ESET File Security for Microsoft Windows Server

ユーザーズマニュアル

目次

Chapter 5
用語集
P.237

■本書について

○本書は、ESETセキュリティ ソフトウェア シリーズ ライセンス製品の共通ガイドとしてまとめています。

○文中に設けているアイコンは、該当するプログラムを示しています。「ESET Endpoint Security」はSアイコン、「ESET Endpoint アンチウイルス」はAアイコン、「ESET File Security for Microsoft Windows Server」はFSアイコン、「ESET NOD32アンチウイルス」はNMアイコンです。

■お断り

○本書は、本書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搭載されている機能が異なっている場合があります。また本書の内容は、改訂などにより予告なく変更することがあります。

[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。さまざま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、次のような主要機能があります。

- ●自動除外—動作を円滑にするために、重要なサーバファイルを自動的に検出して除外します。
- ●eShell（コマンドラインインタフェース）—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新しいコマンドラインインタフェースです。
- ●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を作成するESET SysRescueという高性能な内蔵ツールを使用して、さまざまな問題を解決します。

ESET File Security for Microsoft Windows Serverでは、スタンドアロンのMicrosoft Windows Server 2000、2003、および2008をサポートしています。ESET Remote Administratorを利用して、大規模ネットワークでESET File Security for Microsoft Windows Serverをリモートから管理できます。

1.2 保護の種類

ESET File Security for Microsoft Windows Server製品は、ウイルス・スパイウェア対策機能を有しています。この保護機能は、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、悪意のあるシステム攻撃から保護します。悪意のあるコードを含むウイルスが検出されると、ウイルス対策機能およびスパイウェア対策機能がまずブロックし、次に駆除、削除、または移動して隔離することにより、ウイルスを排除できます。

1.3 ユーザーインターフェース

ESET File Security for Microsoft Windows Serverには、グラフィカルユーザーインターフェイス(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キーを押してプログラムの任意の場所からアクセスできる詳細設定ツリーもあります。

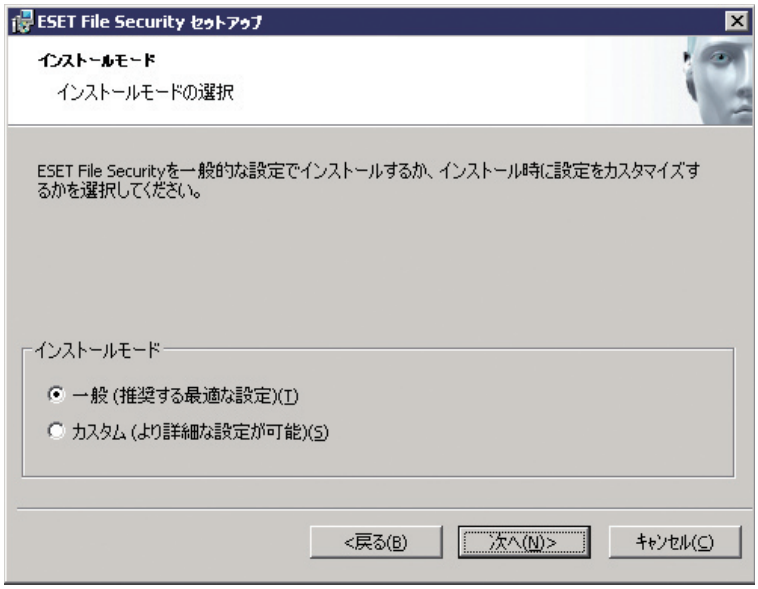
F5を押すと、詳細設定ツリーウィンドウが開き、設定可能なプログラム機能のリストが表示されます。各自のニーズにあった設定とオプションを、このウィンドウから指定できます。ツリー構造は [サーバ保護] や [コンピュータの保護] など、いくつかのセクションに分かれています。[サーバ保護] セクションでは、サーバのオペレーティングシステムとシステムファイル特有の自動除外のための設定が含まれています。[コンピュータの保護] セクションには、サーバ自体を保護するために設定可能な多くの項目が含まれています。

[Chapter 2]
インストール

2.1 インストールについて

ESET File Security for Microsoft Windows Serverのインストーラーを起動すると、インストールウィザードが表示されるので、その案内に従って基本 設定を行ってください。インストールには以下の2種類があります。

1.一般インストール
2.カスタムインストール



NOTE

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よう強くお勧めします。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。

2.2 一般インストール

一般インストールモードのインストールプロセスでは、最小設定のESET File Security for Microsoft Windows Serverが高速でインストールされます。一般インストールは既定のインストールモードであり、固有の設定に対して特定の要件を必要としない場合に推奨します。

インストールモードを選択して [次へ] をクリックすると、ユーザー名とパスワードを入力するよう求められます。ユーザー名およびパスワードを指定することによって、ウイルス定義データベースの自動アップデートが可能になるため、この入力は、システムを保護する上で重要な役割を果たします。

製品の購入後または登録後に受け取ったユーザー名およびパスワードを、対応するフィールドに入力します。使用可能なユーザー名とパスワードを現在お持ちでない場合は、製品をインストール後にプログラムから直接入力できます。

次のステップでは、ThreatSense.Net早期警告システムを設定します。ThreatSense.Net早期警告システムによって、ESETは新しいマルウェアを迅速かつ継続的に把握し、お客様をすばやく保護することができます。早期警告システムによってESETのウイルスラボに新しい脅威を提出できます。ウイルスラボで、これらが解析および処理され、ウイルス定義ファイルに追加されます。既定では、[ThreatSense. Net早期警告システムを有効にする] オプションが選択されています。疑わしいファイルの提出に関する詳細設定を変更するには、[詳細設定...] をクリックします。

インストールプロセスの次のステップでは、[望ましくない可能性があるアプリケーションの検出] を設定します。潜在的に望ましくない可能性があるアプリケーションは、必ずしも悪意があるとは限りませんが、オペレーティングシステムの動作に悪影響を及ぼす可能性があります。

これらのアプリケーションは、その他のプログラムに同梱されていることが多く、インストールプロセス時に気がつきにくいことがあります。これらのアプリケーションはインストール時に通知を表示しますが、同意なしにインストールできるので、ユーザーが安易にインストールしてしまうこともあります。

ESET File Security for Microsoft Windows Serverでこのような脅威を検出できるようにする（推奨）には、[望ましくない可能性があるアプリケーショ ンの検出を有効にする]オプションを選択します。この機能を使用しない場合は、[望ましくない可能性があるアプリケ
ーションの検出を無効にする] を選択します。標準インストールモードの最後のステップでは、[インストール] ボタンをクリックしてインストールを確認します。

▸▸▸ NOTE

詳細なインストール手順については、「ユーザーズガイド 基本インストール編」をご参照ください。

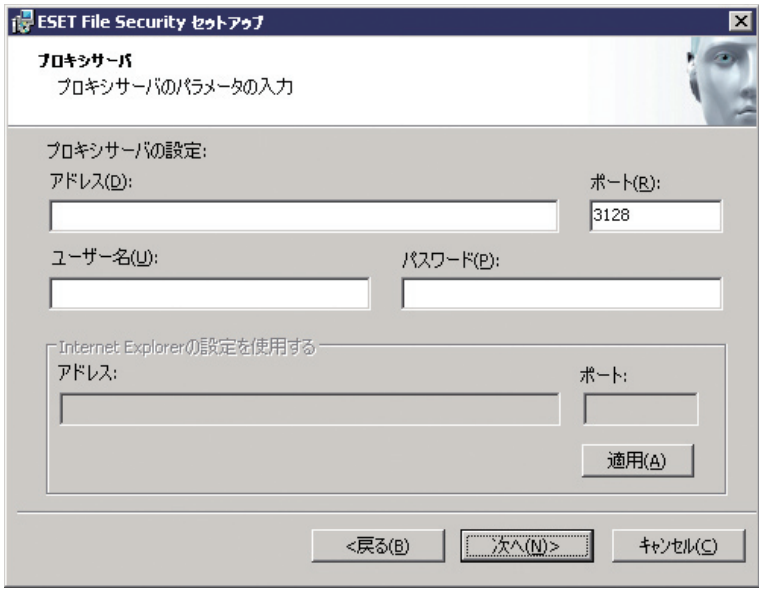
2.3 カスタムインストール

カスタムインストールは、インストールプロセスでESET File Security for Microsoft Windows Serverを設定するユーザー向けです。インストールモードを選択して [次へ] をクリックすると、インストール先の場所を選択するよう求められます。既定では、
C:\Program Files\ESET\ESET File Securityにインストールされます。場所を変更するには、[参照...] をクリックします (既定のインストール場所を利用することをお勧めします)。

次に、[ユーザー名] および [パスワード] を入力します。このステップは、一般インストールと同じです。

ユーザー名およびパスワードを入力し、[次へ] をクリックして [インターネット接続の設定] の設定に進みます。

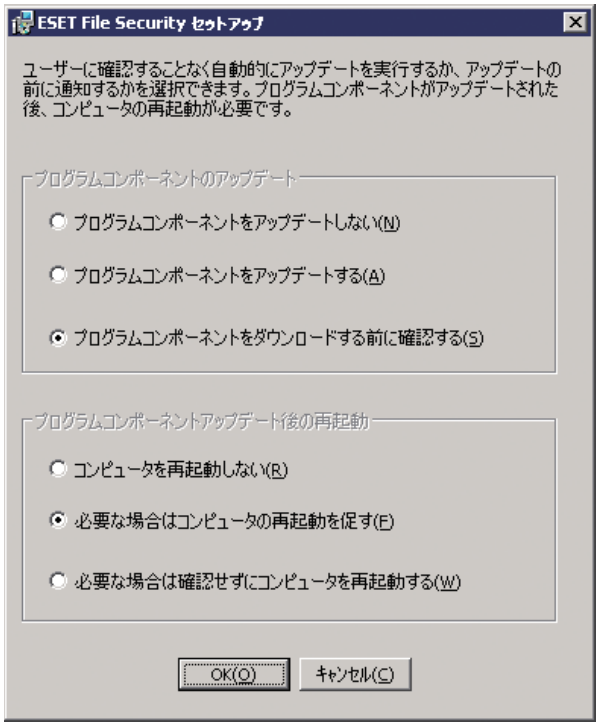
プロキシサーバーを使用してWebアクセスしている環境では、ウイルス定義データベースのアップデートが正しく動作するように適切に設定する必要があります。プロキシサーバーを自動的に設定させるには、既定の [インターネット接続でプロキシサーバを使用しているかどうか不明。Internet Explorerと同じ設定を使用する (推奨)] を選択し、[次へ] をクリックします。プロキシサーバーを使用しない場合は、[プロキシサーバを使用しない] オプションを選択します。



プロキシサーバの詳細を入力したい場合は、プロキシサーバの設定を手動で設定できます。プロキシサーバの設定を行うには、[プロキシサーバを使用する] を選択し、[次へ] をクリックします。[アドレス] フィールドにプロキシサーバーのIPアドレスまたはURLを入力します。[ポート] フィールドには、プロキシサーバーが接続を受け付けるポートを指定します (既定では3128です)。プロキシサーバーで認証が要求される場合は、有効な [ユーザー名] と [パスワード] を入力して、プロキシサーバーへのアクセスを可能にする必要があります。必要に応じて、Internet Explorerからプロキシサーバの設定をコピーすることもできます。プロキシサーバの詳細を入力し終えた場合は、[適用] をクリックし、選択内容を確認します。

[次へ] をクリックして、[自動アップデートの設定] に進みます。このステップでは、システムで自動的なプログラムコンポーネントのアップデート (PCU) を処理する方法を指定できます。詳細設定にアクセスするには、[変更...] をクリックします。

プログラムコンポーネントをアップデートしない場合は、[プログラムコンポーネントをアップデートしない] を選択します。[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] オプションを選択すると、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ウィンドウが表示されます。プログラムコンポーネントの更新ファイルを自動的にダウンロードするには、[プログラムコンポーネントをアップデートする] オプションをオンにします。



NOTE

通常、プログラムコンポーネントのアップデート後の再起動は、[コンピュータを再起動しない] オプションを選択することをお勧めします。最新のコンポーネントのアップデートは、スケジュールによるか、手動によるか、その他によるかを問わず、サーバを次回再起動すると有効になります。[必要な場合はコンピュータの再起動を促す] を選択すると、コンポーネントのアップデート後にサーバを再起動するよう通知させることができます。この設定では、サーバをすぐに再起動することも、再起動を延期して後で行うこともできます。
通常は[コンピュータを再起動しない] に設定しておくことをお勧めします。

次のインストールウィンドウには、プログラム設定を保護するためのパスワードを設定するオプションがあります。[環境設定をパスワードで保護する] オプションを選択し、[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] フィールドに入力するパスワードを選びます。

次の2つのインストールステップ、具体的には [ThreatSense.Net早期警告システム] および [望ましくない可能性があるアプリケーションの検出] は、標準インストールモードのステップと同じです。

[インストールの準備ができました] ウィンドウで [インストール] をクリックしてインストールを完了します。

2.4 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、「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。

2.5 新しいバージョンへのアップグレード

ESET File Security for Microsoft Windows Serverの新しいバージョンは、機能を強化するためや、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を修正するために発行されます。新しいバージョンへのアップグレードは、複数の方法のうちのいずれかで行います。

1.新しいバージョンを手動でダウンロードし、前のインストール内容の上にインストールする。
インストールを開始するときに、[現在の設定を使用] チェックボックスをオンにして、現在のプログラム設定を保持することを選択できます。

2.ネットワーク環境でESET Remote Administratorによる自動展開を使用してアップグレードする。

2.6 コンピュータの検査

ESET File Security for Microsoft Windows Serverのインストール後は、悪意のあるコードを見つけるためにコンピューターの検査を実行する必要があります。そのために、メインプログラムウインドウから［コンピュータの検査］をクリックし、［Smart検査］をクリックします。コンピュータの検査の詳細については、「コンピュータの検査」を参照してください。

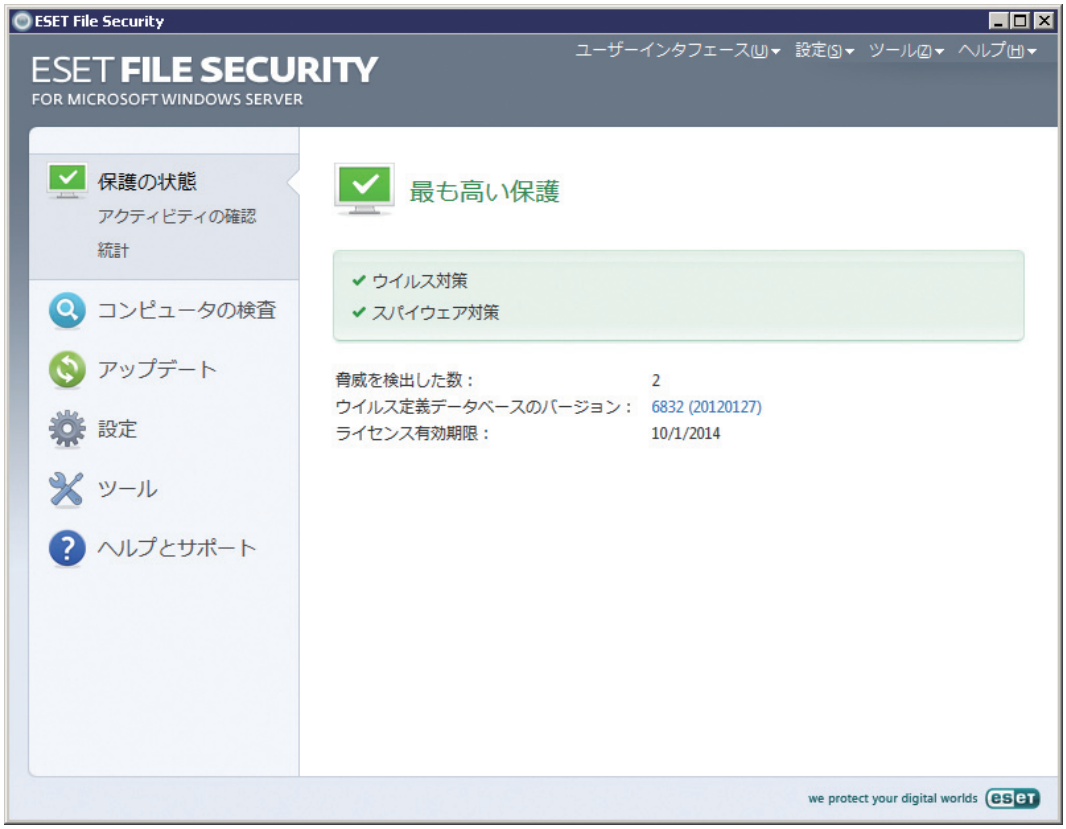
[Chapter 3]
初心者向けガイド

3.1 ユーザーインターフェースのデザインの概要

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

次に、メインメニューにあるオプションについて説明します。

保護の状態	ESET File Security for Microsoft Windows Serverの保護の状態に関する情報が表示されます。[アクティビティの確認]サブメニューと[統計]サブメニューがあります。
コンピュータの検査	このオプションを使用すると、[コンピュータの検査]の設定や検査を行うことができます。
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が表示やアップデートを行うことができます。
設定	このオプションを選択すると、コンピューターのセキュリティレベルを調整することができます。[詳細モード]を有効にすると、[ウイルス・スパイウェア対策]サブメニューが表示されます。
ツール	[ログファイル]、[隔離]、[スケジューラ]、および[SysInspector]にアクセスできます。
ヘルプとサポート	ヘルプ、ESET製品のナレッジベース、およびカスタマケアサポートを開くリンクにアクセスできます。



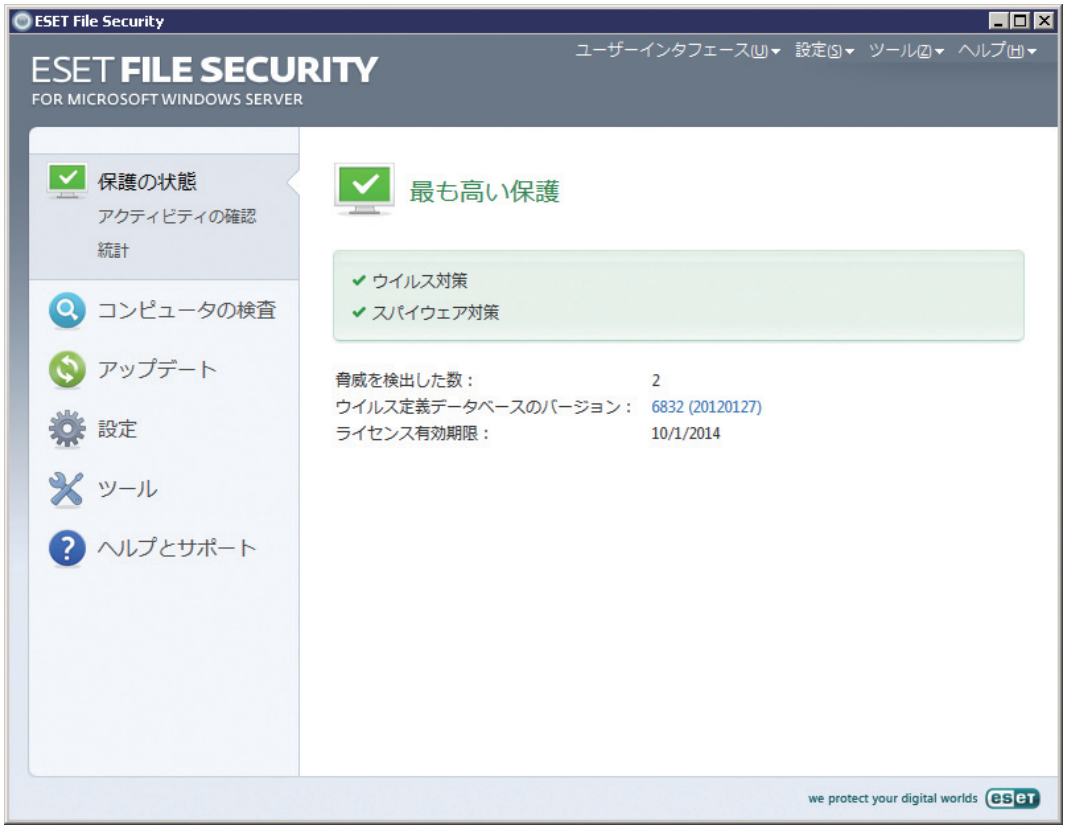
3.1.1　システムの動作の確認

[保護の状態] を表示するには、メインメニューの一番上のオプションをクリックします。プライマリウィンドウには、ESET File Security for Microsoft Windows Serverの動作状態の概要と、[アクティビティの確認] および [統計] の2つの項目を持つサブメニューが表示されます。このいずれを選択しても、システムの詳細情報が表示されます。

完全に機能する状態でESET File Security for Microsoft Windows Serverが稼動している場合、[保護の状態] は緑色で表示されます。そうでない場合は、オレンジ色または赤になり、注意が必要であることを示します。

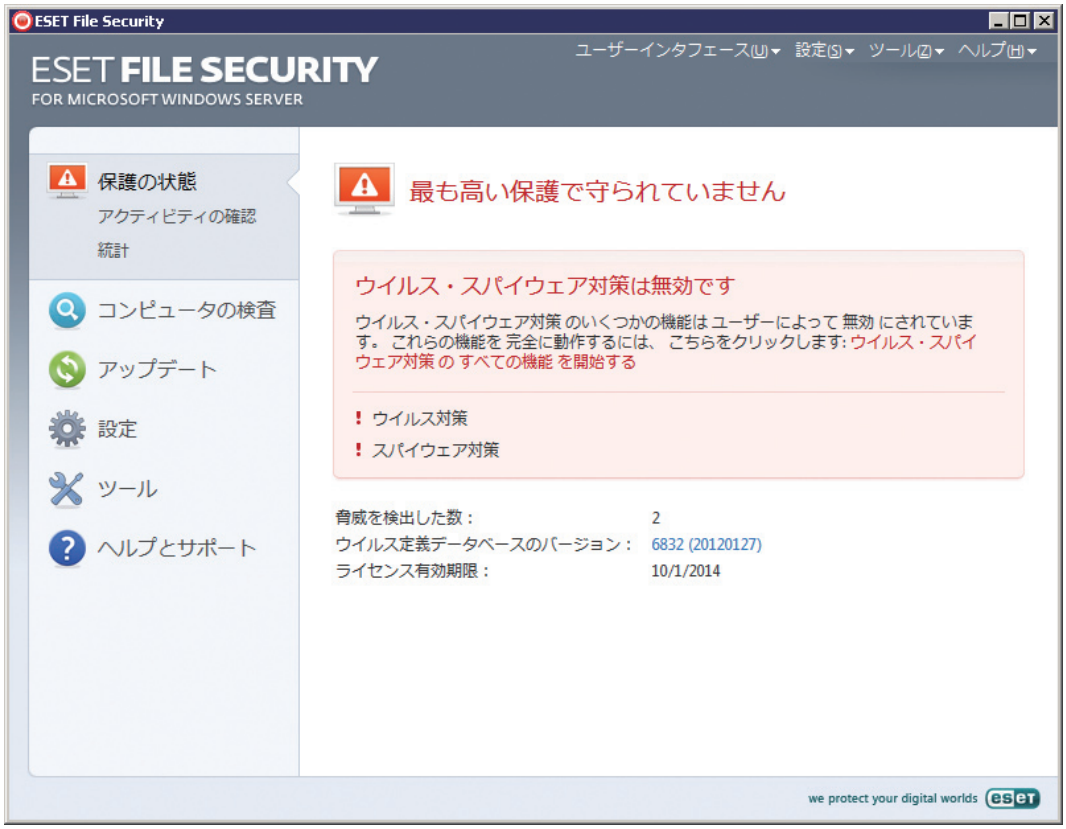
[アクティビティの確認] サブメニュー項目をクリックすると、リアルタイム（横軸）グラフの形でファイルシステムの現在のアクティビティを監視できます。縦軸は、読み取りデータ（青線）と書き込みデータ（赤線）の量を表します。

[統計] サブメニューでは、感染したオブジェクト、駆除済みオブジェクト、および無感染オブジェクの数を確認できます。ドロップダウンリストにあるたくさんのモジュールから選択できます。



3.1.2 プログラムが正しく動作しない場合の解決方法

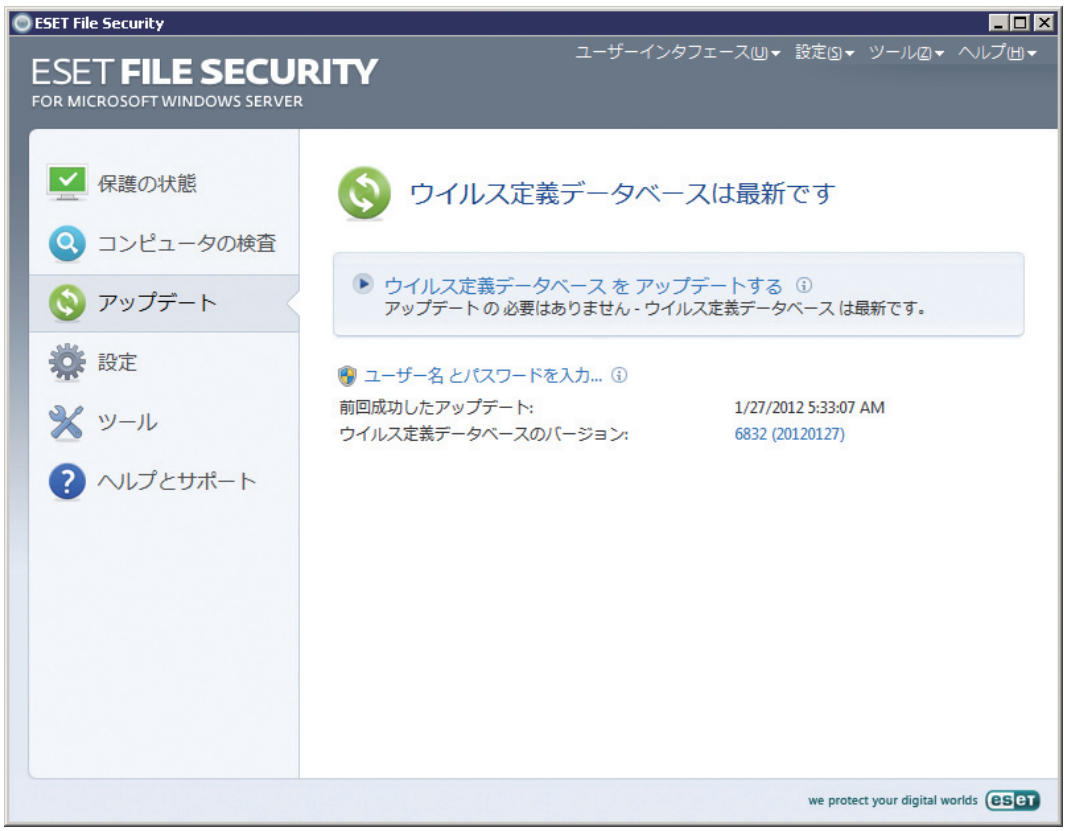
モジュールが正しく動作している場合は、緑のチェックマークが表示されます。正しく動作していない場合は、エクスクラメーションマークまたはオレンジの通知アイコンが表示され、モジュールに関する詳細情報や、推奨される解決策も表示されます。各モジュールのステータスを変更するには、メインメニューの [設定] をクリックし、必要なモジュールをクリックします。



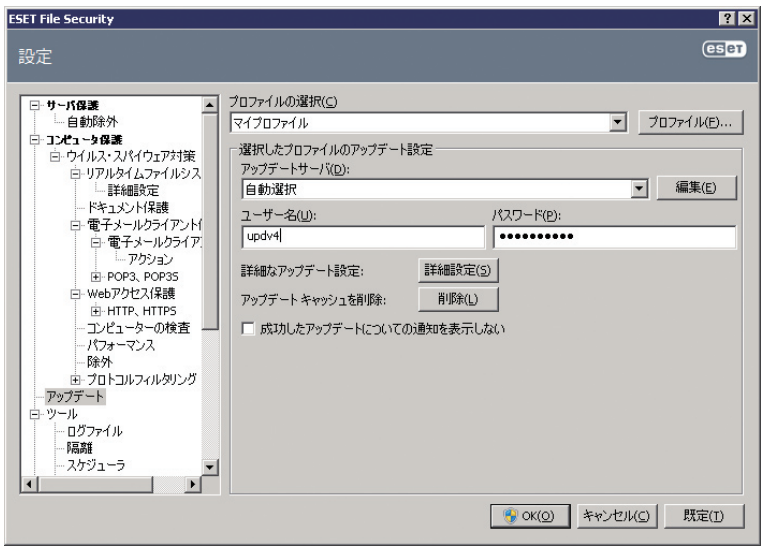
3.2 アップデートの設定

悪意のあるコードからの保護を完璧なものにするには、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が必要不可欠です。メインメニューの [アップデート] を選択し、プライマリウィンドウの [ウイルス定義ファイルをアップデートする] をクリックして、データベースの新しいアップデートを確認します。[ユーザー名とパスワードの設定...] をクリックすると表示されるダイアログボックスに、購入時に受け取ったユーザー名とパスワードを入力する必要があります。

ESET File Security for Microsoft Windows Serverをインストールするときにユーザー名とパスワードを入力した場合、ここでは入力を求められません。

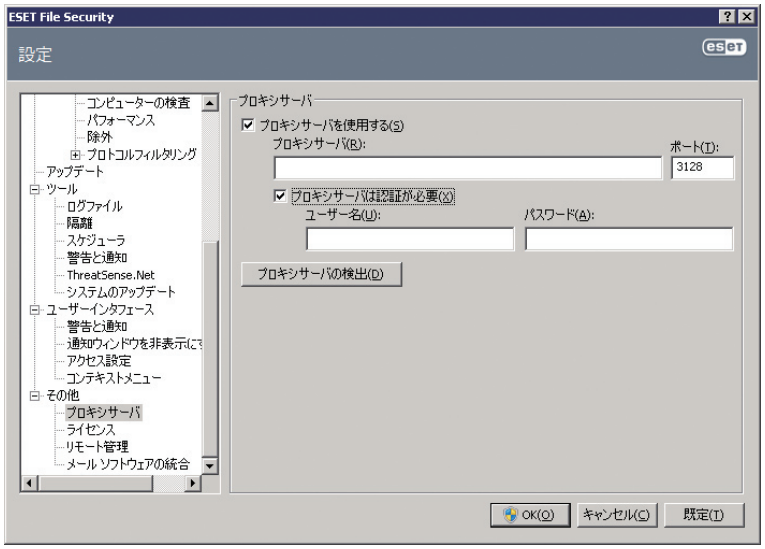


メインメニューの [設定] をクリックしてから [環境設定で詳細な設定をする...] をクリックするかまたはF5を押すと表示される [詳細設定] ウィンドウには、追加のアップデートオプションがあります。[詳細設定] ツリーで [アップデート] をクリックします。[アップデートサーバ] ドロップダウンメニューには、[自動選択] が設定されています。テストモード、プロキシサーバへのアクセス、LAN接続、ウイルス定義のコピーの作成など、詳細な更新オプションを設定するには、[詳細設定] ボタンをクリックします。


ESET File Security
設定
eset
サーバ保護
自動除外
コンピュータ保護
ウイルス・スパイウェア対策
リアルタイムファイルシス
詳細設定
ドキュメント保護
電子メールクライアント
電子メールクライア
アクション
POP3、POP3S
Webアクセス保護
HTTP、HTTPS
コンピューターの検査
パフォーマンス
除外
プロトコルフィルタリング
アップデート
ツール
ログファイル
隔離
スケジューラ
プロファイルの選択(C)
マイプロファイル
プロファイル(E)...
選択したプロファイルのアップデート設定
アップデートサーバ(D):
自動選択
編集(E)
ユーザー名(U):
updv4
パスワード(P):
詳細なアップデート設定:
詳細設定(S)
アップデート キャッシュを削除:
削除(L)
成功したアップデートについての通知を表示しない
OK(O)
キャンセル(C)
既定(T)

3.3 プロキシサーバーの設定

インターネット接続を管理するためにプロキシサーバを使用しているシステムでESET File Security for Microsoft Windows Serverを使用する場合は、[詳細設定]でプロキシサーバを指定する必要があります。[プロキシサーバの設定]ウィンドウにアクセスするには、F5を押して [詳細設定] ウィンドウを開き、[詳細設定] ツリーから [その他] > [プロキシサーバ] をクリックします。[プロキシサーバを使用する] オプションを選択し、[プロキシサーバ] (IPアドレス) フィールドと [ポート] フィールドに入力します。必要に応じて [プロキシサーバで認証を要求する] オプションを選択し、[ユーザー名] および [パスワード] を入力します。



この情報が手元にない場合でも、[プロキシサーバの検出] ボタンをクリックすることで、プロキシサーバの設定の自動検出できる場合があります。

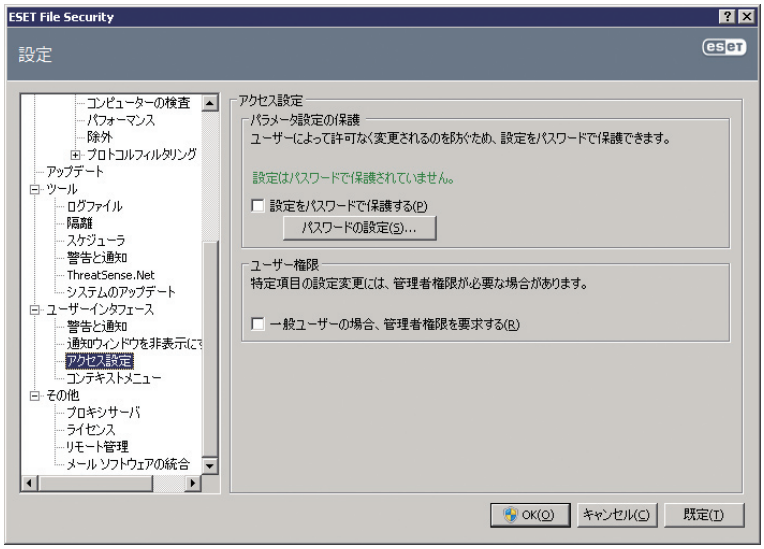
NOTE

アップデートプロファイルごとにプロキシサーバのオプションが異なる場合があります。その場合は、[詳細設定] ツリーの[アップデート] をクリックして、プロキシサーバを設定してください。

3.4 設定の保護

ESET File Security for Microsoft Windows Serverの設定は社内のセキュリティポリシーの観点から非常に重要な場合があります。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、メインメニューで [設定] > [環境設定で詳細な設定をする...] > [ユーザーインターフェイス] > [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て、[パスワードの設定...] ボタンをクリックします。

[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]
ESET File Security for Microsoft Windows Server の操作

[Chapter 4]
ESET File Security for Microsoft Windows Server の操作

4.1 ESET File Security for Microsoft Windows Serverサーバ保護

ESET File Security for Microsoft Windows Serverのウイルス・スパイウェア対策は、リアルタイムファイルシステム保護、Webアクセス保護、および電子メールクライアント保護など重要な機能によってサーバを保護できます。ESET File Security for Microsoft Windows Serverにおける各タイプの保護については、「コンピュータの保護」のセクションを参照してください。またESET File Security for Microsoft Windows Serverには、自動除外という機能もあります。この機能は、重要なサーバアプリケーションとサーバ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。これによって、ウイルス対策ソフトウェアを実行する場合に潜在する競合のリスクが最小化されて、サーバの全体的なパフォーマンスが向上されます。

4.1.1 自動除外

サーバアプリケーションやオペレーティングシステムの開発者は、開発する大部分の製品の重要な作業ファイルおよびフォルダーをウイルス対策ソフトウェアの検査の対象外にすることを推奨しています。これはウイルス対策ソフトウェアの検査が、サーバーのパフォーマンスに悪影響を与えたり、競合を起こしたり、一部のアプリケーションをサーバーで実行できなくするおそれさえあるためです。除外機能は、ウイルス対策ソフトウェアを実行する場合に潜在する競合のリスクを最小化し、サーバの全体的なパフォーマンスを向上するために有用です。

ESET File Security for Microsoft Windows Serverは、重要なサーバアプリケーションとサーバ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。リストに追加されたサーバプロセスおよびアプリケーションは、該当するチェックボックスをチェックして有効（既定）にするか、またはチェックを外して無効にすることがで次のような効果が得られます。

1）アプリケーション/オペレーティングシステムの除外が有効になっている場合、そのアプリケーション/オペレーティングシステムのすべての重要なファイルおよびフォルダは、検査から除外するファイルのリストに追加されます（[詳細設定]
＞[コンピュータの保護]＞[ウイルス・スパイウェア対策]＞[除外]）。サーバを再起動するたびに除外の自動チェックが実行されて、リストから削除されている除外があれば、その除外が戻されます。自動除外を必ず常に適用したい場合は、この設定をお勧めします。

2）アプリケーション/オペレーティングシステムの除外を無効にしたとき、そのアプリケーション/オペレーティングシステムの重要なファイルおよびフォルダは、検査から除外されるファイルのリストに残ります（[詳細設定]＞[コンピュータの保護]＞[ウイルス・スパイウェア対策]＞[除外]）。ただし、サーバを再起動するたびに、それらのファイルおよびフォルダが自動的にチェックされて [除外] リストで更新されることはありません（上のポイント1を参照）。この設定は、経験豊富なユーザーが標準の除外の一部を削除したり変更したりする場合にお勧めします。削除された設定は、コンピューターの再起動後も維持されます。

[詳細設定]＞[コンピュータの保護]＞[ウイルス・スパイウェア対策]＞[除外] で手動で入力したユーザー定義の除外対象は、上記の設定の影響を受けません。

サーバアプリケーション/オペレーティングシステムの自動除外は、マイクロソフト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。

http://support.microsoft.com/kb/822158
http://support.microsoft.com/kb/245822
http://support.microsoft.com/kb/823166
http://technet.microsoft.com/en-us/library/bb332342%28EXCHG.80%29.aspx
http://technet.microsoft.com/en-us/library/bb332342.aspx

4.2 ESET File Security for Microsoft Windows Serverコンピュータの保護

ESET File Security for Microsoft Windows Serverには、サーバを保護するために必要な多くのツールが含まれています。ESET File Security for Microsoft Windows Serverのウイルス・スパイウェア対策は、常駐シールド（リアルタイムファイルシステム保護）、Webアクセス保護、および電子メールクライアント保護というさまざまなタイプの保護によってサーバを保護します。

4.2.1 ウイルス・スパイウェア対策

ウイルスからの保護機能は、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、悪意のあるシステム攻撃から保護します。悪意のあるコードを含むウイルスが検出されると、ウイルスからの保護モジュールがまずブロックし、次に駆除、削除、または移動して隔離することにより、ウイルスを排除できます。

4.2.1.1 リアルタイムファイルシステム保護

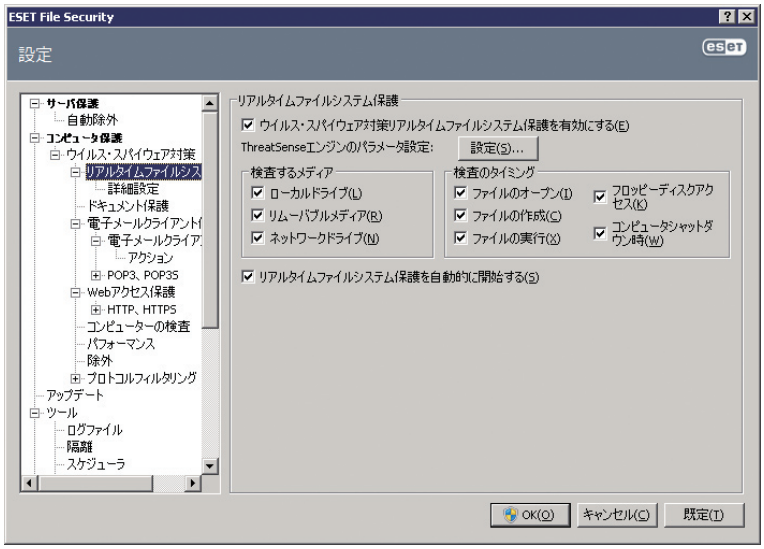
リアルタイムファイルシステム保護では、システムで発生する、様々なイベントを監視します。リアルタイムファイルシステム保護はファイルをコンピューター上で開いたり、新規作成したり、または実行したりするときに、悪意のあるコードがないかをスキャンします。リアルタイムファイルシステム保護は、システム起動時に開始されます。

検査の設定

リアルタイムファイルシステム保護では、あらゆる種類のメディアを調べます。検査はさまざまなイベントがトリガになって行われます。ThreatSenseテクノロジーの検出方法（詳細は「ThreatSenseエンジンのパラメーターの設定」のセクションを参照）を使用するリアルタイムファイルシステム保護は、新規作成ファイルと既存ファイルで動作が異なることがあります。新規作成ファイルの場合、より深いレベルの検査を適用できます。

スマート最適化オプションが有効な場合、リアルタイムファイルシステム保護使用時のシステムへの負荷を最小限にするために、検査済みのファイルは、新たなウイルス定義データベースが提供されるかファイルが変更されていない限り再検査されません。なお、オプションが無効の場合、全てのファイルがアクセスのたびに検査されます。このオプションを変更するには、[詳細設定] ウィンドウを開き、[詳細設定] ツリーで [ウイルス・スパイウェア対策] > [リアルタイムファイルシステム保護] をクリックします。次に、[ThreatSenseエンジンのパラメータ設定] の横の [設定...] ボタンをクリックし、[その他] をクリックして、[スマート最適化を有効にする] オプションを選択または選択解除します。

既定では、リアルタイムファイルシステム保護はシステム起動時に起動し、中断されることなく検査が行われます。特殊な場合（別のリアルタイムスキャナと競合する場合など）は、[リアルタイムファイルシステム保護を自動的に開始する] オプションの選択を解除すると、OSの起動時にリアルタイムファイルシステム保護は無効な状態で開始されます。



■ 検査するメディア

既定では、多く種類のメディアに対して潜在的な脅威が検査されます。

ローカルドライブ	すべてのハードドライブを検査します。
リムーバブルメディア	フロッピーディスク、USB記憶装置など。
ネットワークドライブ	すべてのマップドライブを検査します。

既定の設定を変更するのは、あるメディアの検査によりデータ転送が極端に遅くなるときなど、特別な場合だけにすることをお勧めします。

■ 検査のタイミング（イベント発生時の検査）

既定では、すべてのファイルに対して、開いたり、実行したり、作成したりするときに、ファイルの検査が行われます。既定の設定によりコンピューターが最大限のレベルでリアルタイムに保護されるので、既定の設定は変更しないことをお勧めします。

[フロッピーディスクアクセス] オプションでは、フロッピードライブへのアクセス時に、フロッピーのブートセクタが検査されます。[コンピュータのシャットダウン] オプションでは、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が検査されます。現在ではブートウイルスはほとんどありませんが、別のソースからブートウイルスに感染する可能性が依然としてあるため、これらのオプションは有効にしたままにしておくことをお勧めします。

■ 詳細検査オプション

詳細な設定オプションが、[コンピュータの保護] > [ウイルス・スパイウェア対策] > [リアルタイムファイルシステム保護] > [詳細設定] にあります。

新規作成または変更されたファイルに適用する追加のThreatSenseパラメータ-新しく作成されたファイルや変更されたファイルは、既存のファイルに比べて感染の可能性が高いといえます。そのため、それらのファイルは、検査パラメータが追加されて検査されます。通常のウイルス定義ベースの検査方法に加えて、アドバンスドヒューリスティックが使用されます。その結果、検出率が大幅に向上します。新規作成されたファイルに加え、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、実際のサイズにかかわらず検査されます。アーカイブ検査設定を変更するには、[既定のアーカイブ検査設定] オプションの選択を解除します。

実行したファイルに適用する追加のThreatSenseパラメータ-既定では、ファイルが実行されている場合、アドバンスドヒューリスティックは使用されません。一方、このオプションを有効にしたい場合は [ファイル実行時のアドバンスドヒューリスティック] オプションをチェックします。アドバンスドヒューリスティックを使用するには高度なシステム要件が必要なため、一部のプログラムの実行速度が低下する場合があります。

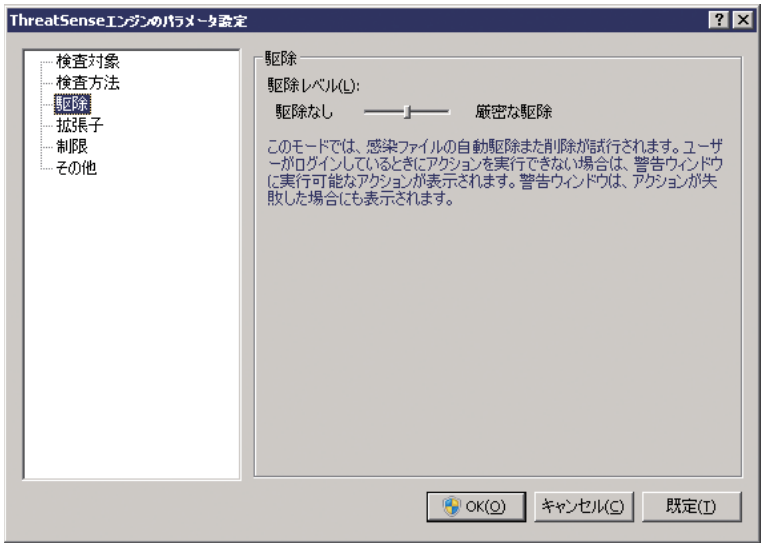
駆除レベル

リアルタイムファイルシステム保護機能には、3つの駆除レベルがあります。駆除レベルを選択するには、[リアルタイムファイルシステム保護] セクションの [設定...] ボタンをクリックしてから、[駆除] をクリックします。

●第1レベルの [駆除なし] では、検出された各侵入に適用できる各種オプションがある警告ウィンドウが表示されます。各侵入に関してアクションを個別に選択する必要があります。このレベルは、侵入が発生したときに実行する必要のあるステップを理解している経験豊富なユーザー向けです。

●第2レベルでは、あらかじめ指定されたアクションが自動的に適用、実行されます（侵入の種類に応じて異なります）。感染しているファイルの検出と削除は、画面右下のメッセージにより通知されます。感染していないファイルも格納しているアーカイブ内でマルウェアが見つかった場合や、感染している対象に対してあらかじめアクションが指定されていない場合は、自動的には処理されません。

●第3レベルの［厳密な駆除］では、感染している対象はすべて、マルウェアが駆除されます。このレベルでは正常なファイルまで失われてしまう可能性があるので、限られた状況でのみ使用することをお勧めします。



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、安全なシステムを維持するために最も必要不可欠な要素です。そのため、パラメータを変更する際には注意が必要です。特定の状況に限ってパラメータを変更することをお勧めします。たとえば、特定のアプリケーションや別のウイルス対策プログラムのリアルタイムスキャナとの競合がある場合などです。

ESET File Security for Microsoft Windows Serverのインストール後は、最大レベルのシステムセキュリティをユーザーに提供するように全ての設定が最適化されています。既定の設定に戻すには、［リアルタイムファイルシステム保護］ウィンドウ（［詳細設定］>［ウイルス・スパイウェア対策］>［リアルタイムファイルシステム保護］）の右下にある［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る（ウイルスを検出することができる）ことを確認するため、eicar.comのテストファイルを使用します。このテストファイルは、あらゆるウイルス対策プログラムが検出できる特殊な無害のファイルです。このファイルは、EICAR（European Institute for Computer Antivirus Research）が、ウイルス対策プログラムの機能をテストする目的で作成しました。ファイルeicar.comは、http://www.eicar.org/download/eicar.comからダウンロードできます。

▸▸▸ NOTE

リアルタイムファイルシステム保護の確認を実行する前に、Webアクセス保護を無効にする必要があります。Webアクセス保護が有効ままでは、Webアクセス保護にてファイルを検出してしまい、テストファイルをダウンロードすることができません。

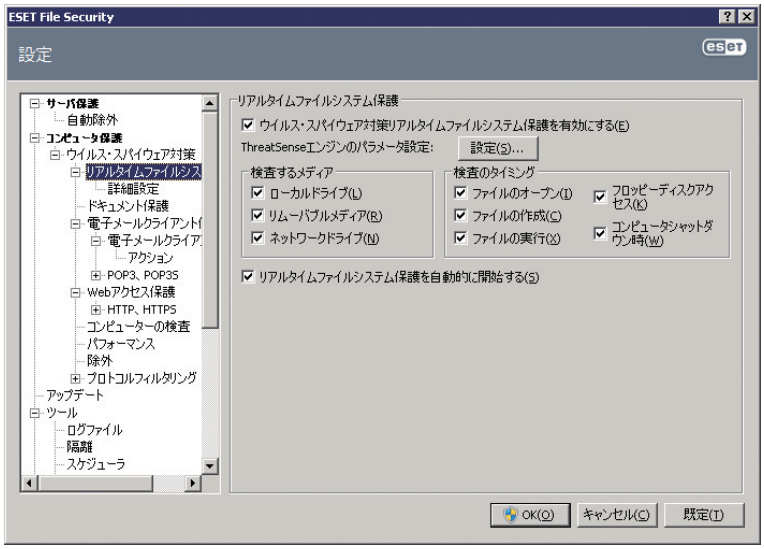
リアルタイムファイルシステム保護が機能しない場合の解決方法

次の章では、リアルタイムファイルシステ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。

リアルタイムファイルシステム保護が無効である

ユーザーが不注意にリアルタイムファイルシステム保護を無効にしてしまった場合、再開する必要があります。リアルタイムファイルシステム保護を再開するには、[設定] > [ウイルス·スパイウェア対策] に移動し、メインプログラムウィンドウの [リアルタイムファイルシステム保護] セクションの [ウイルス·スパイウェア対策リアルタイムファイルシステム保護を有効にする] のチェックボックスを選択します。

システム起動時にリアルタイムファイルシステム保護が開始されなかった場合、原因はおそらく [リアルタイムファイルシステム保護を自動的に開始する] オプションが無効にされていたためと考えられます。このオプションを有効にするには、[詳細設定] (F5) に移動し、[詳細設定] ツリーにある [リアルタイムファイルシステム保護] をクリックします。ウィンドウの下部にある [詳細設定] セクションで [リアルタイムファイルシステム保護を自動的に開始する] チェックボックスが選択されていることを確認します。



リアルタイムファイルシステム保護がマルウェアの検出と駆除を行わない場合

コンピュータ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ことを確認します。2つのリアルタイム保護シールド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。システムから他のウイルス対策プログラムをアンインストールすることをお勧めします。

リアルタイムファイルシステ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する] オプション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、他のプログラムとの競合が原因であることがあります。

4.2.1.2 電子メールクライアント保護

電子メールの保護では、POP3プロトコルで受信したメール通信が検査されます。

受信メッセージを検査するときには、ThreatSenseスキャンエンジンに用意されている詳細なスキャン方法が全て使用されます。そのため、アーカイブ（圧縮ファイル）の一部に、悪意のあるプログラムが含まれていても検出が可能です。POP3プロトコル通信のスキャンは、使用されるメールクライアントからは独立して動作しています。

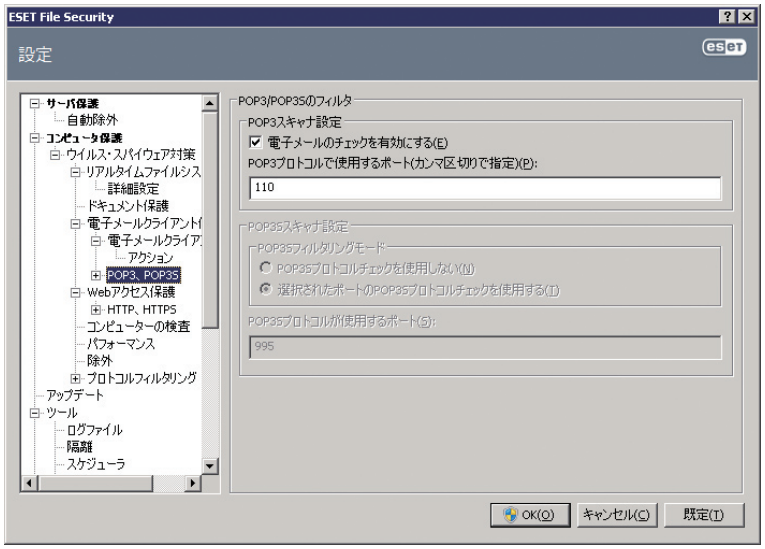
POP3検査

POP3プロトコルは、メールクライアントアプリケーションでのメール通信の受信に最もよく使用されているプロトコルです。ESET File Security for Microsoft Windows Serverでは、使用しているメールクライアントに関係なく、このプロトコルを保護できます。

この検査を行う保護機能は、システムの起動時に自動的に起動されます。この機能が正常に動作するように、有効になっていることを確認してください。POP3検査は、メールクライアントを設定し直さなくても、自動的に実行されます。既定では、TCPポート110での通信が全てスキャンされますが、他の通信ポートも必要に応じて追加できます。ポート番号はカンマで区切る必要があります。

デフォルトでは、暗号化された通信は検査されません。

POP3/POP3Sフィルタリングを使用するには、まず、プロトコルフィルタリングを有効にする必要があります。POP3/POP3Sのオプションがグレー表示されている場合は、詳細設定ツリーで［コンピュータの保護］＞［ウイルス・スパイウェア対策］＞［プロトコルフィルタリング］に移動し、［アプリケーションプロトコルフィルタリングを有効にする］をチェックします。フィルタリングと設定の詳細については、「プロトコルフィルタリング」を参照してください。



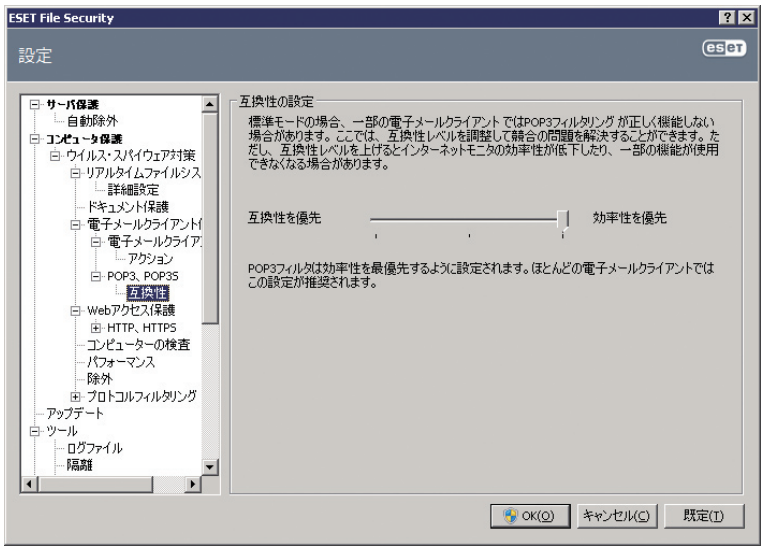
■ 互換性

メールプログラムによっては、POP3フィルタリングに問題が発生することがあります。たとえば、インターネット接続が遅い、検査のためにタイムアウトが発生するなどです。その場合には、互換性レベルを変更してみてください。互換性レベルを下げると、駆除処理の速度が向上することがあります。POP3フィルタリングの互換性レベルを調整するには、［詳細設定］ツリーで［ウイルス・スパイウェア対策］＞［メールの保護］＞［POP3、POP 3S］＞［互換性］に移動します。

[効率性を優先] を有効にすると、感染したメッセージからマルウェアが削除され、マルウェアについての情報が元の電子メールの件名の前に挿入されます ([削除] または [駆除] が有効になっているか、または厳密または既定の駆除レベルが有効になっている必要があります)。

[互換性:中] では、メッセージの受信方法が変更されます。メッセージは少しずつメールクライアントに送られます。メッセージの転送が完了すると、マルウェアがいないかどうかスキャンされます。このレベルの検査では、駆除レベルおよび検査通知の処理 (通知警告が件名とメール本文に追加されます) は、[効率性を優先] の設定と同じです。

[互換性を優先] レベルでは、感染しているメッセージを受信したことを報告する警告ウィンドウが表示されます。配信されたメッセージの件名にもメール本文にも、感染しているファイルについての情報は何も追加されません。また、マルウェアは自動的には削除されません。マルウェアの削除は、ユーザーがメールクライアントから実行する必要があります。

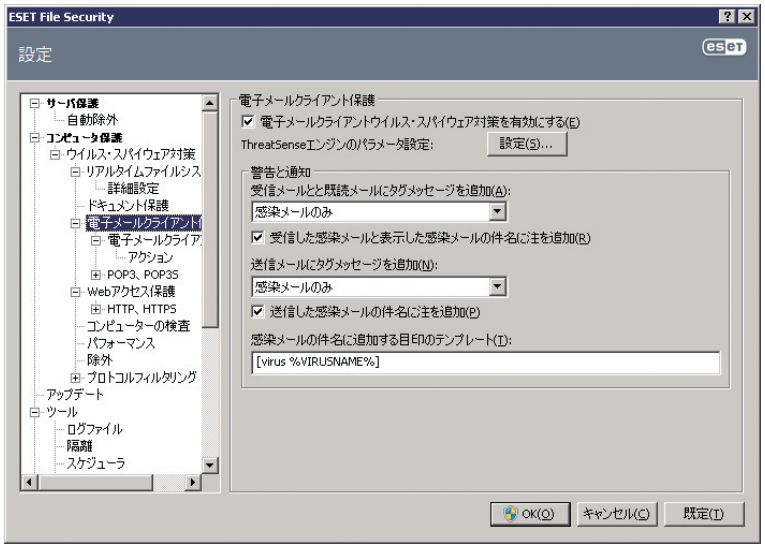


メールクライアントとの統合

ESET File Security for Microsoft Windows Serverをメールクライアントと統合すると、メールメッセージにおいて悪意のあるコードから積極的に保護するレベルが向上します。サポートされているメールクライアントであれば、ESET File Security for Microsoft Windows Serverでこの統合を有効化できます。統合が有効であれば、ESET File Security for Microsoft Windows Serverはメールクライアントのツールバーに登録されて、効率的にメールを保護できるようになります。統合の設定は、[設定] > [環境設定で詳細な設定をする...] > [その他] > [メールソフトウェアとの統合] にあります。メールソフトウェアとの統合では、サポートされているメールクライアントとの統合を有効化できます。現在サポートされているメールクライアントは、Microsoft Outlook、Outlook Express、Windows Mail、Windows Live Mail、およびMozilla Thunderbirdです。

メールクライアントでの作業時にシステムの速度が低下する場合は、[受信ボックス内の変更時にチェックを無効にする] オプションを選択します。Kerio Outlook Connector Storeからメールをダウンロードするときに、このような状況が発生する場合があります。

メールの保護を有効にするには、[設定] > [法再設定のツリー全体を表示する...] > [コンピュータの保護] > [ウイルス・スパイウェア対策] > [電子メールクライアント保護] をクリックし、[電子メールクライアントウイルス・スパイウェア対策を有効にする] オプションを選択します。



■ メール本文への検査通知の追加

ESET File Security for Microsoft Windows Serverで検査する各メールは、検査通知を件名または本文に追加することができます。この機能により、受信者が感じる信頼性が向上します。また、マルウェアが検出された場合、そのメールまたは送信者の脅威レベルについての貴重な情報を得ることができます。

この機能に対するオプションは、[詳細設定] > [コンピュータの保護] > [ウイルス・スパイウェア対策] > [電子メールクライアント保護] にあります。[受信メールとkidokuメールにタグメッセージを追加] および [送信メールにタグメッセージを追加] を選択できます。検査したすべてのメールまたは感染メールのみのどちらにタグメッセージを追加するか、またはまったく追加しないかを指定することもできます。

ESET File Security for Microsoft Windows Serverでは、感染メッセージ元の件名にメッセージを追加することもできます。件名への追加を有効にするには、[受信した感染メールと表示した感染メールの件名に注を追加] オプションと [送信した感染メールの件名に注を追加] オプションの両方を選択します。

通知の内容は、[感染メールの件名に追加する目印のテンプレート] フィールドで変更できます。前述したように変更すると、特定の件名を持つメールをフィルタリングして別のフォルダに移動できるため、感染メールのフィルタリング処理を自動化しやすくなります (使用しているメールクライアントでサポートされている場合)。

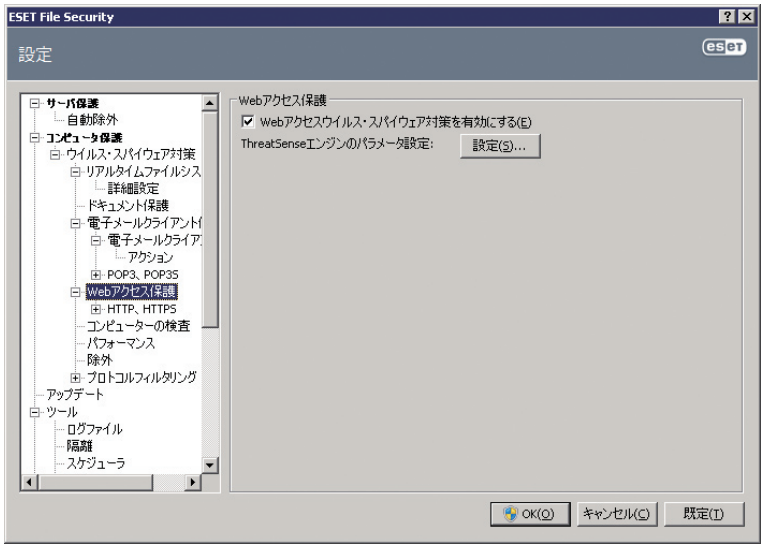
マルウェアの削除

ウイルスに感染しているメールを受信した場合、警告ウィンドウが表示されます。警告ウィンドウには、送信者名、メール、およびマルウェアの名前が表示されます。ウィンドウの下部には、検出された対象に使用できる、[駆除] [削除]、または [何もしない] というオプションがあります。基本的に、[駆除] または [削除] を選択することをお勧めします。特定な状況で、ウイルスに感染しているメールを受信したい場合には、[何もしない] を選択します。

電子メールクライアント保護のThreatSenseエンジンのパラメータの設定で、駆除の設定が [厳密な駆除] になっている場合、情報を提示するだけで、感染している対象に使用できるオプションは何もない情報ウィンドウが、表示されます。

4.2.1.3 Webアクセス保護

インターネット接続は、パーソナルコンピューターの標準機能です。残念ながら、悪意のあるコードを転送する主要な媒体にもなっています。したがって、Webアクセス保護を入念に検討することが不可欠です。[Webアクセスウイルス・スパイウェア対策を有効にする] オプションを選択することを、強くお勧めします。このオプションは、[詳細設定] (F5) > [コンピュータの保護] > [ウイルス・スパイウェア対策] > [Webアクセス保護] にあります。

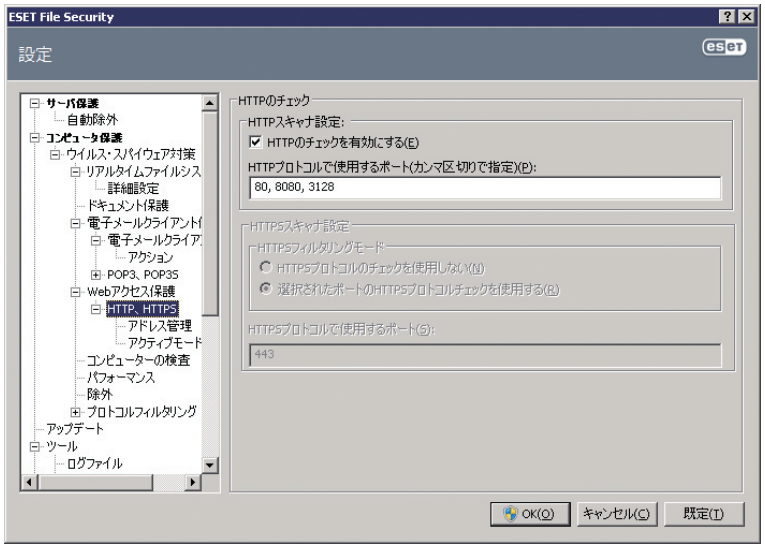


HTTP、HTTPS

Webアクセス保護は、インターネットブラウザとリモートサーバとの通信 (HTTP (Hypertext Transfer Protocol) およびHTTPS (暗号化通信) のルールに準拠) を監視しています。既定では、ESET File Security for Microsoft Windows Serverは、大半のインターネットブラウザが標準を使用するTCPポートが検査対象として指定されています。HTTPスキャナ設定オプションは [詳細設定] (F5) > [ウイルス・スパイウェア対策] > [Webアクセス保護] > [HTTP、HTTPS] で変更できます。HTTPフィルタのメインウィンドウでは、[HTTPのチェックを有効にする] オプションを選択または選択解除できます。また、HTTP通信に使用するポート番号も指定できます。既定では、ポート番号は80、8080、および3128があらかじめ指定されています。HTTPSのチェックは、次のモードで実行できます。

HTTPSプロトコルのチェックを使用しない-暗号化通信はチェックされません。

選択したポートに対してHTTPSプロトコルのチェックを使用する-[HTTPSで使用するポート] で定義されているポートに関してのみHTTPSのチェックを行います。

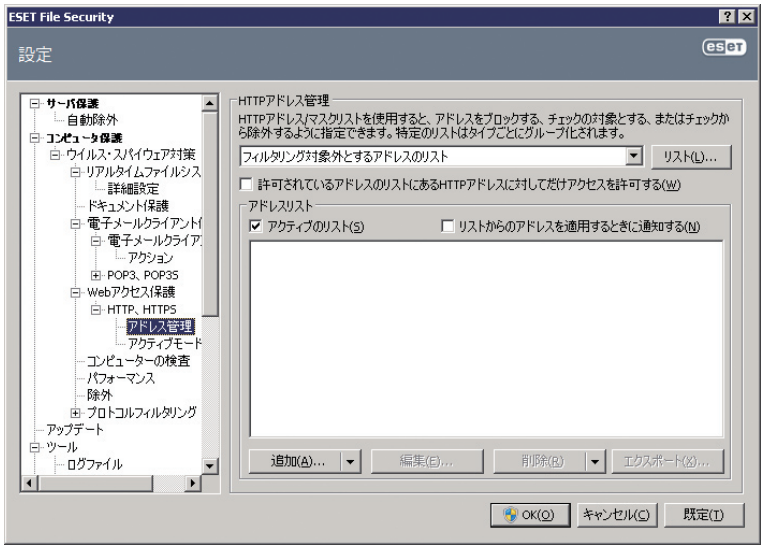


■ アドレス管理

このセクションでは、ブロック、許可、またはチェックから除外するHTTPアドレスを指定できます。[追加...] > [編集...] > [削除...]、および [エクスポート...] の各ボタンを使用して、アドレスの一覧を管理します。

ブロックされるアドレスの一覧にあるWebサイトにはアクセスできなくなります。除外されるアドレスの一覧にあるWebサイトには、悪意のあるコードがあるかどうかを検査せずにアクセスできます。[許可するアドレスのリスト内のHTTPアドレスのみにアクセスを許可する] オプションをチェックすると、許可するアドレスの一覧にあるアドレスのみにアクセスでき、その他のHTTPアドレスは全てブロックされます。

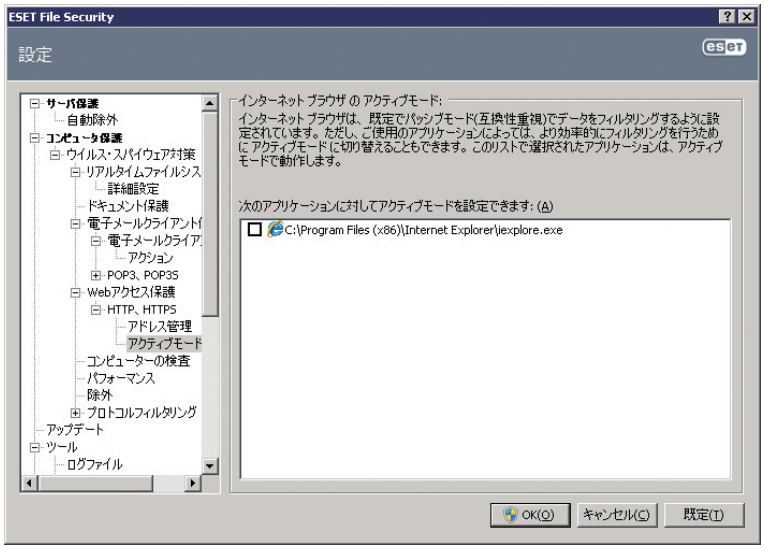
全ての一覧で、特殊記号の*（アスタリスク）および?（疑問符）を使用できます。アスタリスクは任意の文字列を、疑問符は任意の記号をそれぞれ表します。除外アドレスを指定する際には、細心の注意を払ってください。その一覧には信頼できる安全なアドレスだけを指定します。同様に、記号の*および?を一覧内で正しく使用してください。一覧を有効にするには、[アクティブのリスト] を選択します。現在の一覧からアドレスを入力するときに通知が必要な場合は、[リストからアドレスを適用するときに通知する] を選択します。



■ アクティブモード

Webブラウザとしてマークされたアプリケーションの一覧には、[HTTP、HTTPS] の [Webブラウザ] サブメニューから直接アクセスできます。

[アクティブモード] では転送されるデータがまとめて検査されます。アクティブモードが無効の場合、アプリケーションの通信はバッチ処理で段階的に検査されます。これにより、データ確認処理の効果は低下しますが、一覧に列挙されたアプリケーションに対する互換性は向上します。使用中に何も問題が発生しなければ、目的のアプリケーションの横にあるチェックボックスをチェックして、アクティブ検査モードを有効にすることをお勧めします。



4.2.1.4 コンピュータの検査

コンピューターの動作が異常で感染していると思われる場合には、オンデマンドのコンピュータのスキャンを実行して、コンピューターにマルウェアがいないかどうかを調べます。セキュリティの観点からは、感染が疑われるときだけコンピュータのスキャンを実行するのではなく、通常のセキュリティ手段の一環として定期的に実行することが重要です。検査を定期的に行うと、ディスクに保存されたときにリアルタイムスキャナーで検出されなかったマルウェアでも、検出できる場合があります。リアルタイムスキャナーで検出できないケースとは、感染時にリアルタイムスキャナーが無効に設定されていた場合や、ウイルス定義データベースが最新でない場合、アーカイブファイル内にウイルスが含まれる場合などです。

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

スキャンの種類

コンピュータの検査には次の2種類があります。[Smart検査] では、検査パラメーターを追加で設定することなく、簡単にシステムを検査します。[カスタム検査] では、あらかじめ定義した検査プロファイルを選択することや、特定の検査対象を選択することができます。

■ Smart検査

Smart検査を使用すると、コンピュータの検査をすぐに開始して、ユーザーが操作しなくても感染しているファイルからウイルスを駆除できます。主な利点は、簡単に操作でき、スキャンを詳細に設定しなくても済むことです。Smart検査では、ローカルドライブにある全てのファイルが検査されます。検出されたマルウェアがあれば、自動的に駆除または削除されます。駆除のレベルは自動的に既定値に設定されます。駆除の種類の詳細については、「駆除」を参照してください。

■ カスタム検査

カスタム検査は、スキャン対象やスキャン方法などのスキャンパラメータを自分で指定したい場合に最適なソリューションです。カスタム検査の利点は、パラメータを詳細に設定できることです。設定はユーザー定義の検査プロファイルに保存できます。これは、同じパラメーターで検査を繰り返し実行する場合に便利です。

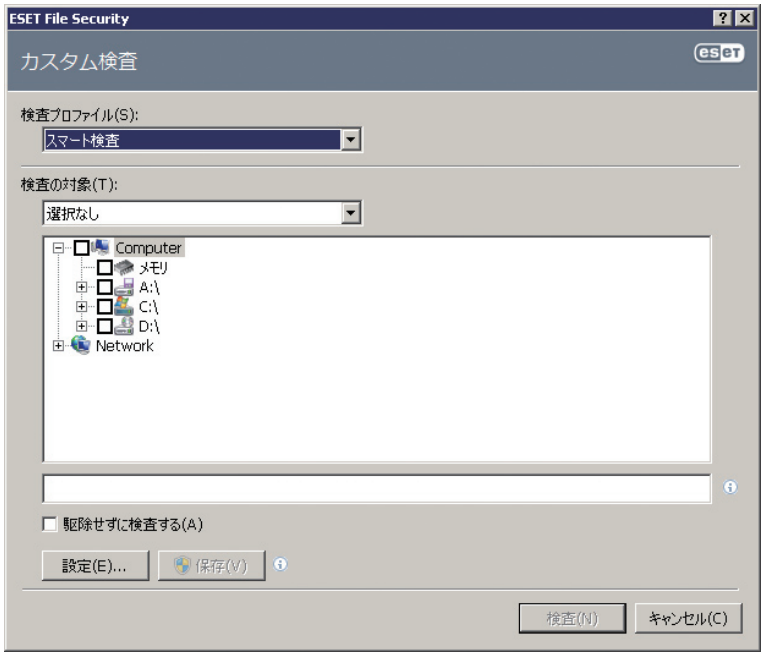
検査の対象を選択するには、[コンピュータの検査] > [カスタム検査] を選択し、[検査の対象] ドロップダウンメニューからオプションを選択するか、またはツリー構造から個別の対象を選択します。検査対象をさらに細かく指定することもできます。そのためには、対象にするフォルダーまたはファイルのパスを入力します。システムの検査で追加の駆除アクションを実行する必要がない場合は、[駆除せずに検査する] オプションを選択します。[設定...] > [駆除] をクリックして、3つの駆除レベルから選択することもできます。

スキャン対象

[スキャン対象] ドロップダウンメニューを使用すると、ウイルスを検査するファイル、フォルダー、およびデバイス（ディスク）を選択できます。

プロファイル設定に依存	選択された検査プロファイルに設定されている対象を選択します。
リムーバブルメディア	フロッピーディスク、USB記憶装置、CD/DVDを選択します。
ローカルドライブ	システムのすべてのハードディスクを選択します。
ネットワークドライブ	マップされたすべてのドライブを選択します。
選択なし	すべての選択をキャンセルします。

検査の対象をさらに細かく指定することもできます。そのためには、検査の対象に含めるフォルダーまたはファイルのパスを入力します。コンピューター上で使用できるすべてのデバイスを表示しているツリー構造から対象を選択します。

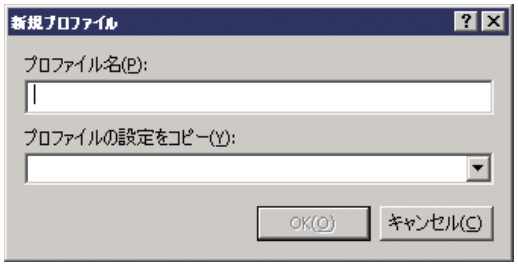


スキャンのプロファイル

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

新しいプロファイルを作成するには、[詳細設定] ウィンドウ（F5）を開き、[コンピュータの保護] > [コンピュータの検査] > [プロファイル...] をクリックします。[設定プロファイル] ウィンドウには、既存のスキャンプロファイルと、新しいプロパティを作成するためのオプションを表示するドロップダウンメニューがあります。ニーズに合った検査プロファイルを作成するための参考情報として、「ThreatSenseエンジンのパラメーターの設定」にある検査設定の各パラメーターの説明を参照してください。

例:既にあるSmart検査の設定は部分的にしか自分のニーズを満たさないので、独自の検査プロファイルを作成する必要があるとします。(ランタイム圧縮形式と安全でない可能性があるアプリケーションは、検査しません。また、[厳密な駆除]を適用することにします。)[設定プロファイル]ウィンドウで[追加...]ボタンをクリックします。[プロファイル名]フィールドに新しいプロファイルの名前を入力し、[プロファイルの設定をコピー]ドロップダウンメニューから[スマート検査]を選択します。次に、残りのパラメータを調整し、自分の要件に合わせます。



コマンドライン

ESET File Security for Microsoft Windows Serverのコンピュータの検査は、コマンドラインから手動で起動することも("ecls"コマンドを使用します)、バッチ("bat")ファイルを使用して起動することもできます。

コマンドラインからオンデマンドスキャナを実行する際には、次のパラメータおよびスイッチを使用することができます。

一般的なオプション

/help	ヘルプの表示と終了を実行します
/version	バージョン情報の表示と終了を実行します
/base-dir=FOLDER	FOLDERからモジュールをロードします
/quar-dir=FOLDER	FOLDERを隔離します
/aind	アクティビティインジケータを表示します

対象:

/files	ファイルを検査します(既定)
/no-files	ファイルを検査しません
/boots	ブートセクタを検査します(既定)
/no-boots	ブートセクタを検査しません
/arch	アーカイブを検査します(既定)
/no-arch	アーカイブを検査しません
/max-archive-level=LEVEL	アーカイブの階層を最大LEVELレベルまで検査します
/scan-timeout=LIMIT	最大でLIMIT秒間アーカイブを検査します。検査時間がこの上限に達すると、アーカイブの検査が停止し、次のファイルの検査に移ります
/max-arch-size=SIZE	アーカイブのうち、SIZE未満のファイルのみスキャンします
/mail	電子メールを検査します
/no-mail	電子メールファイルを検査しません
/sfx	自己解凍アーカイブを検査します
/no-sfx	自己解凍アーカイブを検査しません
/rtp	ランタイム圧縮形式を検査します
/no-rtp	ランタイム圧縮形式を検査しません

/exclude=FOLDER	FOLDERを検査対象から除外します
/subdir	サブフォルダを検査します（既定）
/no-subdir	サブフォルダ検査しません
/max-subdir-level=LEVEL	サブフォルダの階層を最大LEVELレベルまで検査します（既定値0=無制限）
/symlink	シンボリックリンクをたどります（既定）
/no-symlink	シンボリックリンクをスキップします
/ext-remove=EXTENSIONS	コロン区切りのEXTENSIONS（拡張子）に該当するファイルのみを検査対象にします
/ext-exclude=EXTENSIONS	コロン区切りのEXTENSIONS（拡張子）に該当するファイルを検査対象から除外します

検査方法:

-adware	アドウェア/スパイウェア/リスクウェアを検査します
-no-adware	アドウェア/スパイウェア/リスクウェアを検査しません
-unsafe	潜在的に危険性のあるアプリケーションを検査します
-no-unsafe	潜在的に危険性のあるアプリケーションを検査しません
-unwanted	潜在的に不要なアプリケーションを検査します
-no-unwanted	潜在的に不要なアプリケーションを検査しません
-pattern	シグネチャを使用します。
-no-pattern	シグネチャを使用しません
-heur	ヒューリスティックを有効にします
-no-heur	ヒューリスティックを無効にします
-adv-heur	アドバンスドヒューリスティックを有効にします
-no-adv-heur	アドバンスドヒューリスティックを無効にします

駆除:

-action=ACTION	感染対象にACTIONを実行します。使用可能なアクション:none、clean、prompt
-quarantine	感染ファイルを隔離フォルダにコピーします（ACTIONの補足）
-no-quarantine	感染ファイルを隔離フォルダにコピーしません

ログ:

-log-file=FILE	ログをFILEに出力します
-log-rewrite	ログファイルを上書きします（既定-append）
-log-all	感染していないファイルも記録します
-no-log-all	感染していないファイルは記録しません（既定）

検査の終了コードの例:

0	脅威は検出されませんでした
1	脅威は検出されましたが駆除されませんでした。
10	いくつかの感染ファイルは残ります
101	アーカイブエラー
102	アクセスエラー
103	内部エラー

▸▸▸ NOTE

100番台の終了コードは、ファイルが検査されなかったため、感染している可能性があることを意味します。

4.2.1.5 パフォーマンス

このセクションでは、ウイルス検査に使用するThreatSense検査スレッドの数を設定できます。マルチプロセッサマシンでThreatSense検査スレッドを増やせば、検査速度を上げることができます。許容値は1～20です。

NOTE

ここでの変更は、再起動後に適用されます。

4.2.1.6 プロトコルフィルタリング

POP3およびHTTPアプリケーションプロトコルに対するウイルスからの保護機能は、あらゆる高度なマルウェアスキャン技術をシームレスに統合するThreatSense検査エンジンによって実施されます。この検査は、使用しているインターネットブラウザやメールクライアントに関係なく、自動的に動作します。[アプリケーションプロトコルフィルタリングを有効にする] オプションを選択している場合は、[フィルタリングのための通信リダイレクト] では次のオプションが使用可能です。

HTTPおよびPOP3ポート-既知のHTTPポートおよびPOP3ポートに対する通信の検査を制限します。

インターネットブラウザまたは電子メールクライアントとしてマークされたアプリケーション-ブラウザとしてマークしたアプリケーション（[Webアクセス保護] > [HTTP、HTTPS] > [Webブラウザ]）および電子メールクライアントとしてマークしたアプリケーション（[電子メールクライアント保護] > [POP3、POP3S] > [メールクライアント]）の通信をフィルタする場合のみ、このオプションを有効にします。

インターネットブラウザまたは電子メールクライアントとしてマークされたポートとアプリケーション-ポートおよびブラウザの両方に対してマルウェアを検査します。

NOTE

Windows Vista Service Pack 1およびWindows Server 2008以降では、新しい通信フィルタリング方法が使用されます。したがって、[フィルタリングのための通信リダイレクト] セクションは使用不可です。

SSL

ESET File Security for Microsoft Windows Serverでは、SSLプロトコルでカプセル化されたプロトコルを検査できます。信頼できる証明書、不明な証明書、またはSSL保護された通信の検査から除外されている証明書を使用しているSSL保護された通信に対して、さまざまなスキャンモードを使用できます。

SSLプロトコルを常に検査する	検査から除外されている証明書によって保護されている通信を除く、SSL保護されたすべての通信を検査する場合、このオプションを選択します。署名された不明な証明書を使用する新しい通信が確立されても、その事実が通知されることはなく、通信は自動的にフィルタされます。信頼できるとマークした信頼できない証明書（信頼できる証明書のリストに追加されている証明書）でサーバにアクセスする場合、サーバへの通信は許可され、通信チャネルのコンテンツはフィルタされます。
アクセスしていないサイトについて確認する（除外を設定できます）	SSL保護された新しいサイト（不明な証明書を使用して）を入力すると、アクション選択ダイアログが表示されます。このモードでは、検査から除外するSSL証明書のリストを作成できます。
SSLプロトコルチェックを使用しない	このオプションを選択すると、プログラムはSSL上の通信を検査しません。

信頼できるルート認証局ストア（[プロトコルフィルタリング] > [SSL] > [証明書]）を使用して証明書を検証できない場合

証明書の有効性について尋ねる	実行するアクションを選択するよう求めます。
証明書を使用する通信をブロックする	証明書を使用するサイトへの通信を切断します。

証明書（[プロトコルフィルタリング] > [SSL] > [証明書]）が無効または破損している場合

証明書の有効性について尋ねる	実行するアクションを選択するよう求めます。
証明書を使用する通信をブロックする	証明書を使用するサイトへの通信を切断します。

■ 信頼できる証明書

ESET File Security for Microsoft Windows Serverが信頼できる証明書を保管する統合された信頼できるルート認証局ストアに加えて、信頼できる証明書のカスタムリストを作成できます。このリストは、[詳細設定]（F5）> [プロトコルフィルタリング] > [SSL] > [証明書] > [信頼できる証明書] を選択することによって表示できます。

■ 除外される証明書

[除外される証明書] セクションには、安全と見なされている証明書があります。このリストにある証明書を使用する暗号化通信のコンテンツに対してウイルスの検査を行いません。安全が保証されており、その証明書を使用する通信を検査する必要のないWeb証明書のみ除外することをお勧めします。

4.2.1.7 ThreatSenseエンジンのパラメータの設定

ThreatSenseは、複雑なウイルス検出方法で構成される技術の名前です。この技術はプロアクティブなので、新しいウイルスが広がる初期の段階でも保護することができます。この技術では、システムのセキュリティを大幅に強化するために連携して動作するさまざまな方法（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）の組み合わせが使用されます。検査エンジンは、複数のデータストリームを同時に検査して、最大限の効率および検出率を確保することができます。また、ThreatSense技術によってルートキットを除去することもできます。

ThreatSense技術の設定オプションを使用すると、ユーザーはさまざまな検査パラメーターを指定することができます。

●検査するファイルの種類および拡張子
●さまざまな検出方法の組み合わせ
●駆除のレベルなど

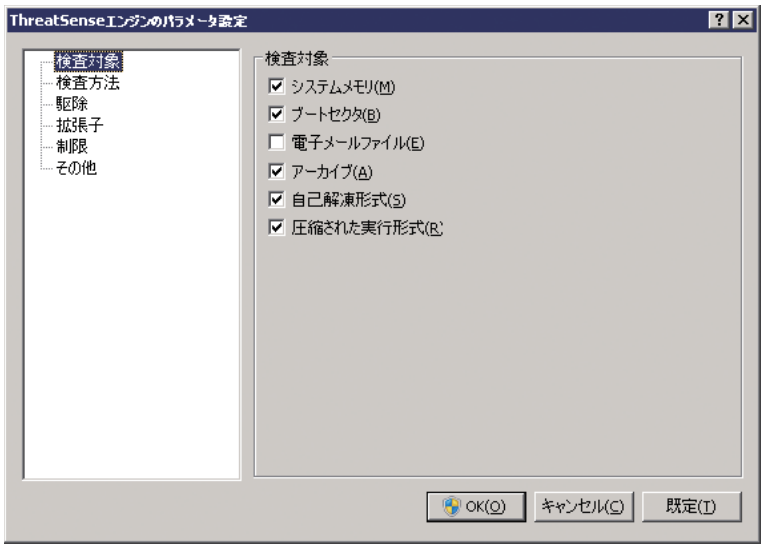
設定ウィンドウにアクセスするには、ThreatSense技術を使用する任意の機能（下記を参照）の設定ウィンドウにある [設定...] ボタンをクリックします。セキュリティシナリオごとに異なる設定が必要になることがあります。これを念頭に、ThreatSenseは、次の保護モジュールについて個々に設定することができます。

●リアルタイムファイルシステム保護
●システムのスタートアップファイルのチェック
●電子メール保護
●Webアクセス保護
●コンピュータの検査

ThreatSenseのパラメータは機能ごとに高度に最適化されているので、パラメータを変更すると、システムの動作に大きく影響することがあります。たとえば、常にランタイム圧縮形式をスキャンするようにパラメータを変更したり、ファイルシステムのリアルタイム保護モジュールでアドバンスドヒューリスティックを有効にしたりすると、システムの処理速度が低下することがあります（通常は、新しく作成されたファイルのみがこれらの方法を使用してスキャンされます）。そのため、コンピュータの検査を除く全ての機能について、ThreatSenseの既定のパラメーターを変更しないことをお勧めします。

対象の設定

[検査対象] セクションでは、検査対象とするファイル形式を指定できます。

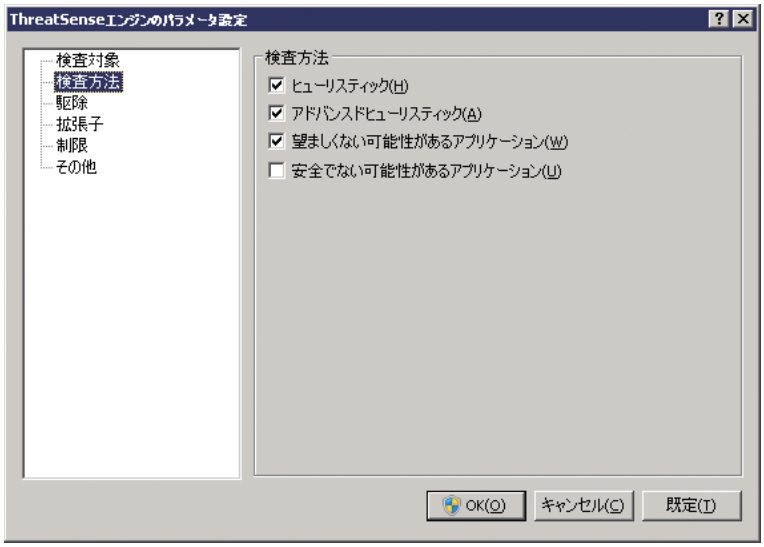


システムメモリ	システムメモリを攻撃するウイルスを検査します。
ブートセクタ	マスタブートレコードのウイルスを検出するためにブートセクタを検査します。
電子メールファイル	電子メールメッセージが含まれている特殊なファイルを検査します。
アーカイブ	圧縮されたファイル（.rar、.zip、.arj、.tarなど）の内部を検査します。
自己解凍形式	アーカイブファイルの一種で、通常はファイル拡張子が.exeになっているファイルに含まれているファイルを検査します。
圧縮された実行形式	標準的な静的圧縮形式（UPX、yoda、ASPack、FGSなど）に加え、メモリに展開される圧縮された実行形式（標準のアーカイブ形式とは異なる）を検査します。

検査方法

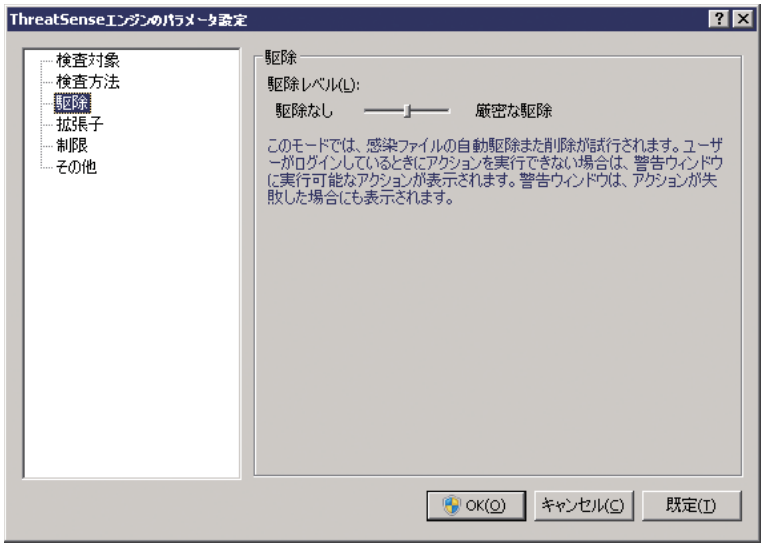
[検査方法] セクションでは、システムのマルウェアの検査時に使用される方法を選択できます。使用可能なオプションは次のとおりです。

ヒューリスティック	ヒューリスティックは、悪意のあるプログラムの活動を解析するアルゴリズムを使用します。ヒューリスティック検出法の主な利点は、存在しなかった、またはこれまでのウイルス定義ファイルで特定されていなかった、悪意のある新しいマルウェアを検出できる能力です。
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ています。アドバンスドヒューリスティックによって、プログラムの検出能力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	望ましくない可能性があるアプリケーションは、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。最も大きな変化としては、不要なポップアップウィンドウ、隠しプロセスの開始と実行、システムリソースの使用率の増加、検索結果の変更、アプリケーションがリモートサーバと通信するなどがあります。
潜在的に危険性のあるアプリケーション	潜在的に危険性のあるアプリケーションは、市販の適正なソフトウェアに使用される分類です。これには、リモートアクセスツールなどのプログラムが含まれます。そのため、既定ではこのオプションは無効に設定されています。



駆除

駆除設定により、感染ファイルからウイルスを駆除するときのスキャナの動作が決まります。駆除には、3つのレベルがあります。



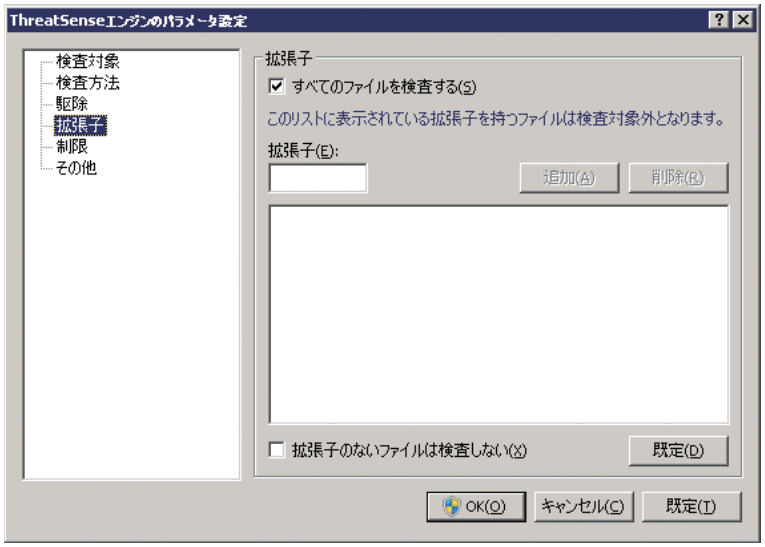
駆除なし	感染しているファイルが自動的に駆除されることはありません。警告ウィンドウが表示され、アクションを選択することができます。
標準的な駆除	感染ファイルが自動的に駆除または削除されます。適切なアクションを自動的に選択できなかった場合は、ユーザーがその後のアクションを選択することができます。その後のアクションとして選択した内容は、あらかじめ指定したアクションを完了できなかった場合にも表示されます。
厳密な駆除	全ての感染ファイルが駆除または削除されます(アーカイブも対象)。ただし、システムファイルは除きます。感染ファイルを駆除できなかった場合は、警告ウィンドウでアクションを選択することができます。

CAUTION

既定のモード(標準的な駆除)で、アーカイブファイル全体が削除されるのは、アーカイブ内の全てのファイルが感染している場合のみです。問題のないファイルが検査対象に含まれている場合には、アーカイブファイルは削除されません。厳密な駆除モードでは、感染しているアーカイブファイルが検出された場合、感染していないファイルがあっても、アーカイブ全体が削除されます。

拡張子

拡張子は、ファイル名の一部であり、ピリオドで区切られています。拡張子は、ファイルの種類と内容を規定します。ThreatSenseパラメータ設定のこのセクションでは、スキャンするファイルの種類を指定できます。



既定では、拡張子に関係なく、全てのファイルがスキャンされます。スキャンから除外するファイルの一覧には、どの拡張子でも追加できます。[全てのファイルをスキャンする] オプションを選択解除すると、リストが変更されて、スキャン対象のファイル拡張子が表示されます。[追加] および [削除] のボタンを使用することで、目的の拡張子のスキャンを有効にしたり禁止したりできます。

拡張子のないファイルのスキャンを有効にするには、[拡張子のないファイルをスキャンする] オプションをチェックします。

特定のファイルの種類を検査すると、その拡張子を使用しているプログラムが正常に動作できなくなる場合に、ファイルを除外する必要が生じることがあります。たとえば、MS Exchange Serverを使用しているときには、拡張子.edb、.eml、および.tmpを除外すると良いでしょう。

制限

[制限] セクションでは、検査対象のオブジェクトの最大サイズおよびネストされたアーカイブのレベルを指定できます。最大オブジェクトサイズ-検査対象のオブジェクトの最大サイズを定義します。これにより、ウイルス対策機能では、指定した値より小さいサイズのオブジェクトのみが検査されます。一般的には既定値を変更する理由はないので、その値を変更しないことをお勧めします。上級ユーザーが大きいオブジェクトを検査から除外する必要がある場合のみ、このオプションを変更してください。

オブジェクトの最大検査時間(秒):	オブジェクトを検査する最長時間を定義します。ここでユーザー定義の値が入力されていると、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ウイルス対策機能は検査を停止します。
スキャン対象の下限ネストレベル	アーカイブの検査の最大レベルを指定します。一般的な環境では既定値(10)を変更する理由はないので、その値を変更しないことをお勧めします。ネストされたアーカイブ数が原因で検査が途中で終了した場合、アーカイブは未チェックのままになります。
スキャン対象ファイルの最大サイズ:	このオプションを使用すると、検査対象のアーカイブ(抽出された場合)に格納されるファイルの最大ファイルサイズを指定できます。この結果検査が途中で終了したアーカイブは、未チェックのままになります。

その他

代替データストリーム(ADS)を検査	NTFSファイルシステムによって使用される代替データストリーム(ADS)は、通常の検査技術では検出できないファイルおよびフォルダの関連付けです。多くのマルウェアが、自らを代替データストリームに見せかけることによって、検出を逃れようとします。
低優先でバックグラウンドで検査	検査が行われるたびに、一定の量のシステムリソースが使用されます。システムリソースにかなりの負荷がかかるプログラムを使用している場合、優先度が低い検査をバックグラウンドで実行することによって、プログラムのためにリソースを節約することができます。
すべてのオブジェクトをログに記録	このチェックボックスをチェックすると、感染していないファイルを含め、スキャンされた全てのファイルがログファイルに記録されます。
SMART最適化を有効にする	検査済みのファイルは新たなウイルス定義データベースが提供されるか、フィルがが変更されていない限り再検査されなくなります。
最終アクセスのタイムスタンプを保持	データバックアップシステムでの利用などを考慮して、検査済みファイルへのアクセス日時を更新せずに元のまま保持するには、このオプションをチェックします。
検査ログをスクロールする	このチェックボックスを使用すると、ログのスクロールを有効/無効にすることができます。チェックボックスをオンにすると、表示ウィンドウ内で情報が上にスクロールされます。
別のウィンドウで検査通知を表示	検査結果に関する情報を含む独立したウィンドウを開きます。

4.2.1.8 マルウェアが検出された場合

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、メールや、コンピューターのリムーバブルデバイス(USB、外付けハードディスク、CD、DVD、フロッピーディスクなど)など、さまざまです。
使用しているコンピューターが、マルウェアに感染している兆候を示している場合(遅くなる、頻繁にフリーズするなど)、次の処置を取ることをお勧めします。

●ESET File Security for Microsoft Windows Serverを開き、[コンピュータの検査] をクリックします。
●[Smart検査]をクリックします。(詳細については、「Smart検査」を参照してください。)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。

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

ESET File Security for Microsoft Windows Serverでのマルウェアの一般的な処理例として、リアルタイムのファイルシステムモニター(駆除レベルは既定値)によりマルウェアが検出されたことを前提に説明します。モニタ機能は、ファイルからウイルスを駆除するか、ファイル自体を削除しようとします。リアルタイムファイルシステム保護モジュールにあらかじめ指定されたアクションがない場合は、警告ウィンドウが表示され、オプションを選択するよう求められます。選択できるオプションは通常、[駆除]、[削除]、および [何もしない] のいずれかです。[何もしない] はお勧めできません。感染しているファイルが、そのままにされるからです。例外は、そのファイルが「無害なのに誤って感染が検出された」と確信できる場合です。

駆除と削除-ウイルスが悪意のあるコードをファイルに付けて攻撃している場合に、駆除を行いますこの場合、元の状態に戻すため、まず感染しているファイルからのウイルスの駆除を試みます。ファイルが悪意のあるコードでのみ構成されている場合には、全体が削除されます。

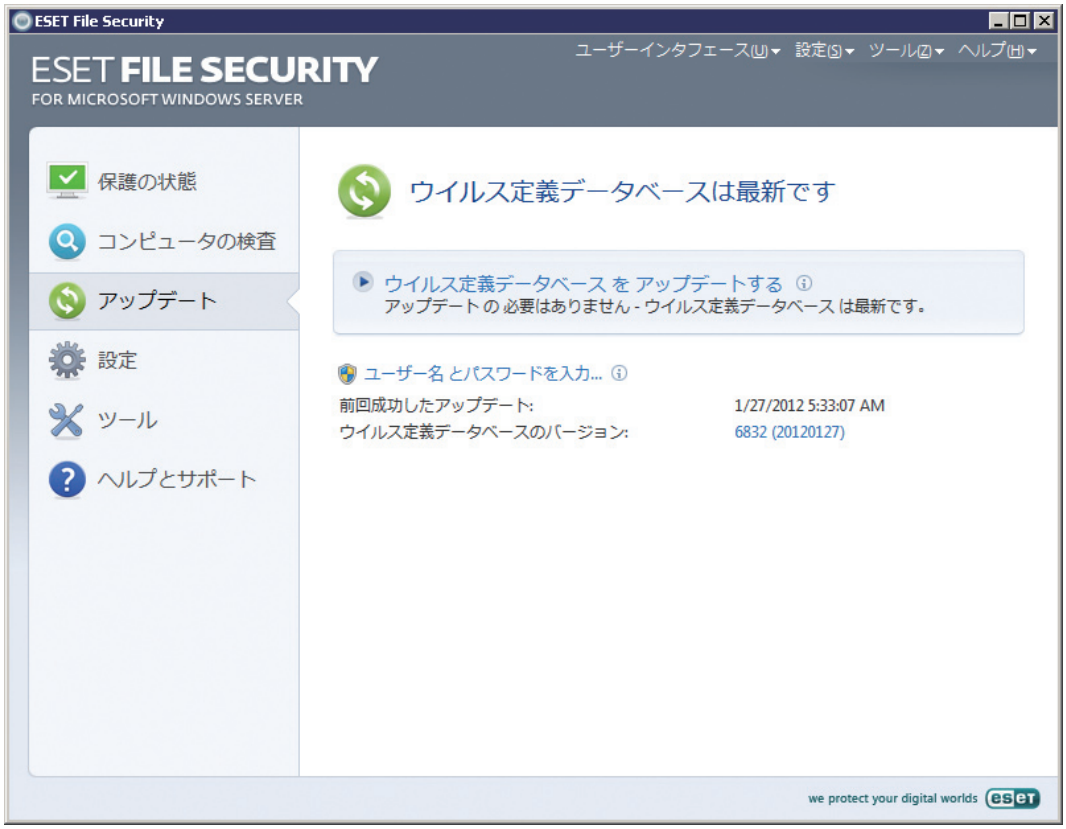
感染しているファイルが、システムプロセスによって"ロック"または使用されている場合、通常は開放後でなければ削除できません(通常は再起動後)。
アーカイブのファイルの削除-既定の駆除モードでは、アーカイブファイルに感染ファイルしか含まれていない場合にのみ、アーカイブファイル全体が削除されます。つまり、感染していない無害なファイルが検査対象に含まれている場合には、アーカイブは削除されません。厳密な駆除では、アーカイブに感染ファイルが1つでも含まれていれば、アーカイブ内の他のファイルのステータスに関係なく、アーカイブが削除されますので注意が必要です。

4.3 プログラムのアップデート

最大レベルのセキュリティを確保するためには、ESET File Security for Microsoft Windows Serverの定期的なアップデートが大前提になります。アップデート機能により、プログラムはウイルス定義データベースのアップデートとシステムコンポーネントのアップデートという2つの方法で、常に最新の状態に保たれます。

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。プライマリウィンドウには、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。ウイルス定義ファイルの番号はリンクになっており、このリンクをクリックすると、そのアップデートで追加されたウイルス情報の一覧が表示されます。

さらに、ESETのアップデートサーバにアクセスするためのアップデート設定オプション（ユーザー名、パスワードなど）に加えて、アップデートプロセスを手動で開始するための［ウイルス定義ファイルをアップデートする］オプションも使用可能です。

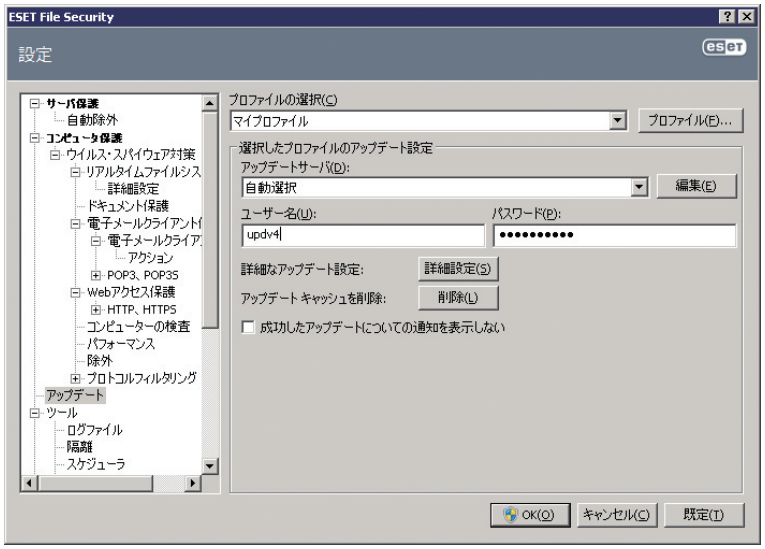


NOTE

ユーザー名とパスワードは、ESET File Security for Microsoft Windows Serverの購入後にESETにより提供されます。

4.3.1 アップデートの設定

アップデート設定セクションでは、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。既定では、[アップデートサーバ] ドロップダウンメニューは自動的に [自動選択] に設定され、最もネットワークトラフィックが少ないESETサーバからアップデートファイルが自動的にダウンロードされます。アップデート設定オプションは、[詳細設定] ツリー (F5キー) の [アップデート] にあります。



使用可能なアップデートサーバのリストにアクセスするには、[アップデートサーバ] ドロップダウンメニューを使用します。新しいアップデートサーバを追加するには、[選択されたプロファイルの更新設定] セクションの [編集...] をクリックし、[追加] ボタンをクリックします。ESET社のアップデートサーバーからウイルス定義データベースをアップデートする場合は「ユーザー名」、「パスワード」にライセンス情報 (ユーザー名、パスワード) を入力してください。

4.3.1.1 アップデートプロファイル

アップデートプロファイルは、さまざまなアップデートの設定用およびアップデートタスク用に作成できます。アップデートプロファイルの作成は、モバイルユーザーにとって特に便利です。定期的に変わるインターネット接続のプロパティに合わせて代替プロファイルを作成できるためです。

[プロファイルの選択] ドロップダウンメニューには、既定で [マイプロファイル] に設定される、現在選択されているプロファイルが表示されます。新しいプロファイルを作成するには、[プロファイル...] ボタンをクリックしてから [追加...] ボタンをクリックし、[プロファイル名] に独自の名前を入力します。新しいプロファイルを作成する際、[プロファイルの設定をコピー] ドロップダウンメニューから既存のプロファイルを選択して、そのプロファイルから設定をコピーすることができます。

プロファイル設定ウィンドウでは、使用可能なサーバのリストからアップデートサーバを指定するか、または新しいサーバを追加することができます。既存のアップデートサーバのリストにアクセスするには、[アップデートサーバ] ドロップダウンメニューを使用します。新しいアップデートサーバを追加するには、[選択されたプロファイルの更新設定] セクションの [編集...] をクリックし、[追加] ボタンをクリックします。

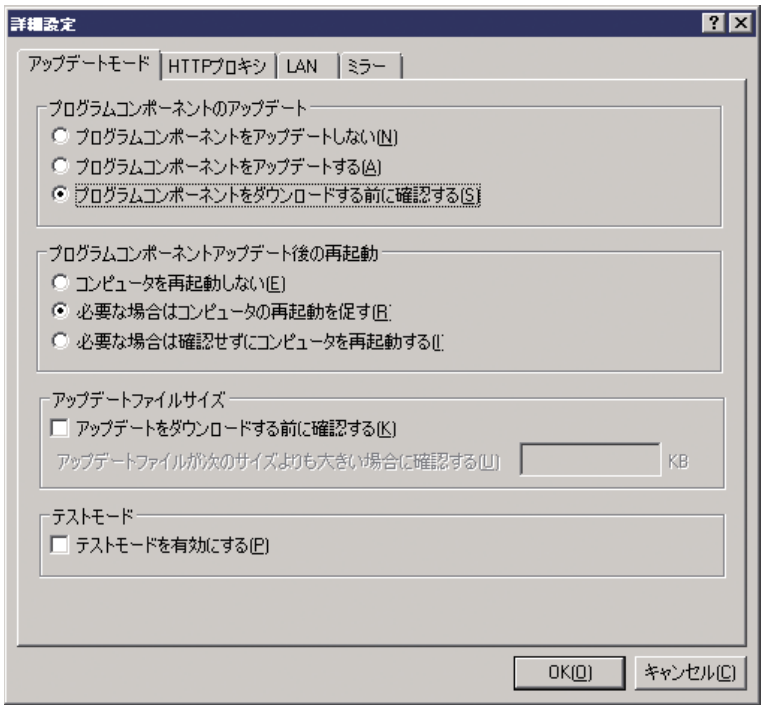
4.3.1.2 アップデートの詳細設定

[アップデートの詳細設定] を表示するには、[詳細設定...] ボタンをクリックします。アップデートの [詳細設定] のオプションには、[アップデートモード] > [HTTPプロキシ] > [LAN]、および [ミラー] の設定があります。

アップデートモード

[アップデートモード] タブには、プログラムコンポーネントの更新に関連するオプションがあります。
[プログラムコンポーネントのアップデート] セクションでは、次の3つのオプションが使用可能です。

プログラムコンポーネントをアップデートしない	新しいプログラムコンポーネントのアップデートはダウンロードされません。
プログラムコンポーネントをアップデートする	新しいプログラムコンポーネントのアップデートは自動的に行われます。
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	既定のオプションです。プログラムコンポーネントのアップデートが使用可能になったときに、承認するのか拒否するのかを求められます。



プログラムコンポーネントをアップデートした後、全てのモジュールが完全に機能するように、システムを再起動しなければならない場合があります。[プログラムコンポーネントアップデート後の再起動] セクションで、次の3つのオプションのいずれかを選択することができます。

●コンピュータを再起動しない
●必要な場合はコンピュータの再起動を促す
●必要な場合は確認せずにコンピュータを再起動する

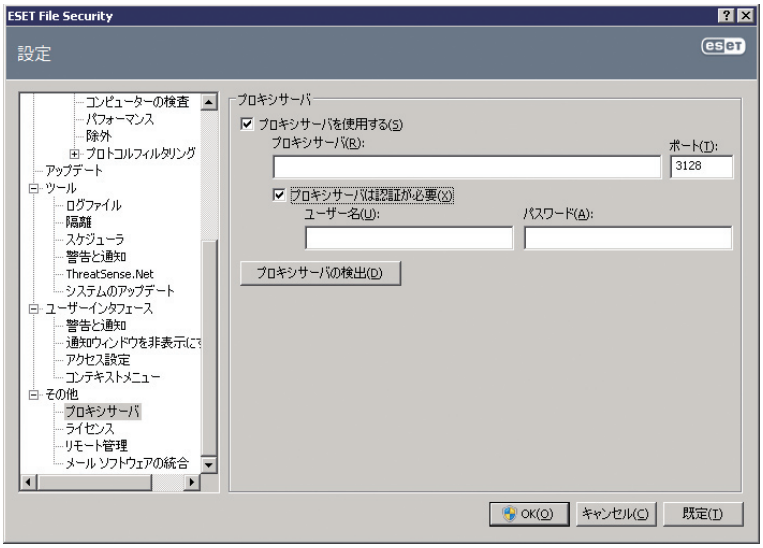
既定のオプションは、[必要場合はコンピュータの再起動を促す] です。最も適したオプションの選択は、これらの設定が適用される個々のワークステーションによって異なります。ワークステーションとサーバとでは異なる点に注意してください。たとえば、プログラムの更新後にサーバを自動的に再起動すると、重大な損害が生じることがあります。

プロキシサーバー

ESET File Security for Microsoft Windows Serverでは、[詳細設定] ツリーの2つのセクションにプロキシサーバの設定があります。

まず、[その他] > [プロキシサーバ] でプロキシサーバーの設定を行うことができます。プロキシサーバーをこのレベルで指定すると、ESET 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できるようになります。ここで設定するパラメーターは、インターネットへの接続を必要とする全てのモジュールで使用されます。

プロキシサーバー設定をこのレベルで指定するには、[プロキシサーバーを使用する] チェックボックスをオンにし、プロキシサーバーのアドレスを [プロキシサーバ] フィールドに入力し、プロキシサーバーの [ポート] 番号を指定します。



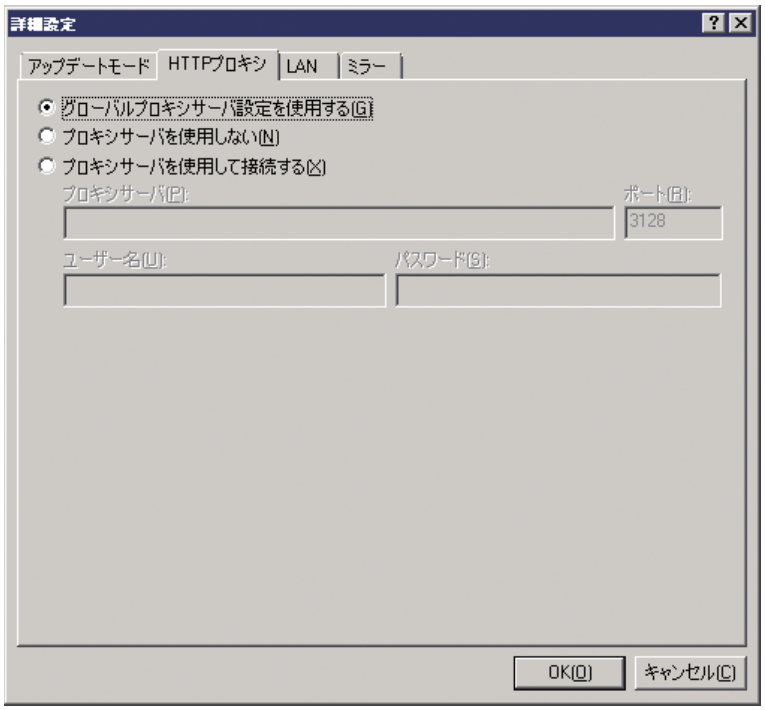
プロキシサーバーとの通信に認証が必要な場合、[プロキシサーバは認証が必要] チェックボックスをオンにし、有効なユーザー名とパスワードをそれぞれのフィールドに入力します。[プロキシサーバの検出] ボタンをクリックすると、プロキシサーバの設定が自動的に検出されて入力されます (Internet Explorerで指定したパラメータがコピーされます)。

NOTE

この機能では、認証データ(ユーザー名およびパスワード) は取得されません。手動で入力する必要があります。プロキシサーバの設定は、アップデートの [詳細設定] でも行うことができます。この設定は、特定の更新プロファイルに適用されます。特定のアップデートプロファイルに対するプロキシサーバの設定オプションは、アップデートの[詳細設定]の[HTTPプロキシ]タブにあります。次の3つのオプションからいずれかを選択できます。

- グローバルプロキシサーバ設定を使用する
- プロキシサーバを使用しない
- プロキシサーバを使用して接続する (接続は、接続プロパティによって定義されます)

[グローバルプロキシサーバ設定を使用する] オプションを選択した場合は、上記の [詳細設定] ツリーの [その他] > [プロキシサーバ] ですでに指定したプロキシサーバの設定オプションが使用されます。



ESET File Security for Microsoft Windows Serverのアップデートでプロキシサーバを使用しないことを指定するには、[プロキシサーバを使用しない] オプションを選択します。

ESET File Security for Microsoft Windows Serverのアップデートでプロキシサーバを使用する必要があり、グローバル設定 ([その他] > [プロキシサーバ]) で指定したプロキシサーバと異なる場合は、[プロキシサーバを使用して接続する] オプションを選択する必要があります。その場合は、[プロキシサーバ] (アドレス)、[ポート] (通信用) および、必要な場合はプロキシサーバの [ユーザー名] と [パスワード] をここで指定する必要があります。

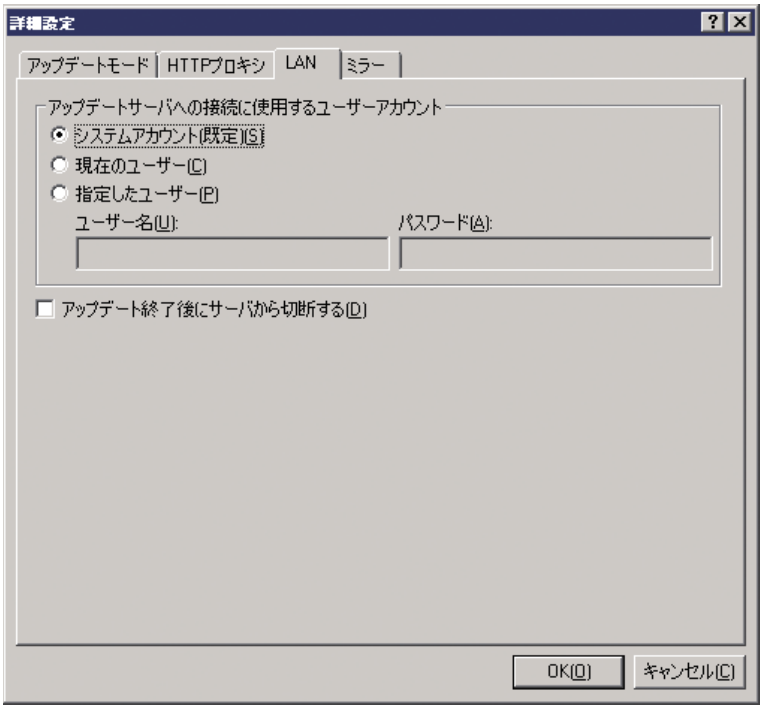
プロキシサーバの設定がグローバルに設定されておらず、ESETFile Securityをアップデートするにはプロキシサーバに接続する必要がある場合も、このオプションを選択する必要があります。

プロキシサーバの既定の設定は、[グローバルプロキシサーバ設定を使用する] です。

LANへの接続

NTベースのオペレーティングシステムを実行しているローカルサーバからアップデートする場合は、既定で、ネットワーク接続ごとに認証が必要です。ほとんどの場合、ローカルシステムアカウントにはミラーフォルダ (アップデートファイルのコピーが格納されたフォルダ) にアクセスする十分な権限がありません。この場合は、アップデートの設定セクションでユーザー名とパスワードを入力するか、あるいはプログラムがアップデートサーバ (ミラー) へのアクセスに使用する既存のアカウントを指定してください。

このアカウントを設定するには、[LAN] タブをクリックします。[アップデートサーバへの接続アカウント] セクションには、オプションとして、[システムアカウント (既定)] > [現在のユーザー]、および [指定されたユーザー] があります。



システムアカウントを認証に使用するには、[システムアカウント (既定)] を選択します。一般に、アップデートの設定のメインセクションで認証データが指定されていない場合、認証プロセスは実行されません。

現在ログインしているユーザーアカウントを使用して認証が行われるようにするには、[現在のユーザー] を選択します。この方法の欠点として、ログインしているユーザーがいない場合、プログラムはアップデートサーバに接続できません。

特定のユーザーアカウントが認証に使用されるようにするには、[指定されたユーザー] を選択します。

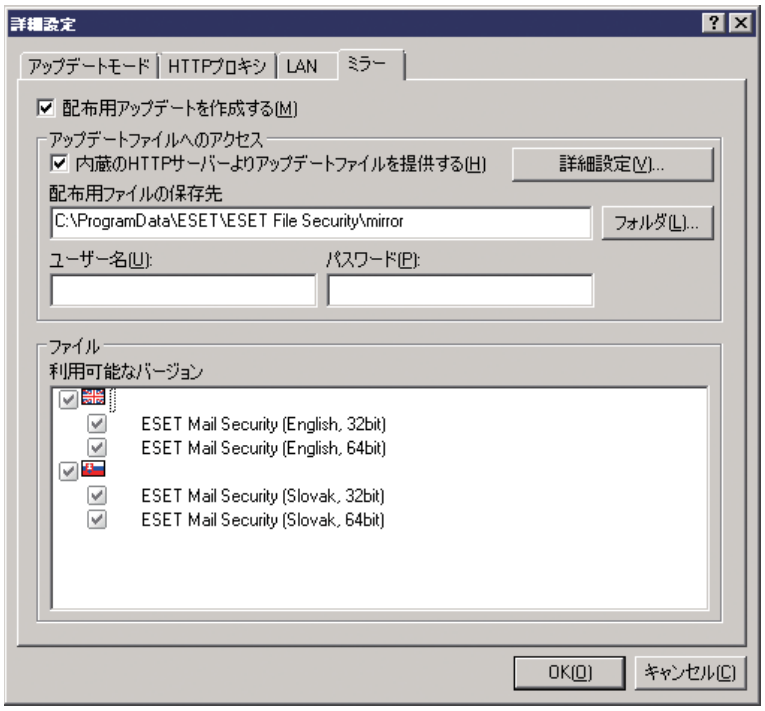
CAUTION

[現在のユーザー] または[指定されたユーザー] オプションが有効になっている場合、エラーが発生することがあります。アップデートの設定のメインセクションでLANの認証データを入力することをお勧めします。このアップデートの設定セクションで、認証データ(ユーザー名とパスワード) を、ユーザー名については<ドメイン名>¥<ユーザー >のように入力します(ワークグループの場合は、<ワークグループ名>¥<名前>のように入力します)。ローカルサーバのHTTPバージョンから更新する場合、認証は不要です。

アップデートファイルのコピーの作成-ミラー

ESET File Security for Microsoft Windows Serverでは、ネットワークにある他のワークステーションをアップデートするために使用できるアップデートファイルのコピーを作成できます。ミラーからクライアントワークステーションをアップデートすると、ネットワークの負荷分散が最適化されると共に、インターネット接続の帯域幅が節約されます。

ローカルミラーサーバの設定オプションは、ライセンスマネージャでESET File Security for Microsoft Windows Serverの [詳細設定] セクションにある有効なライセンスキーを追加した後で、アップデートの [詳細設定] セクションからアクセスできます。このセクションにアクセスするには、F5を押し、[詳細設定] ツリーの [アップデート] をクリックします。次にアップデートの [詳細設定] ボタンをクリックして [ミラー] タブを選択します。



ミラー設定の最初のステップでは、[配布用アップデートを作成する] オプションを選択します。このチェックボックスをチェックすると、アップデートファイルへのアクセス方法やミラー化されたファイルへのパスなど、他のミラー設定オプションがアクティブになります。

ミラーを有効にする方法については、「ミラーからのアップデート」で詳しく説明します。

ミラーのアップデートファイルを保存するための専用フォルダは、[配布用ファイルの保存先] セクションで定義します。ローカルコンピューターまたは共有ネットワークフォルダ上のフォルダを参照するには、[フォルダ...] をクリックします。指定したフォルダの認証が必要な場合は、[ユーザー名] フィールドと [パスワード] フィールドで認証データを指定する必要があります。ユーザー名およびパスワードは、<ドメイン>/<ユーザー>または<ワークグループ>/<ユーザー>という形式で入力する必要があります。対応するパスワードを必ず指定してください。

ミラーを設定するときは、ダウンロードするアップデートファイルのコピーの言語バージョンを指定することもできます。言語バージョンの設定は、[ファイル] セクションの [使用可能なバージョン] にあります。

■ ミラーからのアップデート

ミラーを設定する基本的な方法は2とおりあります。アップデートファイルを納めたフォルダを共有ネットワークフォルダにする方法と、HTTPサーバで公開する方法です。

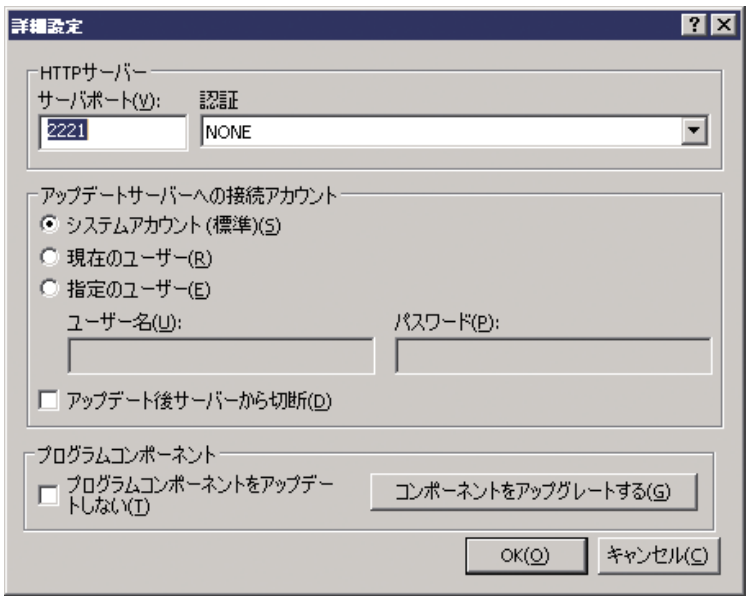
内部HTTPサーバを使用したミラーへのアクセス

これは、あらかじめ定義されたプログラム設定で指定されている既定の設定です。HTTPサーバを使用してミラーにアクセスできるようにするために、アップデートの [詳細設定] を開き [ミラー] タブに移動し、[配布用アップデートを作成する] オプションを選択します。

[ミラー] タブの [詳細設定] セクションでは、HTTPサーバでリスンする [サーバポート] およびHTTPサーバで使用する [認証] の種類を指定できます。既定では、サーバポートは、2221に設定されています。[認証] オプションでは、更新ファイルへのアクセスに使用する認証の方法を定義します。使用できるオプションは、[NONE]、[Basic]、[NTLM] です。ユーザー名およびパスワード認証でbase64エンコードを使用する場合は、[Basic] を選択してください。[NTLM] を選択すると、安全なエンコード方法でエンコードされます。認証については、更新ファイルを共有するワークステーション上で作成されたユーザーが使用されます。既定の設定は [NONE] で、認証なしでアップデートファイルにアクセスすることができます。

CAUTION

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



ミラーの設定が完了したら、ワークステーションにアクセスし、http://<サーバのIPアドレス>:2221という形式で新しいアップデートサーバを追加します。これを行うには、次の手順を実行します。

●ESET製品の [詳細設定] を開き、[アップデート] をクリックします。
●[アップデートサーバー] ドロップダウンメニューの横にある [編集] をクリックし、http://<サーバのIPアドレス>:2221という形式で新しいアップデートサーバを追加します。
●アップデートサーバのリストから、新しく追加したこのサーバを選択します。

システム共有を使用したミラーへのアクセス

まず、ローカルデバイスまたはネットワークデバイスに共有フォルダを作成する必要があります。ミラーのフォルダを作成する際には、フォルダにアップデートファイルを保存するユーザーに"書き込み"アクセス権を提供し、ミラーフォルダからESET File Security for Microsoft Windows Serverをアップデートする全てのユーザーに"読み取り"アクセス権を提供する必要があります。

次に、アップデートの [詳細設定] セクション ([ミラー] タブ) で [内部のHTTPサーバよりアップデートファイルを提供する] チェックボックスのチェックを外して、ミラーへのアクセスを設定します。

共有フォルダがネットワーク内の別のコンピューターにある場合は、そのコンピューターへのアクセスに使用する認証データを指定する必要があります。認証データを指定するには、ESET File Security for Microsoft Windows Server の [詳細設定] (F5) を開き、[アップデート] をクリックします。[設定...] ボタンをクリックし、[LAN] タブをクリックします。この設定は、「LANへの接続」に記載されている更新の場合と同じです。

ミラーの設定が完了したら、ワークステーションにアクセスし、アップデートサーバとして¥¥UNC¥PATHを設定します。この操作を完了するには、次の手順を実行します。

●ESET製品の [詳細設定] を開き、[アップデート] をクリックします。
●[アップデートサーバ] の横の [編集] をクリックし、¥¥UNC¥PATHという形式で新しいサーバを追加します。
●アップデートサーバのリストから、新しく追加したこのサーバを選択します。

››› NOTE

正しく動作するには、ミラーフォルダのパスをUNCパスとして指定する必要があります。マップされたドライブからのアップデートは動作しない場合があります。

■ ミラーアップデートの問題のトラブルシューティング

ほとんどの場合、ミラーサーバからのアップデート時に発生する問題は、ミラーフォルダのオプションが正しく指定されていないこと、ミラーフォルダへの認証データが正しくないこと、ミラーからアップデートファイルをダウンロードするローカルワークステーションが正しく設定されていないことのいずれかが原因です。また、これらの原因が組み合わさって、問題が発生することもあります。以下では、ミラーからのアップデート時に発生する可能性がある、よくある問題の概要を紹介します。

ESET File Security for Microsoft Windows Serverミラーサーバへの接続エラーが報告される—原因として、ローカルワークステーションのアップデートファイルのダウンロード元であるアップデートサーバ (ミラーフォルダのネットワークパス) が正しく指定されていないことが考えられます。フォルダを検証するには、Windowsの [スタート] メニューをクリックし、[ファイル名を指定して実行] をクリックしてフォルダ名を入力し、[OK] をクリックします。フォルダの内容が表示されます。

ESET File Security for Microsoft Windows Serverでユーザー名とパスワードが要求される—原因として、アップデートセクションで認証データ (ユーザー名とパスワード) が正しく入力されていないことが考えられます。ユーザー名とパスワードは、プログラムのアップデート元のアップデートサーバへのアクセスを許可するために使用されます。認証データが適切な形式で正しく入力されていることを確認してください。たとえば、ドメイン/ユーザー名またはワークグループ/ユーザー名および対応するパスワードです。"全てのユーザー"がミラーサーバにアクセス可能であっても、全てのユーザーがアクセスを許可されているわけではありません。"全てのユーザー"とは、全ての認証されていないユーザーを意味するのではなく、全てのドメインユーザーがフォルダにアクセスできることを意味します。つまり、"全てのユーザー"がフォルダにアクセス可能な場合でも、アップデートの設定セクションでドメインユーザー名とパスワードを入力する必要があります。

ESET File Security for Microsoft Windows Serverミラーサーバへの接続エラーが報告される—ミラーのHTTPバージョンへのアクセスについて定義されているポート上の通信がブロックされています。

4.3.2 アップデートタスクの作成方法

アップデートを手動で開始するには、メインメニューの [アップデート] をクリックした後で、[ウイルス定義データベースをアップデートする] をクリックします。

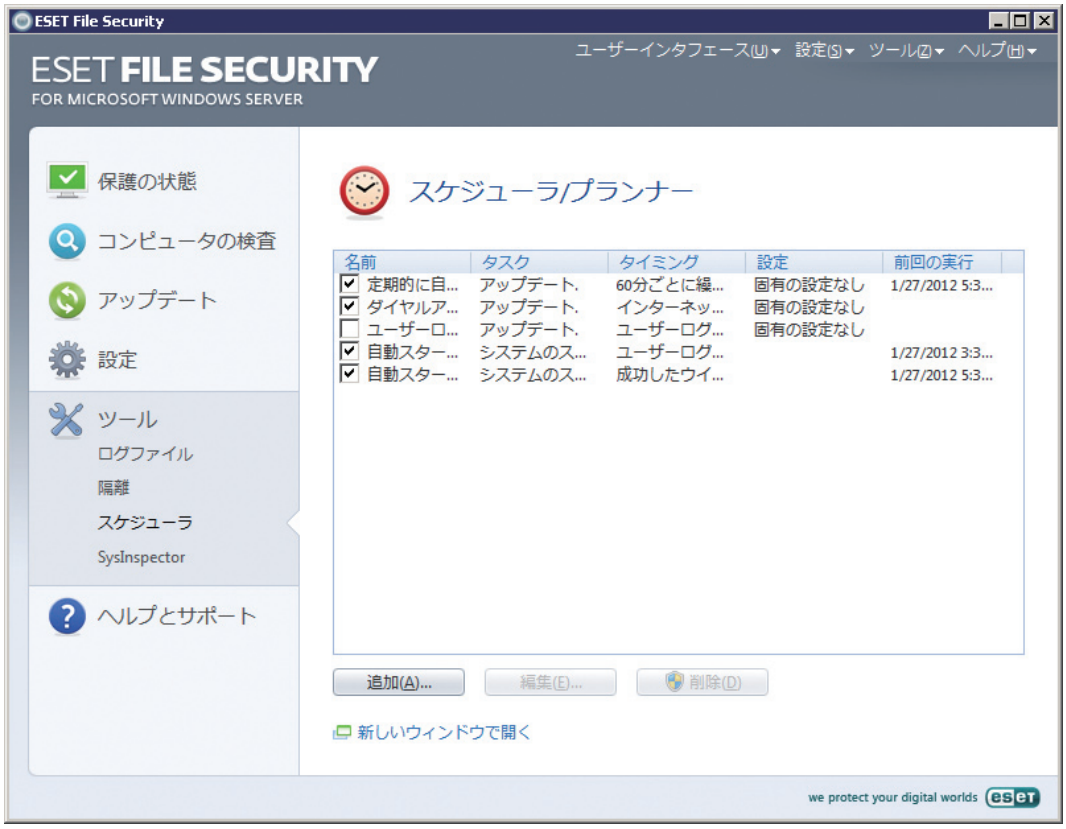
アップデートはスケジュールされたタスクとしても実行できます。スケジュールされたタスクを設定するには、[ツール] > [スケジューラ] をクリックします。ESET File Security for Microsoft Windows Serverでは、次のタスクが既定で有効になっています。

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

4.4 スケジューラ

スケジューラは、ESET File Security for Microsoft Windows Serverのメインメニューの[ツール]にあります。スケジューラには、スケジュール済みの全てのタスクと設定プロパティ(あらかじめ定義した日付、時刻、使用する検査プロファイルなど)の一覧が表示されます。



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。

●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)
●自動スタートアップファイルのチェック(成功したウイルス定義データベースのアップデート)

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

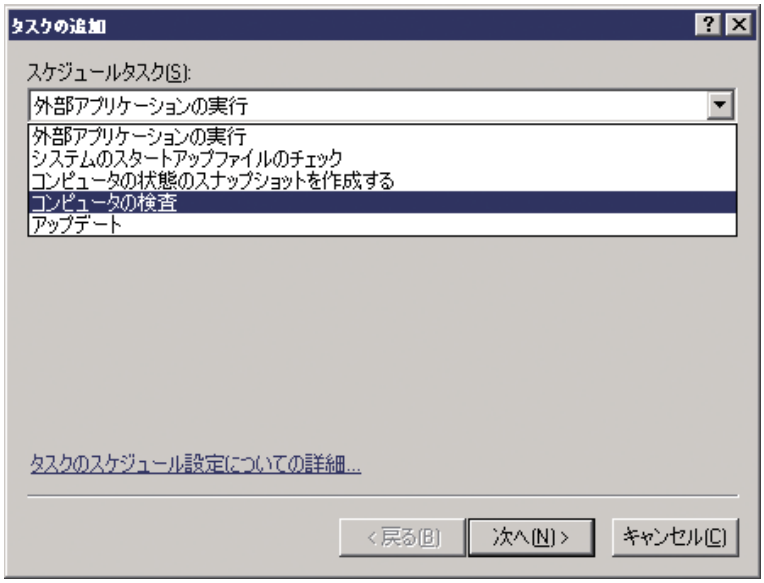
4.4.1 タスクをスケジュールする目的

スケジューラでは、スケジュールされたタスクが、あらかじめ定義された設定やプロパティと共に管理され、開始されます。設定およびプロパティには、日時のほか、タスクの実行時に使用される所定のプロファイルなどの情報が含まれます。

4.4.2 新しいタスクの作成

スケジューラで新しいタスクを作成するには、[追加...] ボタンをクリックするか、または右クリックしてコンテキストメニューから [追加...] を選択します。次の5種類のスケジュールされたタスクが使用可能です。

●外部アプリケーションの実行
●システムのスタートアップファイルのチェック
●コンピュータの状態のスナップショットの作成する
●コンピュータの検査
●アップデート



スケジュールされたタスクの中で最もよく使用されるのが [アップデート] です。[アップデート] を例にして新しいアップデートタスクを追加する方法を説明します。

[スケジュールタスク] ドロップダウンメニューから [アップデート] を選択します。[次へ] をクリックし、[タスク名] フィールドにタスクの名前を入力します。タスクの頻度を選択します。使用可能なオプションは次のとおりです。[1回]、[繰り返し]、[毎日]、[毎週]、および [イベントの発生時] です。選択された頻度に基づいて、さまざまな更新パラメーターが提示されます。次に、スケジュールされた時刻にタスクを実行できない場合や完了できない場合に実行するアクションを定義することができます。次の3つのオプションが使用可能です。

●次のスケジュール設定日時まで待機する
●実行可能になりしだい実行
●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（[タスクの実行間隔] スクロールボックスで、間隔を定義することができます）。

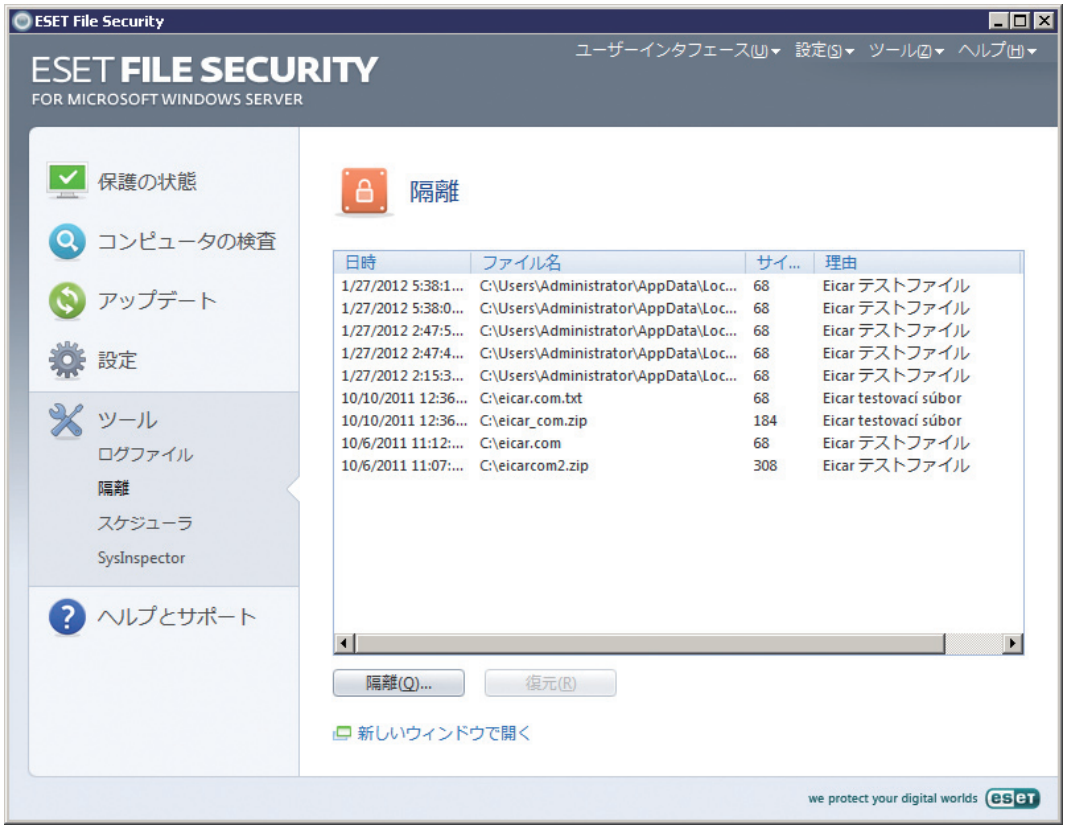
次のステップでは、現在のスケジュールされたタスクに関する情報の概要ウィンドウが表示されます。[固有のパラメータを使用してタスクを実行する] チェックボックスは自動的にチェックされます。[終了] ボタンをクリックします。

ダイアログウィンドウが表示され、スケジュールされたタスクに使用するプロファイルを選択することができます。ここでは、アップデートに使用するプロファイルとアップデートに使用するセカンダリプロファイルを指定することができます。セカンダリプロファイルは、プライマリプロファイルを使用してタスクを実行できない場合に使用されます。[アップデートプロファイル] ウィンドウで [OK] をクリックして確認します。新しくスケジュールされたタスクが、現在スケジュールされているタスクのリストに追加されます。

4.5 隔離

隔離の主な役割は、感染ファイルを安全に保存することです。ファイルを駆除できない場合、ファイルの削除が安全でないまたは推奨されない場合、あるいはESET File Security for Microsoft Windows Serverで誤って検出された場合、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もできます。これは、ファイルの動作が疑わしいにもかかわらず、ウイルス対策スキャナによって検出されない場合にお勧めします。隔離したファイルは、ESETのウイルスラボに提出して分析を受けることができます。



隔離フォルダーに保存されているファイルは、隔離の日時、感染ファイルの元の場所のパス、ファイルサイズ（バイト単位）、理由（"ユーザーによって追加されました"など）、およびウイルスの合計（複数のマルウェアを含むアーカイブの場合など）を表示するテーブルで参照することができます。

4.5.1　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、ESET File Security for Microsoft Windows Serverにより自動的に隔離されます（警告ウィンドウでユーザーがこのオプションをキャンセルしなかった場合）。必要に応じて、[隔離...] ボタンをクリックして不審なファイルを手動で隔離することもできます。この場合、対象のファイルは元の場所から削除されません。この操作にはコンテキストメニューも使用することができます。[隔離] ウィンドウ内で右クリックし、[隔離...] を選択します。

4.5.2　隔離フォルダからの復元

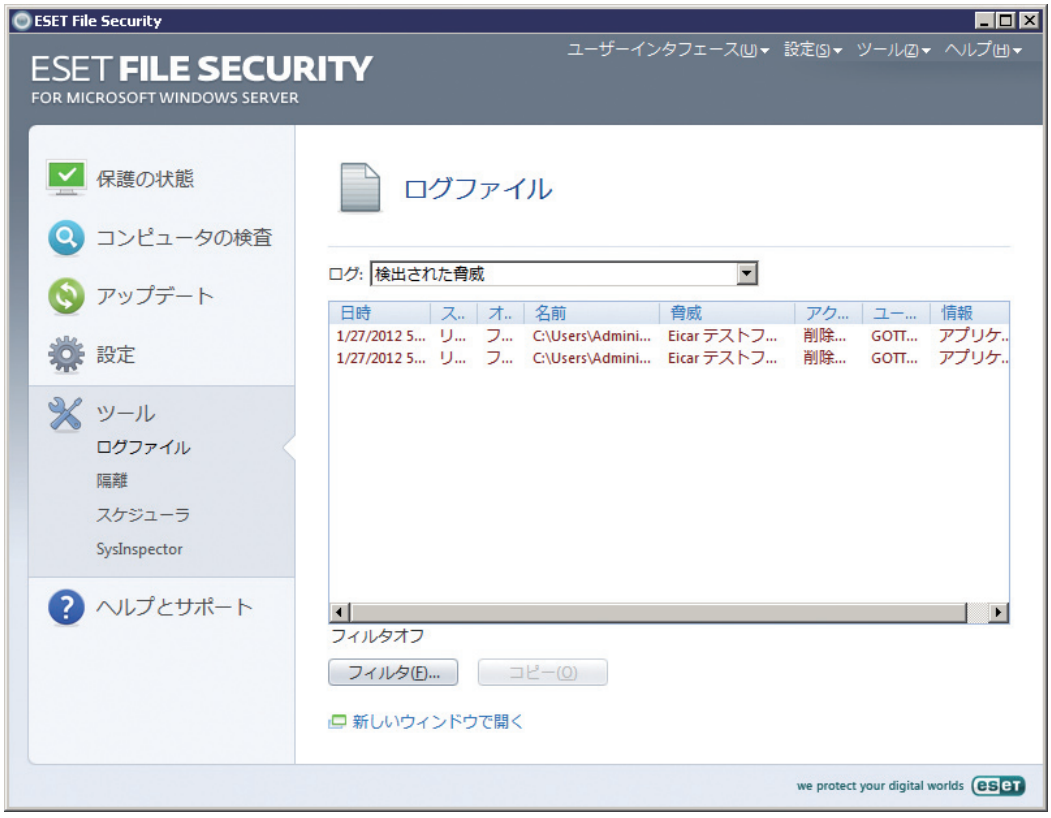
隔離されているファイルを、元の場所に復元することができます。この操作には、[復元] 機能を使用します。[復元] は、[隔離] ウィンドウで特定のファイルを右クリックして、コンテキストメニューから選択することができます。コンテキストメニューには、[復元先を指定] オプションもあります。このオプションを使用すると、隔離される前の場所とは異なる場所にファイルを復元することができます。

▸▸▸ NOTE

害のないファイルが誤って隔離された場合は、そのファイルを復元した後でスキャンから除外してください。

4.6 ログファイル

ログファイルには、発生した全ての重要なプログラムイベントに関する情報や、検出されたウイルスの概要が表示されます。ログは、システムの分析、ウイルスの検出、およびトラブルシューティングで重要なツールとして使用されます。ログへの記録はバックグラウンドでアクティブに実行され、ユーザーの操作を必要としません。情報は、ログの詳細レベルに関する現在の設定に基づいて記録されます。ESET File Security for Microsoft Windows Server環境からテキストメッセージとログを直接表示することができます。



ログファイルにアクセスするには、メインメニューで [ツール] > [ログファイル] をクリックします。ウィンドウの最上部にある [ログ] ドロップダウンメニューを使用して、目的のログの種類を選択します。使用可能なログは次のとおりです。

検出された脅威	このオプションを選択すると、マルウェアの検出に関連する情報が表示されます。
イベント	このオプションは、システム管理者およびユーザーが問題を解決するために使用します。イベントログには、ESET File Security for Microsoft Windows Serverによって実行された全ての重要なアクションが記録されます。
コンピュータの検査	このウィンドウには、完了した全ての検査結果が表示されます。エントリーをダブルクリックすると、検査結果の詳細がそれぞれ表示されます。

各セクションで、エントリーを選択し、[コピー] ボタンをクリックすると、表示されている情報をクリップボードに直接コピーすることができます。CTRLキーおよびSHIFTキーを使用して複数エントリを選択できます。

4.6.1　ログのフィルタ

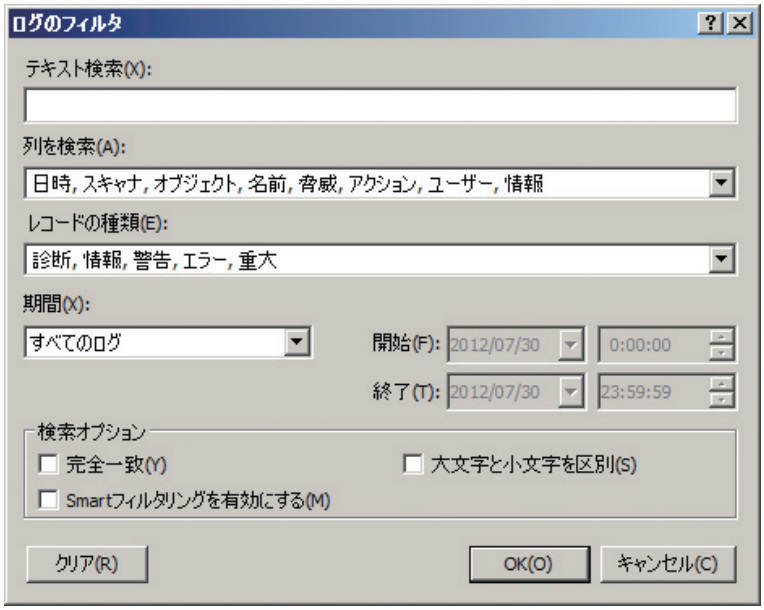
ログのフィルタは、ログファイルのレコードの中から必要なレコードのみを抽出することのできる便利な機能です。レコード件数が多い場合、特に威力を発揮します。

フィルタリングでは、フィルタする対象文字列の入力、調べるカラムの指定、レコードの種類の選択、期間の設定を行ってレコードの数を絞り込むことができます。フィルタオプションを指定すると、その条件に該当するレコードのみが [ログファイル] ウィンドウに表示され、効率的にログを調べることができます。

[ログのフィルタ] ウィンドウを開くには、[ツール] > [ログファイル] にある [フィルタ...] ボタンを1回押すか、またはショートカットキーのCtrl+Shift+Fを使用します。

NOTE

特定のレコードを検索するには、フィルタの代わりにログ内検索機能を使用すると便利です。フィルタで絞り込んだレコード群を対象にログ内検索を実行するという二段階の検索も可能です。



フィルタオプションを指定すると、その条件に該当するレコードのみが [ログファイル] ウィンドウに表示されます。この結果、レコードの除外と絞り込みが行われて、目的のレコードを見つけやすくなります。使用するフィルタオプションが詳細であればあるほど、結果がさらに絞り込まれます。

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表示されます。可読性を向上させるために、それ以外のレコードは表示されません。

列を検索

フィルタリングの検査対象にするカラムを選択します。フィルタリングに使用するカラムはいくつでも選択できます。既定では、イベントログでは、すべてのカラムのチェックボックスが選択されています。

●日時
●機能
●イベント

●ユーザー

レコードの種類
表示するレコードの種類を選択できます。特定の1種類のレコードを選択することも、複数の種類を同時に選択することも、すべての種類のレコードを表示する（既定）こともできます。

●診断
●情報
●警告
●エラー
●重大

期間
期間でレコードをフィルタする場合にこのオプションを使用します。次のいずれかを選択できます。

●ログ全体（既定）―期間によってフィルタせず、ログ全体を表示します。
●前日―前日から現在までのログを表示します。前日分のログは含みません。
●先週―先週から現在までのログを表示します。先週分のログは含みません。
●先月―先月から現在までのログを表示します。先月分のログは含みません。
●期間―期間を選択すると、期間（日時）を正確に指定して、指定した期間内に生成されたレコードのみを表示できます。

上記のフィルタリング設定以外にも複数のオプションがあります。

完全一致のみ	[対象]テキストボックスで指定した文字列と単語として完全に一致するレコードのみを表示します。
大文字と小文字を区別	大文字と小文字を含めて[対象]テキストボックスの文字列と一致するレコードのみを表示します。
Smartフィルタリングを有効にする	ESET File Security for Microsoft Windows Server独自の方法によるフィルタリングを行う場合に、このオプションを使用します。

フィルタリングオプションを設定し終えたら、[OK] ボタンを押してフィルタを適用します。フィルタオプションの条件に該当するレコードのみが [ログファイル] ウィンドウに表示されます。

4.6.2 ログ内検索

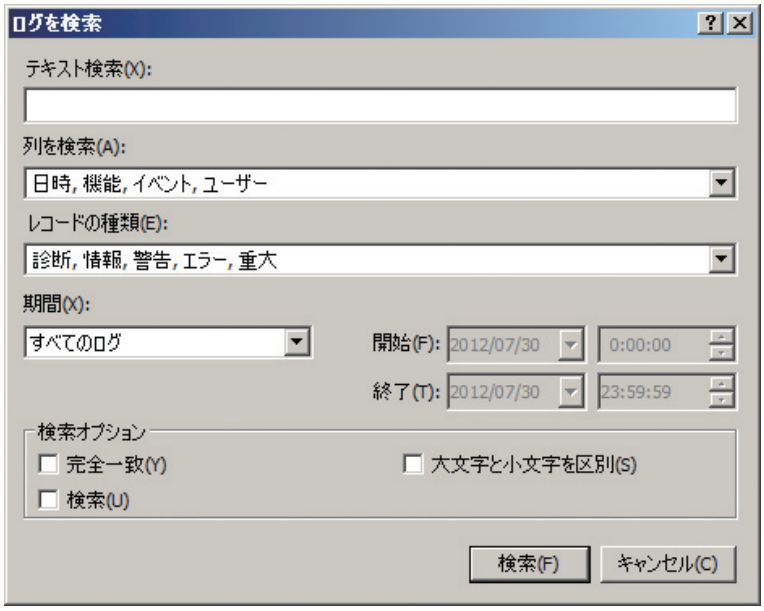
ログのフィルタに加えてログファイル内の検索機能も使用できます。この機能は、ログのフィルタから独立して使用することもできます。ログ内の特定のレコードを探す場合に有用です。この検索機能は、ログのフィルタ同様、特にレコードが多すぎる場合などに、目的の情報を探すために役立ちます。

ログ内検索では、検索する対象文字列の入力、調べるカラムの指定、レコードの種類の選択、および期間内に生成されたレコードのみを検索するための期間の設定を行うことができます。一定の検索オプションを指定することによって、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] ウィンドウで検索されます。

ログ内を検索するには、Ctrl+Fキーを押して [ログ内検索] ウィンドウを開きます。

NOTE

ログ内検索機能はログのフィルタと組み合わせて使用できます。まず、ログのフィルタを使用してレコードを絞り込んでから、フィルタされたレコード内のみの検索を開始できます。



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。それ以外のレコードは表示されません。

列を検索

検索の対象にするカラムを選択します。検索に使用する1つ以上のカラムをチェックできます。既定では、すべてのカラムがチェックされています。

- 日時
- 機能
- イベント
- ユーザー

レコードの種類

検索するレコードの種類を選択できます。特定の1種類のレコードを選択することも、複数の種類を同時に選択することも、すべての種類のレコードを検索する（既定）こともできます。

●診断
●情報
●警告
●エラー
●重大

期間

特定の期間内のレコードのみを検索する場合に、このオプションを使用します。次のいずれかを選択できます。

●ログ全体（既定）―期間内で検索するのではなく、ログ全体を検索します
●前日―前日から現在までのログを表示します。前日分のログは含みません。
●先週―先週から現在までのログを表示します。先週分のログは含みません。
●先月―先月から現在までのログを表示します。先月分のログは含みません。
●期間―期間を選択すると、期間（日時）を正確に指定して、指定した期間内に生成されたレコードのみを検索できます。

上記の検索設定以外にも複数のオプションがあります。

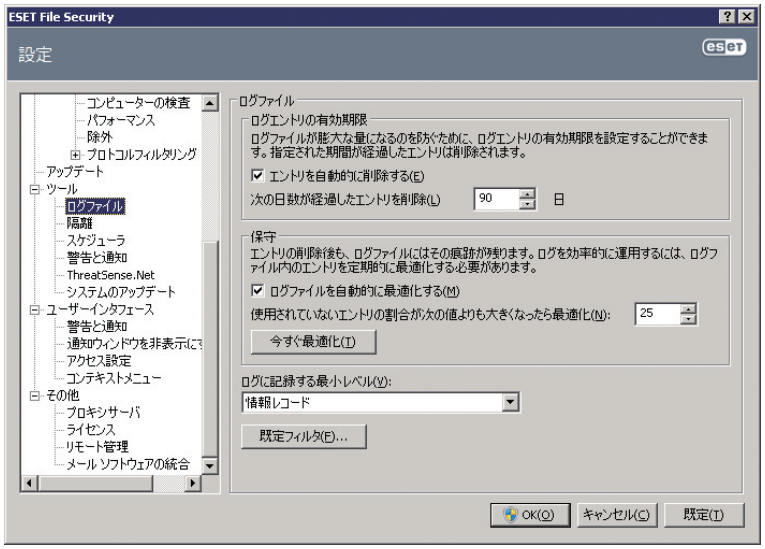
完全一致のみ	[対象]テキストボックスで指定した文字列と単語として完全に一致するレコードのみを検索します。
大文字と小文字を区別	大文字と小文字を含めて[対象]テキストボックスの文字列と一致するレコードのみを検索します。
上方向に検索	現在の位置から上方へ検索します。検索オプションを設定し終えたら、[検索]ボタンをクリックして検索を開始します。検索は、一致する最初のレコードが見つかった時点で停止されます。検索を続けるには、[検索]ボタンを再度クリックします。ログファイルは、現在の位置（強調表示されているレコード）を起点に、上から下へ検索されます。

4.6.3　ログの保守

ESET File Security for Microsoft Windows Serverのログの設定には、プログラムのメインウィンドウからアクセスすることができます。[設定]＞[環境設定で詳細な設定をする...]＞[ツール]＞[ログファイル] をクリックします。ログファイルの次のオプションを指定することができます。

●エントリを自動的に削除する
　指定した日数より古いログエントリが自動的に削除されます。
●ログファイルを自動的に最適化する
　未使用のレコードが指定した割合を超えると、ログファイルが自動的に最適化されます。
●ログに記録する最小レベル
　ログに記録する最小レベルを指定します。次のオプションを使用することができます。

診断レコード	プログラムの詳細な調整に必要な全ての情報と下記の全てのレコードを記録します。
情報レコード	アップデートの成功メッセージを含むすべての情報メッセージと下記のすべてのレコードを記録します。
警告	重大なエラー、エラー、および警告メッセージを記録します。
エラー	"ファイルのダウンロードエラー "などのエラーメッセージと致命的なエラーのみを記録します。
重大な警告	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。



4.7 ESET SysInspector

4.7.1 ESET SysInspectorの概要

ESET SysInspectorは、お使いのコンピューターを徹底的に検査し、収集されたデータを総合的に表示するアプリケーションです。インストールされているドライバやアプリケーション、ネットワーク接続、重要なレジストリエントリなどの情報は、疑わしいシステム動作（ソフトウェアやハードウェアの互換性の問題やマルウェア感染によるものなど）の調査に役立てることができます。

ESET SysInspectorにアクセスする方法は2通りあります。ESET File Security for Microsoft Windows Serverの統合バージョンを使用するか、またはユーザーズサイトから無償のスタンドアロンバージョン（SysInspector.exe）をダウンロードします。[ESET SysInspector] を開くには、[Tools] > [ESET Sys Inspector] をクリックします。どちらのバージョンも機能的には同じであり、同一のプログラムコントロールをもっています。ダウンロード用バージョンと統合バージョンのどちらでも、システムスナップショットを.xmlファイルにエクスポートし、ディスクに保存することができます。ただし、統合バージョンでは、[ツール] > [ESET SysInspector] を使って、システムスナップショットを直接保存することもできます。

ESET SysInspectorによるコンピュータの検査には少々時間がかかります。ご使用のハードウェアの設定、オペレーティングシステム、およびコンピューターにインストールされているアプリケーションの数に応じて、数十秒から数分かかると思われます。

NOTE

弊社ユーザーズサイトは、以下のURLからアクセスできます。

http://canon-its.jp/product/eset/users/

4.7.1.1 ESET SysInspectorの起動

[スタート] メニューからESET SysInspectorを実行できます（[プログラム] > [ESET] > [ESET File Security]）。アプリケーションがシステムを検査している間、お待ちください。お使いのハードウェアと収集されるデータによって異なりますが、これには数十秒から数分間かかる可能性があります。

4.7.2 ユーザーインターフェースとアプリケーションの使用

メインウィンドウは、使いやすいように4つの主要セクションに分かれています。プログラムのコントロールはメインウィンドウの上部、ナビゲーションウィンドウは左側、説明ウィンドウは中央右側、詳細ウィンドウはメインウィンドウの下部右側にそれぞれ配置されています。ログ状況のセクションには、ログの基本パラメータ（使用されているフィルタ、フィルタタイプ、ログは比較の結果かどうかなど）が一覧表示されます。

4.7.2.1 プログラムコントロール

ここでは、ESET SysInspectorで使用可能なすべてのプログラムコントロールについて説明します。

❶ファイル

[ファイル] をクリックすると、後で調査するために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。公開を目的としている場合は、[送信に適した形式] でログを生成することをお勧めします。この形式のログでは、機密情報（現在のユーザ名、コンピューター名、ドメイン名、現在のユーザ特権、環境変数など）は省かれます。

NOTE

以前に保存したESET SysInspectorレポートをメインウィンドウにドラッグアンドドロップするだけで、それらのレポートを開くことができます。

❷ツリー

すべてのノードを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。

❸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さまざまな機能が含まれます。

❹ヘルプ

アプリケーションとその機能に関する情報が含まれます。

❺詳細

この設定は、メインウィンドウに表示される情報に影響し、情報を処理しやすくします。"基本"モードでは、システム内の一般的な問題に対する解決策を見つけるための情報にアクセスできます。"中間"モードでは、あまり一般的でない詳細が表示されます。"完全"モードのESET SysInspectorでは、極めて具体的な問題の解決に必要な全ての情報が表示されます。

❻アイテムのフィルタリング

アイテムのフィルタリングは、システム内の疑わしいファイルまたはレジストリエントリを見つけるために最もよく使用される方法です。スライダを調整することで、リスクレベルによってアイテムをフィルタできます。スライダーを最左端（リスクレベル1）にすると、全ての項目が表示されます。スライダを右に動かすと、現在のリスクレベルより低いリスクレベルのアイテムが除外され、表示されたレベルのアイテムよりも疑わしいアイテムのみが表示されます。スライダーを最右端にすると、既知の有害な項目のみが表示されます。

リスク6～9に分類されている全ての項目には、セキュリティリスクが生じる可能性があります。ESETの何らかのセキュリティソリューションを使用していない場合は、ESET SysInspectorでそのようなアイテムが見つかった後、ESET Online Scannerでシステムを検査することをお勧めします。ESET Online Scannerは無料のサービスです。

▸▸▸ NOTE

項目のリスクレベルは、項目の色とリスクレベルのスライダーの色を比べることにより迅速に判別できます。

❼検索

[検索] を使用して、特定のアイテムを、その名前または名前の一部によって簡単に見つけることができます。検索要求の結果は、説明ウィンドウに表示されます。

❽戻る

左矢印または右矢印をクリックすることで、説明ウィンドウ内で前に表示された情報に戻ることができます。左矢印と右矢印をクリックする代わりに、それぞれBackSpaceキーとスペースキーを使用できます。

❾ステータスセクション

ナビゲーションウィンドウ内の現在のノードを表示します。

重要

赤で表示されているアイテムは、プログラムによって潜在的な危険性があるとマークされた不明アイテムです。項目が赤で表示されている場合でも、ファイルの削除が可能であることを自動的に意味する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、または不要かどうかを確認してください。

4.7.2.2 ESET SysInspectorにおけるナビゲーション

ESET SysInspectorでは、さまざまな種類の情報が、ノードと呼ばれる複数の基本セクションに分けられています。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、またはノードの名前の横にあるまたはをクリックします。ナビゲーションウィンドウでノードおよびサブノードのツリー構造内を参照すると、説明ウィンドウに各ノードのさまざまな詳細情報が表示されます。説明ウィンドウでアイテムを参照すると、各アイテムの追加の詳細情報が詳細ウィンドウに表示されます。

ナビゲーションウィンドウのメインノード、および説明ウィンドウと詳細ウィンドウの関連情報についての説明を次に示します。

[実行中のプロセス]

このノードには、ログの生成時に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。説明ウィンドウには、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の名前、ファイルのリスクレベルなど、各プロセスに関する追加の詳細情報が表示されます。

詳細ウィンドウには、ファイルサイズやハッシュなど、説明ウィンドウで選択した項目に関する追加情報が表示されます。

››› NOTE

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、毎日24時間稼動し、他のユーザーアプリケーションに対して基本的かつ重要な機能を提供します。場合によっては、ESET SysInspectorツールに表示されるそれらのプロセスのファイルパスが¥??¥で始まることもあります。これらの記号はプロセスの起動前最適化を可能にするもので、システムにとって安全です。

[ネットワーク接続]

説明ウィンドウには、ナビゲーションウィ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、アプリケーションの接続先となるリモートアドレスと共に表示されます。DNSサーバのIPアドレスをチェックすることもできます。

詳細ウィンドウには、ファイルサイズやハッシュなど、説明ウィンドウで選択した項目に関する追加情報が表示されます。

[重要なレジストリエントリ]

スタートアッププログラムやブラウザヘルパオブジェクト（BHO）を指定するものなど、システムに関するさまざまな問題に関連することが多い選択されたレジストリエントリのリストが表示されます。

説明ウィンドウには、特定のレジストリエントリにどのファイルが関連しているかが示されます。詳細ウィンドウでは、追加の詳細情報を確認できます。

[サービス]

説明ウィンドウには、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。詳細ウィンドウで、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を確認できます。

[ドライバ]

システムにインストールされているドライバのリストです。

[重大なファイル]
説明ウィンドウには、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。

[システム情報]
ハードウェアとソフトウェアに関する詳細情報、およびESET環境変数とユーザ権限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、説明ウィンドウと詳細ウィンドウに表示されます。

バージョン情報
ESET SysInspectorに関する情報です。

4.7.2.3 比較

比較機能を使用すると、ユーザーは既存の2つのログを比較できます。この機能により、両方のログで共通していない一連のアイテムが表示されます。システムの変更を追跡するには、この機能が適しています。これは、悪意のあるコードの活動を検出するのに有用なツールです。

起動後、新しいログが作成され、新しいウィンドウに表示されます。[ファイル]＞[ログの保存]に移動して、ログをファイルに保存します。これで、ログファイルを後で開いて表示できるようになります。既存のログを開くには、[ファイル]＞[ログを開く]メニューを使用します。ESET SysInspectorのメインプログラムウィンドウで一度に表示できるログは1つです。

2つのログの比較には、現在アクティブなログと、ファイルに保存されているログを表示できるという利点があります。ログを比較するには、[ファイル]＞[ログの比較]オプションを使用し、[ファイルの選択]を選択します。プログラムのメインウィンドウで、選択したログがアクティブなログと比較されます。比較ログには、2つのログの相違のみが表示されます。

NOTE
2つのログファイルを比較する場合は、[ファイル]->[ログの保存]を選択し、ログをZIPファイルとして保存します。これで、両方のファイルが保存されます。後でそのファイルを開くと、保存されているログが自動的に比較されます。

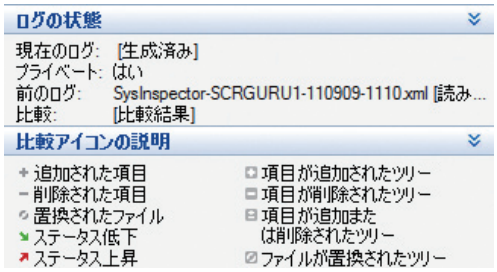
表示されたアイテムの横に、比較対象のログの相違を示す記号がESET SysInspectorによって表示されます。
－のマークの付いた項目はアクティブログのみに見つかり、開かれた比較ログには見つからなかったものです。＋が付いているアイテムは、開かれているログにのみ存在し、アクティブなログには存在しないものです。

項目の横に表示される全ての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構造セクション
－ 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構造セクション
◇ 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構造セクション
↘ リスクレベルが、以前のログよりも低下している

リスクレベルが、以前のログよりも上昇している

左下隅に表示される説明セクションでは、全ての記号が説明され、比較対象のログの名前も表示されます。



比較ログはいずれもファイルに保存して、後で開くことができます。

例
システムに関する初期情報を記録したログを生成して、previous.xmlという名前のファイルに保存します。システムに変更を行った後、ESET SysInspectorを開いて、新しいログを生成します。current.xmlという名前のファイルにログを保存します。

これら2つのログの相違を追跡するには、[ファイル] > [ログの比較] に移動します。2つのログの相違を示した比較ログが作成されます。

次のコマンドラインオプションを使用した場合も同様の結果が得られます。

SysIsnpector.exe current.xml previous.xml

4.7.3 コマンドラインパラメータ

ESET SysInspectorでは、次のパラメータを使用してコマンドラインからレポートを生成できます。

/gen	GUIを実行せずにコマンドラインから直接ログを生成します。
/privacy	機密情報を除外してログを生成します。
/zip	生成されたログを圧縮ファイルとして直接ディスクに格納します。
/silent	ログ生成の進捗状況バーは表示されません。
/help,/?	コマンドラインパラメータに関する情報を表示します。

例
特定のログを直接ブラウザに読み込むには、次のように指定します。SysInspector.exe"c:¥clientlog.xml"ログを現在の場所に生成するには、次のように指定します。SysInspector.exe/genログを特定のフォルダに生成するには、次のように指定します。SysInspector.exe/gen="c:¥folder¥"ログを特定のファイル/場所に生成するには、次のように指定します。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には、次のように指定します。SysInspector.exe/gen="c: ￥mynewlog.zip"/privacy/zip
2つのログを比較するには、次のように指定します。SysInspector.exe"current.xml""original.xml"

NOTE

ファイル/フォルダの名前に空白が含まれている場合は、名前を引用符(逆コンマ)で囲む必要があります。

4.7.4　サービススクリプト

サービススクリプトは、ESET SysInspectorを使用するユーザーがシステムから不要なオブジェクトを簡単に削除できるよう手助けをするツールです。

サービススクリプトを使用すると、ユーザーはESET SysInspectorログの全体、または選択した部分をエクスポートできます。エクスポートした後、不要なオブジェクトに削除対象のマークを付けることができます。その後、修正したログを実行して、マークを付けたオブジェクトを削除できます。

サービススクリプトは、過去にシステムの問題を診断した経験のある上級ユーザー向けです。そうではないユーザが変更を行うと、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。

例
コンピューターが、ご使用の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は、次の手順を実行してください。

●ESETSysInspectorを実行して、システムスナップショットを新規に生成します。
●ツリー構造の左側のセクションで最初の項目を選択して、Ctrlキーを押しながら最後の項目を選択し、全ての項目をマークします。
●選択したオブジェクトを右クリックして、[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] コンテキストメニューオプションを選択します。
●選択したオブジェクトが新しいログにエクスポートされます。これは、手順全体の中で最も重要なステップです。新しいログを開いて、削除対象のすべてのオブジェクトの-属性を+に変更します。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にマークが付いていないことを確認してください。
●ESET SysInspectorを開き、[ファイル] > [サービススクリプトの実行] をクリックして、スクリプトへのパスを入力します。
●[OK] をクリックしてスクリプトを実行します。

4.7.4.1　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のメインウィンドウで、メニューツリー（左ペイン）の任意のアイテムを右クリックします。コンテキストメニューで、[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] オプションまたは [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] オプションを選択します。

››› NOTE

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。

4.7.4.2　サービススクリプトの構造

スクリプトのヘッダの最初の行には、エンジンバージョン（ev）、GUIバージョン（gv）、およびログバージョン（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。スクリプトのこの部分は変更しないでください。

ファイルの残りの部分は、複数のセクションに分かれており、そこでアイテムを編集する（つまり、アイテムがスクリプトによって処理されることを示す）ことができます。アイテムの前にある"-"記号を"+"記号に置き換えることで、アイテム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) :

このセクションには、システム内で実行されているすべてのプロセスのリストが含まれます。各プロセスは、そのUNCパスと、それに続くアスタリスク (*) 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、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) :

このセクションには、現在使用されているシステムモジュールのリストが示されます。

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"+"でマークされています。スクリプトが実行されると、この特定のモジュールを使用しているプロセスが認識され、それらが終了されます。

03) TCP connections (TCP接続) :

このセクションには、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
[...]

スクリプトを実行すると、マークされたTCP接続内のソケットの所有者が見つけられ、ソケットが停止されて、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) :

このセクションには、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) [...]

スクリプトが実行されると、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サーバ関連のエントリ):
このセクションには、現在のDNSサーバ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 [...]

スクリプトが実行されると、マークされたDNSサーバエントリが削除されます。

06) Important registry entries (重大なレジストリエントリ):
このセクションには、重要なレジストリエントリ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/ [...]

スクリプトが実行されると、マークされたエントリが削除されるか、0バイト値に縮小されるか、またはその既定値にリセットされます。特定のエントリに適用されるアクションは、エントリのカテゴリと特定のレジストリのキー値によって異なります。

07) Services (サービス):
このセクションには、システム内の登録済みサービスのリストが示されます。

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
[...]

スクリプトが実行されると、マークされたサービスとそれらの依存サービスは停止され、アンインストールされます。

08) Drivers (ドライバ) :
このセクションには、インストール済みのドライバのリストが示されます。

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
[...]

スクリプトが実行されると、選択したドライバがシステムから登録解除され、削除されます。

09) Critical files (不可欠なファイル) :
このセクションには、オペレーティングシステムが正常に機能するために不可欠なファイルに関する情報が含まれます。

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
-::1localhost
[...]

選択したアイテムは、削除されるか、またはその元の値にリセットされます。

4.7.4.3 サービススクリプトの実行

目的のアイテムをすべてマークし、スクリプトを保存して閉じます。[ファイル] メニューの [サービススクリプトの実行] オプションを選択して、ESET SysInspectorのメインウィンドウから、編集したスクリプトを直接実行します。スクリプトを起動すると、次のような内容のメッセージが表示されます。「サービススクリプト"%Scriptname% "を実行しますか?」これを確認すると、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別の警告が表示される場合があります。[実行] をクリックしてスクリプトを起動します。ダイアログウィンドウに、スクリプトが正常に実行されたことが示されます。スクリプトの一部だけが処理された可能性がある場合、次のような内容のメッセージがダイアログウィンドウに表示されます。「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?」[はい] を選択して、実行されなかった操作が記載されている複雑なエラーレポートを表示します。

スクリプトが認識されなかった可能性がある場合、次のような内容のメッセージがダイアログウィンドウに表示されます。「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?」これは、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。スクリプトファイルを再度開いてスクリプト内のエラーを修正するか、または新しいサービススクリプトを作成します。

4.7.5 ショートカット

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

生成

Ctrl+G	標準のシステムステータスの確認
Ctrl+H	機密情報をログに記録する可能性もあるシステムチェックを実行します

項目のフィルタリング

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

表示

Ctrl+5	ベンダによる表示、全てのベンダ
Ctrl+6	ベンダによる表示､Microsoftのみ
Ctrl+7	ベンダによる表示、他の全てのベンダ
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、項目の元の場所に移動します
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を開きます
Ctrl+R	該当するエントリをレジストリエディタで開きます
Ctrl+Z	ファイルまで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	全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（ログには現在のログにある項目が表示されます）
Ctrl+Alt+3	削除された項目のみを表示します（ログには前回のログにある項目が表示されます）
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

4.7.6 FAQ

01 ESET SysInspectorを実行するには管理者特権が必要ですか？

ESET SysInspectorを実行するには管理者特権は必要ありませんが、収集される情報の中には管理者アカウントからのみアクセスできるものもあります。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。

02 ESET SysInspectorではログファイルが作成されますか？

ESET SysInspectorでは、コンピュータの設定のログファイルを作成できます。このログファイルを保存するには、メインメニューの［ファイル］>［ログを保存］を選択します。ログはXML形式で保存されます。既定では、ファイルは% USERPROFILE%¥My Documents¥ディレクトリに保存されます。ファイルの命名規則は、SysInpsector-% COMPUTERNAME% -YYMMDD-HHMM.XMLとなります。ログファイルを保存する前に、そのファイルの場所と名前を、必要に応じて別のものに変更できます。

03 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で作成されたログファイルを表示するには、プログラムを実行し、メインメニューで［ファイル］>［ログを開く］を選択します。ログファイルをESET SysInspectorアプリケーションにドラッグアンドドロップすることもできます。ESET SysInspectorのログファイルを頻繁に表示する必要がある場合は、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。こうしておくと、ログファイルをこの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。セキュリティ上の理由で、Windows VistaとWindows7では異なるセキュリティアクセス許可を持つウィンドウ間でのドラッグアンドドロップが許可されない場合があります。

04 ログファイル形式の仕様は使用できますか？ SDKは使用できますか？

現時点では、プログラムは開発途中であるため、ログファイルの仕様やSDKは使用できません。プログラムのリリース後、カスタマのフィードバックと要望に基づいて提供する可能性があります。

05 ESET SysInspectorでは、特定のオブジェクトによってもたらされるリスクはどのように評価されますか？

多くの場合、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重み付けする一連のヒューリスティックルールを使用して、オブジェクト（ファイル、プロセス、レジストリキーなど）にリスクレベルを割り当てます。これらのヒューリスティックに基づいて、オブジェクトに1-良好（緑）9-危険（赤）のリスクレベルが割り当てられます。左側のナビゲーションペインでは、オブジェクトが持つ最大リスクレベルを基にセクションが色分けされます。

06 リスクレベル"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？

ESET SysInspectorの評価により、オブジェクトが悪意のあるものであることが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について動作が異常でないかどうかを詳細に検証する必要があるかを、迅速に判断できるように設計されています。

07 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？

多くのアプリケーションと同様に、ESET SysInspectorでは、このソフトウェアが公開済みのESETであり改変されていないことを保証できるようにするために、"証明書"へのデジタル署名を使用しています。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、Microsoft Windows下で動作する全てのデジタル署名プログラムの標準的な動作です。

08 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ものです。ルートキットとして動作する悪意のあるコードによってシステムが攻撃を受けると、ユーザーはデータの損傷や盗用などのリスクにさらされます。専用のルートキット対策ツールが無ければ、ルートキットの検出はほとんど不可能です。

09 "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、ESET SysInspectorは、まず、ファイルにデジタル署名が埋め込まれているかどうかを探します。埋め込まれていれば、ファイル内のIDが検証に使用されます。ファイルにデジタル署名がない場合、ESIは、処理する実行可能ファイルについての情報を含む、対応する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、そのCATファイルのデジタル署名が実行可能ファイルの検証プロセスに適用されます。

"MSによって署名済み"というマークのあるファイルが、異なる"会社名"エントリを持つ場合があるのはこのためです。例: Windows2000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。このアプリケーションの主要な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、そのファイルをMicrosoftによって署名されたファイルとマークします。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。

4.7.7 ESET File Security for Microsoft Windows Serverの機能としてのESET Sysinspector

ESET SysInspectorセクションをESET File Security for Microsoft Windows Serverで開くには、[ツール]>[ESET SysInspector] をクリックします。ESET SysInspectorウィンドウでの管理システムは、コンピュータ検査ログまたはスケジュールされたタスクの管理システムとほぼ同じです。システムのスナップショットを伴う全ての操作(作成、表示、比較、削除、エクスポート)には、1回または2回のクリックでアクセスできます。

ESET SysInspectorウィンドウには、作成時刻、短いコメント、スナップショットを作成したユーザの名前、およびスナップショットの状態など、作成されたスナップショットに関する基本的な情報が表示されます。

スナップショットを [比較]、[作成]、または [削除] するには、ESET SysInspectorウィンドウでスナップショットのリストの下にある、該当するボタンを使用します。これらのオプションはコンテキストメニューでも使用できます。選択したシステムスナップショットを表示するには、[表示] コンテキストメニューオプションを使用します。選択したスナップショットをファイルにエクスポートするには、スナップショットを右クリックして [エクスポート...] を選択します。

次に、使用可能なオプションについて詳しく説明します。

比較	既存の2つのログを比較できます。現在のログと以前のログの間の変更を追跡するのに適しています。このオプションを有効にするには、比較する2つのスナップショットを選択する必要があります。
作成	新しいレコードを作成します。この操作を実行するには、まずレコードに関する短いコメントを入力する必要があります。現在生成されているスナップショットの作成の進行状況を確認するには、[ステータス]カラムを参照してください。完了したスナップショットはすべて、作成済みの状態になります。
削除	エントリをリストから削除します。
エクスポート...	選択したエントリをXMLファイル(または圧縮バージョン)で保存します。

4.8 ESET SysRescue

ESET SysRescueは、ESET File Security for Microsoft Windows Serverを格納する起動可能なディスクを作成するためのユーティリティです。ESET SysRescueの主な利点は、ESET File Security for Microsoft Windows Serverがホストオペレーティングシステムから独立して稼動する一方で、ディスクおよびファイルシステム全体に直接アクセスできることにあります。本機能は、オペレーティングシステムの実行中では削除ができないマルウェアに対して効果を発揮します。

4.8.1 レスキュー CDの作成方法

ESET SysRescueウィザードを開始するには、[スタート]＞[プログラム]＞[ESET]＞[ESET FileSecurity]＞[ESET SysRescue]をクリックします。

まず、Windows AIKとブートメディアの作成に適したデバイスがあるかどうかがチェックされます。コンピューターにWindows AIKがインストールされていない場合（または破損していたり正しくインストールされていない場合）、インストールオプション、またはWindows AIKフォルダまでのパスを入力するオプションがウィザードに表示されます。

次のステップでは、ESET SysRescueを保存する対象のメディアを選択します。

4.8.2 対象の選択

CD/DVD/USBに加えて、ISOファイルにESET SysRescueを保存することもできます。後で、ISOイメージをCD/DVDに書き込むことができます。

対象メディアにUSBを選択した場合に、特定のコンピューターでブートが行われないことがあります。一部のBIOSバージョンでは、BIOSに関する問題が報告されることがあります。ブートマネージャの起動処理が終了し、次のエラーメッセージが表示されます。

ファイル:¥boot¥bcd
状態:0xc000000e
情報:ブート設定データの読み込み時にエラーが発生しました

このメッセージが表示された場合、USBメディアでなくCDを選択することをお勧めします。

4.8.3 設定

ESET SysRescueの作成を開始する前に、インストールウィザードでは、コンパイルパラメータがESET SysRescueウィザードの最終ステップで表示されます。それらのパラメータを変更するには、[変更...] ボタンをクリックします。使用可能なオプションは次のとおりです。

●フォルダ
●ESETアンチウイルス詳細
●インターネットプロトコル
●起動可能なUSBデバイス（対象のUSBデバイスの選択時）
●書き込み（対象のCD/DVDドライブの選択時）

MSIインストールパッケージを指定していなかったり、コンピューターにESETセキュリティソリューションをインストールしていないと、[作成] ボタンは使用できません。インストールパッケージを選択するには、[変更] ボタンをクリックして、[ESETアンチウイルス] タブに移動します。ユーザ名とパスワードを入力しなかった場合も（[変更] > [ESETアンチウイルス]）> [作成] ボタンは無効になります。

4.8.3.1 フォルダ

一時フォルダは、ESET SysRescueのコンパイル時に必要なファイルの作業ディレクトリです。ISOフォルダは、コンパイルの完了後に、生成されたISOファイルが保存されるフォルダです。このタブには、全てのローカルドライブとマッピングされているネットワークドライブ、および使用可能な空き領域がリストされます。表示されているフォルダの一部が、空き領域の不十分なドライブにある場合、十分な空き領域のある別のドライブを選択することをお勧めします。ディスクの空き領域が不足していると、コンパイルが途中で終了する場合があります。

外部アプリケーション	ESET SysRescueメディアから起動後に実行またはインストールする追加プログラムを指定できます。
外部アプリケーションを含める	外部プログラムをESET SysRescueのコンパイルに追加できます。
選択されたフォルダ	ESET SysRescueディスクに追加するプログラムを格納するフォルダです。

4.8.3.2 ESETウイルス対策

ESET SysRescue CDを作成する際、コンパイラが使用するESETファイルのソースとして、2種類を選択できます。

[ESSフォルダ] -ESET製品のインストール先フォルダにある既存ファイル。
[MSIファイル] -MSIインストーラに含まれているファイルが使用されます。次に、選択によっては、(Nup) ファイルの場所を更新できます。通常、既定オプション [ESS/EAVフォルダ/MSIファイル] が設定されているはずです。ウイルス定義データベースの古いバージョンまたは新しいバージョンを使用するためといった場合によっては、カスタムの [アップデートフォルダ] を選択してもかまいません。

ユーザ名とパスワードのソースとして、次の2つのうちのどちらかを使用できます。

インストール済みのESS/EAV-ユーザ名とパスワードは、現在インストールされているESET File Security for Microsoft Windows Serverからコピーされます。
ユーザ指定-該当するテキストボックスに入力されたユーザ名とパスワードが使用されます。

NOTE

ESET SysRescue CD上のESET File Security for Microsoft Windows Serverは、インターネットからか、またはESET SysRescue CDが実行されているコンピューターにインストールされているESET Securityソリューションからアップデートされます。

4.8.3.3 詳細設定

[詳細] タブでは、コンピューターのメモリ容量に従ってESET SysRescue CDを最適化できます。[576MB以上] を選択すると、CDのコンテンツがシステムメモリ (RAM) に書き込まれます。[576MB未満] を選択すると、WinPEが実行されるときに常にRecovery CDにアクセスされます。

[外部ドライバ] セクションでは、特定のハードウェア用のドライバ (通常はネットワークアダプタ) を挿入できます。WinPEは、幅広いハードウェアをサポートするWindows Vista SP1をベースにしていますが、時にはハードウェアが認識されないこともあります。そのようなときは、ドライバを手動で追加する必要があります。ESET SysRescueのコンパイルにドライバを追加するには、手動 ([追加] ボタン) と自動 ([自動検索] ボタン) の2つの方法があります。手動で追加する場合は、該当する.infファイルへのパスを選択する必要があります (適用可能な*.sysファイルがそのフォルダ内になければなりません)。自動的に追加する場合は、指定のコンピューターのオペレーティングシステムでドライバが自動的に検索されます。自動追加は、ESET SysRescue CDの作成先コンピューターで使用しているのと同じネットワークアダプタを備えたコンピューターで、ESET SysRescueを使用する場合にのみ使うことをお勧めします。作成時にESET SysRescueドライバがコンパイルに組み込まれるため、ユーザが後で検索する必要はありません。

4.8.3.4 インターネットプロトコル

ここでは、ESET SysRescueの後で、基本ネットワーク情報を設定し、事前定義接続を設定することができます。

IPアドレスをDHCP (動的ホスト構成プロトコル) サーバーから自動的に取得するには、[自動的にIPアドレスを取得する] を選択します。

あるいは、ネットワーク接続で、手動で指定したIPアドレス (静的IPアドレスとも呼ばれる) を使用することもできます。適切なIP設定を構成するには、[カスタム] を選択します。このオプションを選択する場合、[IPアドレス] を指定し、LANおよび高速インターネット接続の場合は [サブネットマスク] を指定する必要があります。[優先DNSサーバー] および [代替DNSサーバー] に、プライマリおよびセカンダリのDNSサーバーアドレスを入力します。

4.8.3.5 起動可能なUSBデバイス

対象のメディアとしてUSBデバイスを選択した場合、[起動可能なUSBデバイス] タブで、使用可能なUSBデバイスのいずれかを選択できます (複数のUSBデバイスがある場合)。

ESET SysRescueのインストール先として適切な対象 [デバイス] を選択します。

CAUTION

選択したUSBデバイスは、ESET SysRescueの作成時にフォーマットされます。デバイス上の全てのデータが削除されます。

[クイックフォーマット] オプションを選択した場合、フォーマットによりすべてのファイルが領域から除去されますが、ディスクの不良セクタは検査されません。USBデバイスが事前にフォーマット済みであって損傷を受けていないことが確実であれば、このオプションを使用します。

4.8.3.6 書き込み

書き込み先メディアとしてCDまたはDVDを選択した場合、[書き込み] タブで書き込みパラメータを追加指定できます。

[ISOファイルを削除する]	ESET SysRescue CDの作成後に一時ISOファイルを削除する場合、このチェックボックスをオンにします。
[削除有効]	高速消去と完全消去を選択できます。
[書き込みデバイス]	書き込みに使用するデバイスを選択します。

CAUTION

これは既定のオプションです。再書き込み可能なCD/DVDを使用した場合、CD/DVD上のすべてのデータが消去されます。

[メディア] セクションには、CD/DVDデバイス内のメディアに関する情報が表示されます。

[書き込み速度]	ドロップダウンメニューから速度を選択します。書き込み速度を選択する際には、書き込みデバイスの処理能力と使用するCD/DVDの種類を考慮に入れる必要があります。

4.8.4 ESET SysRescueの操作

レスキューCD/DVD/USBが効果的に機能するためには、ESET SysRescueブートメディアからコンピューターを起動する必要があります。ブートの優先度はBIOSで変更できます。また、コンピューターの起動時にブートメニューを使用することもできます。通常は、マザーボード/BIOSのバージョンによって、F9～F12のいずれかのキーを使用します。

ブートメディアからのブート後にESET File Security for Microsoft Windows Serverが起動します。ESET SysRescueが使用されるのは特定の状況に限られているので、通常のESET File Security for Microsoft Windows Serverバージョンにある保護モジュールやプログラム機能の中には不要なものもあります。それらは、[コンピュータの検査]、[アップデート] および [設定] の一部のセクションのみに絞り込まれます。ウイルス定義データベースをアップデートする機能は、ESET SysRescueの最も重要な機能です。コンピュータ検査を開始する前にこのプログラムをアップデートすることをお勧めします。

4.8.4.1 ESET SysRescueの使用

実行可能（.exe）ファイルを変更するウイルスがネットワーク内のコンピューターに感染したと仮定します。ESET File Securityは、多くの感染済みファイルを駆除できますが、起動中のファイルについては、セーフモードでＯＳを起動したうえで駆除を試みる必要があります。ただし、Windowsの基本プロセスの1つであるexplorer.exeなどは、セーフモードでも起動するため駆除が困難な場合があり、このような感染ファイルにはアクション（駆除・削除）が取れないため、感染したままになることもあります。

このようなケースでは、ESET SysRescueを使用することで問題を解決できることがあります。ESET SysRescueの起動には、ホストオペレーティングシステムのどのコンポーネントも必要ないので、ディスク上のどのファイルでも処理（駆除や削除）できるためです。

4.9 ユーザーインターフェース

ESET File Security for Microsoft Windows Serverのユーザーインターフェースの設定オプションを使用すると、各自のニーズに合わせて作業環境を調整することができます。こららの設定オプションは、ESET File Security for Microsoft Windows Serverの [詳細設定] ツリーの [ユーザーインターフェイス] からアクセスできます。

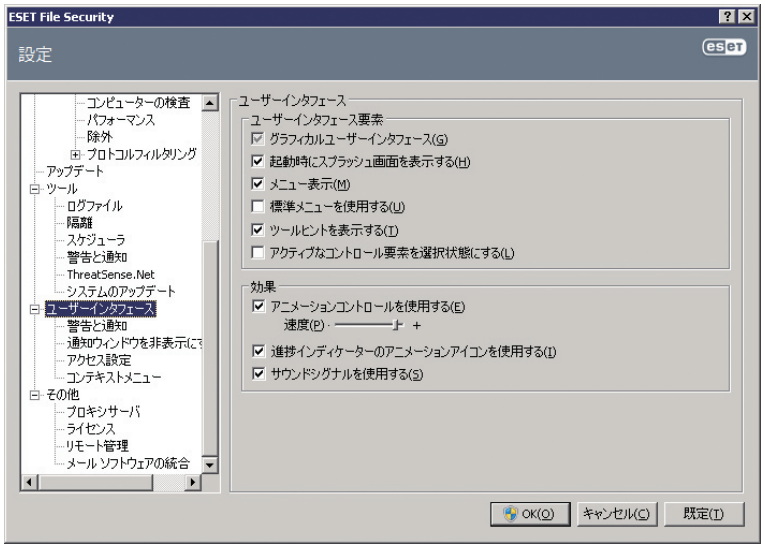
グラフィカル要素によってコンピューターのパフォーマンスが低下する場合や、その他の問題が発生する場合は、[グラフィカルユーザーインターフェース] オプションを無効にする必要があります。また、視覚に障害のあるユーザーの場合も、画面に表示されるテキストの読み上げ専用アプリケーションと競合するグラフィカルインタフェースをオフにすることができます。

ESET File Security for Microsoft Windows Serverのスプラッシュウィンドウを無効にするには、[起動時にスプラッシュウィンドウを表示する] オプションの選択を解除します

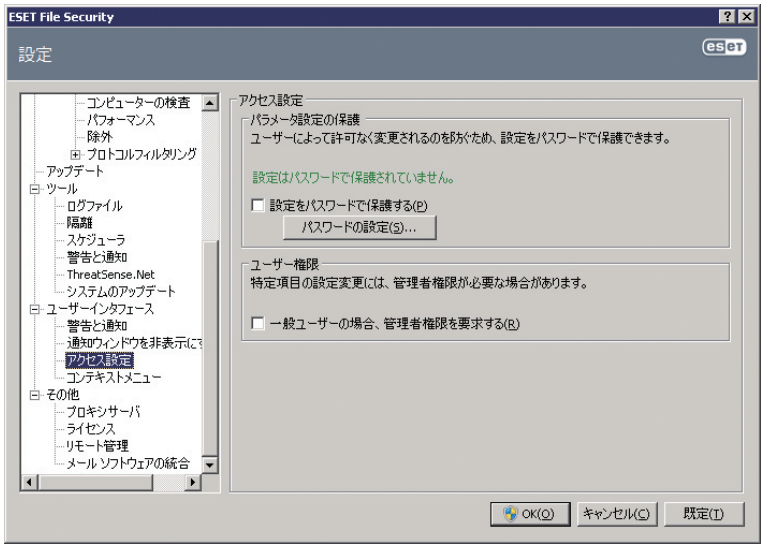
[ツールヒントを表示する] オプションが有効化されている場合は、オプションの上にカーソルを置くと、そのオプションの簡単な説明が表示されます。[アクティブなコントロール要素を選択状態にする] チェックボックスをチェックすると、現在マウスカーソルのアクティブな領域の下にある要素が強調表示されます。強調表示されている要素をマウスでクリックすると、その要素が有効になります。

アニメーション効果の速度を変更するには、[アニメーションコントロールを使用する] オプションを選択し、[速度] スライダーバーを右または左に動かします。

さまざまな操作の進行状況を表示するアニメーションアイコンの使用を有効にするには、[進捗インディケーターのアニメーションアイコンを使用する] オプションを選択します。



[ユーザーインターフェイス] 機能には、ESET File Security for Microsoft Windows Serverの設定パラメータをパスワードで保護するオプションなども含まれています。このオプションは、[設定の保護] サブメニューの [ユーザーインターフェイス] の下にあります。システムの最大限のセキュリティを確保するには、プログラムを正しく設定することが重要です。許可なく変更が行われた場合、重要なデータが失われることがあります。設定パラメータを保護するパスワードを設定するには、[パスワードの設定...] をクリックします。



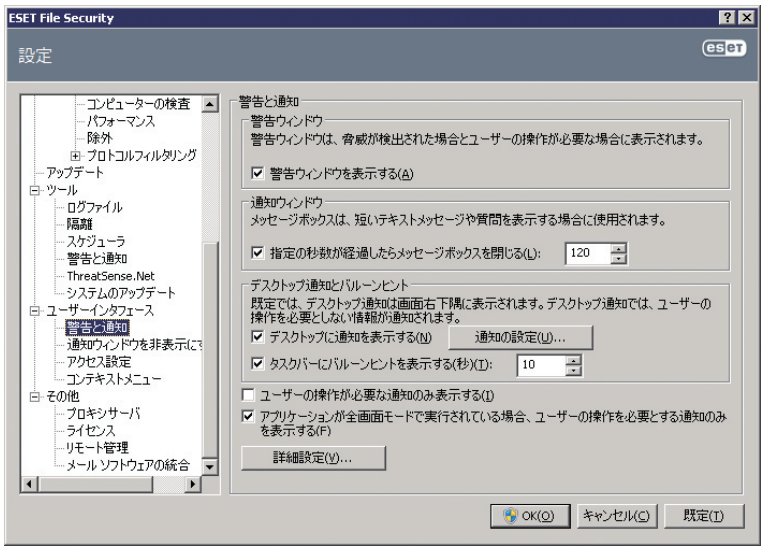
4.9.1 警告と通知

[ユーザーインターフェイス] の下の [警告と通知の設定] セクションでは、ウイルス警告やシステム通知をESET File Securityでどのように処理するかを設定することができます。

最初の項目は [警告を表示する] です。このチェックボックスのチェックを外すと、全ての警告ウィンドウが表示されなくなります。この設定が適しているのは、特定の限られた状況のみです。ほとんどのユーザーには、既定の設定のままにすることをお勧めします (チェックボックスをオンにします)。

指定の時間が経過した後で自動的にポップアップウィンドウを閉じる場合、[指定の秒数が経過したらメッセージボックスを閉じる] オプションを選択します。警告ウィンドウを手動で閉じなかった場合、指定した時間が経過すると、自動的にウィンドウが閉じられます。

デスクトップ通知とバルーンヒントは参考情報のみを示しています。ユーザーの操作を提案するものや要求するものではありません。画面の右下にある通知領域に表示されます。デスクトップ通知の表示を有効にするには、[デスクトップに通知を表示する] オプションを選択します。[通知の設定...] ボタンをクリックすると、通知の表示時間やウィンドウの透明度などの詳細なオプションを変更することができます。
通知の動作をプレビューするには、[プレビュー] ボタンをクリックします。バルーンヒントの表示時間を設定するには、[タスクバーにバルーンヒントを表示する (表示する秒数)] を使用します。



[詳細設定...] をクリックして、追加の [警告と通知] 設定オプションを開きます。ユーザーの操作が必要な通知のみ表示する] があります。このオプションを使用すると、ユーザーの操作を必要としない警告や通知の表示をオンまたはオフにすることができます。対話的でないすべての通知を抑制するには、[アプリケーションが全画面モードで実行されている場合、ユーザーの操作を必要とする通知のみを表示する] を選択します。警告および通知の表示を開始する重大度を、[表示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選択できます。

このセクションの最後の機能では、マルチユーザー環境での通知の表示先を設定できます。[マルチユーザーシステムの場合、以下のユーザーの画面に通知を表示する] フィールドでは、ESET File Security for Microsoft Windows Serverからの重要な通知を受け取るユーザーを定義することができます。通常は、システム管理者またはネットワーク管理者です。このオプションは、全てのシステム通知が管理者に送信される場合、ターミナルサーバに特に便利です。

4.9.2 ターミナルサーバでのGUIの無効化

この章では、Windowsターミナルサーバで稼動している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。ターミナルサーバでは、この動作は一般に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。

1. regedit.exeを実行します。
2. HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Runに移動します。
3. eguiを右クリックし、[修正...] を選択します。
4. 既存の文字列の末尾に、/terminalを追加します。

正しく設定した、eguiの [値] データの例を次に示します。
"C:¥Program Files¥ESET¥ESET File Security¥egui.exe" /hide /waitservice /terminal

この設定を元に戻して、ESET File Security for Microsoft Windows ServerのGUIの自動起動を有効にするには、/terminalを削除します。eguiレジストリの [値] にアクセスするには、ステップ1.～3.を繰り返します。

4.10 eShell

eShell(ESET Shell)は、ESET File Security for Microsoft Windows Serverのコマンドラインインタフェースです。グラフィカルユーザーインターフェイス(GUI)の代用として、GUIに通常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、プログラム全体の設定と管理を行うことができます。

GUIで使用可能なすべての機能のほかに、スクリプトを実行して、設定、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可能です。eShell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も有用です。

このセクションでは、eShellの検索方法と使用方法を説明し、すべてのコマンドを示しながら特定のコマンドの使用目的とその実行内容について説明します。

eShellを実行するモードには対話モードと単一コマンド/バッチモードの2つがあります。

●対話モードは、単一のコマンドを実行するだけでなく、設定の変更や、ログの表示などでeShellを操作する場合に有用です。対話モードは、まだ慣れていないコマンドがある場合にも使用できます。対話モードでは、コンテキストを検索しやすくなります。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、eShellの対話モードを開始しないコマンドだけ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を指定して、eshellと入力します。例:eshell set av document status enabled

▸▸▸ NOTE

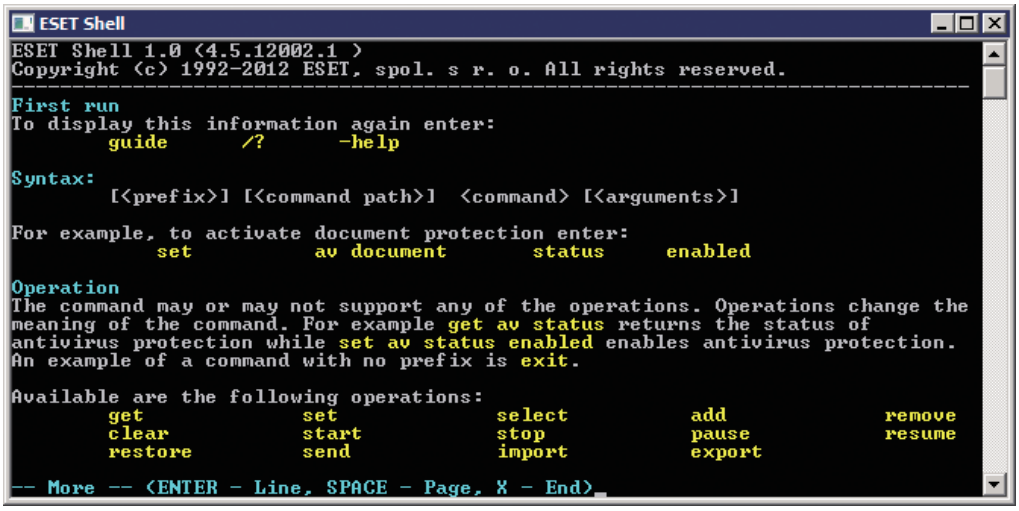
Windowsのコマンドプロンプトからeshellコマンドを実行するか、あるいはバッチファイルを実行するには、まずこの機能を有効にする必要があります(コマンドset general access batchを対話モードで実行する必要があります)。set batchコマンドの詳細については、「4.10.2.60　コンテキスト-GENERAL ACCESSのBATCH」を参照してください。

eShellの対話モードは、次の2つの方法のいずれか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] を選択する。

Windowsのコマンドプロンプトで、eshellと入力して、Enterキーを押す。

※eShellの初回起動時(対話モード)には、初期画面が表示されます。



この画面には、eShellのいくつかの基本的な使用例と、構文、プリフィクス、コマンドパス、省略形、エイリアスなどが表示されます。

NOTE

初期画面を再度表示するには、guideコマンドを入力します。

NOTE

コマンドの大文字と小文字は区別されません。大文字と小文字のいずれも使用でき、コマンドは区別なく実行されます。

4.10.1 使用方法

構文

コマンドの構成では、プレフィックス、コンテキスト、パラメータ、オプションなどを配置する位置を示します。下記にeShell全体で使用されている汎用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 AV DOCUMENT STATUS ENABLED

SET-プレフィックス
AV DOCUMENT-特定のコマンドのパス、つまり、このコマンドのコンテキスト
STATUS-コマンド本体
ENABLED-コマンドのパラメータ

コマンドとHELPまたは?を組み合わせて使用すると、その特定のコマンドの構文が表示されます。たとえば、CLEANLEVEL HELPと入力するとCLEANLEVELコマンドの構文が表示されます。

構文:
[get] | restore cleanlevel
set cleanlevel none | normal | strict

ここで、[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cleanlevelコマンドの既定値であることを示します。つまり、プレフィックスを指定しないで、コマンドcleanlevelを実行した場合、実際には、既定のプレフィックス(ここでは、get cleanlevel)が使用されます。プレフィックスを指定しないでコマンドを使用すると時間の節約になります。大部分のコマンドでは、通常は、getプレフィックスが既定値ですが、個々のコマンドについて既定のプレフィックスが何であるかと、実際に所定どおりの操作が実行されるのかをあらかじめ確認してください。

▸▸▸ NOTE

コマンドの大文字と小文字は区別されません。大文字と小文字のいずれも使用でき、コマンドは区別なく実行されます。

プレフィックス/操作

単一の操作です。たとえば、GETプレフィックスでは、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、または状態が表示されます(たとえば、GET AV STATUSは、現在の保護の状態を表示します)。一方、SETは、機能を設定するかまたは状態を変更します(たとえば、SET AV STATUS ENABLEDは、保護を有効化します)。

次に、eShellで使用できる周知のプレフィックスを示します。ただし、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
SELECT-項目の選択
ADD-項目の追加

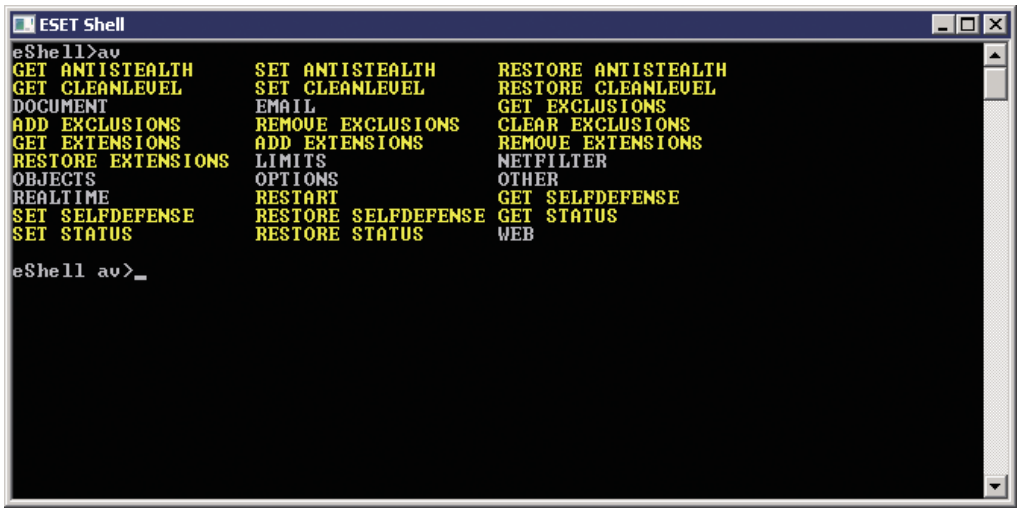
REMOVE-項目の削除
CLEAR-すべてのアイテム/ファイルを削除
START-アクションを開始する
STOP-アクションを停止する
PAUSE-アクションを中断するRESUME-アクションを再開する
RESTORE-既定の設定/オブジェクト/ファイルを復元
SEND-オブジェクト/ファイルを送信する
IMPORT-ファイルからインポートする
EXPORT-ファイルにエクスポートする

プレフィックスGETおよびSETなどをサポートしているコマンドは多くありますが、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、ツリー構造を形成する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。eShellを実行した時点では、ルートレベルになっています。

eShell>

そのままコマンドを実行することもできれば、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。たとえば、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できるコマンド、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。

上のレベルに戻る必要がある場合は、..（ドット2個）を使用します。たとえば、現在のコンテキストが

eShell av options>

の場合に、..を入力すると、1レベル上がって、下記のレベルになります。

eShell av>

または、現在のレベルeShell av options>（ルートから2レベル下）からルートに戻るには、そのまま、....と入力します（ドット2個とドット2個をスペースで区切る）。このように入力すると、2レベル上、この場合はルートに移動します。この方法は、コンテキストツリーのレベルの深さを問わず使用できます。目的のレベルに移動するために必要な数の..を使用してください。

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入っているコマンドの場合は、パスを入力しません。たとえば、GET AV STATUSを実行するには、次のように入力します。

GET AV STATUS-ルートコンテキスト（コマンドラインはeShell>）
GET STATUS-コンテキストAV（コマンドラインはeShell av>）
..GET STATUS-コンテキストAV OPTIONS（コマンドラインはeShell av options>）

パラメータ
特定のコマンドが実行するアクションです。たとえば、コマンドCLEANLEVELでは次のパラメータを使用できます。

none-駆除なし
normal-標準的な駆除
strict-厳密な駆除

パラメータの別の例としては、ENABLEDやDISABLEDがあります。これらのパラメータは、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
eShellでは、コンテキスト、コマンド、およびパラメータを簡略化できます（パラメータはスイッチまたは代替オプションの場合に限る）。数値、名前、パスなどの具体的な値を持つパラメータやプレフィックスは簡略化できません。

簡略形式の例:

set status enabled=>set stat en
add av exclusions C:¥path¥file.ext=>add av exc C:¥path¥file.ext

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、たとえば、ABOUTとAVの場合、簡略化したコマンドとして、Aを入力しても、eShellでは、この2つのコマンドのいずれを実行するのかを特定できません。その結果、エラーメッセージおよび"A"で開始されてい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

AV-コンテキストに対する変更　av

次に、1文字以上追加（たとえば、AB）すれば、コマンドが限定されたため、eShellでは、ABOUTコマンドを実行します。

NOTE

コマンドを要求どおりに確実に実行するには、コマンドやパラメータを省略形にせず、完全な形式を使用することをお勧めします。それにより、コマンドが要求どおりに実行されて、無用な失敗がなくなります。このことは、バッチファイル/スクリプトでは、特に当てはまります。

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）help-?
（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

"（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意味します。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ことがあります。たとえば、コマンドEXITには、下記のエイリアスがあります。
CLOSE
QUIT
BYE

eShellを終了する場合は、EXITコマンド自体を使用することも、その任意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、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、このコマンドdetections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から直接実行できます）。

eShellでは、独自のエイリアスを定義できます。エイリアスの作成方法については、「コンテキスト - GENERAL ESHELL」のALIASを参照してください。

保護されたコマンド

一部のコマンドは保護されており、パスワードを入力を求められる場合があります。パスワードで保護されたコマンドの詳細については、「コンテキスト - GENERAL ESHELL」のPASSWORDしてください。

Guide

コマンドGUIDEを入力すると、eShellの使用方法を説明する初期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（eShell>）.

Help

コマンドHELPを単独で使用すると、現在のコンテキストで使用可能なすべてのコマンドとプレフィクスおよびサブコンテキストが表示されます。各コマンド/サブコンテキストの短い説明も示されます。特定のコマンドのパラメータとしてHELPを使用した場合は（例:CLEANLEVEL HELP）、そのコマンドの詳細が表示されます。コマンドの構文、操作、パラメータ、およびエイリアスとそれぞれの短い説明が表示されます。

コマンド履歴

eShellでは、前に実行したコマンドの履歴を保持しています。履歴の保持は、現在のeShell対話セッションにのみ適用されます。eShellを終了すれば、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および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ことも、最初から全体を入力し直さないで変更することもできます。

CLS/画面の消去

コマンドCLSを使用すると画面を消去できます。Windowsのコマンドプロンプトや同じようなコマンドラインインタフェースの場合と同様の機能です。

EXIT/CLOSE/QUIT/BYE

eShellを閉じる、つまり終了する場合、この任意のコマンドを使用できます。

4.10.2 コマンド

このセクションでは、eshellで使用可能なeコマンドと各コマンドの説明を示します。

NOTE

コマンドの大文字と小文字は区別されません。大文字と小文字のいずれも使用でき、コマンドは区別なく実行されます。

ＲＯＯＴコンテキストに用意されているコマンド:

ABOUT

プログラムに関する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が稼動しているサーバ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

BATCH

eShellバッチモードを開始します。これは、バッチファイル/スクリプトを実行する場合に非常に有用であり、バッチファイルで使用することをお勧めします。バッチモードを有効にするために、START BATCHをバッチファイルまたはスクリプトに入れる最初のコマンドにします。この機能を有効すると、パスワードの入力などの対話的な入力は求められず、不足しているパラメータは既定値で置換されます。この結果、ユーザーの操作を待つために、eShellがバッチファイルの途中で停止しなくなります。この方法により、バッチファイルは停止しないで実行されます(ただし、エラーがあるときや、バッチファイル内のコマンドが正しくないときを除く)。

コンテキストパス:

root

構文:

[start] batch

操作:

start-eShellをバッチモードで開始する
コンテキストパス:

root

例:

start batch-eShellバッチモードを開始する

GUIDE

初期画面を表示します

コンテキストパス:
root

PASSWORD

パスワードで保護されたコマンドを実行する場合、通常は、パスワード147の入力を求められます。これは、セキュリティ上の理由です。主にウイルスからの保護機能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などに適用されています。このようなコマンドは、実行ごとにパスワードを要求します。なお、毎回パスワードを入力しないために、パスワードをセットすることができます。セットしたパスワードは、eShellに記録されます。パスワードで保護されたコマンドを実行するときに、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。

▸▸▸ NOTE

セットしたパスワードは、現在のeShell対話セッションに限って有効です。セットしたパスワードは、eShellを終了すると削除されます。eShellを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場合にも非常に有用です。下記に、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保護を無効にします。
※このバッチを実行するには、事前に対話モードで下記のコマンドが実行されている必要があります。
Set general access batch always

コンテキストパス:
root

構文:
[get] | restore password
set password [plain<password>]

操作:
get-パスワードを表示する
set-パスワードを設定または削除する
restore-パスワードを削除するパラメータ:
plain-パスワードの入力をパラメータに切り替える
password-パスワード

例:
set password plain<yourpassword>-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-パスワードをクリアする

例:
get password-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"*"を表示するだけで

パスワード自体は表示しません)。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>-定義したパスワードを設定する場合に使用します。
restore password-このコマンドは、定義したパスワードをクリアします。

STATUS
GUI同様、現時点におけるESET File Security for Microsoft Windows Serverの保護の状態に関する情報を表示します。

コンテキストパス:
root

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

操作:
get–ウイルス・スパイウェア対策のステータスを表示する
set–ウイルス・スパイウェア対策を無効化/有効化する
restore–意帝の設定/オブジェクト/ファイルを復元

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

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

VIRLOG
これは、DETECTIONSコマンドのエイリアスです。検出されたマルウェアに関する情報を表示する必要がある場合に有用です。このコマンドの詳細および使用方法については、「コンテキスト - TOOLS LOG」のDETECTIONSを参照してください。

WARNLOG
これは、EVENTSコマンドのエイリアスです。さまざまなイベントに関する情報を表示する必要がある場合に有用です。このコマンドの詳細および使用方法については、「コンテキスト - TOOLS LOG」のEVENTSを参照してください。

4.10.2.1 コンテキスト-AV

ANTISTEALTH
アンチステルス技術を有効にする

構文:
[get] | restore antistealth
set antistealth disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

CLEANLEVEL
駆除レベル

構文:
[get] | restore cleanlevel
set cleanlevel none | normal | strict

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
none-駆除なし
normal-標準的な駆除
strict-厳密な駆除

EXCLUSIONS
除外管理

構文:
[get] | clear exclusions
add | remove exclusions<exclusion>

操作:
get-現在の設定/状態を表示する
add-項目の追加
remove-項目の削除

パラメータ:
exclusion-除外するファイル/フォルダ/マスク

EXTENSIONS
拡張子

構文:
[get] | restore extensions
add | remove extensions<extension>|/all |/extless

操作:
get-現在の設定/状態を表示する
add-項目の追加
remove-項目の削除
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
extension-拡張子
/all-すべてのファイル
/extless-拡張子のないファイル

RESTART
ESETカーネルを再起動

構文:
restart

SELFDEFENSE
自己防衛を有効にする

構文:
[get] | restore selfdefense
set selfdefense disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

STATUS
ウイルス・スパイウェア対策のステータス。

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

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

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

4.10.2.2 コンテキスト-AV DOCUMENT

CLEANLEVEL
駆除レベル

構文:
[get] | restore cleanlevel
set cleanlevel none | normal | strict

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
none-駆除なし
normal-標準的な駆除
strict-厳密な駆除

EXTENSIONS
拡張子

構文:
[get] | restore extensions
add | remove extensions<extension>|/all |/extless

操作:
get-現在の設定/状態を表示する
add-項目の追加
remove-項目の削除
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
extension-拡張子
/all-すべてのファイル
/extless-拡張子のないファイル

INTEGRATION
ドキュメント保護をシステムに統合する

構文:
[get] | restore integration
set integration disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

STATUS
ドキュメント保護

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

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.3 コンテキスト-AV DOCUMENT LIMITS ARCHIVE

LEVEL
スキャン対象の下限ネストレベル。

構文:
[get] | restore level set level<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-レベルは1～20、または既定の設定はOSIZEスキャン対象のファイルの最大サイズ(kB)。

構文:
[get] | restore size set size<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-サイズ/kB(1～3145728)、既定の設定は0サイズ/kB(1～3145728)、既定の設定は0

4.10.2.4 コンテキスト-AV DOCUMENT LIMITS OBJECTS

SIZE
オブジェクトの最大サイズ(kB)

構文:
[get] | restore size
set size<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-サイズ/kB(1～3145728)、既定の設定は0

TIMEOUT
オブジェクトの最大検査時間(秒)

構文:
[get] | restore timeout
set timeout<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-時間/秒、既定の設定は0時間/秒、既定の設定は0

4.10.2.5 コンテキスト-AV DOCUMENT OBJECTS

ARCHIVE

アーカイブを検査する

構文:

[get] | restore archive

set archive disabled | enabled

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

disabled-機能の無効化/設定の無効化

enabled-機能の有効化/設定の有効化

EMAIL

電子メールファイルを検査する

構文:

[get] | restore email

set email disabled | enabled

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

disabled-機能の無効化/設定の無効化

enabled-機能の有効化/設定の有効化

RUNTIME

圧縮された実行形式を検査する

構文:

[get] | restore runtime

set runtime disabled | enabled

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

SFX
自己解凍形式を検査する

構文:
[get] | restore sfx
set sfx disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.6 コンテキスト-AV DOCUMENT OPTIONS

ADVHEURISTICS
アドバンスドヒューリスティックを使用する

構文:
[get] | restore advheuristics
set advheuristics disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

HEURISTICS
ヒューリスティックを使用する

構文:
[get] | restore heuristics
set heuristics disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

UNSAFE
安全ではない可能性があるアプリケーションを検出する

構文:
[get] | restore unsafe
set unsafe disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

UNWANTED
望ましくない可能性があるアプリケーションを検出する

構文:
[get] | restore unwanted
set unwanted disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.7 コンテキスト-AV DOCUMENT OTHER

LOGALL

すべてのオブジェクトをログに記録する

構文:

[get] | restore logall

set logall disabled | enabled

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

disabled-機能の無効化/設定の無効化

enabled-機能の有効化/設定の有効化

OPTIMIZE

SMART最適化を有効にする

構文:

[get] | restore optimize

set optimize disabled | enabled

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

disabled-機能の無効化/設定の無効化

enabled-機能の有効化/設定の有効化

4.10.2.8 コンテキスト-AV EMAIL

ACTION

感染メールに対して実行するアクション

構文:

[get] | restore action

set action none | delete | movedeleted | moveto

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
none-何もしない
削除-メールを削除する
movedeleted-メールをごみ箱に移動する
moveto-メールを指定のフォルダに移動する

CLIENTS
電子メールクライアント

構文:
[get] clients
add | remove clients<path>

操作:
get-現在の設定/状態を表示する
add-項目の追加
remove-項目の削除

パラメータ:
path-アプリケーションパス

NOTE

アプリケーションを指定したフィルタリングのみの場合は、どのアプリケーションが電子メールクライアントとして機能するかを指定する必要があります。アプリケーションが電子メールクライアントとしてマークされていない場合、メールは検査されない可能性があります。

QUARANTINE
感染メール用フォルダです。

構文:
[get] | restore quarantine
set quarantine<string>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-フォルダ名

STATUS
ウイルススパイウェア対策メールクライアント保護

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

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.9 コンテキスト-AV EMAIL GENERAL

CLEANLEVEL
駆除レベル

構文:
[get] | restore cleanlevel
set cleanlevel none | normal | strict

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
none-駆除なし
normal-標準的な駆除
strict-厳密な駆除

EXTENSIONS
拡張子

構文:
[get] | restore extensions
add | remove extensions<extension>|/all |/extless

操作:
get-現在の設定/状態を表示する
add-項目の追加
remove-項目の削除
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
extension-拡張子
/all-すべてのファイル
/extless-拡張子のないファイル

4.10.2.10 コンテキスト-AV EMAIL GENERAL LIMITS ARCHIVE

LEVEL

スキャン対象の下限ネストレベルスキャン対象の下限ネストレベル

構文:
[get] | restore level
set level<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-レベルは1～20、または既定の設定は0レベルは1～20、または既定の設定は0

SIZE

スキャン対象のファイルの最大サイズ(kB)スキャン対象のファイルの最大サイズ(kB)

構文:
[get] | restore size
set size<number>

操作:
ｘｘget-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-サイズ/kB(1～3145728)、既定の設定は0サイズ/kB(1～3145728)、既定の設定は0

4.10.2.11 コンテキスト-AV EMAIL GENERAL LIMITS OBJECTS

SIZE

オブジェクトの最大サイズ(kB)

構文:
[get] | restore size
set size<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-サイズ/kB（1～3145728）、既定の設定は0

TIMEOUT
オブジェクトの最大検査時間（秒）

構文:
[get] | restore timeout set timeout<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-時間/秒、既定の設定は0時間/秒、既定の設定は0

4.10.2.12　コンテキスト-AV EMAIL GENERAL OBJECTS

ARCHIVE
アーカイブを検査する

構文:
[get] | restore archive
set archive disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

EMAIL
電子メールファイルを検査する

構文:
[get] | restore email
set email disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

RUNTIME
圧縮された実行形式を検査する

構文:
[get] | restore runtime
set runtime disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

SFX
自己解凍形式を検査する

構文:
[get] | restore sfx
set sfx disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.13 コンテキスト-AV EMAIL GENERAL OPTIONS

ADVHEURISTICS
アドバンスドヒューリスティックを使用する

構文:
[get] | restore advheuristics
set advheuristics disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

HEURISTICS
ヒューリスティックを使用する

構文:
[get] | restore heuristics
set heuristics disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

UNSAFE
安全ではない可能性があるアプリケーションを検出する

構文:
[get] | restore unsafe
set unsafe disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

UNWANTED
望ましくない可能性があるアプリケーションを検出する

構文:
[get] | restore unwanted
set unwanted disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.14 コンテキスト-AV EMAIL GENERAL OTHER

LOGALL
すべてのオブジェクトを記録する

構文:
[get] | restore logall
set logall disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

OPTIMIZE
SMART最適化を有効にする

構文:
[get] | restore optimize
set optimize disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.15 コンテキスト-AV EMAIL MESSAGE CONVERT

PLAIN

メール本文をテキスト形式に変換する

構文:

[get] | restore plain

set plain disabled | enabled

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

disabled-機能の無効化/設定の無効化

enabled-機能の有効化/設定の有効化

4.10.2.16 コンテキスト-AV EMAIL MODIFY

TEMPLATE

感染メールの件名に追加する目印のテンプレート

構文:

[get] | restore template

set template [<string>]

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

string–本文

4.10.2.17 コンテキスト-AV EMAIL MODIFY RECEIVED

BODY

受信メールと既読メールにタグメッセージを追加

構文:

[get] | restore body

set body never | infected | all

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
never-追加しない
infected-感染メールのみ
all-すべてのメール

SUBJECT
受信した感染メールと表示した感染メールの件名に注を追加

構文:
[get] | restore subject
set subject disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.18 コンテキスト-AV EMAIL MODIFY SENT

BODY
送信メールにタグメッセージを追加

構文:
[get] | restore body
set body never | infected | all

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
never-追加しない
infected-感染メールのみ
all-すべてのメール

SUBJECT
送信した感染メールの件名に注を追加

構文:
[get] | restore subject
set subject disabled | enabled

操作:
get-現在の設定/状態を表示する
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.19 コンテキスト-AV EMAIL OEXPRESS/WINMAIL

INTEGRATION
Outlook ExpressWindowsメールに統合する

構文:
[get] | restore integration
set integration disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.20 コンテキスト-AV EMAIL OUTLOOK

FORCEADDIN
古いMicrosoft Outlookバージョンで COMアドインを使用する

構文:
[get] | restore forceaddin
set forceaddin 2010newer | 2007newer | allversions

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
2010newer-Microsoft Outlook 2010以降
2007newer-Microsoft Outlook 2007以降
allversions-Microsoft Outlookの全バージョン

INTEGRATION
Microsoft Outlookに統合する

構文:
[get] | restore integration
set integration disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

SYNCFIX
Microsoft Outlookにおける同期競合問題を解決できるようにする

構文:
[get] | restore syncfix set syncfix<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元
0-無効3-完全に有効にする、その他の有効値

4.10.2.21 コンテキスト-AV EMAIL OUTLOOK RESCAN

ONCHANGE
受信ボックス内の変更時にチェックを無効にする

構文:
[get] | restore onchange
set onchange disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.22 コンテキスト-AV EMAIL PROTOCOL POP3

COMPATIBILITY

互換性の設定

構文:

[get] | restore compatibility

set compatibility compatible | both | effective

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

compatible-互換性を優先

both-互換性:中レベル

effective-効率性を優先

››› NOTE

標準の設定では互換性の設定は中レベルに設定されていますが、一部の電子メールクライアントはPOP3フィルタリングとの連携で正しく機能しない場合があります。次の設定では、互換性レベルを調整して競合の問題を解決することができます。ただし、互換性レベルを上げるとインターネットモニタの効率性が低下したり、一部の機能を使用できなくなる場合があります。

PORTS

POP3プロトコルで使用するポート

構文:

[get] | restore ports set ports [<string>]

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

string–カンマ区切りのポート番号

USE

電子メールのチェックを有効にする

構文:

[get] | restore use

set use disabled | enabled

操作:

get-現在の設定/状態を表示する

set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.23 コンテキスト-AV EMAIL PROTOCOL POP3S

COMPATIBILITY
互換性の設定

構文:
[get] | restore compatibility
set compatibility compatible | both | effective

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
compatible-互換性を優先
both-互換性:中レベル
effective-効率性を優先

▸▸▸ NOTE
標準の設定では互換性の設定は中レベルに設定されていますが、一部の電子メールクライアントはPOP3Sフィルタリングとの連携で正しく機能しない場合があります。次の設定では、互換性レベルを調整して競合の問題を解決することができます。ただし、互換性レベルを上げるとインターネットモニタの効率性が低下したり、一部の機能を使用できなくなる場合があります。

MODE
POP3Sフィルタリングモード

構文:
[get] | restore mode
set mode none | ports | clients

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
none-POP3Sプロトコルチェックを使用しない
ports-選択されたポートのPOP3Sプロトコルチェックを使用する

clients-選択されたポートを使用する電子メールクライアントとしてマークされたアプリケーションにPOP3Sプロトコルチェックを使用する

PORTS
POP3Sプロトコルが使用するポート

構文:
[get] | restore ports set ports [<string>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string–カンマ区切りのポート番号

4.10.2.24 コンテキスト-AV EMAIL RESCAN

ONUPDATE
アップデート後に再度検査を行う

構文:
[get] | restore onupdate
set onupdate disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.25 コンテキスト-AV EMAIL SCAN

OTHERMODULES
ほかの機能の検査結果を受け入れる

構文:
[get] | restore othermodules
set othermodules disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

PLAIN
テキスト形式のメール本文を検査する

構文:
[get] | restore plain
set plain disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

READ
既読メール

構文:
[get] | restore read
set read disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

RECEIVED
受信メール

構文:
[get] | restore received
set received disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

RTF

RTF形式のメール本文を検査する

構文:
[get] | restore rtf
set rtf disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

SENT

送信メール

構文:
[get] | restore sent
set sent disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.26 コンテキスト-AV EMAIL THUNDERBIRD

INTEGRATION

Mozilla Thunderbirdに統合する

構文:

[get] | restore integration

set integration disabled | enabled

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

disabled-機能の無効化/設定の無効化

enabled-機能の有効化/設定の有効化

4.10.2.27 コンテキスト-AV EMAIL WINLIVE

INTEGRATION

Windows Live Mailに統合する

構文:

[get] | restore integration

set integration disabled | enabled

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

disabled-機能の無効化/設定の無効化

enabled-機能の有効化/設定の有効化

4.10.2.28 コンテキスト-AV LIMITS ARCHIVE

LEVEL

スキャン対象の下限ネストレベル

構文:

[get] | restore level set level<number>

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-レベルは1～20、または既定の設定は0
SIZEスキャン対象のファイルの最大サイズ(kB)

構文:
[get] | restore size
set size<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-サイズ/kB(1～3145728)、既定の設定は0

4.10.2.29 コンテキスト-AV LIMITS OBJECTS

SIZE
オブジェクトの最大サイズ(kB)

構文:
[get] | restore size
set size<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-サイズ/kB(1～3145728)、既定の設定は0

TIMEOUT
オブジェクトの最大検査時間(秒)

構文:
[get] | restore timeout
set timeout<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-時間/秒、既定の設定は0

4.10.2.30 コンテキスト-AV NETFILTER

AUTOSTART
アプリケーションプロトコル保護を自動的に開始する

構文:
[get] | restore autostart
set autostart disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

EXCLUDED
プロトコルフィルタリングの対象外とするアプリケーション

構文:
[get] excluded
add | remove excluded<path>

操作:
get-現在の設定/状態を表示する
add-項目の追加remove-項目の削除パラメータ:
path-アプリケーションパス

MODE
フィルタリングのための通信リダイレクト

構文:
[get] | restore mode
set mode ports | application | both

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
ports-HTTP/POP3ポート
application-インターネットブラウザまたは電子メールクライアントとしてマークされたアプリケーション
both-インターネットブラウザまたは電子メールクライアントとしてマークされたポートとアプリケーション

STATUS

アプリケーションプロトコルフィルタリングを有効にする

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

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.31 コンテキスト-AV NETFILTER PROTOCOL SSL

BLOCKSSL2

古いプロトコルSSL v2を使用した暗号化通信をブロックする

構文:
[get] | restore blockssl2
set blockssl2 disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

EXCEPTIONS

証明書に基づいて作成された例外を適用する

構文:
[get] | restore exceptions
set exceptions disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

MODE
SSLプロトコルフィルタリングモード。

構文:
[get] | restore mode
set mode allways | ask | none

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
allways-常にSSLチェックを使用する
ask-(除外を設定可能な)未訪問のサイトについて尋ねる
none-SSLプロトコルチェックを使用しない

4.10.2.32 コンテキスト-AV NETFILTER PROTOCOL SSL CERTIFICATE

ADDTOBROWSERS
ルート証明書を既知のブラウザに追加する

構文:
[get] | restore addtobrowsers
set addtobrowsers disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

NOTE

SSL暗号化トラフィックを適切に確認するために、信頼できるルート認証局ストアに、証明書の署名に使用されるESET,spol.sr.oのルート証明書が追加されます。

EXCLUDED

SSL通信がコンテンツの検査から除外される証明書のリスト

構文:
[get] excluded
remove excluded<name>

操作:
get-現在の設定/状態を表示する
remove-項目の削除

パラメータ:
name-証明書の名前

NOTTRUSTED

証明書が無効または破損している場合

構文:
[get] | restore nottrusted
set nottrusted ask | block

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
ask-証明書の有効性を確認する
block-証明書を使用する通信をブロックする

TRUSTED

信頼できるとしてマークされている証明書のリスト

構文:
[get] trusted
remove trusted<name>

操作:
get-現在の設定/状態を表示する
remove-項目の削除パラメータ:

name-証明書の名前

UNKNOWNROOT
信頼できるルート認証局ストアを使用して証明書を検証できない場合

構文:
[get] | restore unknownroot set unknownroot ask | block

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
ask-証明書の有効性を確認する
block-証明書を使用する通信をブロックする

4.10.2.33 コンテキスト-AV OBJECTS

ARCHIVE
アーカイブを検査する

構文:
[get] | restore archive
set archive disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

BOOT
ブートセクタを検査する

構文:
[get] | restore boot
set boot disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

EMAIL

電子メールファイルを検査する

構文:
[get] | restore email
set email disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

MEMORY

システムメモリを検査する

構文:
[get] | restore memory
set memory disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

RUNTIME

圧縮された実行形式を検査する

構文:
[get] | restore runtime
set runtime disabled | enabled

操作:
get-現在の設定/状態を表示する

set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

SFX
自己解凍形式を検査する

構文:
[get] | restore sfx
set sfx disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.34 コンテキスト-AV OPTIONS

ADVHEURISTICS
アドバンスドヒューリスティックを使用す

構文:
[get] | restore advheuristics
set advheuristics disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

HEURISTICS
ヒューリスティックを使用する

構文:
[get] | restore heuristics

set heuristics disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

UNSAFE
安全ではない可能性があるアプリケーションを検出する

構文:
[get] | restore unsafe
set unsafe disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

UNWANTED
望ましくない可能性があるアプリケーションを検出する

構文:
[get] | restore unwanted
set unwanted disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.35 コンテキスト-AV OTHER

LOGALL

すべてのオブジェクトをログに記録する

構文:
[get] | restore logall
set logall disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

OPTIMIZE

SMART最適化を有効にする

構文:
[get] | restore optimize
set optimize disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.36 コンテキスト-AV REALTIME

AUTOSTART

リアルタイムファイルシステム保護を自動的に開始する

構文:
[get] | restore autostart
set autostart disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

CLEANLEVEL
駆除レベル

構文:
[get] | restore cleanlevel
set cleanlevel none | normal | strict

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
none-駆除なし
normal-標準的な駆除
strict-厳密な駆除

EXTENSIONS
拡張子

構文:
[get] | restore extensions
add | remove extensions<extension>|/all |/extless

操作:
get-現在の設定/状態を表示する
add-項目の追加
remove-項目の削除
restore-既定の設定/オブジェクト/ファイルを復元
パラメータ:
extension-拡張子
/all-すべてのファイル
/extless-拡張子のないファイル

STATUS
リアルタイムファイルシステム

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

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.37 コンテキスト-AV REALTIME DISK

FLOPPY
リムーバブルメディア

構文:
[get] | restore floppy
set floppy disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

LOCAL
ローカルドライブ

構文:
[get] | restore local
set local disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

NETWORK
ネットワークドライブ

構文:
[get] | restore network
set network disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.38 コンテキスト-AV REALTIME EVENT

CREATE
ファイルの作成

構文:
[get] | restore create
set create disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

EXECUTE
ファイルの実行

構文:
[get] | restore execute
set execute disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

FLOPPYACCESS
フロッピーディスクアクセス

構文:
[get] | restore floppyaccess
set floppyaccess disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

OPEN
ファイルのオープン

構文:
[get] | restore open
set open disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

SHUTDOWN
コンピューターシャットダウン時

構文:
[get] | restore shutdown
set shutdown disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.39 コンテキスト-AV REALTIME EXECUTABLE

ADVHEURISTICS
ファイル実行時のアドバンスドヒューリスティック

構文:
[get] | restore advheuristics
set advheuristics disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.40 コンテキスト-AV REALTIME EXECUTABLE FROMREMOVABLE

ADVHEURISTICS
リムーバブルメディアからの実行ファイルのアドバンスドヒューリスティック

構文:
[get] | restore advheuristics
set advheuristics disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

EXCLUSION
USBドライブ除外対象

構文:
[get] | restore exclusion
select exclusion none |<drive>| all

操作:
get-現在の設定/状態を表示する
select-項目の選択する
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
none-すべてのドライブを選択解除する
drive-選択/選択解除するドライブのドライブ文字
all-すべてのドライブを選択する

NOTE

このオプションを使用すると、ファイル実行時にアドバンスドヒューリスティックを使用する検査に例外を設定できます。ハードドライブのアドバンスドヒューリスティック設定は、選択されたデバイスに適用されます。

4.10.2.41 コンテキスト-AV REALTIME LIMITS ARCHIVE

LEVEL

スキャン対象の下限ネストレベル

構文:
[get] | restore level set level<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-レベルは1～20、または既定の設定は0

SIZE

スキャン対象のファイルの最大サイズ(kB)

構文:
[get] | restore size
set size<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-サイズ/kB(1～3145728)、既定の設定は0

4.10.2.42 コンテキスト-AV REALTIME LIMITS OBJECTS

SIZE

オブジェクトの最大サイズ（kB）

構文:

[get] | restore size set size<number>

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

number-サイズ/kB（1～3145728）、既定の設定は0

TIMEOUT

オブジェクトの最大検査時間（秒）

構文:

[get] | restore timeout

set timeout<number>

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

number-時間/秒、既定の設定は0

4.10.2.43 コンテキスト-AV REALTIME OBJECTS

BOOT

ブートセクタを検査する

構文:

[get] | restore boot

set boot disabled | enabled

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

disabled-機能の無効化/設定の無効化

enabled-機能の有効化/設定の有効化

RUNTIME
圧縮された実行形式を検査する

構文:
[get] |restore runtime
set runtime disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.44 コンテキスト-AV REALTIME ONWRITE

ADVHEURISTICS
新規作成または変更されたファイルに対する「アドバンスドヒューリスティック」検査を有効にする

構文:
[get] | restore advheuristics
set advheuristics disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

RUNTIME
新規作成または変更された「圧縮された実行形式」を検査する

構文:
[get] | restore runtime
set runtime disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

SFX
新規作成または変更された「自己解凍形式」を検査する

構文:
[get] | restore sfx
set sfx disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.45 コンテキスト-AV REALTIME ONWRITE ARCHIVE

LEVEL
スキャン対象の下限ネストレベル

構文:
[get] | restore level
set level<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-レベル(0～20)

SIZE
最大ファイルサイズ(Kb)

構文:
[get] | restore size set size<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-サイズ(kB)

4.10.2.46 コンテキスト-AV REALTIME OPTIONS

ADVHEURISTICS
アドバンスドヒューリスティックを使用する

構文:
[get] | restore advheuristics
set advheuristics disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

HEURISTICS
ヒューリスティックを使用する

構文:
[get] | restore heuristics
set heuristics disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

UNSAFE
安全ではない可能性があるアプリケーションを検出する

構文:
[get] | restore unsafe
set unsafe disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

UNWANTED
望ましくない可能性があるアプリケーションを検出する

構文:
[get] | restore unwanted
set unwanted disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.47　コンテキスト-AV REALTIME OTHER

LOGALL
すべてのオブジェクトをログに記録する

構文:
[get] | restore logall
set logall disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

OPTIMIZE
SMART最適化を有効にする

構文:
[get] | restore optimize
set optimize disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.48 コンテキスト-AV REALT IME REMOVABLE

BLOCK
リムーバブルメディアをブロック

構文:
[get] | restore block
set block disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/ステータスを設定するset-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

EXCLUSION
許可されているリムーバブルメディア

構文:
[get] | restore exclusion
select exclusion none |<drive>| all

操作:
get-現在の設定/状態を表示する
select-項目の選択
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
none-すべてのドライブを選択解除する
drive-選択/選択解除するドライブのドライブ文字
all-すべてのドライブを選択する

NOTE

このオプションを使用すると、リムーバブルメディア(CD、フロッピーディスク、USBドライブ)へのアクセスを有効にできます。メディアをマークすると、マークしたメディアにアクセスしようとしたときにアクセス制限が解除されます。

4.10.2.49 コンテキスト-AV WEB

BROWSERS

インターネットブラウザ

構文:
[get] browsers
add | remove browsers<path>

操作:
get-現在の設定/状態を表示する
add-項目の追加
remove-項目の削除パラメータ:
path-アプリケーションパス

NOTE

セキュリティを強化するには、インターネットブラウザとして使用するアプリケーションをすることを推奨します。アプリケーションがWebブラウザとしてマークされていない場合、そのアプリケーションを使用して送受信されるデータが検査されないことがあります。

CLEANLEVEL

駆除レベル

構文:
[get] | restore cleanlevel
set cleanlevel none | normal | strict

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
none-駆除なし
normal-標準的な駆除
strict-厳密な駆除

EXTENSIONS

拡張子

構文:
[get] | restore extensions
add | remove extensions<extension>|/all |/extless

操作:
get-現在の設定/状態を表示する
add-項目の追加
remove-項目の削除
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
extension-拡張子
/all-すべてのファイル
/extless-拡張子のないファイル

STATUS
Webアクセス保護

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

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.50 コンテキスト-AV WEB ADDRESSMGMT

ADDRESS
選択したリストのアドレス管理

構文:
[get] | clear address
add | remove address<address>
import | export address<path>

操作:
get-現在の設定/状態を表示する
add-項目の追加
remove-項目の削除
import-ファイルからインポート

export-ファイルにエクスポート
clear-すべてのアイテム/ファイルの削除
パラメータ:
address-アドレス
path-ファイルパス

LIST

HTTPアドレスリスト管理

構文:
[get] list
set list<listname>disabled | enabled
select | remove list<listname>
add list allowed<listname>| blocked<listname>| excluded<listname>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
select-編集用に選択
add-項目の追加remove-項目の削除パラメータ:
listname-リスト名
disabled-リストを使用しない
enabled-リストを使用する
allowed-許可するアドレスのリスト
blocked-ブロックされるアドレス/マスクのリスト
excluded-フィルタリング対象外とするアドレスのリスト

››› NOTE

選択したリスト(xのマークが付いている)を編集するには、'av web addressmgmt address'コマンドを使用します

NOTIFY

リストからのアドレスを適用するときに通する

構文:
[get] | restore notify
set notify disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

WHITELISTED
許可されているアドレスのリストにあるHTTPアドレスに対してだけアクセスを許可する

構文:
[get] | restore whitelisted
set whitelisted disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.51 コンテキスト-AV WEB LIMITS ARCHIVE

LEVEL
スキャン対象の下限ネストレベル

構文:
[get] | restore level set level<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-レベルは1～20、または既定の設定は0

SIZE
スキャン対象のファイルの最大サイズ(kB)

構文:
[get] | restore size set size<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元パラメータ:
number-サイズ/kB(1～3145728)、既定の設定は0

4.10.2.52 コンテキスト-AV WEB LIMITS OBJECTS

SIZE

スキャン対象ファイルの最大サイズ（kB）

構文:

[get] | restore size set size<number>

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

number-サイズ/kB（1～3145728）、既定の設定は0

TIMEOUT

オブジェクトの最大検査時間（秒）

構文:

[get] | restore timeout set timeout<number>

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

number-時間/秒、既定の設定は0

4.10.2.53 コンテキスト-AV WEB OBJECTS

ARCHIVE

アーカイブを検査する

構文:

[get] | restore archive

set archive disabled | enabled

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

disabled-機能の無効化/設定の無効化

enabled-機能の有効化/設定の有効化

EMAIL
電子メールファイルをする

構文:
[get] | restore email
set email disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

RUNTIME
圧縮された実行形式を検査する

構文:
[get] | restore runtime
set runtime disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

SFX
自己解凍形式を検査する

構文:
[get] | restore sfx
set sfx disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.54 コンテキスト-AV WEB OPTIONS

ADVHEURISTICS

アドバンスドヒューリスティックを使用する

構文:
[get] | restore advheuristics
set advheuristics disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

HEURISTICS

ヒューリスティックを使用する

構文:
[get] | restore heuristics
set heuristics disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

UNSAFE

安全ではない可能性があるアプリケーションを検出する

構文:
[get] | restore unsafe
set unsafe disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

UNWANTED
望ましくない可能性があるアプリケーションを検出する

構文:
[get] | restore unwanted
set unwanted disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.55 コンテキスト- AV WEB OPTIONS BROWSERS

ACTIVEMODE
インターネットブラウザのアクティブモード

構文:
[get] activemode
add | remove activemode<path>

操作:
get-現在の設定/状態を表示する
add-項目の追加
remove-項目の削除

パラメータ:
path-アプリケーションのパス

▸▸▸ NOTE
リストに追加されたプログラムは、Webブラウザリストに自動的に追加されます。

4.10.2.56 コンテキスト-AV WEB OTHER

LOGALL

すべてのオブジェクトをログに記録する

構文:
[get] | restore logall
set logall disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

OPTIMIZE

SMART最適化を有効にする

構文:
[get] | restore optimize
set optimize disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.57 コンテキスト-AV WEB PROTOCOL HTTP

PORTS

HTTPプロトコルで使用するポート

構文:
[get] | restore ports set ports [<string>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-コロン区切りのポート番号

USE
HTTPのチェックを有効にする

構文:
[get] | restore use
set use disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.58 コンテキスト-AV WEB PROTOCOL HTTPS

MODE
HTTPSフィルタリングモード

構文:
[get] | restore mode
set mode none | ports | browsers

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
none-HTTPSプロトコルのチェックを使用しない
ports-選択されたポートのHTTPSプロトコルのチェックを使用する
browsers-選択されたポートを使用するインターネットブラウザーとしてマークされたアプリケーションのHTTPSプロトコルチェックを使用する

PORTS
HTTPSで使用するポート

構文:
[get] | restore ports set ports [<string>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string– カンマ区切りのポート番号

4.10.2.59 コンテキスト-GENERAL

CONFIG
設定をインポート/エクスポート

構文:
import | export config<path>

操作:
import-ファイルからインポート
export-ファイルにエクスポート

パラメータ:
path-ファイルパス

LICENSE
ライセンス管理

構文:
[get] license
import license<path>
export license<ID><path>
remove license<ID>

操作:
get-現在の設定/状態を表示する
remove-項目の削除
import-ファイルからインポート
export-ファイルにエクスポート

パラメータ:
path-ライセンスファイルのパス
ID-ライセンスID

4.10.2.60 コンテキスト-GENERAL ACCESS

ADMIN

管理者権限を要求する

構文:

[get] | restore admin

set admin disabled | enabled

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

disabled-機能の無効化/設定の無効化

enabled-機能の有効化/設定の有効化

BATCH

eShellが実行されている場合は、入力されているコマンドを引数として実行する

構文:

[get] | restore batch

set batch disabled |<time>| always

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

disabled-無効

time-間隔/分単位（1 ～ 1440分間）

always-常時

PASSWORD

設定をパスワードで保護する

構文:

[get] | restore | set password

操作:

get-パスワードを表示する

set-パスワードの設定

restore-パスワードをリセットする

NOTE

このパスワードは、パスワードで保護されたコマンドに使用されます。パスワードで保護されたコマンドを実行する場合、通常は、パスワードの入力を求められます。これは、セキュリティ上の理由です。ウイルスからの保護機能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などに適用されます。そのようなコマンドは、実行ごとにパスワードを要求します。代わりに、現在のeShellセッションに対してこのパスワードを定義すれば、パスワードの入力を求められなくなります。

対話的にパスワードを入力する場合は（推奨）、パラメータを空にします。パスワードをリセットするには、空のパスワードを入力します。

例:
get password-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"*"を表示するだけでパスワード自体は表示しません）。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-パスワードを設定する場合に使用し、そのままパスワードを入力します（パスワードを入力しない場合、設定の保護は使用されません）

restore password-このコマンドは既存のパスワードを削除します（設定の保護は使用されません）

同等なGUI:
GUIを使用する設定方法については、「設定の保護」を参照してください。

4.10.2.61 コンテキスト-GENERAL ESHELL

ALIAS
エイリアス管理

構文:
[get] | clear | restore alias
add alias [.] <alias>=<command>
remove alias<alias>
import | export alias<path>

操作:
get-現在の設定/状態を表示する
add-項目の追加
remove-項目の削除
import-ファイルからインポート
export-ファイルにエクスポート
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
.-グローバルエイリアスを作成する
alias-新規エイリアス
command–対応するコマンド（コマンドの有効性は確認されない）
path-ファイルパス

LISTER
分割表示

構文:
[get] | restore lister
set lister disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.62 コンテキスト-GENERAL ESHELL COLOR

ALIAS
エイリアスの色

構文:
[get] | restore alias
set alias [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
black-黒
navy-紺
grass-若草色
ltblue-ライトブルー
brown-茶
purple-紫
olive-オリーブグリーン
ltgray-ライトグレー
gray-グレー
blue-青
green-緑
cyan-シアン
red-赤
magenta-マゼンダ

yellow-黄
white-白

COMMAND
コマンドの色

構文:
[get] | restore command

set command [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
black-黒
navy-紺
grass-若草色
ltblue-ライトブルー
brown-茶
purple-紫
olive-オリーブグリーン
ltgray-ライトグレー
gray-グレー
blue-青
green-緑
cyan-シアン
red-赤
magenta-マゼンダ
yellow-黄
white-白

CONTEXT
コンテキストの色

構文:
[get] | restore context
set context [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

操作:
get-現在の設定/状態を表示する

set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
black-黒
navy-紺
grass-若草色
ltblue-ライトブルー
brown-茶
purple-紫
olive-オリーブグリーン
ltgray-ライトグレー
gray-グレー
blue-青
green-緑
cyan-シアン
red-赤
magenta-マゼンダ
yellow-黄
white-白

DEFAULT
基本色

構文:
[get] | restore default
set default [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
black-黒
navy-紺
grass-若草色
ltblue-ライトブルー
brown-茶
purple-紫
olive-オリーブグリーン
ltgray-ライトグレー
gray-グレー
blue-青

green-緑
cyan-シアン
red-赤
magenta-マゼンダ
yellow-黄
white-白

DISABLED

使用できない色

構文:
[get] | restore disabled
set disabled [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
black-黒
navy-紺
grass-若草色
ltblue-ライトブルー
brown-茶
purple-紫
olive-オリーブグリーン
ltgray-ライトグレー
gray-グレー
blue-青
green-緑
cyan-シアン
red-赤
magenta-マゼンダ
yellow-黄
white-白

ERROR

エラーの色

構文:
[get] | restore error
set error [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
black-黒
navy-紺
grass-若草色
ltblue-ライトブルー
brown-茶
purple-紫
olive-オリーブグリーン
ltgray-ライトグレー
gray-グレー
blue-青
green-緑
cyan-シアン
red-赤
magenta-マゼンダ
yellow-黄
white-白

INTERACTIVE
対話式操作の色

構文:
[get] | restore interactive
set interactive [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
black-黒
navy-紺
grass-若草色
ltblue-ライトブルー
brown-茶
purple-紫
olive-オリーブグリーン

ltgray-ライトグレー
gray-グレー
blue-青
green-緑
cyan-シアン
red-赤
magenta-マゼンダ
yellow-黄
white-白

LIST1

リストの色1

構文:
[get] | restore list1
set list1 [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
black-黒
navy-紺
grass-若草色
ltblue-ライトブルー
brown-茶
purple-紫
olive-オリーブグリーン
ltgray-ライトグレー
gray-グレー
blue-青
green-緑
cyan-シアン
red-赤
magenta-マゼンダ
yellow-黄
white-白

LIST2

リストの色2

構文:
[get] | restore list2
set list2 [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

操作
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
black-黒
navy-紺
grass-若草色
ltblue-ライトブルー
brown-茶
purple-紫
olive-オリーブグリーン
ltgray-ライトグレー
gray-グレー
blue-青
green-緑
cyan-シアン
red-赤
magenta-マゼンダ
yellow-黄
white-白

SUCCESS
状態良好の色

構文:
[get] | restore success
set success [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]
操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
black-黒
navy-紺
grass-若草色
ltblue-ライトブルー

brown-茶
purple-紫
olive-オリーブグリーン
ltgray-ライトグレー
gray-グレー
blue-青
green-緑
cyan-シアン
red-赤
magenta-マゼンダ
yellow-黄
white-白

WARNING
警告の色

構文:
[get] | restore warning
set warning [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元
パラメータ:
black-黒
navy-紺
grass-若草色
ltblue-ライトブルー
brown-茶
purple-紫
olive-オリーブグリーン
ltgray-ライトグレー
gray-グレー
blue-青
green-緑
cyan-シアン
red-赤
magenta-マゼンダ
yellow-黄
white-白

4.10.2.63 コンテキスト- GENERAL ESHELL OUTPUT

UTF8

UTF8エンコード出力

構文:

[get] | restore utf8

set utf8 disabled | enabled

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

disabled-機能の無効化/設定の無効化

enabled-機能の有効化/設定の有効化

NOTE

正しく表示するには、コマンドラインに'Lucida Console'などのTrueTypeフォントを使用する必要があります。

4.10.2.64 コンテキスト- GENERAL ESHELL STARTUP

LOADCOMMANDS

起動時にすべてのコマンドをロード

構文:

[get] | restore loadcommands

set loadcommands disabled | enabled

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

disabled-機能の無効化/設定の無効化

enabled-機能の有効化/設定の有効化

STATUS

起動時に保護の状態を表示

構文:

[get] | restore status

set status disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.65 コンテキスト- GENERAL ESHELL VIEW

CMDHELP

コマンド失敗時にヘルプを表示

構文:
[get] | restore cmdhelp
set cmdhelp disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

COLORS

カラーを使用

構文:
[get] | restore colors
set colors disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

FITWIDTH

幅に合わせてテキストをトリミング

構文:
[get] | restore fitwidth
set fitwidth disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

GLOBAL
グローバルコマンドを表示

構文:
[get] | restore global
set global disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

HIDDEN
非表示コマンドを表示

構文:
[get] | restore hidden
set hidden disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

OPERATIONS
コマンドリストに操作を表示

構文:
[get] | restore operations
set operations disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

SHORTLIST
コンテキスト変更時に短縮形コマンドリストを表示

構文:
[get] | restore shortlist
set shortlist disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

SYNTAXHINT
コマンド構文のヒントを表示します。

構文:
[get] | restore syntaxhint
set syntaxhint disabled | enabled
操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化

enabled-機能の有効化/設定の有効化

VALUESONLY
説明を含めないで値を表示

構文:
[get] | restore valuesonly
set valuesonly disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.66 コンテキスト- GENERAL PERFORMANCE

SCANNERS
ThreatSenseの検査スレッド数

構文:
[get] | restore scanners set scanners<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-数（1～20）

4.10.2.67 コンテキスト-GENERAL PROXY

ADDRESS
プロキシサーバーアドレス

構文:
[get] | restore address set address [<string>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-アドレス

DETECT
プロキシサーバ設定の検出

構文:
detect

LOGIN
ユーザー名

構文:
[get] | restore login set login [<string>] 操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-ユーザー名

PASSWORD
パスワード

構文:
[get] | restore password
set password [plain<password>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

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

PORT
サーバーポート

構文:
[get] | restore port set port<number>

操作:
get-現在の設定/状態を表示する

set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-ポート番号

USE
プロキシサーバを使用する

構文:
[get] | restore use
set use disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.68 コンテキスト- GENERAL QUARANTINE RESCAN

UPDATE
アップデート後は毎回隔離ファイルを検査する

構文:
[get] | restore update
set update disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.69 コンテキスト- GENERAL REMOTE

INTERVAL
サーバへの接続間隔

構文:
[get] | restore interval set interval<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-時間/分（1～1440）

USE
リモート管理サーバに接続する

構文:
[get] | restore use
set use disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.70 コンテキスト- GENERAL REMOTE SERVER PRIMARY

ADDRESS
サーバのアドレス

構文:
[get] | restore address set address [<string>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-アドレス

ENCRYPT
接続が安全ではないサーバには接続しない

構文:
[get] | restore encrypt
set encrypt disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

PASSWORD
パスワード

構文:
[get] | restore password
set password [plain<password>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
plain–パラメータとしてパスワードを入力する方式に切り替える
password-パスワード

PORT
サーバポート

構文:
[get] | restore port set port<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-ポート番号

4.10.2.71 コンテキスト- GENERAL REMOTE SERVER SECONDARY

ADDRESS
サーバのアドレス

構文:
[get] | restore address set address [<string>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-アドレス

ENCRYPT
接続が安全ではないサーバには接続しない

構文:
[get] | restore encrypt
set encrypt disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

PASSWORD
パスワード

構文:
[get] | restore password
set password [plain<password>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

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

PORT
サーバポート

構文:
[get] | restore port set port<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-ポート番号

4.10.2.72 コンテキスト- GENERAL TS.NET

EXCLUSION
提出から除外する

構文:
[get] | restore exclusion
add | remove exclusion<exclusion>

操作:
get-現在の設定/状態を表示する
add-項目の追加
remove-項目の削除
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
exclusion–除外

FROM
連絡先の電子メールアドレス

構文:
[get] | restore from set from [<string>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-電子メールアドレス

LOGING
ログを有効にする

構文:
[get] | restore loging
set loging disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

SENDING
不審なファイル

構文:
[get] | restore sending
set sending none | ask | auto

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
none–分析のために提出しない
ask–提出前に確認する
auto-確認せずに送信する

VIA
提出

構文:
[get] | restore via
set via auto | ra | direct

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
auto-リモート管理者経由または直接ESETへ
ra-リモート管理者経由
direct-直接ESETへ

WHEN
提出するタイミング

構文:
[get] | restore when set when asap | update

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
asap–即時
update-アップデート時

4.10.2.73 コンテキスト- GENERAL TS.NET STATISTICS

SENDING
匿名の統計情報を提出する

構文:
[get] | restore sending
set sending disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化
WHEN
提出するタイミング

構文:
[get] | restore when set when asap | update

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
asap –即時
update-アップデート時

4.10.2.74 コンテキスト- SCANNER

CLEANLEVEL

駆除レベル

構文:

[get] | restore cleanlevel

set cleanlevel none | normal | strict

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

none-駆除なし

normal-標準的な駆除

strict-厳密な駆除

EXTENSIONS

拡張子

構文:

[get] | restore extensions

add | remove extensions<extension>|/all |/extless

操作:

get-現在の設定/状態を表示する

add-項目の追加

remove-項目の削除

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

extension-拡張子

/all-すべてのファイル

/extless-拡張子のないファイル

PROFILE

コンピュータの検査のプロファイル管理

構文:

[get] profile

select | remove profile<name>

add profile new:<name> [copyfrom:<name>]

操作:
get-現在の設定/状態を表示する
select-項目の選択
add-項目の追加 remove-項目の削除 パラメータ:
name-プロファイル名
new-新規プロファイル
copyfrom-プロファイルの設定をコピー

››› NOTE

他のコンテキストコマンド はアクティブプロファイル(xとマークされている) を参照します。アクティブプロファイル を選択するには、'select scanner profile <プロファイル名>'を使用します。

SCAN

コンピュータの検査

構文:
[get] | clear scan
start scan [elevate] [readonly] [profile:<name>] [target:<path>|<X>:¥ $ {Boot}| $ [Memory]]
[target:<path>] […]
pause | resume | stop scan<ID>| all

操作:
get–実行中の検査と完了した検査を表示する
start-選択したプロファイルについてのコンピュータの検査を実行する
stop-検査を中止する
resume-中断した検査を再開する
pause-検査を中断する
clear-完了した検査をリストから削除するパラメータ:
elevate–管理者として検査する
readonly-駆除せずに検査する
profile–プロファイルを使用する
name–プロファイル名
target–検査対象を指定する
path–検査対象のパス
X–ドライブ文字
$ {Boot}–ディスク'X'のブートセクターの検査
$ {Memory}–メモリ検査
ID–検査ID (実行済み検査の識別用ナンバー)
all–すべての検査IDを対象にする

TARGET

アクティブプロファイルで検査する対象

構文:
[get] target
add | remove target<path>|<X>:¥$ {Boot}| $ {Memory}

操作:
get-現在の設定/状態を表示する
add-項目の追加 remove-項目の削除パラメータ:
path-検査の対象/ローカルまたはネットワークのパス
X-ドライブ文字
$ {Boot}-ディスク'X'のブートセクター検査
$ {Memory}-メモリ検査

NOTE

ブートセクタの検査の場合は、X:¥$ {Boot}と入力します。ここで、'X'は、検査対象のドライブ文字です。

4.10.2.75 コンテキスト-SCANNER LIMITS ARCHIVE

LEVEL

スキャン対象の下限ネストレベル

構文:
[get] | restore level set level<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-レベルは1～20、または既定の設定は0

SIZE

スキャン対象のファイルの最大サイズ(kB)

構文:
[get] | restore size set size<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-サイズ/kB(1～3145728)、既定の設定は0

4.10.2.76 コンテキスト-SCANNER LIMITS OBJECTS

SIZE

オブジェクトの最大サイズ（KB）

構文:

[get] | restore size set size<number>

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

number-サイズ/kB（1～3145728）、既定の設定は0

TIMEOUT

オブジェクトの最大検査時間（秒）

構文:

[get] | restore timeout set timeout<number>

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

number-時間/秒、既定の設定は0

4.10.2.77 コンテキスト-SCANNER OBJECTS

ARCHIVE

アーカイブを検査する

構文:

[get] | restore archive

set archive disabled | enabled

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

disabled-機能の無効化/設定の無効化

enabled-機能の有効化/設定の有効化

BOOT
ブートセクタを検査する

構文:
[get] | restore boot
set boot disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

EMAIL
電子メールファイルを検査する

構文:
[get] | restore email
set email disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

MEMORY
システムメモリを検査する

構文:
[get] | restore memory
set memory disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

RUNTIME
圧縮された実行形式を検査する

構文:
[get] | restore runtime
set runtime disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

SFX
自己解凍形式を検査する

構文:
[get] | restore sfx
set sfx disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.78 コンテキスト-SCANNER OPTIONS

ADVHEURISTICS
アドバンスドヒューリスティックを使用する

構文:
[get] | restore advheuristics
set advheuristics disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

HEURISTICS
ヒューリスティックを使用する

構文:
[get] | restore heuristics
set heuristics disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

UNSAFE
安全ではない可能性があるアプリケーションを検出する

構文:
[get] | restore unsafe
set unsafe disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

UNWANTED
望ましくない可能性があるアプリケーションを検出する

構文:
[get] | restore unwanted
set unwanted disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.79 コンテキスト-SCANNER OTHER

ADS
代替データストリーム（ADS）を検査

構文:
[get] | restore ads
set ads disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

LOGALL
すべてのオブジェクトをログに記録する

構文:
[get] | restore logall
set logall disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

LOWPRIORITY
低優先でバックグラウンドで検査

構文:
[get] | restore lowpriority
set lowpriority disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

OPTIMIZE

SMART最適化を有効にする

構文:
[get] | restore optimize
set optimize disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

PRESERVETIME

最終アクセスのタイムスタンプを保持

構文:
[get] |restore preservetime
set preservetime disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

SCROLL
検査ログをスクロールする

構文:
[get] | restore scroll
set scroll disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.80 コンテキスト-SERVER

AUTOEXCLUSIONS
自動除外の管理

構文:
[get] | restore autoexclusions select autoexclusions<server>操作:
get-現在の設定/状態を表示する
select-項目の選択
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
server-サーバ名

4.10.2.81 コンテキスト-TOOLS

QUARANTINE
隔離

構文:
[get] quarantine
add quarantine<path>
send | remove | restore quarantine<ID>

操作:
get-現在の設定/状態を表示する
add-項目の追加
remove-項目の削除
restore-既定の設定/オブジェクト/ファイルを復元
send–オブジェクト/ファイルを送信

パラメータ:
path-ファイルパス
ID-隔離されたファイルのID

STATISTICS
統計

構文:
[get] | clear statistics

操作:
get-統計の表示
clear-統計のリセット

SYSINSPECTOR
SysInspector

構文:
[get] sysinspector
add | remove sysinspector<name>export sysinspector<name>to:<path>操作:
get-現在の設定/状態を表示する
add-項目の追加
remove-項目の削除
export-ファイルにエクスポートパラメータ:
name-コメント
path-ファイル名(.zipまたは.xml)

4.10.2.82 コンテキスト-TOOLS ACTIVITY

FILESYSTEM
ファイルシステム

構文:
[get] filesystem [<count>] [seconds | minutes | hours [<year>-<month>]]

4.10.2.83 コンテキスト-TOOLS LOG

DETECTIONS
検出されたマルウェアのログ

構文:
[get] detections [count<number>] [from<year>-<month>-<day><hour>:<minute>:<second>]
[to<year>-<month>-<day><hour>:<minute>:<second>]
clear detections

操作:
get-現在の設定/状態を表示する

clear-すべてのアイテム/ファイルを削除

パラメータ:
count-選択されたレコード数を表示する
number-レコード数
from-指定された時間のレコードを表示する
year-年
month-月
day-日
hour-時間
minute-分
second-秒
to-選択された時間までのレコードを表示する

エイリアス:
virlog

例:
get detections from 2011-04-14 01:30:00-20114年4月14日01:30:00以降に検出されたすべてのマルウェアを表示します
(コマンドを正常に機能させるには、日付を定義するときに時刻も含める必要あり)。
clear detections-ログ全体を削除します。

EVENTS
イベントログ

構文:
[get] events [count<number>] [from<year>-<month>-<day><hour>:<minute>:<second>] [to<year>-<month>-<day><hour>:<minute>:<second>]
clear events

操作:
get-現在の設定/状態を表示する
clear-すべてのアイテム/ファイルを削除

パラメータ:
count-選択されたレコード数を表示する
number-レコード数
from-指定された時間のレコードを表示する
year-年
month-月
day-日
hour-時間
minute-分
second-秒

to-選択された時間までのレコードを表示する
エイリアス:
warnlog

例:
get events from 2011-04-14 01:30:00-20114年4月14日01:30:00以降に発生したすべてのイベントを表示します（コマンドを正常に機能させるには、日付を定義するときに時刻も含める必要あり）。
clear events-ログ全体を削除します。

FILTER
表示するイベントの種類

構文:
[get] | restore filter
set |add | remove filter [[none] [critical] [errors] [warnings] [informative] [diagnostic] |all] [smart]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
none-レコードなし
critical–重大な警告
errors-エラー
warnings–警告
informative-情報レコード
diagnostic-診断レコード
all-すべてのレコード
smart–Smartフィルタリング

SCANS
'コンピュータの検査'ログまたはログリスト

構文:
[get] scans [id:<id>] [count:<number>] [from:<year>-<month>-<day><hour>:<minute>:<second>]
[to:<year>-<month>-<day><hour>:<minute>:<second>]
clear scans

操作:
get-現在の設定/状態を表示する
clear-すべてのアイテム/ファイルを削除

パラメータ:
id-IDを使用してコンピュータ検査の詳細を表示する

count-選択された個数のレコードのみを表示する
number-レコード数
from-選択された時間のレコードのみを表示する
year-年
month-月
day-日
hour-時間
minute-分
second-秒
to-選択された時間のレコードのみを表示する

VERBOSITY
ログに記録する最小レベル

構文:
[get] | restore verbosity
set verbosity critical | errors | warnings | informative | diagnostic

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
critical–重大な警告
errors-エラー
warnings-警告
informative-情報レコード
diagnostic-診断レコード

4.10.2.84 コンテキスト-TOOLS LOG CLEANING

TIMEOUT
ログエントリの有効期限（日）

構文:
[get] | restore timeout set timeout<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-日数（1～365）

USE
エントリを自動的に削除する

構文:
[get] | restore use
set use disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.85 コンテキスト-TOOLS LOG OPTIMIZE

LEVEL
使用されていないエントリの割合が次の値よりもおおきくなったら最適化

構文:
[get] | restore level set level<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-使用されていないレコードの割合（1～100）

USE
ログファイルを自動に最適化する

構文:
[get] | restore use
set use disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.86 コンテキスト-TOOLS NOTIFICATION

VERBOSITY

通知の最小レベル

構文:

[get] | restore verbosity

set verbosity critical | errors | warnings | informative | diagnostic

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

critical–重大な警告

errors-エラー

warnings-警告

informative-情報レコード

diagnostic-診断レコード

4.10.2.87 コンテキスト-TOOLS NOTIFICATION EMAIL

FROM

送信者アドレス

構文:

[get] | restore from set from [<string>]

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

string-電子メールアドレス

LOGIN

ユーザー名

構文:

[get] | restore login set login [<string>]

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string–ユーザー名

PASSWORD
パスワード

構文:
[get] |restore password
set password [plain<password>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
plain–パラメータとしてパスワードを入力する方式に切り替える
password-パスワード

SERVER
SMTPサーバ

構文:
[get] | restore server set server [<string>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-アドレス

TO
受信者アドレス

構文:
[get] | restore to set to [<string>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-電子メールアドレス

USE
イベント通知をメールで送信する

構文:
[get] | restore use
set use disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.88 コンテキスト-TOOLS NOTIFICATION MESSAGE

ENCODING
警告メッセージのエンコード

構文:
[get] | restore encoding
set encoding nolocal | localcharset | localencoding | ISO-2022-JP

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
nolocal–各地域のアルファベット文字を使用しない
localcharset–各地域のアルファベット文字を使用する
localencoding–各地域の文字エンコーディングを使用する
ISO-2022-JP-ISO-2022-JPエンコードを使用する（日本語版のみ）

4.10.2.89 コンテキスト-TOOLS NOTIFICATION MESSAGE FORMAT

EVENT
イベントメッセージの書式

構文:
[get] | restore detection set detection [<string>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-メッセージの書式
メッセージのフォーマットオプションは次のとおり。
% TimeStamp % -イベントの日時
% Scanner % -イベントを検出した機能
% ComputerName % -コンピューター名
% ProgramName % -イベントの原因となったプログラム
% ErrorDescription % -エラーの説明

メッセージフォーマットについては、キーワード(パーセント記号"% "で囲まれた部分)を対応する値に置き換える必要があ ります。

NOTE

ESET File Security for Microsoft Windows Serverのウイルスメッセージおよび警告には、既定のフォーマットがあります。このフォーマットを変更することはお勧めしません。自動メール処理システムを使用している場合は、このフォーマットを変更できます。

DETECTION

脅威メッセージの書式

構文:
[get] | restore event set event [<string>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-メッセージの書式
メッセージのフォーマットオプションは次のとおり。
% TimeStamp % -イベントの日時
% Scanner % -イベントを検出した機能
% ComputerName % -コンピューター名
% ProgramName % -イベントの原因となったプログラム
% InfectedObject % -感染しているオブジェクト(ファイル、電子メール…)
% VirusName % -ウイルス名

メッセージフォーマットについては、キーワード(パーセント記号"% "で囲まれた部分)を対応する値に置き換える必要があります。

NOTE

ESET File Security for Microsoft Windows Serverのウイルスメッセージおよび警告には、既定のフォーマットがあります。このフォーマットを変更することはお勧めしません。自動メール処理システムを使用している場合は、このフォーマットを変更できます。

4.10.2.90 コンテキスト-TOOLS NOTIFICATION WINPOPUP

ADDRESS

通知の送信先コンピューター名

構文:

[get] | restore address set address [<string>]

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

string-コンピューター名はカンマ区切りで指定

TIMEOUT

メッセージの送信間隔

構文:

[get] | restore timeout set timeout<number>

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元パラメータ:

number-間隔/秒単位（1～3600）

USE

イベント通知をメッセンジャーサービスでLAN上のコンピューターに送信する

構文:

[get] | restore use

set use disabled | enabled

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.91　コンテキスト-TOOLS SCHEDULER

ACTION

スケジュールされたタスクのアクション

構文:
[get] action
set action external | logmaintenance | startupcheck | status | scan | update | asrulesupdate

操作:
get-現在の設定/状態を表示する
set-値/状態を設定

パラメータ:
external-外部アプリケーションの実行
logmaintenance-ログの保守
startupcheck–システムのスタートアップファイルのチェック
status-コンピューターの状態のスナップショットを作成する
scan-コンピュータの検査
update-アップデート
asrulesupdate–迷惑メール対策エンジンルールのアップデート

TASK

スケジュールされたタスク

構文:
[get] | select task [<ID>]
set task<ID>disabled | enabled
add task<task_name>
remove | start task<ID>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
select-項目の選択
add-項目の追加
remove-項目の削除
start-タスクの開始パラメータ:
ID-タスクID
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化
task_name-タスク名

TRIGGER
タスクの実行

構文:
[get] trigger
set trigger once | repeat | daily | weekly | event

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
パラメータ:
once-1回
repeat-繰り返し
daily-毎日
weekly-毎週
event-イベントごと

4.10.2.92 コンテキスト-TOOLS SCHEDULER EVENT

INTERVAL
以下の時間内は1回しか実行しない

構文:
[get] interval
set interval<hours>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定パラメータ:
hours-時間数（1～720時間）

TYPE
タスクを実行するイベント

構文:
[get] type
set type startup | firststartup | dialup | engineupdate | appupdate | logon | detection

操作:
get-現在の設定/状態を表示する
set-値/状態を設定

パラメータ:
startup-コンピュータの起動
firststartup-その日の最初のコンピュータ起動時
dialup-インターネット/VPNへのダイヤルアップ接続

engineupdate-成功したウイルス定義データベースのアップデート
appupdate-成功したプログラムコンポーネントのアップデート
logon-ユーザのグオン
detection-ウイルス検出

4.10.2.93 コンテキスト-TOOLS SCHEDULER FAILSAFE

EXECUTE

タスクが実行されなかった場合のアクション

構文:
[get] execute
set execute asap | iftimeout | no

操作:
get-現在の設定/状態を表示する
set-値/状態を設定

パラメータ:
asap-実行可能になり次第実行する
iftimeout-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
no-次のスケジュール設定日時まで待機

▸▸▸ NOTE

制限を設定するには、次のように入力します。
SET TOOLS SCHEDULER EDIT FAILSAFE TIMEOUT<HOURS>

TIMEOUT

タスクの実行間隔（時間）

構文:
[get] timeout
settimeout<hours>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定

パラメータ:
hours-時数（1～720時間）

4.10.2.94 コンテキスト-TOOLS SCHEDULER PARAMETERS CHECK

LEVEL

検査レベル

構文:
[get] level
set level [before_logon | after_logon | most_frequent | frequent | common | rare | all]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定

パラメータ:
before_logon-ユーザーのログオン前に実行されるファイル
after_logon-ユーザーのログオン後に実行されるファイル
most_frequent-最も使用頻度が高いファイルのみ
frequent-使用頻度が高いファイル
common-使用頻度が中程度のファイル
rare-使用頻度が低いファイル
all–すべての登録ファイル

PRIORITY

検査の優先度

構文:
[get] priority
set priority [normal | low | lowest | idle]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定パラメータ:
normal-通常
low-低
lowest-最低
idle-アイドル時

4.10.2.95 コンテキスト-TOOLS SCHEDULER PARAMETERS EXTERNAL

ARGUMENTS

パラメータ

構文:
[get] arguments
setarguments<arguments>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定

パラメータ:
arguments-パラメータ

DIRECTORY

作業フォルダ

構文:
[get] directory
set directory<path>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定

パラメータ:
path-パス

EXECUTABLE

実行可能ファイル

構文:
[get] executable
set executable<path>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定

パラメータ:
path-パス

4.10.2.96 コンテキスト-TOOLS SCHEDULER PARAMETERS SCAN

PROFILE

検査プロファイル

構文:
[get] profile
set profile<profile>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定

パラメータ:
profile-プロファイル名

READONLY

駆除せずに検査する

構文:
[get] readonly
set readonly disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

TARGET

検査の対象

構文:
[get] | clear target
add | remove target<path>

操作:
get-現在の設定/状態を表示する
add-項目の追加
remove-項目の削除
clear-すべてのアイテム/ファイルを削除

パラメータ:
path-検査のパス/対象

4.10.2.97　コンテキスト-TOOL SSCHEDULER PARAMETERS UPDATE

PRIMARY

アップデート時に使用するプロファイル

構文:
[get] primary
set primary [<profile>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定パラメータ:
profile-プロファイル名

SECONDARY

アップデート時に使用するセカンダリプロファイル

構文:
[get] secondary
set secondary [<profile>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定

パラメータ:
profile-プロファイル名

4.10.2.98　コンテキスト-TOOLS SCHEDULER REPEAT

INTERVAL

タスクの実行間隔（分）

構文:
[get] interval
set interval<minutes>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定

パラメータ:
minutes-時間/分（1～720時間）

4.10.2.99 コンテキスト-TOOLS SCHEDULER STARTUP

DATE

タスクの実行日

構文:
[get] date
set date<year>-<month>-<day>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定

パラメータ:
year-年
month-月
day-日

DAYS

次の曜日にタスクを実行する

構文:
[get] days
Set | add | remove days none [monday] [tuesday] [wednesday] [thurdsday] [friday] [saturday] [sunday] | all

操作:
get-現在の設定/状態を表示する
set-値/状態を設定

パラメータ:
none-曜日の指定なし
monday-月曜日
tuesday-火曜日
wednesday-水曜日
thurdsday-木曜日
friday-金曜日
saturday-土曜日
sunday-日曜日
all-毎日

TIME

タスクの実行時刻

構文:
[get] time

settime<hour>:<minute>:<second>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定

パラメータ:
hour-時間
minute-分
second-秒

4.10.2.100　コンテキスト-UPDATE

CACHE
アップデートキャッシュのクリア

構文:
clear cache

COMPONENTS
プログラムコンポーネントのアップデート

構文:
[get] | restore components
set components never | allways | ask

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
never-プログラムコンポーネントをアップデートしない
allways-プログラムコンポーネントをアップデートする
ask-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

LOGIN
ユーザー名

構文:
[get] | restore login set login [<string>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-名前

NOTE
購入時または登録時に受け取ったユーザー名とパスワードを入力してください。登録メールからコピー(Ctrl+C) してペースト(Ctrl+V) することを強くお勧めします。

PASSWORD
パスワード

構文:
[get] | restore password
set password [plain<password>]

操作:
get-パスワードを表示する
set-パスワードの設定または削除
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
plain–パラメータとしてパスワード入力に切り替える
password-パスワード

NOTE
購入時または登録時に受け取ったユーザー名とパスワードを入力してください。登録メールからコピー(Ctrl+C) してペースト(Ctrl+V) することを強くお勧めします。

PRERELEASE
テストモードを有効にする

構文:
[get] | restore prerelease
set prerelease disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

PROFILE
アップデートプロファイル管理

構文:
[get] profile
select | remove profile<name>
add profile new:<name> [copyfrom:<name>]

操作:
get-現在の設定/状態を表示する
select-項目の選択
add-項目の追加
remove-項目の削除

パラメータ:
name-プロファイル名
new-新規プロファイル
copyfrom–次のプロファイルの設定をコピー

▸▸▸ NOTE

他のコンテキストコマンドはアクティブプロファイル(xとマークされている) を参照します。アクティブプロファイルを選択するには、select update profile<profilename>を使用します。

SERVER

アップデートサーバ

構文:
[get] | restore server
select | add | remove server<server>

操作:
get-現在の設定/状態を表示する
select-項目の選択
add-項目の追加
remove-項目の削除
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
server-サーバアドレス

STATUS

アップデート状態を表示する

構文:
[get] status

UPDATE

アップデート

構文:
start | stop update

操作:
start-アップデートの実行
stop-アップデートのキャンセル

4.10.2.101 コンテキスト-UPDATE CONNECTION

DISCONNECT
アップデート終了後にサーバから切断する

構文:
[get] | restore disconnect
set disconnect disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

LOGIN
ユーザー名

構文:
[get] | restore login
set login [<string>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-名前

PASSWORD
パスワード

構文:
[get] | restore password
set password [plain<password>]

操作:
get-パスワードを表示する
set-パスワードを設定または削除する
restore-既定の設定/オブジェクト/ファイルを復元パラメータ:
plain-パスワードをパラメータとして入力するように切り替える
password-パスワード

RUNAS
アップデートサーバーへの接続に使用するユーザーアカウント

構文:
[get] | restore runas
set runas system | current | specified

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
system-システムアカウント（既定）
current-現在のユーザー
specified-指定したユーザー

4.10.2.102　コンテキスト- UPDATE MIRROR

FOLDER
配布用ファイルの保存先

構文:
[get] | restore folder set folder [<string>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-フォルダのパス

LOGIN
ユーザー名

構文:
[get] | restore login set login [<string>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-名前

PASSWORD
パスワード

構文:
[get] | restore password
set password [plain<password>]

操作:
get-パスワードを表示します。
set-パスワードを設定または削除する
restore-既定の設定/オブジェクト/ファイルを復元パラメータ:
plain-パスワードをパラメータとして入力するように切り替える
password-パスワード

USE
配布用アップデートを作成する

構文:
[get] | restore use
set use disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

VERSIONS
アップデートバージョンの管理

構文:
[get] | restore versions select versions<version>

操作:
get-利用可能なバージョンの表示
select-アップデートバージョンの選択/選択解除
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
version-バージョン名

4.10.2.103　コンテキスト-UPDATE MIRROR SERVER

AUTHORIZATION

認証

構文:
[get] | restore authorization
set authorization none | basic | ntlm

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
none–NONE
basic–Basic
ntlm-NTLM

PORT

サーバーポート

構文:
[get] | restore port set port<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-ポート番号

USE

内蔵のHTTPサーバーよりアップデートファイルを提供する

構文:
[get] | restore use

set use disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

4.10.2.104 コンテキスト-UPDATE NOTIFICATION

DOWNLOAD
アップデートをダウンロードする前に確認する

構文:
[get] | restore download
set download disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

HIDE
成功したアップデートについての通知を表示しない

構文:
[get] | restore hide
set hide disabled | enabled

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
disabled-機能の無効化/設定の無効化
enabled-機能の有効化/設定の有効化

SIZE
アップデートファイルが次のサイズ(kB)より大きい場合に確認する

構文:
[get] | restore size set size<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-ファイルサイズ(0～2097151kB)

▸▸▸ NOTE

0を指定するとアップデート通知が無効になります。

4.10.2.105 コンテキスト-UPDATE PROXY

LOGIN

ユーザー名

構文:
[get] | restore login set login [<string>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-名前

MODE

HTTPプロキシの設定

構文:
[get] | restore mode
set mode global | noproxy | userdefined

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元パラメータ:
global-プロキシサーバのグローバル設定を使用する
noproxy-プロキシサーバを使用しないuserdefined-プロキシサーバ経由で接続する

PASSWORD

パスワード

構文:
[get] | restore password
set password [plain<password>]

操作:
get-パスワードを表示します。
set-パスワードを設定または削除する
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
plain-パスワードをパラメータとして入力するように切り替える
password-パスワード

PORT
サーバポート

構文:
[get] | restore port set port<number>

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
number-ポート番号

SERVER
プロキシサーバ

構文:
[get] | restore server set server [<string>]

操作:
get-現在の設定/状態を表示する
set-値/状態を設定
restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:
string-サーバアドレス

4.10.2.106　コンテキスト-UPDATE SYSTEM

NOTIFY

アップデートが未適用の場合に次のレベルから通知

構文:

[get] | restore notify

set notify no | optional | recommended | important | critical

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

no–通知しない

optional-オプションのアップデート

recommended-推奨されるアップデート

important-重要なアップデート

critical-重大なアップデート

RESTART

プログラムコンポーネントアップデート後の再起動

構文:

[get] | restore restart

set restart never | ask | auto

操作:

get-現在の設定/状態を表示する

set-値/状態を設定

restore-既定の設定/オブジェクト/ファイルを復元

パラメータ:

never–コンピュータを再起動しない

ask–必要な場合はコンピュータの再起動を促す

auto–必要な場合は確認せずコンピュータを再起動する

4.11 設定のインポート/エクスポート

ESET File Security for Microsoft Windows Serverの設定のインポートとエクスポートは、[設定]で[設定をインポートおよびエクスポートする]をクリックして使用できます。

インポートおよびエクスポートのいずれにも、.xmlファイルタイプを使用します。エクスポートは、ESET File Security for Microsoft Windows Serverの現在の設定をバックアップする必要がある場合に便利です。エクスポートしたデータは基本となる設定ファイルとして、他のESET File Security for Microsoft Windows Serverに対して適用する場合にも利用できます。

4.12 Threat Sense.Net

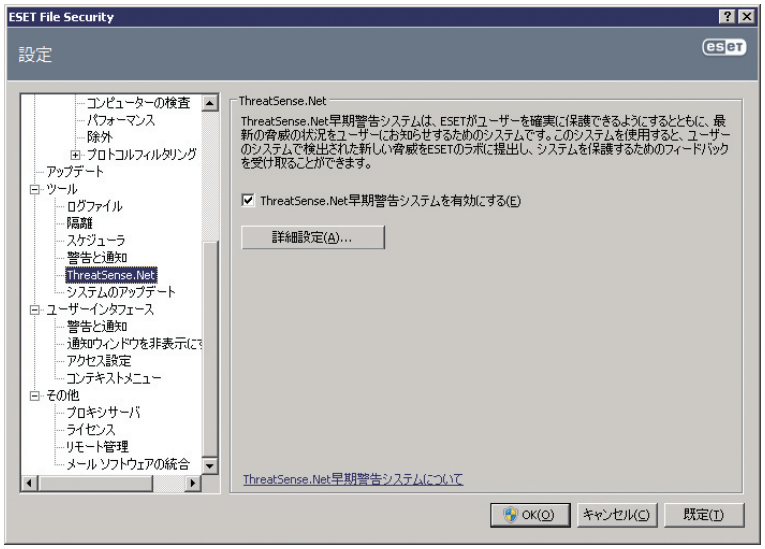
ThreatSense.Net早期警告システムにより、ESETは新しいマルウェアを迅速かつ継続的に把握することができます。

ThreatSense.Net早期警告システムでは、検出された疑わしいファイルのサンプル、そのファイルのパス、ファイル名、日時、ウイルスがコンピューターに侵入したプロセス、およびコンピューターのオペレーティングシステムについての情報を収集します。そして、その情報を元に解析を行い新しいマルウェアかどうか判定します。

この結果、ユーザーやコンピューターに関する情報（ディレクトリパスのユーザー名など）は、新しいウイルスに迅速に対応する以外の目的でこの情報が使用されることはありません。

既定では、ESET File Security for Microsoft Windows Serverは、詳しい解析を受けるために疑わしいファイルをESETのウイルスラボに提出する前に確認メッセージが表示されるように設定されています。.doc、.xlsなど特定の拡張子を持つファイルは常に除外されます。お客様やお客様の会社で送信したくない特定のファイルがあれば、他の拡張子を追加することもできます。

ThreatSense.Netの設定の設定は、[詳細設定] ツリーで [ツール] > [ThreatSense.Net] の順に選択します。[ThreatSense早期警告システムを有効にする] オプションを選択して有効にしてから [詳細設定...] ボタンをクリックします。

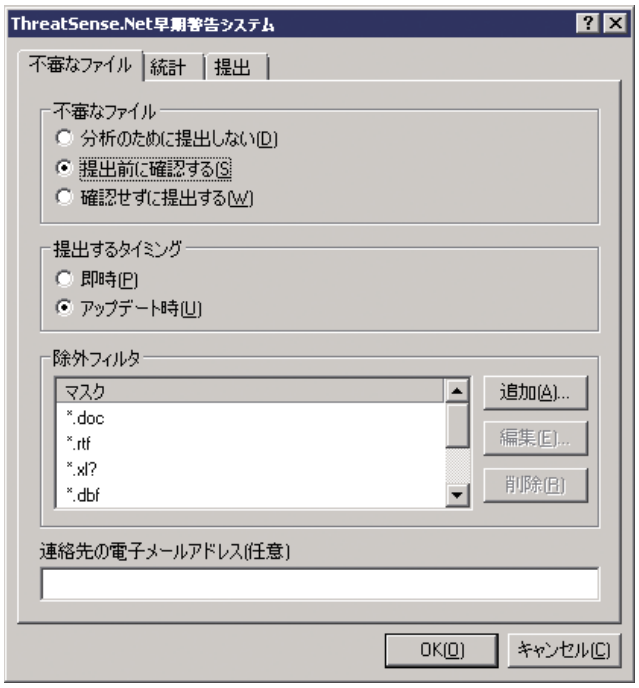


4.12.1 不審なファイル

[不審なファイル] タブでは、ESETのウイルスラボに分析の対象となるファイルや情報の提出方法を設定することができます。

不審なファイルがある場合は、ESETのウイルスラボに提出して分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。

ファイルは、自動的に提出されるように設定できますが、[提出前に確認する] オプションを選択して、解析のために送信されるファイルを判別し、提出を確認することもできます。



ファイルを提出しない場合は、[提出しない] オプションを選択します。この設定自体は統計情報の提出には影響しません。統計情報の提出は独自に設定します（「統計」を参照）。

[提出するタイミング] -既定では、不審なファイルをESETのウイルスラボに送信するために [アップデート時] オプションが選択されています。不審なファイルの提出は、ウイルス定義データベースのアップデート時に行われます。[即時] では、永続的なインターネット接続が利用可能で、不審なファイルをすぐに送信できる場合にお勧めします。

除外フィルタ-除外フィルタを使用すると、特定のファイルやフォルダを提出から除外することができます。たとえば、ドキュメントやスプレッドシートなど、機密情報が含まれている可能性があるファイルを除外することができます。最も一般的なファイルの種類（.docなど）は、既定で除外されます。必要に応じて、除外するファイルの一覧に追加することもできます。

連絡先の電子メールアドレス-不審なファイルと共に [連絡先の電子メールアドレス（任意）] を送信できます。この電子メールアドレスは、分析のために詳しい情報が必要な場合の連絡先として使用されます。詳しい情報が必要でない限り、ESETから連絡することはありません。

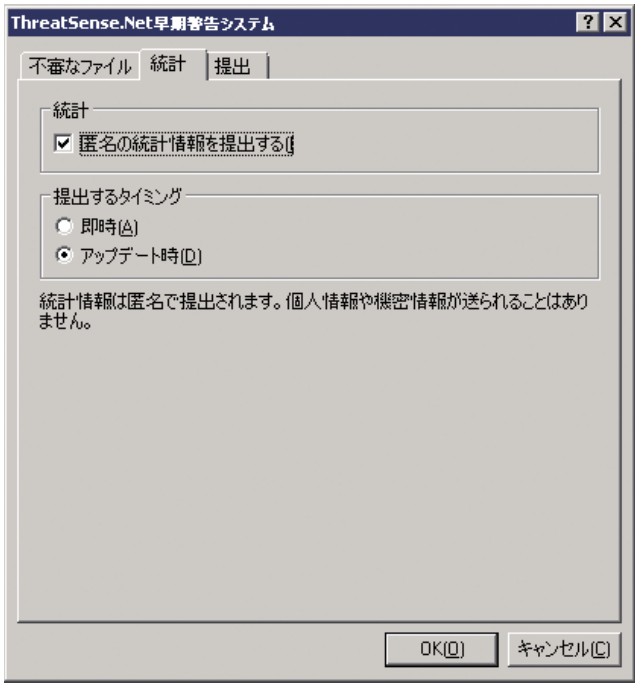
4.12.2 統計

ThreatSense.Net早期警告システムでは、新しく検出されたウイルスに関連するコンピューターについての匿名の情報が収集されます。この情報には、マルウェアの名前、マルウェアが検出された日時、ESETセキュリティ製品のバージョン、オペレーティングシステムのバージョン、およびローカル設定が含まれます。統計は通常、1日1回または2回、ESETのサーバーに配信されます。

提出される統計パッケージの例は次のとおりです。

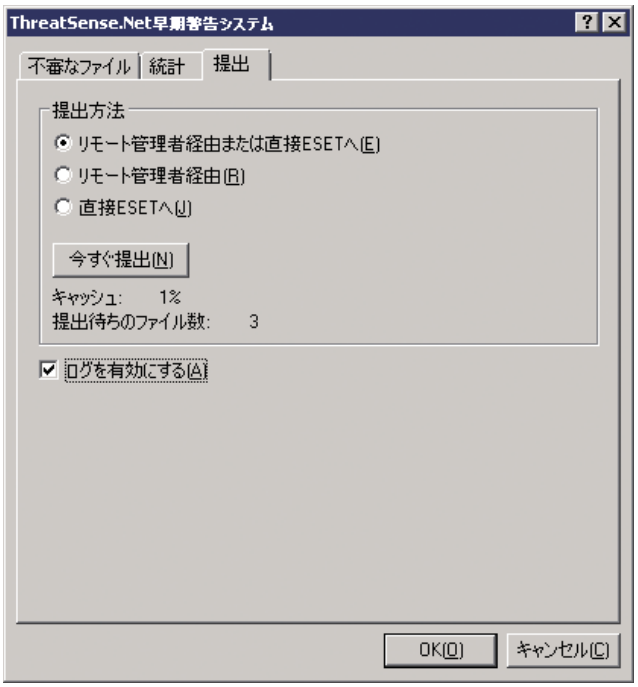
utc_time=2005-04-14 07:21:28
country="Slovakia"
language="ENGLISH"
osver=5.1.2600 NT
engine=5417
components=2.50.2
moduleid=0x4e4f4d41
filesize=28368
filename=C:¥Documents and Settings¥Administrator¥Local Settings¥Temporary Internet Files¥Content.IE5¥C14J8

提出するタイミング-統計情報を提出するタイミングを定義することができます。[可能になり次第] の提出を選択した場合、統計情報が作成されしだい、送信されます。この設定は、永続的なインターネット接続が利用可能な場合に適しています。[アップデート時] を選択した場合、統計情報は次回の更新時にまとめて提出されます。



4.12.3 提出

ファイルと統計情報をESETに提出する方法を選択できます。[リモート管理者経由または直接ESETへ] オプションを選択した場合、使用可能なあらゆる方法によって、ファイルおよび統計情報が提出されます。[リモート管理者経由] オプションを選択した場合、ファイルおよび統計情報がリモート管理サーバに送信された後、ESETのウイルスラボに確実に提出されます。[直接ESETへ] オプションを選択した場合は、全ての疑わしいファイルおよび統計情報がプログラムから直接、ESETのウイルスラボに送信されます。



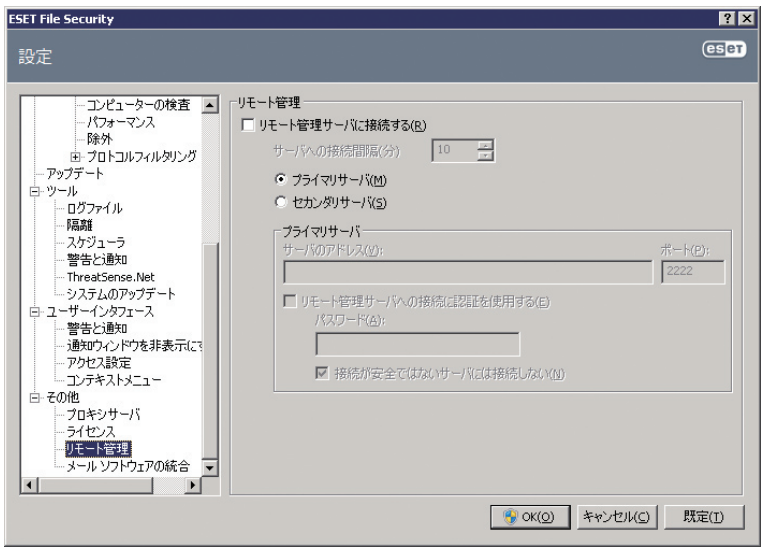
提出待ちのファイルがある場合、この設定ウィンドウの [今すぐ提出] ボタンがアクティブになります。ファイルおよび統計情報を即座に提出するには、このボタンをクリックします。

ファイルおよび統計情報の提出を記録するログを作成するには、[ログを有効にする] オプションを選択します。

4.13 リモート管理

ESET Remote Administrator (ERA) は、セキュリティポリシーの管理や、ネットワーク内の全体的なセキュリティの概要を取得するために使用できる高性能なツールです。特に大規模なネットワークでは効果的を発揮します。ERAによってセキュリティレベルが向上するだけでなく、クライアントワークステーションにおけるESET File Security for Microsoft Windows Serverの管理も容易になります。

リモート管理の設定オプションには、ESET File Security for Microsoft Windows Serverのメインウィンドウからアクセスすることができます。[設定] > [環境設定で詳細な設定をする...] > [その他] > [リモート管理] をクリックします。



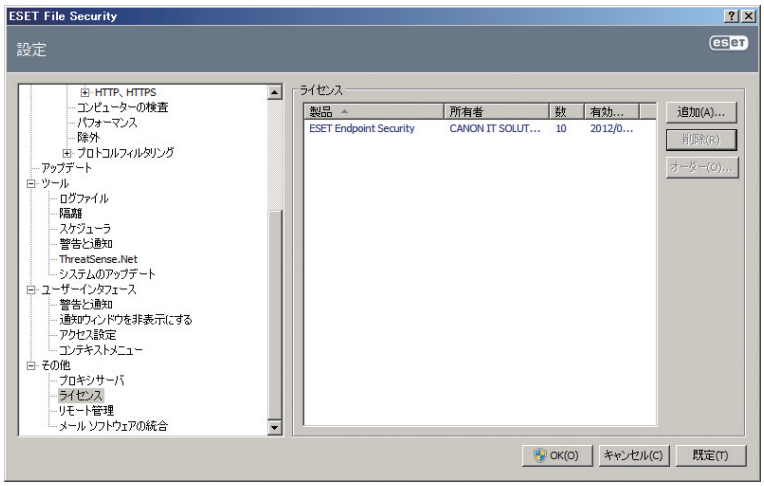
リモート管理を有効にするには、[リモート管理サーバーに接続する] オプションを有効にします。設定を有効にすることで下記のその他のオプションへのアクセスが可能になります。

サーバへの接続間隔(分)	ESET File Security for Microsoft Windows ServerがERAサーバに接続する頻度を指定します。0に設定されている場合、5秒ごとに情報が送信されます。
サーバアドレス	ERAサーバがインストールされているサーバのネットワークアドレスです。
ポート	このフィールドには、接続に使用されるサーバポートが表示されます。既定のポート設定"2222"をそのまま使用することをお勧めします。
リモート管理サーバで認証を要求する	必要に応じて、ERAサーバに接続するためのパスワードを入力できます。

[OK] をクリックして変更内容を確認し、設定を適用します。ESET File Security for Microsoft Windows Serverは、この設定を使用してERAサーバに接続します。

4.14 ライセンス

[ライセンス] では、ESET File Security for Microsoft Windows Serverやライセンスキーを管理できます。ライセンスキーは、購入後に、ユーザー名およびパスワードと一緒に配布されます。ライセンスキーを追加/削除するには、ライセンスマネージャウィンドウの該当するボタンをクリックします。ライセンスマネージャには、詳細設定ツリーの [その他] > [ライセンス] からアクセスすることができます。



ライセンスキーは、購入した製品に関する情報 (所有者、ライセンス数、および有効期限) が記載されたテキストファイルです。

ライセンスマネージャウィンドウでは、[追加...] ボタンを使用して、ライセンスキーの内容をアップロードし、表示することができます。リストからライセンスファイルを削除するには、[削除] ボタンをクリックします。

[Chapter 5]
用語集

5.1 マルウェアの種類

マルウェアとは、ユーザーのコンピューターに入り込み、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。

5.1.1 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を破損させるマルウェアの一種です。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。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。

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。自己を複製するため、ウイルスは"本体"を標的ファイルの末尾に付着させます。コンピューターウイルスの動作を簡単に説明します。感染したファイルの実行後、ウイルスは（元のアプリケーションよりも前に）自身をアクティブにし、事前定義タスクを実行します。元のアプリケーションが実行できるようになるのは、その後です。ウイルスはユーザーが悪意のあるプログラムを自分で偶然または故意に実行したり開いたりしない限り、コンピューターに感染することはできません。

コンピューターウイルスの目的と重大度は、さまざまです。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、自分の技術上の技量を誇示するに過ぎないものもあります。

（トロイの木馬やスパイウェアと比較すると）ウイルスは少なくなっています。悪意のあるソフトウェア開発者にとって金銭的に魅力的ではないためです。また、"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用語として誤用されることがよくあります。この用法は、新しくより正確な用語"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ています。

お使いのコンピューターがウイルスに感染した場合は、感染したファイルを元の状態に復元する、つまりウイルス対策プログラムでファイルからウイルスを駆除する必要があります。

ウイルスの例::OneHalf? Tenga? Yankee Doodle

5.1.2 ワーム

コンピューターワームとは、感染先のコンピューターを攻撃しネットワークを介して蔓延する、悪意のあるコードを含む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、ワームは自己を複製し、自ら移動できることです。ワームは宿主ファイル（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、ネットワークアプリケーションのセキュリティ上の脆弱性を悪用します。

したがって、ワームはコンピューターウイルスよりはるかに実行可能性が高いです。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。自己を単独で急速に複製できる能力があるので、他の種類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されると、迷惑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、他の種類のマルウェアの"輸送手段"となります。

コンピューターがワームに感染した場合は、感染ファイルを削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

よく知られているワームの例:Lovsan/Blaster? Stration/Warezov? Bagle? Netsky

5.1.3 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、こうしてユーザーを騙して実行させようとするマルウェアの1つのクラスとして定義されてきました。しかし、この定義は今日のトロイの木馬には当てはまらないことに注意する必要があります。今日では、偽装する必要はもはやありません。トロイの木馬の唯一の目的は、できるだけ簡単に侵入し、悪意のある目標を達成することです。"トロイの木馬"は、極めて一般的な用語になりました。今日ではマルウェアのどの特定のクラスにも分類されないマルウェアなら、全て該当します。

このカテゴリの範囲は非常に広いので、多くのサブカテゴリに分類されることもよくあります。

ダウンローダ	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	他の種類のマルウェアを弱体化されたコンピューターに落とす(ドロップする)トロイの木馬の一種。
バックドア	リモートの攻撃者と通信して、システムにアクセスし制御できるようにするアプリケーション。
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、リモートの攻撃者にその情報を送信するプログラム。
ダイアラ	情報料代理徴収番号に接続するよう設計されたプログラム。新しい接続が作成されたことにユーザーが気づくのは、ほとんど不可能です。ダイアラで被害を被るのは、ダイヤルアップモデムを使用するユーザーのみです。このモデムは現在ではあまり使用されていません。

トロイの木馬は通常、拡張子が.exeの実行可能ファイルの形式を取ります。トロイの木馬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、削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

よく知られているトロイの木馬の例:NetBus? Trojandownloader.Small.ZL? Slapper

5.1.4 ルートキット

ルートキットとは、自己の存在を隠しながら、インターネットからの攻撃者が、システムに無制限にアクセスできるようにする悪意のあるプログラムです。ルートキットは、システムにアクセス(通常はシステムの脆弱性を悪用します)した後、オペレーティングシステムのさまざまな機能を使用して、ウイルス対策ソフトウェアによる検出を免れます。具体的には、プロセス、ファイル、およびWindowsレジストリデータを隠します。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不可能です。

ルートキットから保護するための検出処理には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、大半のウイルス対策システムがルートキットを排除できます(ウイルス対策システムが、ルートキットに感染しているファイルを検出する、と仮定します)。

2) 通常のテストで検出されない場合、ESET File Security for Microsoft Windows Serverのユーザーは、アンチステルス技術を活用できます。これで、活動しているルートキットの検出と排除が可能です。

5.1.5 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ウィンドウをインターネットブラウザ内に自動的に開いたり、ブラウザ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に同梱されていることが多く、フリーウェアプログラム（通常は便利なアプリケーション）の開発者が、その開発費を賄うことができます。

アドウェア自体は、危険ではありません。ユーザーは広告に悩まされるだけです。危険は、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もある、という事実にあります。

フリーウェア製品を使用することにした場合には、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）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。この場合、残念がるより安心を選ぶ方が賢明です。アドウェアとして検出されるファイルがコンピューターにある場合は、削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

5.1.6 スパイウェア

このカテゴリは、個人情報を当人の同意を得ず、当人が知らないうちに送信する全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メールアドレスや、記録されたキーストロークなどのさまざまな統計データを送信します。

スパイウェアの作成者は、こうした手法はユーザーのニーズと関心に関するデータをさらに見つけ、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のプログラムの作成者が、プログラムに同梱していることがよくあります。これは、収益を上げたり、そのプログラムを購入するよう動機を与えるためです。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もよくあります。これは、スパイウェアが含まれない有料バージョンにアップグレードするよう促すためです。

スパイウェアが組み入れられている、よく知られているフリーウェア製品の例としては、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、削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

5.1.7 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機能を持つ適正なプログラムは、少なくありません。ただし、悪意のあるユーザーの手に渡ると、不正な目的で誤用される可能性があります。ESETFile Security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」は、市販の適正なソフトウェアに使用される分類です。これには、リモートアクセスツール、パスワード解析アプリケーション、キーロガー（ユーザーが入力した各キーストロークを記録するプログラム）などのプログラムが含まれます。

コンピューターに潜在的に危険性のあるアプリケーションが存在して実行されている（しかも、自分ではインストールしていない）ことに気づいた場合には、ネットワーク管理者まで連絡するか、そのアプリケーションを削除してください。

5.1.8 潜在的に不要なアプリケーション

潜在的に不要なアプリケーションは、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ウィンドウが開く。
●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と通信する。