仕組みの正しい理解と身の守り方

# 「知らなかった」では済まされない セキュリティー対策

text：編集部編


Melissa、Laroux、Klez、Nimda、Code Red、BackOrifice、バッファーオーバーフロー……。現在のインターネットには、コンピュータに詳しくない大多数のユーザーを無作為に狙った不正行為が蔓延している。しかし、ユーザーの1人1人がただ漠然と怯えているのではなく、不正行為を正しく理解して対処すれば、不正行為の威力は相対的に減少する。
サーバーへの不正アクセス、データ盗聴、ソーシャルエンジニアリングなどさまざまな不正行為があるが、ここではあくまでも一般的なインターネットユーザーを対象とする。ウイルス対策ソフトがインストールされているだけで安心している人、脆弱性の修正プログラムなんて見たことがない人、そしてここまで読んでいつものように「自分には関係ない」と思った人、そういうユーザーのために「最低限の」セキュリティー対策に絞って解説したい。

## 不正プログラムの種類を知る

2003年3月上旬、インターネットバンキングを悪用して、米大手銀行「シティバンク」の顧客口座から1600万円を引き出した事件で、警視庁が容疑者を不正アクセス禁止法違反と盗みなどの疑いで逮捕した。インターネットカフェのパソコンに、キーボードからの入力の履歴を記録できるツールをあらかじめ仕掛けて、そのパソコンを利用した客のネットバンキングのパスワードなどを盗み、そのパスワードを使って男性になりすまして預金1600万円を別の銀行に開設した仮名口座に振り込み、引き出して盗んだ疑いだ。

ここで使われたのは「トロイの木馬」と呼ばれる類の不正プログラムだ。キー入力を記録するトロイの木馬以外にも、こういったソフトウェアはインターネット上で容易に入手でき、使い方もいたって簡単だ。

これらの不正なプログラムは、まとめて「ウイルス」と呼ばれることが多い。ではウイルスとは何だろう？　旧通産省が定めた「コンピュータウイルス対策基準」の中で図1のように定義されている。ここでいうウイルスとは、簡単に言ってしまえばユーザーのコンピュータ環境に損害を与える有害なプログラムであるということだ。

この定義では、「ウイルス」という言葉を広い意味で使っている。つまり、「有害（不正）プログラム＝ウイルス」ということである。これらの広い意味での不正プログラムをマルウェア（Malware）と呼ぶこともある。マルウェアとは、マリシャスソフトウェア（Malicious Software：悪意のあるソフトウェア）を略したものである。

この広義でのウイルス（マルウェア）を動作の種類で分類すると、「ウイルス」「ワーム」「トロイの木馬」の3つに分けられる。

## ファイルなどに寄生する「ウイルス」

狭義での「ウイルス」は、ファイルなどに寄生するマルウェアを指す。広辞苑による

と、寄生とは「生物が、栄養の大部分や暮らし場所を他の生物体（宿主）に一方的に依存して生活すること」だ。まさに、現実のウイルスの特徴そのものである。もちろん、コンピュータウイルスはプログラムなので、他の生物体ではなく、他のファイルに取り付くということになる。言い換えれば、寄生する宿主ファイルが存在しなければ、ウイルスは存在できないのだ。ウイルスが寄生（感染）しているファイルを開くと、ウイルスが動き出し、感染コンピュータ内にある他のファイルへの感染活動を行う。

コンピュータウイルスが登場したのは今から約20年前だ。1981年に発見されたApple IIで感染を広げる「Elk Cloner」と呼ばれるもの。これは、フロッピーディスクのシステム領域に感染し、感染したフロッピーディスクをやりとりすることでPCの感染を広げていくもので、「ブート感染型ウイルス」と呼ばれる。1986年には、DOSパソコンを狙ったブート感染型ウイルス「Pakistan Brain」が登場した。しかしこのブート感染型は、今ではほとんど見られなくなった。というのも、感染経路がフロッピーディスクの交換に限定されるので伝染スピードが遅いからだ。OSが進化し、ブート感染型がうまく感染できなくなったというのも大きな理由だ。

ウイルスはブート感染型ウイルスからファイル感染型ウイルス、さらに自らプログラムコードを変化させてウイルス対策ソフトに検出されにくくするポリモーフィック型ウイルスへとどんどん複雑に進化している。1995年には、プログラムのファイルだけでなく、ワープロの文書ファイルや表計算のデータファイルに感染するマクロ感染型ウイルスが出てきた。アプリケーションのマクロやVBAスクリプトが高機能化し、それらの機能を使ったウイルスがデータファイルに潜むことが可能になったのが原因だ。

## マルウェア（Malicious Software）悪意のあるプログラム

### ネットワークを使って自己増殖する「ワーム」

ワームは、宿主ファイルを必要としない自己増殖型のマルウェアだ。ユーザーが気づかないうちにネットワークを介して自分自身のコピーを作成していく。具体的には、自分自身を添付したメールを大量に送り付けたり、ネットワークに接続されているコンピュータを自動検索して自分のコピーを置いていったりする。最近では、「password」や「abcde」などの安易なパスワードを設定しているコンピュータを狙うワームもある。

ウイルスが感染コンピュータ内（ウイルスが実行されたコンピュータ）だけで感染を広げるのに対し、ワームは他のコンピュータにも自動的に広がっていく。インターネット環境が整備された今、ワームの感染スピードは恐るべきものになっており、大きな脅威だ。

今でも話題に上ることの多い「Melissa」や「Klez」などは代表的なワームだ。

「コンピュータウイルス対策基準」によるウイルスの定義

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を1つ以上有するもの

**1 自己伝染機能**
自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

**2 潜伏機能**
発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

**3 発病機能**
プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

URL http://www.ipa.go.jp/security/antivirus/kijun952.html

［図1］広義の「ウイルス」定義

**ウイルスとは**

主にブートレコードなどのディスク領域やファイルに寄生するマルウェア。

**感染：**
感染したファイルを実行することで感染が広がる。ファイルの交換によるため、伝播速度は比較的遅いが、メールの普及によって感染速度は上がった。

**活動：**
ファイルの書き換え、ハードディスクの消去などの破壊活動を行ったり、システムを不安定にしたりする。トロイの木馬を仕掛けることもある。

**例：**
CIH、Michelangeloなど

［図2］狭義のウイルスの特徴と動作

## こっそりと悪事を準備する「トロイの木馬」

トロイの木馬は、ウイルスやワームと異なり、他のファイルに寄生もせず、自己増殖して感染したりもしないマルウェアだ。「トロイの木馬」という呼び名は、ギリシア神話に出てくる、トロイ軍の兵を潜ませた木馬に由来すると言われている。人を欺くために善意のものに見せかけた、その実は悪意のプログラムであるということだ。便利なプログラムのように見せかけてダウンロードさせたり、悪意のあるユーザーがネットワークからパソコンに不正アクセスして埋め込んだりすることでパソコンにインストールされる。

画面に嫌がらせのメッセージを表示したり、パソコンに保存されているデータを破壊したりといったものから、パスワードを盗むもの、インターネットを使ってパソコンを遠隔操作する「Back Orifice」やインターネットに接続されたコンピュータを攻撃するものなどインターネットを利用したものに進化している。ユーザーのウェブ閲覧履歴を記録して送信したり、その情報を元にポップアップ広告を勝手に表示する「スパイウェア」と呼ばれる不正プログラムも、トロイの木馬の一種だと言ってもいいだろう。

冒頭で書いたシティバンクの事件では、キーボードからの入力を記録するキーロガーと呼ばれるトロイの木馬が悪用された。

トロイの木馬の歴史は1989年の「AIDS Trojan」から始まる。ワームの普及と同様にインターネットの普及がトロイの木馬にも影響している。

## 現在はセキュリティーホールを利用する複合型がほとんど

近年のマルウェアには2つの大きな特徴がある。

1つは、ウイルス、ワーム、トロイの木馬のそれぞれの機能を組み合わせ、さらには不正アクセスの手法をも加えた複合型になっている点だ。その名のとおり、さまざまな感染方法や発病症状を持つ複合型ウイルスは、まさに冒頭で紹介した「コンピュータウイルス対策基準」が指すものそのものだ。

もう1つは、感染するためにセキュリティーホールを利用するという点だ。単純なウイルスならば感染したファイルを開かなければ感染しなかったが、現在はOSやソフトウェアが持つセキュリティー的に問題のある仕組みを悪用して感染するようになっているのだ（詳しくは後述）。

Code Red、Nimda、Klezなど世界中で猛威をふるっているものはすべてこれらの特徴を持つ。セキュリティーホールを悪用することで、ユーザーが特にファイルを開くなどの操作をしなくても他のコンピュータに自動的に感染を広げることが可能になり、その感染力は従来型のウイルスよりもはるかに強い。最近は「ウイルス」といえばこれを指すようになっている。

## 普通にパソコンを使うだけで感染するウイルスの出現

1996年頃から米国を中心に広がり始め、その後、各国語に翻訳されて世界中でチェーンメール化したデマメールがある。その内容は、"PENPAL GREETINGS!"と題されたメールで届き、そのメールを読

### ワームとは

他のファイルに寄生するとは限らず、ネットワークなどを使って自分のコピーを増やすことが可能なマルウェア。

**感染：**
ネットワークを自動的にスキャンしてアクセス可能な共有ドライブに自分をコピーしたり、メールソフトとそのアドレス帳を使ってメールで自己増殖したりする。

**活動：**
ウイルスと同様の活動に加え、無作為にネットワークにアクセスすることでネットワークを不安定にする。コンピュータ上の書類を無作為にメールで送信することもある。トロイの木馬を仕掛けることもある。

**例：**
Melissa、LoveLetter、Klezなど

［図3］ワームの特徴と動作

### トロイの木馬とは

特に自己増殖や感染の活動はしないが、ユーザーに気づかれない形でシステムに忍び込み、悪意のある活動をするマルウェア。

**感染：**
ウイルスやワームが感染とともに仕込んだり、悪意のあるユーザーが不正アクセスで仕掛けたりする。

**活動：**
ウイルスと同様の活動に加え、第三者が感染コンピュータを遠隔操作したりコンピュータ上の書類を入手したりするために侵入できる裏口を作る。また、感染コンピュータをDDoSの踏み台とすることもある。

**例：**
NetBus、NetSpy、BkDoorなど

［図4］トロイの木馬の特徴と動作

むだけでメールボックスにあるメールの差出人全員に、自分自身を自動転送する新種のウイルスがあるので注意しろ」といったものだ。もちろんこのウイルスは実在しなかった。

ところが、1999年11月に発見されたVBS.BubbleBoy（バブルボーイ）は、まさに、メールを読むだけで感染するウイルスだった。HTML形式のメールで届き、添付ファイルはない。しかし、いったんメールをHTML形式で表示してしまうと、HTMLに埋め込まれた不正なスクリプトが自動的に実行され、感染活動が行われる。感染すると、アドレス帳に登録されているすべてのメールアドレス宛てにウイルスメールを送り付けるというものだ。

**「ファイルを開かなければ大丈夫」から「対策をしなければ感染してしまう」へ**

これ以前は、メールに添付されたファイルさえ開かなければウイルスに感染することはなかったが、このウイルスの登場によって状況は一転した。ウイルスプログラムを実行しなくても、メールを読むだけで、あるいはプレビューするだけで、つまり普通にパソコンを使っているだけでウイルスに感染してしまうようになったのだ。

この時点で、ユーザーがとるべき対策が、「メールの添付ファイルを開く際には細心の注意を払わなければならない」から「どんなメールも安易に読まない」に変化したと言える。

## HTMLメールが作り出した「メールを読むだけで感染する」ウイルス

注意すべきは、「セキュリティーホールを利用しなければ、メールを読むだけで感染する仕組みは実現できない」という事実だ。また、昔のように単なるテキストだけのメールであればこのような問題は起こらなかったことにも注意してほしい。

たとえば、メールソフトの進化により、ウェブページを記述するためのHTMLをメールに使えるようになった。メールに明るい色が使えたり写真や音楽が貼り付けたりできるようになったのだ。ユーザーがこういった便利な機能を使うのは当然だろう。しかし、この機能を実現するために、メールソフト内部では実に複雑な処理が必要となる。その複雑さのために、セキュリティーホールのないソフトウェアを作るのが難しくなり、そのことがウイルスの発生や増殖に拍車を掛けたと言っても過言ではない。

VBS.BubbleBoyが悪用していたセキュリティーホールの内容は、本来はスクリプトから自由に扱えるべきでないActiveXコントロールが「スクリプトに対して安全」と設定されていたというものだ（MS99-032：Scriptlet.TypelibとEyedogのセキュリティー脆弱性）。HTMLメールに含まれたスクリプトが本来扱えないはずの機能を使って感染を広げたのだ。

NimdaやKlezが悪用するセキュリティーホールはまた別のもので、メールのMIMEコードを処理する部分に問題があり、それを悪用することで任意のコードを自動的に実行できるというものだ。不正なヘッダーとMIMEでエンコードされたウイルスファイルを持つメール経由で自分自身を送信し、ユーザーに気づかれることなくウイルスプログラムを実行できたのだ。

このように、「セキュリティーホール」と言ってもさまざまな種類のものがあり、また日々新しいセキュリティーホールが発見され、それを利用するウイルスが作られているのだ。


［図5］HTMLメールで感染するVBS.BubbleBoyウイルス

### メールウイルスが引き起こす人間関係のひび

Klezというウイルスは、感染したパソコンのアドレス帳から適当に選んだメールアドレス宛てにウイルス付きメールを自動的に送信する際に、メールの差出人の情報もアドレス帳にあった適当なメールアドレスの人であるかのように偽造してメールを送る。

これにより、ウイルスメールを受け取った人には、実際にKlezに感染した人とは違う人からウイルスメールが来たように見え、関係ない第三者を巻き込む複雑な事態を引き起こした。さらに悪いことに、Klezは感染したパソコンにあるファイルを適当に添付して送信するので、それが機密情報だった場合には、まったく関係のない第三者が機密情報を持っているように見えてしまうのだ。

単にファイルに感染するのではなく、コミュニケーションの道具として日常使われているメールをウイルスが利用する現在、こういった複雑な問題も発生することにも注意する必要があるだろう。

# ブロードバンド時代の身の守り方

## マルウェアの被害に遭わないためには

最近の複合型ウイルスには単にデータを破壊するだけでなく、パソコン内にある書類を手当たり次第にメールでばらまくものもある。個人情報や機密情報が流出すると、無数にコピーされたり掲示板などに公開されたりして、文字どおり取り返しがつかなくなる。

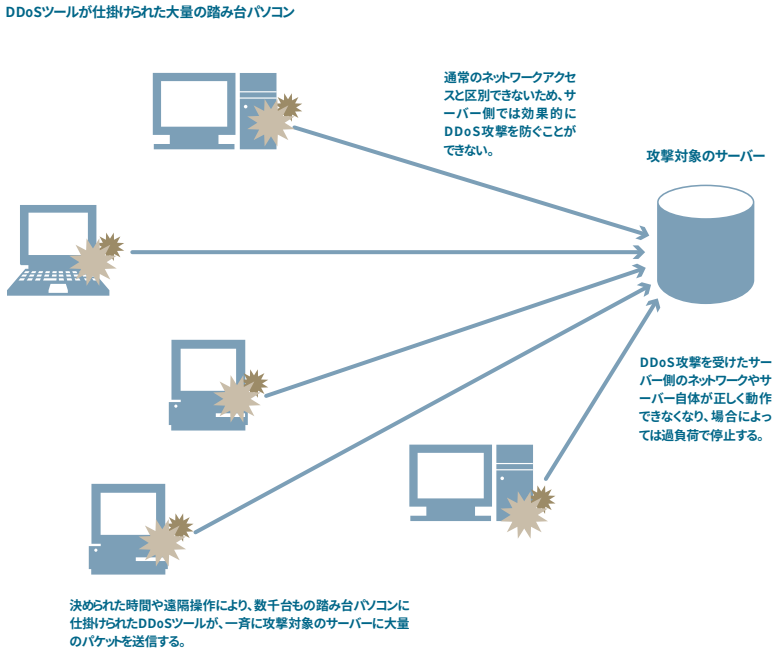
また、情報が盗まれてしまうというだけでなく、感染によってパソコンが悪意のあるユーザーに乗っ取られ、他のパソコンを攻撃するのに使われるということもある。DDoS（分散サービス拒否）という攻撃は、多数のパソコンから同時に特定のサーバーに向けてネットワーク接続を大量に発生させることで、対象のサーバーが正しく機能できないようにする。多くの場合、この攻撃を実際に実行するのは、ウイルスや不正アクセスによってDDoS攻撃用のトロイの木馬を仕込まれた第三者のパソコンだ。こうなると、単なる被害者というだけでなく、他の人に迷惑をかける加害者にもなってしまう（このことを「踏み台」にされるという）。攻撃を受けた側から損害賠償を請求されたり、友人を失ったりすることなりかねない。

しかも、ブロードバンドの常時接続環境では、何が起こっているか理解するまでに、取り返しのつかない状況に陥ってしまっている可能性も高い。では、どのようにして身を守ればいいのだろうか。

## 対策 古いIEはバージョンアップする

これまで述べたように、猛威をふるった多くのウイルスはIEのセキュリティーホールを利用している。Windows 95や98といった古いOSでIE 4.0をそのまま使っているようなパソコンはウイルスの格好の






［図6］DDoS（分散サービス拒否）攻撃の仕組み

的となってしまう。セキュリティー対策がなされた新しいIEにバージョンアップする必要がある。本稿執筆時のIEの最新バージョンはIE 6 SP1だURL。後述するWindows Updateを利用するためにも、古いバージョンのIEからは卒業してほしい。

**Internet Explorerホームページ**
URL http://www.microsoft.com/japan/ie/

## 対策 セキュリティーホールの存在を知り、「パッチ」を適用する

セキュリティーホールを利用して感染するウイルスに対抗するには、セキュリティーホールをなくすのが一番だ。それには、「パッチ」と呼ばれる、欠陥を修正するプログラムを使う。

セキュリティーホールはソフトウェアの開発時に発見されなかったから存在するわけで、ソフトウェアがリリースされて広く利用されるようになってから、第三者がセキュリティーホールの存在を発見して開発元に指摘するのが通常だ。開発元は発見されたセキュリティーホールを修正するパッチを作って配布する。

セキュリティーホールは随時新しいものが発見されるので、自分が使っているOSやソフトウェアに現在どんなセキュリティーホールが見つかっていて、パッチはどこで入手できるのかを、常に調べ続けないといけないということだ。

セキュリティーホールに関する情報は、たとえばINTERNET Watch URL01やZDNet URL02などの代表的なニュースサイトで入手できる。通常は、セキュリティーホールに関する情報が公開される場合には、その修正プログラムを入手する方法も同時に公開されているはずだ。自分の使うOSやアプリケーションに関して「セキュリティーホール」や「脆弱性」といった話がされていれば、記事の内容を詳しく確認する必要がある。ウィンドウズならば、マイクロソフトの「セキュリティスクエア」URL03を確認するのもいいだろう。

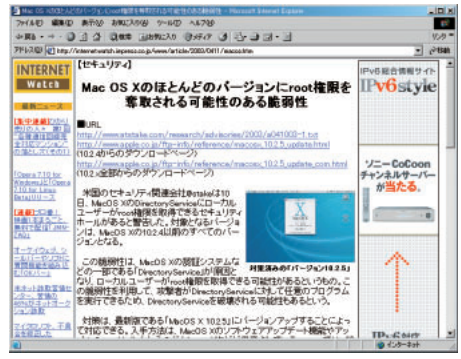
URL01 http://internet.watch.impress.co.jp/
URL02 http://www.zdnet.co.jp/
URL03 http://www.microsoft.com/japan/security/square/

### Windows Updateで手間をかけずに修正プログラムを適用

しかし常に情報を調べ続けるのは大変だ。ウィンドウズならば「Windows Update」の機能を使うのがいい。情報を探し回らなくても、数回クリックするだけで必要なパッチを適用できる。Mac OS 9やMac OS Xにも「ソフトウェアアップデート」という機能があり、簡単に必要なアップデートを適用できる。

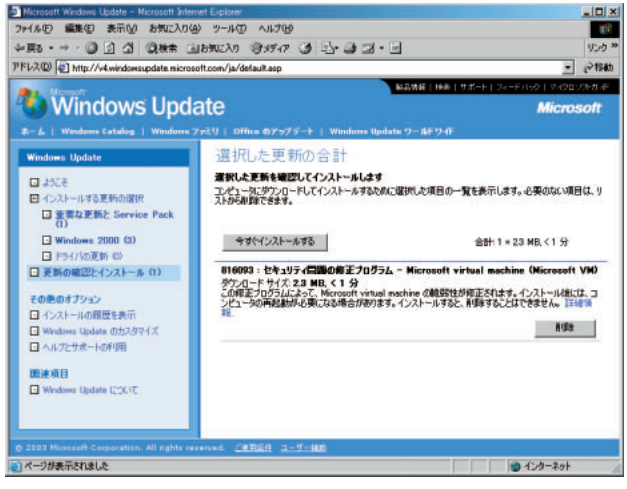
まだ一度もWindows Updateを使ったことがないという人は、今すぐにIEの[ツール]メニューから[Windows Update]を選んでWindows Updateを実行してほしい。週に1回アップデートを実行するだけでかなり安全になる。ある意味で、Windows Updateでシステムを安全に保つことは、インターネット時代の最低限のマナーだと言っても過言ではない。

**自動アップデート機能でセキュリティーホールを修正**





［図7］セキュリティー情報はウェブで積極的に入手




［図8］Windows Updateを使うと簡単にセキュリティーホールを塞げる

## 対策 セキュリティー対策ソフトで守りを強固に

しかし、パッチは提供されるまでには時間がかかるケースもあり、その間はパソコンが無防備になる。また、セキュリティーホールが発見されてからパッチを適用するのは受動的な身の守り方だとも言える。

常に新しいウイルスが作られる中で、自ら進んで安全な環境を保つには、「ウイルス対策ソフト」や「パーソナルファイアーウォール」というソフトウェアを利用する。

### 「ウイルス対策ソフト」と「パーソナルファイアーウォール」で能動的に対策を

「ウイルス対策ソフト」

コンピュータ上にウイルスが潜んでいないかチェックしたり、プログラムの動作を常に監視して、ウイルスやワームの動作があればそれを阻止したりするソフトウェアだ。トロイの木馬やスパイウェアなどの、ウイルス／ワーム以外のマルウェアを対象とする対策ソフトウェアもここに含めて考えていいだろう。

ウイルス対策ソフトには2つの役割がある。1つは、パソコンの中に潜む「ウイルスの検出」、もう1つは、感染してしまったファイルの「ウイルス駆除」だ。

ウイルス対策ソフトはウイルスを検出・駆除するためにさまざまな技術を使う。もっともベーシックな方法は、ウイルス定義ファイルというデータベース（パターンファイルやワクチンとも呼ばれる）を使うものだ。新種のウイルスが発見されるたびにウイルス検出用データがデータベースに追加される。

「パーソナルファイアーウォール」

パーソナルファイアーウォールは、基本的には、ワームによる無差別攻撃や悪意のあるユーザーによる不正アクセスを防ぐのが仕事だ。パソコン内のインターネットへの出入り口でネットワークを通過する情報を監視して、不正なアクセスを遮断してしまうのだ。また、ネットワーク的に無防備なパソコンを探す「ポートスキャン」という攻撃準備行動も、パーソナルファイアーウォールで自動的にブロックできる。

さらにパーソナルファイアーウォールでは、アプリケーションごとに利用するポートと通信の方向を限定できる。つまり、たとえばOutlook以外のメールソフトやプログラムからはメールを送信できないようにするといったことが可能になる。

また、万が一、キーボード操作を記録したファイルや書類ファイルを盗み出すトロイの木馬が仕掛けられていたとしても、アプリケーションごとに利用するポートと通信の方向を限定することにより、情報が流出する瀬戸際でブロックできる。

IDS（侵入検知システム）というプログラムも、ファイアーウォールと同様に不正アクセスの行為を検知してブロックするプログラムだ。ウイルス定義ファイルのようなパターンを元に通信データを調べるなど、ファイアーウォールよりも高度な機能があるものが多いが、ここでは複雑になることを避けるためにファイアーウォールの中に含めて考える。

代表的なウイルス対策ソフト／パーソナルファイアーウォール製品

| 名称 | ウイルス対策機能 | ファイアーウォール機能 | 対応OS | 発売元 | 価格 |
|---|---|---|---|---|---|
| ウイルスバスター2003 | ○ | ○ | Win | トレンドマイクロ | 8,500円 |
| Norton AntiVirus 2003 | ○ | | Win | シマンテック | 6,800円 |
| Norton AntiVirus for Macintosh 8.0 | ○ | | Mac | シマンテック | 9,800円 |
| Norton Personal Firewall 2003 | | ○ | Win | シマンテック | 6,800円 |
| Norton Personal Firewall for Macintosh 2.0 | | ○ | Mac | シマンテック | 9,800円 |
| Norton Internet Security 2003 | ○ | ○ | Win | シマンテック | 9,800円 |
| Norton Internet Security for Macintosh 2.0 | ○ | ○ | Mac | シマンテック | 13,800円 |
| McAfee.comウイルススキャンオンライン | ○ | | Win | ソースネクスト | 1,980円 |
| McAfee.comパーソナルファイアウォールPlus | | ○ | Win | ソースネクスト | 1,980円 |
| McAfee.comインターネットセキュリティSuper | ○ | ○ | Win | ソースネクスト | 2,980円 |
| PestPatrol | △* | | Win | アークン | オープン価格 |
| RealSecure BlackICE PC Protection | | ○** | Win | アクト・ツー | 9,800円 |

*PestPatrolはスパイウェアなどの、ウイルス／ワーム以外のマルウェア対策の機能を持つ。 **RealSecure BlackICE PC ProtectionはIDS（侵入検知システム）の機能を持つ。

シマンテック URL http://www.trendmicro.co.jp/　トレンドマイクロ URL http://www.symantec.co.jp/　ソースネクスト URL http://www.sourcenext.info/mcafee/

アークン URL http://www.pestpatrol.jp/　アクト・ツー URL http://blackice.jp/

ウイルス対策ソフトはマルウェアという「もの」を検出し、パーソナルファイアーウォールはマルウェアなどによる不正アクセスという「行為」を検出する。万能に見えるウイルス対策ソフトだが、有害な「もの」しかブロックすることができない。逆に、パーソナルファイアーウォールもすでにパソコン内に潜んでいる有害プログラムを見つけ出すことはできない。このため、相補う2つのソフトを組み合わせて使うことが有効になる。

## ウイルス対策ソフト使用時の注意

ウイルス対策ソフトを使ううえでの注意点がいくつかあるので紹介する。細かい設定方法はソフトウェアごとに異なるので、ソフトウェアのマニュアルを参照してほしい。

### 複数のウイルス対策ソフトをインストールしない

ほとんどの場合、複数のウイルス対策ソフトをインストールしてはいけない。2つのウイルス対策ソフトの動作が衝突して問題を引き起こす可能性が高い。

### 常時監視機能は必ずオンにする

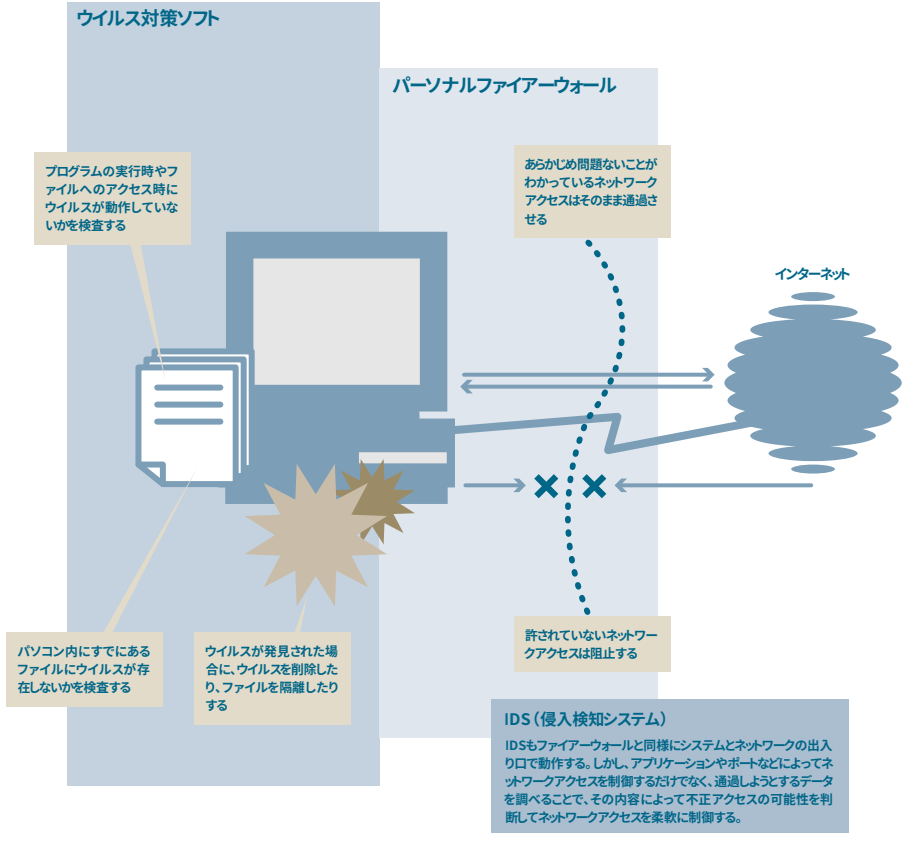
常時監視機能とは、プログラムを実行するとき、ファイルを開くとき、ファイルをコピーするときなどに自動的にウイルス検査をしてくれるというものだ。この機能をオンにすることにより、添付ファイルを誤って開くなどのウイルスに感染する行為をしてしまっても、ウイルス対策ソフトによりウイルスの動作をブロックできる。

### ウイルス定義ファイルを定期的に更新する

前述のように、ウイルス定義ファイルは、毎月200種類とも300種類とも言われる新種のウイルスが発見されるたびに更新される。逆に言うと、常に最新の定義ファイルを使わないと新しいウイルスには対応できないとうことだ。少なくとも週に一度は更新された定義ファイルがないかを確認するべきだ。ソフトウェアによって多少違うが、たいていボタン1つでインターネットを通じて定義ファイルを更新できる。定期スケジュールや全自動で定義ファイルを更新するような設定もできるはずだ。

### 定期的にパソコン全体のウイルス検査を行う

知らず知らずのうちに侵入しているウイルスを発見するために、定期的にパソコン全体のウイルス検査をする必要がある。「新しいウイルス定義ファイルに更新したらスキャンする」や「毎月10日はスキャンの日」などのように決めて、定期的にパソコン全体のスキャンを実行するべきだ。




［図9］ウイルス対策ソフトとパーソナルファイアーウォールの違い

### プロバイダーのウイルスチェックサービス

メールを使って感染するウイルスは、プロバイダーのウイルスチェックサービスを利用することでも防げる。

サービスによって異なるが、基本的には送受信するすべてのメールを自動的にウイルスチェックして、ウイルスメールであれば自動的にウイルスを駆除するかメールを破棄したうえで、ウイルスメールの報告をしてくれるというものだ。

ウイルス対策ソフトの起動し忘れや、ウイルス定義ファイルを更新していなかったなどのミスがないのがメリットだ。

こういったサービスを無料または月あたり数百円で利用できるプロバイダーも多いので、自分の利用しているプロバイダーのサービスメニューを確認してみるといい。

ただし、この方法で防げるのはメールを使ったウイルスやワームの感染だけなので注意してほしい。それ以外のウイルスは防げない。

# ［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的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