コンピュータウイルス被害報告

総合情報処理センター　小　倉　広　実

ogura@cc. hirosaki-u. ac. jp

センターの３実習室、附属図書館、人文学部、教育学部、医学部、農学生命科学部各１室のサテライト端末室に配置された441台のパソコンで2001年９月から2002年２月までの半年間に情報処理センターのパソコンで検出したウイルスは以下の表の通りである。

ウイルス名	9	10	11	12	1	2	合計
Exploit-MIME					1		1
Exploit-Nocnoc				5			5
JS/Exploit					10	23	33
JS/IEStart	1	28	26	216	166	87	524
JS/IEStart. gen. c					13		13
JS/IllWill			1	7	4		12
JS/Kak@M	2						2
JS/Seeker. gen. e			84	16	19	29	148
JS/Seeker. gen. f			5		15		20
JS/Seeker. gen. h			10	8		12	30
JS/Seeker. gen. m				13			13
JS/Seeker. gen. o			21			5	26
JS/Seeker. i			19				19
JS/Seeker. p						5	5
JS/Seeker. t						1	1
JS/Winbomb						1	1
New AOL		1					1
New BackDoor		2					2
New Win32		5			3		8
PWS-gen. Hooker				18			18
SNIFFER. EXE	2						2
Spam/AnonMail	1						1
SunOS/BoxPoison. defaced					3		3
Univ/f						1	1
Unsafe JS		2	6				8
VBS/Haptime			1	3			4
VBS/Haptime. a@MM			4		2		6
VBS/Haptime@MM	2	2	10		1		15
VBS/LoveLetter@MM		3	2				5
W32/BleBla. b@MM	2						2
W32/Hybris. gen@MM		22					22
W32/Myparty. a@MM					1		1
W32/Nimda. eml					1		1
W32/Nimda. gen@MM					4		4
W32/Nimda. htm		4	49	3	18	3	77
W32/SirCam. gen@MM	4	7					11
W32/SirCam@MM		2					2
W32/Ska@M			7				7
合　　計	14	78	245	289	261	167	1054

個々のウイルスの情報は、http://www. nai. com/japanで確認できる。

この半年間で検出されたウイルス数は1054で、昨年３月から８月までの半年に検出されたウイルスの数541（HIROIN No.17）のほぼ２倍になっている。これはメールの添付ファイルを開いて感染するウイルスだけではなく、Webブラウザ（Internet Exploler等）のセキュリティホールを悪用してページを閲覧しただけで感染するようなウイルスも登場してきていることも影響しているものと考えられる。このことから、情報処理振興事業協会（http://www.ipa.go.jp）では、「パソコンユーザのためのウイルス対策７箇条」を改定してセキュリティに関しても注意を促している。

１．最新のウイルス定義ファイルに更新しワクチンソフトを活用すること
　ワクチンソフトがインストールされていても定義ファイルが古いと新しいウイルスを検出できない。定義ファイルは週に1度は更新する。特に感染力のあるウイルスが見つかった場合は、ワクチンソフトのメーカのwebページをチェックし、対応している定義ファイルに更新する。

２．メールの添付ファイルは、開く前にウイルス検査を行うこと

３．ダウンロードしたファイルは、使用する前にウイルス検査を行うこと

４．アプリケーションのセキュリティ機能を活用すること
　［コントロールパネル］−［インターネットオプション］−［セキュリティ］−［レベルのカスタマイズ］で「中」以上にする。

５．セキュリティパッチをあてること
　Windows Update（HIROIN No.15）を必ず行うこと。

６．ウイルス感染の兆候を見逃さないこと
①　システムやアプリケーションが頻繁にハングアップする。システムが起動しない。
②　ファイルが無くなる。見知らぬファイルが作成されている。
③　タスクバーなどに妙なアイコンができる。
④　ウイルス添付されたメールに対する苦情メールが届いた。
⑤　直感的にいつもと何かが違うと感じる。
　どれかひとつでも当てはまればウイルス感染の可能性があるので、速やかにネットワークケーブルをパソコンからはずし（ネットワークを介して他のパソコン等に被害を拡大させないため）ウイルス検査を行う。

７．ウイルス感染被害からの復旧のためデータのバックアップを行うこと
　ウイルスにより破壊されたデータは、ワクチンソフトで修復することはできない。ウイルス感染被害からの復旧のため、日頃からデータのバックアップをとる習慣をつけておく。