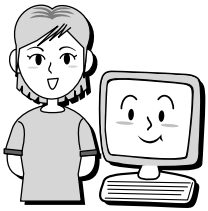
セキュリティ対策ツール

ガイドブック（フレッツ 光ネクスト/フレッツ 光ライト版　バージョン5対応）

NTT西日本

こんなときには、このマニュアル

使う前に



フレッツ 光ネクスト/
フレッツ 光ライト
超カンタン設定ガイド

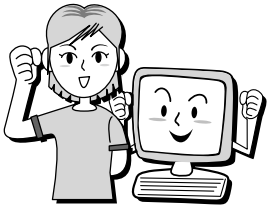
使い始めたら

ガイドブック

「自分に合った使いかたをしたい。
でも、面倒な設定はしたくない。」
という方にピッタリ。
使いかたに合わせた設定を簡単に
説明しています。

本書です

しっかり活用するなら



こまったときは

「とにかく、インストールして早く使い始めたい！」という方にピッタリ。これ1冊で、簡単にインストールできます。

※ フレッツ 光ネクスト/フレッツ 光ライト 超カンタン設定ガイドはフレッツ 光ネクスト、フレッツ 光ライト開通工事時に工事担当者よりお渡ししております。

ヘルプ

本ツールの画面右上には ? 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。

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

セキュリティ対策ツール　サポート情報

http://f-security.jp/

※ お電話でのお問い合わせについては、「フレッツサービスお申込み内容のご案内」に記載の電話番号へおかけください。

目次

はじめに

基本的な使いかた

こんなときは

1 セキュリティ対策ツールでできること

セキュリティ対策ツールは、ウイルスやスパイウェア、オンライン詐欺などのWebの脅威、不正アクセス、個人情報の流出など、様々な危険からパソコンとお客さまを保護する総合セキュリティツールです。

ウイルスから保護します

ウイルスが侵入しないよう常に監視するのはもちろんのこと、もしウイルスが侵入してしまっても適切に処理できます。また、自動アップデート機能により、日々進化するウイルスにいち早く対応します。

スパイウェアから保護します

個人情報を盗み出そうとしたり、迷惑な広告を表示したりするスパイウェアの活動を常に監視します。スパイウェアとの関連が疑われる不審な動作も見逃しません。

不正アクセスから保護します

パソコンとネットワークとのデータのやり取りを常に監視して、ネットワークを使った不正アクセスや攻撃からパソコンを保護します。

危険なWebサイトから保護します

金融機関やクレジットカード会社のWebサイトを装って、パスワードやクレジットカード番号をだまし取ろうとするオンライン詐欺への対策も行います。オンライン詐欺メールの判定、オンライン詐欺サイトの警告や表示防止など、二重三重の対策が講じられています。

迷惑メールを判定します

大量に届く迷惑メールの中から通常のメールを探し出すのは至難の業。送られてきたメールが迷惑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。

個人情報の流出を防止します

パスワードやクレジットカードの番号が、悪意のある第三者に知られてしまうと一大事。外部に流出してはならない個人情報をしっかりブロックできるので安心です。

お子さまがネットワークを安心して利用できる環境を実現

お子さまがネットワークを安全に利用するために、有害情報を扱うホームページの表示の規制や、ネットワークやパソコンの利用時間帯の設定を、Windowsユーザーアカウントごとに設定できます。

2 これからご利用になる方へ

セキュリティ対策ツールの準備がお済みでない方は、準備の流れやプログラムの動作環境などをご確認ください。

ご利用開始までの流れ

本ツールのインストールの基本的な流れは以下のとおりです。

1. 動作条件を確認する

はじめに動作条件を確認してください(9ページ)。

2. 本ツールをインストールする

超カンタン設定ガイドの手順に従って本ツールをインストールします。

3. ウイルスやスパイウェアを検索する

インストールが完了したら、アップデートを行い(20ページ)、ウイルスやスパイウェアの検索を行ってください(22ページ)。本ツールのインストール前に侵入していたウイルスやスパイウェアがある場合、この検索で発見、処理できます。

以上でインストールの手順は完了です！

! ご注意

フレッツ 光ライトでのセキュリティ対策ツールのご利用について

- 「フレッツ 光ライト」での「セキュリティ対策ツール」の利用量も通信料の対象です。パターンファイルの更新等320MBを超える利用量が必要となる場合があります。「セキュリティ対策ツール」の機能については、お客さまにて利用有無を設定することが可能です。

※ セキュリティ対策ツールの技術供与元であるトレンドマイクロ社が提供する機能（カテゴリ指定によるＵＲＬフィルタ機能、Web脅威対策機能（セキュリティツールバー機能を含む）、ソフトウェア安全性評価サービス機能及び迷惑メール対策ツールにおけるオンライン判定サービス機能とリンク判定機能等）を利用する際に必要となる通信や、公式ホームページなどセキュリティ対策ツールのリンクから外部サイトへ遷移する際の通信については、利用量を加算いたします。（本ツールの各機能についてはお客さまにて利用有無を設定することが可能です。）

セキュリティ対策ツールの動作環境

セキュリティ対策ツールを使用するうえでの動作環境（2013年11月現在）について説明します。

対応しているOS（オペレーティングシステム）やその動作環境は、変更されることがあります。NTT西日本の公式ホームページ（http://flets-w.com/）などで最新の情報を確認のうえ、使用してください。記載されていない環境で使用すると、セキュリティ対策ツールが正しく機能しない場合があります。あらかじめご了承ください。

対応OS

- Windows 8.1/Windows 8.1 Pro
- Windows 8/Windows 8 Pro
- Windows 7 Ultimate/Professional/Home Premium/Starter
  （Service Packなし、およびService Pack1に対応）
- Windows Vista Ultimate/Business/Home Premium/Home Basic
  （Service Pack 2に対応）
- Windows XP Professional/Home Edition
  （Service Pack 3に対応）

ご注意

- いずれのOSも日本語版のみの対応です。
- Windows 8.1、Windows 8、Windowis 7、およびWindows Vistaでは32ビット環境と64ビット環境の両方で動作します。
- Windows XP Professional x64 Editionには対応していません。
- Windows XP Media Center Edition / Tablet PC Editionには対応していません。
- Windows RTには対応していません。
- Windows 8.1/Windows 8 Enterprise、Windows 7 Enterprise、およびWindows Vista Enterpriseには対応していません。
- 記載されていないOS（Windows 95 / 98 / Me（Millennium Edition）/ NT、Mac OSなど）、エディションでは使用できません。

- Boot CampやエミュレータをWindows環境には正式対応しておりません。
- Service Pack(サービスパック)については上記のバージョンを適用してください。

CPU

- Windows 8.1の場合：800MHz以上(1GHz以上推奨)
- Windows 8の場合：800MHz以上(1GHz以上推奨)
- Windows 7の場合：800MHz以上(1GHz以上推奨)
- Windows Vistaの場合：800MHz以上(1GHz以上推奨)
- Windows XPの場合：450MHz以上(800MHz以上推奨)

メモリ

- Windows 8.1の場合：1GB以上
- Windows 8の場合：1GB以上
- Windows 7の場合：1GB以上
- Windows Vistaの場合：512MB以上(1GB以上推奨)
- Windows XPの場合：256MB以上(512MB以上推奨)

ハードディスク

- 950MB以上のハードディスクの空き容量

! ご注意

- カレントドライブに550MB以上の空き容量、インストールドライブに400MB以上の空き容量が必要です。
- RAID-0/RAID-1に対応しています。その他のRAIDレベルはサポートしていません。

ディスプレイ

- 解像度800×600以上、High Color(65,536色)以上

Webブラウザ

- Microsoft Internet Explorer 7.0/8.0/9.0/10.0/11.0

! ご注意

- Internet Explorer 10.0はWindows 8のデスクトップモードのみサポート対象となります。(2013年11月現在)
  最新の対応情報は、サポート情報サイト(http://f-security.jp/v6/support/faq/200201.html#soft)をご確認ください。
- Internet Explorer 11.0はWindows 8.1のデスクトップモードのみサポート対象となります。(2013年11月現在)
  最新の対応情報は、サポート情報サイト(http://f-security.jp/v6/support/faq/200201.html#soft)をご確認ください。

ご利用に関するご注意

- すでにほかのセキュリティ対策製品をお使いの場合は、これらの製品を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。
- 動作環境（システム要件）に記載されているOSの種類やハードディスク容量などは、OSのサポート終了、弊社製品の改良などの理由により、予告なく変更される場合があります。
- 必要メモリ容量およびハードディスク容量は、パソコンの環境によって異なる場合があります。また、実際のご利用に必要な容量は、ログファイルのサイズ、パターンファイルのサイズなど利用状況に応じて変化しますのでご注意ください。
- セキュリティ対策ツールをお使いになる前に、使用許諾契約書を必ずお読みください。
- セキュリティ対策ツールの仕様は予告なく変更される場合があります。
- セキュリティ対策ツールをインストールするとWindows Defender（Windowsのスパイウェア対策機能）が無効に設定されます。
- Web脅威対策機能および有害サイト規制機能では、Webサイトが安全かどうかの判定のために、お客さまがアクセスしたURLの情報を暗号化してトレンドマイクロ社のサーバに送信します。
- 「ソフトウェア安全性評価サービス」では、プログラムが安全かどうかの判定のために、プログラムの情報を暗号化して技術供与元であるトレンドマイクロ社のサーバに送信します。
- 本バージョンでは、パーソナルファイアウォール機能が省かれ、「ファイアウォールチューナー」という機能が追加されています。ファイアウォールチューナーは 、Windowsファイアウォールにはない IDS（侵入検知システム）機能と、ネットワークウイルスからの防御を提供している機能です。Windowsファイアウォールと併用することでより高いセキュリティを保つことができます。
- パターンファイルのアップデートや、サポート情報サイトをご利用になるには、パソコンをフレッツ 光ネクスト、またはフレッツ 光ライトに正しく接続する必要があります。カテゴリ指定によるURLフィルタ機能、Web脅威対策機能、ソフトウェア安全性評価サービス機能および迷惑メール対策ツールにおけるオンライン判定サービス機能とリンク判定機能、Microsoft Updateをご利用になるには、パソコンをインターネットに正しく接続する必要があります。
- Windowsのサービスパックに関しては、必ず9ページの対応オペレーティングシステムをご確認ください。

各機能に対応するWebブラウザおよびメールソフト

本ツールの各機能は、次のソフトウェアおよびサービスにおいて正しく動作することを確認しています。記載されていないソフトウェア、またはサービスをご利用の場合、各機能の動作はサポート対象外となります。

Web 脅威対策機能、有害サイト規制、個人情報の保護機能に対応するWebブラウザ

- Microsoft Internet Explorer 7.0、8.0、9.0、10.0、11.0
- Mozilla Firefox
- Google Chrome
  * Internet Explorer 10.0はWindows 8のデスクトップモードのみサポート対象となります。(2013年11月現在)
    最新の対応情報は、サポート情報サイト(http://f-security.jp/v6/support/faq/200201.html#soft)をご確認ください。
  * Internet Explorer 11.0はWindows 8.1のデスクトップモードのみサポート対象となります。(2013年11月現在)
    最新の対応情報は、サポート情報サイト(http://f-security.jp/v6/support/faq/200201.html#soft)をご確認ください。
  * Google Chromeは、ポート80番を利用する通信のみサポートされます。
  * Mozilla Firefox、Google Chromeの対応バージョン詳細は、サポート情報サイト(http://f-security.jp/v6/support/faq/200201.html#soft)をご確認ください。

迷惑メール対策ツールに対応するメールソフト

- Microsoft Outlook 2003、2007、2010
- Microsoft Outlook Express 6.0 Service Pack 3
- Microsoft Windows メール
- Windows Live メール 2009
  * Microsoft Outlook 2010 64ビット版には対応していません。
  * Windows Live メール 2009はPOP3のみ対応しています。
  * IMAPプロトコルをサポートしていません。

送受信メール検索に対応するメールソフト

- Microsoft Outlook 2003、2007、2010
- Microsoft Outlook Express 6.0 Service Pack 3
- Microsoft Windows メール
- Windows Live メール 2009
- Mozilla Thunderbird 3.0

個人情報の保護機能に対応するメールソフト

- Microsoft Outlook 2003、2007、2010
- Microsoft Outlook Express 6.0 Service Pack 3
- Microsoft Windows メール
- Mozilla Thunderbird 3.0

個人情報保護機能に対応するインスタントメッセンジャー

- ICQ 6.5、7.0
- MSN Messenger 7.5
- Windows Live Messenger 8.1、9.0、2009、2010
- Yahoo!メッセンジャー 8.1、9.0、10.0

セキュリティツールバー（Webサイト安全性評価）に対応するWebブラウザ

- Microsoft Internet Explorer 7.0、8.0、9.0、10.0、11.0
- Mozilla Firefox
  * Windows Vista、Windows 7のMicrosoft Internet Explorerの64ビット版には対応していません。
  * Internet Explorer 10.0はWindows 8のデスクトップモードのみサポート対象となります。（2013年11月現在）
    最新の対応情報は、サポート情報サイト（http://f-security.jp/v6/support/faq/200201.html#soft）をご確認ください。
  * Internet Explorer 11.0はWindows 8.1のデスクトップモードのみサポート対象となります。（2013年11月現在）
    最新の対応情報は、サポート情報サイト（http://f-security.jp/v6/support/faq/200201.html#soft）をご確認ください。
  * Mozilla Firefoxの対応バージョン詳細は、サポート情報サイト（http://f-security.jp/v6/support/faq/200201.html#soft）をご確認ください。
  * Google ChromeにおいてもWebサイト安全性評価結果が表示される場合があります。

Webサイト安全性評価に対応する各検索エンジン

- Google
- Bing
- Yahoo!
- Biglobe
- OCN
- Infoseek
- goo

SNS評価機能に対応するサービス

- facebook
- Twitter
- myspace
- mixi

WebメールのURL評価機能に対応するサービス

- Hotmail
- Yahoo!メール
- Gmail

ブラウザガードに対応するWebブラウザ

- Microsoft Internet Explorer 7.0、8.0、9.0、10.0、11.0
- Mozilla Firefox

* Internet Explorer 10.0はWindows 8のデスクトップモードのみサポート対象となります。(2013年11月現在)
最新の対応情報は、サポート情報サイト(http://f-security.jp/v6/support/faq/200201.html#soft)をご確認ください。

* Internet Explorer 11.0はWindows 8.1のデスクトップモードのみサポート対象となります。(2013年11月現在)
最新の対応情報は、サポート情報サイト(http://f-security.jp/v6/support/faq/200201.html#soft)をご確認ください。

* Mozilla Firefoxの対応バージョン詳細は、サポート情報サイト(http://f-security.jp/v6/support/faq/200201.html#soft)をご確認ください。

3 本ツールの起動とメイン画面の表示

本ツールは、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。

本ツールの起動

本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。

本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）に本ツールのアイコンが表示されます。

セキュリティ対策ツールのアイコン

ヒント

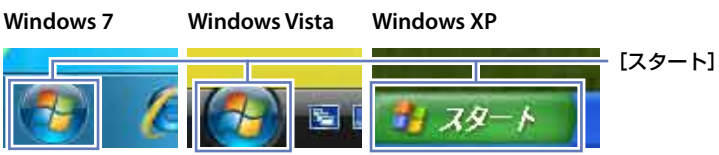
- Windows 8.1 / Windows 8の場合は、デスクトップモードで通知領域（タスク バー）の をクリックするとアイコンが表示されます。
- Windows 7の場合は、通知領域（タスクトレイ）左側の をクリックするとアイコンが表示されます。
- Windows Vista / Windows XPの場合は、通知領域（タスクトレイ）にアイコンが表示されます。表示されない場合は をクリックしてください。
- 手動で起動する場合は、以下の「メイン画面を表示する」と同じ手順を行ってください。
- 通知領域（タスクトレイ）のアイコンは、本ツールの動作状況によって表示が切り替わります。詳細については、「通知領域（タスクトレイ）のアイコン」（19ページ）をご覧ください。

メイン画面を表示する

セキュリティ対策ツールを起動する。

【Windows 7、Windows Vista、Windows XPの場合】

デスクトップ左下の[スタート]をクリック。



スタートメニューが表示されます。

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

メイン画面が表示されます。

【Windows 8.1、Windows 8の場合】

デスクトップモードの右下の通知領域(タスクトレイ)の をクリックすると表示される、セキュリティ対策ツールのアイコンをダブルクリック。

メイン画面が表示されます。

ヒント

メイン画面はWindows 7、Windows Vista、Windows XPにおいても、通知領域（タスクトレイ）にある本ツールのアイコンをダブルクリックして表示できます。

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（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、本ツールは終了せず、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

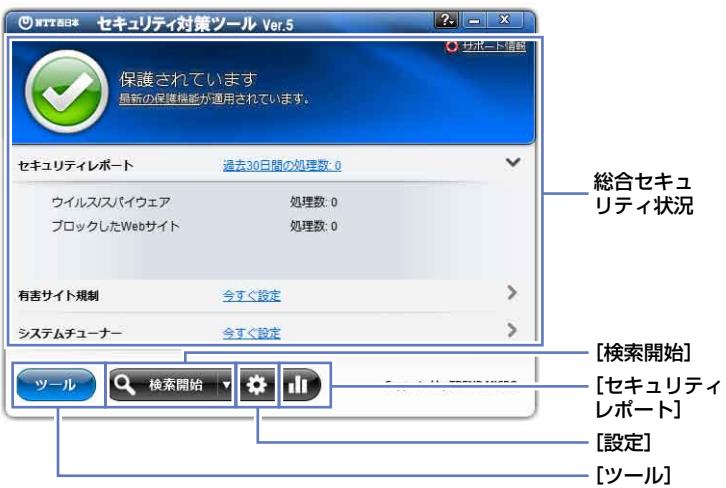
本ツールを終了するには？

本ツールの終了は、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、「本ツールを終了するには？」（59ページ）をご覧ください。

4 本ツールの画面構成

本ツールでは、操作や設定の変更をメイン画面で行います。ここでは、本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



総合セキュリティ状況	パソコンの保護の状況を確認できます。
検索開始	ウイルスやスパイウェアの検索を行います(22ページ)。
設定	本ツールの各種設定を行います。
セキュリティレポート	セキュリティレポートを表示します。
ツール	ツールを表示します。

ヒント

それぞれの画面については、画面右上の ? からヘルプを表示して確認してください。

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)に表示されている本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。本ツールが正常に動作しています。
	ウイルスなどの検索や本ツールのアップデートが行われています。このアイコンが表示されている間は、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。
	重要な保護機能が無効になっている状態です。設定内容をご確認ください。もしくは、ご契約が廃止または停止状態のため、シリアル番号が利用できません。契約状態について不明な場合は、0800-2002116までお問合せください。

ヒント

パソコンの状態によっては、本ツールのアイコンが隠れている場合があります。アイコンを表示するには、通知領域(タスクトレイ)横の矢印ボタンをクリックしてください。

5 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。本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

本ツールの初期設定は、アップデートを自動的に行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。

ご注意

アップデート機能をご利用になるパソコンを、フレッツ 光ネクストまたはフレッツ 光ライトに正しく接続する必要があります。

ヒント

一定期間、パソコンをネットワークに接続していないと、ポップアップやメイン画面にアップデートをうながすメッセージが表示されることがあります。メッセージに従ってアップデートを行ってください。

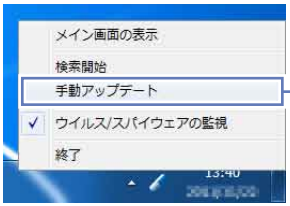
手動でアップデートする

ご注意

アップデートをする前に、以下のことを確認してください。

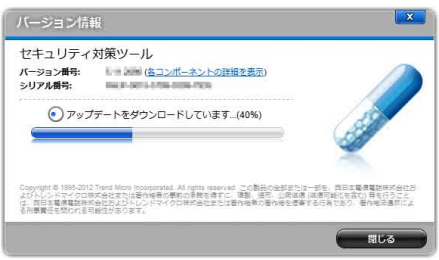
- **ネットワークに接続していますか？**
  アップデートを実行するためには、アップデートを実行するパソコンが、フレッツ 光ネクストまたはフレッツ 光ライトに正しく接続されている必要があります。通信機器の電源や接続をご確認ください。

1 通知領域(タスクトレイ)のセキュリティ対策ツールのアイコンをクリックし、[手動アップデート] をクリックします。



[手動アップデート]

2 アップデートが実行されます。



アップデートが完了したら、[閉じる]ボタンを押してください。

以上が手動アップデートの手順になります。

ヒント

メイン画面からの手動アップデートについて

セキュリティ対策ツールのメイン画面右上の ? ボタンから[バージョン情報]をクリックしても、手動アップデートが実行されます。

「再起動してください」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、画面の案内に従ってパソコンを再起動してください。

6 ウイルスやスパイウェアを検索する

インストールとアップデートが完了したら、ウイルスやスパイウェアの検索を行ってください。

こんなときには手動での検索が必要です

本ツールの初期設定は、リアルタイムでウイルスやスパイウェアの侵入を監視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、以下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。

- **本ツールをインストールした直後**
- **しばらくアップデート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(20ページ)。

1 メイン画面を表示して(16ページ)、[検索開始]をクリック。

[検索進捗]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など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」(24ページ)を参照し、処理結果を確認してください。

ヒント

手順1の[検索進捗]画面で[検索完了後にコンピュータを自動的にシャットダウン]のチェックボタンをオンにすると、検索完了後にPC を自動的にシャットダウンさせることができます。
その場合は次回パソコン起動時に結果画面が表示されます。

3 処理が完了したら[閉じる]をクリック。

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

［未解決の脅威］をクリックし、表示されている内容を確認します。

通常、未解決の脅威に対してはアクセス拒否が適用されるので、お使いのパソコンは感染から保護されます。

［解決済みの脅威］パネルおよび［削除されたCookie］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。

ヒント

処理済みの脅威の詳細を確認するには?

1 メイン画面（18ページ）の（セキュリティレポート）をクリック。
セキュリティレポートが表示されます。

2 画面右下の［詳細の表示］をクリック。
ログ画面が表示されます。

3 ログ項目をクリック。
画面右側に脅威の詳細が表示されます。

クッキーが削除されているのは？

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サイトの利便性の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検出され、ウイルス/スパイウェア検索を実行すると自動的に削除されます。

7 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うえ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

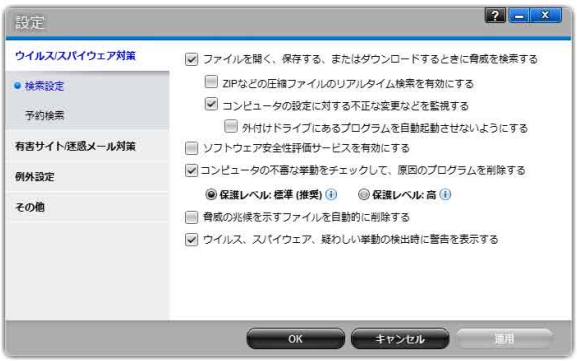
ウイルスやスパイウェアはパソコンの動作に悪影響を与えるソフトウェアです。これらのソフトウェアはネットワークやデータの受け渡しなどを通じてパソコンに侵入し、データを改ざんしたり、情報を流出させたりするといった活動を行います。

「ウイルス/スパイウェア対策」機能で対策

ウイルスやスパイウェア対策の設定は、メイン画面から[設定]ボタンをクリックして[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]画面では、ウイルス/スパイウェアの監視の有効/無効、また、監視の結果のポップアップの有無、予約検索などを設定できます。詳細はヘルプを参照してください。

【ウイルス/スパイウェア対策画面】



ヒント

画面右上の ? ボタンをクリックすると、オンラインヘルプが表示されます。詳細な設定方法は、ヘルプの[基本的な設定]内の[ウイルス/スパイウェア対策]の項目を参照してください。

8 不正アクセスを監視し、ネットワーク対策をするには？

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、Windowsファイアウォールを併用し、ファイアウォールチューナーを有効にすることで、より高いセキュリティを保つことができます。

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アクセスなどの外部からの攻撃に備えておく必要があります。

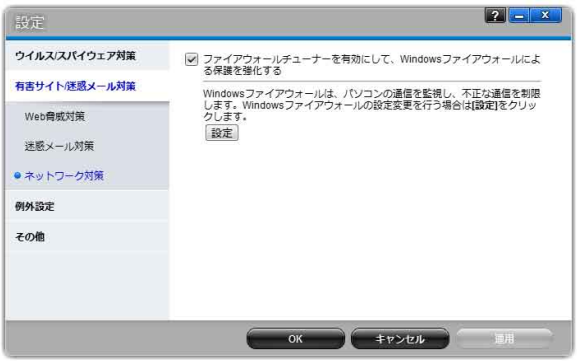
また、Webブラウザやメールソフトのような、ネットワークを利用するためのソフトウェアがネットワークに接続するのは当然ですが、最近はアップデートや情報更新などの目的でネットワークを活用するソフトウェアが増えています。

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。

「ネットワーク対策」機能で対策

ネットワーク対策の設定は、メイン画面から[設定]ボタンをクリックして[有害サイト/迷惑メール対策]画面の[ネットワーク対策]で行います。[ネットワーク対策]画面ではWindowsファイアウォールを強化するファイアウォールチューナーの有効/無効や、Windowsファイアウォールの設定ができます。詳細はヘルプを参照してください。

【ネットワーク対策画面】



ヒント

- ファイアウォールチューナーを有効にすることにより、攻撃パケットや、ネットワークウイルスなどの危険な通信をブロックします。
- 画面右上の ? ボタンをクリックすると、オンラインヘルプが表示されます。詳細な設定方法は、ヘルプの[基本的な設定]内の[ネットワーク対策]の項目を参照してください。

9 Webサイトやメールを用いた犯罪や有害情報による被害を防ぐには？

オンライン詐欺は、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、オンライン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。

また、お子さまがいるご家庭でも安心してパソコンをご利用いただけるように、有害な情報を遮断したり、パソコンやWebサイトの利用時間を制限することもできます。

オンライン詐欺の基礎知識

オンライン詐欺とは、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。

オンライン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。

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、オンライン詐欺のメールが特に問題になっています。

ヒント

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/迷惑メール対策」カテゴリの機能で対策

オンライン詐欺、迷惑/詐欺メール、有害サイトへ対策するための設定は、メイン画面から[設定]ボタンをクリックして[有害サイト/迷惑メール対策]画面で行います。

[有害サイト/迷惑メール対策]画面から、[Web脅威対策]、[迷惑メール対策]の設定ができます。詳細はヘルプを参照してください。

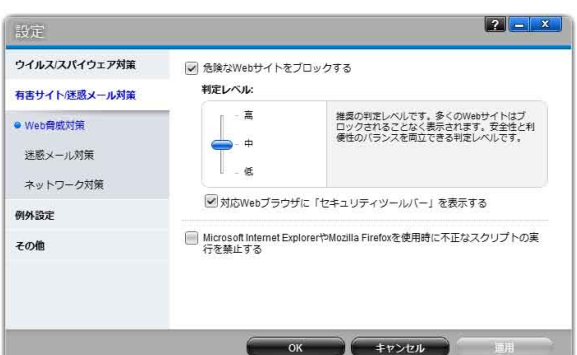
ヒント

画面右上の ? ボタンをクリックすると、オンラインヘルプが表示されます。詳細な設定方法は、ヘルプの[基本的な設定]内の[Web脅威対策]、[迷惑メール対策]の項目を参照してください。

Web脅威対策

オンライン詐欺で使われる偽装サイトなどの危険なWebサイトの表示を制限して、詐欺などの危険から守ります。

※ Web脅威対策機能は技術供与元であるトレンドマイクロ社が提供する機能となります。トレンドマイクロ社が定める使用許諾契約書(http://www.trendmicro.co.jp/products/security/nttwest/agreement.asp)に同意いただいたうえで本機能をご利用ください。



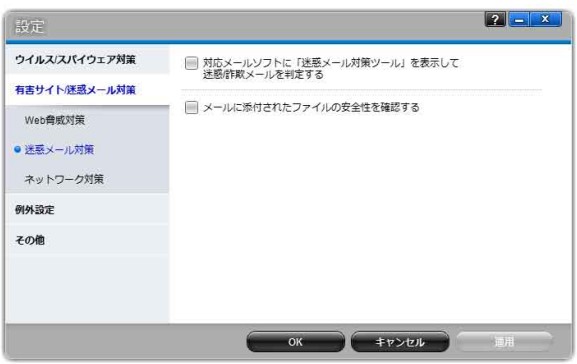
Web脅威対策の判定レベル

Web脅威対策の判定レベルは次の中から選択します。通常は、「中」(初期設定)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サイトへのアクセスはブロックされるため、オンライン詐欺やその他のWebサイト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	オンライン詐欺に関連するWeb サイトをブロックします。脅威の兆候を示すものもブロックの対象となりますが、多くのWebサイトはブロックされることなく表示されます。安全性と利便性のバランスを両立できる判定レベルです。
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サイトからの脅威に対して最低限必要な対策を行います。

迷惑メール対策

迷惑メール対策ツールに対応するメールソフト(12ページ)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。迷惑メール対策ツールは、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。



ご注意

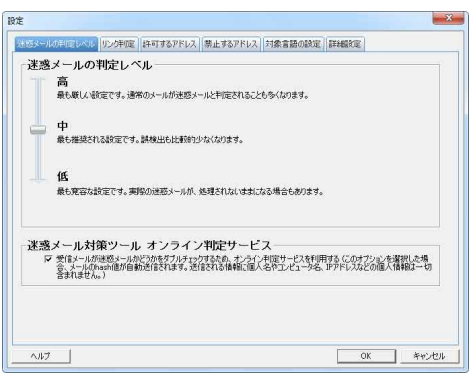
「迷惑/詐欺メールの判定」を有効にすると、本機能に対応するメールソフトを起動してから操作できるようになるまで、時間がかかる場合があります。

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。

迷惑メールの判定レベル

迷惑メールの判定レベルと、判定のために最新の情報をオンラインデータベースに問い合わせる機能（オンライン判定サービス）の設定が行えます。

※ 迷惑メール対策ツールにおけるオンライン判定サービス機能は技術供与元であるトレンドマイクロ社が提供する機能となります。トレンドマイクロ社が定める使用許諾契約書（http://www.trendmicro.co.jp/products/security/nttwest/agreement.asp）に同意いただいたうえで本機能をご利用ください。



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」（初期設定）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。

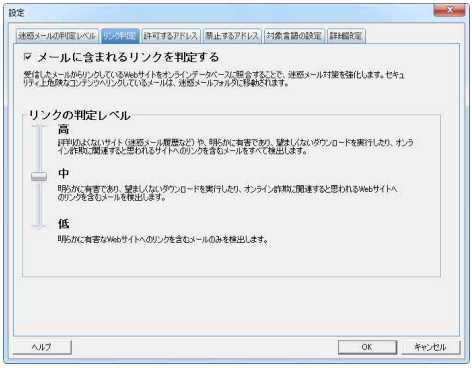
ご注意

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。

リンク判定

受信したメールからリンクしているWebサイトをオンラインデータベースに照合することで、迷惑/詐欺メール対策を強化します。セキュリティ上危険なコンテンツへリンクしているメールは、迷惑メールフォルダに移動されます。

※ 迷惑メール対策ツールにおけるリンク判定機能は技術供与元であるトレンドマイクロ社が提供する機能となります。トレンドマイクロ社が定める使用許諾契約書（http://www.trendmicro.co.jp/products/security/nttwest/agreement.asp）に同意いただいたうえで本機能をご利用ください。

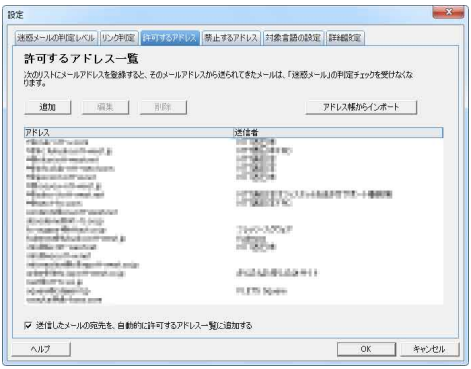


リンクの判定レベルは次の中から選択します。通常は、「中」（初期設定）に設定してください。

高	有害なWebサイト、オンライン詐欺の疑いのあるWebサイト、評判の低いWebサイトへのリンクが含まれているメールをすべて検出します。
中	有害なWebサイト、オンライン詐欺の疑いのあるWebサイトへのリンクが含まれているメールを検出します。
低	有害なWebサイトへのリンクが含まれているメールのみを検出します。

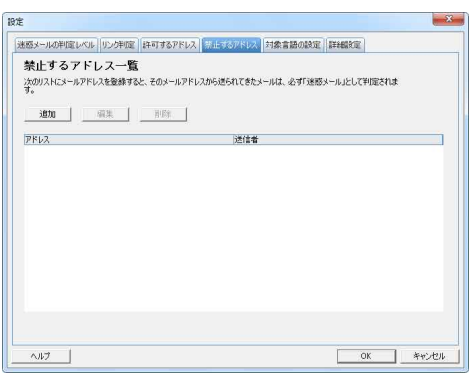
許可するアドレス

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。



「有害サイト規制」で対策

特定のカテゴリのWebサイトを開けないようにしたり、Webサイトの閲覧を特定の間帯のみに制限する設定は、[有害サイト規制]機能で行います。

有害サイト規制の設定は、メイン画面の[ツール]ボタンをクリックして[有害サイト規制]ボタンから行います。詳細はヘルプを参照してください。

ヒント

画面右上の ? ボタンをクリックすると、オンラインヘルプが表示されます。詳細な設定方法は、ヘルプの[ツール]内の[有害サイト規制]の項目を参照してください。

URLフィルタ

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ができます。

※ 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社が提供する機能となります。トレンドマイクロ社が定める使用許諾契約書（http://www.trendmicro.co.jp/products/security/nttwest/agreement.asp）に同意いただいたうえで本機能をご利用ください。

Webサイト使用時間

お子さまなど、Webアクセスする時間を制限させたい対象ユーザに対し、Webサイトを閲覧できる時間を設定することができます。また、1 日のパソコン の使用時間に上限を設定することが可能です。

ご注意

- 制限された時間帯では、Webサイトへアクセスできないだけでなく、Webブラウザ以外のソフトウェアが行う通信も遮断される場合があります。
- 有害サイト規制でユーザごとに異なる設定を行うためには、あらかじめWindowsユーザーアカウントの設定が必要です。詳しくはWindowsのヘルプをご覧ください。

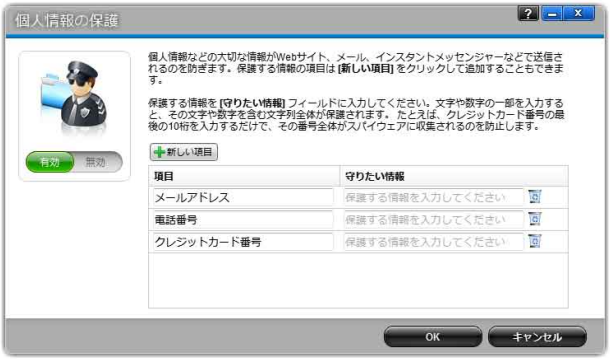
「個人情報の保護」で対策

個人情報が外部に送信されないよう保護する設定は、[個人情報の保護]機能で行います。

個人情報の保護の設定は、メイン画面の[ツール]ボタンをクリックして[個人情報の保護]ボタンから行います。詳細はヘルプを参照してください。

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。



ヒント

画面右上の ? ボタンをクリックすると、オンラインヘルプが表示されます。詳細な設定方法は、ヘルプの[ツール]内の[個人情報の保護]の項目を参照してください。

10 こんな機能もあります

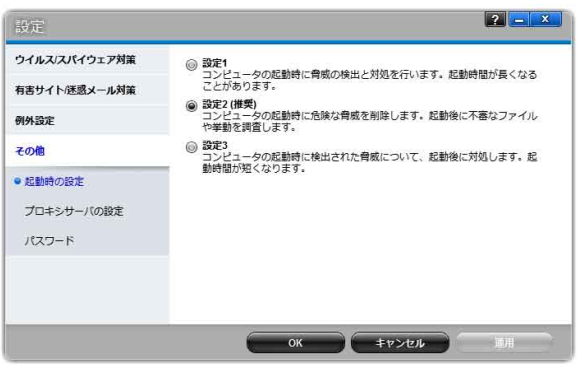
本ツールには、ここまでに紹介してきた機能のほかにも便利な機能があります。

その他の設定はこの画面で！

起動時の設定、プロキシサーバの設定、パスワードの設定は、メイン画面から[設定]をクリックし、[その他]画面で行います。

詳細はヘルプを参照してください。

【その他画面】



ヒント

- 画面右上の ? ボタンをクリックすると、オンラインヘルプが表示されます。詳細な設定方法は、ヘルプの[基本的な設定]内の[起動時の設定]、[プロキシサーバの設定]、[パスワード]の項目を参照してください。
- 起動時の設定では、コンピュータの起動時に、本ツールがドライバやサービスを読み込むタイミングを設定します。変更された設定は、コンピュータの再起動後に有効になります。
- パスワードを設定することによって、ほかの人に設定内容を変更されたり、セキュリティ対策ツールをアンインストールされたりしないようにすることができます。また、次の機能をご利用いただくには、パスワードの設定が必要です。
  * 有害サイト規制(35ページ)
  * 個人情報の保護機能(37ページ)

ご注意

- パスワードを忘れると本ツールの再インストールが必要になります。パスワードのヒントを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では、プロキシサーバの設定がなされている場合、最新版へのアップデートが実行できない場合があります。

11 複数のパソコンにインストールするには？

セキュリティ機能ライセンス・プラス（有料）を申し込んで、シリアル番号を追加してからインストールを進める手順をご案内します。

セキュリティ機能ライセンス・プラスを申し込んでインストールする

ご注意

- セキュリティ申込・設定ツールからセキュリティ機能ライセンス・プラスをお申し込みになる場合、1つのシリアル番号を追加するたびに基本工事費・交換機等工事費が発生します。複数のシリアル番号を同時に追加されたいお客さまは、お客さま窓口0800-2002116へお申し込みください。
- 「フレッツ 光ライト」での「セキュリティ対策ツール」の利用量も通信料の対象です。パターンファイルの更新等320MBを超える利用量が必要となる場合があります。「セキュリティ対策ツール」の機能については、お客さまにて利用有無を設定することが可能です。

※ セキュリティ対策ツールの技術供与元であるトレンドマイクロ社が提供する機能（カテゴリ指定によるURLフィルタ機能、Web脅威対策機能（セキュリティツールバー機能を含む）、ソフトウェア安全性評価サービス機能及び迷惑メール対策ツールにおけるオンライン判定サービス機能とリンク判定機能等）を利用する際に必要となる通信や、公式ホームページなどセキュリティ対策ツールのリンクから外部サイトへ遷移する際の通信については、利用量を加算いたします。（本ツールの各機能についてはお客さまにて利用有無を設定することが可能です。）

1 開通時にお渡ししているCD-ROM（フレッツ簡単セットアップツール）を、追加するシリアル番号を利用するパソコンのディスクドライブに挿入する。

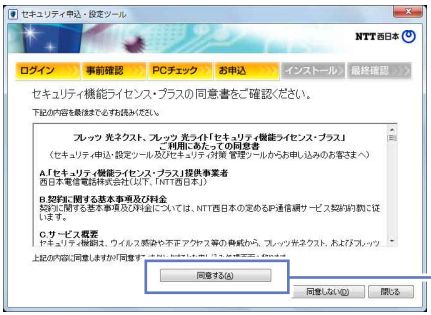
2 画面の案内に従いセキュリティ対策ツールのインストールを開始する。

詳しくは「フレッツ 光ネクスト/フレッツ 光ライト超カンタン設定ガイド」をご覧ください。

3 [追加]をクリックする。

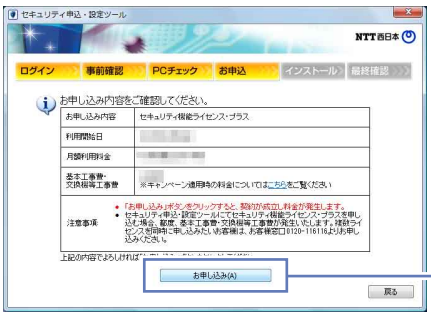
[追加]

4 同意書の内容を確認し、同意できる場合は[同意する]をクリックする。



[同意する]

5 お申し込み内容を確認し、[お申し込み]をクリックする。



[お申し込み]

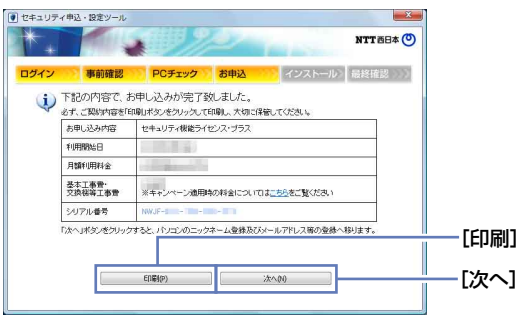
ご注意

画面は2012年10月現在のものです。実際の料金などはお申し込み時に表示される内容をご確認ください。

ヒント

お申し込みの処理を行うため、しばらくお待ちいただく場合があります。

6 お申し込みの結果を確認し、内容を[印刷]してから[次へ]をクリックする。



ご注意

- 画面は2012年10月現在のものです。実際の料金などはお申し込み時に表示される内容をご確認ください。
- プリンタを接続していない場合、[印刷]機能はご利用いただけません。

7 画面の案内に従いセキュリティ対策ツールのインストールを進める。

詳しくは「フレッツ 光ネクスト/フレッツ 光ライト超カンタン設定ガイド」をご覧ください。

12 登録したニックネームやメールアドレスを変更する

インストール時にご登録いただいたメールアドレスが変わった場合は、すみやかに変更手続きを行ってください。

メールアドレスやニックネームを変更する

ご登録いただいているメールアドレスには、セキュリティに関するお知らせをお届けします。重要なお知らせもありますので、ご利用になるメールアドレスが変わった場合は、以下の手順で新しいメールアドレスを登録してください。

ニックネームは、インストール後にお客さまがわかりやすいものに変更することができます。

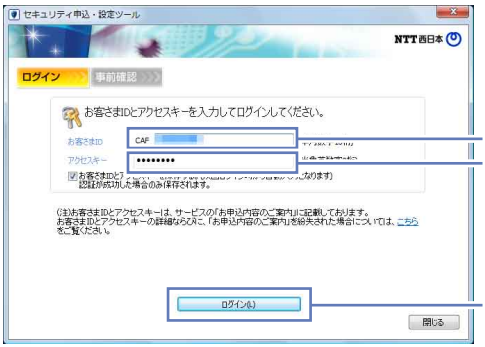
1 セキュリティ申込・設定ツールを起動する。

デスクトップにある[セキュリティ申込・設定ツール]のショートカットをダブルクリックしてください。

ヒント

- Windows 8.1、Windows 8をご利用の場合は、デスクトップモードの[セキュリティ申込・設定ツール]のショートカットより起動してください。もしくは、[すべてのアプリ]を表示し、[セキュリティ申込・設定ツール]のタイルをタップまたはクリックして起動しても起動できます。
- Windows 7、Windows Vista、Windows XPをご利用の場合は、「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]→[セキュリティ申込・設定ツール]の順にクリックしても起動できます。

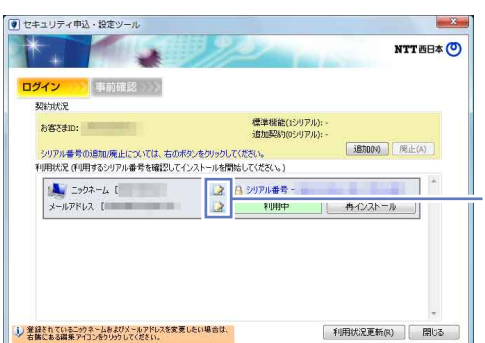
2 「お客さまID」と「アクセスキー」を入力して［ログイン］をクリック。



3 「契約状況」画面で変更したい項目の編集アイコンをクリック。

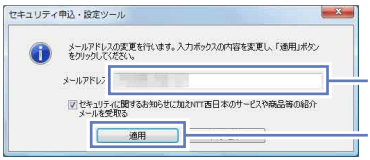
ご契約いただいているシリアル番号の一覧が表示されます。「利用中」と表示されているものが、現在ご利用いただいているシリアル番号です。

シリアル番号1つに対して1つのニックネームと1つのメールアドレスを登録することができます。変更したい項目の右にある編集アイコンをクリックしてください。



4 登録されている情報を書き換えて[適用]をクリック。

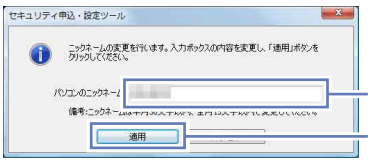
メールアドレスを変更する場合



[メールアドレス]

[適用]

ニックネームを変更する場合



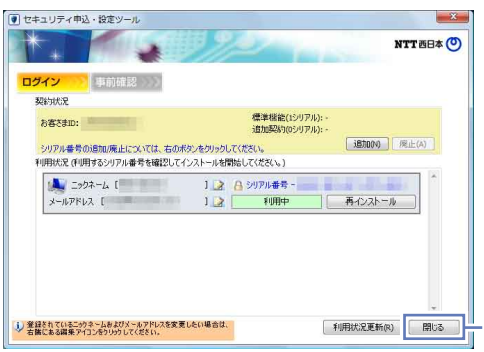
[パソコンのニックネーム]

[適用]

ヒント

- メールアドレスは半角で入力してください。
- ニックネームには半角文字と全角文字の両方が入力できます。
- 複数の項目を変更する場合は、手順3と4を繰り返してください。

5 [閉じる]をクリック。



[閉じる]

「契約状況」画面が閉じます。

13 メッセージが表示されたときは？

本製品は、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

メッセージのアイコンについて

メッセージのアイコンは以下の3種類あり、危険性の高さを表しています。


危険性が高いとき


注意を要するとき


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

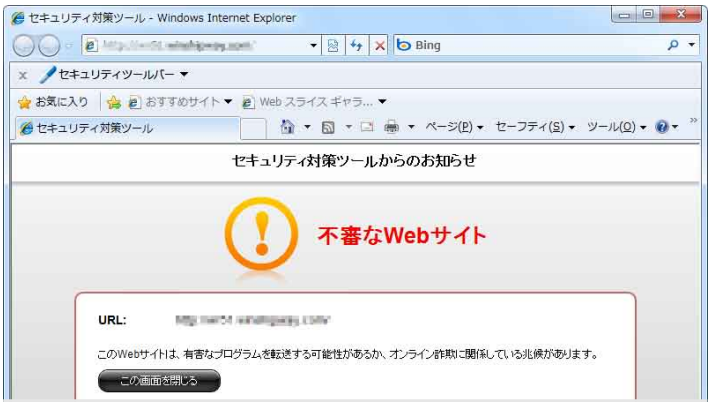
セキュリティレポート

1か月の間に、コンピュータでどのような脅威が見つかったか、また処理を行ったかという履歴などを表示します。

メイン画面(18ページ)の  (セキュリティレポート)をクリックすると表示されます。また、[セキュリティレポート]画面左下の[このレポートを毎月表示]チェックボックスをオンにすると、毎月表示されます。

その他のメッセージ

有害サイトや偽装サイトの可能性があるページを表示しようとしたときは、Webサイトが以下のような内容に置き換えて表示されます。



ウイルスやスパイウェアに関するメッセージ

疑わしいファイルを削除しました

ウイルスなどの脅威が含まれるファイルが自動的に削除された場合に表示されます。処理は不要ですのでご安心ください。
[詳細の表示]をクリックすると、見つかった脅威の情報を確認できます。

コンピュータを再起動して脅威の削除を完了する

トロイの木馬や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]をクリックしてください。

疑わしい動作や不審な変更に関するメッセージ

プログラムを停止しました

コンピュータの設定に対して、不審な変更が見つかり、自動的にブロックされた場合に表示されます。
処理は不要ですのでご安心ください。
[詳細の表示]をクリックすると、見つかった変更の情報を確認できます。

その他のメッセージ

「守りたい情報」の送信を中断しました

保護されている個人情報の送信が自動的にブロックされた場合に表示されます。
ブロックされたデータを確認してください。

保護機能が無効です

推奨される保護機能が無効にされた場合に表示されます。
特別な理由がない限り、推奨される保護機能は有効にすることをおすすめします。

保護機能が最新ではありません

一定期間以上アップデートが実行されなかった場合に表示されます。
ご契約の回線に正しく接続していることを確認し、[確認]ボタンを押してアップデートをしてください。

14 ネットワーク接続で困ったときは？

本ツールのインストール後、ネットワークに接続できなくなった場合は、以下の点を確認してください。

ネットワークに接続できなくなった

本ツールの設定によってはネットワークに接続できなくなることがあります。以下の点をご確認ください。

1. 不正変更の監視の設定を確認する

特定のソフトウェアでネットワークに接続できない場合は「不正変更の監視の設定を確認する」(51ページ)の手順に従って、設定を確認してください。

2. Web脅威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「Web脅威対策の設定を確認する」(51ページ)の手順に従って、設定を確認してください。

3. 有害サイト規制の設定を確認する

特定のWebサイトが表示できない場合は「有害サイト規制の設定を確認する」(52ページ)の手順に従って、設定を確認してください。

4. 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」(22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。

5. 以上を確認しても接続できない場合は……

本ツール以外の原因によるものと推測されます。NTT西日本のIPカスタマサポートへご相談ください。

不正変更の監視の設定を確認する

不正変更の監視機能が、ソフトウェアの正常な設定変更をブロックしていることにより、ネットワークへの接続ができなくなる場合があります。

以下の手順でいったん不正変更の監視を無効にして、ネットワークに接続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(16ページ)。
2. (設定)をクリック。
3. 画面左側の[ウイルス/スパイウェア対策]をクリック。
   [検索設定]画面が表示されます。
4. [コンピュータの設定に対する不正な変更などを監視する]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。[コンピュータの設定に対する不正な変更などを監視する]チェックボックスをオンに戻してください。

不正変更の監視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、[ウイルス/スパイウェア対策]画面右上の 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。

Web脅威対策の設定を確認する

Web脅威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。

以下の手順でいったんWeb脅威対策を無効にして、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(16ページ)。
2. (設定)をクリック。
3. 画面左側の[有害サイト/迷惑メール対策]をクリック。
   [Web脅威対策]画面が表示されます。

4 [危険なWebサイトをブロックする]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。[危険なWebサイトをブロックする]のチェックボックスをオンに戻してください。

Web脅威対策を無効にしてWebサイトが表示されるようになった場合は、[Web脅威対策]画面右上の ? 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。

有害サイト規制の設定を確認する

有害サイト規制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。

以下の手順でいったん有害サイト規制を無効にして、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(16ページ)。

2 画面左下の[ツール]をクリックし、[有害サイト規制]をクリック。
[有害サイト規制]画面が表示されます。

3 [OK]をクリック。
パスワードを要求される場合は、有害サイト規制初回設定時に設定したパスワードを入力してください。

4 [無効]をクリック。

5 [OK]をクリック。

この状態で、Webサイトやソフトウェアが利用できない場合は、別の原因が考えられます。手順4で[有効]をクリックし、有害サイト規制を有効に戻してください。

有害サイト規制を無効にしてWebサイトが表示されるようになった場合は、[有害サイト規制]画面の ? 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。

ネットワークを利用するソフトウェアが使えない

「ネットワークに接続できなくなった」(50ページ)の手順に従って原因を確認してください。この手順で原因を特定できない場合は、ソフトウェアの販売元にお問い合わせいただくことをおすすめいたします。

メールが送受信できなくなった

「ネットワークに接続できなくなった」(50ページ)の手順に従って原因を確認してください。この手順で原因を特定できない場合は、本ツール以外の原因によるものと推測されます。NTT西日本のIPカスタマサポートへご相談ください。

15 パソコンやOSを変更するときについて知りたい

インストール前に不明な点や困ったことがあった場合は以下の内容をご覧ください。

パソコンを買い換えたときに必要なことは？

新しいパソコンに、以前のパソコンで使用していたシリアル番号を選択して本ツールをインストールしてください。新たなシリアル番号は必要ありません。

ヒント

インストール手順については、「フレッツ 光ネクスト/フレッツ 光ライト超カンタン設定ガイド」をご覧ください。

パソコンを買い増したときに必要なことは？

1つのシリアル番号で、複数のパソコン、複数のOSに本ツールをインストールすることはできません。

買い増したパソコンにインストールする際に、セキュリティ申込・設定ツールから「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。

詳しくは、40ページをご覧ください。

Windowsの再インストールやリカバリのときに必要なことは？

再インストールやリカバリの完了後に、本ツールのインストールを行ってください。

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？

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してください。

本ツールの動作環境について最新の情報は、NTT西日本の公式ホームページ(http://flets-w.com/)をご覧ください。

2 ＜対応していない場合＞

対応するまで新しいWindowsやサービスパック(SP)のご利用はお控えください。

＜対応している場合＞

ホームページで案内する手順に従い、新しいWindowsやサービスパック(SP)に対応する準備をしてください。セキュリティ対策ツールのアンインストールが必要な場合があります。

3 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。

ご注意

セキュリティ対策ツールをインストールしたまま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。事前に対応情報をご確認ください。

ヒント

現在使用しているセキュリティ対策ツールのバージョンがわからない場合は、メイン画面上部のタイトル部分をご覧ください。

16 インストールやバージョンアップについて知りたい

インストールやバージョンアップに関する疑問や困ったことについては以下の内容をご覧ください。

バージョンアップするには？

セキュリティ申込・設定ツールを起動すると、自動的にセキュリティ対策ツールの最新バージョンがないか確認を行います。

最新バージョンがあった場合は、画面の案内に従ってバージョンアップを進めてください。なお、現在お使いのバージョンを手動でアンインストールする必要はありません。

ヒント

セキュリティ申込・設定ツールは次のいずれかの方法で起動できます。

- デスクトップにある［セキュリティ申込・設定ツール］のショートカットをダブルクリックする。Windows 8.1、Windows 8の場合は、デスクトップモードにてご利用ください。
- Windows 7、Windows Vista、Windows XPをご利用の場合、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］→［セキュリティ申込・設定ツール］の順にクリックする。

インストールのときにメッセージが表示された

「他のセキュリティソフトが入っています」と表示された場合

アンインストールしない場合、本ツールが正常に動作しないおそれがあります。画面の案内に従って、指定のソフトウェアをアンインストールしてください。

シリアル番号を無くしてしまったときは？

セキュリティ対策ツールのシリアル番号は、お申し込み時にNTT 西日本から送付した＜フレッツサービスお申し込み内容のご案内＞に記載されています。

＜フレッツサービスお申し込み内容のご案内＞を紛失された場合は、「0800-2002116」にお問い合わせください。

自動でバージョンアップされる？

自動ではバージョンアップされません。バージョンアップのための操作が必要になります。

ヒント

関連するお問い合わせ

バージョンアップするには？（56ページ）

バージョンアップした場合に何が引き継がれる？

旧バージョンのセキュリティ対策ツールから本バージョン（Ver.5）のセキュリティ対策ツールにバージョンアップした場合の設定などの引き継ぎについては、次のようになります。

- Ver.2、Ver.3からバージョンアップする場合は、シリアル番号と、プロキシサーバの設定が引き継がれます。
- 旧バージョンのセキュリティ対策ツールの使用中に作成されたログ（履歴）情報を、本バージョンのセキュリティ対策ツールで確認することはできません。

本ツールのアンインストール方法について

アンインストールは以下の手順で行ってください。

ご注意

アンインストールを行うときは、本ツールのメイン画面を閉じてください。

1 Windows 7、Windows Vista、Windows XPをご利用の場合は、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。

Windows 8.1、Windows 8をご利用の場合は、［アプリ］画面の［Windows システム ツール］の［コントロール パネル］をクリックし、［プログラムのアンインストール］を選択し［セキュリティ対策ツール］をダブルクリック。

［セキュリティ対策ツール インストーラ］画面が表示されます。

2 画面の案内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。

ヒント

本ツールに設定したパスワードを忘れてしまったときは？

あらかじめ設定したヒントを参照しても思い出せない場合は、セキュリティ対策ツールサポート情報（84ページ）をご覧ください。

17 その他のことについて知りたい

ほかのトピックで解決しなかった疑問や困ったことについてはこちらをご覧ください。72ページの「よくあるお問い合わせ早見表」とあわせてご覧ください。

操作や設定についてのよくあるお問い合わせは、ヘルプにも記載されています。

本ツールを終了するには？

本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、本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、デスクトップ右下の通知領域（タスクトレイ）にある本ツールのアイコン 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

- パソコンの状態によっては、本ツールのアイコンが隠れている場合があります。アイコンを表示するには、通知領域（タスクトレイ）横の矢印ボタンをクリックしてください。
- 本ツールの終了後、再び起動したい場合は、「メイン画面を表示する」（16ページ）の手順を行ってください。

ウイルス/スパイウェアの監視を一時的に停止するには？

デスクトップ右下の通知領域（タスクトレイ）にある本ツールのアイコン を右クリックし、［ウイルス/スパイウェアの監視］をクリックしてチェックをはずしてください。

再開するには同じ操作を繰り返して、チェックを付けてください。安全のため、ウイルス/スパイウェアの監視は、30分後自動的に有効になります。

ヒント

パソコンの状態によっては、本ツールのアイコンが隠れている場合があります。アイコンを表示するには、通知領域（タスクトレイ）横の矢印ボタンをクリックしてください。

セキュリティ対策ツールのアイコンに「！」マークがついたのはなぜ？

セキュリティ対策ツールは動作していますが、以下のいずれかの問題があります。

- アップデートが1回も行われていない。
- アップデートが一定期間行われていない。
- 推奨機能が無効になっている。

デスクトップ右下の通知領域（タスクトレイ）にある本ツールのアイコン をダブルクリックしてメイン画面を開き、［総合セキュリティ状況］画面の上部に表示されるメッセージに従って対処してください。

ヒント

パソコンの状態によっては、本ツールのアイコンが隠れている場合があります。アイコンを表示するには、通知領域（タスクトレイ）横の矢印ボタンをクリックしてください。

アップデートが失敗してしまう場合は？

最新版へのアップデートの途中でエラーが発生する場合、さまざまな原因が考えられます。表示されるエラーメッセージの内容をご確認ください。主な原因と対処方法は以下のとおりです。

アップデートが始まらない（登録状態についてのエラーが表示される）

- シリアル番号が解約などの理由で無効になっていないか確認してください。
- 複数のパソコンに同じシリアル番号を選択してセキュリティ対策ツールをインストールした場合は、最後にインストールしたパソコンでしかアップデート機能は利用できません。

アップデートが始まらない（ネットワーク関連のエラーが表示される）

- パソコンとネットワーク機器との接続をご確認ください。
- Windowsのネットワーク設定が適切かご確認ください。
- プロキシサーバを利用する設定に変更した場合は、アップデートの設定からこれを解除してみてください。

それでも通信できない場合は、サーバメンテナンス中の可能性があります。NTT西日本の公式ホームページから工事情報（http://www.ntt-west.co.jp/info/construction/）をご確認いただくか、IPカスタマサポートへご相談ください。

アップデートの途中でエラーが発生した

パソコンを再起動したあとに再度アップデートを実行してください。

それでも問題が解決しない場合は、セキュリティ対策ツール　サポート情報(84ページ)をご覧ください。

メモリが不足していると表示された

パソコンを再起動したあとに再度アップデートを実行してください。

ディスクの空き容量が不足していると表示された

Windowsのごみ箱を空にするなどして、空き容量を増やしてください。少なくとも数十MBの空き容量が必要です。

さらにセキュリティを向上させるためにはどのような設定を行えばよいですか？

Web脅威対策機能とソフトウェア安全性評価サービスを有効にすると、より迅速に最新の脅威に対応できるようになります。

個人情報の漏えいが心配な場合は、個人情報の保護機能を利用するとともに、ファイアウォールチューナーをご利用ください。

ただし、これらの機能を有効にすると、パソコンの動作速度やポップアップメッセージの表示頻度に影響を及ぼす可能性があります。

検索するといつもcookieというスパイウェアが見つかる

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、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。クッキーの利用目的が不明な場合は、サイト管理者にお問合せください。

「_restore」フォルダからウイルスが見つかる場合は？

Windows 7、Windows Vista、Windows 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。

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。

ウイルス検索が突然始まる場合は？

自動的に実行されるウイルス検索は、「予約検索」と呼ばれる機能です。初期設定では、予約検索が設定されています。この設定を変更するには、次の手順に従ってください。手順については、ヘルプにも記載されています。

1. メイン画面を表示する（16ページ）。
2. [設定]画面の[ウイルス/スパイウェア対策]をクリック。
3. [予約検索]をクリック。
   [予約検索]設定画面が表示されます。
4. ドロップボックスで予約検索を実行したい曜日や時間に変更できます。予約検索が不要な場合は、[コンピュータの予約検索を実行する]のチェックボックスをオフにすることもできます。
5. [OK]をクリック。

設定内容が保存され、画面が閉じます。

バックグラウンドで実行されている処理の状況を表示するには？

ウイルス/スパイウェア検索やアップデートがバックグラウンドで実行されている場合は、デスクトップ右下の通知領域（タスクトレイ）にある本ツールのアイコン をダブルクリックすると、状況を表示することができます。

ヒント

パソコンの状態によっては、本ツールのアイコンが隠れている場合があります。アイコンを表示するには、通知領域（タスクトレイ）横の矢印ボタンをクリックしてください。

シリアル番号を画面で確認したい

本ツールのシリアル番号は［バージョン情報］画面で確認できます。

1 メイン画面右上の ? ボタンをクリック。

2 ［バージョン情報］をクリック。
［バージョン情報］画面が表示されます。

通常メールが迷惑メールとして処理される場合は？

迷惑メール判定のレベル(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

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]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]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、トレンドマイクロ社に送信され、画面が閉じます。

ご注意

「迷惑メール対策ツール」では、本ツールの改良の目的および迷惑メールの判定精度の向上のため、技術供与元であるトレンドマイクロ社のサーバに該当メールを送信します。また、迷惑メールの削減、迷惑メールによる被害の抑制を目指している政府関係機関に対して迷惑メール本体を開示する場合があります。

暗号化されたメールのメール検索は？

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あとにウイルスに対する処理が行われます。

通知領域（タスクトレイ）にアイコンが見あたらない

セキュリティ対策ツールが終了している可能性があります。本ツールを起動してください（16ページ）。起動が完了すれば、  が通知領域（タスクトレイ）に表示されます。

ヒント

パソコンの状態によっては、本ツールのアイコンが隠れている場合があります。アイコンを表示するには、通知領域（タスクトレイ）横の矢印ボタンをクリックしてください。

通知領域（タスクトレイ）に表示されるアイコンの形状については、19ページをご覧ください。

初期設定で無効になっている機能があるが問題ない？

NTT西日本が推奨する機能はあらかじめ有効に設定されています。無効になっている機能は、機能を確認し、必要がある場合にお使いください。

インストールしたらパソコンの動作が遅くなった

ウイルスの侵入を未然に防止するには、プログラムやファイルの動きを常に監視する必要があり、そのためにはパソコンに若干の負荷がかかります。このため、ウイルス対策を行っていない環境と比較した場合、多少の動作速度の差が発生します。

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。

バージョン情報を調べたい場合は？

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バージョン情報画面から確認できます。

メイン画面右上の ? ボタンをクリックして[バージョン情報]をクリックすると、セキュリティ対策ツールのバージョン番号が確認できます。各パターンファイルや検索エンジンのバージョンなどを確認したい場合は、[各コンポーネントの詳細を表示]をクリックしてください。

パスワードを忘れてしまった場合は？

あらかじめお客さまにて設定された、本ツールの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。

パスワードを忘れてしまったときは、お客さまが設定したヒントを確認してください。それでも思い出せない場合は、サポートツールを使って旧バージョンをアンインストール後、新しいバージョンの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ので、詳しくはセキュリティ対策ツール　サポート情報(84ページ)をご覧ください。

有害サイト規制機能やWeb脅威対策機能で、サーバに送信される情報とは何ですか？

「Webレピュテーションサービス」「Web脅威対策」「URLフィルタ」では、Webサイトの安全性の判定のために、お客様がアクセスしたURLの情報等(ドメイン、IPアドレス等を含む)を暗号化して技術供与元であるトレンドマイクロ社のサーバに送信します。

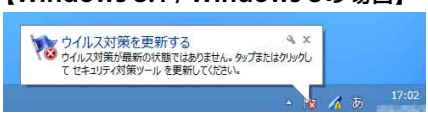
サーバに送信されたURL情報は、Webサイトの安全性の確認、および本機能の改良の目的にのみ利用されます。

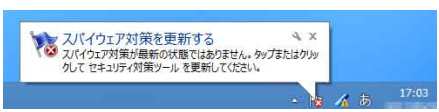
また、これらの機能を有効にしたうえで、コモンゲートウェイインタフェースアプリケーションを使用しているサーバで構築されているWebサイトにアクセスし、ID、パスワード等を入力した場合には、お客様がアクセスしたWebページのURLにお客様が入力したID、パスワード等が含まれた状態でトレンドマイクロ社のサーバに送信される場合があります。この場合、トレンドマイクロ社では、お客様がアクセスするWebページの安全性の確認のため、これらのお客様より受領した情報にもとづき、お客様がアクセスするWebページのセキュリティチェックを実施します。

「ウイルス対策を更新する／スパイウェア対策を更新する」(Windows 8.1 / Windows 8の場合)、「セキュリティ対策ツールを更新する」(Windows 7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)、「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)というポップアップメッセージが表示される場合は？

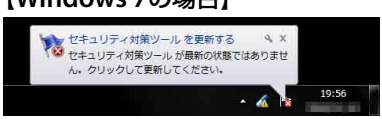
Windows セキュリティセンター、またはWindows アクションセンター(Windows 8.1 / Windows 8、Windows 7の場合)により、ご利用のパソコンのウィルス対策ソフトの状態が表示されます。

【Windows 8.1 / Windows 8の場合】

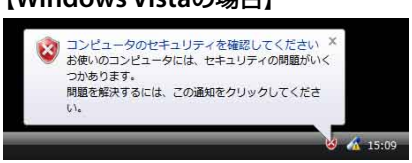




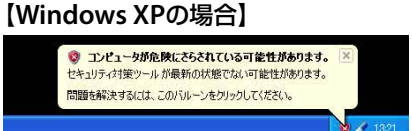
【Windows 7の場合】



【Windows Vistaの場合】



【Windows XPの場合】



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。

ケース1：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、またはWindows アクションセンター（Windows 8.1 / Windows 8、Windows 7の場合）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。

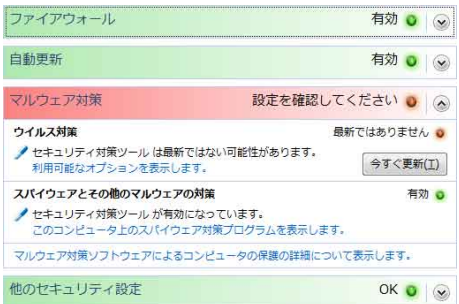
ケース2：セキュリティ対策ツールに適用されているパターンファイルのバージョンが一定期間更新されていない。

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一定期間以上更新されていない場合、Windows セキュリティセンター、またはWindows アクションセンター（Windows 8.1 / Windows 8、Windows 7の場合）が警告を表示します。また、Windows セキュリティセンター、Windows アクションセンターの状態が次のように表示されます。

【Windows アクションセンターの場合】（Windows 8.1 / Windows 8）

【Windows アクションセンターの場合】（Windows 7）

【Windows セキュリティセンターの場合】



警告が表示された場合、ネットワークに正しく接続しているかを確認して、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。

個人情報の外部送信が正しくブロックされない場合は？

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。

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、「各機能に対応するWebブラウザおよびメールソフト」（12ページ）を参照してください。

ウイルスなどの検出履歴を見るには？

メイン画面から  （セキュリティレポート）ボタンをクリックすると各種ログを確認できます。

18 よくあるお問い合わせ早見表

本書で解説しているよくあるお問い合わせの一覧です。

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ファイルの記載が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。

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。

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。

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。

OS(オーエス)

オペレーティングシステム(76ページ)と同義。

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 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機能です。

- あ -

アクセスポイント

無線LANの通信を中継する機器です。

アップデート

NTT西日本のサーバから最新のパターンファイルや検索プログラムなどをダウンロードし、お使いのツールを最新の状態に更新することです。本ツールのパターンファイルや、検索プログラムなどをアップデートすることで、新種のウイルスやスパイウェアに対応できます。

インスタントメッセンジャー

ネットワークを利用して、複数の相手とリアルタイムにコミュニケーションがとれるソフトウェアです。メッセージをやり取りしたり、音声通話機能で会話できるほか、ファイルを送受信することもできます。

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、パソコンがフレッツ 光ネクストまたは、フレッツ 光ライトを契約している回線に、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。本書では、特に記載のない限り、トロイの木馬を含めてウイルスと表記しています。

オペレーティングシステム

パソコンを動かすための基本的なソフトウェアです。パソコンの起動時には、パソコンで使用しているオペレーティングシステムの名前が、最初に画面表示されます。

オンライン詐欺

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。

- か -

カスタム検索

本ツールの検索機能の1つです。任意の場所を指定して検索することが可能です。

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。

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

オンライン詐欺目的で、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、追加台数分のあら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 -

通知領域（タスクトレイ）

Windowsのデスクトップ右下にある、時計などが表示されている部分のことです。パソコンを起動すると、本ツールのアイコン  が通知領域（タスクトレイ）に表示されます。また、パソコンの状態によっては、本ツールのアイコンが隠れている場合があります。アイコンを表示するには、通知領域（タスクトレイ）横の矢印ボタンをクリックしてください。

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。

ファーミング詐欺

DNSサーバやhostsファイルを改変することで、ユーザが入力した正しいホスト名(ドメイン名)を、まったく別のIPアドレスに変換させて偽装サイトに誘い込む詐欺です。

多くの場合、偽装サイトは本物そっくりに作られているため、気がつかないうちにパスワードやクレジットカード番号などの個人情報をだまし取られる危険性があります。

不正アクセス

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。不正侵入とも呼びます。

不正変更の監視

本ツールの機能の1つです。スパイウェアの中には、パソコンの設定に不正な変更を加えたり、ほかのプログラムを介してネットワークに接続したりするものがあります。不正なものと思われる変更が見つかった場合にポップアップメッセージで警告されるため、スパイウェアによる被害を未然に防ぐことができます。

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。

ポート番号

ネットワーク上の通信で、通信相手のアプリケーションを特定するための番号です。パソコンの各アプリケーションは、あらかじめ定められたポート番号を使用して、データをやり取りします。

- ま -

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。

迷惑メール対策ツール

本ツールの機能の1つで、Microsoft Outlook、Microsoft Outlook Expressおよび Microsoft Windows メール専用のアドインツールとして提供されています。迷惑/詐欺メールを判定し、自動的に「迷惑メールフォルダ」に移動します。

- や -

有害サイト規制

本ツールの機能の1つで、有害な情報を含むおそれのあるWebサイトにアクセスしないようにします。

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。

- 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

ま

や

ら

輸出規制について

お客様は、本ツールおよびそれらにおいて使用されている技術(以下「本ツール等」という)が、外国為替および外国貿易管理法、輸出貿易管理令、外国為替管理令および省令、ならびに、米国輸出管理法令に基づく輸出規制の対象となること、ならびにその他の国における輸出規制対象品目に該当している可能性があることを認識の上、本ツール等を適正な政府の許可なくして、禁輸国もしくは貿易制裁国の企業、居住者、国民、または、取引禁止者、取引禁止企業に対して、輸出もしくは再輸出しないものとします。

お客様は、2011年8月現在、米国により定められる禁輸国が、キューバ、イラン、北朝鮮、スーダン、シリアであること、禁輸国に関する情報が、以下のウェブサイトにおいて検索可能であること、ならびに本ツール等に関連した米国輸出管理法令の違法行為に対して責任があることを認識の上、違法行為が行われないよう、適切な手段を講じるものとします。

http://www.treas.gov/offices/enforcement/ofac/

http://www.bis.doc.gov/complianceandenforcement/ListsToCheck.htm

本ツールの利用により、お客様が米国により現時点で禁止されている国の居住者もしくは国民ではないこと、および本ツール等を受け取ることが禁止されていないことを認識し、お客様は、本ツール等を、大量破壊を目的とした、核兵器、化学兵器、生物兵器、ミサイルの開発、設計、製造、生産を行うために使用しないことに同意するものとします。

免責事項

・本書の記載内容は予告なく変更することがあります。

・本書における記述は、情報を提供する目的で書かれたもので、保証もしくは推奨するものではありません。

・本書に掲載している画像には開発中のものが含まれるため、実際に表示されるものとは異なる場合があります。

・セキュリティ対策ツールは、全てのコンピュータウイルスの検出及び駆除、スパイウェアの検出及び削除、オンライン詐欺の防止、第三者によるアクセスの防止、HPの閲覧制限、個人情報送信の防止、迷惑/詐欺メールの検出、Windows OS及びMicrosoft Office製品の脆弱性診断、不正接続パソコンの検出及び接続制限等を保証するものではなく、セキュリティ対策ツールを提供することに伴い発生する損害については、NTT西日本はその責任を負いません。

困ったときには

オンラインヘルプで問題解決

本ツールの画面右上には ? 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。

セキュリティ対策ツール　サポートページで問題解決

サポートページ

http://f-security.jp/

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　サポート情報

http://f-security.jp/

※ お電話でのお問い合わせについては、「フレッツサービスお申込み内容のご案内」に記載の電話番号へおかけください。