

ブロードバンドユーザー必携のセキュリティツール

Photo: Nakamura Tohru

# ファイアーウォールソフト 徹底比較

個人でもインターネットの常時接続が一般的になってきた。そこで忘れてはならないのがセキュリティ対策。常時接続環境ではクラッキングの危険も倍増するからだ。そこで今回は個人向けセキュリティソフトの実力を目的別に比較してみた。 小山貴弘

フレッツ・ISDNやADSL、CATVインターネット環境の普及により、インターネットの常時接続があたりまえようになってきた。しかし、常時接続の環境は、自らのアクセスの利便性が高くなるだけではない。同時に外部からの悪質なアクセスや攻撃にも常にさらされている状態なのだ。このため、ユーザー1人1人のセキュリティに対する意識が重要となってくる。

個人データの漏洩防止からクラッキング対策まで、インターネットを安全に利用するためにも、個人向けセキュリティソフトによる対策を講じたい。



# セキュリティソフトでクラッカー対策を!

個人ユーザーにはあまりなじみのないセキュリティ対策。まずは、セキュリティソフトがどのような機能を備えているかを知って、自らの環境に最適な対策を考えてみよう。

## 個人にも必要な セキュリティソフト

インターネットが広く普及してくるにつれ企業だけでなく、個人も不正なアクセスや攻撃を仕掛けてくるクラッカーの標的となっており、セキュリティ対策を講じる必要が出てきた。

インターネットに接続されているすべてのパソコンは、IPアドレスで所在を管理されている。クラッカーは、そのIPアドレスを元に、パソコンのインターネットへの窓口となる各ポートやOSのセキュリティホールを突いて、ユーザーのパソコンや内部データにアクセスしてくる。

固定IPの場合はもちろん、フレッツのように毎回IPが変わるサービスでも、長時間アクセスし続けられれば攻撃的になる可能性はある。また、ファイアウォールの設けられた広域LANのような形態のCATVでも、同じLAN内部からのアクセスには、無防備に近い。セキュリティ対策は常時接続ユーザーにとって必須の事項なのだ。

## タイプ別購入術

クラッカーを防ぐための基本は、なんといっても、ファイアウォール(防火壁)の構築だ。これによって、インターネット側からLAN側(家庭内)への不正なアクセスを防御するのだ。(下図参照)ファイアウォールには企業向けの高価な専用ハードウェアもあるが個人ならソフトウェアでも十分だ。個人向けのセキュリティソフトでも、最近ではクッキーの許可、不許可の管理や、不正なプログラムの侵入を防ぐJava アプレットやActiveXコントロールの監視機能のほかにも、パケットフィルタリングや集中的なアクセスを交わすping対応の機能などが装備されているものが増えてきている。こうしたセキュリティソフトを自分のスタイルや目的にあわせて導入すれば安全度は飛躍的に高まる。常時接続に乗り換えたら必ずセキュリティソフトを導入して常時接続のブロードバンド時代を快適、かつ安全に使おう。

## How to Choice

今回は以下3つの視点でセキュリティソフトを選ぶことにする。

目的に合わせてぴったりなソフトを選んで欲しい!

### easy

難しい設定は後回し!  
とにかく、すぐにネットワークにセキュリティをかけたいたい!

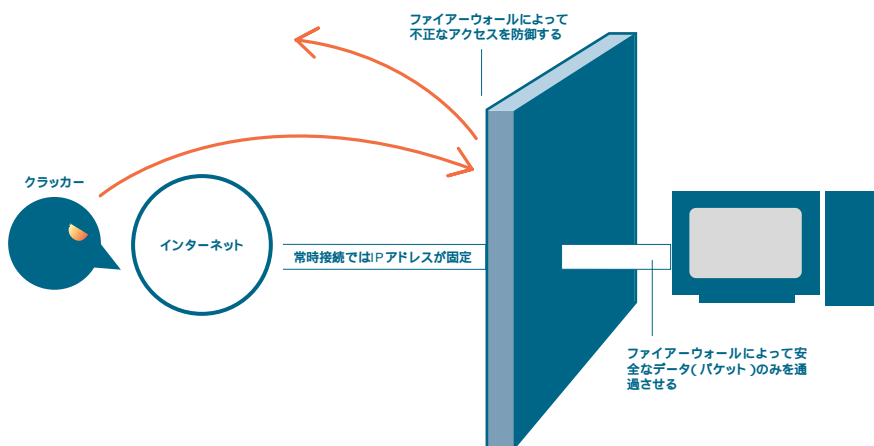
### advance

使いこなす自信アリ!  
おまかせの設定じゃモノ足りない。  
自分で細かく設定したい!

### power

クラッカーを突き止める!  
アクセスログを解析して、十分なセキュリティ対策を講じたい!

ファイアウォールによるクラッキングの防御



ファイアウォールソフトを導入すると、LAN(プライベート)側のパソコンとインターネットの間に、不正アクセスを防ぐための、防護壁が築かれる。ファイアウォールソフトは、FTPやHTTPなどのポートを監視したり、IPアドレスやプロトコルを監視したりすることで、不正なアクセスやクラッカーの攻撃から、ネットワークを守る。



# 知っておきたい、クラッカーの攻撃の手口

セキュリティ対策を行うには、どのような攻撃を受けるのかを知っておくのがイチバン。  
パソコンの安全性を高めるためにも、まずはクラッカーの手口を知っておきたい。

## パソコンに穴が空く？ セキュリティホールとは

連日、ニュースサイトを中心にウィンドウズやブラウザのセキュリティホールに関する報道がなされている。セキュリティホールとは、いわゆる抜け穴のことだ。

OSやブラウザなどどんなプログラムにもバグがある。セキュリティホールとは、特定の条件下において、ユーザーの情報が漏れたり、外部からの侵入が可能になってしまったりするバグを指す。

最近では、マイクロソフト社などOSメーカーの対応も早く、セキュリティホールが発見されると、すぐに修正のためのパッチプログラムが提供される。しかし、ユーザーがパッチを当てないことにはセキュリティホールは空いたままだ。悪意あるウェブサイトやクラッカーはこのセキュリティホールを虎視眈々と狙っている。攻撃の的にならないためにも、定期的にメーカーのウェブサイトをチェックしてパッチプログラムを素早く導入するなど、ユーザー自身の的確な対応も重要だ。

## 「裏口」を作り出す バックドアプログラムとは

ユーザーの知らないところで、リモートコントロールによってアプリケーションが勝手な動作を行ったり、不正侵入の手助けを行ったり、さらには個人情報を送信されたりすることがある。このような、「裏口」をユーザーのパソコンに作り出すのが、バックドアプログラムだ。

このプログラムの侵入経路は多岐にわたる。たとえば、ウェブページに置かれたJavaアプレットやActiveXコントロールからだったり、パソコンへの不正な侵入だったりする。また、ダウンロードしてきたオンラインソフトにバックドアプログラムが隠されているケースもある。このバックドアプログラムに

対応するには、セキュリティソフトを導入するなどの対策をするほか、信頼できないデータはダウンロードしないことが重要だ。

## サービス停止を引き起こす DoS攻撃やping攻撃

省庁のウェブサイトや有名なウェブサイトなどが、クラッカーによる攻撃でサービス停止を引き起こしたという報道は記憶に新しい。これらは、DoS攻撃やping攻撃によるものだ。

DoS攻撃とは、特定のIPアドレス宛てにパケットを大量に送信する攻撃のこと。pingを出す以外にもさまざまなソフトがあり、大量のパケットや不正なパケットを送信することで、システムをダウンさせてし

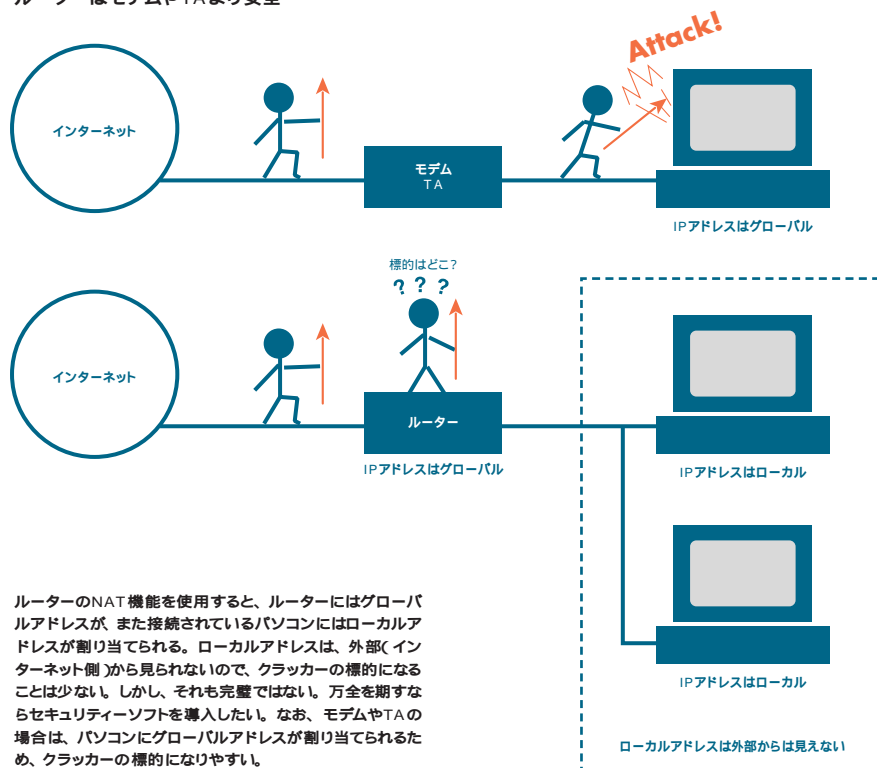
まうものもある。

またpingとは、もともとパケットが送信先のサーバーに届いていることを確認するコマンドのことだ。pingを受け取ったサーバーが返事を返すことで、送信先までのアクセス時間などの計測ができる。このpingを同時刻に一齐に1つのサーバーなどに送信するのがping攻撃だ。

DoSやping攻撃はクラッカーのサイトなどで告知され、世界中の参加者から一齐にデータやpingが送信される。その結果、狙われたサーバーは高負荷によりサービス停止を引き起こすのだ。

防御方法だが、ping攻撃は対応するセキュリティソフトによって防げる。しかし、DoS攻撃はパケット受信による負荷に

ルーターはモデムやTAより安全



ルーターのNAT機能を使用すると、ルーターにはグローバルアドレスが、また接続されているパソコンにはローカルアドレスが割り当てられる。ローカルアドレスは、外部(インターネット側)から見られないので、クラッカーの標的になることは少ない。しかし、それも完璧ではない。万全を期すならセキュリティソフトを導入したい。なお、モデムやTAの場合は、パソコンにグローバルアドレスが割り当てられるため、クラッカーの標的になりやすい。



よって起きるため、完全に防ぐのは難しい。ただ特定のソフトによる攻撃の場合は、セキュリティソフトで遮断できる。

### ルーターのユーザーにはセキュリティソフトは不要？

LANで接続されたパソコンでインターネット接続を共有するために使用するのがルーターだ。ルーターによるインターネット接続の場合、NAT機能によりLANに接続されているパソコンにローカルIPアドレスを割り当てることが多い。この場合、グローバルIPアドレスはルーターに割り当てられ、インターネットからのパケットは、ルーターがローカ

ルIPアドレスを持ったパソコンに送る。

この機能のため、ルーターによる接続ではADSL/CATVモデムやターミナルアダプタに比べて、外部からの侵入を受けにくい。しかし、ルーター接続ならセキュリティ対策が不要というわけではない。不正なアクセスがそのままローカルIPアドレスに変換されて、パソコンに届くケースもある。その際にバックドアプログラムなどが仕掛けられるとクラッカーの思うがままになってしまう。ルーター接続といえども安全性を考えるなら、セキュリティソフトはやはり必須だろう。

### 常時接続時代、自分の身は自分で守る！

高速・常時接続のインフラが普及し、個人ユーザーの導入も盛んだ。これらのサービスを利用してインターネットを活用するなら、セキュリティ対策は無視できない。特に、固定IPアドレスで接続されたパソコンは、クラッカーにとっては絶好の攻撃的だ。すでに生活するうえで欠かせないものとなったインターネットだが、危険性があることは十分に認識しておきたい。

安全にインターネットを利用するためにも、今こそセキュリティソフトの導入を真剣に考える時期にあると言えるだろう。

## 掲載製品主要機能一覧表

製品名	e a s y		a d v a n c e		p o w e r	
	ウイルスバスター 2001	はりインターネット	Norton Internet Security 2001	BlackICE Defender	Internet Security Barrier	WinWrapper 1.0.3
販売元	トレンドマイクロ(株)	(株)メディアヴィジョン	(株)シマンテック	(株)東陽テクニカ 国内総代理店 / (株)アクト・ツー	(株)アクト・ツー	(株)アスキーNT
問い合わせ先	03-5334-3650	03-3222-6841	03-3476-1156	03-3279-0771(東陽テクニカ) / 03-3328-8431(アクト・ツー)	03-3328-8431	03-3465-9721
URL	www.trendmicro.co.jp	www.mvi.co.jp	www.symantec.co.jp	www.act2.co.jp	www.act2.co.jp	www.ant.co.jp
価格	8,500円	3,980円	9,800円	6,500円	16,800円 (キャンペーン価格13,800円)	5,800円
対応OS	Windows95/98/Me/NT4.0/2000	Windows95/98/Me/NT4.0	Windows95/98/Me/NT4.0/2000	Windows95/98/Me/NT4.0/2000	MacOS8.1以上	Windows95/98/NT4.0/2000
対応CPU	ペンティアム133MHz以上(Windows95/98/Me/NT4.0)、ペンティアム166MHz以上(Windows2000)		ペンティアム以上	ペンティアム133MHz以上	PowerPC以上	ペンティアム166MHz以上
必要メモリー	32Mバイト以上(Windows95/98/Me/NT4.0)、64Mバイト以上を推奨	32Mバイト以上	32Mバイト以上(Windows95/98)、64Mバイト以上(WindowsMe/NT4.0)	32Mバイト以上	64Mバイト以上	64Mバイト以上推奨
必要ハードディスク容量	20Mバイト以上	8Mバイト以上	90Mバイト以上(インストール時は100Mバイト以上必要)	50Mバイト以上	18Mバイト以上	3Mバイト以上
対応ブラウザ	インターネットエクスプローラ4.0以上	インターネットエクスプローラ3.0以上、ネットスケープコミュニケーションズ4.0以上(ナビゲーター3.0以上)	インターネットエクスプローラ4.0以上、ネットスケープナビゲーター4.0以上	インターネットエクスプローラ4.0以上、ネットスケープナビゲーター4.0以上	-	-
パケットフィルタリング		-				
クッキー対応	-	-		-		
DoS対応	-	-				
Ping対応	-	-				
Javaアプレット、ActiveX対応						
URLフィルター		-		-		
広告遮断機能	-	-		-		
リアルタイム監視機能						
ログ機能						
自動アップデート機能		-				-
マニュアル						
体験版	同社ウェブサイトからダウンロード可能	-	同社ウェブサイトからダウンロード可能	同社ウェブサイトからダウンロード可能	-	同社ウェブサイトからダウンロード可能
その他	-	要CD-ROMドライブ、16ビット色またはそれ以上のモニタ	統計イベント(ネットワークトラフィックのリアルタイム表示など)機能	COMCTL32.DLL4.72以上がインストールされていること	OpenTransport、InternetConfig 1.1以降が必要 / 800 x 600以上のモニター解像度が必要	-



# easy 早い! 簡単! 便利!

初心者必読!

## 今すぐセキュリティソフトを導入したい人向け

とにかく簡単に、とりあえずセキュリティソフトを導入したいなら。専門用語や難しい設定の仕方をしなくても、インストールするだけですぐ使えるものを選ぶほうがいい。ここでのポイントは機能の豊富さや細かな設定ができるかどうかということよりも、いかに簡単に使えるかということだ。

### ここがオススメ!

設定が簡単  
専門用語が不要  
操作性がよい

### とりあえず導入するなら簡単に設定できるもの

常時接続回線に切り替えたばかりのときは、うれしくてむやみに長時間インターネットに接続してしまいがちだが、セキュリティ対策はしておきたい。とりあえず、最低限のファイアーウォールでも設置している場合と設置していない場合とでは、大きく異なる。知らないうちに個人情報を盗まれたなんてことのないように、常時接続に乗り換えたら、必ずセキュリティソフトは導入するようにしたい。

難しいことはしたくないならば、詳細な設定はできなくてもとにかく簡単に導入できる製品を選べばよい。セキュリティというと、とかく高度な知識が必要のように

聴こえるが、インストールすれば自動的に標準的な設定をしてくれるものも多い。導入後に機能設定を変える場合でもあまり項目のないシンプルな画面でボタン操作のみでき、またメンテナンスについても面倒なテキスト入力などは、いっさいないというものが増えている。最近の製品ならばクッキー管理やパケットフィルタリングなど、ひととおりの機能は備えているので、こうしたものを使えばなにもしないよりはかなり安全度は高まるだろう。

### ウイルス対策も忘れずに

セキュリティ対策において、もっとも基本的かつ重要なことは、個人情報流出やウイルスなどの不正プログラムの侵入を

防ぐことの2点だ。最低限これさえおさえおけば、とりあえずはシステムダウンを狙ったアタックへの対策は考えなくてもよい。それよりは、ウェブページへのアクセスやデータのダウンロード時におけるセキュリティ対策にウェイトをおきたい

最近では常時接続が否かに関わらず、ウェブページを訪れるだけでウイルスを仕掛けられたり、不正侵入の窓口を作るバックドアプログラムを設置されたりするケースも多く、特にパソコンの初心者にとってはウイルス対策機能があることは重要だろう。

とにかくどんなものであれ、なにもないよりはいい。もし、まだなにもセキュリティ対策を取っていないならば、いまずぐ導入しよう。

## easy セキュリティソフトの選択ポイントはここだ!

### ① 導入のしやすさ

はじめてセキュリティ対策を講じる場合には、ソフトの導入と運用が簡単なことが、なんといっても第一条件となる。ソフトのインストール後に特に細かな設定をしなくても、すぐ使えることがポイントだ。

### ② 必要な機能のチェック

個人情報の流出を防ぐのか、それとも不正プログラムの侵入を防ぐのか

ど、目的によって必要な機能は異なる。あたりまえだが、自分の求める機能に対応しているかどうかはきちんと確認してから購入したい。ただし、外部からの侵入には、ほとんどのセキュリティソフトがなんらかの機能を備えている。

### ③ 付加機能の有無

セキュリティとは直接関係ないが、たとえばホームページの先読み機能などが付いていれば、インターネットを始め

たばかりの人にとっては買い得感があるだろう。こうした点に注目するのも1つの手だ。

### ④ 操作性

どんな人にとっても、操作性のよしあしは重要だ。操作のほとんどがボタンのオン/オフや、チェックボックスの操作だけでできれば、特にセキュリティに関する知識がなくても簡単に導入できるだろう。



ウイルス対策機能に簡易セキュリティー機能を搭載

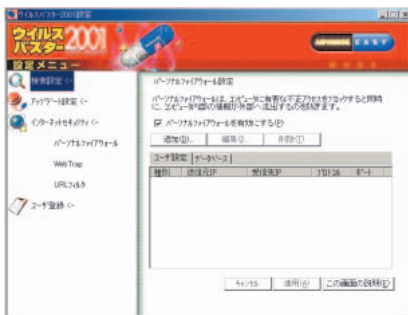
# ウイルスバスター-2001

- 基本的にウイルス対策がメインだが、簡単設定のファイアーウォール機能が利用できる。
- 「EASY」設定では「パーソナルファイアーウォール」などにチェックするだけ。
- Java アプレットやActiveX コントロールを利用した不正なアクセスを阻止するWeb

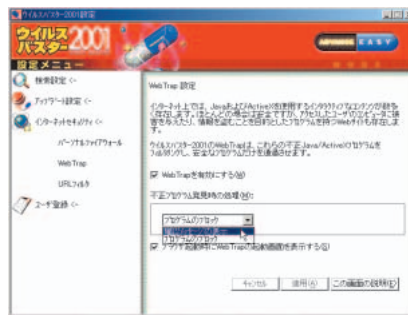
- Trap 機能を搭載。
- 有害なコンテンツを含むURLへのアクセスを制限するURLフィルターを搭載。
- 「ADVANCE」設定では、パケットフィルタリングのルールをユーザーが自分で決めることも可能。



ウイルスバスター2001のメイン画面。「EASY」設定では利用したい項目にチェックを付けるだけ。



「ADVANCE」設定ではパケットフィルタリングの詳細な設定も可能。過去に受信した不正プログラムのデータベースもチェックできる。



WebTrap では、警告、プログラムのロックの2つから設定を選択可能だ。

ウイルスバスター 2001

価格：8,500円  
問い合わせ：トレンドマイクロ(株)  
(03-5334-3650)  
www.trendmicro.co.jp

対応OS：ウィンドウズ95/98/Me/NT4.0/2000(ただしNTではパーソナルファイアーウォール機能の使用は不可)  
必要メモリ：32Mバイト以上(ウィンドウズ95/98/Me/NT4.0)、64Mバイト以上を推奨  
対応ブラウザ：インターネットエクスプローラ4.0以上

ポートブロックによる不正アクセス阻止とクッキー管理機能を実現

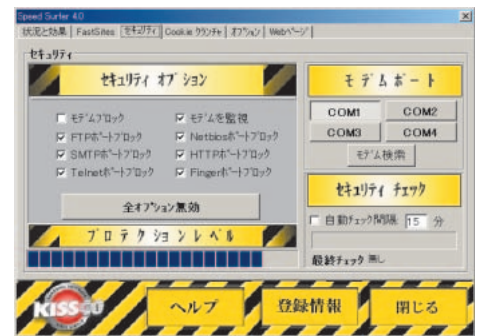
# ぱり2インターネット

ぱり2インターネット

価格：3,980円  
問い合わせ：(株)メディアビジョン  
(03-3222-6841)  
www.mvi.co.jp

対応OS：ウィンドウズ95/98/Me/NT4.0  
必要メモリ：32Mバイト以上  
対応ブラウザ：インターネットエクスプローラ3.0以上、ネットスケープコミュニケーションズ4.0以上(ナビゲーター3.0以上)

- メイン機能はクッキーの送受信の管理機能だが、クッキー送受信時の管理を手軽に設定できる。
- ポートブロックによって外部からの侵入を監視。
- ユーザーが指定したポートを自動的にスキャンできる。また、スキャンした時間を記録可能。
- ウェブページの先読みが可能なので、表示が早くなる。
- オンラインアップデートにも対応。
- モデムを利用しているときでもモデムプロックや監視が可能。



パケットフィルタリングを備えない代わりにポートブロックで外部からの侵入を阻止する仕組みを採用している。



# advance アタックに完全対応!

## 中上級者向け! 幅広いセキュリティ機能がポイント

より高度な機能を求めるユーザーは、導入のしやすさに加えて、セキュリティ対策機能の豊富さが重要となってくる。さまざまなアタックにも十分に対応できるトータル性能の優れたソフトをセレクトしよう。

### ここがオススメ!

さまざまなアタックに対応できる  
より多くの機能を提供  
特定の機能なら業務用並みに充実

### 外部からのアタックへの対応

単に個人情報の漏洩を防ぐだけでなく、より本格的なセキュリティ機能を求めるならば、外部からのアタックを想定した幅広いセキュリティ機能が必要になってくる。たとえば、パケットフィルタリングによるファイアウォール機能の設置やDoS攻撃への対応などだ。Dos攻撃とはDenial of service（サービス停止）の略で、標的となるコンピューターに対して異常なほど大量のpingを行ったり、大量のパケットを送りつけたりすることでサーバーに負荷をかけてサーバーを通信不能にしてしまうことだ。これを完全に防ぐことは難しいが、特定のソフトからの攻撃なら対応できる。

また、ログの記録に対応しているかどうかも重要だ。たとえば監視ログを使えば、

第三者のパソコンへのアタックの踏み台にされた場合にも、ログの履歴をたどることにより、送信元を調べ、ソフトで防御設定を実行すれば、再び踏み台にされにくくなる。こうしたログの記録や不正アクセスの監視、高度な追跡機能などを細かく設定できるかどうかも重要なポイントだろう。アタックを受けた際に侵入者の自動追跡を行い、以後の侵入を禁止する機能が搭載されていれば、なおよいだろう。

### Javaアプレットなどへの対応

そのほかにも「広告遮断機能」には注目したい。これは自動的に複数のウィンドウが立ち上がってくる「ポップアップウィンドウ」による広告や、埋め込み式のパン

ことである。というのも、こうしたポップアップウィンドウの背後に、実行時にクライアントにダウンロードして動作するタイプのアプリケーションである「Javaアプレット」や、インターネットエクスプローラーのプラグインプログラムである「ActiveXコントロール」などを用いた「トロイの木馬」プログラムが仕掛けられていたというケースも少なくないからだ。ユーザーは単に広告を見ただけのつもりが、実はそれによって不正なプログラムに侵されてしまっていたということも十分ありうるので注意したい。本格的なセキュリティを求めるなら、不正なJavaアプレットやActiveXコントロールの対策に対応しているかどうかはチェックしておきたいところである。

## advance セキュリティソフト選択のポイントはここだ!

### ① 搭載機能のチェック

より高度な機能を求める場合には、クッキーの許可、不許可の管理、外部からの侵入を防ぐパケットフィルタリングによるファイアウォール機能があるかということやクラッカーからのアタックを防ぐpingまたはDoS攻撃に対応できるかどうかなど、より広範なセキュリティ機能を搭載していることが重要になる。

### ② セキュリティレベルの選択ができるかどうか

セキュリティレベルを高く設定するほど、ウェブブラウザが不便になることもある。その点を考慮すると、ユーザーの好みにあわせてセキュリティのレベルを自由に設定できるかどうかのポイントとなる。セキュリティレベルの自由なカスタマイズは、快適にインターネットを使うためにも欠かせないポイントだ。

### ③ 詳細なログの採取機能

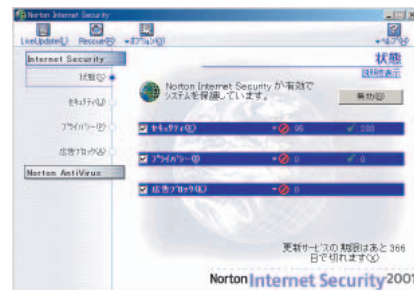
不正なアタックをガードするためにも、その不正アクセスがいったい、いつ、どこからきたものなのかという、詳細を知ることが必要である。セキュリティソフト上で採取できるログの内容には、たとえばネットワークトラフィックの記録やアクセスウェブサイトの履歴、送信をブロックしたクッキー送受信情報のリストがある。



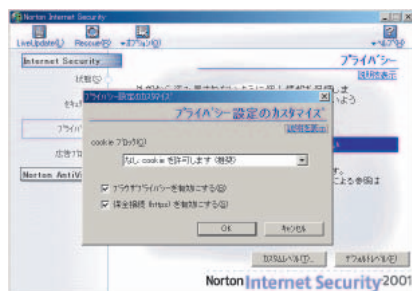
万全なセキュリティー設定で幅広いユーザーをカバー

# Norton Internet Security 2001

- 3段階のセキュリティー設定から選択するだけで、強力なパケットフィルタリング機能を自由に利用できる。
- プライバシー管理機能によってクッキーの送受信を制御できる。
- 外部からのアタックを常に監視し、ユーザーに警告ダイアログを表示。
- ポップアップウィンドウによる広告や、バナー広告を非表示にする機能を搭載し、画面が見やすくなる。
- 各アプリケーションに最適なセキュリティーを自動設定。カスタマイズも可。
- 10段階に圧縮されたファイルに潜むウイルスにも完全対応。



デフォルトレベルでの設定画面。それぞれの項目にチェックするだけ。

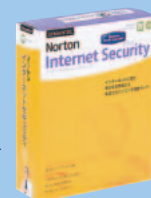


カスタムレベルでは、セキュリティー、プライバシーがそれぞれ3段階で設定でき、さらに詳細なルールの指定も可能だ。



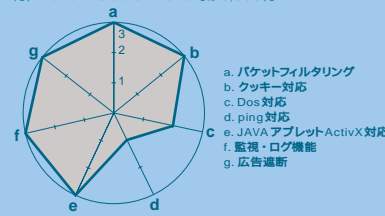
バナー広告も遮断する強力な広告ブロック機能。バナーをゴミ箱アイコンにドラッグすることで登録できる。

Norton Internet Security 2001



価格：9,800円( AntiVirus機能を省いた「Norton Personal Firewall 2001」は6,800円)  
 問い合わせ：(株)シマンテック(03-3476-1156)  
[www.symantec.co.jp](http://www.symantec.co.jp)

対応OS：ウィンドウズ95/98/Me/NT4.0/2000  
 必要メモリー：32Mバイト以上(ウィンドウズ95/98) 64Mバイト以上(ウィンドウズMe/NT4.0)  
 対応ブラウザ：インターネットエクスプローラ 4.0以上、ネットスケープナビゲーター 4.0以上  
 マッキントッシュ版の「Norton Internet Security」は14,800円、「Norton Personal Firewall」は9,800円



外部からの侵入対策に特化したパッケージ

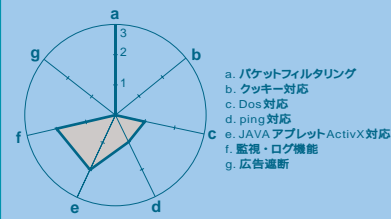
# BlackICE Defender

BlackICE Defender

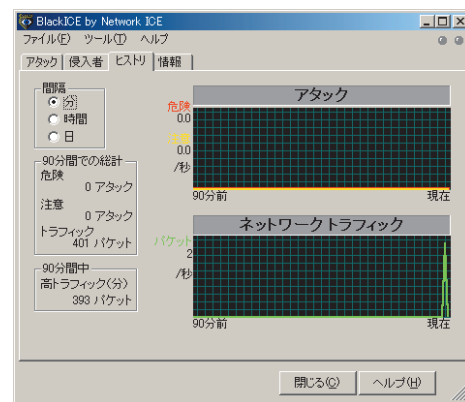
価格：6,500円  
 問い合わせ：(株)東陽テクニカ  
 (03-3279-0771)  
 (株)アクト・ツー  
 (03-3328-8431)  
[www.toyo.co.jp](http://www.toyo.co.jp)  
[www.act2.co.jp](http://www.act2.co.jp)



対応OS：ウィンドウズ95/98/Me/NT4.0/2000  
 必要メモリー：32Mバイト以上  
 対応ブラウザ：特になし



- 4段階のセキュリティー設定から選択するだけで強力なパケットフィルタリング機能が利用できる。
- クラッキングパターンは500種類以上をサポート。攻撃を感知すると、ツールバーのアイコン表示が変化し、アラート音と併せてユーザーに警告を出す。
- 侵入者の自動追跡を行い、以降のアクセスを禁止できる。
- アタックを受けた場合、詳細なログやエラーメッセージをウェブサイトから閲覧できる。
- ギガビットイーサネットに対応。



トラフィックやアタックの回数などをすべてグラフで表示できる。アタックを視覚的に把握でき、以降のセキュリティー対策に役立てられる。





# power ユーザーが自分でカスタマイズできる 上級者ならコレ! 自分でサーバーを構築しているなら迷わず選択!

ウェブアクセス時のセキュリティ対策に加え、外部からの攻撃のすべてに対応する強力なセキュリティ機能を求めるならこれらのセキュリティソフトをすれば、パーソナルユースとしては最強のセキュリティ環境を構築できる。

## ここがオススメ!

セキュリティ機能が強力  
ユーザーによる高度な設定が可能  
機能は個人レベルではパーフェクト

### 詳細に設定できるかどうか

個人で使うなら、前のページで紹介したセキュリティソフトでも実は十分な機能を揃えている。しかし、自分でより詳細に機能の設定をしたいユーザーにとっては、どこまで自分でカスタマイズできるのかも気になるところだろう。

たとえば、自分でサーバーを構築している人なら、不正なアクセスがあるかどうかをポート番号別に設定できるだけでなく、ソースアドレスや処理するアプリケーション別に設定できるかどうか、あるいは時間別に制御できるかどうかということも気になるだろう。

そのほかにも、家族でインターネットを使っているならば、ある特定の単語を登録しておけば、その単語を含むサイトを自動的に表示できなくする「有害サイト防止機能」のようなウェブ選別機能が自由に設定できるかどうかもチェックしたい。

### さらに高度なセキュリティ機能

より高度なセキュリティ機能について考えるならば、ウェブへのアクセス時にパソコンに入り込み、ネットワーク経由で不正にパソコンを操作するためのプログラムであるNetBUSやBackOrificeのような「ネットワークバンドル」などに対応している

かどうかポイントになる。また、頻繁にping攻撃を受けるようならば、外部からのping攻撃に対して、pingを吸収して返事を返さない設定をすることにより、外部からping攻撃を受けたパソコンを見えなくする「ステルス化機能」の有無にも注目したい。また、もし常にサーバーを動かす必要などがあり、不正を検知した場合には、少しでも早く知りたいという人ならば、攻撃を受けたときにダイアログと音で通知してくれるだけでなく、メールで知らせてくれる機能を備えたソフトを選べば、アドレスを携帯電話のものにしておくことで常にサーバーを監視できるだろう。

Product Showcase

## power セキュリティソフトの選択ポイントはここだ!

### ① 詳細な設定ができる

たとえば、不正アクセスへの対応1つとっても、ポート別、アドレス別、アプリケーション別のようにニーズにあわせて個別にセキュリティの管理方法を設定できるかどうかということや、たとえば「有害サイト防止機能」のような機能の検索キーとなる単語を自分で設定できるかどうかなどについても留意したい。

### ② より先進的な機能をサポート

パソコンに対する攻撃の種類にはさまざまなものが存在する。たとえば、OSやTCP/IPドライバーなどの弱点をついたり、偽造した接続要求パケットを繰り返し送信したりすることによってソフトウェアを暴走させ、サービスの低下やクラッシュなどを引き起こす「Land攻撃」や、エラー通知や通信状態の診断を行うプロトコルであるICMP

(Internet Control Message Protocol) を偽造して応答要求パケットを投げる「Smurf攻撃」、OSやTCP/IPドライバーなどが処理できないような断片化されたIPパケットを送りつけてハングアップ引き起こす「Teardrop攻撃」などだ。これらの攻撃に対応しているものはまだあまりないが、こうしたものに対処できるかどうかで判断するのも1つの手だろう。



簡単な設定で強力なセキュリティ環境を構築できる

# Internet Security Barrier

- ・セキュリティ対策、ウイルス対策、有害サイト防止の3つの機能を1つのパッケージに収録。
- ・セキュリティを保つためのネットワーク環境を簡単に設定、変更可能。
- ・活動ゲージによって、そのときのトラフィックが視認できる仕様。
- ・TCP/IPだけでなくAppleTalkの監視も可能。
- ・ping攻撃に対してはブロック機能と、ステルス機能の両方を搭載。
- ・クッキーの受信を制限可能。
- ・バナー広告の非表示ができ、ウェブページが見やすくなる。



モニタリング画面では、各ポートのトラフィックをチェックできる。オプション画面ではトラフィックデータの書き出しも可能。



ネットワーク設定はボタンの切り替えで簡単に変更できる。カスタム設定ではソースや発信元、サービスを自由に設定できる。



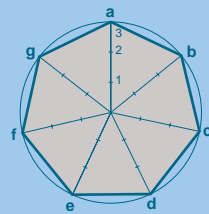
フィルタボタンのウェブタブでは、クッキーに関する設定ができる。送信データの制限や受信の禁止などがチェックボタンで選べる。

Internet Security Barrier

価格：16,800円(キャンペーン価格13,800円)  
問い合わせ:(株)アクト・ツ(03-3328-8431)  
www.actz.co.jp



対応OS：MacOS 8.1以降  
必要メモリー：64Mバイト以上  
対応ブラウザ：特になし



強力なパケットフィルタリング機能を搭載

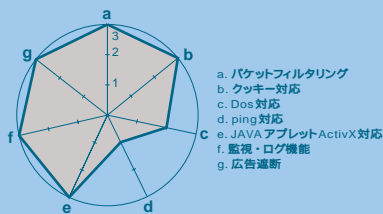
# WinWrapper 1.0.3

WinWrapper 1.0.3

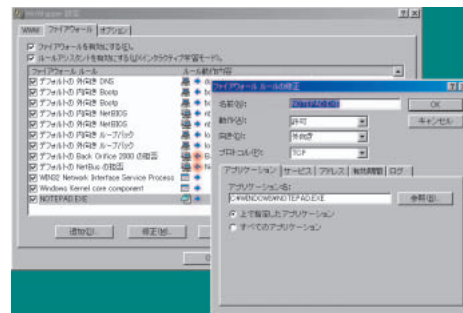
価格：5,800円  
問い合わせ:(株)アスキーNT(03-3465-9721)  
www.actz.co.jp



対応OS：ウィンドウズ95/98/NT4.0/2000  
必要メモリー：64Mバイト以上  
対応ブラウザ：特になし



- ・ユーザーの知らないネットワークへのアクセスを監視。発見時には警告ダイアログ表示。
- ・ダイアログが表示されると、以降の許可、不許可の設定をその場で行える。
- ・不正アクセス時などには、アプリケーションやプロトコルなども表示されるためわかりやすい。
- ・URLを指定してのクッキー許可、不許可のカスタマイズも可能。
- ・ping攻撃を吸収するステルス機能を搭載
- ・画面上部にダッシュボードを表示。リアルタイムで状況が監視できる。
- ・ウィンドウズMeには未対応。



ファイアウォールのカスタマイズ設定画面。パケットの送受信時の設定をあとから変更できる。



## [インターネットマガジン バックナンバーアーカイブ] ご利用上の注意

このPDFファイルは、株式会社インプレスR&D(株式会社インプレスから分割)が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

<http://i.impressRD.jp/bn>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真の撮影者、イラストの作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元(株式会社インプレス R&D)、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D(当時は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接のおよび間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先

**株式会社インプレスR&D**

All-in-One INTERNET magazine 編集部

[im-info@impress.co.jp](mailto:im-info@impress.co.jp)