実施報告

横浜キャンパスネットワークの ウィルスメール対策

萩原　拓郎

近年インターネットではコンピュータウィルスによる被害が拡大し続けている．武蔵工業大学横浜キャンパスでは，被害を減らすためウィルスメール対策システムを導入した．本稿では，ウィルスの検出状況を調査し，導入したウィルス対策システムの効果を検証し，あわせて今後の課題を指摘する．

キーワード：コンピュータウィルス，ウィルス対策，WebShield，ウィルスメール

１　コンピュータウィルス被害の拡大

インターネットでは近年コンピュータウィルス(以下ウィルスと略す)による被害が拡大し続けている．IPA(独立行政法人 情報処理推進機構)への届け出数は，この14年間届け出数が対数的に増加している．［１］(図１)

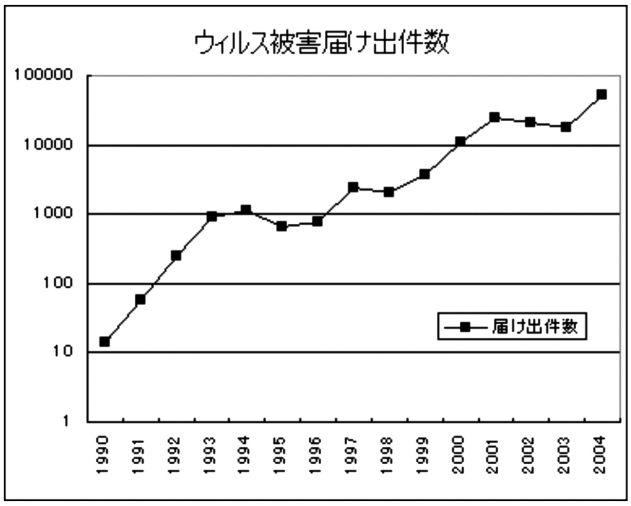

図１　IPA へのウィルス被害届け出件数［１］

ウィルスの主な感染経路はいくつかあるが，近年電子メールの添付ファイルを介したものが多くなっている．こうしたウィルスは電子メールにウィルスを添付して送付し，受信者が添付されたウィルス感染ファイルを実行することでその PC がウィルスに感染する．宛先はウィルス感染ファイルが感染した PC 内のメールアドレスファイルなどから探し出すことが多い．こうしたウィルスは通常の電子メールの配送経路を通って届けられるので，電子メールの配送経路にウィルス対策システムを設置することで駆除できる．

ウィルスの感染経路や方法も新しいものが出てきており［２］［３］，キャンパス内でもウィルスによる感染がしばしば見つかるため，対策が必要となっている．

２　メールサーバ用ウィルス対策システムの設置

情報メディアセンタには横浜キャンパス学生，教職員用の電子メールサーバが設置されており，近年ウィルスを添付したメールの送受信が急増している．キャンパスでのウィルス被害を減らし，利用の際の安全性をより高めることを目的として，2004 年度よりメールサーバ用ウィルス対策システム(McAfee WebShield Appliance(図２))を導入した．

図２　WebShield Appliance[4]

このシステムはキャンパスを出入りする電子メールの本文あるいは添付ファイルにウィルスが含まれていないかチェックし，ウィルスが含まれていた場合ウィルスを即削除する．なお受信者には，ウィルス感染したメールがあった旨のみをメールサーバから伝えるようにしている．

３　ウィルス検知状況

WebShield Appliance の導入により発見されたウィルスの数は図３のようになった．図３は，導入したウィルス対策システムで１週間に発見されたウィルスの合計数をプロットしたものである．システムで発見されたウィルスの特徴としては次のものあった．

HAGIWARA Takuro
武蔵工業大学横浜事務室情報メディアセンター事務課技術員

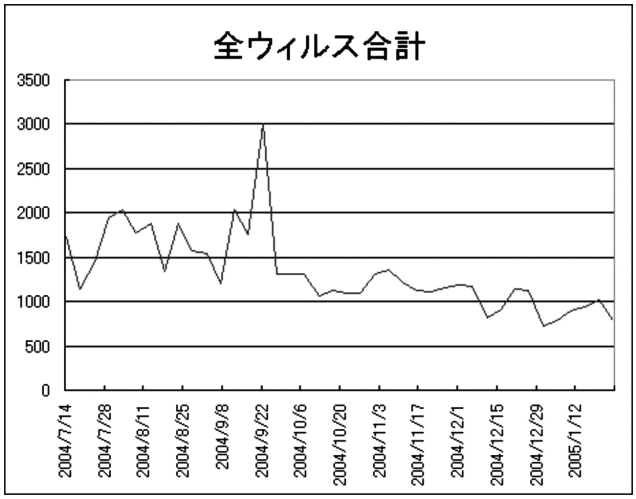

図３　WebShield でのウィルス検知合計数

・発見されたウィルスは全てキャンパス外からキャンパス内へ配送されていた.
・全体的な傾向は減少傾向にある.

ウィルスは全てキャンパス外からキャンパス内へ送信されるメールに含まれていた．これは，キャンパス内でウィルス感染がなかったことを示すのではなく，ウィルスがメール送信のためにキャンパスメールサーバを利用せず直接送信していたためと考えられる.

キャンパス外の PC がウィルス感染した場合には，ウィルスメールは必ずキャンパスのメールサーバに届けられる．このためキャンパス外からキャンパス内へ届けられるウィルスメールはシステムで検知される．ところがキャンパス内の PC がウィルス感染した場合には，ウィルスはキャンパス内のメールサーバを利用せず直接宛先のメールサーバへメールを送信する．このためキャンパスのメールサーバを経由せずにキャンパス外へウィルスメールが送信され，結果としてキャンパス内からのウィルスメール送信が検知されていないと考えられる.

４　今後の課題

クラッカーがウィルス感染メールを自動送信するウィルスソフトをプログラムすることを考えた場合，PC で利用されているメールソフトに設定されているメールサーバを利用しようとすると，世界で利用されている様々なメールソフトそれぞれに対応して設定を読みだせるようにしなければならない．これは手間がかかり，送信できない場合も出てくる．そうする代わりにウィルスソフト独自にメールを配信することで，一般的にメールを送信できるようになる．つまり，キャンパス内のウィルス感染 PC がウィルスの送信の際にキャンパスのメールサーバを使用しないのはこのためと考えられる.

キャンパスへ届くウィルスメールの数は，全体として減少傾向にある．ウィルスメールがキャンパス外から届くメールであることから，この原因はキャンパス外，インターネット全体にあると推測されるが，具体的な原因までは推測できない.

キャンパス内からキャンパス外へ送信されるウィルスメールを検知できないことから，キャンパス内のウィルス感染の現状把握ができていないことになる．大学が外部へ被害を及ぼしているかどうかということであるので，その把握は重要なことである．外部へのメール送信をキャンパスメールサーバからのみに限定することで，状況を把握することができるが通信の制限は問題も多く簡単には実現しづらい.

５　まとめ

メールサーバ用ウィルス対策システムでのウィルス検知結果から次のことが言える.

・キャンパス内へウィルスメールが届けられるのを多数防いでいる.
キャンパスに入ってくる多数のウィルスメールを駆除し，キャンパス内部の PC に対するウィルスの危険生を大きく減少させている.
・キャンパスへ送信されるウィルスメール数は 2004 年７月から徐々に減少している.
減少したといってもまだ多数のウィルスメールが届いており，現状対策も不十分であり今後とも対策が必要である.
・キャンパス内から送信されるウィルスメール数は検知できておらず，現状把握ができていない.
状況把握のためには通信経路の制限を行う必要があり，実現しづらい.

今後もウィルス対策の強化を継続して検討していく必要がある半面，実現のために利用の制限を行うことが必要になる可能性もあるかもしれない.

参考文献

[1] 独立行政法人情報処理推進機構:"2004 年年間および 12 月の発見届出状況(要旨)"
http://www.ipa.go.jp/security/txt/2005/01outline.html
[2] 独立行政法人情報処理推進機構:"2004 年 11 月の発見届出状況(要旨)"
http://www.ipa.go.jp/security/txt/2004/12outline.html
[3] 独立行政法人情報処理推進機構:"2004 年 10 月の発見届出状況(要旨)"

http://www.ipa.go.jp/security/txt/2004/11outl
ine.html
[4] McAfee:"WebShield Appliance"
http://www.mcafeesecurity.com/japan/products/
mcafee/ws.asp