サーバにおけるコンピュータウィルス検査システムの設計と運用

敷田幹文[†] 井口寧[†] 松澤照男[†]

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ともない，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，UNIXサーバ上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我々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サーバの構成法を提案する．また，我々の大学において1年以上にわたって電子メールおよびWebアクセスのウィルスを検査してきた運用結果を分析し，本方法の有効性について議論を行う．

Design of Virus Scan System on Servers

Mikifumi Shikida,[†] Yasushi Inoguchi[†] and Teruo Matsuzawa[†]

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 UNIX server systems. In this paper, we describe problems of computer virus scanner for server, based on our experience on our university network. We propose new schemes for configuration of virus scanner for servers, which solve the problems. We describe analysis of result, which we scanned virus in E-mail and web access during more than one year. And we discuss effectiveness of our method.

1. まえがき

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ともない，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)~5)]．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きわめて難しい．

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[5)~7)]．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，UNIXサーバ上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我々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る．また，我々の大学において1年以上にわたって受信・送信されたすべての電子メールおよびWebアクセスを対象に，提案するウィルス検査システムを運用し，結果を分析することによって，我々の方法の有効性について議論を行う．

以下，2章ではサーバ上での従来のウィルス検査ソフトウェアについて述べ，3章，4章でこれまでの問題を克服するメールサーバおよびHTTPプロキシサーバの設計法を提案し，実際に我々の大学で運用した結

† 北陸先端科学技術大学院大学情報科学センター
Center for Information Science, Japan Advanced Institute of Science and Technology

果を分析する．最後に 5 章で本論文の方法の有効性に関する議論を行う．

2. サーバ上のウィルス検査法

本章では，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，我々の大学で導入したトレンドマイクロ社の InterScan VirusWall[8] 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 などの各プロトコルを介して転送されるファイルを，転送時にユーザに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に要求が来ると，そのまま元のプロキシサーバに伝える．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，いったん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に転送する．

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

本学では，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☆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分からないため，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きわめて困難である．
- SPAM 対策などの機能
  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ただ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

☆ 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．

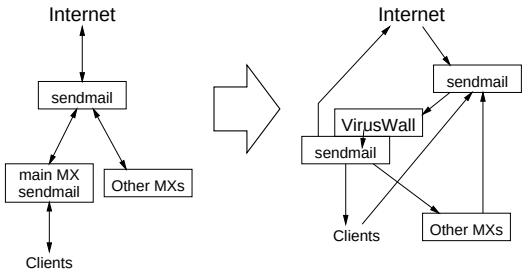

図 1 メールサーバの構成変更
Fig. 1 System structure of our mail server.

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ほか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．すなわち，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 右側のような構成に変更した．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．
- 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．

一般的な構成法では，メールサーバ上の sendmail をウィルス検査ソフトウェアに入れ替える．これに対して我々の方法では，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．図 1 右側は複雑な制御を行っているように見えるが，2 つの sendmail と VirusWall の全体で 1 つのメールサーバの働きをしているにすぎず，メールの出入り口はそれぞれ 1 カ所のみである．

この構成を実現するためには，各ノードで以下の設定を行う．1) 上流の sendmail は入口専用であり SPAM 対策などを施すが，メールの配送は静的に VirusWall へ送るのみである．2) VirusWall は受け取ったメールのウィルス検査のみを行い，これも静的に次の sendmail へ配送する．3) 下流の sendmail は出口専用であり，受け取ったメールを学内の他のメールサーバやスプールへ配送する．

これによって，学内外とも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，従来どお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．ここで，上流 sendmail の入口部分と下流 sendmail の出口部分の設定は，VirusWall 導入前とほぼ同様の設定内容でよい．

表 1 12 カ月間の運用結果
Table 1 Result for one year.

平均配送メール数	13,093 通/日
スキャンしたファイルの総数	393,489 個
スキャンしたファイル数の平均	1,078 個/日
ファイル添付率	8.23 %
検出ウィルスの総数	1,649 個
平均検出ウィルス数	4.5 個/日
添付ファイルのウィルス感染率	0.42 %
ユーザ数	約 1,300 人
ウィルスを受信した学内ユーザ数	381 人
受信者の平均受信回数	4.43 回
ウィルスを発信した学内ユーザ数	166 人
発信者の平均発信回数	1.60 回

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．2001 年 4 月末までの約 16 カ月間の運用結果について述べる．

3.3.1 運用期間全体の分析

これまでに運用してきた 16 カ月の中で，3 月末を境にユーザの入れ替わりが多く，ユーザの計算機利用状況に 1 年間の周期性が予想されるため，2000 年 4 月から 2001 年 3 月までの 12 カ月のみに限定して集計した結果を**表 1** に示す．

この結果から，ユーザ 1 人あたりで計算すると，1 年間に 平均 302 個 の添付ファイルを扱うこととなり，添付ファイルのウィルス感染率から，1.27 個 のウィルスを受け取ることが推測される．すなわち，各ユーザは平均でも年に 1 度はウィルスに遭遇するといえる．なお，後に述べるように，ウィルス数は急速に増加しており，インターネット上の電子メールユーザにとって無視できない状況になっているといえる．また，我々の大学内では，日常的に UNIX を利用し，UNIX 上で電子メールを読み書きしているユーザが多く，Windows 上でメールを読み書きするユーザはおおよそ半数以下であると推測している．したがって，組織全体

表 2 ウィルス別検出数
Table 2 Numbers of detected viruses.

503	TROJ_HYBRIS.B
219	TROJ_MTX.A
94	TROJ_NAVIDAD.A
52	VBS_KAKWORM.A
51	TROJ_NAVIDAD.E
38	TROJ_PRETTY_PARK
37	O97M_TRISTATE
35	TROJ_SKA
34	TROJ_HYBRIS.D
24	TROJ_HYBRIS.A
20	VBS_LOVELETTER-O
⋮	⋮
1,326	合計

表 3 検出ウィルスの実装方法別集計
Table 3 Numbers of categorized viruses.

分類	検出数
Windows 実行形式	1,002
Office マクロ	146
VB スクリプト	129
JavaScript	1
MIME	48
計	1,326

で Windows 環境に統一し，電子メールでのファイル添付を多用して業務を行っている組織では，本学での結果よりも高い確率となることが予想できる．

一方，16 カ月間全体では，合計 1,864 個のウィルスを検出している．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頻繁に観測できた．これは，1) 関連する複数ファイルを 1 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 件と考えて処理した．その結果，**表 2** に示すように，合計ウィルス検出数は 1,326 個であった．以降はこの条件で処理した結果について述べる．これらのウィルスを，ウィルスの種類ごとに集計し，検出数が上位のものを表 2 に示す．最近騒がれている HYBRIS, MTX，NAVIDAD が上位を占めていることが確認できる．

また，検出したウィルスを，その実装方法によって分類した数を**表 3** に示す．ほとんどが Microsoft Windows や Microsoft Office などを狙ったものであることが分かる．これ以外の分類方法として，広がる方法や目的（影響）などによる分類も考えられるが，一般性のあるそれぞれの明確な定義がなく，境界も曖昧であるため，ウィルス情報を提供する各団体[9),10)] によっても分類が異なっているのが実情である．

表 4 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．

表 4 検出ウィルスの学内外別集計
Table 4 Numbers of viruses into/out-of our organization.

	学内宛	混在	学外宛
学内発	87	3	42
学外発	1,229	39	5

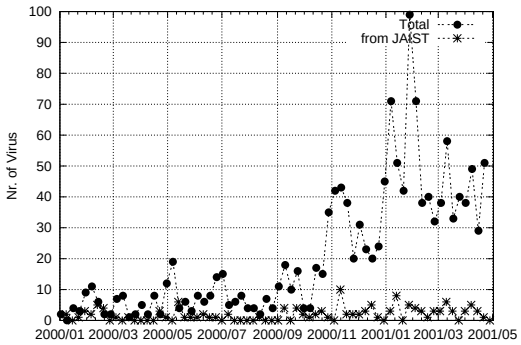

図 2 メールサーバにおける週ごとのウィルス検出数
Fig. 2 Weekly detected viruses.

3.3.2 時系列分析

検出したウィルス数の時系列変化を**図 2** に示す．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．縦軸は 1 週間に検出したウィルス数である．

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．これはすなわち，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．

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 0.78 であるのに対し，学内の場合は 0.029 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** となる．これらの結果から，インターネット上のウィルスは急激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あまり増加していない，と推測することができる．

次に，インターネット上のウィルスがどのような速度で広がっているかを調査するため，個々のウィルスごとに検出数の時系列変化を調査した．表 2 に示した

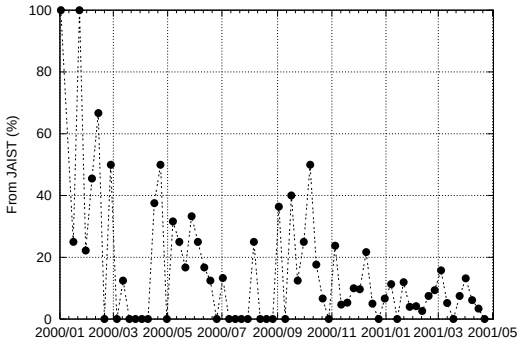

図 3 週ごとのウィルス検出数のうち学内発メールの割合
Fig. 3 Percentage of viruses from our organization.

表 5 個別調査した 6 種のウィルス
Table 5 Major six viruses.

ウィルス名	定義ダウンロード日
TROJ_HYBRIS.B	2000/11/8
TROJ_MTX.A	2000/8/30
TROJ_NAVIDAD.A	2000/11/8
TROJ_NAVIDAD.E	2000/11/30
TROJ_HYBRIS.A	2000/11/8
VBS_LOVELETTER-O	2000/5/5

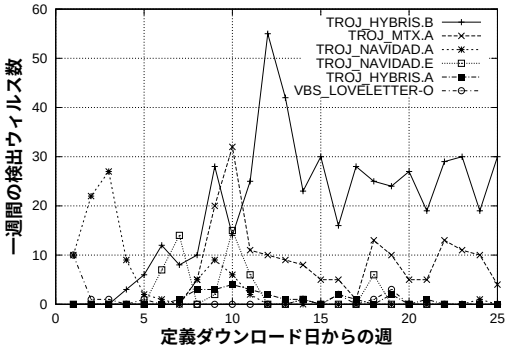

図 4 定義日からの週ごとの検出ウィルス数
Fig. 4 Weekly graph for major six viruses.

検出数が多いウィルスのうち，運用期間中に発見されて，その対応日が分かっている**表 5** の 6 種について調べた．ただし，各ウィルスが発生した正確な日付は不明であり，その後ウィルス検出ソフトウェアメーカ側で認識し，対応する定義が公開されることになる．そのため，本学側で認識できるのは定義ファイルが公開された後であり，表 5 の日付は定義をダウンロードした日になっている．なお，定義ファイルの更新確認は毎日行っており，公開されてからの時間的遅延は 24 時間以内である．

上記 6 種のウィルスについて，時系列変化をグラフ化したものを**図 4** に示す．これを見ると，多くのウィルスは発生してから実際に身近に広まるまでに数週間の時間差があるので，本システムによる対応で十分間に合っていると考えられる．また，いったん広まった後は徐々に減少する傾向にある．ただし，2000 年 5 月初めに爆発的に広まってニュースとなった LOVELETTER ウィルスの場合は，定義ファイルをダウンロードした後の第 1 週に集中している．さらにログの詳細を調べた結果，ダウンロードした当日にも 3 個検出されたことが分かった．このようなケースもあるため，ウィルス検出ソフトウェアが対応する前に学内に侵入する可能性も否定できないことが分かる．

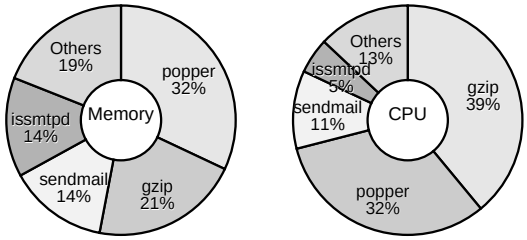

図 5 ウィルス検査プロセスが占めるメモリと CPU 時間の割合
Fig. 5 Memory usage and CPU time of virus scan system.

3.3.3 サーバの負荷分析

図 5 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 カ月間，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 サービスなどに比べてかなり小さく，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分かる．なお，いずれも比較的大きく消費している `gzip` は，バックアップのために一時的に使用したものである．

4. HTTP アクセスのウィルス検査

本学では，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 などに設置する場合，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．たとえば，上流から受信したデータは逐次クライアント側に送信し，遅延を最小限におさえている．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に送信を行う．
  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 万アクセスのうち，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いえない．
  ログには十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 6** に示す構成変更を行った．

図 6 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．

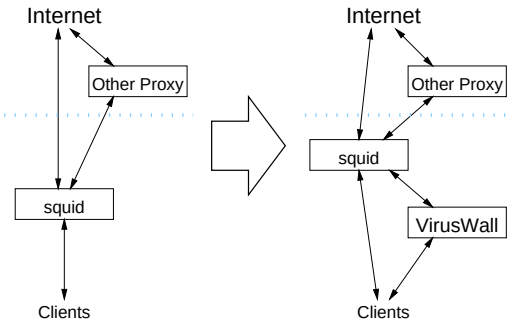

図 6 プロキシサーバの構成変更
Fig. 6 System structure of our proxy server.

- 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．

HTTP アクセスにおいては，たとえば JPEG 画像などウィルスが含まれている可能性がきわめて低く，**検査をする必要のないファイル**がある．VirusWall では，上流へ HTTP でアクセスした際に返される Content-Type 情報を利用し，音 (audio/*)，画像 (image/*)，動画 (video/*) など，指定したタイプの場合には検査しないで通過させる機能を持っている．しかし，我々のテストではそのような検査しないファイルの場合にも遅延やタイムアウトが発生していた．

一般的な構成法では，プロキシサーバ上のソフトウェア（squid など）をウィルス検査ソフトウェアに入れ替える．すなわちすべてのアクセスがいったん VirusWall を通過するため，前述の問題によりスムーズなアクセスとならない．これに対して我々の方法では，VirusWall をこれまでのプロキシサーバの下流プロキシサーバとし，**各クライアントから両方へアクセスできる**ようにした．

この構成を実現するためには，各ノードで以下の設定を行う．1) 上流のプロキシサーバは学外の上流プロキシサーバにアクセスを行うもので，導入前の設定とまったく同じである．2) VirusWall はクライアントから受け取ったリクエストを静的に上流プロキシサーバに伝え，返信はウィルス検査の後クライアントに送られる．3) 各クライアントでは，JavaScript によるプロキシ自動設定スクリプトによってウィルス検査の

必要性を判断し，必要であれば VirusWall にリクエストし，それ以外は上流のプロキシサーバに直接リクエストを出す．

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どおりのアクセスが可能となった．

ただし，この判別はクライアントがリクエストを出す前に行われるため，目的サーバから届く Content-Type 情報などを参照できず，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．具体的には，Windows 実行形式（com，exe），Office 文書（doc，xls）などを検査している．そのため，CGI など，ファイル内容と異なる拡張子が URL に付いていた場合には正しく判別できない可能性がある．

4.3 試験運用

本学では，運用上の理由により HTTP アクセスの検査は全学での本運用には至っていないが，2000 年 7 月から現在まで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．

テストユーザは数十人であるが，現在までにウィルスは検出できていない．本システムの導入を検討していた 1999 年頃は，たとえば国立機関の公式ホームページ上でウィルスに感染した文書が公開されたこともあったが，最近はウィルスに対する理解が広まり，そのようなことが減ったためと思われる．文献 4) によると，電子メールによるウィルスは 1999 年まではウィルス報告の 4 割程度で残りは他のプロトコルによるものであったが，2000 年から状況が変わり，現在は電子メール以外によるウィルスは全体の 1 割以下であると報告されている．また，テストユーザのほとんどは本学事務局職員で，業務に関係した特定のページをアクセスすることが多い．これに対して，本システムを全学で本運用すると様々なページへの参照が発生し，ウィルス検査が効果を発揮すると予想している．

5. 議論

本論文の方式を，関連研究や一般的構成法と比較し議論を行う．また運用の結果得られたウィルス情報について述べる．

5.1 電子メールのウィルス検査

組織内のメールサーバ上でのウィルス検査システムの導入例は，文献 6) や文献 7) でも報告されている．文献 6) では一般的なインストール方法を採用している．すなわち，メールサーバ上の **sendmail をウィルス検査ソフトウェアに入れ替える**という方法で，導入前に sendmail で行っていた処理をすべて検査ソフトウェアに行わせる必要がある．文献 6) では本論文と異なる商品を導入しているが，SPAM 対策の不備，ログ機構の欠陥，配送制御の制限が多いことなど，本論文と類似の問題が指摘されている．

これに対し，我々の方法では，図 1 右側に示したように，**ウィルス検査ソフトウェアを 2 つの sendmail で挟む**構成とした．この構成では，ウィルス検査ソフトウェアはウィルスの検査のみを行い，配送制御や SPAM 対策などの設定はすべて sendmail 側で行う．また，ログの記録も導入前と同様 sendmail で行われる．これによって，単に検査ソフトウェアの問題を回避するというだけでなく，導入前に蓄積していた設定や障害対応に関するノウハウや，ログ解析などの補助ツールもそのまま利用できるという利点がある．また sendmail は広く利用されているため新たな情報の入手も容易である．本方式によってサーバの台数が増えるという欠点はあるが，組織内サーバの管理者にとって，安定したサービスの提供や管理コストの削減が必要であり，本論文の方式による利点は大きい．

5.2 HTTP アクセスのウィルス検査

HTTP アクセスのウィルス検査ソフトウェアでは，検査サーバ自身がプロキシサーバとして働き，上位のプロキシサーバもしくは目的 web サーバとクライアントの間に入って通過するファイル内のウィルスを検査する構成が一般的である．扱うファイルには様々な種類があり，音や画像などにはウィルスが感染している可能性はきわめて低いため，検査サーバ内でファイルタイプによって判別し，感染の可能性が高いファイルのみの検査が行われている．しかし，我々のテストでは，検査が行われず素通りするファイルにおいても遅延の影響があり，テストユーザが体感できる程度の性能劣化があった．HTTP アクセスの場合には，電子メールとは異なり対話型ユーザインタフェースであるため，遅延などがユーザに与える影響が大きいと考えられる．

これに対し，本論文の方法では，ウィルス検査サーバより手前のクライアント内でファイルの種類を判別し，感染の可能性が低い場合にはウィルス検査サーバを通さない構成とした．これによって，ほとんどのファイルでは従来とまったく同じ性能でアクセスでき，感染の可能性が低くない場合のみ自動的に検査が行われるシステムが構築できた．クライアント内で判別する機構はブラウザのプロキシ自動設定機能を利用しているので，設定スクリプトはネットワーク上で共有され

ており，クライアント側のメンテナンスコストもほとんどない．

ただし，検査サーバ上で判別する場合には，実際に上流へアクセスした後に HTTP プロトコルで通知されるファイルの種類（Content-Type）を利用しているのに対し，クライアント側で判別する場合には，上流へアクセスする前に判別する必要があるため URL の文字列情報のみから判断している．したがって正しく判断できない場合がありうる．

本方式の妥当性を明らかにするために，実際にアクセスされたファイルの URL において，VirusWall 内とクライアント側でウィルス感染の可能性をどう判断するかシミュレーションを行った．URL としては本学で実運用しているプロキシサーバのログを用いて最近実際にアクセスされた約 4 万件を利用した．その結果，ほとんどの URL において判別が一致していたが，VirusWall で検査が不要とするファイルに対してクライアント側で要検査と判断する場合が全体の 0.18%，検査が必要とするファイルに対してクライアント側で検査不要と判断する場合が 0.40%あった．不一致の場合を個別に調査したところ，前者は CGI スクリプトがテキストファイルや画像ファイルを出力する場合で，後者は各種アプリケーションのデータファイルがほとんどであった．後者は VirusWall が不明なファイルタイプをすべて検査対象としていることに起因しているが，電子メールのウィルス分析結果から，ほとんどのウィルスは特定の OS，アプリケーションを狙ったものであることが分かっている．以上の結果から，ファイルの内容を参照せずに URL のみから判断してもほとんどの場合に問題ないといえる．少数の場合には問題となることがあるが，本方式によってユーザが体感できる影響を削減できるため，ウィルス検査を実施するユーザの割合が増えれば，組織全体では検査されないアクセスが減るといえる．

5.3 インターネット上のウィルス

本論文では，1 つの大学全体の実運用環境においてやりとりされたすべての電子メールをもとに，コンピュータウィルスがどの程度含まれているかを調査した．これまでも，国内の組織におけるウィルス被害の報告に基づく統計[4),10),11)] は存在したが，これらはユーザが被害に気付いて，さらに被害情報収集機関に報告を行った場合のみを扱っている[12)]．しかし，ウィルスはその特性上，ユーザが気付かないうちに感染し，さらに別のユーザに伝えることが多いため，被害報告だけでは実際に起きている影響の程度を調べることができない．インターネット上におけるウィルスの流量の実際の数値は本論文で初めて明らかになったといえる．ウィルス検出の実運用結果を基に分析を行うことによって，コンピュータウィルスの問題が，短期間のうちに現在のインターネットでのきわめて深刻な問題となり，さらに急速に影響が拡大しつつあることを明確にした．

6. むすび

本論文では，電子メールおよび 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，サーバ上でウィルス検査システムを効果的に運用する新たな構成法を提案した．現在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，セキュリティ機能，およびその他の運用管理に関する機能が十分ではないが，本論文の方法で従来のソフトウェアと組み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，本学において実際に運用した結果に基づいて述べた．

しかし，サーバ上の検査のみではウィルスを完全に防御することができない．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 本研究を進めるにあたり，各種サーバのログ情報解析などにご協力いただきました本学情報科学センターの上埜元嗣技官，間藤真人技官に深く感謝いたします．

参考文献

1) Choen, F.B.: *A Short Course on Computer Viruses*, 2nd edition, Wiley Professional Computing (1994).
2) Soh, B.C., Dillon, T. S. and County, P.: Quantitative risk assessment of computer virus attacks on computer networks, *Computer Networks and ISDN Systems*, Vol.27, No.10, pp.1447–1456 (1995).
3) Thimbleby, H., Anderson, S. and Cairns, P.: A Framework for Modelling Trojans and Computer Virus Infection, *The Computer Journal*, Vol.41, No.7 (1998).
4) 情報処理振興事業協会：2001 年上半期ウイルス発見届出状況．http://www.ipa.go.jp/security/txt/attach/2001_07-1.html
5) 敷田幹文，井口 寧，三輪信介，丹 康雄，松澤照男：大規模サーバにおけるウィルス検査システムの運用法，情報処理学会研究報告 DSM-19, pp.7–12 (2000).

6) 山守一徳，太田義勝：SPAM メールの不正中継防止対策とウィルス対策，分散システム/インターネット運用技術シンポジウム論文集，情報処理学会，pp.109–114 (2001).
7) 広島大学情報メディア教育研究センター．http://www.media.hiroshima-u.ac.jp/
8) トレンドマイクロ株式会社：InterScan VirusWall for UNIX 操作マニュアル (1998).
9) トレンドマイクロ株式会社：ウィルスデータベース．http://inet.trendmicro.co.jp/virusinfo/default1.asp
10) 株式会社シマンテック：定期ウィルスレポート．http://www.symantec.com/region/jp/news/year01/010705b.html
11) トレンドマイクロ株式会社：マンスリーウイルスランキング． http://www.trendmicro.co.jp/virusinfo/monthly_ranking/mvr010705.htm
12) 情報処理振興事業協会：ウイルス対策．http://www.ipa.go.jp/security/isg/virus.html

(平成 13 年 5 月 9 日受付)
(平成 13 年 10 月 16 日採録)

敷田 幹文（正会員）

1965 年生．1995 年東京工業大学理工学研究科情報工学専攻博士後期課程修了．博士（工学）．同年，北陸先端科学技術大学院大学情報科学センター助手．2001 年，同助教授．大規模分散システム，グループウェアに関する研究に従事．ACM，日本ソフトウェア科学会各会員．

井口 寧（正会員）

1967 年生．1991 年東北大学工学部機械工学科卒業．1997 年北陸先端科学技術大学院大学情報科学研究科博士後期課程修了．現在，同大学院情報科学センター助手．情報環境の構築および維持・管理，ならびに超並列システムの実装方式に関する研究に従事．また，1994 年〜1997 年日本学術振興会特別研究員として超並列システムの相互結合網に関する研究を行う．博士（情報科学）．IEEE，電子情報通信学会各会員．

松澤 照男（正会員）

1948 年生．1973 年信州大学大学院工学研究科修士課程修了．同年信州大学医学部助手．1986 年沼津工業高等専門学校助教授．1991 年北陸先端科学技術大学院大学助教授．1995 年同教授．情報環境の構築および維持・管理，数値流体力学におけるハイパフォーマンスコンピューティングの研究に従事．医学博士．日本機械学会，日本数値流体力学会，日本流体力学会等各会員．