ESET Smart Security V4.2
ESET NOD32 Antivirus V4.2
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、本プログラムの基本的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。

スタートアップガイドをご覧いただいたうえでこちらをお読みください。

■本書について

- 本書は２種類のプログラムである「ESET Smart Security V4.2」と「ESET NOD32アンチウイルス V4.2」共通のガイドとしてまとめています。節番号下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 Smart Security V4.2」は ESS アイコン、「ESET NOD32アンチウイルス V4.2」は EAV アイコンです。掲載画面は「ESET Smart Security V4.2」を利用しています。「ESET NOD32アンチウイルス V4.2」をご利用のお客様は、実際の画面と異なる場合があります。ご容赦ください。

■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度押すことを「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度押すことを「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。
- Microsoft、Windows、Windows Vista、Outlook、Windows Live、Internet Explorer、Excelは、米国 Microsoft Corporationの米国およびその他の国における登録商標です。
- ESET、ESET Smart Security、NOD32、ThreatSenseは ESET, LLCならびに ESET s.r.o.の商標または登録商標です。本プログラムの著作権は、ESET s.r.o.に帰属します。本スタートアップガイドの著作権は、キヤノン ITソリューションズ株式会社に帰属します。その他の製品名および社名などは、各社の商標または登録商標です。

ESET Smart Security V4.2 / ESET NOD32アンチウイルス V4.2

設定ガイド●目次●

Part.4 「アップデート」画面での操作

Part.5 「設定」画面での操作 1
（ウイルス・スパイウェア対策編）

Part.6 「設定」画面での操作 2 （ファイアウォール編）

Part.7 「設定」画面での操作 3 （迷惑メール対策編）

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

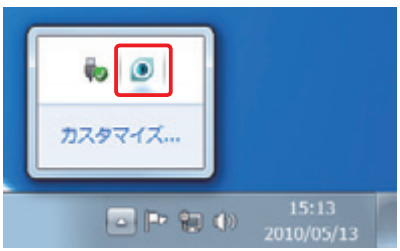
00013

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

EAV ESS

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。最初はこの通知領域アイコンの操作から学びます。

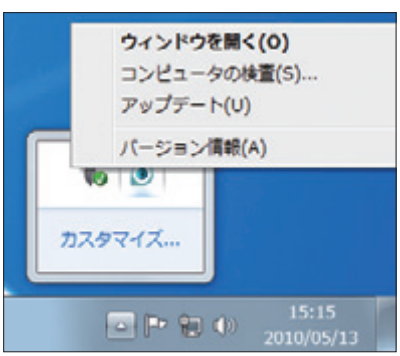
■ 通知領域アイコンと基本画面



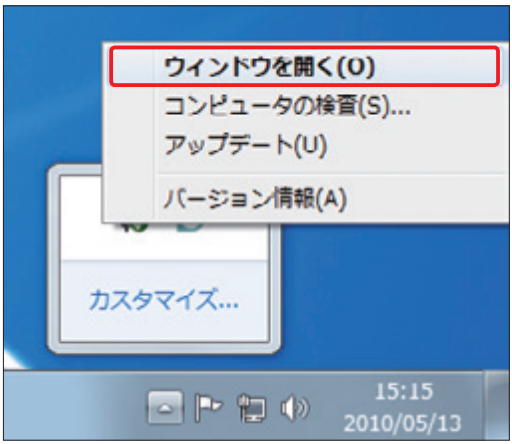
① 本プログラムのアイコンは、Windows へのログオン後に、通知領域に表示されます。本プログラムの動作を変更するには、同アイコンをクリックします。

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

基本画面を表示する手順は次の通りです。通知領域のアイコンをクリックし、表示されるメニューから［ウィンドウを開く］をクリックします。

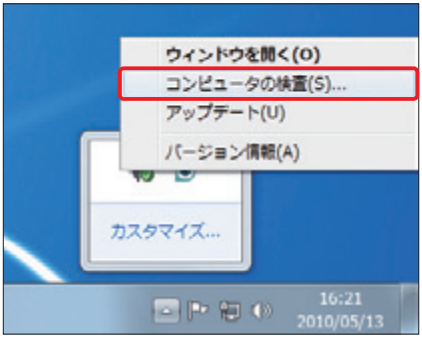
4

基本画面が表示されます。

POINT

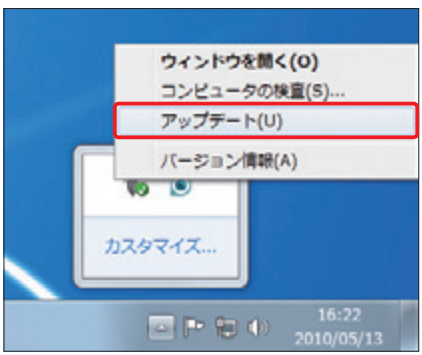
基本画面はアイコンをダブルクリックすることでも表示させることができます。

■ 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。

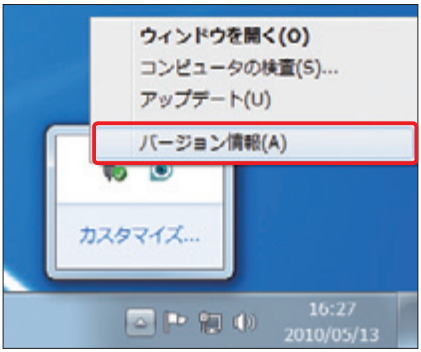


2

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、アップデートが始まります。

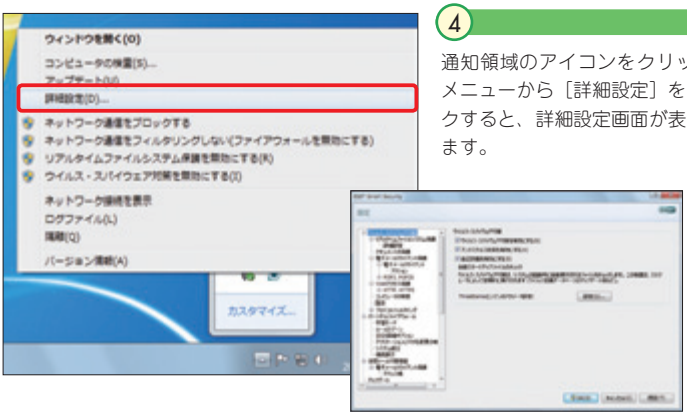
CAUTION

画面は「標準モード」時のものです。画面モードの切り替え方法については、12 ページをご覧ください。



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。

CAUTION

画面は「詳細モード」時のものです。画面モードの切り替え方法については、12 ページをご覧ください。

POINT

［ネットワーク通信をブロックする］［ネットワーク通信をフィルタリングしない］［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。また、［ネットワーク接続を表示］［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。

標準モードと詳細モード ▸▸ 操作方法

00014

1-2 画面モードを切り替えるには

EAV ESS

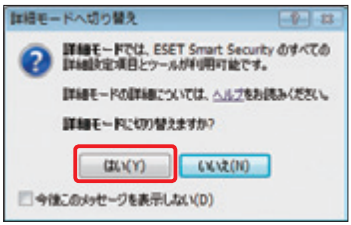
本プログラムでは「標準モード」「詳細モード」の２種類のモードが用意されています。前者は基本的な機能に関する操作を行い、後者は本プログラムの詳細機能を操作するモードです。最初に各モードの切り替え方法を紹介します。

■ 標準モードから詳細モードへ

① 基本画面の左下にあるステータスバーには、現在のモードが表示されています。[変更]をクリックします。

POINT

本プログラムの既定値は「標準モード」です。「詳細モード」に変更すると「メニューバー」および「ツール」ボタンが表示されます。ツールではログファイルの確認やスケジュール設定などが容易に行えます。

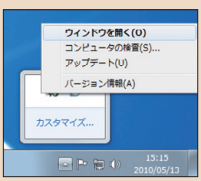


2

「詳細モードへ切り替え」画面が表示されます。［はい］をクリックします。

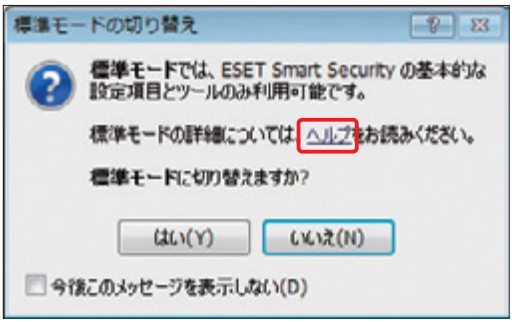
POINT

標準モードに設定すると、通知領域に表示されている本プログラムのアイコンをクリックした場合、表示内容が右図のように変わります。詳細モード時の表示画面は、11 ページをご覧ください。



3

①～②の手順で「詳細モード」に切り替わります。



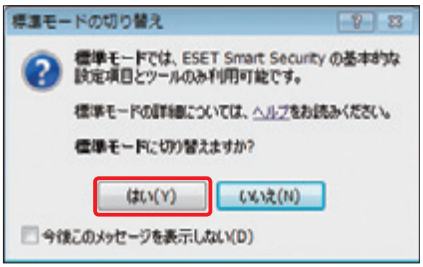
4

「詳細モードへ切り替え」画面（もしくは「標準モードへ切り替え」画面）の［ヘルプ］をクリックすると、操作方法に関するヘルプが表示されます。

■ 詳細モードから標準モードへ　その①

1

本プログラムの基本画面で、ステータスバーの［変更］をクリックします。



2

「標準モードの切り替え」画面が表示されます。［はい］をクリックします。

■ 詳細モードから標準モードへ　その②

1

「標準モード」に切り替えるには、❶メニューバーの［ユーザーインタフェース］をクリックし、表示されたメニューから、❷［詳細モード］をクリックすることでも行えます。

POINT

メニューバーの[ユーザーインタフェース] にある[ウィンドウレイアウトのリセット] を選択することで、変更したウィンドウレイアウトを既定値に戻すことができます。

詳細モード ▸ 各機能

00015

1-3 各機能を確認するには

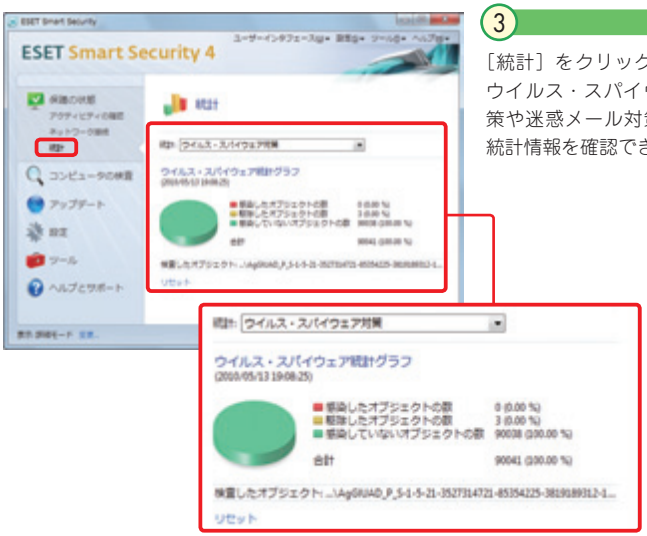
EAV ESS

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 詳細モードでは［保護の状態］ボタンに、３つの項目が用意されています。［アクティビティの確認］をクリックすると、ファイルシステムやネットワークの活動状況などを確認できます。

② ［ネットワーク接続］をクリックすると、パーソナルファイアウォールの状態を確認できます。監視している各モジュールが接続しているIPアドレスやデータ転送容量を確認できます。



3

［統計］をクリックすると、ウイルス・スパイウェア対策や迷惑メール対策機能の統計情報を確認できます。

POINT

［統計］のプル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。

■ コンピューターの検査

1

［コンピュータの検査］ボタンはウイルスチェック時に使用します。同ボタンからは、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

［アップデート］ボタンにある［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更新できます。また、アップデートがうまく行なわれない場合は［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

詳細モードでは［設定］ボタンに、３つの項目が用意されています。［ウイルス・スパイウェア対策］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」、ウェブページ閲覧時のウイルス侵入を防ぐ「Web アクセス保護」といった各保護機能の状態を確認・変更できます。なお、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」の項目が表示される場合もあります。

2

［パーソナルファイアウォール］では、ネットワーク通信フィルタリングや、フィルタリングモードの設定を行えます。

3

［迷惑メール対策機能］では、迷惑メール対策の設定を行えます。同機能の有無を、［無効にする］または［有効にする］をクリックすることで切り替えることができます。また、誤認識する場合は［ユーザーのホワイトリスト］をクリックして電子メールアドレスやドメインの登録を行いましょう。

ツール

1

詳細モードでは、[ツール] ボタンに、4つの項目が用意されています。ウイルスの検出などのログを確認するには、[ログファイル] をクリックします。「検出された脅威」「イベント」「コンピュータの検査」「パーソナルファイアウォールのログ」の4種類のログを確認できます。

POINT

画面のように [ツール] ボタンが表示されていないときは、12ページを参考に「詳細モード」への切り替えを行ってください。

2

[隔離] では、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（P.127 参照）。

3

［スケジューラ］では、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。

4

［SysInspector］では、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等の情報を保存しておき、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。

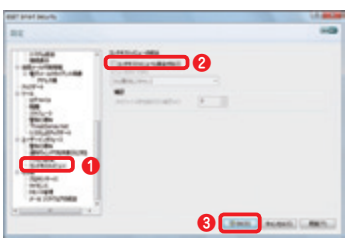
コラム

■ コンテキストメニューから項目を非表示にするには

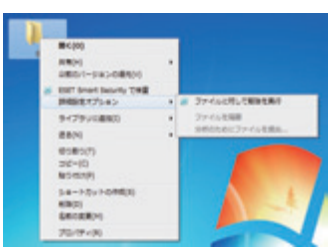
コンテキストメニューとは、ファイル・フォルダなどを右クリックして表示されるメニューのことですが、これを非表示にすることもできます。たとえば複数人でパソコンをお使いで、他の人に操作をしてほしくないときなど、設定しておくとよいでしょう。非表示にするための設定は次の通りです。

1 12 ～ 13 ページを参考に画面モードを「詳細モード」に切り替えます。

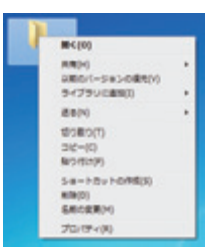
2 ❶［設定］ボタンをクリックし、❷［詳細設定のツリー全体を表示する］をクリックします。



3 ❶［ユーザーインタフェース］の［コンテキストメニュー］をクリックし、❷［コンテキストメニューに統合する］のチェックを外し、❸［OK］ボタンをクリックします。以上で設定は終了です。



設定前



設定後

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

00016

2-1 コンピューターの保護の状態を確認するには

EAV ESS

既定値の設定では、コンピューターは最大限に保護されています。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。

■ ウイルス対策機能を確認・有効にするには

❶

タスクから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、すべての対策機能が有効になった通常状態です。

❷

ウイルス・スパイウェア対策機能が無効になっていると❶❷画面のような警告が表示されます。

3

ウイルス・スパイウェア対策を有効にするには、［ウイルス・スパイウェア対策のすべての機能を開始する］をクリックします。これで機能が有効になり、手順②の警告も表示されなくなります。

■ 電子メール保護機能を確認・有効にするには

1

電子メール保護機能が無効になっていると❶❷画面のような警告が表示されます。

2

電子メール保護機能を有効にするには、[電子メール保護を有効にする]をクリックします。これで機能が有効に戻り、手順①の警告も表示されなくなります。

■ Web アクセス保護機能を確認・有効にするには

1

Web アクセス保護機能が無効になっていると❶❷画面のような警告が表示されます。

2

Web アクセス保護機能を有効にするには、［Web アクセス保護を有効にする］をクリックします。これで Web アクセス保護機能が有効に戻り、手順①の警告も表示されなくなります。

ESS

■ パーソナルファイアウォール機能を確認・有効にするには

1

パーソナルファイアウォール機能が無効になっていると❶❷画面のような警告が表示されます。

2

パーソナルファイアウォール機能を有効にするには、［フィルタリングモードを有効にする］をクリックします。これでパーソナルファイアウォール機能が有効に戻り、手順①の警告も表示されなくなります。

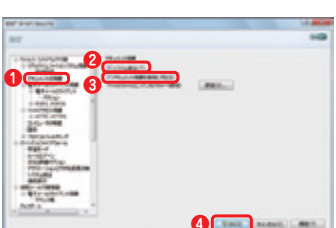
コラム

■ 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

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードに切り替えます。❶タスクの［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

設定画面が開いたら、❶左のツリーから［ドキュメントの保護］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。

保護の状態 ▸▸ 感染ファイル

00017

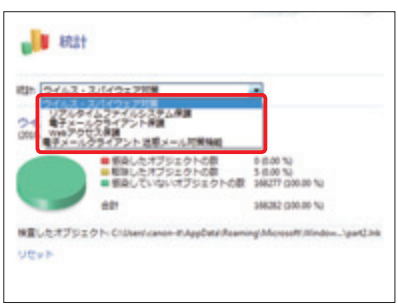
2-2 検出したウイルスの数や状況を確認するには

EAV ESS

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

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えます。❶タスクの［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］のプル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・スパイウエア対策」「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」「電子メールクライアント迷惑メール対策機能」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。

POINT

画面のように「保護の状態」下に項目が表示されない場合は、12 ページを参考に「詳細モード」への切り替えを行ってください。

保護の状態 ▸▸ ファイアウォール

00018

2-3 ESS パーソナルファイアウォールの詳細な通信状態を確認するには

パーソナルファイアウォールの通信状態は、「保護の状態」の「ネットワーク接続」で確認できます。

1

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えます。❶タスクの「保護の状態」ボタンをクリックし、❷［ネットワーク接続］をクリックします。

POINT

画面のように「保護の状態」下に項目が表示されない場合は、12 ページを参考に「詳細モード」への切り替えを行ってください。

2

コンピューター上でネットワーク接続を行っているプロセス（アプリケーション）の一覧が表示されます。詳細情報を確認するには、［＋］ボタンをクリックします。

3

プロセス（アプリケーション）の状態（リッスン中など）や使用プロトコル、通信速度、総転送量を確認できます。

4

UDP の接続情報を確認するには、❶項目を右クリックし、❷表示されるメニューから［TCP 接続のみを表示］を選択してチェックを外します。（すでに外れている場合は上記の操作は不要です）

5

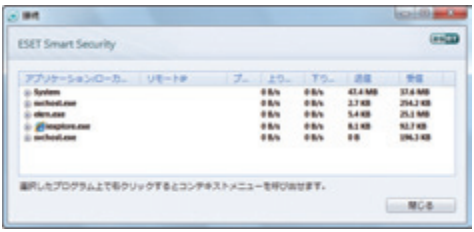
TCP に加えて UDP の接続情報も表示されます。

6

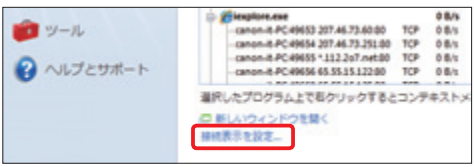
接続情報の表示は IP アドレスからホスト名の表示に切り替えることが可能です。❶項目を右クリックし、❷表示されるメニューから［ホスト名を解決］を選択してチェックを入れます。これで各ホスト名が表示されます。

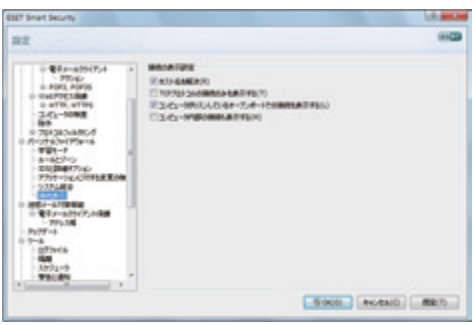
コラム

■ 通信状態の監視と接続表示の設定について



手順⑥の画面にある［新しいウィンドウを開く］をクリックすると、通信状態を別ウィンドウで開くことができます。





手順④や⑥で行った変更は、次の手順でも行うことができます。手順②から手順⑥の画面下段にある［接続表示を設定 ...］をクリックすると表示設定画面が表示されるので、変更したい項目のチェックをオン（またはオフ）にし、［OK］ボタンをクリックします。

POINT

［既定］ボタンをクリックすると、各項目が既定値に戻ります。設定変更後に意図しない動作が発生する時にご使用ください。

保護の状態 ▸ 迷惑メール

00019

2-4 ESS 迷惑メール対策機能の動作を確認するには

ESET Smart Security の迷惑メール対策機能によって分類されたメールを確認するには「電子メールクライアント迷惑メール対策機能」を開きます。

1

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えます。❶タスクの「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。

POINT

画面のように「保護の状態」下に項目が表示されない場合は、12 ページを参考に「詳細モード」への切り替えを行ってください。

2

❶［統計］のプルダウンボタンをクリックし、❷表示されるメニューから［電子メールクライアント迷惑メール対策機能］をクリックします。

3

ここでは、本プログラムがインストールされてからの情報が表示されます。

コラム

■迷惑メールの統計上のリセットについて

1

迷惑メールの統計情報をリセットしたいときは、❶［リセット］をクリックします。

2

ダイアログが表示されたら、❷［はい］ボタンをクリックします。統計情報がリセットされます。

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

00020

3-1 EAV ESS ハードディスクのウイルス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「ローカルディスクの検査」を行う手順を説明します。

1

1-1 を参考に基本画面を開き、タスクの［コンピュータの検査］ボタンをクリックします。

2

表示内容が「コンピュータの検査」に切り替わったら、［Smart検査］をクリックします。

3

ウイルス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しょう。

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。また、デスクトップなどにある単独のファイルやフォルダを検査する場合は、ファイルなどを右クリックし、表示されるメニューから[ESET Smart 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

00021

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

EAV ESS

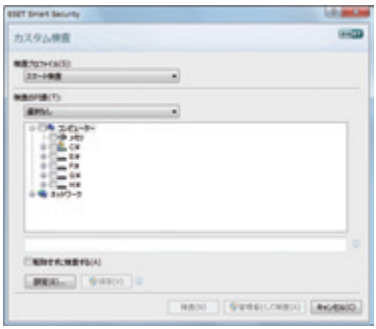
特定のフォルダやネットワーク上の共有フォルダを対象にウイルス検査を行うには「カスタム検査」を実行します。

1

1-1 を参考に基本画面を開き、タスクの［コンピュータの検査］ボタンをクリックします。

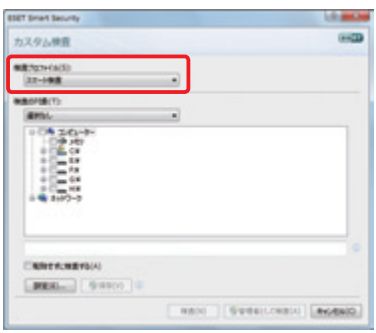
2

「コンピュータの検査」に表示が切り替わったら、［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。

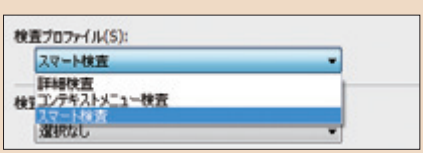


4

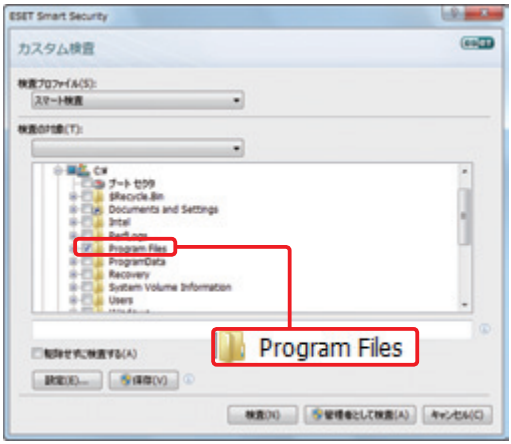
プロファイルの選択を行います。既定値では「スマート検査」が設定されています。そのほか、「詳細検査」「コンテキストメニュー検査」の項目が用意されています。使用するプロファイルをドロップダウンリストから選んでください。

POINT

手順④で選択できるプロファイル内容は次のとおりです。

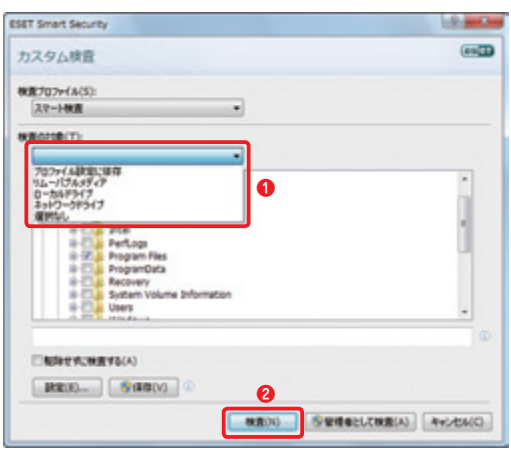


詳細検査：メモリも含めたすべてのファイルの検査が可能です。
コンテキストメニュー検査：コンテキストメニューから検査を行う場合に使用されます。
スマート検査：詳細設定と同様ですが、アーカイブファイル (ZIP 形式などで圧縮されたファイル) 内のファイルは対象に加えません。



5

今回は一例としてProgram Filesフォルダ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(ディレクトリ)が表示されたら、Program Filesのボックスをクリックしてチェックを入れてください。これで検査対象の設定は完了しました。



6

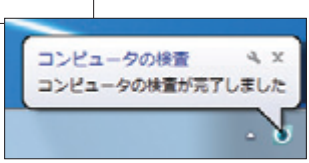
また、手順⑤の操作に代わって、カテゴリによって検査対象を選択することも可能です。❶「検査の対象」のドロップダウンリストからは「プロファイル設定に依存」「リムーバブルメディア」「ローカルドライブ」「ネットワークドライブ」の4種類が選択可能です。最後に❷［検査］ボタンをクリックします。

7

ウイルス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しょう。



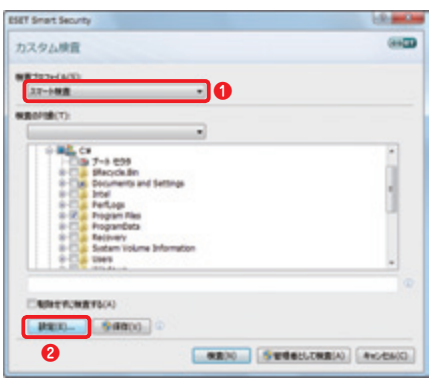
コンピューターの検査 ▸▸ カスタム検査

00022

3-3 カスタム検査の詳細設定を変更するには

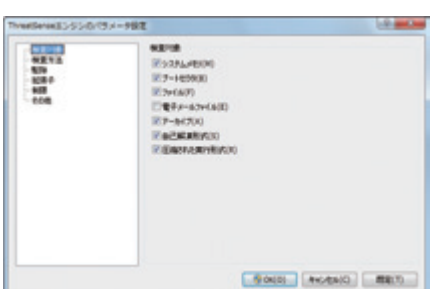
EAV ESS

カスタム検査は既定値で十分な効果を発揮するように設定済みですが、場面に応じて動作やウイルス検査内容を変更する手順を説明します。



1

3-2 の手順①、②を行い、検査対象やプロファイルを選ぶためのダイアログを表示します。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うことができます。

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

00023

4-1 EAV ESS 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更新したい方は、手動でアップデートを行うこともできます。

1

1-1 を参考に基本画面を開き、❶タスクの［アップデート］ボタンをクリックします。画面が切り替わったら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 エラーが発生するときは

アップデートが正常に行われないときは、更新サーバが一時停止しているか、更新サーバに接続する際のユーザー名とパスワードが間違っている可能性があります。後者の場合は 4-2 をご参照ください。

アップデート ▸▸ アップデート用ユーザー設定 00024

4-2 アップデート用のユーザー名とパスワードを入力・更新するには

EAV ESS

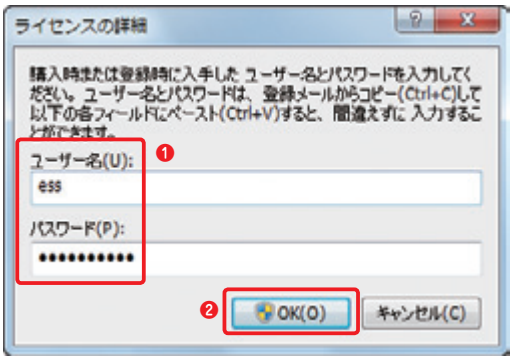
ユーザー名とパスワードの入力を求められてアップデートが失敗するときは、アップデート用のユーザー名およびパスワードが誤って入力されている可能性があります。

1

1-1 を参考に基本画面を開き、タスクの［アップデート］ボタンをクリックします。

2

画面が切り替わったら［ユーザー名とパスワードを入力］をクリックします。



3

「ライセンスの詳細」ダイアログが表示され、ユーザー名およびパスワードの入力が可能になります。❶誤って入力されている場合は、各入力欄に正しいユーザー名およびパスワードを入力して、❷[OK]ボタンをクリックします。

4

[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、アップデートが完了することを確認します。

アップデート ▸ アップデート自動実行

00025

4-3 アップデートをすべて自動で行うには

EAV ESS

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

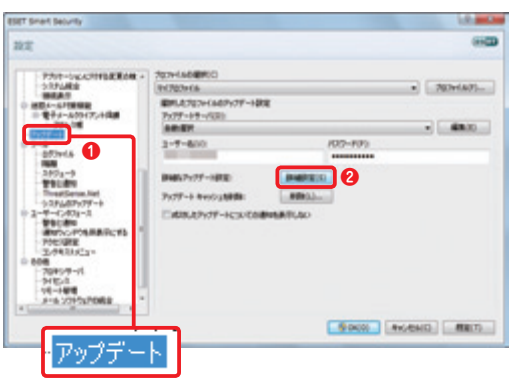
標準モードを「詳細モード」に切り替えます。1-1 を参考に基本画面を開き、❶ステータスバーの［変更］をクリックします。❷続いて［はい］ボタンをクリックします。

2

［設定］ボタンをクリックします。

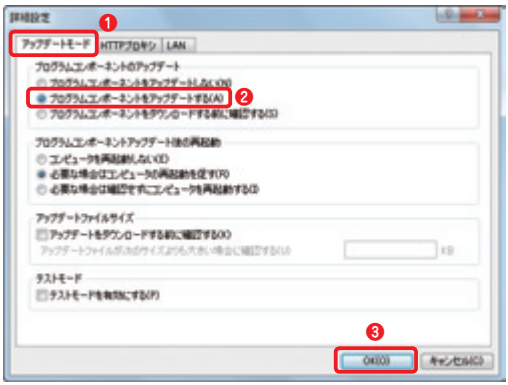
3

［詳細設定のツリー全体を表示する］をクリックして、設定画面を開きます。



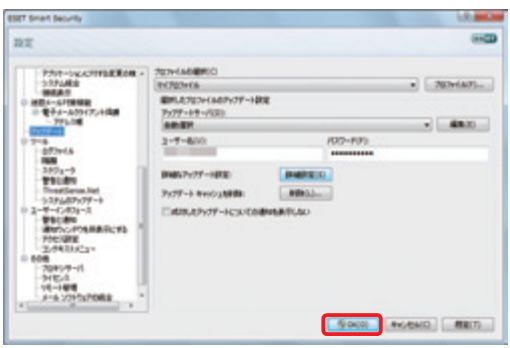
4

設定画面が開いたら、❶左のツリーから［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。



5

［詳細設定］ダイアログが表示されたら、❶［アップデートモード］タブにある❷［プログラムコンポーネントをアップデートする］をクリックしてチェックを入れ、❸［OK］ボタンをクリックします。



6

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。プログラムコンポーネントがアップデートされた場合、パソコンを再起動する必要がありますのでご注意ください。

CAUTION　アップデートの自動実行について

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 4-4 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。初期値では、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 00026

4-4 EAV ESS 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

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えます。❶タスクの［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1
（ウイルス・スパイウェア対策編）

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 00027

5-1 保護機能を一時的に無効にするには

EAV ESS

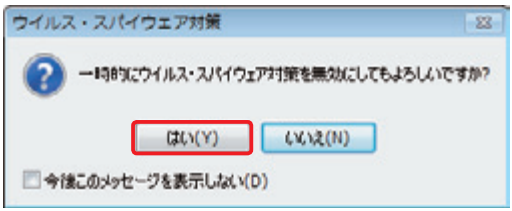
本プログラムが原因で問題が発生している可能性がある場合は、各機能を一時的に無効にしてみましょう。

1

1-1 を参考に基本画面を開き、1-2 を参考に「詳細モード」へ切り替えてから、❶タスクの［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］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

[保護の状態]ボタンをクリックし、警告が表示されていることを確認します。

設定 ▸▸ 除外拡張子の追加

00028

5-2 ウイルス検査をしない拡張子を設定するには

EAV ESS

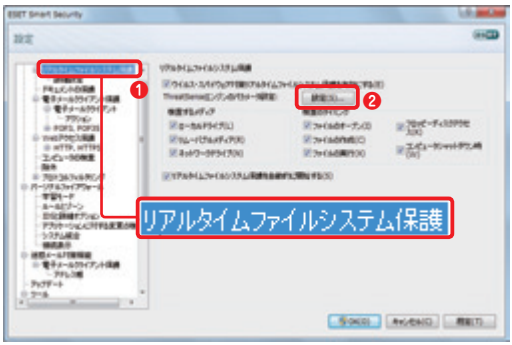
特定の拡張子をウイルス検査から除外するためには、対象となる拡張子を登録します。ウイルス検査に要する時間を短縮できます。

1

1-1 を参考に基本画面を開き、1-2 を参考に「詳細モード」へ切り替えてから、❶タスクの［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］をクリックします。

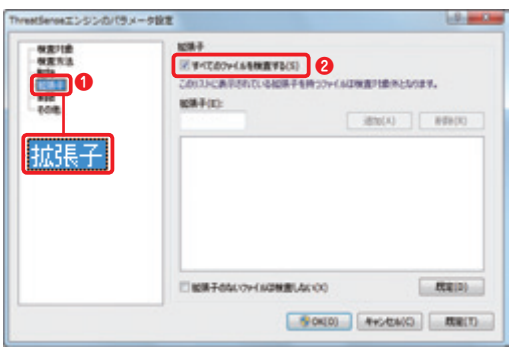
2

「リアルタイムファイルシステム保護」の［設定］をクリックし、設定画面を開きます。



3

左のツリー❶［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表示されます。❷［設定］ボタンをクリックします。

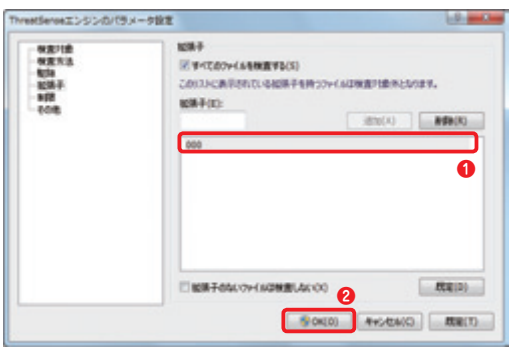


4

［ThreatSense エンジンのパラメータ設定］ダイアログが開きます。拡張子の編集を行なうため、❶［拡張子］をクリックします。続いて、❷「すべてのファイルを検査する」にチェックを入れます。

5

除外する拡張子を追加するには❶「拡張子」のフォームに任意の拡張子（画面の例では「000」）を入力し、❷［追加］ボタンをクリックします。



6

❶一覧に手順⑤で入力した拡張子が加わり、除外する拡張子が登録されます。最後に設定を有効にするため❷［OK］ボタンをクリックします。

設定 ▸ サイズと検査時間 00029

5-3 検査ファイルのサイズと時間を設定するには

EAV ESS

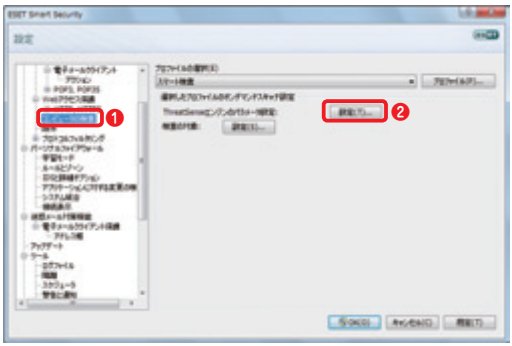
特定サイズ以上のオブジェクト（ファイル）をウイルス検査の対象から除外するには、検査を行うファイルの最大サイズを設定します。また、オブジェクト（ファイル）の最大検査時間も併せて設定すると検査時間を短縮できます。

1

1-1 を参考に基本ダイアログを開き、1-2 を参考に「詳細モード」へ切り替えてから、❶タスクの［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］をクリックします。

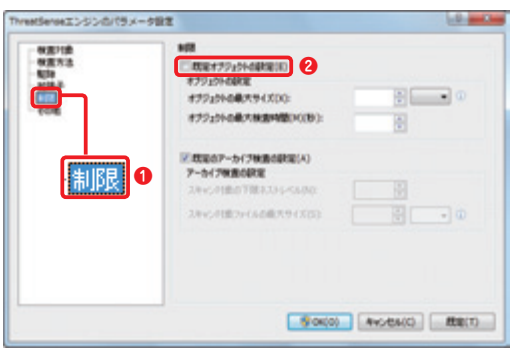
2

［コンピュータの検査の設定］をクリックします。



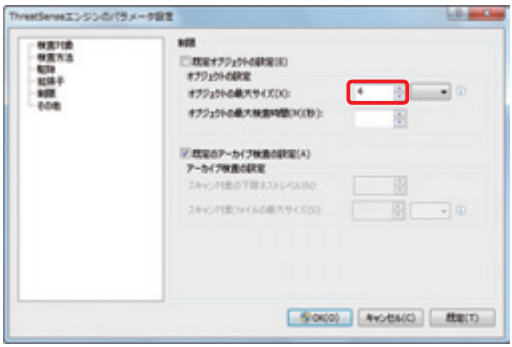
3

左のツリーに❶［コンピュータの検査］が選択された状態で設定画面が表示されます。❷［設定］ボタンをクリックします。



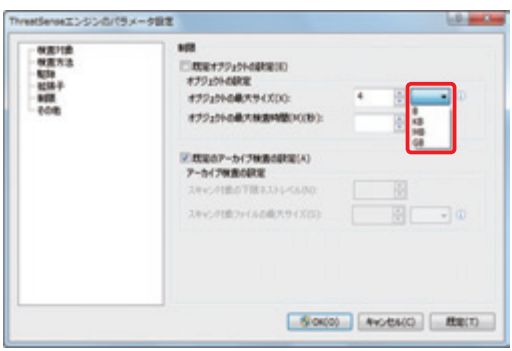
4

❶［制限］をクリックします。❷［既定オブジェクトの設定］のチェックを外します。



5

オブジェクト（ファイル）の最大サイズを設定します。設定したいサイズを入力します。

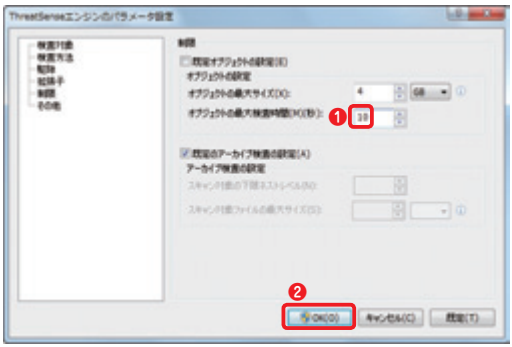


6

サイズの「単位」をプルダウンボタンをクリックして設定します。

POINT

この設定を行うと、設定したサイズ以下のオブジェクト（ファイル）を対象に検査が実行され、設定サイズより大きいオブジェクト（ファイル）の検査は実行されません。

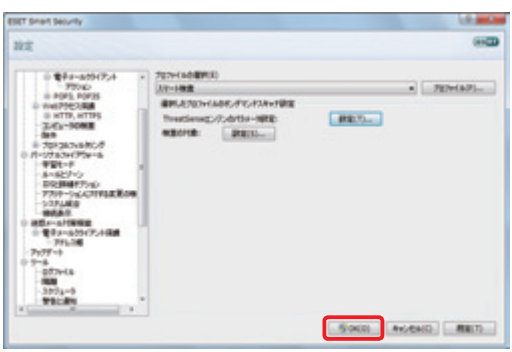


7

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。［ThreatSense エンジンのパラメータ設定］ダイアログを閉じます。

POINT

この設定は、オブジェクト(ファイル)の検査時間を秒単位で設定するものです。



8

設定ダイアログの［OK］ボタンをクリックし、設定ダイアログを閉じます。

設定 ▸ 階層の制限

00030

5-4 検査対象とする圧縮ファイルの階層を制限するには

EAV ESS

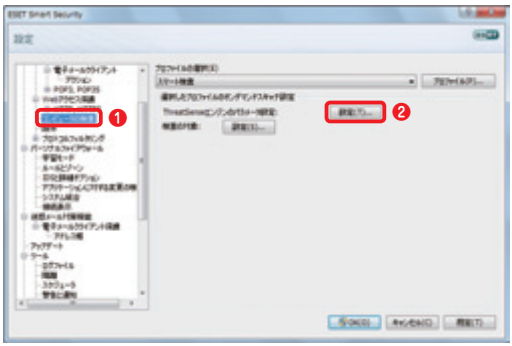
アーカイブ（圧縮）ファイルが階層的に納められている場合、検査を行う階層を制限することで、アーカイブファイルの検査時間を短縮できます。

1

1-1 を参考に基本画面を開き、1-2 を参考に「詳細モード」へ切り替えてから、❶タスクの［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］をクリックします。

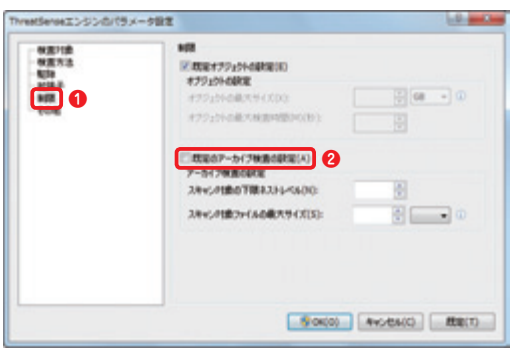
2

［コンピュータの検査の設定］をクリックします。



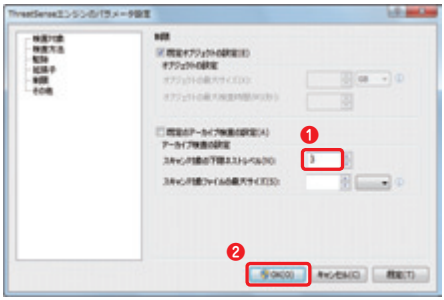
3

左のツリーに❶［コンピュータの検査］が選択された状態で画面が表示されます。❷［設定］ボタンをクリックします。



4

［ThreatSense エンジンのパラメータ設定］ダイアログが開きます。❶［制限］をクリックします。❷［既定のアーカイブ検査の設定］のチェックを外します。

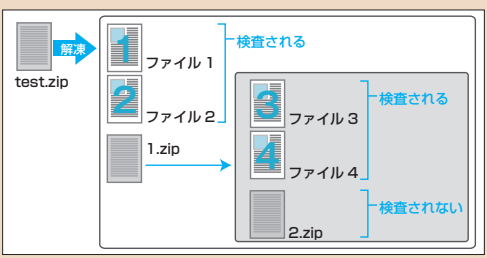


5

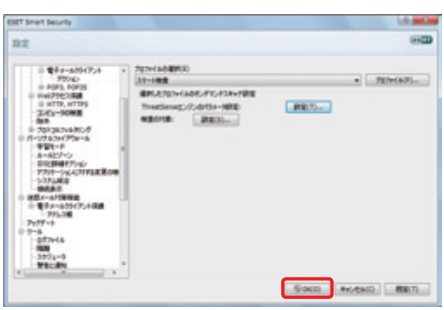
❶スキャン対象の下限ネストレベル（階層数）を入力します。
❷［OK］ボタンをクリックし、［ThreatSense エンジンのパラメータ設定］ダイアログを閉じます。

POINT

この設定を行うと、設定した階層数より下のアーカイブ（圧縮）ファイル内の検査が行われません。たとえば、スキャン対象の下限ネストレベル（階層数）を「2」に設定した場合に、test.zip というファイル内に 1.zip というアーカイブファイルが存在し、1.zip 内に 2.zip、2.zip 内に 3.zip と階層的にアーカイブファイルが納められたファイルの検査すると、test.zip および 1.zip を解凍して得られたファイルのみ検査が行われ、2.zip 内のファイル（3.zip 含む）の検査は行われません。



スキャン対象の下限ネストレベルを2に設定した場合



6

設定ダイアログの［OK］ボタンをクリックし、設定ダイアログを閉じます。

設定 ▸ 最大サイズの制限 00031

5-5 検査対象とする圧縮ファイル内のファイルの最大サイズを制限するには

EAV ESS

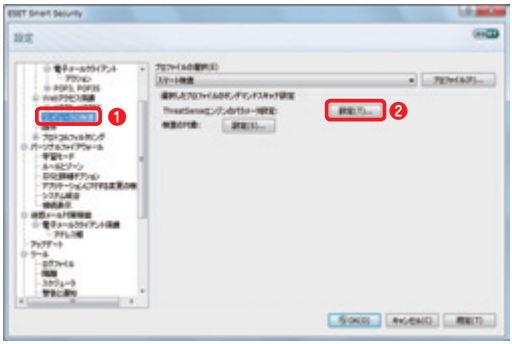
アーカイブ（圧縮）ファイル内のファイル検査を行う場合も、検査するファイルの最大サイズを設定できます。この設定を行うと、アーカイブファイルの検査時間を短縮できます。

1

1-1 を参考に基本画面を開き、1-2 を参考に「詳細モード」へ切り替えてから、❶タスクの［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］をクリックします。

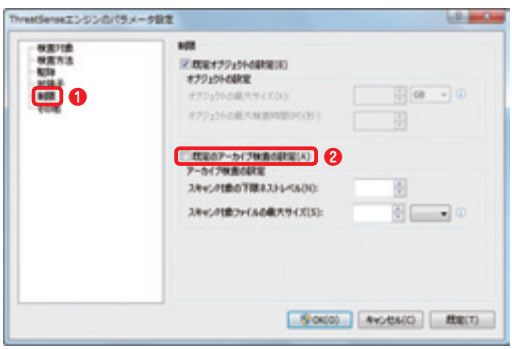
2

［コンピュータの検査の設定］をクリックします。



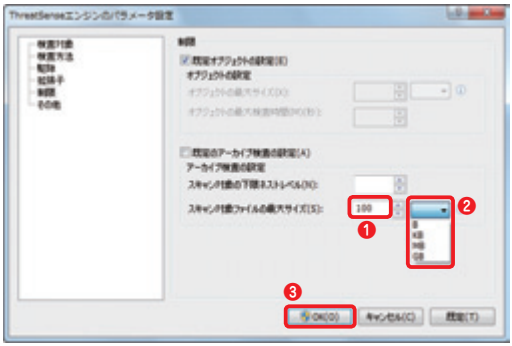
3

左のツリーに❶［コンピュータの検査］が選択された状態で設定画面が表示されます。❷［設定］ボタンをクリックします。



4

［ThreatSense エンジンのパラメータ設定］ダイアログが開きます。❶［制限］をクリックします。❷［既定のアーカイブ検査の設定］のチェックを外します。

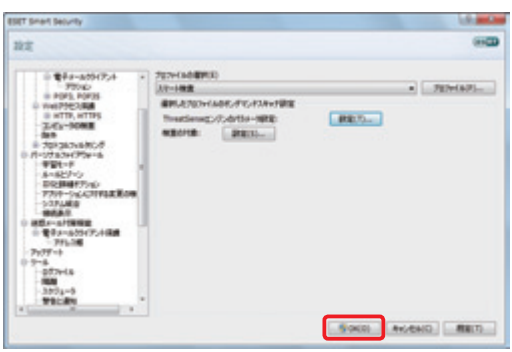


5

❶スキャン対象ファイルの最大サイズを入力します。❷サイズの「単位」をプルダウンボタンをクリックして設定します。❸［OK］ボタンをクリックし、［ThreatSense エンジンのパラメータ設定］ダイアログを閉じます。

POINT

この設定を行うと、アーカイブ（圧縮）ファイルを解凍して得られたファイルのサイズが、設定サイズ以下であるものを対象に検査を行います。解凍後のサイズが、設定サイズより大きい場合は、検査を行いません。



6

設定ダイアログの［OK］ボタンをクリックし、設定ダイアログを閉じます。

設定 ▸ 詳細設定

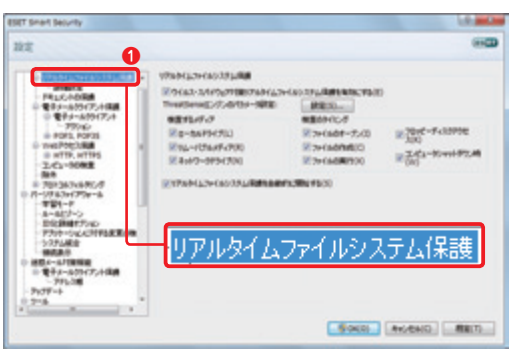
00032

5-6 EAV ESS ファイル / 電子メール /Web保護の詳細な設定を行うには

電子メール保護や Web 保護といった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

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えてから、❶タスクの［設定］ボタン、❷［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❸［設定］と順番にクリックします。



2

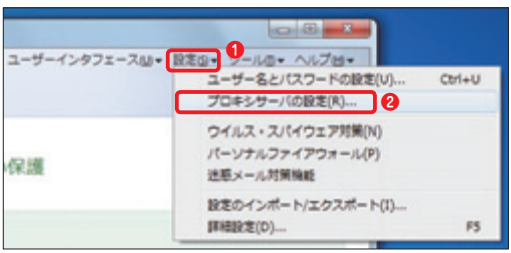
❶［リアルタイムファイルシステム保護］が選択された状態で設定画面が開きます。なお、手順①でドキュメント保護の［設定］、電子メールクライアント保護の［設定］、Web アクセス保護の［設定］をクリックした場合は、それぞれの詳細設定を行うことができます。

設定 ▸ プロキシサーバの設定 00033

5-7 プロキシサーバを設定するには

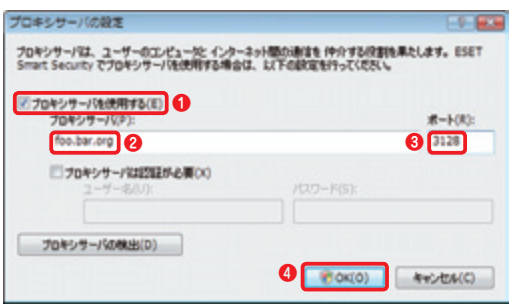
EAV ESS

プロキシサーバを経由してネットワーク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の設定が必要です。



①

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードに切り替えてから、メニューバーの❶［設定］をクリックし、表示されたメニューから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。最後に❹［OK］ボタンをクリックすれば設定完了です。

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を自動検出することができます。

設定 ▸ インポートとエクスポート 00034

5-8 詳細設定を保存・復元するには

EAV ESS

ここでは、詳細設定をファイルに出力し、保存・復元するための手順を紹介します。

① 1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えてから、❶タスクの［設定］ボタンをクリックします。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。

Part.6
「設定」画面での操作２
（ファイアウォール編）

ここでは、本プログラムの「設定」画面における「ファイアウォール」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 ▸▸ 通信の遮断 00035

6-1 ESS 緊急時にすべての通信を遮断するには

ウイルスの侵入やネットワーク経由の攻撃を発見した際には、パーソナルファイアウォールの機能を使って、通信の遮断を行いましょう。

1

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えてから、❶タスクの［設定］ボタンをクリックします。❷［パーソナルファイアウォール］、❸［すべてのネットワーク通信を遮断する］の順番にクリックします。

2

これで、❶［ネットワークフィルタリング］の状態が遮断に変化し、すべての通信が遮断されます。再度元の状態に戻すときは、❷［フィルタリングモードに切り替え］をクリックします。

設定 ▸▸ フィルタリングの無効化 00036

6-2 ESS パーソナルファイアウォールを無効にするには

パーソナルファイアウォールが原因で、ネットワーク経由のアクセスが正常に行われない場合は、一時的にパーソナルファイアウォールを無効にしましょう。ただし、保護されていない状態となることを重々ご承知ください。

1

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えてから、❶タスクの［設定］ボタンをクリックします。❷［パーソナルファイアウォール］、右画面にある ❸［フィルタリングをしない］の順番にクリックします。

2

これで、❶［ネットワーク通信フィルタリング］の状態が無効に変化し、パーソナルファイアウォールのフィルタリングが無効になります。再度元の状態に戻すときは、❷［フィルタリングモードへ切り替え］をクリックします。

設定 ▸▸ 保護モード　00037

6-3 ESS ネットワークコンピューターの保護モードを変更するには

本プログラムは、プログラムのセットアップ直後など新しいネットワークを検出した場合に保護モードの設定を行う必要があります。この設定をあとから変更したい場合は、以下の手順で実行します。

基本画面が標準モードに設定されている場合の保護モードの設定方法

①

1-1 を参考に基本画面を開き、❶タスクの［設定］ボタンをクリックし、❷［ネットワークコンピュータの保護モードを変更する］をクリックします。

②

設定画面が表示されたら、❶公共の場所で使用する場合は［厳密に保護］、家庭や会社内で使用する場合は［共有を許可］にチェックを入れ、❷［OK］ボタンをクリックします。

POINT

1 台のパソコンで無線 LAN と有線 LAN の両方を同時に使用している場合など、複数のアクティブなネットワークが検出された場合は、手順②の設定画面の前に［サブネット選択］ダイアログが表示されます。その場合は、設定を変更したいネットワークをクリックし、［次へ］ボタンをクリックします。また、保護モードを［厳密に保護］に設定すると、LAN 上に設定された共有パソコンなどが見えない状態に設定されます。家庭や会社内などでファイル共有やプリンタ共有を行う場合は、［共有を許可］に設定してください。

3

基本画面が詳細モードに設定されている場合は、❶タスクの［設定］→❷［パーソナルファイアウォール］ボタンとクリックし、❸［信頼されたゾーンの設定］をクリックします。画面が表示されたら手順②を参考に設定を行います。

POINT

パーソナルファイアウォールを「自動フィルタリングモード」以外のモードで使用している場合は、［ネットワークコンピュータでのコンピュータの保護モードの変更］をクリックします。

コラム

■ファイアウォールのフィルタリングモードについて

本プログラムのファイアウォールには、5 種類のフィルタリングモードが準備されています。それぞれのフィルタリングモードは、以下のような特徴があります。

フィルタリングモード	概要
自動モード	このモードは、ルールを定義せずに、ファイアウォールを容易に使用したいユーザーに適しています。このモードでは外向きの通信はすべて許可されますが、内向きの通信はすべて拒否されます。既定値では、このモードが選択されています。
例外付きの自動モード	このモードは、ユーザーが作成したカスタムルールを例外ルールとして使用できる自動モードです。 自動モードで使用しつつ、作成したカスタムルールも有効にしたいときに選択します。
対話モード	対話モードは、検出された通信に適合するルールがない場合に、その通信の許可 / 拒否をユーザーが選択できるモードです。決定した通信ルールは、次回以降使用するパーソナルファイアウォールの新規ルールとして登録したり、一時的な使用にとどめることもできます。
ポリシーベースモード	このモードでは、定義されていない通信すべてがブロックされる上級者向けのモードです。
学習モード	このモードは、パーソナルファイアウォールの初期設定に適したモードです。ほとんどの通信が許可され、通信を許可するルールを簡単に作成できます。ただし、学習モードでは、安全を確保できないため、常時使用には適していません。

設定 ▸▸ 信頼ゾーンの編集 00038

6-4 ESS パーソナルファイアウォールで「信頼ゾーン」を設定するには

信頼ゾーンは、家庭や会社内のネットワークなど信頼できるネットワークの設定です。通常、保護モード設定時に自動で最適な設定がなされますが、手動でこの設定を変更したい場合は、下記の手順を実行してください。

1

1-1 を参考に基本画面を開き、1-2 を参考に［詳細モード］に切り替えてから、タスクの［設定］ボタンをクリックします。

CAUTION 信頼ゾーンの設定について

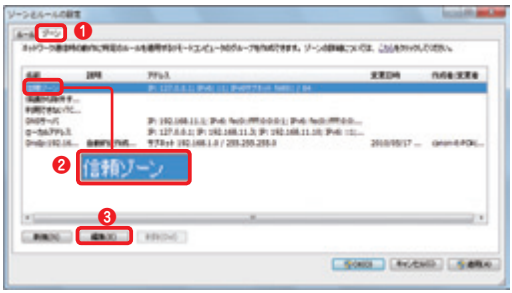
信頼ゾーンの編集は、「自動フィルタリングモード」以外のフィルタリングモードを使用している場合のみ行えます。［自動フィルタイングモード］を使用している場合は、他のフィルタリングモードに切り替えてから設定を行ってください。

2

❶［パーソナルファイアウォール］をクリックし、❷［ルールとゾーンの設定］をクリックします。

CAUTION 今回追加する信頼ゾーン

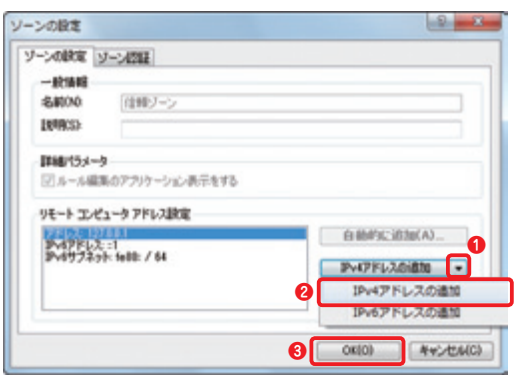
信頼ゾーンの編集では、単一の IP アドレスや任意のアドレス範囲を設定できますが、ここでは、「192.168.1.0/255.255.255.0］の範囲の登録を例に説明しています。



3

［ゾーンとルールの設定］ダイアログが表示されます。❶［ゾーン］タブをクリックし、❷［信頼ゾーン］を選択してから、❸［編集］ボタンをクリックします。信頼ゾーンを編集するダイアログが表示されます。以降の手順を参考に、信頼ゾーンを編集してください。

■ 信頼ゾーンを追加するには

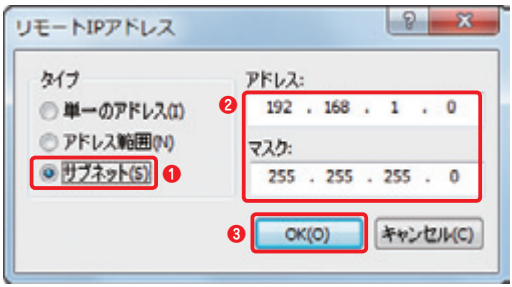


1

セットアップ時に登録された信頼ゾーンが表示されています。新たに信頼ゾーンを追加するため、❶［IPv4 アドレスの追加］のドロップダウンリストをクリックし、表示されるメニューから❷［IPv4 アドレスの追加］をクリック、❸［OK］ボタンをクリックします。

POINT

IPv6 のネットワーク環境をご利用の場合は、［IPv6 アドレスの追加］をクリックします。

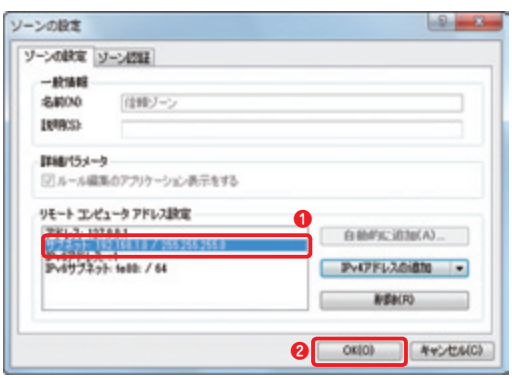


2

❶［サブネット］にチェックを入れ、❷「アドレス」に信頼ゾーンに追加したいネットワークアドレス（IP アドレス）を入力し、「マスク」にサブネットマスクを入力します。❸［OK］ボタンをクリックします。

POINT

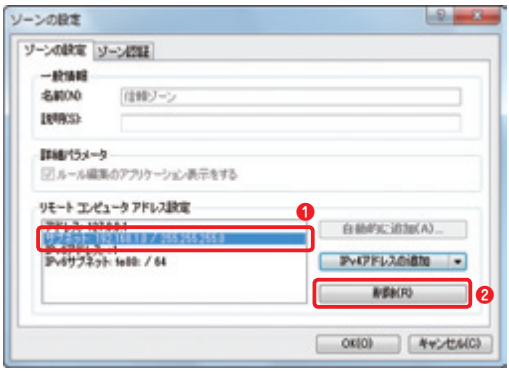
マスクの内容は自動的に入力されます。なお、1 つの IP アドレスを登録する場合は［単一のアドレス］を、IP アドレス範囲を登録する場合は［アドレス範囲］にチェックを入れてください。



3

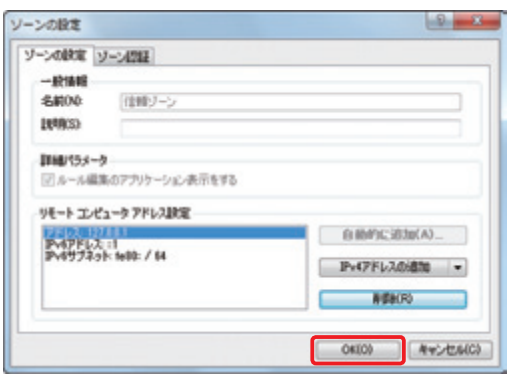
信頼ゾーンの登録が完了しました。上記手順②で追加したアドレスが、❶［リモートコンピュータアドレス設定］に表示されます。❷［OK］ボタンをクリックしてダイアログを閉じてください。

■ 信頼ゾーンを削除するには



1

登録した内容を削除するときは、❶削除したい項目をクリックし、❷［削除］ボタンをクリックします。



2

手順①で選択した項目が削除されました。［OK］ボタンをクリックしてダイアログを閉じてください。

設定 ▸▸ ルールの手動設定　00039

6-5 ESS パーソナルファイアウォールを「対話モード」で使うには

パーソナルファイアウォールの既定値は自動フィルタリングモードに設定されていますが、通信の可否を手動で行う「対話型フィルタリングモード」も用意されています。

1

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えてから、❶タスクの［設定］❷［パーソナルファイアウォール］ボタンをクリックし、❸［対話型フィルタリングモードへ切り替え］をクリックします。

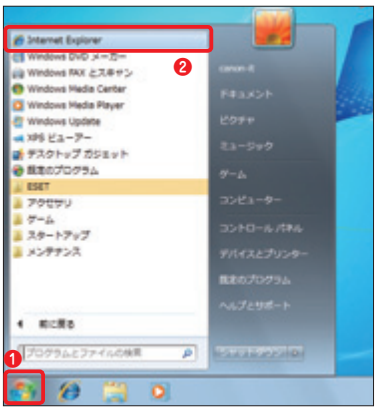
2

パーソナルファイアウォールのフィルタリング設定が「自動フィルタリングモード」から「対話型フィルタリングモード」に切り替わりました。

POINT

元に戻す時は［自動フィルタリングモードへ切り替え］をクリックします。

■ 対話モードの動作を確認する



1

ここでは、Internet Explorer を例として対話モードでの通信の許可方法を説明します。タスクバーにある Internet Explorer アイコンをクリックするか、❶［スタート］ボタンをクリックし、スタートメニューから❷ Internet Explorer を起動します。

2

Internet Explorer が通信を開始したことを示すダイアログが表示されます。通信を許可する場合は、❶［アクションを記憶する］にチェックを入れ、❷［許可］ボタンをクリックします。

POINT

「対話モード」使用時、「Generic Host Process for Win32 Services」が許可を求めてくる場合がありますが、これは Windows サービスの汎用ホストプロセス「Svchost.exe」です。特に問題がない場合は通信を許可することをお勧めします。

表示される

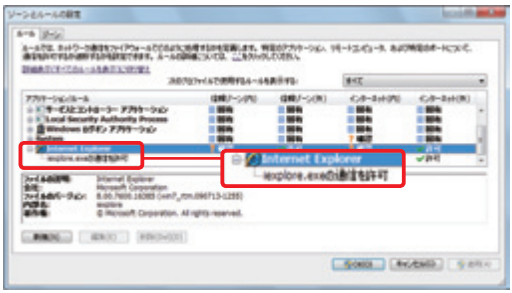
3

手順②のダイアログの左下にある［▼設定の表示］をクリックすると、拡張表示に切り替わります。拡張表示ではルールを作成する際のアプリケーション名や接続先、接続に用いるポートなどを個別に設定可能です。

■ ファイアウォールに設定されているルールを確認するには

1

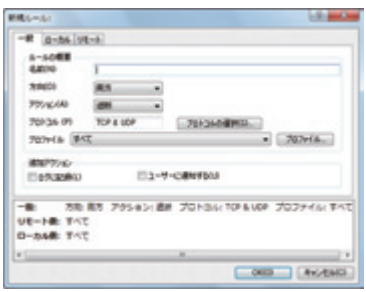
ESET Smart Security の基本画面でタスクの［設定］ボタン→［パーソナルファイアウォール］をクリックして表示を切り替えた状態で、［ルールとゾーンの設定］をクリックします。



2

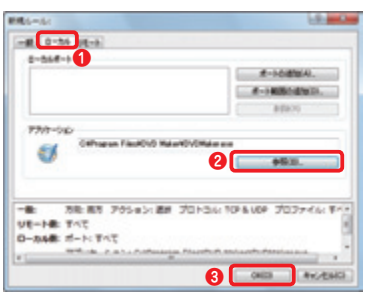
「ゾーンとルールの設定」ダイアログが表示され、ルールを確認することができます。

■ 新しいルールを作成する



1

新しいルールを作成するには上記手順②の画面にある［新規］ボタンをクリックして表示される「新規ルール」ダイアログから設定します。［一般］タブで、ルール名［名前］、データの流れを示す［方向］、通信の可否を指定する［アクション］を設定します。



2

❶［ローカル］タブをクリックし、❷アプリケーションを［参照］ボタンで参照し、❸［OK］ボタンをクリックすれば設定完了です。

POINT

ネットワーク接続を必要とするアプリケーションが、特定のポートを使用する場合、［ポートの追加］もしくは［ポート範囲の追加］ボタンから設定することができます。

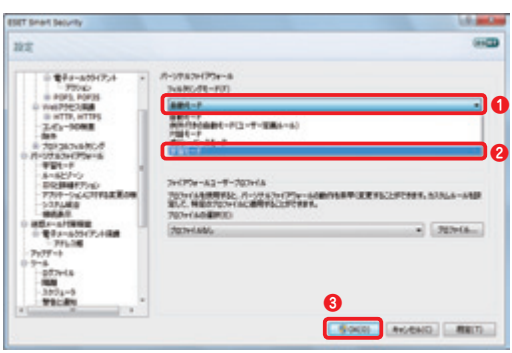
設定 ▸▸ 学習フィルタリングモード　00040

6-6 ESS パーソナルファイアウォールを「学習モード」で使うには

パーソナルファイアウォールのフィルタリングモードには、ルール作成ポリシーに基づいて、通信許可ルールを自動的に作成する「学習モード」が搭載されています。ここでは、その設定方法を説明します。

1

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えてから、❶タスクの［設定］ボタンをクリックします。❷［パーソナルファイアウォール］をクリックし❸［パーソナルファイアウォールの詳細設定］をクリックします。



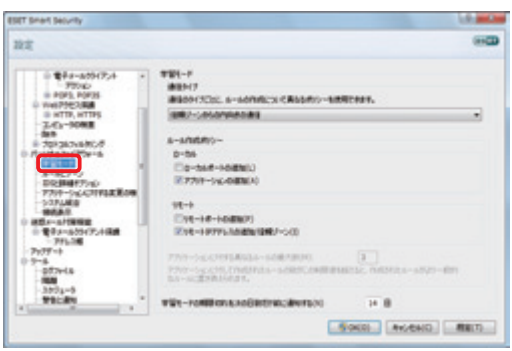
2

❶フィルタリングモードのプルダウンボタンをクリックし、❷［学習モード］を選択します。❸［OK］ボタンをクリックします。

③

パーソナルファイアウォールのフィルタリングモードの設定が、「学習フィルタリングモード」に切り替わりました。

■学習モードのルール作成ポリシーの設定方法



①

前ページの手順を参考に「パーソナルファイアウォールの詳細設定」ダイアログを開き、[学習モード]をクリックします。右画面に表示されている各学習モードでルール作成ポリシーなどを確認・設定できます。

POINT

「学習モード」の目的は、通信を許可するルールをできるだけ簡単に設定することです。「学習モード」では、ほとんどの通信が許可されます。そのため、「学習モード」を常時使用することは推奨されません。必要なプログラムが通信可能であることを確認後、「例外付きの自動モード」などに変更してください。

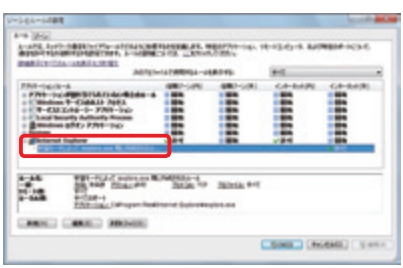
■学習フィルタリングモードのルール作成について

①

学習モードでは、InternetExporerなどの通信を利用するアプリケーションを使用すると、自動的にフィルタリングルールが作成されます。また、フィルタリングルールが作成された場合は、画面左下に通知画面が表示されどのようなファイアウォールルールが作成されたかを表示します。

コラム

■ 作成されたルールを確認するには



学習フィルタリングモードによって作成されたルールを確認したい場合は、1-1 を参考に基本画面を開き、1-2 を参考に「詳細モード」へ切り替えます。

❶［設定］ボタンをクリックし、❷［パーソナルファイアウォール］をクリックして、❸［ルールとゾーンの設定］をクリックします。「ゾーンとルールの設定」ダイアログが表示され、ルールを確認できます。

設定 ▸▸ ファイアウォールプロファイル 00041

6-7 ESS ファイアウォールプロファイルを作成するには

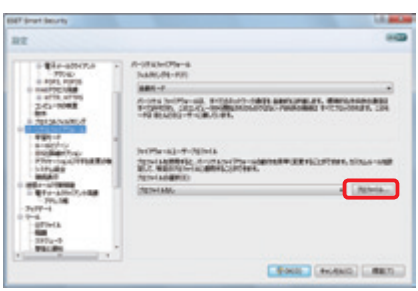
パーソナルファイアウォールの動作を素早く変更したいときは、プロファイルを使用します。プロファイルを作成しておくと、独自のカスタムルールを作成し、それを特定のプロファイルに適用できます。

1

1-1 を参考に基本画面を開き、❶タスクの［設定］の❷［パーソナルファイアウォール］ボタンをクリックし、❸［パーソナルファイアウォールの詳細設定］をクリックします。

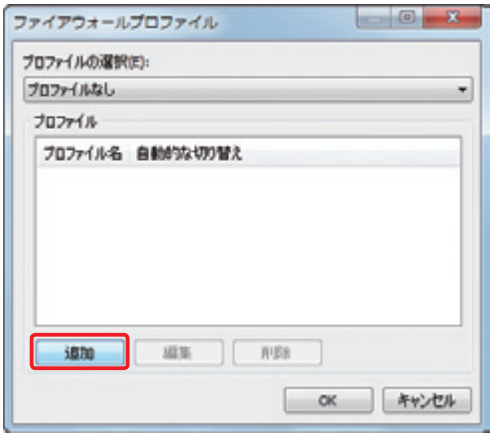
POINT

特定の通信向けに作成したカスタムルールの有効 / 無効を簡単に切り替えることができるのがプロファイルです。たとえば、ゲーム用に作成したカスタムルールを普段は無効にしておき、ゲームをするときだけ有効にするという場合などに使用できます。プロファイルは、いつでも手動で変更できるほか、特定の条件を満たすと自動的に変更するように設定することもできます。



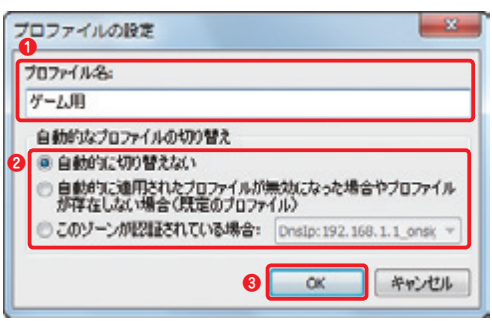
2

［パーソナルファイアウォール］が選択された状態で、ダイアログが開きます。［プロファイル］ボタンをクリックします。



3

［ファイアウォールプロファイル］ダイアログが開きます。［追加］ボタンをクリックします。

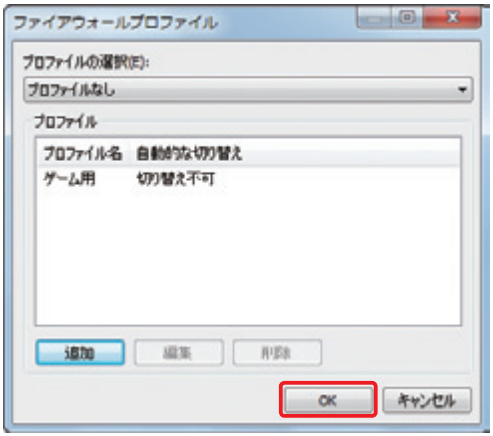


4

［プロファイルの設定］ダイアログが開きます。❶［プロファイル名］に作成したいプロファイルの名称を入力し、❷「自動的なプロファイルの切り替え」の設定を行い、❸［OK］ボタンをクリックします。

POINT

「自動的なプロファイルの切り替え」の既定値は、［自動的に切り替えない］に設定されています。［このゾーンが認証されている場合］を選択すると該当するゾーンのネットワークに接続した場合に自動でプロファイルが変更されます。

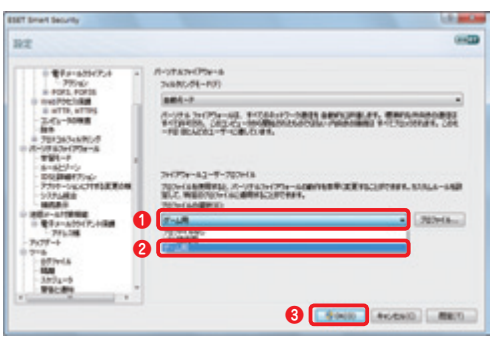


5

［ファイアウォールプロファイル］ダイアログに作成したプロファイルが登録されます。［OK］ボタンをクリックします。

POINT

複数のプロファイルを作成する場合は、手順③と手順④の作業を繰り返し行います。また、プロファイルをクリックし、［削除］ボタンをクリックするとプロファイルを削除できます。［編集］ボタンをクリックすると、作成済みプロファイルの内容を変更できます。



6

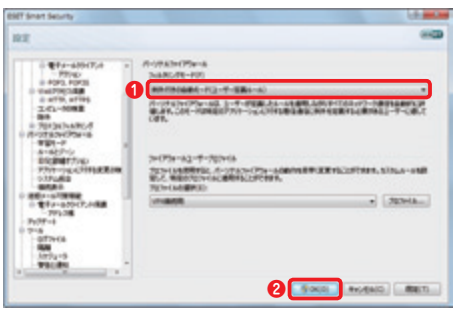
作成したプロファイルを使用する場合は、❶［プロファイルの選択］プルダウンボタンをクリックし、❷使用したいプロファイルを選択して、❸［OK］ボタンをクリックします。

設定 ▸▸ カスタムルール

00042

6-8 ESS パーソナルファイアウォールにカスタムルールを追加するには

ネットワークゲームなど通信を使用するアプリケーションは、パーソナルファイアウォールを使用していると動作しない場合があります。そのような場合は、手動でカスタムルールを登録します。



1

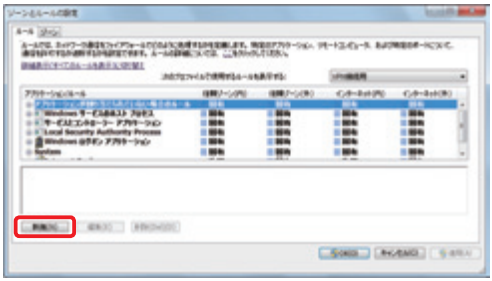
6-6 を参考にパーソナルファイアウォールを❶［自動モード］以外に設定し、❷［OK］ボタンをクリックします。

CAUTION カスタムルールの作成について

カスタムルールの作成は、「自動フィルタリングモード」では行えません。カスタムルールを作成する場合は、フィルタリングモードを「自動フィルタリングモード」以外に変更してください。また、作成したカスタムルールは、［自動フィルタリングモード］では適用されません。

2

基本画面から［ルールとゾーンの設定］をクリックします。

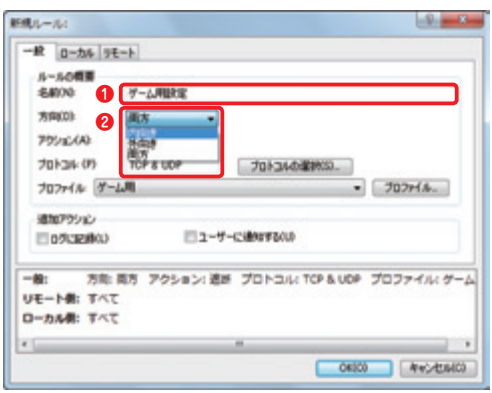


3

［ゾーンとルールの設定］ダイアログが表示されます。［新規］ボタンをクリックします。ここでは、「TCP」プロトコルの「1723」番のポートをインターネット側（リモート側）からアクセスできるようにする設定を例に手順を紹介します。

POINT

ネットワークゲームなどが動作しないために、特定のアプリケーション用にカスタムルールを作成する場合は、購入製品のマニュアルやヘルプなどでどのようなルールを登録しなければならないかを事前に調べておいてください。

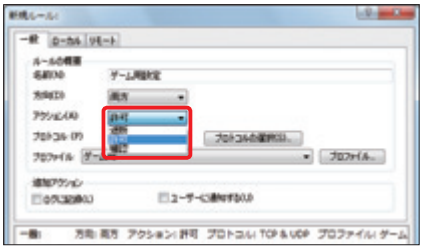


4

［新規ルール］ダイアログが開きます。❶新規ルールに付ける［名前］を入力し、❷データの流れの方向を示す［方向］を設定します。ここでは、インターネット側からのアクセスを許可するのでプルダウンメニューから「内向き」を選択します。

POINT

［方向］は、「内向き（相手から開始される接続）」「外向き（自分から開始する接続）」「両方」の中から設定できます。

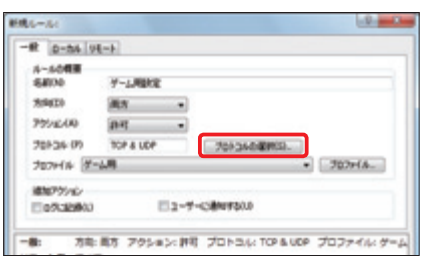


5

通信の可否を指定する「アクション」を設定します。ここでは、インターネット側からの接続を許可するのでプルダウンメニューから［許可］を選択します。

POINT

［アクション］は、「許可」「拒否」「確認」の中から設定できます。「確認」を設定するとこのアクションが発生したときにその接続を許可するかどうかの確認ダイアログが表示されます。



6

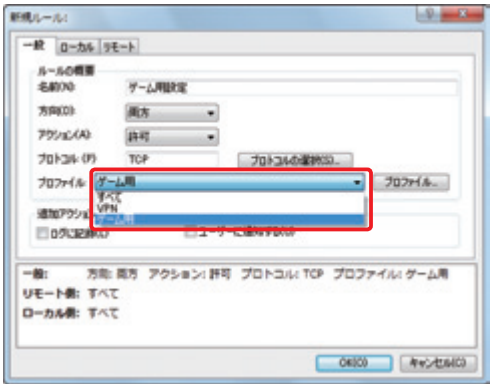
「プロトコル」の設定を行います。ここでは、「TCP」プロトコルを設定します。［プロトコル選択］ボタンをクリックします。

7

「プロトコルの選択」ダイアログが開きます。❶「名前」のプルダウンリストから「TCP」を選択し、❷［OK］ボタンをクリックします。

POINT

プロトコルの設定は、プロトコル番号を入力することでも行えます。プロトコル番号で設定する場合は、「番号」欄に設定したいプロトコル番号を入力し、［OK］ボタンをクリックします。

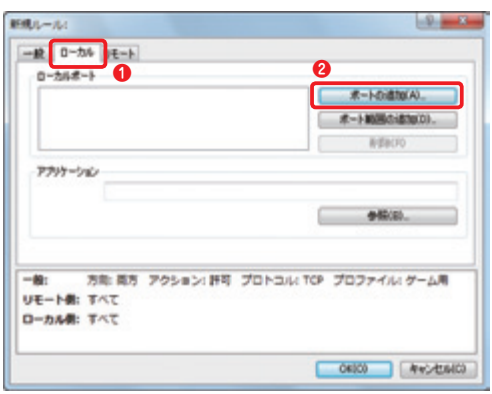


8

特定のプロファイルで使用できるようにする場合は、［プロファイル］のプルダウンリストから使用するプロファイルを選択します。

POINT

作成するカスタムルールをすべてのプロファイルで使用する場合は、［すべて］を選択します。また、［プロファイル］ボタンをクリックすると、新しいプロファイルを作成できます。

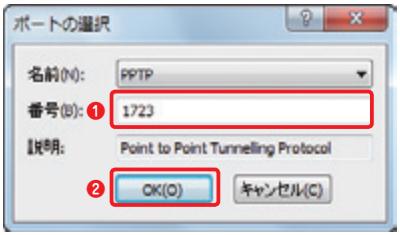


9

❶［ローカル］タブをクリックし、ローカル（自端末）の設定を行います。ネットワーク接続を必要とするアプリケーションが特定の「ポート」を使用する場合は、そのポート番号を登録します。ここでは、「1723」番のポートを登録します。❷［ポートの追加］ボタンをクリックします。

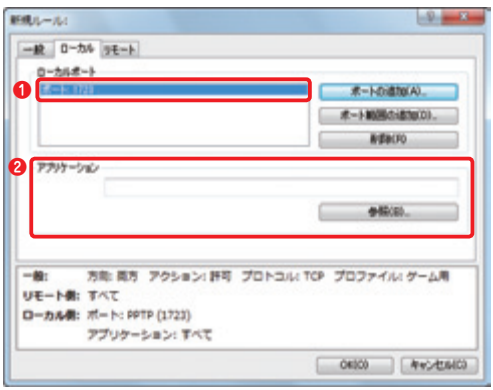
POINT

［ポート範囲の追加］ボタンをクリックすると使用するポートを範囲で指定できます。



10

❶［番号］欄にポート番号を入力し、❷［OK］ボタンをクリックします。ポート番号を入力すると［名前］に表示されているプロトコル名も自動的に変更されます。また、ポートの名前がわかっている場合は、［ポートの選択］をクリックし、メニューから選択することもできます。

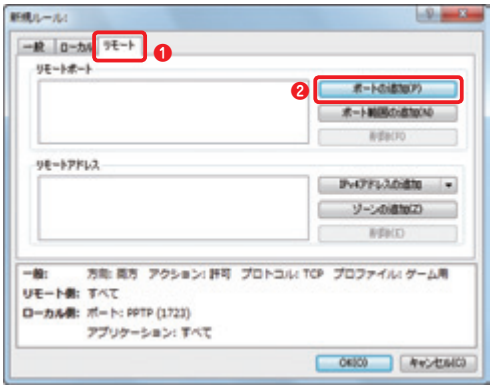


11

❶「ローカルポート」欄にポート番号が追加されます。複数のポートを設定する場合は、手順⑨と手順⑩の作業を繰り返して行います。設定が終わったら、❷「アプリケーション」を設定します。使用するアプリケーションがわからないときは、空白を設定しておくと「すべて」のアプリケーションが対象になります。

POINT

［参照］ボタンをクリックすると「ファイルを参照」ダイアログが開き、使用するアプリケーションを設定できます。アプリケーションを設定しておくと、そのアプリケーションのみが対象となります。

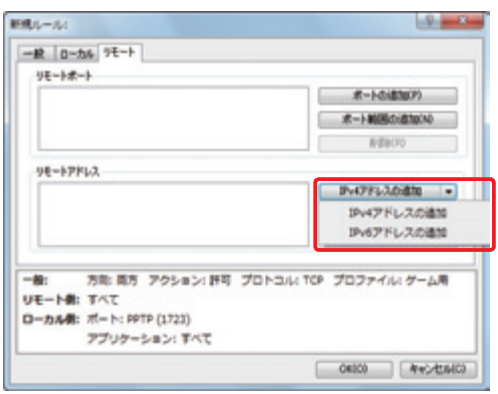


12

❶［リモート］タブをクリックし、リモートの設定を行います。特定のポート番号からの接続を許可する場合は、リモートコンピューターのポート番号を登録します。ポートを追加する場合は、❷［ポートの追加］ボタンをクリックし、手順⑩を参考にポートを追加します。

CAUTION

ここでは、特定のポート番号からの接続を許可するわけではないので、ポートの追加を行っていません。

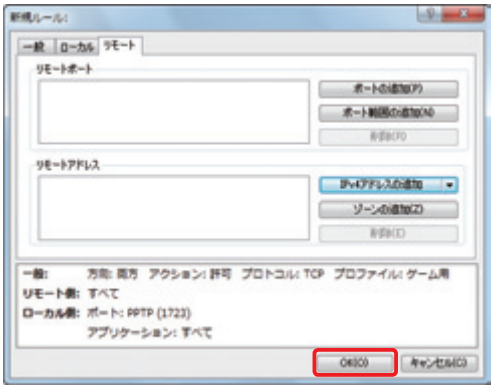


13

「リモートアドレス」の設定を行います。特定のIPアドレスからの接続を許可する場合は、リモートコンピューターのIPアドレスを登録します。プルダウンボタンをクリックし、メニューから「IPv4アドレスの追加」または「IPv6アドレスの追加」をクリックして「リモートIPアドレス」ダイアログが開いたら、IPアドレスの入力を行い、［OK］ボタンをクリックします。

CAUTION

ここでは、特定のIPアドレスからの接続を許可するわけではないので、リモートアドレスの追加を行っていません。



14

すべての設定が終わったら、[OK] ボタンをクリックします。

15

❶「ゾーンとルールの設定」ダイアログに作成したルールが登録されます。新しいルールを登録する場合は、手順③からの作業を繰り返し行います。すべてのルールを登録したら、❷ [OK] ボタンをクリックします。

POINT

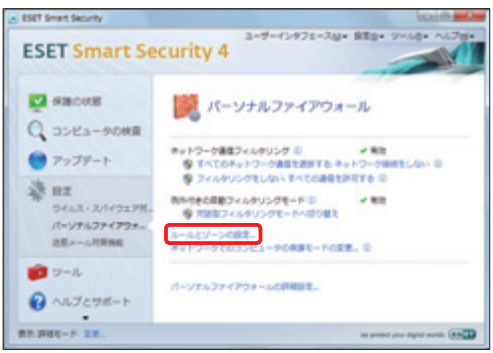
ネットワークゲームなどの通信を利用するアプリケーション用のカスタムルールを作成した場合は、ルールを作成後、必ず、動作を確認してください。

設定 ▸ プロファイル自動切り替え 00043

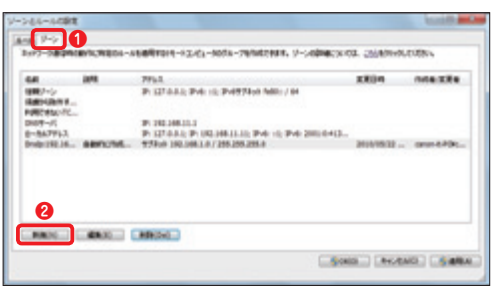
6-9 ESS プロファイルの自動切り替えを行うには

ファイアウォールプロファイルを使用すると、自宅や公衆無線 LAN サービス、会社など接続するネットワークに応じたファイアウォールルールを自動的に適用できます。ここでは、その設定方法を説明します。

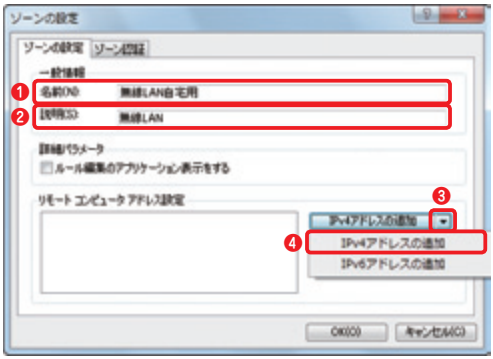
ここでは、あらかじめ指定しておいたデフォルトプロファイルを通常は使用し、自宅の無線 LAN に接続した時だけ、自宅の無線 LAN 用プロファイルに自動的に切り替える方法を説明します。プロファイルの作成方法は、6-7 をご参照ください。また、カスタムルールの作成方法は、6-8 をご参照ください。



① 6-6 を参考にパーソナルファイアウォールを［自動モード］以外に設定し、［ルールとゾーンの設定］をクリックします。



② ［ゾーンとルールの設定］ダイアログが表示されます。❶［ゾーン］タブをクリックし、❷［新規］ボタンをクリックします。

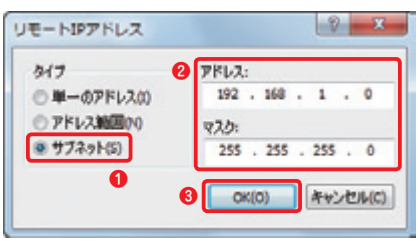


3

［ゾーンの設定］ダイアログが表示されます。❶名前の欄に作成するゾーンの名称を入力し、❷説明欄にゾーンの説明を入力します。❸［IPv4 アドレスの追加］の横にある矢印のボタンをクリックし、❹メニューから［IPv4 アドレスの追加］を選択します。

POINT

IPv6 のネットワーク環境をご利用の場合は、［IPv6 アドレスの追加］をクリックします。

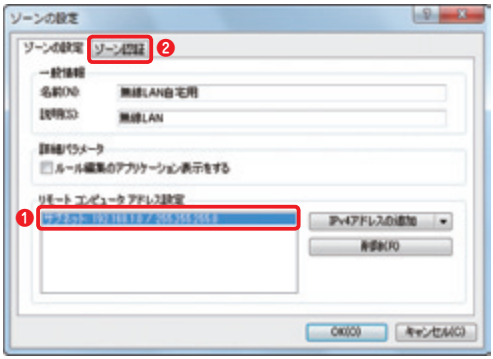


4

❶［サブネット］にチェックを入れ、❷「アドレス」に信頼ゾーンに追加したいネットワークアドレス（IP アドレス）を入力し、「マスク」にサブネットマスクを入力します。❸［OK］ボタンをクリックします。

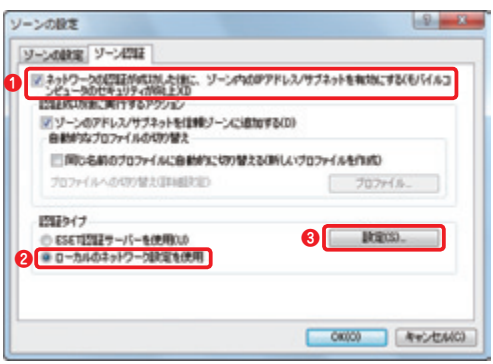
POINT

入力するネットワークアドレスは、ご使用の環境によって異なります。事前にネットワークアドレスやサブネットマスクなどの設定に必要な情報を確認してから設定を行ってください。なお、［単一のアドレス］にチェックを入れると 1 つの IP アドレスを登録でき、［アドレス範囲］にチェックを入れると IP アドレス範囲を登録できます。



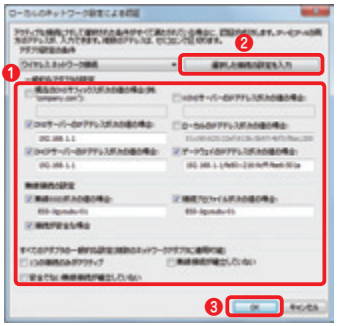
5

❶［リモートコンピュータアドレス設定］に設定したサブネットが追加されます。❷［ゾーン認証］タブをクリックします。



6

❶［ネットワーク認証が成功した後に、…］にチェックを入れ、❷「認証タイプ」に［ローカルのネットワーク設定を使用］にチェックを入れます。❸［設定］ボタンをクリックします。



7

［ローカルのネットワーク設定による認証］ダイアログが表示されます。認証に使用する条件を設定します。❶認証条件に使用したい項目にチェックを入れ、IP アドレス等の設定を行います。❷［選択した接続の設定を入力］ボタンをクリックすると、現在、接続中のネットワーク設定を自動入力できます。❸設定が終わったら、［OK］ボタンをクリックします。なお、無線 LAN 接続固有の設定については、Windows XP ではご利用いただけません。

POINT

複数のネットワークアダプターが有効な場合は、［アダプタ設定の条件］欄のプルダウンボタンをクリックするとアダプターを選択できます。

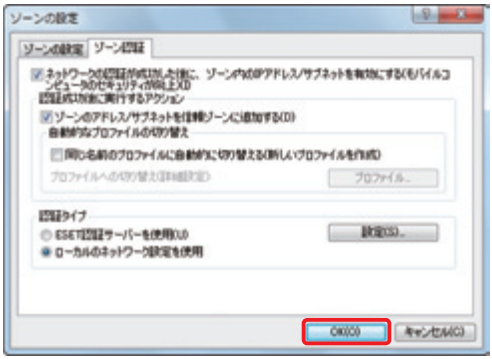
コラム

■ ［ローカルのネットワーク設定による認証］について

［ローカルのネットワーク設定による認証］では、認証条件を設定しておき、その条件を満たした場合に認証が成功します。認証条件に使用できる項目は、ネットワークアダプターで使用される汎用的な設定項目と無線 LAN 接続固有の設定項目、複数のネットワークアダプターに適用可能項目があります。

汎用的な設定項目は、「DNS サフィックス」「WINS サーバーの IP アドレス」「DNS サーバーの IP アドレス」「ローカルの IP アドレス」「DHCP サーバーの IP アドレス」「ゲートウェイの IP アドレス」の 6 種類があります。ご使用のネットワーク環境にあわせて、設定を行ってください。なお、一般的なネットワーク環境では、DHCP サーバーによって IP アドレスを割り当てるのが一般的です。DHCP サーバーは、常に同じ IP アドレスを割り当てるわけではないので「ローカルの IP アドレス」の設定を行うと認証に失敗する可能性が高くなりますのでご注意ください。

無線 LAN 接続固有の設定は、「SSID(ESSID)」［接続プロファイルが次の値の場合」「接続が安全な場合」の 3 種類があります。会社や自宅、公衆無線 LAN サービスなど無線 LAN を使用する場合は、「SSID」を使ってネットワーク環境を使い分けるのがお勧めです。また、「接続が安全な場合」をチェックすると、暗号化が行われている無線 LAN 環境での使用が前提となります。

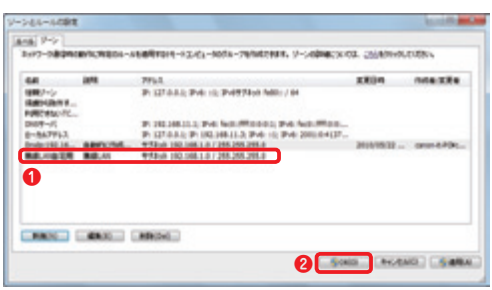


8

［ゾーンの設定］ダイアログに戻ります。［OK］ボタンをクリックします。

POINT

［同じ名前のプロファイルに自動的に切り替える］にチェックを入れ、［OK］ボタンをクリックすると、手順③で設定した名称で新規プロファイルが作成され、手順⑦で設定した条件を満たすときに自動的にプロファイルが変更されるように設定されます。

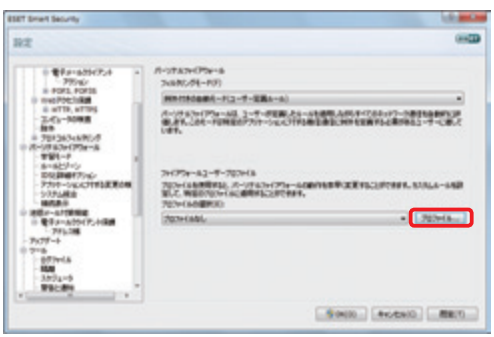


9

❶［ゾーンとルールの設定］ダイアログに作成したゾーンが登録されます。
❷［OK］ボタンをクリックします。

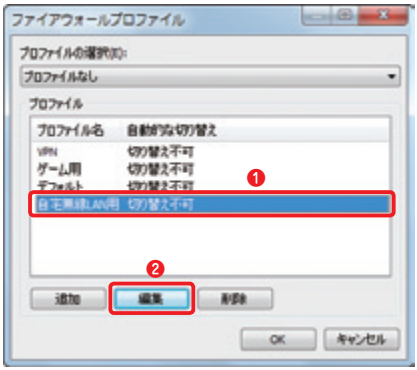
10

基本画面に戻ります。❶［設定］ボタン→❷［パーソナルファイアウォール］とクリックし、❸［パーソナルファイアウォールの詳細設定］をクリックします。



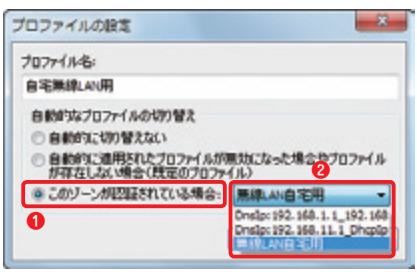
11

［パーソナルファイアウォール］が選択された状態で、ダイアログが開きます。［プロファイル］ボタンをクリックします。



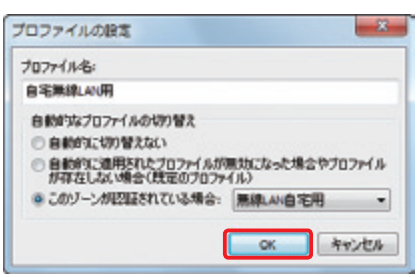
12

［ファイアウォールのプロファイル］ダイアログが開きます。❶自動切り替えを行いたい、プロファイルをクリックし、❷［編集］ボタンをクリックします。



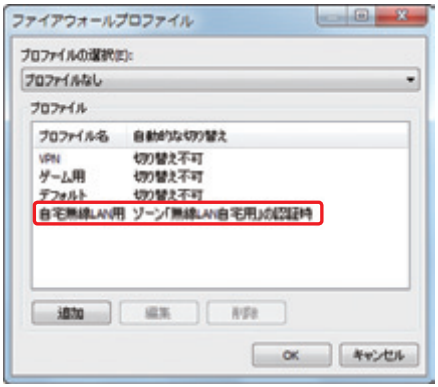
13

［プロファイルの設定］ダイアログが開きます。❶［このゾーンが認証されている場合］にチェックを入れ、❷プルダウンボタンをクリックし、リストから自動切り替えしたいネットワークを選択します。



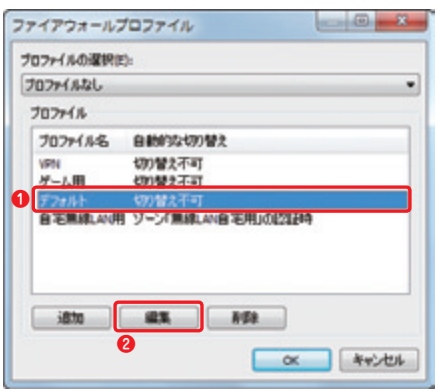
14

［OK］ボタンをクリックします。



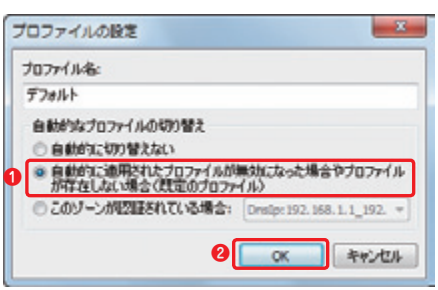
15

［ファイアウォールのプロファイル］ダイアログに戻ります。自動切り替え欄に設定した内容が反映されます。他のプロファイルも自動で切り替えたい場合は、手順⑫～手順⑭の作業を繰り返し行います。すべての設定を行ったら、手順⑯に進みます。



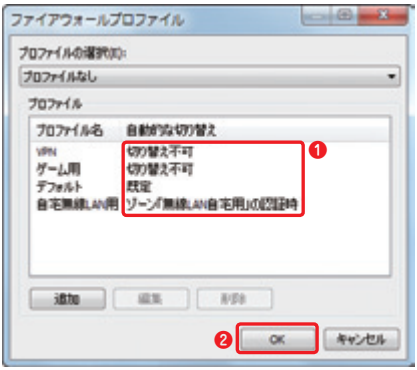
16

通常時に使用するプロファイルの設定を行います。❶既定で使用したいプロファイルをクリックし、❷［編集］ボタンをクリックします。



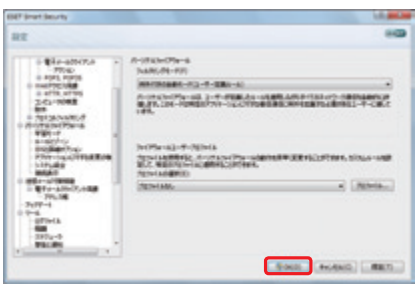
17

［プロファイルの設定］ダイアログが表示されます。❶［自動的に適用されたプロファイルが無効になった場合やプロファイルが存在しない場合（既定のプロファイル）］にチェックを入れ、❷［OK］ボタンをクリックします。



18

［ファイアウォールのプロファイル］ダイアログに戻ります。❶自動的な切り替え欄に設定した内容が反映されます。❷［OK］ボタンをクリックします。



19

手順⑪のダイアログに戻ります。［OK］ボタンをクリックします。

20

自宅の無線 LAN に接続している場合は、プロファイルが切り替わったことを知らせる通知画面が表示されます。また、自宅の無線 LAN に接続していない場合は、デフォルトプロファイルが使用されます。

CAUTION ファイアウォールルール自動切り替え時の注意点

ファイアウォールルールの自動切り替えを使用する場合は、［例外付き自動モード］または［ポリシーベースモード］などの［自動フィルタリングモード］以外のファイアウォールのフィルタリングモードでご使用ください。［自動フィルタリングモード］では、カスタムルールが適用されないため、ファイアウォールプロファイルを変更しても、その設定が反映されません。

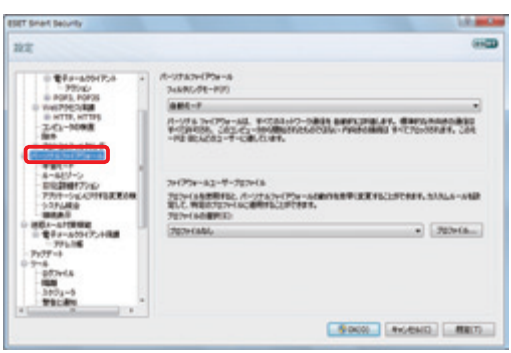
設定 ▸▸ 詳細設定

00044

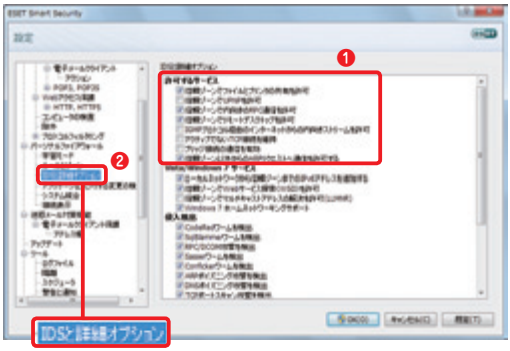
6-10 ESS パーソナルファイアウォールの詳細設定を行うには

パーソナルファイアウォールに関する詳細設定項目は、詳細設定画面に数多く用意されています。フィルタリング設定の操作や動作設定、表示設定などこれまで紹介してきた各設定も、ここから一括して行えます。

① 1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えてから、❶タスクの［設定］ボタンをクリックします。❷［パーソナルファイアウォール］をクリックし❸［パーソナルファイアウォールの詳細設定］をクリックします。

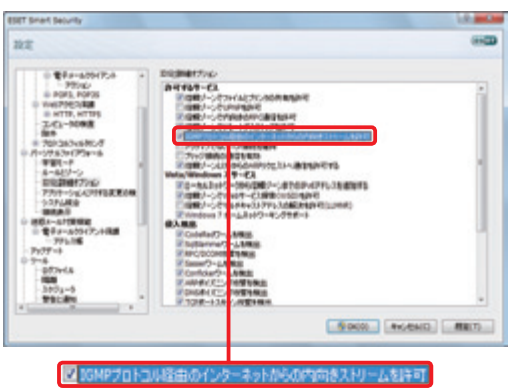


② ［パーソナルファイアウォール］が選択された状態で、ダイアログが開きます。



3

ユーザーが手動設定する必要性の高い項目としては、❶［許可するサービス］があります。❷［IDS と詳細オプション］をクリックすると表示されます。



4

IP マルチキャストを使った動画配信サービスなどを受ける場合は、［IGMP プロトコル経由のインターネットからの内向きストリームを許可］のチェックをオンにします。信頼ゾーンに割り当てたパソコンに対し、IGMP（Internet Group Management Protocol）を使った、インターネットからのストリームデータの受信を許可します。

POINT

Windows Media Player 11/12 など、LAN 内でユニバーサル PnP（UPnP）を使用するアプリケーションでの通信を許可するには、「信頼ゾーンで UPNP を許可」にチェックを入れ、［OK］ボタンをクリックします。

Part.7
「設定」画面での操作３
（迷惑メール対策編）

ここでは、本プログラムの「設定」画面における「迷惑メール対策」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

00045

7-1 ESS 迷惑メール対策機能を一時的に無効にするには

本プログラムの迷惑メール対策機能が原因で正常に電子メールを受信できない場合は、一時的に本機能を無効にしてトラブルを回避しましょう。

1

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えてから、❶タスクの［設定］ボタンをクリックします。❷［迷惑メール対策機能］をクリックし、❸［一時的に迷惑メール対策機能を無効にする］をクリックします。❹ダイアログが表示されたら［はい］ボタンをクリックします。

2

迷惑メール対策機能が一時的に無効となります。再度有効にする場合は［有効にする］をクリックするか、パソコンを再起動します。

設定 ▸ リスト編集 00046

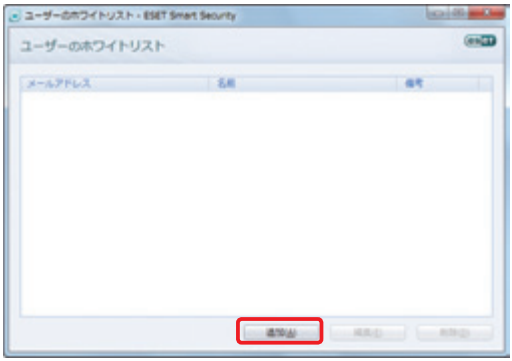
7-2 ESS ホワイトリスト / ブラックリストを編集するには

友人からの電子メールが迷惑メールと誤認識される場合はホワイトリストに登録します。また、迷惑メール送信元の電子メールアドレスをブラックリストに登録することもできます。

■ ホワイトリストの項目を追加するには

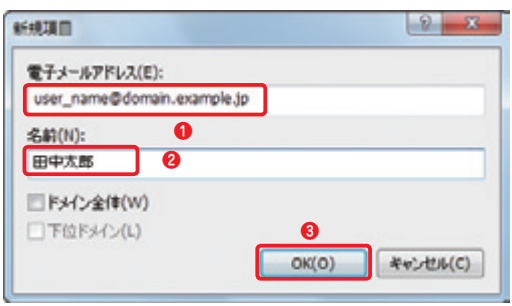
① 1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えてから、タスクの［設定］ボタンをクリックします。

② ❶［迷惑メール対策機能］をクリックし、❷［ユーザーのホワイトリスト］をクリックします。



3

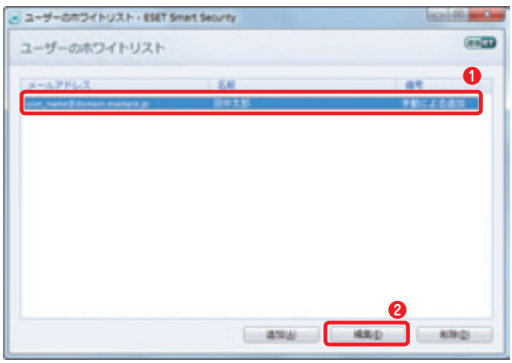
安全な電子メールアドレスを登録するホワイトリストの編集が可能になります。新規に電子メールアドレスを登録する場合は、［追加］ボタンをクリックします。



4

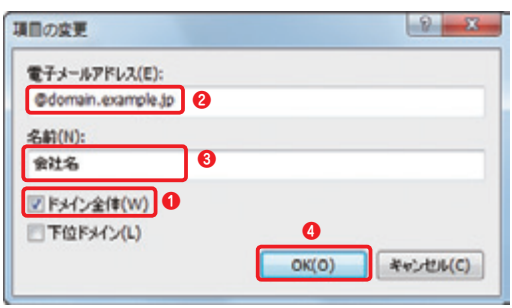
「新規項目」ダイアログが表示されたら、❶「電子メールアドレス」に電子メールアドレスを、❷「名前」に送信者の氏名などわかりやすい名称を入力して、❸［OK］ボタンをクリックします。

■ ホワイトリストの項目を編集するには



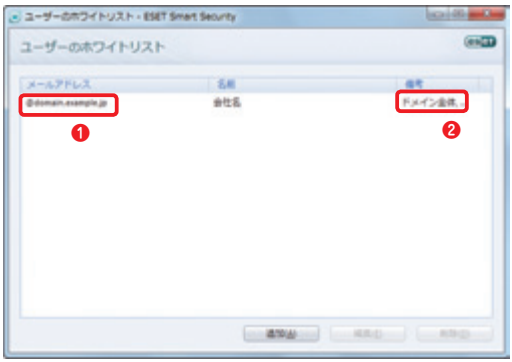
1

登録した電子メールアドレスを編集する場合は、❶一覧から編集するメールアドレスを選択し、❷［編集］ボタンをクリックします。



2

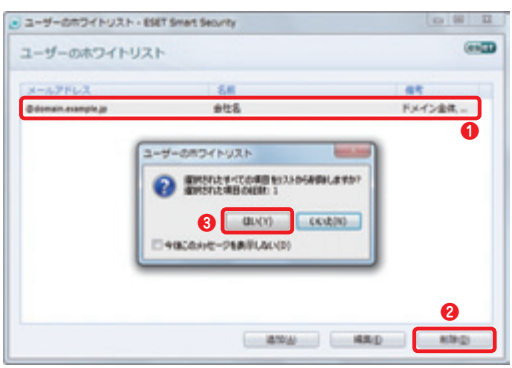
項目を変更するためダイアログが表示されます。例えばドメイン単位でのホワイトリスト登録を行う場合は、❶［ドメイン全体］にチェックを入れてから、❷「電子メールアドレス」を編集し、❸「名前」に会社名などを入力し、❹［OK］ボタンをクリックします。



3

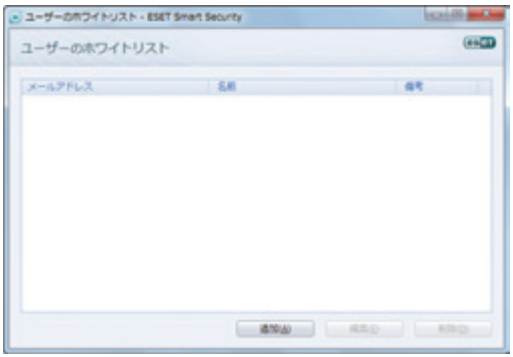
❶メールアドレスと❷ホワイトリストの項目が「ドメイン全体」に修正されました。

■ ホワイトリストの項目を削除するには



1

今度は既存項目を削除しましょう。❶一覧から削除したいメールアドレスを選択し、❷[削除]ボタンをクリックします。確認ダイアログが表示されたら❸[はい]ボタンをクリックします。



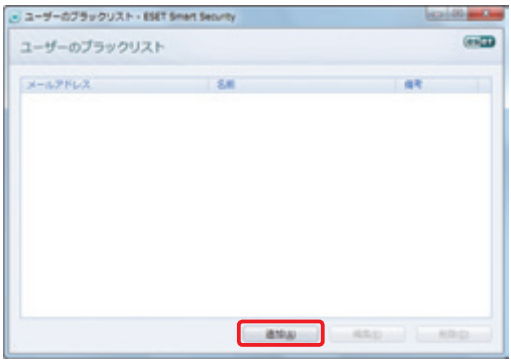
2

手順①で選択した項目が削除されました。誤った電子メールアドレスを登録した場合は、この手順で削除してください。

■ ブラックリストを編集するには

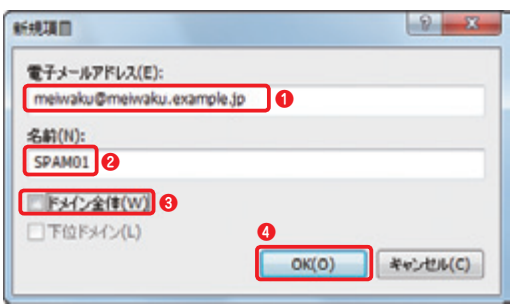
1

迷惑メールを確実に振り分けるためにブラックリストの登録を行います。P.113の手順①を参考に基本画面を開き、❶［迷惑メール対策機能］をクリックし、❷［ユーザーのブラックリスト］をクリックします。



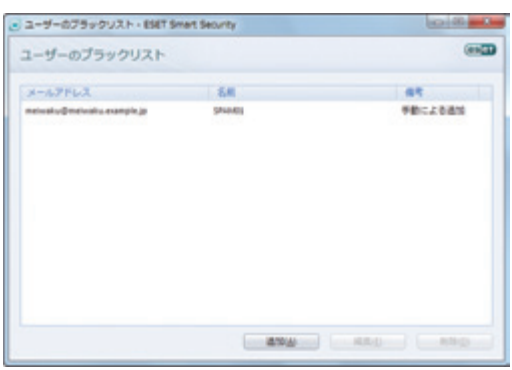
2

ブラックリストが開いて編集が可能になります。ホワイトリスト編集と同じように［追加］ボタンをクリックします。



3

❶「電子メールアドレス」に迷惑メールの電子メールアドレスもしくはドメイン名を、❷［名前］にわかりやすい名称を入力し、（必要に応じて ❸［ドメイン全体］にチェックを入れてから）❹［OK］ボタンをクリックします。



4

メールアドレスがブラックリストに登録されます。

設定 ▸ カウンタのリセット

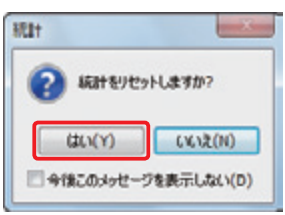
00047

7-3 ESS 迷惑メールカウンタをリセットするには

迷惑メール総数を数えるカウンタをリセットするときは、ESET Smart Security のカウンタリセット機能を使用します。

1

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードに切り替えてから、❶［保護の状態］、❷［統計］とクリックし、❸プルダウンボタンをクリックし、メニューから［電子メールクライアント迷惑メール対策機能］を選択します。❹［リセット］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

迷惑メールのカウンタがリセットされます。

設定 ▸▸ 詳細設定

00048

7-4 ESS 迷惑メール対策機能の詳細設定

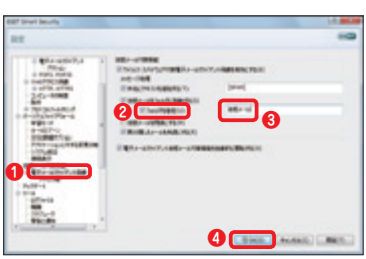
迷惑メールに関する詳細設定項目は、詳細設定画面に数多く用意されています。これらは詳細設定画面から一括設定できます。

1

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えてから、❶タスクの［設定］❷［迷惑メール対策機能］、❸［迷惑メール対策機能の詳細設定］の順番にクリックします。

2

［迷惑メール対策機能］が選択された状態で、詳細設定が開きます。



3

迷惑メールを指定のフォルダに振り分ける場合は、❶［電子メールクライアント保護］、❷［フォルダを指定］にチェックを入れ、❸フォルダ名を入力後、❹［OK］ボタンをクリックします。

Part.8
「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、より踏み込んだ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 00049

8-1 詳細なログファイルを確認するには

EAV ESS

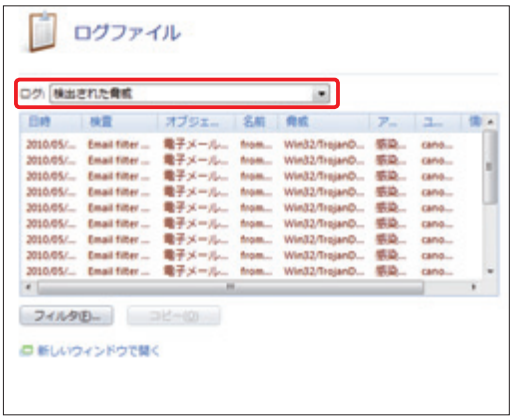
ウイルスの発見・駆除や検査、アップデート情報などのログファイルを確認するには、詳細モードに切り替えると表示される「ツール」ボタンから参照します。

1

1-1 を参考に本プログラムの基本画面を開き、1-2 を参考に詳細モードへ切り替えてから、タスクの［ツール］ボタンをクリックします。

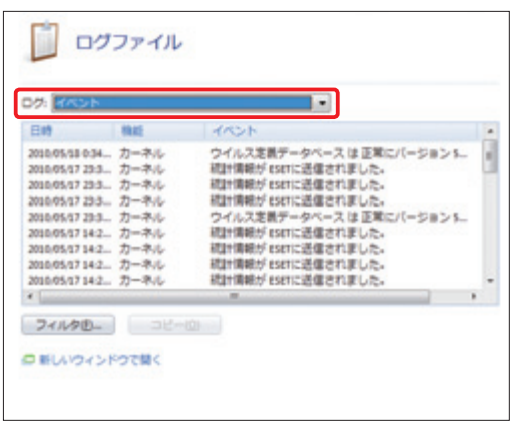
2

［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」のプルダウンリストから「検出された脅威」を選択した場合、発見したウイルスが一覧形式で表示されます。

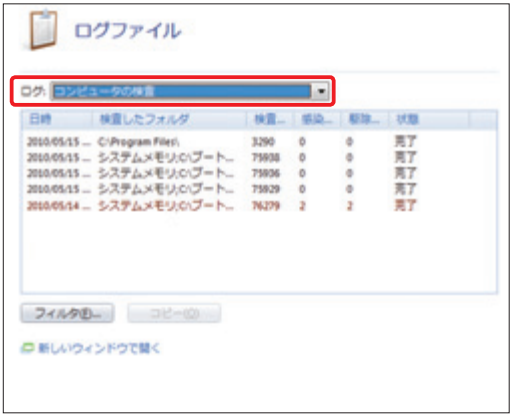


4

「ログ」のプルダウンリストから［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。

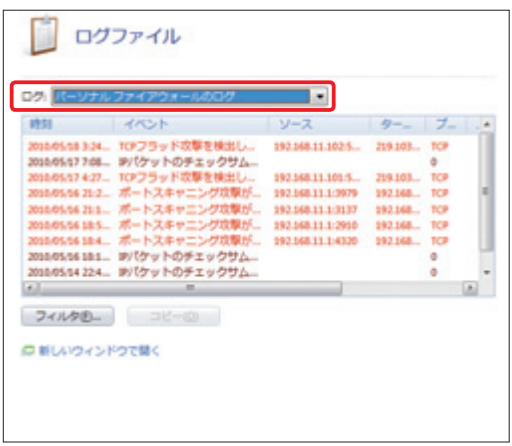
POINT

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」「パーソナルファイアウォールのログ（ESET NOD32アンチウイルスは不可）」の4種類です。



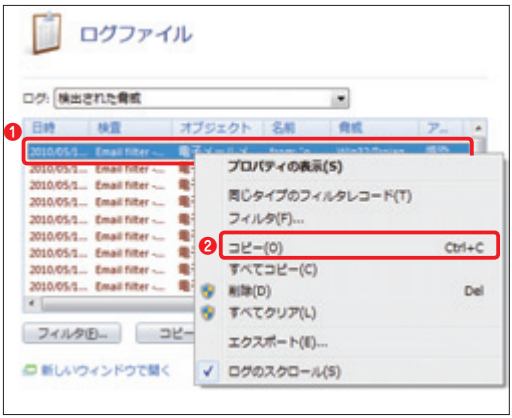
5

「ログ」のプルダウンリストから［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」のプルダウンリストから［パーソナルファイアウォールのログ］を選ぶと、パーソナルファイアウォールが遮断したパケットなどを確認できます。

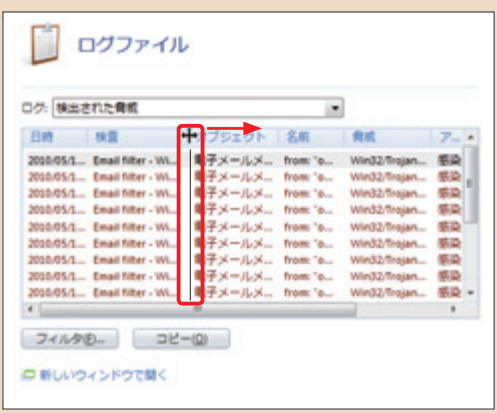


7

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。また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。すべてのログを消去するときは［すべてクリア］をクリックします。

POINT

各レコードの端をドラッグすることで、表示領域を拡大することができます。画面のように名前の内容が長い場合は、「名前」の右端を右方向にドラッグします。



ツール ▸ 隔離ファイルの確認・追加 00050

8-2 各種検査で隔離されたファイルを確認・追加するには

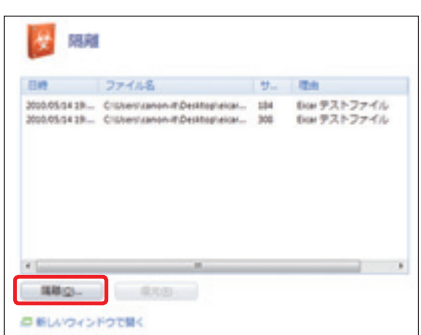
EAV ESS

本プログラムでは、ウイルスを発見すると、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

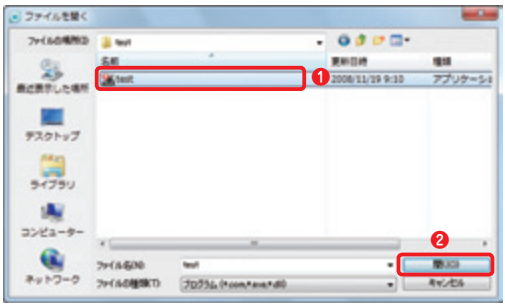
1

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えてから、❶タスクの［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

00051

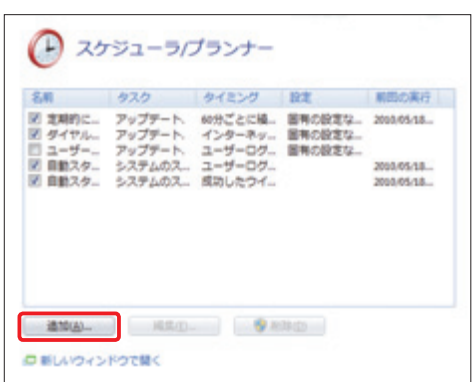
8-3 自動検査・アップデートのスケジュールを設定するには

EAV ESS

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行えます。

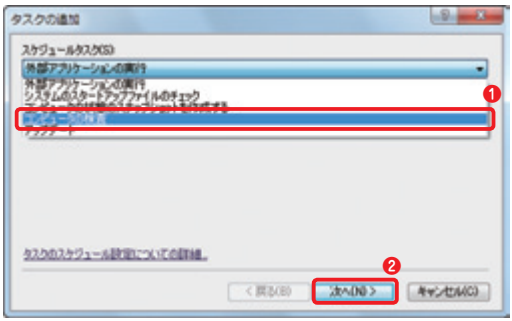
1

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えてから、❶タスクの［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。



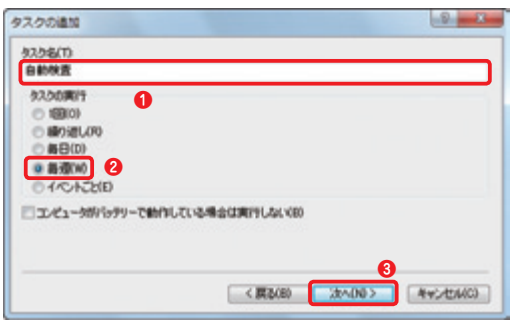
2

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、プルダウンリストから、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。

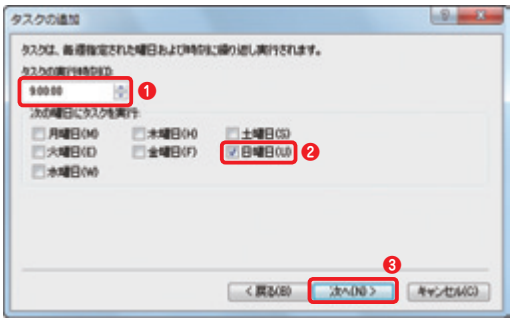


4

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。

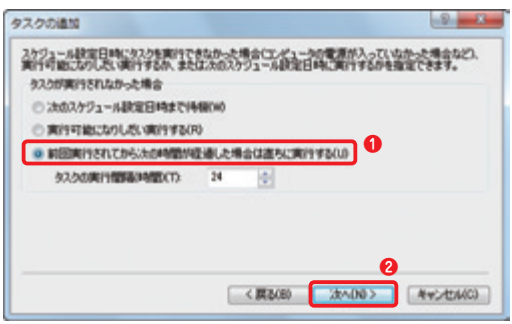
POINT

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。



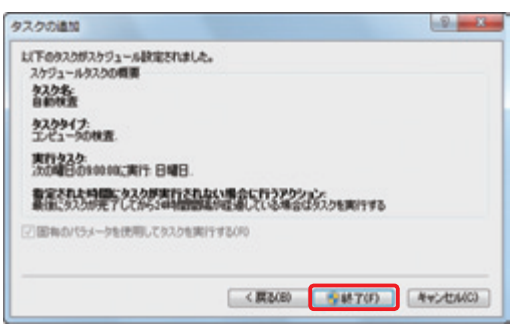
5

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」にあるスピンボタンで任意の時間を選択し、❷［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［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］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。また、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

00052

8-4 コンピューターの様々な情報を確認するには

EAV ESS

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。

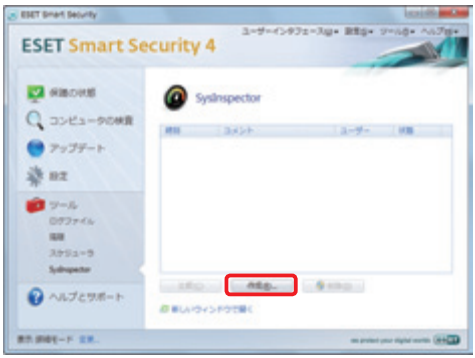
1

1-1 を参考に基本画面を開き、1-2 を参考に「詳細モード」へ切り替えてから、❶タスクの［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

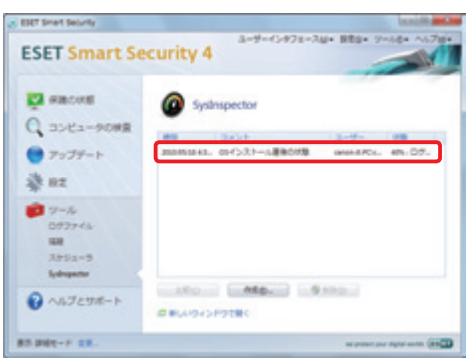


1

P.132 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、保存した情報を比較できます。また、スケジューラを利用して、1 月間隔など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

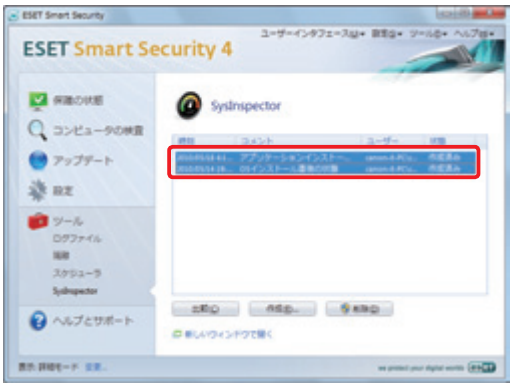
① P.132 の手順を参考に「SysInspector」の操作画面を開き、閲覧したい情報をダブルクリックします。

CAUTION

Windows Vista および Windows 7 を使用している場合は、手順①の実行後に「ユーザーアカウント制御」ダイアログが表示されることがあります。このダイアログが表示されたら、［はい］または［続行］ボタンをクリックしてください。

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 P.132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。

CAUTION

WindowsVista および Windows 7 を使用している場合は、手順①の実行後に「ユーザーアカウント制御」ダイアログが表示されることがあります。このダイアログが表示されたら、［はい］ または［続行］ ボタンをクリックしてください。

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。

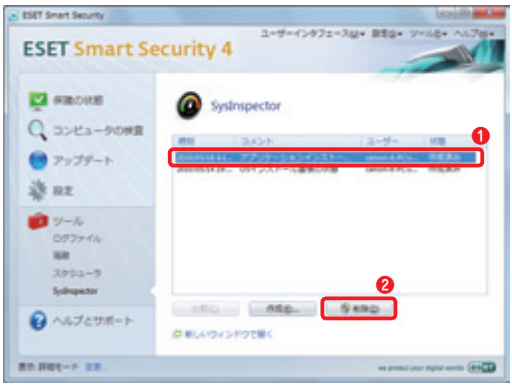
4

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］のプル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 P.132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

00053

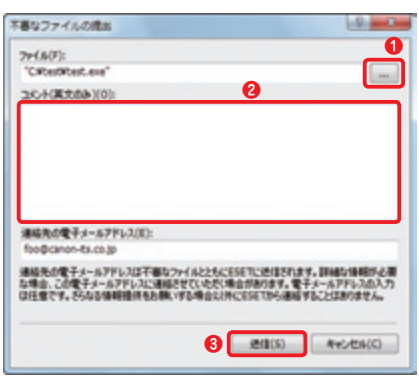
8-5 新種のウイルスと判定されたファイルを提出するには

EAV ESS

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発見したときは、同ファイルをESET 社までお送りください。以下に手順を紹介します。

1

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えてから、❶タスクの［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」について

連絡先の電子メールアドレスの入力は任意です。

Part.9
「ツール」画面での操作２
（SysRescue機能編）

ここでは、CD/DVD や USB 機器（USB メモリや USB HDD など）から本プログラムを起動し、ウイルスチェック等を行える「SysRescue」の使い方について説明しています。

ツール ▸▸ SysRescue の作成 00054

9-1 SysRescue ディスクを作成するには

EAV ESS

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

1-1 を参考に基本画面を開き、1-2 を参考に詳細モードへ切り替えます。タスクの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。

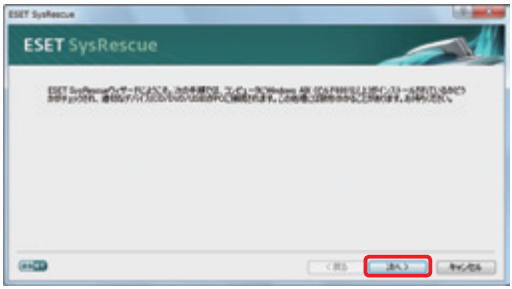
CAUTION

Windows 7/Vista を使用している場合は、「ユーザーアカウント制御」ダイアログが表示されることがあります。このダイアログが表示されたら、Windows 7 の場合は、［はい］ボタンをクリックします。Windows Vista の場合は、［続行］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。パッケージ版をご使用の場合は、製品 CD-ROM に 32bit プラットフォーム用のインストーラーが収録されていますので、Windows のデスクトップなど任意の場所にあらかじめコピーしておいてください。また、ダウンロード版をご使用の場合は、展開先フォルダ内に 32bit プラットフォーム用のインストーラーが格納されています。



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

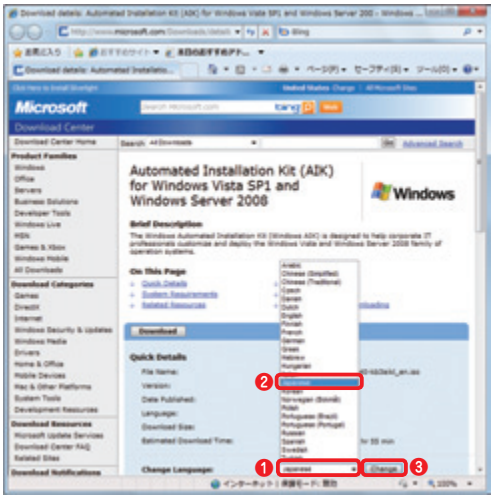
SysRescue の使用には、Windows AIK ビルド 6001 以上をインストールする必要があります。Windows AIK ビルド 6001 以上がインストールされていない場合は手順③へ、インストールされている場合は手順⑪へ進んでください。

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⑪に進んでください。

POINT

初期値とは異なるフォルダに 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を選択します。



4

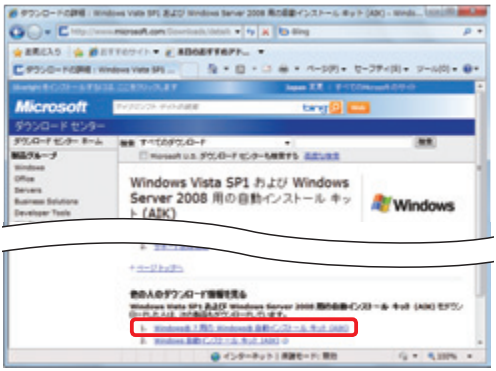
マイクロソフト社の Windows AIK ダウンロードページが開きます。❶［Change Language:］のプルダウンボタンをクリックし、❷［Japanese］を選択して、❸［Change］ボタンをクリックします。Windows XP/Windows Vista をご使用の場合は、手順⑤へ、Windows 7 をご使用の場合は、手順⑥へ進んでください。

5

Windows XP/Windows Vista をご使用の場合は、［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、手順⑧に進みます。

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で記録型 DVD ディスクに記録できます。



6

Windows 7 をご使用の場合は、ページを一番下までスクロールし、[1. 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

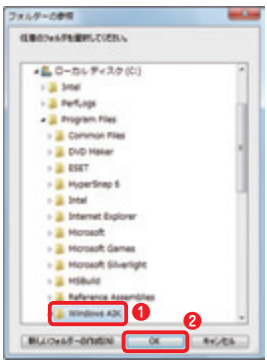
このページで、[Windows 7 用の Windows 自動インストールキット（AIK）] が表示されない場合は、以下の URL を参照してください。
なお、この URL は予告なく変更される場合があります。
http://www.microsoft.com/downloads/details.aspx?FamilyID=696dd665-9f76-4177-a811-39c26d3b3b34&DisplayLang=ja

7

Windows 7用のWindows AIKのダウンロードページが開きます。[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ダブルクリックし、記録型 DVD ディスクに記録して、Windows AIK のインストールを行い、手順⑧に進みます。

8

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。



9

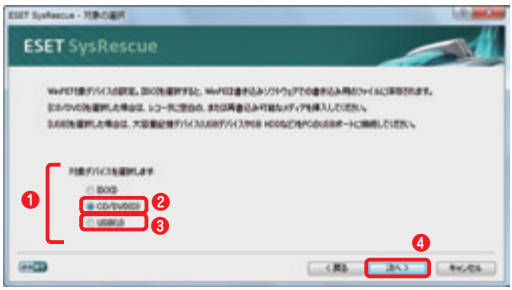
[フォルダーの参照] ダイアログが表示されます。❶ Windows AIK のインストールフォルダーを指定し、❷ [OK] ボタンをクリックします。

10

[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⑩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。



11

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 メモリや USB HDD）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

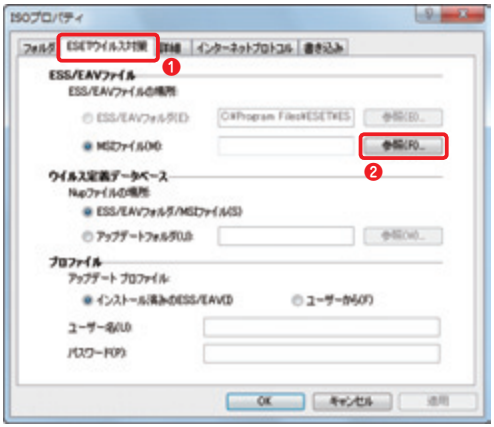
作成先（対象デバイス）に ISO を選択した場合は、HDD 内に ISO イメージファイルを作成します。ISO イメージファイルは、市販の CD/DVD ライティングソフトを使用して、CD/DVD の作成に使用できます。また、Windows 7 を使用している場合は、作成した ISO イメージファイルをダブルクリックすると CD/DVD に記録できます。

12

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⑰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⑬に進みます。

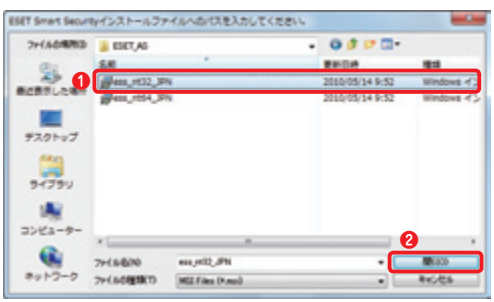
POINT

［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⑬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。



13

「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 ファイルの［参照］ボタンをクリックします。



14

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⑮のあとに、それを知らせるダイアログが表示されます。

15

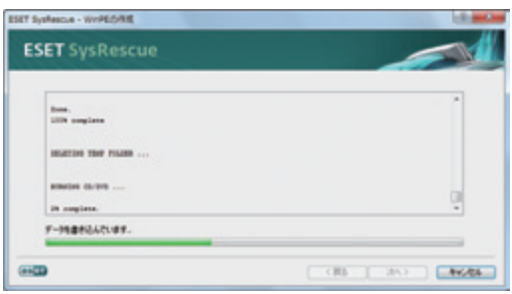
「ISO プロパティ」ダイアログに戻ります。［OK］ボタンをクリックします。

16

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。

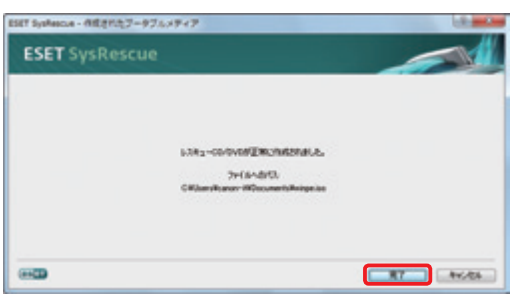
17

データが記録された USB 機器（USB メモリーや USB HDD）、CD-RW、DVD ±RW、DVD-RW 等を作成先に使用した場合は、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。



18

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。



19

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 00055

9-2 SysRescue ディスクから起動するには

EAV ESS

SysRescue ディスクは、それ単体で起動でき、Windows を使用することなく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させ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等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.10
「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 ▸ FAQ の確認

00056

10-1 ヘルプと FAQ（よくある質問）を見るには

EAV ESS

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

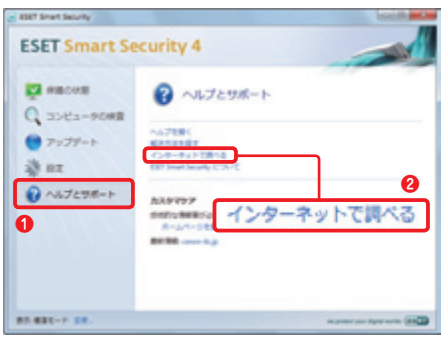
1-1 を参考に基本画面を開き、❶タスクの［ヘルプとサポート］ボタンをクリックします。❷［ヘルプを開く］をクリックすると、ヘルプが表示されます。

ヘルプ ▸ ナレッジベース 00057

10-2 サポート情報を検索するには

EAV ESS

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



1

1-1 を参考に基本画面を開き、❶タスクの［ヘルプとサポート］ボタンをクリックします。次に、❷［インターネットで調べる］をクリックします。

2

サポート情報の Web ページにアクセスし、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（ダイヤルアップ環境であれば、事前にダイヤルアップ接続を行う）で実行してください。

ヘルプ ▸ Web ページ

00058

10-3 本製品に関するWebサイトにアクセスするには

EAV ESS

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

1-1 を参考に基本画面を開き、❶タスクの［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（ダイヤルアップ環境であれば、事前にダイヤルアップ接続を行う）で実行してください。