SPAMメールの不正中継防止対策とウィルス対策

山守 一徳[†]， 太田 義勝[††]

本学で実施したSPAMメールの不正中継防止対策とウィルス対策について詳細に述べ，問題点を明らかにする． 採用した不正中継防止のための手法は，学内メールサーバへのすべてのメールを大学入り口のメールゲートウェイで中継させる手法である．実現には３行に亘ってDNSサーバのMX行による設定を書き直し，かつメールサーバの配送経路をSTATIC設定する方法を採用した．ファイアウォールのルールにより学内のメールサーバは学外から直接にメールを受信できなくしている．類似した方式は既にいくつかの大学で実現されているためそれらとの比較を行う． また，採用したウィルス対策のための手法は，メールゲートウェイにウィルスチェックサーバを導入し，添付ファイル付きメールをチェックする手法である．この手法を採用するにあたり比較検討した事項について述べる．さらに，ウィルスチェックサーバを導入してみてわかった問題点について報告する． 最後に，本学で実施した方法は，不正中継は防ぐことはできるがメールアドレスを騙ったSPAMによるDoS攻撃を防ぐことはできないなど問題点が残されており，それらの残された課題の対策案について述べる．

Open Relay Countermeasures for SPAM Mail and Virus Countermeasures

Kazunori YAMAMORI[†], Yoshikatsu OHTA[††]

We performed open relay countermeasures for SPAM mail and virus countermeasures in our university. This paper describes its detail and makes its problem clear. The open relay countermeasure adopted here is a method that all mails to inner mail servers are relayed by a mail gateway at the entrance of our university. In the implementation, we modified 3 MX lines of DNS severs and added STATIC relay of mail servers. And the inner mail servers cannot receive mails from outside directly because of firewall rules. Similar methods were performed in other universities. This paper describes comparison amomg those methods. The virus countermeasure adopted here is a method that virus check server is installed in the mail gateway. The virus check server checks all mails with additional files. This paper describes comparison among other implementations. And it describes problems that we could find after introducing the virus check server. Lastly, our method has a problem that it cannot defense DoS attack of SPAM mail which lies about the mail address. We propose an idea for the problem.

1 はじめに

電子メールの利用が急速に広まる中でSPAMメールという受け手にとって迷惑なメールが届けられる問題が跡を絶たない状況にある．SPAMメールはメールサーバの中継機能を使って届けられることが通常であり，メールサーバの管理者は，不正な中継に使われないように注意を払うことが責務である．しかし，メールサーバの管理者の技量が，それほど高くないことがよくある．特に大学では，研究室単位にメールサーバを立ち上げ，その管理者が実際には学生である場合に，卒業と伴に管理ができない状態になってしまうことがよく見受けられる．また，マシン管理者が意識していないのにsendmailなどのMTA (Mail Tarnsfer Agent) が自動起動されていることもある．そのようなメールサーバを狙っての不正中継利用者が跡を絶たず，不正に利用された場合はサーバ管理者の責任であるとして高を括っている訳にはいかないのが，大学全体のネットワーク管理者の悩みである．

† 三重大学 情報処理センター
Information Processing Center, Mie University
yamamori@cc.mie-u.ac.jp
†† 三重大学 工学部
Faculty of Engineering, Mie University
ohta@cs.info.mie-u.ac.jp

そこで，学内の至る所にあるメールサーバを学外から直にメールを受信しないようにし，一旦，大学入り口の１か所のメールゲートウェイでメールを受信してから配送する方式を採用し実行に移した．これにより，学内の至る所にあるメールサーバが不正中継防止対策を施してあるか心配することがなくなり，大学入り口の１か所のメールゲートウェイのみ不正中継防止対策を強固に行えばよいこととなった．

一方，ネットワークを介して流れ込むコンピュータウィルスについても，ますます数が増えてきている傾向にあり，悩ましい問題である．パソコン自身にウィルス駆除ソフトをインストールすることが増えてはきているものの，バージョンが古かったりパターンファイルが古かったりして駆除対策は後追いの形になってしまっている．最近は，各教官が電子メールアドレスを公開していることもあり，添付ファイルにウィルスを忍ばせて，いたずらでウィルスを送ってくることも心配され，ネットワークの健全な運営のためにはこの対策も必須のものとなってきている．そこで，本学ではウィルスチェックサーバを大学入り口のメールゲートウェイにインストールし，メールに付いてくるウィルスをそこで除去することを行った．

以下では，それらの対策を詳細に述べ問題点を明らかにする．

2　不正中継防止対策

2.1　メール受け口の１本化

本学では，メールサーバの数は142台ある．それらのメールサーバが学外からのメールを直接受け取るのでなく，一旦，大学入り口にある窓口役のメールゲートウェイで受け取り，そこから配信する方式を採用した．その実現のために，学内すべてのDNSサーバの中のMX行の書き直しを行い，すべてのメールサーバのMXの指定を窓口役のメールゲートウェイに向けた．

また本学では，トップレベルから直下にあるドメインの数は，18個あり，その配下にあるドメインは150個ある．窓口役のメールゲートウェイからは直下にあるドメインのメールサーバへ配送し，そのメールサーバは，さらにその下にあるサブドメインのメールサーバへ配送する方式を採用した．そのため，配送を行うメールサーバは，STATIC設定の機能を用い配送経路を指定した．この方式の良い点は，末端のメールサーバの変更に関して，窓口役のメールゲートウェイの配送経路を変更しなくても良い点にある．この方式を採用した理由は，末端のメールサーバは変更が発生しやすく，追加なども各学部での裁量に任せてあるため，柔軟に運用されてきた実情があったからである．

2.2　ファイアウォールによる遮断

MXの行をすべて窓口役のメールゲートウェイに向けたとしても，不正中継利用者がMXを使わずにメールを送ってくる場合も考えられる．25番ポートを指定し，メールサーバにtelnetすることでそのことは可能である．そこで，窓口役以外のメールサーバは，学外から直接にメールを受け取らないようにファイアウォールで遮断を行った．具体的には，ポート番号25番の届け先に持つTCPプロトコルについて窓口役以外のIPアドレスを届け先とするデータを遮断する．ただし，学内には研究に用いるため遮断して欲しくないメールサーバも存在するため，それは例外とすることにした．

2.3　メールゲートウェイの２重化

学外からメールを受け取るメールゲートウェイを１本化することは，そのメールゲートウェイが停止したときに全学でメールを受信できないという欠点が存在する．本方式を採用するにあたり学内から最も反対意見が強かったのはこの点である．そこで，メールゲートウェイを２重化することを行った．本来の窓口役のメールゲートウェイが止まったときに，バックアップ用のメールゲートウェイによって学外からメールを受け取り学内へ配送することにした．このため，各メールサーバを指定するMXの行は本来のメールゲートウェイだけでなく，バックアップ用のメールゲートウェイへも指定を追加することになった．

なお，採用した方式では，トップレベルから直に配送されるメールサーバがさらにその配下に配送するために，その中間メールサーバが停止したときも末端までメールが届かないという問題が起きる．この問題の解決のためには，中間のメールサーバも２重化することが考えられるが，結果的に後述するウィルスチェックサーバの設定によって

そこまで必要とされなくなった.

2.4 設定方法

今回の実現のためには，DNS サーバの中の設定で，FQDN に対する MX 行指定を変更することと，配送するメールサーバの中の設定で，STATIC にメールを配送する設定を行うことが必要である．以下に順に述べる．

（1）MX 行の変更

DNS サーバの中で，/etc/named/ ディレクトリの下に named.conf ファイルで指定されたファイル名が存在し，その中に MX 行の記述を使って，メールサーバのマシン名を指定している箇所が存在する．その行を 3 行の形に変更する．通常は図 1 のように記述をしている．その箇所を図 2 のように変更する．

```
IN  MX  0  メールサーバ名.
```

図 1　対策前の MX 行

```
IN  MX  0  メールゲートウェイ名.
IN  MX  10  待機系のメールゲートウェイ名.
IN  MX  20  メールサーバ名.
```

図 2　対策後の MX 行

（2）STATIC 配送の設定

メールサーバの中の設定で，sendmail.def の def ファイルを使って説明すると，

```
STATIC_ROUTE_FILE=static-route
```

と任意のファイル名 (この例では static-route) 指定し，その static-route のファイルの中身に

```
STATIC  ドメイン名 smtp:[メールサーバ名]
```

と書き，CF コマンドを使って sendmail.cf を作成する．static-route のファイルは sendmail.cf と同じ場所に置く．

2.5 他の方法との比較

MX の行を書き換えてメールの受け口を 1 本化する方法には，多くの方法が存在する．N 大学 [1, 2] においては，学外向け DNS と学内向け DNS を用意し，学内向け DNS から学内の全ての MX のデータを自動的に収集し，窓口役のメールゲートウェイに向けて書き直した MX のデータを学外向け DNS の中に自動記述させることで，外から届くメールはその窓口役のメールに集約できるようにしている．この方法は，学外向け MX の自動生成ソフトを構築しなければならない点が問題である．このソフト構築が技量を要するため，本学では採用をしなかった．

一方，O 大学 [3] では，図 3 のような記述をしており，本学とは MX の行の並び順に違いがある．

```
IN  MX  0   メールサーバ名.
IN  MX  10  メールゲートウェイ名.
```

図 3　O 大学の MX 行

この設定をした後にメールサーバに直接届けられる経路をファイアウォールで遮断することにより，学外からはメールゲートウェイのところへメールが配送されるようになる．この方式は，導入時の変更作業が少ないという利点がある．しかし，ファイアウォールで遮断することが前提となっており，遮断ログが多発するところと遮断をしない状態になると不正中継に使われる危険が発生するところが問題である．特に本学の場合，ファイアウォールは 2 重化されていないため，ファイアウォール故障時には古いルータへ物理的に置き換えるという策を取っているので，その事態が起きたときに，学内のメールサーバが一斉に外から見えることになり，不正中継に使われる危険性が高い．よって，本学ではその策を採用することができない．

本学で採用した方式は，MX 行の書き換えと中継するメールサーバの STATIC 配送設定の作業を伴うため，学内の DNS サーバおよびメールサーバ管理者の同意が必要である．幸いにも本学は，中規模クラスの大学であることもあり，サーバの台数も極端には多くなく，それぞれの管理者の同意も得られたので本方式を採用することができた．

3 ウィルス対策

3.1 ウィルスチェックサーバの導入

不正中継防止対策のために導入された窓口役のメールゲートウェイをメールが通過することを利用して，そのメールゲートウェイ上でウィルスチェックを行うこととした．通過するすべてのメールの添付ファイルにコンピュータウィルスが含まれていないかを調べ，含まれていた場合には添付ファイルを削除または修復してから，本来の届け先へメールを送ることを行う．導入したソフトは，Symantec 社の NortonAntiVirus for Solaris Gateways である．通過するメールをウィルスチェックサーバソフトへ

取り込む方法は，そのマシン上のポート番号25番のsendmailプロセスの代わりに，ウィルスチェックサーバの専用プロセスが動いてポート番号25番に応答するという方法である．NortonAntiVirus for Solaris Gatewaysでは，Solaris上でsendmailに代わるプロセスが動き，さらに添付ファイル中のウィルスのチェックとウィルスのパターンファイル更新処理を行う．WindowsNTServer上では検出されたウィルスが新種のものであるか調べ，Symantec社へ新種報告のメール発信ができる．Solarisマシンはメモリーが多い方が良いとのことによりUltra-Sparc II 440MHz，メモリ512MB，ハードディスク18GBのワークステーション（GP7000Sm10）を利用している．WindowsNTServerマシンはPentium III 600MHz，メモリ256MB，ハードディスク20GBのDOS/Vパソコン（PRIMERGY ES210）を利用している．

3.2 比較検討

導入にあたり比較検討した点を述べる．特に検討した点は以下の5つである．（1）ネットワークを流れるデータから抽出して検出する方式を採用するか，または各パソコンにウィルスチェックソフトをインストールして検出する方式を採用するか（2）チェックする対象範囲はメールだけかHTTPやFTPのデータもチェックするか（3）ファイアウォールからデータを取り出すか，またはメールゲートウェイからデータを取り出すか（4）OSは何を使用するか（5）導入費用および年間保守費はいくらか．以下，これらの項目について述べる．

（1） 各パソコンにウィルスチェックソフトをインストールする方式としては，大量ライセンス購入向きにNorton Education Suiteなどが存在した．その実現方法は，WWWサーバにウィルスチェックソフトを置いておき，必要な人は各自でダウンロードしてインストールしてもらうという方法であるが，この方法は以下の問題があった．(a) パターンファイルの更新が確実に実行される保証がない．(b) インストール自身もユーザが行う作業であり実行される保証がない．(c) インストール条件で他のソフトがインストールされていると正常にインストールできないことがあるという事例が報告された．(d) Macintosh用ウィルスチェックソフトは大量購入用の価格が用意されておらず，全学分を用意するとその費用がかなりを占める．(e) WindowsNTServer用は値段が別設定され高価である (f) Windows用は大量購入用の商品があるが，全学分のライセンス数を購入すると高額になる．以上の理由により，各パソコンにウィルスチェックソフトをインストールする方法は却下された．

（2） メールだけでなくHTTPプロトコルやftpプロトコルにより転送されるファイルの中にコンピュータウィルスが含まれていないかを調べるには，ファイアウォールを通過するデータを横取りして調べる方式を採用すれば可能である．その製品としては，TrendMicro社のInterScan VirusWallとSymantec社のNorton AntiVirus for Firewallsなどが存在した．しかし，本学では，HTTPプロトコル，ftpプロトコルによるデータまで調べると応答速度が遅くなり，現状でも学外回線が細いために応答速度が遅いと苦情が多発している中で，さらに遅くすることは得策ではない．利用者から同意を取り付けることは不可能と判断した．そこで，メールの添付ファイルにコンピュータウィルスが含まれているかを調べるだけの方式を採用することとした．

（3） メールのみを調べるとしてもファイアウォールを通過するデータを横取りする方式とメールゲートウェイを通過するデータを横取りする方式が考えられる．現にInterScan VirusWallは，両方式とも実現可能であり，Norton AntiVirus for Firewallsは前者，NortonAntiVirus for Solaris GatewaysとNorton AntiVirus for Internet E-mail Gatewaysは後者で実現可能である．しかし，ファイアウォールを通過するデータを横取りする方式は，ファイアウォール自身の処理にさらに負担を掛けることになり，得策ではない．InterScan VirusWallはCheck Point Software Technologies社のFireWall-1とCVP(Content Vectoring Protocol)連携によりデータチェックすることが可能であるが，他の組織における導入事例で，プロセスが止まってしまいメールが配送できないという情報が入手できたため，ファイアウォールを通過するデータを横取りする方式は採用しないこととした．

（4） 用いるOSは，これまでの運用実績よりSolarisを採用した．Solarisで稼動する製品は，InterScan VirusWallとNortonAntiVirus for Solaris Gatewaysが存在した．Norton AntiVirus for Internet E-mail GatewaysはWindowsNTで稼動するため

却下された.

(5) 購入すべきライセンス数は導入することにより恩恵を受けるパソコンの台数であり，本学の場合，ネットワークに接続している全装置数から算出して5000ライセンス数が必要である．InterScanVirusWallは250ユーザ以上は無制限ライセンスとなりその価格は250万円，年間保守費が無制限ライセンスで87.5万円である．一方，NortonAntiVirus for Solaris Gatewaysは，5000ライセンスで105万円，年間保守費は35万円であった．両者の値段の差が無視できないほど大きいのは明らかである．この値段の差が最終決定に大きく左右した.

以上のことより，NortonAntiVirus for Solaris Gatewaysを採用した.

3.3 設定方法

受け取るメールアドレスの@の後ろに記述されるすべてのドメイン名をすべて列挙して記述する必要がある．そして，個々にそれらを届ける先のメールサーバを指定する．このメールサーバの指定の仕方は，マシン名で記述する方法もあるが，IPアドレスで記述した方が問題が起きない.

また，同時接続数の上限を入力と出力それぞれに指定する．この制限を超えてメールの配送要求が届くとキュー用ディレクトリに保存されてから処理される．そのディレクトリに溜まったファイルが多すぎる場合は，同時接続数の数を増やす．本学では入出力ともに100として運用している.

3.4 ウィルスチェックサーバの問題点

(1) 届いたメールを配送する先は，ドメイン名ごとに指定する必要がある.

ワイルドカードを使った記述の方法が認められていないので，すべてのメールアドレスに使うドメイン名を列挙して記述しないといけない．受信するメールアドレスの@の以降に記述される文字列をすべて列挙する必要がある．@の後ろはドメイン名で良いところをマシン名まで記述している場合がよくあるが，その場合はマシン名まで記述しないと配送ができない．不正中継の拒否の仕方が，この@以降の文字列に完全一致しないものは中継を拒否する方式になっているためである.

(2) 指定した配送先をマシン名で記述するとそのMX指定された先に配送してしまう.

ドメイン名ごとに配送する先のマシン名を記述するのであるが，そのマシン名がさらにMX指定をしている場合，そのMXによる指定先へ配送してしまう．このことは，本学では，MX行を窓口役のメールサーバに向けているため，配送先は窓口役のメールサーバへ配送されることとなり，結果的にToo Many HopsのBounceエラーを発生させてしまう．対策としては，配送先をマシン名による記述でなくIPアドレスによる記述にする．IPアドレスで記述するとMXで指定された先へは配送しないため，Too Many HopsのBounceエラーは起きなくなる． 配送先をマシン名で記述させておきながらMX指定された先に配送してしまう仕様について，その理由をメーカに尋ねても明確な回答はない.

(3) 指定した配送先のマシンが，HELOに対し，FQDNでなく，マシン名のみを返す場合には配送に失敗する.

理由をメーカに尋ねても明確な回答はない.

(4) 受け取りを拒否する条件指定ができない.

sendmailでは，受け取りを拒否する条件を指定できるが，その機能が存在しない．具体的には，SPAMLISTに記載されたメールサーバから発信したメールは受け取りを拒否するとか，FROM:の行が空であるメールを受け取り拒否するといった設定をすることができない.

(5) Open Relay状態であるかのように見える.

25番ポートを指定しウィルスチェックサーバにtelnetをし，HELOによるハンドシェークをした後にRelay To:を入力された時に，不正中継対策のされているsendmailではrejectされるが，ウィルスチェックサーバでは，この時点でrejectをしないため，不正中継対策をしていないように見えてしまい，不正利用者から中継に使おうとしたメールが届けられてしまう.

(6) ウィルスチェックサーバからメールを配送する配送先について，一覧印刷ができない.

配送先の記述行は本学の場合，168行にも及ぶ．設定内容は画面で確認するしかなく，一覧印刷の機能はない．管理上，どのように記述されているかを提示し関係者に確認をもらうという作業を実施することができない.

(7) ログの出力の時間遅れがある.

表 1: 処理をしたメール数

処理内容	件数
メールゲートウェイへ来たメール	169279
不正中継拒否したメール	147
ウィルス検出したメール	110

時間範囲を指定し，その中の配送結果をレポートの形で出力するログ出力機能が存在するが，配送結果がログに現れてくるまでに時間がかかる．そのため，リアルタイムにデバックをするためのデータとしてログ出力を使えない．

（8）表示が英語に変わってしまうことがある．

WEB ブラウザ表示の方式で，各種設定やログレポート出力などを行うことができ，その画面が日本語対応されている．しかし，何故かその表示が英語に変わってしまうことが起きる．

4 運用結果

2000 年 11 月 10 日から 12 月 10 日の 1 ヶ月の間にメールゲートウェイで処理をしたメールの数を表 1 に示す．

不正中継拒否したメールは，OpenRelay ができると思って送りつけてくるために数が多いが，コンピュータウィルスの数も結構多い．このことより導入効果は大変高いと言える．

5 残された課題と対策案

不正中継の対策は完成したが，メールサーバをダウンさせるような DoS 攻撃のような SPAM メールについての対策が不充分である．From: と To: を偽称して本学のドメイン名を持ちいて存在しないユーザ名を記述し，Bcc:に本来の届けたいユーザのメールアドレスを記述したメールを出されると，From: と To:のメールサーバ間では UserUnknown のために Bounce エラーを起こし，メールサーバに過負荷が掛かる．特に，攻撃の場合には，存在しないユーザ名を大量に自動発生させてメールを発信してくるため，メールサーバがダウンしてしまうことが起きる．ウィルスチェックサーバの場合，Bounce メールが集中して起こると設定変更ウィンドウも応答がない状態になる．

この対策案としては，ウィルスチェックサーバの前段に sendmail が稼動するメールサーバを追加し，そのメールサーバがウィルスチェックサーバへ転送するという多段のメールゲートウェイ構成にすることが考えられる．メールサーバでは，sendmail.cf 中のパラメータで MaxDaemonChildren = 20, DoubleBounce = nobody の設定を行うのが良い．MaxDaemonChildren は，多数の sendmail プロセスがプロセステーブルを埋めつくし，システムが異常になるのを防ぎ，DoubleBounce = nobody はエラーメールのログが溢れるのを防ぐ効果がある．

現在は，対策案を実施していないため，大量にエラーメールが発生し続けているときには，ファイアウォールで発信元 IP アドレスに対し遮断する方法を取る予定である．

6 まとめ

本学で採用した不正中継防止対策とウィルス対策について述べた．導入時に比較検討した点および設定方法について詳細に述べ，問題点についても明らかにした．期間的にはまだ短いが運用して発見されている中継拒否された数やウィルスの数などから，この導入の効果は大きいと思われる．導入にあたっては，できるだけ費用の掛からない製品を選択したので，費用対効果も大きいと言える．残念なことに，メールサーバをダウンさせる攻撃に対する対策については完成していないので，その点が今後の課題である．

文献

[1] 長谷川明生，”メールゲートウェイ実現のためのツールの開発”，名古屋大学大型計算機センター研究開発部研究報告 No.26，pp.3-9，Oct.2000.

[2] 山口由紀子，”SPAM メール中継被害の防止対策について”，名古屋大学大型計算機センター研究開発部研究報告 No.26，pp.23-28，Oct.2000.

[3] 山井成良，大隈淑弘，林伸彦，宮下卓也，岡本卓爾，”岡山大学における電子メールのセキュリティ対策”，学術情報処理研究 No.4 2000，pp.79-83，Oct.2000.