法人向けサーバー専用製品

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。

改定日　2017/4/30

目　次

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。

- クラスタ機能—ESET 製品はそれぞれ通信をして構成や通知などのデータを交換します。さらに、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。クラスター全体で製品の構成は同じです。Windows Failover Cluster と Network Load Balancing (NLB) Cluster は、ESET File Security for Microsoft Windows Server によってサポートされています。また、クラスタメンバーを手動で追加できます。その際、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。
- 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。これにより、ファイルサーバーに保存されたユーザーデータを選択して検査することもできます。
- 自動除外—動作とパフォーマンスを円滑にするために、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。
- Log Collector—ESET File Security for Microsoft Windows Server の構成と様々なログなどの情報を自動的に収集します。また、ESET が問題を迅速に解決するために必要な診断情報を簡単に収集できます。
- eShell（コマンドラインインターフェース）—経験豊富なユーザーと管理者向けに、ESET 製品を管理するための総合的なオプションを提供するコマンドラインインターフェースです。
- 自己防衛機能—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する技術です。
- 効果的なトラブルシューティング—システムを診断する ESET SysInspector と、ブート可能なレスキュー CD または USB を作成する ESET SysRescue Live という高性能なツールを使用して、様々な問題を解決します。

ESET File Security for Microsoft Windows Server では、スタンドアローンとクラスター環境の Microsoft Windows Server 2003、2008、2012 をサポートしています。

■新機能

ESET File Security for Microsoft Windows Server には、次の新機能が統合されています。

- クラスタリングのサポート
- 除外プロセス（サードパーティのソフトウェアとの互換性向上）
- グラフィカルユーザーインターフェース（GUI）の機能強化
- ルールベースのフィルタリング検査（ファイルルールの定義とオンデマンド検査の指定フォームの実行を実現）
- フィッシング対策保護
- 仮想環境の最適化
- Hyper-V 検査 - Microsoft Hyper-V Server 上の仮想マシン (VM) ディスクを検査できます。特定の VM にエージェントをインストールする必要はありません。

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 製品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。
http://canon-its.jp/product/eset/license/eep_adv/spec.html#spec6

! 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「ウイルス対策」、「アップデート」、「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、「Web とメール」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、「Web とメール」モジュールと競合する場合があります。 上記 OS では、「Web とメール」機能を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。

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 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。

2.2 標準インストール

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。

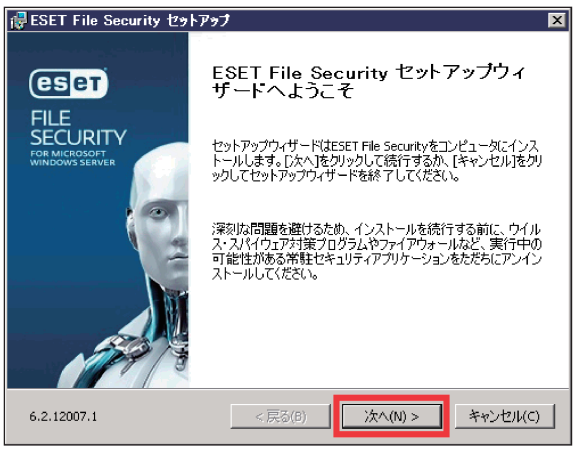
! 重 要

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

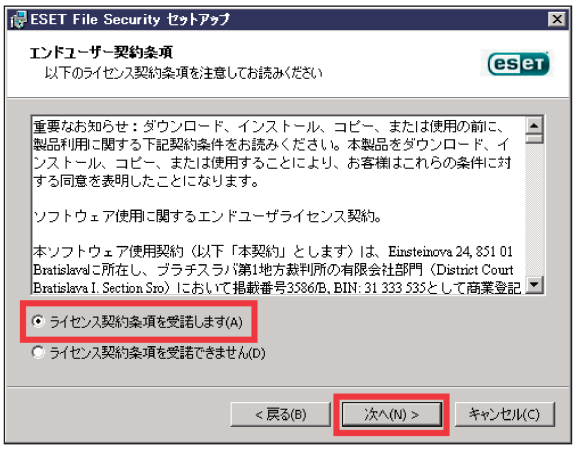
1 ダウンロードしたインストーラーを起動します。

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。

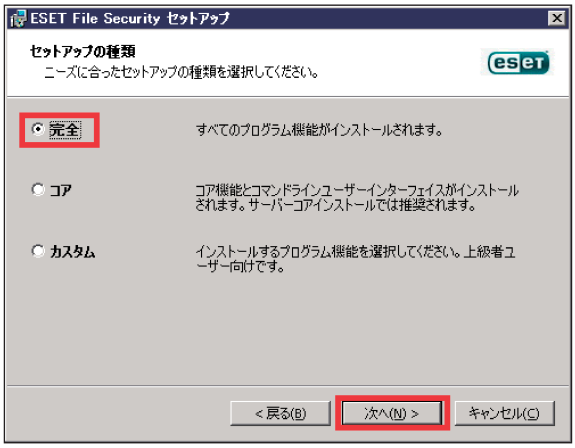


続く

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。



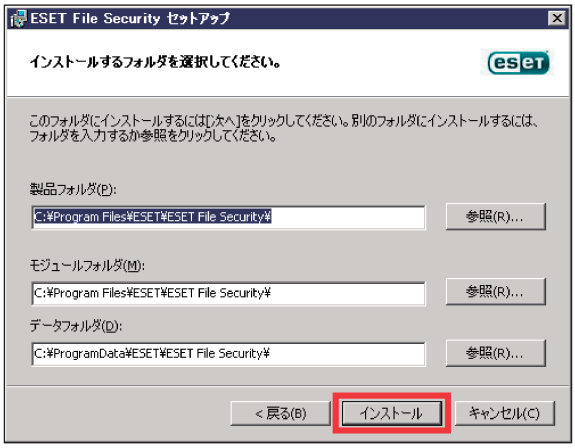
インストールするプログラムを選択したい場合は、［カスタム］をチェックして［次へ］ボタンをクリックします。手順は「2.3 カスタムインストール」へ進みます。

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 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

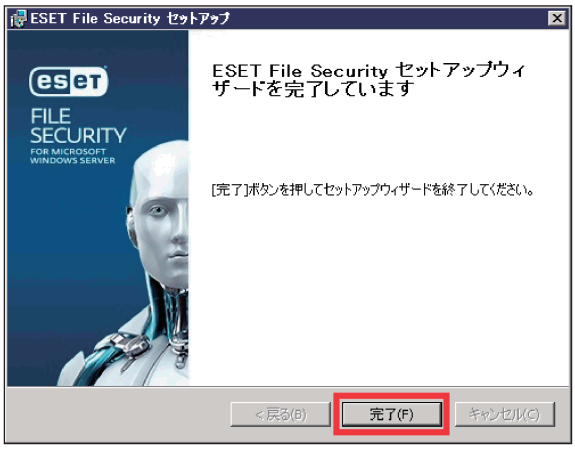
5 ［インストール］ボタンをクリックします。



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。

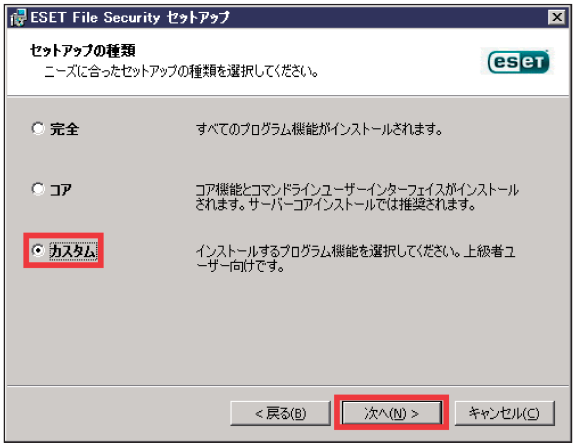
2.3 カスタムインストール

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 標準インストール」手順③の続き

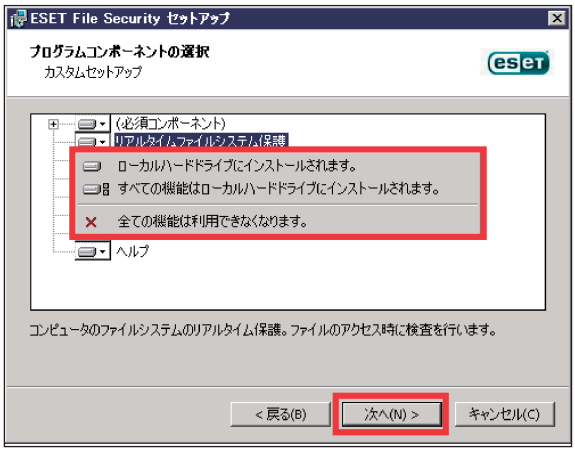
1 ［カスタム］をチェックして［次へ］ボタンをクリックします。



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。

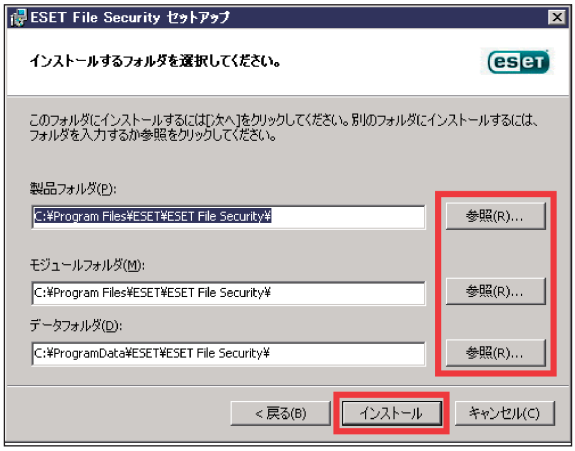
ローカルハードドライブにインストールされます。	既定で選択されています。
すべての機能はローカルハードドライブにインストールされます。	選択済みのツリーの下にすべての機能がインストールされます。
全ての機能は利用できなくなります。	機能やコンポーネントを使用できなくなります。



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。

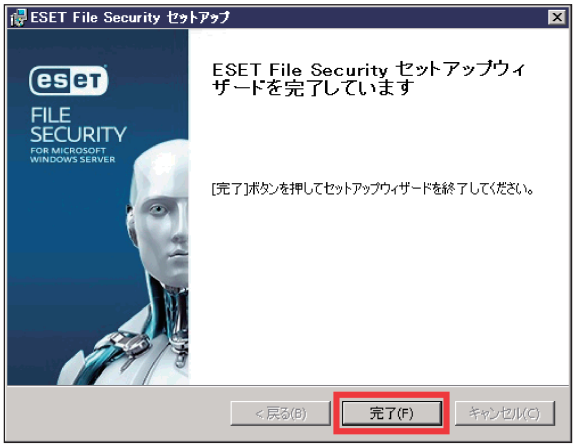
変更しない場合は、［インストール］ボタンをクリックします。



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。

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。
- セキュリティ管理者：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。

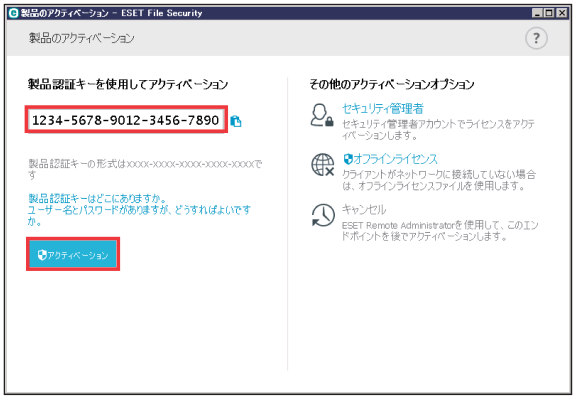
! 重 要

製品をアクティベーションすると、ウイルス定義データベース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

操作手順

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 と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。



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。

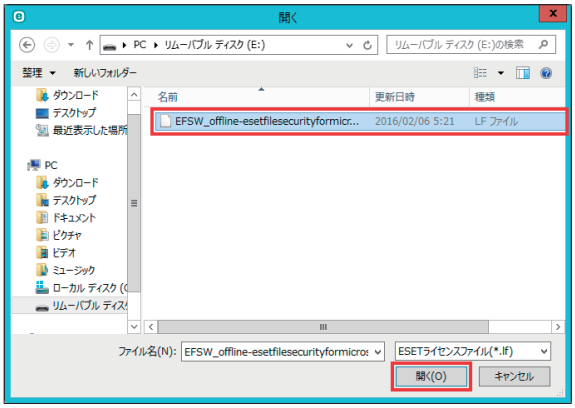
操作手順

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。

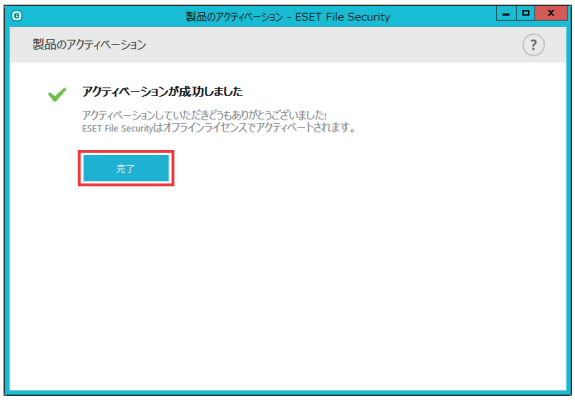
4. ［オフラインライセンス］をクリックします。

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 コンピューター」を参照してください。
また、Windows Update やウイルス定義データベース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、「5.1.18　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

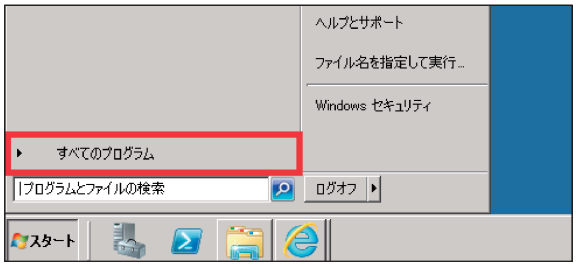
最新バージョンのインストーラーをダウンロードして、インストーラーを実行します。詳細な手順については、「2.1 インストール手順」を参照してください。

2.7 アンインストール

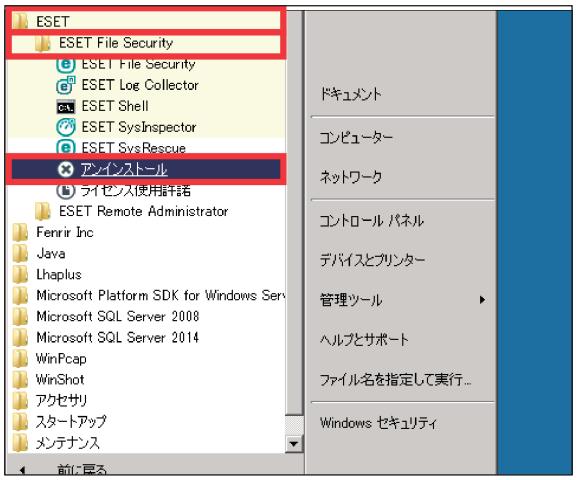
ESET File Security for Microsoft Windows Server のアンインストール方法を説明します。

操作手順

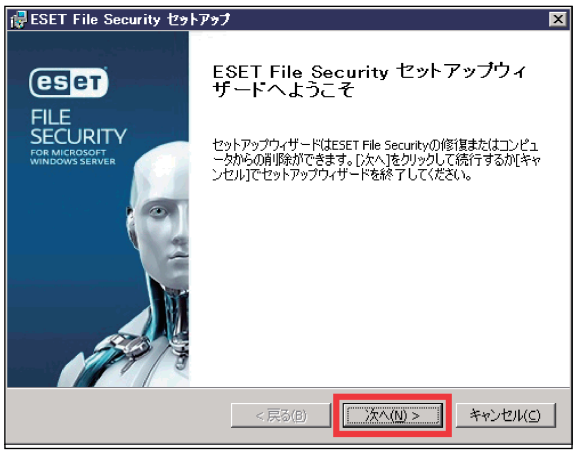
1 ［スタート］ボタンをクリックし［すべてのプログラム］を選択します。



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



3 セットアップウィザードが起動します。［次へ］ボタンをクリックします。



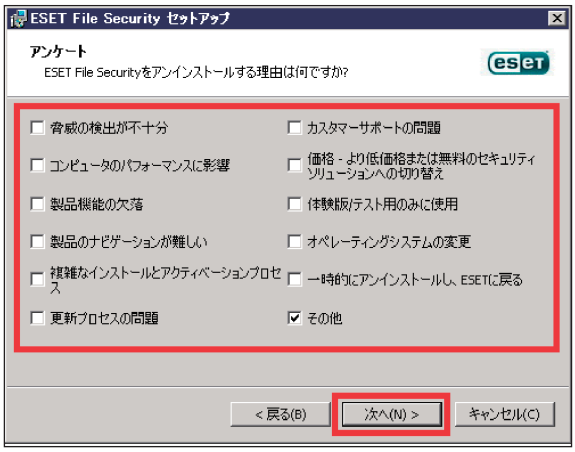
続く

4 ［削除］ボタンをクリックします。

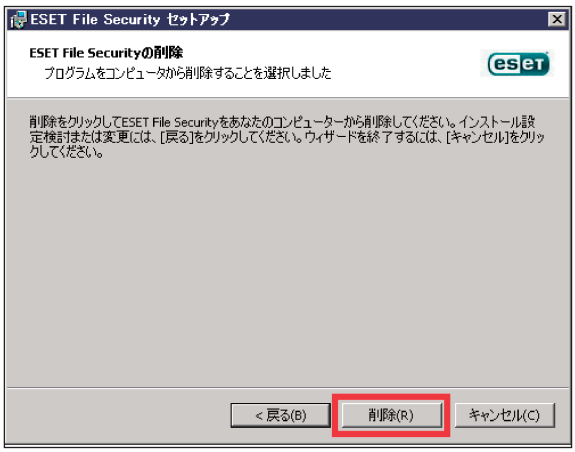
ワンポイント

［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。

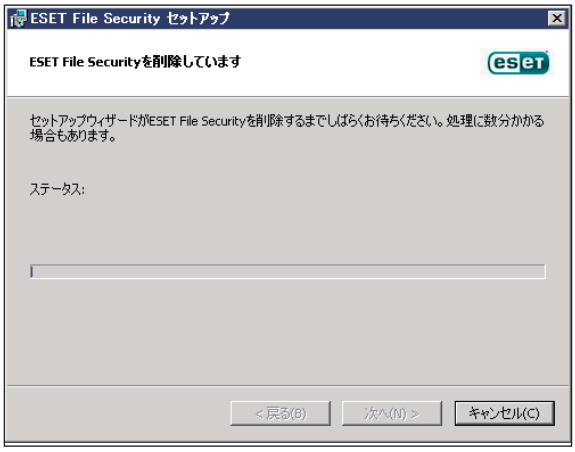


6 ［削除］ボタンをクリックします。



続く

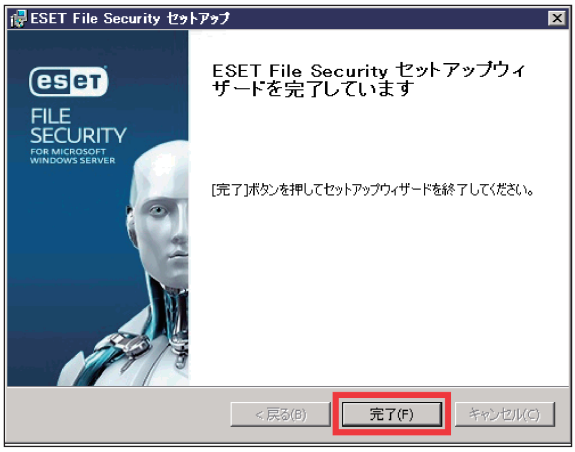
7 「削除をしています」画面が表示されます。完了までお待ちください。



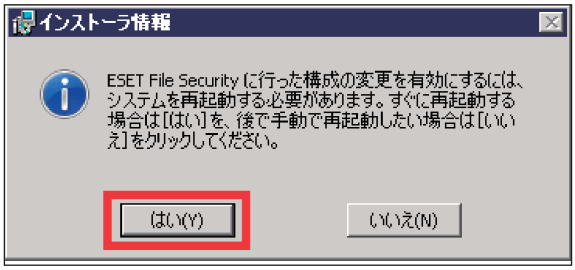
ワンポイント

「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、ウイルス定義データベース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、検出された脅威、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、スマート検査、カスタム検査、またはリムーバブルメディア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	ウイルス定義データベース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]、[ESET Log Collector]、[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
- ウイルス定義データベースが最新でない
- 製品のライセンスの有効期限が切れている

■主な解決策

ウイルス対策・スパイウェア対策による保護は無効です	「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。ウイルス対策・スパイウェア対策による保護をふたたび有効にするには、メインメニューの［設定］＞［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。
ウイルス定義データベースは最新ではありません	ウイルス定義データベースの新しいバージョンが公開されています。 最新のウイルス定義データベースにアップデートするには、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。
ライセンスの有効期限が過ぎています	ライセンスの有効期限が過ぎると、ウイルス定義データベース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

- Web アクセス保護が無効になっている
- 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（ウイルス定義データベース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

オペレーティングシステムが最新の状態ではありません	「監視」メニューのプライマリウインドウに表示されている該当メッセージを確認します。［詳細情報］をクリックすると、使用可能なアップデートのリストが表示されます。［システムアップデートの実行］をクリックしてアップデートを実行します。
Web アクセス保護は無効になっています	Web アクセス保護を再有効化するには、セキュリティ通知をクリックしてから、［Web アクセス保護を有効にする］をクリックします。
ライセンスの有効期限がまもなく切れます	ライセンスの有効期限が切れると、アップデートができなくなります。ライセンスの更新を行ってください。

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

製品ホームページの FAQ：http://eset-support.canon-its.jp/?site_domain=business

3.3 アップデートの設定

ウイルス定義データベース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、［今すぐアップデート］をクリックして、最新のウイルス定義データベースを確認します。
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。

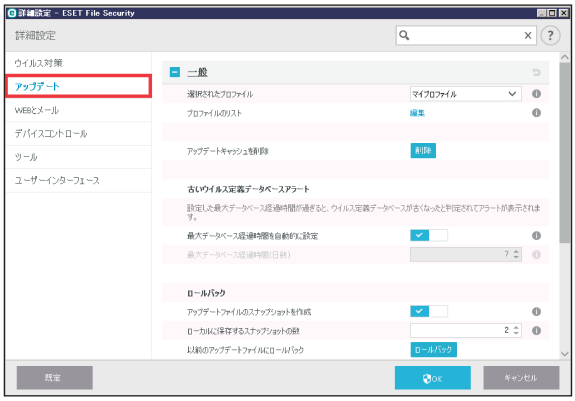
操作手順

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。



［アップデートサーバー］は、既定では［自動選択］が設定されています。
アップデートモード、HTTP プロキシ、アップデートサーバー接続アカウントの設定など、詳細なアップデートオプションを設定することができます。

ワンポイント

アップデート時に問題が発生した場合は、アップデートキャッシュを削除すると問題が解消される場合がります。［アップデートキャッシュを削除］をクリックして削除します。

!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。

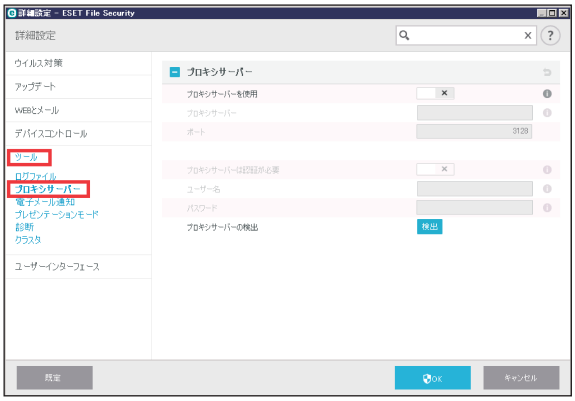
操作手順

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

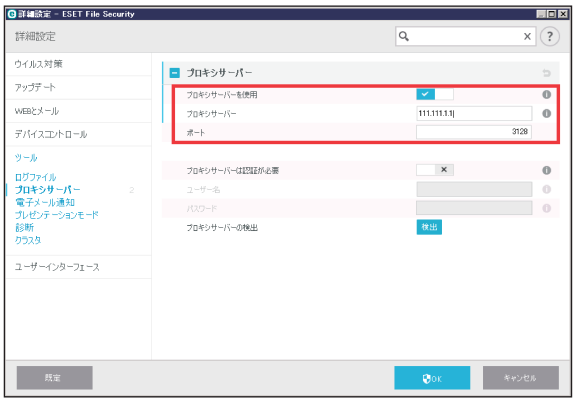
キーボードの【F5】キーを押して「詳細設定」画面を表示させることもできます。

2 ［ツール］の［プロキシサーバー］をクリックします。



続く

❸ [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。

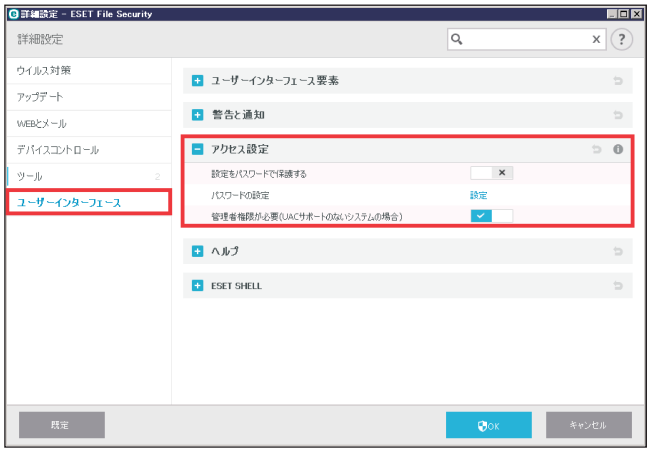
ワンポイント

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。設定パラメータをパスワードで保護するには、メインメニューの［設定］をクリックして［詳細設定］をクリックするか、キーボードの【F5】キーを押します。［ユーザーインターフェース］の［アクセス設定］をクリックし、［設定をパスワードで保護する］オプションを選択します。

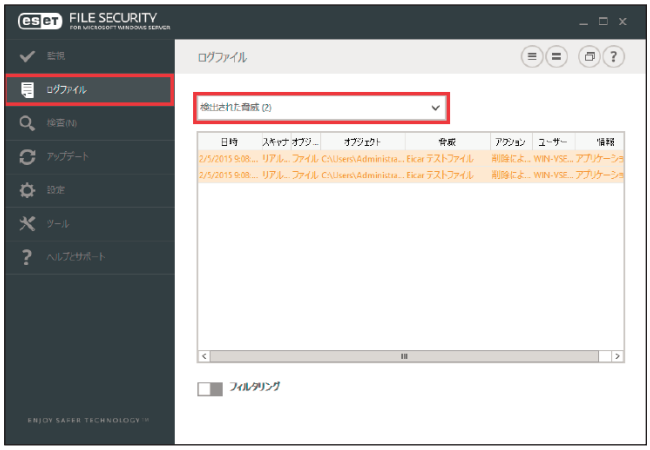
［新しいパスワード］フィールドおよび［新しいパスワードの確認］フィールドにパスワードを入力し、［OK］をクリックします。このパスワードは、ESET File Security for Microsoft Windows Server の設定を変更する場合に必ず必要になります。



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。情報は「ログに記録する最低レベル」で設定されているログレベルに基づいて記録されます。ログに記録された情報は、ESET 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。

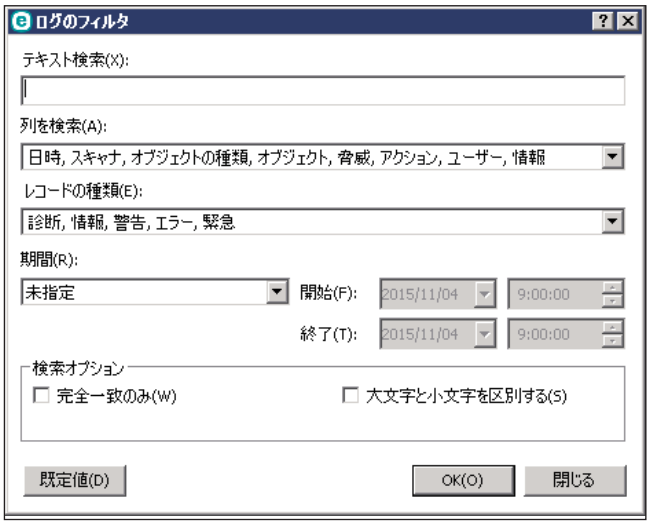


ログファイルを表示するには、「ログファイル」画面のドロップダウンメニューから目的のログタイプを選択します。

使用可能なログタイプは次のとおりです。

検出された脅威	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。
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。
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。

「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表示	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。
フィルタを無効にする	「ログのフィルタ」画面の設定を無効にします。
フィルタをクリア	「ログのフィルタ」画面の設定をクリアします。
コピー／すべてコピー	選択したログまたはすべてのログ情報をクリップボードにコピーします。
削除／すべて削除	選択したログまたはすべてのログを削除します。ログを削除するには、管理者権限が必要です。
エクスポート／すべてエクスポート	選択したログまたはすべてのログを XML 形式のファイルにエクスポートします。
検索	「ログを検索」画面が表示され、ログを検索できます。
次を検索／前を検索	前後のログを選択します。
ログのスクロール	チェックすると、新しいログが追加されたときに自動的にスクロールして、最新のログが表示されるようになります。

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、ウイルス定義データベースが古い場合、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	P35 参照
スマート検査	P35 参照
カスタム検査	P35 参照
リムーバブルメディア検査	P36 参照
前回の検査を再実行	P36 参照
Hyper-V 検査	P37 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。

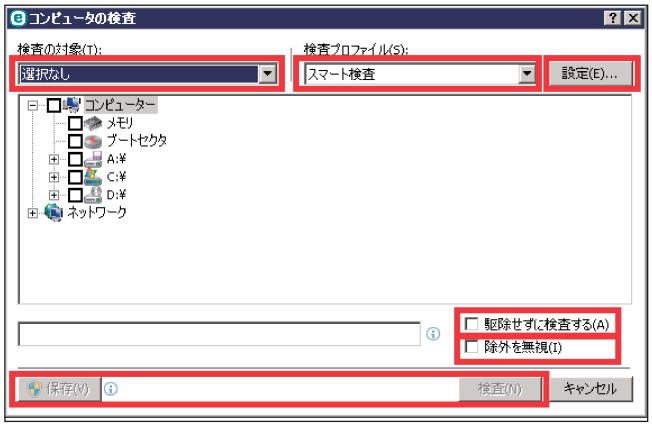
■スマート検査

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　リアルタイム検査」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、［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、［駆除せずに検査する］をチェックします。検査を実行する際には、［設定］＞［THREATSENSE パラメータ］をクリックし、「駆除」

で 3 つの駆除レベルを選択できます。
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、［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。

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

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。

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、数秒から 1 分程かかる場合があります。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、「4.5.9　スケジューラ」を参照してください。

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。

4.3 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 はウイルス定義データベース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という 2 つの方法で、常に最新の状態を保つことができます。
「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、ウイルス定義データベースのバージョンも表示されます。ウイルス定義データベースのバージョンは、ESET 製品の Web サイトへのリンクになっており、クリックするとアップデートで追加されたすべてのウイルス定義データベースの一覧が表示されます。
また、［今すぐアップデート］をクリックして、アップデートを手動で開始することもできます。

! 重 要

ウイルス定義データベース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、アップデート時に［製品のアクティベート］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。

!重 要

アップデートファイルが正常にダウンロードされると、「アップデート」画面に「アップデートは不要です－ウイルス定義データベースは最新です。」というメッセージが表示されます。表示されない場合は、プログラムが古くなっています。ウイルス定義データベースはできるだけ早くアップデートしてください。ダウンロード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。
「ウイルス定義データベースは最新ではありません」－このエラーは、ウイルス定義データベースをアップデートしようとして何回か失敗すると表示されます。アップデートの設定を確認してください。このエラーが起こる原因として認証データが正しく入力されていない、または接続設定が適切ではないことが考えられます。

次のエラーを確認してください。

- 「無効なライセンス」－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ません。認証データを確認してください。「詳細設定」画面にはその他のアップデートオプションがあります。メインメニューの［ヘルプとサポート］＞［ライセンスを管理］をクリックして、正しい製品認証キーを入力します。
- 「アップデートファイルのダウンロード中にエラーが発生しました」－このエラーはインターネット接続の設定が正しくないことが原因の場合があります。インターネット接続を確認してください。インターネット接続が確立されていないか、コンピューターの接続に問題がある可能性があります。インターネット接続について確認してください。

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 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、「5.1.9 アップデート」の「■ HTTP プロキシ」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 3 つのタブで構成されています。

- サーバー
- コンピューター
- ツール

各タブをクリックすると、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。

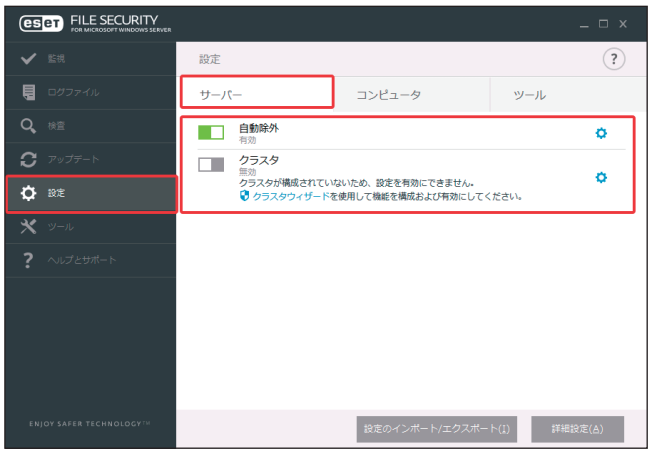
 をクリックして無効にした保護機能の多くは、コンピューターを再起動すると再度有効になります。特定の機能の詳細設定を行うには、機能名の右側にある⚙をクリックします。

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	ESET Cluster 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。ESET Cluster を設定する方法の詳細については、「5.1.17　クラスタ」の「●クラスタウィザード」を参照してください。

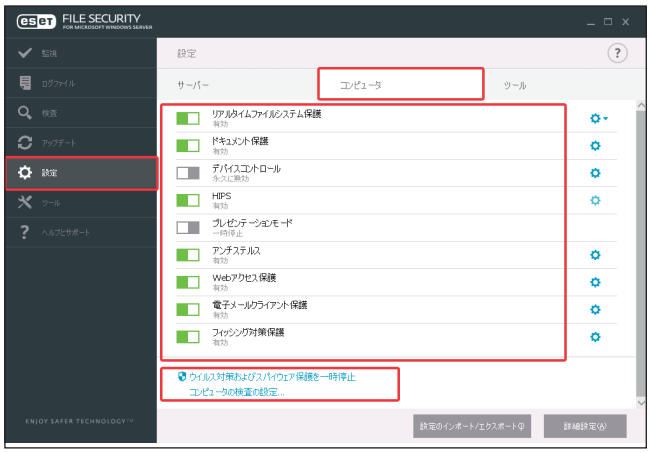
「設定」画面の下部には次のオプションがあります。

4.4.2 コンピューター

コンピューターの保護などに関する設定をします。

メインメニューの［設定］＞［コンピュータ］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。

「コンピュータ」画面では、次の機能を有効／無効を選択して設定します。



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。
ドキュメント保護	Microsoft Office ドキュメントを開く前の検査、および Internet Explorer により自動的にダウンロードされたファイル（Microsoft ActiveX 要素など）の検査を行います。
デバイスコントロール	拡張フィルター / 権限を検査、ブロック、または調整して、ユーザーからの指定デバイスへのアクセス方法やその作業方法を定義できます。
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動作します。
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、ポップアップウイ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を通知する警告画面が表示され、メイン画面がオレンジ色に変わります。
アンチステルス	ルートキットは、自己をオペレーティングシステムから見えなくすることができるため、通常のテスト技術を使用して検出することはできません。アンチステルス機能を使用すると、ルートキットなどの危険なプログラムを検出できます。
Web アクセス保護	HTTP または HTTPS 経由のトラフィックを検査して、悪意のあるソフトウェアを検出します。
電子メールクライアント保護	POP3 と IMAP プロトコルで受信した電子メールを監視します。
フィッシング対策保護	非合法の Web サイトが合法的なサイトに偽装し、パスワードや金融データ、その他の機密データの取得を試みるフィッシングから保護します。

! 重　要

ドキュメント保護は既定では無効になっています。必要な場合は、スイッチ をクリックして有効にしてください。

ウイルス対策およびスパイウェア保護を一時停止

操作手順

1. 「設定」画面下部の［ウイルス対策およびスパイウェア保護を一時停止］をクリックし、ドロップダウンメニューから無効にする時間を選択します。

2. ［適用］をクリックします。

   ウイルス・スパイウェア対策保護が一時的に無効になります。
   保護を再度有効にするには、［ウイルス・スパイウェア対策を有効にする］をクリックします。

「設定」画面の下部には次のオプションがあります。

- ［詳細設定］をクリックするか、【F5】キーを押して、詳細設定のオプションを設定します。
- ［設定のインポート／エクスポート］をクリックして、XML 設定ファイルを使用した設定パラメーターを読み込んだり、現在の設定パラメーターを設定ファイルに保存します。詳細については、「5.2.4　設定のインポート／エクスポート」を参照してください。

4.4.3　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、「5.1.12　ログファイル」の「■診断ロギング」を参照してください。

4.5 ツール

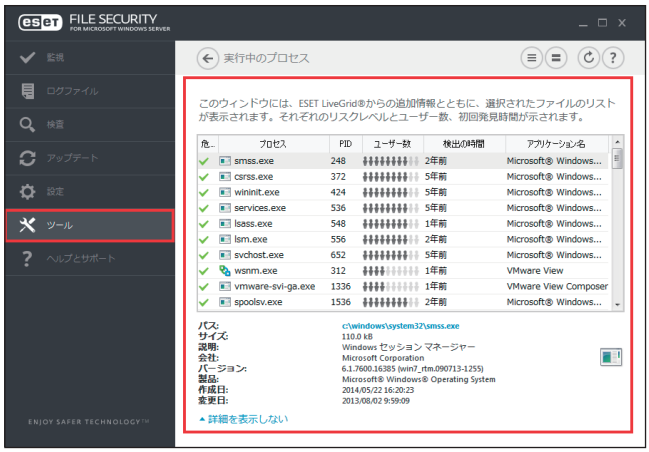
ツールには、ESET File Security for Microsoft Windows Server を管理するための機能や上級ユーザー向けのオプション機能などが用意されています。
「ツール」画面を表示するには、メインメニューの［ツール］をクリックします。

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。	P46 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。	P47 参照
ESET Log Collector	システムおよび ESET 製品のログを収集します。	P48 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。	P49 参照
クラスタ	クラスタ機能の状態が表示されます。	P50 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。	P50 参照
ESET SysInspector	システムの詳細情報を収集します。	P61 参照
ESET SysRescue Live	マルウェアの駆除ツールです。	P78 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。	P79 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。	P86 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。	P88 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 Live Grid 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。

危険レベル	ESET File Security for Microsoft Windows Server および ESET Live Grid 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 Live Grid 技術によって収集されます。
検出の時間	ESET Live Grid 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。

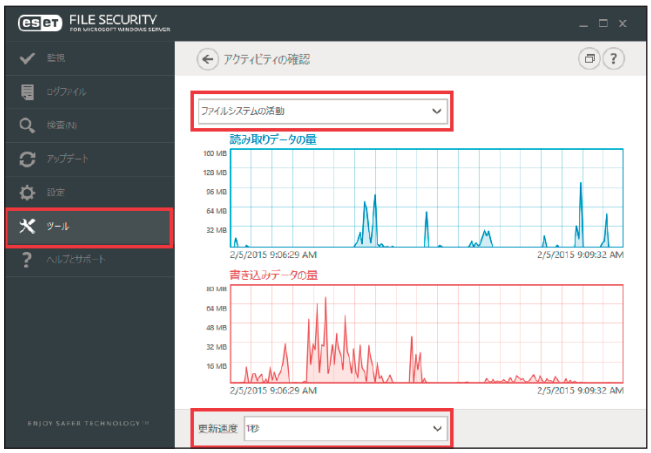
ワンポイント
ファイル評価は、実行中のプログラムまたはプロセス以外のファイルに対してもチェックできます。チェックするファイルを選択して右クリックし、コンテキストメニューから［詳細設定オプション］＞［ファイル評価のチェック］を選択します。

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。

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。



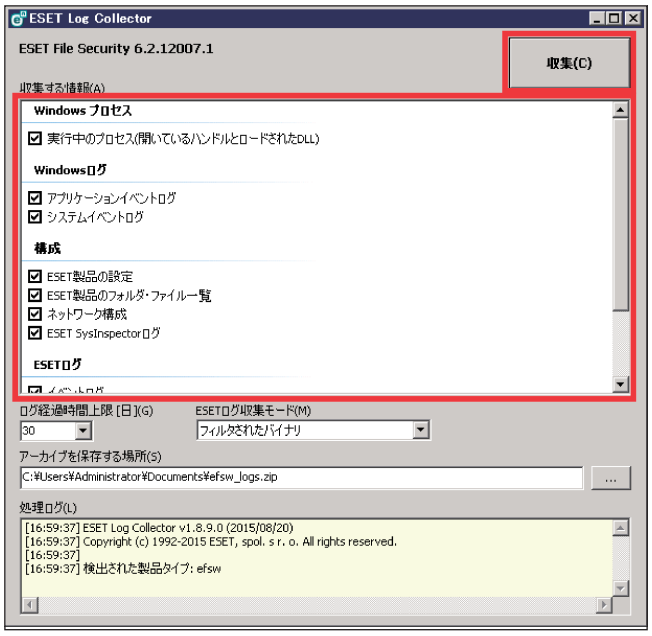
グラフは読み取りデータ量（青）と書き込みデータ量（赤）の 2 種類が表示されます。グラフの縦軸はデータ量を表しており、データ量に応じて KB（キロバイト）／MB（メガバイト）／GB（ギガバイト）で表示されます。グラフの横軸は期間を示しており、設定された更新間隔でリアルタイムに表示されます。
時間間隔を変更するには、［更新速度］ドロップダウンメニューから選択します。選択できる更新間隔は次のとおりです。

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 ESET Log Collector

ESET Log Collector は、構成やログなどの情報を、サーバーから自動的に収集します。カスタマーサポートでは、ログの提供をお願いする場合があります。ESET Log Collector を使用すると、必要な情報を簡単に収集できます。
ESET Log Collector を表示するには、メインメニューの［ツール］＞［ESET Log Collector］をクリックします。



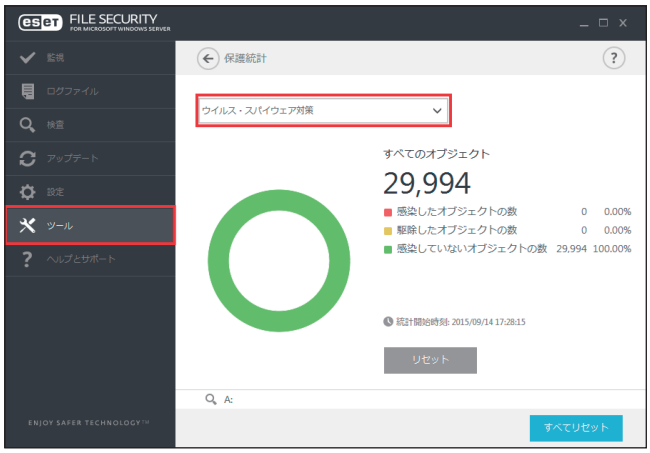
収集するログをチェックボックスで選択します。既定では、すべてのログが選択されています。ログの保存場所を指定して［保存］をクリックします。ログファイル名は自動的に設定されます。［収集］をクリックすると、ログの収集が開始されます。

ログ収集中は、画面下部の「処理ログ」ウインドウで進行中の処理を確認することができます。終了するとログファイル名（emsx_logs.zip など）一覧が表示され、正常にログファイルが保存されたことを示します。

4.5.4 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。

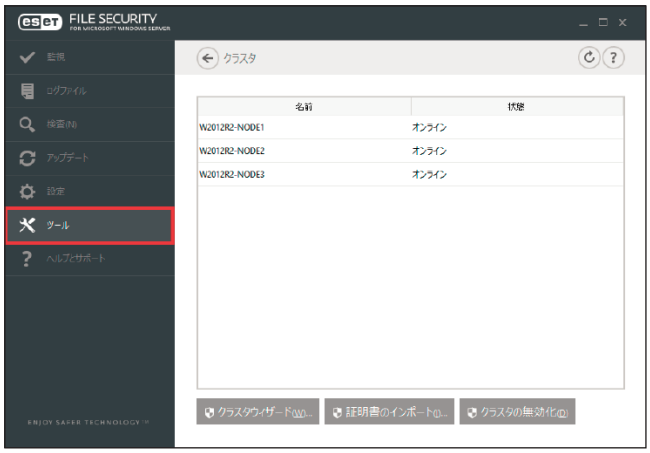
表示可能な統計グラフは次のとおりです。

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 アクセスおよびフィッシング対策	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。

4.5.5 クラスタ

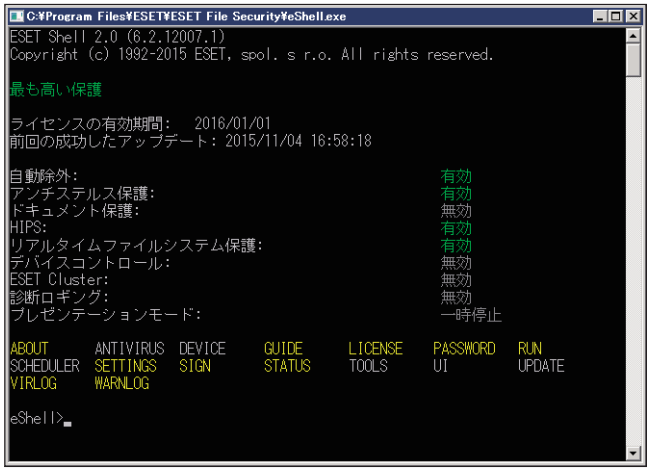
クラスタ（ESET Cluster）を活用すると、ESET サーバー製品が相互に通信し、構成や通知などのデータを交換できます。また、製品インスタンスのグループが正しく動作するために必要なデータを同期することもできます。
「クラスタ」画面を表示するには、メインメニューの［ツール］＞［クラスタ］をクリックします。



クラスタの詳細については、「5.1.17 クラスタ」を参照してください。

4.5.6 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

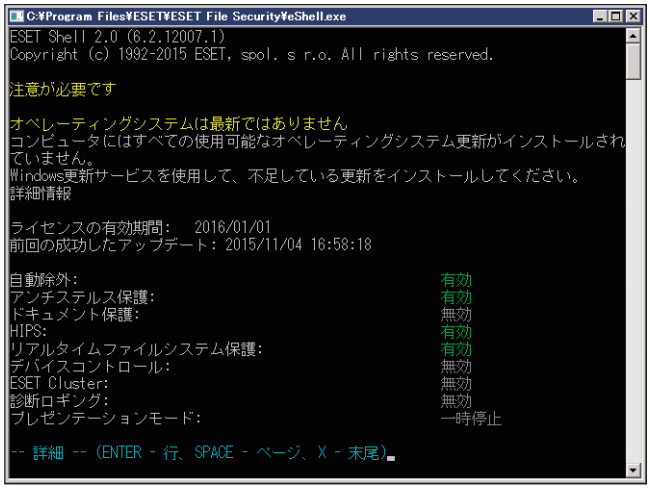
対話モードは、次の 2 つの方法を使用して開始できます。

- 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

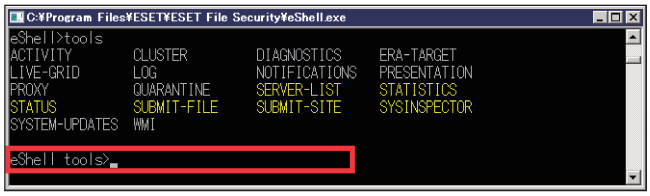
プレフィックス GET と SET は多くのコマンドでサポートされますが、EXIT などプレフィックスを使用しないコマンドもあります。

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。

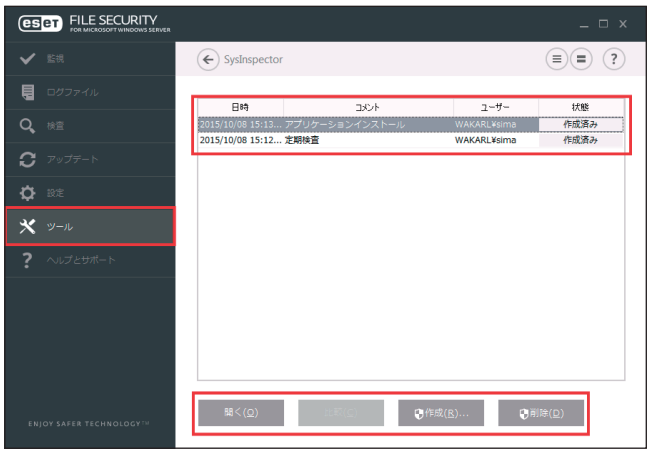
Windows コマンドプロンプトから署名されたバッチファイルを実行するか、スケジュールタスクとして実行するには、次のコマンドを使用します。

```
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`

4.5.7 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。

開く	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。

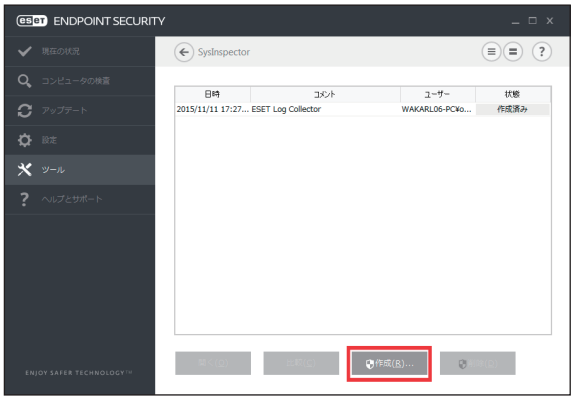
STEP1	ESET File Security for Microsoft Windows Server の「詳細設定」で「ESET SysInspector] を起動します。
STEP2	ESET SysInspector で、その時点のコンピューターの状態のスナップショットを作成します。
STEP3	スナップショットを開くと SysInspector アプリケーションが起動して分析結果が表示されます。この画面でコンピューターの状態を確認します。

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。

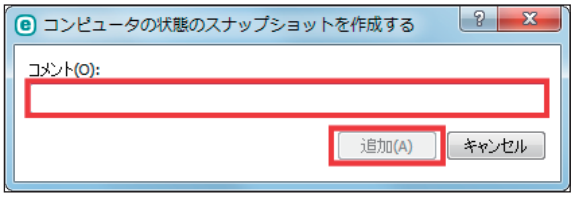
操作手順

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

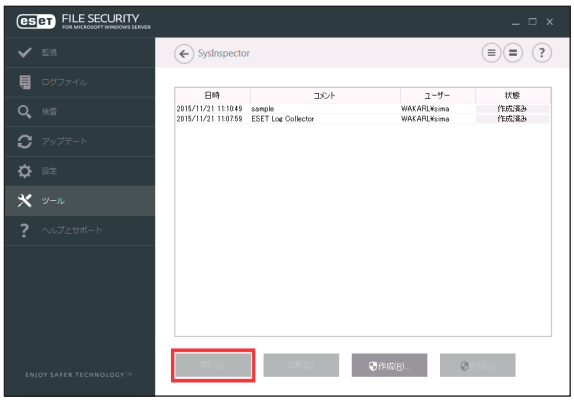


2. 作成するスナップショットについてのコメントを入力して［追加］をクリックします。

※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［開く］をクリックします。

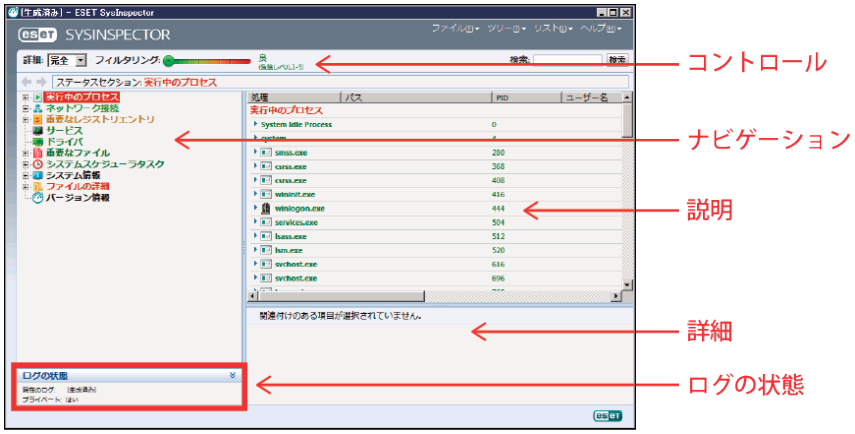


続く

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、［送信用］でログを生成することをお勧めします。このログでは、機密情報（ユーザー名、コンピューター名、ドメイン名、現在のユーザー特権、環境変数など）は含まれません。 **ワンポイント** 以前に保存したログは、メイン画面にドラッグアンドドロップするだけで開くことができます。
ツリー	すべてのノードをツリー上で展開したり閉じたりできます。また、選択したセクションをサービススクリプトにエクスポートすることもできます。
リスト	プログラム内でのナビゲーションをより容易にするための機能のほか、オンラインでの情報検索などの他の様々な機能が含まれます。
ヘルプ	ESET SysInspector とその機能に関する情報を確認できます。

詳細	メイン画面に表示される情報を基本、中、完全から選択できます。 「基本」モードは、システムの一般的な問題に対する解決策を探すための情報が表示されます。 「中」モードは、一般的ではない詳細な情報が表示されます。 「完全」モードでは、特殊な問題の解決に必要なすべての情報が表示されます。
フィルタリング	システム内の疑わしいファイルまたはレジストリーエントリーを見つけるために、危険度に応じて情報を絞り込むことができます。スライダーを動かすと、危険レベルごとに項目をフィルターできます。スライダーを左端（危険レベル 1）に設定すると、すべての項目が表示されます。スライダーを右に動かすと、表示されているレベルより不審な項目のみが表示されます。スライダーを右端（危険レベル 9）まで移動すると、既知の有害な項目のみが表示されます。危険レベル 6 ～ 9 の項目は、すべてセキュリティリスクが生じる可能性があります。 **ワンポイント** 項目の危険レベルは、項目の色と危険レベルのスライダーの色を比較すると簡単に判別できます。
検索	特定のアイテムを名前または名前の一部によって検索します。検索結果は、説明ウインドウに表示されます。
⬅/➡	左矢印または右矢印をクリックすることで、説明ウインドウ内に表示される情報を切り替えることができます。【BackSpace】キーと【スペース】キーを押しても戻ることができます。
ステータスセクション	ナビゲーションウインドウ内の現在のノードを表示します。 **！重　要** 赤色で表示されている項目は、SysInspector によって潜在的な危険性があると判定された不明な項目です。ただし、赤色で表示されていても削除してよい項目というわけではありません。削除する前に、ファイルが本当に危険かどうか、不要かどうかを確認してください。

●ナビゲーションエリアの使い方

ESET SysInspector では、情報が、ノードと呼ばれる複数の基本セクションに分けてナビゲーションエリアに表示されます。サブノードがある場合は、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

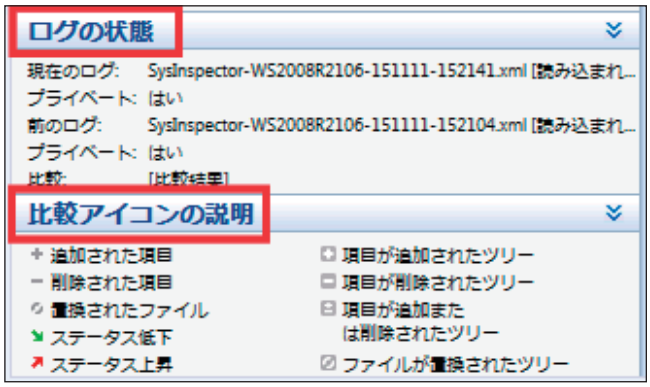
現在表示されているログと、保存されたログを比較します。［ファイル］＞［ログの比較］＞［ファイルの選択］をクリックし、比較するログを選択します。比較が実行され、2 つのログで異なる項目のみが画面に表示されます。

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「'」（アポストロフィー）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？

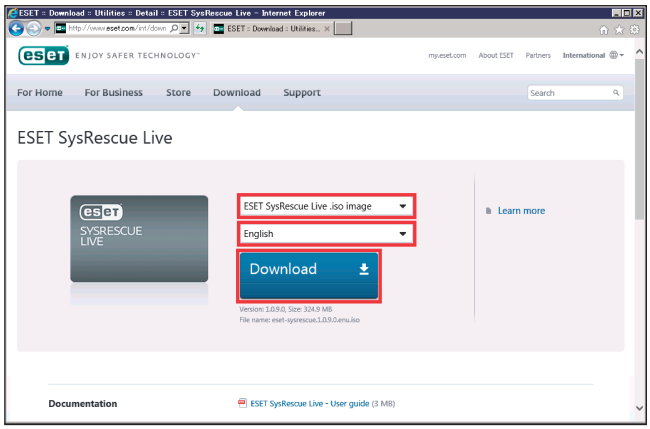
実行可能ファイルのデジタル署名を識別するときにファイルに埋め込まれたデジタル署名をチェックします。デジタル署名が検出されると、その情報を使ってファイルを検証します。デジタル署名が見つからない場合、ESET SysInspector は処理する実行可能ファイルに関する情報を収めた CAT ファイル（セキュリティカタログ - % systemroot%\system32\catroot）の検索を開始します。該当する CAT ファイルが見つかると、CAT ファイルのデジタル署名を使って検証します。「Signed by MS」というマークのあるファイルが、異なる「CompanyName」エントリーを持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

4.5.8 ESET SysRescue Live

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

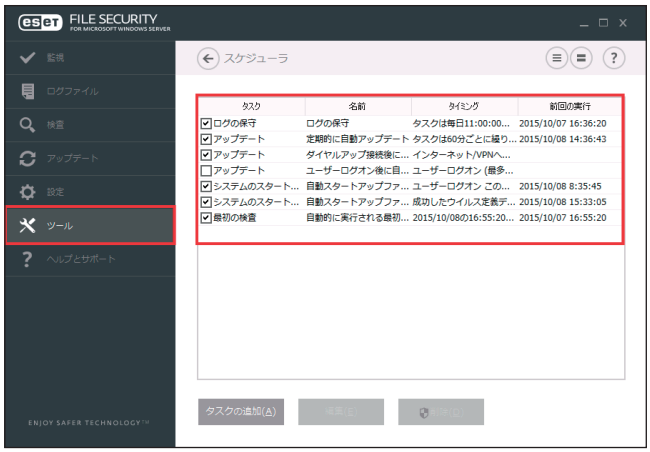
メインメニューの［ツール］＞［ESET SysRescue Live］を選択すると、リンク先の ESET の Web サイトが表示されます。ESET SysRescue Live の使用方法は、ユーザーズサイトで公開している「ESET SysRescue Live 手順書」を参照してください。



4.5.9 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）
- 自動起動ファイルの検査（ウイルス定義データベースの正常なアップデート後）
- 自動的に実行される最初の検査

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。

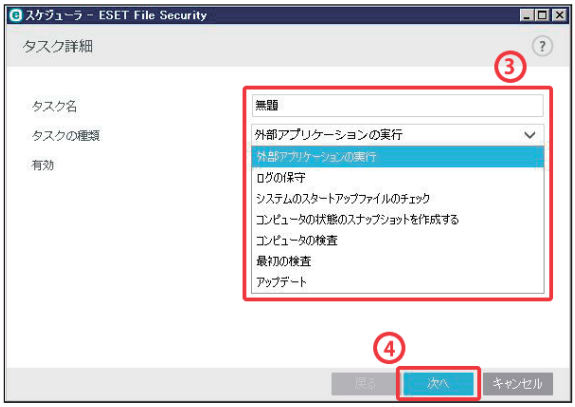
■新しいタスクの追加

次の 7 種類のタスクを追加することができます。

外部アプリケーションの実行	外部アプリケーションを実行します。
ログの保守	ログファイルには削除されたデータの痕跡も収められています。「ログの保守」タスクはシステムを効率的に運用するために、ログファイル内のデータを定期的に最適化します。
システムスタートアップファイルのチェック	システムの起動時またはログイン時に実行されるファイルを検査します。
コンピューターの状態のスナップショットを作成する	ドライバーやアプリケーションなど、システムコンポーネントの情報を収集し、各コンポーネントの危険レベルを評価するための ESET SysInspector コンピュータースナップショットを作成します。
コンピュータの検査	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。
最初の検査	プログラムのインストール後またはクライアントコンピューターの再起動後、指定した時間が経過すると、コンピューターの検査を低優先で実行します。
アップデート	ウイルス定義データベースおよびプログラムコンポーネントをアップデートします。

操作手順

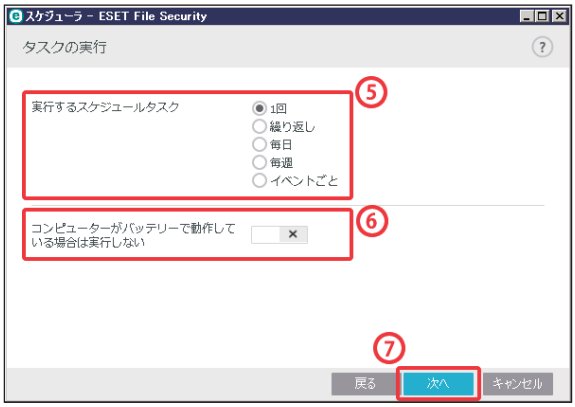
1. ［タスクの追加］をクリックします。
2. タスク名を入力します。
3. 「タスクの種類」プルダウンメニューから目的のタスクを選択します。



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 • ウイルス定義データベースのアップデートに成功 • プログラムコンポーネントのアップデートに成功 • ユーザのログオン • ウイルスの検出 詳細は「4.5.10　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

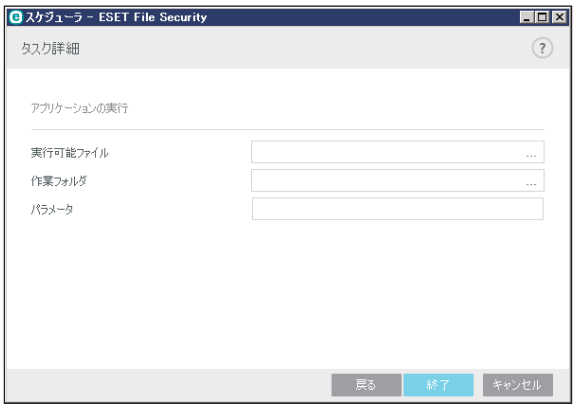
10 指定した時刻にタスクが実行されなかった場合に、タスクを再度実行するタイミングを選択します。

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「4.5.11 タスクが実行されなかった場合」を参照してください。

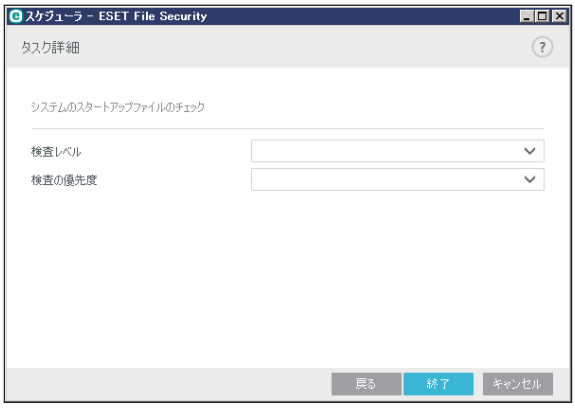
11 各項目を設定します。表示される項目は、手順 3 で選択した「タスクの種類」によってかわります。

• **[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。
	検査レベル	既定の検査レベルです。
	使用頻度が高いファイル	使用頻度が高いファイルが検査対象です。
	最も多く使用されるファイルのみ	最も多く使用されるファイルのみが検査対象です。 検査対象のファイルが最少です。
	ユーザーのログオン前に実行されるファイル	ユーザーがログオンしていない状態でアクセスできるファイルが含まれます（サービス、ブラウザヘルパーオブジェクト、Winlogon 通知、Windows スケジューラーのエントリー、既知の dll などのスタートアップにあるすべてのファイル）。
	ユーザーのログオン後に実行されるファイル	ユーザーがログオンした後にのみアクセスできる場所にあるファイル（特定のユーザーだけが実行するファイルで、通　常　は「HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run」にあるファイル）が含まれます。
検査の優先度	検査の開始時を指定します。	
	アイドル時	システムのアイドル時に実行されます。
	最低	システム負荷が可能な限り低い時に、実行されます。
	低	システム負荷が低い時に実行されます。
	通常	通常時に実行されます。

- **「アップデート」を選択した場合**

デフォルトプロファイルを使用	既定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。

ワンポイント

プロファイルを変更する場合は、［デフォルトプロファイルを使用］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。「4.5.13　アップデートプロファイル」も参照してください。

12 ［終了］をクリックします。

4.5.10 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
- ウイルス定義データベースのアップデートに成功
- プログラムコンポーネントのアップデートに成功
- ユーザのログオン
- ウイルスの検出

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

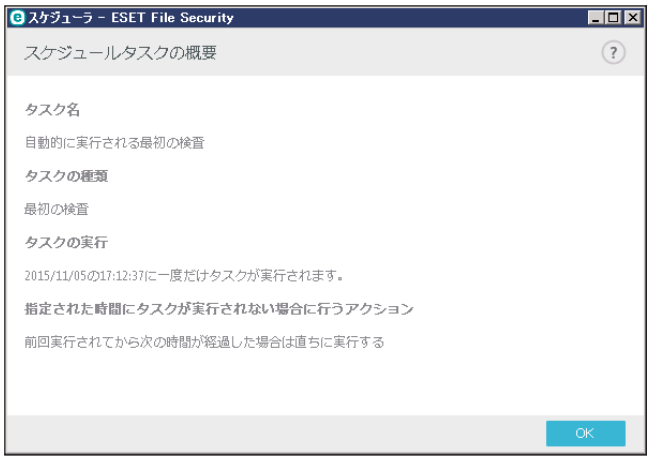
4.5.11 タスクが実行されなかった場合

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。

4.5.12 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。



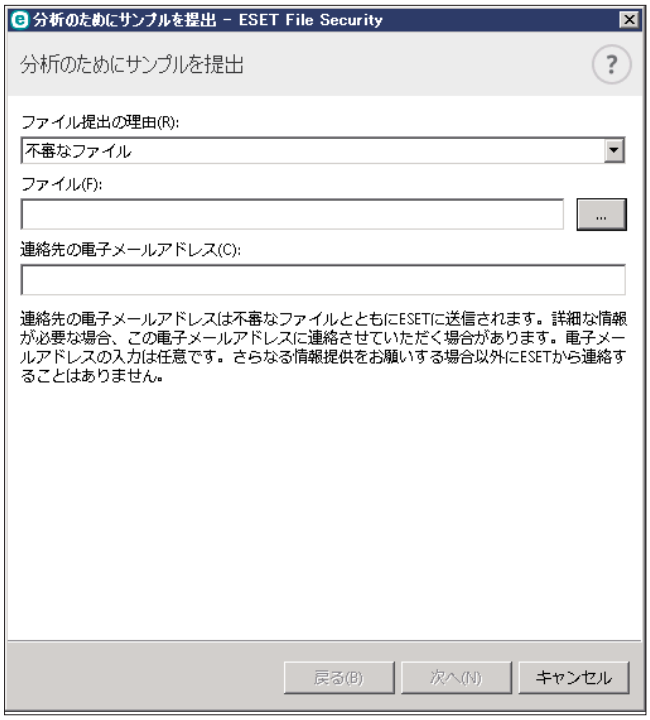
4.5.13 アップデートプロファイル

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。

アップデートプロファイルの詳細については、「5.1.9 アップデート」を参照してください。

4.5.14 分析のためにサンプルを提出

分析のためにファイルまたはサイトを ESET に送信できます。コンピューター上の動作が疑わしいファイル、または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、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。そのファイルが悪意のあるアプリケーションや Web サイトであることが判明すると、その後のアップデートファイルにその検出機能が追加されます。



!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

「ファイル／サイト」ー提出するファイルまたは Web サイトのパスを入力します。
「連絡先の電子メールアドレス」ー連絡先のメールアドレスを入力します。解析のために詳しい情報が必要な場合、このメールアドレスに連絡をする場合があります。メールアドレスの入力は任意です。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。
「ファイル提出の理由」では、次の理由を選択すると、次の画面でそれぞれに応じた状況を入力できるようになります。

不審なファイル

次の内容を入力します。

観察されたマルウェア感染の兆候および症状	コンピューター上にある不審なファイルの動作および症状の説明を入力します。
ファイルの入手元（URL アドレスまたはベンダ）	ファイルの入手元（ソース）の URL アドレス、またはベンダーと入手方法を入力します。
備考および補足情報	不審なファイルの解析処理の助けとなる追加情報または説明を入力します。

■不審なウェブサイト

「サイトの問題点」ドロップダウンメニューから次の 1 つを選択してください。

感染	ウイルスやマルウェアが含まれる Web サイトの場合に選択します。
フィッシング	銀行の口座番号や PIN コードなどの機密データを入手するためによく使用されます。
詐欺	不正または詐欺 Web サイトの場合に選択します。
その他	上記のオプションが該当しない場合に選択します。

■誤検出サイト

感染、詐欺、またはフィッシングサイトと検出されたサイトの内、実際には感染していないサイトは、ESET ウイルスラボに送信をしてください。ファイルのパターンがウイルス定義データベースのパターンと一致する場合、誤検出が発生する場合があります。ウイルス対策とフィッシング対策のエンジンの向上と他のお客さまの保護のために、そのような Web サイトは報告をしてください。

備考および補足情報	不審なファイルを処理する際に役立つ追加情報、または説明を入力します。

■誤検出ファイル

感染していると検出されたファイルの内、実際には感染していないファイルは、ウイルス対策とフィッシング対策のエンジンの向上と他のお客さまの保護のために、ESET ウイルスラボに送信をしてください。ファイルのパターンがウイルス定義データベースのパターンと一致する場合、誤検出が発生する場合があります。

アプリケーション名およびバージョン	プログラム名とバージョン（番号、エイリアスまたはコード名など）を入力します。
ファイルの入手元（URL アドレスまたはベンダ）	ファイルの入手元（ソース）と入手方法を入力します。
アプリケーションの目的	アプリケーションの概要、種類（ブラウザー、メディアプレーヤなど）やその機能などを入力します。
備考および補足情報	疑わしいファイルを処理する助けとなる追加情報または説明を入力します。

※「備考および補足情報」を除く 3 つのパラメーターは、アプリケーションが正当なものであるかどうかを識別し、悪意のあるコードと区別するために必ず入力してください。

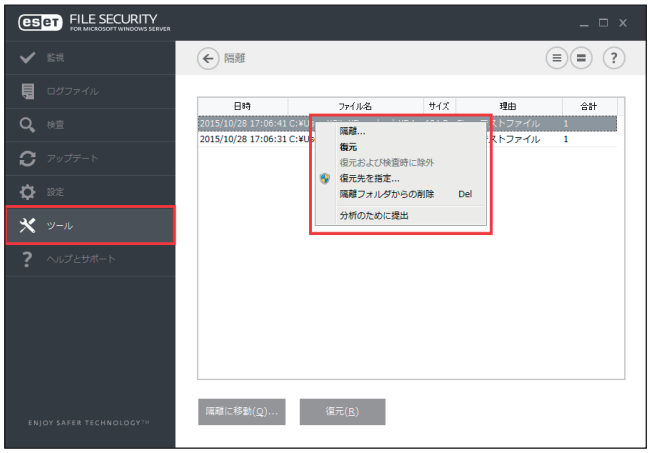
■その他

ファイルを「不審なファイル」、または「誤検出ファイル」に分類できない場合は、これを選択します。

ファイル提出の理由	ファイル送信に関する詳細な説明と送信理由を入力します。

4.5.15 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。

4.6 ヘルプとサポート

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提供されています。「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利用できます。

■ヘルプ

インターネットで調べる	ESET セキュリティ ソフトウェア シリーズのサポート情報が表示されます。FAQ（よくある質問）への回答や、様々な問題に対する一般的な解決策が登録されています。このナレッジベースは定期的にアップデートされており、様々な種類の問題を解決するための最も有効なツールです。
ヘルプを開く	ESET 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。カスタマーサポート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。

■カスタマーサポート

サポート情報トップページ	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。 ※お客さまへサポートをご提供するために、ESET File Security for Microsoft Windows Server の構成、詳細なシステム情報、実行中のプロセス（ESET SysInspector ログファイル）、およびレジストリーデータに関する情報が必要となります。このデータは、技術サポートをお客さまに提供する目的でのみ使用されます。

■サポートツール

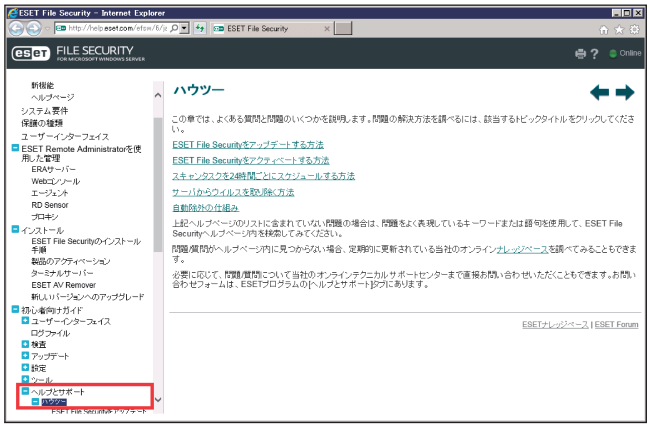
ウイルス情報	様々なタイプのマルウェアの危険と兆候に関する情報を含む、ESET の最新ウイルス情報一覧へのリンクです。
ウイルス定義データベース更新履歴	ESET ウイルスレーダーへのリンクです。ESET ウイルス定義データベースのバージョン情報が含まれています。
ESET 特殊駆除ツール	一般的なマルウェア感染を自動的に特定して駆除します。詳細については、弊社ホームページを参照してください。

■製品およびライセンス情報

ESET File Security について	ESET File Security for Microsoft Windows Server の著作権情報やバージョン情報などが表示されます。
ライセンスを管理	「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、「4.6.4　製品のアクティベーション」を参照してください。

4.6.1　ハウツー

ハウツー画面には、よくある質問が記載されています。
「ハウツー」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］＞［ヘルプ］＞［解決方法を探す］をクリックします。



問題や質問がヘルプページ内に見つからない場合は、サポートセンターにお問い合わせください。

ハウツーでは、次の項目について説明しています。

ESET File Security for Microsoft Windows Server をアップデートする方法	P92 参照
ESET File Security for Microsoft Windows Server をアクティベートする方法	P94 参照
コンピュータの検査タスクを 24 時間ごとにスケジュールする方法	P92 参照
サーバーからウイルスを取り除く方法	P92 参照
自動除外の仕組み	P99 参照

■ ESET File Security for Microsoft Windows Server をアップデートする方法

ESET File Security for Microsoft Windows Server のアップデートは、手動で実行することも自動的に実行することもできます。手動でアップデートを開始するには、ESET File Security for Microsoft Windows Server のメインメニューの［アップデート］＞［今すぐアップデート］をクリックします。

通常のインストール設定では、1 時間ごとに実行される自動アップデートタスクが作成されます。間隔を変更する場合は、スケジューラで設定します。「4.5.9　スケジューラ」を参照してください。

■コンピュータの検査タスクを 24 時間ごとにスケジュールする方法

定期的なコンピューターの検査タスクをスケジュールするには、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。タスクを 24 時間ごとにスケジュールするには、実行するスケジュールタスクを［繰り返し］、タスクの実行を［1440 分］（24 時間）に設定します。

スケジューラの詳細は、「4.5.9　スケジューラ」の内容も参照してください。

■サーバーからウイルスを取り除く方法

コンピューターが、マルウェアに感染している兆候（処理速度が遅くなる、頻繁にフリーズするなど）を示している場合、次の手順を行います。

操作手順

1. メインメニューで［検査］＞［スマート検査］をクリックしてシステムの検査を開始します。
2. スキャンが完了したら、スキャンされたファイル、感染しているファイル、および駆除されたファイルの数をログで確認します。
3. ディスクの一部のみをスキャンするには、［カスタム検査］を選択し、ウイルススキャンをする対象を選択します。

4.6.2 ESET 特殊駆除ツール

Conficker、Sirefef、Necurs などの一般的なマルウェア感染は、ESET 特殊駆除ツールで駆除できます。ESET 特殊駆除ツールを使用するには、メインメニューの［ヘルプとサポート］＞［サポートツール］＞［ESET 特殊駆除ツール］をクリックします。

4.6.3 ESET File Security for Microsoft Windows Server について

インストールされている ESET File Security for Microsoft Windows Server のバージョンと、インストールされているコンポーネント（プログラムモジュール）を確認することができます。「バージョン情報」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］＞［製品情報およびライセンス情報］＞［ESET File Security について］をクリックします。

［コピー］をクリックすると、インストールされたコンポーネントに関する情報をコピーできます。この機能は、トラブルシューティングを行う場合、またはカスタマーサポートに問い合わせる場合に便利です。

4.6.4 製品のアクティベーション

インストールが完了すると、製品のアクティベーションが要求されます。
Windows 画面からアクティベートするには、システムトレイアイコンⓔをクリックし、メニューから［製品のアクティベーション］を選択します。また、メインメニューの［ヘルプとサポート］＞［ライセンスの管理］をクリックし、「製品のアクティベーション」画面からアクティベートすることもできます。

アクティベートするには、次のいずれかの方法を使用できます。

製品認証キー	XXXX-XXXX-XXXX-XXXX-XXXX の形式の一意の文字列。ライセンス所有者を識別し、ライセンスをアクティベートするために使用されます。
オフラインライセンスファイル	ユーザーズサイトからダウンロードします。

メインメニューの［ヘルプとサポート］＞［ライセンスを管理］から、いつでもライセンス情報を管理できます。ESET が製品を識別し、ライセンスを特定するために使用されるライセンス ID が表示されます。ライセンスシステムに登録するときに使用されるユーザー名は、システムトレイアイコンⓔを右クリックすると表示される「バージョン情報」画面に表示されます。

Chapter 5 設定

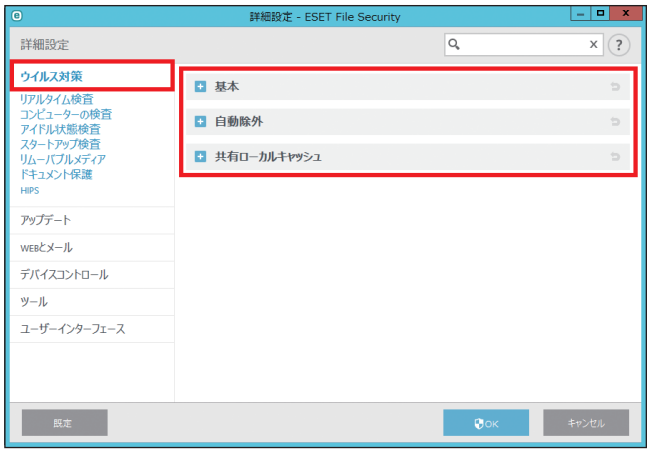
5.1 詳細設定

ウイルス対策、アップデート、WEB とメール、デバイスコントロール、ツール、ユーザーインターフェースの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 ウイルス対策

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。悪意のあるコードを含むウイルスが検出されると、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［ウイルス対策］を選択します。



■基本

スキャナオプション

次の検出を有効または無効にすることができます。この設定は、すべての保護モジュール（リアルタイムファイルシステム保護、Web アクセス保護など）に適用されます。

望ましくない可能性があるアプリケーション	必ずしも悪意があるとは限らないが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるウイルスを検出するかどうかを設定します。
安全ではない可能性があるアプリケーション	悪用される可能性がある市販のソフトウェアを検出する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例としては、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を記録するプログラム）などがあります。既定では無効に設定されています。
疑わしい可能性のあるアプリケーション	圧縮されたプログラムが含まれます。マルウェアの作成者が検知されるのを逃れるためによく使用する方法です。

※この種のアプリケーションの詳細については、「6.1.10　エクスプロイトブロック」を参照してください。

アンチステルス技術
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。

プロセスの除外
特定のプロセスを除外できます。例えば、バックアップソリューションのプロセスの場合、関連するすべてのファイル処理が安全であると見なされて除外されるため、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。

除外フィルタ
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。除外の詳細については、「5.1.2 リアルタイム検査」の「■ THREATSENSE パラメータ」を参照してください。

●侵入物が検出された場合

マルウェアがシステムに侵入する経路は、Web ページ、共有フォルダー、メール、コンピューターのリムーバブルデバイス（USB、外付けハードディスク、CD、DVD、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、次の機能を使用してマルウェアを検出して処理します。
- リアルタイムファイルシステム保護
- Web アクセス保護
- 電子メールクライアント保護
- コンピューターの検査

各機能は標準的な駆除レベルを使用し、マルウェアを検出した際にファイルを駆除して隔離するか、Web 接続の切断を試みます。通知画面は、画面の右下のタスクバーにある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 リアルタイム検査」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、オプションを選択するよう要求されます。選択できるオプションは通常、［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るため、推奨されません。ただし、そのファイルが「無害なのに誤って感染が検出された」と確信できる場合は除きます。

ウイルスの攻撃によって悪意のあるコードがファイルに添付された場合は、駆除を行います。まず、感染しているファイルからウイルスを駆除してファイルを元の状態に戻すことを試みます。ファイルが悪意のあるコードでのみ構成されている場合には、ファイル全体が削除されます。
感染しているファイルが、システムプロセスによって「ロック」または使用されている場合は、再起動後など、ファイルが開放された後に削除されます。

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った場合は（または駆除レベルが［駆除なし］に設定されていた場合）、警告画面が表示され、感染ファイルをどのように処理するかのアクションを選択するよう要求されます。アクションを選択して、［完了］をクリックします。

アーカイブファイルの削除

既定の駆除モードでは、アーカイブファイルがすべて感染ファイルである場合は、アーカイブファイル全体が削除されます。感染していない無害なファイルも含まれている場合には、アーカイブは削除されません。[厳密な駆除]のスキャンを実行する際には注意が必要です。この駆除モードでは、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、そのアーカイブファイル全体が削除されます。

使用しているクライアントコンピューターが、マルウェアに感染している気配（処理速度が遅くなる、頻繁にフリーズするなど）がある場合は、次の処置を行うことをお勧めします。

操作手順

1. メインメニューの［検査］をクリックします。
2. ［スマート検査］をクリックします（詳細については、「5.1.3　コンピューターの検査」を参照してください）。

   ワンポイント
   ディスクの特定の部分だけを検査するには、［カスタム検査］をクリックし、ウイルス検査を行う対象を選択します。

3. スキャン終了後、ログでスキャン済みファイル、感染ファイル、および駆除済みファイルの件数をそれぞれ確認します。

●プロセスの除外

この機能では、ウイルス対策のリアルタイム検査からアプリケーションのプロセスを除外できます。これらを除外することにより、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向上させます。このようにして、オペレーティングシステムの全体的なパフォーマンスを向上させます。

プロセスが除外されると、その実行ファイルは監視されません。また、除外されたプロセスのアクティビティも監視されません。プロセスによって実行されるファイル処理は、検査から除外されます。

［追加］、［編集］、［削除］ボタンを使用して、プロセス除外を管理します。

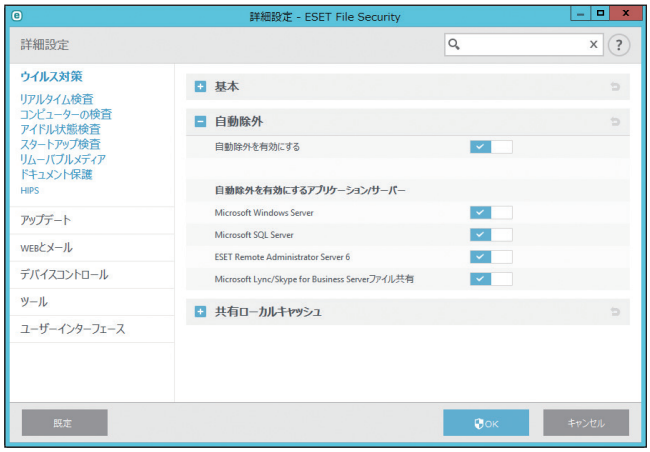
!重　要

プロセスの除外は、ウイルス対策のリアルタイム検査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。

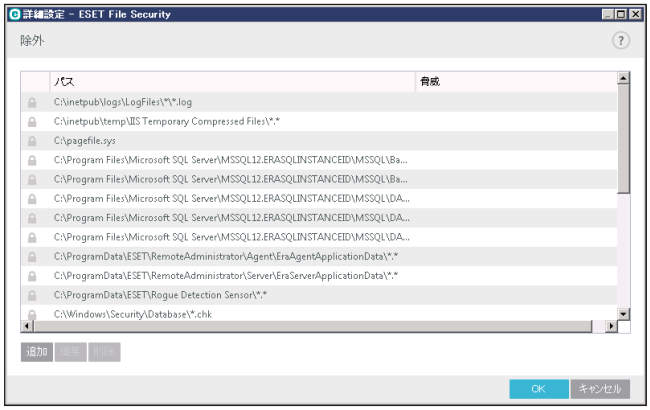
■自動除外



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］＞［ウイルス対策］＞［基本］＞［除外フィルタ］＞［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］＞［ウイルス対策］＞［基本］＞［除外フィルタ］＞［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。詳細については、次のリンクを参照してください。

- https://support.microsoft.com/ja-jp/kb/822158
  （現在サポートされているバージョンの Windows を搭載しているエンタープライズコンピューターでウイルススキャンを行う場合の推奨事項）
- https://support.microsoft.com/ja-jp/kb/245822
  （ウイルス対策ソフトウェアがインストールされている Exchange Server コンピューターのトラブルシューティングに関する推奨事項）
- https://support.microsoft.com/ja-jp/kb/823166
  （Exchange Server 2003 とウイルス対策ソフトウェアの概要）
- https://technet.microsoft.com/ja-jp/library/bb332342(v=exchg.80).aspx
  Exchange 2007 でのファイルレベルのウイルス対策スキャン
- http://technet.microsoft.com/en-us/library/bb332342.aspx
  （Exchange Server 2016 上のオペレーティングシステムのウイルス対策ソフトウェア）

■共有ローカルキャッシュ

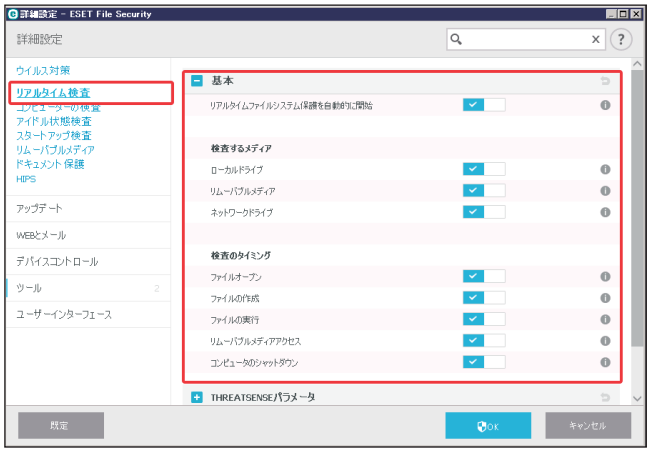
本製品では、本機能はご使用いただけません。

5.1.2 リアルタイム検査

■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［ウイルス対策］＞［リアルタイム検査］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］＞［リアルタイム検査］＞［基本］の下の［リアルタイムファイルシステム保護を自動的に開始］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。

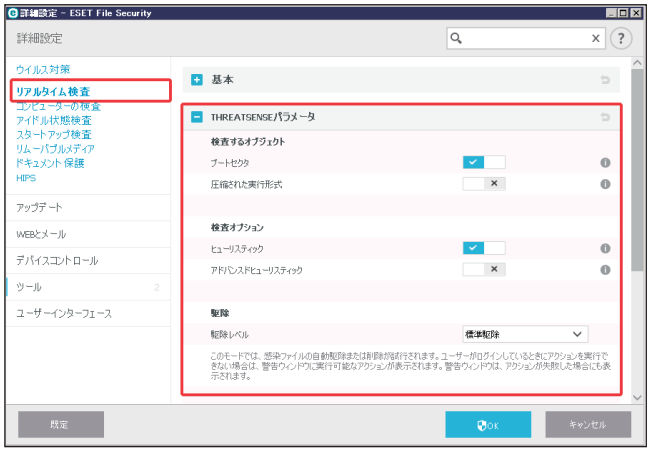
検査のタイミング

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。
コンピュータのシャットダウン	コンピューターのシャットダウン時に、ハードディスクのブートセクターを検査するかどうかを設定します。

■ 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）の検出方法なので、新しいウイルスが広がる初期の段階でシステムを保護することができます。ThreatSense は、システムのセキュリティを大幅に強化するために、コード分析、コードエミュレーション、汎用シグネチャ、ウイルスシグネチャなどを組み合わせて保護します。検査エンジンは、複数のデータストリームを同時に検査することで、最大限の効率および検出率を確保することができます。また、ThreatSense 技術によってルートキットを除去することもできます。



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

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

など

! 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	マスターブートレコードにウイルスがないか、ブートセクターを検査します。
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とおりです。

ヒューリスティック	ヒューリスティックは、悪意のあるプログラムの動きを分析するアルゴリズムです。主な利点は、以前には存在しない、またはこれまでのウイルス定義データベース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	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。

・望ましくない可能性があるアプリケーション

コンピューターのパフォーマンスに悪影響を及ぼす可能性があります。通常、このようなアプリケーションをインストールする前には同意が必要です。このようなアプリケーションをクライアントコンピューターにインストールすると、システムはそれ以前とは違う動作をします。次のような変化が表れます。

－これまでに表示されたことがない新しい画面（ポップアップや広告など）が表示される
－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

・安全ではない可能性のあるアプリケーション

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）などの市販されている、かつ合法的なプログラムが該当します。このオプションは、既定では無効になっています。

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。

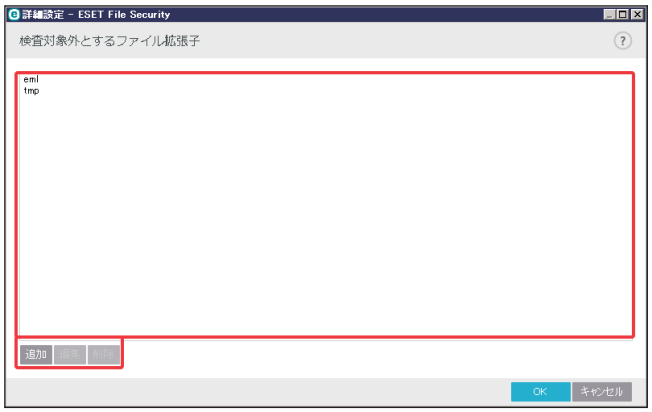
駆除なし	感染しているファイルは自動的に駆除されず、警告画面でユーザーがアクションを選択することができます。ウイルスの侵入が発生したときに実行しなければならないステップを理解している経験豊富なユーザー向けのレベルです。
標準駆除	あらかじめ定義されたアクション（マルウェアの種類によって異なります）に基づいて、感染ファイルを自動的に駆除または削除します。感染しているファイルの検出と削除は、デスクトップ右下の情報メッセージによって通知されます。適切なアクションを自動的に選択できなかった場合は、ユーザーがその後のアクションを選択することができます。あらかじめ定義されているアクションを実行できなかった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

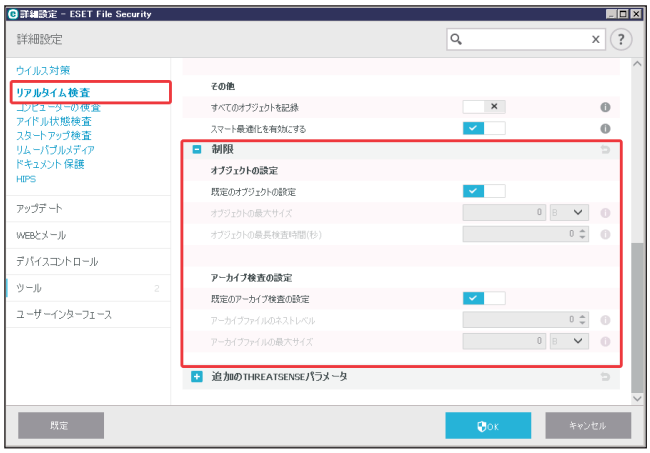
拡張子の指定では、特殊記号の「*」（アスタリスク）および「?」（疑問符）を使用できます。アスタリスクは任意の文字列を、疑問符は任意の記号をそれぞれ表します。特殊記号を使って拡張子を指定する際は、正しい形式で入力してください。

その他

すべてのオブジェクトを記録	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」～「2」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」～「2147483647」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。

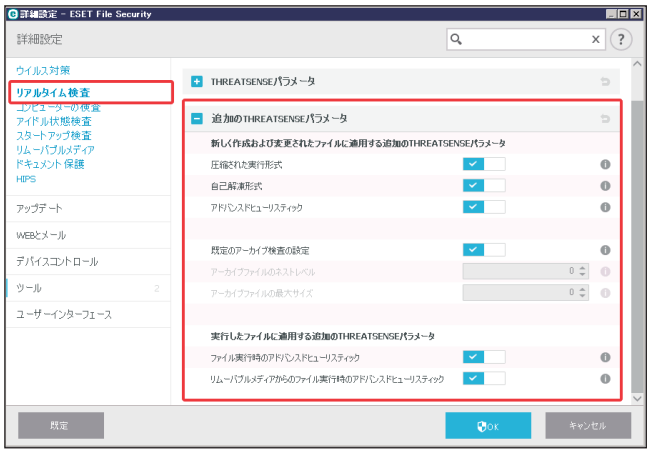
既定のアーカイブ検査の設定	このオプションを有効にすると、既定のアーカイブ検査の設定が使用されます。
スキャン対象の下限ネストレベル	アーカイブ検査のネストレベルを指定します。既定では「10」に設定されており、「0」～「20」に制限できます。
スキャン対象ファイルの最大サイズ	検査対象のアーカイブ（抽出された場合）に含まれているファイルの最大サイズを指定できます。既定では無制限に設定されており、「0」～「2」GB に制限できます。

! 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。一般的なウイルス定義ベース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、ウイルス定義データベース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。
自己解凍形式	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 Live Grid」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（http://www.eicar.org/）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、［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［リアルタイム検査］＞［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自動的に開始］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

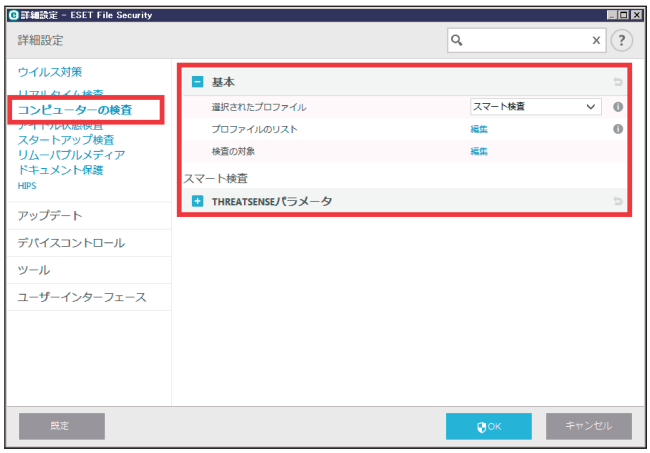
クライアントコンピューターに他のウイルス対策プログラムがインストールされていないか確認します。2 つのリアルタイム保護システムが同時に有効になっていると、互いに競合することがあります。システムに他のウイルス対策プログラムがインストールされている場合は、ESET をインストールする前にそのプログラムをアンインストールすることを推奨します。

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自動的に開始」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 コンピューターの検査

「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［ウイルス対策］＞［コンピューターの検査］を選択します。



■基本

選択されたプロファイル

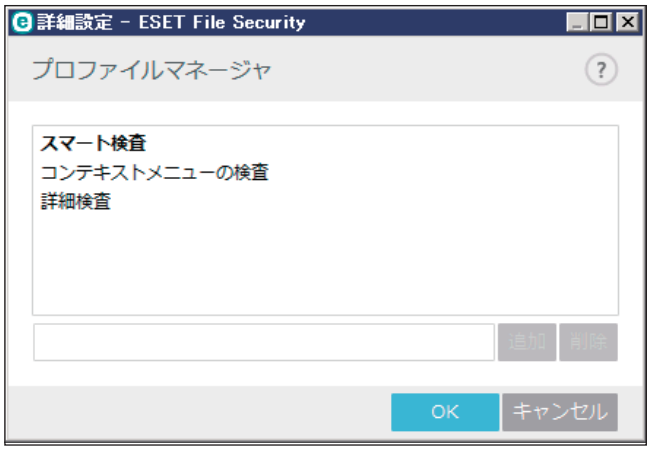
定義済みの次の検査プロファイルを選択します。

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

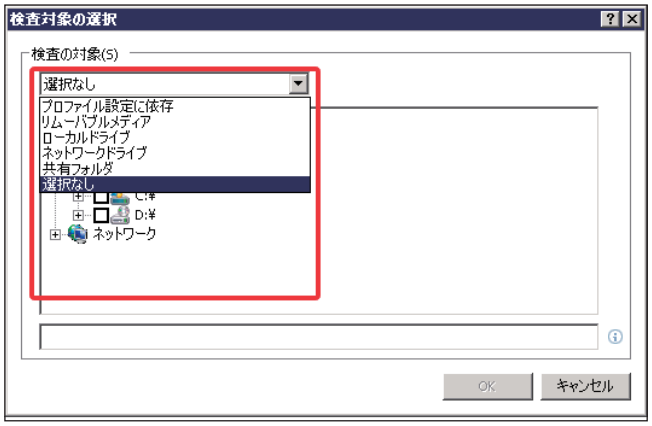
カスタム検査プロファイルを作成します。

［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、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。［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するマルウェアを検査します。
ブートセクタ	マスターブートレコードがウイルスに感染していないかを検査します。
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。
自己解凍形式	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	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。

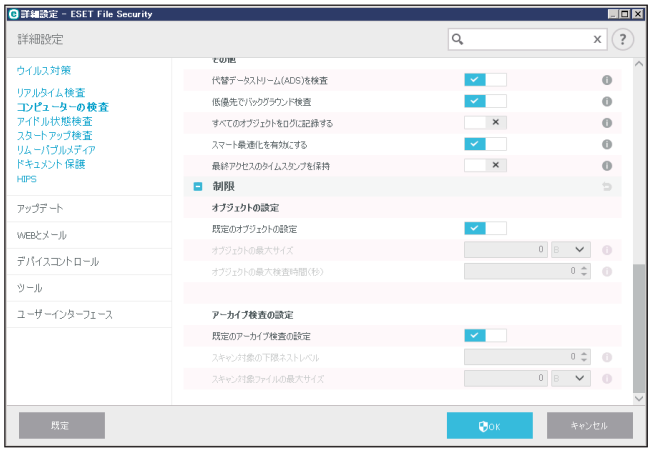
●除外

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記録	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、最長検査時間を設定することもできます。

アーカイブ検査の設定

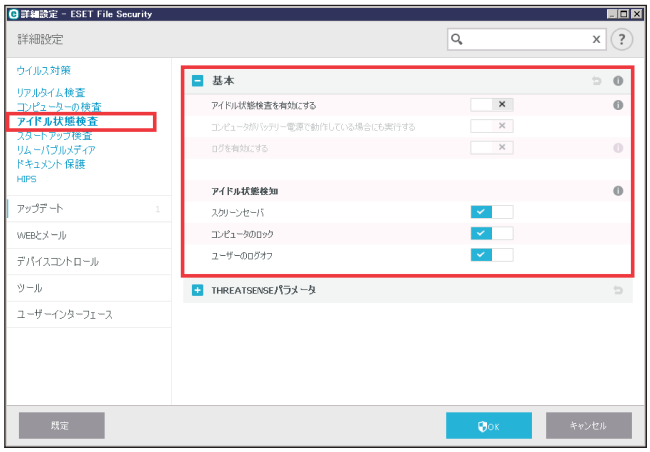
既定のアーカイブ検査の設定	最大で 10 番目のネストレベルまで検査します。実際のサイズにかかわらず検査されます。スキャン対象の下限ネストレベル、スキャン対象ファイルの最大サイズを指定することもできます。

5.1.4 アイドル状態検査

「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［ウイルス対策］＞［アイドル状態検査］を選択します。

■基本

「詳細設定」画面で［アイドル状態検査］＞［基本］の［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。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

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するマルウェアを検査します。
ブートセクタ	マスターブートレコードがウイルスに感染していないかを検査します。
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。
自己解凍形式	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	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記録	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、最長検査時間を設定することもできます。

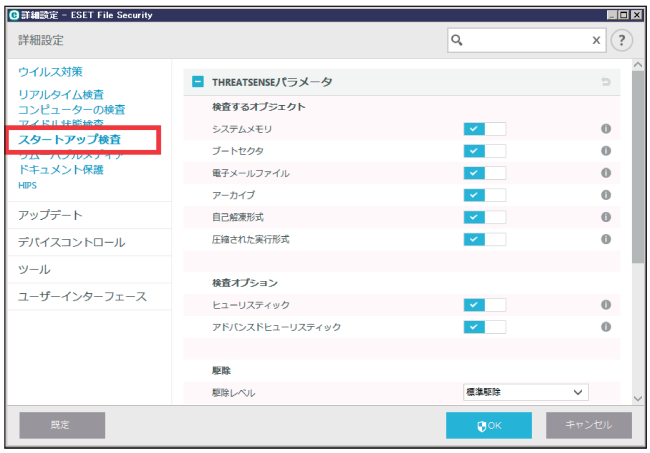
アーカイブ検査の設定

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、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。

5.1.5 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ウイルス定義データベース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。

「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［ウイルス対策］＞［スタートアップ検査］を選択します。スタートアップ時に検査する内容を設定します。



スケジューラタスクの作成と管理の詳細については、「4.5.9 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

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するマルウェアを検査します。
ブートセクタ	マスターブートレコードがウイルスに感染していないかを検査します。
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。
自己解凍形式	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	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。

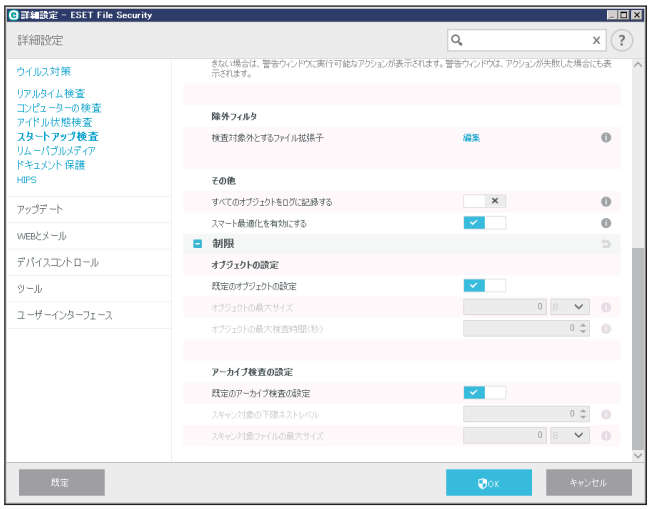
●除外

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記録	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、最長検査時間を設定することもできます。

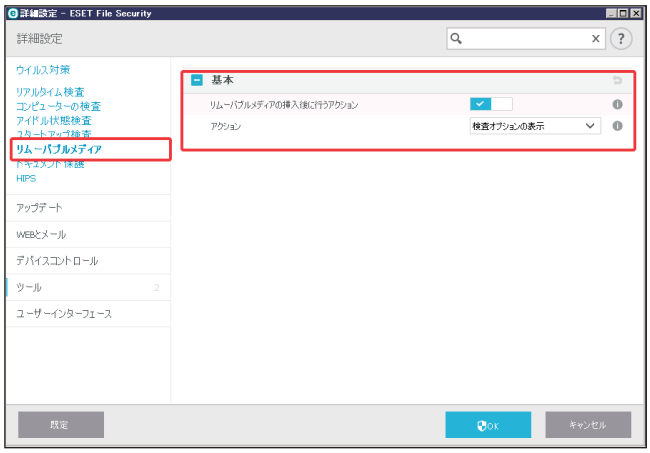
アーカイブ検査の設定

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、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。

5.1.6 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［ウイルス対策］＞［リムーバブルメディア］を選択します。

■基本



［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。

今すぐ検査	リムーバブルメディアの検査を開始します。
後で検査	リムーバブルメディアの検査が延期されます。
設定	「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、「5.1.10 デバイスコントロール」を参照してください。

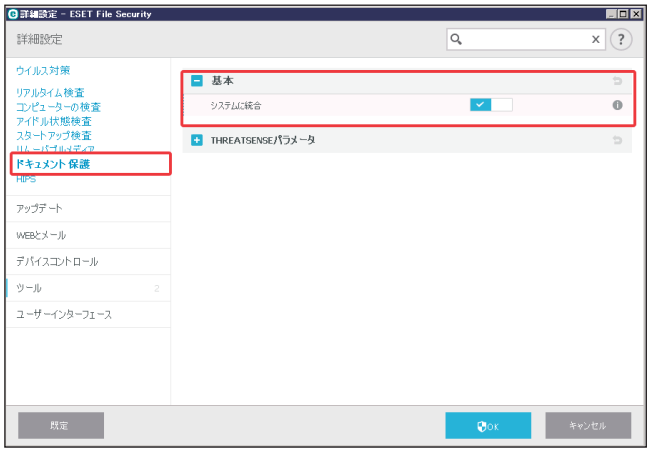
5.1.7 ドキュメント保護

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［ウイルス対策］＞［ドキュメント保護］を選択します。

■基本

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（Microsoft Office 2000 以上、Microsoft Internet Explorer 5.0 以上など）を使用するアプリケーションで有効になります。

■ THREATSENSE パラメータ

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するマルウェアを検査します。
ブートセクタ	マスターブートレコードがウイルスに感染していないかを検査します。
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。
自己解凍形式	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	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。

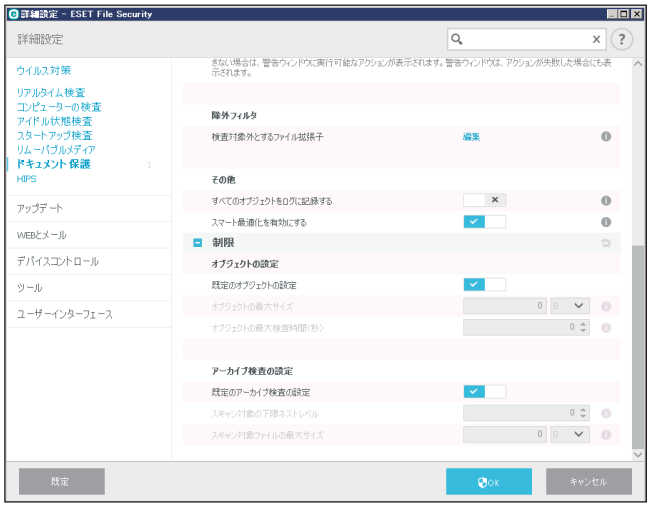
●除外

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記録	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、最長検査時間を設定することもできます。

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、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。

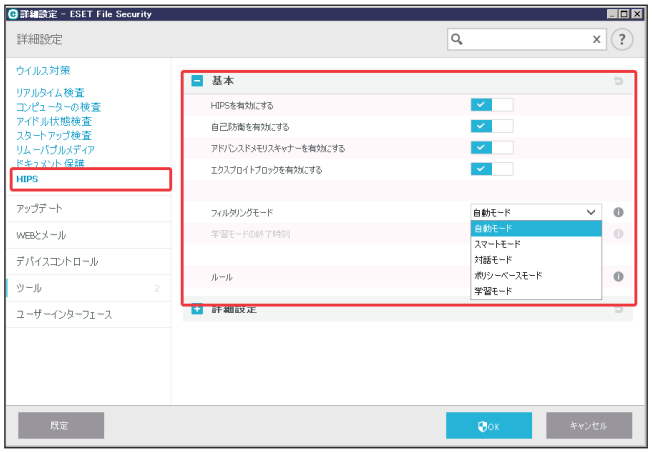
5.1.8 HIPS

! 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［ウイルス対策］＞［HIPS］を選択します。

■基本



HIPS/ 自己防衛

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。

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 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。

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。

自動モード	システムを保護するためにあらかじめ定義されている操作を除いて、すべての操作が有効です。
スマートモード	不審なイベントに関する通知だけを表示します。
対話モード	ユーザーに操作の選択を要求します。
ポリシーベースモード	ルールに従って動作します。ルールにない実行操作はブロックされます。
学習モード	有効にすると、操作の後にルールが作成されます。学習モードで作成されたルールは、手動で作成したルールや、自動モードで作成されるルールより優先度は低くなります。[学習モード] を選択すると、「学習モードの終了時刻」が設定できるようになりますので、学習モードの有効期間を指定してください。有効期間は最大 14 日です。学習モードの有効期間が終了したら、別のフィルタリングモードを選択するか、学習モードを延長してください。また、学習モード中に HIPS で作成したルールを編集することもできます。

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。

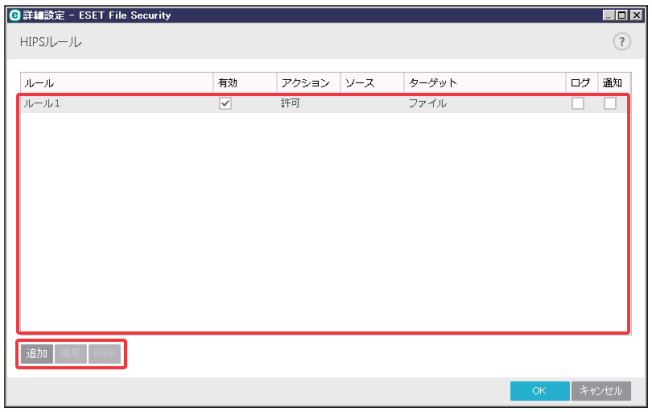
ルールのアクションを［確認］にした場合は、ルールに適合するたびに確認画面が表示され、ユーザーは操作を［遮断］するか［許可］するかを選択できます。指定された時間内にアクションを選択しなかった場合は、ルールに基づいて新しいアクションが選択されます。

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	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	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。

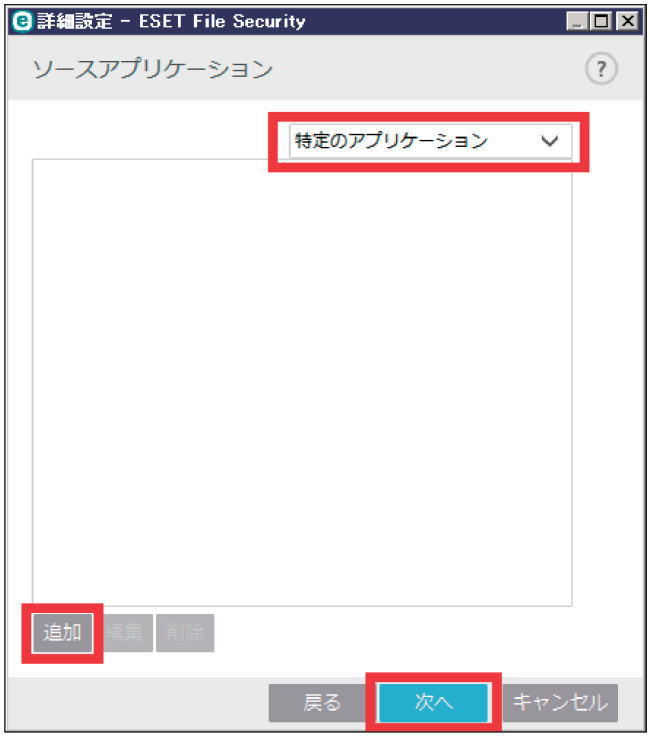
HIPS ルールの追加・編集

［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	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。

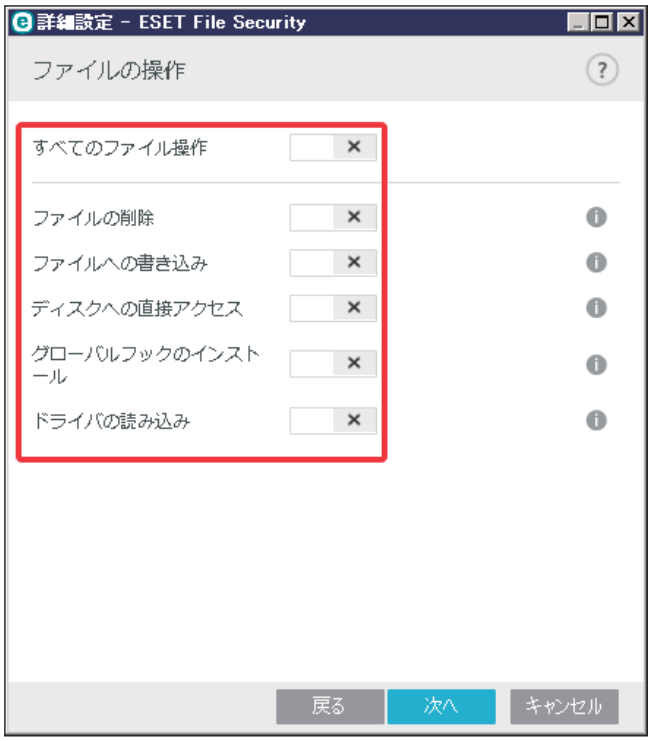
ソースアプリケーションの選択



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

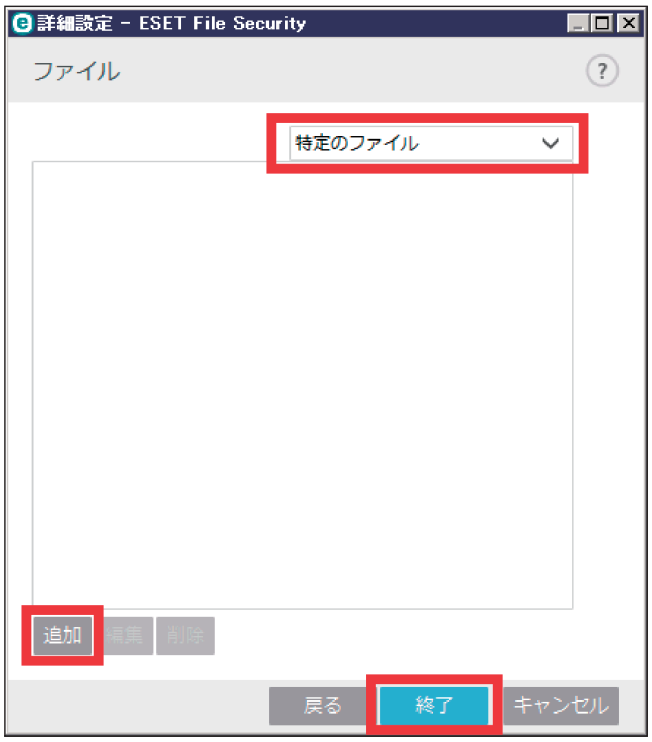
対象となるファイル操作を選択します。



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。
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。

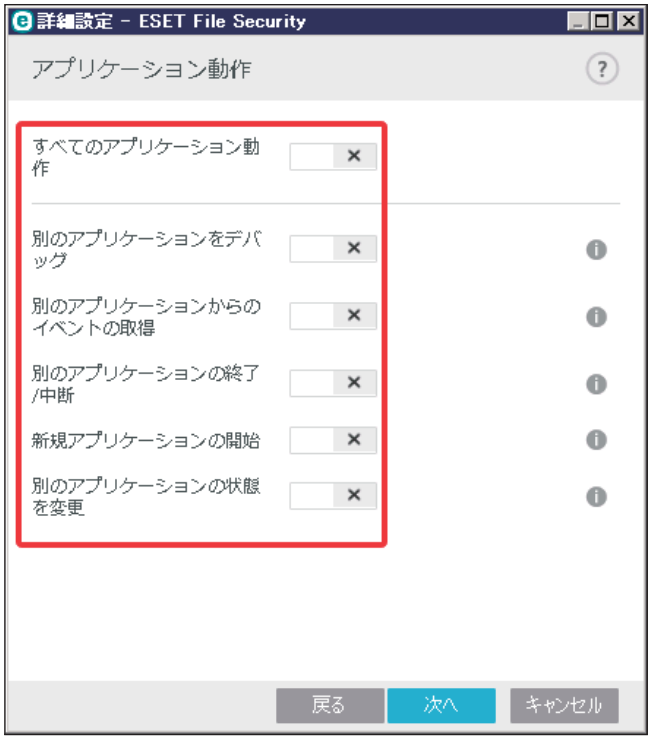
設定が終わったら［次へ］をクリックします。

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。

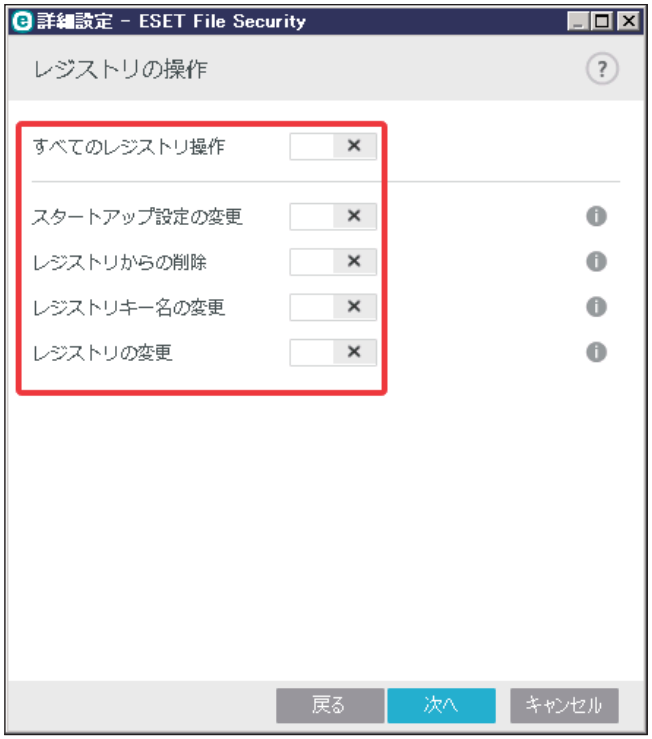
アプリケーション動作



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。

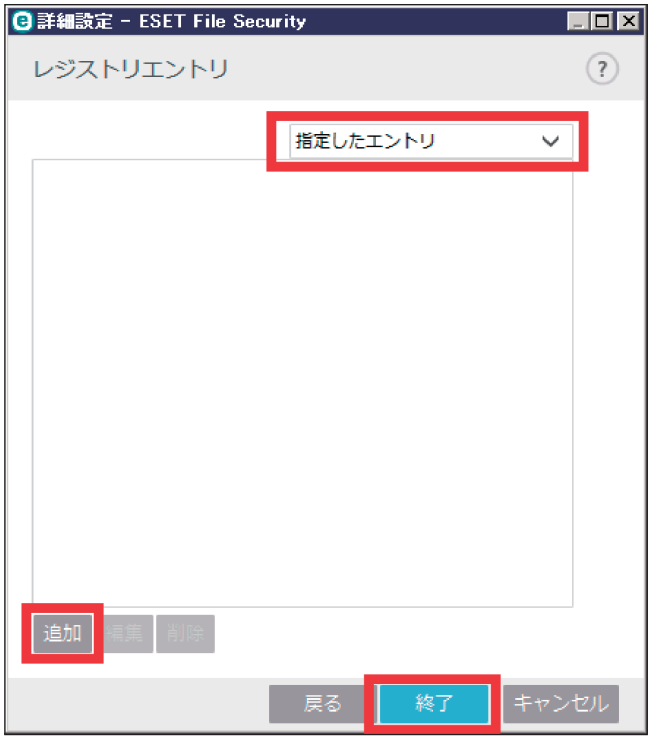
レジストリの操作



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

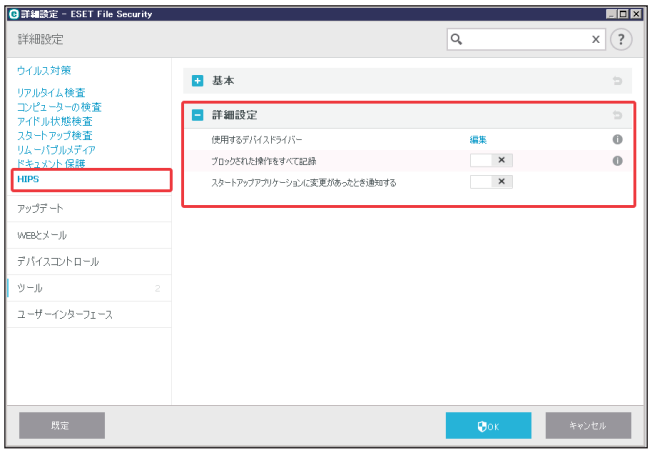
ターゲットの入力では、一定の制限付きでワイルドカードを使用できます。レジストリのパス内では、特定のキーの代わりに「*」（アスタリスク）記号を使用できます。例えば、「HKEY_USERS*\software」は、「HKEY_USER\.default\software」とは一致しますが、「HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software」とは一致しません。
「HKEY_LOCAL_MACHINE\system\ControlSet*」は、有効なレジストリキーパスではありません。「*」の入ったレジストリキーのパスは、「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

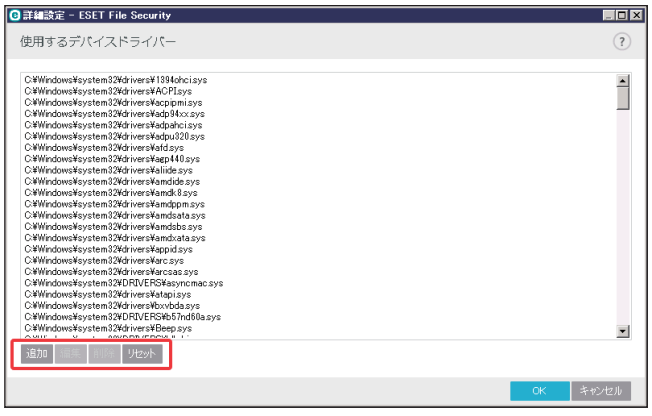
アプリケーションの動作をデバッグ、分析するための設定をします。



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。

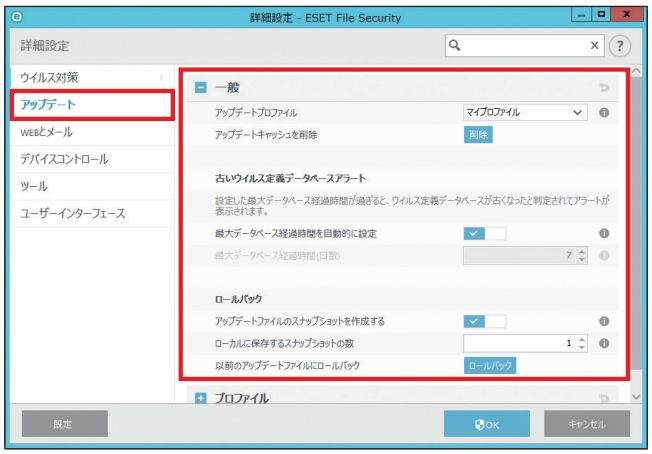
ワンポイント

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。

5.1.9 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。

■一般



アップデートプロファイル	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	ウイルス定義データベース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。	
古いウイルス定義データベースアラート	ウイルス定義データベース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。	
ロールバック	ウイルス定義データベース／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。	
	アップデートファイルのスナップショットを作成	有効にすると、ウイルス定義データベース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。
	以前のアップデートファイルにロールバック	［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	［基本］から［ミラーサーバーの作成］までの設定を編集するプロファイルを選択します。

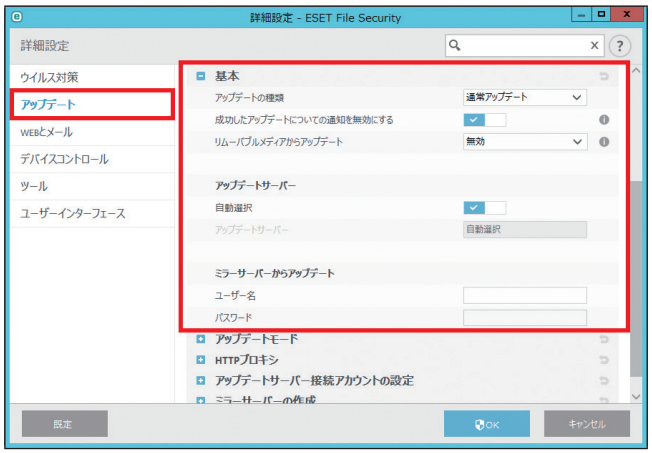
! 重　要

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。

■基本

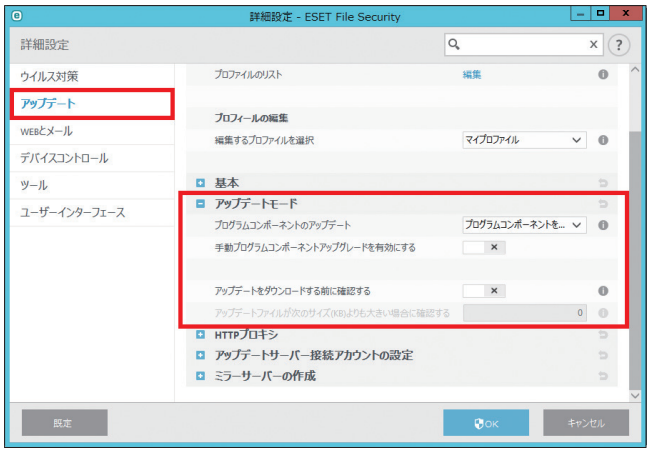
成功したアップデートについての通知を表示しない
画面右下のシステムトレイ通知が無効になります。全画面のアプリケーションまたはゲームを使用しているときに、アップデートが成功した際の通知が表示されないようにします。プレゼンテーションモードではその他のすべての通知がオフになるため、注意が必要です。



アップデートの種類	次の中からアップデート方法を選択します。 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、徹底的な内部テストを経て、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ウイルス定義データベース（実際の環境でテスト済みで、安定しているとみなされるウイルス定義データベース）を提供する特別なサーバーから、アップデートファイルをダウンロードできます。
成功したアップデートについての通知を無効にする	有効にするとシステムトレイに通知が表示されません。
リムーバブルメディアからアップデート	リムーバブルメディアのルートにミラーサーバ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。
アップデートサーバー	アップデートサーバーは、アップデートファイルが保存される場所です。ESET サーバーを使用するときには、[自動選択] を有効にしておくことを推奨します。カスタムアップデートサーバーを使用していて、既定の ESET サーバーに戻したい場合は、[自動選択] を無効にして [アップデートサーバー] のテキストボックスに「AUTOSELECT」と入力すると自動的に ESET サーバーが選択されます。 • ローカルの HTTP サーバーに設定されたミラーサーバーを使用する場合は、アップデートサーバーを次のように設定します。 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 を使用するローカルの HTTP サーバーに設定されたミラーサーバーを使用する場合は、アップデートサーバーを次のように設定します。 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は、アップデートサーバーを次のように設定します。 ¥¥computer_name_or_its_IP_address¥shared_folder
ミラーサーバーからアップデート	アップデートサーバーの認証には、製品認証キーを使用します。ローカルミラーサーバーを使用する場合は、クライアントコンピューターの認証情報を入力して、アップデートを受信する前にミラーサーバーにログインします。既定では、認証が不要のため、[ユーザー名] と [パスワード] のテキストボックスは空のままです。

■アップデートモード

新しい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事前に定義することができます。



ワンポイント

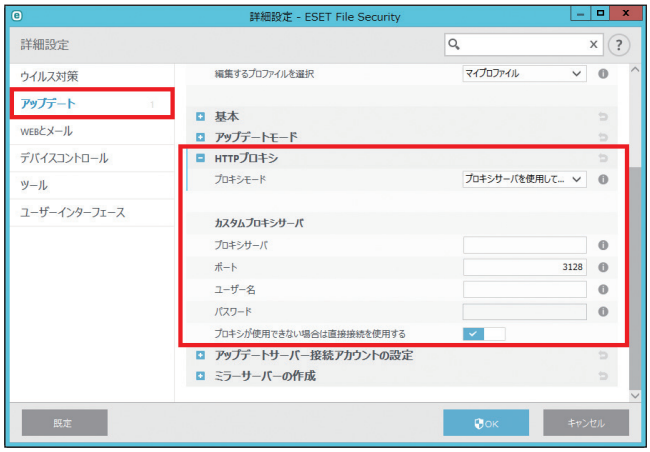
プログラムコンポーネントのアップデートファイルをインストールした後、再起動が必要になることがあります。

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をダウンロードする前に確認する	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が利用可能になったとき、アップデートするかどうかの確認を求められます。
	プログラムコンポーネントを常にアップデートする	プログラムコンポーネントのアップデートが自動的に実行されます。コンピューターの再起動が必要になることがあるので注意してください。
	プログラムコンポーネントをアップデートしない	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。メンテナンス中しか再起動できないサーバーなどに適した設定です。
手動プログラムコンポーネントアップグレードを有効にする	既定は無効に設定されています。有効にすると「アップグレード」ペインで新しいプログラムのアップデートを確認できます。本機能は、日本語版ではご使用になれません。	
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。既定値は「0」KB、制限値は「0」～「2000000」KB です。	

!重　要

最適なオプションは、設定が適用されるワークステーションによって異なります。ワークステーションとサーバーとでは異なる点に注意してください。例えば、プログラムのアップデート後にサーバーを自動的に再起動すると、重大な損害が生じることがあります。この場合は、［プログラムコンポーネントをアップデートしない］を選択してください。

■ HTTP プロキシ



［プロキシモード］

プロキシサーバーを使用しない	アップデートにプロキシサーバーを使用しません。
プロキシサーバー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］＞［プロキシサーバー］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（下記参照）。
グローバルプロキシサーバー設定を使用する（既定値）	「詳細設定」画面の［ツール］＞［プロキシサーバー］で既に指定されているプロキシサーバーの設定オプションが使用されます。

［カスタムプロキシサーバ］

プロキシサーバー	サーバー名を設定します。
ポート	ポート番号を設定します（プロキシサーバーの規定値は「3128」）
ユーザー名	必要な場合はユーザー名を設定します。
パスワード	必要な場合はパスワードを設定します。
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。

！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。プロキシサーバー経由でインターネットに接続するためにパスワードが必要であることが分かっている場合にのみ入力してください。

■アップデートサーバー接続アカウントの設定

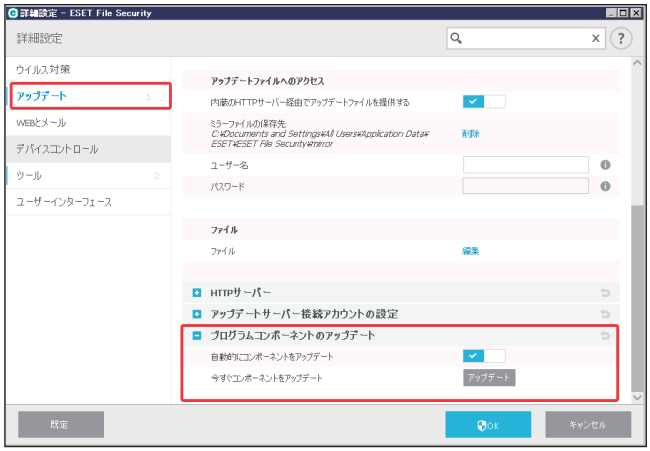
本製品では、本機能はご使用いただけません。

■ミラーサーバーの作成

本製品では、本機能はご使用いただけません。

●プログラムコンポーネントのアップデート

この項目では次の内容を設定できます。



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。

●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。

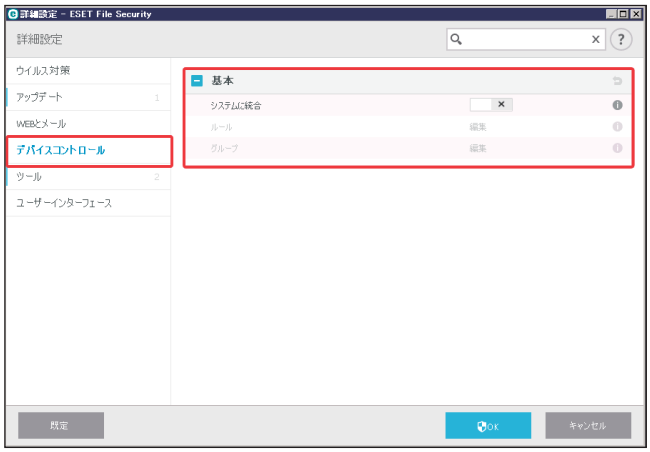
- 定期的に自動アップデート
- ダイヤルアップ接続後に自動アップデート
- ユーザーログオン後に自動アップデート

各アップデートタスクは、ユーザーのニーズに合わせて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、「4.5.9 スケジューラ」を参照してください。

5.1.10 デバイスコントロール

自動デバイスコントロール（CD/DVD/USB など）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。

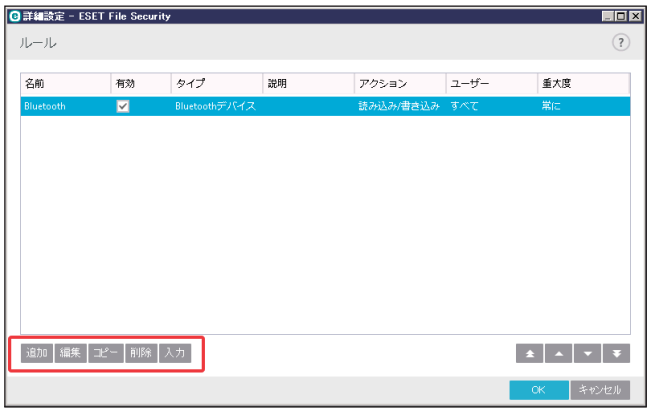


［システム統合］を有効にするとデバイスコントロール機能が有効になります。この変更を有効にするには、クライアントコンピューターの再起動が必要になります。

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。

■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。

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、ユーザーごとのアクション制御はできません。

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が許可され、読み込み／書き込みが可能です。
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

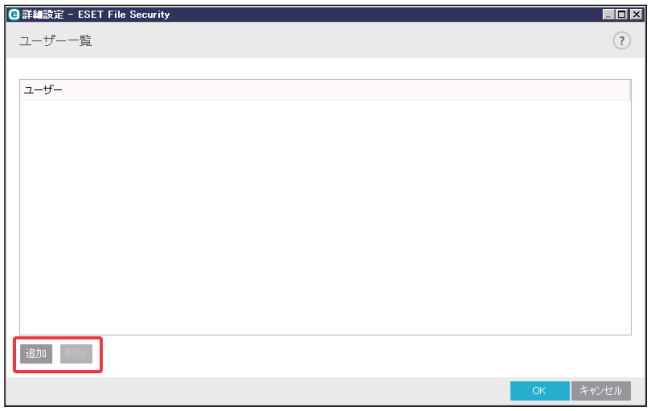
デバイスのパラメーターを確認するには、デバイスのタイプのルールを作成し、デバイスをクライアントコンピューターに接続してから、デバイスコントロールログでデバイスの詳細を確認します。

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

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。

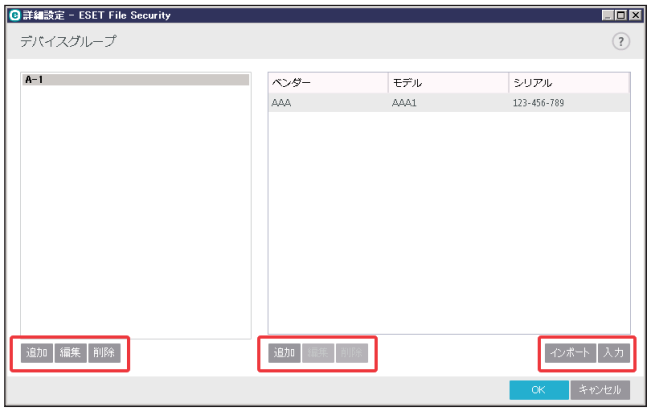
■グループ

! 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。

5.1.11 ツール

「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。

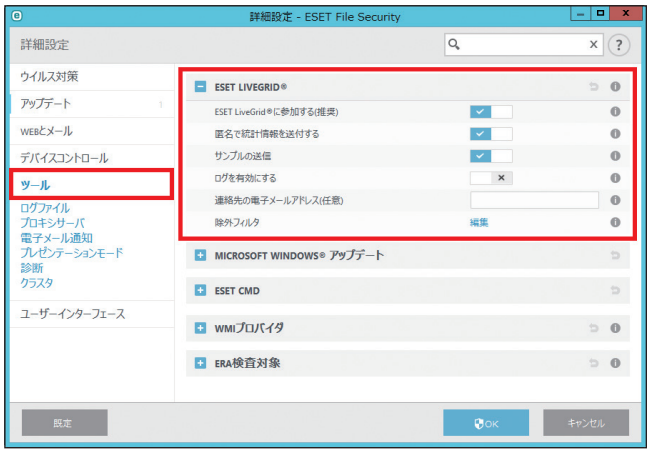
■ ESET LIVEGRID

ESET Live Grid 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 Live Grid を操作したり、ESET Live Grid 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。

1. ESET Live Grid 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ウイルス定義データベースのアップデートよりも遅くなることがあります。
2. ESET Live Grid 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。

ESET Live Grid 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。

既定では、ESET File Security for Microsoft Windows Server は詳細な分析を受けるために、不審なファイルを ESET ウイルスラボに送信するように設定されています。「.doc」または「.xls」など、特定の拡張子の付いたファイルは機密情報が含まれている可能性があるため、常に除外されます。送信したくない特定のファイルがあれば、他の拡張子を除外の対象に追加することもできます。
ESET Live Grid 評価システムは、クラウドベースのホワイトリストとブラックリストを提供します。
「詳細設定」画面の［ツール］＞［ESET LIVEGRID］を選択します。



次の項目について設定できます。

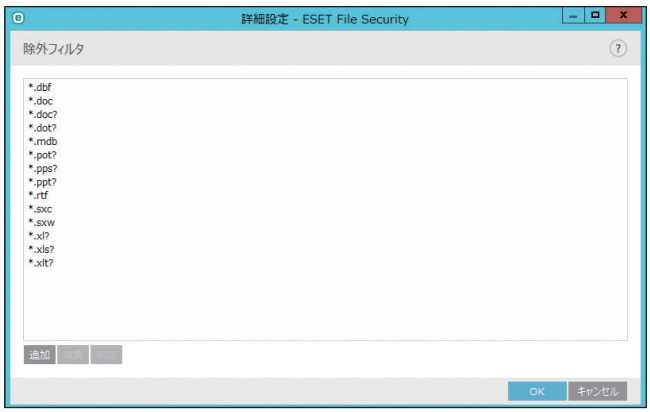
ESET LiveGrid に参加する（推奨）	有効にすると、新しいウイルスと危険なコードが検出された場所に関する匿名の情報を ESET のウイルスラボに提出します。ESET Live Grid 評価システムは、解析済みのウイルスをクラウドのホワイトリストおよびブラックリストのデータベースと比較し、ESET マルウェア対策ソリューションの効率化を図ります。
匿名の統計情報を送信	有効にすると、脅威名、脅威を検出した日時、検出方法、関連付けられたメタデータ、製品バージョン、設定（システム情報を含む）など、新しく検出された脅威に関する情報を ESET が収集します。
サンプルの送信	有効にすると、脅威に似ているファイルや、標準ではない特性や動作を持つ不審なファイルは、分析するために ESET に送信されます。
ログを有効にする	有効にすると、ファイルと統計情報の送信を記録するイベントログが作成されます。
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。
除外フィルタ	［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（下記参照）。

ワンポイント

ESET Live Grid 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。

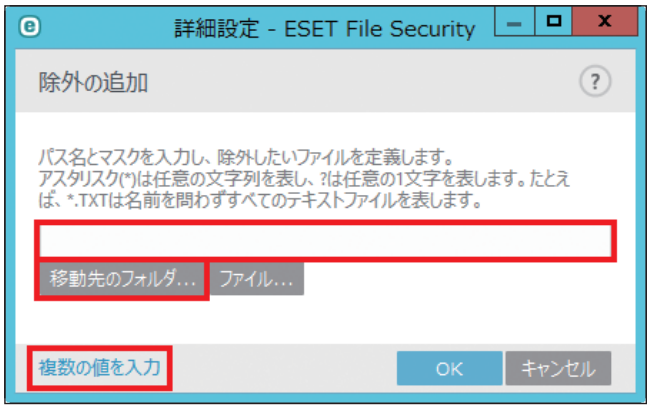
●除外フィルタ

ESET Live Grid の「除外」の［編集］オプションでは、分析を受けるために ESET のウイルスラボに不審なファイルを提出する際に除外されるファイルのフィルターを設定することができます。



ファイル種類の追加、編集、削除ができます。

［追加］または［編集］をクリックすると「除外の追加」または「除外の編集」画面が表示されます。

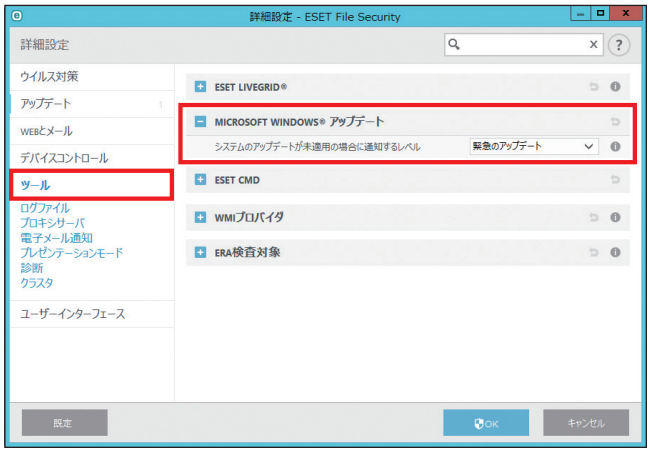


除外するファイルを定義します。「＊」は任意の文字列を、「？」は任意の 1 文字を表します。
例えば「*.txt」は拡張子 txt を持つすべてのファイルを表します。
［フォルダ］、［ファイル］をクリックするとフォルダやファイルを指定することもできます。
［複数の値を入力］をクリックすると一度に複数の値を指定することができます。

不審なファイルがある場合は、ESET ウイルスラボに提出して分析を受けることができます。分析の結果、そのファイルが悪意のあるアプリケーションであることが判明すると、以降のウイルス定義データベースのアップデートで反映されます。

■ MICROSOFT WINDOWS UPDATE

Microsoft Windows Update では、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 Update 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

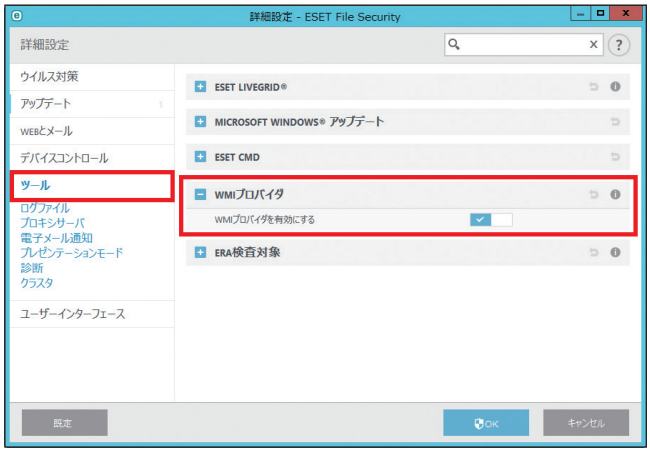
システムアップデートの通知後、アップデートサーバーでステータスの検証を行った後、「システムのアップデート」画面が表示されます。そのため、通知レベルの設定後はすぐにシステムのアップデートができない場合があります。

■ WMI プロバイダー

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_GreylistLog
- ESET_SpamLog

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
Edition	「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

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_GreylistLog

ESET_GreylistLog 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「Greylist」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」。
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
Action	実行されたアクション
TimeToAccept	電子メールが許可されるまでの時間（分）

ESET_SpamLog

ESET_SpamLog 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「Spamlog」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」。
Sender	電子メール送信者
Recipients	電子メール受信者
Subject	電子メール件名
Received	受信時刻
Score	「0 ～ 100」パーセントで表された迷惑メールのスコア
Reason	電子メールが迷惑メールに設定された理由
Action	実行されたアクション
DiagInfo	詳細な診断情報

●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
```

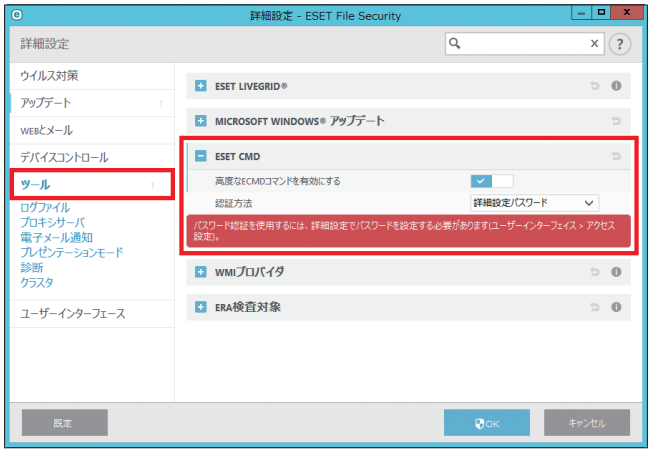
■ ERA 検査対象

本製品では、本機能はご使用いただけません。

■ 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。ERA 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

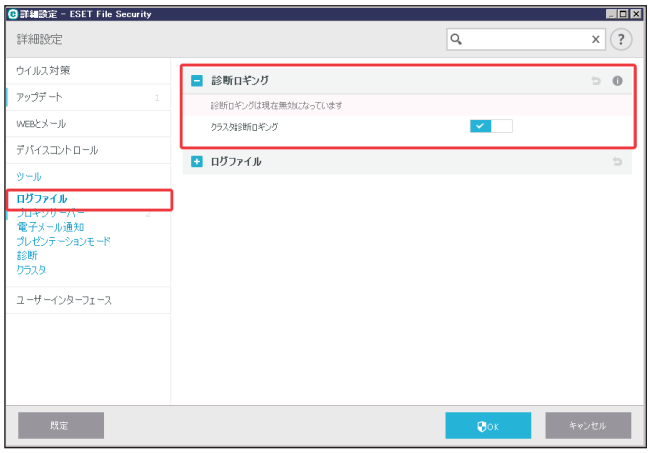
1. ユーザーズサイトから XmlSignTool をダウンロードします。
2. 管理者として実行を使用してコマンドプロンプトを開きます。
3. XmlSignTool.exe を置いたフォルダに移動します。
4. コマンドを実行し、.xml 設定ファイルに署名します。

   使用方法：
   XmlSignTool <xml ファイルパス >
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。

5.1.12 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。

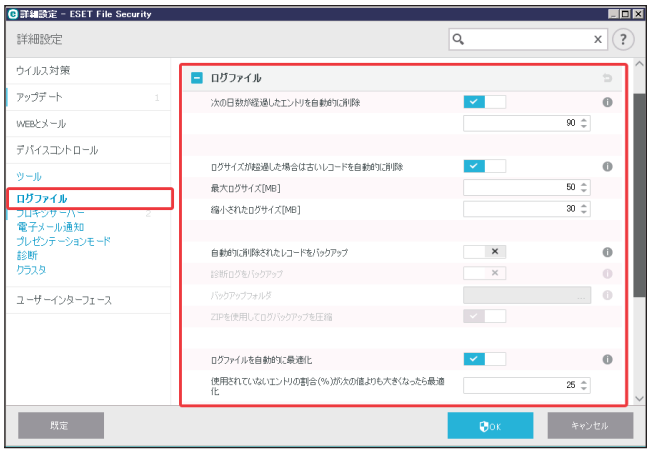
■診断ロギング



診断ロギング機能のうち、クラスタ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。

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。
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。
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。

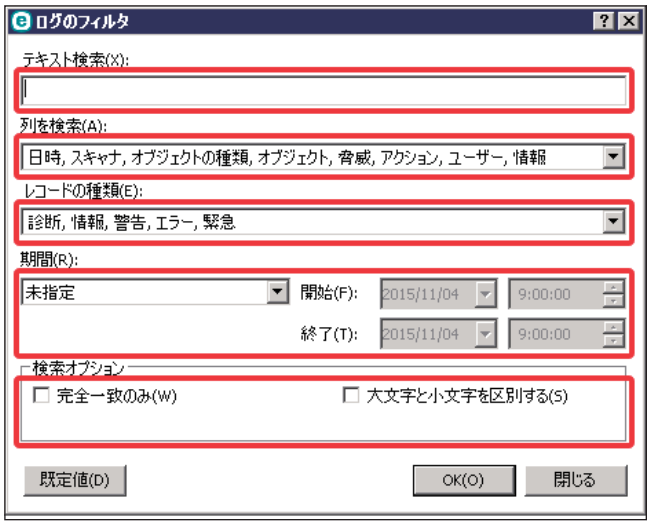
! 重　要

サポートセンターより、問題をより迅速に解決できるように、クライアントコンピューターのログを提供するように依頼させていただく場合があります。ESET Log Collector を使用すると、必要な情報を簡単に収集できます。ESET Log Collector の詳細については、「4.5.3　ESET Log Collector」を参照してください。

●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」といったエラーを記録します。
緊急	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。

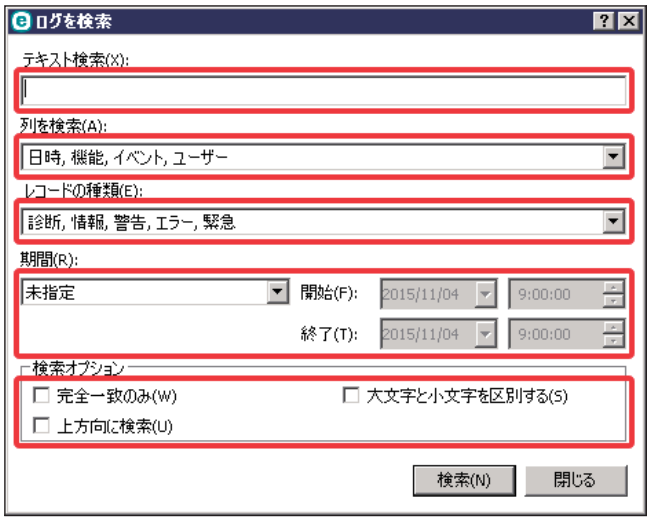
その他に次の項目を設定します。

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」といったエラーを記録します。
緊急	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。

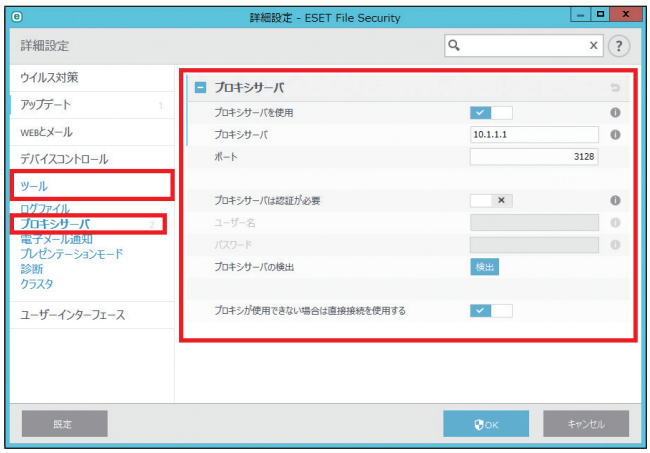
期間	結果を表示する期間を指定します。 ・未指定（既定）ー期間内で検索するのではなく、ログ全体を検索します。 ・昨日 ・先週 ・先月 ・期間ー正確な期間（日時）を指定して、指定した期間のレコードのみを検索できます。
開始／終了	検索結果を表示する期間を指定します。
完全一致のみ	「テキスト検索」のテキストボックスで指定した文字列と単語と完全一致レコードのみを検索します。
大文字と小文字を区別	大文字と小文字を区別した上で、「テキスト検索」のテキストボックスの文字列と一致するレコードのみを検索します。
上方向に検索	現在の位置から上方向へ検索します。

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。

5.1.13 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。

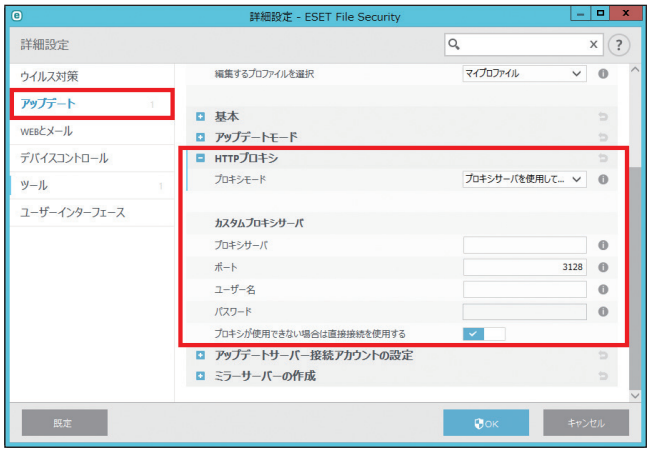
「設定」画面で［詳細設定］をクリックし、「詳細設定」画面で［ツール］＞［プロキシサーバ］を選択します。



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。

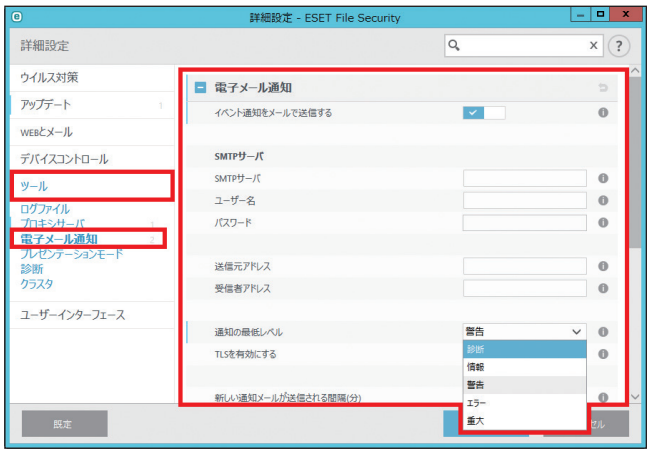
プロキシサーバー設定は詳細設定のアップデート設定内（[詳細設定] > [アップデート] > [HTTP プロキシ]）からも定義できます。



「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］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。ウイルス定義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、「5.1.9　アップデート」の「■ HTTP プロキシ」を参照してください。

5.1.14 電子メール通知

選択されたイベントが発生すると、自動的にメールで通知することができます。
「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］＞［電子メール通知］を選択します。



! 重 要

TLS 暗号化機能を備えた SMTP サーバーがサポートされています。

［イベント通知をメールで送信］を有効にして次の設定をします。

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。
通知の最低レベル	送信する通知の最低詳細レベルを指定します。診断、情報、警告、エラー、重大から選択します。
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。
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。
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。

メッセージの書式

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。「●メッセージの書式」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。「●メッセージの書式」も参照してください。
各地域のアルファベット文字を使用	Windows の地域設定に基づいて、電子メールメッセージは ANSI 文字コードを使用して（例えば、「windows-1250」）でエンコードされます。この項目を無効にしたままの場合、メッセージは ACSII 7 bit（例えば、「á」は「a」に変換され、不明な記号は「?」（疑問符）に変換されます）でエンコードされます。
各地域の文字エンコーディングを使用	電子メールメッセージのソースは Quoted-printable（QP）書式でエンコードされます。この書式では、ASCII 文字を使用し、特殊な文字を 8 bit 書式（áéíóú）の電子メールで正確に送信できます。

●メッセージの書式

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。

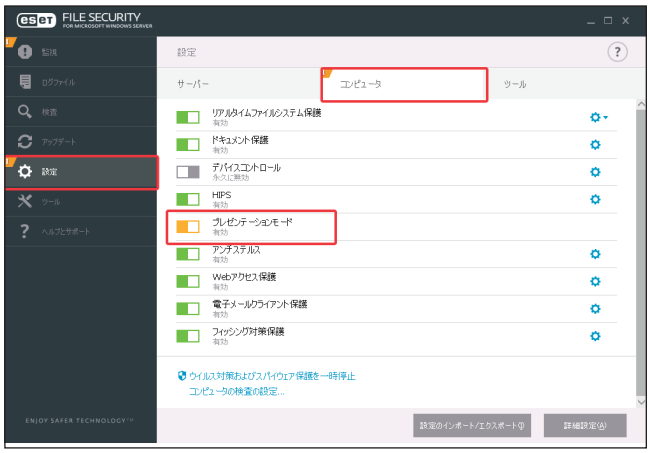
%TimeStamp%	イベントの日時
%Scanner%	関連するモジュール
%ComputerName%	警告が発生したクライアントコンピューターの名前
%ProgramName%	警告を生成したプログラムの名前
%InfectedObject%	感染しているファイルやメールなどの名前
%ErrorDescription%	ウイルス以外のイベントの説明

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。

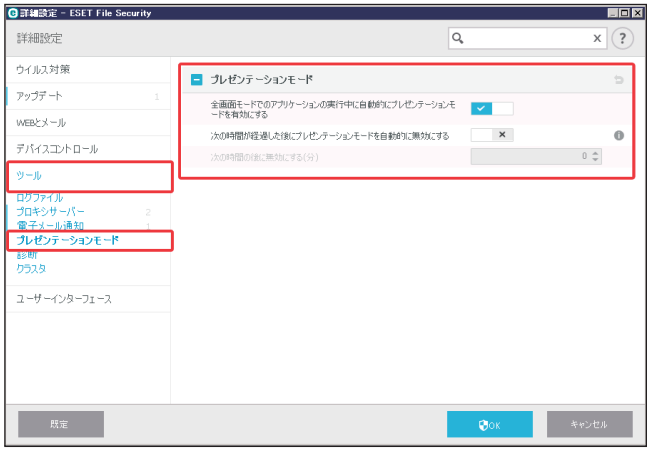
5.1.15 プレゼンテーションモード

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。



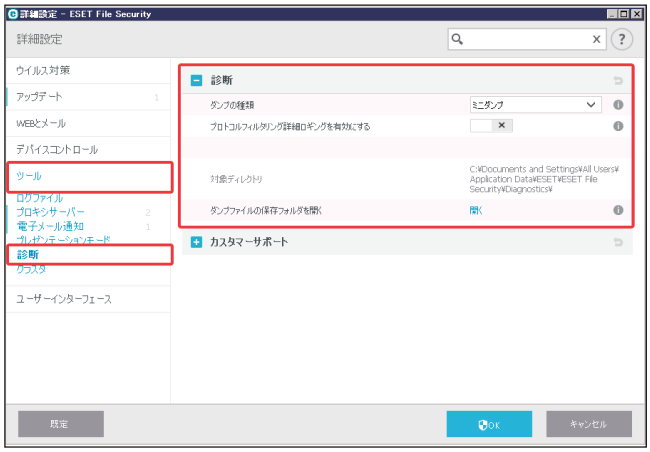
全画面モードでのアプリケーションの実行中に自動的にプレゼンテーションモードを有効にする	アプリケーションを全画面モードで起動したときに、プレゼンテーションモードが自動的に開始されます。アプリケーションを終了すると、プレゼンテーションモードは自動的に停止します。ゲームやプレゼンテーションなど、全画面で使用するアプリケーションを使用する場合に便利です。
次の時間が経過した後にプレゼンテーションモードを自動的に無効にする	プレゼンテーションモードが自動的に停止する時間を分単位で設定できます。制限値は「0」～「2000」分です。

5.1.16 診断

■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。



「ダンプの種類」では次のオプションのいずれかを選択します。

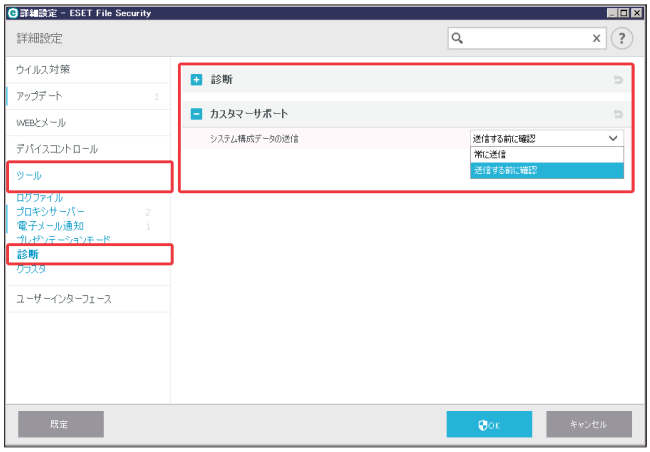
無効にする	ダンプファイルを生成しません。
ミニダンプ	アプリケーションがクラッシュした原因を特定するための最低限の情報を記録したダンプファイルを生成します。保存領域が限られているときに便利です。ただし、記録される情報が限られるため、クラッシュ時に実行されていたスレッドが直接の原因ではない場合、ダンプファイルを解析しても原因を特定できない場合があります。
完全なメモリダンプ	アプリケーションのクラッシュ時、システムメモリーのすべての内容を記録したダンプファイルを生成します。ダンプファイルには、生成したときに実行されていたプロセスデータが含まれます。

その他に次の項目を設定できます。

プロトコルフィルタリング詳細ロギングを有効にする	プロトコルフィルタリング詳細ロギングの機能をチェックボックスで有効または無効にします。
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。

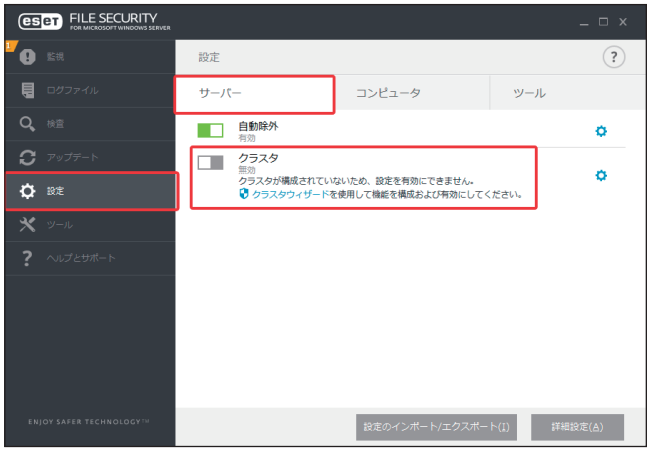
■カスタマーサポート

カスタマーサポートに、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］＞［カスタマーサポート］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。



5.1.17 クラスタ

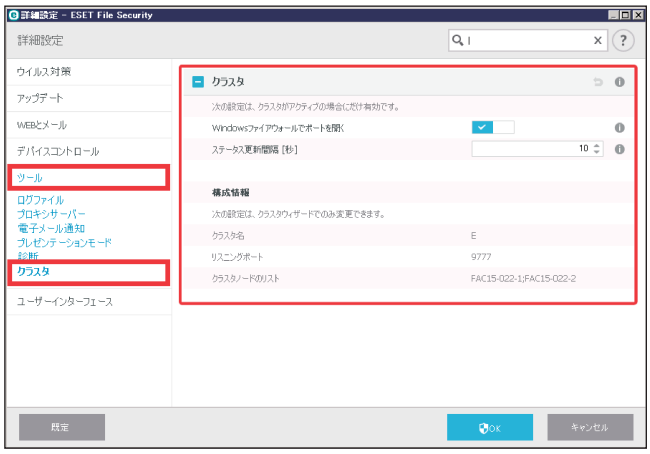
クラスタを使うと、ESET サーバー製品は相互に通信し、構成や通知などのデータを交換します。また、製品グループが正しく動作するために必要なデータを同期することができます。例えば、Windows Failover Cluster やネットワーク負荷分散（NLB）クラスター内のノードをグループで管理する場合に有用です。ESET Cluster では、インスタンス間でこの整合性を保証します。
クラスタが構成されると「設定」メニューの「サーバー」で［クラスタ］が有効になります。
クラスタを構成するには、この画面で［クラスタウィザード］をクリックします。



■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。

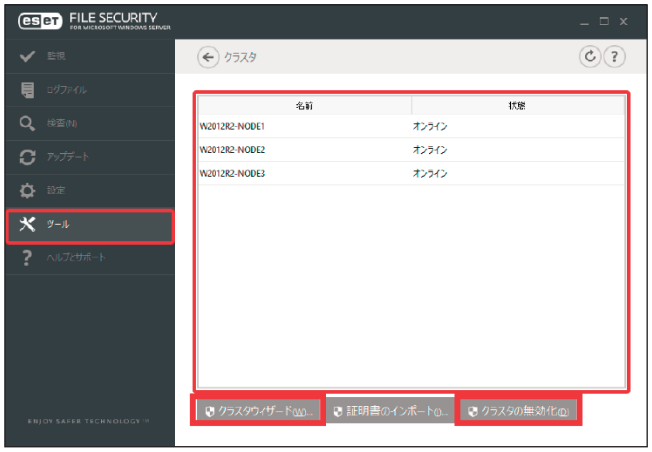
クラスタが構成され有効な場合のみ設定できます。



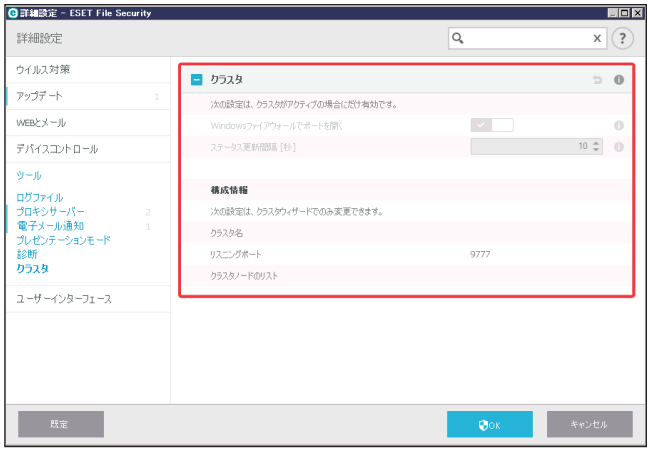
Windows ファイアウォールでポートを開く	Windows ファイアウォールでポートを開く場合に有効にします。
ステータス更新間隔	ステータスの更新間隔を秒数で指定します。

■クラスタの有効 / 無効

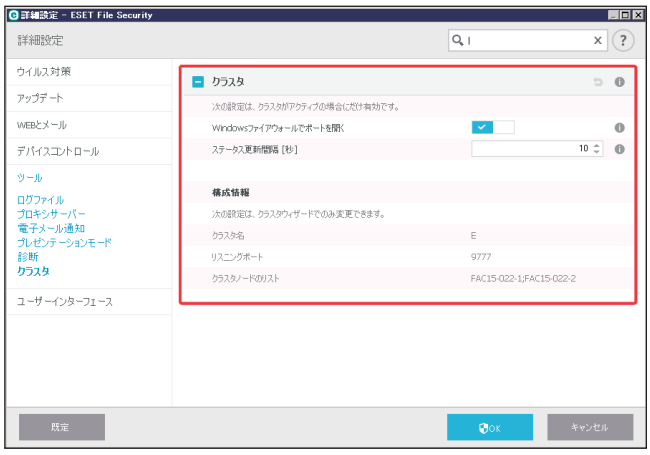
クラスタを正しく設定または無効にするには、メインメニューの［ツール］＞［クラスタ］をクリックし、「クラスタ」画面下部の［クラスタウィザード］または［クラスタの無効化］を使用します。



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。



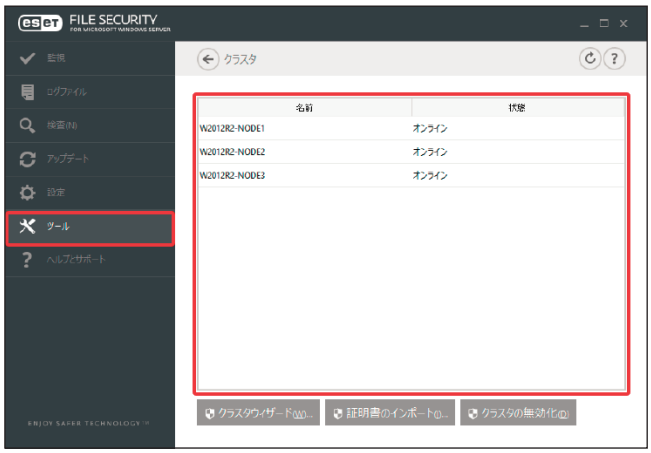
クラスタが詳細設定のオプションで正しく構成されている場合は、次のような画面になります。



クラスタに関する詳細情報については、「4.5.5　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）

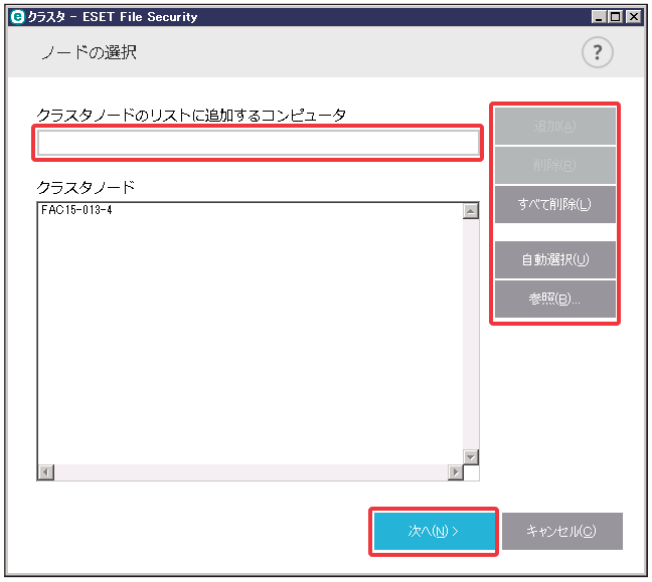
クラスタを設定する最初のステップはノードの追加です。[自動選択] または [参照] オプションのいずれかを使用してノードを追加します。または、[クラスタノードのリストに追加するコンピュータ] のテキストボックスにサーバー名を入力して、[追加] ボタンをクリックします。

[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。

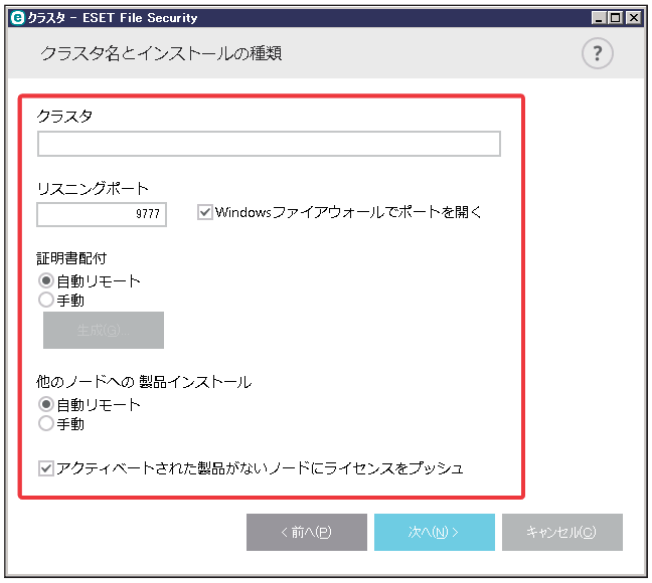
既存のクラスタが存在する場合は、上記と同じ手順で新しいノードを追加できます。

!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。	

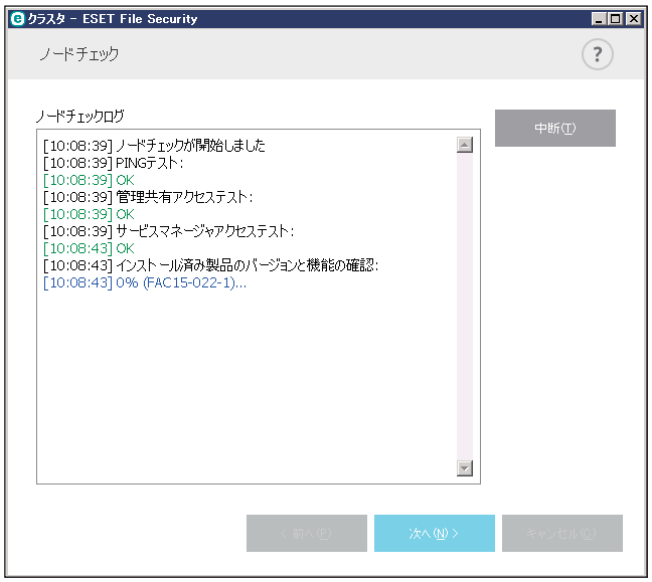
！重 要

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。

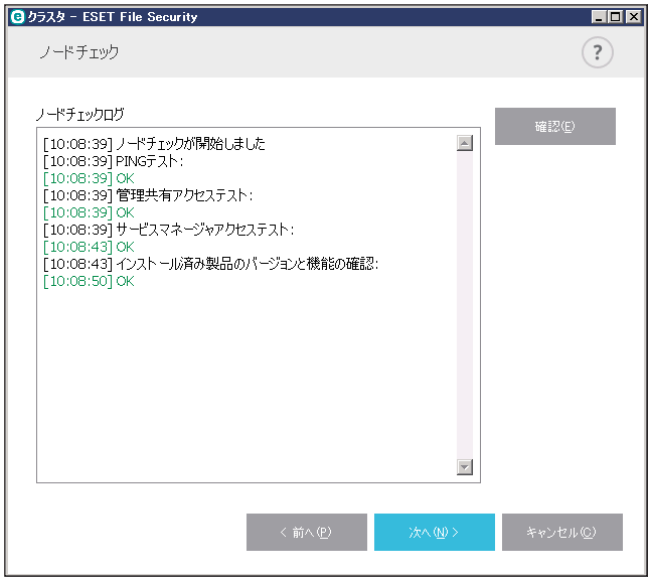
●クラスタウィザード（3 ページ目）

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

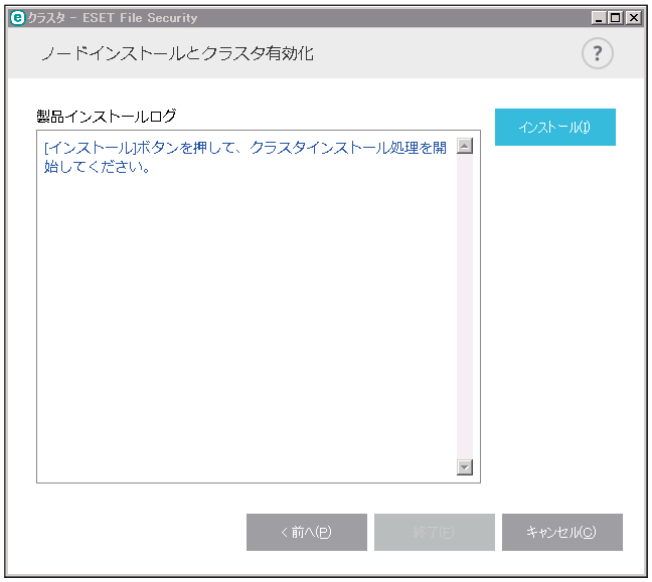


ノードチェックが完了すると次のレポートが表示されます。



●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。

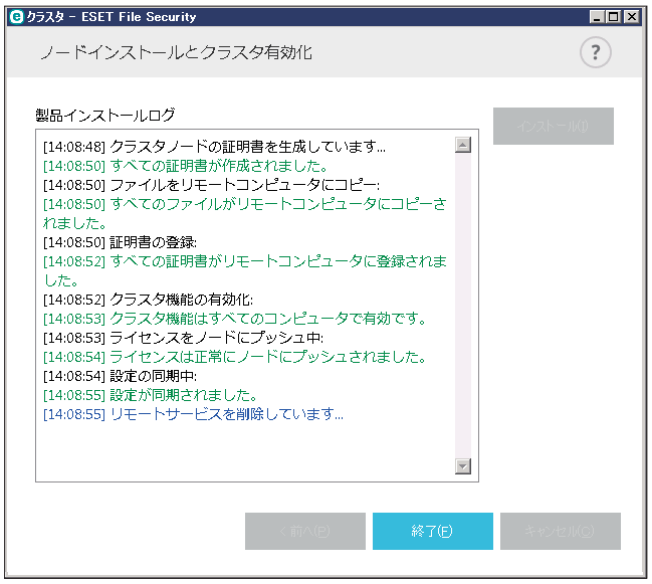


!重　要

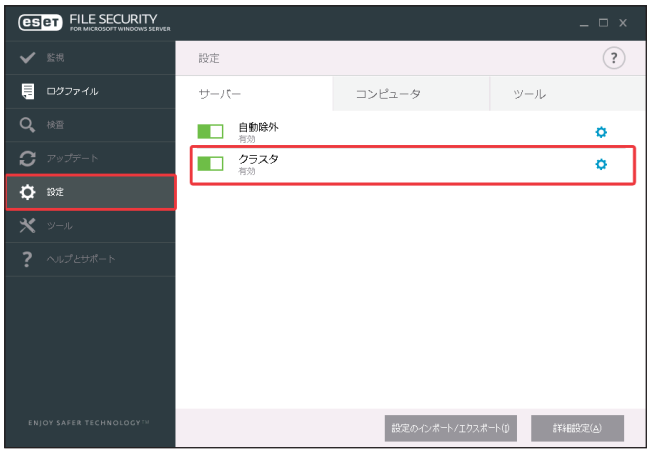
異なるプラットフォーム（32 bit と 64 bit）を持つノードで自動リモートインストールを使用しようとするとプラットフォームの違いが検出されます。このようなノードでは手動でインストールします。

!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

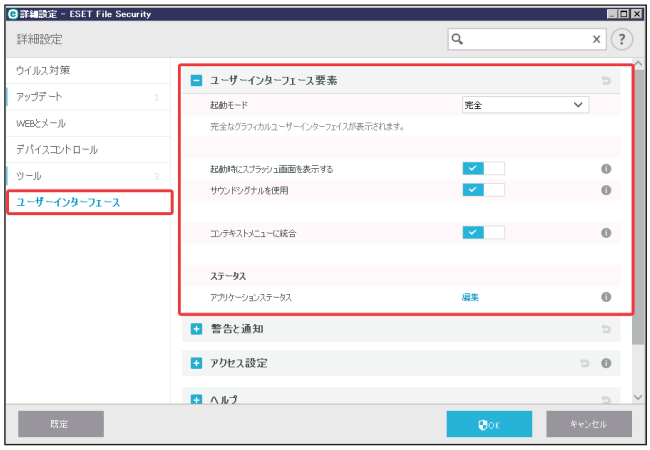
1. 「クラスタ」画面下部の［証明書のインポート］をクリックすると、証明書（クラスタウィザードの使用中に生成される）が含まれているフォルダーに移動します。
2. 証明書ファイルを選択し、［開く］をクリックします。

5.1.18 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。

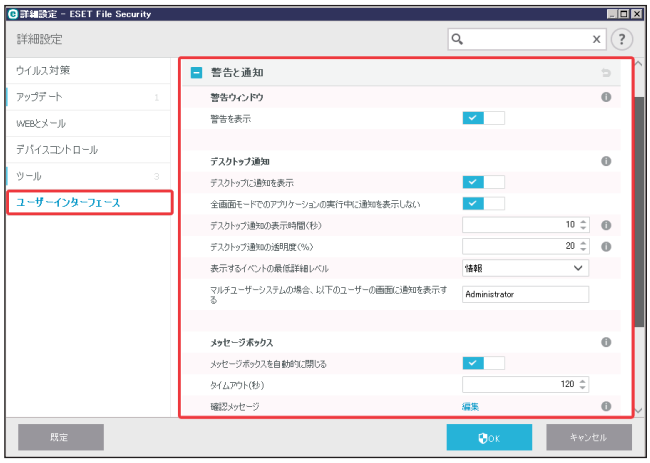
完全	すべての GUI を表示します。
ターミナル、端末	通知やアラートは表示されません。このモードは管理者によってのみ設定できます。

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	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	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。

■警告と通知

「警告と通知」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

「警告を表示する」をオフにすると、すべての警告画面が表示されなくなります。この設定は、特定の限られた状況でのみ使用してください。既定の設定（有効）のままで使用することを推奨します。

デスクトップ通知

デスクトップに通知を表示する	画面右下に表示されるデスクトップ通知とバルーンヒントの表示を ON/OFF します。
全画面モードでのアプリケーションの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。
デスクトップ通知の表示時間	表示時間を 3 ～ 30 秒で設定できます。既定値は以下のとおりです。 デスクトップ通知の表示時間（秒）：10 秒 デスクトップ通知の透明度（%）：20% 表示するイベントの最低詳細レベル：情報 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：Administrator
デスクトップ通知の透明度　通知	エリアの表示の透明度を 0 ～ 80% で設定します（0 の場合は透過しません）。 既定値は以下のとおりです。 デスクトップ通知の表示時間（秒）：10 秒 デスクトップ通知の透明度（%）：20% 表示するイベントの最低詳細レベル：情報 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：Administrator
表示するイベントの最低詳細レベル	最低レベルを、診断、情報、警告、エラー、重大から選択します（次ページ参照）。
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	OS がマルチユーザーの設定の場合、どのユーザーに通知を表示するかを指定します。

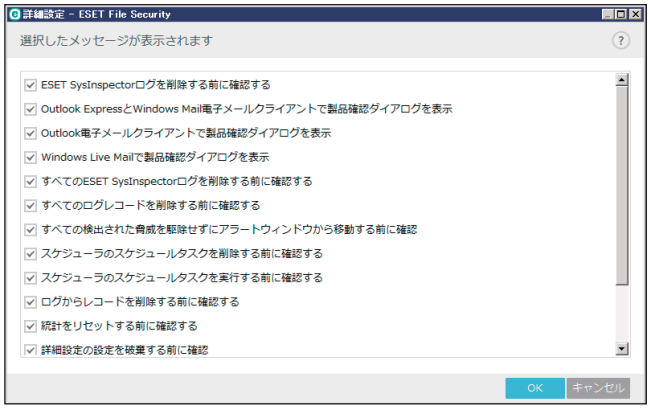
「表示するイベントの最低詳細レベル」ドロップダウンメニューからは、警告および通知を表示するレベルを選択できます。

診断	プログラムおよび上記のすべてのレコードを微調整する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」といった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。

メッセージボックス

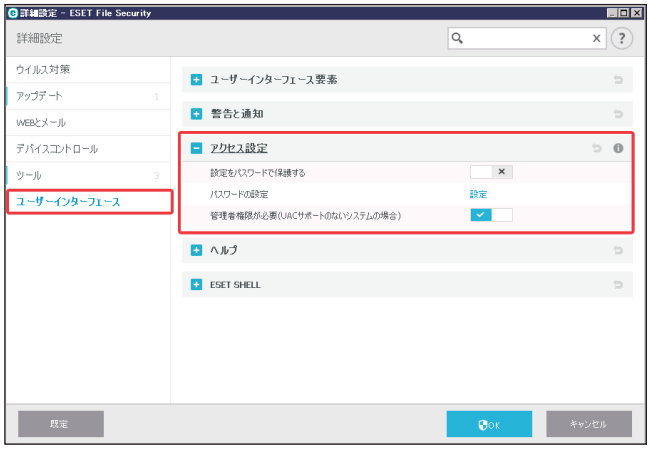
メッセージボックスは指定した時間が経過すると、自動的に閉じるように設定することができます。この機能を有効にするには、「メッセージボックスを自動的に閉じる」のチェックボックスをオンにします。メッセージボックスのポップアップが自動的に閉じる時間 10 ～ 999 秒で指定できます。

［確認メッセージ］の［編集］をクリックすると、表示できる確認メッセージを選択することができます。



■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。

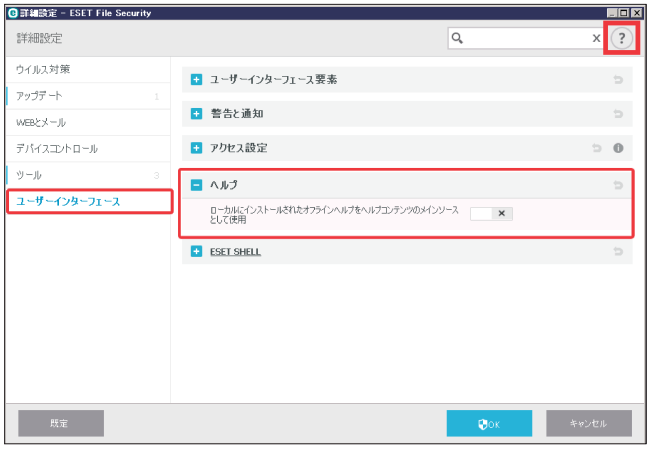
設定をパスワードで保護する	ESET File Security for Microsoft Windows Server の設定パラメーターをパスワードで保護します。「アイコン（無効）」をクリックすると、「パスワードの設定」画面が表示されるので、新しいパスワードと確認用のパスワードを入力し、［OK］をクリックします。保護を解除する場合は、「アイコン（有効）」をクリックし、設定されているパスワードを入力して［OK］をクリックします。
パスワードの設定	［設定］リンクをクリックすると、パスワードを変更できます。
制限された管理者アカウントの場合、完全な管理者権限が必要	有効にすると、管理者権限が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。

■ヘルプ

【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。

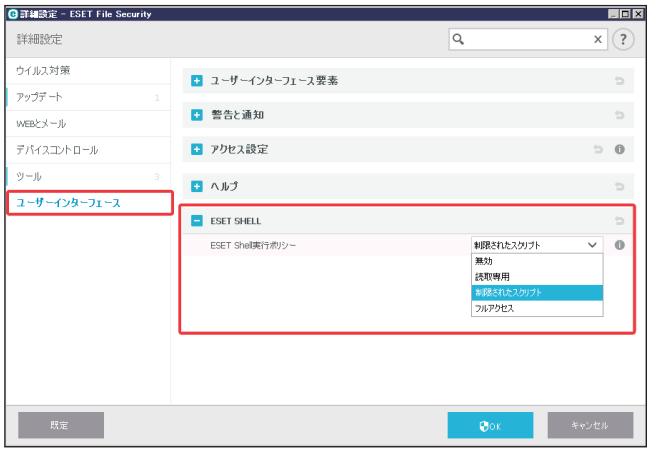
インターネットに接続している場合には、最新バージョンのオンラインヘルプが自動的に表示されます。

「詳細設定」画面の［ユーザーインターフェース］＞［ヘルプ］の「ローカルにインストールされたオフラインヘルプをヘルプコンテンツのメインソースとして使用」のチェックボックスをオンにすると、オフラインヘルプがメインソースとして使用されます。



■ 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。

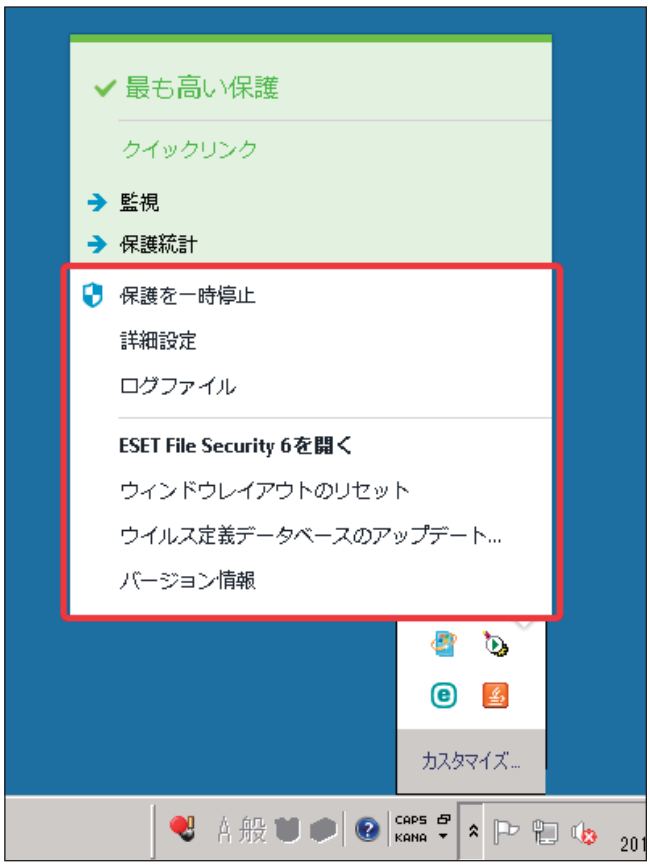
```
set ui ui gui-start-mode full
set ui ui gui-start-mode terminal
```

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。

5.2 その他の設定操作

5.2.1 システムトレイアイコンでの設定

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。

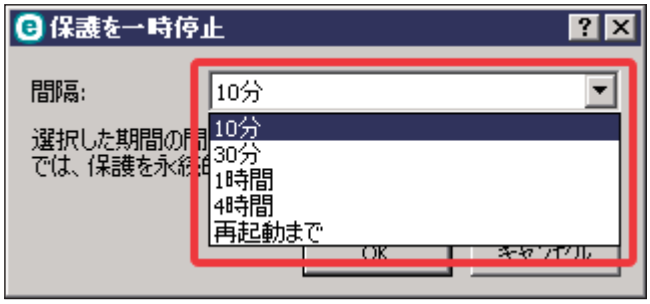


メニューには次の項目が表示されます。

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 6 を開く	ESET File Security for Microsoft Windows Server を開きます。
ESET File Security 6 を非表示	表示されている ESET File Security for Microsoft Windows Server の画面を非表示にします。
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。
ウイルス定義データベースのアップデート	ウイルス定義データベース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

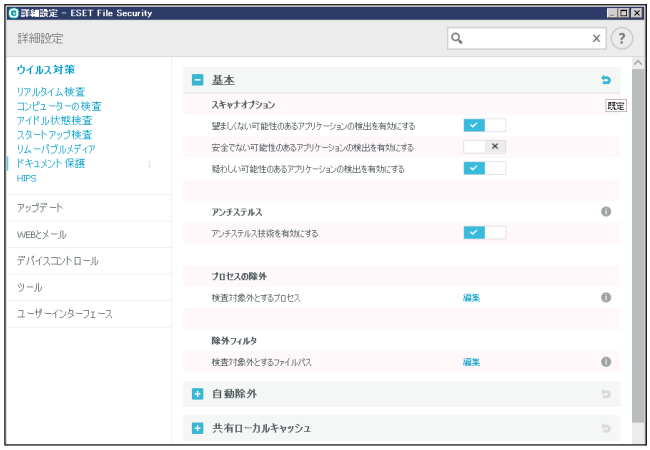
システムトレイアイコンを使用して、ウイルス対策とスパイウェア対策を一時的に無効にすると、「保護を一時停止」画面が表示されます。ここで選択した期間（間隔）の間、ウイルス対策とスパイウェア対策の保護を無効にします（保護を永続的に無効にするには、詳細設定から行います）。保護を無効にすると、システムが脅威にさらされる可能性があります。無効にする際は十分注意してください。

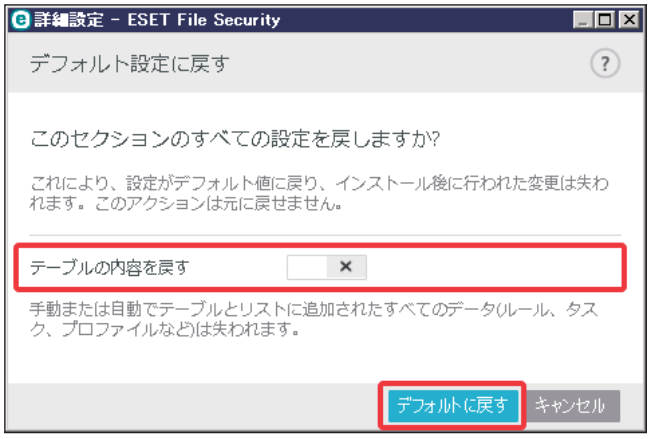


「間隔」ドロップダウンメニューから、すべてのウイルス・スパイウェア対策保護機能を無効にする期間を設定します。

5.2.2 設定を元に戻す

各設定項目の右端にある↩をクリックすると、「デフォルト設定に戻す」画面が表示されます。［デフォルトに戻す］をクリックすると、既定の設定に戻すことができます。





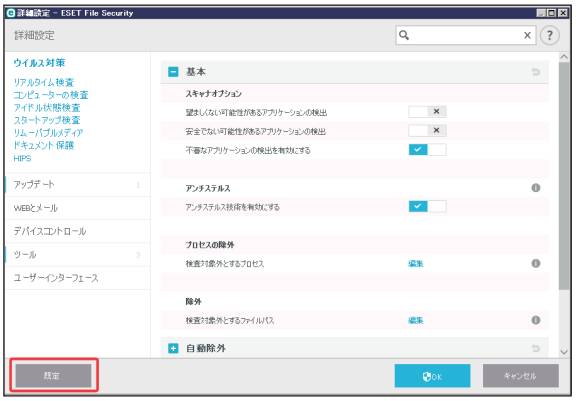
［テーブルの内容を戻す］を有効にすると、手動または自動で追加されたルール、タスク、プロファイルが失われ、デフォルトの設定に戻ります。

5.2.3 デフォルト設定に戻す

ESET File Security for Microsoft Windows Server のすべてのモジュール、プログラム設定が新規インストール時の状態にリセットされます。

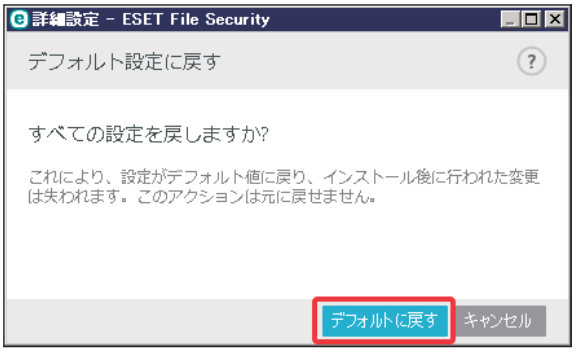
操作手順

1. 「詳細設定」画面下部の［既定］ボタンをクリックします。



2. ［デフォルトに戻す］をクリックします。

手動、自動で追加されたルール、タスク、プロファイルが失われてデフォルトの設定に戻ります。

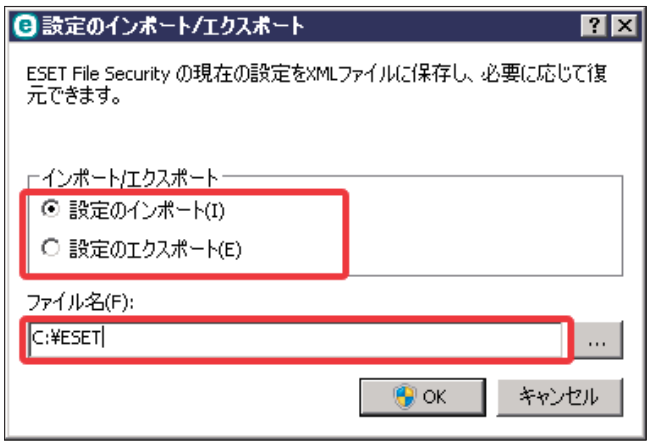


5.2.4 設定のインポート／エクスポート

設定内容のインポートとエクスポートは、メインメニューの［設定］＞［設定のインポート／エクスポート］をクリックします。

［設定のインポート］または［設定のエクスポート］を選択し、「ファイル名」フィールドに保存するファイル名とディレクトリーを指定して［OK］をクリックします。インポートとエクスポートには、いずれも XML ファイル形式が使用されます。

ESET File Security for Microsoft Windows Server の現在の構成をバックアップする必要がある場合は、この機能を使用します。後から他のコンピューターにインポートをして同じ設定を適用することができます。



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 ウイルス

コンピューターウイルスとは、コンピューター上の既存のファイルにあらかじめ追加されている、または後から追加される悪意のあるコードのことです。ウイルスは生物学上のウイルスにちなんで名付けられました。生物学上のウイルスと同じような手法でコンピューター間に蔓延していくからです。「ウイルス」という用語は、あらゆる種類のマルウェアを意味するかのように誤って使用されることがよくあります。この用法は徐々に敬遠されるようになり、より正確な用語である「マルウェア」（悪意のあるソフトウェア）へと次第に言い換えられるようになっています。

コンピューターウイルスは、主に実行可能ファイルとドキュメントを攻撃します。コンピューターウイルスに感染すると、元のアプリケーションよりも前に悪意のあるコードが呼び出されて実行されます。ウイルスは、ユーザーが書き込み権限を持つすべてのファイルに感染することができます。

コンピューターウイルスの目的と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 圧縮プログラム

圧縮プログラムは、複数のマルウェアを 1 つのパッケージにロールアップするランタイム自己解凍実行可能ファイルです。

最も一般的な圧縮プログラムには、UPX、PE_Compact、PKLite、ASPack があります。別の圧縮プログラムを使用して圧縮した場合、同じマルウェアが異なって検出されることがあります。圧縮プログラムには、シグネチャーを時間の経過と共に変化させ、マルウェアの検出と削除を困難にする機能もあります。

6.1.8 潜在的に危険性の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 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。

6.1.9 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

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 Live Grid 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 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。