コンピュータウイルス❷

猛威をふるうメール悪用タイプ デマメール添付ファイルは特に注意が必要

昨年の情報処理振興事業協会（IPA）によるコンピュータウイルスの届け出件数の推移を左ページに示した（資料3-3-9）。これは日本国内だけの数値であるが、2000年から急激に届け出数が増えていることがわかる。2001年は2か月間だけの数値なので、かなりの急増加といえよう。原因としては次の要因が考えられる。

（1）2000年2月頃の省庁ウェブページの改竄事件が一般新聞や週刊誌をにぎわし、インターネットに対する認識が広く普及した。

（2）このところラブレターなどのウイルスが猛威をふるっているので、一般の関心も高まってきた。

この届け出件数の数値は氷山の一角と見た方がよく、届け出られていないもの、感染に気がついていない場合も相当数にのぼると想像される。

ウイルスの種類

コンピュータウイルスの定義は、IPAのコンピュータウイルス対策基準によれば、「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムで、自己伝染機能、潜伏機能、発病機能の内1つ以上を有するもの」となっている。

コンピュータウィルスを性質によって分類すると、次のように整理できる。

・ブートセクター感染型ウイルス

OS立ち上げの時に必ず実行されるブートプログラムがある場所にウイルスデータが書き込まれる。OSの再インストールでは修復できない場合もある。

・ファイル感染型ウイルス

OSやプログラムなどにウイルスが仕込まれている。プログラムを実行すると発症する。

・マクロ感染型ウイルス

WordやExcelなどのアプリケーションのマクロ機能を利用して仕掛けられる。データファイルを開くとアプリケーションプログラムを通してパソコンに感染し、他のデータにも伝染していく。

・トロイの木馬型ウイルス（ワーム、爆弾など）

当該プログラムを実行することにより、何がしかの望ましくない動作をするプログラムで、一般的には伝染しない。実行結果として、ファイルを消したり漏洩させたりなどの被害があるが、ワクチンソフトでは対象外としている場合が多い。

・メール機能を悪用して感染するウイルス

最近急増しており、さまざまなタイプがある。主に添付ファイルが伝染経路になっているが、HTML形式の本文部分に感染している場合もある。テキスト形式の本文に感染することはない。添付ファイルはむやみにクリックしてはいけない。このほかに、ウイルスではないが、「デマメール」と呼ばれるものがある。

重要 警告

もし、"JOIN THE CREW"というタイトルのe-mailを受け取ったら、絶対に開かないで下さい。～略～この文書をできるだけ多くの人に送ってください。…

これはスパムに相当するデマメールだが、定期的に現れる傾向がある。このようなメールの添付ファイルは、とくに注意が必要である。

メールを悪用するウイルス

このところ特に急増しているのが、メールを悪用するタイプであり、最近のIPA届け出数の90%近くを占めている。かつてはフロッピーディスクなどによって感染経路が物理的に特定できていたが、メールを悪用されると知らない間に感染してしまうことも多い。特に添付ファイルは厳重な注意が必要である。

ウイルスを防ぐ手立て

ウイルスを防ぐには、大きく分けて2つの段階がある。

（1）メールサーバーなどで、通過するパケットデータを見て、ウイルスチェックと駆除を行う。

（2）個々のパソコン上のファイルがウイルスに感染していないかチェックし、感染していれば駆除する。

いくつかのワクチンメーカーがあるが、一番重要なのは、ウイルスを発見するためのパターン情報を常に最新にしておくことである。これが実現されなければ、ワクチン効果はゼロに等しくなってしまう。

感染したら最初にすべきこと

ウイルスに感染したことがわかったら、最初にすることは、そのパソコンをネットワークから切り離すことである。電源を入れても立ち上がらなくなっている可能性があるので、先に電源を切ってはいけない。下記などへ速やかに連絡をして欲しい。

・IPAセキュリティセンター

・コンピュータ緊急対応センター

また、感染したパソコンは、何が起こったか把握できていない限り、基本的には再利用しないと考えるのが無難である。

（安田直義　株式会社ディアイティ）

情報処理振興事業協会（IPA）
www.ipa.go.jp

Jump 02 コンピュータウイルス対策基準
www.ipa.go.jp/security/antivirus/kijun952.html

IPAセキュリティセンター
www.ipa.go.jp/security/

コンピュータ緊急対応センター（JPCERT/CC）
www.jpcert.or.jp

［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