実践報告

鳴門教育大学情報教育ジャーナル No. 6 pp. 57-58 2009

鳴門教育大学におけるコンピュータウイルス感染状況

曽根直人*，林　秀彦*

高度情報研究教育センターでは，学内で利用される PC に対してウイルス対策ソフトの導入を推進している。教職員が利用する PC に対してはセンターがライセンスを持つウイルス対策ソフトを希望者に提供し，学内のセキュリティ向上に勤めている。本稿では，センターが提供するウイルス対策ソフトで検出したウイルスの情報をまとめ，学内におけるコンピュータウイルス感染状況を報告する。

［キーワード： ウイルス感染，USB メモリ］

1. はじめに

ICT 技術の普及により学内でも多くの PC が LAN に接続され，多岐にわたる教員・学生等の研究・教育利用の要求に応える有機的な情報システムを構成している。LAN を介して，メールやデータなど様々な情報の交換や，Web ページへのアクセスを通した情報収集といった作業は日常的に行われている。一方，コンピュータウイルスはますます巧妙になり，種々のウイルス感染が確認される状況にある。例えば，Mal_Otorun1，HTML_IMRAME.AZ，TROJ_IFRAME.CP 等のウイルス感染が報告されており，ネットワークを介した感染に加え，最近では USB フラッシュメモリなどを介してセキュリティの低い PC を狙った感染活動を行っている。LAN 環境では，ひとたびネットワーク内にウイルス感染 PC が持ち込まれると，感染が急速に広がる場合が多い。そこで，個々の PC でセキュリティを確保することが重要になる。高度情報研究教育センターでは学内のセキュリティ向上のため，ウイルス対策ソフトを一括してライセンス契約し，希望者へ配布している。

本稿では，センターが提供したウイルス対策ソフトにより報告された学内の感染状況をまとめ，学内における被害状況を推測する。これらの現状のデータに基づき，計画的に対策を講じることで，これまで以上に安心・安全な情報環境の維持・向上を図りたい。

2. 学内での感染状況

平成 20 年 4 月 1 日から平成 21 年 3 月 10 日までの 343 日間に報告されたウイルス検知情報を示す。図 1 は月別の検知数を示す。手動検査は端末で対象フォルダを指定し手動で検査を行った結果の検知数，リアルタイムはリアルタイムスキャンでの検知数，ScanNow はサーバからの一斉検査により検知された数を示す。図1より，7月に検知数が増加していることが分かる。

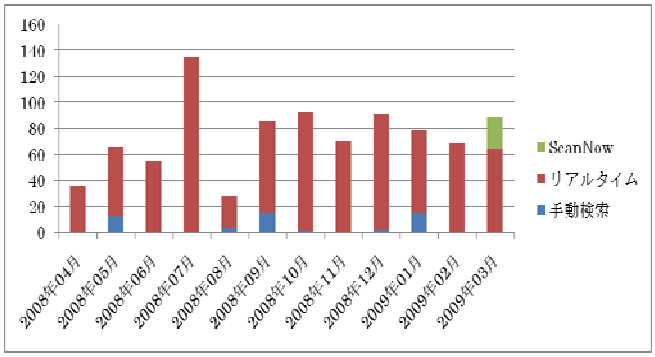

図 1　月別のウイルス検知数

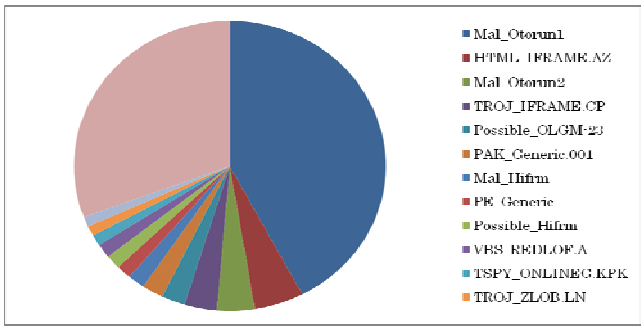

図 2　検知されたウイルスの種類

ウイルス対策ソフトはトレンドマイクロ社のウイルスバスターコーポレートエディション 8.0 を利用し，合計 551 端末にウイルス対策ソフトがインストールされている。この間に検知されたウイルスは 898 個であった。検知されたウイルスの分類を図 2 に示す。上位のウイルスについてより詳しくまとめたものが表 1 である。

表 1　ウイルス感染の内容

名前	検出数	特徴
Mal_Otorun1	380	USB 感染
HTML_IFRAME.AZ	46	改竄された Web ページ閲覧
Mal_Otorun2	35	USB 感染
TROJ_IFRAME.CP	30	改竄された Web ページ閲覧
Possible_OLGM-23	22	トロイの木馬（オンラインゲーム）

＊　鳴門教育大学 大学院 自然・生活系教育部

特に目立つのは”Mal_Otorun1”や”Mal_Otorun2”と呼ばれるUSB感染タイプのウイルスである。これらは合計415回も検出されており，検出されたウイルスのうち実に46%を占めている。図3にこれら2種のウイルスの検知数を月別に集計したものを示す。5月以降は夏期休暇の8月を除き30件以上の検知が続いている。トレンドマイクロ社のウイルス感染被害レポートでも”Mal_Otorun1”は2008年2月に初めて報告され，2月から5月の間被害報告数も1位になっている。

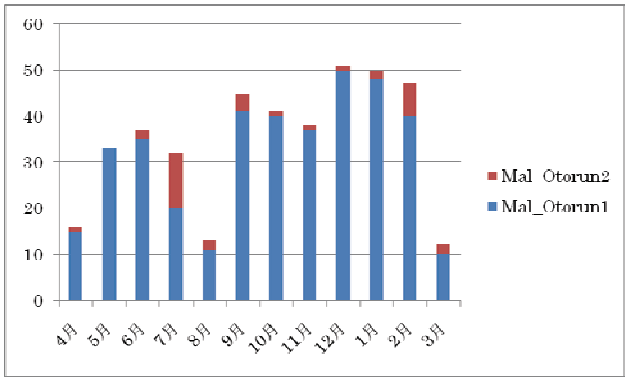

図3　USB感染タイプのウイルス

3.　考察

ウイルスの検知数は7月に最大の135になっている。7月に最も多く検知されていたのは”HTML_IFRAME.AZ”で28回検知されている。さらに詳しくログを確認すると，短時間に検知が集中している。これはウイルスが仕組まれたWebページを利用者がアクセスし，それを集中的に検知したものと考えられる。つまり報告はされているものの実際に端末がウイルスに感染していたわけではない。したがって単純に感染報告数の集計は学内のウイルス感染状況を直接反映しているわけではないことに注意する必要がある。

次にUSB感染タイプのウイルスについて考察を行う。感染報告がなされた学生アカウントについて，最初に感染が報告された日付から最後に感染が報告された日付の日数を求めたものを図4に示す。

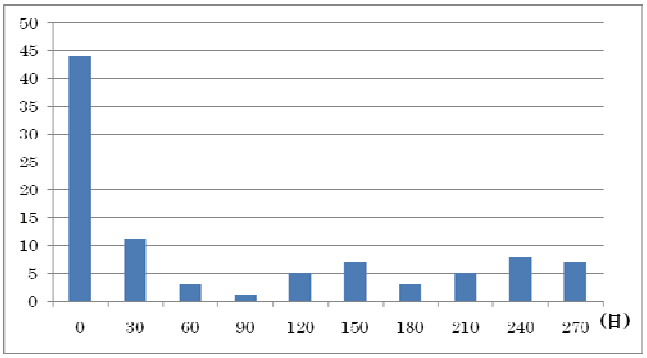

図4 ウイルス感染状況の経過

もっとも度数が多いのは0日の44であり，1度はUSBメモリに感染したもののその後は感染を予防できているユーザの数である。一方，数日後に感染が報告されたユーザは合計すると50アカウントになる。つまり，USBメモリに感染したユーザは半数以上が後日再感染している。これらのユーザは普段利用しているPCで十分な感染への対策ができていないと考えられる。そのようなPCではUSB感染タイプ以外のウイルスにも感染している可能性が高い。今後もウイルスやネットワークやUSBなど様々な媒介により感染活動を行うことが予想されるため，全学的に利用するPC全てでセキュリティを保つ必要がある。高度情報研究教育センターでは学内の教職員に対してウイルス対策ソフトを導入してもらうべく導入状況の調査を行った。その結果，80%程度の教職員から導入済みとの報告があった。学生に関してはOSのアップデートといった対策に加えて低価格や個人利用では無料で利用できるウイルス対策ソフトの情報を提供し，コストの負担を低く抑えながらもセキュリティを向上させる方法をより積極的に啓発活動を進める必要がある。

4.　おわりに

本稿では，センターが提供するウイルス対策ソフトで検出したウイルスの情報をまとめ，学内におけるコンピュータウイルス感染状況を報告した。学内でもUSB感染タイプのウイルスが流行しており，全学的な規模でのウイルス対策が必要である。センターではユーザには，「利用しているPCのセキュリティが低くウイルスに感染すれば他の人にも迷惑をかける」という意識を持ってもらい，安全なICT環境の構築には一人一人の心がけが重要であるということを理解してもらえるよう，講習会や授業での啓発活動を行いたい。

参 考 文 献

[1] ウイルス感染被害レポート，
http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/2008/index.html