コンピュータウイルスの動向

牧野 二郎●弁護士

検出・届出件数とも過去最高ながら感染率は減少
ボットウイルスなど新しい動きに的確な対策必要

コンピュータウイルスは引き続き次々と発生し、その種類を増加させている。ウイルス届出件数は、2004年の水準を超えて、過去最多件数である5万4,174件になった。とくに、w32/Mytobが出現して70種類もの亜種が作られたことなど目立った動きが見られたが、感染率は徐々に減少し、2004年は1.2%であったものが、2005年にはわずか0.4%にまで減少した。これはメールサーバーへのウイルスソフトの実装による防御や、ユーザーがウイルス対策ソフトを導入する率が高まったことの成果と見ることができる。

ウイルスの動き

届けられたウイルスでは、W32/Netsky、W32/Sober、そしてW32/Mytobが多数届けられている。中でもW32/Soberについては2005年12月だけで1,000万件を越える異常な数が検出されていたが、その後2006年1月に活動を停止するように設定されていたことから、2006年には以前の水準に戻っている。

2005年に届けられたウイルスの種類は171種類、そのうち新しいウイルスは51種類にのぼる。2004年に新しく届けられたウイルスは53種類であることから、毎年新しい種類のウイルスが50種類程度生産、配布されていることになる。新しいウイルスが発見されると、ウイルス対策ソフトが新しいパターンファイルを作り、迅速に対応しているため、効果的に感染を防止している様子がわかる。しかし、新種のウイルスの動きからも、ウイルスの蔓延という事実は明らかであり、引き続きウイルス対策を的確に行う必要性がある。

ボットウイルスの対策

2005年9月に警告が出されたものにボットウイルスがある。これはコンピュータウイルスの一種で、感染すると、そのパソコンを外部からコントロールできるようにしてしまうソフトウエアである。その動作がロボットに似ていることから、「ボット」と呼ばれている。このボットは、感染すると、新しいウイルス対策ソフトのパターンファイルのダウンロードを妨害したり、ウイルス対策ソフト自体を止めてしまったり、予想外の行動を起こすことがあるため、感染に気づくことが困難であり、注意が必要とされている。

感染経路は多様で、感染しやすいとされている。電子メールに添付されて添付ファイルの実行によって感染する場合、ウイルスの埋め込まれたウェブを閲覧することで感染する場合、スパムメールの指定するサイトへ誘導されて感染する場合、不正アクセスされて感染する場合、バックドアから感染する場合、インスタントメッセンジャーサービスを介して感染する場合、PtoPソフトの利用による感染の場合などがある。

感染すると、外部の指令サーバーからの指令を受けて、スパムメールの送信基地となったり、DDoS攻撃のサイトとなったり、ネットワーク上のセキュリティの脆弱なサイトを不正アクセスで感染させたり、同じく脆弱なパソコンの情報を収集したり、スパイ活動をするとされる。外部の指令サーバーを中心に、巨大なネットワークを構成することから「ボットネットワーク」と呼ばれ、かつてのDDoS攻撃のときに利用された「ゾンビ」と同様なものが大量に現れ、かつ連動する危険性が指摘されている。

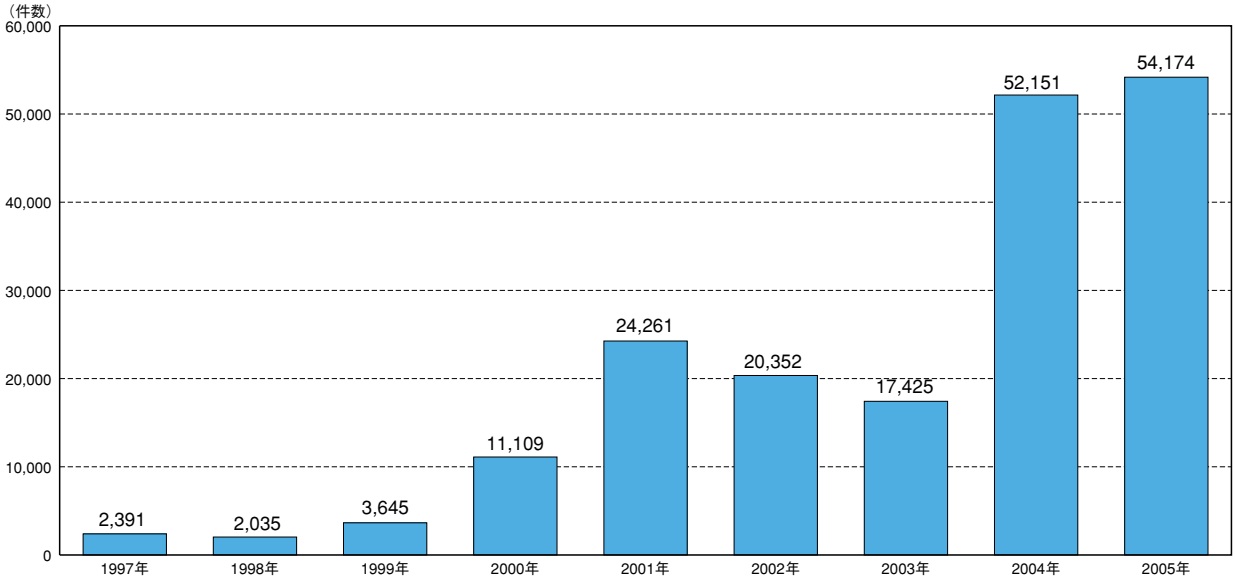
効果的対策としては、コンピュータを最新の状態に維持することである。Windows UpdateまたはMicrosoft Updateを実施することによって最新状態にすることができる。さらにウイルス対策ソフトのパターンファイルを最新のものにすることが必要である。このときウイルス対策ソフトへのアクセスが妨害されたり、ダウンロードができない場合は、すでにボットウイルスに感染している危険があるため、各自のパソコンのHOSTSファイルを調べ、ほかのサイトへ接続するように仕組まれていないかを調査することが必要となる（詳細はIPAの「ボット対策について」(*1) を参照）。

ウイルス対策ソフトの「押し売り」流行

セキュリティ対策ソフト、ウイルス対策ソフトの押し売りが流行しているとのことで、相談件数が急増している。ホームページの閲覧中に「あなたのパソコンは『ブラックウォーム』に関される恐れがあります。ご覧のセキュリティソリューションをダウンロードするのお勧めします」（一部日本語がおかしいがそのまま引用）と表示される。ダウンロードするとパソコンが不具合を起こしたり、クレジット決済をして購入するまで、しつこく購入を促すメッセージを表示し続け

届出件数は昨年同様5万件を突破、感染数は0.4%に抑制

資料6-4-5　コンピュータウイルスの届出状況



出所　IPA「2005年のコンピュータウイルス届出状況」2006年1月【1.届出件数】

ウイルスの届出が昨年同様5万件を突破している。届出される件数は、実際のものとは異なり限定されたものと考えられ、その背後には相当大きなウイルスの蔓延があると考えられる。ただ、これだけの数が発生し、報告されているのに対して、感染事例は0.4%と最小限に抑えられており、ウイルス対策が効果的に進められていると言ってよい。

Netskyが引き続き猛威、年末に急伸したSoberは2006年1月に収束

資料6-4-6　コンピュータウイルスの種別

ウイルス名称	検出数	届出件数
W32/Netsky	30,918,224	12,782
W32/Sober	12,955,209	1,240
W32/Mytob	5,152,918	5,123
W32/Bagle	658,663	4,060
W32/Lovgate	456,343	2,867
W32/Mydoom	390,344	4,149
W32/Zafi	358,266	2,000
W32/Bagz	122,283	1,865
W32/Klez	93,898	2,697
W32/Bugbear	10,325	1,438
その他のウイルス	203,985	15,953
合 計	51,320,458	54,174

（備考：件数には亜種の届出を含む）

2004年に亜種を含めて大量発生したNetskyが引き続き猛威をふるっている。メールに添付されて拡散するものなので、メールの的確な管理によって防止できる。2番目の検出数にあがっているSoberは2006年1月停止の設定となっており、同年2月以降は完全に収束している。全体のウイルス検出件数は5,000万件を超え、引き続き十分な注意が必要である。

出所　IPA「2005年のコンピュータウイルス届出状況」2006年1月【2.届出ウイルス】

るため、やむなく購入するケースが急増している。

　不正な表示が続く場合には、不正なソフトウェアが入っている危険もあるので、オンラインスキャンサービスを利用してスパイウェアの検出、駆除をする必要がある。

（*1）IPA「ボット対策について」
http://www.ipa.go.jp/security/antivirus/bot.html

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2012年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

http://IWParchives.jp/

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、データ、URL、名称など）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・図の作成者、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掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したり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される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期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。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp