ESET File Security for Microsoft Windows Server 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。

○ 本マニュアルの著作権は、キヤノンマーケティングジャパン株式会社に帰属します。本マニュアルの一部または全部を無断で複写、複製、改変することはその形態を問わず、禁じます。

○ ESET、NOD32、ThreatSense、LiveGrid、ESET Endpoint Security、ESET Endpoint アンチウイルス、ESET File Security、ESET Security Management Center は、ESET, spol. s r.o. の商標です。

○ Microsoft、Windows、Windows Vista、Windows Server、Internet Explorer、Outlook、Windows Live、ActiveX は、米国 Microsoft Corporation の米国、日本およびその他の国における登録商標または商標です。

○ FireWire は、米国およびその他の国で登録されている Apple Inc. の商標です。

改定日　2019/9/2

目　次

Chapter 1 はじめに	1.1	ESET File Security for Microsoft Windows Server について 4
	1.2	動作環境 6
	1.3	ユーザーインターフェース 7
Chapter 2 インストール	2.1	インストール手順 8
	2.2	完全インストール 10
	2.3	カスタムインストール 13
	2.4	アクティベーション 15
	2.5	ターミナルサーバー 20
	2.6	最新バージョンへのアップグレード 21
	2.7	アンインストール 22
Chapter 3 ご利用開始時の 確認・設定事項	3.1	画面構成 25
	3.2	保護状態の確認 26
	3.3	アップデートの設定 28
	3.4	プロキシサーバーの設定 30
	3.5	設定の保護 32
	3.6	ESET Security Management Center との接続 34
Chapter 4 メインメニューの操作	4.1	ログファイル 35
	4.2	検査 38
	4.3	アップデート 48
	4.4	設定 50
	4.5	ツール 57
Chapter 5 設定	5.1	詳細設定 102
Chapter 6 用語集	6.1	マルウェアの種類 234

Chapter 1 はじめに

1.1 ESET File Security for Microsoft Windows Server について

ESET File Security for Microsoft Windows Server は、Microsoft Windows Server 環境専用に設計された統合ソリューションです。様々なタイプのマルウェア攻撃から効率的にしっかりと保護します。ESET File Security for Microsoft Windows Server で実装する保護は、2 種類あります。ウイルス対策とスパイウェア対策です。

ESET File Security for Microsoft Windows Server には、次の主要機能があります。

OneDrive 検査	Office 365 for Business の OneDrive クラウドストレージにあるファイルを検査できる機能です。
自動除外	動作とパフォーマンスをスムーズにするために、重要なアプリケーションとサーバーファイルを自動的に検出して除外します。
自己防衛	ESET のセキュリティソリューションが変更されたり、無効にされたりしないように保護します。
効果的なトラブルシューティング	さまざまな問題を解決するためのツールを内蔵しています。ESET SysInspector はシステムを診断します。ESET SysRescue Live はブート可能なレスキュー CD を作成します。
クラスタ機能	ワークステーションをノードに結合すると、すべてのクラスタメンバーで 1 つの構成ポリシーを配布できるため、管理がさらに自動化されます。クラスタ自体の作成は、インストールされたノードで実行できます。すべてのノードをリモートでインストールできます。ESET サーバー製品はそれぞれ通信し、構成や通知などのデータを交換するだけでなく、グレーリストデータベース、および製品インスタンスのグループが正しく動作するために必要なデータを同期することができます。クラスタ全体で製品の構成は同じです。Windows Failover Cluster および Network Load Balancing（NLB）Cluster は ESET File Security for Microsoft Windows Server によってサポートされます。また、クラスタメンバーを手動で追加できます。特定の Windows Cluster は必要ありません。クラスタ機能はドメインとワークグループ環境の両方で動作します。
コンポーネントベースのインストール	追加または削除するコンポーネントを選択できます。
ストレージ検査	ローカルサーバーのすべての共有ファイルを検査します。これで、ファイルサーバーに保存されたユーザーデータだけを選択して検査できます。

プロセスの除外	ウイルス対策リアルタイム検査から特定のプロセスを除外します。専用サーバー（アプリケーションサーバー、ストレージサーバーなど）の重要なロールのため、あらゆる種類の致命的なインシデントからのタイムリーな回復の保証に定期的なバックアップが欠かせません。バックアップ速度、プロセス整合性、サービスの可用性を改善するために、ファイルレベルのウイルス対策保護と競合すると見なされる一部の手法がバックアップ中に使用されます。同様の問題は、仮想マシンのライブ移行中にも発生する可能性があります。両方の状況を回避する唯一の効果的な方法は、ウイルス対策ソフトウェアを無効にすることです。たとえば、バックアップソリューションのプロセスの場合、このような除外されたプロセスに基づくすべてのファイル処理が無視され、安全であると見なされるため、バックアップ処理の中断を最小限に抑えることができます。なお、除外を作成するときには注意してください。除外されたバックアップツールは、アラートをトリガーせずに感染ファイルにアクセスできます。このため、拡張権限がリアルタイム保護モジュールでのみ許可されています。
eShell	eShell は、経験豊富なユーザーと管理者向けに、ESET サーバー製品を管理するための総合的なオプションを提供する、新しいコマンドライン管理インタフェースです。
ESET Security Management Center	ESET Security Management Center と接続することにより、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。ESMC の詳細については、ESET Security Management Center ユーザーズマニュアルを参照してください。
Hyper-V 検査	Microsoft Hyper-V Serverexlink 上の仮想マシン（VM）ディスクの検査を実行できる新しい技術です。特定の VM 上で「エージェント」は不要です。

1.1.1 保護の種類

ESET File Security for Microsoft Windows Server の保護機能には、次の 2 種類があります。

- ウイルス対策保護
- スパイウェア対策保護

ウイルス・スパイウェア対策の保護機能は、ESET File Security for Microsoft Windows Server の基本機能の一つです。ファイル、メール、インターネット通信を検査して、悪意のある攻撃からシステムを保護します。
検出されたウイルスは保護モジュールによりブロックされ、駆除、削除、隔離することで排除されます。

1.2 動作環境

ESET File Security for Microsoft Windows Server は Windows サーバー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参照してください。
https://eset-info.canon-its.jp/business/endpoint_protection_adv/spec.html

! 重 要

ESET File Security for Microsoft Windows Server は、クライアント OS にインストールすることはできません。クライアント OS をご使用の場合は、ESET Endpoint Security または ESET Endpoint アンチウイルス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 ユーザーインターフェース

ESET File Security for Microsoft Windows Server には、直感的に操作可能なグラフィカルユーザーインターフェース（GUI）があります。GUI によって、プログラムの主な機能に迅速かつ簡単にアクセスできます。

メイン GUI に加えて、【F5】キーを押してメイン GUI からアクセスできる詳細設定画面もあります。

【F5】キーを押すと、「詳細設定」画面が開き、設定可能なプログラム機能のメニューが表示されます。各自のニーズにあった設定とオプションを、「詳細設定」画面から指定できます。左側のメニューには、カテゴリーの「検出エンジン」、「アップデート」、「ネットワーク保護」、「WEB とメール」、「デバイスコントロール」、「ツール」、および「ユーザーインターフェース」が表示されます。一部のメインカテゴリーにはサブカテゴリーがあります。左側のメニューの項目（カテゴリーまたはサブカテゴリー）をクリックすると、該当する設定が右側のペインに表示されます。

GUI の詳細については、「3.1 画面構成」を参照してください。

Chapter 2 インストール

2.1 インストール手順

ESET File Security for Microsoft Windows Server のインストーラーは、ビルドインの Administrator アカウントで実行する必要があることに注意してください。その他のユーザーには、管理者グループのメンバーでない限り、十分なアクセス権が与えられません。従って、ビルドインの Administrator アカウントを使用する必要があり、Administrator 以外のユーザーアカウントでは、インストールを正常に完了することができません。

インストーラーを実行するには次の 2 通りの方法があります。

- ［管理者］アカウントの資格情報を使用してローカルにログインし、インストーラーを実行する。
- 他のユーザーとしてログインした場合、管理者としてコマンドプロンプトを開き、Administrator のアカウント資格情報を入力して Administrator としてコマンドを実行できるようにしてから、インストーラーを実行するコマンドを入力します（例：msiexec /i efsw_nt64_jpn）。
  ※「efsw_nt64_jpn」の部分は、実際に使用するインストーラー名に置き換えてください。

インストーラーを起動し、使用許諾契約（EULA）に同意すると、インストールウィザードが表示されるので、その案内に従って設定処理を行ってください。ライセンス契約の条項に同意しない場合、ウィザードは続行されません。
インストールには以下の 3 通りのタイプがあります。

完全	このインストールタイプを推奨します。 ESET File Security for Microsoft Windows Server のすべての機能をインストールします。このインストールを選択すると、製品をインストールするフォルダーを指定するだけでインストールできます。既定のインストールフォルダーを変更せずにそのままインストールすることを推奨します。インストーラーは、すべての機能を自動的にインストールします。 ※ Windows Server 2008、Windows Server 2008 R2 では「標準」と表示され、「ネットワーク保護」コンポーネント（「WEB とメール」機能、「ネットワーク保護」機能）が選択されていません。 上記 OS の API プラットフォームに問題があり、当該コンポーネントと競合する場合があるため、インストールしないことを推奨します。
コア	このインストールタイプは、Windows Server の Core インストールオプションです。インストール手順は、完全インストールと同じですが、インストーラーはコア機能のみとコマンドラインユーザーインターフェースを選択します。コアインストールは主に Windows Server Core 用ですが、特に必要がある場合には、標準の Windows Server にインストールすることもできます。標準インストールと比較した場合の主な違いは、標準の Windows Server にコアとしてインストールした場合、ESET File Security for Microsoft Windows Server には GUI がないということです。これは、ESET File Security for Microsoft Windows Server で作業しているときには、コマンドラインユーザーインターフェースのみ使用できることを意味しています。
カスタム	カスタムインストールタイプでは、ESET File Security for Microsoft Windows Server のプログラム機能を選択し、お使いのシステムにインストールすることができます。インストールするために選択する機能／コンポーネントの標準的なリストが表示されます。ウィザードインストールに加えて、コマンドライン経由で ESET File Security for Microsoft Windows Server のサイレントインストールを選択することもできます。このタイプのインストールでは、インストールウィザードを使用しません。自動インストールなどに適しています。このタイプのインストールでは、ユーザーの操作は不要です。

- サイレントインストール
  コマンドライン経由のフルインストール：`msiexec /i <packagename> /qn /l*xv msi.log`

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 File Security for Microsoft Windows Server をインストールする	P10 参照
STEP 2	アクティベーションを行う	P15 参照

!重 要

可能であれば、新規にインストールして設定した OS に ESET File Security for Microsoft Windows Server をインストールすることを強くお勧めします。既存のシステムに以前の ESET File Security for Microsoft Windows Server または ESET NOD32 Antivirus がインストールされている場合は、以前の製品をアンインストールし、サーバーを再起動してから新しく ESET File Security for Microsoft Windows Server をインストールすることをお勧めします。

!重 要

他社のウイルス対策ソフトウェアをシステムで使用していた場合は、ESET File Security for Microsoft Windows Server をインストールする前に、完全にアンインストールしてください。

!重 要

Windows Server 2016 以降に ESET File Security for Microsoft Windows Server をインストールしている場合、Microsoft は、Windows Defender 機能をアンインストールし、Windows Defender ATP 登録を解除して、複数のウイルス対策製品がコンピューターにインストールすることが原因で発生する問題を回避することを推奨しています。

2.2 完全インストール

このインストールタイプを推奨します。ESET File Security for Microsoft Windows Server のすべての機能をインストールします。このインストールを選択すると、製品をインストールするフォルダーを指定するだけでインストールできます。既定のインストールフォルダーを変更せずにそのままインストールすることを推奨します。インストーラーは、すべての機能を自動的にインストールします。

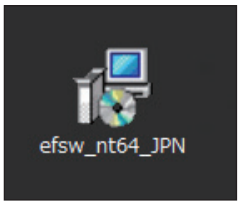
その他にコアインストールとカスタムインストールがあります。カスタムインストールを行う場合は、手順③まで操作を行った後「2.3 カスタムインストール」に進みます。

! 重 要

ESET File Security for Microsoft Windows Server 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。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。

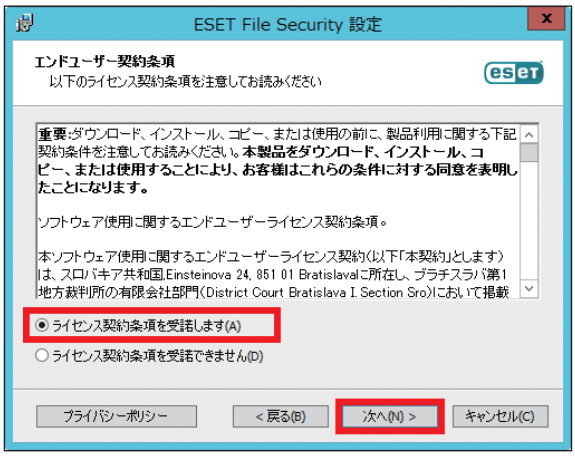


2 インストーラーが起動します。［次へ］ボタンをクリックします。

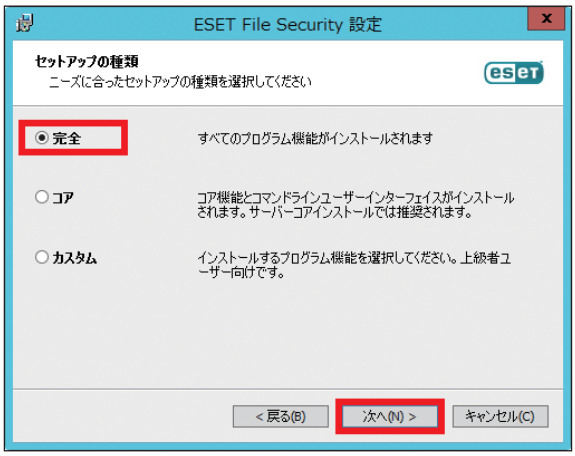


続く

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 ［完全］をチェックして［次へ］ボタンをクリックします。



インストールするプログラムを選択したい場合は、［カスタム］をチェックして［次へ］ボタンをクリックします。手順は「2.3 カスタムインストール」へ進みます。

ワンポイント

［コア］インストールは、Windows Server Core で使用します。コアコンポーネントだけがインストールされ、ESET File Security for Microsoft Windows Server には GUI がありません。また、必要に応じて、標準 Windows Server でコアインストールを実行できます。

続く

5 ［インストール］ボタンをクリックします。



ワンポイント

・［参照］ボタンをクリックしてインストール先を変更できますが、推奨されません。
・「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。

6 インストール完了までお待ちください。［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 File Security for Microsoft Windows Server 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 6 の後にサーバ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］をクリックしてサーバ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。



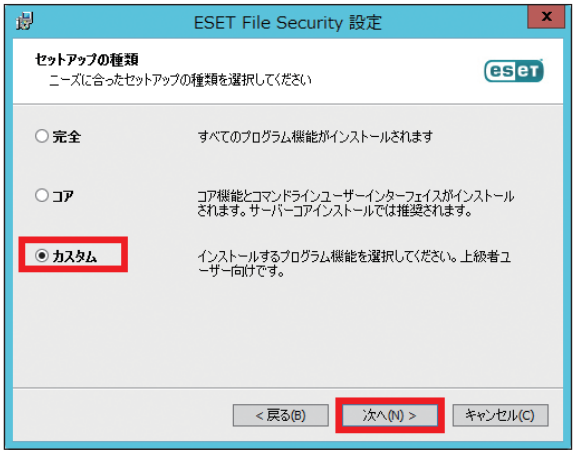
2.3 カスタムインストール

ESET File Security for Microsoft Windows Server を必要なコンポーネントだけにカスタマイズすることができます。コンポーネントを既存のインストールに追加するか、削除できます。初期インストール中に使用した .msi インストーラーパッケージを実行するか、［プログラムと機能］（Windows コントロールパネルからアクセス可能）に移動します。ESET File Security for Microsoft Windows Server を右クリックし、［変更］をクリックします。手動で実行する場合と同じ方法でインストーラーを開きます。

操作手順

「2.2 完全インストール」手順③の続き

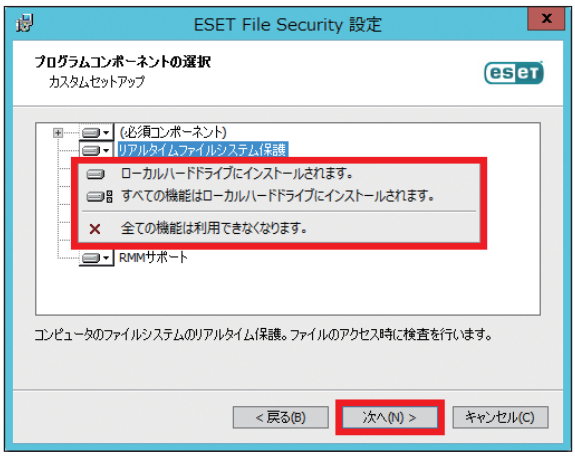
1 ［カスタム］をチェックして［次へ］ボタンをクリックします。



2 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。



続く

3 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てインストールするフォルダーを指定し、［インストール］ボタンをクリックします。

変更しない場合は、［インストール］ボタンをクリックします。



ワンポイント

・［参照］ボタンをクリックしてインストール先を変更できますが、この操作は推奨されません。
・「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。

4 インストール完了までお待ちください。［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 File Security for Microsoft Windows Server 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 4 の後にサーバ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］をクリックしてサーバ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またはオフラインライセンス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 File Security for Microsoft Windows Server に適用しアクティベーションすることができます。

! 重 要

製品をアクティベーションすると、検出エンジンが最新バージョンに更新されます。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［アクティベーション］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 File Security for Microsoft Windows Server 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。

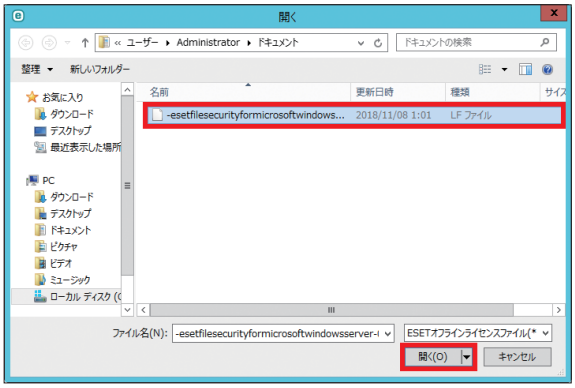


4. ［オフラインライセンス］をクリックします。



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 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。



2.4.3 アクティベーションが成功すると

操作手順

プログラムのメイン画面が表示され、「監視」画面に現在のステータスが表示されます。



ワンポイント

注意が必要な項目が赤や黄色で表示されますので、内容を確認して各設定を行ってください。すべての項目が解決されると監視ステータスが緑色になり、「最も高い保護」が表示されます。各設定の詳細については、「4.4.2 コンピュータ」を参照してください。
また、Windows Update や検出エンジンのアップデートなどに関する通知も表示されます。

2.5　ターミナルサーバー

ターミナルサーバーとして動作する Windows Server に ESET File Security for Microsoft Windows Server をインストールしている場合に、ユーザーのログインのたびに ESET File Security for Microsoft Windows Server の GUI が起動しないようにすることができます。無効にする具体的な手順については、「5.1.23　ユーザーインターフェース」の「●ターミナルサーバーでの GUI の無効化」を参照してください。

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 File Security for Microsoft Windows Server の新しいバージョンが提供されます。最新バージョンへのアップグレードには、次の 2 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「管理」メニュー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「Chapter3　インストール」を参照してください。

続く

2.7 アンインストール

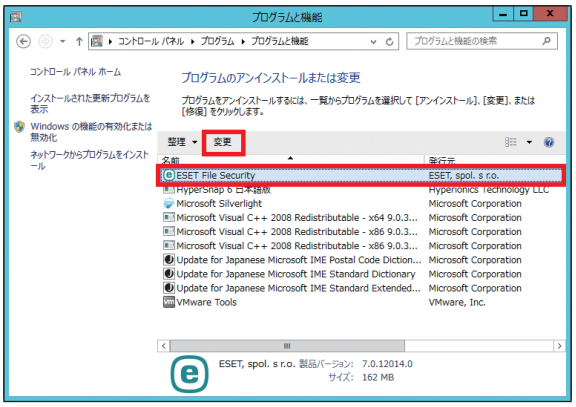
ESET File Security for Microsoft Windows Server のアンインストールは、インストールに使用した「.msi」インストーラーパッケージをダブルクリックして起動するか、「コントロールパネル」の「プログラムと機能」から行えます。

操作手順

1 コントロールパネルを起動し、「プログラムのアンインストール」をクリックします。



2 [ESET File Security] をクリックし、[変更] 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。



続く

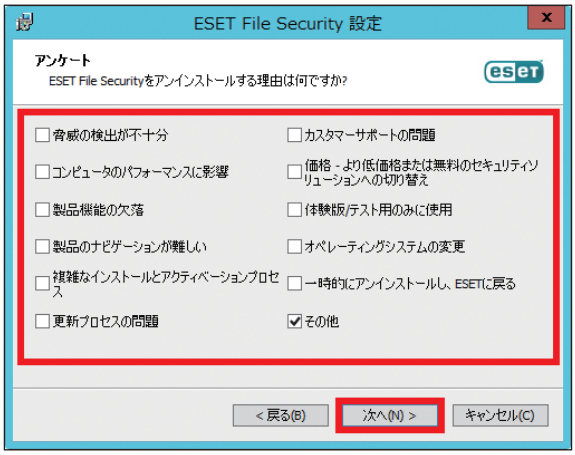
4 ［削除］ボタンをクリックします。



ワンポイント

［修正］をクリックすると、機能の追加または削除ができます。
［修復］をクリックすると、インストールのエラーの修復ができます。

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。

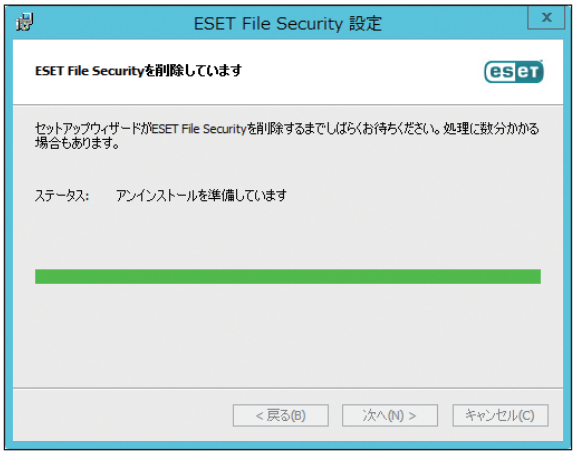


6 ［削除］ボタンをクリックします。



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。



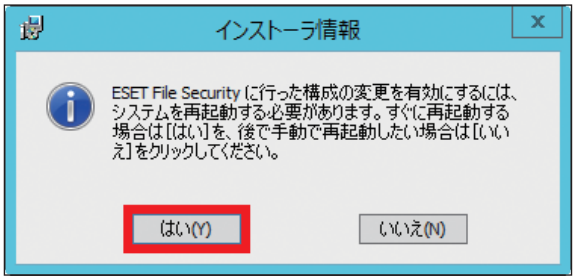
ワンポイント

「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 「［完了］ボタンを押してセットアップウィザードを終了してください。」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 再起動を促す画面が表示されます。［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 File Security for Microsoft Windows Server 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

監視	保護の状態、ライセンス有効期限、検出エンジンの最終アップデート日時、基本統計、システム情報が表示されます。
ログファイル	発生した重要なイベントに関する情報が含まれるログファイルを確認できます。これらのファイルには、検出、イベント、コンピュータの検査などの情報が含まれています。
検査	ストレージ検査、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、OneDrive 検査の設定や実行を行うことができます。また、前回実行した検査を再度実行することもできます。
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を表示し、アップデートが使用可能な場合は通知します。
設定	サーバーおよびコンピューターのセキュリティ設定を変更することができます。
ツール	セキュリティの管理を強化するツールの他に、システムと保護に関する詳細情報が表示されます。 [実行中のプロセス]、[アクティビティの確認]、[保護統計]、[クラスタ]、[ESET Shell]、[ESET SysInspector]、[ESET SysRescue Live]、[スケジューラ] にアクセスできます。また、分析用にサンプルを提出したり、隔離状況を確認できます。
ヘルプとサポート	製品ホームページのサポート情報、ヘルプページ、解決方法の情報の 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

保護状態を確認するには、メインメニューの一番上の［監視］をクリックします。
プライマリウインドウには、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。そうでない場合は、オレンジ色または赤色になり、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。
また、プライマリウインドウには頻繁に使用される機能と前回のアップデート情報も表示されます。



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
- 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。メインメニューの［設定］＞［コンピュータ］＞［リアルタイムファイルシステム保護］を有効にする、または同じ画面下部の［ウイルス対策およびスパイウェア保護を有効にする］をクリックします。
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が一時停止になっている
- オペレーティングシステムが最新の状態でない（Windows Update の最新データがインストールされていない）
- 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てアップデートできない）
- ライセンスの有効期限がせまっている

■主な解決策

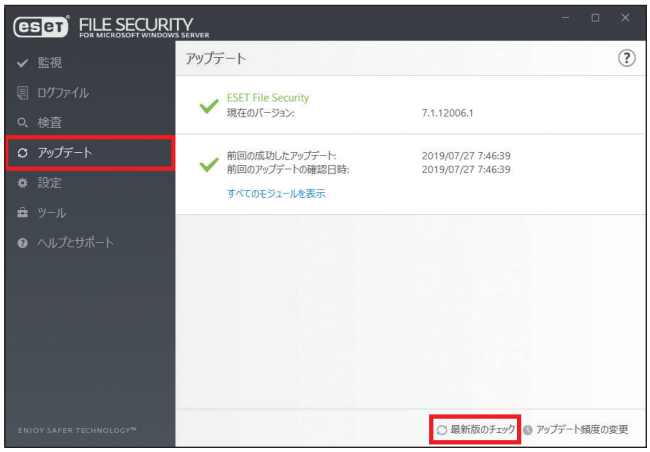
Web アクセス保護が無効になっています	Web アクセス保護を再有効化するには、セキュリティ通知をクリックしてから、［Web アクセス保護を有効にする］をクリックします。
電子メールクライアント保護が一時停止しています	「電子メールクライアント保護」が一時停止しています。［設定］メニューの［Web とメール］より、［電子メールクライアント保護］をクリックして有効にします。

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 File Security for Microsoft Windows Server 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］＞［詳細設定］をクリックします。



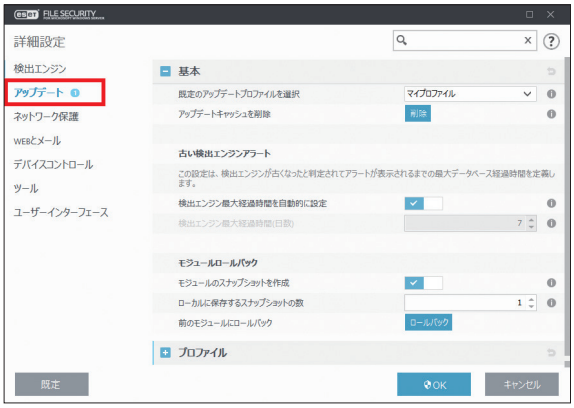
ワンポイント

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。

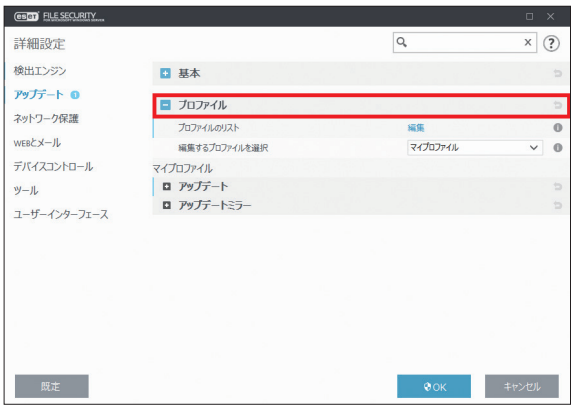
続く

❷ ［アップデート］をクリックします。

「基本」セクションでは、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。



！重　要

ライセンスのアクティベーションが行われていない場合は、アップデートすることができません。
製品認証キーは、［ヘルプとサポート］メニューの［ライセンスを管理］から入力します。

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

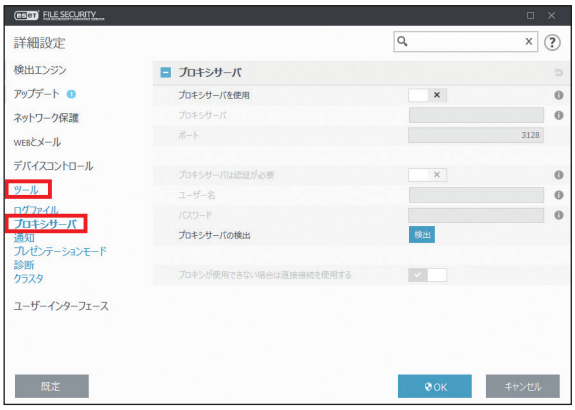
1 メインメニューの［設定］＞［詳細設定］をクリックします。



ワンポイント

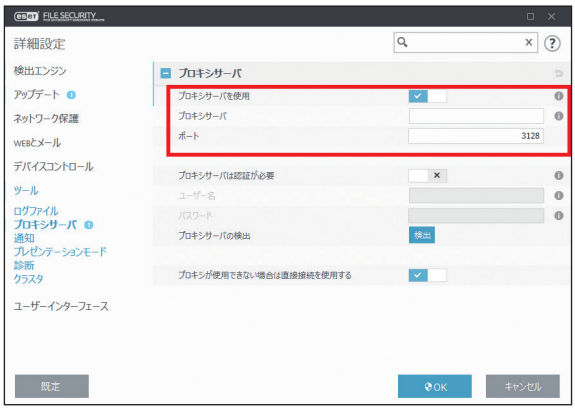
キーボードの【F5】キーを押して「詳細設定」画面を表示させることもできます。

2 ［ツール］の［プロキシサーバー］をクリックします。



続く

3 [プロキシサーバーを使用] 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。



プロキシサーバーとの通信に認証が必要な場合は、[プロキシサーバーは認証が必要] オプションを選択して、「ユーザー名」と「パスワード」を入力します。[検出] をクリックすると自動的にプロキシサーバーの設定が検出されて取り込まれます。

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異なる場合があります。異なる場合は、「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 File Security for Microsoft Windows Server 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

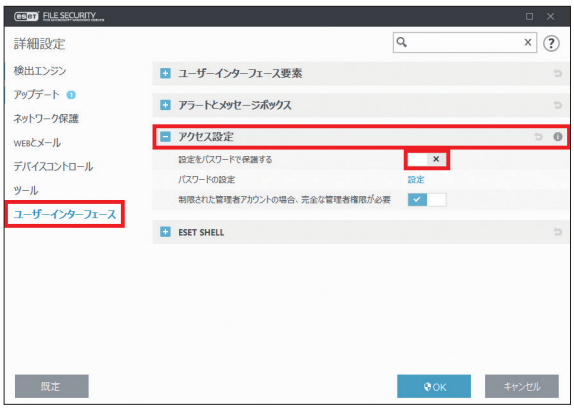
1 メインメニューの［設定］メニューから［詳細設定］をクリックします。



ワンポイント

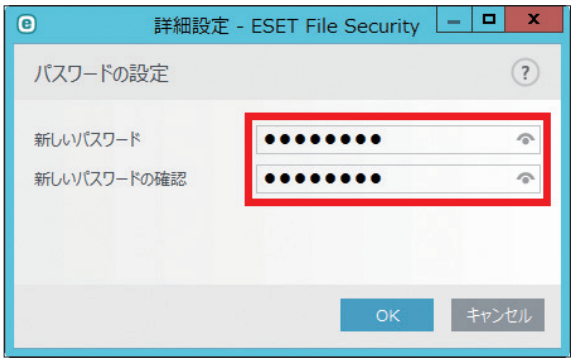
キーボードの【F5】キーを押して「詳細設定」画面を表示させることもできます。

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。



続く

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 File Security for Microsoft Windows Server の設定を変更する場合に必要になります。

3.6 ESET Security Management Center との接続

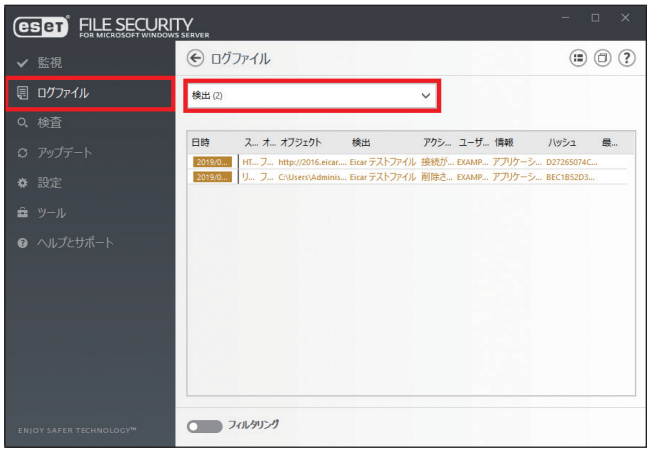
ESET Security Management Center はネットワーク環境にある ESET 製品を管理できるアプリケーションです。ESET Security Management Center は「ESET Management エージェント」経由で ESET File Security for Microsoft Windows Server との通信を行います。

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　エージェント展開処理」を参照してください。

Chapter 4 メインメニューの操作

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。ログに記録された情報は、ESET File Security for Microsoft Windows Server 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」画面を表示するには、メインメニューの［ログファイル］をクリックします。



ログファイルを表示するには、「ログファイル」画面のドロップダウンメニューから目的のログタイプを選択します。

使用可能なログタイプは次のとおりです。

検出	ESET File Security for Microsoft Windows Server 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。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が記録されます。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。
イベント	ESET File Security for Microsoft Windows Server によって実行されたすべての重要なアクションが記録されています。ESET File Security for Microsoft Windows Server 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。
コンピュータの検査	ESET File Security for Microsoft Windows Server 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。ログはコンピューター制御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。
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	ボットネット保護および IDS（ネットワーク攻撃保護）によってブロックされたファイルのレコードを表示します。
フィルタされた 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。
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。
OneDrive 検査	OneDrive 検査結果のリストを表示します。

「ログファイル」画面下部のフィルタリングスイッチをクリックすると、フィルタリング条件を定義することができる「ログのフィルタ」画面が表示されます。



ログのエントリーを右クリックすると、コンテキストメニューで次の項目を実行できます。

表示	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。

4.2 検査

「検査」はウイルス対策の重要な機能で、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。感染が疑われるときだけコンピューターを検査するのではなく、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。コンピューターの検査を実行すると、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、リアルタイムファイルシステム保護では検出されないウイルスを検出することができます。
「検査」画面を表示するには、メインメニューの［検査］をクリックします。



コンピューターの検査には次の 6 種類があります。

ストレージ検査	P38 参照
スマート検査	P38 参照
カスタム検査	P38 参照
リムーバブルメディア検査	P39 参照
前回の検査を再実行	P39 参照
Hyper-V 検査	P40 参照
OneDrive 検査	P42 参照

■ストレージ検査

共有フォルダーを検査します。サーバー上に共有フォルダがない場合は、ストレージ検査は行えません。

■スマート検査

スマート検査は、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。「スマート検査」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、「5.1.2 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。

■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。設定した検査パラメーターは、ユーザー定義の検査プロファイルに保存できます。検査プロファイルに保存しておくと、同じパラメーターで繰り返し検査を実行できます。
検査の対象を選択するには、メインメニューの［検査］＞［カスタム検査］をクリックして、「コンピューターの検査」画面を表示します。次に ⚙ 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プロファイルを選択するか、ツリー構造から検査対象をチェックします。対象にするフォルダーまたはファイルのパスを入力して、検査対象を指定す

ることもできます。駆除アクションを実行する必要がない場合は、⚙をクリックして、[駆除せずに検査する] をチェックします。
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。



■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、スマート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］をクリックしても実行できます。

■前回の検査を再実行

前回の検査と同じ設定（ストレージ、スマート、カスタムなど）で検査を再度実行します。

■ Hyper-V 検査

Microsoft Hyper-V Server 上の仮想マシン（VM）を検査できます。特定の仮想マシンに検査ソフトウェアをインストールする必要はありません。詳細については、「4.2.1 Hyper-V 検査」を参照してください。

!重 要

仮想マシンの検査は、少なくとも月に 1 回は実行することをお勧めします。Hyper-V 検査は、メインメニューの［ツール］＞［スケジューラ］から、スケジュールされたタスクとして設定することができます。

■ OneDrive 検査

OneDrive クラウドストレージにあるユーザーのファイルを検査できます。詳細については、「4.2.2 OneDrive 検査の設定」を参照してください。

4.2.1 Hyper-V 検査

Microsoft Hyper-V Server 上の仮想マシン（VM）を検査します。ウイルス対策は、Hyper-V サーバーに管理者権限を使ってインストールします。

Hyper-V 検査には、現在ブートセクターおよびオペレーティングメモリーの検査は実装されていません。

サポート対象のオペレーティングシステム

- Windows Server 2008 R2（オフライン時のみ検査可能）
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

ハードウェア要件

仮想マシンを実行するサーバーにパフォーマンスの問題が発生していないことを確認してください。
Hyper-V 検査はほとんど CPU のリソースのみを使用して行われますが、オンラインの仮想マシンの検査では十分な空きディスク領域が必要です。スナップショットと仮想ディスクで使用される領域の 2 倍以上の空き（使用可能）ディスク領域が必要になります。

固有の制限事項

- RAID ストレージ、スパンボリューム、および動的ディスクでの検査は、動的ディスクの性質によりサポートされていません。このため、可能なかぎり、VM で動的ディスクタイプを使用しないことをお勧めします。
- 検査は常に現在の VM で実行され、チェックポイントまたはスナップショットには影響しません。
- クラスタのホストで実行されている Hyper-V はサポートされていません。
- Windows Server 2008 R2 で実行されている Hyper-V ホストの仮想マシンは、ThreatSense パラメーター（駆除しない）で選択された駆除レベルに関係なく、読み取り専用モードでのみ検査できます。

! 重　要

ESET File Security for Microsoft Windows Server は、仮想ディスクの MBR の検査をサポートしますが、これらを対象とした読み取り専用検査のみがサポートされます。この設定は、[詳細設定]（F5）> 検出エンジン > [Hyper-V 検査] > [ThreatSense パラメーター] > [ブートセクター] で変更できます。

検査対象の仮想マシンがオフライン（オフに切り替え）

Hyper-V Management と仮想ディスクを使用し、仮想マシンの OS のディスクを検出して接続します。このように、汎用ハードドライブのファイルにアクセスする場合と同じディスクのコンテンツにアクセスできます。

検査対象の仮想マシンがオンライン（実行中、一時停止、保存済み）

Hyper-V Management と仮想ディスクを使用し、仮想マシンの OS のディスクを検出して接続します。現在ディスクへの汎用接続はできないため、仮想マシンのスナップショットを作成し、スナップショット経由で読み取り専用モードでディスクに接続します。スナップショットは検査の完了後に削除されます。
スナップショットの作成は、最大 1 分かかります。多数の仮想マシンを検査する場合は、スピードの問題も考慮してください。

ワンポイント

Hyper-V 検査は、オンラインとオフラインの仮想マシン用の読み取り専用検査です。

命名規則

Hyper-V 検査のファイル名は次の書式で付けられます。

```
VirtualMachineName\DiskX\VolumeY
```

X はディスク数、Y はボリューム数を示しています。

例：「Computer\Disk0\Volume1」

末尾の数字は、仮想マシンのディスクマネージャに表示される順序と同じ順番で付与されます。

この命名規則は、検査対象のリスト、進行状況バー、ログファイルで使用されます。

■検査の実行

次の 3 つの方法で検査は実行できます。

オンデマンド	ESET File Security for Microsoft Windows Server のメインメニュー［検査］＞［Hyper-V 検査］をクリックすると、検査対象の使用可能な仮想マシン（認識されている場合）のリストが表示されます。検査の対象は任意の仮想マシン、ディスクで、ディレクトリー、ファイルを選択することはできません。 検査可能なリストを表示するには、特定の仮想ディスクに接続する必要があり、表示に数秒かかる場合があります。
スケジューラ	詳細については、「4.5.8 スケジューラ」を参照してください。
ESET Security Management Center からサーバー検査のクライアントタスクを使用	ESET Security Management Center のサーバー検査クライアントタスクを使って実行します。

検査が完了すると、通知と［ログの表示］リンクが表示されます。リンクをクリックすると、実行された検査の詳細を表示できます。すべての検査が［ログファイル］セクションに表示されるため、Hyper-V 検査のログを表示するには、ドロップダウンメニューから「Hyper-V 検査」を選択します。

複数の Hyper-V 検査を同時に実行することができます。

考慮事項

- オンラインで仮想マシンの検査を実行する場合、検査対象の仮想マシンのスナップショットを作成する必要があります。スナップショットの作成中は、仮想マシンの一部の処理が制限または無効になる場合があります。
- オフラインで仮想マシンの検査を実行しているときは、検査が完了するまでオフにできません。
- Hyper-V Manager では、異なる仮想マシンに同じ名前を指定できます。この場合、検査ログを確認するときにクライアントコンピューターを識別できない場合があります。

4.2.2 OneDrive 検査の設定

OneDrive検査を使用すると、Microsoft OneDrive for Business クラウドストレージに保存されたファイルを検査できます。OneDrive 検査では、電子メール、SharePoint ファイル、連絡先、予定表などの他の種類のデータは検査されません。

OneDrive 検査を使用し始めるには、ESET OneDrive スキャナーを Microsoft OneDrive/Microsoft Office 365/Microsoft Azure に登録します。OneDrive 検査設定ページには、登録状況（既に登録されている場合）、登録詳細（テナント ID、アプリケーション ID、オブジェクト ID、および証明書サムプリント）が表示されます。

ESET OneDrive スキャナーの登録または登録解除は、[検査] > [OneDrive 検査] とクリックして「OneDrive 検査の設定」画面から行えます。登録を行う場合は、[登録] をクリックし、画面の指示に従って設定を行います。また、登録解除を行う場合は、[登録解除] をクリックします。



登録を行った場合は、フォルダー構造でユーザーと、検査対象として選択できるファイルの一覧を表示する検査メニューが表示され、OneDrive 検査を使用できるようになります。OneDrive 検査は、OneDrive for Business のユーザーによって並べ替えられた任意のファイルを検査できます。

! 重 要

OneDrive 検査は、OneDrive for Business クラウドストレージからファイルをダウンロードし、ローカルで検査を実行します。検査が完了すると、ダウンロードされたファイルは削除されます。OneDrive から大量のデータをダウンロードすると、ネットワークトラフィックに影響するので注意してください。

! 重 要

ESET OneDrive スキャナーを新しい Microsoft OneDrive for Business/Office 365 アカウントに登録する場合は、以前のアカウントで使用していた ESET OneDrive スキャナーを登録解除し、新しい Microsoft OneDrive for Business/Office 365 管理者アカウントで登録する必要があります。

ESET OneDrive スキャナーは、Office 365 および Azure でアプリケーションとして登録されます。

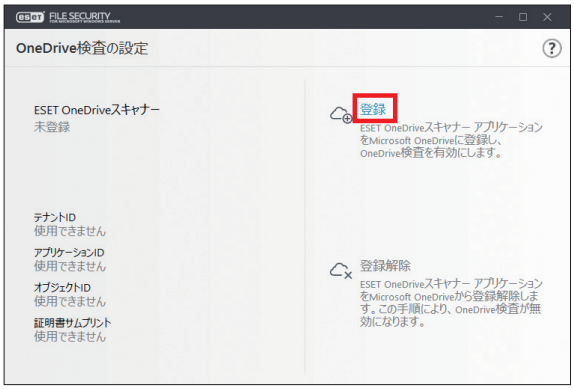
Office 365 ポータルの場合は、[マイアカウント] ページでアプリ権限をクリックすると、ESET OneDrive スキャナーが一覧表示されます。Azure の場合は、[Azure Active Directory] > [アプリの登録] に移動し、[すべてのアプリケーションを表示] をクリックすると、ESET OneDrive スキャナーが一覧に表示されます。アプリをクリックすると、詳細が表示されます。

4.2.2.1 ESET OneDrive スキャナーの登録

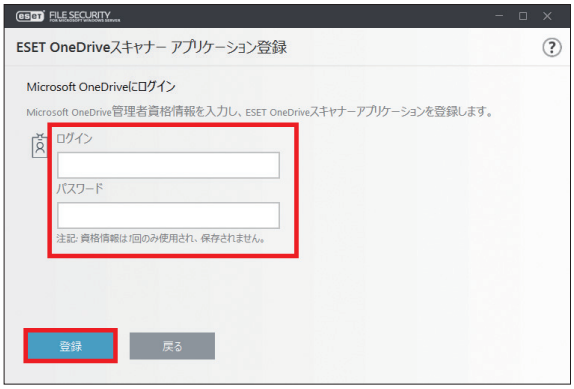
ESET OneDrive スキャナーを Microsoft OneDrive/Office 365/Azure に登録するには、以下の手順で行います。

操作手順

1. ［検査］>［OneDrive 検査］をクリックします。
2. ［登録］をクリックします。



3. Microsoft OneDrive/Office 365 管理者アカウント資格情報を入力します。ログインにユーザー名を入力し、パスワードを入力して、［登録］をクリックします。Microsoft OneDrive へのアプリケーション登録が完了するまで待機します。



4. ESET OneDrive スキャナーでは、許可メッセージに一覧表示される 4 種類の権限が必要です。［許可］をクリックすると、ESET File Security OneDrive スキャナーは、OneDrive クラウドストレージにあるデータにアクセスできます。
5. Web ブラウザーでこの情報を送信するように指示された場合は、［続行］をクリックします。
6. Web ブラウザーを閉じると、ESET OneDrive スキャナー登録ウィザードで、登録が成功しましたというメッセージが表示されます。［完了］をクリックします。

! 重 要

ESET OneDrive スキャナー登録処理は、Microsoft のポータル（OneDrive、Office 365、Azure など）にログインしているかによって、特定の状況で異なる場合があります。登録ウィザードウィンドウの画面の指示およびメッセージに従ってください。

ESET OneDrive スキャナー登録中にエラーメッセージが表示される場合は、以下を参照してください。

エラーメッセージ	エラーメッセージ詳細
予期しないエラーが発生しました。	ESET File Security for Microsoft Windows Server で問題が発生した可能性があります。しばらくたってから ESET OneDrive スキャナー登録を再試行してください。問題が解決しない場合は、サポートセンターに連絡してください。
Microsoft OneDrive に接続できませんでした。	ネットワーク / インターネット接続を確認し、ESET OneDrive スキャナー登録を再実行してください。
Microsoft OneDrive で予期しないエラーが発生しました。	HTTP 4xx エラーが返され、エラーメッセージ応答に応答がありません。この問題が解決しない場合は、サポートセンターに連絡してください。
Microsoft OneDrive で次のエラーが発生しました。	Microsoft OneDrive サーバーは、特定のエラーコード / 名前のエラーを返しました。エラーを表示をクリックしてください。
セットアップタスクはタイムアウトしました。	ESET OneDrive スキャナー登録設定タスクに時間がかかりすぎています。しばらくたってから ESET OneDrive スキャナー登録を再試行してください。
セットアップタスクはキャンセルされました。	実行中の登録タスクをキャンセルしました。登録を完了する場合は、ESET OneDrive スキャナー登録を再試行してください。
別のセットアップタスクがすでに実行中です。	登録タスクは既に実行中です。最初の登録処理が完了するまでお待ちください。

4.2.2.2 ESET OneDrive スキャナーの登録解除

ESET OneDrive スキャナーの登録解除処理では、Microsoft OneDrive/Office 365/Azure から証明書と ESET OneDrive スキャナーを削除します。この処理では、ローカル依存関係を削除し、登録オプションをもう一度使用可能にします。

操作手順

1. ［検査］>［OneDrive 検査］をクリックし、［登録解除］をクリックして、ESET OneDrive スキャナー登録解除 / 削除処理を開始します。登録解除ウィザードが開きます。
2. ［登録解除］をクリックし、Microsoft OneDrive からの登録解除が完了するまで待機します。
3. 登録解除処理が正常に完了した場合は、登録解除ウィザードで該当するメッセージが表示されます。

一部のエラーメッセージでは、ローカル依存関係（接続の問題、Microsoft OneDrive に存在しないアプリなど）を削除するオプションがあります。ESET OneDrive スキャナーをローカルで削除するには、次の手順を実行します。

操作手順

1. 再試行ボタンが動作せず、問題が解決しない場合は、ローカルで［削除］をクリックし、ESET OneDrive スキャナーローカル依存関係を削除する登録解除処理を進めます。
2. ダイアログボックスが表示されたら、［はい］をクリックして、ESET OneDrive スキャナーのローカル削除を続行します。ESET OneDrive 検査は使用できなくなります。再登録を実行する必要があります。

! 重　要

ローカル依存関係を削除しても、Azure ポータルでのアプリ登録は変更されず、Office 365 ポータルでのアプリ権限も変更されません。Microsoft OneDrive サーバーとのネットワークまたは接続の問題のため、ESET OneDrive スキャナーをローカルで削除した場合は、手動で Azure のアプリ登録から ESET OneDrive スキャナーを削除する必要があります。

登録解除失敗などのエラーメッセージが表示される場合は、Microsoft OneDrive サーバーとの一般的なネットワークまたはインターネット接続の問題や、ESET OneDrive スキャナーが Microsoft OneDrive に登録されていないなど、さまざまな理由が考えられます。エラーメッセージの一覧と対処方法については、以下の表を参照してください。

エラーメッセージ	エラーメッセージ詳細
Azure アプリケーションへの接続が失敗しました。インターネット接続がありません。	ネットワーク / インターネット接続を確認し、もう一度登録解除を実行します。Microsoft OneDrive からの ESET OneDrive スキャナーの削除を行わず、登録解除処理を続行する場合は、ローカルで削除をクリックします。
アクセストークンを取得できませんでした。Microsoft OneDrive で予期しないエラーが発生しました。	ESET OneDrive スキャナーが Microsoft OneDrive に登録されていない可能性があります。ESET OneDrive スキャナーは、Azure ポータルで手動で削除された可能性があります。ESET OneDrive スキャナーが Microsoft OneDrive または Azure ポータルにあることを確認してください。ESET OneDrive スキャナーが一覧にない場合は、ローカルで削除をクリックして、登録解除処理を続行します。
アクセストークンを取得できませんでした。Microsoft OneDrive でサーバーエラーが発生しました。	Microsoft OneDrive は HTTP 5xx エラーを返しました。現在、登録解除タスクを完了できません。しばらくたってから登録解除を再試行してください。
Microsoft OneDrive で次のエラーが発生しました。	Microsoft OneDrive サーバーは、特定のエラーコード / 名前のエラーを返しました。エラーを表示をクリックしてください。
別のセットアップタスクがすでに実行中です。	登録解除タスクは既に実行中です。最初の登録解除処理が完了するまでお待ちください。

4.2.3 検査ウィンドウと検査ログ

検査ウィンドウは、検査の場所、見つかった脅威数（該当する場合）、検査済みオブジェクト数、検査時間を含む、現在検査されているオブジェクトを示します。検査ウィンドウは、以下の手順で表示できます。

操作手順

1. 検査中に［検査ウィンドウを開く］をクリックします。



2. 検査ウィンドウが表示されます。



ワンポイント

検査を一時的に中断する場合は、一時停止をクリックします。再開オプションは、検査が一時停止しているときに使用できます。

3. 検査が完了すると、検査ログが表示されます。



●ログをフィルタリングする

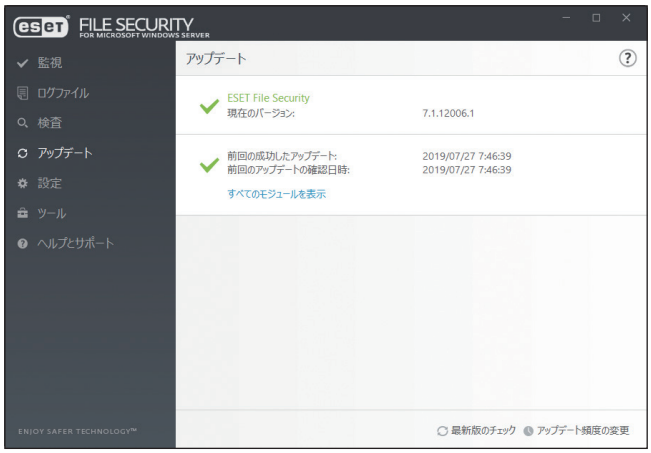
検査ウィンドウの フィルタリングをクリックすると、ログフィルタリングウィンドウが開き、フィルタリングまたは検索条件を定義できます。また、ログエントリを右クリックすると、コンテキストメニューが表示され、以下の操作を行えます。ログフィルタリングウィンドウの詳細については、「4.1 ログファイル」を参照してください。

アクション	使用方法
同じレコードのフィルタリング	これは、選択したものと同じタイプのレコードのみを表示する、ログフィルタリングをアクティブ化します。
フィルタ ...	このオプションをクリックすると、ログのフィルタリングウィンドウが表示され、特定のログエントリのフィルタ条件を定義することができます。
フィルタを有効にする	フィルタ設定を有効にします。最初にフィルタリングをアクティブ化するときには、設定を定義する必要があります。
フィルタを無効にする	フィルタリングをオフにします（下にあるスイッチのクリックと同じ）。
コピー	選択 / 強調表示されたレコードに関する情報をクリップボードにコピーします。
すべてコピー	ウィンドウにあるすべてのレコードに関する情報をコピーします。
エクスポート ...	選択 / 強調表示されたレコードに関する情報を XML ファイルにエクスポートします。
すべてエクスポート ...	ウィンドウのすべての情報を XML ファイルにエクスポートします。

4.3 アップデート

セキュリティを高めるには、ESET File Security for Microsoft Windows Server を定期的にアップデートするのが最善の方法です。ESET File Security for Microsoft Windows Server は検出エンジンで常に最新の状態を保つことができます。「アップデート」画面を表示するには、メインメニューの［アップデート］をクリックします。

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。アップデートの間隔を変更するには、［アップデート頻度の変更］をクリックするか、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、「4.5.8 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 File Security for Microsoft Windows Server 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。
5	**アップデート頻度の変更**	スケジューラータスク定期自動アップデートのタスクのタイミングを編集できます。詳細は、「4.5.8 スケジューラ」を参照してください。

! 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 File Security for Microsoft Windows Server 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。

4.3.1 アップデートプロセス

［今すぐアップデート］をクリックすると、アップデートファイルのダウンロードが開始され、アップデートの進行状況が表示されます。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。



●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 - サーバが見つかりません。」
  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。

4.3.2 アップデートのためのプロキシサーバーの構成

インターネット接続にプロキシサーバーを使用している場合は、ESET File Security for Microsoft Windows Server にプロキシサーバーを設定する必要があります。プロキシサーバーの構成について詳しくは、「5.1.8 アップデート」の「プロキシサーバ」を参照してください。

4.4 設定

ESET File Security for Microsoft Windows Server の動作を細かく設定することができます。



設定オプションは次の 5 つの項目で構成されています。

- サーバー
- コンピューター
- ネットワーク
- Web とメール
- ツール

各項目をクリックすると、対応する保護機能の詳細を設定できます。

設定オプションの操作方法

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。

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。

4.4.1 サーバー

サーバーの設定では、自動除外とクラスタ機能の設定を行うことができます。これらの機能により、サーバーのパフォーマンスを維持したり、ESET 製品同士の通信を設定したりすることができます。

「サーバー」画面を表示するには、メインメニューの［設定］＞［サーバー］をクリックします。

各機能は、スイッチ を使用して有効／無効を切り替えます。特定の項目の設定を編集するには、歯車 をクリックします。



設定の「サーバー」画面では、次の内容が表示されます。

自動除外	重要なサーバーアプリケーションとサーバーのオペレーティングシステムファイルを識別し、自動的に除外リストに追加します。これにより、ウイルス対策ソフトウェアを実行する際に潜在する競合のリスクが最小化され、サーバーの全体的なパフォーマンスが向上します。
クラスタ	クラスタを設定するには、［クラスタウィザード］のリンクをクリックします。クラスタを設定する方法の詳細については、「5.1.22　クラスタ」の「●クラスタウィザード」を参照してください。
OneDrive 検査の設定	ESET OneDrive スキャナーを Microsoft OneDrive に登録 / 登録解除できます。

4.4.2 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。

4.4.3 ネットワーク



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。

■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

ネットワーク攻撃保護（IDS）やボットネット保護が原因となっている接続の問題を解決できます。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。

4.4.4 Web とメール



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。
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。

4.4.5 ツール

ツールの設定では、診断ロギング機能の設定を行います。
診断ロギングでは、診断ログに書き込むコンポーネントを構成します。「ツール」画面表示するには、メインメニューの［設定］＞［ツール］をクリックします。スイッチ を使用して機能を有効／無効に切り替えます。特定の項目の設定を編集するには、歯車 をクリックします。



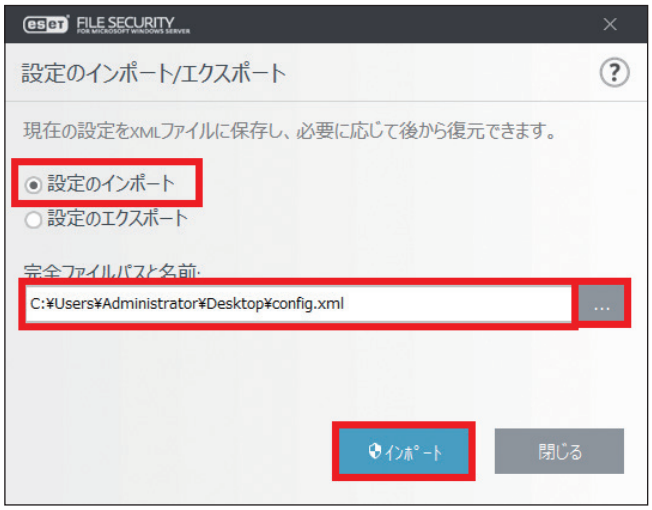
診断ロギングー診断ログに書き込むコンポーネントを構成します。診断ロギングを有効にすると、ログが有効になる時間（10 分有効化、30 分有効化、1 時間有効化、4 時間有効化、24 時間有効化、再起動まで有効化、永久に有効化）を選択できます。このタブに表示されないコンポーネントは常に診断ログに書き込まれます。
詳細設定については、「5.1.17　ログファイル」の「■ロギングフィルター」を参照してください。

4.4.6 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 File Security for Microsoft Windows Server 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。

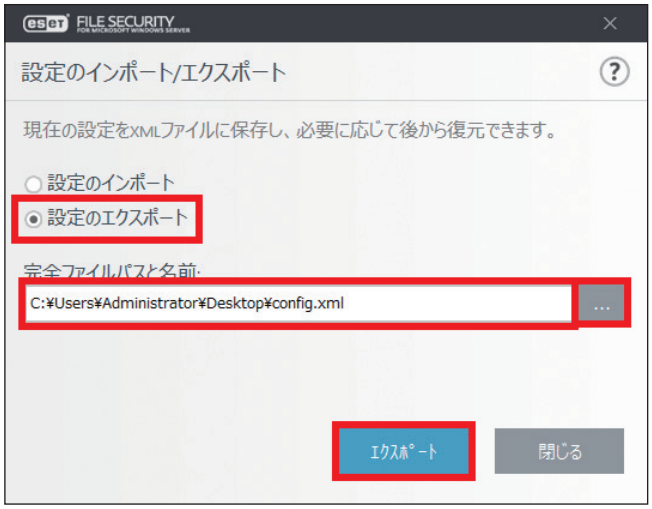
■設定のインポート

「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［OK］をクリックし、［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、［OK］をクリックし、［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。

4.5 ツール

ツールには、ESET File Security for Microsoft Windows Server 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。
「ツール」画面を表示するには、メインメニューの［ツール］をクリックします。

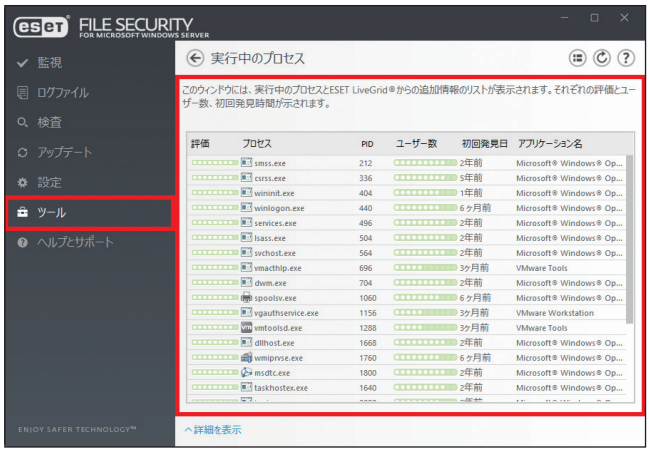


ツールには次の機能が含まれています。
「ツール」画面では次の項目が設定できます。

実行中のプロセス	実行中のプロセスが ESET LiveGrid からの情報とともに表示されます。	P58 参照
アクティビティの確認	ファイルシステムの活動をグラフ表示で確認できます。	P60 参照
保護統計	ウイルスおよびスパイウエア対策の保護統計を表示します。	P61 参照
クラスタ	クラスタ機能の状態が表示されます。	P62 参照
ESET Shell	コマンドラインインターフェースを起動します。	P62 参照
ESET SysInspector	システムの詳細情報を収集します。	P73 参照
ESET SysRescue Live	マルウェアの駆除ツールです。	P90 参照
スケジューラ	タスクの追加、編集やスケジュール管理などを行います。	P91 参照
分析のためにサンプルを提出	不審なファイルやサイトの情報を ESET に提出して分析できます。	P98 参照
隔離	安全に隔離された感染ファイルの詳細の確認や復元などを行います。	P99 参照

4.5.1 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 File Security for Microsoft Windows Server 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」画面を表示するには、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。



画面に表示される内容は次のとおりです。

評価	ESET File Security for Microsoft Windows Server 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）に危険レベルを割り当てます。危険レベルには「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

「危険レベル」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

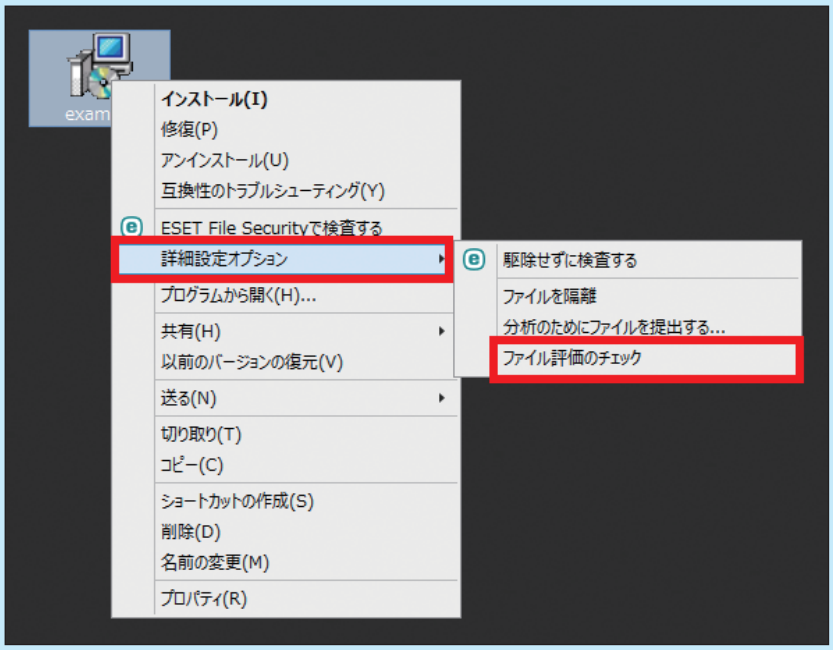
「危険レベル」に「緑」（良）のマークが付いたアプリケーションは、感染していないことが判明しており（ホワイトリストに記載）、検査から除外されます。検査から除外するのは、「コンピュータの検査」または「リアルタイムファイルシステム保護」の検査速度を向上させるための仕組みです。

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。

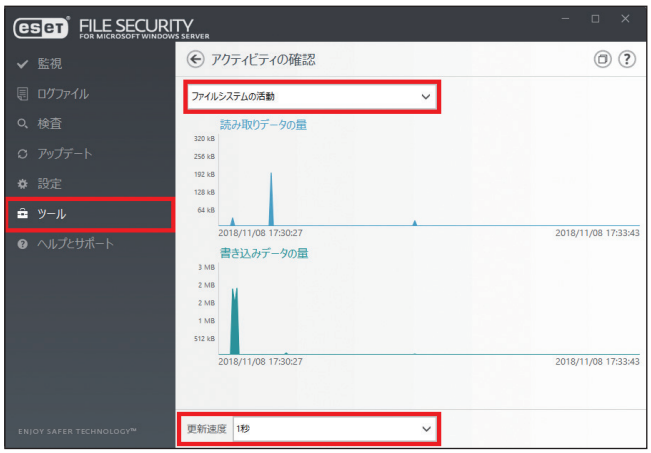
ワンポイント

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。



4.5.2 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。



グラフは読み取りデータ量（青）と書き込みデータ量（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。

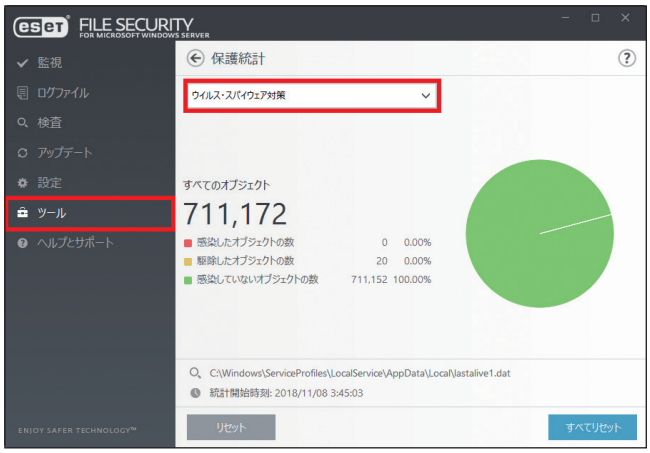
1 秒	グラフは 1 秒おきに更新され、直近 10 分間のアクティビティが表示されます。
1 分（直前の 24 時間）	グラフは 1 分おきに更新され、直近 24 時間のアクティビティが表示されます。
1 時間（先月）	グラフは 1 時間おきに更新され、直近 1 カ月間のアクティビティが表示されます。
1 時間（選択した月）	グラフは 1 時間おきに更新され、選択した月のアクティビティが表示されます

ファイルシステムの活動
このグラフの縦軸は、読み込みデータ（青）と書き込みデータ（赤）の量を KB（キロバイト）／MB（メガバイト）／GB（ギガバイト）で表示します。

4.5.3 保護統計

保護統計では、ESET File Security for Microsoft Windows Server の保護機能に関連する統計データをグラフで確認できます。

保護統計を表示するには、メインメニューの［ツール］＞［保護統計］をクリックします。



ドロップダウンメニューから統計を表示する保護機能を選択すると、選択した保護機能のグラフと凡例が表示されます。凡例の項目にカーソルを合わせると、その項目のデータのみがグラフに表示されます。

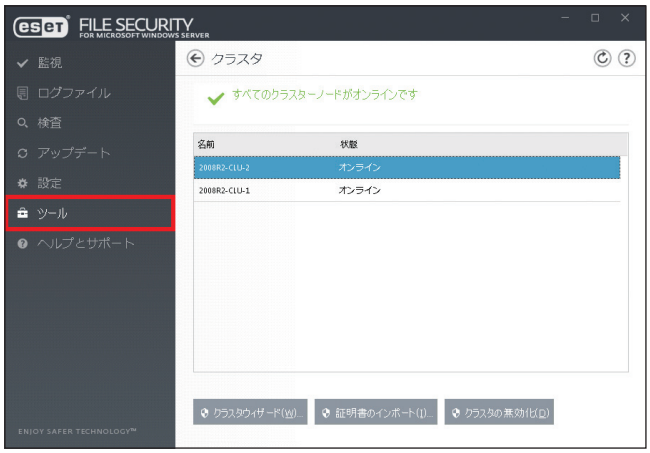
表示可能な統計グラフは次のとおりです。

ウイルス・スパイウェア対策	感染オブジェクトおよび駆除済みオブジェクトの数を表示します。
ファイルシステム保護	読み込まれたオブジェクト、またはファイルシステムに書き込まれたオブジェクトを表示します。
電子メールクライアント保護	電子メールクライアントが送信または受信したオブジェクトを表示します。
Web アクセスとフィッシング対策	Web ブラウザーによってダウンロードされたオブジェクトを表示します。

統計グラフの横には、検査済みオブジェクト数、感染オブジェクト数、駆除済みオブジェクト数、未感染のオブジェクト数が表示されます。［リセット］をクリックすると、表示中の保護機能の統計情報が削除されます。［すべてリセット］をクリックすると、すべての保護機能の統計情報が削除されます。

4.5.4 クラスタ

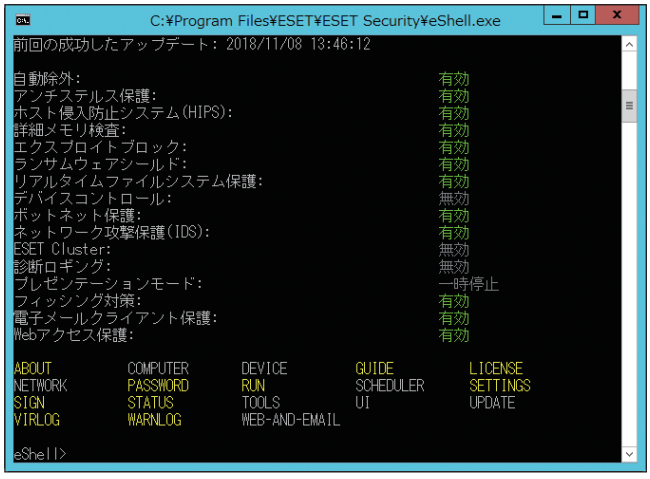
クラスタ（ESET Cluster）を活用すると、ESET サーバー製品が相互に通信し、構成や通知などのデータを交換できます。また、製品インスタンスのグループが正しく動作するために必要なデータを同期することもできます。
「クラスタ」画面を表示するには、メインメニューの［ツール］＞［クラスタ］をクリックします。



クラスタの詳細については、「5.1.22 クラスタ」を参照してください。

4.5.5 ESET Shell

ESET Shell は、ESET File Security for Microsoft Windows Server のコマンドラインインターフェースです。グラフィカルユーザーインターフェース（GUI）の代わりに、プログラム全体の設定と管理を行うことができます。ESET Shell では、GUI に備わっているほぼすべての機能とオプションを使用できます。
GUI で使用可能な機能のほかに、スクリプトを実行して、設定や設定の変更、またはアクションの実行を自動化することもできます。ESET Shell は、GUI よりもコマンドラインのほうが使いやすいユーザーにとっては便利です。
「ESET Shell」画面を表示するには、メインメニューの［ツール］＞［ESET Shell］をクリックします。



● ESET Shell のモードについて

ESET Shell には、対話モードと単一コマンド／バッチモードの 2 つのモードがあります。

- 対話モードは、コマンドを実行するだけでなく、設定の変更や、ログの表示などのタスクで ESET Shell を操作する場合に使用できます。また、ESET Shell が検索しやすくなり、特定のコンテキストで使用できる、有効なコマンドも表示されます。
- 単一コマンド／バッチモードは、対話モードで使用されていないコマンドのみを実行する必要がある場合に使用できます。この操作を実行するには、Windows のコマンドプロンプトで適切なパラメーターを指定して、eshell と入力します。

例：

```
eshell get status
```

または

```
eshell set antivirus status disabled
```

バッチ／スクリプトモードで特定のコマンド（上記の 2 番目の例）を実行するには、事前にいくつかの設定を構成する必要があります。構成されていない場合は、「アクセスが拒否されました」というメッセージが表示されます。

! 重　要

- すべての機能を使用するためには、管理者として ESET Shell を実行してください。Windows のコマンドプロンプトを使用して単一のコマンドを実行するときも同様に、コマンドプロンプトを管理者として実行してください。そうでない場合は、一部のコマンドを実行できません。
- Windows のコマンドプロンプトから eShell コマンド、またはバッチファイルを実行するには、設定を行う必要があります。バッチファイルの実行の詳細については、「■バッチファイル／スクリプト」を参照してください。

●対話モード

対話モードは、次の 2 つの方法を使用して開始できます。

- Windows の［スタート］メニューから［スタート］＞［すべてのプログラム］＞［ESET］＞［ESET File Security］＞［ESET Shell］を選択します。
- Windows のコマンドプロンプトで、eshell と入力して、【Enter】キーを押す。
  ※ ESET Shell の初回起動時には、初期画面（ガイド）が表示されます。

ワンポイント

初期画面を再度表示するには、guide コマンドを入力します。この画面には、ESET Shell の基本的な使用例と、構文、プレフィックス、コマンドパス、省略形、エイリアスなどが表示されます。

次回 ESET Shell を実行すると、次の画面が表示されます。



!重 要

コマンドには、大文字と小文字のいずれも使用でき、区別されずに実行されます。

●カスタマイズ

ESET Shell は ui eshell コンテキストでカスタマイズできます。スクリプトのエイリアス、色、言語、実行ポリシーを構成したり、非表示のコマンドと一部の他の設定を表示させることもできます。

■使い方

構文

コマンドはプレフィックス、コンテキスト、引数、オプションなどで構成されています。下記に ESET Shell で使用する一般的な構文を示します。

```
[<prefix>] [<command path>] <command> [<arguments>]
```

例（ドキュメント保護の有効化）：

```
SET ANTIVIRUS DOCUMENT STATUS ENABLED
```

SET ープレフィックス
ANTIVIRUS DOCUMENT ー特定のコマンドのパス（コンテキスト）
STATUS ーコマンド本体
ENABLED ーコマンドのパラメーター

コマンドと「?」を引数として使用すると、その特定のコマンドの構文が表示されます。例えば、STATUS ? と入力すると STATUS コマンドの構文が表示されます。

構文：

```
[get] | status
set status enabled | disabled
```

[get] は、[ ]（角括弧）で囲まれています。これは、プレフィックス GET が status コマンドの既定値であることを示しています。プレフィックスを指定しないで status を実行した場合は、既定のプレフィックス（この例では、get status）が使用されます。これによりコマンド入力が簡略化できます。GET はほとんどのコマンドの既定のプレフィックスですが、個々のコマンドの既定のプレフィックスについて、あらかじめ確認してください。

! 重 要

コマンドには、大文字と小文字のいずれも使用でき、区別されずに実行されます。

プレフィックス／操作

プレフィックスは一つの操作を表します。例えば、GET プレフィックスは、ESET File Security for Microsoft Windows Server の特定の機能の設定内容が表示されるか、状態が表示されます（例えば、GET ANTIVIRUS STATUS は、現在の保護の状態を表示します）。SET プレフィックスは、機能を設定するか状態を変更します（例えば、SET ANTIVIRUS STATUS ENABLED は、保護を有効にします）。

使用できるプレフィックスを次に示します（特定のコマンドがすべてのプレフィックスをサポートしているわけではありません）。

GET	現在の設定／状態を表示する
SET	値／状態を設定する
SELECT	項目を選択する
ADD	項目を追加する
REMOVE	項目を削除する
CLEAR	すべてのアイテム／ファイルを削除する
START	アクションを開始する
STOP	アクションを停止する
PAUSE	アクションを中断する
RESUME	アクションを再開する
RESTORE	既定の設定／オブジェクト／ファイルを復元する
SEND	オブジェクト／ファイルを送信する
IMPORT	ファイルからインポートする
EXPORT	ファイルにエクスポートする

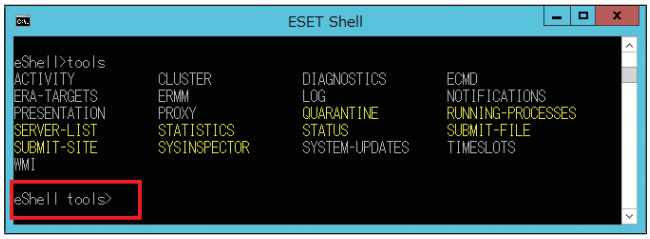
プレフィックス GET と SET は多くのコマンドでサポートされますが、EXIT などプレフィックスを使用しないコマンドもあります。

コマンドパス／コンテキスト

コマンドは、ツリー構造のコンテキスト内で使用されます。ツリーの最上位はルートです。実行すると、ルートレベルが表示されます。

```
eShell>
```

そのままコマンドを実行するか、コンテキスト名を入力してツリー内を移動することもできます。例えば、TOOLS コンテキストを開始すると、このコンテキストで使用できるすべてのコマンドとサブコンテキストが表示されます。



黄色で示された項目は実行可能なコマンド、灰色で示された項目は開始できるサブコンテキストです。サブコンテキストには、コマンドがさらに含まれています。
上の階層に戻る必要がある場合は、「..」（ドット 2 個）を使用します。例えば、現在のコンテキストが

```
eShell antivirus startup>
```

の場合、「..」（ドット 2 個）を入力すると、1 階層上がって、次の階層になります。

```
eShell antivirus>
```

現在のレベル eShell antivirus startup>（ルートから 2 階層下）からルートに戻るには、そのまま、「.. ..」（ドット 2 個とドット 2 個をスペースで区切る）と入力します。このように入力すると、2 階層上、この場合はルートに移動します。「\」（バックスラッシュ）を使用すると、現在のコンテキストツリー内の階層に関係なく、直接ルートに戻ることができます。上位階層の特定のコンテキストに移動する場合は、該当する数の「..」（ドット 2 個）を使用して、対応する階層に移動します。ただし、区切り文字としてスペースを使用します。例えば、3 階層上に移動する場合は、次のように入力します。「.. .. ..」（ドット 2 個をスペースで区切って 3 回繰り返す）
パスは、現在のコンテキストからの相対パスです。現在のコンテキストに含まれているコマンドの場合は、パスを入力しません。例えば、GET ANTIVIRUS STATUS を実行するには、次のように入力します。

GET ANTIVIRUS STATUS ールートコンテキスト（コマンドラインは `eShell>`）
GET STATUS ーコンテキスト ANTIVIRUS（コマンドラインは `eShell antivirus>`）
.. GET STATUS ーコンテキスト ANTIVIRUS STARTUP
（コマンドラインは `eShell antivirus startup>`）

! 重　要

「..」（ドット 2 個）を 1 個の「.」（ドット）で代替することができますが、「.」（ドット 1 個）を使用するときは、「..」（ドット 2 個）を混ぜて使用することはできません。

例：
. GET STATUS ーコンテキスト ANTIVIRUS STARTUP
（コマンドラインは `eShell antivirus startup>`）

パラメーター

コマンドに対して実行するアクションです。例えば、コマンド CLEAN-LEVEL（ANTIVIRUS REALTIME ENGINE にあります）では次のパラメーターを使用できます。

none	駆除なし
normal	標準的な駆除
strict	厳密な駆除

パラメーターには、他に ENABLED や DISABLED などがあります。これらのパラメーターは、特定の機能を有効または無効にする場合に使用します。

省略形／簡略化されたコマンド

コンテキスト、コマンド、およびパラメーターを簡略化することができます（パラメーターはスイッチまたは代替オプションの場合に限ります）。ただし、数値、名前、パスなどの具体的な値を持つパラメーターやプレフィックスは簡略化できません。

簡略化の例：

```
set status enabled => set stat en
add antivirus common scanner-excludes C:\path\file.ext => add ant com scan C:\path\file.ext
```

例えば、ABOUT と ANTIVIRUS のように 2 つのコマンドまたはコンテキストが同じ文字で開始されている場合、簡略化したコマンドとして、A を入力しても、この 2 つのコマンドのどちらを実行するのかを特定できません。エラーメッセージと「A」で始まるコマンドの一覧が表示されます。この一覧からコマンドを選択できます。

```
eShell>a
```

次のコマンドが一意ではありません：a

このコンテキストでは次のコマンドを使用できます。

```
ABOUT          プログラムに関する情報を表示する
ANTIVIRUS      コンテキストウイルス対策に変更する
```

次に 1 文字以上追加（例えば、AB）すれば、コマンドが限定され、ABOUT コマンドを実行します。

! 重　要

コマンドを確実に実行するには、コマンドやパラメーターを省略形にせず、完全な形式で入力してください。バッチファイル／スクリプトでは特に注意してください。

自動入力

Windows コマンドプロンプトの自動入力と似た機能です。Windows コマンドプロンプトではファイルパスが入力されますが、コマンド、コンテキスト、および処理名も入力されます。ただし、パラメーターの入力はサポートされていません。コマンドを入力するときには、【Tab】キーを押して、使用可能なコマンドを入力するか、次の使用可能なコマンド候補を表示します。【Shift】キー＋【Tab】キーを押すと、前のコマンドに戻ります。省略形と自動入力を併用することはできません。例えば、antivir real scan と入力して、【Tab】キーを押しても、何も表示されません。代わりに、antivir と入力してから、【Tab】キーを押し、antivirus と入力して、real と入力して【Tab】キーを押し、scan と入力して【Tab】キーを押します。
scan-create、scan-execute、scan-open などのすべての使用可能なコマンド候補が表示されます。

エイリアス

エイリアスは、コマンドの実行に使用できる代替名です（コマンドにエイリアスが割り当てられている場合）。既定のエイリアスとして、次のものがあります。

- （グローバル）close - exit
- （グローバル）quit - exit
- （グローバル）bye - exit
- warnlog - tools log events
- virlog - tools log detections
- antivirus on-demand log - tools log scans

「（グローバル）」は、現在のコンテキストと関係なく、任意の場所でそのコマンドを使用できることを示しています。また、1 つのコマンドにエイリアスが複数割り当てられている場合があります。例えば、コマンド EXIT には、下記のエイリアスがあります。

- CLOSE
- QUIT
- BYE

ESET Shell を終了する場合は、EXIT コマンドを使用するか、そのエイリアスを使用することもできます。エイリアス VIRLOG は、コマンド DETECTIONS のエイリアスであり、このコマンドは、TOOLS LOG コンテキストにあります。この方法により、DETECTIONS コマンドは、ROOT コンテキストから使用可能になります。TOOLS コンテキスト、LOG コンテキストの順に開始する必要はなく、ROOT から直接実行できるようになります。
独自のエイリアスを定義できます。コマンド ALIAS は UI ESHELL コンテキストにあります。

パスワードで保護された設定

ESET File Security for Microsoft Windows Server の設定はパスワードで保護できます。GUI を使用するか、ESET Shell で set ui access lock-password コマンドを使用して、パスワードを設定します。この後、特定のコマンド（設定またはデータを変更するコマンドなど）でパスワードを対話モードで入力します。パスワードを繰り返し入力したくない場合は、set password コマンドを使用して、パスワードを記憶できます。これにより、パスワードが必要なコマンドを実行するたびに、パスワードが自動的に入力されます。パスワードは ESET Shell を終了するまで記憶されます。

Guide/Help
コマンド GUIDE または HELP を入力すると、ESET Shell の使用方法を説明する画面が表示されます。このコマンドは、ROOT コンテキストから使用できます。

コマンド履歴
以前実行したコマンドの履歴が保存されています。保存された履歴は、現在の対話セッションにのみ適用されます。ESET Shell を終了すると、コマンド履歴は削除されます。履歴内の移動には、キーボードの上矢印キーと下矢印キーを使用します。目的のコマンドが見つかった場合は、それを再度実行するか、入力を修正して実行することができます。

CLS ／画面の消去
CLS コマンドを使用すると画面を消去することができます。

EXIT/CLOSE/QUIT/BYE
ESET Shell を閉じる（終了する）場合に、このコマンドを使用します。

■コマンド

基本的なコマンドについて説明します。

! 重　要
コマンドには、大文字と小文字のいずれも使用でき、区別されずに実行されます。

ROOT コンテキストに用意されているコマンドの例：

ABOUT
プログラム情報が表示されます。インストールされている製品の名前、バージョン番号、インストールされているコンポーネント（各コンポーネントのバージョン番号を含む）、および ESET File Security for Microsoft Windows Server がインストールされているサーバーとオペレーティングシステムの基本情報が表示されます。

コンテキストパス：
`root`

PASSWORD
パスワード保護されたコマンドを実行する場合、パスワードの入力が要求されます。これは、ウイルス対策保護を無効にするコマンドや、ESET File Security for Microsoft Windows Server の機能に影響する可能性のあるコマンドを実行する場合に発生します。これらのコマンドは、実行ごとにパスワードが要求されます。あらかじめパスワードを設定しておくことで、次回からのパスワード入力を省略することができます。こうすることにより、パスワードで保護されたコマンドを実行したときに、セットされたパスワードが自動的に使用されるためパスワードを毎回入力する必要がなくなります。

! 重　要
セットしたパスワードは、現在の対話セッションでのみ有効です。ESET Shell を終了するとパスワードは削除されます。再度開始した場合は、パスワードを再度セットする必要があります。

パスワードのセットは、バッチファイル／スクリプトを実行する際にも役立ちます。パスワードのセットを含むバッチファイルの例を示します。

```
eshell start batch "&" set password plain <yourpassword> "&" set status disabled
```

この連結コマンドは、バッチモードを開始し、使用するパスワードを定義してパスワード保護を無効にします。

コンテキストパス：

```
root
```

構文：

```
[get] | restore password
set password [plain <password>]
```

操作：

get ーパスワードを表示する
set ーパスワードを設定または削除する
restore ーパスワードをクリアする

パラメーター：

plain ーパラメーターとしてパスワードを入力する方式に切り替える
password ーパスワード

例：

set password plain <yourpassword> ーパスワードで保護されたコマンドに使用するパスワードを設定する
restore password ーパスワードをクリアする

例：

get password ーパスワードが設定されているかどうかを確認する場合に使用します（「*」（アスタリスク）が表示され、パスワード自体は表示されません）。「*」（アスタリスク）が表示されない場合は、パスワードは設定されていません。
set password plain <yourpassword> ー定義したパスワードを設定する
restore password ー定義したパスワードをクリアする

STATUS
GUI と同様に現在の ESET File Security for Microsoft Windows Server の保護状態の情報を表示します。

コンテキストパス：
`root`

構文：
`[get] | restore status`
`set status disabled | enabled`

操作：
get ーウイルス・スパイウェア対策のステータスを表示する
set ーウイルス・スパイウェア対策を無効／有効にする
restore ー既定の設定／オブジェクト／ファイルを復元する

パラメーター：
disabled ーウイルス対策保護を無効にする
enabled ーウイルス対策保護を有効にする

例：
get status ー現在の保護の状態を表示する
set status disabled ー保護を無効にする
restore status ー保護を既定の設定（有効）に戻す

VIRLOG
DETECTIONS コマンドのエイリアスです。検出された脅威に関する情報を表示します。

WARNLOG
EVENTS コマンドのエイリアスです。様々なイベントに関する情報を表示します。

■バッチファイル／スクリプト

ESET Shell は自動化用の強力なスクリプトツールとして使用できます。バッチファイルを使用するには、バッチファイルを作成し、eShell とコマンドを記述します。

例：
```
eshell get antivirus status
```

コマンドは連結することができます。例えば、特定のスケジュールタスクのタイプを取得する場合は、次のように入力します。

```
eshell select scheduler task 4 "&" get scheduler action
```

通常、項目の選択（この場合はタスク番号 4）は、現在実行中の ESET Shell のインスタンスにのみ適用されます。これら 2 つのコマンドを順番に実行した場合、2 番目のコマンドが失敗し、「タスクが選択されていないか、選択されたタスクが存在しません」というエラーが発生します。

セキュリティ上の理由から、デフォルトでは、実行ポリシーは「制限されたスクリプト」として設定されています。これにより、ESET Shell を監視ツールとして使用できますが、ESET File Security for Microsoft Windows Server の構成を変更することはできません。保護の無効化などのセキュリティに影響する可能性があるコマンドを実行すると、「アクセスが拒否されました」というメッセージが表示されます。構成を変更するようなコマンドを実行するには、署名されたバッチファイルを使用することをお勧めします。

Windows コマンドプロンプトで入力されたコマンドを使用して、構成を変更する必要がある場合は、ESET Shell にフルアクセスの権限を付与する必要があります（この操作は推奨されません）。フルアクセスを付与するには、ui eshell shell-execution-policy コマンドを、インタラクティブモードで実行します。または、GUI で［詳細設定］＞［ユーザーインターフェース］＞［ESET SHELL］の順に選択して実行することもできます。

署名されたバッチファイル

署名を使用して、一般的なバッチファイル（*.bat）を保護できます。スクリプトは、設定保護で使用されているものと同じパスワードで署名されます。スクリプトに署名するには、まず、設定保護を有効にします。この操作は、GUI を使用するか、ESET Shell 内から set ui access lock-password コマンドを使用して、実行できます。設定保護パスワードが設定されると、バッチファイルに署名できます。

バッチファイルに署名するには、sign <script.bat> をルートコンテキストから実行します。script.bat は、署名するスクリプトへのパスです。署名で使用するパスワードを入力して確認します。このパスワードは、設定保護パスワードと一致しなければなりません。署名は、コメントの形式でバッチファイルの最後に配置されます。スクリプトが以前に署名されている場合は、署名が新しい署名に置換されます。

！重　要

以前に署名されたバッチファイルを修正する場合は、もう一度署名して置換する必要があります。

！重　要

設定保護パスワードを変更する場合は、すべてのスクリプトにもう一度署名する必要があります。もう一度署名を行わない場合、設定保護パスワードを変更した時点で、スクリプトを実行できなくなります。スクリプトに署名するときに入力したパスワードは、ターゲットシステムの設定保護パスワードと一致する必要があるためです。

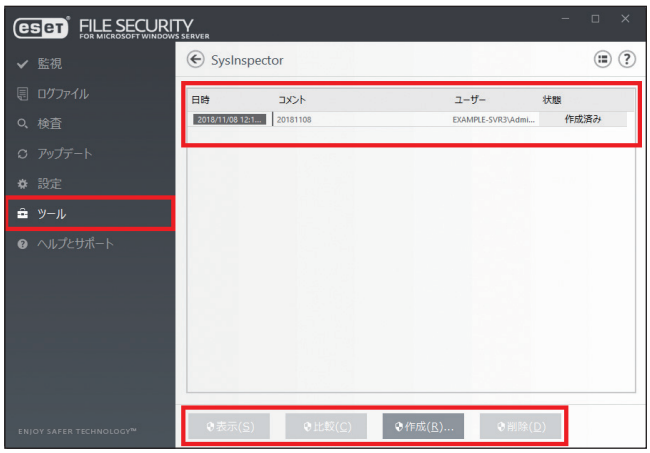
Windows コマンドプロンプトから署名されたバッチファイルを実行するか、スケジュールタスクとして実行するには、次のコマンドを使用します。

```
eshell run <script.bat>
```

script.bat はバッチファイルへのパスです。例：`eshell run d:\myeshellscript.bat`

4.5.6 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	選択したログを一覧から削除します。

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。

■コンピューターステータスのスナップショットを作成

[作成] をクリックし、コメントを入力して、[追加] ボタンをクリックします。ハードウェア構成とシステムデータによっては、ログの作成に時間がかかる場合があります。詳しくは、「操作手順」を参照してください。

■ ESET SysInspector の実行

ESET Sysinspector は、コンピューターを検査し、インストールされている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詳細な情報を収集するアプリケーションです。疑わしいシステムの動作がある場合に、それがソフトウェアやハードウェアの互換性による問題なのか、それともマルウェアの感染が原因なのかを調べるのに役に立ちます。

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。

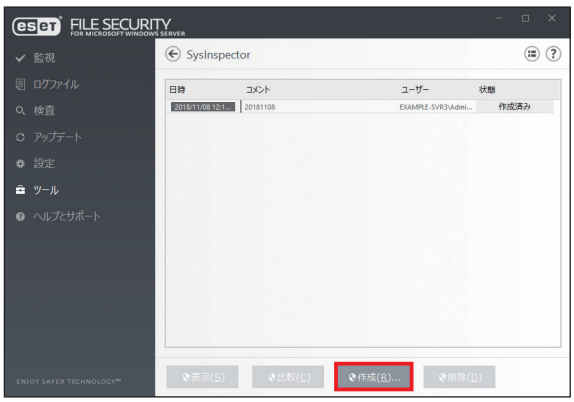
STEP1	ESET File Security for Microsoft Windows Server の「詳細設定」で「ESET SysInspector] を起動します。
STEP2	ESET SysInspector で、その時点のコンピューターの状態のスナップショットを作成します。
STEP3	スナップショットを開くと SysInspector アプリケーションが起動して分析結果が表示されます。この画面でコンピューターの状態を確認します。

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。

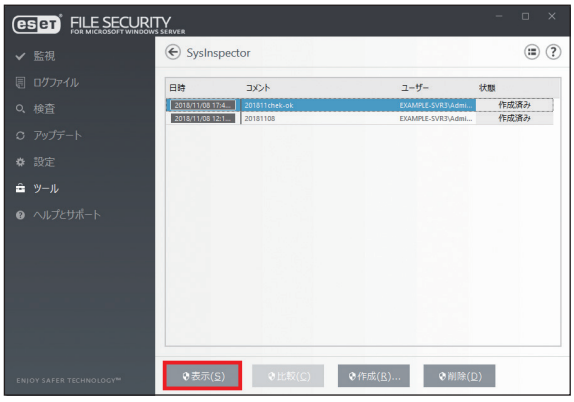


2. 作成するスナップショットについてのコメントを入力して［作成］をクリックします。

※ファイル名は実行時の日時から自動的に付けられます。

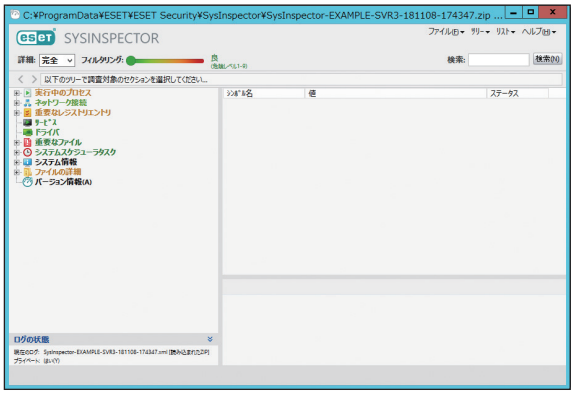


3. 作成したスナップショットを選択して［表示］をクリックします。



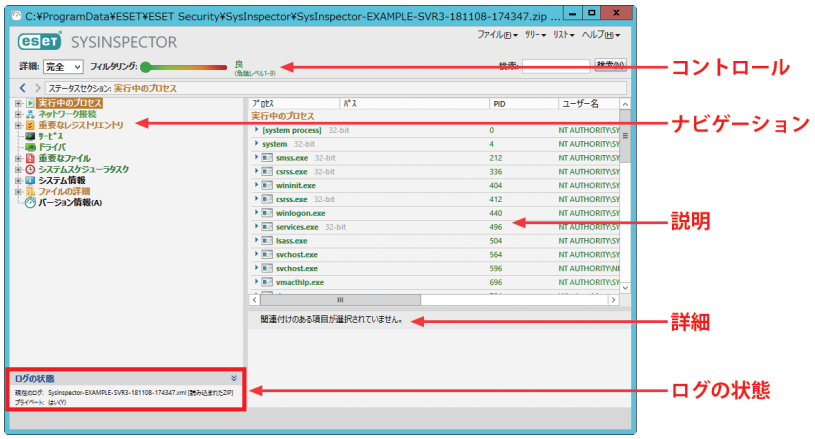
続く

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。



■ SysInspector 画面の使い方

ESET SysInspector のメイン画面は 4 つのセクションに分かれています。「プログラムコントロール」はメイン画面の上部、「ナビゲーション」ウインドウは左側、「説明」ウインドウは中央右側、「詳細」ウインドウはメイン画面の下部右側にそれぞれ配置されています。メイン画面の下部左側の「ログの状態」ウインドウには、ログの基本パラメーター（使用されているフィルター、フィルタータイプ、ログの比較の結果など）が一覧表示されます。



● SysInspector の操作

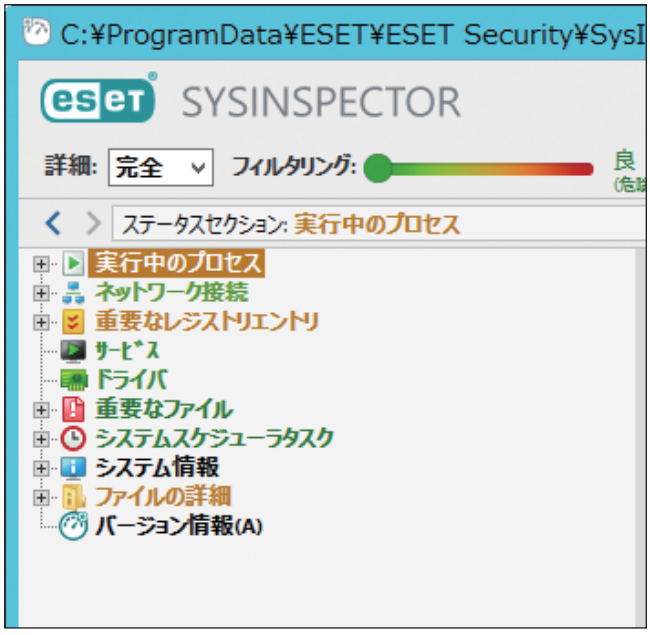
ESET SysInspector には、次の機能があります。

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、［生成］＞［送信用］を選択し、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、各ノードをサブノードに展開して追加情報を確認することができます。ノードの展開／折りたたみを行うには、ノードの名前をダブルクリックするか、名前の横にある＋ または －をクリックします。ナビゲーションウインドウで項目を選択すると、説明ウインドウに情報が詳細に表示されます。説明ウインドウで項目を参照すると、詳細ウインドウに詳細情報が表示されます。



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。

ESET SysInspector で使用できるショートカットキーは、次のとおりです。

ファイル

Ctrl+O	特定ファイルのログを開きます。
Ctrl+S	作成したログを保存します。

生成

Ctrl+G	コンピューターの状態の標準スナップショットを生成します。
Ctrl+H	コンピューターの状態のスナップショットを生成します（機密情報もログに記録される可能性があります）。

項目のフィルタリング

1, O	良好、危険レベル 1 ～ 9 の項目が表示されます。
2	良好、危険レベル 2 ～ 9 の項目が表示されます。
3	良好、危険レベル 3 ～ 9 の項目が表示されます。
4, U	不明、危険レベル 4 ～ 9 の項目が表示されます。
5	不明、危険レベル 5 ～ 9 の項目が表示されます。
6	不明、危険レベル 6 ～ 9 の項目が表示されます。
7, B	危険、危険レベル 7 ～ 9 の項目が表示されます。
8	危険、危険レベル 8 ～ 9 の項目が表示されます。
9	危険、危険レベル 9 の項目が表示されます。
-	危険レベルを下げます。
+	危険レベルを上げます。
Ctrl+9	フィルタリングモード、同等以上のレベルにフィルターされます。
Ctrl+0	フィルタリングモード、同等レベルのみにフィルターされます。

表示

Ctrl+5	ベンダーによる表示、すべてのベンダーを表示します。
Ctrl+6	ベンダーによる表示、Microsoft のみを表示します。
Ctrl+7	ベンダーによる表示、他のすべてのベンダーを表示します。
Ctrl+3	完全な詳細を表示します。
Ctrl+2	中程度の詳細を表示します。
Ctrl+1	基本的な表示です。
Backspace	1 ステップ戻ります。
Space	1 ステップ進みます。
Ctrl+W	ツリーを展開します。
Ctrl+Q	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、項目の元の場所に戻ります。
Ctrl+P	項目についての基本情報を表示します。
Ctrl+A	項目についての完全情報を表示します。
Ctrl+C	現在の項目のツリーをコピーします。
Ctrl+X	項目をコピーします。
Ctrl+B	選択した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	選択した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で開きます。
Ctrl+Z	ファイルのパスをコピーします（項目がファイルに関連付けられている場合）。
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	すべての項目を表示します。
Ctrl+Alt+2	追加された項目のみを表示します（現在のログと同じ項目にについてのログが表示されます）。
Ctrl+Alt+3	削除された項目のみを表示します（前回のログと同じ項目にについてのログが表示されます）。
Ctrl+Alt+4	置き換えられた項目のみを表示します（ファイルも含まれます）。
Ctrl+Alt+5	ログ間の相違のみを表示します。
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	プログラムを閉じます。
Alt+Shift+F4	確認せずにプログラムを閉じます。
Ctrl+I	統計をログに記録します。

●ログの比較

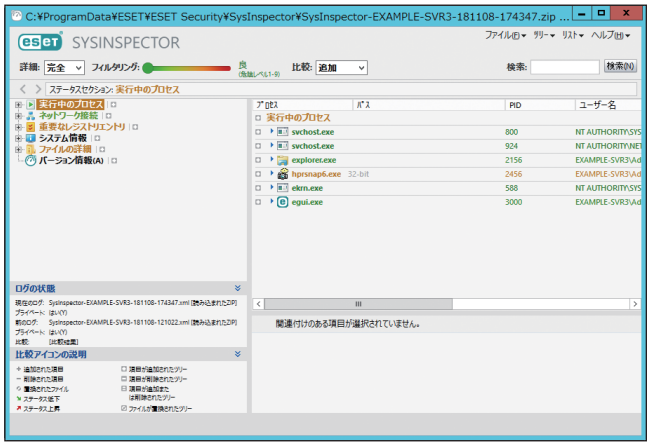
2 つのログを比較して、相違項目を洗い出します。ログの比較はシステムの変更を追跡し、悪意のあるコードを検出するのに役立ちます。

ログの保存／表示

起動後、自動的に新しいログが作成されます。ログをファイルに保存するには、［ファイル］＞［ログの保存］をクリックします。既存のログを開くには、［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。

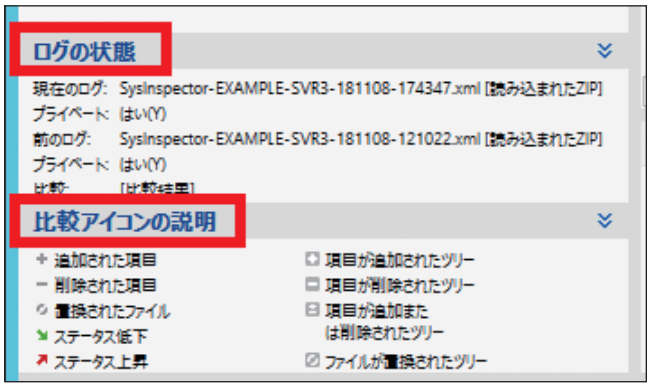


リストに表示される記号は、次の意味を表します。

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。



［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。

■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み

  ```
  SysInspector.exe "c:\clientlog.xml"
  ```

- ログを現在の場所に生成する

  ```
  SysInspector.exe /gen
  ```

- ログを特定のフォルダーに生成する

  ```
  SysInspector.exe /gen="c:\folder\"
  ```

- ログを特定のファイル／場所に生成する

  ```
  SysInspector.exe /gen="c:\folder\mynewlog.xml"
  ```

- ログを、機密情報を除外して直接圧縮ファイルとして生成する

  ```
  SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip
  ```

- 2 つのログを比較する

  ```
  SysInspector.exe "current.xml" "original.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「'」（シングルクォーテーション）で囲む必要があります。

■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,AEQC*↓
- 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*↓
```

続く

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行は変更しないでください。

ヘッダ行以下は、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（重大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。

■ 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イ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？

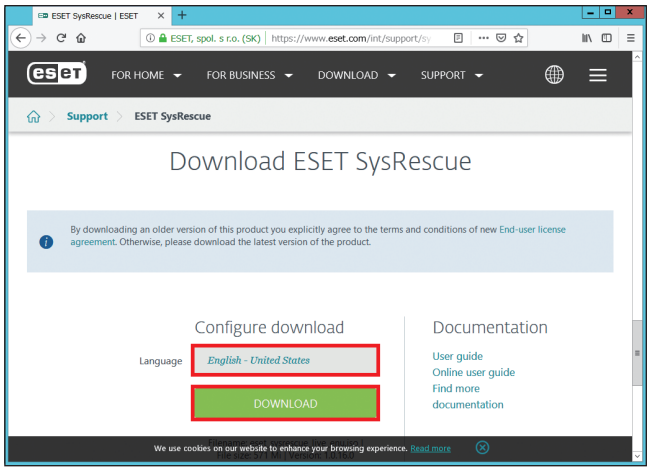
実行可能ファイルのデジタル署名を識別するときにファイルに埋め込まれたデジタル署名をチェックします。デジタル署名が検出されると、その情報を使ってファイルを検証します。デジタル署名が見つからない場合、ESET SysInspector は処理する実行可能ファイルに関する情報を収めた CAT ファイル（セキュリティカタログ - % systemroot%\system32\catroot）の検索を開始します。該当する CAT ファイルが見つかると、CAT ファイルのデジタル署名を使って検証します。「Signed by MS」というマークのあるファイルが、異なる「CompanyName」エントリーを持つ場合があるのはこのためです。

例：
Windows 2000 では、C:\Program Files\Windows NT にハイパーターミナルアプリケーションがあります。メインアプリケーションの実行可能ファイルはデジタル署名されていませんが、ESET SysInspector ではこのファイルを Microsoft により署名されているものとしてマークします。この理由は、C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat における参照が C:\Program Files\Windows NT\hypertrm.exe（ハイパーターミナルアプリケーションの主要な実行可能ファイル）をポイントし、「sp4.cat」が Microsoft によってデジタル署名されているためです。

4.5.7 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。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。



4.5.8 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」画面を表示するには、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。



「スケジューラ」画面でタスクの追加または削除を行うことができます。
「スケジューラ」画面内でスケジュールを選択して右クリックすると、[タスクの詳細を表示]、[今すぐ実行]、[追加]、[編集]、［削除］を実行できます。各タスクのチェックボックスタスクの有効 / 無効を切り替えます。

既定では、次のスケジュールされたタスクがスケジューラに表示されます。

- ログの保守
- 定期的に自動アップデート
- ダイヤルアップ接続後に自動アップデート
- ユーザーログオン後に自動アップデート
- 自動スタートアップファイルのチェック（ユーザーのログオン後）
- 自動スタートアップファイルのチェック（検出エンジンのアップデート後）

既存のスケジュールされたタスク（既定のタスクとユーザー定義のタスク）の設定を編集するには、タスクを右クリックして［編集］をクリックするか、または変更するタスクを選択して［編集］をクリックします。

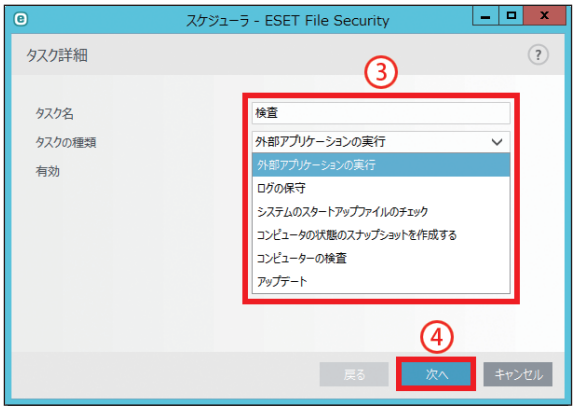
■新しいタスクの追加

次の 6 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。
Hyper-V 検査	Hyper-V 内の仮想ディスクを検査します。Hyper-V 利用環境のみで表示されます。

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」プル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しました。 • 製品アップデート成功 • ユーザログオン • 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。

続く

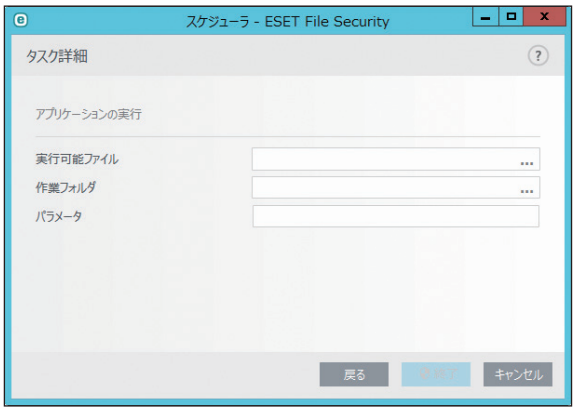
10 指定した時刻にタスクが実行されなかった場合に、タスクを再度実行するタイミングを選択します。

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。

詳細は「■タスクが実行されなかった場合」を参照してください。

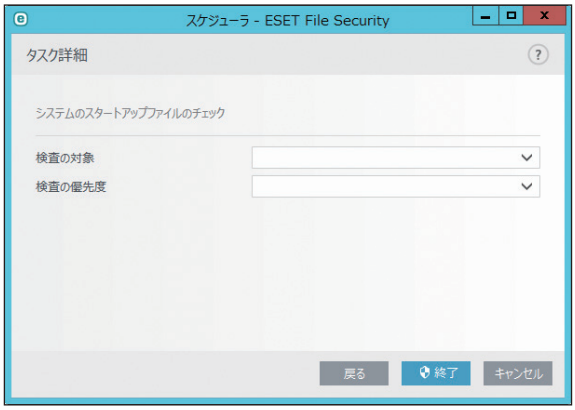
11 各項目を設定します。表示される項目は、手順 3 で選択した「タスクの種類」によってかわります。

• **［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。

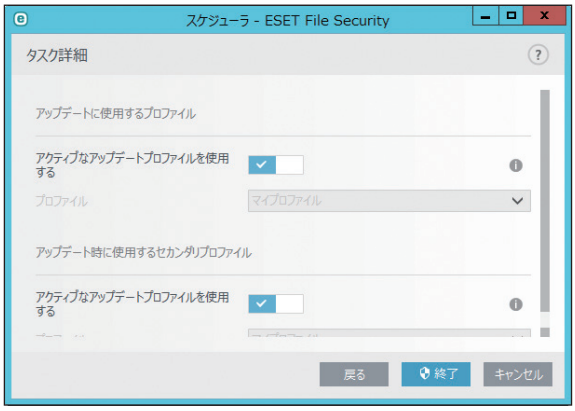
• **［システムのスタートアップファイルのチェック］を選択した場合**



続く

検査レベル	システム起動時のファイル検査レベルを指定します。	
	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最も低い時に、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の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しました。
- 製品アップデート成功
- ユーザログオン
- 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。

■タスクが実行されなかった場合

あらかじめ定義した時刻にタスクが実行されなかった場合、次にタスクを実行する時期を指定することができます。

次のスケジュール設定日時まで待機	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。

■スケジューラータスクの詳細

スケジューラの一覧でタスクをダブルクリックするか、スケジュール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、「スケジュールタスクの概要」画面が表示されます。この画面には、選択したスケジュールタスクに関する詳細情報が表示されます。



■アップデートプロファイル

2 つの異なるアップデートサーバーを使ってアップデートする場合、それぞれのアップデート用プロファイルを作成する必要があります。最初のサーバーでアップデートファイルのダウンロードに失敗すると、自動的に次のサーバーに接続されます。これは、通常は LAN 内のミラーサーバーからアップデートを行っているが、外出先では ESET サーバーに接続してアップデートするような場合に便利です。最初のプロファイルでのダウンロードが失敗すると、次のプロファイルが自動的に ESET のアップデートサーバーからアップデートファイルをダウンロードします。

アップデートプロファイルの詳細については、「5.1.8　アップデート」を参照してください。

4.5.9 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。

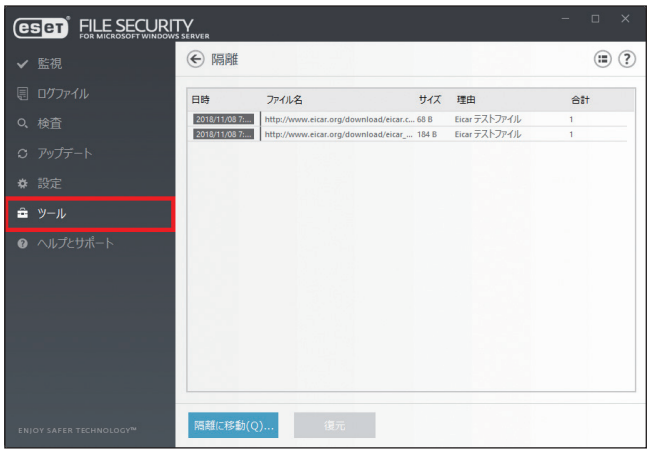
6. 必要に応じてファイルおよび Web サイトの補足情報を入力し、［完了］をクリックします。

! 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。

4.5.10 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」画面を表示するには、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とみなされている場合は、［復元して検査から除外］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。

■隔離から削除

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。

! 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してください。

■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 のウイルスラボに提出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。

4.5.11 ヘルプとサポート

ESET File Security for Microsoft Windows Server 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	P100 参照
テクニカルサポート	P100 参照
サポートツール	P101 参照
製品およびライセンス情報	P101 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。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 File Security for Microsoft Windows Server 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。ESET 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。
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

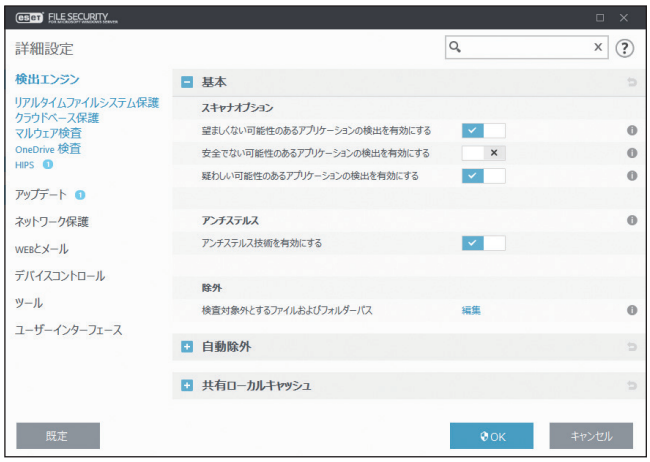
ESET File Security について	バージョン情報やインストール済のコンポーネントについて確認できます。
製品のアクティベーション	製品のアクティベーション画面を開きます。詳細については「2.4 アクティベーション」を参照してください。

Chapter 5 設定

5.1 詳細設定

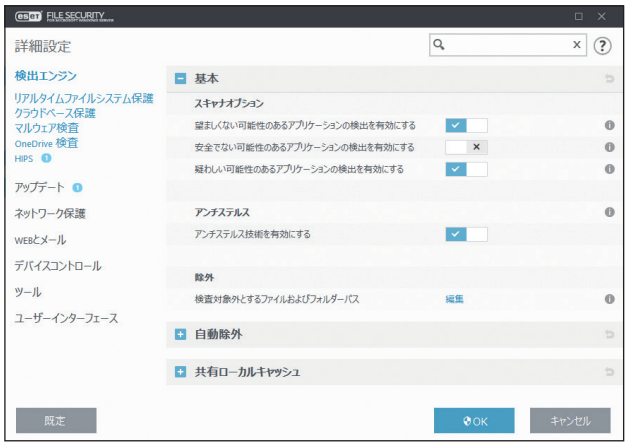
ESET File Security for Microsoft Windows Server に備わっている各機能について詳細な設定を行うことができます。「詳細設定」画面を表示するには、メインメニューの［設定］＞［詳細設定］をクリックするか、【F5】キーを押してアクセスします。





5.1.1 検出エンジン

ファイル、メール、およびインターネット通信を検査することにより、悪意のある攻撃からコンピューターを保護します。脅威が検出されると、まず保護機能がブロックし、次に駆除、削除、隔離のいずれかを行って、ウイルスを排除します。「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［検出エンジン］を選択します。

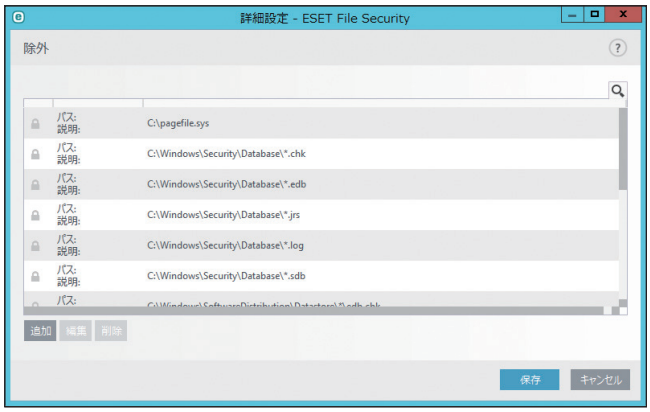


■基本

スキャナオプション	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	望ましくない可能性があるアプリケーションは、明確な悪意があるソフトウェアではありませんが、追加の望ましくないアプリケーションをインストールしたり、デジタルデバイスの動作を変更したり、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したり、他の不明確な目的を持っていたりする可能性があります。このカテゴリには、広告表示ソフトウェア、ダウンロードラッパー、各種ブラウザーツールバー、誤解を招く動作のソフトウェア、バンドルウェア、トラックウェアなどがあります。ここでは、この種のアプリケーションの検出を行うかどうかを設定します。
	安全で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	この分類は、悪意のある目的で悪用される可能性がある商業的、合法的なソフトウェアです。安全ではない可能性があるアプリケーションは、不正な目的で悪用される可能性のある、市販の適正なソフトウェアです。このカテゴリには、クラッキングツール、ライセンスキー生成、ハッシュツール、リモートアクセスまたはコントロールツール、パスワード解析アプリケーション、キーロガーなどが含まれます。ここでは、この種のアプリケーションの検出を行うかどうかを設定します。このオプションは、既定では無効になっています。
	疑わしい可能性のあるアプリケーションの検出を有効にする	マルウェアの存在を隠すためにリバースエンジニアリングの阻止または実行ファイルの内容を曖昧にする圧縮または暗号化されたソフトウェアを検出するかどうかを設定します。このカテゴリには、マルウェアを圧縮するために使用されるパッカーまたはプロテクターで圧縮されたすべての不明なアプリケーションが含まれます。
アンチステルス	アンチステルス技術を有効にする	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。
除外	検査対象外とするファイルおよびフォルダーパス	指定したファイルやフォルダーを検査から除外します。すべてのファイルやフォルダーでウイルスが検出できるように、基本的には除外しないことをお勧めします。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がある場合などは、必要に応じて除外を設定してください。除外フィルタの詳細については、「●除外」を参照してください。

●除外

除外を利用すると、特定のファイルやフォルダーを検査の対象外に指定できます。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、特別な場合以外はスキャン除外設定を行わないことをお勧めします。
「検査対象外とするファイルおよびフォルダーパス」の［編集］を選択します。

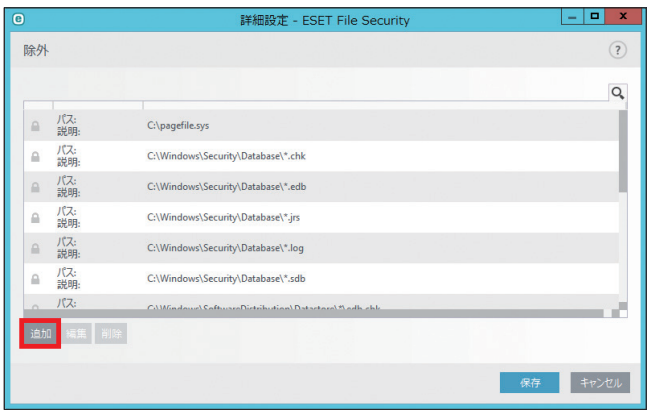


パス	検査から除外するファイルやフォルダーのパスが表示されます。
脅威	マルウェアの脅威警告画面で［設定の表示］>［検出対象外］をクリックするか、［設定］>［隔離］をクリックし、隔離するファイルのコンテキストメニューから［検出からの復元と除外］を選択すると、マルウェアの名前が表示されます。この場合、表示されているマルウェアのみが検査の対象外になり、他のマルウェアは検査対象となります。したがって、マルウェアの名前が表示されているファイルが後で他のマルウェアに感染した場合は、検出エンジンによって検出されます。なお、検査対象外にできるのは、特定の種類のマルウェアのみです。
ハッシュ	検査から除外するハッシュ値（SHA1）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	パスを編集します。
削除	パスを削除します。

検査対象からファイルやフォルダーを除外する手順は次の通りです。

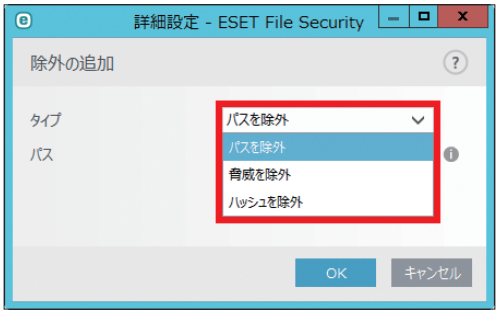
操作手順

1 ［追加］をクリックします。



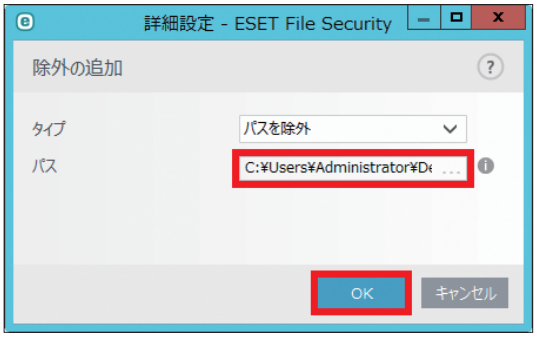
続く

2 除外タイプを選択します。タイプのドロップダウンリストから除外のタイプを選択します。



パスを除外	このコンピューターで特定のパスを除外します。
脅威を除外	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、および不審なアプリケーションに適用されます。
ハッシュを除外	ファイルタイプ、場所、名前、または拡張子に関係なく、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。

3 パスの入力や脅威名、ハッシュ、説明など、手順 2 で選択した除外タイプに応じた設定を行い、［OK］ボタンをクリックします。



パス	除外したいファイルまたはフォルダーのパスを入力します。この設定は、タイプに「パスを除外」または「脅威を除外」を選択したときに行います。
脅威名	脅威の名称を入力します。この設定は、タイプに「脅威を除外」を選択したときに行います。脅威を除外する場合は、「@NAME= 脅威名」の形式で有効な脅威名を入力します。例えば、以下のように入力します。 入力例 @NAME=Win32/Adware.Optmedia @NAME=Win32/TrojanDownloader.Delf.QQI @NAME=Win32/Bagle.D
ハッシュ	ハッシュ（SHA1）を入力します。この設定は、「ハッシュを除外」を選択したときに行います。
説明	除外するファイルの説明を入力します。この設定は、「ハッシュを除外」を選択したときに行います。

続く

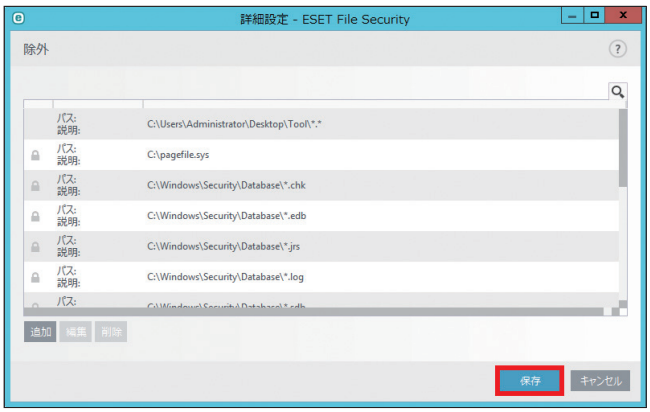
ワンポイント

ファイルを指定する場合、ワイルドカードを使用すると、複数のファイルを指定できます。「?」（疑問符）は 1 つの可変文字を表し、「*」（アスタリスク）は 0 文字以上の可変文字列を表します。なお、ハッシュを指定する場合はワイルドカードは使用できません。

例

- 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を含めたドライブ全体を除外するには、「*」を使用します。
- 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文字が使用されており、一部の文字しかわからない場合は、「?」疑問符を使用します。例えば、文字数が 5 文字で、最初の文字が「D」であることのみわかっている場合は、「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。

4 選択したファイルやフォルダーが「除外」のリストに登録されます。［保存］ボタンをクリックします。



!重　要

除外に設定されていると、リアルタイムファイルシステム保護機能とコンピューターの検査機能はファイル内の脅威を検出しません。

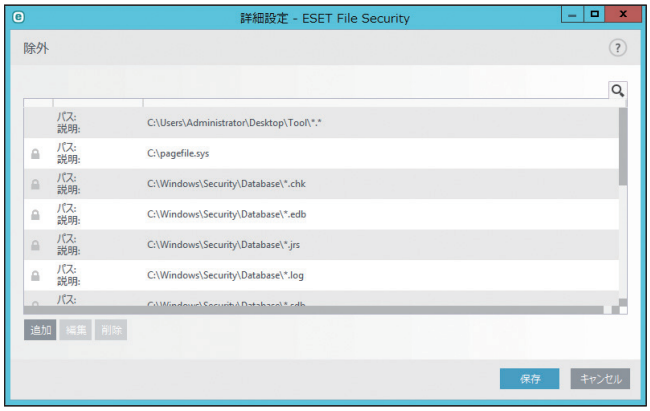
■自動除外



ウイルス対策ソフトウェアの検査が、パフォーマンスに悪影響を与えたり、競合してアプリケーションが実行できなくなることを防ぐために、アプリケーションやオペレーティングシステムのファイルは、ウイルス対策ソフトウェアの検査対象外にすることが推奨されています。
除外機能を使用することで競合のリスクを最小化し、サーバーの全体的なパフォーマンスを向上させることができます。

重要なサーバーアプリケーションとサーバーのオペレーティングシステムファイルを識別して、除外リストに自動的に追加します。［自動除外を有効にするアプリケーション / サーバー］の下に、除外が作成された検出済みサーバーアプリケーションが一覧表示されます。すべての自動除外は既定で有効に設定されています。各サーバーアプリケーションの自動除外の有効 / 無効は、それぞれの製品名のスイッチで選択します。

1.「自動除外を有効にする」が有効になっている場合、重要なファイル、フォルダーのすべてが、除外リストに追加されます。サーバーを再起動するたびに、自動除外のチェックが実行され、リストが更新されます。



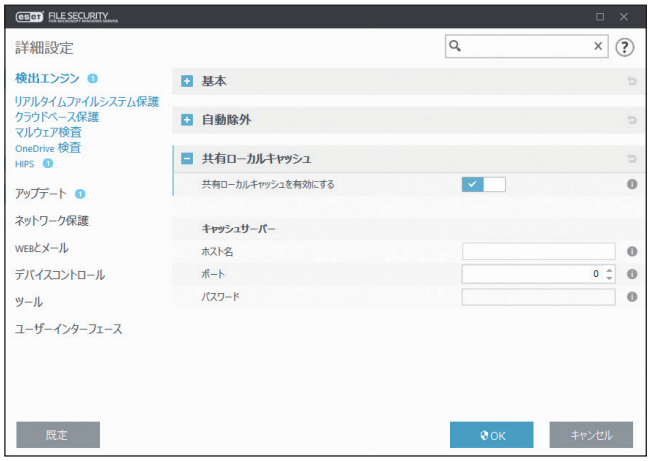
除外リストを表示するには、［詳細設定］＞［検出エンジン］＞［基本］＞「検査対象外とするファイルおよびフォルダーパス」の［編集］をクリックします。自動除外されたファイルやフォルダーのパスと、脅威の内容が表示されます。
自動除外を常に適用したい場合は、この設定を推奨します。

2.「自動除外を有効にする」を無効に変更しても、既存の「除外リスト」は削除されずに一覧に残ります。ただし、サーバーの再起動を行っても、自動除外の更新は行われません。この設定は、標準の除外リストの一部を変更、削除したい場合に使用できます。
サーバーを再起動せずに、リストから手動で削除することもできます。

［詳細設定］＞［検出エンジン］＞［基本］＞「検査対象外とするファイルおよびフォルダーパス」の［編集］＞［追加］で手動で入力したユーザー定義の除外対象は、上記設定の影響を受けません。

サーバーアプリケーション／オペレーティングシステムの自動除外は、Microsoft の推奨事項に基づいて選択されます。

■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 File Security for Microsoft Windows Server 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には次の内容があります。

ホスト名	キャッシュが保存されているクライアント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）。
パスワード	必要に応じて、共有ローカルキャッシュのパスワードを設定します。

●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 File Security for Microsoft Windows Server 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。

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

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、「5.1.2 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

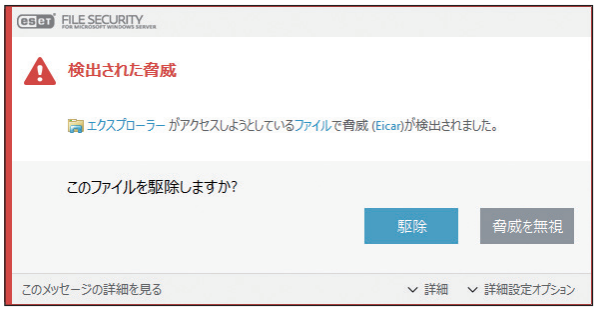
駆除とは、ウイルスに感染したファイルからウイルスだけを取り除き、正常なファイルに戻すことです。削除とは、感染したファイルそのものを削除することです。ウイルスの種類によっては駆除が難しく、場合によってはファイルを削除しなければなりません。



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［駆除なし］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

既定の駆除モードでは、アーカイブ内のすべてのファイルが感染ファイルの場合、アーカイブファイルは削除されます。感染していないファイルが含まれている場合、アーカイブは削除されません。厳密な駆除モードでは、アーカイブに感染ファイルが 1 つでも含まれていれば、アーカイブ内の他のファイルの状態に関係なく、アーカイブが削除されます。そのため、厳密な駆除モードを実行する際には注意が必要です。

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、「5.1.4.1　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

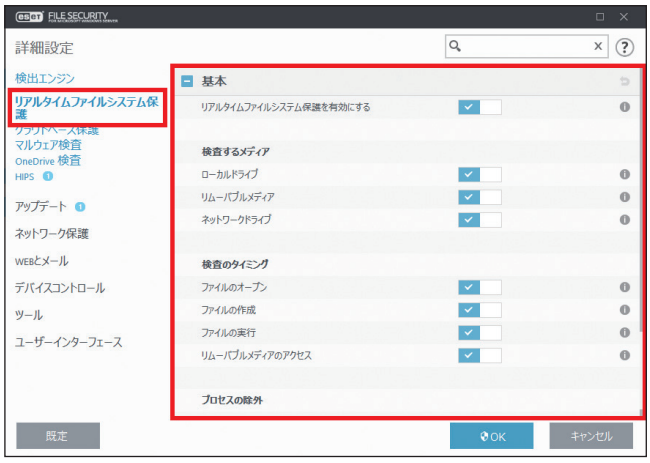
コンピューターの特定の領域だけを検査する場合は、［カスタム検査］をクリックし、ウイルスを検査する対象を選択します。

5.1.2　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では、クライアントコンピューター上で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すべて検査します。リアルタイムファイルシステム保護は、システム起動時に開始されます。

「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［リアルタイムファイルシステム保護］を選択します。



既定では、リアルタイムファイルシステム保護はシステム起動時に起動し、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、［詳細設定］＞［リアルタイムファイルシステム保護］＞［基本］の下の［リアルタイムファイルシステム保護を有効にする］オプションの選択を解除すると、リアルタイム保護を無効にできます。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を検査します。

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。

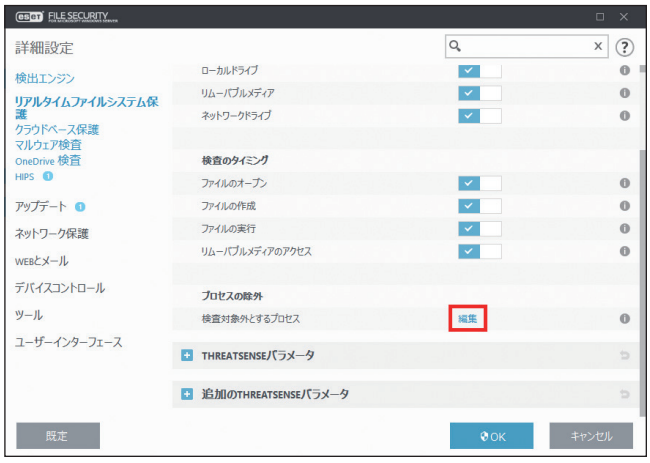
検査のタイミング

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推奨します。

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。

●プロセスの除外

プロセスの除外機能は、リアルタイムファイルシステム保護から指定したアプリケーションプロセスを除外します。これにより、競合の可能性のリスクを最小化し、除外されたアプリケーションのパフォーマンスを改善します。バックアップソリューションのプロセスの場合、プロセスの除外を利用することで、そのプロセスに基づくすべてのファイル処理が無視され、バックアップ処理の中断を最小限に抑えることができます。なお、除外を作成するときには注意してください。除外されたアプリケーションプロセスは、アラートをトリガーせずに感染ファイルにアクセスできます。検査からプロセスの除外するには、「検査対象外とするプロセス」の［編集］を選択します。



!重　要

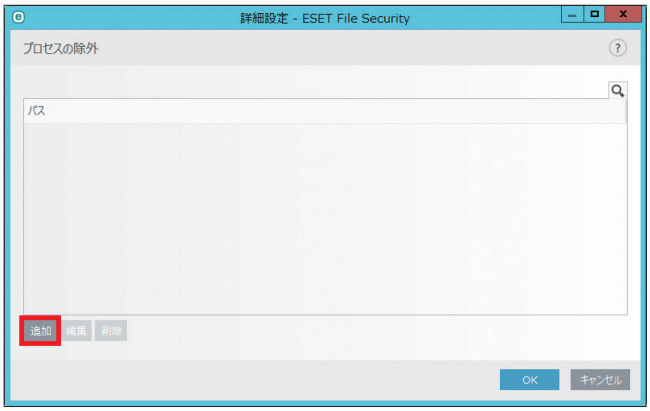
プロセスの除外は、リアルタイムファイルシステム保護からのみ除外されます。例えば、Web アクセス保護ではプロセスは除外されません。Web ブラウザの実行ファイルを除外しても、ダウンロードされたファイルは検査されます。これにより、侵入を検出することができます。Web ブラウザの除外を作成することは推奨しません。

! 重 要

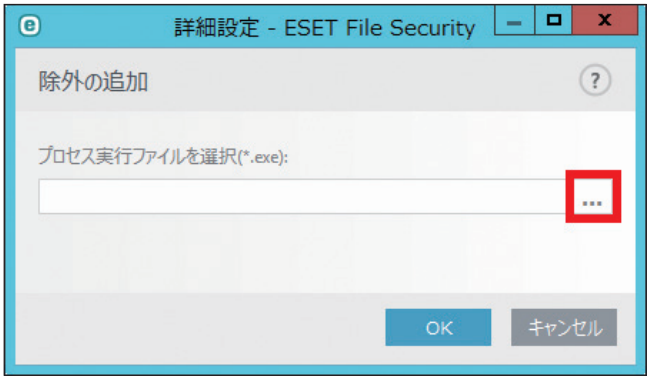
HIPS は除外されたプロセスの評価を実行します。このため、HIPS が有効な状態で新しく除外されたプロセスをテストすることを推奨します（問題が発生する場合は、HIPS を無効にします）。HIPS を無効にしても、プロセス除外には影響しません。HIPS が無効な場合、除外されたプロセスはパスを使用して特定します。

操作手順

1 ［追加］をクリックします。

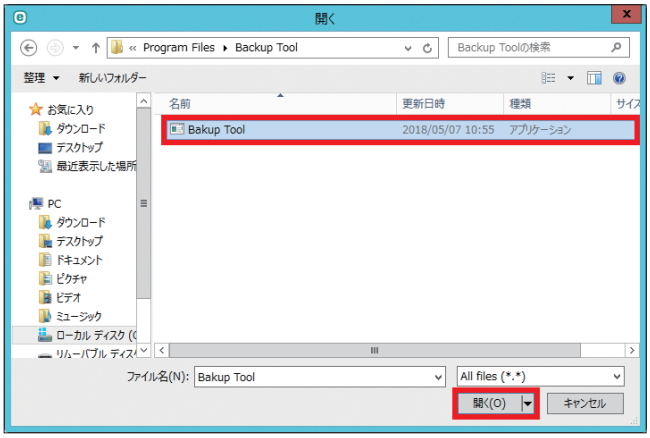


2 …をクリックします。



続く

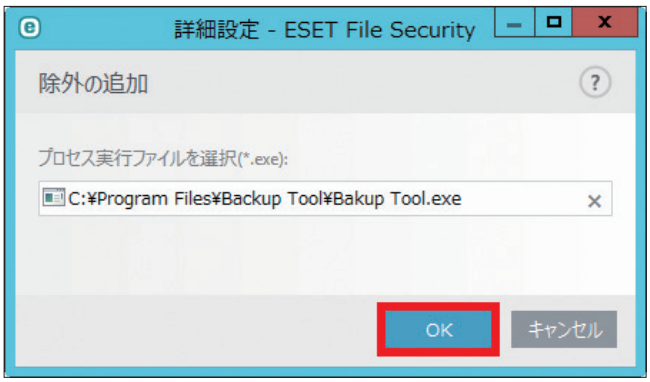
3 除外したいプロセス実行ファイルを選択し、［開く］ボタンをクリックします。



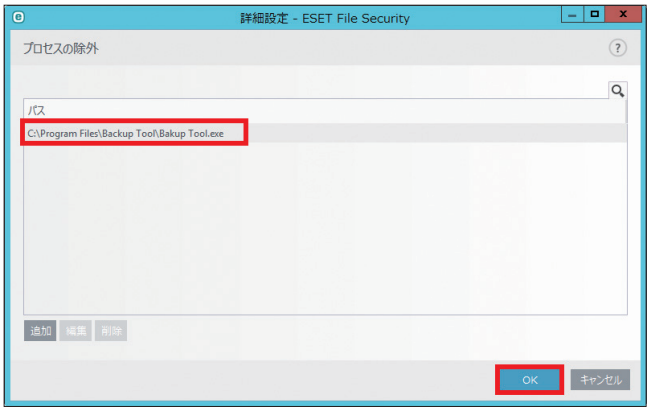
ワンポイント

プロセス実行ファイルを選択するときに、参照機能を使用しない場合は、手動で実行ファイルの「完全パス」を入力する必要があります。完全パスを入力しない場合、プロセスの除外は正しく動作せず、HIPS がエラーを報告する場合があります。

4 ［OK］ボタンをクリックします。

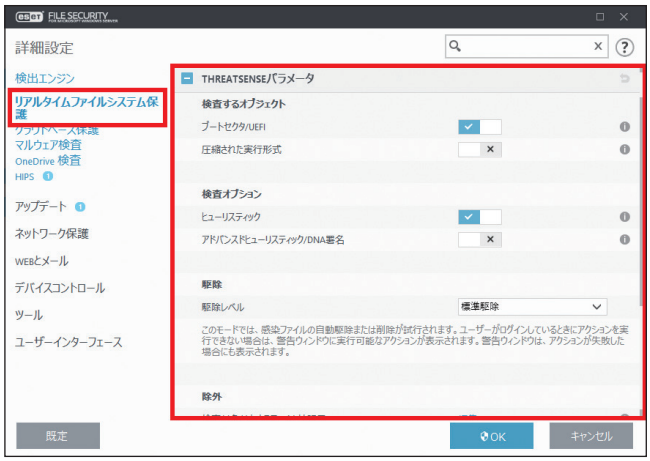


5 選択したプロセス実行ファイルが、「プロセスの除外」リストに登録されます。［OK］ボタンをクリックします。



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）の検出方法であるため、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。



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
- 駆除レベル

など

! 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ため、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、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、リアルタイムファイル保護機能のアドバンスドヒューリスティックを有効にすると、システムの処理速度が低下することがあります（通常は、新しく作成されたファイルのみがこの検査対象です）。コンピューターの検査を除くすべての機能について、THREATSENSE の既定のパラメーターを変更しないことを推奨します。

検査するオブジェクト

ここでは、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します。

ブートセクタ /UEFI	ブートセクタおよび 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。
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。

検査オプション

システムへの侵入を検査するときに使用する方法を選択します。使用可能なオプションは次の通りです。

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。

駆除

駆除の設定により、感染ファイルからウイルスを駆除するときの動作が決まります。リアルタイムファイルシステム保護検査には 3 つの駆除レベルがあります。

駆除なし	感染しているファイルは自動的に駆除されず、警告画面でユーザーがアクションを選択することができます。ウイルスの侵入が発生したときに実行しなければならないステップを理解している経験豊富なユーザー向けのレベルです。
標準駆除	あらかじめ定義されたアクション（マルウェアの種類によって異なります）に基づいて、感染ファイルを自動的に駆除または削除します。感染しているファイルの検出と削除は、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。適切なアクションを自動的に選択できなかった場合は、ユーザーがその後のアクションを選択することができます。あらかじめ定義されているアクションを実行できなかった場合も同様です。
厳密な駆除	すべての感染ファイルが駆除または削除されます（システムファイルを除く）。感染ファイルを駆除できなかった場合は、アクションを選択する警告画面が表示されます。

! 重　要

感染しているファイルがアーカイブに含まれている場合、アーカイブの処理方法は 2 つあります。「標準駆除」モードでは、アーカイブに含まれている検査対象のファイルがすべて感染ファイルである場合のみ、アーカイブが削除されます。「厳密な駆除」モードでは、アーカイブに感染ファイルが 1 つでも含まれている場合、アーカイブ内の他のファイルの感染に関係なく、アーカイブが削除されます。

除外

拡張子は、ファイル名の一部であり、ピリオドで区切られています。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 File Security for Microsoft Windows Server 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。

「検査対象外とするファイル拡張子」画面では次の操作ができます。

- ［追加］および［削除］のボタンを使用して、特定のファイル拡張子を検査の対象外にしたり、対象外リストから削除することができます。
- リストに新しい拡張子を追加するには、［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］を選択すると、改行、カンマ、セミコロンで区切られた複数のファイル拡張子を追加できます。複数の入力値が有効な場合、拡張子がリストに表示されます。
- リスト内の拡張子を選択し、［削除］をクリックすると、リストからその拡張子が削除されます。
- 選択した拡張子を編集する場合は、［編集］をクリックします。

ワンポイント

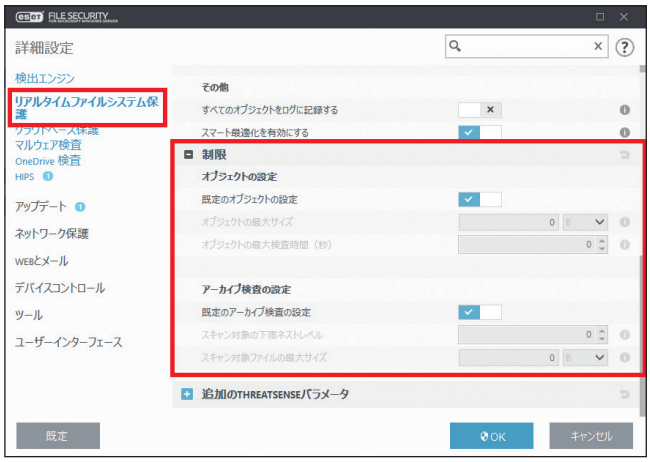
拡張子の指定では、特殊記号の「*」（アスタリスク）および「?」（疑問符）を使用できます。アスタリスクは任意の文字列を、疑問符は任意の記号をそれぞれ表します。特殊記号を使って拡張子を指定する際は、正しい形式で入力してください。

その他

すべてのオブジェクトをログに記録する	この機能を有効にすると、検査されたすべてのファイルがログファイルに表示されます。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リストに記録されます。
スマート最適化を有効にする	この機能を有効にすると、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、最適な設定が使用されます。様々な保護モジュールで高度に検査を行い、それぞれで異なる検査方法を使用して、それらを特定のファイルタイプに適用します。この機能を無効にすると、特定の保護モジュールの THREATSENSE コアのユーザー定義設定のみが検査の実行時に適用されます。

●制限

検査対象のオブジェクトの最大サイズおよびアーカイブファイルのネストレベルを指定できます。



オブジェクトの設定

次の項目について設定できます。

既定のオブジェクトの設定	このオプションを有効にすると、既定のオブジェクトの設定が使用されます。
オブジェクトの最大サイズ	検査対象のオブジェクトの最大サイズを定義します。これにより、指定した値より小さいサイズのオブジェクトのみが検査されます。上級ユーザーが大きいサイズのオブジェクトを検査から除外する必要がある場合のみ、このオプションを使用してください。既定では無制限に設定されており、「0」～「3」GB に制限できます。
オブジェクトの最長検査時間（秒）	オブジェクトの検査の最長時間を定義します。ここでユーザー定義の値を入力すると、検査が終わっているかどうかにかかわらず、その時間が経過すると検査は停止します。既定では無制限に設定されており、「0」～「4294967295」秒に制限できます。

アーカイブ検査の設定

次の項目について設定できます。

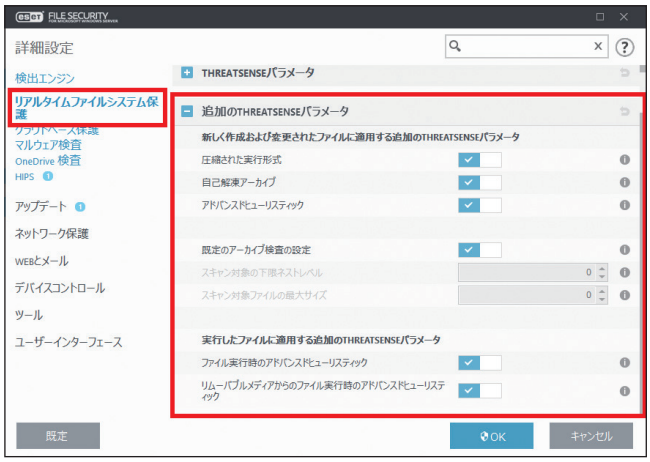
既定のアーカイブ検査の設定	このオプションを有効にすると、既定のアーカイブ検査の設定が使用されます。
スキャン対象の下限ネストレベル	アーカイブ検査のネストレベルを指定します。既定では「10」に設定されており、「0」～「20」に制限できます。
スキャン対象ファイルの最大サイズ	検査対象のアーカイブ（抽出された場合）に含まれているファイルの最大サイズを指定できます。既定では無制限に設定されており、「0」～「2」GB に制限できます。

！重　要

一般的な環境では既定値を変更する必要はないため、必要な場合以外はその値を変更しないことを推奨します。

■追加の THREATSENSE パラメータ

この項目では次の内容を設定できます。



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	新規に作成したファイルや修正したファイルは、感染のリスクが既存ファイルよりも高くなります。そのため、それらのファイルは、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ともに、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することができます。新規に作成したファイル以外にも、自己解凍形式のファイル（SFX）および圧縮された実行形式（内部圧縮された実行可能ファイル）も検査されます。既定では、アーカイブは最大で 10 番目のネストレベルまで検査され、ファイルサイズにかかわらず検査されます。
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。
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。
アドバンスドヒューリスティック	高いレベルのプログラミング言語で記述された悪意のあるコードを検出します。
既定のアーカイブ検査の設定	最大で 10 番目のネストレベルまで検査します。実際のサイズにかかわらず検査されます。スキャン対象の下限ネストレベル、スキャン対象ファイルの最大サイズを指定することもできます。
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はファイル実行時には使用しません。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推奨します。
ファイル実行時のアドバンスドヒューリスティック	コードが実行される前に高度なヒューリスティックが仮想環境でコードを展開し、動作を評価します。
リムーバブルメディアからのファイル実行時のアドバンスドヒューリスティック	コードがリムーバブルメディアから実行される前に高度なヒューリスティックが仮想環境でコードを展開し、動作を評価します。

●リアルタイムファイルシステム保護の設定の変更

リアルタイムファイルシステム保護は、システムを安全に維持するための重要な機能です。パラメーターを変更する際には注意してください。特定の状況に限ってパラメーターを変更することをお勧めします。

ESET File Security for Microsoft Windows Server インストール後は、システムセキュリティが最大保護を発揮するようにすべての設定が最適化されています。既定の設定に復元するには、画面の各タブのタイトル横にある既定ボタン をクリックします。

●リアルタイムファイルシステム保護の確認

リアルタイムファイルシステム保護が機能していて、かつウイルスが検出されることを確認するには、テストウイルスファイルを使用します。ウイルス対策製品のテスト用のウイルスは、「Eicar test file」が有名です。このテスト用のウイルスは無害ですが、ご使用中のコンピューターなどでウイルスと検出される可能性がありますのでご注意ください。「Eicar test file」の詳しい説明やダウンロード方法につきましては、EICAR の WEB サイトでご確認ください。

! 重　要

リアルタイムファイルシステム保護を確認する前に、Web アクセス保護を一時的に無効にする必要があります。Web アクセス保護が有効になっていると、テストファイルが検出され、ダウンロードできません。リアルタイムファイルシステム保護を確認したら、すぐに Web アクセス保護を再度有効にしてください。

●リアルタイムファイルシステム保護が機能しない場合の解決方法

この項目では、リアルタイム保護使用時に発生することがあるトラブル、およびその解決方法について説明します。

リアルタイム保護が無効である

ユーザーの不注意などによってリアルタイム保護を無効にしてしまった場合は、保護を再度有効にする必要があります。リアルタイム保護を有効にするには、メインメニューの［設定］に移動し、［コンピュータ］＞［リアルタイムファイルシステム保護］のスイッチをクリックして有効にします（ の状態）。次に詳細設定画面で［リアルタイム保護］＞［基本］をクリックします。［リアルタイムファイルシステム保護を有効にする］が有効になっていることを確認します。

リアルタイム保護がマルウェアの検出と駆除を行わない

クライアントコンピューターに他のウイルス対策プログラムがインストールされていないか確認します。2 つのリアルタイム保護システムが同時に有効になっていると、互いに競合することがあります。システムに他のウイルス対策プログラムがインストールされている場合は、ESET をインストールする前にそのプログラムをアンインストールすることを推奨します。

リアルタイム保護が開始されない

「リアルタイムファイルシステム保護を有効にする」が有効であるにもかかわらず、リアルタイムファイルシステム保護がシステム起動時に開始されない場合は、他のプログラムとの競合が考えられます。この問題を解決するには、サポートセンターにお問い合わせください。

5.1.3 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 File Security for Microsoft Windows Server 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 File Security for Microsoft Windows Server 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

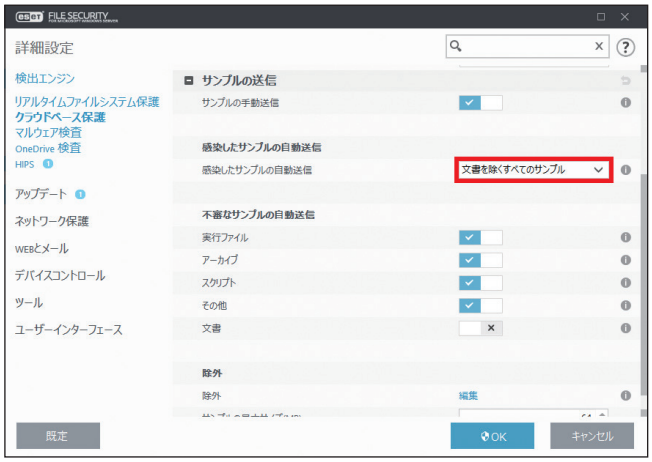
ESET LiveGrid は、新しく検出されたウイルスに関連して、クライアントコンピューターに関する情報を収集します。この情報には、ウイルスが検出されたファイルのサンプルまたはコピー、ファイルのパス、ファイル名、日時、ウイルスがコンピューターに侵入したプロセス、コンピューターのオペレーティングシステムについての情報が含まれます。
「詳細設定」画面で、［クラウドベース保護］をクリックします。



ESET LiveGrid に参加する（推奨）	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。
ESET LiveGrid フィードバックシステムを有効にする	有効にすると、データが詳細分析のために ESET に送信されます。
クラッシュレポートと診断データを送信	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信する	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。

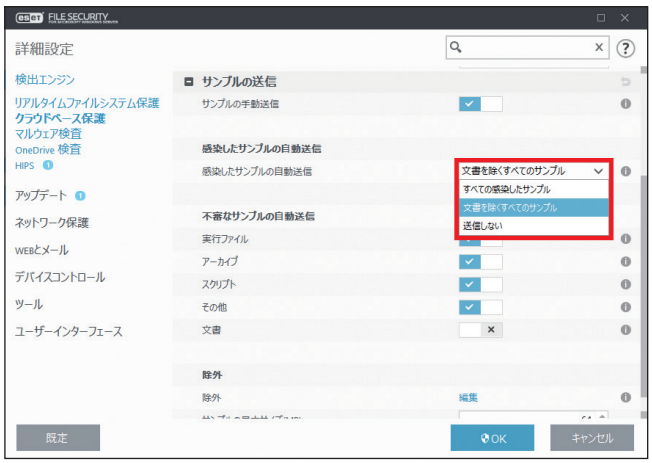
●サンプルの送信



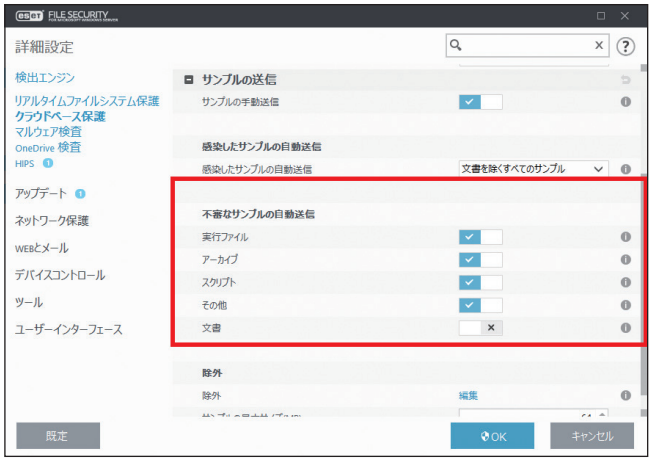
「サンプルの手動送信」では、疑わしいファイルなどのサンプルを手動で ESET に送信するための項目を「ツール」メニューや［ツール］→［隔離］で表示される画面のコンテキストメニューに表示するかどうかの設定を行えます。既定では、この設定が有効に設定されており、「ツール」メニューをクリックして表示される項目内に［分析のためにサンプルを提出］が表示されます。また、［隔離］をクリックして、検出されたファイルを右クリックすると、コンテキストメニューに［分析のためにサンプルを提出］が表示されます。この設定を無効に設定すると、これらの項目が表示されなくなります。

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。



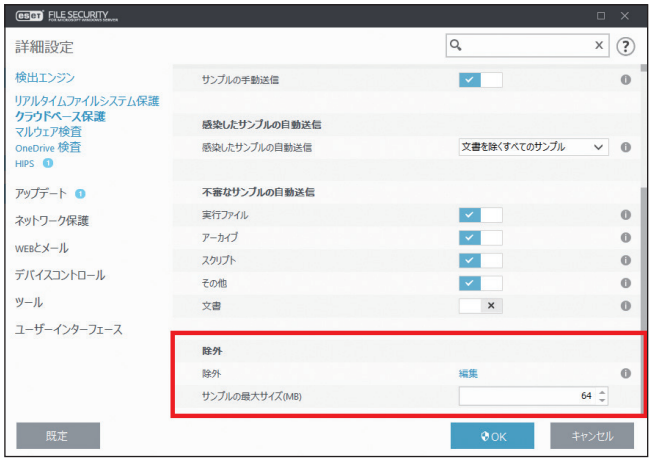
不審なサンプルの送信



「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。
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

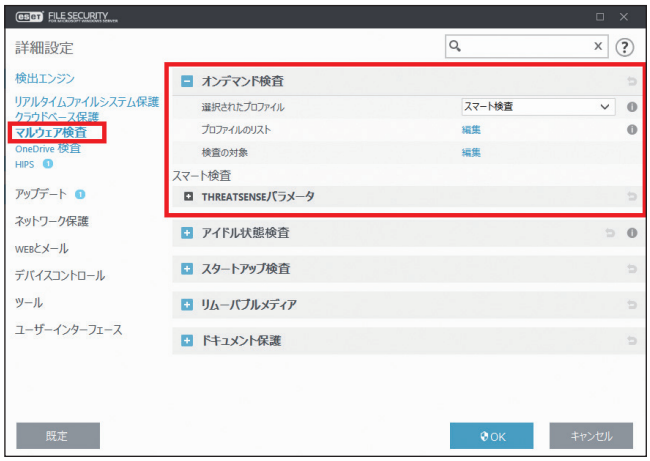


除外を使用すると、特定のファイル / フォルダーを送信から除外できます。

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。

5.1.4 マルウェア検査

「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［検出エンジン］＞［マルウェア検査］を選択します。



5.1.4.1 コンピューターの検査

選択されたプロファイル

定義済みの次の検査プロファイルを選択します。

スマート検査

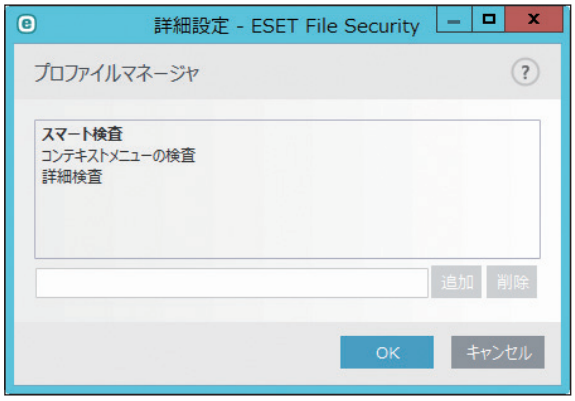
コンテキストメニューの検査

詳細検査

プロファイルのリスト

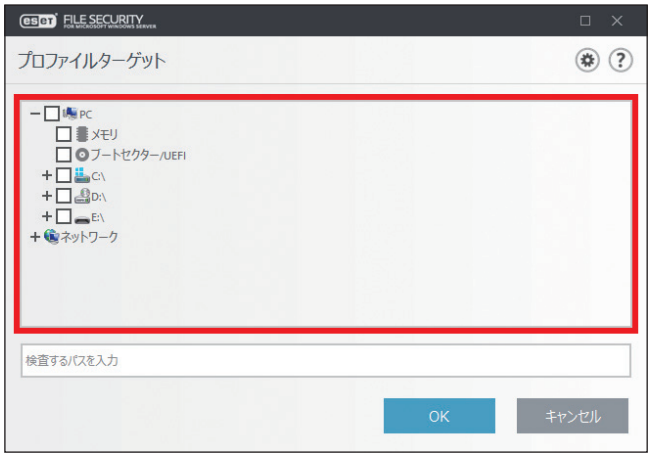
カスタム検査プロファイルを作成します。

［編集］をクリックして「プロファイルマネージャ」画面でカスタムプロファイルを追加するかプロファイルを編集します。

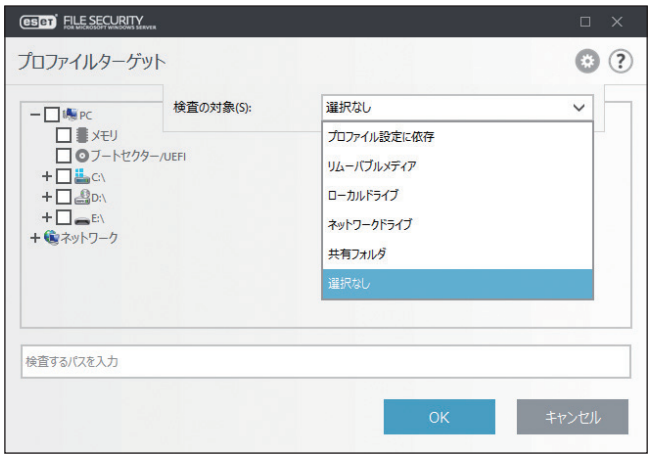


検査の対象

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］をクリックし、⚙をクリックしてドロップダウンメニューからオプションを選択するか、ツリーのフォルダーから特定の対象を選択します。



「検査の対象」画面では、検査する対象（メモリー、ドライブ、セクター、ファイル、フォルダー）を定義することができます。コンピューター上で使用できるすべてのフォルダーを表示しているツリーから対象を選択します。⚙をクリックすると表示される［検査の対象］ドロップダウンメニューでは、事前定義されている次の検査対象を選択できます。



プロファイル設定に依存	選択された検査プロファイルに設定されている対象を選択します。
リムーバブルメディア	フロッピーディスク、USB フラッシュドライブ、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。
共有フォルダ	共有されるローカルサーバー上のすべてのフォルダーを選択します。
選択なし	すべての選択を解除します。

■ THREATSENSE パラメータ

次のパラメータを設定します。



●検査するオブジェクト

システムメモリ	システムメモリ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 DBX（Outlook Express 用）、EML のファイルを検査します。
アーカイブ	一般的なアーカイブファイルを検査します。
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。

●検査オプション

ヒューリスティック	悪意あるプログラムの活動を分析します。
アドバンスド ヒューリスティック /DNA 署名	高いレベルのプログラミング言語で記述された悪意あるコードを検出します。

●駆除

感染ファイルの自動駆除、削除のモードを「駆除なし」「標準駆除」「厳密な駆除」から選択します。

●除外

拡張子は、ファイル名の一部であり、ピリオドで区切られた末尾の文字です。拡張子は、ファイルの種類と内容を規定しています。この THREATSENSE パラメータ設定では、検査するファイルの種類を指定する方法を説明します。

●その他

代替データストリーム（ADS）を検査	NTFS ファイルシステムで使用されるファイルとフォルダの関連付けである代替データストリームを検査します。
低優先でバックグラウンド検査	優先度が低い検査をバックグラウンドで実行してシステムへの負荷を減らします。
すべてのオブジェクトをログに記録する	検査したすべてのファイルを記録します。
スマート最適化を有効にする	定義済みの設定を使用して、もっとも効率的な組み合せでシステム保護を実行します。
最終アクセスのタイムスタンプを保持	検査済みの時間ではなく、元のタイムスタンプを保持します。

●制限



オブジェクトの設定

既存のオブジェクトの設定	すべてのオブジェクトを検査します。
オブジェクトの最大サイズ	検査対象のオブジェクトの最大サイズを定義します。
オブジェクトの最大検査時間	スキャナーがオブジェクトを処理する最大時間を定義します。

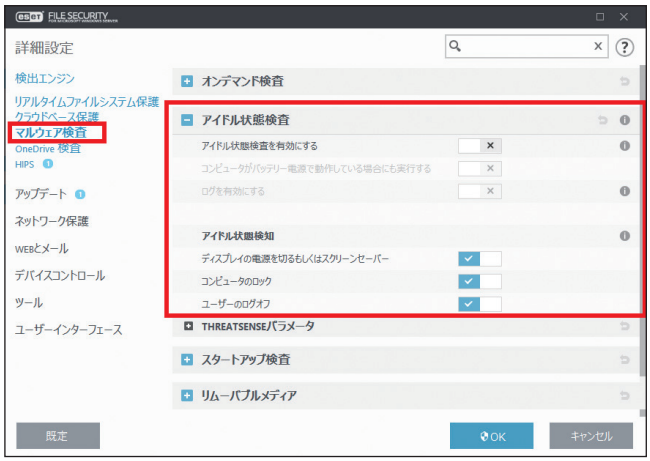
アーカイブ検査の設定

既定のアーカイブ検査の設定	最大で 10 番目のネストレベルまで検査します。実際のサイズにかかわらず検査されます。
スキャン対象の下限ネストレベル	アーカイブ検査のネストレベルを指定します。
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るファイルの最大サイズを指定します。

5.1.4.2 アイドル状態検査

■基本

「詳細設定」画面で［検出エンジン］＞［マルウェア検査］＞［アイドル状態検査］で有効 / 無効を切り替えます。クライアントコンピューターがアイドル状態になると、すべてのローカルドライブでコンピューターの検査が実行されます。



アイドル状態検査を有効にする	コンピューターがアイドル状態になると検査を開始します。
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	ノートコンピューターがバッテリーで駆動している場合でもアイドル検査を実行します。
ログを有効にする	検査ログを記録します。
アイドル状態検知	コンピューターのどの動作をアイドル状態とするかを設定します。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 / コンピュータのロック / ユーザーのログオフ状態の場合に、アイドル状態検査を実行するかどうかを各々設定します。

■ 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、「5.1.4 マルウェア検査」の「■ THREATSENSE パラメータ」を参照してください。

5.1.4.3 スタートアップ検査

既定では、自動起動ファイルの検査はシステム起動時および検出エンジンのアップデート時に実行されます。スタートアップ検査は、スケジューラおよびタスクの設定に従って行われます。スケジューラタスクの作成と管理の詳細については、「4.5.8 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。

● 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、「5.1.4 マルウェア検査」の「■ THREATSENSE パラメータ」を参照してください。

●自動スタートアップファイルのチェック

システム起動時のファイルチェックスケジュールタスクを作成するときに、次のようなパラメータを調整するオプションが用意されています。

検査対象

システム起動時に実行されるファイルの検査のレベルを指定します。ファイルは次の基準に従って昇順で整理されます。

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

次の 2 つの検査対象グループも含まれます。

ユーザーログオン前のファイル実行
ユーザーがログオンしていない状態でアクセスできる場所のファイルが含まれます（サービス、ブラウザヘルパーオブジェクト、Winlogon 通知、Windows スケジューラのエントリ、既知の dll といったスタートアップの場所にあるすべてのファイル）。

ユーザーログオン後のファイル実行
ユーザーがログオンした後にのみアクセスできる場所にあるファイル（特定のユーザーだけが実行するファイル、通常は HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run にあるファイル）が含まれます。

検査対象のファイルのリストは、上記の各グループごとに固定されます。

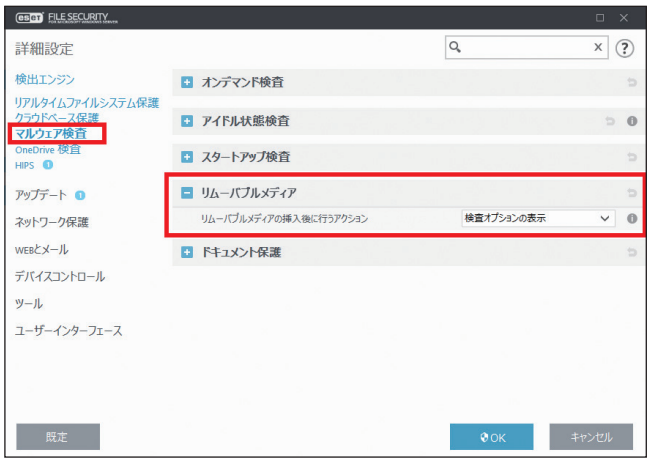
検査の優先度

検査をいつ開始するかを決定するために使用する優先度レベルには、以下のものが用意されています。

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

5.1.4.4 リムーバブルメディア

リムーバブルメディア（CD/DVD/USB メモリーなど）をコンピューターに接続すると、ESET File Security for Microsoft Windows Server はリムーバブルメディアを自動的に検査します。望ましくないファイルが格納されているリムーバブルメディア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。
「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［マルウェア検査］＞［リムーバブルメディア］を選択します。



［リムーバブルメディアの挿入後に行うアクション］でこの機能の有効 / 無効を選択します。

リムーバブルメディアの挿入後に実行するアクション

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。
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。

［検査オプションの表示］では、リムーバブルメディアを挿入すると、次のオプションが表示されます。

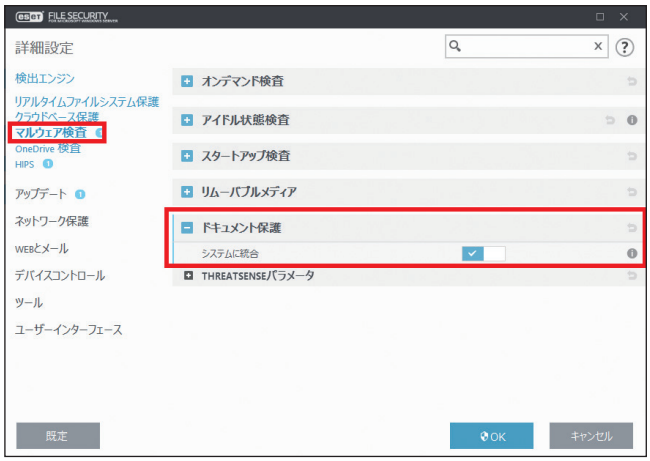
すぐに検査	リムーバブルメディアの検査を開始します。
検査しない	リムーバブルメディアの検査が延期されます。
セットアップ	「詳細設定」画面を表示します。
選択したオプションを常に使用する	チェックすると、以降コンピューターにリムーバブルメディアを接続したときに、同じアクションが実行されます。

また、ESET File Security for Microsoft Windows Server 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、「5.1.14 デバイスコントロール検査」を参照してください。

5.1.4.5 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。

「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［マルウェア検査］＞［ドキュメント保護］を選択します。ドキュメント保護機能を有効にする場合は、［システムに統合］をチェックします。



ドキュメント保護機能は、Microsoft Antivirus API を使用するアプリケーションで有効になります。

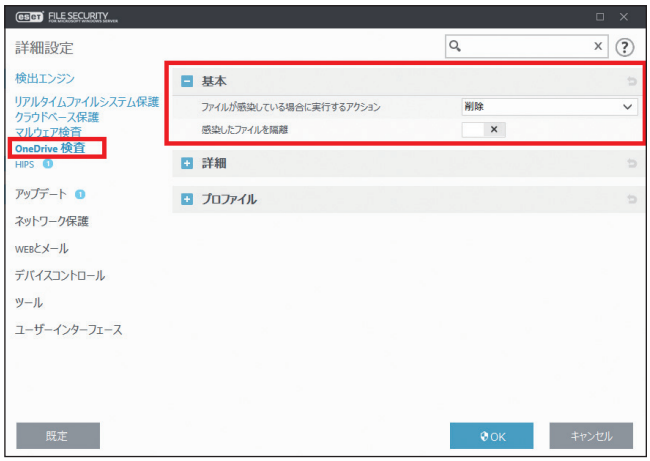
● THREATSENSE パラメータ

［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、「5.1.4 マルウェア検査」の「■ THREATSENSE パラメータ」を参照してください。

5.1.5 OneDrive 検査

OneDrive 検査では、OneDrive 検査に関する設定を行えます。「設定」画面で、［詳細設定］をクリックし、「詳細設定」画面で［OneDrive 検査］を選択します。

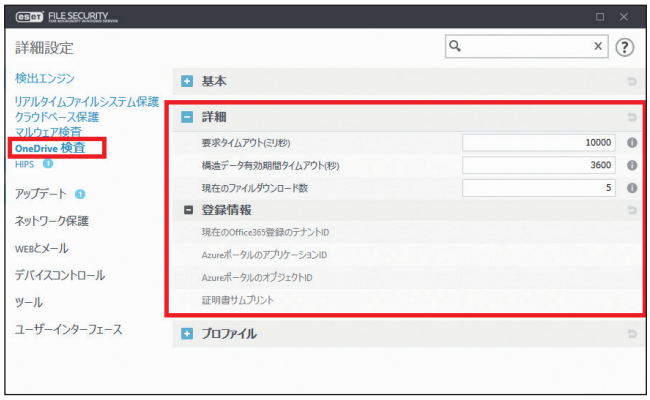
■基本



OneDrive 検査のアクションと隔離について設定できます。

ファイルが感染している場合に実行するアクション	［アクションなし］または［削除］の中からファイルが感染している場合に実行するアクションを選択できます。［アクションなし］を選択した場合、ファイルの変更は適用されません。［削除］を選択すると、ファイルを隔離に移動し、OneDrive のファイルを削除します。ただし、ファイルは、OneDrive のごみ箱にあります。
感染したファイルを隔離	有効にすると、削除に設定されたファイルは隔離に移動されます。この設定を無効にすると、ファイルは隔離に保存されません。

■詳細



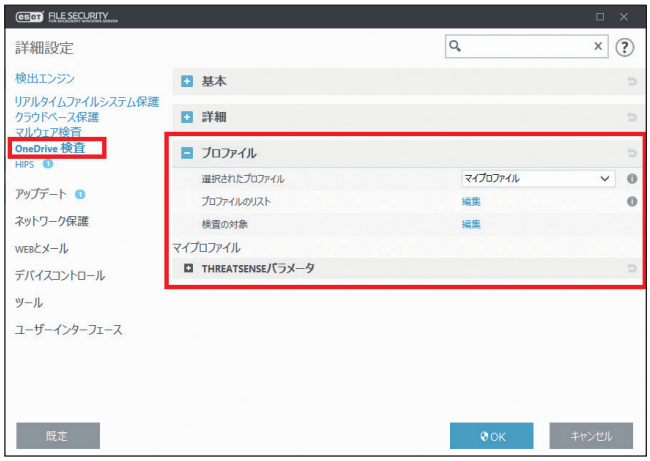
OneDrive 検査登録に関する情報の表示やタイムアウトおよび同時ダウンロード数などを設定できます。

要求タイムアウト（ミリ秒）	サーバーが OneDrive からの応答を待機する時間を設定します。この値を低く設定しすぎると、検査と構造取得が失敗する場合があります。
構造データの有効期間タイムアウト（秒）	構造データが最新であるとみなされる期間を設定します。このタイムアウトの後、再アクセスが発生した場合に構造データは再度、OneDrive から取得されます。
現在のファイルダウンロード数	OneDrive からファイルを取得するために同時ダウンロード数を設定します。この数値を増やすと、検査が高速化しますが、ネットワークトラフィックが増大する可能性があります。

●登録情報

現在の Office365 登録のテナント ID	Office365 のテナント ID が表示されます。
Azure ポータルのアプリケーション ID	Azure ポータルのアプリケーション ID が表示されます。
Azure ポータルのオブジェクト ID	Azure ポータルのオブジェクト ID が表示されます。
証明書サムプリント	証明書サムプリントが表示されます。

■プロファイル



OneDrive 検査で利用するプロファイルに関する設定を行えます。

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設定です。
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。

● THREATSENSE パラメータ

［THREATSENSE パラメータ］をクリックすると、OneDrive 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、「5.1.4　マルウェア検査」の「■ THREATSENSE パラメータ」を参照してください。

5.1.6 Hyper-V 検査

現在のバージョンの Hyper-V 検査は、Hyper-V のオンラインまたはオフライン仮想システムの検査をサポートします。Hyper-V 検査では、ホストされた Windows Hyper-V システムと仮想システムの状態によって以下のような検査をサポートしています。

Hyper-V 機能がある仮想システム	Windows Server 2008 R2 SP2 Hyper-V	Windows Server 2012 Hyper-V	Windows Server 2012 R2 Hyper-V	Windows Server 2016 Hyper-V
オンライン VM	検査なし	読み取り専用	読み取り専用	読み取り専用
オフライン VM	読み取り専用 / 駆除	読み取り専用 / 駆除	読み取り専用 / 駆除	読み取り専用 / 駆除

ハードウェア要件

サーバーには、仮想マシンを実行する際のパフォーマンスの問題がありません。検査アクティビティは、主に、CPU リソースを使用します。オンライン VM の検査では空きディスク領域が必要です。ディスク領域は、チェックポイントスナップショットと仮想ディスクで使用される領域の 2 倍以上でなければなりません。

固有の制限事項

- RAID ストレージ、スパンボリューム、および動的ディスクでの検査は、動的ディスクの性質によりサポートされていません。このため、可能なかぎり、VM で動的ディスクタイプを使用しないことをお勧めします。
- 検査は常に現在の VM で実行され、チェックポイントまたはスナップショットには影響しません。
- クラスタのホストで実行されている Hyper-V は現在 ESET File Security for Microsoft Windows Server によってサポートされていません。
- Windows Server 2008 R2 SP2 で実行されている Hyper-V ホストの仮想マシンは ThreatSense パラメーター（駆除しない）で選択された駆除レベルに関係なく、読み取り専用モードでのみ検査できます。

! 重　要

ESET File Security for Microsoft Windows Server は、仮想ディスク MBR の検査をサポートしますが、これらの対象の読み取り専用検査のみがサポートされます。この設定は、［詳細設定］（F5）>［検出エンジン］>［Hyper-V 検査］>［ThreatSense パラメーター］>［ブートセクター］で変更できます。

検査対象の仮想マシンがオフライン - オフ状態に切り替わりました

ESET File Security for Microsoft Windows Server は、Hyper-V Management を使用して、仮想ディスクを検出して接続します。このように、ESET File Security for Microsoft Windows Server には、汎用ドライブのデータとファイルにアクセスする場合のように、仮想ディスクの内容にアクセスできます。

検査対象の仮想マシンがオンライン - 実行中、一時停止、保存状態

ESET File Security for Microsoft Windows Server は Hyper-V Management を使用して、仮想ディスクを検出します。これらのディスクへの実際の接続はできません。このため、ESET File Security for Microsoft Windows Server は、仮想マシンのチェックポイント / スナップショットを作成してから、チェックポイント / スナップショットに接続します。検査が完了したら、チェックポイント / スナップショットは削除されます。つまり、読み取り専用検査は、実行中の仮想マシンが検査アクティビティの影響を受けないため、実行できます。

ESET File Security for Microsoft Windows Server が、検査中にスナップショットまたはチェックポイントを作成するには最大 1 分かかります。多数の仮想マシンで Hyper-V 検査を実行するときには、この点を考慮してください。

命名規則

Hyper-V 検査のモジュールは次の命名規則に従います。

VirtualMachineName¥DiskX¥VolumeY

X はディスク数、Y はボリューム数です。

例 :
Computer¥Disk0¥Volume1

数字のサフィックスは、VM のディスクマネージャに表示される順序と同じ検出順で、追加されます。この命名規則は、検査対象のツリー構造リスト、進行状況バー、ログファイルで使用されます。

検査の実行

- オンデマンド
  ［Hyper-V 検査］をクリックすると、検査可能な仮想マシンおよびボリュームのリストが表示されます。検査する仮想マシン、ディスク、またはボリュームを選択し、検査をクリックします。
- スケジューラータスクを作成
- ESET Security Management Center の「サーバー検査」クライアントタスクを使用
- eShell 経由での管理および開始

複数の Hyper-V 検査を同時に実行できます。検査が完了したときには、ログファイルへのリンクが付いた通知を受信します。

想定される問題

- オンライン仮想マシンの検査を実行するときには、特定の仮想マシンのチェックポイント / スナップショットを作成する必要があります。チェックポイント / スナップショットの作成中には、仮想マシンの一部の汎用処理が制限または無効化される場合があります。
- オフライン仮想マシンの検査中は、検査が完了するまでオンにできません。
- Hyper-V Manager では、2 つの異なる仮想マシンに同じ名前を指定できるため、検査ログの確認中にコンピュータを識別できない場合があります。

5.1.7 HIPS

! 重 要

HIPS 設定の変更は、経験豊富なユーザーのみが行ってください。HIPS の設定を誤ると、システムが不安定になる可能性があります。

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。「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［検出エンジン］＞［HIPS］を選択します。

■基本



HIPS を有効にする / 自己防衛を有効にする

ESET File Security for Microsoft Windows Server 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壊されたり無効化されたりしないようにする、自己防衛技術が組み込まれています。これにより、システムは常時確実に保護されます。［HIPS を有効にする］と［自己防衛を有効にする］で変更した内容は、コンピューターの再起動後に有効になります。HIPS システム全体を無効にする場合にも、コンピューターの再起動が必要になります。

保護されたサービスを有効にする

Microsoft は、Microsoft Windows Server 2012 R2 で保護されたサービスの概念を導入しました。これにより、マルウェア攻撃に対するサービスが防止されます。ESET File Security for Microsoft Windows Server のカーネルは、既定で保護されたサービスとして実行されます。この機能は、Microsoft Windows Server 2012 R2 以降のサーバーオペレーティングシステムで利用できます。

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からの保護を強化します。既定では、有効に設定されています。詳細については、「6.1.11 詳細メモリ検査（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

「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します。既定では、有効に設定されています。詳細については、「6.1.10 エクスプロイトブロック」を参照してください。

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、「6.1.8 ランサムウェア」を参照してください。

フィルタリングモード

フィルタリングモードは、次の 5 つのいずれかで実行できます。

ルール付き自動モード	システムを保護するための定義済みルールを除いて、すべての操作が有効です。ルールで拒否されたアクションを除くすべてが許可されます。
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	ユーザールール／定義済み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、ルール付き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。この設定は、フィルタリングモードに「学習モード」を選択した場合に表示されます。

HIPS ルールの設定

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、パーソナル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。ルール作成および HIPS 操作の詳細については、「HIPS ルールの追加・編集」を参照してください。

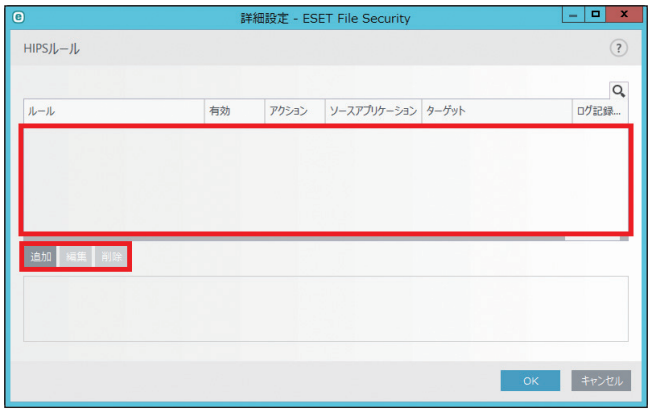
ルールのアクションを［確認］にした場合は、ルールに適合するたびに確認画面が表示され、ユーザーは操作を［遮断］するか［許可］するかを選択できます。指定された時間内にアクションを選択しなかった場合は、ルールに基づいて新しいアクションが選択されます。

確認画面では、HIPS が検出した新しいアクションを基にルールを作成します。「詳細表示」をクリックすると、そのアクションを許可またはブロックする条件を定義できます。この方法で作成したルールは手動で作成したルールと同等にみなされます。そのため、確認画面から作成したルールは、この画面を表示させたルールよりも汎用的なルールになることがあります。つまり、ルール作成後に同じ操作をした際、同じ確認画面が表示されることがあります。

［このプロセスに対するアクションを一時的に記憶する］では、ルールまたはフィルタリングモードの変更、HIPS モジュールの更新、またはシステムの再起動まで、同じアクション（許可／遮断）が使用されます。これら 3 つのアクションのいずれかが実行された後は、一時的なルールは削除されます。

● HIPS ルール画面

この画面には、設定されている HIPS ルールが表示されます。



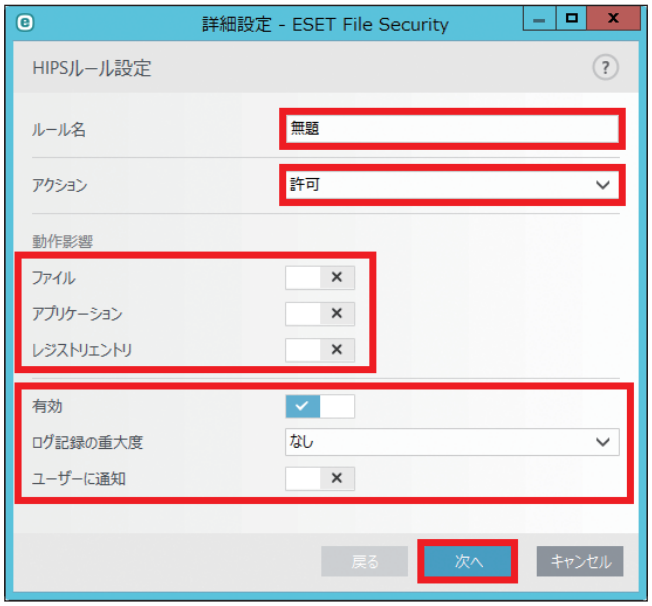
ルール	ユーザーが設定した名前、または自動選択されたルール名が表示されます。
有効	ルールの有効／無効を切り替えます。無効にした場合もルールはリストに残ります。
アクション	条件が一致した場合に実行するアクションを［許可］、［ブロック］、［確認］から指定します。
ソースアプリケーション	このアプリケーションによってイベントが起動された場合のみ、ルールが使用されます。
ターゲット	操作が定義されたターゲット（ファイル、アプリケーション、レジストリエントリー）に関連付けられている場合にのみ、このルールが使用されます。
ログ記録の重大度	このルールに関する情報を HIPS ログに記録します。
通知	イベントが起動された場合に、ポップアップが画面の右下隅に表示されて通知します。

画面のボタンでは次の操作ができます。

追加	新しいルールを追加して作成します。
編集	選択したエントリーを編集します。
削除	選択したエントリーを削除します。

HIPS ルールの追加・編集

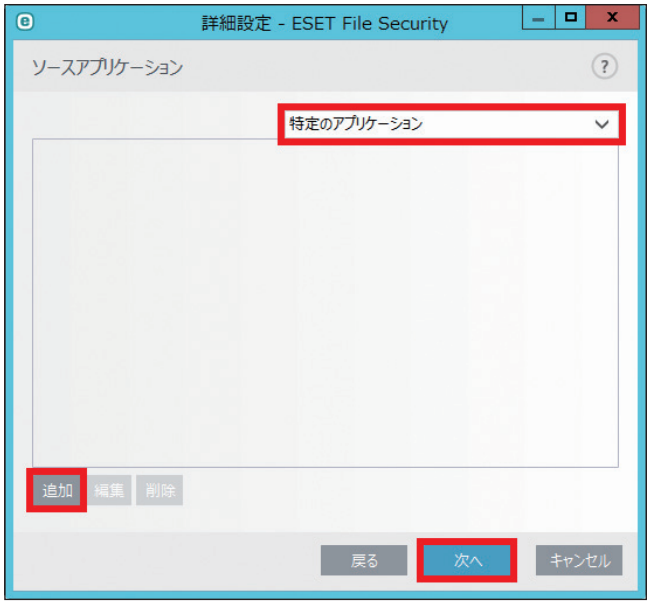
［追加］または［編集］をクリックして、次の画面で詳細を設定します。



ルール名	ユーザーが設定した名前、または自動選択されたルール名が表示されます。
アクション	ルールの条件が一致した場合に実行するアクションを［許可］、［ブロック］、［確認］から指定します。
動作影響	ルールが適用される対象を選択します。
ファイル	ルールは、操作がファイルと関連する場合に限り使用されます。設定ウィザードの「ファイル」画面のドロップダウンメニューから特定のファイルを選択し、［追加］をクリックして、新しいファイルまたはフォルダーを選択します。または、ドロップダウンメニューから［すべてのファイル］を選択してすべてのファイルを追加します。
アプリケーション	ルールは、アプリケーションによってイベントが起動された場合に限り使用されます。設定ウィザードの「アプリケーション」画面ドロップダウンメニューから特定のアプリケーションを選択し、［追加］をクリックして、新しいファイルまたはフォルダーを選択します。または、ドロップダウンメニューから［すべてのアプリケーション］を選択してすべてのアプリケーションを追加します。 ※「ソースアプリケーション」画面についても、この「アプリケーション」画面と同様に操作します。
レジストリエントリ	ルールは、操作がレジストリエントリーと関連する場合に限り使用されます。設定ウィザードの「レジストリエントリ」画面ドロップダウンメニューから［指定したエントリ］を選択し、［追加］をクリックして、新しいファイルまたはフォルダーを選択します。または、ドロップダウンメニューから［すべてのエントリ］を選択してすべてのエントリーを追加します。
有効	ルールの有効／無効を切り替えます。無効にした場合もルールはリストに残ります。
ログ記録の重大度	このルールに関する情報を HIPS ログに記録します。
ユーザーに通知	イベントが起動された場合に、ポップアップが画面の右下隅に表示されて通知します。

設定が終わったら［次へ］をクリックします。

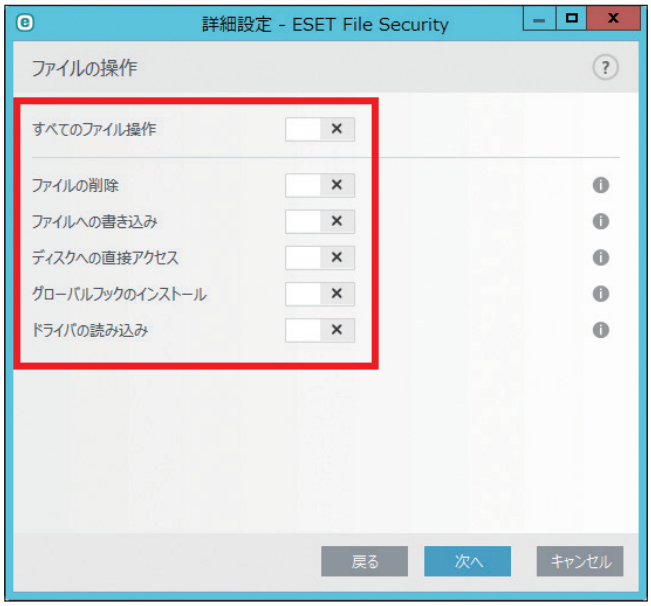
ソースアプリケーションの選択



対象となるソースアプリケーションを選択します。
「すべてのアプリケーション」または「特定のアプリケーション」を選択します。
「特定のアプリケーション」を選択した場合は［追加］をクリックしてアプリケーションを追加します。
設定したら［次へ］をクリックします。

ファイルの操作

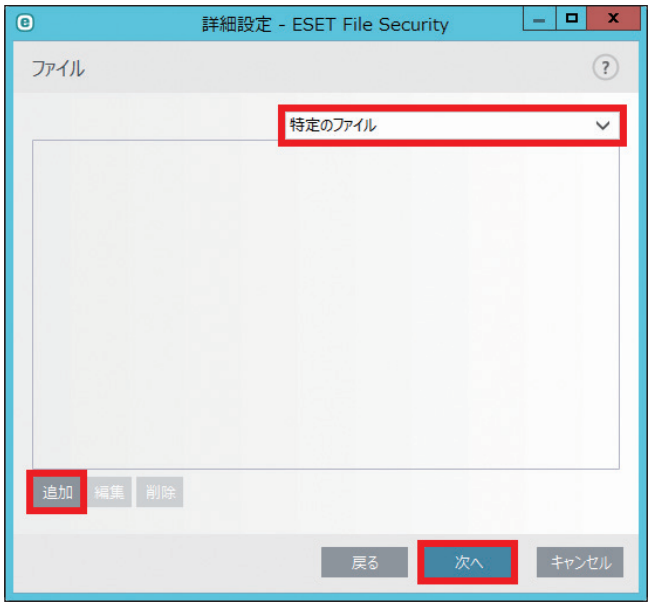
対象となるファイル操作を選択します。



すべてのファイル操作	すべてのファイル操作に対してルールが適用されます。
すべてのファイルの削除	アプリケーションはターゲットファイルを削除する場合にルールが適用されます。
ファイルへの書き込み	アプリケーションはターゲットファイルに書き込む場合にルールが適用されます。
ディスクへの直接アクセス	アプリケーションが Windows の標準的でない方法で、ディスクからの読み取りまたは書き込みを行おうとした場合にルールが適用されます。ディスクへの直接アクセスにより、対応するルールの適用されずにファイルが変更される場合があります。この動作は、マルウェアが検知されるのを逃れようとしたり、バックアップソフトウェアがディスクの正確なコピーを作成しようとしたり、またはパーティションマネージャーがディスクボリュームを認識しようとすることで引き起こされる場合があります。
グローバルフックのインストール	MSDN ライブラリーからの SetWindowsHookEx 関数の呼び出しに対してルールが適用されます。
ドライバの読み込み	システムへのドライバーのインストールと読み込みに対してルールが適用されます。

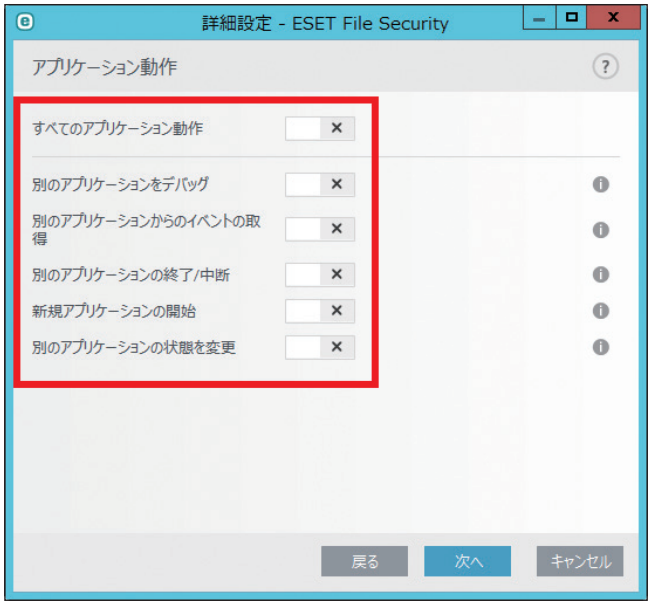
設定が終わったら［次へ］をクリックします。

ファイルの選択



対象となるファイルを選択します。
「すべてのファイル」または「特定のファイル」を選択します。
「特定のファイル」を選択した場合は［追加］をクリックしてファイルを追加します。
設定したら［次へ］をクリックします。

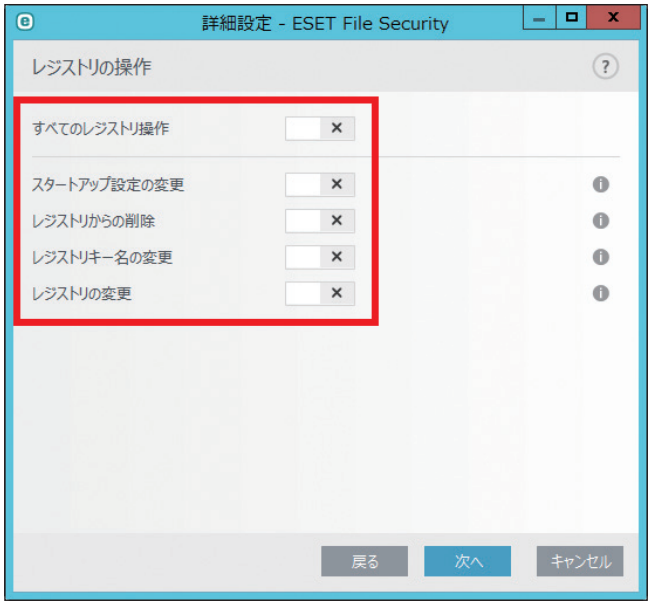
アプリケーション動作



すべてのアプリケーション動作	すべてのアプリケーション動作に対してルールが適用されます。
別のアプリケーションをデバッグ	デバッガをプロセスに追加します。アプリケーションのデバッグ中にそのアプリケーションの動作の詳細を表示して変更し、そのデータにアクセスする場合にルールが適用されます。
別のアプリケーションからのイベントの取得	ソースアプリケーションは、別のアプリケーションを対象としたイベントを取得しようとする場合にルールが適用されます（キーロガーがブラウザーのイベントのキャプチャーを試みるなど）。
別のアプリケーションの終了 / 中断	別のアプリケーションの中断、再開、終了の場合にルールが適用されます（Process Explorer または Processes ペインから直接アクセス可能）。
新規アプリケーションの開始	新しいアプリケーションまたはプロセスの開始の場合にルールが適用されます。
別のアプリケーションの状態を変更	ソースアプリケーションは、ターゲットアプリケーションのメモリーに書き込みを試みているか、代わりにコードを実行しようとしています。重要なアプリケーションをターゲットアプリケーションとして設定することによって保護する場合にルールが適用されます。

設定が終わったら［次へ］をクリックします。

レジストリの操作



すべてのレジストリ操作	すべてのレジストリ操作に対してルールが適用されます。
スタートアップ設定の変更	スタートアップ設定（Windows 起動時に実行するアプリケーションの定義）の変更時にルールが適用されます。
レジストリからの削除	レジストリキーまたはその値を削除した場合にルールが適用されます。
レジストリキー名の変更	レジストリキーの名前を変更した場合にルールが適用されます。
レジストリの変更	レジストリキーの値の変更、新しい値の作成、データベースツリー内のデータの移動、またはレジストリキーのユーザー権限、またはグループ権限の設定を行った場合にルールが適用されます。

設定が終わったら［次へ］をクリックします。

レジストリエントリ



対象となるレジストリのエントリを選択します。
「すべてのエントリ」または「指定したエントリ」を選択します。
「指定したエントリ」を選択した場合は［追加］をクリックしてレジストリエントリのキーをを追加します。
［レジストリエディタを開く］をクリックすると、Windows のレジストリエディターを起動して、キーを選択することもできます。
設定したら［終了］をクリックして HIPS ルールの作成を終了します。

! 重　要

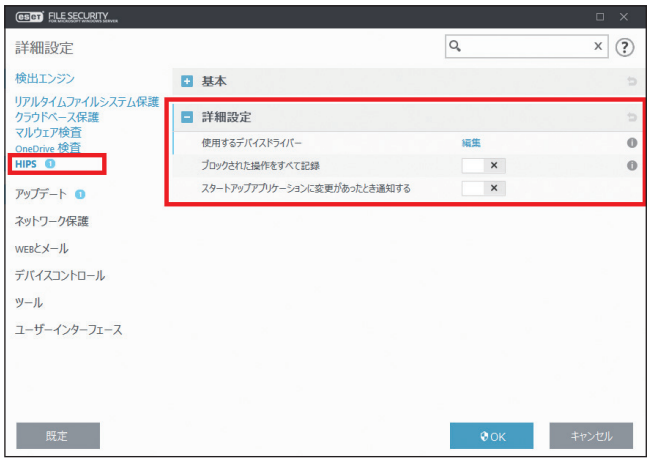
ターゲットの入力では、一定の制限付きでワイルドカードを使用できます。レジストリのパス内では、特定のキーの代わりに「*」（アスタリスク）記号を使用できます。例えば、「HKEY_USERS*\software」は、「HKEY_USER\.default\software」とは一致しますが、「HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software」とは一致しません。
「HKEY_LOCAL_MACHINE\system\ControlSet*」は、有効なレジストリキーパスではありません。「*」の入ったレジストリ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

! 重　要

一般的すぎるルールを作成すると、これに対する警告が表示されます。

■詳細設定

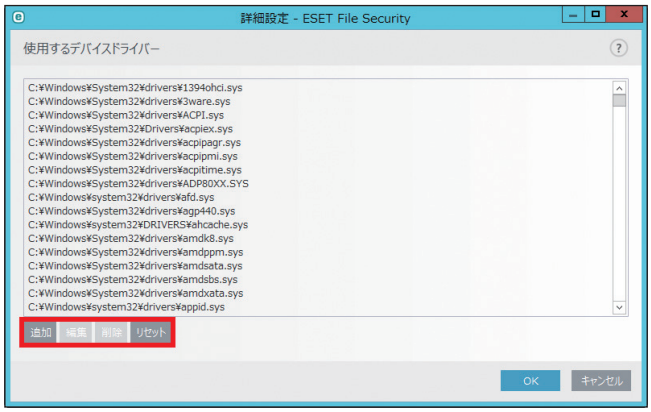
アプリケーションの動作をデバッグ、分析するための設定をします。



使用するデバイスドライバー	ユーザールールで明確に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。 ［編集］をクリックすると「使用するデバイスドライバー」を追加、編集できます（下記参照）。
ブロックされた操作をすべて記録	ブロックされたすべての操作が HIPS ログに記録されます。
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、デスクトップ通知を表示します。

使用するデバイスドライバー

明確にユーザールールでブロックされている場合を除き、このリストに表示されるドライバーは、HIPS フィルタリングモードに関係なく、常に使用されます。



この画面では次の操作が実行できます。

追加	新しいドライバーを追加します。
編集	選択したドライバーのパスを編集します。
削除	ドライバーをリストから削除します。
リセット	システムドライバーを再度読み込みます。

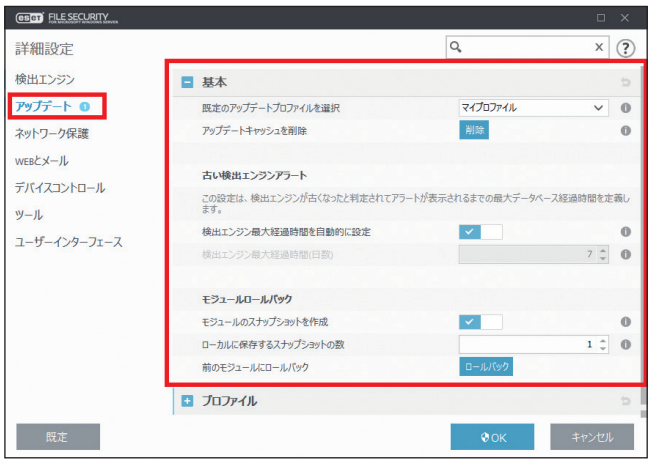
ワンポイント

手動で追加したドライバーを一括で削除する場合は、[リセット] をクリックします。これは、複数のドライバーを追加し、手動でリストから削除できない場合に有効です。

5.1.8 アップデート

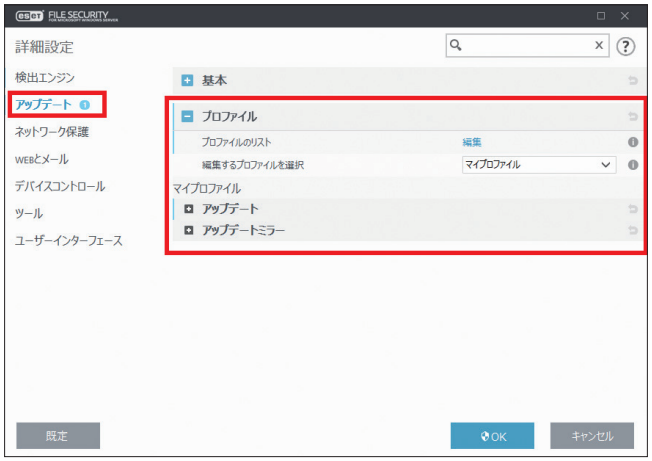
アップデートサーバーやそれらのサーバーの認証データなど、アップデートファイルの送信元の情報を指定します。「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［アップデート］を選択します。

■基本



規定のアップデートプロファイルを選択	使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。	
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。	
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「2」、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。

■プロファイル



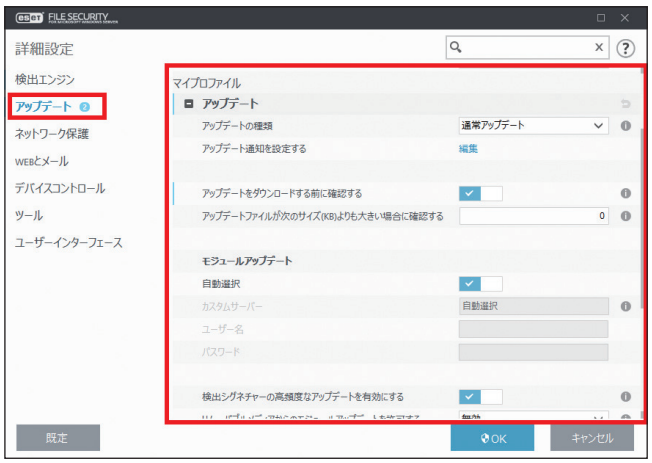
プロファイルのリスト	プロファイルの追加や削除ができます。新しいプロファイルを作成するには、［編集］リンクをクリックし、空白フィールドにプロファイル名を入力して、［追加］をクリックします。
編集するプロファイルを選択	設定を編集するプロファイルを選択します。

！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入力することが重要です。ファイアウォールを設定している場合は、ESET プログラムのインターネット通信（HTTP 通信）が許可されていることを確認してください。
既定では、［基本］タブの［アップデートの種類］が［通常アップデート］に設定されています。アップデートファイルは、最低限のネットワークトラフィックで ESET サーバーから自動的にダウンロードされます。

以下の項目でマイプロファイルの設定ができます。

●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。
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。

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 社のアップデートサーバーを使用するときには、既定のままにします。

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、手動でアップデートサーバーを指定します。

ミラーサーバーにアクセスする基本的な方法は 2 つあります。アップデートファイルを保存した共有ネットワークフォルダーにアクセスする方法とクライアントが HTTP サーバー上にあるミラーにアクセスする方法です。

- 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。

!重 要

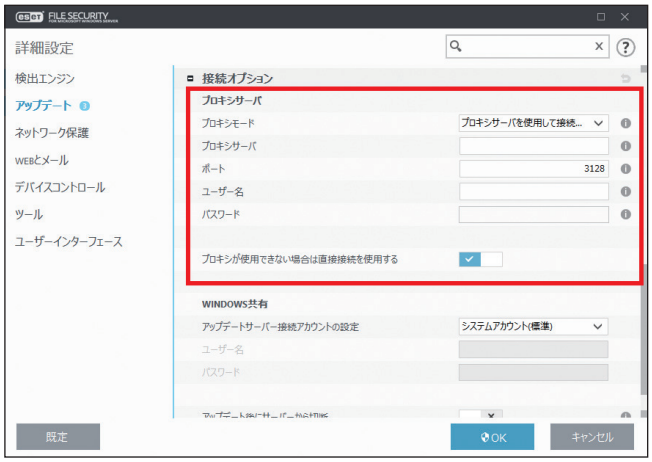
プログラムコンポーネントのアップデートを利用するためには、ESET 社のリポジトリサーバーに接続できる環境が必要です。ミラーサーバーからモジュールをアップデートする設定にしていても、プログラムコンポーネントのアップデートを利用するために、ESET 社のリポジトリサーバーに接続できる必要があります。必要に応じてプロキシサーバーの設定を行ってください。
また、プログラムコンポーネントアップデートはプログラムのアップデート後は再起動が必要になるため、ESET File Security for Microsoft Windows Server の運用環境に応じてアップデートモードを設定してください。

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 に変更がある場合、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

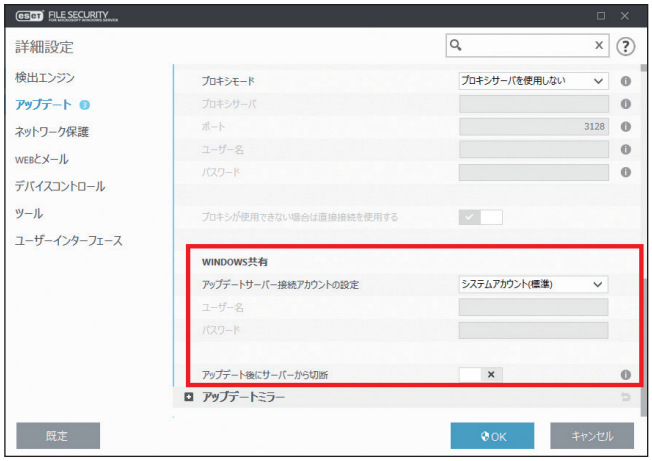


プロキシモード	プロキシサーバを使用しない	アップデートにプロキシサーバーを使用しません。
	プロキシサーバを使用して接続する	アップデートにプロキシサーバーを使用します。選択すると「カスタムプロキシサーバー」の設定項目が有効になるので、必要に応じて、プロキシサーバー、ポート（既定は「3128」）、ユーザー名、パスワードを設定します。また、［プロキシが利用できない場合は直接接続を使用する］を有効に設定すると、アップデート時に設定したプロキシサーバーが利用できない場合に、プロキシサーバーをバイパスしてアップデートします。 プロキシサーバーは、次のような場合に設定します。 • 「詳細設定」画面の［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 File Security for Microsoft Windows Server 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。
	プロキシが使用できない場合は直接接続を使用する	プロキシサーバーに接続できない場合は、プロキシサーバーをバイパスして直接 ESET 社のアップデートサーバーと通信します。

! 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 File Security for Microsoft Windows Server 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 File Security for Microsoft Windows Server 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。	

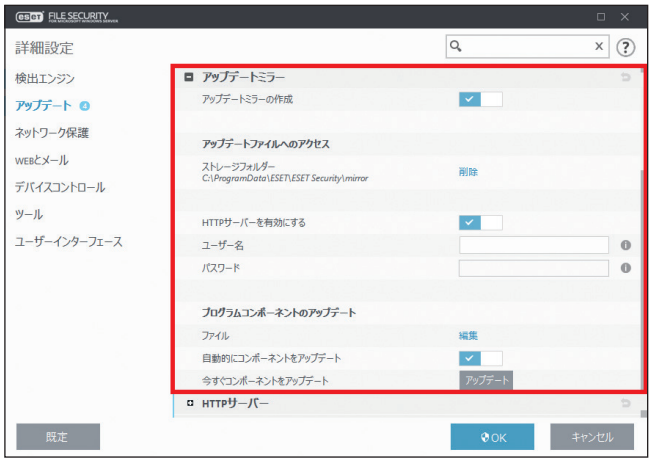
●アップデートミラー

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。

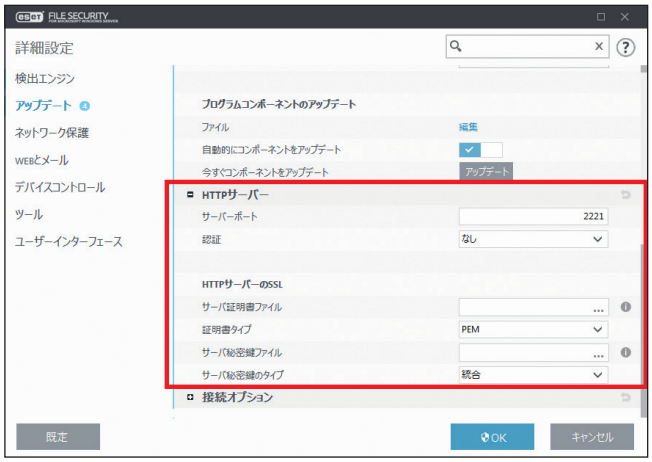
「詳細設定」画面で［アップデート］>［プロファイル］>［アップデートミラー］をクリックすると、「アップデートミラーの作成」画面が表示されます。



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 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。

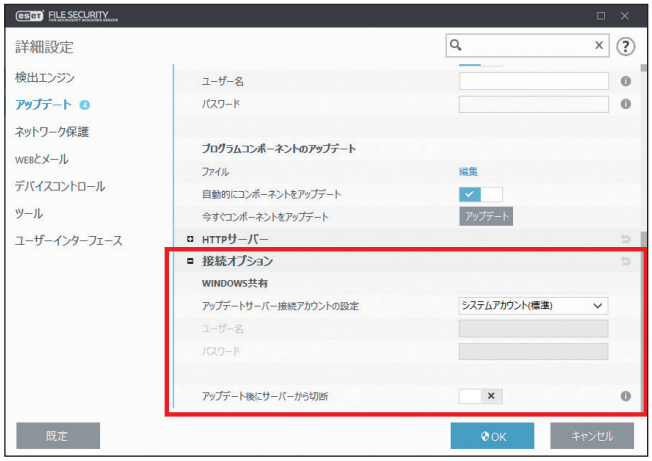
HTTP サーバー

「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 File Security for Microsoft Windows Server 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。

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 File Security for Microsoft Windows Server 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。

5.1.8.1 アップデートのロールバック

モジュールロールバックを行う場合、検出エンジンおよびプログラムモジュールアップデートを一時停止する期間を指定する時間間隔をドロップダウンメニューから選択する必要があります。



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

検出エンジンのバージョンは最も古いものにダウングレードされて、ローカルのコンピューターファイルシステムにスナップショットとして保存されます。

5.1.8.2 スケジュールタスク - アップデート

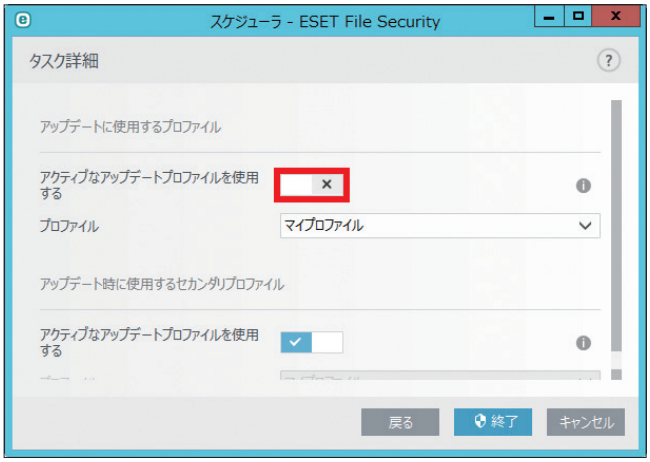
2 つのアップデートサーバからプログラムをアップデートする場合、2 つの異なるアップデート用プロファイルを作成する必要があります。最初のサーバでアップデートファイルのダウンロードに失敗すると、自動的に次のサーバに切り替えられます。これは、通常はローカル LAN のアップデートサーバーからアップデートを行っているが、別のネットワークからインターネットに接続することも多いノートパソコンなどに最適です。その場合、最初のプロファイルが失敗すると、次のプロファイルが自動的に ESET のアップデートサーバーからアップデートファイルをダウンロードします。

操作手順

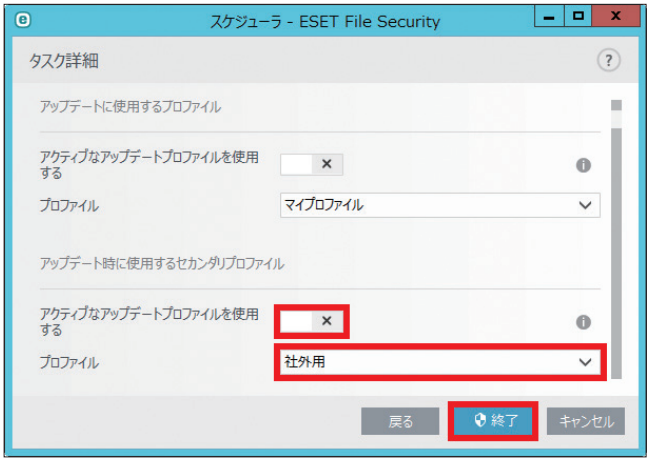
1. アップデート用のプロファイルを 2 つ以上作成しておきます。
2. ［ツール］>［スケジューラ］とクリックし、スケジューラを表示します。
3. ［定期的に自動アップデート］のアップデートタスクをクリックし、［編集］をクリックします。

続く

4 スケジュールの設定を行っていき、「タスク詳細」画面が表示されたら、「アクティブなアップデートプロファイルを使用する」の をクリックして にしてアップデートで使用する 1 つ目のプロファイルを選択します。



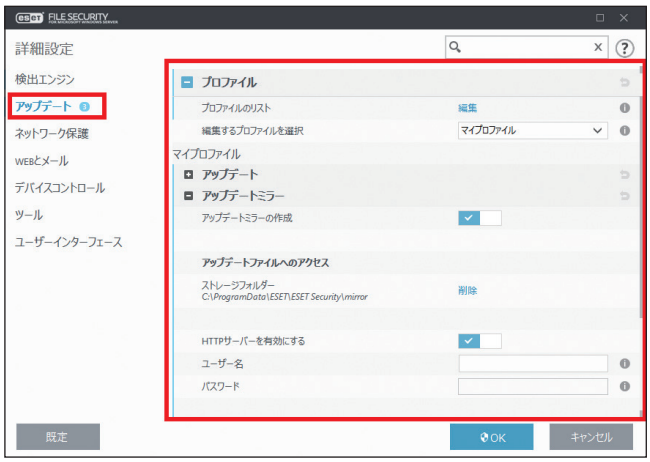
5 もう 1 つの「アクティブなアップデートプロファイルを使用する」の をクリックして にしてアップデートで使用する 2 つ目のプロファイルを選択します。



6 [終了] ボタンをクリックして、タスクを適用します。

5.1.8.3 配布用アップデート

LAN 環境でミラーサーバーにアップデートファイルを置くと、クライアントコンピューターごとに ESET 社のアップデートサーバーからアップデートファイルをダウンロードしないため、ネットワークの負荷を軽減することができます。クライアントワークステーションでミラーを作成するには、「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] とクリックし、[アップデートミラーの作成] を有効にします。これにより、アップデートファイルへのアクセス方法やミラーファイルへのパスなど、他のミラー設定オプションが有効になります。



ミラーファイルの保存先の指定

ミラーのアップデートファイルを保存するフォルダーは、[ストレージフォルダー] で指定します。保存先は既定では C ドライブの「/ProgramData/ESET/ESET Security/mirror」に指定されています。変更する場合は [削除] をクリックした後 [編集] をクリックして新たに指定します。指定したフォルダーの認証が必要な場合は、[ユーザー名] と [パスワード] を入力して認証データを指定します。選択した保存先フォルダーが、ネットワークディスクにある場合、選択したフォルダーに対する書き込み権限があるユーザー名とパスワードを指定する必要があります。ユーザー名は、<ドメイン> / <ユーザー> または <ワークグループ> / <ユーザー> という形式で入力します。対応するパスワードを必ず指定してください。

HTTP サーバーを有効にする

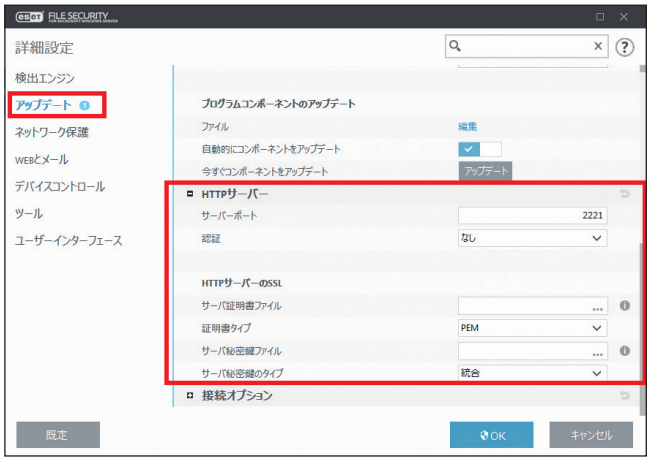
内部 HTTP サーバーを利用してアップデートファイルの配布を行う場合は、「HTTP サーバーを有効にする」の設定を有効にします。また、必要に応じて、ユーザー名やパスワードを設定します。

プログラムコンポーネントのアップデート

ここでは、プログラムコンポーネントのアップデートについて以下の設定を行います。

ファイル	ミラーを構成するときには、ダウンロードするアップデートの言語バージョンを設定できます。[編集] をクリックすると、この設定を行えます。
自動的にコンポーネントをアップデート	プログラムコンポーネントのアップデートにより、新しい機能のインストールと、既存の機能の更新を行うことができます。自動的にアップデートが実行されるようにすることもできますが、アップデートするかどうかをユーザーが確認するように設定することもできます。プログラムコンポーネントのアップデートファイルをインストールした後は、再起動が必要になることがあります。
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



内部 HTTP サーバーを利用する場合のポート番号や認証、SSL の設定などを行います。以下の項目について設定を行えます。

サーバーポート	既定のポートは 2221 に設定されています。別のポートを使用している場合は、この値を変更します。	
認証	アップデートファイルにアクセスするために使用される認証方法を［なし］［基本］［NTLM］の中から設定します。	
	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は、このオプションを選択します。
	NTLM	このオプションを選択すると、安全なエンコード方法でエンコードされます。認証については、アップデートファイルを共有するワークステーション上で作成されたユーザーが使用されます。
	なし	既定の設定です。認証なしでアップデートファイルにアクセスできます。

！重　要

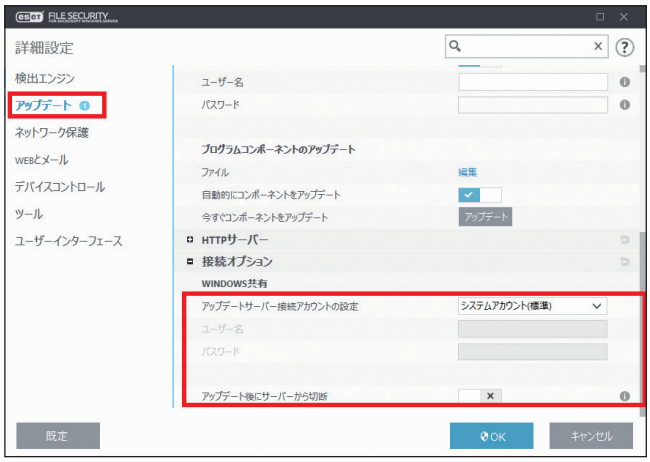
HTTP サーバー経由によるアップデートファイルへのアクセスを許可する場合、ミラーフォルダーは、ミラーフォルダーを作成する ESET File Security for Microsoft Windows Server のインスタンスと同じコンピューターに置かれている必要があります。

HTTP サーバーの SSL

HTTPS（SSL）サポートを使用した HTTP サーバーを実行する場合、「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。証明書タイプは ASN、PEM、PFX が使用できます。セキュリティが強化された HTTPS プロトコルを使用してアップデートファイルをダウンロードできます。HTTPS プロトコルを使用したデータ転送やログイン資格情報を追跡するのはほぼ不可能とされています。既定では、［サーバ秘密鍵のタイプ］は［統合］に設定されています。秘密鍵は選択した証明書チェーンファイルの一部です。

●接続オプション

この項目では次の内容を設定できます。



WINDOWS 共有

「アップデートサーバー接続アカウントの設定」のドロップダウンメニューから［システムアカウント（標準）］、［現在のユーザー］、［指定したユーザー］のオプションを選択できます。ユーザー名とパスワードの設定はオプションです。

アップデートファイルをダウンロードした後もサーバーとの接続がアクティブとなる場合は、［アップデート後にサーバから切断］を有効にして強制的に切断します。

■クライアントコンピューターでのアップデートミラーの設定

アップデートミラーの設定後、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を追加する必要があります。手順は次のとおりです。

操作手順

1. ［詳細設定］＞［アップデート］＞［プロファイル］＞［アップデート］をクリックします。
2. モジュールアップデートの［自動選択］をオフにし、次のいずれかの形式で、［カスタムサーバー］のテキストボックスに新しいサーバーを追加します。
   - http:// ＜サーバーの IP アドレス＞ :2221
   - https:// ＜サーバーの IP アドレス＞ :2221（SSL を使用する場合）

システム共有を使用したアップデートミラーへのアクセス

まず、ローカルデバイスまたはネットワークデバイスに共有フォルダーを作成します。アップデートミラーのフォルダーを作成する際には、アップデートファイルをミラーフォルダーに保存するユーザーに「書き込み」アクセス権を付与します。また、ミラーフォルダーから ESET File Security for Microsoft Windows Server をアップデートするすべてのユーザーに「読み取り」アクセス権を付与します。

次に、「詳細設定」画面から［アップデート］＞［プロファイル］＞［アップデートミラー］＞［アップデートミラーの作成］にアクセスし、［HTTP サーバーを有効にする］のチェックを外します。プログラムのインストールパッケージでは、このチェックボックスは既定でチェックされています。

共有フォルダーがネットワーク内の別の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へのアクセスに使用する認証データを入力する必要があります。認証データを入力するには、「詳細設定」＞［アップデート］＞［プ

ロファイル］＞［アップデート］＞［接続オプション］＞［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。

アップデートミラーの設定が完了した後、次の手順を使用して、クライアントコンピューターでアップデートサーバーとして ¥¥UNC¥PATH 形式でパスを設定します。

操作手順

1. ［詳細設定］＞［アップデート］＞［プロファイル］＞［アップデート］をクリックします。
2. モジュールアップデートの［自動選択］をオフにします。
3. ［アップデートサーバー］をクリックし、¥¥UNC¥PATH 形式を使用して新しいサーバーを追加します。

！重　要

アップデートが正しく動作するには、ミラーフォルダーのパスを 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からのアップデートは正しく動作しない場合があります。

●ミラーアップデートの問題のトラブルシューティング

ミラーサーバーからのアップデート中に発生する問題は、次の原因である可能性があります。

- ミラーフォルダーオプションの指定が正しくない
- ミラーフォルダーへの認証データが正しくない
- ミラーからアップデートファイルをダウンロードするローカルワークステーションの設定が正しくない

以下では、ミラーからのアップデート時に発生する可能性がある、よくある問題の概要を紹介します。

ミラーサーバーへの接続エラーが報告される

原因として、ローカルワークステーション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 のスタートボタンをクリックし、［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］をクリックします。次に、フォルダーパスを入力して、［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てください。

ユーザー名とパスワードが要求される

原因として、［アップデート］の項目で認証データ（ユーザー名とパスワード）が正しく入力されていないことが考えられます。ユーザー名とパスワードは、プログラムのアップデート元のアップデートサーバーへのアクセスを許可するために使用されます。認証データが適切な形式で正しく入力されていることを確認してください。例えば、＜ドメイン＞／＜ユーザー名＞または＜ワークグループ＞／＜ユーザー名＞とそれに対応するパスワードを入力します。「すべてのユーザー」がミラーサーバ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。この場合、アップデートの設定セクションでドメインユーザー名とパスワードを入力する必要があります。

ミラーサーバーへの接続エラーが報告される

ミラーの HTTP バージョンへのアクセスについて、定義されているポート上の通信がブロックされています。

●アップデートタスクの作成方法

アップデートを手動で開始するには、メインメニューの［アップデート］＞［今すぐアップデート］をクリックします。

アップデートは、スケジューラでタスクとしてあらかじめ登録して実行することができます。スケジュールされたタスクとして設定するには、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。既定では、次のタスクが有効になっています。

- 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

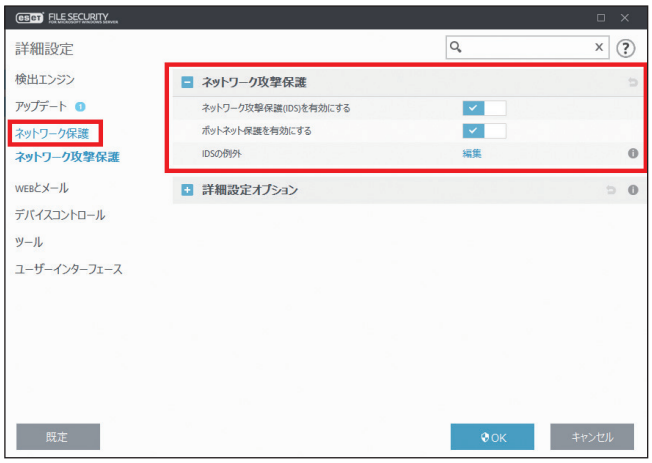
各アップデートタスクは、ユーザーのニーズに合わせて設定を変更することができます。また、既定のアップデートタスクとは別に、ユーザー定義の設定で新しいアップデートタスクを追加することもできます。アップデートタスクの追加と設定の詳細については、「4.5.8 スケジューラ」を参照してください。

5.1.9 ネットワーク保護

「ネットワーク保護」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］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。
ブロック	ブロック動作について「既定」「はい」「いいえ」から選択します。
通知	通知について「既定」「はい」「いいえ」から選択します。

［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。

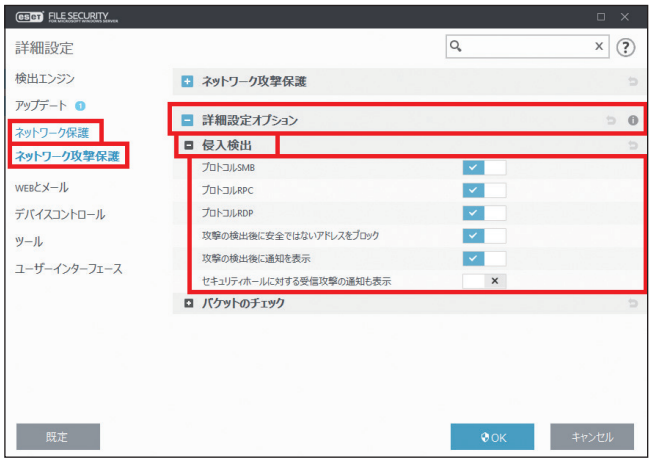
設定した IDS 例外は上から下に順番に評価されます。矢印アイコンで設定の順番を変更することができます。

■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。

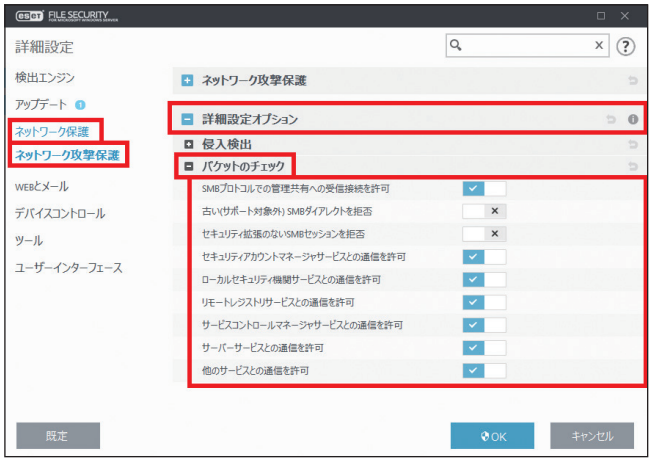


侵入検出

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。
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。

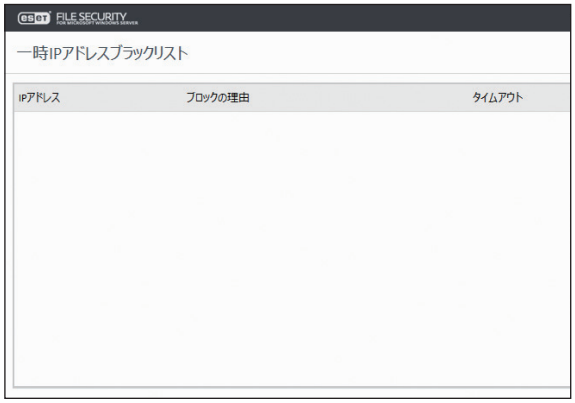


パケットのチェック

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。
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。

5.1.9.1 一時 IP アドレスブラックリスト

攻撃の元であると検出され、一定の時間、接続をブロックするためにブラックリストに追加された IP アドレスの一覧を表示します。また、ロックされた IP アドレスを表示します。一時 IP アドレスブラックリストは、［設定］>［ネットワーク］>［一時 IP アドレスブラックリスト］とクリックすることで表示できます。一時 IP アドレスブラックリストには、ブロックまたはロックされている IP アドレスが表示されるほか、以下のような情報や操作が行えます。



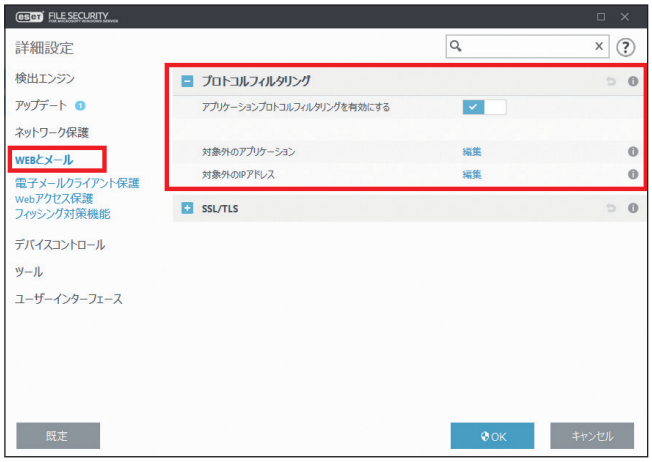
ブロックの理由	アドレスから遮断される攻撃のタイプを示します（TCP ポートスキャン攻撃など）。
タイムアウト	アドレスがブラックリストで期限切れになる日時を示します。
削除 / すべて削除	期限切れになる前に一時ブラックリストから選択した IP アドレスを削除するか、すべてのアドレスをすぐにブラックリストから削除します。
例外の追加	選択した IP アドレスのファイアウォール除外を IDS フィルタリングに追加します。

5.1.10 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。

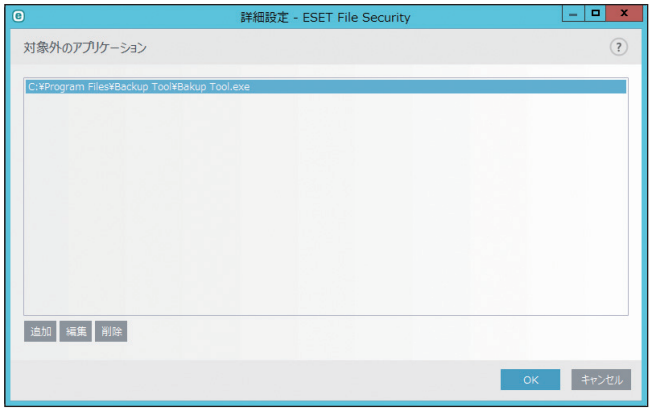


アプリケーションプロトコルフィルタリングを有効にする	プロトコルフィルタリングの有効／無効を設定します。ほとんどの ESET File Security for Microsoft Windows Server（Web アクセス保護、電子メールプロトコル保護、フィッシング対策）はプロトコルフィルタリングを利用しており、無効にすると動作しません。
対象外のアプリケーション	特定のアプリケーションをプロトコルフィルタリングから除外します。プロトコルフィルタリングで互換性の問題があるときに有効です（詳細は「●対象外のアプリケーション」を参照してください。）。
対象外の IP アドレス	特定のリモート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

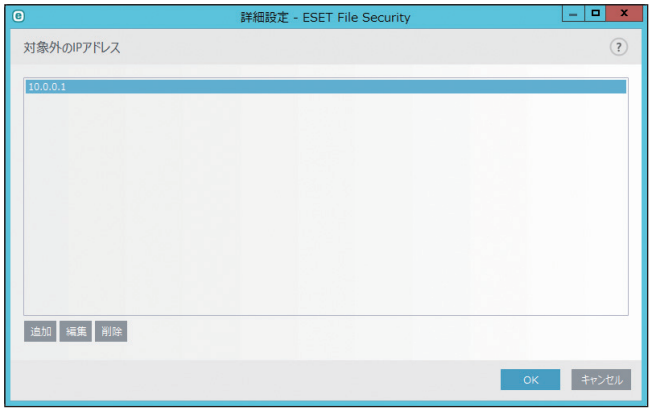


追加	クリックすると、「アプリケーションの追加」画面が表示され、プロトコルフィルタリングを利用しているアプリケーションとサービスが一覧で表示されます。対象外にするアプリケーションやサービスを選択し、［OK］をクリックします。
編集	対象外のアプリケーションやサービスを編集します。
削除	対象外のアプリケーションやサービスを削除します。

●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。

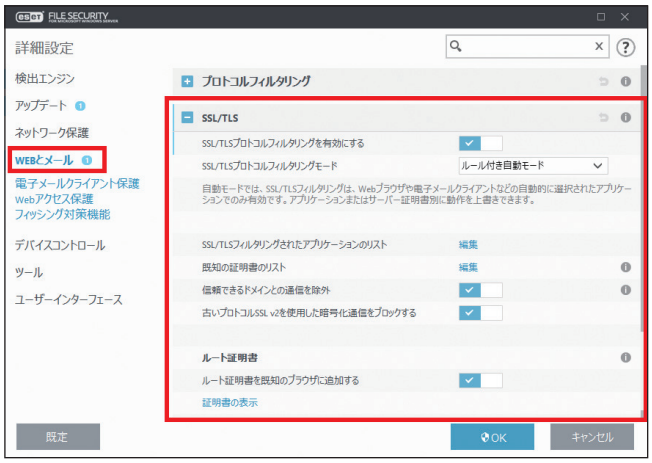


追加	プロトコルフィルタリングから除外するリモートアドレスの IP アドレス／アドレス範囲／サブネットを追加します。
編集	対象外の IP アドレスを編集します。
削除	対象外の IP アドレスを削除します。

■SSL/TLS

ESET File Security for Microsoft Windows Server 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 File Security for Microsoft Windows Server の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 File Security for Microsoft Windows Server 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」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ブラウザに追加する	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 File Security for Microsoft Windows Server 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 File Security for Microsoft Windows Server 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 File Security for Microsoft Windows Server 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 File Security for Microsoft Windows Server 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 File Security for Microsoft Windows Server 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。

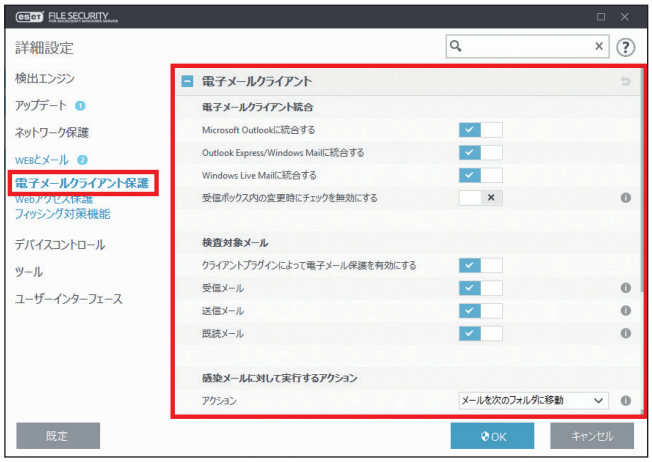


名前	証明書の名前が表示されます。
証明書の発行者	証明書の作成者名が表示されます。
証明書の表題	表題パブリックキーフィールドのパブリックキーに関連付けられたエンティティが表示されます。
アクセス	SSL 通信時のアクションが表示されます。［許可］または［ブロック］に設定されている場合は、信頼性に関係なく、証明書で保護された通信を許可またはブロックします。［自動］に設定されている場合は、信頼できる証明書は通信を許可し、信頼できない証明書はユーザーにアクションを確認します。［確認］に設定されている場合は、常にアクションをユーザーに確認します。
検査	SSL 通信時の検査アクションが表示されます。［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。

5.1.11 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 File Security for Microsoft Windows Server 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 File Security for Microsoft Windows Server 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 File Security for Microsoft Windows Server 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

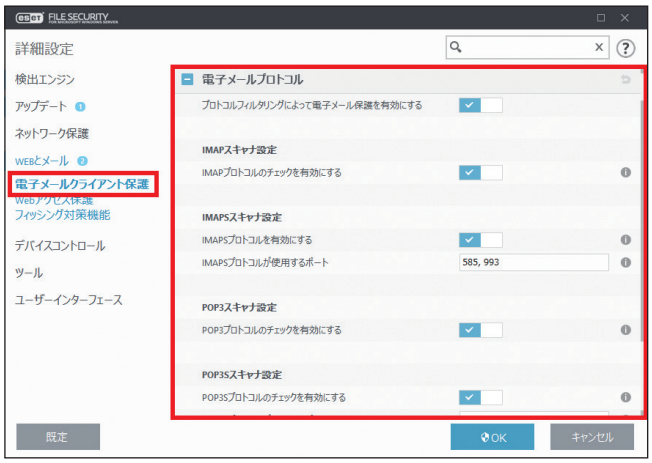
クライアントプラグインによって電子メール保護を有効にする	電子メールクライアントによる電子メールクライアント保護が無効な場合でも、プロトコルフィルタリングによる電子メールクライアントの確認は有効です。
受信メール	受信メールを検査します。
送信メール	送信メールを検査します。
既読メール	既読メールを検査します。

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 File Security for Microsoft Windows Server 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

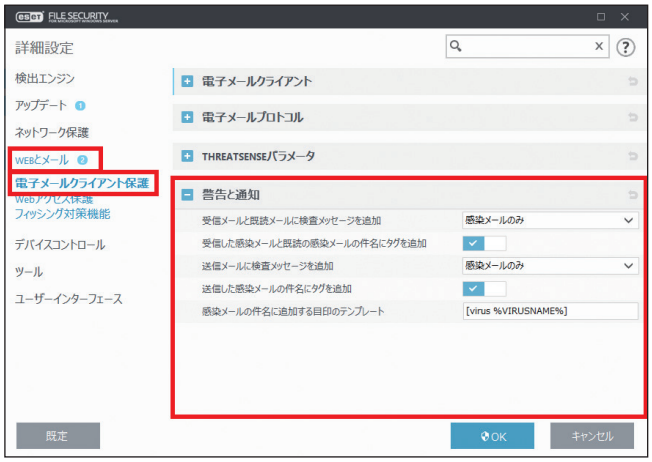
電子メールクライアント保護では、検査対象や検出方法などを設定できます。詳細については、「5.1.2 リアルタイムファイルシステム保護」の「■ THREATSENSE パラメータ」を参照してください。

●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

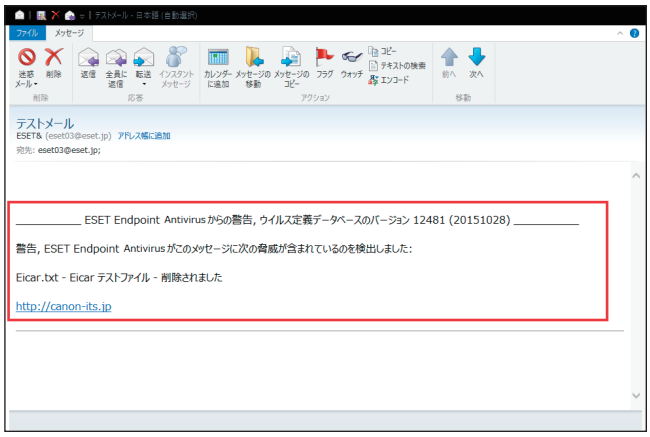
電子メールクライアント保護では、POP3/IMAP プロトコルで受信したメール通信を検査します。ESET File Security for Microsoft Windows Server は、Microsoft Outlook 用のプラグインおよびその他の電子メールクライアントを使用して、電子メールクライアントからの全通信（POP3、MAPI、IMAP、HTTP）を検査します。受信メッセージは、ThreatSense エンジンパラメーターの設定に従って検査するため、検出エンジンと照合する前に悪意のあるコードを検出できます。POP3/IMAP プロトコルの通信検査は、電子メールクライアントか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

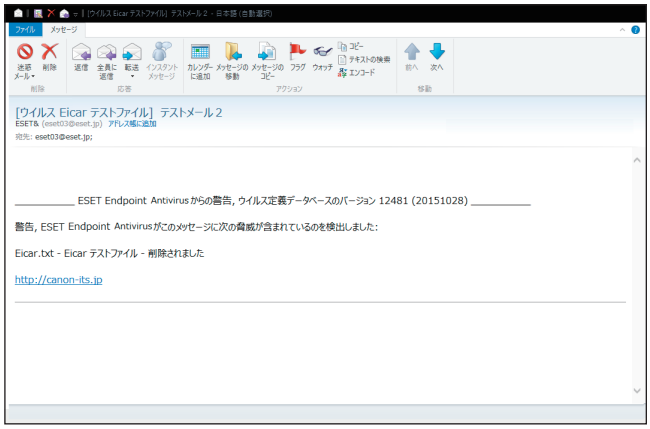
タグの追加

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。



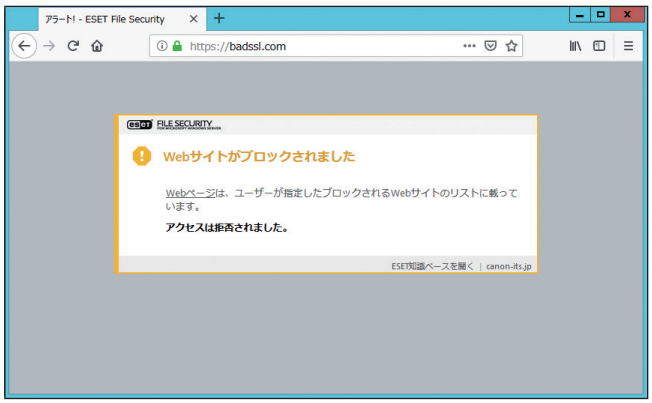
!重 要

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。

5.1.12 Web アクセス保護

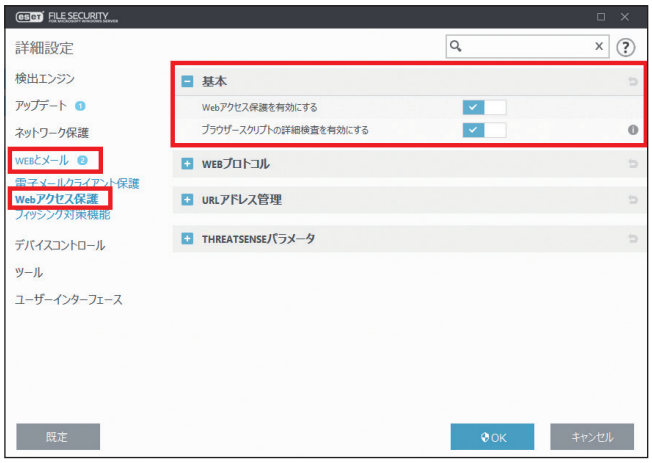
インターネット接続は、コンピューターの標準機能です。しかし、コンピューターによるインターネット接続は、悪意のあるコードを転送する主要な方法になっています。Web アクセス保護は、Web ブラウザーとリモートサーバーとの間で行われる HTTP および HTTPS のルールに準拠した通信を監視します。

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。



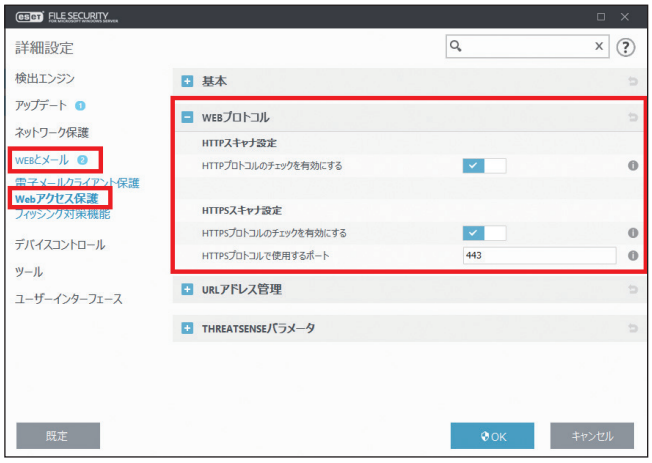
「詳細設定」画面で、［WEB とメール］>［Web アクセス保護］をクリックします。

■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 File Security for Microsoft Windows Server 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

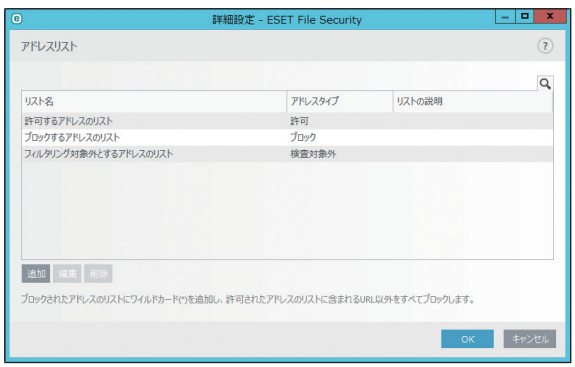
ESET File Security for Microsoft Windows Server は HTTPS プロトコルの検査もサポートしています。HTTPS 通信では、暗号化チャンネルを使用して、サーバーとクライアント間で情報を送受信します。ESET File Security for Microsoft Windows Server は、SSL（Secure Socket Layer）および TLS（Transport Layer Security）プロトコルを使用した通信を検査します。HTTPS プロトコルの検査は、オペレーティングシステムのバージョンに関係なく、HTTPS プロトコル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。

暗号化された接続の検査の有効／無効の設定は、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] で行えます。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】）キー > [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] または [HTTPS 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 プロトコルフィルタリングを有効にする	HTTPS プロトコルフィルタリングの有効 / 無効を設定します。
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。

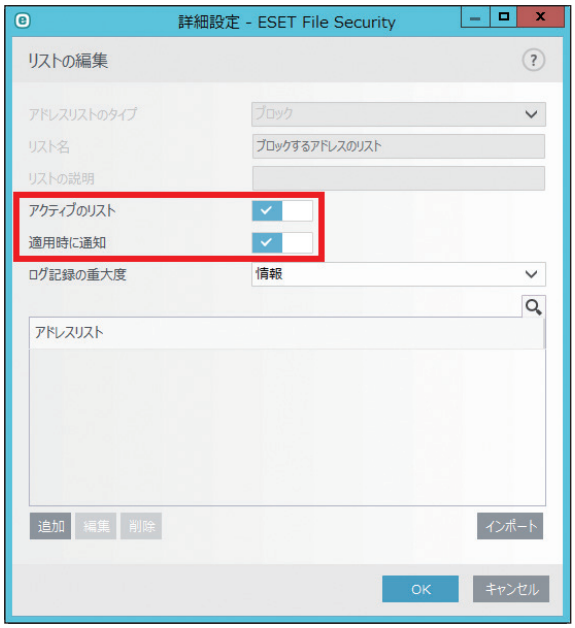


URL アドレス管理では、許可、ブロック、検査から除外する HTTP アドレスを指定できます。既定では、次の 3 つのリストを使用できます。

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

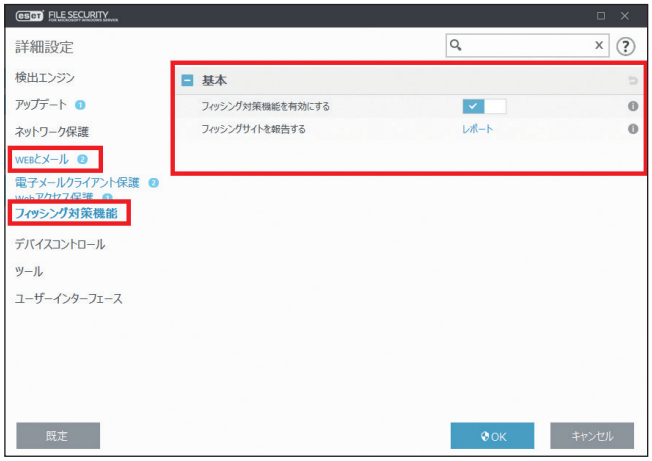
■THREATSENSE パラメータ

[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、「5.1.2 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。

5.1.13 フィッシング対策

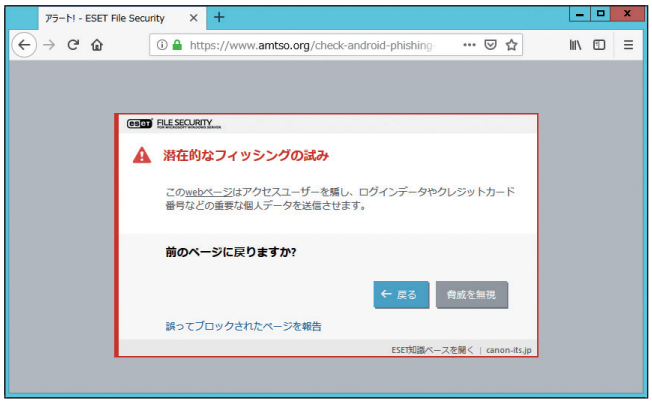
フィッシングとは、ソーシャルエンジニアリング（機密情報を入手するためにユーザーを操ること）を用いる犯罪行為です。フィッシングは、銀行の口座番号や PIN コードなどの機密データを入手するためによく使用されます。
ESET File Security for Microsoft Windows Server はフィッシング対策機能を搭載しており、フィッシングサイトへのアクセスをブロックできます。

「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

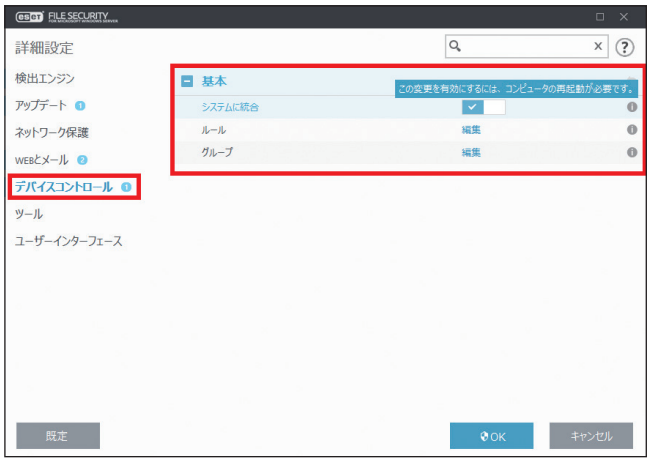
ESET にフィッシングサイトを報告する前に、次の基準を 1 つでも満たしていることを確認してください。

- 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。）

5.1.14 デバイスコントロール検査

自動デバイスコントロール（CD/DVD/USB など）機能を備えています。このモジュールを使用すると、ユーザーからの特定デバイスへのアクセス方法やその作業方法を定義できます。この機能は、不審なファイルを保存したデバイスの使用を防止したい管理者にとって便利です。

「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［デバイスコントロール］を選択します。

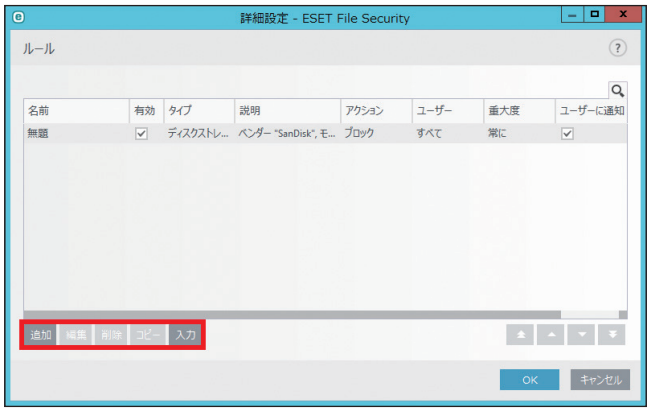


［システム統合］を有効にするとデバイスコントロール機能が有効になります。この変更を有効にするには、クライアントコンピューターの再起動が必要になります。

ルールでブロックされているデバイスが挿入されると、通知画面が表示され、デバイスへのアクセスはブロックされます。

■デバイスルール

［ルール］で［編集］をクリックすると「ルール」画面が開きます。この画面で、ユーザーがクライアントコンピューターに接続する外付けデバイスを細かく管理することができます。



ユーザー単位またはユーザーグループ単位で、さらに複数の追加パラメーターに基づいて特定のデバイスを許可またはブロックできます。これは、ルール設定で指定します。ルール一覧には、外部デバイスの名前とタイプ、クライアントコンピューターに外部デバイスを接続した後に実行するアクション、およびログの重大度などのルールの詳細が表示されます。

「ルール」画面では次の操作ができます。

追加／編集	ルールを追加または編集します。
コピー	選択したルールをコピーして新しいルールを作成します。
削除	選択したルールを削除します。
入力	クライアントコンピューターに接続されている外部デバイスのデバイスパラメーターが自動的に入力されます。

ルールは優先度順に一覧表示されます。優先度が高いルールが上位に表示されます。画面右下の矢印ボタンをクリックしてリスト内での上下移動を行い、優先順位を変更できます。複数のルールを選択して必要なアクションを適用できます。ログエントリーは、ESET File Security for Microsoft Windows Server のメインメニューで［ログファイル］をクリックし、「ログファイル」画面のドロップダウンメニューから［デバイスコントロール］を選択して表示することができます。

ルールの追加

デバイスコントロールルールでは、ルール基準に適合するデバイスがクライアントコンピューターに接続されたときに実行されるアクションを定義します。

「ルール」画面で編集したい項目を選択し、[編集] をクリックします。新規作成を行うときは [追加] をクリックします。



名前と有効化

ルール名を「名前」のテキストボックスに入力します。「有効」のチェックボックスで、ルールを無効または有効にします。ルールを削除せずに無効にしたい場合に便利です。

デバイスのタイプ

外部デバイスのタイプをドロップダウンメニューから選択します。サポートされている外部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 プリンター
- FireWire ストレージ
- Bluetooth デバイス
- スマートカードリーダー
- イメージングデバイス
- モデム
- LPT/COM ポート
- ポータブルデバイス
- すべてのデバイスタイプ

デバイスのタイプは、デバイスがクライアントコンピューターに接続されているときに、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メモリカードリーダーが含まれます。スマートカードリーダーとは、SIM カード、認証カードなど、集積回路が埋め込まれているスマートカードを読み取るリーダーのことです。イメージングデバイスは、スキャナーやカメラなどです。これらのデバイスはユーザーに関する情報は提供せず、そのアクションの情報だけを提供します。従って、イメージングデバイスをブロックする場合は、全体としてブロックする必要があります。

アクション

ストレージデバイス以外のデバイスで選択できるアクションは、許可またはブロックのいずれかです。それに対して、ストレージデバイスのルールについては、次のいずれかのアクション（権限）を選択できます。

読み込み / 書き込み	デバイスへの完全なアクセスを許可します。
ブロック	デバイスへのアクセスはブロックされます。
読み取り専用	デバイスからの読み込みだけが許可されます。
警告	デバイスに接続するたびに、許可またはブロックするかの警告が通知され、ログが作成されます。デバイスは記憶されないため、同じデバイスに後から接続する場合にも、再度警告が通知されます。

デバイスのタイプによっては、選択できないアクション（権限）もあります。

追加パラメーター

追加のパラメーターでは、デバイスに合わせてルールの詳細を設定できます。いずれのパラメーターでも大文字と小文字は区別されません。

条件	デバイスまたはデバイスグループを指定します。
ベンダー	ベンダー名または ID によるフィルタリングに使用します。
モデル	デバイスのモデル名を入力します。
シリアル番号	外部デバイスには通常独自のシリアル番号が付与されています。CD/DVD の場合は、CD/DVD ドライブではなく、そのメディアのシリアル番号を入力します。

！重　要

「ベンダー」、「モデル」、「シリアル」のフィールドが空の場合、ルールを適用する際にはこれらの項目は無視されます。すべてのフィールドのパラメーターでは、大文字と小文字は区別されず、ワイルドカード（*、?）はサポートされません。

ワンポイント

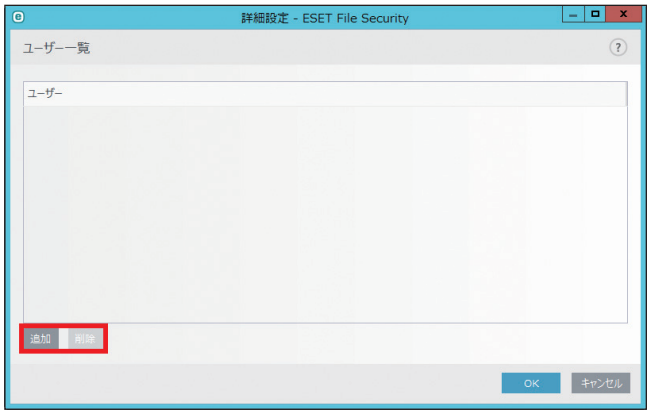
デバイスのパラメーターを確認するには、デバイスのタイプのルールを作成し、デバイスをクライアントコンピューターに接続してから、デバイスコントロールログでデバイスの詳細を確認します。

ログ記録の重大度

常に	すべてのイベントを常にログに記録します。
診断	プログラムの微調整で必要となる情報をログに記録します。
情報	すべての情報メッセージ（アップデートの成功メッセージを含む）と上記のすべてのログを記録します。
警告	エラーおよび警告メッセージをログに記録します。
なし	ログは記録されません。

ユーザー一覧

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



「ユーザー一覧」画面のボタンでは次の操作ができます。

追加	表示される「ユーザーまたはグループの選択」画面で［オブジェクトの種類］をクリックし、検索するオブジェクトの種類を選択します。
削除	選択されたユーザーを一覧から削除します。

! 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

ユーザーに通知

「ユーザーに通知」では、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。

検出されたデバイス

「ルール」画面で［入力］をクリックすると、「検出されたデバイス」画面が表示されます。画面には、現在接続されているすべてのデバイスの概要と次の情報が表示されます。この情報には、デバイスタイプ、ベンダー（デバイスの製造元）、モデル、シリアル番号（ある場合）などが含まれます。検出されたデバイスのリストからデバイスを選択し、［OK］をクリックすると、「ルール」画面が開き、定義済みの情報が表示されます。



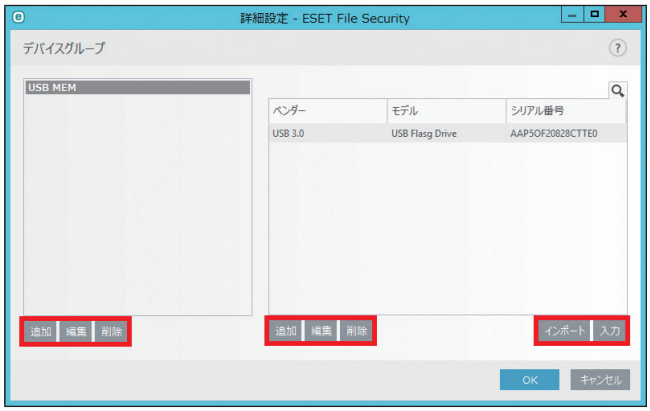
■デバイスグループ

!重 要

クライアントコンピューターに接続されたデバイスは、セキュリティリスクとなる可能性があります。

「デバイスグループ」画面を表示するには、[デバイスコントロール] > [基本] > [グループ] > [編集] をクリックします。
「デバイスグループ」画面は、左右に分かれます。画面右側には、該当するグループに属するデバイスが一覧表示されます。画面左側には、既存のグループのリストが表示されます。画面右側に表示するデバイスを含むグループを選択します。

「デバイスグループ」画面を開き、グループを選択すると、一覧からデバイスを追加、編集または削除できます。また、ファイルからインポートして、グループにデバイスを追加することもできます。[入力] をクリックすると、クライアントコンピューターに接続されたすべてのデバイスが「検出されたデバイス」画面に一覧表示されます。リストからデバイスを選択し、[OK] をクリックするとグループに追加されます。



「デバイスグループ」画面のボタンでは次の操作ができます。

追加	名前を入力してグループを新しく追加するか、デバイスを既存のグループに追加できます。オプションで、ベンダー名、モデル、シリアル番号などの詳細を指定できます。この操作は、ボタンをクリックした左右の画面によって異なります。
編集	選択したグループの名前またはグループに含まれるデバイスのパラメーター（ベンダー、モデル、シリアル番号）を変更できます。
削除	選択したグループまたはデバイスを削除します。
インポート	ファイルからデバイスのシリアル番号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概要と次の情報が表示されます。この情報には、デバイスタイプ、ベンダー、モデル、シリアル番号（ある場合）などが含まれます。

設定が完了したら、[OK] をクリックします。変更を保存せずに「デバイスグループ」を終了するには、[編集] をクリックします。

ワンポイント

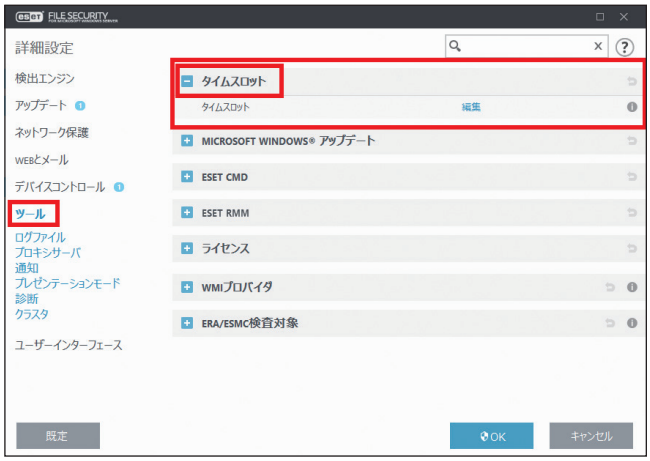
異なるルールが定義された様々なデバイスのグループを作成できます。また、読み込み／書き込みまたは読み取り専用アクションがあるルールが定義されたデバイスのグループは、1 つだけ作成できます。これにより、デバイスをクライアントコンピューターに接続したときに、認識されていないデバイスはデバイスコントロールによってブロックされます。

5.1.15 ツール設定

「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［ツール］を選択します。

■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

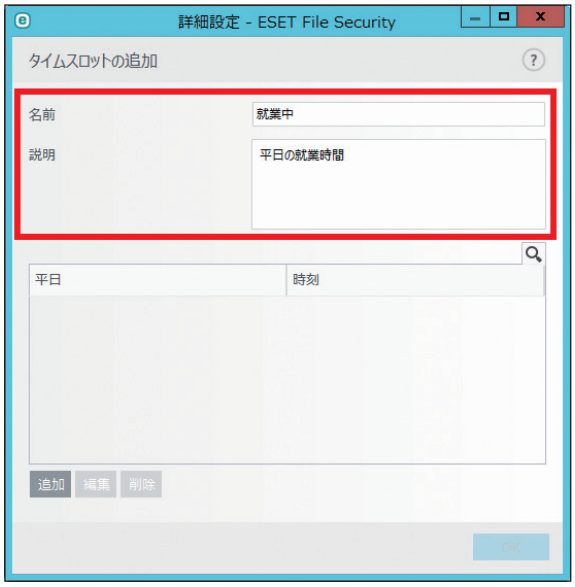
タイムスロットの追加や編集、削除を行うときは、［詳細設定］画面で［ツール］>［タイムスロット］>「タイムスロット」の［編集］をクリックします。



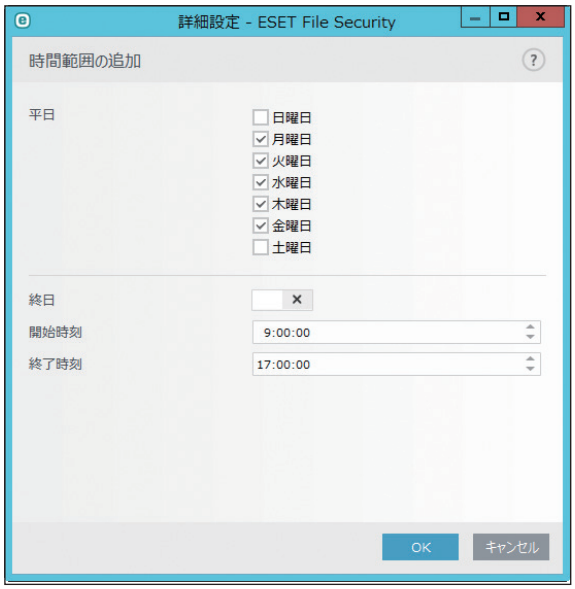
追加	新しいタイムスロットを追加します。
編集	作成済みのタイムスロットを編集します。
削除	選択したタイムスロットを削除します。

●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。

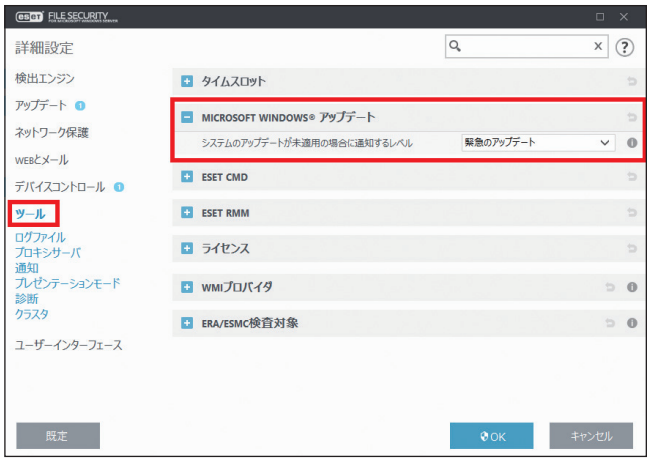
ワンポイント

「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

Microsoft Windows アップデートは、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 File Security for Microsoft Windows Server 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。



使用可能な通知レベルは次のとおりです。

通知しない	Microsoft Windows アップデートの更新は通知されません。
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。

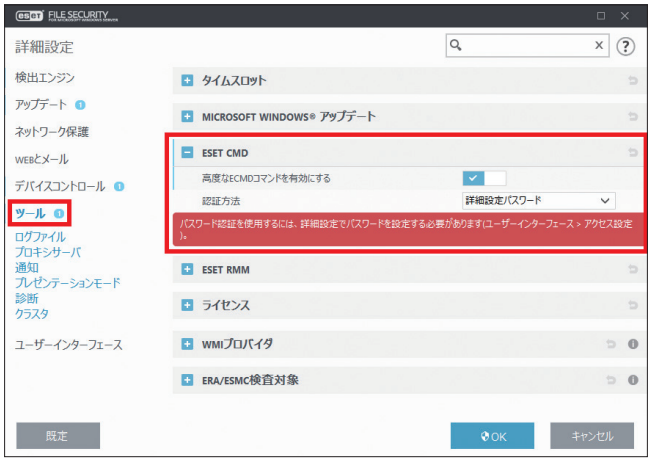
! 重　要

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。ESMC 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 File Security for Microsoft Windows Server 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

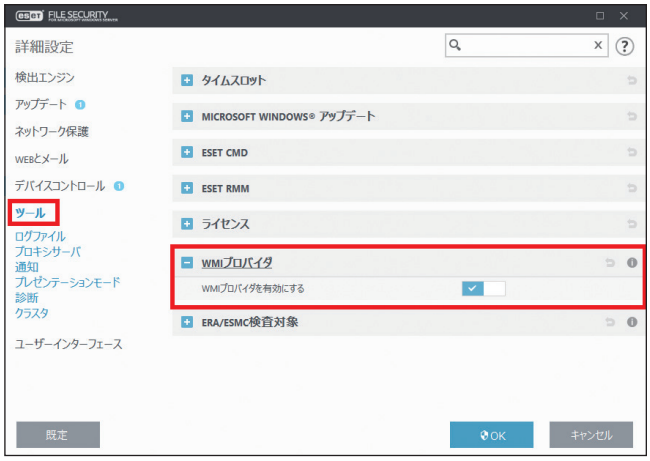
ライセンスでは、ESET File Security for Microsoft Windows Server が ESET ライセンスサーバーに接続する間隔の設定を行えます。ESET ライセンスサーバーへの接続間隔の変更は、「間隔チェック」で行います。既定では、「自動」に設定されており、1 時間に数回接続を行っています。ネットワークトラフィックが増大した場合には、「間隔チェック」の設定を［制限］に変更すると、負荷が低減されます。制限が選択されると、ESET File Security for Microsoft Windows Server は 1 日に 1 回またはコンピューターが再起動す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

■ WMI プロバイダ

Windows Management Instrumentation（WMI）は、エンタープライズ環境で管理情報にアクセスするための標準技術である Web-Based Enterprise Management（WBEM）に準拠した Microsoft Windows に実装される機能です。
WMI の詳細については、http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx を参照してください。

ESET WMI プロバイダーは、ESET 固有のソフトウェアまたはツールを必要とせずに、エンタープライズ環境で ESET 製品のリモート監視ができるようにします。WMI 経由で基本製品、ステータス、統計情報を収集することで管理者が ESET 製品を監視する能力を高めます。管理者は WMI の様々なアクセス方法（コマンドライン、スクリプト、他社製のエンタープライズ監視ツール）を使用して、ESET 製品の状態を監視できます。

ESET WMI プロバイダーでは、基本製品情報、インストール済み機能と保護状態、個別スキャナーの統計、および製品ログファイルに読み取りアクセスできます。
「WMI プロバイダを有効にする」を有効にすることより、標準の WMI インフラストラクチャーおよびツールの使用と、製品と製品ログの状態の読み取りが可能になります。



●収集できるデータ

ESET 製品に関連付けられたすべての WMI クラスは「root\ESET」ネームスペースにあります。次のクラスが現在実装されています。

一般：

- ESET_Product
- ESET_Features
- ESET_Statistics

ログ：

- ESET_ThreatLog
- ESET_EventLog
- ESET_ODFileScanLogs
- ESET_ODFileScanLogRecords
- ESET_ODServerScanLogs
- ESET_ODServerScanLogRecords
- ESET_HIPSLog
- ESET_URLLog
- ESET_DevCtrlLog
- ESET_GreylistLog
- ESET_MailServeg
- ESET_HyperVScanLogs
- ESET_HyperVScanLogRecords

ESET_Product クラス

ESET_Product クラスには 1 つのインスタンスのみがあります。このクラスのプロパティは、インストール済みの ESET 製品の基本情報を参照します。

ID	「essbe」などの製品タイプ ID
Name	「ESET Security」などの製品名
FullName	「Microsoft SharePoint Server」などの製品のエディション
Version	「4.5.15013.0」などの製品バージョン
VirusDBVersion	「7868 (20130107)」などのウイルスデータベースのバージョン
VirusDBLastUpdate	ウイルスデータベースの最終更新日時のタイムスタンプ。この文字列には WMI 日時形式のタイムスタンプが含まれます。例えば、「20130118115511.000000+060」です。
LicenseExpiration	ライセンスの有効期限。この文字列には WMI 日時形式のタイムスタンプが含まれます。例えば、「20130118115511.000000+060」です。
KernelRunning	クライアントコンピューターで「eKrn」サービスが実行中かどうかを示すブール値。例えば「TRUE」です。
StatusCode	製品の保護ステータスを示す数字。0：緑（OK）、1：オレンジ（警告）、2：赤（エラー）。
StatusText	「0」以外のステータスコードの理由を説明するメッセージ。メッセージがない場合は空です。

ESET_Features クラス

ESET_Features クラスには、製品機能数に応じて、複数のインスタンスがあります。
各インスタンスの内容は次のとおりです。

Name	機能名（名前のリストは以下に示します）
Status	機能のステータス。0：非アクティブ、1：無効、2：有効。

現在認識されている製品機能を示す文字列のリスト

CLIENT_FILE_AV	リアルタイムファイルシステムウイルス対策保護
CLIENT_WEB_AV	クライアント Web ウイルス対策保護
CLIENT_DOC_AV	クライアントドキュメントウイルス対策保護
CLIENT_NET_FW	クライアントパーソナルファイアウォール
CLIENT_EMAIL_AV	クライアント電子メールウイルス対策保護
CLIENT_EMAIL_AS	クライアント電子メール迷惑メール対策保護
SERVER_FILE_AV	保護されたファイルサーバー製品のファイルのリアルタイムウイルス対策保護。例えば、ESET File Security for Microsoft Windows Server の場合には、「SharePoint」のコンテンツデータベースにあるファイルです。
SERVER_EMAIL_AV	保護されたサーバー製品の電子メールのウイルス対策保護。例えば、「Exchange」または「IBM Lotus Domino」の電子メールです。

SERVER_EMAIL_AS	保護されたサーバー製品の電子メールの迷惑メール対策保護。例えば、「Exchange」または「IBM Lotus Domino」の電子メールです。
SERVER_GATEWAY_AV	ゲートウェイ上の保護されたネットワークプロトコルのウイルス対策保護
SERVER_GATEWAY_AS	ゲートウェイ上の保護されたネットワークプロトコルの迷惑メール対策保護

ESET_Statistics クラス

ESET_Statistics クラスには、製品のスキャナー数に応じて、複数のインスタンスがあります。
各インスタンスの内容は次のとおりです。

Scanner	特定のスキャナーの文字列コード。例えば、「CLIENT_FILE」です。
Total	検査されたファイルの合計数
Infected	検出された感染ファイル数
Cleaned	駆除されたファイル数
Timestamp	この統計が最後に変更されたタイムスタンプ。WMI 日時形式。例えば、「20130118115511.000000+060」です。
ResetTime	統計カウンターが最後にリセットされたタイムスタンプ。WMI 日時形式。例えば、「20130118115511.000000+060」です。

現在認識されているスキャナーを示す文字列のリスト

- CLIENT_FILE
- CLIENT_EMAIL
- CLIENT_WEB
- SERVER_FILE
- SERVER_EMAIL
- SERVER_WEB

ESET_ThreatLog クラス

ESET_ThreatLog クラスには複数のインスタンスがあり、それぞれのインスタンスが「Detected threats」ログのログレコードを表します。
各インスタンスの内容は次のとおりです。

ID	このログレコードの一意の ID
Timestamp	ログレコードの作成タイムスタンプ（WMI 日時形式）
LogLevel	「0 ～ 8」の数字で表されるログレコードの重要度。重要度の値は次のレベルに対応します。「Debug」、「Info-Footnote」、「Info」、「Info-Important」、「Warning」、「Error」、「SecurityWarning」、「Error-Critical」、「SecurityWarning-Critical」。
Scanner	このログイベントを作成したスキャナーの名前
ObjectType	このログイベントを作成したオブジェクトのタイプ
ObjectName	このログイベントを作成したオブジェクトの名前
Threat	「ObjectName」および「ObjectType」プロパティで記述されたオブジェクトで検出された脅威名
Action	脅威が特定された後に実行されたアクション
User	このログイベントを作成したユーザーアカウント
Information	イベントの詳細情報
Hash	このイベントを作成したオブジェクトのハッシュ

ESET_EventLog

ESET_EventLog クラスには複数のインスタンスがあり、それぞれのインスタンスが「Events」ログのログレコードを表します。
各インスタンスの内容は次のとおりです。

ID	このログレコードの一意の ID
Timestamp	ログレコードの作成タイムスタンプ（WMI 日時形式）
LogLevel	「0 ～ 8」の数字で表されるログレコードの重要度。重要度の値は次のレベルに対応します。「Debug」、「Info-Footnote」、「Info」、「Info-Important」、「Warning」、「Error」、「SecurityWarning」、「Error-Critical」、「SecurityWarning-Critical」。
Module	このログイベントを作成したモジュールの名前
Event	イベントの説明
User	このログイベントを作成したユーザーアカウント

ESET_ODFileScanLogs

ESET_ODFileScanLogs クラスには複数のインスタンスがあり、各インスタンスはオンデマンドファイル検査レコードを表します。これは、ログの GUI「On-demand computer scan」リストに対応します。
各インスタンスの内容は次のとおりです。

ID	このオンデマンドログの一意の ID
Timestamp	ログの作成タイムスタンプ（WMI 日時形式）
Targets	スキャンの対象フォルダー／オブジェクト
TotalScanned	検査されたオブジェクトの合計数
Infected	検出された感染オブジェクト数
Cleaned	駆除されたオブジェクト数
Status	検査処理のステータス

ESET_ODFileScanLogRecords

ESET_ODFileScanLogRecords クラスには複数のインスタンスがあり、各インスタンスは、ESET_ODFileScanLogs クラスのインスタンスで表される検査ログのいずれかにあるログレコードを表します。このクラスのインスタンスは、すべてのオンデマンド検査／ログのログレコードを提供します。特定の検査ログのインスタンスだけが必要な場合、LogID プロパティでフィルタリングする必要があります。
各インスタンスの内容は次のとおりです。

LogID	このレコードが属する検査ログの ID（ESET_ODFileScanLogs クラスのインスタンスのいずれかの ID）
ID	この検査ログレコードの一意の ID
Timestamp	ログレコードの作成タイムスタンプ（WMI 日時形式）
LogLevel	「0 ～ 8」の数字で表されるログレコードの重要度。重要度の値は次のレベルに対応します。「Debug」、「Info-Footnote」、「Info」、「Info-Important」、「Warning」、「Error」、「SecurityWarning」、「Error-Critical」、「SecurityWarning-Critical」。
Log	実際のログメッセージ

ESET_ODServerScanLogs

ESET_ODServerScanLogs クラスには複数のインスタンスがあり、各インスタンスはオンデマンドサーバー検査の実行を表します。
各インスタンスの内容は次のとおりです。

ID	このオンデマンドログの一意の ID
Timestamp	ログの作成タイムスタンプ（WMI 日時形式）
Targets	スキャンの対象フォルダー／オブジェクト
TotalScanned	検査されたオブジェクトの合計数
Infected	検出された感染オブジェクト数
Cleaned	駆除されたオブジェクト数
RuleHits	ルールヒットの合計数
Status	検査処理のステータス

ESET_ODServerScanLogRecords

ESET_ODServerScanLogRecords クラスには複数のインスタンスがあり、各インスタンスは、ESET_ODServerScanLogs クラスのインスタンスで表される検査ログのいずれかにあるログレコードを表します。このクラスのインスタンスは、すべてのオンデマンド検査／ログのログレコードを提供します。特定の検査ログのインスタンスだけが必要な場合、LogID プロパティでフィルタリングする必要があります。
各インスタンスの内容は次のとおりです。

LogID	このレコードが属する検査ログの ID（ESET_ ODServerScanLogs クラスのインスタンスのいずれかの ID）
ID	この検査ログレコードの一意の ID
Timestamp	ログレコードの作成タイムスタンプ（WMI 日時形式）
LogLevel	「0 ～ 8」の数字で表されるログレコードの重要度。重要度の値は次のレベルに対応します。「Debug」、「Info-Footnote」、「Info」、「Info-Important」、「Warning」、「Error」、「SecurityWarning」、「Error-Critical」、「SecurityWarning-Critical」。
Log	実際のログメッセージ

ESET_SmtpProtectionLog

ESET_SmtpProtectionLog クラスには複数のインスタンスがあり、それぞれのインスタンスが「Smtp protection」ログのログレコードを表します。各インスタンスの内容は次のとおりです。

ID	この検査ログレコードの一意の ID
Timestamp	ログレコードの作成タイムスタンプ（WMI 日時形式）
LogLevel	[0-8] の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します。Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
HELODomain	HELO ドメインの名前
IP	ソース IP アドレス
Sender	電子メール送信者
Recipient	電子メール受信者
ProtectionType	使用される保護の種類
Action	実行されたアクション
Reason	アクションの理由
TimeToAccept	電子メールが許可されるまでの分数

ESET_HIPSLog

ESET_HyperVScanLogRecords クラスには複数のインスタンスがあり、それぞれのインスタンスが「HIPS」ログのログレコードを表します。各インスタンスの内容は次のとおりです。

ID	このログレコードの一意の ID
Timestamp	ログレコードの作成タイムスタンプ（WMI 日時形式）
LogLevel	[0-8] の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します。Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
Application	ソースアプリケーション
Target	処理のタイプ
Action	HIPS が実行するアクション。例 : 許可、拒否
Rule	アクションを実行するルールの名前
AdditionalInfo	-

ESET_URLLog

ESET_URLLog クラスには複数のインスタンスがあり、それぞれのインスタンスが「フィルタリングされた Web サイト」ログのログレコードを表します。各インスタンスの内容は次のとおりです。

ID	このログレコードの一意の ID
Timestamp	ログレコードの作成タイムスタンプ（WMI 日時形式）
LogLevel	[0-8] の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します。Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
URL	URL
Status	URL で発生した処理。例 : Web コントロールによりブロック
Application	URL にアクセスしようとしたアプリケーション
User	アプリケーションを実行したユーザーアカウント

ESET_DevCtrlLog

ESET_DevCtrlLog クラスには複数のインスタンスがあり、それぞれのインスタンスが「デバイスコントロール」ログのログレコードを表します。各インスタンスの内容は次のとおりです。

ID	このログレコードの一意の ID
Timestamp	ログレコードの作成タイムスタンプ（WMI 日時形式）
LogLevel	[0-8] の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します。Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
Device	デバイス名
User	ユーザーアカウント名
UserSID	ユーザーアカウント SID
Group	ユーザーグループ名
GroupSID	ユーザーグループ SID
Status	デバイスで発生した処理。例 : 書き込みブロック
DeviceDetails	デバイスの詳細情報
EventDetails	イベントに関する詳細情報

ESET_MailServerLog

ESET_MailServerLog クラスには複数のインスタンスがあり、それぞれのインスタンスが「Mail server」ログのログレコードを表します。各インスタンスの内容は次のとおりです。

ID	このログレコードの一意の ID
Timestamp	ログレコードの作成タイムスタンプ（WMI 日時形式）
LogLevel	［0-8］の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します。Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
IPAddr	ソース IP アドレス
HELODomain	HELO ドメインの名前
Sender	電子メール送信者
Recipient	電子メール受信者
Subject	電子メールの件名
ProtectionType	現在のログレコードに記述されたアクションを実行した保護タイプ。例 : ウイルス対策、迷惑メール対策、ルール
Action	実行されたアクション
Reason	特定の ProtectionType によって、アクションがオブジェクトで実行された理由

ESET_HyperVScanLogs

ESET_HyperVScanLogs クラスには複数のインスタンスがあり、各インスタンスは Hyper-V ファイル検査実行を表します。これは、ログの GUI「Hyper-V」リストに対応します。各インスタンスの内容は次のとおりです。

ID	このログレコードの一意の ID
Timestamp	ログレコードの作成タイムスタンプ（WMI 日時形式）
Targets	検査のターゲットコンピューター / ディスク / ボリューム
TotalScanned	検査されたオブジェクトの合計数
Infected	検出された感染オブジェクト数
Cleaned	駆除されたオブジェクト数
Status	検査処理のステータス

ESET_HyperVScanLogRecords

ESET_HyperVScanLogRecords クラスには複数のインスタンスがあり、各インスタンスは、ESET_HyperVScanLogs クラスのインスタンスで表される検査ログのいずれかにあるログレコードを表します。このクラスのインスタンスは、すべての Hyper-V 検査 / ログのログレコードを提供します。特定の検査ログのインスタンスだけが必要な場合、LogID プロパティでフィルタリングする必要があります。各クラスインスタンスの内容は次のとおりです。

LogID	このレコードが属する検査ログの ID（ESET_HyperVScanLogs クラスのインスタンスのいずれかの ID）
ID	このログレコードの一意の ID
Timestamp	ログレコードの作成タイムスタンプ（WMI 日時形式）
LogLevel	［0-8］の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します。Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
Log	実際のログメッセージ

ESET_NetworkProtectionLog

ESET_NetworkProtectionLog クラスには複数のインスタンスがあり、それぞれのインスタンスが「Network protection」ログのログレコードを表します。各インスタンスの内容は次のとおりです。

ID	このログレコードの一意の ID
Timestamp	ログレコードの作成タイムスタンプ（WMI 日時形式）
LogLevel	［0-8］の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します。Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
Event	ネットワーク保護アクションをトリガーするイベント
Action	ネットワーク保護で実行されたアクション
Source	ネットワークデバイスのソースアドレス
Target	ネットワークデバイスの宛先アドレス
Protocol	ネットワーク通信保護
RuleOrWormName	イベントに関連するルールまたはワーム名
Application	ネットワーク通信を開始したアプリケーション
User	このログイベントを作成したユーザーアカウント

ESET_SentFilesLog

ESET_SentFilesLog クラスには複数のインスタンスがあり、それぞれのインスタンスが「Sent files」ログのログレコードを表します。各インスタンスの内容は次のとおりです。

ID	このログレコードの一意の ID
Timestamp	ログレコードの作成タイムスタンプ（WMI 日時形式）
LogLevel	[0-8] の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します。Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
Sha1	送信されたファイルの SHA-1 ハッシュ
File	送信されたファイル
Size	送信されたファイルのサイズ
Category	送信されたファイルのカテゴリ
Reason	ファイルを送信する理由
SentTo	ファイルが送信された ESET 部門
User	このログイベントを作成したユーザーアカウント

ESET_OneDriveScanLogs

ESET_OneDriveScanLogs クラスには複数のインスタンスがあり、各インスタンスは OneDrive 検査実行を表します。これは、ログの GUI「OneDrive」リストに対応します。各インスタンスの内容は次のとおりです。

ID	この OneDrive ログの一意の ID
Timestamp	ログの作成タイムスタンプ（WMI 日時形式）
Targets	スキャンの対象フォルダ / オブジェクト
TotalScanned	検査されたオブジェクトの合計数
Infected	検出された感染オブジェクト数
Cleaned	駆除されたオブジェクト数
Status	検査処理のステータス

ESET_OneDriveScanLogRecords

ESET_OneDriveScanLogRecords クラスには複数のインスタンスがあり、各インスタンスは、ESET_OneDriveScanLogs クラスのインスタンスで表される検査ログのいずれかにあるログレコードを表します。このクラスのインスタンスは、すべての OneDrive 検査 / ログのログレコードを提供します。特定の検査ログのインスタンスだけが必要な場合、LogID プロパティでフィルタリングする必要があります。各インスタンスの内容は次のとおりです。

LogID	このレコードが属する検査ログの ID（ESET_OneDriveScanLogs クラスのインスタンスのいずれかの ID）
ID	この OneDrive ログの一意の ID
Timestamp	ログの作成タイムスタンプ（WMI 日時形式）
LogLevel	［0-8］の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します。Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
Log	実際のログメッセージ

●収集されたデータへのアクセス

Windows コマンドラインと「PowerShell」で ESET WMI データにアクセスすることができます。すべての最新の Windows オペレーティングシステムで動作します。他のスクリプト言語やツールを使ってアクセスすることもできます。

スクリプトを使用しないコマンドライン

wmic コマンドラインツールは、定義済みまたは任意のカスタム WMI クラスにアクセスするために使用できます。

ローカルコンピューターの製品に関する詳細情報を表示する

```
wmic /namespace:\\root\ESET Path ESET_Product
```

ローカルコンピューターの製品の製品バージョン番号だけを表示する

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

IP 10.1.118.180 のリモートコンピューターの製品に関する詳細情報を表示する

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

ローカルコンピューターの製品に関する詳細情報を取得して表示する

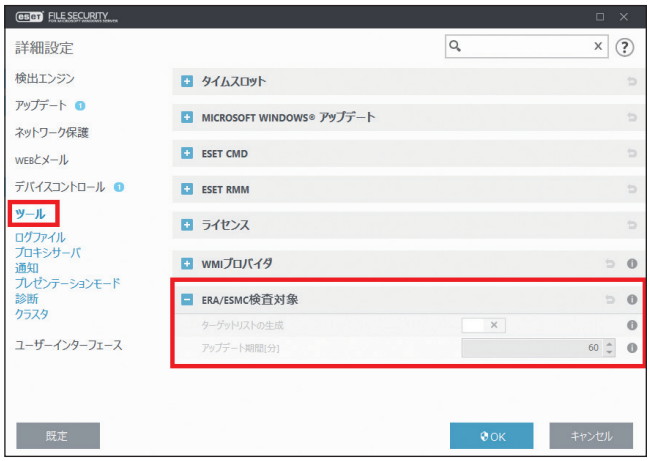
```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

IP 10.1.118.180 のリモートコンピューターの製品に関する詳細情報を取得して表示する

```
$cred = Get-Credential              # ユーザーに認証情報を入力させ変数に格納する
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -cred $cred
```

■ ERA/ESMC 検査対象

ESET File Security for Microsoft Windows Server と ESET Management エージェントが同じサーバー上にインストールされている場合、検査対象のリストを作成することができます。



「ターゲットリストの生成」機能を使用すると、ESET File Security for Microsoft Windows Server は現在使用可能な検査対象のリストを作成します。このリストは［アップデート期間（分）］の設定に従って、定期的に生成されます（既定では「60」分に設定されています）。「サーバー検査」クライアントタスクを実行する必要がある場合、ESET Management エージェントはリストを収集し、その特定のサーバーでオンデマンド検査の検査対象を選択します。

5.1.16 上書きモード

ESET File Security for Microsoft Windows Server 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 File Security for Windows Server（V6+）] 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。

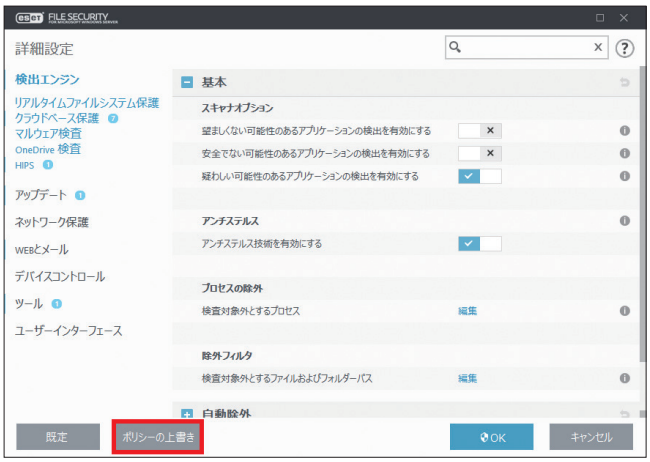


上書きモードを有効にする	上書きモードを有効にします。	
最大上書き時間	上書きモードを有効にする時間を設定します。 最大で 4 時間上書きモードを有効にすることができます。	
上書き後にコンピューターを検査する	有効にすると上書きモードを終了させた後に、コンピューターの検査が実行されます。	
認証タイプ	Active directory ユーザー	上書きモードを利用するユーザーを指定します。
	パスワード	上書きモードを利用する際のパスワードを設定します。 カスタムパスワードの項目にパスワードを入力します。

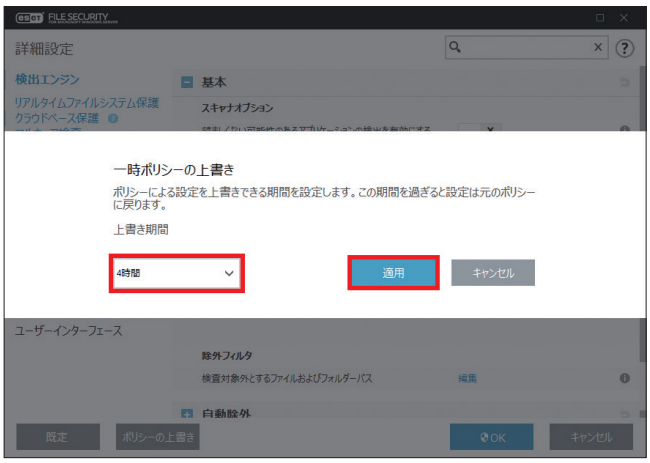
クライアントコンピューター側の操作手順

操作手順

1. ESET File Security for Microsoft Windows Server 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 File Security for Microsoft Windows Server 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

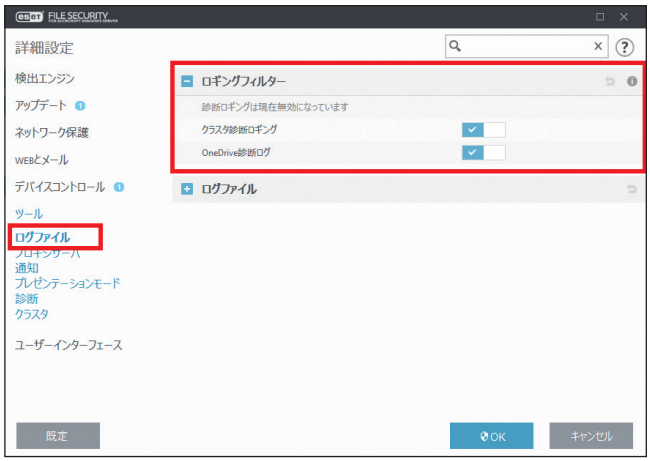
操作手順

1. ユーザーが上書きモードを使用し、ESET File Security for Microsoft Windows Server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。

5.1.17 ログファイル

ログファイルに関する詳細な設定をします。
「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［ツール］＞［ログファイル］を選択します。

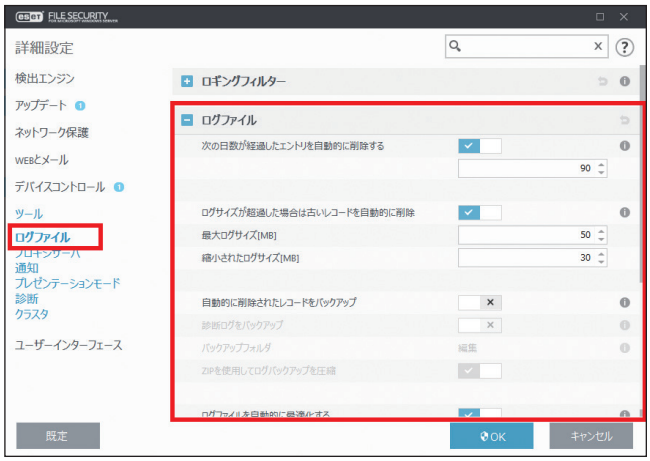
■ロギングフィルター



クラスタ診断ロギングの有効 / 無効と OneDrive 診断ロギングの有効／無効を設定します。

■ログファイル

ログファイルの詳細について設定します。



次の日数が経過したエントリを自動的に削除する	指定された日数を経過したログエントリーは自動的に削除されます。既定では「90」日に設定されており、「1」～「100」日に制限できます。
ログサイズが超過した場合は古いレコードを自動的に削除	ログサイズが「最大ログサイズ［MB］」を超過すると、「縮小されたログサイズ［MB］」になるまで古いログレコードが削除されます。最大ログサイズは既定では「50」MB に設定されており、最大「10000」MB に制限できます。縮小されたログサイズは既定では「30」MB に設定されており、最小「1」MB に制限できます。縮小されたログサイズは、最大ログサイズよりも小さい値である必要があります。
自動的に削除されたレコードをバックアップ	自動的に削除されたログレコードとファイルは指定されたディレクトリーにバックアップされ、任意で ZIP ファイルに圧縮されます。
診断ログをバックアップ	削除された診断ログを自動的にバックアップします。無効にすると、診断ログレコードはバックアップされません。この設定は「自動的に削除されたレコードをバックアップ」を有効にした場合に設定が行えます。

バックアップフォルダ	ログバックアップが保存されるフォルダーを使用して、圧縮されたログバックアップを有効にできます。この設定は「自動的に削除されたレコードをバックアップ」を有効にした場合に設定が行えます。
ZIP を使用してログバックアップを圧縮	ZIP を使用してログバックアップフォルダーを圧縮します。この設定は「自動的に削除されたレコードをバックアップ」を有効にした場合に設定が行えます。
ログファイルを自動的に最適化する	［使用されていないエントリの割合（%）が次の値よりも大きくなったら最適化］フィールドに指定した断片化の割合を超えると、ログファイルは自動的に最適化されます。既定では「25」に設定されており、「1」～「100」% に制限できます。
ログファイルを最適化する	［最適化］をクリックすると、ログファイルの最適化をすぐに開始します。空のログエントリーがすべて削除され、パフォーマンスとログ処理速度が改善します。特にログに多数のエントリー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］をオンにすると、ログファイルとは別のファイル形式でログを保存できます。
次の項目を設定できます。

保存先のフォルダ	ログファイルを保存するディレクトリーを指定します。
タイプ	テキストファイル形式を選択すると、ログがテキストファイルに保存されます。データはタブ区切りです。CSV ファイル形式の場合は、カンマ区切りのデータで保存されます。イベントを選択すると、ファイルではなく、Windows イベントログにログが保存されます（コントロールパネルのイベントビューアーで表示できます）。
すべてのログファイルを削除	「タイプ」ドロップダウンメニューで現在選択されているすべての保存済みログが消去されます。

●ログのフィルタ

ログには、重要なシステムイベントに関する情報が保存されます。ログのフィルタ機能を使用すると、特定の種類のイベントに関するレコードをフィルタリングすることができます。
「ログのフィルタ」画面を表示するには、「ログファイル」画面で特定のログを選択して右クリックして、［フィルタ］をクリックします。



「テキスト検索」フィールドに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を使用して、検索を絞り込みます。

「レコードの種類」ドロップダウンメニューから次のレコードログの種類を 1 つ以上選択します。

診断	プログラムおよび上記のすべてのレコードを微調整するために必要となる情報をログに記録します。
情報	すべての情報メッセージ（アップデートの成功メッセージを含む）と上記のすべてのレコードを記録します。
警告	エラーおよび警告メッセージを記録します。
エラー	（ファイルのダウンロード中にエラーが発生しました）などのエラーを記録します。
重大	重大なエラー（ウイルス対策保護の開始エラーなど）のみを記録します。

その他に次の項目を設定します。

期間	結果を表示する期間を指定します。 •未指定（既定）ー期間内でフィルタリングするのではなく、ログ全体をフィルタリングします。 ・昨日 ・先週 ・先月 ・期間ー正確な期間（日時）を指定して、指定した期間のレコードだけをフィルタリングできます。
開始／終了	検索結果を表示する期間を指定します。
完全一致のみ	特定の完全一致を検索して結果の精度を高めます。
大文字と小文字を区別する	フィルタリングで大文字または小文字を区別します。

●ログ内検索

ログ内の特定のレコードを探す場合役立ちます。この検索機能は、ログのフィルタと同様に、特にレコードが多い場合などに、すばやく目的の情報を探すために役立ちます。

「ログを検索」画面を表示するには、「ログファイル」の一覧画面で特定のログを選択して右クリックして［検索］をクリックします。



ログの検索を使用するときには、「テキスト検索」フィールドに特定の文字列を入力して検索します。「列を検索」ドロップダウンメニューを使用して列でフィルタリングし、［レコードの種類］を選択し、［期間］を設定して、特定の期間のレコードのみを検索できます。必要に応じて検索オプションを指定することにより、その検索オプションに応じた関連するレコードのみが「ログファイル」画面の一覧表で検索されます。

テキスト検索	文字列を入力します（単語または単語の一部）。この文字列を含むレコードのみが検索されます。
列を検索	検索の対象とする列を選択します。検索に使用する種類を次の中から 1 つ以上チェックします。既定では、すべての列がチェックされています。 ・日時 ・検査したフォルダ ・検査数 ・感染数 ・駆除数 ・状態

「レコードの種類」ドロップダウンメニューから次のレコードログの種類を 1 つ以上選択します。

診断	プログラムおよび上記のすべてのレコードを微調整するために必要となる情報をログに記録します。
情報	すべての情報メッセージ（アップデートの成功メッセージを含む）と上記のすべてのレコードを記録します。
警告	エラーおよび警告メッセージを記録します。
エラー	（ファイルのダウンロード中にエラーが発生しました）などのエラーを記録します。
重大	重大なエラー（ウイルス対策保護の開始エラーなど）のみを記録します。

その他に次の項目を設定します。

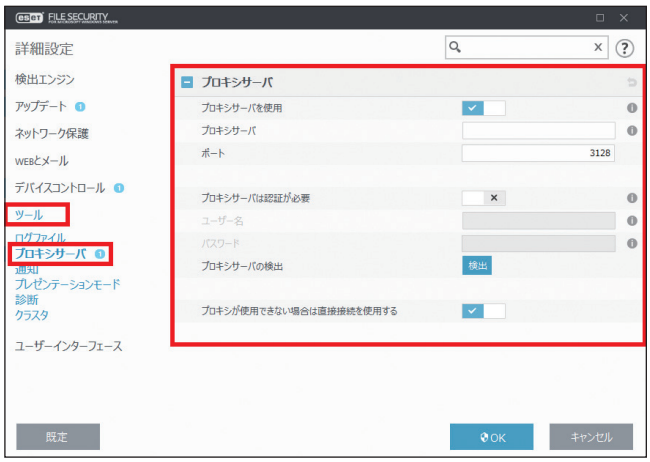
期間	結果を表示する期間を指定します。 ・未指定（既定）－期間内で検索するのではなく、ログ全体を検索します。 ・昨日 ・先週 ・先月 ・期間－正確な期間（日時）を指定して、指定した期間のレコードのみを検索できます。
開始／終了	検索結果を表示する期間を指定します。
完全一致のみ	「テキスト検索」のテキストボックスで指定した文字列と単語と完全一致レコードのみを検索します。
大文字と小文字を区別	大文字と小文字を区別した上で、「テキスト検索」のテキストボックスの文字列と一致するレコードのみを検索します。
上方向に検索	現在の位置から上方向へ検索します。

検索オプションを設定し終えたら、［検索］をクリックして検索を開始します。検索は、一致する最初のレコードが見つかった時点で停止します。再度［検索］をクリックすると、次に一致したレコードで停止します。ログファイルは、現在の位置（強調表示されているレコード）を起点に、下方向へ検索されます。

5.1.18 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。この場合は、次の設定をしないと、プログラムの自動更新は行われません。
次の方法でプロキシサーバーを設定します。

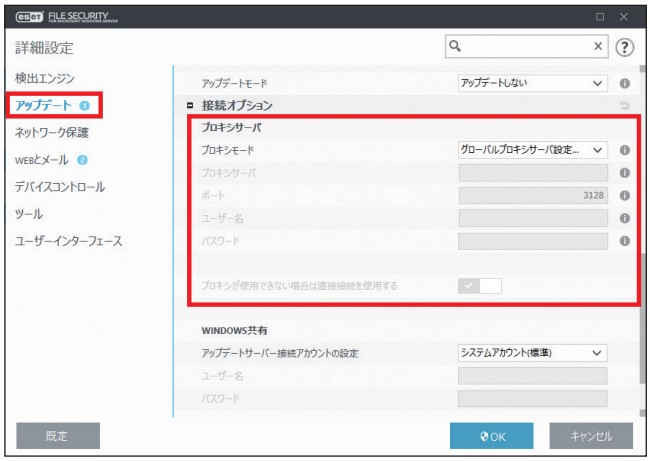
「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［ツール］＞［プロキシサーバ］を選択します。



ここでプロキシサーバーを設定すると、ESET File Security for Microsoft Windows Server 全般で使用されるプロキシサーバーの設定として利用されます。

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	サーバーのアドレスを指定します。
ポート	サーバーのポート番号を指定します。プロキシサーバーの既定のポート番号は「3128」です。
プロキシサーバは認証が必要	ユーザー認証が必要なサーバーの場合は有効にします。
ユーザー名	ユーザー名を指定します。
パスワード	パスワードを指定します。
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アップデートします。

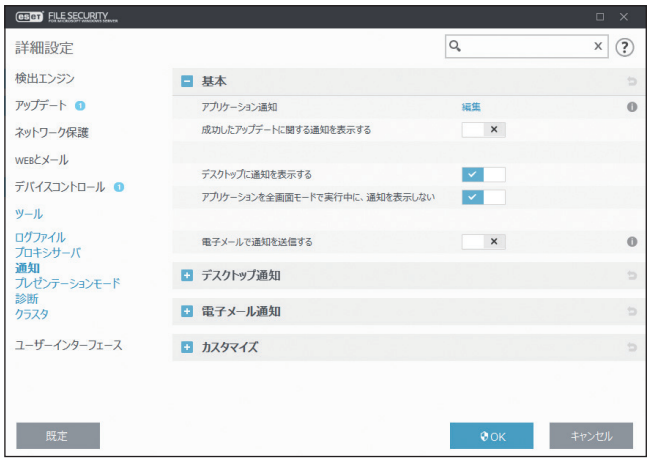
プロキシサーバー設定は詳細設定のアップデート設定内（[詳細設定] > [アップデート] > [プロファイル] > [アップデート] > [接続オプション] > [プロキシサーバ]）からも定義できます。



「プロキシモード」ドロップダウンメニューから［プロキシサーバを使用して接続する］を選択します。この設定は、特定のアップデートプロファイルに適用されます。検出エンジンのアップデートを様々な場所から受信するノート型コンピューターなどにお勧めします。この設定の詳細については、「5.1.8　アップデート」を参照してください。

5.1.19　通知

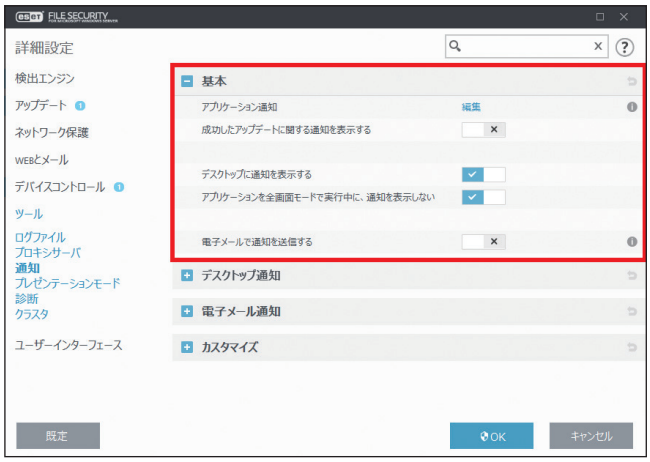
ESET File Security for Microsoft Windows Server は、発生したイベントを様々な方法でユーザーに通知できます。通知の設定を行うには、「詳細設定」画面で、［ツール］>［通知］をクリックします。ここでは、以下のタイプの通知に関しての設定が行えます。



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

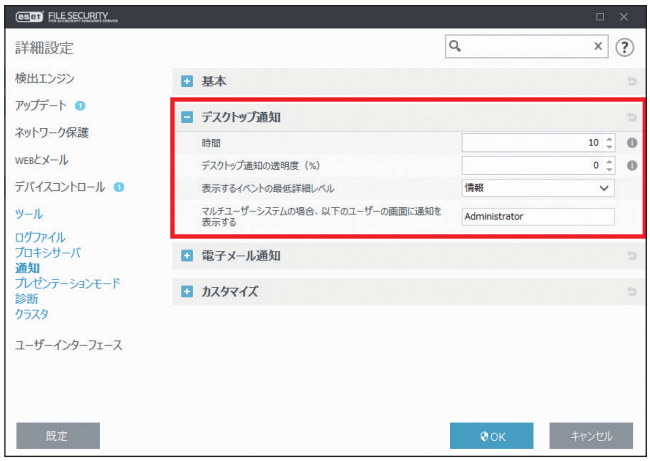
「基本」セクションでは、次の項目を調整できます。



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。
成功したアップデートに関する通知を表示する	有効にすると、製品がコンポーネントと検出エンジンモジュールをアップデートするときに通知を表示します。
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	全画面モードでアプリケーションが実行されているときはデスクトップ通知を表示しません。
電子メールで通知を送信する	有効にすると、電子メール通知を有効にします。

■デスクトップ通知

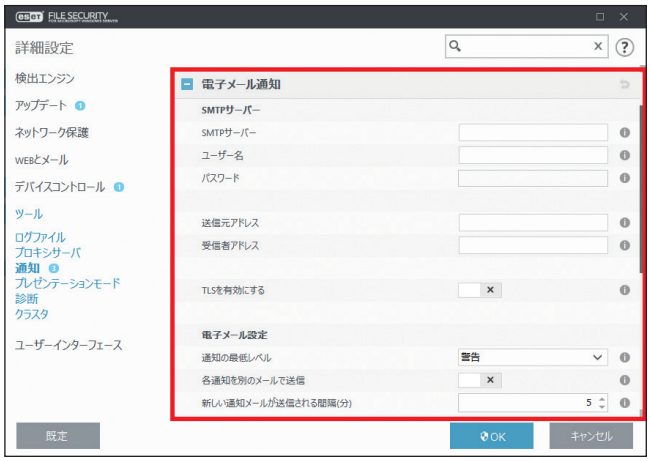
デスクトップ通知は、タスクバーの横に小さいポップアップウィンドウで表示されます。既定では、10 秒間表示され、ゆっくりと消えるように設定されています。既定では、ESET File Security for Microsoft Windows Server が製品のアップデートの成功したり、新しく接続されたデバイスを検出したり、ウイルス検査タスクが完了したり、脅威を検出したりしたときに、ユーザーに通知する主な手段として利用されています。「デスクトップ通知」セクションでは、ポップアップ通知の動作をカスタマイズできます。



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。この設定は、「基本」セクションの「電子メールで通知を送信する」を有効に設定してから行います。



● 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	通知メールを送信するために使用される SMTP サーバーを指定します。
ユーザー名 **パスワード**	SMTP サーバーで認証が必要な場合、ユーザー名とパスワードを指定します。
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指定します。
受信者アドレス	通知メールのヘッダーに表示される受信者アドレスを指定します。
TLS を有効にする	TLS 暗号化を使用して通知メッセージを保護します。

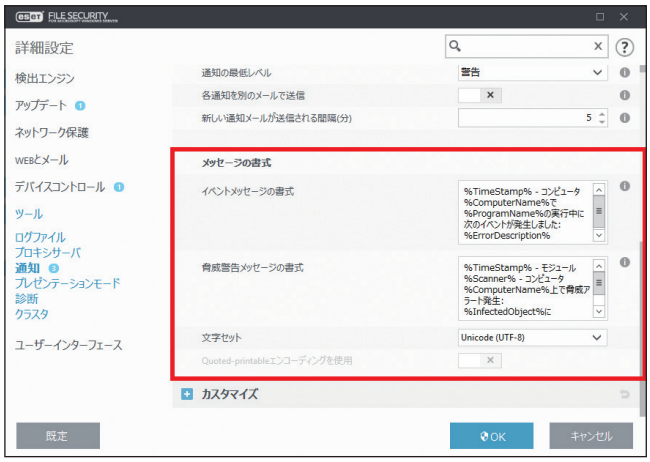
●電子メール設定

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	自動的に挿入されるイベントメッセージの一部を定義します。下記ワンポイントを参照してください。
脅威警告メッセージの書式	自動的に挿入される脅威警告の一部を定義します。下記ワンポイントも参照してください。
文字セット	電子メールメッセージの文字コードを設定します。設定は、「ローカル」「Unicode（UTF-8）」「Ascii（7bit）」「Japanese（ISO-2022-JP）」の中から選択できます。
Quoted-printable エンコーディングを有効にする	電子メールメッセージのソースを、Quoted-printable（QP）書式でエンコードします。この設定は、文字セットに「ローカル」を選択した場合に設定できます。

ワンポイント

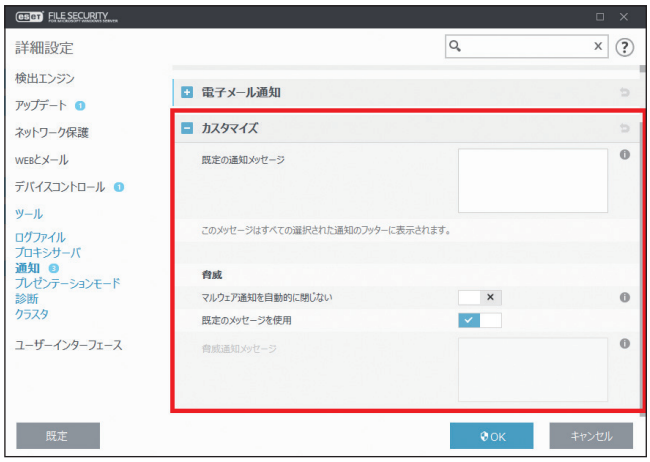
メッセージ内では次のキーワードを使うことができます。指定されている実際の情報でキーワード（「%」記号で区切られた文字列）が置き換えられます。次のキーワードを使うことができます。

%TimeStamp%	イベントの日時
%Scanner%	関連するモジュール
%ComputerName%	警告が発生したクライアントコンピューターの名前
%ProgramName%	警告を生成したプログラムの名前
%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
%ErrorDescription%	ウイルス以外のイベントの説明

キーワード「%InfectedObject%」と「%VirusName%」はマルウェア警告メッセージのみで使用され、「%ErrorDescription%」はイベントメッセージのみで使用されます。

■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。

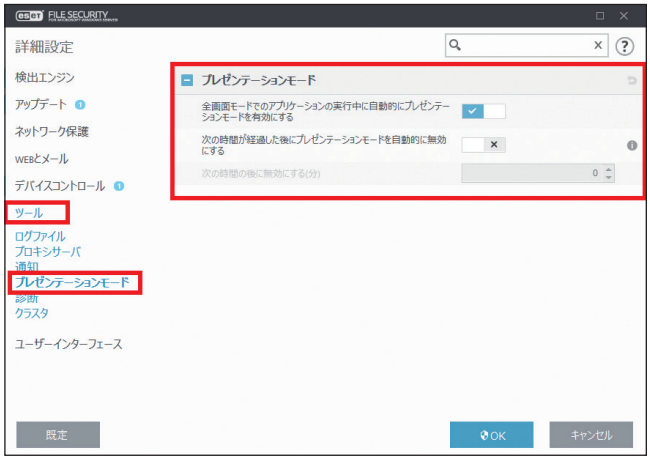
5.1.20 プレゼンテーションモード

プレゼンテーションモードは、ポップアップウインドウ、アップデート、スケジュールタスクを無効にして、CPU の使用量を最小化します。システムの保護は引き続きバックグラウンドで実行されます。プレゼンテーション中など、セキュリティの処理でコンピューターの動作が中断されたくない時に便利な機能です。

プレゼンテーションモードを使用するときは、メインメニューの［設定］＞［コンピュータ］で、「プレゼンテーションモード」を有効にします。



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発生するため、タスクバーの状態アイコンに黄色の「！」マークが追加され、警告が表示されます。この警告は「監視」画面（メインメニューの［監視］をクリック）でも確認でき、「プレゼンテーションモードは有効です」が黄色で表示されます。
「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［ツール］＞［プレゼンテーションモード］を選択し、詳細な設定をします。

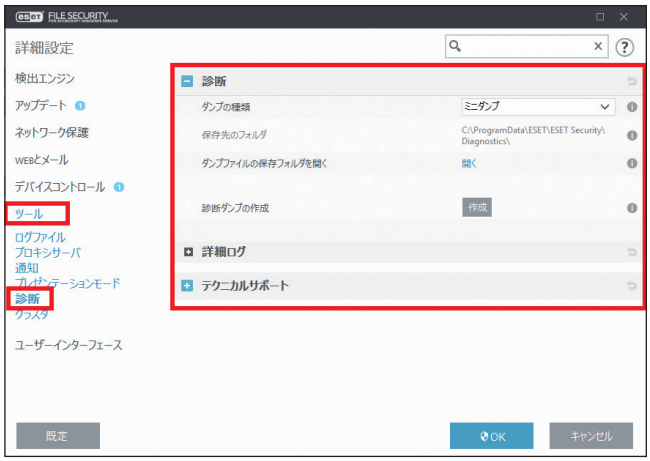


全画面モードでのアプリケーションの実行中に自動的にプレゼンテーションモードを有効にする	アプリケーションを全画面モードで起動したときに、プレゼンテーションモードが自動的に開始されます。アプリケーションを終了すると、プレゼンテーションモードは自動的に停止します。ゲームやプレゼンテーションなど、全画面で使用するアプリケーションを使用する場合に便利です。
次の時間が経過した後にプレゼンテーションモードを自動的に無効にする	プレゼンテーションモードが自動的に停止する時間を分単位で設定できます。制限値は「0」～「2000」分です。

5.1.21 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、様々な問題をデバッグまたは修正できます。

「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［ツール］＞［診断］を選択します。



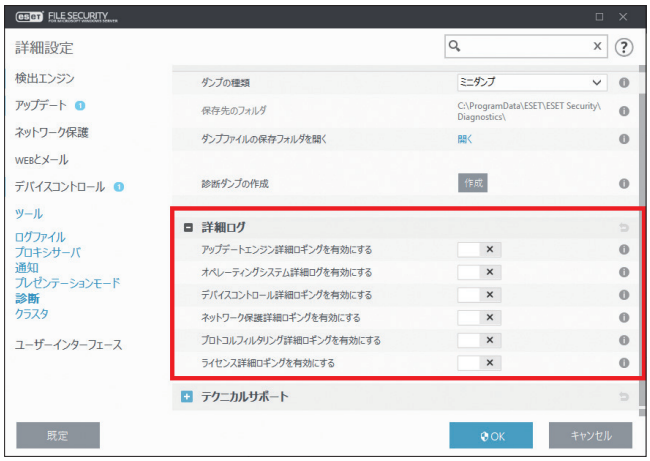
■診断

「診断」セクションでは、ESET プロセス（.ekm など）のアプリケーションクラッシュダンプの種類や保存先フォルダーなどに関する設定を行います。

ダンプの種類	メモリダンプを使用しない	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。
	完全なメモリダンプ	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。	

●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。



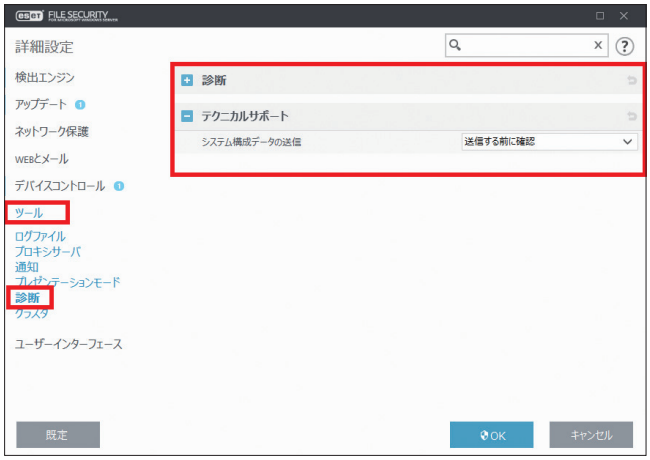
アップデートエンジン詳細ロギングを有効にする	有効に設定すると、アップデート処理中に発生するすべてのイベントを記録します。
オペレーティングシステム詳細ログを有効にする	実行中のプロセス、CPU アクティビティ、ディスク処理などのオペレーティングシステムに関する追加情報が収集されます。
デバイスコントロール詳細ロギングを有効にする	有効に設定すると、デバイスコントロールで発生するすべてのイベントを記録します。
ネットワーク保護詳細ロギングを有効にする	有効に設定すると、PCAP 形式でファイアウォール経由のすべてのネットワークデータ転送を記録します。
プロトコルフィルタリング詳細ロギングを有効にする	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。
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。

■テクニカルサポート

テクニカルサポートに、システム構成データを送信する方法を設定します。

「詳細設定」画面の［ツール］＞［診断］＞［テクニカルサポート］をクリックします。

「システム構成データを送信」ドロップダウンメニューから［常に送信］または［送信する前に確認］を選択します。



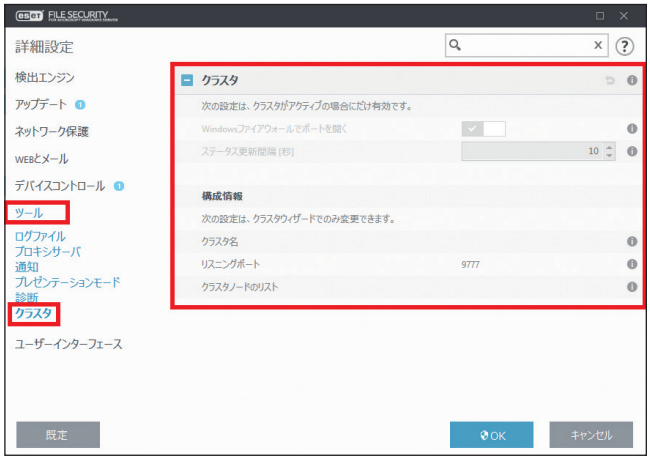
5.1.22 クラスタ

クラスタを使うと、ESET サーバー製品は相互に通信し、構成や通知などのデータを交換します。また、製品グループが正しく動作するために必要なデータを同期することができます。例えば、Windows Failover Cluster やネットワーク負荷分散（NLB）クラスター内のノードをグループで管理する場合に有用です。ESET Cluster では、インスタンス間でこの整合性を保証します。
クラスタが構成されると「設定」メニューの「サーバー」で［クラスタ］が有効になります。
クラスタを構成するには、この画面で［クラスタウィザード］をクリックします。



■クラスタの詳細設定

「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［ツール］＞［クラスタ］を選択し、クラスタの詳細な設定をします。
クラスタが構成され有効な場合のみ設定できます。



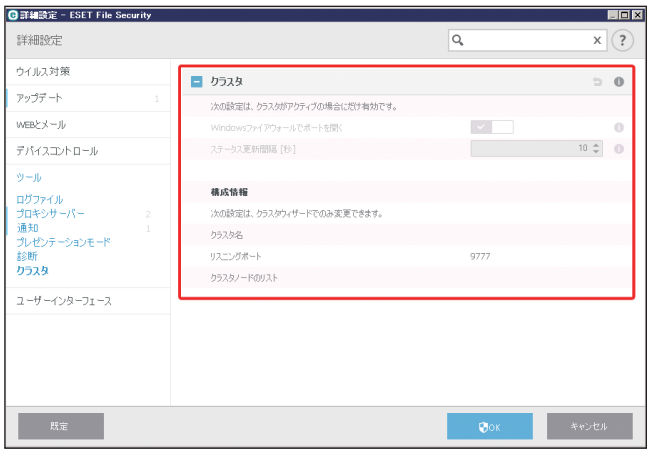
Windows ファイアウォールでポートを開く	Windows ファイアウォールでポートを開く場合に有効にします。
ステータス更新間隔	ステータスの更新間隔を秒数で指定します。

■クラスタの有効 / 無効

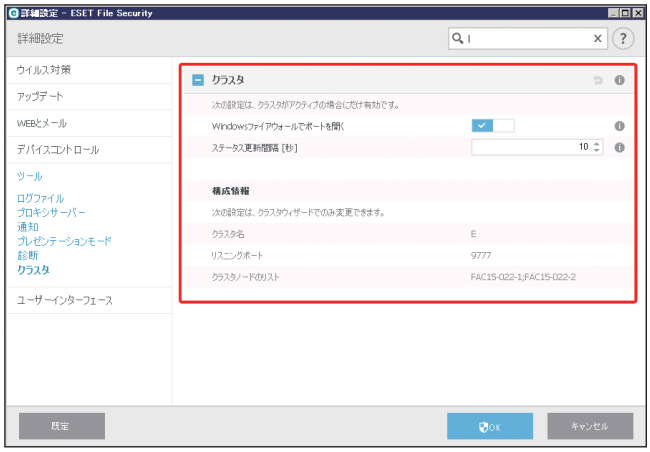
クラスタを正しく設定または無効にするには、メインメニューの［ツール］＞［クラスタ］をクリックし、[クラスタウィザード］または［クラスタの無効化］を使用します。



クラスタが構成されておらず無効な場合は、次の画面が表示されます。



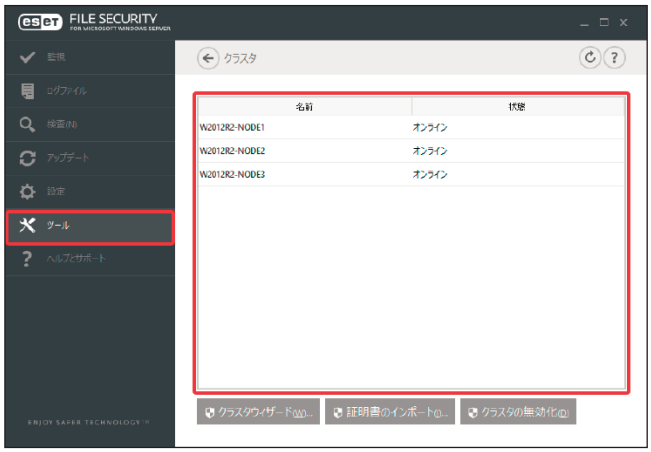
クラスタが詳細設定のオプションで正しく構成されている場合は、次のような画面になります。



クラスタに関する詳細情報については、「4.5.4　クラスタ」を参照してください。

■クラスタの構成

クラスタのステータスページを表示するには、メインメニューの［ツール］＞［クラスタ］をクリックします。正しく設定されていると、ステータスページは次のように表示されます。



クラスタを設定するには、［クラスタウィザード］をクリックします。ウィザードを使用してクラスタを設定する方法の詳細については、「●クラスタウィザード」を参照してください。

クラスタを設定する際、ノードを追加するには次の 2 つの方法があります。

- 既存の Windows Failover Cluster / NLB クラスタを使用して自動的に追加する（自動選択）
- ワークグループまたはドメインにあるクライアントコンピューターを参照して手動で追加する（参照）

自動選択	Windows Failover Cluster / NLB クラスターのメンバーであるノードを自動的に検出し、クラスタに追加します。
参照	サーバー名（同じワークグループのメンバーまたは同じドメインのメンバーのいずれか）を入力してノードを手動で追加することができます。

！重　要

クラスタ機能を使用するために、サーバーが Windows Failover Cluster / NLB クラスターのメンバーである必要はありません。Windows Failover Cluster または NLB クラスターは必須ではありません。

ESET にノードを追加した後、各ノード上に ESET File Security for Microsoft Windows Server をインストールします。これは、クラスタ設定中に自動的に行われます。
ESET Cluster ノード上の ESET File Security for Microsoft Windows Server のリモートインストールに必要な資格情報としては、ドメインシナリオの場合はドメイン管理者の資格情報を、ワークグループシナリオの場合はすべてのノードが同じローカル管理者アカウントの資格情報を使用していることが必要になります。

クラスタでは、既存の Windows Failover Cluster / NLB クラスターのメンバーとして自動で追加したノードと手動で追加したノードの組み合わせを使用することもできます（同じドメインにある場合）。

！重　要

ドメインノードとワークグループノードを組み合わせることはできません。

クラスタを使用するための他の要件：

クラスタノード上に ESET File Security for Microsoft Windows Server をインストールする前に、Windows ファイアウォールでファイルとプリンターの共有を有効にする必要があります。

［クラスタの無効化］をクリックすると、クラスタを無効にすることができます。各ノードは、無効にしたクラスタに関するイベントログに記録を書き込みします。その後、すべての ESET のファイアウォールルールは Windows ファイアウォールから削除されます。元のノードは以前の状態に戻り、必要に応じて他のクラスタで再度使用することができます。新たなノードを既存クラスタに追加するには、次の項目で記載している［クラスタウィザード］を実行する方法と上記の手順があります。

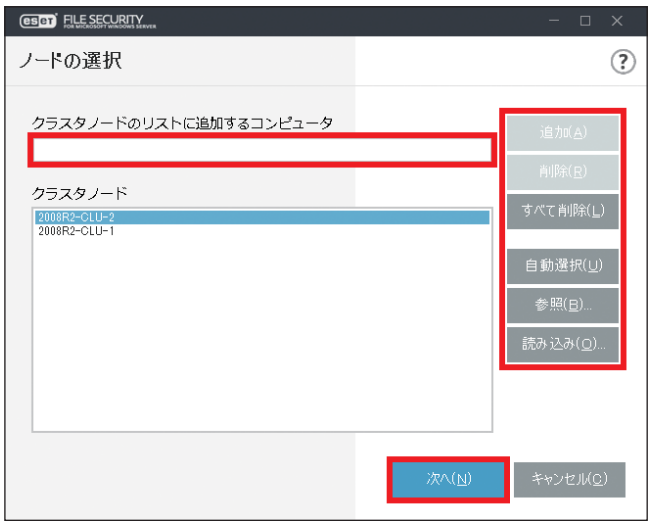
●クラスタウィザード（1 ページ目）

クラスタを設定する最初のステップはノードの追加です。［自動選択］または［参照］オプションのいずれかを使用してノードを追加します。または、［クラスタノードのリストに追加するコンピュータ］のテキストボックスにサーバー名を入力して、［追加］ボタンをクリックします。

［自動選択］を使用すると、既存の Windows Failover Cluster / NLB クラスターから自動的にノードを追加します。クラスタを作成するために使用するサーバーは、ノードを自動追加するためには Windows Failover Cluster / NLB クラスタのメンバーである必要があります。NLB クラスターには、クラスタがノードを正しく検出するためにクラスタのプロパティで有効にする［リモート制御許可］機能が必要です。クラスタ内の特定のノードのみを追加する場合、新たに追加したノード一覧の入手後に、不要なものを削除することができます。
［参照］＞［詳細設定］をクリックすると、ドメインまたはワークグループ内のクライアントコンピューターを検索してノードを選択できます。これで、ノードをクラスタに手動で追加することができます。

ノードを追加する別の方法は、［クラスタノードのリストに追加するコンピュータ］のテキストボックスに追加するサーバーのホスト名を入力して、［追加］をクリックします。

［次へ］をクリックし、クラスタノードのリストに表示されているクラスタノードを追加する手順を進めます。



リスト内のクラスタノードを削除するには、ノードを選択して［削除］をクリックします。また、リストを完全に消去するには［すべて削除］をクリックします。

既存のクラスタが存在する場合は、上記と同じ手順で新しいノードを追加できます。

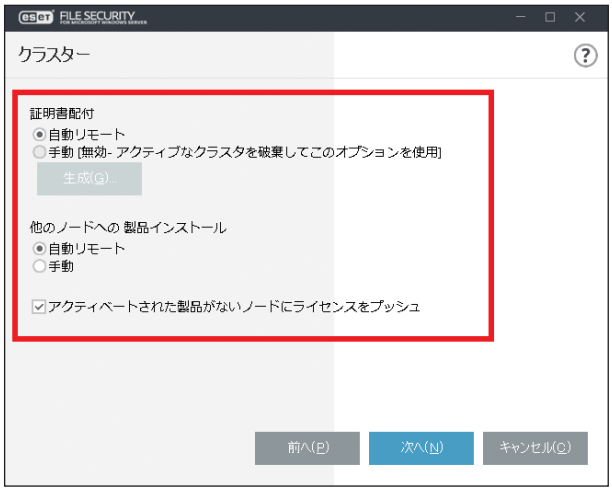
！重　要

リストに残っているすべてのクラスタノードは、オンラインでアクセス可能でなければなりません。ローカルホストはクラスタノードに既定で追加されます。

●クラスタウィザード（2 ページ目）

クラスター名、証明書配付モードおよび他のノードに製品をインストールする方法を定義します。





画面に表示される項目は次のとおりです。

クラスタ	クラスター名を入力します。	
リスニング ポート	リスニングポートを入力します。既定では「9777」に設定されています。	
Windows ファイアウォールでポートを開く	チェックを入れると、ルールを確認するときに Windows ファイアウォールでポートが開放されます。	
証明書配付	自動リモート	証明書が自動的にリモートでインストールされます。
	手動	［生成］をクリックすると、「フォルダーの参照」画面が開きます。証明書の保存先フォルダーを選択します。ルート証明書と、クラスタを設定しているノード（ローカルコンピューター）を含む各ノードの証明書が作成されます。［OK］をクリックして、ローカルコンピューターの証明書を登録することもできます。証明書は手動でインポートする必要があります。証明書のインポートについて詳しくは、「●クラスタウィザード（4 ページ目）」の「証明書のインポート」を参照してください。
他のノードへの製品インストール	自動リモート	ESET File Security for Microsoft Windows Server は、各ノードに自動的にリモートでインストールされます（例えば、オペレーティングシステムが同じプラットフォームの場合）。
	手動	ESET File Security for Microsoft Windows Server を手動でインストールする場合に選択します（例えば、複数のノードに異なるオペレーティングシステムのプラットフォームがある場合）。
アクティベートされた製品がないノードにライセンスをプッシュ	チェックをいれると、ノードの ESET File Security for Microsoft Windows Server がアクティベートされます。	

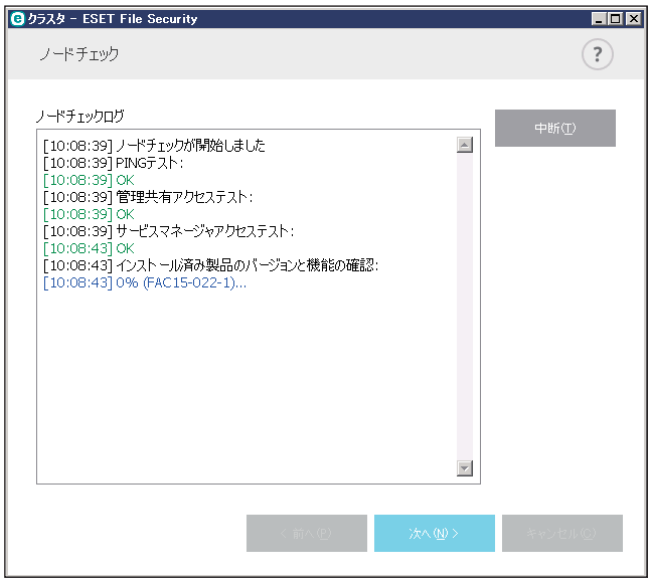
！重　要

オペレーティングシステムのプラットフォーム（32 bit および 64 bit）が混在している環境でクラスタを作成する場合は、ESET File Security for Microsoft Windows Server を手動でインストールする必要があります。これは、次のステップの間に検出され、ログ画面でこの情報を参照することができます。

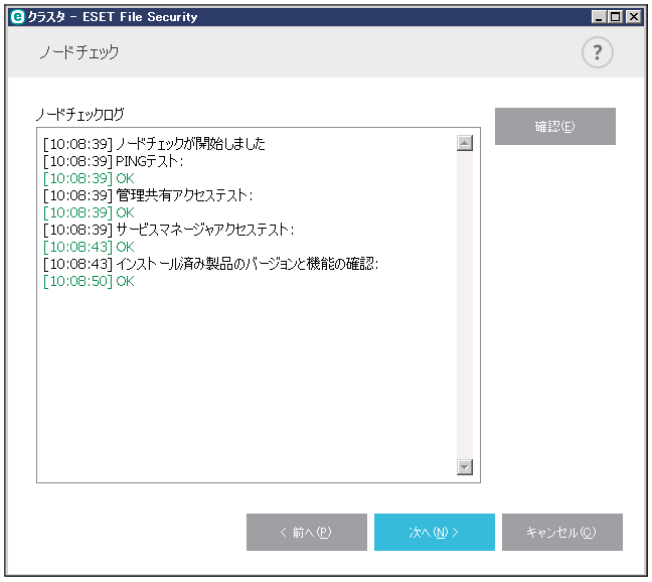
●クラスタウィザード（3 ページ目）

インストールの詳細を指定した後、ノードチェックが実行されます。
ノードチェックログで次の確認内容を参照することができます。

- 既存のノードがオンラインである
- 新しいノードがアクセス可能である
- ノードがオンラインである
- 管理者共有がアクセス可能である
- リモート実行が可能である
- 製品の正しいバージョンがインストールされている、または製品がインストールされていない（自動インストールが選択されている場合のみ）
- 新規証明書の存在

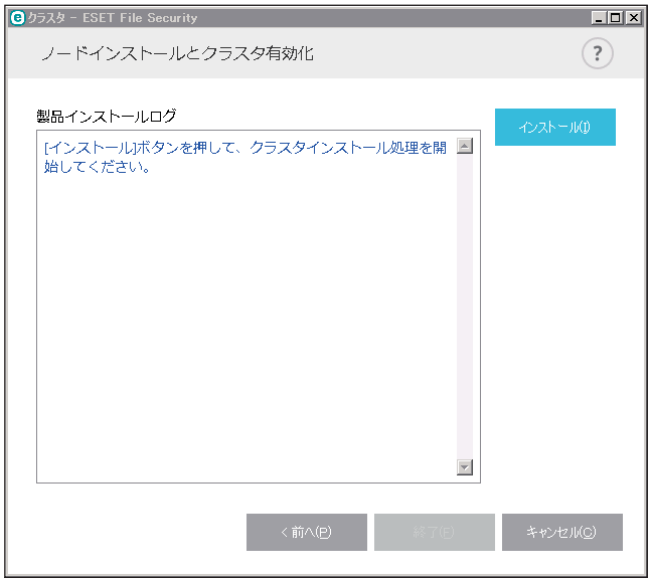


ノードチェックが完了すると次のレポートが表示されます。



●クラスタウィザード（4 ページ目）

クラスタの初期化中に製品をリモートコンピューターにインストールする必要がある場合、インストーラーパッケージは %ProgramData%\ESET\ < Product_name > \Installer ディレクトリーにインストーラーが存在するかどうかを確認します。インストーラーパッケージが検索されない場合は、ユーザーが検索する必要があります。

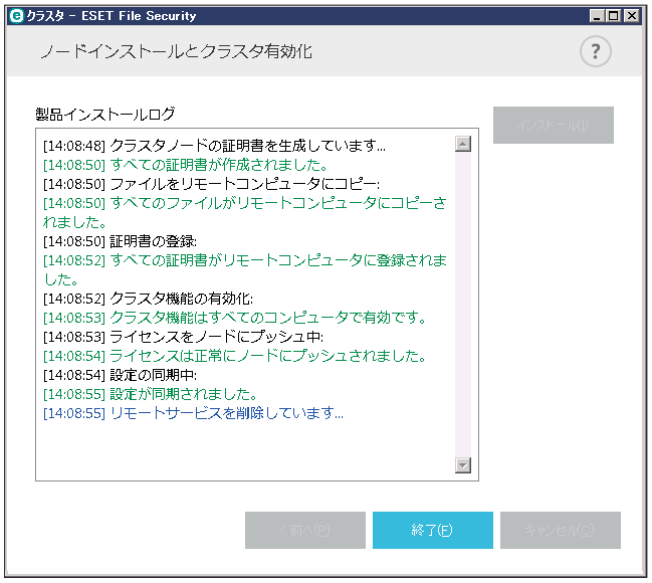


!重　要

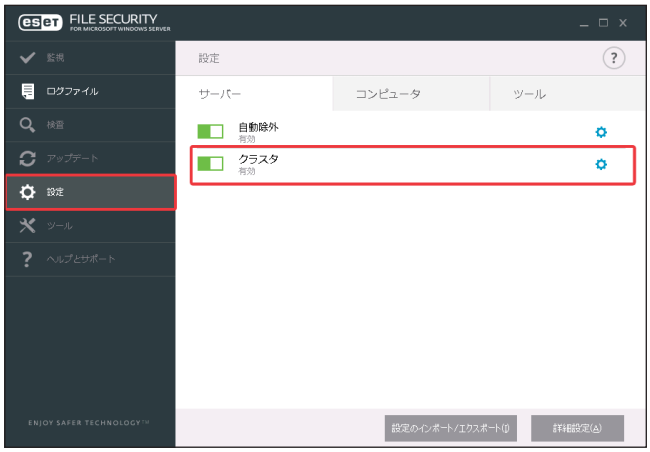
異なるプラットフォーム（32 bit と 64 bit）を持つノードで自動リモートインストールを使用しようとするとプラットフォームの違いが検出されます。このようなノードでは手動でインストールします。

!重　要

ESET File Security for Microsoft Windows Server の古いバージョンが一部のノードに既にインストールされている場合は、クラスターを作成する前に、これらのノードで新しいバージョンを再インストールする必要があります。これにより、ノードが自動的に再起動する場合があります。再起動する前に警告画面が表示されます。



クラスタを正しく構成すると、「設定」画面の「サーバー」ページで［クラスタ］が有効（緑スイッチアイコン）になります。



また、「クラスタ」画面で現在の状態を確認することができます（メインメニューの［ツール］＞［クラスタ］）。



証明書のインポート

操作手順

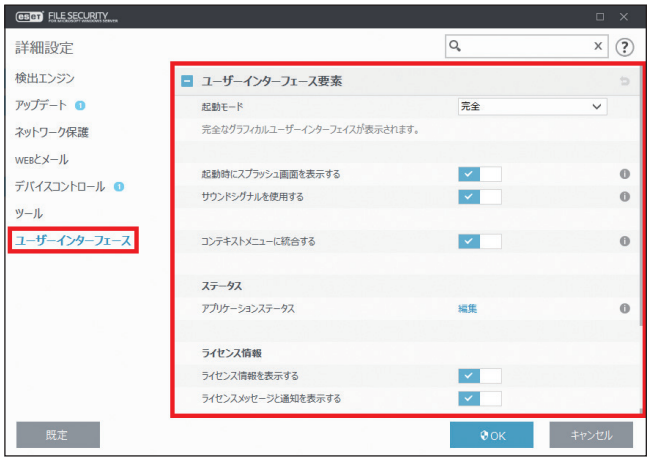
1. 「クラスタ」画面下部の［証明書のインポート］をクリックすると、証明書（クラスタウィザードの使用中に生成される）が含まれているフォルダーに移動します。
2. 証明書ファイルを選択し、［開く］をクリックします。

5.1.23 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 File Security for Microsoft Windows Server 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。
「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［ユーザーインターフェース］を選択します。

■ユーザーインターフェース要素

作業環境をカスタマイズできます。



「ユーザーインターフェース要素」の項目では、作業環境を調整できます。視覚的要素によってコンピューターのパフォーマンスが低下する場合などは、起動モードを［ターミナル、端末］に設定してください。

「起動モード」ドロップダウンメニューをクリックして、次の GUI 起動モードを選択します。

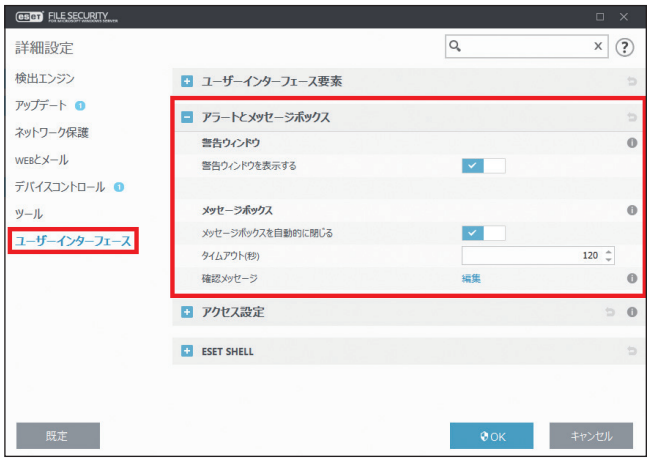
完全	すべての GUI を表示します。
ターミナル、端末	通知やアラートは表示されません。このモードは管理者によってのみ設定できます。

その他に次の項目を設定できます。

起動時にスプラッシュ画面を表示する	無効にすると、ESET File Security for Microsoft Windows Server 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	コントロール要素をコンテキストメニュー（右クリックで表示されるメニュー）に統合します。
アプリケーションステータス	［編集］をクリックすると、メインメニューの「監視」のプライマリーウインドウに表示するアプリケーションステータスを選択できます。
ライセンス情報を表示する	無効にすると、「監視」のライセンス情報が非表示になり、［ヘルプとサポート］画面のライセンスの有効期限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。

■アラートとメッセージボックス

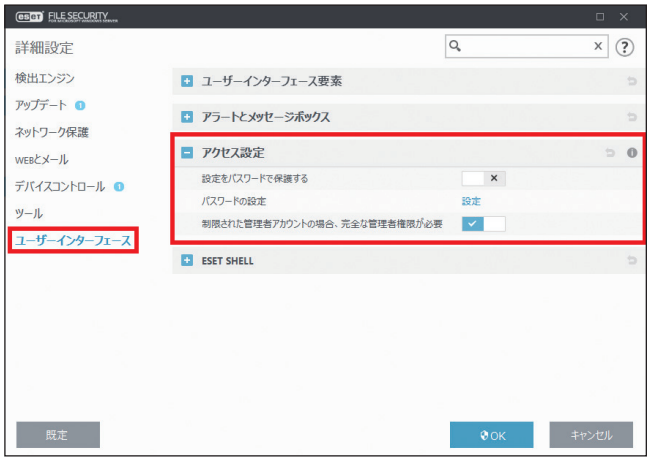
「アラートとメッセージボックス」セクションでは、警告メッセージやシステム通知（ウイルスの検出メッセージやアップデートの成功メッセージなど）をどのように表示するかを設定できます。



警告ウィンドウ	「警告ウィンドウを表示する」を無効にすると、すべての警告画面が表示されなくなります。無効にするのは特定の限られた状況のみです。通常は、有効のままにすることをお勧めします。	
メッセージボックス	メッセージボックスを自動的に閉じる／タイムアウト（秒）	有効にすると、「タイムアウト（秒）」で指定した時間の経過後、警告や通知が自動的に閉じます。警告や通知は手動で閉じることもできます。既定値は「120」秒、制限値は「10」～「999」秒です。
	確認メッセージ	［編集］をクリックすると、確認メッセージの有効／無効を設定できます。

■アクセス設定

システムのセキュリティを最大限確保するには、ESET File Security for Microsoft Windows Server を正しく設定することが重要です。権限のないユーザーなどによって ESET File Security for Microsoft Windows Server 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 File Security for Microsoft Windows Server 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。パスワード保護の設定を表示するには、「詳細設定」画面の［ユーザーインターフェース］＞［アクセス設定］をクリックします。



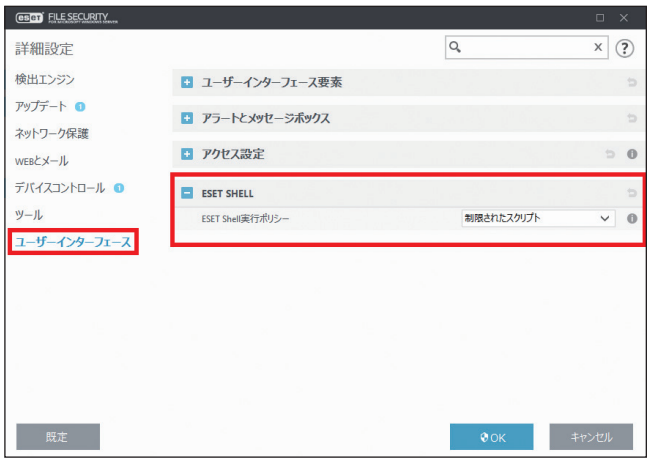
この項目では次の内容を設定できます。

設定をパスワードで保護する	ESET File Security for Microsoft Windows Server の設定パラメーターをパスワードで保護します。「アイコン（無効）」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、「アイコン（有効）」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、管理者権限がないユーザーの場合、設定変更時に管理者の認証情報の入力を要求されます。

■ ESET SHELL

ESET Shell を使用して、設定、機能、データへのアクセス権を設定することができます。

ESET SHELL を表示するには、「詳細設定」画面の［ユーザーインターフェース］＞［ESET SHELL］をクリックします。



ESET Shell 実行ポリシーは次の内容から選択できます。

無効	ESET Shell は無効になります。ESET Shell の構成は、「ui eshell」コンテキストでのみ許可されます。ESET Shell の表示はカスタマイズできますが、セキュリティ製品の設定またはデータにはアクセスできません。
読取専用	ESET Shell は監視ツールとして使用できます。インタラクティブモードとバッチモードではすべての設定を表示できますが、読み取り専用モードのため、設定、機能、またはデータの修正はできません。
制限されたスクリプト	既定のモードです。インタラクティブモードでは、すべての設定、機能、またはデータを表示して修正できます。バッチモードは読み取り専用モードのため、設定とデータは修正できません。ただし、署名されたバッチファイルを使用している場合は、設定を変更し、データを修正できます。
フルアクセス	インタラクティブモードとバッチモードの両方で、すべての設定に無制限にアクセスできます。すべての設定を表示して修正できます。このモードは、管理者アカウントでのみ使用できます。また、UAC が有効な場合は、管理者権限が必要になります。

●ターミナルサーバーでの GUI の無効化

この項目では、Windows ターミナルサーバーで稼働している ESET File Security for Microsoft Windows Server の GUI を、ユーザーセッションで無効にする方法を説明します。

通常、ESET File Security for Microsoft Windows Server の GUI は、リモートユーザーがサーバーにログオンして、端末セッションを作成するたびに開始されます。ターミナルサーバーでは、この動作は通常望ましくありません。端末セッションで GUI を無効にするには、次の手順を実行します。

操作手順

eShell で `setui ui gui-start-mode terminal` コマンドを実行します。

GUI がターミナルモードになります。

ワンポイント

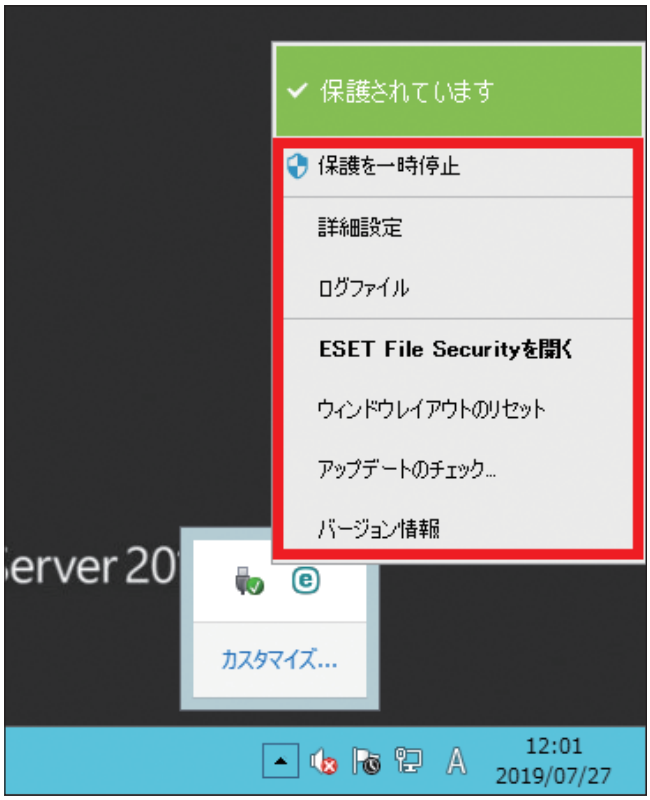
GUI 起動には次の 2 つのモードがあります。

```
set ui ui gui-start-mode full
set ui ui gui-start-mode terminal
```

現在のモードを確認するには、`get ui ui gui-start-mode` コマンドを実行します。

■システムトレイアイコン

システムトレイアイコンⓔを右クリックすると、メニューが表示されます。このメニューから、いくつかの設定オプションや機能にアクセスできます。



メニューには次の項目が表示されます。

保護を一時停止	一時的に保護を停止する場合はここから設定します。ファイル、Web、およびメール通信を制御して、ウイルス・スパイウェア対策を無効にするための確認画面が表示されます。
詳細設定	「詳細設定」画面を表示するには、このオプションを選択します。他にも、【F5】キーを押すか、メインメニューの［設定］＞［詳細設定］から「詳細設定」画面を表示することもできます。
ログファイル	ログファイルには、発生したすべての重要なプログラムイベントに関する情報が保存され、検出されたマルウェアの概要が表示されます。
ESET File Security を開く	ESET File Security for Microsoft Windows Server を開きます。
ウィンドウレイアウトのリセット	ESET File Security for Microsoft Windows Server の画面を既定のサイズにリセットし、画面中央の位置に移動します。
アップデートのチェック	検出エンジンのアップデートを開始し、最大保護を確保します。
バージョン情報	システム情報、インストールされている ESET File Security for Microsoft Windows Server のバージョンの詳細、およびインストールされているプログラムモジュールが表示されます。著作権情報は、ページの下部に表示されます。

保護を一時停止

システムトレイアイコンを使用して、ウイルス対策とスパイウェア対策を一時的に無効にすると、「保護を一時停止」画面が表示されます。ここで選択した期間（間隔）の間、ウイルス対策とスパイウェア対策の保護を無効にします（保護を永続的に無効にするには、詳細設定から行います）。保護を無効にすると、システムが脅威にさらされる可能性があります。無効にする際は十分注意してください。



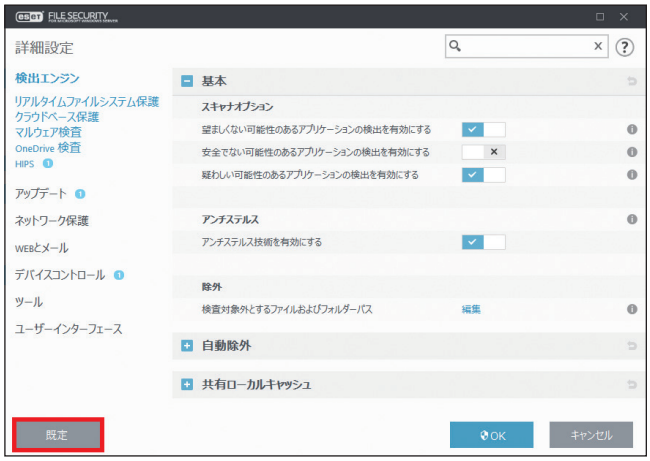
「間隔」ドロップダウンメニューから、すべてのウイルス・スパイウェア対策保護機能を無効にする期間を設定します。

5.1.24 デフォルト設定に戻す

「詳細設定」画面で、設定を既定値に復元できます。2 つのオプションがあります。すべてを既定値に戻すか、特定のセクションの設定のみを戻すことができます。

●すべての設定を戻す

［既定］をクリックすると、詳細設定のすべてのセクションのすべての設定が、ESET File Security をインストールした後の状態に戻されます。

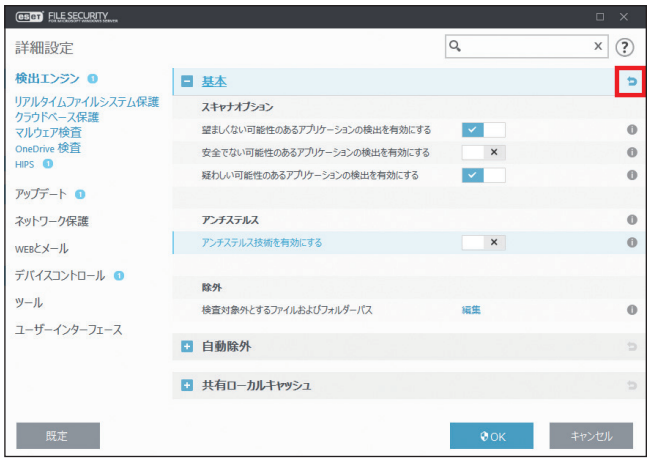


！重　要

既定値に戻すをクリックすると、すべての変更が失われます。このアクションは元に戻せません。

●このセクションのすべての設定を元に戻す

元に戻したいセクションの ↩ をクリックすると、選択したセクションのモジュール設定を値に戻します。このセクションのすべての変更は失われます。



5.1.25 ヘルプとサポート

【F1】キーを押すか、「詳細設定」画面右上の［?］ボタンをクリックすると、「オンラインヘルプ」画面が開きます。ESET File Security for Microsoft Windows Server には、オフラインヘルプもインストールされています。オフラインヘルプは、インターネットに接続していない場合などに開きます。



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 脅威

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影響度は多種多様です。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。

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。

従って、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	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
ダイヤラー	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です。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様々な機能を使用して、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。大半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、アドウェアなしで目的のプログラム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うこともあります。これは、そのアドウェアが頻繁にシステムに「合法的に」アクセスする可能性があることを意味します。ユーザーがアドウェアのインストールに同意したからです。

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様々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 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を感染させます。このタイプのプログラムによって、ハッカーが同時に複数のコンピュータを乗っ取り、これらのコンピュータをボット（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を感染させます。このような大規模な感染コンピュータのグループがボットネットと呼ばれます。コンピュータが感染し、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）で使用されることができます。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使用することもできます（迷惑メール、ウイルスの送信、または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）。

6.1.8 ランサムウェア

強奪目的で使用される特定の種類のマルウェアソフトウェア。アクティブ化されると、ランサムウェアは、被害者が料金を支払うまでデバイスまたはデータへのアクセスを防止します。

6.1.9 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。

6.1.10 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、包括的な様々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。

6.1.11 詳細メモリ検査（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。

6.1.12 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アプリケーションは多くあります。これが、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 File Security for Microsoft Windows Server にはこのような脅威を検出するオプションがあります。
「潜在的に危険性のあるアプリケーション」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。

潜在的に危険性のあるアプリケーションが存在し、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に連絡するか、そのアプリケーションを削除してください。

6.1.13 潜在的に不要なアプリケーション

必ずしも悪意があるとは限りませんが、コンピューターのパフォーマンスに悪影響を与える可能性のあるアプリケーションです。通常、このようなアプリケーションをインストールするには同意が必要です。このようなアプリケーションをコンピューターにインストールすると、インストール前とは異なる状態でシステムが動作します。
最も大きな違いは次のとおりです。

- これまでに表示されたことがない新しい画面が開く
- 隠しプロセスがアクティブになり、実行される
- システムリソースの使用率が高くなる
- 検索結果が異なる
- アプリケーションがリモートサーバーと通信する