ESET Endpoint Security
ユーザーズマニュアル

■お断り

○本マニュアルは、作成時のソフトウェアおよびハードウェアの情報に基づき作成されています。ソフトウェアのバージョンアップなどにより、記載内容とソフトウェアに記載されている機能が異なる場合があります。また、本マニュアルの内容は、改訂などにより予告なく変更することがあります。

改定日　2020/1/31

目　次

Chapter 1 はじめに

1.1 ESET Endpoint Security について

ESET Endpoint Security は、コンピューターのセキュリティ対策に新しいアプローチで取り組んでいます。最新バージョンの ThreatSense 検査エンジンは、ファイアウォールおよび迷惑メール対策機能を備え、高い精度と軽快な動作を実現しつつ、コンピューターにとって脅威となる攻撃とマルウェアを常に警戒します。

ESET Endpoint Security は、ESET 社の長期にわたる取組によって保護機能の最大化とシステムリソース消費量の最小化を実現した完全なセキュリティソリューションです。人工知能に基づく高度な技術は、システムのパフォーマンスを低下させたり、コンピュータ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、およびその他のインターネット経由の攻撃の侵入を強力に阻止します。

ESET Endpoint Security は ESET Security Management Center と接続することにより、ネットワークに接続された複数のコンピューターを簡単に一元管理し、ポリシーとルールの適用、検出の監視、リモート設定などが可能になります。

1.2 動作環境

ESET Endpoint Security は Windows クライアントオペレーティングシステム専用の製品です。動作環境については、弊社ホームページをご参照ください。
https://eset-info.canon-its.jp/business/endpoint_protection_adv/spec.html

! 重 要

ESET Endpoint Security は、サーバー OS にインストールすることはできません。サーバー OS をご使用の場合は、ESET File Security for Microsoft Windows Server をインストールしてください。具体的な動作環境については、上記製品ホームページを参照してください。

1.3 ご利用にあたって

ウイルス対策ソフトを導入しているだけでは、不正侵入とマルウェアが引き起こす危険を完全に排除することはできません。最大限の保護と利便性を得るためには、ウイルス対策ソフトを正しく使用し、セキュリティルールを守ることが重要です。

■定期的にアップデートする

毎日数千種類のマルウェアが新たに作成されています。ESET では、これらのウイルスを毎日解析し、アップデートファイルをリリースしています。保護レベルを継続的に向上させるために、定期的にアップデートを行ってください。
アップデートの設定方法については「3.3 アップデートの設定」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

多くのマルウェアは効率的に広めるために、システムの脆弱性を悪用するように作成されています。そのため、ソフトウェアベンダ各社は、システムの脆弱性を悪用されないためにセキュリティアップデートファイル（セキュリティパッチ）を定期的にリリースしています。これらのセキュリティアップデートファイルは、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 ブラウザーは、セキュリティアップデートファイルが定期的にリリースされています。

■重要なデータをバックアップする

マルウェアによってオペレーティングシステムの誤操作が引き起こされ、重要なデータが喪失されることがあります。定期的に DVD や外付けハードディスクなどの外部媒体にバックアップを行ってください。システム障害が発生したときにバックアップされたデータを使用して素早く復旧することができます。

■コンピューターにウイルスがいないか定期的にスキャンする

検出エンジンは毎日アップデートされています。定期的にコンピューター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

多くのマルウェアは、ユーザーが操作を行わないと実行されずに蔓延することはありません。新しいファイルを開くときに注意をすれば、マルウェアの蔓延を防ぐことができます。マルウェアの蔓延を防ぐ有効的なルールのいくつかは次のとおりです。

- 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は注意する。特に、大量に送信されたメールや、知らない送信者からのメールの添付ファイルに注意する。
- 日々の作業では、コンピューターの管理者アカウントを使用しない。

Chapter 2 インストール

2.1 インストール手順

インストーラーを利用した手動インストールの手順について記載しています。以下の手順に沿ってインストール作業を実施します。
リモートインストールを行う場合は、『ESET Security Management Center ユーザーズマニュアル』を参照してください。

STEP 1	ESET Endpoint Security をインストールする	P8 参照
STEP 2	アクティベーションを行う	P15 参照
STEP 3	コンピューターの検査を行う	P19 参照

2.2 標準インストール

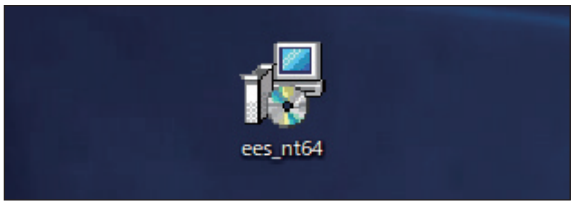
標準インストールには、ほとんどのユーザーに適した設定オプションが用意されています。特定の設定を行わない場合は、標準インストールでインストールを行います。
詳細インストールを行う場合は手順④まで操作を行った後「2.3 詳細インストール」に進みます。

! 重 要

ESET Endpoint Security をインストールする前に、他のウイルス対策ソフトがインストールされていないことを確認してください。2 つ以上のウイルス対策ソフトが 1 台のコンピューターにインストールされていると、互いに競合し重大な問題が発生する場合がありますので、他のウイルス対策ソフトはアンインストールしてください。

操作手順

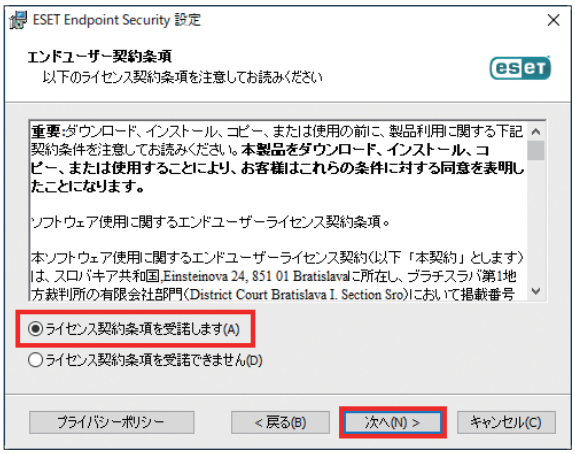
1 ダウンロードしたインストーラーを起動します。



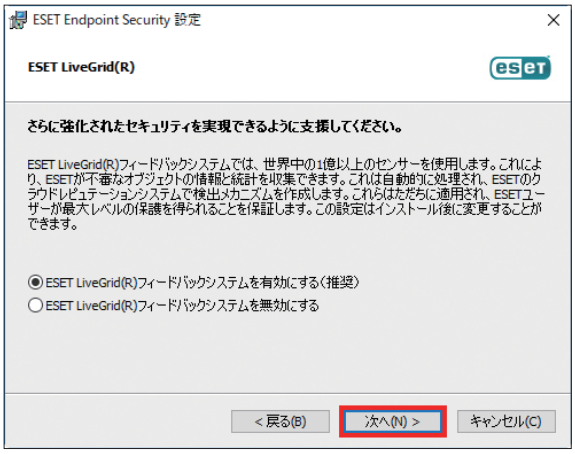
2 インストーラーが起動します。［次へ］ボタンをクリックします。

続く

3 エンドユーザー契約条項の内容を確認し［ライセンス契約条項を受諾します］を選択し［次へ］ボタンをクリックします。



4 ESET LiveGrid を有効にする場合は、［ESET LiveGrid（R）フィードバックシステムを有効にする（推奨）］のチェックを確認して［次へ］ボタンをクリックします。

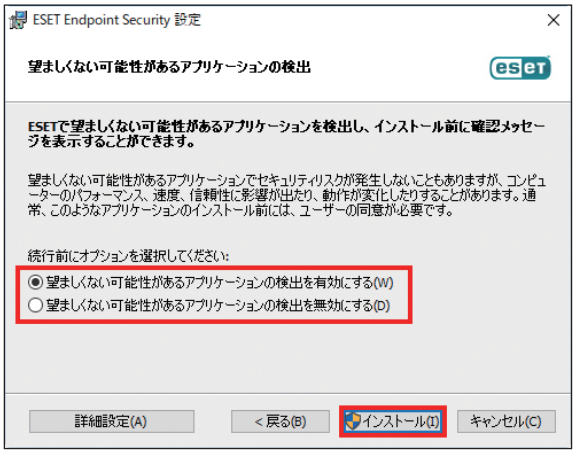


ワンポイント

ESET LiveGrid（早期警告システム）は新しく検出したウイルスの統計情報や、疑わしいファイルが検出された場合に ESET 社へ情報の送信を行います。
ESET 社へ届いた情報が解析および処理され、早く正確にマルウェアを検出することが可能になります。

続く

5 望ましくない可能性があるアプリケーションの検出有無を選択します。



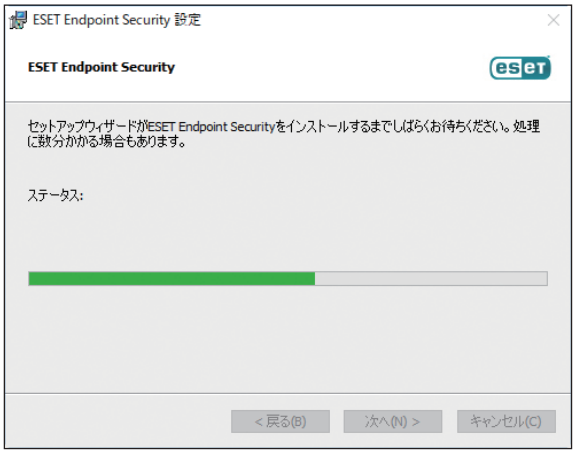
ワンポイント

望ましくない可能性があるアプリケーションの検出の詳細は「4.6.2 リアルタイムファイルシステム保護」の「●検査オプション」を参照してください。

6 [インストール] ボタンをクリックします。

詳細な設定を行いインストールしたい場合は、[詳細設定] ボタンをクリックします。手順は「2.3 詳細インストール」へ進みます。

7 インストール完了までお待ちください。



ワンポイント

「ユーザーアカウント制御」画面が表示された場合は、[はい] ボタンをクリックします。

続く

8 [完了] ボタンをクリックします。

9 「製品のアクティベーション」画面が表示されます。「2.4 アクティベーション」へ進みます。

ワンポイント

ESET Endpoint Security を旧バージョンから上書きインストールした場合は、手順 8 の後にコンピューターの再起動を促すダイアログボックスが表示されます。この画面が表示されたときは、[今すぐ再起動] をクリックしてコンピューターの再起動を行ってください。すぐに再起動を行わない場合は、[後で通知する] をクリックして、後で再起動を行ってください。

2.3 詳細インストール

詳細インストールは、プログラムを微調整した経験があるユーザーや、インストール時に詳細設定を変更したいユーザーを対象としています。

操作手順

「2.2 標準インストール」手順④の続き

1 ［詳細設定］ボタンをクリックします。

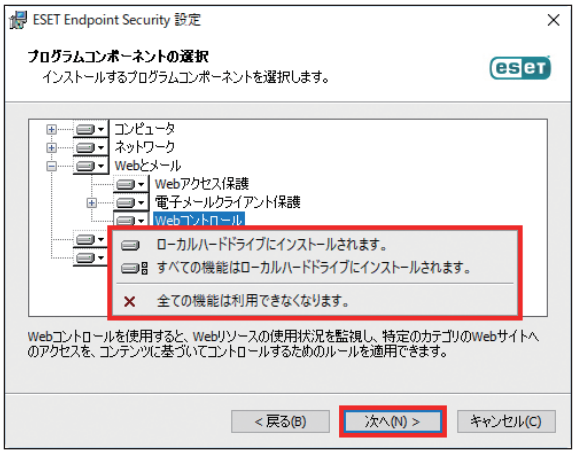
2 インストールするフォルダーを変更する場合は、「製品フォルダ」、「モジュールフォルダ」、「データフォルダ」の［参照］ボタンをクリックしインストールするフォルダーを指定します。（特別な理由がない場合は推奨しません）変更をしない場合はそのまま［次へ］ボタンをクリックします。

続く

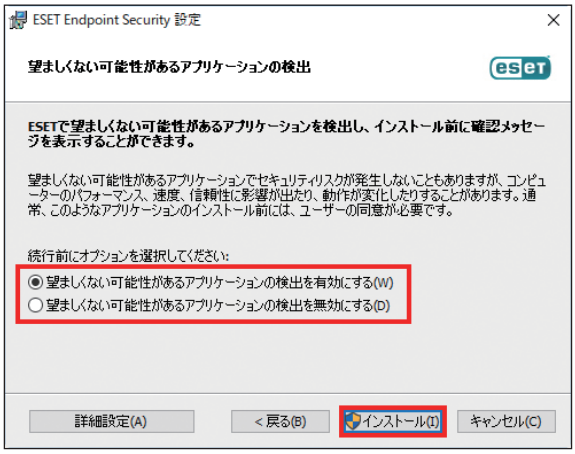
❸ プログラムコンポーネントの選択を行い［次へ］ボタンをクリックします。

コンポーネントツリーを展開して機能を選択すると、3 つのインストールオプションが表示されます。

「ローカルハードドライブにインストールされます。」	既定で選択されています。
「すべての機能はローカルハードドライブにインストールされます。」	選択済みのツリーの下にすべての機能がインストールされます。
「全ての機能は利用できなくなります。」	機能やコンポーネントを使用できなくなります。



❹ 望ましくない可能性があるアプリケーションの検出有無を選択します。



ワンポイント

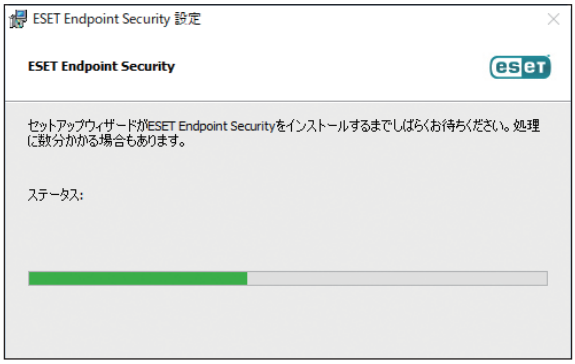
望ましくない可能性があるアプリケーションの検出の詳細は「4.6.2　リアルタイムファイルシステム保護」の「●検査オプション」を参照してください。

続く

5 [インストール] ボタンをクリックします。

詳細な設定を行いインストールしたい場合は、[詳細設定] ボタンをクリックします。手順は「2.3 詳細インストール」へ進みます。

6 インストール完了までお待ちください。



ワンポイント

「ユーザーアカウント制御」画面が表示された場合は、[はい] ボタンをクリックします。

7 [完了] ボタンをクリックします。

「製品のアクティベーション」画面が表示されます。「2.4 アクティベーション」へ進みます。

ワンポイント

ESET Endpoint Security を旧バージョンから上書きインストールした場合は、手順 7 の後にコンピューターの再起動を促すダイアログボックスが表示されます。この画面が表示されたときは、[今すぐ再起動] をクリックしてコンピューターの再起動を行ってください。

2.4 アクティベーション

インストール完了後に、「製品のアクティベーション」画面が表示されます。
アクティベーションには次の 3 つの方法がありますが、日本では製品認証キーを使用してアクティベーションします。

・製品認証キーを使用してアクティベーション：事前に入手した製品認証キーを入力する。
・ESET ビジネスアカウント：日本では使用しません。
・オフラインライセンス：ユーザーズサイトからダウンロードします。

ワンポイント

管理者が ESET Security Management Center の「製品のアクティベーション」タスクにより、リモートから製品認証キーを ESET Endpoint Security に適用しアクティベーションすることができます。詳細は『ESET Security Management Center ユーザーズマニュアル』の「8.8.17　製品のアクティベーション」を参照してください。

! 重　要

本製品は、アクティベーションを行わないと、検出エンジンの更新を行えないほか、製品の多くの機能を利用できません。必ずアクティベーションを実施してください。

2.4.1 製品認証キーを使用してアクティベーション

! 重　要

製品認証キーを使用して、アクティベーションするためにはコンピューターが ESET 社のライセンスサーバーに HTTPS で接続できる環境が必要です。

操作手順

1 ［購入した製品認証キーを使用］をクリックします。

続く

2 製品認証キーを入力して［続行］ボタンをクリックします。

製品認証キーを使用してアクティベーションするためには、コンピューターが ESET 社のライセンスサーバーに HTTPS で接続できる環境が必要です。
必要に応じて、プロキシサーバーの設定を行います。
プロキシサーバーの設定手順は「3.4 プロキシサーバーの設定」を参照してください。

3 ユーザーアカウント制御画面が表示されたときは［はい］または［続行］ボタンをクリックします。

4 アクティベーションが行われます。

5 アクティベーションが完了したら、［完了］ボタンをクリックします。

ワンポイント

任意のタイミングで製品ライセンスを変更するには、メインメニューの［ヘルプとサポート］をクリックします。カスタマーサポートに問い合わせる際に、ライセンスを識別するために必要になるライセンス ID が表示されます。

2.4.2 オフラインライセンスファイルを使用してアクティベーション

! 重 要

インターネット接続が行えないコンピューターのアクティベーションを行うには、「オフラインライセンスファイル」が必要になります。オフラインライセンスファイルは、弊社ユーザーズサイトからダウンロードできます。ダウンロードしたオフラインライセンスファイルは、アクティベーションを行うコンピューターで読み出せるようにしておいてください。

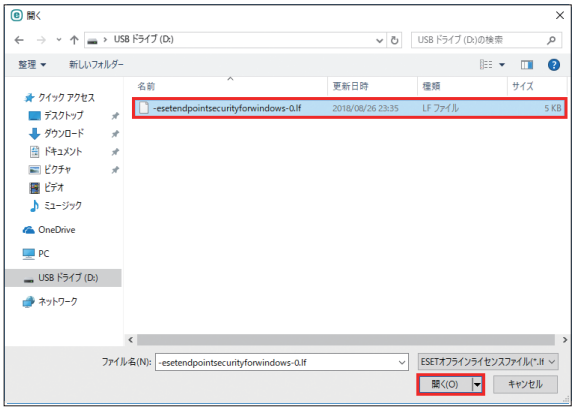
操作手順

1. オフラインライセンスファイルをコンピューターで読み出せる状態にします。
2. ESET Endpoint Security のメイン画面で［ヘルプとサポート］をクリックします。
3. ［製品のアクティベーション］ボタンをクリックします。

4. ［オフラインライセンス］をクリックします。

続く

5 オフラインライセンスファイルをクリックし、［開く］ボタンをクリックします。



6 ユーザーアカウント制御画面が表示されたときは［はい］または［続行］をクリックします。

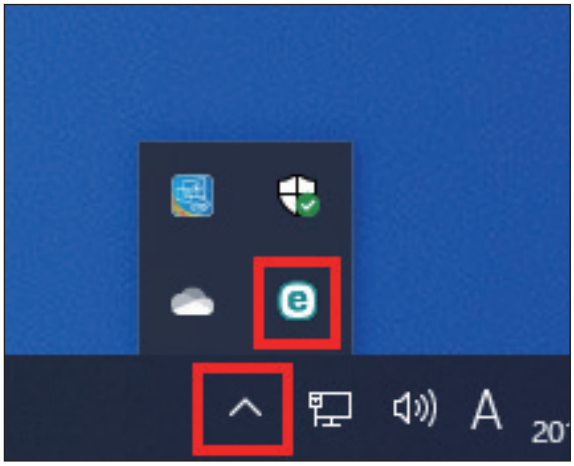
7 自動的にアクティベーションが完了します。［完了］ボタンをクリックします。

2.5 コンピューターの検査

インストール後の初回検査が有効になっている場合は、インストール、アップデートの完了後に自動的にコンピューターの初回検査が実行されます。初回検査の他に、コンピューターの検査を実行することを推奨しています。ESET Endpoint Security を起動して「コンピューターの検査」から検査を行います。

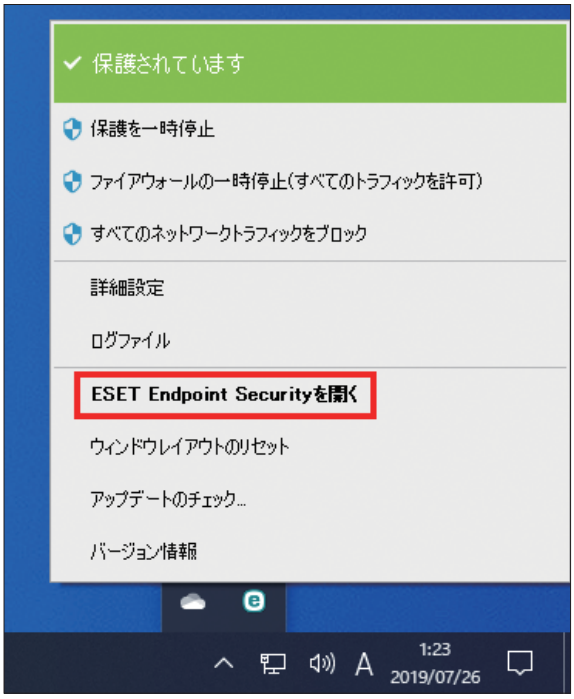
操作手順

1 通知領域のアイコンを右クリックします。



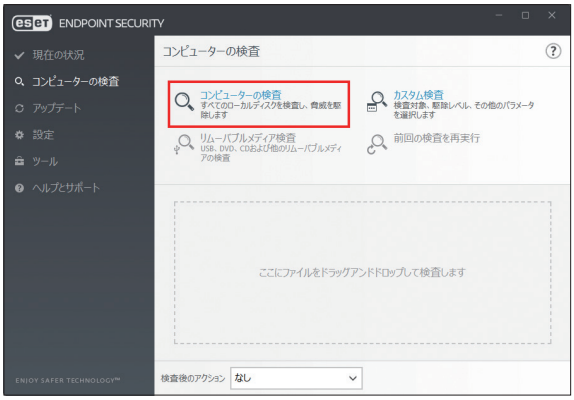
ワンポイント
通知領域にアイコンが表示されていない場合は［隠れているインジケーターを表示します］ボタンからアイコンを右クリックします。

2 ［ESET Endpoint Security を開く］をクリックします。



続く

3 ［コンピューターの検査］をクリックし、［コンピューターの検査］をクリックします。



2.6　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アップデートで解決できない問題の、修正や改良を行うために、ESET Endpoint Security の新バージョンが提供されています。最新バージョンへのアップグレードには、次の 3 つの方法があります。

■手動で最新バージョンをダウンロードし、以前のバージョンに上書きする

最新バージョンのインストーラーをダウンロードして、インストーラーを実行します。詳細な手順については、「2.1　インストール手順」を参照してください。

■ ESET Security Management Center 経由のネットワーク環境で自動展開する

ESET Security Management Center のクライアントタスクにある、「ソフトウェアインストール」を使用して最新バージョンを上書きインストールします。詳細は『ESET Security Management Center ユーザーズマニュアル』の「8.8.15 ソフトウェアインストール」または、「7.3.2.10　製品インストール」を参照してください。

■インターネットから自動で最新バージョンへアップグレードする

ESET 社のアップデートサーバーに最新バージョンへのアップデートファイルが使用可能になった場合に、ESET Endpoint Security はインターネットからそのファイルをダウンロードして、プログラムのバージョンアップを実行します。詳細な手順については、「4.6.6　アップデート」の「プログラムコンポーネントのアップデート」を参照してください。

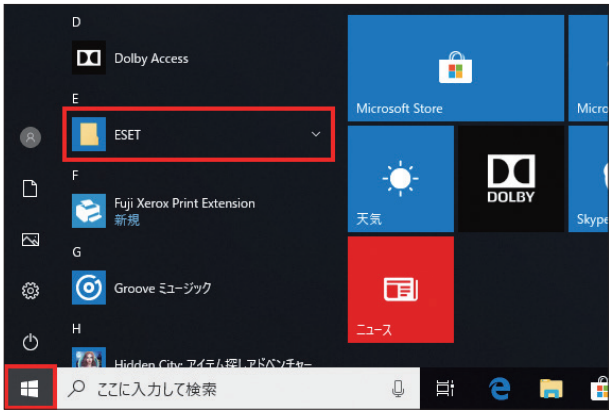
2.7 アンインストール

ESET Endpoint Security のアンインストール方法を説明します。

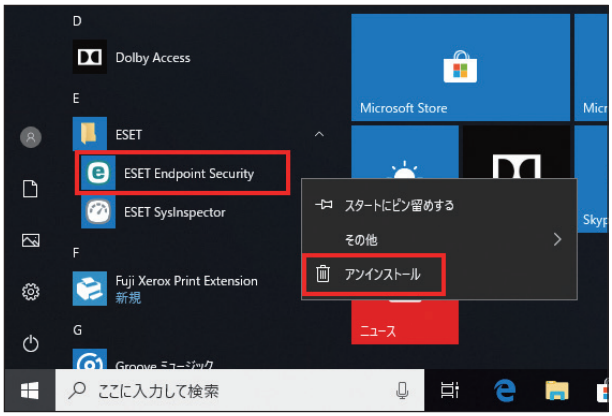
■ Windows 10 の場合

操作手順

1 ［スタート］ボタンをクリックし、［ESET］をクリックします。



2 ［ESET Endpoint Security］を右クリックし、［アンインストール］をクリックします。

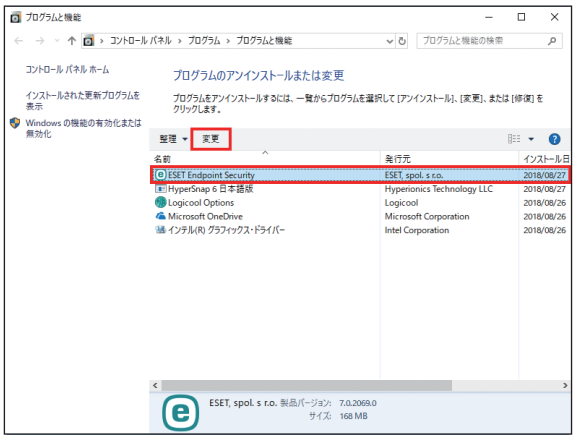


ワンポイント

Windows 8.1 Update を利用している場合は、スタート画面からすべてのアプリを表示し、［ESET Endpoint Security］を右クリックし、［アンインストール］をクリックすると、P.26 の手順③の画面が表示されます。

続く

3 ［プログラムと機能］が表示されます。［ESET Endpoint Security］をクリックし、［変更］をクリックします。



4 セットアップウィザードが起動します。［次へ］ボタンをクリックします。

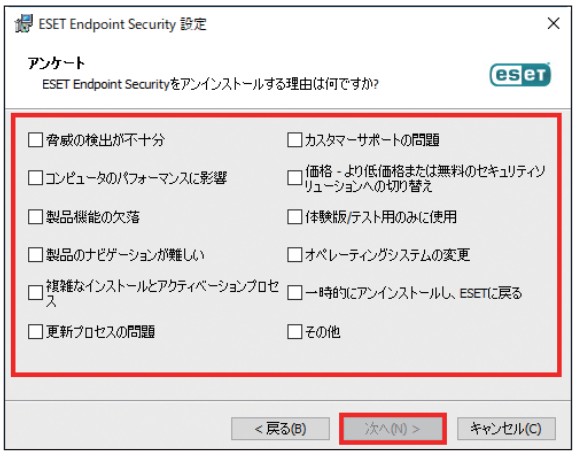
ワンポイント

設定をパスワードで保護している場合、パスワードの入力を求められます。

5 ［削除］ボタンをクリックします。

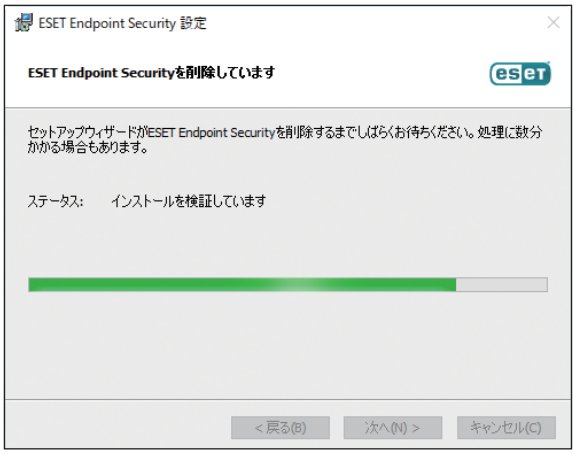
続く

6 「アンケート」画面が表示されますので、アンインストールする理由にチェックを入れ、［次へ］ボタンをクリックします。



7 ［削除］ボタンをクリックします。

8 「削除をしています」画面が表示されます。完了までお待ちください。



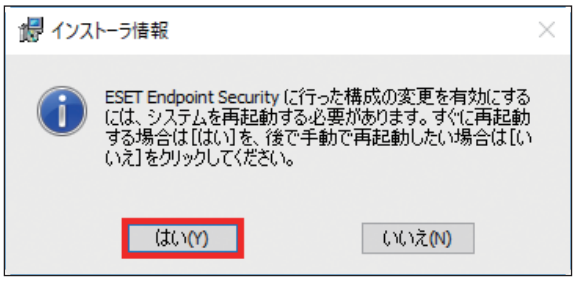
ワンポイント

「ユーザーアカウント制御」画面が表示された場合は、［はい］ボタンをクリックします。

続く

9 「ESET Endpoint Security セットアップウィザードを完了しています」と表示されたら、アンインストールは完了です。［完了］ボタンをクリックします。

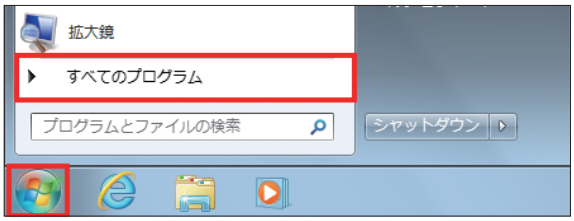
10 ［はい］ボタンをクリックするとコンピューターが再起動されます。［いいえ］ボタンをクリックしたときは、コンピューターを手動で再起動してください。



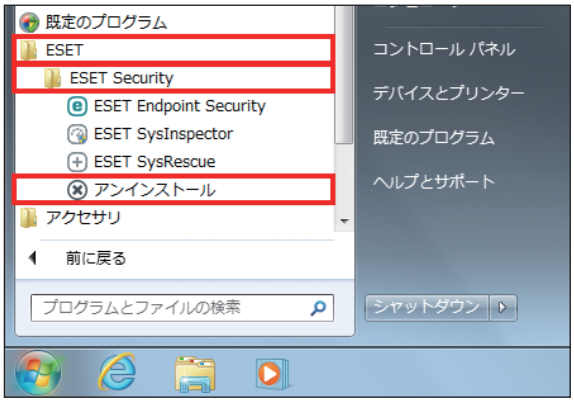
■ Windows 7 の場合

操作手順

1 ［スタート］ボタンをクリックし、［すべてのプログラム］を選択します。



2 ［ESET］を選択し、［ESET Endpoint Security］の［アンインストール］をクリックします。



3 セットアップウィザードが起動します。［次へ］ボタンをクリックします。

ワンポイント

設定をパスワードで保護している場合、パスワードの入力を求められます。

続く

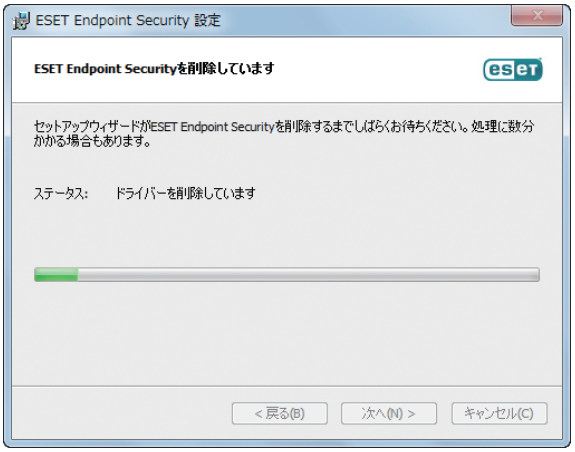
4 ［削除］ボタンをクリックします。

5 「アンケート」画面が表示されますので、アンインストールする理由にチェックを入れ、［次へ］ボタンをクリックします。

6 ［削除］ボタンをクリックします。

続く

7 「削除をしています」画面が表示されます。完了までお待ちください。

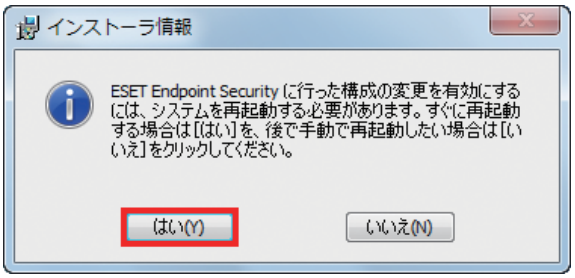


ワンポイント

「ユーザーアカウント制御」画面が表示された場合は、［はい］ボタンをクリックします。

8 「ESET Endpoint Security セットアップウィザードを完了しています」と表示されたら、アンインストールは完了です。［完了］ボタンをクリックします。

9 ［はい］ボタンをクリックするとコンピューターが再起動されます。
［いいえ］ボタンをクリックしたときは、コンピューターを手動で再起動してください。



Chapter 3 ご利用開始時の確認・設定事項

3.1 画面構成

ESET Endpoint Security のメイン画面は、各メニューが並んでいる「メインメニュー」とメインメニューで選択された機能が表示される「プライマリウインドウ」に分かれています。

■各メニューについて

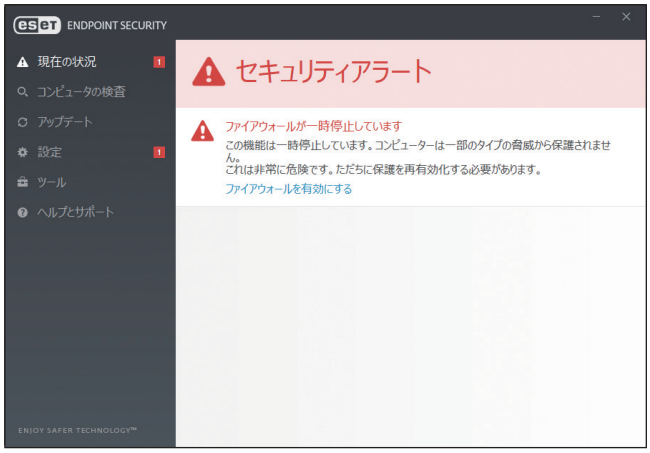
現在の状況	保護の状態、ライセンス有効期限が確認できます。
コンピューターの検査	スマート検査、カスタム検査、リムーバブルメディア検査、前回の検査の再実行が行えます。
アップデート	検出エンジンのアップデートに関する情報が表示されます。
設定	コンピューター、ネットワーク、Web とメールの設定を確認、変更することができます。
ツール	[ログファイル]、[実行中のプロセス]、[セキュリティレポート]、[アクティビティの確認]、[ネットワーク接続]、[ESET SysInspector]、[スケジューラ]、[ESET SysRescue Live]、[隔離] にアクセスできます。分析のためにサンプルを送信することもできます。
ヘルプとサポート	ヘルプファイル、製品ホームページの FAQ、ESET の Web サイトのリンクを利用できます。また、カスタマーサポート、サポートツール、製品アクティベーションへのリンクも利用できます。

3.2 保護状態の確認

「現在の状況」画面には、利用しているコンピューターのセキュリティと現在の保護レベルが表示されています。各モジュールが正しく動作している場合は、緑色の表示になります。正しく動作していない場合は、赤色もしくは黄色の表示になり問題、注意の内容が表示されます。モジュールを修正するための推奨される解決策が表示されますので内容を確認してください。各モジュールの設定を変更するにはメインメニューの［設定］から行えます。

緑色の表示は「最も高い保護」の状態を示しています。各機能が正しく動作しています。

赤色の表示は「保護に重大な問題」があることを示しています。



主な理由

- リアルタイムファイルシステム保護が無効になっている
- ファイアウォールが一時停止している
- 検出エンジンが最新でない
- 製品のライセンスの有効期限が切れている
- フィッシング対策保護が機能していない

■主な解決策

リアルタイムファイルシステム保護が一時停止しています	「リアルタイムファイルシステム保護」が無効になっています。[設定]メニューの［リアルタイムファイルシステム保護］をクリックして有効にします。
ファイアウォールが一時停止しています	「ファイアウォール」が無効になっています。［設定］メニューの［ネットワーク］タブより、［ファイアウォール］をクリックして有効にします。
ライセンスが期限切れです	ライセンスの有効期限が過ぎると、検出エンジンのアップデートができません。警告ウインドウの指示に従ってライセンスの更新を行ってください。

黄色の表示は「注意が必要」な状態を示しています。

主な理由

・電子メールクライアント保護または迷惑メール対策機能が一時停止になっている
・アップデートに関する問題がある（検出エンジンが期限切れになっている）
・ライセンスの有効期限がせまっている

■主な解決策

電子メールクライアント保護が一時停止しています	「電子メールクライアント」が一時停止しています。［設定］メニューの［Webとメール］タブより、［電子メールクライアント保護］をクリックして有効にします。
ライセンスは間もなく有効期限切れとなります	ライセンスの有効期限が切れると、検出エンジンのアップデートができなくなります。ライセンスの更新を行ってください。

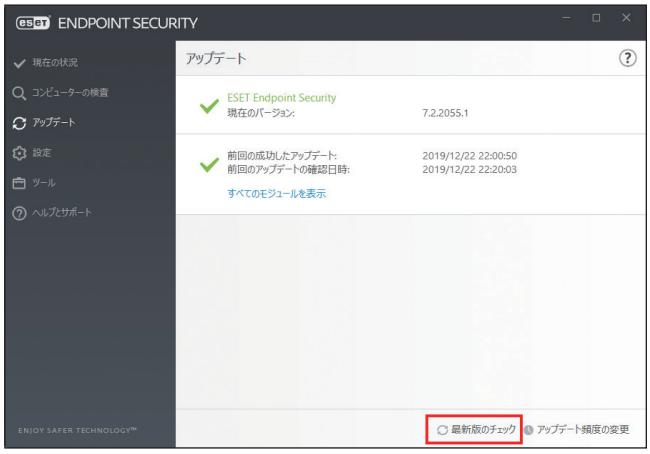
提示された解決策を使用して問題が解決されない場合は、[ヘルプとサポート］をクリックしてヘルプ情報を確認するか、製品ホームページの FAQ を参照してください。それでも解決されない場合は、サポートセンターへご連絡ください。

製品ホームページの FAQ

https://eset-support.canon-its.jp/?site_domain=business

3.3 アップデートの設定

検出エンジンのアップデートとプログラムコンポーネントのアップデートは、悪意のあるコードからコンピューターを保護するための重要な作業です。メインメニューから［アップデート］メニューを選択し、［最新版のチェック］をクリックして、最新の検出エンジンを確認します。
ESET Endpoint Security のインストール作業中に、アクティベーションを行わなかった場合、「アクティベート」画面が表示されますのでアクティベーションを行ってください。



アップデートに関する設定は、「詳細設定」画面で確認、変更することができます。

操作手順

1 メインメニューの［設定］メニューから［詳細設定］をクリックします。

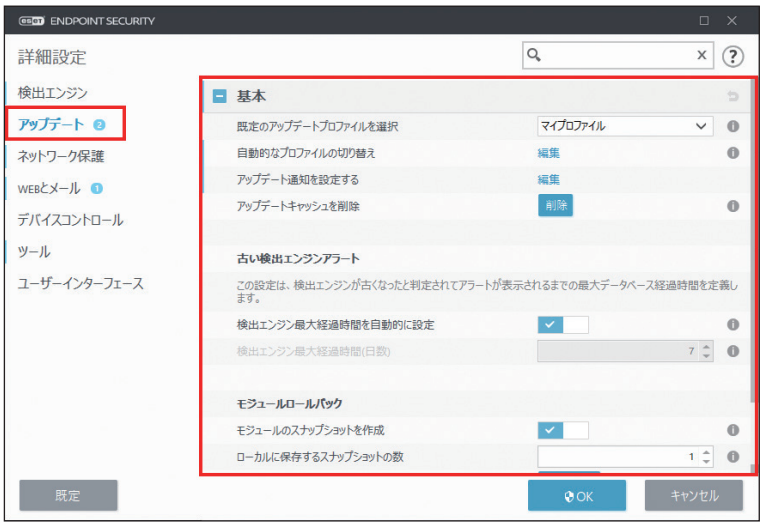
ワンポイント

キーボードの【F5】キーを押して「詳細設定」画面を表示させることもできます。

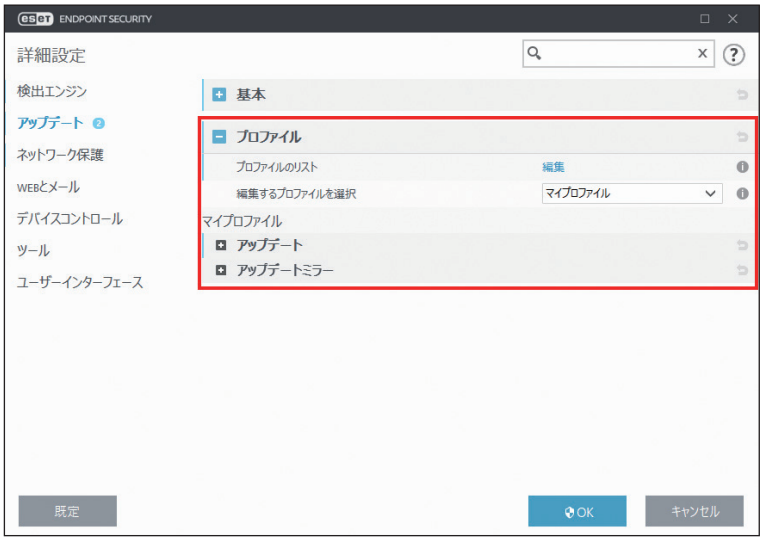
続く

2 ［アップデート］をクリックします。

「基本」セクションでは、既定のアップデートプロファイルの選択やアップデートキャッシュの削除、古い検出エンジンアラート、モジュールロールバックの設定を行えます。更新時に問題が発生した場合、［アップデートキャッシュを削除］の［削除］をクリックすると一時アップデートキャッシュが削除されます。



［プロファイル］をクリックすると、選択したプロファイルの詳細な設定を行えます。［アップデート］をクリックすると、アップデートの種類やモジュールアップデートに利用するアップデートサーバーの設定、プロキシサーバーの設定を行う接続オプションなどの設定を行えます。また、［アップデートミラー］をクリックすると、アップデートミラーの作成に関する設定を行えます。



3.4 プロキシサーバーの設定

インターネット接続を制御するためにプロキシサーバーを使用している場合は、「詳細設定」画面で「プロキシサーバー」（IP アドレス）と「ポート」の設定をします。

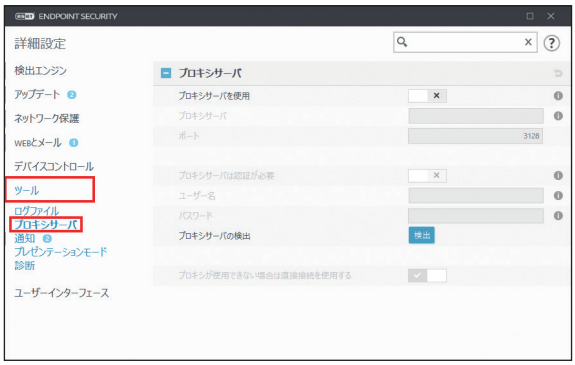
操作手順

1 メインメニューの［設定］メニューから［詳細設定］をクリックします。

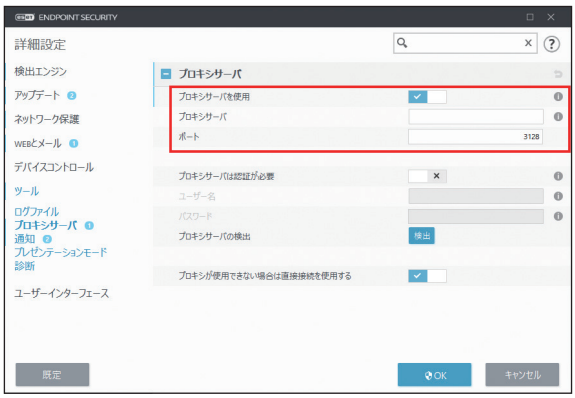
ワンポイント

キーボードの【F5】キーを押して「詳細設定」画面を表示させることもできます。

2 ［ツール］をクリックし、［プロキシサーバ］をクリックします。



3 「プロキシサーバを使用」オプションを選択して、「プロキシサーバー」（IP アドレスまたは URL）、「ポート」を入力します。



ワンポイント

アップデートプロファイルごとにプロキシサーバーのオプションが設定可能です。必要に応じて、「詳細設定」画面のアップデートから設定します。

3.5 設定の保護

ESET Endpoint Security の設定は、セキュリティポリシーの観点から、非常に重要になります。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。許可なく変更されるのを防ぐために、プログラムの設定を、パスワードで保護することができます。

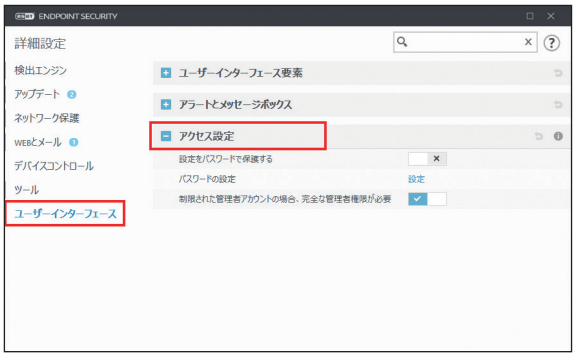
操作手順

1 メインメニューの［設定］メニューから［詳細設定］をクリックします。

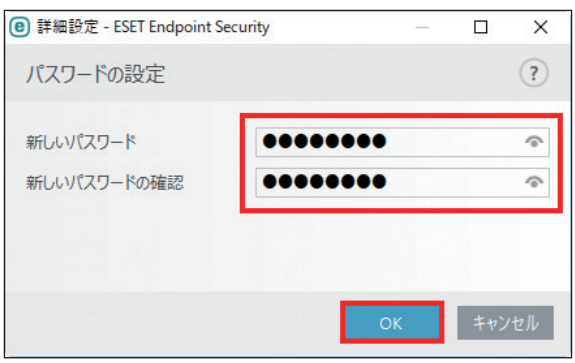
ワンポイント

キーボードの【F5】キーを押して「詳細設定」画面を表示させることもできます。

2 ［ユーザーインターフェース］をクリックし、［アクセス設定］をクリックして、「設定をパスワードで保護する」オプションを選択します。



3 「新しいパスワード」と「パスワードの確認」に同じパスワードを入力して［OK］ボタンをクリックします。

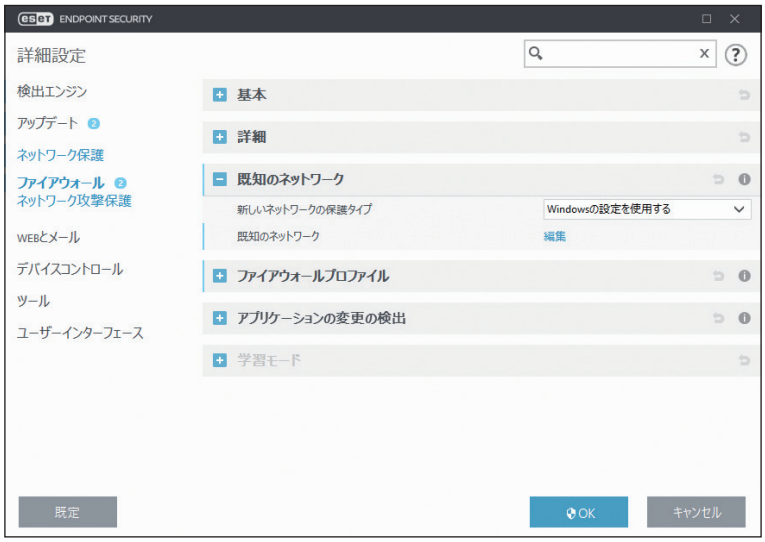


ワンポイント

設定したパスワードは、ESET Endpoint Security の設定を変更する場合に必要になります。

3.6 信頼ゾーンの設定

ネットワーク環境でコンピューターを保護するには、信頼ゾーンを設定する必要があります。信頼ゾーンを設定して共有を許可すると、他のユーザーに自分のコンピューターへのアクセスを許可できます。
信頼ゾーンの検出は、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実行されます。既定では、Windows の設定が利用され、通常は、信頼ゾーンを定義する必要はありません。「信頼ゾーンの設定」画面は、「詳細設定」画面を表示し、［ネットワーク保護］>［ファイアウォール］>［既知のネットワーク］で表示できます。



! 重 要

信頼済みゾーンを誤って設定すると、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。

ワンポイント

既定では、信頼済みゾーン内のコンピューターは共有ファイルおよびプリンターへのアクセスが許可されており、受信 RPC 通信が有効です。さらに、リモートデスクトップの共有も可能です。

3.7 ESET Security Management Center との接続

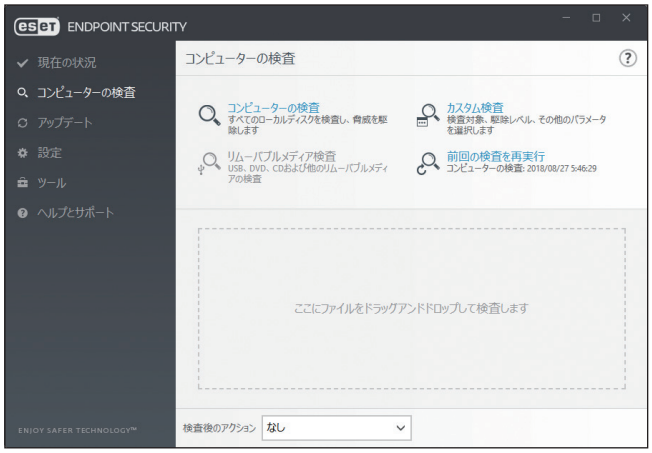
ESET Security Management Center はネットワーク環境にある ESET 製品を管理できるアプリケーションです。ESET Security Management Center は「ESET Management エージェント」経由で ESET Endpoint Security との通信を行います。ESET Security Management Center との通信を行うには、「ESET Management エージェント」のインストールが必要です。「ESET Management エージェント」のインストールについては『ESET Security Management Center ユーザーズマニュアル』の「7.3　エージェントの展開」を参照してください。

Chapter 4 ESET Endpoint Security の使い方

この章では、コンピューターの検査、ESET Endpoint Security の設定、ツール類の使い方について説明します。

4.1 コンピューターの検査

「コンピュータの検査」メニューでは、コンピューター上のファイルやフォルダーの検査を実施します。感染が疑われるときだけコンピューターの検査を実行するのではなく、通常のセキュリティ対策の一環として定期的（1 か月に 1 回など）に実行することが重要です。
検査を行うと、「リアルタイムファイルシステム保護」が無効に設定されている場合、検出エンジンが古い場合、ファイルをディスクに保存したときにウイルスが検出されなかった場合など、リアルタイムに検出されなかったウイルスを検出することができます。
「コンピュータの検査」メニューには、コンピューターの検査、カスタム検査、リムーバブルメディア検査の 3 種類があります。リアルタイムファイルシステム保護については「4.3.1 コンピュータ」を参照してください。

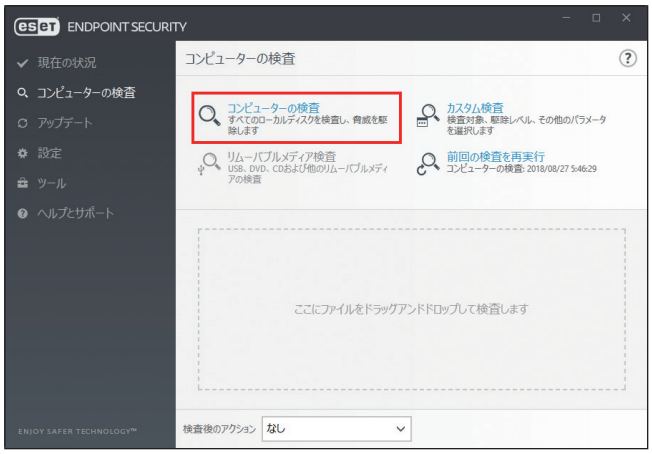


！重 要

検査は最低でも 1 か月に 1 回は実行することをお勧めします。メインメニューの［ツール］>［スケジューラ］で、コンピューターの検査をタスクとして設定できます。設定方法については「4.4.7 スケジューラ」を参照してください。

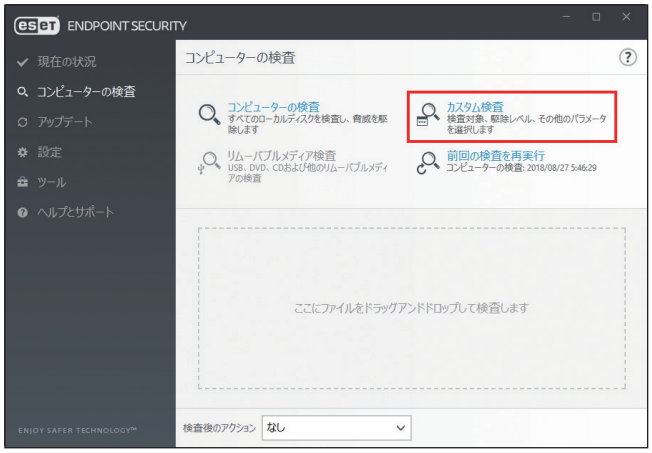
4.1.1 コンピューターの検査

コンピューターの検査は、コンピューターの検査を行い、感染しているファイルからウイルスを自動的に駆除します。「コンピューターの検査」をクリックするだけで、詳細な検査パラメーターの設定を行うことなく、ローカルドライブにあるすべてのファイル検査が実行されます。駆除レベルは既定で設定されていますが、変更することができます。駆除レベルについては、「4.6.2 リアルタイムファイルシステム保護」の「●駆除」を参照してください。



4.1.2 カスタム検査

カスタム検査は、検査対象や検査方法など検査パラメーターを指定する検査方法です。
カスタム検査は、ウイルス対策プログラムを使用した経験のある上級ユーザー向けです。



■カスタム検査の設定

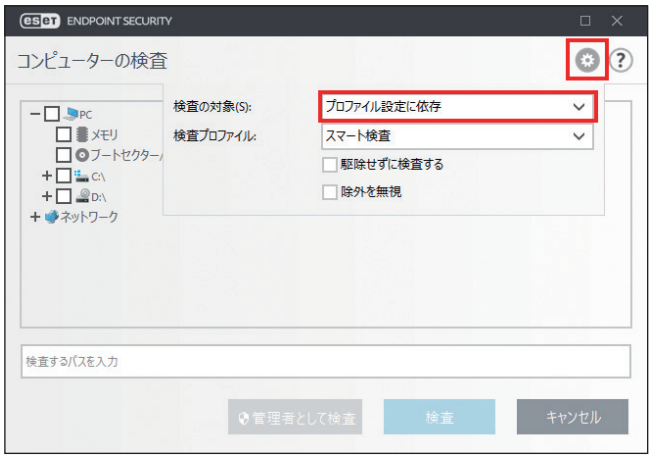
［カスタム検査］をクリックすると、「コンピューターの検査」画面が表示されます。

●検査の対象の選択

検査の対象は、次の 3 つの方法で選択できます。

事前定義されている検査対象を選択する

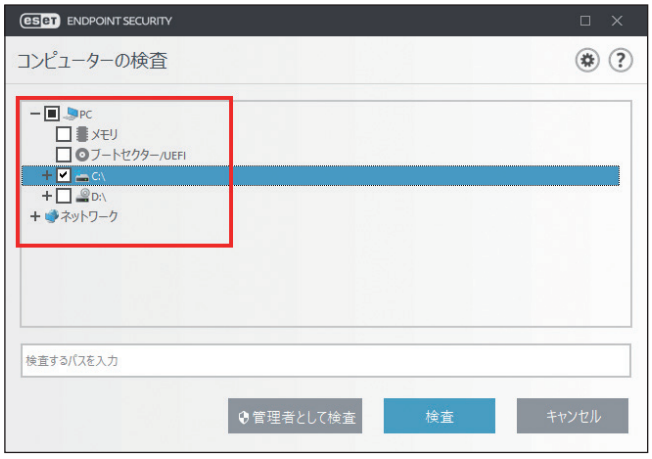
⚙をクリックして [検査の対象] ドロップダウンメニューからオプションを選択します。



プロファイル設定に依存	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 メモリー、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。
選択なし	すべての選択をキャンセルします。

検査対象ウィンドウのフォルダーツリー構造から選択する

検査対象ウィンドウのフォルダーツリー構造から、検査を行いたいフォルダーやドライブなどを選択します。

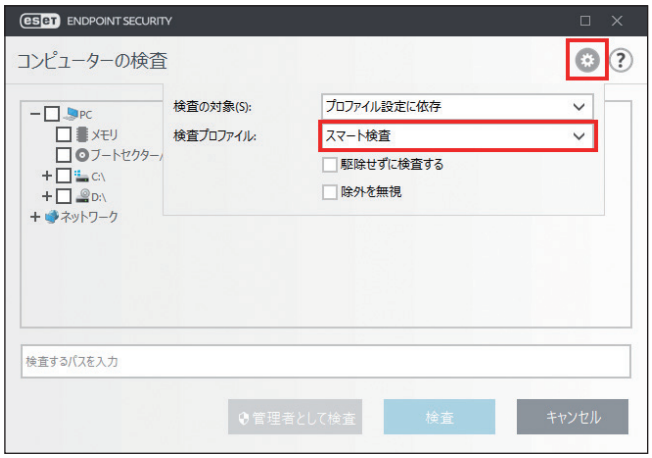


検査対象を直接指定する

検査対象ウィンドウのフォルダーツリー構造下の空白フィールドに検査を行いたいパスを直接入力します。この方法は、検査対象ウィンドウのフォルダーツリー構造内で対象を選択しておらず、かつ［検査の対象］ドロップダウンメニューで［選択なし］を選択している場合のみ利用できます。

●検査プロファイルの選択

選択した対象の検査に使用するプロファイルを、[検査プロファイル] ドロップダウンメニューから選択できます。⚙をクリックするとメニューが表示され、[検査プロファイル] ドロップダウンメニューを表示できます。既定のプロファイルは、[スマート検査] です。[詳細検査] と [コンテキストメニュー検査] の 2 つの事前定義された検査プロファイルも用意されています。検査プロファイルの詳細な設定は、［詳細設定］画面の［コンピューターの検査］の［THREATSENSE パラメータ］で行えます。使用可能なオプションについては、「4.6.2　リアルタイムファイルシステム保護」の「■ THREATSENSE パラメータ」を参照してください。



●駆除せずに検査する

⚙をクリックし、［駆除せずに検査する］にチェックを入れると、感染しているファイルやフォルダーを検出したときに、これらが自動的に駆除されず、現在の保護状態の概要が表示されます。

●除外を無視

⚙をクリックし、［除外を無視］にチェックを入れると、検査対象外として指定されたファイル拡張子を含めて検査を実行します。

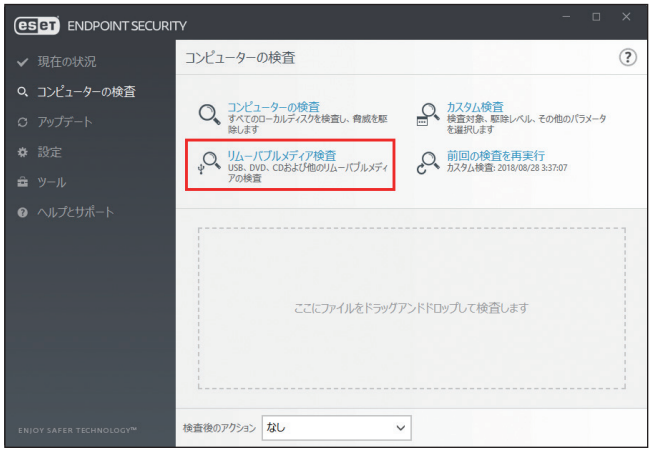
●検査の実行

検査を実行するときは、[検査] または [管理者として検査] をクリックします。[検査] をクリックすると、設定したカスタムパラメーターを利用して検査を実行します。[管理者として検査] をクリックすると、管理者アカウントで検査を実行できます。検査対象のファイルにアクセスするための権限がないユーザーでログインしている場合は、[管理者として検査] をクリックします。なお、現在ログインしているユーザーが管理者としてユーザアカウント制御を呼び出せない場合、[管理者として検査] は使用できません。

4.1.3 リムーバブルメディア検査

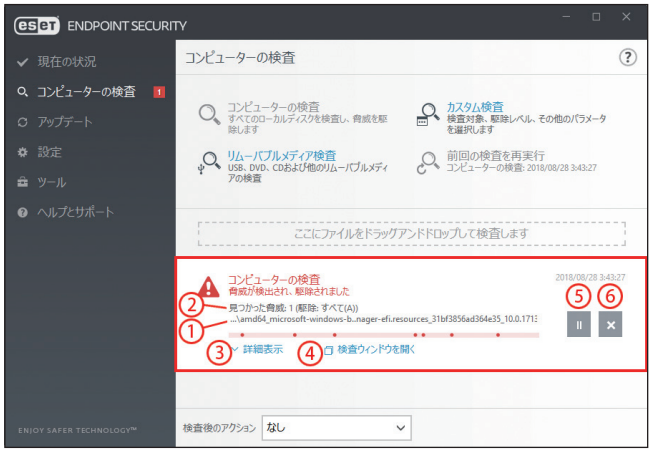
コンピューターに接続されているリムーバブルメディア（CD/DVD/USB メモリーなど）を、コンピューターの検査と同じように検査します。「リムーバブルメディア検査」は、USB メモリーをコンピューターに接続し、マルウェアや他の潜在的な脅威の存在を検査したいときに便利です。

リムーバブルメディア検査は、[カスタム検査] をクリックし、⚙をクリックして [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] をクリックして実行することもできます。



4.1.4 検査の進行状況

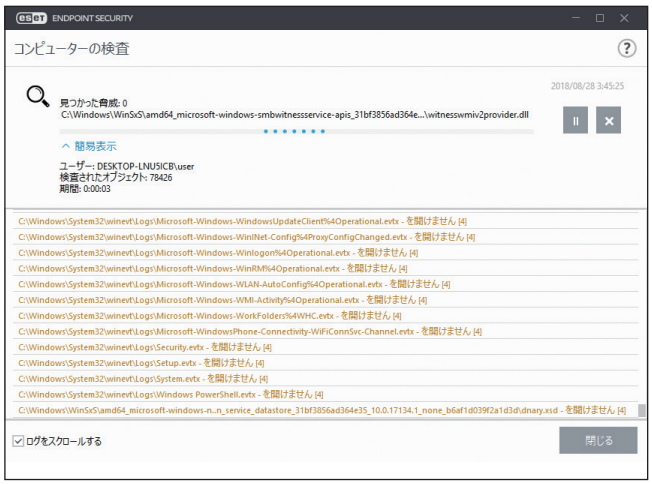
検査の実行中は、検査の現状および悪意のあるコードを含むファイルの数に関する情報が表示されます。また、[検査ウィンドウを開く] をクリックすると、検査の進行状況を表示する検査ウィンドウを表示します。



①対象	現在検査している対象の名前と保存場所が表示されます。
②見つかった脅威	検出された脅威の総数が表示されます。
③詳細表示	検査を行っているユーザー名、検査されたオブジェクトの数、検査時間などの情報を表示します。［簡易表示］をクリックすると、元の表示に戻ります。［簡易表示］は、詳細表示を行っている場合に表示されます。
④検査ウィンドウを開く	検査の進行状況を表示する検査ウィンドウを表示します。
⑤中断	検査を中断します。［再開］をクリックすると、検査を続行します。［再開］は、検査を中断した場合に表示されます。
⑥中止	検査を中止します。

●検査ウィンドウ

検査ウィンドウには、検査の現状および悪意のあるコードを含むファイルの数に関する情報や検査ログが表示されます。



! 重　要

パスワードで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ませんが、エラーではありません。

対象	現在検査している対象の名前と保存場所が表示されます。
見つかった脅威	検出された脅威の総数が表示されます。
中断	検査を中断します。
再開	検査を続行します。［再開］は検査を中断した場合に表示されます。
中止	検査を終了します。
ログをスクロールする	チェックすると、新しいエントリーが追加されるたびに検査ログが自動的にスクロールします。

4.2 アップデート

コンピューターのセキュリティを最大限確保するには、ESET Endpoint Security を定期的にアップデートするのが最善の方法です。ESET Endpoint Security は検出エンジンのアップデートとシステムコンポーネントのアップデートという 2 つの方法で、常に最新の状態を保つことができます。

メインメニューの [アップデート] をクリックすると、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確認できます。また、[すべてのモジュールを表示] をクリックすると、インストールされたモジュールのリストが表示され、モジュールのバージョンと最後のアップデートを確認できます。
また、[最新版のチェック] をクリックすると、アップデートを手動で開始できます。既定では、1 時間ごとに自動的にアップデートが実行されるタスクが登録されています。間隔を変更するには、メインメニューの [ツール] > [スケジューラ] をクリックします。スケジューラの詳細については、「4.4.7 スケジューラ」を参照してください。

①現在のバージョン	ESET Endpoint Security のビルド番号。
②前回の成功したアップデート	最終更新日時。検出エンジンが最新、つまり最近の日付になっていることを確認してください。
③前回のアップデートの確認日時	モジュールのアップデートを最後に試行した日時。
④すべてのモジュールを表示	クリックすると、インストールされたモジュールのリストを開き、モジュールのバージョンと最後のアップデート日時を確認できます。

! 重 要

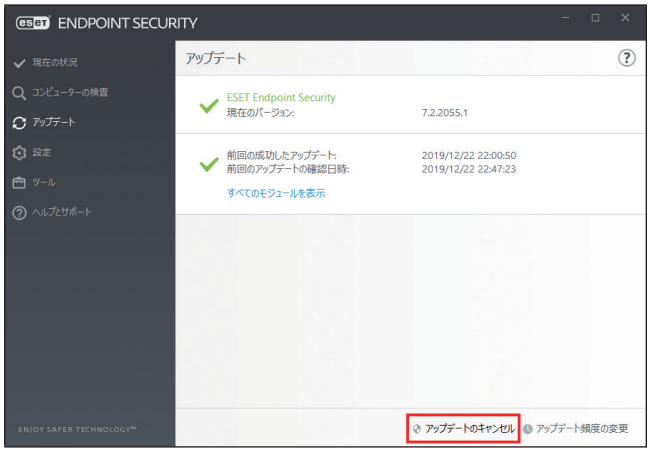
検出エンジンとプログラムコンポーネントのアップデートは、悪意のあるコードからコンピューターを保護するための重要な機能です。設定や操作には注意してください。

! 重 要

ESET Endpoint Security のインストール時にライセンスを入力しなかった場合は、[ヘルプとサポート] をクリックし、[製品のアクティベーション] をクリックして製品認証キーを入力すると、ESET のアップデートサーバーにアクセスすることができます。また、オフラインライセンスファイルで ESET Endpoint Security をアクティベートし、アップデートを試みる場合、赤色の情報「検出エンジンアップデートがエラー終了しました」が表示されたときは、ミラーサーバーからのみアップデートをダウンロードできます。

アップデートのプロセス

[最新版のチェック]をクリックすると、アップデートが始まります。アップデートの進行状況バーが表示されます。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。



! 重 要

検出エンジンは、通常 1 日に数回アップデートされます。前回のアップデートから 1 日以上経過している場合、プログラムが古くなっており、感染しやすくなっています。検出エンジンはできるだけ早くアップデートしてください。

アップデートの失敗

アップデートが正常に行われなかった場合は、次のメッセージが表示されます。

- **「検出エンジンは最新ではありません」**

検出エンジンのアップデートに複数回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。失敗の原因として最も多いのは、製品認証キーが正しく入力されていない、またはインターネット接続設定が適切ではないことです。

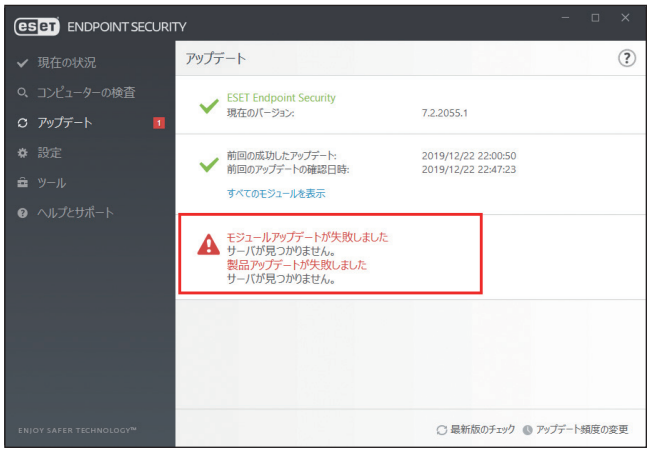
このメッセージは、アップデートの失敗に関する次の 2 つのメッセージ（モジュールアップデートが失敗しました）に関連します。

- **「モジュールアップデートが失敗しました - アクティベーションされていません。」**

アップデート設定で製品認証キーが正しく入力されていないため、ライセンスが無効になっています。製品認証キーを確認し、[ヘルプとサポート]をクリックして、[製品のアクティベーション]をクリックし、製品認証キーを入力してください。

- **「モジュールアップデートが失敗しました - サーバに接続できません。」**

インターネット接続の設定が正しくない可能性があります。Web ブラウザーで任意の Web サイトを表示するなどして、インターネット接続が正しく設定されているか確認してください。Web サイトが表示されない場合は、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ー（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。



4.3 設定

ESET Endpoint Security の設定オプションを使用すると、コンピューター、ネットワーク、Web とメールの各セクションの保護レベルを調整することができます。各セクションをクリックすると、対応する保護機能の詳細を設定できます。

4.3.1 コンピュータ

個別の機能を一時的に無効にするには、機能名の左側にある をクリックします。ただし、無効にすると、コンピューターのセキュリティレベルが低下する可能性がありますので注意してください。
無効な機能を再度有効にするには、 をクリックして に戻します。

リアルタイムファイルシステム保護	ファイルオープン、作成、実行時、悪意のあるコードがないか検査します。すべてのファイルが対象になります。
デバイスコントロール	USB メモリーや CD、DVD、USB 接続の HDD などのデバイスへのアクセスを制御するデバイスコントロールの有効／無効を設定します。
HIPS	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対処します。
アドバンストメモリスキャナー	エクスプロイトブロックとともに動作し、隠蔽や暗号化の使用によって、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。
エクスプロイトブロック	Web ブラウザー、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悪用される種類のアプリケーションを防御します。
ランサムウェアシールド	ランサムウェア保護は HIPS 機能の一部として動作し、ランサムウェアと疑わしき動作を検知して、ブロックすることでコンピューターを保護します。ランサムウェア保護を実行するには、LiveGrid 評価システムを有効にする必要があります。
プレゼンテーションモード	ソフトウェアを中断したくないとき、ポップアップウィンドウを表示させたくないとき、CPU の使用量を最小化したいときなどに使用します。プレゼンテーションモードを有効にすると、潜在的なセキュリティリスクが存在するため、メイン画面がオレンジ色になり、警告が表示されます。

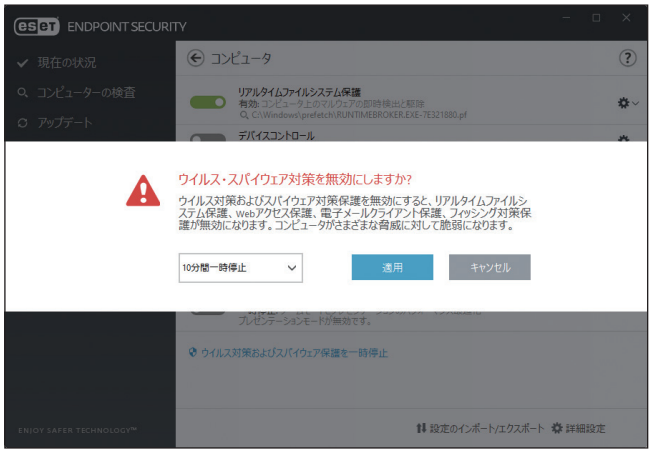
！重　要

をクリックして無効にした保護機能の多くは、コンピューターを再起動すると再度有効になります。
特定の機能の詳細設定を行うには、機能名の右側にある をクリックします。

●ウイルス対策およびスパイウェア保護を一時停止

ウイルス・スパイウェア対策の保護を一時的に無効にします。

［ウイルス対策およびスパイウェア保護を一時停止］をクリックすると、一時停止の設定画面が表示されます。



一時停止期間を選択して［適用］をクリックします。

4.3.2 ネットワーク

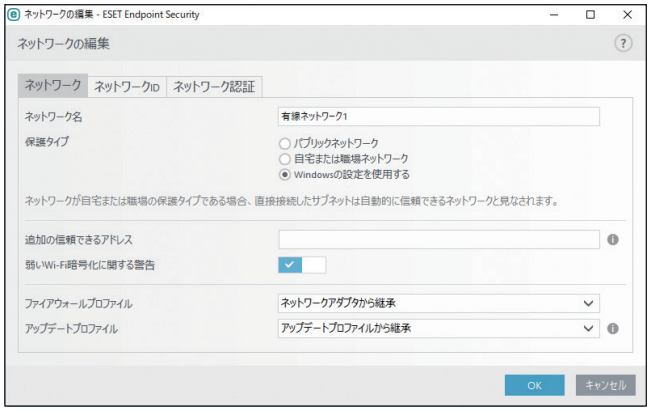
ファイアウォール	ファイアウォールのフィルタリングモードを調整できます。⚙ をクリックして動作を選択するか、［設定］を選択して詳細を設定することもできます。
ネットワーク攻撃保護（IDS）	ネットワークトラフィックの内容を分析して、ネットワーク攻撃から保護します。有害だと見なされるすべてのトラフィックがブロックされます。
ボットネット保護	コンピューターで実行中のソフトウェアによって送信されるネットワークトラフィックの内容を解析し、有害だとみなされるすべてのトラフィックがブロックされます。

■接続されたネットワーク

［接続されたネットワーク］をクリックすると、接続されたネットワークが表示されます。ネットワークに関するさまざまな設定を行えます。

・「ネットワークの編集」画面

⚙をクリックすると、「ネットワークの編集」画面が表示されます。「ネットワークの編集」画面では、選択したネットワークの接続に関するさまざまな設定を行えます。設定の詳細については「4.6.7　ネットワーク保護」の「■　既知のネットワーク」の「●既知のネットワークエディター」を参照してください。



・「ネットワーク接続の変更」画面

ネットワークの場所（[パブリックネットワーク］や［自宅または職場ネットワーク]）をクリックすると、「ネットワーク接続の変更」画面が表示され、ネットワークの種類を変更できます。

パブリックネットワーク	ファイルやフォルダーを共有せず、他のユーザーから参照できないようにするにはこの種別を選択します。
自宅 / 職場ネットワーク	共有を有効にして、他のユーザーがファイルやフォルダーにアクセスできるようにします。
詳細	接続中ネットワークのネットワークアドレスなどの詳細情報が表示されます。

・ネットワークアダプタ

各ネットワークアダプター、割り当てられたファイアウォールプロファイル、信頼ゾーンが表示されます。

［ネットワークアダプタ］をクリックすると検出されたネットワークアダプタの一覧が表示されます。

■一時 IP アドレスブラックリスト

攻撃元であると判断され、接続をブロックするためにブラックリストに追加されている IP アドレスの一覧が表示されます。

［一時 IP アドレスブラックリスト］をクリックするとリスト画面が表示されます。

リスト画面では次の操作ができます。

削除	選択した IP アドレスをリストから削除します。
すべて削除	すべての IP アドレスをリストから削除します。
例外の追加	選択した IP アドレスに対してファイアウォール例外を設定します。

■トラブルシューティングウィザード

ファイアウォールが原因となっている接続の問題を解決できます。詳細については、「4.6.7 ネットワーク保護」の「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。

4.3.3 Web とメール

Web コントロール	不適切または有害なコンテンツを含む、Web サイトへのアクセスをブロックします。また、システム管理者は、27 個の Web サイトカテゴリを使用して、アクセスをコントロールできます。
Web アクセス保護	HTTP または HTTPS 経由のすべての通信トラフィックで、悪意のあるソフトウェアを検査します。
電子メールクライアント保護	メールクライアントのプラグインプログラムとして動作し、送受信したメールを検査します。
迷惑メール対策機能	迷惑メールから保護します。
フィッシング対策機能	パスワード、金融データ、その他の機密データを収集する目的で偽装した、非合法の Web サイトへのアクセスをブロックします。

4.3.4 設定のインポート／エクスポート

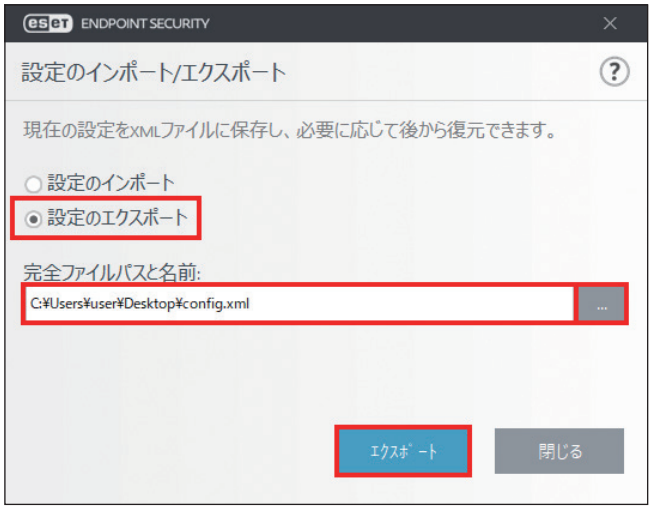
xml 形式のファイルを使用して、ESET Endpoint Security の設定をインポートまたはエクスポートできます。設定を後で復元できるように現在の設定をバックアップする場合や、同じ設定内容を複数のコンピューターに適用する場合などに便利です。

■設定のインポート

「設定」画面で［設定のインポート／エクスポート］＞［設定のインポート］を選択します。「完全ファイルパスと名前」フィールドに設定ファイルのファイル名を入力するか、［...］をクリックしてインポートする設定ファイルを指定して［インポート］をクリックします。

■設定のエクスポート

「設定」画面の［設定のインポート／エクスポート］＞［設定のエクスポート］を選択します。「完全ファイルパスと名前」フィールドに設定ファイルの保存場所とファイル名（config.xml など）を入力するか、[...] をクリックして保存先のフォルダーを選択し、［エクスポート］をクリックします。



!重　要

エクスポートしたファイルを指定したフォルダーに書き込む権限がない場合は、エクスポート中にエラーが表示されることがあります。

4.4 ツール

ツールには、ESET Endpoint Security を管理するための機能や上級ユーザー向けのオプション機能などが用意されています。

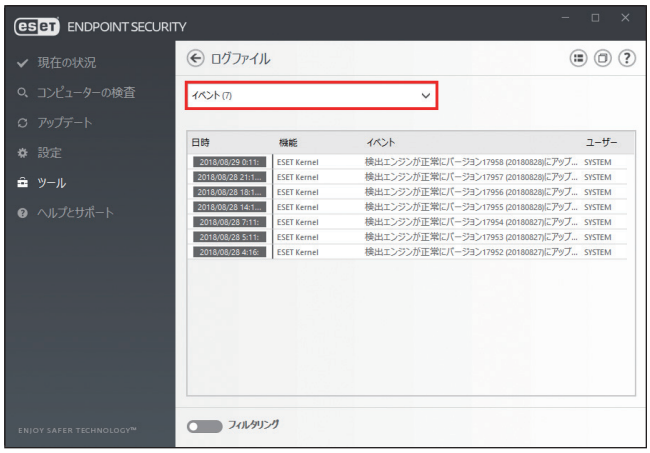
4.4.1 ログファイル

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記録されるため、検出されたウイルスの概要を確認できます。ログは、システムの分析、ウイルスの検出、トラブルシューティングの重要なツールとして使用できます。

ログへの記録はバックグラウンドで実行され、ユーザーの操作を必要としません。情報は「ログに記録する最低レベル」で設定されているログレベルに基づいて記録されます。

ログに記録された情報は、ESET Endpoint Security で表示できます。また、ログファイルのアーカイブもできます。

■ログファイルの確認



ログファイルを確認するには、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。確認できるログの種類は次のとおりです。

検出	ESET Endpoint Security で検知されたウイルスについての詳細情報が記録されています。記録される情報は、検出時刻、ウイルスの名前、場所、実行されたアクション、ウイルスの検出時にログインしていたユーザーの名前などです。ログをダブルクリックすると、詳細が別画面で表示されます。
イベント	ESET Endpoint Security によって実行された、重要なアクション、発生したイベントや、エラーに関する情報がすべて記録されています。ESET Endpoint Security で問題が発生したときは、「イベントログ」の情報から、問題点を確認できる場合があります。
コンピューターの検査	ESET Endpoint Security によって実行されたクライアントコンピューターの検査結果が記録されています。ログは検査したフォルダーごとに記録されます。ログをダブルクリックすると、詳細が別画面で表示されます。
ブロックされたファイル	ブロックされてアクセスできなかったファイルのレコードを表示します。ファイルをブロックした理由とソースモジュール、ファイルを実行したアプリケーションとユーザーを示します。
送信されたファイル	脅威に似ていたり標準ではない特性や動作を持つ不審なファイルとして、分析のために ESET に送信されたファイルを表示します。
監査ログ	設定または保護状態の変更が実行されたときの情報が記録されています。記録されている情報は、設定または保護の状態が変更されたときの日時、変更された設定または機能の種類、変更内容や変更された設定の数の説明、変更場所などのソース、ユーザーの情報などです。
HIPS	ログの記録対象に指定したルールが記録されています。操作を呼び出したアプリケーション、結果（ルールが許可されたのか禁止されたのか）、作成されたルール名が記録されます。
ネットワーク保護	ファイアウォールによって検出されたすべてのリモート攻撃が記録されています。コンピューターに対するすべての攻撃についての情報を確認できます。「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。ログを解析することにより、システムへの不正アクセスの防止に役立つ場合があります。特定のネットワークによる攻撃の詳細については、「4.6.7 ネットワーク保護」の「●許可されたサービス」を参照してください。
フィルタリングされた Web サイト	Web アクセス保護または Web コントロールによってブロックされた Web サイトが記録されています。Web サイトへのアクセスを試みた時刻、URL、ユーザー、アプリケーションを確認できます。
迷惑メール対策機能	迷惑メールと判定された電子メールと関連する情報が記録されます。
Web コントロール	ブロックまたは許可された、URL アドレスと分類方法の詳細が記録されています。「実行したアクション」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表示されます。
デバイスコントロール	コンピューターに接続されたリムーバブルメディアなどのデバイスの情報が記録されています。ログに記録されるのは、デバイスコントロールルールに一致するデバイスのみで、一致しない場合は記録されません。記録される情報は、デバイスタイプ、シリアル番号、ベンダー名、メディアのサイズなどです。

■ログの操作

ログを選択して【Ctrl】キーと【C】キーを押すと、画面に表示されている情報をクリップボードにコピーできます。【Ctrl】キーまたは【Shift】キーを押しながらログをクリックすると、複数のログを選択できます。

フィルタリングの をクリックすると、フィルタリング条件を定義できる「ログのフィルタ」画面が表示されます。

ログを右クリックするとコンテキストメニューが表示され、次の機能を実行できます。

表示	選択したログの詳細画面が表示されます（一部の種類のログのみ）。
同じレコードをフィルタ	同じタイプ（診断、警告など）の情報だけが表示されるようになります。
フィルタ	「ログのフィルタ」画面が表示され、ログのフィルタリング条件を定義できます。
フィルタをクリア	「ログのフィルタ」画面の設定をクリアします。
コピー／すべてコピー	選択したログまたはすべてのログ情報をクリップボードにコピーします。
削除／すべて削除	選択したログまたはすべてのログを削除します。ログを削除するには、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	選択したログまたはすべてのログを XML 形式のファイルにエクスポートします。
検索	「ログを検索」画面が表示され、ログを検索できます。
次を検索／前を検索	前後のログを選択します。

■ログのフィルタ／検索

ログには、重要なシステムイベントに関する情報が記録されます。ログのフィルタ／検索機能では、検索条件を指定して特定の種類のログのみを絞り込み表示できます。ログのフィルタ／検索機能を使用するには、ログを右クリックし、［フィルタ］または［検索］をクリックします。

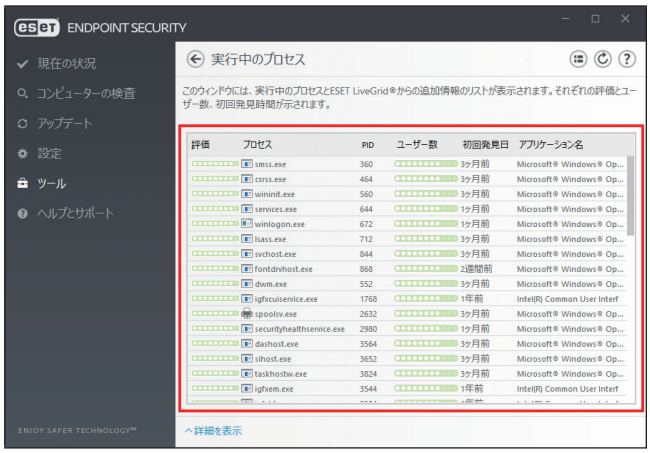
ログのフィルタ

ログの検索

テキスト検索	検索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から対象とする列を指定します。	
レコードの種類	ドロップダウンメニューからログの種類を選択します。	
	診断	プログラムおよびすべてのログを微調整するログです。
	情報	アップデートの成功を含むすべての情報メッセージおよび「診断」に含まれるすべてのログです。
	警告	重大なエラー、エラー、警告メッセージのログです。
	エラー	ファイルのダウンロード中に発生したエラーや重大なエラーのログです。
	重大	ウイルス対策保護の開始エラー、ファイアウォールエラーなど、緊急の対策が必要なエラーのログです。
期間	ドロップダウンメニューから対象の期間を指定します。「期間」を選択した場合、開始日時と終了日時を指定します。	
完全一致のみ	チェックすると、検索条件と完全に一致するログのみ表示されます。	
大文字と小文字を区別する	チェックすると、大文字と小文字を区別してログを検索します。	
既定値	設定を既定値に戻します。	

4.4.2 実行中のプロセス

実行中のプロセスは、クライアントコンピューター上で実行中のプログラムまたはプロセスを表示し、新規のウイルスを即座に ESET に通知し、その通知を継続します。ESET Endpoint Security は実行中のプロセスについて詳細な情報を提供し、ESET LiveGrid 技術でクライアントコンピューターを保護します。
実行中のプロセスを表示するには、メインメニューの［ツール］>［実行中のプロセス］をクリックします。
ESET LiveGrid が無効になっている場合、「実行中のプロセス」は表示されません。
ESET LiveGrid の設定については、「4.6.15 ツール」を参照してください。



「実行中のプロセス」画面には、次の情報が表示されます。

評価	ESET Endpoint Security および ESET LiveGrid 技術が、各オブジェクトの特性を検証して悪意のあるアクティビティである可能性をランク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）に危険レベルの評価を割り当てます。評価には「1：良好（緑）」から「9：危険（赤）」のレベルがあります。
プロセス	クライアント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が表示されます。Windows タスクマネージャーを使用して、クライアントコンピューターで動作中のプロセスをすべて表示することもできます。
PID	Windows オペレーティングシステムで実行中のプロセスの ID が表示されます。
ユーザー数	アプリケーションを使用するユーザーの数が表示されます。「ユーザー数」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が表示されます。
アプリケーション名	プログラムまたはプロセスの名前が表示されます。

ワンポイント

「評価」に「オレンジ」（不明）が表示されていても、必ずしも悪意のあるアプリケーションというわけではありません。通常は、単に新しいアプリケーションというだけで、「オレンジ」（不明）が表示されます。

ワンポイント

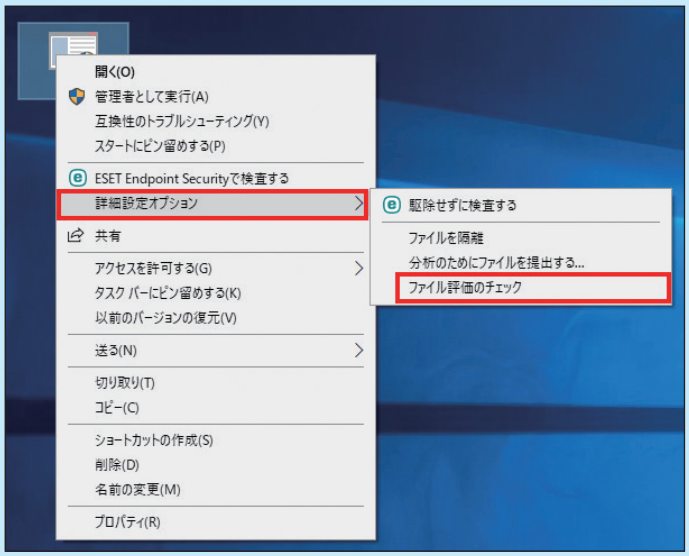
「評価」に「緑」（良）のマークが付いたアプリケーションは、感染していないことが判明しており（ホワイトリストに記載）、検査から除外されます。検査から除外するのは、「コンピューターの検査」または「リアルタイムファイルシステム保護」の検査速度を向上させるための仕組みです。

一覧からプロセスを選択して［詳細を表示］をクリックすると、次の情報が表示されます。

パス	クライアントコンピューター上のアプリケーションの場所が表示されます。
サイズ	ファイルサイズが KB（キロバイト）または MB（メガバイト）のどちらかの単位で表示されます。
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の特性が表示されます。
会社	ベンダーまたはアプリケーションプロセスの名前が表示されます。
バージョン	アプリケーション発行元からの情報に基づくファイルのバージョンが表示されます。
製品	アプリケーション名および商号が表示されます。
作成日	アプリケーションが作成された日時が表示されます。
変更日	アプリケーションが最後に変更された日時が表示されます。

ワンポイント

危険レベルの評価は、実行中のプログラムまたはプロセスとして動作していないファイルに対しても実行できます。任意のファイルの危険レベルを評価するには、対象のファイルを右クリックし、コンテキストメニューから［詳細設定オプション］>［ファイル評価のチェック］をクリックします。



4.4.3 セキュリティレポート

セキュリティレポートでは、ESET Endpoint Security の保護機能に関連する統計情報を確認できます。
セキュリティレポートを表示するには、メインメニューの［ツール］>［セキュリティレポート］をクリックします。

セキュリティレポートでは、降順の数値に基づいて次のカテゴリの統計情報の概要を表示します。また、ゼロ値のカテゴリは表示されません。

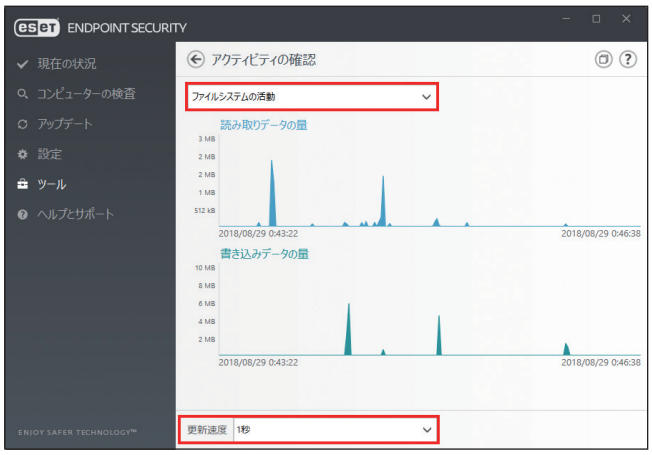
検査された文書	検査された文書オブジェクト数を表示します。
検査されたアプリケーション	検査された実行可能なオブジェクト数を表示します。
検査された他のオブジェクト	他の検査されたオブジェクト数を表示します。
検査された Web ページオブジェクト	検査された Web ページオブジェクト数を表示します。

統計情報のカテゴリの下には、世界地図が表示され、実際のウイルスの発生状況を確認できます。各国のウイルスの存在は色で示され、色が濃いほど、数が多いことを示します。データがない国は灰色で表示されます。世界地図の国の上にマウスカーソルを置くと、選択した国のデータが表示されます。特定の大陸を選択すると、自動的に拡大されます。

また、右上端の⚙をクリックすると、セキュリティレポート通知の有効 / 無効の設定や統計情報の表示期間を選択できます。表示期間は、過去 30 日間のデータの表示または製品がアクティベーションされた時点以降のデータの表示を選択できます。ESET Endpoint Security のインストール期間が 30 日未満の場合は、インストール日数のみを選択できます。30 日間の期間が、既定で設定されています。

4.4.4 アクティビティの確認

現在のファイルシステムアクティビティをグラフ形式で確認できます。
アクティビティを表示するには、メインメニューの［ツール］>［アクティビティの確認］をクリックします。



「ファイルシステムの活動」のグラフは読み取りデータの量（青）と書き込みデータの量（赤）の 2 種類が表示されます。グラフの縦軸はデータ量を表しており、データ量に応じて KB（キロバイト）／MB（メガバイト）／GB（ギガバイト）で表示されます。グラフの横軸は期間を示しており、設定された更新間隔でリアルタイムに表示されます。
時間間隔を変更するには、［更新速度］ドロップダウンメニューから選択します。選択できる更新間隔は次のとおりです。

1 秒	グラフは 1 秒おきに更新され、直近 10 分間のアクティビティが表示されます。
1 分（直前の 24 時間）	グラフは 1 分おきに更新され、直近 24 時間のアクティビティが表示されます。
1 時間（先月）	グラフは 1 時間おきに更新され、直近 1 カ月間のアクティビティが表示されます。
1 時間（選択した月）	グラフは 1 時間おきに更新され、選択した月のアクティビティが表示されます。

ドロップダウンメニューから［ネットワークアクティビティ］を選択すると、受信データの量（青）と送信データの量（赤）のグラフに切り替わります。グラフの見かたは「ファイルシステムの活動」と同じです。

4.4.5 ネットワーク接続

ネットワーク接続には、アクティブな接続と保留中の接続が一覧で表示されます。ネットワーク接続は、外部と通信しているアプリケーションを管理するのに役立ちます。
ネットワーク接続一覧を表示するには、メインメニューの［ツール］>［ネットワーク接続］をクリックします。

一覧の最初の行には、アプリケーションの名前とデータ転送速度が表示されます。[+] をクリックすると、アプリケーションによって確立されている接続名と詳細が表示されます。
「ネットワーク接続」画面には、次の情報が表示されます。

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、および通信ポートが表示されます。
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が表示されます。
プロトコル	使用されている転送プロトコルが表示されます。
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が表示されます。
送信／受信	送信中および受信中のデータ量が表示されます。

一覧からネットワーク接続を選択して［詳細を表示］リンクをクリックすると、ネットワーク接続に関する詳細情報が表示されます。

一覧を右クリックするとコンテキストメニューが表示され、次の機能を実行できます。

ホスト名を解決	名前解決が可能な場合は、すべ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、FODN 形式で表示されます。
TCP 接続のみを表示	チェックすると、一覧には TCP プロトコル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	チェックすると、現時点で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。
コンピューター内部の接続を表示	チェックすると、リモート側がローカルシステム（ローカルホスト）の接続のみが表示されます。

アプリケーションまたはプロセスを右クリックした場合は、コンテキストメニューから次の機能を実行できます。

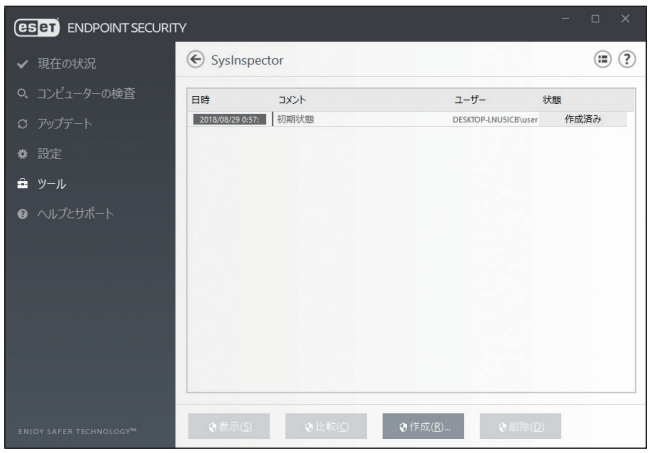
指定したプロセスの通信を一時的に拒否	アプリケーションの現在の接続を拒否します。新しい接続が確立されるときは、ファイアウォールではあらかじめ定義されたルールが使用されます。
指定したプロセスの通信を一時的に許可	アプリケーションの現在の接続を許可します。新しい接続が確立されるときは、ファイアウォールではあらかじめ定義されたルールが使用されます。

接続名を右クリックした場合は、コンテキストメニューから次の機能を実行できます。

指定した接続の通信を拒否	確立されている通信を切断します。通信の拒否は、確立されている接続の場合のみ使用できます。
更新間隔	確立されている接続の更新間隔を選択します。
最新の情報に更新	「ネットワーク接続」画面の表示を更新します。

4.4.6 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の詳細な情報を収集して、コンポーネントごとの危険レベルを評価するアプリケーションです。ESET SysInspector によって収集した情報で、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に感染したと思われるシステム動作を判別することができます。
ESET SysInspector を使用するには、メインメニューの［ツール］>［ESET SysInspector］をクリックします。



「SysInspector」画面には、作成されたログの情報が一覧で表示されます。

日時	ログの作成日時が表示されます。
コメント	ログに登録されているコメントが表示されます。
ユーザー	ログを作成したユーザーの名前が表示されます。
状態	ログの作成状態が表示されます。

「SysInspector」画面では次の操作ができます。

表示	選択したログを ESET SysInspector で開きます。ログをダブルクリックしても開くことができます。
比較	選択した 2 つのログを比較します。
作成	新しいログを作成します。ログファイルの作成中は「状態」に進行状況バーと作成済みログのパーセンテージが表示されます。「作成済み」と表示されたら、ログファイルの作成は完了です。
削除	選択したログを削除します。

ログを右クリックするとコンテキストメニューが表示され、次の機能を実行できます。

表示	選択したログを ESET SysInspector で開きます。
比較	選択した 2 つのログを比較します。
作成	新しいログを作成します。ログファイルの作成中は「状態」に進行状況バーと作成済みログのパーセンテージが表示されます。「作成済み」と表示されたら、ログファイルの作成は完了です。
削除	選択したログを削除します。
すべて削除	すべてのログを削除します。
エクスポート	選択したログを XML 形式のファイルまたは zip 形式のアーカイブにエクスポートします。

4.4.7 スケジューラ

スケジューラは、実行時間や実行するアクションなどをタスクとして登録し、自動で定期的にタスクを実行する機能です。

スケジューラを設定するには、メインメニューの［ツール］>［スケジューラ］をクリックします。
スケジューラには、登録されているタスクの設定内容（タスクのタイプ、名前、実行のタイミングなど）が一覧で表示されます。

［タスクの追加］、［編集］、［削除］をクリックすると、タスクの追加、編集、削除ができます（「■新しいタスクの追加」参照）。
タスクを右クリックするとコンテキストメニューが表示され、次の機能を実行できます。

- タスクの詳細を表示（「■タスクの詳細確認」参照）
- 今すぐ実行
- 追加
- 編集
- 削除

タスクの有効／無効を設定するには、各タスクのチェックボックスをオン／オフにします。

既定では、次のタスクが登録されています。

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

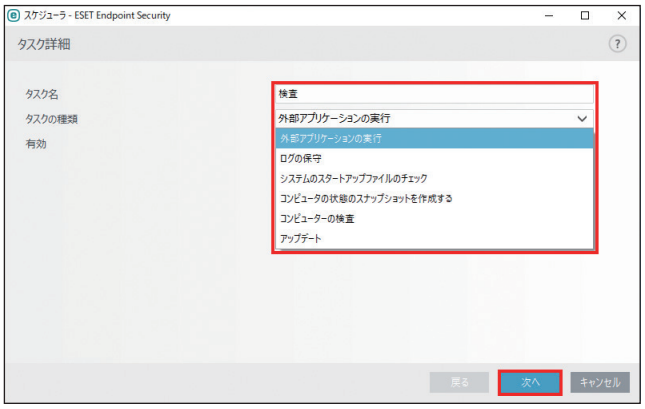
■新しいタスクの追加

次の 7 種類のタスクを追加することができます。

外部アプリケーションの実行	外部アプリケーションを実行します。
ログの保守	ログファイルには削除されたデータの痕跡も収められています。「ログの保守」タスクはシステムを効率的に運用するために、ログファイル内のデータを定期的に最適化します。
システム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時に実行されるファイルを検査します。
コンピューター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、システムコンポーネントの情報を収集し、各コンポーネントの危険レベルを評価するための ESET SysInspector コンピュータースナップショットを作成します。
コンピューターの検査	コンピューター上のファイルやフォルダーを検査します。
アップデート	検出エンジンおよびプログラムコンポーネントをアップデートします。

操作手順

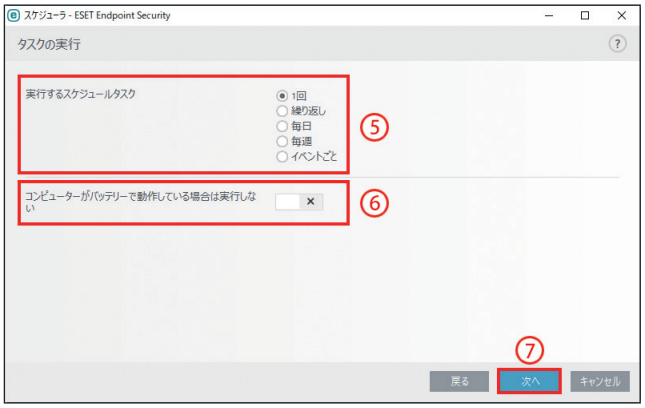
1. ［タスクの追加］をクリックします。
2. タスク名を入力します。
3. 「タスクの種類」ドロップダウンメニューから目的のタスクを選択します。



4. タスクが有効になっていることを確認し、［次へ］をクリックします。

続く

5 タスクを実行するタイミングを選択します。



1回	指定した日時にタスクを実行します。
繰り返し	指定した間隔でタスクを繰り返し実行します。
毎日	毎日指定した時刻にタスクを実行します。
毎週	毎週指定した曜日と時刻にタスクを実行します。
イベントごと	次のいずれかのイベントの発生時にタスクを実行します。 • コンピューターの起動時 • 一日の最初のコンピューター起動時 • 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 • 製品のアップデート成功 • ユーザのログオン • ウイルスの検出 詳細は「■タスク開始のタイミング－イベントのトリガー」を参照してください。

6 バッテリー電源で動作しているノートパソコンなどで、システムリソースを最小化するためにタスクを実行しないようにする場合は、［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］を有効にします。

7 ［次へ］をクリックします。

8 タスクの実行時刻を指定します。

設定内容は、手順 5 で設定したタスクのタイミングによって異なります。

9 ［次へ］をクリックします。

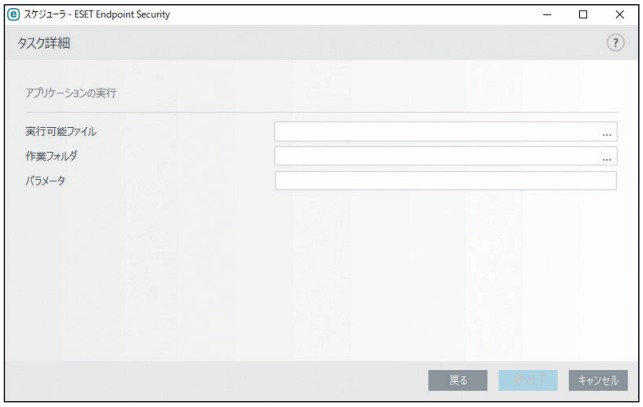
10 指定した時刻にタスクが実行されなかった場合に、タスクを再度実行するタイミングを選択します。

次のスケジュール設定日時まで待機	次のスケジュール設定日時に実行されます（24 時間後など）。
実行可能になり次第実行する	タスクの実行を妨げている原因が解消され次第実行されます。
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	指定した時間が経過するとタスクが再度実行されます。 「前回実行からの時間（時間）」で時間を設定します。

続く

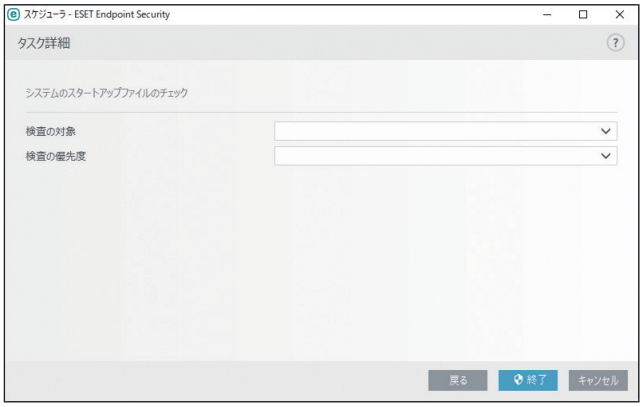
⓫ 各項目を設定します。表示される項目は、手順 3 で選択した「タスクの種類」によってかわります。

- **［外部アプリケーションの実行］を選択した場合**



実行可能ファイル	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フォルダーを指定します。実行可能ファイルの一時的なファイルが、選択したフォルダーに作成されます。
パラメータ	必要に応じて、アプリケーションのコマンドラインパラメーターを入力します。

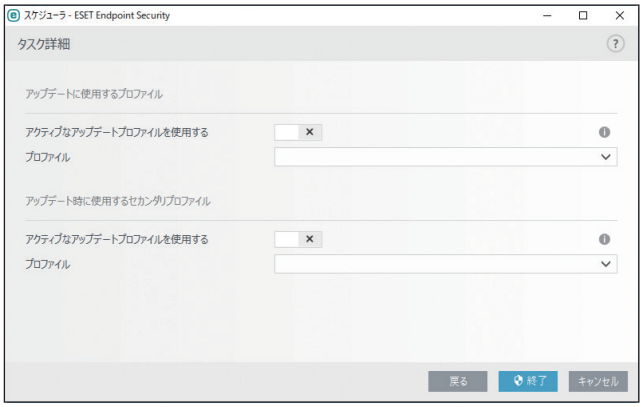
- **［システムのスタートアップファイルのチェック］を選択した場合**



続く

検査の対象	システム起動時の検査の対象を指定します。	
	すべての登録されたファイル	登録されているすべてのファイルが検査対象です。検査対象ファイルは最多です。
	使用頻度が低いファイル	使用頻度が低いファイルも検査対象に含みます。
	一般的に使用されるファイル	一般的に使用されるファイルが検査対象です。
	使用頻度が高いファイル	使用頻度が高いファイルが検査対象です。
	最も多く使用されるファイルのみ	最も多く使用されるファイルのみが検査対象です。検査対象のファイルが最少です。
	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 スケジューラーのエントリー、既知の dll などのスタートアップ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で、通常は「HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run」にあるファイル）が含まれます。
検査の優先度	検査の開始時を指定します。	
	アイドル時	システムのアイドル時に実行されます。
	最低	システム負荷が可能な限り低い時に、実行されます。
	低	システム負荷が低い時に実行されます。
	通常	通常時に実行されます。

- **「アップデート」を選択した場合**



アクティブなアップデートプロファイルを使用する	アクティブなアップデートプロファイルを使用する場合に選択します。
プロファイル	ドロップダウンメニューから使用したいプロファイルを選択します。この設定は［アクティブなアップデートプロファイルを使用する］を無効にした場合に設定できます。

続く

ワンポイント

プロファイルを変更する場合は、[アクティブなアップデートプロファイルを使用する] を無効にして、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。セカンダリプロファイルを変更する場合も、同様に操作します。

⑫ [終了] をクリックします。

■タスクの詳細確認

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、タスクの詳細を確認できます。

■タスク開始のタイミング－イベントのトリガー

次のいずれかのイベントによってタスクを開始できます。

- コンピューターの起動時
- 一日の最初のコンピューター起動時
- 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
- 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

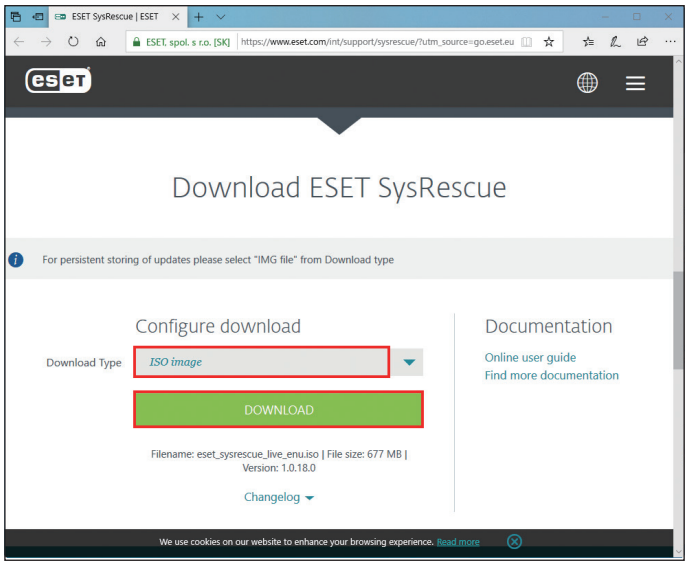
イベントによって開始されるタスクをスケジュールする際には、タスクを実行する最短間隔を指定することができます。例えば、1 日に複数回クライアントコンピューターにログオンする場合、その日および翌日の初回ログオン時にのみタスクを実行するには、「一日の最初のコンピューター起動時」を選択します。

4.4.8 ESET SysRescue Live

ESET SysRescue Liveは、ESET Securityソリューションを格納するブート可能ディスクを作成するためのユーティリティーです。本機能を使うと、ESET Security ソリューションがホストオペレーティングシステムから独立して稼動し、ディスクとファイルシステムに直接アクセスすることができます。また、オペレーティングシステムの実行中には削除ができない侵入物に対して効果を発揮します。

メインメニューの［ツール］＞［ESET SysRescue Live］を選択すると、リンク先の ESET の Web サイトが表示されます。画面をスクロールして、ダウンロードの種類や言語を選択し、［DOWNLOAD］をクリックします。

ESET SysRescue Live の使用方法はユーザーズサイトで公開している『ESET SysRescue Live 手順書』を参照してください。



4.4.9 分析のためにサンプルを提出

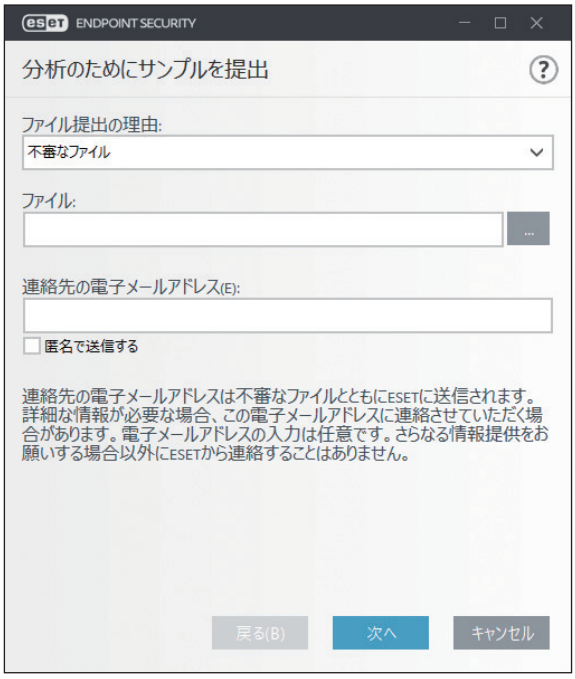
クライアントコンピューター上での動作が疑わしいファイルや、インターネット上で疑わしいサイトが見つかった場合は、ファイルまたは Web サイトを ESET のウイルスラボに提出して解析を受けることができます。解析の結果、悪意のあるアプリケーションや Web サイトであることが判明すると、以降のアップデートファイルに検出結果が追加されます。

分析用ファイルを ESET に提出する手順は、次のとおりです。

操作手順

1. メインメニューの［ツール］>［分析のためにサンプルを提出］をクリックします。

   「分析のためにサンプルを提出」画面が表示されます。



2. ［ファイル提出の理由］ドロップダウンメニューから、伝えたい内容に最も近いものを選択します。
   - 不審なファイル
   - 不審なウェブサイト（何らかのマルウェアに感染している Web サイト）
   - 誤検出ファイル（感染と検出されたが未感染であるファイル）
   - 誤検出サイト
   - その他

3. 「ファイル」で提出するファイルを指定するか、「サイト」で Web サイトの URL を入力します。

4. 「連絡先の電子メールアドレス」に連絡先のメールアドレスを入力します。

   電子メールアドレスの入力は任意です。解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します。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。

5. ［次へ］をクリックします。

6. 必要に応じてファイルおよび Web サイトの補足情報を入力し、［完了］をクリックします。

! 重 要

ESET に分析用ファイルを提出する前に、次の基準を 1 つ以上満たしていることを確認してください。

- ファイルまたは Web サイトがまったく検出されない。
- ファイルまたは Web サイトが誤って脅威として検出される。

4.4.10 隔離

隔離の主な目的は、感染ファイルを安全に保存することにあります。ファイルを駆除できない場合、またはファイルの削除が危険で推奨されない場合は、ファイルを隔離する必要があります。

任意のファイルを選択して隔離することができます。ファイルの動作が疑わしいにもかかわらず、ウイルス対策機能によって検出されない場合は、隔離機能の使用をお勧めします。隔離したファイルは、分析のために ESET のウイルスラボに提出できます。
隔離ファイルの一覧を表示するには、メインメニューの［ツール］>［隔離］をクリックします。

「隔離」画面には、隔離フォルダーに保存されているファイルが一覧で表示されます。一覧には隔離した日時、隔離したファイルの元の場所のパス、ファイルサイズ（バイト単位）、隔離した理由（「ユーザーによって追加」など）、ウイルスの数（複数のウイルスが紛れ込んだアーカイブの場合など）が表示されます。

■ファイルの隔離

ウイルス検出によって削除されたファイルは、警告画面でユーザーが隔離を無効にしない限り自動的に隔離されます。［隔離に移動］をクリックするか、一覧で右クリックして［隔離］をクリックすると、不審なファイルを手動で隔離できます。隔離したファイルは元の場所から削除されます。

■隔離フォルダーからの復元

隔離されているファイルを、元の場所に復元できます。隔離されているファイルを復元するには、一覧でファイルを選択して［復元］をクリックするか、一覧でファイルを右クリックして［復元］をクリックします。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とみなされている場合は、［復元および検査時に除外］を選択することもできます。また、一覧でファイルを右クリックして［復元先を指定］をクリックすると、隔離される前の場所とは異なる場所にファイルを復元できます。

! 重 要

害のないファイルが誤って隔離された場合は、ファイルを復元した後で検査から除外することができます。除外の設定については、「4.6.1 検出エンジン」の「4.6.1.2 除外」を参照してください。

■隔離フォルダーからの削除

一覧でファイルを右クリックして［隔離フォルダからの削除］をクリックするか、一覧でファイルを選択してキーボードの【Delete】キーを押すと、隔離フォルダーから隔離されたファイルを削除できます。複数のファイルを選択して、一度に削除することもできます。

■隔離からのファイルの提出

ウイルス対策機能によって検出されなかった疑わしいファイルを隔離した場合、またはファイルが脅威として誤って検出されて隔離された場合は、ファイルを ESET のウイルスラボに送信することができます。隔離フォルダーからファイルを提出するには、ファイルを右クリックし、［分析のために提出］をクリックします。

4.5 ヘルプとサポート

ESET Endpoint Security には、トラブルシューティングツール、および発生する可能性のある問題の解決に役立つサポート情報が含まれています。
「ヘルプとサポート」画面を表示するには、メインメニューの［ヘルプとサポート］をクリックします。

「ヘルプとサポート」画面には次の項目が含まれています。

ヘルプ	P74 参照
テクニカルサポート	P74 参照
サポートツール	P75 参照
製品およびライセンス情報	P75 参照

■ヘルプ

ESET ナレッジベースの検索	ESET セキュリティ ソフトウェア シリーズのサポート情報が表示されます。FAQ（よくある質問）への回答や、様々な問題に対する一般的な解決策が登録されています。このナレッジベースは、定期的にアップデートされており、様々な種類の問題を解決するための最も有効なツールです。
ヘルプを開く	ESET Endpoint Security のヘルプページを開きます。
解決方法を探す	FAQ の解決策を探すには、これを選択します。サポートセンターにお問い合わせいただく前に、このセクションを確認してください。

■テクニカルサポート

サポート要求の送信	このリンクをクリックすると、「システム構成データの送信」画面が表示されます。［続行］をクリックすると、ESET 社にシステム構成データが送信されます。サポートセンターより指示があった場合にのみ行ってください。

■サポートツール

脅威情報	様々なタイプのマルウェアの危険と兆候に関する情報を含む、ESET の最新ウイルス情報一覧へのリンクです。
検出エンジンの更新履歴	ESET ウイルスレーダーへのリンクです。検出エンジンのバージョン情報が含まれています。
ESET Log Collector	ESET Log Collector のダウンロードページへのリンクです。システム情報やログファイルなど必要な情報を、サーバーから自動的に収集することができます。詳細については、「5.5 ESET Log Collector」を参照してください。
ESET 特殊駆除ツール	一般的なマルウェア感染を自動的に特定して駆除します。

■製品およびライセンス情報

ESET Endpoint Security について	バージョン情報やインストール済のコンポーネントについて確認できます。
製品のアクティベーション	製品のアクティベーション画面を開きます。詳細については「2.4 アクティベーション」を参照してください。

4.6 詳細設定

4.6.1 検出エンジン

ESET Endpoint Security は、ファイル、電子メール、インターネット接続を制御することで、悪意のあるシステム攻撃からコンピューターを保護します。たとえば、マルウェアに分類されたオブジェクトが検出された場合、修復が開始されます。検出エンジンは、最初にブロックし、その後に駆除、削除、または隔離に移動して、マルウェアを排除します。検出エンジンの詳細を設定するには、メインメニューの［設定］>［詳細設定］をクリックするか、【F5】キーを押して「詳細設定」画面を表示し、［検出エンジン］をクリックします。

4.6.1.1 リアルタイム保護および機械学習保護

「リアルタイム保護および機械学習保護」カテゴリでは、以下のカテゴリの「報告」および「保護」のレベルを設定できます。

! 重 要

ESET Endpoint Security バージョン 7.2 以降では、バージョン 7.1 以下のときにあった「検出エンジン」セクションのオン / オフボタンがありません。オン / オフボタンは、「最大」、「標準」、「最小」、「オフ」のしきい値に代わりました。

マルウェア	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。「ウイルス」という用語がよく間違って使用されますが、「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。
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、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。
不審なアプリケーション	不審なアプリケーションには、圧縮形式またはプロテクタで圧縮されたプログラムが含まれます。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	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。

ワンポイント

機械学習保護は高度な保護であり、機械学習に基づいて検出を改善する高度なレイヤーとして検出エンジンの一部になっています。

■マルウェア検査

マルウェア検査のスキャナー設定は、「リアルタイム保護および機械学習保護」カテゴリとオンデマンド検査の「オンデマンド保護および機械学習保護」カテゴリで設定できます。既定では、[マルウェア検査] > [オンデマンド検査] > [オンデマンド保護および機械学習保護] カテゴリで「リアルタイムファイルシステム保護設定を使用」が有効に設定されています。この設定が有効なときには、関連するオンデマンド検査の設定が「リアルタイム保護および機械学習保護」カテゴリから継承されます。詳細については、「4.6.4　マルウェア検査」の「●オンデマンド保護および機械学習保護」を参照してください。

■報告設定

脅威が見つかり、マルウェアとして分類される検出が発生すると、情報が検出ログに記録され、デスクトップ通知が有効に設定されている場合はデスクトップ通知が発生します。報告のしきい値は、「マルウェア」「望ましくない可能性のあるアプリケーションアプリケーション」「不審なアプリケーション」「安全ではない可能性があるアプリケーション」の各カテゴリごとに設定できます。また、報告のしきい値は、現在の保護しきい値よりも高いしきい値を設定できます。報告のしきい値の設定は、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。報告のしきい値（またはレベル）は、以下の基準で設定できます。

しきい値	説明
最大	しきい値を最大感度に設定します。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脅威として特定される場合があります。
標準	しきい値を標準に設定します。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	しきい値を最小に設定します。この設定は、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	報告を無効に設定します。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。なお、マルウェアではオフを使用できません。これは、安全でない可能性があるアプリケーションの既定値です。

● ESET Endpoint Security の保護モジュールの使用可否

選択したカテゴリのしきい値の保護モジュールの使用可否（有効または無効）は以下のとおりです。

	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

*ESET Endpoint Security バージョン 7.2 以降で提供されています。

●製品バージョン、プログラムモジュールの確認方法

製品バージョン、プログラムモジュールを確認するには、メインメニューの［ヘルプとサポート］>［ESET Endpoint Security について］をクリックし、バージョン情報画面を表示します。バージョン情報画面の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。また、［インストールされたコンポーネント］ボタンをクリックすると、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基本事項は、以下のとおりです。

- 「標準」しきい値は、ほとんどの設定で推奨されます。
- 「最小」しきい値は、前のバージョンの ESET Endpoint Security（7.1 以下）の保護レベルに相当します。これは、セキュリティソフトウェアにオブジェクトの誤検出を最小化することが優先される環境で推奨されます。
- 報告の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。
- 現実的には、100%の検出率や 0%の誤検出率は保証されません。
- ESET Endpoint Security 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、そのオブジェクトはブロックされ、その後、駆除、削除、または隔離に移動されます。保護のしきい値（またはレベル）は、以下の基準で設定できます。

しきい値	説明
最大	報告された最大（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）が開始されます。すべてのエンドポイントが最大感度で検査されます。誤って報告されたオブジェクトを検出除外に追加するときは、この設定が推奨されます。
標準	報告された標準（以下）レベルの検出はブロックされます。自動修復（たとえば駆除）が開始されます。
最小	報告された最小レベルの検出はブロックされます。自動修復（たとえば駆除）が開始されます。
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。マルウェアではオフを使用できません。これは、安全でない可能性があるアプリケーションの既定値です。

● ESET Endpoint Security 7.1 以下のポリシー変換表

ESET Security Management Center のポリシーでは、各カテゴリに ON/OFF スイッチがありません。ESET Security Management Center ポリシーで、ESET Endpoint Security バージョン 7.1 以下に設定を行った場合、以下のようになります。

ESET Security Management Center ポリシー設定値	最大	標準	最小	オフ
ESET Endpoint Security バージョン 7.1 以下に適用される設定値	✓	✓	✓	✗

ESET Endpoint Security バージョン 7.1 以下からバージョン 7.2 以降にアップグレードする場合、しきい値の状態は次のようになります。

アップグレード前の設定値	✓	✗
アップグレード後の設定値	標準	オフ

■ベストプラクティス

●管理されていない環境（個別のクライアントワークステーション）

既定の推奨値をそのまま使用してください。

●管理された環境

通常、これらの設定は、ポリシー経由でワークステーションに適用されます。

1. 初期フェーズ

このフェーズは最大で 1 週間かかる場合があります。

- すべてのカテゴリの報告のしきい値を「標準」に設定するか、必要に応じて、「最大」に設定します。
- マルウェアの保護のしきい値を、「標準」に設定します。
- 他のカテゴリの保護のしきい値を「最小」に設定します。

! 重 要

このフェーズでは、保護のしきい値を最大に設定することは推奨されません。誤検出を含むすべての検出が修復（駆除）されるためです。

- 検出ログから誤検出のオブジェクトを特定し、検出除外に追加します。

2. 移行フェーズ

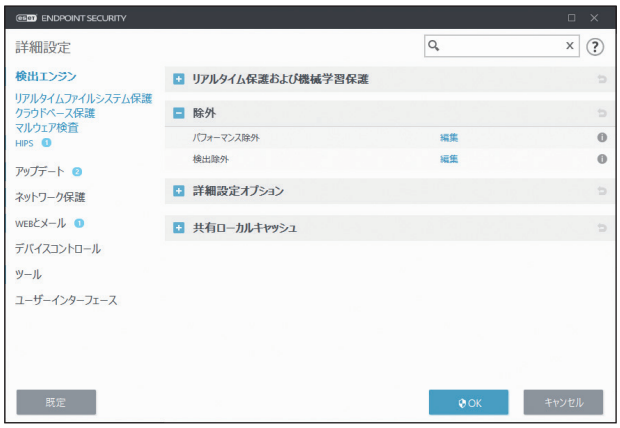
- 「本番フェーズ」のテストとして、一部のワークステーションに実装します。ネットワークのすべてのワークステーションには実装しないでください。

3. 本番フェーズ

- すべての保護しきい値を、「標準」に設定します。
- リモートで管理するときには、ESET Endpoint Security の該当する定義済みウイルス対策ポリシーを使用します。
- 保護しきい値の「最大」は、最高の検出率が必要で、オブジェクトの誤検出が許容される場合に設定してください。
- 検出ログまたは ESET Security Management Center レポートに見つかっていない検出があるかどうかを確認してください。

4.6.1.2 除外

「除外」カテゴリでは、特定オブジェクトを検出エンジンから除外する設定を行えます。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、除外を作成しないことをお勧めします。ただし、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。除外には、「パフォーマンス除外」と「検出除外」があります。
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。パフォーマンス除外は、ファイルレベルで、ゲームアプリケーションの検査を除外したり、異常なシステム動作やパフォーマンスが増加したときに便利です。
検出除外では、検出名、パス、またはハッシュを使用して、オブジェクトを駆除から除外できます。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。



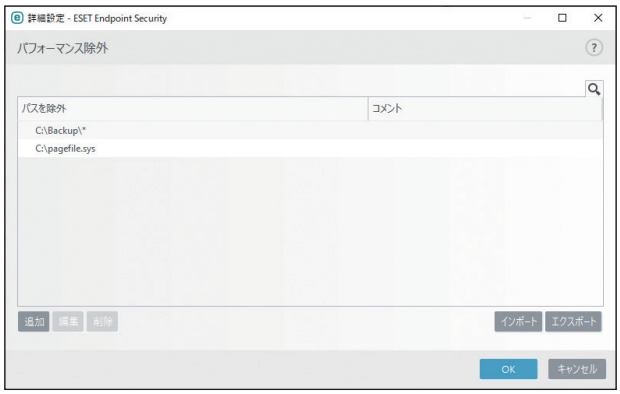
! 重 要

以下の他の種類の除外と混同しないよう注意してください。

- 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可用性の改善が必要になる場合があります）。詳細は、「4.6.2 リアルタイムファイルシステム保護」の「●プロセスの除外」を参照してください。
- 除外されたファイル拡張子：詳細は、「4.6.2 リアルタイムファイルシステム保護」の「■ THREATSENSE パラメータ」の「●除外」を参照してください。
- HIPS の除外：詳細は、「4.6.5 HIPS」の「■基本」の「除外」を参照してください。
- クラウドベース保護の除外フィルター：詳細は、「4.6.3 クラウドベース保護」の「除外」を参照してください。

■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。たとえば、コンピューターの処理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を検査する場合や、検査と競合するソフトウェア（バックアップソフトウェア）がインストールされている場合など、特別な場合以外は除外設定を行わないでください。パフォーマンス除外を作成したいときは、[設定] > [詳細設定] > [検出エンジン] > [除外] > [パフォーマンス除外] > [編集] とクリックし、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します。ファイルとフォルダーを検査から除外するには、[追加] ボタンをクリックして、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。



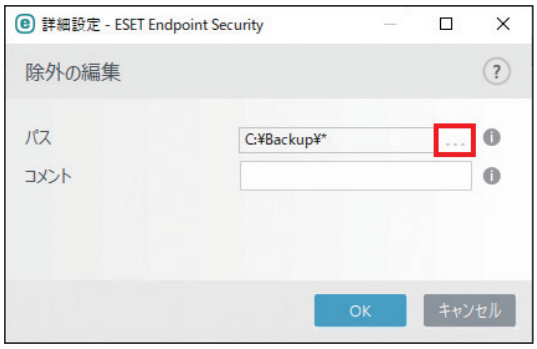
パス	検査から除外するファイルやフォルダーのパスが表示されます。
コメント	除外するファイルやフォルダーのコメントが表示されます。
追加	検査から除外するファイルやフォルダーのパスを追加します。
編集	選択したエントリーを編集します。
削除	選択肢たエントリーを削除します。また、CTRL キーを押しながらクリックすると、複数のエントリを選択できます。

! 重　要

登録された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。

●パフォーマンス除外の追加または編集

「除外の追加」ダイアログウィンドウは、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	除外したいファイルやフォルダーのパスを入力します。…をクリックすると、該当するファイルやフォルダーのパスを選択できます。手動で入力する場合は、「●パス除外形式」を参照してください。
コメント	除外したいファイルやフォルダーのコメントを入力します。コメントの入力は任意です。

●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。なお、パスの途中でワイルドカードを使用することはお控えください。

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。
- すべてのファイルとサブフォルダーも含めドライブ全体を除外するには、「*」を使用します。例えば、D ドライブ全体を除外するには、「D:¥*」のように入力します。
- doc ファイルのみを除外する場合は、「*.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さまざまな文字が使用されており、最初の文字（たとえば "D"）のみが明らかな場合は、「D????.exe」という形式を使用します。疑問符は、不足している（不明な）文字の代わりになります。

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、「%PROGRAMFILES%¥*（必ずパスの最後に ¥ マークまたは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、「%PROGRAMFILES%¥Excluded_Directory¥*」を使用します。また、以下のシステム変数が、パス除外形式で利用できます。ただし、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。

%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%PROGRAMFILES%
%PROGRAMFILES(X86)%

%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%

アスタリスクを使用したパスの除外

- **アスタリスクを使用したその他の除外例**

C:¥Tools¥*	パスの最後が ¥ マーク（バックスラッシュ）とアスタリスクで、フォルダーとすべての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¥*.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	正確なパスにある特定のファイルを除外します。

- **パフォーマンス除外の例外**

C:¥Tools¥*.*	C:¥Tools¥* と同じ動作（「*.*」と混同しないでください。これは Tools フォルダーの拡張子のファイルのみを除外します）。

- **正しくない手動で入力された除外の例**

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¥	「C:¥Tools¥*」のようにパスの最後にアスタリスクを必ず追加してください。

パスの中間のワイルドカード

パスの中央でワイルドカードを使用しないことをお勧めします（例：「C:¥Tools¥*¥Data¥file.dat」）。なお、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。

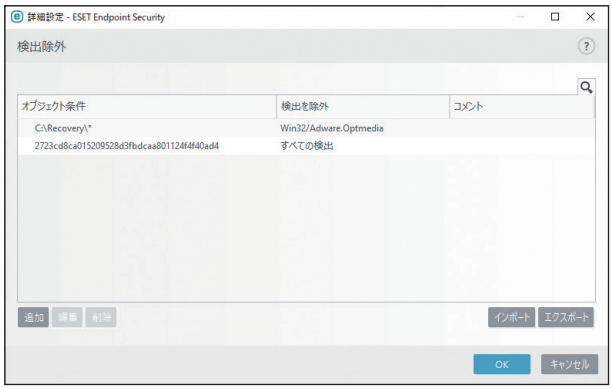
除外の順序

- 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。（ファイアウォールルールでは、ルールは最上位から最下位へと実行されます）
- スキャナーによっては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。
- 同時に作用するルールの作成は避けてください。

■検出除外

検出除外では、検出名、オブジェクトパス、またはハッシュをフィルタリングして、オブジェクトを駆除から除外できます。また、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、以下の画面のような除外設定が行われている場合、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 内にあるときに除外されます。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。

検出除外は、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作成することをお勧めします。検出除外を追加するには、［設定］>［詳細設定］>［検出エンジン］>［除外］>［検出除外］>［編集］とクリックします。「検出除外」画面で、［追加］ボタンをクリックすると、除外するファイルやフォルダー、ハッシュ、検出名などをリストに追加できます。



オブジェクト条件	検査から除外するオブジェクトの条件が表示されます。表示される条件は、追加した条件（ファイルやフォルダーのパス、ハッシュ）によって異なります。
検出を除外	検出名を追加した場合は、検出名が表示されます。パスやハッシュを追加したときは、「すべての検出」と表示されます。
コメント	除外する条件のコメントが表示されます。
追加	検出対象外とするオブジェクトを追加します。
編集	選択したエントリーを編集します。
削除	選択肢たエントリーを削除します。また、CTRL キー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。

●検出除外オブジェクト条件

検出除外に追加するオブジェクトは、以下の条件で追加できます。

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名がある場合、それは特定の検出に対してのみファイルの除外が行われ、他の検出には行われないことを意味します。ただし、ファイルが後から他のマルウェアに感染した場合は検出されます。このような除外は、一定の種類の侵入物にのみ使用できます。これは、侵入物をレポートする警告ウィンドウで作成する（[設定の表示] オプションをクリックしてから [検出対象外] を選択）か、または [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て、コンテキストメニューから [検査からの復元と除外] を選択して作成できます。
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（SHA1）に基づいて、ファイルを除外します。

● ESET Security Management Center での検出除外設定

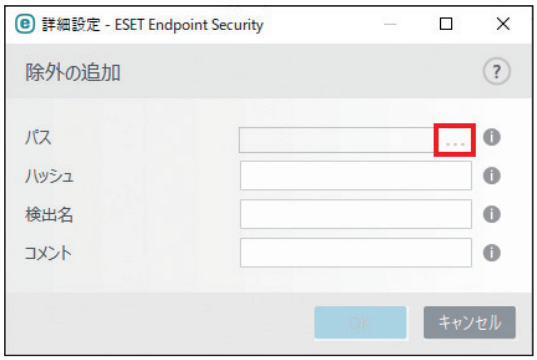
ESET Security Management Center Ver7.1 には、検出除外管理のための新しいウィザードがあり、検出除外を作成し、別のコンピューターまたはグループに適用できます。

- **ESET Security Management Center から検出除外が上書きされる可能性**

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

●検出除外の追加または編集

「検出除外」画面で、［追加］ボタンをクリックすると、除外するファイルやフォルダー、ハッシュ、検出名などを検出除外のリストに追加できます。また、検出除外によって侵入の例外を設定することは、非常に危険です。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の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	除外したいファイルやフォルダーのパスを入力します。…をクリックすると、該当するファイルやフォルダーのパスを選択できます。手動で入力する場合は、「●パス除外形式」を参照してください。
ハッシュ	除外したいハッシュ（SHA-1）を入力します。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	ESET 検出名を入力します。検出名を入力するときは、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てください。［ツール］>［ログファイル］とクリックし、ドロップダウンメニューから［検出］を選択すると、検出されたオブジェクトの情報を確認できます。これは、誤検出サンプルが ESET Endpoint Security で検出されているときに役立ちます。また、ESET Endpoint Security アラートウィンドウから検出を除外するときは、次のような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
コメント	検出除外を行うパスやハッシュ、検出名のコメントを入力します。コメントの入力は、任意です。

●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）。

操作手順

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. 検出ログで検出除外したいログ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。

4.6.1.3 詳細設定オプション

「詳細設定オプション」カテゴリでは、アンチステルスや AMSI のオン / オフを設定できます。

アンチステルスを有効にする	オペレーティングシステムから見えないルートキットなど、危険なプログラムを検出する高度な保護機能です。アンチステルスを有効にすると、通常の検査技術では検出できないプログラムでも検出できます。
AMSI による詳細検査を有効にする	Microsoft Antimalware Scan Interface ツールで、アプリケーション開発者は新しいマルウェアを防御できます。この機能は Windows 10 でのみ利用できます。

4.6.1.4 共有ローカルキャッシュ

共有ローカルキャッシュを使用すると、ファイルとフォルダーの検査情報がキャッシュサーバーの共有キャッシュに保存されます。新しい検査を実行する際は、ESET Endpoint Security がキャッシュサーバーのキャッシュにある検査済みファイル情報を検索し、ファイル情報が一致すれば検査から除外されます。これにより、ネットワーク上での検査の重複がなくなり、仮想環境のパフォーマンスが向上します。
キャッシュサーバーの設定は次のとおりです。

ホスト名	キャッシュがあるコンピューターの名前または IP アドレス。
ポート	通信で使用されるポート番号（共有ローカルキャッシュと同じ）。制限値は「0」～「65535」です。
パスワード	ESET 共有ローカルキャッシュのパスワード。必要に応じて設定。

4.6.1.5 マルウェアが検出されたとき

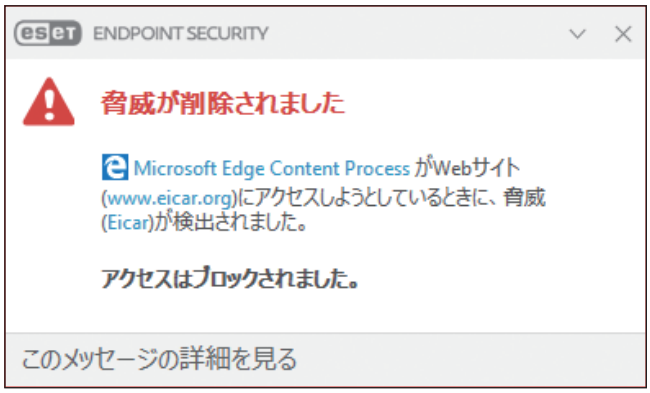
マルウェアがシステムに侵入する経路は、Web サイト、共有フォルダー、メール、リムーバブルデバイス（USB メモリー、外付けハードディスク、CD、DVD、フロッピーディスクなど）など、様々です。

標準的な動作

ESET Endpoint Security は、基本的に次の機能でマルウェアを検出して処理します。

- リアルタイム検査
- Web アクセス保護
- 電子メールクライアント保護
- コンピューターの検査

各機能は、標準的な駆除レベルを使用してファイルを駆除し、駆除したファイルを隔離するか、接続を切断します。通知画面は、デスクトップ右下の通知領域に表示されます。駆除レベルと動作の詳細については、「4.6.2 リアルタイムファイルシステム保護」の「●駆除」を参照してください。



●駆除と削除

リアルタイムファイルシステム保護にあらかじめ指定されたアクションがない場合は、警告画面が表示され、ウイルスに感染したファイルに対するアクションを選択できます。選択できるアクションは通常、[駆除]、[削除]、[何もしない]のいずれかです。[何もしない]を選択すると、感染ファイルが駆除されないまま残りますので、そのファイルが「無害なのに誤って感染が検出されたことが確実」な場合のみ選択してください。
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、ファイルを元の状態に戻すため、まず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は、ファイルそのものを削除します。

ワンポイント

駆除とは、ウイルスに感染したファイルからウイルスだけを取り除き、正常なファイルに戻すことです。削除とは、感染したファイルそのものを削除することです。ウイルスの種類によっては駆除が難しく、場合によってはファイルを削除しなければなりません。

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）。

●複数の脅威

コンピューター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［常にエンドユーザーに確認する］に設定されている場合は、警告画面が表示され、感染ファイルに対するアクションを選択できます。感染ファイルに対するアクションを一覧から選択します。

●アーカイブファイルの削除

アーカイブファイル内に感染していないファイルがなく、感染ファイルのみある場合は、アーカイブファイル全体が削除されます。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、駆除レベルの設定に従って処理されます。

使用しているコンピューターの処理速度が遅くなる、頻繁にフリーズするなど、マルウェアに感染している兆候がある場合は、次の処置をお勧めします。

操作手順

1. メインメニューの［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］をクリックします。
   詳細については、「4.1　コンピューターの検査」を参照してください。
3. 検査の終了後、ログで検査済みファイル、感染ファイル、駆除済みファイルの件数をそれぞれ確認します。

ワンポイント

コンピューターの特定の領域だけを検査する場合は、［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。

4.6.2　リアルタイムファイルシステム保護

「リアルタイムファイルシステム保護」ではリアルタイムファイルシステム保護の設定ができます。
リアルタイムファイルシステム保護は、システム起動時に有効になり、ファイルのオープン、作成、実行などのイベントが発生したとき、ファイル内に悪意のあるコードがないかを検査します。
リアルタイムファイルシステム保護は、安全なシステムを維持するために必要不可欠な機能です。パラメーターを変更する際には注意してください。パラメーターの変更は、特定のアプリケーションや別のウイルス対策プログラムのリアルタイムスキャナーと競合する場合など、特別な場合のみ行うことをお勧めします。

ワンポイント

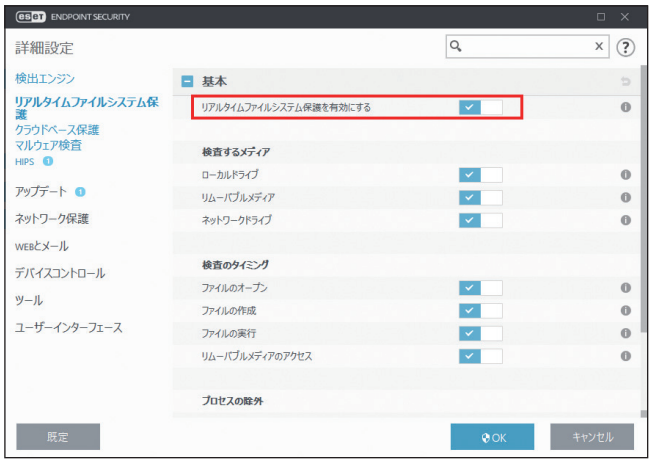
リアルタイムファイルシステム保護は、ファイルアクセスなど、様々なシステムイベントが発生するたびに、すべての種類のメディアを確認します。ThreatSense テクノロジーの検出方法を使用するリアルタイムファイルシステム保護は、新規作成ファイルと既存ファイルで検査方法が異なることがあります。新規作成ファイルの場合、より高いレベルの検査を適用します。
ThreatSense テクノロジーの検出方法の詳細については、「4.6.2　リアルタイムファイルシステム保護」の「■ THREATSENSE パラメータ」を参照してください。

ワンポイント

ESET Endpoint Security の既定の設定は、最大レベルでシステムを保護できるように最適化されています。既定の設定に戻すには、各機能の右側にある ⚙ をクリックするか、【F5】キーを押して「詳細設定」画面を表示し、［既定］をクリックします。

■基本

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、常にイベントを検査します。別のリアルタイムスキャナーと競合するなど、リアルタイムファイルシステム保護を無効にしたい場合は、［検出エンジン］>［リアルタイムファイルシステム保護］>［基本］>「リアルタイムファイルシステム保護を有効にする」を無効にします。無効状態では危険なため別のリアルタイムスキャナーとの競合などの問題が解決したら、有効に戻してください。



●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存在しないか検査します。

ローカルドライブ	システムのハードディスクをすべて検査します。
リムーバブルメディア	CD/DVD、USB メモリー、Bluetooth デバイスなどを検査します。
ネットワークドライブ	システムに割り当てられているネットワークドライブをすべて検査します。

ワンポイント

既定の設定の変更は、特定のメディアを検査するとデータ転送が極端に遅くなるなど、特別な場合のみ行うことをお勧めします。

●検査のタイミング（イベント発生時の検査）

既定では、ファイルを開く、作成する、実行するなどのイベントが発生すると、ファイルを検査します。

ファイルのオープン	ファイルを開いたときに検査を行うかどうかを設定します。
ファイルの作成	ファイルを新しく作成したとき、またはファイルの内容を変更したときに、検査を行うかどうかを設定します。
ファイルの実行	ファイルを実行したときに検査を行うかどうかを設定します。
リムーバブルメディアのアクセス	ストレージに空き容量がある特定のリムーバブルメディアを利用するときに、検査を行うかどうかを設定します。

! 重　要

コンピューターが最大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。

●プロセスの除外

指定したプロセスの実行ファイルをスキャン対象から除外します。［検査対象外とするプロセス］の［編集］をクリックすると、「プロセスの除外」画面が表示され、［追加］ボタンをクリックすると、除外したいプロセスを登録できます。

■ THREATSENSE パラメータ

ThreatSense は、ウイルスを検出する高度な技術です。この技術はプロアクティブ（事前対応型）の検出方法なので、新しいウイルスが広がる初期の段階でシステムを保護することができます。ThreatSense は、システムのセキュリティを大幅に強化するために、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などを組み合わせて保護します。検査エンジンは、複数のデータストリームを同時に検査することで、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。

設定できるパラメーター

ThreatSense エンジンの設定オプションを使用すると、様々な検査パラメーターを指定できます。

- 検査するファイルの種類および拡張子
- 様々な検出方法の組み合わせ
- 駆除のレベル

など

ThreatSense エンジンパラメーターを設定できる保護機能

ThreatSense エンジンパラメーターを設定するには、「詳細設定」画面で ThreatSense 技術を使用する機能の［THREATSENSE パラメータ］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できるように、ThreatSense は次の保護機能ごとに設定することができます。

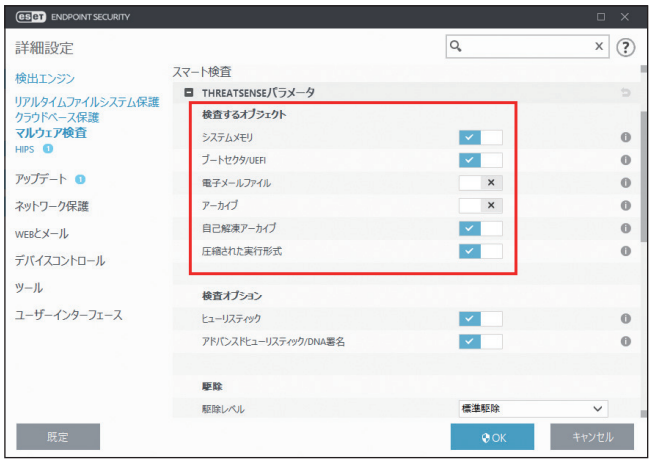
- リアルタイムファイルシステム保護
- マルウェア検査
- アイドル状態検査
- スタートアップ検査
- リムーバブルメディア
- ドキュメント保護
- 電子メールクライアント保護
- Web アクセス保護

! 重　要

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。例えば、通常は新しく作成されたファイルのみが検査対象となりますが、リアルタイムファイルシステム保護機能で常に圧縮された実行形式を検査するようにパラメーターを変更したり、アドバンスドヒューリスティックを有効にしたりすると、システムの処理速度が低下することがあります。コンピューターの検査以外の機能については、ThreatSense 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

「検査するオブジェクト」セクションでは、検査するコンピューターのコンポーネントおよびファイルを定義できます。



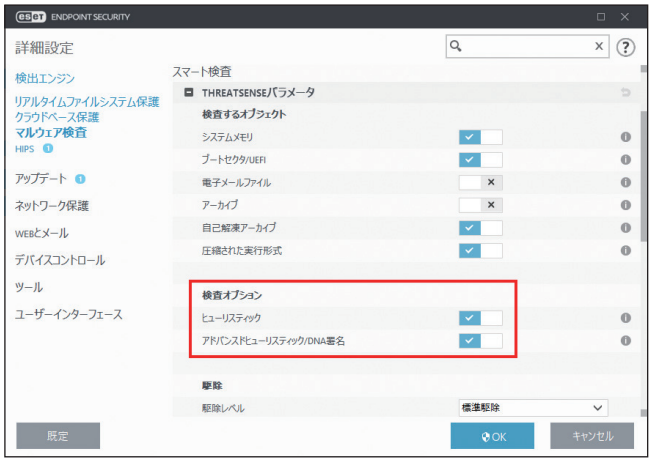
システムメモリ	システムメモリーを攻撃対象とするマルウェアを検査します。
ブートセクタ/UEFI	ブートセクターおよび UEFI のルートキット、ブートキット、他のマルウェアを検査します。
電子メールファイル	拡張子が DBX（Outlook Express）および EML の電子メールファイルを検査します。
アーカイブ	以下の拡張子のアーカイブを検査します。 ARJ、BZ2、CAB、CHM、DBX、GZIP、ISO/BIN/NRG、LHA、MIME、NSIS、RAR、SIS、TAR、TNEF、UUE、WISE、ZIP、ACE、その他多数。
自己解凍アーカイブ	解凍に特殊なプログラムを必要としない自己解凍形式（SFX）のアーカイブを検査します。
圧縮された実行形式	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ファイル（UPX、yoda、ASPack、FSG など）や標準とは異なる解凍形式で圧縮された実行形式ファイルを検査します。

ワンポイント

検査するオブジェクトに表示される項目は、選択した機能によって異なります。上の画面は、［マルウェア検査］を選択した場合を例に解説しています。

●検査オプション

「検査オプション」セクションでは、システムを検査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。



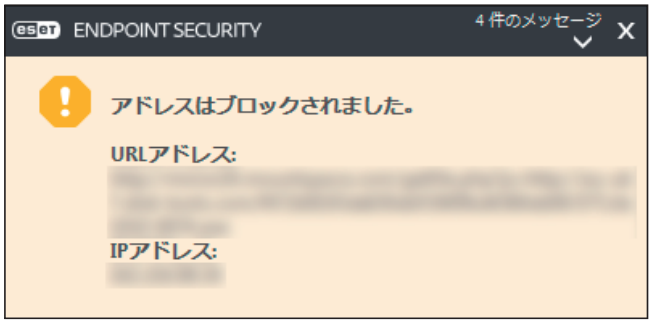
ヒューリスティック	ヒューリスティックは、悪意のあるプログラムの動きを分析するアルゴリズムです。主な利点は、以前には存在しない、またはこれまでの検出エンジンにない悪意のあるソフトウェアを特定できる点です。欠点は、誤検出の可能性がある点です。
アドバンスドヒューリスティック/DNA 署名	アドバンスドヒューリスティックは、ESET が開発した独自のヒューリスティックアルゴリズムで構成されています。このアルゴリズムは、コンピューターワームやトロイの木馬を検出するために最適化され、高度なプログラミング言語で記述されています。アドバンスドヒューリスティックを使用すると、脅威の検出機能が大幅に向上します。

潜在的な脅威が検出された場合

望ましくない可能性があるアプリケーションが検出された場合は、実行するアクションを選択できます。

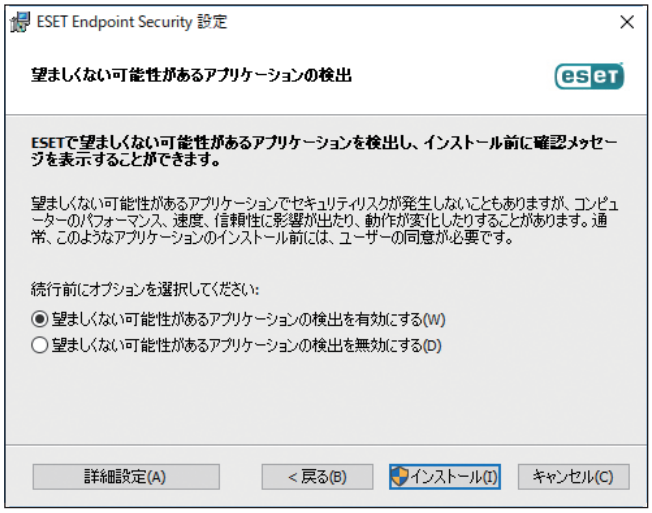
- 駆除／切断：アクションを終了し、潜在的な脅威がシステムに侵入するのを防ぎます。
- 何もしない：潜在的な脅威がシステムに進入するのを許可します。
- 今後中断せずにコンピューターでアプリケーションを実行できるようにするには、［設定の表示］をクリックし、［検出から除外］をチェックします。

検出された望ましくない可能性があるアプリケーションを駆除できない場合は、デスクトップの右下に「アドレスはブロックされました」という通知が表示されます。通知の詳細を確認するには、メインメニューの［ツール］>［ログファイル］をクリックし、ドロップダウンメニューから［フィルタリングされた Web サイト］を選択します。



望ましくない可能性があるアプリケーションに関する設定

ESET Endpoint Security をインストールするとき、ソフトウェアラッパーなどの望ましくない可能性があるアプリケーションの検出を有効にするかどうかを設定できます。



望ましくないアプリケーションの検出設定は、設定オプションで変更できます。変更するには、次の操作を行います。

操作手順

1. ESET Endpoint Security を開きます。ESET Endpoint Security の開き方については「2.5 コンピューターの検査」の手順 1 ～ 2 を参照してください。
2. 【F5】キーを押します。
3. ［検出エンジン］をクリックし、次の各機能のしきい値を変更します。
   - マルウェア
   - 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
4. ［OK］をクリックします。

ソフトウェアラッパー

ソフトウェアラッパーは、特殊なタイプの修正アプリケーションで、ファイルホスティング Web サイトの一部で使用されます。ソフトウェアラッパーはサードパーティ製のツールですが、ツールバーやアドウェアなどの追加ソフトウェアもインストールします。追加されたソフトウェアは、Web ブラウザーのホームページや検索設定を変更する場合があります。多くの場合、ファイルホスティング Web サイトはソフトウェアベンダーやダウンロード受信者に、設定が変更されたことを通知しないため、変更を回避することができません。このため、ESET Endpoint Security はソフトウェアラッパーを望ましくない可能性のあるアプリケーションのタイプに分類しています。ユーザーはソフトウェアラッパーをダウンロードするかどうかを設定できます。

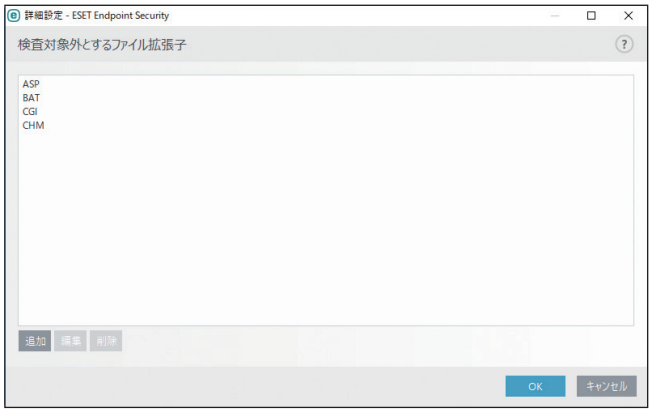
●駆除

感染ファイルからウイルスを駆除するときのレベルには、4 つのレベルがあります。

常に感染を修正する	オブジェクトの駆除中に感染の修復を試みます。ユーザー操作はありません。ごく一部の場合（システムファイルなど）で、感染を修正できない場合は、報告されたオブジェクトは元の場所に残されます。「常に感染を修正する」は、管理された環境で推奨される既定の設定です。
安全な場合に感染を修正し、安全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感染の修復を試みます。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、感染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。ほとんどの場合、この設定が推奨されます。
安全な場合は感染を修正する、安全でない場合は確認する	オブジェクトの駆除中に感染の修復を試みます。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。
常にエンドユーザーに確認する	オブジェクトの駆除中にエンドユーザーにインタラクティブウィンドウが表示され、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。

●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。既定では、拡張子に関係なく、すべてのファイルが検査されます。除外では検査対象外とする拡張子を指定します。除外で追加した拡張子のファイルは検査対象外となり、削除した拡張子のファイルは検査対象となります。



ESET Endpoint Security では、どのような拡張子でも検査対象外に指定できます。ファイルの検査によってプログラムが正常に動作しなくなる場合は、その拡張子を検査から除外する必要があります。例えば、MS Exchange Server を使用しているときは、拡張子 .edb、.eml、.tmp を除外します。

拡張子の管理

検査対象外となっている拡張子を表示するには、メインメニューの［設定］>［詳細設定］をクリックするか、【F5】キーを押して「詳細設定」画面を表示し、各保護機能の［THREATSENSE パラメータ］>「検査対象外とするファイル拡張子」の［編集］リンクをクリックします。

拡張子を追加するには、「検査対象外とするファイル拡張子」画面で［追加］をクリックし、拡張子を入力して［OK］をクリックします。［複数の値を入力］をクリックすると、改行、「,」（カンマ）、「;」（セミコロン）を使って、複数の拡張子を入力できます。

拡張子を編集するには、「検査対象外とするファイル拡張子」画面の拡張子一覧で対象の拡張子を選択し、［編集］をクリックします。

拡張子を削除するには、「検査対象外とするファイル拡張子」画面の拡張子一覧で対象の拡張子を選択し、［削除］をクリックします。

ワンポイント

拡張子の指定では、特殊記号の「*」（アスタリスク）および「?」（疑問符）を使用できます。アスタリスクは任意の文字列を、疑問符は任意の記号をそれぞれ表します。特殊記号を使って拡張子を指定する際は、正しい形式で入力してください。

●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を設定する場合は、「その他」セクションで設定できます。

すべてのオブジェクトをログに記録する	感染していないファイルを含め、検査されたすべてのファイルがログファイルに記録されます。例えば、アーカイブ内にマルウェアが見つかった場合は、アーカイブ内の駆除ファイルもログファイルに記録されます。
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、検査の速度を最高に保ちながら、最も効率的な検査レベルが確保されるように最適化されます。保護機能に応じた検査方法を使用して、高度な検査を行います。スマート最適化を無効にすると、ThreatSense コアのユーザー定義設定のみが検査に適用されます。

●制限

「制限」セクションでは、検査対象オブジェクトの最大サイズやアーカイブのネストレベルなどを指定できます。

オブジェクトの設定

既定のオブジェクトの設定	既定の設定でオブジェクトを検査するかどうかを設定します。無効にすると、「オブジェクトの最大サイズ」および「オブジェクトの最長検査時間（秒）」を設定できます。
オブジェクトの最大サイズ	検査対象のオブジェクトの最大サイズを設定します。最大サイズを設定すると、指定した値より小さいサイズのオブジェクトのみ検査されます。上級ユーザーがサイズの大きいオブジェクトを検査から除外する場合のみ、設定を変更してください。既定値は無制限、制限値は「0」～「2」GB です。
オブジェクトの最長検査時間（秒）	オブジェクト検査の最長時間を設定します。最長時間を設定すると、検査が終了しているかどうかにかかわらず、設定した時間が経過した時点で検査を停止します。既定値は無制限、制限値は「0」～「2147483647」秒です。

アーカイブ検査の設定

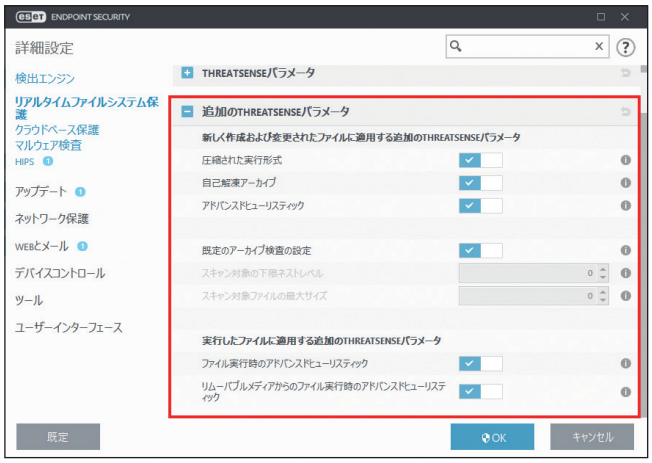
既定のアーカイブ検査の設定	既定の設定でアーカイブを検査するかどうかを設定します。無効にすると、「スキャン対象の下限ネストレベル」および「スキャン対象ファイルの最大サイズ」を設定できます。
スキャン対象の下限ネストレベル	検査するアーカイブのネストレベルを指定します。既定値は「10」、制限値は「0」～「20」です。
スキャン対象ファイルの最大サイズ	検査対象のアーカイブに含まれているファイルの最大サイズを指定します。既定値は無制限、制限値は「0」～「2」GB です。

！重　要

一般的な環境では既定値を変更しないことをお勧めします。

■追加の THREATSENSE パラメータ

「追加の THREATSENSE パラメータ」は、［リアルタイムファイルシステム保護］を選択した場合に設定できます。



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	新しく作成したファイルや修正したファイルは、既存ファイルより感染の可能性が高いため、検査パラメーターを追加して検査します。一般的な検出エンジンの検査方法と合わせて、アドバンスドヒューリスティックが使用されます。これにより、検出エンジンのアップデートの公開前でも新しいウイルスを検出でき、検出率が大幅に向上します。
圧縮された実行形式 **自己解凍アーカイブ** **アドバンスドヒューリスティック**	詳細については、「4.6.2　リアルタイムファイルシステム保護」の「■THREATSENSE パラメータ」を参照してください。
既定のアーカイブ検査の設定	自己解凍形式のファイル（SFX）および内部圧縮された実行形式のファイルを検査します。既定では、アーカイブは最大で 10 番目のネストレベルまで検査され、実際のサイズに関係なく検査されます。 詳細については、「4.6.2　リアルタイムファイルシステム保護」の「■THREATSENSE パラメータ」を参照してください。
実行したファイルに適用する追加の THREATSENSE パラメータ	既定では、アドバンスドヒューリスティック検査をファイル実行時に使用する設定となっています。この機能を使用するには、「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。

ワンポイント

「スマート最適化」ではリアルタイムファイルシステム保護のシステムへの負荷を最小限にするため、すでに検査されたファイルは変更がない限り、次回、検出エンジンが変更されるまで検査されません。検出エンジンがアップデートされた場合は、すぐにファイルが再検査されます。「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。

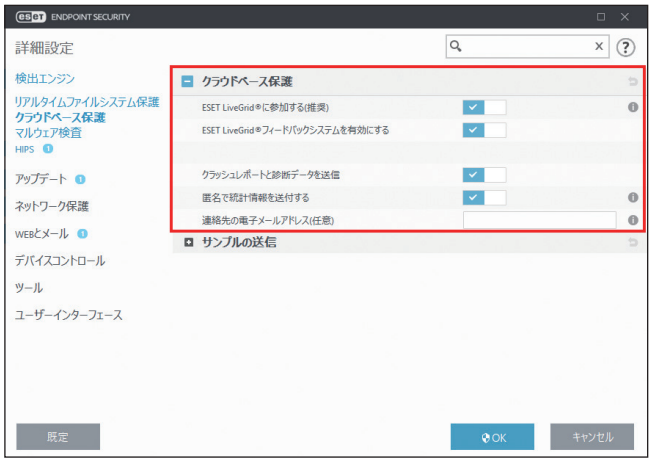
4.6.3 クラウドベース保護

ESET LiveGrid は、複数のクラウド技術で構成される高度な早期警告システムです。レピュテーションに基づいて新しく発生する脅威を検出し、ホワイトリストを使用して検査の精度を向上させます。新しい脅威の情報はリアルタイムでクラウドに送信されるため、ESET ウイルスラボでは迅速に対応することが可能となり、常に最大の保護を提供できます。ユーザーは、直接 ESET LiveGrid を操作したり、ESET LiveGrid に用意されている追加情報を閲覧して、稼働中のプロセスやファイルの評価を確認したりすることができます。
ESET Endpoint Security をインストールするときには、次のオプションのいずれかを選択します。

- ESET LiveGrid を無効にします。ESET Endpoint Security の機能は一切失われませんが、場合によっては、新しい脅威への対応が検出エンジンのアップデートよりも遅くなることがあります。
- ESET LiveGrid を有効にします。新しいウイルスと危険なコードが検出された場合、その情報を匿名で ESET に送信して詳しい解析を受けることができます。ESET は送信されたウイルスを解析することで、ウイルス検出機能を最新のものにできます。

■クラウドベース保護

ESET LiveGrid は、新しく検出されたウイルスに関連して、クライアントコンピューターに関する情報を収集します。この情報には、ウイルスが検出されたファイルのサンプルまたはコピー、ファイルのパス、ファイル名、日時、ウイルスがコンピューターに侵入したプロセス、コンピューターのオペレーティングシステムについての情報が含まれます。
「詳細設定」画面で、［クラウドベース保護］をクリックします。

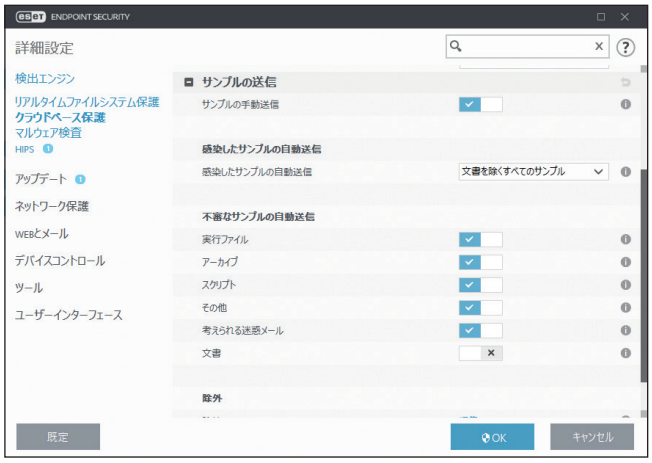


ESET LiveGrid に参加する（推奨）	有効にすると、新しいウイルスと危険なコードが検出された場所に関する匿名の情報を ESET のウイルスラボに提出します。
ESET LiveGrid フィードバックシステムを有効にする	ESET LiveGrid フィードバックシステムは、検査済みファイルをクラウドのホワイトリストおよびブラックリスト項目のデータベースと比較し、ESET マルウェア対策ソリューションの効率化を図ります。有効にすると、この機能が有効になります。
クラッシュレポートと診断データを送信	有効にすると、クラッシュレポートと診断データを ESET に送信します。
匿名で統計情報を送付する	有効にすると、脅威名、脅威を検出した日時、検出方法、関連付けられたメタデータ、製品バージョン、設定（システム情報を含む）など、新しく検出された脅威に関する情報を ESET が収集します。
連絡先の電子メールアドレス（任意）	不審なファイルに添付する連絡先の電子メールアドレスを入力します。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します。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。

ワンポイント

ESET LiveGrid を無効にしても、有効中に収集していたデータが残っている場合は ESET に送信されます。すべてのデータが送信されると、データはそれ以上収集されません。

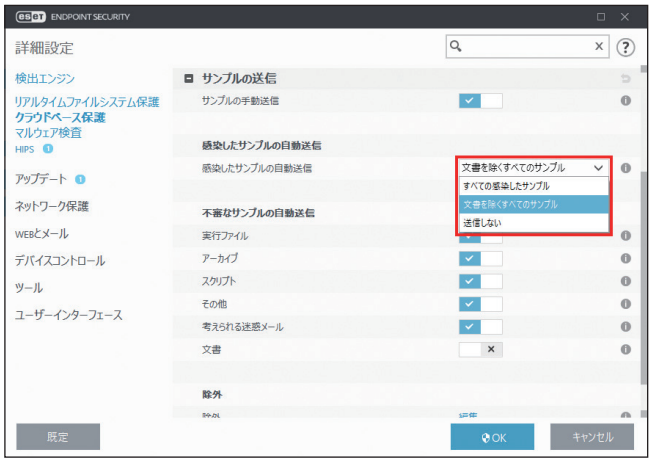
●サンプルの送信



「サンプルの手動送信」では、疑わしいファイルなどのサンプルを手動で ESET に送信するための項目を「ツール」メニューや［ツール］→［隔離］で表示される画面のコンテキストメニューに表示するかどうかの設定を行えます。既定では、この設定が有効に設定されており、「ツール」メニューをクリックして表示される項目内に［分析のためにサンプルを提出］が表示されます。また、［隔離］をクリックして、検出されたファイルを右クリックすると、コンテキストメニューに［分析のためにサンプルを提出］が表示されます。この設定を無効に設定すると、これらの項目が表示されなくなります。

感染したサンプルの自動送信

「感染したサンプルの送信」セクションでは、感染したサンプルを ESET に送信するときの設定を行えます。既定では、［文書を除くすべてのサンプル］が選択されており、文書を除くすべての感染サンプルが ESET に送信されます。［すべての感染したサンプル］を選択すると、感染したファイルすべてが送信されます。［送信しない］を選択すると、感染したファイルを ESET に送信しません。



不審なサンプルの送信

「不審なサンプルの送信」セクションでは、不審なファイルを ESET に送信するときの設定を行えます。

実行ファイル	「.exe」「.dll」「.sys」などの実行ファイルを送信します。
アーカイブ	「.zip」「.rar」「.7z」「.arch」「.arj」「.bizp2」「.gzip」「.ace」「.arc」「.cab」などのアーカイブファイルタイプを含みます。
スクリプト	「.bat」「.cmd」「.hta」「.js」「.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」「.swf」「.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	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 に送信します。
文書	アクティブなコンテンツがある Office 文書や PDF が含まれます。

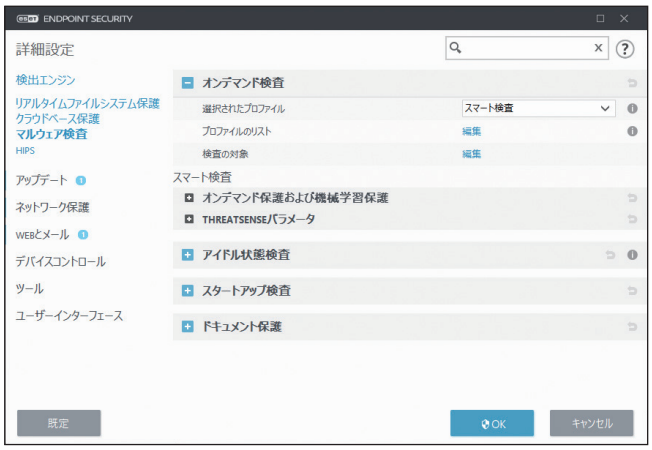
除外

除外を使用すると、特定のファイル / フォルダーを送信から除外できます。

除外	［編集］リンクをクリックすると「除外フィルタ」画面が表示され、特定のファイルまたはフォルダーを送信対象から除外できます。除隊対象となったファイルやフォルダーは、疑わしいコードを含んでいても、ESET のウイルス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拡張子（.doc など）は、既定で登録されています。必要に応じて、除外するファイルやフォルダーを追加できます。ドキュメントやスプレッドシートなど、機密情報が含まれる可能性があるファイルを除外する場合に便利です。
サンプルの最大サイズ（MB）	ESET に送信するサンプルの最大ファイルサイズを設定します。規定では「64MB」が設定されています。

4.6.4 マルウェア検査

メインメニューの「マルウェア検査」から各検査の設定が行えます。各検査の詳細については、「4.1 コンピューターの検査」を参照してください。



■オンデマンド検査

選択されたプロファイル	定義済みの検査プロファイルの選択をドロップダウンメニューから行えます。プロファイルは、オンデマンドスキャナーが使用する特定のパラメーターセットです。
プロファイルのリスト	［プロファイルのリスト］の横の［編集］をクリックすると、「プロファイルマネージャ」画面が表示され、新しいカスタム検査プロファイルを作成できます。「プロファイルマネージャ」画面には、既存の検査プロファイルが一覧で表示され、新しいプロファイルを作成するための入力欄があります。入力欄に新しく作成するプロファイル名を入力し、［追加］>［OK］をクリックすると、プロファイル名が登録されます。
検査の対象	検査対象を選択できます。特定の対象のみを検査する場合は、［検査の対象］の横の［編集］をクリックすると、「プロファイルターゲット」画面が表示されます。「プロファイルターゲット」画面の⚙をクリックし、ドロップダウンメニューから事前定義されている検査対象を選択するか、フォルダー（ツリー）構造から検査対象を選択します。検査対象の選択の詳細については、「4.1.2 カスタム検査」の「■カスタム検査の設定」の「●検査の対象の選択」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

マルウェア検査のスキャナー設定は、「リアルタイム保護および機械学習保護」カテゴリとオンデマンド検査の「オンデマンド保護および機械学習保護」カテゴリで設定できます。既定では、[マルウェア検査] > [オンデマンド検査] > [オンデマンド保護および機械学習保護] カテゴリで「リアルタイムファイルシステム保護設定を使用」が有効に設定されています。この設定が有効なときには、関連するオンデマンド検査の設定が「リアルタイム保護および機械学習保護」カテゴリから継承されます。

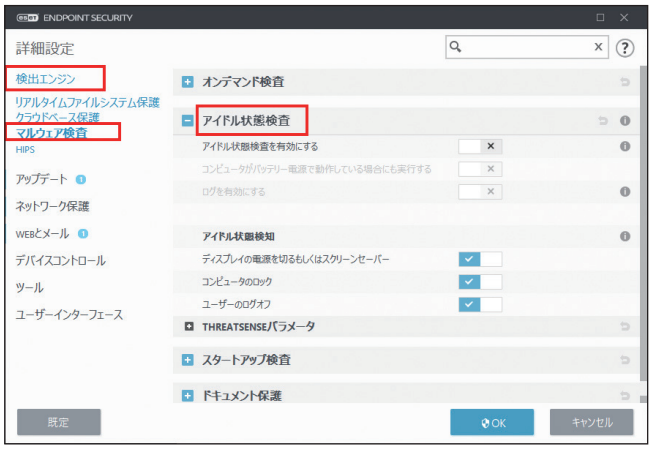
マルウェア検査のスキャナー設定を独自に設定したいときは、「リアルタイムファイルシステム保護設定を使用」を無効に設定し、「マルウェア」「望ましくない可能性のあるアプリケーションアプリケーション」「不審なアプリケーション」「安全ではない可能性があるアプリケーション」の各カテゴリのしきい値を設定してください。また、しきい値の設定の詳細については、「4.6.1.1　リアルタイム保護および機械学習保護」の「■報告設定」および「■保護設定」を参照してください。

● THREATSENSE パラメータ

[THREATSENSE パラメータ] をクリックすると、オンデマンド検査の検査パラメーターを設定できます。詳細については、「4.6.2　リアルタイムファイルシステム保護」の「■ THREATSENSE パラメータ」を参照してください。

■アイドル状態検査

アイドル状態検査を設定するには、メインメニューの［設定］>［詳細設定］をクリックするか、【F5】キーを押して「詳細設定」画面を表示し、［検出エンジン］>［マルウェア検査］>［アイドル状態検査］をクリックします。



「アイドル状態検査を有効にする」を有効にすると、アイドル状態時にすべてのローカルドライブでコンピューターの検査が実行されます。

既定では、アイドル状態検査はバッテリー電源で動作しているとき（ノートパソコンなど）は実行されません。バッテリー電源で動作しているときでもアイドル状態検査を実行するには、「コンピュータがバッテリー電源で動作している場合にも実行する」を有効にします。

ログファイルにアイドル状態検査の結果を記録するには、「ログを有効にする」を有効にします。記録されたログは、メインメニューの［ツール］>［ログファイル］をクリックし、ドロップダウンメニューから［コンピューターの検査］を選択すると確認できます。

●アイドル状態検知

コンピューターが以下の状態の場合に、アイドル状態検査を開始するように設定できます。

- 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

● THREATSENSE パラメータ

［THREATSENSE パラメータ］をクリックすると、アイドル状態検査の検査パラメーターを設定できます。詳細については、「4.6.2　リアルタイムファイルシステム保護」の「■ THREATSENSE パラメータ」を参照してください。

■スタートアップ検査

スタートアップ検査では、システムの起動時または検出エンジンのアップデート時に、ファイルの検査を実行します。スタートアップ検査は、［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で起動します。スタートアップ検査の設定を変更するには、メインメニューの［ツール］>［スケジューラ］をクリックし、［システムのスタートアップファイルのチェック］を選択して［編集］をクリックします。
スケジューラタスクの作成と管理の詳細については、「4.4.7　スケジューラ」の「■新しいタスクの追加」を参照してください。

●システムのスタートアップファイルのチェック

検査の対象

スタートアップ検査のスケジュールタスクを作成するときに、検査の対象を指定します。選択できる検査の対象は次のとおりです。

すべての登録されたファイル	登録されたすべてのファイルを検査します。検査対象のファイル数が最大となる検査レベルです。
使用頻度が低いファイル	使用頻度が低いファイルも含めて検査します。
一般的に使用されるファイル	一般的に使用されるファイルを検査します。
使用頻度が高いファイル	使用頻度が高いファイルに絞って検査します。
最も多く使用されるファイルのみ	最も使用頻度が高いファイルのみ検査します。検査対象のファイル数が最小となる検査レベルです。
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くても実行が許可されるファイルを検査します（サービス、ブラウザー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ー、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実行が許可されるファイルを検査します（特定のユーザーだけが実行するファイル、HKEY_CURRENT_USER¥ SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run にあるファイル）

検査対象のファイルの一覧は、グループごとに固定されます。

検査の優先度

スタートアップ検査のスケジュールタスクを作成するときに、検査の優先度を指定します。選択できる優先度は次のとおりです。

- アイドル時：システムが待機時のみ、スタートアップ検査が実行されます。
- 最低：システム負荷が最低の場合に、スタートアップ検査が実行されます。
- 低：システム負荷が低い場合に、スタートアップ検査が実行されます。
- 通常：システム負荷が平均的な場合に、スタートアップ検査が実行されます。

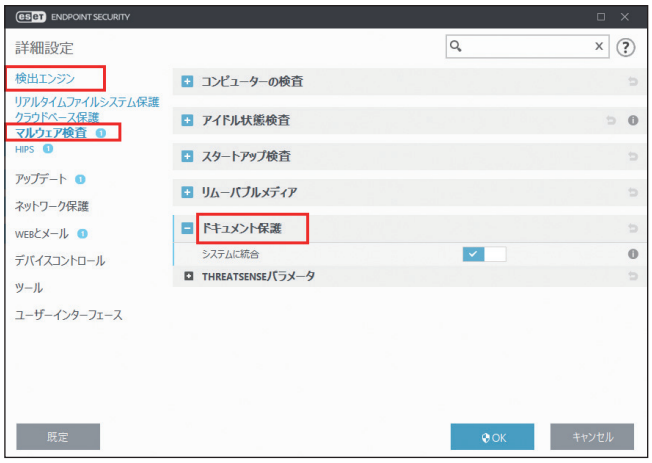
■THREATSENSE パラメータ

［THREATSENSE パラメータ］をクリックすると、スタートアップ検査の検査パラメーターを設定できます。詳細については、「4.6.2　リアルタイムファイルシステム保護」の「■ THREATSENSE パラメータ」を参照してください。

■ドキュメント保護

ドキュメント保護では、Microsoft Office ドキュメントを開く前の検査、および Internet Explorer によって自動的にダウンロードされたファイル（Microsoft ActiveX コンポーネントなど）の検査を行います。リアルタイムファイルシステム保護にドキュメント保護を加えることでさらに強力な保護を提供します。ただし、ドキュメント保護を使用するとコンピューターのパフォーマンスが低下することがあります。大量の Microsoft Office ドキュメントを扱わない場合は無効にすることをお勧めします。

ドキュメント保護を変更するには、［詳細設定］をクリックするか、【F5】キーを押して「詳細設定」画面を表示し、［検出エンジン］>［マルウェア検査］>［ドキュメント保護］をクリックします。



ドキュメント保護の設定は、［システムに統合］オプションで有効／無効を設定できます（既定ではオフ）。
ドキュメント保護は、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有効になります。

● THREATSENSE パラメータ

［THREATSENSE パラメータ］をクリックすると、ドキュメント保護の検査パラメーターを設定できます。詳細については、「4.6.2　リアルタイムファイルシステム保護」の「■ THREATSENSE パラメータ」を参照してください。

4.6.5 HIPS

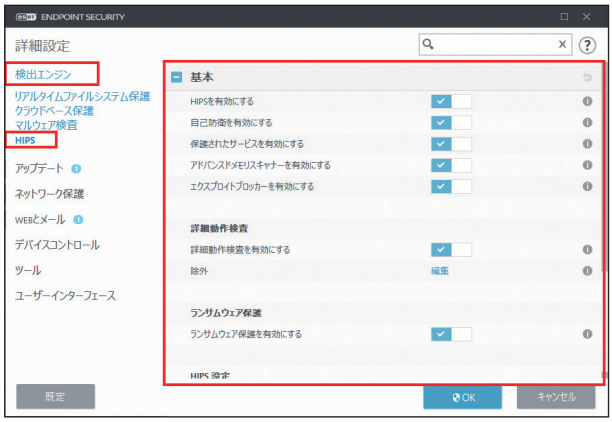
HIPS（ホストベース進入防止システム）は、コンピューターに悪影響を与えようとする活動やマルウェアからシステムを保護します。HIPS は、高度な動作分析とネットワークフィルタリングの検出機能を連動させて、実行中のプロセス、ファイル、レジストリキーを監視します。HIPS はリアルタイムファイルシステム保護やファイアウォールとは異なります。

■基本

HIPS を設定するには、メインメニューの［設定］>［詳細設定］をクリックするか、【F5】キーを押して「詳細設定」画面を表示し、［検出エンジン］>［HIPS］>［基本］をクリックします。
また、HIPS の有効／無効の設定状態は、メインメニューの［設定］>［コンピュータ］タブの［HIPS］に表示されます。

！重　要

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。



HIPS を有効にする	ESET Endpoint Security では既定で HIPS が有効です。HIPS をオフにすると、自己防衛や保護されたサービス、アドバンスドメモリスキャナー、エクスプロイトブロッカーなどの HIPS 機能が無効になります。HIPS のオン／オフの設定変更は、オペレーティングシステムを再起動すると有効になります。
自己防衛を有効にする	ESET Endpoint Security には、悪意のあるソフトウェアによってウイルス・スパイウェア対策の保護機能が破損されたり無効化されたりしないようにする HIPS の一部として、自己防衛技術が組み込まれています。自己防衛は、重要なシステムおよび ESET のプロセス、レジストリキー、およびファイルを改ざんから防止します。インストール時には、ESET Management エージェントも保護されます。自己防衛の有効／無効の設定変更は、オペレーティングシステムを再起動すると有効になります。
保護されたサービスを有効にする	ESET Service（ekrn.exe）の保護を有効にします。有効にすると、サービスは保護された Windows プロセスとして起動し、マルウェアによる攻撃を防御します。このオプションは、Windows 8.1 および Windows 10 で使用できます。
アドバンスドメモリスキャナーを有効にする	アドバンスドメモリスキャナー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、「6.4.2　アドバンスドメモリスキャナー」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、「6.4.1　エクスプロイトブロック」を参照してください。

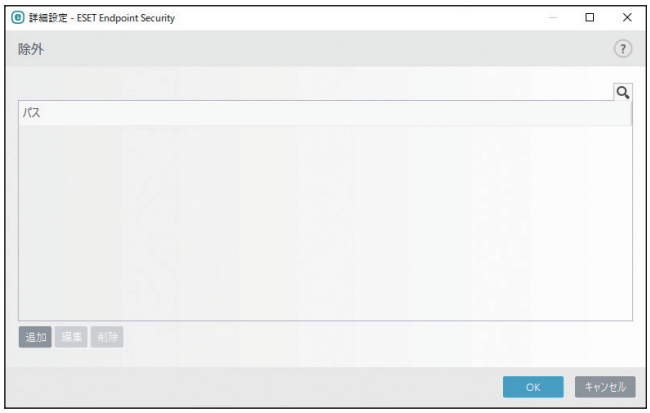
●詳細動作検査

- **詳細動作検査を有効にする**

「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の設定です。この HIPS の拡張機能は、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。

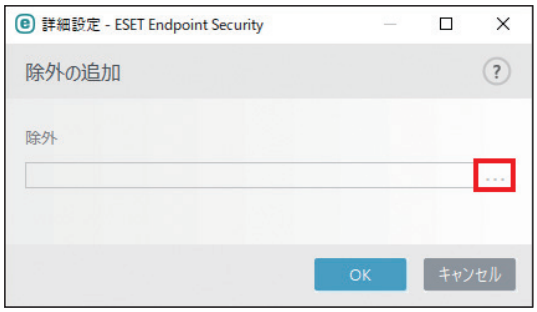
- **除外**

「詳細動作検査」カテゴリの除外では、HIPS 詳細動作検査から除外するプロセスを追加できます。 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。除外を作成したいときは、［設定］>［詳細設定］>［検出エンジン］>［HIPS］>「除外」の［編集］とクリックし、除外したいプロセスをリストに追加します。除外したいプロセスの追加は、［追加］ボタンをクリックして、オブジェクトのパスを入力するか、ツリー構造でパスを選択します。



パス	除外するオブジェクトのパスが表示されます。
追加	除外するオブジェクトのパスを追加します。
編集	選択したエントリーを編集します。
削除	選択肢たエントリーを削除します。また、CTRL キー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。

除外したいプロセスを追加するには、「除外」画面で［追加］ボタンをクリックして、「除外の追加」ダイアログウィンドウを表示し、オブジェクトのパスを入力するか、…をクリックしてツリー構造からパスを選択します。



●ランサムウェア保護

ランサムウェア保護は HIPS 機能の一部として動作し、ランサムウェアと疑わしき動作を検知して、ブロックすることでコンピューターを保護します。ランサムウェア保護を実行するには、LiveGrid 評価システムを有効にする必要があります。詳細については、「6.4.7　ランサムウェアシールド」を参照してください。

HTTPS 設定

フィルタリングモード

フィルタリングモードには、次の 5 つのモードがあります。

ルール付き自動モード	システムを保護するためにあらかじめ定義されている操作を除いて、すべての操作が有効です。
スマートモード	不審なイベントに関する通知だけを表示します。
対話モード	ユーザーに操作の選択を要求します。
ポリシーベースモード	ルールに従って動作します。ルールにない実行操作はブロックされます。
学習モード	有効にすると、操作の後にルールが作成されます。学習モードで作成されたルールは、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。[学習モード] を選択すると、「学習モードの終了時刻」と「学習モードの期限切れの後に設定されるモード」を設定できます。「学習モードの終了時刻」では、学習モードの有効期間を指定してください。学習モードの有効期間が終了したら、「学習モードの期限切れの後に設定されるモード」で設定したフィルタリングモードが設定されます。「学習モードの期限切れの後に設定されるモード」では、「ルール付き自動モード」「スマートモード」「対話モード」「ポリシーベースモード」「ユーザーに確認する」の中から選択できます。
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戻るフィルタリングモードを定義します。

ルール

HIPS 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［編集］リンクをクリックすると、「HIPS ルール」画面が表示され、ルールの作成、編集、削除ができます。

ルールのアクションを［確認］にした場合は、ルールに適合するたびに確認画面が表示され、ユーザーは操作を［遮断］するか［許可］するかを選択できます。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。

確認画面では、HIPS が検出した新しいアクションと、アクションの条件を基にルールを作成できます。詳細なパラメーターは、［詳細表示］をクリックすると表示できます。
［ルールの作成］をチェックすると、ルールを作成できます。確認画面で作成したルールは、手動で作成したルールと優先度は同じです。このため、確認画面を表示させた場合より汎用的に扱われます。確認画面からルールを作成した場合でも、同じ操作で確認画面を表示することができます。
［このプロセスに対するアクションを一時的に記憶する］をチェックすると、操作に対する許可／拒否のアクションが一時的に記憶され、同じ操作によって確認画面が表示されるたびに同じアクションが使用されます。一時的に記憶されたアクションは、ルールまたはフィルタリングモードの変更、HIPS 機能のアップデート、システムの再起動のいずれかを行うと削除されます。

アプリケーションの動作制限設定

例として、アプリケーションの不要な動作を制限する方法について説明します。

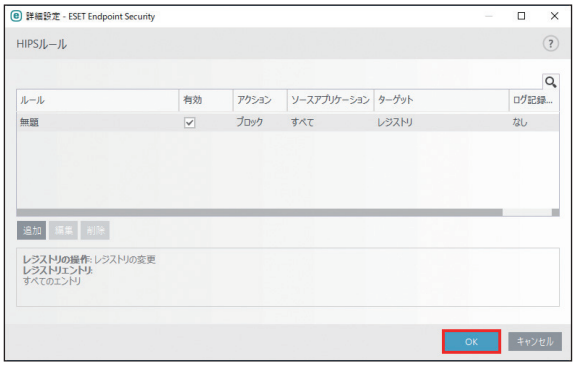
操作手順

1. ［HIPS］＞［基本］＞ルールの［編集］をクリックします。
2. ［追加］をクリックします。
3. 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］を選択します。
4. 動作影響から制限をしたい項目を選択します。
   「ユーザーに通知」を有効にすると、ルールが適用されるたびに通知が表示されます。

   ワンポイント
   ルールを適用する対象として選択した項目に応じて、次に表示される設定画面の内容が変化します。
5. ［次へ］をクリックします。
   「ソースアプリケーション」画面が表示されます。
6. ドロップダウンメニューから項目を選択します。
   すべてのアプリケーションに新しいルールが適用されます。
7. ［次へ］をクリックします。
8. 制限を行いたい項目を有効にします。
   各項目の説明は製品ヘルプに記載されています。【F1】キーを押すと表示されます。
9. ［次へ］をクリックします。
10. ドロップダウンメニューから項目を選択し、［追加］をクリックして保護する 1 つ以上のアプリケーションを追加します。
11. ［終了］をクリックします。

続く

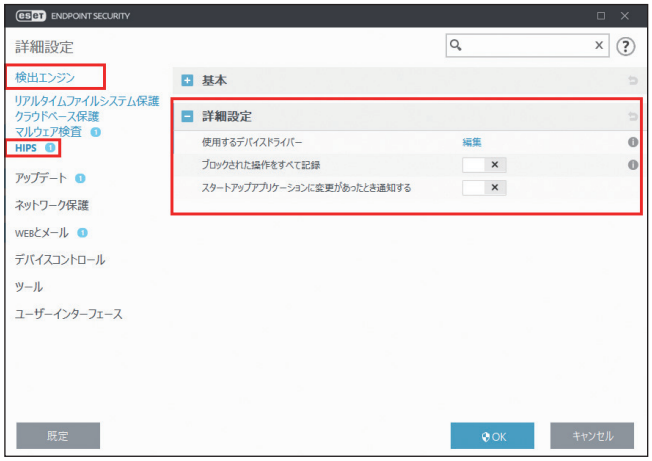
⑫［OK］をクリックして作成したルールを保存します。



■詳細設定

詳細設定では、アプリケーションの動作をデバッグおよび分析する機能を設定できます。

HIPS の詳細を設定するには、メインメニューの［設定］>［詳細設定］をクリックするか、【F5】キーを押して「詳細設定」画面を表示し、［検出エンジン］>［HIPS］>［詳細設定］をクリックします。

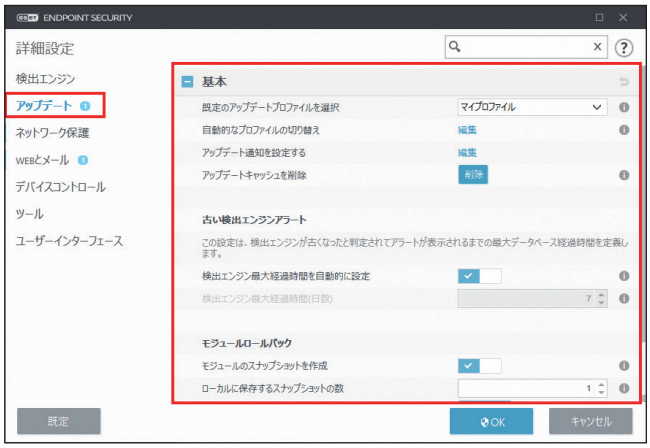


使用するデバイスドライバー	ユーザールールでブロックされない限り、設定されたフィルタリングモードに関係なく、選択したドライバーは常に使用されます。
ブロックされた操作をすべて記録	ブロックされたすべての操作がログに記録されます。
スタートアップアプリケーションに変更があったとき通知する	アプリケーションがシステムスタートアップに追加または削除されるたびに、デスクトップ右下の情報メッセージで通知されます。

4.6.6 アップデート

アップデートの設定を行うには、メインメニューの［設定］>［詳細設定］をクリックするか、【F5】キーを押して「詳細設定」画面を表示し、［アップデート］をクリックします。アップデートの設定では、アップデートサーバーやアップデートサーバーの認証データなど、アップデートファイルの送信元の情報を指定します。

■基本



既定のアップデートプロファイルを選択	現在使用中のアップデートプロファイルが、ドロップダウンメニューに表示されます。ドロップダウンメニューから使用するプロファイルを変更できます。	
自動的なプロファイルの切り替え	自動プロファイル切り替え機能により、接続したネットワークに応じてアップデートプロファイルを自動切り替えできます。接続したネットワークに応じてアップデートプロファイルを変更したいときは、［編集］をクリックします。「自動的なプロファイルの切り替え」画面が表示れるので、アップデートプロファイルを変更したいネットワークをクリックし、［編集］をクリックすると、選択したネットワークのアップデートプロファイルを選択できます。	
アップデート通知を設定する	［編集］をクリックすると、表示されるアプリケーション通知を選択できます。通知をデスクトップに表示するか、電子メールで送信するかを選択できます。詳細については、「4.6.18　通知」の「●アプリケーション通知」を参照してください。	
アップデートキャッシュを削除	検出エンジンのアップデート時に問題が発生した場合は、［削除］をクリックして、一時アップデートファイルとキャッシュを削除します。	
古い検出エンジンアラート	検出エンジンが古くなったことを通知するまでの時間（日数）を設定できます。既定値は「7」日、制限値は「1」～「365」日です。	
	検出エンジン最大経過時間を自動的に設定	この設定をオンにすると、ESET の推奨値が検出エンジン最大経過時間として設定されます。この設定の既定値は、オンです。オフに設定すると、「検出エンジン最大経過時間（日数）」を設定できます。
	検出エンジン最大経過時間（日数）	この設定は、「検出エンジン最大経過時間を自動的に設定」がオフに設定されているときに設定できます。既定値は「7」日に設定されており、「1」～「365」日の中から任意の日数を設定できます。

モジュールロールバック	検出エンジン／プログラムコンポーネントの新規アップデートが不安定な場合や、破損している疑いのある場合は、前のバージョンにロールバックし、ロールバックより後のアップデートを無効にできます。	
	モジュールのスナップショットを作成	有効にすると、検出エンジンとプログラムコンポーネントのスナップショットを作成します。
	ローカルに保存するスナップショットの数	コンピューターに保存するスナップショットの数を設定します。既定値は「1」、制限値は「1」～「99」です。
	前のモジュールにロールバック	［ロールバック］をクリックすると、使用できる最も古いスナップショットにロールバックし、アップデートを休止する期間をドロップダウンメニューから選択できます。アップデートを有効にするには、［アップデートを許可］をクリックします。

！重　要

アップデートファイルを正しくダウンロードするには、すべてのアップデートパラメーターを正しく設定してください。ファイアウォールを使用している場合は、ESET プログラムのインターネットとの通信（HTTP 通信）が許可されていることを確認してください。

●アップデートプロファイル

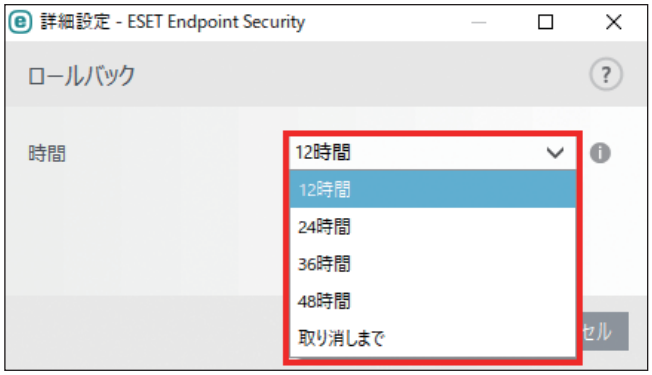
様々なアップデート設定およびアップデートタスクを、アップデートプロファイルとして作成することができます。アップデートプロファイルを作成すると、インターネット接続のプロパティが常に変わるデバイスの使用時に、代替プロファイルをすぐに設定できるので便利です。

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［編集］リンクをクリックし、「プロファイル名」フィールドにプロファイルの名前を入力して、［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で新しく作成したプロファイルを選択すると、そのプロファイルに対してアップデートの設定やアップデートタスクの作成ができるようになります。

●モジュールロールバック

「詳細設定」画面で［アップデート］>「前のモジュールにロールバック」の［ロールバック］をクリックすると、「ロールバック」画面が表示されます。「ロールバック」画面では、検出エンジンおよびプログラムコンポーネントのアップデートを休止する期間を選択します。



手動で解除するまで、アップデート機能を無期限に休止する場合は、［取り消しまで］を選択します。アップデートの無期限休止には潜在的なセキュリティリスクがあるため、［取り消しまで］の選択は推奨しません。

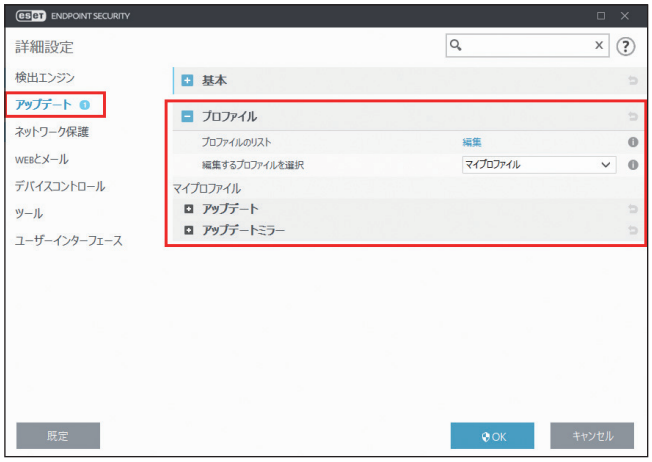
ロールバックを実行すると、検出エンジンのバージョンは使用できる最も古いバージョンにダウングレードされ、ローカルのクライアントコンピューターにスナップショットとして保存されます。

例

検出エンジンの最新バージョンは 10646 番で、検出エンジンのスナップショットとして 10645 番と 10643 番が保存されているとします。

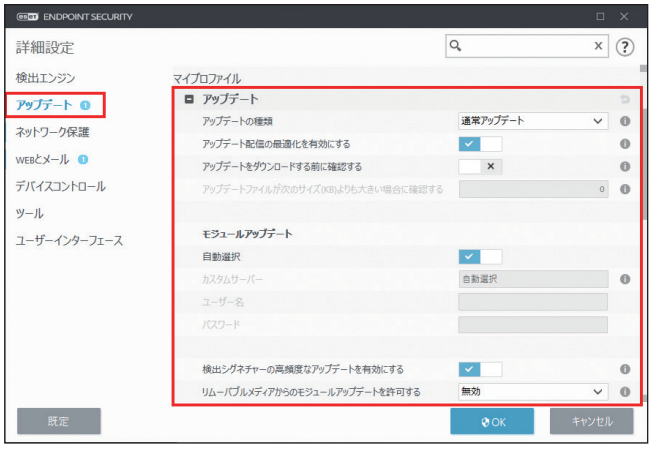
「ローカルに保存するスナップショットの数」が「2」に設定されている状態で［ロールバック］をクリックすると、検出エンジン（プログラムモジュールを含む）は、10643 番に復元されます（復元には時間がかかることがあります）。メインメニューの［アップデート］をクリックして、検出エンジンのバージョンがダウングレードされたことを確認します。クライアントコンピューターの電源がオフになっていて、10644 番をダウンロードする前に新しいアップデートが利用できるようになった場合、10644 番への復元はできません。

■プロファイル



プロファイルのリスト	プロファイルの追加や削除ができます。新しいプロファイルを作成するには、［編集］リンクをクリックし、空白フィールドにプロファイル名を入力して、［追加］をクリックします。
編集するプロファイルを選択	［アップデート］および［アップデートミラー］の設定を編集するプロファイルを選択します。

●アップデート



アップデートの種類	既定では「通常アップデート」に設定されており、最低限の通信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］を選択すると、内部テストを経て、近いうちに一般に公開されるアップデートファイルをダウンロードします。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が、「テストモード」でダウンロードしたアップデートファイル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絶対に選択しないでください。 ［遅延アップデート］を選択すると、12 時間以上遅延している最新バージョンの検出エンジン（実際の環境でテスト済みで、安定しているとみなされる検出エンジン）を提供する特別なサーバーから、アップデートファイルをダウンロードできます。
アップデート配信最適化を有効にする	この設定を有効にすると、CDN（コンテンツ配信ネットワーク）からアップデートファイルをダウンロードできます。この設定を無効にすると、専用 ESET アップデートサーバーが過負荷状態になったときに、ダウンロードが中断され、速度が低下する場合があります。ファイアウォールによって ESET アップデートサーバー IP アドレスへのアクセスのみに制限されているときや、CDN サービスへの接続が動作していないときに無効にすると役立ちます。
アップデートをダウンロードする前に確認する	有効にすると、新しいアップデートが利用できるようになったときに、情報メッセージが表示されます。情報メッセージは、アップデートファイルのサイズが「アップデートファイルが次のサイズ（kB）よりも大きい場合に確認」で指定した値よりも大きい場合に表示されます。
アップデートファイルが次のサイズよりも大きい場合に確認する	新しいアップデートが利用できるようになったときに、情報メッセージを表示するアップデートファイルのサイズを指定します。既定値は「0」KB、制限値は「0」～「2000000」KB です。

! 重　要

ESET Endpoint Security V7 をミラーサーバー経由でアップデートする場合は、V7 に対応したミラーツールを使用するか、ESET Endpoint アンチウイルス /ESET Endpoint Security V7 でミラーサーバーを作成する必要があります。

モジュールアップデート

モジュールアップデートに利用するアップデートサーバーの設定を行います。アップデートサーバーとは、アップデートファイルが保存されている場所です。既定では、「自動選択」が有効になっています。ESET サーバーを使用するときには、既定のままにすることをお勧めします。

既定以外のアップデートサーバーを使用する場合は、「自動選択」を無効にして、「カスタムサーバー」フィールドにアップデートサーバーパスを入力します。

- ローカルの HTTP サーバーを使用する場合
  http://< クライアントコンピューター名または IP アドレス >:2221
- SSL を利用するローカルの HTTP サーバーを使用する場合
  https://< クライアントコンピューター名または IP アドレス >:2221
- ローカル共有フォルダーを使用する場合
  ￥￥< クライアントコンピューター名または IP アドレス > ￥< 共有フォルダー > ￥shared_folder

検出シグネチャーの高頻度なアップデートを有効にする

検出シグネチャーは 10 分間隔でアップデートされます。このアップデートは、スケジューラのアップデートタスク無効時も動作します。この設定を無効にすると、検出率に悪影響を及ぼす可能性があります。

リムーバブルメディアからのモジュールアップデートを許可する
リムーバブルメディアのルートにアップデートミラーで作成されたファイルが含まれている場合は、そのリムーバブルメディアからアップデートできます。［自動］が選択されている場合は、バックグラウンドでアップデートが実行されます。［常に確認する］が選択されている場合は、確認のアップデートダイアログが表示されます。

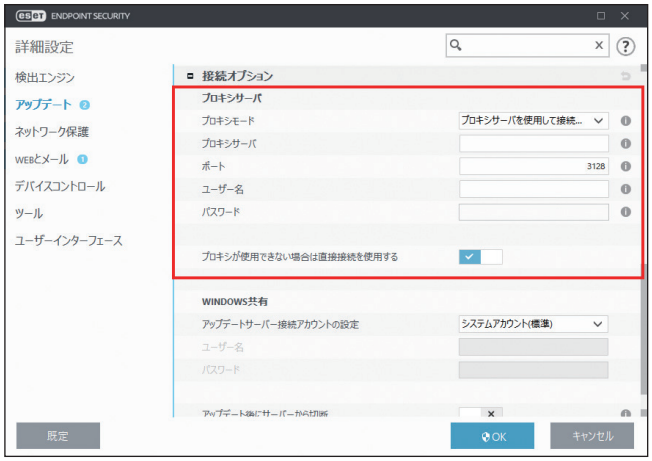
プログラムコンポーネントのアップデート
プログラムコンポーネントのアップデートでは、ESET 社のアップデートサーバーに最新バージョンへのアップデートファイルが使用可能になったときの動作をあらかじめ設定できます。プログラムコンポーネントのアップデートによって、ESET Endpoint Security がバージョンアップされて新しい機能が提供されたり、既存の機能が変更されたりします。

! 重　要
プログラムコンポーネントのアップデートを利用するためには、ESET 社のリポジトリサーバーに接続できる環境が必要です。ミラーサーバーからモジュールをアップデートする設定にしていても、プログラムコンポーネントのアップデートを利用するために、ESET 社のリポジトリサーバーに接続できる必要があります。必要に応じてプロキシサーバーの設定を行ってください。
また、プログラムコンポーネントアップデートはプログラムのアップデート後は再起動が必要になるため、ESET Endpoint Security の運用環境に応じてアップデートモードを設定してください。

アップデートモード	アップデート前に確認する	プログラムコンポーネントのアップデートが利用可能になったとき、「現在の状況」と「アップデート」に新しいアップデートが利用できることが表示されます。
	自動アップデート	プログラムコンポーネントのアップデートファイルが自動的にダウンロードされてインストールされます。EULA に同意するかどうかのポップアップ通知が表示されます。
	アップデートしない	既定の設定です。プログラムコンポーネントのアップデートは実行されません。
カスタムサーバー	プログラムコンポーネントのアップデートで利用するアップデートサーバーのパスを入力します。HTTP(S) リンク、SMB ネットワーク共有パス、ローカルディスクドライブ、またはリムーバブルメディアのパスを入力します。ネットワークドライブの場合、マッピングされたドライブ文字の代わりに、UNC パスを利用できます。	
ユーザー名	アップデートサーバーでユーザー認証を行っている場合は、認証に利用するユーザー名を入力します。ユーザー認証を行っていない場合は、空欄にしておきます。	
パスワード	アップデートサーバーでユーザー認証を行っている場合は、認証に利用するパスワードを入力します。ユーザー認証を行っていない場合は、空欄にしておきます。	

●接続オプション
「接続オプション」では、選択しているアップデートプロファイルのプロキシサーバーの設定や Windows ベースのオペレーティングシステムで運用しているローカルサーバーにアクセスするための認証用のアカウントを設定します。

プロキシサーバー

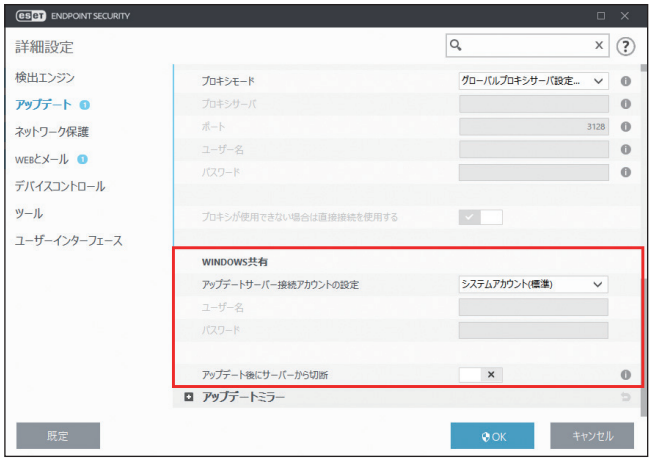


プロキシモード	プロキシサーバを使用しない	アップデートにプロキシサーバーを使用しません。
	プロキシサーバを使用して接続する	アップデートにプロキシサーバーを使用します。選択すると「カスタムプロキシサーバー」の設定項目が有効になるので、必要に応じて、プロキシサーバー、ポート（既定は「3128」）、ユーザー名、パスワードを設定します。また、［プロキシが利用できない場合は直接接続を使用する］を有効に設定すると、アップデート時に設定したプロキシサーバーが利用できない場合に、プロキシサーバーをバイパスしてアップデートします。 プロキシサーバーは、次のような場合に設定します。 • 「詳細設定」画面の［ツール］>［プロキシサーバ］で設定したプロキシサーバーとは異なるプロキシサーバーを使用してアップデートする場合 • アップデートファイルの取得のみプロキシサーバーを使用する場合 • クライアントコンピューターがプロキシサーバーを介してインターネットに接続している場合 プロキシサーバーの設定は、ESET Endpoint Security のインストール時に Internet Explorer から取得されます。ISP を変更するなど、インストール後に変更した場合は、HTTP プロキシの設定が正しいかどうか確認してください。設定が正しくない場合、プロキシサーバーに接続できません。
	グローバルプロキシサーバ設定を使用する	既定の設定です。「詳細設定」画面の［ツール］>［プロキシサーバ］で設定されているプロキシサーバーを使用します。

！重　要

「カスタムプロキシサーバー」の「ユーザー名」や「パスワード」などの認証データは、プロキシサーバーへのアクセスに使用されます。「ユーザー名」や「パスワード」は、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ときにパスワードが必要な場合のみ入力してください。ここで入力するのは、ESET Endpoint Security のユーザー名とパスワードではありません。

WINDOWS 共有



アップデートサーバー接続アカウントの設定	システムアカウント（標準）	システムアカウントを使用して認証する場合に選択します。
	現在のユーザー	現在ログインしているユーザーアカウントを使用して認証する場合に選択します。ログインしているユーザーがいない場合、ESET Endpoint Security はアップデートサーバーに接続できません。
	指定したユーザー	特定のユーザーアカウントを使用して認証する場合に選択します。システムアカウントでアップデートサーバーの接続に失敗した場合に選択してください。ユーザーアカウントは、ローカルサーバー上のアップデートファイルディレクトリーにアクセスできなければなりません。アクセスできないユーザーアカウントの場合は、アップデートサーバーに接続できません。
アップデート後にサーバーから切断	有効にすると、アップデートファイルのダウンロード後にサーバーとの接続を強制的に切断します。	

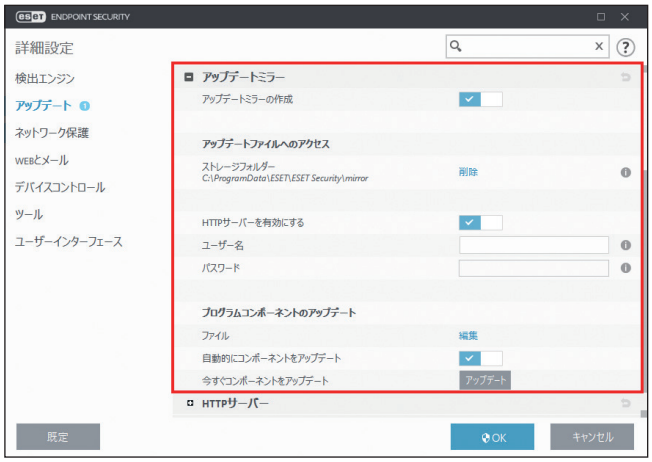
●アップデートミラー

アップデートミラーを作成すると、ネットワーク内の他のクライアントコンピューターをアップデートするための、アップデートファイルのコピーを作成することができます。アップデートミラーにアップデートファイルのコピーを作成すると、コンピューターごとに繰り返しアップデートファイルをダウンロードする必要がないので便利です。また、アップデートファイルがローカルのアップデートミラーにコピーされ、すべてのクライアントコンピューターに配信されるため、通信トラフィックの負荷が分散され、インターネット接続の帯域幅を節約できます。

ワンポイント

アップデートミラーへのアクセス方法の詳細については、「●アップデートミラーからのアップデート」を参照してください。アップデートミラーにアクセスする基本的な方法は、アップデートファイルを格納しているフォルダーを共有ネットワークフォルダーとして表示するか、クライアントコンピューターから HTTP サーバー上にあるアップデートミラーにアクセスするか、の 2 つです。

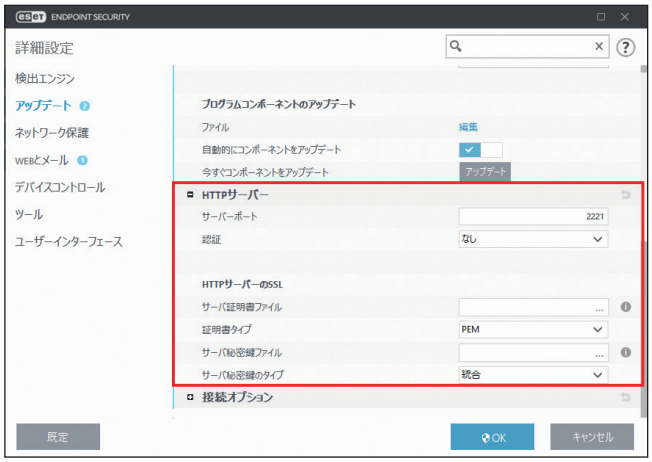
「詳細設定」画面で［アップデート］>［プロファイル］>［アップデートミラー］をクリックすると、「アップデートミラーの作成」画面が表示されます。



アップデートミラーの作成	有効にすると、アップデートファイルへのアクセス方法やミラー化されたファイルへのパスなどの設定項目が有効になり、アップデートミラーを作成できるようになります。	
アップデートファイルへのアクセス	ストレージフォルダー	アップデートファイルを保存するフォルダーを指定します。既定では「C:¥ProgramData¥ESET¥ESET Endpoint Security¥mirror」が保存先に指定されています。ローカルコンピューターの他のフォルダーまたは共有ネットワークフォルダーに変更するには、［削除］リンクをクリックしてフォルダーの指定を削除してから、［編集］リンクをクリックしてフォルダーを指定します。
	HTTP サーバーを有効にする	有効にすると、内臓の HTTP サーバー経由でアップデートファイルにアクセスできます。認証情報は必要ありません。
	ユーザー名／パスワード	アップデートファイルが保存されているフォルダーへのアクセスに認証が必要な場合は、「ユーザー名」と「パスワード」を入力します。 指定されている保存先フォルダーが、Windows オペレーティングシステムで運用しているネットワークディスクにある場合は、指定されているフォルダーに対する書き込み権限があるユーザー名とパスワードを入力する必要があります。ユーザー名は、「< ドメイン >/< ユーザー >」または「< ワークグループ >/< ユーザー >」という形式で入力します。パスワードは必ず指定してください。
プログラムコンポーネントのアップデート	ファイル	［編集］ファイルをクリックすると、ダウンロードするアップデートファイルの言語を指定できます。ミラーサーバーでサポートされている言語を選択してください。
	自動的にコンポーネントをアップデート	有効にすると、プログラムコンポーネントが自動的にアップデートされ、新しい機能のインストールと既存の機能のアップデートが行われます。無効にすると、プログラムコンポーネントをアップデートするかどうかを選択できます。有効にした場合、プログラムコンポーネントのアップデート後に、再起動することがあります。
	今すぐコンポーネントをアップデート	［アップデート］をクリックすると、プログラムコンポーネントを最新バージョンにアップデートします。

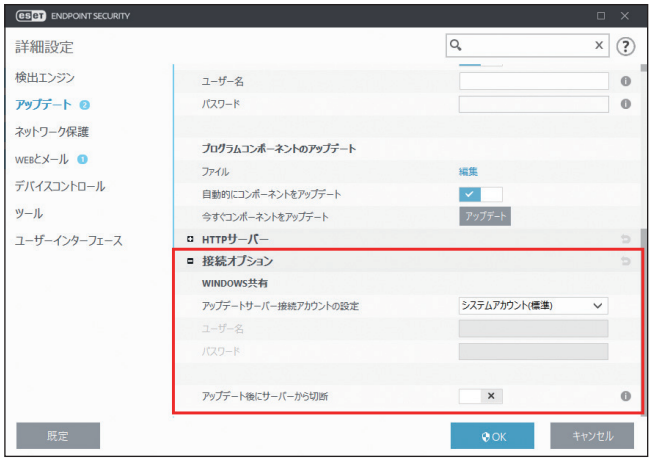
HTTP サーバー

「アップデートミラー」内にある［HTTP サーバー］をクリックすると、「HTTP サーバー」画面が表示されます。



サーバーポート	HTTP サーバーのポート番号を設定します。既定では「2221」に設定されています。	
認証	アップデートファイルにアクセスするときの認証方法を、ドロップダウンメニューから選択します。	
	なし	既定の設定です。認証しない場合に選択します。
	基本	基本のユーザー名およびパスワード認証で base64 エンコードを使用する場合に選択します。
	NTLM	安全なエンコード方法で認証する場合に選択します。認証は、アップデートファイルを保存するコンピューター上で作成されたユーザーを使用します。
HTTP サーバーの SSL	セキュリティ強化のため、HTTPS プロトコルを使用してアップデートファイルをダウンロードします。 HTTPS（SSL）サポートの HTTP サーバーを使用する場合は、「サーバ証明書ファイル」を追加するか、自己署名証明書を生成します。自己署名証明書のタイプは、「サーバ証明書のタイプ」ドロップダウンメニューから［ASN］、［PEM］、［PFX］を選択できます。「サーバ秘密鍵のタイプ」は既定で［統合］に設定されているため、サーバ秘密鍵は選択したサーバ証明書のチェーンファイルの一部となります。そのため「サーバ秘密鍵ファイル」は既定で無効となっています。	

接続オプション



アップデートサーバー接続アカウントの設定	システムアカウント（標準）	システムアカウントを使用して認証する場合に選択します。
	現在のユーザー	現在ログインしているユーザーアカウントを使用して認証する場合に選択します。ログインしているユーザーがいない場合、ESET Endpoint Security はアップデートサーバーに接続できません。
	指定したユーザー	特定のユーザーアカウントを使用して認証する場合に選択します。システムアカウントでアップデートサーバーの接続に失敗した場合に選択してください。ユーザーアカウントは、ローカルサーバー上のアップデートファイルディレクトリーにアクセスできなければなりません。アクセスできないユーザーアカウントの場合は、アップデートサーバーに接続できません。
アップデート後にサーバーから切断	有効にすると、アップデートファイルのダウンロード後にサーバーとの接続を強制的に切断します。	

●アップデートミラーからのアップデート

アップデートミラーとは、クライアントコンピューターがアップデートファイルをダウンロードできるリポジトリです。アップデートミラーの構成には、HTTP サーバーと共有ネットワークフォルダーの 2 種類があります。

！重　要

ESET Endpoint Security V7 をアップデートミラー経由でアップデートする場合は、V7 に対応したミラーツールを使用するか、ESET Endpoint アンチウイルス /ESET Endpoint Security V7 でミラーサーバーを作成する必要があります。

HTTP サーバーを使用したアップデートミラーへのアクセス

内蔵の HTTP サーバーを使用してアップデートミラーにアクセスできるようにするには、「詳細設定」画面で［アップデート］>［プロファイル］>［アップデートミラー］をクリックして［アップデートミラーの作成］を有効にし、「HTTP サーバー」セクションで、HTTP サーバーの「サーバーポート」、「認証」タイプを設定します。詳細については、「HTTP サーバー」を参照してください。

！重　要

HTTP サーバー経由でアップデートファイルへのアクセスを許可する場合、アップデートミラーは ESET Endpoint Security のインスタンスと同じコンピューターに設置されている必要があります。

HTTPS（SSL）サポートの HTTP サーバーを使用してアップデートミラーにアクセスできるようにするには、「サーバ証明書ファイル」を追加するか、自己署名証明書を生成します。詳細については、「HTTP サーバー」を参照してください。

! 重　要

アップデートミラーからの検出エンジンのアップデートに数回失敗すると、「アップデート」画面に無効なユーザー名またはパスワードエラーが表示されます。このエラーの一般的な原因は、設定した認証データが正しくないことです。メインメニューの［設定］>［詳細設定］をクリックするか、【F5】キーを押して「詳細設定」画面を表示し、［アップデート］>［プロファイル］>［アップデートミラー］をクリックして、「ユーザー名」と「パスワード」が正しく設定されているか確認してください。

- **アップデートミラーの構成手順**

ESET Endpoint Security をアップデートミラーとし、内部 HTTP サーバー経由でアップデートファイルを配布するには、次の操作を行います。

操作手順

1. メインメニューの［設定］>［詳細設定］をクリックするか、【F5】キーを押します。
   「詳細設定」画面が表示されます。
2. ［アップデート］>［プロファイル］>［アップデート］をクリックし、「アップデートサーバー」の「自動選択」が有効になっていることを確認します。
3. ［アップデートミラー］をクリックし、「アップデートミラーの作成」と「HTTP サーバーを有効にする」を有効にします。

ワンポイント

内部 HTTP サーバー経由でアップデートしない場合は、「HTTP サーバーを有効にする」を無効にします。

- **クライアントコンピューターの設定**

アップデートミラーの設定が完了したら、クライアントコンピューター上に新しいアップデートサーバー（追加したアップデートミラー）を追加します。
アップデートサーバーを追加する手順は、次のとおりです。

操作手順

1. メインメニューの［設定］>［詳細設定］をクリックするか、【F5】キーを押します。
   「詳細設定」画面が表示されます。
2. ［アップデート］>［プロファイル］をクリックします。
3. 「自動選択」を無効にします。
4. 「アップデートサーバー」フィールドに、次のいずれかの形式でサーバーのパスを入力します。
   SSL を使用しない場合：http://< サーバーの IP アドレス >:2221
   SSL を使用する場合：https://< サーバーの IP アドレス >:2221

• **共有ネットワークフォルダーを使用したアップデートミラーの構成手順**

共有ネットワークフォルダーを使用してミラーサーバーを構成します。構成の手順は、次のとおりです。

操作手順

1. ローカルデバイスまたはネットワークデバイスに共有フォルダーを作成します。
2. 作成した共有フォルダーにアクセス権を設定します。
   共有フォルダーにアップデートファイルを保存するユーザーに「書き込み」アクセス権を付与します。
   アップデートミラーからアップデートするすべてのユーザーに「読み取り」アクセス権を付与します。
3. メインメニューの［設定］>［詳細設定］をクリックするか、【F5】キーを押します。
   「詳細設定」画面が表示されます。
4. ［アップデート］>［プロファイル］>［アップデートミラー］をクリックし、［アップデートミラーの作成］を有効にします。
5. 「ストレージフォルダー」にパスが表示されているときは、［削除］をクリックすると、保存先が削除されます。
6. 「ストレージフォルダー」の［編集］をクリックし、作成した共有フォルダーを指定します。

ワンポイント

ネットワーク共有フォルダーがネットワーク内の別のクライアントコンピューターにある場合は、そのコンピューターにアクセスするための認証データを設定する必要があります。認証データを設定するには、メインメニューの［設定］>［詳細設定］をクリックするか、【F5】キーを押して「詳細設定」を表示し、［アップデート］>［プロファイル］>［アップデートミラー］>［接続オプション］>［アップデートサーバー接続アカウントの設定］をクリックします。設定の詳細については、「WINDOWS 共有」を参照してください。

• **クライアントコンピューターの設定**

アップデートミラーの設定が完了したら、クライアントコンピューター上にアップデートサーバーを追加します。アップデートサーバーを追加する手順は、次のとおりです。

操作手順

1. メインメニューの［設定］>［詳細設定］をクリックするか、【F5】キーを押します。
   「詳細設定」画面が表示されます。
2. ［アップデート］>［プロファイル］をクリックします。
3. 「自動選択」を無効にします。
4. 「アップデートサーバー」フィールドに「\\UNC\PATH」と入力します。

!重 要

アップデートを正しく実行するには、アップデートサーバーのパスを UNC パスとして指定する必要があります。マップされたドライブを指定すると、アップデートは正しく実行されない場合があります。

ワンポイント

「アップデートミラー」の「プログラムコンポーネントのアップデート」セクションでは、プログラムコンポーネント（PCU）の制御に関する設定ができます。既定では、ダウンロードされたプログラムコンポーネントは、自動的にローカルのミラーサーバーにコピーされます。設定の詳細については、「プログラムコンポーネントのアップデート」を参照してください。

●アップデートミラーからのアップデートに関するトラブルシューティング

アップデートミラーからのアップデート中に発生する問題の原因は、次のとおりです。

- アップデートミラーのフォルダーの指定が正しくない
- アップデートミラーのフォルダーにアクセスするための認証データが正しくない
- アップデートミラーからアップデートファイルをダウンロードするローカルコンピューターの設定が正しくない
- 上記 3 つのエラーの組み合わせ

! 重　要

ESET Endpoint Security V7 をアップデートミラー経由でアップデートする場合は、V7 に対応したミラーツールを使用するか、ESET Endpoint アンチウイルス /ESET Endpoint Security V7 でミラーサーバーを作成する必要があります。

アップデートミラーからのアップデート時に発生する問題の概要を紹介します。

アップデートミラーへの接続エラーが通知される

原因として、ローカルコンピューターのアップデートファイルのダウンロード元であるアップデートサーバー（ミラーフォルダーのネットワークパス）が正しく指定されていないことが考えられます。フォルダーを確認するには、Windows の［スタート］ボタン > すべてのプログラム > アクセサリ >［ファイル名を指定して実行］をクリックし、ミラーフォルダーのフォルダー名を入力して、［OK］をクリックします。フォルダーの内容が表示されるか確認します。

ESET Endpoint Security でユーザー名とパスワードが要求される

原因として、「詳細設定」画面のアップデートセクションで、認証データ（ユーザー名とパスワード）が正しく設定されていないことが考えられます。ユーザー名とパスワードは、アップデートファイルのダウンロード元であるアップデートサーバーにアクセスするために使用されます。認証データが適切な形式で正しく設定されていることを確認してください。

例えば、ユーザー名は「< ドメイン >/< ユーザー名 >」または「< ワークグループ >/< ユーザー名 >」という形式で入力する必要があり、ユーザー名に対応するパスワードを入力する必要があります。また、「すべてのユーザー」がアップデートミラーにアクセス可能であっても、「すべてのユーザー」がアクセスを許可されているわけではありません。「すべてのユーザー」とは、すべての認証されていないユーザーを意味するのではなく、すべてのドメインユーザーがフォルダーにアクセスできることを意味します。つまり、「すべてのユーザー」がフォルダーにアクセス可能な場合でも、「詳細設定」画面のアップデートセクションでドメインユーザー名とパスワードを設定する必要があります。

アップデートミラーへの接続エラーが通知される

HTTP サーバーを使用したアップデートミラーへのアクセスで定義されているポート上の通信がブロックされています。

! 重　要

OS のファイアウォール機能や ESET Endpoint Security のファイアウォール機能によって、通信がブロックされていないか確認してください。

●アップデートタスクの作成

メインメニューの「アップデート」>［今すぐアップデート］をクリックすると、手動でアップデートすることができますが、スケジューラ機能でアップデートタスクを作成して実行することもできます。

アップデートタスクを作成するには、メインメニューの［ツール］>［スケジューラ］をクリックします。ESET Endpoint Security では、次のタスクが既定で設定されています。

- 定期的に自動アップデート
- ダイヤルアップ接続後に自動アップデート
- ユーザーログオン後に自動アップデート

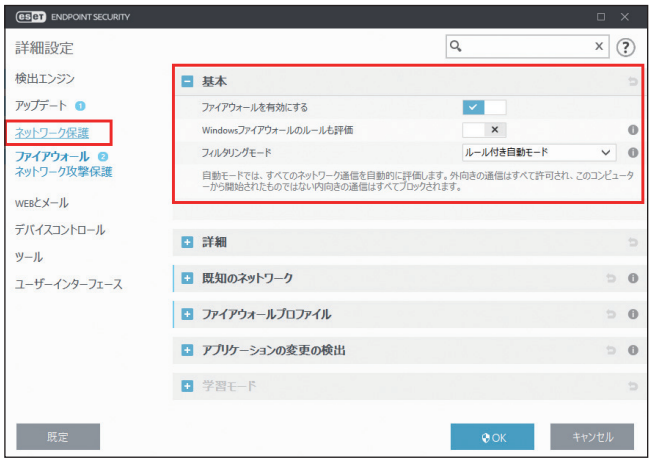
既定のアップデートタスクは、ニーズに合わせて変更できます。また、既定のアップデートタスクとは別に、新しいアップデートタスクを作成することもできます。アップデートタスク作成の詳細については、「4.4.7　スケジューラ」を参照してください。

4.6.7 ネットワーク保護

ファイアウォールは、システムで送受信されるすべての通信トラフィックを検査し、指定したフィルタリングルールに基づいて個々のネットワーク接続を許可または拒否します。ファイアウォールによって、リモートコンピューター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。また、HTTP、POP3、IMAP プロトコルをウイルスから保護することもできます。

■基本

ファイアウォールを設定するには「詳細設定」画面で［ネットワーク保護］＞［ファイアウォール］＞［基本］をクリックします。

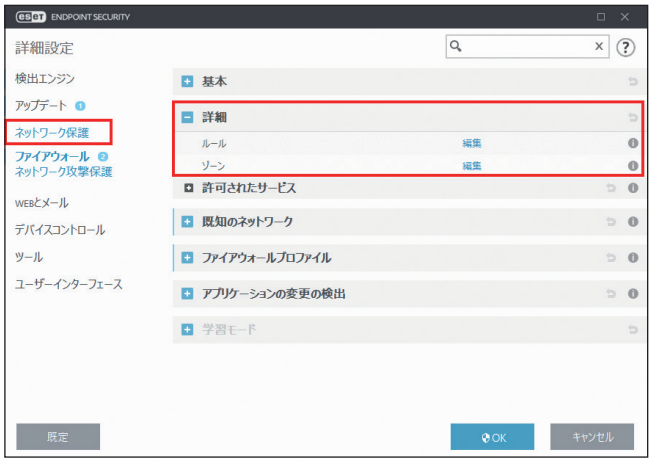


ファイアウォールを有効にする	ファイアウォールの有効／無効を設定します。	
Windows ファイアウォールのルールも評価	ルール付き自動モードで、ファイアウォールのルールによって明示的にブロックされていない場合は、Winoows ファイアウォールで許可された受信トラフィックを許可します。	
フィルタリングモード	4 つのフィルタリングモードから選択します。ファイアウォールの動作は、フィルタリングモードによって異なります。	
	ルール付き自動モード	既定のモードです。ルールを定義せずに、ファイアウォールを簡単に使用したいユーザー向けのモードです。ルールを定義することもできますが、必須ではありません。自動モードでは、特定のシステムのすべての送信トラフィックが許可され、ほとんどの受信トラフィック（「IDS と詳細オプション」の「許可するサービス」で許可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ルールを定義できるモードです。通信トラフィックが検出されたとき、適用されるルールがなければ、不明なネットワーク接続を通知する画面が表示されます。通知画面では、ネットワーク接続を許可するか拒否するかを選択できます。さらに、許可または拒否の決定を、ファイアウォールの新しいルールとして保存することもできます。新しいルールとして保存すると、以降は同じ種類のすべてのネットワーク接続がルールに従って許可または拒否されます。

フィルタリングモード	ポリシーベースモード	ルールで定義されていないすべてのネットワーク接続をブロックするモードです。必要かつ安全なネットワーク接続のみを許可するルールを定義できる経験豊富なユーザー向けのモードです。定義したルールに適用されないネットワーク接続は、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するモードです。ファイアウォールの初期設定に適しています。既定のパラメーターに従ってルールが保存されるため、ユーザーの操作は必要ありません。学習モードではシステムの安全を確保できないため、必要なルールが作成されるまでの一時的な使用としてください。

■詳細

［詳細］をクリックすると、ルールの作成、ゾーンの編集などを行えます。



ルール	ルールを追加して、ファイアウォールが通信トラフィックを処理する方法を定義できます（次項参照）。
ゾーン	複数の IP アドレスで構成されるゾーンを作成できます（●ゾーン参照）。

ファイアウォールプロファイルを使用すると、様々な状況ごとに複数のルールを指定して、ファイアウォールの動作をカスタマイズできます。詳細については、「■ファイアウォールプロファイル」を参照してください。

●ルールの設定と運用

ルールとは、通信トラフィックを検査する条件と、条件に一致したときのアクションを定義したものです。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たときに実行するアクションを定義できます。

ネットワーク接続は受信と送信に分けることができます。受信は、リモートコンピューターがローカルシステムとの接続を確立しようとする動作です。送信は受信とは反対の動作で、ローカルシステムがリモートコンピューターとの接続を確立しようとする動作です。

不明な通信が新たに検出された場合は、その接続を許可するか拒否するかを慎重に検討してください。受信者側が送信を要求していない接続、安全ではない接続、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コンピューターおよびアプリケーションに特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コンピューター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、このような接続を検出し、切断することができます。

! 重 要

一部の定義済みルールは「詳細」の「許可されたサービス」で関連付けられているため、直接無効にすることはできません。無効にする場合は、「詳細」の「許可されたサービス」で無効に変更してください。

ルールの設定

メインメニューの［設定］＞［詳細設定］＞［ネットワーク保護］＞［ファイアウォール］＞［詳細］＞［ルール］の［編集］リンクをクリックすると、「ファイアウォールルール」画面が表示され、ファイアウォールルールを設定できます。また、［すべてのルール（定義済みを表示）を表示］をチェックすると、すべてのルールが一覧表示されます。

名前	ルールの名前が表示されます。
有効	ルールの有効／無効を設定します。ルールを有効にするには、チェックボックスをチェックします。
プロトコル	ルールで有効なプロトコルが表示されます。
プロファイル	ルールで有効なファイアウォールプロファイルが表示されます。
アクション	通信を検出したときのアクション（拒否／許可／確認）が表示されます。
方向	通信の方向（受信／外向き／双方向）が表示されます。
ローカル	ローカルコンピューターの IP アドレスとポートが表示されます。
リモート	リモートコンピューターの IP アドレスとポートが表示されます。
アプリケーション	ルールを適用するアプリケーションが表示されます。
追加	新しいルールを作成します。
編集	既存のルールを編集します。
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。
すべてのルール（定義済み）を表示	チェックすると、ESET Endpoint Security によって定義されたルールも表示されます。ESET Endpoint Security によって定義されたルールは無効にできますが、削除することはできません。
／／／	ルールの優先度を変更できます（ルールは上から順に適用されます）。

ワンポイント

検索フィールドを使用すると、名前やプロトコル、ポートなどでルールを検索できます。

! 重 要

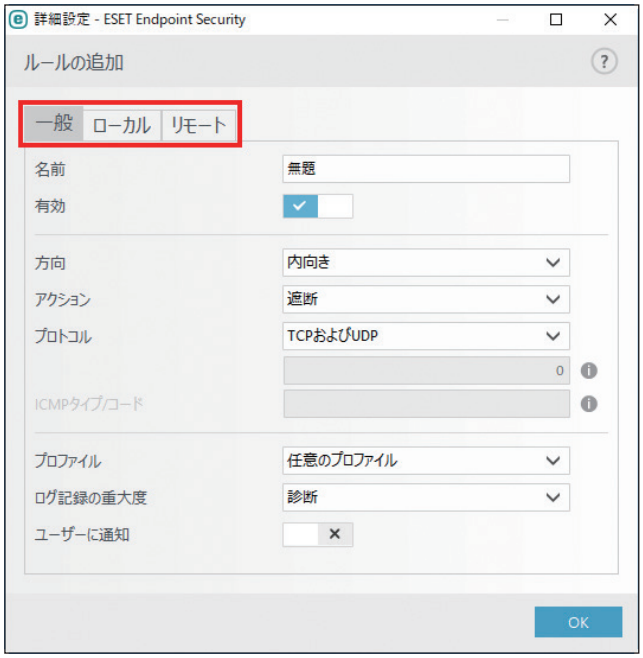
ルールは優先度順に一覧表示されます。最上位に表示されているルールが最も優先度の高いルールとなります。各ネットワーク接続に対して優先度順にルールがチェックされ、最初に一致したルールのアクションが使用されます。

ルールの編集

リモート側のネットワークアドレスやポート番号など、監視対象のパラメーターが変更された場合は、ルールを変更する必要があります。ルールが条件を満たせず、指定したアクションが適用できないようなパラメーターの変更が行われた場合、指定し接続が拒否されアプリケーションの動作に問題が発生する場合があります。

「ファイアウォールルール」画面で［追加］をクリックするか、一覧からルールを選択して［編集］をクリックすると、ルールの編集画面が表示されます。ルールの編集画面には、次の 3 つのタブがあります。

一般	ルール名（名前）、接続の方向、アクション（許可／拒否／確認）、プロトコル、ルールを適用するプロファイルを指定します。
ローカル	ローカルポートまたはポート範囲、通信するアプリケーションの名前など、ローカルコンピューターに関する情報が表示されます。IP アドレスを指定したり、［追加］をクリックして定義済みまたは作成したゾーンを追加したりすることもできます。
リモート	リモートポート（ポート範囲）に関する情報が表示されます。指定したルールのリモート IP アドレスを指定したり、［追加］をクリックして定義済みまたは作成したゾーンを追加したりできます。



新しいルールを作成するには、次の項目を設定します。

名前	ルールの名前を入力します。
方向	ルールが適用される接続方向を選択します。
アクション	通信がルールに一致したときに実行するアクションを選択します。
プロトコル	このルールが有効なプロトコルを選択します。
ICMP タイプ／コード	番号で識別される ICPM メッセージです（例：0 は「エコー応答」）。 既定では、すべてのプロファイルに対してすべてのルールが有効です。
プロファイル	ルールを適用するファイアウォールプロファイルを選択します。
ログ記録の重大度	有効にすると、ルールに関連付けられているアクティビティがログに記録されます。
ユーザーに通知	有効にすると、ルールが適用されたときに通知が表示されます。

新しいルールを作成する例として、Web ブラウザーがネットワークにアクセスできるようにするルールについて説明します。この例では、次の設定を行う必要があります。

- ［一般］タブの［方向］を［外向き］、［アクション］を［許可］、［プロトコル］を［TCP および UDP］を選択し、TCP および UDP プロトコルを介した送信通信を有効にします。
- ［ローカル］タブの［アプリケーション］の［...］をクリックして、Web ブラウザーを指定します（Internet Explorer の場合は iexplore.exe）。
- ［リモート］タブの［ポート］に 80 を入力して、標準のインターネット閲覧を許可します。

●ゾーン

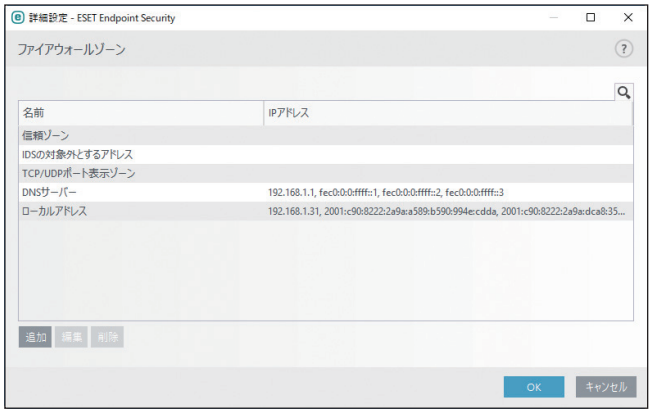
信頼ゾーンは、ファイアウォールが既定の設定を使用して受信トラフィックを許可するネットワークアドレスのグループです。信頼ゾーン内のファイル共有やリモートデスクトップなどの機能は、「ファイアウォール」の「詳細」＞「許可されたサービス」で設定されます。

実際の信頼ゾーンは、コンピューターが現在接続しているネットワークに基づいて、各ネットワークアダプターに対して動的に個別に計算されます。ゾーンエディターで信頼ゾーン内に定義されたアドレスは常に信頼されます。ネットワークアダプターが既知のネットワークに接続している場合、そのネットワークに設定された「追加の信頼できるアドレス」が、ネットワークアダプターの信頼ゾーンに追加されます。ネットワークの保護タイプが「自宅／職場ネットワーク」の場合、直接接続されたすべてのサブネットは信頼ゾーンに含まれます。各ネットワークアダプターの信頼ゾーンを確認するには、メインメニューの［設定］＞［ネットワーク］＞［接続されたネットワーク］＞［ネットワークアダプタ］をクリックします。

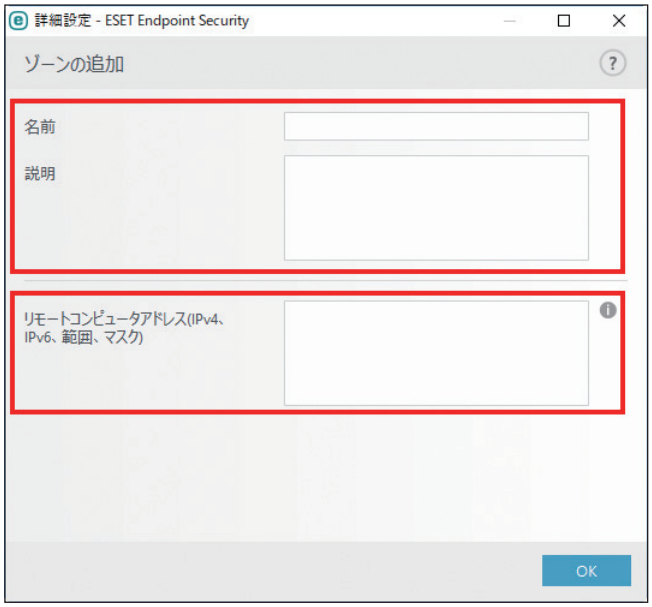
ゾーンの設定

ゾーンは IP アドレスのグループであり、複数のルールで同じグループの IP アドレスを利用するときに有効です。

ゾーンを設定するには、メインメニューの［設定］>［ネットワーク］>［ファイアウォール］の ⚙ >［設定］をクリックするか、【F5】キーを押して「詳細設定」画面を表示し、［ネットワーク保護］>［ファイアウォール］>［詳細］>［ゾーン］の［編集］リンクをクリックして「ファイアウォールゾーン」画面を表示します。



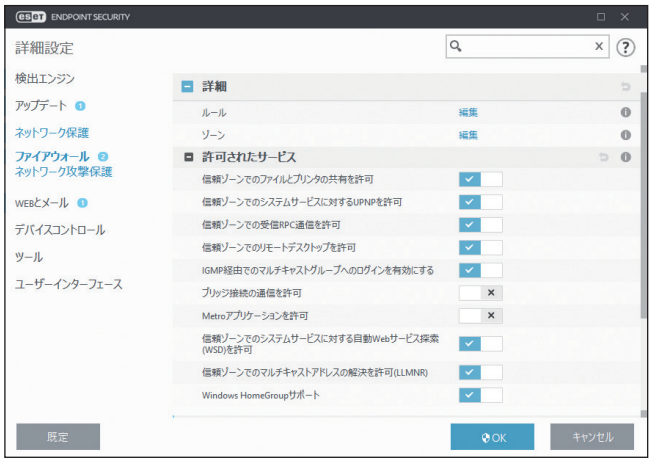
新しいゾーンを追加するには、［追加］をクリックして「ゾーンの追加」画面を表示します。



ゾーンの名前、説明を入力し、「リモートコンピュータアドレス（IPv4、IPv6、範囲、マスク）」フィールドにリモート IP アドレスを追加します。

●許可されたサービス

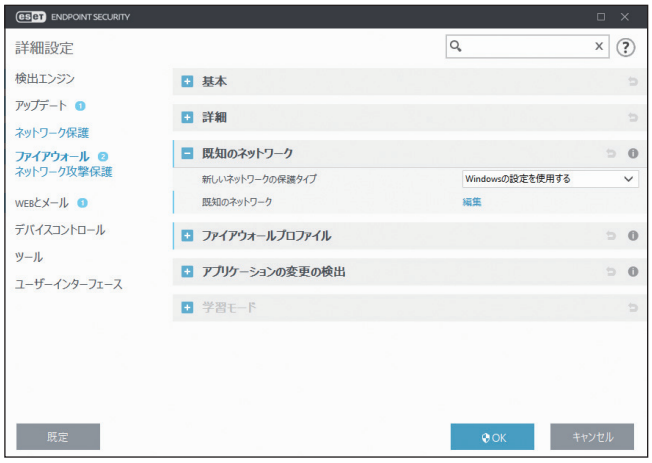
「許可されたサービス」セクションでは、共有ネットワークサービスのネットワーク権限を設定できます。ここでは、以下の項目についてサービスの有効 / 無効を設定できます。



信頼ゾーンでファイルとプリンタの共有を許可	信頼済みゾーン内のコンピューターに、共有ファイルおよび共有プリンターへのアクセスを許可します。
信頼ゾーンでのシステムサービスに対する UPNP を許可	システムサービスの受信および送信時の UPnP プロトコル要求を許可します。UPnP（ユニバーサルプラグアンドプレイ）は、Windows Vista 以降のオペレーティングシステムで使用されています。
信頼ゾーンでの受信 RPC 通信を許可	信頼ゾーンからの TCP 接続を有効にして、MS RPC Portmapper および RPC/DCOM サービスへのアクセスを許可します。
信頼ゾーンでのリモートデスクトップを許可	Microsoft Remote Desktop Protocol (RDP) プロトコルでの接続を有効にして、RDP を利用するプログラム（リモートデスクトップ接続など）を信頼ゾーン内のコンピューターで使用可能にします。
IGMP 経由でのマルチキャストグループへのログインを有効にする	IGMP プロトコル (インターネットグループ管理プロトコル) を使用するプログラムによって生成されたビデオストリーミングなど、内向きおよび外向きの IGMP および内向き UDP マルチキャストストリームを許可します。
ブリッジ接続の通信を許可	ブリッジされた接続を終了せずに保持します。
Metro アプリケーションを許可	Metro 環境で実行している Windows Store アプリケーションの通信を、Metro アプリケーションマニフェストに従って許可します。ESET ファイアウォール設定で対話モードまたはポリシーベースモードを選択しているかどうかにかかわらず、このオプションは Metro アプリケーションのすべてのルールと例外より優先されます。この設定は、Windows 8 以降でのみ利用できます。
信頼ゾーンでのシステムサービスに対する自動 Web サービス探索 (WSD) を許可	信頼ゾーンからファイアウォールを通じて WSD 要求の送受信を行うことを許可します。WSD はローカルネットワーク上でサービスを見つけるために使用されるプロトコルです。
信頼ゾーンでマルチキャストアドレスの解決を許可 (LLMNR)	LLMNR（リンクローカルマルチキャスト名前解決）は、DNS サーバーや DNS クライアントを設定しなくても IPv4 と IPv6 の両方のホストで同じローカルリンク上のホストの名前解決ができる DNS パケットベースのプロトコルです。このオプションでは、信頼ゾーンからファイアウォールを通じた DNS 要求の受信が許可されます。
Windows Home Group サポート	Windows 7 以降のオペレーティングシステムのホームグループサポートを有効にします。ホームグループでは、ホームネットワーク上のファイルやプリンターを共有できます。

■既知のネットワーク

パブリックネットワークや企業ネットワーク外のネットワークに頻繁に接続するコンピューターを使用している場合は、接続先の新しいネットワークの信頼性を検証することをお勧めします。ネットワークが定義されると、ESET Endpoint Security はネットワーク ID で設定された様々なネットワークパラメーターを使用して、信頼できる自宅／職場ネットワークと認識します。コンピューターは、信頼できるネットワークに似た IP アドレスを使用してネットワークに接続することがあります。このような場合、ESET Endpoint Security は不明なネットワークを信頼できる自宅／職場ネットワークとみなすことがあります。ネットワーク認証を使用して、このような状況を回避することをお勧めします。



●既知のネットワークリストによるネットワーク接続の検証

ネットワークアダプターがネットワークに接続されたり、ネットワーク設定が構成されたりすると、ESET Endpoint Security は既知のネットワークリストから新しいネットワークと一致するレコードがないか検索します。「ネットワーク ID」と「ネットワーク認証」（オプション）が一致した場合は、新しいネットワークは接続済みに設定されます。レコードが既知のネットワークと一致しなかった場合は、次回ネットワークに接続するときに識別できるように、ネットワーク構成を設定して、新しいネットワークを作成します。

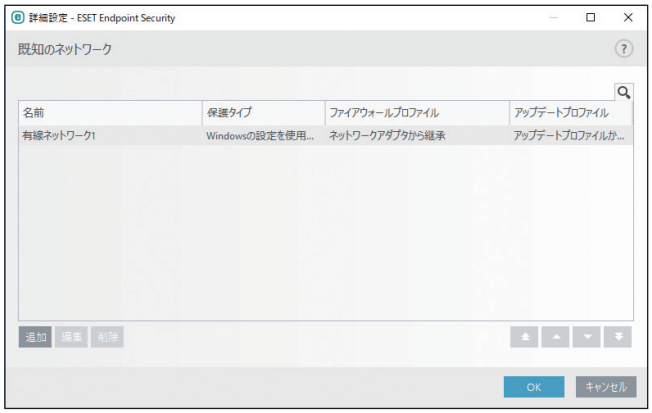
新しいネットワークの保護タイプ	Windows の設定を使用する	Windows の設定に従って自動的に設定されます。そのため、特定の機能（ファイル共有やリモートデスクトップなど）にアクセスできるようになります。
	ユーザーに確認する	ネットワークの保護タイプをユーザーに確認します。
	パブリックに設定	自動的にパブリックネットワークに設定されます。

！重　要

新しいネットワークの保護タイプで［パブリックに設定］を選択すると、接続先のネットワークが自動的にパブリックネットワークに設定されます。このため、新しいネットワークから、特定の機能（ファイル共有やリモートデスクトップなど）にアクセスできなくなります。

●既知のネットワークエディター

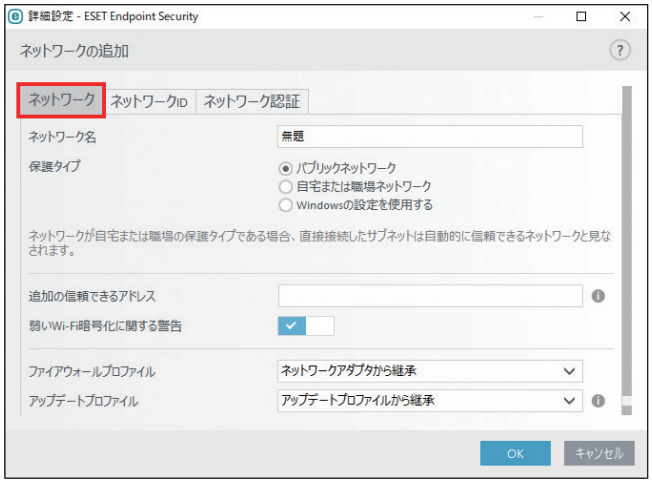
既知のネットワークエディター画面では、既知のネットワークを手動で編集できます。
既知のネットワークを手動で編集するには、「詳細設定」画面で［ネットワーク保護］＞［ファイアウォール］＞［既知のネットワーク］を選択し、「既知のネットワーク」の［編集］をクリックします。



名前	既知のネットワークの名前が表示されます。
保護タイプ	ネットワークの保護タイプが「自宅／職場ネットワーク」と「パブリックネットワーク」、「Windows の設定を使用する」のどれに設定されているかが表示されます。
ファイアウォールプロファイル	ネットワークに設定されているファイアウォールプロファイルのルールフィルターが表示されます。
アップデートプロファイル	ネットワークに設定されているアップデートプロファイルが表示されます。
追加	新しい既知のネットワークを作成します。
編集	既存の既知のネットワークを編集します。
削除	既存の既知のネットワークを削除します。
／／／	既知のネットワークの優先度を変更できます（ネットワークは上から順に検索されます）。

「既知のネットワーク」画面で［追加］をクリックするか、一覧から既知のネットワークを選択して［編集］をクリックすると、ネットワークの編集画面が表示されます。ネットワークの編集画面は、次の 3 つのタブがあります。

ネットワーク



ネットワーク名	ネットワーク名を設定します。
保護タイプ	「パブリックネットワーク」「自宅または職場ネットワーク」「Windows の設定を使用する」を選択します。
追加の信頼できるアドレス	ネットワークの保護タイプに関係なく、既知のネットワークに接続されたネットワークアダプターを信頼ゾーンに常に追加します。
弱い Wi-Fi 暗号化に関する警告	セキュリティの低い Wi-Fi の暗号化を利用している場合に警告を表示します。
ファイアウォールプロファイル	ファイアウォールプロファイルを設定します。
アップデートプロファイル	このネットワークに設定された時に使用するアップデートプロファイルを設定します。

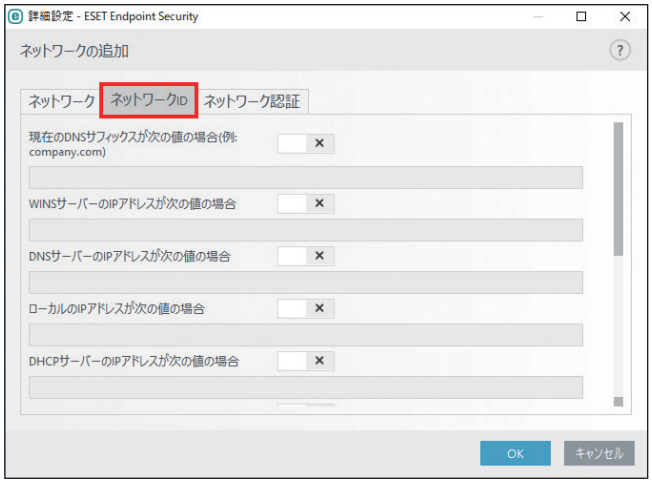
ワンポイント

メインメニューの［設定］>［ネットワーク］タブの［接続されたネットワーク］の一覧で表示されているネットワークは、次の条件を満たしています。

- ネットワーク ID：すべての設定済みパラメーターがアクティブな接続パラメーターと一致しています。
- ネットワーク認証：認証サーバーが選択されている場合、ESET Authentication Server との認証が正常に実行されています。
- ネットワーク制限（Windows XP/ Windows Server 2003 のみ）：すべての選択されたグローバル制限が適用されています。

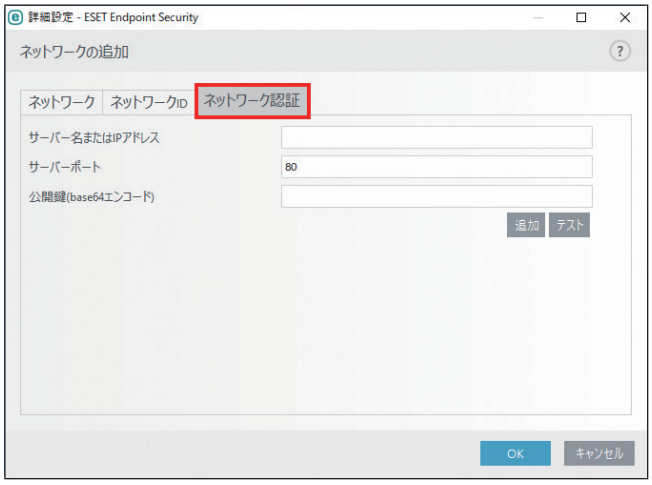
ネットワーク ID

ネットワーク ID は、ローカルのネットワークアダプターのパラメーターに基づいて実行されます。すべての選択されたパラメーターは、アクティブなネットワーク接続のパラメーターと比較されます。IPv4 および IPv6 アドレスはいずれも許可されます。



ネットワーク認証

ネットワーク認証によってネットワーク内のサーバーが検索され、非対称暗号化（RSA）を使用してサーバーが認証されます。サーバーを認証するには、認証中のネットワークの名前が、認証サーバーで設定されているゾーン名と一致する必要があります。名前は大文字と小文字が区別されます。



サーバー名または IP アドレス	IP アドレス、DNS、NetBIOS 名で指定します。
サーバーポート	ポート番号を指定します。既定は 80 です。
公開鍵（base64 エンコード）	ネットワーク認証の公開鍵を指定します。［追加］をクリックすると選択して指定できます（下記参照）。［テスト］をクリックすると公開鍵をテストできます。

公開鍵のインポート

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）：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）

■ファイアウォールプロファイル

ファイアウォールのルールを作成または編集するときに、ルールをプロファイルに割り当てることで、ファイアウォールの動作を制御できます。ネットワークインターフェイスでプロファイルが有効な場合、グローバルルール（プロファイルの指定がないルール）とネットワークインターフェイスの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。複数のプロファイルを作成しておけば、異なるルールをネットワークアダプターやネットワークに割り当てるだけで、ファイアウォールの動作を簡単に変更できます。

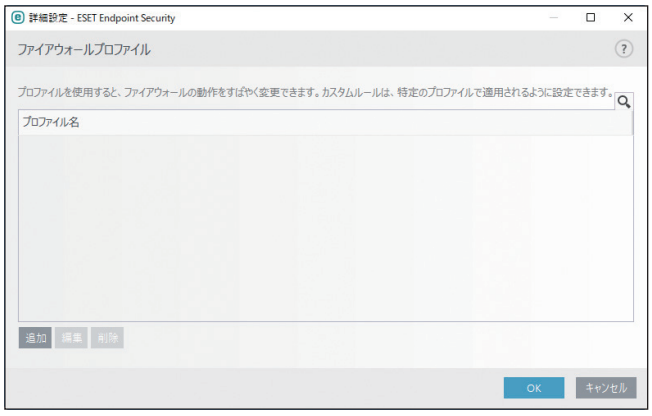
プロファイルを編集するには、「詳細設定」画面で、［ネットワーク保護］>［ファイアウォール］>［ファイアウォールプロファイル］を選択して、「プロファイルのリスト」の［編集］をクリックします。

●グローバルデフォルトプロファイル

ネットワークまたはアダプタのプロファイルがない場合に適用されるプロファイルを指定します。

●プロファイルのリスト

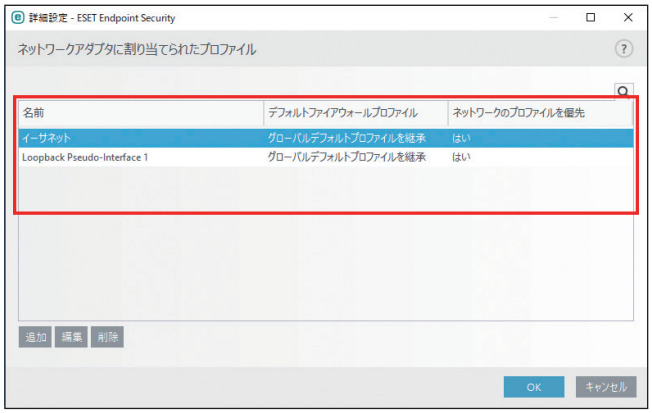
［編集］をクリックしてプロファイルを追加、編集します。



［追加］をクリックしてプロファイルを追加します。
［編集］でプロファイル名の編集、［削除］でプロファイルの削除ができます。

●ネットワークアダプターに割り当てられたプロファイル

コンピューターにあるすべてのネットワークアダプターは「ネットワークアダプタに割り当てられたプロファイル」の一覧に自動的に追加されます。プロファイルにルールを設定しておけば、プロファイルを切り替えるだけで、ファイアウォールの動作を変更できます。

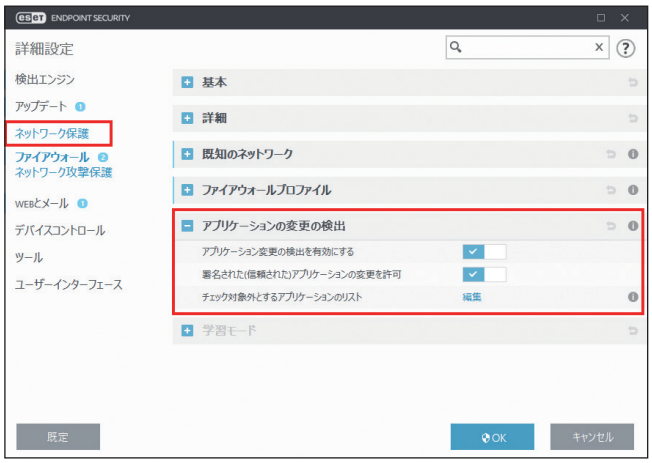


名前	ネットワークアダプターの名前が表示されます。
デフォルトファイアウォールプロファイル	接続先のネットワークでプロファイルが設定されていないか、ネットワークアダプターがネットワークプロファイルを使用するように設定されていない場合は、既定のプロファイルが使用されます。
ネットワークのプロファイルを優先	「ネットワークのプロファイルを優先」を有効にすると、ネットワークアダプターは接続されたネットワークに割り当てられているファイアウォールプロファイルを使用します（可能な場合のみ）。
追加	新しいネットワークアダプターを追加します。
編集	既存のネットワークアダプターを編集します。
削除	既存のネットワークアダプターを削除します。

■アプリケーションの変更の検出

アプリケーションの変更の検出は、アプリケーションで構成されているファイアウォールルールが別のアプリケーションによって悪用されるのを防止する機能です。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、デスクトップ右下の情報メッセージによって通知されます。

「詳細設定」画面で、[ネットワーク保護] > [ファイアウォール] > [アプリケーションの変更の検出] をクリックします。



アプリケーションの変更の検出を有効にする	有効にすると、アプリケーションの更新、感染、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	有効にすると、アプリケーションに別のアプリケーションと同じ有効なデジタル署名がある場合は、変更を通知しません。
チェック対象外とするアプリケーションのリスト	［編集］リンクをクリックすると、「チェック対象外とするアプリケーションのリスト」画面が表示されます。通知を表示せず、変更を許可するアプリケーションを追加、編集、削除できます。

■学習モード

学習モードでは、システムで確立した各通信トラフィックのルールを自動的に作成して保存します。「学習モード」セクションを表示するには、［詳細設定］（【F5】キー）>［ネットワーク保護］>［ファイアウォール］>［基本］で［フィルタリングモード］に［学習モード］を設定します。

！重　要

学習モードでは、ファイアウォールによる通信トラフィックのフィルタリングは行われず、すべての通信トラフィックの送受信が許可されるため、システムの安全は確保されません。学習モードは必要なルールが作成されるまでの一時的な使用としてください。

「詳細設定」画面で［ネットワーク保護］>［ファイアウォール］>［学習モード］を選択します。

学習モードの終了時刻	学習モードを有効にする期間を選択します。指定した期間が過ぎると、「学習モードの期限切れの後に設定されるモード」で設定したフィルタリングモードが設定されます。
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、ESET Endpoint Security 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。詳細については、フィルタリングモードを参照してください。
信頼ゾーンからの受信トラフィック	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や、信頼ゾーン内のリモートコンピューターからの受信トラフィックです。
信頼ゾーンへの送信トラフィック	ローカルアプリケーションから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ーへの送信トラフィックです。
受信インターネットトラフィック	リモートコンピューターから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へのインターネット経由のトラフィックです。
送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ローカルアプリケーションから別のコンピューターへのインターネット経由のトラフィックです。

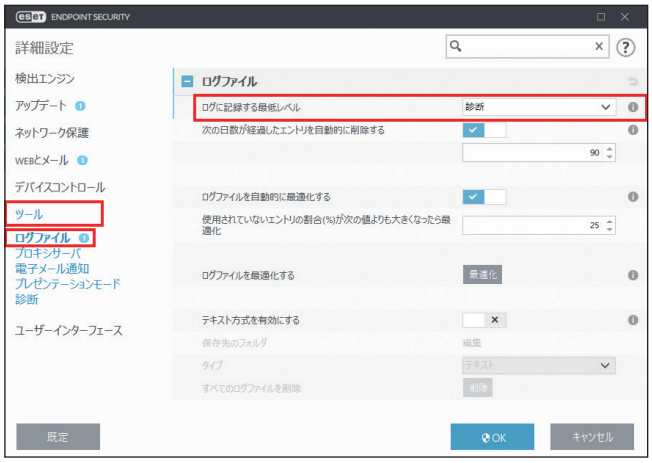
通信タイプごとに、ルールを作成するためのパラメーターを設定できます。

ローカル	ローカルポートの追加	ルールにネットワーク通信のローカルポート番号を追加するかどうかを設定します。送信トラフィックの場合、一般的にはランダムなポート番号が生成されるため、受信トラフィックのみで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	ルールにローカルアプリケーションの名前を追加するかどうかを設定します。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）を作成するのに最適です。例えば、Web ブラウザーや電子メールクライアントのみ通信を有効にすることができます。
リモート	リモートポートの追加	ルールにネットワーク通信のリモートポート番号を追加するかどうかを設定します。例えば、標準的なポート番号（HTTP-80、POP3-110 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 / 信頼ゾーンを追加	ローカルシステムとリモートアドレス／ゾーン間のすべてのネットワーク接続を定義するルールに、リモート IP アドレスまたは信頼ゾーンを追加するかどうかを設定します。特定のコンピューターまたはコンピューター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様々なポートを介して様々な 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複数のルールを作成します。「アプリケーションに対する異なるルールの最大数」では、1 つのアプリケーションに対して作成できるルールの最大数を指定します。既定値は「3」、制限値は「1」～「99」です。	

●ファイアウォールのログの確認

ESET Endpoint Security のファイアウォールでは、重要なすべてのイベントがログファイルに記録されます。ログファイルはメインメニューの［ツール］>［ログファイル］をクリックし、ドロップダウンメニューから［ネットワーク保護］を選択すると表示できます。

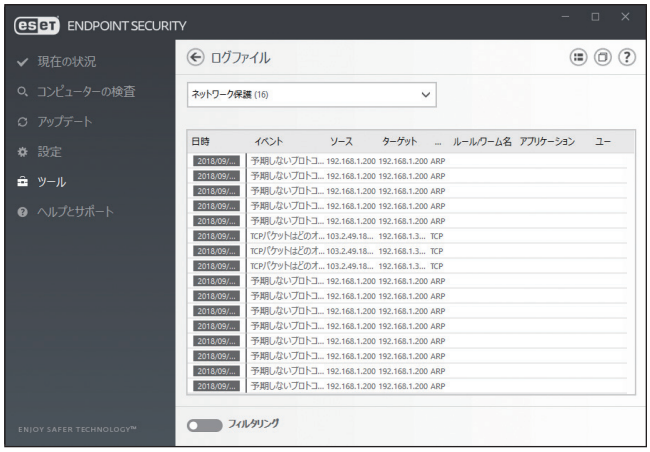
すべての拒否された接続がログに記録されるようにするには、メインメニューの［設定］>［詳細設定］をクリックするか、【F5】キーを押して「詳細設定」画面を表示し、［ツール］>［ログファイル］をクリックして、［ログに記録する最低レベル］ドロップダウンメニューから［診断］を選択します。



ファイアウォールログに記録されるデータ

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の重要なツールです。ファイアウォールのログには次のデータが記録されます。

- イベントの日時
- イベントの名前
- ソースネットワークアドレス
- 宛先のネットワークアドレス
- ネットワーク通信プロトコル
- 適用されたルールまたはワームの名前（特定された場合）
- 関連するアプリケーション
- 侵入が検出されたときにログインしていたユーザーの名前



ファイアウォールログの分析

ログ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。次のような要素は潜在的なセキュリティリスクの兆候があります。

- 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

これらの要素を詳しく分析することで、セキュリティリスクを最小限にとどめることができます。

●ネットワーク接続の確立と検出

ファイアウォールは、新しく確立されたネットワーク接続を検出します。新しい接続に対して実行されるアクションは、ファイアウォールで設定されているフィルタリングモードによって決まります。

フィルタリングモードが「ルール付き自動モード」または「ポリシーベースモード」の場合

あらかじめ定義されているアクションが自動的に実行されます。

フィルタリングモードが「対話モード」の場合

新しいネットワーク接続を検出するたびに確認画面が表示されます。確認画面には、接続に関する詳細情報が表示されます。また、接続を許可するか拒否するかを選択することができます。同じネットワーク接続を繰り返し許可する場合は、接続の新しいルールを作成することをお勧めします。［アクションを記憶する（ルールを作成する）］をチェックして接続を許可または拒否すると、ファイアウォールの新しいルールとして保存されます。以降は、ファイアウォールで同じネットワーク接続が認識されると、自動的にルールが適用されます。［このプロセスに対するアクションを一時的に記憶する］をチェックすると、許可／拒否のアクションが一時的に記憶され、同じネットワーク接続が認識されるたびに同じアクションが実行されます。一時的に記憶されたアクションは、アプリケーションの再起動、ルールまたはフィルタリングモードの変更、ファイアウォールの更新、システムの再起動のいずれかを行うと削除されます。

新しいルールを作成する際は、安全であることがわかっているネットワーク接続だけを許可してください。すべての接続を許可すると、ファイアウォールの役割を果たすことができません。ネットワーク接続に関する重要なパラメーターは次のとおりです。

- ローカルアプリケーション：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。
- リモートコンピューター：信頼できる既知のアドレスへの接続のみを許可します。
- ポート番号：通常の状況では、共通ポート（ポート番号 80 の Web トラフィックなど）を許可する必要があります。

マルウェアは多くの場合、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様々な攻撃から保護するための有効なツールとなります。

●ファイアウォールの問題解決

ESET Endpoint Security をインストールした状態で接続の問題が発生した場合は、ファイアウォールが原因になっているかどうかを複数の方法で判断できます。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方法は、次のとおりです。

- トラブルシューティングウィザード
- 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
- 詳細 PCAP ロギング
- プロトコルフィルタリングの問題解決

トラブルシューティングウィザード

トラブルシューティングウィザードでは、すべてのブロックされた接続をバックグラウンドで監視し、特定のアプリケーションまたはデバイスのファイアウォールに関する問題の解決策を案内します。トラブルシューティングウィザードに従って問題やアクションを選択すると、新しいファイアウォールルールを作成できます。トラブルシューティングウィザードは、メインメニューの［設定］>［ネットワーク］>［トラブルシューティングウィザード］をクリックすると表示されます。

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、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。ファイアウォールでブロックしたくない項目をログで確認する場合は、メインメニューの［ツール］>［ログファイル］で、プルダウンメニューから［ネットワーク保護］を選択し、項目を右クリックして［同様のイベントを今後ブロックしない］を選択すると、ルールまたは IDS 例外を作成できます。問題が解決したら、ロギングをオフにします。

ロギングを使用すると、ファイアウォール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。

ログの詳細については、「4.6.16 ログファイル」を参照してください。

ワンポイント

ブロックされたすべての接続をログに記録すると、問題のないログも多数含まれるため、確認したいログが見つけにくくなる可能性があります。

・ログからルールを作成

本バージョンでは、ログからルールを作成できます。メインメニューの［ツール］>［ログファイル］をクリックし、ドロップダウンメニューから［ネットワーク保護］を選択すると、ファイアウォールのログが一覧に表示されます。目的のログを右クリックし、［同様のイベントを今後ブロックしない］を選択すると、通知画面に作成された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できるようにするには、ESET Endpoint Security を次のように設定する必要があります。

- ［詳細設定］（【F5】キー）>［ツール］>［ログファイル］をクリックし、［ログに記録する最低レベル］ドロップダウンメニューから［診断］を選択します。
- ［詳細設定］（【F5】キー）>［ネットワーク保護］>［ネットワーク攻撃保護］>［詳細設定オプション］>［侵入検出］をクリックし、「セキュリティホールに対する受信攻撃の通知も表示」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

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画面が表示されます。通知画面のリンクをクリックすると、イベントの詳細を確認し、必要に応じてイベントの例外を設定できます。

! 重　要

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、ファイアウォールや IDS からの通知が繰り返される可能性があります。通知から直接例外を作成し、ファイアウォールが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。

詳細 PCAP ロギング

詳細 PCAP ロギングは、CITS カスタマーサポートに複雑なログファイルを提供するための機能です。CITS カスタマーサポートから要請があった場合のみ使用してください。詳細 PCAP ロギング機能は大量のログファイルが生成されるため、コンピューターの処理速度が低下するおそれがあります。

プロトコルフィルタリングの問題解決

Web 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、プロトコルフィルタリングに問題がないかを確認します。メインメニューの［設定］>［詳細設定］をクリックするか、【F5】キーを押して「詳細設定」画面を表示し、「詳細設定」>［WEB とメール］>［プロトコルフィルタリング］をクリックして、［アプリケーションプロトコルフィルタリングを有効にする］を無効にします。プロトコルフィルタリングの問題が解決したら、次の各問題を確認して、対応してください。

! 重　要

問題が解決したら、必ず「アプリケーションプロトコルフィルタリングを有効にする」を有効に戻してください。無効のままだと Web ブラウザーと電子メールクライアントが保護されなくなります。

・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 プロトコルフィルタリングが有効な場合、一時的に無効にしてください。問題が解決した場合は、問題がある通信を除外すると、SSL フィルタリングが有効な状態で更新することができます。
- SSL プロトコルフィルタリングを無効にしても問題が解決しない場合は、SSL プロトコルフィルタリングを有効に戻してから、SSL プロトコルフィルタリングモードを「対話モード」に切り替えます。アプリケーションの更新に戻ると、暗号化された通信トラフィックについての通知画面が表示されます。アプリケーション名が一致しており、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。通知画面が表示されなくなったら、SSL プロトコルフィルタリングモードを「自

動モード」に戻します。

- 問題のアプリケーションが Web ブラウザーまたは電子メールクライアント以外の場合は、プロトコルフィルタリングの除外されたアプリケーションで除外できます。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除外されたアプリケーションの一覧に登録されているため、手動で追加する必要はありません。

! 重 要

Web ブラウザーまたは電子メールクライアントは除外されたアプリケーションに追加しないでください。システムが危険にさらされます。

・ネットワーク上のデバイスへのアクセスに関する問題

Web カメラの Web サイトを開けない、メディアプレイヤーで動画を再生できないなど、ネットワーク上のデバイスの機能を使用できない場合は、デバイスの IPv4 および IPv6 アドレスを除外されたアドレスの一覧に追加します。

・特定の Web サイトの問題

URL アドレス管理を使用すると、プロトコルフィルタリングから特定の Web サイトを除外できます。例えば、https://www.example.com にアクセスできない場合は、除外されたアドレスの一覧に *example.com* を追加します。

・「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」というエラーメッセージが表示される問題

SSL プロトコルフィルタリングを有効にすると、ESET Endpoint Security はインストールされたアプリケーションの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アプリケーションが信頼することを確認します。Firefox、Opera など、一部のアプリケーションでは、実行中にこの処理ができません。タスクマネージャーの［プロセス］タブで、実行中にルート証明書をインポートできないアプリケーション（firefox.exe、opera.exe など）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問題

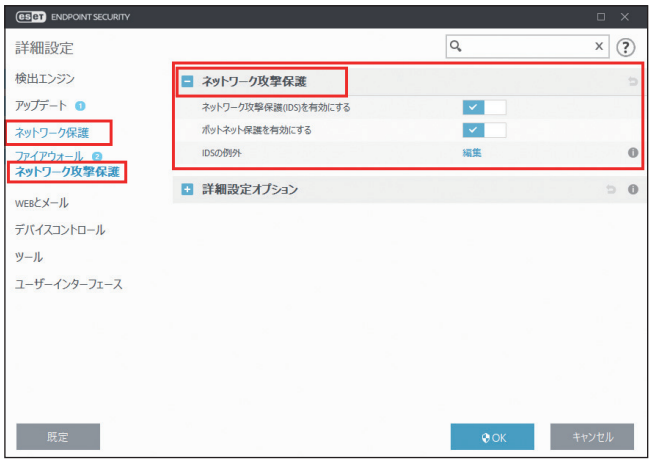
一般的に、ルート証明書のインポートが失敗したことを意味します。まず、ルート証明書をインポートできないアプリケーションが実行されていないことを確認します。次に、SSL プロトコルフィルタリングを無効にし、もう一度有効にします。これでルート証明書のインポートが再度実行されます。

4.6.8 ネットワーク攻撃保護

「ネットワーク攻撃保護」では、コンピューターで実行中のサービスの一部に信頼ゾーンからアクセスするように構成し、コンピューターに被害を与えるために使用されるおそれがあるさまざまなタイプの脅威の検出を有効または無効にできます。

■ネットワーク攻撃保護

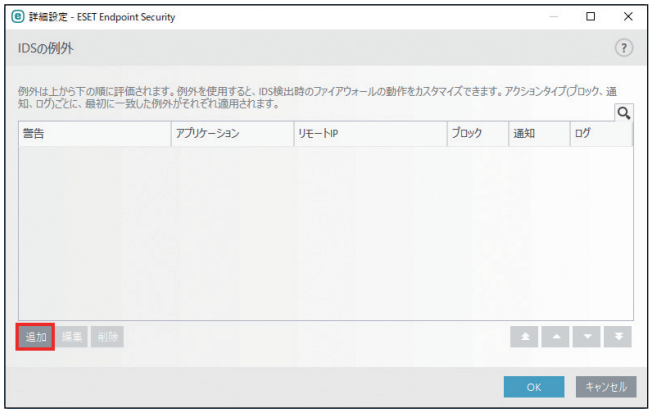
ネットワーク攻撃保護を設定するには、「詳細設定」画面で［ネットワーク保護］＞［ネットワーク攻撃保護］＞［ネットワーク攻撃保護］をクリックします。



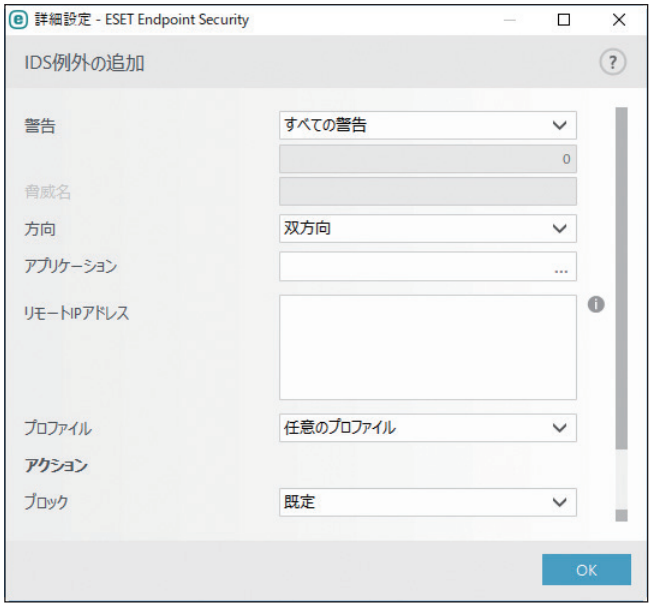
ネットワーク攻撃保護（IDS）を有効にする	通信トラフィックの内容を分析し、ネットワーク攻撃から保護します。有害であるとみなされるすべての通信トラフィックがブロックされます。
ボットネット保護を有効にする	コンピューターが感染した場合や、ボットが通信を試みているときに、一般的なパターンに基づいて、悪意のあるコマンドとの通信およびコントロールサーバーを検出してブロックします。
IDS の例外	「IDS の例外」では、例外を設定することで IDS 検出におけるファイアウォールの動作をカスタマイズできます（詳細は「● IDS の例外」を参照してください）。

● IDS の例外

「IDS の例外」では、例外を設定することで IDS 検出におけるファイアウォールの動作をカスタマイズできます。「IDS の例外」を設定するには、【F5】キーを押して「詳細設定」画面を表示し、［ネットワーク保護］＞［ネットワーク攻撃保護］＞［IDS の例外］の［編集］リンクをクリックして「IDS の例外」画面を表示します。



［追加］をクリックすると「IDS 例外の追加」画面が表示されます。



警告	警告の種類を選択します。
脅威名	脅威名を入力します。この設定は、選択した警告の種類によっては、入力できません。
方向	通信の方向を選択します。
アプリケーション	対象のアプリケーションの実行ファイルを指定します。
リモート IP アドレス	IP アドレスまたはサブネットを設定します。複数設定する場合は「,」で区切ります。
プロファイル	使用するプロファイルを指定します。
アクション	「ブロック」「通知」「ログ」に対する動作を「既定」「除外する」「除外しない」から選択します。
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。特定のアプリケーション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します。

［編集］をクリックすると設定されている IDS 除外を編集できます。
［削除］をクリックすると設定されている IDS 除外を削除できます。

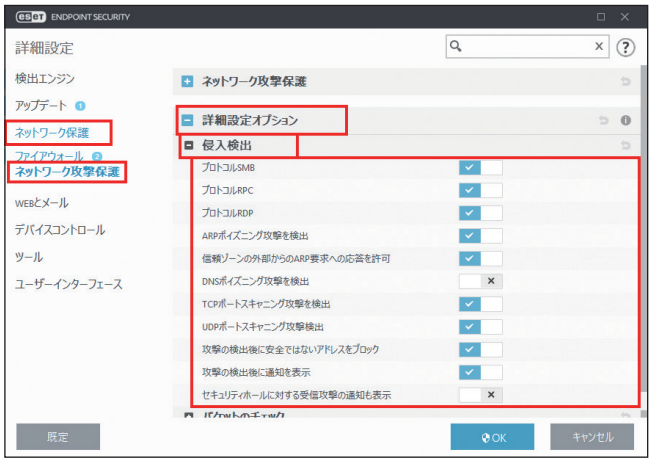
設定した IDS 例外は上から下に順番に評価されます。矢印アイコンで設定の順番を変更することができます。

■詳細設定オプション

「詳細設定オプション」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を検出する、詳細なフィルタオプションを設定できます。

●侵入検出

侵入検出の設定を行うときは、「詳細設定」画面で［ネットワーク保護］＞［ネットワーク攻撃保護］＞［詳細設定オプション］＞［侵入検出］をクリックします。

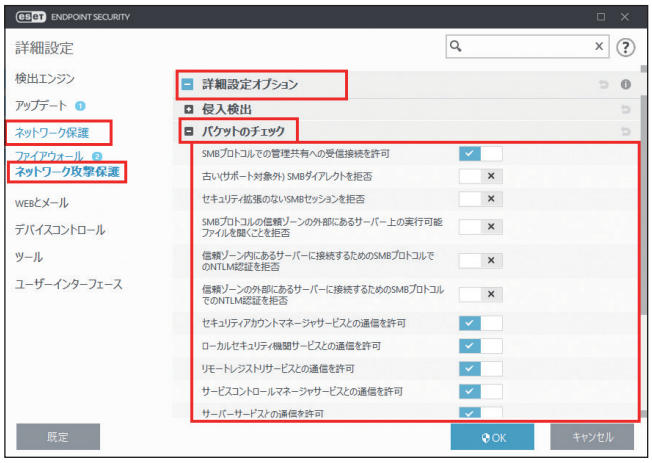


侵入検出

プロトコル SMB	SMB プロトコルの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。
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やネットワークスイッチにおける盗聴を検出します。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。
信頼ゾーンの外部からの ARP 要求への応答を許可	信頼ゾーン以外の IP アドレスを含む ARP 要求にシステムが応答するようにする場合は、このオプションを選択します。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によって使用されます。
DNS ポイズニング攻撃を検出	DNS 要求に対して悪意のある偽の Web サイトに誘導する偽の回答（攻撃者が送信）である DNS ポイズニングの受信を検出します。
TCP ポートスキャニング攻撃を検出	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ために、ポートアドレスにクライアント要求を送信してホストの開いているポートを調べるポートスキャニングソフトウェアによる攻撃を検出します。
UDP ポートスキャニング攻撃を検出	UDP ポートスキャニングによる攻撃を検出します。
攻撃の検出後に安全ではないアドレスをブロック	攻撃元の IP アドレスは、一定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。
攻撃の検出後に通知を表示	システムトレイに通知を表示します。
セキュリティホールに対する受信攻撃の通知も表示	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

パケットのチェックの設定を行うときは、「詳細設定」画面で［ネットワーク保護］＞［ネットワーク攻撃保護］＞［詳細設定オプション］＞［パケットのチェック］をクリックします。



パケットのチェック

SMB プロトコルでの管理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 セッションを拒否します。
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します。
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	信頼ゾーンに属していないサーバー上の共有フォルダーにある実行可能ファイルを開こうとすると接続を切断します。
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	信頼ゾーンの外側にあるサーバーでの NTLM 認証を切断します。
信頼ゾーンの外部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	信頼ゾーンの内側にあるサーバーでの NTLM 認証を切断します。
セキュリティアカウントマネージャサービスとの通信を許可	セキュリティアカウントマネージャサービスとの通信を許可します。
ローカルセキュリティ機関サービスとの通信を許可	ローカルセキュリティ機関サービスとの通信を許可します。
リモートレジストリサービスとの通信を許可	リモートレジストリサービスとの通信を許可します。
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	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します。

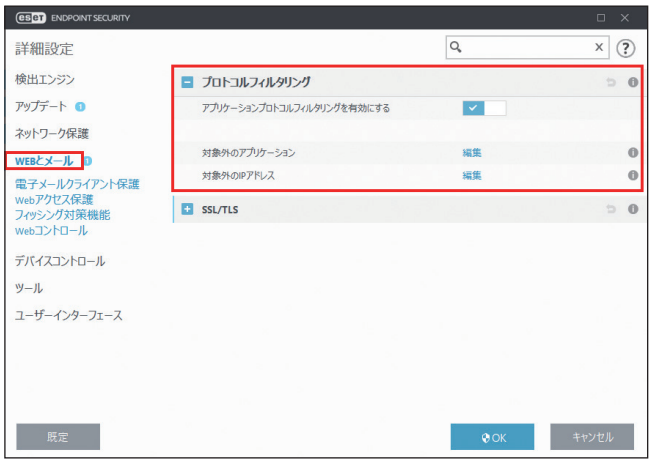
サーバーサービスとの通信を許可	サーバーサービスとの通信を許可します。
他のサービスとの通信を許可	他のサービスとの通信を許可します。
TCP 接続状態のチェック	すべての TCP パケットが既存の接続に属しているかどうかを調べます。接続に属さないパケットがある場合、パケットは削除されます。
TCP 接続状態のチェック	すべての TCP パケットが既存の接続に属しているかどうかを調べます。接続に属さないパケットがある場合、パケットは削除されます。
TCP プロトコルオーバーロードを検出	TCP プロトコルオーバーロードを検出します。
ICMP プロトコルメッセージのチェック	ICMP プロトコルの脆弱性を利用する攻撃を防止します。
ICMP プロトコルの秘密データを検出	ICMP プロトコルがデータ転送に使用されていないかどうかを調べます。

4.6.9 WEB とメール

■プロトコルフィルタリング

プロトコルフィルタリングとは、高度なマルウェアスキャン技術を統合した、ThreatSense 検査エンジンのアプリケーションプロトコルに対するウイルス対策機能です。プロトコルフィルタリングは、使用している Web ブラウザーや電子メールクライアントに関係なく、自動的に動作します。

プロトコルフィルタリングを設定するには、「詳細設定」画面で、［WEB とメール］>［プロトコルフィルタリング］をクリックします。

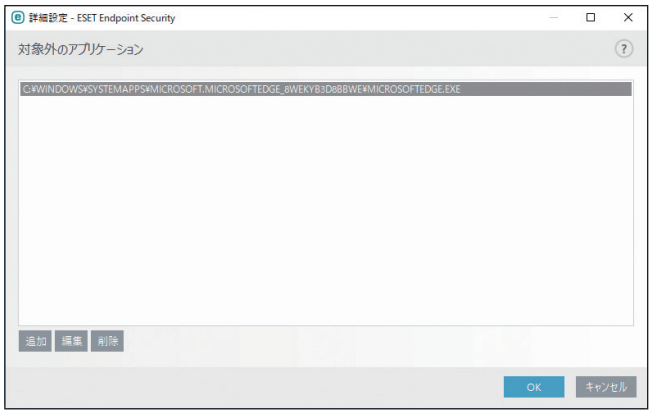


アプリケーションプロトコルフィルタリングを有効にする	プロトコルフィルタリングの有効／無効を設定します。ほとんどの ESET Endpoint Security コンポーネント（Web アクセス保護、電子メールプロトコル保護、フィッシング対策、Web コントロール）はプロトコルフィルタリングを利用しており、無効にすると動作しません。
対象外のアプリケーション	特定のアプリケーションをプロトコルフィルタリングから除外します。プロトコルフィルタリングで互換性の問題があるときに有効です（詳細は「●対象外のアプリケーション」を参照してください。）。
対象外の IP アドレス	特定のリモートアドレスをプロトコルフィルタリングから除外します。プロトコルフィルタリングで互換性の問題があるときに有効です（詳細は「●対象外の IP アドレス」を参照してください。）。

●対象外のアプリケーション

特定のネットワーク対応アプリケーションの通信をプロトコルフィルタリングから除外するには、対象外のアプリケーションリストに対象のアプリケーションを追加します。追加したアプリケーションの HTTP/POP3/IMAP 通信では、マルウェアが検査されません。プロトコルフィルタリングを有効にすると正常に機能しないアプリケーションのみ登録することをお勧めします。

対象外のアプリケーションリストを表示するには、「対象外のアプリケーション」の［編集］リンクをクリックします。

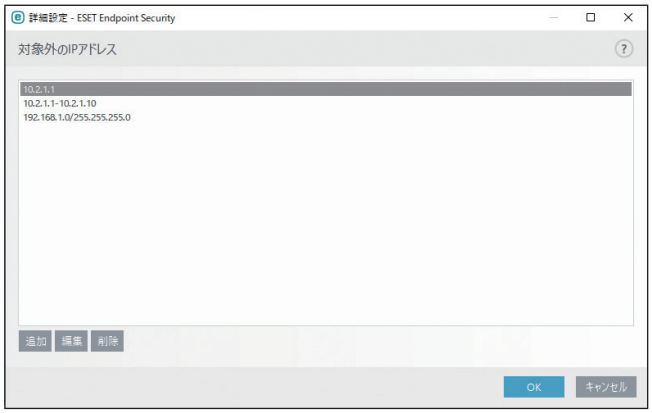


追加	クリックすると、「アプリケーションの追加」画面が表示され、プロトコルフィルタリングを利用しているアプリケーションとサービスが一覧で表示されます。対象外にするアプリケーションやサービスを選択し、［OK］をクリックします。
編集	対象外のアプリケーションやサービスを編集します。
削除	対象外のアプリケーションやサービスを削除します。

●対象外の IP アドレス

特定の IP アドレスとの通信をプロトコルフィルタリングから除外するには、対象外の IP アドレスリストに対象の IP アドレスを追加します。登録した IP アドレスとの HTTP/POP3/IMAP 通信では、マルウェアが検査されません。信頼できる IP アドレスのみ登録することをお勧めします。

対象外の IP アドレスリストを表示するには、「対象外の IP アドレス」の［編集］リンクをクリックします。



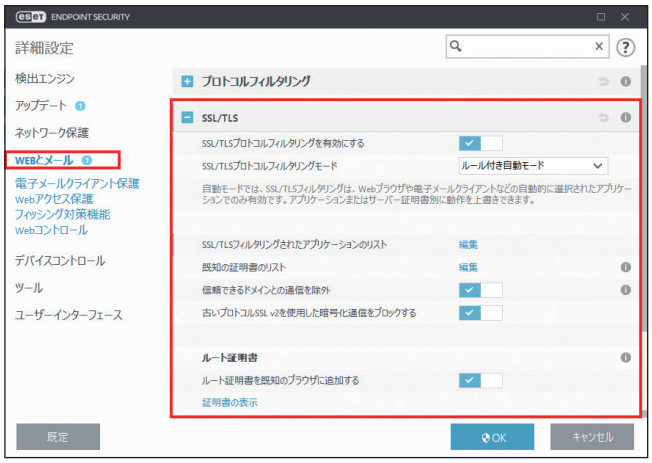
追加	プロトコルフィルタリングから除外するリモートアドレスの IP アドレス／アドレス範囲／サブネットを追加します。
編集	対象外の IP アドレスを編集します。
削除	対象外の IP アドレスを削除します。

● Web と電子メールクライアント

悪意のある多数のコードがインターネットを通じて広まっているため、コンピューターを保護するには、安全にインターネットを閲覧できることが非常に重要です。悪意のあるコードは、Web ブラウザーの脆弱性や不正なリンクを利用して、気付かれないようにシステムに侵入します。そのため、ESET Endpoint Security では Web ブラウザーのセキュリティに重点を置いています。Web とメールクライアントでは、ネットワークに接続する各アプリケーションを Web ブラウザーとして指定することができます。選択したパスから通信しているアプリケーション、または既にプロトコルを使用しているアプリケーションを Web とメールクライアントのリストに追加します。

■SSL/TLS

ESET Endpoint Security は SSL プロトコルを使用する通信で脅威を検査できます。SSL 通信の検査には、信頼できる証明書、不明な証明書、SSL 通信の検査対象から除外された証明書を使用する、様々な検査モードがあります。
SSL 通信の検査を設定するには、「詳細設定」画面で、［WEB とメール］>［SSL/TLS］をクリックします。



SSL/TLS プロトコルフィルタリングを有効にする	SSL/TLS プロトコルフィルタリングの有効／無効を設定します。無効にすると、SSL 通信は検査されません。	
SSL/TLS プロトコルフィルタリングモード	ルール付き自動モード	検査対象から除外された証明書で保護されている通信以外の SSL 通信を検査します。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は、ユーザーに通知されず、通信は自動的にフィルタリングされます。また、信頼できる証明書に登録されている信頼できない証明書を使用してサーバーにアクセスした場合は、通信は許可され、通信チャネルのコンテンツがフィルタリングされます。
	対話モード	不明な証明書を使用して新しい SSL 通信を行う場合に、アクション選択画面が表示されます。アクション選択画面では、検査から除外する SSL 証明書のリストを作成できます。
	ポリシーベースモード	ルールに従って動作します。ルールにない実行動作は、ブロックされます。
SSL/TLS フィルタリングされたアプリケーションのリスト	SSL/TLS フィルタリングされたアプリケーションのリストは、特定のアプリケーションに対する ESET Endpoint Security 動作をカスタマイズできます。SSL/TLS プロトコルフィルタリングモードで対話モードが選択された場合に選択されたアクションを記憶できます。詳細について、「● SSL/TLS フィルタリングされたアプリケーションのリスト」を参照してください。	
既知の証明書のリスト	特定の SSL 証明書に対する ESET Endpoint Security の動作をカスタマイズできます。詳細については、「●既知の証明書のリスト」を参照してください。	

信頼できるドメインとの通信を除外	信頼できるドメインとの通信をフィルタリングから除外するかどうかの設定を行います。ドメインの信頼性は、ビルトインのホワイトリストによって決定されます。
古いプロトコル SSLv2 を使用した暗号化通信をブロックする	SSL プロトコルの従来のバージョンを使用した通信をブロックするかどうかを設定します。

●ルート証明書

Web 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。

ルート証明書を既知の Web ブラウザーに追加	ESET ルート証明書が既知の Web ブラウザー（Opera、Firefox など）に自動的に追加されます。また、システム証明書の保存先を使用する Web ブラウザー（Internet Explorer など）には、証明書が自動的に追加されます。
証明書の表示	ESET Endpoint Security でサポートしていない Web ブラウザーに証明書を適用します。

●証明書の有効性

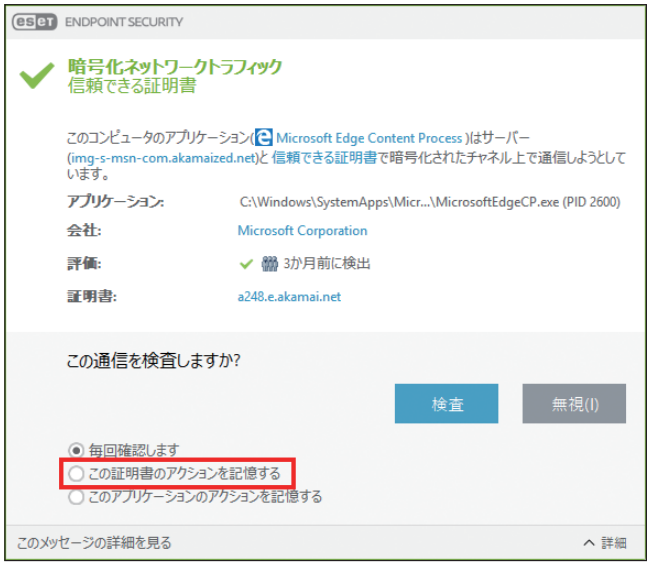
信頼できるルート認証局ストアを使用して証明書を検証できない場合	銀行などの多くの大企業で使用されている Trusted Root Certification Authorities（TRCA）ストアによって署名された証明書は、ユーザーによって自己署名されており、信頼できるとみなしても必ずしもリスクにはならないため、検証できない場合があります。［証明書の有効性を確認］を選択すると、ユーザーは暗号化通信の確立時にアクションを選択するよう求められます。［証明書を使用する通信をブロック］を選択すると、未検証の証明書を使用した Web サイトへの暗号化接続を常にブロックします。
証明書が無効または破損している場合	期限切れ、または不正に自己署名されている証明書を使用する通信は、ブロックすることをお勧めします。

暗号化された SSL 通信

SSL プロトコルを検査するようにコンピューターが設定されている場合、次の 2 つの状況でアクションの選択を求めるダイアログボックスが表示されます。

Web サイトが検証不可能または無効な証明書を使用し、ESET Endpoint Security の設定が証明書の有効性を確認するように設定されている場合は、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。

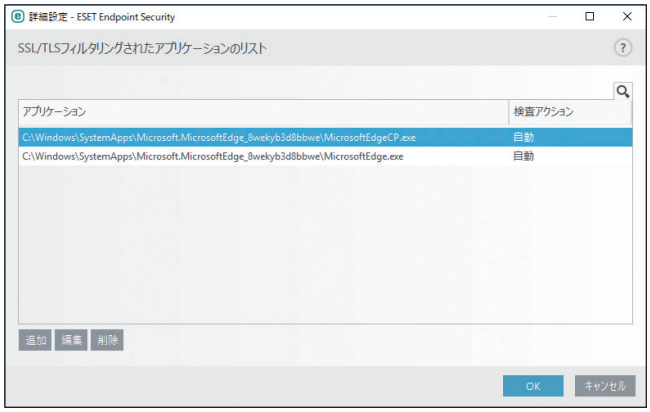
SSL/TLS プロトコルフィルタリングモードが「対話モード」に設定されている場合は、トラフィックを検査するか無視するかを確認するダイアログボックスが表示されます。SSL トラフィックが修正または検査されていないことを確認するアプリケーションが起動している場合、ESET Endpoint Security は SSL トラフィックを無視し、アプリケーションを動作させ続けます。



いずれの場合も、［この証明書のアクションを記憶する］をチェックしてからアクションを選択すると、選択したアクションを記憶できます。記憶されたアクションは「既知の証明書のリスト」に保存されます。

● SSL/TLS フィルタリングされたアプリケーションのリスト

SSL/TLS フィルタリングされたアプリケーションのリストを使用すると、特定のアプリケーションに対する ESET Endpoint Security の動作をカスタマイズし、対話モードが SSL/TLS プロトコルフィルタリングモードで選択された場合に選択されたアクションを記憶できます。［詳細設定］（【F5】キー）> ［Web とメール］> ［SSL/TLS］> ［SSL/TLS フィルタリングされたアプリケーションのリスト］の［編集］リンクをクリックすることで、SSL/TLS フィルタリングされたアプリケーションのリストウィンドウを表示および編集できます。

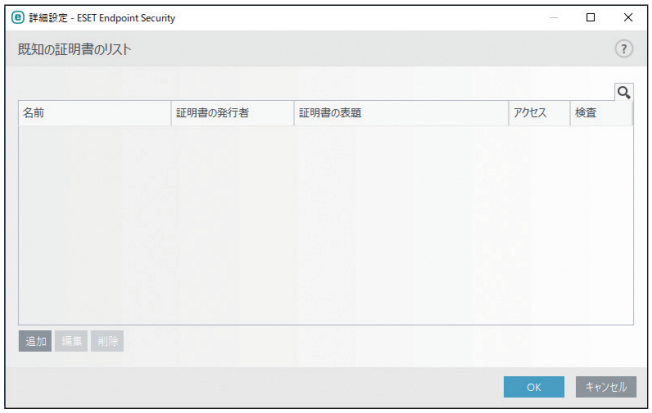


アプリケーション名	アプリケーションの名前。
検査アクション	スキャンまたは無視を選択して通信をスキャンまたは無視します。 自動を選択すると、自動モードでは検査し、対話モードでは確認を行えます。［確認する］を選択すると、常に処理方法をユーザーに確認します。
追加	フィルタリングされたアプリケーションを追加します。
編集	設定するアプリケーションを選択し、［編集］をクリックすると、「フィルタリングされたアプリケーションの編集」画面表示され、検査アクションを編集できます。
削除	削除したアプリケーションを選択し、［削除］をクリックすると、そのアプリケーションを削除できます。

●既知の証明書のリスト

既知の証明書のリストを使用すると、特定の SSL 証明書に対する ESET Endpoint Security の動作をカスタマイズし、SSL/TLS プロトコルフィルタリングモードが「対話モード」に設定されているときに、選択されたアクションを記憶できます。

既知の証明書のリストを表示するには「詳細設定」画面で、［WEB とメール］>［SSL/TLS］>「既知の証明書のリスト」の［編集］リンクをクリックします。

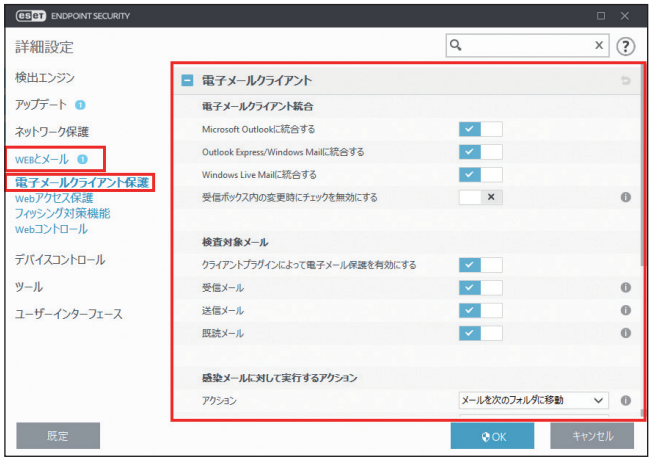


名前	証明書の名前が表示されます。
証明書の発行者	証明書の作成者名が表示されます。
証明書の表題	表題パブリックキーフィールドのパブリックキーに関連付けられたエンティティが表示されます。
アクセス	SSL 通信時のアクションが表示されます。［許可］または［ブロック］に設定されている場合は、信頼性に関係なく、証明書で保護された通信を許可またはブロックします。［自動］に設定されている場合は、信頼できる証明書は通信を許可し、信頼できない証明書はユーザーにアクションを確認します。［確認］に設定されている場合は、常にアクションをユーザーに確認します。
検査	SSL 通信時の検査アクションが表示されます。［検査］または［無視］に設定されている場合は、証明書で保護された通信を検査または無視します。［自動］に設定されている場合は、SSL/TLS プロトコルフィルタリングモードが［自動モード］の場合は検査し、［対話モード］の場合はユーザーにアクションを確認します。［確認］に設定されている場合は、常に検査アクションをユーザーに確認します。
追加	SSL 証明書を追加します。
編集	SSL 証明書を編集します。
削除	SSL 証明書を削除します。

4.6.10 電子メールクライアント保護

■電子メールクライアント

ESET Endpoint Security を電子メールクライアントと統合すると、電子メールに含まれる悪意のあるコードからコンピューターを保護するレベルが向上します。統合できるのは ESET Endpoint Security でサポートしている電子メールクライアントのみです。統合すると、電子メールクライアントに ESET Endpoint Security のツールバーが挿入され（新しいバージョンの Windows Live Mail を除く）、電子メールを効率的に保護できます。統合を有効にするには「詳細設定」画面で、［WEB とメール］>［電子メールクライアント保護］>［電子メールクライアント］をクリックします。



電子メールクライアント統合

次の電子メールクライアントの統合の有効／無効を設定します。

- Microsoft Outlook
- Outlook Express / Windows メール
- Windows Live メール

電子メールの保護は、電子メールクライアントの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。暗号化された電子メールを電子メールクライアントが受信した場合、電子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。サポートしている電子メールクライアントとそのバージョンの総合リストは、弊社ホームページ「対応しているメールソフトウェアについて」を参照してください。

https://eset-support.canon-its.jp/faq/show/161?site_domain=business

！重　要

統合していない場合でも、電子メールプロトコル保護機能によって、POP3 および IMAP プロトコルによる電子メール通信は保護されます。

ワンポイント

Kerio Outlook Connector Store から電子メールを受信するときに、システムの速度が低下する場合は、「受信ボックスの内容変更時のチェックを無効にする」を有効にしてください（Microsoft Outlook のみ有効）。

検査対象メール

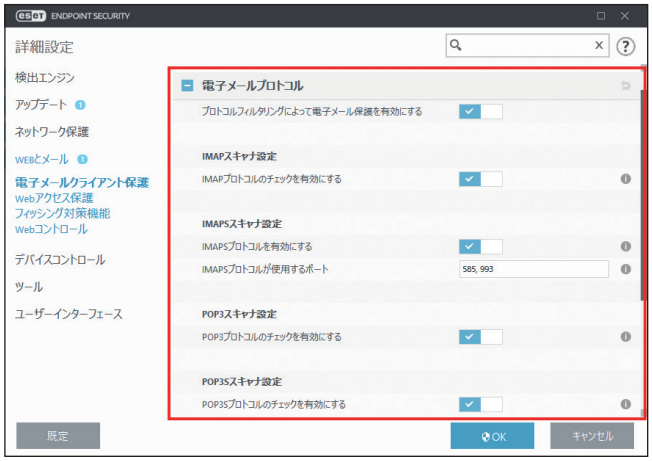
クライアントプラグインによって電子メール保護を有効にする	電子メールクライアントによる電子メールクライアント保護が無効な場合でも、プロトコルフィルタリングによる電子メールクライアントの確認は有効です。
受信メール	受信メールを検査します。
送信メール	送信メールを検査します。
既読メール	既読メールを検査します。

感染メールに対して実行するアクション

アクション	何もしない	感染している添付ファイルは特定されますが、電子メールはそのまま残ります。
	メールの削除	感染メールの受信が通知され、メールは削除されます。
	メールをごみ箱に移動する	感染メールを自動的にゴミ箱（削除済みフォルダー）に移動します。
	メールを次のフォルダに移動	感染メールを指定したフォルダーに自動的に移動します。[移動先のフォルダ] に感染メールを移動させるフォルダー名を入力します。
移動先のフォルダ	感染した電子メールを移動するフォルダーを指定します。	
アップデート後に再度検査を行う	有効にすると、検出エンジンのアップデート後に、再度電子メールを検査します。	
ほかの機能の検査結果を受け入れる	有効にすると、電子メールプロトコル検査の検査結果を反映します。	

■電子メールプロトコル

IMAP、IMAPS、POP3、POP3S プロトコルは、電子メールクライアントの電子メール受信で使用されるプロトコルです。ESET Endpoint Security は、使用する電子メールクライアントに関係なく、また電子メールの設定を変更しなくても、これらのプロトコルを検査します。



プロトコルフィルタリングによって電子メール保護を有効にする	電子メールプロトコル保護有効 / 無効を設定します。
IMAP プロトコルのチェックを有効にする	IMAP プロトコル検査の有効 / 無効を設定します。
IMAPS プロトコルを有効にする	IMAPS プロトコル検査の有効 / 無効を設定します。
IMAPS プロトコルが使用するポート	IMAPS プロトコルのポートを設定します。
POP3 プロトコルのチェックを有効にする	POP3 プロトコル検査の有効 / 無効を設定します。
POP3S プロトコルのチェックを有効にする	POP3S プロトコル検査の有効 / 無効を設定します。
POP3S プロトコルが使用するポート	POP3S プロトコルのポートを設定します。

■THREATSENSE パラメータ

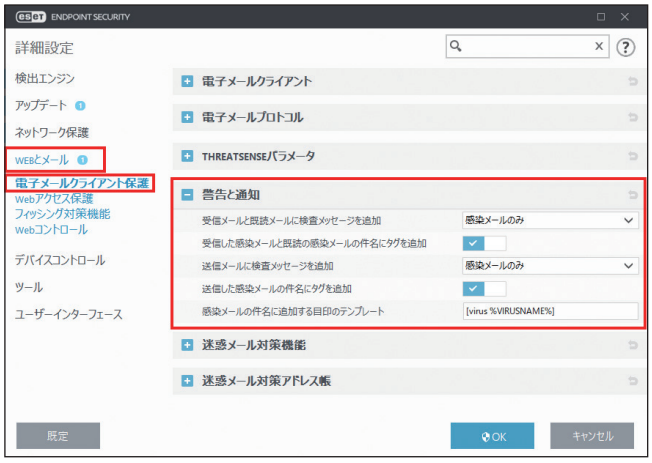
電子メールクライアント保護では、検査対象や検出方法などを設定できます。詳細については、「4.6.2 リアルタイムファイルシステム保護」の「■ THREATSENSE パラメータ」を参照してください。

●制限

既定のオブジェクトの設定	既定のオブジェクトの設定の有効 / 無効を設定します。
オブジェクトの最大サイズ	設定を無効にした場合、最大サイズを指定します。
オブジェクトの最大検査時間	設定を無効にした場合、検査の最長時間を秒数で指定します。
既定のアーカイブ検査の設定	既定のアーカイブ検査の設定の有効 / 無効を設定します。
スキャン対象の下限ネストレベル	設定を無効にした場合、アーカイブのネストレベルを設定します。
スキャン対象ファイルの最大サイズ	設定を無効にした場合、最大サイズを指定します。

■警告と通知

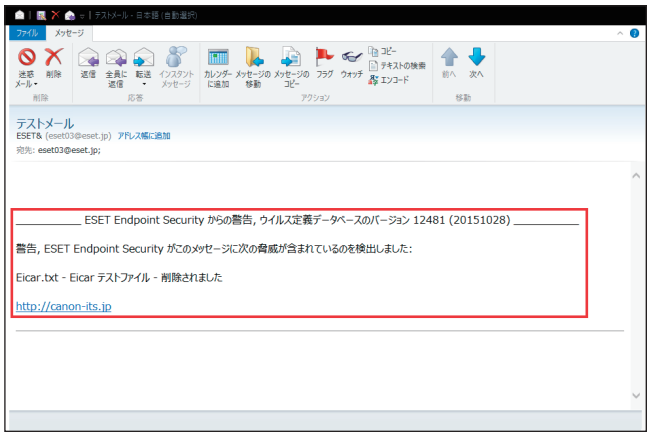
電子メールクライアント保護では、POP3/IMAP プロトコルで受信したメール通信を検査します。ESET Endpoint Security は、Microsoft Outlook 用のプラグインおよびその他の電子メールクライアントを使用して、電子メールクライアントからの全通信（POP3、MAPI、IMAP、HTTP）を検査します。受信メッセージは、ThreatSense エンジンパラメーターの設定に従って検査するため、検出エンジンと照合する前に悪意のあるコードを検出できます。POP3/IMAP プロトコルの通信検査は、電子メールクライアントからは独立しています。



検査結果通知の追加

検査結果の通知を受信／既読メールおよび送信メールに追加できます。「受信メールと既読メールに検査メッセージを追加」および「送信メールに検査メッセージを追加」で、検査通知の追加方法を選択します。

追加しない	検査結果の通知は追加されません。
感染メールのみ	悪意のあるコードを含んでいる電子メールに検査結果の通知が追加されます。
すべての検査済みメール	検査したすべてのメールに検査結果の通知が追加されます。



! 重 要

HTML メールやメール本文自体がマルウェアで偽装されている場合、検査メッセージが追加されないことがあります。

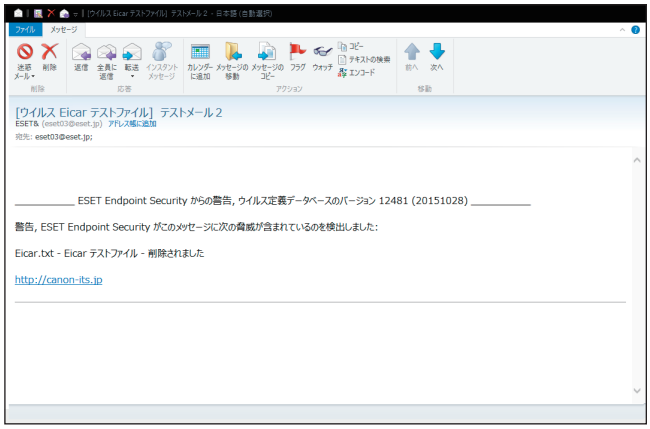
タグの追加

感染している受信メールおよび既読メールの件名にウイルス警告を追加する場合は、「受信した感染メールと既読の感染メールの件名にタグを追加」を有効にします。

感染している送信メールの件名にウイルス警告を追加する場合は、「送信した感染メールの件名にタグを追加」を有効にします。ウイルス警告の追加は、感染している電子メールを件名でフィルタリングする場合に有効です（電子メールクライアントでサポートされている場合）。また、感染している電子メールやマルウェアについての貴重な情報を得ることができます。

感染メールの件名に追加する目印のテンプレート

感染メールの件名に追加するプレフィックス形式を変更するには、「感染メールの件名に追加する目印のテンプレート」のフィールドで編集します。既定ではメッセージの件名「Hello」が、プリフィクス値「[VIRUS]」（[VIRUS] Hello の形式）に置き換えられます。変数の「%VIRUSNAME%」は検出されたマルウェアに置き換えられます。

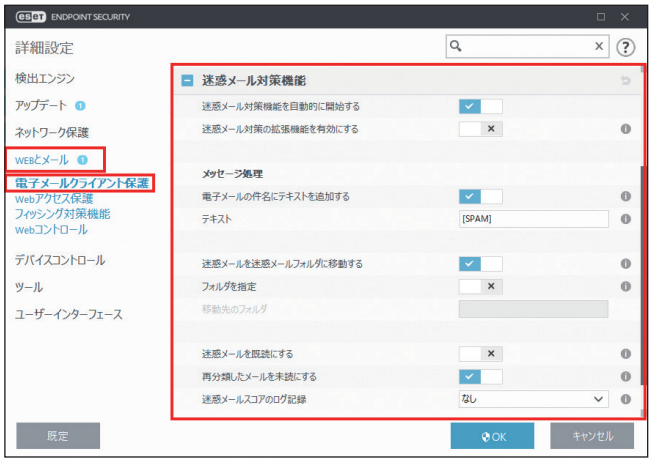


! 重 要

件名に 2 バイトの文字を使用すると、使用している電子メールクライアントによっては文字化けする場合がありますので使用しないでください。

■迷惑メール対策機能

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 80% を占めています。この問題に対処するための機能が、迷惑メール対策機能です。メールセキュリティの複数の機能を組み合わせることで、迷惑メール対策機能のフィルタリング機能を強化し、受信ボックスから常に迷惑メールを駆除した状態にします。



迷惑メール検出の働き

あらかじめ定義された信頼済みのアドレス（ホワイトリスト）と迷惑メールアドレス（ブラックリスト）に基づいて、受信者側が要求していない電子メールを識別します。アドレス帳から抽出したすべてのアドレスが、自動的にホワイトリストに追加されます。さらに、ユーザーが安全と分類したアドレスもすべてホワイトリストに追加されます。

迷惑メール検出の主な方法は、電子メールのプロパティの検査です。受信メールは、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、その他）に基づいて検査されます。そして、検査結果として生成されるインデックス値により、受信メールが迷惑メールかどうかが判定されます。

迷惑メール対策機能の設定

「迷惑メール対策機能を自動的に開始する」を有効にすると、システムの起動時に迷惑メール対策機能が自動的に起動します。

「迷惑メール対策の拡張機能を有効にする」を有効にすると、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の能力が向上します。

迷惑メール対策機能のパラメーター設定

迷惑メール対策機能では、次のような様々なパラメーターを設定できます。

メッセージ処理

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電子メールの件名に、「追加するテキスト」に入力したプリフィクス文字列を追加できます。 既定の文字列は「[SPAM]」です。
迷惑メールを迷惑メールフォルダに移動する	有効にすると、迷惑メールは既定の迷惑メールフォルダーに移動します。
フォルダを指定	有効にすると、「移動先のフォルダ」で指定したフォルダーに迷惑メールを移動します。
迷惑メールを既読にする	有効にすると、迷惑メールが自動的に既読になります。
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、その後迷惑メールではないと分類された電子メールを未読にします。

迷惑メールスコアのログ記録

ESET Endpoint Security の迷惑メール対策用エンジンでは、すべての検査済み電子メールに迷惑メールスコアが割り当てられます。迷惑メールスコアは、迷惑メール対策ログに記録されます。迷惑メール対策ログの記録方法は、次の 3 つから選択できます。

なし	迷惑メールスコアは迷惑メール対策ログに記録されません。
再分類して迷惑メールに設定	迷惑メールとして分類された電子メールの迷惑メール対策ログに、迷惑メールスコアが記録されます。
すべて	すべての迷惑メール対策ログに迷惑メールスコアが記録されます。

迷惑メール対策ログを確認するには、メインメニューの［ツール］>［ログファイル］をクリックし、ドロップダウンメニューから［迷惑メール対策機能］を選択します。

迷惑メール対策エンジン詳細ロギングを有効にする

「詳細設定」画面で［ツール］>［診断］>「迷惑メール対策エンジン詳細ロギングを有効にする」を有効に設定すると、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（「4.6.20　診断」の「■診断」を参照）。

! 重　要

迷惑メールフォルダーの電子メールを右クリックし、［ESET Endpoint Security］>［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、電子メールが受信トレイに移動します。受信トレイの電子メールを右クリックし、［ESET Endpoint Security］>［選択したメッセージを迷惑メールとして再分類］を選択すると、電子メールが迷惑メールフォルダーに移動します。複数の電子メールを選択して、同時に迷惑メールに分類することもできます。

ワンポイント

ESET Endpoint Security の迷惑メール対策機能のサポート、電子メールクライアントについては、以下、弊社ホームページを参照してください。
https://eset-info.canon-its.jp/business/endpoint_protection_adv/spec.html

■迷惑メール対策アドレス帳

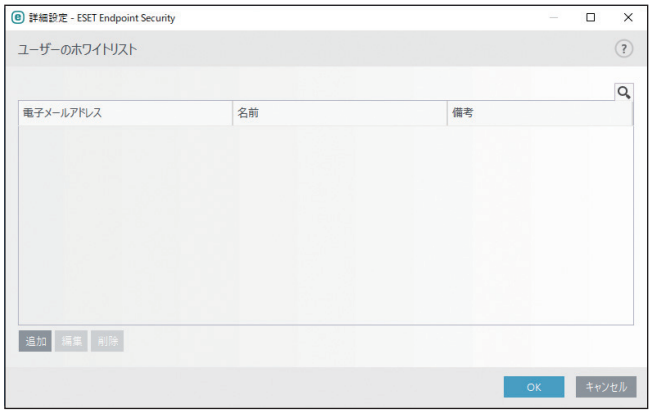
受信者側が要求していない電子メールから保護するために、ESET Endpoint Security では電子メールアドレスを専用のリストに分類することができます。ホワイトリストには安全とみなされた電子メールアドレスが登録されます。ホワイトリストに登録されているアドレスからの電子メールは、常に受信メールフォルダーに格納されます。

ブラックリストには、迷惑メールとして分類された電子メールアドレスが登録されます。ブラックリストに登録されているアドレスからの電子メールは、すべて迷惑メールとして分類されます。

例外リストには、ホワイトリストまたブラックリストに登録されているアドレスの中から、例外として必ず迷惑メールかどうかのチェックを行うアドレスを登録します。例外リストにアドレスを登録すれば、そのアドレスが仮にアドレス帳などから自動的にホワイトリストに追加された場合でも、例外として検査対象とすることができます。

ユーザーのアドレスリストを許可する	ユーザーがメールクライアントで作成したアドレス帳を有効にします。
グローバルアドレスを許可する	すべてのメールユーザー、配布グループ、リソースが入ったグローバルアドレス帳を有効にします。
ユーザーのホワイトリスト	連絡先のリスト。［編集］をクリックすると、安全であると見なされ、メッセージを受信したいアドレスを追加、編集、削除できます。
ユーザーのブラックリスト	連絡先のリスト。［編集］をクリックすると、危険であると見なされ、メッセージを受信したくないアドレスを追加、編集、削除できます。
ユーザーの例外リスト	例外リストには、ホワイトリストまたはブラックリストに登録されているアドレスの中から、例外として必ず迷惑メールかどうかのチェックを行うアドレスを登録します。例外リストにアドレスを登録すると、そのアドレスが仮にアドレス帳などから自動的にホワイトリストに追加された場合でも、例外として検査対象とすることができます。［編集］をクリックすると、除外リストの編集を行えます。
グローバルホワイトリスト／グローバルブラックリスト／グローバル例外リスト	グローバルリストは、ESET Security Management Center を使用して、ネットワークのすべてのワークステーションにグローバルのスパム対策ポリシーを適用する場合などに使用できます。

リスト画面では、［追加］、［編集］、［削除］をクリックして、電子メールアドレスの追加や編集、削除ができます。



●ユーザーのホワイトリストに自動的に追加

アドレス帳からアドレスを追加する	アドレス帳のリストをホワイトリストに追加します。
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ホワイトリストに追加します。
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と再分類されたメールの送信者アドレスをホワイトリストに追加します。

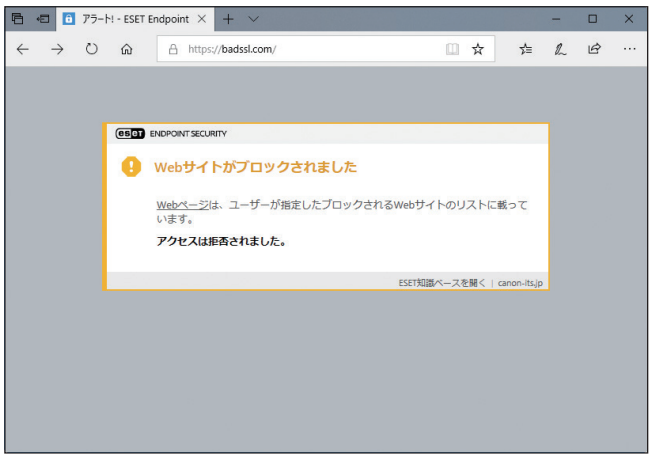
●ユーザーの例外リストに自動的に追加

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のアドレスを例外リストに追加します。

4.6.11 Web アクセス保護

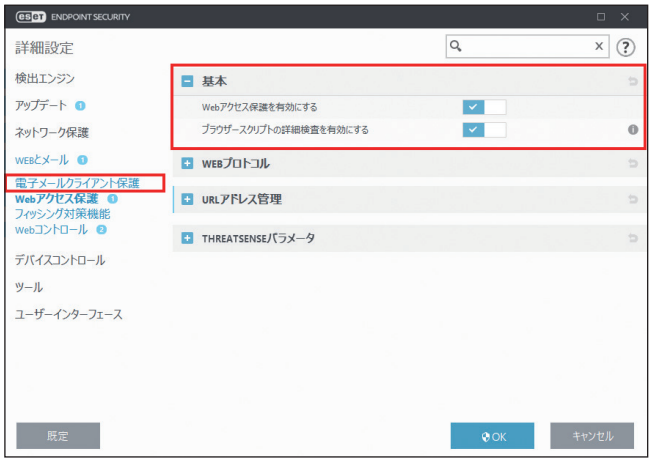
インターネット接続は、コンピューターの標準機能です。しかし、コンピューターによるインターネット接続は、悪意のあるコードを転送する主要な方法になっています。Web アクセス保護は、Web ブラウザーとリモートサーバーとの間で行われる HTTP および HTTPS のルールに準拠した通信を監視します。

Web アクセス保護によって、悪意のあるコンテンツが含まれている Web サイトへのアクセスをブロックします。悪意のあるコンテンツが含まれているかどうか不明な Web サイトは、読み込み時に ThreatSense スキャンによって検査を行い、悪意のあるコンテンツを検出すると、アクセスをブロックします。Web アクセス保護には、ブラックリストによるブロックとコンテンツによるブロックの 2 つの保護レベルがあります。



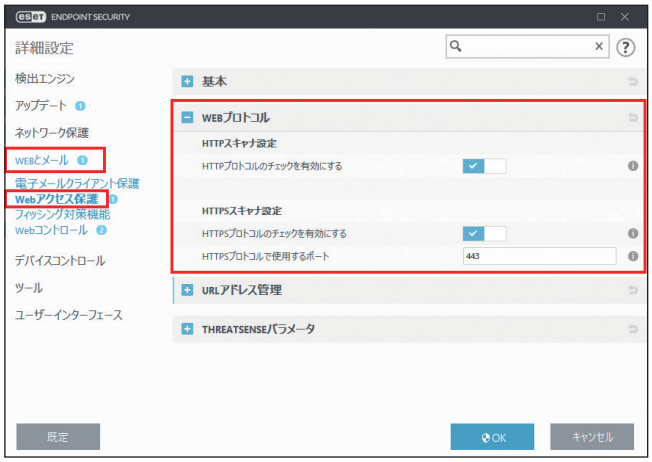
「詳細設定」画面で、［WEB とメール］>［Web アクセス保護］をクリックします。

■基本



Web アクセス保護を有効にする	Web アクセス保護の有効 / 無効を設定します。
ブラウザースクリプトの詳細検査を有効にする	「ブラウザースクリプトの詳細検査を有効にする」を有効すると、インターネットブラウザーで実行されるすべての JavaScript プログラムがウイルス対策スキャナーによって検査されます。

■WEB プロトコル



● HTTP スキャナ設定

既定では、ESET Endpoint Security はほとんどの Web ブラウザーで使用される HTTP プロトコルを監視するように設定されています。

Windows Vista 以降では、Web プロトコルを設定しなくても、すべてのアプリケーションのすべてのポートで、HTTP トラフィックが常に監視されます。

● HTTPS スキャナ設定

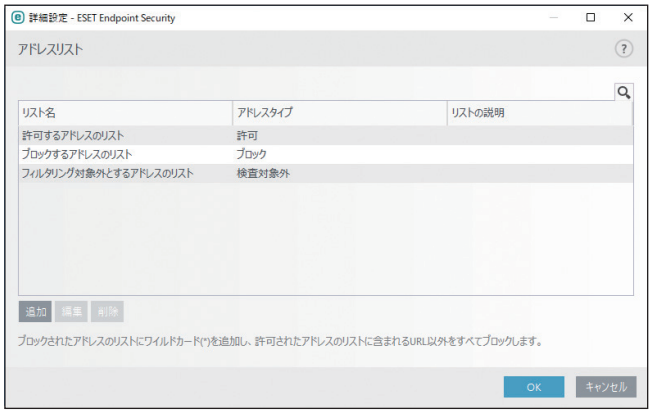
ESET Endpoint Security は HTTPS プロトコルの検査もサポートしています。HTTPS 通信では、暗号化チャンネルを使用して、サーバーとクライアント間で情報を送受信します。ESET Endpoint Security は、SSL（Secure Socket Layer）および TLS（Transport Layer Security）プロトコルを使用した通信を検査します。HTTPS プロトコルの検査は、オペレーティングシステムのバージョンに関係なく、HTTPS プロトコルで使用されるポートの HTTPS トラフィックだけを検査します。既定の設定が使用されている場合は、暗号化された接続は検査されません。暗号化された接続の検査を有効にするには、詳細設定画面を表示し、［Web とメール］＞［SSL/TLS］をクリックし、［SSL/TLS プロトコルフィルタリングを有効にす

る]を選択します。また、HTTP プロトコルや HTTPS プロトコルのチェックの有効 / 無効の設定は、[詳細設定] (F5) > [Web とメール] > [Web アクセス保護] > [Web プロトコル] > [HTTP スキャナ設定] で行えます。

HTTP プロトコルのチェックを有効にする	すべてのポートの HTTP チェックをします。
HTTPS プロトコルで使用するポート	HTTPS プロトコルで使用するポートを設定します。

■URL アドレス管理

「URL アドレス管理」のセクションでは、ブロック、許可、またはチェックから除外する HTTP アドレスを指定できます。「URL アドレス管理」の「アドレスリスト」で［編集］をクリックします。

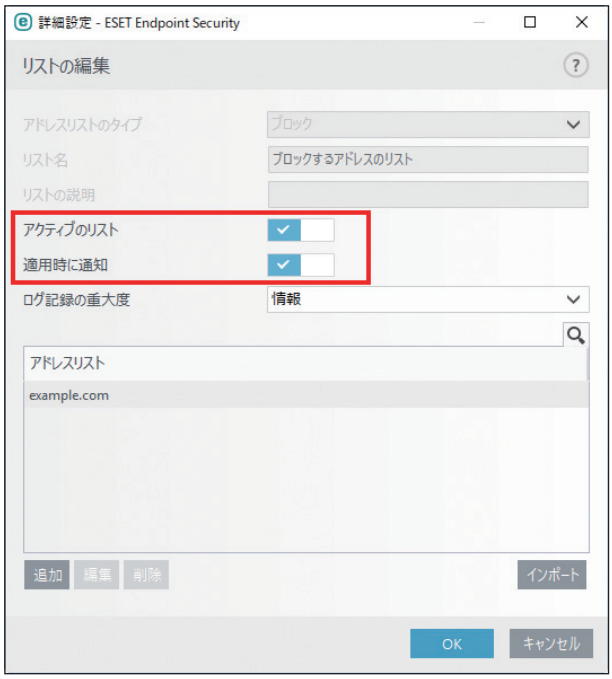


URL アドレス管理では、許可、ブロック、検査から除外する HTTP アドレスを指定できます。既定では、次の 3 つのリストを使用できます。

許可するアドレスのリスト	ブロックする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だけにアクセスできます。このリストのアドレスは、ブロックするアドレスのリストよりも優先されるため、このリストとブロックするアドレスのリストの両方に登録されている場合にも、アクセスが許可されます。
ブロックするアドレスのリスト	ユーザーは、基本的に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。
フィルタリング対象外とするアドレスのリスト	このリストに追加すると、悪意のあるコードのチェックが実行されなくなります。

追加	新しいアドレスリストを作成します。URL アドレスの種類に応じてグループ分けする場合に便利です。例えば、外部パブリックブラックリストの URL アドレスと独自のブラックリストの URL アドレスを、別々のブロックするアドレスリストに登録しておけば、それぞれのアドレスリストを更新するだけで最新のブラックリストが作成できます。
編集	既存のアドレスリストにアドレスを追加したり、アドレスを削除したりできます。
削除	既存のアドレスリストを削除できます。既定のアドレスリストは削除できません。

アドレスリストを有効にするには、アドレスの編集時に「アクティブのリスト」を有効にします。アドレスリストの URL にアクセスしたときに通知する場合は、「適用時に通知」を有効にします。
許可するアドレスリストに登録されているアドレスを除いて、すべての HTTP アドレスをブロックする場合は、ブロックするアドレスリストのアドレスに「*」を追加します。



HTTPS アドレスをフィルタリングする場合は、「SSL/TSL プロトコルフィルタリングを有効にする」を有効にする必要があります。無効の場合は、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。

ワンポイント

すべてのアドレスリストで、特殊記号の「*」（アスタリスク）および「?」（疑問符）を使用できます。アスタリスクは任意の数字または文字を表します。疑問符は任意の 1 文字を表します。検査対象外のアドレスを指定する際は、信頼できる安全なアドレスだけを登録する必要があるため、細心の注意を払って特殊記号を使用してください。

ワンポイント

HTTPS アドレスをフィルタリングする場合は、「HTTPS プロトコルフィルタリングを有効にする」を有効にする必要があります。無効の場合は、アクセスした HTTPS サイトのドメインのみが追加されます

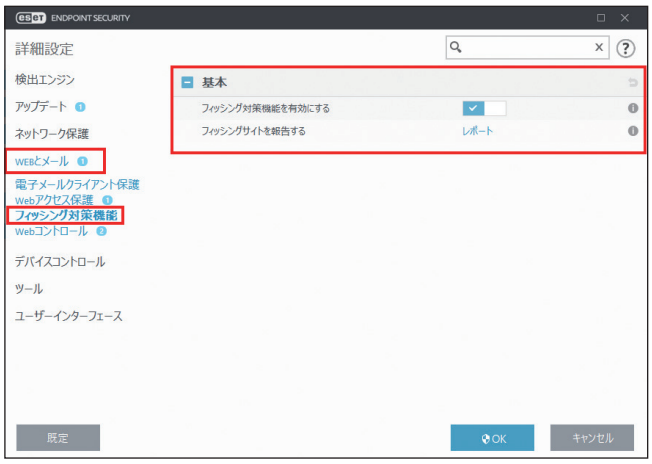
■THREATSENSE パラメータ

[THREATSENSE パラメータ]をクリックすると、Web アクセス保護の検査パラメーターを設定できます。詳細については、「4.6.2　リアルタイムファイルシステム保護」の「■ THREATSENSE パラメータ」を参照してください。

4.6.12 フィッシング対策

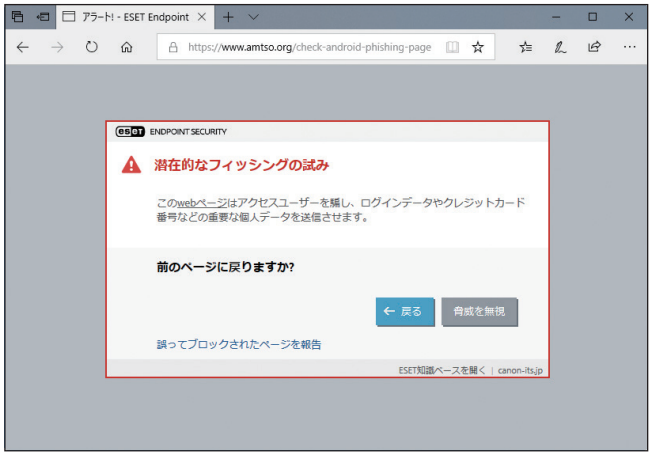
フィッシングとは、ソーシャルエンジニアリング（機密情報を入手するためにユーザーを操ること）を用いる犯罪行為です。フィッシングは、銀行の口座番号や PIN コードなどの機密データを入手するためによく使用されます。
ESET Endpoint Security はフィッシング対策機能を搭載しており、フィッシングサイトへのアクセスをブロックできます。

「詳細設定」画面で、［WEB とメール］>［フィッシング対策機能］をクリックします。



フィッシング対策機能を有効にする	フィッシング対策機能の有効 / 無効を切り替えます。
フィッシングサイトを報告する	［レポート］をクリックすると、ESET 社の「フィッシングページを報告する」サイトにジャンプします。ここでフィッシングページの URL などを報告することができます。

フィッシングサイトにアクセスすると、次の警告画面が Web ブラウザーに表示されます。それでも Web サイトにアクセスする場合は、［脅威を無視］をクリックします。



!重 要

［脅威を無視］の選択は推奨しません。

! 重 要

ホワイトリストに登録されている潜在的なフィッシングサイトは、既定では数時間後に有効期限が切れます。潜在的なフィッシング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。メインメニューの［設定］>［詳細設定］をクリックするか、【F5】キーを押して「詳細設定」画面を表示し、［WEB とメール］>［Web アクセス保護］>［URL アドレス管理］>「アドレスリスト」の［編集］リンクをクリックし、「アドレスリスト」画面を表示します。［許可するアドレスのリスト］を選択して［編集］をクリックし、許可する Web サイトをリストに追加します。

フィッシングサイトの報告

「フィッシングサイトを報告」の［レポート］リンクをクリックすると、フィッシングサイトおよび悪意のある Web サイトを分析のための報告を ESET に送信できます。

! 重 要

ESET にフィッシングサイトを報告する前に、次の基準を 1 つでも満たしていることを確認してください。

- Web サイトがまったく検出されない
- Web サイトが誤ってウイルスとして検出される（この場合は、誤検出されたフィッシングサイトを報告してください。）

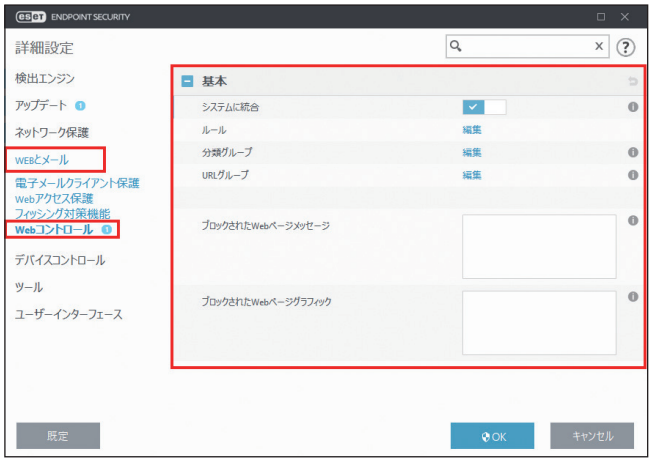
4.6.13 Web コントロール

Web コントロールでは、知的財産権に違反する Web サイトへのアクセスなど、法的責任を負うリスクから会社を保護する設定を行うことができます。Web コントロールを設定することで、作業生産性に悪影響を与える可能性のある不適切または有害な Web サイトやコンテンツに従業員がアクセスできないようにします。

Web コントロールでは、対象ユーザーまたはグループに対して、適切でない内容を掲載していると考えられる Web サイトへのアクセスをブロックします。さらに、企業やシステム管理者は、27 以上のカテゴリー（分類）と 140 以上のサブカテゴリーをあらかじめ定義して、該当するカテゴリーの Web サイトへのアクセスを禁止できます。

■基本

「詳細設定」画面で、［WEB とメール］>［Web コントロール］をクリックします。



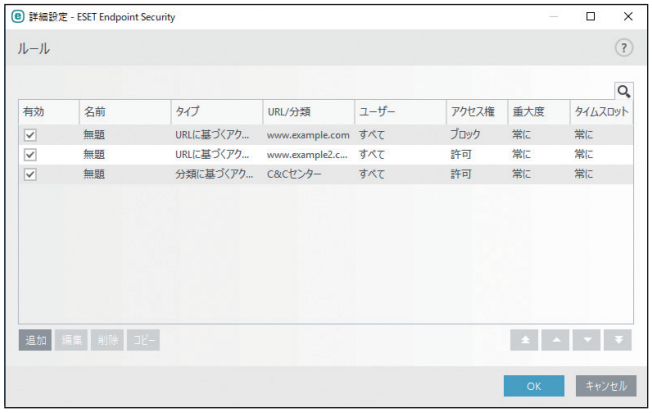
システムに統合	Web コントロールの有効／無効を設定します。
ルール	［編集］リンクをクリックすると、「ルール」画面が表示されます。詳細については、「●ルール」を参照してください。

分類グループ	［編集］リンクをクリックすると、「分類グループ」画面が表示されます。詳細については、「●分類グループ」を参照してください。
URL グループ	［編集］リンクをクリックすると、「URL グループ」画面が表示されます。詳細については、「● URL グループ」を参照してください。
ブロックされた Web ページメッセージ	Web サイトがブロックされたときに表示するメッセージをカスタマイズします。
ブロックされた Web ページグラフィック	メッセージとともに表示する画像の URL を設定します。画像は自動的に 90 × 30 ピクセルに調整されます。

●ルール

「詳細設定」画面の「ルール」の［編集］リンクをクリックすると、「ルール」画面が表示されます。「ルール」画面には、URL に基づくルールまたは分類に基づくルールが一覧で表示されます。

ルール一覧には、ルールの名前、タイプ、実行するアクション、ログ記録の重大度などが表示されます。また［有効］チェックボックスでは、ルールの有効／無効を切り替えることができます。ルールを削除せずに無効にしたい場合に便利です。

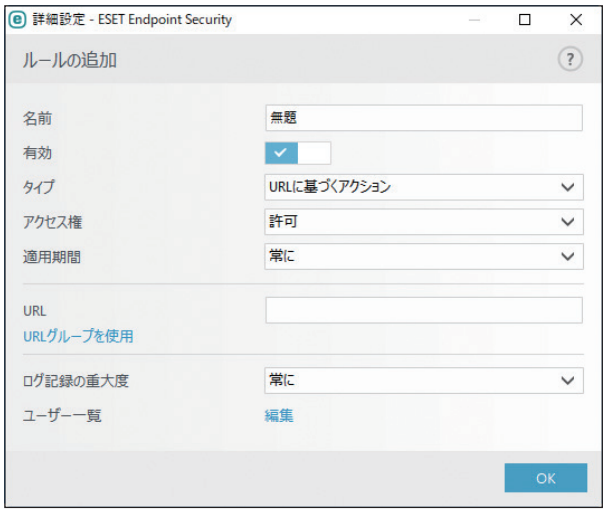


「ルール」画面では、次の操作ができます。

追加	新しいルールを追加します。
編集	ルールを編集します。
コピー	選択したルールで定義されている内容がコピーされた状態で、新しいルールを作成します。
削除	ルールを削除します。
／／／	ルールの優先度を変更します（ルールは最上位から最下位へと実行されます）。URL に基づくルールは、分類に基づくルールよりも常に優先度が高くなります。例えば、URL に基づくルールが分類に基づくルールの下にある場合でも、URL に基づくルールの方が優先度が高く、先に実行されます。

Web コントロールルールの追加

「ルールの編集」画面では、Web コントロールのフィルタリングルールを作成または変更できます。



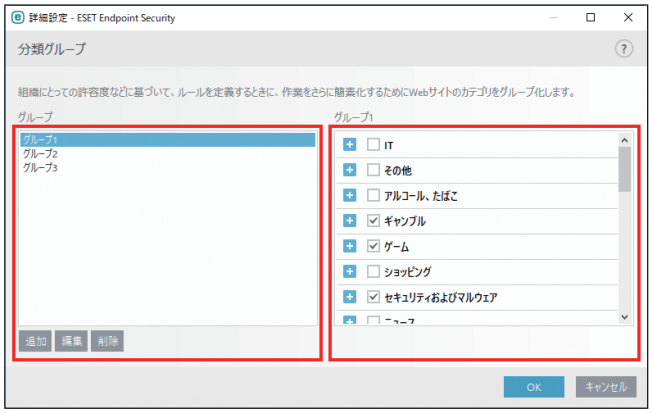
名前	識別しやすいように、ルールの説明を入力します。	
有効	ルールの有効／無効を設定できます。ルールを削除せずに無効にしたい場合に便利です。	
タイプ	URL に基づくアクション	特定の Web サイトへのアクセスを制御するルールの場合に選択します。「URL」フィールドに URL を入力します。
	分類に基づくアクション	特定のカテゴリで Web サイトへのアクセスを制御するルールの場合に選択します。［URL 分類］ドロップダウンメニューからカテゴリを選択します。
アクセス権	許可	URL または分類で指定した Web サイトへのアクセスを認可します。
	警告	URL または分類で指定した Web サイトへアクセスする際に、警告を表示します。
	ブロック	URL または分類で指定した Web サイトへのアクセスをブロックします。
適用期間	特定の期間に作成されたルールを適用できます。ドロップダウンメニューから、タイムスロットを選択します。タイムスロットの詳細については、「4.6.15　ツール」の「■タイムスロット」を参照してください。	
URL	「タイプ」で［URL に基づくアクション］を選択した場合に表示されます。URL または URL グループを指定します。［URL グループを使用］／［URL を使用］リンクをクリックすると、URL または URL グループの指定を切り替えることができます。指定した URL にアクセスする際に、「アクセス権」で選択したアクションが実行されます。	
URL 分類	「タイプ」で［分類に基づくアクション］を選択した場合に表示されます。分類または分類グループを指定します。［グループを使用］／［分類を使用］リンクをクリックすると、分類または分類グループの指定を切り替えることができます。指定した分類の Web サイトにアクセスする際に、「アクセス権」で選択したアクションが実行されます。	
ログ記録の重大度	常に	Web コントロールルールのすべてのアクション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	アップデート成功のメッセージを含むすべての情報メッセージとアクションをログに記録します。
	警告	重大なエラー、エラー、警告メッセージをログに記録します。
	なし	ログは記録しません。
ユーザー一覧	［編集］リンクをクリックすると「ユーザー一覧」画面が表示され、Web コントロールルールを適用するユーザーまたはユーザーグループを指定できます。ユーザーを指定しない場合は、Web コントロールルールはすべてのユーザーに適用されます。	

! 重 要

「URL」フィールドでは、特殊記号の「*」（アスタリスク）および「?」（疑問符）は使用できません。複数の上位レベルドメイン（TLD）がある Web サイトを含む URL グループを指定する場合は、各 TLD を個別に追加する必要があります。URL グループにドメインを追加すると、追加した TLD と TLD に所属するサブドメイン（sub.examplepage.com など）のすべてのコンテンツが、URL に基づくアクションに従ってブロックまたは許可されます。

●分類グループ

「詳細設定」画面の「分類グループ」の［編集］リンクをクリックすると、「分類グループ」画面が表示されます。「分類グループ」画面は、2 つのエリアで構成されています。左側のエリアには、分類グループが一覧で表示されます。分類グループを追加、編集、削除することもできます。右側のエリアには、カテゴリーおよびサブカテゴリーの一覧が表示されます。カテゴリーの ＋ をクリックすると、サブカテゴリーが表示されます。カテゴリーには、成人向けカテゴリーや一般的に不適切なカテゴリー、一般的に問題がないとみなされるカテゴリーが含まれます。



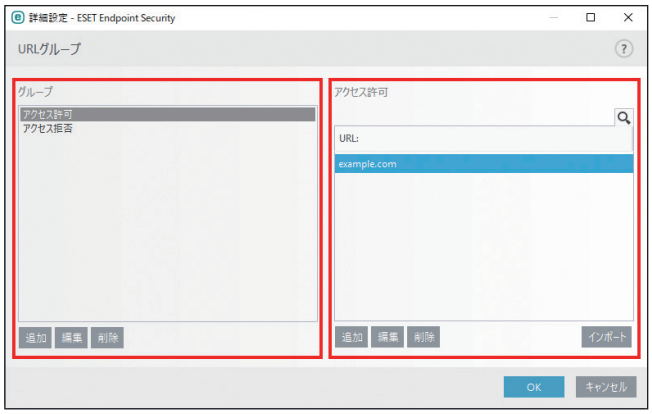
分類グループを編集するには、左側のエリアで対象のグループを選択し、右側のエリアでカテゴリーおよびサブカテゴリーの有効／無効を設定します。

カテゴリーの例

- その他
  通常は、イントラネット、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る Web サイトも、このカテゴリーに含まれます。
- 未解決
  Web 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 サイトです。
- 未分類
  まだ Web コントロールデータベースにない未知の Web サイトです。
- プロキシ
  通常は、Web コントロールフィルターによって禁止されている Web サイトに匿名でアクセスするための、アノニマイザー、リダイレクト、パブリックプロキシサーバーなどの Web サイトです。
- ファイル共有
  不快な内容や成人向けの写真、画像、電子書籍などのコンテンツが含まれている危険性がある Web サイトです。

● URL グループ

「詳細設定」画面の「URL グループ」の［編集］リンクをクリックすると、「URL グループ」画面が表示されます。「URL グループ」画面では、特定の Web サイトへのアクセスを制御するために、複数の URL を含むグループを作成できます。「URL グループ」画面は、2 つのエリアで構成されています。左側のエリアには、グループが一覧で表示されます。グループを追加、編集、削除することもできます。右側のエリアには、選択したグループに含まれる URL が一覧で表示されます。URL を追加、編集、削除、インポートすることもできます。



新しいグループを作成する手順は、次のとおりです。

操作手順

1. グループエリアの［追加］をクリックします。
2. グループの名前を入力し、［OK］をクリックします。
   グループが追加されます。
3. グループ一覧で作成したグループを選択します。
4. URL エリアの［追加］をクリックします。
   ［インポート］をクリックすると、URL が記述されたファイル（値は改行区切り、UTF-8 エンコーディングの *.txt など）から URL を取り込むことができます。
5. URL を入力し、［OK］をクリックします。
   グループに URL が追加されます。

! 重　要

特定の Web サイトを制御する方が、カテゴリーで Web サイトを制御するより、精度が高くなることがあります。分類グループやグループを作成する場合は注意してください。

4.6.14 デバイスコントロール

デバイスコントロール機能は、CD/DVD/USB メモリーなどのデバイスをコンピューターで使用するとき、読み込み／書き込みの許可、ブロック、警告表示など、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る機能です。使ってほしくないファイルが格納されているデバイスの使用を防止したいコンピューター管理者にとって便利な機能です。

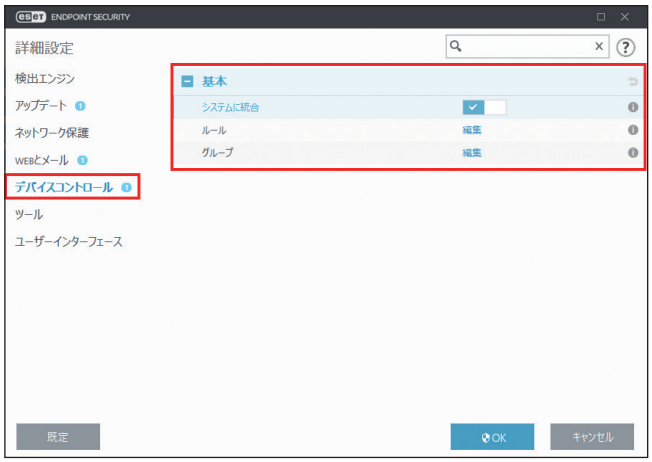
サポートするデバイス

デバイスコントロール機能でサポートするデバイスは次のとおりです。

- ディスクストレージ（HDD、USB リムーバブルディスク）
- CD/DVD
- USB プリンタ
- 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
- すべてのデバイスタイプ

■基本

「詳細設定」画面で、［デバイスコントロール］をクリックします。



システムに統合	デバイスコントロール機能の有効 / 無効を設定します。
ルール	［編集］をクリックすると「ルール」画面が表示されます。「●ルール」を参照してください。
グループ	［編集］をクリックすると「デバイスグループ」画面が表示されます。「●グループ」を参照してください。

●ルール

デバイスコントロールエディターは「ルール」の［編集］リンクをクリックすると表示できます。デバイスコントロールエディターには既存のルールが登録されています。デバイスコントロールエディターを使用すると、コンピューターで使用するデバイスを管理できます。

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、アクセスの許可またはブロックを定義できます。
ルール一覧には、外部デバイスの名前とタイプ、デバイスにアクセスしたときに実行するアクション、ログの重大度などが表示されます。「有効」チェックボックスのチェックを外すと、ルールは無効になります。

「ルール」画面では、次の操作ができます。

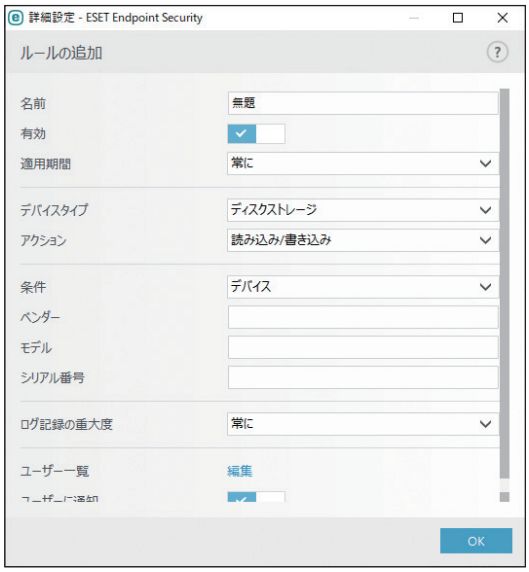
追加	新しいルールを追加します。
編集	ルールを編集します。
コピー	選択したルールで定義されている内容がコピーされた状態で、新しいルールを作成します。
削除	ルールを削除します。
入力	コンピューターに接続されているリムーバブルディスクのパラメーターを自動的に入力します。
／／／	ルールの優先度を変更します。

! 重　要

デバイスの機種やデバイス側の設定によって意図しないタイプで認識される場合があります。確実にデバイスのタイプを確認する場合は、デバイスの接続後に［入力］ボタンをクリックしてデバイスを表示させてください。

●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、コンピューターからデバイスにアクセスしようとしたときに実行するアクションを定義します。



名前	識別しやすいように、ルールの説明を入力します。
有効	ルールの有効／無効を設定できます。ルールを削除せずに無効にしたい場合に便利です。
適用期間	特定の期間に作成されたルールを適用できます。ドロップダウンメニューから、タイムスロットを選択します。タイムスロットの詳細については、「4.6.15　ツール」の「■タイムスロット」を参照してください。
デバイスタイプ	デバイスのタイプ（ディスクストレージ／CD/DVD／USB プリンタ／FireWire ストレージなど）をドロップダウンメニューから選択します。デバイスのタイプは、オペレーティングシステムから引き継がれます。デバイスのタイプは、デバイスがコンピューターに接続されていれば、デバイスマネージャーで確認できます。 ストレージデバイスには、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ー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 カードや認証カードなど、集積回路が埋め込まれているカードです。イメージングデバイスとは、スキャナーやカメラなどのデバイスです。 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、汎用的なデバイスを確実にブロックできます。
アクション	デバイスへのアクセスについて、次のいずれかのアクションを定義できます。 **ワンポイント** デバイスのタイプによっては、選択できないアクションがあります。ストレージデバイスタイプのデバイスの場合、4 つのアクションすべてを選択できます。ストレージデバイス以外のデバイスでは、3 つのアクションを選択できます。デバイスのタイプが 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 ポートポータブルデバイスの場合は、［読み込み専用］アクションは選択できません。
読み込み／書き込み	デバイスへの完全アクセスを許可します。
読み込み専用	デバイスからの読み込みアクセスだけを許可します。
ブロック	デバイスへのアクセスをブロックします。

アクション	警告	デバイスにアクセスするたびに、アクセスを許可するかブロックするかの通知画面を表示し、ログに記録します。デバイスは記憶されません。一度アクセスしたデバイスでも、アクセスするたびに通知画面が表示されます。
条件	［デバイスグループ］または［デバイス］を選択します。	
追加パラメーター	ルールを微調整したり、デバイスに合わせて変更したりするのに使用します。いずれのパラメーターも大文字と小文字は区別しません。 **!重　要** 追加パラメーターが定義されていない場合、ルール照合時は追加パラメーターを無視します。 また、追加パラメーターではワイルドカード（*、?）はサポートしていません。 **ワンポイント** Bluetooth デバイスの場合、OS の Bluetooth ドライバのみ指定可能です。接続する Bluetooth デバイスごとの制御はできません。	
	ベンダー	入力したベンダー名または ID によってフィルタリングを行います。
	モデル	デバイスの名前を入力します。
	シリアル番号	デバイス独自のシリアル番号を入力します。 CD/DVD の場合は、CD ドライブではなく、デバイス独自のシリアル番号があります。
ログ記録の重大度	常に	デバイスコントロールルールのすべてのアクション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	アップデート成功のメッセージを含むすべての情報メッセージと、アクション、診断の情報をログに記録します。
	警告	重大なエラー、エラー、警告メッセージをログに記録します。
	なし	ログは記録しません。
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します。ユーザーまたはユーザーグループを指定するには、［編集］リンクをクリックし、「ユーザー一覧」画面を表示します。ユーザーまたはユーザーグループを追加するには、［追加］をクリックして「ユーザーまたはグループの選択」画面を表示し、ユーザーまたはユーザーグループを選択します。 ユーザーまたはユーザーグループを削除するには、ユーザー一覧からユーザーまたはユーザーグループを選択し、［削除］をクリックします。	
ユーザーに通知	デバイスへのアクセスをブロックした場合などのイベントが発生したときに、ユーザーに通知を行うかどうかの設定を行います。	

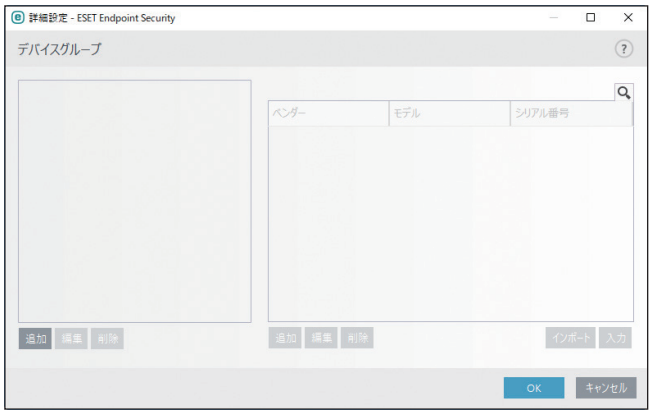
!重　要

［デバイスのタイプ］で次のデバイスを選択した場合、ユーザールールでフィルタリングすることはできません。実行されるアクションに関する項目についてのみフィルタリングできます。

- イメージングデバイス
- モデム
- LPT/COM ポート

●グループ

「グループ」の［編集］をクリックして、デバイスグループを追加、編集します。

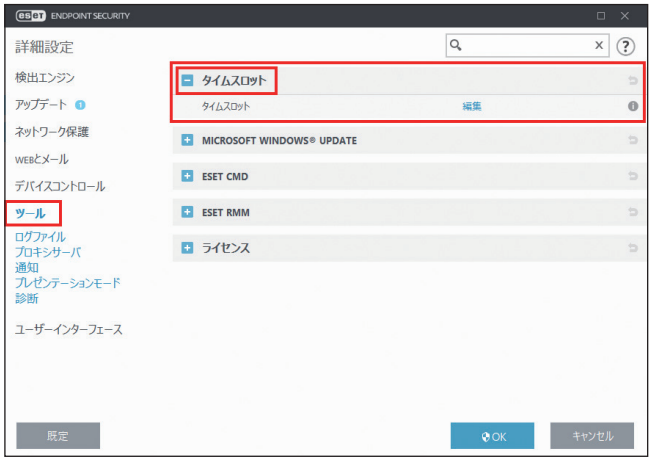


左側ペイン	追加	新しいデバイスグループを追加します。
	編集	デバイスグループ名を編集します。
	削除	デバイスグループを削除します。
右側ペイン	追加	デバイスグループにデバイスを追加します。ベンダー、モデル、シリアルを登録します。
	編集	登録されているデバイスの内容を編集します。
	削除	登録されているデバイスを削除します。
	インポート	テキストファイルからデバイスのリストをインポートします。
	入力	現在接続されているすべてのデバイスのデバイスタイプ、ベンダー名、モデル名、シリアルが表示されます。

4.6.15 ツール

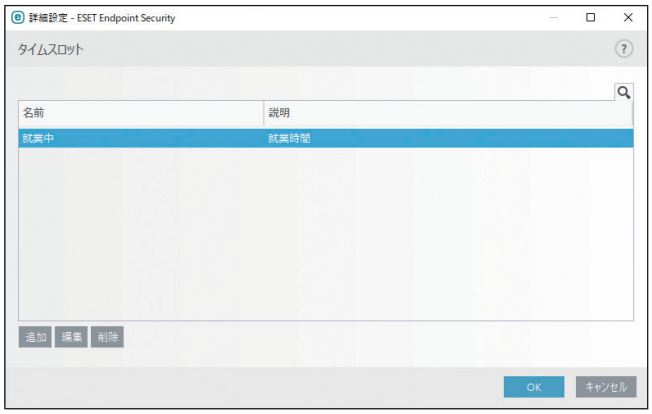
■タイムスロット

タイムスロットでは、就業時間や週末などの時間の範囲を定義できます。タイムスロットで定義した時間の範囲は、デバイスコントロールや Web コントロールのルールに割り当てられます。たとえば、就業時間の定義を作成し、その定義をデバイスコントロールや Web コントロールのルールで割り当てると、就業時間内のみ有効なルールを適用できます。タイムスロットを設定するには、［詳細設定］画面で［ツール］>［タイムスロット］をクリックします。



●タイムスロットの編集

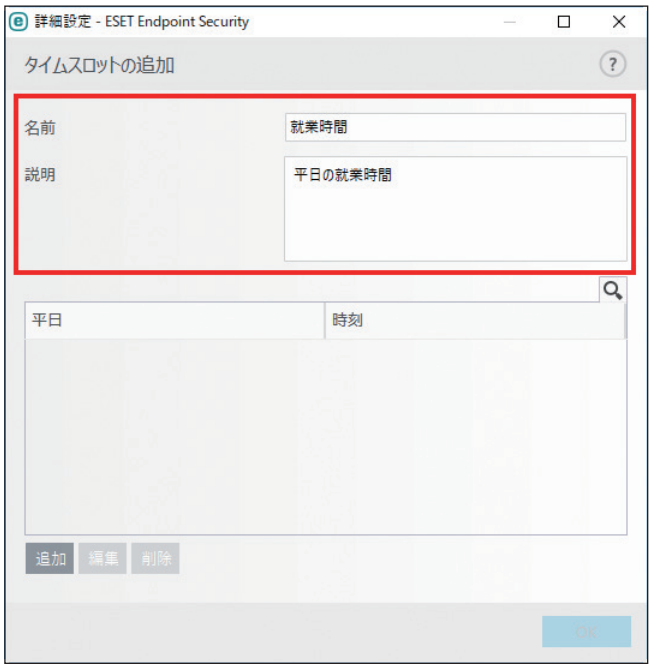
タイムスロットの追加や編集、削除を行うときは、［詳細設定］画面で［ツール］>［タイムスロット］>「タイムスロット」の［編集］をクリックします。



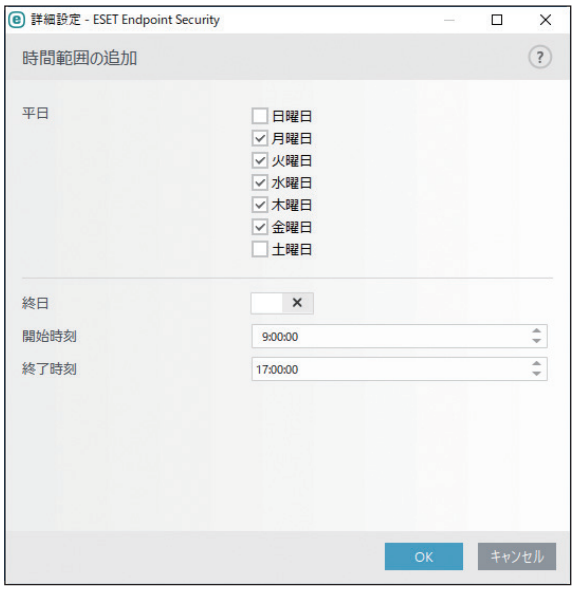
追加	新しいタイムスロットを追加します。
編集	作成済みのタイムスロットを編集します。
削除	選択したタイムスロットを削除します。

●タイムスロットの追加

「タイムスロット」画面で、［追加］をクリックするか、一覧からタイムスロットを選択して［編集］をクリックすると、「タイムスロットの追加」画面が表示されます。



タイムスロットの名前や説明を入力し、［追加］をクリックすると、「時間範囲の追加」画面が表示されます。



「時間範囲の追加」画面で、曜日や開始時刻、終了時刻などの設定を行って、［OK］をクリックすると、「タイムスロットの追加」画面に曜日と時間範囲が追加されます。

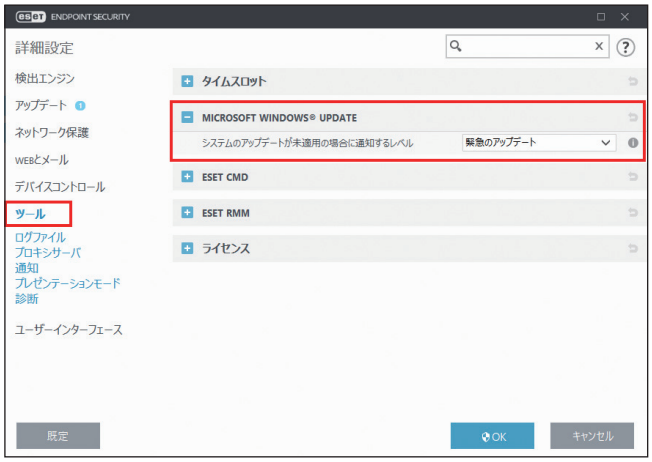
ワンポイント

「タイムスロットの追加」」画面に追加する、曜日と時間範囲は、複数追加できます。たとえば、月曜日は 9:00 ～ 18:00、火曜日は 10:00 ～ 19:00 というように曜日ごとに時間範囲を登録することもできます。

■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コンピュータ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すぐにインストールすることが不可欠です。ESET Endpoint Security は、設定したレベルに従って、実行していないシステムアップデートがある場合に通知します。

「詳細設定」画面で、［ツール］>［MICROSOFT WINDOWS UPDATE］をクリックします。



［Microsoft Windows システム更新を通知する］ドロップダウンメニューから通知レベルを選択します。選択できる通知レベルは次のとおりです。

通知しない	システムアップデートは通知されません。
オプションのアップデート	優先度が低レベル以上に設定されているシステムアップデートが通知されます。

推奨アップデート	優先度が普通レベル以上に設定されているシステムアップデートが通知されます。
重要なアップデート	優先度が重要レベル以上に設定されているシステムアップデートが通知されます。
緊急のアップデート	緊急のシステムアップデートのみが通知されます。

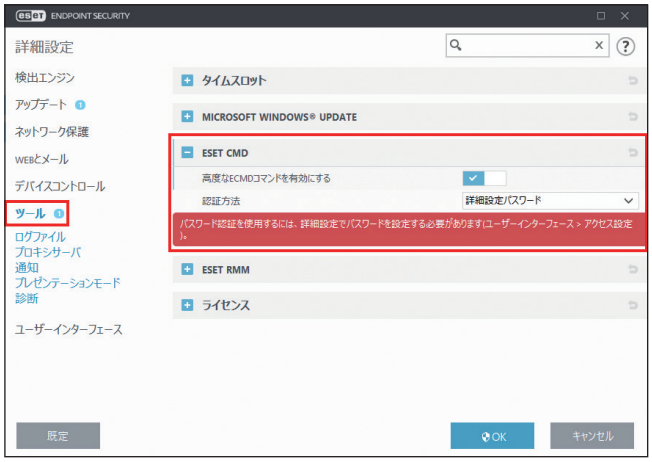
! 重　要

システムアップデートの通知後、アップデートサーバーでステータスの検証を行った後、「システムのアップデート」画面が表示されます。そのため、通知レベルの設定後はすぐにシステムのアップデートができない場合があります。

■ ESET CMD

ESET CMD は高度な ECMD コマンドを有効にすることで、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るようにする機能です。ESET CMD を有効にすると、2 つの認証方法を使用できます。

「詳細設定」画面で、［ツール］＞［ESET CMD］をクリックします。



高度な ECMD コマンドを有効にする	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する機能を有効にするかどうかを設定します。	
認証方法	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	パスワード保護を使用します。インポートする設定ファイルについて［ユーザーインターフェース］＞［アクセス設定］で設定したパスワードと一致するか確認します。インポートする XML ファイルをツールを用いて署名する必要があります。

! 重　要

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コマンドプロンプトを開く必要があります。また、コマンド実行時には、インポート先 / エクスポート先のフォルダーが存在する必要があります。

ワンポイント

ECMD コマンドはローカルコンピューター上でのみ実行できます。ESET Security Management Center のクライアントタスクの［コマンドの実行］タスクを利用した場合は動作しません。

ESET CMD の使用例

コンフィグファイル名を settings.xml、フォルダー名を c:¥config とした場合

- 設定のエクスポートコマンド：

```
ecmd /getcfg c:¥config¥settings.xml
```

- 設定のインポートコマンド：

```
ecmd /setcfg c:¥config¥settings.xml
```

XML 設定ファイルの署名方法

操作手順

1. ユーザーズサイトから XmlSignTool をダウンロードします。
2. 管理者として実行を使用してコマンドプロンプトを開きます。
3. XmlSignTool.exe を置いたフォルダーに移動します。
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 2 <xml ファイルパス >

   ! 重 要

   /version パラメーターの値は、ESET Endpoint Security のバージョンによって異なります。V7 では、パラメーターに「/version 2」を指定してください。「/version 1」のパラメーターは、V6 の場合に指定します。

5. XmlSignTool からパスワード入力を要求されたら、［ユーザーインターフェース］>［アクセス設定］で設定したパスワードと同じパスワードを入力します。

   ! 重 要

   アクセス設定パスワードの変更を行った後に、古いパスワードで署名された設定ファイルをインポートしたい場合は、変更後の新しいパスワードで .xml 設定ファイルを再度度署名する必要があります。

■ ESET RMM

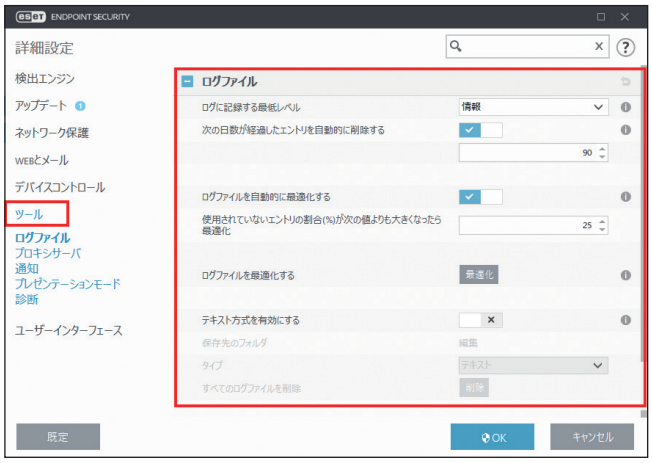
ESET RMM は、日本ではサポート対象外の機能です。

■ライセンス

ライセンスでは、ESET Endpoint Security が ESET ライセンスサーバーに接続する間隔の設定を行えます。ESET ライセンスサーバーへの接続間隔の変更は、「間隔チェック」で行います。既定では、「自動」に設定されており、1 時間に数回接続を行っています。ネットワークトラフィックが増大した場合には、「間隔チェック」の設定を［制限］に変更すると、負荷が低減されます。制限が選択されると、ESET Endpoint Security は 1 日に 1 回またはコンピューターが再起動するときにのみライセンスサーバーを確認します。

4.6.16 ログファイル

ログを設定するには、「詳細設定」画面で、［ツール］>［ログファイル］をクリックします。

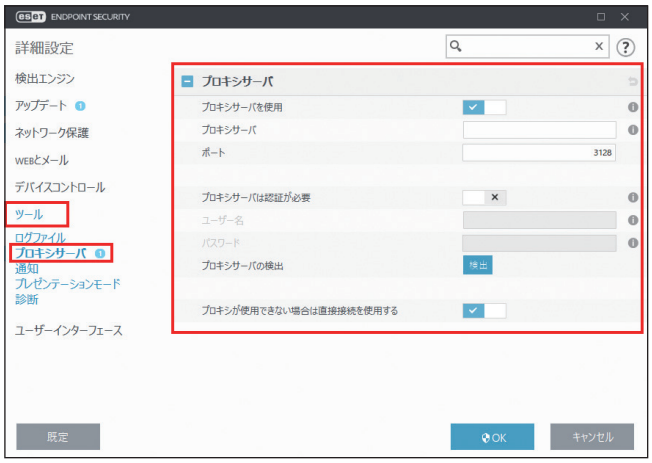


ログに記録する最低レベル	ドロップダウンメニューから、ログを記録する最低レベルを設定します。	
	診断	プログラムおよびすべてのイベントを微調整するのに必要な情報を記録します。
	情報	アップデートの成功メッセージを含むすべての情報メッセージおよび「診断」に含まれるすべての情報を記録します。
	警告	重大なエラー、エラー、警告メッセージを記録します。
	エラー	ファイルのダウンロード中に発生したエラーなど、エラーや重大なエラーを記録します。
	重大	ウイルス対策保護の開始エラー、ファイアウォールエラーなど、緊急の対策が必要なエラーを記録します。
次の日数が経過したエントリを自動的に削除する	有効にすると、指定した日数より古いログファイルが自動的に削除されます。既定値は「90」日、制限値は「1」～「100」日です。	
ログファイルを自動的に最適化する	有効にすると、「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」で指定した値を超えると、ログファイルが自動的に最適化されます。既定値は「25」%、制限値は「1」～「100」% です。	
ログファイルを最適化する	［最適化］をクリックすると、空のログファイルがすべて削除され、ログの処理パフォーマンスおよび記録速度が向上します。ログに多数の情報が含まれている場合に有効です。	
テキスト方式を有効にする	有効にすると、ログファイルをテキスト形式で記録できます。 「対象ディレクトリ」の［編集］をクリックすると、テキスト形式ログの保存先を指定できます。 ［タイプ］ドロップダウンメニューから、ログのファイル形式を選択できます。 ［すべてのログファイルを削除］をクリックすると、テキスト形式のログファイルがすべて削除されます。	

4.6.17 プロキシサーバー

大規模な LAN ネットワークでは、コンピューターがプロキシサーバーを介してインターネットに接続している場合があります。ESET Endpoint Security をこのような環境で運用するには、プロキシサーバーを定義する必要があります。

「詳細設定」画面で、［ツール］>［プロキシサーバ］をクリックします。



プロキシサーバを使用	プロキシサーバーの使用を有効にします。
プロキシサーバ	プロキシサーバーのアドレスを設定します。
ポート	プロキシサーバーが使うポートを設定します。既定値は「3128」です。
プロキシサーバは認証が必要	プロキシサーバーで認証が必要な場合は有効にして、ユーザー名、パスワードを設定します。
プロキシサーバの検出	［検出］をクリックすると、自動的にプロキシサーバーが検出されて設定が取り込まれます。 ※認証データ（ユーザー名とパスワード）は検出で取り込まれないため、手動で入力してください。
プロキシが使用できない場合は直接接続を使用する	プロキシサーバーが利用できない場合に、プロキシサーバーをバイパスしてインターネットに接続します。

4.6.18 通知

ESET Endpoint Security は、発生したイベントを様々な方法でユーザーに通知できます。通知の設定を行うには、「詳細設定」画面で、［ツール］>［通知］をクリックします。ここでは、以下のタイプの通知に関しての設定が行えます。

アプリケーション通知	各アプリケーション通知について、デスクトップに表示するか、メールで送信するかを設定できます。
デスクトップ通知	デスクトップ通知は、デスクトップのタスクバーの横にポップアップウィンドウとして表示されます。
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情報を送信します。
通知のカスタマイズ	デスクトップ通知などにカスタム通知を追加します。

■基本

「基本」セクションでは、次の項目を調整できます。

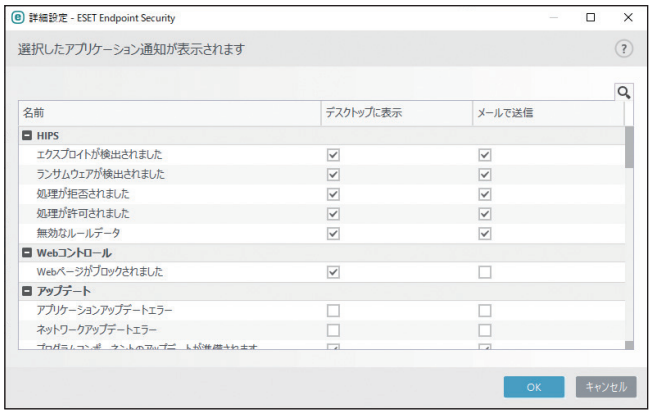
アプリケーション通知	［編集］リンクをクリックすると、「選択したアプリケーション通知が表示されます」画面が表示され、特定のアプリケーション通知を有効または無効に設定できます。画面は、3 つの列に分割して表示されます。通知名は最初の列にカテゴリ別で並べ替えられます。アプリケーションイベントを通知する方法は、対応する列の「デスクトップに表示」または「メールで送信」のチェックボックスをオン／オフで設定します。
セキュリティレポート通知を表示する	有効にすると、新しいバージョンのセキュリティレポートが生成されたときに通知を表示します。
デスクトップに通知を表示する	無効にすると、システムタスクバーの横のポップアップ通知を非表示にします。このオプションは有効にし、新しいイベントが発生したときに製品が通知を発行できるようにすることをお勧めします。
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	有効にすると、すべての非インタラクティブ通知を抑制します。

●アプリケーション通知

アプリケーション通知の表示を調整するには、「詳細設定」画面で［通知］>［基本］をクリックし、「アプリケーション通知」の［編集］をクリックします。通知のリストは 3 つの列に分割して表示されます。通知名は最初の列にカテゴリ別で並べ替えられます。アプリケーションイベントを通知するときは、対応する列の「デスクトップに表示」または「メールで送信」のチェックボックスをオンにします。

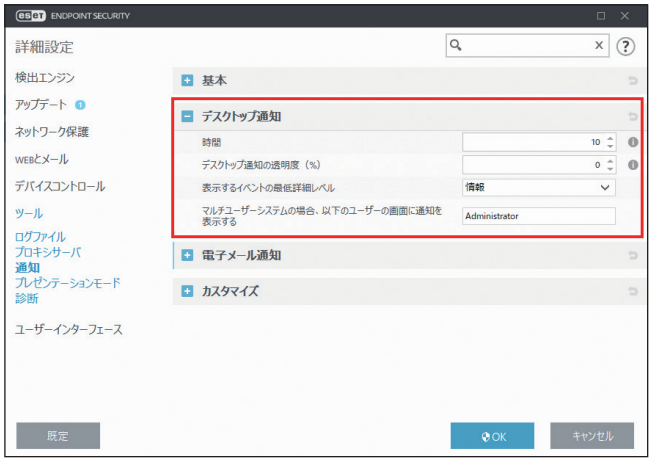
また、メッセージが表示される時間や表示するイベントの詳細レベルなどのデスクトップ通知の一般設定は、「デスクトップ通知」セクションで行います。詳細については、「■デスクトップ通知」を参照してください。

電子メールで通知を行うときのメッセージ形式の設定や SMTP サーバーの設定は、「電子メール」セクションで行います。詳細については、「■電子メール通知」を参照してください。



■デスクトップ通知

デスクトップ通知は、タスクバーの横に小さいポップアップウィンドウで表示されます。既定では、10 秒間表示され、ゆっくりと消えるように設定されています。既定では、ESET Endpoint Security が製品のアップデートの成功したり、新しく接続されたデバイスを検出したり、ウイルス検査タスクが完了したり、脅威を検出したりしたときに、ユーザーに通知する主な手段として利用されています。「デスクトップ通知」セクションでは、ポップアップ通知の動作をカスタマイズできます。

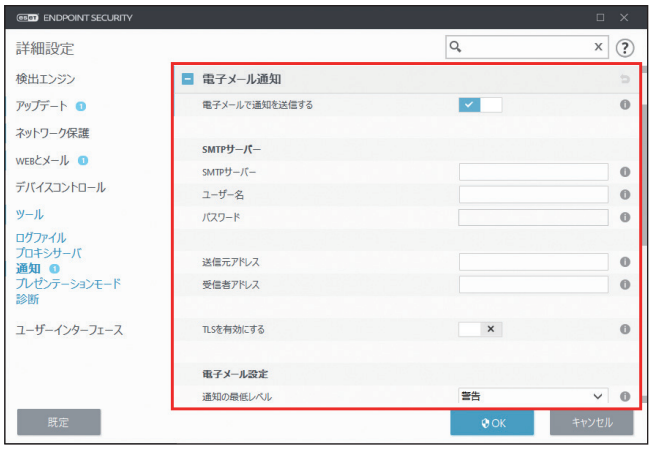


時間	通知メッセージが表示される時間を設定します。値は 3 ～ 30 秒でなければなりません。
デスクトップ通知の透明度（%）	通知メッセージの透明度を割合で設定します。サポートされている範囲は 0 (透明ではない) から 80 (非常に高い透明度) です。

表示するイベントの最低詳細レベル	ドロップダウンメニューから、表示する通知の最低重要度を選択できます。	
	診断	プログラムおよびすべてのレコードを微調整するのに必要な情報を通知します。
	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すべてのレコードを通知します。
	警告	重大なエラーと警告メッセージ (例 :「アンチステルスが正しく実行されていないか、アップデートが失敗しました」) を通知します。
	エラー	エラー (例 :「ドキュメント保護が起動していません」) や重大なエラーを通知します。
	重大	重大なエラー (ウイルス対策保護の開始エラーや感染したシステム) のみを通知します。
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	マルチユーザー環境でコンピューターを利用している場合に通知を表示するユーザーを設定します。フィールドには、システム通知やその他の通知を受け取るユーザーを指定します。通常は、システム管理者またはネットワーク管理者を指定します。すべてのシステム通知が管理者に通知される場合、ターミナルサーバーを使用している場合に便利です。	

■電子メール通知

「電子メール通知」セクションでは、電子メール通知を利用する場合の各種設定を行います。電子メール通知を利用するには、「電子メールで通知を送信する」を有効にする必要があります。



● SMTP サーバー

SMTP サーバーに関する設定を行います。

SMTP サーバ	通知を送信するために使用する SMTP サーバーを入力します。
ユーザー名／パスワード	SMTP サーバーで認証を要求する場合、有効なユーザー名とパスワードを入力します。
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元アドレスを入力します。
受信者アドレス	通知メールのヘッダーに表示される受信者アドレスを入力します。
TLS を有効にする	有効にすると、警告と通知メッセージが TLS 暗号化で保護されます。

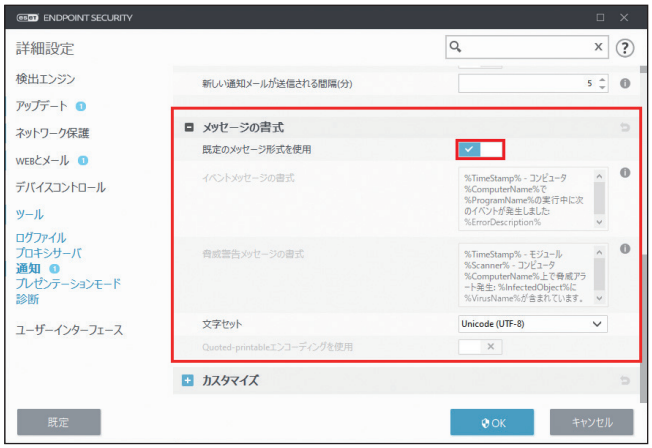
●電子メール設定

送信する電子メールの間隔や通知のレベルなどについて設定を行います。

通知の最低レベル	ドロップダウンメニューから、通知を送信する最低レベルを選択します。	
	診断	プログラムおよびすべてのイベントを微調整するのに必要な情報を通知します。
	情報	すべての情報メッセージと「診断」に含まれるすべての情報を通知します。
	警告	重大なエラーと警告メッセージ（例：「アンチステルスが正しく実行されていないか、アップデートが失敗しました」）を通知します。
	エラー	エラー（例：「ドキュメント保護が起動していません」）や重大なエラーを通知します。
	重大	重大なエラー（ウイルス対策保護の開始エラーやシステムの感染など）のみを通知します。
各通知を別のメールで送信	有効にすると、個別の通知ごとに電子メールを送信します。受信者は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）	新しい通知を送信する間隔を分単位で指定します。「0」に設定すると、通知がすぐに送信されます。既定値は「5」分、制限値は「0」～「9999」分です。	

●メッセージの書式

脅威警告などのイベントが発生したときのメッセージの書式や文字セットの設定を行います。



イベントメッセージの書式	リモートコンピューターで表示されるイベントメッセージの形式を編集します。
脅威警告メッセージの書式	脅威警告メッセージには定義済みの既定の形式があります。書式は変更しないことをお勧めします。ただし、自動メール処理システムを使用している場合など、状況によっては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	送信するメッセージの文字セットを選択します。文字セットは、「ローカル」「Unicode（UTF-8）」「Ascii（7bit）」「Japanese（ISO-2022-JP）」から選択できます。また、「ローカル」を選択した場合は、「Quoted-printable エンコーディングを使用」の設定を行えます。この設定を有効にすると、電子メールメッセージのソースが Quoted-printable（QP）書式でエンコードされます。

メッセージでは、指定されている実際の情報でキーワード（% 記号で区切られた文字列）が置き換えられます。使用可能なキーワードは次のとおりです。

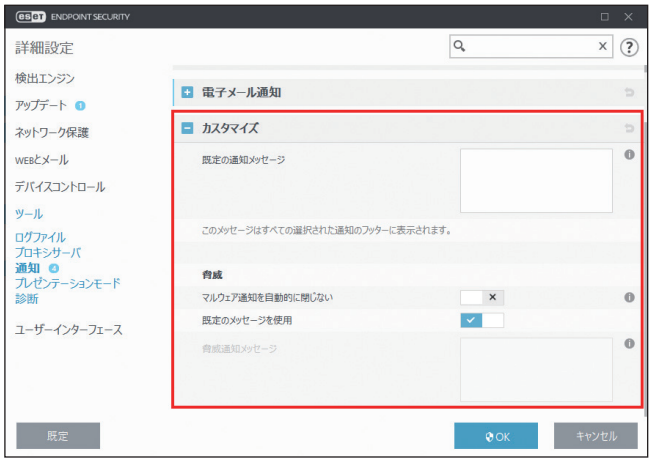
%TimeStamp%	イベントの日時
%Scanner%	関連するモジュール
%ComputerName%	警告が発生したコンピュータの名前
%ProgramName%	警告を生成したプログラム
%InfectedObject%	感染しているファイルやメールなどの名前
%VirusName%	ウイルスの ID
%Action%	侵入に対する処理
%ErrorDescription%	ウイルス以外のイベントの説明

ワンポイント

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ます。
また、「%ErrorDescription%」は、イベントメッセージのみで使用されます。

■カスタマイズ

「カスタマイズ」セクションでは、通知で使用されるメッセージをカスタマイズできます。



既定の通知メッセージ	通知のフッターに表示される既定のメッセージを編集します。
マルウェア通知を自動的に閉じない	有効にすると、手動で閉じるまでマルウェア通知が画面に表示されます。
既定のメッセージを使用	無効にすると、脅威がブロックされたときにカスタム通知メッセージが通知されます。通知するカスタム通知メッセージは、「脅威通知メッセージ」フィールドに入力します。

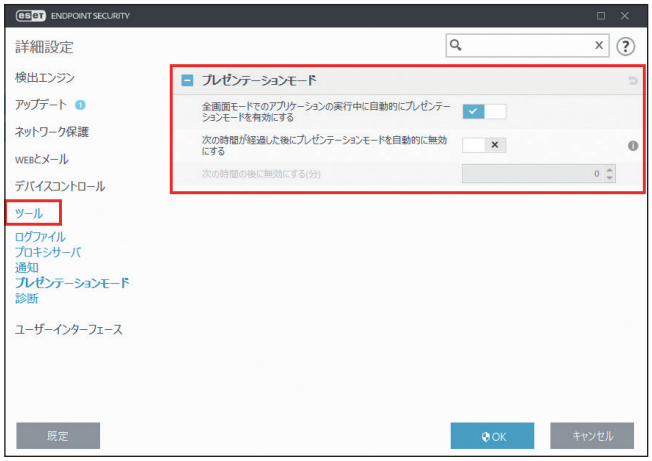
4.6.19 プレゼンテーションモード

プレゼンテーションモードは、ソフトウェアを中断せずに使用したい、ポップアップウインドウを表示させたくない、CPU の使用量を最小化したい、ウイルス検査でプレゼンテーションを中断したくない、などの要望に応えるための機能です。プレゼンテーションモードを有効にすると、すべてのポップアップウィンドウが無効になり、ESET Endpoint Security のスケジューラーが停止します。また、システムの保護はバックグラウンドで実行され、ユーザーの操作は必要ありません。

プレゼンテーションモードの詳細を設定するには、「詳細設定」画面で、［ツール］>［プレゼンテーションモード］をクリックします。

! 重 要

ファイアウォールが「対話モード」の場合にプレゼンテーションモードを有効にすると、インターネットへの接続時に問題が発生することがあります（インターネットに接続するゲームを行うときなど）。通常、問題が発生したときにはアクションの確認画面が表示されますが（通信のルールや例外が定義されている場合を除く）、プレゼンテーションモードではユーザーの操作は無効になっているため、アクションを選択することができません。この問題を解決するには、問題が発生する可能性のあるアプリケーションごとに通信ルールを定義するか、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てください。
また、プレゼンテーションモードが有効なときに、セキュリティ上のリスクが存在する Web サイトまたはアプリケーションにアクセスした場合、ユーザーとの対話処理が無効なため、ブロックの説明や警告が表示されませんので注意してください。



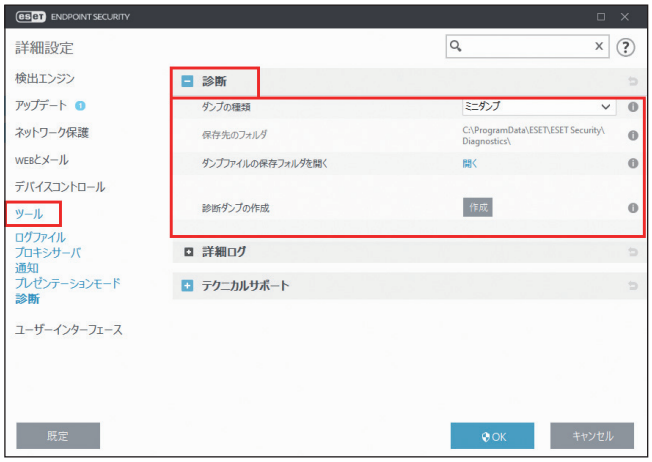
全画面モードでのアプリケーションの実行中に自動的にプレゼンテーションモードを有効にする	アプリケーションを全画面モードで起動したときに、プレゼンテーションモードが自動的に開始されます。アプリケーションを終了すると、プレゼンテーションモードは自動的に停止します。ゲームやプレゼンテーションなど、全画面で使用するアプリケーションを使用する場合に便利です。
次の時間が経過した後にプレゼンテーションモードを自動的に無効にする	プレゼンテーションモードが自動的に停止する時間を分単位で設定できます。制限値は「0」～「2000」分です。

4.6.20 診断

診断を設定するには「詳細設定」画面で［ツール］＞［診断］をクリックします。

■診断

診断では、ESET のプロセス（.ekm など）のアプリケーションクラッシュダンプに関する設定をします。ダンプファイルは、アプリケーションがクラッシュしたときに生成されます。開発者はダンプファイルを使用して、さまざまな問題をデバッグまたは修正できます。



ダンプの種類	メモリダンプを生成しない	ダンプファイルを生成しません。
	ミニダンプ	アプリケーションがクラッシュした原因を特定するための最低限の情報を記録したダンプファイルを生成します。保存領域が限られているときに便利です。ただし、記録される情報が限られるため、クラッシュ時に実行されていたスレッドが直接の原因ではない場合、ダンプファイルを解析しても原因を特定できない場合があります。
	完全	アプリケーションのクラッシュ時、システムメモリーのすべての内容を記録したダンプファイルを生成します。ダンプファイルには、生成したときに実行されていたプロセスデータが含まれます。
保存先のフォルダ	ダンプファイルが作成されるディレクトリーが表示されます。	
ダンプファイルの保存フォルダを開く	［開く］リンクをクリックすると、「対象ディレクトリ」に表示されているフォルダーが Explorer で表示されます。	
診断ダンプの作成	［作成］をクリックすると、診断ダンプの作成を行います。	

ワンポイント

ログファイルは「C:¥ProgramData¥ESET¥ESET Security¥Diagnostics¥」に保存されています。

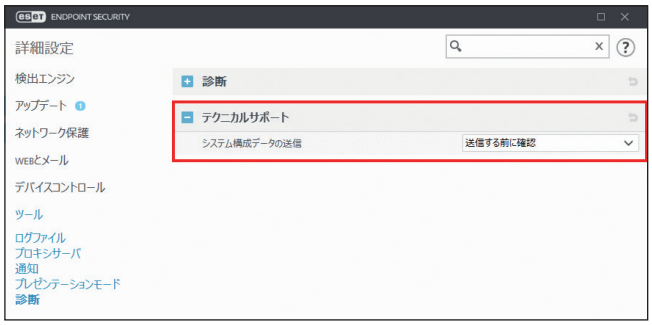
●詳細ログ

様々なイベントの詳細ログを保存するかどうかの設定を行います。

Web コントロール詳細ロギングを有効にする	有効に設定すると、Web 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。
アップデートエンジン詳細ロギングを有効にする	有効に設定すると、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。
オペレーティングシステム詳細ログを有効にする	有効に設定すると、実行中のプロセス、CPU アクティビティ、ディスク処理などのオペレーティングシステムに関する追加情報が収集されます。
カーネル詳細ログを有効にする	有効に設定すると、ESET カーネルで発生するすべてのイベントを記録します。
スキャナー詳細ログを有効にする	有効に設定すると、スキャナーで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	有効に設定すると、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。
ネットワーク保護詳細ロギングを有効にする	有効に設定すると、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。
プロトコルフィルタリング詳細ロギングを有効にする	有効に設定すると、PCAP 形式でプロトコルフィルタリング経由のすべてのプロトコルフィルタリングデータ転送を記録します。
メモリ追跡を有効にする	有効に設定すると、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。
ライセンス詳細ロギングを有効にする	有効に設定すると、ライセンスサーバーとのすべての通信を記録します。
迷惑メール対策エンジン詳細ロギングを有効にする	有効に設定すると、迷惑メール対策検査中に処理中に発生するすべてのイベントを記録します。

■テクニカルサポート

システム構成データを ESET に送信する前に確認するかどうかを設定できます。



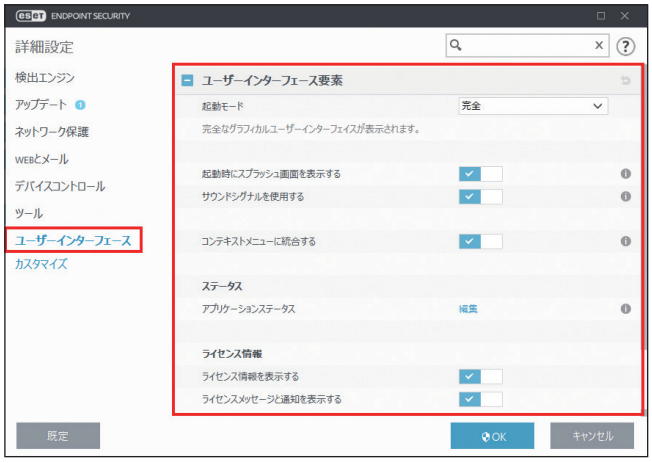
システム構成データの送信	「送信する前に確認」または「常に送信」から選択します。

4.6.21 ユーザーインターフェース

「ユーザーインターフェース」では、ESET Endpoint Security のグラフィカルユーザーインターフェース（GUI）を作業環境に合わせて設定できます。
ユーザーインターフェースを設定するには、「詳細設定」画面で、［ユーザーインターフェース］をクリックします。

4.6.21.1 ユーザーインターフェース要素

「ユーザーインターフェース要素」セクションでは、ESET Endpoint Security のグラフィカルユーザーインターフェース（GUI）を調整できます。



起動モード	ドロップダウンメニューから GUI の起動モードを選択します。	
	完全	すべての GUI を表示します。
	最低	GUI は使用できますが、通知のみが表示されます。
	手動	通知および警告は表示されません。
	サイレント	GUI、通知、警告は表示されません。GUI は管理者だけが起動できます。システムリソースを節約したいときに有効です。
起動時にスプラッシュ画面を表示する	無効にすると、ESET Endpoint Security の起動時にスプラッシュ画面が表示されなくなります。	

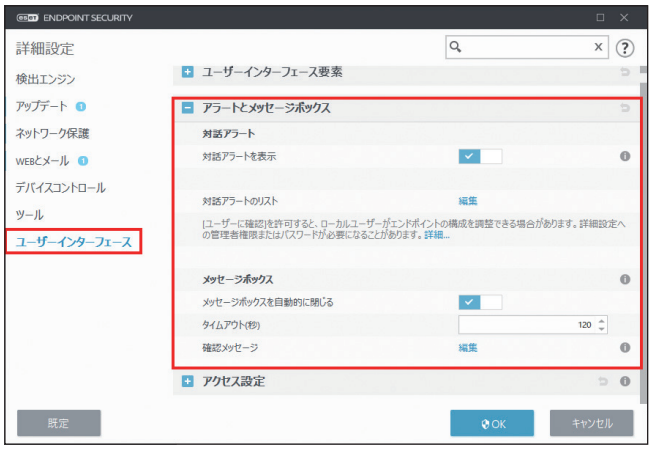
サウンドシグナルを使用する	有効にすると、脅威の発見や検査終了など、重要なイベントが発生したときに警告音を鳴らします。
コンテキストメニューに統合する	有効にすると、クライアントコンピューター上のオブジェクトを右クリックしたとき、コンテキストメニューに ESET Endpoint Security のコントロールメニューが表示されます。
アプリケーションステータス	「アプリケーションステータス」の［編集］をクリックすると、「現在の状況」画面に表示されるステータスの有効／無効を設定できます。
ライセンス情報を表示する	無効にすると、［保護ステータス］および［ヘルプとサポート］画面のライセンス情報が非表示になります。
ライセンスメッセージと通知を表示する	無効にすると、ライセンスが期限切れの場合にのみ、通知とメッセージが表示されます。

！重　要

「起動モード」を［最低］にしてクライアントコンピューターを再起動すると、ESET Endpoint Security の通知は表示されますが、GUI は表示されません。「起動モード」を［完全］に戻すには、管理者権限で［スタート］>［すべてのプログラム］>［ESET］>［ESET Endpoint Security］>［ESET Endpoint Security］をクリックするか、ポリシーを使用して ESET Security Management Center 経由で実行します。

4.6.21.2　アラートとメッセージボックス

「アラートとメッセージボックス」セクションでは、ユーザーによる決定が必要な場合のインタラクティブなアラートウィンドウに関する設定が行なえます。



■対話アラート

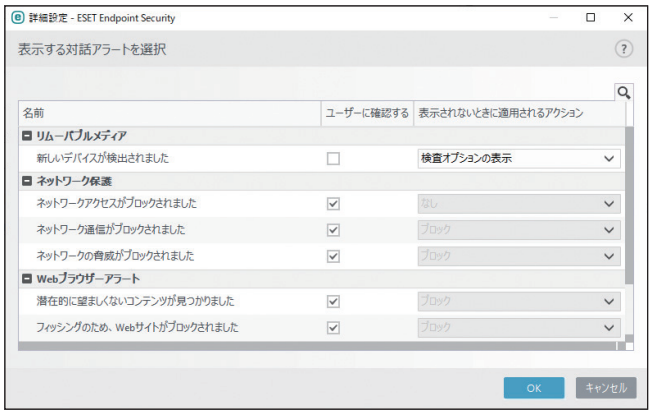
検出があった場合またはユーザーの介入が必要な場合には、インタラクティブなアラートウィンドウが表示されます。

●対話アラートを表示

「対話アラートを表示」を無効にすると、すべてのアラートウィンドウとブラウザー内のダイアログが非表示になり、定義済みの既定のアクションが自動的に選択されます。たとえば、「フィッシング Web サイトの可能性」などのアラートはブロックされます。管理されていないユーザーの場合、このオプションは既定の有効のまま使用することを勧めします。また、管理されたユーザーの場合、この設定を有効にし、対話アラートのリストでユーザーの定義済みアクションを選択します。

●対話アラートのリスト

設定可能な対話アラートの動作の調整は、「対話アラートのリスト」の［編集］をクリックし、「表示する対話アラートを選択」画面で対話アラートの調整を行います。「ユーザーに確認する」のチェックボックスを「オン」にすると、対応したイベントが発生したときに対話アラートが表示されます。チェックボックスを「オフ」に設定すると、対話アラートが表示されないときに適用するアクションを選択できます。以下の対話アラートについて設定できます。



●リムーバブルメディア

新しいデバイスが検出されました

コンピューターで新しいデバイス（CD、DVD、USB メモリーなど）を接続したときに表示する対話アラートの設定を行います。「ユーザーに確認する」のチェックボックスを「オン」にすると、イベントが発生したときに対話アラートが表示されます。チェックボックスを「オフ」に設定すると、適用するアクションを以下の 3 種類の中から選択できます。

検査オプションの表示	コンピューターにリムーバブルメディアを接続すると、アクションの選択画面が表示されます。
検査しない	コンピューターに接続したリムーバブルメディアを検査しません。
自動デバイス検査	コンピューターに接続したリムーバブルメディアを自動的に検査します。

表示されないときに適用される「アクション」で［検査オプションの表示］を選択した場合、コンピューターに新しいデバイスが接続されると、次の画面が表示され、アクションを選択できます。

すぐに検査	デバイスの検査を開始します。
検査しない	デバイスの検査が延期されます。
セットアップ	「詳細設定」画面を表示します。
選択したオプションを常に使用する	チェックすると、以降コンピューターにデバイスを接続したときに、同じアクションが実行されます。

ワンポイント

ESET Endpoint Security には、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もあります。詳細については、「4.6.14　デバイスコントロール」を参照してください。

●ネットワーク保護

ネットワークアクセスがブロックされました

ESET Security Management Center からのこのワークステーションのコンピューターをネットワークから隔離するクライアントタスクがトリガーされたときに表示されます。「ユーザーに確認する」のチェックボックスを「オフ」にした場合、表示されないときに適用されるアクションには、「なし」のみが選択できます。

ネットワーク通信がブロックされました

ネットワークの攻撃が検知され、ネットワーク通信がブロックされたときに表示されます。「ユーザーに確認する」のチェックボックスを「オフ」にした場合、表示されないときに適用されるアクションには、「ブロック」のみが選択できます。

ネットワークの脅威がブロックされました

コンピュータのアプリケーションがネットワーク上の別のコンピュータ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別のユーザーがネットワーク上のポートを検査しようとしている場合など、ネットワークの脅威を検出しブロックしたときに表示されます。「ユーザーに確認する」のチェックボックスを「オフ」にした場合、表示されないときに適用されるアクションには、「ブロック」のみが選択できます。

● Web ブラウザーアラート

潜在的に望ましくないコンテンツが見つかりました

Web サイトで望ましくない可能性があるコンテンツを検出し、ブロックしたときに表示されます。「ユーザーに確認する」のチェックボックスを「オフ」にした場合、表示されないときに適用されるアクションに「ブロック」または「許可」を選択できます。

フィッシングのため、Web サイトがブロックされました

接続先 Web サイトがフィッシングサイトとして検出され、ブロックしたときに表示されます。「ユーザーに確認する」のチェックボックスを「オフ」にした場合、表示されないときに適用されるアクションに「ブロック」または「許可」を選択できます。

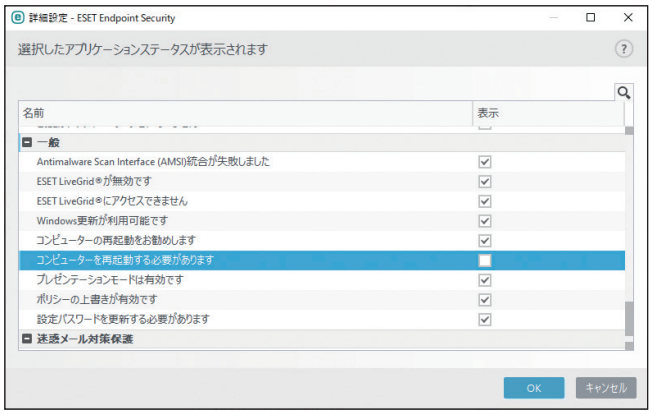
●コンピュータ

これらのアラートが発生していると、ユーザーインターフェースの色が変わります。

コンピューターを再起動する（必須）

コンピューターを再起動する必要があるときに赤色のアラートで表示されます。「ユーザーに確認する」のチェックボックスを「オフ」にした場合、表示されないときに適用されるアクションには「なし」のみが選択できます。「なし」を選択すると、このアラートの表示を無効に設定できます。

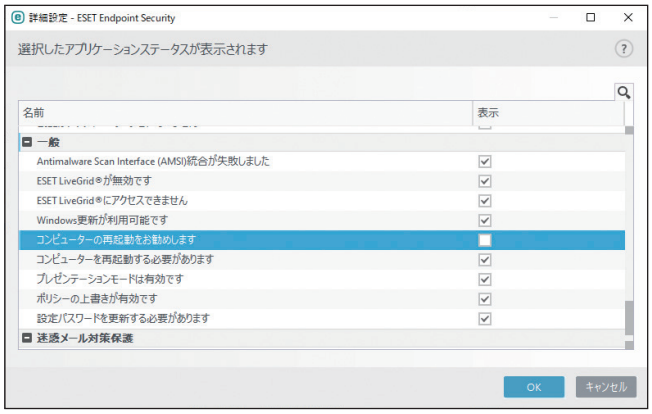
また、ESET Endpoint Security のメインプログラムウィンドウでアプリケーションステータスを無効にしたいときは、「選択したアプリケーションステータスが表示されます」画面で設定します。「選択したアプリケーションステータスが表示されます」画面は、「詳細設定」画面を表示し、［ユーザーインターフェース］>［ユーザーインターフェース要素］とクリックし、「アプリケーションステータス」の［編集］をクリックし、［コンピューターを再起動する必要があります］のチェックボックスをオフにします。



コンピューターを再起動する（推奨）

コンピューターの再起動が推奨されるときに黄色のアラートで表示されます。「ユーザーに確認する」のチェックボックスを「オフ」にした場合、表示されないときに適用されるアクションには「なし」のみが選択できます。「なし」を選択すると、このアラートの表示を無効に設定できます。

また、ESET Endpoint Security のメインプログラムウィンドウでアプリケーションステータスを無効にしたいときは、「選択したアプリケーションステータスが表示されます」画面で設定します。「選択したアプリケーションステータスが表示されます」画面は、「詳細設定」画面を表示し、［ユーザーインターフェース］>［ユーザーインターフェース要素］とクリックし、「アプリケーションステータス」の［編集］をクリックし、［コンピューターの再起動をお勧めします］のチェックボックスをオフにします。



！重　要

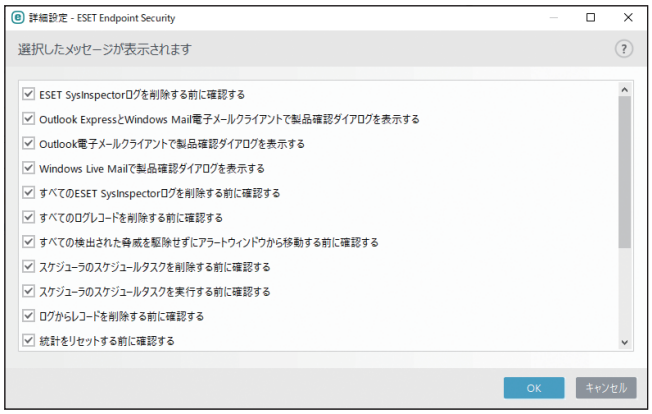
対話アラートには、検出エンジン、HIPS、ファイアウォールの対話ウィンドウは含まれません。これらの動作は、特定の機能で個別に設定することができます。

■メッセージボックス

メッセージボックスは、短いテキストメッセージや質問を表示する場合に使用されます。特定の時間が経過した後で自動的にメッセージボックスを閉じるには、[自動的にメッセージボックスを閉じる] を有効に設定します。また、「タイムアウト（秒）」でメッセージボックスを閉じるまでの時間を設定できます。

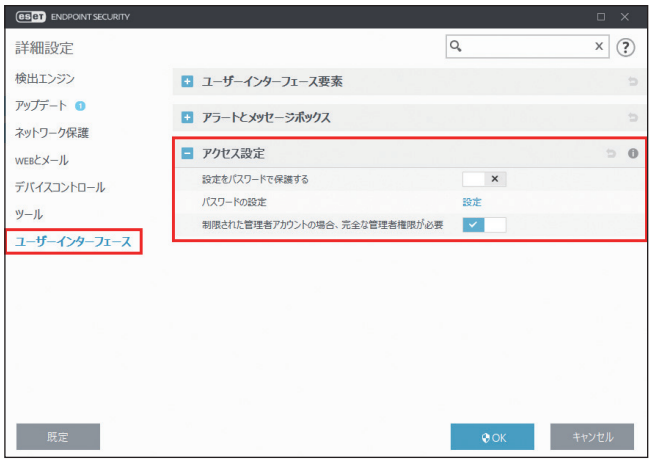
- **確認メッセージ**

［編集］をクリックすると、アクションが実行される前に、ESET Endpoint Security で表示される確認メッセージのリストが表示されます。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設定できます。



4.6.21.3 アクセス設定

システムのセキュリティを最大限に確保するには、ESET Endpoint Security を正しく設定することが重要です。資格のないユーザーによって ESET Endpoint Security の設定が変更されると、セキュリティレベルが低下し重要なデータが失われることがあります。「アクセス設定」セクションでは、認証されていないユーザーによる変更を防ぐために、ESET Endpoint Security の設定パラメーターをパスワードで保護することができます。



設定をパスワードで保護する	ESET Endpoint Security の設定パラメーターをパスワードで保護します。 をクリックすると、「パスワードの設定」画面が表示されるので、新しいパスワードと確認用のパスワードを入力し、［OK］をクリックします。保護を解除する場合は、 をクリックし、設定されているパスワードを入力して［OK］をクリックします。
パスワードの設定	［設定］リンクをクリックすると、パスワードを変更できます。
制限された管理者アカウントの場合、完全な管理者権限が必要	有効にすると、ESET Endpoint Security で管理者認証資格情報を入力するように求められます。

Chapter 5 上級者向けガイド

5.1 プロファイル

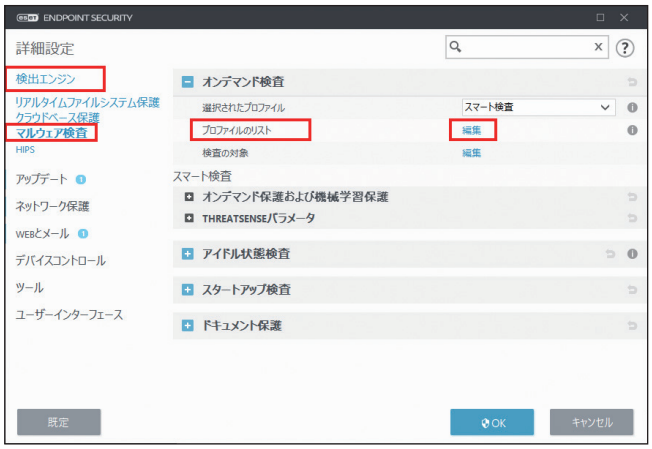
コンピューターの検査とアップデートでは、プロファイルを使って同じ設定の作業を簡略化することができます。

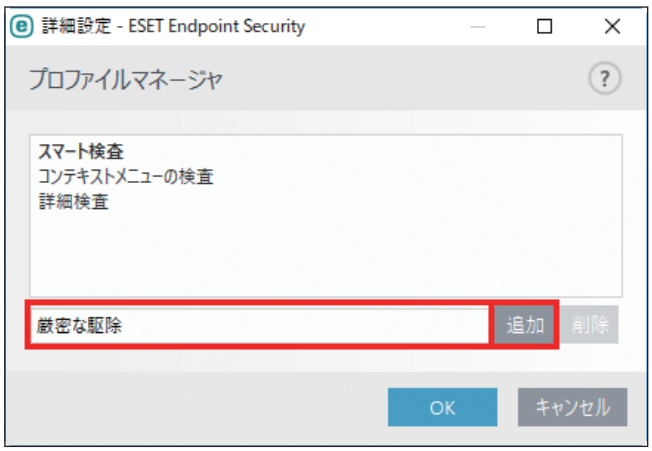
5.1.1 コンピューターの検査

検査パラメーターをプロファイルとして保存しておくと、次回以降の検査を同じパラメーターで実行することができます。検査対象や検査方法などのパラメーターを、定期的に行う検査ごとにプロファイルとして保存することをお勧めします。

■プロファイルの作成

新しいプロファイルを作成するには、メインメニューの［設定］>［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］をクリックして、「プロファイルのリスト」の［編集］をクリックします。プロファイル名を入力して［追加］をクリックすると、新しいプロファイルが作成されます。既定のプロファイルとして、［スマート検査］、［コンテキストメニューの検査］、［詳細検査］が登録されています。





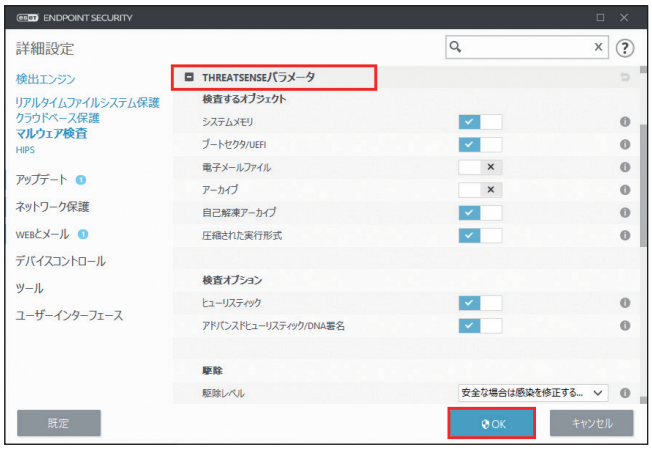
ワンポイント

プロファイルを削除するには、一覧でプロファイルを選択し、［削除］をクリックします。ただし、既定のプロファイルは削除できません。

■パラメーターの設定

「選択されたプロファイル」のドロップダウンメニューでプロファイルを選択して、「THREATSENSE パラメータ」セクションでパラメーターを設定します。

例えば、事前登録されている「スマート検査」は限定された目的で設定されています。このパラメーターを、ニーズに合わせて変更できます。パラメーターを設定したら［OK］をクリックしてプロファイルを保存します。



ワンポイント

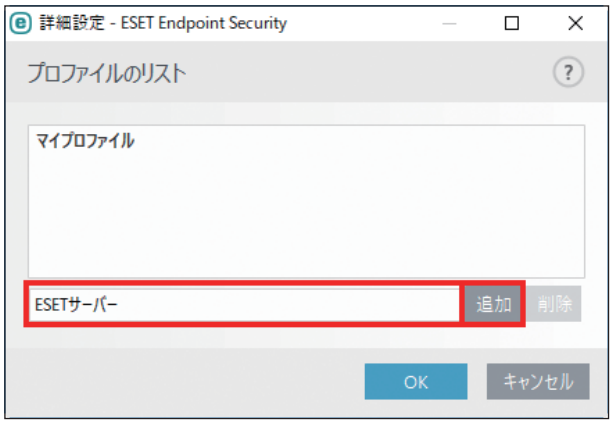
「THREATSENSE パラメータ」セクションの各パラメーターの横にある ⓘ にカーソルを合わせると、各パラメーターの説明が表示されます。

5.1.2 アップデート

アップデートの設定をプロファイルとして保存して、次回のアップデートに使用したり、他のコンピューターで使用することができます。カスタムアップデートプロファイル（「マイプロファイル」以外のプロファイル）は、アップデートサーバーへの接続方法が複数ある場合に作成します。コンピューター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作成してください。

■プロファイルの作成

新しいプロファイルを作成するには、メインメニューの［設定］>［詳細設定］>［アップデート］>［プロファイル］をクリックして、「プロファイルのリスト」の［編集］をクリックします。新しいプロファイル名を入力して［追加］をクリックすると、新しいプロファイルが作成されます。既定のプロファイルとして、［マイプロファイル］が登録されています。

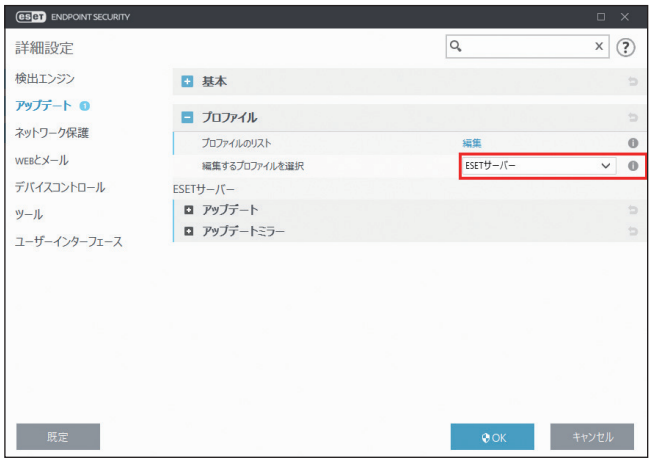


ワンポイント

プロファイルを削除するには、一覧でプロファイルを選択し、［削除］をクリックします。ただし、「マイプロファイル」は削除できません。

■パラメーターの設定

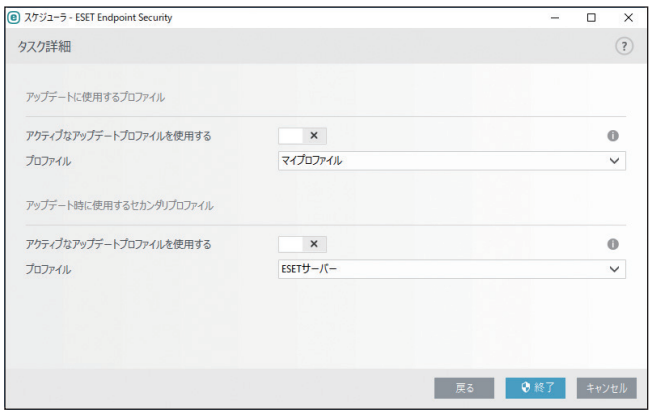
「プロファイル」セクションの「編集するプロファイルを選択」のドロップダウンメニューから新しく作成したプロファイルを選択すると、「アップデート」セクションでアップデートパラメーターを設定できます。



■プロファイルの設定例

例えば、通常はローカルネットワーク内のアップデートミラーに接続してアップデートを実行しているが、出張などでアップデートミラーに接続できないときは ESET のアップデートサーバーから直接ファイルをダウンロードするという運用方法があります。この場合、1 つ目のプロファイルではローカルサーバーに接続し、2 つ目のプロファイルでは ESET のアップデートサーバーに接続するというパラメーターを設定します。

2 つのプロファイルを作成したら、メインメニューの［ツール］>［スケジューラ］でアップデートタスクを作成して、1 つ目のプロファイルをデフォルトプロファイル、2 つ目のプロファイルをセカンダリプロファイルに指定します。



5.2 コマンドライン

ESET Endpoint Security の保護機能は、コマンドライン（ecls コマンド）から手動で起動したり、バッチファイル（bat）を使用して起動したりできます。「ecls.exe」は、既定では「C:\Program Files\ESET\ESET Endpoint Security」に格納されています。

ESET コマンドライン検査は、次の書式で指定します。
ecls [OPTIONS..]FILES..

5.2.1 ESET コマンドラインで使用できるパラメーターおよびスイッチ

■オプション

/base-dir=FOLDER	FOLDER からモジュールをロードします。
/quar-dir=FOLDER	FOLDER を隔離します。
/exclude=MASK	MASK と一致するファイルを検査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	検査対象に含めるサブフォルダー階層の下限レベルを指定します。
/symlink	シンボリックリンクを追跡します（既定）。
/no-symlink	シンボリックリンクをスキップします。
/ads ADS	ADS を検査します（既定）。
/no-ads ADS	ADS を検査しません。
/log-file=FILE	ログを FILE に出力します。
/log-rewrite	ログ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ログに記録します。
/no-log-all	感染していないファイルはログに記録しません（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。

■検査オプション

/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検査します（既定 0 ＝制限なし）。
/max-arch-level=LEVEL	検査対象とするアーカイブのネストレベルを指定します。
/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検査します（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検査します（既定 0 ＝制限なし）。
/mail	電子メールファイルを検査します（既定）。
/no-mail	電子メールファイルを検査しません。
/mailbox	受信ボックスを検査します（既定）。
/no-mailbox	受信ボックスを検査しません。
/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します（既定）。
/no-suspicious	不審なアプリケーションを検査しません。
/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=EXTENSIONS	コロンで区切られた EXTENSIONS のみを検査します。	
/ext-exclude=EXTENSIONS	コロンで区切られた EXTENSIONS 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次のとおりです。	
	none（既定）	自動駆除を実行しません。
	standard	感染したファイルを自動的に駆除または削除します。
	strict	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、駆除を試行せずにファイルを削除します。
	delete	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	ヘルプを表示／終了します。
/version	バージョン情報を表示／終了します。
/preserve-time	最終アクセスのタイムスタンプを保持します。

■終了コード

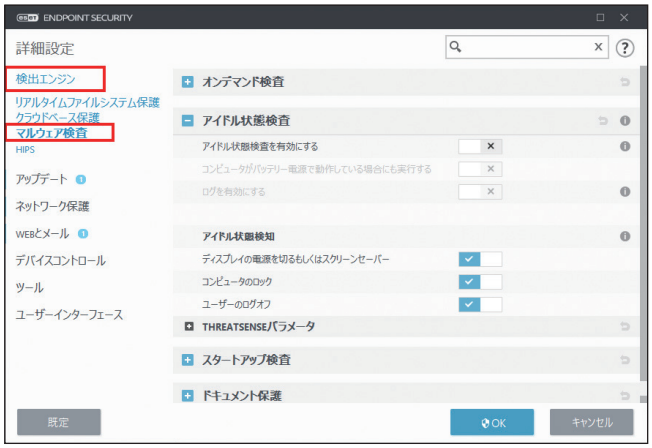
0	マルウェアは検出されませんでした。
1	マルウェアが検出され、駆除されました。
10	一部のファイルは検査できません（マルウェアの可能性あり）。
50	マルウェアが検出されました。
100	エラー

！重　要

「100」を超える終了コードは、ファイルが検査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。

5.3 アイドル状態でのコンピューター検査

コンピューターがアイドル状態のときに、コンピューターを検査するかどうかを設定できます。
アイドル状態検知を設定するには、メインメニューの［設定］>［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］をクリックします。



コンピューターが次の状態のときに、検査を実行するかどうかを設定します。

- 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
- コンピューターのロック
- ユーザーのログオフ

5.4 ESET SysInspector

ESET SysInspector は、コンピューターを詳細にチェックして、ドライバー、アプリケーション、ネットワーク接続、レジストリーなどの情報を収集します。これらの情報を使って、ソフトウェア、ハードウェアの互換性の問題やセキュリティ上問題のあるシステム動作など、広範囲に危険性レベルを評価することができます。

5.4.1 ESET SysInspector の実行

SysInspector によるコンピューターの分析は、次の流れで操作します。

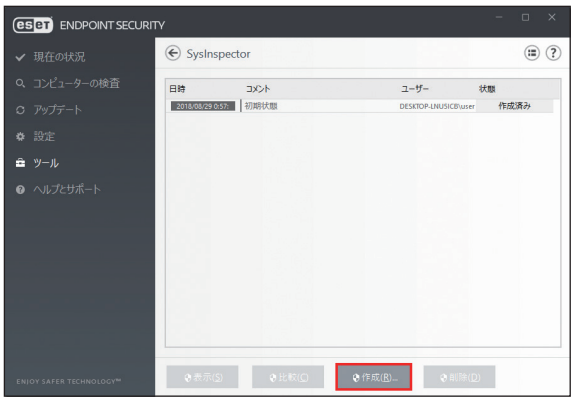
STEP1	ESET Endpoint Security の「詳細設定」で「ESET SysInspector] を起動します。
STEP2	ESET SysInspector で、その時点のコンピューターの状態のスナップショットを作成します。
STEP3	スナップショットを開くと SysInspector アプリケーションが起動して分析結果が表示されます。この画面でコンピューターの状態を確認します。

ESET SysInspector によるコンピューターの検査は、10 秒から数分かかります。

次の手順で ESET SysInspector を実行します。

操作手順

1. ［ツール］＞［ESET SysInspector］を選択して、「SysInspector」画面で［作成］をクリックします。

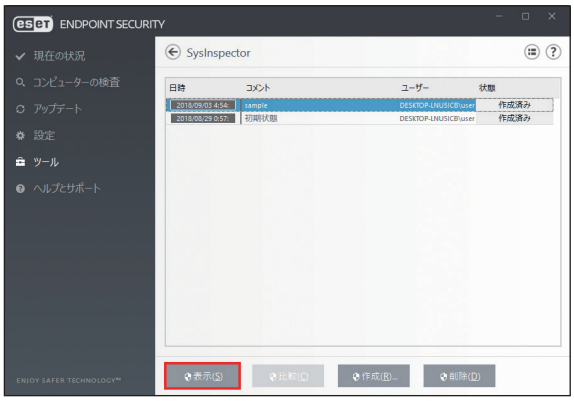


2. 作成するスナップショットについてのコメントを入力して［作成］をクリックします。

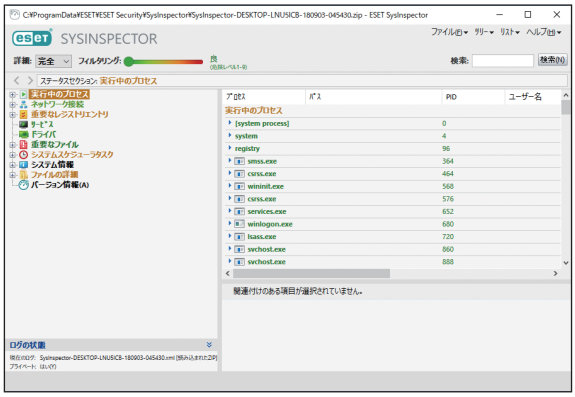
※ファイル名は実行時の日時から自動的に付けられます。

3. 作成したスナップショットを選択して［表示］をクリックします。

続く

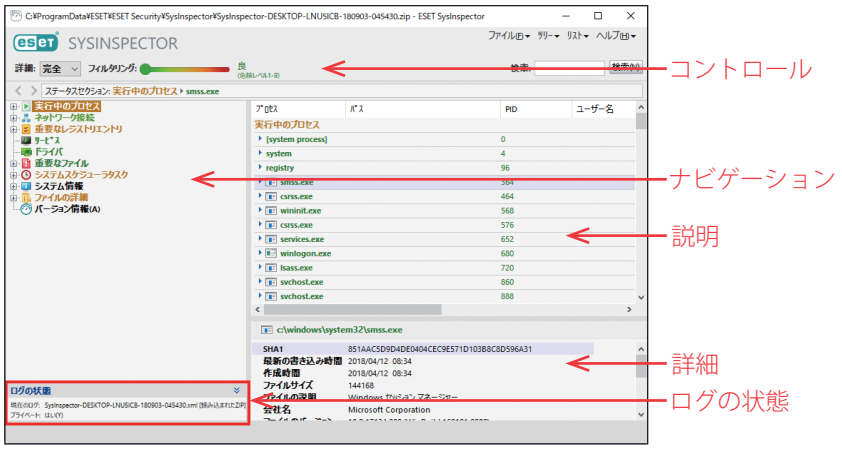


4 SysInspector が起動して、スナップショットを使ってコンピューターの状態を詳細に分析します。



5.4.2 SysInspector 画面の使い方

ESET SysInspector のメイン画面は、大きく 4 つのエリアに分かれています。
コントロールエリアはメイン画面の上部、ナビゲーションエリアは左側、説明エリアは右側、詳細エリアは下部に配置されています。「ログの状態」エリアには、使用されているフィルター、フィルタータイプ、ログは比較の結果かどうかなど、ログの基本パラメーターが表示されます。



■SysInspector の操作

ESET SysInspector には、次の機能があります。

ファイル	現在のシステムステータスを保存したり、以前に保存されたログを開いたりできます。ログを公開する場合は、［送信用］でログを生成することをお勧めします。このログでは、機密情報（ユーザー名、コンピューター名、ドメイン名、現在のユーザー特権、環境変数など）は含まれません。 **ワンポイント** 以前に保存したログは、メイン画面にドラッグアンドドロップするだけで開くことができます。
ツリー	すべてのノードをツリー上で展開したり閉じたりできます。また、選択したセクションをサービススクリプトにエクスポートすることもできます。
リスト	プログラム内でのナビゲーションをより容易にするための機能のほか、オンラインでの情報検索などの他の様々な機能が含まれます。
ヘルプ	ESET SysInspector とその機能に関する情報を確認できます。
詳細	メイン画面に表示される情報を基本、中、完全から選択できます。 「基本」モードは、システムの一般的な問題に対する解決策を探すための情報が表示されます。 「中」モードは、一般的ではない詳細な情報が表示されます。 「完全」モードでは、特殊な問題の解決に必要なすべての情報が表示されます。
フィルタリング	システム内の疑わしいファイルまたはレジストリーエントリーを見つけるために、危険度に応じて情報を絞り込むことができます。スライダーを動かすと、危険レベルごとに項目をフィルターできます。スライダーを左端（危険レベル 1）に設定すると、すべての項目が表示されます。スライダーを右に動かすと、表示されているレベルより不審な項目のみが表示されます。スライダーを右端（危険レベル 9）まで移動すると、既知の有害な項目のみが表示されます。危険レベル 6 ～ 9 の項目は、すべてセキュリティリスクが生じる可能性があります。 **ワンポイント** 項目の危険レベルは、項目の色と危険レベルのスライダーの色を比較すると簡単に判別できます。
検索	特定のアイテムを名前または名前の一部によって検索します。検索結果は、説明ウインドウに表示されます。

⬅/➡	左矢印または右矢印をクリックすることで、説明ウインドウ内に表示される情報を切り替えることができます。【BackSpace】キーと【スペース】キーを押しても戻ることができます。
ステータスセクション	ナビゲーションウインドウ内の現在のノードを表示します。 **!重　要** 赤色で表示されている項目は、SysInspector によって潜在的な危険性があると判定された不明な項目です。ただし、赤色で表示されていても削除してよい項目というわけではありません。削除する前に、ファイルが本当に危険かどうか、不要かどうかを確認してください。

■ナビゲーションエリアの使い方

ESET SysInspector では、情報がノードと呼ばれる複数の基本セクションに分けてナビゲーションエリアに表示されます。サブノードがある場合は、サブノードを展開して追加情報を確認できます。ノードの展開／折りたたみは、ノード名をダブルクリックするか、ノード名の横にある ⊞ または ⊟ をクリックします。ナビゲーションエリアで項目を選択すると、説明エリアに情報が表示されます。説明エリアで項目を選択すると、詳細エリアに詳細情報が表示されます。

●ナビゲーションエリアのメインノード

次に、ナビゲーションウインドウのメインノードと、説明ウインドウおよび詳細ウインドウの関連情報について説明します。

実行中のプロセス	スナップショット作成時実行されていたアプリケーションとプロセスに関する情報が含まれます。説明ウインドウには、プロセスによって使用されたダイナミックライブラリとシステム内のそれらのライブラリの場所、アプリケーションベンダーの名前、ファイルの危険レベルなど、各プロセスに関する追加の詳細情報が表示されます。 詳細ウインドウには、ファイルサイズやハッシュなど詳細な情報が表示されます。 **ワンポイント** オペレーティングシステムは、複数の重要なカーネルコンポーネントで構成されます。これらのコンポーネントは、常時稼動し、他のユーザーアプリケーションに対して重要な機能を提供します。カーネルコンポーネントのプロセスのファイルパスが「\??\」で始まる場合があります。「\??\」は起動前にプロセスを最適化するもので、システムにとっては安全です。
ネットワーク接続	説明ウインドウには、ナビゲーションウインドウで選択したプロトコル（TCP または UDP）を使用してネットワーク経由で通信するプロセスとアプリケーションのリストが表示されます。また、アプリケーションの接続先となるリモートアドレスも一緒に表示されます。DNS サーバーの IP アドレスをチェックすることもできます。 詳細ウインドウには、ファイルサイズやハッシュなど、詳細情報が表示されます。
重要なレジストリエントリ	システムの問題に関連するレジストリーエントリーが表示されます。 説明ウインドウで、特定のレジストリーエントリーに関連するファイルを確認できます。
サービス	説明ウインドウには、Windows サービスとして登録されているファイルのリストが表示されます。詳細ウインドウで、サービスを開始するための設定方法と、ファイルに関する特定の詳細情報を確認できます。
ドライバ	説明ウインドウには、システムにインストールされているドライバーのリストが表示されます。
重要なファイル	説明ウインドウには、Microsoft Windows オペレーティングシステムに関連する重要なファイルの内容が表示されます。
システムスケジューラタスク	説明ウインドウには、Windows タスクスケジューラによって開始されるタスクのリストが表示されます。
システム情報	説明ウインドウには、ハードウェアとソフトウェアに関する詳細情報、および set 環境変数、ユーザー権限、システムイベントログに関する情報が表示されます。
ファイルの詳細	「プログラムファイル」フォルダー内の重要なシステムファイルおよびファイルのリストです。ファイル固有の追加情報は、説明ウインドウと詳細ウインドウで確認できます。
バージョン情報	説明ウインドウには、ESET SysInspector のバージョンに関する情報およびプログラムモジュールのリストが表示されます。
検索結果	説明ウインドウには、検索結果の詳細が表示されます。

■キーボードショートカット

ESET SysInspector で使用できるキーボードショートカットは、次のとおりです。

●ファイル

Ctrl + O	既存のログを開きます。
Ctrl + S	作成したログを保存します。

●生成

Ctrl + G	標準のスナップショットを生成します。
Ctrl + H	機密情報を含めたスナップショットを生成します。

●項目のフィルタリング

1、O	良好、危険レベル 1 ～ 9 のノードを表示します。
2	良好、危険レベル 2 ～ 9 のノードを表示します。
3	良好、危険レベル 3 ～ 9 のノードを表示します。
4、U	不明、危険レベル 4 ～ 9 のノードを表示します。
5	不明、危険レベル 5 ～ 9 のノードを表示します。
6	不明、危険レベル 6 ～ 9 のノードを表示します。
7、B	危険、危険レベル 7 ～ 9 のノードを表示します。
8	危険、危険レベル 8 ～ 9 のノードを表示します。
9	危険、危険レベル 9 のノードを表示します。
-	フィルタリングの危険レベルを下げます。
+	フィルタリングの危険レベルを上げます。
Ctrl + 9	フィルタリングレベルと同等以上の危険レベルのノードを表示します。
Ctrl + 0	フィルタリングレベルと同等の危険レベルのノードのみ表示します。

●表示

Ctrl + 5	すべてのベンダーを表示します。
Ctrl + 6	Microsoft のみ表示します。
Ctrl + 7	Microsoft 以外のすべてのベンダーを表示します。
Ctrl + 3	完全な詳細情報を表示します。
Ctrl + 2	中程度の詳細情報を表示します。
Ctrl + 1	基本的な情報を表示します。
BackSpace	1 つ前の情報に戻ります。
Space	1 つ先の情報に進みます。
Ctrl + W	ノードのツリーを展開します。
Ctrl + Q	ノードのツリーを折りたたみます。

●その他のコントロール

Ctrl + T	検索結果で選択した後、項目の元の場所に移動します。
Ctrl + P	項目の基本情報を表示します。
Ctrl + A	項目のすべての情報を表示します。
Ctrl + C	選択している項目のツリーをコピーします。
Ctrl + X	選択している項目の情報をコピーします。
Ctrl + B	選択しているファイルについての情報をインターネット上で検索します。
Ctrl + L	選択しているファイルが格納されているフォルダーを開きます。
Ctrl + R	該当するエントリーをレジストリーエディターで開きます。ただし、このショートカットは日本語 OS では利用できません。
Ctrl + Z	項目がファイルに関連付けられている場合、ファイルまでのパスをコピーします。
Ctrl + F	検索フィールドに切り替えます。
Ctrl + D	検索結果を閉じます。
Ctrl + E	サービススクリプトを実行します。

●比較

Ctrl + Alt + O	比較元と比較先のログを開きます。
Ctrl + Alt + R	比較を取り消します。
Ctrl + Alt + 1	すべての情報を表示します。
Ctrl + Alt + 2	追加された情報のみを表示します。画面には現在のログにある情報が表示されます。
Ctrl + Alt + 3	削除された情報のみを表示します。画面には前回のログにある情報が表示されます。
Ctrl + Alt + 4	置き換えられた情報のみを表示します（ファイルを含む）。
Ctrl + Alt + 5	変更された情報のみを表示します。
Ctrl + Alt + C	比較結果を表示します。
Ctrl + Alt + N	現在のログを表示します。
Ctrl + Alt + P	前回のログを開きます。

●その他

F1	ヘルプを表示します。
Alt + F4	ESET SysInspector を閉じます。
Alt + Shift + F4	確認せずに ESET SysInspector を閉じます。
Ctrl + I	統計をログに記録します。

■ログの比較

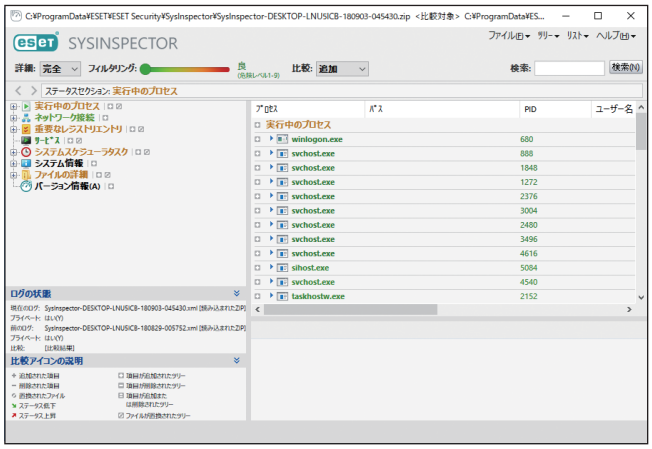
2 つのログを比較して、相違項目を洗い出します。ログの比較はシステムの変更を追跡し、悪意のあるコードを検出するのに役立ちます。

●ログの保存／表示

ESET SysInspector アプリケーションが起動すると、自動的に新しいログが作成されます。［ファイル］>［ログの保存］をクリックすると、ログを保存できます。保存したログを開くには、［ファイル］>［ログを開く］をクリックします。

●ログ比較の実行

現在表示されているログと、保存されたログを比較します。［ファイル］>［ログの比較］>［ファイルの選択］をクリックし、比較するログを選択します。比較が実行され、2 つのログで異なる項目のみが画面に表示されます。

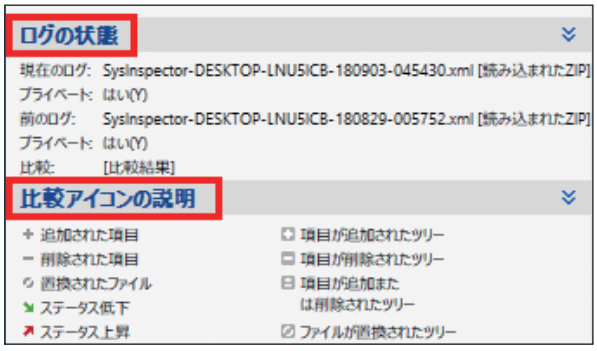


リストに表示される記号は、次の意味を表します。

項目の横に表示される記号について次に説明します。

	以前のログには存在しない新しい値
	新しい値を含むツリー
	以前のログにのみ存在する、削除された値
	削除された値を含むツリー
	変更されている値／ファイル
	変更された値／ファイルを含むツリー
	危険レベルが以前のログよりも低下
	危険レベルが以前のログよりも上昇

画面左下の「ログの状態」セクションには、比較対象のログの名前が表示されます。また、「比較アイコンの説明」セクションでは、すべての記号の説明が表示されます。



ワンポイント

［ファイル］>［ログの保存］で比較ログをファイルに保存して、後で開くことができます。

5.4.3 コマンドラインからのログ生成

次のパラメーターを使用して Windows のコマンドラインからログを生成することもできます。

/gen	ESET SysInspector を起動せずにコマンドラインから直接ログを生成します。
/privacy	機密情報を省略したログを生成します。
/zip	生成されたログを ZIP アーカイブ形式で保存します。
/silent	コマンドラインからログを生成するときに、進捗状況を示す画面を表示しません。
/blank	ログの生成／読み込みを行わずに ESET SysInspector を起動します。

例：

- ログを SysInspector アプリケーションに読み込む

```
SysInspector.exe .\clientlog.xml
```

- コマンドラインからログを生成する

```
SysInspector.exe /gen=.\mynewlog.xml
```

- 機密情報を除外して、圧縮形式のログ生成する

```
SysInspector.exe /gen=.\mynewlog.zip /privacy /zip
```

- 2 つのログを比較して違いを確認する

```
SysInspector.exe new.xml old.xml
```

! 重　要

ファイル／フォルダーの名前に空白が含まれている場合は、名前を引用符「'」（アポストロフィー）で囲む必要があります。

5.4.4 サービススクリプト

サービススクリプトを使用すると、システムから不要なオブジェクトを簡単に削除できます。

サービススクリプトを使用して不要なオブジェクトを削除するには、必要なセクションをサービススクリプトファイルとしてエクスポートし、不要なオブジェクトに削除対象のマークを付けます。このサービススクリプトファイルを実行すると、マークを付けたオブジェクトがシステムから削除されます。

! 重　要

サービススクリプトは、上級ユーザー向けのツールです。十分な知識がないユーザーがシステムを変更すると、オペレーティングシステムの障害を引き起こす可能性があります。

■サービススクリプトの使用例

ウイルス対策プログラムでは検出されないウイルスに感染している疑いがある場合にプロセスやモジュールをコンピューターから削除することができます。

操作手順

1. ESET SysInspector を起動して、システムスナップショットを新規に生成します。
2. ナビゲーションエリアで最初のセクションをクリックした後、【Shift】キーを押しながら最後のセクションをクリックして、すべてのセクションを選択します。
3. 選択したセクションを右クリックし、［選択したセクションをサービススクリプトにエクスポート］をクリックします。

   選択したセクションがサービススクリプトファイルとしてテキストファイル形式でエクスポートされます。
4. エクスポートしたサービススクリプトファイルをテキストエディターなどで開いて、削除対象のすべてのオブジェクトの先頭にある「-」記号を「+」記号に変更します。

！重　要

サービススクリプトで最も重要な手順です。オペレーティングシステムの重要なファイルやオブジェクトを「+」記号に変更していないことを確認してください。

```
ESET SystemStatus log, versions: ev 1254 (20150924), gv EES 6.2.2021.1, lv 1.0
Session start: 13 Nov 2015, 08:13:16
Session end: 13 Nov 2015, 08:14:37
Flags: 64bit, AntiStealth
Description: SysInspector-JUNMOBILE-151113-081314

01) Running processes:
- system *0,263A*
- system *4,263A*
- c:¥windows¥system32¥smss.exe *352,F99D*
- c:¥windows¥system32¥csrss.exe *528,A7D9*
- c:¥windows¥system32¥wininit.exe *604,AECC*
- c:¥windows¥system32¥services.exe *724,B9DC*
- c:¥windows¥system32¥lsass.exe *732,EF1A*
- c:¥windows¥system32¥svchost.exe *840,A512*
- c:¥windows¥system32¥svchost.exe *916,B20E*
- c:¥windows¥system32¥svchost.exe *316,5156*
- c:¥windows¥system32¥svchost.exe *372,229B*
- c:¥windows¥system32¥svchost.exe *432,929C*
- c:¥windows¥system32¥svchost.exe *812,E150*
- c:¥windows¥system32¥svchost.exe *1048,513A*
- c:¥windows¥system32¥wudfhost.exe *1136,ECC7*
- c:¥windows¥system32¥dashost.exe *1464,6F03*
- c:¥windows¥system32¥wudfhost.exe *1488,8537*
- c:¥windows¥system32¥svchost.exe *1796,59B5*
- c:¥program files (x86)¥fortinet¥forticlient¥scheduler.exe *1884,D359*
```

5. ESET SysInspector の［ファイル］>［サービススクリプトの実行］をクリックし、手順 4 で属性を変更したサービススクリプトファイルを選択します。
6. ［はい］をクリックしてサービススクリプトを実行します。

■サービススクリプトの生成

サービススクリプトを生成するには、ESET SysInspector のナビゲーションエリアで任意のセクションを右クリックし、コンテキストメニューから［すべてのセクションをサービススクリプトにエクスポート］をクリックするか、セクションを範囲選択してから右クリックし、コンテキストメニューから［選択したセクションをサービススクリプトにエクスポート］をクリックします。

！重　要

2 つのログを比較しているときは、サービススクリプトをエクスポートすることはできません。

■サービススクリプトの構造

サービススクリプトのヘッダーの行には、エンジンバージョン（ev）、GUI バージョン（gv）、ログバージョン（lv）に関する情報が記載されています。このデータを使用して、スクリプトを生成した .xml ファイル内の変更内容を追跡し、実行中に不整合が発生するのを防ぐことができます。スクリプトのヘッダー行は変更しないでください。

ヘッダー行以下は、セクションに分かれており、内容を編集することができます。項目の前にある「-」記号を「+」記号に置き換えることで、項目が処理対象としてマークされます。スクリプト内の各セクションは、空の行によって区切られています。各セクションには、番号とタイトルが付けられています。

01) Running processes（実行中のプロセス）

システム内で実行されているすべてのプロセスが含まれます。各プロセスは、UNC パスと、「*」（アスタリスク）で囲まれた CRC16 ハッシュコードによって識別されます。

例：

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

この例では、プロセス「module32.exe」が選択されています（「+」記号でマークされています）。このプロセスは、サービススクリプトの実行時に終了します。

02) Loaded modules（読み込まれたモジュール）

現在使用されているシステムモジュールの一覧が表示されます。

例：

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

この例では、モジュール「khbekhb.dll」が選択されています（「+」記号でマークされています）。サービススクリプトを実行すると、モジュール「khbekhb.dll」を使用しているプロセスが終了します。

03) TCP connections（TCP 接続）
既存の TCP 接続に関する情報が含まれます。

例：
```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds),
owner:
System
[...]
```

サービススクリプトを実行すると、「+」記号でマークされた TCP 接続内のソケットの所有者が発見され、ソケットが停止し、システムリソースが解放されます。

04) UDP endpoints（UDP エンドポイント）
既存の UDP エンドポイントに関する情報が含まれます。

例：
```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

サービススクリプトを実行すると、「+」記号でマークされた UDP エンドポイントのソケットの所有者が分離され、ソケットが停止されます。

05) DNS server entries（DNS サーバー関連のエントリー）
現在の DNS サーバーのコンフィグレーションに関する情報が含まれます。

例：
```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

サービススクリプトを実行すると、「+」記号でマークされた DNS サーバーエントリーが削除されます。

06) Important registry entries（重要なレジストリーエントリー）

重要なレジストリーエントリーに関する情報が含まれます。

例：

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

サービススクリプトを実行すると、「+」記号でマークされたエントリーが削除されるか、0 バイト値に縮小されるか、既定値にリセットされます。エントリーに適用されるアクションは、エントリーのカテゴリーとレジストリーのキー値によって異なります。

07) Services（サービス）

システム内の登録済みサービスの一覧が表示されます。

例：

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state:
Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll,
state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state:
Stopped,
startup: Manual
[...]
```

サービススクリプトを実行すると、「+」記号でマークされたサービスとその依存サービスが停止し、アンインストールされます。

08) Drivers（ドライバー）

インストール済みのドライバーの一覧が表示されます。

例:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

サービススクリプトを実行すると、「+」記号でマークされたドライバーは停止します。ドライバーによっては、停止しないことがあります。

09) Critical files（不可欠なファイル）

オペレーティングシステムが正常に機能するために必要なファイルに関する情報が表示されます。

例:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

サービススクリプトを実行すると、「+」記号でマークされたファイルは削除されるか、元の値にリセットされます。

■サービススクリプトの実行

次の操作でサービススクリプトを実行します。

操作手順

1. テキストエディターを使って、サービススクリプトファイルで操作対象となる項目を「+」記号でマークし、保存して閉じます。
2. ESET SysInspector で［ファイル］>［サービススクリプトの実行］をクリックします。

   サービススクリプトが起動し、「サービススクリプト<ファイル名>を実行しますか？」というメッセージが表示されます。
3. ［はい］をクリックします。

   ワンポイント
   「実行しようとしているサービススクリプトが署名されていない」という警告が表示される場合があります。
4. ［実行］をクリックします。

   サービススクリプトが実行され、サービススクリプトが正常に実行されたことを示すダイアログボックスが表示されます。

●表示されるメッセージ

「サービススクリプトは部分的に実行されました。エラーレポートを表示しますか？」
スクリプトの一部が処理されませんでした。［はい］をクリックすると、実行されなかったスクリプトが記載されているエラーレポートが表示されます。

「選択したサービススクリプトは署名されていません。署名されていない不明なスクリプトを実行すると、コンピューターのデータに深刻なダメージを与えるおそれがあります。スクリプトを実行し、アクションを実行してもよろしいですか？」
サービススクリプトが認識されませんでした。サービススクリプト内の不整合（見出しが損傷している、セクションタイトルが壊れている、セクション間の空の列が失われているなど）によって引き起こされた可能性があります。スクリプト内のエラーを修正するか、新しいサービススクリプトを作成して再度実行してください。

5.4.5 FAQ

ESET SysInspector を実行するには管理者権限が必要ですか？

管理者権限は必要ありませんが、管理者アカウントでなければ収集できない情報があります。標準ユーザーまたは制限付きユーザーが実行した場合は、動作環境に関する情報の収集量は少なくなります。

ESET SysInspector ではログファイルが作成されますか？

コンピューターに関する詳細なログファイルが作成されます。ログを保存するには、[ファイル] > [ログの保存] をクリックします。既定では、ファイルは % USERPROFILE%¥My Documents¥ ディレクトリーに保存されます。ファイル名は、SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML のフォーマットで自動的に付けられます。保存場所とファイル名を必要に応じて変更できます。

ESET SysInspector のログファイルを表示するにはどうしたらいいですか？

ESET SysInspector を実行し、コントロールエリアの［ファイル］>［ログを開く］をクリックします。ログファイルを ESET SysInspector のメイン画面にドラッグアンドドロップして開くこともできます。ログファイルを頻繁に表示する場合は、デスクトップに SYSINSPECTOR.EXE ファイルへのショートカットを作成することをお勧めします。ログファイルをショートカットにドラッグアンドドロップして表示することができます。

ワンポイント

セキュリティ上の理由で、Windows Vista と Windows 7 では異なるセキュリティアクセス許可を持つウィンドウ間でのドラッグアンドドロップが許可されない場合があります。

ログファイルの形式についての詳細情報はありますか？ SDK は使用できますか？

現時点では、ログファイルの仕様は開示していません。また、SDK は使用していません。

ESET SysInspector ではリスクをどのように評価していますか？

ESET SysInspector は、各オブジェクトの特性を検証して悪意のある活動である可能性をランク付けする一連のヒューリスティックルールを使用します。オブジェクト（ファイル、プロセス、レジストリーキーなど）に「1：良好（緑）」～「9：危険（赤）」の危険レベルを割り当てます。画面左側のナビゲーションエリアでは、オブジェクトの最大危険レベルを基にセクションが色分けされます。

危険レベル「6：不明（赤）」は、オブジェクトが危険であることを意味しますか？

これは評価でオブジェクトが悪意のあるものと確定されるわけではありません。セキュリティの専門家による判断が必要です。ESET SysInspector は、セキュリティの専門家がシステムのどのオブジェクトの動作を詳細に検証する必要があるかを、迅速に判断する手助けになるように設計されています。

ESET SysInspector の実行時にインターネットに接続するのはなぜですか？

ESET SysInspector には、改変されていないことを確認できるように「証明書」のデジタル署名が付けられています。証明書を検証するために、オペレーティングシステムは証明機関にソフトウェア発行元を問い合わせて確認します。これは、Windows オペレーティングシステムで動作するすべてのデジタル署名プログラムの標準的な動作です。

アンチステルス技術とはどのようなものですか？

アンチステルス技術は、ルートキットを効率的に検出するための技術です。
ルートキットとして動作する悪意のあるコードはデータの破壊や盗難などを引き起こします。専用のルートキット対策ツールがなければ、ルートキットの検出はほとんど不可能です。

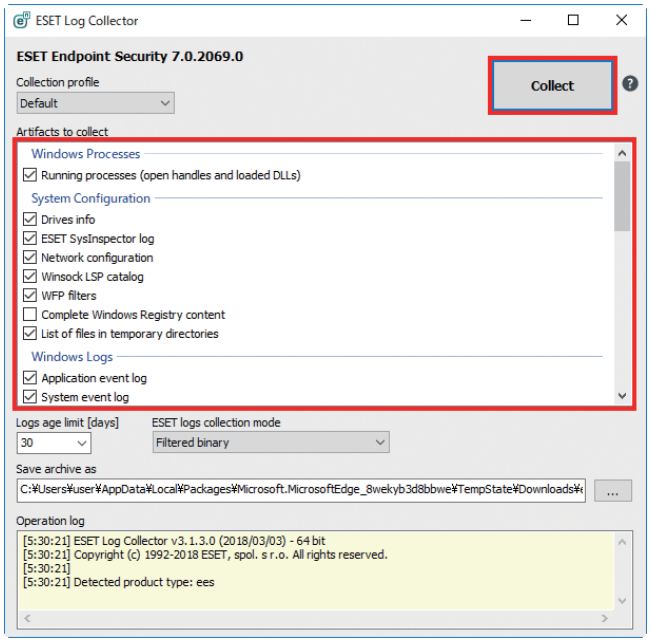
「MS によって署名済み」としてマークされたファイルが、異なる「会社名」エントリーを同時に持つことがあるのはなぜですか？

実行可能ファイルのデジタル署名を識別するときにファイルに埋め込まれたデジタル署名をチェックします。デジタル署名が検出されると、その情報を使ってファイルを検証します。デジタル署名が見つからない場合、ESET SysInspector は処理する実行可能ファイルに関する情報を収めた CAT ファイル（セキュリティカタログ - % systemroot%¥system32¥catroot）の検索を開始します。該当する CAT ファイルが見つかると、CAT ファイルのデジタル署名を使って検証します。「Signed by MS」というマークのあるファイルが、異なる「CompanyName」エントリーを持つ場合があるのはこのためです。

5.5 ESET Log Collector

ESET Log Collector を使うと、構成やログなど必要な情報を、サーバーから自動的に収集することができます。ESET カスタマーサポートでは、ログの提供をお願いする場合があります。こうした際、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 は［メインメニュー］＞［ヘルプとサポート］＞「ESET Log Collector」のリンクからダウンロードできます。



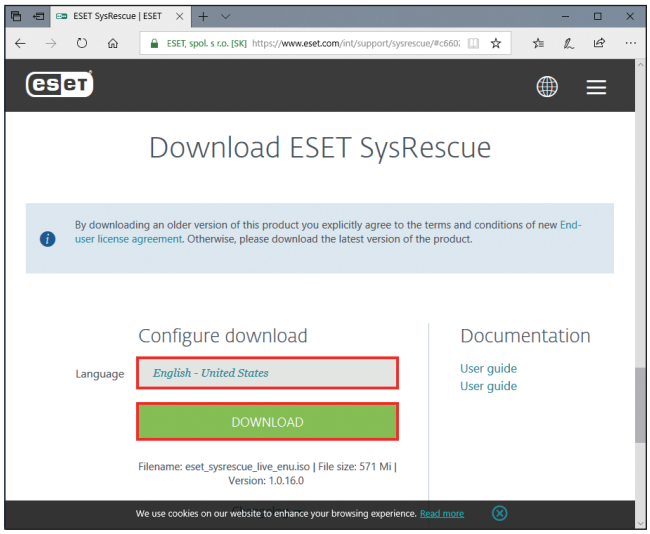
収集するログをチェックボックスで選択します。既定では、すべてのログが選択されています。ログの保存場所を指定して［保存］をクリックします。ログファイル名は自動的に設定されます。［Collect］をクリックすると、ログの収集が開始されます。

ログ収集中は、画面下部の「処理ログ」ウインドウで進行中の処理を確認することができます。終了するとログファイル名（emsx_logs.zip など）一覧が表示され、正常にログファイルが保存されたことを示します。

5.6 ESET SysRescue Live

ESET SysRescue Live は、ESET クライアント製品のブート可能ディスクを作成するためのユーティリティーです。ESET クライアント製品を ISO イメージを使って、オペレーティングシステムから独立して稼動し、ディスクとファイルシステムに直接アクセスできるようになります。また、オペレーティングシステムの実行中には削除ができない侵入物に対して効果を発揮します。

メインメニューの［ツール］＞［ESET SysRescue Live］を選択すると、リンク先の ESET の Web サイトが表示されます。ダウンロードの種類と言語を選択し、［ダウンロード］をクリックします。
詳しくは『ESET SysRescue Live ユーザーガイド』を参照してください。



5.7 ポリシーの上書き

ESET Endpoint Security のバージョン 6.5 以上がコンピューターにインストールされている場合は、ポリシーの上書き機能を使用できます。ポリシーの上書きモードでは、ESET Security Management Center のポリシーが適用された設定がある場合でも、クライアントコンピューター側で、インストールされた ESET 製品の設定を変更できます。上書きモードを利用させる際の認証方法は、特定の Active directory ユーザーを指定するか、パスワードを設定します。

! 重 要

上書きモードを有効にした場合は ESET Security Management Center から無効にできません。上書き時間が終了するか、クライアントコンピューター側で上書きの終了を行った場合にのみ、上書きモードが無効にされます。

ポリシーの上書き機能の設定方法

操作手順

1. ESET Security Management Center にログインします。
2. [管理] > [ポリシー] > [新しいポリシー] に移動します。
3. [設定] 画面で、[ESET Endpoint for Windows] を選択します。
4. [上書きモード] をクリックし、上書きモードのルールを設定します。
5. コンピューターにポリシーを適用します。

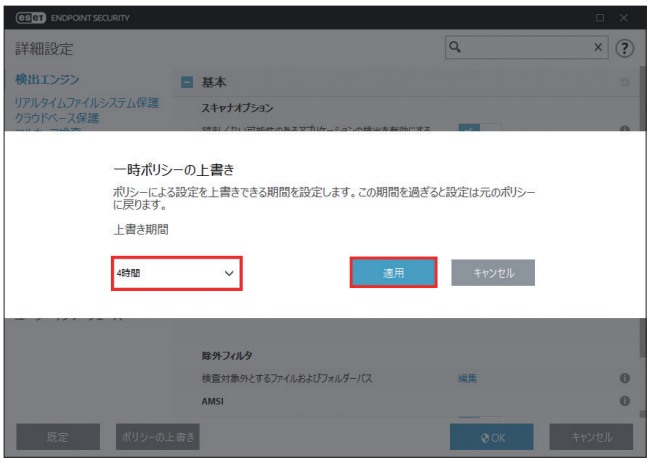
上書きモードを有効にする	上書きモードを有効にします。	
最大上書き時間	上書きモードを有効にする時間を設定します。 最大で 4 時間上書きモードを有効にすることができます。	
上書き後にコンピューターを検査する	有効にすると上書きモードを終了させた後に、コンピューターの検査が実行されます。	
認証タイプ	Active directory ユーザー	上書きモードを利用するユーザーを指定します。
	パスワード	上書きモードを利用する際のパスワードを設定します。 カスタムパスワードの項目にパスワードを入力します。

クライアントコンピューター側の操作手順

操作手順

1. ESET Endpoint Security の［設定］画面で［詳細設定］を選択します。
2. ［ポリシーの上書き］を選択します。

3. 上書き時間を選択して、適用を選択します。



4. ESET Security Management Center で設定した認証タイプに応じて、認証され上書きモードが有効になります。

●上書きモードの使用例

ユーザーの ESET Endpoint Security の設定に問題があり、一部の重要な機能または Web アクセスなどがブロックされる場合、管理者はユーザーに割り当てられたポリシーを上書きする権限を与えることができます。ユーザーが設定した新しい設定は ESET Security Management Center を用いて収集し、管理者はそこから新しいポリシーを作成できます。

ポリシーの変換手順

操作手順

1. ユーザーが上書きモードを使用し、ESET Endpoint Security の設定を編集します。
2. ESET Security Management Centerで該当のコンピューターを選択し、[詳細を表示] > [コンフィグレーション] を選択します。
3. [設定のリクエスト] を選択します。
4. しばらく待ち、コンフィグレーションが取得できたら、コンフィグレーションを開いて確認し、ポリシーに変換を選択します。
5. 新しく作成したポリシーをコンピューターに適用します。

Chapter 6 用語集

6.1 マルウェアの種類

マルウェアとは、コンピューターに入り込んで損害を与えようとする悪意があるソフトウェアのことです。

6.1.1 ウイルス

コンピューターウイルスとは、コンピューター上の既存のファイルにあらかじめ追加されている、または後から追加される悪意のあるコードのことです。ウイルスは生物学上のウイルスにちなんで名付けられました。生物学上のウイルスと同じような手法でコンピューター間に蔓延していくからです。「ウイルス」という用語は、あらゆる種類のマルウェアを意味するかのように誤って使用されることがよくあります。この用法は徐々に敬遠されるようになり、より正確な用語である「マルウェア」（悪意のあるソフトウェア）へと次第に言い換えられるようになっています。

コンピューターウイルスは、主に実行可能ファイルとドキュメントを攻撃します。コンピューターウイルスに感染すると、元のアプリケーションよりも前に悪意のあるコードが呼び出されて実行されます。ウイルスは、ユーザーが書き込み権限を持つすべてのファイルに感染することができます。

コンピューターウイルスの目的と重大さは多種多様です。ハードディスクからファイルを意図的に削除できるウイルスもあり、このようなウイルスは大変危険です。一方、実質的には被害を及ぼさないウイルスもあります。作成者が単にユーザーを困らせ、自分の技量を誇示することだけが目的のウイルスもあります。

コンピューターがウイルスに感染して駆除できない場合は、詳しい検査のために感染したファイルを ESET ラボに送ることができます。場合によっては、駆除が不可能であるためクリーンなコピーに置き換える必要があるほど改ざんされていることがあります。

6.1.2 ワーム

コンピューターワームとは、ネットワークを介して感染先のコンピューターを攻撃して蔓延する、悪意のあるコードの入ったプログラムを指します。ウイルスとワームの基本的な違いは、ワームは独自に伝播できることです。ワームは宿主のファイル（またはブートセクター）に依存しません。ワームはアドレス帳の電子メールアドレスを介して広がるか、またはネットワークアプリケーションのセキュリティ上の脆弱性を悪用します。

したがって、ワームはコンピューターウイルスよりはるかに危険性が高いです。インターネットは広く普及しているため、ワームはリリースから数時間、場合によっては数分で世界中に蔓延することがあります。自己増殖する能力があるので、他のマルウェアよりはるかに危険です。

システム内でワームが活性化すると、多くの不都合な事態が引き起こされることがあります。ファイルの削除、システムパフォーマンスの低下だけでなく、プログラムが動かなくなることすらあります。コンピューターワームはその本来の性質ゆえに、他のマルウェアの「搬送手段」となります。

コンピューターがワームに感染した場合は、悪意のあるコードが含まれている可能性が高いため、感染ファイルを削除することをお勧めします。

6.1.3 トロイの木馬

従来、コンピューター分野でのトロイの木馬は、自己を有益なプログラムに見せかけ、ユーザーを騙して実行させようとするマルウェアの 1 つとして定義されてきました。
トロイの木馬の範囲は非常に広いので、多くのサブカテゴリーに分類できます。

ダウンローダー	インターネットから他のマルウェアをダウンロードする機能を備えた悪意のあるプログラム。
ドロッパー	被害を受けるコンピューターに他のマルウェアを取り込む悪意のあるプログラム。
バックドアー	ネットワークを通じてコンピューターにアクセスし、遠隔操作できるようにする悪意のあるプログラム。
キーロガー（キーストロークロガー）	ユーザーが入力した各キーストロークを記録し、ネットワークを通じてその情報を送信するプログラム。
ダイアラー	ユーザーのインターネットサービスプロバイダーではなく、有料情報サービスを介して接続するよう設計された悪意のあるプログラム。新しい接続が作成されたことにユーザーが気づくのは、ほとんど不可能です。ダイアラーで被害を受けるのは、ダイヤルアップモデムを使用するユーザーのみです。今日ではあまり使用されていません。

コンピューター上のファイルがトロイの木馬として検出された場合、悪意のあるコードしか入っていない可能性が高いため、ファイルを削除することをお勧めします。

6.1.4 ルートキット

ルートキットとは、攻撃者が自己の存在を隠しながらシステムに無制限にアクセスできるようにする悪意のあるプログラムです。ルートキットは、システムにアクセス（通常はシステムの脆弱性を悪用します）した後、オペレーティングシステムのさまざまな機能を使用して、ウイルス対策ソフトウェアによる検出を免れます。具体的には、プロセス、ファイル、Windows レジストリーデータを隠します。そのため、通常のテスト技術を使用して検出することはほとんどできません。

ルートキットの検出処理には 2 つのレベルがあります。

1. システムへのアクセスを試みているときには、まだシステム内には存在しないので、活動していません。このレベルなら、ルートキットに感染しているファイルを検出できればたいていのウイルス対策システムはルートキットを排除できます。
2. 通常の検査で検出されない場合は、ESET Endpoint Security のアンチステルス技術を利用して、アクティブなルートキットを検出して駆除できます。

6.1.5 アドウェア

アドウェアは、広告機能をサポートしているソフトウェアです。広告を表示するプログラムが、このカテゴリーに分類されます。アドウェアアプリケーションは、広告が表示される新しいポップアップ画面を Web ブラウザー内に自動的に開いたり、Web ブラウザーのホームページを変更したりすることがよくあります。アドウェアは、フリーウェアプログラムの開発者が開発費を賄うことができるように、フリーウェアによく添付されています。

アドウェア自体は、危険ではありません。ユーザーが広告に悩まされるだけです。危険なのは、アドウェアがスパイウェアと同様に、追跡機能を発揮することがあるということです。

フリーウェア製品を使用する場合には、インストールプログラムに特に注意してください。ほとんどのインストールプログラム（インストーラー）は、アドウェアプログラムを追加でインストールすることをユーザーに通知します。アドウェアのインストールをキャンセルし、目的のプログラムのみをインストールできることが一般的です。

場合によっては、アドウェアをインストールしないと目的のプログラムをインストールできなかったり、機能が制限されてしまったりすることがあります。このようなプログラムをインストールした場合は、ユーザーがアドウェアのインストールに同意したことになり、アドウェアが頻繁にかつ「合法的に」システムにアクセスする危険性があります。後悔しないように、このようなプログラムはインストールしないほうが賢明です。

アドウェアとして検出されるファイルがコンピューターにある場合は、悪意のあるコードが含まれている可能性が高いため、削除することをお勧めします。

6.1.6 スパイウェア

このカテゴリーには、ユーザーの同意も認識もないまま個人情報を送信するすべてのアプリケーションが該当します。スパイウェアは追跡機能を使用して、アクセスした Web サイトの一覧、ユーザーの連絡先リストにある電子メールアドレス、記録されたキーストロークなどのさまざまな統計データを送信します。

スパイウェアの作成者は、こうした手法はユーザーのニーズと関心を調査し、的を絞った広告を出せるようにすることが目的であると主張します。問題は、有益なアプリケーションと悪意のあるアプリケーションとの間に明確な境界線がなく、しかも引き出された情報が悪用されることはない、とだれも断言できないことです。スパイウェアが収集したデータには、セキュリティコード、PIN、銀行の口座番号などが含まれていることがあります。スパイウェアはフリーバージョンプログラムの作成者がプログラムに同梱したり、プログラムのインストール中にスパイウェアが含まれていることをユーザーに知らせることがよくあります。これは、スパイウェアが含まれていない有料バージョンにアップグレードするよう促すことで、収益を上げたり、プログラムを購入する動機を与えようとしているためです。

スパイウェアが組み入れられている有名なフリーウェア製品として、P2P（ピアツーピア）ネットワークのクライアントアプリケーションがあります。Spyfalcon や Spy Sheriff を始めとする多数のプログラムは、スパイウェアの特定のサブカテゴリーに属します。これらは一見、スパイウェア対策プログラムに見えますが、実はそれ自体がスパイウェアプログラムなのです。

スパイウェアとして検出されるファイルがコンピューターにある場合は、悪意のあるコードが含まれている可能性が高いため、削除することをお勧めします。

6.1.7 圧縮プログラム

圧縮プログラムは、複数のマルウェアを 1 つのパッケージにロールアップするランタイム自己解凍実行可能ファイルです。

最も一般的な圧縮プログラムには、UPX、PE_Compact、PKLite、ASPack があります。別の圧縮プログラムを使用して圧縮した場合、同じマルウェアが異なって検出されることがあります。圧縮プログラムには、シグネチャーを時間の経過と共に変化させ、マルウェアの検出と削除を困難にする機能もあります。

6.1.8 安全ではない可能性があるアプリケーション

ネットワークに接続されたコンピューターの管理を容易にする機能を持つ適正なプログラムはたくさんあります。ただし、悪意のあるユーザーの手に渡ると、不正な目的で悪用される可能性があります。ESET Endpoint Security にはこのようなマルウェアを検出するオプションがあります。

「安全ではない可能性があるアプリケーション」は、市販の適正なソフトウェアに適用される分類です。これには、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）などのプログラムが含まれます。

安全ではない可能性があるアプリケーションがコンピューターで実行されている（しかも、自分ではインストールしていない）ことに気づいた場合には、ネットワーク管理者まで連絡するか、そのアプリケーションを削除してください。

6.1.9 望ましくない可能性があるアプリケーション

望ましくない可能性があるアプリケーションは、アドウェアを含んだり、ツールバーをインストールしたり、その他の不明確なオブジェクトを含んだりするプログラムです。場合によっては、ユーザーが望ましくない可能性があるアプリケーションを使用するリスクよりも利点の方が大きいと感じることがあります。このため、このようなアプリケーションには、トロイの木馬やワームなどのマルウェアと比べて、低いリスクのカテゴリーが割り当てられています。

■望ましくない可能性があるアプリケーションが検出された場合

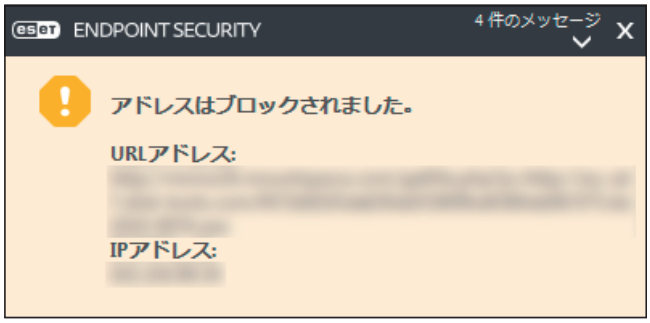
次の警告画面が表示されます。

ユーザーは実行するアクションを選択できます。

駆除／切断	アクションを終了し、潜在的な脅威がシステムに侵入するのを防ぎます。
何もしない	潜在的な脅威がシステムに侵入するのを許可します。

今後中断せずにコンピューターでアプリケーションを実行できるようにするには、［設定の表示］をクリックし、［検出対象外］をチェックします。

望ましくない可能性があるアプリケーションが検出され、駆除できない場合は、デスクトップの右下に「アドレスがブロックされました」という通知が表示されます。通知の詳細を確認するには、メインメニューの［ツール］>［ログファイル］をクリックし、ドロップダウンメニューから［フィルタリングされた Web サイト］を選択します。



■望ましくない可能性があるアプリケーションに関する設定

ESET Endpoint Security をインストールするとき、望ましくない可能性があるアプリケーションの検出を有効にするかどうかを設定できます。

また、望ましくないアプリケーションの検出設定は、設定オプションで変更できます。変更するには、次の操作を行います。

操作手順

1. ESET Endpoint Security を開きます。

   詳しくは「2.5　コンピューターの検査」の操作手順①、②を参照してください。

2. 【F5】キーを押します。

3. ［検出エンジン］をクリックし、次の各機能のしきい値を設定します。

   - マルウェア
   - 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

続く

4 [OK] をクリックします。

■ソフトウェアラッパー

ソフトウェアラッパーは特殊なタイプの修正アプリケーションで、ファイルホスティング Web サイトの一部で使用されます。ソフトウェアラッパーはサードパーティ製のツールですが、ツールバーやアドウェアなどの追加ソフトウェアもインストールします。追加されたソフトウェアは、Web ブラウザーのホームページや検索設定を変更する場合があります。多くの場合、ファイルホスティング Web サイトはソフトウェアベンダーやダウンロード受信者に設定が変更されたことを通知しないため、変更を回避することができません。このため、ESET Endpoint Security はソフトウェアラッパーを望ましくない可能性のあるアプリケーションのタイプに分類しています。ユーザーはソフトウェアラッパーをダウンロードするかどうかを設定できます。

IDS と詳細オプションに関する詳細は、「4.6.7 ネットワーク保護」の「●許可されたサービス」を参照してください。

6.1.10 ボットネット

ボットまたは Web ロボットは自動マルウェアプログラムであり、ネットワークアドレスのブロックを検査し、脆弱なコンピューターを感染させます。ボットを利用することでハッカーが同時に複数のコンピューターを乗っ取り、コンピューターをボット（ゾンビ）に変えることができます。一般的に、ハッカーはボットを使用して、多数のコンピューターを感染させます。このような大規模な感染コンピューターのグループがボットネットと呼ばれます。コンピューターが感染してボットネットのメンバーになると、分散型サービス拒否攻撃（DDoS）で使用されます。また、ユーザーが知らない間に、インターネット上での自動乗っ取りを実行するためにコンピューターが使用されることもあります（迷惑メール、ウイルスの送信、銀行の認証情報やクレジットカード番号などの個人情報の窃盗など）。

6.2 リモート攻撃の種類

攻撃者がリモートシステムを弱体化させる特別な手法は、いくつかのカテゴリーに分類できます。

6.2.1 ワーム攻撃

コンピューターワームとは、ネットワークを介して感染先のコンピューターを攻撃して蔓延する、悪意のあるコードが入ったプログラムを指します。ネットワークワームは、さまざまなアプリケーションに存在するセキュリティ上の脆弱性を悪用します。インターネットを通じて、ワームはリリースから数時間以内に世界中に蔓延することがあります。

ほとんどのワーム攻撃は、ファイアウォールの既定のセキュリティ設定で回避できます。また、パブリックネットワークではパブリックネットワーク保護タイプを選択し、最新のセキュリティパッチを適用して、オペレーティングシステムとプログラムを最新の状態に保つことが重要です。

6.2.2 DoS 攻撃

DoS（サービス拒否）とは、対象のユーザーがコンピューターやネットワークを使用できないようにする行為です。攻撃を受けたユーザー間の通信は妨害されるので、正常に機能し続けることができなくなります。DoS 攻撃にさらされたコンピューターを正常に機能させるには、通常再起動する必要があります。

ほとんどの場合、標的とされるのは Web サーバーであり、目的はある程度の期間ユーザーがサーバーを使用できなくすることです。

6.2.3 ポートスキャン

ポートスキャンは、ネットワークホスト上のどのポートが開いているかを特定するのに使用されます。ポートスキャナーは開いているポートを見つけるためのソフトウェアです。

ポートとは、受信データと送信データを処理する仮想の出入り口のことです。セキュリティの観点では、ポートは重要な要素です。ネットワークが大規模な場合、ポートスキャナーが収集した情報が、潜在的な脆弱性を特定するのに役立つことがあります。このような使用法は合法です。

ただし、ポートスキャンは、セキュリティを低下させようとするハッカーが悪用することもよくあります。ハッカーが行う最初の手順としては、パケットが各ポートに送信されます。その応答の種類に応じて、使用中のポートを判断することができます。スキャン自体は無害ですが、潜在的な脆弱性をあらわにし、攻撃者がリモートコンピューターを制御できるようにする可能性もあることに注意してください。

ネットワーク管理者は、未使用のポートをすべてブロックし、使用中のポートを無許可のアクセスから保護するようにすることをお勧めします。

6.2.4 DNS キャッシュポイズニング

DNS（ドメインネームサーバー）キャッシュポイズニングを使用すると、ハッカーは任意のコンピューターの DNS サーバーを騙し、偽のデータを提供して正規の（本物の）データであると信じさせることができます。特定の期間キャッシュされる偽の情報を利用して、攻撃者は DNS からの IP アドレスの返答を書き換えることができます。その結果、インターネット上の Web サイトにアクセスしようとするユーザーが、本来のコンテンツではなくコンピューターウイルスやワームをダウンロードさせられることがあります。

6.2.5 TCP 非同期

TCP 非同期とは、TCP ハイジャック攻撃で使用される手法です。あるプロセスで受信パケットのシーケンス番号が、所定のものと異なることが要因となります。所定のものでないシーケンス番号のパケットは、破棄されます（または、現在の通信画面に存在する場合には、バッファメモリーに保存されます）。

非同期処理では、双方の通信端末が、受信パケットを破棄します。リモートの攻撃者はこの部分に侵入して、正しいシーケンス番号を持つパケットを送り込むことができます。通信を操作したり、変更したりすることもできます。

TCP ハイジャック攻撃の目的は、サーバー／クライアント通信や P2P 通信を妨害することです。多くの攻撃は、各 TCP セグメントに認証を使用することで回避できます。また、使用しているネットワークデバイス向けの推奨設定を使用してください。

6.2.6 SMB リレー

SMBRelay と SMBRelay2 は、リモートコンピューターに攻撃を仕掛けることができる特殊なプログラムです。このプログラムは、Server Message Block ファイル共有プロトコルを利用します。このプロトコルは NetBIOS の上位層で機能します。LAN 内でフォルダーやディレクトリーを共有する場合、このファイル共有プロトコルを使用するのが一般的です。

ローカルネットワーク通信内では、パスワードハッシュが交換されます。

SMBRelay は、UDP ポート 139 と 445 で接続を受信し、クライアントとサーバー間で交換されるパケットを中継して、パケットを書き換えます。認証後、クライアントは接続を切断されます。SMBRelay は、新しい仮想の IP アドレスを作成します。新しいアドレスには、コマンド「`net use\\192.168.1.1`」でアクセスできます。これ以降、このアドレスは、Windows のネットワーク機能で使用できます。SMBRelay はネゴシエーションと認証以外の SMB プロトコル通信を中継します。クライアントコンピューターが接続している限り、リモートの攻撃者はこの IP アドレスを利用できます。

SMBRelay2 は SMBRelay と同じ原理で機能しますが、IP アドレスではなく NetBIOS 名を使用する点が異なります。どちらも「中間者」攻撃を実行できます。この場合リモートの攻撃者は、2 つの通信端末間で交換されるメッセージの読み取り、挿入、変更を密かに行えます。このような攻撃にさらされたコンピューターは、応答しなくなるか、突然再起動することがよくあります。

SMB リレーによる攻撃を避けるため、認証パスワードか認証鍵の使用をお勧めします。

6.2.7 ICMP 攻撃

ICMP（インターネット制御メッセージプロトコル）は、広く使用されている一般的なインターネットプロトコルです。主にさまざまなエラーメッセージを送信するために、ネットワークに接続されたコンピューターによって使用されます。

リモートの攻撃者は、ICMP プロトコルの脆弱性を悪用しようとします。ICMP プロトコルは、認証を必要としない一方向の通信用に設計されています。そのため、リモートの攻撃者は、いわゆる DoS 攻撃（サービス拒否攻撃）や、認証されていないユーザーに受信および送信パケットへのアクセス権を与える攻撃を開始することができます。

ICMP 攻撃の一般的な例として、ping フラッド、ICMP_ECHO フラッド、smurf 攻撃があります。ICMP 攻撃にさらされたコンピューターは処理速度が大幅に低下し（これは、インターネットを使用するすべてのアプリケーションに該当します）、インターネットへの接続に関する問題が発生します。

6.3 メール

メール（電子メール）は、多数の利点を備えた最新の通信形態で、柔軟性、速度、直接性があり、1990 年代の初めには、インターネットの普及において重要な役割を果たしました。

しかし、匿名性が高いため、電子メールとインターネットには迷惑メールなどの不正な活動の余地があります。迷惑メールは、受信者側が送信を要求していない広告、デマ、悪意のあるソフトウェア（マルウェア）を拡散します。送信費が最小限であること、また、迷惑メールの作成者には新しい電子メールアドレスを入手するさまざまなツールがあることから、ユーザーに対する迷惑行為や危険性は増加しています。さらに、迷惑メールの量や多様性のために、規制することは非常に困難です。電子メールアドレスを長く使用するほど、迷惑メールエンジンデータベースに登録される可能性が高くなります。回避策をいくつか紹介します。

- 可能な場合、インターネットに電子メールアドレスを公開しない。
- 信頼できる個人のみに電子メールアドレスを知らせる。
- 可能な場合、一般的なエイリアスを使用しない。複雑なエイリアスを使用するほど、追跡される可能性が低くなります。
- 受信ボックスに届いた迷惑メールに返信しない。
- インターネットフォームに記入する際に注意する。特に、「はい。情報を受信します。」のようなチェックボックスには注意してください。
- 仕事専用と友人専用など、用途ごとに異なる電子メールアドレスを使用する。
- 電子メールアドレスを定期的に変更する。
- 迷惑メール対策ソリューションを使用する。

6.3.1 広告

インターネット広告は、最も急速に普及している広告の 1 つです。マーケティング上の主な利点は、経費が最小限で済み、直接的に訴えることができること以外に、メッセージがほぼ瞬時に配信されることにあります。多くの企業では、メールをマーケティングツールとして使用して、既存顧客および見込み客と効果的に連絡を取り合っています。

この種の広告は適正なものです。ユーザーは製品に関する商業上の情報を受け取ることに関心がある可能性があるからです。しかし、多くの企業が、受信者側が送信を要求していない商業メッセージを大量に送っています。このような場合、メール広告は迷惑メールになってしまいます。

一方的に送信されてくるメールの量が実際に問題になっており、減少する兆しはありません。こうしたメールの作成者はたいてい、迷惑メールを適正なメッセージに見せかけようとします。

6.3.2 デマ

デマはインターネットを通じて広がる偽情報です。デマは通常、電子メールや ICQ、Skype などの通信ツールを経由して送信されます。メッセージ自体はジョークや都市伝説であることがほとんどです。

コンピューターウイルスとしてのデマは、受信者に恐怖、不安、および疑念（FUD）を抱かせ、ファイルを削除させたり、パスワードを取得させたりします。また、その他の有害な操作をシステムに対して実行する「検出不可能なウイルスがある」と信じ込ませます。

一部のデマは、他のユーザーにメッセージを送信するよう求め、デマを拡散させます。携帯電話によるデマ、援助の訴え、海外からの送金の申し出などがあります。ほとんどの場合、作成者の意図を突き止めることは不可能です。

知り合い全員に転送するよう求めるメッセージは、確実にデマであると考えられます。デマの疑いがあるメッセージを受け取った場合は、安易に転送などしないよう、注意してください。

6.3.3 フィッシング

フィッシングとは、ソーシャルエンジニアリング（機密情報を入手するためにユーザーを操ること）のさまざまな手法を用いる犯罪行為を指します。その目的は、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ことです。

入手するための一般的な手口は、信頼できる人物や企業（金融機関や保険会社など）を装い、電子メールを送ることです。この電子メールは本物そっくりに見えることがあり、成り済ます相手が使用しているグラフィックやインターネットコンテンツが含まれているのが一般的です。データの確認や金融業務を装い、銀行の口座番号やユーザー名、パスワードなど個人データを入力するようユーザーに指示します。このようなデータは、一度提出すると簡単に盗まれ悪用されてしまいます。

銀行、保険会社、およびその他の合法的な企業が、受信者側が送信を要求していない電子メールでユーザー名とパスワードを入力するように要求することは決してありません。

6.3.4 迷惑メール詐欺の特定

メールボックス内の迷惑メール（受信者が送信を要求していないメール）を特定するためのチェック項目がいくつかあります。受信メールが次のチェック項目のいくつかに該当する場合は、迷惑メールの可能性があります。

- 送信元アドレスが連絡先リスト内の連絡先のものではない。
- 多額のお金が提供されるが、最初に少額を提供する必要がある。
- データの確認や金融業務を装い、銀行の口座番号やユーザー名、パスワードなどの個人データを入力するよう求められる。
- 外国語で記載されている。
- 関心のない製品を購入するよう求められる。
  購入することにした場合は、メールの送信元が信頼できるベンダーであることを確認してください（本来の製品製造元に問い合わせてください）。
- 迷惑メールフィルターを騙そうとして、単語のスペルを間違えている。
  例えば、「viagra」の代わりに「vaigra」と記載している場合などです。

■ルール

ウイルス対策ソリューションと電子メールクライアントでは、ルールは電子メール機能を操作するためのツールとなります。ルールは次の 2 つの論理的部分で構成されます。

1. 条件
   例：受信メールがある特定の電子メールアドレスからのものである
2. アクション
   例：電子メールを削除したり、指定フォルダーに移動したりする

ルールの数と組み合わせは、迷惑メール対策ソリューションに応じて異なります。ルールは、迷惑メールを防ぐための手段となります。よくある例は、次のとおりです。

1. 条件：受信メールに、迷惑メールメッセージ特有の語がいくつか含まれる。
2. アクション：受信メールを削除する。

1. 条件：受信メールに、拡張子が .exe の添付ファイルが含まれる。
2. アクション：添付ファイルを削除してから、受信メールをメールボックスに配信する。

1. 条件：雇用者からの受信メールである。
2. アクション：受信メールを「仕事」フォルダーに移動する。

迷惑メール対策プログラムで複数のルールを組み合わせることで、メールを適切に管理し、迷惑メールフィルタリングの精度を向上させることをお勧めします。

■ホワイトリスト

一般的にホワイトリストとは、受け入れられる物や人物、または許可を与えられている物や人物の一覧を指します。「メールホワイトリスト」という用語は、ユーザーが電子メールを受信したいと思う相手の連絡先の一覧を意味します。このようなホワイトリストは、電子メールアドレス、ドメイン名、IP アドレスで構成されています。

ホワイトリストを「除外モード」で使用すると、一覧にない電子メールアドレス、ドメイン、IP アドレスからの電子メールは受信されません。「除外モード」でない場合は、一覧にない電子メールアドレス、ドメイン、IP アドレスからの電子メールでも削除されず、別の方法でフィルタリングされます。

ホワイトリストは、ブラックリストとは正反対の原則に基づきます。ホワイトリストの保守は、ブラックリストより簡単です。ホワイトリストとブラックリストの両方を使用して、迷惑メールをより効果的にフィルタリングすることをお勧めします。

■ブラックリスト

一般的にブラックリストとは、受け入れられない、または禁止されている品目や人物の一覧のことです。仮想世界では、電子メールの受信を拒否するためのテクニックです。

ブラックリストには、2 種類あります。ユーザーが迷惑メール対策ソフトウェアを使用して作成したブラックリストと、定期的にアップデートされる専門機関が作成したインターネット上にあるブラックリストです。

迷惑メールを防ぐにはブラックリストの使用は不可欠ですが、ブロックすべき新しい項目が毎日発生するため保守が困難です。迷惑メールをより効果的にフィルタリングするには、ホワイトリストとブラックリストの両方を使用することをお勧めします。

■除外リスト

通常、除外リストには、偽装されている可能性がある電子メールアドレスと迷惑メールの送信に使用されている可能性がある電子メールアドレスが含まれます。除外リストに登録されている電子メールアドレスから送信された電子メールに対しては、迷惑メールの検査を常に行います。既定では、電子メールクライアントのアカウントにあるすべての電子メールアドレスは、除外リストに入っています。

■サーバー側での検査

サーバー側での検査とは、受信メール数とユーザーの反応に基づいて、大量の迷惑メールを特定するための手法のことです。各電子メールは、その内容に基づいて固有のデジタルな「痕跡」を残します。痕跡で電子メールの内容を知ることはできません。2 通のメッセージが同じであれば痕跡も同じであり、異なれば痕跡も異なります。

ある電子メールが迷惑メールとしてマークされた場合、その痕跡がサーバーに送信されます。サーバーが迷惑メールとしてマークされた電子メールと同じ痕跡をさらに受信すると、痕跡は迷惑メール痕跡データベースに格納されます。受信メールを検査する際に、電子メールの痕跡がサーバーに送信されます。サーバーは迷惑メールとして既にマークされている電子メールの痕跡に関する情報を返します。

6.4 ESET 技術

6.4.1 エクスプロイトブロック

エクスプロイトブロックは、Web ブラウザー、PDF リーダー、電子メールクライアント、Microsoft Office コンポーネントなど、一般的に利用されるアプリケーションの保護を強化するための機能です。エクスプロイトを示す可能性がある不審なプロセスを監視します。悪意のあるファイルの検出に特化する技術と比べ、包括的なさまざまな技術を採用しているため、保護レイヤーが追加され、攻撃者への対応が強化されます。

エクスプロイトブロックによって不審なプロセスが特定されると、プロセスがただちに停止され、脅威に関するデータが記録されます。記録されたデータは ESET LiveGrid クラウドシステムに送信されます。送信されたデータは ESET 脅威ラボによって処理され、すべてのユーザーを未確認の脅威とゼロデイ攻撃（対応策がない新しくリリースされたマルウェア）からより効果的に保護するために使用されます。

6.4.2 アドバンスドメモリスキャナー

アドバンスドメモリスキャナーは、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。標準のエミュレーションまたはヒューリスティックでは脅威が検出されない場合、アドバンスドメモリスキャナーによって不審な動作を特定し、システムメモリーに現れたときには脅威を検査できます。

アドバンスドメモリスキャナーは、高度に難読化されたマルウェアに対しても有効ですが、エクスプロイトブロックとは異なり、後から実行される機能です。つまり、脅威が検出されたときには、悪意のある活動が既に実行されているというリスクがあります。ただし、他の検出方法が失敗する場合に備えることができるという効果があります。

6.4.3 ESET LiveGrid

ThreatSense.Net 高度早期警告システム上に構築された ESET LiveGrid は、ESET ユーザーが世界中で提出したデータを収集し、ESET のウイルスラボに送信します。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 は、ユーザー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 のマルウェア研究者はこの情報を使用して、脅威の特性と範囲の正確なスナップショットを構築し、適切な目標に集中できるようにします。ESET LiveGrid データは自動処理される機能の中で優先度の高いものです。

また、レピュテーションシステムを導入し、マルウェア対策ソリューションの全体的な効率を改善します。実行ファイルまたはアーカイブがユーザーのシステム上で検査されているときに、まずハッシュタグが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で比較されます。ホワイトリストで検出された場合、検査されたファイルはクリーンとみなされ、今後の検査対象から除外するように設定されます。ブラックリストで検出された場合、脅威の特性に応じて適切なアクションが実行されます。一致するものがない場合、ファイルは徹底的に検査されます。この検査の結果に基づいて、ファイルは脅威または脅威以外に分類されます。このアプローチは、検査のパフォーマンスに対して好ましい影響を及ぼします。

レピュテーションシステムによって、1 日に数回検出エンジン経由でシグネチャーがユーザーに配信される前に、マルウェアサンプルを効果的に検出できます。

6.4.4 ボットネット保護

ボットネット保護は、ネットワーク通信プロトコルを解析して、マルウェアを検出します。ボットネットマルウェアは、近年変更されていないネットワークプロトコルとは対照的に、頻繁に変更されています。ボットネット保護によって、コンピューターをボットネットネットワークに接続しようとするマルウェアを防止できます。

6.4.5 Java エクスプロイトブロック

Java エクスプロイトブロックは、既存の ESET エクスプロイトブロック保護を拡張したものです。Java を監視し、エクスプロイトのような動作を探します。ブロックされたサンプルはマルウェアアナリストに送信できます。アナリストは署名を作成し、別のレイヤー（URL ブロック、ファイルダウンロードなど）で Java エクスプロイトの試みをブロックできます。

6.4.6 スクリプトに基づく攻撃保護

スクリプトに基づく攻撃保護には、Web ブラウザーの JavaScript に対する保護と、Powershell のスクリプト（wscript.exe および cscript.exe）に対する Antimalware Scan Interface（AMSI）保護があります。
スクリプトに基づく攻撃保護は次の Web ブラウザーをサポートします。

- Mozilla Firefox
- Google Chrome
- Internet Explorer
- Microsoft Edge

6.4.7 ランサムウェアシールド

ランサムウェアはマルウェアの一種で、システムの画面をロックしたり、ファイルを暗号化することで、ユーザーがシステムにアクセスできないようにします。ランサムウェアシールドは、個人データを修正しようとするアプリケーションとプロセスの動作を監視します。アプリケーションの動作が悪意があると見なされた場合、またはレピュテーションに基づく検査によって不審なアプリケーションが示された場合、そのアプリケーションがブロックされるか、ユーザーがそれをブロックまたは許可するかを確認します。

6.4.8 DNA 検出

検出タイプには、非常に固有のハッシュから、悪意のある動作とマルウェア特性の複雑な定義である ESET DNA 検出までがあります。悪意のあるコードは、攻撃者が簡単に修正したり、難読化したりすることができますが、オブジェクトの動作はそれほど簡単には変更できません。ESET DNA 検出は、この原理を利用するために設計されました。

コードと、その動作の根源である正確な「遺伝子」を深く分析し、ESET DNA 検出を行います。これを使用して、ディスクにあるか、実行中のプロセスメモリーにあるかどうかに関係なく、潜在的に不審なコードを評価します。DNA 検出は、特定の確認済みのマルウェアサンプル、確認済みのマルウェアファミリーの新しいバリアント、または悪意のある動作を示す遺伝子を持つ未確認または未知のマルウェアさえも特定できます。

6.4.9 UEFI スキャナー

Unified Extensible Firmware Interface（UEFI）スキャナーは、ホストベースの侵入防止システム（HIPS）の一部であり、コンピューターの UEFI を保護します。UEFI はブートプロセスの最初にメモリーに読み込まれるファームウェアです。コードは、主基板に半田付けされたフラッシュメモリーチップにあります。感染すると、攻撃者は、システム再インストールおよび再起動の影響を受けないマルウェアを展開できます。また、このマルウェアのレイヤーは、ほとんどのマルウェア対策ソリューションで検査されないため、マルウェア対策ソリューションでは検出されずに残る可能性があります。

UEFI スキャナーは自動的に有効にされます。メインプログラムウィンドウでコンピューター検査を手動で開始するには、［コンピューター検査］>［カスタム検査］をクリックし、［ブートセクター /UEFI］をクリックします。コンピューターの検査の詳細は、「4.1 コンピューターの検査」を参照してください。

また、お使いのコンピューターが UEFI マルウェアに感染した場合は、UEFI ファームウェアを最新のバージョンにアップデートすることをお勧めします。