コンピューターウイルスの動向

鈴木 直美 ●フリーライター

改ざんサイトでの感染や脆弱性修正直後に狙われるケースも多発
オートラン悪用ウイルスまん延、感染経路も「外部媒体」急増

コンピューターウイルス（トロイの木馬やワーム、スパイウェアなども含む）は、かつてのような愉快犯的なものはすっかり影を潜め、パスワードを盗み取ったり、システムを乗っ取ってボット化するなど、もっぱら犯罪行為の手段のひとつとして使われるようになった。感染経路は、かつて主流だったメールから、ウェブやUSBメモリーなどのリムーバブルメディアへと広がりを見せ、改ざんされた正規サイトでの感染や、USBメモリーを介したオフィス内のPCへの感染といった、これまでの常識が通用しない盲点を突く手口が流行。バイナリを短期間で次々に更新し、ウイルス対策ソフトの検出を逃れるという手法も用いられるようになった。コンピューターウイルスの脅威に、収束の気配は見えない。

SQLインジェクションによる正規サイト改ざん多発

ウェブアプリケーションの脆弱性を突き、データベースを不正に操作するSQLインジェクション攻撃が、これまでにない規模で展開され、国内のサイトが次々に改ざんされた。その大半は、攻撃サイトに置いたスクリプトを閲覧者に実行させ、ウイルスに感染させようとするもの。同様の手口は、2007年の下半期にも多数報告されたが、2008年3月から年末まで幾度となく繰り返された攻撃の規模は、前年の比ではなく、企業や自治体、公的機関のサイトから個人サイトに至るまで、脆弱性を持つ国内のサイトが次々と改ざんされていった。

すでに前年から使われていた攻撃ツールに加えて、この年には攻撃コードを実装したボットネットも登場。脆弱性を放置しているサイトに対し、完全に自動化された無差別攻撃が展開され、一夜のうちに訪問者に危害を加えるサイトに豹変するという事態を招いた。

脆弱性の修正直後に狙われるケースも多発

ソフトウェアの脆弱性が未修整のまま悪用されるゼロデイ攻撃は、前年に引き続き減少したものの、Internet ExplorerやAdobe Reader、Word、Excel、一太郎などに対する攻撃が発生した。また、修正された脆弱性が修正直後から狙われるケースも多発しており、ブラウザとブラウザ経由で直接制御可能なコンポーネントの脆弱性問題は、2008年の大きな脅威となった。

コード実行の脆弱性は、サイトに誘導するだけで悪質なプログラムを自動実行できるため、攻撃者の格好のターゲットになっている。先のサイト改ざんでも、ブラウザーのコンポーネントとして動作するFlashPlayerやAdobe Readerなどの人気の高いソフトウェアの脆弱性がもっぱら悪用されており、7月には同じくコンポーネントとして動作するSnapshot Viewerの脆弱性が、12月にはブラウザー本体であるIE 7の脆弱性が、修正パッチの提供前に悪用。改ざんサイトの誘導先に攻撃コードが仕掛けられるという、深刻な事態になった。

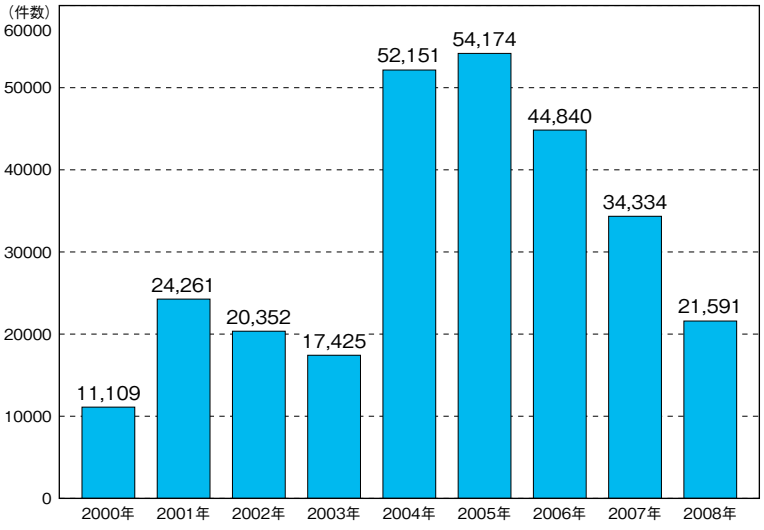
オートランを悪用するウイルスまん延

CDなどの自動演奏の実現やアプリケーションのインストールをわかりやすくするために、Windowsにはメディア挿入時などに決められた処理を自動実行するオートランと呼ばれる機能が搭載されている。オートランは、USBメモリーなどのリムーバブルメディア全般に対しても機能するため、これを感染手段として悪用するウイルスが多数登場。中には、USB製品の製造過程で感染パソコンを使用したために、製品にウイルスが混入してしまったケースや、店頭に置かれたデジタルカメラのプリント受付機が感染したケースも報告された。

IPA（独立行政法人情報処理推進機構）が全国1万の企業と千の自治体を対象に行ったアンケート調査では、2002年をピークとして横ばいから減少を続けていたウイルス遭遇・感染率が、2008年には2.7ポイント上昇し60.9%となった。遭遇・感染したウイルスは、オートランを悪用する「W32/Autorun」が39.8%と最も多く、想定される感染経路も「外部媒体、持ち込みクライアント」が急増。企業は13.8ポイント上昇の37.4%、自治体は35.7ポイント上昇の59.6%と、いずれも最多を占めており、全体で4割を超える感染経路となった。

ウイルスの届出数、感染数ともに減少

資料6-2-5　コンピューターウイルスの届出件数の推移



ウイルスの届出は、前年の3万4334件から2万1591件へと大幅に減少した。届出されたウイルスは136種類（前年166種類）、検出数は273万4604件（前年714万1379件）、実害のあった感染数は70件（前年80件）と、いずれも減少している。これらは届出によるものであり、実際の状況を類推できるような数値ではないが、トレンドマイクロが発表した2008年のデータでも、日本国内での感染被害の総報告数は、前年の6万3726件から5万6880件と約1割の減少を示している。

出所　IPA「2008年のコンピュータウイルス届出状況」2009年1月
http://www.ipa.go.jp/security/txt/2009/documents/2008all-vir.pdf

USBメモリーウイルス「Autorun」が猛威をふるう

資料6-2-6　届出ウイルスの種別

ウイルス名称	検出数	届出件数
W32/Netsky	2,331,291	4,867
W32/Autorun	190,248	1,223
W32/Mytob	58,081	1,704
W32/Mydoom	30,349	1,882
W32/Mywife	26,322	1,001
W32/Virut	17,329	1,222
W32/Mimai	12,467	499
W32/Klez	10,718	1,262
W32/Zafi	9,743	438
W32/Bagle	9,615	1,778
その他のウイルス	38,441	5,715
合計	2,734,604	21,591

NetskyやMytobといった、古参のマスメーリング型ウイルスが依然上位を占めているが、2008年9月に新たに登場したAutorunが10～11月に大量に検出され、両者の間に食い込む結果となった。Autorunは、俗にUSBメモリーウイルスなどと呼ばれている、リムーバブルメディアを介して感染を広げるタイプのワーム。ただし、実際に感染（発見）経路をリムーバブルメディアとする届出は極めて少なく、メールによって大量にばらまかれたものがカウントされた結果だ。

出所　IPA「2008年コンピュータウイルスの届出状況」2009年1月
http://www.ipa.go.jp/security/txt/2009/documents/2008all-vir.pdf

ファイル共有ソフトを介した情報流出は減少

ウイルス感染による「Winny」や「Share」などのファイル共有ソフトを介した情報流出は、前年から大きく減少し、公表・報道された数は44.6%減の87件。流出した個人情報は73.9%減の22万人となった。IPAのアンケート調査でも、被害経験のあった企業・自治体は前年の2.2%から1.4%に減少しており、ファイル共有ソフトを使用するリスクの認知や対策が、ある程度進んだものとみられる。そんな中にあっても、夏には神奈川県のシステム開発を受託した孫請け会社の社員がウイルスに感染し、県下の公立高生11万人全員の個人情報が流出するという大規模な流出事故も発生。この事案では、流出情報の取得者が取得ファイルを故意に流す「再放流」の問題も浮き彫りになった。

参考文献
・IPA「2008年 国内における情報セキュリティ事象被害状況調査-報告書-」2009年5月
http://www.ipa.go.jp/security/fy 20 /reports/isec-survey/documents/2008 _isec_domestic.pdf

［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