福島高専のネットワークシステムにおけるウィルス対策とその効果について

The Preventive Measures Against Computer Viruses and its Effect in the Computer Network System of Fukushima National College of Technology

（平成17年9月受理）

大槻 正伸*（OHTSUKI Masanobu）
山田 貴浩*（YAMADA Takahiro）
青木 寿博**（AOKI Toshihiro）
内田 修司**（UCHIDA Shuji）
島村 浩***（SHIMAMURA Hiroshi）
高木 克久****（TAKAGI Katsuhisa）

Abstract

In the Computer Network System of Fukushima National College of Technology there are two preventive measures against computer viruses, *Trend Micro's Interscan "Virus Wall" and McAfee's Managed Virus scan "Asap"*. Those were introduced in March 2003, September 2004 respectively and after introducing those measures there was no virus troubles caused by mails from outside.

We report the background of introducing those measures, an outline of the systems, and the effect of it.

1．はじめに

コンピュータネットワークが発達し、ネットワークが故障すると様々な業務に影響が出るほどネットワークが社会に浸透し、まさにインフラになった現在、1台 1 台のコンピュータよりもむしろネットワークシステム全体に対して、ウィルス、スパイウェア、不法侵入等に対する対策を講じ、情報セキュリティの確保をすることがますます重要になっている。特に、ウィルス対策の重要性は大きい[1), 2), 6)]。

コンピュータウィルスがネットワークシステム内のたった1台のコンピュータにでも感染すれば、そのコンピュータのみならず、他のネットワーク内コンピュータに被害を与え、ひいては、ネットワークシステム全体にも支障をきたす可能性まで考えられる。また、ウィルス感染は、インターネットが普及した現在、ウィルス発見当時よりもはるかに短時間に広範囲に広がり、その被害を拡大する。

したがって、ウィルス対策はできる限り迅速に、ウィルスを含むファイルの除去、隔離等の処置を施す必要がある。

コンピュータウィルスは1986年にその第一号が発見されて以来、その種類は増加し、現在では知られているウィルスの数は10万種を超えると言われている。過去10年間のウィルス被害（届出）件数は Fig.1 のようになっていることが報告されている[5)]。

福島高専ではウィルス対策として、McAfee 社の Asap[4)]、トレンドマイクロ社の Virus Wall[3)] とよばれる二重の対策を導入しており、ウィルス対策に関してはかなりの成功を収めている。

＊福島工業高等専門学校　電気工学科（いわき市平上荒川字長尾 30）
＊＊福島工業高等専門学校　物質工学科（いわき市平上荒川字長尾 30）
＊＊＊福島工業高等専門学校　コミュニケーション情報学科（いわき市平上荒川字長尾 30）
＊＊＊＊福島工業高等専門学校　技術室（いわき市平上荒川字長尾 30）

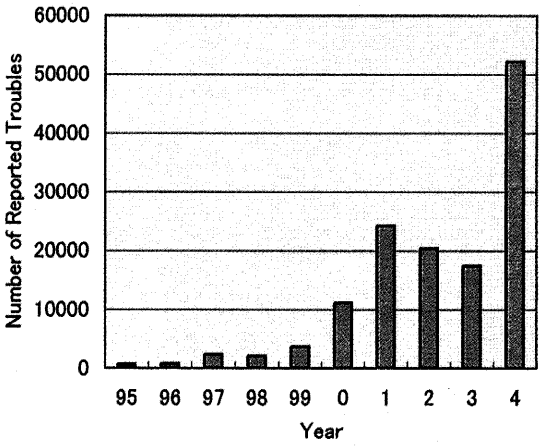


Fig.1 The Number of Reported Virus Troubles (Last 10 years)

ここでは、ウィルス対策システムを導入するに至った経緯、導入したシステムの概要、導入後の効果、今後のあるべき方向等について報告、考察する。

2．ウィルス対策システム導入まで

福島高専では、2002 年までは、ウィルス対策は各自責任をもって行うこととされており、セキュリティポリシーも整備されていなかった。

幸いにも、大きなウィルス被害は発生していなかったが、それでもいくつかウィルストラブルが発生している。

このトラブル時にはいずれも情報処理教育センター員が中心となり、センター内各サーバのログ等をもとにウィルス感染したと思われるパソコンを推定し、そのパソコンのある場所まで出向きワクチンソフトで対策をした。

このような、対症療法的なウィルス対策は、新種のウィルス発生等に対して後手にまわることが多く、効率としては非常に悪い。また、各自がウィルス対策ソフトを研究費等で購入するというのも予算的にも効率が悪いことは明らかである。

そこで、よりシステマティックにウィルス対策を講じることが必要になってきた。

3．ウィルス対策システムの導入

3．1 導入経緯

福島高専では、現在結果的に 2 つの異なるシステムでウィルス対策を行っている。

その導入の経緯について述べる。

2003 年 3 月にトレンドマイクロ社「InterScan Virus Wall」を導入した。これは、後述するように、外部から福島高専へのメール、福島高専から外部へのメールについて、メールにウィルスがついていないかどうかをチェックし、ウィルスがあれば除去するシステムである。

主にウィルスが侵入するのは、外部からのメールであること、また本校から外部に送信するメールにより外部社会へ迷惑をかけないことが重要であるから、これでウィルス対策はかなり安全になったといえる。

しかし、その後この Virus Wall のチェックを通り抜けるウィルスが現れ、また、外部から持ち込んだ、ウィルスに感染したパソコンを LAN に接続することで発生したウィルストラブルもあり、LAN に接続してある各パソコンのレベルでのウィルス対策も是非必要であることが認識された。

そこで 2003 年 10 月にはマカフィー社ウィルス対策システム「Managed virus scan Asap」を導入した。

これは、詳しくは後述するが、Windows パソコンでウィルスが動き出した瞬間にそれを感知し処置するものである。

システム導入の 2003 年当時、「ウィルスの種数は 6 万種以上、内 Macintosh のウィルスは数 10 種、UNIX、Linux 系のウィルスも数 10 種、残り大部分 6 万種以上は Windows、Dos のウィルスである（99.5%以上は Windows、Dos のウィルス）」という報告がなされていた。またこの状況は現在も大きくは変わっていないので、Windows のウィルス対策が最重要課題となっている。そのため Windows パソコンに限定して強く対策を講じたのである。

このように 2 つ別の会社の提供するシステムによるウィルス対策は、LAN システムのよりよい安全性を確保していることになるがその理由は以下のとおりである。

新種のウィルスが次々と生まれる現状では、完璧なウィルス対策システムはあり得ない。したがって、各会社のウィルス対策製品にはどこかしら「穴」があるが、その穴は会社により異なっているのが普通である。独立して新種のウィルスに対して対策をしている 2 社のシステムを入れた方が、同じ会社の同じ対策のものを 2 製品導入するよりも、対策の穴は小さくなる（2 社共通の穴をつかれたときのみウィルスが侵入することになるが、その確率は低くなる）。

上記 2 つの対策により、現在はウィルスに対しては相当強い学内 LAN システムになっていると思われる。

3．2　2つのウィルス対策システムの概要

以下で、この2つのシステムの概要について述べる。

【トレンドマイクロ社「InterScan Virus Wall」】

このシステム（以下「Virus Wall」という）はFig.2のように学内にVirus Wall用サーバを設置し、メールサーバが外部からメールを受信したとき、あるいは、学内から外部へのメールがメールサーバに届いたとき、メールサーバは、まず一旦Virus Wallサーバへメールを渡す。Virus Wallサーバはメールにウィルスがついていないどうかをチェックし、ウィルスがついていた場合、それを除去する等の処置をする。

チェック、処置が終了したメールは再びメールサーバに渡され、メールサーバはVirus Wallサーバのチェックを通ったメールを通常通り配信する。

Virus Wallは、この他不正侵入、不正アクセスのチェック、ブロック等も可能ではあるが、そのためにメールチェック機能の効率、インターネット環境の効率が下がる恐れがあることなどから、現在は上述のようにメールチェックのみを行うようにシステムを設定してある。

またVirus Wallサーバは、トレンドマイクロ社の最新ウィルス情報を持っているサーバに一日一回（午前3時に）アクセスし、最新ウィルスデータを更新し、常に最新のウィルス情報で、チェックするようになっている。

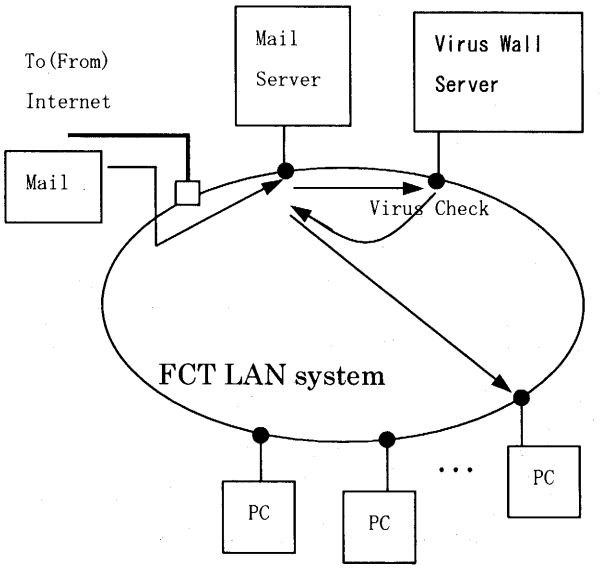


Fig.2　Image of the Virus Wall System

上述で分かるように、Virus Wallのみの対策の場合は、

（・1）学内のパソコン同士のメールのやりとりに対してはウィルスチェックをしない。

（・2）トレンドマイクロ社の対策が実施されていない、あるいは対策は講じられたが、それが本校のVirus Wallサーバに反映されていないような新種のウィルスがメールについてきたときウィルス侵入の危険がある。

（・3）メール以外の経路（ウィルスのついたフロッピー持込等）でウィルスがLANシステムに侵入したときにもウィルストラブルの危険がある。

という問題点がある。

しかし、実際にウィルスが侵入したとしても、次に述べるマカフィー社Asapによりウィルスを除去することができる。

【マカフィー社「Managed virus scan Asap」】

このシステム（以下Asapという）は、学内にサーバを持たないシステムである。Fig.3のように、学内のWindowsパソコンユーザ（AsapはWindowsパソコンにのみ適用される）は、インターネット経由で、マカフィー社のサーバに、ホームページアクセスする感覚でアクセスし、ウィルス対策ソフト（およびウィルスデータ）をダウンロードし、常にウィルスチェックを行うようにする。

ただし、ユーザは一回対策ソフトをダウンロードすれば、次回パワーオン時からは何も意識せず、対策ソフトは自動的に立ち上がり機能し、またデータ更新も自動的になされる。

各パソコンで稼動している対策ソフトは、ウィルスがパソコンで動き始めた時点で（例えば、ウィルスのついたファイルを含むフロッピーやUSBメモリを使用し、そのファイルがメモリにロードされたき）ウィルスを感知し、除去、隔離等の処置を施すシステムになっている。2005年9月現在で、学内のWindowsパソコン約450台がこの対策を実施している。

なお、ウィルス最新データを各450台のパソコンがマカフィー社のサーバから一斉にダウンロードするとネットワークのトラフィック量が非常に多くなることが懸念される。しかし、このシステムでは、学内のパソコンがパワーオンした時に、周りのパワーオンしている学内パソコンに最新ウィルスデータをもったパソコンが存在しないかを問い合わせ、最新データがあった場合はそこから受け取る方式にしてあるため、マカフィー社―福島高専間のトラフィック量が多くなることがないように工夫されている。

もしも、ウィルスがVirus Wallのチェックを通り抜け、あるパソコン上で動作を始めたとしても、Asap

により、除去、隔離等の処置がなされるため、まず確実にウィルスの感染を防ぐことができる。

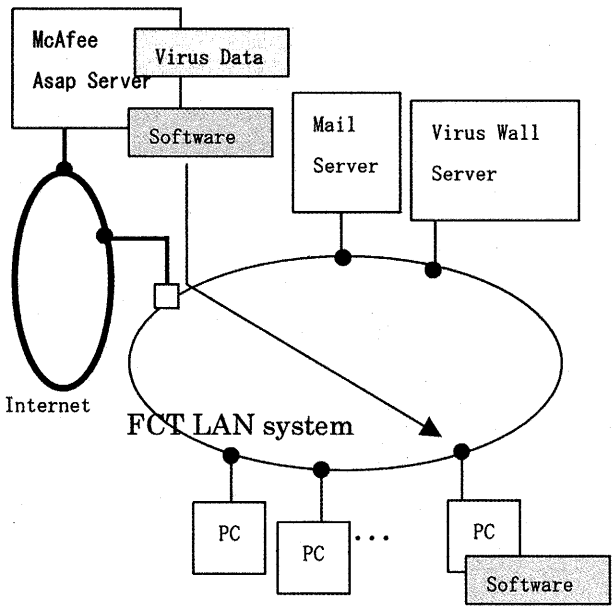


Fig.3　Image of the Asap System

4．ウィルス対策システムの成果

4．1　ここ一年間のウィルス検出数

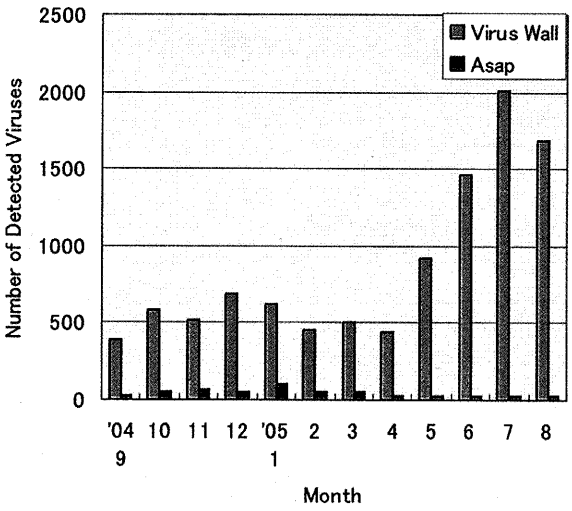
Fig.4 に Virus Wall、および Asap によるこの一年間のウィルス検出数の月別統計を示す。

この一年間（2004 年 9 月～2005 年 8 月）で Virus Wall で検出されたウィルス数は 10266 件、Asap による検出は 532 件である。

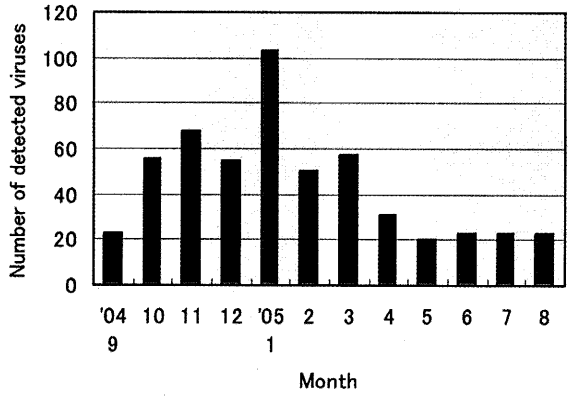
すなわち、おおよそ 95%は Virus Wall が検出し処理するが、残り 5%程度は何らかの経路により学内 LAN に接続しているパソコンに入り込み、Asap により検出されている。これを見ると、この 2005 年 5～6 月から Virus Wall によるウィルス検出数が急増していることも分かる。

ここ 1 年間で Virus Wall により検出されたウィルスの種類は、多いものから 5 種類をあげて Fig.5 に示す。コンスタントにメールについてくる WORM_NETSKY（この一年間で 4661 件）、2005 年 5 月ごろから急激に多く検出されるようになった WORM_MYTOB（同 4918 件）が特に目立つ。

また Fig.6 には Virus Wall 導入後現在までのウィルス検出件数を示す（Fig.4(1)と一部重複）。2004 年 1 月からウィルス検出件数が急激に増加し、2005 年 5 月でさらに増加したことが見てとれる。



(1) By Virus Wall and Asap



(2) By Asap only

Fig.4　The numbers of detected viruses by Virus wall and Asap (Last one year)

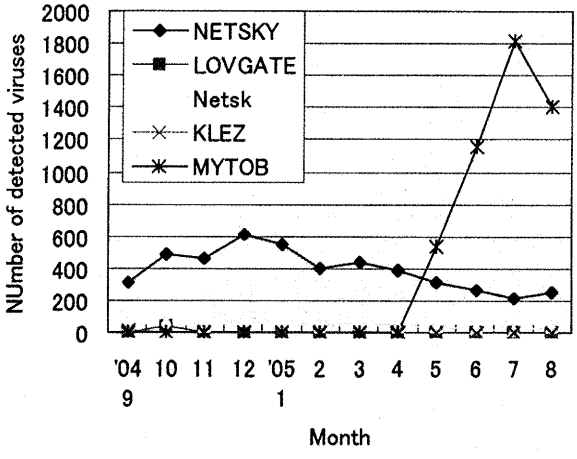


Fig.5　5 most times detected viruses

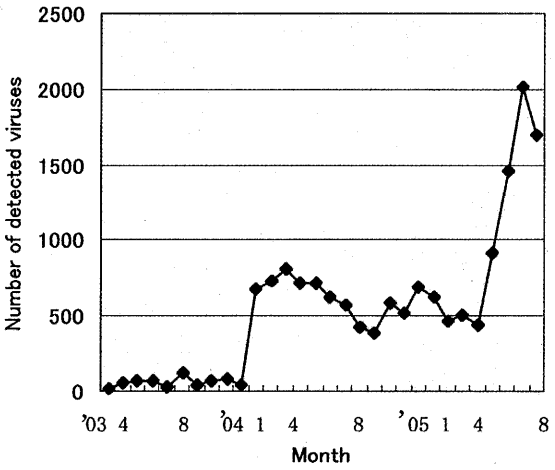


Fig.6 The number of detected viruses by Virus Wall (ToTal)

4．2 ウィルス対策システム導入以降と今後の課題

この２つのウィルス対策システムを導入してからは、外部からのメールにより発生したウィルストラブルは皆無である。

しかし、実際のところウィルス感染によるトラブルは３件発生している。

うち２件は、教員が新しいWindowsパソコンを購入し、Asapを組み込まずに学内LANに接続したことによるもの、もう１件は図書館の図書検索用パソコンにAsapを組み込んでいなかったことによるものである。

新しいパソコンには、最初はウィルスは存在しないが、これだけウィルスが飛び交っている現状ではLANに接続するとすぐにウィルスに感染してしまう。

これらのウィルス感染のトラブルでは、ウィルスをばら撒きはしたが、他のパソコンに感染させパソコンの機能にダメージを与えるという被害ではなかった。他のパソコンに感染してもほとんどのパソコンはAsapによる対策がなされているため、すぐに除去された（と推定される）からである。しかし、感染したパソコンからは異常に多数のメールが送信されたため、LANのトラフィック量が増加し、LANシステムにダメージを与えるものであった。

いずれにしても、よく言われるように、「ウィルストラブルは外部からよりは内部が原因」「セキュリティ崩壊は内部の一番弱いところから」であった。

今後の課題としては、次のことがあげられる。

(1)セキュリティポリシーの充実、ポリシー遵守の徹底化をはかり、学内の全教職員がウィルス対策を正しくとるように意識するようになること（それには、Fig.4～Fig.6のとおり、裏の我々の意識しないところで２つのシステムが相当数のウィルスを検知し処理している現状の周知も必要であろう。）

(2)ウィルス以外の、スパイウェア、不正侵入対策等も充実させていくこと（最近ではAsapにスパイウェア駆除等の機能が充実してきている）。

(3)個人情報保護法等に関連する、ウィルス以外の情報漏洩等に対するセキュリティの確保。

このように、ネットワークシステムのセキュリティを確保するには、ウィルス等のLANシステムやパソコンにダメージを与えるものに対する対策はもちろん、より広い視点から、

- スパイウェア（パソコンハード等には影響を与えないがパソコン内の情報をばらまいたりするソフトウェア）対策、
- 不正侵入対策、
- 人間によるパソコン(USBメモリ等)持ち出し等、様々な情報の漏洩等に対する対策

等をも含めて、技術・工学的側面、人的側面も考慮し、従来よりも広い眼で見てセキュリティ問題を考えていく時期にあると考えられる。

参考文献

1） 伊藤 敏幸、ネットワークセキュリティが分かる本、オーム社、2002年

2） 渋川 栄樹、図解入門 よくわかる最新ネットワーク管理の基本と極意、秀和システム、2004年

3） トレンドマイクロ社ホームページ
http://www.trendmicro.co.jp/home/

4） McAfee社ホームページ
http://www.mcafeesecurity.com/japan/

5） IPA（情報処理振興事業協会）セキュリティセンターホームページ
http://www.ipa.go.jp/security/

6）山本 隆雄他、コンピュータウィルス、講談社ブルーバックス，1993年