コンピュータウイルスの動向

鈴木 直美●フリーライター

愉快犯型が減少、金銭詐取を目的とするウイルスが主流に
ゼロデイ攻撃急増、ボット蔓延、Winny情報流出も深刻化

コンピュータウイルス（トロイの木馬やワーム、スパイウェアなども含む）もまた、以前のような愉快犯から金銭目当ての犯罪へとシフトした。ひたすら感染を広げることに喜びを覚えたり、派手な演出や破壊活動で話題になることを目的とした趣味的なものは少なくなり、パスワードを盗み取ったり、システムを乗っ取ったりなどの実益本位のウイルスが幅をきかせている。

目的の変化に伴い、ウイルスは密かに侵入し静かに活動するようになり、脆弱性を突いて知らない間に感染させる手法や、利用者の心理を突いて感染させるソーシャルエンジニアリング的な手法が積極的に使われるようになった。セキュリティソフトの検出を逃れるために、次々と形を変えた亜種が登場し、身を隠すためにルートキットが使われるなど、セキュリティソフトとのいたちごっこが続く。不特定多数に感染を広げるのではなく、特定の相手を狙う標的型（スピア型）の攻撃が増えているのも特徴だ。メールなどを使って急速に拡散するウイルスと異なり、ベンダーが検体を入手するのに時間がかかるため、対策が後手にまわるケースが目立った。

ゼロデイ攻撃急増

年末に見つかったWMF（Windows MetaFile）の脆弱性が未修正のまま迎えた2006年は、マイクロソフト製品の未パッチの脆弱性を狙う、いわゆるゼロデイ攻撃が多発した。OSやブラウザーなどのソフトウェアの脆弱性は、利用者に気付かれずにプログラムを実行する格好の標的であり、サイトを閲覧するだけで感染するといった深刻な事態を招く。2006年は、とくにWordやExcelなどのアプリケーションを狙ったゼロデイ攻撃が多く、5月のWordを皮切りに、Microsoft Office製品だけでも年末までに9件の脆弱性が未修正のまま悪用された。国産のワープロソフト一太郎もその洗礼を受け、2件のゼロデイ攻撃が発生している。この傾向は2007年に入ってからも続くが、Office系アプリケーションの場合には、特定の機関などを標的としたスピア型の攻撃が多い。

ボットの蔓延が深刻化

PCの遠隔操作を目的に仕掛けられるウイルスの一種、ボットの蔓延が深刻化し、総務省と経産省は共同でボット対策プロジェクトを始動した。ボットは、感染しても即座に表立った活動はせず、外部からの指示を受けてスパムの配信やサイトへの攻撃、情報漏えいなどのさまざまな活動を行う。このため感染に気付きにくく、ひとたび活動を始めると大きな被害をもたらす結果となる。セキュリティ企業の報告では、1時間200～300ドルでボットネットがレンタルされているといい、新たなサイバー犯罪の脅威となっている。プロジェクトの事前調査では、国内だけで40～50万台のPCが感染しているとみられ、12月にポータルサイト「サイバークリーンセンター」を開設し、無料の駆除ツールの配布などを始めた。同プロジェクトが意図的に攻撃を受けさせることを目的に、ネット上に設置したおとりPC「ハニーポット」は、翌3月末までに3万1082種、のべ97万4999個のボットを収集した。

エンドユーザー狙う押し売りソフト

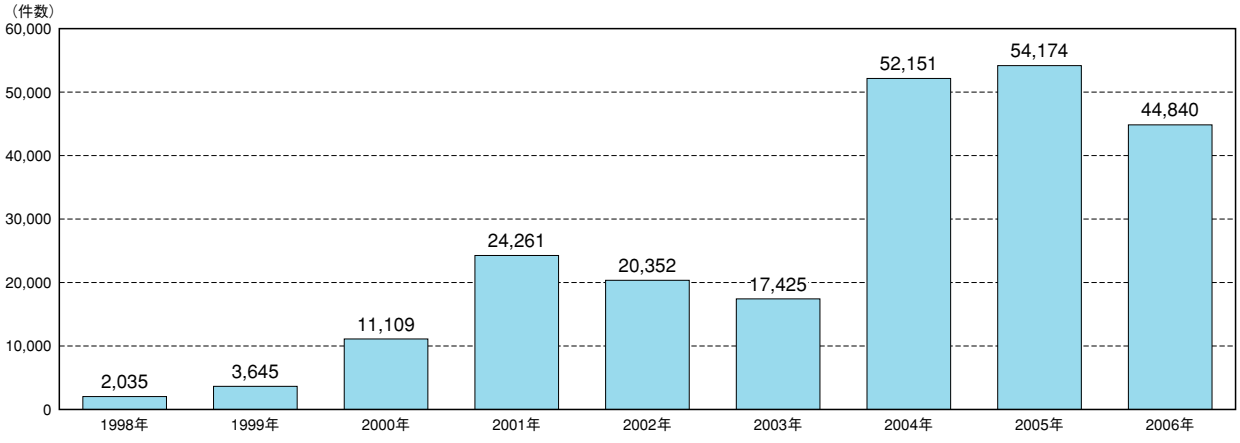
「エラーが検出されました」「スパイウェアが見つかった」などといって利用者の不安をあおって購入させようとする、詐欺的セキュリティソフトの被害が春ごろから急増した。海外では前年秋から大流行していたもので、日本語版の登場とともに国内にも波及。秋には同様の詐欺的セキュリティソフトの日本語版が次々に登場し、掲示板やブログ、著名なサイトの広告などを使って誘導。国内でも被害者が続出した。海外では、実際にウイルスを仕込んだ上で対策ソフトを売りつけたり、PC内のファイルを勝手に暗号化し、復号化ソフトや解除キーを売りつけようとする手口も報告されており、エンドユーザーから直接現金を巻き上げる詐欺・恐喝ソフトには、引き続き警戒が必要だ。

止まらないWinny情報流出

暴露型ウイルスに感染したPCから、WinnyなどのP2Pソフトを介して情報が流出する事故が多数発覚した。2006年に公表・報道されたものだけでも、3月の49件をピークに1年間で220件。うち190件が個人情報を含んでおり、年間に公表・報道された個人情報流出事故の約1割を占める深刻な事態となった。P2Pソフトは、もっぱら音楽ファイルなど

届出は減少するも蔓延の状況は変わらず

資料6-4-5　コンピュータウイルスの届出件数の推移



IPA「2006 年のコンピュータウイルス届出状況」2007年1月【1.届出件数】

ウイルスの届出は、前年の5万4174件から4万4840件へと減少に転ずるものの、2004年に次ぐ3番目の届け出件数を記録。実害のあった感染数は年々減少の方向にあり、前年の0.4%から0.2%となった。届出ベースのデータからは、メールサーバなどに導入されたウイルス対策ソフトが、既知のウイルスを大量にブロックした結果が主に報告されている様子がうかがえる。ちなみにIPAが企業と自治体を対象に毎年実施している実態調査（前年の2005年版）では、有効回答1683件中、769件が年間にウイルスに遭遇した経験があると答え、うち260件、のべ2834台が実際に感染したとある。

新旧マスメーリング型ワームが猛威ふるう、新型は次々と亜種が登場

資料6-4-6　届出ウイルスの種別

ウイルス名称	検出数	届出件数
W32/Netsky	15,229,481	10,664
W32/Mytob	1,884,064	4,405
W32/Sober	1,654,680	583
W32/Bagle	782,044	4,012
W32/Stration	659,969	1,484
W32/Looked	598,458	114
W32/Mywife	477,414	2,633
W32/Mydoom	274,227	3,081
W32/Nuwar	173,888	5
W32/Lovgate	130,471	1,742
その他のウイルス	353,438	16,117
合計	22,218,134	44,840

（備考：件数には亜種の届出を含む）

IPA「2006 年のコンピュータウイルス届出状況」2007年1月【2.届出ウイルス】

大量のメールを送信して感染を広げるマスメーリング型のワームは、その性格から、わずかでも感染者がいれば大量に検出される。検出数こそ激減したものの、2004年に登場したNetskyやBagle、2005年に登場したMytob、Soberといった古参たちが、2006年も上位を占める結果となった。Strationは2006年の夏に、Nuwarは年末に登場したマスメーリング型の新種。ウイルス対策ソフトの検出をかいくぐるように、亜種が次々と送り出されたため、実際に感染した被害者は相当数にのぼる。Lookedも2006年の新種だが、こちらはネットワーク共有を介して感染を広げるとともに、プログラムファイルに自身を埋め込む本来の意味でのウイルスの機能をもつ。ファイル感染型は、自身を隠すのにも有効なため、復調の兆しがある。

の無断配信に利用されており、利用者が自ら信頼できないファイルを開いてしまうため感染は後を絶たず、2007年に入ってからも月10件前後のペースで公表・報道が続いている。もちろん、公表された事故は氷山の一角に過ぎず、未公表の深刻な流出事故はこの数倍、軽微なものを含むと十数倍の流出事故が起きているのが現状だ。

［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