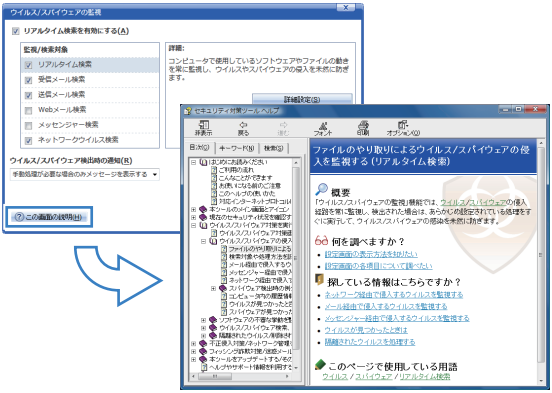
セキュリティ対策ツール　Ver.1　設定ガイド
【操作・設定ガイド】

掲載の情報は、2008年9月現在のものです。

問題解決に役立つ情報源

オンラインヘルプで問題解決

セキュリティ対策ツールの画面には[この画面の説明]というボタンがあります。このボタンをクリックすると、その画面に関するヘルプトピックが表示されます。また、メイン画面の[ヘルプとサポート]から表示することもできます。



セキュリティ対策ツール　サポートページで問題解決

http://www.flets-west.jp/redir/sec/to_top.html

セキュリティ対策ツールに関するよくあるご質問など、困ったときに役立つサポート情報を掲載しています。

セキュリティ対策ツールのインストールや設定、ウイルス情報などに関するお問い合わせ

NTT西日本セキュリティサポートセンタ
お問い合わせ
https://f-security.jp/qa/

0120-248303（携帯電話・PHSからもご利用になれます）
※受付時間　9:00 ～ 18:00（土・日・祝日も受付）
年末年始12月29日～ 1月3日は休業とさせていただきます。
メールでのお問い合わせ：customer@f-security.jp

操作・設定ガイド - 目次

セキュリティ対策ツールの基本操作

セキュリティ対策ツールを使いこなす

メッセージが表示されたときは

よくある質問と回答

1 セキュリティ対策ツールの起動とメイン画面の表示

セキュリティ対策ツールは、パソコンが起動すると自動的に起動してパソコンの保護を開始します。メイン画面を開くと、ウイルスやスパイウェアの検索を行ったり、設定を変更したりできます。

セキュリティ対策ツールの起動

セキュリティ対策ツールは自動的に起動します。このため、起動するための操作は通常必要ありません。

セキュリティ対策ツールが動作している間は、デスクトップ右下の通知領域（タスクトレイ）にセキュリティ対策ツールのアイコンが表示されます。

ヒント

- 手動で起動する場合は、下記の「メイン画面を表示する」と同じ手順を行ってください。
- 通知領域（タスクトレイ）のアイコンは、セキュリティ対策ツールの動作状況によって表示が切り替わります。詳細については、「通知領域（タスクトレイ）のアイコン」（9ページ）をご覧ください。

メイン画面を表示する

1 デスクトップ左下の［スタート］をクリック。

Windows Vista　　Windows XP

スタートメニューが表示されます。

2 [すべてのプログラム]→[NTTW]→[セキュリティ対策ツール]の順にクリック。

メイン画面が表示されます。

ヒント

メイン画面は通知領域(タスクトレイ)にあるセキュリティ対策ツールのアイコンをダブルクリックしても表示できます。

メイン画面を閉じるには？

メイン画面を閉じるには、画面右上の [X] (閉じる)をクリックしてください。なお、メイン画面を閉じても、セキュリティ対策ツールは終了せず、パソコンの保護が維持された状態となります。

[閉じる]

ヒント

セキュリティ対策ツールを終了するには？

セキュリティ対策ツールの終了は、ウイルスの侵入や不正アクセスからパソコンを保護できなくなるためおすすめしません。やむを得ず終了する場合は、「セキュリティ対策ツールを終了するには？」(75ページ)をご覧ください。

2 セキュリティ対策ツールの画面構成

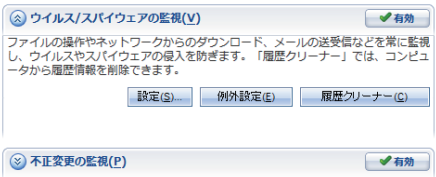
セキュリティ対策ツールでは、操作や設定の変更をメイン画面で行います。ここでは、セキュリティ対策ツールの画面構成の概要について説明します。

メイン画面の構成

カテゴリボタン	セキュリティ対策ツールの機能が6種類のカテゴリに分類されています。それぞれのボタンをクリックすると、カテゴリの機能が画面の右側に表示されます。
総合セキュリティ状況	パソコンの保護が適切に行われているかどうかを確認できます。
検索開始	ウイルスやスパイウェアの検索とセキュリティ診断を行います(12ページ)。
アップデート開始	セキュリティ対策ツールのアップデートを行います(11ページ)。

各カテゴリの画面について

各カテゴリの設定画面では、各種機能の有効と無効の切り替えや確認、設定の変更などができます。



/	クリックして各機能の詳細を表示したり、非表示にしたりします。
有効 / 無効	各機能の状態です。クリックして有効と無効を切り替えることができます。

ヒント

それぞれの画面については、[ヘルプとサポート]からヘルプを表示したり、それぞれの画面に用意されている[この画面の説明]をクリックして表示される画面で確認してください。

通知領域(タスクトレイ)のアイコン

デスクトップ右下の通知領域(タスクトレイ)に表示されているセキュリティ対策ツールのアイコンは、状態に応じて次の4種類に切り替わります。

	通常の状態です。セキュリティ対策ツールが正常に動作しています。このアイコンがアニメーションで表示されている場合は、ウイルスなどの検索やセキュリティ対策ツールのアップデートが行われていますので、パソコンの電源を切ったり再起動したりしないでください。
	有効にすることを推奨している機能が無効になっているなど、設定になんらかの問題があります。メイン画面の総合セキュリティ状況を確認して問題を解決してください。また、緊急ロック(48ページ)が有効になっている場合もこのアイコンで表示されます。
	セキュリティ対策ツールの起動処理を行っています。
	セキュリティ機能が利用停止状態か、廃止状態のため、セキュリティ対策ツールを利用することができません。 セキュリティ機能を廃止された方は、必要に応じてセキュリティ対策ツールのアンインストールをお願いします。

3 アップデートする

パソコンを危険にさらすウイルスやスパイウェアなどの脅威は日々進化しています。セキュリティ対策ツールをアップデートして、最新の脅威に対応できるようにしてください。

初期設定では自動アップデート機能が有効になっています

セキュリティ対策ツールの初期設定は、アップデートを自動的に行う「インテリジェントアップデート」という機能が有効になっています。このため、通常は手動でアップデートする必要はありません。インテリジェントアップデートの設定を変更する方法についてはヘルプを参照してください。

! ご注意

アップデートに必要なデータはセキュリティ専用サーバから取得します。インテリジェントアップデートを有効にしている場合は、パソコンを常にネットワークに接続しておいてください。

手動でアップデートする

ご注意

アップデートに必要なデータはセキュリティ専用サーバから取得します。アップデートをする前に、パソコンがネットワークに接続されていることを確認してください。

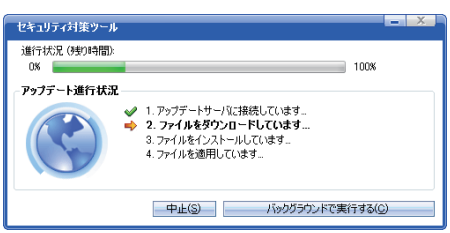
1 メイン画面を表示して（5ページ）、[アップデート開始]をクリック。

[アップデート開始]

アップデートがはじまり、進行状況が表示されます。

ヒント

設定によっては、[パターンファイルやプログラムの最新版が見つかりました]画面が表示されることがあります。



アップデートが完了すると進行状況の画面が自動的に閉じて、メイン画面に戻ります。

ヒント

「Windows ファイアウォールを有効にしますか？」と表示されたときは？

アップデートの内容によっては、一時的にパーソナルファイアウォールを終了する必要があるため、その間は代わりにWindows ファイアウォールを有効にするかどうかを確認する画面が表示されます。この場合は、画面の指示に従ってWindows ファイアウォールを有効にしてください。

「今すぐコンピュータを再起動してもよろしいですか？」と表示されたときは？

アップデートの内容によっては、パソコンの再起動を促す画面が表示されます。この場合は、画面の指示に従ってパソコンを再起動してください。

4 ウイルスやスパイウェアを検索する

パソコンをウイルスやスパイウェアから保護するには、定期的な検索が必要です。セキュリティ対策ツールは、検索を定期的に自動で行い、パソコンを保護します。

こんなときには手動での検索が必要です

セキュリティ対策ツールの初期設定は、定期的にウイルスやスパイウェアを検索する状態になっています。通常、手動で検索する必要はありません。

ただし、次のような場合はパソコンにウイルスやスパイウェアが潜んでいる可能性があるので、手動で検索を行ってください。

- **セキュリティ対策ツールをインストールした直後**
- **しばらくアップデートおよび検索を行わなかったとき**

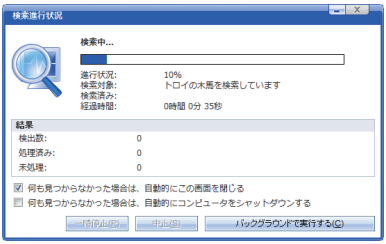
手動で検索する

ご注意

検索する前に、アップデートを行ってください(10ページ)。

1 メイン画面を表示して(5ページ)、[検索開始]をクリック。

[検索進行状況]画面が表示されます。

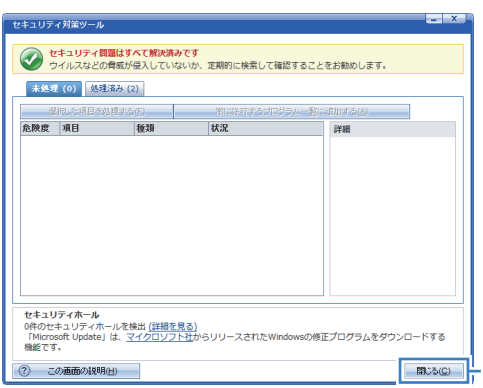


検索が完了すると、検索結果が表示されます。

2 検索結果に応じて処理を行う。

ウイルスやスパイウェアが検出された場合は「ウイルスやスパイウェアが見つかったときは」(14ページ)を参照して処理を行ってください。

3 処理が完了したら[閉じる]をクリック。

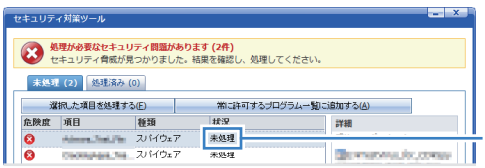


[閉じる]

メイン画面に戻ります。

ウイルスやスパイウェアが見つかったときは

1 [未処理]と表示されているウイルスやスパイウェアを選択。



手動で対応が必要なウイルスやスパイウェアは、「未処理」パネルに表示されます。

「処理済み」パネルに表示されている項目は、すでに対応が完了しています。手動での対応は必要ありません。

2 [選択した項目を処理する]をクリック。

選択した項目が削除されます。

削除しても問題ないかどうかがわからない場合は、画面右側の詳細情報を確認してください。

ヒント

クッキーとは？

クッキー(cookie)は、Webサイトがユーザの識別や入力情報の保存などの目的でユーザ側のパソコンに一時的に記録する情報です。一般的にはWebサイトの利便性向上のために使われますが、広告の効果測定に使われることもあります。クッキーがパソコンに被害を与えることはありませんが、個人情報の保護という観点からは不適切と思われる使われかたをしているクッキーはスパイウェアの一種として認知されています。

ご注意

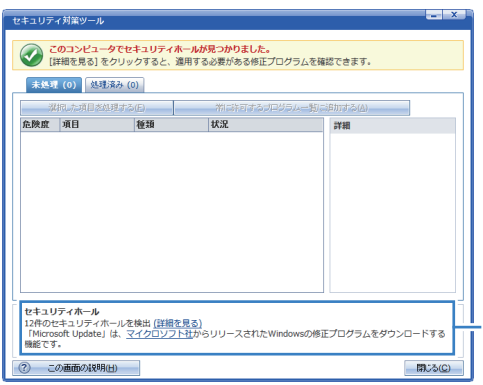
見つかったスパイウェアが、すべて害のあるものとは限りません。スパイウェアを削除する場合は、必ず詳細情報を確認してください。

3 [未処理]の項目がほかにもある場合は続けて処理を行う。

手順2を繰り返して、[未処理]と表示されている項目をすべて処理します。

セキュリティホールが見つかったときは

セキュリティホールは、セキュリティ上問題があると認知されている、ソフトウェアの欠陥です。セキュリティホールが見つかった場合は、[詳細を見る]をクリックして内容を確認し、Microsoft Updateを行います。



[セキュリティホール]

ご注意

Microsoft Updateのご利用には、インターネットへの接続環境が必要です。

Microsoft Updateは、マイクロソフト社が提供しているサービスです。不明な点についてはマイクロソフト社にお問い合わせください。

5 ウイルスやスパイウェアの被害に遭わないようにするには？

ウイルスやスパイウェアはパソコンに悪影響を与える不正ソフトウェアの一種で、パソコンを利用する上での脅威として代表的なものです。

セキュリティ対策ツールは、ウイルスやスパイウェアの被害からパソコンを保護します。

ウイルスやスパイウェアの基礎知識

ウイルスやスパイウェアはパソコンの動作に悪影響を与えるソフトウェアです。これらのソフトウェアはネットワークやデータの受け渡しなどを通じてパソコンに侵入し、データを改ざんしたり、情報を流出させたりするといった活動を行います。

セキュリティ対策ツールでのウイルスおよびスパイウェア対策

セキュリティ対策ツールでは、次のような対策でウイルスやスパイウェアの被害からパソコンを保護します。

処理されるデータをすべて監視します

ファイルの操作やメールの送受信、ネットワークによる通信などで処理されるデータを常に監視して、ウイルスやスパイウェアの侵入を防止します。

手動でウイルスやスパイウェアの検索を行えます

ハードディスクなどの記憶媒体にウイルスやスパイウェアが潜んでいないかどうか検索できます。スケジュールを設定して定期的に検索することもできます。

ヒント

初期設定でウイルスやスパイウェアの侵入を防止できる？

ウイルスやスパイウェアからパソコンを保護するための標準的な設定はあらかじめ適用されており、侵入を防止できます。

こんなことができます(主な機能)

- ウイルスやスパイウェアの侵入を入口でブロック。あなたのパソコンを守ります(ウイルス/スパイウェアの監視、18ページ)。
- 侵入してしまったウイルスやスパイウェアも、すぐに検出して処理します(予約検索/手動検索、18ページ)。

ウイルスやスパイウェアの対策はこの画面で!

ウイルスやスパイウェア対策の設定は、[ウイルス/スパイウェア対策]画面で行います。

[ウイルス/スパイウェア対策]画面は、[ウイルス/スパイウェアの監視]、[不正変更の監視]、[予約検索/手動検索]、[隔離ファイルの管理]で構成されています。

ここでは各項目の概要についてご説明します。詳細はヘルプを参照してください。

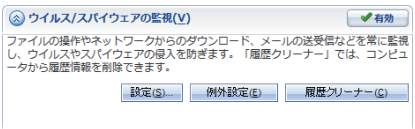
ヒント

ヘルプは、[ヘルプとサポート]画面の[ヘルプ]を選択すると表示されます。

詳細な設定方法は[ウイルス/スパイウェア対策を実行する]内の[ウイルス/スパイウェア対策画面の見かたと使いかた]を参照してください。

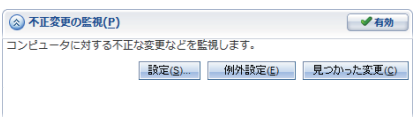
ウイルス/スパイウェアの監視

パソコンで使用しているソフトウェアやファイルの操作、ネットワークからのダウンロード、メールの送受信などを常に監視し、ウイルスやスパイウェアの侵入を防ぎます。「履歴クリーナー」では、パソコンから履歴情報を削除できます。



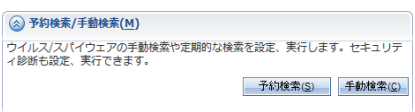
不正変更の監視

パソコンの設定に対する不正な変更などを監視します。



予約検索/手動検索

ウイルス/スパイウェアの手動検索や定期的な検索を実行するように設定できます。また、セキュリティ診断も実行できます。



隔離ファイルの管理

ウイルス検索によって隔離したファイルを確認、処理できます。また、過去に削除したスパイウェアを削除前の状態に復元します。

6 不正侵入を監視し、ネットワークを管理するには？

ネットワークへの接続中は、外部からの攻撃に備えておく必要があります。また、様々なソフトウェアがネットワークを利用します。

セキュリティ対策ツールでは、ネットワークを監視して、危険を排除できます。

ネットワーク監視の基礎知識

ネットワークを利用して外部のパソコンと接続できるということは、外部のパソコンもこちらのパソコンと接続できるということです。ネットワークを利用するときは不正侵入などの外部からの攻撃に備えておく必要があります。

また、Webブラウザやメールソフトのような、ネットワークを利用するためのソフトウェアがネットワークに接続するのは当然ですが、最近はアップデートや情報更新などの目的でネットワークを活用するソフトウェアが増えています。

どのソフトウェアがどのような目的でネットワークを利用しようとしているのかについてきちんと確認することも必要です。

セキュリティ対策ツールでのネットワーク利用対策

セキュリティ対策ツールでは、次のような対策でソフトウェアのネットワーク利用を監視します。

外部からの攻撃を監視します

OSやソフトウェアの欠陥、設定の不備などを狙う外部からの攻撃を防止します。

ソフトウェアによるネットワークの利用を監視します

ソフトウェアによるネットワークの利用の可否を確認します。

登録された情報の送信を防止します

Webブラウザ、メール、インスタントメッセンジャーで送信されるデータを監視して、登録された情報の送信を防止するように設定できます（32ページ）。

ヒント

初期設定でネットワークを監視できる？

外部からの攻撃やソフトウェアによるネットワークの利用を監視する[パーソナルファイアウォール]は初期設定で有効になっています。

こんなことができます(主な機能)

- 外部のパソコンからの不正なアクセスを防ぎます(パーソナルファイアウォール、21ページ)。
- ネットワークへの不正侵入を防ぎます(無線LANパトロール、21ページ)。
- ネットワーク上のセキュリティ対策ツールを一元管理します(ホームネットワーク管理、21ページ)。

不正侵入の監視/ネットワークの管理はこの画面で！

不正侵入の監視、ネットワークの管理の設定は、[不正侵入対策/ネットワーク管理]画面で行います。

[不正侵入対策/ネットワーク管理]画面は、[パーソナルファイアウォール]、[無線LANパトロール]、[ホームネットワーク管理]、[ネットワーク接続状況]で構成されています。

ここでは各項目の概要についてご説明します。詳細はヘルプを参照してください。

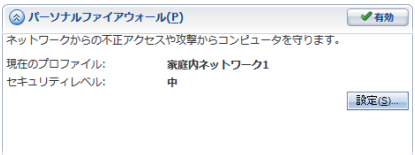
ヒント

ヘルプは、[ヘルプとサポート]画面の[ヘルプ]を選択すると表示されます。

詳細な設定方法は[不正侵入対策/ネットワーク管理を実行する]内の[不正侵入対策/ネットワーク管理画面の見かたと使いかた]を参照してください。

パーソナルファイアウォール

ネットワークからの不正アクセスや攻撃からパソコンを守ります。



無線LANパトロール

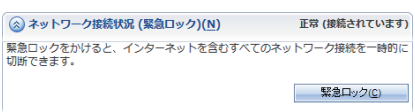
お使いのネットワークに接続されているパソコンやネットワーク機器を検索し、不正侵入がないかを確認できます。

ホームネットワーク管理

同一ネットワーク上のパソコンに対して、ウイルス検索やアップデートなどを実行できます。

ネットワーク接続状況(緊急ロック)

ネットワークウイルス感染の拡大や、外部のパソコンからの不正アクセスを防ぐために、インターネットを含むすべてのネットワークへの接続を一時的に切断できます。



7 フィッシング詐欺による個人情報の漏えいや迷惑メールの被害に遭わないようにするには？

フィッシング詐欺は、あらかじめ用意した金融機関などの偽のWebサイトへ誘導し、クレジットカード情報などの個人情報をだまし取る犯罪です。セキュリティ対策ツールは、フィッシング詐欺で使われる偽のWebサイトへのアクセス制限や、一方的に送られてくる迷惑メール・詐欺メールの判別を行うなどの複数の手段で被害を防止します。

フィッシング詐欺の基礎知識

フィッシング詐欺とは、金融機関などを装ったメールを送りつけるなどして偽のWebサイトへと誘導し、ログイン情報やクレジットカード情報などをだまし取ろうとする詐欺のことです。

フィッシング詐欺の被害に遭わないようにするには、送られてきたメールや表示したWebサイトが本物かどうかということをきちんと見分けることが重要となります。

セキュリティ対策ツールでのフィッシング詐欺対策

セキュリティ対策ツールでは、次のような対策でフィッシング詐欺による被害を防止します。

フィッシング詐欺の疑いがあるWebサイトを判定します

表示しようとしているWebサイトを判定し、フィッシング詐欺を行っている可能性がある場合は危険度に応じたメッセージを表示します。また、フィッシング詐欺を行っていることが認知されているWebサイトを表示しないように設定できます。

ヒント

初期設定でフィッシング詐欺を防止できる？

フィッシング詐欺対策は初期設定では無効になっています。このため初期設定では処理することができません。有効にした場合、誤ってフィッシング詐欺を行っているWebサイトを表示しようとしても、危険度に応じて警告が表示されます。

迷惑メールや詐欺メールの基礎知識

迷惑メールは、宣伝を目的として不特定多数に一方的に送信されるメールの総称です。

また、詐欺メールは詐欺行為を目的として送信されるメールの総称です。最近では、フィッシング詐欺のメールが特に問題になっています。

セキュリティ対策ツールでの迷惑メールおよび詐欺メール対策

セキュリティ対策ツールでは、次のような対策で迷惑メールや詐欺メールによる被害を防止します。

迷惑／詐欺メールの疑いがあるメールを判定します

送られてきたメールが迷惑／詐欺メールであるかどうかを判定し、疑いがあるものは「迷惑メールフォルダ」に自動的に振り分けます。

ヒント

初期設定で迷惑メールや詐欺メールを処理できる？

初期設定では、迷惑メールや詐欺メールの対策は無効になっています。このため、初期設定では処理することはできません。

迷惑メールや詐欺メールの判定は常に正しく行われる？

迷惑メールや詐欺メールは、送信元の情報やメールの内容などをもとに多角的に分析して判定していますが、迷惑メールや詐欺メールを正常なメールと判定することや、正常なメールを迷惑メールや詐欺メールと判定することもあります。

有害サイトや偽装サイトの基礎知識

有害サイトとは、成人向けの情報や違法行為に関する情報、飲酒やギャンブルに関する情報など、特に未成年者にとって有害な情報を扱っているWebサイトのことです。また、偽装サイトとは、著名なWebサイトを偽装したWebサイトのことです。

セキュリティ対策ツールでの有害サイトおよび偽装サイト対策

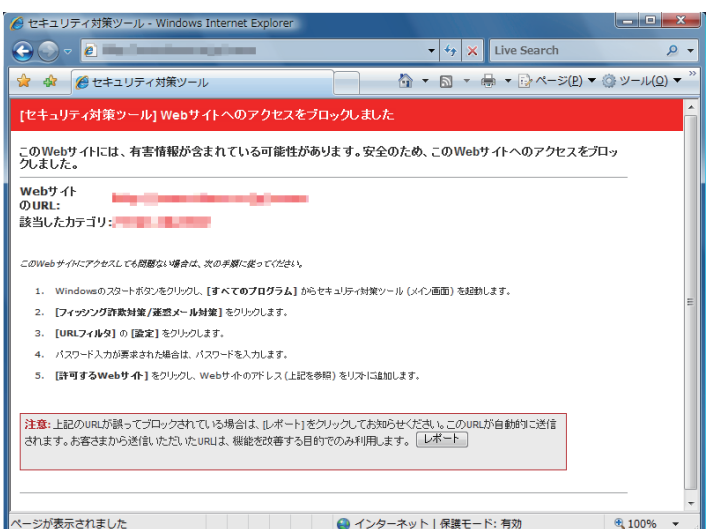
セキュリティ対策ツールでは、次のような対策で有害サイトや偽装サイトの表示を防止します。

指定された種類の内容やURLのWebサイトの表示を防止します

表示しようとしているWebサイトがあらかじめ指定された種類の内容やURLである場合、そのWebサイトの表示を防止するように設定できます。

有害サイトや偽装サイトを表示しようとしたときの画面

指定された有害サイトや偽装サイトを表示しようとすると、Webサイトが次のような内容に置き換えられて表示されます。



ヒント

初期設定で有害サイトや偽装サイトの表示を防止できる？

初期設定では、すべてのWebサイトが表示されます。

個人情報の漏えいの基礎知識

普段から名前や住所、クレジットカード番号などの個人情報の取り扱いに気をつけていても、お子さまがうっかり個人情報を漏らしてしまうことや、友人から送られてきたメールを転送しようとして友人の個人情報を漏らしてしまうようなことは充分に考えられます。

セキュリティ対策ツールでの個人情報の漏えい対策

セキュリティ対策ツールでは、次のような対策で個人情報の漏えいを防止します。

登録された情報の送信を防止します

Webブラウザ、メール、インスタントメッセンジャーで送信されるデータを監視して、登録された情報の送信を防止するように設定できます。

ヒント

初期設定で個人情報の漏えいを防止できる？

個人情報の漏えいを防止するには、セキュリティ対策ツールに保護したい個人情報を登録する必要があります。このため、初期設定では漏えいを防止することはできません。

こんなことができます（主な機能）

- フィッシング詐欺から、あなたの個人情報を守ります（フィッシング詐欺対策、26ページ）。
- 迷惑メールや詐欺メールを自動的に判定します（迷惑/詐欺メールの判定、27ページ）。
- 有害な情報を含むおそれのあるWebサイトへのアクセスを防ぎます（URLフィルタ、30ページ）。
- 個人情報の漏えいを防ぎます（個人情報の保護、32ページ）。

フィッシング詐欺/迷惑メール対策はこの画面で！

※フィッシング詐欺対策機能とカテゴリ指定によるURLフィルタ機能は技術供与元であるトレンドマイクロ株式会社が提供しています。

フィッシング詐欺や迷惑メール対策の設定は、[フィッシング詐欺/迷惑メール対策]画面で行います。

[フィッシング詐欺/迷惑メール対策]画面は、[フィッシング詐欺対策]、[迷惑/詐欺メールの判定]、[URLフィルタ(Webアクセス規制)]、[個人情報の保護]で構成されています。

ここでは各項目の概要についてご説明します。詳細はヘルプを参照してください。

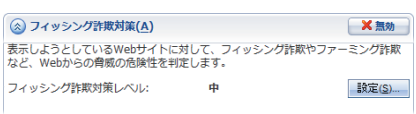
ヒント

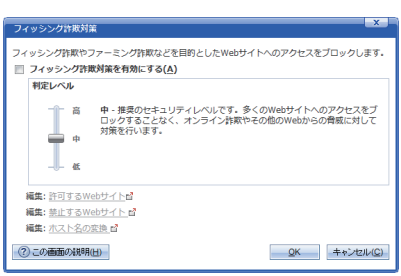
ヘルプは、[ヘルプとサポート]画面の[ヘルプ]を選択すると表示されます。

詳細な設定方法は[フィッシング詐欺対策/迷惑メール対策を実行する]内の[フィッシング詐欺/迷惑メール対策の見かたと使いかた]を参照してください。

フィッシング詐欺対策

フィッシング詐欺で使われる偽装サイトにアクセスしないようにしたり、一方的に送られてくる勧誘/広告メール(いわゆる迷惑メール)を判別したりといった複数の機能を組み合わせることで、大切な個人情報をフィッシング詐欺の危険から総合的に守ります。





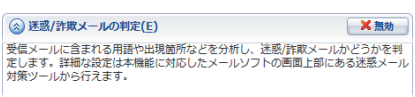
フィッシング詐欺対策の判定について

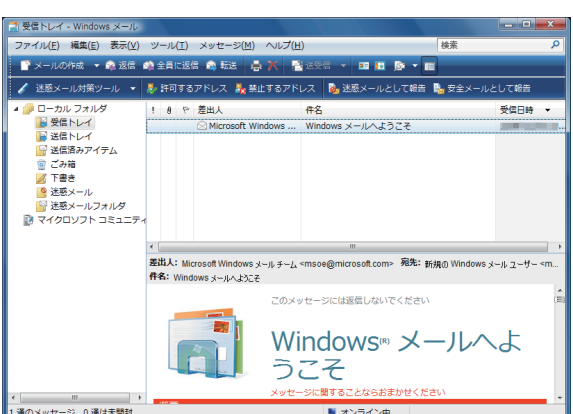
フィッシング詐欺対策の判定レベルは次の中から選択します。通常は、「中」に設定してください。

高	安全性が高いと評価されているWebサイトのみを表示できます。それ以外のWebサイトはブロックされるため、オンライン詐欺やその他のWebからの脅威に対してセキュリティレベルが高くなります。
中	推奨のセキュリティレベルです。多くのWebサイトへのアクセスをブロックすることなく、オンライン詐欺やその他のWebからの脅威に対して対策を行います。
低	安全性が非常に低いと評価されているWebサイトのみを表示できないようにすることで、オンライン詐欺やその他のWebからの脅威に対して最低限必要な対策を行います。

迷惑/詐欺メールの判定

Microsoft Outlook、Microsoft Outlook ExpressおよびMicrosoft Windowsメール専用のツールとして、「迷惑メール対策ツール」を利用するかどうかを設定できます。





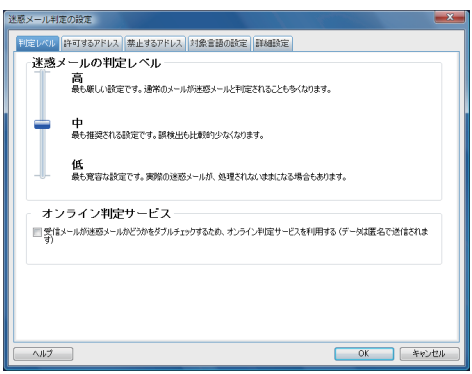
ご注意

「迷惑/詐欺メールの判定」を有効にすると、本機能に対応するメールソフトを起動してから操作できるようになるまで、時間がかかる場合があります。

これは本機能がメールソフトの起動時に迷惑メールの検索を行っているためです。本機能は「受信トレイ」内および本機能が作成する「迷惑メールフォルダ」内の未読メールを対象に検索を行うため、これらの未読メールを既読にするか削除して検索対象を減らすと、動作が改善する場合があります。

判定レベル

迷惑メールの判定レベルを「高」、「中」、「低」から選択できます。



迷惑メールの判定について

迷惑メールの判定レベルは次の中から選択します。通常は、「中」に設定してください。

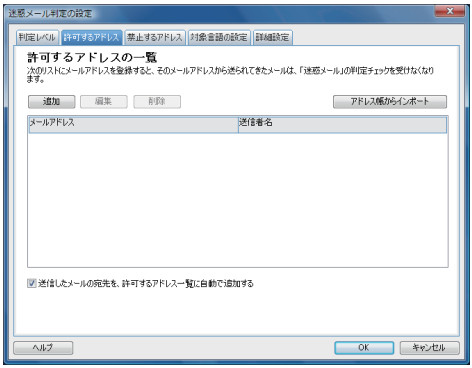
高	最も厳しい基準で判定する設定です。迷惑メールと判定できる要素が少しでもあれば迷惑メールと判定します。正常なメールを迷惑メールとして判定する確率が高くなります。
中	推奨する設定です。適切に判定する確率が最も高くなります。
低	最もゆるい基準で判定する設定です。迷惑メールと判定できる要素がいくつもそろったときに迷惑メールと判定します。正常なメールを迷惑メールとして判定する確率は低くなります。

ご注意

詐欺メールには、迷惑メールの判定とは異なる判定基準が用いられます。

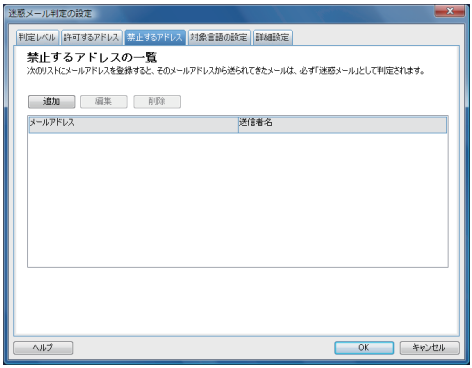
許可するアドレス

友人や企業からのお知らせなどのメールアドレスを登録して、信頼できる相手から送られてくるメールを誤って迷惑メールまたは詐欺メールと判定されないようにできます。



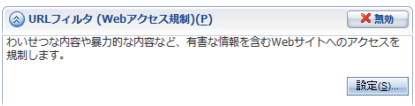
禁止するアドレス

迷惑メールを繰り返し送ってくる相手のメールアドレスを登録して、必ず迷惑メールまたは詐欺メールとして判定されるようにできます。



URLフィルタ（Webアクセス規制）

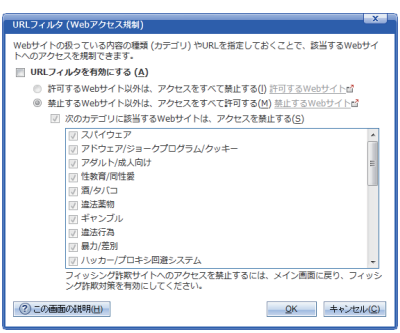
わいせつな内容や暴力的な内容など、有害な情報を含むWebサイトや、詐欺などを目的とした偽装サイトにアクセスしないようにできます。



URLフィルタ（Webアクセス規制）

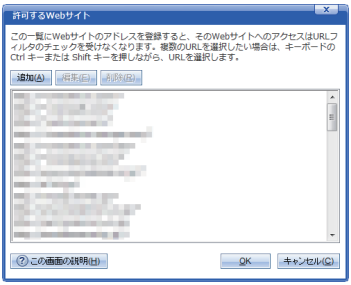
URLフィルタの有効と無効を切り替えることができます。[許可するWebサイト]の設定と組み合わせて特定のWebサイトのみを表示できるようにしたり、[禁止するWebサイト]の設定を組み合わせて指定したWebサイトを表示しないようにしたりできます。

また、カテゴリを指定して包括的にWebサイトの表示を禁止することもできます。



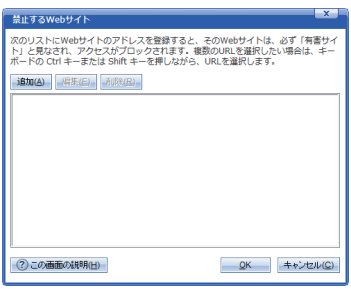
許可するWebサイト

表示を許可するWebサイトのURLを登録します。ここに登録されているWebサイトは、[禁止するカテゴリ]で表示が禁止されているカテゴリに属していても表示させることができます。



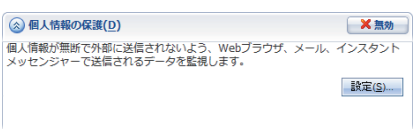
禁止するWebサイト

表示を禁止するWebサイトのURLを登録します。ここに登録されているWebサイトは、[禁止するカテゴリ]で表示が禁止されていないカテゴリに属していても表示されなくなります。



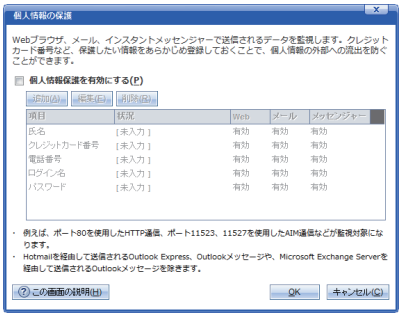
個人情報の保護

個人情報が無断で外部に送信されないよう、保護したい個人情報をあらかじめ設定しておき、Webブラウザ、メール、インスタントメッセンジャーでその情報が外部に送信されるのを防ぎます。



[個人情報の保護]の[設定]をクリックすると、[個人情報の保護]画面が表示されます。この画面で保護したい個人情報を登録したり削除したりできます。

それぞれの項目についての詳細はヘルプを参照してください。


個人情報の保護
Webブラウザ、メール、インスタントメッセンジャーで送信されるデータを監視します。クレジットカード番号など、保護したい情報をあらかじめ登録しておくことで、個人情報の外部への流出を防ぐことができます。
個人情報保護を有効にする(P)
追加(A)...
編集(E)...
削除(D)...
項目
状況
Web
メール
メッセンジャー
氏名 [未入力] 有効 有効 有効
クレジットカード番号 [未入力] 有効 有効 有効
電話番号 [未入力] 有効 有効 有効
ログイン名 [未入力] 有効 有効 有効
パスワード [未入力] 有効 有効 有効
例えば、ポート80を使用したHTTP通信、ポート11523、11527を使用したAIM通信などが監視対象になります。
Hotmailを経由して送信されるOutlook Express、Outlookメッセージや、Microsoft Exchange Serverを経由して送信されるOutlookメッセージを除きます。
この画面の説明(H)
OK
キャンセル(C)

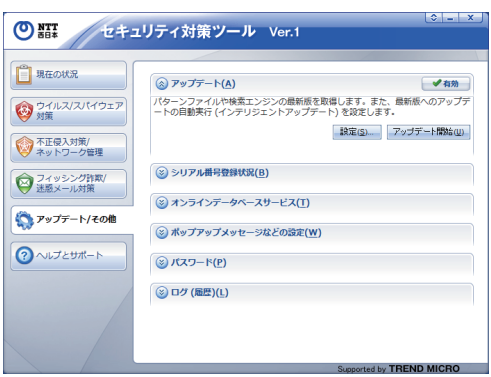
8 こんな機能もあります

セキュリティ対策ツールには、ここまでに紹介してきた機能のほかにも便利な機能があります。

その他の設定はこの画面で！

アップデート、オンラインデータベースサービス、ポップアップメッセージ、パスワードなどの設定、ログ（履歴）の表示は［アップデート/その他］画面で行います。

ここでは各項目の概要についてご説明します。詳細はヘルプを参照してください。



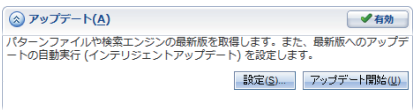
ヒント

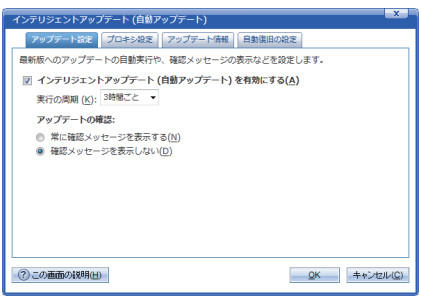
ヘルプは、［ヘルプとサポート］画面の［ヘルプ］を選択すると表示されます。

詳細な設定方法は［本ツールをアップデートする/その他の設定を行う］内の［アップデート/その他画面の見かたと使いかた］を参照してください。

アップデート

アップデートとはセキュリティ対策ツールで監視するウイルスなどの情報を集めたファイルを最新のファイルに更新することです。新たに出現したウイルスなどを検出して対応するためには、常にファイルを最新の状態にアップデートしておく必要があります。初期設定では3時間ごとに自動でアップデート(インテリジェントアップデート)されますが、最新版へのアップデートの自動実行周期や、確認メッセージの表示などを設定できます。

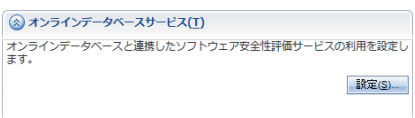


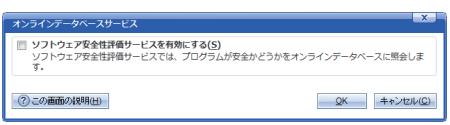


オンラインデータベースサービス

「ソフトウェア安全性評価サービス」を有効にしていると、お使いのソフトウェアが安全かどうかをオンラインデータベースに照会します。

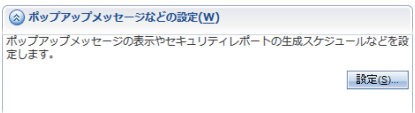
※ ソフトウェア安全性評価サービス機能は、技術供与元であるトレンドマイクロ株式会社が提供する機能となります。

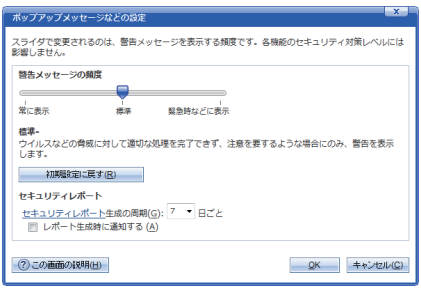




ポップアップメッセージなどの設定

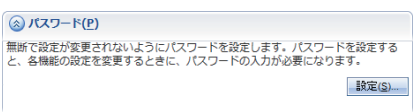
ウイルスやスパイウェアが見つかったときなどに、確認のポップアップメッセージを表示するかどうかや、セキュリティレポートを生成する周期を設定できます。

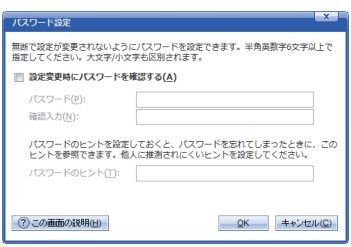




パスワード

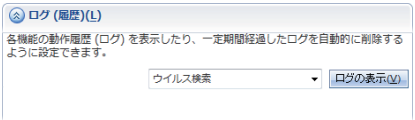
ほかの人に設定内容を変更されないように、パスワードを設定できます。





ログ(履歴)

各機能の動作履歴(ログ)を表示したり、一定期間経過したログを自動的に削除するように設定できます。



9 お子さまがいる場合におすすめの設定は？

最近では、お子さまがインターネットを使って宿題の調べ物をするような例が一般化しています。セキュリティ対策ツールでは、お子さまを有害な情報や個人情報の漏えいなどから保護するように設定できます。

お子さまを保護するための基礎知識

お子さまをインターネット上の脅威から保護するには、次のような点に注意する必要があります。

- 有害な情報に触れさせないようにする。
- 掲示板などに個人情報を書き込めないようにする。
- 迷惑メールや詐欺メールに触れさせないようにする。
- セキュリティ対策ツールの設定をお子さまが変更できないようにする。

セキュリティ対策ツールでお子さまをインターネット上の脅威から保護するための対策

セキュリティ対策ツールでは、次のような対策でお子さまをインターネット上の脅威から保護できます。

有害な情報に触れさせないようにできます

表示しようとしているWebサイトがあらかじめ指定された種類の内容やURLのものである場合、そのWebサイトの表示を防止するように設定できます（30ページ）。

個人情報の漏えいを防止できます

Webブラウザ、メール、インスタントメッセンジャーで送信されるデータを監視して、登録された情報の送信を防止するように設定できます（32ページ）。

迷惑メールや詐欺メールの疑いがあるメールを判定します

送られてきたメールが迷惑メールや詐欺メールであるかどうかを判定するように設定できます（27ページ）。

パスワードで設定を変更できないようにできます

パスワードを設定して、セキュリティ対策ツールの設定を変更できないようにできます(35ページ)。

ヒント

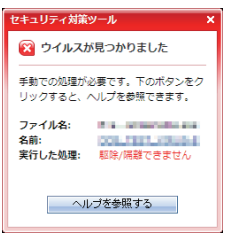
初期設定でお子さまをインターネット上の脅威から保護することができる？

前記の対策は初期設定では有効にされていません。必要に応じて設定を行ってください。

10 メッセージが表示されたときは？

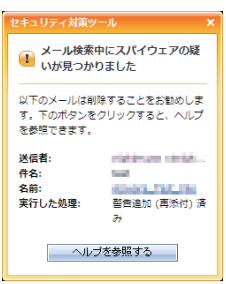
本ツールは、何らかの危険を見つけたときや処理を行ったときにメッセージを表示します。危険性の高さはメッセージの枠の色で確認できます。

メッセージの種類



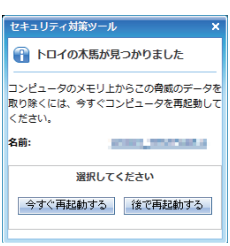
危険性が高いときのメッセージ - 赤色の枠

危険性が高いときは赤色の枠でメッセージが表示されます。



注意を要するときのメッセージ - 黄色の枠

注意を要するときは黄色の枠でメッセージが表示されます。

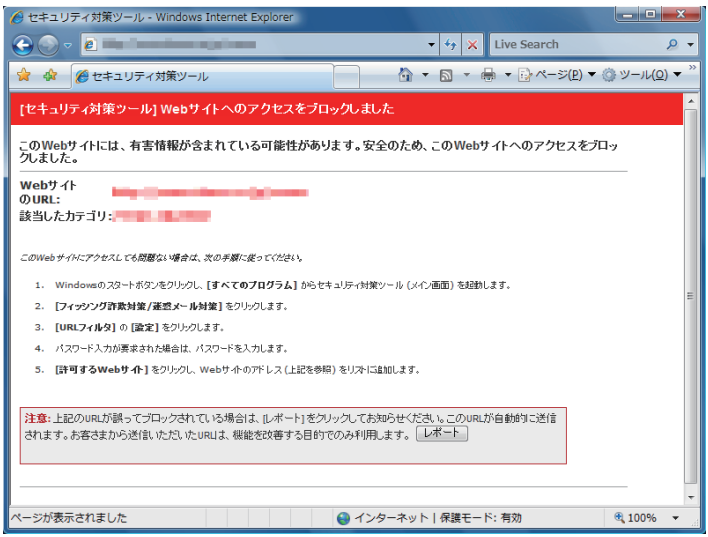


報告のみのメッセージ - 青色の枠

問題が見つかったものの正常に処理できたときなどの報告は青色の枠でメッセージが表示されます。

その他のメッセージ

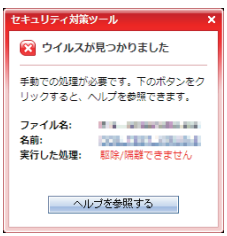
指定された有害サイトや偽装サイトを表示しようとしたときは、Webサイトが次のような内容に置き換わって表示されます。



11 赤色の枠でメッセージが表示されたときは？

ウイルスやスパイウェアなどの脅威を見つけ、手動での処理や判断が必要な場合に赤色の枠でメッセージが表示されます。このメッセージが表示された場合は情報をきちんと確認し、あわてずに対処してください。

メッセージ一覧



ウイルス（トロイの木馬、スパイウェアの疑い）が見つかりました

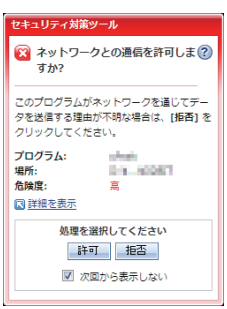
ウイルスまたはトロイの木馬、スパイウェアが見つかり、自動で駆除または隔離できなかった場合に表示されます。

処理方法

1 ウイルスまたはトロイの木馬、スパイウェアの［名前］をクリックする。

2 ［概要］をクリックし、ウイルスまたはトロイの木馬、スパイウェアの特徴を確認する。

3 ［対応方法］をクリックし、画面の指示に従ってウイルスまたはトロイの木馬、スパイウェアを手動で処理する。



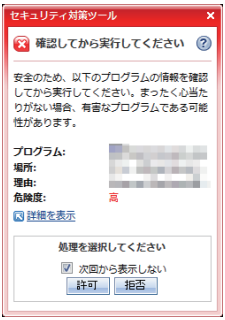
ネットワークとの通信を許可しますか？

パーソナルファイアウォールにより、ネットワークを通じてデータを受信または送信しようとしているソフトウェアが見つかった場合に表示されます。

処理方法

1 ［詳細を表示］をクリックし、ソフトウェアの詳細情報を確認する。

2 ソフトウェアを実行させてもよい場合は［許可］を、実行させたくない場合は［拒否］をクリックする。



確認してから実行してください

パソコンの設定に対して、スパイウェアとの関連が疑われる不審な変更が見つかった場合に表示されます。

危険度に応じて赤色または黄色の枠で表示されます。

処理方法

1 ［詳細を表示］をクリックし、プログラムの詳細情報を確認する。

2 プログラムを実行させてもよい場合は［許可］を、実行させたくない場合は［拒否］をクリックする。

ヒント

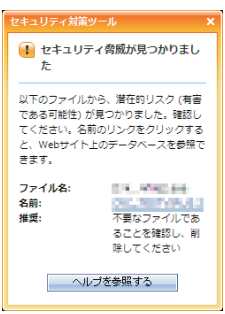
ソフトウェアのインストール中に表示された場合は、インストールに伴う設定の変更である可能性があるため、詳細情報をご確認の上、変更を許可することをおすすめします。

［次回から表示しない］にチェックを入れて［許可］または［拒否］を選択すると、該当ソフトウェアが許可対象または拒否対象として例外設定され、同じソフトウェアに対するメッセージは表示されなくなります。例えば、一度拒否したソフトウェアを再度使用する必要が生じた場合などは、［不正変更の監視］の［例外設定］から該当ソフトウェアの拒否登録を削除する必要があります。詳しくはヘルプの「例外処理を行うソフトウェアを設定する」を参照ください。

12 黄色の枠でメッセージが表示されたときは？

注意を要する脅威を見つけた場合に黄色の枠でメッセージが表示されます。危険度が不明な場合もあるので、情報を確認して適切に対処してください。

メッセージ一覧



セキュリティ脅威が見つかりました

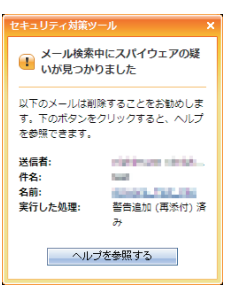
ファイルから潜在的な危険が見つかった場合に表示されます。

処理方法

1 ［名前］に表示されているファイル名をクリックする。

2 ［概要］をクリックし、ファイルの特徴を確認する。

3 ［対応方法］をクリックし、画面の指示に従ってファイルを手動で処理する。



スパイウェアの疑いが見つかりました

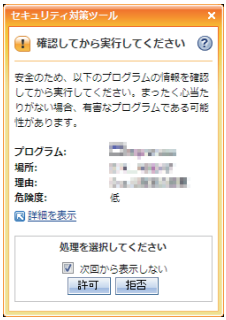
スパイウェアの疑いがあるソフトウェアが見つかった場合に表示されます。

処理方法

1 ［名前］に表示されているスパイウェア名をクリックする。

2 ［概要］をクリックし、スパイウェアの特徴を確認する。

3 ［対応方法］をクリックし、画面の指示に従ってスパイウェアを手動で処理する。



確認してから実行してください

パソコンの設定に対して、スパイウェアとの関連が疑われる不審な変更が見つかった場合に表示されます。

危険度に応じて赤色または黄色の枠で表示されます。

処理方法

1 [詳細を表示]をクリックし、プログラムの詳細情報を確認する。

2 プログラムを実行させてもよい場合は[許可]を、実行させたくない場合は[拒否]をクリックする。

ヒント

ソフトウェアのインストール中に表示された場合は、インストールに伴う設定の変更である可能性があるため、詳細情報をご確認の上、変更を許可することをおすすめします。

[次回から表示しない]にチェックを入れて[許可]または[拒否]を選択すると、該当ソフトウェアが許可対象または拒否対象として例外設定され、同じソフトウェアに対するメッセージは表示されなくなります。例えば、一度拒否したソフトウェアを再度使用する必要が生じた場合などは、[不正変更の監視]の[例外設定]から該当ソフトウェアの拒否登録を削除する必要があります。詳しくはヘルプの「例外処理を行うソフトウェアを設定する」を参照ください。

hostsファイルの変更が見つかりました

hostsファイルの記述の変更が見つかった場合に表示されます。hostsファイルの記述を変更した覚えがない場合は[削除]をクリックしてください。

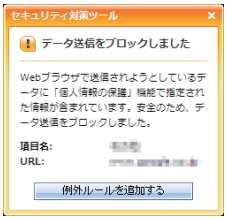
処理方法

1 [詳細を表示]をクリックし、プログラムの詳細情報を確認する。

2 プログラムを実行させてもよい場合は[許可]を、実行させたくない場合は[削除]をクリックする。

ご注意

hostsファイルが書き換えられると、Webブラウザに正しいURLを入力しても詐欺サイトなどの別のWebサイトに誘導されるおそれがあります。



データ送信をブロックしました

保護されている個人情報が、Webブラウザやメール、インスタントメッセンジャー経由で送信されるのをブロックした場合に表示されます。

ヒント

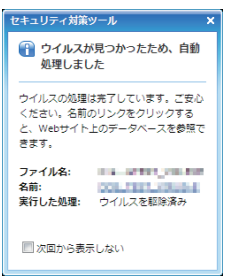
Webブラウザで個人情報が送信された場合、[例外ルールを追加する]をクリックすると、ブロックされた個人情報の送信を例外的に許可します。

許可したURLは、[個人情報の保護]画面に、[許可するWebサイト]として登録され、次回以降の個人情報の送信がブロックされなくなります。

13 青色の枠でメッセージが表示されたときは？

ウイルスやスパイウェアなどの脅威を見つけ、自動的に処理したときに青色の枠でメッセージが表示されます。

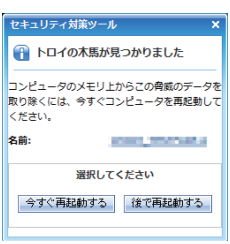
メッセージ一覧



ウイルス（トロイの木馬、スパイウェアの疑い）が見つかったため、自動処理しました

ウイルスまたはトロイの木馬、スパイウェアの疑いが見つかり、自動で駆除、隔離またはファイルの削除をした場合に表示されます。

ウイルスまたはトロイの木馬、スパイウェアの処理は完了しているので、ご安心ください。



トロイの木馬（スパイウェアの疑い）が見つかりました

トロイの木馬またはスパイウェアが見つかり、ファイル削除の処理や、改変されたシステム情報の修復を行うために、再起動が必要な場合に表示されます。

通常は［今すぐ再起動する］をクリックしてください。

14 よくある質問と回答 Q&A

インターネット(ネットワーク)の接続に関する質問と回答

Q ネットワークに接続できなくなった場合は?

A お客さまのパソコンのセキュリティ状況やセキュリティ対策ツールの設定によってはインターネットなどのネットワークに接続できなくなることがあります。次の点をご確認ください。

1. ウイルスやスパイウェアの検索を行う

「ウイルスやスパイウェアを検索する」(12ページ)の手順に従って、ウイルスやスパイウェアの検索を行ってください。

2. 緊急ロックの設定を確認する

「緊急ロックの設定を確認する」(48ページ)に従って、緊急ロックの設定を確認してください。

3. パーソナルファイアウォールの設定を確認する

「パーソナルファイアウォールの設定を確認する」(48ページ)の手順に従って、パーソナルファイアウォールの設定を確認してください。

4. フィッシング詐欺対策の設定を確認する

特定のWebサイトが表示できない場合は「フィッシング詐欺対策の設定を確認する」(49ページ)の手順に従って、フィッシング詐欺対策の設定を確認してください。

5. URLフィルタの設定を確認する

特定のWebサイトが表示できない場合は「URLフィルタの設定を確認する」(50ページ)の手順に従って、URLフィルタの設定を確認してください。

6. 以上を確認しても接続できない場合は……

セキュリティ対策ツール以外の原因によるものと推測されます。お使いのパソコンの販売元やご契約のプロバイダにお問い合わせいただくことをおすすめします。

緊急ロックの設定を確認する

デスクトップ右下の通知領域(タスクトレイ)にあるセキュリティ対策ツールのアイコン(9ページ)が  になっている場合、緊急ロックが有効になっている可能性があります。

緊急ロックが有効になっているとインターネットを含むすべてのネットワークに接続できません。このアイコンを右クリックすると表示されるメニューから[緊急ロックを解除]を選択し、緊急ロックを解除してください。

パーソナルファイアウォールの設定を確認する

パーソナルファイアウォールが適切に設定されていないために、ネットワークが利用できなくなる場合があります。

次の手順でいったんパーソナルファイアウォールを無効にして、ネットワークに接続できるようになるか確認してください。

ご注意

パーソナルファイアウォールを無効に設定すると、警告が表示されることがあります。

1 メイン画面を表示する(5ページ)。
2 画面左側の[不正侵入対策/ネットワーク管理]をクリック。
3 [パーソナルファイアウォール]の[設定]をクリック。
[パーソナルファイアウォール]画面が表示されます。
4 [パーソナルファイアウォールを有効にする]のチェックボックスをオフにする。
5 [OK]をクリック。
パーソナルファイアウォールが無効になります。

この状態で、ネットワークに接続できない場合は、別の原因が考えられます。[パーソナルファイアウォールを有効にする]のチェックボックスをオンに戻してください。

パーソナルファイアウォールを無効にしてネットワークに接続できるようになった場合は、[パーソナルファイアウォール]画面の[この画面の説明]をクリックしてヘルプを表示し、次の設定を確認してください。

- Webブラウザやメールソフトなど、種類の異なるソフトウェアでネットワークに接続できない場合は、プロファイルを切り換えてみてください。
- メールソフトでは接続できないが、Webブラウザでは接続できるというように、一部のソフトウェアでネットワークに接続できなくなっている場合は、パーソナルファイアウォールの例外ルールの設定を確認してください。

フィッシング詐欺対策の設定を確認する

フィッシング詐欺対策が適切に設定されていないために、特定のWebサイトが表示できなくなる場合があります。

次の手順でいったんフィッシング詐欺対策を無効にして、Webサイトが表示できるようになるかどうか確認してください。

1 メイン画面を表示する(5ページ)。
2 画面左側の[フィッシング詐欺/迷惑メール対策]をクリック。
3 [フィッシング詐欺対策]の[設定]をクリック。
[フィッシング詐欺対策]画面が表示されます。
4 [フィッシング詐欺対策を有効にする]のチェックボックスをオフにする。
5 [OK]をクリック。

この状態で、Webサイトが表示できない場合は、別の原因が考えられます。[フィッシング詐欺対策を有効にする]のチェックボックスをオンに戻して

ください。

フィッシング詐欺対策を無効にしてWebサイトが表示されるようになった場合は、[フィッシング詐欺対策]画面の[この画面の説明]をクリックしてヘルプを表示し、設定を確認してください。

URLフィルタの設定を確認する

URLフィルタが適切に設定されていないために、特定のWebサイトが表示できなくなる場合があります。

次の手順でいったんURLフィルタを無効にして、Webサイトが表示できるようになるかどうか確認してください。

1. メイン画面を表示する(5ページ)。
2. 画面左側の[フィッシング詐欺/迷惑メール対策]をクリック。
3. [URLフィルタ(Webアクセス規制)]の[設定]をクリック。
   [URLフィルタ(Webアクセス規制)]画面が表示されます。
4. [URLフィルタを有効にする]のチェックボックスをオフにする。
5. [OK]をクリック。

この状態で、Webサイトが表示できない場合は、別の原因が考えられます。[URLフィルタを有効にする]のチェックボックスをオンに戻してください。

URLフィルタを無効にしてWebサイトが表示されるようになった場合は、[URLフィルタ(Webアクセス規制)]画面の[この画面の説明]をクリックしてヘルプを表示し、設定を確認してください。

Q ネットワークを利用するソフトウェアが使えない場合は?

A パーソナルファイアウォールが、ソフトウェアの通信をブロックしている可能性があります。次の手順で、パーソナルファイアウォールの設定を確認してください。

1. メイン画面を表示する(5ページ)。
2. 画面左側の[不正侵入対策/ネットワーク管理]をクリック。
3. [パーソナルファイアウォール]の[設定]をクリック。
   [パーソナルファイアウォール]画面が表示されます。
4. [プロファイルの変更]をクリック。
5. [プロファイルの設定]画面の[編集]をクリック。
6. [例外ルール(プログラム)]タブを選択。

7 正常に通信できないソフトウェアの項目をダブルクリックするか、選択して[編集]をクリック。

[プロファイルの設定]画面が表示されます。

8 [簡易設定]を選択。

9 [許可]を選択。

10 [OK]をクリック。

11 [OK]をクリック。

12 [OK]をクリック。

13 [OK]をクリック。

メイン画面に戻ります。

ヒント

手順8で[詳細設定]を選択すると、プロトコルやポート番号を指定して設定することもできます。詳細はヘルプを参照してください。

また、手順6で[例外ルール(プロトコル)]をクリックすると、ソフトウェアを限定せずにプロトコルやポート番号を指定して設定することもできます。詳細はヘルプを参照してください。

なお、ネットワークへの接続機器であるルータが通信をブロックしていることもあります。上記の設定を行っても改善されない場合は、ルータの設定もご確認ください。

Q LAN上のほかのパソコンに接続できなくなった場合は?

A セキュリティ対策ツールの「パーソナルファイアウォール」機能とWindowsの「Windows ファイアウォール」の両方が有効になっていると、接続できなくなる場合があります。

次の手順でWindows ファイアウォールを無効にしてください。

Windows XPの場合

1 デスクトップ左下の[スタート]メニューから[コントロールパネル]をクリック。

[コントロールパネル]画面が表示されます。

2 [ネットワークとインターネット接続]をクリック。

3 [Windows ファイアウォール]をクリック。

[Windows ファイアウォール]画面が表示されます。

4 [無効]を選択して、[OK]をクリック。

Windows ファイアウォールが無効になります。

Windows Vistaの場合

1 デスクトップ左下の[スタート]メニューから[コントロールパネル]をクリック。

[コントロールパネル]画面が表示されます。

2 [ネットワークとインターネット]をクリック。

3 [Windows ファイアウォール]の下の[Windows ファイアウォールの有効化または無効化]をクリック。

[ユーザー アカウント制御]画面が表示されます。

4 [続行]をクリック。

[Windows ファイアウォールの設定]画面が表示されます。

5 [無効]を選択して、[OK]をクリック。

Windows ファイアウォールが無効になります。

ウイルスやスパイウェアに関する質問と回答

Q 「ネットワークウイルスを処理しました」と頻繁に表示されるが大丈夫?

A この場合は、ネットワークウイルスの処理に成功しているので問題ありません。

このメッセージは、外部のパソコンに感染したウイルスが、ネットワークを通じて侵入を試みているときなどに表示されます。

Q 検索するといつもcookieというスパイウェアが見つかるが大丈夫?

A 通常は問題ありません。

クッキー(cookie)は、Webサイトがユーザの識別や入力情報の保存などの目的でユーザ側のパソコンに一時的に記録する情報です。

クッキーがパソコンに被害を与えることはありませんが、広告の効果測定などの目的で、個人情報の保護という観点からは不適切と思われる使われかたをしていることもあるため、スパイウェアとして検出しています。

メールに関する質問と回答

Q メールが送受信できなくなったときは?（エラーメッセージとして、「0x8004210A」や「0x800CCC15」が表示される）

A パーソナルファイアウォールが、Microsoft OutlookやOutlook Expressの通信をブロックしている可能性があります。

「ネットワークを利用するソフトウェアが使えない場合は？」(50ページ)と同様の手順で、[パーソナルファイアウォール例外ルール(プログラム)]画面の「Microsoft Outlook」や「Outlook Express」の設定を確認してください。

インストールやバージョンアップに関する質問と回答

Q アップデート機能でインストールできる?

A インストールできません。

Q アンインストールの方法は?

A アンインストールは次の手順で行ってください。

アンインストールを行うときは、セキュリティ対策ツールのメイン画面を閉じてください。

1 デスクトップ左下の[スタート]メニューから[すべてのプログラム]→[NTTW]→[セキュリティ対策ツール]→[削除(アンインストール)]の順にクリック。

[セキュリティ対策ツール]画面が表示されます。

2 画面の指示に従ってアンインストールを行う。

セキュリティ対策ツールがアンインストールされます。

Q 新しくパソコンを購入した場合は?

A 1つのシリアル番号で、複数のパソコン、複数のOSにセキュリティ対策ツールをインストールすることはできません。新規に購入したパソコンにセキュリティ対策ツールをインストールする場合は、元のパソコンにインストールされているセキュリティ対策ツールをアンインストールするか、ライセンスを追加するためにNTT西日本へ「セキュリティ機能ライセンス・プラス」を

お申し込みください。

また、セキュリティ対策ツールをインストールする前に、新しいパソコンに他のウイルス対策製品やファイアウォール製品がインストールされていないか確認してください。もし、他のウイルス対策製品やファイアウォール製品がインストールされていた場合は、必ずアンインストールしてからセキュリティ対策ツールをインストールしてください。

古いパソコンと新しいパソコンの両方にセキュリティ対策ツールをインストールしたい場合は、「セキュリティ機能ライセンス・プラス」をご契約いただき、新たなシリアル番号をご用意ください。

「セキュリティ機能ライセンス・プラス」のお申し込みは、「0120-116116」にてお申し込みいただけます。

! ご注意

セキュリティ対策ツールは１つのシリアル番号（１ライセンス）につき、１つのOSにのみインストールできます。

Q 複数のパソコン／ OSにインストールする場合は?

A 1つのシリアル番号で、複数のパソコン、複数のOSにセキュリティ対策ツールをインストールすることはできません。セキュリティ対策ツールを複数のパソコンにインストールしたい場合は、別途NTT西日本に「セキュリティ機能ライセンス・プラス」をお申し込みいただき、台数分のシリアル番号をご用意いただく必要があります。同一のシリアル番号を使用して複数のパソコンにインストールする等のご利用形態では、先に使用していたパソコンではセキュリティ対策ツールのアップデートが利用できなくなるため、最新のセキュリティ環境を保つことができません。

「セキュリティ機能ライセンス・プラス」のお申し込みは、「0120-116116」にてお申し込みいただけます。

Q デュアルブートマシンにセキュリティ対策ツールをインストールする場合は?

A 1台のパソコンに複数のOSが導入されている場合でも別途NTT西日本に「セキュリティ機能ライセンス・プラス」をお申し込みいただき、OSと同数分のシリアル番号をご用意いただく必要があります。同一のシリアル番号を使用して複数のOSにインストールするなどのご利用形態では、先に使用していたOSではセキュリティ対策ツールが利用できなくなるため、セキュリティも最新の状態に保つことができなくなります。

「セキュリティ機能ライセンス・プラス」のお申し込みは、「0120-116116」にてお申し込みいただけます。

Q Windowsの再インストールやパソコンのリカバリのときに必要なことは?

A 再インストールやパソコンのリカバリの完了後、セキュリティ対策ツールをインストールしてください。

Q Windowsをバージョンアップしたり、サービスパック(SP)を適用したりする場合に必要なことは?

A Windowsをバージョンアップしたりサービスパック(SP)を適用する場合は、以下の手順で行ってください。

1. 本ツールが新しいWindowsやサービスパック(SP)に対応しているか確認する。
2. 本ツールの動作環境について最新の情報は、「http://flets-w.com/next/service/policy/index.html」を参照してください。

   本ツールが新しいWindowsやサービスパック(SP)に対応していない場合は、対応するまでお待ちください。
3. 必要に応じて新しいWindowsやサービスパック(SP)に対応している最新版のセキュリティ対策ツールを入手する。

   現在使用しているセキュリティ対策ツールが新しいWindowsやサービスパック(SP)に対応していない場合は、案内に従って最新版を入手します。
4. 現在インストールされているセキュリティ対策ツールをアンインストールする。

   アンインストールの手順については、「アンインストールの方法は?」(53ページ)を参照してください。
5. Windowsをバージョンアップまたはサービスパック(SP)を適用する。
6. 新しいWindowsやサービスパック(SP)に対応したセキュリティ対策ツールをインストールする。

! ご注意

万が一セキュリティ対策ツールをアンインストールせずにWindowsをバージョンアップしたりサービスパック(SP)を適用したりすると、セキュリティ対策ツールが正常に動作しなくなるおそれがあります。この場合、Windowsの再インストールが必要になる場合があります。

その他の質問と回答

Q バージョン情報を調べたい場合は?

A 現在ご利用中のセキュリティ対策ツールのプログラム、パターンファイル、検索エンジンなどのバージョンは、セキュリティ対策ツールのメイン画面から確認できます。

メイン画面左側の[ヘルプとサポート]をクリックして[バージョン情報]をクリックすると、次のような画面が表示されます。

Q パスワードを忘れてしまった場合は?

A パスワードを忘れると、パスワードで保護されたすべての機能が利用できなくなります。セキュリティ対策ツールをアンインストールすることもできなくなるので注意してください。

万一パスワードを忘れてしまった場合は、セキュリティ対策ツールがインストールされているフォルダ(初期値はC:¥Program Files¥NTTW¥Security_2008_ver1¥Data¥)内のサポートツール(TISSuprt.exe)を使ってアンインストール後、再インストールを行う必要があります。

サポートツールの使用を誤ると、セキュリティ対策ツールが正しく実行されなくなる場合があります。サポートツールを利用する場合は、ヘルプを参照してください。

Q 「_restore」フォルダからウイルスが見つかる場合は?

A Windows VistaおよびXPの「システムの復元」という機能では、システムが正常に動作している状態で、オペレーティングシステムやシステムファイルのバックアップ(復元ポイント)を保存します。

このバックアップが保存されたときに、お使いのパソコンがウイルスに感染していた場合、バックアップされたファイルにはウイルスが含まれてしまいます。セキュリティ対策ツールで全ドライブに対してウイルス検索を実行しても、バックアップされたファイルはパソコンの障害回復に利用されるデータが含まれるため、ウイルスを駆除またはこのファイルを削除することができません。そのため、バックアップファイルが保存されているバックアップフォルダ（例：C:¥System Volume Information¥_restore）からウイルスが検出されてしまいます。

この問題を回避するには、保存されているバックアップファイルをいったん破棄して、お使いのパソコンに感染ファイルがない状態でバックアップファイルを作成する必要があります。

Windows XPで復元ポイントを破棄するには、次の手順に従ってください。

1. デスクトップ左下の［スタート］メニューから［コントロールパネル］をクリック。
2. ［パフォーマンス］→［システム］の順にクリック。
3. ［システムの復元］タブを選択。
4. ［システムの復元を無効にする］のチェックボックスをオンにして［OK］をクリック。
5. 「システムの復元を無効にしますか？」という確認メッセージが表示されたら、［はい］をクリック。

これでシステムの復元ポイントが破棄されます。この状態でセキュリティ対策ツールでウイルス検索を実行します。ウイルスが見つかった場合は、正しく処理が実行されたことを確認します。

引き続き復元ポイントを再作成します。次の手順に従ってください。

1. デスクトップ左下の［スタート］メニューから［ヘルプとサポート］をクリック。

   ［ヘルプとサポートセンター］画面が表示されます。
2. ［コンピュータへの変更をシステムの復元で元に戻す］をクリック。

   ［システムの復元］画面が表示されます。
3. ［復元ポイントを作成］を選択し、画面の指示に従って復元ポイントを作成します。

Windows Vistaを使用したシステムの復元の破棄、および再作成の方法については、Windowsのヘルプなどを参照してください。

Q パソコンの動作が以前と比べて遅くなった場合は?

A セキュリティ対策ツールをインストールすると、ファイルにアクセスするたびにウイルス検索を実行する「リアルタイム検索」機能が有効になります。リアルタイム検索は非常に高速で実行されますが、ファイルへのアクセスが発生するたびにウイルス検索が実行されるため、インストール前よりもパソコンの動作が遅くなったように感じられることがあります。

ただし、これはウイルスが侵入しないようにするために欠かせない処理であるため、セキュリティ対策ツールをアンインストールしたり、リアルタイム検索を無効にすることはおすすめできません。

たとえば、リアルタイム検索で検索する対象を変更してみたり、一時的にリアルタイム検索を無効にすることは可能です。ただし、リアルタイム検索の設定をむやみに変更すると、ウイルスが侵入する原因にもなります。設定の変更は慎重に行ってください。

Q 利用しているアプリケーションなどで通信が急にできなくなりました。どうしたらよいですか?

A セキュリティ対策ツールのパーソナルファイアウォールにおいて、アプリケーションを指定して例外ルールを登録した場合は、プログラムの変更などによりアプリケーションのバージョンが変更されると通信ができなくなることがあります。また、システムプログラムを指定した場合も、オペレーティングシステムのプログラムがMicrosoft Updateなどによりバージョンアップするとプログラムが変更となるので通信ができなくなることがあります。その場合は、当該の例外ルールを選択してアプリケーションやシステムプログラムを再度指定してください。

また、セキュリティレベルで「高」「中」「中低」を選択した場合や、例外ルールでアクセス処理を「警告」に設定した場合は、通信の送信時に「ソフトウェアによりネットワークへのアクセスが要求されています。」といった警告画面が表示されます。

表示された警告画面で[拒否]をクリックした場合は、例外ルールの最上部に当該通信の拒否ルールが追加され、以後その通信は常に拒否されますので、通信を許可したい場合は、通信の拒否ルールとして登録された当該の設定内容を削除または変更してください。

Q セキュリティ対策ツール：「例外メール検出のお知らせ」というメールが届いた場合は?

A セキュリティ対策ツールの受信メール（POP3）検索機能では、メールヘッダが異常なメールや、壊れたメールなどを受信した場合に、これらのメールを「例外メール」と判断して処理を実行します。

「例外メール」と判断された場合、「セキュリティ対策ツール：例外メール検出のお知らせ」という件名のメールが届きます。このメールは開いても安全です。このメールには、元のメールがテキストファイルに変換されて添付されています。ウイルスが添付されている可能性がありますので、添付ファイルは開かずに削除することをおすすめします。

Q 暗号化されたメールのメール検索は?

A PGP（Pretty Good Privacy）をはじめとしたデータの暗号化においては、秘密鍵および公開鍵を持つ同士のみが、決められた鍵を使用してデータの復号を行う仕組みになっています。

このため、セキュリティ対策ツールのメール検索機能では、暗号化されたデータの内容を検証することができず、ウイルスを検出できません。

なお、メール内にウイルスが含まれていた場合でも、リアルタイム検索が有効な状態であればデータの復号が実行された後にウイルスに対する処理が行われます。

Q ネットワーク経由で使用するソフトを利用する方法は?

A インスタントメッセンジャーやオンライン銀行サービス用のソフトウェアなど、ネットワークを経由してデータを送受信するソフトウェアをお使いの場合、パーソナルファイアウォールの設定を変更しないと、ネットワーク経由でのデータ送受信機能を利用できなくなる場合があります。これは、パーソナルファイアウォールの機能の性質上、安全かどうかを判断できないネットワークアクセスをブロックする必要があるためです。

使用するアプリケーションの安全性に問題がないことをご判断いただいた上で、お客さまがお使いの環境に応じてパーソナルファイアウォールを手動で設定してください。次に簡単な設定例をご紹介します。

たとえば、ネットワーク経由でチャットを楽しむソフトウェアをお使いだと想定します。このソフトウェアには、チャット相手にネットワーク経由で画像ファイルを送信する機能があります。セキュリティ対策ツールのインス

トール後、この画像ファイルの送信機能が利用できなくなってしまったとします。この場合、パーソナルファイアウォールの設定を、次の手順で変更します。

1 メイン画面を表示する(5ページ)。

2 画面左側の[不正侵入対策/ネットワーク管理]をクリック。

3 [パーソナルファイアウォール]の[設定]をクリック。
[パーソナルファイアウォール]画面が表示されます。

4 [プロファイルの変更]をクリック。
[プロファイルの設定]画面が表示されます。

5 [編集]をクリック。

6 [例外ルール(プログラム)]タブを選択して、[追加]をクリック。
[パーソナルファイアウォール例外ルール(プログラム)]画面が表示されます。

7 次の内容を設定します。

項目	設定
例外ルールの名前	「チャットソフト用」など、この設定にふさわしい名前をつけます。
対象	「指定のプログラム」を選択して[参照]をクリックします。チャットソフトの実行プログラムのファイル(例:chat.exe)を探して選択します。多くの場合実行プログラムは「[マイコンピュータ]→[ローカルディスク(C:)]→[Program Files]」と辿った先に存在します。
設定	「簡易設定」または「許可」を選択します。

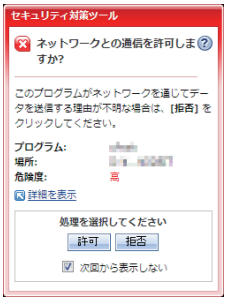
ご注意

パーソナルファイアウォールのプロファイルを編集する場合は、事前に起動中の他のアプリケーションをすべて終了してください。他のアプリケーションを起動したままプロファイルを編集すると、設定どおりにアクセスが許可またはブロックされない場合があります。

8 [OK]をクリック。
[プロファイルの設定]画面に戻ります。

9 [OK]をクリック。

Q 「ネットワークとの通信を許可しますか?」という画面が表示される場合は?



A ネットワークを介してデータを送受信するプログラムをお使いの場合、「ネットワークとの通信を許可しますか?」という画面が表示されることがあります。これはパーソナルファイアウォールで次のような設定がされている場合です。

- パーソナルファイアウォールのセキュリティレベルを「高」または「中」にしている場合
- 特定の送信アクセスが発生した場合に、警告を表示するように例外ルールを設定している場合

[次回から表示しない]のチェックボックスをオンにして[許可]をクリックすると、このアクセスが許可されます。以降は同じ種類のアクセスが発生しても、警告画面は表示されなくなります。

ただし、1度許可したプログラムであってもバージョンアップした場合は、警告画面が表示される場合があります。

[次回から表示しない]のチェックボックスをオンにして、[拒否]をクリックすると、このアクセスはブロックされます。以降は同じ種類のアクセスがすべてブロックされます。ただし、1度拒否したプログラムであってもバージョンアップした場合は、警告画面が表示される場合があります。

例外設定に関する詳細は、ヘルプを参照してください。

Q デスクトップ右下の通知領域(タスクトレイ)からポップアップ表示を消すには?

A セキュリティ対策ツールでデスクトップ右下からポップアップメッセージが表示されるのは、次のケースが考えられます。いくつかのケースでは、非表示にできないものがあります。詳細は、次の表を参照してください。

項目	説明
リアルタイム検索が有効になりました	リアルタイム検索の有効／無効を切り替えた場合に表示されます。 このポップアップメッセージを非表示にすることはできません。
緊急ロックがかかりました	緊急ロックの有効／無効を切り替えた場合に表示されます。 このポップアップメッセージを非表示にすることはできません。
受信メールを検索しました	受信メール(POP3)の検索が開始された場合に表示されます。 このポップアップメッセージを非表示にする方法については35ページを参照してください。
送信メールを検索しました	送信メール(SMTP)の検索が開始された場合に表示されます。 このポップアップメッセージを非表示にする方法については35ページを参照してください。
Webメールを検索しました	Webメールの添付ファイルのダウンロードが開始された場合に表示されます。 このポップアップメッセージを非表示にする方法については35ページを参照してください。
管理者からのリクエストにより、ウイルス検索を開始しました	ホームネットワークの管理者から、ウイルス検索のリクエストを受けた場合に表示されます。 このポップアップメッセージを非表示にすることはできません。

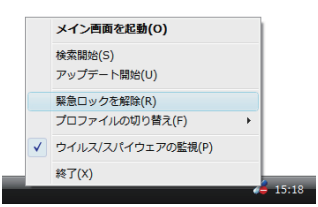
項目	説明
管理者からのリクエストにより、アップデートを開始しました	ホームネットワークの管理者から、アップデートのリクエストを受けた場合に表示されます。 このポップアップメッセージを非表示にすることはできません。
管理者からのリクエストにより、セキュリティ診断を開始しました	ホームネットワークの管理者から、セキュリティ診断のリクエストを受けた場合に表示されます。 このポップアップメッセージを非表示にすることはできません。
管理者からのリクエストにより、設定が変更されました	ホームネットワークの管理者から、設定変更のリクエストを受けた場合に表示されます。 このポップアップメッセージを非表示にすることはできません。
プロファイルが切り替わりました	パーソナルファイアウォールのプロファイルを切り替えた場合に表示されます。 このポップアップメッセージを非表示にすることはできません。

Q 緊急ロックを解除するには?

A 緊急ロック機能を解除する前に、パソコン上にウイルスや不正プログラムが残っていないか、ウイルス検索を実行してください。次のいずれかの方法で緊急ロックを解除できます。

通知領域(タスクトレイ)上のアイコンから解除する

1 通知領域(タスクトレイ)に表示されたセキュリティ対策ツールのアイコン を右クリック。



2 表示されたメニューから[緊急ロックを解除]を選択してチェックをはずす。

次のようなポップアップメッセージが表示され、緊急ロックが解除されます。

Q URLフィルタ機能やフィッシング詐欺対策機能で、サーバに送信される情報とは何ですか?

A URLフィルタ機能やフィッシング詐欺対策機能については、お客さまがアクセスしようとしているWebサイトやソフトウェアが安全かどうかを判定するために、お客さまがアクセスしたWebサイトのURLおよびIPアドレスを暗号化して有害サイトを管理するデータベースサーバに送信し、データベースと照合することで安全かどうかの判定を行っています。

Webサイトの安全性を判定するにあたっては、WebサイトのURLおよびIPアドレスの情報のみが送信され、それ以外の情報が送信されることはありません。ただし、セキュリティ上問題のある一部のWebサイトなどでは、URLの末尾に個人情報を含むパラメータがデータベースサーバに送信される可能性があります(パラメータとは以下の例では「name=west_taro」の部分が該当します)。パラメータを含むURLの場合、パラメータを除いたURLの情報のみが蓄積されるため、お客さまの個人情報がデータベースに蓄積されることはありません。また、蓄積されたURLおよびIPアドレスの情報は、セキュリティ対策機能の改善の目的にのみ利用され、それ以外の目的で利用されることはありません。

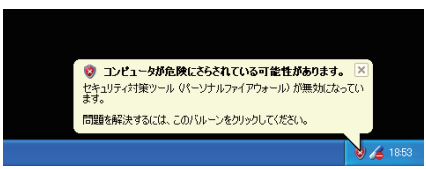
(例)

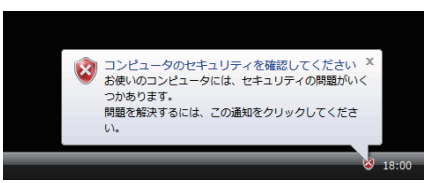
http://www.example.co.jp/securitymeasure.asp?name=west_taro

※本機能は技術供与元であるトレンドマイクロ株式会社が提供する機能であり、お客さまがアクセスしたWebサイトのURLおよびIPアドレスの情報はトレンドマイクロ株式会社のデータベースに送信、蓄積されます。これらの情報はWebサイトの安全性判定とセキュリティ対策機能の改善の目的にのみ利用されます。

Q 「コンピュータが危険にさらされている可能性があります。」(Windows XP の場合)、「コンピュータのセキュリティを確認してください」(Windows Vistaの場合)というポップアップメッセージが表示される場合は?

A Windows XP SP2から搭載されたWindows セキュリティセンターにより、ご利用のパソコンのウイルス対策ソフトの状態が表示されるようになりました。





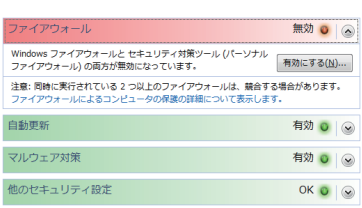
このメッセージが表示された場合、次の原因が考えられます。

アップデートにともない、セキュリティ対策ツールが再起動している。

アップデートにより、パターンファイルなどを読み込むため、セキュリティ対策ツール自体が再起動します。このとき、Windows セキュリティセンターがセキュリティ対策ツールが起動していないと判断するためにメッセージが表示されますが、一時的なものであり、問題はありません。

パーソナルファイアウォールが無効に設定されている。

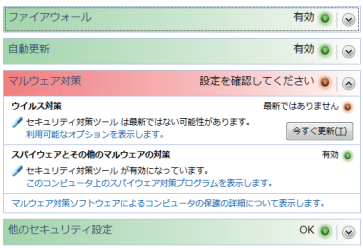
Windows セキュリティセンターが次の表示になっている場合、セキュリティ対策ツールのパーソナルファイアウォールが無効に設定されています。



不正アクセスからパソコンを守るために、セキュリティ対策ツールのパーソナルファイアウォールを有効に設定することをおすすめします。

セキュリティ対策ツールに適用されているパターンファイルのバージョンが10日以上更新されていない。

セキュリティ対策ツールに適用されているパターンファイルのバージョンが10日以上更新されていない場合、Windows セキュリティセンターが警告を表示します。また、Windows セキュリティセンターの状態が次のように表示されます。

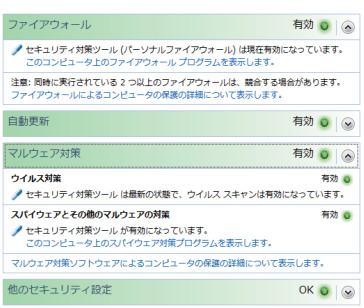


警告が表示された場合、セキュリティ対策ツールの手動によるアップデートを実行し、最新のパターンファイルを適用してください。また、セキュリティ対策ツールを常に最新の状態に保つために、インテリジェントアップデートを有効に設定することをおすすめします。

Q Windows セキュリティセンターからセキュリティ対策ツールの状態を確認するには?

A Windows XP SP2以降とWindows Vistaに搭載されているWindows セキュリティセンターでは、ウイルス対策やファイアウォールの状態を確認できます。

セキュリティ対策ツールのリアルタイム検索、パーソナルファイアウォールが有効に設定されている場合、Windows セキュリティセンターでは次のように表示されます。



この図は有効に設定されている状態です(Windows Vistaの場合)。

パソコンのセキュリティを高めるために、リアルタイム検索、パーソナルファイアウォールは有効に設定することをおすすめします。

Q ウイルス検索が突然始まる場合は?

A 自動的に実行されるウイルス検索やセキュリティ診断は、「予約検索」と呼ばれる機能です。初期設定では、3つの予約検索設定が設定されています。この設定を無効にするには、次の手順に従ってください。

1. メイン画面を表示する(5ページ)。
2. 画面左側の[ウイルス/スパイウェア対策]をクリック。
3. [予約検索/手動検索]の[予約検索]をクリック。
   [予約検索]画面が表示されます。
4. 不要な予約検索設定のチェックボックスをオフにする。
5. [OK]をクリック。
   設定内容が保存され、画面が閉じます。

Q 見つかったウイルス名やスパイウェア名から詳細情報を調べるには?

A ウイルス検出をお知らせする画面がまだ開いている場合は、表示されたウイルス名をクリックすると、ウイルスデータベースにアクセスできます。

ウイルス検出をお知らせする画面をすでに閉じてしまった場合は、次の手順でウイルス情報を調べます。

1. メイン画面を表示する(5ページ)。
2. 画面左側の[アップデート/その他]をクリック。
3. [ログ(履歴)]にあるメニューから[ウイルス検索]または[スパイウェア検索]を選択して[ログの表示]をクリック。
   [ログ(履歴)]画面が表示されます。
4. 調べたいウイルス名を選択し、[詳細情報]をクリック。
   Webブラウザが起動し、ウイルスデータベースに登録されたウイルス情報が表示されます。

! ご注意

ウイルスデータベースにアクセスするには、インターネットへの接続環境が必要です。

Q 通常メールが迷惑メールとして処理される場合は?

A 迷惑メール判定機能は、メールの件名や本文に含まれる特定のキーワードなどを元に迷惑メールを判定します。このため、広告性の強いメールなどの場合、迷惑メールと判定されることがあります。

これを踏まえた上で、迷惑メール判定の精度を設定する方法には、次の3つがあります。

迷惑メール判定レベルを下げる

頻繁に誤判定が起こる場合は、迷惑メールの判定レベルを下げることで対応できます。判定レベルを下げれば、「迷惑メール」と判定されていたメールも、通常メールとして受信することが可能になります。

判定レベルを下げる方法は、ヘルプを参照してください。

送信者のメールアドレスを、迷惑メールの監視の例外アドレスとして登録する

セールの案内メールなど、広告要素が強く、判定レベルを下げただけでは通常メールと判断されないような場合、送信者のメールアドレスを例外アドレスとして登録できます。

詳細については、ヘルプを参照してください。

メールの判定について報告する

「迷惑メール対策ツール」の判定の結果、誤って判定されたメールを、技術供与元であるトレンドマイクロ株式会社に報告できます。

1 Microsoft Outlook、Microsoft Outlook ExpressまたはMicrosoft Windows メールの受信トレイ、または迷惑メールフォルダなどから、誤って判定されたメールを選択する。

2 迷惑メールとして報告する場合は [迷惑メールとして報告] ボタンを、安全メールとして報告する場合は [安全メールとして報告] ボタンをクリックする。

[迷惑メールとして報告]画面または[安全メールとして報告]画面が表示されます。

3 画面の内容を確認し、はい をクリックする。

選択されたメールが、トレンドマイクロ株式会社に送信され、画面が閉じます。

ヒント

[次回からこのダイアログを表示しない]のチェックボックスをオンにすると、次回から確認する画面が表示されなくなります。

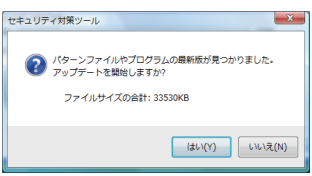
ご注意

お客さまからお送りいただいた情報は、迷惑／詐欺メール判定の精度をより高める目的でのみ利用します。お客さまから送信していただいたメールは、システムにより自動処理されます。このため、お送りいただいたメールに関するご質問などには、サポート窓口などにお問い合わせいただいても、回答はいたしかねます。あらかじめご了承ください。

Q アップデートが突然始まる場合は?

A インテリジェントアップデート機能を有効にしていると、セキュリティ専用サーバに最新版パターンファイルが見つかった場合、自動的にダウンロードが開始されます。

パソコンの使用中に突然アップデートが開始されないよう、ダウンロードを実行する前に「アップデートを実行しますか」という確認メッセージを表示させることができます。



アップデートの前に確認メッセージを表示するよう設定するには、次の手順に従ってください。

1. メイン画面を表示する(5ページ)。
2. 画面左側の[アップデート/その他]をクリック。
3. [アップデート]の[設定]をクリック。
   [インテリジェントアップデート(自動アップデート)]画面が表示されます。
4. [アップデート設定]タブを選択。
5. [インテリジェントアップデート(自動アップデート)を有効にする]の

チェックボックスをオンにする。

6 [常に確認メッセージを表示する]を選択。

7 [OK]をクリックして、設定を保存します。

Q 個人情報の外部送信が正しくブロックされない場合は?

A 個人情報保護設定が、正しく実行されていない可能性があります。次の点をご確認ください。

クレジットカード番号のどの部分をキーワードとして設定しましたか?

たとえばクレジットカード番号が「1234-5678-9012-3456」の場合、保護する個人情報を「1234567890123456」と設定していませんか?個人情報保護機能では、指定した個人情報とまったく同一の文字列が見つかった場合にのみ、送信をブロックします。

「1234567890123456」など、数字の並び順は同一でもハイフン(-)が除かれた文字列が外部に送信された場合、データの送信はブロックされません。

半角/全角文字、大文字/小文字の違いはありませんか?

個人情報保護機能では、半角文字と全角文字、大文字と小文字を異なる文字として識別します。設定した情報が全角数字であった場合、半角数字で記述された番号の外部送信はブロックされません。

キーワードの途中にスペースや改行が含まれていませんか?

たとえば、キーワードとして「12345678」と設定していた場合、「1234<スペース>5678」や「1234<改行>5678」などの文字列の送信はブロックされません。スペースや改行も、文字情報の一部として判断されます。

監視の対象に「メール」を含めていますか?

個人情報保護を設定する際には、設定したキーワードを監視する対象を選択します。

監視の対象には、「メール」、「Webブラウザ」、「インスタントメッセンジャー」の3つがあります。「メール」が監視対象として選択されているかを確認してください。

対応するメールソフトやWebブラウザを使用していますか?

個人情報保護機能の動作保証対象外のメールソフトやWebブラウザをご利用の場合、個人情報の外部送信がブロックされない場合があります。

個人情報保護機能の動作環境については、インストールガイドの「インストールをはじめましょう」を参照してください。

なお、個人情報保護機能では、指定のブラウザを使用したHTTP通信、ポート25を使用したSMTP通信、指定のインスタントメッセンジャーを使用した通信のみを監視対象として設定できます。他のポートを使用した通信は監視されませんのでご注意ください。

Q 特定のWebサイトでのみ個人情報の送信を許可する場合は?

A 個人情報を送信するサイトを「例外Webサイト」に設定することで、個人情報を送信できるようになります。

ここでは、クレジットカード番号を保護する設定をしている場合に、Webサイト「www.shop.ntt-west.co.jp」(例)でのみ、クレジットカード番号を送信できるように設定する手順を説明します。

1 メイン画面を表示する(5ページ)。

2 画面左側の[フィッシング詐欺/迷惑メール対策]をクリック。

3 [個人情報の保護]の[設定]をクリック。
[個人情報の保護]画面が表示されます。

4 [個人情報保護を有効にする]のチェックボックスをオンにする。

5 保護されている個人情報の一覧から「クレジットカード番号」を選択し、[編集]をクリック。
[個人情報の保護]画面が表示されます。

6 [例外設定(許可するWebサイト)]をクリック。
[個人情報の保護]画面が表示されます。

7 [追加]をクリック。
[Webサイトの追加]画面が表示されます。

8 [URLを追加/編集する]を選択し、「www.shop.ntt-west.co.jp」(例)と入力して[OK]をクリック。
[個人情報の保護]画面に戻ります。

9 URLが追加されていることを確認して、[OK]をクリック。
[個人情報の保護]画面に戻ります。

10 [OK]をクリック。
[個人情報の保護]画面に戻ります。

11 [OK]をクリックして、設定を保存します。

これで、Webサイト「www.shop.ntt-west.co.jp」(例)上では、クレジット

カード番号を送信できるようになります。なお、例外Webサイト上での個人情報の送信履歴は、個人情報保護ログに「例外許可」と記録されます。

Q ホームネットワークで、同一ネットワーク内のパソコンが見つからない場合は?

A Windows ファイアウォール機能が有効になっている可能性があります。

Windows ファイアウォール機能が有効になっているパソコンを、ホームネットワーク管理機能で検出することはできません。検出するには、Windows ファイアウォール機能を無効にする必要があります。

Windows ファイアウォール機能を無効にするには、次の手順に従ってください。

Windows XPの場合

1 デスクトップ左下の[スタート]メニューから[コントロールパネル]を選択。

[コントロールパネル]画面が表示されます。

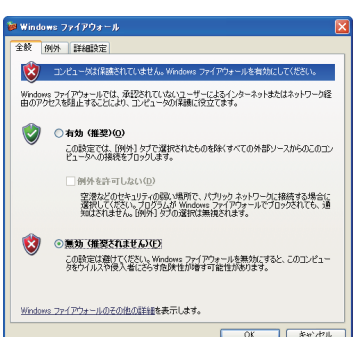
2 [ネットワークとインターネット接続]をクリック。

3 [Windows ファイアウォール]をクリック。

[Windows ファイアウォール]画面が表示されます。

4 [無効]を選択して、[OK]をクリック。

Windows ファイアウォールが無効になります。



Windows Vistaの場合

1 デスクトップ左下の[スタート]メニューから[コントロールパネル]を

選択。

[コントロールパネル]画面が表示されます。

2 [ネットワークとインターネット]をクリック。

3 [Windows ファイアウォール]の下の[Windows ファイアウォールの有効化または無効化]をクリック。

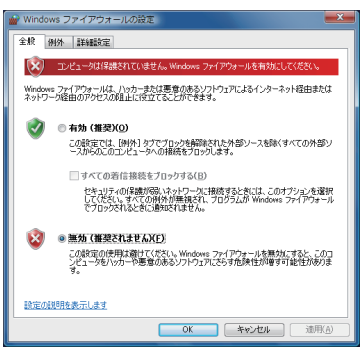
「ユーザー アカウント制御」画面が表示されます。

4 [続行]をクリック。

[Windows ファイアウォールの設定]画面が表示されます。

5 [無効]を選択して、[OK]をクリック。

Windows ファイアウォールが無効になります。



Q パーソナルファイアウォールのログから攻撃元を判断するには?

A 送信元IPアドレスから、そのIPアドレスを管理する組織名や連絡先などの情報を調べることは可能です。

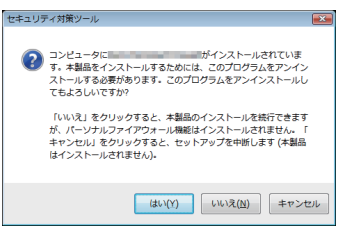
しかし、通常不正アクセスを仕掛ける人物は公開プロキシや他のパソコンを中継(踏み台)にしているため、実際の攻撃元を特定することは難しく、またそのIPアドレスにPingなどを試してしまうことによって、逆に攻撃元に自分の存在を知らせてしまう危険があります。

なお、セキュリティ対策ツールのログに記録されているアクセスはすべてブロックされた記録のため、侵入されている心配はありません。

Q 他社ファイアウォール製品がインストールされた状態でセキュリティ対策ツールをインストールした場合は?

A 他社ファイアウォール製品がインストールされている状態で、セキュリティ対策ツールをインストールしようとすると、次のような画面が表示されます。「いいえ」を選択すると、プログラムの競合を防止するため、セキュリティ対策ツールのパーソナルファイアウォール関連機能（パーソナルファイアウォール機能、無線LANパトロール機能、緊急ロック機能、ネットワークウイルス検索機能）がインストールされません。これらの機能を利用するためには、セキュリティ対策ツールのインストール時に次の画面で「はい」を選択し、先に他社ファイアウォール製品をアンインストール（削除）してセキュリティ対策ツールのインストールをする必要があります。

他社ファイアウォール製品をアンインストールせずにセキュリティ対策ツールをインストールした場合、パーソナルファイアウォール関連機能を有効にするためには、セキュリティ対策ツールと他社ファイアウォール製品を削除した後に、再度セキュリティ対策ツールをインストールし直す必要があります。



Q パーソナルファイアウォールのログ（履歴）が大量に記録されているが大丈夫?

A ログに記録されているものはパーソナルファイアウォールがブロックしたアクセスです。ログの記録量が多いからといって、ただちに不正侵入を心配する必要はありません。

ただし、パーソナルファイアウォールが必要なアクセスまでブロックしてしまっている可能性もあります。たとえば、企業で使用している場合に、プロファイルが「家庭内ネットワーク1」に設定されている場合は、「社内ネットワーク」に変更したほうが適切に処理されるようになります（21ページ）。

Q ウイルスなどの検出履歴を見るには?

A [アップデート/その他]の[ログ（履歴）]で見ることができます。次の手順で操作してください。

1 メイン画面を表示する(5ページ)。

2 画面左側の[アップデート/その他]をクリック。

3 [ログ(履歴)]にあるメニューからログの種類を選択して、[ログの表示]をクリック。

ログ(履歴)が表示されます。

Q URLに日本語を含むWebサイトにアクセスしたときURLフィルタ機能は動作しますか?

A 動作しません。また、URLフィルタ機能の例外設定において、日本語などの全角文字(ダブルバイト文字)を含むURLを設定できません。同様に、URLフィルタ機能の設定画面でWebブラウザの「履歴」や「お気に入り」から日本語などを含むURLのインポートは行えません。

Q ホームネットワーク管理機能で家庭内のLANに接続した他のパソコンの管理ができない場合は?

A ホームネットワーク管理機能の通信では、UDP 40116番ポートを使用しています。

Windows ファイアウォールを使用している場合は、設定を無効にするか、これらのポートを開く必要があります。

Q セキュリティ対策ツールを終了するには?

A セキュリティ対策ツールを終了すると、ウイルスの侵入や不正アクセスなどからパソコンを保護できません。パソコンの電源が入っている間は、セキュリティ対策ツールを常に起動しておくことをおすすめします。

やむを得ず終了する場合は、画面右下の通知領域(タスクトレイ)にあるセキュリティ対策ツールのアイコン を右クリックし、表示されたメニューから[終了]を選択してください。

ヒント

セキュリティ対策ツールの終了後、再び起動したい場合は、「メイン画面を表示する」(5ページ)の手順を行ってください。

Q 受信したメールの添付ファイルが表示されない場合は?

A Outlook Expressを使用していて、「次の添付ファイルは安全でないため、メールからのアクセスが削除されました」と表示される現象は、セキュリティ対策ツールではなく、Outlook Expressによるものです。Outlook Expressの設定につきましては、マイクロソフト社へお問い合わせください。

用語集

- アルファベット -

hostsファイル(ホスツ-)

ホスト名(ドメイン名)とIPアドレスの対応が記載されているファイルです。通常、ホスト名とIPアドレスの対応はパソコンがDNSサーバに問い合わせることで確認されるため、このファイルが使われることはあまりありません。

ただし、WindowsではhostsファイルのDNSサーバへの問い合わせ結果より優先されます。このため、hostsファイルを書き換えて正規のアドレスを入力しても偽のWebサイトが表示されるようにする「ファーミング詐欺」に利用されることがあります。

本ツールはhostsファイルの改変も検出できます。

IPv6(アイピーブイシックス)

IPv6は、「Internet Protocol Version 6」の略です。Internet Protocol(インターネットプロトコル)とは、インターネットで共通に使われている通信手順(プロトコル)の名前です。現在一般に使われているものは、IPv4(バージョン 4)ですが、これの次のバージョンがIPv6です。インターネットの普及に伴い、IPv4で利用できるアドレス空間はあと数年で枯渇するといわれていますが、128ビットの広大なアドレス空間を持つIPv6を利用することで解決されます。

IPアドレス(アイピー -)

ネットワークにおいて個体を識別するための番号で、IPは、Internet Protocolの略です。「192.168.0.1」のように、4組の数字で構成されます。

IPアドレスは、外部に接続しないネットワークで使用できるプライベート(ローカル) IPアドレスと、外部に接続できるグローバルIPアドレスの2種類に分類できます。グローバルIPアドレスはプロバイダなどから割り当てられるものを使用します。

MACアドレス(マック-)

ネットワークカードなどのネットワーク機器に割り当てられている固有の番号で、MACは、Media Access Controlの略です。物理アドレスとも呼ばれるとおり、IPアドレスがソフトウェアとしての番号であるのに対し、MACアドレスはハードウェアとしての番号であるといえます。

Microsoft Update(マイクロソフトアップデート)

WindowsやMicrosoft Office製品の安定性と安全性を向上させるために、マイクロソフト社が提供しているサービスです。

POP3(ポップスリー)

メールソフトがメールサーバに保管されたメールを取得するためのプロトコル(通信手順の規格)で、Post Office Protocol Version 3の略です。

SMTP(エスエムティーピー)

メールソフトからメールサーバまたはメールサーバどうしでメールを転送するためのプロトコル(通信手順の規格)で、Simple Mail Transfer Protocolの略です。

URLフィルタ(ユーアールエル-)

特定のWebサイトの表示を防止するセキュリティ対策ツールの機能です。表示の防止は、カテゴリの指定やURLの指定により行えます。

Webメール(ウェブ-)

メールの送受信をWebブラウザで行えるサービスです。送受信したメールはサービス提供会社のサーバに保管されるため、場所を問わずに利用できます。

Windows Update(ウィンドウズアップデート)

Windowsの安定性と安全性を向上させるために、マイクロソフト社が提供しているサービスです。

Windowsサービス(ウィンドウズ-)

Windowsの起動時やログイン時、あるいは任意の時点で自動的に起動し、システムの一部として動作するソフトウェアです。

Windows ファイアウォール(ウィンドウズ-)

Windows XP SP2以降に標準で搭載されているファイアウォール機能です。Windowsファイアウォールでは内部から外部への通信に制限がなく、ファイアウォールとしては簡易的なものと言えます。

- あ -

圧縮ファイル

データ量を減らすために形式を変換したファイルです。データ量を減らすための変換を圧縮、元に戻すことを解凍と呼ぶことが一般的です。圧縮形式(変換形式)としてはzip形式、lzh形式などがあり、圧縮・解凍ソフトで、圧縮および解凍を行えます。圧縮・解凍ソフトはアーカイブソフト、アーカイバとも呼ばれます。

セキュリティ対策ツールは一般的な圧縮形式に対応しており、圧縮ファイルの中のウイルスも見つけられます。

アップデート

機能の向上や問題点の修正などを目的として、ソフトウェアを構成するファイルの一部を差し替えることです。

インテリジェントアップデート

セキュリティ対策ツールのアップデートを自動的に行う機能です。設定された間隔でアップデートの有無を確認し、アップデートできる場合は自動で行います。インテリジェントアップデートを利用する場合、ネットワークに常に接続されている必要があります。

ウイルス

パソコンに悪影響を与える不正ソフトウェアの一種です。どのような悪影響があるかはウイルスによって異なりますが、典型的な例としては、パソコンに侵入してデータの破壊などの活動を行い、自らをコピーしてネットワークやメールなどの手段を用いて別のパソコンへと被害を広げようとするものが挙げられます。

- か -

隔離

ウイルスやウイルスに感染したファイルが動作しないようにする処理です。隔離したものがパソコンに悪影響を与えることはありません。隔離したファイルは[ウイルス/スパイウェア対策]画面の[隔離ファイルの管理]で元に戻したり、削除したりできます。

感染

ウイルスが侵入し、実行されたか実行できる状態にあることです。

緊急ロック

ネットワーク接続を一時的に切断するセキュリティ対策ツールの機能です。ウイルス感染や不正アクセスの被害拡大を防ぐ目的などで使用します。

駆除

ウイルスを削除したり、ファイルからウイルスを取り除いたりする処理です。駆除に成功したファイルは安全に開けます。

- さ -

詐欺メール

金融機関などを装って送りつけられるメールです。メール内のリンクをクリックすると、あらかじめ用意されている偽サイトに誘導されるので注意が必要です。

シリアル番号

お客さまがセキュリティ対策ツールをお使いのパソコンにインストールする際に使用する20けたの英数字で構成されるユニークな識別番号です。シリアル番号はNTT西日本から＜お申し込み内容のご案内＞でお知らせします。また、同一のシリアル番号を2台以上のパソコンでご利用いただくことはできません。2台以上のパソコンでセキュリティ機能をご利用になる場合は、「セキュリティ機能ライセンス・プラス」をご契約いただくことで、追加台数分の新たなシリアル番号をご提供します。

なお、シリアル番号はお客さまからのお申し出などにより変更することはできません。

スクリプト

スクリプト言語と呼ばれる、簡易的なソフトウェア開発言語を使用して作成されたソフトウェアです。スクリプト言語には、Webサイトを中心に使われるJavaScript（ジャバスクリプト）などがあります。

スパイウェア

パソコンに悪影響を与える不正ソフトウェアの一種です。ウイルスとの違いは個人情報の収集や広告表示の強制などを主な目的としている点です。多くのスパイウェアは、ウイルスが持つようなほかのパソコンへの感染活動は行わず、便利なソフトウェアと称してインストールを要求するなどして、パソコンに侵入します。

セーフモード

Windowsの起動形態の1つで、通常の方法では起動しなくなったときなど、問題が発生した場合の解決に使用します。最小限のソフトウェア構成で起動するため、問題が起きていても多くの場合で起動できます。

セキュリティホール

ソフトウェアの設計ミスなどで生じたセキュリティ上問題のある欠陥です。

- た -

トロイの木馬

パソコンに悪影響を与える不正ソフトウェアの一種です。パソコンに侵入すると、バックドアと呼ばれる不正な侵入経路を作り、パソコンを外部から操作できるようにするなどします。

- な -

ネットワークウイルス

OSを始めとするソフトウェアのセキュリティホールに乗じてパソコンに侵入するウイルスです。ネットワークを通じてほかのパソコンに接続し、セキュリティホールを悪用して感染するため、急速に被害が広がります。Microsoft Updateで提供される更新プログラムをきちんと適用してセキュリティホールをなくしておくことが重要です。

- は -

バージョンアップ

ソフトウェアの設計や操作性を見直すなどの大きな改定を行ったときに、バージョンを改めることです。また、古いバージョンのソフトウェアを新しいバージョンのものと入れ替える作業もバージョンアップと呼ばれます。

パターンファイル

セキュリティ対策ツールを構成するファイルの1つで、既知のウイルスやスパイウェアの特徴(パターン)を記録したものです。パターンファイルはセキュリティ対策ツールがウイルスやスパイウェアの判定を行う際の判定手段となります。

ファイアウォール

パソコンとネットワークの間でのデータのやり取りを監視し、パソコンを外部の攻撃などから守る機能です。

セキュリティ対策ツールが搭載しているパーソナルファイアウォールは、ソフトウェアやプロトコル、ポート番号に対し、それぞれ送受信の方向を指定して制御できます。

フィッシング詐欺

金融機関などを装ったメールを送りつけるなどして偽のWebサイトへと誘導し、ログイン情報やクレジットカード情報などをだまし取ろうとする詐欺です。情報を釣り上げることから英語では「fishing」を言い換えた「phishing」と表記します。

セキュリティ対策ツールはフィッシング詐欺に利用されているWebサイトを検出し、警告を表示します。

不正侵入

不正な手段でパソコンに接続し、パソコン内のデータを抜き取ったり、パソコンを悪用したりすることです。不正アクセスとも呼びます。

プロキシ

内部のパソコンの代わりに外部サーバへの接続を行い、データのやり取りを仲介します。単にプロキシと呼ぶ場合、Webブラウザとwebサーバとのやりとりを仲介するHTTPプロキシのことを指す場合がほとんどです。

プロトコル

パソコン同士がデータをやり取りするために必要な手順などを定めた規格のことです。インターネットの基礎となるデータの転送方法を定めたインターネットプロトコル（Internet Protocol、IP）、WebブラウザとWebサイトのデータのやり取りについて定めたHTTP（Hypertext Transfer Protocol）などがあります。

プロファイル

セキュリティ対策ツールでは、通信環境に応じて切り替えられるファイアウォールの設定を指します。

- ま -

マクロ

ワープロソフトや表計算ソフトなどで一連の処理をあらかじめ記録しておき、あとで実行できるようにするしくみで、定型処理の自動化などの目的で利用されます。Microsoft OfficeではVBA（Visual Basic for Application）と呼ばれるソフトウェア開発言語で記録されており、この言語を使用したウイルスも存在しています。

無線LAN

無線通信でデータを送受信するLANのことです。家庭では無線LANのアクセスポイント機能を持ったルータを設置して利用することが一般的です。LANケーブルによる接続とは異なり、家の外から第三者に接続されてしまうおそれがあるため、セキュリティ対策をきちんと施すことが重要です。

迷惑メール

受信者の意思を無視して送りつけられる広告メールなどの総称です。SPAM（スパム）とも呼ばれます。

- や -

予約検索

ウイルス検索などを設定された周期で行うセキュリティ対策ツールの機能です。スパイウェアの検索やセキュリティ診断も行えます。

- ら -

リアルタイム検索

ファイルの読み込みや書き込みを常に監視し、ウイルスに感染している場合は適切な処理を行うセキュリティ対策ツールの機能です。

ルータ

異なるネットワークの間を接続するための機器です。家庭では、ADSLや光ファイバ接続(FTTH)の接続に使用するブロードバンドルータと呼ばれるルータを指すことがほとんどです。

ログ

セキュリティ対策ツールでは、過去に検出されたウイルスやアップデートの実行日時などを記録した履歴を指します。ログによって、セキュリティ対策ツールが過去にどのような処理を行ったかを確認できます。

索引

は

ま

や

ら