ESET Cyber Security Pro V6.0
ESET Cyber Security V6.0
操作設定ガイド

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。
この操作設定ガイドでは、本プログラムの詳細な操作や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。
掲載画面は主に「ESET Cyber Security Pro V6.0」を使用しています。
他のバージョンをご利用のお客様は、一部の内容が異なる場合があります。
予めご容赦ください。

■本書について

○本書は、Mac OS X用プログラム「ESET Cyber Security Pro V6.0」「ESET Cyber Security V6.0」の操作設定ガイドです。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 Cyber Security Pro V6.0」は P アイコン、「ESET Cyber Security V6.0」は C アイコンです。掲載画面は主に「ESET Cyber Security Pro V6.0」を使用しています。他の製品やバージョン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

○本プログラムに組み込まれている初期設定を「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」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」と表記しています。

■お断り

ESET Cyber Security Pro V6.0 / ESET Cyber Security V6.0

操作設定ガイド●目次●

Part.1
本プログラムの主な機能と基礎知識

ここでは、本プログラムの主な機能と基礎知識についてご紹介しています。

主な機能

1-1 本プログラムの主な機能を知ろう

P C

本プログラムは、さまざまな脅威からご利用のコンピューターを保護する機能を搭載した総合セキュリティソフトです。多彩な機能を搭載しながら、煩雑な操作を自動化し、容易な操作を実現しています。

主な機能

●ウイルスの駆除・隔離をすべて自動的に処理

ウイルス発見時の駆除や隔離といった煩雑な操作は、自動的に処理されます。そのため、ユーザーはウイルスの存在を意識することなく、コンピューターを常に安全な状態に保つことができます。

独自技術でウイルス対策を強化

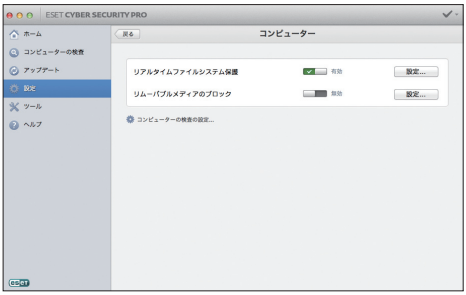
本プログラムは、ウイルス感染を未然に防ぎます。従来のウイルス定義データベースを使用した検出方法だけでなく、独自の技術である「ヒューリスティック手法」や「アドバンスドヒューリスティック手法」によって既知のウイルスだけでなく、新種・未知のウイルスの検出も可能です。

POINT

「ヒューリスティック手法」や「アドバンスドヒューリスティック手法」とは、ファイル内のプログラムコードを解析し、プログラムの挙動分析と動作検証を行って、ウイルス検出を行う手法です。ウイルス定義データベースを使用した検出方法だけでは、新種・未知のウイルスは防げません。本プログラムは、これらの機能を搭載してウイルス対策を強化しています。

コンピューター全般の保護機能

●リアルタイムファイルシステム保護 P C



リムーバブルメディアやLAN経由など外部からコピーしたファイルにウイルスが含まれている場合、ウイルスを検知すると警告メッセージを発し、OSへのウイルスの侵入を未然に防ぎます。また、リムーバブルメディア（CD/DVD/USBメモリーなど）検出時にウイルス検査を実行することもできます。

● ESET Live Grid P C

ESET Live Gridは、新しい脅威に対処する先進の早期警告システムです。ESETウイルスラボは、クラウドから得たウイルス関連情報をリアルタイムに活用することで、常に防御策を最新に保って定常的な保護に努めています。

Webやメール関連の保護機能

● Webアクセス保護 P C

Webアクセス保護は、Webアクセス時に使用するHTTP通信の保護を行い、マルウェアなどの侵入を防ぎます。

●電子メールクライアント保護 P C

メールの通信をチェックし、添付ファイルによるウイルス感染やマルウェアの侵入を防ぎます。

ネットワーク関連の保護機能

●パーソナルファイアウォール P

ネットワーク通信を監視し、不審な通信を遮断、必要な通信のみを許可することができます。ファイアウォールを通過させるアプリケーションの設定は、既定値では自動的に行われますが、使用用途に応じて詳細な設定を行うこともできます。

●ペアレンタルコントロール（保護者機能） P

ペアレンタルコントロールは、不快な内容などを掲載していると考えられる Web サイトを閲覧できないようにブロックできます。この機能を使用すると、児童や青少年に不適切なサイトへアクセスできないように設定できます。

動作環境

[対応 OS]

Mac OS X v10.6 Snow Leopard
OS X v10.7 Lion
OS X v10.8 Mountain Lion
OS X v10.9 Mavericks
※サーバー OSは対象外です。

[CPU]

インテルプロセッサー（32bitまたは 64bit）
※ Power PCは対象外です。

[メモリー]

512MB 以上

[ハードディスク]

150MB 以上の空き容量（推奨：1GB 以上の空き容量）

※オペレーティングシステムがあるドライブにインストールする場合は，できる限り 1GB 以上の空き容量を確保した上でインストール作業を実施してください。また，特別な理由がない限りインストール先は標準設定のままでインストールすることを推奨します。

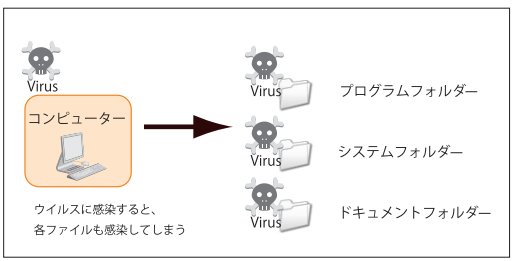
主な機能

1-2 セキュリティの基礎を知ろう

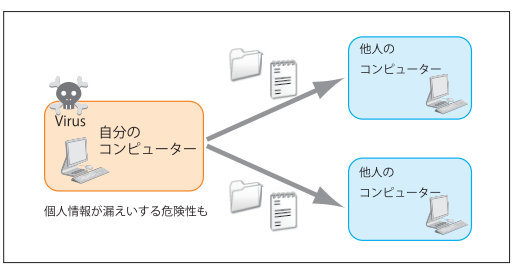
P C

ウイルスとは、どのような存在なのでしょうか。ここでは本プログラムから一歩離れて、ウイルスやセキュリティの基礎などについて説明します。

ウイルスとは何？



ウイルス（コンピューターウイルス）とはコンピューターに感染し、自己増殖や破壊活動を行うプログラムの総称です。主にWebページの閲覧やファイルのダウンロード時に感染します。



ウイルスに感染すると、ファイルの破損や特定アプリケーションの実行速度低下、データの改ざんなどが行われ、被害は甚大です。特に、情報漏えいは社会的信用度が著しく落ちてしまいます。

POINT

ウイルスの種類を大別すると、セキュリティホール（システムのセキュリティ上の弱点）などを悪用して侵入し、破壊活動を行うもの、有用なアプリケーションに見せかけて侵入する「トロイの木馬」、指定時刻など一定条件を満たすと自動的に破壊動作を開始する「ロジックボム」、ユーザーの操作履歴などを収集する「スパイウェア」などがあります。

より強固なセキュリティ対策を行うには？

Apple 社が提供するソフトウェア･アップデートを適用すると、より強固なセキュリティ環境が築けます。ソフトウェア・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。ソフトウェア・アップデートを適用し、常に OS を最新の状態に維持することが、セキュリティ対策において重要なポイントとなります。

POINT

ソフトウェア・アップデートは、手動で行うこともできます。手動で行う場合は、メニューバーの❶［アップルメニュー］をクリックし、❷［ソフトウェア･アップデート］をクリックします。

主な機能 ▸▸ キーワード

1-3 さまざまな用語を知ろう

P C

本書で使われている説明では、数多くのコンピューター用語が用いられています。ここでは、コンピューター用語の説明を行います。

HTTP	Webページ閲覧時に利用されるプロトコルです。主にTCP80番ポートや8080番ポートが利用されます。
IPv4アドレス	データを送受信する機器を判別するために用いられ、192.0.2.10などの数字で表記されます。通信を行ううえで、機器の住所のような役割を持ちます。
OS（オペレーティングシステム）	コンピューターの基本的な部分を操作するための基本プログラム。ワードプロセッサーや表計算ソフトなど一般的なソフトウェアはOS上で動作します。Mac OS XはOSのひとつです。
POP3	電子メールの受信時に利用されるプロトコルです。主にTCP110番ポートが利用されます。
Live Grid	ESET Live Gridは、新しい脅威に対処する先進の早期警告システムです。ESETウイルスラボは、クラウドから得たウイルス関連情報をリアルタイムに活用することで、常に防御策を最新に保って定常的な保護に努めています。
Web	インターネットなどで一般的に用いられるドキュメントシステムです。Webサービスを提供するサーバーをWebサーバーと呼び、SafariのようにWebサーバーへのアクセスやWebページの表示を行うソフトウェアをWebブラウザーと呼びます。
アカウント	コンピューターやネットワーク上の資源を利用するための権利を持つユーザー名などを指します。本プログラムではアップデートサーバーへの接続時に必要となります。
アップデート	ソフトウェアの小規模な更新を意味し、本プログラムではプログラム本体やウイルス定義データベースのアップデートを意味します。

アドウェア	広告表示などを目的としたソフトウェアです。Safariのホームページ（起動時に閲覧するページ）を書き換えるタイプも存在します。
ウイルス	様々な経路から感染しコンピューター内のデータを破壊するプログラムです。行動パターンによって様々な別称があり、WordやExcelといったソフトウェア上のマクロを用いて自己増殖や破壊活動を行う「マクロウイルス」、電子メールなどを通じて自己増殖や破壊活動を繰り返す「ワーム」などが存在し、これらの総称として使われることもあります。
ウイルス定義データベース	ウイルスの特徴を収録したファイルで、本プログラムなどのウイルス対策ソフトがウイルスの検出に使用します。他のウイルス対策ソフトでは「パターンファイル」と称することもあります。
拡張子	ファイルの種類を定義する方法のひとつ。ファイル名末尾の「.（ドット）」以下を指します。
隔離	本プログラムにおける隔離とは、ウイルスとして検出されたファイルを隔離フォルダーに保存する処理を指します。また、隔離されたウイルス感染ファイルは無効化処理が施されているため安全です。
駆除	本プログラムではウイルスに感染したファイルからウイルスだけを取り除き、正常なファイルに戻すことを指します。ただしウイルスの種類によっては駆除が難しく、場合によってはファイルを削除しなければなりません。
サーバー	Webや動画配信などの色々なサービスを提供するコンピューターを指します。
スパイウェア	ユーザーのWebアクセス履歴や操作パターンなどを収集し、送信するプログラムです。
セキュリティホール	ソフトウェアの設計ミスなどによって生じた、セキュリティ上の弱点を指します。インターネットに接続しているコンピューターの場合、OSのセキュリティホールに攻撃を受ける危険性があります。現在では、OSだけでなくアプリケーションのセキュリティホールを突く攻撃も増加しています。
トラフィック	ネットワーク上を移動するデータ、もしくはネットワーク上を移動するデータの情報量を指します。

トロイの木馬	従来のトロイの木馬は、自己を有益なプログラムに見せかけ、ユーザーを騙して実行させようとするものが一般的でしたが、現在では、この限りではありません。他の種類に分類されないほとんどのマルウェアがトロイの木馬として分類されます。トロイの木馬には、多くの種類があり、代表的なものにダウンローダー、バックドア、キーロガーなどのプログラムがあります。ダウンローダーは、インターネットから他のマルウェアをダウンロードする機能を搭載したプログラムで、バックドアは、リモートの攻撃者と通信して、システムにアクセスし制御できるようにするプログラム、キーロガーは、ユーザーが入力した各キーストロークを記録し、リモートの攻撃者にその情報を送信するプログラムです。
ヒューリスティック手法	プログラムやファイルのコード解析と仮想環境上でウイルスの挙動分析と動作検証を実行して、新種・未知のウイルス検出を行います。
ファイアウォール	外部から企業や家庭内 LAN などへの侵入、もしくは意図しない外部へのアクセスを防ぐ機能です。「パーソナルファイアウォール」は、内外に流れるデータの送受信を制御するのが一般的です。
フィッシングメール	金融機関などからの案内メールを装い、暗証番号やクレジットカード番号などを詐取する詐欺メールなどを指します。
プログラムコンポーネント	本プログラムではプログラム本体のアップデート時に更新されるプログラムのパーツを意味します。
プロトコル	コンピューターが他のコンピューターと通信を行うには、データの送受信の手続き方法など様々な約束ごとが必要になります。この約束ごとをプロトコルと呼びます。
ポート	データを送受信するアプリケーションを判別するために、主に IP アドレスとセットで用いられます。各ポートは番号で表記されます。たとえばメールソフトウェアは電子メールの受信のために TCP110番ポートを、Web ブラウザーは閲覧のために TCP80番ポートをそれぞれ利用します。
マルウェア	ウイルスやスパイウェアなど、悪意を持ったソフトウェアの総称です。

迷惑メール（スパムメール）	ユーザーの許可を得ずに広告表示などを目的として無差別に送信されてくる電子メールを指します。
リアルタイムファイルシステム保護	ファイルの読み込み／書き込み／実行時などに、ファイルを検査する機能です。
リモート攻撃	攻撃者が、ネットワーク（インターネットなど）を利用して別のコンピューターを攻撃することを指します。リモート攻撃には、Webサーバーなど利用できなくするDoS(Denial of Service)攻撃、DNSサーバーを騙し、悪意のあるサーバーに接続させ、ワームやウイルスをダウンロードさせるDNS侵害、データの送受信で利用されるポート番号のうち空いているポートチェックするポートスキャン、Windowsネットワークで使用されているSMB（Server Message Block）ファイル共有プロトコルを利用して攻撃を行うSMBリレー、さまざまなエラーメッセージを送信するために使用されるICMP（インターネット制御メッセージプロトコル）を利用して攻撃を行うICMP攻撃などがあります。
ルートキット	動作中のプログラムをユーザーから見えなくする機能を持ったプログラムです。悪意のある侵入者が遠隔地のコンピューターを不正に操作するために用いるパッケージを「ルートキット」と称することもあります。
ファイアウォールルール	ファイアウォールが通信を許可するか否かを判断するための設定情報を指します。本プログラムのパーソナルファイアウォール機能では、既定のルールの他にユーザーが自分でルールを作成できます。
ログファイル	様々な過程を詳細に記録したファイルを指しますが、本プログラムではウイルス検査を行った日時や検査したファイル名などを記録しています。
ワーム	感染先のコンピューターを攻撃しネットワークを介して蔓延する悪意のあるプログラムを指します。ワームは、広い意味ではウイルスの一種とされますが、その特徴は異なります。ワームは自己を複製し、自ら移動でき、宿主ファイルに依存しません。このため、ワームは、ウイルスよりはるかに実行される可能性が高く、インターネットを利用することで、リリース後、数時間以内に世界中に蔓延でき、場合によっては、数分で広まります。自己を単独で急速に複製できるワームは、他の種類のマルウェアやウイルスなどよりはるかに危険です。

Part.2
本プログラムの画面構成と画面操作

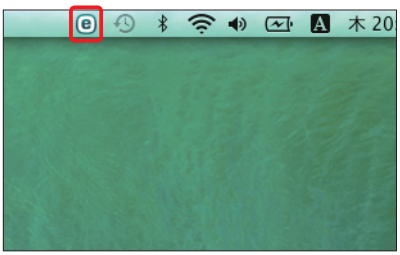
ここでは、本プログラムの画面構成とその基本的な操作方法についてご紹介しています。

メインウィンドウ ▸▸ メニューバー

2-1 P C メニューバーの主な操作について

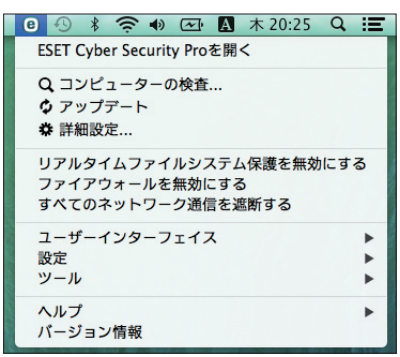
本プログラム起動時には、メニューバーにアイコンが表示され、クリックするとメニューから各種操作を行えます。最初にこのメニューバーのアイコンの操作を説明します。

メニューバーアイコンとメインウィンドウ



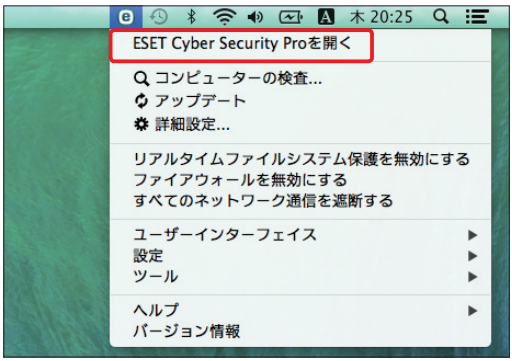
1

本プログラムのアイコンは、OS 起動後に、メニューバーに表示されます。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。



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、本プログラムのメインウィンドウを呼び出すことができます。



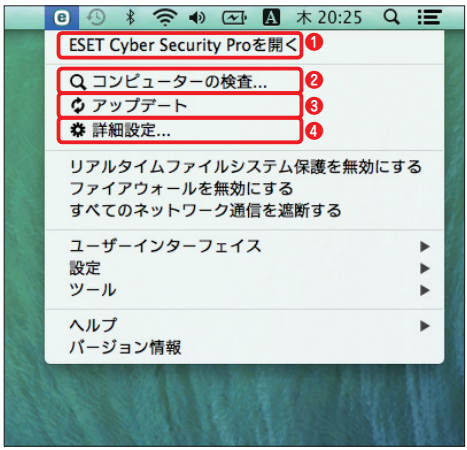
3

メインウィンドウを表示する手順は次の通りです。メニューバーのアイコンをクリックし、表示されるメニューから［ESET Cyber Security Pro を開く］または［ESET Cyber Security を開く］をクリックします。

4

メインウィンドウが表示されます。

表示メニュー



メニューバーのアイコンをクリックすると、メニューが表示されます。❶［ESET Cyber Security Pro を開く］または［ESET Cyber Security を開く］をクリックすると、メインウィンドウが開きます。❷［コンピューターの検査］をクリックすると、コンピューターの検査が実行されます。❸［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実行されます。❹［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

表示されたメニューから［リアルタイムファイルシステム保護を無効にする］［ファイアウォールを無効にする］をクリックすると、それぞれの機能が停止します。特に理由のない場合、これらは選択しないでください。また、［ユーザーインターフェイス］→［ウィンドウレイアウトを初期状態に戻す］を選択すると、ウィンドウレイアウトを初期状態に戻します。［設定］または［ツール］を選択し、メニューから項目を選択すると、対応した画面が表示されます。［バージョン情報］をクリックすると、バージョン情報の画面が表示されます。

主な機能 ▸▸ 各機能

2-2 各機能を確認するには

P C

本プログラムでは各機能がすぐに利用できるように、「ホーム」「コンピューターの検査」「アップデート」「設定」「ツール」「ヘルプ」といった項目を用意しています。ここではメインメニューの各機能を説明します。

メインウィンドウの画面構成

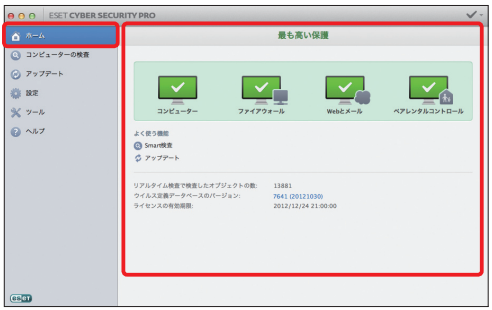
1

メインウィンドウには、各機能を呼び出すためのボタンが並ぶ❶「メインメニュー」と、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❷「プライマリウィンドウ」があります。

2

❶［プログラムメニュー］ボタン（画面右上）をクリックすると、❷「プログラムメニュー」が表示されます。プログラムメニューでは、Smart 検査の実行や保護統計の確認、各種保護機能の有効無効の切り替えなどが行えます。

ホーム



「ホーム」では、本プログラムの現在の状態を確認できます。プライマリウィンドウには、各保護機能へのリンクやよく使う機能へのリンクが準備されており、「ライセンスの有効期限」も確認できます。

コンピューターの検査

「コンピューターの検査」はウイルス検査時に使用します。このボタンからは、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。

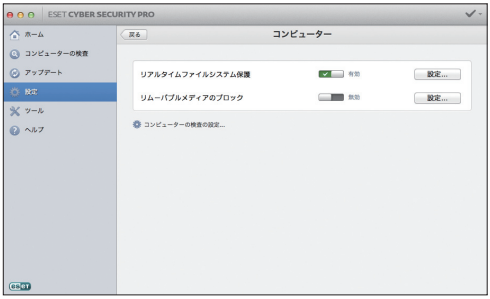
アップデート

「アップデート」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、ここでは、製品のアクティベーションが行えます。アクティベーション済みの場合は、ライセンス情報などが表示されます。

設定

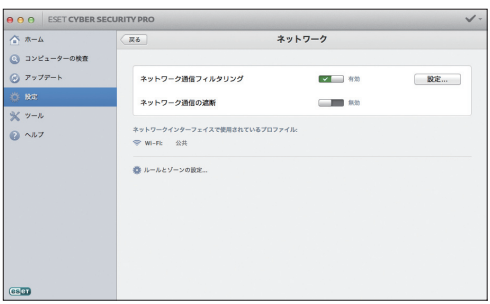
1

「設定」では、本プログラムに搭載されている各種保護機能の状態を確認・変更できます。保護機能は、「コンピューター」「ファイアウォール」「Web とメール」「ペアレンタルコントロール」の 4 つのカテゴリに分類されています。



2

手順①のプライマリウィンドウで［コンピューター］をクリックすると、OS へのウイルスの侵入を未然に防ぐ「リアルタイムファイルシステム保護」や「リムーバブルメディアのブロック」の状態を確認・変更できます。



3

手順①のプライマリウィンドウで［ファイアウォール］をクリックすると、パーソナルファイアウォール機能の状態を確認・変更できます。なお、本機能は ESET Cyber Security Pro でのみご利用いただけます。

4

手順①のプライマリウィンドウで［Web とメール］をクリックすると、Web ページ閲覧時のウイルスの侵入を防ぐ「Web アクセス保護」や、メールを検査する「電子メールクライアント保護」、「フィッシング対策」などの状態を確認・変更できます。

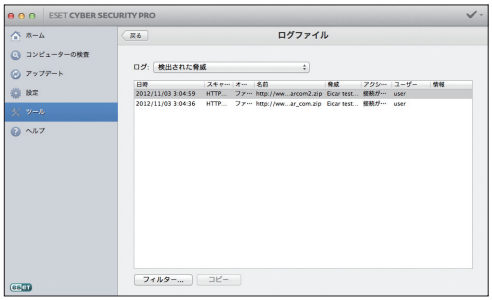
5

手順①のプライマリウィンドウで［ペアレンタルコントロール］をクリックすると、不快な内容などを掲載していると考えられるWebサイトを閲覧できないようにブロックする「ペアレンタルコントロール」の状態を確認・変更できます。なお、本機能はESET Cyber Security Proでのみご利用いただけます。

ツール

1

「ツール」には、各種ログ情報の確認や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「スケジューラー」などの各種ツールが配置されています。

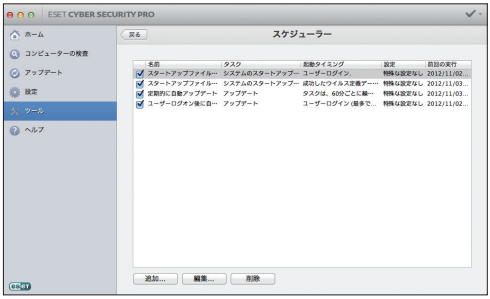


2

手順①のプライマリウィンドウで［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」「コンピューターの検査」「ファイアウォール」「ペアレンタルコントロール」のログを確認できます。

3

手順①のプライマリウィンドウで［保護統計］をクリックすると、本プログラムがインストールされてからのウイルス・スパイウェア対策やオンデマンド検査、リアルタイム検査、電子メール保護、Web アクセス保護の統計情報を確認できます。

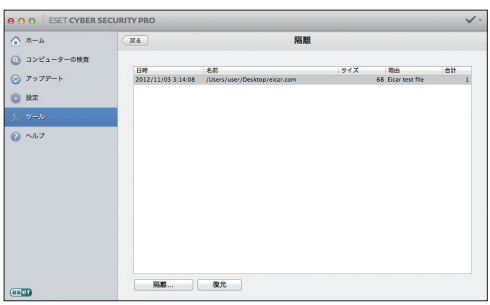


4

手順①のプライマリウィンドウで［スケジューラー］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。

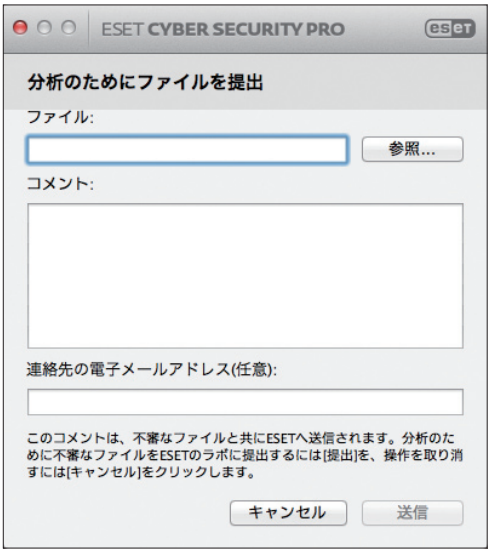


5

手順①のプライマリウィンドウで［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。

6

手順①のプライマリウィンドウで［実行中のプロセス］をクリックすると、現在実行中のプロセスを確認できます。



7

手順①のプライマリウィンドウで［分析のためにファイルを提出］をクリックすると、不審なファイルなどをESET社に送信できます。

ヘルプとサポート

［ヘルプ］をクリックすると、トラブル発生時に役立つヘルプやWebページへのリンク、カスタマーサポートへの連絡方法などが表示されます。お困りの際に参照してください。

Part.3
「ホーム」画面での操作

ここでは、本プログラムの「ホーム」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

3-1 P C コンピューターの保護の状態を確認・有効にするには

「ホーム」で表示される「コンピューターの保護」の状態の既定値は、「最も高い保護」です。ここでは、「ホーム」のプライマリウィンドウに表示される保護状態について説明します。

「最も高い保護」で守られている場合

メインウィンドウを開き、❶［ホーム］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、❸各機能に「✓」が入っていれば、すべての対策機能が有効になった通常状態です。なお、ペアレンタルコントロールは必要に応じてご利用ください。

「最も高い保護」で守られていない場合

1

例えばリアルタイムファイルシステム保護が無効になっていると、画面に❶❷のような警告が表示され、❸「⚠」のアイコンが付きます。この機能を有効にしたい場合は、❹［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

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、画面に❶❷のような警告が表示され、❸「⚠」のアイコンが付きます。この機能を有効にしたい場合は、❹［フィルタリングモードを開始する］をクリックします。なお、本機能はESET Cyber Security Proでのみご利用いただけます。

3

Webアクセス保護機能が無効になっていると、画面に❶❷のような警告が表示され、❸「⚠」のアイコンが付きます。この機能を有効にしたい場合は、❹［Webアクセス保護を有効にする］をクリックします。

4

電子メールクライアント保護機能が無効になっていると、画面に❶❷のような警告が表示され、❸「⚠」のアイコンが付きます。この機能を有効にしたい場合は、❹［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。

5

ペアレンタルコントロールが無効になっていると、警告画面は表示されませんが、「ペアレンタルコントロール」に「…」のアイコンが付きます。なお、本機能はESET Cyber Security Pro でのみ利用いただけます。

POINT

複数の機能が無効になっている場合は、❶無効になっている機能それぞれの警告画面が表示されます。無効になっている機能をすべて有効にしたいときは、❷［プログラムメニュー］ボタンをクリックし、❸［すべての問題の解決を試みます］をクリックします。

OS が最新でない場合

1

OS の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［未適用のアップデート］をクリックします。

2

ダイアログが表示されます。［今すぐインストール］ボタンをクリックします。

3

アップデート画面が表示されますので、［アップデート］ボタンをクリックして、アップデートを行ってください。

Part.4
「コンピューターの検査」画面での操作

ここでは、本プログラムの「コンピューターの検査」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

4-1 P C 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 メインウィンドウを開き、［コンピューターの検査］ボタンをクリックします。

2 表示内容が「コンピューターの検査」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、進行状況を示すバーが表示されます。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、終了したいときは［中止］ボタンをクリックします。

4

検査が完了するとダイアログが表示されます。ウイルスなどが検出されていないことを確認し、［OK］ボタンをクリックします。

5

［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 ▸▸ カスタム検査

4-2 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

P C

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 メインウィンドウを開き、［コンピューターの検査］ボタンをクリックします。

2 「コンピューターの検査」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。「Smart 検査」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

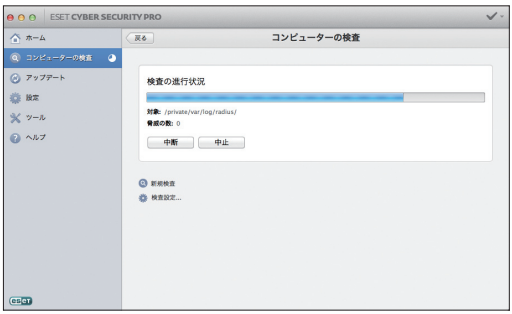
［検査の対象］を選択します。今回は、一例として起動ドライブ（ここでは、「Macintosh HD」）の「アプリケーションフォルダー」を検査対象にします。▶をクリックします。

6

❶「/Volumes」以外のすべてのフォルダーにチェックを入れ、❷［検査］ボタンをクリックします。

POINT

「/Volumes」にチェックを入れると、接続（マウント）中の他のパソコンの共有フォルダーやUSBメモリーなども検査対象となり、検査に時間がかかる場合があるので、ご注意ください。



7

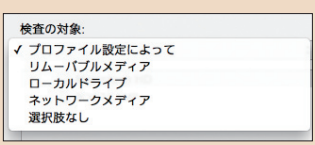
ウイルスの検査が始まり、進行状況を示すバーが表示されます。終了までお待ちください。
一時的に中断したいときは［中断］ボタン、検査の途中で終了したいときは［中止］ボタンをクリックします。

8

検査が完了するとダイアログが表示されます。ウイルスなどが検出されていないことを確認し、❶［OK］ボタンをクリックし、❷［OK］ボタンをクリックして検査を終了します。

POINT

手順⑤で「検査の対象」のドロップダウンリストを使用すると、カテゴリによる検査を行えます。選択できるカテゴリには、「プロファイル設定によって」「リムーバブルメディア」「ローカルドライブ」「ネットワークメディア」の 4 種類があります。



コンピューターの検査 ▸▸ カスタム検査

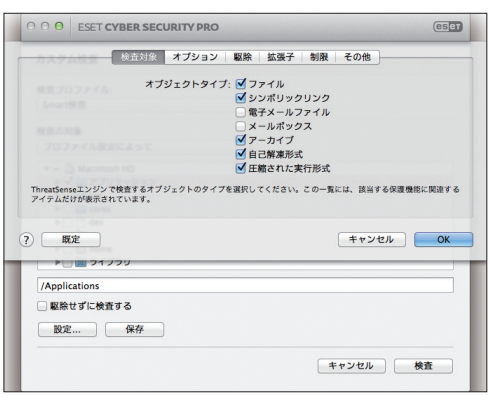
4-3 カスタム検査の詳細設定を変更するには

P C

カスタム検査は場面に応じて動作やウイルス検査内容を変更することができます。ここではその手順を説明します。

1

40 ページの手順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。

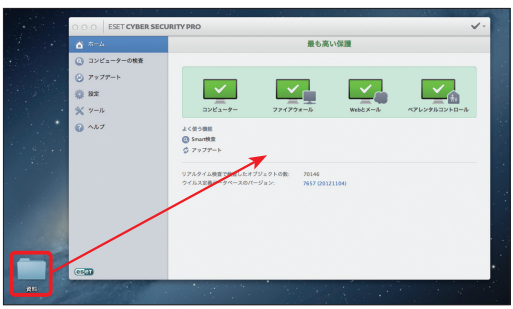


2

「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。

4-4 P C 簡単な操作でファイルやフォルダーを検査するには

本プログラムには、手軽なウイルス検査の方法としてファイルやフォルダーをメインウィンドウにドラッグ & ドロップするという方法が準備されています。



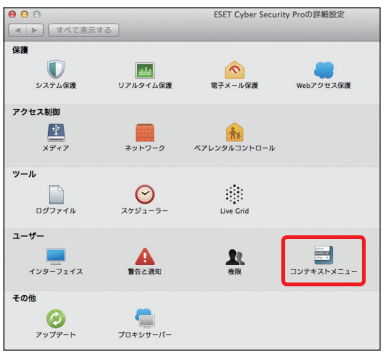
① 本プログラムのメインウィンドウを開きます。ウイルス検査を行いたいフォルダーをメインウィンドウにドラッグ & ドロップします。

② ウイルス検査が実施されます。ウイルス検査が完了したらダイアログが表示されます。❶［OK］ボタンをクリックし、❷［OK］ボタンをクリックします。

コラム

コンテキストメニューで検査を実施するには

本プログラムは、［Ctrl］キーを押しながらクリック（副ボタンのクリック）したときに表示されるコンテキストメニューから、ファイルやフォルダーのウイルス検査を実施できます。この機能を使用したいときは、以下の手順でコンテキストメニューを有効に設定します。



1

53 ページの手順を参考に詳細設定画面を表示し、［コンテキストメニュー］ボタンをクリックします。

2

❶［コンテキストメニューに統合する］にチェックを入れ、❷［OK］ボタンをクリックします。OS を再起動するか、ログアウトして再度ログインします。

3

フォルダーまたはファイルを［Ctrl］キーを押しながらクリックします。❶［サービス］→❷［ESET Cyber Security Pro - 検査］または［ESET Cyber Security - 検査］と選択します。選択したフォルダー / ファイルのウイルス検査（駆除なし）が実施されます。

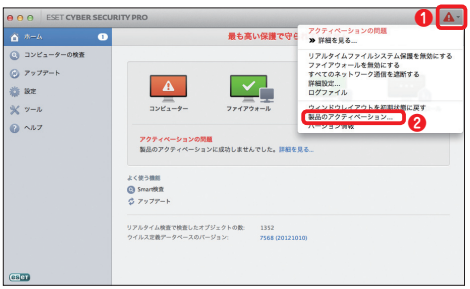
Part.5
「アップデート」画面での操作

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 ▸▸ アクティベーション

5-1 P C 製品のアクティベーションを行うには

本プログラムを利用するには、製品のアクティベーションを行う必要があります。ここでは、アクティベーションを行う手順を説明します。体験版から製品版への移行など、ユーザー名とパスワードを再入力する際も同じ手順です。



1

メインウィンドウを開き、❶［プログラムメニュー］ボタンをクリックし、❷［製品のアクティベーション］をクリックします。

2

［製品のアクティベーション（有効化）の種類］画面が開きます。❶「ユーザー名とパスワードを入力して使用する」がチェックされていることを確認し、❷［次へ］ボタンをクリックします。

POINT

製品のアクティベーション画面は、メニューバーにある本プログラムのアイコンをクリックし、メニューから［製品のアクティベーション］をクリックすることでも表示できます。

3

ユーザー登録メールに記載されている、❶「ユーザー名」と❷「パスワード」を入力し、❸［アクティベーション］ボタンをクリックします。

4

アクティベーションに成功すると、自動的にウイルス定義データベースのアップデートが開始されます。ウイルス定義データベースのアップデートが完了したら、アクティベーションは完了です。

アップデート ▸▸ 手動アップデート

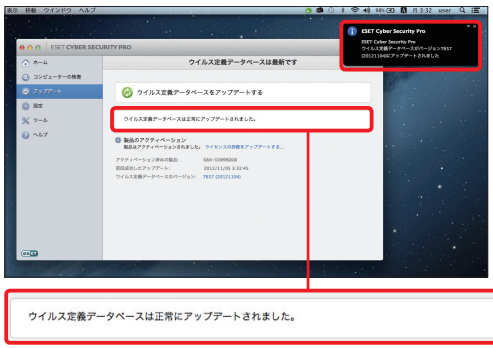
5-2 P C ウイルス定義データベースのアップデートを手動で行うには

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、手動でアップデートを行うこともできます。

メインウィンドウから実施する

❶

メインウィンドウを開き、❶［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。



❷

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。

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。

メニューバーのアイコンから実施する

1

❶メニューバーにある本プログラムのアイコンをクリックし、❷［アップデート］をクリックします。

2

メインウィンドウが開き、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

アップデートが完了すると、「ウイルス定義データベースは正常にアップデートされました。」と表示されます。

ウイルス定義データベースは正常にアップデートされました。

アップデート ▸▸ 自動アップデートの確認

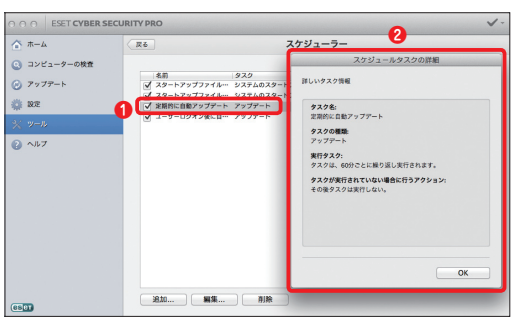
5-3 自動アップデートの設定を確認するには

P C

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

メインウィンドウを開きます。❶［ツール］ボタンをクリックし、❷［スケジューラー］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。

アップデート ▸▸ プロキシサーバー

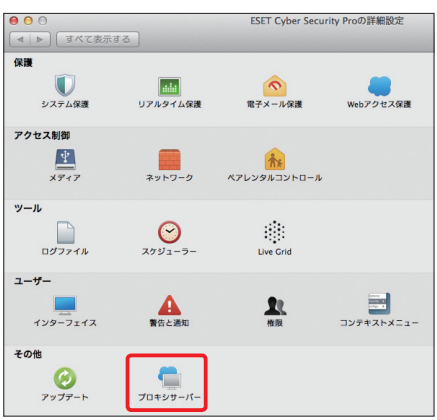
5-4 プロキシサーバーを設定するには

P C

プロキシサーバー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ーの設定が必要です。ここでは、プロキシサーバーの設定手順を説明します。

1

メインウィンドウを開き、❶［設定］ボタンをクリックして、❷［詳細設定を表示する］をクリックします。



2

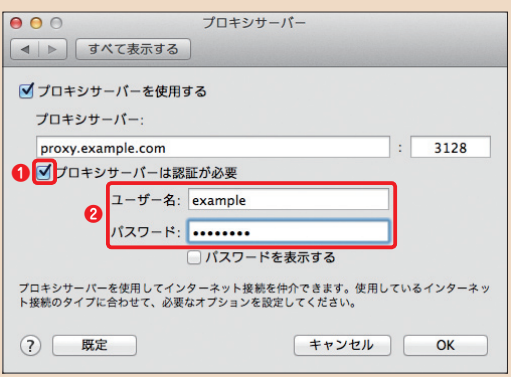
［詳細設定］画面が表示されます。［プロキシサーバー］ボタンをクリックします。

3

❶［プロキシサーバーを使用する］にチェックを入れます。❷IP アドレスまたはホスト名を入力し、❸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

プロキシサーバーにユーザー認証が設定されている場合は、❶［プロキシサーバーは認証が必要］にチェックを入れ、❷「ユーザー名」欄と「パスワード」欄にプロキシサーバーの接続に利用するユーザー名とパスワードを入力します。



Part.6
「設定」画面での操作1
（コンピューター編）

ここでは、本プログラムの「設定」画面における「リアルタイムファイルシステム保護」など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。

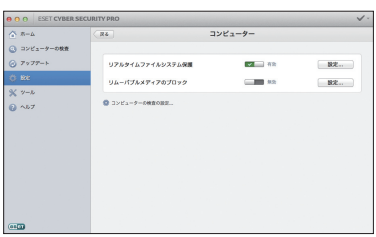
設定 ▸▸ 画面構成

6-1 P C 「設定」のメインウィンドウの画面構成

「設定」のプライマリウィンドウでは、本プログラムに搭載されている各種保護機能の状態の確認や設定が行えます。ここでは、「設定」のプライマリウィンドウの画面構成を説明します。

①

基本画面を開いて、❶［設定］ボタンをクリックすると、❷プライマリウィンドウに本プログラムに搭載されている各種保護機能がカテゴリーごとに表示されます。保護機能は、「コンピューター」「ファイアウォール」「Web とメール」「ペアレンタルコントロール」の 4 つの項目に分類されています。

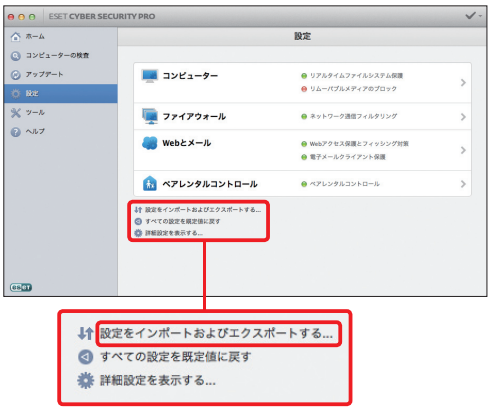


②

手順①のプライマリウィンドウで［コンピューター］［ファイアウォール］［Web とメール］［ペアレンタルコントロール］の項目名をクリックすると、対応した項目の動作状態の確認や動作の有効 / 無効の切り替え、各種設定変更などが行えます。ここでは、例として「コンピューター」の画面を掲載しています。

POINT

「コンピューター」の詳細な設定については、次ページ以降をご参照ください。「ファイアウォール」は、ESET Cyber Security Pro にのみ搭載された機能です。この機能の詳細な設定については、79 ページ以降をご参照ください。「Web とメール」の詳細な設定については、103 ページ以降をご参照ください。「ペアレンタルコントロール」は、ESET Cyber Security Pro にのみ搭載された機能です。この機能の詳細な設定については、117 ページをご参照ください。



3

手順①のプライマリウィンドウで［設定をインポートおよびエクスポートする］をクリックすると、本プログラムの設定をファイルに保存したり、保存しておいたファイルを読み出すことで設定を復元できます。詳細については、78 ページをご参照ください。

4

手順①のプライマリウィンドウで［詳細設定を表示する］をクリックすると、「詳細設定」画面を表示でき、本プログラムの詳細な設定を行えます。詳細については、次ページ以降をご参照ください。

設定 ▸▸ 一時無効化

6-2 リアルタイムファイルシステム保護機能を一時的に無効にするには

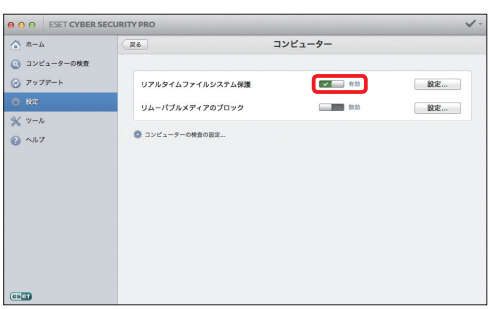
P C

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、リアルタイムファイルシステム保護機能を一時的に無効にしてみましょう。

リアルタイムファイルシステム保護機能を無効にする

1

メインウィンドウを開き、❶［設定］ボタンをクリックし、❷［コンピューター］をクリックします。

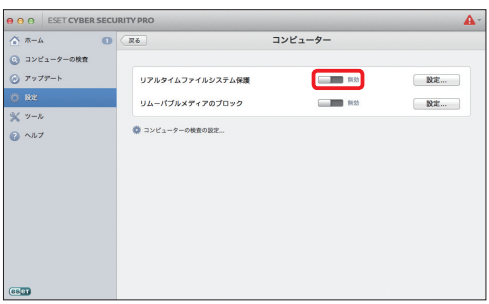


2

［有効／無効］スイッチをクリックします。

3

ダイアログが表示されます。［無効］ボタンをクリックします。



4

リアルタイムファイルシステム保護が無効になります。

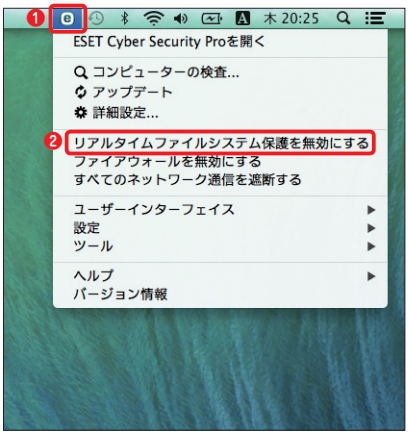
5

［ホーム］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。

コラム

メニューバーのアイコンから無効にするには

リアルタイムファイルシステム保護機能の有効・無効は、メニューバーの本プログラムのアイコンをクリックして表示されるメニューから、以下の手順で切り替えることもできます。



1

❶メニューバーにある本プログラムのアイコンをクリックして、❷［リアルタイムファイルシステム保護を無効にする］をクリックします。

2

ダイアログが表示されます。［無効］ボタンをクリックします。

設定 ▸▸ 除外拡張子の追加

6-3 ウイルス検査をしない拡張子を設定するには

P C

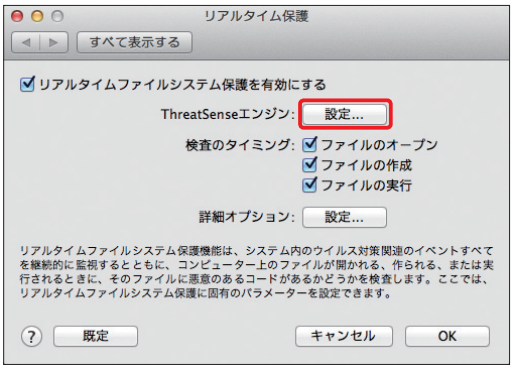
特定の拡張子をウイルス検査から除外するには、対象となる拡張子を登録します。

1

メインウィンドウを開き、❶［設定］ボタンをクリックし、❷［コンピューター］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］ボタンをクリックします。

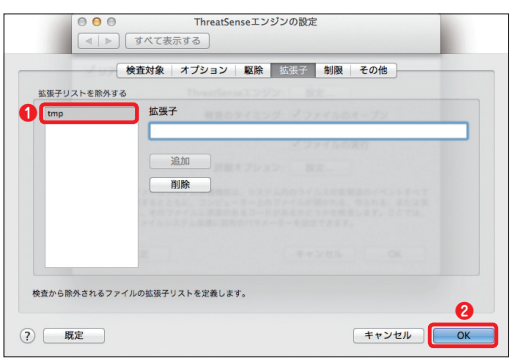


3

［リアルタイム保護］画面が表示されます。ThreatSense エンジンの［設定］ボタンをクリックします。

4

［ThreatSense エンジンの設定］ダイアログが開きます。❶［拡張子］をクリックします。❷拡張子の欄に除外したいファイルの拡張子（ここでは、「tmp」）を入力し、❸［追加］ボタンをクリックします。



5

❶除外リストに入力した拡張子が登録されます。❷登録を終了するときは、［OK］ボタンをクリックし、手順③の画面に戻ったら、［OK］ボタンをクリックします。

設定 ▸▸ 除外対象の登録

6-4 P C ウイルス検査をしないフォルダーやファイルを設定するには

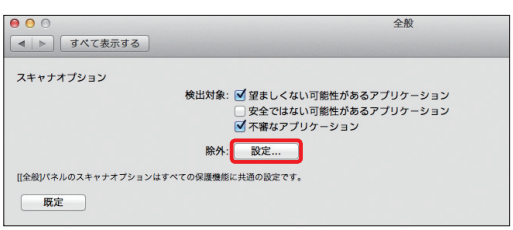
本プログラムでは、特定のフォルダーやファイルをリアルタイム検査やコンピューターの検査から除外できます。ここでは、検査から除外したいフォルダーやファイルの登録方法を紹介します。

1

メインウィンドウを開き、❶［設定］ボタンをクリックし、❷［詳細設定を表示する］をクリックします。

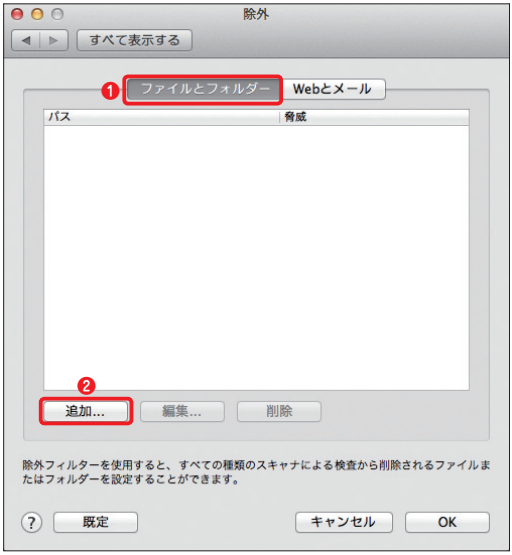
2

［全般］ボタンをクリックします。



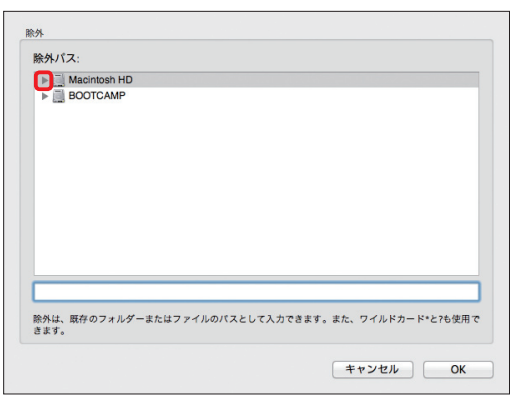
3

［設定］ボタンをクリックします。



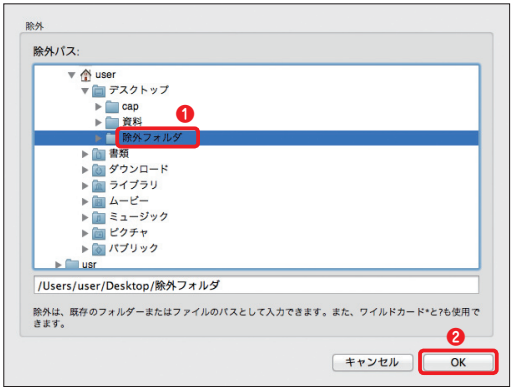
4

「除外」画面が表示されます。❶［ファイルとフォルダー］をクリックし、❷［追加］ボタンをクリックします。



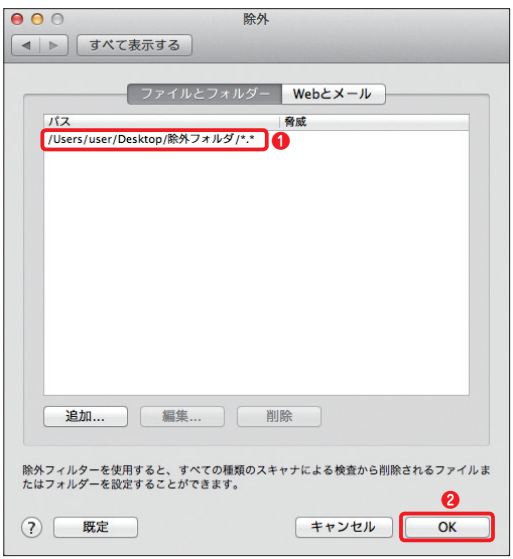
5

［▶］をクリックします。



6

❶除外したいフォルダーをクリックし、❷［OK］ボタンをクリックします。



7

❶選択したフォルダーが除外リストに登録されます。❷登録を終了する場合は、［OK］ボタンをクリックします。

POINT

既定値では「*.*」となりますが「*」とすることで拡張子のないファイルも対象に含まれます。

設定 ▸▸ サイズと検査時間

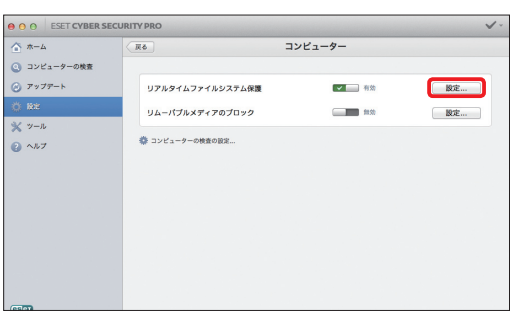
6-5 検査ファイルのサイズと時間を設定するには

P C

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。

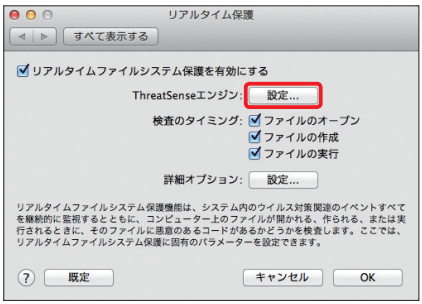
1

メインウィンドウを開き、❶［設定］ボタンをクリックし、❷［コンピューター］をクリックします。



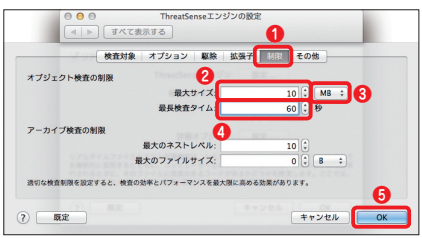
2

リアルタイムファイルシステム保護の［設定］ボタンをクリックします。



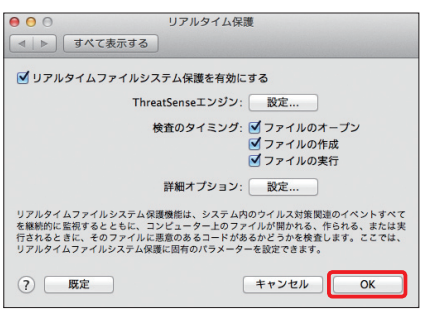
3

「リアルタイム保護」画面が表示されます。「ThreatSense エンジン」の［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オブジェクト（ファイル）の最大サイズを入力し、❸右のドロップダウンリストから単位を選択します。❹最大検査時間（秒単位）を入力し、❺［OK］ボタンをクリックします。



5

［リアルタイム保護］画面に戻ります。［OK］ボタンをクリックします。

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。

設定 ▸▸ 階層の制限

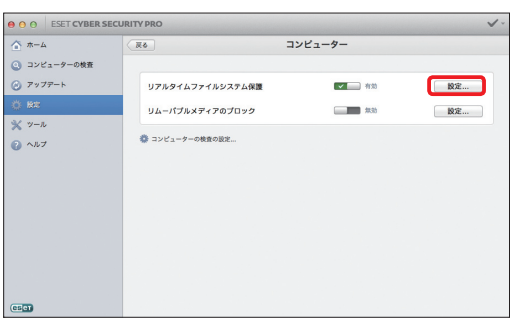
6-6 検査対象とする圧縮ファイルの階層とサイズを制限するには

P C

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。

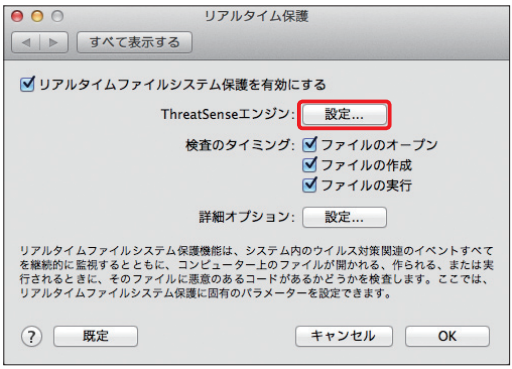
1

メインウィンドウを開き、❶［設定］ボタンをクリックし、❷［コンピューター］をクリックします。



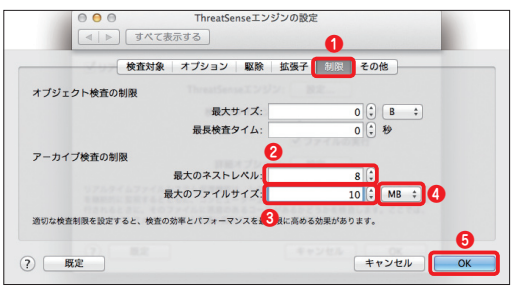
2

リアルタイムファイルシステム保護の［設定］ボタンをクリックします。



3

［リアルタイム保護］画面が表示されます。「ThreatSense エンジン」の［設定］ボタンをクリックします。



4

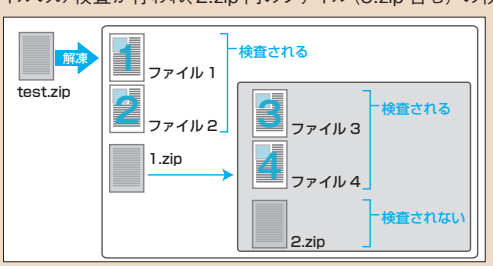
❶［制限］をクリックします。❷スキャン対象の最大ネストレベル（階層数）を入力し、❸最大ファイルサイズを入力します。❹右のドロップダウンリストから単位を選択します。❺［OK］ボタンをクリックします。

5

［リアルタイム保護］画面に戻ります。［OK］ボタンをクリックします。

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

設定 ▸▸ 駆除方法

6-7 P C ウイルスを検出したときの駆除の方法を設定するには

ウイルスを検出したときの動作には、「駆除なし」「標準的な駆除」「厳密な駆除」の３種類があります。ここでは、設定を変更する方法を紹介します。

1

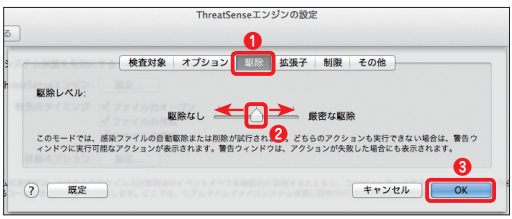
メインウィンドウを開き、❶［設定］ボタンをクリックし、❷［詳細設定を表示する］をクリックします。

2

「詳細設定」画面が表示されます。ここでは、例として［リアルタイム保護］の設定を変更します。［リアルタイム保護］ボタンをクリックします。

3

［設定］ボタンをクリックします。



4

❶［駆除］をクリックし、❷スライドバーをドラッグして駆除の方法を設定して、❸［OK］ボタンをクリックします。

5

［システム保護］画面に戻ります。［すべて表示する］ボタンをクリックします。

POINT

ウイルス駆除方法は、各保護機能ごとに設定できます。

コラム

駆除レベルについて

駆除レベルには、「駆除なし」「標準的な駆除」「厳密な駆除」の 3 種類があり、それぞれ以下のような特徴があります。

レベル	特徴
駆除なし	感染ファイルの自動駆除を行いません。ウイルスなどを検出したときは、警告画面が表示され、動作をユーザーが選択できます。
標準的な駆除	感染ファイルの自動駆除または削除を試行します。適切な動作が選択できなかったときは、ユーザーがその後の動作を選択できます。
厳密な削除	システムファイルを除く、すべての感染ファイルが自動的に駆除または削除されます。圧縮ファイル内にあるファイルが感染していた場合は、圧縮ファイル全体が削除されるので注意してください。

設定 ▸▸ 権限ユーザー

6-8 権限ユーザーの追加と削除

P C

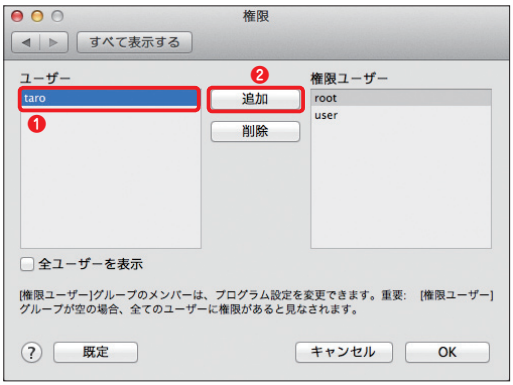
本プログラムは、「権限ユーザー」に登録されたユーザーアカウントのみが各種設定を変更できます。ここでは、権限ユーザーの登録 / 削除の方法を紹介します。

1

メインウィンドウを開き、❶［設定］ボタンをクリックし、❷［詳細設定を表示する］をクリックします。

2

「詳細設定」画面が表示されます。［権限］ボタンをクリックします。



3

❶設定の変更を許可したいユーザーを「ユーザー」グループから選択し、❷「追加」ボタンをクリックします。

4

❶選択したユーザーが「権限ユーザー」グループに追加されました。❷［OK］ボタンをクリックします。

POINT

本プログラムの各種設定を変更できるのは、「権限ユーザー」グループに登録されたユーザーアカウントのみです。ここでは、「権限ユーザー」グループに登録する方法を説明しましたが、「権限ユーザー」グループに登録されたユーザーを削除したいときは、「権限ユーザー」グループから削除したいユーザーを選択し、［削除］ボタンをクリックします。また、「権限ユーザー」グループから全てのユーザーを削除すると全てのユーザーに設定変更を行う権限があるとみなされます。

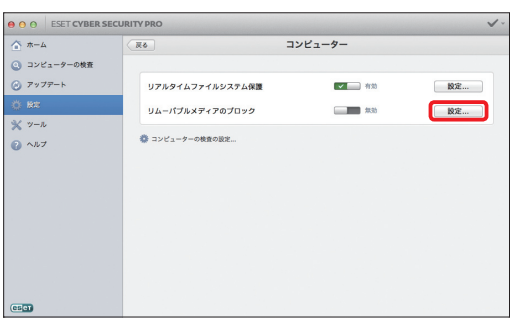
設定 ▸▸ アクセス禁止

6-9 P C リムーバブルメディアへのアクセスを禁止するには

本プログラムには、CD/DVD や USB メモリーなどのリムーバブルメディアの接続を自動的に遮断する機能を搭載しています。ここでは、その設定方法を紹介します。

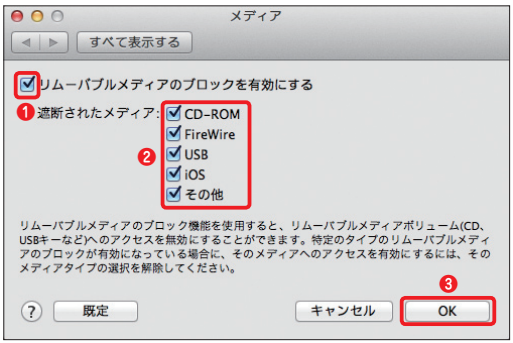
1

メインウィンドウを開き、❶［設定］ボタンをクリックし、❷［コンピューター］をクリックします。



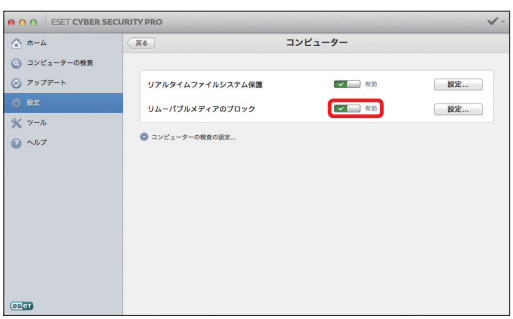
2

リムーバブルメディアのブロックの［設定］ボタンをクリックします。



3

❶［リムーバブルメディアのブロックを有効にする］にチェックを入れ、❷ブロックしたいメディアにチェックを入れます。❸［OK］ボタンをクリックします。



4

リムーバブルメディアのブロックが有効になりました。

設定 ▸▸ インポートとエクスポート

6-10 P C 設定をインポート・エクスポートするには

ここでは、設定をインポート・エクスポートするための手順を紹介します。

1

メインウィンドウを開き、❶［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

設定をファイルに保存するには、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［参照 ...］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

設定をインポートするには、手順②で［設定のインポート］を選択し、［参照...］ボタンをクリックしてインポートする設定ファイルを選択します。

Part.7
「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

7-1 P 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

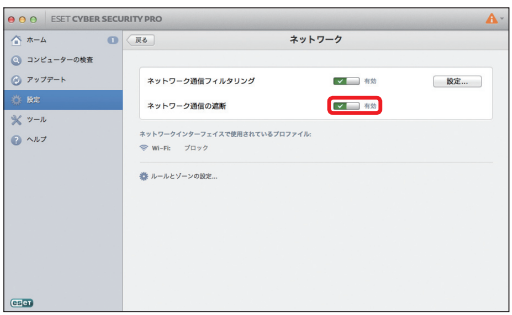
メインウィンドウを開き、❶［設定］ボタンをクリックします。❷［ファイアウォール］をクリックします。

2

［ネットワーク通信の遮断］の［有効／無効］スイッチをクリックします。

3

ダイアログが表示されます。［有効］ボタンをクリックします。



4

ネットワーク通信の遮断が有効になります。

5

❶［ホーム］ボタンをクリックすると、❷ネットワーク通信が遮断されていることが確認できます。❸遮断を無効にしたいときは、［ネットワークトラフィックの遮断を無効にする］をクリックします。

POINT

ネットワーク通信の遮断は、メニューバーの本プログラムのアイコンをクリックし、メニューから［すべてのネットワーク通信を遮断する］をクリックすることでも行えます。

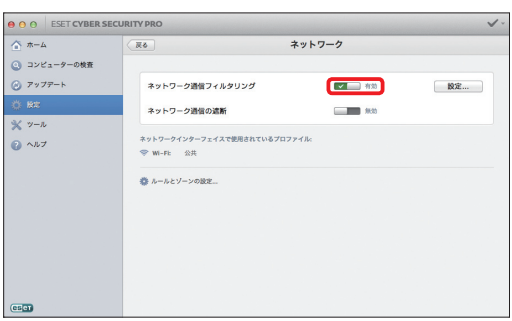
設定 ▸▸ フィルタリングの無効化

7-2 P パーソナルファイアウォールを一時的に無効にするには

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」となることをご承知ください。

1

メインウィンドウを開き、❶［設定］ボタンをクリックし、❷［ファイアウォール］をクリックします。

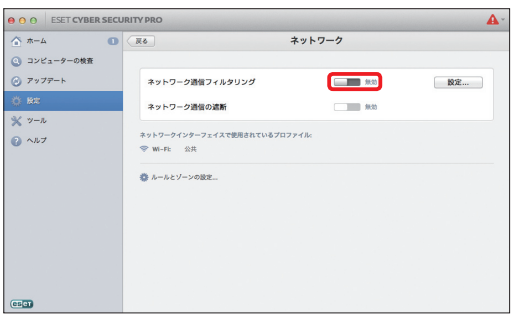


2

［有効／無効］スイッチをクリックします。

3

ダイアログが表示されます。［無効］ボタンをクリックします。



4

パーソナルファイアウォールが無効になります。

5

❶［ホーム］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。❸パーソナルファイアウォールを有効に戻したいときは、［フィルタリングモードを開始する］をクリックします。

POINT

パーソナルファイアウォールの無効化は、メニューバーの本プログラムのアイコンをクリックし、表示されるメニューで［ファイアウォールを無効にする］を選択することでも行えます。

設定 ▸▸ 対話モード

7-3 P 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、ファイアウォールを容易に利用したいユーザー向けの「自動モード」に設定されていますが、通信の可否を手動で選択する「対話モード」も用意されています。

対話モードを設定する

1

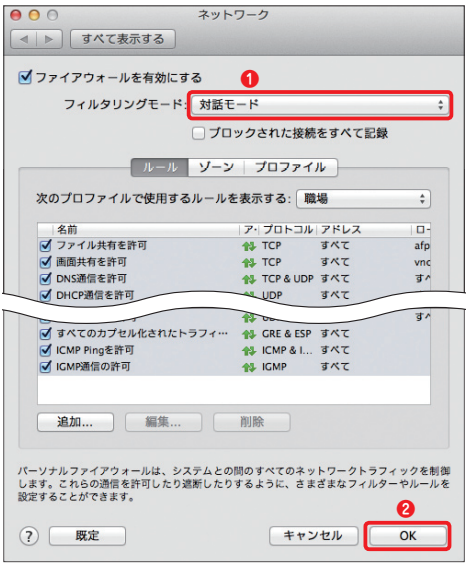
メインウィンドウを開き、❶［設定］ボタンをクリックし、❷［ファイアウォール］をクリックします。

2

［設定］ボタンをクリックします。

POINT

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、一時的なルールにとどめることもできます。



3

［ネットワーク］の設定画面が開きます。❶［フィルタリングモード］のドロップダウンリストで［対話モード］を選択し、❷［OK］ボタンをクリックします。

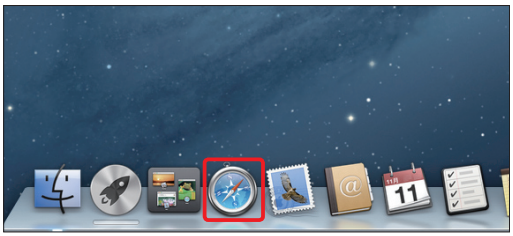
4

新しいネットワークが検出されると、ダイアログが表示されます。❶利用するプロファイルをドロップダウンリストから選択し、❷［OK］ボタンをクリックします。

POINT

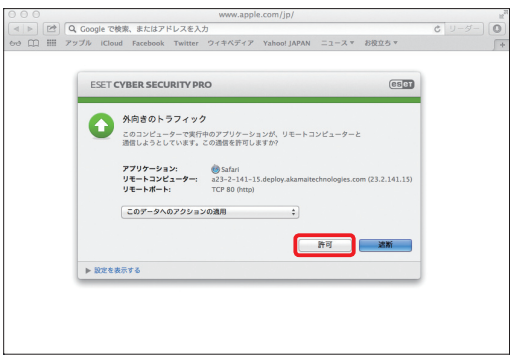
［ネットワークを記憶する］にチェックを入れると、検出したネットワークの設定を新規ゾーンに追加できます。ゾーンの詳細および新規ゾーンの追加については、98 ページ以降をご参照ください。

対話モードの動作を確認する



1

ここでは、「Safari」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。Dock にある［Safari］アイコンをクリックします。



2

Safari 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。［許可］ボタンをクリックするとその通信が許可されます。

POINT

対話モードでは、選択したプロファイルに規定されていない通信が発生するとその通信を許可するかどうかのダイアログが表示されます。［許可］ボタンをクリックするとその通信が許可され、［遮断］ボタンをクリックするとその通信を遮断できます。

発生した通信をルールとして追加する

①

前ページの手順②のダイアログで、❶ドロップダウンリストから［アクションを記憶する（ルールを作成する）］を選択し、❷［許可］ボタンをクリックすると、その通信をルールとして追加できます。

②

手順①のダイアログで［設定を表示する］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できます。

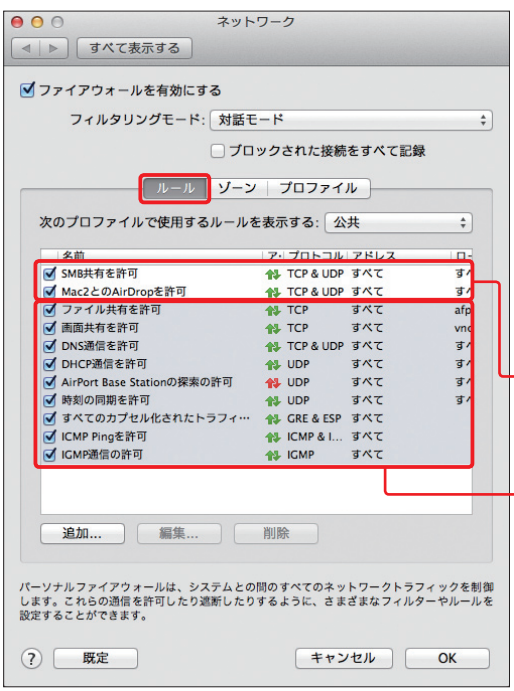
POINT

手順①のダイアログで、［このプロセスに対するアクションを一時的に記憶する］を選択すると、そのルールを一時的に記憶し、パソコンが再起動されるまで同じ通信が発生したときにダイアログを表示しないようにできます。［このデータへのアクションの適用］を選択した場合は、選択したプロファイルに規定されていない通信が発生するたびに、その通信を許可するかどうかのダイアログが表示されます。

設定されているルールを確認するには

1

メインウィンドウを開き、［設定］→［ファイアウォール］とクリックし、［設定］ボタンをクリックします。



2

［ネットワーク］の設定画面が開きます。❶［ルール］が選択されていることを確認します。❷手動で追加したルールが白背景で表示され、既定値で設定されているルールがグレー背景で表示されます。

手動で追加したルール

既定値で設定されているルール

設定 ▸▸ ファイアウォールプロファイル

7-4 P ファイアウォールプロファイルを作成するには

プロファイルは、パーソナルファイアウォールの制御に利用されるルール群です。既定値では、［家庭］［公共］［職場］の３種類のプロファイルが準備されており、新規プロファイルを作成することもできます。

プロファイルを作成する

1

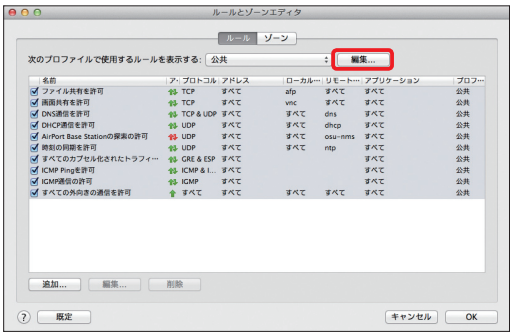
メインウィンドウを開き、❶［設定］ボタンをクリックし、❷［ファイアウォール］をクリックします。

2

［ルールとゾーンの設定］をクリックします。

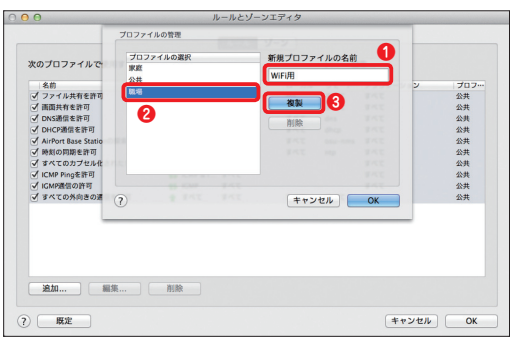
POINT

パーソナルファイアウォールは、プロファイルごとに規定されたルール（パーソナルファイアウォールルール）に基いて各種通信の制御を行います。新規プロファイルは、既定値で準備されている［家庭］［公共］［職場］の３種類のプロファイルのルールを元に作成します。プロファイルの切り替え方法については、98 ページ以降をご参照ください。



3

［ルールとゾーンエディタ］が開きます。［編集］ボタンをクリックします。

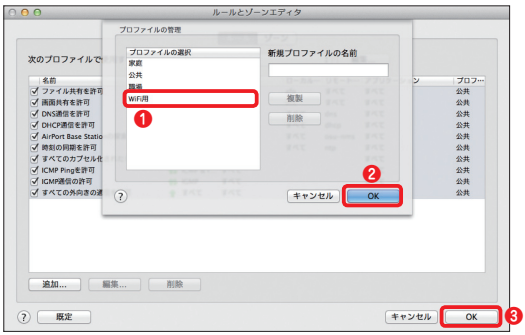


4

［プロファイルの管理］画面が開きます。❶作成するプロファイルの名称を入力し、❷ルールの複製元として利用するプロファイルをクリックします。❸［複製］ボタンをクリックします。

POINT

新規作成したプロファイルには、手順④で選択したプロファイルのルールが既定値として登録され、手動で独自のルールを追加することもできます。



5

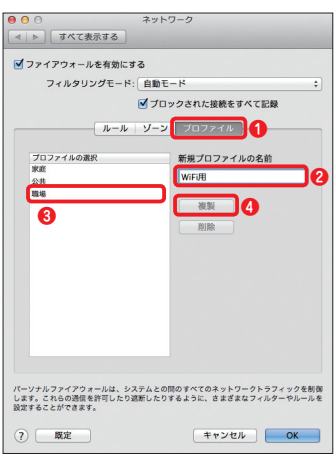
❶プロファイルが登録されます。❷［OK］ボタンをクリックします。［ルールとゾーンエディタ］に戻ります。❸［OK］ボタンをクリックします。

POINT

誤ってプロファイルを登録した場合は、削除したいプロファイルをクリックし、［削除］ボタンをクリックします。なお、既定値で登録されている［家庭］［公共］［職場］の３種類のプロファイルは削除できません。

コラム

［ネットワーク］画面からプロファイルを登録する



新規プロファイルの登録は、［ネットワーク］画面からも行えます。［ネットワーク］画面から登録を行うときは、メインウィンドウを開き、［設定］→［ファイアウォール］とクリックし、［設定］ボタンをクリックします。［ネットワーク］画面が開いたら、❶［プロファイル］をクリックし、❷作成するプロファイルの名称を入力して、❸ルールの複製元として利用するプロファイルをクリックします。❹［複製］ボタンをクリックすると、プロファイルが登録されます。

設定 ▸▸ カスタムルール

7-5 P 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

無線 LAN 対応プリンターなどの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、プロファイルに手動でカスタムルールを登録します。

1

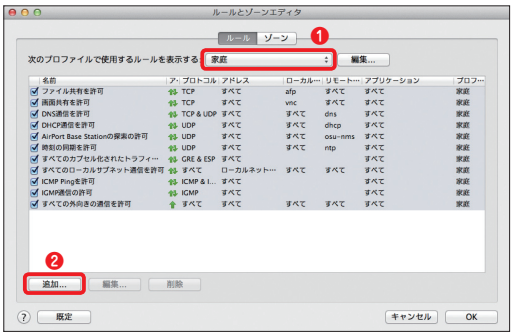
メインウィンドウを開き、❶［設定］ボタンをクリックし、❷［ファイアウォール］をクリックします。

POINT

カスタムルールの作成は、プロファイルごとに行う必要があります。また、カスタムルールは、手動で作成できるほか、対話モードで作成することもできます。対話モードを利用したルールの作成方法は、87 ページをご参照ください。

2

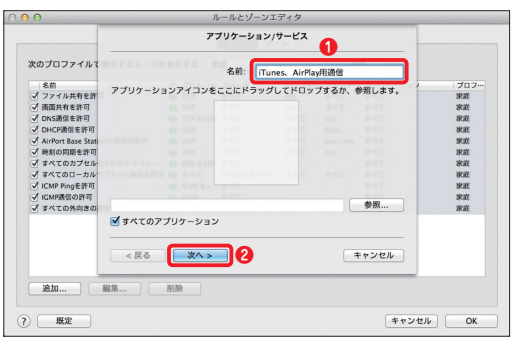
［ルールとゾーンの設定］をクリックします。



3

［ルールとゾーンエディタ］が開きます。❶カスタムルールを登録したいプロファイルをドロップダウンリストから選択し、❷［追加］ボタンをクリックします。

ここでは、「iTunes、AirPlay用通信」の設定を例に手順を紹介します。

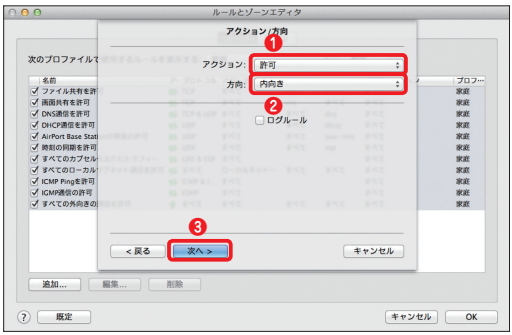


4

［アプリケーション/サービス］画面が開きます。❶新規ルールに付ける［名前］を入力し、❷［次へ］ボタンをクリックします。

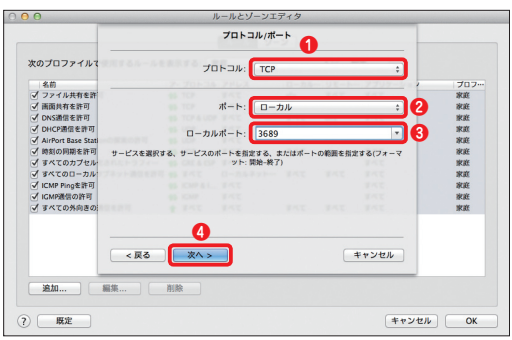
POINT

［すべてのアプリケーション］のチェックを外し、［参照］ボタンをクリックして、アプリケーションの実行ファイルを選択すると、そのアプリケーションのみが利用できるルールを作成できます。



5

❶通信を許可するかどうかを設定するアクションを設定（ここでは、［許可］）し、❷データの流れの方向を示す方向（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［内向き］）を設定します。❸［次へ］ボタンをクリックします。

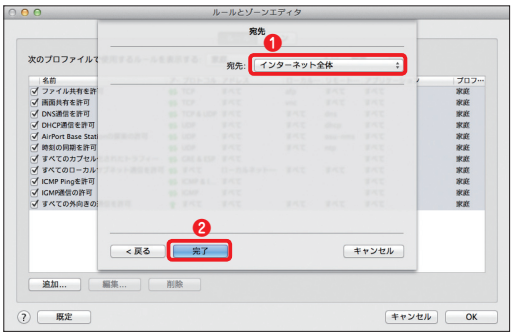


6

プロトコル / ポートの設定を行います。❶プロトコル（ここでは、ドロップダウンリストから「TCP」プロトコル）を選択します。❷ポート（ここでは、ドロップダウンリストから［ローカル］）を選択します。❸ポート番号を入力するか、ドロップダウンリストからサービス名を選択します。ここでは、［3689］を入力します。❹［次へ］ボタンをクリックします。

POINT

ここでは、特定のポート番号への外部からの接続を許可しているので、「ローカルポート」の設定を行っています。

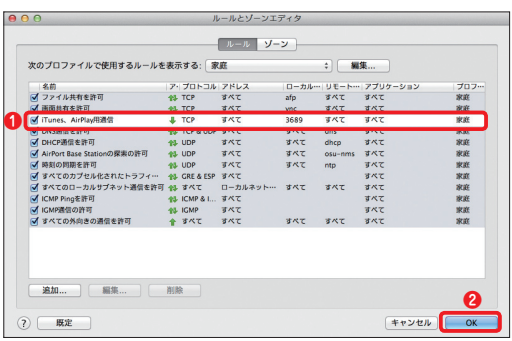


7

❶宛先（ここでは、［インターネット全体］）を選択し、❷［完了］ボタンをクリックします。

POINT

宛先は、「IP アドレス」「IP アドレス範囲」「サブネット」「ローカルネットワーク」「インターネット全体」から選択できます。



8

❶［ルールとゾーンエディア］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

手動登録したルールは、白背景で表示され、既定値で登録されているルールは、グレーの背景で表示されます。また、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 ▸▸ ルールの有効／無効の切り替え

7-6 P 利用するルールの有効／無効を切り替えるには

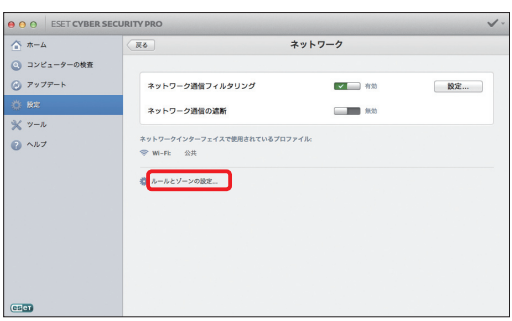
各プロファイルに登録されているルール（パーソナルファイアウォールルール）は、必要に応じて有効 / 無効を切り替えることができます。ここでは、ルールの有効 / 無効の切り替え方法を説明します。

1

メインウィンドウを開き、❶［設定］ボタンをクリックし、❷［ファイアウォール］をクリックします。

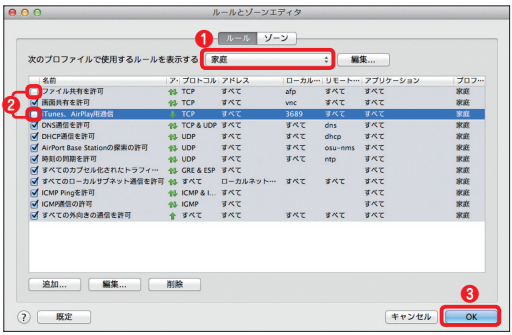
POINT

ルールの有効 / 無効の切り替えは、プロファイルごとに設定を行う必要があります。



2

［ルールとゾーンの設定］をクリックします。



3

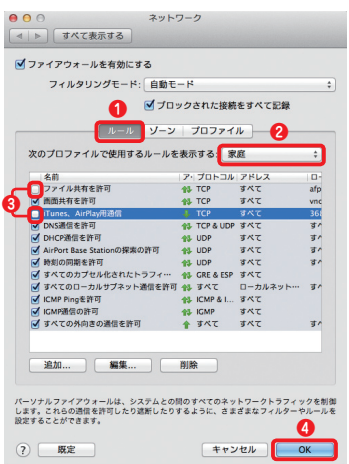
［ルールとゾーンエディタ］が開きます。❶ルールの有効 / 無効を選択したいプロファイルをドロップダウンリストから選択し、❷無効にしたいルールのチェックを外します。❸［OK］ボタンをクリックします。

POINT

既定値では、すべてのルールにチェックが入っており、有効な状態に設定されています。

コラム

［ネットワーク］画面からルールの有効 / 無効を設定する



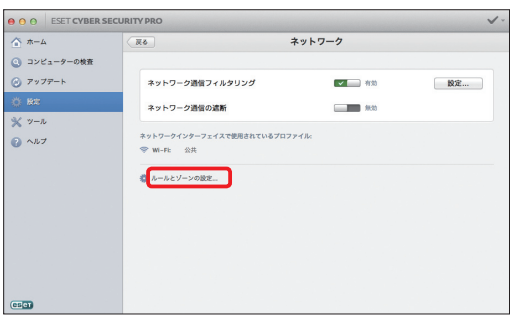
ルールの有効 / 無効の切り替えは、［ネットワーク］画面からも行えます。［ネットワーク］画面から登録を行うときは、メインウィンドウを開き、［設定］→［ファイアウォール］とクリックし、［設定］ボタンをクリックします。［ネットワーク］画面が開いたら、❶［ルール］が選択されていることを確認し、❷プロファイルを選択します。❸無効にしたいルールのチェックを外し、❹［OK］ボタンをクリックします。

設定 ▸▸ プロファイルの切り替え

7-7 P ファイアウォールプロファイルの自動切り替えを行うには

パーソナルファイアウォールは、あらかじめ登録しておいたネットワークの条件（アクティベーター）によって使用するプロファイルを自動的に切り替えることができます。ここでは、その設定方法を説明します。

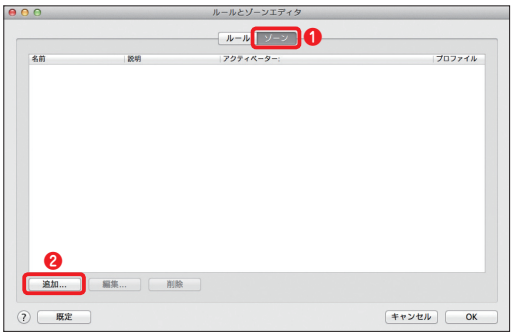
1 メインウィンドウを開き、❶［設定］ボタンをクリックし、❷［ファイアウォール］をクリックします。



2 ［ルールとゾーンの設定］をクリックします。

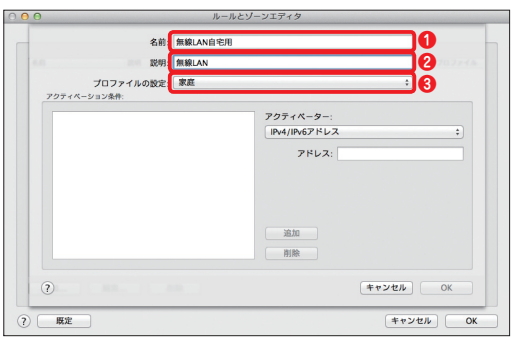
POINT

現在利用中のプロファイルは、［ネットワークインターフェイスで使用されているプロファイル］で確認できます。



3

［ルールとゾーンエディタ］が開きます。❶［ゾーン］をクリックし、❷［追加］ボタンをクリックします。



4

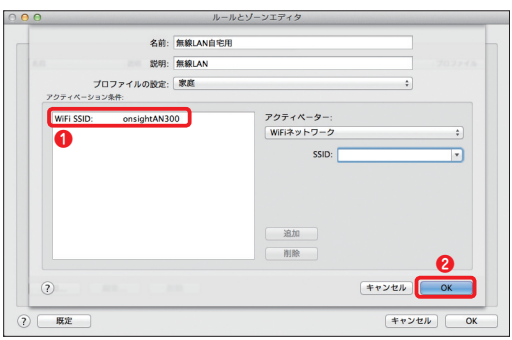
ここでは、自宅の無線LANに接続したときに［家庭］プロファイルでパーソナルファイアウォールを管理し、それ以外の場所では、［公共］プロファイルで管理する方法を紹介します。❶［名前］欄に作成するゾーンの名称を入力し、❷［説明］欄にゾーンの説明を入力します。❸［プロファイルの設定］のドロップダウンリストから利用するプロファイル（ここでは、［家庭］）を選択します。

5

❶［アクティベーター］のドロップダウンリストからアクティベーター（ここでは、［WiFi ネットワーク］）を選択し、❷［SSID］のドロップダウンリストから接続に使用する SSID を選択します。❸［追加］ボタンをクリックします。

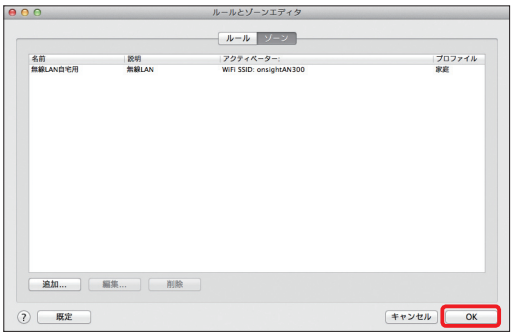
POINT

ここでは、WiFi ネットワークの SSID を条件に利用してプロファイルの設定を変更する方法を紹介しています。［アクティベーター］の設定は、WiFi ネットワークだけでなく、IPv4/IPv6 アドレスやアドレス範囲、サブネット、インターフェースなどを条件に指定できます。詳細については、102 ページをご参照ください。



6

❶プロファイルを切り替えるための条件が登録されます。❷［OK］ボタンをクリックします。



7

［ルールとゾーンエディタ］に戻ります。［OK］ボタンをクリックします。

POINT

ゾーンを選択して、［編集］ボタンをクリックすると、そのゾーンに関する編集が行えます。また、［削除］ボタンをクリックすると、そのゾーンを削除できます。また、［既定］ボタンをクリックすると、［ルールとゾーンエディタ］で設定したすべての内容を既定値に戻します。

8

接続したネットワークが条件（ここでは、指定したSSIDによるWi-Fiネットワークに接続されたとき）を満たすと、プロファイルが自動的に切り替わります。

POINT

ゾーンの登録は、［ネットワーク］画面からも行えます。［ネットワーク］画面から登録を行うときは、メインウィンドウを開き、［設定］→［ファイアウォール］とクリックし、［設定］ボタンをクリックします。［ネットワーク］画面が開いたら、［ゾーン］→［追加］ボタンとクリックして、手順④～⑦を参考にゾーンの登録を行います。

コラム

アクティベーターについて

プロファイルの切替条件として設定するアクティベーターは、複数の条件を登録できます。ただし、複数の条件を登録したときは、指定した条件のうちいずれか 1 つを満たすとプロファイルが切り替わります。指定した条件をすべて満たした場合ではない点に注意してください。また、アクティベーターは、以下の 5 種類の中から選択できます。

アクティベーター	内容
IPv4/IPv6 アドレス	単一の IPv4 または IPv6 アドレスを指定します。特定の IP アドレスで利用しているときにプロファイルを切り替えたいときに利用します。
IPv4/IPv6 アドレス範囲	IPv4 または IPv6 のアドレス範囲で指定します。範囲の設定は、開始アドレスと終了アドレスで指定します。指定範囲の IP アドレスを利用している場合にプロファイルが切り替わります。
IPv4/IPv6 サブネット	IPv4 または IPv6 の管理単位で指定します。設定を行うときは、ネットワークアドレス（例えば、192.168.1.0）とサブネットマスク（例えば、24 ビット）で設定します。この管理単位内の IP アドレスを利用している場合にプロファイルが切り替わります。
WiFi ネットワーク	無線 LAN のネットワークを指定します。指定は、SSID（ESSID）で設定します。指定した SSID（ESSID）の無線 LAN に接続するとプロファイルが切り替わります。
インターフェース	ネットワークの接続に利用するインターフェース単位で設定します。たとえば、イーサネットや WiFi などで設定を行います。インターネットなどを指定したインターフェースで利用してしているときにプロファイルが切り替わります。

Part.8
「設定」画面での操作 3
（Webとメール編）

ここでは、本プログラムの「設定」画面における「Web とメール」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 ▸▸ Web 保護一時無効

8-1 Web アクセス保護を一時的に無効にするには

P C

Web サイトの閲覧にいつも以上に時間がかかったり、サイトそのものが開けなかったりするときは、一時的に本機能を無効にして動作を確認してみましょう。

1

メインウィンドウを開き、❶［設定］ボタンをクリックして、❷［Web とメール］をクリックします。

2

［Web アクセス保護］の［有効／無効］スイッチをクリックします。

3

ダイアログが表示されます。［無効］ボタンをクリックします。

4

Web アクセス保護が無効になります。

5

❶［ホーム］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。❸［Web アクセス保護を有効にする］をクリックすると、Web アクセス保護が有効になります。

設定 ▸▸ 閲覧制限

8-2 Web ページの閲覧を制限するには

P C

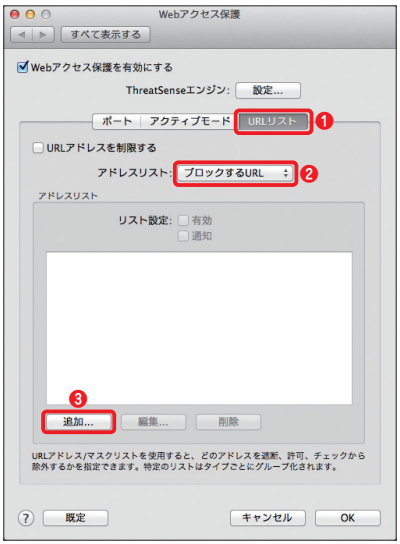
本プログラムは、特定の Web ページの閲覧を制限したり、登録した Web ページ以外を閲覧できないように設定できます。ここでは、その方法を説明します。

1

ここでは、一例として「http://www.example.com」のドメイン全体の閲覧を制限します。メインウィンドウを開き、❶［設定］ボタンをクリックして、❷［Web とメール］をクリックします。

2

［Web アクセス保護］の［設定］ボタンをクリックします。



3

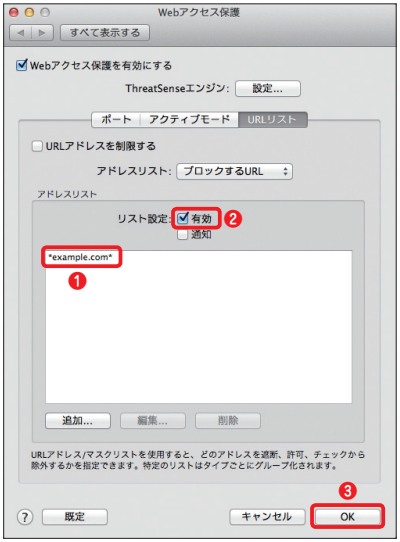
❶［URL リスト］をクリックします。❷［アドレスリスト］のドロップダウンリストで［ブロックする URL］を選択し、❸［追加］ボタンをクリックします。

4

❶登録したいURLアドレス（ここでは、「*example.com*」）を入力し、❷［OK］ボタンをクリックします。

POINT

ドメイン全体を対象とするときは、ドメイン名を「*（アスタリスク）で囲み「*example.com*」の形式で入力します。「http://www.example.com」と入力すると、トップページのみが対象となり、ファイル名（.html）まで指定するとそのページのみが、対象となります。ドメイン内の特定のパスを対象とするときは、「http://www.example.com/test/*.*」の形式で入力します。

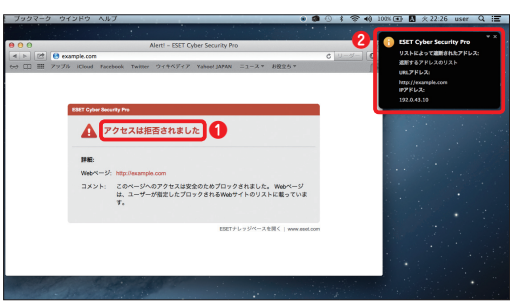


5

❶ URL アドレスがリストに登録されます。複数の Web ページを登録したい場合は、手順③④の作業を繰り返します。すべての Web ページを登録したら、❷［リスト設定］の［有効］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。

POINT

登録した URL アドレスを削除したいときは、削除したい URL をクリックし、［削除］ボタンをクリックします。また、［編集］ボタンをクリックすると、選択した URL アドレスを編集できます。



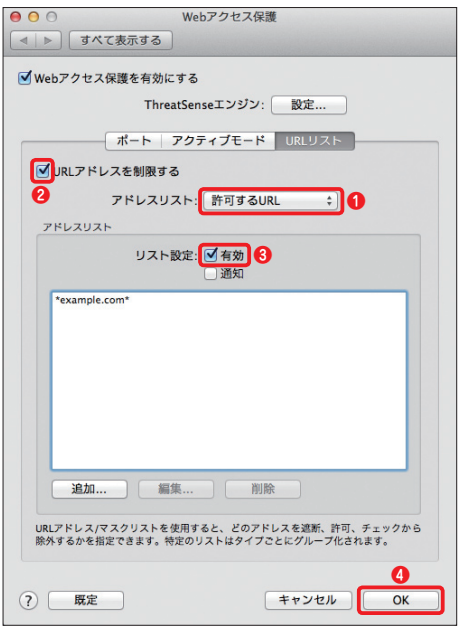
6

閲覧を制限されたWebページにアクセスすると、❶［アクセスは拒否されました］と画面に表示されます。また、手順⑤の画面で、［通知］にチェックを入れると、❷画面右上に通知画面が表示されます。

コラム

特定の Web ページのみ閲覧を許可するには

特定の Web ページの閲覧のみを許可したいときは、❶［アドレスリスト］のドロップダウンリストで［許可する URL］を選択し、手順④を参考に許可したい URL アドレスを登録します。❷［URL アドレスを制限する］にチェックを入れ、❸［リスト設定］の［有効］をクリックしてチェックを入れます。❹［OK］ボタンをクリックします。



設定 ▸▸ メール保護一時無効

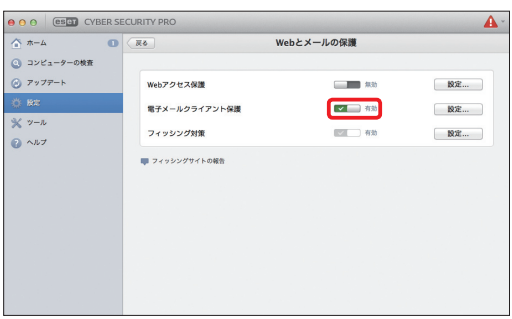
8-3 電子メールクライアント保護を一時的に無効にするには

P C

メールの送受信に失敗する頻度が高いなど、本プログラムの保護機能が原因と疑われるときは、一時的に電子メールクライアント保護を無効にして動作を確認してみましょう。

1

メインウィンドウを開き、❶［設定］ボタンをクリックして、❷［Web とメール］をクリックします。



2

［電子メールクライアント保護］の［有効］をクリックします。

3

ダイアログが表示されます。［無効］ボタンをクリックします。

4

電子メールクライアント保護が無効になります。

5

❶［ホーム］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。❸［リアルタイムファイルシステム保護を有効にする］をクリックすると、電子メールクライアント保護が有効になります。

設定 ▸▸ プロトコル検査の無効化

8-4 P C Web とメールの検査をしない通信を設定するには

本製品では、Web アクセス保護や電子メールクライアント保護機能を有効にしたまま、Web アクセスやメールの送受信で発生する特定の通信の検査を行わないように設定できます。ここでは、その手順を説明します。

Web アクセスで発生する特定の通信の検査を無効にする

1

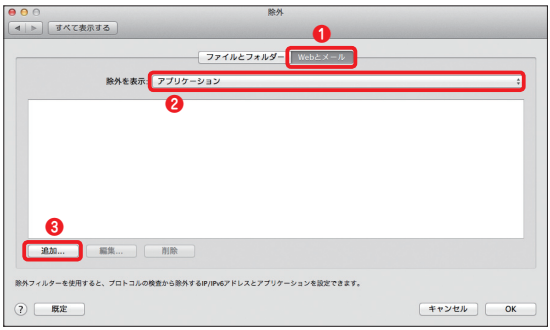
メインウィンドウを開き、❶［設定］ボタンをクリックして、❷［詳細設定を表示する］をクリックします。

2

［全般］ボタンをクリックします。

3

［設定］ボタンをクリックします。

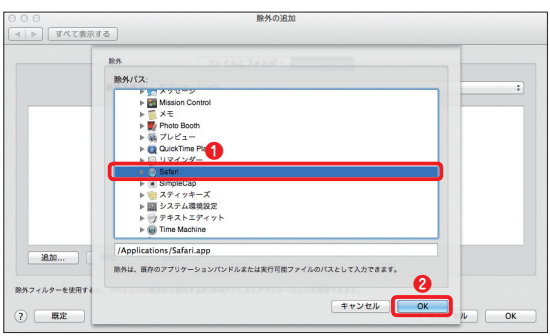


4

❶［Webとメール］をクリックし、アプリケーションを登録する場合は、❷［除外を表示］のドロップダウンリストで［アプリケーション］を選択します。❸［追加］ボタンをクリックします。

POINT

［除外を表示］のドロップダウンリストで［IP/IPv6 アドレス］を選択すると、プロトコル検査を実施しない IP/IPv6 アドレスを設定できます。なお、検査を行わない Web サイトは必ず、「IP アドレス」で登録する必要があります。ドメイン名では、登録できません。



5

検査を行わないアプリケーションに❶Web ブラウザー（ここでは［Safari］）を選択し、❷［OK］ボタンをクリックします。

6

❶選択したアプリケーションがリストに登録されます。❷［OK］ボタンをクリックします。

POINT

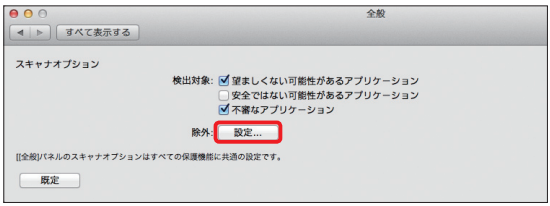
［既定］ボタンをクリックすると、設定を既定値に戻せます。また、登録されたアプリケーションをクリックし、［削除］ボタンをクリックすると、そのアプリケーションを削除できます。

電子メールの送受信で発生する特定の通信の検査を無効にする

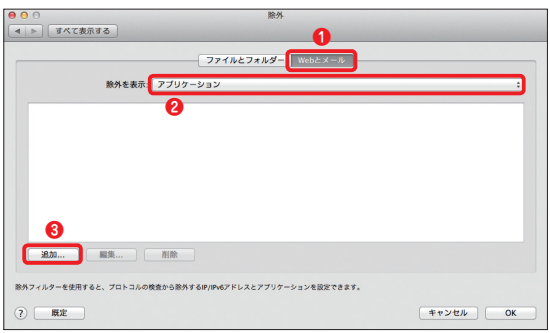
1

メインウィンドウを開き、❶［設定］ボタンをクリックして、❷［詳細設定を表示する］をクリックします。

2 ［全般］ボタンをクリックします。



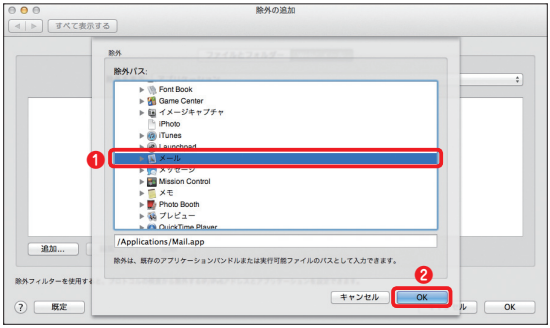
3 ［設定］ボタンをクリックします。



4 ❶［Webとメール］をクリックし、❷［除外を表示］のドロップダウンリストで［アプリケーション］を選択します。❸［追加］ボタンをクリックします。

POINT

［除外を表示］のドロップダウンリストで［IP/IPv6 アドレス］を選択すると、プロトコル検査を実施しない IP/IPv6 アドレスを設定できます。なお、検査を行わない Web サイトは必ず、「IP アドレス」で登録する必要があります。ドメイン名では、登録できません。



5

検査を行わないアプリケーションに❶メールアプリケーション（ここでは［メール］）を選択し、❷［OK］ボタンをクリックします。

6

❶選択したアプリケーションがリストに登録されます。❷［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、設定を既定値に戻せます。また、登録されたアプリケーションをクリックし、［削除］ボタンをクリックすると、そのアプリケーションを削除できます。

Part.9
「設定」画面での操作 4
（ペアレンタルコントロール編）

ここでは、本プログラムの「設定」画面における「ペアレンタルコントロール」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 ▸▸ 一時無効

9-1 P ペアレンタルコントロール（保護者機能）とは

ペアレンタルコントロール（保護者機能）を利用すると、子供や青少年が閲覧できる Web ページを制限できます。ここでは、ペアレンタルコントロールの概要と有効／無効の切り替えについて説明します。

ペアレンタルコントロールの有効 / 無効を切り替える

1

ペアレンタルコントロールの対象となっているユーザーが、許可されていないカテゴリの Web ページを開くと、左のような画面が表示されます。

2

ペアレンタルコントロールを無効にするときは、メインウィンドウを開き、❶［設定］ボタンをクリックして、❷［ペアレンタルコントロール］をクリックします。

3

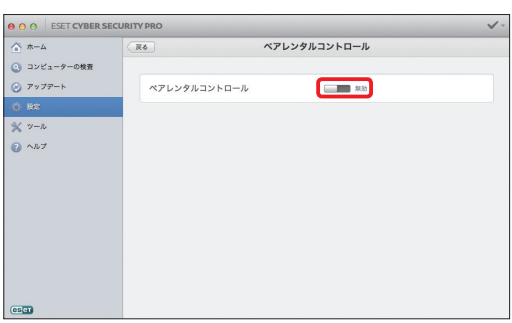
［ペアレンタルコントロール］の［有効／無効］スイッチをクリックします。

POINT

本プログラムの既定値では、ペアレンタルコントロール機能は無効に設定されています。

4

ダイアログが表示されます。［無効］ボタンをクリックします。



5

ペアレンタルコントロールが無効になります。

6

❶［ホーム］ボタンをクリックすると、❷ペアレンタルコントロールが無効に設定されていることが確認できます。

ユーザーごとに有効 / 無効を切り替える

1

メインウィンドウを開き、❶［設定］ボタンをクリックして、❷［ペアレンタルコントロール］をクリックします。

2

ペアレンタルコントロールを無効にしたいユーザーの［有効／無効］スイッチをクリックします。

3

選択したユーザーのペアレンタルコントロールが無効になります。再度有効にしたいときは、再度［有効／無効］スイッチをクリックします。

コラム

ペアレンタルコントロールを設定する

本プログラムの既定値では、ペアレンタルコントロール機能は無効に設定されています。ペアレンタルコントロールを利用するときは、以下の手順で設定します。なお、この機能を利用する場合は、保護者用の管理者ユーザーアカウントと児童や青少年用の標準ユーザーアカウントをそれぞれ作成し、マルチユーザーで 1 台のコンピューターを利用することをお勧めします。また、設定に際しては、本プログラムの設定変更が簡単に行えないように、権限ユーザーの設定を行ってください。

1

メインウィンドウを開き、［設定］→［ペアレンタルコントロール］とクリックします。［ペアレンタルコントロール］の［有効／無効］スイッチをクリックします。

2

❶ペアレンタルコントロールを利用するユーザーの［有効／無効］スイッチをクリックします。❷ 122 ページ以降の手順を参考に、ペアレンタルコントロールを利用するユーザーの［設定］ボタンをクリックし、閲覧を許可する項目の設定を行います。

設定 ▸▸ 許可項目

9-2 P 閲覧を許可する項目を設定するには

ペアレンタルコントロールでは、本プログラムがあらかじめ準備している項目ごとに閲覧の可否を設定します。ここでは、閲覧を許可する項目の設定手順を紹介します。

1

メインウィンドウを開いて、❶［設定］ボタンをクリックし、❷［ペアレンタルコントロール］をクリックします。

2

項目を設定したいユーザーの［設定］ボタンをクリックします。

3

はじめて設定を行う場合またはプロファイルを変更したいときは、設定プロファイルのドロップダウンリストから利用するプロファイルを選択します。閲覧項目の変更を行う場合は、手順④に進みます。

4

❶許可したい項目にチェックを入れ、❷［OK］ボタンをクリックします。

POINT

表示されている項目の上にマウスポインターを置くと、その項目の詳細な内容が右側のウィンドウに表示されます。

設定 ▸▸ 例外ページの登録

9-3 P Web ページの例外を登録するには

特定の Web ページを常に閲覧可能または閲覧不可にするには、その Web ページを事前に例外登録しておきます。ここでは、特定の Web ページを例外として登録する手順を紹介します。

例外を設定する

1 メインウィンドウを開いて、❶［設定］ボタンをクリックし、❷［ペアレンタルコントロール］をクリックします。

2 ［Web ページの例外を設定］をクリックします。

3

常に閲覧可能な Web ページを登録するときは、❶登録したい Web ページの URL を入力し、❷対象とするユーザーのアクションに［許可］を設定します。❸［OK］ボタンをクリックします。

4

常に閲覧不可の Web ページを登録するときは、❶登録したい Web ページの URL を入力し、❷対象とするユーザーのアクションに［遮断］を設定し、❸［OK］ボタンをクリックします。

登録した例外ページを確認する

1

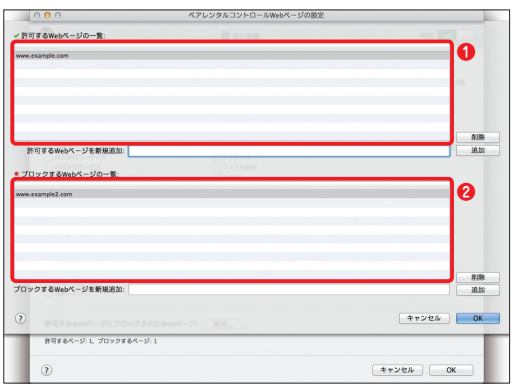
メインウィンドウを開いて、❶［設定］ボタンをクリックし、❷［ペアレンタルコントロール］をクリックします。

2

設定を確認したいユーザーの［設定］ボタンをクリックします。

3

［許可するWebページとブロックするWebページ］の［設定］ボタンをクリックします。



4

❶許可するWebページと❷ブロックするWebページの一覧が表示されます。

POINT

［許可するWebページを新規追加］または［ブロックするWebページを新規追加］の欄にURLを入力し、［追加］ボタンをクリックすると、許可またはブロックするWebページを追加できます。また、登録されているWebページをクリックし、［削除］ボタンをクリックするとそのWebページの登録を削除できます。

設定 ▸▸ アカウント追加

9-4 P ユーザーアカウントを追加するには

ペアレンタルコントロールで制御するユーザーアカウントは、以下の手順追加できます。

1

メインウィンドウを開いて、❶［設定］ボタンをクリックし、❷［ペアレンタルコントロール］をクリックします。

2

［新しいユーザーアカウントを作成］をクリックします。Mac OS のアカウント設定画面が開きます。新しいユーザーアカウントを作成してください。

3

メインウィンドウを開き、［設定］→［ペアレンタルコントロール］とクリックすると、ペアレンタルコントロールに作成したユーザーが追加されていることが確認できます。

POINT

［ロールが未定義です］をクリックし、ドロップダウンリストから利用するプロファイルを選択すると、そのユーザーのペアレンタルコントロールが有効になります。また、手順③の画面に登録したユーザーが表示されないときは、本プログラムのメインウィンドウを一度閉じ、再度開き直すか、OS を再起動してメインウィンドウを開き直してください。

Part.10
「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 ▸▸ ログの閲覧

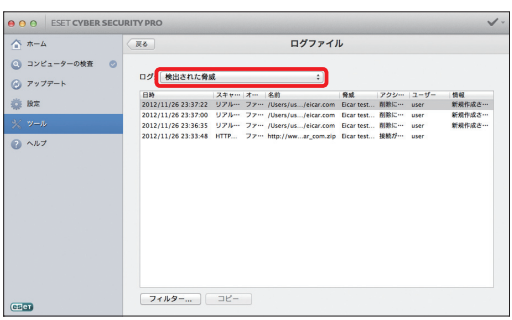
10-1 詳細なログファイルを確認するには

P C

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」のプライマリウィンドウから参照します。

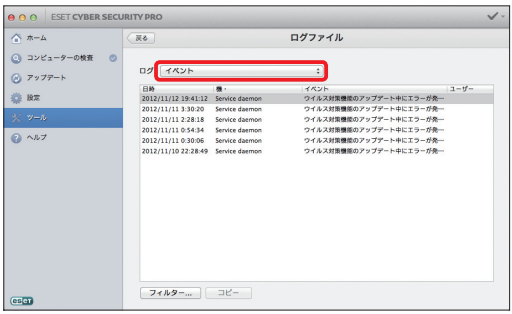
1

メインウィンドウを開き、❶［ツール］ボタンをクリックし、❷［ログファイル］をクリックします。



2

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」を選択した場合、発見したウイルスが表示されます。

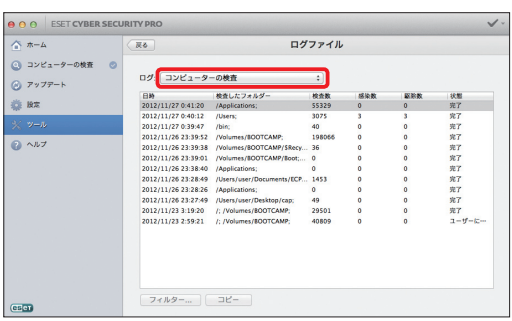


3

「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。

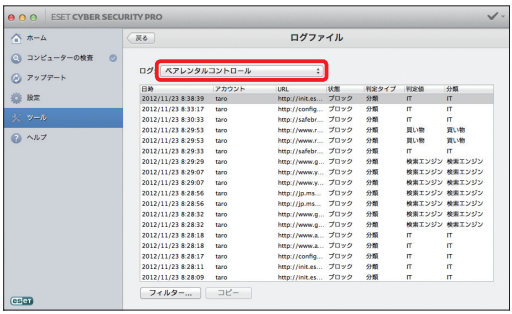
POINT

閲覧できるログは「検出された脅威」「イベント」「コンピューターの検査」「ペアレンタルコントロール（ESET Cyber Security Proのみ）」「ファイアウォール（ESET Cyber Security Proのみ）」の5種類です。



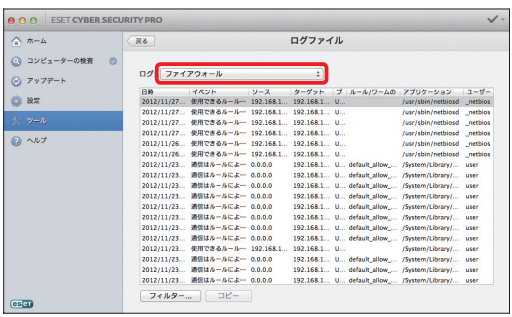
4

「ログ」のドロップダウンリストから［コンピューターの検査］を選ぶと、コンピューター検査の結果を確認できます。



5

［ログ］のドロップダウンリストから［ペアレンタルコントロール］を選ぶと、ペアレンタルコントロールによってブロックされた Web サイトなどを確認できます。



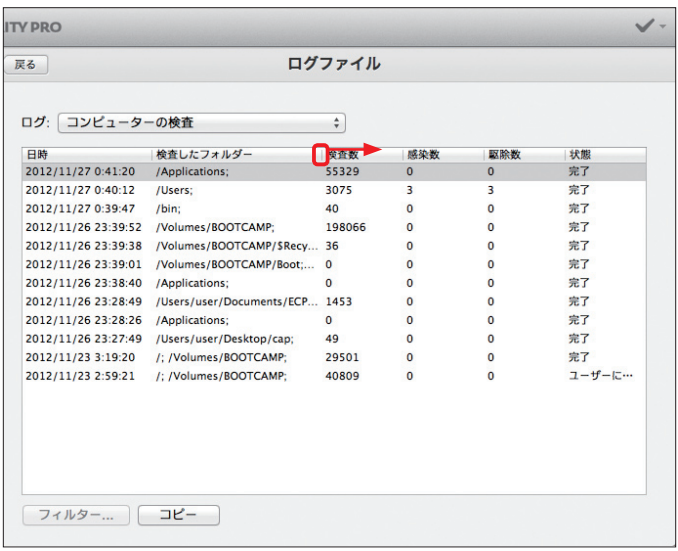
6

［ログ］のドロップダウンリストから［ファイアウォール］を選ぶと、パーソナルファイアウォールが遮断した通信の情報などを確認できます。

コラム

表示領域を変更するには

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 ▸▸ ログファイルの詳細設定

10-2 P C ログファイルの詳細設定を行うには

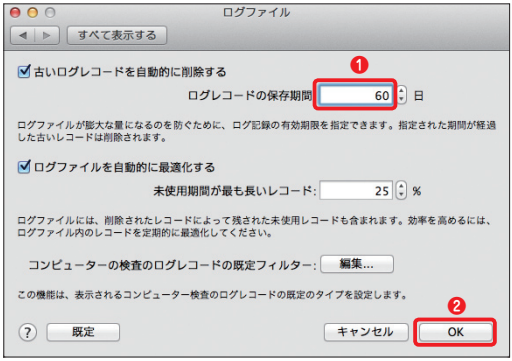
本プログラムの既定値では、各種ログの保存期間を「90 日」に設定しています。ここでは、ログの保存期間の変更手順を紹介します。

1

メインウィンドウを開き、❶［設定］ボタンをクリックし、❷［詳細設定を表示する］をクリックします。

2

［ログファイル］ボタンをクリックします。



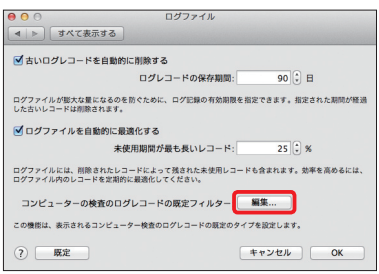
3

［ログファイル］ダイアログが表示されます。❶ログレコードの保存期間を入力し、❷［OK］ボタンをクリックします。

コラム

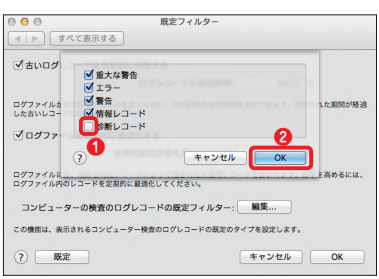
既定値で表示されるログの内容を変更するには

既定値で表示されるログの内容を変更したいときは、以下の手順で行います。



1

［コンピューターの検査のログレコードの既定フィルター］の［編集］ボタンをクリックします。



2

❶既定値で表示したくないフィルターのチェックを外し、❷［OK］ボタンをクリックします。

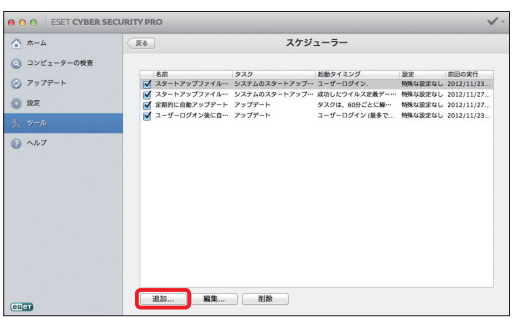
ツール ▸▸ スケジュール設定

10-3 P C 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を追加できます。

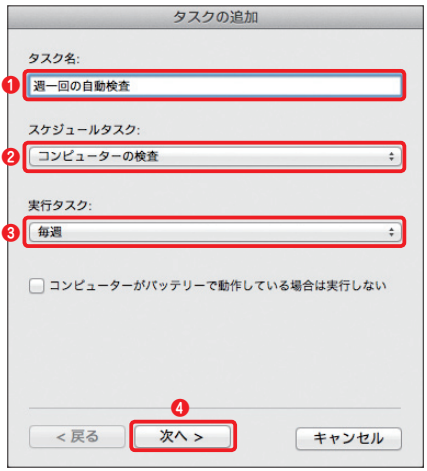
1

メインウィンドウを開き、❶［ツール］ボタンをクリックします。❷［スケジューラー］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。ここでは、例として毎週日曜日にコンピューターの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

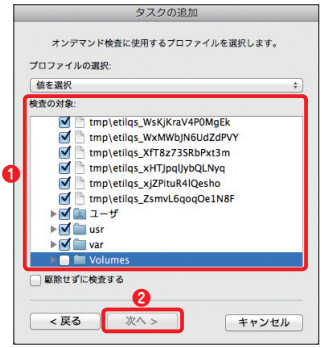
「タスクの追加」画面が表示されます。❶タスク名を入力し、❷スケージュールタスクのドロップダウンリストから［コンピューターの検査］を選択して、❸実行タスクのドロップダウンリストから［毎週］を選択します。❹［次へ］ボタンをクリックします。

4

❶プロファイルの選択のドロップダウンリストから、［Smart 検査］を選択し、❷起動ドライブ（ここでは、「Macintosh HD」）左のチェックボックスにチェックを入れ、❸［▶］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は、手順③-❷で［アップデート］を選択することによって作成できます。

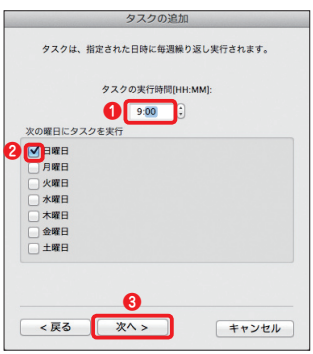


5

❶「/Volumes」以外のすべてのフォルダーにチェックを入れ、❷［次へ］ボタンをクリックします。

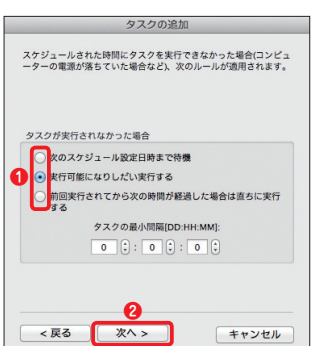
POINT

「/Volumes」にチェックを入れると、接続（マウント）中の他のパソコンの共有フォルダーやUSBメモリーなども検査対象となり、検査に時間がかかる場合があるので、ご注意ください。



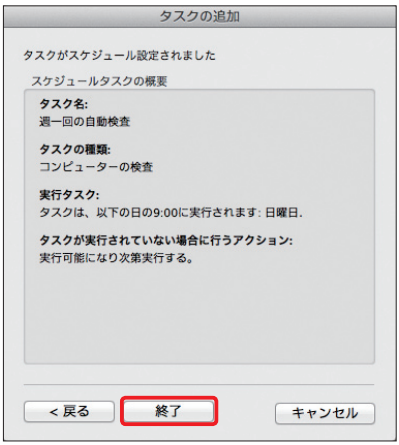
6

タスクの実行時刻と曜日を選択します。❶タスクを実行する時刻を設定し、❷実行する曜日（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。



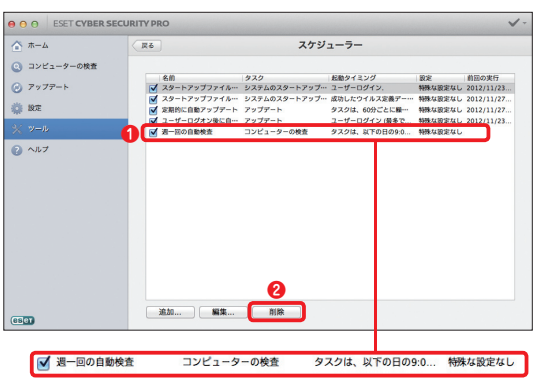
7

❶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。❷［次へ］ボタンをクリックします。



8

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。



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す。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 ▸▸ 統計の閲覧

10-4 これまでの各種統計データを閲覧するには

P C

「保護統計」をプライマリウィンドウに表示すると、本プログラムをインストールしてからの保護統計データを閲覧できます。

統計データを閲覧する

1 メインウィンドウを開き、❶［ツール］ボタンをクリックし、❷［保護統計］をクリックします。

2 ［統計］のドロップダウンリストから［ウイルス・スパイウェア対策］を選ぶと、ウイルス・スパイウェア対策の統計グラフを閲覧できます。

POINT

ウイルス・スパイウェア対策は、「オンデマンド検査」「リアルタイム検査」「電子メールクライアント保護」「Web 保護」の 4 つの保護機能で構成されます。手順②で表示される情報は、4 つのアクセス保護機能の全体の統計データとなります。

3

［統計］のドロップダウンリストから［オンデマンド検査］を選ぶと、オンデマンド検査の統計グラフを閲覧できます。

4

［統計］のドロップダウンリストから［リアルタイム検査］を選ぶと、リアルタイムファイルシステム保護の統計グラフを閲覧できます。

5

［統計］のドロップダウンリストから［電子メールクライアント保護］を選ぶと、電子メールクライアント保護の統計グラフを閲覧できます。

6

［統計］のドロップダウンリストから［Web アクセス保護］を選ぶと、Web アクセス保護の統計グラフを閲覧できます。

統計データをリセットする

1

メインウィンドウを開き、❶［ツール］ボタンをクリックし、❷［保護統計］をクリックします。

2

❶リセットしたい統計（ここでは、［ウイルス・スパイウェア対策］）をドロップダウンリストから選択し、❷［リセット］をクリックします。統計情報がリセットされます。

POINT

「ウイルス・スパイウェア対策」を選択して、［リセット］をクリックするとすべての統計情報がリセットされます。「オンデマンド検査」「リアルタイム検査」「電子メール保護」「Web 保護」を選択した場合は、その項目の統計情報のみがリセットされます。

ツール ▸▸ 隔離ファイルの確認・追加

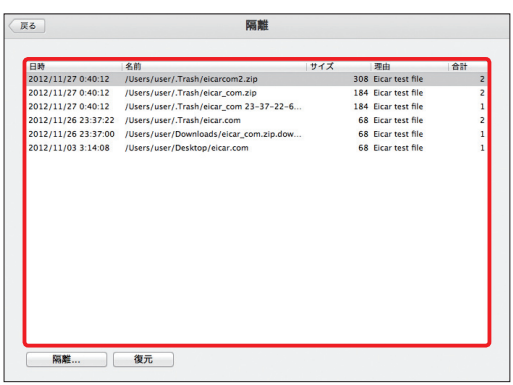
10-5 P C 各種検査で隔離されたファイルを確認・復元するには

本プログラムではウイルスを検出すると、検出されたファイルを無効化して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

メインウィンドウを開き、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効化されているため、隔離している限り安全です。

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［復元］ボタンをクリックします。

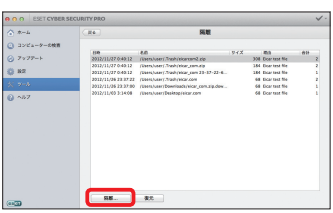
POINT

復元したいファイルに対して［Ctrl］キーを押しながらクリック（副ボタンのクリック）し、［復元先を指定］を選択すると、復元先を指定してファイルの復元が行えます。

コラム

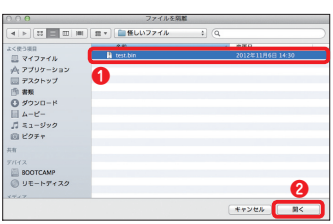
疑わしいファイルを手動で隔離するには

疑わしいファイルを手動で隔離するには、以下の手順で行います。



1

［隔離］ボタンをクリックします。



2

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。

ツール ▸▸ 実行中のプロセス評価

10-6 現在実行中のプロセス（ソフトウェア）を評価するには

P C

悪意のあるソフトウェアが侵入すると、見慣れない不審なソフトウェアが動作します。本プログラムでは、ESET Live Grid の機能を利用して実行中のプロセスを評価しています。

1

メインウィンドウを開き、❶［ツール］ボタンをクリックし、❷［実行中のプロセス］をクリックします。

2

現在動作しているプロセス（ソフトウェア）の一覧が、表示されます。❶ソフトウェアをクリックすると、❷そのソフトウェアの情報が表示されます。

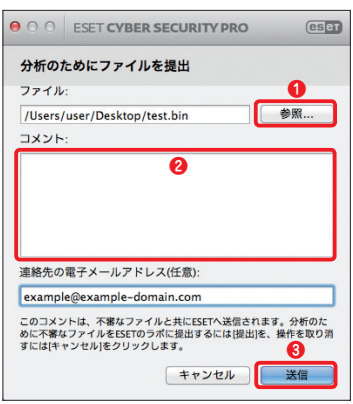
ツール ▸▸ 検体の提出

10-7 P C ウイルスの可能性がある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 社のウイルスラボまでお送りください。以下に手順を紹介します。

1

メインウィンドウを開き、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［参照 ...］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 ▸▸ ESET Social Media Scanner

10-8 ESET Social Media Scanner を使うには

P C

ESET Social Media Scanner は、Facebook や Twitter に投稿されたコメントが安全かどうかのチェックやオンラインスキャン機能によってコンピューターの検査を行う機能です。ここでは、その初期設定について説明します。

1

メインウィンドウを開き❶［ツール］ボタンをクリックします。❷［ESET Social Media Scanner］をクリックします。

2

Web ブラウザーが起動し、Social Media Scanner の設定ページが表示されます。ここでは、Facebook を例に ESET Social Media Scanner の使い方を説明します。［Facebook を保護］ボタンをクリックします。

3

Facebook のログイン画面が表示されます。❶Fecebook で利用しているメールアドレスを入力し、❷パスワードを入力します。❸［ログイン］ボタンをクリックします。

4

［パスワードを保存］ボタンをクリックします。

5

❶［許可］ボタンをクリックし、❷［OK］ボタンをクリックします。

6

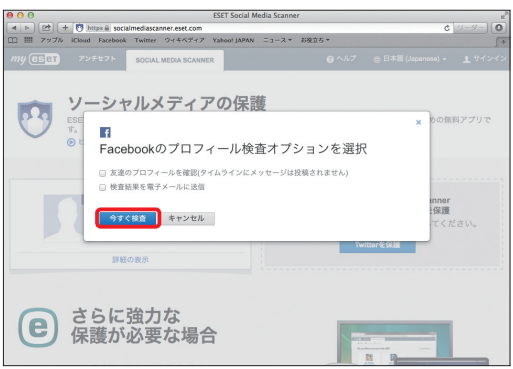
［OK］ボタンをクリックします。

POINT

手順⑤と⑥の作業は、Facebook の保護を行うときに初回のみ必要な手順です。次回からは、この手順は表示されません。

7

Social Media Scannerの設定ページに戻ります。［プロフィール検査の開始］ボタンをクリックすると、プロフィールの検査を実行します。



8

［今すぐ検査］ボタンをクリックします。

9

［脅威は検出されませんでした］が表示されたら、安全です。

POINT

手順⑧で［詳細の表示］をクリックすると、ステータスレポートや検査履歴、各種設定の変更などの作業が行えます。

コラム

Twitter のプロフィールの保護

Twitter のプロフィールを保護したいときは、手順②で［Twitter を保護］ボタンをクリックして、Twitter のログイン画面ページが表示されたら、❶ユーザー名またはメールアドレスを入力し、❷パスワードを入力して、❸［連携アプリを認証］ボタンをクリックすれば設定は完了です。Social Media Scanner の設定ページに戻りますので、［プロフィール検査の開始］ボタンをクリックすると、プロフィールの検査が実行されます。

Part.11
「ヘルプ」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。

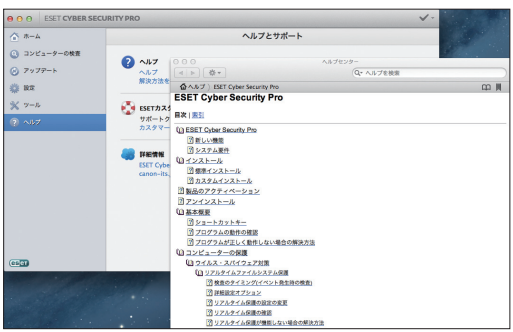
ヘルプ ▸▸ ヘルプの確認

11-1 P C ヘルプを見るには

本書がお手元にない場合などに本プログラムの機能を確認するときは、「ヘルプ」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

メインウィンドウを開き、❶［ヘルプ］ボタンをクリックし、❷［ヘルプ］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

11-2 P C サポート情報やよくある質問（FAQ）を確認するには

本プログラムに関するよくある質問（FAQ）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

メインウィンドウを開き、❶［ヘルプ］ボタンをクリックします。❷［解決方法を探す］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。また、このホームページから「お問い合わせ窓口」をご利用いただけます。

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 ▸▸ バージョン確認

11-3 P C 本プログラム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お問い合わせの際には、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

メインウィンドウを開き、❶［ヘルプ］ボタンをクリックし、❷［ESET Cyber Security Pro について］または［ESET Cyber Security について］をクリックします。

2

❶製品のバージョンが表示されます。❷［詳細情報］をクリックします。

3

本プログラムの詳細なバージョン情報が表示されます。［OK］ボタンをクリックすると、この画面が閉じます。

POINT

バージョン情報の確認は、❶メニューバーの本プログラムのアイコンをクリックし、❷［バージョン情報］をクリックすることでも行えます。