ESET File Security
for Microsoft Windows Server
設定ガイド

このたびは、弊社製品をお買い上げいただき、誠にありがとうございます。
この設定ガイドでは、本プログラムの詳細な設定方法を説明しています。
ご使用の前にぜひご一読いただくことをお奨めします。

■本書の表記について

- 本プログラムをインストール後、設定の変更を全く加えていない状態を「既定値」と表記しています。
- アイコンやボタンなどにマウスポインタ（↖）を合わせ、マウスの左ボタンを 1 回押すことを「クリック」、素早く 2 回押すことを「ダブルクリック」、マウスの右ボタンを 1 回押すことを「右クリック」と表記しています。
- ダイアログなどのチェックボックス、およびラジオボタンをクリックし、☑ ◉ の状態にすることを「チェックを入れる」「チェックをオンにする」と表記しています。

■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、改定などにより予告なく変更することがあります。
- 本製品の一部またはすべてを無断で複写、複製、改変することはその形態を問わず、禁じます。
- 本書の著作権は、キヤノン ITソリューションズ株式会社に帰属します。本プログラムの著作権は、ESET, spol, s.r.o.に帰属します。
- ESET、NOD32、ESET File Security、ThreatSenseは、ESET, spol. s.r.o.の商標です。
- Microsoft、Windows、Windows Vista、Windows Server、SQL Server、Excel、Internet Explorerは、米国 Microsoft Corporationの米国、日本およびその他の国における登録商標または商標です。

ESET File Security

設定ガイド●目次●

Part.5 「設定」画面での操作

Part.6 「ツール」画面での操作

Part.7 「ヘルプとサポート」画面での操作

Part.8 サーバ保護機能

Part.9 コマンドラインインターフェースで操作するには～ eShell の使用方法

Part.1
本プログラムの画面構成と画面操作

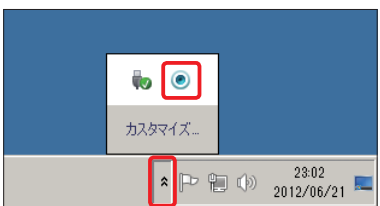
ここでは、本プログラムの画面構成とその基本的な操作方法についてご紹介しています。

基本画面 ▸▸ 通知領域

1-1 通知領域のアイコンから表示設定を切り替えるには

本プログラム起動時には、通知領域にアイコンが表示され、ダブルクリックすることで基本画面が起動し、クリックするとメニューから各種操作を行えます。最初にこの通知領域アイコンの操作をご紹介します。

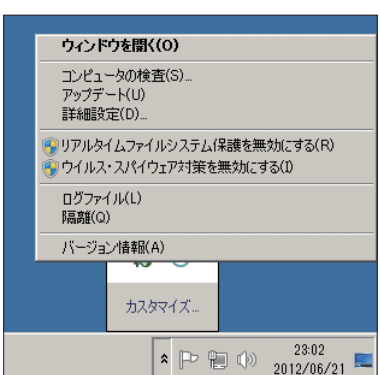
通知領域アイコンと基本画面



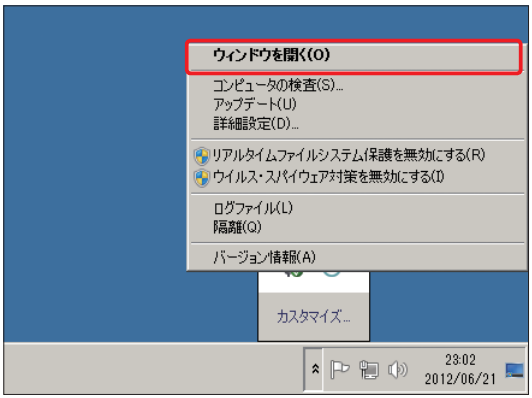
① 本プログラムのアイコンは、Windowsへのログオン後に、通知領域に表示されます。本プログラムの動作を変更するには、同アイコンをクリックします。

POINT

通知領域にアイコンが表示されていない場合は、「隠れているインジケーターを表示します」ボタンをクリックします。



② メニューが表示されました。ここから各表示設定の切り替えや、本プログラムの基本画面を呼び出すことができます。



3

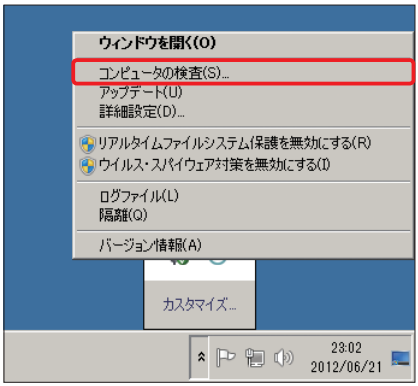
表示されるメニューの［ウィンドウを開く］をクリックします。

基本画面

4

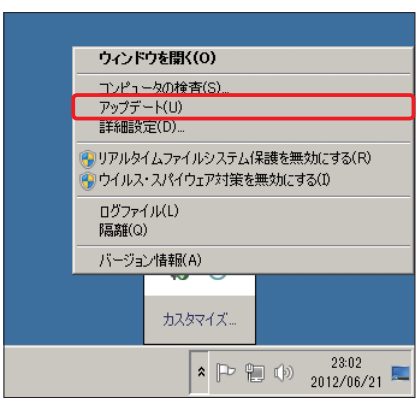
基本画面が表示されます。基本画面には、❶各機能を呼び出すためのボタンが並ぶ「メインメニュー」と、❷メインメニューで選択された機能の状態などを表示する「プライマリウィンドウ」があります。

それぞれの表示メニューについて



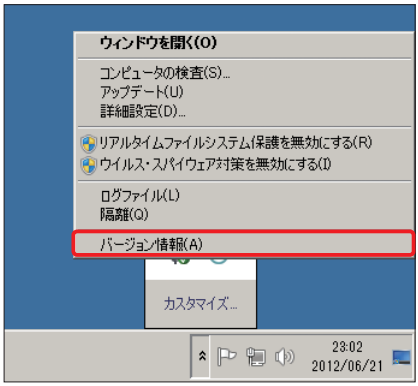
1

通知領域のアイコンをクリックし、メニューから［コンピュータの検査］をクリックすると、コンピューターの検査画面が表示されます。



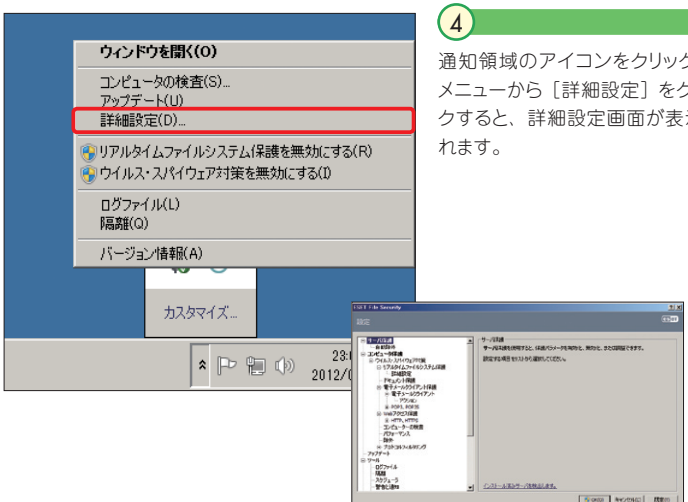
2

通知領域のアイコンをクリックし、メニューから［アップデート］をクリックすると、ウイルス定義データベースのアップデートが始まります。



3

通知領域のアイコンをクリックし、メニューから［バージョン情報］をクリックすると、本プログラムのバージョン情報が表示されます。



4

通知領域のアイコンをクリックし、メニューから［詳細設定］をクリックすると、詳細設定画面が表示されます。

POINT

［ログファイル］［隔離］をクリックすると、対応した画面が表示されます。なお、［リアルタイムファイルシステム保護を無効にする］［ウイルス・スパイウェア対策を無効にする］をクリックすると、それぞれの機能が停止されるため、特に理由のない場合は選択しないでください。

詳細モード ▸▸ 各機能

1-2 各機能を確認するには

本プログラムでは各機能がすぐに利用できるように、「保護の状態」「コンピュータの検査」といった項目を用意しています。ここでは各機能を説明します。

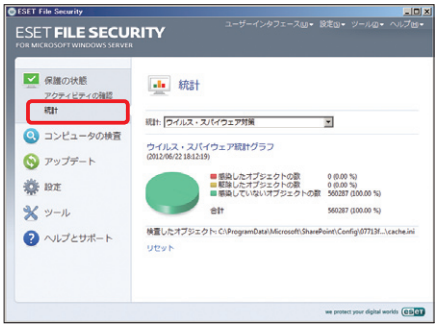
保護の状態

1

「保護の状態」では、本プログラムの現在の状態をプライマリウィンドウに表示します。また、メインメニューには、[アクティビティの確認] と [統計] の 2つの項目が準備されています。

2

[アクティビティの確認] をクリックすると、ファイルシステムの活動状況を確認できます。



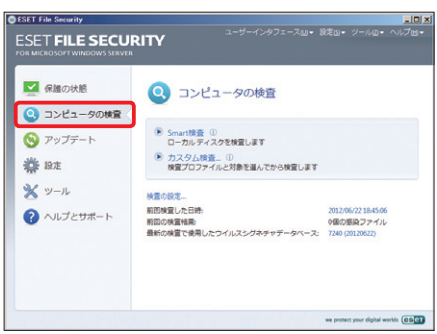
3

［統計］をクリックすると、ウイルス・スパイウェア対策の統計情報を確認できます。

POINT

［統計］のドロップダウンボタンをクリックし、表示されるメニューから各統計を選択することで、必要とする情報を表示させることができます。

コンピュータの検査



1

［コンピュータの検査］はウイルス検査時に使用します。ローカルディスクを検査する［Smart検査］、任意のドライブやフォルダーなどを検査する［カスタム検査］を呼び出せます。

アップデート

1

❶［アップデート］をクリックし、❷［ウイルス定義データベースをアップデートする］をクリックすると、ウイルス定義データベースをアップデートできます。なお、アップデートがうまく行われない場合は❸［ユーザー名とパスワードを入力］をクリックして、設定をご確認ください。

設定

1

「設定」では、本プログラムに搭載されているウイルス・スパイウェア対策保護の状態を確認できます。また、ここから本プログラムの各種設定を行うこともできます。

2

［設定］にある［ウイルス・スパイウェア対策の保護］をクリックすると、ウイルスの侵入を監視する「リアルタイムファイルシステム保護」、送受信メールの検査を行う「電子メールクライアント保護」といった各保護機能の状態を確認・変更できます。

POINT

本プログラムには、Word や Excel に埋め込まれたウイルスを検出する「ドキュメント保護」や Web 閲覧時にマルウェアなどの侵入を防ぐ「Web アクセス保護」などの機能も搭載していますが、これらの保護機能の既定値は、無効に設定されています。これらの保護機能が有効になっていると、その状態も［設定］のプライマリウィンドウに表示されます。

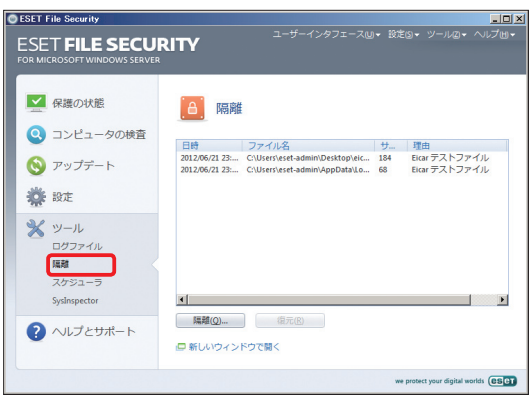
ツール

1

「ツール」には、各種ログ情報の確認やシステム情報を確認する「SysInspector」、ウイルスの隔離情報、決められた作業をスケジュール実行する「スケジューラ」などの各種ツール類が配置されています。

2

［ログファイル］をクリックすると、「検出された脅威」「イベント」「コンピュータの検査」のログを確認できます。



3

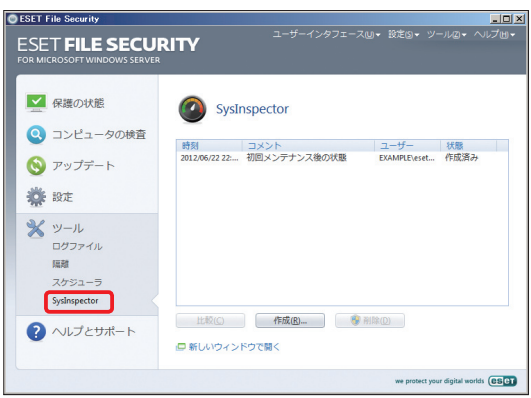
［隔離］をクリックすると、ウイルスとして隔離されたファイルを確認できます。ファイルが誤って隔離された場合は、ここから復元操作を行うことができます。

4

［スケジューラ］をクリックすると、ウイルス定義データベースの自動アップデートや自動スタートアップファイルの検査といったスケジュールを設定できます。

POINT

新しいスケジュールを追加するには、画面下にある［追加］ボタンをクリックして、必要な操作をウィザード形式で行います。



5

［SysInspector］をクリックすると、インストールされているソフトウェアや重要なレジストリなどの情報を保存できます。アプリケーションの追加、削除を行った場合に変更されたファイルなどの情報を確認することもできます。

ヘルプとサポート

1

［ヘルプとサポート］ボタンでは、トラブル発生時に役立つヘルプや Web ページへのリンク、テクニカルサポートへの連絡方法などが用意されています。お困りの際に参照してください。

Part.2
「保護の状態」画面での操作

ここでは、本プログラムの「保護の状態」画面でのさまざまな確認方法についてご紹介しています。

保護の状態 ▶ 警告画面への対処

2-1 コンピューターの保護の状態を確認するには

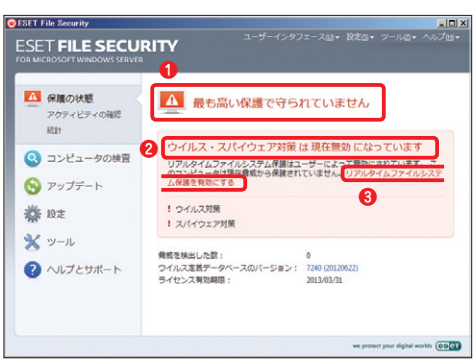
既定値の設定では、「最も高い保護」となります。現在の保護の状態を確認し、保護機能の有効 / 無効を切り替える方法を紹介します。

「最も高い保護（既定値）」で守られている場合

1

本プログラムの基本画面を開き、❶［保護の状態］ボタンをクリックします。❷「最も高い保護」というメッセージが表示されていれば、既定値の設定がすべて有効になった通常状態です。

「最も高い保護」で守られていない場合



1

リアルタイムファイルシステム保護が無効に設定されている場合、❶❷の画面のような警告が表示されます。保護機能を有効にする場合は、❸［リアルタイムファイルシステム保護を有効にする］をクリックします。

2

リアルタイムファイルシステム保護が有効になり「最も高い保護」に戻ります。

3

電子メール保護が無効に設定されている場合、❶❷の画面のような警告が表示されます。保護機能を有効にする場合は、❸［電子メール保護を有効にする］をクリックします。

4

電子メール保護が有効になり「最も高い保護」に戻ります。

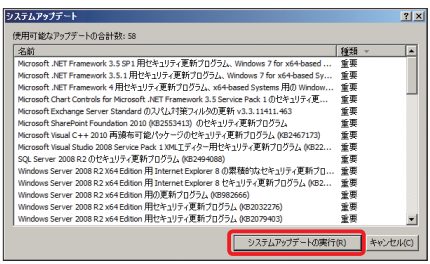
コラム

OS が最新でない場合

OS のアップデートは、OS のバグ修正だけでなく、セキュリティホールの修正なども行われています。本プログラムには、OS の重要なアップデートが適用されているかを自動検出する機能が搭載されています。

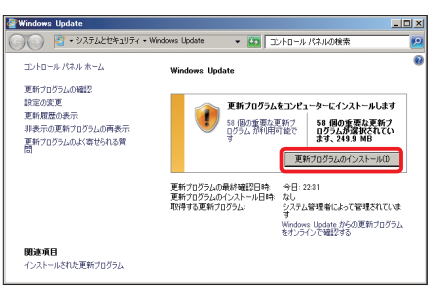
1

OS の重要なアップデートを行っていないと、❶のような警告画面が表示されます。❷［ここ］をクリックします。



2

使用可能なアップデートのリストが表示されます。［システムアップデートの実行］をクリックします。



3

Windows Updateが表示されますので、［更新プログラムのインストール］ボタンをクリックして、アップデートを行ってください。

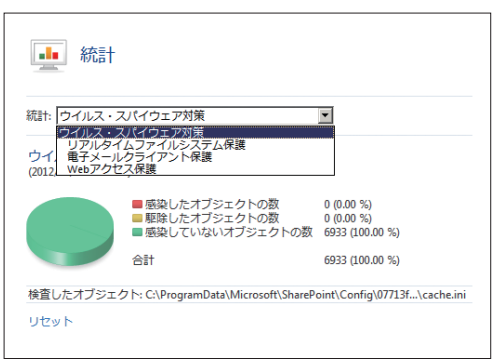
保護の状態 ▸▸ 感染ファイル

2-2 検出したウイルスの数や状況を確認するには

検出したウイルスの数や状況を確認するには、「保護の状態」を開き、「統計」をクリックします。

1

本プログラムの基本画面を開き、❶［保護の状態］ボタンをクリックし、❷［統計］をクリックします。



2

［統計］のドロップダウンボタンをクリックすると、表示されるメニューから「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」「電子メールクライアント保護」「Webアクセス保護」を選択することができます。それぞれの統計が表示されます。

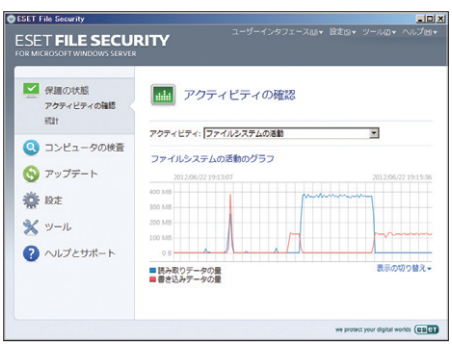
コラム

アクティビティの確認について

悪意のあるソフトウェアが侵入すると、ハードディスクへのアクセスが急増することがあります。［保護の状態］には、ハードディスクへのアクセス統計を確認できる［アクティビティの確認］も準備されており、これで、ハードディスクの利用状況を確認できます。［アクティビティの確認］は、以下の手順で表示できます。

1

本プログラムの基本画面を開き、❶［保護の状態］ボタンをクリックし、❷［アクティビティの確認］をクリックします。



2

ファイルシステムの活動状況が表示されます。

Part.3
「コンピュータの検査」画面での操作

ここでは、本プログラムの「コンピュータの検査」画面でのさまざまな操作方法についてご紹介しています。

コンピューターの検査 ▸▸ ハードディスク検査

3-1 ハードディスクのウイルス検査（Smart 検査）を実行するには

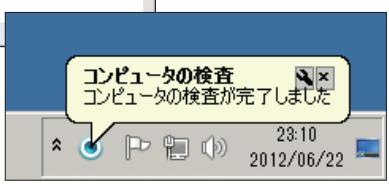
ここではコンピューターに接続されたハードディスクなどを対象にする「Smart 検査」を行う手順を説明します。

1 本プログラムの基本画面を開き、［コンピュータの検査］ボタンをクリックします。

2 ［Smart検査］をクリックします。

3

コンピュータの検査が始まります。進行状況を示すバーとパーセンテージが表示されます。検査が終了するまでお待ちください。一時的に中断したいときは［中断］ボタン、終了したい時は［中止］ボタンをクリックします。



4

検査が完了すると画面のように終了を示すメッセージとバルーンが表示されます。［OK］ボタンをクリックして検査を終了します。

POINT

［検査ログを表示する］をクリックすると、検査内容の詳細情報を確認できます。デスクトップなどにある単独のファイルやフォルダーを検査する場合は、ファイルなどを右クリックし、メニューから[ESET File Securityで検査]をクリックします。ウイルスが発見された場合に自動的に駆除・削除を行うには、ファイルなどを右クリックし、メニューから［詳細設定オプション］→［ファイルに対して駆除を実行］をクリックします。

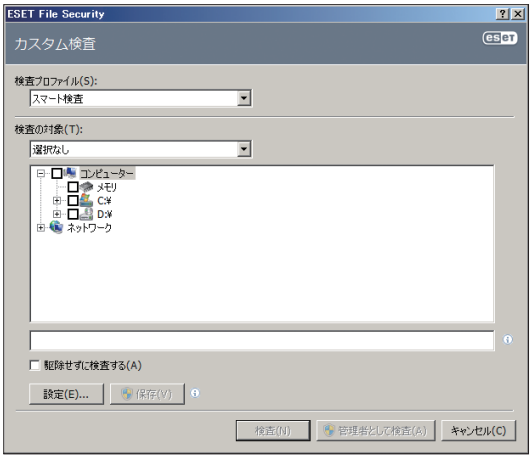
コンピューターの検査 ▸▸ カスタム検査

3-2 さまざまな設定でウイルス検査（カスタム検査）を行うには

特定のフォルダーやネットワーク上の共有フォルダーを対象にウイルス検査を行うには「カスタム検査」を実行します。

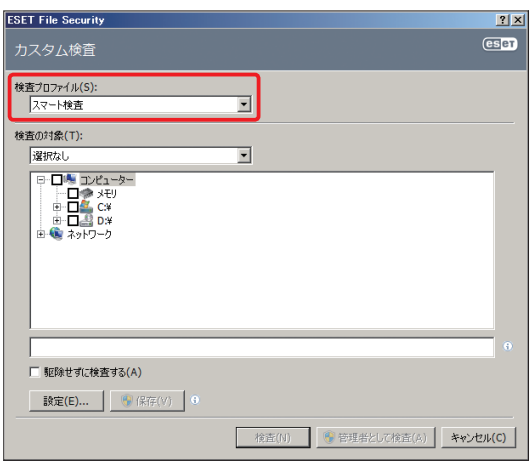
1 本プログラムの基本画面を開き、［コンピュータの検査］ボタンをクリックします。

2 ［カスタム検査］をクリックします。



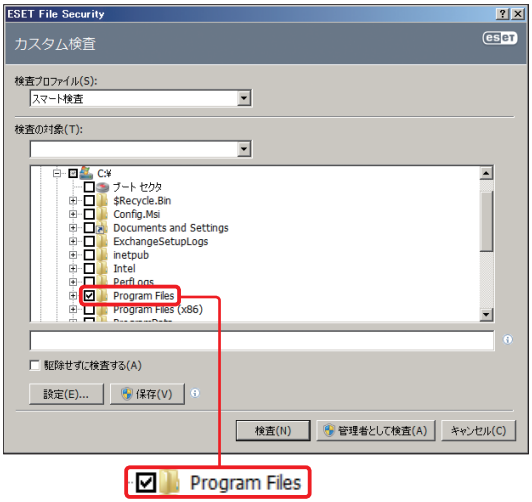
3

検査対象やプロファイルを選ぶためのダイアログが表示されます。



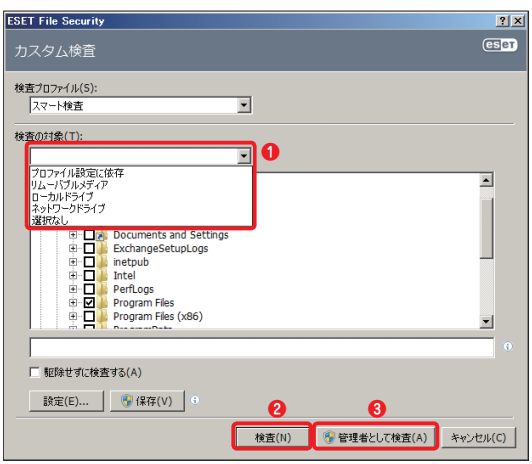
4

プロファイルの選択を行います。既定値では「スマート検査」が設定されています。そのほか、「詳細検査」「コンテキストメニュー検査」の項目が用意されています。使用するプロファイルをドロップダウンリストから選んでください。



5

今回は一例としてProgram Filesフォルダーを検査対象にします。まずは、Cドライブの［+］ボタンをクリックします。フォルダー（ディレクトリ）が表示されたら、Program Filesのボックスにチェックを入れます。これで検査対象の設定は完了しました。



6

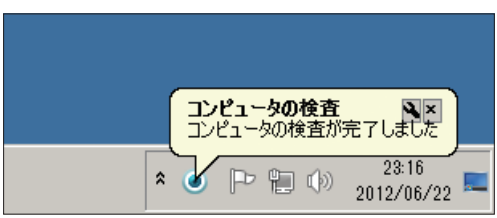
手順⑤の操作に代わって、カテゴリによって検査対象を選択することも可能です。❶「検査の対象」のドロップダウンリストからは「プロファイル設定に依存」「リムーバブルメディア」「ローカルドライブ」「ネットワークドライブ」の4種類が選択可能です。最後に❷［検査］ボタンまたは❸［管理者として検査］ボタンをクリックします。

7

コンピュータの検査が始まります。進行状況を示すバーとパーセンテージを参考に、終了までお待ちください。一時的に中断したいときは［中断］ボタン、終了したい時は［中止］ボタンをクリックします。

8

検査が完了すると画面のように終了を示すメッセージとバルーンが表示されます。［OK］ボタンをクリックして検査を終了します。



コンピューターの検査 ▸▸ 検査対象の設定

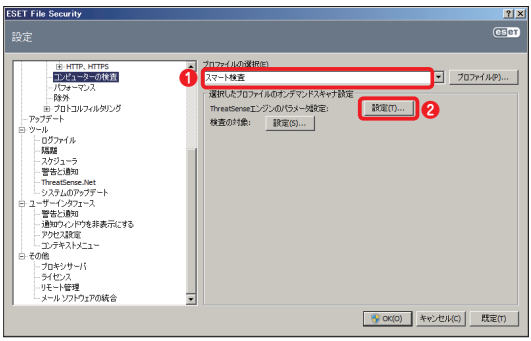
3-3 検査対象にするファイルの条件を設定するには

本プログラムは、「コンピュータの検査」実施時の検査対象ファイルに関する条件を設定できます。この機能を利用すると、指定条件のファイルを検査対象から除外でき、コンピューターの検査にかかる時間を短縮できます。

特定の拡張子のファイルを検査対象から除外する

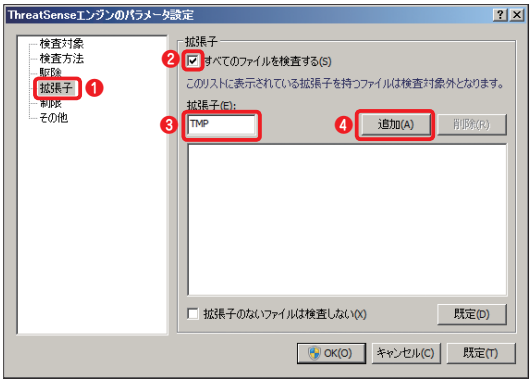
1

本プログラムの基本画面を開き、❶［コンピュータの検査］ボタンをクリックし、❷［検査の設定］をクリックします。



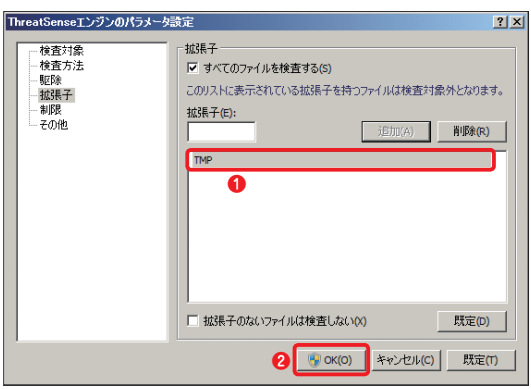
2

❶設定を行うプロファイルをドロップダウンリストから選択し、❷［ThreatSense検査エンジンのパラメータ設定］の［設定］ボタンをクリックします。



3

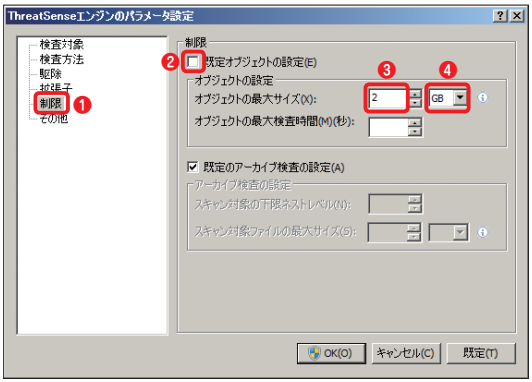
［ThreatSense エンジンのパラメータ設定］ダイアログが開きます。❶［拡張子］をクリックし、❷［すべてのファイルを検査する］にチェックを入れます。❸除外する拡張子（ここでは、「TMP」）を入力し、❹［追加］ボタンをクリックします。



4

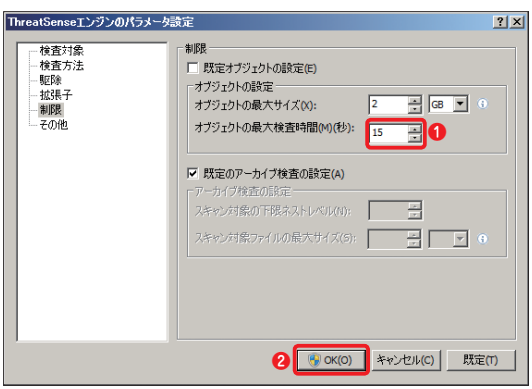
❶除外する拡張子がリストに登録されます。❷［OK］ボタンをクリックします。

ファイルのサイズと最大検査時間を設定する



1

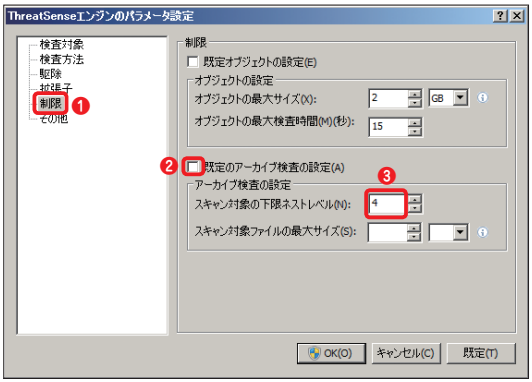
32ページの手順を参考に、［Threat-Senseエンジンのパラメータ設定］ダイアログを開きます。❶［制限］をクリックし、❷［既定オブジェクトの設定］のチェックを外します。❸オブジェクト（ファイル）の最大サイズを入力し、❹サイズの「単位」を設定します。



2

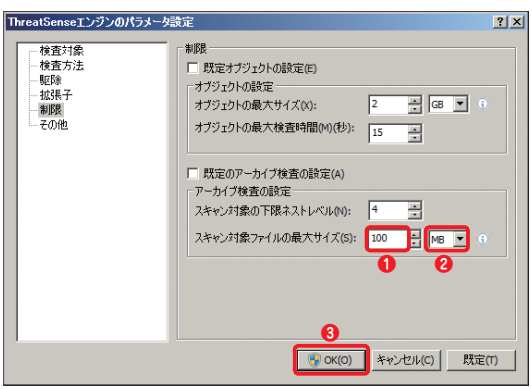
❶オブジェクト（ファイル）の最大検査時間を入力し、❷［OK］ボタンをクリックします。

検査対象とする圧縮ファイルの階層とサイズを制限する



1

32ページの手順を参考に、［ThreatSenseエンジンのパラメータ設定］ダイアログを開きます。❶［制限］をクリックし、❷［既定のアーカイブ検査の設定］のチェックを外します。❸スキャン対象の下限ネストレベル（階層数）を入力します。



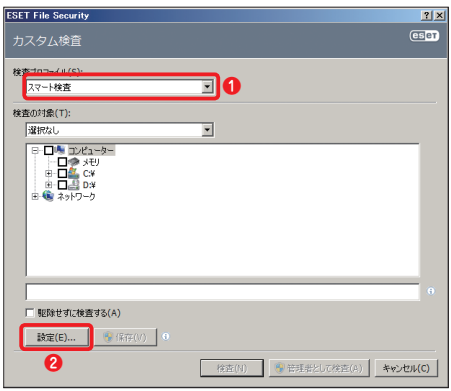
2

❶スキャン対象ファイルの最大サイズを入力し、❷サイズの「単位」を設定します。❸［OK］ボタンをクリックします。

コラム

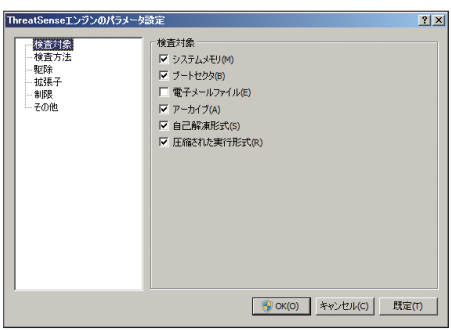
カスタム検査の詳細設定について

「コンピュータの検査」実施時の検査対象ファイルに関する条件は、［カスタム検査］ダイアログからも設定できます。［カスタム検査］ダイアログから設定を行うときは、以下の手順で行います。



1

28ページの手順を参考に［カスタム検査］ダイアログを表示します。設定を変更するプロファイルを❶ドロップダウンリストから選び、❷［設定］ボタンをクリックします。



2

「ThreatSenseエンジンのパラメータ設定」画面が表示され、カスタム検査に関する詳細設定を行えます。

Part.4
「アップデート」画面での操作

ここでは、本プログラムの「アップデート」画面でのさまざまな操作方法についてご紹介しています。

アップデート ▸▸ 手動アップデート

4-1 ウイルス定義データベースのアップデートを手動で行うには

本プログラムのウイルス定義データベースは、既定値では自動的にアップデートされますが、ファイルの検査を行う前に最新の定義データベースにアップデートしたい方は、手動でアップデートを行うこともできます。

1

本プログラムの基本画面を開き、❶［アップデート］ボタンをクリックします。❷［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。

2

アップデートが完了すると、「ウイルス定義データベースのアップデートが成功しました」と表示されますので、［OK］ボタンをクリックしてください。

CAUTION

アップデートが正常に行われないときは、アップデートサーバーが一時停止しているか、アップデートサーバーへの接続設定が間違っている可能性があります。後者の場合は、スタートアップガイドの 14 ページをご参照ください。

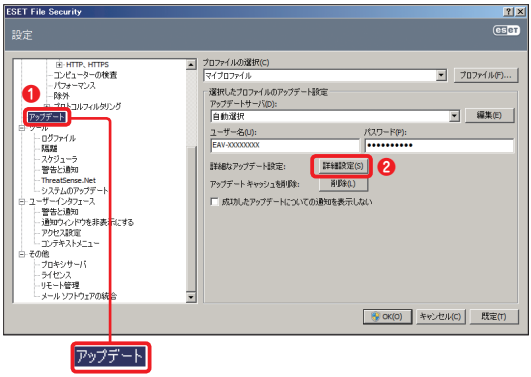
アップデート ▸▸ アップデート自動実行

4-2 プログラムコンポーネントのアップデートを行うには

本プログラムでは、ウイルス定義データベースのアップデートの他に、プログラムコンポーネントがアップデートされる場合があります。プログラムコンポーネントのアップデートを自動で行う設定を紹介します。

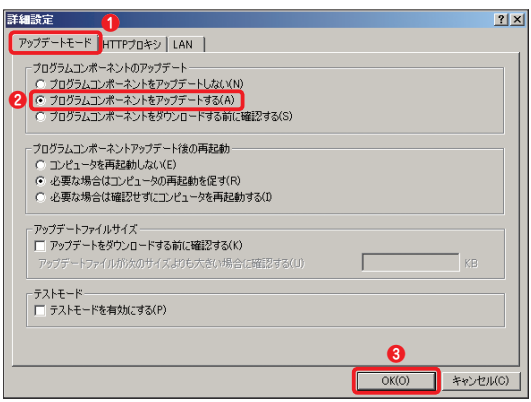
1 ［設定］ボタンをクリックします。

2 ［詳細設定のツリー全体を表示する］をクリックします。



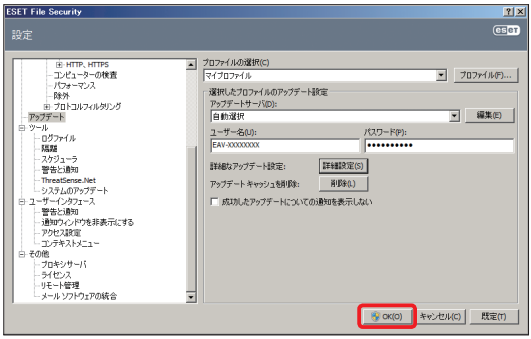
3

❶［アップデート］をクリックし、❷［詳細設定］ボタンをクリックします。



4

❶［アップデートモード］タブをクリックし、❷［プログラムコンポーネントをアップデートする］にチェックを入れ、❸［OK］ボタンをクリックします。



5

設定を有効にするため［OK］ボタンをクリックしてください。これでプログラムコンポーネントのアップデートが自動で行われます。

CAUTION

プログラムコンポーネントがアップデートされた場合、コンピューターを再起動する必要がありますのでご注意ください。コンピューターを再起動させたくない場合は、［プログラムコンポーネントをアップデートする］をチェックしないでください。

CAUTION

プログラムコンポーネントの自動アップデートは、次ページで説明しているスケジュールタスクの設定に自動アップデートの設定が登録されていることが前提となります。既定値では、この設定が有効に設定されており、このセクションの設定を行うことで、ウイルス定義データベースの自動アップデートだけでなく、プログラムコンポーネントも自動アップデートできます。

アップデート ▸▸ 自動アップデートの確認

4-3 自動アップデートの設定を確認するには

本プログラムではあらかじめ自動アップデートの設定がスケジュールタスクとして登録されています。ここでは、その内容を確認する手順を紹介します。

1

本プログラムの基本画面を開き、❶［ツール］ボタンをクリックし、❷［スケジューラ］をクリックします。

2

❶［定期的に自動アップデート］をダブルクリックすると、❷スケジュール内容を示すダイアログが表示されます。

Part.5
「設定」画面での操作

ここでは、本プログラムの「設定」画面における「ウイルス・スパイウェア対策」に関するさまざまな操作方法についてご紹介しています。

設定 ▸▸ 一時無効化

5-1 保護機能を一時的に無効にするには

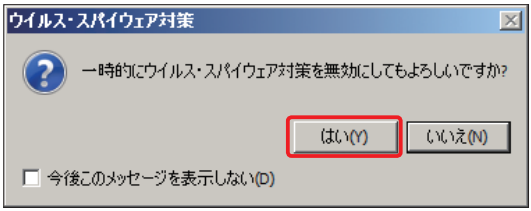
本プログラムが原因で問題が発生している可能性がある場合は、各機能を一時的に無効にしてみましょう。

1

本プログラムの基本画面を開き、❶［設定］ボタンをクリックし、❷［ウイルス・スパイウェア対策保護］または、❸［ウイルス・スパイウェア対策の設定］をクリックします。

2

［一時的にウイルス・スパイウェア対策を無効にする］をクリックします。



3

ダイアログが表示されます。［はい］ボタンをクリックします。

4

ウイルス・スパイウェア対策保護を無効にすると、各項目が無効になります。

5

❶［保護の状態］ボタンをクリックし、❷警告が表示されていることを確認します。

設定 ▸▸ 除外ファイル

5-2 ウイルス検査をしないファイルやフォルダーを設定するには

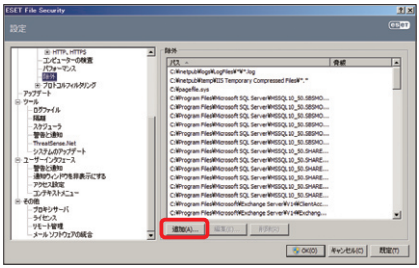
本プログラムでは、特定のフォルダーやファイルを検査から除外できます。ここでは、検査から除外したいフォルダーやファイルの登録方法を説明します。

1

本プログラムの基本画面を開き、❶［設定］ボタンをクリックして、❷［ウイルス・スパイウェア対策保護］または❸［ウイルス・スパイウェア対策の設定］をクリックします。

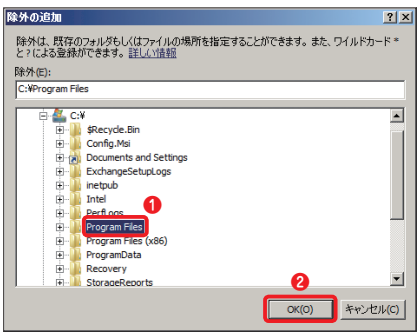
2

［除外の編集］をクリックします。



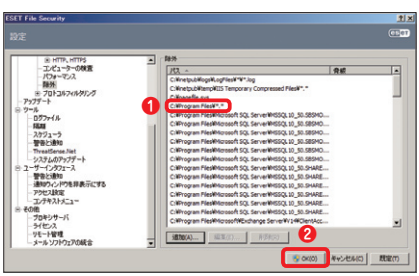
3

［追加］ボタンをクリックします。



4

今回は一例として、Program Filesフォルダーを検査から除外します。Cドライブの［+］ボタンをクリックします。フォルダーが表示されたら、❶［Program Flies］をクリックして、❷［OK］ボタンをクリックします。



5

❶選択したフォルダーが除外フォルダーとして登録されます。❷［OK］ボタンをクリックします。

POINT

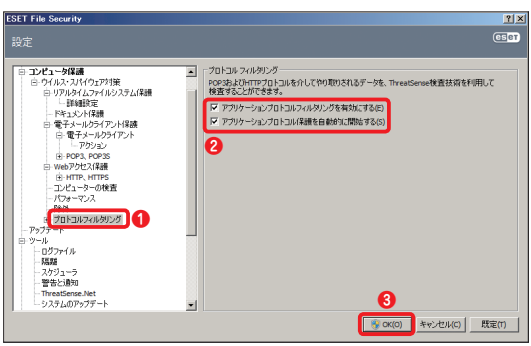
手順④でファイルを選択すると、そのファイルを除外ファイルとして登録できます。また、本プログラムには、重要なサーバーアプリケーションとOS のシステムファイルを識別して、除外リストに自動的に登録する「自動除外」機能も搭載しています。自動除外機能の詳細については、94 ページをご参照ください。

設定 ▸▸ Web アクセス保護

5-3 Web アクセス保護を設定するには

本プログラムには、Web 閲覧時にマルウェアの侵入などを防ぐ「Web アクセス保護」を搭載していますが、この機能は、既定値では無効に設定されています。ここでは、Web アクセス保護を有効にする手順を紹介します。

1 本プログラムの基本画面を開き、❶［設定］ボタンをクリックして、❷［詳細設定のツリー全体を表示する］をクリックします。



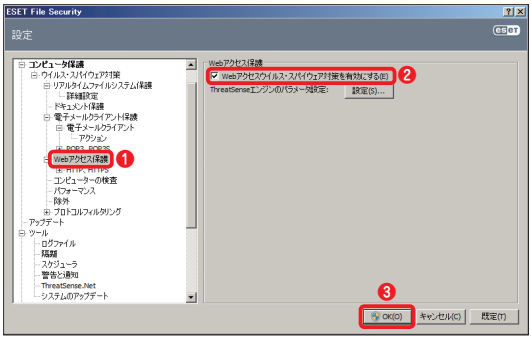
2 「コンピュータ保護」のツリーにある❶［プロトコルフィルタリング］をクリックし、❷［アプリケーションプロトコルフィルタリングを有効にする］と［アプリケーションプロトコル保護を自動的に開始する］にチェックを入れ、❸［OK］ボタンをクリックします。

3

Webアクセス保護が有効になります。

4

手順③でWebアクセス保護が❶「無効」と表示されたときは、❷［詳細設定のツリー全体を表示する］をクリックします。



5

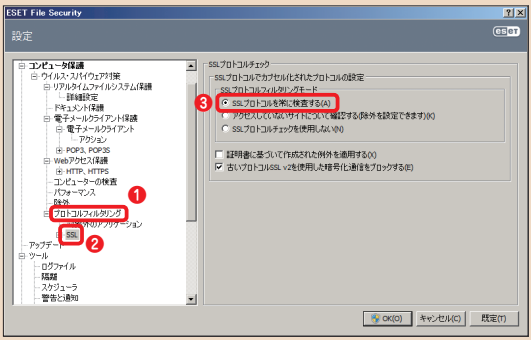
「コンピュータ保護」のツリーにある❶［Webアクセス保護］をクリックし、❷［Webアクセスウイルス・スパイウェア対策を有効にする］にチェックを入れ、❸［OK］ボタンをクリックします。

6

Webアクセス保護が有効になります。

POINT

Web アクセス保護の既定値では、情報を暗号化して通信を行う SSL（Secure Socket Layer）の検査を行いません。SSL の検査も行いたい場合は、❶［プロトコルフィルタリング］をクリックし、❷［SSL］をクリックします。❸［SSL プロトコルを常に検査する］にチェックを入れます。



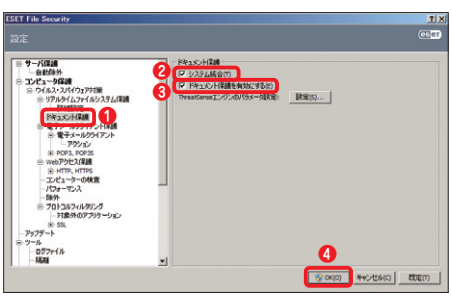
コラム

ドキュメント保護について

本プログラムには、Word や Excel に埋め込まれたウイルスを検出する「ドキュメント保護」機能も搭載しています。既定値では、この機能が無効に設定されています。有効にする場合は、以下の手順を行います。

1

本プログラムの基本画面を開き、❶［設定］ボタンをクリックして、❷［詳細設定のツリー全体を表示する］をクリックします。



2

ウイルス・スパイウェア対策のツリーにある❶［ドキュメント保護］をクリックし、❷［システム統合］と❸［ドキュメント保護を有効にする］にチェックを入れます。❹［OK］ボタンをクリックします。

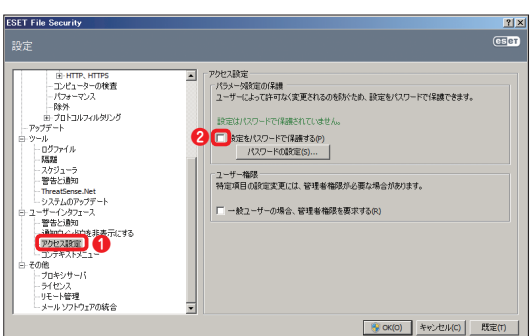
設定 ▸▸ アクセス保護

5-4 アクセス設定を行うには

本プログラムには、設定をパスワードで保護する機能が用意されています。自由に設定変更できないようにパスワードで設定を保護したいときは、以下の手順で設定を行います。

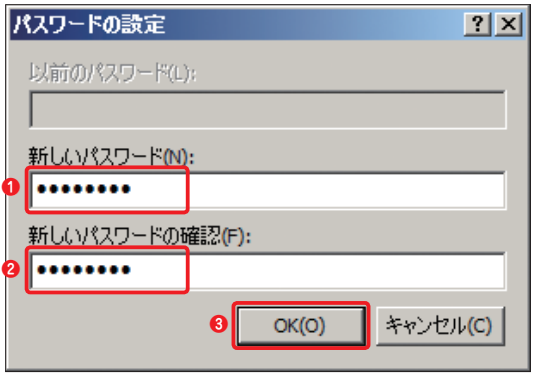
1

本プログラムの基本画面を開き、❶［設定］ボタンをクリックして、❷［詳細設定のツリー全体を表示する］をクリックします。



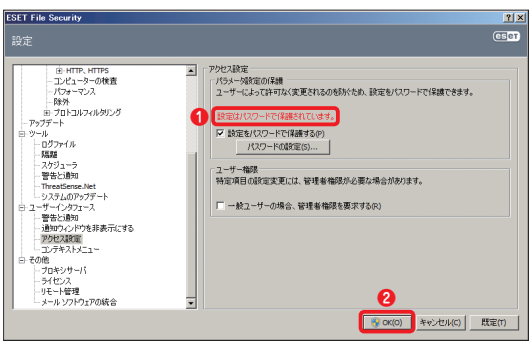
2

［ユーザーインタフェース］の❶［アクセス設定］をクリックし、❷［設定をパスワードで保護する］をクリックします。



3

❶設定したいパスワードを入力し、❷入力したパスワードを再入力します。❸［OK］ボタンをクリックします。



4

❶パスワード保護が設定されます。❷［OK］ボタンをクリックします。

POINT

設定したパスワードを変更したいときは、［パスワードの設定］ボタンをクリックします。また、パスワード保護を無効にしたいときは、［設定をパスワードで保護する］のチェックを外します。

CAUTION

設定したパスワードを忘れると、設定変更やアンインストールが行えなくなります。設定したパスワードを忘れないようにご注意ください。

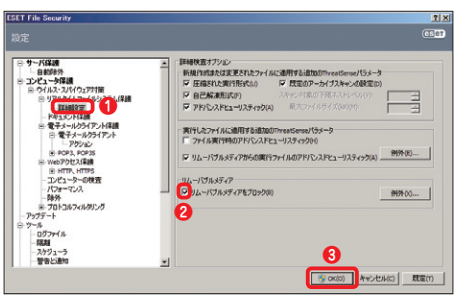
設定 ▸▸ リムーバブルメディア

5-5 リムーバブルメディアの読み出しを制限するには

本プログラムには、コンピューターにセットしたUSBメモリーやCD/DVDディスクなどのリムーバブルメディアの読み出しをブロックする機能が備わっています。ここでは、その機能の使い方を説明します。

1

本プログラムの基本画面を開き、❶［設定］ボタンをクリックして、❷［詳細設定のツリー全体を表示する］をクリックします。



2

❶［リアルタイムファイルシステム保護］の［詳細設定］をクリックし、❷［リムーバブルメディアをブロック］にチェックを入れます。❸［OK］ボタンをクリックします。

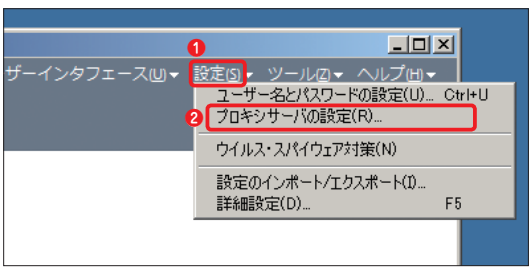
POINT

［例外］ボタンをクリックすると、読み出しに利用するUSBポートを指定できます。これによって、指定したUSBポート以外でUSB機器を読み出せないように設定できます。

設定 ▸▸ プロキシサーバーの設定

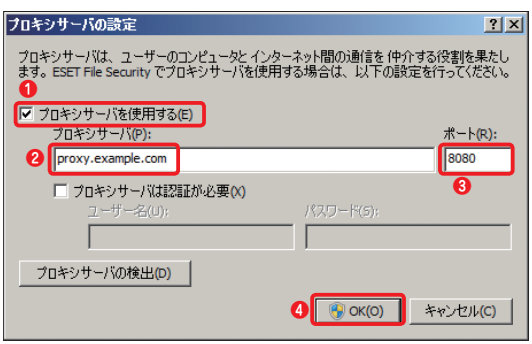
5-6 プロキシサーバーを設定するには

プロキシサーバーを経由してインターネットにアクセスしている場合は、アップデートを行うためにプロキシサーバーの設定が必要です。



1

本プログラムの基本画面を開き、メニューバーの❶［設定］をクリックし、❷［プロキシサーバの設定］をクリックします。



2

❶［プロキシサーバを使用する］にチェックを入れ、❷「プロキシサーバ」欄にサーバ名、❸「ポート」欄にポート番号を入力します。❹［OK］ボタンをクリックします。

POINT

［プロキシサーバの検出］ボタンをクリックすると、Internet Explorer で設定されたプロキシサーバーを自動検出します。

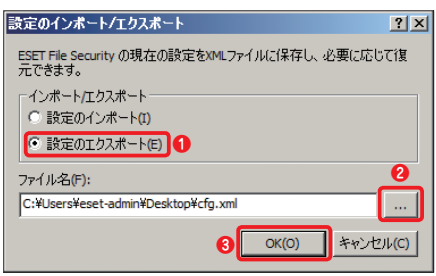
設定 ▸▸ インポートとエクスポート

5-7 詳細設定をインポート・エクスポートするには

ここでは、詳細設定をファイルに出力し、インポート・エクスポートするための手順を紹介します。

1

本プログラムの基本画面を開き、❶［設定］ボタンをクリックし、❷［設定をインポートおよびエクスポートする］をクリックします。



2

設定を保存するには、❶［設定のエクスポート］をクリックしてチェックを入れ、❷［…］ボタンをクリックしてファイル名、保存場所を設定してから、❸［OK］ボタンをクリックします。

POINT

設定を復元するには、手順②で［設定のインポート］を選択し、［…］ボタンをクリックして復元する設定ファイルを選択します。

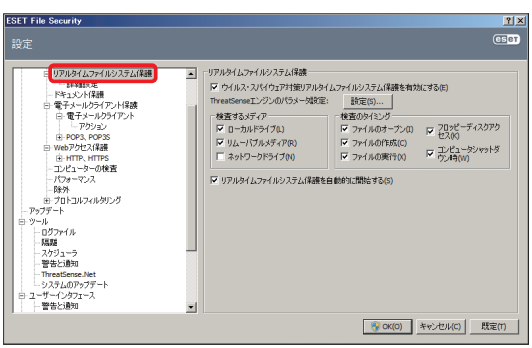
設定 ▸▸ 詳細設定

5-8 各種保護機能の詳細な設定を行うには

電子メール保護などの本プログラムの各保護機能には詳細設定項目が用意されています。ここでは、それぞれの詳細設定項目を呼び出すための手順をご紹介します。

1

本プログラムの基本画面を開き、❶［設定］ボタンをクリックし、❷［ウイルス・スパイウェア対策の設定］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❸［設定］をクリックします。



2

［リアルタイムファイルシステム保護］が選択された状態で設定画面が開きます。なお、手順①で電子メールクライアント保護の❹［設定］をクリックすると、電子メールクライアント保護の詳細設定を行えます。

Part.6
「ツール」画面での操作

本プログラムでは「ツール」を利用することで、詳細な設定や確認が可能になります。ここでは、それらのさまざまな操作方法についてご紹介しています。

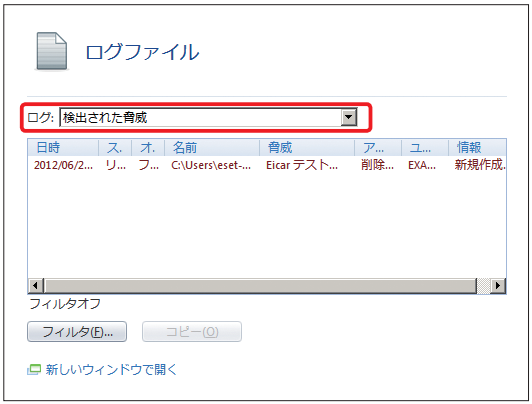
ツール ▸▸ ログファイルの確認

6-1 詳細なログファイルを確認するには

ウイルスの検出・駆除や検査、アップデート情報などのログファイルを確認するには、「ツール」のプライマリウインドウから参照します。

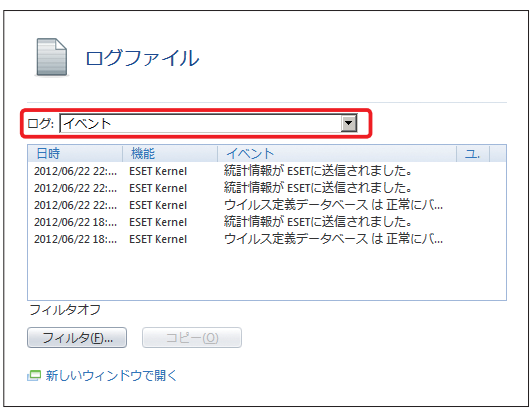
1 本プログラムの基本画面を開き、［ツール］ボタンをクリックします。

2 ［ログファイル］をクリックします。



3

ログ閲覧の画面が表示されます。［ログ］のドロップダウンリストから［検出された脅威］を選択すると、発見したウイルスが一覧形式で表示されます。

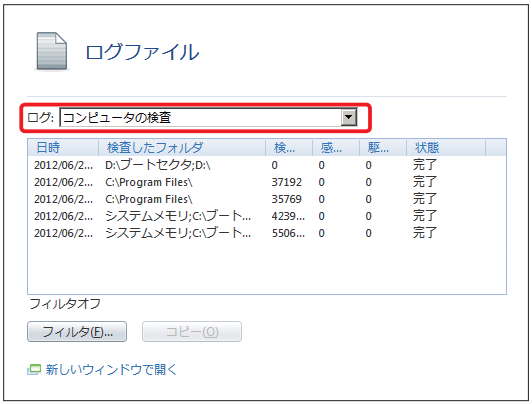


4

［ログ］のドロップダウンリストから［イベント］を選ぶと、アップデートなど本プログラムに関する情報を確認できます。

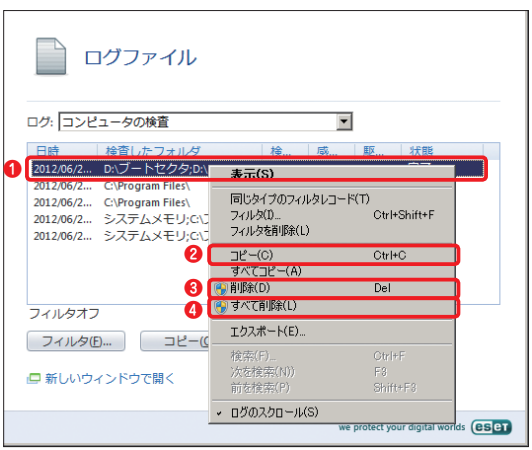
POINT

閲覧できるログは［検出された脅威］［イベント］［コンピュータの検査］の3種類です。



5

［ログ］のドロップダウンリストから［コンピュータの検査］を選ぶと、オンデマンドコンピューター検査の動作結果を確認できます。



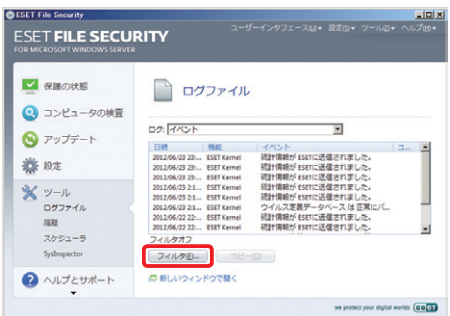
6

ログファイルの内容は、テキストエディタなどにコピーできます。❶対象を右クリックし、メニューから❷［コピー］をクリックします。❸選択しているログを消去するときは［削除］をクリックします。❹すべてのログを消去するときは［すべて削除］をクリックします。

コラム

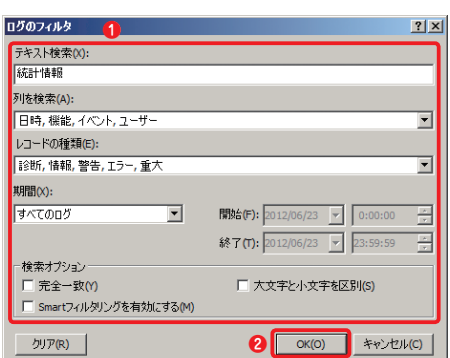
ログの絞り込みを行うには

フィルタを利用すると、表示するログファイルの内容を絞り込むことができます。ログの絞り込みを行う場合は、以下の手順で行います。



1

［フィルタ］ボタンをクリックします。



2

❶絞り込み条件を指定し、❷［OK］ボタンをクリックします。

ツール ▸▸ 隔離ファイルの確認・追加

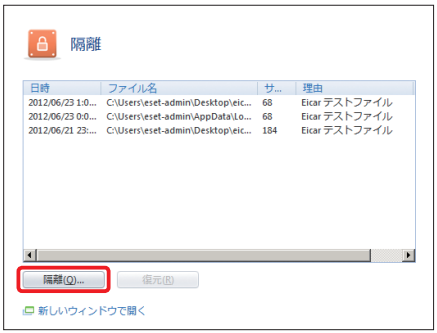
6-2 各種検査で隔離されたファイルを確認・復元するには

本プログラムでは、ウイルスを検出すると、隔離する仕組みになっています。
ここでは隔離ファイルに関する操作手順を紹介します。

隔離されたファイルを確認するには

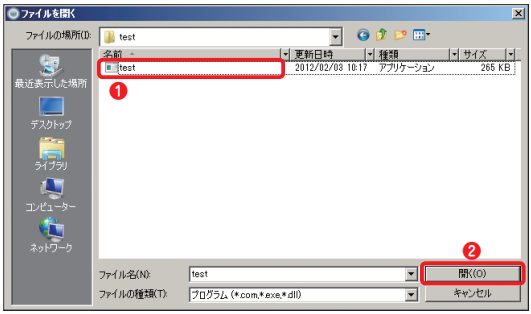
1

本プログラムの基本画面を開き、❶［ツール］ボタンをクリックし、❷［隔離］をクリックします。



2

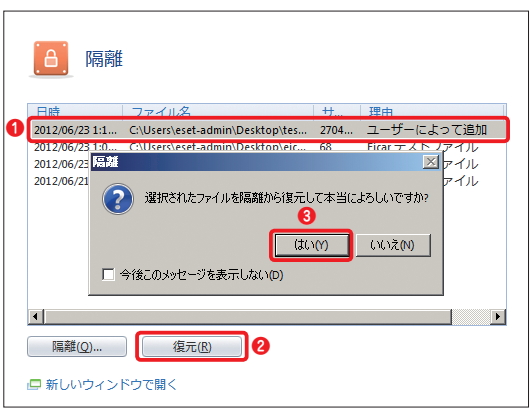
本プログラムが隔離しているウイルスの一覧が表示されます。これらのファイルは無力化されているため、安全です。手動でウイルスや疑わしいファイルを隔離するには［隔離］ボタンをクリックします。



3

ファイル選択ダイアログが表示されます。❶隔離したいファイルを選んでから、❷［開く］ボタンをクリックします。

隔離されたファイルを復元するには



1

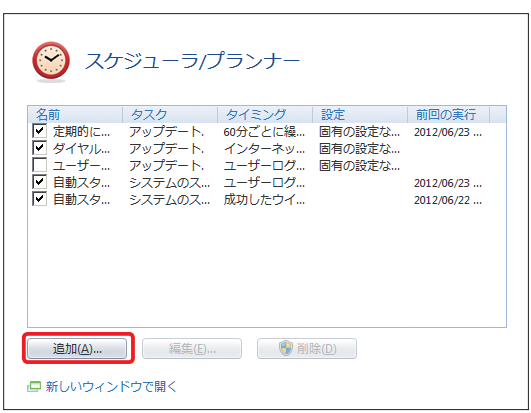
隔離したファイルを復元させるには、一覧から、❶復元したいファイルを選択し、❷［復元］ボタンをクリックします。確認ダイアログが表示されるので、❸［はい］ボタンをクリックします。

ツール ▸ スケジュール設定

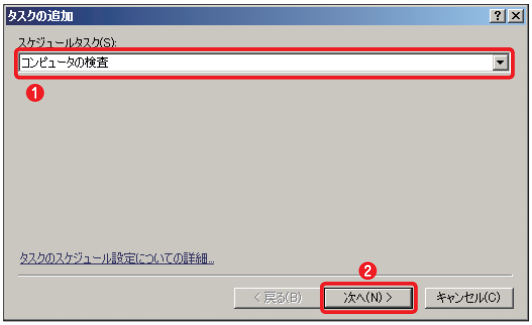
6-3 自動検査・アップデートのスケジュールを設定するには

本プログラムではウイルス定義データベースの自動アップデートなどがあらかじめスケジュールされていますが、必要に応じて、新たなスケジュール設定を追加できます。

1 本プログラムの基本画面を開き、❶［ツール］ボタンをクリックします。❷［スケジューラ］をクリックします。

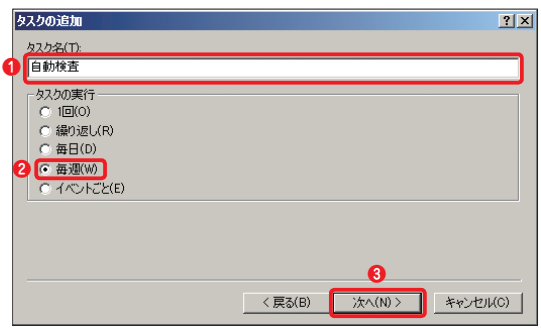


2 現在設定されているスケジュールの一覧が表示されます。例として毎週日曜日にウイルス検査を行うスケジュールを作成します。［追加］ボタンをクリックします。



3

「タスクの追加」ウィザードが起動したら、ドロップダウンリストから、❶［コンピュータの検査］を選択し、❷［次へ］ボタンをクリックします。

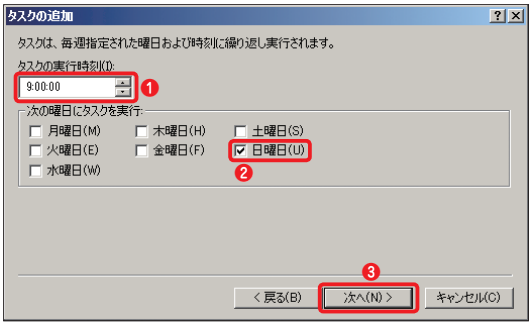


4

タスクの名前、タスクを実行する間隔を指定します。❶タスク名に任意の名前を入力し（例：自動検査）、❷［毎週］にチェックを入れてから、❸［次へ］ボタンをクリックします。

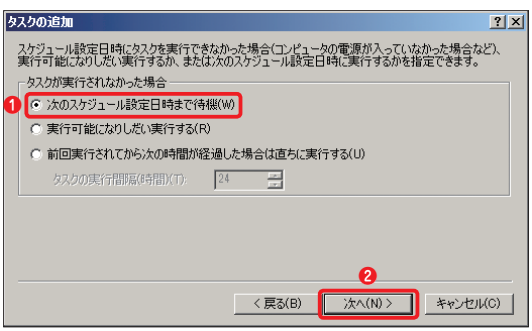
POINT

ウイルス定義データベースのアップデートに関するタスク作成も、手順③で［アップデート］を選択することによって設定できます。



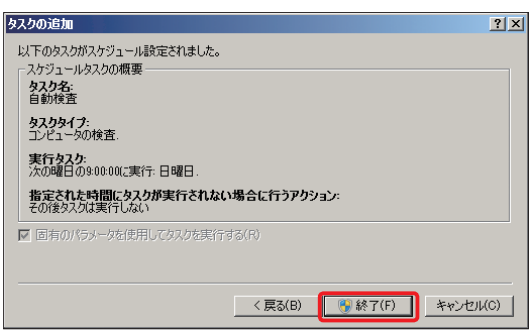
5

タスクの実行時刻と曜日を選択します。❶「タスクの実行時刻」で任意の時間を選択し、❷検査を行う曜日（ここでは「日曜日」）にチェックを入れてから、❸［次へ］ボタンをクリックします。



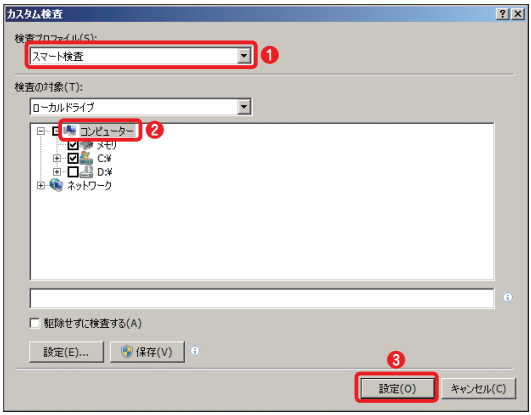
6

タスクが実行されなかったときのアクションを選択します。❶［次のスケジュール設定日時まで待機］にチェックを入れてから、❷［次へ］ボタンをクリックします。



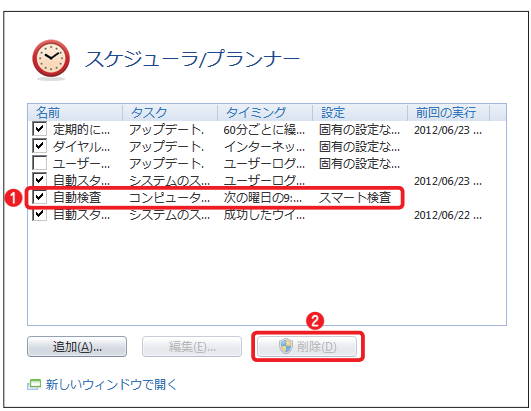
7

設定内容の確認を行います。設定に誤りがある場合は［戻る］ボタンをクリックして再設定してください。問題がなければ［終了］ボタンをクリックします。



8

検査内容を設定するダイアログが表示されます。❶「検査プロファイル」を設定し、❷検査したい対象にチェックを入れ、❸［設定］ボタンをクリックしてください。



9

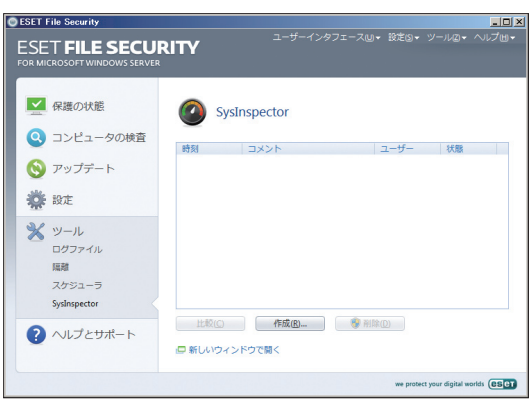
❶スケジュールタスクの一覧に、新たなタスクが追加されました。なお、不要になったスケジュールは項目の先頭にあるチェックを外すか、❷項目を選択して［削除］ボタンをクリックします。

ツール ▸ SysInspector

6-4 コンピューターの様々な情報を確認するには

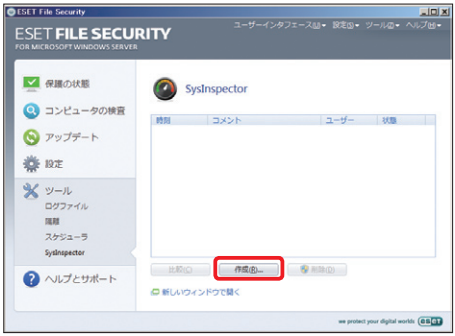
コンピューターで使用されている各種プログラムや重要なレジストリなどの情報を確認するときには、「SysInspector」を使用します。ここでは、その使い方について説明します。

1 本プログラムの基本画面を開き、❶［ツール］ボタンをクリックし、❷［SysInspector］をクリックします。



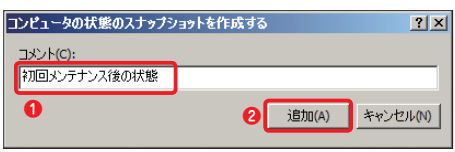
2 「SysInspector」の操作画面に切り替わります。

現在のコンピューターの状態のスナップショット（情報）を保存するには



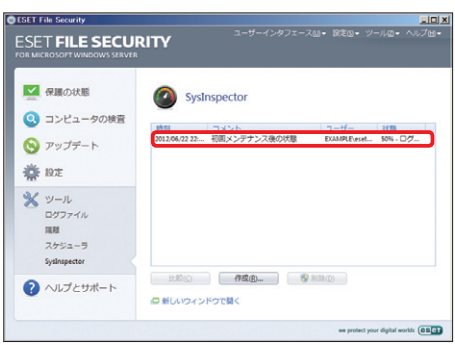
1

前ページの手順を参考に「SysInspector」の操作画面を開き、［作成］ボタンをクリックします。



2

ダイアログが開きます。❶コメントを入力し、❷［追加］ボタンをクリックします。



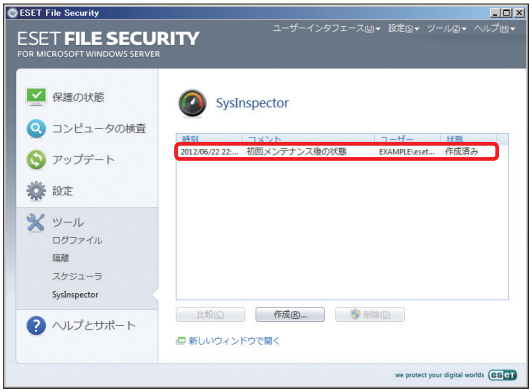
3

現在のコンピューターの状態が保存されます。保存中は、「状態」欄に進捗状況が表示されます。保存が終了すると、「状態」欄に「保存済み」と表示されます。

POINT

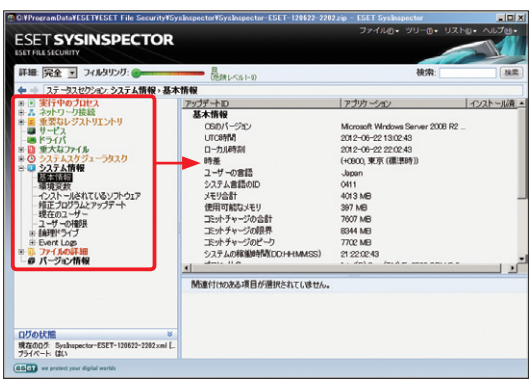
コンピューターの状態（情報）の保存は、何度でも行え、保存した情報は比較することもできます。なお、スケジューラを利用して、定期的に情報を保存することもできます。

保存したスナップショット（情報）を確認するには



1

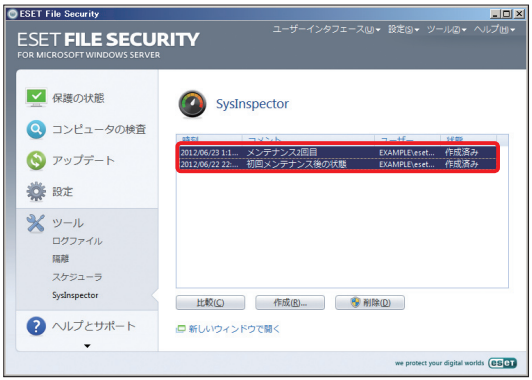
70ページの手順を参考に「SysInspector」の操作画面を開き、閲覧したい情報をダブルクリックします。



2

SysInspectorが起動します。左に表示された項目をクリックすることで、各種情報を確認できます。

保存したスナップショット（情報）を比較するには



1

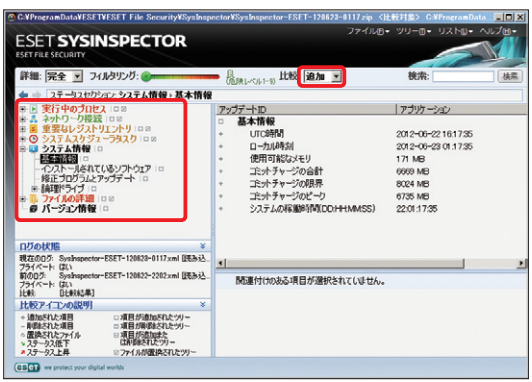
70ページの手順を参考に「SysInspector」の操作画面を開き、比較したいスナップショットを「CTRL」キーを押しながら、クリックして選択します。

2

［比較］ボタンをクリックします。

3

スナップショット（情報）の比較が開始されます。比較中は、進捗状況が表示されます。

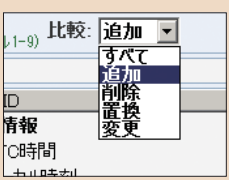


4

SysInspectorが起動します。左に表示された項目をクリックすることで、比較結果を確認できます。

POINT

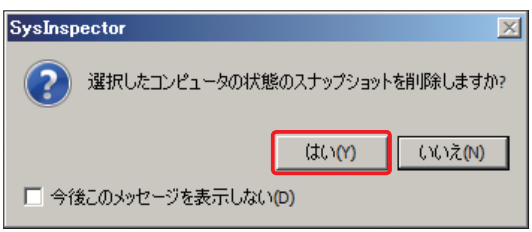
比較結果の表示方法は「すべて」「追加」「削除」「置換」「変更」の５種類から選択できます。たとえば、「変更」を選択すると変更点のみが表示できます。表示方法の変更は、［比較］のドロップダウンリストで行えます。



保存したスナップショット（情報）を削除するには

1

70ページの手順を参考に「SysInspector」の操作画面を開き、❶削除したい情報をクリックし、❷［削除］ボタンをクリックします。



2

ダイアログが表示されます。［はい］ボタンをクリックします。

3

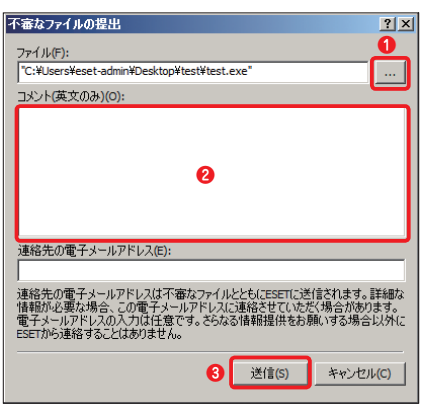
選択した情報が削除されます。

ツール ▸ 検体の提出

6-5 未知のウイルスと判定されたファイルを提出するには

ウイルスとしては検出されませんが、ウイルスの可能性があると判断されたファイルや明らかに動作に異常が見られるファイルを検出したときは、該当するファイルを ESET 社までお送りください。以下に手順を紹介します。

1 本プログラムの基本画面を開き、❶［ツール］ボタンをクリックし、❷［分析のためにファイルを提出］をクリックします。



2 ダイアログが表示されたら❶［...］ボタンをクリックしてファイルを選択してから、❷「コメント」欄に症状やファイルの動作など詳細説明を加えます*。最後に❸［送信］ボタンをクリックします。

* コメントは本製品の開発元である ESET 社へ直接送られます。英語以外のコメント内容は ESET 社で確認できない可能性がありますので、あらかじめご了承ください。

CAUTION

連絡先の電子メールアドレスの入力は任意です。

ツール ▸▸ SysRescue の作成

6-6 SysRescue ディスクを作成するには

SysRescue を使用するには、SysRescue が記録された起動可能な専用の CD/DVD または USB 機器 (USB メモリーや USB HDD) を準備する必要があります。ここでは、その作成手順を紹介します。

1

本プログラムの基本画面を開き、❶［ツール］ボタンをクリックし、❷［レスキューCDの作成］をクリックします。

POINT

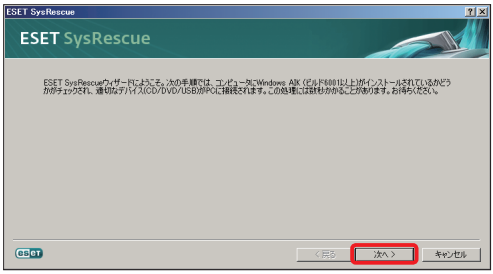
「ユーザーアカウント制御」画面が表示されたときは、［はい］ボタンをクリックします。

コラム

64bit 環境で SysRescue ディスクを作成するには

64bitプラットフォームの Windows で本プログラムをご使用の場合は、SysRescue ディスクの作成に本プログラムの 32bitプラットフォーム用のインストーラー（拡張子「.msi」のファイル）が必要になります。弊社ユーザーズサイトからあらかじめインストーラー（拡張子「.msi」ファイル）をダウンロードしてからご利用ください。

ユーザーズサイト : http://canon-its.jp/product/eset/users/index_fs.html

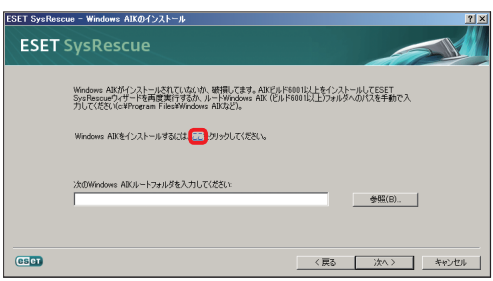


2

SysRescueウィザードが開きます。［次へ］ボタンをクリックします。

POINT

SysRescue の使用には、Windows AIK ビルド 6001 以上をインストールする必要があります。Windows AIK ビルド 6001 以上がインストールされていない場合は手順③へ、インストールされている場合は手順⑩へ進んでください。

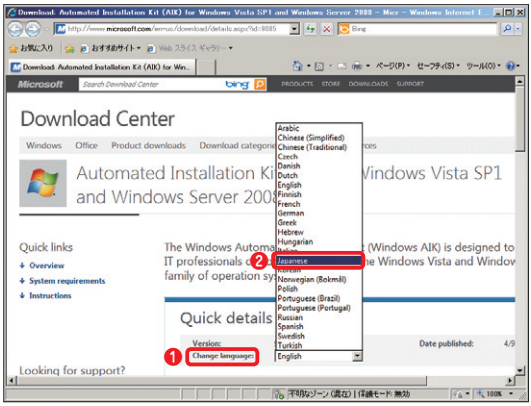


3

Windows AIKがインストールされていない場合、または既定値と異なるフォルダーにインストールされている場合は、Windows AIKのインストール画面が表示されます。Windows AIKのインストールを行う場合は、［ここ］の文字をクリックします。すでにインストール済みの場合は、手順⑩に進んでください。

POINT

既定値とは異なるフォルダーに Windows AIK をインストールしている場合は、［参照］ボタンをクリックし、インストールフォルダーを選択します。



4

Microsoft社のWindows AIKダウンロードページが開きます。❶[Change Language:]のドロップダウンボタンをクリックし、❷[Japanese]を選択します。

5

日本語表示に変わります。ページを一番下までスクロールし、[Windows 7 用の Windows 自動インストールキット（AIK）]をクリックします。

POINT

このページで、[Windows 7 用の Windows 自動インストールキット（AIK）]が表示されない場合は、以下の URL を参照してください。なお、この URL は予告なく変更される場合があります。

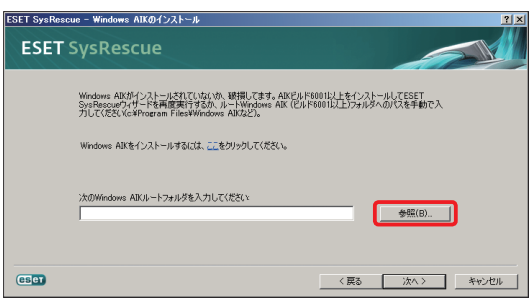
http://www.microsoft.com/downloads/ja-jp/details.aspx?FamilyID=696DD665-9F76-4177-A811-39C26D3B3B34

6

［ダウンロード］ボタンをクリックし、ファイルをダウンロードします。また、ダウンロードしたファイルを市販の DVDライティングソフトなどを使用して記録型 DVDディスクに記録し、Windows AIK のインストールを行います。

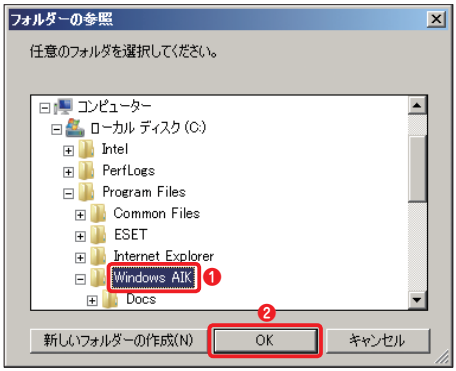
POINT

ダウンロードした Windows AIK のファイルは、ISO イメージと呼ばれるファイル形式です。この形式のファイルは、市販の CD/DVD ライティングソフトなどで記録型 DVD ディスクに記録できます。

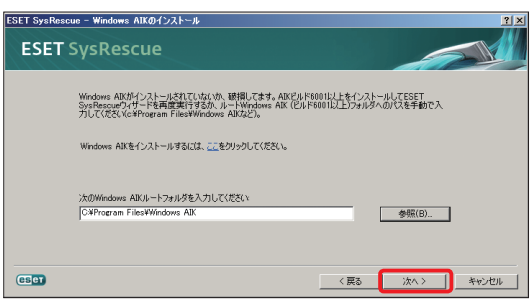


7

Windows AIKのインストールが終了したら、［参照］ボタンをクリックします。



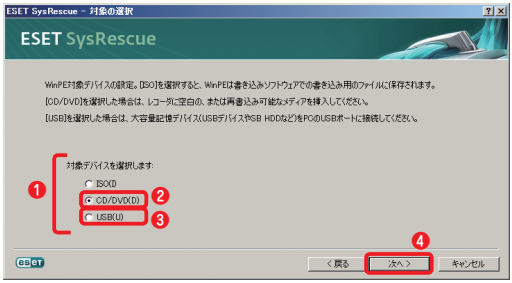
8 ［フォルダーの参照］ダイアログが表示されます。❶Windows AIKのインストールフォルダーを指定し、❷［OK］ボタンをクリックします。



9 ［Windows AIKのインストール］画面に戻ります。［次へ］ボタンをクリックします。

POINT

手順⑧の作業がうまくいかない場合は、［キャンセル］ボタンをクリックし、手順①から作業をやり直してください。

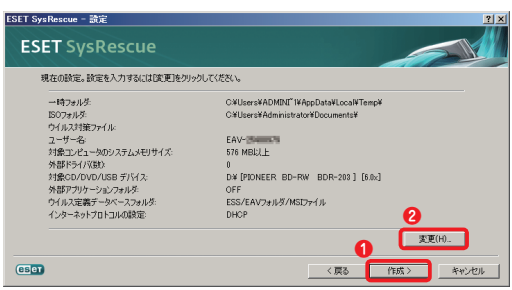


10

❶作成先（対象デバイス）を選択します。❷CD/DVD を選択した場合は、メディアをドライブにセットします。❸USB を選択した場合は、USB 機器（USB メモリー）を接続します。❹準備が完了したら、［次へ］ボタンをクリックします。ここでは CD/DVD を選択します。

POINT

Windows Server 2003環境の場合、Microsoftより修正ファイル Windows Server 2003用 Image Mastering API V20（KB932716）を適用後、「IMAPI CD-Burning COM Service」を起動する必要があります。なお、作成先（対象デバイス）に「ISO」を選択した場合は、HDD内にISOイメージファイルを作成します。

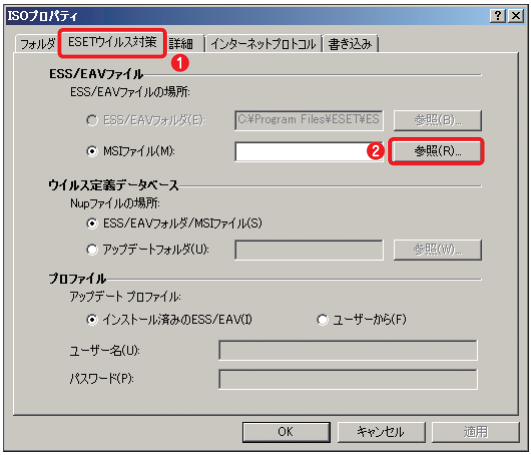


11

❶32bit 版をご使用の場合は、設定を確認し、［作成］ボタンをクリックして手順⑯に進みます。❷64bit 版をご使用の場合は［変更］ボタンをクリックし、手順⑫に進みます。

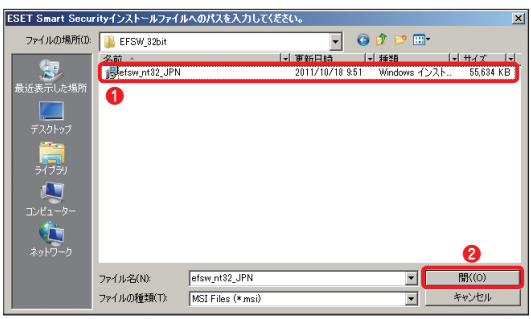
POINT

［変更］ボタンをクリックすると詳細な設定が行えます。64bit 環境で SysRescue を作成する場合は、必ず、［変更］ボタンをクリックし、手順⑫に進んでください。また、作成先（対象デバイス）を変更したい場合は、［戻る］ボタンをクリックしてください。



12

「ISOプロパティ」ダイアログが開きます。❶［ESETウイルス対策］タブをクリックし、❷ ESS/EAVファイル欄の［参照］ボタンをクリックします。

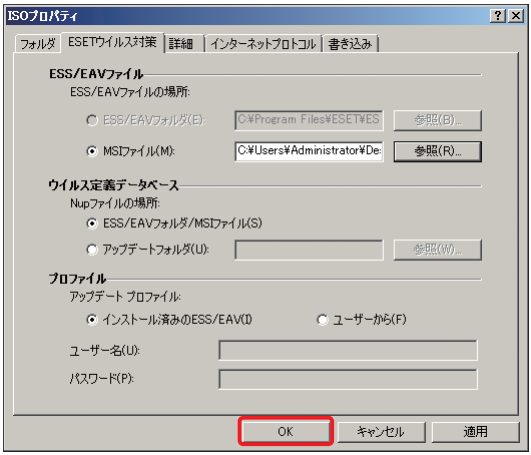


13

ダイアログが開きます。❶本プログラムの32bitプラットフォーム用のインストーラ（拡張子「.msi」ファイル）を選択し、❷［開く］ボタンをクリックします。

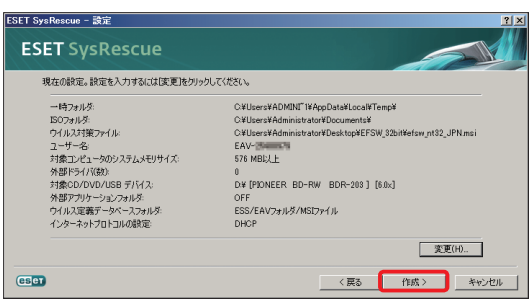
POINT

本プログラムで利用するインストーラーは、拡張子「.msi」のファイルです。32bit プラットフォーム用と 64bit プラットフォーム用のインストーラーがあります。間違えないように 32bit プラットフォーム用を選択してください。また、間違って64bit プラットフォーム用のインストーラーを選択した場合は、手順⑭のあとに、それを知らせるダイアログが表示されます。



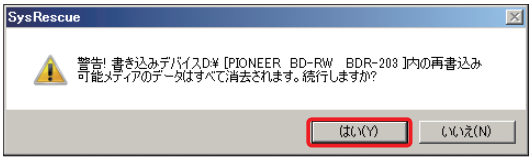
14

［ISOプロパティ］ダイアログに戻ります。［OK］ボタンをクリックします。



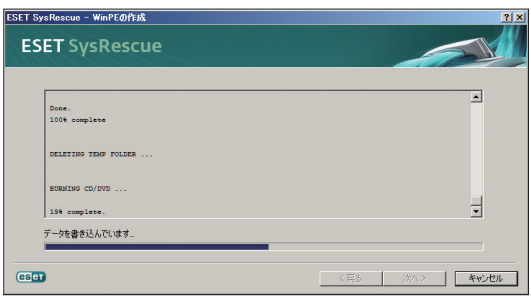
15

設定画面に戻ります。設定内容を確認し、［作成］ボタンをクリックします。



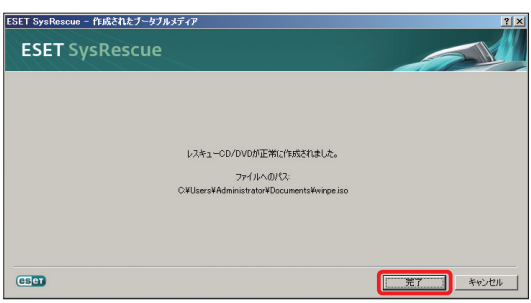
16

データが記録されたUSB機器（USBメモリーやUSB HDD）やCD-R、DVD-Rなどを作成先に指定した場合は、内容が消去されることを確認する画面が表示されます。続行する場合は、［はい］ボタンをクリックします。



17

作成作業が開始されます。作業中は、進捗状況が表示されます。



18

作成が終了したら、［完了］ボタンをクリックし、SysRescueウィザードを終了します。

ツール ▸▸ 作成ディスクの起動

6-7 SysRescue ディスクから起動するには

SysRescue ディスクを用いると、Windows を起動させずに本プログラムの簡易機能を使用できます。ここでは、SysRescue ディスクの起動方法について説明します。

1

作成した SysRescue ディスクが最優先で起動するようにコンピューターの起動方法の設定を行います。CD/DVD を作成した場合は CD/DVD が、USB 機器（USB メモリーや USB HDD）を作成した場合は USB 機器が最優先で起動するようにコンピューターを設定してください。

POINT

起動順の変更は、ご使用のコンピューターのマニュアルなどを参考に行ってください。

2

コンピューターに SysRescue ディスクをセットし、電源をオンにします。

3

SysRescue が起動します。使用方法については、基本的に Windows 上で使用する場合と同じですので、そちらをご参照ください。

POINT

SysRescue が起動しない場合は、起動順の設定が間違っている可能性があります。再度確認してください。

Part.7
「ヘルプとサポート」画面での操作

ここでは、本プログラムのヘルプとサポートについてご紹介しています。

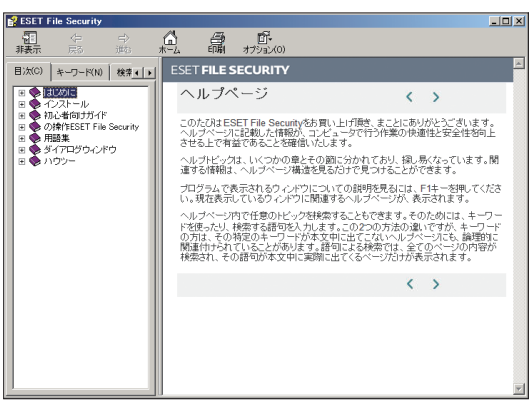
ヘルプ ▸▸ ヘルプの確認

7-1 ヘルプを見るには

本書がお手元にない場合など、迅速に本プログラムの機能を確認するときはヘルプ機能をご覧ください。基本的な使い方だけでなく技術的な解説も収録されています。

1

本プログラムの基本画面を開き、❶［ヘルプとサポート］ボタンをクリックし、❷［ヘルプを開く］をクリックします。



2

ヘルプが表示されます。

ヘルプ ▸▸ ナレッジベース

7-2 サポート情報を検索するには

本プログラムに関するよくある質問とその回答を弊社ホームページ上にて公開していますので、ぜひご活用ください。

1

本プログラムの基本画面を開き、❶［ヘルプとサポート］ボタンをクリックします。❷［インターネットで調べる］をクリックします。

2

弊社ホームページのサポート情報にアクセスし、本プログラムに関するサポート情報を閲覧することができます。

POINT

インターネットにアクセスできる状態で実行してください。

ヘルプ ▸▸ Web ページ

7-3 本製品に関するWebサイトにアクセスするには

本製品に関する Web サイトではアップデート情報などの各情報を提供しております。最新のウイルス情報などを確認する際にご活用ください。

1

本プログラムの基本画面を開き、❶［ヘルプとサポート］ボタンをクリックし、❷［ホームページを参照］をクリックします。

2

本製品に関する Web サイトにアクセスし、本製品の様々な情報を確認できます。

POINT

インターネットにアクセスできる状態で実行してください。

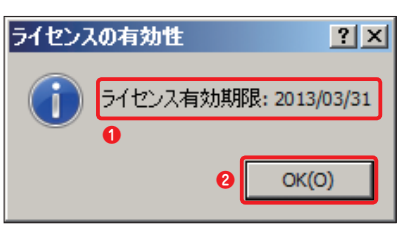
ヘルプ ▸▸ ライセンスの有効期間

7-4 ライセンスの有効期間を確認するには

本プログラムのライセンス期限の確認は、以下の手順で行えます。

1

本プログラムの基本画面を開き、❶メニューバーの［ヘルプ］をクリックし、❷［ライセンスの有効性の確認］をクリックします。



2

❶ライセンスの有効期限を示すダイアログが表示されます。❷［OK］ボタンをクリックするとダイアログが閉じます。

POINT

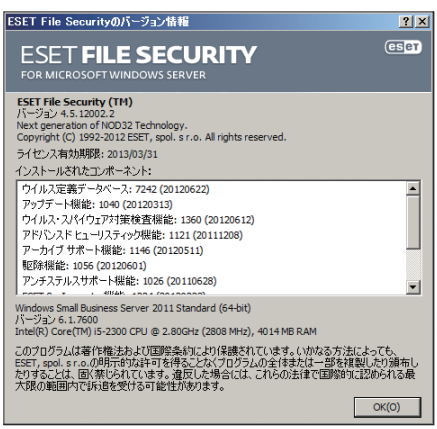
本プログラムのライセンス期限は、［保護の状態］のプライマリウィンドウにも表示されています。

ヘルプ ▸ バージョン情報

7-5 本製品のバージョン情報を確認するには

サポートセンターへのご質問の際には、本プログラムのバージョン情報が必要になる場合があります。ここでは、バージョン情報の確認手順を紹介します。

1 本プログラムの基本画面を開き、❶［ヘルプとサポート］ボタンをクリックし、❷［ESET File Security について］をクリックします。



2 本プログラムのバージョン情報が表示されます。

POINT

本プログラムのバージョン情報は、メニューバーの［ヘルプ］をクリックし、［バージョン情報］をクリックすることでも表示されます。

Part.8
サーバ保護機能

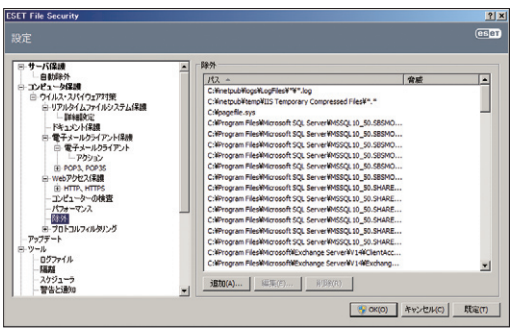
ここでは、本プログラムに搭載されたサーバ保護機能について
ご紹介します。

サーバ保護機能 ▸ サーバ保護

8-1 サーバ保護機能とは

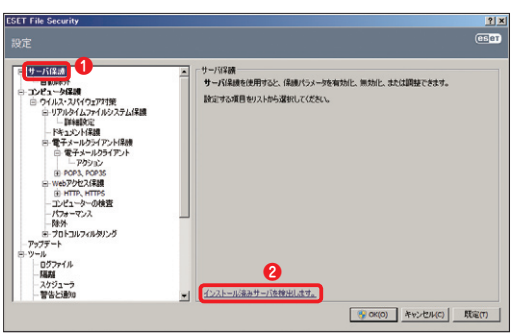
本プログラムには、重要なサーバーアプリケーションと OS のシステムファイルを識別して、除外リストに自動的に登録する「自動除外」機能を搭載しています。ここでは、サーバ保護の概要と有効・無効の切り替えについて説明します。

「自動除外」の有効 / 無効を切り替える



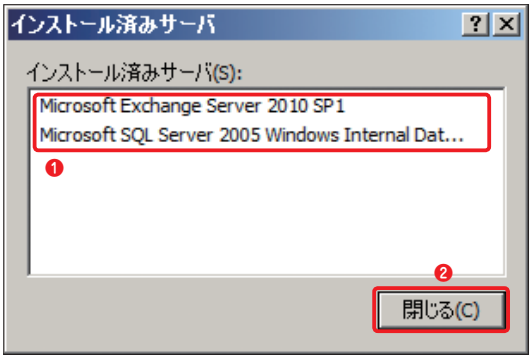
1

既定値では、サーバ保護の「自動除外」機能が有効に設定されています。この機能が有効に設定されていると、インストール済みのサーバー機能と OS のシステムファイルが除外リストに自動登録され、潜在する競合のリスクとサーバーの全体的なパフォーマンスへの影響を最小化します。



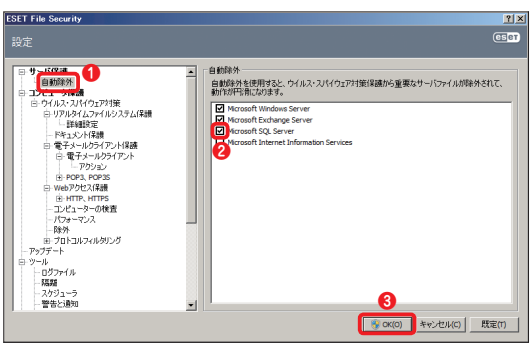
2

インストールされているサーバ機能を確認したいときは、❶［サーバ保護］をクリックし、❷［インストール済みサーバを検出します］をクリックします。



3

❶インストールされているサーバ機能の一覧が表示されます。❷［閉じる］ボタンをクリックし、ダイアログを閉じます。



4

「自動除外」機能の有効・無効を切り替えたいときは、❶［自動除外］をクリックし、❷自動除外を無効にしたいサーバー機能のチェックを外し、❸［OK］ボタンをクリックします。

POINT

「自動除外」が有効になっていると、サーバーを再起動するたびに除外の自動チェックが実行されます。そして、リストから削除された重要なファイルやフォルダーがあれば、そのファイルやフォルダーを、除外リストに再度、自動登録します。また、自動除外が無効になっていると、サーバーを再起動しても除外リストから削除されたファイルやフォルダーの自動再登録は行われません。自動除外は、ウイルス対策によるサーバーへの影響を最小化することでパフォーマンスを維持するために搭載された機能です。通常、この設定は、有効にしたまま利用することをお勧めします。

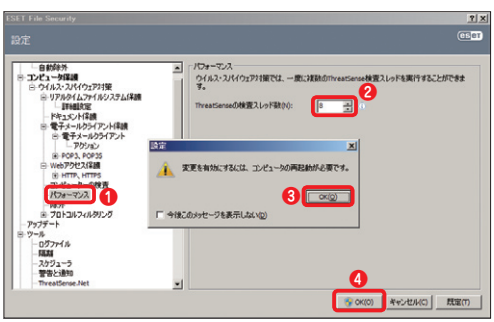
サーバ保護機能 ▸▸ 検査スレッド

8-2 検査速度を向上させるには ～ ThreatSense の検査スレッド数の設定

本プログラムは、ウイルス検査で利用する ThreatSense の検査スレッド数の設定が行えます。マルチプロセッサ環境で本プログラムを利用する場合は、ThreatSense 検査スレッドを増やすことで検査速度を上げることができます。

1

本プログラムの基本画面を開き、❶［設定］ボタンをクリックし、❷［詳細設定のツリー全体を表示する］をクリックします。



2

❶［パフォーマンス］をクリックし、❷ ThreatSense の検査スレッド数を入力します。❸ダイアログが表示されたら［OK］ボタンをクリックします。❹［OK］ボタンをクリックして［設定］ダイアログを閉じ、コンピューターを再起動します。

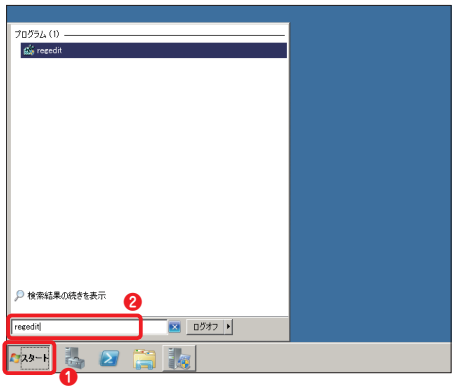
POINT

設定できる ThreatSense の検査スレッド数は、「1 ～ 20」です。また、この設定は、コンピューターを再起動しないと有効になりません。設定を変更した場合は、コンピューターを必ず再起動してください。

コラム

Windows ターミナルサーバでの GUI の無効化について

本プログラムの基本画面（GUI）は、リモートユーザーがサーバーにログオンして、端末セッションを作成するたびに開始されます。ターミナルサーバーで本プログラムを利用する場合、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、次の手順で設定します。なお、この設定は、レジストリの変更を行います。操作には、注意してください。

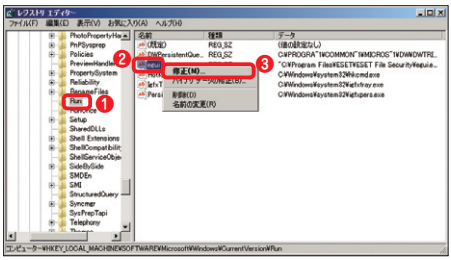


1

❶［スタート］ボタンをクリックし、❷検索ボックスに［regedit］と入力して、［Enter］キーを押します。

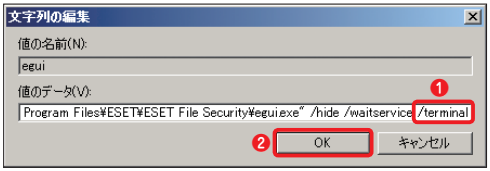
CAUTION

［ユーザーアカウント制御］ダイアログが表示された場合は、［はい］ボタンまたは［続行］ボタンをクリックします。



2

レジストリエディターが起動します。❶［HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run］を開きます。❷［egui］を右クリックし、❸［修正］をクリックします。



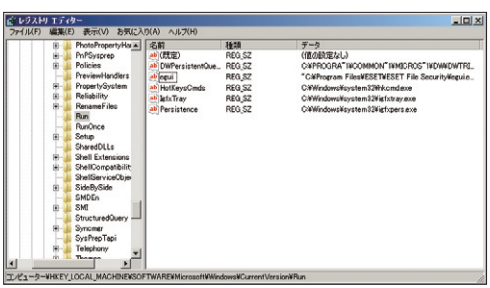
3

❶既存の文字列の末尾に、半角スペースを入力して［/terminal］の文字を追加し、❷［OK］ボタンをクリックします。

POINT

手順③で文字列を追加した場合の egui の［値］データは、以下のようになります。

"C:¥Program Files¥ESET¥ESET File Security¥egui.exe" /hide /waitservice /terminal



4

［閉じる］ボタンをクリックして、レジストリエディターを終了し、コンピューターを再起動します。

POINT

設定を既定値に戻し、GUI を有効にしたい場合は、［/terminal］の文字列を削除してください。

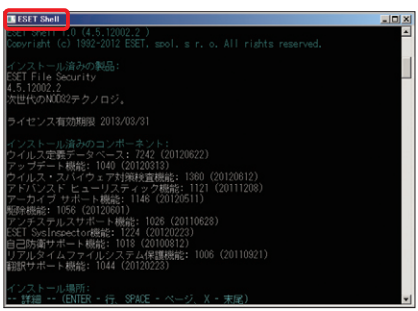
Part.9
コマンドライン インターフェースで 操作するには ～ eShell の使用方法

本プログラムには、コマンドラインインターフェース「eShell」が搭載されています。ここでは、eShell の使い方を説明します。

eShell ▸▸ eShell とは

9-1 eShell とは

eShell は、本プログラムの各種操作が行えるコマンドラインインターフェースです。eShell 専用のウィンドウで作業する「対話モード」と Windows のコマンドプロンプトから利用する単一コマンド / バッチモードがあります。

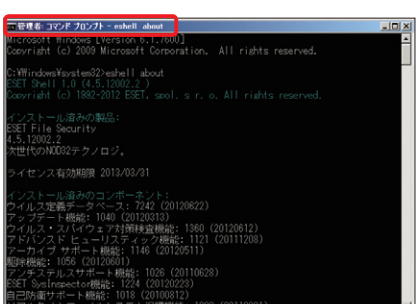


1

対話モードは、eShell専用のウィンドウで各種操作を行います。実行する各種操作は、階層構造で分類されており、そのままコマンドを実行できるだけでなく、コンテキスト名と呼ばれるフォルダーに相当する分類名を入力してツリー内を移動することもできます。

POINT

対話モードでは、コンテキストを移動するとそのコンテキストで利用できるすべてのコマンドとサブコンテキストが一覧表示されます。



2

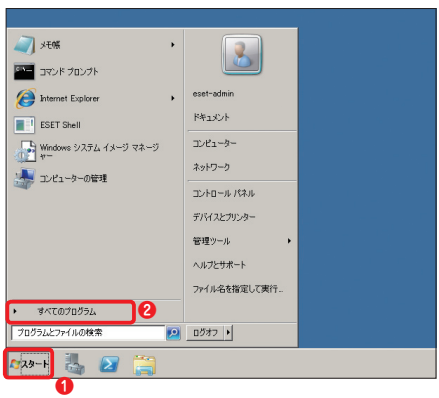
単一コマンド / バッチモードでは、Windows のコマンドプロンプトから本プログラムの各種操作が可能です。複数の操作をまとめて実行するバッチ処理を行う場合などに便利な上級者向けの操作方法です。

eShell ▸▸ 対話モード

9-2 eShell を対話モードで利用するには

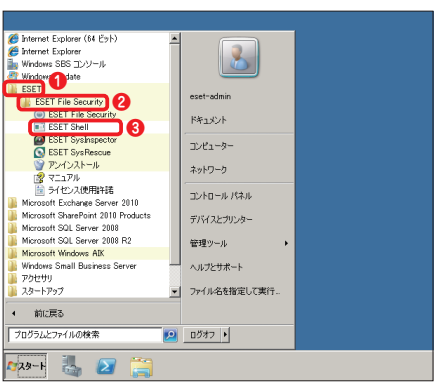
ここでは、本プログラムの各種操作が行えるコマンドラインインターフェース「eShell」の対話モードで利用する方法について紹介します。

対話モード専用のウィンドウを開く



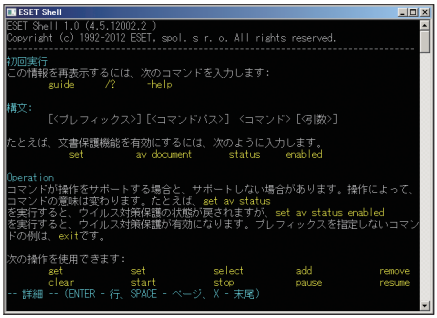
1

❶［スタート］ボタンをクリックし、❷［すべてのプログラム］または［プログラム］をクリックします。



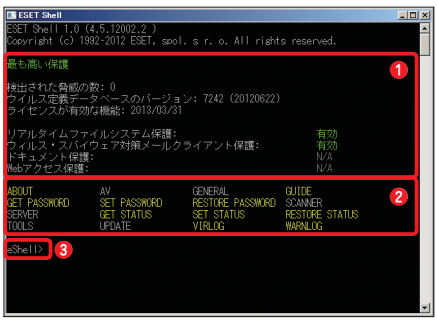
2

❶［ESET］をクリックし、❷［ESET File Security］をクリックして、❸［ESET Shell］をクリックします。



3

eShellが起動します。初めてeShellを起動したときは、eShellの簡単な使い方などを表示する［guide］コマンドが自動実行されます。［X］キーを押すと、末尾を表示します。



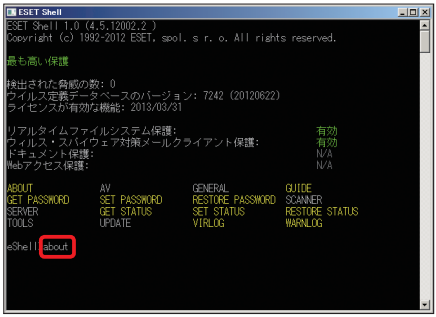
4

2度目以降は、❶現在の保護の状態などに加え、❷利用可能なコマンドやコンテキストなどが表示されます。❸作業を行うときは、［eShell>］と表示されたプロンプトにコマンドまたはコンテキストを入力し、［Enter］キーを押します。

POINT

［eShell>］と表示されたプロンプトは、現在のコンテキスト位置を示し、［eShell>］と表示された状態を「ルート」と呼びます。コンテキストを移動すると表示が変更されます。また、黄色の文字で表示されているのが、現在のコンテキスト位置で利用できるコマンド一覧です。白の文字で表示されているのがコンテキストです。eShell のコマンド構成については、106 ページのコラムをご参照ください。

コマンドを実行する

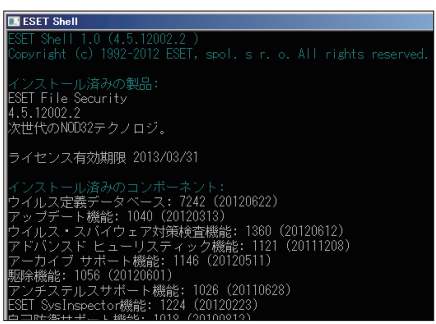


1

ここでは、例として製品情報を表示する「ABOUT」コマンドを実行します。［eShell>］と表示されたプロンプトに［about］と入力し、［Enter］キーを押します。

POINT

入力するコマンドやコンテキストは、大文字 / 小文字を区別していません。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。



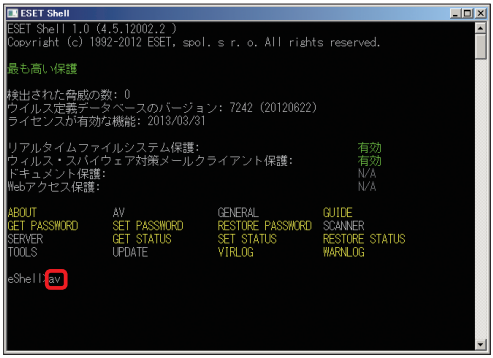
2

［ABOUT］コマンドが実行され、製品情報が表示されます。［X］キーを押すと、末尾を表示します。

POINT

プロンプトに［cls］と入力し、［Enter］キーを押すと、表示されている情報をすべて消去できます。また、［↑］キーや［↓］キーを押すとeShellのウィンドウを開いてから実行したコマンドの履歴をプロンプトに表示できます。

コンテキストを移動する

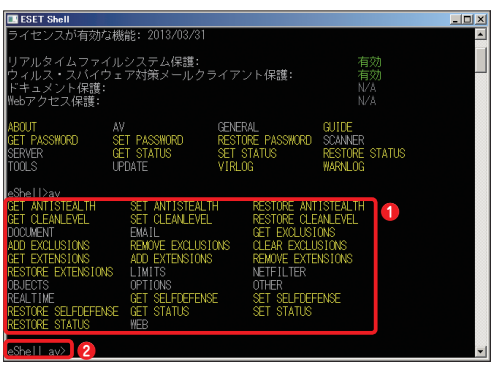


1

ここでは、例として「AV」コンテキストに移動します。［eShell>］と表示されたプロンプトに［AV］と入力し、［Enter］キーを押します。

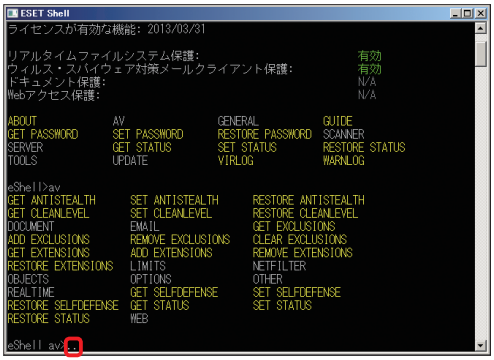
POINT

［eShell>］と表示されたプロンプトは、現在のコンテキスト位置を示します。［eShell>］と表示された状態を「ルート」と呼びます。



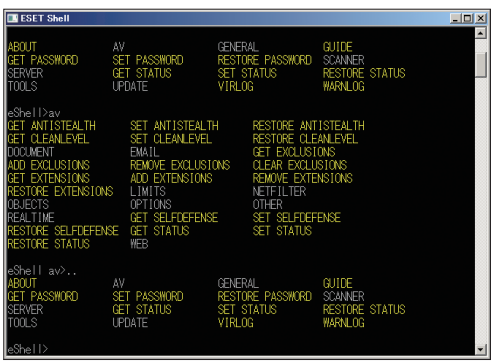
2

コンテキストが移動し、❶そのコンテキストで利用できるすべてのコマンドとサブコンテキストが一覧表示されます。また、❷プロンプトの表示が［eShell コンテキスト名 >］（ここでは、［eShell av>］）に変わります。



3

1つ前のコンテキスト（ここでは、ルート）に戻るには、プロンプトに［..］（半角ピリオドを2度入力）と入力し、［Enter］キーを押します。



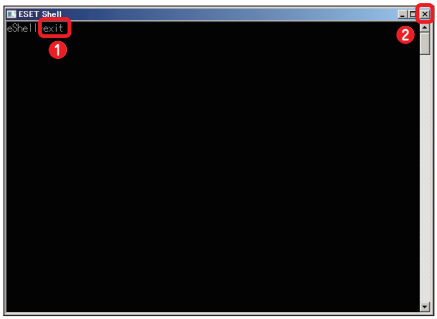
4

1つ前のコンテキスト（ここでは、ルート）に戻ります。

POINT

［.. ..］と半角スペースで区切って、［..］を2度続けて入力すると、2つ前のコンテキストに戻ります。

eShell の専用ウィンドウを閉じる



1

❶プロンプトで［exit］と入力し、［Enter］キーを押すか、❷ウィンドウの［閉じる］ボタンをクリックします。

コラム

eShell のコマンド構成について

eShell で利用される操作コマンドは、❶実行する操作を示す［プレフィックス］、❷特定のコマンドのパスを示す［コンテキスト］または［サブコンテキスト］、❸実際に実行する［コマンド］、❹コマンドが実行する動作を設定する［オプション］の 4 項目で構成されます。これらを以下のような構成で入力し、各種操作を行います。

コマンド構成
［❶プレフィックス］［❷コンテキスト］［❸コマンド］［❹オプション］

実際の操作例（リアルタイムファイルシステム保護の有効化）

SET AV REALTIME STATUS ENABLED

プレフィックス　コンテキスト　コマンド　オプション

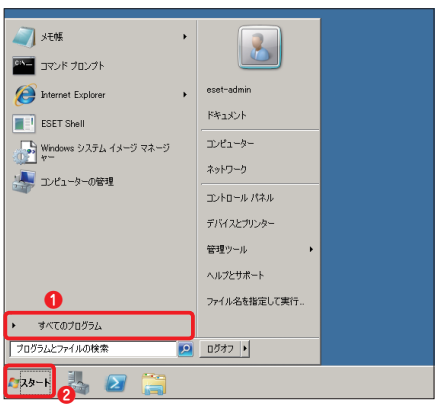
POINT

eShell で利用できる操作には、GUIDE や ABOUT など特定の引数やプレフィックスを使用しないコマンドも存在します。また、コンテキストを移動した場合、そのコンテキストは入力しません。たとえば、上記の例の場合、［AV REALTIME］コンテキストに移動しているときは、［SET STATUS ENABLED］と入力します。

eShell ▸▸ 単一コマンド / バッチモード

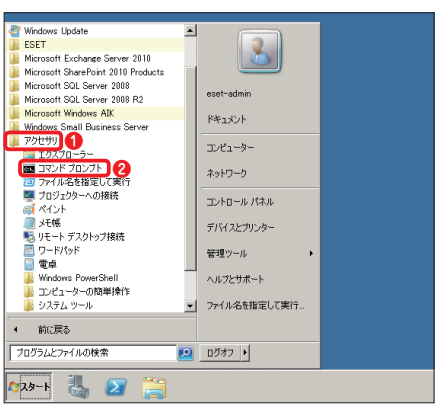
9-3 eShell を単一コマンド / バッチモードで利用するには

ここでは、eShell を単一コマンド / バッチモードで利用する方法について紹介します。



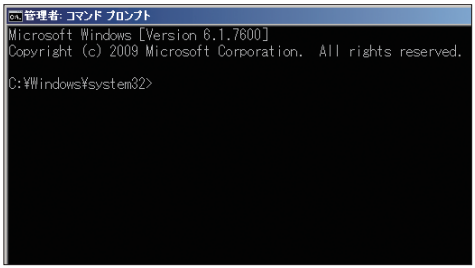
1

❶［スタート］ボタンをクリックし、❷［すべてのプログラム］または［プログラム］をクリックします。



2

❶［アクセサリ］をクリックし、❷［コマンド プロンプト］をクリックします。

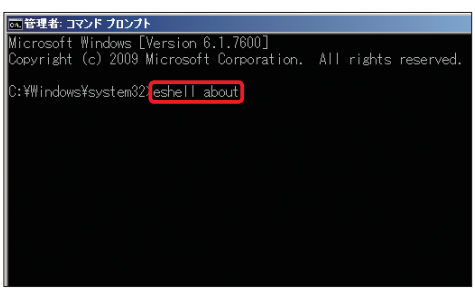


3

コマンドプロンプトが起動します。eShellで実行する操作を、［eShell］と入力後、半角スペースを入力し、［プレフィックス］［コンテキスト］［コマンド］［オプション］の形式で入力して、［Enter］キーを押します。

POINT

入力するコマンドやコンテキストは、大文字 / 小文字を区別していません。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。

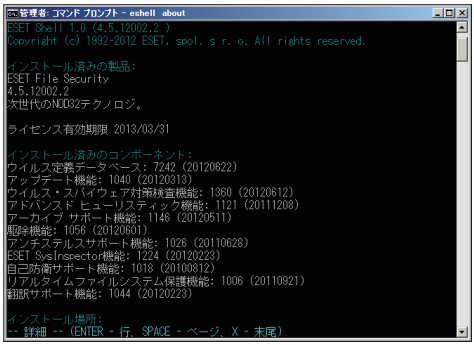


4

ここでは、例として、［ABOUT］コマンドを実行します。プロンプトに［eshell about］と入力し、［Enter］キーを押します。

CAUTION

単一コマンド / バッチモードで eShell を利用する場合、既定値では、オプションを指定した操作を実行できません。この操作を行いたいときは、110 ページの手順を参照してこの機能を有効にする必要があります。



5

［ABOUT］コマンドが実行され、製品情報が表示されます。［X］キーを押すと、末尾を表示します。コマンドプロンプトを終了する場合は、［exit］と入力し、［Enter］キーを押すか、［閉じる］ボタンをクリックします。

コラム

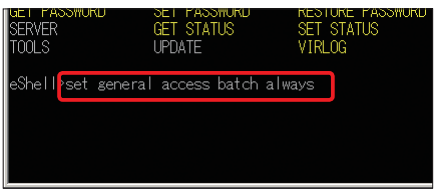
単一コマンド / バッチモードの既定値について

単一コマンド / バッチモードで eShell を利用する場合の既定値は、オプションを指定した操作が無効に設定されています。このため、既定値で利用できる操作は、オプションを指定することなく利用できる「guide」「help」「about」などの一部コマンドの実行や指定コンテキスト内にあるコマンドの表示に限定されます。オプションを指定した操作を単一コマンド / バッチモードで利用できるようにするには、次ページの手順を参考にしてこの機能の利用を有効に設定する必要があります。

eShell ▸▸ オプション設定

9-4 単一コマンド / バッチモードのオプション設定を有効にするには

Windows のコマンドプロンプトから利用する単一コマンド / バッチモードの既定値は、オプションを指定できません。この機能を有効にするには、以下のコマンドを対話モードで実行します。

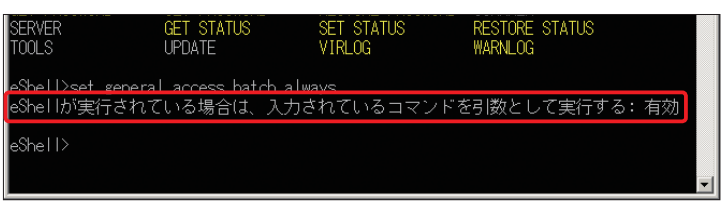


1

101ページの手順を参考にeShellの操作ウィンドウを開きます。[eShell>] と表示されたプロンプトに [set general access batch always] と入力し、[Enter] キーを押します。

2

単一コマンド / バッチモードで引数やオプションを利用できるように設定が変更されます。



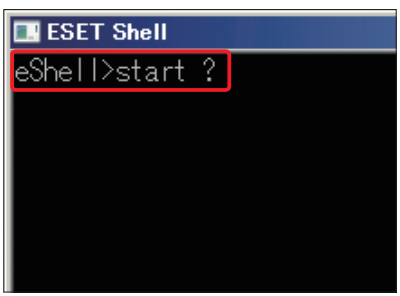
POINT

同様の操作は、[GENERAL] → [ACCESS] とコンテキストを移動し、[eShell general access>] と表示されたプロンプトから [set batch always] と入力して [Enter] キーを押すことでも設定できます。

9-5 eShell のヘルプの利用法

eShell では、本プログラムに関するさまざまな操作を行うため数多くのコマンドが準備されています。ここでは、eShell のヘルプの使い方を紹介します。

eShell 専用ウィンドウでヘルプを表示する❶～プレフィックス

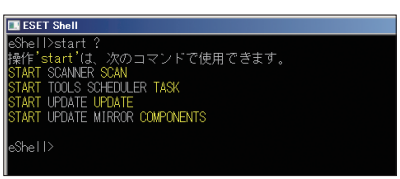


1

101ページの手順を参考に eShell の操作ウィンドウを開きます。プレフィックスのヘルプを表示したいときは、[[プレフィックス名] ?] と入力し、[Enter] キーを押します。ここでは、例として [START] プレフィックスのヘルプを表示します。[start ?] と入力し、[Enter] キーを押します。

POINT

eShell で利用できるプレフィックスについては、115 ページをご参照ください。



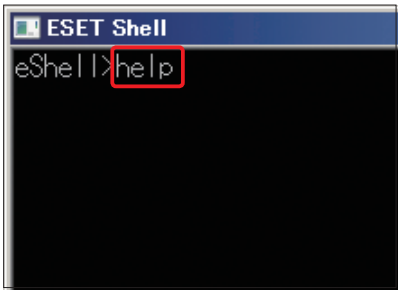
2

指定したプレフィックス（ここでは、[START] プレフィックス）のヘルプが表示されます。

POINT

同様の操作は、[[プレフィックス名] help] と入力することでも行えます。上記の例の場合は、[start help] とすると [START] プレフィックスのヘルプが表示されます。

eShell 専用ウィンドウでヘルプを表示する❷～コンテキスト

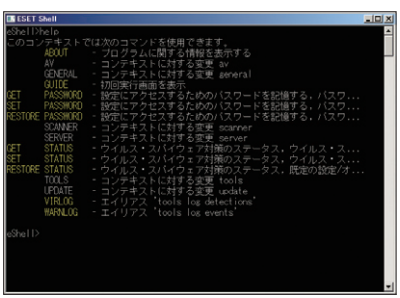


1

101ページの手順を参考に eShell の操作ウィンドウを開きます。現在のコンテキストで利用できるコマンドなどのヘルプを表示したいときは、[help] また [?] と入力し、[Enter] キーを押します。

POINT

ここでは、[eShell>] プロンプトで実行しているので、ルートで利用できるコマンドなどのヘルプが表示されます。



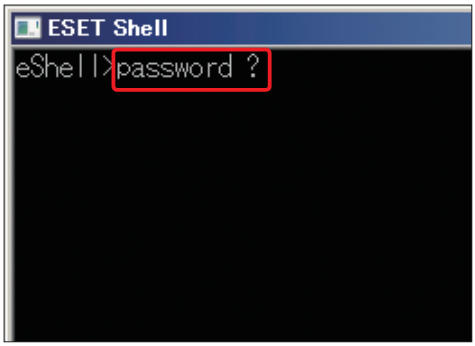
2

現在のコンテキストで利用できるコマンドなどのヘルプが表示されます。

POINT

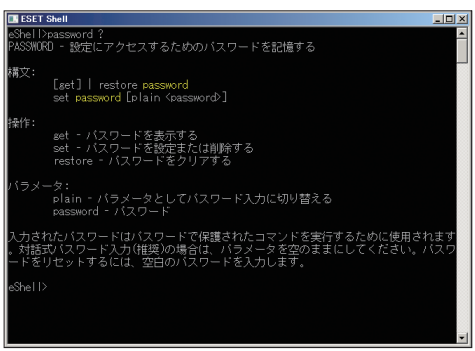
同様の操作は、[[コンテキスト名] help] と入力することでも行えます。上記の例の場合は、[help] とするとルートのコンテキストのヘルプが表示されます。

eShell 専用ウィンドウでヘルプを表示する❸〜コマンド



1

101ページの手順を参考にeShellの操作ウィンドウを開きます。コマンドのヘルプを表示したいときは、［［コマンド名］?］と入力し、［Enter］キーを押します。ここでは、例として［PASSWORD］コマンドのヘルプを表示します。［password ?］と入力し、［Enter］キーを押します。



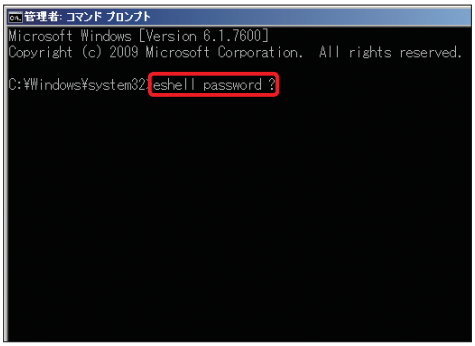
2

指定したコマンド（ここでは、［PASSWORD］コマンドのヘルプが表示されます。

POINT

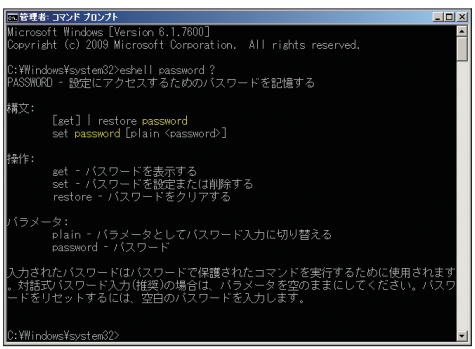
同様の操作は、［［コマンド名］help］と入力することでも行えます。上記の例の場合は、［password help］とすると［PASSWORD］コマンドのヘルプが表示されます。

単一コマンド / バッチモードでヘルプを表示する



1

107ページの手順を参考にコマンドプロンプトを開きます。コマンドのヘルプを表示したいときは、[eshell [コマンド名] ?] と入力し、[Enter] キーを押します。ここでは、例として [PASSWORD] コマンドのヘルプを表示します。[eshell password ?] と入力し、[Enter] キーを押します。



2

指定したコマンド(ここでは、[PASSWORD] コマンドのヘルプが表示されます。

POINT

同様の操作は、[eshell [コマンド名] help] と入力することでも行えます。上記の例の場合は、[eshell password help] と入力しても [PASSWORD] コマンドのヘルプが表示されます。また、コンテキストのヘルプを表示したいときは、[eshell [コンテキスト名] ? (または [help])] と入力します。プレフィックスのヘルプを表示したいときは、[eshell [プレフィックス名] ? (または [help])] と入力します。

コラム

eShell で利用できるプレフィックス一覧

ここでは、eShell で利用できるプレフィックスの一覧を紹介します。実際に利用する場合は、本プログラムのヘルプや eShell で表示されるヘルプなども併せてご参照ください。

■ プレフィックス一覧

GET	現在の設定 / 状態を表示します
SET	値 / 状態を設定します
SELECT	項目を選択します
ADD	項目を追加します
REMOVE	項目を削除します
CLEAR	すべての項目 / ファイルを削除します
START	アクションを開始します
STOP	アクションを停止します
PAUSE	アクションを中断します
RESUME	アクションを再開します
RESTORE	既定の設定 / オブジェクト / ファイルを復元します
SEND	オブジェクト / ファイルを送信します
IMPORT	ファイルからインポートします
EXPORT	ファイルにエクスポートします

POINT

プレフィックスは、実行する操作内容となります。たとえば、「GET」プレフィックスは、特定の機能の設定内容が表示されるか、ステータスが表示されます。なお、どのプレフィックスをサポートするかはコマンドによって異なります。