2004年5月号/特別付録
日経PC21 保存版

ウイルス「予防&撃退」マニュアル

まさか!? のときも安心

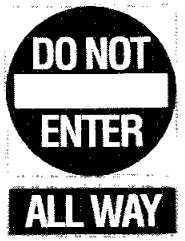
基礎知識 **敵を知る**
ウイルスの特徴と傾向をガッチリつかむ

予防法 **守りを固める**
感染しないための予防法をしっかり習得

対処法 **感染が疑わしいときは**
慌てずに確認、修復を進めるための手順

まさか!? のときも安心

ウイルス 予防 撃退 マニュアル



電子メールやインターネットが普及して、パソコンがぐんと便利になった一方で、新種のコンピューターウイルスが増え、その手口はどんどん巧妙化しています。感染すると大量のウイルスメールをばらまき、被害者は即、加害者に。もはや、ウイルス対策は、すべてのパソコンユーザーの常識です。本書では、ウイルスについての基礎知識から、感染しないための予防法、そして「感染したかも?」というときの対処法をまとめました。ぜひ、お手元においてご活用ください。

日経PC21編集部

CONTENTS

■敵を知る

■守りを固める

■感染が疑わしいときは

※本書ではウィンドウズXPを対象に解説していますが、ウイルスの基礎知識、ウイルス対策ソフトの使い方、感染時の対処法などの考え方は98/Meも同じです。お役立てください。

敵を知る

基本知識

コンピューターウイルスから自分のパソコンを守るには、「敵」がどんなものなのか知ることが大切だ。まずはその特徴を見てみよう。

コンピューターウイルスって何？

●メールやインターネットを使うならウイルス対策が必要だ

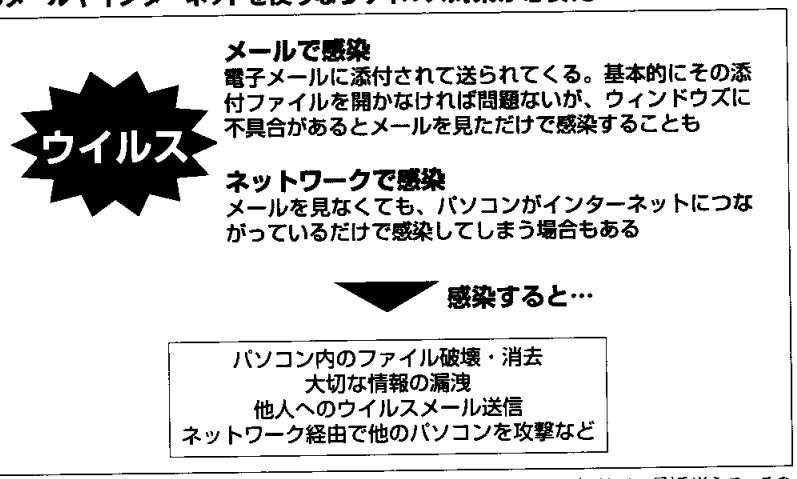


図1　ウイルスには「メールで感染するもの」と「ネットワークから感染するもの」がある。最近増えているのはネットワーク型のウイルスだ。感染するとウイルスメールを大量送信したり、ほかのパソコンを攻撃するものもある

データを破壊したり、大量のウイルスメールをばらまくなど、パソコンの安全を脅かすコンピューターウイルス（以下ウイルス）。かつてはメールの怪しい添付ファイルさえ開かなければ感染することはなかったが、現在では、ユーザーが何もしなくても、「セキュリティーホール（不具合）」を悪用して、勝手にメールの添付ファイルを開いて感染させたり、インターネットにつなぐだけで感染する悪質なウイルスが増えている（図1）。

今や「何もしなければ感染しない」のではなく、「何も（対策を）しなければ感染してしまう」のだ。しかも、感染すれば今度は自分がウイルスメールを大量送信して加害者になってしまう。取引先などにウイルスを送れば信用問題、賠償問題にもなりかねない。ウイルス対策はもはや、パソコンユーザーの常識だ。

対策の第一歩は「敵を知る」こと。ウイルスの特徴や傾向を知っておこう。まず、ウイルスはその性質によって、ほかのファイルに寄生するもの、自分のコピーを大量送信して自己増殖する「ワーム」、あとから侵入するための仕掛けを作る「トロイの木馬」などがある（図2）。最近ではこれら複数の特徴を兼ね備えた複合型のウイルスも多い。

●ウイルスにはいろいろなタイプがある

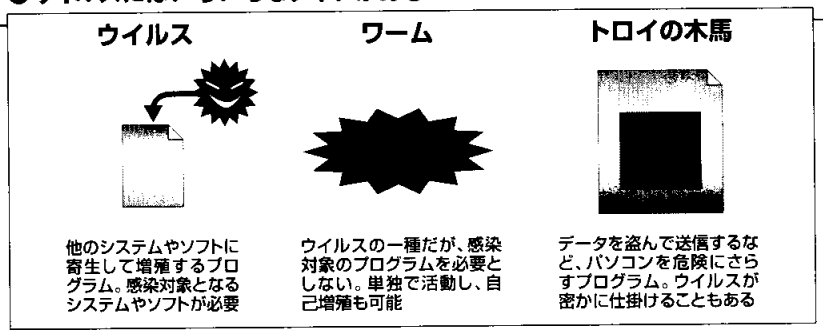


図2　一口にコンピューターウイルスといっても、厳密にはウイルス、ワーム、トロイの木馬などの種類がある。本記事ではこれらを総称してウイルスと呼ぶ。最近ではこれらを組み合わせた複合型のウイルスも増えている

ウイルスの感染経路は、(1)メールの添付ファイルとして送られてくる、(2)ネットワーク経由で感染する、の2つが圧倒的に多い。添付ファイル型は、じわじわと感染が広がることが多く、その後、長期間にわたって流行する傾向にある。一方、ネットワーク感染型は感染スピードが速く、中にはわずか数時間で世界中に広がった例もある。だがその分終息も早い。ウイルスごとに「発見から7日間での感染報告件数」をまとめたのが図3だ。ブロードバンド回線の普及で常時接続ユーザーが増えたところへ、ネットワーク型ウイルスが登場し、短期間に一気に感染が広がる傾向は今後も続くと予想されている。

●発見から7日間の感染報告件数は増加中

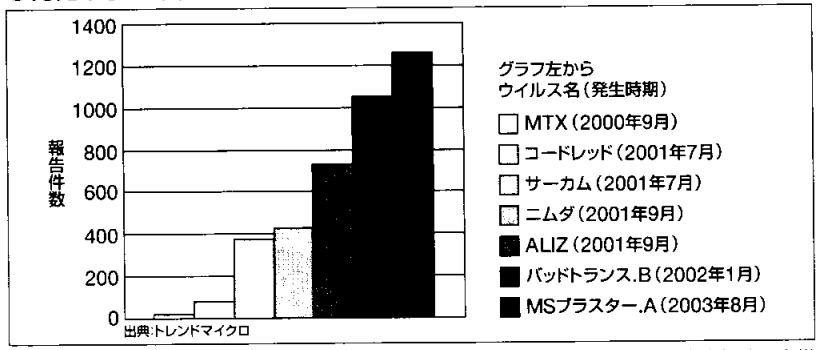


図3　歴代のウイルスを並べてみると、最初の7日間で感染する件数が増加している。感染経路の多様化などにより、短期間で広い範囲に感染するようになっている

敵を知る…… 基本知識

メールの添付ファイルには要注意

●ウイルスは添付ファイルでやってくる

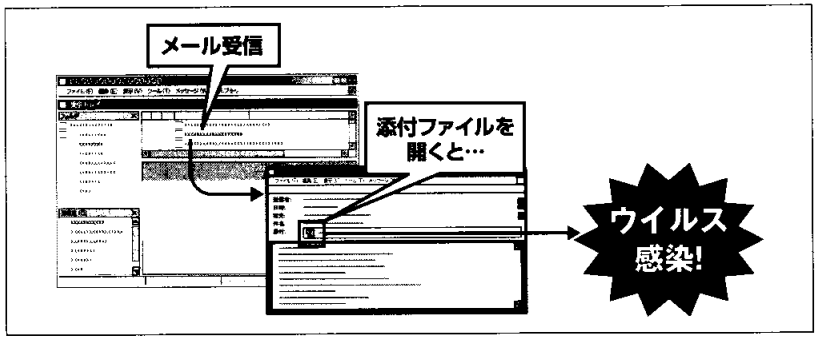


図1　ウイルスはメールの添付ファイルとしてやってくるケースが多い。基本的にウイルスは添付ファイルを開いたときに感染するので、怪しいメールを受け取ったら絶対に添付ファイルを開かないことが大切だ

メールの添付ファイルに注意

- ウイルスはメールの添付ファイルとして送られてくることが多い
- 心当たりのない怪しい添付ファイルは絶対に開かない

ウイルスの感染経路としてよく使われるのがメールだ。メールの添付ファイルにウイルスが潜み、受信者がそのファイルをうっかり開く(＝実行する)とウイルスが活動を開始する(図1)。

動き出したウイルスは、まずパソコン内のアドレス帳などからメールアドレスを収集する。次に、集めた宛先に自分自身のコピーを添付したウイルスメールを送信する。こうして次々と他のパソコンに感染を広げていくわけだ。こうした動きは"裏で"行われるため、感染していても、感染に気付かずに使い続けているユーザーも多い。

では実際に、どのような添付ファイルに気をつければよいのだろう。その手がかりになるのが図2にまとめた拡張子(ファイル名の末尾、3文字の英文字＝ファイルの種類を表す)だ。もちろん、これらの拡張子がついているファイルすべてがウイルスとは限らないが、特に注意してほしい。こうしたファイルがメールで届いても、原則は開かないことだ。

拡張子は怪しいファイルを見つける手がかりとなるが、ウィンドウズやメールソフトの設定によっては拡張子が表示されていない場合もある。これを利用して、拡張子を二重に付けてユーザーをだまそうとするウイルスもある。

例えば「image.jpg.vbs」と拡張子を二重に付けた場合、拡張子が表示されない設定になっていると、そのファイルは「image.jpg」とあたかも画像ファイルかのように見えてしまう。

ファイル名に拡張子が表示されない設定になっている場合は、フォルダを開いた画面で「ツール」→「フォルダオプション」を選択。「表示」タブで「登録されている拡張子は表示しない」のチェックを外して、表示させよう。

メールの添付ファイルはちょっとした文書や写真を送るときに便利だが、開くときは念には念を入れて安全を確認しよう。見知らぬ相手からの添付メールはもちろん、知り合いからのメールでも安心できない。ウイルスは送信者を詐称することがあるためだ。逆に、自分がメールにファイルを添付するときは内容を明記しよう。

●ウイルスによく使われる添付ファイル

EXE	プログラムの実行ファイル。悪意あるプログラムはファイル削除やウィンドウズの破壊などを行える。無警戒に開くのは危険だ。ただし「自己解凍形式」の圧縮ファイルの可能性もある
COM	これも開くとプログラムが実行される。「www.●●●.com」のようにインターネットのアドレスに見せかけるものもあるので注意
BAT	複数のプログラムを連続実行するためのファイル。ファイルを書き換えられたり削除される危険がある
VBS	プログラム言語の「VBスクリプト」(Visual Basic Script)で書かれたプログラム。ウィンドウズの不具合を利用してウイルスを感染させる際に使われることが多い
HTML	ウェブページを記述するためのファイル形式だが、最近はメールに用いることも多い。インターネット・エクスプローラ(IE)に不具合があると、見ただけでウイルスに感染することがある
URL	実行すると指定されたウェブページを開く。ファイル自体は無害だが、訪問先のウェブページにウイルスが仕込まれている可能性もある(拡張子は表示されない)
PIF	ウィンドウズ上でMS-DOSのプログラムを実行するときに使う設定ファイル
SCR	ウィンドウズ用のスクリーンセーバーのファイル形式。実体はEXEファイルとほぼ同じで、プログラムを実行する

図2　ウイルスの添付ファイルによく使われる拡張子。これ以外のファイル形式なら安心というわけではないが、怪しいファイルを見分けるひとつの手がかりになる

メール本文を表示しただけで感染

●ウィンドウズに不具合があると「見ただけ」で感染する

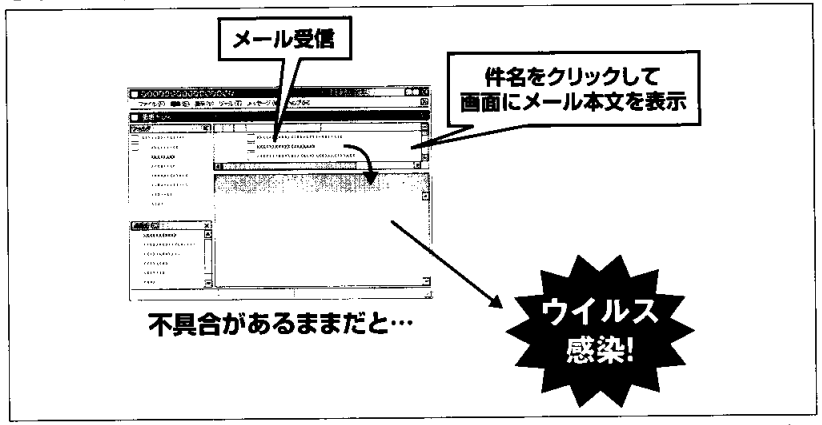


図1　ウィンドウズに不具合があるままだと、メールを表示させただけでウイルスに感染してしまうこともある。防ぐにはウィンドウズアップデートを定期的に実行してウィンドウズを最新状態に保てばよい

"見るだけで感染"しないために

ウィンドウズに不具合があるとメール本文を見ただけで感染するおそれも

ウィンドウズアップデートを必ず実行し、常に最新状態に保っておこう

添付ファイルを開かなくとも、メールを見ただけ、パソコン画面に表示させただけで感染するウイルスもある(図1)。

これは「セキュリティーホール」と呼ばれるウィンドウズの不具合を悪用したものだ。通常、メールソフトは添付ファイルを受け取ると、それを開く(=実行する)かどうかをユーザーに確認する。だが、ウィンドウズにセキュリティーホールがあると、メールの本文に埋め込まれた特定の文字列が、このセキュリティーホールを通じて、メールに添付されたウイルスファイルを勝手に開いてしまうのである(図2)。ユーザーはメールを見ただけ、パソコンの画面に表示させただけで感染する。

2001年10月に発見されて大流行したウイルス「クレズ」も、こうしたウイルスの1つだった。だが、マイクロソフトがこの不具合を直す修正プログラムを提供したのは2001年の3月。クレズが登場する半年以上も前のことだ。この半年間に修正プログラムを実行していれば、メールが届いても添付ファイルは自動実行されず、クレズに感染することはなかったのだ。だが、適用していないユーザーが多く、クレズは大流行してしまった。

さらに、このクレズの教訓は十分生かされたとは言い難い。1年後の2002年10月に登場した「バグベアー」というウイルスもまったく同じ不具合を利用し、やはり大流行したのだ。1年半の間、修正プログラムを利用していないユーザーが多かったということだ。

最近ではインターネットにつなぐだけで感染するウイルスも登場しているが、これもセキュリティーホールを悪用したものだ(次のページで解説)。

こうしたウイルスを防ぐにはウィンドウズアップデートを実行して修正プログラムを適用し、ウィンドウズを最新の状態に保てばよい(p.20～23)。それを怠ってウイルスに感染してしまったときのダメージと比べれば、はるかに簡単な作業である。

●不具合を悪用してウイルスを自動実行

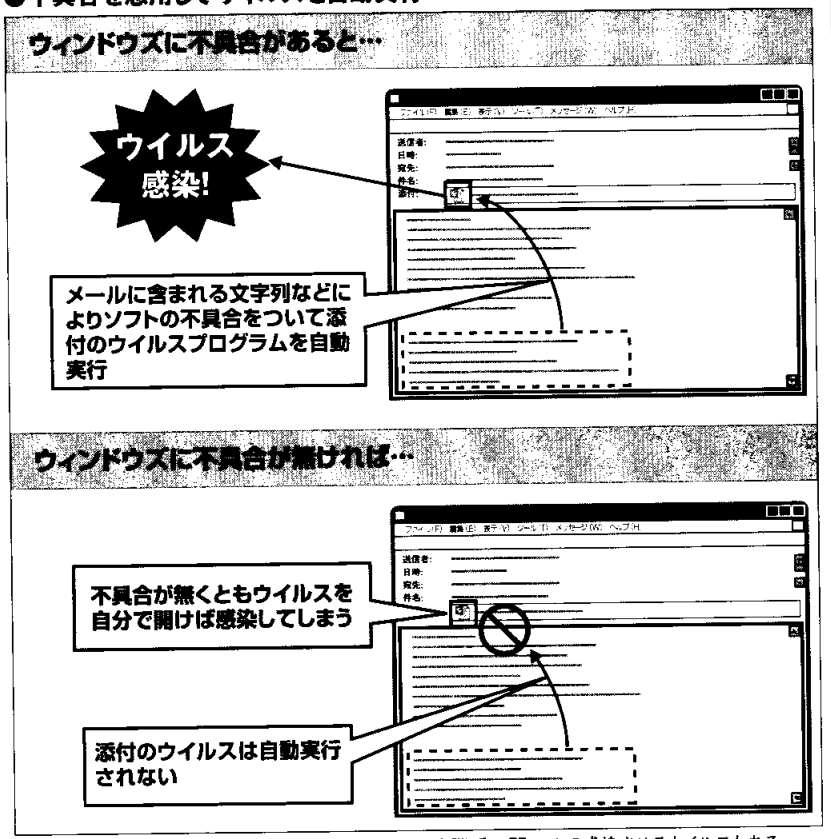


図2　ウィンドウズの不具合を悪用して、添付ファイルを勝手に開かせて感染させるウイルスもある

敵を知る…… 基本知識

インターネットにつないだだけで感染

●気付かないうちにネットからウイルスが侵入

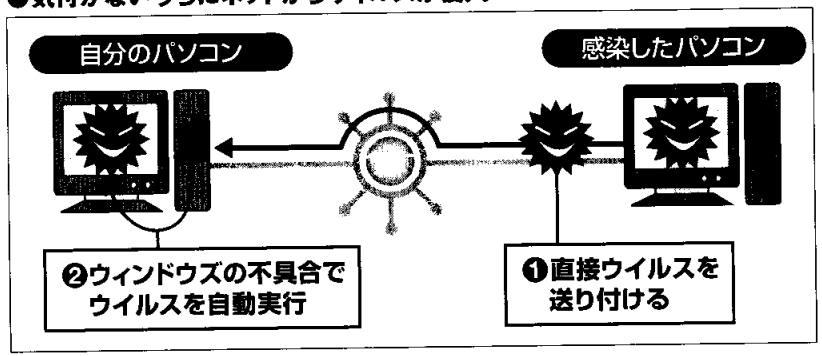


図1　ネットワーク型のウイルスは不特定多数のパソコンに、ウイルスを送り付けてくる。ウィンドウズに不具合があると、インターネットにつないだだけで、知らない間に侵入されてしまう。さらに、特定の日に特定の企業のウェブページに攻撃を仕掛けるといった悪さをすることも

"つないだだけで感染"を防ぐ

インターネットにつながっているだけで感染するウイルスも登場

感染の広がりが速いのでウィンドウズや対策ソフトのこまめなアップデート、ファイアウオールが必要

最近、急増しているのがネットワーク経由で感染するウイルスだ(図1)。ユーザーがメールを開いたり、ウェブページを見るなどのアクションを起こさなくても、インターネットにつないだだけで自動的に感染する。2003年8月に登場して大流行した「MSブラスター」が記憶に新しい。感染したパソコンが次から次へと攻撃を繰り返すので、ネットワーク型ウイルスは、メールで広がるウイルスよりも、短期間のうちに爆発的に広がるのが特徴だ。

また、メールの添付ファイルやネットワーク経由など、複数のルートを使って感染を広げるウイルスも増えている。2001年9月に発見されたニムダはその草分けとも言える存在だ(図2)。メール本文を表示させるだけで感染するばかりか、会社のLANなどのネットワーク経由でも感染する。さらに、特定のサーバーを攻撃して、サーバーに不具合があるとウイルスはそこから侵入し、サーバー上のウェブページを改変してしまう。そしてそのウェブページにアクセスしたユーザーも、改変されたページを見ただけで感染する。メール、ウェブ、ネットワークと、いくつもの感染経路を持つ複合型のウイルスだ。

メールだけでなくネットワークを利用するウイルスは今後も増えると予想さ

●増えてきた複合型ウイルス(ニムダの感染例)

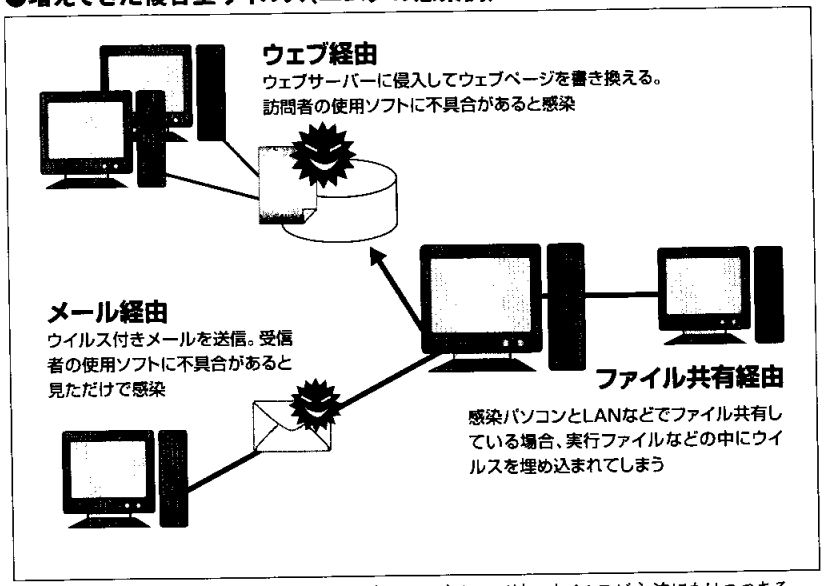


図2　メール、ネットワークなど複数の感染方法を組み合わせて持つウイルスが主流になりつつある

れているが、誰もがインターネットにつないだだけで自動的に感染してしまうわけではない。ネットワーク型ウイルスが狙うのも、ウィンドウズの「セキュリティーホール」だ。まずは、ウィンドウズアップデート(p.20～23で解説)をきちんと実行して、セキュリティーホールをふさいでおくことが大切だ。

また、「ファイアウオール」(p.34参照)や「ルーター」(p.19参照)を導入することによってもネットワーク型ウイルスは防ぐことができる。ファイアウオールは通信の出入りを監視して、不正なアクセスをブロックするものだ。一方のルーターは、複数のパソコンをインターネットに接続する機器だが、個々のパソコンのアドレスを外から隠し、ファイアウオールの代わりとなる。逆に言えば、これらがない状態は、どんなアクセスも"素通し"にしてしまう危険な状態と言える。

ファイアウオール機能はウィンドウズXPにも標準装備されているが、ウイルス対策ソフトがファイアウオール機能を備えているものも多く、しかも設定が簡単だ。ウイルス対策ソフトを使っているなら、ファイアウオール機能を確認して、ウイルスチェックと併せて利用しよう。これからのウイルス対策には「通信の見張り番」は欠かせないもの、と覚えておこう。

感染するとどんな被害にあう?

●代表的なウイルスの動作

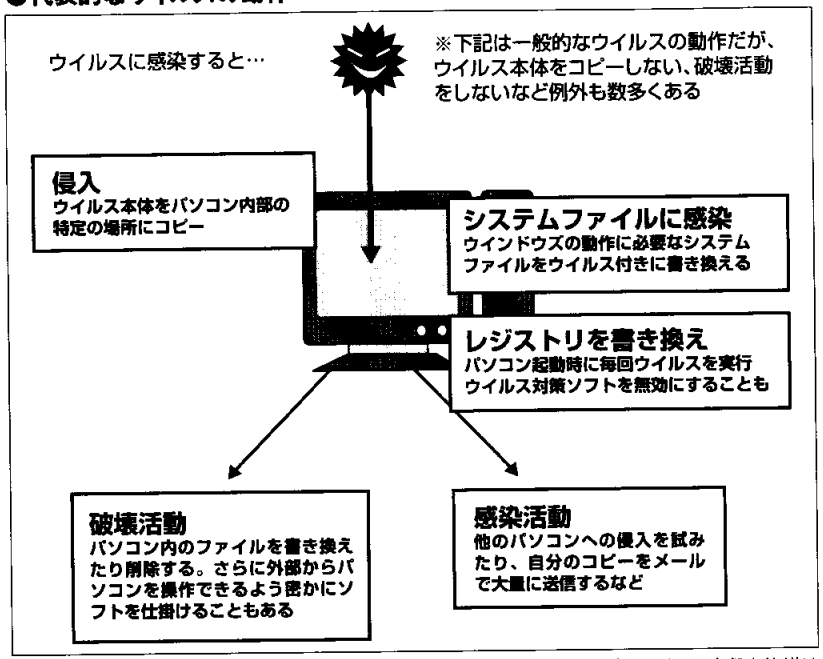


図1　ウイルスの活動内容は多種多様だ。ファイルを消したり、特定のウェブサーバーに攻撃を仕掛けるといった破壊的な活動をしたり、パソコン内の文書を外部にばらまくなど情報漏洩につながる活動をするものも少なくない

感染すると加害者に

感染すると ウイルスメールを送り、加害者になる

ファイルを削除されたり ウェブサイトを攻撃したり 情報を漏らされることも

ウイルスはパソコン内部に侵入するとさまざまな活動を行う。パソコンのハードディスクに自分自身をコピーし、ウィンドウズの起動時に常に実行されるように「レジストリ」というウィンドウズの設定ファイルを書き換えるものもある(図1)。

ユーザーが感染に気付くのは症状が現れたとき。一昔前は、決まった日になると画面に花火を打ち上げる、ファイルを消してしまうなど、被害を受けるのは主に自分のパソコンだった。だが、インターネットの普及に伴い、それだけでは済まなくなっている。例えば2003年8月に登場した「MSブラスター」や2004年1月に現れた「マイドゥーム」などは、特定の日になると一斉に特定企業のウェブサーバーを攻撃するプログラムが仕込まれていた。多数の感染者による一斉攻撃にさらされ、一時ウェブサイトがダウンしたケースもある。

パソコン内の情報を盗み出そうとするウイルスも見つかっている。2003年6月に発見された「バグベアー」は、感染先のパソコンにユーザーのキー入力を記録するソフトを仕込む。ユーザーが入力したパスワードが筒抜けになる可能性があるのだ。ほかにもパソコンを遠隔操作できるようにする仕掛けを残したり、任意のファイルを拾い出して勝手にメールで送信してしまうものもある。

感染活動も進化している。以前はアウトルック・エクスプレスなどのメールソフトを使ってメールを送信するウイルスが多かったが、現在ではウイルス自身がメール送信機能(SMTPサーバー)を持っているものが多い(図2)。パソコン内のアドレス帳や、ウェブページの履歴などからメールアドレスを拾い出し、片っ端から自分自身のコピーを送信する。だがメールソフトを使わないので送信履歴は残らない。このため何カ月も感染に気付かずウイルスメールを周囲に送り続けてしまうユーザーも実際にいる。感染は、単にパソコンの被害だけにとどまらず、個人や企業の信用問題にもなりかねないのだ。

●ウイルス自身が送信機能を持ち、気付かぬうちにウイルスメールを送信

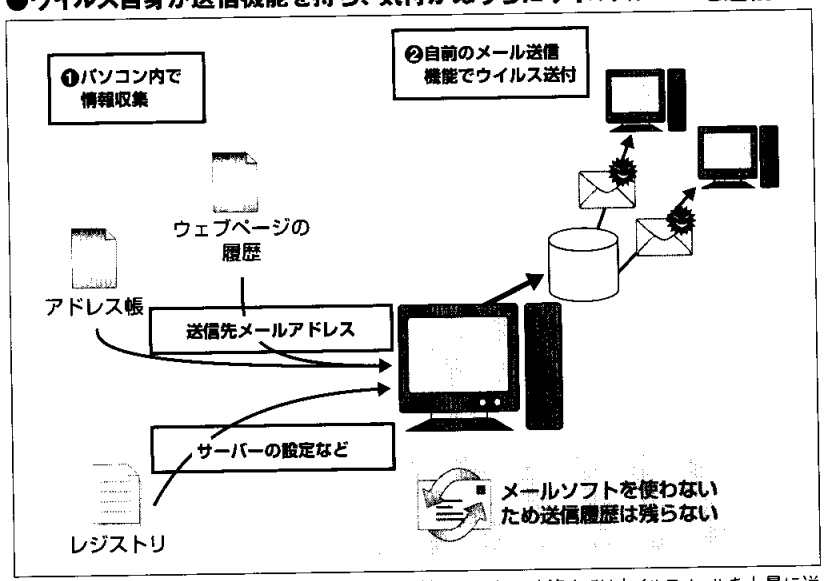


図2　ウイルスは独自のメール送信機能(SMTP)を持ち、アドレスを盗んではウイルスメールを大量に送信する。ユーザーのメールソフトに送信履歴はなく、痕跡を残さない

最近のウイルスの巧妙化する手口

ウイルスは、感染を広げるためにあの手この手を使ってやってくる。添付ファイルを開かせるための巧妙な手口には、もはや感心させられるほどだ。

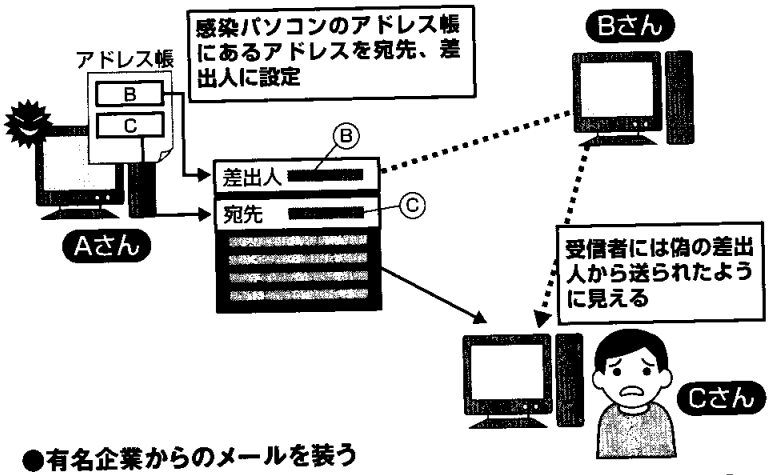
まず、差出人の詐称だ。ウイルスメールを送信する際に、感染先パソコンのアドレス帳から抜き出した任意のメールアドレスを送信者に設定する(図1)。その際に、任意のファイルを盗んで添付するものもある。「04年度予算表」「売上管理表」「××企業向け見積書」といった企業の重要ファイルがウイルスによって流出したこともある。

また、マイクロソフトやウイルス対策ソフトメーカーからのセキュリティー情報のメールを装うウイルスもある。「修正プログラムを送ります」とウイルスファイルを添付して送ってくるのだ。最近では「メッセージが届きませんでした」というメールサーバーからのエラーメッセージを装う「マイドゥーム」が流行した。

マイドゥームは添付ファイルのアイコンも偽装している。実際は実行ファイル(拡張子は「exe」)なのに、メモ帳アイコンなどになっているのだ。アイコンだけ見てテキストファイルだからと安心して実行すると、感染してしまう。通常のファイル圧縮に利用する「ZIP」ファイルのウイルスも登場しており、添付ファイルには用心が必要だ。

また、これまでは件名や本文が英語のウイルスがほとんどだったが、「日本語」のウイルスも登場。ほかにも、わざわざパスワードをかけたファイルを添付して、メール本文に書いてあるパスワードを入力させて感染させるウイルスも登場している。どんどん巧妙になるウイルスに引っかからないためには、ウイルス情報に敏感になる以外にはない。

●送信者も受信者もアドレス帳から抽出。差出人を詐称する



●有名企業からのメールを装う

(例)
差出人：support@microsoft.com
件名：Your password
添付ファイル：password.pif

●添付ファイルのアイコンを工夫

(例)


ejfwixqfyqe.exe


Document.scr

添付ファイルのアイコンを電卓やメモ帳に見せかける。ファイルを開くと実際に電卓やメモ帳が起動するが、その裏でユーザーに気付かれないように感染活動を開始する

巧妙化するウイルスの手口

- メールの差出人を詐称。知り合いからのメールでも添付ファイルは慎重に扱おう
- 有名企業を装ったり、エラーメッセージに似せたウイルスメールもある

「デマウイルス」にも注意しよう

「×××というウイルスが大流行中です。このウイルスには対策ソフトが効きません。あなたのパソコンのシステムフォルダに○○○というファイルがあったら、それがウイルスです。危険なので、すぐに削除してください。なお、友達などにもこの情報を至急知らせてあげてください」。

このようなメールは、デマウイルスと呼ばれている。厳密にはウイルスではなく、言葉でユーザーを巧みにだますイタズラだ。メッセージを見て、慌ててシステムフォルダの○○○というファイルを消すと、実はそれがウィンドウズの重要なファイルで、起動できなくなったりする。ユーザー自身にパソコンを破壊させてしまうわけだ。

悪いことに、誰かがこのメッセージを信じて転送すると、受け取った人も友人からの情報ということで信じてしまいやすい。こうしてデマウイルスは人々の"善意"によって広まっていく。このようなメールを受け取ったら、対策ソフトメーカーのウェブサイトなどで真偽を確認すること、そして安易に転送しないことが大切だ。

ウイルスの最新情報はここでチェック

対策ソフトメーカーのウェブをチェック

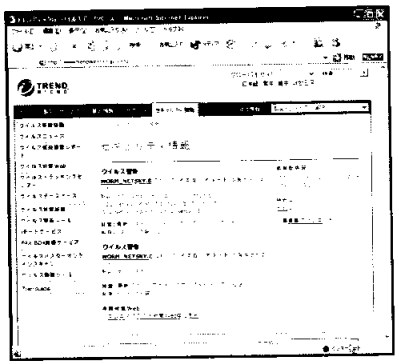
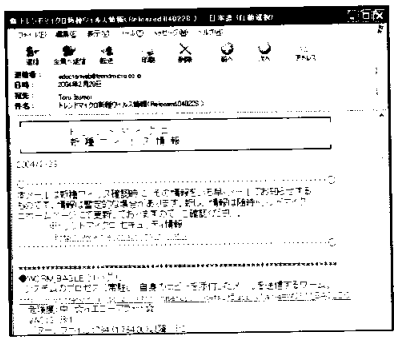


図1　ウイルスの詳細な情報がいち早く掲載されるので「感染したかも」と思ったらまずチェックしよう。ウイルスの基礎知識を学べるコーナーや感染してしまった場合の駆除ツールも手に入る。トレンドマイクロ(http://www.trendmicro.com/jp/home/personal.htm)、シマンテック(http://www.symantec.com/region/jp/homecomputing/)



メールによる通知を利用

図2　注意を要するウイルスが発生したときなどにメールで知らせてくれるサービスもある。いつ発生するかわからないウイルスに対応する上で心強い味方だ。左はトレンドマイクロのウイルス警告メール(http://www.trendmicro.com/jp/security/email/overview.htm)

最新のセキュリティー動向をつかむ

- **新種ウイルスの発生情報やその特徴など、ウイルス情報を入手する**
- **日頃からニュースをチェック。セキュリティー意識を持つようにしよう**

「まさか自分が感染するとは思いませんでした」と、とあるソフトメーカーの社員が自らのウイルス感染について話してくれたことがある。海外出張で2週間ほど留守にして、帰ってから自宅のパソコンを起動。留守中にたまったメールを早くチェックしようと、メールソフトを一番に開いて、知り合いからのメールと添付ファイルを開いたという。

「すぐに変だと気付いたんです。メールの本文が英語だったし、おかしいと。海外出張だったので英文メールに慣れてしまっていたのも不運でした。ウイルス対策ソフトを更新してから全スキャンを行ったら、感染していたんです。新種のウイルスでした。血の気がサーッと引きましたね。パソコンには取引先のメールアドレスも入ってましたから。大騒ぎして周囲にお詫びのメールを送りまくり、パソコンは結局、再セットアップしました。あとで聞いたらそのとき、大流行中のウイルスの亜種だったんです」

ウイルスは日々進化を続けている。亜種(最初に登場したウイルスを真似たウイルスをいう)をも含めると毎月数百に上る大量のウイルスが発生している。そうした中でパソコンを安全に保つには、ユーザーのセキュリティーに対する意識が大切だ。

「コンピューターウイルス？なにそれ？」「ウイルス対策？特に何もしてません」では、もはや済まされないのだ。ウイルスについて知り、特徴や流行情報を入手して、日頃からセキュリティー意識を持つことが重要だ。

ウイルスに関する詳しい情報を得るには、何と言ってもウイルス対策ソフトメーカーのウェブサイトを見るとよい(図1)。ウイルスの特徴、感染経路、症状など、詳細な情報を入手できる。

特に危険なウイルスが発生した場合に、それをメールで知らせてくれるサービスもある(図2)。ぜひ登録しておきたいサービスだ。ニュースサイトをチェックして、ウイルスの動向やウィンドウズの不具合など、セキュリティー情報を把握しておくことも大切だ(図3)。IPA(情報処理推進機構)もウイルスの地域別感染状況など、ユニークな統計情報を公開している(図4)。日頃からニュースなどでセキュリティー情報をチェックして、セキュリティーに対する意識を高めておくことが大切だ。

ニュースサイトをチェック

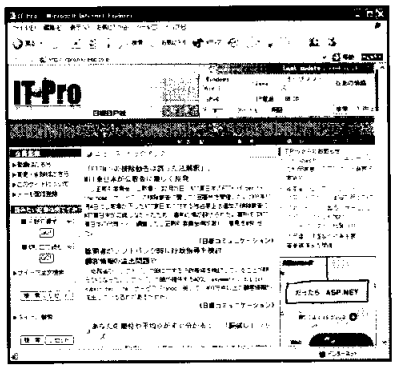
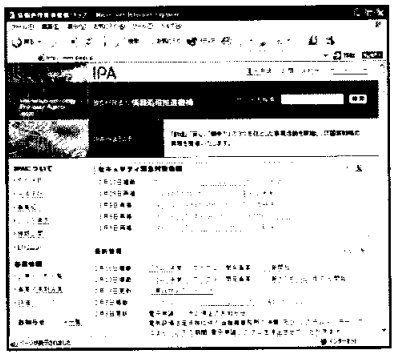


図3　新たに発見された不具合や、現在流行しているウイルスといったセキュリティー関連の最新ニュースを把握するにはニュースを読むのが一番だ。見出しだけでも目を通す習慣を付けたい。右はITPro(http://itpro.nikkeibp.co.jp/)



IPA(情報処理推進機構)

図4　日本のITの発展のために設立された独立行政法人。セキュリティー関連情報の収集、分析している。ウイルス発生の届け出を受け付けており、地域別の被害件数の推移などの情報を掲載している(http://www.ipa.go.jp/)

守りを固める

予防法

ウイルスに感染すると周囲に大きな迷惑をかける上に、修復・復旧には時間も費用もかかる。何より感染しないための対策が重要だ。

ウイルス対策の方法は4つ

ウイルス対策のポイント

1. ウィンドウズアップデートは必ず実行する
2. ウイルス対策ソフトを導入しウイルスを検出、駆除する
3. ウイルス対策ソフトを導入しファイアウオールを利用する
4. メールソフトのセキュリティー設定も忘れずに

ウィンドウズには「セキュリティーホール」と呼ばれるセキュリティー上の不具合がある。最近の多くのウイルスはこの不具合を悪用し、メール本文を表示させただけで添付ファイルを勝手に開いたり、インターネットにつないだだけでウイルスに感染させる。ウイルス対策の第一歩は、このセキュリティーホールをふさぐことだ。これには「ウィンドウズアップデート」を利用する。インターネット経由でウィンドウズのセキュリティーホールなどの不具合を修正できる機能だ。随時、修正プログラムが用意されるので、常に最新の修正プログラムをインストールすることが大切だ(図1)。

対策を講じていても、ウイルスに感染することはある。そのときは市販のウイルス対策ソフトで検知・駆除する(図2)。ただし、対策ソフトは感染を予防するのが主な機能。感染してからソフトを買ってきたのでは手遅れになる可能性がある。感染する前に必ず導入しておこう。

また、最近急増し、短時間に被害を拡大させているのはネットワークに接続するだけで感染するネットワーク型のウイルス。これを防ぐにはファイアウオールと呼ばれる「壁」を設ければよい。外からの通信を見張り、不正なアクセスをブロックする機能だ。ウィンドウズXPには、ファイアウオール機能が標準付属しているが、設定がわかりにくいのが難点(図3)。市販のウイルス対策ソフトに付属するファイアウオール機能を利用するとよい。

また、メールソフトもセキュリティー機能を備えている(図4)。使い方に応じた設定をしておこう。次のページから、それぞれの使い方を詳しく解説する。

●ウィンドウズアップデートを実行

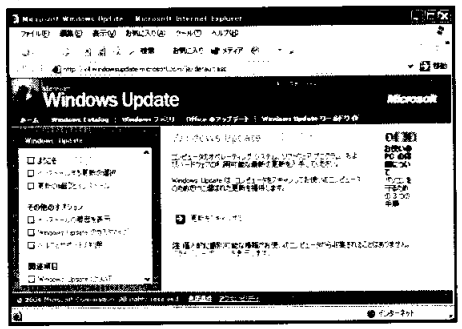


図1　ウィンドウズのセキュリティー上の不具合は日々報告されている。これを埋めるためにウィンドウズアップデートは不可欠

●ウイルス対策ソフトを導入

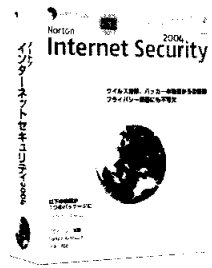


図2　ウイルスを検知・駆除するには市販のウイルス対策ソフトの導入が必要。新種のウイルスに対応するため、ウイルス対策ソフト自身のアップデートも不可欠だ

●ファイアウオールを設定

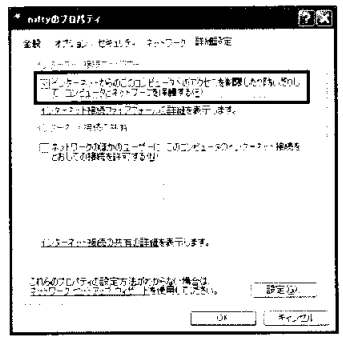


図3　XPにもファイアウオール機能があるが対策ソフト導入がお薦めだ

●メールソフトも設定

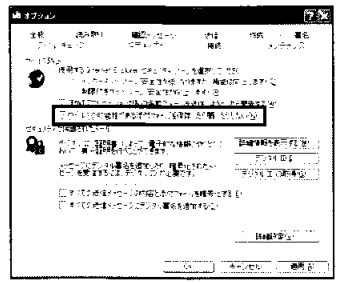
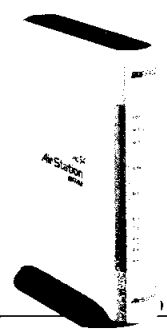


図4　アウトルック・エクスプレスでは、危険な添付ファイルは開かないといった設定が行える

ルーターでも、ネットワーク型ウイルスを防げる

複数台のパソコンからインターネットに接続するために、ルーターを使用している家庭も多いだろう。実は、ルーターの導入でセキュリティーも強化される。ルーターは出入りするデータを監視する機能を持っているので、それ自身がファイアウオールの役割を果たしてくれるのだ。



複数台のパソコンからインターネット接続するために必要なルーターだが、セキュリティーも強化できる。パソコン一台でも利用可能。価格は一万円前後から。写真はバッファローの無線LANルーター

インターネットに接続する際にはパソコンごとに個別のアドレスが設定されるが、このアドレスをターゲットに攻撃や侵入を受けることがある。ところが、ルーターがあると、内部のパソコンに設定されるアドレスと外部に公開されるアドレスが自動的に切り替えられるため、外部からの侵入を困難にするのだ。

守りを固める…… 予防法

ウィンドウズアップデートを実行する

随時、実行するクセをつけよう

ウィンドウズアップデートはセキュリティー対策の第一歩

定期アップデートが基本。しばらく怠ってしまったら、自分で実行するべし

パソコンを買った状態のままで使い続けるのは、実は危険なこと。ウィンドウズには、「セキュリティーホール」といわれるセキュリティー上の不具合が存在し、このセキュリティーホールを攻撃するウイルスが増えているからだ。ウィンドウズを購入したままの状態で使い続けているのは、いわば家中の窓やドアのカギをかけていないのと同じ。危険に身をさらしている状態だ。

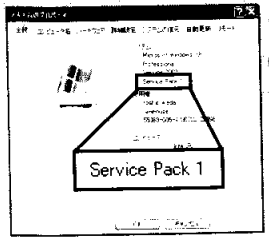
マイクロソフトはセキュリティーホールが発見されると、これをふさぐ修正プログラムを開発し、配布している。ウィンドウズアップデート機能を使えば、インターネットを介して、いま使っているパソコンを自動検索し、足りない修正プログラムを表示してくれる。ユーザーはメニューから導入したい修正プログラムを選ぶだけで、ダウンロードからインストールまで自動実行できる仕組みだ。

ウィンドウズアップデートは定期的に実行しておくのが基本。p.22～23では定期的に自動実行する手順を解説している。けれども「重要な更新」がある場合や、しばらく使用していなかったパソコンを使い始める場合には、自分でアップデートを行うことが必要だ。

手順は右の通り(図1～図6)。修正プログラムが複数表示されることもあるが、大事なのは「重要な更新」。「重要な更新」はすべて、必ず実行しよう[注1]。

SP1が導入されてないパソコンは危険!

ウィンドウズの修正プログラムをまとめたのが「サービスパック」だ。2002年秋に登場したウィンドウズXPのSP1(サービスパック1)には、それまでに報告されているセキュリティーホールの修正プログラムが含まれている。「スタート」→「コントロールパネル」→「パフォーマンスとメンテナンス」→「システム」と開き、今一度自分のウィンドウズを確認してみよう。もし未導入の場合はウィンドウズアップデートで導入しよう[注2]。



「システム」の「全般」タブで「システム」の項目に「Service Pack 1」の表示を確認

[注1]インターネットの接続回線によってはアップデートにかなりの時間がかかる場合もある
[注2]サービスパックのCD-ROMは下記で入手できる
https://s.microsoft.com/japan/products/shop/

●アップデートの手順

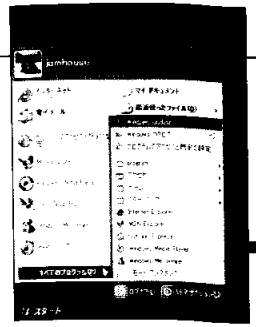


図1 「スタート」ボタンをクリックし、「すべてのプログラム」→「Windows Update」を選択

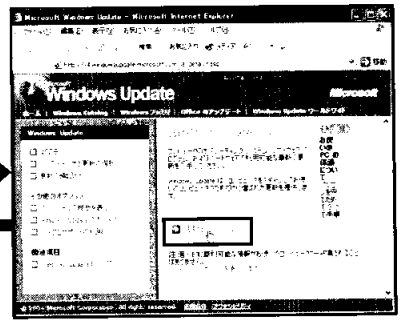


図2 更新プログラムがあるかどうか確認するため「更新をスキャンする」をクリック

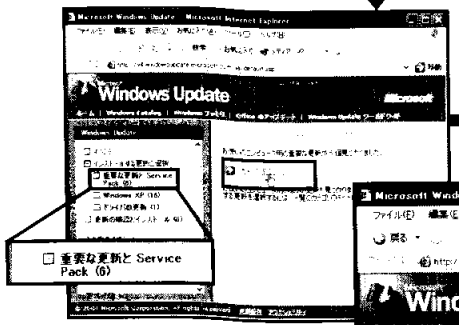


図3 画面左側の「重要な更新とServicePack」のカッコ内数字が(0)以外なら「更新の確認とインストール」をクリック

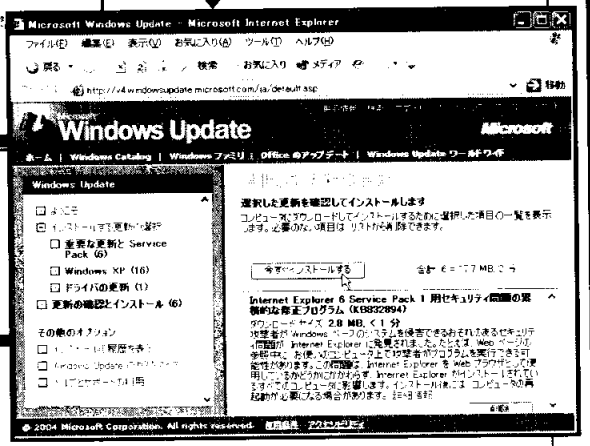


図4 更新すべきプログラムの内容を確認。「今すぐインストールする」をクリックする

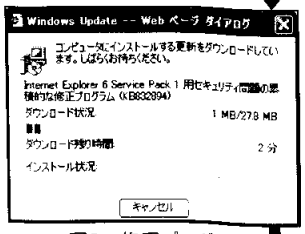


図5 修正プログラムのダウンロードがスタート。しばらく更新を行っていないと、数時間かかることもある

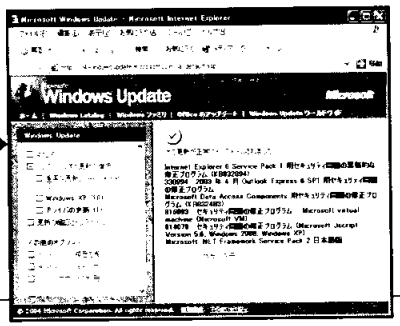


図6 図3で表示された6つの「重要な更新」のアップデートが完了。修正プログラムの内容によっては、このあと再起動が必要になる

ウィンドウズアップデートを自動更新

自動更新の設定を確認しよう

ウィンドウズアップデートを自動更新させる設定で常に最新の状態に保つ

パソコンの使い方に応じて更新方法を設定する

前ページでも解説したように、ウィンドウズアップデートはウイルス対策の第一歩。自分でアップデートする必要が生じることもあるが、ウィンドウズには、更新情報が追加されたときに、更新を通知して(図1)、自動でアップデートを行う設定が用意されている。

パソコンの設定を確認しよう

まず、自分のパソコンで、ウィンドウズアップデートの自動更新設定を確認しよう。「スタート」メニューから「コントロールパネル」を開き、「パフォーマンスとメンテナンス」をクリック。「コンピュータの基本的な情報を表示する」を選び、「システムのプロパティ」画面で「自動更新」タブを開く(図2～図5)。

初期設定では「コンピュータを常に最新の状態に保つ」にチェックが入っており、「更新をダウンロードする前に通知して、コンピュータにインストールする前に再度通知する」設定になっている。ウィンドウズを起動したときに、図1のような更新を知らせるメッセージが表示されるのがそれだ。更新を知らせるメッセージが表示されたら、これをクリックして更新作業を行おう。どのような更新が行われるのか確認しながら更新したい人は、この設定のままにしておけばよい。

すべて自動で、実行したいという場合は「更新を自動的にダウンロードして、指定したスケジュールでインストールする」設定を選ぶ[注]。その都度メッセージを確認する手間が不要で、ダウンロードは自動実行され、インストールも設定したスケジュールで自動実行される。ただし、設定した時間にパソコンの電源が入っていないとインストールは行われないので注意しよう。

電源を入れている時間が限られている人は「更新を自動的にダウンロードして、インストールの準備ができたら通知する」設定にしておくとよい。ダウンロードまでは自動で行われ、通知領域に表示されたアイコンをクリックするとインストールできる。いずれもダウンロードやインストールはバックグラウンドで行われるため、作業が中断されることはない。

●更新を知らせるメッセージ

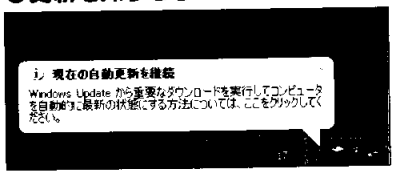


図1 ウィンドウズアップデートの更新を知らせるメッセージが表示されたらクリックする。あとは指示に従って更新手順を実行する

[注]更新の完全自動化は20ページ下の囲み記事で解説したSP1(サービスパック1)導入後のウィンドウズで可能

●自動アップデートを設定する手順

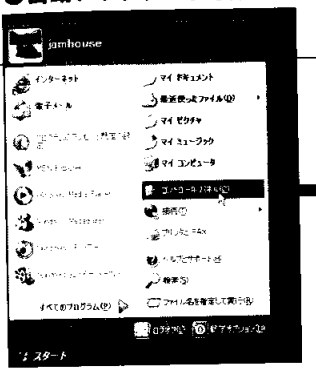


図2 「スタート」メニュー→「コントロールパネル」を選択

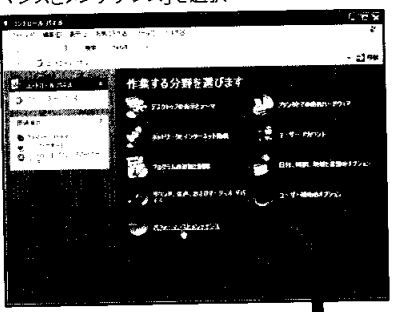


図3 コントロールパネルが起動したら、「パフォーマンスとメンテナンス」を選択

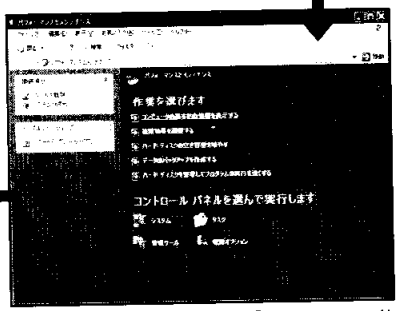


図4 メニューが表示されたら、「コンピュータの基本的な情報を表示する」をクリックする

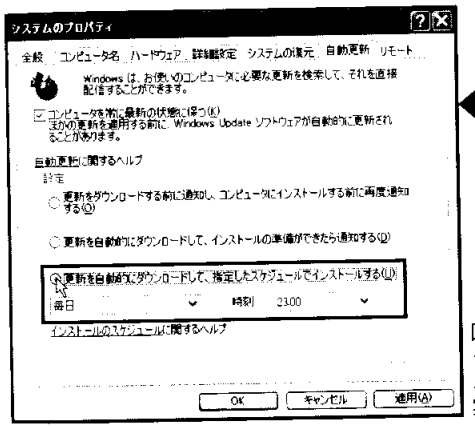


図5 「システムのプロパティ」が開いたら、「自動更新」タブを選択する。常に自動的にダウンロードしてインストールしたいなら、左のように設定。インストールを実行する時刻も設定しよう

登場間近のサービスパック2では

ウィンドウズXPのアップデートプログラムがまとめて提供される「サービスパック」の第2弾として、2004年の夏頃までにはSP2が登場予定だ。3月時点はベータ版が提供されている。

SP2で強化されるのは「ファイアウォール機能」「インターネット・エクスプローラ、アウトルック・エクスプレスのセキュリティー機能」など。セキュリティー面での重要な更新が含まれている。ウィンドウズを安全に使い続けたいなら、もちろんSP2の導入も必須だ。提供が始まったら、必ず入手して利用しよう。

ウイルス対策ソフトは必須!

感染する前に必ず導入しよう

ウイルス対策ソフトの導入はもはや「常識」と考えよう

これから導入するならファイアウオール機能付きのソフトを購入するとよい

利用には期間制限がある。更新料を支払って継続して使おう

最新のウイルスデータを元にパソコンにウイルスが侵入していないかチェックし、検出して駆除するのがウイルス対策ソフトだ。メールやインターネットを使うなら、ウイルス対策ソフトの利用はもはや常識。自分のパソコンを守るだけでなく、感染メールを送信して加害者にならないためにも、必ず購入しよう。最近のパソコンはウイルス対策ソフトがプリインストールされているものも多い。きちんと動作を確認しておこう。

ここでは主なウイルス対策ソフトを紹介する(図1～図3)。いずれも「常にウイルスの怪しい動きを監視する」「送受信中のメールの添付ファイルをチェックする」「定期的にパソコン内の全ファイルをチェックする」といった基本的な機能を備えたものだ。

また、最近はインターネットに接続するだけで感染するタイプのウイルスが増えているため、メールだけでなく通信の出入りを監視するファイアウオール機能は欠かせない。これから購入するなら、必ずファイアウオール機能付きのウイルス対策ソフトを選ぼう。

そして忘れてはいけないのが利用期限の更新とソフトのバージョンアップだ。ウイルス対策ソフトには購入時から1年間の利用期限が設けられている。更新料を支払って継続して利用すること。さらに、ソフトはバージョンアップによって最新のウイルス検出に対応する機能を追加しているので、バージョンアップは欠かせない。次のページからはソフトの使い方を解説する。

ウイルスバスター2004

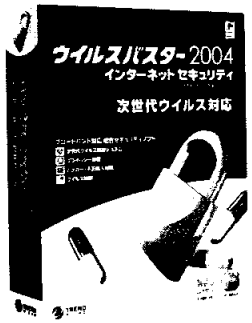


図1 「ウイルスバスター2004インターネットセキュリティ」(トレンドマイクロ)、実売価格:五五〇〇円前後、利用期限は一年間。更新料は三〇〇〇円

ウイルス検索、ファイアウオール機能などの基本機能に加え、駆除ツールを自動的にダウンロードする自動修復機能を備える。基本的な設定は3クリック以内ででき、設定が簡単なので初心者向き。2003年版を利用中でも購入後1年以内なら無料で2004年版にアップグレード可能。●http://www.trendmicro.com/jp/

ノートンインターネットセキュリティ

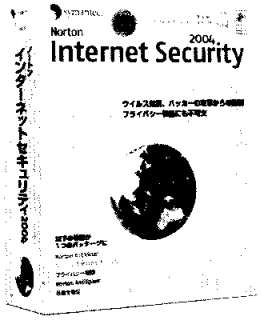


図2 「ノートンインターネットセキュリティ2004」(シマンテック)、実売価格:七八〇〇円前後、利用期限一年間。更新料四〇〇〇円

ウイルス対策ソフト「ノートンアンチウイルス」と、ファイアウオールソフトなどがセットになっている。基本機能に加え、子供が見られるサイトを限定できる保護者機能を備えるほか、ユーザーごとの利用設定も行える。アップグレード版は4000円でインターネットでも購入できる。●http://www.symantec.co.jp/

マカフィー・インターネットセキュリティ

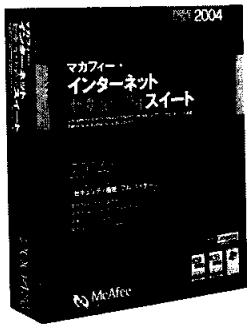


図3 「マカフィー・インターネットセキュリティスイート6.0」(日本ネットワークアソシエイツ)、実売価格:四四〇〇円前後、利用期限は一年間。更新料は要問い合わせ

ウイルス対策、ファイアウオールなどの機能が統合されたソフト。ファイアウオールでは攻撃元を追跡できる機能を備えるほか、安全度を数値で表すスコア表示が採用されるなどユニークな特徴を備えている。個人情報保護やスパム対策機能も用意されている。●http://www.nai.com/japan/

プロバイダーのセキュリティーサービスを活用

大手プロバイダーの多くは、送受信メールをウイルスチェックするサービスを月額数百円で提供している。ウイルスメールを自分が送受信する前にプロバイダーがブロックしてくれる。例えば、@niftyでは月額200円で送受信メールの添付ファイルをチェック。メールで届くウイルスばかりではないので対策ソフトと併用するとよい。

●主な大手プロバイダーのメール・ウイルスチェックサービス

@nifty	月額200円
ビッグローブ	月額300円[注1]
OCN	月額200円
DION	月額409円
ASAHIネット	月額200円
Yahoo! BB	月額490円[注2]

[注1]ホームページのセキュリティー管理を含む
[注2]メール以外のハードディスクなどのウイルスチェックを含む

ウイルス対策ソフトの使い方❶ 定義ファイルを更新して常に最新に保つ

●定義ファイルの更新とは

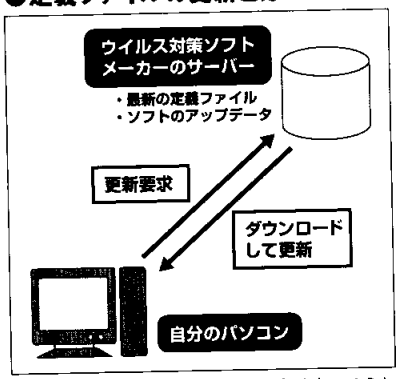


図1　定義ファイルはウイルスの手配書のようなもの。インターネットを通じて更新する

ウイルス対策ソフトは、初期設定で使っていれば大きな問題がないように、あらかじめ設定されている。だが、その仕組みや使い方を知らずにいては、急場のときの対応に困る。ここからはウイルス対策ソフトの使い方を解説していく。

まずは一番肝心な「ウイルス定義ファイルの更新」だ。ウイルス定義ファイルは、日々発生している新種のウイルスを検出するための"ウイルスの手配書"のようなもの。対策ソフトのメーカーは、新しいウイルスが報告されるとすぐに新しい定義ファイルを作成して、インターネットを通じてユーザーに提供する(図1)。対策ソフトはこの定義ファイルに基づいて、新種のウイルスを検出・駆除する。だから、定義ファイルは常に最新に更新しておく必要がある。

定義ファイルを更新するには、定期的なアップデートが必要だ。また、しばらく更新を怠ったあとや、緊急時には手動でアップデートしたほうがよい。

アップデートで更新されるのは、ウイルスの定義ファイル、ファイアウオールの設定ファイル、ソフトウェアそのもののアップデートデータなどさまざま。ウイルスバスター2004(図2～図4)、ノートンインターネットセキュリティ2004(図5～図8)はともに初期設定で自動アップデートが有効になっているが、念のため設定を確認しておこう。

正しく使わなければ感染する

- **新種ウイルスを発見するには最新の定義ファイルが必要**
- **定義ファイル更新に定期的なアップデートは欠かせない**

ウイルスバスター2004

●アップデートの設定を開始

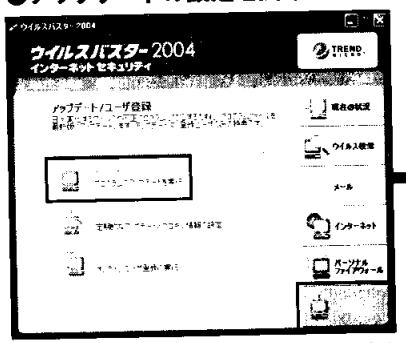


図2　「アップデート/ユーザ登録」をクリックすると、「最新版にアップデート」「アップデート設定」のメニューが表示される

●手動で「最新版にアップデート」

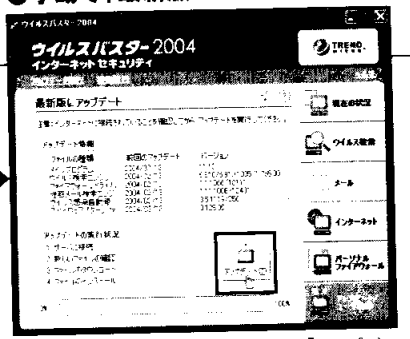


図3　図2で「最新版に～」を選んだら「アップデート」ボタンをクリックするだけで、アップデートがスタートする。前回のアップデート日などを確認できる

●自動の「アップデート設定」

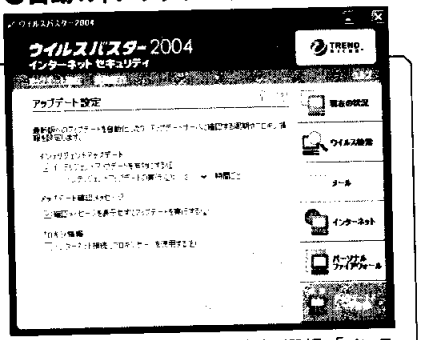
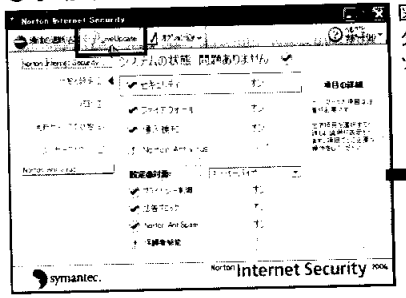


図4　図2で「アップデート設定」を選択。「インテリジェントアップデート」は定期的な自動更新の設定だ。必ず有効にしておこう

ノートンインターネットセキュリティ2004

●手動で最新版にアップデート



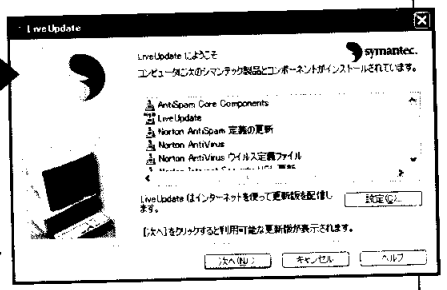


図5　トップメニューで「LiveUpdate」ボタンをクリック。ウイルス定義ファイルほかソフト自体のアップデートもできる

図6　LiveUpdateがスタートしたら、ウィザードに従って「次へ」ボタンをクリックしながら、手順を進めていく

●自動アップデートの設定

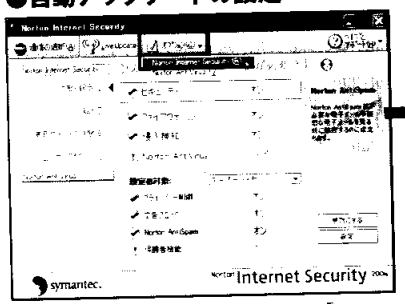


図7　「オプション」ボタンをクリックして「Norton Internet Security」を選択する

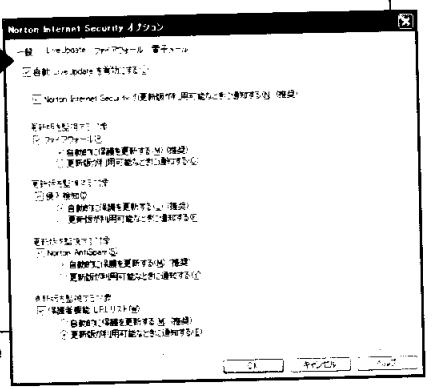


図8　「LiveUpdate」タブを選択し、「自動LiveUpdateを有効にする」のチェックを確認

ウイルス対策ソフトの使い方❷
常時監視機能でウイルスをチェック

常に起動してチェック

- ファイルを開く、コピーする／移動するなどさまざまなポイントでウイルスチェック
- 常時監視する機能は常に有効にしておく
- 発見後の駆除方法は、初期設定のままでOK

●常駐監視の仕組み

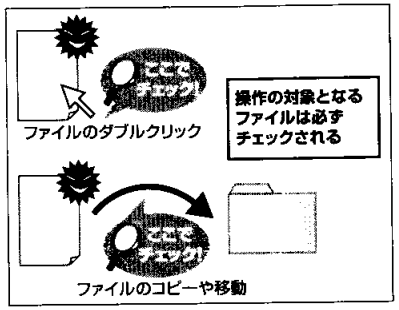


図1　ウイルスの常駐監視中、ファイル操作を行うと同時にチェックが実行される

ウイルス対策ソフトは、前のページで解説した最新のウイルス定義ファイルという「手配書」を元にウイルスを検出する。その検出のために用意されているのが「常時監視」機能と「送受信メールのチェック」機能だ。そしてファイルを個別にチェックする方法もある。ここでは「常時監視」機能について説明する。

ウイルスにはさまざまなタイプがあり、活動方法もそれぞれに違う。パソコンのメモリーに常駐して起動するたびに繰り返し活動するもの、あとから個人情報を持ち出すための仕掛けを作るもの、エクセルやワードのファイルに潜んでファイルを開いた時点で感染させるものなど、潜伏場所、活動の方法、タイミングもさまざまだ。

そこで、ウイルス対策ソフトはあらゆるウイルスをチェックするため、パソコンの電源を入れた時点から常に起動して、プログラムの動作や、ファイルのダブルクリック、コピー、移動などの操作のタイミング、フロッピーなどのメディアを挿入した時点など、さまざまなポイントでウイルスをチェックし、ウイルスによる怪しい動きがないかを見張っている。これが対策ソフトの「常時監視」機能だ(図1)。

ウイルスバスター2004では「リアルタイム検索」機能として(図2、図3)、ノートンインターネットセキュリティ2004では「Auto-Protect(オートプロテクト)」機能(図4～図6)という名前で搭載されている。初期設定ではこの常駐機能が有効になっているので、パソコンの起動時から監視を開始してくれる。パソコンを安全に使い続けるため、この機能をオフにしてはならない。

また、ウイルス発見時の駆除方法も設定できるが、これは初期設定のままで問題ない。基本的にはユーザーが特別な操作を行わなくても、自動的に駆除や修復が実行されるようになっている(検出時の対応はp.46参照)。

ウイルスバスター2004

●リアルタイム検索の設定を確認

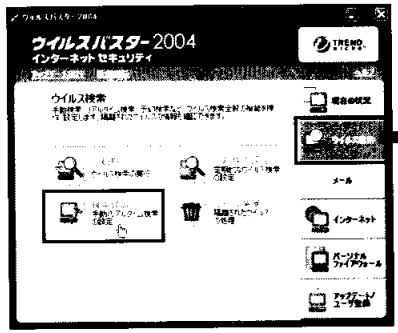


図2　「ウイルス検索」ボタンをクリックし、メニューから「検索設定」をクリックする

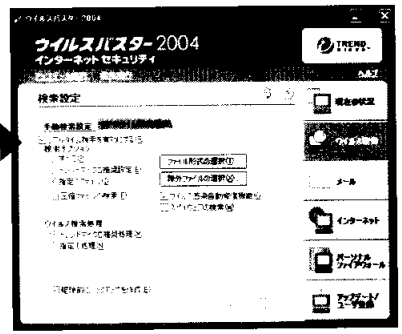


図3　「リアルタイム検索」の有効を確認。処理方法は「トレンドマイクロ推奨処理」

ノートンインターネットセキュリティ2004

●Auto-Protectの設定を確認

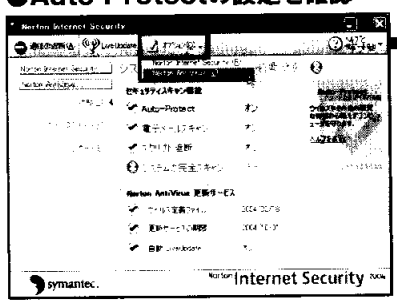


図4　トップページから「オプション」→「Norton AntiVirus」を選択する

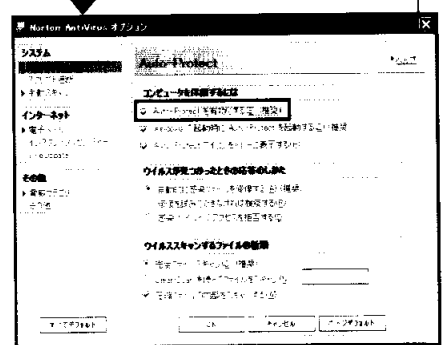


図5　「Auto-Protectを有効にする」にチェックがあることを確認。他も初期設定のままでよい

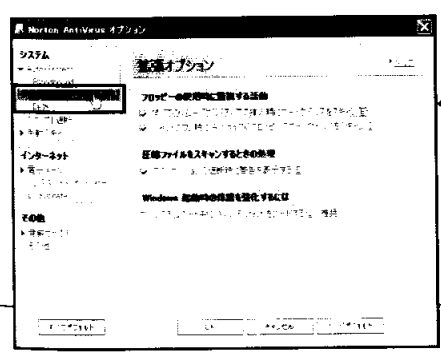


図6　「拡張」をクリックすると、フロッピードライブのチェック方法なども詳細に設定できる

ウイルス対策ソフトの使い方③ 送受信メールのウイルスをチェック

受信メールの添付ファイルを格納前にチェックする

これからは送信メールのウイルスチェックも重要

ほとんどのウイルスはメールでやってくる。添付ファイルとして届くものと、メール本文を表示させただけで感染するものもある。身に覚えのない英文メールなどは決して開かないこと。送信者が知人であっても信用はできないので注意しよう(p.14参照)。

ウイルス対策ソフトは、受信メールの添付ファイルをウイルスチェックする機能を備えている。メールの受信時に添付ファイルをチェックし、ウイルスだと判断したら、駆除した状態でメールソフトに格納する(図1)。送信時のチェックも可能だ。自分のパソコンが感染している場合に、取引先などにウイルスメールを送らないように、右の手順(図2～図3、図5～図6)で確認し、設定がオフになっていたら、有効にしておこう。

また、ウイルスバスター2004、ノートンインターネットセキュリティ2004は、煩わしいスパムメール(迷惑メール)をチェックし、件名に表示する機能も備えている(図4、図7)。

●受信メールのウイルスをチェック

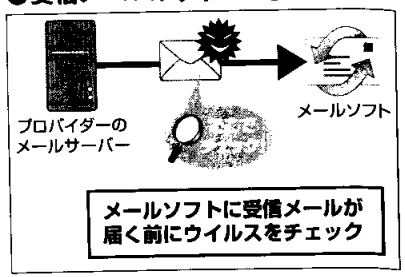


図1　受信したメールがメールソフトに格納される前に添付ファイルをチェックする

ウイルスバスター2004

●送受信メールのチェック

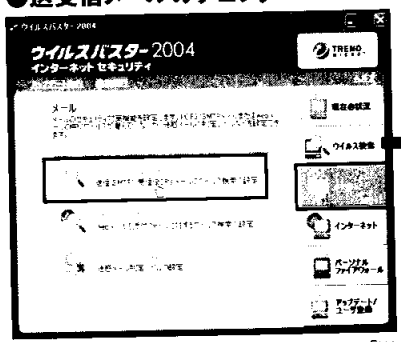


図2　「メール」ボタンをクリックし、メニューから「送受信メール検索設定」を選択する

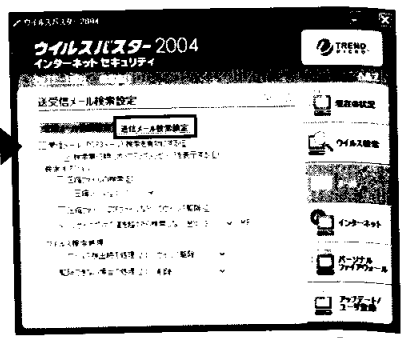


図3　受信メール検索設定を確認したら、「送信メール検索設定」をクリックして確認しよう

●迷惑メールの監視

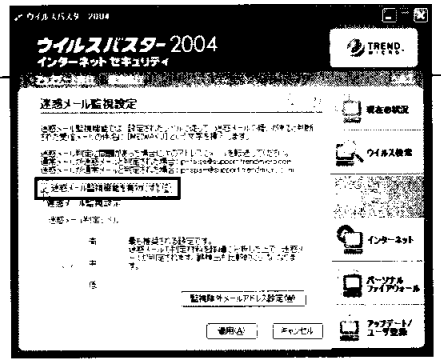


図4　図2のメニューから「迷惑メール監視設定」を選択し、「迷惑メール監視機能を有効にする」をチェック。受信メールが迷惑メールと判断されたら、メールの件名に「MEIWAKU」と表示される

ノートンインターネットセキュリティ2004

●送受信メールのチェック

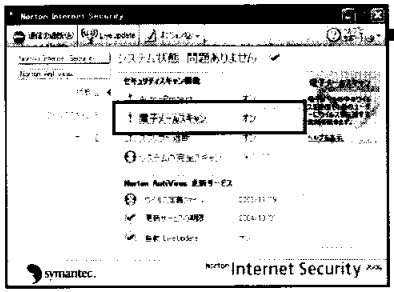


図5　「オプション」→「Norton AntiVirus」を選択し、「電子メールスキャン」が「オン」になっていることを確認

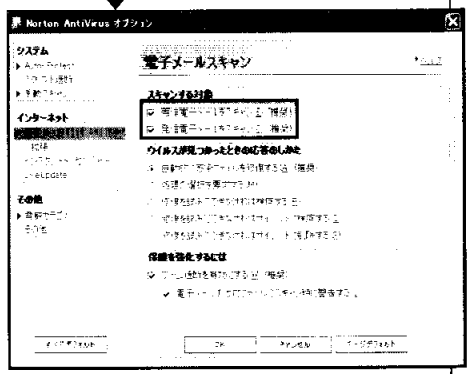


図6　「電子メール」の「着信電子メール」(受信)、「発信電子メール」(送信)、いずれのチェックもオンであることを確認する

●スパムメールの監視

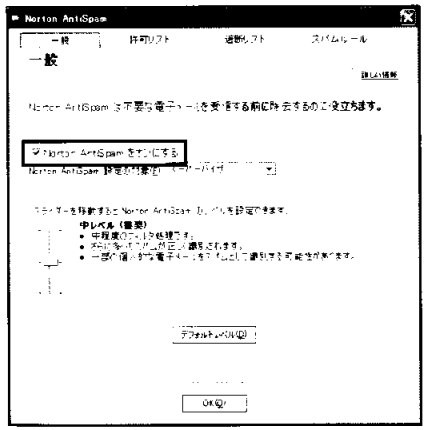


図7　トップページから、「NortonAntiSpam」の設定画面を開き、「NortonAntiSpamをオンにする」にチェックを入れる。スパムと判断されたメールの件名には「NortonAntiSpam」と表示される

ウイルス対策ソフトの使い方④
怪しいファイル／全システムをチェック

チェック方法を覚えておこう

- 怪しいと思ったファイルは必ずチェックする
- 定期的に全システムをスキャンしよう

p.26～27のウイルス定義ファイルの更新設定によって定義ファイルを常に最新に保ち、p.28～31で紹介したウイルス対策ソフトの「常時監視機能」と「送受信メールのウイルスチェック機能」が正しく動作していれば、ほとんどのウイルスはチェックできる。

だが、定義ファイルの更新のタイミングによっては、更新が間に合わずに感染してしまうこともある。おかしいと思ったら（p.48～49参照）、すぐにウイルス対策ソフトでチェックすること。特定のファイルについてウイルスチェックを行う方法と、パソコンの全システムをチェックする方法を覚えておこう。

まず、チェックを行う前にウイルス定義ファイルを更新して必ず最新のものにする。CD-ROMやフロッピーディスクなどからコピーしたファイルなど、個別のファイルをチェックする場合は、右クリックメニューから行う（図1、図5）。

ドライブごと、あるいはシステム全体のチェックも一気にできる（図2～図4、図6～図8）が、ハードディスクの容量が大きい場合、全システムのチェックには数時間かかることもある。

チェックの実行中は他の作業もできるが、動作速度が遅くなるので、余裕があるときに実行するか、パソコンを使わない時間に自動実行されるように定期チェックのスケジュールを設定しておくとよい［注］。その際、設定した時刻にパソコンの電源が入っていないと動作しないので注意する。また、チェックの途中に一時停止することも可能。その場合には続きから再開できる。

ウイルスバスター2004

●ファイルごとのウイルスチェック

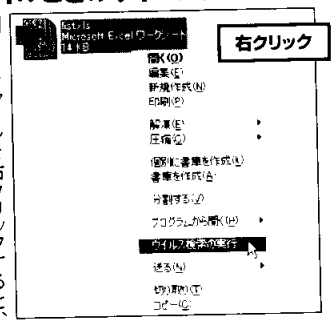


図1　ファイルを右クリックすると、「ウイルス検索の実行」というメニューが表示されるので、選択して実行する

●全システムのウイルスチェック

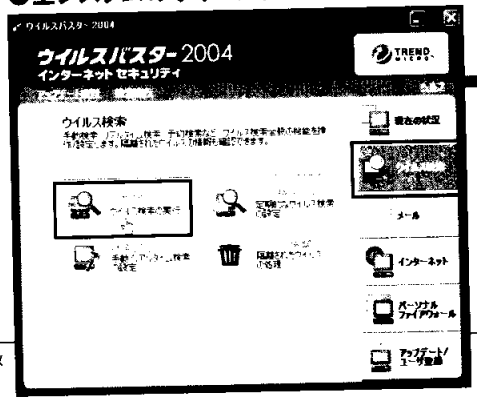


図2　「ウイルス検索」ボタンをクリックし、メニューから「手動検索」を選択する

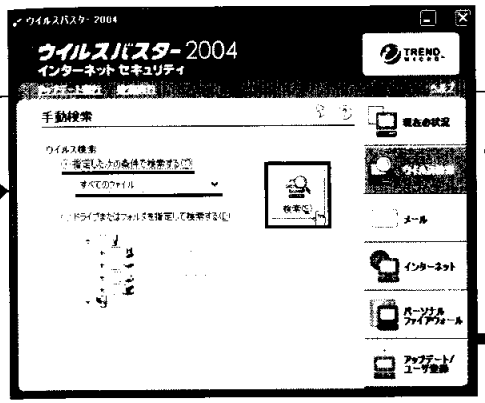


図3　「すべてのファイル」を条件に設定し、「検索」ボタンをクリックする

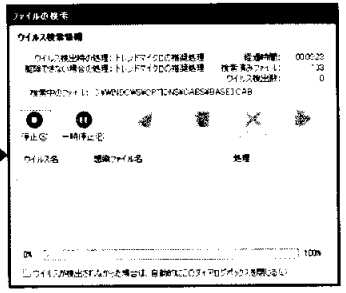


図4　検索がスタート。万が一発見された場合には、ウイルス名とそれに対する処理が表示される

ノートンインターネットセキュリティ2004

●ファイルごとのウイルスチェック

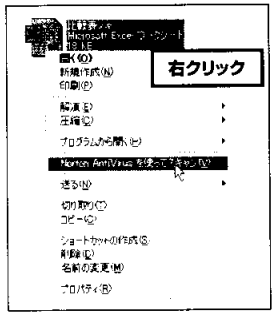


図5　ファイルを右クリックすると、「NortonAntiVirusを使ってスキャン」というメニューが表示されるので、選択して実行する

●全システムのウイルスチェック

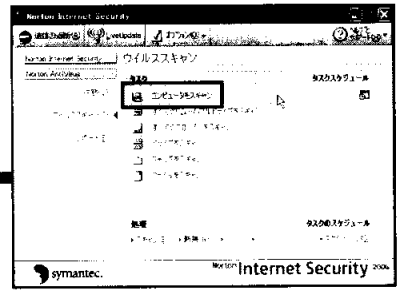


図6　メニューから「ウイルススキャン」を選択し、「コンピュータをスキャン」のアイコンをクリックする

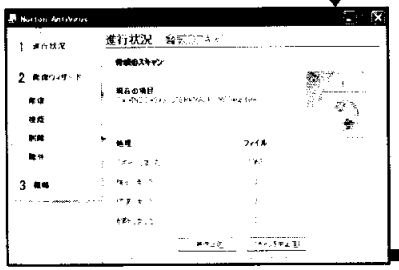


図7　「進行状況」として、スキャン結果が表示される。「一時停止」をクリックすれば、後でスキャンを再開できる

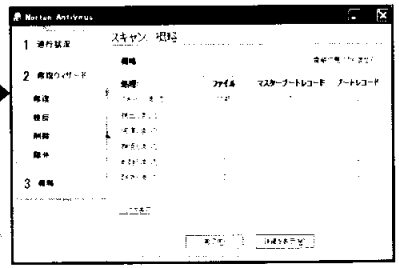


図8　スキャンが完了すると、結果が表示される。検出された場合、処理方法も確認できる

［注］定期的なスキャンの設定はウイルスバスター2004なら図2のメニューから「予約検索設定」を選んで設定する。ノートンインターネットセキュリティ2004では図6で「タスクスケジュール」を選択して設定する

ファイアウオール機能も必ず導入

ネットワーク型ウイルス対策に必須

- **ネットワーク型ウイルスはファイアウオールがないと防げない**
- **ウィンドウズXP付属のファイアウオール機能はわかりづらい**
- **市販ソフトなら接続場所ごとの設定を選ぶだけと簡単**

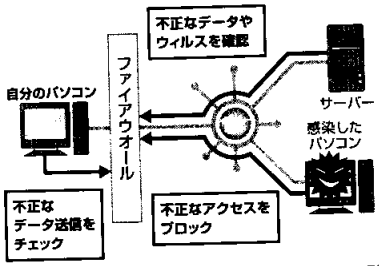


図1　ファイアウオールは通信の見張り番だ。監視して不正な通信をブロックする

ウイルス対策ソフトでは防ぐことができないのが、最近急増中のネットワークに接続しただけで感染するウイルスだ(p.10参照)。これを防ぐには「ファイアウオール」か「ルーター」が必要だ。

ファイアウオールとは、パソコンに出入りする通信データをチェックし、許可したデータのみを通過させ、それ以外のデータを遮断する機能のことだ(図1)。「防火壁」という意味の通り、不正なアクセスをブロックする。

複数のパソコンをインターネット接続するためにルーターをすでに使っている場合は、基本的にはファイアウオールは必要ない(p.19参照)[注1]。ルーターを使っていない場合は必ず導入しよう。

ウィンドウズXPは、標準でファイアウオールの機能を備えているが、使い方に応じて詳細な設定をしようとすると、設定が難しい(図2、図3)。ウイルス対策ソフトのファイアウオール機能を利用するのがお薦めだ。ウイルスバスター2004(図4、図5)、ノートンインターネットセキュリティ2004(図6、図7)では、自宅、会社など、接続する場所ごとの設定があらかじめ用意されている。これを選択するだけで最適な設定で利用できる。

なお、複数のファイアウオール機能が同時に起動していると、不具合が起こる可能性がある。ウイルス対策ソフトのファイアウオール機能を使うなら、ウィンドウズXPのファイアウオール機能を使う必要はない[注2]。

●ウィンドウズXPのファイアウオール

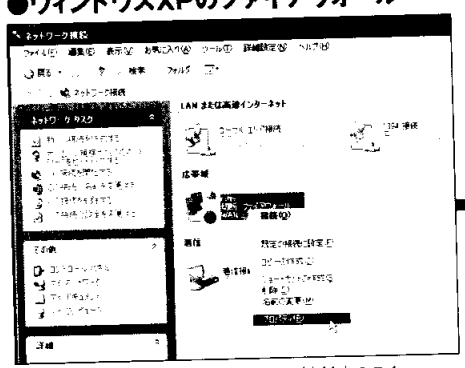


図2　ウィンドウズXPの「ネットワーク接続」でアイコンを右クリックして、「プロパティ」を選択

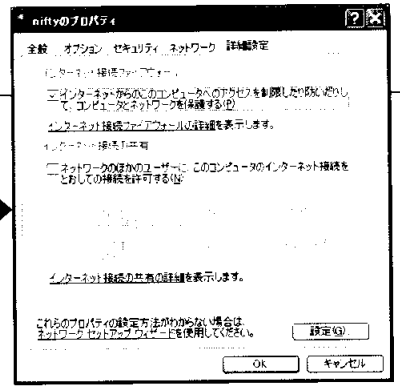


図3　プロパティが開いたら、「詳細設定」タブを選択し、「インターネットからのこのコンピュータへのアクセスを制限～」にチェックを入れる。「設定」ボタンをクリックすれば、詳細設定が行えるが、一般ユーザーに設定は難しい

ウイルスバスター2004

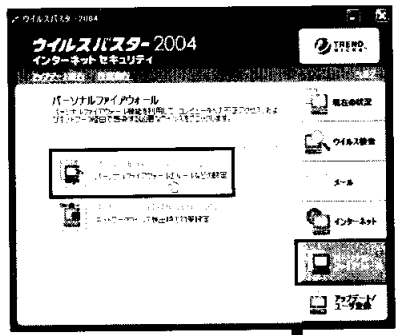


図4　「パーソナルファイアウオール」ボタンをクリックし、メニューから「パーソナルファイアウオール設定」を選択

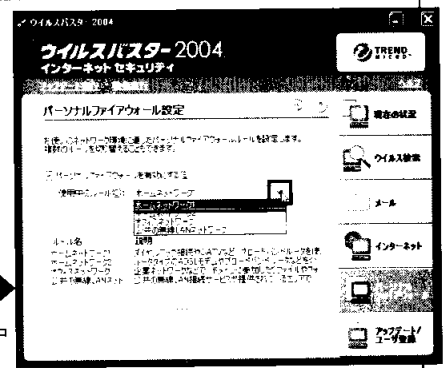


図5　「有効にする」のチェックを確認したら、「使用中のルール」を接続場所に応じて選択する

ノートンインターネットセキュリティ2004

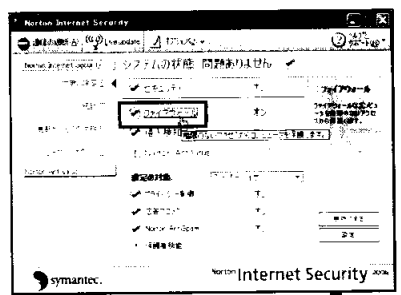


図6　トップページで「ファイアウオール」を選択し、「設定」をクリックする

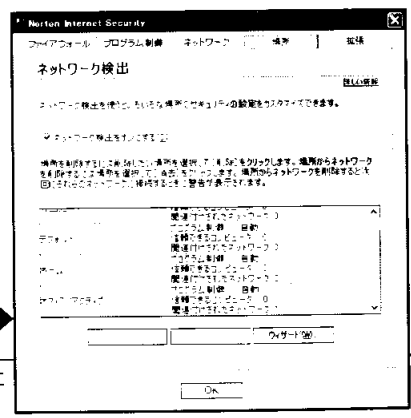


図7　「場所」タブを選択し、一覧から接続場所に応じた設定を選択する

[注1]ルーターからノートパソコンを外して外に持ち出して使う場合などはファイアウオールがないと危険
[注2]ウィンドウズXPのファイアウオール機能は初期設定ではオフになっている。ウイルスによってはウイルス対策ソフトを無効化するものもある。その場合はXPのファイアウオール機能を使おう

メールソフトの設定❶ アウトルック・エクスプレスの添付ファイル

メールの添付ファイルに注意

あらかじめ、怪しい添付ファイルは開かない設定にしておく

エクセルやワードなど特定の拡張子を指定して開けるように設定

メールの添付ファイルとして届くウイルスは多く、「怪しい添付ファイルは開かない」のが原則だ。

アウトルック・エクスプレスには、メールの添付ファイルで届くウイルスに対抗する機能がある。「exe」「com」などウイルスによく使われる拡張子のファイルを開かない設定だ。メールが届いて添付ファイルを開こうとしても、メニューから開くことも保存することもできない(図1)。もしも、このような設定になっていない場合には、安全のため「添付ファイルを保存したり開いたりしない」設定にしておこう(図2、図3)。

パソコンによってはエクセルやワードなどのファイルも開けない設定になっている。「マクロウイルス」が含まれている可能性があるためだ。しかし、ビジネスで使用するファイルまで開けないのは困りものだ。エクセルやワードなど特定の拡張子のファイルを開けるように設定を変更しておこう(図4、図5)。

ただし、取引のある相手からのメールがウイルスに感染していることもあり得る。いきなり開かずに、いったん保存してウイルスチェックしてから開く方法がお勧めだ(図6、図7)。また、自分が添付ファイルを送るときは、受け取る側が余計な心配をしなくて済むように、件名や本文に何のファイルを添付しているか明記するとよい。

●添付ファイルを開かない

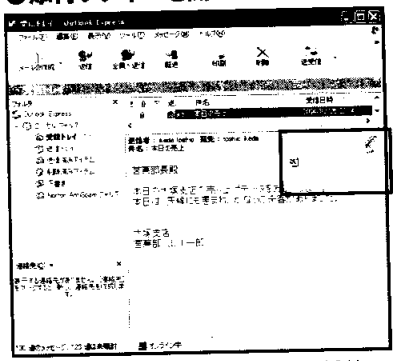


図1 ウイルスによく使われる拡張子の添付ファイルは開けないようになっている

●設定を確認しよう

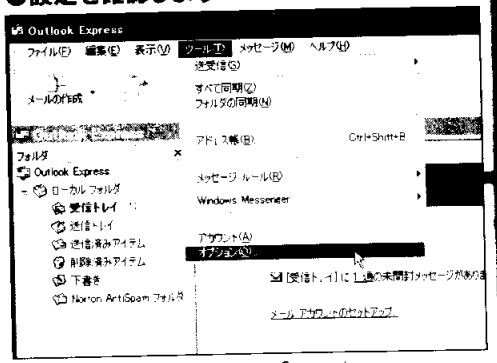


図2 アウトルック・エクスプレスの「ツール」メニューから「オプション」を選択して「オプション」ダイアログを開く

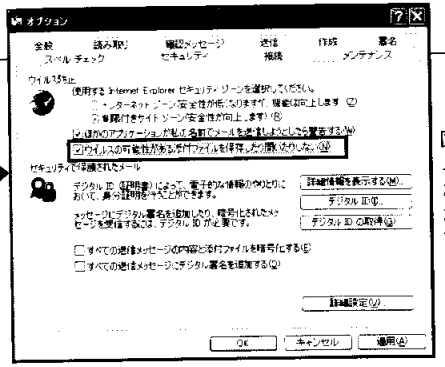


図3 「セキュリティ」タブを開き、「ウイルスの可能性がある添付ファイルを保存したり開いたりしない」をオンにする。いったんアウトルック・エクスプレスを終了して、再起動しよう

●特定の拡張子を変更する

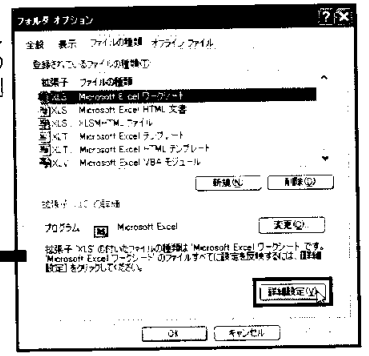


図4 フォルダを開いた画面で、「ツール」メニューの「フォルダオプション」を開き、「ファイルの種類」タブで「Microsoft Excelワークシート」を選択し「詳細設定」ボタンをクリック

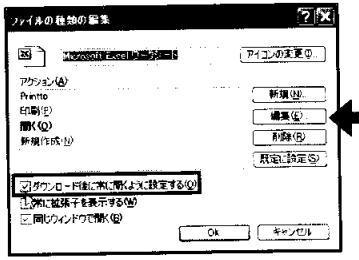


図5 「ダウンロード後に常に開くように設定する」をオンにする

●添付ファイルを保存してウイルスチェック

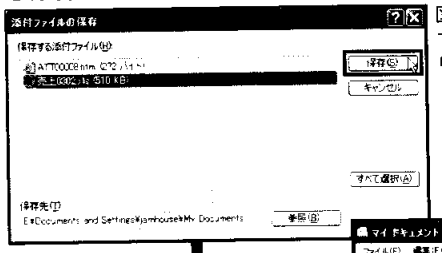


図6 「添付ファイルの保存」ダイアログでファイルを選択したら「保存」ボタンをクリック

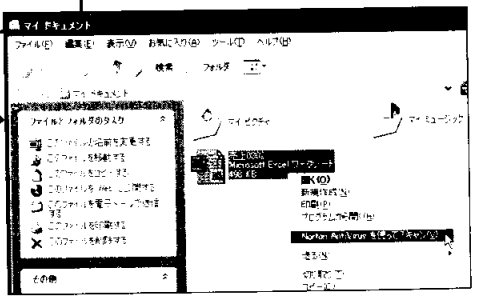


図7 保存したファイルのアイコンを右クリックして「Norton AntiVirus を使ったスキャン」を選択。ウイルスチェックを行う。問題がなければファイルを開く

メールソフトの設定②
アウトルック・エクスプレスの表示形式

「表示しただけで感染」を防ぐ

メールは常にテキスト形式で受信する

送信メールもテキスト形式にする

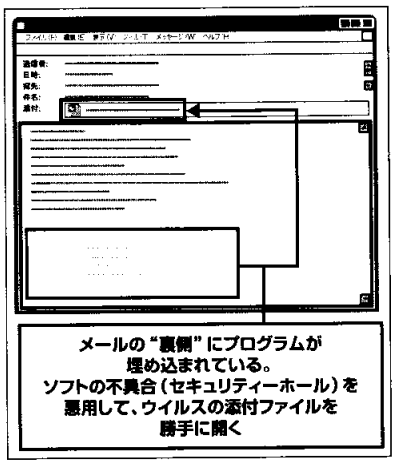
メールには、テキスト形式とHTML(エイチ・ティー・エム・エル)形式の2種類がある。テキスト形式は、テキストデータ、つまり文字だけで作成されたメールだ。もう1つのHTML形式は図1のように、ウェブページと同様に、文字に色やサイズを設定でき、画像や音声をメール中に埋め込むこともできる形式だ。

表現力という点では、HTMLメールのほうが勝る。例えば、打ち合わせの場所を記した地図をメール中に埋め込めば、文字だけの説明よりずっとわかりやすい。しかし、セキュリティーの点ではHTMLメールは使わないほうがよい。

なぜなら、アウトルック・エクスプレス(以下OE)がHTMLメールを表示するときは、インターネット・エクスプローラ(以下IE)のプログラムを使うからだ。つまり、もしもIEのセキュリティーホールを悪用するプログラムがHTMLメールに含まれていたら、表示しただけでウイルスに感染する危険がある。HTMLメールにはウイルスが潜んでいる可能性があるということだ。

OEでは、常にテキスト形式でメールを表示して、HTMLメールをプレビューウィンドウに表示しないように設定を変更しておこう(図2～図5)。メールを送信するときもHTML形式ではなく、テキスト形式で送るように設定しよう(図6)。

●メール本文にウイルスが埋め込まれている



ブラウザーのセキュリティーホールを悪用したプログラムが埋め込まれることがある

●HTMLメールは危ない

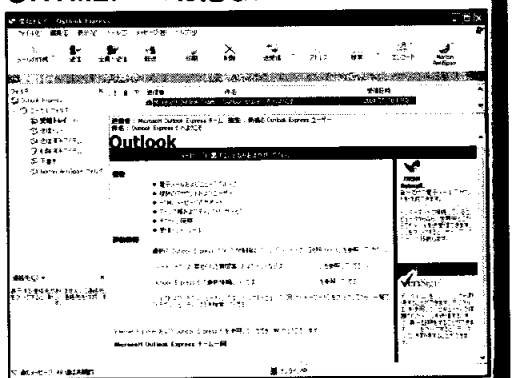


図1　HTMLメールはウェブページと同じ。見た目は華やかだが、ウイルスが潜む危険がある

●テキスト形式で表示するように設定変更する

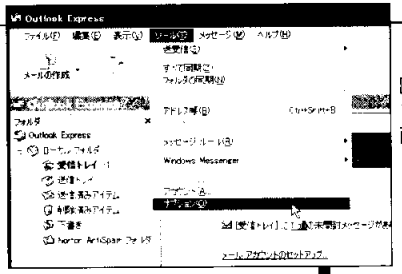


図2　OEのメニューから「ツール」→「オプション」を選択して「オプション」設定画面を開く

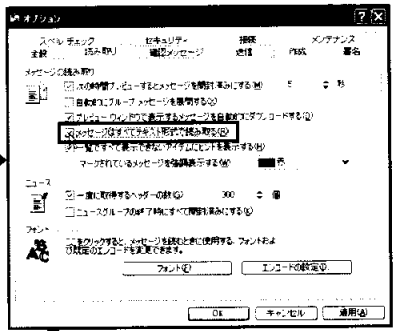


図3　「読み取り」タブで「メッセージはすべてテキスト形式で読み取る」にチェックを入れて「OK」を押す

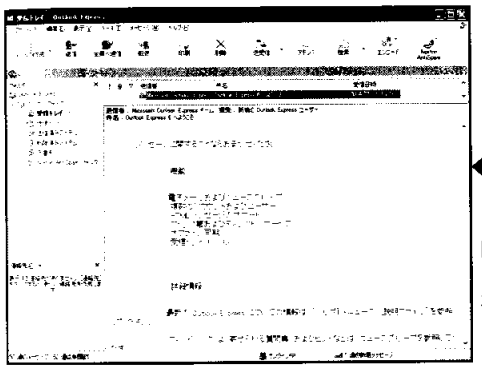
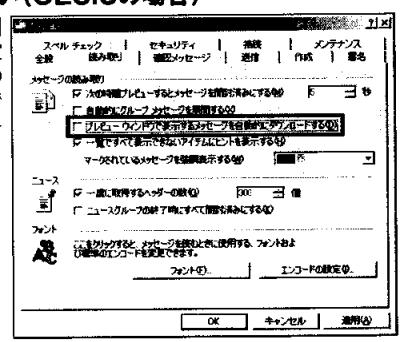


図4　図1のHTMLメールも文字情報だけが表示されるようになり、画像などは表示されない。これなら埋め込まれたプログラムは起動しない

●メッセージをすぐに表示しない(OE5.5の場合)

図5　OEの「ヘルプ」→「バージョン情報」でバージョンが5.5の場合は、図3の設定ができないので「オプション」ダイアログの「読み取り」タブで「プレビューウィンドウで表示するメッセージを自動的にダウンロードする」のチェックを外し「OK」をクリック



●常にテキスト形式で送信する

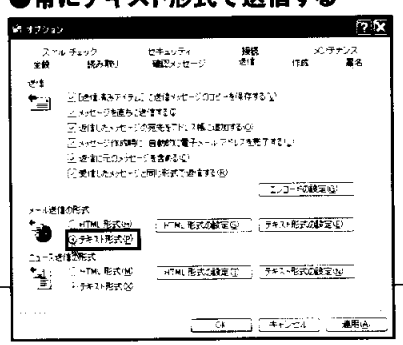


図6　OEの「ツール」→「オプション」で開く画面の「送信」タブで「メール送信の形式」で「テキスト形式」を指定。「OK」をクリック

守りを固める…… 予防法

久しぶりに電源を入れるときは危険!

いきなりつないではダメ

接続していきなり感染するのを防ぐためファイアウオールを確認

ウィンドウズのアップデートをまずは実行

ウイルス対策ソフトのアップデートを続いて実行

日々報告されるセキュリティーホールや、新種のウイルスに対応するため、「ウィンドウズアップデート」と「ウイルス対策ソフトの定義ファイルの更新」はパソコンを使い続ける限り欠かせないものと肝に銘じておこう。

そして、注意しなければならないのは、長期の旅行や出張などで、久しぶりにパソコンの電源を入れるときだ。留守中、パソコンの電源が入っていない間はアップデートはされていない。その間に新しいセキュリティーホールを悪用するような、現在の定義ファイルでは発見できない新種のウイルスが流行している可能性もある。留守中のメールを早くチェックしたいところだが、電源を入れたら右ページの手順で作業しよう。

まず、常時接続の場合、パソコンを起動してインターネットに接続した途端にネットワーク型のウイルスに感染する可能性がある。パソコンを起動する前に、いったん通信ケーブルは外しておく。そして、電源を入れたらウイルス対策ソフトの動作を確認して、ファイアウオール機能がオンになっていることを確認。それからケーブルを接続する。

続いて、手動でウィンドウズのアップデートを実行する(p.20参照)。自動アップデートを待つ間に感染する可能性があるためだ。そしてウイルス対策ソフトのアップデートも手動で実行する。自動アップデートには実は数分から10分のタイムラグがあるので、即座に手動で行っておこう(p.23参照)。

ウィンドウズも対策ソフトも最新の状態にしてから、いよいよメールソフトを起動する。もちろん、p.36で解説したように添付ファイルやHTMLメールはすぐに開かないようにしておくこと。かなり手間がかかるが、安全のためにはこれらの手順が必要だ。

ウィンドウズセキュリティーアップデートCDを使う手も

マイクロソフトは2004年2月、「ウィンドウズセキュリティアップデートCD」の無償配布を開始した。このCDには2003年10月までのXP/Me/2000/98/98SEの修正プログラムが入っている。これ以前からアップデートされていないパソコンがあるなら下記サイトからCDを入手しよう。

http://www.microsoft.com/japan/security/protect/order/

●いきなりメール受信はもっとも危険

1 いったんケーブルを外す

常時接続環境の場合、パソコンの電源を入れると同時にインターネットに接続される。以前使用したときにファイアウオール設定を変更している可能性があるなら、まずはいったんケーブルを外した状態で電源を入れよう

2 ファイアウオールの動作を確認

パソコンが起動したら、ファイアウオールが有効になっているかどうか、確認しよう(p.34参照)。市販ソフトを使用する場合には、「場所」の設定も現在の環境に合っているかどうか、確認しておくことが必要だ

3 ケーブルをつなぐ

ファイアウオールが問題なく動作していることを確認したら、ケーブルを接続。常時接続環境なら、すぐに接続が開始されるが、されない場合には接続の修復を実行するか、ウィンドウズを再起動しよう

4 ウィンドウズアップデートを実行

まずは、セキュリティーホールなど、ウィンドウズの問題点を解決するために、ウィンドウズアップデートを実行する。自動アップデートを待たずに、すぐに手動で実行すること(p.20参照)

5 ウイルス対策ソフトのアップデートを実行

ウィンドウズアップデートに引き続き、ウイルス対策ソフトのアップデートを実行(p.23参照)。こちらも、自動アップデートまでタイムラグがあるので、手動で実行しておくこと

6 メール受信などアプリケーションを起動

メールソフトを起動し、添付ファイルやHTMLメールがすぐ開かないようになっているか、まずは確認する。問題なければ、いよいよたまっていたメールをダウンロードして読もう

感染が疑わしいときは —— 対処法

パソコンの調子が何だかおかしい。ひょっとしたらウイルスに感染したかも？ そんなときの確認方法、対処法を知っておこう。

こんなときは感染を疑おう

普段からパソコンの調子を観察

- **怪しいファイルをうっかり開いたときは危ない**
- **パソコンの動きが異様に遅くなったら、要注意**
- **「感染しているのでは」と忠告されたら、念のためチェック**

●怪しいファイルをうっかり開いた

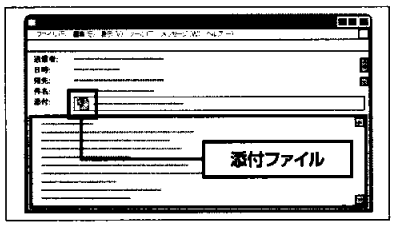


図1　メールで届いた怪しい添付ファイルをうっかり開いてしまうのは危険

●パソコンの動作が遅い

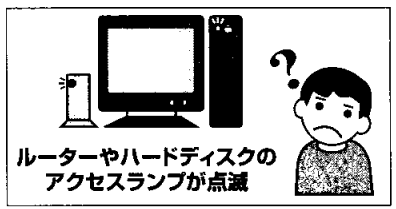


図2　何もしていないのに、ランプが点滅したらウイルスがパソコンを働かせている可能性あり

●外部からの忠告

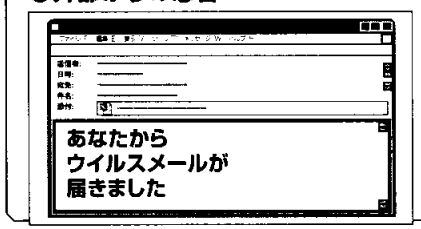


図3　ウイルスが、あなたの名前で勝手に友達にメールを送ったかもしれない

たとえウイルス対策ソフトをインストールしていても、ウイルス感染を完全に防げるとは限らない。定義ファイルの更新が間に合わなかったり、うっかりウイルス検索機能をオフにしたまま使っているかもしれないからだ。また、最近のウイルスは感染しても、画面に何か特別な表示を出すこともなく、大きな変化を起こさないものが多い。ユーザーに感染を気付かせず、パソコンからメールアドレスを盗んで感染メールを大量に送信し、感染を広げることが目的だからだ。

予防に気を配ると同時に、自分のパソコンがウイルスに感染していないか、普段から注意を払っておこう。

「うっかり」「遅い」「忠告」に注意

まず、メールで届いた怪しい添付ファイルを自分でうっかり開いてしまったときには、ひとまずウイルス感染を疑おう(図1)。ファイルを開いたのに何も表示されなかったり、送信者に問い合わせて「何も送っていない」と言われたら、かなり危ない。すぐにウイルス対策ソフトで全システムチェックを行おう。

パソコンの動作がどうも遅い、重いというときも、気をつけよう(図2)。何もしていないのにハードディスクやルーターのアクセスランプが頻繁に点滅しているのも危険な兆候だ。裏でウイルスがせっせと感染メールを大量に発信しているからかもしれない。アクセスランプの点滅だけで感染していると判断はできないが、注意するに越したことはない。

また、ウイルス対策ソフトを実行中のはずが、いつの間にかタスクトレイからソフトのアイコンが消えていた、というときは感染の可能性が非常に高い。感染すると、ウイルス対策ソフトの機能を停止させるウイルスが多数存在するからだ。ウイルス対策ソフトが正常に動かなくなったら、すぐに感染を疑おう。

送った覚えがないのに、「あなたからおかしなメールが届いた」と忠告を受けた場合も要注意だ(図3)。あなたのパソコンに感染したウイルスが、その人に勝手にメールを送ったためかもしれない。ただし、別のだれかのパソコンが感染して、あなたのメールアドレスを詐称した可能性もある(図4)。その場合は、忠告してくれた人と共通の知人が感染している可能性が高い。念のためウイルスチェックを行って、仲間にもウイルスチェックを勧めるとよいだろう。

なお、メールでウイルスが届いても、ウイルス対策ソフトが発見して処理していれば、問題はない。むやみにおびえるのではなく、ウイルスについての基礎知識や感染情報を把握して、パソコンをよく観察することが大切だ。

感染しているのは、だれ？

最近、送信者の名前やアドレスを詐称するウイルスが増えている。感染すると、パソコンのアドレス帳などからアドレスを拾い出し、適当な宛先に、適当な送信者名でメールを送る。そのため、ウイルスメールが届いても、送信者欄にあるメールアドレスの持ち主が感染しているとは限らない。

あなたの名前でウイルスメールをもらった知らない相手から「あなた、だれ？」と返信メールが届くこともある。ウイルスの仕業と知っておこう。

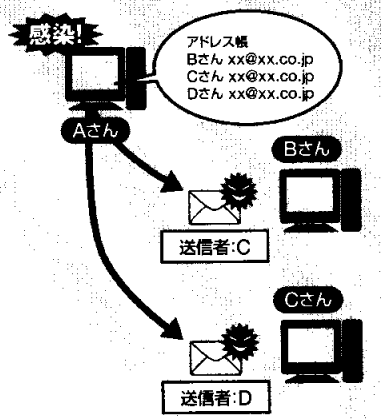


図4　Aさんのパソコンに感染したウイルスがCさんやDさんの名前でメールを送る

感染が疑わしいときは…… 対処法

感染したかもしれないときの手順

●感染したかも!? と思ったら、この手順で確認しよう

怪しいなと思ったら…

「ひょっとして感染？」と思ったら、慌てずに手順を追って確認しよう。まず、本当に感染しているのか、何というウイルスに感染したのか、ウイルスの名前を確認。感染している場合には、ネット接続を切って駆除を実行しよう。

① 全システムチェック

ウイルス対策ソフトの定義ファイルを最新に更新し、全システムをチェック。ソフトがないときは「オンライン検索」で。感染していたら、ウイルスの名前を確認(p.46〜49)。

非感染 → セーフ！ 作業完了

感染 → ウイルス発見

② ネット接続を切る

ウイルスに感染すると、インターネットを介して感染はどんどん広まっていく。感染を確認したら、自分が加害者にならないために、すぐにネット接続を切る(p.50〜51)。

③ ウイルスを駆除

ネット接続を切ったら、じっくりと慌てずに駆除に取りかかろう。まずウイルスを取り除き、パソコンの設定を元の状態に戻す必要がある。無料の駆除ツールを使うと簡単だ(p.52〜57)。

うまくいかない ← ③

④ 再セットアップ

パソコンが正常に起動しないなど、どうしてもうまく駆除できないときには、最終手段として再セットアップがある。面倒だが、確実にウイルスを駆除できる(p.58〜65)。

⑤ もう一度全システムチェック

駆除が済んだら、もう一度全システムチェックを行って、ウイルスに感染していないことを確認しよう。また、二度と感染しないために、防御策を徹底するべし。

駆除OK → ⑤

作業完了

「ひょっとして感染したかも？」と思っても、慌ててはいけない。まず、ウイルス対策ソフトの全システムチェックで、本当に感染しているかを確認しよう。感染している場合は、あとで駆除するために、何というウイルスに感染したのか知ることが重要だ(①)。

感染が確実とわかったら、すぐにネットとの接続を切ろう。そのまま接続していると、感染を拡大させてしまう(②)。

ネットとの接続を切ったら、じっくり駆除に取りかかろう。ウイルスはウィンドウズの設定を勝手に書き換えることがある。完全に駆除するためには、ウイルスファイルを削除するだけでなく、書き換えられた設定を元に戻す作業が必要だ。ウイルス対策ソフトメーカーが無料で配布している「駆除ツール」を使えば、両方を一度にやってくれる(③)。

それでもうまくいかないときの最終手段として、再セットアップがある。パソコンを工場出荷時の設定に戻せば、ウイルスは完全に駆除できる(④)。

無事に作業が終了したら、念のためにもう一度全システムチェックを実施しよう(⑤)。次のページから、これら一連の手順を詳しく解説する。

落ちついて手順を追って対処

- まず、何というウイルスに感染したかを確認すること
- 感染が確実なら、ネット接続を切る
- ウイルス退治には、無料の駆除ツールを使うと簡単

感染が疑わしいときは…… 対処法

❶全システムチェック<その1>
ウイルス対策ソフトでウイルスが検出されたら

処理の内容に注目

「検出」と「感染」は違う。メール受信時に発見されても、処理されれば問題ない

「駆除できません」でも、「削除しました」なら大丈夫。ウイルス対策ソフトの処理用語を知っておこう

怪しいと思ったら、まずウイルス対策ソフトの定義ファイルを最新の状態に更新して、全システムのチェックを実行しよう(p.32～33)。ウイルスが発見されると対策ソフトがメッセージを表示する。

ウイルス対策ソフトの処理報告では、図1のように用語が区別されている。ウイルスの種類によって処理方法は違い、処理報告の読み取り方は少しわかりにくい。例えばファイル全体がウイルスであれば、ファイルからウイルスを分離する「駆除」や「修復」という処理は、そもそも実行不可能。ウイルスバスターで「駆除できませんでした」と表示されても、「隔離しました」「削除しました」と表示されれば、問題ないのだ。同様に、ノートンインターネットセキュリティで「修復できませんでした」と表示されても、「検疫しました」「削除しました」と表示されれば、問題ない。

ただし、ウイルスによってはパソコンの設定を改変するものがある。最新のウイルスバスター2004には、こうした改変も元に戻す自動修復機能があるが、同じウイルスバスターでも古いバージョンの製品や、その他のウイルス対策ソフトにはウイルスが改変した設定を戻す機能を持っていない。対策ソフトの全システムチェックでウイルスを検出して、「駆除・修復しました」「隔離・検疫しました」「削除しました」と表示されても、念のため、ウイルス名を確認して「駆除ツール」をダウンロードして実行しておこう。

全システムチェック以外では

全システムチェック以外でウイルスが発見された場合には、実際には感染していないこともある。

例えば、ウイルスメールが届いた場合、メール検索にひっかかれば、感染前に処理されるが、ウイルスを発見したという報告は表示される(図2)。「ウイルスが見つかりました」という表示があっても、検索の種類が「受信メール(POP3)検索」になっていて、「隔離・検疫しました」「削除しました」などと表示されれば、未然に防御できて感染していないと考えてよい。ファイルをインターネットからダウンロードしたり、CD-ROMからコピーするといった外部とのやり取りで警告が出たときも、同様だ。

しかし、外部とのやり取りがないときに、常時監視機能でウイルスが発見された場合は注意が必要だ(図3)。ウイルス定義ファイルの更新が間に合わなかったなどの理由で入り込んだウイルスが、定義ファイルを更新したために発見された可能性がある。

いずれの場合でも、ウイルス検出後、感染しているのか、未然に防げたのか判別できないときは、念のため検出したウイルスの名前を確認して、そのウイルス用の駆除ツールを入手(p.52～53)、実行しておけば安心だ。

●ウイルス対策ソフトの「用語」の意味

ウイルスバスター	ノートンアンチウイルス	処理の内容
駆除	修復	ファイルからウイルスを除去し、クリーンな状態に戻す
隔離	検疫	ウイルスが感染したファイルを、安全な場所に移動し、再感染しないようにする
削除	削除	感染したファイルを削除する

図1　ソフトによって同じ処理でも用語が変わる。ウイルスの種類によって実行できる処理が異なるので、注意しよう

●ウイルス対策ソフトがウイルスを検出すると

ウイルスバスター2004

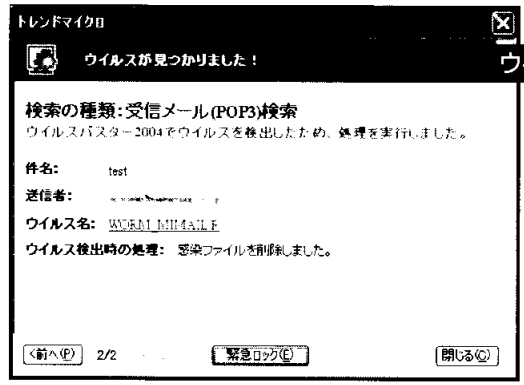


図2　「検索の種類」で、どんな状況でウイルスが発見されたかを確認。また、「ウイルス検出時の処理」が無事に終了したかもチェックしよう。この画面では受信メールからの発見なので問題はない。感染していると思われる場合は、「緊急ロック」でネット接続を切り(p.50)、ウイルス名を確認しよう

ノートンインターネットセキュリティ2004

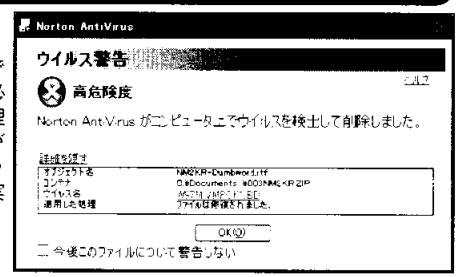


図3　常時監視機能(Auto-Protect)でウイルスが発見された場合は、注意が必要だ。定義ファイルの更新遅れなどの理由ですでに感染してしまっている可能性が高い。「削除しました」と表示されてもネット接続を切り、駆除ツールを入手して実行しよう

感染が疑わしいときは…… 対処法

❶全システムチェック<その2>
対策ソフトがない場合はオンライン検索を使う

オンライン検索の過信は禁物

- 対策ソフトがないとき、急場の確認には使える
- ウイルス対策ソフトの代わりにはならない
- 接続を続けると感染拡大の恐れあり

感染が怪しまれるが、ウイルス対策ソフトを持っていない。そんなときには、オンラインのウイルス検索サービスを利用しよう。対策ソフトメーカーのウェブサイトにアクセスして、ウイルス感染を確かめる方法だ。ただし、この方法では感染の有無やウイルス名を確認するだけで、駆除はできない。また、検索している間にも、ウイルス感染を広める可能性がある。感染が確実なら、インターネットの接続を切り(p.50)、ウイルス対策ソフトを買いに走ったほうがよい。

ここでは、「ウイルスバスターオンラインスキャン」と「シマンテックセキュリティチェック」を紹介しよう。

ウイルスバスターオンラインスキャンでは、該当ページを開いたら、説明をよく読んで、最下部の「検索画面を表示する」をクリック(図1)。すると、セキュリティー警告の画面が表示される。「Trend Micro, Inc.」をクリックして、電子証明書を表示し、会社名などを確認しよう。「はい」をクリックすると、ドライブの選択画面が表示される(図3)。「マイコンピュータ」をチェックして全ドライブを選択し、「検索」をクリックすると、検索が開始される。検索には数十分はかかるので、しばらく待とう。もしウイルスが発見されたら、ウイルス名を正確にメモしてから、通信を切断する。

シマンテックセキュリティチェックの場合は、チェックサイトへのリンクをクリックし(図5)、「ウイルス検出」の「開始」をクリックする。図2と同様の画面が表示されたら、今度は「Symantec Corporation」をクリックして電子証明書を確認しよう。セキュリティー警告は2回表示される。こちらはドライブの選択は行わないので、「はい」をクリックすると全ドライブについて検索が開始される。

●オンライン検索の手順

ウイルスバスターオンラインスキャン

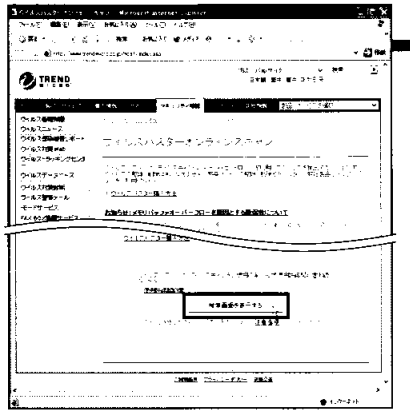


図1 ウイルスバスターオンラインスキャン(http://www.trendmicro.co.jp/hcall/index.asp)のページを開いて、最下部にある「検索画面を表示する」をクリックする

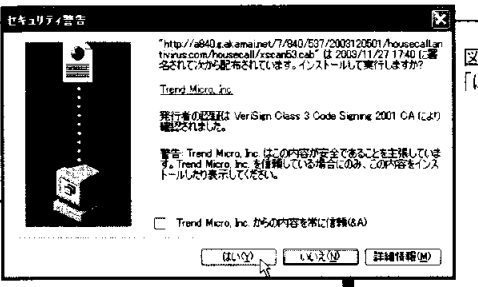


図2 「Trend Micro, Inc.」を確認して「はい」をクリック

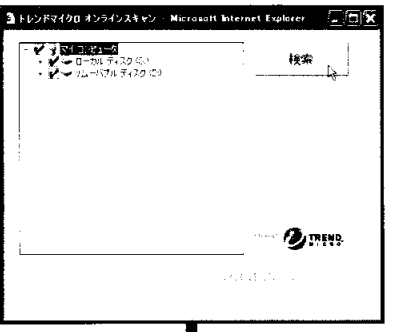


図3 検索するドライブを選択する画面。「マイコンピュータ」をクリックすると、全ドライブが指定されるので、その状態で「検索」をクリックする

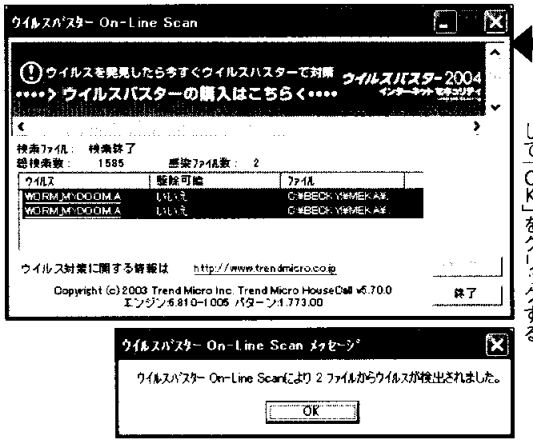


図4 検索が開始される。ドライブの容量などによって異なるが、数十分かかるので、そのまま待とう。ウイルスが発見されると左上画面のように表示されるので、ウイルス名を正確にメモしよう。検索終了後、左下のようなメッセージが表示されたら、内容を確認して「OK」をクリックする

シマンテック セキュリティチェック

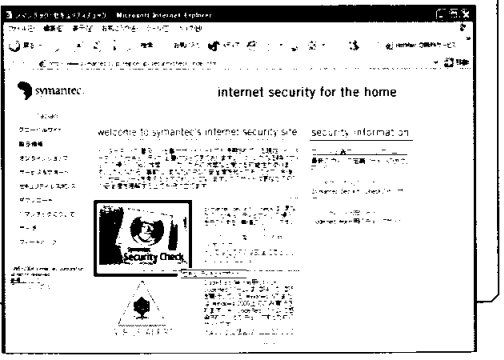


図5 シマンテックセキュリティチェック(http://www.symantec.co.jp/region/jp/securitycheck/)から、チェックサイトへのリンクをクリック。「ウイルス検出」の「開始」をクリックすると図2と同様の画面が2回表示されるので、「はい」をクリックすると検索が開始される

感染が疑わしいときは…… 対処法

❷ネット接続を切る
感染メール送信を防ぐため通信ケーブルを抜く

加害者にならないことが重要

ウイルス感染メールを知人に送信してしまったら自分が加害者になる

感染を確認したら、できるだけ早くインターネット接続を切る

ウイルスに感染すると、ウイルスはウイルスメールを勝手に大量送信して、感染を広げようとする。自分が感染したために、ウイルスメールをばらまいてしまったら大変だ。周囲の信用を失うばかりか、取引先などに送った場合は、賠償問題になることもある。万が一感染しても、感染を拡大させないことが大切だ。

そのためには、感染が確認されたら、直ちにインターネットとの接続を切ることが最優先。ウイルスの駆除方法は、そのあとでゆっくり考えればよい。

一番簡単なのは、通信ケーブルを抜いて、物理的に接続できないようにすること(図1)。無線LAN機能を内蔵するパソコンなどでケーブルがない場合は、無線LANの親機(アクセスポイントやルーターなど)の通信ケーブルを抜く。

ウィンドウズXPの操作でも通信の接続を無効にできる。コントロールパネルのネットワーク接続で、「有効」になっている接続アイコンを右クリックし、「無効にする」を選択する(図2)。

なお、ウィンドウズ98やMeには、簡単に接続をオン・オフする機能はない。また、ウィンドウズの操作は、場合によってはウイルスに乗っ取られる可能性がある。ADSLモデムの電源を切るなど、できるだけ物理的な切断を実行しよう。

ウイルスバスターやノートンインターネットセキュリティには、緊急時にインターネット接続を遮断する機能がある。ウイルスバスターでは、ウイルス発見時の画面に、直ちにすべてのインターネット接続が切断される「緊急ロック」ボタンが用意されている(図3)。タスクトレイのアイコンを右クリックして現れるメニューにも「緊急ロック」ボタンがある(図4、図5)。

ノートンインターネットセキュリティでは、タスクトレイのアイコンをダブルクリックして、メインメニューを表示し、「通信の遮断」をクリックすれば、接続を切断できる(図6)。また、タスクトレイのアイコンを右クリックして現れるメニューで「通信の遮断」を選択してもよい。

●ケーブルを抜いて接続を切る

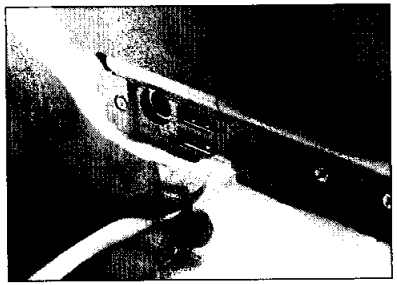


図1　インターネット接続を切るためには、LANケーブルを抜くなど、物理的に切断するのがいちばん確実で速い

●接続を無効にする

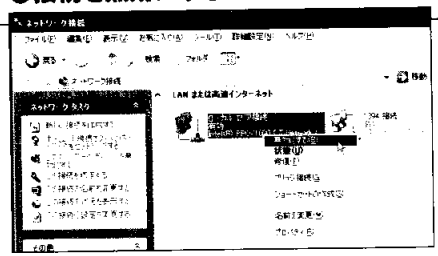


図2　「スタート」→「コントロールパネル」→「ネットワークとインターネット接続」→「ネットワーク接続」を選択。「有効」になっている接続アイコンを右クリックして「無効にする」を選択すると切断される

ウイルスバスター2004

●ウイルス発見時に通信を切断する設定

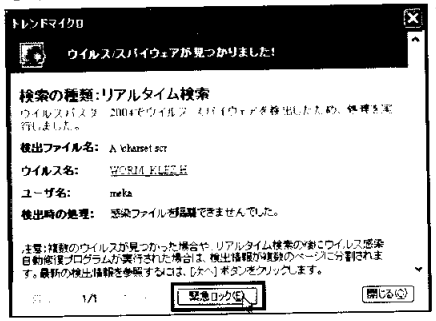


図3　ウイルス発見を知らせるウィンドウには「緊急ロック」ボタンがある。感染したとわかったら、ここをクリックすると、直ちにインターネット接続を切断できる

●タスクトレイのアイコンから切断

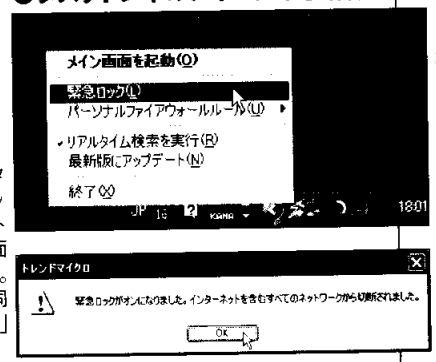


図4、図5　タスクトレイのウイルスバスターのアイコンを右クリックして、「緊急ロック」を選択すると、即座にインターネット接続が切断される(図4)。確認の画面が表示されるので「OK」をクリックしよう。接続を元に戻すには、ロックのときと同様、アイコンを右クリックして「緊急ロック」を選択する(図5)

ノートンインターネットセキュリティ2004

●ウイルス発見時に通信を切断する設定

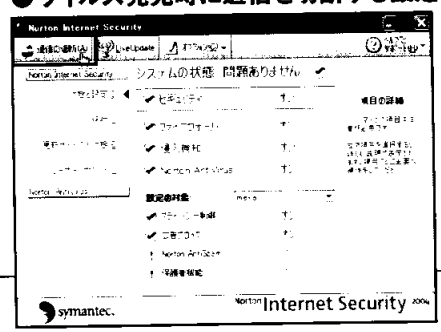


図6　ノートンインターネットセキュリティでは、タスクトレイのアイコンをダブルクリックしてメインメニューを表示。「通信の遮断」をクリックすると、切断できる

感染が疑わしいときは…… 対処法

③ウイルスを駆除する<その1>
感染したウイルス用の駆除ツールを入手する

他のパソコンから入手

駆除ツールは、ウイルス別に用意されている

感染していないパソコンからダウンロードする

ウイルスの中には、ウィンドウズの設定を勝手に書き換えるものがある。この場合、ウイルス対策ソフトだけではパソコンは元に戻らない。完全に駆除するには、そのウイルスに対応した「駆除ツール」が必要だ。主なウイルスの駆除ツールは、対策ソフトメーカーのウェブサイトで無料で配布されているので、ウイルスに感染したときは必ず対策ソフトメーカーのウェブサイトを確認して、駆除ツールをダウンロードして実行しよう。

ただし、感染したパソコンをインターネットに接続すると、ウイルスの感染を拡大させかねない(p.50)。知人や職場などの感染していないパソコンを使ってダウンロードするのがお勧めだ。インターネットカフェなどを利用してもよい。駆除ツールは小さなプログラムなので、フロッピーディスクやUSBメモリーなどで持ち運べる。

トレンドマイクロの「ウイルス駆除ツール」ページには、ウイルス名が並んでいるので、自分が感染したウイルス名をクリックする(図1)。ここには駆除ツールの使い方が詳しく書かれているので、よく読もう(図2)。できれば印刷して持ち帰るとよい。次にファイルのダウンロードの画面が現れるので、「保存」をクリック(図3)。「名前を付けて保存」ダイアログが表示されたら、保存場所を指定して「保存」をクリックすれば、ファイルがダウンロードされる。あとはフロッピーなどにコピーして、駆除ツールを感染したパソコンに移し、アイコンをダブルクリックして実行するだけだ。

シマンテックセキュリティ・レスポンスでも、操作はほぼ同じ(図4、図5)。なお、最新のウイルス以外なら、ウイルス対策ソフトのパッケージ製品に、それまでに発見された主なウイルスの駆除ツールを収録したCD-ROMが付属している場合があるので、これを利用する手もある。

●駆除ツールの入手方法

トレンドマイクロウイルス駆除ツール

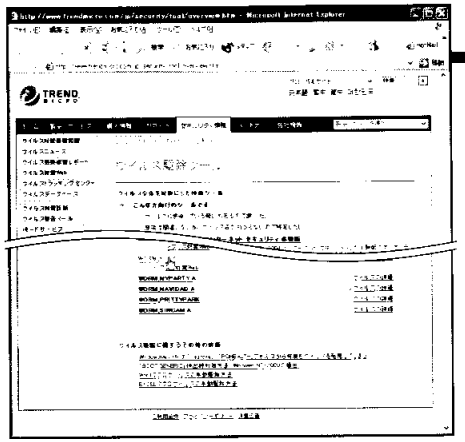


図1　ウイルス駆除ツールのページ(http://www.trendmicro.com/jp/security/tool/overview.htm)で、駆除したいウイルスの名前をクリック

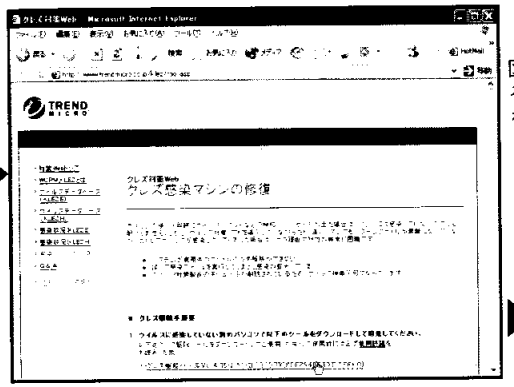


図2　使用方法や注意事項の説明が表示されるので、よく読んで、駆除ツールのダウンロード先をクリックする

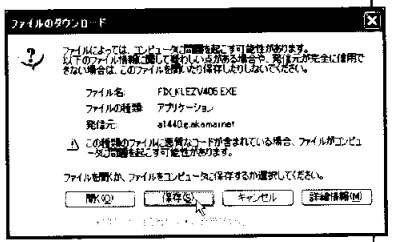


図3　「保存」をクリックすると、保存場所を指定する画面が表示される。わかりやすい場所を指定し、「保存」をクリック。アイコンをダブルクリックして実行しよう

シマンテック セキュリティ・レスポンス

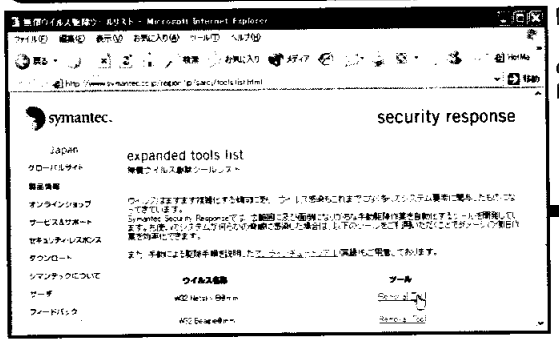


図4　「無償ウイルス駆除ツールリスト」(http://www.symantec.co.jp/region/jp/sarcj/tools.list.html)で、そのウイルスのツールをクリックする

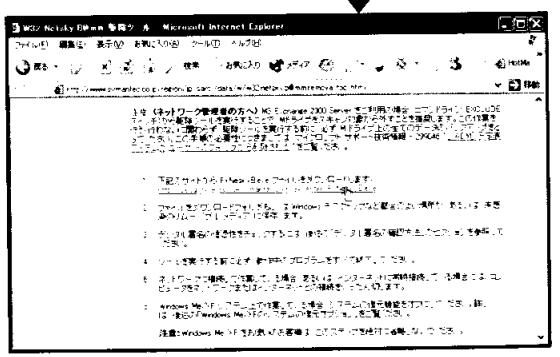


図5　説明ページが開くので、よく読み、駆除ツールのリンクをクリックする。あとは、図3と同様に保存。アイコンをダブルクリックして実行しよう

③ウイルスを駆除する<その2>「システムの復元」機能を使う

ウィンドウズの状態を戻す機能

- ウィンドウズをある時点での状態に戻す機能
- 感染した時期がはっきりしていないと使えない
- 復元ポイント以降に行った設定はすべて無効になる

「システムの復元」は、ウィンドウズの設定を定期的に保存しておき、万が一ウィンドウズの調子が悪くなったときに、以前の状態に戻せる機能だ(図1)。ウィンドウズMe/XPで利用できる。

ウイルスの駆除ツールが手に入らないときには、ウイルス対策ソフトでウイルスファイルを削除した後に、この機能を使ってウイルスが変更した設定を元に戻そう。ただし、ウイルスにいつ感染したかわからなければ、どの時点に戻すべきかわからない。また、戻した復元ポイント以降に行った設定はすべて無効になってしまう[注]ので、アプリケーションの再インストールなどが必要になることもある。感染の時期が最近で、いつ感染したかはっきりしている場合のみに利用しよう。

システムを復元するには、「スタート」メニューから、「すべてのプログラム」→「アクセサリ」→「システムツール」→「システムの復元」を選択すると「システムの復元」ウィザードが起動する。「コンピュータを以前の状態に復元する」が選択されていることを確認し、「次へ」をクリックしよう(図2)。ウィンドウズの設定を変更したときには、自動的に復元ポイントが作成されている。復元ポイントが存在する日付は太字で表示されるので、確実に感染前の日付をクリックして、右欄で復元ポイントを選択する(図3)。「次へ」をクリックすると、確認画面が表示されるので、説明をよく読んで「次へ」をクリックする(図4)。すると、システムの復元が実行され、自動的に再起動が行われる。再起動後に説明が表示されるので、内容を確認して「OK」をクリックする(図5)。この時点でウィンドウズの設定は、指定した復元ポイントに戻っている。

●「システム復元」の仕組み

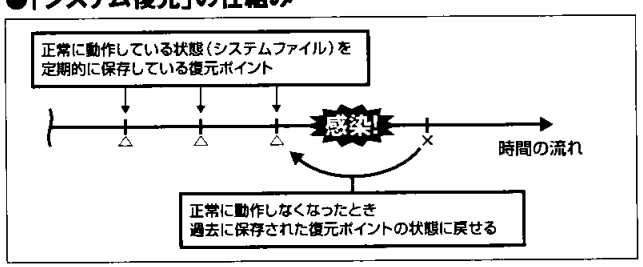


図1 ウィンドウズの設定を変更する度に復元ポイントが自動的に記録される。ウイルスを削除後、感染前の復元ポイントに戻せば、ウイルスが変更した設定は無効になる

[注]復元ポイント以降に更新したウィンドウズアップデートの内容は失われるため、復元直後には必ずウィンドウズアップデートを行って最新の状態にしておこう

●システムの復元ツールを使う

図2、図3 「スタート」→「すべてのプログラム」→「アクセサリ」→「システムツール」→「システムの復元」を選択するとウィザードが起動するので、「次へ」をクリックする(図2)。ウイルスに感染する前で、一番最近だと思われる復元ポイントを選択し、「次へ」をクリックする(図3)

図2

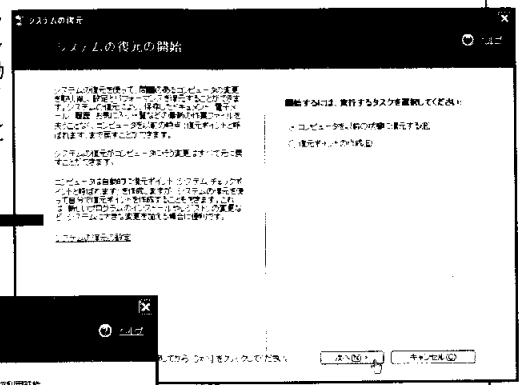


図3

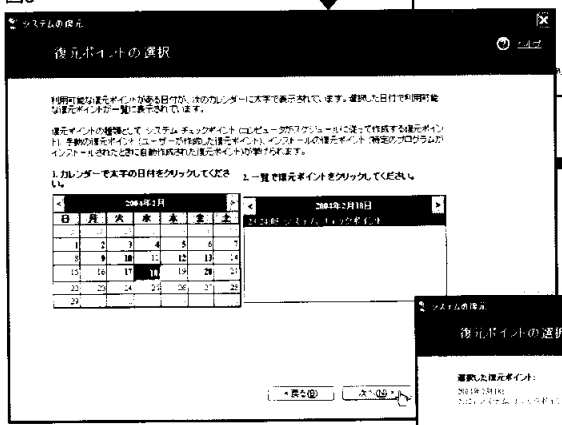


図4

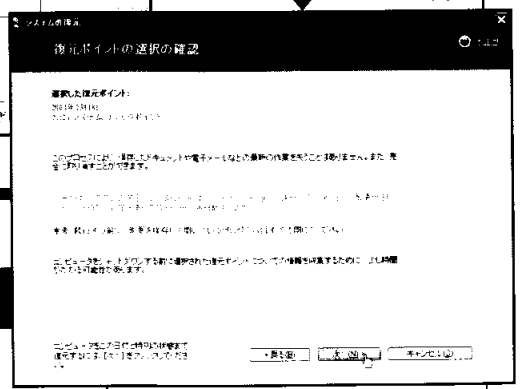


図5

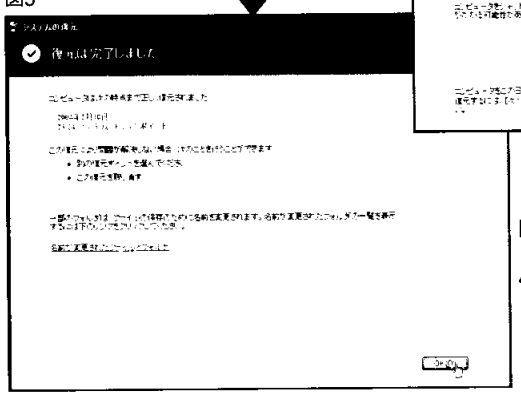


図4、図5 選択した復元ポイントを確認する。説明を読み、「次へ」をクリックする(図4)。ウィンドウズがシャットダウンされ、システムが復元された後に再起動が実行される。復元終了のメッセージが表示されたら、「OK」をクリックする(図5)。この後、念のため全システムのウイルスチェックを行おう

感染が疑わしいときは…… 対処法

④パソコンが起動しないときは<その1>「セーフモード」で起動する

セーフモードは"限定"モード

パソコンが起動しないときセーフモードなら起動できる場合がある

セーフモードでは、利用できる周辺機器や操作がかなり限定される

ウィンドウズは、調子が悪くなると起動できなくなることがある。そこで機能を最低限に絞り、ともかく起動できるようにするのがセーフモードだ。ウイルス感染によってパソコンが起動しなくなってしまったら、セーフモードを試そう。

セーフモードの起動方法は、パソコンによって違う場合があるので、マニュアルを確認しよう。ほとんどの機種では、電源スイッチを入れ、メーカーロゴなどが表示されている間に「F8」キーを押し続けると、ウィンドウズ拡張オプションメニュー[注]が起動する(図1)。マウスは使えないので、キーボードの矢印キーを使って「セーフモード」を選択し、「Enter」キーを押すと「オペレーティングシステムの選択」画面になる(図2)。通常は1種類しか登録されていないので、そのまま「Enter」キーを押す。

ユーザー名選択の画面が表示されたら、ユーザー名を選択し、必要ならパスワードを入力して「Enter」キーを押す。確認のメッセージが表示されるので、「はい」をクリックすると(図3)、セーフモードでパソコンが起動する(図4)。

セーフモードでは、壁紙は表示されず、画面サイズが最小になるので、アイコンが大きく見える。また、画面の四隅に「セーフモード」と表示される。

この状態でウイルス駆除ツールの実行、システムの復元、データのバックアップなどを実行できる。ただし、CD-Rへは書き込めないので、バックアップにはUSBメモリーやUSB接続のポータブルハードディスクなどを活用しよう。USBメモリーは、USBポートに差し込んで読み書きできるフラッシュメモリーで、128MBのものが6000円程度。ポータブルハードディスクは40GBクラスで2万～3万円で購入できる。日常のバックアップに使うにも便利だ。

●セーフモードの特徴

- **セーフモードとは必要最小限の機能のみの起動モードである**
- **画面サイズと色数が最小限なので、アイコンが大きく見えるなど、画面の印象が変わる。また、画面の四隅に「セーフモード」と表示される**
- **USBメモリーなど大容量記憶装置は接続可能だが、CD-Rへの書き込みはできない**
- **インターネットへの接続は、「セーフモードとネットワーク」のときのみ可能**

[注]ウィンドウズMe以前では「起動メニュー」と呼ぶ

●セーフモードで起動

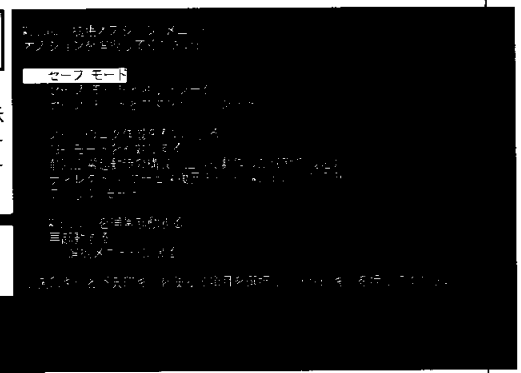


図1　電源を入れ、メーカーロゴなどが表示されているときに「F8」キーを押すとメニューが表示されるので、矢印キーで「セーフモード」を選択

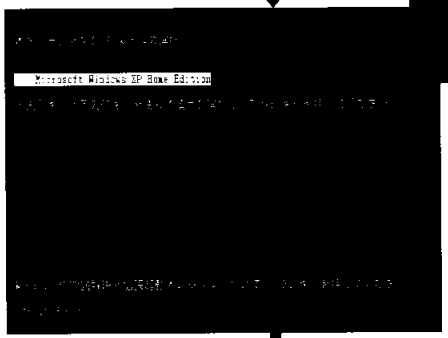


図2　起動するOSを選択する。通常は1つしかないので、そのまま「Enter」キーを押せばよい

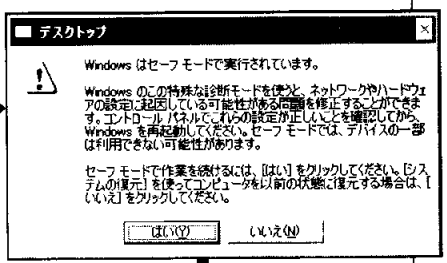


図3　通常の起動時と同様にログインアカウントを選択すると、このメッセージが表示されるので、「はい」をクリックする

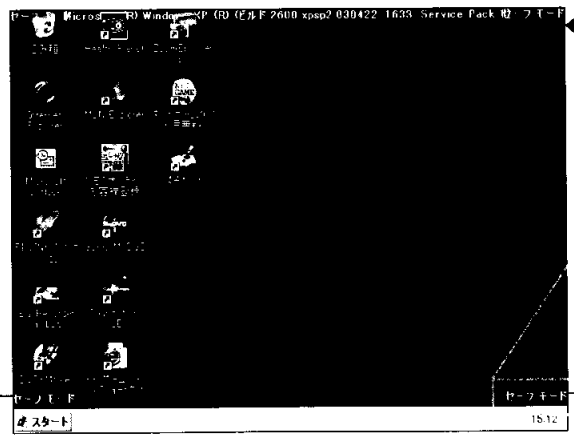


図4　セーフモードで起動した画面。画面サイズは最小で、四隅に「セーフモード」と記載されている。この状態で、データのバックアップや駆除ツールを実行できる

④パソコンが起動しないときは<その2>
最後の手段「再セットアップ」の手順

すべてをーからやり直す

- **ウイルスとともに、これまでのデータや設定はすべて消え、工場出荷時の状態になる**
- **エクセルなどのソフトは、再インストールする必要がある場合も**
- **ウィンドウズアップデートや定義ファイルの更新をまず行う**

●再セットアップに必要なもの

パソコンに付属の説明書と再セットアップ用のCD-ROMなど用意しよう

パソコンがセーフモードでも起動できない場合や、駆除ツールが入手できず、うまく駆除できない場合、最後の手段として再セットアップがある。ハードディスクをフォーマット(初期化)して、ウィンドウズを最初からインストールし直し、工場出荷時の状態に戻す方法だ。

ハードディスクをフォーマットすると、これまでにインストールしたアプリケーションや自分で作ったデータは、すべて消去される。セーフモードなどで起動できる場合は、必要なデータをあらかじめバックアップしよう(手順①)。

再セットアップの方法は、パソコンのメーカーや機種によって異なるので、パソコンに付属の説明書をよく読んで、指示に従おう。再セットアップ用の付属CD-ROMを使う場合と、ハードディスク内に圧縮して保存されたデータを利用する場合がある(手順②)。

再セットアップ後のパソコンは、ウィンドウズアップデートやウイルス定義ファイルが長期に渡って更新されていない状態だ。まずウイルス対策ソフトのインストールとインターネット接続設定を行って、p.40の長期間起動しなかったときの手順を実行しよう(手順③)。

防御策が整った時点で、一度全システムチェックを行う(手順④)。ウイルスに感染していなければ、まず、オフィスソフトなどのアプリケーションをインストールして設定し直そう(手順⑤⑥)。

バックアップデータを元に戻す際には、注意が必要だ。ウイルスがもしデータに紛れ込んでいたら、再び感染してしまう。まず、バックアップデータのウイルスチェックを行って、ウイルスがいないことを確認し(手順⑦⑧)、それからデータを元の場所にコピーする(手順⑨)。

すべての作業が終わったら、もう一度全システムチェックを実行しよう。ウイルスに感染していないことを確認すれば完了だ(手順⑩)。

●再セットアップの手順

① 重要なデータをバックアップ

再セットアップでは、ウイルスとともにこれまでのデータや設定はすべて消えてしまう。必要なデータはすべてバックアップする(p.60〜63)。

② パソコンの説明書に従って再セットアップ

再セットアップの方法は、パソコンのメーカーや機種によって異なる。パソコンに付属の説明書をよく読んでから、実行しよう。

③ 長期間起動しなかったときの手順を実行

セットアップ直後は無防備な状態だ。まず、ウイルス対策ソフトをインストールしてから、インターネットに接続できるようにし、長時間起動しなかったときの手順を実行する(p.40)。

④ 全システムチェック

ウイルス対策ソフトの定義ファイルが最新になっていることを確認し、全システムチェックを実行する。

⑤ ウイルスがいないことを確認

全システムチェックでウイルスが検出されなければ、ウイルスを駆除できていることになるので、パソコンを元の状態に戻す作業を開始する。

⑥ アプリケーションをインストール

ソフトを再インストールする。機種によってはプリインストールされていたエクセルやワードも再インストールが必要な場合がある。

⑦ バックアップしたデータをウイルスチェック

バックアップしたデータをウイルスチェックする。万が一バックアップデータにウイルスが紛れ込んでいれば、また感染してしまうからだ。

⑧ ウイルスがいないことを確認

バックアップデータにウイルスが紛れ込んでいないことを確認したら、バックアップデータを元に戻す作業を開始する。

⑨ バックアップデータをハードディスクに戻す

バックアップしておいたデータを元の場所に戻して、再び利用できるようにする(p.64〜65)。

⑩ もう一度全システムチェック

パソコンが元の状態に戻ったら、念のためにもう一度全システムチェックを実行し、ウイルスに感染していないことを確認する。

感染が疑わしいときは…… 対処法

再セットアップの前にバックアップ

大事なものだけに絞るのがコツ

ほとんどのデータは マイドキュメントにある

バックアップするのは 本当に大事なものに絞る

メールの保存場所は アウトルック・エクスプレスの オプションで確認できる

パソコンを再セットアップすると、ハードディスクに保存されていたデータはすべて消去されてしまう。必要なものは、再セットアップ前に別のメディアにバックアップしよう。ただし、欲張って何もかもバックアップすると作業に時間がかかる。バックアップは、消えてしまうと取り返しがつかないものや、作り直すのに時間がかかるものなどに絞るほうがよい(図1)。また、緊急時のバックアップの手間を少なくするためにも、大切なデータは普段からこまめにバックアップしておくことをお勧めする。

エクセルなどで作成したデータは、特に別のフォルダを指定していなければ、「マイドキュメント」にある。大容量のポータブルハードディスクなどが利用可能なら、マイドキュメントをまるごとバックアップするとよいだろう。

アウトルック・エクスプレス(以下OE)のメールは、マイドキュメントとは異なる場所に保管されている。OEを開いて「ツール」→「オプション」を選択し、「メンテナンス」タブを開く(図2)。「保存フォルダ」をクリックすると、メールの保存場所が表示される。書き留めるには長いので、保存場所を左端から右端までドラグしてすべて選択し、右クリックして「コピー」を選択しよう(図3)。

次にマイドキュメントを開き、「アドレス」欄のアドレスを選択して反転状態にする。これを右クリックして「貼り付け」を選択すると、アドレスがメールの保存フォルダに置き換わる(図4)。この状態で、アドレス欄の右端にある「移動」ボタンをクリック。開いたフォルダに表示されているのがメールデータだ。

ここにあるすべてのファイルを選択し、右クリックで「コピー」を選択。バックアップ先のフォルダを右クリックして「貼り付け」を選択する。これでメールデータのすべてをバックアップフォルダにコピーできる。

●バックアップするもの

<バックアップが必要なもの>

- エクセルやワードで作成した文書ファイルやテンプレートで、簡単に作り直せないもの
- メールのデータ
- アドレス帳(メールソフト、ハガキ作成ソフト、携帯電話のメモリー編集ソフトなどについてチェック)
- ブラウザーの「お気に入り」
- 画像データ

<バックアップが必要でないもの>

- アプリケーションソフトなど

図1 後から作り直せないものや、作り直すのに非常に時間がかかるものをバックアップする

●メールのバックアップ

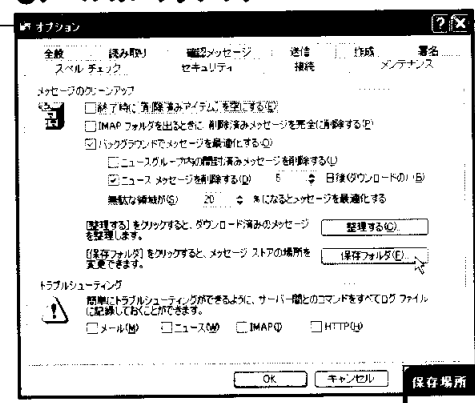


図2 アウトルック・エクスプレスで「ツール」→「オプション」→「メンテナンス」と選択して、「保存フォルダ」をクリック

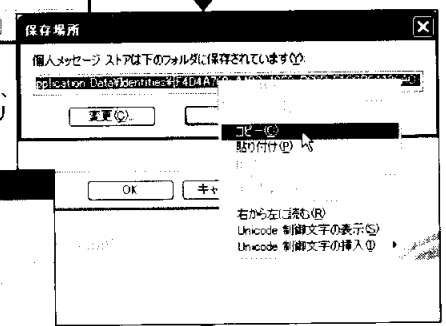


図3 保存場所をドラグしてすべて選択し、右クリックして「コピー」を選択。「OK」をクリックする

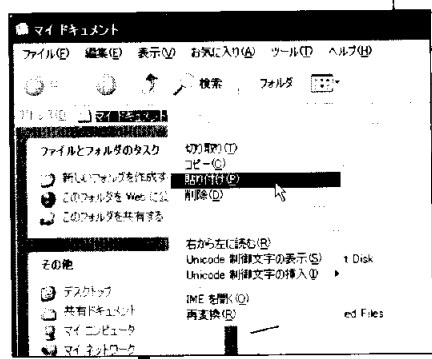


図4 マイドキュメントの「アドレス」欄でアドレスを選択し、右クリックして「貼り付け」を選択。アドレス欄の右端にある「移動」をクリックする

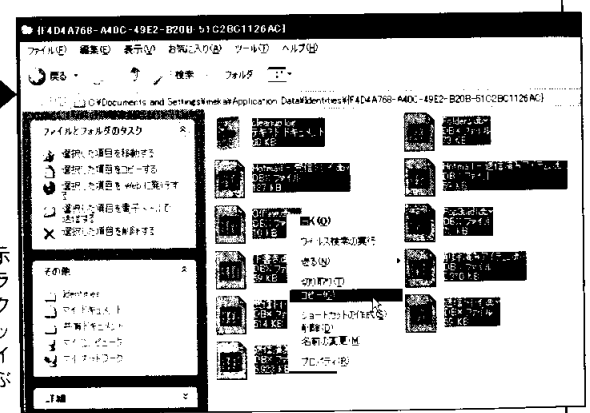


図5 メールの保存フォルダが表示されるので、すべてのファイルをドラグして選択する。それらを右クリックして「コピー」を選択。あとは、バックアップ用のフォルダまたはドライブを右クリックし、「貼り付け」を選ぶとファイルがコピーされる

アドレス帳とお気に入りをバックアップ

インポート/エクスポートを活用

アドレス帳とお気に入りは、インポート/エクスポート機能でバックアップできる

アウトルック・エクスプレスのアドレス帳や、インターネット・エクスプローラの「お気に入り」は、データを他のプログラムで利用するためのインポート/エクスポート機能を利用すれば、簡単にバックアップできる。

アドレス帳は「ファイル」→「エクスポート」→「アドレス帳(WAB)」を選択し(図1)、保存場所とファイル名、ファイルの種類を指定すると、アドレス帳のデータすべてを指定したファイルに書き出せる(図2、図3)。また、アウトルック・エクスプレスでは「ツール」→「アカウント」→「エクスポート」を選択すると、メールアカウント設定のバックアップもできる。

お気に入りは、インターネット・エクスプローラで「ファイル」→「インポートおよびエクスポート」を選択。すると、ウィザードが起動する(図4)。図5の画面で「お気に入りのエクスポート」を選び、図6で保存したいお気に入りフォルダを選択。すべて保存するときは画面の一番上の「Favorites」を選択しておけばよい。図7で保存場所を指定。初期設定のまま変更しなければ、マイドキュメントの「bookmark.htm」というファイルにデータが書き出される。

●アドレス帳のバックアップ

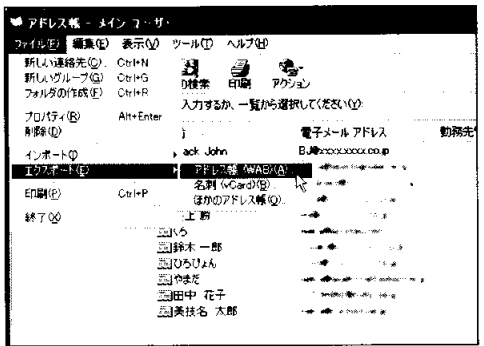


図1 アドレス帳を開いて、メニューバーから「ファイル」→「エクスポート」→「アドレス帳(WAB)」を選択する

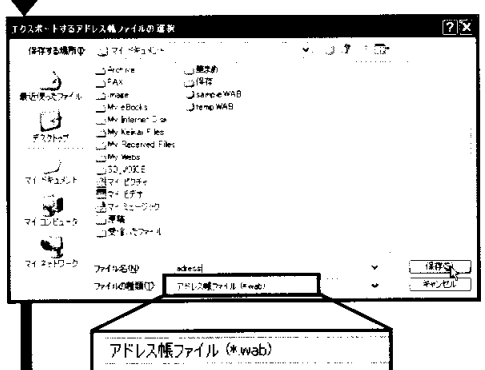


図2 保存場所はマイドキュメントなどわかりやすい場所にして、適当なファイル名を入力する。ファイルの種類は、「アドレス帳ファイル(*.wab)」を選択し、「保存」をクリック

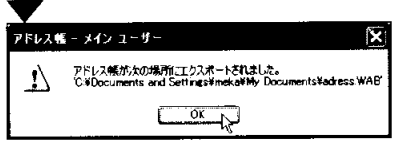


図3 メッセージを確認して「OK」をクリックする。指定した場所にファイルが保存されているので、バックアップフォルダにコピーする

●「お気に入り」のバックアップ

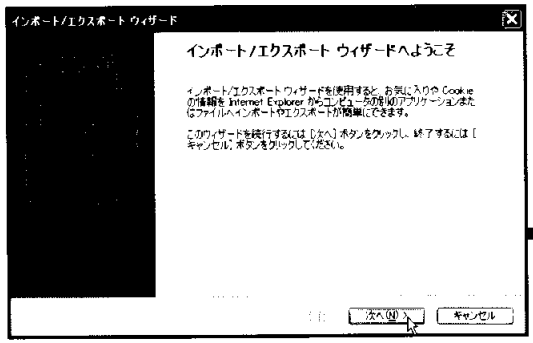
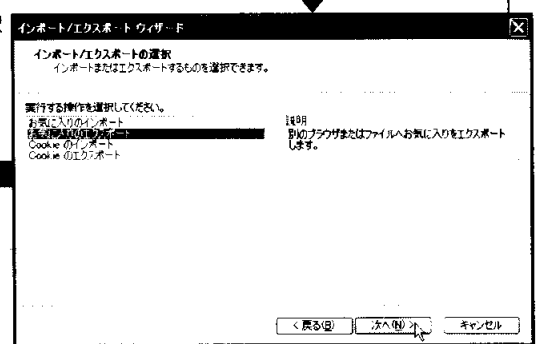


図4 インターネット・エクスプローラで「ファイル」→「インポートおよびエクスポート」を選択し、「次へ」をクリックする

図5 「お気に入りのエクスポート」を選択して、「次へ」をクリックする



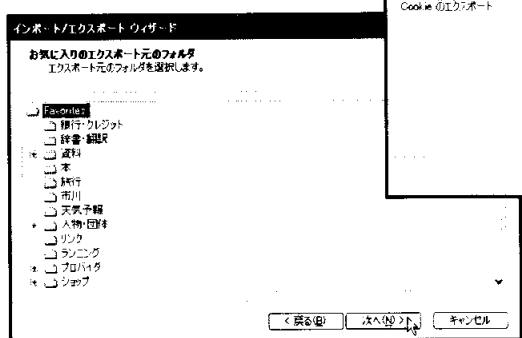


図6 すべてバックアップするときは、「エクスポート元のフォルダ」は、「Favorites」を選択し、「次へ」をクリックする

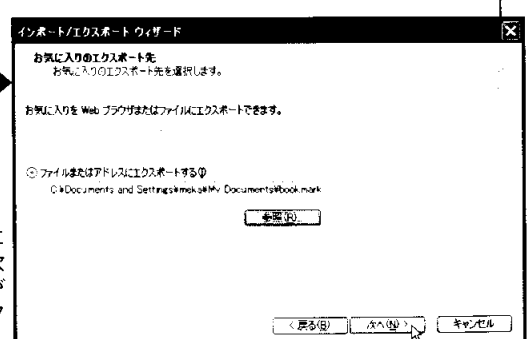


図7 「ファイルまたはアドレスにエクスポートする」を選択し、「次へ」をクリック。確認のメッセージが表示されるので、「OK」をクリックする

感染が疑わしいときは…… 対処法

バックアップしたデータを元の場所に戻す

保存場所を確認して戻す

- **アプリケーションソフトのデータは、先にソフトをインストールしてから戻す**
- **メールは、保存フォルダを確認して戻す**
- **エクスポートしたデータは、インポート機能で戻す**

再セットアップ後、バックアップファイルを戻すときは、アプリケーションを再インストールしてからにしよう。バックアップしていた設定ファイルが上書きされてしまうかもしれないからだ。

アウトルック・エクスプレスのメールデータを戻すには、p.61の図2～図5と同じ手順で保存フォルダを開き、バックアップしたファイルを上書きコピーする(図1)。

エクスポート機能でバックアップしたアウトルック・エクスプレスのアドレス帳や、インターネット・エクスプローラの「お気に入り」は、インポート機能で読み込む。アドレス帳は「ファイル」→「インポート」→「アドレス帳(WAB)」を選択(図2)。図3で、バックアップしておいたファイルを選択すればよい。

お気に入りは、「ファイル」→「インポートおよびエクスポート」でウィザードが起動。画面の説明に従って「お気に入りのインポート」を選択し(図4)、保存しておいたファイルを指定(図5、図6)。インポート先のフォルダは「Favorites」を選択する(図7)。

●アウトルック・エクスプレスのメールを戻す

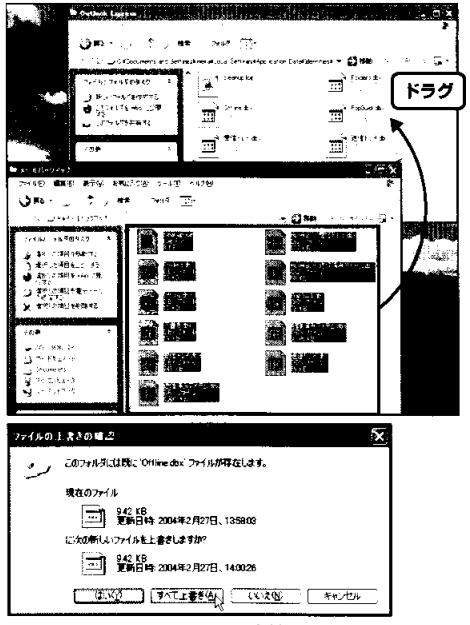


図1　p.61の図2～図5と同じ方法でメールの保存場所を開き、バックアップしておいたファイルを、そのフォルダにすべてドラグ。現れた画面で「すべて上書き」をクリックする

●アドレス帳データを戻す

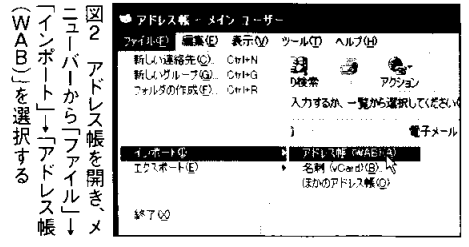


図2　アドレス帳を開き、メニューバーから「ファイル」→「インポート」→「アドレス帳(WAB)」を選択する

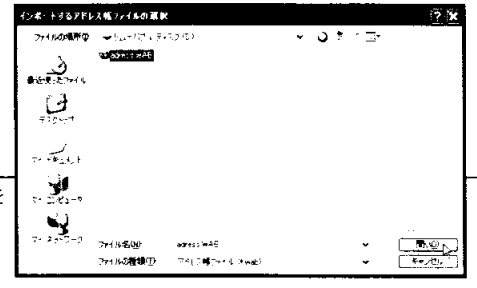


図3　バックアップしておいたファイルを選択して「開く」をクリックする

●「お気に入り」を戻す

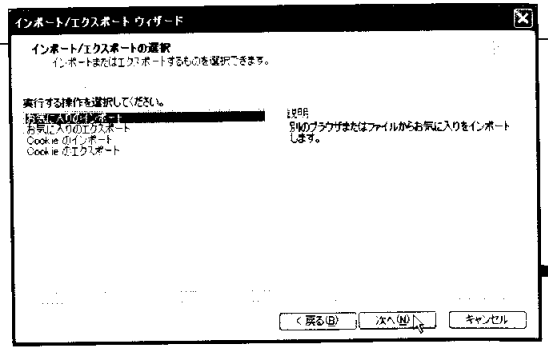


図4　インターネット・エクスプローラで「ファイル」→「インポートおよびエクスポート」を選択し、「次へ」をクリック。「お気に入りのインポート」を選択して「次へ」をクリック

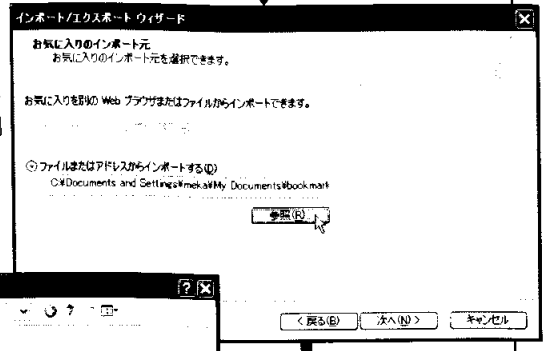


図5　インポート元を指定する画面で「ファイルまたはアドレスからインポートする」を選択して「参照」ボタンをクリックする

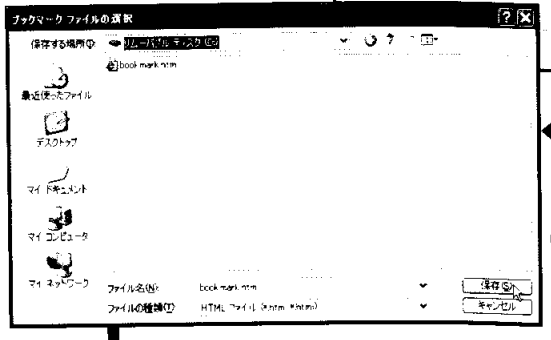


図6　バックアップしておいたファイルを選択して「保存」をクリック。元の画面に戻るので「次へ」をクリックする

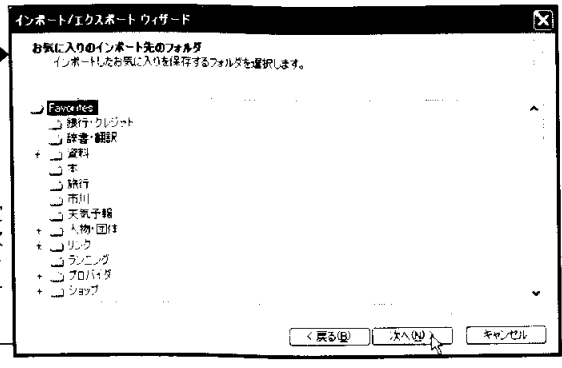


図7　ここでインポート先を指定する。「Favorites」を選択して「次へ」をクリック。あとは「完了」をクリックすると、お気に入りデータが読み込まれる

キーワード別索引（五十音順）

2004年 5月1日発行
発行人●斎野 亨
編集長●大用昌之
文●池田利夫（ジャムハウス）、出雲井 亨、梅方久仁子
写真●スタジオ・キャスパー
発行●日経BP社
発売●日経BP出版センター
〒102-8622 東京都千代田区平河町2-7-6
アートディレクション●Aleph Zero Co.,ltd.
制作●朝日メディアインターナショナル
印刷・製本●凸版印刷