技術ノート

コンピュータウイルスの傾向と当所電算システムにおける対策

北原　枢*　土屋敏夫*　能條自大*　大畑敏美*

The tendency towards computer viruses and virus protection in TIRI-network.

Kaname KITAHARA, Toshio TSUCHIYA, Yorio NOJO and Toshimi OOHATA

１．はじめに

現在はブロードバンド時代といわれ，インターネットは短期間のうちに以前と比べ物にならないほど普及している。都立産業技術研究所も平成 8 年度より学術研究ネットワーク SINET に接続し，東京都所属の研究機関向けに試験研究機関等共同利用電算システム（以下，当所電算システム）を運営し，ネットワークの活用を推進している。

しかしながら，ネットワークの普及とともにそれを悪用したコンピュータウイルスも絶え間なく登場しており，利用には注意が必要である。

ここでは，当所電算システムでのウイルス対策を紹介し，昨今のコンピュータウイルスの状況と当所電算システムでの検出状況について考察する。

２．当所電算システムでのウイルス対策

当所電算システムには約 300 台のパーソナルコンピュータが接続され，Web 閲覧，メール，ファイル共有サービス等を提供している。

平成 12 年度よりインターネットとの接続口にトレンドマイクロ株式会社の InterScan VirusWall を設置し Web 経由及び当所電算システム発行メールアカウントによる送受信についてウイルスチェックをしている。システム内の各端末にはウイルスバスターコーポレートエディションを導入した。ウイルスパターンファイルについては自動更新を行っている。

これ以外にシステム更新後に各研究室等で購入し，システムへの接続申請のあったものについては，端末側のワクチンソフトは特に義務付けられていない状態で，利用者各自の対応と InterScan VirusWall によるネットワーク経由のチェックのみであった。

３．コンピュータウイルスの状況

3.1　近年のコンピュータウイルスの状況

コンピュータウイルスは感染・発症法の特徴等によっていくつかに分類される。近年のコンピュータウイルスは増殖にネットワーク，特にメール機能を利用するものが多くなっている。情報処理振興事業協会[1]への届出は表１のようなものになっている。セキュリティホール悪用ウイルスもメール機能を利用しており，全体の 94%がメール機能を有していることになる。

表１　ウイルスの種類　（2002 年は 1～6 月）

ウイルスの種類	1999 年		2000 年		2001 年		2002 年	
セキュリティホール悪用ウイルス	0 件	0 %	507 件	4.6 %	6338 件	26.1 %	8604 件	74.3 %
メール悪用ウイルス	1138 件	30.9 %	6629 件	60.2 %	14263 件	58.8 %	2326 件	20.1 %
マクロウイルス	2013 件	54.8 %	3393 件	30.5 %	2812 件	11.6 %	480 件	4.1 %
その他のウイルス	524 件	14.2 %	528 件	4.7 %	848 件	3.5 %	159 件	1.5 %
全体合計	3675 件		11120 件		24261 件		11569 件	

特にセキュリティホール悪用ウイルスについてはメール機能に加え，2001 年にマイクロソフト セキュリティ情報 MS01-020[2]として発表された問題を利用しており「見ただけで発症」という現象を引起し，他のものより感染力が強い傾向にある。

3.2　所内での傾向（2002 年前半）

InterScan VirusWall 及びウイルスバスターコーポレートエディションによる検出結果（表２）を見ると所内においてもメール経由でのコンピュータウイルスの検出が圧倒的に多い。

当所電算システムでは外部 POP サーバアクセスを禁止していなかったため，InterScan VirusWall を経由せず端末にメールが到着してから端末側ウイルスバスターで検出されるという状況も存在していた。セキュリティホール悪用ウイルスの持つ危険性を考え，2002 年 6 月に外部 POP サーバへのアクセスをファイアウォールで禁

*情報システム技術グループ

止した。外部 POP サーバへのアクセスについてはそれほど利用されていなかったが，全端末にワクチンソフトが導入されていない状態であったため以前から問題視されていた。

表２　所内での検出数（2002 年前半）

ウイルスの種類	１月	２月	３月	４月	５月	６月
セキュリティホール悪用ウイルス	57 件	12 件	4 件	74 件	111 件	60 件
メール悪用ウイルス	42 件	22 件	14 件	4 件	1 件	1 件
マクロウイルス	2 件	0 件	0 件	0 件	1 件	2 件
その他のウイルス	6 件	14 件	22 件	10 件	11 件	1 件
全体合計	107 件	48 件	40 件	88 件	124 件	64 件

平成 12 年度システム更新時においては，ウイルス対策もしっかりしていたと考えられるが，ワクチンソフト未導入端末数の増加により，全体として安全度は下がりつつあった。

４．　考察

4.1　W32/Frethem の出現と感染

2002 年 7 月 15 日に広まった W32/Frethem については，InterScan VirusWall のウイルスパターンは間に合わず，メールを経由して当所電算システム内に入った。添付ファイルが開かれることで発症・増殖活動を開始し，修正プログラムが適用されていない端末にも送られ，「見ただけ発症」も起きてしまった。13 台の端末において発症，外部の方にもご迷惑をおかけすることとなった。

感染力が強いコンピュータウイルスについてはワクチンソフトも必ずしも有効でないことが見せ付けられた形となり，緊急時体制の確認と見直しが現在実施されている。セキュリティホールをふさぐ修正プログラムの適用，ワクチンソフトの導入の義務付け等が行われた。

4.2　コンピュータウイルス対策の課題

セキュリティホール悪用ウイルスが利用する MS01-020 の問題が公になったのは 2001 年 3 月末である。その後，これを利用したコンピュータウイルスは後を絶たない。このセキュリティホールは，Microsoft® Internet Explorer に関する動作上の問題で「意図せずプログラムが実行されてしまうことがある」というものである。これにメール機能を加えネットワークを巧妙に利用し，感染力の強いコンピュータウイルスとなっているのである。このような感染力が強いコンピュータウイルスの登場においては，ワクチンソフトの導入はもちろんだが，それをもって安全とは言えない状況にある。なぜならウイルスパターンの作成・配布が間に合わない可能性があるからである。これに対応してゆくためには

・セキュリティホールは確実にふさぎシステム上の安全性を確保する
・利用する際に未確認のファイルを取り扱う場合は注意する

ということが必要である。2001 年後半にセキュリティホール悪用ウイルスが猛威を振るった時期に所内向けにセキュリティホールをふさぐ修正プログラムの適用の案内を出した。しかし，今年度に入っても未適用のものが確認されていた。世間一般では，そのセキュリティホールの存在すら知らずに利用している方々もいると考えられる。今後のシステム管理は，利用者のセキュリティに関する啓蒙もしていかなければ全体の安全は確保できない。利用者側の意識向上も切に望まれる。安全確保・利用者意識向上のためにはシステム側での利用制限等の積極的な対応を考えていかねばならない。

５．むすび

当所電算システムでの W32/Frethem の感染・発症・増殖までの過程を調査すると，コンピュータウイルスに関する知識の不十分なことが対応の遅れを招いた部分もあり，教育・啓蒙活動が必要不可欠であることも確認されることとなった。これを機会として，コンピュータウイルス対策だけなく，セキュリティ確保に向けた教育コンテンツを作成し，知識普及活動を実施している。

ネットワークは情報共有を容易にし，コンピュータは作業の多くの処理を担ってくれることで人間社会に貢献している。しかしながらその利便性は悪用することも可能である。コンピュータがどうであるかだけでなく，それを使うのは人間であることを意識して利用しなければならない。インターネットはグローバルである。日常の現実生活からもう一歩踏み込んだ視点で眺めてみることも必要である。

参考文献

1) 情報処理振興事業協会セキュリティセンター，http://www.ipa.go.jp/security/
2) Microsoft TechNet（セキュリティ情報 MS01-020），http://www.microsoft.com/japan/technet/security/bulletin/ms01-020.asp

（原稿受付　平成 14 年 8 月 1 日）