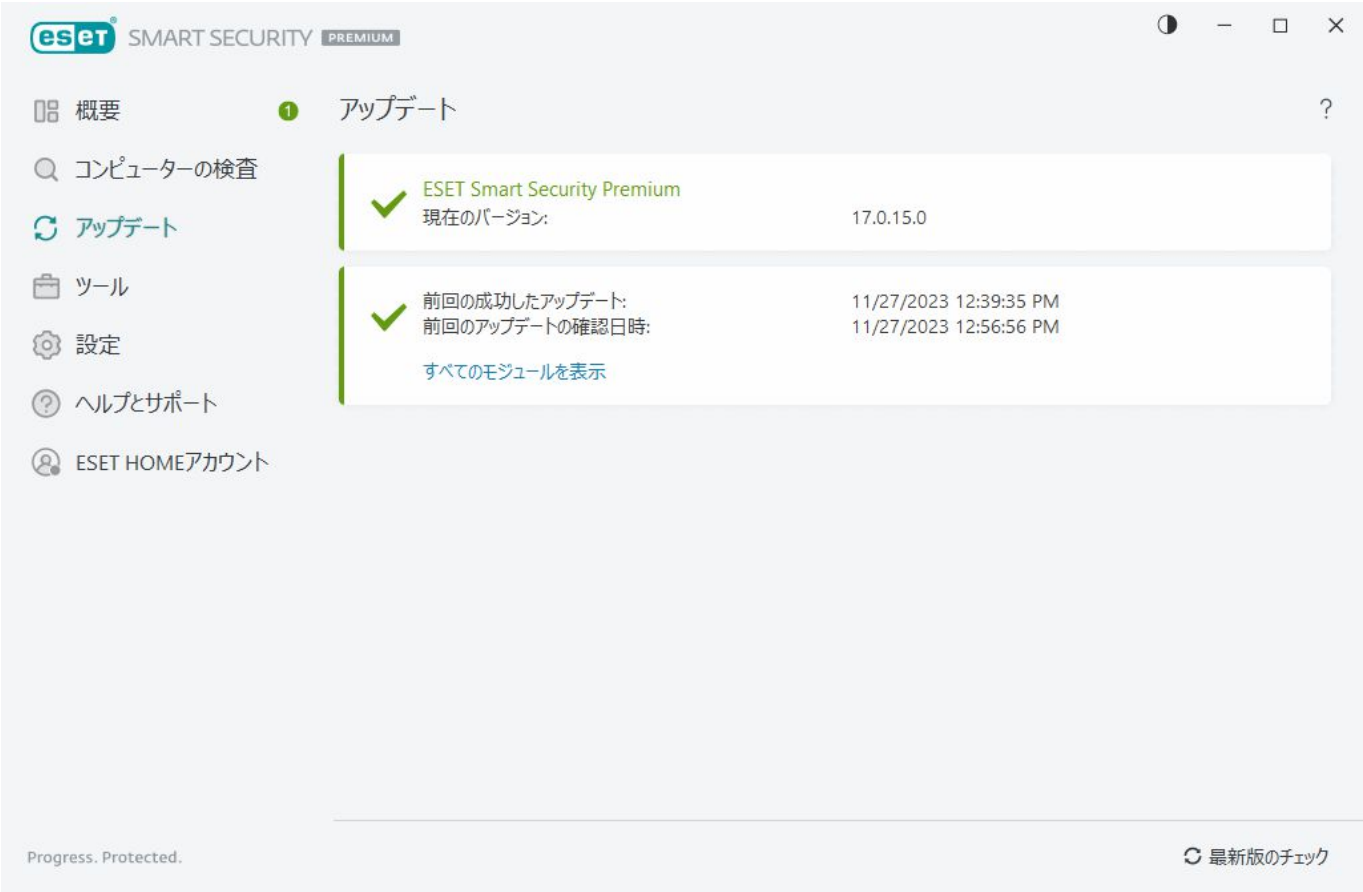
アクション	使用状況
コピー	ハイライトされたレコードをクリップボードにコピーします。ショートカット: Ctrl+C
すべてコピー	ウィンドウのすべてのレコードをコピーします。
エクスポート	クリップボードでハイライトされたレコードををXMLファイルにエクスポートします。
すべてエクスポート	ウィンドウのすべてのレコードがXMLファイルにエクスポートされます。
検出の説明	ハイライトされた侵入の危険と兆候に関する情報を含むESETの脅威に関する情報へのリンクです。

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 Security Ultimate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 Security Ultimateをアクティベーションする必要がありますESET Security Ultimate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。



現在のバージョン – インストール済みの現在の製品バージョンの数を表示します。

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

前回のアップデートの確認日時 – 成功アップデートを確認した最終日を記載します。

すべてのモジュールを表示 – インストールされたプログラムモジュールの一覧が表示されます。

最新版のチェックをクリックして、使用可能な最新のESET Security Ultimateを確認します。

アップデートプロセス

[**最新版のチェック**]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

モジュールアップデート失敗メッセージが表示される場合は、次の問題が原因である可能性があります。

1. **無効なサブスクリプション** – アクティベーションに使用されたサブスクリプションが無効であるか、有効期限が切れています。メインプログラムウィンドウで、**ヘルプとサポート>サブスクリプションの変更**をクリックし、製品をアクティベーションします。

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。** – これは間違ったインターネット接続設定によるものです。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。ご利用のインターネットサービスプロバイダ(ISP)に、有効なインターネット接続があるかどうか確認してください。

新しい製品バージョンのESET Security Ultimateへのアップデートが成功した後に必ずコンピューターを再起動し、すべてのプログラムモジュールが正しく更新されたことを確認してください。定期モジュールアップデート後にコンピューターを再起動する必要はありません。

詳細については、「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を参照してください。

ダイアログウィンドウ – 再起動が必要

ESET Security Ultimate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 Security Ultimateの新バージョンが提供されています。

新しいバージョンのESET Security Ultimateは、プログラムアップデート設定に基づいて自動的にインストールするか、新しいバージョンをダウンロードして以前のバージョンに上書きインストールして手動でインストールできます。

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**概要**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。

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 Security Ultimate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。

ツール

ツールメニューには、セキュリティを強化し、ESET Security Ultimate管理をシンプルにするための機能があります。使用可能なツールは次のとおりです。

ログファイル

実行中のプロセス (ESET Security UltimateでESET LiveGrid®が有効になっている場合)

セキュリティレポート

ネットワーク接続 (ESET Security Ultimateでファイアウォール が有効にされている場合)

ESET SysInspector

スケジューラ

システムクリーナー

ネットワーク検査

分析のためにサンプルを提出(ESET LiveGrid®構成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の重要な部分です。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 Security Ultimate環境から直接、ログをアーカイブするだけでなく、テキストメッセージとログを表示することができます。

ログファイルにアクセスするには、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。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。

• **検出** – このログにはESET Security Ultimate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、スキャナータイプ、オブジェクトタイプ、オブジェクトの場所、検出の名前、実行されたアクション、侵入の検出時にログインしていたユーザーの名前、ハッシュ、最初の発生が含まれます。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 Security Ultimate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** – このウィンドウには、完了した全ての検査結果が表示されます。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、選択した検査の詳細が表示されます。

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

• **HIPS** – 記録対象としてマークされた特定のHIPSルールのレコードが示されます。このプロトコルは、操作をトリガ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)、およびルール名を表示します。

• **ブラウザーの保護** – ブラウザーに読み込まれた検証されていないファイルまたは信頼できないファイルのレコードが含まれます。

• **ネットワーク保護** – ネットワーク保護ログには、ファイアウォール、ネットワーク攻撃保護(IDS)、ボットネット保護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アクセス保護またはペアレンタルコントロール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。各ログでは、特定のWebサイトへ接続をした際の時間、URLアドレス、ユーザー、およびアプリケーションを確認できます。

• **電子メールクライアント迷惑メール対策** – 迷惑メールとマークされたメールメッセージと関連するレコードが示されます。

• **Parental Control** – ペアレンタルコントロールによってブロックまたは許可されたWebページが表示されます。[判定タイプ]列と[判定値]列には、フィルタリングルールがどのように適用されたかが示されます。

• **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。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。

• **Webカメラアクセス制御** - Webカメラ保護でブロックされたアプリケーションのレコードがあります。

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**または**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** – 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。

• **フィルタをクリア** – 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** – ウィンドウで選択した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** – 選択し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/すべてエクスポート** – 選択したレコードまたはすべての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。

• **検出の説明** – 記録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。

• **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)。

• **ブラウザーの保護の許可リストに追加**- ブラウザーの保護の許可リストウィンドウを開き、項目をリストに追加します。

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/検索オプションを構成した後、**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。

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 Security Ultimateは実行中のプロセスについて詳細な情報を提供し、ESET LiveGrid®技術でユーザーを保護します。

評価 – 多くの場合ESET Security Ultimateおよび技術では、各オブジェクトのESET LiveGrid®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1 – 良好(緑)9 – 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。

問題なし(緑)でマークされた既知のアプリケーションはクリーン(ホワイトリストに入っている)であり、検査から除外されます。

PID – プロセスID番号は、プロセスの優先度の調整など、さまざまな関数呼び出しでパラメーターとして使用できます。

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。

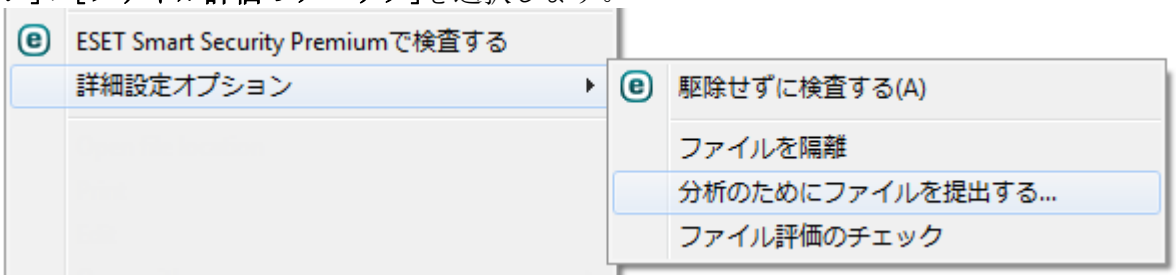
不明(オレンジ)は必ずしも悪意があるソフトウェアであるとはかぎりません。通常は、単に新しいアプリケーションというだけです。疑わしいファイルが見つかった場合は、ESETのリサーチラボに提出してファイルを解析に送信できます。そのファイルが悪意のあるアプリケーションであることが判明すると、その後のアップデートファイルにその検出が追加されます。

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。

アプリケーションをクリックすると、そのアプリケーションに関する次の詳細が表示されます。

- **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/変更日** – 作成日時(修正)。

また、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のレピュテーションも確認できます。そのためには、ファイルエクスプローラーでファイルを右クリックし、**[詳細設定オプション] > [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。
- **ペアレンタルコントロールでブロックされたWebページ** - ペアレンタルコントロールでブロックされたWebページ数を表示します。
- **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。
- **検出された迷惑メール** – 検出された迷惑メール数を表示します。
- **ブロックされたWebカメラへのアクセス** – ブロックされたWebカメラへのアクセス数を表示します。
- **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。
- **ESET LiveGuardによって分析されたファイル** - ESET LiveGuardによって分析されたサンプル数を表示します。

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。

セキュリティレポートの最後の部分では、次の機能を有効にすることができます。

- ESET LiveGuard
- Secure Data
- ペアレンタルコントロール
- アンチセフト

この機能が有効になると、セキュリティレポートで「機能停止」と表示されなくなります。

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 Security Ultimate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** > 通知 > **対話アラート** > **確認メッセージ** > **編集**で**統計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。

ネットワーク接続

[ネットワーク接続]セクションには、アクティブな接続と保留中の接続のリストが表示されます。このリストは、発信接続を確立しているすべてのアプリケーションを管理するために有用です。

グラフアイコン をクリックし、ネットワークアクティビティを開きます。

1行目には、アプリケーション名とデータ転送速度が表示されます。アプリケーションが行った接続のリスト(および詳細な情報)を表示するには、**>**をクリックします。

列

アプリケーション/ローカルIP – アプリケーションの名前、ローカルIPアドレス、および通信ポート。

リモートIP – 特定のリモートコンピューターのIPアドレスとポート番号。

プロトコル – 使用されている転送プロトコル。

上り速度/下り速度 – 送信データおよび受信データの現在の速度。

送信/受信 – 接続内で交換されるデータの量。

詳細を表示 – このオプションを選択すると、選択した接続に関する詳細情報が表示されます。

次の追加オプションを表示するには、接続を右クリックします。

ホスト名を解決 – 可能な場合、全てのネットワークアドレスが、数字によるIPアドレス形式ではなくDNS形式で表示されます。

TCP接続のみを表示 – リストにはTCPプロトコルスイートに属する接続のみが表示されます。

リスンしている接続を表示 – このオプションを選択すると、現時点では通信が確立されていない接続のうち、システムがポートを開いており、接続を待機しているもののみが表示されます。

コンピュータ内部の接続を表示 – このオプションを選択すると、リモート側がローカルシステム(つまり、localhost)の接続のみが表示されます。

更新間隔 – アクティブな接続を更新する頻度を選択します。

最新の情報に更新 - [**ネットワーク接続**]ウィンドウを読み込み直します。

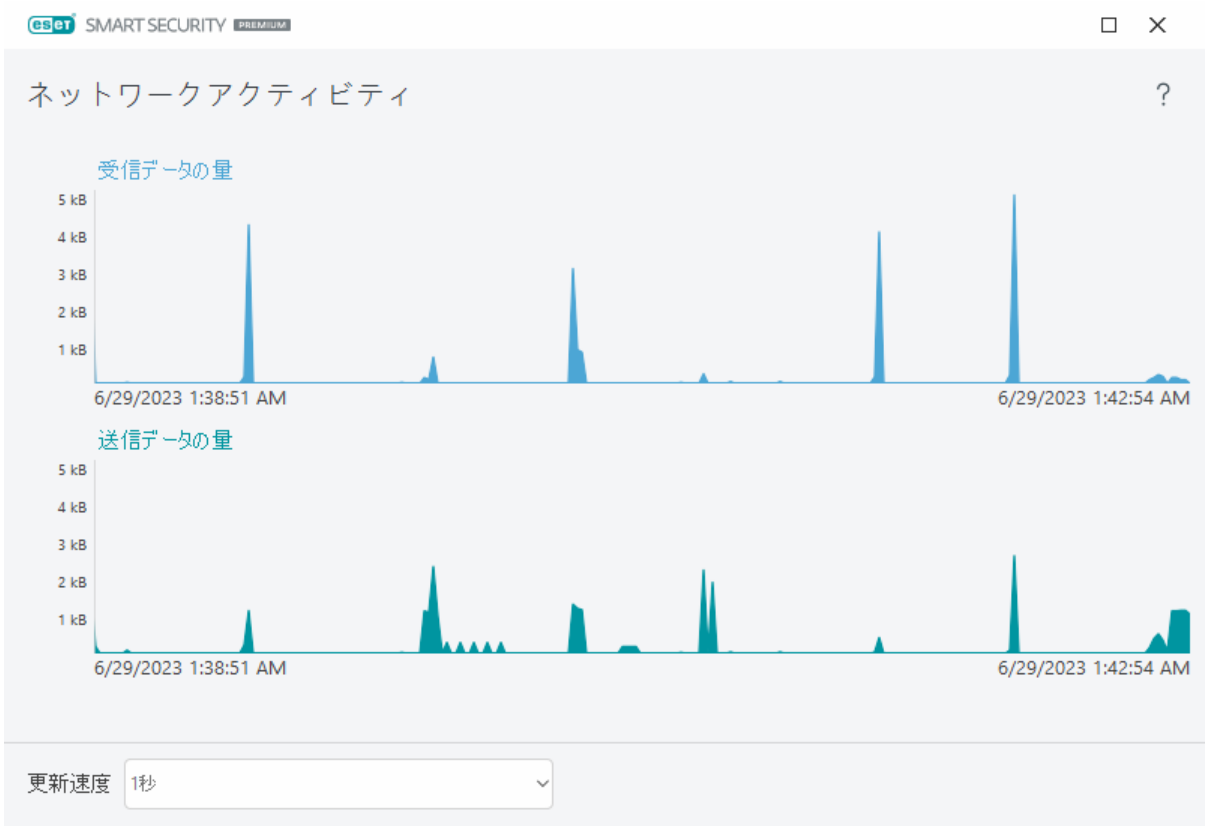
以下のオプションは、アクティブな接続ではなく、アプリケーションまたはプロセスをクリックしないと使用できません。

指定したプロセスの通信を一時的に拒否 – 指定したアプリケーションの現在の接続を拒否します。新しい接続が確立される場合、ファイアウォールではあらかじめ定義されたルールが使用されます。設定の説明は、ファイアウォールルールセクションで参照することができます。

指定したプロセスの通信を一時的に許可 – 指定したアプリケーションの現在の接続を許可します。新しい接続が確立される場合、ファイアウォールではあらかじめ定義されたルールが使用されます。設定の説明は、ファイアウォールルールセクションで参照することができます。

ネットワークアクティビティ

現在の**ネットワークアクティビティ**をグラフ形式で表示するには、**ツール > ネットワーク接続**をクリックし、グラフアイコン をクリックします。グラフの最下部は、ネットワークアクティビティを選択された期間に基づいてリアルタイムで示す時系列です。時間間隔を変更するには、 **更新速度** のドロップダウンメニューから選択します。



使用可能なオプションは次のとおりです。

- **1 秒** – グラフは1秒おきに更新され、時系列は直近4分間を表示します。
- **1分(直前の24時間)** – グラフは1分おきに更新され、時系列は直近24時間を示します。
- **1時間(先月)** – グラフは1時間おきに更新され、時系列は直近1ヶ月間を示します。

グラフの縦軸は送受信されたデータの量です。グラフの上にカーソルを置くと、特定の時刻に送受信されたデータの正確な量が表示されます。

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 Security Ultimate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。 モジュールのアップデート、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)。スケジュールされたタスクのリストを既定に戻し、すべての変更を削除するには、**既定値**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**
- **ユーザーログオン後に自動アップデート**
- **システムのスタートアップファイルのチェック**(ユーザーのログオン後)
- **システムのスタートアップファイルのチェック**(検出エンジンの正常なアップデート後)

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**]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. プル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**– 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. タスクをアクティベーションする(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)には、**有効**の横のトグルを有効にし、**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**
- **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** – 最初にスキップされたタスクの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。以下でスピナーを使用して時間を設定します。

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。

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)。

検査を中断できませんを選択すると、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。

システムクリーナー

システムクリーナーは、脅威を駆除した後にコンピュータを利用可能な状態に復元することを支援するツールです。マルウェアは、レジストリエディターや、タスクマネージャー、またはウィンドウズアップデートなどのシステムユーティリティを無効にすることがあります。システムクリーナーは、1回のクリックで、特定のシステムの既定値および設定を復元します。

システムクリーナーは、5つの設定カテゴリから問題を報告します。

- **セキュリティ**: Windows Updateなどのコンピューターの脆弱性が高くなる設定の変更
- **システム設定**: ファイルの関連付けなどのコンピューターの動作を変更する可能性があるシステム設定の変更
- **システム表示**: デスクトップ壁紙などのシステムの表示に影響する設定
- **無効な機能**: 無効になる可能性がある重要な機能とアプリケーション
- **Windowsシステム復元**: システムを以前の状態に復元できるWindowsシステム復元機能の設定

次の場合にシステムクリーニングが求められます。

- 脅威が検出されたとき
- ユーザーが[**リセット**]**をクリックするとき**

変更を確認し、適切な場合には設定をリセットできます。

管理者権限のあるユーザーのみがシステムクリーナーでアクションを実行できます。

ネットワーク検査

ネットワーク検査は、信頼できるネットワーク(自宅または職場ネットワーク)の脆弱性(開いているポートまたは弱いルーターパスワードなど)を特定できます。また、接続されたデバイスのリスト、タイプ別に分類されたデバイス(プリンター、ルーター、モバイルデバイスなど)があり、ネットワーク(ゲームコンソール、IoT、または他のスマートホームデバイスなど)に接続されたユーザーを示します。

ネットワーク検査は、脆弱なルーターを特定し、ネットワークに接続したときの保護レベルを引き上げます。

ネットワーク検査ではルーターは再構成されません。ルーターの専用インターフェースを使用して、自分で変更します。ホームルーターは、分散サービス妨害攻撃(DDoS)を起動するために使用されるマルウェアに対して非常に脆弱です。ルーターパスワードがユーザーによって既定値から変更されていない場合は、ハッカーが簡単に推測し、ルーターにログインして、再構成するか、ネットワークを危険にさらすことができます。

十分に長さのある、数字、記号、大文字を含む強力なパスワードを作成されることを強く推奨します。パスワードのクラッキングを困難にするには、異なる種類の文字を使います。

接続しているネットワークが信頼できるネットワークに設定されている場合は、ネットワークを「マイネットワーク」に設定できます。**[マイネットワーク]に設定**をクリックし、マイネットワークタグをネットワークに追加します。このタグはESET Security Ultimateでネットワークの横に表示され、識別しやすくなり、セキュリティの概要も改善されます。**[マイネットワーク]の設定を解除**をクリックすると、タグを削除します。

ネットワークに接続された各デバイスは、基本情報とともにリストビューに表示されます。特定のデバイスをクリックすると、デバイスを編集したり、デバイスに関する詳細情報を表示したりできます。

ネットワークドロップダウンメニューでは、次の条件に基づいてデバイスをフィルタリングできます。

- 特定のネットワークに接続されたデバイス
- **すべてのネットワーク**に接続されたデバイス
- 分類されていないデバイス

アイコンをクリックすると、デバイスを編集したり、デバイスの詳細情報を表示したりできます。簡単に見つけ出せるよう、ルーター近くに最近接続したデバイスが表示されます。

右上の歯車⚙をクリックして、ネットワークで新しいデバイスが検出されたときに通知するかどうかを選択します。

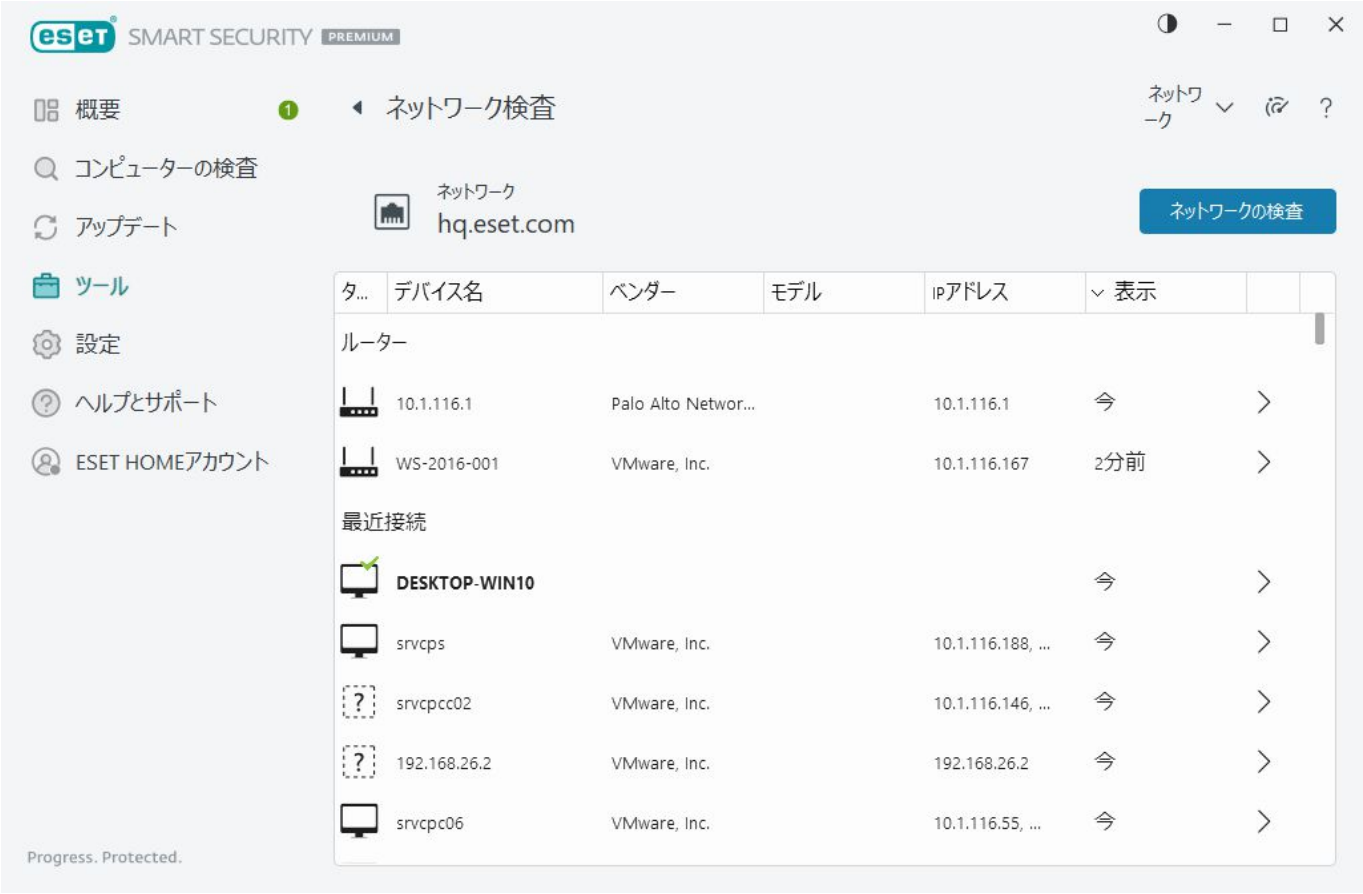
[**ルーターの検査**]をクリックし、現在接続されているルーターの検査を手動で実行します。**ネットワークの検査**は、信頼できるネットワークでのみ使用できます。ネットワーク設定を確認または編集するには、ネットワーク接続プロファイルを参照してください。

次の検査オプションから選択できます。

- すべてを検査する
- ルーターのみを検査する

- デバイスのみを検査する

信頼できるネットワークでのみネットワーク検査を実行してください。信頼できないネットワークで実行する場合は、潜在的な危険があることを認識してください。



ルーター検査が完了すると、デバイスに関する基本情報へのリンクがある通知が表示されるか、テーブルまたはソーナービューの不審なデバイスをダブルクリックできます。[**トラブルシューティング**]をクリックして最近ブロックされたコミュニケーションを確認します。ファイアウォールトラブルシューティングの詳細

ネットワーク検査モジュールでは2つの通知が表示されます。

- **ネットワークに接続された新しいデバイス** – ユーザーの接続中に以前に表示されていないデバイスがネットワークに接続された場合、通知が表示されます。
- **検出された新しいネットワークデバイス** – 信頼できるネットワークに再接続し、以前に表示されていないデバイスがある場合に表示されます。

いずれの通知タイプも、許可されていないデバイスがネットワークに接続しようとしていることを通知します。**デバイスの表示**をクリックすると、デバイス詳細情報が表示されます。

ネットワーク検査でデバイスに表示されるアイコンの意味は何ですか。

★	黄色の星アイコンは、ネットワークの新しいデバイスや、ESET によって初めて検出されたデバイスを示します。

	黄色の注意アイコンは、ルーターに脆弱性が含まれている可能性があることを示します。問題の詳細については、製品のアイコンをクリックしてください。
	赤い警告アイコンは、ルーターに脆弱性が含まれ、感染している可能性があるデバイスを示します。問題の詳細については、製品のアイコンをクリックしてください。
	ESET製品にルーターの詳細情報があるが、セキュリティリスクがないため、緊急の対応が必要がない場合、青いアイコンが表示されることがあります。詳細については、製品のアイコンをクリックしてください。

ネットワーク検査のネットワークデバイス

デバイスについての詳細情報が次の内容を含めここで確認できます。

- デバイス名
- デバイスのタイプ
- 前回表示
- ネットワーク名
- IPアドレス
- MACアドレス
- OS

鉛筆のアイコンは、デバイスの名前を修正したり、デバイスの名前やタイプを変更したりできます。

履歴から削除 – デバイスリストからデバイスを削除します。このオプションは、現在ネットワークに接続されていないデバイスでのみ使用できます。

デバイスのタイプごとに、次のアクションを使用できます。

ルーター

ルーター設定 – Webインターフェイスまたはモバイルアプリケーションを使用するか、**ルーターインターフェイスを開く**をクリックして、ルーター設定にアクセスできます。インターネットサービスプロバイダーによって提供されているルーターを使用している場合は、検出されたセキュリティの問題を解決するために、インターネットサービスプロバイダーサポートリソースまたはルーターの製造元に問い合わせなければならない場合があります。必ずルーターのユーザーガイドに記載されている適切な安全上の注意に従ってください。
保護 – ルーターとネットワークをサイバーセキュリティ攻撃から保護するには、次の基本的な推奨事項に従ってください。

ネットワークデバイス

デバイスID – ネットワークに接続されているデバイスが不明な場合は、デバイス名の下のベンダーまたは製造元名を確認します。これにより、デバイスの種類を特定しやすくなります。将来の参照のため、デバイス名を変更することができます。
デバイスの切断 – ネットワークまたはデバイスに接続されているデバイスが安全であることを確認できない場合は、ルーター設定でこのデバイスのネットワークアクセスを管理するか、ネットワークのパスワードを変更してください。
保護 – 攻撃および悪意のあるソフトウェアからデバイスを保護するには、デバイスにサイバーセキュリティ保護をインストールし、オペレーティングシステムとインストールされているソフトウェアを常に最新の状態に保ちます。保護を継続するために、保護されていないWi-Fiネットワークに接続しないでください。

このデバイス

このデバイスはネットワークのコンピューターを表します。
ネットワークアダプター–ネットワークアダプタ情報を表示します。

通知|ネットワーク検査

下記は、 ESET Security Ultimateがルーターで脆弱性の問題を検出した際に表示される通知です。各通知には簡単な説明が含まれ、ルーターの脆弱性リスクを最小限にするために実行すべきソリューションや手順も示されます。ルーターの変更について不明な点がある場合は、ルーターの製造元またはインターネットプロバイダーに問い合わせることをお勧めします。

潜在的な脆弱性が見つかりました
ルーターには、攻撃とエクスプロイトを容易にする既知の脆弱性が含まれる可能性があります。ルーターのファームウェアをアップデートしてください。

脆弱性が見つかりました
ルーターには、攻撃とエクスプロイトを容易にする既知の脆弱性が含まれます。ルーターのファームウェアをアップデートしてください。

マルウェアが検出されました
ルーターはマルウェアに感染しています。ルーターを再起動し、検査を繰り返します。

弱いルーターパスワード
ルーターのパスワードが弱く、他者が簡単に推測できます。ルーターでパスワードを変更します。

悪意があるネットワークリダイレクト
インターネットトラフィックが悪意のあるWebサイトにリダイレクトされているようです。これはルーターが不正アクセスされていることを意味することがあります。ルーターでDNSサーバー設定を変更します。

オープンネットワークサービス
ルーターは他者が悪用できるネットワークサービスを実行しています。これは、構成が適切ではないか、不正アクセスされているルーターによる可能性があります。ルーターの構成を確認してください。

注意が必要なオープンネットワークサービス
ルーターは他者が悪用できるネットワークサービスを実行しています。これは、構成が適切ではないか、不正アクセスされているルーターによる可能性があります。ルーターの構成を確認してください。

古いファームウェア
ルーターのファーウェアが古く、脆弱性が含まれる可能性があります。ルーターのファームウェアをアップデートしてください。

悪意があるルーター設定
ルーターが使用するDNSサーバーは悪意があり、危険なWebサイトに接続される可能性があります。これはルーターが不正アクセスされていることを意味することがあります。ルーターでDNSサーバー設定を変更します。

ネットワークサービス
ルーターは共通ネットワークサービスを実行しています。これらはネットワークによって必要で、安全であると考えられます。ルーターの構成を確認してください。

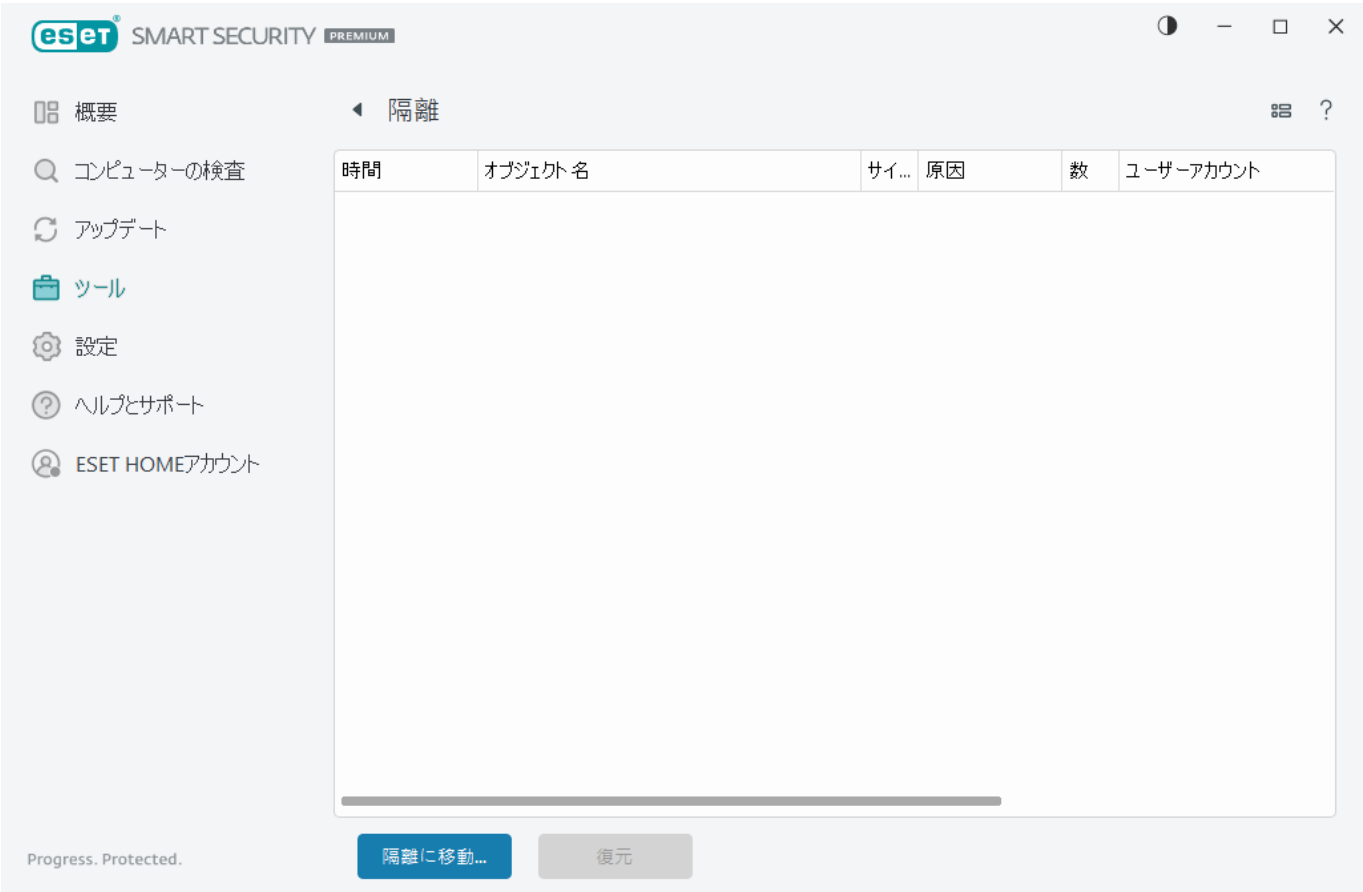
隔離

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 Security Ultimate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)。



ファイルの隔離

ESET Security Ultimate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。

a.駆除できない

b.安全でないか、削除することが推奨される

c.ESET Security Ultimateによって誤って検出された場合

d.ファイルが不審な動作をしているが、保護で検出されない場合

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。

a.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。

b.ファイルを右クリックし、**詳細設定オプション > ファイルを隔離**をクリックします。

c.**隔離**ウィンドウから**隔離に移動...**をクリックします。

d.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。隔離のすべてのアイテムを選択して削除する場合は、キーボードの**Ctrl + A**と**Delete**を押します。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。

検出の説明

項目を右クリックし、**検出の説明** をクリックすると、記録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が開きます。

図解手順
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 Security Ultimateで隔離されたファイルを復元する
- ESET Security Ultimateで隔離されたファイルを削除する
- ESET製品で検出が通知されました。何をすればよいですか。

隔離が失敗しました

特定のファイルを隔離に移動できない理由は次のとおりです。

- **読み取り権限がない** – ファイルの内容を表示できません。
- **書き込み権限がない** – ファイルの内容を修正できません。つまり、新しいコンテンツを追加したり、既存のコンテンツを削除したりできません。
- **隔離しようとしているファイルが大きすぎる** – ファイルサイズを減らす必要があります。

エラーメッセージ「隔離が失敗しました」を受信するときに、**詳細**をクリックします。隔離エラーリストウィンドウが表示され、ファイル名と理由、ファイルを隔離できない理由が表示されます。

分析のためにサンプルを提出

コンピューター上の疑わしいファイル、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)。

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

次の方法のいずれかを使用して、サンプル送信(ファイルまたはWebサイト)を分析用にESETに送信できます。

1. 製品のサンプル送信フォームを使用します。**ツール > 分析のためにサンプルを提出**にあります。送信されるサンプルの最大サイズは256MBです。

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/WinZIP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、迷惑メールの誤検知またはペアレンタルコントロールモジュールによって誤って分類されたWebサイトを報告するには、ESETナレッジベース記事を参照してください。

分析のサンプルを選択フォームで、**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)
- 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。**匿名で送信する**を選択すると、空欄になります。

> **ESETから連絡することはありません**
> 詳しい情報が必要でない限り、ESETから連絡することはありません。毎日、何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、このファイルの入手経緯を入力します。

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。

> 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 – 不審なサイト

サイトの問題点はなにですか。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**は、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。

- 上記のオプションが送信するサイトを参照していない場合は、**その他**を選択します。

備考および補足情報 – 不審なWebサイトの分析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 – 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。

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。

[**設定**]メニューには次のセクションに分割されます。

コンピュータ保護

インターネット保護

ネットワーク保護

セキュリティツール

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。

コンピュータ保護

プログラムのメインウィンドウ > **設定**の**コンピュータ保護**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。

- リアルタイムファイルシステム保護 – ファイルは全て、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。
- ESET LiveGuardは、特に、新しい脅威を軽減するために設計された、クラウドベース保護の層を追加します。

o**プロアクティブ保護** - ESET LiveGuard分析結果を受信するまで、新しいファイルの実行をブロックします。分析中のファイルをブロック解除する場合は、ファイルを右クリックし、**ESET LiveGuardによって分析されたファイルのブロック解除**をクリックします。

- デバイスコントロール – このモジュールを使用すると、拡張フィルタ/権限を検査、ブロック、または調整して、ユーザーによる指定デバイス(CD/DVD/USB...)へのアクセス方法や作業方法を選択できます。

- 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。

- ゲームモード – ゲームモードを有効または無効にします。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、ゲームモードを有効にするとメインウィンドウがオレンジに変わります。

- Webカメラアクセス制御のWebカメラにアクセスするプロセスとアプリケーションを制御します。

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。

リアルタイムファイルシステム保護の場合、歯車アイコンをクリックして、次のオプションから選択します。

- **設定** - リアルタイムファイルシステム保護詳細設定を開きます。

- **除外の編集** - 除外設定ウィンドウが開き、ファイルやフォルダーを検査から除外することができます。

Webカメラアクセス制御の場合、歯車アイコンをクリックして、次のオプションから選択します。

- **設定** - Webカメラアクセス保護詳細設定を開きます。

- **再起動するまですべてのアクセスをブロック** – コンピューターの再起動までWebカメラへのすべてのアクセスをブロックします。

- **すべてのアクセスを永久にブロック** – この設定が無効になるまでWebカメラへのすべてのアクセスをブロックします。

- **すべてのアクセスのブロックを停止** - Webカメラアクセスのブロック機能を無効にします。このオプションは、Webカメラアクセスがブロックされている場合にのみ使用できます。

ウイルス対策およびスパイウェア対策保護を一時停止 – ウイルス・スパイウェア対策保護機能すべてを無効にします。保護を無効にすると、ウィンドウが開き、**間隔**ドロップダウンメニューで保護を無効にする時間を決定できます。上級者ユーザーであるか、ESETテクニカルサポートの指示があった場合にのみ使用してください。

マルウェアが検出された

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、CD、DVDなど)など、さまざまです。

標準的な動作

ESET Security Ultimate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、「駆除レベル」を参照してください。

コンピューターで感染したファイルを検査する

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。

1.ESET Security Ultimateを開き、[**コンピューターの検査**]をクリックする

2.[**コンピューターの検査**]をクリックします。(詳細は「コンピューターの検査」を参照してください)。

3.検査終了後、ログで検査済みファイル、感染ファイル、および駆除済みファイルの件数をそれぞれ確認します。

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

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 Security Ultimate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。ファイルに対するアクションを選択して(アクションは、リストでファイルごとに個別に設定)、[**完了**]をクリックします。

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。

インターネット保護

インターネット接続は、パーソナルコンピュータの標準機能です。残念ながら、悪意のあるコードを転送する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** > **インターネット保護**を開き、ESET Security Ultimateのインターネット保護を強化する機能を設定します。

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。

ペアレンタルコントロールモジュールは、インターネット上の不適切なコンテンツや有害なコンテンツをブロックすることによって、お子様を保護します。

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サイトが誤って脅威として検出される。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 Security Ultimate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。

電子メールクライアント迷惑メール対策は、迷惑メールメッセージをフィルター処理します。

電子メールクライアント迷惑メール対策の場合、歯車アイコンをクリックして、次のオプションから選択します。

• **設定** - 電子メールクライアント迷惑メール対策の詳細設定を開きます。

• **ユーザーアドレスリスト**(有効な場合) – ダイアログウィンドウが開きます。アドレスを追加、編集、削除して、迷惑メール対策ルールを定義できます。このリストのルールは現在のユーザーに適用されます。

• **グローバルアドレスリスト**(有効な場合) – ダイアログウィンドウが開きます。アドレスを追加、編集、削除して、迷惑メール対策ルールを定義できます。このリストのルールはすべてユーザーに適用されます。

フィッシング対策機能

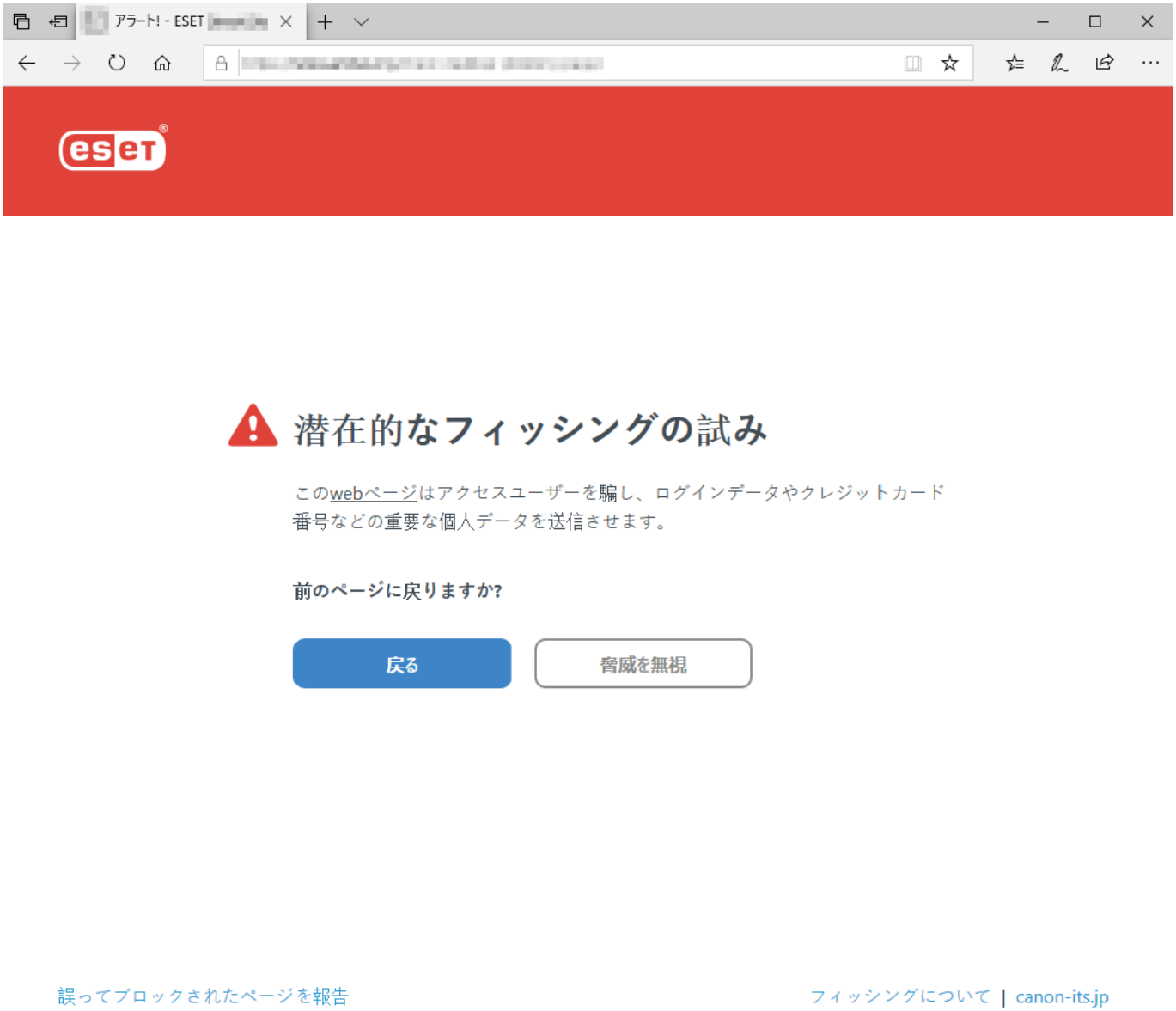
フィッシングはソーシャルエンジニアリング(機密情報を入手するためにユーザーを操る)を使用する犯罪活動です。フィッシングは、銀行の口座番号やPINなどの機密データにアクセスするために使用されます。詳細については、用語集を参照してくださいESET Security Ultimateはフィッシング対策機能を提供し、このようなコンテンツを配布することが知られているWebページをブロックできます。

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 Security Ultimate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。

ペアレンタルコントロール

ペアレンタルコントロール機能では、ペアレンタルコントロールを設定できます。この機能には、子どもを保護するためと、デバイスおよびサービスの使用に対する制限を設定するために有用な、保護者向けの自動化ツールが用意されています。この機能の目的は、子供や青少年が不適切または有害なコンテ

ンツのページにアクセスしないようにすることにあります。

[ペアレンタルコントロール]セクションでは、対象ユーザーに対して適切でない内容を掲載していると考えられるWebページをブロックします。さらに、事前に定義された40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。

特定のユーザーアカウントに対してペアレンタルコントロールを有効にするには、次の手順に従います。

1. ESET Security Ultimateでは、既定でペアレンタルコントロールが無効になっています。ペアレンタルコントロールを有効化するには2つの方法があります。

   • プログラムのメインウィンドウから、**設定 > インターネット保護 > ペアレンタルコントロール**でトグルアイコンをクリックし、ペアレンタルコントロールの状態を有効に変更します。

   • 詳細設定 > **保護 > Webアクセス保護 > ペアレンタルコントロール**を開き、**ペアレンタル コントロールを有効にする**の横にあるトグルを有効にします。

2. メインプログラムウィンドウから、**設定 >インターネット保護>ペアレンタルコントロール**をクリックします。**ペアレンタルコントロール**の横に**有効**が表示されますが、矢印記号をクリックした後に、次のウィンドウで**[子アカウントを保護...]**または**[親アカウント]**をクリックし、目的のアカウントに対してペアレンタルコントロールを設定する必要があります。次のウィンドウに年齢を入力すると、アクセスレベルおよび推奨の適正年齢のWebページが決まります。これで、指定されたアカウントでのペアレンタルコントロールが有効になります。アカウント名の下の**[ブロックされたコンテンツと設定…]**をクリックし、分類タブで、許可またはブロックする分類をカスタマイズします。分類に一致しないカスタムWebページを許可またはブロックするには、例外タブをクリックします。

ESET Security Ultimateの製品のメインウィンドウの**[設定]**ペインにある**[インターネット保護]** > **[ペアレンタルコントロール]**をクリックするとメインウィンドウが表示されます。

Windowsユーザーアカウント

既存のアカウントのロールを作成した場合は、ここに表示されます。スライダー  をクリックすると、ペアレンタルコントロールの横の緑のチェックマーク  が表示されます。アクティブなアカウントで、[ブロックされたコンテンツと設定...]をクリックすると、 このアカウントのWebページの許可された分類の一覧と、ブロックまたは許可されたWebページの一覧が表示されます。

このウィンドウの下部には、次が含まれます。

Webサイトの例外を追加... – 特定のWebサイトは、個別にそれぞれのペアレンタルアカウントの設定に従って許可またはブロックすることができます。

ログを表示 – ペアレンタルコントロールアクティビティの詳細ログを表示します。(ブロックされたページ、アカウント、ページがブロックされた理由、カテゴリなど) 選択した基準に基づいて、  **[フィルタリング]**をクリックしてこのログのフィルタを行うこともできます。

ペアレンタルコントロール

ペアレンタルコントロールを無効にした後、**ペアレンタルコントロールを無効にする**ウィンドウが表示されます。ここでは、保護が無効になる間隔を設定できます。その後、このオプションは**[停止中]**または**[永久に無効にする]**に変わります。

ESET Security Ultimate内の設定をパスワードで保護することが重要です。このパスワードは、[アクセス設定]セクションで設定できます。パスワードを設定しないと**[すべての設定をパスワードで保護し、不正な変更を予防する。]**という警告が表示されます。[ペアレンタルコントロール]で設定された制限は、標準ユーザーアカウントにのみ影響します。管理者はすべての制限を無視できるため、影響を受けません。

> ペアレンタルコントロールが正しく機能するには、ネットワークトラフィックスキャナーHTTP(S)トラフィック検査、およびファイアウォールを有効にする必要があります。これらの機能はすべて、既定で有効になっています。

Webサイト例外

Webサイトの例外を追加するには、**[設定]** > **[インターネット保護]** > **[ペアレンタルコントロール]** をクリックし、**[Webサイトの例外を追加]**をクリックします。

例外URLフィールドにURLを入力し、(許可)または(ブロック)を各固有のユーザーアカウントに対して選択し、**OK**をクリックしてリストに追加します。

リストからURLアドレスを削除するには、**設定 > インターネット保護 > ペアレンタルコントロール**をクリックし、**[ブロックされたコンテンツと設定...]**を任意のユーザーアカウントでクリックし、**例外**タブで例外を選択し、**削除**をクリックします。

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

特定のWebページをブロックするか許可するほうが、1つの分類のWebページをブロックまたは許可するより、精度が高くなることがあります。これらの設定を変更したり、分類やWebページをリストに追加する場合は注意してください。

ユーザーから例外をコピーする

作成した例外をコピーするドロップダウンメニューからユーザを選択します。

アカウントからカテゴリをコピーする

既存の修正されたアカウントからブロックまたは許可される分類のリストをコピーできます。

ネットワーク保護

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** > **ネットワーク保護**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、そのモジュールの詳細設定にアクセスします。

ファイアウォール - ESET Security Ultimate設定に基づいてすべてのネットワーク通信をフィルタリングします。

設定 - ファイアウォールの詳細設定を開きます。ここでは、ファイアウォールでネットワーク通信を処理する方法を定義できます。

ファイアウォールの一時停止(すべてのトラフィックを許可) – ファイアウォールのすべてのフィルタリングオプションが無効になり、すべての着信および発信が許可されます。ネットワークトラフィックフィルタリングがこのモードのときに、**[ファイアウォールを有効にする]**をクリックして、ファイアウォールを再有効化します。

すべてのトラフィックを遮断 – すべての内向きおよび外向きの通信は、ファイアウォールによってブロックされます。このオプションは、セキュリティ上の重大なリスクの疑いがあってシステムをネットワークから切断する必要がある場合にのみ使用してください。ネットワークトラフィックフィルタリングが**すべてのトラフィックをブロック**モードのときに、**[すべてのトラフィックのブロックを停止]**をクリックすると、ファイアウォールを標準の動作に復元します。

ルール付き自動モード – (別のフィルタリングモードが有効な場合) – クリックすると、フィルタリングモードを自動フィルタリングモードに変更します(ユーザー定義ルールを使用)。

対話モード – (別のフィルタリングモードが有効な場合) – クリックすると、フィルタリングモードを対話フィルタリングモードに変更します。

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。保護されていないワイヤレスネットワークや保護が弱いネットワークに接続するとESET Security Ultimateによって通知されます。

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。

ネットワーク接続 – どのネットワークアダプタに接続されているかと、詳細情報を示します。

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。

ネットワーク接続

どのネットワークアダプタに接続されているかを示すものです。ネットワーク接続を表示するには、プログラムのメインウィンドウ > **設定** > **ネットワーク保護** > **ネットワーク接続**を開きます。

一覧で接続をダブルクリックすると、その詳細とネットワークアダプタの詳細が表示されます。

特定のネットワーク接続にカーソルを合わせ、**信頼済み**列のメニューアイコン をクリックして、次のいずれかのオプションを選択します。

- **編集** - ネットワーク保護の設定ウィンドウが開き、ネットワーク保護プロファイルを特定のネットワークに割り当てることができます
- **消去** – ネットワーク接続設定を既定にリセットします
- **ネットワーク検査でネットワークを検査** - ネットワーク検査を開き、ネットワーク検査を実行します。
- **「マイネットワーク」に設定** – 「マイネットワーク」タグをネットワークに追加します。このタグはESET Security Ultimateでネットワークの横に表示され、識別しやすくなり、セキュリティの概要も見やすくなります
- **「マイネットワークの設定を解除** – 「マイネットワーク」タグを削除します。ネットワークがすでにタグ付けされている場合にのみ使用できます

ネットワーク接続詳細

ネットワーク接続の一覧で接続をダブルクリックすると、その詳細とネットワークアダプタの詳細が表示されます。ネットワーク接続とアダプタの詳細は、ネットワークアクセス保護で設定しようとしているネットワークを識別するのに役立ちます。

ネットワーク接続詳細:

- ネットワーク接続の状態
- 最初のネットワーク検出の日時
- ネットワークが最後にアクティブだった時刻
- このネットワークへの接続に費やされた合計時間
- ネットワーク接続プロファイル

- Windowsで定義されているネットワーク接続プロファイル
- 保護ネットワーク保護設定(ネットワークが信頼されているかどうか)

ネットワークアダプタの詳細:

- 接続の種類(有線、仮想など)
- ネットワークアダプタ名
- アダプタの説明
- IPアドレスとMACアドレス
- ネットワークのIPv4およびIPv6アドレスとサブネット
- DNSサフィックス
- DNSサーバーのIP
- DHCPサーバーのIP
- 既定のゲートウェイIPとMACアドレス
- アダプタMACアドレス

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** > **ネットワーク保護** > **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。

ファイアウォールルールを開くをクリックして、ウィザードによって作成されたルールを表示します。また、詳細設定 > **保護** > **ネットワークアクセス保護** > **ファイアウォール** > **ルール** > **編集**で、ウィザードによって作成されたルールを確認することができます。

> 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。これを表示するには、プログラムのメインウィンドウ > **設定** > **ネットワーク保護** > **一時的にブロックされたIPアドレスを解決**を開き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 Security Ultimate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** > **ネットワーク保護** > **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。

ファイアウォールの問題の解決

ESET Security Ultimate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、ファイアウォールが原因になっているかどうかを判断できます。さらに、ファイアウォールを使用すると、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。

ファイアウォール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
- ファイアウォール通知からの例外の作成
- 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 Security Ultimate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 Security Ultimate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。

ファイアウォール通知からの例外の作成

ESETファイアウォールが悪意のあるネットワークアクティビティを検出すると、イベントを説明する通知ウィンドウが表示されます。この通知にはリンクがあり、イベントの詳細を確認し、必要に応じてこのイベントのルールを設定できます。

ネットワークアプリケーションまたはデバイスがネットワーク規格を正しく実装していない場合、ファイアウォールIDS通知が繰り返しトリガーされる可能性があります。通知から直接例外を作成し、ESETファイアウォールがこのアプリケーションまたはデバイスを検出しないようにできます。

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**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。

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 Security Ultimate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。

ESET Windowsホーム製品でネットワークトラフィックスキャナーを管理する方法については、ナレッジベース記事を参照してください。

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。

新しいネットワークが検出されました

既定ではESET Security Ultimateは、新しいネットワーク接続が検出されたときに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 Security Ultimate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。

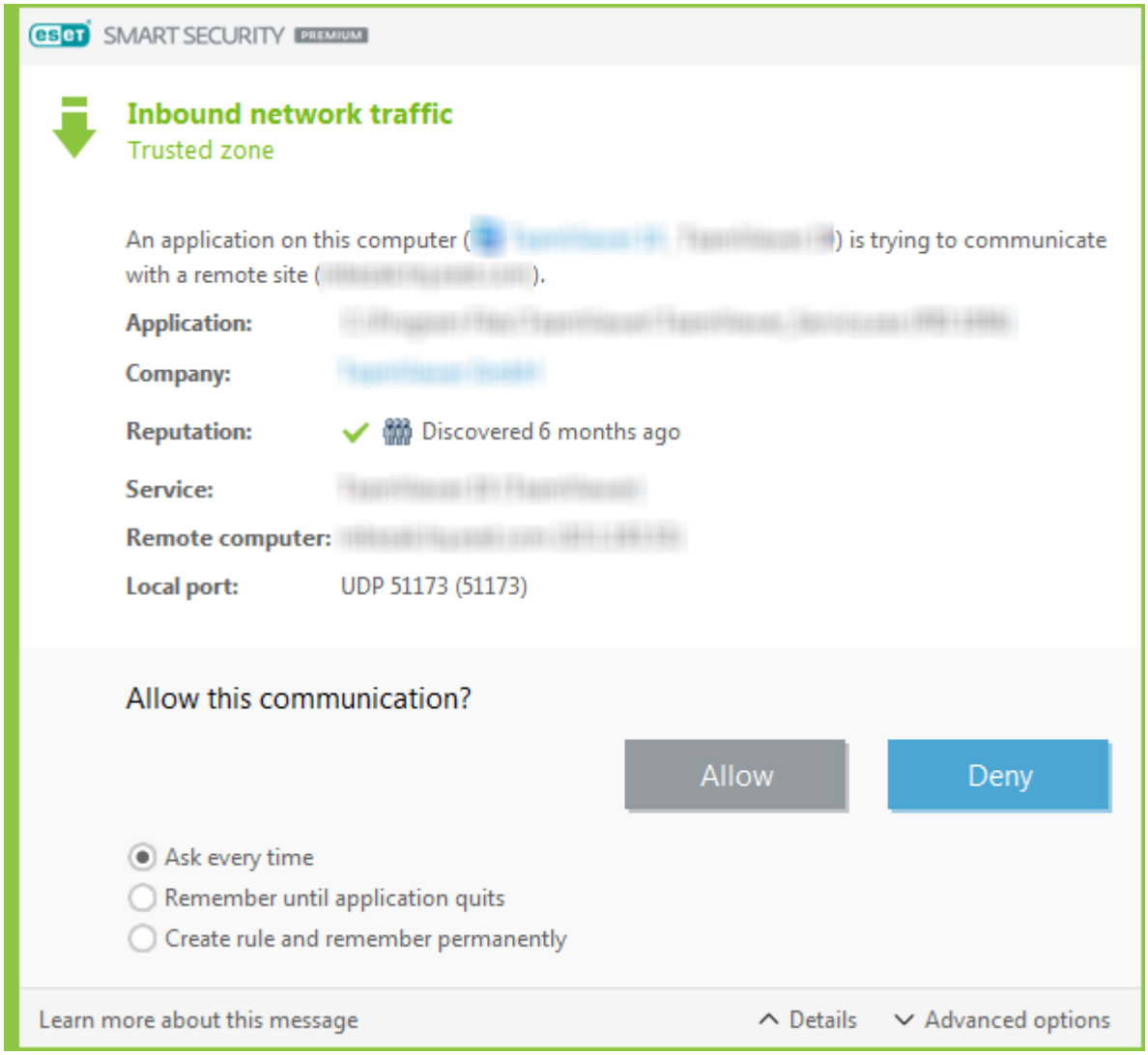
ユーザ定義プロファイル - 作成したプロファイルの1つをドロップダウンメニューから選択できます。このオプションは、1つ以上のカスタムプロファイルを作成した場合にのみ使用できます。

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。

接続の確立 – 検出

ファイアウォールでは、新しく確立された各ネットワーク接続が検出されます。有効なファイアウォールモードによって、新しいルールに対して実行されるアクションが決まります。**ルール付き自動モード**または**ポリシーベースモード**を有効にする場合、ファイアウォールはあらかじめ定義されたアクションをユーザーの操作なしで実行します。

対話モードでは、新しいネットワーク接続の検出を報告する情報ウィンドウが表示されます。このウィンドウには、接続に関する詳細情報も表示されます。接続の**許可**または**拒否**(ブロック)を選択できます。ダイアログウィンドウで同じ接続を繰り返し許可する場合は、その接続の新しいルールを作成することをお勧めします。そのためには、**ルールを作成し、永久に記憶**を選択し、ファイアウォールの新しいルールとしてそのアクションを保存します。その後、ファイアウォールで同じ接続が認識されると、ユーザー対話を必要としないで既存のルールが適用されます。



新しいルールを作成する際は、安全であることが確実な接続だけを許可してください。すべての接続が許可されると、ファイアウォールはその目的を達成することができません。接続に関する重要なパラメーターは次のとおりです。

アプリケーション – 実行ファイルの場所とプロセスID不明なアプリケーションとプロセスの接続を許可しないでください。

署名者 – アプリケーションの発行者名。テキストをクリックすると、会社のセキュリティ証明書が表示されます。

レピュテーション – 接続のリスクレベル。接続には次のリスクレベルが割り当てられます。良(緑)、不明(オレンジ)、または危険(赤)。この割り当てには、各接続の特性、ユーザー数、検出時間を検査する一連のヒューリスティックルールが使用されます。この情報は、ESETLiveGrid®技術によって収集されます。

サービス – サービスの名前（アプリケーションがWindowsサービスの場合）。

リモートコンピューター – リモートデバイスのアドレス。不明なアプリケーションやプロセスの接続を許可することはお勧めしません。

リモートポート – 通信ポート。通常の状況では、共通ポート(ポート番号80、443のWebトラフィックなど)を許可できます。

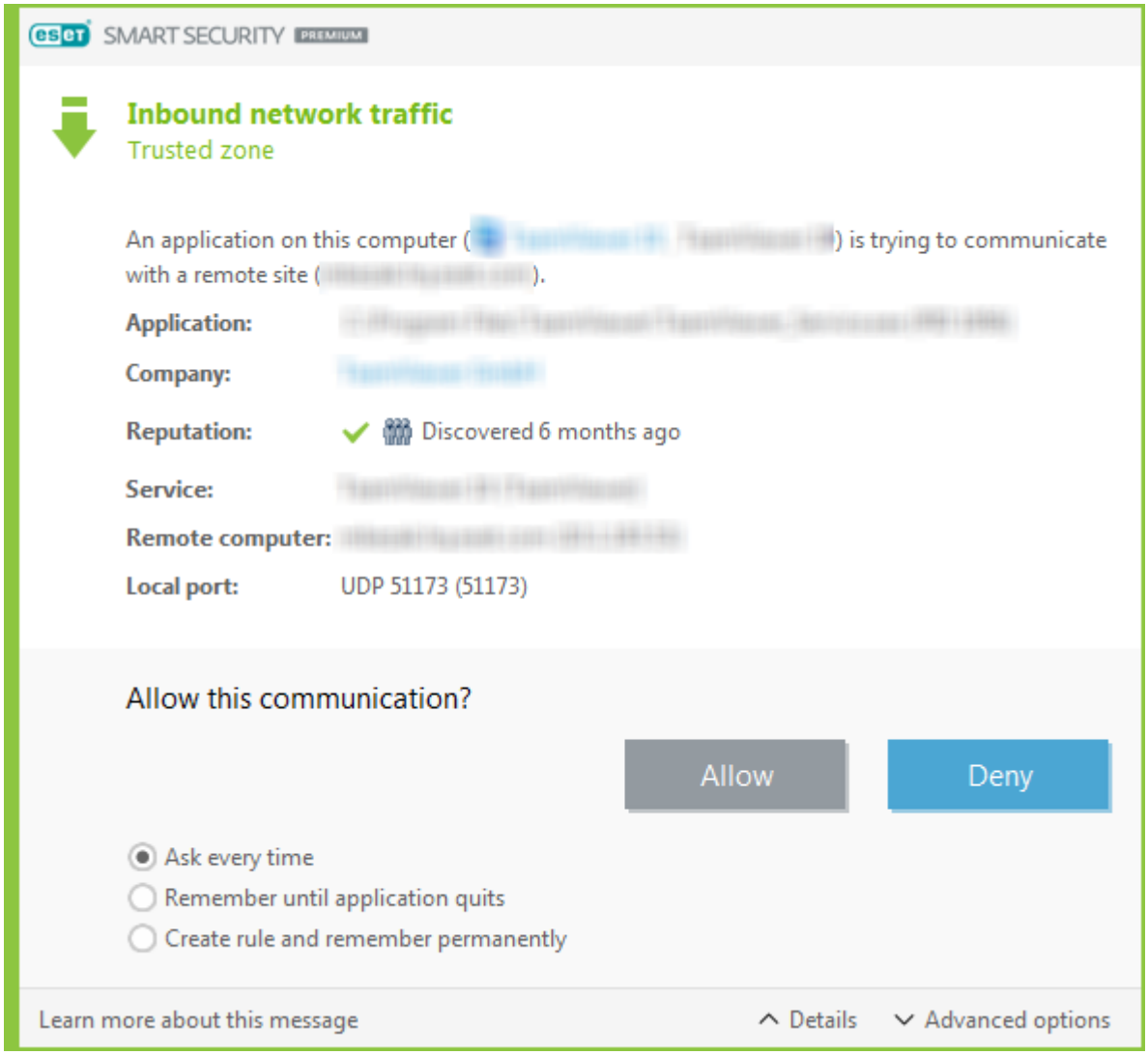
コンピューターの侵入は、多くの場合、インターネットや表示されない接続を使用してリモートシステムに感染して増殖します。ルールが正しく設定されていれば、ファイアウォールは、悪意のあるコードによるさまざまな攻撃から保護するための有効なツールとなります。

アプリケーションの変化

ファイアウォールが、コンピュータから発信する外側への接続を確立するために使用されるアプリケーションに変化が生じたことを検出しました。アプリケーションが単に新しいバージョンに更新されたに過ぎない可能性もありますが、悪意のあるアプリケーションによって変化させられた可能性もあります。正当な変更を加えた覚えがない場合には、接続を拒否し、最新のウイルス定義データベースを使用してコンピュータをスキャンすることをお勧めします。

信頼された内向きの通信

信頼ゾーン内の内向き通信の例:
コンピュータで実行されているローカルアプリケーションとの通信を確立しようとしている、信頼ゾーン内のリモートコンピュータ。



アプリケーション – リモートデバイスからアクセスされるアプリケーション。

アプリケーションパス – アプリケーションの場所。

Microsoft Storeアプリケーション - Microsoft Store内のアプリケーションの名前。

署名者 – アプリケーションの発行者名。テキストをクリックすると、会社のセキュリティ証明書が表示されます。

評価 - ESET LiveGrid®技術によって取得されたアプリケーションの評価。

サービス – 現在コンピューターで実行中のサービスの名前。

リモートコンピュータ – コンピューター上のアプリケーションとの通信を確立しようとしているリモートコンピュータ。

リモートポート – 通信に使用されるポート。

毎回確認 – ルールの既定のアクションを**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。

アプリケーションが終了するまで記憶 - ESET Security Ultimateは、次の再起動まで、選択したアクションを記憶しています。

ルールを作成し、永久に記憶 – 通信を許可または拒否する前にこのオプションを選択すると、ESET

Security Ultimateによってそのアクションが記憶され、そのリモートコンピューターからアプリケーションに再度アクセスするときに使用されます。

許可 – 外向きの通信を許可します。

拒否 – 外向きの通信を拒否します。

ルールの編集 - ファイアウォールルールエディターを使用してルールプロパティをカスタマイズできます。

信頼された外向きの通信

信頼ゾーン内の外向き通信の例:
ローカルネットワーク内または信頼ゾーンのネットワーク内の別のコンピュータとの接続を確立しようとしている、ローカルアプリケーション。

アプリケーション – リモートデバイスからアクセスされるアプリケーション。

アプリケーションパス – アプリケーションの場所。

Microsoft Storeアプリケーション - Microsoft Store内のアプリケーションの名前。

署名者 – アプリケーションの発行者名。テキストをクリックすると、会社のセキュリティ証明書が表示されます。

評価 - ESET LiveGrid®技術によって取得されたアプリケーションの評価。

サービス – 現在コンピューターで実行中のサービスの名前。

リモートコンピュータ – コンピューター上のアプリケーションとの通信を確立しようとしているリモー

トコンピュータ。

リモートポート – 通信に使用されるポート。

毎回確認 – ルールの既定のアクションを**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。

アプリケーションが終了するまで記憶 - ESET Security Ultimateは、次の再起動まで、選択したアクションを記憶しています。

ルールを作成し、永久に記憶 – 通信を許可または拒否する前にこのオプションを選択すると、ESET Security Ultimateによってそのアクションが記憶され、そのリモートコンピューターからアプリケーションに再度アクセスするときに使用されます。

許可 – 外向きの通信を許可します。

拒否 – 外向きの通信を拒否します。

ルールの編集 - ファイアウォールルールエディターを使用してルールプロパティをカスタマイズできます。

内向きの通信

受信インターネット接続の例:
コンピュータで実行されているアプリケーションと通信しようとしているリモートコンピュータ。

アプリケーション – リモートデバイスからアクセスされるアプリケーション。

アプリケーションパス – アプリケーションの場所。

Microsoft Storeアプリケーション - Microsoft Store内のアプリケーションの名前。

署名者 – アプリケーションの発行者名。テキストをクリックすると、会社のセキュリティ証明書が表示されます。

評価 - ESET LiveGrid®技術によって取得されたアプリケーションの評価。

サービス – 現在コンピューターで実行中のサービスの名前。

リモートコンピュータ – コンピューター上のアプリケーションとの通信を確立しようとしているリモートコンピュータ。

リモートポート – 通信に使用されるポート。

毎回確認 – ルールの既定のアクションを**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。

アプリケーションが終了するまで記憶 - ESET Security Ultimateは、次の再起動まで、選択したアクションを記憶しています。

ルールを作成し、永久に記憶 – 通信を許可または拒否する前にこのオプションを選択すると、ESET Security Ultimateによってそのアクションが記憶され、そのリモートコンピューターからアプリケーションに再度アクセスするときに使用されます。

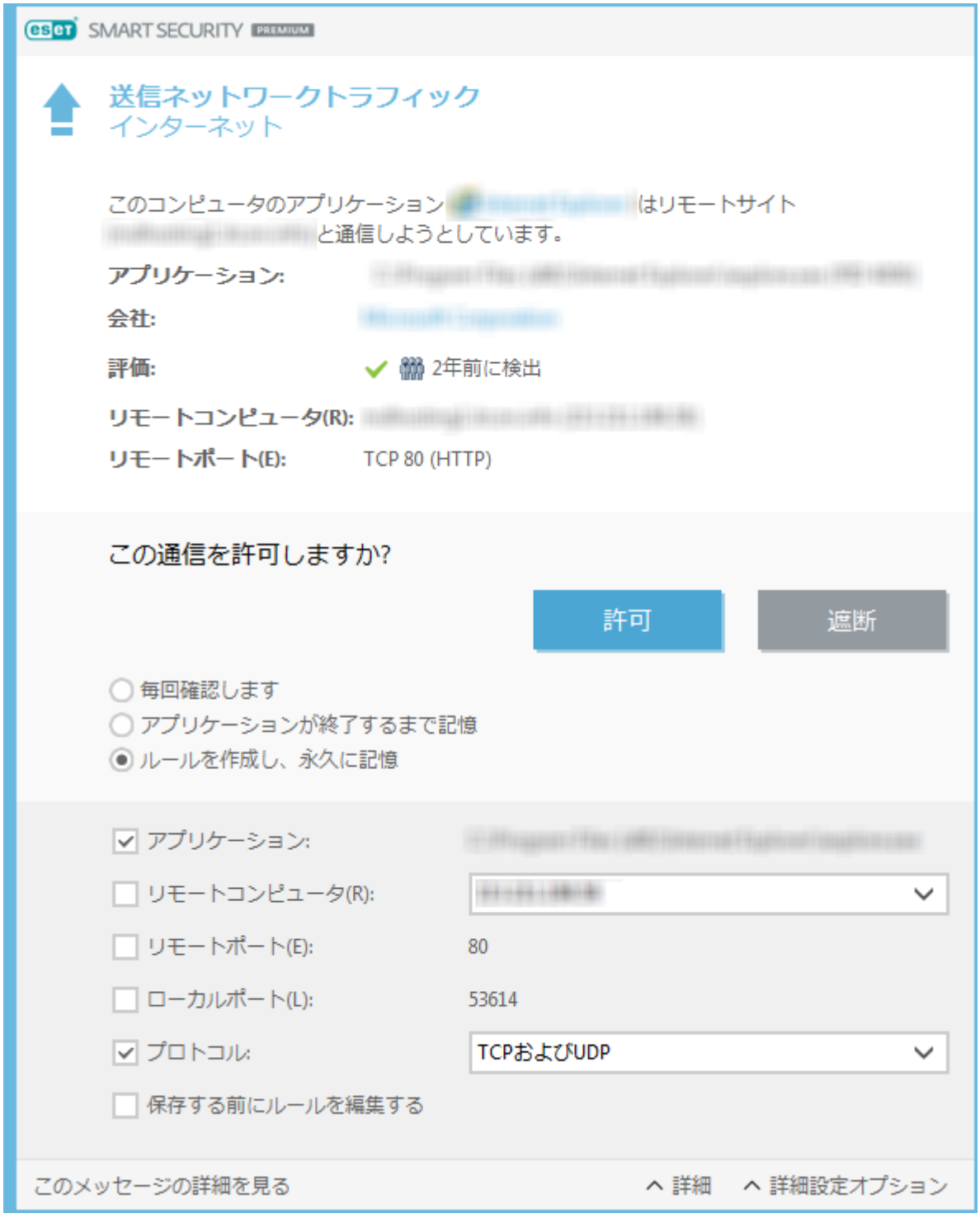
許可 – 外向きの通信を許可します。

拒否 – 外向きの通信を拒否します。

ルールの編集 - ファイアウォールルールエディターを使用してルールプロパティをカスタマイズできます。

外向きの通信

送信インターネット接続の例:
インターネット接続を確立しようとしているローカルアプリケーション。



アプリケーション – リモートデバイスからアクセスされるアプリケーション。

アプリケーションパス – アプリケーションの場所。

Microsoft Storeアプリケーション - Microsoft Store内のアプリケーションの名前。

署名者 – アプリケーションの発行者名。テキストをクリックすると、会社のセキュリティ証明書が表示されます。

評価 - ESET LiveGrid®技術によって取得されたアプリケーションの評価。

サービス – 現在コンピューターで実行中のサービスの名前。

リモートコンピュータ – コンピューター上のアプリケーションとの通信を確立しようとしているリモートコンピュータ。

リモートポート – 通信に使用されるポート。

毎回確認 – ルールの既定のアクションを**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。

アプリケーションが終了するまで記憶 - ESET Security Ultimateは、次の再起動まで、選択したアクションを記憶しています。

ルールを作成し、永久に記憶 – 通信を許可または拒否する前にこのオプションを選択するとESET Security Ultimateによってそのアクションが記憶され、そのリモートコンピューターからアプリケーションに再度アクセスするときに使用されます。

許可 – 外向きの通信を許可します。

拒否 – 外向きの通信を拒否します。

ルールの編集 - ファイアウォールルールエディターを使用してルールプロパティをカスタマイズできます。

接続の表示設定

次の追加オプションを表示するには、接続を右クリックします。

ホスト名を解決 – 可能な場合、全てのネットワークアドレスが、数字によるIPアドレス形式ではなくDNS形式で表示されます。

TCP接続のみを表示 – リストにはTCPプロトコルスイートに属する接続のみが表示されます。

リスンしている接続を表示 – このオプションを選択すると、現時点では通信が確立されていない接続のうち、システムがポートを開いており、接続を待機しているもののみが表示されます。

コンピュータ内部の接続を表示 – このオプションを選択すると、リモート側がローカルシステム(つまり、localhost)の接続のみが表示されます。

更新間隔 – アクティブな接続を更新する頻度を選択します。

最新の情報に更新 - [**ネットワーク接続**]ウィンドウを読み込み直します。

セキュリティツール

プログラムのメインウィンドウ > **設定** > **セキュリティツール**を開き、次のモジュールを調整します。

バンキングとブラウジング保護 – オンライン処理中に金融データを保護するための強化された保護レイヤーです。バンキングとブラウジング保護詳細設定で**すべてのブラウザーを保護**を有効にすると、サポートされているWebブラウザーがすべて保護モードで起動します。

ブラウザーのプライバシーおよびセキュリティ—デジタルフットプリントを残さずに、オンラインアクティビティをプライベートかつ安全に保ちます。

アンチセフト – アンチセフトを有効にすると、紛失または盗難の際にコンピューターを保護します。

Secure Data - Secure Dataを有効にすると、データを暗号化し、個人情報や機密情報の悪用を防止できます。

Password Manager – Password Managerはパスワードと個人データを保護して保存します。

VPN – データを保護し、匿名IPアドレスで不要な追跡を回避します。

Identity Protection—個人情報、信用情報、財務情報を保護します。

バンキングとブラウジング保護

バンキングとブラウジング保護は、オンライン処理中に金融データを保護するための強化された保護レイヤーです。

既定では、すべてのサポートされているWebブラウザーが安全モードで起動します。これにより、自動的に、1つのセキュアーブラウザーウィンドウで、インターネットを閲覧したり、インターネットバンキングにアクセスしたり、オンライン購入と取引を行ったりできます。

ESET LiveGrid®レピュテーションシステムを有効(既定で有効)にし、バンキングとブラウジング保護が正常に動作することを保証する必要があります。

セキュアーブラウザの動作を構成するには、バンキングとブラウジング保護の詳細設定を参照してください。**すべてのブラウザーを保護**を無効にする場合は、メインプログラムウィンドウ > **概要** > **バンキングとブラウジング保護**で、または**バンキングとブラウジング保護**デスクトップアイコンをクリックして、セキュアーブラウザにアクセスできますWindowsで既定に設定されたブラウザーは安全モードで起動します。

HTTPS暗号化通信の使用は、ブラウジングの保護に必要となります。次のブラウザは、バンキングとブラウジング保護をサポートしています。

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+

ARMプロセッサーが搭載されているデバイスではFirefoxおよびMicrosoft Edgeのみがサポートされます。

バンキングとブラウジング保護の詳細については、次のESETナレッジベース記事(英語およびその他の言語)をお読みください。

- ESETバンキングとブラウジング保護を使用する方法
- ESET Windowsホーム製品でのバンキングとブラウジング保護の一時停止または無効化
- ESETバンキングとブラウジング保護—一般的なエラー
- ESET用語集 | バンキングとブラウジング保護

ブラウザー内通知

セキュアーブラウザーは、ブラウザー内通知とブラウザーフレームの色でユーザーに現在の状態を通知します。

ブラウザー内通知は右側のタブに表示されます。

ブラウザー内通知を展開するにはESETアイコンをクリックします。通知を最小化するには、通知テキストをクリックします。通知と緑のブラウザーフレームを閉じるには、閉じるアイコンをクリックします。

情報通知と緑のブラウザーフレームのみを非表示にできます。

ブラウザー内通知

通知タイプ	状況
情報通知と緑のブラウザーフレーム	最大の保護が保証されます。既定では、ブラウザー内通知が最小化されます。ブラウザー内通知を展開し、**設定**をクリックして、セキュリティツール設定を開きます。
警告とオレンジ色のブラウザーフレーム	セキュアーブラウザーで、重大ではない問題に関する注意が必要です。問題または解決策の詳細については、ブラウザー内通知の手順に従ってください。
セキュリティアラートと赤いブラウザーフレーム	ブラウザーは、ESETバンキングとブラウジング保護で保護されません。ブラウザーを再起動して、保護がアクティブな状態であることを確認してください。ブラウザーに読み込まれたファイルとの競合を解決するには、ログファイル > [**バンキングとブラウジング保護**]を開き、次回ブラウザーを起動しても、ログファイルが読み込まれないことを確認してください。問題が解決しない場合は、ナレッジベース記事の手順に従い、ESETテクニカルサポートに問い合わせてください。

ブラウザーのプライバシーおよびセキュリティ

ブラウザーのプライバシーおよびセキュリティ機能は、サポートされているブラウザーで利用可能なカスタム拡張機能を使用して有効にできます(Google ChromeMozilla FirefoxMicrosoft Edgeのみ)。

拡張機能をインストールして有効にするには:

1. ESET Security Ultimateの最新バージョンを使用し、更新後にコンピューターを正常に再起動してください。
2. ブラウザーを開きます。

3. 拡張機能はブラウザーにインストールされます。

4. 拡張機能を有効にすると、拡張機能の詳細ページがブラウザーに表示されます。

ブラウザーのプライバシーおよびセキュリティブラウザー拡張機能のメインメニューは、次のセクションに分かれています。

概要

セキュア検索

検索結果の検査の横にあるトグルアイコン  をクリックして機能を有効にし、クリックしても安全な結果を確認します。セキュア検索は、リストのリンクアドレスを評価しますが、必ずしもWebサイトにマルウェアが含まれていないことを意味するわけではありません。その後、当社の検出エンジンがWebサイト上のマルウェアを検出します。

ブラウザークリーンアップ

閲覧データを削除するか、定期的なクリーンアップを設定します。**リストに追加する**ことでCookieを受け入れ、ブラウザークリーンアップを実行した後もログインしたままにするWebサイトを追加できます。

- **1 回限りのクリーンアップ** –ドロップダウンメニューから時間範囲を選択し、削除するデータ タイプを選択します。すべてのデータ、プライベート、カスタムの選択をオプションから選択できます。

- **定期的なクリーンアップ**-**定期的なクリーンアップ**の横にあるトグルアイコン  **をクリックして**、この機能を有効にします。ドロップダウンメニューから時間範囲を選択し、定期的に削除するデータタイプを選択します。すべてのデータ、プライベート、カスタムの選択をオプションから選択できます。

カスタムデータオプションには、次のカテゴリがあります。

- 閲覧履歴
- ダウンロード履歴
- CookieとWebサイトのデータ
- キャッシュされた画像とファイル
- パスワードとサインインデータ
- フォームの自動入力データ

メタデータクリーンアップ

メタデータクリーンアップ機能は、メディアファイル、ドキュメント、およびその他のサポートされているファイル形式で共有されるEXIFメタデータを介して公開される可能性のあるプライバシーデータを制御します。**画像をアップロードするたびにメタデータを消去**の横にあるトグルアイコン  をクリックすると、メタデータを削除できるようになります。

メタデータクリーンアップが正しく機能することを確認するには、ブラウザーを再起動する必要があります。

ブラウザー内通知を受信の横にあるトグルアイコン  をクリックして、メタデータクリーンアップ後に通知を表示できるようにします。

Webサイト設定の確認

Webサイトの権限に簡単にアクセスして管理し、Webサイトが使用できる情報を制御します。

- **通知** – 通知を**許可/ブロック**するWebサイトや、ブラウザー拡張機能で**毎回確認**するかどうかを確認します。

詳細設定

ブラウザークリーンアップ

Cookieの詳細設定

Cookieを受け入れ、ブラウザークリーンアップを実行した後もログインしたままにするWebサイトの一覧。テキストフィールドにURLアドレスを入力し、**追加**をクリックします。特定のWebサイトの横にあるマイナスアイコン をクリックすることで、リストからいつでも削除できます。

ページの下部には、ブラウザーで現在開いている推奨ドメインのリストがあります。特定のWebサイトが表示されない場合は、**リストを更新**し、プラスアイコン をクリックして、許可されたCookieリストに追加します。

Webサイト設定の確認

Webサイトの権限に簡単にアクセスして管理し、Webサイトが使用できる情報を制御します。

- **通知** – 通知を**許可/ブロック**するWebサイトや、ブラウザー拡張機能で**毎回確認**するかどうかを確認します。

外観

好みに合わせてインターフェースの配色をカスタマイズします。**ライト**または**ダーク**チェックボックスをオンにすると、好みの配色を選択できます。

アンチセフト

自宅から職場への毎日の通勤や他の公共の場所への外出時には、パーソナルデバイスが常に紛失や盗難のリスクにさらされています。アンチセフトは、デバイスの紛失・盗難に備えて、ユーザーレベルのセキュリティを強化する機能です。アンチセフトでは、デバイスの使用を監視したり、ESET HOMEでIPアドレスによる位置検出機能を使用して紛失中のデバイスを追跡したりできるので、デバイスの回収と個人データの保護に役立ちます。

IPアドレスによる位置検出Webカメラによる写真撮影、ユーザーアカウント保護、デバイス監視を備えているアンチセフトは紛失・盗難にあったコンピューターやデバイスが、今どこに有るかを調べる際に、個人ユーザーおよび法執行機関を支援します。ESET HOMEでは、コンピューターまたはデバイスで実行されるアクティビティを確認できます。

ESET HOMEでアンチセフトの詳細を確認するには、ESET HOMEオンラインヘルプを参照してください。

ユーザーアカウント管理の制限により、ドメインのコンピューターではアンチセフトが正常に動作しない場合があります。

アンチセフトを有効にした後、メインプログラムウィンドウ > 設定 > セキュリティツール > アンチセフトでデバイスのセキュリティを最適化できます

最適化オプション

架空アカウントが作成されていません

架空アカウントを作成すると、紛失または盗難されたデバイスの場所を特定できる可能性が高くなります。デバイスを紛失に設定すると、アンチセフトはアクティブなユーザーアカウントへのアクセスをブロックして、機密データを保護します。デバイスの使用を試行したユーザーは、架空アカウントの使用のみが許可されます。架空アカウントは、権限が制限されたゲストアカウントの形式です。デバイスが「回復済み」に設定されるまでは、既定のシステムアカウントとして使用されます。他のユーザーアカウントにログインしたり、ユーザーのデータにアクセスしたりできません。

i コンピューターが通常状態のときに、誰かが架空アカウントにログインすると、いつでも、コンピューターでの不審なアクティビティに関する情報が記載された通知が電子メールで送信されます。電子メール通知を受信した後、コンピューターを「紛失」に設定するかどうかを決定できます。

架空アカウントを作成するには、**架空アカウントの作成**をクリックし、**架空アカウントの名前**をテキストフィールドに入力して、**作成**をクリックします。

架空アカウントが作成されたら、**架空アカウント設定**をクリックして、アカウントの名前を変更または削除します。

Windowsアカウントパスワード保護

ユーザーアカウントはパスワードで保護されていません。1つ以上のユーザーアカウントがパスワードで保護されていない場合は、この最適化警告が表示されます。コンピューターのすべてのユーザー(**架空アカウント**を除く)のパスワードを作成すると、この問題が解決されます。

ユーザーアカウントのパスワードを作成するには、**Windowsアカウント**の管理をクリックしてパスワードを変更するか、次の手順に従います。

1. キーボードでCTRL+Alt+Deleteを押します。
2. **パスワードの変更**をクリックします。
3. **古いパスワード**フィールドは空欄にします。
4. **新しいパスワード**と**新しいパスワードの確認**フィールドにパスワードを入力し、**Enter**キーを押します。

Windowsアカウントの自動ログイン

ユーザーアカウントで自動ログインが有効にされています。このため、アカウントは不正アクセスから保護されません。1つ以上のユーザーアカウントで自動ログインが有効な場合は、この最適化警告が表示されます。この最適化の問題を解決するには、**自動ログインを無効にする**をクリックします。

架空アカウントの自動ログイン

デバイスの**架空アカウント**では自動ログインが有効です。デバイスが通常状態にある場合、ユーザーの実際のアカウントへのアクセスに問題が発生したり、コンピューターの「紛失」状態に関する誤報を送信したりする可能性があるため、自動ログインを使用しないことをお勧めします。この最適化の問題を解決するには、**自動ログインを無効にする**をクリックします。

ESET HOMEアカウントにログインします

アンチセフトを有効/無効にし、ESET HOMEでデバイスの位置情報や情報にアクセスするにはESET HOMEアカウントにログインします。

ESET HOMEアカウントにログインするには、次のいくつかの方法があります。

- **ESET HOME電子メールアドレスとパスワードを使用する**– ESET HOMEアカウントの作成に使用した**電子メールアドレス**と**パスワード**を入力し、**ログイン**をクリックします。

• **Googleアカウント/AppleIDを使用** – **Google**で続行または**Apple**で続行をクリックして、適切なアカウントにログインします。ログインが成功するとESET HOME確認Webページが表示されます。続行するにはESET製品ウィンドウに戻ります。Googleアカウント/AppleIDログインの詳細については、ESET HOMEオンラインヘルプの手順を参照してください。

• **QRコードのスキャン** - **QRコードのスキャン**をクリックしてQRコードを表示しますESET HOMEモバイルアプリを開き、QRコードをスキャンするか、デバイスカメラでQRコードを読み取ります。詳細については、ESET HOMEオンラインヘルプの手順を参照してください。

⚠ログイン失敗 – 一般的なエラー

ESET HOMEアカウントをお持ちではない場合は、**アカウントの作成**をクリックして登録するか、ESET HOMEオンラインヘルプの手順を参照してください。
パスワードを忘れた場合は、**パスワードを忘れた場合**をクリックし、画面の手順に従うか、ESET HOMEオンラインヘルプの手順を参照してください。

アンチセフトはMicrosoft Windows Home Serverをサポートしていません。

デバイス名を設定

デバイス名フィールドは、すべてのESET HOMEサービスで識別子として表示されるコンピューター(デバイス)の名前を表します。既定では、コンピューターのコンピューター名が使用されます。デバイス名を入力するか、既定の名前を使用して、**続行**をクリックします。

アンチセフトが有効/無効にされました

このウィンドウには、アンチセフトを有効/無効にするときに確認メッセージが表示されます。

• 有効 – デバイスはアンチセフトによって保護され、アカウントを使用してESET HOMEポータルでリモートでセキュリティを管理できます。

• 無効 – このデバイスではアンチセフトが無効です。このデバイスの<%ESET_ANTTHEFT%>に関連するすべてのデータはESET HOMEポータルから削除されます。

新しいデバイスの追加に失敗

アンチセフトのアクティベーション中にエラーが発生しました。

最も一般的なシナリオは次のとおりです。

• ESET HOMEへのログインエラー

• インターネット接続が有効になっていません(または、インターネットが一時的に機能していません)

問題を解決できない場合は、ESETテクニカルサポートに問い合わせてください。

Secure Data

Secure Dataは、コンピューターとリムーバブルドライブのデータを暗号化して、個人データを保護したり、悪用を防止したりできるESET Security Ultimateの機能です。詳細については、ESET Secure Data FAQを参照してください。

Secure Dataを有効にするには、次のオプションのいずれかを選択します。

- プログラムのメインウィンドウ > **概要**で、**Secure Data**の横にある**設定**をクリックします。
- プログラムのメインウィンドウ > **設定** > **セキュリティツール** > で、トグル**Secure Data**を有効にします。

ESET Endpoint Encryptionが既にインストールされているコンピューターにはSecure Dataをインストールできません。

Secure Dataを有効にすると、メインプログラムウィンドウで、**設定** > **セキュリティツール** > **Secure Data**をクリックし、次の暗号化オプションのいずれかを選択します。

- 暗号化仮想ドライブを作成
- リムーバブルドライブのファイルを暗号化

暗号化仮想ドライブを作成

Secure Dataを使用して、暗号化された仮想ドライブを作成することができます。ハードドライブの使用可能な空き領域があるかぎり、作成できるドライブ数に制限はありません。次の手順に従って、暗号化された仮想ドライブを作成します。

1. メインプログラムウィンドウで、**設定 > セキュリティツール > Secure Data > 仮想ドライブの作成**をクリックします。

2. **参照**をクリックして、仮想ドライブを保存する場所を選択します。

3. 仮想ドライブの名前を入力し、**保存**をクリックします。

4. **ドライブの最大容量**ドロップダウンメニューを使用して、仮想ドライブのサイズを設定し、**続行**をクリックします。

5. 仮想ドライブのパスワードを設定します。仮想ドライブのパスワードを設定しますWindowsアカウントにログインしたときに、仮想ドライブを自動的に復号化しない場合は、**このWindowsアカウントで自動的に復号化**をオフにして、続行をクリックします。**続行**をクリックします。

6. **完了**をクリックします。暗号化された仮想ドライブが作成され、使用できます。**PC**を開くと、ローカルディスクとして表示されます。

暗号化されたドライブに、コンピューターの再起動後にアクセスするには、作成した暗号化ドライブファイル(`.eed`ファイルタイプ)を参照し、ダブルクリックします。メッセージが表示されたら、暗号化ドライブを作成したときに設定したパスワードを入力します。ドライブはマウントされPCの下のローカルディスクとして表示されます。暗号化されたドライブがローカルディスクとしてマウントされた後は、コンピューターからログオフするか再起動するまで、そのWindowsコンピューターの他のユーザーもそのローカルディスクと復号された内容を使用できます。

> **仮想ドライブは削除できますか。**
> はい。暗号化された仮想ドライブを削除するには、ESET Secure Data FAQの手順に従いますを

リムーバブルドライブのファイルを暗号化

Secure Dataでは、リムーバブルドライブで暗号化されたフォルダーを作成できます。次の手順に従い、リムーバブルドライブのファイルを暗号化します。

1. リムーバブルドライブ(USBフラッシュドライブUSBハードディスク)をコンピューターに挿入または接続します。

2. メインプログラムウィンドウで**設定 > セキュリティツール > Secure Data > リムーバブルドライブの暗号化**をクリックします。

3. 暗号化する接続されたリムーバブルドライブを選択して、**続行**をクリックします。
更新をクリックすると、暗号化可能なドライブのリストを更新します。暗号化されたドライブまたはサポートされていないドライブは一覧に表示されません。
ESET Security Ultimateをインストールせずに、任意のWindowsデバイスで、選択したリムーバブルドライブ上の保護されたフォルダーを復号化する場合は、**Windowsデバイスでフォルダーを復号**を選択します。

4. 暗号化されたディレクトリのパスワードを設定します。仮想ドライブのパスワードを設定しま

す□Windowsアカウントにログインしたときに、仮想ドライブを自動的に復号化しない場合は、**このWindowsアカウントで自動的に復号化**をオフにして、続行をクリックします。**続行**をクリックします。

5. リムーバブルドライブが保護され、そのドライブで暗号化されたディレクトリを使用できるようになります。

リムーバブルドライブをSecure Dataがインストールされていないコンピューターに接続すると、暗号化されたフォルダーは表示されません。リムーバブルドライブをSecure Dataがインストールされているコンピューターに接続する場合は、パスワードを入力して、リムーバブルドライブを復号する必要があります。パスワードを入力しない場合は、暗号化されたフォルダーが表示されますが、アクセスできません。

Password Manager

Password ManagerはESET Security Ultimateに含まれています。

これはパスワードと個人データを保護して保存するパスワードマネージャーです。これには□Webフォームを自動的に正確に入力して、時間を短縮するためのフォーム入力機能もあります。

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

- Password Manager インストール
- Password Managerの使用を開始します□
- ESET HOMEでPassword Managerストアを管理

VPN

ESET VPNはESET Security Ultimateパッケージの一部です□VPNでは、データを安全に保ち、不要な追跡を回避し、匿名IPアドレスでセキュリティを強化してオンラインのプライバシーを高められます。

VPNの使用を開始するには、**VPNをダウンロードしてインストール**をクリックします。

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

- VPNはじめに□
- VPNインストール□
- VPNの操作□

Identity Protection

ESET Identity Protectionは、個人情報、信用情報、財務情報を保護するセキュリティソリューションです□Identity Protection継続的な監視を提供することにより、個人情報の違法な販売を検出します□Identity Protectionを使用すると□IDが危険にさらされた直後に、携帯電話、コンピューター、またはタブレットに通知が届きます。

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

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 Security Ultimate.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 Security Ultimate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。

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。

サブスクリプション

• サブスクリプション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サブスクリプション変更の問題の解決策を検索します。

• サブスクリプションの変更 – 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。デバイスがESET HOMEに接続している場合は、ESET HOMEアカウントからサブスクリプションを選択するか、新しいサブスクリプションを追加します。

インストールされている製品

• 新機能の紹介 – これをクリックすると、新しい機能と改善された機能に関する情報ウィンドウが開きます。

• ESET Security Ultimate について - ESET Security Ultimate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。

• **製品の変更** – クリックすると、現在のサブスクリプションでESET Security Ultimateが異なる製品ラインに変更できるかどうかが表示されます。

ヘルプページ – このリンクをクリックするとESET Security Ultimate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 Security Ultimateの概要

このウィンドウには、インストールされたESET Security Ultimate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。

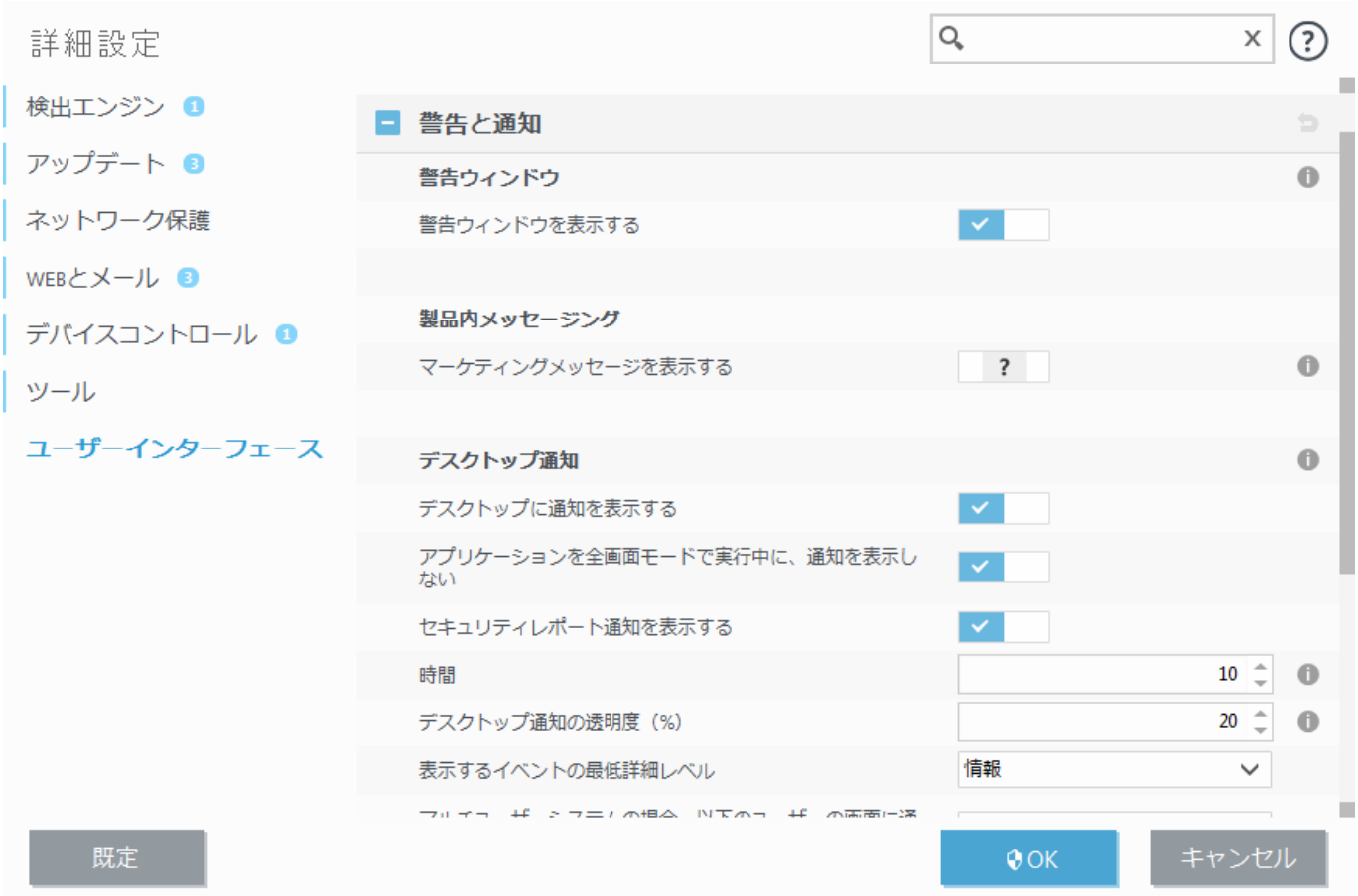
ESETニュース

このウィンドウでは定期的にESET Security UltimateのESETニュースを通知します。

製品内メッセージングは、ESETニュースとその他の連絡事項をユーザーに通知するために設定されています。マーケティングメッセージを送信するには、ユーザーの同意が必要です。このため、マーケティングメッセージは、既定では、ユーザーに送信されません(疑問符が表示されます)。このオプションを有効にするとESETマーケティングメッセージを受信することに同意しますESETマーケティング資料に関心がない場合は、**マーケティングメッセージを表示する**オプションを無効にします。

通知ウィンドウからマーケティングメッセージの受信を有効または無効にするには、次の手順に従います。

1. 詳細設定を開きます
2. **通知 > 対話アラート**をクリックします。
3. **マーケティングメッセージの表示**オプションを修正します。



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 Security Ultimate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（サブスクリプション詳細情報、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。

ESET HOMEアカウント

メインプログラムウィンドウ > **ESET HOMEアカウント**で、ESET HOMEアカウント接続ステータスを確認できます。

このデバイスはESET HOMEアカウントに接続されていません。

ESET HOMEに接続をクリックすると、デバイスをESET HOMEに接続し、サブスクリプションと保護されたデバイスを管理できます。サブスクリプションを更新、アップグレード、または拡張し、重要な詳細情報を表示できますESET HOME管理ポータルまたはモバイルアプリでは、別のサブスクリプションを追加したり、製品をデバイスにダウンロードしたり、製品セキュリティステータスを確認したり、電子メールでサブスクリプションを共有したりできます。詳細については、ESET HOMEオンラインヘルプをご覧

ください。

このデバイスはESET HOMEアカウントに接続されています。

ESET HOMEポータルまたはモバイルアプリを使用して、リモートでデバイスのセキュリティを管理できます。**App Store**または**Google Play**をクリックして、携帯電話でスキャンできるQRコードを表示し、App StoreまたはGoogle PlayからESET HOMEモバイルアプリをダウンロードします。

ESET HOMEアカウント—ESET HOMEアカウント名。

デバイス名— ESET HOMEアカウントに表示されるこのデバイスの名前。

ESET HOMEを開く – 管理ポータルESET HOMEを開きます。

ESET HOMEアカウントからデバイスを切断するには、**ESET HOMEから切断する > 切断**をクリックします。アクティベーションで使用されるサブスクリプションは引き続きアクティブです。デバイスは保護されます。

ESET HOMEに接続します

デバイスをESET HOMEに接続して、すべてのアクティベーションされたESETサブスクリプションとデバイスを表示して管理します。サブスクリプションを更新、アップグレード、または拡張し、重要なサブスクリプション詳細情報を表示できます。ESET HOME管理ポータルまたはモバイルアプリでは、別のサブスクリプションを追加したり、製品をデバイスにダウンロードしたり、製品セキュリティステータスを確認したり、電子メールでサブスクリプションを共有したりできます。詳細については、ESET HOMEオンラインヘルプをご覧ください。

あなたのデバイスをESET HOMEに接続してください:

インストール中にESET HOMEに接続している場合、またはアクティベーション方法として**ESET HOMEアカウントを使用**を選択したときには、ESET HOMEアカウントの使用の手順に従ってください。

ESET HOMEアカウントに追加されたサブスクリプションで既にESET HOMEがインストールおよびアクティベーションされている場合は、ESET HOMEポータルを使用してデバイスをESET Security Ultimateに接続できます。ESET HOMEオンラインヘルプガイドの手順に従い、ESET Security Ultimateで接続を許可してください。

1. メインプログラムウィンドウで**ESET HOMEアカウント** > **ESET HOMEに接続**をクリックするか、**このデバイスをESET HOMEアカウントに接続**通知で**ESET HOMEに接続**をクリックします。

2. ESET HOMEアカウントにログインします

ESET HOMEアカウントをお持ちではない場合は、**アカウントの作成**をクリックして登録するか、ESET HOMEオンラインヘルプの手順を参照してください。
パスワードを忘れた場合は、**パスワードを忘れた場合**をクリックし、画面の手順に従うか、ESET HOMEオンラインヘルプの手順を参照してください。

3. **デバイス名**を設定し、**続行**をクリックします。

4. 接続が成功した後、詳細ウィンドウが表示されます。**完了**をクリックします。

ESET HOMEへのログイン

ESET HOMEアカウントにログインするには、次のいくつかの方法があります。

- **ESET HOME電子メールアドレスとパスワードを使用する**– ESET HOMEアカウントの作成に使用した**電子メールアドレス**と**パスワード**を入力し、**ログイン**をクリックします。

- **Googleアカウント/AppleIDを使用** – **Google**で続行または**Apple**で続行をクリックして、適切なアカウントにログインします。ログインが成功するとESET HOME確認Webページが表示されます。続行するにはESET製品ウィンドウに戻ります。GoogleアカウントまたはAppleIDログインの詳細については、ESET HOMEオンラインヘルプの手順を参照してください。

- **QRコードのスキャン** - **QRコードのスキャン**をクリックしてQRコードを表示しますESET HOMEモバイルアプリを開き、QRコードをスキャンするか、デバイスカメラでQRコードを読み取ります。詳細については、ESET HOMEオンラインヘルプの手順を参照してください。

ESET HOMEアカウントをお持ちではない場合は、**アカウントの作成**をクリックして登録するか、ESET HOMEオンラインヘルプの手順を参照してください。
パスワードを忘れた場合は、**パスワードを忘れた場合**をクリックし、画面の手順に従うか、ESET HOMEオンラインヘルプの手順を参照してください。

ログイン失敗 – 一般的なエラー

ログイン失敗 – 一般的なエラー

入力した電子メールアドレスと一致するアカウントが見つかりませんでした

入力した電子メールアドレスがどのESET HOMEアカウントにも一致しません。**戻る**をクリックして、正しい電子メールアドレスとパスワードを入力してください。

ログインするにはESET HOMEアカウントを作成する必要があります。ESET HOMEアカウントをお持ちではない場合は、**戻る** > **アカウントの作成**をクリックして登録するか、新しいESET HOMEアカウントの作成を参照してください。

ユーザー名とパスワードが一致しません。

入力したパスワードが入力した電子メールアドレスと一致しません。**戻る**をクリックし、正しいパスワードを入力して、入力した電子メールアドレスが正しいことを確認します。それでもログインできない場合は、**戻る** > **パスワードを忘れた場合**をクリックして、パスワードをリセットし、画面の手順に従うか、ESET HOMEパスワードを忘れた場合を参照してください。

選択したログインオプションがアカウントと一致しません

ご使用のアカウントはソーシャルメディアアカウントに連携されています。ESET HOMEにログインするには、**Googleで続行**または**Apple**で続行をクリックして、適切なアカウントにログインします。ログインが成功すると、ESET HOME確認Webページが表示されます。ESET HOMEポータルでESET HOMEアカウントからソーシャルメディアアカウントを切断できます。

パスワードが正しくありません

ESET Security Ultimateが既にESET HOMEに接続され、ログインに必要な変更を行い(Anti-Theftの無効化など)、入力したパスワードがアカウントと一致しない場合は、このエラーが発生することがあります。**戻る**をクリックして、正しいパスワードを入力します。それでもログインできない場合は、**戻る > パスワードを忘れた場合**をクリックして、パスワードをリセットし、画面の手順に従うか、ESET HOMEパスワードを忘れた場合を参照してください。

ESET HOMEでのデバイスの追加

ESET HOMEアカウントに追加されたライセンスサブスクリプションで既にESET HOMEがインストールおよびアクティベーションされている場合は、ESET HOMEポータルを使用してデバイスをESET Security Ultimateに接続できます。

1. デバイスに接続要求を送信します。

2. ESET Security UltimateではESET HOMEアカウント名で**このデバイスをESET HOMEアカウントに接続**ダイアログウィンドウが表示されます。**許可**をクリックすると、デバイスが上記のESET HOMEアカウントに接続されます。

操作がない場合、接続要求は約30分後に自動的にキャンセルされます。

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 Security Ultimate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。

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
- プライバシー設定

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、オブジェクトを検出から除外できます。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。

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。

検出除外除外されたファイル拡張子HIPS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(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)。

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。

パスを選択するか、手動で入力する

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。

除外対象のフォーマット

- 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

除外のシステム変数

%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。

パスの中間のワイルドカードはサポートされません

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。

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。(ルールが上から下へ実行されるファイアウォールルールの場合)。
- 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。

除外対象のフォーマット

• 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

除外のシステム変数

%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

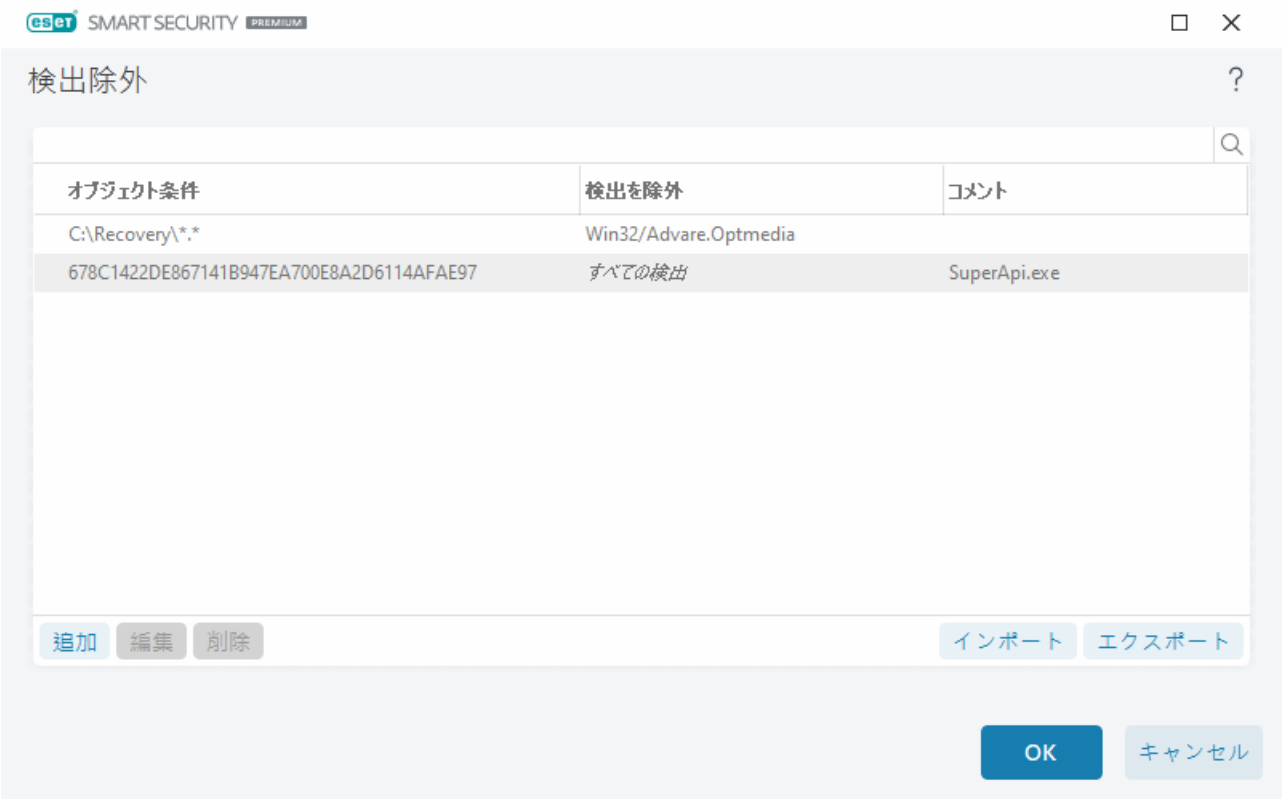
次の変数は、パス除外形式で使用できます。
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
ユーザー固有のシステム変数(*%TEMP%*または*%USERPROFILE%*など)、あるいは環境変数(*%PATH%*など)はサポートされていません。

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、オブジェクトを検出から除外できます。

検出除外の仕組み

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。

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

検出エンジンから(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

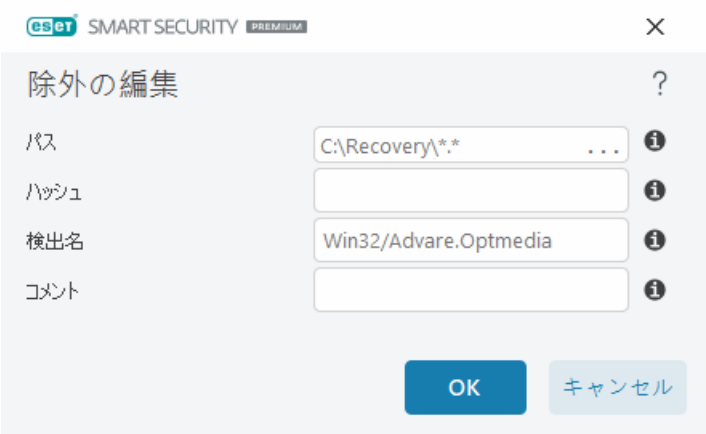
- **パス** – 指定されたパス(またはすべて)の検出除外を制限します。
- **検出名** – 除外されるファイルの横に検出の名前がある場合、ファイルは特定の検出に対してのみ除外され、完全には除外されません。このファイルが後で他のマルウェアに感染した場合は検出されます。
- **ハッシュ** – ファイルタイプ、場所、名前、拡張子に関係なく、指定されたハッシュSHA-1に基づいて、ファイルを除外します。

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 Security Ultimate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。

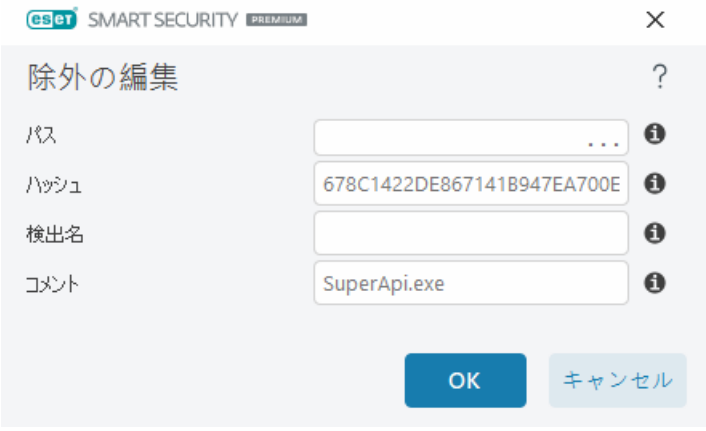
パス除外形式を参照してください。



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。



検出名による除外
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 Security Ultimate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 Security Ultimate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
- ペアレンタルコントロール
- ブラウザーのプライバシーおよびセキュリティ
- バンキングとブラウジング保護
- 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。

ESET LiveGuardは、特に、新しい脅威を軽減するために設計された保護の層を追加する機能です。有効にすると、マルウェアであることがまだ確認されてなかったり、マルウェアが隠されている可能性がある不審なサンプルが自動的にESETクラウドに送信されます。

使用可能なオプションは次のとおりです。

ESET LiveGrid®に参加する（推奨）ESET LiveGrid®フィードバックシステムESET LiveGuard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。レピュテーションシステム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、コンピューターの情報を収集しますESET LiveGuard機能は、サンドボックスで動作を分析することで、新しい未知の脅威を検出します。

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ESET LiveGuardプロアクティブ保護では、分析結果を受信するまで、新しいファイルの実行がブロックされます。

ESET LiveGrid®に参加する(推奨)を有効にする

ESET LiveGrid®レピュテーションシステムは、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。

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、コンピューターの情報を収集します。この情報には次の内容が含まれることがあります。

- 脅威が発生したファイルのサンプルまたはコピー
- ファイルへのパス
- ファイル名
- 日付と時刻
- コンピューターで脅威が発生したプロセス
- コンピューターのオペレーティングシステムに関する情報

既定ではESET Security Ultimate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。

関連するデータの送信に関する詳細は、プライバシーポリシーをお読みください。

ESET LiveGrid®を有効にしないという選択をすることもできます。

ソフトウェアの機能は失われませんが、場合によってはESET LiveGrid®を有効にするとESET Security Ultimateでの新しい脅威への反応が高速になることがあります。以前にESET LiveGrid®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。

用語集でESET LiveGrid®を参照してください。
ESET Security Ultimate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®とESET LiveGuardの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、サンドボックスで動作を分析することで、新しい未知の脅威を検出しますESET LiveGuardが有効な場合にのみESET LiveGrid®を有効にできます。

• **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

• **匿名で統計情報を送付する** – 脅威名、脅威の日時、検出方法、関連付けられたメタデータ、製品バージョンと設定（システム情報を含む）などの新しく検出された脅威に関する情報を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（既定の最大サイズは64MB）使用可能なオプションは次のとおりです。

• **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 Security Ultimate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、不明な動作のサンプルなどです（既定の最大サンプルサイズは64MBです）。

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

• **アーカイブ** - .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cabなどのアーカイブファイルタイプが含まれます。

• **スクリプト** - .bat, .cmd, .hta, .js, .vbs, .ps1などのスクリプトファイルタイプが含まれます。

• **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。

• **ESETのサーバーから実行ファイル、アーカイブ、スクリプト、他のサンプル、および可能性がある迷惑メールを削除** - ESET LiveGuardによって分析に送信されたサンプルを削除するタイミングを定義します。

• **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。

• **ESETのサーバーから文書を削除** - ESET LiveGuardによって分析に送信された文書を削除するタイミングを定義します。

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 > **検出エンジン > クラウドベース保護 > サンプルの送信**を開いて、**除外**の横の**編集**をクリックします。除外.download.domain.com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

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。

ESET LiveGuard

ESET LiveGuardは、特に、新しい脅威を軽減するために設計された、クラウドベース保護の層を追加する機能です。

有効にすると、マルウェアであることがまだ確認されてなかったり、マルウェアが隠されている可能性がある不審なサンプルが自動的にESETクラウドに送信されます。送信されたサンプルはサンドボックスで実行されESETの高度なマルウェア検出エンジンによって評価されます。マルウェアサンプルまたは不審な迷惑メールはESET LiveGrid®に送信されます。電子メール添付ファイルは個別に処理されESET LiveGuardに送信されます。ESET Cloudでは、送信されたファイルの範囲とファイル保持期間を定義できます。アクティブなコンテンツ(マクロJavaScript)を含む文書とPDFファイルは既定では送信されません。

ESET LiveGuardは次の場所で有効または無効にできます。

- プログラムのメインウィンドウ > **設定** > **コンピューター保護**
- 詳細設定 > **検出エンジン** > **クラウドベース保護**

ESET LiveGuardの詳細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** > **ESET LiveGuard**を開きます。

検出後のアクション – 分析されたサンプルが脅威と評価された場合に実行するアクションを設定します。

プロアクティブ保護 - ESET LiveGuardによって分析されるファイルの実行を許可またはブロックします。不審なファイルの場合、分析が完了するまで、プロアクティブ保護によって実行がブロックされます。プロアクティブ保護は次のソースからファイルを検出します。

- サポートされているWebブラウザーを使用してダウンロードされたファイル
- メールクライアントからダウンロードされたファイル
- サポートされているアーカイブユーティリティのいずれかを使用して、暗号化されていないアーカイブまたは暗号化されたアーカイブから展開されたファイル
- リムーバブルデバイスで実行されたファイルと開いたファイル

以下の表のサポートされているアプリケーションを参照してください。

Webブラウザー	メールクライアント	アーカイブユーティリティ	リムーバブルデバイス
Internet Explorer	Microsoft Outlook	WinRAR	USBフラッシュドライブ
Microsoft Edge	Mozilla Thunderbird	WinZIP	USBハードドライブ
Chrome	Microsoft Mail	Microsoft Explorerのビルトイン解凍ツール	CD/DVD
Firefox		7zip	フロッピーディスク
Opera			内蔵カードリーダー
Brave 参照			

> **注意**
> ESET Security Ultimateでは`explorer.exe`がアーカイブユーティリティと認識されるためWindows Explorerを使用して、除外された場所から保護された場所にコピーされたファイルは、プロアクティブ保護によってブロックされます。

> プロアクティブ保護が**分析結果を受信するまで実行をブロック**に設定され、分析中のファイルをブロック解除する場合は、ファイルを右クリックし、**ESET LiveGuardによって分析されたファイルのブロック解除**をクリックします。

分析結果の最大待機時間(分) – この時間の後、分析が完了したかどうかに関係なく、分析されたファイルがブロック解除されます。

ESET LiveGuardは通知を使用して分析ステータスを通知します。以下の使用可能な通知を参照してください。

通知タイトル	説明
分析のためファイルがブロックされました	ファイルはESET LiveGuardによってブロックされていますESET LiveGuardはファイルを分析し、安全であることを保証します。次のオプションのいずれかを待機するか、選択できます。 • **ファイルのブロックを解除** – ファイルをブロック解除しますが、分析が続行します。結果に関する通知が表示されます。ファイルの整合性が確認できない場合は、この方法は推奨されません。 • **設定の変更** – [コンピューターの保護]設定ウィンドウが開き、ESET LiveGuardとプロアクティブ保護を無効にできます。
ファイルがブロック解除されました	ファイルは今後ブロックされません。分析が続行され、結果に関する通知が表示されます。ファイルを開くことができます。
ファイルはまだ分析中です	ESET LiveGuardには、分析を完了する時間が必要です。必要に応じてファイルを開けます。
脅威が削除されました	ESETLiveGuardは分析を完了しました。ファイルには脅威が含まれていました。ファイルは駆除されました。
使用するファイル安全に使用できます	ESET LiveGuardは分析を完了しました。ファイルは安全に使用できます。

ESET LiveGuardが正しく機能しない場合は、メインプログラムウィンドウ > **概要**タブに通知が表示されます。通知の手順に従い、問題を解決します。問題を解決できない場合は、テクニカルサポートに問い合わせてください。

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 Security Ultimate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 Security Ultimate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 Security Ultimate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。

• **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。

ホスト侵入防止システム(HIPS)

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。

Host-based Intrusion Prevention System (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 Security Ultimateのプログラムのメインウィンドウ > **設定** > **コンピューターの保護**に表示されます。

HIPS

HIPSを有効にする - ESET Security Ultimate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 Security Ultimate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。

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。

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。

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。
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 Security Ultimate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。

> **終わらないHIPS通知**
> 通知の表示を停止するには、**詳細設定** > 検出エンジン > **HIPS** > **ホスト侵入防止システム**で、フィルタリングモードを**自動**に変更します。

学習モード終了

学習モードでは、ルールが自動的に作成され、保存されます。作成したすべてのルールは、HIPSルール設定で確認できます。このモードは、HIPSの初期設定に最適ですが、短時間だけオンにしておく必要があります。事前定義されたパラメーターに従い、ESETSecurityUltimateによってルールが保存されるため、ユーザーによる操作は必要ありません。セキュリティリスクを回避するために、オペレーティングシステム内で実行されている必要なプロセスのすべてのルールが作成された後、**対話**モードまたは**ポリシーベースモード**に切り替えます。

設定を変更しない場合は、この決定を延期することができます。

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[**拒否**]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

HIPSシステムにある、ユーザーが定義したか自動追加されたルールのリストです。ルール作成およびHIPS操作の詳細については、HIPSルール設定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スライダーバーを無効にします。

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、小さい通知ウィンドウが右下に表示されます。

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。(ルールが上から下へ実行されるファイアウォールルールの場合)。

- 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ルールの編集

まず、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、小さい通知ウィンドウが右下に表示されます。

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**指定したエントリ**を選択し、**[追加]**をクリックして、手動で入力します。あるいは、**レジストリエディタを開く**を選択してレジストリからキーを選択します。または、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アプリケーションを追加します。

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。

主要な操作の説明

ファイルの操作

- **ファイルの削除** – アプリケーションはターゲットファイルを削除する許可を求めています。
- **ファイルへの書き込み** – アプリケーションはターゲットファイルに書き込む許可を求めています。
- **ディスクへの直接アクセス** – アプリケーションは標準的でない方法でディスクからの読み出しまたは書き込みを行おうとしており、通常のWindowsの手順をたどりません。この結果、対応するルールの適用なしにファイルが変更される場合があります。この動作は、マルウェアが検知されるのを逃れようとしたり、バックアップソフトウェアがディスクの正確なコピーを作成しようとしたり、またはパーティションマネージャがディスクボリュームを認識しようとしたりすることで引き起こされる場合があります。
- **グローバルフックのインストール** - MSDNライブラリからのSetWindowsHookEx関数の呼び出しを指します。
- **ドライバの読み込み** – システムへのドライバのインストールと読み込み。

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。

ターゲットの入力では、一定の制限付きでワイルドカードを使用できます。レジストリのパス内では、特定のキーの代わりに *(アスタリスク)記号を使用できます。たとえば、*HKEY_USERS*\software*は、*HKEY_USER\.default\software*とは一致しますが、*HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*とは一致しません。*HKEY_LOCAL_MACHINE\system\ControlSet**は、有効なレジストリキーパスではありません。*の入ったレジストリキーのパスは、「このパスまたはこの記号の後の任意のレベルの任意のパス」を意味します。ファイルターゲットに対してワイルドカードを使用する方法はこの方法だけです。最初に、パスの特定の部分が評価された後、ワイルドカード記号(*)に続くパスが評価されます。

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**の横のスライダーバーを選択すると、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

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。

自動的なプロファイルの切り替え – アップデートプロファイルを特定のネットワーク接続プロファイルに割り当てることができます。

検出エンジンまたはモジュールアップデートのダウンロード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/キャッシュを消去します。

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。

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(HTTP通信)を許可されていることを確認してください。

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。

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が次のサイズ(KB)よりも大きい場合に確認する – アップデートファイルのサイズが指定された値を超えた場合に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

検出シグネチャーの高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。

製品のアップデート

アプリケーションの機能アップデート – 新しいバージョンのESET Security Ultimateを自動的にインストールします。

接続オプション

アップデートをダウンロードするためにプロキシサーバーを使用するには、「接続オプション」セクション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 Security Ultimate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 Security Ultimate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**の**ロールバック**をクリックした場合、検出エンジンおよびプログラムモジュールアップデートを一時停止する期間を指定する時間間隔を**時間**ドロップダウンメニューから選択する必要があります。

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推奨されません。

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。

ロールバック時間間隔

詳細設定 > **アップデート** > **アップデート**の**ロールバック**をクリックした場合、検出エンジンおよびプログラムモジュールアップデートを一時停止する期間を指定する時間間隔を**時間**ドロップダウンメニューから選択する必要があります。

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推奨されません。

製品のアップデート

製品のアップデートセクションでは、使用可能なときに、新しい機能アップデートを自動的にインストールできます。

アプリケーション機能アップデートによって、新しい機能が導入されたり、これまでのバージョンで既に存在する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。アプリケーション機能のアップデートファイルをインストールした後、コンピューターの再起動が必要な場合があります。

アプリケーション機能のアップデート –有効にすると、アプリケーション機能のアップデートが自動的に実行されます。

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 Security Ultimate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。

- 詳細設定 > **接続**で定義されているもの以外のプロキシサーバーは、ESET Security Ultimate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]**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 Security Ultimate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InternetExplorer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。

> このセクションの**ユーザー名**と**パスワード**フィールドは、プロキシサーバー固有です。 これらのフィールドには、プロキシサーバーにアクセスするためにユーザー名とパスワードが必要な場合にのみ入力してください。これらのフィールドはPRODUCTNAMEユーザー名とパスワードではありません。また、プロキシサーバー経由でインターネットにアクセスするためにパスワードが必要なことがわかっている場合にのみ入力してください。

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
- 報告設定
- 保護設定

検出応答

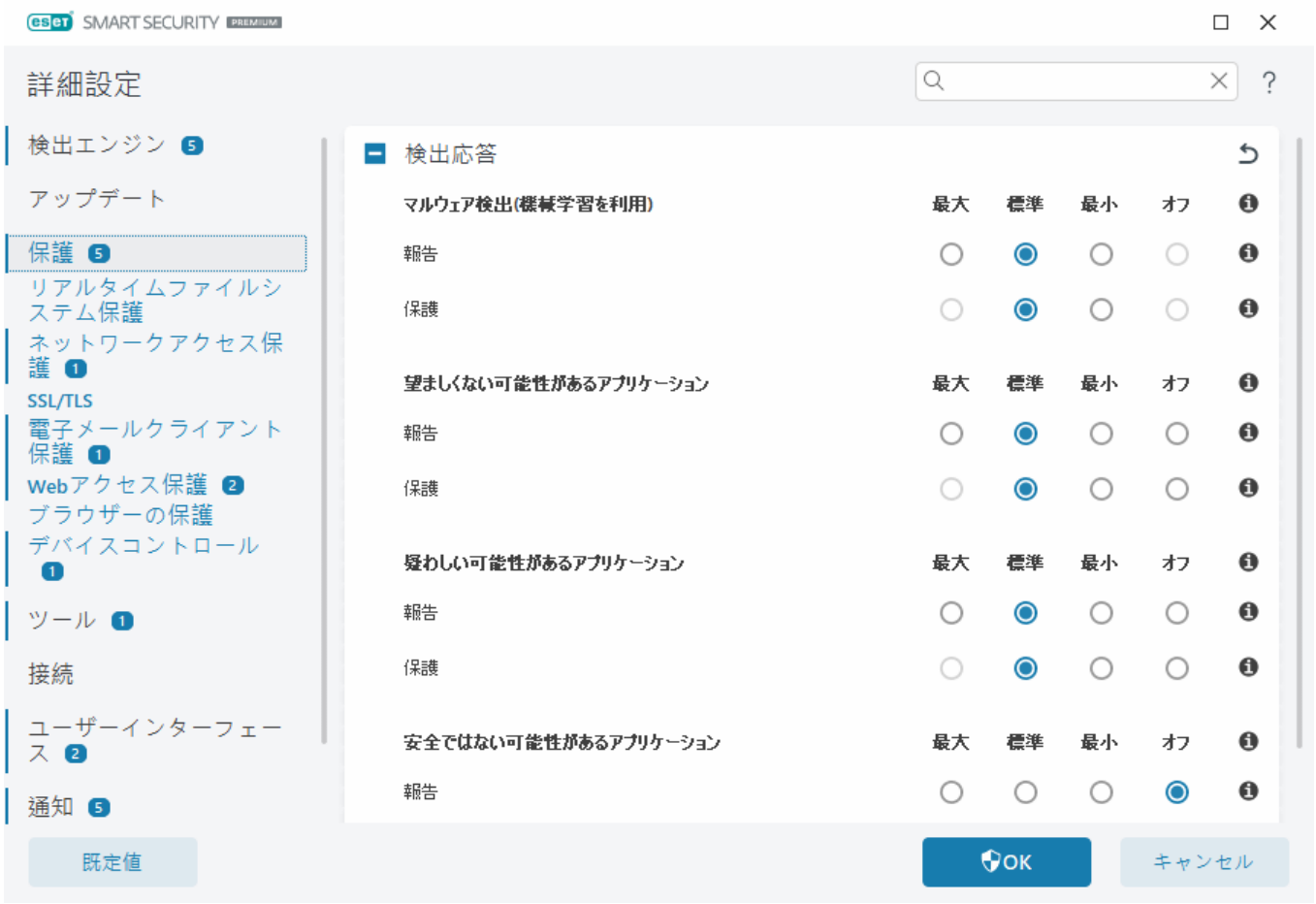
検出応答を使用すると、次のカテゴリのレポートおよび保護レベルを設定できます。

- **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 Security Ultimate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 Security Ultimate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 Security Ultimate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。
- 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 Security Ultimate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

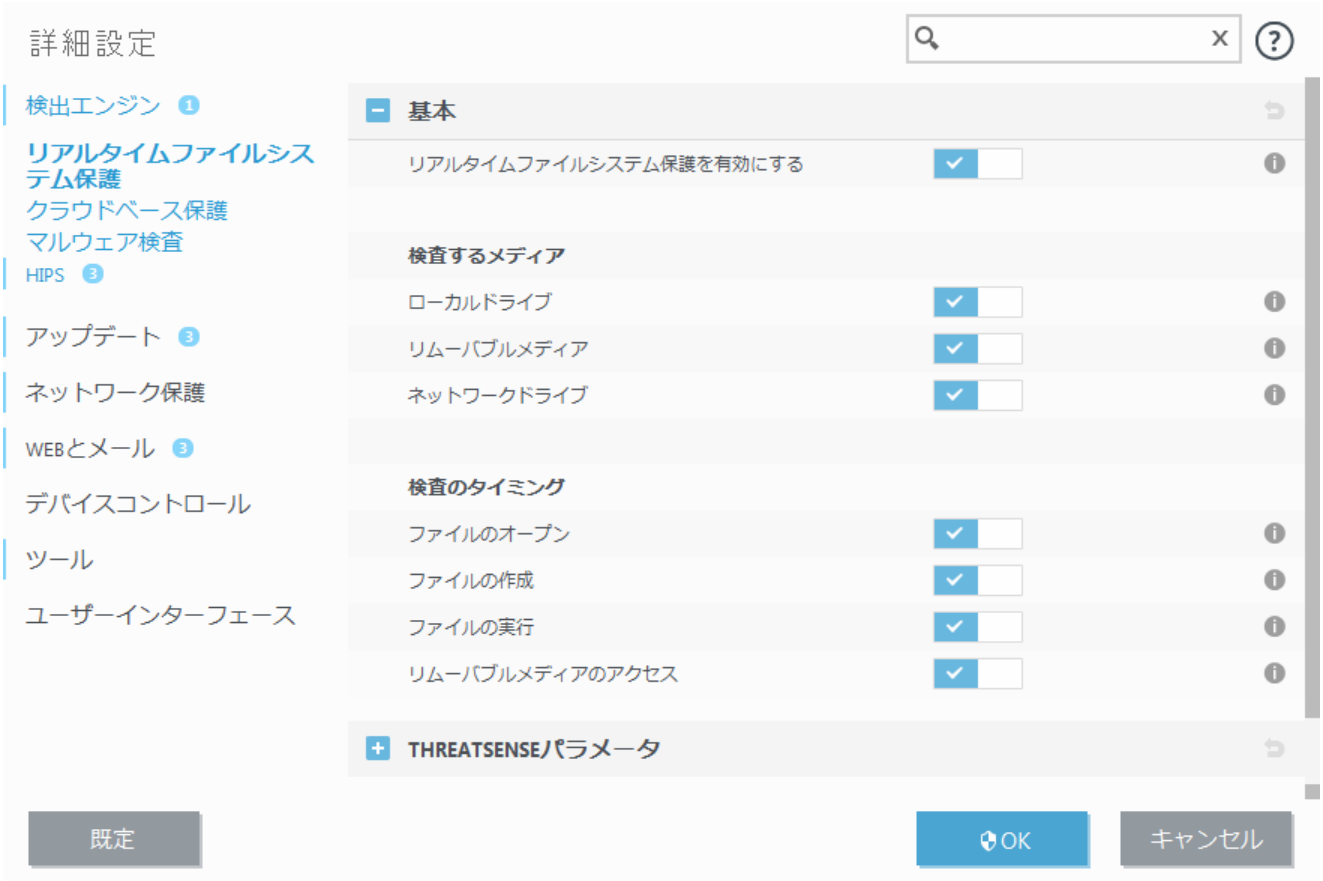
カテゴリに分類されたオブジェクトが報告されると、そのオブジェクトがブロックされ、その後に駆除、削除、または隔離に移動されます。

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。 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。

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 Security Ultimate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 Security Ultimate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 Security Ultimate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、*www.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、[**コンピュータ保護**] > [**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

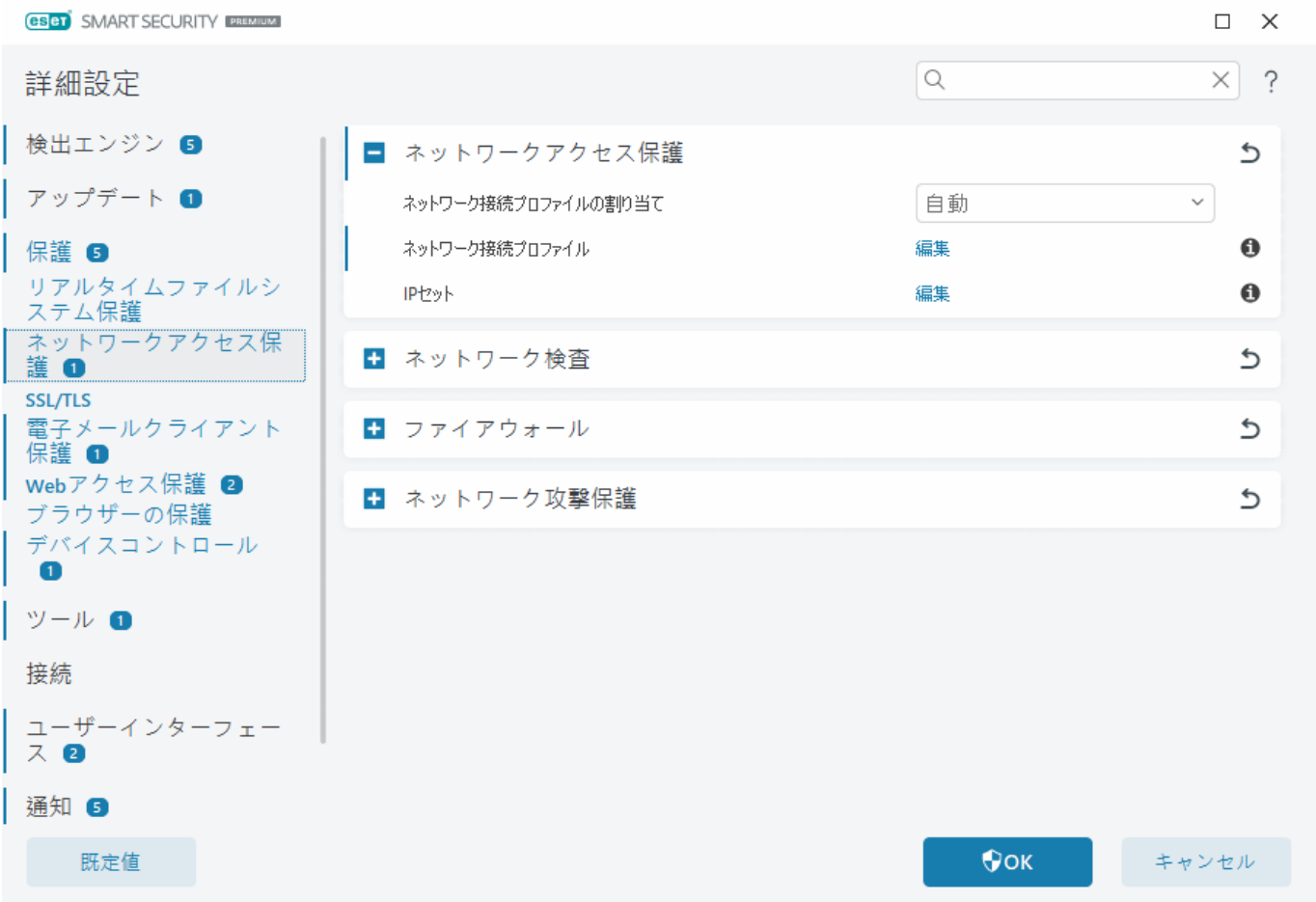
コンピュータに他のウイルス対策プログラムがインストールされていないことを確認します。2つのウィルス対策ソフトが同時にインストールされていると、互いに競合することがありますESETをインストールする前に、システムから他のウイルス対策プログラムをアンインストールすることをお勧めします。

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細かく設定できます。その設定に基づいて、特定のネットワークのコンピューターへのアクセスを許可/拒否し、コンピューターなどからネットワークデバイスへのアクセスを許可/拒否できます。既定で、ESET Security Ultimateではセキュリティを最大限に高めるために、ファイアウォールルールと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に対するファイアウォールの動作を制御できます。

IPセット - IPアドレスの論理グループを1つ作成するIPアドレスのコレクションを定義できます。これはファイアウォールルールに使用できます。

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 Security Ultimateネットワーク保護の動作を制御できます。ファイアウォールルール IDSルール、または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。ネットワーク接続にそれぞれ異なるルールが割り当てられた複数のプロファイルを作成することで、ファイアウォールの動作を容易に変更できます。

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** > **ネットワーク保護** > **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、ファイアウォールルールを適用し、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 Security Ultimate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(現在のネットワークの詳細を知りたい場合は、ネットワーク接続を参照してください)。

アダプタ

アダプタタイプ – 選択したアダプタタイプでネットワーク接続が確立されている場合にプロファイルを適用します。
アダプタ名 – ネットワークアダプタ名が一致する場合にプロファイルを適用します。
アダプタIP – ネットワークアダプタの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、認証サーバーネットワーク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、複数のファイアウォールルールまたは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 Security Ultimateには内部ルールが適用される定義済みの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*)

ネットワーク検査

ネットワーク検査は、信頼できるネットワーク(自宅または職場ネットワーク)の脆弱性(開いているポートまたは弱いルーターパスワードなど)を特定できます。また、接続されたデバイスのリスト、タイプ別に分類されたデバイス(プリンター、ルーター、モバイルデバイスなど)があり、ネットワーク(ゲームコンソールIoTまたは他のスマートホームデバイスなど)に接続されたユーザーを示します。ネット

ワーク検査は、詳細設定 > **保護** > **ネットワークアクセス保護** > **ネットワーク検査**で設定できます。

ネットワーク検査を有効にする – ネットワーク検査は、オープンポートや脆弱なルーターのパスワードなど、ホームネットワークの脆弱性を特定するのに役立ちます。また、接続されているデバイスのリストも表示され、デバイスの種類別に分類されます。

新しく検出されたネットワーク脅威を通知する – 新しいデバイスがネットワークで検出されると通知します。

ファイアウォール

ファイアウォールは、内部ルールとユーザーが定義したルールに基づいて、コンピューター上のすべての受信および送信ネットワークトラフィックをコントロールします。これにより、個々のネットワーク接続が許可または拒否されます。ファイアウォールを使用することで、リモートデバイスによる攻撃から保護したり、潜在的に危険なサービスをブロックしたりすることができます。

ファイアウォールを設定するには、詳細設定 > **保護** > **ネットワークアクセス保護** > **ファイアウォール**を開きます。

ファイアウォール

ファイアウォールを有効にする

システムのセキュリティを保証するために、この機能を有効にすることをお勧めします。ファイアウォールを有効にすると、ネットワークトラフィックは両方向で検査されます。

ルール

ルール設定では、信頼済み接続およびインターネット内で個々のアプリケーションによって生成されるトラフィックに適用されたすべてのファイアウォールルールを表示し、編集することができます。

ボットネットがコンピューターを攻撃するときにIDSルールを作成できます。ルールは、編集をクリックして、**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 > IDSルール**から修正できます。

Windowsファイアウォールのルールも評価

自動フィルタリングモードではESETルールで明示的にブロックされていないかぎりWindowsファイアウォールのルールで許可された受信トラフィックも許可します。

フィルタリングモード

ファイアウォールの動作は、フィルタリングモードによって異なります。フィルタリングモードは、必要なユーザー操作のレベルにも影響します。

ESET Security Ultimate ファイアウォールでは次のフィルタリングが利用できます。

フィルタリングモード	説明
ルール付き自動モード	既定のモードです。このモードは、ルールを定義する必要なく、ファイアウォールを容易かつ簡便に使用したいユーザーに適しています。カスタムのユーザー定義ルールを作成できますが、**自動モード**では必須ではありません。ルール付き自動モードでは、付与されたシステムのすべての送信トラフィックが許可され、ほとんどの応答(IDSと詳細オプション/許可されたサービスで指定された信頼ゾーンからの一部のトラフィックを除く)がブロックされます。
対話モード	ファイアウォールのカスタム設定を作成できます。通信が検出された際、その通信に適用されるルールがなければ、不明な接続を報告するダイアログウィンドウが表示されます。このダイアログウィンドウでは、通信を許可するか拒否するかを選択できます。さらに、許可するか拒否するかの決定を、ファイアウォールの新規ルールとして保存することもできます。ユーザーが新しいルールを作成するように選択すると、それ以降、その種類の全ての接続がルールに従って許可または拒否されます。
ポリシーベースモード	接続を許可する特定のルールによって定義されていない全ての接続がブロックされます。経験豊富なユーザーは、このモードを使用することで、必要かつ安全な接続のみを許可するルールを定義することができます。その他の不明な接続は、ファイアウォールによってブロックされます。
学習モード	ルールを自動的に作成して保存します。このモードはファイアウォールの初期設定で最適ですが、長時間オンにしないでください。事前定義されたパラメーターに従い、ESET Security Ultimateによってルールが保存されるため、ユーザーによる操作は必要ありません。学習モードではセキュリティに対するリスクを回避するために、必要な通信の全てのルールが完成するまでの間のみ使用してください。

学習モードの終了時刻 – 学習モードが自動的に終了する日時を設定します。いつでも手動で学習モードをオフにすることもできます。

学習モードの期限切れの後に設定されるモード – 学習モードの期間が終了した後に、ファイアウォールが戻るフィルタリングモードを定義します。フィルタリングモードの詳細については、上記の表をご覧ください。終了後に**ユーザーに確認**オプションでファイアウォールフィルタリングモードに変更するには、管理者権限が必要です。

学習モード設定 - **編集**をクリックして、学習モードで作成されたルールを保存するためのパラメータを設定します。

アプリケーションの変更の検出

ファイアウォールルールが存在する、変更されたアプリケーションが接続を確立しようとすると、アプリケーションの変更検出機能によって通知が表示されます。

学習モード

学習モードでは、システムで確立した各通信のルールを自動的に作成または保存します。事前定義されたパラメーターに従い、ESET Security Ultimateによってルールが保存されるため、ユーザーによる操作は必要ありません。

このモードはシステムをリスクにさらす可能性があるため、ファイアウォールの初期設定時にのみ推奨されます。

詳細設定 > **保護** > **ネットワークアクセス保護** > **ファイアウォール** > **ファイアウォール** > **フィルタリングモード**のドロップダウン メニューから**学習**を選択して、学習モードオプションをアクティベーションします。**学習モードの設定**の横にある**編集**をクリックして、次のオプションを設定します。

学習モードでは、ファイアウォールでの通信のフィルタリングが行われません。全ての通信の送受信が許可されます。このモードでは、コンピュータはファイアウォールにより完全に保護されている状態ではなくなります。

信頼ゾーンからの受信トラフィック – 信頼ゾーン内の受信接続の例には、コンピューターで実行されているローカルアプリケーションとの通信を確立しようとしている、信頼ゾーン内のリモートデバイスがあります。

信頼ゾーンへの送信トラフィック – ローカルネットワーク内または信頼ゾーンのネットワーク内の別のデバイスとの接続を確立しようとしている、ローカルアプリケーション。

受信インターネットトラフィック – コンピューターで実行されているアプリケーションと通信しようとしているリモートデバイス。

送信インターネットトラフィック – 別のデバイスとの接続を確立しようとするローカルアプリケーション。

各セクションでは、新しく作成したルールに追加するパラメータを定義できます。

ローカルポートの追加 – ネットワーク通信のローカルポート番号が含まれます。送信通信の場合、一般的にはランダムな番号が生成されます。そのため、このオプションは受信通信のみに有効にすることをお勧めします。

アプリケーションの追加 – ローカルアプリケーションの名前が含まれます。このオプションは、将来のアプリケーションレベルのルール(アプリケーション全体の通信を定義するルール)に最適です。たとえばWebブラウザまたはメールクライアントのみに通信を有効にすることができます。

リモートポートの追加 – ネットワーク通信のリモートポート番号が含まれます。たとえば、標準的なポート番号(HTTP - 80POP3 - 110など)に関連付けられた特定のサービスを許可または拒否できます。

リモートIPアドレスの追加/信頼済みゾーンを追加 – ローカルシステムとそのリモートアドレス/ゾーン間の全てのネットワーク接続を定義する新しいルールに、リモートIPアドレスまたはゾーンをパラメーターとして使用できます。このオプションは、特定のデバイスまたはデバイスネットワークのグループに対するアクションを定義する場合に最適です。

アプリケーションに対する異なるルールの最大数 – アプリケーションがさまざまなポートを介してさまざまなIPアドレスと通信する場合などに、学習モードのファイアウォールはこのアプリケーションに対して適切な数のルールを作成します。このオプションにより、1つのアプリケーションに対して作成できるルールの数を制限できます。

ファイアウォールルール

ファイアウォールルールは、すべてのネットワーク接続を効果的にテストするために使用される条件およびそれらの条件に割り当てられたすべてのアクションのセットを表します。ファイアウォールルールを使用すると、各種ネットワーク接続が確立されるときに実行されるアクションを定義できます。

ルールは上から下へと評価され、最初の列に優先度が表示されます。評価中の各ネットワーク接続に対して、最初に一致するルールのアクションが使用されます。

接続は着信と発信に分けることができます。着信は、ローカルシステムとの接続を確立しようとしているリモートデバイスによって開始されます。外向き通信は、その逆向きの通信です。ローカルシステムがリモートデバイスに接続します。

新しい未知の通信が検出された場合、慎重にそれを許可または拒否するかどうかを検討する必要があります。受信者側が送信を要求していない接続、安全でない接続、または不明な接続は、システムにセキュリティ上のリスクをもたらします。このような接続が確立された場合は、コンピューターに接続しようとしているリモートデバイスおよびアプリケーションに注意することをお勧めします。個人データを取得して送信しようとしたり、他の悪意のあるアプリケーションをホストワークステーションにダウンロードしようとしたりするマルウェアが多数あります。ファイアウォールを使用すると、ユーザーはこのような接続を検出し、切断することができます。

ファイアウォールルールは、詳細設定 > **保護** > **ネットワークアクセス保護** > **ファイアウォール** > **ルール** > **編集**で表示および編集できます。

ファイアウォールルールが多数ある場合は、フィルターを使用して特定のルールのみを表示できます。ファイアウォールルールをフィルター処理するには、ファイアウォールルールリストの上にある**その他のフィルター**をクリックします。次の条件に基づいてルールをフィルタリングできます。

- 元
- 方向
- アクション
- 可用性

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

右上の検索アイコン🔍をクリックしてルールを検索します。

列

優先度 – ルールは上から下へと評価され、最初の列に優先度が表示されます。

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

アプリケーション – ルールの適用先のアプリケーション。

方向 – 通信の方向(内向き/外向き/双方向)。

アクション – 通信のステータス(拒否/許可/確認)を表示します。

名前 – ルールの名前ESETアイコンは、定義済みのルールを表します。

適用回数 – ルールが適用された合計回数。

展開アイコンをクリックして、ルールの詳細を表示します。

コントロール要素

追加 - 新しいルールを作成します

編集 - 既存のルールを変更します

削除 – 既存のルールを削除します。

コピー – 選択したルールのコピーを作成します。

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

ファイアウォールルールの追加または編集

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

図解手順

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。

- ファイアウォールを使用して特定のポートを開く、閉じる(許可または拒否)
- ESET Security Ultimateでのログファイルからのファイアウォールルールの作成

ファイアウォールルールを追加または編集するには、詳細設定 > **保護** > **ネットワークアクセス保護** > **ファイアウォール** > **ルール** > **編集**を開きます。ファイアウォールルールウィンドウで、**追加**または**編集**をクリックします。

名前 – ルールの名前を入力します。

有効 – トグルをクリックしてルールをアクティベーションします。

ファイアウォールルールのアクションと条件を追加します。

アクション

アクション – このルールで定義された条件に一致する通信を**許可/ブロック**するか、通信が確立されるたびにESET Security Ultimateで**確認**するかを選択します。
ログルール – ルールが適用されると、ログファイルに記録されます。
ログ記録の重大度 – このルールのログ記録の重大度を選択します。
[ユーザーに通知]を選択すると、ルールが適用されたときに通知が表示されます。

アプリケーション

このルールを適用するアプリケーションを指定します。
アプリケーションパス - **...**をクリックし、アプリケーションに移動するか、アプリケーションのフルパスを入力します(例えばC:\Program Files\Firefox\Firefox.exe)アプリケーションの名前のみを入力しないでください。
アプリケーション署名 – アプリケーション署名(公開者の名前)に基づいてルールをアプリケーションに適用できます。**有効な署名**を持つアプリケーション、または**特定の署名者によって署名**されたアプリケーションにルールを適用する場合に、ドロップダウンメニューから選択します。**特定の署名者によって署名**されたアプリケーションを選択する場合は、**署名者の名前**フィールドで署名者を定義する必要があります。
Microsoft Storeアプリケーション – ドロップダウンメニューでMicrosoft Storeからインストールされたアプリケーションを選択します。
サービス – アプリケーションの代わりにシステムサービスを選択できます。ドロップダウンメニューを開き、サービスを選択します。
子プロセスに適用 – 一部のアプリケーションでは、アプリケーションウィンドウが1つしか表示されないのに、複数のプロセスが実行される場合があります。トグルをクリックして、指定したアプリケーションのすべてのプロセスに対してルールを有効にします。

方向

このルールの通信**方向**を選択します。
- **双方向** – 内向きおよび外向きの通信
- **内向き** – 内向きの通信のみ
- **外向き** – 外向きの通信のみ

IPプロトコル

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

ローカルホスト

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

ローカルポート

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

リモートホスト

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

リモートポート

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

プロファイル

ファイアウォールルールは、特定のネットワーク接続プロファイルに適用できます。
すべて – ルールは、使用されているプロファイルに関係なく、すべてのネットワーク接続に適用されます。
選択 – 選択したプロファイルに基づいて、特定のネットワーク接続にルールが適用されます。選択したいプロファイルの横にあるチェックボックスをオンにします。

この例では、新しいルールを作成してFirefox Webブラウザーアプリケーションがインターネット/ローカルネットワークWebサイトにアクセスできるようします。
1.**アクション**セクションで、**アクション > 許可**を選択します。
2.**アプリケーション**セクションで、Webブラウザーの**アプリケーションパス**を指定します(例えばC:\Program Files\Firefox\Firefox.exe)アプリケーションの名前のみを入力しないでください。
3.**方向**セクションで、**方向 > 外向き**を選択します。
4.**IPプロトコル**セクションで、**プロトコル**ドロップダウンメニューから**TCP & UDP**を選択します。
5.**リモートポート**セクションで、**ポート**番号*80,443*を追加し、標準閲覧を許可します。

アプリケーションの変更の検出

ファイアウォールルールが設定されているアプリケーションが変更され、接続を確立しようとすると、アプリケーションの変更検出機能によって通知が表示されます。アプリケーションの変更は、一時的または永久的に元のアプリケーションを別の実行ファイルの別のアプリケーションで置き換える(ファイアウォールルールの悪用に対する保護)メカニズムです。

この機能は、一般的にアプリケーションの変更を検出するためのものではありません。既存のファイアウォールルールの悪用を防止するものであり、特定のファイアウォールルールが存在するアプリケーションだけが監視されます。

アプリケーションの変更の検出を編集するには、詳細設定 > **保護 > ネットワークアクセス保護 > ファイアウォール > アプリケーションの変更の検出**を開きます。

アプリケーションの変更の検出を有効にする – 選択すると、アプリケーションに対する変更(更新、感染、その他の変更)が監視されます。変更されたアプリケーションが接続を確立しようとすると、ファイアウォールによって通知されます。

署名された(信頼された)アプリケーションの変更を許可 – 変更の前後でアプリケーションに同じ有効なデジタル署名がある場合は通知しません。

検出対象外とするアプリケーションのリスト – このウィンドウでは、通知を表示せずに、変更が許可されている個別のアプリケーションを追加または削除できます。

検出対象外とするアプリケーションのリスト

ESET Security Ultimateのファイアウォールは、ルールが存在するアプリケーションの変更を検出します(「アプリケーションの変更の検出」を参照)。

しかし、特定のアプリケーションではこの機能を使用せず、ファイアウォールによる検査から除外したいと思うこともあるかもしれません。

追加 – ウィンドウが開き、変更の検出から除外されるアプリケーションのリストに追加するアプリケーションを追加できます。オープンネットワーク通信で実行中のアプリケーションの一覧から選択できます。このようなアプリケーションではファイアウォールルールが存在するか、特定のアプリケーションを追加します。

編集 – ウィンドウが開き、変更の検出から除外されるアプリケーションのリストにあるアプリケーションの場所を変更できます。オープンネットワーク通信で実行中のアプリケーションの一覧から選択できます。このようなアプリケーションではファイアウォールルールが存在するか、手動で場所を変更します。

削除 – 変更の検出から除外されるアプリケーションのリストからエントリを削除します。

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。

> 図解手順
> 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 Security UltimateでIPアドレスをIDSから除外する

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。

> 図解手順
> 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 Security UltimateでIPアドレスをIDSから除外する

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支配を削除する場合は、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)。

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 Security Ultimate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、 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検出を選択します。
3.**...**をクリックして、この通知を適用するアプリケーションパスを選択します。
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 Security Ultimate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。

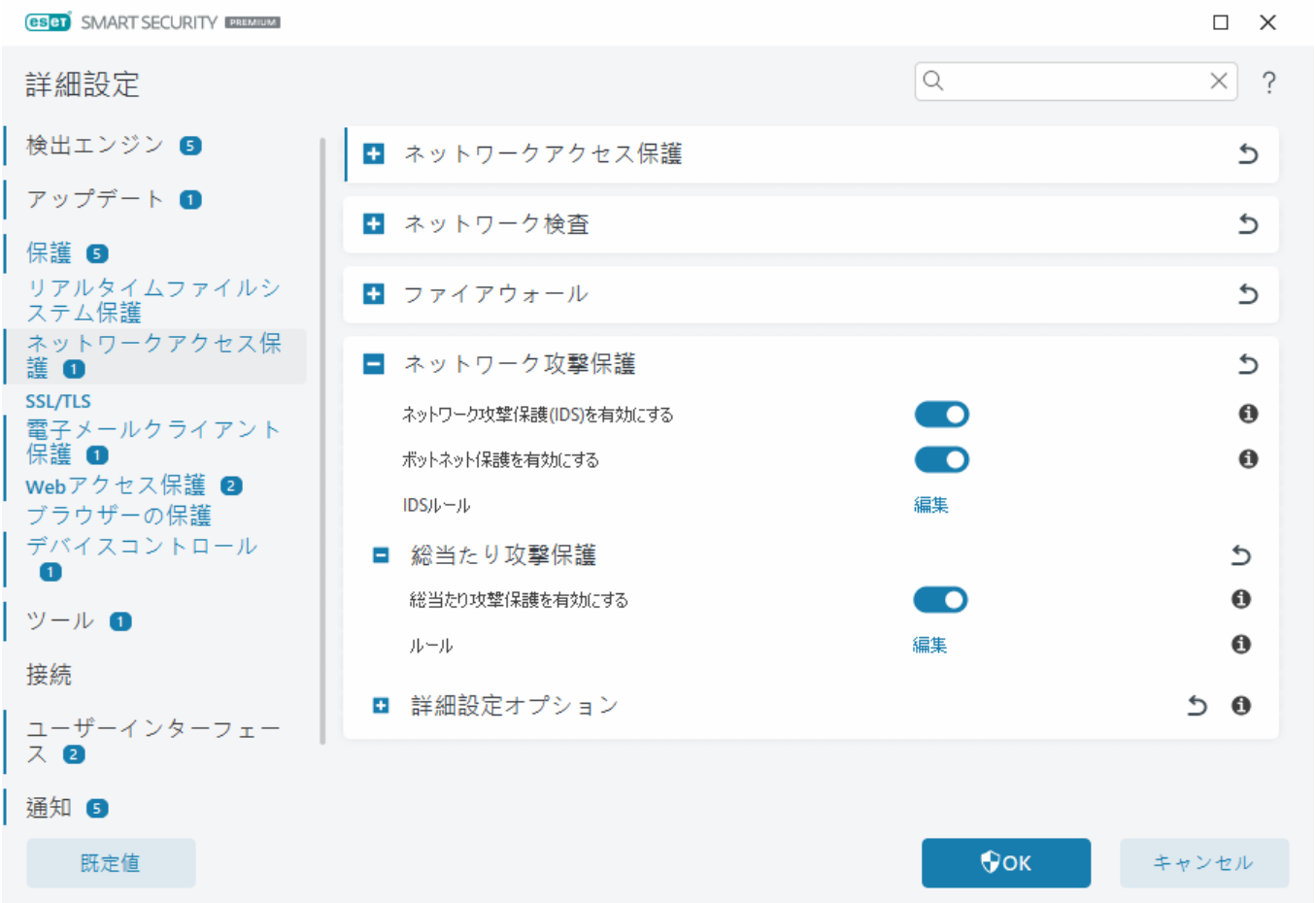
繰り返し通知を表示しない場合は、特定のタイプの**検出**の脅威と見なしません。
1.**追加**をクリックして、新しいIDSルールを追加します。
2.**検出**ドロップダウンメニューから特定の検出を選択します。例：**セキュリティ拡張なしSMBセッション**、または**伝送制御プロトコルポートスキャン攻撃**。
3.受信通信の場合は、ドロップダウンメニューで**受信**を選択します。
4.**通知**ドロップダウンメニューを**いいえ**に設定します。
5.**ログ**ドロップダウンメニューを**はい**に設定します。
6.**アプリケーション**を空白のままにします。
7.通信から特定のIP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 Security Ultimate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、ルールの章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 – 新しいルールを作成します。

編集 – 既存のルールを変更します。

削除 – ルールのリストから既存のルールを削除します。

 **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 – カスタムルールを設定し、特定のプロファイルに適用できます。

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。

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

侵入検出は、デバイスネットワーク通信で悪意のあるアクティビティを監視します。

- **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。
- **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)。
- **ARPポイズニング攻撃を検出** – 中間者攻撃によるARPポイズニング攻撃の検出、またはネットワークスイッチにおける盗聴の検出。ARP(アドレス解決プロトコル)は、Ethernetアドレスを決定するためにネットワークアプリケーションまたはデバイスによって使用されます。
- **TCP/UDPポートスキャニング攻撃を検出** – ポートスキャニングソフトウェア、すなわち、アクティブなポートを見つけてサービスの脆弱性を悪用することを目的として、広い範囲のポートアドレスにクライアント要求を送信し、ホストの開いているポートを調べるように設計されたソフトウェアによる攻撃を検出します。この攻撃の詳細については、「用語集」を参照してください。
- **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

ネットワーク経由で転送されるデータをフィルタ処理するパケット分析の一種。

- **SMBプロトコルでの管理用共有への受信接続を許可** – 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ダイアレクトを拒否** - 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ーで古いバージョンのWindowsを搭載したコンピューター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。

• **セキュリティ拡張のないSMBセッションを拒否** - 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。

• **SMBプロトコルの信頼ゾーンの外部にあるサーバー上の実行可能ファイルを開くことを拒否** – ファイアウォールの信頼ゾーンに属していないサーバー上の共有フォルダにある実行可能ファイル(.exe.dll)を開こうとすると、接続がドロップされます。信頼できるソースから実行可能ファイルをコピーすることは合法です。信頼できるソースから実行ファイルをコピーすることは合法ですが、この検出によって不審なファイルが悪意のあるサーバーで開かれるリスクを低減します(共有された悪意のある実行ファイルへのハイパーリンクをクリックして開くファイルなど)。

• **信頼ゾーン内にあるサーバーに接続するためのSMBプロトコルでのNTLM認証を拒否** - NTLM (両方のバージョン)認証スキームを使用するプロトコルは、資格情報転送攻撃(SMBプロトコルではSMBリレー)攻撃の対象になります。信頼ゾーンの外側にあるサーバーでのNTLM認証を遮断すると、信頼ゾーンの外側にある悪意のあるサーバーによって資格情報が転送されるリスクが軽減されます。同様に、信頼ゾーン内のサーバーによるNTLM認証を遮断することも考えられます。

• **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(Confickner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

ESETSecurityUltimate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 Security Ultimate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 Security Ultimate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 Security Ultimate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 Security Ultimate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 Security Ultimate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。

> 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ホーム製品の証明書通知
> • 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 Security Ultimate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 Security Ultimate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 Security Ultimate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 Security Ultimate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ホーム製品の証明書通知
> • 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
- アドレスリスト管理
- 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 Security Ultimate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 Security Ultimate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 Security Ultimate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 Security Ultimate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 Security Ultimate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。

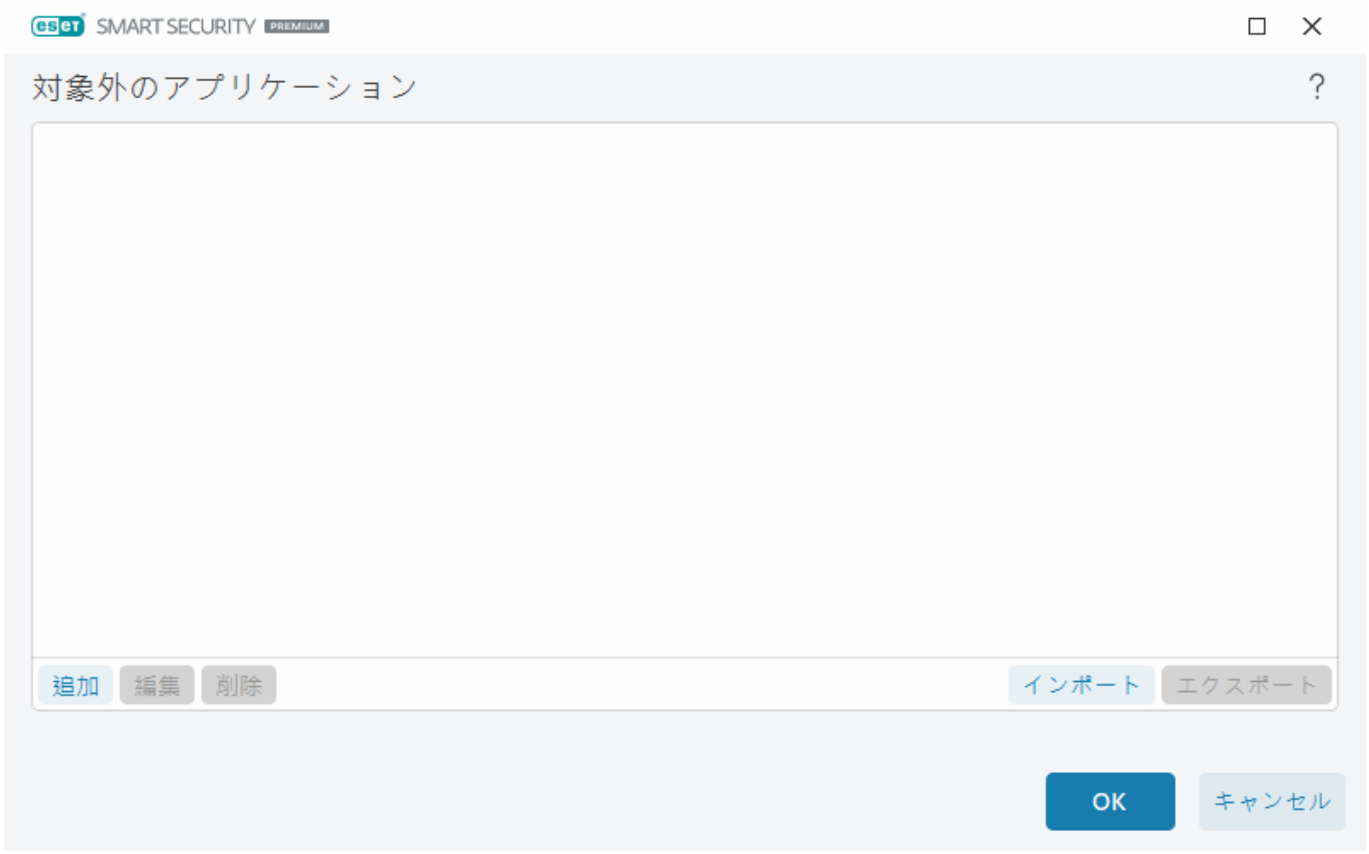
対象外のアプリケーション

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。



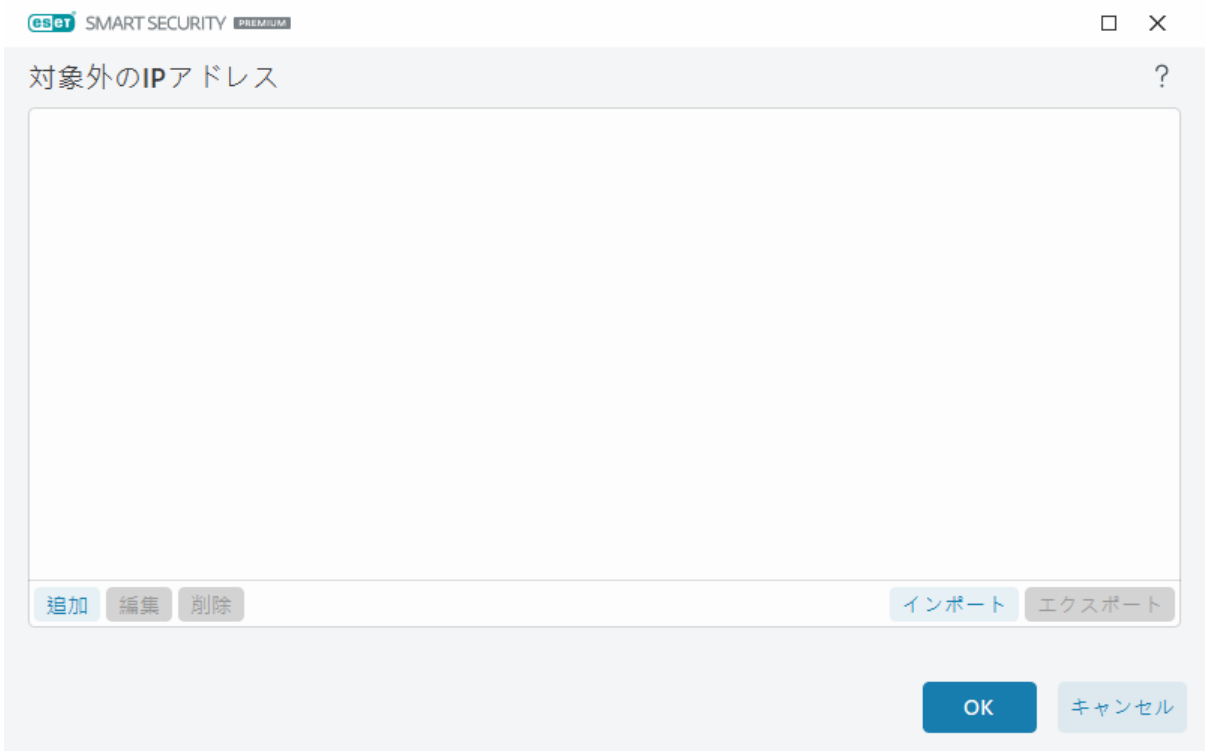
除外されたIP

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。

リモートポイントのIPアドレス/アドレス範囲/サブネットを除外するには、**追加**をクリックします。

編集をクリックして、選択したIPアドレスを変更します。

削除をクリックして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 Security Ultimate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。

迷惑メールを検査

受信者側が送信を要求していないメールつまり迷惑メールは、電子通信分野における最大の問題の1つとなっています。迷惑メールは全メール通信の実に50%も占めています。電子メールクライアント迷惑メール対策は、この問題からの保護に役立ちます。メールセキュリティの複数の原則を組み合わせることにより、電子メールクライアント迷惑メール対策のフィルタリング機能が強化されて、受信ボックスは常にクリーンな状態が保持されます。迷惑メール検出の場合、1つの重要な原理は、定義済みの信頼できるアドレス(許可)と迷惑メールアドレス(ブロック)に基づいて、未承諾の電子メールを認識します。

迷惑メール検出に使用される主な方法は、メールメッセージプロパティの検査です。受信メッセージは、基本的な迷惑メール対策基準(メッセージ定義、統計ヒューリスティック、認識アルゴリズムやその他の固有の方法)に基づいてスキャンされます。そして、結果として生成されるインデックス値により、あるメッセージが迷惑メールかどうかが判定されます。

電子メールクライアント迷惑メール対策を有効にする – 有効にすると、迷惑メールがないか受信したメッセージを検査します。

高度な迷惑メールスキャナーを使用 – 追加の迷惑メール対策データが定期的にダウンロードされ、迷惑メール対策機能が向上し、結果が向上します。

迷惑メールスコアのログ記録 - ESET Security Ultimateの迷惑メール対策用エンジンでは、全ての検査済みメッセージに迷惑メールスコアが割り当てられます。このメッセージは、迷惑メール対策保護ログに記録されます(プログラムのメインウィンドウ > **ツール** > **ログファイル** > **電子メールクライアント迷惑メール対策**)

- **なし** – 迷惑メール検査のスコアは記録されません。
- **再分類して迷惑メールに設定**- SPAMとしてマークされたメッセージに迷惑メールスコアを記録する場合、これを選択します。
- **すべて**– ログに迷惑メールスコア付きで全てのメッセージが記録されます。

迷惑メールフォルダのメッセージをクリックし、**[選択したメッセージを迷惑メールではないメールに再分類]**を選択すると、メッセージが受信トレイに移動されます。受信トレイにある迷惑メールだと考えられるメッセージをクリックし、**[メッセージを迷惑メールに再分類]**を選択すると、メッセージが迷惑メールフォルダに移動されます。複数のメッセージを選択し、同時にすべてのメッセージに対して実行できます。

添付ファイル処理最適化 – 最適化が無効な場合、すべての添付ファイルがただちに検査されます。電子メールクライアントのパフォーマンスが低下する場合があります。

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 Security Ultimate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 Security Ultimateで統合を有効にできます。統合が有効な場合、ESET Security Ultimate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 Security Ultimateがインストールされると、ウイルス対策保護と電子メールクライアント迷惑メール対策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。

迷惑メール – 選択したメールを迷惑メールとしてマークします。マークすると、迷惑メールのシグネチャを格納するセントラルサーバにメールの"フィンガープリント"が送信されます。複数のユーザーからさらに別の似通った"フィンガープリント"がサーバに送信されると、そのメールは迷惑メールとして分類されます。

信頼メール – 選択したメールを信頼メールとしてマークします。

迷惑メールアドレス（ブロック：迷惑メールアドレスのリスト）– 新しい送信元アドレスをブロックとしてアドレスリストに追加します。ブラックリスト内のアドレスから受信したメッセージはすべて、自動的に迷惑メールとして分類されます。

> スプーフィングに注意してください。スプーフィングとは、メールの送信元アドレスを偽造し、メールの受信者を騙してメールを読ませ、返信させるものです。

信頼できるアドレス（許可：信頼できるアドレスのリスト）– 新しい送信元アドレスを許可としてアドレスリストに追加します。許可されたアドレスから受信したメッセージはすべて、自動的に迷惑メールとして分類されません。

ESET Security Ultimate – アイコンをダブルクリックするとESET Security Ultimate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。

迷惑メール対策の設定 - メールボックス保護の設定オプションを表示します。

アドレス帳 - アドレスリスト管理ウィンドウが開きます。このウィンドウから、除外アドレス、信頼アドレス、および迷惑メールアドレスのリストにアクセスできます。

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 Security Ultimate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 Security Ultimate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。

ESET Security Ultimateの電子メールクライアント迷惑メール対策では、メッセージの次のパラメータを設定できます。

電子メールの件名にテキストを追加する – 迷惑メールとして分類されたメールの表題にカスタムのプリフィクス文字列を追加することができます。既定の**テキスト**は"[SPAM]"です。

迷惑メールフォルダに移動する – 有効にすると、迷惑メールメッセージが既定の迷惑メールフォルダに移動され、迷惑メールではないメールとして再分類されたメッセージが受信トレイに移動されます。電子メールメッセージを右クリックし、コンテキストメニューからESET Security Ultimateを選択すると、該当するオプションを選択できます。

カスタムフォルダに移動 – 有効にすると、迷惑メールメッセージは以下に指定されたフォルダに移動されます。

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。

検出を含むメッセージがある場合、既定ではESET Security Ultimate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。

迷惑メールを既読にする – 迷惑メールが自動的に既読に設定されます。これによって、"正当"なメールに集中できます。

再分類したメールを未読にする – 最初に迷惑メールとして分類され、後で"正当"であるとマークされたメールが未読として表示されます。

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。

アドレスリスト管理

ESET Security Ultimateの電子メールクライアント迷惑メール対策機能により、アドレス帳のさまざまなパラメーターを設定できます。アドレス帳を設定するには、詳細設定 > **保護** > **電子メールクライアント保護** > **アドレスリスト管理**を開きます。

ユーザーのアドレスリストを有効にする – このオプションを有効にすると、ユーザーのアドレスリストを有効にします。

ユーザーのアドレスリスト - 電子メールアドレスのリスト。アドレスを追加、編集、または削除して、迷惑メール対策ルールを定義できます。このリストのルールは現在のユーザーに適用されます。

グローバルアドレスリストを有効にする – このデバイスのすべてのユーザーが共有するグローバルアドレスリストを有効にする場合、このオプションを有効にします。

グローバルアドレスリスト - 電子メールアドレスのリスト。アドレスを追加、編集、または削除して、

迷惑メール対策ルールを定義できます。このリストのルールはすべてユーザーに適用されます。

自動的に許可し、ユーザーのアドレスリストに追加

アドレス帳のアドレスを信頼済みとして処理する – 連絡先リストのアドレスがユーザーのアドレスリストに追加されずに、信頼済みとして処理されます。

送信メールの宛先メールアドレスを追加する – 送信メッセージの受信者アドレスを、ユーザーのアドレスリストに許可として追加します。

迷惑メールではないメールとして再分類されたメッセージからアドレスを追加する – 迷惑メールではないメッセージに再分類されたメッセージの送信元アドレスを、ユーザーのアドレスリストに許可として追加します。

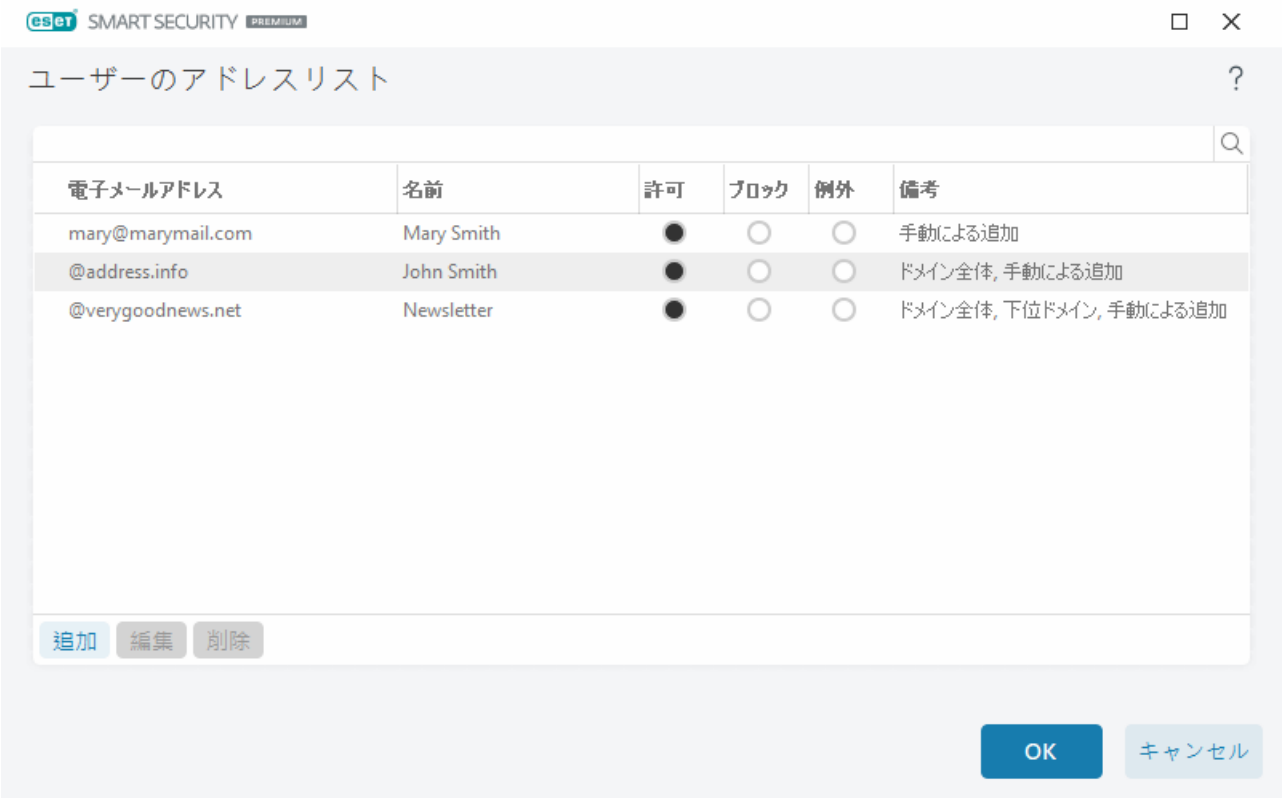
ユーザーのアドレスリストに自動的に例外として追加

自分のアカウントからアドレスを追加 – 既存の電子メールクライアントアカウントからアドレスをユーザーのアドレスリストに例外として追加します。

アドレスリスト

未承諾メールから保護するためにESET Security Ultimateでは、アドレスリストの電子メールアドレスを分類できます。

アドレスリストを編集するには、詳細設定 > **保護** > **電子メールクライアント保護** > **アドレスリスト管理**を開き、**ユーザーのアドレスリスト**または**グローバルアドレスリスト**の横の**編集**をクリックします。



列

電子メールアドレス – ルールが適用されるアドレス。ワイルドカードはサポートされていません。

名前 – カスタムルール名。

許可/ブロック/例外 – 電子メールアドレスに対して実行するアクションを決定するために使用されるラジオボタン(アクションをすばやく変更するには、優先列のラジオボタンをクリックします)。

- **許可** – 安全であると見なされ、メッセージを受信するアドレス。
- **ブロック** – 安全ではない/迷惑メールと見なされ、メッセージを受信したくないアドレス。
- **例外** – 常に迷惑メール検査が実行されるアドレス。偽装され、迷惑メールの送信で使用される可能性があるアドレス。

備考 – ルールの作成方法と、ドメイン/下位ドメイン全体に適用されるかどうかに関する情報。

アドレスの管理

- **追加** – クリックすると、新しいアドレスのルールを追加します。
- **編集** – 選択してクリックすると、既存のルールを編集します。
- **削除** – アドレスリストからルールを削除する場合は、選択してクリックします。

アドレスの追加/編集

このウィンドウでは、アドレスリスト管理のアドレスを追加または編集し、実行されるアクションを設定できます。

電子メールアドレス – ルールが適用されるアドレス。

名前 – カスタムルール名。

アクション – 連絡先の電子メールアドレスが**電子メールアドレス**フィールドで指定されたアドレスと一致する場合に実行するアクション。

- **許可** – 安全であると見なされ、メッセージを受信するアドレス。
- **ブロック** – 安全ではない/迷惑メールと見なされ、メッセージを受信したくないアドレス。
- **例外** – 常に迷惑メール検査が実行されるアドレス。偽装され、迷惑メールの送信で使用される可能性があるアドレス。

ドメイン全体 – 連絡先のドメイン全体(**電子メールアドレス**フィールドに指定したアドレスだけでなく、*address.info*ドメインのすべての電子メールアドレス)にルールを適用する場合に、このオプションを選択します。

下位ドメイン – 連絡先の下位ドメイン(*address.info*はドメインを表し、*my.address.info*はサブドメインを表す)にルールを適用する場合に、このオプションを選択します。

アドレス処理結果

新しいアドレスを追加したり、電子メールアドレスに対して実行されるアクションを変更したりするときにESET Security Ultimateで通知メッセージが表示されます。通知メッセージの内容は、実行しようとしているアクションによって異なります。

次回からメッセージを表示せずに自動的にアクションを実行するには、**今後このメッセージを表示しない**チェックボックスをオンにします。

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

駆除設定により、感染ファイルからウイルスを駆除するときのESET Security Ultimateの動作が決まります。駆除には、4つのレベルがあります。

ThreatSenseには、次の修復(駆除など)レベルがあります。

ESET Security Ultimate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。
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。

駆除レベル	説明
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。

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エンジンパラメーター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利用できます。

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。

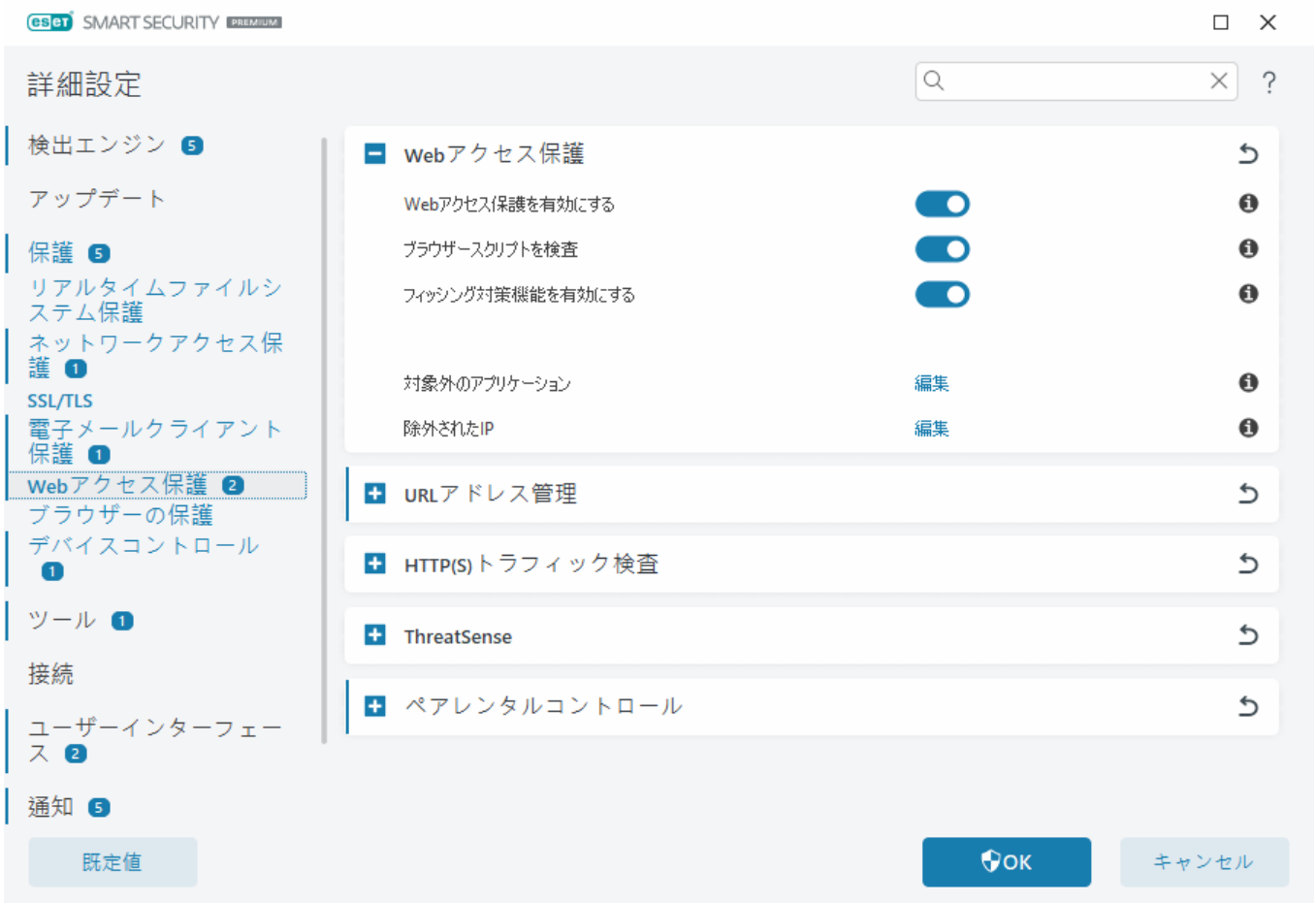
> 既定のままWebアクセス保護を有効にしておき、アプリケーションやIPアドレスを除外しないことを強くお勧めします。

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。

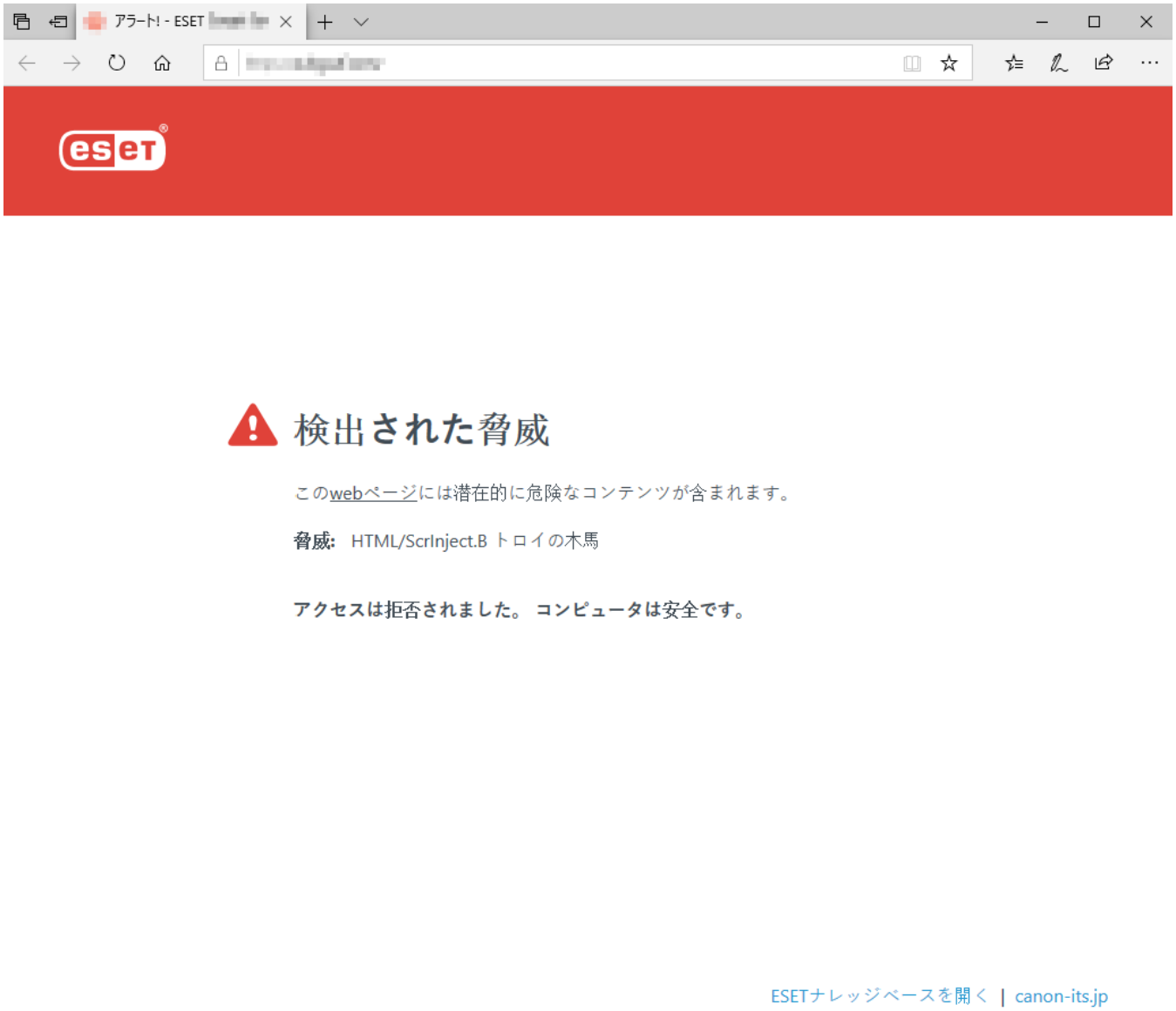
フィッシング対策機能を有効にする – 有効にすると、フィッシングWebページがブロックされます。詳細については、「フィッシング対策保護」を参照してください。

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。



図解手順

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。

- Webアクセス保護で安全なWebサイトがブロックされないようにする
- ESET Security Ultimateを使用してWebサイトをブロックする

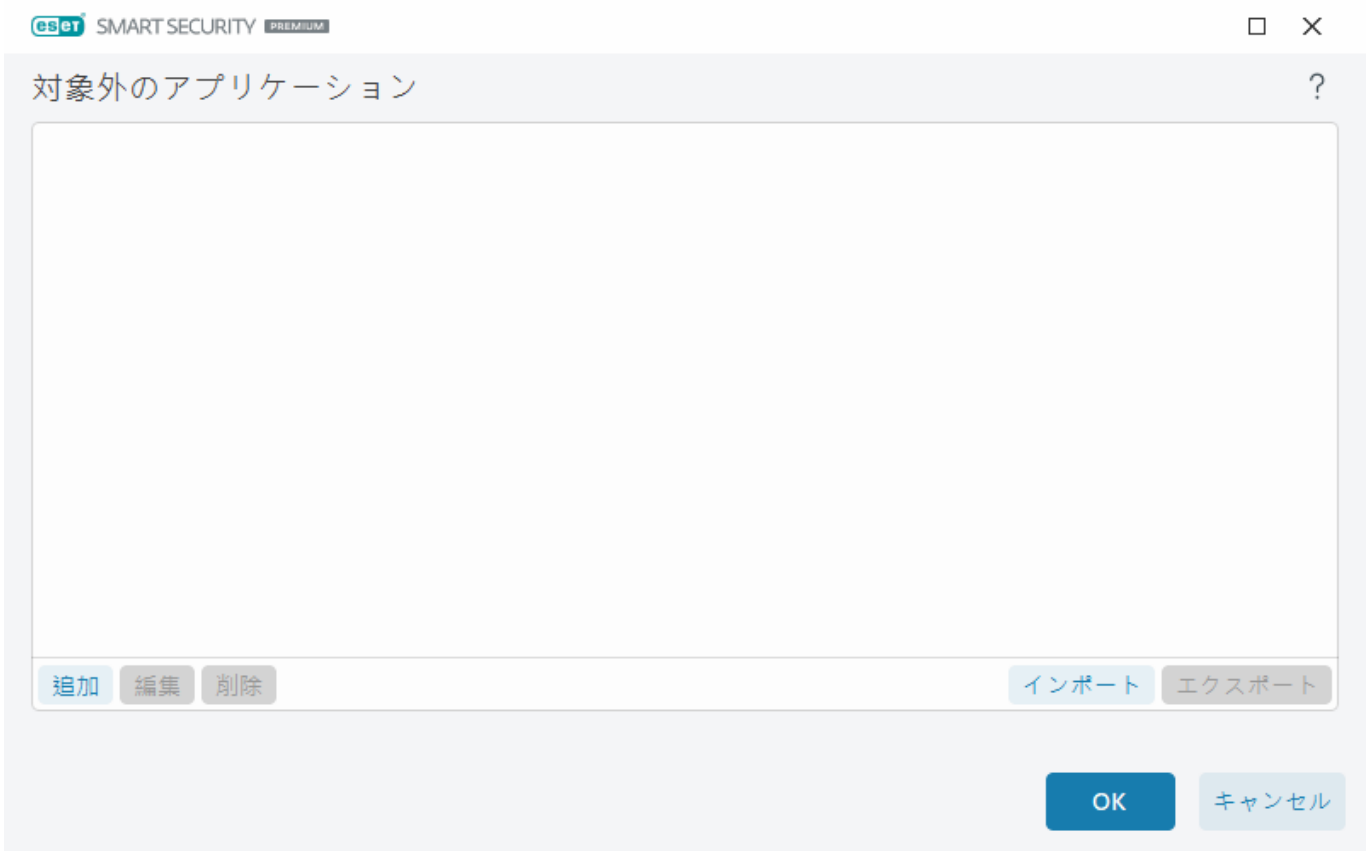
対象外のアプリケーション

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。



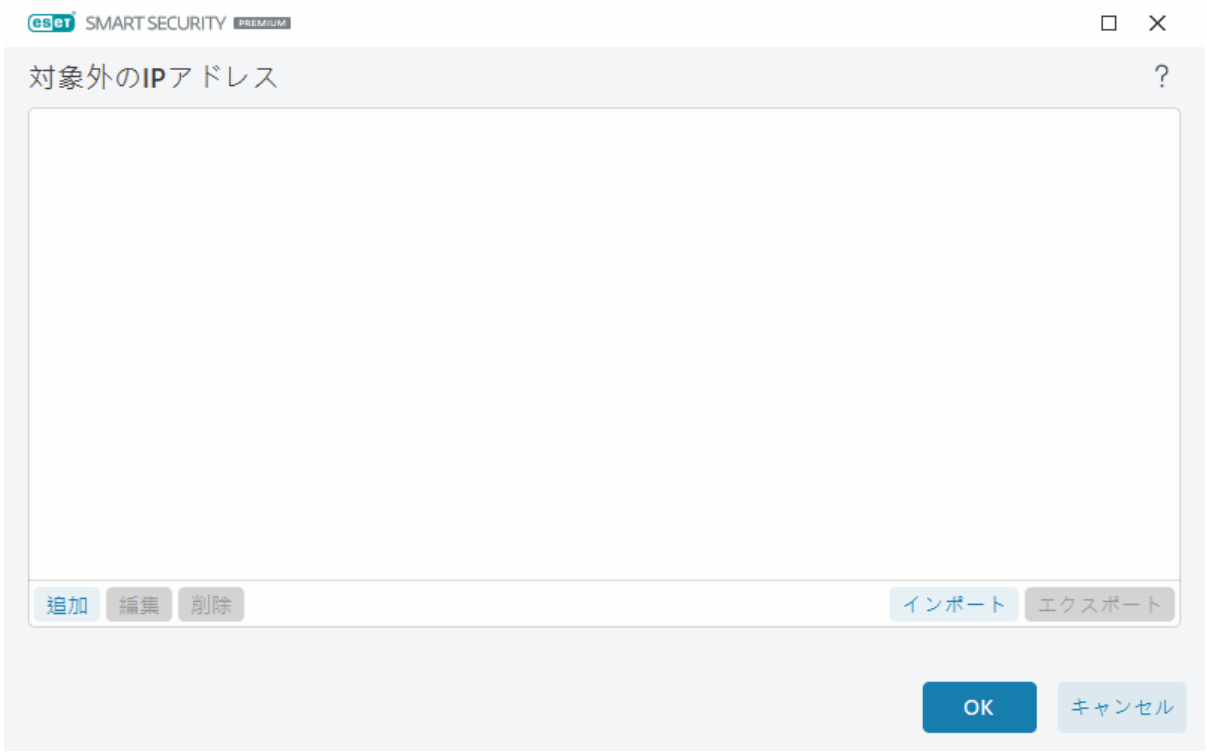
除外されたIP

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。

リモートポイントのIPアドレス/アドレス範囲/サブネットを除外するには、**追加**をクリックします。

編集をクリックして、選択したIPアドレスを変更します。

削除をクリックして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*から*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。

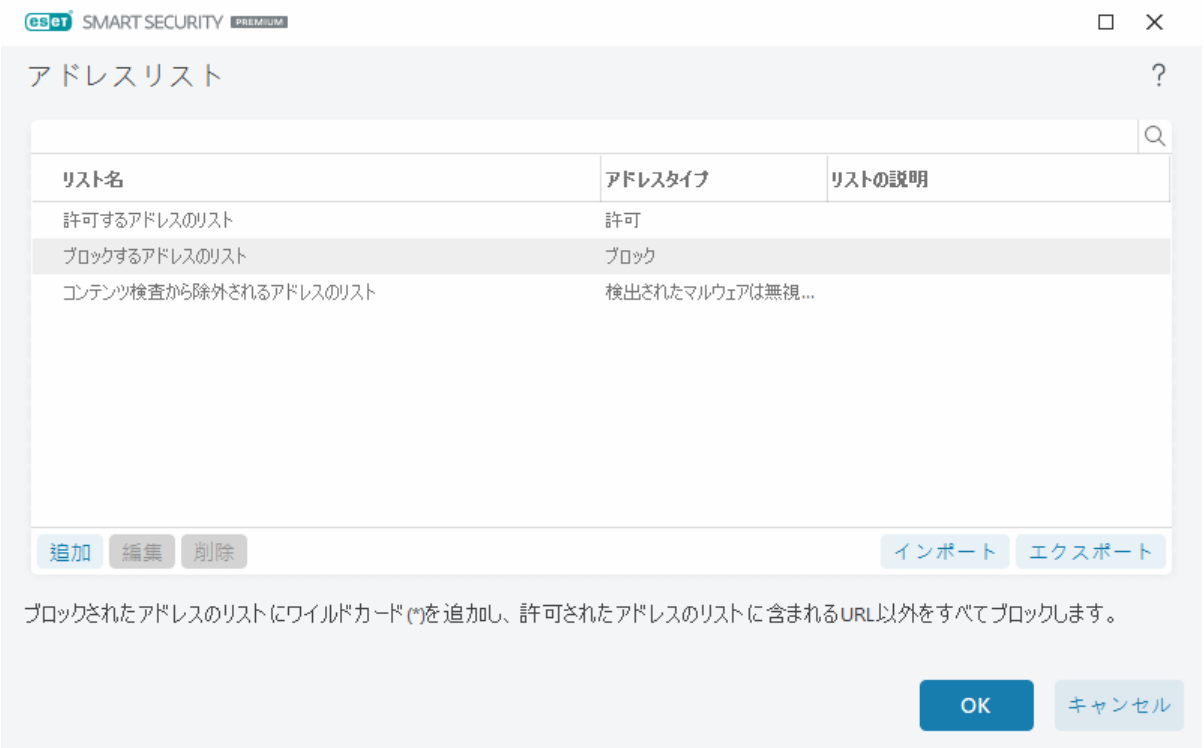
ブロックするアドレスのリストのWebサイトは、**許可するアドレスのリスト**にも重複して登録されている場合を除いて、アクセスできません。**コンテンツ検査から除外されるアドレスのリスト**のWebサイトは、アクセス時に悪意のあるコードがあるかどうかの検査が行われません。

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。

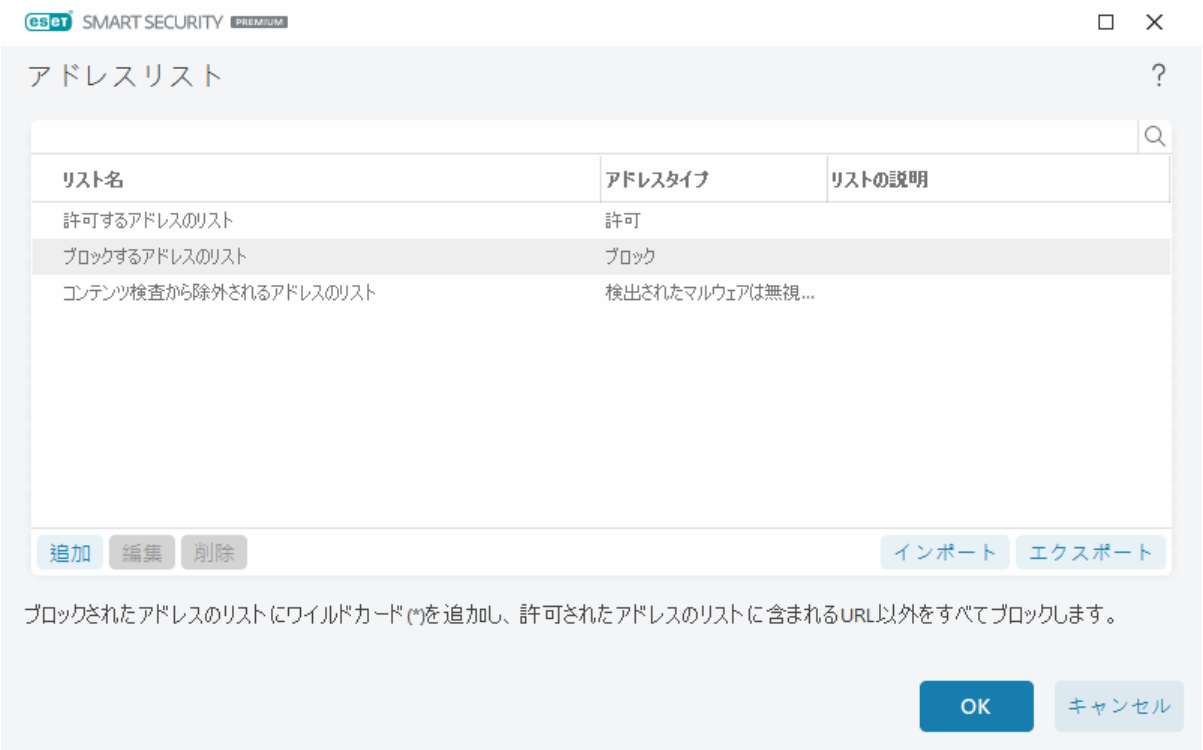
既定では、次の3つのリストを使用できます。

• **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。



> 図解手順
> 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。
> • Webアクセス保護で安全なWebサイトがブロックされないようにする
> • ESET Windowsホーム製品を使用してWebサイトをブロックする

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。

ログ記録の重大度 - Webサイトへのアクセス時に使用されている特定のリストに関する情報をログファイルに書き込むことができます。

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)。

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参照してください。

ESET Security Ultimate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。

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。これは、例えば、マスク*.domain.comが*http://anydomain.com/anypath#.domain.com*と一致しないように(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)、マスクの迂回を回避するためです。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。例えば、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。

HTTP(S)トラフィック検査

既定で、ESET Security Ultimate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 Security Ultimate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 Security Ultimate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

駆除設定により、感染ファイルからウイルスを駆除するときのESETSecurityUltimateの動作が決まります。駆除には、4つのレベルがあります。

ThreatSenseには、次の修復(駆除など)レベルがあります。

ESET Security Ultimate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。
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。

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エンジンパラメーター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利用できます。

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。

ペアレンタルコントロール

ペアレンタルコントロールを有効にするオプションにより、ペアレンタルコントロールがESET Security Ultimateに統合されます。ユーザーアカウントの横にある**編集**をクリックして、特定のユーザーがインターネット上の不適切なコンテンツ、または有害なコンテンツにアクセスするの制限するため、ペアレンタルコントロールで使用されたWindowsユーザーアカウントを関連づけることができます。

ユーザーアカウント

詳細設定 > **保護** > **Webアクセス保護** > **ペアレンタルコントロール** > **ユーザーアカウント** > **編集**で、特定のユーザーがインターネット上の不適切なコンテンツ、または有害なコンテンツにアクセスするの制限するため、ペアレンタルコントロールで使用されたWindowsユーザーアカウントを関連づけることができます。

列

Windowsアカウント – ユーザーの名前。

有効 – 有効になっている場合、特定のユーザーアカウントのペアレンタルコントロールが有効にな

ります。

ドメイン – ユーザーが属するドメイン名。

生年月日 – このアカウントが属するユーザーの年齢。

コントロール要素

追加 - ユーザーアカウントの操作ダイアログが表示されます。

編集 – このオプションでは、選択したアカウントを編集できます。

削除 – 選択したアカウントを削除します。

更新 – ユーザーアカウントを追加した場合ESET Security Ultimateはこのウィンドウを再度開くことなく、ユーザーアカウントの一覧を更新します。

ユーザーアカウント設定

ウィンドウには3つのタブがあります。

一般

有効の横にあるトグルをオンにすると、以下で選択したWindowsアカウントのペアレンタルコントロールがオンになります。

まず、コンピューターからシステムアカウントを**選択**します。ペアレンタルコントロールで設定された制限は、標準のWindowsアカウントのみに適用されます。管理者アカウントの権限は制限に優先されます。

保護者がアカウントを使用する場合は**親のアカウント**を選択します。

アクセスレベルを決定するには、また年齢に適切なwebページのアクセスルールを設定するには、このアカウントの**お子様の生年月日**を入力します。

ログ記録の重大度

ESET Security Ultimateでは、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。このログファイルはメインメニューから直接表示することができます。[**ツール**] > [**ログファイル**]をクリックし、[**ログファイル**]ドロップダウンメニューから**[Parental Control]**を選択します。

- **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** – 許可およびブロックされた例外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。
- **なし** – ログは記録されません。

例外

例外を作成することで、例外リストにない Web サイトへのユーザーアクセスを許可・拒否することができます。カテゴリを使用するのではなく、特定のウェブサイトへのアクセスをコントロールしたい場合に便利です。ひとつのアカウントで作成された例外は、コピーでき、他のアカウントでも使用できます。

これは、似たような年齢の子供たちにまったく同じルールを作成したい場合などに便利です。

追加をクリックして新規例外を作成します。ドロップダウンメニューを使用して**アクション**を指定、この例外を適用する **例外URL** を入力し、次に**OK**をクリックします。既存の例外の一覧に状態が表示された例外が追加されます。

追加 – 新しい例外を作成します。

編集 – 選択した例外の**例外URL**または**操作**を編集します。

削除 – 選択された例外をフィルタから削除します。

コピー – 作成した例外をコピーするドロップダウンメニューからユーザを選択します。

ここで定義する例外は、選択したアカウントに対して定義されている分類に優先されます。たとえば、アカウントの[**ニュース、ポータル・検索**]カテゴリはブロックされていても、例外として許可しているニュースWebページがある場合、許可されたWebページにはアクセスできます。[例外]セクションで行った変更をすべて見ることができます。

カテゴリ

分類タブで、ブロックしたい、またはそれぞれのアカウントに許可したい一般的な web サイトのカテゴリを定義します。カテゴリの横のスイッチをオンにして許可します。スイッチをオフにすると、そのアカウントではカテゴリが許可されません。

コピー – 既存の修正されたアカウントからブロックまたは許可される分類のリストをコピーできます。

カテゴリ

カテゴリの横の**有効**列のチェックボックスをオンにして許可します。チェックボックスをオフにすると、そのアカウントではカテゴリが許可されません。

ユーザーに知られていない可能性があるカテゴリー(グループ)の例を次に示します。

- **その他** – 通常は、イントラネット、127.0.0.0/8、192.168.0.0/16などのプライベート(ローカル)IPアドレスです。403または404エラーコードが表示された場合、そのWebサイトはこの分類にも一致します。

- **未解決** – この分類には、ペアレンタルコントロールデータベースエンジンへの接続時のエラーによって解決されなかったWebページが含まれます。
- **未分類** – まだペアレンタルコントロールデータベースにない未知のWebページです。
- **動的** – 他のWebサイトの他のページにリダイレクトするWebページ。

ブラウザーの保護

ブラウザーの保護は、ブラウザーのメモリを他のプロセスによる検査から保護し、キーロガーに対する保護を強化し、マルウェアによって変更されたオンライン決済関連データをクリップボードからセキュアーブラウザに貼り付けるのを防ぐ、セキュリティとプライバシーを保護する別のレイヤーです。ブラウザー保護を設定するには、詳細設定 > **保護** > **ブラウザーの保護**を開き、次の設定オプションから選択します。

- バンキングとブラウジング保護
- ブラウザー保護の許可リスト
- ブラウザーのフレーム

バンキングとブラウジング保護

バンキングとブラウジング保護は、詳細設定 > **保護** > **ブラウザーの保護** > **バンキングとブラウジング保護**で設定できます。

バンキングとブラウジング保護

バンキングとブラウジング保護を有効にする – バンキングとブラウジング保護を有効にすると、サポートされているすべてのWebブラウザーが既定でセキュアモードで起動します。

ブラウザーの保護

すべてのブラウザーを保護を有効にすると、保護モードでサポートされているWebブラウザーがすべて起動します。

拡張機能のインストールモード - ESETによって保護されたブラウザーへのインストールを許可する拡張機能を、ドロップダウンメニューから選択できます。

- **必須の拡張機能** – 特定のブラウザーベンダーによって開発された最も重要な拡張機能のみ。
- **すべての拡張機能** – 特定のブラウザーでサポートされているすべての拡張機能。

> 拡張機能インストールモードを変更しても、以前にインストールされたブラウザー拡張機能には影響しません。

セキュアーブラウザー

拡張メモリ保護 – 有効にすると、保護されたブラウザーのメモリが他のプロセスによって検査から保護されます。

キーボード保護 – 有効にすると、セキュアーブラウザーにキーボードから入力した情報は他のアプリ

ケーションから隠すことができます。これにより、キーロガーに対する保護が強化されます。

クリップボード保護 – 有効にするとESET Security Ultimateでは、マルウェアによって変更されたオンライン決済関連データがクリップボードからセキュアーブラウザに貼り付けられなくなります。これにより、悪意のあるソフトウェアによって行われる潜在的な変更に対する保護が保証されます。

ブラウザーのフレーム – 保護されたブラウザーのフレームの表示設定をパーソナライズします。

ブラウザー保護許可リスト – ブラウザー保護の許可リストに追加されたファイルを管理します。

ブラウザーのプライバシーおよびセキュリティ

ブラウザーのプライバシーおよびセキュリティを有効にする – この機能を無効にすると、ブラウザーのプライバシーおよびセキュリティ拡張機能は、すべてのWindowsアカウントでサポートされているすべてのブラウザーからアンインストールされます。

ブラウザーのプライバシーおよびセキュリティ通知の表示– 有効にするとESET Security Ultimateブラウザーのプライバシーおよびセキュリティの通知が表示されます。

ブラウザースクリプトスキャナー

ブラウザースクリプトの詳細検査を有効にする – 有効にすると、ウイルス対策スキャナーは、インターネット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。

00

デバイスコントロール

ESET Security Ultimate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(HDDUSB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 Security Ultimate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。

異なるルールが適用されるさまざまなデバイスのグループを作成できます。また、**許可**または**ブロック**アクションがあるルールが適用されるデバイスのグループは、1つだけ作成できます。これにより、コンピューターに接続したときに、デバイスコントロールによって認識されていないデバイスがブロックされます。

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

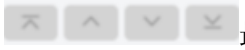
デバイスコントロールルールエディタウィンドウには既存のルールが表示されます。

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、およびデバイスの追加パラメーター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。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。

[**追加**]または[**編集**]をクリックしてルールを管理します。[**コピー**]をクリックして、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。 ルールをクリックすると表示されるXMLストリングは、クリップボードにコピーできます。システム管理者はこれを利用することにより、内などでこれらのデータをエクスポート/インポートしたり使用することができます。

CTRLキーを押しながらクリックすると、複数のルールを選択してアクション(削除やリスト内での上下移動など)をすべての選択済みルールに適用できます。**有効**チェックボックスでは、ルールを無効または有効にできます。これは、ルールを保持する場合に便利です。

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。**

ログエントリは、メインプログラムウィンドウ > **ツール** > ログファイルで確認できます。

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。

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。非表示のデバイスをすべて表示する場合は、**非表示のデバイスを表示**を選択します。

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。

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。

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

ESET Security Ultimateでは、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。このログファイルはメインメニューから直接表示することができます。[**ツール**]をクリックします> [**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[**デバイスコントロール**]を選択します。

- **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ます。
- **なし** – ログは記録されません。

ユーザー一覧

ルールを特定のユーザーまたはユーザーグループに限定する場合は、**ユーザー一覧**の横の**編集**をクリックして、ユーザーまたはユーザーグループをユーザーリストに追加します。

- **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。

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。

変更内容を保存するには、[**OK**]をクリックします。変更を保存せずに**デバイスグループ**を終了する場合は、**編集**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は、4つのアクションをすべて使用できます。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)。

Webカメラ保護

Webカメラアクセス制御では、コンピューターのWebカメラにアクセスするプロセスとアプリケーションが通知されます。アプリケーションがカメラにアクセスしようとすると、通知が表示され、アクセスを**許可**または**禁止**できます。アラートウィンドウの色は、アプリケーションのレピュテーションによって異なります。

Webカメラアクセス制御の設定オプションは、詳細設定 > **保護** > **デバイスコントロール** > **Webカメラアクセス制御**で変更できます。

ESET Security UltimateでWebカメラアクセス保護機能を有効にするには、**Webカメラアクセス保護を有効にする**の横のスライダーバーを有効にします。

Webカメラアクセス制御が有効になると、**ルール**が有効になり、ルールエディターウィンドウを開けるようになります。

変更され、有効なデジタル署名(プログラムコンポーネントのアップデートなど)があるルールがあるアプリケーションのアラートをオフにするには、**変更されたアプリケーションのWebカメラアクセスアラートを無効にする**の横のスライダーバーを有効にします。

Webカメラ保護ルールエディター

このウィンドウには既存のルールが表示され、実行したアクションに基づいてコンピューターのWebカメラにアクセスするアプリケーションとプロセスを制御できます。

使用できるアクションは次のとおりです。

- **アクセスの許可**
- **アクセス禁止**

- **確認**（アプリケーションがWebカメラにアクセスしようとするたびにユーザーに確認する）

[通知]列のチェックボックスをオフにすると、アプリケーションがWebカメラにアクセスするときに通知の受信を停止します。

> 図解手順
> ESET Security UltimateでWebカメラルールを作成および編集する方法

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

駆除設定により、感染ファイルからウイルスを駆除するときのESETSecurityUltimateの動作が決まります。駆除には、4つのレベルがあります。

ThreatSenseには、次の修復(駆除など)レベルがあります。

ESET Security Ultimate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。
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。

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エンジンパラメーター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利用できます。

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 Security Ultimate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。
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。

駆除レベル	説明
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定義します。

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 Security Ultimate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 Security Ultimate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。

- Microsoft Windows® アップデート
- ESET CMD
- ログファイル
- ゲームモード
- 診断

Microsoft Windows® アップデート

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 Security Ultimateは、詳細設定 > **ツール**で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。

ダイアログウィンドウ – システムアップデート

オペレーティングシステムのアップデートがある場合は、ESET Security Ultimateのメインプログラムウィンドウ>**概要**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 Security Ultimate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 Security Ultimate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。

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`

高度なecmdコマンドはローカルでのみ実行できます。

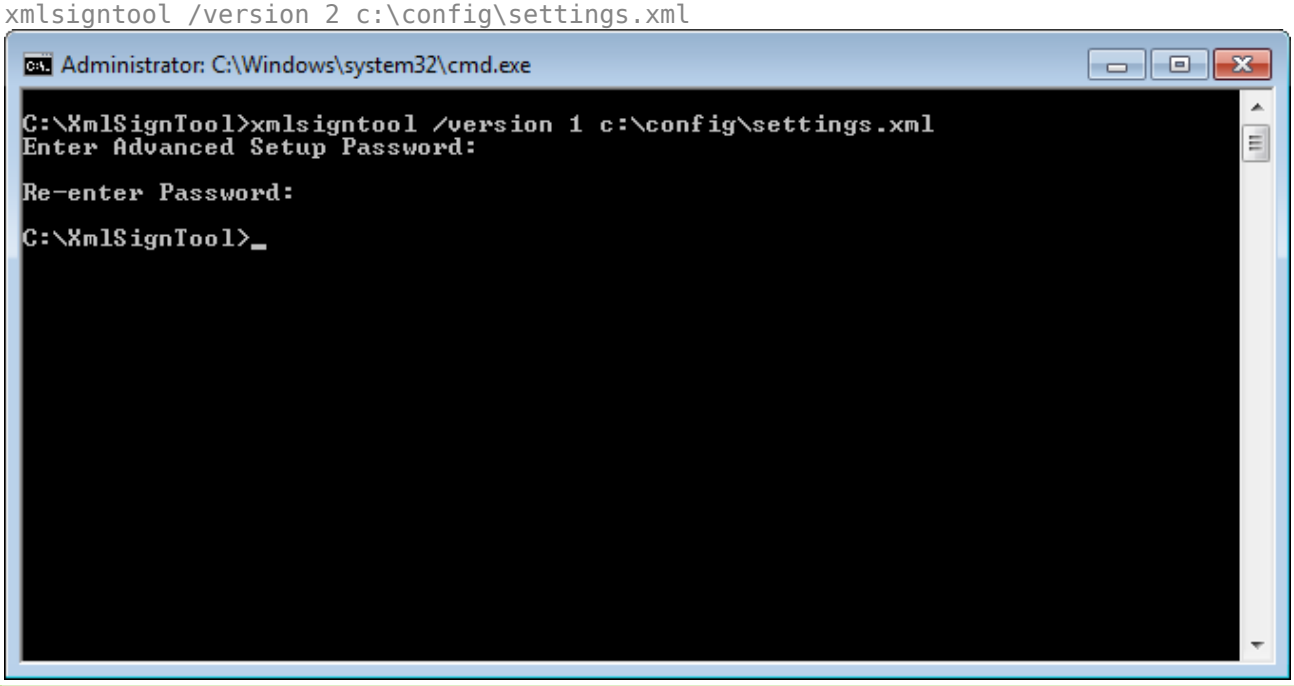
*.xml*設定ファイルの署名:

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 Security Ultimateのバージョンによって異なります。11より前のバージョンのESET Security Ultimateでは、`/version 1`を使用します。現在のバージョンのESET Security Ultimate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 Security Ultimate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 Security Ultimate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。

ログファイル

ESET Security Ultimateのログ設定は、、詳細設定 > **ツール** > **ログファイル**にあります。[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。

ログに記録する最低レベル – 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、ファイアウォール、など)。

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値を超えると、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。このプロセスによって空のログエントリがすべて削除され、ログの処理の速度が向上します。この向上は、特にログに多数のエントリが含まれている場合に顕著に見られます。

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。

- **保存先のフォルダー** – ログファイルが保存されるディレクトリ(テキスト/CSVのみ)。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**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)。
- **すべ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。

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。

ゲームモード

ゲームモードは、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。ゲームモードは、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。

メインプログラムウィンドウの**設定 > コンピューター保護**で  をクリックするか、**ゲームモード**の横の  をクリックして、ゲームモードを有効または無効にできます。ゲーム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、**ゲーム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 > ゲームモード**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ゲーム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、ゲームモードが開始され、アプリケーションが終了すると停止します。

[ゲームモードを次の後に自動的に無効にする]チェックボックスをオンにすると、ゲームモードが自動的に無効になるまでの時間を定義できます。

ファイアウォールが対話モードの場合に、ゲームモードを有効にすると、インターネットとの接続時に問題が発生することがあります。これは、インターネットに接続するアプリケーションを開始するときに問題となります。通常は、このようなアクションについて確認するよう求められますが(通信ルールまたは例外が定義されていない場合)、ゲームモードではユーザーとの対話処理が無効になります。通信を許可するには、この動作が起こる可能性がある全てのアプリケーションで通信のルールを定義するか、またはファイアウォールで別のフィルタリングモードを使用します。ゲームモードが有効な場合に、セキュリティ上の潜在的なリスクが存在するWebサイトまたはアプリケーションにアクセスすると、ユーザーとの対話処理が無効なため説明や警告が表示されることなくブロックされることに注意してください。

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 Security Ultimate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

マーケティングメッセージで詳細ログを有効にする – 製品内のマーケティングメッセージに関連するすべてのイベントを記録します。

迷惑メール対策エンジン詳細ロギングを有効にする – 迷惑メール対策検査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ESET迷惑メール対策エンジンに関連する問題を診断および修正できます。

アンチセフトエンジン詳細ロギングを有効にする – アンチセフトで発生するすべてのイベントを記録し、問題の診断と解決ができます。

ブラウザーの保護詳細ログを有効にする – バンキングとブラウジング保護で発生するすべてのイベントを記録します。

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 – ESET LiveGrid®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ESET LiveGrid®に関連する問題を診断および修正できます。

ドキュメント保護の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。

ESET LiveGuard詳細ログを有効にする – ESET LiveGuardで発生するすべてのイベントを記録し、問題の診断と解決ができます。

カーネル詳細ログを有効にする - ESETカーネル(ekrn)で発生すべてのイベントを記録します。

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またはESET License Manager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を記録します。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。

ペアレンタルコントロール詳細ロギングを有効にする – ペアレンタル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、開発者はペアレンタル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。

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べてのイベントを記録します。

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。

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。

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 Security Ultimate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 Security Ultimateとそのモジュールは自動的に更新されません。ESET Security Ultimate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 Security Ultimate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。

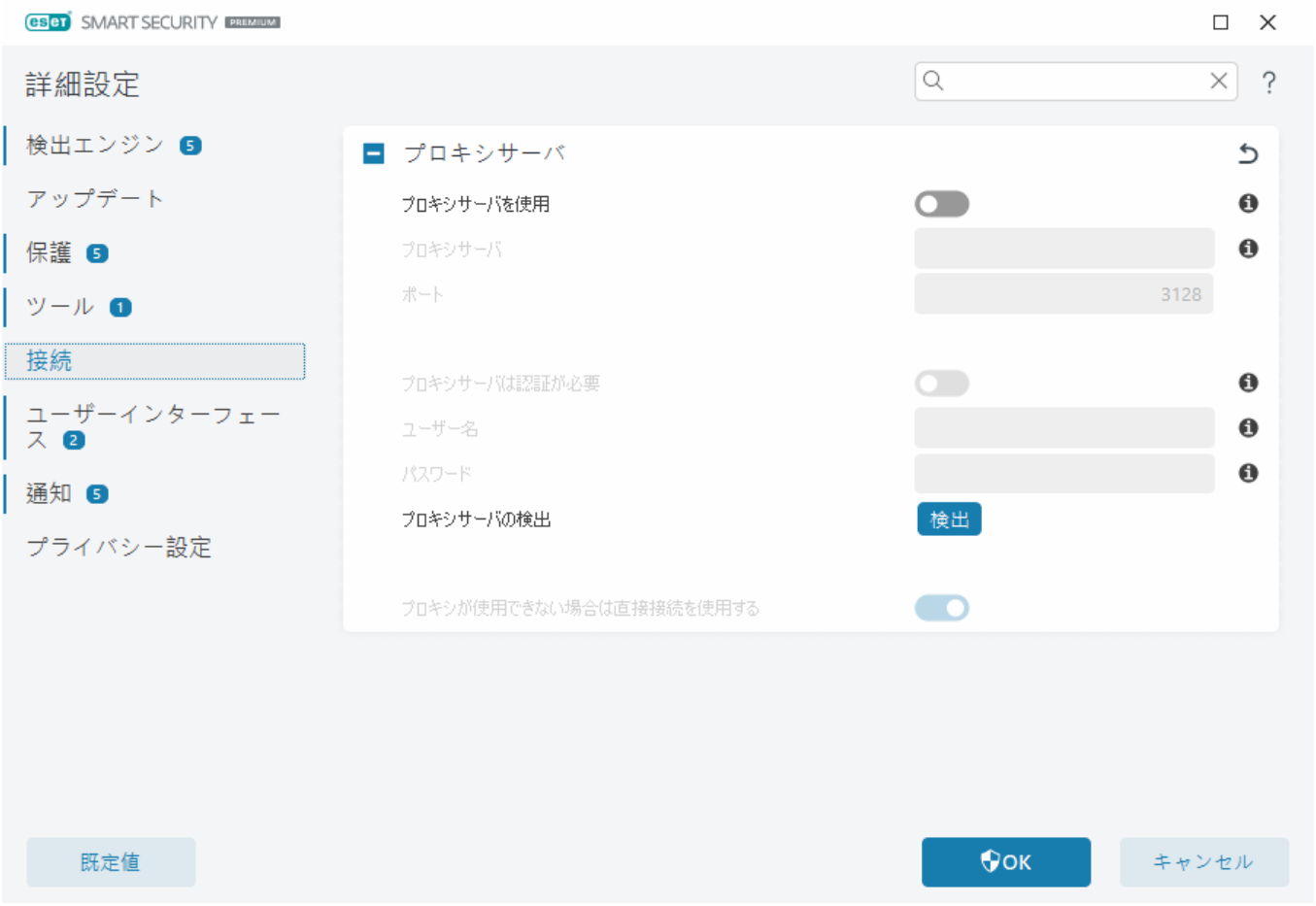
プロキシサーバーとの通信に認証が必要な場合、**プロキシサーバーは認証が必要**をオンにし、有効な**ユーザー名**と**パスワード**を該当のフィールドに入力します。**プロキシサーバーの検出**をクリックして、プロキシサーバー設定を自動的に検出して設定します。ESET Security UltimateはInternet ExplorerまたはGoogle Chromeのインターネットオプションで指定されたパラメータをコピーします。

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 Security Ultimate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 Security Ultimate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。

ユーザーインタフェース要素

詳細設定 > **ユーザーインタフェース** > **ユーザーインタフェース要素**ではESET Security Ultimate作業環境(GUI)をニーズに合わせて調整できます。

色モード – ドロップダウンメニューからESET Security Ultimate 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 Security Ultimateの配色を設

定します。

- **ダークモード** - ESET Security Ultimateには暗い配色(ダークモード)があります。
- **ライトモード** - ESET Security Ultimate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 Security Ultimate GUIの配色を選択することもできます。

起動時にスプラッシュ画面を表示する – 起動中にのESET Security Ultimateにスプラッシュ画面が表示されます。

サウンドシグナルを使用する – 検査中に脅威が発見されたり検査が終了したなどの重要なイベントが発生したとき、がサウンドを再生します。

透明の背景 - メインプログラムウィンドウで透過的なバックグラウンド効果を有効にします。透過的な背景は、最新のWindowsバージョン(RS4以降)でのみ使用できます。

コンテキストメニューに統合する - ESET Security Ultimate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。

アクセス設定

ESET Security Ultimate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 Security Ultimate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 Security Ultimate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。

保護された詳細設定にアクセスするときには、パスワードの入力ウィンドウが表示されます。パスワードがわからない場合は、下の**パスワードの復元**オプションをクリックして、サブスクリプション登録で使用される電子メールアドレスを入力しますESETは、確認コードと、パスワードのリセット方法が記載された電子メールを送信します。

- 詳細設定をロック解除する方法

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。

詳細設定のパスワード

ESET Security Ultimate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。

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。

このパスワードは詳細設定にアクセスするために必要です。

パスワードを忘れた場合は、ESETHOME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。

紛失したESET製品認証キー、サブスクリプションの有効期限、またはESET Security Ultimateのその他のサブスクリプション情報を回復するには、製品認証キーを紛失したを参照してください。

スクリーンリーダーのサポート

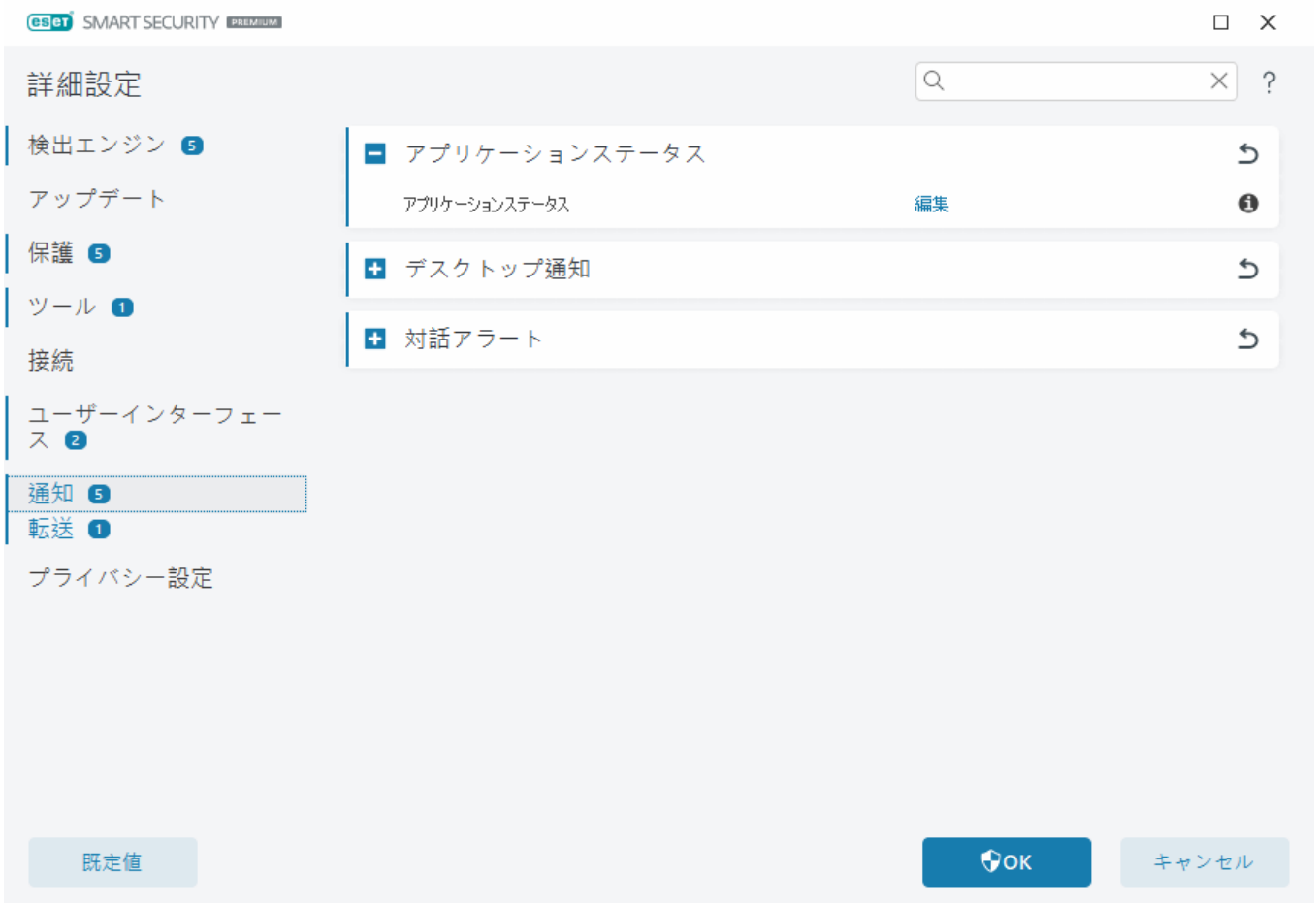
ESET Security Ultimateはスクリーンリーダーと併用できるため、視覚障がいをお持ちのESETユーザーでも製品を操作したり、設定を構成したりすることができます。次のスクリーンリーダーがサポートされています(JAWS, NVDA, Narrator)。

スクリーンリーダーソフトウェアが確実に正しくESET Security Ultimate GUIにアクセスできるようにするには、ナレッジベース記事の手順に従ってください。

通知

ESET Security Ultimate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 > **概要**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。



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 > **概要**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。

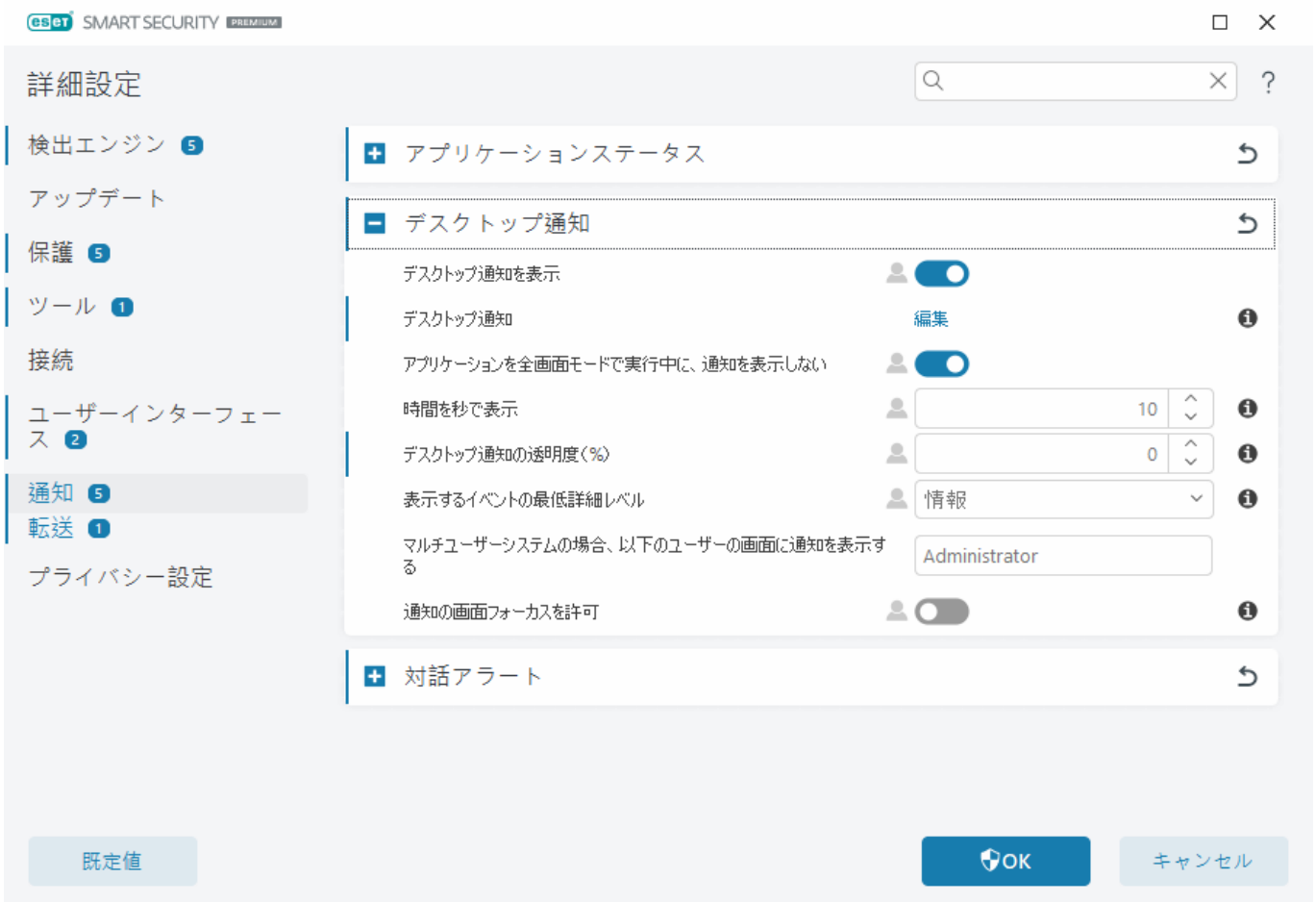
ダイアログウィンドウ – アプリケーションステータス

このダイアログウィンドウでは、表示するアプリケーションステータスを選択できます。たとえば、ウイルス・スパイウェア対策保護を一時停止したり、ゲームモードを有効にしたりするときになどです。

また、製品がアクティベーションされていない場合や、サブスクリプション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。

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、ゆっくりと消えます。通知には、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が含まれます。



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。

o**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が表示されます。

o**情報** – アップデートの成功メッセージを含めて、標準以外のネットワークイベントなどすべての情報メッセージと、上記のすべてのレコードが表示されます。

o**警告** – 警告メッセージ、エラーおよび重大なエラーが表示されます(例: アップデートが失敗した)。

o**エラー** – エラー(例: ドキュメント保護が起動していない)と重大なエラーが表示されます。

o**重大** – 重大なエラー(例: ウイルス対策保護の起動エラーや感染したシステム)のみが表示されます。

マルチユーザーシステムの場合、以下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 – 通知に画面フォーカスが置かれ、**ALT + Tab**メニューでアクセスできるようにします。

デスクトップ通知リスト

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**表示**チェックボックスを選択します。

全般

セキュリティレポート通知を表示する – 新しいセキュリティレポートが生成されるときに通知を受信します。

新機能の通知を表示する – 無効にすると、最新の製品バージョンの新機能と強化された機能すべてに関する通知。

ファイルが分析のために送信されました - ESET Security Ultimateが分析のためにファイルを送信するたびに通知を受信します。

ネットワーク検査

新しく検出されたネットワークデバイスについて通知– 新しいデバイスがネットワークに接続されたときに通知を受信します。

ネットワーク保護

ネットワークプロファイルが変更された – ネットワークプロファイルが変更されたときに通知を受信します。

Wi-Fi保護警告 – 脆弱なパスワードまたはパスワードなしでWi-Fiネットワークに接続しようとすると、通知を受け取ります。

アップデート

プログラムコンポーネントのアップデートが準備されます – 新しいバージョンのESET Security Ultimateのアップデートが準備されたときに通知を受信します。

検出エンジンが正常にアップデートされました – 製品が検出エンジンモジュールをアップデートするときに通知を受信します。

モジュールが正常にアップデートされました – 製品がプログラムコンポーネントをアップデートするときに通知を受信します。

メッセージが表示される時間や、表示するイベントの詳細レベルといったデスクトップ通知の一般設定を設定するには、詳細設定 > **通知**のデスクトップ通知を参照してください。

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
- 機能が多い製品に変更
- 機能の少ない製品に変更
- 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
- モジュールアップデートエラーを解決
- ネットワークの脅威がブロックされました
- Webサイト証明書が取り消されました

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 Security Ultimate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ESETはこのオプションをオンにすることをお勧めします。

製品内メッセージング

製品内メッセージングは、ESETニュースとその他の連絡事項をユーザーに通知するために設定されています。マーケティングメッセージを送信するには、ユーザーの同意が必要です。このため、マーケティングメッセージは、既定では、ユーザーに送信されません(疑問符が表示されます)。このオプションを有効にするとESETマーケティングメッセージを受信することに同意しますESETマーケティング資料に関心がない場合は、**マーケティングメッセージを表示する**オプションを無効にします。

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。

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**を開き、**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 Security Ultimate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。

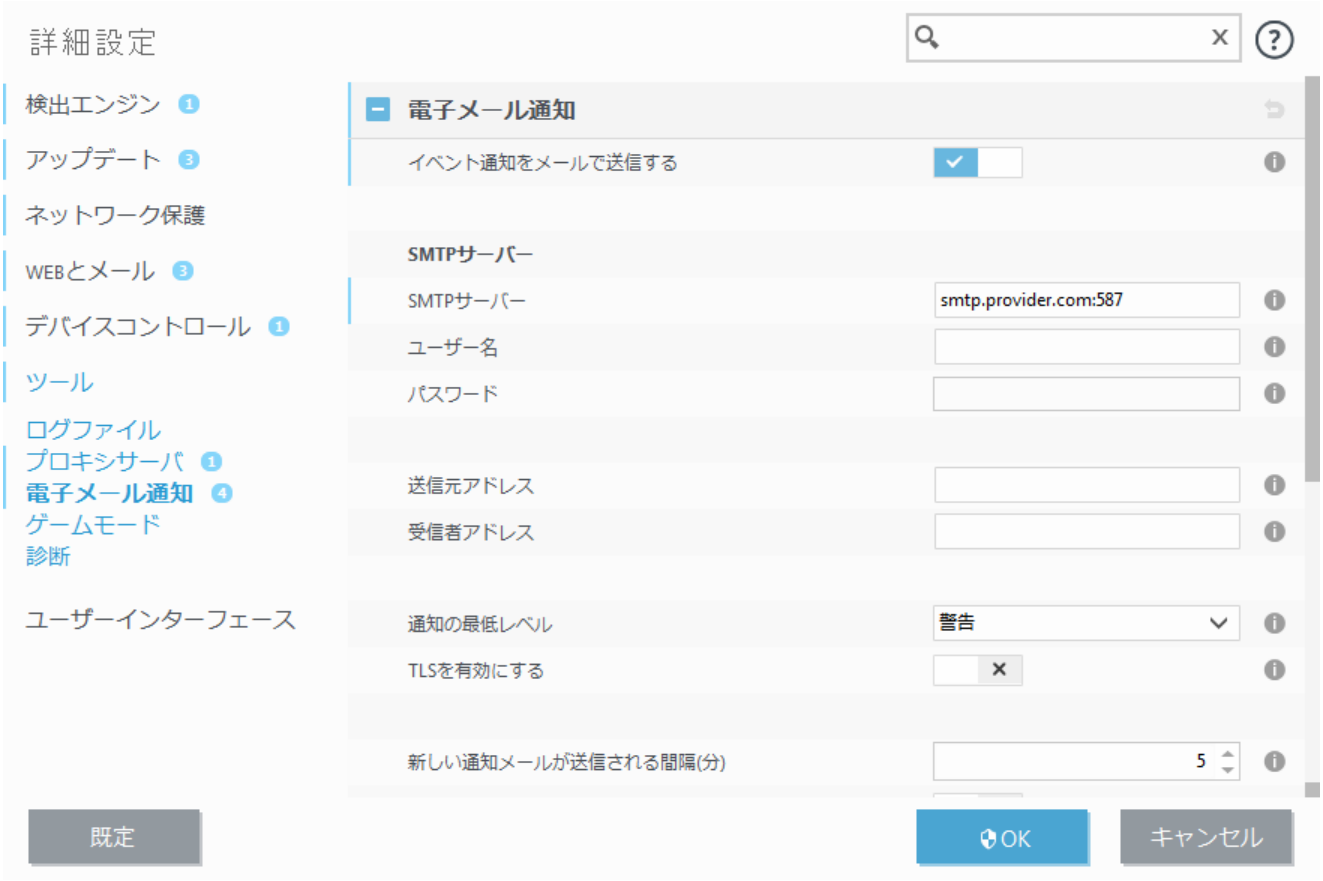
確認メッセージに関連した特定の機能の詳細:

- 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
- 迷惑メール対策処理結果通知を表示する
- 電子メールクライアントの迷惑メール対策処理結果通知を表示する
- 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

転送

ESET Security Ultimate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**を開き、**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。



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する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 Security Ultimateでサポートされます。

ユーザー名とパスワード - SMTPサーバが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。

TLSを有効にする – TLS暗号化を使用してSecure Alertと通知を保護します。

SMTP接続のテスト – テスト電子メールが受信者の電子メールアドレスに送信されますSMTPサーバー、ユーザー名、パスワード、送信者のアドレス、受信者のアドレスを入力する必要があります。

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**既定のメッセージ形式を使用**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。定義済みの書式を使用することをお勧めします。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。

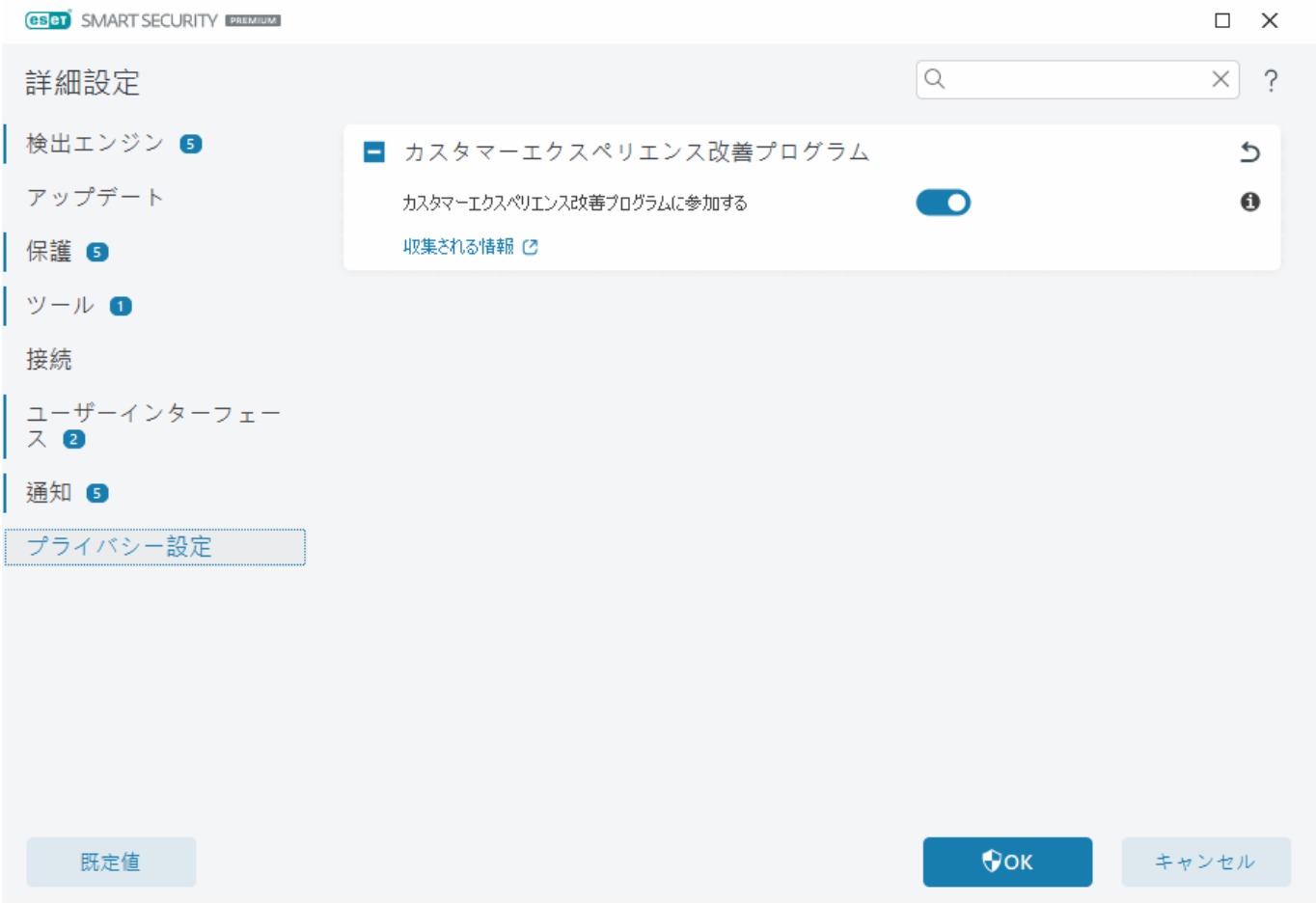
- **%TimeStamp%**– イベントの日時
- **%Scanner%**– 関連するモジュール

- **%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。

プライバシー設定

詳細設定 > **プライバシー設定**を開きます。



カスタマーエクスペリエンス改善プログラム

カスタマーエクスペリエンス改善プログラムに参加するの横のスライダーバーを有効にすると、カスタマーエクスペリエンス改善プログラムに参加できます。参加することで、製品の使用に関連する匿名情報をESETに提供します。収集されたデータは、ESETがお客様の経験を改善するために役立ち、第三者と共有されることはありません。収集される情報

デフォルト設定に戻す

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。

デフォルト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 Security Ultimate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。 使用可能なオプションは • none（既定）- 自動駆除を実行しません。 • 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。 • 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)。 • 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。 • 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 (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	一部のファイルはスキャンできません(マルウェアの可能性あり)

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。

FAQ

以下では、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 Security Ultimateをアップデートする方法
- ESET Security Ultimateが脅威を検出した
- PCからウイルスを取り除く方法
- アプリケーションに通信を許可する方法
- アカウントでペアレンタルコントロールを有効にする方法
- スケジューラで新しいタスクを作成する方法
- 検査タスクをスケジュールする方法(毎週)
- 詳細設定をロック解除する方法
- ESET HOMEから製品のアクティベーション解除を解決する方法

現在の問題が上記の一覧に含まれていない場合は、ESET Security Ultimateオンラインヘルプを検索してみてください。

問題/質問の答えがESET Security Ultimateオンラインヘルプで見つからない場合、定期的に更新されているオンラインESETナレッジベースを調べてみることもできます。よく読まれているナレッジベースの記事へのリンクを以下に示します。

- サブスクリプションを更新する方法
- ESET製品のインストール時にアクティベーションエラーが発生しました。これは何を意味しますか。
- 製品認証キーを使用して ESET Windows ホーム製品をアクティベーションします
- ESETホーム製品をアンインストールまたは再インストールします
- ESETのインストールが完了する前に終了したというメッセージが表示されます。
- サブスクリプションを更新した後で実行する必要があることは何でしょうか (Home のユーザー)
- メールアドレスを変更したときは何をすればよいですか。
- ESET製品を新しいコンピューターまたはデバイスに転送する

- Windowsをセーフモードまたはセーフモードとネットワークで起動する方法
- 安全なWebサイトがブロックされないようにする
- スクリーンリーダーソフトウェアによるESET GUIへのアクセスを許可する

必要に応じて、問題/質問について当社のテクニカルサポートまでお問い合わせいただくこともできます。

ESET Security Ultimateをアップデートする方法

ESET Security Ultimate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。間隔を変更する必要がある場合は、[**ツール**] > [スケジューラ]に移動してください。

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。

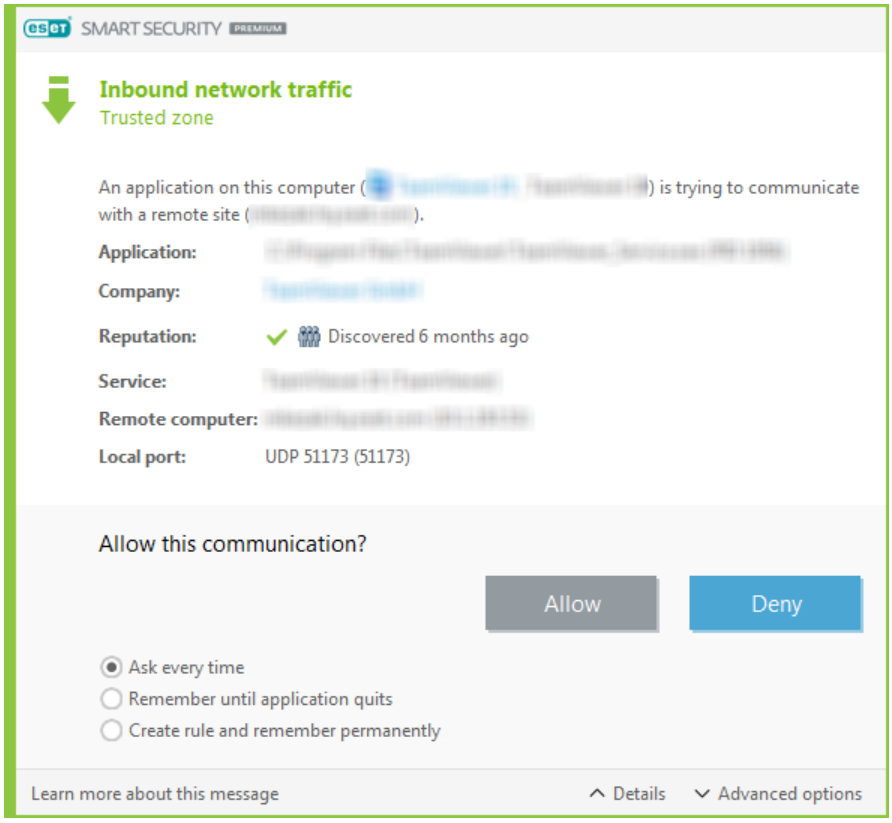
1. プログラムのメインウィンドウで、**コンピューターの検査**をクリックします。
2. **コンピューターの検査**をクリックし、システムの検査を開始します。
3. スキャンが完了したら、スキャンされたファイル、感染しているファイル、および駆除されたファイルの数をログで確認します。
4. ディスクの選択した部分だけを検査するには、**カスタム検査**をクリックし、ウイルスを検査する対象を選択します。

詳細については、以下を参照してください。

- ESETナレッジベース記事
- 隔離

アプリケーションに通信を許可する方法

対話モードで新しい接続が検出された場合、適合するルールがなければ、接続を**許可**するか**拒否**するかを決定する必要があります。ESET Security Ultimateで、アプリケーションが接続を確立しようとするたびに同じアクションを実行するには、**ルールを作成し、永久に記憶**チェックボックスをチェックします。



ファイアウォール設定ではESET Security Ultimateでアプリケーションが検出される前に、アプリケーションの新しいファイアウォールルールを作成できます。メインプログラムウィンドウ > **設定** > **ネットワーク保護** > **ファイアウォール** > **設定** > **詳細** > **ルール** > **編集**をクリックします。

追加ボタンをクリックして、**一般**タブで、ルールの名前、方向、および通信プロトコルを入力します。このウィンドウでは、ルールが適用されたときに実行するアクションを定義することができます。

ローカルタブで、アプリケーションの実行可能ファイルのパスとローカルの通信ポートを入力します。**リモート**タブをクリックして、リモードアドレスとリモートポートを入力します(該当する場合)。アプリケーションが再度通信しようとするとすぐに、新しく作成したルールが適用されます。

アカウントでペアレンタルコントロールを有効にする方法

特定のユーザーアカウントに対してペアレンタルコントロールを有効にするには、次の手順に従います。

1. ESET Security Ultimateでは、既定でペアレンタルコントロールが無効になっています。ペアレンタルコントロールを有効化するには2つの方法があります。

   • プログラムのメインウィンドウから、**設定** > **インターネット保護** > **ペアレンタルコントロール**でトグルアイコンをクリックし、ペアレンタルコントロールの状態を有効に変更します。

   • 詳細設定 > **保護** > **Webアクセス保護** > **ペアレンタルコントロール**を開き、**ペアレンタル コントロールを有効にする**の横にあるトグルを有効にします。

2. メインプログラムウィンドウから、**設定** > **インターネット保護** > **ペアレンタルコントロール**をクリックします。**ペアレンタルコントロール**の横に**有効**が表示されますが、矢印記号をクリックした後に、次のウィンドウで[**子アカウントを保護...**]または[**親アカウント**]をクリックし、目的のアカウントに対してペアレンタルコントロールを設定する必要があります。次のウィンドウに年齢を入力すると、

アクセスレベルおよび推奨の適正年齢のWebページが決まります。これで、指定されたアカウントでのペアレンタルコントロールが有効になります。アカウント名の下の**[ブロックされたコンテンツと設定…]**をクリックし、分類タブで、許可またはブロックする分類をカスタマイズします。分類に一致しないカスタムWebページを許可またはブロックするには、例外タブをクリックします。

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次のとおりです。**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**(**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[**追加**]をクリックします。
2. タスクの名前を入力し、**タスクの種類**ドロップダウンメニューから**オンデマンドコンピューターの検査**を選択します。
3. タスクの頻度として**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。

パスワード保護された詳細設定をロック解除する方法

保護された詳細設定にアクセスするときには、パスワードの入力ウィンドウが表示されます。パスワードがわからない場合は、**パスワードの復元**をクリックして、サブスクリプション登録で使用される電子メールアドレスを入力しますESETは確認コードが記載された電子メールを送信します。確認コードを入力し、新しいパスワードを作成して確認します。確認コードは7日間有効です。

ESET HOMEアカウントを使用したパスワードの復元 – アクティベーションで使用されるサブスクリプションがESET HOMEアカウントに関連付けられている場合には、このオプションを使用します。ESET HOMEアカウントにログインするために使用する電子メールアドレスを入力します。

電子メールアドレスを忘れた場合、またはパスワードの復元ができない場合は、**テクニカルサポートに問い合わせる**をクリックしてくださいESET Webサイトが開き、テクニカルサポート部門に問い合わせることができます。

テクニカルサポート用のコードの生成 – このオプションでは、テクニカルサポート用のコードを生成します。テクニカルサポートから提供されたコードをコピーして、**確認コードがある**をクリックします。確認コードを入力し、新しいパスワードを作成して確認します。確認コードは7日間有効です。

詳細については、ESET Windowsホーム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 HOMEから製品のアクティベーション解除を解決する方法

アクティベーションされていません

このエラーメッセージは、サブスクリプション所有者がESET HOMEポータルからESET Security Ultimateをアクティベーション解除したかESET HOMEアカウントと共有されたサブスクリプションが共有されなくなったときに表示されます。この問題を解決するには次の手順を実行します。

- **アクティベーション**をクリックして、アクティベーション方法のいずれかを使用してESET Security Ultimateをアクティベーションします。
- サブスクリプション所有者によってESET Security Ultimateがアクティベーション解除されたか、サブスクリプションが共有されていないことをサブスクリプション所有者に問い合わせてください。所有者はESET HOMEで問題を解決することができます。

製品がアクティベーション解除されています。デバイスが切断されました

このエラーメッセージは、ESET HOMEからデバイスを削除した後に表示されます。この問題を解決するには次の手順を実行します。

- **アクティベーション**をクリックして、アクティベーション方法のいずれかを使用してESET Security Ultimateをアクティベーションします。
- ESET Security Ultimateがアクティベーション解除され、デバイスがESET HOMEから切断されたという情報をサブスクリプション所有者に連絡してください。

• 自分がサブスクリプション所有者で、これらの変更を認識していない場合は、ESET HOMEアクティビティフィードを確認してください。疑わしいアクティビティが見つかった場合は、ESET HOMEアカウントパスワードを変更し、ESETテクニカルサポートに連絡してください

製品がアクティベーション解除されています。デバイスが切断されました

このエラーメッセージは、ESET HOMEからデバイスを削除した後に表示されます。この問題を解決するには次の手順を実行します。

• **アクティベーション**をクリックして、アクティベーション方法のいずれかを使用してESET Security Ultimateをアクティベーションします。

• ESET Security Ultimateがアクティベーション解除され、デバイスがESET HOMEから切断されたという情報をサブスクリプション所有者に連絡してください。

• 自分がサブスクリプション所有者で、これらの変更を認識していない場合は、ESET HOMEアクティビティフィードを確認してください。疑わしいアクティビティが見つかった場合は、ESET HOMEアカウントパスワードを変更し、ESETテクニカルサポートに連絡してください

アクティベーションされていません

このエラーメッセージは、サブスクリプション所有者がESET HOMEポータルからESET Security Ultimateをアクティベーション解除したかESET HOMEアカウントと共有されたサブスクリプションが共有されなくなったときに表示されます。この問題を解決するには次の手順を実行します。

• **アクティベーション**をクリックして、アクティベーション方法のいずれかを使用してESET Security Ultimateをアクティベーションします。

• サブスクリプション所有者によってESET Security Ultimateがアクティベーション解除されたか、サブスクリプションが共有されていないことをサブスクリプション所有者に問い合わせてください。所有者はESET HOMEで問題を解決することができます。

0

カスタマーエクスペリエンス改善プログラム

カスタマーエクスペリエンス改善プログラムに参加することで、製品の使用に関連する匿名情報をESETに提供します。データ処理の詳細については、プライバシーポリシーをご覧ください。

同意

プログラムへの参加は任意であり、お客様の同意が必要です。参加した後は、一切のアクションは不要であり、自動的に処理されます。お客様は、いつでも、製品設定を変更することで、同意を取り消すことができます。このようにすることでESETはお客様の匿名データの処理を続けることができなくなります。

いつでも、製品設定を変更することで、同意を取り消すことができます:

- ESET Windowsホーム製品でカスタマーエクスペリエンス改善プログラム設定を変更する

収集される情報の種類

製品の操作に関するデータ

この情報によってESETは製品の使用方法に関する詳細を理解することができます。これによりESETは、頻繁に使用される機能、ユーザーが修正する設定、または製品の使用に費やされた時間などを把握することができます。

デバイスに関連するデータ

ESETは、製品が使用されている場所やデバイスについて理解するためにこの情報を収集します。一般的な例としては、デバイスモデル、国、バージョン、オペレーティングシステム名などがあります。

エラー診断データ

エラーおよびクラッシュの状況に関する情報も収集されます。たとえば、発生したエラーと原因となったエラーが収集されます。

なぜこの情報が収集されるのですか。

この匿名情報によりESETはお客様のために製品を改善することができます。この情報は、できるかぎり、関連性が高く、使いやすく、エラーのない製品を開発するうえで役立ちます。

誰がこの情報を管理するのですか。

ESET, spol. s r.o.はプログラムで収集されるデータの単独の管理者です。この情報が第三者と共有されることはありません。

エンドユーザーライセンス契約

発効日：2021年10月19日

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

エンドユーザー使用許諾契約

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

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

本ソフトウェアのインストール時、ダウンロード時、コピー時または使用時に、[同意します]オプションをクリックすることにより、本契約の条件に明示的に同意し、プライバシーポリシーを承諾するもの

とします。本契約の規定またはプライバシーポリシーに同意しない場合は、直ちに[同意しない]オプションをクリックし、インストールまたはダウンロードを取り消すか、本ソフトウェア、インストールメディア、付属ドキュメント、および購入時の領収書を破棄するかESETまたは本ソフトウェアの供給者にそれを返却してください。

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

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

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

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

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

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

されます。本契約または供給者によって許可されている場合を除き、お客様はライセンスを第三者と共有すること、または第三者がライセンスを使用することを許可することが禁止されています。ライセンスキーが危険にさらされた場合は、速やかに供給者に通知してください。

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

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

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

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

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

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

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

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

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

情報および侵入は次のソフトウェア機能によって収集される場合があります。

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

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

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

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

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

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

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

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

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

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

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

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

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

f) お客様は、本ソフトウェアおよびその機能を、他のエンドユーザーがそれらのサービスにアクセスする可能性を制限しない方法でのみ使用することに同意するものとします。供給者は、可能な限り多くのエンドユーザーがサービスを利用できるようにするために、個別のエンドユーザーに提供されるサービスの範囲を制限する権利を留保します。サービスの範囲を制限することにより、本ソフトウェアのすべ

ての機能を使用することもできなくなり、本ソフトウェアの特定の機能に関連する供給者のサーバー上またはサードパーティのサーバー上のデータおよび情報も削除されることとします。

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

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

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

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

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

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

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

13.**責任の制限**。準拠法によって許可される最大限の範囲において、いかなる場合も、供給者、その被雇用者、ライセンス供給者は、どのような態様で発生したものであろうと、契約、違法行為、怠慢、または責任の発生を定めるその他の事実のいずれに起因するものであるかを問わず、本ソフトウェアのインストール、本ソフトウェアの使用、または本ソフトウェアが使用できないことにより発生した、利益、収益、または売上の損失、データの喪失、補用品またはサービスの購入にかかった費用、物的損害、人

的損害、事業の中断、企業情報の喪失、特別損害、直接損害、間接損害、偶発的損害、経済的損害、補填損害、懲罰的損害、特別または派生的損害に対し、一切責任を負わないものとします。これは、たとえ供給者、そのライセンス供給者、または関係者がそのような損害の可能性について通知を受けていた場合であっても同様です。一部の国および法律では、免責を認めず、しかし限定された範囲の責任を負うことは許可しています。その場合、供給者、その被雇用者、ライセンス供給者、または関係者の責任は、お客様がライセンスの対価として支払った金額を限度とします。

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

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

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

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

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

19.**輸出管理規制**

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

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

ii. 米国、シンガポール、英国、欧州連合またはその加盟国、本契約の義務が履行される国、あるいはESETまたはその関連会社が登録または事業を行う国の政府、州、規制当局が課した経済、金融、貿易、

制裁、制限、禁止、輸出入禁止、資金または資産の移転の禁止、サービス提供の禁止、あるいは同等の対策。

（上記第i項および第ii項で参照される法律、ならびに「貿易管理法」）。

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

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

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

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

20.**通知**。すべての通知、ならびに本ソフトウェアおよびドキュメントの返却は、本契約の第22条に従い、本契約、プライバシーポリシ□□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。

契約書の補遺

ネットワーク接続デバイスセキュリティ評価。ネットワーク接続デバイスセキュリティ評価には、次のように追加の条項が適用されます。

本ソフトウェアには、ネットワーク接続デバイスセキュリティ評価の一部としてライセンス情報に関連する、ローカルネットワークのデバイスの存在、タイプ、名前IPアドレス、およびMACアドレスなど、ローカルネットワークのデバイスに関する情報とローカルネットワーク名が必要な、エンドユーザーのセキュリティとローカルネットワークのデバイスのセキュリティを確認する機能があります。これらの情報には、ルーターデバイスのワイヤレスセキュリティタイプとワイヤレス暗号化タイプも含まれます。この機能は、ローカルネットワークのデバイスを保護するためのセキュリティソフトウェアソリューションの利用状況に関する情報も提供する場合があります。

データの悪用に対するAnti-Theftの保護。データの悪用に備える保護対策には、次のように追加の条項が適用されます。

本ソフトウェアには、コンピューターの窃盗と直接関連して、重要なデータの損失または悪用を防止する機能が含まれています。この機能は、本ソフトウェアの既定の設定でオフにされています。アクティベーションするにはESET HOMEアカウントを作成する必要があります。 これによって、コンピューターの窃盗の際に、データ収集が有効になります。本ソフトウェアのこの機能を有効にする場合は、盗まれたコンピューターに関するデータが収集され、供給者に送信されます。これには、コンピューターのネットワーク位置情報データ、コンピューター画面に表示された内容のデータ、コンピューターの構成のデータ、およびコンピューターに接続されたカメラによって記録されたデータ(「データ」)が含まれることがあります。エンドユーザーは、コンピューターの窃盗が原因の問題を修正する目的でのみ、この機能で取得されESET HOMEアカウントに送信されたデータを使用する資格があります。この機能の目的に限り、供給者は、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、データを処理します。供給者は、データが取得された目的を達成するために必要な期間の間、エンドユーザーがデータにアクセスすることを許可するものとします。ただし、この期間は、プライバシーポリシーで規定された保持期間を超えないものとします。データの悪用に対する保護は、エンドユーザーが合法的にアクセスできるコンピューターおよびアカウントでのみ使用されるものとします。不法使用は管轄当局に報告されます。供給者は関連する法律を遵守し、悪用の場合には法執行機関を支援します。お客様は、自身がESET HOMEアカウントにアクセスするためのパスワードを保護する責任を有することを認め、パスワードをいかなる第三者にも開示しないことに同意します。エンドユーザーは、許可の有無を問わず、データの悪用保護機能ESET HOME アカウントを使用したすべての活動に責任を負いますESET HOMEアカウントが危険にさらされた場合は、ただちに供給者に通知してください。データの悪用に備える保護対策の追加条項はESET Internet SecurityおよびESET Smart Security Premiumエンドユーザーにのみ適用されるものとします。

ESET Secure DataESET Secure Dataには、次のように追加の条項が適用されます。

1. 定義ESET Secure Dataのこれらの追加条項では、次の単語には次の対応する意味があります。

a) 「情報」本ソフトウェアを使用して暗号化または復号化される情報またはデータ。

b) 「製品」ESET Secure Dataソフトウェアおよびマニュアル;

c) 「ESET Secure Data」電子データの暗号化および復号化で使用されるソフトウェア。

複数形のすべての参照には、単数形が含まれるものとします。男性形のすべての参照には、女性形および中性形が含まれるものとします。また逆も同様とします。特定の定義がない単語については、本契約で規定された定義に従って使用されるものとします

2. 追加のエンドユーザー宣言。お客様は次のことを認め、同意するものとします。

a) 情報を保護、管理、およびバックアップするのはお客様の責任です。

b) ESET Secure Dataをインストールする前に、コンピューターのすべての情報およびデータ(重要な情報

とデータを含むがこれらに限定されない)を完全にバックアップしてください。

c) お客様は、ESET Secure Dataのセットアップおよび利用に必要なすべてのパスワードまたはその他の情報を安全に記録しておく必要があります。また、すべての暗号化キー、ライセンスコード、鍵ファイル、およびその他のデータのコピーを別のストレージメディアにバックアップする必要があります。

d) お客様は製品の使用について責任を負うものとします。供給者は、情報またはデータの保存場所または保存方法に関係なく、情報またはデータ(情報を含むがこれに限定されない)の不正または誤った暗号化または復号化の結果として生じる一切の損失、請求、または損害について責任を負わないものとします。

e) 供給者はあらゆる合理的な手順を講じ、ESET Secure Dataの完全性およびセキュリティを保証することに努めていますが、セキュリティのフェールセーフレベルに依存する領域、あるいは核施設、航空機ナビゲーション、制御、または通信システム、兵器および防衛システム、生命維持または生命監視システムを含む(ただしこれらに限定されない)有害または危険の可能性がある領域において、製品(またはそのいずれか)を使用することは禁止されています。

f) 本製品によって提供されたセキュリティと暗号化のレベルが要件に適していることを確認することはお客様の責任です。

g) お客様は、このような使用がスロバキア共和国または製品が使用される他の国、地域、州などにおけるすべての適用される法律および規制に準拠することの保証を含め(ただしこれに限定されない)、製品(またはそのいずれか)を使用する責任を負うものとします。お客様は、製品を使用する前に、あらゆる政府(スロバキア共和国または他国)の禁止措置に抵触しないことを保証する必要があります。

h) ESET Secure Dataは時々供給者のサーバーに接続し、ライセンス情報、使用可能なパッチ、サービスパック、およびESET Secure Dataの動作を改善、維持、修正、または強化できるその他のアップデートを確認し、プライバシーポリシーに準拠した方法で機能に関連する一般システム情報を送信する場合があります。

i) 供給者は本ソフトウェアの使用中に生成または保存されたパスワード、設定情報、暗号化キー、ライセンスアクティベーションコード、およびその他のデータの損失、窃盗、悪用、破損、損害、または破壊から生じる一切の損失、損害、費用、または請求については責任を負わないものとします。

ESET Secure Dataの追加条項はESET Smart Security Premiumエンドユーザーにのみ適用されるものとします。

Password Managerソフトウェア。Password Managerソフトウェアには、次のように追加の条項が適用されます。

1. 追加のエンドユーザー宣言。添付文書1はESET Smart Security Premiumエンドユーザーにのみ適用されるものとします。

a) Password Managerソフトウェアを使用して、人間の生命または財産が危険にさらされる可能性がある重要なアプリケーションを運用すること。お客様は、Password Managerソフトウェアがこのような目的では設計されておらず、このような場合における障害は、供給者が責任を負わない死亡、人身傷害、または重大な財産または環境への損害につながる可能性があることを理解するものとします。

PASSWORD MANAGERソフトウェアは、核施設、航空機ナビゲーションまたは通信システム、航空交通管制、および生命維持または兵器システムの設計、開発、保守、または運用を含む(ただしこれらに限定されない)、フェールセーフ制御が必要な危険な環境で使用することを目的としておらず、そのような目的で設計またはライセンス供与されていません。供給者はこのような目的への適合性の明示的または暗示的な保証を具体的に放棄します。

b) 本契約あるいはスロバキア共和国または管轄地域の法律に抵触する方法でPassword Managerソフトウェアを使用すること。特に、Password Managerソフトウェアを使用して、有害なコンテンツ、あるいはス

トレージ(Password Managerソフトウェアの追加条項では、「ストレージ」は供給者または供給者以外の第三者、およびユーザーデータ の同期とバックアップを有効するためにユーザーが管理するデータストレージ領域を意味します)のアカウント、または他のPassword Managerソフトウェアまたはストレージユーザーのアカウントとデータへのアクセスを取得する試みを含む(ただしこれらに限定されない)、不法行為で使用される可能性があるコンテンツ、または何らかの方法で法律または第三者の権利(知的財産権を含む)を侵害するコンテンツを含む、不法行為を実施または促進することは禁止されています。これらの規定に違反した場合、供給者はただちに本契約を解除し、必要な救済策の費用をお客様に課し、返金の可能性を排除してお客様がPassword Managerソフトウェアを使用できないようにするために必要な手順を講じる資格があります。

2. 責任の制限PASSWORD MANAGERソフトウェアは「現状有姿」で提供されます。一切の明示的または暗示的な保証はありません。本ソフトウェアはお客様の責任で使用するものとします。開発者は、データ同期およびバックアップ目的でPASSWORDMANAGERソフトウェアから外部ストレージに送信されたデータを含む、データの損失、損害、サービス可用性の制限については責任を負いませんPASSWORD MANAGERを使用してデータを暗号化することによって、供給者はそのデータのセキュリティに関する一切の責任を課されないものとします。お客様は、PASSWORD MANAGERソフトウェアを使用して取得、使用、暗号化、保存、同期、または送信されたデータが第三者のサーバーに保存されることがあるということにも明示的に同意するものとします(同期およびバックアップサービスが有効な場合のPASSWORD MANAGERソフトウェアの使用にのみ適用)。供給者がその独自の裁量においてこのような第三者のストレージWebサイトWebポータル、サーバー、またはサービスを使用することを選択した場合、供給者はこのような第三者のサービスの品質、セキュリティ、または可用性について責任を負わないものとします。また、いかなる範囲においても、供給者はお客様に対して第三者の契約または法的義務違反、あるいは本ソフトウェアの使用中に発生した損害、利益の損失、財務的または非財務的損害、またはいかなる他の種類の損失について責任を負わないものとします。供給者はPASSWORD MANAGERソフトウェアを使用して取得、使用、暗号化、保存、同期、または送信されたデータあるいはストレージのデータの内容について責任を負いません。お客様は、供給者が保存されたデータの内容にアクセスできず、データの監視ができず、法的に有害なコンテンツを削除できないことを確認するものとします。

このような改良が何らかの形式でお客様から提出されたフィードバック、アイデア、または提案に基づいて作成された場合においても、供給者はPassword MANAGERソフトウェアに関連する改良、アップグレード、および修正(「改良」)に対するすべての権限を有します。お客様は、このような改良の使用許諾料を含む一切の補償を受け取る権利がないものとします。

供給者企業およびライセンサーは、たとえこのような請求および責任が法的または衡平法上の理論に基づいていたとしても、いかなる方法においても、お客様または第三者によるソフトウェアの使用、

いかなる仲介企業または代理店の使用または不使用、あるいはセキュリティの販売または購入に起因して生じるもしくはそれに関連する一切の種類の請求および義務に対する責任を負わないものとします。供給者企業およびライセンサーは、このような損害請求が法律または衡平法の理論に基づいているかどうかにかかわらず、お客様に対して、第三者のソフトウェアPASSWORD MANAGERソフトウェアを使用してアクセスされるデータ、お客様がPASSWORD MANAGERを使用すること、使用またはアクセスできないこと、あるいはPASSWORD MANAGER経由で提供されたデータから生じるかそれに関連する一切の直接的、付随的、特殊的、間接的、または結果的な損害の責任を負わないものとします。本条項から除外される損害には、事業利益の損失、個人または財産に対する損害、事業の中断、事業または個人情報の損失(ただしこれらに限定されない)があります。 管轄地域によって、付随的または結果的損害の制限が認められない場合があるため、本制限事項がお客様には適用されない場合があります。このような場合、供給者の責任の範囲は適用される法律の下で認められた最低限になります。

株価、分析、市場情報、ニュース、財務データを含むソフトウェア経由で提供される情報には遅延や不正確性、または瑕疵や省略がある可能性があります。供給者企業およびライセンサーはこのような点に関して責任を負わないものとします。供給者は、いかなる時点においても、お客様への事前の通知なくPASSWORD MANAGERソフトウェアの何らかの要素または機能、あるいはPASSWORD MANAGERソフトウェアのすべてまたは一部の機能または技術の使用を変更または終了する場合があります。

本項の条項が何らかの理由により無効になった場合、または適用される法の下で供給者が損失、損害な

どに対する責任を負うと見なされる場合、両当事者は、お客様に対する供給者の責任はお客様が支払ったライセンス料金の合計金額を上限とすることに同意するものとします。

お客様は、あらゆる第三者(その権限がPASSWORD MANAGERソフトウェアまたはストレージで使用されるデータによって影響されたデバイスの所有者または当事者を含む)の請求、責任、損害、コスト、費用、このような当事者がお客様によるPASSWORD MANAGERソフトウェアの使用の結果として発生しうる料金に対して、供給者およびその従業員、子会社、関係会社、再ブランディング、および他のパートナーを補償、保護、および無害に保つことに同意するものとします。

3.Password Managerソフトウェアのデータ。特に明示的に明記されていないかぎり、お客様が選択してPassword Managerソフトウェアデータベースに保存されるすべてのデータはコンピューターまたはお客様が定義した他のストレージデバイス上に暗号化された形式で保存されます。お客様は、Password Managerソフトウェアデータベースまたは他のファイルの削除または損害が発生した場合には、そこに保存されているすべてのデータが不可逆的に失われることを理解し、このような損失のリスクを理解および承諾するものとします。お客様の個人データがコンピューターに暗号化された形式で保存されるということは、マスターパスワードを知り得た人物が情報を窃盗または悪用したり、データベースを開く目的でお客様が定義したアクティベーションデバイスにアクセスできないことを意味するものではありません。お客様は、すべてのアクセス方法のセキュリティを管理する責任を負うものとします

4. 供給者またはストレージへの個人データの転送。そのように選択した場合、タイムリーなデータ同期およびバックアップを保証する目的でのみ、Password Managerソフトウェアは Password Managerソフトウェアデータベースからパスワード、ログイン情報、アカウント、およびIDなどの個人データをインターネット経由でストレージに転送または送信します。データは暗号化された形式でのみ転送されます。パスワード、ログイン情報、または他のデータをオンラインフォームに入力する目的でPassword Managerソフトウェアを使用する場合、お客様が指定したWebサイトにインターネット経由で情報を送信する必要があります。このデータ転送はPassword Managerソフトウェアによって開始されないため、供給者は各種供給者によってサポートされるWebサイトとのこのような連携のセキュリティについては責任を負いかねます。インターネット上のあらゆる処理は、Password Managerソフトウェアと連動しているかどうかにかかわらず、お客様独自の裁量およびリスクで行われ、このような素材またはサービスのダウンロードまたは使用から生じるコンピューターシステムへの損害またはデータの損失についてはお客様が単独で責任を負うものとします。価値のあるデータの損失リスクを最小化するために、供給者は、お客様がデータベースおよび他の重要なファイルを定期的に外部デバイスにバックアップすることをお勧めします。供給者は損失または破損したデータの復元については一切の支援を提供いたしかねます。ユーザ PCのファイルの破損または削除の場合に供給者がユーザーデータベースファイルのバックアップサービスを提供する場合、このようなバックアップサービスには一切の保証がなく、供給者はいかなる場合でも責任を負わないものとします。

Password Managerソフトウェアを使用することによって、お客様は、本ソフトウェアが時々供給者のサーバーに接続し、ライセンス情報、使用可能なパッチ、サービスパック、およびPassword Managerソフトウェアの動作の改良、メンテナンス、修正、または機能強化につながる可能性がある他のアップデートを確認することに同意するものとします。本ソフトウェアは、プライバシーポリシーに準拠し、Password Managerソフトウェアの機能に関連する一般システム情報を送信する場合があります。

5. アンインストール情報および手順。データベースに保持するすべての情報は、Password Managerソフトウェアをアンインストールする前にエクスポートする必要があります。

Password Managerソフトウェアの追加条項はESET Smart Security Premiumエンドユーザーにのみ適用されるものとします。

ESET LiveGuard.ESET LiveGuardには、次のように追加の条項が適用されます。

本ソフトウェアには、エンドユーザーによって送信されたファイルの追加の分析機能が含まれています。供給者は、エンドユーザーが提出したファイル、ならびにプライバシーポリシーおよび関連する法規制に準拠した分析結果のみを使用するものとします。

ESET LiveGuardの追加条項はESET Smart Security Premiumエンドユーザーにのみ適用されるものとします。

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

プライバシーポリシー

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

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

個人データの処理の法的根拠

ESETが個人データの保護に関連する該当する法的フレームワークに従って使用するデータ処理には、ほとんど法的根拠がありませんESETにおける個人データの処理は、主に、エンドユーザーとの エンドユーザー使用許諾契約 (EULA)の履行(GDPR第6 (1) (b)条)に必要です。これは、明示的な記載がないかぎりESETの製品またはサービスの提供に適用されます。例:

- 正当な利益という法的根拠(GDPR第6 (1) (f)条)。これにより、お客様がサービスを使用する方法、ならびにESETが提供できる最高の保護、サポート、およびエクスペリエンスに対するお客様の満足度に関するデータを処理できます。適用される法律では、マーケティングも正当な利益と認識されているため、通常はお客様とのコミュニケーションで使用されるCookieについては、この概念を適用します。

- 同意(GDPR第6 (1) (a)条)ESETがこの法的根拠を最も適切な根拠であると見なすとき、または法律で義務付けられている場合には、特定の状況においてESETがお客様の同意を求める場合があります。

- 電子通信、請求または課金文書の保持に関する要件の規定など、法的義務の遵守(GDPR第6 (1) (c)条)。

データ共有と機密保持

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

基本的に、ESETは、欧州連合(EU)でデータを処理します。ただし、お客様の居住国(EU外での製品またはサービスの利用)またはお客様が選択するサービスによってはEU外の国にお客様データを転送しなけれ

ばならない場合があります。たとえばESETは、クラウドコンピューティングに関連してサードパーティサービスを使用しています。このような場合ESETはサービスプロバイダーを厳選し、契約、技術、組織的な対策を導入して、適切なレベルのデータ保護を保証します。原則としてESETは、EUの標準契約条項と補足契約規制(必要な場合)に同意します。

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

データセキュリティ

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、すぐに該当する監督当局とデータ主体として影響を受けるエンドユーザーに通知します。

データの主体の権利

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

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

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

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

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

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

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

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

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

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

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

個人データの処理

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

ライセンスおよび請求データ。名前、電子メールアドレス、製品認証キー、(該当する場合)住所、会社名、決済データは、適用法またはお客様の同意に従って、ライセンスのアクティベーション、製品認証キーの提供、有効期限のリマインダー、サポート依頼、ライセンスが本物であることの検証、サービスの提供、および他の通知(マーケティングメッセージを含む)を支援する目的で、ESETによって収集および処理されますESETは、10年間請求情報を保持する法的義務を負っています。ただし、ライセンス情報は、遅くともライセンスの有効期限から12か月間経過した後に匿名化されます。

アップデートおよび他の統計情報。処理される情報には、製品がインストールされているプラットフォームを含むインストール処理とコンピューターに関する情報、およびオペレーティングシステム、ハードウェア情報、インストールIDライセンスIDIPアドレスMACアドレス、製品の構成設定といった製品の動作と機能に関する情報が含まれます。これらの情報は、アップデートおよびアップグレードサービスの提供、ならびにESETバックエンドインフラストラクチャのメンテナンス、セキュリティ、改善の目的で処理されます。

この情報はエンドユーザーを特定する必要がないため、ライセンスおよび請求目的で必要な個人を識別する情報とは別に保持されます。保持期間は最大4年間です。

ESET LiveGrid®レピュテーションシステム。侵入に関連する単方向ハッシュは、検査されたファイルを、クラウドのホワイトリストおよびブラックリスト項目のデータベースと比較することで、マルウェア対策ソリューションを効率化するESET LiveGrid®レピュテーションシステムの目的で処理されます。この処理中にエンドユーザーが特定されることはありません。

ESET LiveGrid®フィードバックシステム。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

- 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

- IPアドレスおよび地理情報、IPパケット、URLおよびイーサネットフレームなどのインターネットの使用に関する情報

- 含まれるクラッシュダンプファイルと情報。

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

ESET LiveGrid®フィードバックシステム経由で取得および処理されるすべての情報は、エンドユーザーを特定せずに使用されます。

ネットワーク接続デバイスセキュリティ評価。セキュリティ評価機能を提供するために、ESETは、ライセンス情報に関連する、ローカルネットワークのデバイスの存在、タイプ、名前、IPアドレス、およびMACアドレスなど、ローカルネットワークのデバイスに関する情報とローカルネットワーク名を処理します。これらの情報には、ルーターデバイスのワイヤレスセキュリティタイプとワイヤレス暗号化タイプも含まれます。エンドユーザーを識別するライセンス情報は、ライセンスの有効期限から最大12か月間匿名化されます。

テクニカルサポート。サポート要求に含まれる連絡先・ライセンス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。テクニカルサポートで処理されたデータは4年間保管されます。

データの悪用に対するAnti-Theftの保護。https://home.eset.comでESET HOMEアカウントを作成し、コンピューターの盗難に対処してエンドユーザーがこの機能を有効にした場合は、次の情報が収集および処理されます。位置情報データ、スクリーンショット、コンピューターの構成に関するデータ、コンピューターのカメラによって記録されたデータ。収集されたデータは、3か月間の保持期間の間、ESETのサーバーまたはESETのサービスプロバイダーのサーバーに保管されます。

Password Manager Password Managerの機能を有効にした場合、ログイン詳細情報に関するデータは暗号化された形式でお客様のコンピューターまたは他の指定されたデバイスに保存されます。同期サービスを有効にすると、暗号化データはESETサーバーまたはサービスプロバイダーのサーバーに保存され、このようなサービスが保証されますESETもサービスプロバイダーも、暗号化されたデータにはアクセスできません。お客様のみがデータを復号化するための鍵を保有しています。 この機能を無効にすると、データが削除されます。

ESET LiveGuard.ESET LiveGuard機能を有効にする場合は、エンドユーザーがあらかじめ定義および選択したファイルなどのサンプルを送信する必要があります。リモート分析に選択したサンプルは、ESETサービスにアップロードされ、分析の結果がコンピューターに送信されます。不審なサンプルは、ESET LiveGrid®フィードバックシステムによって収集される情報の方法で処理されます。

カスタマーエクスペリエンス改善プログラム。お客様が カスタマーエクスペリエンス改善プログラム のアクティベーションを選択した場合、お客様の同意に基づき、当社の製品の使用に関連する匿名のテレメトリー情報が収集され、使用されます。

ESETの製品およびサービスを使用する個人が製品またはサービスを購入したエンドユーザーではなくESETとエンドユーザーライセンス契約を締結していない場合(例: エンドユーザーの従業員、家族、エンドユーザーライセンス契約に従ってエンドユーザーから製品またはサービスの使用を許可された人)GDPR第6(1)f)条の解釈に従い、ESETの合法的な利益において、データの処理が実行され、エンドユー

ザーが許可したユーザーはエンドユーザーライセンス契約に従ってESETが提供する製品およびサービスを使用できるものとします。

連絡先情報

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

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