ご注意

1. 本ソフトウェアの著作権は、トレンドマイクロ株式会社および米国TREND MICRO 社にあります。
2. 本ソフトウェアおよびマニュアルの一部または全部を無断で使用、複製、レンタルすることはできません。
3. ソフトウェアは、コンピュータ１台につき１セット購入が原則となります。
4. 本ソフトウェアおよびマニュアルは、本製品の使用許諾契約書のもとでのみ使用することができます。
5. 本ソフトウェアおよびマニュアルを運用した結果の影響については、いっさいの責任をおいかねますのでご了承ください。
6. 本ソフトウェアの仕様、およびマニュアルに記載されている事柄は、将来予告なしに変更されることがあります。
7. 本マニュアルは、製品開発時に制作されています。したがって、本製品の仕様および画面は本マニュアルの記述と一部異なることもあります。ご了承ください。製品の仕様、操作の変更点についてはヘルプおよびReadMe ファイルをご参照ください。ご使用前にはCD-ROM 内のReadMe ファイルを必ずお読みください。
8. 本マニュアルは万全を期して制作いたしましたが、万一記載に誤りや不完全な点がありましたらご容赦ください。

動作環境

「ウイルスバスター 98」の動作環境は以下の通りです。

本体	Windows95またはWindows98が動作するPC/AT互換機、NEC PC-9801シリーズ、PC-9821シリーズ、PC-98NXシリーズ
CPU	i486DX2 66MHz以上（Pentium 100MHz以上を推奨）
メモリ	16MB以上（32MB以上推奨）
ハードディスク	12MBの空き容量が必要（インストール時）
OS	Windows95、Windows98
ソフトウェア	インターネット経由のアップグレード機能を使用するには、Internet Explorer、Netscape NavigatorなどのWebブラウザが必要（Internet Explorer 4.01以上を推奨）

WebTrap

WebTrap機能はHTTPプロキシサーバーとして動作します。使用するアドレスおよびポートは以下の通りです。

サーバー名	LOCALHOST
アドレス	127.0.0.1
接続ポート	8431

アクティブデスクトップとアクティブチャンネル

アクティブデスクトップとアクティブチャンネルを使用する場合は、以下のアイテムおよびチャンネルが表示されます。

アクティブデスクトップ	TREND MICRO JAPAN
アクティブチャンネル	VIRUS FORECAST

ウイルスバスター 98 へようこそ

「ウイルスバスター 98」のお買い上げありがとうございます。
本製品は Windows98 に完全対応し、マクロウイルスや不正 Java アプレットといった悪質なプログラムからコンピュータを守る、新世代のウイルス・セキュリティソフトウェアです。
また、「ウイルスバスター 98」は大幅な高速化を実現し、前バージョン「ウイルスバスター 97」に比べ、200% の高速化（当社比、ベンチマークテストによる）を達成いたしました。

インターネットが普及し、新しい技術が広まり、より便利になってきました。しかし、その反面、その技術を悪用し、他人のコンピュータをクラッシュさせたり、データを破壊したりするような事も増えているのです。
「ウイルスバスター 98」には、マクロウイルス対策には定評ある MacroTrap を搭載、不正 Java アプレットや不正 ActiveX コントロールといったインターネット・ウイルスへの対策としては、ダウンロードをブロックする WebTrap 機能を搭載し、危険なプログラムの実行を防止します。
また、従来からあるウイルスにも、既知のウイルス 12,000 種に対応し、新種のウイルスに対しては、インターネットから自動的に最新のウイルスパターン・ファイルおよびプログラムにアップデートして、防衛します。

弊社では、常に最新の技術を研究し、ウイルスやその他の不正なプログラムからコンピュータを守るための技術を開発しています。しかし、コンピュータや通信の技術革新が続くかぎり、新しい手口のウイルスや不正プログラムも開発されます。これらに対抗するためには、常に新しい技術を取り入れて対抗していくより他にはないのです。弊社は、全力でこの問題に取り組んでいきます。これからもトレンドマイクロ製品をよろしくお願いいたします。

目次

第1章　はじめに

本章では、「ウイルスバスター98」の特長、ウイルス対策ソフトウェアの役割、ウイルスおよびその他の不正プログラムについて説明します。

■ウイルスバスター 98 とは

「ウイルスバスター 98」は、Windows98 と Internet Explorer 4.0 に対応したウイルス対策ソフトウェアです。
「ウイルスバスター98」は、従来からあるウイルス以外に、不正 Java アプレットや、不正 ActiveX コンポーネントの実行をブロックする WebTrap 機能を備え、同時に大幅な高速化を達成いたしました。

ウイルスバスター 98 の特長

「ウイルスバスター 98」は、以下のような特長を備えています。

高速で軽快

「ウイルスバスター 98」では、リアルタイムでのウイルス動作監視部分と、手動によるウイルス検索機能を分離し、ウイルス動作監視機能だけをメモリに常駐し、ファイルおよびディスクに対するウイルス検索機能は必要なときに呼び出すように変更し、メモリ常駐量を減少させました。
また、プログラムの動作方法の見直しにより、前バージョン「ウイルスバスター 97」に比べ、200% の高速化（当社比、ベンチマークテストによる）を達成いたしました。

未知のマクロウイルスも発見する MacroTrap

近年になって著しく増加した、E-mail の添付ファイル等、E-mail 経由での感染が多いマクロウイルスも、定評ある MacroTrap を搭載し、未知のマクロウイルスも含め、確実にマクロウイルスを発見し駆除します。

不正 Java アプレットと不正 ActiveX コントロールをブロックする WebTrap

Internet ExplorerまたはNetscape Navigatorといった Webブラウザの使用中に、不正 Java アプレットと ActiveX コントロールのダウンロードをブロックする WebTrap 機能を提供します。

アクティブチャンネルによるウイルス情報

Internet Explorer 4.0 のアクティブデスクトップおよびアクティブチャンネルの「購読」機能を利用し、自動的にウイルス情報やウイルスパターン・ファイルのアップデート情報をお届けします。

インターネットでのアップデート

インターネットを利用されている場合、ウイルスパターン・ファイルだけでなく、プログラムもアップデートできます。
もちろん、BBS やフロッピーディスク、CD-ROM によるウイルスパターン・ファイル更新機能も搭載しています。

ユーザーインターフェース

ユーザーインターフェースを一新しました。新しくデザインされたインターフェースは、より洗練され、使いやすいものになりました。

圧縮ファイル、E-mail 添付ファイルへの対応

「ウイルスバスター 98」は、E-mail の添付ファイルや圧縮ファイルを開くことなく、添付ファイル内や圧縮ファイル内の各ファイルに対してウイルス検索をおこなえます。
「ウイルスバスター 98」は、以下の形式の添付ファイルおよび圧縮ファイルに対応しています。

対応圧縮形式	拡張子	補足
PKZIP	.ZIP	自己解凍形式も対応
ARJ	.ARJ	自己解凍形式も対応
LHA	.LZH	自己解凍形式も対応
TAR	.TAR	
GNU-ZIP	.ZIP	
UNIX-zip	.ZIP	
UNIX compress	.TAR	
MS-compress	.EX_ , .DO_ , .XL_	
PKLITE	.COM , .EXE	
LZEXE	.EXE	
DIET	.EXE	
Cabinet	.CAB	
メール添付形式	**拡張子**	**補足**
UUENCODE	.UU	メール添付ファイル
BINHEX	.HQX	メール添付ファイル
MIME		メール添付ファイル

ウイルス対策ソフトウェアとは

ウイルス検索の手法

現在、ウイルス対策ソフトウェアで使用されているウイルス検出の方法は「パターンマッチング方式」、「ルールベース法式」、「チェックサム方式」の３種類に大別されます。ウイルスバスター 98 では「パターンマッチング方式」によるウイルス検索と「ルールベース法式」によるリアルタイム検索機能を搭載しています。
それぞれのウイルス検出方法の特長は次のとおりです。

パターンマッチング方式

コンピュータ・ウイルスの特徴を示す一定のパターンのデータベースと照らし合わせて検索し、ウイルスと一致するパターンが検索対象内に発見された場合に、「ウイルス感染」と判定する方法です。この方法は、発見済みのウイルスに関しては、もっとも確実な方法です。しかし、この方法は、未発見のウイルスには対処できず、常に新しいデータベースを参照する必要があります。

ルールベース方式

メモリに常駐して、ウイルス特有の動作を監視します。システム領域や実行ファイルへの書き込み、メモリへの常駐といった、疑わしい動作をした場合に、「ウイルス感染」と判定する方法です。この方法は、ウイルス以外の「ロジック爆弾」や「トロイの木馬」といった、不正なプログラムの動作を止められる特長があります。しかし、「ルールベース法式」は、発見したウイルスが何かを判別できないため、ウイルスを駆除できません。「パターンマッチング方式」と併用して、ウイルスを特定し、駆除します。

チェックサム方式

プログラムやデータのチェックサムのデータを保存し、前回に保存したチェックサムと比較し、変更があった場合に、「ウイルス感染」と判定する方法です。
データファイルに感染するマクロウイルスの脅威が大きくなった現在では、あまり使われない方法です。

新種ウイルスとウイルスパターン・ファイル

「パターンマッチング方式」のウイルス検索に使用するコンピュータ・ウイルスの特徴を示す一定のパターンのデータベースを「ウイルスパターン」、このデータを格納したファイルを「ウイルスパターン・ファイル」といいます。このファイルを、常に最新に更新することで、新しいウイルスに対応できます。
「ウイルスバスター 98」は、インターネット経由で自動的にウイルスパターン・ファイルおよびプログラムをアップデートできます。
もちろん、インターネット以外でも、BBS あるいはフロッピーディスクからウイルスパターン・ファイルをアップデートできます。

WebTrap 機能

ネットサーフィンは、役に立ち、また楽しいものですが、中には悪意を持った Java アプレットや ActiveX コントロール(インターネット・ウイルス)を公開しているホームページもあり、そこにアクセスすると悪質なプログラムがダウンロードされ、実行されてしまうことがあります。
これらは、高いセキュリティを設定しておくことにより、ある程度まで回避できますが、高いセキュリティを設定しておくと、画像や動画が表示されなかったり、セキュリティの問い合わせが表示されてわずらわしいといったことで、ついセキュリティのレベルを下げてしまいがちです。
また高いセキュリティを設定していても、「OK」ボタンをクリックしてしまうと、不正なプログラムの侵入を許してしまうことになります。
これらの、悪意のあるプログラムに対しても、「ウイルスバスター 98」はプロキシサーバーとして動作する「WebTrap」を搭載し、不正なプログラムのダウンロードをブロックし、コンピュータへの侵入を許しません。

■ウイルスとは

コンピュータ・ウイルスはコンピュータ・システムに密かに感染して破壊活動をおこなうことを目的としたプログラムです。ウイルスは他のプログラムに自分自身のコードを付着させたり、ハードディスクのパーティション・テーブルやブートセクタに自分自身のコードを付着させて感染し、行動を起こすタイミングを待ち、特定の条件(例:13日の金曜日にウイルス感染したプログラムが起動されるなど)が成立すると、発病します。
無害なウイルスもありますが、ハードディスクやデータを破壊するものも少なくありません。

ウイルスの分類

ウイルスには多くの種類があります。また、それらは感染方法や感染先の違いからいくつかに分類できます。現在世界に存在しているMS-DOSウイルスは、8,000以上とも言われています。1986年の「パキスタン・ブレイン」からほぼ10年の間にそれだけの種類に増加したことは驚異的と言えます。また、PC以外では、Amigaのウイルスが約80種類、Macintoshのウイルスは約30種類確認されています。
ウイルスは、実行型プログラムファイルに感染する「ファイル感染型」とディスクのブートセクタなどに感染する「システム領域感染型」に大別されます。また、ファイルおよびシステム領域のいずれにも感染できる「複合感染型」やMicrosoft Wordの文書ファイルなどに感染する「マクロウイルス」も確認されています。
Windows 95の環境では、Windows 95が、MS-DOSとの互換性を持つため、MS-DOS用ウイルスの85%が動作するといわれています。

コンピュータウイルスの種類

コンピュータ・ウイルスは、感染する対象によって、以下のように分けられます。

システム領域感染型	フロッピーディスクやハードディスクのシステム領域に感染するウイルス。メモリに常駐するものが多い
ファイル感染型	ファイルに感染するウイルス。ほとんどのものは実行型のプログラムファイル（拡張子が.COM, .EXE, .SYS等のファイル）だけに感染する。マクロウイルスもデータファイルに感染するため、この分類に含まれることがある
複合感染型	システム領域とファイルの両方に感染するウイルス
マクロウイルス	ファイル感染型。一部のプログラムのデータファイルに感染するウイルス。マクロ言語などを利用するため、MacintoshとPCなど、異なるプラットフォームのコンピュータでも感染できる

感染方法により、以下のように分類されます。

上書き感染型	ファイル感染型。感染先のファイルのオリジナルデータを上書きして感染するウイルス。通常、駆除できない
直接感染型	ファイル感染型。感染ファイルを実行することで、他の未感染ファイルを探して直接的に再感染するウイルス。メモリには常駐しない
メモリ常駐型	ファイル感染型。感染ファイルを実行することで、ウイルスがメモリに常駐して、次に実行されるプログラム・ファイルに間接的に感染するタイプ。システム感染型ウイルスもメモリ常駐型に含まれる

ウイルスの特徴から分類する場合もあります。

ステルス型（メモリ常駐型）	ウイルス自身がユーザーやワクチンに発見されないように様々な工夫を凝らしたタイプ
ミューテーション型 ポリモーフィック型（メモリ常駐型）	ファイル感染型。感染する度に毎回異なった方法の暗号化をウイルス自身に施すタイプ。従来の検索型ウイルス・チェッカーでは発見が困難
ネットワーク型（ファイル感染型）	ネットワークＯＳのセキュリティ機能を突破してネットワーク環境内で感染できる。（システム感染型はネットワークを通じて感染出来ない）

ウイルスの感染を防ぐには

ウイルス対策ソフトウェアを使用する以外の方法では、コンピュータ・ウイルスの感染を完全に防止することは困難です。それでも、適切な対策を取ることで被害を最小限に抑えられます。そのため、ウイルスの感染を少しでも防ぐような対策をたてることが重要です。
次の方法を参考にしてください。

出所が不明なプログラムは使用しない。
出所が不明なフロッピーディスクは使用しない。
入手したプログラムは必ずウイルス検査をおこなう。
使っているコンピュータは、定期的にウイルス検査をおこなう。
コンピュータの利用状況を把握する。
また、ディスク全体のバックアップを作成しておくと、コンピュータ・ウイルスに感染したときに、ウイルス除去後の復旧作業が非常に楽になります。ただし、ウイルス感染前に作成したバックアップでないと意味がありませんので、定期的にウイルス検査とバックアップをおこなうことをお奨めします。

マクロウイルス

マクロウイルスとは、ワープロや表計算ソフトウェアのマクロ言語で作成され、文書やワークシートといったデータファイルに感染するウイルスです。
1995年8月に最初に発見されたマクロウイルスはMicrosoft Wordの文書に感染するものでした。以降、マクロウイルスの種類は増加する一方で、すでに数百種といわれています。また、感染する対象のデータファイルも Microsoft Excel、Lotus 1-2-3、AmiPro、Microsoft PowerPoint などに広がっています。
マクロウイルスは、それぞれのアプリケーションのマクロ言語で作成されているので、OSやCPUなどのプラットフォームには影響されません。ウイルスが作成されたアプリケーションさえあれば、どのコンピュータ上にも感染します。たとえば、Microsoft Wordのマ

クロウイルスは、 Microsoft Word が動きさえすれば、Windows、Macintosh を問わずに感染します。機種や OS に依存しないウイルスの出現は、ウイルスの脅威が新たな段階に入ったことを意味します。さらに、ウイルス本体がマクロであり、ウイルスの作成や改造がすべてアセンブラ(機械語)で書かれていた従来のウイルスに比べて容易なことが、マクロウイルスの種類が増大する一因となっています。

また、インターネットの E-mail の添付ファイルがウイルスに感染することで、短い時間で感染が広がります。

インターネット E-mail や、World Wide Web の普及によって世界中が結ばれて、簡単に文書ファイルが交換できるようになり便利になった反面、新しい形の危険にさらされているのです。

コンピュータ環境に新たな脅威をもたらしたマクロウイルスを、弊社では、従来のウイルスと区別する意味で、「第三世代ウイルス」と呼んでいます。

インターネット・ウイルス(第四世代型ウイルス)

インターネットの普及と、技術の発展により、Web ブラウザは単に HTML 文書を表示するだけでなく、Java アプレットや ActiveX コントロールといったプログラムが実行できるプラットフォームへと進化し、より便利になりました。

しかし、便利になった反面、まったく新しいタイプの悪意のある不正プログラムが出現しました。インターネットのサイトに、不正なプログラムを公開し、ユーザーがそのサイトに接続したとたんそのプログラムをユーザーのコンピュータに送り込み、破壊活動をおこないます。

しかも、そうしたウイルスは、Java アプレットや ActiveX コントロールで作成され、OS やコンピュータの機種を選びません。また、インターネットの仕組みを利用して潜伏するので、どこにでも移動できます。

また、これらの悪質なプログラムは、正規の方法で送信されるため、ファイアウォールを備えた企業ネットワークでも、その活動を防止できません。
これらの不正Javaアプレットと不正ActiveX コントロールを弊社では「第四世代ウイルス」または「インターネット・ウイルス」と呼んでいます。
第四世代ウイルスとして確認されているものとしては以下のようなものがあります。

Wasful.Java	実行するとCPUとメモリ・リソースを勝手に消費してしまう
Attackthreads.JAVA	黒いウィンドウでディスプレイを覆い、画面をブラック・アウトしてしまう
Ubgrateful.JAVA	電子メールのユーザーを偽造する
PenPal.JAVA	ユーザー名とパスワードを盗む

第2章　導入

本章では、「ウイルスバスター 98」のインストール方法と、起動方法について説明します。

■インストールとアンインストール

インストール前の準備

インストールするシステムの確認

インストールの前に、本マニュアルの「動作環境」を参照し、ご使用のコンピュータの確認をしてください。

フロッピーディスクの準備

「ウイルスバスター 98」はインストール時に、「救済ディスク」を作成します。「救済ディスク」の作成には、2HD のフロッピーディスクが 2 枚必要になります。インストール前にあらかじめご用意ください。

「救済ディスク」は、システム感染型のウイルスに感染したときに、システムを復旧するために使用するディスクです。

Web ブラウザのプロキシ設定のメモ

インストール時に「WebTrap 機能を使用する」を選択すると、「通常使用する Web ブラウザ」として設定されている Web ブラウザのプロキシ設定が変更されます。インストール前に、プロキシ設定を控えておくことをお薦めします。

「Internet Explorer」のプロキシ設定を確認する手順は以下の通りです。

1. ［スタートメニュー］→［設定］→［コントロールパネル］
とクリックしてコントロールパネルを開き、［インターネット］アイコンをダブルクリックして開きます。［インターネットのプロパティ］が表示されます。

2.［接続］タブをクリックし、［プロキシ　サーバー］の設定を確認します。
［プロキシサーバーを利用してインターネットにアクセス］のチェックボックスがオフになっている場合は、プロキシサーバーを使用していません。
［プロキシサーバーを利用してインターネットにアクセス］のチェックボックスがオンになっている場合は、［ポート］欄の数値を控えます。
また、［詳細］ボタンをクリックして表示される［プロキシ設定］画面の［サーバー］欄の［HTTP］の項目を控えます。
インストール後にインターネット接続が正しく動作しなくなった場合などに、このメモをもとにインストール前の設定に戻すことができます。
Internet Explorer 以外の Web ブラウザをお使いの場合は、それぞれのマニュアルまたはヘルプ等を参照しておいてください。

動作中の「ウイルスバスター」の終了

動作している「ウイルスバスター 97」あるいは以前のバージョンの「ウイルスバスター」などがある場合は、すべて終了させます。動作中の「ウイルスバスター」があると、インストールが正常におこなえない場合があります。

インストール

1. インストーラの起動

起動している他のプログラムがあれば、すべて終了してください。
CD-ROM をドライブに挿入します。自動的にメニューが起動します。メニューから［ウイルスバスター 98 のインストール］を選択します。
自動的にメニューが起動しない場合は、以下の手順でインストーラーを起動します。
［スタートメニュー］→［ファイル名を指定して実行］をクリックします。
［ファイル名を指定して実行］のウインドウが表示されます。
「名前」欄に以下のように入力し、［OK］をクリックします。

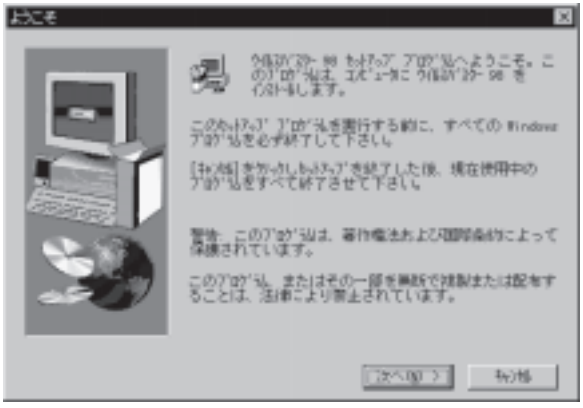
D（CD-ROM のドライブ名）:\VB98\Disk1\SETUP.EXE

2．旧バージョンのアンインストール

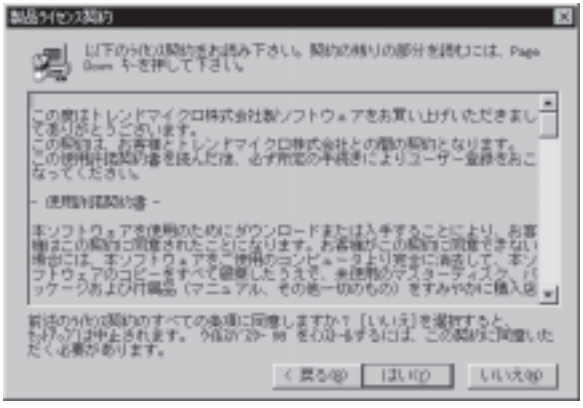
セットアッププログラムは以前のバージョンの「ウイルスバスター」を自動的に検索し、旧バージョンが見つかるとそのプログラムを自動的にアンインストールします。
旧バージョンを正常にアンインストールできなかった場合、インストールは中断されます。巻末の「トラブルシューティング」を参照して、再度インストールをおこなってください。

3. セットアップの開始とライセンス契約の確認

「ウイルスバスター98」のセットアップが開始され、［ようこそ］画面が表示されます。



［次へ］ボタンをクリックすると、［製品ライセンス契約］画面が表示されます。



ライセンスに同意し、インストールを続ける場合は［はい］ボタンをクリックします。［いいえ］ボタンをクリックするとインストールは中止されます。

4．ウイルス検索

［インストール前のウイルス検索］画面が表示され、自動的にインストール先ドライブのルートディレクトリ、Windows フォルダ、Microsoft Office フォルダのウイルス検索をおこないます。
ファイル感染型ウイルスが発見された場合、メッセージとともに「ウイルス駆除」、「ファイル名変更」、「ファイル削除」、「放置」の処理を選択する画面になります。選択した処理が終了すると、インストールが続行されます。
メモリ常駐型ウイルスが発見された場合、インストールは中止されます。本章の「インストール中にウイルスが発見された場合」の項目を参照し、ウイルスを駆除してから、再度インストールをおこなってください。

5. ユーザー情報の入力

ウイルス検索が終了すると、［ユーザの情報］画面が表示されます。

「名前」、「会社名」（個人で使用される場合は空白のままにします）、「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、同梱の「シリアル番号シール」を参照してください。シリアル番号は、半角の英数字で入力します。日本語入力システム(IME)が起動しているときは、オフにして入力します。

6. インストール先の選択

［インストール先の選択］画面が表示されます。

初期設定では、「C:\Program Files\ｳｲﾙｽﾊﾞｽﾀｰ98」にインストールされます。インストール先を変更する場合は、［インストール先のフォルダ］欄の［参照］ボタンでインストール先を選択できます。
［次へ］ボタンをクリックします。

7. プログラムフォルダの選択

［プログラムフォルダの選択］画面が表示されます。

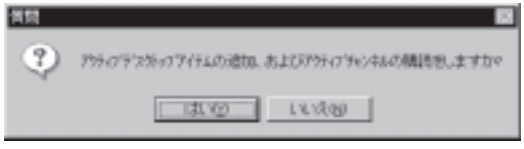
インストールするプログラムフォルダを選択するか、任意のフォルダを作成します。このとき、［スタートメニュー］フォルダは選択できません。
［次へ］ボタンをクリックします。

8．ファイルのコピー

ファイルのコピーが開始されます。コピーの進行状況は、棒グラフで表示されます。

9. アクティブデスクトップ・アイテムとアクティブチャンネルの設定

「TREND MICRO VIRUS FORCUST」をデスクトップに追加し、アクティブチャンネルの購読をおこなうかどうかを選択します。この機能を設定すると、弊社より、ウイルス関連情報が自動的に配信されます。
［はい］を選ぶと、それぞれのアイテムが追加されます。この機能はInternet Explorer 4.0がインストールされていて、アクティブデスクトップを使用する場合だけ有効になります。
［いいえ］を選ぶと、各アイテムの追加はされません。
この設定はインストール終了後に変更できます。



10. WebTrap の設定

WebTrapを使用するかどうか選択します。WebTrapを使用する場合は、［はい］ボタンをクリックします。

11. 救済ディスクの作成

救済ディスクを作成します。救済ディスクは、システム感染型のウイルスに感染したシステムを復旧するために使用します。
救済ディスクを作成するには、2HDのフロッピーディスクが2枚必要です。
救済ディスクは、インストール後に作成することもできます。
救済ディスクの作成方法は、本章の「救済ディスクの作成」の項目を参照してください。

12. インストールの終了

ファイルのコピーが終了すると、［セットアップの完了］画面が表示されます。

インストール終了後に、Readmeをすぐに表示する場合は、［はい、Readmeを今、読みます］のチェックボックスをオンにします。
Readmeには、マニュアルに記載されなかった事項や、注意事項について書かれています。チェックボックスをオンにして、Readmeをお読みになることをお薦めします。
インストール終了後、すぐに「リアルタイムモニタ」を起動する場合は、［はい、リアルタイムモニタを今、起動します］のチェックボックスをオンにします。
［終了］をクリックすると、インストールは終了します。

インストール時にウイルスが見つかった時は

「ウイルスバスター 98」のインストール中にファイル感染型ウイルスが発見された場合は、［ウイルス発見!］画面が表示され、ウイルス感染ファイルの処理をおこないます。

処理を選択して、［次へ］ボタンをクリックすると、ウイルス感染ファイルが処理されます。

［キャンセル］ボタンをクリックすると、インストールは中止されます。

インストール中にメモリ中にウイルスが発見された場合または、ウイルスの処理に失敗した場合は、インストールは中止されます。

インストールをおこなうには、ウイルスを駆除する必要があります。この場合、ウイルス駆除をおこなうにはパッケージに同梱された「駆除ディスク」が必要です。駆除方法の詳細は、駆除ディスク内の README.TXT を参照してください。

「駆除ディスク」を使用してウイルス駆除をおこなうには、ウイルス感染していない MS-DOS システムディスクと、作業用に使用するフォーマット済みのフロッピーディスク(2HD)1 枚が必要です。

なお、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ので、不明な点がありましたら、弊社サポートセンターにご相談ください。

なお、サポート窓口につきましては同梱「サポートサービスメニュー」をご覧ください。

アンインストール

ウイルスバスター 98 のアンインストールは、アンインストール・プログラムでおこないます。

1.「ウイルスバスター 98」の終了

「ウイルスバスター 98」と「リアルタイムモニタ」の起動中には、アンインストールはおこなえません。「ウイルスバスター 98」と「リアルタイムモニタ」を終了してからアンインストールを開始してください。
終了の手順は、本章の「起動と終了」の項を参照してください。

2. アンインストーラーの起動

［スタートメニュー］→［プログラム］→［ウイルスバスター 98］の［ウイルスバスター 98 のアンインストール］をクリックします。

3. アンインストールの確認

［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ます。［はい(Y)］を選択します。

4．アンインストールの実行

インストールされたファイル、フォルダ、スタートメニューの項目が削除され、変更されたシステム設定が元に戻されます。
以上でアンインストールは終了です。
アンインストールが終了したら、システムを再起動してください。
なお、アンインストーラーでは、ログファイルおよび、移動されたウイルス感染ファイルは削除されません。また完全にアンインストールされずにファイルやフォルダが残っている場合があります。このようなときには、アンインストール後、システムを再起動し、マイコンピュータやエクスプローラを使用して削除します。

■ユーザー登録について

インストールが終了したら、ユーザー登録をおこなってください。ユーザー登録は、同梱の「ユーザー登録ハガキ」またはインターネットによる「オンライン登録」で登録できます。なお、ユーザー登録はハガキまたはオンラインのどちらか一方だけでおこなってください。

オンライン登録の手順

「オンライン登録」をおこなうには、インターネット接続ができる環境と Web ブラウザが必要です。
オンライン登録をおこなう手順は以下の通りです。
［スタートメニュー］→［プログラム］→［ウイルスバスター 98］→［オンライン登録］をクリックするか、ウイルスバスター 98 のプログラムフォルダにインストールされた［オンライン登録］アイコンを開くと、Web ブラウザが起動し、［オンライン登録］ページが表示されます。
ダイアルアップ接続でご利用の場合は、［接続］ダイアログが表示され、インターネット接続後にページが表示されます。また、オンライン登録終了後、インターネットへの接続は自動では切断されませんので、ブラウザを閉じ、接続を終了してください。

■起動と終了（アンロード）

「ウイルスバスター 98」は、ウイルス検索プログラム「ウイルスバスター 98」と、ファイルの入出力時にウイルス検索をリアルタイムでおこなう「リアルタイムモニタ」、インターネットの接続時にインターネット・ウイルス(不正 Java アプレットおよび不正 ActiveX コントロール)のダウンロードをブロックする「WebTrap」の 3 つのプログラムで構成されます。
ここでは、それぞれのプログラムの起動と終了の方法を説明します。

起動

それぞれのプログラムの起動方法を説明します。

ウイルスバスター98

「ウイルスバスター98」の起動方法は以下の3種類です。

・［スタートメニュー］→［プログラム］→［ウイルスバスター98］の、［ウイルスバスター98］を選択します。
・タスクトレイの［リアルタイムモニタ］の「アイコン」を右クリックして、表示されたメニューから［ウイルスバスター98の起動］を選択します。
・クイック起動バーの「ウイルスバスター98」のアイコンをダブルクリックします。

リアルタイムモニタ

「ウイルスバスター98」をインストールすると、［リアルタイムモニタ］は次回のシステム起動時から自動的に実行されます。タイトル画面を表示し、タスクトレイに格納されます。
「リアルタイムモニタ」を手動で起動する場合は、［スタートメニュー］→［プログラム］→［ウイルスバスター98］の、［リアルタイムモニタ］を選択します。

WebTrap

「WebTrap」は、「ウイルスバスター98」で「使用する」に設定した後にWebブラウザを起動すると自動的に起動します。「WebTrap」を使用する場合は、リアルタイムモニタが動作していることが必要です。
「WebTrap」は［インターネット］設定画面で設定します。
ただし、インターネット接続中は、［インターネット］設定画面での設定変更はおこなわないでください。インターネット接続が切断されることがあります。

終了（一時停止）

それぞれのプログラムの終了方法を説明します。

ウイルスバスター 98

メイン画面の［終了］ボタンをクリックするか、右上のクローズボックスをクリックします。

リアルタイムモニタ

タスクトレイの「ウイルスバスター 98」のアイコンを、右クリックして表示されるメニューから、「リアルタイムモニタの終了」を選択します。プログラムは終了します。

一時停止

インターネットに接続して、「WebTrap」が動作している場合は、必ずブラウザをすべて終了し、接続を切断してからリアルタイムモニタを終了してください。
また、タスクトレイの「リアルタイムモニタ」のアイコンを、右クリックして表示されるメニューから、「リアルタイムモニタの停止」を選択すると、一時的にリアルタイムモニタを停止できます。リアルタイムモニタの停止中はリアルタイム検索をおこないません。ただし、予約検索、WebTrap、自動アップデートは動作します。

再開

停止した「リアルタイムモニタ」を再び実行するには、タスクトレイの「リアルタイムモニタ」のアイコンを、右クリックして表示されるメニューから、「リアルタイムモニタの再開」を選択します。

WabTrap

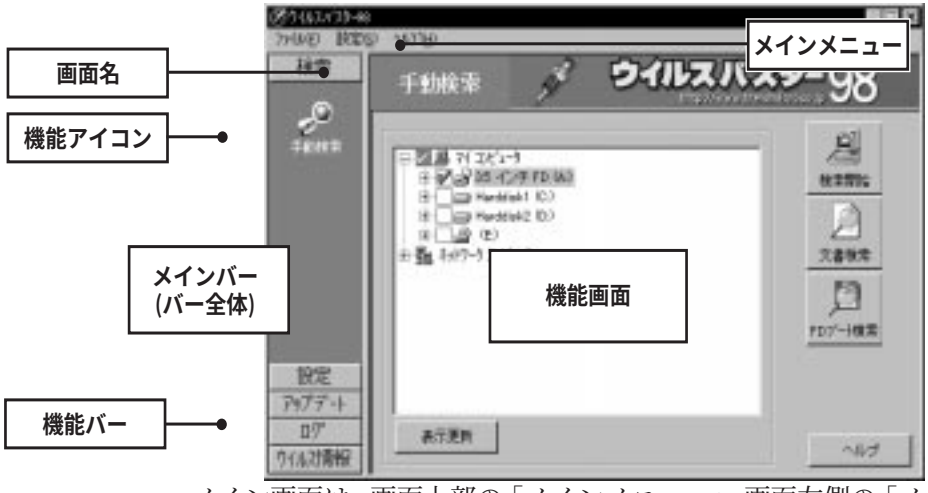
「WebTrap」は、「ウイルスバスター 98」の［設定］画面で「使用しない」設定にすると、Web ブラウザを起動しても動作しなくなります。Webブラウザの起動中にインターネットの設定変更をおこなったり、「リアルタイムモニタ」の終了はおこなわないでください。インターネットの接続が切断されるなど、正常に動作できなくなります。

■メイン画面の見方

ここでは、ウイルス検索プログラム「ウイルスバスター 98」の画面構成について説明します。

各部の名称

「ウイルスバスター 98」を起動すると、次のような画面が表示されます。
画面の各部の名称は以下の通りです。



メイン画面は、画面上部の「メインメニュー」、画面左側の「メインバー」、画面右側の「機能画面」に分けられます。

メインバー

［メインバー］は、実行する機能画面をすばやく選択するためのバーです。
［メインバー］には機能のグループを選択する［機能バー］と、グループ内から個別の機能を選択する［機能アイコン］があります。
［機能バー］を選択し、［機能アイコン］をクリックすると、それぞれの画面が表示されます。
何らかの設定を変更すると、「設定を保存しますか」という確認メッセージが表示されます。

機能画面

［メインバー］または［メインメニュー］で選択した画面が表示されます。
画面名は、左上隅の［画面名称］欄に表示されます。
画面構成は各機能画面によって異なります。画面の内容は、各機能の項目で説明します。

メインバーの設定

［メインバー］に表示されている［機能アイコン］のサイズを変更できます。
［メインバー］のエリア内で右クリックすると、「Large Size」「Small Size」というメニューが表示されます。使用したい［機能アイコン］のサイズを選択します。
［機能アイコン］のサイズは［機能バー］ごとに設定します。
［機能アイコン］をドラッグ & ドロップすることで、［機能バー］内での並びを変更できます。また、［機能バー］とメイン画面の境界はドラッグして左右に移動できます。
これらの機能は、起動するたびに設定する必要があります。

■ヘルプの使い方

「ウイルスバスター98」には各画面に［ヘルプ］ボタンがあります。［ヘルプ］ボタンをクリックすると、その画面のヘルプが表示されます。
［ヘルプ］メニューの［ウイルスバスター98のヘルプ］を選択するか、［トピックの検索］を選択しても、ヘルプを参照できます。

ウイルスパターン・ファイルと検索エンジンの表示

［ヘルプ］メニューの［バージョン情報］を選択すると、［バージョン情報］画面を表示します。

「ウイルスバスター98」のバージョン情報、ライセンスとシリアル番号、リソースの情報、ウイルスパターン・ファイルと検索エンジンのバージョン情報を表示します。

トレンドマイクロ Web ページの表示

［ヘルプ］メニューの［トレンドマイクロ Web ページ］を選択すると、自動的に Web ブラウザが起動し、トレンドマイクロのサイトが表示されます。この機能を使用するには、インターネットに接続ができ、Web ブラウザが使用できる環境が必要です。

■救済ディスクについて

救済ディスクは、システム感染型のウイルスに感染したシステムを復旧するために使用します。
救済ディスクは、インストール時に作成しますが、インストール後に作成することもできます。
Windowsがプリインストールされた機種の一部では、救済ディスクの作成に失敗するものがあります。救済ディスクの作成に失敗した場合は、巻末の「トラブルシューティング」を参照してください。

フロッピーディスクの準備

救済ディスクを作成するには、2HDのフロッピーディスクが2枚必要です。
それぞれのディスクに同梱の「起動用ディスク」「検索用ディスク」のラベルを貼ります。
フロッピーディスクは、自動的にフォーマットされます。フォーマット済みのディスクを使う必要はありません。

救済ディスクの更新

OSのアップグレードをおこなった場合など、システムに変更を加えた場合は、救済ディスクを新しく作り直す必要があります。システムに変更を加えた後に、元の救済ディスクを使用してシステムを復旧すると、システムに重大な損傷を与え、ハードディスクにアクセスできなくなります。
特にWindows95からWindows98にアップグレードした場合は、必ず救済ディスクを作り直してください。

旧製品の救済ディスク

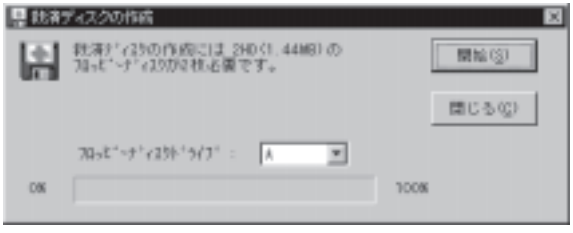
ウイルスバスター 95 / 97 で作成した救済ディスクは、「ウイルスバスター 98」では使用できません。
必ず「ウイルスバスター 98」で救済ディスク新しく作成して使用してください。
ウイルスバスター 95 / 97 の救済ディスクを使用した場合、システムに重大な損傷を与え、ハードディスクにアクセスできなくなります。

救済ディスクの作成方法

救済ディスクの作成手順は以下の通りです。

1 救済ディスクの作成プログラムの起動 .

[スタートメニュー]→[プログラム] →[ウイルスバスター 98] →[救済ディスクの作成]と選択します。
救済ディスクの作成プログラムが起動します。



フロッピーをドライブに入れ、ターゲットドライブ欄でフロッピーディスクドライブを選択し、 [開始] ボタンをクリックします。

2. 検索用ディスクのフォーマット

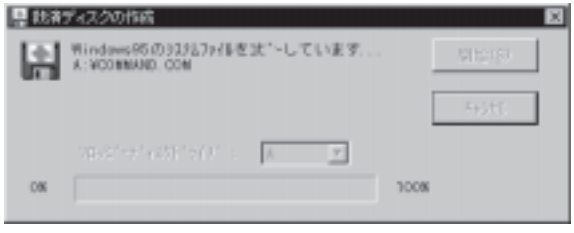
検索用ディスクのフォーマットをおこないます。
ドライブに検索用ディスクをセットし、[はい]ボタンをクリックします。

フォーマット開始画面が表示されます。
フォーマットしていないディスクの場合は、「フォーマットの種類」に「通常のフォーマット」を、フォーマット済みのディスクの場合は「クイックフォーマット」を選び、[開始]ボタンをクリックします。「ボリュームラベル」欄は入力する必要はありません。

3. 起動用ディスクの作成

検索用ディスクのフォーマットが終了すると、続いて起動用ディスクを作成します。

ドライブに起動用ディスクをセットし、[OK]ボタンをクリックします。検索用ディスクと同じ手順でフロッピーディスクをフォーマットします。フォーマットが終了すると、起動ディスクに必要なファイルをコピーします。



ファイルのコピーの進行状況は、ウインドウ下のバーで表示されます。

4. 検索用ディスクの作成

起動用ディスクの作成が終了すると、次の画面が表示されます。
ディスクをドライブから取り出して、ライトプロテクトをかけます。

検索用ディスクをドライブにセットし、[OK]ボタンをクリックします。
ディスクに必要なファイルをコピーします。
ファイルのコピーの進行状況は、ウインドウ下のバーで表示されます。
ファイルのコピーが終了すると、検索用ディスク作成終了のメッセージが表示されます。
ドライブから取り出して、ライトプロテクトをかけます。
これで、救済ディスクの作成は終了です。

PC-9801 / PC-9821 シリーズの救済ディスクの作成方法

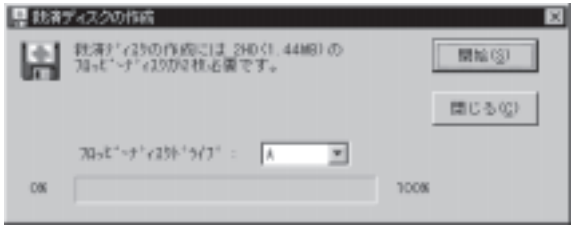
救済ディスクを作成するには、フォーマット済みの 2HD のフロッピーディスクが 2 枚必要です。

1. 起動ディスクの作成

フロッピーディスクの 1 枚は、Windows95 または Windows98 の起動ディスクを作成します。
Windows の起動ディスクの作成の手順は以下の通りです。
1.[スタートメニュー]→[設定]→[コントロールパネル]でコントロールパネルを開き、[アプリケーションの追加と削除]を開きます。
2.[起動ディスク]タブをクリックして [起動ディスク]画面を表示し、[ディスク作成] をクリックします。
起動ディスクが作成されます。
このディスクに同梱の「起動用ディスク」のラベルを、もう 1 枚のディスクに「検索用ディスク」のラベルを貼ります。

2. 救済ディスクの作成プログラムの起動 .

[スタートメニュー]→[プログラム] →[ウイルスバスター 98] →[救済ディスクの作成]と選択します。
救済ディスクの作成プログラムが起動します。



ターゲットドライブ欄でフロッピーディスクドライブを選択し、[開始] ボタンをクリックします。

3. 起動用ディスクの作成

起動用ディスクを作成します。

ドライブに起動用ディスクをセットし、[OK]ボタンをクリックします。
起動ディスクに必要なファイルをコピーします。

ファイルのコピーの進行状況は、ウインドウ下のバーで表示されます。

4. 検索用ディスクの作成

起動用ディスクの作成が終了すると、次の画面が表示されます。
ディスクをドライブから取り出して、ライトプロテクトをかけます。

検索用ディスクをドライブにセットし、[OK]ボタンをクリックします。
ディスクに必要なファイルをコピーします。
ファイルのコピーの進行状況は、ウインドウ下のバーで表示さ
ファイルのコピーが終了すると、メッセージが表示されます。
ドライブから取り出して、ライトプロテクトをかけます。
これで、修復ディスクの作成は終了です。

第3章　リアルタイム検索

本章では、ファイルの入出力時にリアルタイムでウイルス検索を行なう、「リアルタイムモニタ」について説明します。

■リアルタイムモニタとは

「リアルタイムモニタ」は、ファイルの入出力時にリアルタイムで自動的にウイルス検査をおこないます。この機能により、ウイルスを常に監視し、コンピュータへの侵入を防止できます。

■リアルタイムモニタの起動・一時停止・終了

「ウイルスバスター 98」をインストールすると、次回のシステム起動時より「リアルタイムモニタ」が自動的に起動し、タスクトレイに格納されます。

起動

通常は、Windows 起動時に自動的に起動されます。
「リアルタイムモニタ」を自動的に起動していない場合や、なんらかの理由で終了した場合に起動する手順は以下の通りです。
［スタートメニュー］→［プログラム］→［ウイルスバスター 98］の［リアルタイムモニタ］をクリックします。

一時停止と再開

「リアルタイムモニタ」を停止するには、タスクトレイの［リアルタイムモニタ］アイコンを右クリックすると表示されるメニューから、［リアルタイムモニタの停止］を選択します。
リアルタイムモニタを一時停止すると、リアルタイム検索はおこないませんが、予約検索、WebTrap、自動アップデートは動作します。
一時停止した検索を再開するときは、タスクトレイの［リアルタイムモニタ］アイコンを右クリックし、［リアルタイムモニタの再開］を選択します。

リアルタイムモニタの状態は、以下のアイコンで示されます。

 　リアルタイムモニタ実行中

 　リアルタイムモニタ停止中

終了

「リアルタイムモニタ」を終了させるには、タスクトレイのアイコンを右クリックし、表示されたメニューから［リアルタイムモニタを終了］を選択します。

■リアルタイムモニタの設定

「リアルタイムモニタ」の検索対象、ウイルス感染ファイルの発見時の処理を設定します。

リアルタイム検索設定画面の表示

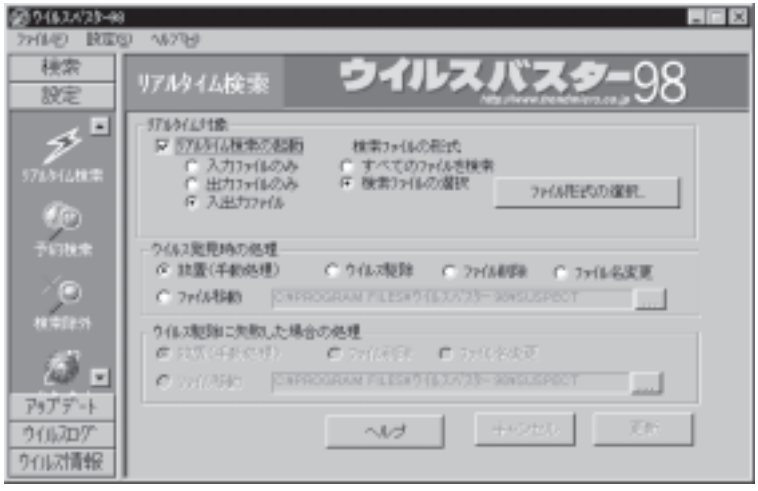
「リアルタイムモニタ」の設定は、ウイルス検索プログラム「ウイルスバスター 98」の［リアルタイム検索］設定画面でおこないます。［リアルタイム検索設定］画面の表示方法は以下の通りです。

1.「ウイルスバスター 98」の起動

タスクトレイの［リアルタイムモニタ］アイコンを右クリックして表示されるメニューから、［ウイルスバスター 98 を起動］を選択し「ウイルスバスター 98」を起動します。

2.［リアルタイム検索］設定画面の表示

［設定］バーの［リアルタイム検索］アイコンをクリックします。
または、［設定］メニューの［リアルタイム検索］を選択します。
［リアルタイム検索］設定画面が表示されます。



設定を変更したら、［更新］ボタンをクリックして、設定を保存します。
［キャンセル］ボタンをクリックすると、設定を保存せずに前の設定に戻ります。

リアルタイム検索の初期設定

リアルタイム検索は、「ウイルスバスター 98」の導入時には、以下のように設定されています。

監視対象	すべての入出力ファイル
ウイルス発見時の処理	放置（手動処理）

リアルタイム検索の検索設定

［検索指定］欄では、リアルタイムの起動（＝ ON）、検索対象、検索するファイル形式などを設定します。

検索指定欄	内容
リアルタイム検索の起動	このチェックボックスをオンにすると、リアルタイムでウイルス検索をおこないます。
入力ファイルのみ	ディスクなどから読込むファイルを検索します
出力ファイルのみ	ディスクなどに書込むファイルを検索します
入出力ファイル	入力・出力ファイルをともに検索します
検索ファイルの形式欄	**内容**
すべてのファイルを検索	全てのファイルをウイルス検索します
選択したファイル を検索	選択した拡張子のファイルだけをウイルス検索します。
［ファイル形式の選択］ボタン	選択した拡張子のファイルだけをウイルス検索する場合に、拡張子の選択画面を表示するボタンです。「ファイル形式の選択」の操作手順は次の項目を参照してください。

ウイルス検索対象の設定

コンピュータ・ウイルスは全てのファイルに感染するわけではありません。画像ファイルなど、ウイルス感染しないファイルもあります。ウイルスは、基本的に実行可能な種類のファイルに感染します。「ウイルスバスター 98」は、特定の拡張子のみを指定してウイルス検索をおこなえます。

［すべてのファイルを検索］と［検索ファイルの選択］のどちらかを選択します。［検索ファイルの選択］では、「ウイルスバスター 98」の初期設定では、以下のファイルをウイルス検索します。

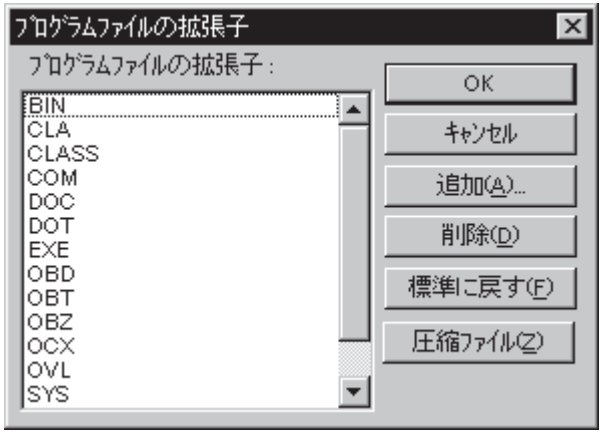
拡張子	.BIN , .CLA , .CLASS , .COM , .DOC , .DOT, .EXE , .OBD, .OBT , .OBZ , .OCX, .OVL , .SYS, .XLS , .XLT

システム領域の検索の設定

［システム領域の検索］のチェックボックスをオンにすると、パーティションテーブル及びブートセクタに対してウイルス検索します。

検索するファイル形式の変更

［検索ファイルの選択］を選択した場合、検索するファイル形式を変更するには以下の手順でおこないます。
［検索設定］画面で、［検索ファイルの選択］を選択し、［ファイル形式の選択］ボタンをクリックします。
［プログラムファイルの拡張子］画面が表示されます。



OK	変更した設定を保存して検索設定画面に戻ります。
キャンセル	変更した設定を保存しないで、検索設定画面に戻ります。
追加	［追加］ボタンをクリックすると、「追加する拡張子」画面が表示されます。［追加する拡張子］欄に半角英数文字で３文字の拡張子を入力し、［OK］ボタンをクリックします。
削除	指定した拡張子を削除します。「プログラムファイルの拡張子」欄から削除する拡張子を選択し、［削除］ボタンをクリックします。
標準に戻す	検索するファイル形式を初期設定に戻します。
圧縮ファイル	検索をおこなうファイルに圧縮ファイルの拡張子を追加します。

設定が終了したら、[OK] ボタンをクリックして、[検索設定] 画面に戻ります。
設定の変更は、次回の検索から有効となります。
検索ファイル形式の拡張子は、少なくとも１種類は指定してください。指定がなければ検索は実行できません。

圧縮ファイルの検索の設定

[圧縮ファイルの検索] ボタンをクリックすると、検索するファイルの拡張子に、圧縮ファイルの拡張子が追加されます。
[圧縮ファイルの検索] ボタンをクリックして追加される、検索可能な圧縮ファイルは以下の通りです。

圧縮形式	検索対象の拡張子	その他
ZIP (ZIP 2互換) GNU ZIP UNIX ZIP	.ZIP	パスワード指定がある場合は検索できません
LZH (LHA 2.1x互換)	.LZH	
Cabinet	.CAB	
LZEXE	.EXE	
MS-COMPRESS	.CO_, .EX_, .DO_, .XL_	圧縮前の拡張子は .COM ,.EXE ,.DOC ,.XLS

圧縮ファイル内の圧縮ファイルを検査することが可能です。2段階の圧縮まで対応しています。
また、圧縮ファイル内にウイルス感染ファイルを発見した場合、圧縮ファイルに対してはウイルスの処理をおこなえません。一度圧縮ファイルを解凍してからウイルスの処理をおこなってください。
圧縮形式のバージョンによっては、検査できない場合があります。

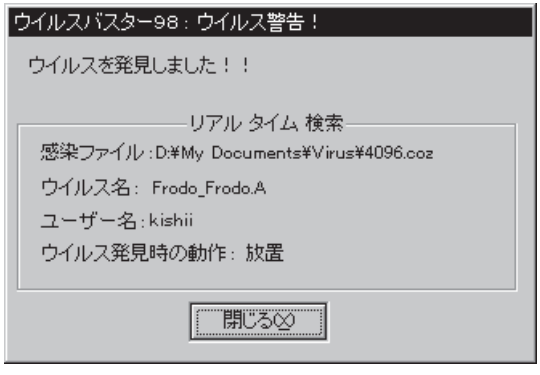
なお、追加される圧縮ファイル以外に、以下の形式に対応しています。

圧縮形式	その他
PKLITE	拡張子は .COM , .EXE
TAR	拡張子は.TAR
UNIX Compress	
エンコード形式	
UUEncode	
MIME	暗号化されている場合は対応しません。
BinHex	

これらの形式のファイルを検索する場合は、対応する拡張子(特定の拡張子がない形式もあります)を入力するか、あるいは「すべてのファイルを検索」を選択します。

ウイルス感染ファイルの処理の設定

［ウイルス発見時の処理］欄では、リアルタイム検索によって発見された感染ファイルの処理方法を指定します。
ウイルスが発見されると、以下のような画面が表示されます。



ウイルス感染ファイルの処理に［放置］が指定されている場合は、ファイルの処理はおこなわれません。ただし、ファイルのオープンといった処理は実行されず、ウイルス感染の拡大は止められます。

それ以外の、［ファイル削除］、［ウイルス駆除］、［ファイル移動］、［拡張子変更］が選択されている場合は、自動的に処理が実行され、処理がおこなわれたことをユーザーに報告します。

ウイルス発見時の処理

以下の 5 種類の処理から選択します。

放置	ウイルスに対して処理をおこないません。 ただし、ファイルのオープンといった実行しようとした処理は実行できません。
ウイルス駆除	ファイルからウイルスを取り除きます。ファイルからウイルスを駆除できなかった場合は、次の「駆除失敗時の処理」にしたがって、処理をおこないます。
ファイル削除	ウイルス感染ファイルそのものを削除します
拡張子変更	ウイルス感染ファイルの拡張子を変更して、実行不可能にします。 リネームをおこなうと、拡張子が「.VIR」に変更されます。拡張子が.VIRで同名のファイルが既にある場合には、.V01にリネームされます。.V01が既にある場合には、.V02となります。（.V99まで）
ファイル移動	ウイルス感染ファイルを指定したフォルダに移動します。初期設定では移動先のフォルダ名は、"C: \Program Files\ウイルスバスター98\SUSPECT"です。

ウイルス発見時の自動処理使用時の注意

［ウイルス駆除］、［ファイル削除］、［拡張子変更］、［ファイル移動］の自動処理は、システムファイルや重要なファイルであっても処理を実行し、中止できません。
これらの処理は自動処理が実行されても安全であることをご確認のうえ、設定してください。
安全かどうかわからない場合は、［放置］を選択し、ウイルス発見後に「ウイルスバスター 98」の手動検索で感染ファイルを処理することをお薦めします。

感染ファイル移動先の指定時の注意

移動先のフォルダには、フロッピーなどの交換可能なメディアおよびネットワークドライブを指定しないでください。
移動先のフォルダが書込み禁止などの理由で、移動ができない場合、ウイルス・ログには、「移動に失敗しました」と記述されます。

ウイルス駆除に失敗したときの処理の設定

ウイルスを発見し、「ウイルス駆除」をおこなったときに、何らかの理由でそのウイルスを駆除できなかった場合におこなう処理を設定します。
上書き感染型ウイルスのように、感染時にもとのファイルを破壊するウイルスや、変種や亜種のウイルスなどは、発見できても駆除できない場合があります。
こういった場合におこなう処理を「放置」、「ファイル削除」、「拡張子変更」、「ファイルの移動」から選択します。
それぞれの処理については「ウイルス発見時の処理」を参照してください。なお、「ファイル放置」を選択すると、「ウイルス発見」のログが残る以外、感染ファイルに対してなにもしません。

■リアルタイム検索のログ

リアルタイム検索について、発見されたウイルスおよびウイルス感染ファイルについての記録（ウイルス・ログ）が作成されます。
検索ログは、ウイルス検索で発見されたウイルス感染ファイルを記録します。
リアルタイムの検索ログの内容を参照するには、「ウイルスバスター 98」を起動して、［ログ表示］バーの［ログ表示］アイコンをクリックします。
［ログ表示］画面が表示され、「ウイルスバスター 98」が起動した時点のログファイルが表示されます。
「ウイルスバスター 98」がすでに起動していた場合は、［ログ表示］画面で［更新］ボタンをクリックします。
ログの管理については「第9章　ログファイル」を参照してください。

第4章　ウイルス検索

本章では、ファイル・フォルダ・ドライブに対するウイルス検索プログラム「ウイルスバスター 98」について説明します。

■ウイルス検索プログラム「ウイルスバスター 98」とは

「ウイルスバスター 98」のウイルス検索プログラムは、ファイルとドライブに対してウイルス検索をおこないます。
本マニュアルでは、このウイルス検索プログラムを「ウイルスバスター 98」といいます。
「ウイルスバスター 98」をインストールすると、「リアルタイムモニタ」が動作し、ウイルスの感染、感染ファイルの侵入を防止します。しかし、何らかの理由で「リアルタイムモニタ」を停止している時にファイルがコピーされた場合などはウイルス感染の可能性が残ります。
このような場合、あるいは新しいウイルスパターン・ファイルに更新したときに、「ウイルスバスター 98」を使用してファイルやドライブに対してウイルス検索をおこないます。
また、フロッピー、MO、CD-ROM などのメディアを新しく入手した場合や、他人にメディアを渡す前のウイルスチェックに「ウイルスバスター 98」の手動検索を使用します。
ウイルス検索は、「ウイルスバスター 98」の［手動検索］画面でおこないます。

■「ウイルスバスター 98」の起動

「ウイルスバスター 98」を起動するには、「スタートメニュー」から起動する方法と「タスクトレイ」の「リアルタイムモニタ」および「クイック起動ツールバー」から起動する方法の 3 種類があります。それぞれの起動方法について説明します。

スタートメニュー

［スタートメニュー］→［プログラム］→［ウイルスバスター 98］→［ウイルスバスター 98］の順にクリックします。

リアルタイムモニタからの起動

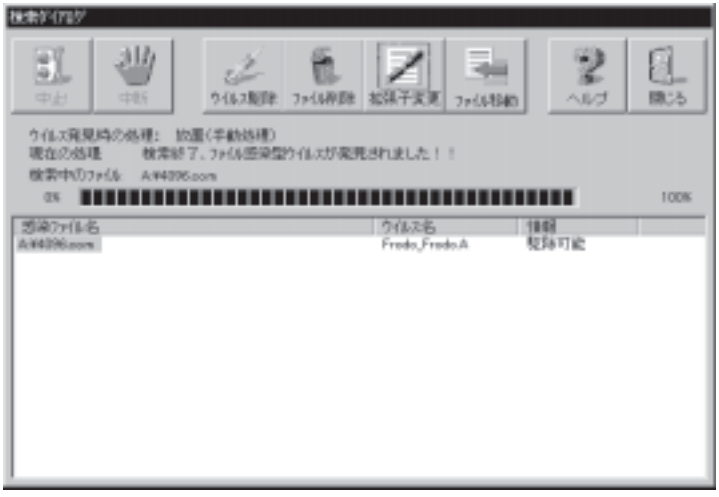
タスクトレイの「ウイルスバスター 98」のアイコンを右クリックし、メニューから［ウイルスバスター 98 を起動］を選択します。

クイック起動ツールバーからの起動

Internet Explorer 4.0 の［クイック起動ツールバー］から「ウイルスバスター 98」のアイコンを選択します。
「ウイルスバスター 98」の起動時には、［手動検索］画面が表示されます。

■ウイルス検索の開始

「ウイルスバスター 98」でウイルス検索をおこなうには、[手動検索]画面でウイルス検索をおこなうドライブまたはフォルダを選択し、[検索開始] ボタンをクリックします。
ウイルス検索が開始されます。



ウイルスが発見されなかった場合

ウイルスが発見されずに検索を終了すると、「検索終了」画面が表示されます。

ウイルスが発見された場合

「ウイルスバスター 98」は、ウイルス検索でウイルス感染を発見すると、「ウイルス発見」のウインドウを表示し、ユーザーは感染ファイルの処理を選択できます。

ウイルス感染ファイルの処理については「第 6 章　ウイルスを発見時の処理」を参照してください。
また、ウイルス感染ファイルの処理は自動でおこなうこともできます。感染ファイルの自動処理を選択した場合は、ウイルスが発見されると、設定された処理がおこなわれます。
自動処理の設定およびウイルス検索の詳細な設定は［検索設定］画面でおこないます。詳しくは「ウイルス検索の設定」を参照してください。

■その他の検索開始方法

「ウイルスバスター 98」でのウイルス検索方法は、［検索］画面からおこなう以外に、以下の方法があります。

右クリック

［マイコンピュータ］または［エクスプローラ］でドライブ、フォルダまたはファイルを選択して右クリックし、表示されたメニューから、［ウイルスバスター 98］を選びます。
選択されたドライブ、フォルダまたはファイルのウイルス検索が実行されます。

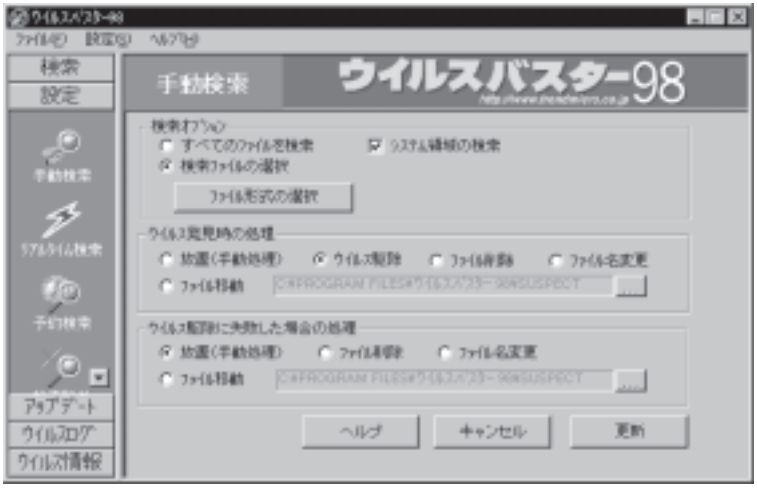
ドラッグ & ドロップ検索

［マイコンピュータ］または［エクスプローラ］でドライブ、フォルダまたはファイルを選択し、「ウイルスバスター 98」のメイン画面にドラッグ & ドロップします。
選択されたドライブ、フォルダまたはファイルのウイルス検索が実行されます。

■ウイルスバスター98の設定

［手動検索］設定画面の表示

［設定］バーの［手動検索］アイコンをクリックします。
または、［設定］メニューから［手動検索］を選びます。
［手動検索］設定画面が表示されます。



この画面では、ウイルス検索の対象、ウイルス発見時の自動処理および、ウイルス駆除に失敗したときの処理を設定します。
ここで設定された内容は、手動検索および予約検索に共通で使用されます。

ウイルス検索対象の設定

コンピュータ・ウイルスはすべてのファイルに感染するわけではありません。画像データのファイルなど、ウイルス感染が発生しないファイルもあります。ウイルスは、基本的に実行可能な種類のファイルに感染します。
「ウイルスバスター98」は、特定の拡張子のみを指定してウイルス検索をおこなえます。

［すべてのファイルを検索］または［検索ファイルの選択］のどちらかを選択します。［検索ファイルの選択］を選んだ場合は、初期設定では、以下のファイルをウイルス検索します。

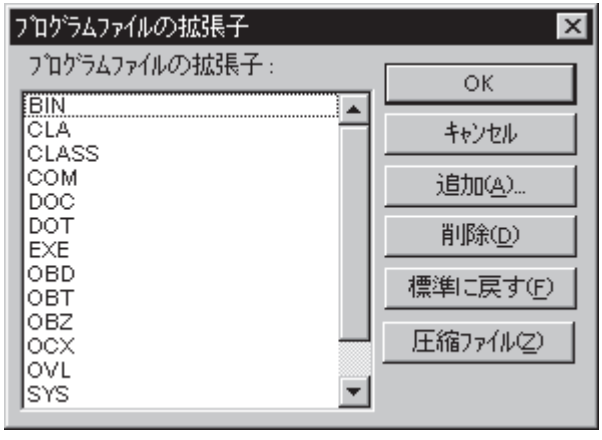
拡張子	.BIN , .CLA , .CLASS , .COM , .DOC , .DOT, .EXE , .OBD, .OBT , .OBZ , .OCX, .OVL , .SYS, .XLS , .XLT

システム領域の検索の設定

［システム領域の検索］のチェックボックスをオンにすると、パーティション・テーブル及びブートセクタに対してウイルス検索します。

検索するファイル形式の変更

［検索ファイルの選択］を選択した場合、検索するファイル形式を変更するには以下の手順でおこないます。
［検索設定］画面で、［検索ファイルの選択］を選択し、［ファイル形式の選択］ボタンをクリックします。
［プログラムファイルの拡張子］画面が表示されます。



OK	変更した設定を保存して検索設定画面に戻ります。
キャンセル	変更した設定を保存しないで、検索設定画面に戻ります。
追加	［追加］ボタンをクリックすると、「追加する拡張子」画面が表示されます。［追加する拡張子］欄に半角英数文字で３文字の拡張子を入力し、［OK］ボタンをクリックします。
削除	指定した拡張子を削除します。「プログラムファイルの拡張子」欄から削除する拡張子を選択し、［削除］ボタンをクリックします。
標準に戻す	検索するファイル形式を初期設定に戻します。
圧縮ファイル	検索をおこなうファイルに圧縮ファイルの拡張子を追加します。

設定が終了したら、［OK］ボタンをクリックして、［検索設定］画面に戻ります。設定の変更は、次回の検索から有効となります。
検索ファイル形式の拡張子は、少なくとも１種類は指定してください。指定がなければウイルス検索はおこなえません。

圧縮ファイルの検索の設定

［圧縮ファイルの検索］ボタンをクリックすると、検索するファイルの拡張子に、圧縮ファイルの拡張子が追加されます。
［圧縮ファイルの検索］ボタンをクリックして追加される、検索可能な圧縮ファイルは以下の通りです。

圧縮形式	検索対象の拡張子	その他
ZIP (ZIP 2互換) GNU ZIP UNIX ZIP	.ZIP	パスワード指定がある場合は検索できません
LZH (LHA 2.1x互換)	.LZH	
Cabinet	.CAB	
LZEXE	.EXE	
MS-COMPRESS	.CO_, .EX_, .DO_, .XL_	圧縮前の拡張子は .COM ,.EXE ,.DOC ,.XLS

圧縮ファイル内の圧縮ファイルを検査することが可能です。2段階の圧縮まで対応しています。

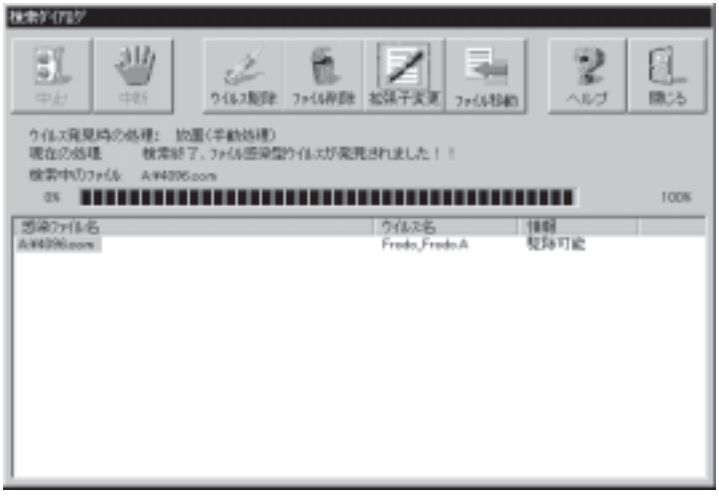
また、圧縮ファイル内にウイルス感染ファイルを発見した場合、圧縮ファイルに対してはウイルスの処理をおこなえません。一度圧縮ファイルを解凍してからウイルスの処理をおこなってください。
なお、追加される圧縮ファイル以外に、以下の形式に対応しています。

圧縮形式	その他
PKLITE	拡張子は .COM , .EXE
TAR	拡張子は.TAR
UNIX Compress	
エンコード形式	
UUEncode	
MIME	暗号化されている場合は対応しません。
BinHex	

これらの形式のファイルを検索する場合は、対応する拡張子(特定の拡張子がない形式もあります)を入力するか、あるいは［すべてのファイルを検索］を選択します。
圧縮形式のバージョンによっては、検査できない場合があります。

ウイルス感染ファイルの処理の設定

「ウイルスバスター98」は、ウイルス検索でウイルス感染を発見すると、「ウイルス発見」のウインドウを表示し、ユーザーは感染ファイルの処理を選択できます。
また、あらかじめ設定しておくことで、感染ファイルの処理を自動的におこなうこともできます。
［ウイルス発見時の処理］欄では、手動検索または予約検索によって発見された感染ファイルの処理方法を指定します。
ウイルスが発見されると、次のような画面が表示されます。



このとき、自動処理が設定されていると、ウイルス感染ファイルは自動で処理されるため、処理を選択するボタンは灰色で表示され、使用できません。

ウイルス発見時の自動処理使用時の注意

［ウイルス駆除］、［ファイル削除］、［拡張子変更］、［ファイル移動］の自動処理は、システムファイルや重要なファイルであっても処理を実行し、中止できません。これらの処理は自動処理が実行されても安全であることをご確認のうえ、設定してください。

安全かどうかわからない場合は、［放置］を選択し、ウイルス発見後に「ウイルスバスター 98」の手動検索で感染ファイルを処理することをお薦めします。

ウイルス発見時の処理

以下の 5 種類の処理が設定できます。

放置(手動処理)	ウイルスに対して自動処理をおこないません。 ウイルス発見時に、ユーザーが感染ファイルに対する処理を選択します
ウイルス駆除	ファイルからウイルスを取り除きます。ファイルからウイルスを駆除できなかった場合は、次の「駆除失敗時の処理」にしたがって、処理をおこないます
ファイル削除	ウイルス感染ファイルそのものを削除します
拡張子変更	ウイルス感染ファイルの拡張子を変更して、実行不可能にします リネームをおこなうと、拡張子が「.VIR」に変更されます。拡張子が.VIRで同名のファイルが既にある場合には、.V01にリネームされます。.V01が既にある場合には、.V02となります（.V99まで）
ファイル移動	ウイルス感染ファイルを指定したフォルダに移動します。初期設定では移動先のフォルダ名は、"C: \Program Files\ウイルスバスター98\SUSPECT"です

感染ファイル移動先の指定時の注意

移動先のフォルダには、フロッピーなどの交換可能なメディアおよびネットワークドライブを移動先のフォルダとして指定しないでください。

移動先のフォルダが書込み禁止などの理由で、移動ができなかった場合、ウイルス・ログには、「移動に失敗しました」と記録されます。

ウイルス駆除に失敗したときの処理の設定

ウイルスを発見し、「ウイルス駆除」をおこなったときに、何らかの理由でそのウイルスを駆除できなかった場合におこなう処理を設定します。

上書き感染型ウイルスのように、感染時にもとのファイルを破壊するウイルスや、変種や亜種のウイルスなどは、発見できても駆除できない場合があります。

こういった場合におこなう処理を「ファイル放置」、「ファイル削除」、「拡張子変更」、「ファイル移動」から選択します。

それぞれの処理については「ウイルス感染ファイルの処理の設定」を参照してください。

なお、「ファイル放置」を選択すると、「ウイルス発見」のログが残る以外、感染ファイルに対してなにもしません。

第５章　自動検索（予約検索）

本章では、フォルダ・ドライブに対するウイルス検索を定期的に自動実行する、「予約検索」機能と Windows 95 / Windows 98 の起動時にウイルス検索をおこなう「起動時のウイルス検索」について説明します。
この２種類のウイルス検索は、共に「予約設定」画面で設定します。
「予約検索」は、「第４章　ウイルス検索」と同じ方法でウイルスを検索します。
「予約検索」を設定すると、指定日の指定時刻になると、自動的に「ウイルスバスター 98」が起動され、バックグラウンドでウイルス検索がおこなわれます。
なお、この機能を使用するには、コンピュータ本体の電源が入っていて、なおかつ「リアルタイムモニタ」が起動されている場合に限ります。
「ウイルスバスター 98」は、 Windows 95 / Windows 98 起動時に自動的にウイルス検索をおこなえます。この機能はオンにしておくことをお薦めします。
予約検索機能を使用する場合は、自動アップデート機能と同じ時刻に設定しないようにご注意ください。

■予約検索

「予約検索」は、「第４章　ウイルス検索」と同じ方法でウイルスを検索します。
「予約検索」を設定すると、指定日の指定時刻になると、自動的に「ウイルスバスター 98」が起動され、バックグラウンドでウイルス検索がおこなわれます。
なお、この機能を使用するには、コンピュータ本体の電源が入っていて、なおかつ「リアルタイムモニタ」が起動されている場合に限ります。
予約検索を設定する手順は次の通りです。

■「予約検索」設定画面の表示

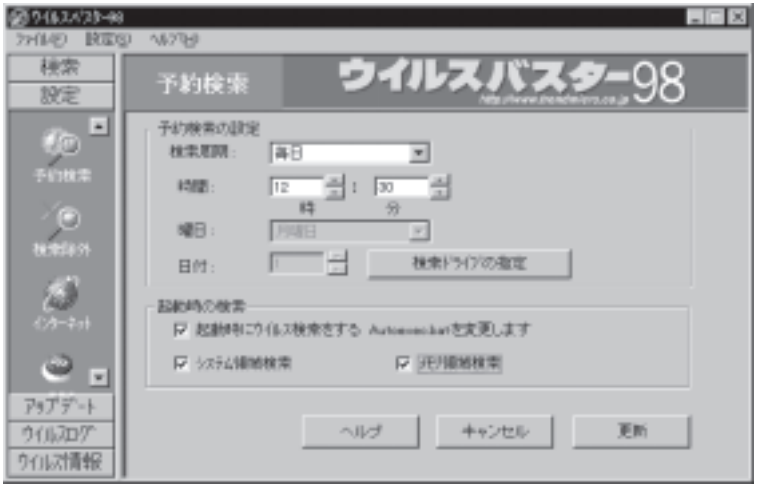
予約検索の設定は、「予約検索」設定画面でおこないます。「予約検索」設定画面を表示する手順は以下の通りです。

1.「ウイルスバスター 98」を起動する

タスクトレイの［リアルタイムモニタ］のアイコンを右クリックし、メニューから［ウイルスバスター 98 を起動］を選びます。

2. 予約設定画面を開く

［設定］バーの［予約検索］をクリックします。
または、［設定］メニューから［予約検索設定］を選びます。
［予約検索］画面が表示されます。



3．予約検索設定画面の更新

予約検索の設定が終了したら、［OK］ボタンをクリックし、変更した設定を保存してください。［キャンセル］ボタンをクリックすると、変更する前の設定に戻ります。

予約検索のオン／オフ

［検索周期］欄で［検索しない］を選択すると、「予約検索」はおこないません。
［検索しない］以外の周期を選択すると、「予約検索」が設定されます。

検索周期と時間の設定

検索の周期と、検索を実行する時間を設定します。

検索周期の選択

検索周期は、「毎日」「週１回」「月１回」から選択します。

検索時刻の設定

時間欄でウイルス検索をおこなう時間を設定します。この項目は、検索周期の設定が、「毎日」「週１回」「月１回」のいずれの場合も、設定する必要があります。

曜日の設定

曜日欄でウイルス検索を行なう曜日を設定します。この項目は、検索周期に、「週１回」が選択されている場合に設定します。

日付の設定

日付欄でウイルス検索をおこなう日付を設定します。この項目は、検索周期に、「月１回」が選択されている場合に設定します。

検索ドライブの設定

予約検索でウイルス検索をおこなう対象のドライブを指定します。予約検索が行われる対象は、ここで設定したドライブにあり、［検索設定］画面の［ウイルス検索対象の設定］で設定された種類のファイルです。
ウイルス検索をおこなうドライブを指定する手順は次の通りです。

1. ドライブ選択画面の表示

［予約検索設定］画面の［検索ドライブの選択］ボタンをクリックします。［予約検索ドライブの設定］画面が表示されます。

2. ドライブの選択

ウイルス検索をおこなうドライブをクリックします。ドライブは複数選択できます。ドライブを選択したら［OK］ボタンをクリックします。［予約検索設定］画面に戻ります。

［キャンセル］ボタンをクリックすると、設定を変更せずに［予約検索設定］画面に戻ります。

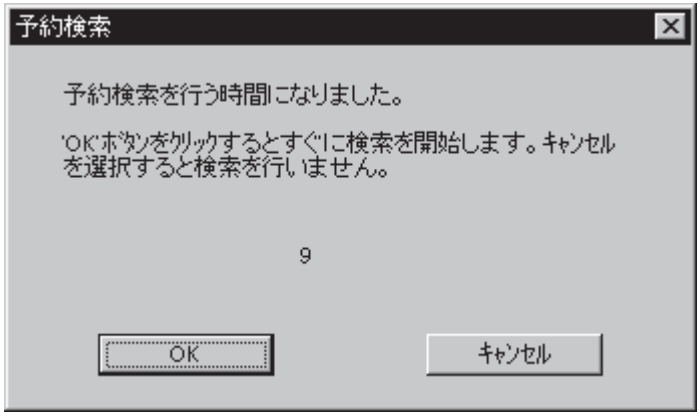
ドライブを選択しないと、すべてのローカルドライブをウイルス検索します。

検索設定

予約検索時の検索設定は、手動のウイルス検索と同じ設定が使用されます。ウイルス検索の設定は、「第4章　ウイルス検索」の「ウイルス検索プログラムの設定」を参照してください。

■予約検索の実行

「予約検索」を設定すると、指定日の指定時刻になると、自動的に「ウイルスバスター 98」が起動され、ウイルス検索がおこなわれます。



［OK］ボタンをクリックするか、ウインドウ内の数字が自動的にカウントされて 0 になると、ウイルス検索を開始します。
［キャンセル］ボタンをクリックすると、ウイルス検索をおこないません。

■起動時のウイルス検索

「ウイルスバスター 98」は、Windows 95 / Windows 98 起動時に自動的にウイルス検索をおこなえます。
起動時におこなうウイルス検索は、メモリ内およびシステム領域に限られます。この機能はオンにしておくことをお薦めします。
ここではWindows 95 / Windows 98 起動時におこなうウイルス検索の設定について説明します。

起動時のウイルス検索の設定

設定画面では以下の設定がおこなえます。
システムの起動時に検索をおこなうかどうか、および「メモリ検索」、「システム領域の設定」が設定できます。

[起動時に検索をおこなう]

チェックボックスをオンにすると、Windowsの起動時にウイルス検索をおこないます。このため、Windowsの起動にすこし時間がかかるようになります。

[メモリ検索]

チェックボックスをオンにすると、コンピュータの起動時にメモリ内のウイルス検索をおこないます。

[システム領域検索]

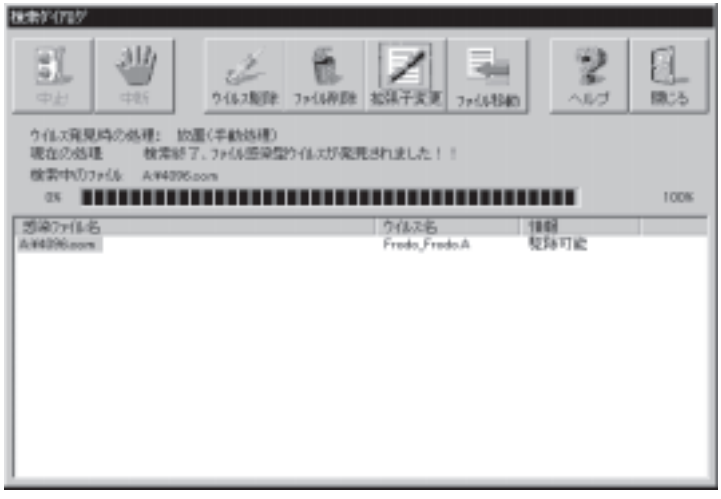
チェックボックスをオンにすると、コンピュータの起動時にシステム領域内のウイルス検索をおこないます。

第6章　ウイルスを発見したら

本章では、ウイルス検索やリアルタイム検索でウイルスが発見された場合の処理、および、誤検出時の監視除外の設定について説明します。

■ウイルス発見時の操作

「ウイルスバスター98」は、ウイルスを発見すると［検索ダイアログ］画面でウイルス名称と感染ファイル名を表示します。
また、発見されたウイルスはすべてログファイルに記録され、参照できます。ログファイルについては「第9章　ログファイル」を参照してください。
ウイルス感染ファイルの自動処理が設定されている場合は、この画面を表示した後、自動的に指定された処理を実行します。



「ウイルスバスター98」のウイルス処理方法は、「ウイルス駆除」、「ファイル削除」、「ファイル名変更」、「ファイル移動」の４種類があります。
ウイルス感染ファイルを選択して、実行する処理のボタンをクリックします。

［検索ダイアログ］画面を終了するには［閉じる］ボタンをクリックします。［閉じる］ボタンをクリックすると、ウイルス感染ファイルに対して、何の処理もおこないません。

■ウイルスの処理

「ウイルスバスター 98」でおこなえるウイルス感染ファイルの処理は以下の通りです。

ファイル削除

ウイルス感染ファイルを削除します。感染ファイルが削除されると、ウイルスもなくなります。もっとも確実なウイルスの処理方法です。
システム感染型のウイルスは「ファイル削除」はできません。
バックアップファイルや、アプリケーションのオリジナルディスクがある場合には、ウイルス感染ファイルを削除し、バックアップを使用するか、アプリケーションを再インストールすることをお薦めします。

拡張子変更

ファイルの拡張子を変更して、ウイルスの含まれたプログラムやデータファイルを誤って実行したり、開いたりすることを防止します。
システム感染型のウイルスは「拡張子変更」できません。
しかし、「拡張子変更」はあくまでも一時的な処理です。ウイルスコードは除去されません。最終的に「駆除」または「削除」する必要があります。
拡張子を変更されたファイルの拡張子は .VIR となります。
同じファイル名がすでにある場合は、リネームファイルの拡張子は .VI0 となります。

拡張子変更の例

ウイルス感染ファイルの「TEST.EXE」の拡張子を変更すると、ファイル名は「TEST.VIR」となります。

また、拡張子を変更された「TEST.VIR」が同じフォルダにある時に、さらに「TEST.COM」の拡張子を変更すると、ファイル名は「TEST.VI0」となります。
ファイル名が同じファイルの拡張子を変更する場合の拡張子を変更できるファイル数は 99 個までです。

ウイルス駆除

ウイルスのコードを除去し、ファイルを正常な状態に戻します。
システム感染型のウイルスも駆除できます。
駆除に失敗した場合や、上書き感染型ウイルスのようにウイルスの構造上駆除できないものであれば、「ウイルス駆除失敗時の処理」にしたがってウイルス感染ファイルを処理します。
「ウイルス駆除失敗時の処理」の詳細は次項を参照してください。

ファイル移動

ウイルス感染ファイルを指定したフォルダに隔離して、ウイルスの含まれたプログラムやデータファイルを誤って実行したり、開いたりすることを防止します。
移動先のフォルダの初期設定は、" C:\Program Files\ ウイルスバスター 98\SUSPECT " です。
システム感染型のウイルスは「ファイル移動」できません。
「ファイル移動」は一時的な処理です。ウイルスコードは除去されません。最終的に「ウィルス駆除」または「ファイル削除」する必要があります。

■ウイルス駆除失敗時の処理

ウイルス感染ファイルからのウイルス駆除に失敗したり、上書き感染型ウイルスのようにウイルスが構造上駆除できないものであれば、「ウイルス駆除失敗時の処理」にしたがってウイルス感染ファイルを処理します。

「ウイルス駆除失敗時の処理」におこなえるウイルス感染ファイルの処理は「放置」、「ファイル削除」、「拡張子変更」、「ファイル移動」の4種類があります。

「ファイル削除」、「拡張子変更」、「ファイル移動」はウイルス発見時の処理と同様です。「ウイルスの処理」を参照してください。

「放置」を選択すると、ウイルス感染ファイルに何の操作もおこないません。ただし、ウイルス発見の記録はログファイルに記録されますので、後でログファイルを参照し、処理できます。

■誤検出と検索除外の設定

ウイルスに感染していないファイルに対して「ウイルス発見」の報告をすることを「誤警告」といいます。

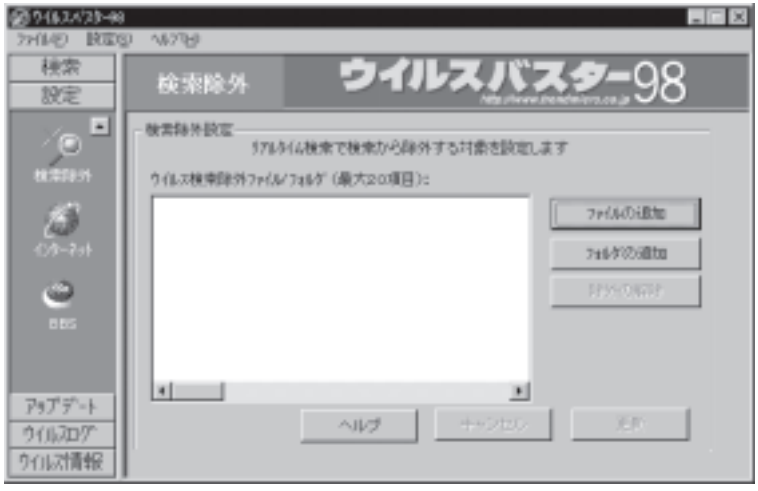
ウイルス検索時に、あきらかにウイルスが含まれていないプログラムに対して「ウイルス発見」の報告がされる場合は、ほとんどの場合、新しいバージョンのウイルスパターン・ファイルに更新することで解決されます。

新しいパターンに更新して、もういちどウイルス検索をおこなうことをお勧めします。

最新パターン使用時や、パターン更新がすぐにおこなえない環境の場合は、「ウイルス発見」が報告されるファイルを一時的にウイルス検索の対象から外すことができます。これを「検索除外」といいます。

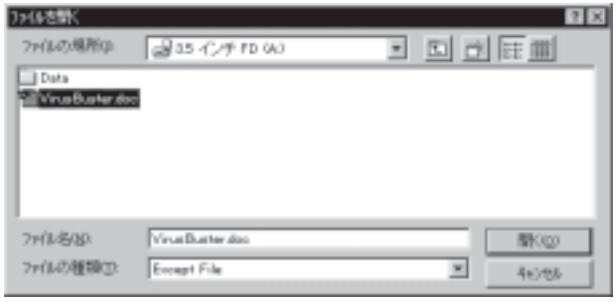
検索除外設定画面の表示

「検索除外」の対象のファイルは、［検索除外］画面で設定します。
「検索除外」設定画面を表示する手順は以下の通りです。
［設定］バーの［検索除外］をクリックします。
または、［設定］メニューから［検索除外設定］を選びます。
［検索除外］画面が表示されます。



ウイルス検索除外ファイルの追加

ウイルス検索をおこなわないファイルを指定します。
［ファイルの追加］ボタンをクリックします。ファイルを選択する画面が表示されます。



ファイルを選択して、［開く］ボタンをクリックします。
指定されたファイルが検索除外ファイルに指定されます。

ウイルス検索除外フォルダの追加

ウイルス検索をおこなわないフォルダを指定します。
［フォルダの追加］ボタンをクリックします。

フォルダを選択して、［OK］ボタンをクリックします。
指定されたフォルダが検索除外フォルダに指定されます。
この場合､除外の指定をしたフォルダに含まれるすべてのファイルと、サブフォルダすべてに対してウイルス検索をおこないません。

ウイルス検索除外ファイル／フォルダの削除

検索除外に設定されたファイルまたはフォルダがある場合、そのファイルまたはフォルダをウイルス検索の対象に戻せます。
誤検出により、ウイルス検索をおこなっていない対象がある場合は、新しいウイルスパターン・ファイルを入手したときは、ウイルス検索の対象に戻すことをお薦めします。
ウイルス検索除外ファイル／ディレクトリから､削除するものを選び、［除外の解除］ボタンをクリックします。

第7章　アップデート

本章では、ウイルスパターン・ファイルと、ウイルスパターン・ファイルのアップデート方法について説明します。

■新種ウイルスとウイルスパターン・ファイル

ウイルスパターン・ファイルとは、ウイルス識別情報のデータベースです。

「ウイルスバスター98」は、このウイルスパターン・ファイルを使用して既知のウイルスの感染を識別します。新種のウイルスに対しては、対応したウイルスパターン・ファイルにアップデートすることが必要です。

また、新しい種類のウイルスに対しては、検索プログラムをアップデートする必要がある場合があります。

現在、毎日のように新しいウイルスは作られているため、常に最新のウイルスパターン・ファイルとプログラムにアップデートすることがウイルス対策のポイントとなります。

パターンとエンジンのバージョン情報

ウイルスパターン・ファイルおよびプログラムのバージョン情報はメイン画面の［ヘルプ］メニュー→［バージョン情報］で確認できます。

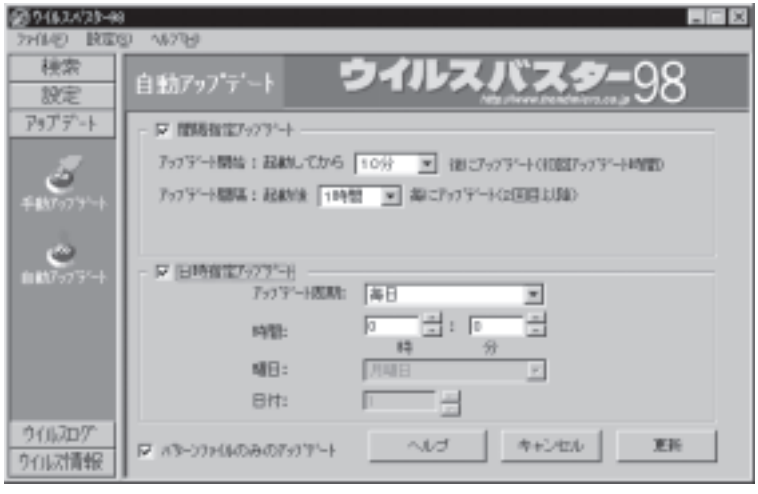
■自動アップデート

インターネットに常時接続可能の環境の場合、「ウイルスバスター98」は設定した時間にしたがって、ウイルスパターン・ファイルおよびプログラムのアップデートを自動的におこなえます。
自動アップデート機能は設定された時間に自動的にインターネットに接続してアップデートをおこないます。
弊社の Web サイトをチェックし、アップデートされたプログラムまたはウイルスパターン・ファイルがあればダウンロードしします。このとき、現在使用中のものより新しいプログラムまたはウイルスパターン・ファイルがなければなにもしません。
プログラムがアップデートされると、確認画面を表示し、ダウンロード後に「ウイルスバスター 98」を再起動します。

なお、この機能を使用するには、コンピュータ本体の電源が入っていて、なおかつ「リアルタイムモニタ」が起動されている場合に限ります。「リアルタイムモニタ」は一時停止していても動作します。
自動アップデート機能を使用する場合は、予約検索と同じ時刻に設定しないようにご注意ください。

自動アップデートの設定

［アップデート］バーの［自動アップデート］アイコンをクリックするか、［ファイル］メニューから［アップデート］の［自動アップデート］を選択します。
［自動アップデート］設定画面が表示されます。



自動アップデート機能は、「間隔指定アップデート」と「予約アップデート」の 2 種類の方法で設定できます。
ウイルスパターン・ファイルだけダウンロードし、プログラムをダウンロードしない場合は、［パターンファイルのみのアップデート］のチェックボックスをオンにします。このチェックボックスがオンの場合は、確認をおこなわずにアップデートします。

間隔指定アップデート

「間隔指定アップデート」は、毎日、「リアルタイムモニタ」起動後に一定時間が経過するごとに弊社の Web サイトをチェックし、新しいプログラムまたはウイルスパターン・ファイルがあればダウンロードします。
間隔指定アップデート機能を使用する場合は、チェックボックスをオンにし、初回のアップデートと、2 回目以降のアップデート間隔を選択します。

アップデート開始

1 回目のアップデートは、「リアルタイムモニタ」を起動してから、何十分後に 1 回目のアップデートをおこなうかを設定します。
10 分から設定可能ですが、ネットワーク接続が確立されていないと、ダウンロードに失敗します。

アップデート間隔

2回目以降のアップデートを何時間ごとにおこなうかを設定します。

日時指定アップデート

「日時指定アップデート」機能は、日時または週を指定して弊社の Webサイトをチェックし、アップデートされたプログラムまたはウイルスパターン・ファイルがあればダウンロードします。
「日時指定アップデート」機能を使用する場合は、チェックボックスをオンにします。
アップデートの周期と、検索を実行する時間を設定します。

アップデート周期の選択

アップデート周期は、「毎日」「週 1 回」「月 1 回」から選択します。

アップデート時刻の設定

アップデートをおこなう時間を設定します。

曜日の設定

アップデートを行なう曜日を設定します。この項目は、アップデート周期に、「週１回」が選択されている場合に設定します。

日付の設定

アップデートを行なう日付を設定します。この項目は、検索周期に、「月１回」が選択されている場合に設定します。

ダイアルアップ接続の場合

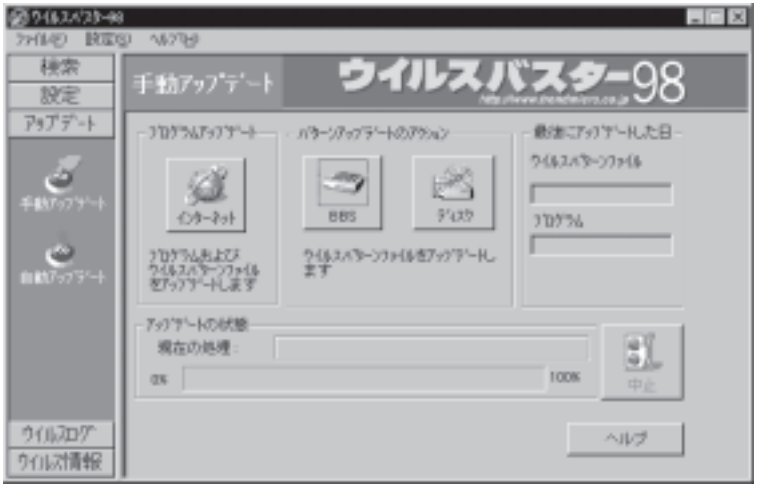
ダイアルアップ接続でインターネットをご利用の場合は、アップデート開始時点でインターネットの接続をおこないます。
ダイアルアップルーター以外でご利用の場合は、終了後も自動で接続を切りませんので、ご注意ください。

■手動操作でのアップデート

ウイルスパターン・ファイルは、インターネットで自動的に更新する以外に、手動操作でインターネット、BBS、あるいはディスクから更新できます。
ここでは、手動操作での更新方法を説明します。
手動操作でウイルスパターン・ファイルをアップデートするには、どの方法も、［手動アップデート］画面でおこないます。

手動アップデート画面

［アップデート］バーの［手動アップデート］アイコンをクリックするか、［ファイル］メニューから［アップデート］の［手動アップデート］を選択します。
［手動アップデート］画面が表示されます。



インターネット

インターネットからウイルスパターン・ファイルおよびウイルス検索エンジンをアップデートします。
［手動アップデート］画面で、［インターネット］ボタンをクリックします。

インターネットから手動操作でウイルスパターン・ファイルを更新するには、Internet Explorer 3.0 または Netscape Navigator 2.0 以上の Web ブラウザがインストールされ、インターネットへの接続環境があることが必要です。
また、LAN 接続や、リアルタイムでのインターネット翻訳ソフトを使用していて、プロキシサーバーを使用している場合は、［インターネット］設定画面で［HTTP プロキシの設定］の欄でプロキシサーバを使用する設定をおこなう必要があります。
［インターネット］の設定については「第 8 章　インターネット」を参照してください。

BBS

コンピュータにモデムが接続されている場合、弊社 BBS から最新のウイルスパターン・ファイルをダウンロードしてアップデートできます。
はじめて BBS にアクセスする場合は、モデムの設定をおこないます。2 度目以降のアクセスの場合は、［BBS］ボタンをクリックするだけで、ウイルスパターン・ファイルをアップデートできます。
BBS によるアップデートの手順は以下の通りです。
［BBS］ボタンをクリックします。「ウイルスバスター 98」が弊社 BBS に接続し、ファイルのダウンロードを開始します。ダウンロードの進行状況は、画面下のバーで表示されます。
ダウンロードが終了すると、ウイルスパターン・ファイルを自動的に更新し、接続を切断します。
以上で更新は終了です。

モデムの設定

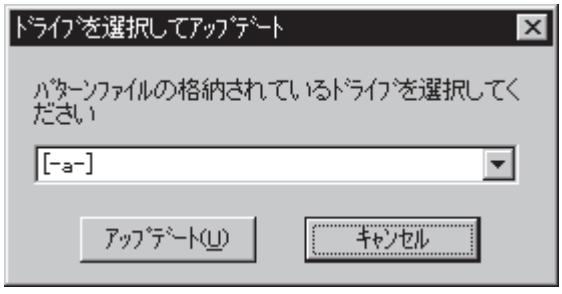
BBS にアクセスして、ウイルスパターン・ファイルをダウンロードするには、モデムの設定をおこなう必要があります。
モデムの設定は、始めてアクセスする前に一度だけおこないます。2 度目以降は、設定の必要はありません。
モデム設定の手順は以下のとおりです。

［設定］バーの［BBS］をクリックするか、［設定］メニューの［BBS］を選択します。
［BBS 設定］画面が表示されます。

［Com ポート］、［通信速度］、［ダイヤルモード］の３項目を接続されているモデムにあわせて設定します。
その他の設定は変更する必要はありません。
BBS は毎月 10 日、20 日、30 日はメンテナンスのために運休します。

ディスク

フロッピーディスクを使用して、ウイルスパターン・ファイルをアップデートできます。
フロッピーディスクによるアップデートの手順は以下の通りです。
［ローカルディスク］ボタンをクリックします。ウイルスパターン・ファイルのあるドライブを指定する［ドライブを選択してアップデート］ウインドウが表示されます。



ドライブを選択して、［アップデート］ボタンをクリックします。指定されたドライブから、ウイルスパターン・ファイルを読み込みます。アップデートの進行状況は、画面下のバーで表示されます。以上で更新は終了です。

第8章　インターネット

「ウイルスバスター 98」は、インターネットからユーザーが気がつかないうちにダウンロードされて実行されるインターネット・ウイルス(不正なJavaアプレットおよびActiveXコントロール)をブロックするWebTrap機能を搭載しています。また、インターネットを利用して、ウイルスパターン・ファイルおよびウイルス検索エンジンを更新し、また、弊社からの最新情報を自動的に受け取ることができます。

■ WebTrap

インターネットからユーザーが気がつかないうちにダウンロードされて実行されるインターネット・ウイルス(不正なJavaアプレットおよびActiveXコントロール)をブロックするWebTrapについて説明します。

WebTrapの動作中に、不正Javaアプレットもしくは ActiveXコントロールをダウンロードしようとすると、次のような画面が表示されます。

［OK］ボタンをクリックすると、ブロックされたファイルが破棄されます。

この機能は、Internet Explorerのセキュリティが「低く」設定されていて、「ダウンロードするのみ」を選択した場合も動作します。

WebTrapを使用するかどうかは、［インターネット］画面で設定します。設定の詳細は、本章の「インターネットの設定」の項目を参照してください。

WebTrap の動作

WebTrap は、インターネットと Web ブラウザの間に入り、プロキシサーバーとして機能します。Java アプレットおよび ActiveX コントロールをダウンロードすると、そのファイルを検査し、不正なプログラムであればそのプログラムを Web ブラウザに渡さずに破棄します。

WebTrap は、サーバー名「LOCALHOST」、IP アドレス「127.0.0.1」、ポート番号「8431」として動作します。ホスト名、IP アドレス、ポート番号が同一のプロキシサーバーとして動作するソフトウェアがある場合は、正しく動作しません。

■インターネットの設定

インターネット関連の設定は、「インターネット」画面でおこないます。

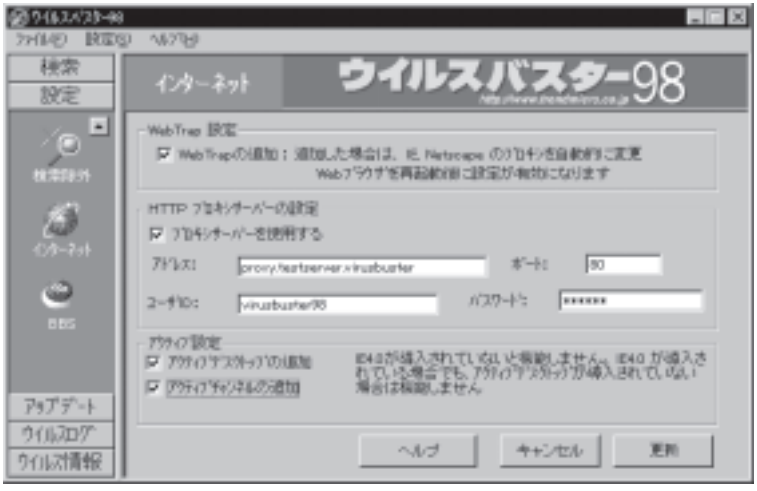
「インターネット」画面では、WebTrap の設定、プロキシサーバーの設定、アクティブデスクトップ、アクティブチャンネルの設定をおこないます。

「インターネット」画面を表示する手順は以下の通りです。

インターネットの設定は、インターネットに接続している間はおこなわないでください。接続が変更されると Web ブラウザなどが正しく動作しなくなることがあります。

インターネット設定画面

［設定］バーの［インターネット］アイコンをクリックするか、［設定］メニューから［インターネット］ を選択します。
［インターネット］設定画面が表示されます。



WebTrap の設定

［WebTrap の追加］のチェックボックスをオンにすると、WebTrap を使用します。この設定は、［更新］ボタンをクリックした後にインターネットに接続したときから有効になります。この機能はリアルタイムモニタがロードされていないと有効になりません。
なお、「ウイルスバスター98」の WebTrap はプロキシ名「LOCALHOST」、IP アドレス「127.0.0.1」、ポート番号「8431」を使用します。
すでにインターネットに接続している場合は、接続中の Web ブラウザの設定は変更されません。

プロキシの設定

「ウイルスバスター 98」が使用するプロキシサーバーの設定をおこないます。
プロキシサーバーがあらかじめインストールされた環境に「ウイルスバスター 98」をインストールした場合は、この欄の値は自動で設定されます。
「ウイルスバスター 98」のインストール後にインターネットプロバイダを変更した場合、プロバイダの設定が変わった場合、または、リアルタイムの Web 翻訳ソフトを導入した場合など、プロキシを変更する場合に入力します。
プロキシサーバーのアドレス、ポート番号、ユーザー ID とパスワードを入力します。ユーザー ID とパスワードは自動アップデートに使用します。自動アップデートを使用しない場合は、入力する必要はありません。
なお、プロキシ名「LOCALHOST」、アドレス「127.0.0.1」、ポート番号「8431」は使用できません。

アクティブデスクトップ・アクティブチャンネルの設定

この欄の項目は Internet Explorer 4.0 がインストールされている場合だけ有効になります。その他の Web ブラウザをお使いの場合は、設定しても機能しません。また、Internet Explorer 4.0 をお使いの場合でも、アクティブデスクトップを使用しない設定になっている場合は、機能しません。
［アクティブデスクトップに追加］のチェックボックスをオンにすると、トレンドマイクロのサイトがアクティブデスクトップに表示されます、
［チャンネルの購読］のチェックボックスをオンにすると、「TREND MICRO JAPAN」がチャンネルバーに追加され、自動的に購読するよう設定されます。
購読の設定を変更するには、チャンネルバーを右クリックして表示されるメニューから［プロパティ］を選びます。設定の詳細は Internet Explorer のヘルプなどを参照してください。

第9章　ログの管理

「ウイルスバスター98」は、ウイルス感染に関するログとインターネット経由のウイルスパターン・ファイルとプログラムのアップデートのログを記録します。

■ウイルスログ

ウイルス感染ファイルが発見されると、自動的にログに記録されます。ウイルス感染が発見された場合、ウイルス感染に関する詳細な情報を表示できます。このログファイルを参照することで、ウイルスの感染経路や、感染の状況がわかります。
また、放置、拡張子変更あるいはファイル移動したファイルについてもログに記録されています。ログを参照して、それらのウイルス感染ファイルに処理をおこなえます。

［ログ表示］画面の表示

［ログ表示］バーの［ウイルスログ］アイコンをクリックするか、［ファイル］メニューから［ログ表示］→［ログ表示］を選択します。［ログ表示］画面が表示され、「ウイルスバスター98」が起動された時点のログが表示されます。

この画面では、指定した日付のログの表示、ログの CSV ファイル(カンマ区切りのテキストファイル)への出力、ログの日付ごとの削除がおこなえます。
このログファイルには、発見されたウイルスの記録が表示されます。ウイルスが発見されていない場合は、記録はありません。

日別のウイルス感染ログの表示

［ログの日付］欄で、表示したい日のログを選択します。
右側の［ウイルス検索ログ］欄にウイルス感染ログが表示されます。
［ウイルス検索ログ］には以下の項目があります。

時間	ウイルスを発見した時刻
ウイルスファイル名	ウイルスに感染したファイル
ウイルス名	感染したウイルスの名称
発見時の動作	ウイルス発見時におこなわれた処理
ユーザ名	感染ファイルを発見したときのユーザー名。 Windowsにログインしたユーザー名が表示される
検索種別	手動検索またはリアルタイム検索のいずれか。予約検索で発見された場合は手動検索と表示される

画面に表示されない項目は［ウイルス検索ログ］欄の最下段のスクロールバーで左右にスクロールして確認できます。

ログの更新

ログには、「ウイルスバスター 98」が起動された時点、または手動検索が終了した時点のログが表示されます。
起動または検索終了後にリアルタイム検索で発見されたウイルス感染ファイルのログは表示されません。このような場合に、［表示更新］ボタンをクリックすると、最新のログが表示されます。

ログのファイル出力

ログが表示されている場合、［ファイル出力］ボタンをクリックすると、ログをファイルに出力できます。ファイル保存ダイアログが表示されます。ファイル名と出力先のフォルダを指定します。

出力ファイルは、一般的な CSV 形式(カンマ区切りのテキスト)です。Microsoft Excel や Microsoft Word などで開けます。

ログの削除

［ログの日付］欄で、削除する日のログを選択し、［削除］ボタンをクリックします。「指定の日付のログが全て削除されます。削除しますか？」と確認されます。［はい］ボタンをクリックすると、ログが削除されます。

■アップデートログ

インターネット経由でプログラムまたはウイルスパターン・ファイルのアップデートをおこなうと、自動的にログに記録されます。BBSまたはローカルディスクからのウイルスパターン・ファイルのアップデートは記録されません。このログファイルを参照することで、アップデートした日付と、アップデートの内容がわかります。

［アップデートログ］画面の表示

［ログ表示］バーの［アップデートログ］アイコンをクリックするか、［ファイル］メニューから［ログ表示］→［アップデートログ表示］ を選択します。
［アップデートログ］画面が表示されます。

この画面では、指定した日付のログの表示、ログの CSV ファイル(カンマ区切りのテキスト)への出力、最新のリリースノートの参照ができます。
このログファイルには、インターネット経由のアップデートの記録が表示されます。アップデートが一度もおこなわれていない場合は、ログおよびリリースノートはありません。

日別のアップデート・ログの表示

［ログの日付］欄で、表示したい日のログを選択します。
右側の［アップデートログ］欄にアップデート・ログが表示されます。
［アップデートログ］には以下の項目があります。

時間	アップデートした時刻
ダウンロード	アップデートしたファイルの種類。以下の3種類があります。 プログラム、ウイルスパターン・ファイル、プログラムとウイルスパターン・ファイル
状況	ダウンロードの成功、または失敗

画面に表示されない項目は［アップデートログ］欄の最下段のスクロールバーで左右にスクロールして確認できます。

ログの更新

ログには、「ウイルスバスター 98」が起動された時点、または手動アップデートが終了した時点のログが表示されます。
画面表示後に行われた自動アップデートのログは表示されません。このような場合に、［表示更新］をクリックすると、最新のログが表示されます。

ログのファイル出力

ログが表示されている場合、［ファイル出力］ボタンをクリックすると、ログを CSV(カンマ区切りのテキスト)形式のファイルに出力できます。
ファイル保存ダイアログが表示されます。ファイル名と出力先のフォルダを指定します。出力ファイルは、一般的な CSV(カンマ区切りのテキスト)形式です。Microsoft Excel や Microsoft Word などで開けます。

ログの削除

［ログの日付］欄で、削除する日のログを選択し、［ログ削除］ボタンをクリックします。［指定の日付のログが全て削除されます。削除しますか？］と確認されます。［はい］ボタンをクリックすると、ログが削除されます。

リリースノートの表示

ウイルスパターン・ファイルまたはプログラムがアップデートされると、アップデート内容について書かれた「リリースノート」が同時にダウンロードされます。

［リリースノート］ボタンをクリックすると、最新のリリースノートを表示します。

第 10 章　ウイルス情報の表示

「ウイルスバスター 98」には、発見済みのウイルスのデータベースが搭載され、ウイルスについての情報を見ることができます。なお、ウイルス情報については、インターネットの弊社サイト(www.trendmicro.co.jp)にも情報が掲載されています。あわせてご利用ください。

■ウイルス情報

［ウイルス情報］バーの［ウイルス情報］アイコンをクリックするか、［ファイル］メニューから［ウイルス情報］→［ウイルス情報］を選択します。
［ウイルス情報］画面が表示されます。

既知のウイルスについての情報を表示します。
ウイルスの種類を「一般的なウイルス」、「システム感染型」、「ファイル感染型」、「マクロウイルス」から選択し、ウイルス名を選択すると、詳細な情報が表示されます。
情報を表示しているときに、［印刷］ボタンをクリックすると、ウイルスの情報が印刷されます。

■ウイルス一覧

［ウイルス情報］バーの［ウイルス一覧］アイコンをクリックするか、［ファイル］メニューから［ウイルス情報］→［ウイルス一覧］を選択します。
［ウイルス一覧］画面が表示されます。

使用中のウイルスパターン・ファイルで検出可能なウイルス一覧を表示します。
ウイルス一覧は、カーソルキーまたはスクロールバーでスクロールして参照できます。
［印刷］ボタンをクリックすると、検出可能なウイルス一覧が印刷されます。なお、ウイルス一覧の印刷には、A4で60枚以上の用紙が必要です。ご注意ください。

ユーザーサポートについて

ユーザーサポートについては、同梱のサポートサービスメニューを参照してください。

■サポート情報の表示

ユーザーサポートサービスを受けるには、製品のシリアル番号が必要になります。
シリアル番号は、同梱のシリアル番号シールに記載されているほか、インストール時に入力したシリアル番号を［ヘルプ］メニューの［バージョン］情報で確認できます。

また、この画面で［サポート情報］ボタンをクリックすると、弊社サポートセンターの連絡先が表示されます。

トラブルシューティング

アンインストールに失敗し、インストールできない

「ウイルスバスター」が動作していると、アンインストールは実行できません。「ウイルスバスター」を終了してからやり直してください。また、「ウイルスバスター」が動作していないのに「ウイルスバスター95」または「ウイルスバスター97」がアンインストールできない場合は、何らかの理由でインストールが正しくおこなわれなかったものと考えられます。

アンインストールできなかった「ウイルスバスター95」または「ウイルスバスター97」と同じフォルダにもういちど「ウイルスバスター95」または「ウイルスバスター97」をインストールしなおして、「ウイルスバスター98」のインストールをおこなうと、インストールが実行できます。

「ウイルスバスター98」をインストールしたらインターネットに接続できなくなった

WebTrapを使用する設定で、リアルタイムモニタがロードされていないと、プロキシサーバとして動作するWebTrapがロードされず、インターネットに接続できません。

WebTrap機能を使う場合は、インターネットに接続する前に「リアルタイムモニタ」を起動しておく必要があります。

リアルタイムモニタが動作している場合は、ブラウザのプロキシ設定をユーザーが変更したか、あるいはリアルタイムWeb翻訳ソフトをインストールした場合など、ユーティリティソフトによってブラウザのプロキシ設定が変更された場合もアクセスできなくなります。

この場合は、「ウイルスバスター98」インストール前に控えておいたプロキシ設定を参考に、元の通りに設定することで、インター

ネットにアクセスできるようになります。その後にもういちど WebTrap の設定をおこないます。
また、Web 翻訳ソフトなどをインストールした場合は、プロキシのアドレスとして「LOCALHOST」または「127.0.0.1」、ポートに「8431」を使用するプロキシ形式を使用しているものがないかどうか確認してください。もしも、アドレスとして「LOCALHOST」または「127.0.0.1」、ポートに「8431」を使用しているソフトウェアがある場合は、そのソフトウェアと WebTrap 機能は併用できません。

2 種類の Web ブラウザの併用

WebTrap の設定は、「通常使うブラウザ」に設定されている Web ブラウザに対しておこないます。
2 つ以上のブラウザを使用している場合は、「通常使うブラウザ」に設定されていないブラウザは、手動でプロキシを設定する必要があります。

不正 Java アプレットがブロックされない

WebTrap を使用しているにもかかわらず、特定のサイトに行くと、システムが停止したり、極端にコンピュータの動作速度が落ちるなど、不正 Java アプレットがある場合に発生すると同じ症状が出る場合、Web ブラウザのキャッシュファイルに不正 Java アプレットなどが(WebTrap導入前に)ダウンロードされて蓄積されていると考えられます。
WebTrapを設定した場合、一度キャッシュをクリアしておくことをお薦めします。
Internet Explorer で、キャッシュをクリアする手順は次の通りです。

1. ［スタートメニュー］→［設定］→［コントロールパネル］とクリックしてコントロールパネルを開き、［インターネット］アイコンをダブルクリックして開きます。［インターネットのプロパティ］が表示されます。
2. ［全般］タブをクリックし、［インターネット一時ファイル］欄の［ファイルの削除］をクリックします。
［ファイルの削除］ウインドウが表示されます。

Internet Explorer 4.0 をご利用の場合は、［すべての購読項目のコンテンツを削除する］のチェックボックスをオンにして［OK］ボタンをクリックします。
Internet Explorer 以外の Web ブラウザをご利用の場合は、お使いの Web ブラウザのマニュアルまたはヘルプを参照して、同様の操作をおこなってください。

救済ディスクの作成に失敗する場合

一部の Windows95 プリインストールモデルのコンピュータをお使いの場合、Windows の Command フォルダに ” DRIVESPACE.BIN ” が入っていないものがあります。
この状態で「救済ディスク」を作成すると、「ファイルのコピーに失敗しました」と表示され、「救済ディスク」を作成できません。
このような場合は、「救済ディスク」の作成の前に、以下の準備をあらかじめおこなっておく必要があります。
2HD のフロッピーディスクを 2 枚ご用意ください。(「救済ディスク」作成用のディスクでかまいません)

1. ［スタートメニュー］→［設定］→［コントロールパネル］でコントロールパネルを開き、［アプリケーションの追加と削除］を開きます。
2. ［起動ディスク］タブをクリックして ［起動ディスク］画面を表示し、［ディスク作成］ をクリックします。
   起動ディスクが作成されます。
3. 作成した、起動ディスク内の DRIVESPACE.BIN を Windows の Command フォルダにコピーします。
4. これで、準備は終了です。
   ［スタートメニュー］ →［プログラム］→［ウイルスバスター 98］→［救済ディスクの作成］の順にクリックして、「救済ディスク」を作成してください。