名古屋大学におけるSPAMメール中継被害の防止策について

山口　由紀子　　長谷川　明生
名古屋大学　大型計算機センター

SPAMメールの中継被害は古くから知られているネットワーク攻撃であり、メールサーバで取るべき対策は広く公開されている。しかしながら、大学の学内ＬＡＮのような開かれたネットワークで、しかも管理者のスキルにばらつきがあるような環境では一向になくならない。そこで、ファイアウォールとメール配送サーバを導入した対策を実施した。

Preventive measures of the SPAM mail relay in Nagoya University

YAMAGUCHI, Yukiko　HASEGAWA, Akiumi
Computation Center, Nagoya University

The damege of SPAM mail relay in open relay mailer is well known since the since before, and the measures are open to the public. However, because LAN of the university is an open network and managers' skills are not even, the SPAM mail relay damage often occurred. Then, we decided to take measures in which Firewall and the mail delivery server are used.

1. はじめに

インターネットの広がりとともに、学外からさまざまなネットワークアタックを受けるようになった。特にSPAMメールの中継の被害は何年も前から発生しているにも関わらず、現在もしばしば発生している。SPAMメール中継の被害を受けないための方策については、被害が発生するたびアナウンスしているため、メールサーバとして運用しているホストでのSPAMメール中継の被害は減ってきている。その一方で、最近はメールサーバ以外のホストでの被害が目立っている。いわゆるspammerは、以前はネームサーバの情報を元にopen relay mailerの捜索を行っていたが、最近はネームサーバのセキュリティが向上してネームサーバの情報が入手しにくくなった。そこで、ネットワーク内のすべてのアドレスについて虱潰し的にport scanを実施してopen relay mailerを捜し出すため、ホストの管理者が気づかないうちに立ち上がっていたsendmailが利用されてしまうというケースが発生している。

このような被害はネットワークに接続しているすべての端末がで正しく設定されていれ

ば発生しないはずであるが、学内ＬＡＮに接続されている１４０００台を越えるのすべての端末で徹底することは難しい。そこで、ファイアウォールとメール配送サーバを導入した全学的な対策を実施することにした。

2. SPAM メール中継の被害状況

図１に２０００年１月～８月の SPAM メール中継の被害状況をまとめた。これらはSPAMメールの受信者などからの苦情メールを集計したものであるため、苦情が届かなかったものについては入っていない。

グラフからわかるように、メールサーバとして管理されているホストより非メールサーバでの被害の方が多い。これらの非メールサーバでは、管理者は苦情が来て初めて sendmail が起動していることに気付き、慌てて sendmail を停止させ、今後自動的に立ち上がることがないように設定を変更するという対策を取ってきた。

８月が特に多いのは、夏休みを利用した受電設備の点検のための停電が学内の各所で実施され、正しく設定されていないホストで復電後に sendmail が立ち上がってしまい、それが SPAM メール中継に利用されてしまったためである。停電から１週間後に被害を受けた例もある。

このような非メールサーバはメールを受信する必要がないため、smtp アクセスを上流で遮断してしまえば SPAM メールの中継に利用されることがない。そこでファイアウォールを利用して全学的に smtp をフィルタリングすることを検討することにした。

3. 防止対策の検討

名古屋大学では nagoya-u.ac.jp 以下１５０ドメインで５００メールサーバが運用されている。このような状況下で smtp アクセスを遮断し、全学を代表してメールを受信して学内に配送するメール配送サーバを運用するためには以下の注意が必要だった。

1. 管理者に負担をかけない。

学外からのメールをメール配送サーバに

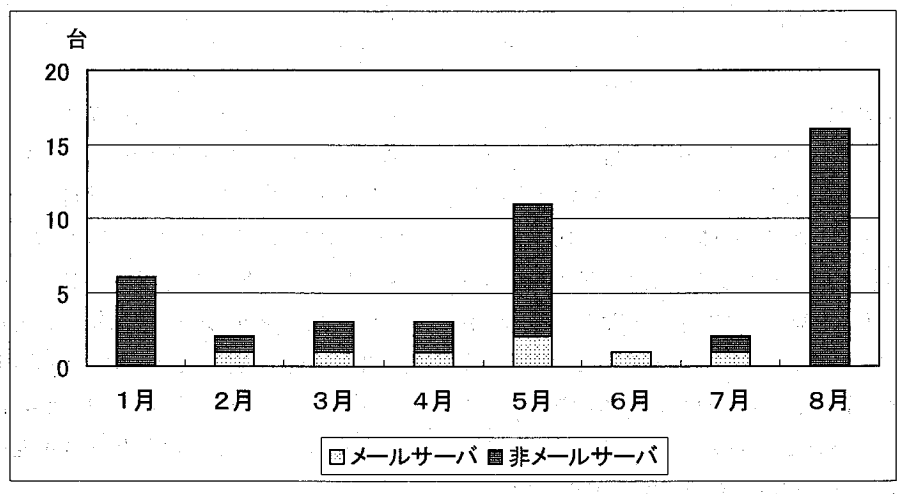

図１　SPAM メール中継を受けたサーバ

集中させるためには、全ドメインのネームサーバで MX レコードの向け先を変更する必要がある。

しかし、ネームサーバ、メールサーバの管理者に設定変更などの負担をかけると、各管理者にとって不都合であるばかりでなく、全管理者の同期がとれにくくなってしまい、対策の実施が困難になってしまう。

2. 一般利用者の使い勝手を変更しない。

学外から POP サーバを利用するために POP before SMTP などのサービスを運用しているメールサーバがある。これらのサーバへの smtp アクセスを遮断してしまうと、POP クライアントの利用者全員に設定を変更してもらう必要が発生し、混乱を招くことになる。

3. 学外へ影響が及ばないようにする。

学内のメールサーバで学会などの仮想ドメインを運用している場合に、ネームサーバが学外で管理されている場合がある。

4. 安定した運用を実現する。

特定のサーバにメール受信を集中させてしまうと、障害発生時に大学全体が孤立してしまう危険性がある。

そこで本学では以下のような対策をとることにした。

1. 一部のメールサーバはファイアウォールで通過許可する。

POP before SMTP や仮想ドメインなど特殊なサービスを行っているメールサーバについては、外部からの smtp アクセスが直接受けられるようにファイアウォールで通過させることにした。

2. 外向けネームサーバを運用する。

各メールサーバ、ネームサーバの管理者が設定をなんら変更することなく移行できるようにするため、ネームサーバを二重化し、nagoya-u.ac.jp の外向けネームサーバを別途設定することにした。外向けサーバは、メール配送サーバ経由でメールを受け取れるように MX レコードを変更した設定で運用する。その他の設定は内向けサーバでの設定と同じ設定で運用する。

一方、学内では従来どおりのネームサーバを運用し、メール配送サーバはその内向けサーバを参照してメールの配送を行うことにした。

3. メール配送サーバを二重化する。

バックアップ用のメール配送サーバを設置することにした。したがって、外向けネームサーバでは MX レコードを一次サーバと二次サーバの両方について設定することにした。

図 2 に SPAM メール対策の運用形態を示す。学内のすべてのメールサーバを smtp を直接受信できるものと受信できないものに分け、直接受信できるメールサーバについてはファイアウォールに通過許可登録する。ファイアウォールは、学外からの smtp アクセスを原則として遮断し、登録されているホストに対してのみ通過させる。また、メール配送サーバ受信したメールを学内の各メールサーバへ配送する。この時原則として nagoya-u.ac.jp 以外のアドレスへのメールは中継しない。

なお、今回の運用形態は SPAM メール中継被害の防止を目的としているものであって、

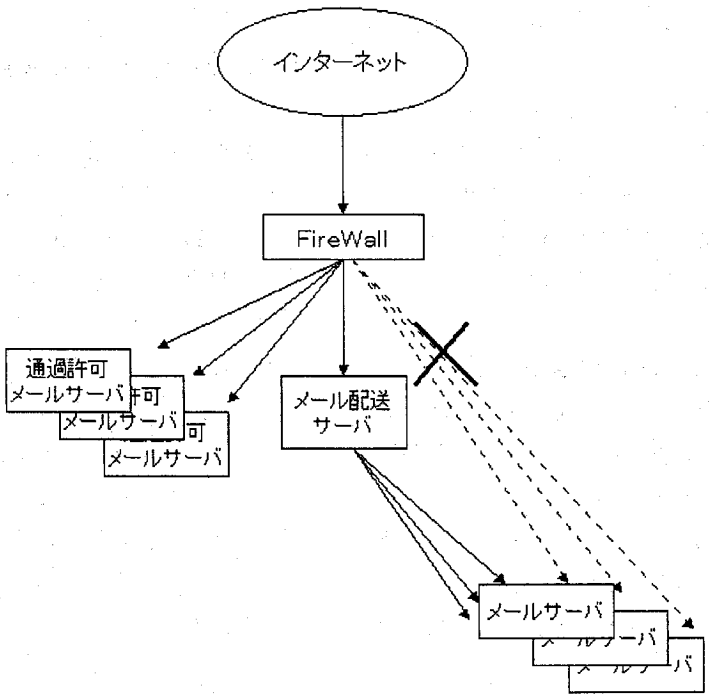

図２　SPAM メール中継防止のための運用形態

学内のメール利用を制限することはできるだけ避けたい。そのため、学外への smtp アクセスは制限しないことにした。

4. 対策実施準備

対策の実施を進めるにあたって、以下の機能を実現した。

４．１　メールサーバ登録システム

学内のメールサーバの管理者に各自が管理しているすべてのメールサーバについて、ファイアウォールの通過登録申請するかメール配送サーバの利用申請するかを検討してもらうことになった。検討の過程で、学外からはメールを受信しない内部専用サーバがあることがわかった。内部専用サーバは、外向けネームサーバで MX レコードを変更する必要がないため、内部専用サーバとしての申請も受け付けることにした。

この申請処理を簡素化するために、電子メールで申請を受け付ける自動登録システムを作成した。申請データは以下のとおりである。

- ✧ 種別
  - Firewall 通過登録申請
  - メール配送サーバ利用申請
  - 内部専用サーバの申請
  - 申請状況の確認
  - 申請の取り消し
- ✧ メールサーバのＩＰアドレス
- ✧ メールサーバのホスト名

✧管理者氏名と連絡先
✧備考

自動登録システムは、記載されている内容についてネームサーバの情報との整合性を確認した上で処理し、申請者に処理結果を通知する。登録データは、ＩＰアドレスをキーとするDBMデータベースとして管理している。なお、外向けネームサーバ用データ生成システムなど他のプログラムで利用するため、CSV 形式のデータも定期的に生成している。また、登録申請だけでなく登録状況の確認と登録の取り消しの機能も実現した。本システムは Perl で記述した。

なお、ファイアウォールで通過許可申請する場合には、SPAM メール中継に対する対策がとられていることを確認するために、mail-abuse.org のチェックリストの結果を備考として添付することにした。

４．２　外向けネームサーバ用データ生成システム

外向けネームサーバ用のデータは、学内で運用されているすべてのネームサーバの設定データを収集して生成する必要がある。そのためのシステムを以下の３つの機能により実現した。

1. nagoya-u.ac.jp のトップドメインから再帰的にドメインをたどり、すべてのドメインの SOA レコードを収集する機能。
2. １で収集した SOA レコードのシリアル番号を保存しているデータと比較し、更新されたドメインについてのみゾーン転送する機能。
3. すべてのドメインのデータから外向けネームサーバのデータを生成する機能。この時、メールサーバ登録システムで作成した CSV 形式のデータを参照しながら、メール配送サーバを利用するメールサーバに関する MX レコードを変更する。

これらの機能は Perl で実現した。現在は、外向けネームサーバのデータを１日１回自動的に更新している。したがって、新しくメールサーバを導入する場合には、メールサーバの登録申請後、実際にファイアウォールへの登録や外向けネームサーバが更新が行われるのは翌日以降となる。

５．運用状況

１２月２６日現在の全メールサーバの申請状況は以下のとおりである。今回、各管理者がメールサーバの運用形態を検討した結果、メールサーバではないホストにまで設定されていた MX レコードの整理もできたため、当初想定していたメールサーバより１００台ほど少なくなった。

メール配送サーバ利用	３０９
ファイアウォール通過登録	７５
内部メールサーバ	７

７月２５日に JPNIC に対し nagoya-u.ac.jp のネームサーバを外向けサーバに変更する依頼を出し、メール配送サーバの運用を開始した。１ヶ月あまりの試験運用を経た後、９月４日にファイアウォールの設定を変更した。それ以後 SPAM メール中継の被害は発生しておらず、本防止策の有効性が実証できた。

図３に７月２５日の運用開始以来、メール配送サーバ（一次サーバ）におけるメール配送数を示す。１０月第二週のメール数が多いのは、ヘッダを詐称した SPAM メールが大量にあっ

たためである。

ヘッダ詐称SPAMメールは発信元（From）や送信先（To）に架空のアドレスを指定し、本来の送り先をBccに記述したメールを大量に送るものである。これにより、SPAMメール中継に利用された第三者のメールサーバだけでなく、詐称したヘッダにアドレスを使われた第四者のメールサーバに大量のエラー通知メールが届くためメールサーバが処理不能になってしまう。実際、メール配送サーバ運用開始から１週間目の８月３日にヘッダ詐称のSPAMメールを大量に受信し、配送先のメールサーバへ送信不能となり、メール配送サーバが２台ともダウンするという障害が発生してしまった。そこで、メール受信能力の見直しを行い、同時に処理できるメール数を減らした。新しい設定では運用が安定し、１０月第二週にヘッダ詐称メールがさらに大量に届いた時にも運用が継続可能であった。

6. おわりに

SPAMメール中継の防止のため、ファイアウォールでのsmtpアクセスの遮断、メール配送サーバによるメール受信の代行、外向けネームサーバによるメール送付先の指定という対策を実施した。実施後SPAMメール中継の被害は発生しておらず、本対策の効果が実証された。

一方、ヘッダを詐称したSPAMメールに本学のアドレスが使用される例は後を絶たない。これについては現状では有効な対策手段がない。

なお、ファイアウォールでの通過許可登録は６ヶ月単位に見直すことにしており、２００１年の春に更新作業を行う必要がある。

参考文献

[1] E. Allman, Sendmail Installation and Operation Guide for Sendmail Version8.10, 2000

[2] D. Barr, dnswalk 8.2 Manual, 1999

[3] M. Fhur, Net-DNS-0.12 Manual 1999

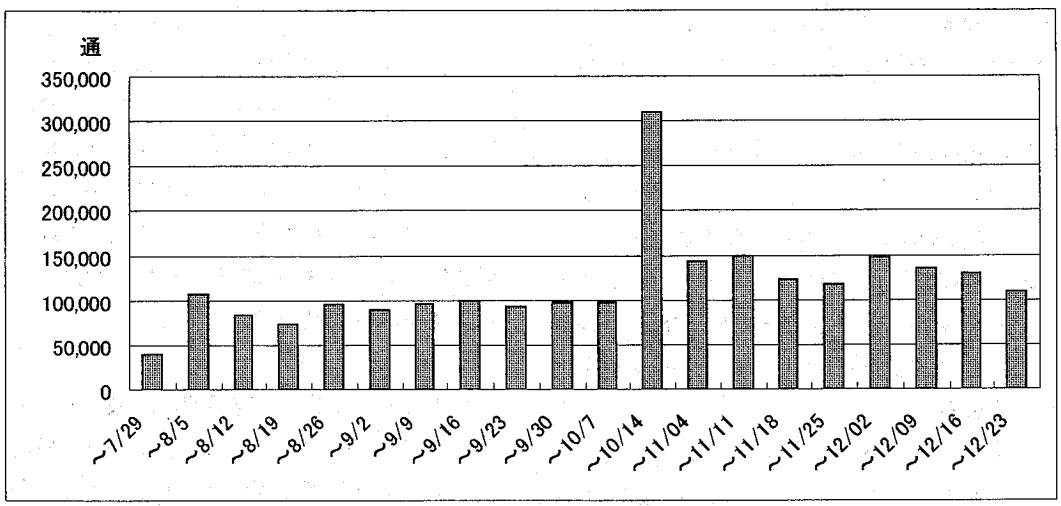

図３　メール配送サーバ通過メール