分散システム／インターネット運用技術 19－2
（2000．9．29）

大規模サーバにおけるウィルス検査システムの運用法

敷田幹文　井口寧　三輪信介
丹康雄　松澤照男

北陸先端科学技術大学院大学 情報科学センター

近年，インターネット上の電子メールやWebアクセスの広がりに伴い，コンピュータシステムに密かに侵入し，自己増殖する，コンピュータウィルスの被害が急速に広まっているが，クライアント上での有効な検査を全ユーザに徹底させることは難しい．一方，サーバ上に検査プログラムを導入し，組織外から到着した時点で検査・駆除することにより，組織内の各クライアントへの感染を未然に防ぐ方法も用いられるようになってきたが，大型UNIXサーバで運用するためには課題も多い．本論文では，サーバ用ウィルス検査ソフトウェアを著者らの大学において運用させた経験から，このソフトウェアの問題点を明らかにし，それらの問題点を解消する方法およびその運用結果について述べ，本方法の有効性を示す．

Virus Scan System on Large-scale Servers

Mikifumi SHIKIDA　Yasushi INOGUCHI　Shinsuke MIWA
Yasuo TAN　Teruo MATSUZAWA

Japan Advanced Institute of Science and Technology

Recently computer virus is rapidly increasing, according to increasing of E-mail and web access on the Internet. However it is not easy to make all users to scan computer virus on each client computer. And computer virus scanner for server is not suitable to large-scale server systems. In this paper, we describe problems of computer virus scanner for server, based on our experience on our university network. We addresses schemes for configuration of virus scanner for servers, and discuss its effectiveness.

1 はじめに

近年，インターネット上の電子メールやWebアクセスの広がりに伴い，コンピュータシステムに密かに侵入し，自己増殖する，コンピュータウィルス(以下，ウィルス)の被害が急速に広まっている[1, 2, 3]．従来は個々のクライアントパソコン上でウィルス検査プログラムを起動し，ハードディスク上の各ファイルを定期的に検査する方法が一般的であった．このようなソフトウェアをパソコン本体に添付して販売するメーカーも多い．

ウィルス検査プログラムでは，有効に働かせるように起動条件を設定し，新規ウィルスの出現に対応するように検査パターンを日々更新する必要がある．しかし，クライアント台数の増大や，新規ユーザの増加によって，組織内の全ユーザにこの作業を徹底させることは極めて難しい．

そのため，最近では，クライアントではなくサーバに検査プログラムを導入し，組織外から到着した時点で検査・削除することにより，組織内の各クライアントへの感染を未然に防ぐ方法が用いられるようになってきた．しかし，このようなソフトウェアはパソコン上で発展してきたもので，大型UNIXサーバで運用するためには課題も多い．

本論文では，サーバ用ウィルス検査ソフトウェアを著者らの大学において運用させた経験から，

このソフトウェアの問題点を明らかにし，それらの問題点を解消する方法および運用結果について述べ，有効性を示す．

以下，2節ではサーバ上でのウィルス検査ソフトウェアについて述べ，3節，4節で我々の大学のメールサーバおよびHTTPプロキシサーバ上での運用について述べる．

2 サーバ上のウィルス検査法

本節では，E-mailやWebページに添付されるウィルスを，組織のインターネットゲートウェイ上で検出・除去する方法について説明する．例として，本学で導入したトレンドマイクロ社のInterScan VirusWall[4]を用いる．

なお，本論文では，このようなウィルス検査システムが検出する対象を総称して「ウィルス」と呼び，これにはワームなど厳密にはコンピュータウィルスに分類しないものも含む．

検索方法：

リアルタイム検索と手動検索の2種類がある．**リアルタイム検索**は，HTTP, FTP, SMTP等の各プロトコルを介して転送されるファイルを，転送時にユーザへファイルが届く前に検索する方法である．一方，**手動検索**は，二次記憶装置内に蓄積されたファイルを一括して検索する方法である．

監視方法：

電子メールの場合，ウィルス検査ソフトウェアをインストールしたホストをその組織のSMTPサーバとする．受信したメールに添付ファイルがあればウィルス検査が行われ，問題がない場合にはそのまま元のメールサーバに配送される．なお，VirusWallでは，元のメールサーバのソフトウェアがsendmailであれば，同一ホスト上で稼動させるようにも設定できる．

一方，HTTP，FTPの場合は，ウィルス検査ソフトウェアがプロキシサーバとして機能する．ユーザのクライアントからウィルス検査ソフトウェアへ要求が来ると，そのまま元のプロキシサーバへ伝える．目的サーバ上のファイルがそのプロキシサーバ経由で戻ってくると，一旦蓄積してウィルス検査を行う．問題がない場合にはそのファイルをクライアント側へ転送する．

ウィルスの通知方法：

電子メールの場合，MIME形式でファイルが添付されていれば，ウィルスを含んでいたパートを削除し，メールの先頭に削除した旨説明する文章を添付する．

一方，HTTPの場合には，ウィルスを含んでいたファイルはクライアントに返さず，代わりに削除した旨説明する文章をHTML形式のファイルとして返す．

3 電子メールのウィルス検査

我々の大学では，2000年1月から学内の全ユーザを対象として，電子メールに添付されているファイルのウィルス検査を行っている．

3.1 電子メール検査の問題

電子メールのウィルス検査をVirusWall[1]を用いて行った場合に，本学で問題になった点を以下に述べる．

- メールヘッダーの配送情報

  通常のメールサーバは，メールを受信した際に時刻や接続相手などの情報をそのメールのヘッダー部にReceived: というタグを付けて追加する．接続相手のIPアドレスを逆引きしたホスト名を付けることもでき，これらの情報はトラブル発生時に有力な手掛かりとなることも多い．しかし，VirusWallはこのような情報の追加をしない．VirusWallから配送を受けるサーバでは手前の配送相手はわからないため，自組織に届く直前のメールサーバの逆引き情報はヘッダーに現れないことになる．なお，接続相手に関してはVirusWallのログに記録されているが，大量のメール配送を行うサーバではこのログと付き合わせて調べることは極めて困難である．

- SPAM対策等の機能

[1]本学で運用に用いたバージョンは2.5および2.6であり，これ以降のリリースで解決されたとされている問題もあるが，どのように解決されたか未確認である．

本学で運用を開始した当時のバージョンでは，SPAM メール対策機能を備えていなかった．最近では，組織の出入口となるメールサーバでは SPAM 対策などのセキュリティ強化機能は必須であり，セキュリティ上の不備な点ができると直ちに大量の不正メールを受信することも珍しくない．

- インストール

  通常， sendmail の起動は `/etc/init.d/sendmail` にあるスクリプトで行われる．VirusWall と sendmail を同一ホストに置く場合はパイプで接続されるため，sendmail の起動方法を変更する必要があり，VirusWall のインストーラは`/etc/init.d/sendmail` を自動的に修正する．しかし，本学の場合，メールサーバのダウンタイムを最小にするために高可用性機能を備えたクラスタ構成をとっており，sendmail の起動方法も通常とは異なる．そのため，インストーラが行った変更が理由で，システムダウン時の自動切替が働かないという障害が発生した．

- ログ

  UNIX では，ほとんどのサービスのログは OS が提供する syslog 機能を利用して蓄積されているが，VirusWall では独自の方法でログを蓄積している．そのため，ログの整理や解析の際にこれまでのノウハウがそのまま利用できず，組織独自の関連ツール類を新規に開発することになる．

3.2 本学における構成

前節で述べた問題点を解消するために，図 1 に示す構成変更を行った．

本学では，学内のほとんどのユーザが利用する主メールサーバの他にいくつかのメールサーバが存在し，入口でこれらの振り分けを行っていた．即ち，ウィルス検査システム導入前は図 1 左側のような構成であった．

これを図 1 右側のような構成へ変更した．この構成は，以下の方針を実現したものである．

- ウィルス検査ソフトウェアは学外から直接アクセスできるところに置かない

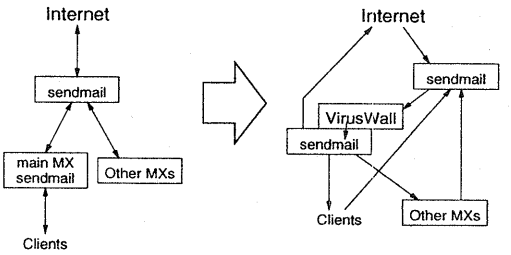

図 1: メールサーバの構成変更

- ウィルス検査は資源に余裕のある主メールサーバ上で行う
- 受信した全メールのウィルス検査を行うため，学内の各メールサーバへの配送は主メールサーバが行う

即ち， 2 つの sendmail によるメールサーバで VirusWall を挟み，一方は学内外からの受信用で，他方を学内外への発信用とした．これによって，学内外共にウィルス検査ソフトウェアに直接アクセスすることがなくなるため，従来通りの機能およびセキュリティを確保することが可能となった．

3.3 運用結果

本学では，2000 年 1 月から現在まで大学全体の主メールサーバ上での運用を行っている．2000 年 8 月末までの 8 ヵ月間の運用結果について述べる．

表 1 に示すように，8 ヵ月間で合計 207 個のウィルスを検出した．ただし，同一の発信・受信者から同一のウィルスが連続して送られる例が何度か観測できた．これは，1) 関連する内容を複数メールに分割して一度に送った，2) テストのための再送を繰り返す，などの理由と推測されるため，10 分以内に再送されたものはまとめて 1 件考えて処理した．

表 1: 検出ウィルスのタイプ別集計

分類	検出数
Office マクロ	73
Windows	67
VB スクリプト	49
MIME	18
計	207

また，検出したウィルスを分類した数も表 1 に

示す．ほとんどが Microsoft Windows や Microsoft Office を狙ったものであることがわかる．

表 2: 検出ウィルスの学内外別集計

	学内宛	混在	学外宛
学内発	31	2	7
学外発	166	1	0

表 2 は，ウィルスが検出された各メールの発信・受信者が学内か学外かで分類したものである．ただし，この判断はログに記録された発信アドレスと受信アドレスを調査し，自組織のドメイン名が含まれているか否かで判別しているため，メーリングリストなどで正しく判別できない可能性もある．

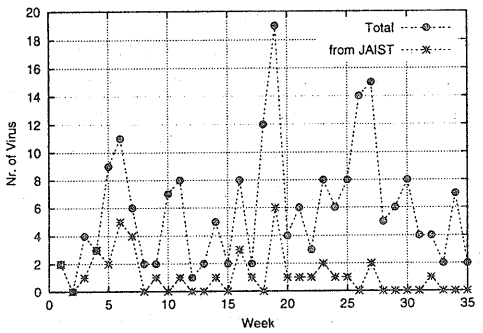

図 2: メールサーバにおける週毎のウィルス検出数

図 2 に，検出したウィルス数の時系列変化を示す．一方の折れ線がウィルスの総数で，他方が学内発メールの内数である．

運用期間の前半では，学外から受信する数が増えると，同時期に学内から発信する数も増える傾向がうかがえる．これは即ち，世の中で広まっているウィルスが学内でも繁殖していると考えることができる．その原因として，1) 検出スクリプトが対応する前に侵入された，2) 電子メール以外の手段で侵入した，という理由が考えられる．一方，運用期間の後半に関しては，この傾向が弱まってきていると言える．

図 2 のそれぞれのデータに対して回帰直線を計算すると，直線の傾きは，総数の場合が 0.08 であるのに対し，学内の場合は -0.05 であった．また，学内発が占める割合を計算してグラフ化すると図 3 となり，このデータの回帰直線の傾きは -1.54 であった．これらの結果から，インターネット上のウィルスは徐々に増加しているにもかかわらず，本学内で繁殖するウィルスは徐々に減少している，と見ることができる．

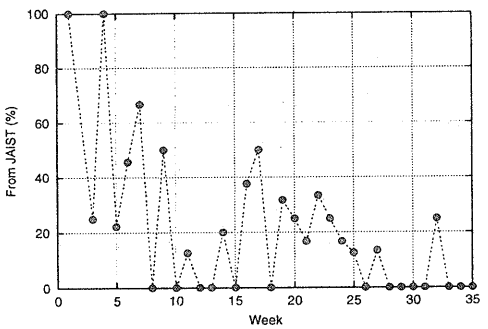

図 3: 週毎のウィルス検出数のうち学内発メールの割合

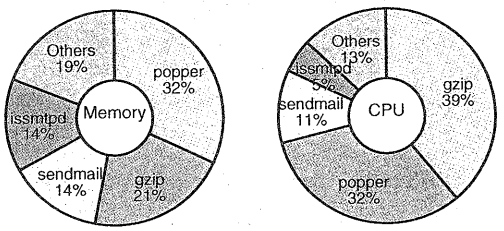

図 4: ウィルス検査プロセスが占めるメモリと CPU 時間の割合

図 4 は，ウィルス検査システムが稼動しているメールサーバ上で主要プロセスがメモリと CPU 時間をどの程度消費しているかを示したものである．これは，2000 年 4 月から 2000 年 8 月までの 5 ヵ月間，Solaris7 のアカウント機能を用いて集計した結果の平均である．図中でウィルス検査プログラムは `issmtpd` という名前になっている．これを見ると，メモリはある程度消費しているが，CPU 時間は `sendmail` の約半分で，POP サービスなどに較べてかなり小さく，全体としてシステムに大きな負荷とはなっていないことがわかる．なお，いずれも比較的大きく消費している `gzip` は，バックアップなどの目的で一時的に使用しているものである．

4 HTTP アクセスのウィルス検査

我々の大学では，2000 年 7 月から学内の一部のユーザを対象として，HTTP アクセスに対するウィルス検査の試験運用を行っている．

4.1 HTTP 検査の問題

HTTP アクセスのウィルス検査を VirusWall を用いて行った場合に，本学で問題になった点を以下に述べる．

- 上流サイトの選択

  本学のプロキシサーバでは，対象 URL に応じて上流の複数のプロキシサーバおよび目的サーバへの直接アクセスを自動選択するように設定している．これはプロキシソフトウェアである squid の機能を用いて実現している．しかし，VirusWall では上流の単一サーバもしくは直接アクセスの二者択一のみしか設定できない．

- アクセス制御

  ウィルス検査ソフトウェア自身がプロキシサーバとして機能するが，このサーバに対する細かなアクセス制御はできない．ファイヤウォールセグメント，DMZ 等に設置する場合，不正なアクセスを受けないように注意する必要がある．

- 遅延

  電子メールの場合には非対話的に配送が行われるが，Web ブラウザからの HTTP アクセスの場合には，対話的にファイル転送が行われる．そのため，通常のプロキシソフトウェアはパフォーマンスを重要視している．例えば，上流から受信したデータは逐次クライアント側へ送信し，遅延を最小限に押さえている．しかし，ウィルス検査ソフトウェアは，上流からファイル全体を受信し，ウィルス検査を終了した後に初めてクライアント側へ送信を行う．

  一般的な Web ブラウザでは複数のコネクションを同時に処理するため，通常のページではユーザが極端な不快感を感じることはあまりないとも考えられる．しかし，単一ファイルのダウンロード時には，ユーザから見ると，そのファイルのウィルス検査が終了するまで相手サーバが応答しないように見える．そのため，ファイルサイズが大きく時間がかかる場合には，ブラウザのタイムアウトやユーザがキャンセルすることもありうる．

- タイムアウト

  これまでにログに残っている約 180 万アクセスの内，約 1 万アクセスがタイムアウトしていた．これは全体の 0.59% であり，無視できるほど小さいとは言えない．

  ログには充分な情報が記録されておらず，どの URL へのアクセスがタイムアウトしたか正確には不明であるが，ウィルス検査の対象となっていない画像などのファイルもかなりタイムアウトしていると思われる．

4.2 本学における構成

前節で述べた問題点を解消するために，図 5 に示す構成変更を行った．

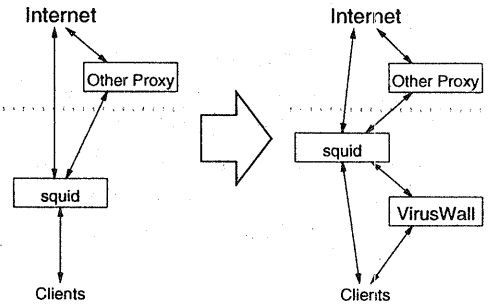

図 5: プロキシサーバの構成変更

図 5 の右側が導入後の構成である．この構成は，以下の方針を実現したものである．

- ウィルス検査ソフトウェアは学外から直接アクセスできるところに置かない
- 遅延やタイムアウトによるユーザへの影響を小さくするため，ウィルス検査を通過しない直接アクセスを許す
- 検査すべきファイルについては自動的にウィルス検査用プロキシサーバを経由するように，代表的クライアント用のプロキシ自動設定ファイルを提供する

このように，クライアントのプロキシ自動設定機能を利用することによって，ユーザが直接意識

することなく，ほとんどのアクセスを占める画像などのウィルス検査が不要なファイルについて従来通りのアクセスが可能となった．

ただし，この判別はアクセス前に行われるため，目的サーバから届く MIME タイプ情報などは参照できず，対象 URL に含まれるファイル名の拡張子部分のみから判別している．そのため，CGI 等の場合に正しく判別できない可能性がある．

5 おわりに

本論文では，電子メールや HTTP アクセスに含まれるコンピュータウィルスを検査するために，大規模な組織のサーバでも運用可能にする構成法について述べた．製品化されているウィルス検査ソフトウェアでは，従来の一般的なサーバソフトウェアが備えている性能やセキュリティ機能が充分ではないが，本論文の方法で従来のソフトウェアと組合わせて構成することによって，実運用可能となることを，本学の実際に運用した結果に基づいて述べた．

しかし，今回の方法のみではウィルスを 100 パーセント防御できない．実際，学外から受信する数が増えると，同時期に学内から発信する数が増える傾向も見られる．今後，ウィルスの検出率をさらに上げるためには，侵入された後の検出など，他の方法も併用する運用を行う必要がある．

謝辞

本研究を進めるに当たって，各サーバの構築等には田中友英君や何人かの学生の方々に協力していただきました．また，日常の管理業務では情報科学センター技官の方々にご協力頂いております．ここに深く感謝致します．

参考文献

[1] Frederick B. Choen. *A Short Course on Computer Viruses*. Wiley Professional Computing, second edition, 1994.

[2] B. C. Soh, T. S. Dillon, and P. County. Quantitative risk assessment of computer virus attacks on computer networks. *Computer Networks and ISDN Systems*, Vol. 27, No. 10, pp. 1447–1456, September 1995.

[3] Harold Thimbleby, Stuart Anderson, and Paul Cairns. A framework for modelling Trojans and computer virus infection. *The Computer Journal*, Vol. 41, No. 7, 1998.

[4] トレンドマイクロ株式会社. InterScan VirusWall for UNIX 操作マニュアル, 1998.