特集1　「何もしていない」あなたが加害者

会社に損害を与えないための セキュリティー security manual マニュアル

text : 株式会社ラック　新井 悠、角田玄司、奥村 允 (p78〜p85)
大澤文孝 (p86〜p91)
JNSA不正プログラム調査WG　渡部 章 (p92〜p93)
illust: Shu-Thang Grafix

Blasterウイルス感染で大騒ぎになった会社も多いだろう。しかし考えてみてほしい。「ウイルスに感染した」あなたは被害を受けたと思うだろうが、あなたのウイルス感染によって、会社は業務効率の低下・復旧作業の人件費など、金銭的な損害を被っているのだ。Blaster感染による損害額はたいしたことがなかったかもしれない。しかし、次に現れる悪質なウイルスにあなたが感染したことが原因で会社が倒産する可能性もないわけではないのだ。
会社のセキュリティーシステムでは、高速かつ大規模に感染する現在のウイルスは防ぎきれない。自分のPCを守るのは最終的にはあなただけなのだ。

あなたのウイルス感染が会社の倒産を招く？

さまざまな経路から襲われるクライアントPC

会社のファイアーウォールだけでは守りきれない現状

Blasterワームは、初めからサーバーではなくクライアントPCの脆弱性を標的にした攻撃だった。このため、セキュリティーに対する意識が薄い多くの会社員が普段何気なく使っている会社のPCが次々と感染し、業務に影響を与える例も少なくなかった。そして、こうした感染の加害者となる可能性は誰にでもある。

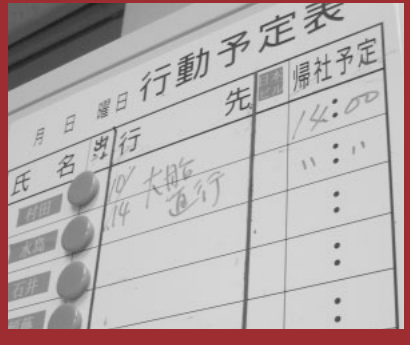
プロローグ～8月の悪夢
普通の会社員が加害者になる実態

8月のお盆休みではあったが、商社の営業担当者であるA氏は多忙な日々を送っていた。多忙ゆえに、彼は電子商取引を利用して商品を購入することが多かった。その日、彼は営業先から会社に戻る途中、自分のノートPCにPHSを接続してインターネット経由でPCの新機種をチェックしていた。すると、突然ウィンドウズの再起動メッセージが画面に表示された。

なんだかPCの調子が変だ

「おかしいな」とは思ったが、表示されたメッセージのカウントダウンは1秒1秒と進んでついに自動的に再起動してしまった。それでも「まあ、いいか」とA氏は気にとめなかった。これまで、PCにまつわるたくさんのトラブルを同僚から耳にしており「これも同じようなことだろう」と。A氏はPCを終了させ、職場へと向かった。

職場に戻ったA氏は、さきほどの自分のノートPCを社内のLANに接続し、メールの受信を始めた。営業先からのメールをチェックして返信する。いつもと何ら変わりない仕事だった。すると、同僚のB子が「あれ？　再起動だって……変だわ」と声を上げた。「私も、さっき再起動のメッセージが表示がされたよ」とA氏の上司であるC課長も言った。そこでA氏は「気にすることはないでしょう」と答えた。しかし、C課長は「でも、重要なデータが飛んでしまったら元も子もないからな……」と言うと



続けざまに「おい！　やっぱり変だ。また再起動だ。どうなってる！」と声を荒らげた。職場に不穏な空気が流れた。

これでは仕事にならない！

職場のパソコンが次々と再起動を繰り返す中、業務は滞り始めていた。そして、C課長に呼び出された情報システム部のD氏がやってきた。C課長は「君、どうなっているんだ、これは。困るよ、こんなんじゃ仕事にならない！」と大声を上げた。D氏は「これは新型のワーム（種類などはP.86）かもしれません。調査させてください」と言うと、多部署の上司に同意を得てからチームを結成した。調査した結果、Blasterワームの仕業であることがわかった。D氏は感染したと考えられる会社のPCに対策ソフトを使用してワームの駆除を行った。しかし、それでは終わらなかった。

次の日も、次の日もPCの再起動が繰り返され、社内でBlasterが蔓延していく。D氏が根本的に改善するためのパッチを適用しようとしても、「おかしなことが起きては困る」とC課長がそれを許さなかった。社内のコンピュータには何度も駆除ツールでBlasterを駆除した。それでも、Blasterに感染するコンピュータが後を絶たない。「Blasterを持ち込んでいる人間がいる」と判断したD氏は、ネットワーク監視ツールを使用し、営業チームのネットワークを一日中監視することにした。自分の通常業務ができなくなってしまうが、これしか手がなかった。

翌朝からD氏が監視ツールを使用し始めたが、何も問題は見つからない。おかしい。昼が過ぎようとしたとき、営業先から帰ってきたA氏が席につき、ネットワークにそのノートPCを接続させた。この動きを追いながら、監視ツールの表示画面に視線を戻したD氏は目を見張った。すさまじい勢いでBlasterワームが感染を広げ始めたのだ。D氏はA氏に「ノートPCのLANケーブルを抜いてください」と叫んだ。なんのことか理解していないA氏に、C課

長が言い放った。「そうか、君だったんだな。おまえが加害者なんだな！」

A氏はなぜそんなことを言われたのかわからずに呆然としていた。PHSで接続した際に感染していたことも知らずに……。

Blasterリローデッド

情報システム部のD氏は、Blasterワームの蔓延を終息させ、本来の仕事に戻ることができた。そして、その直後に……。

「ウェブサイトが見られないんだが」と総務部のH部長から電話があった。すると、次々とD氏のもとに電話がかかってくる。D氏はいやな予感を覚えた。再び社内にBlasterワームが蔓延していたのだった。しかし、今回はまったく手がかりがつかめない。ネットワーク監視ツールを使っても、その根源をつきとめられない。D氏はこれまで何度もパッチの適用という根本的な解決策を進言してきたが、その都度却下されてきた。肩を落としたD氏は、帰宅時の電車の中で、ふと吊り広告に目をやると「無線LAN特集」とあった。D氏は、「これかもしれない」と直感した。

翌日、D氏は無線LAN用の検出ツールを使ってみた。すると、社内にはないはずの無線LANのアクセスポイントが表示された。「きっとこれだ」とD氏は思ったが、無線のため、どの場所にあるかが特定できない。調査は困難だったが、無線LANを使っていることを同僚に自慢していたことが発端で、勝手にアクセスポイントを設置していたのはS氏だということがわかった。S氏は会社の規則を破り、自分のノートPCを会社に持ち込んでいたのだ。

D氏は、S氏の上司であるK係長に「Sさんはご自分のPCを持ち込んでいるようですので、一度ウイルスのチェックをさせていただいたほうがよいですね」と話した。許可をもらったD氏は、K係長とともにS氏のもとへ向かい、「ちょっと、そのノートPCを見せてもらってもいいですか」と尋ねた。S氏はめんどくさそうにD氏を一瞥したが、K係長が目に入ったため「どうぞ」と答えた。D氏がファイルをスキャンすると……あった。Blasterワームの本体である「msblast.exe」が発見された。D氏の報告を聞いたK係長はS氏に言った。「君は自分が会社にどんなことをしたのかわかっているのか？　みんな君の被害者なんだぞ！」

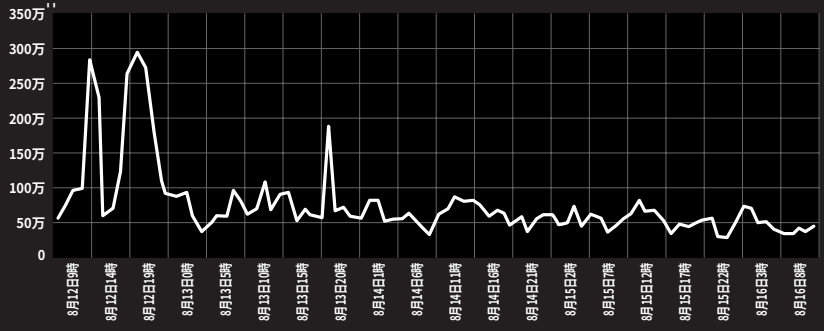
この話はけっして絵空事ではない。どの会社でも起こり得る。

あなたを狙って繰り返される攻撃
Blasterの脅威はまだ終わっていない

筆者が所属している株式会社ラックのJSOC（Japan Security Operation Center）では、2003年8月12日の午前4時ごろから異常なトラフィックが急増していることを検知した。各所に設置されたファイアーウォールの遮断データをグラフで表示させたモニター画面には、とどまることを知らないかのように折れ線グラフが右肩上がりを続けていた（図1）。

現在では、増加傾向は一段落しているものの、引き続き高いレベルを維持しており、感染活動自体は変わらないままの状態にある。

図1：いつまでたっても終わらないBlasterの攻撃

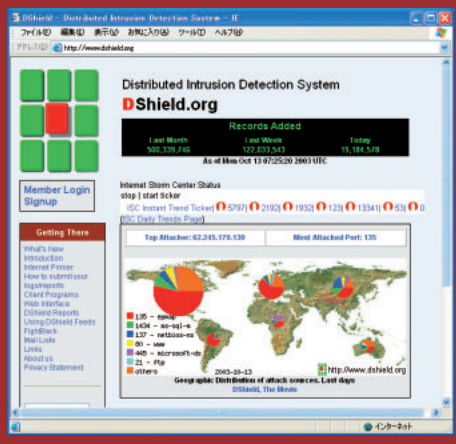


JSOCの全監視顧客のアクセスログの中で、送信先のポート番号がTCP135番（今回の攻撃で利用されたポート）のログの推移。ユーザーが帰宅後に感染したと見られる8月12日19時頃にピークを迎える。その後収束するが、引き続き約50万件と高レベルを維持。

本稿執筆時点においても、インターネット上の攻撃活動状況を集積して公開しているDshield.org（図2）を見ると、相変わらずBlasterワームやその亜種であるWelchiaワームの活動が盛んなことがわかる。

この一方で、数年前に大流行したワームの活動も今もまだ終息していない。いまだにNimdaワームやCodeRedワームによる攻撃は続いているのだ。サーバーがインターネットを経由して悪意あるものに狙われることは、これまで何度もあった。そして、2年前に発生していまだに終息していないNimdaワームのように、個人が利用するクライアントコンピュータも狙われるようになった。セキュリティーホールを利用するワームやウイルスは、マイクロソフト社より配布されている修正プログラムを適用しておけば感染することはない。修正プログラムを適用しないのは、特に、会社の規定でそれを定めているのにそれを怠っていることは、社員の怠慢である。その怠慢が会社に損害を与え、いつの間にか「加害者」になってしまう。狙われているのはあなたなのだ。

衰えないBlasterの活動



主要なファイアーウォールと侵入検知システム（IDS）のログを集めて解析しているDShield.orgのウェブサイト。攻撃元や攻撃されたポート、過去5日間の攻撃出所の地理的分布などが掲載されている。円グラフの赤い部分がBlasterなどのワームによって生じる攻撃。
URL http://www.dshield.org/

大げさではなく数億円に上ることも
あなたの怠慢が金銭的損害を会社に与える

社員のそうした怠慢がどのような損害を会社に与えるのだろうか。セキュリティー事故は、社員には「面倒な出来事」で済むかもしれないが、企業にとっては、直接・間接の金銭的な損害を意味する。

ネットワークセキュリティー保険を手がけるAIU保険会社のファイナンシャル・ライン ITリスクスペシャリストである中江透水氏によると、過失、故意、悪意ある第三者などによるセキュリティー事故で企業が被る損害の内訳は表のようになる。具体的な金額は、企業や事故の規模によって数十万円から数億円まで変わることに注意してほしい。しかし、セキュリティー事故の被害調査を行っているJNSA（日本ネットワークセキュリティ協会）のプロジェクトでは損害額の算出モデルを毎年改良してきているし、保険会社はすでにITセキュリティー保険を商品として販売している。損害額を算出する手法がある程度固まってきているようだ。

従業員の「ついうっかり」が会社に損失をもたらすのは間違いない事実だ。1つ間

表1：セキュリティー事故で企業が受ける損害の種類

区分	概要
直接損害額	逸失利益。復旧までに通常どおり営業を続けていれば得られたはずの利益や、金銭的負担が発生しているのにその便益を得られなかった場合の費用負担（ネットワークの費用が発生しているのにネットワークが使用不能になったなど）。
復旧費	システムを復旧させるためにかかる人件費やその他のコスト。再発を防ぐために新規のセキュリティー機器を導入した場合の導入費用や管理費も通常はここに含まれる。
謝罪広告費	「他人の名誉を毀損した者に対して被害者の名誉を回復するに適当な処分」として謝罪広告を新聞などの媒体に掲載するための費用。
賠償金	第三者に被害を与えてしまい、訴訟されて支払い命令が出た場合に支払う費用。慰謝料。
見舞金	第三者に被害を与えてしまい、組織ないし個人が謝罪の気持ちを伝えるためにかかる費用。賠償金とは異なり、支払いを行う主体者がその額を決めることができる。
訴訟費用（弁護士費用）	訴訟に対応するための費用。目安として、日弁連の出している報酬規程がある。たいていは着手金＋成功報酬。
業務への間接影響	事故や事故からの復旧のために低下した業務効率は損害とみなされる。ITのセキュリティー事故でも、電話やFAXなどを使って業務を継続できるため、通常の企業では業務効率の低下は20パーセント程度とされている（JNSA被害調査WGによる）。
営業継続費	セキュリティー事故が発生した場合、営業状態を復旧させるためにかかる費用。たとえば、インターネットショッピングのサーバーに使っているデータセンターが使用不能になって復旧の目途がたたない場合に、別のデータセンターと回線を契約してバックアップからデータを戻して元の営業状態に近い状態にする場合の費用。
漏えい情報の回収	漏えいした個人情報を回収するための費用。ウェブなどのインターネットを利用した漏えいがあった場合は、回収が非常に困難なものとなるであろうが、可能な限りの努力をしない場合は被害者や行政から、さらに追及される可能性もある。
株価の下落	因果関係が明確に株価に現れた場合は、それも損失の1つとしてあげられる。
機会損失	セキュリティー事故を発生させたことのある事業者が受注する仕事量の減少がこれにあたる。ブランドや信用を下げてしまったことによって表面化しかねないのがこの範疇である。
恐喝	漏えいされた情報を2次的に利用され、その事業者に対して恐喝が行われた場合、これに対応するための費用。
再ブランディング	セキュリティー事故を発生させた事業者が、事業体のブランド力を復活させるための費用。
行政処分に付随して発生するコスト	法律の定めるところにより、事業者に対して改善命令が行政処分として下された場合に、改善するために発生する費用。
インシデントレスポンス費用	セキュリティー事故が発生した場合の初期対応にかかる費用。コンサルタントを雇って社会的な対応について検討し、被害を発生させることにつながったコンピュータを調査して原因を追究するなどのためにかかる費用。
固定費（人件費）	上記すべてにかかる人件費。

違えれば、あなたの怠慢のために巨額の損害賠償を命じられて会社が倒産してしまう可能性もないとは言えないのだ。

具体的な損害額の例と計算

次ページからは、社員が引き起こすセキュリティー事故とその対策を具体的に説明していく。各対策で損害額の例を示していくが、それぞれの例の金額の内訳や、計算の根拠となる背景をここで先に解説しておこう(下図)。例ではわかりやすくするために、営業継続費用や機会損失、ブランド・信用低下による潜在被害とその回復のための費用などは数字から除いてある。実際にはこれらのコストがかかって、さらに損害額はふくらむ可能性が十分にある。また、この金額はあくまでも例示した状況における計算の参考結果であり、会社の規模や状況が変われば金額には大きな違いが出る。また、各例を金額の大小で比較する意図はないことに注意してほしい。

表2　セキュリティーインシデントが会社に与える損害額の例

① Blasterワームがノート PC から社内に感染し、全社の6割に被害で・・・

650万円の損害

Blasterワームに感染したPCを社内ネットワークに持ち込んで社内PCの6割が感染。社外への影響はなし。社内のすべてのPCを再チェックして復旧させるのに5人のスタッフが2日かかったため、その間スタッフの業務効率に影響が出た。営業していたオンライン販売サイト(年間2億円売り上げ、利益率10パーセント)は感染発覚から販売システムへの影響を確認するまでの4時間停止した。外部に対する影響はなかった。

対策→82ページ

② Klez感染でデータファイル削除! 復旧・対策に・・・

770万円の損害

メールで感染していたKlezの活動でサーバーのファイルの一部が感染。内部でも感染が拡大して5割のユーザーが感染し、感染PCがサーバー上のOffice関連のデータファイルを破壊した。すべてのPCとすべてのサーバーでの検出と駆除に担当者5人で2日かかり、ファイルのバックアップからの復旧に担当者1人で1日かかった。バックアップされていなかったデータの復旧に20人が2日を要した。外部にメールで感染を広げており、その対応に一般社員の1.5倍の人件費がかかる責任者2人が2日を要した。

対策→86ページ

③ NachiワームがVPNから侵入、ネットワークダウン!・・・

250万円の損害

NachiワームがVPN経由でネットワークに侵入。感染した台数自体は全体の4割程度だが、ネットワークが輻輳して、利用できない状態が1日続いた。比較的PCに依存した作業をする会社のため、業務に大幅な支障が出た。ネットワーク機能の回復と感染PCの復旧と全社のPCのセキュリティー対策のための作業にスタッフが15人で1.5日かかり、その間各スタッフは業務に影響があった。本社のインターネット接続に1.5M線×2で月額66万円、インターネットVPNによる本社と関東圏リモートオフィス3か所の接続に合計月額42万円かかっていた。

対策→90ページ

④ バックドアを仕掛けられて踏み台にされた先で個人情報漏洩・・・ 1,600万円の損害賠償

社員1人のPCにActiveX経由でバックドアを仕掛けられて、他社サーバーの攻撃の踏み台に使われる。社内には直接の被害はなく、復旧は2時間程度で終わった。しかし、犯人は攻撃先である他社サーバーのセキュリティーホールを突いて侵入し、10万人分の顧客情報を盗みだして公開した。攻撃先では1人あたり500円の見舞金を支払った。踏み台として使われたことに関して攻撃先から損害額の20パーセントの賠償を請求され、裁判費用も発生した。謝罪広告やマスコミ対応などの危機対応に、合計500万円ほどの費用が発生した。

対策→92ページ

インシデント※5	損害額	損害額の内訳						
※1～※5		直接被害額	直接被害単価※6 システム停止時間	復旧に要した人件費	復旧にかかった人日数※7	補償、補填、損害賠償など※8	業務への間接影響	影響を受けた人数 業務のIT依存度※9 業務に影響のあった平均日数※10
①Blasterワームがノート PC から社内に感染し、全社の6割に被害で・・・650万円の損害	\6,621,766	\121,766	\30,441 4時間	\500,000	10.00人日	\0	\6,000,000	600人 0.20 1.00日
②Klez感染でデータファイル削除! 復旧・対策に・・・770万円の損害	\7,700,000	\0	\0 0	\2,550,000	51.00人日	\150,000	\5,000,000	500人 0.20 1.00日
③NachiワームがVPNから侵入、ネットワークダウン!・・・250万円の損害	\2,679,000	\54,000	\2,250 24時間	\1,125,000	22.50人日	\0	\1,500,000	400人 0.30 0.25日
④バックドアを仕掛けられて踏み台にされた先で個人情報漏洩・・・1,600万円の損害賠償	\16,512,000	\5,000,000 ※11	\0 0	\10,000	0.20人日	\11,500,000	\2,000	1人 0.20 0.20日

※1 ここでは、復旧に要した人件費以外のコスト、営業継続費用、喪失情報資産、機会損失、ブランド・信用低下による潜在被害などは数字から除いてあるため、実際にはこれらのコストがかかってさらに損害額は増える可能性がある。
※2 参考資料:IPA/JNSA 2001年度被害調査報告、JNSA 2002年度被害調査報告など。　※3 どの例も従業員1000人でPCが1000台ある会社を想定。ネットワーク用のファイアーウォールは設置されていたが、ウイルス対策などクライアントPCの管理は個別の従業員に任せていた状態を想定。　※4 1人あたり1日の人件費を5万円とする(月間100万円、月あたり20日就労として)。　※5 管理対象PCが100台ごとに対処に1人日かかったとする。
※6 影響を受ける範囲の時間当たりの売り上げまたはコスト。オンラインサイトでは1日18時間有効とする。例3ではネットワーク費用の1時間あたりの費用をここに計上している。　※7 管理対象100台あたり約2人日を基準とした。
※8 裁判に関する弁護士費用は賠償額を1,000万円の場合、着手金が5パーセント、報酬が10パーセント(日弁連報酬等基準規程による)。　※9 一般企業で0.2(JNSA被害調査WGの数字による)。
※10 平均として、復旧にかかった日数÷2。　※11 謝罪広告費、被害者への謝罪の電話や郵送の費用、行政対応、マスコミ対応などの危機管理費。

人のセキュリティーホールが問題

アップデートさえしていれば防げた損害

セキュリティーホールを狙って今年8月に発生し、猛威を振ったBlasterワームだが、マイクロソフトではこのワームに対する修正用プログラムをその約1か月前には提供していた。それにもかかわらず、世界的な被害となったことを見れば、いかにウィンドウズアップデートが実行されていないかがわかるだろう。

Blasterなどは、インターネットエクスプローラやウィンドウズ（OS）の脆弱性（バグ）を突いたワームだ。セキュリティーホールは、一般にはこうした脆弱性を指すが、広く捉えればアプリケーションのバグにとどまらず、図1のように大きく2つに分けられる。「物理的なセキュリティーホール」は建物や設備の構造上の欠陥や不備なので、一社員ではどうすることもできない。そういった物理的なこと以外のものをここでは「論理的なセキュリティーホール」とし、「開発者、管理者」にかかわる事柄を「システムに関する脆弱性」、ユーザーである社員1人1人にかかわる事柄を「人に関する脆弱性」として挙げた。ワームなどの攻撃に社員が対策できるのはこの「論理的なセキュリティーホール」の部分だ。

図1：OSの脆弱性だけではないセキュリティーホール

- ①物理的なセキュリティーホール
  - ・耐震設備、防火設備などの欠陥や不備
  - ・サーバールームなどへの入退室管理設備の欠陥や不備
  - ・電源、回線設備の欠陥や不備……など
- ②論理的なセキュリティーホール
  - ●システムに関する脆弱性
    - ・OSやアプリケーションなど、ソフトウェアのバグ
    - ・ファイアーウォールやサーバーの設定ミス
    - ・ログ解析や監視の不備……など
  - ●人に関する脆弱性
    - ・ずさんなパスワードの管理
    - ・ウイルス対策ソフトのパターンファイルが未更新
    - ・修正パッチの未適用
    - ・セキュリティー意識の低さ……など

対策 1 professi

ウィンドウズアップデートを実行する Blasterワームがノートパソコンから社内

セキュリティーホールを狙ったワームやウイルスに社内ネットワークが感染すれば、復旧作業に人手や費用がかかるのはもちろんのこと、相当な時間も要する。ECサイトならば、信用の損失にもつながってしまう。

面倒くさいは論外

脆弱性をそのままにしておく罪

人に関する脆弱性は、システムやソフトウェアを人が開発や管理、使用しているかぎりなくならない。その中でも特にソフトウェアは、趣味での開発を別にすると通常は「納期」があるので、それに間に合わせようと十分なテストができずにリリースしてしまうこともざらだ。納期にかなりの余裕があったとしても、ソフトウェアのあらゆる利用環境に合わせた入力や操作などの使い方をすべて完璧に想定してテストするのは事実上不可能である。そのため、ソフトウェアのセキュリティーホールはなくならないし、そこを突いてくる攻撃も止まらないのだ。もちろん、開発者の技術力不足や開発者間のコミュニケーション不足によるバグもある。

このようにセキュリティーホールがなくならないのならば、地道に脆弱性を埋めていくしかない。通常、ソフトウェアベンダーはセキュリティーホールやバグが見つかると、それを解消するための修正プログラム（パッチ、Hotfixなどと呼ぶ）を発表する。不具合が見つかるたびにそのパッチを適用（インストール）するわけだ。Blasterなどのワームは特にOSの脆弱性を突いてくるので、社員が普通に使っているPCに対するパッチの適用を面倒くさがらずに適時実施しなければならない。マイクロソフトでは、このパッチの適用方式を「ウィンドウズアップデート」として提供している。

この適用を怠れば、図2のような被害や損害を招く。企業のシステム管理者などが自社のサーバーをいくら気遣っても、一般社員のPCがたった1台でもパッチの適用を怠っていれば、そこを突かれるのだ（図2の①）。社内のほかのPCがパッチを

適用していて、データの改ざんなどの被害を受けなかったとしても、感染したPCからのワームなどの攻撃は断続的に続くために、社内のネットワークトラフィックが急増して負荷がかかり、場合によってはネットワークが止まってしまう。さらに、感染したPCが他社のネットワークに攻撃をして「被害者だったはずが、知らない間に加害者となってしまう」こともありえる(図2の③④)。こうなると、自社のネットワークを復旧させる手間や費用のほかにも、他社から損害賠償を請求されることも考えられるのだ。社員1人がパッチの適用を怠っただけで、このように被害が広がっていくので「そういったことはシステム管理者や技術者が対処するべきことで、自分は関係のないことだ」「自分1人ぐらいは大丈夫だ」などとはとても言っていられない。

8月のBlaster騒ぎでは、東京都世田谷区役所の情報システムが感染して住民基本台帳ネットワークを停止するまでに至った。その原因となったのは、財務部の職員が個人の携帯電話を使って職場のパソコンをインターネットに接続して感染し、それに気づかずに区役所のLANに再び接続したことが原因だそうだ。もちろんパッチは適用していなかっただろう。そしてこの職員は服務規程違反で訓告処分を受け、ワームの駆除費用約100万円を補てんしなければならないという。

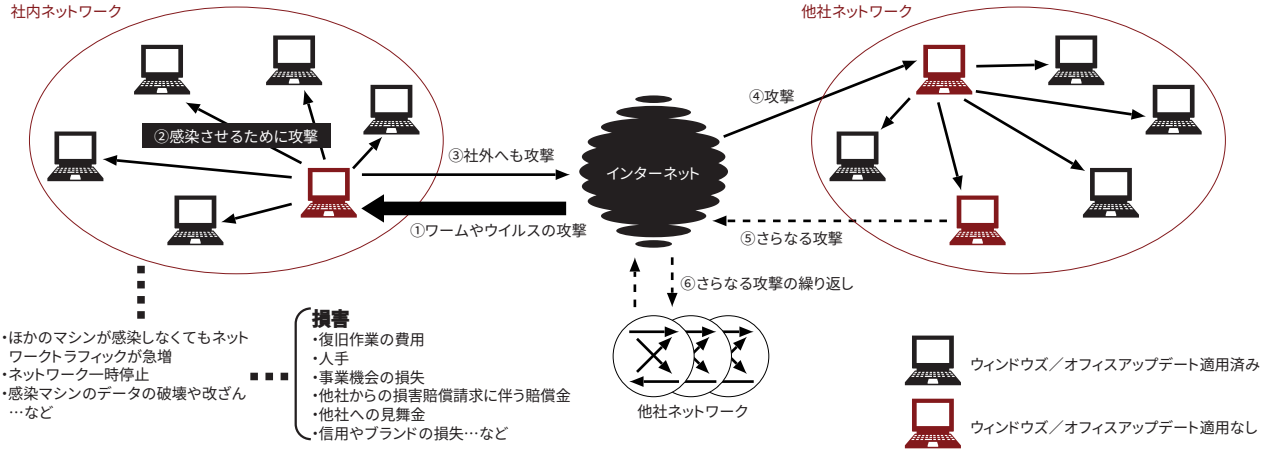
こうしたことが続けば、「あの社員はOSのセキュリティーパッチをほとんど適用したことがないので、我が社にとっては大きいリスクだ」と、実際に被害をもたらさなくても、その前に処罰されてしまうようなことが起こり得るかもしれない。けして大げさな話ではないことを理解してほしい。

o n a l n e g l i g e n c e

に感染し、全社の6割に被害で・・・
約650万円の損害

※社員1000人の企業でオンライン販売サイトにも影響があった場合(詳細は81ページ参照)

図2:たった1台アップデートしないだけでも急速に拡大する損害



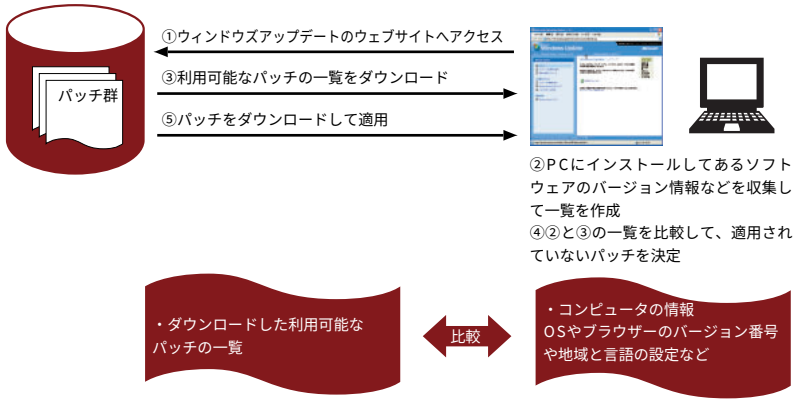
かならずしなければいけない社会人の常識

ウィンドウズとオフィス両方のアップデートを実行せよ

社員であるあなたがまずできるのは、パッチを適時に自分の使っているPCに適用することだ。ウィンドウズでは「ウィンドウズアップデート」を実行することで簡単にパッチを適用できる。ウィンドウズアップデートとは使用しているPCの状態を診断して、システムを最新の状態に保つためのオンラインサービスのことだ。製品が発売されてから見つかった問題の修正や、新機能の追加を半自動的にダウンロードして更新する(図3)。これを実行するだけで、ワームやウイルスが入り込むセキュリティーホールをふさぐことが可能になる。

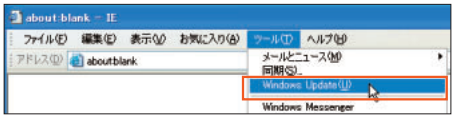
また、マイクロソフトではウィンドウズのほかに企業で広く利用されている「オフィス」アプリケーションのオンラインアップデートも同様な仕組みで用意されている。ワードやエクセルなどのセキュリティーホールを狙ってくるワームなどもあるので、このアップデートも必須だ。ウィンドウズの場合と異なるのは、必要なパッチなどの更新があったときにオフィスのインストールの整合性を維持するために、最初にインストールしたオリジナルCD-ROMか、ネットワーク上のインストールファイルにアクセスする必要がある点だ。ウィンドウズのように自動更新する機能もないので、手間が若干増えるが、ここで面倒くさがってはいけない。それでは、実際にアップデートしてみよう。

図3:ウィンドウズアップデートの仕組み



ウィンドウズアップデート

・ブラウザーを起動したらまずアップデート



1 インターネットエクスプローラのツールバーの「ツール」の「Windows Update」をクリック

2 「更新をスキャンする」をクリック

3 「更新の確認とインストール」をクリック

4 「今すぐインストールする」をクリック

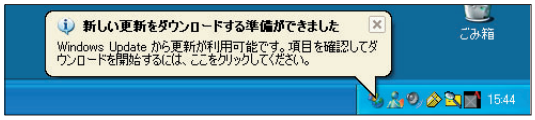
完了 「使用許諾契約に同意しますか」とメッセージが表示された場合には「同意します」をクリックする。また、「システムを再起動しますか」とメッセージが表示されたら直ちに再起動する。最後に「インストールの完了」が表示されれば完了

完了しても気を抜かない

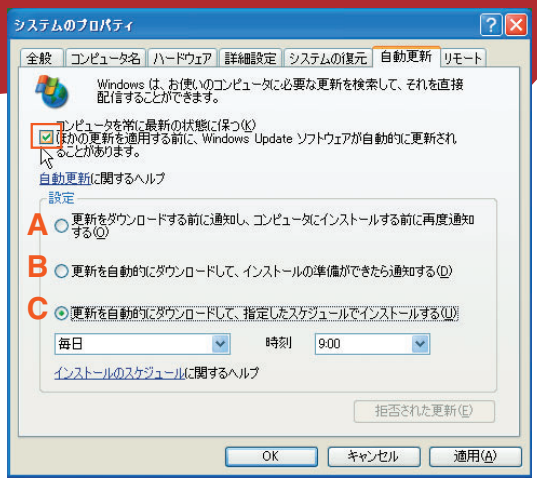
再起動しなければ適用されないパッチなどが複数あった場合は、特に気を付けなければならない。再起動してパッチが適用された後、再び 1 から操作して「現在、利用可能な重要な更新はありません。」と表示されるまで繰り返す。こうしないと1つのパッチが適用されただけで、ほかのパッチが適用されない場合があるからだ。

・自動更新を設定すれば「うっかり」なし

1 「コントロールパネル」の「システム」をクリックして「システムのプロパティ」を開き「自動更新」のタブをクリックする



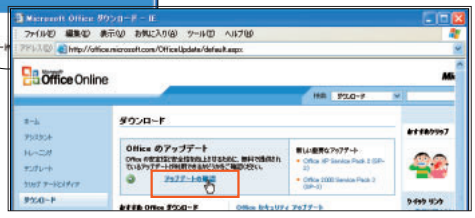
完了 ABCいずれの場合もタスクトレイの地球アイコン、もしくはバルーン表示の部分をクリックして指示に従ってインストールする



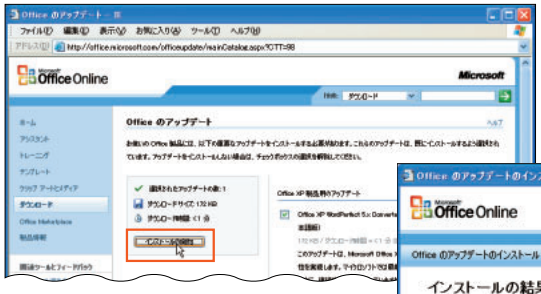
2 「コンピュータを常に最新の状態に保つ」をチェックする。また、設定を好みに応じてチェックして「OK」をクリック。Aは適用するべき更新ファイルがあった場合にダウンロードの準備ができていることをタスクトレイに通知する。Bは更新ファイルがバックグラウンドで自動的にダウンロードされ、インストールの準備ができていることをタスクトレイに通知する。Cは毎日もしくは曜日と時間を設定でき、更新ファイルがあるかどうかをチェックして、更新ファイルがあればバックグラウンドで自動的にダウンロードしてインストールの準備をして、指定した日時になるとインストールする。マイクロソフトが推奨しているのはC。

オフィスアップデート

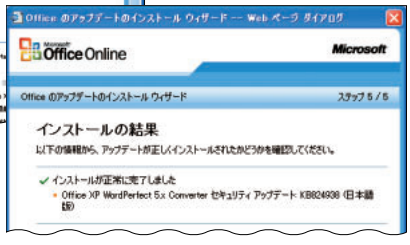
1 ウィンドウズアップデートの画面で「Officeのアップデート」をクリック



2 別ウィンドウが開くので「アップデートの確認」をクリック



3 重要な更新ファイルがあれば表示されるので、確認したら「インストールの開始」をクリック。その後、使用許諾契約書に同意したり、インストールCDを準備したり、指示に従って「次へ」をクリックしていく



完了 「インストールが正常に完了しました」が表示されれば完了

木曜日はアップデートの日？

ウィンドウズとオフィスのアップデートの実行は、毎日出社してPCを立ち上げたときに実行するのが理想的だ。習慣づけるといいが、なかなかそうはいかない人も多いだろう。そこで、最低でも週に一度木曜日に実行することを奨める。過去の経験則では、木曜日に新たな更新ファイルがリリースされることが多いからだ。

「マイクロソフトアップデート」が来年から新登場

10月9日にマイクロソフトのスティーブ・バルマーCEOが発表した新戦略で、ウィンドウズをより安全にする方向性が示された。数週間〜数か月かけて実現していくという新戦略の内容は次のようなものだ。

・2004年内を目途に、ウィンドウズアップデートを「マイクロソフトアップデート」にして、Officeやサーバー製品のパッチもまとめてできる仕組みにする。
・散発的に出ていたセキュリティーパッチは、緊急のものを除いて基本的に1月に1回定期的にリリースする。
・セキュリティーパッチのファイルを30パーセント程度小さくし、またパッチの適用によるシステムの再起動を最大で30パーセント程度減らす。
・ファイアーウォール機能を標準でオンにし、また電子メールやメッセンジャーで悪意のあるファイルを送りつけられることに対する保護を向上させる。

パッチを適用しやすくして、また多少パッチを忘れていてもより安全な状態になるようにするプランだ。セキュリティー関連のわかりやすいドキュメントやツールをさらに増やして安全に対するトレーニングを促進する方針も発表されており、今はまだ面倒なセキュリティー確保もさらにやりやすくなると期待してもいいだろう。

感染経路はメールだけではない

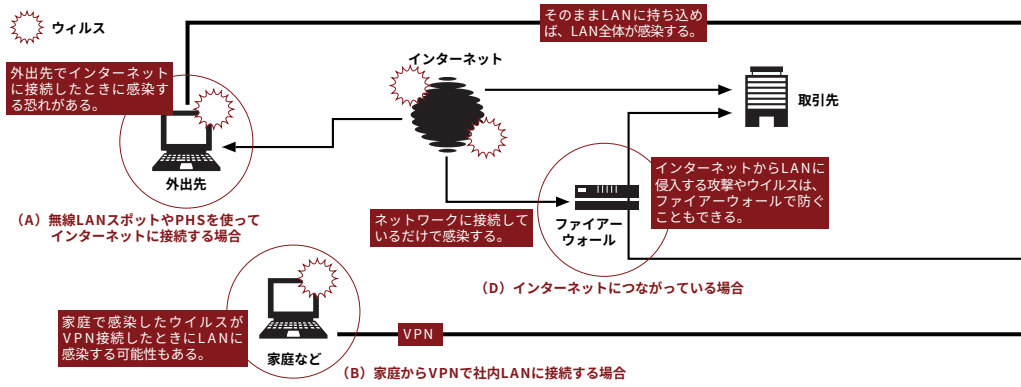
予防と駆除を駆使してウイルスと戦え！

ウイルス対策は、侵入を食い止める“予防”と、侵入してしまったウイルスを“駆除”する方法におおまかに分けられる。具体的には、先に説明したウィンドウズアップデートや、次章で述べるファイアウォールが前者に、ウイルス対策ソフトを使ったファイルのチェックが後者に相当する。

いま、この予防と駆除の2つの方法をいかに効率的に使ってウイルス対策をするかが重要になっている。というのもBlasterに代表される、OSなどのセキュリティーホールを突いて、感染と同時に動作するウイルスが主流となり、もはや事後の駆除では間に合わないからだ。ウイルスの侵入と感染の経路は、無線LANスポットからインターネットに接続する場合（右図A）や、家庭からVPNで社内LANに接続する場合（右図B）のように多岐に渡るため、そのすべてを塞ぐことが重要だ。こうなるとウイルス対策ソフトだけでは万全ではなく、ファイアウォールなど、ほかの方法も併用する必要が出てくる。

ここからは、ウイルスの仕組みを理解したうえで、ウイルス対策ソフトを中心に、いかに予防と駆除を行うべきかを説明する。

図4　ウイルスの感染経路は多岐にわたる



対策 2 Massive

ウイルス対策ソフト導入
Klez感染でデータファイル削除！

ウイルス感染。あなたの不注意が会社に莫大な損害を与えるパターンのもっとも多い要因だ。自社内の感染だけでなく、社外にもウイルスをまいてしまい、失墜した会社の信用をお金に換えると、700万円程度の損害ではすまない。

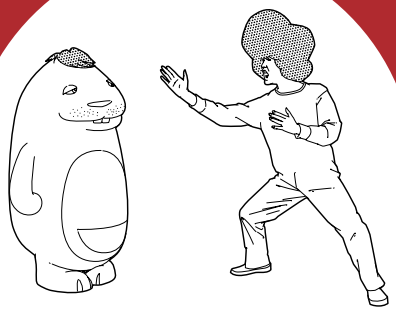
なぜ感染するのかを把握！

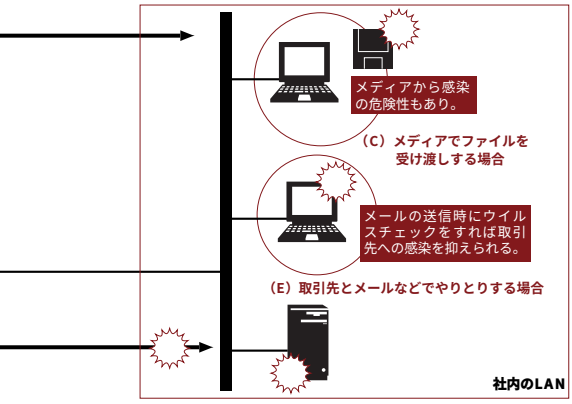
ウイルスのタイプを理解したら3段階で対応

ウイルスとは、感染すると①多量のパケットを送出してネットワークを麻痺させたり、ファイルを削除したりするなどユーザーの意図に反した悪意のある動作をする、②自身のコピーをほかのコンピュータに転送して増殖する、という2つの特徴をもつプログラムのことだ。またこのウイルスは、ファイルに含まれる「ファイル感染型」とネットワークを流れるデータに含まれる「ネットワーク感染型」の2つに大きく分けられるほか、その特徴によってワーム、ウイルス、トロイの木馬などと呼び名が変わる場合がある（右表参照）。

代表的なウイルス・ワーム

名称	種類	感染拡大方法	被害・対策など
Melissa（メリッサ）1999年3月発生	ファイル感染型（マクロ）	ワードのマクロとして構成されたウイルス。感染するとアウトルックを使って、大量の宛て先にウイルスが感染したワードファイルを添付ファイルとして送付する。	送信者が知人の名前となっているメールが送られてくるため、疑いなく開いてしまう人が多く、広い地域で感染した。このころから、「添付ファイルは、誰から来たどのような種類のファイルであれ開かない」という認識が広まった。
Klez（クレズ）2002年春発生	ネットワーク感染型（HTMLメール、添付ファイル）	感染すると、アドレス帳などに記載されたメールアドレス宛てに、自身を感染させるためのメールを送付する。受信者は、メールを開いただけで、このウイルスに感染する。	セキュリティーホールを利用したウイルス。各種ファイルの中身を空にする破壊活動も行う。根本的な対策は、インターネットエクスプローラをバージョンアップし、セキュリティーホールを塞ぐこと。常駐型のウイルス対策ソフトを使っていれば、メールを開く前にウイルス検知できる。
Nimda（ニムダ）2001年9月発生	ネットワーク感染型	ウィンドウズ系サーバーでウェブ機能を提供するIISのセキュリティホールを突いて感染。インターネットエクスプローラのセキュリティホールも突き、クライアントPCにも感染する。コードレッドの発展型。	クライアントPCにも感染するため、大量のネットワークトラフィックが問題となったり、プロバイダーの幹線が一時麻痺するケースもあった。破壊活動は、①他のコンピュータへの無差別な攻撃と改竄（コードレッドと同様）、②アドレス帳に記載されているアドレス宛てのウイルス添付のメールの送付、③共有フォルダーの勝手な公開など。
Blaster（ブラスター）2003年8月発生	ネットワーク感染型	RPCのセキュリティーホールを使って感染するもの。OSのセキュリティーホールが利用されるため、インターネットに接続しているだけで感染する。	クライアントPCを狙って大量に感染を広げた。社員が社内LANに持ち込んだノートパソコンなど、LAN側から感染する例が多かったのも特徴。ファイルに感染せず、メモリー上で活動するため、ファイルのウイルスを検出するだけのソフトでは守れない。また、NachiやWelchiaと呼ばれる亜種では、感染活動のために発生させた大量のネットワークトラフィックが問題となった。





ファイル感染型ウイルスの場合、ウイルスはファイルに含まれているので対策は簡単だ。誰かからメディアやメール経由でもらったり（左図C）、インターネットからダウンロードしたファイルを開いたり、実行したりする前に、ウイルス対策ソフトでウイルスが含まれていないかを調査し、ウイルスが含まれていたならば、その時点でソフトを使って駆除すればいい。ただし、ファイル感染型ウイルスでも、HTMLファイルやHTMLメール内にスクリプトとして含まれる「スクリプトウイルス」は、別の対策が必要だ。スクリプトウイルスの多くは、ウェブブラウザーやメールソフトのセキュリティーホールを悪用し、ユーザーがウェブページを見たり、メールを開いたりするだけで感染することがある（左図E）。このため対策としては、パソコンに常駐してファイルを監視する機構を備えるウイルス対策ソフトを導入し、ウェブブラウザーやメールソフトがHTMLファイルやHTMLメールを開く前に、ウイルスを駆除する仕組みを構築することが不可欠だ。

市販されているウイルス対策ソフトはファイル感染型ウイルスを研究し尽くしていると言っても過言でなく、それらを導入していれば、まずファイル感染型ウイルスが大きな脅威となることはなくなった。ただし、ウイルスは年々新しいものが登場するため、ウイルス対策ソフトのウイルス定義ファイルの更新を怠ると、最新のウイルスが登場したときに、それを発見できずに感染してしまう恐れがある。ウイルス対策ソフトを入れたからといって安心して、ウイルス定義ファイルの更新を怠ると、ウイルス対策ソフトが役にたたないということがあり得るのだ。

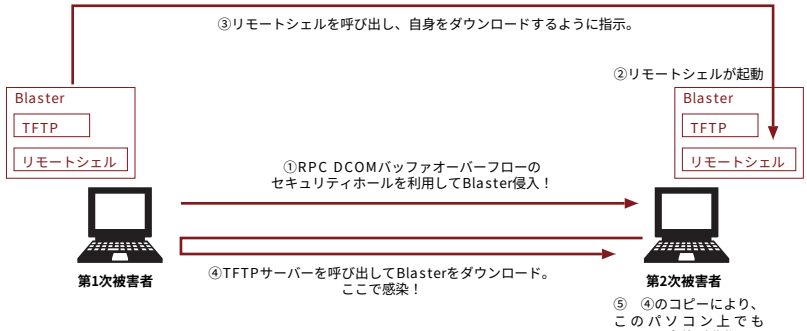
一方、やっかいなのはワームとも呼ばれるネットワーク感染型のウイルスだ。先に大流行したBlasterもネットワーク感染型のウイルスで、左図のように動作するため、ファイル感染型ウイルスの典型例である「メールに変な添付ファイルが付いていたから、それをスキャンして駆除」という、目で見えるような対策方法は採れない。さらにこのウイルスが使うTFTPというプロトコルは、ファイアーウォール機能を持っていないウイルス対策ソフトでは監視できない。つまり、いくらウイルス定義ファイルを最新にしていても、ウイルス対策ソフトだけではBlasterには太刀打ちできないのだ。次ページでは、このタイプのウイルスにどのように対処するかを3段階に分けて解説する。

e l n t e c t i o n

復旧・対策に・・・
770万円の損害

※社員1000人の企業でネットワークの復旧に2日を要した場合（詳細は81ページを参照）

図5　Blasterはネットワーク経由で感染する



Blasterは、RPC DCOMバッファオーバーフローというセキュリティホールを使って実行される。RPC DCOMバッファオーバーフローとは、送信されたデータをそのままプログラムとして実行してしまう危険なセキュリティホール。ウインドウズアップデートを実行すると修復できる。逆に言うと、ウインドウズアップデートを実行しない場合には、いつでも感染する危険性がある。ただし、RPC DCOMバッファオーバーフローは、ウインドウズのファイル共有に使われるTCP 135番が使われるので、ファイアーウォールなどで、このポートを閉じていた場合には、感染しない。

段階1：ファイアーウォールで予防する

ネットワーク感染型のウイルスは、ネットワークを流れるデータにウイルスが仕込まれており、OSのセキュリティーホールを狙って攻撃を仕掛けてくる。このため、何もアプリケーションを実行していなくても、インターネットに接続しているだけで、知らぬ間に感染してしまう。Blasterだけでなく、世間を騒がせたNimdaウイルスも、この種のネットワーク感染型ウイルスだ。

ネットワーク感染型ウイルスはファイルを媒体に感染するわけではないので、ファイルだけをウイルスチェックしているのでは対応できない。さらに、ウイルス対策ソフトの多くが、ネットワーク感染型ウイルスが使うプロトコルなどを監視していないので、まるで役にたたない。

ファイアーウォールと組み合わせ、自分のパソコンとネットワークの間を流れるデータそのものを監視しないと、防ぐことはできないのだ（86ページ上図D）。ファイアーウォールについては90ページから詳しく解説する。

段階2：社内につなぐ前にウイルススキャン

ネットワーク感染型ウイルス対策として重要なことは、ウイルスを社内LANに持ち込まないという配慮だ。多くの企業は、インターネットとの接続点にファイアーウォールやウイルス除去の仕組みを設けており、社内LANは安全に保たれている。

しかし外出先から携帯電話やPHS、無線LANスポットなどでインターネットにアクセスした場合にはどうだろうか。このとき自分のパソコンを守るものは何もなく、ウイルスに感染してしまう恐れがある（86ページ上図A）。感染したパソコンを社内のLANに接続すれば、どんなにインターネットとの接続点を社内LANが守っていても、瞬く間に社内に広がってしまうだろう。外出先、家庭でも社内と同等のセキュリティーシステムを構築し、完全に予防することが望ましい。さらに時間はかかるが、社外のネットワークにつないだ後は、ウイルススキャンをして自分のパソコンが感染していないかチェックするという方法を採るのもいいだろう。

段階3：感染したら隔離してすぐに報告

ウイルスは1台が感染するとどんどん広まるので、早期の発見が被害を最小限に食い止める秘訣だ。そのためには、定期的にハードディスクの全ファイルに対するウイルスチェックが欠かせない。

万一ウイルスに感染していた場合の対処方法も重要だ。感染した自分の失態を責められるのを恐れ、こっそりと自分のパソコンだけからウイルスを除去するのは望ましくない。なぜなら感染がすでに広がっており、ほかのパソコンにも感染してしまっている可能性もあるからだ。

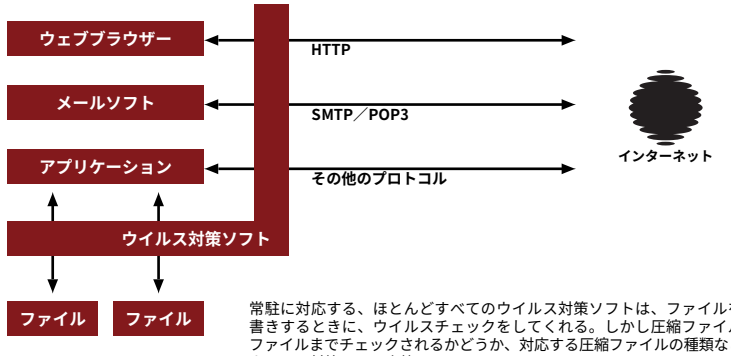
ウイルスの感染に気づいたときには、まず、パソコンからLANケーブルを抜いてLANから隔離し、被害を広げないようにする。そして事態をネットワークの管理者に告げ、社内すべてのパソコンに対して最新のウイルス定義ソフトをダウンロードしたウイルス対策ソフトでウイルスチェックをして、ウイルスをLANから完全に除去する。

自動ウイルススキャンを過信するな！
ウイルス対策ソフトを効率的に運用するポイント

ここからは、実際にウイルス対策ソフトを導入する際に気を付けることを説明していきたい。ウイルス対策ソフトは、先にも説明したとおり、現在見つかっているウイルスの特徴を数値化した「ウイルス定義ファイル」を内蔵しており、それと侵入してきたデータを比較することでウイルスか否かを判断する。ただし既知のウイルスの亜種も発見できるように各ウイルス対策ソフトメーカーは、パターンファイルとの単純な比較ではなく、独自の技術を使っている。そのため発見できるウイルスの種類は、ウイルス対策ソフトによってまちまちだ。右の比較表などを見て、その得意分野を把握してほしい。

図6　ウイルス対策ソフトの仕組み

ネットワークを流れるデータを監視するかどうかは、ウイルス対策ソフトの種類に依存する。ネットワークへの監視をまったくしないウイルス対策ソフトもある。
またネットワークを監視する場合、すべての通信を監視するわけではない。HTTP、SMTP、POP3など、代表的なプロトコルに限られる。



常駐に対応する、ほとんどすべてのウイルス対策ソフトは、ファイルを読み書きするときに、ウイルスチェックをしてくれる。しかし圧縮ファイル内のファイルまでチェックされるかどうか、対応する圧縮ファイルの種類などは、ウイルス対策ソフト次第だ。

ウイルス対策ソフトの基本的な運用は、出入りするすべてのファイルに対して手動でウイルスチェックすることだ。つまり、もらったファイルは開く前にウイルスチェックし、渡すファイルは渡す前にウイルスチェックする。これはメディアに保存して渡す場合も、メールに添付して送受信する場合も同じだ。

近頃のウイルス対策ソフトは、起動時にパソコンに常駐し、常にウイルスの侵入を調べてくれるものも多い。しかしこの機能は過信しないほうがよい。というのは、すべてのパソコン内の動きを監視しているわけではなく、一部の条件を満たしたときにだけ監視するからだ。多くのウイルス対策ソフトは、ファイルを読み書きする場面でウイルスチェックする。しかし圧縮ファイルの中身までチェックしてくれるとは限らない。またいくつかのウイルス対策ソフトは、ウェブやメールなどのデータもチェックする。しかしすべての通信をチェックするわけではなく、メールに関して言えば、POP3はほとんどが対応するが、IMAP4への対応は皆無だ。

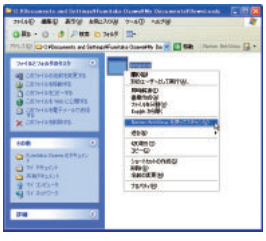
おもなウイルス対策ソフト

		ノートンインターネットセキュリティー2004	ウイルスバスター2004	McAFEE インターネットセキュリティSuper
				
		http://www.symantec.co.jp/	http://www.trendmicro.com/jp/	http://www.sourcenext.info/mcafee/
機能		ウイルス対策、ファイアーウォール、IDS	ウイルス対策、ファイアーウォール、IDS	ウイルス対策、ファイアーウォール
ウイルス対策の機能	動作方式とウイルスの監視対象となるネットワーク	ファイル監視、ネットワーク監視 HTTP、SMTP、POP3、メッセンジャー	ファイル監視、ネットワーク監視 HTTP、POP3、SMTP	ファイル監視のみ —
ファイアーウォールの機能	IPアドレス、ポート単位での通信可否の設定	○	○	△（デフォルトはほとんどのポートが閉じており、設定は、ポートを開けるのみ）
	プログラム単位での通信可否の設定	○	×	○
おもな特徴		ウイルス対策からファイアーウォールまで、ほぼ完璧な機能をもっている。反面、監視するネットワークの通信速度は極端に低下する。ユーザーインターフェイスは複雑で、設定項目も専門用語が多いことから、初心者には向かない。	ネットワーク感染型のウイルスが流行ると、それを防ぐファイアーウォールの設定もウイルス定義ファイルの一部として提供されるので、ほとんど設定なしで利用できる。反面、中上級者が求める、高度なカスタマイズはできない。	ウイルスに関しては、ネットワークを監視しないため、ネットワーク感染型ウイルスについては、ファイアーウォール機能で個別に対応することになる。ネットワークを監視しないので通信速度が大きく低下するようなことはない。

つまり、常駐でのウイルスチェックには、どうしても漏れが生ずるのだ。そのため面倒ではあるが、定期的にハードディスクに保存された全ファイルに対するウイルスチェックを欠かすことができない。全ファイルに対するウイルスチェックは時間がかかるが、感染しそうな拡張子のファイルしか調査しないようにすれば、いくらかチェックに要する時間を短縮できる。そのほか、効率的なウイルススキャンの方法を下で説明しているので、参照してもらいたい。

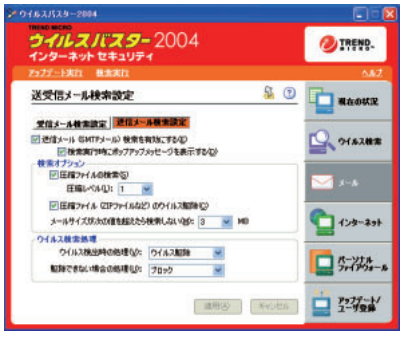
効率的なウイルススキャンを実行する！

ここでは、時間のかかるウイルススキャンを効率的に行う方法とウイルスチェックによって起こるメールの送受信の不具合への対応方法を、代表的なウイルス対策ソフトを例に公開する。ただし、これを行うのは定期的に全ファイルスキャンをしていることが前提だ。

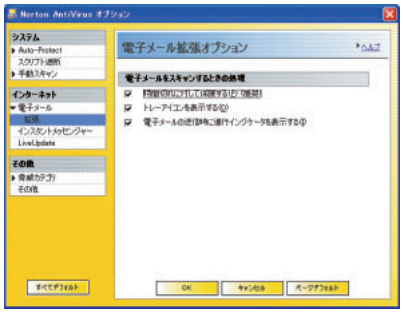


ウイルス対策ソフトをインストールすると、エクスプローラが拡張され、右クリックして簡単にウイルスチェックできるようになるものが多い。誰かからもらったファイル、誰かに渡すファイルに対しては、ウイルスチェックすることを心懸ける。

スキャンにかかる時間を短縮したければ、特定の拡張子をもつファイルだけを調べればいい。ウイルス対策ソフトは感染しそうな拡張子をリスト化してくれる機能をもっているので、これを参考にするといい。また、いくつかのフォルダーを除外するチェックもできる。たとえば、テキストファイルや画像ファイルが大量に保存されていて、ウイルスに感染していないと断言できるフォルダーを除外すると、全体のチェックにかかる時間を大幅に短縮できる。



ウイルスバスターの場合には、送信時などにウイルスチェックするメールのサイズを調整できる。チェックするメールのサイズが大きすぎるとサーバーのタイムアウトが起こり、メールの送信ができない場合がある。このタイムアウトを抑制する機能などを活用しよう。



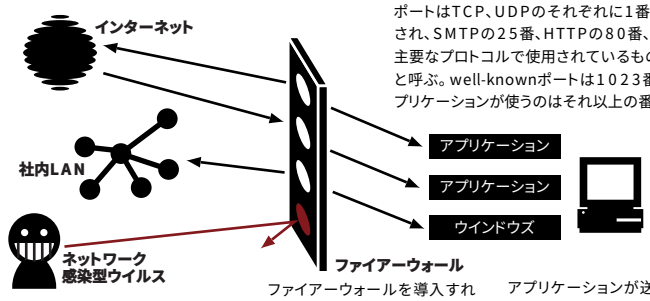
ノートンアンチウイルスの場合には、[時間切れに対して保護する]のチェックで設定する。チェックを付けると、メール送受信時に一定時間ごとにダミーのヘッダーが送信され、ウイルスチェックに時間がかかってもタイムアウトを抑えられる。

会社のファイアーウォールに頼ってはダメ!
パーソナルファイアーウォールで直接的攻撃を防ぐ

インターネットにおいて重要な要素となるのが「ポート」だ。ポートはアプリケーションがデータを送受信する通り道で、アプリケーションは、通信するときに必ずいずれかのポートを用いる。また、ネットワーク型のウイルスもこのポートを用いて、標的となるパソコンにアクセスする。したがって、ウイルスが利用すると思われるポートを閉じれば、ネットワーク感染型のウイルスを抑えられる。これがファイアーウォールの基本的な仕組みで、さらにそれを発展させ、攻撃のデータかどうかを判定して警告し、自動的にポートを閉じてくれるのがIDS(侵入検知システム)だ。つまり、不要なポートは閉じ、不正なアクセスなどが入れないようにして、インターネットからの攻撃を受けないようにするのが、ファイアーウォールの役割なのだ(右図)。

近年ウイルス対策ソフトの多くがファイアーウォール機能を備えている。これは、ウイルス対策ソフトが監視するウェブやメールだけでは、ネットワーク感染型のウイルスの侵入を抑えきれないためだ。ここからは、ウイルス対策ソフトと補完関係にあるファイアーウォールを使ってセキュリティーを高める方法を説明する。

図7　ファイアーウォールの基本的な仕組み



ポートはTCP、UDPのそれぞれに1番～65535番まで用意され、SMTPの25番、HTTPの80番、POP3の110番など、主要なプロトコルで使用されているものをwell-knownポートと呼ぶ。well-knownポートは1023番以下にあり、普通のアプリケーションが使うのはそれ以上の番号のポートとなる。

ネットワーク感染型ウイルスは、アプリケーションやウインドウズのセキュリティーホールをもつポートを狙うので、ポートを閉じれば、ウイルスも阻止できる。

ファイアーウォールを導入すれば、アプリケーションやウインドウズには、安全な場所からのデータしか入らない。そのため、万一セキュリティーホールがあったとしても安心。

アプリケーションが送受信するデータは、必ずポートを通る。そこで、インターネットからのデータ、LANからのデータなど、「どこから来ているデータなのか」、そして、「どこに向かうデータなのか」を調べ、特定のポートでの通信を許可するかどうかを決定する。

対策 3 person

パーソナルファイアーウォールとIDSを導入
Nachiワームが VPNから侵入、

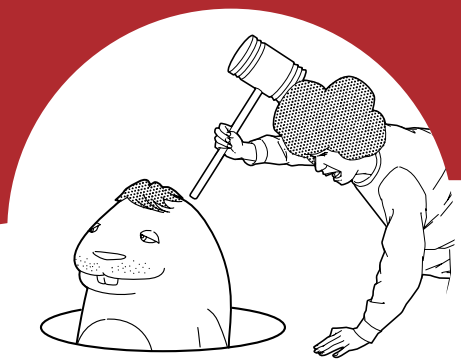
Blasterの亜種として発生したNachi。このウイルスは感染すると大量のパケットをまき散らし、ネットワークを圧迫するというタイプのウイルスだった。このNachiもBlaster同様ウイルス対策ソフト単体では太刀打ちできない。

ただ導入するだけではダメ
正しいポートの開け閉めがパソコンを守る

ファイアーウォールの難しい点は、「どのような通信を許し」「どのような通信を許さないのか」という判断基準だ。

どのような通信を許すのかは環境によって大きく異なる。たとえば、LAN環境ならファイル共有のポートでの通信を許したいだろうが、インターネットに直接つないでいる環境なら、許したくないだろう。つまり利用している場所もファイアーウォールの設定に関わる要素となる。もっとも社内LANや家庭内LANにおいて、ルーターを用いた環境ならば、ルーターでファイアーウォール機能を実現する方法もある。ただし、これではLAN内にVPNなどで侵入してきたウイルスには太刀打ちできない。やはり、個人のパソコンにファイアーウォールソフトを導入するのが、どんな環境であれ安全な方法だ。ちなみに、このようにルーターなどでLAN自体にファイアーウォール機能を実現するものに対して、パソコン自体にファイアーウォールを設定するものをパーソナルファイアーウォールと呼ぶ。

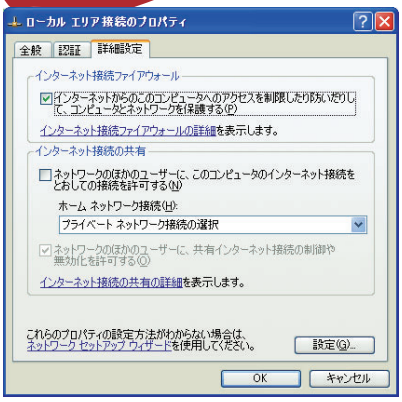
さて、どの通信を許すかという判断基準だが、多くのファイアーウォールソフトはインストールするとパソコンに常駐し、プログラムが通信し始めようとする場面を検知し、通信していいかをユーザーに尋ねる。そのため設定そのものは複雑ではない。プログラムの利用するポートが安全なものであると確認できれば、許可を与えるだけでいいのだ。しかし意味もわからず、メッセージが表示されるたびに通信に許可を与えると、ファイアーウォールにどんどん穴が空き、セキュリティー的に脆くなるので注意したい。安全性と利便性は相反するものなので、安全性重視なら、ウェブ



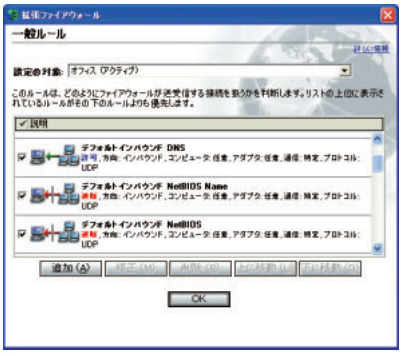
ブラウザーやメールソフトなど、業務に最低限必要なプログラムにだけ許可を与えるのがいいだろう。

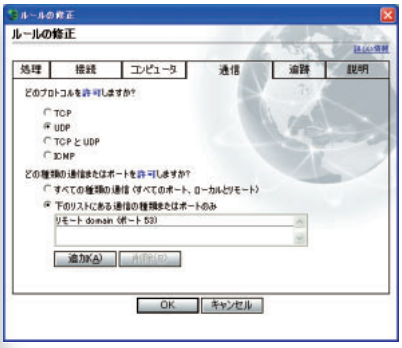
またファイアーウォールソフトでは、LAN内のパソコンなど、ある一定範囲のIPアドレスをもつパソコンと無条件に通信を許すこともできる。この機能を使うと、ポート単位で通信のセキュリティーを設定する煩わしさはなくなる。ただし、その設定をすると、ウイルスのデータにも通信を許してしまい、LANの1台のパソコンがネットワーク感染型のウイルスに感染したとき、そのパソコンからの感染を防ぐことができなくなり、危険性は高まる。よって安全重視なら、面倒でもIPアドレス単位ではなくポート単位で設定すべきだ。

ウィンドウズXPだけでもファイアーウォールは構築できる！



特にソフトを購入しなくても、ウィンドウズXPの簡易的なファイアーウォール機能を使うという手もある。この機能をオンにすると、「インターネット側には通信できるけれども、インターネットからの通信はできない」という構成となる。ファイアーウォールソフトをインストールしないなら、この機能をオンにしておくのが無難。





ファイアーウォールソフト（画面はノートンインターネットセキュリティーでは、上記のようにきめ細かくポートごとの通信の可否を設定できる。

a l F i r e w a l l

ネットワークダウン！・・・
250万円の損害

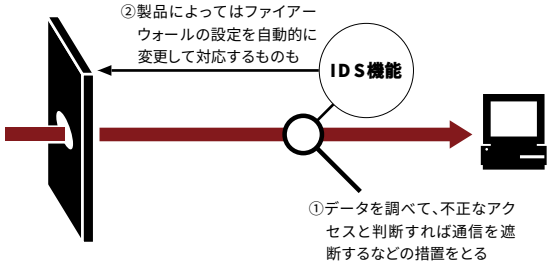
※社員1000人の企業でネットワークが1日停止した場合（詳細は81ページを参照）

ファイアーウォールでも心配なら
IDSでより安全性の高い環境を構築

ファイアーウォールの発展形に当たるのがIDSだ。IDSはネットワークを監視して、不正な一連の攻撃と思わしき通信や壊れたデータの大量の送付などを発見したときに、実際に攻撃が行われる前に、そのIPアドレスをもつ送信者からの通信を一定時間停止したり、ファイアーウォールの設定を変えてそのポートを閉じるといったインテリジェントな働きをするものだ。また、NimdaやBlasterなどの攻撃のパケットを自動除去するものもある。

IDSはおもにサーバーを過負荷な攻撃から守るときに用いるものだが、個人向けファイアーウォールソフトでもIDS機能を統合したものは多い。IDS機能がない場合、ファイアーウォールのポートの設定に従って通過するため、ポート設定を誤ると攻撃データが入ってきてしまう。しかしIDSに対応していれば、既知の攻撃パターンであれば、攻撃とみなして除去するので、より安全度が高い。

図8 IDSの仕組み



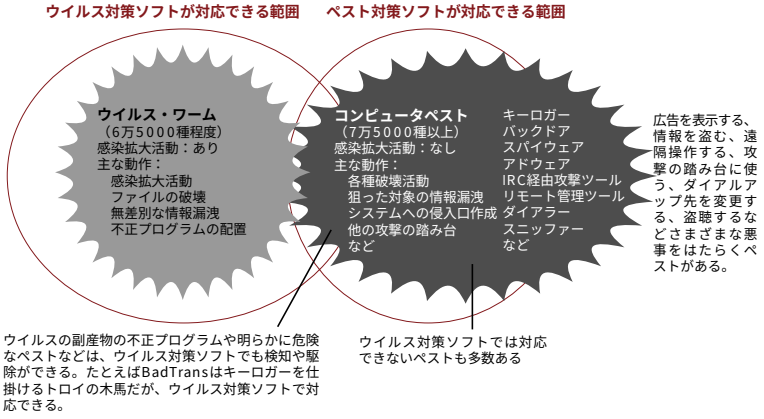
ウイルスとは違う不正プログラム
知らない間に忍び込むコンピュータペスト

ウイルス対策やファイアーウォールでクライアントPCのセキュリティーは万全かと言うと実はそうでもない。最近、ウイルスやワーム以外に個人や企業に実害をもたらす不正プログラム（コンピュータペストやマルウェアとも呼ばれる）の問題がクローズアップされている。個人情報を盗むキーロガーやスパイウェア、不正アクセスの目的で利用されるハッカーツールや攻撃ツールなどの悪質なものも多くある。

たとえば、キーロガーがパソコンに仕込まれると、キーボードの入力が犯人に筒抜けになり、パスワードなどが盗まれて不正アクセスに利用される。バックドアと呼ばれる裏口を設置されると、コンピュータを犯人に自由に使われてしまう。こういったツールが知らない間にパソコンに仕掛けられ、知らない間に他のコンピュータに不正侵入や攻撃をする踏み台として使われて加害者となってしまうこともあるのだ。

これらの不正プログラムが仕込まれている状態で会社のネットワークに接続したら、会社に与える損害は、システムの停止、営業機会の喪失、訴訟問題、信用の失墜など計り知れないものがある。

図9 ウイルス対策ソフトではすべてのペストは防げない



対策 4 Uninui

不正プログラム対策ソフトを導入
バックドアを仕掛けられて踏み台に

ウイルスやワーム以外の悪意をもったプログラムを「コンピュータペスト」と呼ぶ。勝手に広告を表示されるぐらいならばまだいいが、バックドアやキーロガーを仕掛けられると、その先にはウイルスとは比べものにならない大きな損害が待ちかまえている。

感染拡大はないがウイルス対策ソフトでは対処不能なものも
被害範囲は狭いがピンポイントで重大な被害が

ウイルスはプログラムやマクロを含むドキュメントに取り付いて感染を拡大させ、ワームはネットワーク経由で増殖する。一方、ペストは増殖をしない独立したアプリケーションとしてPCにインストールされる場合が多い。正式なプログラムの一部としてインストールされる場合もあるが、悪質なペストの多くはウイルスと同様にメール添付で送られてきたり、ウェブサイトやP2Pファイル交換ソフトで入手したりするプログラムに仕掛けられている。セキュリティーホールを狙って忍び込む場合もある。

ウイルスやワームは個人がいたずら目的で配布する愉快犯的なものが多く、自己増殖する性質上発見が簡単だ。被害数は多いが、重要なファイルを削除されたりばらまかれたりしなければ、実際の被害額は復旧のためにネットワークを止めた費用やその間の営業機会の喪失や作業効率の低下といったものとなる。一方、ペストの目的は、盗聴・不正侵入・攻撃といった実被害だ。その性質上、姿を隠しているものが多いために発見が困難だ。また、一度被害が発覚するとその被害額は多大になることが多い。

ペストの中には通常の使い方をすれば有害ではないものもあることに注意が必要だ。たとえば、離れたところにあるPCを遠隔操作するリモート管理ツールはシステム管理者には必須のツールだが、悪用すれば強力なハッキングツールとなる。

ウイルス・ワームとペストの違い

	ウイルス・ワーム	コンピュータペスト
原産	海外産がほとんど	海外産＋日本産
感染の発覚しやすさ	簡単	困難
被害額×被害数	少額×多数	高額×少数

基本的な防ぎ方や対処法はウイルスと同様
不正プログラムの駆除には専用対策ツールを使う

対策ツールを使わなくてもできる対策として、ペストの侵入経路を絶って侵入を防止する方法がある。ウイルス対策の基本と同様の手法がペストにも適用できるのだ。

コンピュータペストの基本的な防ぎ方

	侵入パターン	防ぎ方
①	ウェブの閲覧時にActiveXやJavaなどのスクリプトを悪用して侵入	ブラウザーのセキュリティー設定を強化する（右図参照）
②	OSやプログラムのセキュリティーホールを悪用して侵入	ウィンドウズアップデートなどのプログラム更新を実施する
③	情報収集を目的としたクッキーとして侵入	定期的にクッキーやウェブ閲覧履歴の整理と削除を実施する
④	HTML形式のメールにスクリプトを忍ばせておいて侵入	メーラーの設定でHTML形式のメール受信とスクリプトの自動実行機能をオフにする
⑤	ウイルスの侵入と同じくメールにプログラム自体を添付して侵入	出所のはっきりしない怪しいメールや添付ファイルは削除し、絶対に開かない
⑥	社員など他人が直接パソコンに仕掛けて侵入（内部犯罪）	パソコンの起動時やスクリーンセーバーのパスワードロックを設定する

ActiveXは必ず情報を確認してから実行

IEの［ツール］メニューから［インターネットオプション］を選び、［セキュリティ］タブで地球アイコンの［インターネット］ゾーンを選ぶ。このレベルを少なくとも「中」にしておこう。また、下図のようなActiveXのセキュリティー警告が表示される場合は安易に「はい」を押さずに内容をよく確認することが大切だ。

t e d S o f t w a r e

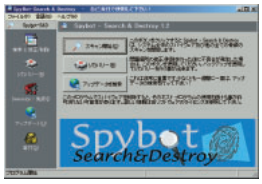
された先で個人情報漏洩・・・
1,600万円の損害賠償

※10万人分の顧客情報流出で20パーセントの過失責任を問われた場合（詳細は81ページを参照）

スパイウェアやキーロガーなどのペストの検出や駆除ができる専用対策ツールを利用することで、ウイルス対策ソフトなどの既存セキュリティー技術の弱点を補完できる。これらのツールはウイルス対策ソフトと同様にファイルをスキャンする形で使う。パターンファイルを更新する必要がある点もウイルス対策ソフトと同様だ。

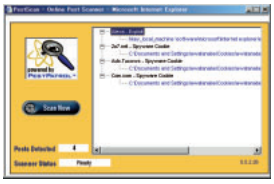
ペストパトロール（PestPatrol）
スパイウェア、キーロガー、ハッカーツール、攻撃ツールなどのコンピュータペストに網羅的に対応している商用ツール。NSTL（National Software Testing Labs）のペスト検出検査では、ノートンアンチウイルス2001によるペストの検出率は45パーセント程度に対し、ペストパトロールでは85パーセントのペストを検出していた。日本語版、8,500円
URL http://www.pestpatrol.jp/

アドアウェア（Ad-aware）
スパイウェア専用の商用ツール。英語版、39.95ドル（スタンダード版は無料）
URL http://www.lavasoftusa.com/



スパイボット（Spybot）
スパイウェア専用のフリーソフト。日本語インターフェイスあり
URL http://security.kolla.de/

アンチキーロガー（Anti Keyloger）
キーロガー専用の商用ツール。英語版、59.95ドル
URL http://www.anti-keyloggers.com/



ペストスキャン（PestScan）
スパイウェア、キーロガー専用の無料のオンラインスキャナー（検出のみ）
URL http://www.pestpatrol.jp/index_pestscan.html

［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