ウイルス対策について

山口政光

横浜国立大学総合情報処理センター
〒240-8501　横浜市保土ヶ谷区常盤台 79-5
Tel :045-339-4392　Fax::045-339-4393
yamakuti@ynu.ac.jp

Countermeasure for Computer-Virus

Yamaguchi Masamitsu

Information Processing Center, Yokohama National University
79- 5 Tokiwadai, Hodogayaku , Yokohama 240-8501, JAPAN
Tel :+81-45-339-4392　Fax:+81-45-339-4393

概要

本学が行ってきたコンピュータウイルスに関する対策を説明し、システム導入時に留意すべきことを実施事例として報告する。

キーワード

コンピュータウイルス、ウイルス駆除、電子メール、メールゲートウェイ、レイヤー４スイッチ

１．はじめに

本学では、３年前に授業用のパソコン３００台の３割がコンピュータウイルスに感染したことから、ウイルスワクチンを選定して、授業用パソコンにインストールするとともに、学内のネットワーク接続利用者に、廉価で配布して、ウイルス対策を行ってきた。
しかし、昨年夏から発生した新種のウイルスは、電子メールを感染媒体とするためウイルスに無関心な人を直撃して、感染・発症が多発する事態となった。
そこで、ＳＩＮＥＴとの接続点を通過する電子メール全てに対して、ウイルスの検知・駆除をするメールゲートウェイシステムを導入したが、予想しなかったほどの絶大な効果をあげている。
ウイルス対策の実施時例として、経過とともに導入して気が付いた留意すべきことを報告する。

２．発端

1999 年 4 月にコンピュータウイルス「PE-CIH（別称：チェリノブイリ）」が大発生したが、数日の間に授業用のパソコン 300 台の 32%が感染した。
特に、学生に自由開放している教室では 110 台のパソコンが全数感染していた。
とりあえず、トレンドマイクロ社のウイルスバスター９８を使って 300 台のクリーニングを行った。
このウイルスは､5 月 26 日に発症して HDD をフォーマットするものであったから､時間的な余裕はあったが､授業コマを避けての駆除作業は３日間を費やした。

３．ベンチマークテスト

表-1 に示す５社のワクチンソフトを入手し、手元に保管していたウイルスの検知・駆除状態を調べた。
また、InfoWorld 社、Forrester Research 社、PC-Computing 誌、IPA、等の評価結果を参照し、サーバ管理できることも考慮して、Trend Micro 社のウイルスバスター９８を選定した。

社　名	ワクチンソフト名	リアルタイム検索		手動検索	備　考
		PE-CIH	Happy99	MO検知 ﾌｧｲﾙ数	
Trend Micro	ウイルスバスター98	○	○	41	ｻｰﾊﾞ管理可能 MAC に非対応
Symantec	Norton AntiVirus	○	△	38	設定方法難解
Network Associates	virus Scan	○	×	38	使用方法難解
Core	Virus Safe	×	×	37	
CSE	SWEEP	○	×	38	リアルタイム検索なし

表-1　ベンチマークテスト　　1999-6-17 濱名技官

４．ウイルスバスター

ウイルスバスターを契約する段階になって、Trend Micro 社は価格をボリュームディスカウントしていて、購入価格が 300 台でも 1,000 台でもほぼ同じ 100 万円であることが判明した。
そこで、1,000 台を購入して、センターの教室に充当した残りの 700 台を学内の希望者に１台 500 円で配布することとして募集を行った。ところが、当初の希望数が 1,000 台を超えてしまったので、1000 台を追加契約した。この 2,000 台はその後の１年間で希望者に配布完了し、さらに 1,000 台を別契約している。
なお、このボリュームディスカウントは他製品にも適用されるので、Server Protect もアカデミック価格の 80%引で購入できる。現在 55 台を契約して稼働している。

本年 3 月に更新した研究・教育用計算機システムのパソコン(742 台)に対しては、仕様の中にウイルスバスターの Corporate Edition でサーバ管理することと指定し、別契約（リース）で稼働している。
なお、授業用パソコン教室の他、事務系職員のパソコン(350 台)と経済学部の一部は、Corporate Edition によってサーバで一括管理する方式を取っている。

不特定多数の人が利用する授業用パソコンに導入するウイルスバスターはサーバ管理しなければならない。なぜなら、個別のウイルスバスターでは、駆除に失敗したときに手働操作によって措置しなければならないが、放置されることが多く、その事実を管理者が把握できないので、感染したまま使われてしまうからである。サーバ管理すれば、感染状況が逐一管理者にメールで通報されるし、ログも残る。

５．感染・発症数

ウイルスバスターを導入して以来２年間の、ウイルスに感染・発症して駆除処理やＯＳの再インストール等を実施したパソコンの月別発生台数を図-1 に示す。

昨年 8 月以降に急激に発生数が増えたのは、ウイルスの性質が変り、ＩＥの脆弱性を利用して電子メールに添付して感染を広げる形式のものが現れたことによる。
ここで感染・発症したパソコンを調査すると、ワクチンソフトがインストールされていないか、インストー

ルされていても、パソコン購入時に添付していたものが期限切れになっていたり、パターンファイルの更新をしていなかったために、ウイルスを検知・駆除できなかったものである。
折に触れて廉価配布の案内をし、ワクチンソフトの重要性を宣伝していたが、感染後にあわてて配布申請をしてくるケースがほとんどであり、事が起きる前に予防としてワクチンソフトを入れることを徹底することの難しさを痛感したときである。

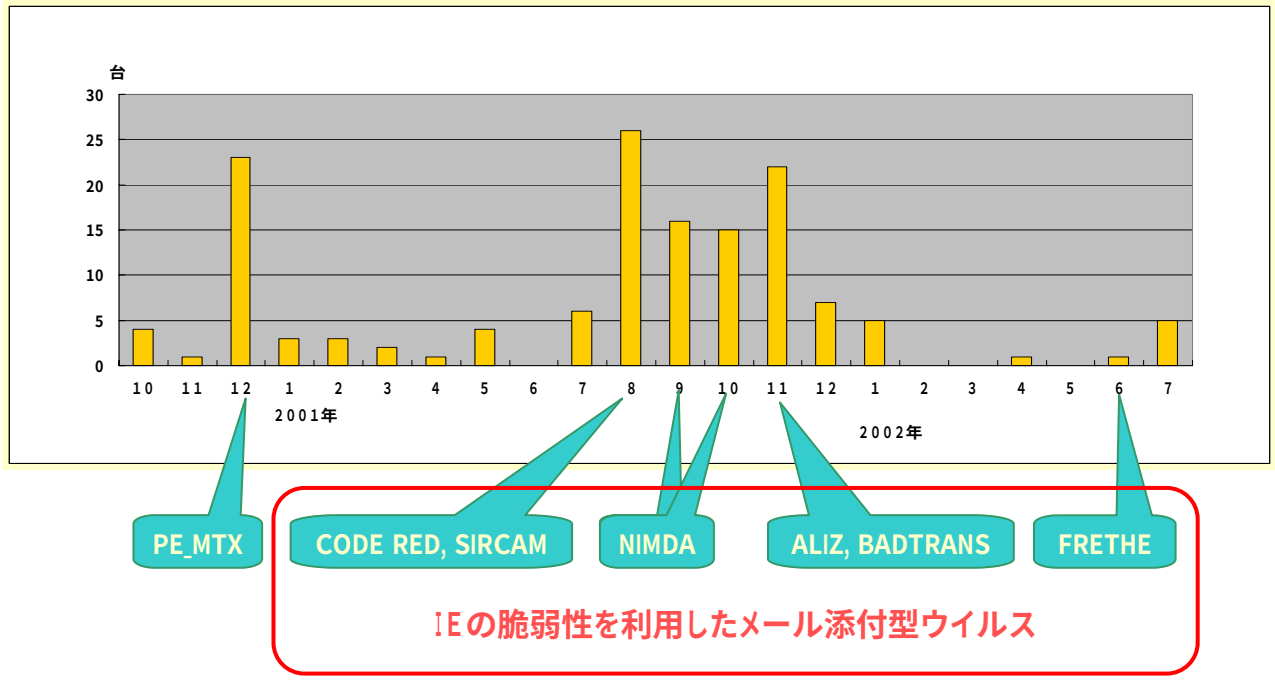


図-1 ウイルス感染・発症パソコン台数

６．個別ワクチンの課題

(1)関心のない人が感染する

前述のように、関心のない人にワクチンソフトを入れてもらうことは大変難しい。
しかし、これがセキュリティホールとなって、学内に多数の２次感染者を発生したこともあり、ある程度強制する制度が必要である。いずれ策定されるセキュリティポリシーに盛込みたいと思っている。

(2)ウイルスが放置される

サーバ管理しているパソコンを見ていると、ウイルスバスターが働いても、完全に駆除できなくて隔離されたり拡張子変更をした場合に、手動で当該ファイルを削除しなければならないが、これを行わないケースが多々ある。これは、いわば保菌状態であり好ましいことではない。サーバ管理者がログを見て、駆除に奔走する状態が続いている。
個人で個別に入れているワクチンにも同じことが起きていると思われる。

(3)授業用パソコンはサーバ管理すること

不特定多数のユーザが使用するパソコンにウイルスバスターを適用するときにはサーバ管理にして、管理者がこまめにログを見て対処しなければ、感染したまま稼働させる危険がある。

(4)登録台帳管理と経費処理が膨大

希望者に１台 500 円／年で有償配布しているが、経費処理としては校費の振替え手続を行っている。このためには、3000 台の使用者の台帳管理をするが、退官・退職・職場異動を追跡する労力が馬鹿にならない。毎年数 10 台の行方不明が出る。
セキュリティ対策費として共通経費を要求しているが、なかなか認められない。

７．メールゲートウェイ

メール添付型のウイルスの蔓延に対処するには、全てのメールを網羅的にウイルスチェックすることが有効である。
これを実施するために、本年４月にメールゲートウェイシステムを導入した。
全てのメールをウイルス駆除サーバに迂回させるには、ＤＮＳを書換えて学内に存在するメールサーバの中継サーバと位置づける方法もあるが、本学内にはセンターが承認しているメールサーバが 114 台もあり、ＤＮＳサーバも多数存在するので、書換えを徹底することは不可能であると判断し、ファイアウォールの直下にＬ４スイッチを置いて強制的に迂回させる方式をとった。

【機器構成】　Ｌ４スイッチ　……ACEDiretctor3　１台
ウイルス駆除サーバ……ＨＰ社　LP2000r ２台
（Pen Ⅳ、1.26GHz、RedHat Linux 7.2J）
ウイルス駆除ソフト……InterScan VirusWall v3.6

Ｌ４スイッチを通過する全てのＳＭＴＰをウイルス駆除サーバ２台へ負荷分散しながら迂回させ、ウイルスがあったときには駆除した後、宛先に転送する。
ウイルス駆除サーバの内部でのメールの動きを図-2 に示す。

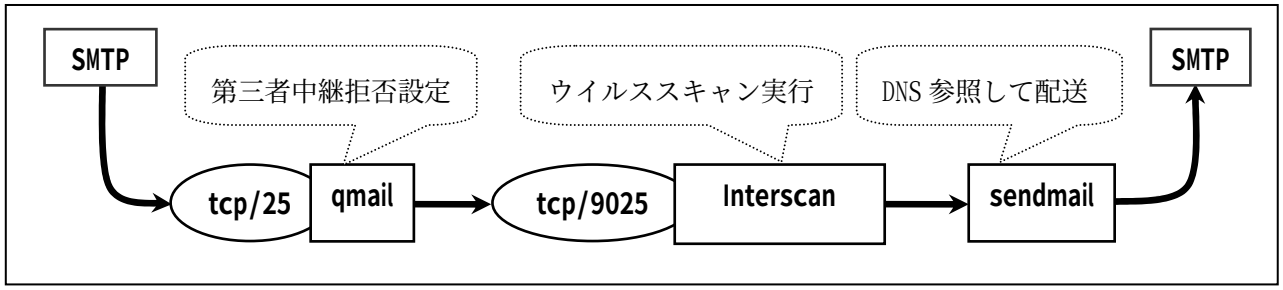


図-2 ウイルス駆除サーバ内部のメール転送フロー

図-3 に、このウイルス駆除サーバにおいて、添付ファイルの中にウイルスを見つけて削除した後に配信されたメールを示す。ヘッダーの網掛け部分が、ウイルス駆除サーバが付記した部分である。

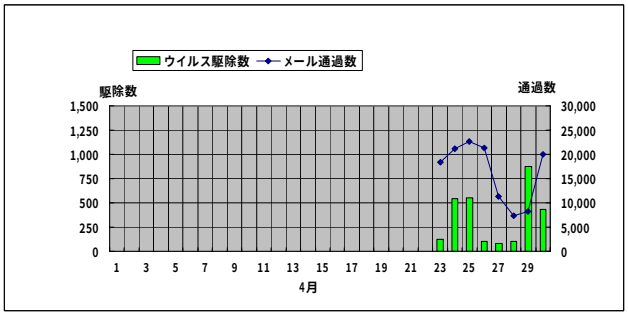
```
Return-Path: <*****@nns.ne.jp>
   Received: from mailgw2.ipc.ynu.ac.jp (mailgw2.ipc.ynu.ac.jp [133.34.7.22]) by
             aplsrvky01.ipcn.ynu.ac.jp (8.11.6/8.11.6) with ESMTP id g796jLH27005
             for <ipc-adm@ynu.ac.jp>; Fri, 9 Aug 2002 15:45:21 +0900 (JST)
   Received: from mailgw2.ipc.ynu.ac.jp (localhost.localdomain [127.0.0.1]) by
             mailgw2.ipc.ynu.ac.jp (8.11.6/8.11.6) with SMTP id g796jKD00405 for
             <ipc-adm@ynu.ac.jp>; Fri, 9 Aug 2002 15:45:20 +0900
   Received: (qmail 397 invoked from network); 9 Aug 2002 15:45:20 +0900
   Received: from unknown (HELO nns.ne.jp) (210.141.237.20) by
             mailgw2.ipc.ynu.ac.jp with SMTP; 9 Aug 2002 15:45:20 +0900
   Received: from Ofljk (blue12.nns.ne.jp [61.193.128.142]) by nns.ne.jp
             (8.9.3/3.7W) with SMTP id PAA76384 for <ipc-adm@ynu.ac.jp>; Fri, 9 Aug
             2002 15:45:16 +0900 (JST)
        Date: Fri, 9 Aug 2002 15:45:16 +0900 (JST)
  Message-Id: <200208090645.PAA76384@nns.ne.jp>
        From: ******** <******@mx2.nns.ne.jp>
          To: ipc-adm@ynu.ac.jp
```

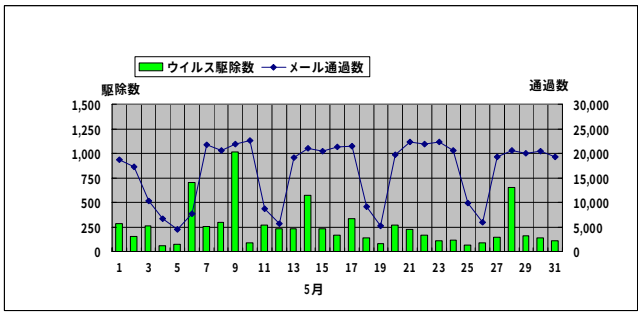
```
          Subject: The Garden of Eden
     MIME-Version: 1.0
     Content-Type: multipart/alternative; boundary=Zc418p496Z000H1n8f68uc7Y
           Status: U
 X-Mozilla-Status: 8001
X-Mozilla-Status2: 00000000
          X-UIDL: @,0"!QK7!!#$Y!!A\R"!

---------- A result message of dealing with a virus in your mail, from viruswall :
mailgw2.ipc.ynu.ac.jp ---------------

src.pif is removed from here because it contains a virus.
```

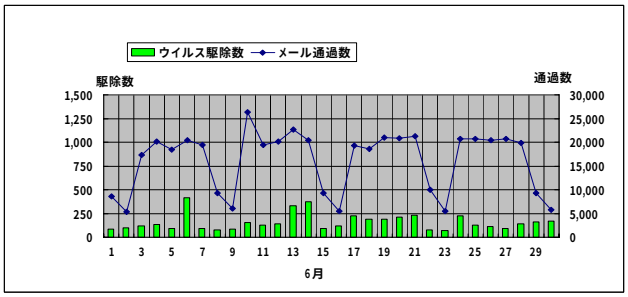
図-3 ウイルス駆除後のメール

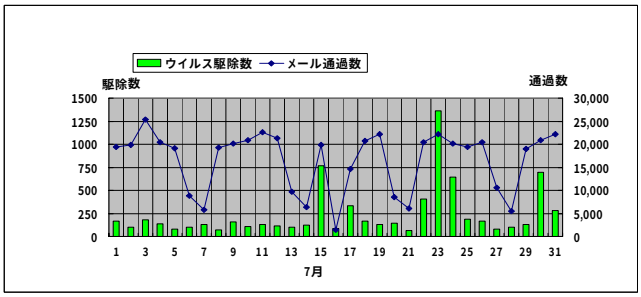
このメールゲートウェイのメール処理数と駆除したウイルス数を図-4 に示す。

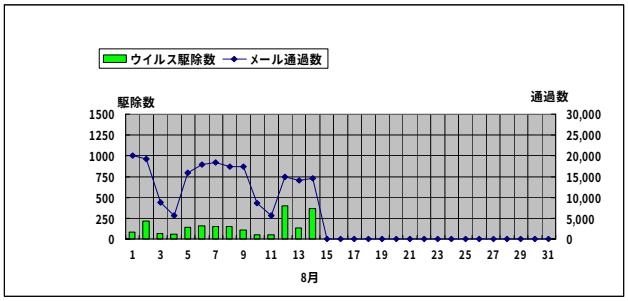
稼働直後に KLEZ ウイルスが大発生し、通過するメールの 10%がウイルスメールであった日や 1,000 通以上も駆除した日もあり、大活躍である。
これまでの４ヶ月間に駆除したウイルスメールの数は２万通を超えている。
学内のユーザからは安心していられるようになったとの評価ももらっている。











最大値（１日当り）
メール通過数　：26,292 通 (2002/6/10)
ウイルス駆除数：1,365 通 (2002/7/23)
駆　除　率　　：10.5 % (2002/4/29)

延駆除数（4ヶ月）：21,754 通

図-4 メールゲートウェイ処理実績

８．メールゲートウェイ構成のポイントと課題

(1)信頼性

学内全てのメールサーバの代理転送サーバになることから、安定運用が必須である。
特に処理能力として、同時セッション数を考慮する必要がある。通常の運転状態においては、メール処理数が１日３万通弱であることから推察しても、同時セッション数は１０もあれば充分である。しかし、学内のメールサーバが稼働しているときに、このウイルス駆除サーバを停止した場合、再立上げと同時にそれぞれのサーバのメールキューに溜っていたメールが連続的に吐出されてくるため、セッションが足りなくなってハングアップする事態となる。本学の例では、同時セッション数が４０ではハングアップが発生した。１５０にしたところ発生していない。

(2)ＯＳ

InterScan VirusWall のライセンス価格は、最初の１台目は 250 万円であるが、追加は同一のＯＳであれば 20 万円となるが、違うＯＳではマルチプラットフォームディスカウントとして半額の 125 万円となる。他のメールサーバにも InterScan VirusWall を適用しやすくするために、主要なメールサーバのＯＳと合わせて導入することを勧める。

(3)Ｗｅｂメール、Ｗｅｂページへの適用

最近のウイルスは Java Script に潜むものがあることと、Ｗｅｂメールの利用が増えていることから、ＨＴＴＰもウイルスチェックすることが望ましい。InterScan VirusWall は設定すればＷｅｂにも適用できるが、サーバの処理能力を充分に考慮する必要がある。

(4)学内相互のメールには非力

このメールゲートウェイはファイアウォールを通過するメールを対象としていることから当然であるが、学内に存在するメールサーバ同士のメールには関与しない。
７月に発生した FRETHEM では、メールゲートウェイのパターンファイルが更新される前に侵入したウイルスによって５台のパソコンが２次感染した。
これを防止するには、全てのメールサーバにワクチンを入れなければならない。

(5)リムーバルメディアには非力

リムーバルメデイアで持込まれるウイルスに対しては当然関与できない。
同じように、学外で使用したときに感染したノートパソコンを学内ＬＡＮに接続してウイルスをまき散らす事例もあるので、メールゲートウェイがあっても、全てのパソコンに個別のワクチンを入れておくことの重要性は変らない。

(6)学外サーバからのＰＯＰには非力

学外のメールサーバからＰＯＰで取込むメールに対しても関与できない。
ウイルスチェック付きのプロバイダーを使うか、個々のパソコンにワクチンを入れることが必要である。

９．まとめと今後の課題

このようなウイルス対策を行ってきたが、学内で感染・発症するパソコンは相変らず皆無にはならない。
しかし、その発生台数は激減していることと、メールゲートウェイが稼働しているおかげで、発症しても学外に迷惑をかけることがなくなったことが、システム管理者として心休まるところである。
今後は、学内相互の感染を防止するために主要なメールサーバに InterScan VirusWall を搭載することと、学内ネットワークに接続するパソコンの条件として、ワクチンソフトの搭載を強制するような方向付けをしたい。
手さぐりで導入してきたウイルス対策の内情報告が皆様の参考になれば幸いである。