TREND MICRO

ウイルスバスター2003

リアルセキュリティ

www.trendmicro.co.jp

TREND MICRO

ガイドブック

Guide Book

TREND MICRO
ウイルスバスター2003 リアルセキュリティ

ガイドブック

目　次

このガイドブックの見方

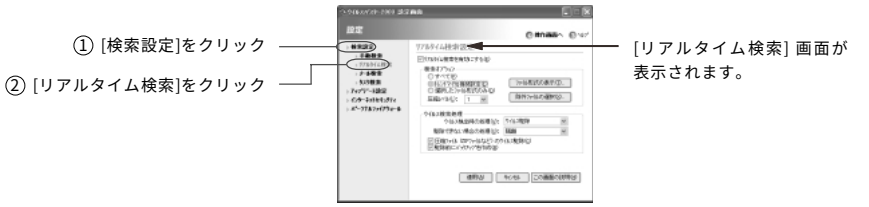
このガイドブックでは、手順などの説明に次のような表現を使います。

■　メニューを選択する

たとえば ...

> *「設定メニューから [検索設定]→[リアルタイム検索] を選択して、[リアルタイム検索設定] 画面を表示します。」*

このような指示があったら、「設定画面」の左側に表示されている**「検索設定」**を最初にクリックします。次に、表示される項目から**「リアルタイム検索」**をクリックします。



■　機能の有効 / 無効を切り替える

ウイルスバスター 2003 では、クリック 1 つでさまざまな機能を有効にしたり、無効にすることができます。

本書では、機能の有効 / 無効を切り替える場合に、「[○○] チェックボックスをオン (またはオフ) にします。」といった説明をします。チェックボックスの**オン**と**オフ**とはそれぞれ次の状態を指します。

チェックボックスオン：☑　　**チェックボックスオフ：**☐

■　アイコンについて

また、このガイドブックにはいくつかの「アイコン」が出てきます。それぞれのアイコンには、次のような意味があります。

このアイコンが出てきたら、ウイルスバスターの操作や設定の手順について説明します。

注意

このアイコンが出てきたら、ウイルスバスターの操作や機能について、注意していただきたいことを説明しています。注意事項をよく読んで、ウイルスバスターを正しくお使いください。

動作環境

対応OS	Microsoft Windows 98 Microsoft Windows 98 Second Edition Microsoft Windows Millennium Edition Microsoft Windows NT Workstation 4.0 Service Pack 6a以上 Microsoft Windows 2000 Professional Service Pack 2以上 Microsoft Windows XP Home Edition Microsoft Windows XP Professional ※ 本製品は、日本語環境でのみ動作いたします。
ハードウェア環境	次のマイクロプロセッサ (または互換プロセッサ) を搭載したPC/AT互換機 ※マルチプロセッサには対応しません。 ※NEC PC-9800/9821シリーズには対応しません。 Microsoft Windows 98/98 SE/Me/NT Workstationをお使いの場合： Pentium 166MHz以上 Microsoft Windows 2000/XPをお使いの場合： Pentium 300MHz以上
ソフトウェア環境	Microsoft Internet Explorer 4.01 Service Pack 2以上
メモリ	Microsoft Windows 98/98 SE/Me/NT Workstationをお使いの場合： 32MB以上　(64MB以上を推奨) Microsoft Windows 2000 Professionalをお使いの場合： 64MB以上　(128MB以上を推奨) Microsoft Windows XPをお使いの場合： 128MB以上
ハードディスク	25MB以上のハードディスク空き容量 ※ RAID環境には対応しません。
ディスプレイ	解像度 800×600以上、High Color (65536色) 以上をサポート

注意　必要なメモリ容量、ハードディスク容量はシステム環境によって異なる場合があります。対応 OS およびその動作環境は変更される場合があります。最新の情報については Readme をお読みください。

インターネット接続を必要とする機能のご使用にあたって

※ ウイルスバスター2003のオンラインユーザ登録、ファイルのダウンロード、ウイルス情報およびその他のWebページの閲覧、e-mailの送信などの機能をご利用になるにはインターネット接続環境が必要です。
※ インターネットへの接続には、インターネットプロバイダへの加入および接続形態に応じた接続機器 (モデム、ターミナルアダプタなど) が必要です。
※ インターネットに接続した場合の通信費はお客さまの負担となります。
※ インターネット接続にダイヤルアップルータを使用している場合、設定によってはインテリジェントアップデート実行時などに自動的にダイヤルアップされ、課金が発生してしまう場合があります。自動的にダイヤルアップされないようにするには、ルータの設定を変更する必要がありますのでご注意ください。

第 1 章 ウイルスバスターをはじめよう

ウイルスバスター 2003 をお使いいただき、誠にありがとうございます。

ウイルスバスター 2003 は、お使いのコンピュータを、コンピュータウイルスや不正アクセスから守るためのセキュリティソフトウェアです。

ウイルスバスター 2003 のウイルス検索機能では、リアルタイムでウイルスの侵入を監視します。また、近年増加している e-mail を使ったウイルス攻撃や、コンピュータに侵入する不正プログラムをリアルタイムでブロックすることができます。

また、パーソナルファイアウォール機能では、許可したくないアクセスや、外部から仕掛けられる攻撃から、お使いのコンピュータを守ります。

第 1 章では、次の項目について解説します。

ウイルスバスター 2003 の機能紹介

ウイルスバスター 2003 では、従来からのウイルス対策機能、パーソナルファイアウォール機能、インターネットセキュリティ対策機能を強化しました。また、新しい機能も追加されています。

ウイルス対策

ウイルスバスター 2003 のインストールが完了すると、ただちにリアルタイム検索が有効になり、ウイルスの監視を開始します。リアルタイム検索では、お使いのコンピュータ上で、ファイルを開く、保存するなどの操作をする際に、ウイルス検索を実行します。

従来のリアルタイム検索、手動検索、タスク検索、POP3 メール検索に加えて、ウイルスバスター 2003 では、Web メールに対するウイルス検索も可能になりました。

参照「リアルタイム検索」→ 46 ページ

参照「手動検索」→ 54 ページ

参照「POP3 メール /Web メール検索」→ 63 ページ

参照「タスク検索」→ 69 ページ

柔軟な設定が可能になったパーソナルファイアウォール

Power Up!

パーソナルファイアウォール機能では、お使いのコンピュータを外部からの不正アクセスから守ります。パーソナルファイアウォール機能は、ADSL やケーブル接続など、インターネットの常時接続が日常化している今、外部からの悪質な操作や攻撃的なアクセスの防止に欠かせない機能といえます。

ウイルスバスター 2003 のパーソナルファイアウォールでは、セキュリティレベルを高 / 中 / 低の 3 段階で調整することができます。

セキュリティレベルで設定されたファイアウォール機能に、除外ルールを設定して、信頼できる接続だけを許可したり、特定のサービス（ホームページの閲覧、メールの送受信など）だけを許可するなど、柔軟な設定が可能になりました。

また、無線 LAN による公共のインターネット接続サービスを利用する場合に、ウイルスバスター 2003 では、ボタン 1 つで無線 LAN 環境に適したセキュリティ設定に切り替えることができます。

参照「パーソナルファイアウォール」→ 107 ページ
参照「無線 LAN 環境でのセキュリティ」→ 114 ページ
参照「付録：はじめてのパーソナルファイアウォール」→ 125 ページ

インターネットセキュリティ

ウイルスバスター 2003 では、インターネットを安全に利用していただくための機能として、WebTrap (ウェブトラップ) 機能と URL フィルタ機能を用意しました。WebTrap 機能では、インターネット経由で不正なプログラムがお使いのコンピュータに侵入するのを防ぎます。また、URL フィルタ機能では、指定した Web サイトへアクセスしないように設定することができます。

参照「WebTrap 機能について」→ 100 ページ
参照「URL フィルタ機能について」→ 102 ページ

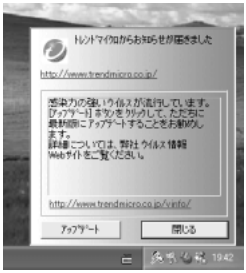
インテリジェントアップデート

Power Up!

ウイルスバスター 2003 を最新の状態でお使いいただくためには、アップデートが欠かせません。インテリジェントアップデート機能を使えば、ウイルスバスター 2003 がアップデートの必要があるかどうかを自動的に確認して、必要であれば通知します。また、アップデートが必要な場合に、確認画面を表示せずにアップデートを自動的に実行することもできます。

参照「インテリジェントアップデート」→ 93 ページ

ウイルス緊急警告機能 NEW!



大規模感染が心配される危険度の高いウイルスの情報や、誤って開くと危険な e-mail の件名など、ウイルスに関する警告情報を、インターネット経由でお知らせします。インターネットから受信した警告情報は、デスクトップ上でポップアップで表示されます。

参照「ウイルス緊急警告」→ 44 ページ

ウイルス処理アシスタント NEW!

ウイルスバスター 2003 がウイルスを検出して、感染ファイルを安全なフォルダに移動した場合に、その移動された感染ファイルをどのように処理したらよいかを案内してくれる、ヘルプ画面を用意しました。

参照「ウイルスを駆除できない場合どうすればいいの？」→ 81 ページ

緊急ロック機能

ウイルスバスター 2003 の緊急ロック機能では、コンピュータに被害を与える不正プログラムを誤って実行してしまったり、ウイルスが見つかった時に、他のコンピュータへ被害を広めないよう、インターネットを含むネットワーク接続を一時的に切断することができます。

緊急ロックでネットワークから切断したら、あとは落ち着いてウイルスバスター 2003 でウイルスを処理するだけです。他のコンピュータに被害を拡大してしまうような事態も、未然に防ぐことができます。

> 注意 緊急ロック機能は、パーソナルファイアウォールをインストールしている場合にのみ利用できる機能です。

参照「緊急ロック機能」→ 43 ページ

トロイの木馬自動修復機能

ウイルスバスター 2003 には、トロイの木馬自動修復機能が内蔵されています。コンピュータを起動するたびに、このトロイの木馬自動修復機能が作動し、パソコン内に「トロイの木馬」を見つけると、すぐに駆除します。駆除処理が実行されると、トロイの木馬が書き換えたファイルが修復されて、さらにトロイの木馬が作成したファイルも自動的に削除されます。

従来のウイルス対策ソフトウェアでは、システムファイルに感染したウイルスを駆除したり、システム内に入り込んでしまった「トロイの木馬」などの不正プログラムを駆除することができませんでした。

ウイルスバスター 2003 のトロイの木馬自動修復機能では、ウイルスバスターに含まれる「トロイの木馬情報」を元にファイルを検索して、駆除します。「トロイの木馬情報」は、ウイルスバスターのアップデートと一緒に、最新の情報が自動的にウイルスバスター 2003 に組み込まれます。

ウイルスバスター 2003 の CD-ROM について

ウイルスバスター 2003 のパッケージ (箱) を店頭などでお買い求めいただいた場合、ウイルスバスター 2003 のプログラムなどが収録された CD-ROM が付属しています。

このウイルスバスター 2003 の CD-ROM を、お使いのコンピュータの CD-ROM ドライブに挿入すると、次の画面が表示されます。

ウイルスバスター 2003 の CD-ROM を挿入すると自動的に表示される画面

この画面から、ウイルスバスター 2003 のインストール実行や CD-ROM に収録されている駆除ツールを利用することができます。

■ インストール

ウイルスバスター 2003 のインストールプログラムが起動します。インストール手順については、13 ページを参照してください。

■ マニュアルを見る

ウイルスバスター 2003 の CD-ROM には、ウイルスバスター 2003 付属のガイドブック (本書) が PDF 形式で収録されています。[マニュアルを見る] をクリックすると、PDF 形式のガイドブックが表示されます。

注意 PDF 形式のガイドブックを表示するには、Acrobat Reader がインストールされている必要があります。

■ ツールボックス

ウイルスによっては、感染した際にお使いのコンピュータの情報が改変されてしまう場合があります。コンピュータの情報が改変された場合、特別なツールを使用して、改変された情報を元に戻すことができます。ウイルスバスター 2003 の CD-ROM には、このような専用のツールがいくつか収録されています。

[ツールボックス] をクリックすると、駆除ツールが格納されている CD-ROM 上のフォルダが開きます。フォルダ内の「INDEX.HTM」ファイルをダブルクリックしてください。Web ブラウザが起動して、CD-ROM に収録されている駆除ツールが一覧で表示されます。

注意 この時点ではインターネット接続は必要ありません。駆除ツールによっては、インターネット接続が必要になる場合がありますので、表示される画面で確認してください。

使用する駆除ツールのリンクをクリックすると、そのツールの使用方法などが表示されます。

■ ウイルスバスター for PDA

ウイルスバスター 2003 の CD-ROM には、次の PDA 機器用のウイルスバスタープログラムが収録されています。

- Palm OS 用：ウイルスバスター for Palm OS
- Pocket PC 用：ウイルスバスター for Pocket PC
- EPOC 用：PC-cillin for EPOC

[ウイルスバスター for PDA] をクリックすると、PDA 用のウイルスバスタープログラムが収録されているフォルダが開きます。

PDA 用のウイルスバスターの動作環境、使用方法については、フォルダ内の Readme などを参照してください。

> 注意 ウイルスバスター for PDA は、サポート対象外です。ウイルスバスター クラブセンターでは、ウイルスバスター for PDA に関するお問い合わせなどは受け付けておりませんので、あらかじめご了承ください。

■ 閉じる

この画面を閉じます。

この画面が自動的に表示されない場合は ...

お使いのコンピュータにウイルスバスター 2003 の CD-ROM を挿入しても、画面が表示されない場合は、お使いのコンピュータの [マイ コンピュータ] から、挿入した CD-ROM 内の「Autorun (または、Autorun.exe)」をダブルクリックしてください。画面が表示されます。

ウイルスバスター 2003 のインストール

インストールする前に

ウイルスバスター 2003 をインストールして、正常に動作させるためには、お使いのコンピュータ上で Windows が正常に動作している必要があります。ウイルスに感染するなどして、Windows が正常に動作していない場合には、ウイルスバスター 2003 のインストールを開始する前に、OS の修復インストールまたは再インストールが必要です。

動作環境の確認

ウイルスバスター 2003 のインストールを始める前に、5 ページの「動作環境」を参照して、インストールするコンピュータの動作環境を確認してください。

旧バージョンまたは他社製品のアンインストール

ウイルスバスター 2003 をインストールするには、旧バージョンのウイルスバスター（または他社のウイルス対策製品）をアンインストール（削除）する必要があります。

他社のウイルス対策製品のアンインストール方法については、各製品に付属しているマニュアルなどを参照していただくか、製造元にお問い合わせください。

手順：旧バージョンのウイルスバスターをアンインストールする

注意 Windows NT/2000/XP の場合、アンインストール時に管理者権限が必要です。

1. 使用中のプログラムを終了します。
2. お使いの OS にあわせて、次のいずれかの手順を実行して下さい。

   Windows XP の場合：

   a) Windows の [スタート] メニューから [コントロールパネル] を選択します。

   b) [プログラムの追加と削除] をダブルクリックします。[プログラムの追加と削除] 画面が表示されます。

   Windows 98/Me/NT/2000 の場合：

   a) Windows の [スタート] メニューから [設定]→[コントロールパネル] の順に選択します。

   b) [アプリケーションの追加と削除] をダブルクリックします。 [アプリケーションの追加と削除] 画面が表示されます。

3. 現在インストールされているプログラムの一覧から、インストールされているウイルスバスターのバージョンを選択し、[追加と削除] または [削除] ボタンをクリックします。
4. 「インストールを続行するには次のアプリケーションを閉じる必要があります」というメッセージが表示されたら、表示されたアプリケーションを終了して [再試行] ボタンをクリックするか、[無視] をクリックして、アンインストールを続行します。
5. アンインストールが完了したら、コンピュータを再起動します。

注意 旧バージョンのウイルスバスターをアンインストールして、再起動を促すメッセージが表示されたら、お使いのコンピュータを必ず再起動してください。再起動しないと、ウイルスバスター 2003 を正常にインストールできなくなる可能性があります。

アンインストールがうまくいかない場合は、旧バージョンをインストールし直し（インストール先は同じフォルダを選択）、再度アンインストールを実行してください。

旧バージョンのシリアル番号について

ウイルスバスタークラブ会員契約期間中であれば、ウイルスバスター 2002 でお使いいただいた同じシリアル番号で、ウイルスバスター 2003 をインストールすることができます。

ウイルスバスター 2003 をインストールする

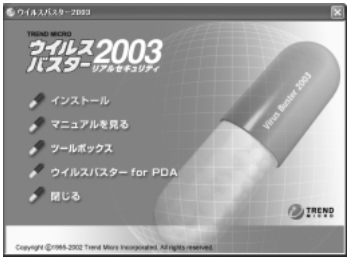
次の手順に従って、ウイルスバスター 2003 をインストールしましょう。インストールが完了したら、19 ページのインストール後の注意事項をよくお読みください。

手順：ウイルスバスター 2003 をインストールする

1. インストールプログラムを起動する

メールソフトなどのアプリケーションやプログラムを実行している場合は、すべて終了してください。

ウイルスバスター 2003 の CD-ROM を CD-ROM ドライブに挿入します。表示された画面から [インストール] を選択します。



CD-ROM を挿入すると表示される画面

図のような画面が自動的に表示されない場合は、[マイ コンピュータ] から、挿入した CD-ROM の**SETUP**フォルダにある「SETUP」（または、「SETUP.EXE」）プログラムを探し、ダブルクリックしてプログラムを起動してください。

注意 Microsoft Windows NT/2000/XP の場合、インストール時に管理者権限が必要です。

2. セットアップを開始する

ウイルスバスター 2003 のセットアップが開始され、[ウイルスバスター2003 InstallShield ウィザードへようこそ] 画面が表示されます。

[次へ] ボタンをクリックしてください。

セットアップ開始画面

次のページにつづく

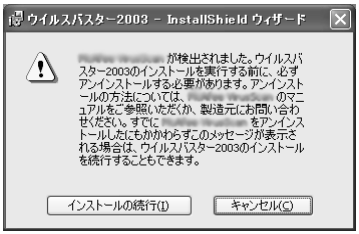
旧バージョンのウイルスバスターまたは他社のウイルス対策製品が見つかると ...

セットアッププログラムは、旧バージョンのウイルスバスター（および他社のウイルス対策製品）がないか検索します。

旧バージョンのウイルスバスターが見つかると、アンインストールを促す画面が表示されます。[アンインストール] ボタンをクリックすると、旧バージョンのウイルスバスターがアンインストールされます。旧バージョンのアンインストールが終了したら、必ずコンピュータを再起動してから、手順 1 に戻って、ウイルスバスター 2003 のインストールを開始してください。

旧バージョンのウイルスバスターが見つかった場合

他社のウイルス対策製品が見つかると、他社のウイルス対策製品のアンインストールを促すメッセージが表示されます。他社のウイルス対策製品をアンインストールするには、[キャンセル] ボタンをクリックして、ウイルスバスター 2003 のインストールを中断します。



他社のウイルス対策製品が見つかった場合

他社のウイルス対策ソフトウェアをすでにアンインストールしているにもかかわらず、他社の製品が検出されたことを知らせるメッセージが表示される場合、[インストールの続行] ボタンをクリックして、ウイルスバスター 2003 のインストールを続行することができます。

注意 他社のウイルス対策ソフトウェアがインストールされたまま、ウイルスバスター 2003 をインストールすると、システムが不安定になるなど、不具合の原因になります。他社のウイルス対策ソフトウェアが確実にアンインストールされていることを確認して下さい。

3. 使用許諾契約を確認する

使用許諾契約に同意しインストールを続ける場合は [使用許諾契約の条項に同意します] を選択して [次へ] ボタンをクリックしてください。

同意いただけない場合は、[キャンセル] ボタンをクリックし、ウイルスバスター 2003 のインストールを終了します。

使用許諾契約をよくお読みください

4. ウイルス検索

システムのウイルス検索が開始されます。

ウイルスが検出された場合は、18 ページの「インストール時にウイルスが見つかったら ...」を参照してください。

システムのウイルスを検索しています

検索の対象となるファイル
Windows がインストールされたドライブのルートと Windows のシステムフォルダの、拡張子が SYS、COM、EXE、DOC、DOT、XLA、XLS、XLT、DOS のファイルが検索対象となります。インストール完了後、お使いのコンピュータ上のすべてのドライブの全ファイルを対象にウイルス検索を実行することをお勧めします。

5. ユーザ情報を入力する

ユーザ情報（ユーザ名、所属、シリアル番号）を入力し、[次へ] ボタンをクリックします。シリアル番号は半角の英数字で入力します。シリアル番号を入力しないと、体験版（試用期間 30 日限定）としてインストールされます。

シリアル番号は、CD-ROM ケースに記載されている番号です。

シリアル番号は正しく入力しましょう

6. インストール先を選択する

初期設定では、次のフォルダにプログラムがインストールされます。

C:\Program Files\Trend Micro\Virus Buster 2003

特に変更の必要がなければ、初期設定のまま [次へ] をクリックします。

インストール先を変更する場合は、[変更] ボタンでインストール先を選択してください。インストール先を確認して、[次へ] ボタンをクリックします。

インストール先の選択

次のページにつづく

7. パーソナルファイアウォールのインストール

パーソナルファイアウォールをインストールするかどうかを選択して、[次へ] ボタンをクリックします。

パーソナルファイアウォールは、ウイルスバスター 2003 のインストール完了後に、いつでもインストール / アンインストールすることができます。パーソナルファイアウォールを後からインストールする方法については、107 ページを参照してください。

パーソナルファイアウォールのインストール選択

■ チェックボックスオン：パーソナルファイアウォールはインストールされます。

■ チェックボックスオフ：パーソナルファイアウォールはインストールされません。

他社のファイアウォール製品がインストールされている場合 ...

他社のファイアウォール製品がインストールされていると、他社のファイアウォール製品が検出されたことをお知らするメッセージが表示されます。他社のファイアウォール製品をアンインストールしてから、ウイルスバスター 2003 のインストールを再度実行していただくか、ウイルスバスター 2003 のパーソナルファイアウォールをインストールしないことをお勧めします。

注意 他社のファイアウォール製品をインストールしたまま、ウイルスバスター 2003 のパーソナルファイアウォールをインストールすると、プログラムが競合し、パーソナルファイアウォールが正常に機能しなくなる可能性があります。

他社のファイアウォール製品をアンインストールするには、[キャンセル] をクリックして、ウイルスバスター 2003 のインストールを中断してください。

8. インターネット自動接続オプションの選択

アップデートを実行したり、トレンドマイクロからウイルス緊急警告を受信するためには、インターネット接続が必要です。

この画面では、インターネットへの自動接続を許可するかどうかを選択してください。

インターネット自動接続オプションの選択

■ インターネットへの自動接続を許可する

このオプションを選択した場合、コンピュータがインターネットに接続されていると、アップデートが自動的に実行されます。また、トレンドマイクロからのウイルス緊急警告を受信することができます。

ADSL やケーブル接続など、常時接続環境でお使いの方にはお勧めの設定です。

> 注意 インターネット接続にダイヤルアップルータをお使いの環境でこのオプションを選択すると、ルータの設定によっては自動的にダイヤルアップ接続を開始して、課金が発生する場合があります。インターネット接続のたびに課金が発生する環境では、ご注意ください。

■インターネットへの自動接続を許可しない

このオプションを選択すると、アップデートを手動で実行する必要があります。また、トレンドマイクロからウイルスに関するお知らせを受信する機能も無効に設定されます。

このインターネットへの自動接続を許可する / 許可しないの設定に従って、インテリジェントアップデートおよびウイルス緊急警告の有効 / 無効の設定が決定されます。それぞれのオプションを選択した場合のアップデートとウイルス緊急警告の初期設定については、次を参照して下さい。

参照「インテリジェントアップデート」→ 93 ページ

参照「ウイルス緊急警告」→ 44 ページ

ウイルスバスター 2003 のインストール完了後に、それぞれの機能の設定画面で、有効 / 無効を切り替えることは可能です。

9. インストールの開始

インストールを開始する準備が完了したことをお知らせする画面が表示されたら、[インストール] をクリックします。インストールが開始されます。

[インストール] ボタンをクリックするとインストールが開始されます

次のページにつづく

10. インストールの完了

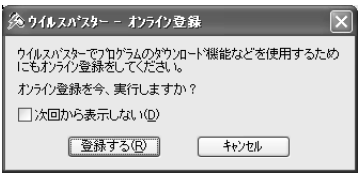
インストールが完了したことをお知らせする画面が表示されます。[終了] をクリックすると、インストールが完了します。

インストールは完了です

11. オンラインユーザ登録を実行する

インストールが完了したことをお知らせする画面と同時に、オンライン登録を促す画面が表示されます。

[登録する] ボタンをクリックして、すぐにオンライン登録をしましょう。



すぐにオンラインユーザ登録をしましょう

オンライン登録の方法については、25 ページの「オンラインユーザ登録の実行」を参照してください。

注意 ウイルスバスター 2003 をご使用の前に Readme ファイルを必ずお読みください。Readme ファイルには本書作成時に記載できなかった情報や、注意事項が記載されています。Readme を参照するには、Windows の [スタート] メニューから [プログラム] (Windows XP の場合[すべてのプログラム])→[トレンドマイクロ ウイルスバスター 2003]→[お読みください] の順に選択します。

インストール時にウイルスが見つかったら ...

インストール時にウイルスが検出されると「ウイルスが見つかりました！」のメッセージが表示されます。

検出したウイルスの処理方法を選択して [OK] ボタンをクリックすると、選択した処理方法でウイルスが処理されます。

コンピュータのメモリ内でウイルスが検出された場合、ウイルスバスター 2003 のインストールは中止されます。インストールを実行するには、メモリ内に潜むウイルスを駆除する必要があります。

メモリ内のウイルス駆除作業には、OS に関する高度な知識が必要な場合もあります。不明な点がありましたら、トレンドマイクロの「ウイルスバスタークラブセンター」にお問い合わせください。

インストール完了後の注意事項

メール検索設定

ウイルスバスター 2003 では、メール検索機能を有効にするために、インストール時にお使いのメールソフト (例：Microsoft Outlook Express) のアカウント情報を自動的に変更します。

e-mail を受信する際に使用するサーバとユーザ名の設定が次の通りに変更されます。

	変更前	変更後
受信用サーバ (POP3)	mail.company.ne.jp (例)	localhost
ユーザ名	<ユーザ名>	<ユーザ名>/mail.company.ne.jp (例)

通常、ユーザ名は、メールアドレスの @ マークより前の部分です

メールアカウント情報の変更は、お客さまがメールサーバから受信する e-mail に対して、ウイルスバスター 2003 がウイルス検索を実行できるようにするために必要です。メールアカウント情報の変更により e-mail が受信できなくなることはありません。

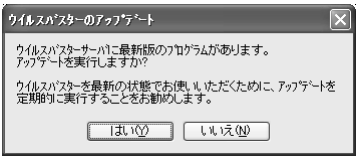
タスク検索設定

ウイルスバスター 2003 をインストールすると、初期設定で次のタスク検索が有効になり、指定された日時に指定された検索対象に対してウイルス検索が自動的に実行されるようになります。

検索対象	実行周期	開始時刻
すべてのファイル	毎月1日	15:00
Cドライブ	毎週水曜日	12:00

ウイルスバスター 2003 の設定画面で、これらのタスク検索を実行しないように設定することもできます。タスク検索については、69 ページを参照してください。

インストール直後のアップデート実行



シリアル番号を入力して、ウイルスバスター 2003 をインストールすると、数分後にアップデートの実行を促す画面が表示されます。この画面は、インストール後に 1 度だけ表示され、オンラインユーザ登録前に 1 度だけこの画面からアップデートを実行することができます。

[いいえ] または 画面右上の [X] (閉じる) ボタンをクリックしてこの画面を閉じた後のアップデートの実行には、ユーザ登録が必要になります。

注意 ウイルスバスター 2003 のインストール時に、手順 8 でインターネット自動接続を許可しないオプションを選択した場合には、この画面は表示されません。

注意 アップデートの実行にはインターネット接続が必要です。インターネット接続に伴い発生する通信料金はお客さまのご負担になります。

アップデート設定

ウイルスバスター 2003 のインストール時に、[インターネット自動接続を許可する] オプションを選択していると、初期設定では 3 時間ごとにインターネットに接続して、アップデートが必要かどうかを確認します。

お使いのコンピュータで、インターネット接続にプロキシサーバをお使いの場合、[インテリジェントアップデート設定] 画面でプロキシ情報を入力していただく必要があります。

ユーザ認証が必要なプロキシサーバをお使いの場合には、ユーザ名とパスワードも必ず入力してください。

注意 アップデートを実行するには、オンラインユーザ登録が必要です。オンラインユーザ登録については、25 ページを参照してください。

ウイルスバスターのインストールが終わったら？

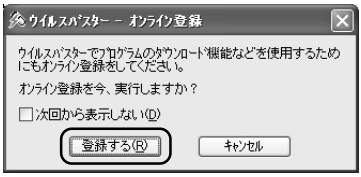
ウイルスバスター 2003 のインストールが完了すると、お使いのコンピュータの監視を始めます。初期設定のウイルスバスター 2003 でも十分なウイルス対策を行えます。お使いの環境に応じて、ウイルス検索設定やセキュリティ設定を変更してください。

また、ウイルスバスター 2003 をインストールした後も、定期的にアップデートを実行して、常に最新のウイルスに対応できるように心がけましょう。

まずはオンラインユーザ登録

パターンファイルやプログラムの最新版をインターネット経由でアップデートするためには、オンラインユーザ登録が必要です。

ウイルスバスター 2003 のインストールが完了すると、オンライン登録の実行を促すメッセージが表示されるので、**[登録する]** ボタンをクリックして、すぐにオンライン登録をしましょう（体験版としてインストールした場合は、オンライン登録を促す画面は表示されません）。



ユーザ登録により、自動的に「ウイルスバスタークラブ」会員に登録され、会員だけのさまざまな特典を受けることができます。

最新版にアップデート

ウイルスバスター 2003 を購入したばかりでも、新しいパターンファイルが公開されている場合があります。オンラインユーザ登録を完了したら、すぐに最新版にアップデートしましょう。

全ドライブ検索で安全確認

全ドライブ検索を実行しましょう。インストール時のウイルス検索（15 ページのインストール手順 4）では、一部のフォルダ内の特定のファイル形式に限定して検索を実行しています。お使いのコンピュータのすべてのドライブ、すべてのファイルに対して全ドライブ検索を実行して、クリーンな状態にしておきましょう。全ドライブ検索の実行方法については、54 ページを参照してください。

救済ディスクを作成

ウイルスバスター 2003 はシステムが起動してはじめて機能するため、システム領域に感染してしまったウイルスを駆除するためには「救済ディスク」が必要です。ウイルスバスター 2003 のインストールが完了したら、すぐに「救済ディスク」を作成しましょう。「救済ディスク」の作成方法については、85 ページの「救済ディスクについて」を参照してください。

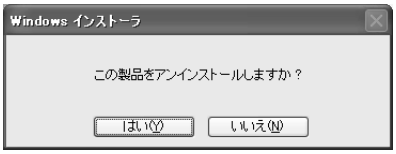
> 注意 救済ディスクを使ったウイルス駆除は、Windows 98/Me でのみお使いいただける機能です。Windows NT/2000/XP 環境では、救済ディスクを作成することができません。

ウイルスバスター 2003 のアンインストール

何らかの理由で、ウイルスバスター 2003 のアンインストール（削除）が必要な場合は、次のいずれかの手順に従ってアンインストールを実行してください。

手順：ウイルスバスター 2003 のアンインストールプログラムを使用する

1. 使用中のプログラムを終了します。
2. Windows の [スタート] メニューから [プログラム] (Windows XP の場合は [すべてのプログラム])→[トレンドマイクロ ウイルスバスター 2003]→[アンインストール] の順に選択します。
3. 「この製品をアンインストールしますか？」というメッセージが表示されたら、[はい] をクリックします。



アンインストール実行の確認メッセージ

4. 「インストールを続行するには次のアプリケーションを閉じる必要があります」というメッセージが表示される場合は、表示されたアプリケーションを終了して [再試行] ボタンをクリックするか、[無視] をクリックして、アンインストールを続行します。
5. アンインストールが完了したら、コンピュータを再起動します。

手順：Windows の [アプリケーションの追加と削除] を使用する

1. 使用中のプログラムを終了します。
2. お使いの OS にあわせて、次のいずれかの手順を実行してください。

   Windows XP の場合：

   a) Windows の [スタート] メニューから [コントロールパネル] を選択します。

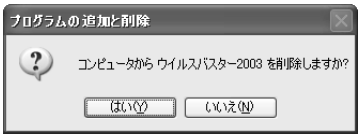
   b) [プログラムの追加と削除] をダブルクリックします。[プログラムの追加と削除] 画面が表示されます。

   Windows 98/Me/NT/2000 の場合：

   a) Windows の [スタート] メニューから [設定]→[コントロールパネル] を選択します。

   b) [アプリケーションの追加と削除] をダブルクリックします。 [アプリケーションの追加と削除] 画面が表示されます。

3. 現在インストールされているプログラムの一覧から、[ウイルスバスター 2003] を選択し、[追加と削除] または [削除] ボタンをクリックします。
4. 「コンピュータからウイルスバスター2003 を削除しますか？」というメッセージが表示されたら、[はい] をクリックします。



アンインストール実行の確認メッセージ

5. 「インストールを続行するには次のアプリケーションを閉じる必要があります」というメッセージが表示される場合は、表示されたアプリケーションを終了して [再試行] ボタンをクリックするか、[無視] をクリックして、アンインストールを続行します。
6. アンインストールが完了したら、コンピュータを再起動します。

第 2 章 ユーザ登録とユーザ特典

最新のパターンファイルやプログラムをインターネット経由でアップデートするには、オンラインユーザ登録を実行して「ライセンスキー」を入手し、さらにそのライセンスキーを登録していただく必要があります。ウイルスバスター 2003 をインストールしたら、すぐにオンラインユーザ登録を実行して、いつでも最新のパターンファイルやプログラムが入手できるようにしておきましょう。

また、ユーザ登録をしていただくと、「ウイルスバスタークラブ」会員として自動的に登録され、さまざまな特典を受けることができます。

第 2 章では、次の項目について解説します。

シリアル番号とライセンスキー

シリアル番号とライセンスキーとは？

お使いのコンピュータを最新のウイルスや不正プログラムから保護するためには、ウイルスバスター 2003 を定期的にアップデート (更新) して、最新の状態でお使いいただく必要があります。ウイルスバスター 2003 のアップデートを実行するためには、事前にオンラインユーザ登録をしていただく必要があります。

このオンラインユーザ登録に必要となるのが、**シリアル番号**と**ライセンスキー**です。

「シリアル番号」は、購入いただいたウイルスバスター 2003 の CD-ROM ケースに記載されている番号で、ウイルスバスター 2003 のインストール時に入力します。シリアル番号を入力しないと、30 日体験版としてインストールされます。体験版のままウイルスバスター 2003 をお使いいただいている場合、インストールから 30 日が経過すると、ウイルスバスター 2003 を使用することができなくなります。また、体験版では、オンラインユーザ登録を実行することができません。

製品版としてインストールするか、または体験版から製品版にアップグレードすると、オンラインユーザ登録を実行することができます。オンラインユーザ登録画面で必要な情報を入力し、ユーザ登録をしていただくと、お客さま専用の**「ライセンスキー」**が発行されます。このライセンスキーをウイルスバスター 2003 のプログラムに登録することで、ユーザ登録が完了します。ユーザ登録が完了するとインターネット経由で最新のパターンファイルやプログラムにアップデートすることができるようになります。

オンラインユーザ登録の手順

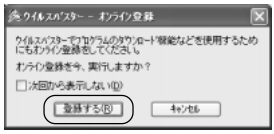
ウイルスバスター 2003 のアップデート機能を利用するためには、インターネット経由でのオンラインユーザ登録が必要です。ウイルスバスター 2003 をインストールしたら、オンラインユーザ登録を実行してください。

オンラインユーザ登録の実行

ウイルスバスター 2003 を製品版としてインストールするか、体験版から製品版にアップグレードしたら、オンラインユーザ登録画面に接続して、オンラインユーザ登録を実行します。オンラインユーザ登録が完了すると、登録したメールアドレスにお客さま専用の「ライセンスキー」が送信されますので、大切に保管してください。

手順：オンラインユーザ登録を実行する

1. ウイルスバスター 2003 のインストール時にシリアル番号を入力すると、インストール完了時に、オンラインユーザ登録を促すメッセージが表示されるので [登録する] ボタンをクリックします。



   ウイルスバスター 2003 の [ユーザ登録] 画面が表示されます。

   インストール直後にオンラインユーザ登録を実行しなかった場合 …
   次の手順に従って、ウイルスバスター 2003 の [ユーザ登録] 画面を表示します。

   a) Windows タスクトレイに表示されたウイルスバスター 2003 のアイコン を右クリックします。

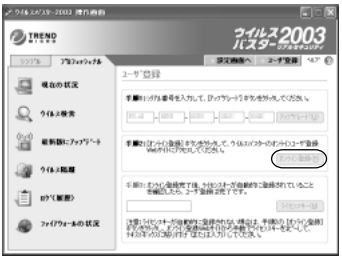
   b) 表示されるメニューから [操作画面を起動] を選択します。ウイルスバスター2003 の操作画面が表示されます。

   c) 操作画面の右上の [ユーザ登録] [ユーザ登録] ボタンをクリックします。

ウイルスバスター 2003 操作画面

次のページにつづく

2. ウイルスバスター 2003 操作画面の [ユーザ登録] 画面が表示されるので、[手順 2] の [オンライン登録] ボタンをクリックします。



3. ブラウザが起動して、オンラインユーザ登録画面に接続されるので、必要な情報を入力して、オンライン登録を実行してください。登録が完了すると、ライセンスキーが発行されます。また、ご登録いただいたメールアドレスにもライセンスキーを通知する e-mail が送信されますので、大切に保管してください。

4. ウイルスバスター 2003 操作画面に戻ります。[ライセンスキー] テキストボックスに、オンラインユーザ登録時に発行されたライセンスキーが自動的に入力されていることを確認したら、オンラインユーザ登録サイトの画面を閉じます。

ライセンスキーが自動的に登録されなかったら ...

ライセンスキーが自動的に登録されない場合は、手順 3 で発行されたライセンスキーをウイルスバスター 2003 操作画面に手動で入力して、[ライセンスキー] ボタンをクリックしてください。

ユーザ登録が完了したことを知らせるメッセージが表示されたら、ユーザ登録は完了です。

インターネット接続環境がない場合のユーザ登録

インターネット接続環境がないコンピュータでウイルスバスター 2003 をお使いの場合は、郵送または FAX でユーザ登録をしてください。ただし、郵送または FAX でユーザ登録をしていただいても、ウイルスバスター 2003 をインターネット経由でアップデートすることはできません。ウイルスバスター 2003 のアップデート機能をお使いいただくためには、オンラインユーザ登録が必要です。

この場合、ウイルスバスタークラブ会員特典のアップデート CD をお申し込みいただき(有料)、CD-ROM に収録されたパターンファイルをお使いいただくことができます。

ウイルスバスターを体験版としてお使いの場合

ウイルスバスター 2003 を体験版としてお使いの場合は、オンラインユーザ登録を実行することができません。オンラインユーザ登録をする前に、製品版にアップグレードする必要があります。

手順:体験版から製品版にアップグレード後オンラインユーザ登録する

1. ウイルスバスター 2003 操作画面を表示します。
2. 操作画面の [ユーザ登録] ボタンをクリックします。
3. [ユーザ登録] 画面が表示されます。[手順 1] にシリアル番号を入力して、[アップグレード] ボタンをクリックします。
4. 次に、[手順 2] の [オンライン登録] ボタンをクリックします。

[ユーザ登録] 画面

5. ブラウザが起動して、オンラインユーザ登録画面に接続されるので、必要な情報を入力して、オンライン登録を実行してください。登録が完了すると、ライセンスキーが発行されます。また、ご登録いただいたメールアドレスにもライセンスキーを通知するメールが送信されますので、大切に保管してください。
6. ウイルスバスター 2003 操作画面に戻ります。[ライセンスキー] テキストボックスに、オンラインユーザ登録時に発行されたライセンスキーが自動的に入力されていることを確認したら、オンラインユーザ登録サイトの画面を閉じます。

ライセンスキーが自動的に登録されなかったら ...

ライセンスキーが自動的に登録されない場合は、手順 3 で発行されたライセンスキーを手動で入力して、[ライセンスキー] ボタンをクリックしてください。

ユーザ登録が完了したことを知らせるメッセージが表示されたら、ユーザ登録は完了です。

ライセンスキーの再発行について

ウイルスバスター 2003 を再インストールしたり、旧バージョンからアップグレードした場合、ライセンスキーを再度登録する必要があります。コンピュータのシステム情報が変更されない限り、以前と同じライセンスキーを登録することができます。「登録内容が一致しません」と表示される場合には、再度オンラインユーザ登録サイトにアクセスして、ライセンスキーを再取得してください。

ユーザ登録すると何ができるの？

ウイルスバスタークラブ会員に自動登録

ウイルスバスター 2003 をお買い上げいただき、ユーザ登録を完了されたお客さまは、ウイルスバスターユーザで構成される「ウイルスバスタークラブ」の会員として**自動的**に登録されます。

豊富な会員特典

トレンドマイクロでは、ウイルスバスタークラブ会員の皆さまに、さまざまな会員特典をご用意しています。

- ユーザ登録 / 更新後 1 年間の e-mail、FAX、電話によるサポート
- パターンファイル、検索エンジン、プログラムのダウンロード
- ウイルスバスターシリーズの新製品への無料アップグレード
- Web ページと e-mail による定期的な情報提供サービス

ウイルスバスタークラブ会員特典内容は、予告なく一部変更または終了する場合があります。

2 年目以降は更新が必要です

「ウイルスバスタークラブ」の初年度年会費は、製品の購入代金に含まれていますので、ユーザ登録完了から 1 年間は、上記の特典を受けることができます。

2 年目以降も引き続き会員特典を利用するには、更新手続きをしていただき、別途年会費をお支払いいただく必要があります。あらかじめご了承ください。

更新の時期が近づきましたら、更新手続きのご案内をお送りいたします。

ウイルスバスター 2003 を使って、効果的にウイルス対策を行なうためには、定期的にアップデートを実行することが必要です。アップデートを実行するには、オンラインユーザ登録が必要です。ウイルスバスター 2003 をインストールしたら、忘れずにオンラインユーザ登録をしましょう。

オンラインユーザ登録によりウイルスバスタークラブ会員として登録されると、アップデートだけでなく、さまざまな会員特典を受けることができます。

第 3 章 クイックツアー

ウイルスバスター 2003 では、ウイルスの監視だけではなく、コンピュータにすでに入り込んでしまったウイルスを検出、駆除したり、検出されたウイルスを確認したりすることができます。

ウイルスバスター 2003 を使いこなすために、第 3 章ではウイルスバスターの基本的な使い方を説明します。次の項目について解説します。

ウイルスバスター 2003 のウイルス対策

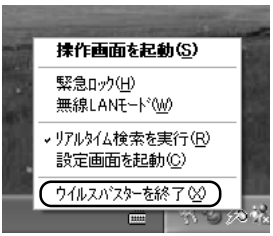
ウイルスバスター 2003 をインストールすると、コンピュータが起動している間は常にウイルスバスターがウイルスを監視するように設定されます。**ウイルスバスターを手動で開始する必要はありません。**

ウイルスバスター 2003 の起動と終了

ウイルスバスター 2003 では、ファイルの読み込み / 書き込みなどの動作を監視しています。このため、OS の上書きインストール時や、ドライブのエラーチェックを実行する時、または CD-R/RW ドライブを使ってデータを CD に書き込む場合などに、処理を妨げる原因になる場合があります。このような場合には、ウイルスバスター 2003 の検索機能を一時的に停止することができます。

手順：リアルタイム検索機能を一時的に停止する

1. Windows タスクトレイに表示されたウイルスバスター 2003 のアイコン を右クリックします。
2. 表示されるメニューから [ウイルスバスターを終了] を選択します。



3. 「ウイルスバスターを終了しますか？…」という確認メッセージが表示されたら[はい] をクリックします。
4. タスクトレイからアイコン表示が消え、ウイルスバスター 2003 の検索機能が停止します。

ウイルスバスターは終了したままにせず、後で必ず起動してください。ウイルスや不正プログラムの侵入を防ぐために、ウイルスバスター 2003 を常に起動しておくことをお勧めします。

手順：ウイルスバスターを起動する

1. Windows の [スタート] メニューから [プログラム] (Windows XP の場合は [すべてのプログラム]) → [トレンドマイクロ ウイルスバスター 2003] → [リアルタイムエージェント] の順に選択します。
2. ウイルスバスター 2003 が起動し、アイコンがタスクトレイに表示されます。アイコンが赤く表示されていれば、ウイルスバスター 2003 のリアルタイム検索が有効に機能しています。

リアルタイムエージェントのアイコンは、リアルタイム検索やパーソナルファイアウォールの状態によって、表示が異なります。詳しくは次のセクションを参照してください。

リアルタイムエージェントアイコンの見方

ウイルスバスター 2003 の起動中は、画面右下の Windows タスクトレイ上にウイルスバスターのアイコンが表示されます。このアイコンは、**「リアルタイムエージェント」**と呼ばれ、ウイルスバスター 2003 の動作状況に応じて変化します。アイコンには、次の 4 種類があります。


（赤）ウイルスバスター 2003 が起動されていて、リアルタイム検索も有効です。ウイルスの侵入は常に監視されます。


（グレー）ウイルスバスター 2003 は起動されていますが、リアルタイム検索は無効になっています。ウイルスの侵入はリアルタイムで監視されません。


緊急ロックがかかっています。緊急ロックが有効の間は、ネットワークやインターネットにアクセスできません。


最新版へのアップデート処理を実行中です。

ウイルスバスター 2003 操作画面

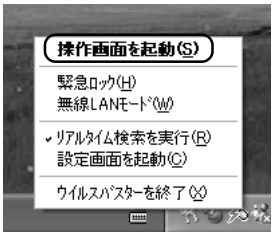
ウイルスバスター 2003 は、「操作画面」と「設定画面」の 2 つの画面で構成されています。また、それぞれの画面の「ヘルプ」メニューから、トレンドマイクロが提供するウイルス最新情報やウイルスバスター 2003 のサポートページにアクセスすることができます。

まずはじめに、ウイルスバスター 2003 の**「操作画面」**について説明します。

操作画面の表示

ウイルスバスター 2003 の操作画面は、「シンプル」モードと「プロフェッショナル」モードに分かれており、ウイルス検索、アップデートなどを実行することができます。ウイルスバスター 2003 の操作画面を表示するには、次のいずれかの手順を実行してください。

- Windows タスクトレイ上に表示されているウイルスバスターのアイコン  をダブルクリックする。
- Windows タスクトレイ上に表示されているウイルスバスターのアイコンを右クリックして、表示されたメニューから [操作画面を起動] を選択する。

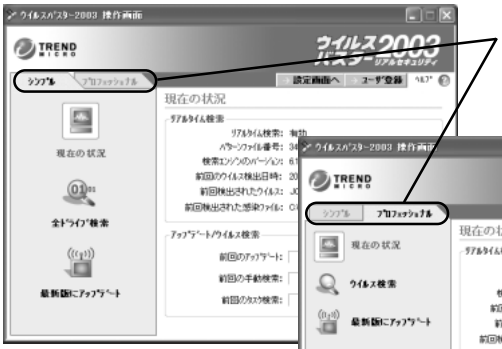


- ウイルスバスター 2003 設定画面で  [操作画面へ] ボタンをクリックする。
- Windows の [スタート] メニューから [プログラム] (Windows XP の場合は[すべてのプログラム])→[トレンドマイクロ ウイルスバスター 2003]→[ウイルスバスター 2003 操作] の順に選択する。

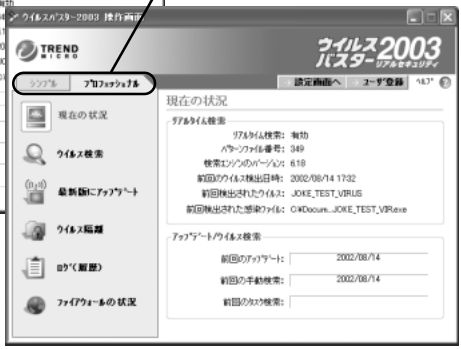
シンプルモードとプロフェッショナルモード

「シンプルモード」は、ウイルスバスター 2003 で特に使用頻度の高い機能だけを集めた画面です。シンプルモードでは、コンピュータ上のすべてのファイルに対するウイルス検索や最新版へのアップデートなどを実行することができます。操作画面で、「プロフェッショナル」モードが表示されている場合は、左のタブから［シンプル］を選択すると、シンプルモードに切り替えることができます。

「プロフェッショナルモード」では、シンプルモードよりもさらに詳細な操作が可能です。特定のドライブに対してウイルス検索を実行したり、ウイルスバスター 2003 の各機能のログ (履歴) 、ファイアウォールの状況などを参照することができます。



シンプルモード



プロフェッショナルモード

ウイルスバスター 2003 の操作画面では、次の操作を実行することができます。

現在の状況 (シンプルモード / プロフェッショナルモード)

現在のウイルスバスターの動作状況を随時確認することができます。

全ドライブ検索 (シンプルモードのみ)

[全ドライブ検索] をクリックすると、コンピュータ上のすべてのファイルに対するウイルス検索が開始されます。全ドライブ検索機能については、54ページの「全ドライブ検索の実行」を参照してください。

ウイルス検索 (プロフェッショナルモードのみ)

[ウイルス検索] 画面では、「手動検索」と「タスク検索」の 2 種類のウイルス検索を実行することができます。

「手動検索」では、お使いのコンピュータのドライブやフォルダを選択して、ウイルス検索を実行することができます。手動検索については、55 ページの「ドライブ / フォルダを指定してウイルス検索を実行」を参照してください。

「タスク検索」では、「タスク」と呼ばれるウイルス検索の対象やウイルスが検出された場合の処理方法などを事前に定義した作業を、ボタン1つで実行することができます。タスク検索については、69 ページの「タスク検索」を参照してください。

最新版にアップデート (シンプルモード / プロフェッショナルモード)

パターンファイルやプログラムを最新版にアップデートすることができます。最新版へのアップデート機能については、96ページの「手動アップデートの実行」を参照してください。

ウイルス隔離 (プロフェッショナルモードのみ)

ウイルスバスター2003では、ウイルス感染ファイルや感染の疑いのあるファイルを、安全な場所に隔離して処理することができます。[ウイルス隔離] 画面では、隔離されたファイルをどのように処理したらよいかを教えてくれる [ウイルス処理アシスタント] を参照しながら、隔離された感染ファイルを削除したり、ウイルス駆除を実行することができます。ウイルス隔離機能については、81ページの「ウイルスを駆除できない場合はどうすればいいの？」を参照してください。

ログ (履歴) の表示 (プロフェッショナルモードのみ)

ウイルスバスター 2003 では、ウイルス検出、アップデートなどのウイルスバスター 2003 の動作状況を、履歴として「ログ」に記録しています。[ログ (履歴)] 画面では、記録された内容を確認したり、ログをファイルに保存することができます。ログについては、41 ページを参照してください。

ファイアウォールの状況 (プロフェッショナルモードのみ)

[ファイアウォールの状況] 画面では、パーソナルファイアウォールがブロックしたアクセスの状況を確認したり、緊急ロックのオン/オフや無線LANモードの切り替えなどの操作が可能です。

ウイルスバスター 2003 のパーソナルファイアウォールがインストールされていない場合には、このボタンは表示されません。

緊急ロックのオン / オフについては、43 ページの「緊急ロック機能」を参照してください。

無線LANモードの切り替えについては、114ページの「無線LAN環境でのセキュリティ」を参照してください。

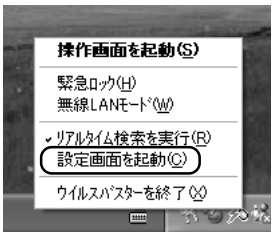
ウイルスバスター 2003 設定画面

ウイルスバスター 2003 の設定画面では、ウイルスバスター 2003 のウイルス検索やセキュリティ機能の有効 / 無効の切り替え、検索などの詳細な条件を設定することができます。

設定画面の表示

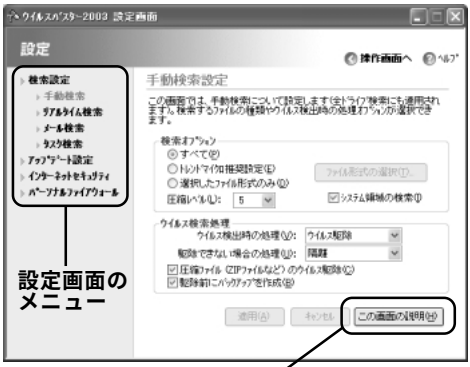
ウイルスバスター 2003 の設定画面では、ウイルスバスターの各機能の有効 / 無効の切り替えや、操作の詳細な条件を設定することができます。

ウイルスバスター 2003 の設定画面を表示するには、次のいずれかの手順を実行してください。



- タスクトレイに表示されているウイルスバスターのアイコン を右クリックして、表示されたメニューから [設定画面を起動] を選択する。
- ウイルスバスター 2003 操作画面から 設定画面へ [設定画面へ] ボタンをクリックする。
- Windows の [スタート] メニューから [プログラム (Windows XP の場合 [すべてのプログラム])] → [トレンドマイクロ ウイルスバスター 2003] → [ウイルスバスター 2003 設定] の順に選択する。

ウイルスバスター 2003 設定画面



設定画面の左側には、メニューが表示されます。各メニュー項目をクリックして選択すると、さらにサブメニューが表示されます (サブメニューが表示されない項目もあります)。表示されたサブメニューをクリックして選択すると、選択した項目に関する設定画面が右側に表示されます。

各設定画面の右下に **[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、表示されている設定画面に関連する説明が表示されます。

検索設定メニュー

検索設定メニューは、次の 4 つのサブメニューで構成されています。

■ 手動検索
[手動検索設定] 画面では、手動でウイルス検索を実行した時にウイルスが検出された場合の処理方法などを設定します。

手動検索の実行方法については、54 ページを参照してください。

[手動検索設定] 画面の詳細については、57 ページを参照してください。

■ リアルタイム検索
[リアルタイム検索設定] 画面では、リアルタイム検索の有効 / 無効の切り替えや、リアルタイム検索実行中にウイルスが検出された場合の処理方法などを設定します。

[リアルタイム検索設定] 画面の詳細については、46 ページを参照してください。

■ メール検索
[メール検索設定] 画面では、メール検索の有効 / 無効の切り替えや、メール検索中にウイルスが検出された場合の処理方法を設定します。

メール検索と [メール検索設定] 画面の詳細については 63 ページを参照してください。

■ タスク検索
[タスク検索設定] 画面では、ウイルス検索対象やウイルスが検出された場合の処理方法を定義して「タスク」と呼ばれるデータとして保存することができます。保存したタスクは、指定した時刻に自動的に実行するように設定したり、ウイルスバスター 2003 操作画面から手動で実行することができます。

タスク検索の詳細については、69 ページを参照してください。

アップデート設定メニュー

アップデート設定メニューを選択すると、右側の画面に [インテリジェントアップデート設定] 画面が表示されます。この画面では、インテリジェントアップデートの有効 / 無効の切り替えや、インテリジェントアップデートを実行する周期などを設定することができます。

インテリジェントアップデートの詳細については、93 ページを参照してください。

インターネットセキュリティメニュー

インターネットセキュリティメニューは、次の 2 つのサブメニューで構成されています。

■ WebTrap
WebTrap（ウェブトラップ）機能は、害のあるプログラムを含む Web サイトにアクセスした場合に、お使いのコンピュータを守る機能です。[WebTrap 設定] 画面では、WebTrap の有効 / 無効を切り替えたり、害のあるプログラムを含む Web サイトにアクセスしようとした際の処理を設定します。

WebTrap 機能の詳細については、100 ページを参照してください。

■ URL フィルタ
URL フィルタ機能では、指定した Web サイトへのアクセスを規制して、その Web サイトを表示しないようにすることができます。[URL フィルタ設定] 画面では、URL フィルタ機能の有効 / 無効を切り替えたり、アクセスを規制する Web サイトを指定したり、規制サイトへアクセスした際の処理を設定します。

URL フィルタ機能については、102 ページを参照してください。

パーソナルファイアウォールメニュー

ウイルスバスター 2003 のパーソナルファイアウォールでは、外部のコンピュータからのアクセスを制限したり、「トロイの木馬」と呼ばれる不正プログラムが使用するポートを監視します。

パーソナルファイアウォールメニューは、次の 3 つのサブメニューで構成されています。

ウイルスバスター 2003 のパーソナルファイアウォールをインストールしていない場合は、このメニューは表示されません。

■ セキュリティレベル
[セキュリティレベル設定] 画面では、パーソナルファイアウォールの有効 / 無効を切り替えたり、「高」、「中」、「低」の 3 つのセキュリティレベルを切り替えることができます。

パーソナルファイアウォールおよびセキュリティレベルについては、107 ページを参照してください。

■ 除外リスト

[セキュリティレベル設定] 画面で選択したセキュリティレベルに対して、ブロック対象から除外したり、ブロック対象に含めるなどして、外部への接続や、外部からの接続をより柔軟にコントロールすることができます。[除外リスト] 設定画面では、除外するアクセスの詳細を定義することができます。

除外リストの詳細については、110 ページの「除外リストの設定」を参照してください。

■ ブロックするポート

ウイルスバスター 2003 では、「トロイの木馬」と呼ばれる不正プログラムが使用するポートを監視して、ブロックします。[ブロックするポート] 画面では、ウイルスバスター 2003 が監視するポートの一覧を確認することができます。

ブロックするポートについては、113 ページの「ブロックするポートの確認」を参照してください。

ウイルスバスター 2003 のヘルプメニュー

ウイルスバスター 2003 の操作画面と設定画面には、それぞれ便利なヘルプメニューが用意されています。

ヘルプメニューを利用しよう

操作画面または設定画面の [ヘルプ] ボタンをクリックして表示されるメニューからは、次の情報にアクセスすることができます。

■ ヘルプ

ウイルスバスター 2003 のオンラインヘルプを表示します。ウイルスバスター 2003 の操作に困った時や機能の説明を参照したい場合に利用します。オンラインヘルプについては、116 ページの「オンラインヘルプを利用する」も参照してください。

[ヘルプ] ボタンをクリックしてメニューを表示

■ サポートニュース

トレンドマイクロの製品サポートサイトへジャンプします。製品サポートサイトを表示するには、インターネット接続が必要です。

■ お問い合わせサイト

ウイルスバスタークラブ会員専用のサポートサイトへジャンプします。サポートページを表示するには、インターネット接続が必要です。

■ 最新ウイルス情報

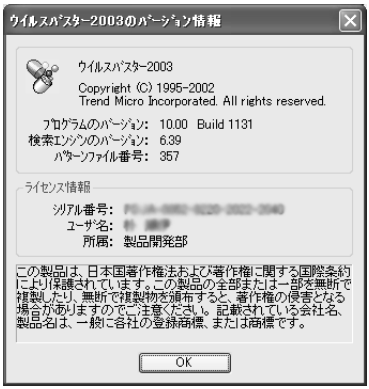
トレンドマイクロのウイルス情報サイトへジャンプします。このサイトでは、現在流行しているウイルスに関する情報や、ウイルスの危険度などの情報を提供しています。ウイルス情報サイトを表示するには、インターネット接続が必要です。

■ ウイルスデータベース

トレンドマイクロのウイルスデータベースサイトへジャンプします。このサイトでは、ウイルス名やキーワードを条件に、特定のウイルスに関する情報を検索することができます。ウイルスデータベースサイトを表示するには、インターネット接続が必要です。

■ バージョン情報

お使いのウイルスバスター 2003 のバージョン情報が表示されます。バージョン情報には、現在使用しているパターンファイル、検索エンジン、プログラムのバージョンが表示されます。

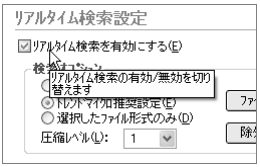


ウイルスバスター 2003 のバージョン情報

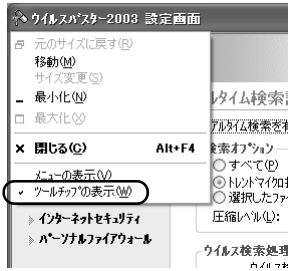
その他の便利な機能

ツールチップ

ウイルスバスター 2003 の操作画面や設定画面上で、マウスのポインタを各オプションやメニュー、ボタンに近づけると、それぞれの機能について簡単な説明が表示されます。これを「ツールチップ」と呼びます。

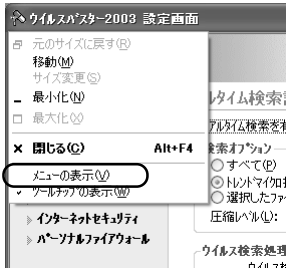


ツールチップの表示 / 非表示は、設定画面の画面左上のアイコン  をクリックして表示されるメニューで、[ツールチップの表示] のチェックマーク (✓) をオン / オフすることで、切り替えることができます。



メニューバー表示

ウイルスバスター 2003 の操作画面および設定画面のメニューバーを表示することができます。初期設定では、メニューバーは表示されません。メニューバーを表示するには、操作画面または設定画面の画面左上のアイコン  または  をクリックして表示されるメニューで、[メニューの表示] を選択します。次回、画面起動時からメニューが表示されるようになります。



メニューが表示されます。

ウイルスバスター 2003 のログ (履歴)

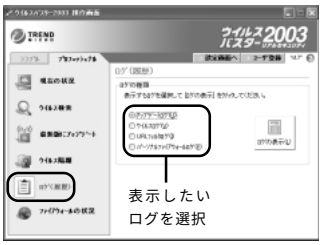
ウイルスバスター 2003 では、アップデート、ウイルス検索、URL フィルタ、パーソナルファイアウォールの動作情報を**「ログ」(履歴)**として管理しています。

ログの表示

ウイルスバスター 2003 の操作画面から、記録されているログの内容を表示して、確認することができます。

手順:ログを表示する

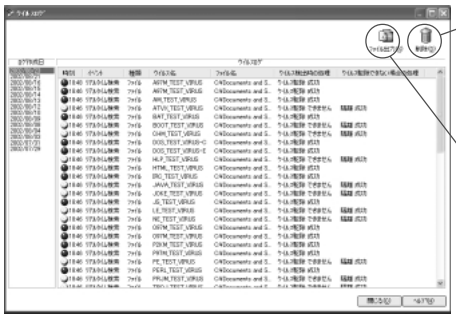
1. ウイルスバスター 2003 操作画面を表示します。
2. シンプルモードが表示されている場合は、左のタブから [プロフェッショナル] を選択してプロフェッショナルモードに切り替えます。
3. [ログ (履歴)] ボタンをクリックします。
4. [ログの種類] から表示したいログの種類を選択して、[ログの表示] ボタンをクリックすると、選択したログが表示されます。



[ログ (履歴)] 画面

ウイルスログの例

ウイルスログには、ウイルスが検出された日時や、処理結果などが記録されています。



ログの出力

表示したログを CSV (カンマ付きテキスト) 形式で保存して、記録を保存することができます。

手順：ログをファイルに出力する

1. ウイルスバスター 2003 操作画面を表示します。
2. シンプルモードが表示されている場合は、左のタブから [プロフェッショナル] を選択してプロフェッショナルモードに切り替えます。
3. [ログ（履歴）] ボタンをクリックします。
4. [ログの種類] から表示したいログの種類を選択して、[ログの表示] ボタンをクリックすると、選択したログが表示されます。
5. ファイルに出力したいログの日付を [ログの作成日] から選択します。
6. 画面右上の [ファイル出力] ボタンをクリックします。
7. [名前をつけて保存] 画面が表示されるので、ファイルの保存先を選択し、ファイル名を入力したら、[保存] ボタンをクリックします。

ログの削除

ウイルスバスター 2003 の各ログは継続的に作成されるため、ログファイルサイズは日々大きくなります。必要に応じてログファイルを手動で削除してください。

手順：ログを削除する

1. ウイルスバスター 2003 操作画面を表示します。
2. シンプルモードが表示されている場合は、左のタブから [プロフェッショナル] を選択してプロフェッショナルモードに切り替えます。
3. [ログ（履歴）] ボタンをクリックします。
4. [ログの種類] から表示したいログの種類を選択して、[ログの表示] ボタンをクリックすると、選択したログが表示されます。
5. 画面右上の [削除] ボタンをクリックします。

[ログの削除] 画面

6. [ログの削除] 画面が表示されます。ドロップダウンリストから日付を選択します。選択した日付より古いログが削除されます。

7. [OK] ボタンをクリックすると、指定した日付より古いログが削除されます。

その他のツールと機能

緊急ロック機能

「緊急ロック」は、コンピュータに被害を与える不正プログラムを誤って実行してしまったり、ウイルスが見つかった時に、他のコンピュータへ被害を広めないように、ただちにインターネット接続や他のコンピュータとの接続を遮断する機能です。

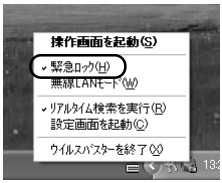
緊急ロックを有効にして、ネットワークを遮断してしまえば、他のコンピュータに被害を拡大してしまうような事態も、未然に防ぐことができます。

注意 ウイルスバスター 2003 のパーソナルファイアウォールがインストールされていない場合には、緊急ロック機能を利用することができません。

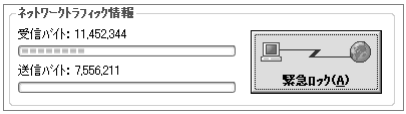
手順：緊急ロックのオン / オフを切り替える

次のいずれかの方法で、緊急ロックのオン / オフを切り替えることができます。

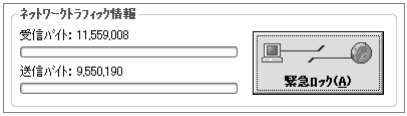
■ Windowsタスクトレイ上に表示されているウイルスバスター 2003 のアイコン を右クリックして、表示されるメニューから [緊急ロック] を選択してオン / オフを切り替えます。緊急ロックをオンにするには、チェックマーク (✓) をつけ、オフにするには、チェックマークを外します。



■ ウイルスバスター 2003 操作画面のプロフェッショナルモード画面で、左側の [ファイアウォールの状況] アイコンをクリックして、表示される [ファイアウォールの状況] 画面の [緊急ロック] ボタンをクリックして、緊急ロックのオン / オフを切り替えます。



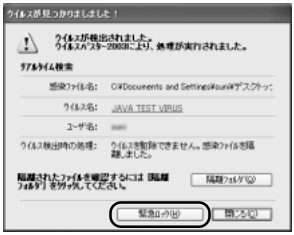
緊急ロックオフ時



緊急ロックオン時

■ ウイルスが検出された時に表示される「ウイルスが見つかりました！」のメッセージの [緊急ロック] ボタンをクリックすると、緊急ロックがオンになります。

この画面から、緊急ロックをオフにすることはできません。緊急ロックをオフにするには、タスクトレイのウイルスバスターのアイコン を右クリックして、表示されるメニューから [緊急ロック] を選択します。



ウイルス検出時に表示されるメッセージ

> **注意** 緊急ロックシステムを有効にすると、すべてのネットワーク接続が遮断されます。e-mail の送受信やインターネットへのアクセスだけでなく、ネットワーク上の他のコンピュータへのアクセスもできなくなります。ウイルスバスターでお使いのコンピュータにウイルス検索を実行するなどして安全が確認されたら、必ず緊急ロックを解除してください。

緊急ロックがオンになると、デスクトップ右下のタスクトレイに表示されるウイルスバスターのアイコンが、 のアイコンに変わります。

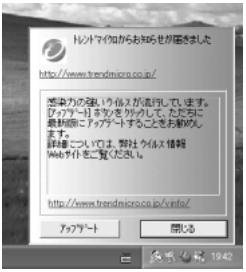
ウイルス緊急警告

ウイルスバスター 2003 の新機能として、ウイルス緊急警告機能では、トレンドマイクロからのウイルス警告をインターネット経由で受信することができます。ウイルス緊急警告では、危険度の高いウイルスの情報や、誤って開くと危険な e-mail の件名など、ウイルスに関する情報をインターネット経由でお知らせします。

> **注意** ウイルス緊急警告を受信するためには、インターネット接続環境が必要です。ダイヤルアップ接続など、インターネット接続のたびに課金が発生する環境では、ご注意ください。

ウイルス緊急警告が有効に設定されている場合、トレンドマイクロからウイルス緊急警告が発信されると、お使いのコンピュータの画面右下に警告メッセージが自動的に表示されます。

表示されたメッセージからトレンドマイクロのウイルス情報サイトにアクセスして、さらに詳しい情報を確認することもできます。



ウイルス緊急警告の例

ウイルス緊急警告の有効化 / 無効化

ウイルスバスター 2003 のインストール時に、インターネットへの自動接続を許可するオプションを選択した場合 (16 ページのインストール手順 8) には、ウイルス緊急警告機能は有効に設定されています。

ウイルスバスター 2003 のインストール完了後に、いつでもウイルス緊急警告の有効 / 無効を切り替えることができます。

手順：ウイルス緊急警告の有効 / 無効の切り替え

1. Windows の [スタート] メニューから [プログラム](Windows XP の場合は [すべてのプログラム]) →[トレンドマイクロ ウイルスバスター 2003]→[ウイルス緊急警告設定] の順に選択します。
2. [ウイルス緊急警告設定] 画面が表示されます。ウイルス緊急警告を受信するには、[ウイルス緊急警告を有効にして、最新の情報を取得できるようにする] チェックボックスをオンにします。

   受信しない場合には、チェックボックスをオフにします。

[ウイルス緊急警告設定] 画面

3. [OK] ボタンをクリックすると、設定を保存して、[ウイルス緊急警告設定] 画面が終了します。

[ウイルス緊急警告設定] 画面の [情報を見る] ボタンをクリックして、トレンドマイクロから最後に取得した情報を確認することもできます。

第 4 章 ウイルス検索

ウイルスバスター 2003 をインストールすると、リアルタイム検索が開始され、ウイルスの監視が始まります。

ウイルスバスター 2003 では、リアルタイム検索以外に、検索を手動で実行する機能や、検索の予約、メール検索などの検索機能も用意しています。

第 4 章では、ウイルスバスター 2003 のウイルス検索機能について説明します。

リアルタイム検索

リアルタイム検索とは

リアルタイム検索機能は、お使いのコンピュータ上で行われるファイルの読み込み / 書き込みを常に（リアルタイムで）監視し、ウイルスに感染しているファイルへのアクセスを防止する機能です。リアルタイム検索が有効であれば、ウイルス感染したファイルが誤って侵入しても、感染ファイルを開く前にウイルスを検出して処理を実行します。初期設定のウイルスバスターでは、リアルタイム検索が有効に設定されています。

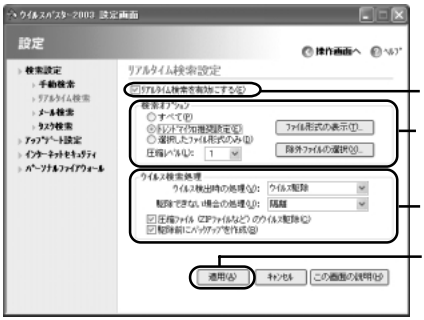
リアルタイム検索の詳細設定

[リアルタイム検索設定] 画面では、リアルタイム検索の有効 / 無効の切り替えや、ウイルス検出時のウイルス処理方法を設定することができます。また、リアルタイム検索の対象とするファイルを指定することもできます。

手順：[リアルタイム検索設定] 画面を表示する

1. ウイルスバスター 2003 の設定画面を表示します。
2. 設定画面で [検索設定]→[リアルタイム検索] を選択して、[リアルタイム検索設定] 画面を表示します。

注意 [リアルタイム検索設定] 画面で設定を変更したら、[適用] ボタンを必ずクリックしてください。[適用] ボタンをクリックしないと、変更した設定は有効になりません。



リアルタイム検索の有効 / 無効の切り替え

検索対象や圧縮レベルの設定

ウイルス検出時の処理設定

設定が完了したら必ず [適用] ボタンをクリック！

[リアルタイム検索設定] 画面

[リアルタイム検索] 画面では、リアルタイム検索に関する次の項目について設定することができます。

リアルタイム検索の有効 / 無効の切り替え

何らかの理由でウイルスバスター 2003 のリアルタイム検索機能を一時的に停止したい場合には、[リアルタイム検索を有効にする] チェックボックスをオフにします。

注意 リアルタイム検索を無効にすると、ウイルスに感染する恐れがあります。特別な理由がない限り、リアルタイム検索は常に有効にしておくことをお勧めします。また、一時的にリアルタイム検索を無効にした場合にも、チェックボックスをオンにして、リアルタイム検索を有効に戻すことをお勧めします。

リアルタイム検索の有効 / 無効の状態は、タスクトレイのウイルスバスターアイコン で確認することができます。

アイコンが**赤**の場合は、リアルタイム検索が**オン**になっています。

アイコンが**グレー**の場合は、リアルタイム検索が**オフ**になっています。

検索対象の選択

リアルタイム検索で検索対象とするファイルの種類を指定することができます。すべてのファイルを検索すると時間が長くかかるため、ウイルスに感染しやすいファイルだけを特定して検索することで、検索時間を短縮することができます。

リアルタイム検索では、次の 3 つのオプションを使って、検索するファイルの種類を指定することができます。

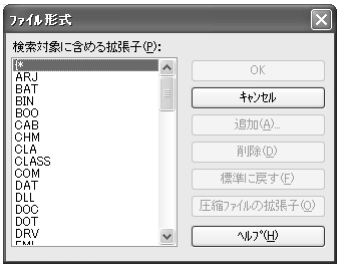
● すべて

ファイルの種類にかかわらず、すべてのファイルをウイルス検索します。これは最も安全なオプションといえますが、安全性と引き換えに検索時間が長くかかります。

● トレンドマイクロ推奨設定

トレンドマイクロが過去の実績や分析から、ウイルス感染する危険があると判断された種類のファイルが、検索対象に設定されます。すべてのファイルを検索する設定に比べて、効率的な検索設定であると言えます。

このオプションを選択したら、[ファイル形式の表示] ボタンをクリックして、推奨設定に含まれるファイルの種類を確認することができます。



推奨設定に含まれるファイルの種類の一覧

● 選択したファイル形式のみ

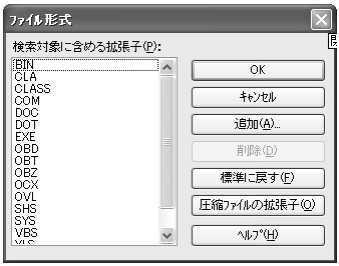
検索したいファイルの種類を自分で指定することができます。

このオプションを選択したら、次の手順に従って検索するファイルの種類を指定します。

手順：検索するファイルの種類を指定する

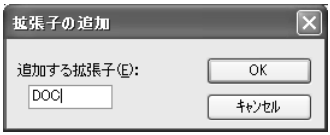
1. [リアルタイム検索設定] 画面の [ファイル形式の選択] ボタンをクリックします。[ファイル形式] 画面が表示されます。

   すでに、いくつかのファイルが検索対象として指定されています。



検索するファイルの種類の一覧

2. ファイルの種類を追加するには、[追加] ボタンをクリックして、[拡張子の追加] 画面のテキストボックスに拡張子を 1 つずつ入力して、[OK] をクリックします。



追加する拡張子の入力画面

拡張子リストから特定の拡張子を削除したい場合は、[ファイル形式] 画面で、削除したい拡張子をリストから選択して [削除] ボタンをクリックします。

[圧縮ファイルの拡張子] ボタンをクリックすると、一般的な圧縮形式で使用される拡張子がまとめて追加されます。

リストを初期設定の状態に戻したい場合は、[標準に戻す] ボタンをクリックします。

3. 検索するファイルの種類をすべて指定したら、[OK] ボタンをクリックして [リアルタイム検索設定] 画面に戻ります。

除外ファイル / フォルダの選択

ウイルスバスター 2003 では、ウイルス検索を実行したくないファイルを、リアルタイム検索の対象から除外することができます。

ウイルスバスター 2003 では、一部のファイルについて、ウイルスに感染していないにもかかわらず感染ファイルとして検出してしまうことがあります。これは、ファイルにウイルスと似たコードが含まれているためですが、複雑なマクロコードを含むファイルなどでは、このような現象が起こる場合があります。

ウイルスバスター 2003 のリアルタイム検索が有効に設定されている状態では、ウイルスと認識されたファイルを開くことができません。この場合に、ファイルを検索対象から除外するように設定することができます。

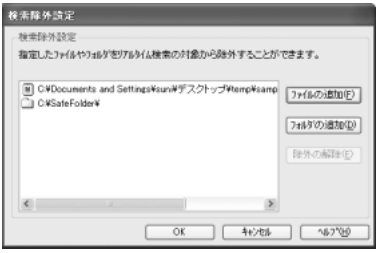
特定のファイルだけではなく、フォルダごと検索対象から除外することもできます。

手順：除外ファイル / フォルダを選択する

1. [リアルタイム検索設定] 画面で、[除外ファイルの選択] ボタンをクリックします。

次のページにつづく

2. 表示される [検索除外設定] 画面で、除外するファイル / フォルダを選択します。



検索から除外するファイル / フォルダの設定画面

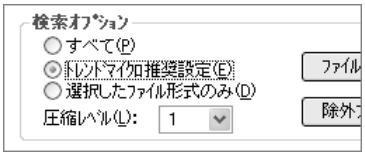
● [ファイルの追加] ボタン
このボタンをクリックして表示される画面で、検索対象から除外したいファイルを選択します。選択したファイルが、[検索除外設定] 画面に表示されます。

● [フォルダの追加] ボタン
このボタンをクリックして表示される画面で、検索対象から除外したいフォルダを選択します。選択したフォルダが、[検索除外設定] 画面に表示されます。

● [除外の解除] ボタン
検索対象から除外するように設定したファイル / フォルダをクリックして選択し、[除外の解除] ボタンをクリックすると、除外から外すことができます。

圧縮ファイルの検索

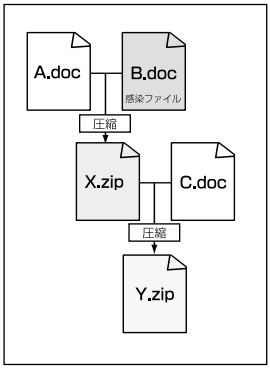
ウイルスバスター 2003 では、ウイルス検索時に圧縮ファイルを自動的に解凍して、ウイルス検索を実行した後、再び圧縮することができます。圧縮ファイルの中には、複数回圧縮されているファイルもあります。[リアルタイム検索設定] 画面の [圧縮レベル] では、何回圧縮されたファイルからウイルスを検出するか設定することができます。



圧縮レベルの設定

たとえば、「A.doc」というファイルとウイルス感染した「B.doc」という 2 つのファイルが「X.zip」というファイルに圧縮されているとします。そして、「X.zip」ファイルと「C.doc」ファイルがさらに、「Y.zip」ファイルに圧縮されているとします。「A.doc」と「B.doc」は 2 回圧縮されていることになります。

この時、[圧縮レベル] が「1」に設定されていると、2 回圧縮されている感染ファイル「B.doc」からウイルスを検出することができません。



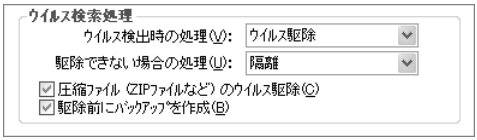
圧縮ファイルの例

[圧縮レベル] が「2」以上に設定されていると、「B.doc」からウイルスを検出することができます。

[圧縮レベル] の値を高くすれば、より深い階層の圧縮ファイルからウイルスを検出することができますが、検索に必要な時間も長くなります。

ウイルス検索処理

リアルタイム検索実行中にウイルス感染ファイルが検出された場合の、感染ファイルの処理方法を設定します。



ウイルス検出時の処理設定

● ウイルス駆除 (初期設定)
感染ファイルからウイルスコードのみが取り除かれます。ウイルスの駆除が成功すると、元のファイルは通常のファイルとして使用することができます。

ウイルスの種類によっては、感染ファイルからウイルスを駆除できない場合があります。ウイルスの駆除を選択した場合には、[駆除できない場合の処理] を設定する必要があります。初期設定では、駆除できない場合は「隔離」処理を実行するように設定されています。

● 隔離
ウイルスが検出されると、感染ファイルが次の隔離フォルダに移動されます。

< ウイルスバスター 2003 インストールフォルダ > \ Quarantine

通常、< ウイルスバスター 2003 インストールフォルダ > は、次のフォルダです。

C: \ Program Files \ Trend Micro \ Virus Buster 2003

隔離フォルダに移動される際に、感染ファイルは特別なファイル形式に変換されるため、隔離フォルダ内では、感染ファイルを開いたりウイルスが実行されたりすることはありません。隔離フォルダ内のファイルは、手動で削除しない限り隔離フォルダ内に保存されます。

隔離フォルダ内のファイルは、操作画面 (プロフェッショナルモード) の [ウイルス隔離] 画面で処理することができます。

[ウイルス隔離] 画面では、隔離されたファイルをどのように処理をしたらよいかをウィザード形式でアドバイスする [ウイルス処理アシスタント] を利用することができます。[ウイルス処理アシスタント] の詳細については、81 ページを参照してください。

● アクセス拒否 (手動処理)
ウイルスが検出された場合でも、感染ファイルに対して特別な処理は実行されませんが、ファイルに対するアクセスがすべて拒否されます。

感染ファイルを開いたり、コピーしたり、ファイル名を変更するなどの処理がすべてブロックされるので、誤って感染ファイルを開いてしまうことはありません。

● 拡張子変更
ウイルスが検出されると、感染ファイルのファイルの拡張子が「VIR」に変更されます。拡張子を変更することで、誤ってファイルを開いてしまうような事故を防ぐことができます。

拡張子を変更する時に、同じ名前のファイルが既に存在する場合には、「VI0」、「VI1」…「VI9」という拡張子に順次変更されます。

● 削除
ウイルスが検出されると、感染ファイル自体が削除されます。削除されたファイルは、コンピュータの「ごみ箱」に移動されるわけではなく、コンピュータ上から完全に削除されます。

注意 一度削除してしまったファイルは、元に戻すことができませんのでご注意ください。

圧縮ファイルの駆除 (ZIP クリーン)

通常のウイルス検索では、圧縮ファイルに格納されているファイルからウイルスが検出されても、ウイルスを駆除することができません。ウイルスバスター 2003 の ZIP クリーン機能を使えば、ZIP および LZH 形式で圧縮されたファイルに対して、ウイルス駆除を実行することができます。ただし、ウイルス駆除を実行することができるのは、1 回解凍して得られるファイルに対してのみです。

手順:圧縮ファイルからウイルスを駆除できるようにする

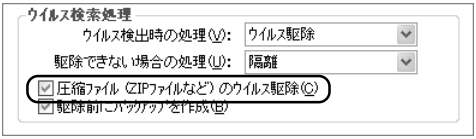
1. [リアルタイム検索設定] 画面の[ウイルス検出時の処理] で「ウイルス駆除」または「削除」が選択されていることを確認してください。

   ウイルス駆除:ウイルス検出時に、圧縮ファイル内の感染ファイルからウイルスコードのみが取り除かれます。

   削除:ウイルス検出時に圧縮ファイル内の感染ファイル自身が削除されます。

注意 [ウイルス検出時の処理] に [アクセス拒否 (手動処理)]、[拡張子変更]、[隔離] が選択されていると ZIP クリーン機能は利用できません。

2. [圧縮ファイル (ZIP ファイルなど) のウイルス駆除] チェックボックスをオンにします。

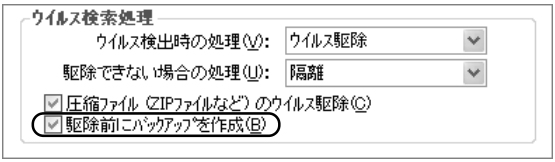


ウイルス検索処理の「圧縮ファイルの駆除」設定

バックアップファイルの作成

ウイルスバスター 2003 では、感染ファイルの駆除処理を実行する前に、ファイルのバックアップを作成するように設定することができます。ウイルス駆除処理中には、感染ファイルが壊れていて復元できなくなったり、複雑なマクロがウイルスと誤認されて削除されてしまう場合があります。ウイルスの駆除処理に「バックアップを作成」オプションを設定しておけば、駆除処理を実行する前のファイルがバックアップフォルダに保存されるので、誤ってデータが失われても元のファイルを取り戻すことができます。

[ウイルス検出時の処理] に「ウイルス駆除」を選択して、[駆除前にバックアップを作成] チェックボックスをオンにしておくと、ウイルス駆除を実行する前に、感染ファイルの拡張子が変更された状態 (RB0、RB1…)でバックアップフォルダに保存されます。バックアップは、次のフォルダに保存されます。



ウイルス検索処理の「バックアップファイル作成」設定

< ウイルスバスター 2003 インストールフォルダ > \ Quarantine \ Backup

通常、< ウイルスバスター 2003 インストールフォルダ > は、次のフォルダです。

C: \ Program Files \ Trend Micro \ Virus Buster 2003

ウイルス駆除に成功しても、バックアップファイルは自動的に削除されません。ウイルス駆除が成功して、バックアップされている元のファイルを削除してもかまわないと判断したら、バックアップファイルを削除してください。バックアップファイルの削除は、操作画面の[ウイルス隔離] 画面から実行することができます。

手動検索

手動検索について

ウイルスバスター 2003 では、必要な時に手動でウイルス検索を実行することができます。手動検索は、次のような場合に実行することをお勧めします。

- ウイルスバスター 2003 のインストール直後、コンピュータ内部にウイルス感染ファイルが潜んでいないかを調べたい。
- ウイルスバスター 2003 を最新版にアップデートするのを、しばらく忘れていた。アップデートしていなかった期間に出現したウイルスに感染していないかを調べたい。
- リアルタイム検索でウイルスが見つかった。他にもウイルスが侵入していないか調べたい。
- リアルタイム検索では、検索対象にされていないファイルがあるので、安全のために、すべてのファイルをウイルス検索しておきたい。

ウイルスバスター 2003 では、手動検索として、次の 3 つの方法を提供しています。

- 全ドライブ検索
- ドライブ / フォルダを指定して検索
- ファイル / フォルダ検索

全ドライブ検索の実行

お使いのコンピュータのすべてのファイルがウイルスに感染していないことを確認するために、すべてのドライブに対してウイルス検索を実行することができます。

全ドライブ検索を実行するには、操作画面のシンプルモードで [全ドライブ検索] をクリックします。クリックと同時に、全ドライブ検索が開始されます。

シンプルモード画面で [全ドライブ検索] ボタンをクリック

[ファイルの検索] 画面で検索の進行状況を表示

全ドライブ検索を停止したい場合には、検索実行中に、[停止] または [一時停止] ボタンをクリックします。

> 注意 全ドライブ検索では、コンピュータのすべてのドライブ内のファイルをウイルス検索します。そのため、検索の実行には数分から数時間程度の時間がかかります。

全ドライブ検索中にウイルスが検出された場合、設定画面の [手動検索設定] 画面で設定された処理が実行されます。

[手動検索設定] 画面の詳細については、57 ページを参照してください。

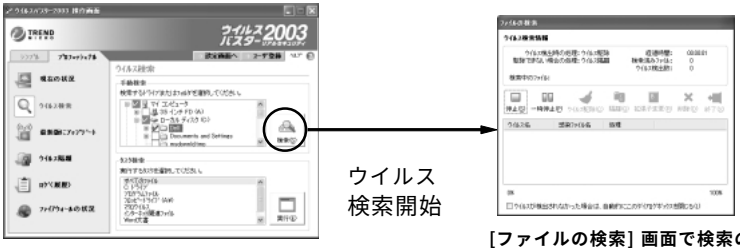
> 注意 全ドライブ検索では、ネットワーク上のマップドライブは検索されません。

ドライブ / フォルダを指定してウイルス検索を実行

お使いのコンピュータの任意のドライブ / フォルダを指定して、ウイルス検索を実行することができます。複数あるドライブを個々に検索したい場合や、特定のディレクトリ以下のフォルダを検索したい場合などに、手動検索を実行してください。

手順：ドライブ / フォルダを指定してウイルス検索を実行する

1. ウイルスバスター 2003 操作画面を表示します。
2. シンプルモードが表示されている場合は、左のタブから [プロフェッショナル] を選択してプロフェッショナルモードに切り替えます。
3. [ウイルス検索] を選択して画面を表示します。
4. [手動検索] のボックスの中に表示されるツリーから、検索したいドライブ / フォルダを選択して、チェックボックスをオン（☑）にします。



ドライブ / フォルダを選択して [検索] ボタンをクリック

[ファイルの検索] 画面で検索の進行状況を表示

次のページにつづく

5. [検索] ボタンをクリックして、手動検索を開始します。

   手動検索を停止したい場合は、[停止] または [一時停止] ボタンをクリックしてください。

> 注意 [手動検索設定] 画面で検索するファイルの種類を指定している場合、選択したドライブ / フォルダに検索対象となる種類のファイルが含まれていない場合には、「検索対象ファイルがありませんでした。」というメッセージが表示されます。

ドライブ / フォルダを指定してウイルス検索中にウイルスが検出された場合、設定画面の [手動検索設定] 画面で設定された処理が実行されます。

[手動検索設定] 画面の詳細については、57 ページを参照してください。

特定のファイル / フォルダにウイルス検索を実行

ウイルスバスター 2003 では、任意のファイル / フォルダに対して簡単にウイルス検索を実行することができます。たとえば受信した e-mail に添付されていた文書ファイルがウイルスに感染していないか確認したい場合など、次のいずれかの方法でウイルス検索を実行することができます。

特定のファイル / フォルダに対してウイルス検索を実行中にウイルスが検出された場合、設定画面の [手動検索設定] 画面で設定された処理が実行されます。

[手動検索設定] 画面の詳細については、57 ページを参照してください。

手順：右クリックでウイルス検索する

1. ウイルス検索を実行したいファイル / フォルダを選択して右クリックします。
2. 表示されるメニューから [ウイルスバスター] を選択します。
3. ウイルスバスターの検索画面が表示され、検索が実行されます。

任意のファイルを右クリックして表示されるメニュー

手順：ファイルをドラッグしてウイルス検索する

1. ウイルスバスター操作画面を表示します。
2. ウイルス検索を実行したいファイル / フォルダを選択して、ウイルスバスター 2003 操作画面上にドラッグします。
3. ウイルスバスター 2003 の検索画面が表示され、検索が実行されます。

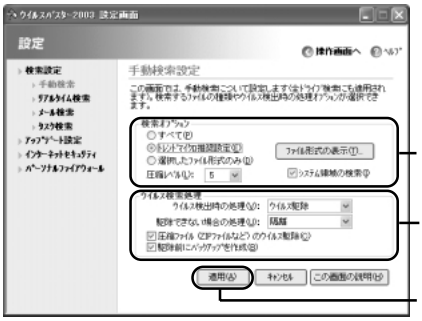
手動検索の詳細設定

[手動検索設定] 画面では、手動検索実行時に検索の対象とするファイルの種類を指定したり、ウイルスが検出された時のウイルス処理方法を設定することができます。

手順：[手動検索設定] 画面を表示する

1. ウイルスバスター 2003 の設定画面を表示します。
2. 設定画面で [検索設定] → [手動検索] を選択して、[手動検索設定] 画面を表示します。

> 注意 [手動検索設定] 画面で設定を変更したら、[適用] ボタンを必ずクリックしてください。[適用] ボタンをクリックしないと、変更した設定は有効になりません。



[手動検索設定] 画面

[手動検索] 画面では、手動検索に関する次の項目について設定することができます。

次のページにつづく

検索対象の選択

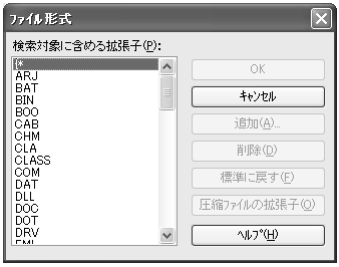
手動検索で検索対象とするファイルの種類を指定することができます。すべてのファイルを検索すると時間が長くかかるため、ウイルスに感染しやすいファイルだけを特定して検索することで、検索時間を短縮することができます。

手動検索では、次の 3 つのオプションを使って、検索するファイルの種類を指定することができます。

● すべて
ファイルの種類にかかわらず、すべてのファイルがウイルス検索されます。これは最も安全なオプションといえますが、安全性と引き換えに検索時間が長くかかります。

● トレンドマイクロ推奨設定
トレンドマイクロが過去の実績や分析をもとにウイルス感染する危険があると判断した種類のファイルが、検索対象に設定されます。推奨設定に含まれるファイルの種類は、ウイルスの発生状況に応じて随時変更されます。

[トレンドマイクロの推奨設定] を選択して、[ファイル形式の表示] ボタンをクリックすると、推奨設定に含まれるファイルの種類の一覧が表示されます。



推奨設定に含まれるファイルの種類の一覧

● 選択したファイル形式のみ
検索したいファイルの種類を自分で指定することができます。

このオプションを選択したら、次の手順に従って検索するファイルの種類を指定します。

手順：検索するファイルの種類を指定する

1. [リアルタイム検索設定] 画面の [ファイル形式の選択] ボタンをクリックします。[ファイル形式] 画面が表示されます。

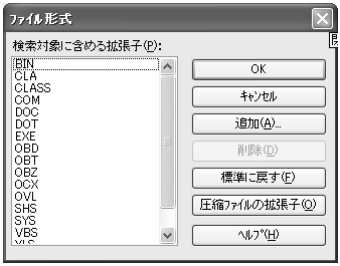
   すでに、いくつかのファイルが検索対象として指定されています。

2. ファイルの種類を追加するには、[追加] ボタンをクリックして、[拡張子の追加] 画面のテキストボックスに拡張子を 1 つずつ入力して、[OK] をクリックします。

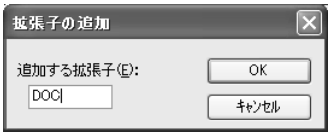
   拡張子リストから特定の拡張子を削除したい場合は、[ファイル形式] 画面で、削除したい拡張子をリストから選択して [削除] ボタンをクリックします。

   [圧縮ファイルの拡張子] ボタンをクリックすると、一般的な圧縮形式で使用される拡張子がまとめて追加されます。

   リストを初期設定の状態に戻したい場合は、[標準に戻す] ボタンをクリックします。



検索するファイルの種類の一覧

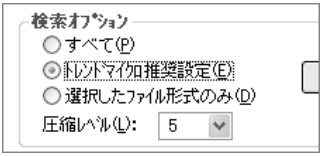


追加する拡張子の入力画面

3. 検索するファイルの種類をすべて指定したら、[OK] ボタンをクリックして [リアルタイム検索設定] 画面に戻ります。

圧縮ファイルの検索

ウイルスバスター 2003 では、ウイルス検索時に圧縮ファイルを自動的に解凍して、ウイルス検索を実行した後、再び圧縮することができます。圧縮ファイルの中には、複数回圧縮されているファイルもあります。[手動検索設定] 画面の [圧縮レベル] では、何回圧縮されたファイルからウイルスを検出するか設定することができます。

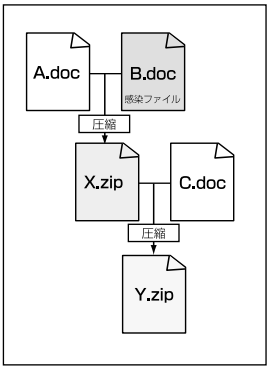


圧縮レベルの設定

たとえば、「A.doc」というファイルとウイルス感染した「B.doc」という 2 つのファイルが「X.zip」というファイルに圧縮されているとします。そして、「X.zip」ファイルと「C.doc」ファイルがさらに、「Y.zip」ファイルに圧縮されているとします。「A.doc」と「B.doc」は 2 回圧縮されていることになります。

この時、[圧縮レベル] が「1」に設定されていると、2 回圧縮されている感染ファイル「B.doc」からウイルスを検出することができません。

[圧縮レベル] が「2」以上に設定されていると、「B.doc」からウイルスを検出することができます。



圧縮ファイルの例

[圧縮レベル] の値を高くすれば、より深い階層の圧縮ファイルからウイルスを検出することができますが、検索に必要な時間も長くなります。

システム領域の検索

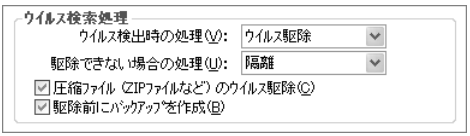
システム領域には、コンピュータの起動に関する大切な情報が保存されており、通常のコンピュータ操作では書き込みなどができないように保護されています。ウイルスバスター 2003 では、手動検索実行時にシステム領域を検索対象に含めることができます。

システム領域感染型ウイルスに感染すると、コンピュータが起動できなくなるなどの危険があります。ウイルスバスター 2003 では、インストール時にシステム領域のウイルス検索を実行しますが、ウイルスバスター 2003 のインストール後に誤ってシステム領域にウイルスが侵入してしまった場合などには、手動検索でシステム領域をウイルス検索することができます。

システム領域を検索対象に含めるには、[手動検索設定] 画面で [システム領域の検索] チェックボックスをオンにしてください。

ウイルス検索処理

手動検索実行中にウイルス感染ファイルが検出された場合の、感染ファイルの処理方法を設定します。



ウイルス検出時の処理設定

● ウイルス駆除 (初期設定)
感染ファイルからウイルスコードのみが取り除かれます。ウイルスの駆除が成功すると、元のファイルは通常のファイルとして使用することができます。

ウイルスの種類によっては、感染ファイルからウイルスを駆除できない場合があります。ウイルスの駆除を選択した場合には、[駆除できない場合の処理] を設定する必要があります。初期設定では、駆除できない場合は「隔離」処理を実行するように設定されています。

● 隔離
ウイルスが検出されると、感染ファイルが次の隔離フォルダに移動されます。

< ウイルスバスター 2003 インストールフォルダ > \ Quarantine

通常、< ウイルスバスター 2003 インストールフォルダ > は、次のフォルダです。

C: \ Program Files \ Trend Micro \ Virus Buster 2003

隔離フォルダに移動される際に、感染ファイルは特別なファイル形式に変換されるため、隔離フォルダ内では、感染ファイルを開いたりウイルスが実行されたりすることはありません。隔離フォルダ内のファイルは手動で削除しない限り隔離フォルダ内に保存されます。

隔離フォルダ内のファイルは、操作画面 (プロフェッショナルモード) の [ウイルス隔離] 画面で処理することができます。

[ウイルス隔離] 画面では、隔離されたファイルをどのように処理をしたらよいかをウィザード形式でアドバイスする [ウイルス処理アシスタント] を利用することができます。[ウイルス処理アシスタント] の詳細については、81 ページを参照してください。

● 放置 (手動処理)
ウイルスが検出された場合、ウイルスログには記録されますが、感染ファイルに対して自動処理は実行されません。

感染ファイルからウイルスを手動で駆除したり、感染ファイルを削除するなどの処理を実行する必要があります。

ウイルス検出時の処理として「放置 (手動処理)」を設定することは推奨しません。誤って感染ファイルを開いてしまわないよう、十分ご注意ください。

● 拡張子変更
ウイルスが検出されると、感染ファイルのファイルの拡張子が「VIR」に変更されます。拡張子を変更することで、誤ってファイルを開いてしまうような事故を防ぐことができます。

拡張子を変更する時に、同じ名前のファイルが既に存在する場合には、「VI0」、「VI1」…「VI9」という拡張子に順次変更されます。

● 削除
ウイルスが検出されると、感染ファイル自体が削除されます。削除されたファイルは、コンピュータの「ごみ箱」に移動されるわけではなく、コンピュータ上から完全に削除されます。

一度削除してしまったファイルは、元に戻すことができませんのでご注意ください。

圧縮ファイルの駆除 (ZIP クリーン)

通常のウイルス検索では、圧縮ファイルに格納されているファイルからウイルスが検出されても、ウイルスを駆除することができません。ウイルスバスター 2003 の ZIP クリーン機能を使えば、ZIP および LZH 形式で圧縮されたファイルに対して、ウイルス駆除を実行することができます。ただし、ウイルス駆除を実行することができるのは、1 回解凍して得られるファイルに対してのみです。

手順:圧縮ファイルからウイルスを駆除できるようにする

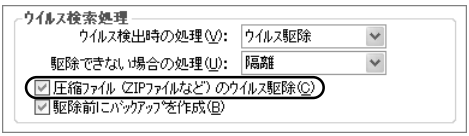
1. [手動検索設定] 画面の[ウイルス検出時の処理] で 「ウイルス駆除」または「削除」が選択されていることを確認してください。

   ウイルス駆除:ウイルス検出時に、圧縮ファイル内の感染ファイルからウイルスコードのみが取り除かれます。

   削除:ウイルス検出時に圧縮ファイル内の感染ファイル自身が削除されます。

注意 [ウイルス検出時の処理] に [放置 (手動処理)]、[拡張子変更]、[隔離] が選択されていると ZIP クリーン機能は利用できません。

2. [圧縮ファイル (ZIP ファイルなど) のウイルス駆除] チェックボックスをオンにします。

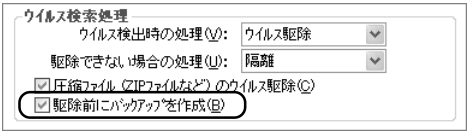


ウイルス検索処理の「圧縮ファイルの駆除」設定

バックアップファイルの作成

ウイルスバスター 2003 では、感染ファイルの駆除処理を実行する前に、ファイルのバックアップを作成するように設定することができます。ウイルス駆除処理中には、感染ファイルが壊れていて復元できなくなったり、複雑なマクロがウイルスと誤認されて削除されてしまう場合があります。ウイルスの駆除処理に「バックアップを作成」オプションを設定しておけば、駆除処理を実行する前のファイルがバックアップフォルダに保存されるので、誤ってデータが失われても元のファイルを取り戻すことができます。

[ウイルス検出時の処理] に「ウイルス駆除」を選択して、[駆除前にバックアップを作成] チェックボックスをオンにしておくと、ウイルス駆除を実行する前に、感染ファイルの拡張子が変更された状態



ウイルス検索処理の「バックアップファイル作成」設定

(RB0、RB1…)でバックアップフォルダに保存されます。バックアップは、次のフォルダに保存されます。

< ウイルスバスター 2003 インストールフォルダ > \ Quarantine \ Backup

通常、< ウイルスバスター 2003 インストールフォルダ > は、次のフォルダです。

C: \ Program Files \ Trend Micro \ Virus Buster 2003

ウイルス駆除に成功しても、バックアップファイルは自動的に削除されません。ウイルス駆除が成功して、バックアップされている元のファイルを削除してもかまわないと判断したら、バックアップファイルを削除してください。バックアップファイルの削除は、操作画面の[ウイルス隔離] 画面から実行することができます。

メールのウイルス検索

メール検索機能とは

ウイルスバスター 2003 のメール検索機能は、インターネット上の受信メールサーバ（POP3）から e-mail をダウンロードする際に、添付ファイルにウイルスが含まれていないかを検索する機能です。また、Web ブラウザを利用して、受信する「Web メール」の添付ファイルからもウイルスを検出することができます。

近年、e-mail を使ったウイルス感染が急増しています。ウイルスバスター 2003 のようなウイルス対策ソフトがインストールされていない環境で、ウイルスに感染した添付ファイルを誤って開いてしまうと、お使いのコンピュータだけでなく他のコンピュータに同様の e-mail を自動送信して感染を広げる悪質なウイルスも流行しています。

急増する e-mail によるウイルス感染からコンピュータを守るためにも、メール検索機能は常に有効にしておくことをお勧めします。初期設定では、メール検索機能が有効に設定されています。ウイルスバスター 2003 が自動的に設定を変更するメールソフトについては、67 ページを参照してください。

ウイルスバスター 2003 では、メール検索機能を有効にするために、インストール時にお使いのメールソフトの設定を自動的に変更しています。ウイルスバスター 2003 インストール時に変更される設定については、19 ページを参照してください。

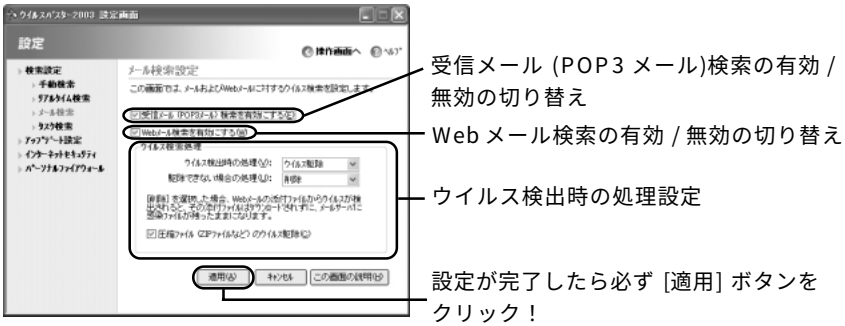
メール検索の詳細設定

[メール検索設定] 画面では、メール検索機能の有効 / 無効の切り替えや、ウイルス検出時の処理方法など、メール検索機能の詳細を設定することができます。

手順：[メール検索設定] 画面を表示する

1. ウイルスバスター 2003 設定画面を表示します。
2. 設定メニューから [検索設定]→[メール検索] を選択して、[メール検索設定] 画面を表示します。

注意 [メール検索設定] 画面で設定を変更したら、[適用] ボタンを必ずクリックしてください。[適用] ボタンをクリックしないと、変更した設定は有効になりません。



[メール検索設定] 画面

[メール検索] 画面では、メール検索に関する次の項目について設定することができます。

受信メール (POP3 メール) 検索の有効 / 無効の切り替え

初期設定では、受信メールに対するウイルス検索は有効に設定されています。メール検索機能を一時的に無効にしたい場合には、[受信メール (POP3 メール) 検索を有効にする] チェックボックスをオフにしてください。

Web メール検索の有効 / 無効の切り替え

初期設定では、Web メールに対するウイルス検索は有効に設定されています。Web メール検索機能を一時的に無効にしたい場合には、[Web メール検索を有効にする] チェックボックスをオフにしてください。

ウイルス検索処理

メール検索実行中にメールの添付ファイルからウイルスが検出された場合の処理方法を設定します。

● ウイルス駆除 (初期設定)
ウイルスに感染していた e-mail の添付ファイルから、ウイルスコードのみが取り除かれます。ウイルスの駆除が成功すると、元のファイルは通常通り e-mail の添付ファイルとして受信します。

ウイルスの種類によっては、感染ファイルからウイルスを駆除できない場合があります。ウイルスの駆除を選択した場合には、[駆除できない場合の処理] を設定する必要があります。初期設定では、駆除できない場合は「削除」処理を実行するように設定されています。

● 放置 (手動処理)
e-mail の添付ファイルからウイルスが検出された場合でも、感染ファイルに対して何の処理も実行されません。受信した e-mail には感染ファイルが添付されたままになっています。

ただし、ウイルスバスター 2003 のリアルタイム検索機能が有効になっていれば、受信した e-mail の添付ファイルを開こうとした時に、リアルタイム検索が実行され、[リアルタイム検索] 設定画面で設定された処理が実行されます。

● 削除
受信メール (POP3 メール) の場合：

添付ファイルからウイルスが検出されると、感染した添付ファイルが削除されて、e-mail本文のみを受信します。受信したe-mailの本文には、ウイルスバスター2003が添付ファイルからウイルスを検出して、感染ファイルを削除したことをお知らせするメッセージが挿入されます。

削除された添付ファイルは、コンピュータの「ごみ箱」に移動されるわけではなく、コンピュータ上から完全に削除されてしまいます。

注意 一度削除してしまったファイルは、元に戻すことができませんのでご注意ください。

Web メールの場合：

Web メールの添付ファイルからウイルスが検出されると、感染したファイルはダウンロードされません。感染ファイルはメールサーバからは削除されずに残ります。

圧縮ファイルの駆除 (ZIP クリーン)

通常のウイルス検索では、圧縮ファイルに格納されているファイルからウイルスが検出されても、ウイルスを駆除することができません。ウイルスバスター 2003 の ZIP クリーン機能を使えば、ZIP および LZH 形式で圧縮されたファイルに対して、ウイルス駆除を実行することができます。ただし、1 回解凍して得られるファイルに対してのみウイルス駆除を実行することができます。

手順：圧縮ファイルからウイルスを駆除できるようにする

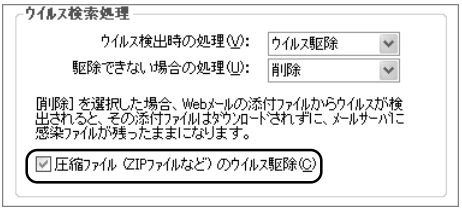
1. [メール検索設定] 画面の[ウイルス検出時の処理] で「ウイルス駆除」または「削除」が選択されていることを確認してください。

   ウイルス駆除：ウイルス検出時に、圧縮ファイル内の感染ファイルからウイルスコードのみが取り除かれます。

   削除：ウイルス検出時に圧縮ファイル内の感染ファイル自身が削除されます。

注意 [ウイルス検出時の処理] に [放置 (手動処理)] が選択されていると ZIP クリーン機能は利用できません。

2. [圧縮ファイル (ZIP ファイルなど) のウイルス駆除] チェックボックスをオンにします。



ウイルス検索処理の「圧縮ファイルの駆除」設定

対応するメールソフト

次のメールソフトをお使いの場合、ウイルスバスター 2003 ではメール検索機能を有効にするために、インストール時にお使いのメールソフトの受信サーバを自動的に「localhost」に変更します。

これにより、メールソフトを使用して e-mail をメールサーバからダウンロードする際に、添付ファイルがウイルス検索されるようになります。

- Microsoft Outlook Express 4.0、5.0、5.5、6.0
- Microsoft Outlook 98、2000、2002
- Netscape Messenger 4.5、4.6、4.7
- Netscape 6.0、6.01、7.0
- Eudora Pro 4.0、4.1、4.2、4.3、5.0
- Becky! Internet Mail ver. 2

注意 メール検索機能のための自動設定に対応するメールの種類やバージョンは変更される場合があります。対応するメールソフトに関する最新の情報は、製品付属の Readme を参照してください。

メールソフトの手動設定

ウイルスバスター 2003 が自動的に設定を変更できないメールソフトをお使いの場合、お使いのメールソフトの設定を手動で変更することで、受信メールの添付ファイルをウイルス検索することができます。

注意 ウイルスバスター 2003 が自動的に設定を変更できないメールソフトは、サポート対象外です。ウイルスバスタークラブセンターでは、メールソフトの手動設定に関するお問い合わせなどは受け付けておりませんので、あらかじめご了承ください。

メールソフトを手動で設定するには、次の手順に従ってください。

次のページにつづく

手順：メールソフトを手動で設定する

1. 接続する POP3 サーバを「localhost」に変更します。

   設定例：　（変更前）mail.xxx.ne.jp

   （変更後）localhost

2. ユーザ名を「実際のユーザ名 / 変更前の POP3 サーバ」に変更します。

   設定例：　（変更前）< ユーザ名 >

   （変更後）< ユーザ名 >/mail.xxx.ne.jp

   * ユーザ名は、通常、e-mail アドレスの @ マークの前の部分です。

メールソフトの設定を変更する方法の詳細については、お使いのメールソフトのマニュアルまたはヘルプを参照してください。

Web メール検索に対応するサービスとブラウザ

ウイルスバスター 2003 の Web メール検索機能は、次のサービスおよびブラウザをお使いの場合、有効になります。

対応するサービス

- AOL メール
- Yahoo!メール
- MSN Hotmail

注意　Microsoft Outlook Express または MSN Explorer を使って Hotmail を受信する場合、Web メールの検索対象にはなりません。

対応するブラウザ

- Microsoft Internet Explorer 4.01 Service Pack 2 以上
- Netscape 6 および 7
- AOL 7.0

タスク検索

タスクとは

ウイルスバスター 2003 では、ウイルス検索する対象やウイルスが見つかった時の対応、ウイルス検索を実行する周期などを、「タスク」と呼ばれるデータに保存しておくことができます。あらかじめタスクを設定しておけば、定期的なウイルス検索を自動的に実行したり、複雑な検索条件も 1 度設定してしまえば、何度でも同じ条件で検索させることもできます。

初期設定のウイルスバスター 2003 には、さまざまな条件でウイルス検索を実行できるタスクが設定されています。

タスクは [検索タスク設定] 画面で自由に追加したり、変更したり、削除したりすることができます。また、保存している「タスク」の有効 / 無効を簡単に切り替えることもできます。

注意 複数のタスクを定期的に実行するように設定する場合は、実行する日時に注意してください。複数のタスクが同一日時に設定された場合、最初に起動されたタスクのみが有効になり、その他のタスクは実行されません。

注意 お使いのコンピュータの電源が入っていない場合、コンピュータがスタンバイ / 休止状態の場合、ログオフ状態の場合などは、タスク検索が実行されません。

タスク検索の実行

ウイルスバスター 2003 操作画面（プロフェッショナルモード）の [ウイルス検索] 画面では、あらかじめ設定された「タスク」を選択して、手動でタスク検索を実行することができます。

手順：タスク検索を実行する

1. ウイルスバスター 2003 操作画面を表示します。
2. シンプルモードが表示されている場合は、左のタブから [プロフェッショナル] を選択してプロフェッショナルモードに切り替えます。
3. [ウイルス検索]をクリックします。

次のページにつづく

4. [タスク検索] のボックスの中に表示されるリストから、実行したいタスクを選択します。初期設定で、いくつかのタスクが設定されています。

5. タスクを選択したら、[実行] ボタンをクリックします。選択されたタスク検索がすぐに実行されます。

タスクを選択して、[実行] ボタンをクリック

ウイルス検索開始

[ファイルの検索] 画面で検索の進行状況を表示

6. タスク検索を停止したい場合は、[停止] または [一時停止] ボタンをクリックしてください。

タスクの編集

[タスク検索設定] 画面で、タスクを自由に追加したり、変更したり、削除したりすることができます。

手順：[タスク検索設定] 画面を表示する

1. ウイルスバスター 2003 設定画面を表示します。
2. 設定メニューから [検索設定] → [タスク検索] を選択して、[タスク検索設定] 画面を表示します。

[タスク検索設定] 画面には、現在設定されているタスクの一覧が表示されます。

[タスク検索設定] 画面

新しい検索タスクの追加

検索対象や検索時刻を指定して、独自の検索タスクを作成することができます。

手順：新しい検索タスクを追加する

1. [タスク検索設定] 画面の 追加(A) [追加] ボタンをクリックします。[タスク設定] 画面が表示されます。
2. [検索対象の選択]、[検索オプションの選択]、[スケジュール]のそれぞれの画面で必要な項目を設定します。

   各画面の設定項目の詳細については、73 ページを参照してください。
3. 設定が完了したら、[OK] ボタンをクリックします。[タスク検索設定] 画面に戻ります。

[タスク検索設定] 画面のタスク一覧に、追加した検索タスクが表示されていることを確認してください。

検索タスクの編集

すでに設定されているタスクを編集して、検索対象、ウイルス検出時の処理方法、検索周期などを変更することができます。

手順：既存の検索タスクを編集する

1. [タスク検索設定] 画面で、編集したい検索タスクをクリックして選択します。
2. 編集(E) [編集] ボタンをクリックします。 選択したタスクが設定されている [タスク設定] 画面が表示されます。
3. [検索対象の選択]、[検索オプションの選択]、[スケジュール]のそれぞれの画面で必要な項目を変更します。

   各画面の設定項目の詳細については、73 ページを参照してください。
4. 設定の変更が完了したら、[OK] ボタンをクリックします。[タスク検索設定] 画面に戻ります。

[タスク検索設定] 画面のタスク一覧に、変更した検索タスクが表示されていることを確認してください。

不要なタスクの削除

不要になったタスクを削除することができます。

注意 削除したタスクは元に戻すことはできません。

手順：不要になったタスクを削除する

1. [タスク検索設定] 画面で、削除したいタスクをクリックして選択します。
2. 削除(D) [削除] ボタンをクリックします。
3.「選択したタスクを削除してよろしいですか？」という確認メッセージが表示されるので、タスクを削除する場合には、[はい] をクリックします。

[タスク検索設定] 画面のタスク一覧から、削除したタスクがなくなっていることを確認してください。

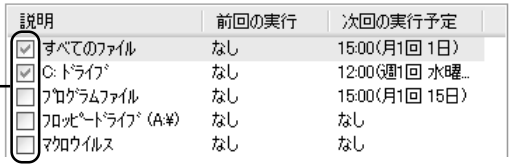
タスクの有効 / 無効を切り替える

一度設定したタスクを削除せずに一時的に無効にすることができます。無効になったタスクは、予定された日時になっても実行されることはありません。

手順：タスクの有効 / 無効を切り替える

[タスク検索設定] 画面に表示されている各タスク名の前にあるチェックボックス(☐)のオン / オフを切り替えることで、それぞれのタスクの有効 / 無効を切り替えることができます。

検索タスクのオン / オフを切り替えます



オン(☑)：タスクは有効です。指定した日時になると、タスクが実行されます。

オフ(☐)：タスクは無効です。指定した日時になっても、タスクは実行されません。

タスク設定の詳細

[タスク設定] 画面は次の 3 つの画面で構成されています。それぞれの画面を表示するには、画面上部のタブをクリックします。

- 検索対象の選択
- 検索オプションの選択
- スケジュール

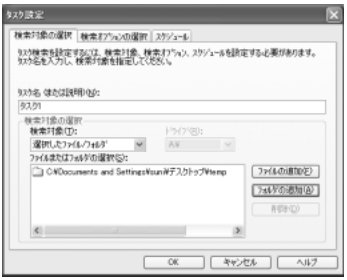
次のページにつづく

検索対象の選択

[検索対象の選択] 画面で、検索タスクに適切な名前を付けたり、検索タスクが実行された時に検索するドライブ、フォルダ、ファイルを指定することができます。

● タスク名

追加 / 編集するタスクに適当な名前を設定します。ウイルスバスター 2003 操作画面のプロフェッショナルモードで [ウイルス検索] ボタンをクリックした時に表示される、タスク一覧に表示されます。タスクの内容が一目でわかるような名前をつけることをお勧めします。



検索タスク設定の[検索対象の設定] 画面

● 検索対象

[全ドライブ]、[選択したドライブ]、[選択したファイル / フォルダ] から選択します。検索対象を指定することで、より詳細な検索を設定することができます。

たとえば、特定のフォルダにファイルを保存して、そのフォルダに対して、定期的にウイルス検索を実行して、ウイルスに感染していないかどうかを確認することができます。

● ドライブ

[検索対象] で [選択したドライブ] を選択した場合に、検索するドライブをリストボックスから選択してください。

● ファイルの追加

[検索対象] で [選択したファイル / フォルダ] を選択した場合に、検索対象のファイルを選択します。このボタンをクリックすると、ファイルを選択する画面が表示されます。検索対象にしたいファイルを選択して [OK] ボタンをクリックします。選択したファイルが、[ファイルまたはフォルダの選択] 一覧に表示されます。

選択したファイルを対象から外すには、ファイルを一覧から選択して、[削除] ボタンをクリックしてください。

● **フォルダの追加**

[検索対象] で [選択したファイル / フォルダ] を選択した場合に、検索対象のフォルダを選択します。このボタンをクリックすると、フォルダを選択する画面が表示されます。検索対象にしたいフォルダを選択して [OK] ボタンをクリックします。選択したフォルダが、[ファイルまたはフォルダの選択] 一覧に表示されます。

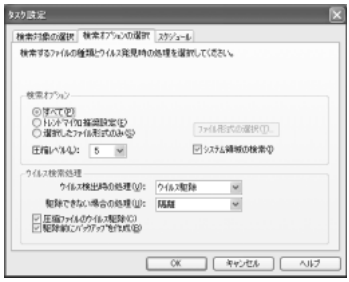
検索対象のフォルダにドライブを選択すると、複数のドライブを同時に検索することができます。

選択したフォルダを対象から外すには、フォルダを一覧から選択して、[削除] ボタンをクリックしてください。

検索オプションの選択

[検索オプションの選択] 画面では、タスク実行中にウイルスが検出された場合の処理方法や、検索対象とするファイルの種類を設定することができます。

この画面での設定内容は、[手動検索設定] 画面と全く同じです。[検索オプションの選択] 画面の詳細については、57 ページの [手動検索設定]画面の詳細を参照してください。



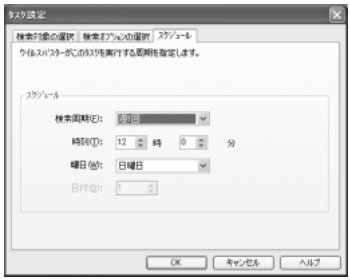
検索タスク設定の[検索オプションの選択] 画面

スケジュール

タスク検索を実行する周期を次のいずれかから選択します。

● なし (初期設定)

[なし] を選択すると、タスクは自動的に実行されません。設定したタスクは、ウイルスバスター 2003 操作画面から手動で実行することができます。タスクを実行するには、操作画面のプロフェッショナルモードで [ウイルス検索] ボタンを選択して表示される画面で、タスクを選択して [実行] ボタンをクリックします。



検索タスク設定の[スケジュール] 画面

● 毎日

[毎日] を選択したら、[時刻] で検索を開始する時刻を指定してください。指定された時刻になると、タスク検索が毎日実行されます。

例：

[時刻] ： [9] 時 [10] 分と指定すると ...

午前 9 時 10 分になると、毎日検索が開始されます。

● 週 1 回

[週 1 回] を選択したら、[曜日] でタスクを実行する曜日を選択してください。また、[時刻] でタスクを開始する時刻を指定してください。

例：

[時刻]:[9] 時 [10] 分

[曜日]:[日曜日]と指定すると ...

毎週日曜日の午前 9 時 10 分になると、検索が開始されます。

● 月 1 回

[月 1 回] を選択したら、[日付] でタスクを実行する日を選択してください。また、[時刻] でタスクを開始する時刻を指定してください。

例：

[時刻]:[9] 時 [10] 分と指定すると ...

[日付]:[1]

毎月 1 日の午前 9 時 10 分になると、検索が開始されます。

[日付] を「31」に設定すると、30 日または 28 日 (うるう年では 29 日) までの月では、そのタスクは実行されません。

タスクに関するすべての設定が完了したら、[タスク設定] 画面で [OK] ボタンをクリックすると、タスクが追加または変更されます。

第 5 章 ウイルスが見つかったら

ウイルスバスター 2003 では、リアルタイム検索が有効に設定されていれば、お使いのコンピュータ上でファイルが開いたり、保存されたり、移動されるたびにウイルス検索が実行されます。また、手動検索やタスク検索機能を使って、特定のファイルやフォルダに対して、手動でウイルス検索を実行することができます。

では、ウイルスバスター 2003 がウイルスを見つけた場合、どうすればよいのでしょう？

この第 5 章では、ウイルスが見つかった場合の対処方法について説明します。

ウイルスが見つかったら？

リアルタイム検索中にウイルスが見つかったことを知るには

リアルタイム検索実行中に、ウイルスが検出されると、「ウイルスが見つかりました！」という警告が表示されます。

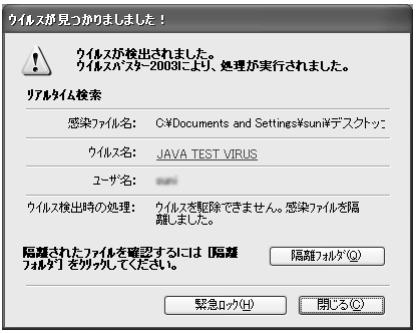
この警告では、次の情報を確認することができます。

■ 感染ファイル名

ウイルスが検出されたファイル名が表示されます。

■ ウイルス名

検出されたウイルスの名前が表示されます。ウイルス名をクリックしてインターネット上の情報ページから、検出されたウイルスについての情報を参照することができます。



リアルタイム検索中にウイルスが検出された時の警告画面

■ ウイルス検出時の処理

ウイルス感染ファイル対して、実行された処理とその結果が表示されます。

初期設定のリアルタイム検索では、ウイルスが見つかった場合に「ウイルス駆除」が実行されます。また、駆除できないウイルスに感染していた場合、感染ファイルは「隔離」されます。

ウイルスが駆除された場合には、次のメッセージが表示されます。

「ウイルスを駆除しました。」

ウイルスを駆除できずに、感染ファイルを隔離した場合には、次のメッセージが表示されます。

「ウイルスを駆除できません。感染ファイルを隔離しました。」

■ 緊急ロックボタン

[緊急ロック] ボタンをクリックして、インターネットを含むすべてのネットワークから瞬時に切断することができます。ネットワークから切断することで、他のコンピュータにウイルスをばらまいてしまう危険を回避することができます。

ウイルスバスター 2003 のパーソナルファイアウォールがインストールされていない場合には、このボタンは表示されません。

■ 隔離フォルダボタン

感染ファイルが隔離された場合に、このボタンが表示されます。この [隔離フォルダ] ボタンをクリックすると、ウイルスバスター 2003 操作画面の [ウイルス隔離] 画面が表示されます。[ウイルス隔離] 画面の「ウイルス処理アシスタント」を利用して、隔離されたウイルスを手動で処理する手順を確認することができます。

メール検索でウイルスが見つかったことを知るには

初期設定では、メール検索実行時にウイルスが検出された場合の処理は、「ウイルス駆除」に設定されています。初期設定のままお使いいただいている場合、メール検索実行中に、ウイルスが検出されると、「ウイルスが見つかりました！」という警告が表示されます。

この警告では、次の情報を確認することができます。

■ 件名

添付ファイルからウイルスが検出された e-mail の件名が表示されます。

■ ウイルス名

検出されたウイルスのウイルス名が表示されます。ウイルス名をクリックしてインターネット上のウイルス情報ページから、検出されたウイルスについての情報を参照することができます。

メール検索中にウイルスが検出された時の警告画面

■ 送信者

ウイルスが検出された e-mail の送信者名とメールアドレスが表示されます。

■ ウイルス検出時の処理

検出されたウイルスに対して、実行された処理とその結果が表示されます。

初期設定のメール検索では、ウイルスが見つかった場合に「ウイルス駆除」が実行されます。また、駆除できないウイルスに感染していた場合、感染ファイルは「削除」されます。

ウイルスが駆除された場合には、次のメッセージが表示されます。

「ウイルスを駆除しました。」

ウイルスを駆除できずに、感染ファイルを削除した場合には、次のメッセージが表示されます。

「メールまたは添付ファイルからウイルスを駆除できませんでした。感染ファイルを削除しました。」

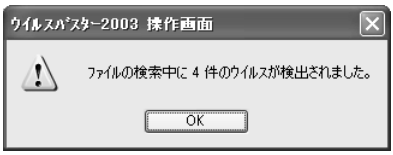
■ 緊急ロックボタン

[緊急ロック] ボタンをクリックして、インターネットを含むすべてのネットワークから瞬時に切断することができます。ネットワークから切断することで、他のコンピュータにウイルスをばらまいてしまう危険を回避することができます。

注意 ウイルスバスター 2003 のパーソナルファイアウォールがインストールされていない場合には、このボタンは表示されません。

手動 / タスク検索中にウイルスが見つかったことを知るには

手動 / タスク検索を開始すると [ファイルの検索] 画面が表示されます。手動検索実行中にウイルスが検出されると、「ファイル検索中に x 件のウイルスが検出されました」というメッセージが表示されます。[ファイルの検索] 画面には、検出されたウイルス、感染ファイル、および処理結果に関する情報が表示されます。



手動検索 / タスク検索中にウイルスが検出された場合のメッセージ

手動検索 / タスク検索中に検出されたウイルス情報

[ファイルの検索] 画面では、感染ファイルを隔離フォルダに移動したり、削除したり、拡張子を変更するなどの処理を実行することができます。

ウイルスを駆除できない場合はどうすればいいの？

初期設定のウイルスバスター 2003 では、リアルタイム検索または手動検索実行中にウイルスが検出された場合は、**「ウイルス駆除」**の処理が実行されます。感染ファイルが何重にも圧縮されている場合や、パスワード保護されている場合などは、ウイルスバスター 2003 では駆除処理を実行することができません。この場合、感染ファイルは**「隔離」**されます。

「隔離」処理によって隔離されたファイルは、ウイルスバスター 2003 のインストールフォルダ以下の隔離フォルダ (**Quarantine** フォルダ) に移動されます。感染ファイルが隔離される際には特別なファイル形式に変換されるため、隔離フォルダ内では感染ファイルのウイルスが実行されることはありません。

ウイルスバスター 2003 操作画面のプロフェッショナルモードから [ウイルス隔離] 画面を表示すれば、隔離フォルダ内のファイルを確認することができます。

隔離された感染ファイルをそのままにしておいても、ウイルスに感染する危険はありません。隔離されたファイルを元の場所に戻したい、必要がないので削除したいなど、何らかの処理を実行したい場合には、[ウイルス隔離] 画面から処理を実行することができます。

また、ウイルスバスター 2003 が対応していない新しいウイルスに感染している場合は、そのウイルスに対応したパターンファイルや検索エンジンが公開されるのを待って、最新版のウイルスバスター 2003 にアップデートしてから処理することもできます。万一システムファイルなどに駆除できないウイルスが感染してしまった場合などは、誤ってファイルを削除してしまうと、コンピュータが起動しないなどのトラブルの原因にもつながります。隔離フォルダ内のファイルは、慎重に処理することをお勧めします。

[ウイルス隔離] 画面から参照することができる「ウイルス処理アシスタント」を利用して、隔離されたファイルに適した処理方法を実行してください。

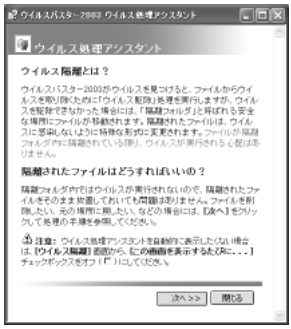
手順：ウイルス処理アシスタントを参照する

1. ウイルスバスター 2003 操作画面を表示します。
2. シンプルモードが表示されている場合は、左のタブから [プロフェッショナル] を選択してプロフェッショナルモードに切り替えます。
3. [ウイルス隔離] ボタンをクリックして画面を表示します。

   [この画面を表示するたびに [ウイルス処理アシスタント] を表示する] チェックボックスがオンになっていると、[ウイルス隔離] 画面が表示されると同時に、「ウイルス処理アシスタント」が表示されます。

   自動的に表示されない場合には、画面右下の [ウイルス処理アシスタント] ボタンをクリックします。

[ウイルス隔離] 画面

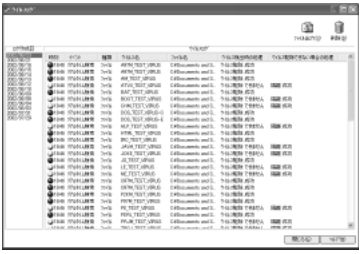


ウイルス処理アシスタント

ウイルスログを参照する

ウイルスバスター 2003 では、検出されたウイルスに関する情報を「ウイルスログ」に記録します。ウイルスログを参照して、検出されたウイルスのウイルス名、感染ファイル名、感染ファイルに対して実行された処理などを確認することができます。

ウイルスログでは、次の情報が表示されます。



ウイルスログの例

- 時刻：ウイルスが検出された時刻が表示されます。
- イベント：ウイルス検索時に実行されていた検索の種類が表示されます。
- 種類：ウイルスが検出された対象 (ファイル /e-mail/Web) が表示されます。
- ウイルス名：検出されたウイルスの名前が表示されます。
- ファイル名：ウイルスが検出されたファイルの「ファイル名」または「e-mailの件名」が表示されます。
- ウイルス検出時の処理：感染ファイルに対して実行された処理とその結果が表示されます。
- ウイルス駆除できない場合の処理：感染ファイルの処理を「ウイルス駆除」に設定している場合に、ウイルス駆除できない感染ファイルに対して実行された処理とその結果が表示されます。

ウイルスログの表示方法、ログをファイルに出力する方法、およびウイルスログの削除方法については、41 ページを参照してください。

トレンドマイクロが提供する情報を参照する

ウイルスデータベースでウイルスに関する情報を調べる

トレンドマイクロでは、これまでに収集したウイルスに関する膨大なデータベースを、一般に公開しています。ウイルスデータベースの Web ページへは、ウイルスバスター 2003 の画面から直接アクセスすることができます。特定のウイルスについて調べたい場合は、ウイルスデータベースを活用してください。

このデータベースには、個々のウイルス別に、ウイルス感染の危険性や感染時の症状、駆除方法などが掲載されています。ウイルス名 (または別名) やキーワード、ウイルスの種類などを条件にデータベースを検索することができます。トレンドマイクロでは、新しく発見されたウイルスに関する情報を、このデータベースに追加しています。

手順：ウイルスデータベースにアクセスする

1. ウイルスバスター 2003 の操作画面または設定画面を表示します。
2. 画面右上のヘルプボタンをクリックします。
3. 表示されたメニューから [ウイルスデータベース] を選択します。

   Web ブラウザが起動し、ウイルスデータベースの Web ページが表示されます。

ヘルプメニューから [ウイルスデータベース] を選択

注意 ウイルスデータベースの Web ページにアクセスするには、インターネット接続が必要です。インターネット接続に伴う通信料金は、お客さまの負担となります。

最新のウイルス情報を調べる

トレンドマイクロでは、コンピュータウイルスの最新情報を一般に公開しています。最新のウイルス情報の Web ページへは、ウイルスバスター 2003 の画面から直接アクセスすることができます。

最新ウイルス情報の Web ページには、感染被害が拡大しているウイルスに関する警告情報や、週間ウイルス被害ランキング、デマウイルスの情報など、役立つ情報が掲載されています。定期的にアクセスして、ウイルスの流行状況を確認しておきましょう。

手順：最新のウイルス情報にアクセスする

1. ウイルスバスター 2003 の操作画面または設定画面を表示します。
2. 画面右上のヘルプボタンをクリックします。
3. 表示されるメニューから [最新ウイルス情報] を選択します。

   Web ブラウザが起動し、最新ウイルス情報の Web ページが表示されます。

ヘルプメニューから [最新ウイルス情報] を選択

注意 ウイルスデータベースの Web ページにアクセスするには、インターネット接続が必要です。インターネット接続に伴う通信料金は、お客さまの負担となります。

救済ディスクについて

注意 救済ディスクを使ったウイルス駆除は、Windows 98/Me でのみお使いいただける機能です。Windows NT/2000/XP 環境では、救済ディスクを作成することができません。

「救済ディスク」は、ウイルスバスター 2003 では駆除することができないウイルスに感染した場合に使用するフロッピーディスクです。次のような場合に、ウイルスバスター 2003 ではウイルスを駆除することができません。

■ システム領域感染型ウイルスに感染した場合

ウイルスバスター 2003 はシステムが起動してはじめて機能するため、システム領域に感染してしまったウイルスは、別の方法で駆除する必要があります。

コンピュータのシステム領域にウイルスが感染した場合、コンピュータを起動するたびにウイルスが活動を開始してしまいます。あらかじめ「救済ディスク」を作成して、コンピュータを起動するための情報と、ウイルスを駆除するためのプログラムを格納しておく必要があります。

■ OS が常に使用しているファイルにウイルスが感染した場合

ウイルスバスター 2003 では、OS が常に使用しているファイルからウイルスを駆除することができません。この場合、「救済ディスク」を使用して、ウイルスを駆除する必要があります。

救済ディスクは、ウイルスに感染していない状態で作成する必要がありますので、ウイルスバスター 2003 をインストールし、最新版にアップデートして、全ドライブ検索を実行した直後に作成することをお勧めします。

注意 Windows NT/2000/XP では、システム領域感染型ウイルスに感染しても、ウイルスとして活動することができないため、危険はありません。Windows NT/2000/XP では、OS ごとにシステムを復旧する方法が用意されています。各 OS でのシステム復旧方法については、OS 付属のマニュアルまたはオンラインヘルプを参照してください。

注意 旧バージョンのウイルスバスターで作成した救済ディスク、他のコンピュータで作成した救済ディスクは使用できません。また、OS のアップグレードなど、システムに変更を加えた場合も、救済ディスクを作成し直す必要があります。不適切な救済ディスクを使用すると、システムに重大な損傷を与えることになり、ハードディスクにアクセスできなくなりますのでご注意ください。

救済ディスクの作成 (Windows 98/Me をお使いの場合のみ)

救済ディスクの作成には、2HD のフロッピーディスクが 7 枚 (※) 必要です。あらかじめご用意ください。

注意 救済ディスクの作成と、救済ディスクを使ったウイルス駆除は、Microsoft Windows 98/Me でのみご利用いただける機能です。

※ フロッピーディスクの枚数が増える場合があります。正確な枚数については、救済ディスク作成時に表示される [救済ディスクの作成] 画面を参照してください。

手順：救済ディスクを作成する

1. Windows の [スタート] メニューから、[プログラム]→ [トレンドマイクロ ウイルスバスター 2003] → [救済ディスク作成] の順に選択してください。
2. [救済ディスクを作成しますか] というメッセージが表示されます。[はい] をクリックしてください。

   救済ディスクの作成プログラムが実行されない場合は、次のフォルダを参照して「Rescue.exe」を実行してください。

   C:\Program Files\Trend Micro\Virus Buster 2003\Rescue

3. [救済ディスクの作成] 画面が表示されます。[すべて] オプションを選択して、[次へ]ボタンをクリックしてください。

4. フロッピーディスクへファイルのコピーが開始されます。フロッピーディスクを 7 枚用意してください。

5. まず 1 枚目のフロッピーディスクをフロッピーディスクドライブに挿入します。画面の [作成先ドライブを選択してください。] で、フロッピーディスクドライブを選択して、[次へ] をクリックします。

6. ファイルをフロッピーディスクにコピーする前に、フロッピーディスクを初期化する必要があります。フロッピーディスクを初期化すると、保存されているデータはすべて削除されますのでご注意ください。初期化形式には、[クイックフォーマット] または [通常のフォーマット] のどちらかを選択してください。フロッピーディスクの初期化が終了したら、[閉じる] をクリックしてください。

7. ファイルがフロッピーディスクにコピーされます。コピーが終了すると、メッセージが表示されますので、フロッピーディスクをフロッピーディスクドライブから取り出してください。

8. 取り出した 1 枚目のフロッピーディスクラベルに**「起動用ディスク」**と記入してください（ラベル名はわかりやすい内容で自由にご記入ください）。

9. 2 枚目のフロッピーディスクをフロッピーディスクドライブに挿入してください。手順 7 と同様にフロッピーディスクを初期化し、初期化が終了したら [閉じる] ボタンをクリックしてください。

10. ファイルがフロッピーディスクにコピーされます。コピーが終了すると、メッセージが表示されます。フロッピーディスクをフロッピーディスクドライブから取り出してください。

11. 取り出した 2 枚目のフロッピーディスクラベルに**「検索用ディスク」**と記入してください（ラベル名はわかりやすい内容で自由にご記入ください）。

12. 3 ～ 7 枚目のフロッピーディスクを、手順 5 ～ 7 の要領で作成します。作成されたフロッピーディスクのラベルには、それぞれ**「パターン用ディスク 1」**、**「パターン用ディスク 2」**、**「パターン用ディスク 3」**、**「パターン用ディスク 4」**、**「パターン用ディスク 5」**と順番に記入してください。

パターンファイル用のフロッピーディスクの作成が終了したら、救済ディスクの作成手順は完了です。作成した救済ディスクは、大切に保管してください。

救済ディスク作成手順で作成するパターンファイル用のフロッピーディスクには、救済ディスク作成時にウイルスバスター 2003 に含まれているバージョンのパターンファイルが収録されます。ウイルスバスター本体のパターンファイルが更新された場合、救済ディスクも更新することをお勧めします。

注意

救済ディスクを使ってウイルスを駆除する

ウイルスバスター 2003 のウイルス駆除機能では、システム領域感染型ウイルスを駆除することができません。ただし、ウイルスに感染していない環境で、あらかじめ救済ディスクを作成しておけば、救済ディスクを使用してシステム領域感染型ウイルスを駆除することができます。

救済ディスクの作成と、救済ディスクを使ったウイルス駆除は、Windows 98/Me でのみご利用いただける機能です。Windows NT/2000/XP をご利用の場合は、各 OS のシステム修復機能を使って、システム領域を復旧することができます。詳しくは、OS 付属のマニュアルまたはオンラインヘルプを参照してください。

注意

旧バージョンのウイルスバスターで作成した救済ディスク、他のコンピュータで作成した救済ディスクは使用できません。また、OS のアップグレードなど、システムに変更を加えた場合も、救済ディスクを作成し直す必要があります。不適切な救済ディスクを使用すると、システムに重大な損傷を与えたり、ハードディスクにアクセスできなる場合がありますのでご注意ください。

注意

手順：救済ディスクを使ってウイルスを駆除する

1. システム領域感染型ウイルスに感染したコンピュータの電源を切ります。
2. 救済ディスクの作成手順で 1 枚目に作成した**「起動用ディスク」**をフロッピーディスクドライブに挿入します。
3. コンピュータの電源を入れます。コンピュータは起動用ディスクを使用して起動されます。
4. 救済ディスクの作成手順で 2 枚目に作成した**「検索用ディスク」**をフロッピーディスクドライブに挿入します。
5. DOS プロンプトが開始されます。画面に次のように入力してください。

   vbscan /v /c

6. **<Enter>** キーを押します。
7. 画面にメッセージが表示されたら、救済ディスクの作成手順で 3 枚目に作成した**「パターン用ディスク 1」**をフロッピーディスクドライブに挿入して、**<Enter>** キーを押します。
8. 次のパターンファイル用ディスクを挿入するようメッセージが表示されたら、**「パターン用ディスク 2」**、**「パターン用ディスク 3」**、**「パターン用ディスク 4」**、**「パターン用ディスク 5」**のフロッピーディスクを順次挿入して、**<Enter>** キーを押します。
9. システム領域を含むすべてのドライブのウイルス検索が終了したら、メッセージが表示されます。これで手順は完了です。

第 6 章 最新版へのアップデート

ウイルスバスター 2003 では、ウイルスパターンと呼ばれる、ウイルスの「指紋」を使って、コンピュータに入り込んだウイルスを識別して、駆除します。

ウイルスは日々作成され、増殖しています。新しいウイルスに対応するためには、このウイルスパターンを常に最新の状態にしておく必要があります。

第 6 章では、まずウイルスとは何かを解説し、ウイルス感染を防ぐための方法ついて説明します。

ウイルスとは

コンピュータウイルスとは？

コンピュータウイルスとは、心ない人間によって意図的に作成された不正プログラムの一種です。その動作が自然界のウイルスに似ていることから、コンピュータウイルスと呼ばれるようになりました。コンピュータウイルスは、自然に発生することはなく、必ず感染源が存在します。

コンピュータウイルスは、e-mail のやりとりや、インターネット上からのファイルのダウンロード、他のコンピュータとのデータ共有、フロッピーディスクや MO ディスクを媒介にしたデータの受け渡しなどを通じて、感染が広がります。

コンピュータウイルスに感染してしまうと、e-mail が勝手に送信される、ハードディスク内のデータが破壊される、外部からコンピュータを操作される、システムが不安定になる、不審なメッセージが画面に表示されるなどの症状が起こります。

コンピュータウイルスの定義

コンピュータウイルスの定義は、ウイルス対策ソフトウェアのメーカーや関係機関によってさまざまな解釈がありますが、一般的には次の行動パターンを持つ不正プログラムをコンピュータウイルスと呼んでいます。

■ **感染**：他のファイルにウイルス自身を付着させる

■ **潜伏**：一定の条件がそろうのを待って悪質な行動をする

■ **発病**：データの破壊、動作の不安定などユーザの意図しない行動をする

また、他のプログラムに感染（寄生）する習性を持たず、プログラム自身がユーザの意図しない行動をする不正プログラムがあります。これらは「ワーム」、「トロイの木馬」などと呼ばれ、本来のウイルスの定義からは外れますが、トレンドマイクロではウイルスと同様に、コンピュータに被害をもたらすものとして、対策を提供しています。

ウイルスに感染しないために

ウイルス対策ソフトウェアを正しく使う

せっかくウイルス対策製品をインストールしても、正しく使用しないと、効果的なウイルス対策を実現することができません。

新しいウイルスは日々作成され、増殖しています。トレンドマイクロでは、新しく発見されるウイルスを解析し、定期的にウイルスパターンファイルを提供しています。最新のウイルスからお使いのコンピュータを守るためには、ウイルスバスター 2003 を常に最新版にアップデートする必要があります。

ウイルスの感染経路を知る

ウイルスはさまざまな経路でコンピュータに感染します。ウイルスの感染経路を知ることは、ウイルス感染を未然に防ぐ上で非常に大切です。

ここでは、ウイルスが侵入しやすい 3 つの主要な感染経路について説明します。

■ e-mail によるウイルス感染

e-mail によって送られるウイルスには、お使いのパソコンに感染してデータを破壊したり、メールソフトに登録されている複数の相手にウイルス付きの e-mail を送ってしまうものなどがあります。添付されたファイルを開く前のウイルスチェックが非常に重要です。

■ インターネット経由でダウンロードしたプログラムからの感染

インターネットにアクセスして、無料ソフトや体験版ソフトをダウンロードしてプログラムを実行した途端、ウイルスに感染してしまうなどの危険があります。ダウンロードしたプログラムを実行する前のウイルスチェックが非常に重要です。

■ フロッピーディスクなどの外部媒体からの感染

フロッピーディスク、MO ディスクなどの記録媒体は、ウイルスに感染している危険が潜んでいます。データのやりとりにこのような記録媒体をお使いになる場合は、ウイルスに感染していないか、事前にチェックする必要があります。

ウイルスバスター 2003 のリアルタイム検索が有効に設定されていれば、前述の主要なウイルス感染経路は、コンピュータ起動時に常に監視されています。ウイルスの侵入を防ぐためにも、常にウイルスバスター 2003 のリアルタイム検索機能を有効に設定することを強くお勧めします。リアルタイム検索については、46 ページを参照してください。

ウイルスパターンファイルとアップデート

コンピュータウイルスには、人間の指紋のようにウイルスごとに特有の特徴があり、これを**「ウイルスパターン」**と呼んでいます。ウイルスパターンファイルは、このウイルスの「指紋」を集めたデータベースです。

ウイルスバスター 2003 では、コンピュータ上で読み込み / 書き込みされるファイルを監視して、ウイルスパターンファイルに含まれるウイルスの「指紋」に一致する情報が含まれていないかを確認します。一致する情報が見つかった場合は、ウイルスに対する処理が実行されます。しかし、データベースに追加されていない、まったく新しいタイプのウイルスに感染した場合、ウイルス感染を見逃してしまう危険性があります。

トレンドマイクロでは、新しいコンピュータウイルスが発見されるたびに、そのウイルスがまん延する前に、ウイルスのパターン（指紋）をウイルスパターンファイル（データベース）に追加し、新しいパターンファイルとして提供しています。ウイルスバスターをお買い上げいただいた後も常に新しく発見されたウイルスを検出できるようにしておくためには、ウイルスバスター 2003 に組み込まれているパターンファイルを、常に最新版にアップデートしていくことが大切なのです。

パターンファイル（データベース）と同じように、検索エンジンやプログラムも、さらにウイルスを正確に検出できるよう日々改良されています。いつまでも古いパターンファイルやプログラムのままでウイルスバスター 2003 を使い続けていると、流行の新型ウイルスに対応できない場合があります。

ウイルスバスター 2003 のアップデートを実行するには、オンラインユーザ登録が必要です。オンラインユーザ登録の詳細については、25 ページを参照してください。

インテリジェントアップデート

インテリジェントアップデートとは？

最新のウイルス対策を実現するためには、ウイルスバスター 2003 を常に最新版に保つ必要があります。トレンドマイクロから新しい**パターンファイル**、**検索エンジン**、**プログラム**が公開されていないかを定期的に確認するのは、つい忘れがちで手間のかかる作業です。インテリジェントアップデート機能は、この確認作業を自動化することができる機能です。

インテリジェントアップデート機能が有効になっていると、ウイルスバスター 2003 は、設定された周期でトレンドマイクロのサーバにアクセスして、新しいプログラムが公開されていないかを確認します。新しいプログラムが公開されていた場合、アップデートを促す通知が表示されます。

インテリジェントアップデート機能の有効 / 無効は、インストール手順 8（16 ページ参照）で選択した「インターネット接続の許可設定」オプションによって、次のように自動設定されます。

■ [インターネットへの自動接続を許可する] を選択した場合

インターネットへの自動接続を許可した場合には、インテリジェントアップデート機能が有効に設定されます。初期設定では、コンピュータを起動してから、3 時間ごとにトレンドマイクロのサーバに新しいプログラムが公開されていないかを確認します。新しいプログラムが公開されていた場合、アップデートを促す通知が表示されます。

インターネット接続にダイヤルアップルータをお使いの環境でこのオプションを選択すると、ルータの設定によっては自動的にダイヤルアップ接続を開始して、課金が発生する場合があります。インターネット接続のたびに課金が発生する環境では、ご注意ください。

■ [インターネットへの自動接続を許可しない] を選択した場合

インターネットへの自動接続を許可しなかった場合には、インテリジェントアップデート機能は無効に設定されます。このオプションを選択した場合には、定期的にアップデートを手動で実行する必要があります。アップデートを手動で実行する方法については、96 ページを参照してください。

注意 インテリジェントアップデート機能を使用するには、インターネット接続環境が必要です。インターネット接続が可能な環境でインテリジェントアップデート機能を無効に設定している場合は、必ず定期的に手動アップデートを実行してください。インテリジェントアップデート機能の注意事項については、Readme も参照してください。

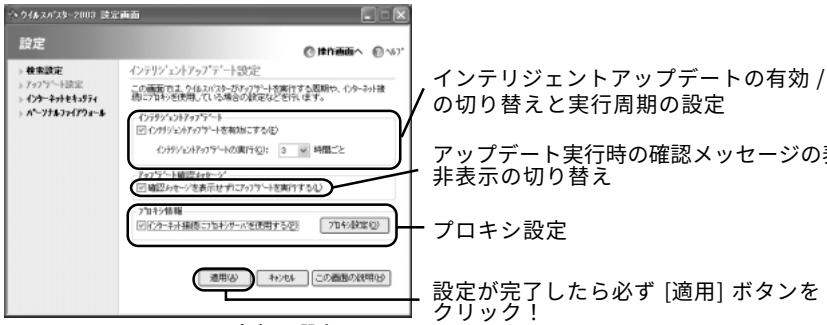
注意 アップデートを実行するには、インターネット接続環境が必要です。インターネット接続にプロキシサーバを使用している場合には、プロキシ情報を設定する必要があります。プロキシ設定については、98 ページを参照してください。

インテリジェントアップデートの設定

インテリジェントアップデートの有効 / 無効は、[インテリジェントアップデート設定] 画面から切り替えることができます。また、インテリジェントアップデート実行時に確認メッセージを表示しないように設定することもできます。

手順：インテリジェントアップデートを設定する

1. ウイルスバスター 2003 設定画面を表示します。
2. 左側のメニューから [アップデート設定] を選択します。[インテリジェントアップデート設定] 画面が表示されます。



[インテリジェントアップデート設定] 画面

[インテリジェント設定] 画面では、次の項目について設定することができます。

■ インテリジェントアップデートの有効 / 無効の切り替え

[インテリジェントアップデートを有効にする] チェックボックスで、インテリジェントアップデート機能の有効 / 無効を切り替えます。

オン☑：インテリジェントアップデート機能は有効になります。チェックボックス下の [インテリジェントアップデートの実行：[xx] 時間ごと] のリストボックスから、インテリジェントアップデートを実行する周期を選択してください。

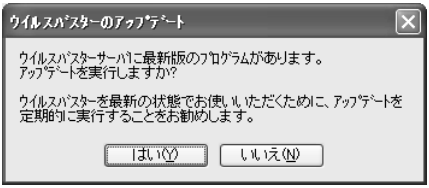
オフ☐：インテリジェントアップデート機能は無効になります。

■ アップデート確認メッセージの表示設定

インテリジェントアップデート機能が有効に設定されていると、指定した周期で最新版が公開されているかどうか確認します。最新版が公開されている場合、アップデートを促すメッセージが表示されます。

このメッセージを表示せずに、自動的にアップデートを実行するようにしたい場合には、[確認メッセージを表示せずにアップデートを実行する] チェックボックスをオンにします。

次回のアップデート実行時から確認メッセージが表示されなくなります。



アップデート確認メッセージ

■ プロキシ情報の設定

アップデートを実行するには、インターネット接続が必要です。インターネット接続にプロキシサーバをお使いの場合には、[インターネット接続にプロキシサーバを使用する] チェックボックスをオンにし、[プロキシ設定] ボタンをクリックして表示される画面で、プロキシサーバの情報や認証情報を入力してください。プロキシサーバについては、98 ページを参照してください。

注意 [インテリジェントアップデート設定] 画面で設定を変更したら、[適用] ボタンを必ずクリックしてください。[適用] ボタンをクリックしないと、変更した設定は有効になりません。

注意 アップデートの実行には、インターネット接続が必要です。アップデートを実行した際のインターネット接続に伴う通信料金はお客さまのご負担になります。

手動アップデートの実行

手動アップデート

インテリジェントアップデート機能を無効に設定している場合には、定期的にアップデートを手動で実行して、ウイルスバスター 2003 を最新の状態に保つようにしてください。

ウイルスバスター 2003 の手動アップデートは、操作画面 (シンプルモード / プロフェッショナルモード) から実行します。

注意 アップデートを実行するには、インターネットに接続する必要があります。

手順：アップデートを手動で実行する

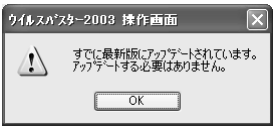
1. ウイルスバスター 2003 操作画面を表示します。
2. [最新版にアップデート]をクリックしてアップデート画面を表示します。

   シンプル：[最新版にアップデート]をクリックすると、ただちにアップデートが開始されます。

   プロフェッショナル：[最新版にアップデート]画面で [アップデート] ボタンをクリックすると、アップデートが開始されます。

シンプルモードでのアップデート

すでに最新版がダウンロードされている場合は、すでに最新版であることを知らせるメッセージが表示されます。



注意 アップデートを実行するには、オンラインユーザ登録が完了している必要があります。また、ウイルスバスタークラブ会員の有効期間が終了している場合、アップデートを実行することはできません。オンラインユーザ登録の詳細については、25 ページを参照してください。

アップデートが失敗したら？

アップデートを実行できない場合、次の原因が考えられます。

■ ユーザ登録が完了していない

アップデート機能を利用するには、オンラインユーザ登録を完了する必要があります。操作画面の [ユーザ登録] 画面を開いて、シリアル番号、ライセンスキーを正しく入力してください。ユーザ登録の詳細については、25 ページを参照してください。

■ ウイルスバスタークラブ会員の有効期間が終了している

オンラインユーザ登録から 1 年が経過すると、ウイルスバスタークラブ会員の有効期間が終了していることをお知らせするメッセージが表示され、アップデートを実行することができません。アップデートを実行するには、ウイルスバスタークラブ会員契約を更新していただく必要があります。

■ インターネット接続できない

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コンピュータがインターネットに接続している必要があります。インターネット接続に障害が発生している場合、ウイルスバスター 2003 ではアップデート処理を実行することができません。

■ プロキシサーバが正しく設定されていない

インターネット接続にプロキシサーバをお使いの場合、ウイルスバスター 2003 のプロキシ設定画面でプロキシサーバ情報を設定する必要があります。初期設定の Web ブラウザに Microsoft Internet Explorer をお使いの場合、ウイルスバスター 2003 のインストール時にプロキシサーバの情報が自動的に読み込まれます。ただし、ユーザ情報やパスワードは手動設定が必要です。プロキシサーバ情報の設定方法については、98 ページを参照してください。

■ サーバが混雑している

ウイルスバスター 2003 では、アップデート実行時にトレンドマイクロのアップデートサーバに接続します。ウイルス大量発生時など、アップデートサーバへの接続が集中する場合に、サーバへ接続しづらくなる場合があります。

このような場合には、しばらくお待ちいただいてから再度アップデートを実行してください。

プロキシサーバ設定

プロキシサーバとは？

プロキシサーバとは、インターネット接続時のセキュリティ対策のために設置されているサーバです。ファイアウォールの内側にあるクライアントからアクセス要求（HTTP、FTP など）を受け付け、ファイアウォール外部への接続を許可する役目を果たしています。

プロキシサーバは、インターネット接続時に取得されたデータをサーバ上に保存しています。次回に同じファイルへのアクセスがあった場合は、保存されたデータが読み込まれるため、インターネット接続のスピードの向上にもつながります。

企業のネットワークや契約しているプロバイダで、インターネット接続にプロキシサーバをお使いの場合は、ウイルスバスター 2003 のアップデート機能を利用するために、プロキシサーバの情報をウイルスバスター 2003 のプロキシ設定画面に入力する必要があります。

> 注意 プロキシサーバの情報については、ネットワーク管理者または各契約プロバイダにお問い合わせください。

プロキシ設定

[インテリジェントアップデート設定] 画面から、プロキシ情報を設定します。

手順：プロキシ情報を設定する

1. ウイルスバスター 2003 設定画面を表示します。
2. 左側のメニューから [アップデート設定] を選択します。[インテリジェントアップデート設定] 画面が表示されます。
3. [プロキシ情報] の [インターネット接続にプロキシサーバを使用する] チェックボックスをオンにします。
4. [プロキシ設定] ボタンをクリックします。[プロキシ] 画面が表示されます。
5. お使いの環境でのプロキシ情報を入力してください。

プロキシ設定画面

■ IP アドレス：お使いのプロキシサーバの IP アドレス (例：192.168.0.11) 、またはホスト名 (例：proxy.company.co.jp) を入力してください。

■ ポート：プロキシサーバで使用するポート番号 (例：80、8080) を入力してください。

■ ユーザ名 / パスワード：プロキシサーバへの接続にユーザ名およびパスワードが必要な場合には、それぞれ入力してください。

6. 必要な情報を入力したら、[OK] ボタンをクリックして、[インテリジェントアップデート設定] 画面に戻ります。

7. [適用] ボタンをクリックして、設定したプロキシ情報を有効にします。

プロキシ設定が完了したら、アップデートを手動で実行して、アップデートが正常に実行されるかどうか確認することをお勧めします。

アップデートログについて

ウイルスバスター 2003 では、実行されたアップデートに関する情報を「アップデートログ」に記録します。アップデートログを参照して、アップデートが実行された日付やアップデートが正常に実行されているかなどを確認することができます。

アップデートログでは、次の情報が表示されます。

■ 時刻：アップデートが実行された時刻が表示されます。

■ ダウンロード：アップデートしたファイルの種類 (パターンファイル、検索エンジン、プログラム) が表示されます。

■ ステータス：アップデートが正常に実行されたかどうかを表示します。

アップデートログの表示方法、ファイルへの出力、およびログの削除方法については、41 ページを参照してください。

第 7 章 ネットワークセキュリティ

ケーブル接続や ADSL などブロードバンド接続により、インターネットへの常時接続が一般家庭にも普及してきた今、ウイルス感染とは別に、不正プログラムによるコンピュータへの被害や、個人情報の流出などが問題となっています。ウイルスバスター 2003 では、お使いのコンピュータを不正アクセスなどから守るための機能も提供しています。

第 7 章では、ウイルスバスターが提供するネットワークセキュリティ機能について説明します。

インターネットセキュリティ

インターネットを安全に利用していただくために、ウイルスバスター2003では、「WebTrap (ウェブトラップ)」と「URL フィルタ」の 2 つの機能を用意しました。

WebTrap 機能について

ウイルスバスター 2003 の WebTrap（ウェブトラップ）機能は、Java、ActiveX などのプログラム言語を使用して作成された、害のあるプログラムを含む Web サイトにアクセスした場合に、不正プログラムのダウンロードをブロックしてお使いのコンピュータを守るための機能です。初期設定のウイルスバスター 2003 では、WebTrap 機能は**無効**に設定されています。

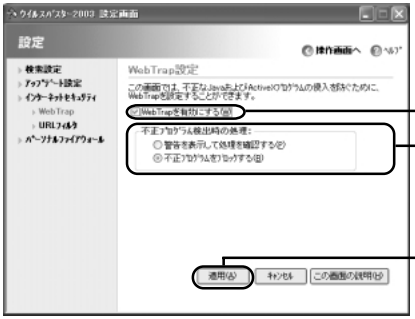
WebTrap 機能を有効にすると、処理を実行するために通信速度に制限が生じる場合があります。特に、ADSL やケーブルテレビなど、高速の通信回線をお使いの場合、通信速度が著しく低下する場合もあります。不正な Java、ActiveX プログラムなどを実行してしまう危険が少ないと判断される場合には、WebTrap 機能は無効のままにしてください。

WebTrap の設定

[WebTrap 設定] 画面から、WebTrap の有効 / 無効の切り替えなどを設定することができます。

手順：WebTrap を設定する

1. ウイルスバスター 2003 設定画面を表示します。
2. 左側のメニューから [インターネットセキュリティ]→[WebTrap] の順に選択します。[WebTrap 設定] 画面が表示されます。



[WebTrap 設定] 画面

3. WebTrap 機能を有効にするには、[WebTrap 機能を有効にする] チェックボックスをオンにします。
4. 不正プログラムを検出した際の処理オプションを選択します。

   警告を表示して処理を確認する：このオプションを選択すると、 害のあるプログラムを含む Web サイトにアクセスした際に、警告メッセージを表示して、そのサイトへのアクセスを許可するかどうかを選択することができます。

   不正プログラムをブロックする：このオプションを選択すると、害のあるプログラムを含む Web サイトにアクセスした際に、警告メッセージを表示して、そのサイトへのアクセスをブロックします。

注意 [WebTrap 設定] 画面で設定を変更したら、[適用] ボタンを必ずクリックしてください。[適用] ボタンをクリックしないと、変更した設定は有効になりません。

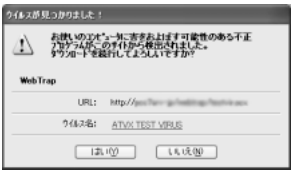
不正プログラムが見つかると …

WebTrap 機能を有効にして、不正プログラムを含む Web サイトにアクセスすると、設定した処理オプションに応じて警告メッセージが表示されます。

■「警告を表示して処理を確認する」オプションの場合

不正プログラムが見つかると、不正プログラムが見つかったことをお知らせするメッセージが表示されます。

Web サイトへのアクセスを中断する場合には、[いいえ] をクリックします。[はい] をクリックすると、Web サイトへのアクセスが続行されます。この場合、不正プログラムがダウンロードされる危険がありますので、ご注意ください。



処理を確認するメッセージ

■「不正プログラムをブロックする」オプションの場合

不正プログラムが見つかると、Web サイトへのアクセスがブロックされたことをお知らせするメッセージが表示されます。

不正プログラムをブロック

URL フィルタ機能について

ウイルスバスター 2003 の URL フィルタ機能は、指定したインターネットサイトへのアクセスを禁止することができる機能です。URL フィルタ機能を使えば、一部の Web サイトへの接続を制限したり、接続時に警告メッセージを表示することができます。また、アクセス制限サイト設定をパスワードで保護して、他の人が許可なく内容を変更できないよう設定することも可能です。

たとえば家族で 1 台のコンピュータを共有しているような環境で、暴力や性的な内容を含むインターネットサイトへお子さまがアクセスするのを防ぎたい場合などに、URL フィルタを効果的に利用することができます。

初期設定では URL フィルタ機能は**無効**になっています。

注意 URL フィルタ機能を有効にすると、処理を実行するためにインターネット通信速度に制限が生じる場合があります。初期設定のウイルスバスターでは、URL フィルタ機能が無効に設定されています。アクセス制限サイトを設定しない場合は、URL フィルタ機能は無効のままにしてください。

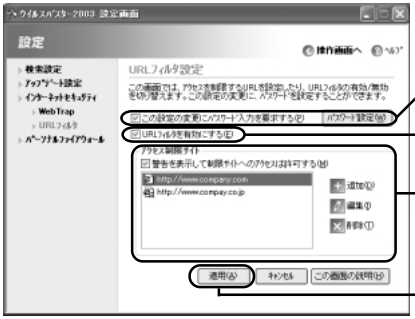
URL フィルタの有効化 / 無効化

[URL フィルタ設定] 画面から、URL フィルタの有効 / 無効を切り替えることができます。

手順：URL フィルタを有効にする

1. ウイルスバスター 2003 設定画面を表示します。
2. 左側のメニューから [インターネットセキュリティ]→[URL フィルタ] の順に選択します。[URL フィルタ設定] 画面が表示されます。

   [URL フィルタ設定] 画面にパスワードを設定している場合、パスワードの入力が求められます。



URL フィルタ設定画面

3. URL フィルタ機能を有効にするには、[URL フィルタを有効にする] チェックボックスをオンにします。

> **注意** [URL フィルタ設定] 画面で設定を変更したら、[適用] ボタンを必ずクリックしてください。[適用] ボタンをクリックしないと、変更した設定は有効になりません。

4. アクセス制限サイトに登録されたサイトにアクセスしようした際に、警告メッセージを表示して、そのサイトへアクセスするかどうかを選択できるようにすることができます。警告メッセージが表示されるようにするには、[警告を表示して制限サイトへのアクセスは許可する] チェックボックスをオンにします。

アクセス制限サイトの追加 / 編集 / 削除

[URL フィルタ設定] 画面で、アクセスを制限するサイトを登録したり、登録されている制限サイトを削除することができます。

手順：アクセス制限サイトを追加 / 編集 / 削除する

1. ウイルスバスター 2003 設定画面を表示します。
2. 左側のメニューから [インターネットセキュリティ]→[URL フィルタ] の順に選択します。[URL フィルタ設定] 画面が表示されます。

   [URL フィルタ設定] 画面にパスワードを設定している場合、パスワードの入力が求められます。
3. [URL フィルタを有効にする] チェックボックスがオンになっていることを確認してください。
4. 追加(D) [追加]、編集(P) [編集]、削除(T) [削除] のいずれかのボタンをクリックして、アクセス制限サイトを編集します。

   追加：[アクセス制限サイトの追加 / 編集] 画面が表示されます。[サイトの URL] テキストボックスには、お使いの Web ブラウザから最後にアクセスしたサイトの URL が自動的に読み込まれます。URL を編集したい場合は、テキストボックスに制限したい URL を入力してください。また、入力した URL のサブページも規制対象にするには、[サブページも規制対象にする] チェックボックスをオンにします。

アクセス規制サイトを入力します

   編集：アクセス制限サイトにすでに登録されている URL を一覧から選択して、このボタンをクリックすると、[アクセス制限サイトの追加 / 編集] 画面が表示されます。制限するサイトの URL を編集することができます。

   削除：アクセス制限サイトにすでに登録されている URL を一覧から選択して、このボタンをクリックすると、アクセス制限一覧から削除されます。

URL フィルタ設定のパスワード設定

[URL フィルタ設定] 画面にパスワードを設定して、他の人が許可なく設定をしないようにすることができます。

手順：URL フィルタ設定にパスワードを設定する

1. ウイルスバスター 2003 設定画面を表示します。
2. 左側のメニューから [インターネットセキュリティ]→[URL フィルタ] の順に選択します。[URL フィルタ設定] 画面が表示されます。
3. [URL フィルタ設定] 画面にパスワードを設定するには、[この設定の変更にパスワードを要求する] チェックボックスをオンにします。
4. 次に [パスワード設定] ボタンをクリックします。パスワードの設定ダイアログが表示されます。
5. [パスワード] テキストボックスに、任意のパスワードを入力します。パスワードは半角英数字で入力してください。

URL フィルタパスワード入力画面

注意 入力した文字は、アスタリスク (*) で表示されます。

6. [パスワードの確認] テキストボックスに、手順 5 で入力したパスワードを再入力します。

注意 入力した文字は、アスタリスク (*) で表示されます。

7. [OK] ボタンをクリックして、[URL フィルタ設定] 画面に戻ります。
8. [適用] ボタンをクリックして、設定を保存します。

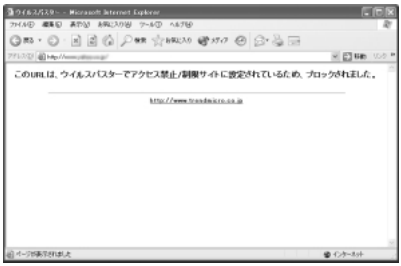
次回、[URL フィルタ設定] 画面にアクセス使用とすると、パスワードの入力が要求されます。

注意 URL フィルタのパスワードの設定は、URL フィルタ機能が無効の場合も有効です。

アクセス制限サイトにアクセスすると …

アクセス制限サイトに登録された Web サイトにアクセスしようとすると、アクセスをブロックします。ただし、警告メッセージを表示して制限サイトへのアクセスを許可するように設定していると、アクセスを許可するかどうかの確認メッセージが表示されるようになります。

■ アクセスをブロックする
制限サイトへアクセスしようとすると、アクセスできないことをお知らせするメッセージが Web ブラウザに表示されます。



制限サイトへのアクセスをブロック

■ 警告メッセージを表示する

制限サイトへアクセスしようとすると、警告メッセージが表示されます。[はい] をクリックすると、制限サイトにアクセスすることができます。

警告メッセージを表示

URL フィルタログについて

ウイルスバスター 2003 では、アクセス制限サイトへのアクセスが発生した場合に、その情報を URL フィルタログに記録します。

URL フィルタログでは、次の情報が表示されます。

■ 時刻：制限サイトへのアクセスが発生した時刻が表示されます。

■ URL サイト：アクセスしようとした制限サイトの URL が表示されます。

■ 結果：制限サイトへのアクセスをブロックしたのか、許可したのかが表示されます。
URL フィルタログの表示方法、ファイルへの出力、およびログの削除方法については、41 ページを参照してください。

パーソナルファイアウォール

パーソナルファイアウォール機能について

コンピュータが急速に普及した現在では、コンピュータのほとんどがインターネットや社内ネットワークに接続していることが一般的になっています。お使いのコンピュータが外部のコンピュータネットワークと接続されている以上、コンピュータへの不正アクセスの危険は常に生じています。

ウイルスバスター 2003 のパーソナルファイアウォール機能を使えば、複雑な設定なしでお使いのコンピュータを不正アクセスから守ることができます。

ウイルスバスター 2003 のパーソナルファイアウォール機能については、本書付録の「はじめてのパーソナルファイアウォール」を活用してください。

パーソナルファイアウォールのインストール / アンインストール

ウイルスバスター 2003 のインストール時に、ウイルスバスター 2003 のパーソナルファイアウォールをインストールしなかった場合、パーソナルファイアウォールに関連するメニューや設定画面は表示されません。

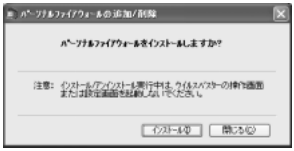
ウイルスバスター 2003 のパーソナルファイアウォール機能を利用するには、パーソナルファイアウォールのインストールが必要です。

手順：パーソナルファイアウォールをインストール / アンインストールする

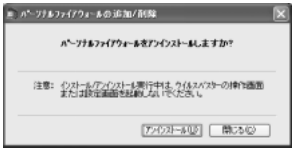
1. ウイルスバスター 2003 のパーソナルファイアウォールのインストールを開始する前に、他社のファイアウォール製品がアンインストールされていることを確認してください。
2. ウイルスバスター 2003 の操作画面 / 設定画面が起動している場合、画面を閉じます。
3. Windows の [スタート] メニューから [プログラム](Windows XP の場合 [すべてのプログラム])→[トレンドマイクロ ウイルスバスター 2003]→[ファイアウォールの追加と削除] の順に選択します。[パーソナルファイアウォールの追加と削除] 画面が表示されます。

4. パーソナルファイアウォールをインストールするには、[インストール] ボタンをクリックします。

   パーソナルファイアウォールをアンインストールするには、[アンインストール] ボタンをクリックします。



パーソナルファイアウォールがインストールされていない場合



パーソナルファイアウォールがインストールされている場合

5. インストール (またはアンインストール) が完了したことをお知らせするメッセージが表示されたら、[閉じる] ボタンをクリックします。

インストールが完了したら、ウイルスバスター 2003 設定画面で、パーソナルファイアウォールメニューが表示されていることを確認してください。

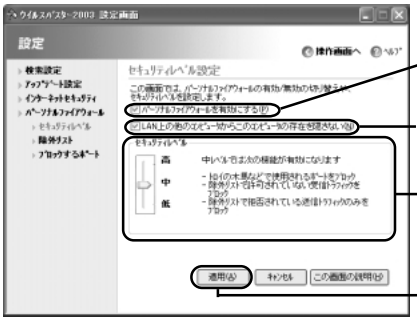
パーソナルファイアウォールの設定

ウイルスバスター 2003 のパーソナルファイアウォールでは、セキュリティレベルを高 / 中 / 低の 3 段階で調整することができます。

初期設定のウイルスバスター 2003 では、パーソナルファイアウォール機能が有効に設定され、セキュリティレベルは**「中」**に設定されています。初期設定では、Web サイトの表示や e-mail の送受信に必要な接続を許可するように「除外リスト」であらかじめ設定されているので、初期設定のままでもインターネット接続や e-mail の送受信には影響ありません。

手順：パーソナルファイアウォールを設定する

1. ウイルスバスター 2003 設定画面を表示します。
2. 左側のメニューから [パーソナルファイアウォール] → [セキュリティレベル] を選択して、[セキュリティレベル設定] 画面を表示します。



パーソナルファイアウォールの有効 / 無効の切り替え

同一ネットワーク上のコンピュータからの接続の許可 / 拒否の切り替え

セキュリティレベルの設定

設定が完了したら必ず [適用] ボタンをクリック！

セキュリティレベル設定画面

3. [セキュリティレベル設定] 画面では、次の項目について設定することができます。

■ パーソナルファイアウォールを有効にする
パーソナルファイアウォールの有効 / 無効を切り替えることができます。初期設定では、**有効**に設定されています。

■ LAN 上の他のコンピュータからこのコンピュータの存在を隠さない
同一ネットワーク上の他のコンピュータからお使いのコンピュータへのアクセスを許可することができます。

セキュリティレベルが「低」に設定されている場合には、送受信アクセスが許可されるため、このオプションは無効です。

■ セキュリティレベル
セキュリティレベルのスライドバーで、セキュリティレベルを「高」、「中」、「低」のいずれかに設定します。それぞれのセキュリティレベルでのブロック対象は次の通りです。

ブロック/許可する対象	高	中	低
コンピュータ内部から外部への**送信**アクセス	ブロック ＊警告を表示	**許可**	許可
コンピュータ外部から内部への**受信**アクセス	ブロック	**ブロック**	許可
除外リストに登録された**送信**アクセス	許可	**ブロック**	-
除外リストに登録された**受信**アクセス	許可	**許可**	-
トロイの木馬が使用するポートを利用した**送受信**アクセス	ブロック	**ブロック**	ブロック
コンピュータに被害を与えたり、 不正アクセスにつながると判断されるパケット	ブロック	**ブロック**	ブロック

4. パーソナルファイアウォールの設定が完了したら、[適用] ボタンをクリックして設定を保存してください。

除外リストの設定

ウイルスバスター 2003 のパーソナルファイアウォール機能有効に設定して、セキュリティレベルを「高」または「中」に設定すると、レベルに応じてお使いのコンピュータから外部への接続や外部からの接続がブロックされます。このパーソナルファイアウォール機能により、外部のコンピュータに全くアクセスすることができなくなってしまったり、サービスを利用することができなくなってしまいます。それぞれのレベルでのブロック対象については、前ページの表を参照してください。

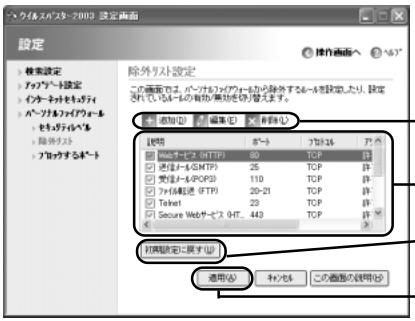
「除外リスト」を使って、特定の種類のアクセスについてブロックする / しないルールを設定することができます。

手順：除外リストを表示する

1. ウイルスバスター 2003 設定画面を起動します。
2. 設定メニューから [パーソナルファイアウォール] → [除外リスト] の順に選択して、[除外リスト設定] 画面を表示します。

> 注意 [除外リスト設定] 画面で設定を変更したら、[適用] ボタンを必ずクリックしてください。[適用] ボタンをクリックしないと、変更した設定は有効になりません。

[除外リスト設定] 画面では、次の項目について設定することができます。



[除外リスト設定] 画面

除外ルールの追加 / 編集 / 削除

新しい除外ルールを作成したり、既存のルールを編集したり、不要になった除外ルールを削除することができます。また、ボタン１つで初期設定のルールに戻すこともできます。

手順：新しい除外ルールを作成する

1. [除外リスト設定] 画面の 追加(D) [追加] ボタンをクリックします。[除外リストルールの追加 / 編集] 画面が表示されます。

   作成するルールについて、次の項目を設定します。

除外ルールの編集画面

■ ルールの説明入力
新しく作成するルールを説明する名称を入力します。

■ アクセス許可 / 拒否の選択
アクセスを許可するのか拒否 (ブロック) するのかを選択します。

注意 セキュリティレベルが「高」に設定されている場合には、「許可」する接続のみ設定することができます。

■ コンピュータの指定
アクセスを許可 / 拒否する対象を選択します。[種類] で選択したオプションによって、IP アドレスや IP アドレスの範囲などを指定します。

■ アクセスの送受信方法の指定
ルールを適用するアクセスの送受信方向を指定します。
　受信：外部からのアクセスに対してルールを適用します。
　送信：外部へのアクセスに対してルールを適用します。

■ 許可 / 拒否するアクセスのポート指定
許可 / 拒否したいアクセスが利用するポート番号を指定します。
　すべてのポート：あらゆるポートを通過するアクセスに適用されます。
　指定したポート：テキストボックスに指定したポートを通過するアクセスのみに適用されます。

■ プロトコルの指定
許可 / 拒否したいアクセスが使用するプロトコルを選択します。

2. すべての情報の設定が完了したら、[OK] ボタンをクリックして、[除外リスト設定] 画面に戻ります。

   除外リストに作成したルールが追加されていることを確認してください。

3. [除外リスト設定] 画面で、[適用] ボタンをクリックして、設定を保存します。

手順：除外ルールを編集する

1. [除外リスト設定] 画面で、編集したいルールをクリックして選択します。
2. [除外リスト設定] 画面の 編集(E) [編集] ボタンをクリックします。[除外リストルールの追加 / 編集] 画面が表示されます。
3. 必要に応じて設定されている情報を編集してください。
4. 編集が完了したら [OK] ボタンをクリックして、[除外リスト設定] 画面に戻ります。
5. [除外リスト設定] 画面で、[適用] ボタンをクリックして、設定を保存します。

手順：除外ルールを削除する

1. [除外リスト設定] 画面で、削除したいルールをクリックして選択します。
2. [除外リスト設定] 画面の 削除(L) [削除] ボタンをクリックします。
3. ルールの削除を確認するメッセージが表示されたら、[はい] をクリックします。選択したルールが削除されます。
4. [除外リスト設定] 画面で、[適用] ボタンをクリックして、設定を保存します。

手順：除外ルールを初期設定に戻す

除外ルールを初期設定に戻すには、[除外リスト設定] 画面の [初期設定に戻す] ボタンをクリックします。初期設定に戻したら、[適用] ボタンをクリックして、設定を保存します。

除外ルールの有効 / 無効の切り替え

設定した除外ルールを削除せずに、一時的に無効にしたり、または一時的に有効にすることができます。

手順：除外ルールの有効 / 無効を切り替える

[除外ルール設定] 画面に表示されている各ルール名の左にあるチェックボックス(☐)のオン / オフを切り替えることで、それぞれのルールの有効 / 無効を切り替えることができます。

オン(☑)：ルールは有効です。

オフ(☐)：ルールは無効です。

ブロックするポートの確認

ウイルスバスター 2003 には、「トロイの木馬」に利用されるポートの情報が登録されています。トロイの木馬ブロック機能が有効であれば、トロイの木馬による「ブロックするポート」を使用したアクセスをブロックすることができます。[ブロックするポート] 画面で、ブロックされるポートの一覧を確認することができます。

手順：ブロックするポートを確認する

1. ウイルスバスター 2003 設定画面を表示します。
2. 左側のメニューから [パーソナルファイアウォール]→[ブロックするポート] の順に選択します。[ブロックするポート] 画面が表示されます。
3. [ブロックするポート] リストが画面に表示されます。

ブロックされるポートの一覧

パーソナルファイアウォールログ

ウイルスバスター 2003 では、パーソナルファイアウォール機能によってブロックされた情報をパーソナルファイアウォールログに記録します。

パーソナルファイアウォールログでは、次の情報が表示されます。

■ 種類：ファイアウォールによってブロックされたアクセスの種類が表示されます。

■ 時刻：ファイアウォールによってアクセスがブロックされた時刻が表示されます。

■ 受信 / 送信：ブロックされたアクセスの送受信方向が表示されます。
受信：外部からお使いのコンピュータに向けたアクセスがブロックされた場合
送信：お使いのコンピュータから外部に向けたアクセスがブロックされた場合

■ プロトコル：ブロックされたアクセスで使用されたプロトコル名 (TCP、UDP、ICMP など) が表示されます。

■ 送信元 IP アドレス：ブロックされたアクセスを送信した送信元 IP アドレスが表示されます。

■ 送信元ポート：ブロックされたアクセスを送信した送信元ポート番号が表示されます。

■ 送信先 IP アドレス：ブロックされたアクセスの送信先 IP アドレスが表示されます。

■ 送信先ポート：ブロックされたアクセスの送信先ポート番号が表示されます。

■ 説明：ブロックされたアクセスの詳細な内容が表示されます。

パーソナルファイアウォールログの表示方法、ファイルへの出力、およびログの削除方法については、41 ページを参照してください。

無線 LAN 環境でのセキュリティ

駅やハンバーガーショップなどの公共の場所で、無線 LAN によるインターネット接続サービスを利用する機会が増えています。このときに心配なのが、他のコンピュータからの不正アクセスです。

ウイルスバスター 2003 の「無線 LAN」モードは、公共の無線 LAN 接続環境に最適なファイアウォール環境を提供する機能です。

家庭や企業など、通常のネットワーク環境でパーソナルファイアウォールを利用する場合、無線 LAN モードに切り替える必要はありません。

手順：操作画面から無線 LAN モードに切り替える

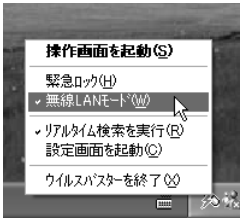
1. ウイルスバスター 2003 操作画面を表示します。
2. シンプルモードが選択されている場合には、[プロフェッショナル] タブをクリックして、プロフェッショナルモードに切り替えます。
3. [ファイアウォールの状況] ボタンをクリックします。[ファイアウォールの状況] 画面が表示されます。
4. [無線 LAN モード] ボタンをクリックします。無線 LAN モードを示すボタンに変更されたことを確認してください。

無線 LAN モードオフ時

無線 LAN モードオン時

手順：ウイルスバスターアイコンから無線 LAN モードに切り替える

1. タスクトレイのウイルスバスターのアイコン を右クリックします。
2. 表示されたメニューから [無線 LAN モード] を選択します。
3. 無線 LAN モードが有効になると、メニューの [無線 LAN モード] の前にチェックマーク [✓] が表示されます。



注意 ウイルスバスター 2003 の無線 LAN モードには、無線 LAN を利用したパケット通信を暗号化したり、アクセスポイントにおけるユーザ認証を行うための機能は実装されていません。

第 8 章 困った時は ...

ウイルスバスター 2003 では、ウイルスバスター 2003 の操作中に困ったことが起きた時のために、オンラインヘルプや Web ページなどさまざまな方法でお客さまをサポートしています。

第 8 章では、オンラインヘルプの使い方など、困った時のための対処方法について説明します。

設定や操作に困った時は ...

オンラインヘルプを利用する

ウイルスバスター 2003 の機能や操作について困ったり、わからないことがある場合は、オンラインヘルプを活用してみましょう。オンラインヘルプを表示するには、ウイルスバスターの各画面から [この画面の説明] ボタンをクリックするか、操作画面 / 設定画面の [ヘルプ] ボタンをクリックして表示されるメニューから [ヘルプ] を選択します。

オンラインヘルプでは、次の 3 つの方法で調べたい項目を検索することができます。

- 「目次」:ヘルプの各項目が目次別に分類されています。調べたい機能、操作方法について解説している項目のタイトルを選択して、内容を表示してください。
- 「キーワード」:調べたい内容をキーワード検索し、関連項目を表示することができます。
- 「検索」:検索したい用語をテキストボックスに入力して、その用語が使われている項目をすべて表示することができます。検索結果は用語の使用頻度のランク順に表示されます。

オンラインヘルプには、各機能や操作の説明の他にも、「よくある質問」や「用語集」も掲載されています。わからないこと、調べたいことがあれば、ウイルスバスタークラブセンターへ連絡する前に、ぜひオンラインヘルプを活用してください。

オンラインヘルプを活用しましょう

製品 Q&A 検索を利用する

トレンドマイクロでは、製品に関してお客さまからよくいただく質問とそれに対する回答や、本書作成後に確認された情報などを、製品 Q&A としてインターネット上で公開しています。ウイルスバスタークラブセンターへお問い合わせいただく前に、製品 Q&A 検索を使って、知りたい情報が公開されているかどうか確認していただくことをお勧めします。

製品 Q&A 検索データベースには、トレンドマイクロホームページのサポートサイトからアクセスすることができます。

> 注意 製品 Q&A 検索データベースを利用するには、インターネット接続が必要です。インターネット接続にともない発生する通信料金はお客さまの負担となります。

ウイルスバスタークラブセンターへ問い合わせる

「ウイルスバスタークラブセンター」では、ユーザ登録を完了して、ウイルスバスタークラブ会員として登録されたお客さまに、e-mail、FAX、電話によるサポートサービスをご提供しています。

FAXでお問い合わせいただく場合は、ウイルスバスター2003のCD-ROM内のSupportフォルダにあるお問い合わせシート（**お問い合わせシート .rtf**）データをご利用ください。

ウイルスバスタークラブセンターへのお問い合わせには、シリアル番号が必要です。また、操作方法やウイルスの処理についてのお問い合わせの場合は、次の情報もあわせてご用意ください。

- ウイルスバスター 2003 の**シリアル番号**、**お客さま番号**
- お使いのウイルスバスター 2003 が使用している**パターンファイル**、**検索エンジン**、**プログラムのバージョン番号**
- ウイルスバスター 2003 がインストールされている**コンピュータ OS** とその**バージョン**
- インターネット接続環境に関する情報（プロバイダ情報、プロキシサーバの有無など）
- エラーメッセージが表示される場合は、その内容
- 問題が起こっている場合は、その問題を再現する方法

> 注意 ウイルスバスタークラブセンターへのお問い合わせに伴って発生する通信料金は、お客さまの負担となります。

よくある質問とその回答

インストール / ユーザ登録に関する質問

Q ウイルスバスター 2002 のシリアル番号を使用できますか？

A ウイルスバスタークラブ会員契約期間中であれば、ウイルスバスター 2003 のインストール時に、ウイルスバスター 2002 でお使いいただいたシリアル番号を使用することができます。

Q ウイルスバスター 2002 のライセンスキーを使用できますか？

A ウイルスバスター 2002 のオンライン登録時に発行されたライセンスキーは、ウイルスバスター 2002 をご利用いただいていた環境であれば、ウイルスバスター 2003 のユーザ登録時にも使用することができます。ウイルスバスター 2002 のユーザ登録時に発行されたライセンスキーは、オンラインユーザ登録完了時に送信された e-mail に掲載されています。
ライセンスキーをなくしてしまった場合は、オンライン登録画面にアクセスして、ライセンスキーを再取得してください。

Q ウイルスバスター 2003 を複数のコンピュータ /OS にインストールできますか？

A ウイルスバスター 2003 の同一シリアル番号を使用して、複数のコンピュータにウイルスバスター 2003 をインストールすることはできません。複数台のコンピュータにインストールしたい場合は、必要台数分のウイルスバスター 2003 を新しく購入していただく必要があります。
また、1 台のコンピュータに複数の OS が導入されている場合でも、1 つの OS につき 1 つずつウイルスバスター 2003 をお買い求め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コンピュータまたは OS にインストールするなどの不正な方法でインストールすると、オンラインユーザ登録ができない、最新版のパターンファイル、検索エンジン、プログラムをダウンロードできないなどのトラブルにつながる場合があります。シリアル番号は、使用許諾書に記載された正しい方法でお使いください。

Q OS を再インストールした後、今までのライセンスキーは使用できますか？

A OS を再インストールした場合、以前のライセンスキーは使用できなくなります。その場合、オンライン登録を再度実行して、ライセンスキーを再取得する必要があります。新しいライセンスキーが発行されたら、ライセンスキーを登録してください。

Q ウイルスバスター 2003 を再インストールしたのですが、ユーザ登録は必要ですか？

A ウイルスバスター 2003 を一度アンインストールして、再度同じコンピュータにインストールした場合は、インストール完了後に [ユーザ登録] 画面で、初回インストール時に取得した「ライセンスキー」を登録する必要があります。
ライセンスキーを忘れてしまった場合は、[ユーザ登録] 画面で再度[オンライン登録]ボタンをクリックして、ライセンスキーを再取得してください。

Q ウイルスバスター 2003 がインストールされたコンピュータの OS をアップグレードしても問題ないですか？

A ウイルスバスター 2003 をインストールしているコンピュータの OS をアップグレードする場合には、OS をアップグレードする前にウイルスバスター 2003 をアンインストールする必要があります。
万一ウイルスバスター 2003 をアンインストールせずに OS をアップグレードすると、ウイルスバスター 2003 が正常に動作しなくなるおそれがあります。この場合、問題の解決には OS の再インストールが必要になる場合もありますので、ご注意ください。

Q オンラインユーザ登録画面に接続できません

A オンラインユーザ登録を実行するには、お使いのコンピュータに Microsoft Internet Explorer 4.01 Service Pack 2 以上がインストールされている必要があります。お使いのコンピュータにインストールされている Web ブラウザのバージョンを確認してください。

Q ライセンスキーが登録できません

A ウイルスバスターのユーザ登録画面で、ライセンスキーを登録しようとすると、「ライセンスキー情報がお使いの環境と一致しません。」というメッセージが表示される場合は、まず正確に入力していただいたかどうかを確認してください。大文字と小文字も区別されますので、よくお確かめください。正しく入力しているにも関わらず、ライセンスキーを登録できない場合は、ウイルスバスター操作画面のユーザ登録画面から再度ユーザ登録を実行して、ライセンスキーを再取得してください。

アップデートに関する質問

Q [最新版にアップデート]が実行されません

A ウイルスバスター 2003 の操作画面で[最新版にアップデート]を実行してもアップデートできない場合、次の原因が考えられます。

■ ユーザ登録が完了していない
アップデート機能を利用するには、オンラインユーザ登録を完了する必要があります。操作画面の [ユーザ登録] 画面を開いて、シリアル番号、ライセンスキーを正しく入力してください。

■ ウイルスバスタークラブ会員の有効期間が終了している
ウイルスバスタークラブ会員の有効期間が終了している場合にも、アップデートを実行することができません。ウイルスバスタークラブ会員の有効期間を確認してください。

■ インターネット接続できない
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コンピュータがインターネットに接続している必要があります。インターネット接続に障害が発生している場合、ウイルスバスター 2003 ではアップデート処理を実行することができません。

■ プロキシサーバが正しく設定されていない
インターネット接続にプロキシサーバをお使いの場合、ウイルスバスター 2003 のプロキシ設定画面でプロキシサーバ情報を設定する必要があります。プロキシサーバ情報の設定方法については、98 ページを参照してください。

■ サーバが混雑している
ウイルス大量発生時などに、アップデートサーバへの接続が集中する場合に、サーバへ接続しづらくなる場合があります。このような場合には、しばらくお待ちいただいてから再度アップデートを実行してください。

操作 / 機能に関する質問

Q 体験版から製品版へ移行したいのですが ...

A シリアル番号を入力せずに、ウイルスバスター 2003 をインストールすると、ウイルスバスターは 30 日体験版としてインストールされます。体験版では、アップデート機能を利用することができません。また、30 日が経過すると、ウイルスバスター 2003 のすべての機能が使用できなくなります。
体験版から製品版へ移行するには、ウイルスバスター 2003 の[ユーザ登録]画面でシリアル番号を入力して、ユーザ登録を実行していただく必要があります。

用語集

圧縮ファイル	圧縮ファイルとは、ファイル圧縮ソフトを使用して作成されたファイルです。ネットワーク経由で送信するために大きなサイズのデータを縮小したり、複数のファイルを1つの小さいサイズのファイルにまとめるなどの用途で使われています。
アップグレード	「アップグレード」は、次の2つの意味で使用します。 ・ウイルスバスターの体験版から製品版に切り替えること ・旧バージョンのウイルスバスターから、新しいウイルスバスターに切り替えること ウイルスバスターが使用するパターンファイルや検索エンジンを新しいバージョンに更新することは、「アップデート」と呼んでいます。
アップデート	ウイルスバスターは、さまざまなウイルスの情報を登録したデータベースである「ウイルスパターンファイル」、ウイルスを見つけるためのプログラムである「検索エンジン」、そしてウイルスバスターのプログラム本体から成り立っています。 新しく発見されたウイルスを見つけるためには、新しいウイルスの情報を持つウイルスパターンファイル、新しいウイルスを見つけることのできる検索エンジンを使う必要があります。現在のパターンファイルや検索エンジンを、新しいものに更新することを、「アップデート」と呼んでいます。
インテリジェントアップデート	インテリジェントアップデート機能は、ウイルスパターンファイルや検索エンジンの最新版が公開されていないかどうかを自動的に確認して、最新版が見つかればお知らせする機能です。最新版が見つかると、アップデートを実行するかどうかを確認する通知が表示されます。
ウイルスパターンファイル (パターンファイル)	コンピュータウイルスには、人間の指紋のようにウイルスごとに特有の特徴があります。トレンドマイクロでは、このウイルスの指紋のことを「ウイルスパターン」と呼んでいます。ウイルスパターンファイルとは、ウイルスの「指紋」を集めたデータベースを意味します。

拡張子	拡張子とは、ファイルの種類を区分するためにファイル名の最後につける2～5つの文字のことです。たとえば、Microsoft Excelを使用して作成したファイルには、「.XLS」などの拡張子が付きます。拡張子を変更すると、元のアプリケーションを使用してファイルを開くことができなくなる場合があります。お使いのコンピュータの設定によっては、拡張子を表示しないように設定されている場合もあります。詳しくは、お使いのOSのマニュアルをご確認ください。
隔離	隔離とは、ファイルを隔離フォルダに移動する処理のことです。隔離フォルダは特別な処理が施されているため、フォルダ内でウイルスが実行されることはありません。隔離されたファイルは、特に必要がない場合は放置しておいても問題ありません。
救済ディスク	救済ディスクは、システム領域感染型ウイルスに感染した場合に、コンピュータのシステムを復旧するために使用するフロッピーディスクです。Windows 98/Meをお使いの場合にのみ、救済ディスク作成プログラムを使って作成することができます。
検索エンジン	検索エンジンとは、ウイルスバスター2003に組み込まれているウイルス検索専用のプログラムです。ウイルス検出の検出率、検索速度をさらに高めるために、トレンドマイクロでは、検索エンジンの改良を重ねています。最新のウイルス対策を実現するためにも、定期的に最新版へのアップデートを実行してください。
検索タスク	検索タスクとは、ウイルス検索する対象や、ウイルスが見つかった時の処理方法、ウイルス検索を実行する周期などを、1つの「仕事」として保存したデータのことです。検索タスクは、決められた周期で自動的に実行させたり、好きな時に手動で実行することもできます。
手動検索	手動検索は、いつでも好きな時に、クリック1つでウイルス検索を実行できる機能です。ウイルス感染が気になる不審なファイルが見つかったり、特定のフォルダ内をウイルス検索したい場合などに、手動検索を実行することができます。
シリアル番号	シリアル番号とは、ウイルスバスター製品に付属する固有の製品番号です。シリアル番号は、20桁の英数字から構成されています。ウイルスバスター2003のパッケージ (箱) を店頭などでお買い上げいただいた場合、シリアル番号はCD-ROMケースに記載されています。
タスクトレイ	タスクトレイとは、Windowsのデスクトップ画面の下のタスクバーの右端に表示される、IMEやボリューム調整のアイコンなどが表示されている部分のことです。 ウイルスバスター2003をインストールすると、コンピュータを起動するたびに、ウイルスバスター2003の起動をお知らせする「リアルタイムエージェント」アイコン がタスクトレイに表示されます。
体験版	体験版とは、ウイルスバスターに30日の使用制限がある状態のことです。シリアル番号を入力せずにウイルスバスター2003をインストールすると、体験版としてインストールされます。体験版では、アップデート機能を利用することができません。30日の期限が切れると、体験版を使用することができなくなります。30日を超えてお使いになる場合には、ウイルスバスター2003の製品版をお買い求めください。
ツールチップ	ウイルスバスター2003の画面上で、マウスのポインタを各オプションやメニュー、ボタンに近づけると、それぞれの機能について簡単な説明が表示されます。これを「ツールチップ」と呼んでいます。

トロイの木馬	「トロイの木馬」は、ファイルやシステムに感染しない不正プログラムの名称です。感染を目的とする不正プログラムをコンピュータウイルスと呼ぶ、従来のコンピュータウイルスの定義からは外れますが、ウイルスと同様にコンピュータに被害をもたらすものであるため、ウイルスバスター2003ではウイルスとして検出しています。
パーソナルファイアウォール	ファイアウォールとは、お客さまがお使いのコンピュータと、LANやインターネットなどのネットワーク間に設ける「防火壁」の役割を果たすものです。ネットワーク経由でコンピュータに送られるデータを、すべてこの「防火壁」を経由して受け取ることで、お使いのコンピュータへの不正アクセスを防ぐことができます。
プロキシサーバ	プロキシサーバとは、インターネット接続時のセキュリティ対策のために設置されているサーバです。ファイアウォールの内側にあるクライアントからアクセス要求 (HTTP、FTPなど) を受け付け、ファイアウォール外部への接続を許可する役目を果たしています。 プロキシサーバでは、インターネット接続時に取得されたデータをサーバ上に保存しています。次に同じファイルへのアクセスがあった場合は保存されたデータが読み込まれるため、インターネット接続のスピードの向上にもつながります。 企業ネットワークや一部のインターネットプロバイダでは、セキュリティと接続速度の高速化の2つの目的から、プロキシサーバを経由してインターネット接続するように設定している場合があります。
ポート番号	ポート番号とは、データ (パケット) の種類ごとに通り道を定めた「道路番号」のようなものです。コンピュータの各アプリケーション (メールソフトやWebブラウザなど) では、あらかじめ定められたポートを使用して、データを出入力しています。
メール検索	メール検索とは、インターネット上のメールサーバ (POP3) またはWebメールシステムからe-mailをダウンロードする際に、e-mailの添付ファイルにウイルスが含まれていないかを検索する機能です。e-mailがコンピュータ内に取り込まれる前の段階でウイルス検索され、ウイルスが見つかった場合は、適切な処理が実行されます。
ライセンスキー	ライセンスキーとは、ウイルスバスター2003のシリアル番号とは別に発行される、ウイルスバスター専用のパスワードのようなものです。シリアル番号を入力済みのウイルスバスター2003から、インターネット上のオンラインユーザ登録画面にアクセスして必要な情報を入力すると、ライセンスキーが発行されます。
リアルタイム検索	リアルタイム検索は、ファイルの読み込み/書き込みを常に (リアルタイムで) 監視し、ウイルスに感染しているファイルを見つけて、適切な処理を実行する機能です。コンピュータを起動すると、リアルタイム検索も有効になります。
リアルタイムエージェント	リアルタイムエージェントとは、Windows画面の右下のタスクトレイに表示される、ウイルスバスターのアイコンのことです。 リアルタイムエージェントのアイコンは、ウイルスバスター2003の状況に応じて表示が変わります。
ログ	ログとは、過去にどのようなウイルスが検出されたか、最新版へのアップデートはどれぐらいの周期で実行されているか、パーソナルファイアウォールが検出した情報に異常がないかどうかなど、過去の履歴情報を登録したものです。ログを確認することで、お使いのコンピュータのセキュリティ状態を確認することができます。

IPアドレス	IPアドレスとは、インターネットプロバイダなどから各コンピュータに割り当てられている、コンピュータの「住所」に相当する番号のことです。「192.162.10.1」のような4つのグループの数字で構成されています。お使いのインターネット環境によって、固定されたIPアドレスが割り当てられている場合と、インターネット接続のたびに異なるIPアドレスが割り当てられる場合があります。
URLフィルタ	URLフィルタは、Webサイトへのアクセスを制限することができる機能です。アクセス制限サイトを設定して、そのサイトにアクセスできないようにしたり、アクセス時に警告メッセージを表示するように設定することができます。
WebTrap（ウェブトラップ）	WebTrapは、Webサイトへのアクセス時に、Java、ActiveXなどのプログラム言語を使用して作成された害のあるプログラムのダウンロードをブロックして、お使いのコンピュータを守るための機能です。
Webメール	Webメールは、Webブラウザを使ってe-mailの送受信ができるサービスです。離れた場所からも気軽にアクセスできるため、利用が急速に拡大しています。Webメールシステムを使ってe-mailを受信した場合、添付ファイルはローカルのコンピュータにダウンロードして開くことになります。ウイルスバスター2003のWebメール検索機能では、添付ファイルのダウンロード時にウイルス検索を実行します。
ZIPクリーン	ZIPクリーンは、圧縮されたZIPファイルを解凍して、ウイルス検索、処理を実行した後に、再びファイルを元の圧縮された状態に自動的に復元できる機能です。通常のウイルス検索では、圧縮ファイルに格納されているファイルからウイルスが検出されても、ウイルスを駆除することはできません。

TREND MICRO

ウイルスバスター2003 リアルセキュリティ

はじめての
パーソナルファイアウォール

1 ファイアウォールって何だろう？

ファイアウォールとは？

ファイアウォールは、コンピュータと外部のネットワークの出入り口に設置される**見張り番**のことです。あなたがインターネットで Web ページをながめたり、メールをやりとりしたり、音楽やゲームのデータをダウンロードしている間にも、コンピュータにはさまざまなデータが出入りしています。

これらのデータの中には、コンピュータのトラブルを引き起こしたり、個人情報を盗むことを目的にした、悪質なデータが含まれている場合があります。ファイアウォールは、このような**悪質なデータの出入りをブロック**するために設置されます。

ファイアウォールは家庭用のコンピュータにも必要なの？

これまでファイアウォールは、企業の社内ネットワークシステムを守るために利用されるのが一般的でした。ところが最近では、家庭用のコンピュータにも、ファイアウォールを設置する動きが広まりつつあります。これは次の背景によるものと考えられます。

1. インターネット常時接続サービスの拡大に伴い、長時間インターネットに接続されているコンピュータが増え、不正にアクセスされる恐れが強まっている。

2. インターネットショッピングやオンラインバンキングなど、インターネットを利用したサービスの普及により、個人情報がネットワーク上でやりとりされる機会が増えている。

3. メールやチャット、掲示板などを利用して、見知らぬ相手とインターネット上で知り合うことにより、思わぬトラブルに巻き込まれる危険が増大している。

コンピュータに保存しておいた大切なデータを無断で書きかえられる、重要な個人情報が盗まれる「ハッキング」の犯罪に遭う、ネットワークに接続できなくなるような悪質ないやがらせを受ける...

インターネットの利便性と引き換えに、このような被害に遭わないようにするために、家庭内でご利用のコンピュータにも、企業でファイアウォールを設置するのと同様のセキュリティ対策が必要な時代になっているといえます。

ファイアウォールのしくみ

ファイアウォールは、通常のアクセスと不正アクセスとを、どうやって見分けているのでしょうか？

通常インターネットでやりとりされるデータは、**パケット**と呼ばれる小さな単位に分割されています。パケットには、データ本来の情報に加えて、***IP アドレス**や***ポート番号**など、たくさんの付随情報が含まれています。

ファイアウォールでは、あらかじめ設定されたルールに従って、パケットの中身を監視している。

ファイアウォールでは、どういうパケットを「**不正アクセス**」と判断するのか、あらかじめルールを決めておきます。このルールに基づいて、コンピュータとインターネットとの間でやりとりされるパケットの付随情報を調べたり、不正アクセス特有の動きがないかを監視します。ルールに違反するパケットがあれば、ブロックされます。

一方、ルールに登録されていないパケットについては、「**正常なアクセス**」とみなされ、ファイアウォールの通過が許可されます。

ウイルスバスター 2003 のパーソナルファイアウォールでは、どのようなパケットをブロックするか、ルールがあらかじめ設定されています。ルールの詳細については、136 ページの「**パーソナルファイアウォールがブロックするパケットの種類と解説**」を参照してください。

用語解説

***IP アドレス**…インターネットプロバイダなどから各コンピュータに割り当てられている、コンピュータの「住所」に相当する番号です。「198.162.10.1」のような 4 つのグループの数字で構成されます。

***ポート番号**…データ（パケット）の種類ごとに通り道を定めた、「道路番号」のようなものです。コンピュータの各アプリケーションでは、あらかじめ定められたポートを使用して、データを入出力しています。

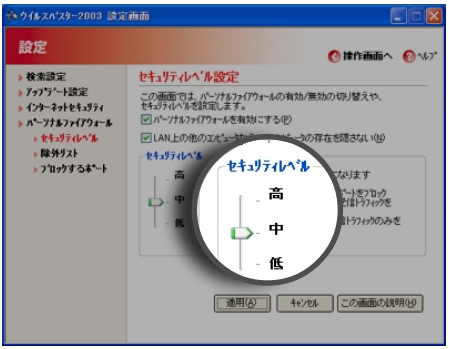
2 パーソナルファイアウォールの 5 つの特徴

特長 1. 選べる 3 つのセキュリティレベル

ウイルスバスター2003のパーソナルファイアウォールでは、セキュリティの強度に応じて「高」、「中」、「低」の 3 つのセキュリティレベルを使い分けることができます。

初期設定（セキュリティレベル「中」）では、通常のインターネット利用に必要なアクセスだけを許可し、それ以外のアクセスをブロックするように設定されています。さまざまな利用環境を考慮して設計されていますので、初期設定のままで安心なセキュリティ環境が実現します。

もちろん、より強力なセキュリティ環境を求める場合は「高」に、セキュリティをゆるめたいという場合には「低」に、というセキュリティレベルの調節も可能です。



初期設定では、最適な「中」レベルに設定されている

セキュリティレベル別ブロック対象一覧

ファイアウォールがブロックする対象は、セキュリティレベルに応じて、次の表のようになります。

ブロック/許可する対象	高	中	低
コンピュータ内部から外部への**送信**アクセス	ブロック ＊警告を表示	**許可**	許可
コンピュータ外部から内部への**受信**アクセス	ブロック	**ブロック**	許可
除外リストに登録された**送信**アクセス	許可	**ブロック**	-
除外リストに登録された**受信**アクセス	許可	**許可**	-
トロイの木馬が使用するポートを利用した**送受信**アクセス	ブロック	**ブロック**	ブロック
コンピュータに被害を与えたり、 不正アクセスにつながると判断されるパケット	ブロック	**ブロック**	ブロック

＊除外リストやトロイの木馬については、以降のページで詳しく解説します。

特長 2.「除外リスト」でアクセスコントロール

セキュリティレベルの設定に加えて、さらに細かくアクセスをコントロールしたいという、コンピュータの中、上級者向けのオプションとして、「**除外リスト**」の設定機能があります。

セキュリティレベル設定が「高」または「中」の場合、送受信アクセスが「ブロック」または「許可」されます（詳細については、前ページの表を参照）。これに対して、**例外ルール**を作成するのが除外リスト設定です。

除外リストの考え方

たとえば、セキュリティレベルが「中」の場合、外部からの受信アクセスがすべてブロックされます。しかし、実際にすべての受信アクセスをブロックすると、通常のインターネットアクセスや、メールの送受信までもがブロックされてしまうことになります。これを避けるために、ブロックしたくないアクセスの情報を**除外リスト**に追加します。

初期設定の除外リスト

初期設定の除外リスト項目について

初期設定の除外リストには、通常のインターネット接続に必要なアクセス情報が、あらかじめ登録されています。

たとえば「**Web サービス**」という項目は、Web ブラウザでインターネット Web サイトを閲覧するために必要な設定です。他にも、メールの送受信（SMTP/POP3）やファイル転送（FTP）などのアクセスが、ブロックされないように設定されています。

＊初期設定の除外リスト項目の詳細については、オンラインヘルプを参照してください。

除外リストの手動設定

パーソナルファイアウォールのインストール後、それまで利用していたネットワークアプリケーションがうまく使えなくなった場合などには、そのアプリケーションの情報を除外リストに追加して、ブロックから除外することができます。

除外リストを手動で設定する方法については、オンラインヘルプを参照してください。ネットワークアクセスに支障がない場合は、初期設定の除外リスト項目を変更せずにお使いいただくことをお勧めします。

特長 3. トロイの木馬をブロック

ハッカーがよく使う手口の 1 つに、「**バックドア型トロイの木馬**」という種類の不正プログラムを侵入先のコンピュータに仕掛けて、コンピュータを乗っ取るという手口があります。バックドア型のトロイの木馬がコンピュータに侵入すると、コンピュータの内部情報などが外部に向けて送信されます。

トロイの木馬ブロックの対象となるポートの一覧

パーソナルファイアウォールには、トロイの木馬が情報の送信ルートに使用するポートの情報があらかじめ登録されています。これらのポートを使用した送受信アクセスが発生した場合は、セキュリティレベル設定に関係なく、*すべてブロックされます。

> * **注意：**トロイの木馬が利用するポートが除外設定で「許可」されていた場合、除外設定が優先され、アクセスが許可されます。

特長 4. 不正アクセスにつながるパケットをブロック

ウイルスバスター2003のパーソナルファイアウォールでは、不正アクセスに利用されそうなパケットをブロックできるように、いくつかのルールがあらかじめ登録されています。

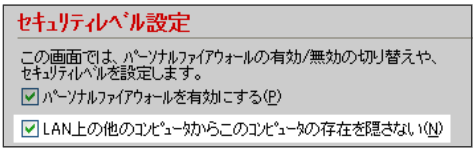
「**不正アクセスに利用されそうなパケット**」とは、たとえばコンピュータが処理不能におちいるような巨大なパケットや、ネットワーク接続状況をさぐるために送られたパケットなどが、それに当たります。

パーソナルファイアウォールの監視中にこれらのパケットが見つかると、セキュリティレベル設定に関係なく、すべてブロックされます。どのようなパケットがブロックされるのかという詳細については、136ページの「**パーソナルファイアウォールがブロックするパケットの種類と解説**」を参照してください。

特長 5. 利用環境に応じた設定機能

ウイルスバスター2003のパーソナルファイアウォールには、コンピュータの利用環境に応じた 2 つの設定機能があります。

LAN を利用している場合



LAN を利用している場合は、チェックをオンに

最近では、家庭内に複数台のコンピュータを設置して、プリンタやフォルダを共有する環境が増えています。

パーソナルファイアウォールで送受信アクセスをブロックすると、同一 ***LAN**（Local Area Network）上の他のコンピュータから、パーソナルファイアウォールがインストールされたコンピュータの存在が見えなくなり、プリンタやフォルダの共有設定も利用できなくなってしまいます。

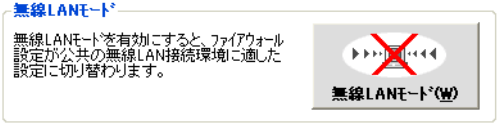
LANを使用している場合には、「**LAN上の他のコンピュータからこのコンピュータの存在を隠さない**」チェックをオンにすることで、プリンタやフォルダの共有設定を利用できるようになります。初期設定で、このチェックは有効に設定されています。

公共の無線 LAN 接続環境でコンピュータを利用する場合

駅やハンバーガーショップなどの公共の場所で、無線LANによるインターネット接続サービスを利用する機会が増えています。このときに心配なのが、他のコンピュータからの不正アクセスです。

ウイルスバスター 2003 の「**無線 LAN モード**」は、公共の無線 LAN 接続環境に最適なファイアウォール環境を提供する機能です。

家庭や企業など、通常のネットワーク環境でパーソナルファイアウォールを利用する場合、無線LANモードに切り替える必要はありません。



ボタンをクリックすると、無線 LAN モードになる（図は通常モード）

用語解説

***LAN**…ローカルエリアネットワーク（Local Area Network）の略で、家庭や企業などで数台のコンピュータ同士を接続して形成する、小規模ネットワークのことを意味します。

3 パーソナルファイアウォールのここが知りたい！

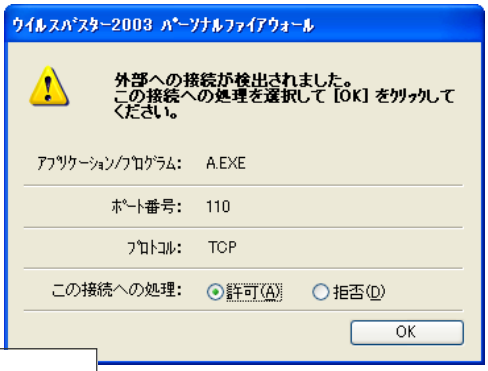
ここでは、ウイルスバスター2003のパーソナルファイアウォールを正しくご利用いただくために必要な、いくつかのヒントをご紹介します。

除外リストの設定方法がよくわかりません。自動的に設定する方法はありませんか？

除外リストの設定には、ネットワークに関する知識が必要です。アクセスをむやみに「許可」してしまうと、不正アクセスそのものを許可してしまうことにもつながりますので、除外リストは慎重に設定する必要があります。

セキュリティレベルを「**高**」に設定すると、コンピュータから外部への送信アクセスが発生した場合に、許可/拒否を選択する警告ダイアログが表示されるようになります。この機能を利用して、必要な送信アクセスだけが許可されるように、除外リストを自動設定することができます。

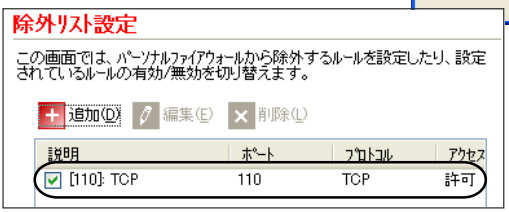
たとえば、セキュリティレベルが「高」の状態で、「**A.EXE**」というアプリケーションを利用するために、外部への送信アクセスを許可する必要があったと仮定します。A.EXEを実行すると、次のような警告ダイアログが表示されます。



外部への送信アクセスが発生！

右のダイアログは、**A.EXE**というアプリケーションで、**110**番のポートを通り、**TCP**プロトコルを使った送信アクセスが発生したことを意味します。

これを「**許可**」すると、アプリケーションの情報が除外リストに自動的に登録されます。



許可したアクセスの情報は、除外リストに自動追加される

* 「拒否」した場合、同一の送信アクセスが発生するたびに警告ダイアログが表示されます。
* 「アプリケーション/プログラム」には、何も表示されない場合があります。
* アクセスを「許可」する場合は、アプリケーション/プログラム名を確認して慎重に操作してください。

パーソナルファイアウォールの、最適なセキュリティレベルを教えてください。

初期設定のセキュリティレベルは「**中**」に設定されています。「中」レベルでは、コンピュータ内部から外部に向けた送信アクセスがすべて許可されます(除外設定されているアクセスはブロックされます)。

「中」レベルでも、十分効果的なセキュリティを実現することができますが、さらに強力なセキュリティを求める場合には「高」レベルに変更し、前ページで説明した除外リストの自動設定により、必要な送信アクセスだけを許可するように設定することもできます。

家庭で無線 LAN 環境を利用しています。この場合、無線 LAN モードに切り替えなければ、パーソナルファイアウォールを利用できないのですか？

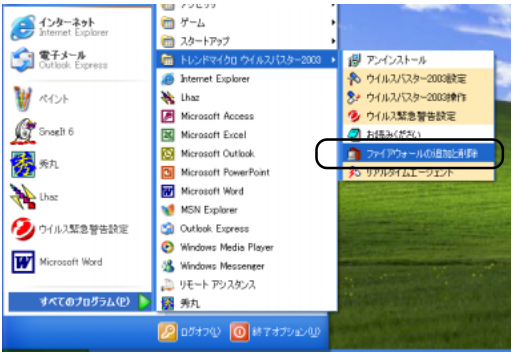
無線 LAN モードは、駅やハンバーガーショップなどの公共の場所で、無線 LAN によるインターネット接続サービスを利用する場合に適したファイアウォール機能です。

ご家庭などで無線LANルータなどを使ってインターネット接続している場合、**無線LANモードに切り替える必要はありません**。パーソナルファイアウォールは通常モードでご利用いただけます。

ウイルスバスター 2003 のパーソナルファイアウォールは、他社製のパーソナルファイアウォールと併用することができますか？

他社製のパーソナルファイアウォールとは、併用することができません。すでに他社製のパーソナルファイアウォールをご利用の場合には、ウイルスバスター 2003 をパーソナルファイアウォール機能抜きでインストールしてください。

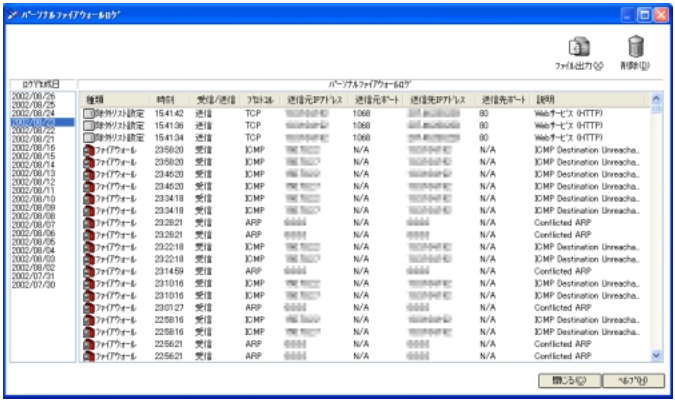
ウイルスバスター 2003 をすでにご利用の環境に、後から他社製のパーソナルファイアウォールをインストールする場合は、他社製品をインストールする前に、ウイルスバスター 2003 のパーソナルファイアウォールをアンインストールする必要があります。



[スタート] メニューから、パーソナルファイアウォールだけをインストール/アンインストールすることができる

ウイルスバスター 2003 のパーソナルファイアウォールが、実際にどんなアクセスをブロックしているかを調べたいのですが？

操作画面（プロフェッショナルモード）の [**ログ (履歴)**] 画面から、[**パーソナルファイアウォールログ**] を参照してください。パーソナルファイアウォールログ画面には、ブロックされたアクセスの情報が、日付ごとに一覧表示されます。



アクセス状況をログの「種類」から調べる

ログの「種類」には、次の 4 種類の情報が表示されます。

ファイアウォール：送受信のどちらかのアクセスが、セキュリティレベル設定に基づいてブロックされたか、または不正アクセスのブロック機能によってアクセスがブロックされたことを意味します。ブロックされたアクセスの詳細は、「**説明**」に表示されます。

HTTP ストリーム検索：HTTP ストリームの監視中に、CodeRed または Nimda によるアクセスがブロックされたことを意味します。ブロックされたアクセスの詳細は、「**説明**」に表示されます。

除外リスト設定：除外リストで「**拒否**」するように設定してあるアクセスが、ブロックされたことを意味します。「**説明**」には、該当した除外リストの項目名が表示されます。

トロイの木馬ブロック：「トロイの木馬ブロック」機能によって、アクセスがブロックされたことを示します。このログが表示される場合、トロイの木馬がコンピュータ内に侵入している可能性があります。トレンドマイクロのウイルス情報Webサイトなどを利用して、トロイの木馬に関する情報を調べることをお勧めします。

アクセス状況を「説明」から調べる

ログの「種類」が「**ファイアウォール**」または「**HTTP ストリーム検索**」の場合、「**説明**」にアクセスの詳細が記録されています。

■セキュリティレベル設定によるブロック

セキュリティレベルが「高」または「中」に設定されている場合には、送受信アクセスのどちらか（または両方）がすべてブロックされます。ログの「説明」に「**セキュリティレベル設定によるブロック**」と表示される場合、セキュリティレベルの設定に基づいて無条件にブロックされたアクセスを意味します。

■ICMP（Internet Control Message Protocol）プロトコルを使ったアクセス

セキュリティレベルに基づいて無条件にブロックされたアクセスのうち、***ICMP** というプロトコルを利用したアクセスについては、ログの「説明」に「**ICMP 〜**」という内容で記録されます。それぞれの意味については、オンラインヘルプを参照してください。

■不正アクセスにつながるパケットのブロック

パーソナルファイアウォールでは、不正アクセスにつながる可能性があるパケットをブロックするように、あらかじめ設定されています。この設定に基づいてパケットがブロックされた場合、ブロックされたパケット情報の詳細がログに記録されます。

ブロックされるパケットの種類については、136 ページを参照してください。

「アクセスブロック = 不正アクセス」ではない

ファイアウォールログに記録されたアクセスの情報は、あくまでもパーソナルファイアウォールによってアクセスがブロックされたことを示すものであり、**不正アクセスが発生したことを意味するものではありません。**

パーソナルファイアウォールは、不正アクセスにつながるおそれのあるアクセスを、あらかじめブロックするために設置するものです。設定をむやみに変更せずに、機能を正しくお使いいただいている限り、不正アクセスの被害に遭う危険を最小限におさえることができます。

用語解説

***ICMP**…Internet Control Message Protocol の略で、ネットワーク接続時に障害が発生した場合に、経路に位置するルータやコンピュータが、障害について送信元に報告するために使用するプロトコルです。

■パーソナルファイアウォールがブロックするパケットの種類と解説

ウイルスバスター2003のパーソナルファイアウォールでは、セキュリティレベル設定にかかわらず、次の種類のパケットをブロックします。これらのパケットは、不正アクセスにつながる可能性があるためブロックされます。「ブロック＝不正アクセスの発生」ではないことにご注意ください。

CodeRed（コードレッド）：2001年の夏、世界中で流行したCodeRedウイルスが、コンピュータのセキュリティホールを利用して侵入するのをパーソナルファイアウォールで検知し、未然にブロックします。

Conflicted ARP（コンフリクテッド アープ）：本来IPアドレスは同一ネットワーク上に1つしか存在しないはずですが、同一のIPアドレスを使用してIPアドレスの重複エラーを起こし、ネットワーク接続を妨害するいやがらせの一種です。

Fragmented IGMP（フラグメンテッド アイジーエムピー）：Windows 95/98が処理できない不正なIGMP(Internet Group Management Protocol)を使用したデータ（パケット）を送信して、受信したコンピュータのシステムを破壊するタイプの攻撃です。

LAND Attack（ランド アタック）：送信元と受信元のIPアドレスが同一という、理論的にはありえないデータ（パケット）を送りつけることで、受信元のコンピュータのシステムを混乱させ、処理速度の低下を引き起こすタイプの攻撃です。

NetBIOS（ネットバイオス）：NetBIOSサービスを使用して、ネットワーク上のコンピュータの存在を確認することを示します。ネットワークコンピュータの一覧を参照するだけでNetBIOSが検出されますが、この行為自体が「不正アクセス」というわけではありません。ネットワーク上のコンピュータの存在を他者に知られることが不正アクセスにつながる危険があるため、「不正アクセス」として検出しています。「LAN上の他のコンピュータからこのコンピュータの存在を隠さない」チェックを有効にしている場合、NetBIOSはブロックされません。

Nimda（ニムダ）：2001年の秋、世界中で猛威をふるったNimdaウイルスが、コンピュータのセキュリティホールを利用して侵入するのをパーソナルファイアウォールで検知し、未然にブロックします。

Ping attack（ピング アタック）：コンピュータに送られてきたPINGリクエストをすべて検出します。本来PING自体はネットワーク接続状況を確認するために用いられるプログラムですが、コンピュータがネットワークに接続されていることがわかると、不正アクセスを試みられる恐れがあるため、ブロックの対象になっています。このタイプのパケットが検出された場合、ログには「ICMP Echo Request」と記録されます。

Overlapping fragment attack（オーバーラッピング フラグメント アタック）：フラグメント化された受信パケットのペイロードを、他のフラグメント化された受信パケットのペイロードと重複（オーバーラップ）させることで、システムを不安定にしたり、破壊しようとする攻撃です。

Ping of death（ピング オブ デス）：PINGを使用して膨大なサイズのデータを送りつける攻撃の一種です。データを受信したコンピュータのシステムが、データを処理できずに破壊される危険があります。

Smurf（スマーフ）：詐称したIPアドレスを使用して複数のコンピュータに対して同時に接続要求を送りつけ、それぞれのコンピュータからの膨大な応答データが、実際にそのIPアドレスを持つコンピュータに送りつけられることにより、処理不能に陥るタイプの攻撃です。このタイプのパケットが検出された場合、ログには「ICMP Echo Reply」と記録されます。

Syn flood（シン フラッド）：詐称したIPアドレスを使用して、コンピュータが処理できないほどの大量の接続要求を送りつける攻撃の一種です。要求を送りつけたIPアドレスに応答しても、IPアドレスが詐称されているため「確認待ち」の状態が続きます。この「確認待ち」状態が続くと、正規の接続要求も受け付けられなくなり、ネットワーク接続ができなくなります。

Teardrop（ティアドロップ）：不完全なデータ（パケット）を送りつけ、コンピュータを処理不能の状態に陥れる攻撃の一種です。システムが不安定になったり、破壊される恐れがあります。

Tiny fragment attack（タイニー フラグメント アタック）：通常は使われないような非常に小さいデータ（パケット）を送信することで、データ処理エラーを引き起こすタイプのいやがらせの一種です。

Too big fragment（トゥー ビッグ フラグメント）：フラグメント化された受信パケットを再構成した後に、IPパケットの最大長である64Kオクテットを超えるパケットを送信するタイプの攻撃です。

Traceroute（トレースルート）：「traceroute」は、異なるコンピュータ間のネットワークのルートを見つけ出すプログラムです。ルートを見つける行為自体に危険はありませんが、見つけられたルートを利用してネットワーク接続が妨害されるなどの悪用が考えられます。このタイプのパケットが検出された場合、ログには「ICMP Traceroute」または「ICMP Echo Reply」と記録されます。

※パーソナルファイアウォールがブロックするパケットの種類は、追加、変更、削除される場合があります。

索 引