— 事例紹介 —

セキュリティー対策の基礎 —SPAMメール編—

総合情報処理センター 松本 豊司

1. SPAM(スパム)とは？

見ず知らずの方からお金がもうかるという内容のまるでねずみ講まがいのメールが来たり、猥褻な情報の案内が来た経験がどなたもあると思います。これがスパムメールと言われるもので、辞書にもしっかりとSPAMの単語が載っています。本センター所蔵の昭和44年発行の研究社の古びた新英和大辞典には"米国George A. Hormel & Co.製の)かん詰肉、[商標名:sp(iced h)am]"とあります。ではなぜかん詰肉の商標名が迷惑な商業メールの総称(他に UCE:Unsolicited Commercial Email, UBE:Unsolicited Bulk Emailと呼ばれることもある)になったかというと、TVの人気番組のコントの中で、"レストランで料理を注文しようとしたら、どの料理にもSPAMが入っていた"ということに由来しているようである。

2. スパムにあなたは無関係？

一般的に本センターのユーザにとっては迷惑なメールを送られてくることがSPAMとの接点と思われていると思います。ですが、もういちど周りを見渡してください。特にあなた自身があるいは所属する学部, 学科, 研究室でメールのサーバを構築し、運用している方は要注意です。UNIX ワークステーションを購入すると多くの場合、あらかじめメールのサーバの機能を実現するソフトウェア sendmail がインストールされており、UNIX ワークステーションを起動すると同時に動作するようになっています(それぞれの大学に応じたローカルな情報を設定しないと完全には機能しない)。また、最近ではパーソナルコンピュータ(Windows マシンやMac)等で簡単にメールサーバが実現できます。この簡単にというのが曲者で後で説明しますが学内、国内あるいは海外の方に迷惑をかけている場合があります。

さて、メールのサーバの機能を実現するソフトウェアの代表が sendmail と言われるもので、この原稿を書いている段階での最新バージョンは sendmail8.9.3 です。このバージョンの違いによってSPAMの対策方法が違います。UNIX のワークステーションの場合は

```
% sendmail -d0.1 -bv
```

あるいは sendmail のバージョンが 8.9 以降の場合は以下のようにすればバージョンがわかります。

```
% sendmail -d0.101
```

本センターで運用しているメールサーバ kenroku での実行例を以下に示します。

```
kenroku% /usr/lib/sendmail -d0.1 -bv
Version 8.8.8+2.7Wbeta7
  Compiled with: LOG MATCHGECOS MIME7TO8 MIME8TO7 NAMED_BIND NDBM NETINET
                 NETUNIX NEWDB NISPLUS QUEUE SCANF SMTP USERDB XDEBUG CANON_OTHER
                 QUICK_RESPONSE MULTI_MAILER CONNECT_HACK RESOLV_HACK STAT_HACK
                 DYNAMIC_TOBUF

============ SYSTEM IDENTITY (after readcf) ============
        (short domain name) $w = kenroku
   (canonical domain name) $j = $w.$m
           (subdomain name) $m = kanazawa-u.ac.jp
                 (node name) $k = kenroku
========================================================
```

このようにVersion 8.8.8+2.7Wbeta7であることがわかります。最新のバージョンが8.9.3であると述べましたので"紺屋の白袴"であることがわかります(機能的には問題ないが、セキュリティの観点からできるだけ新しいバージョンに保つことが望ましい)。

あなたのサーバのバージョンが8.8以前のものだったら設定によりSPAMメールを防ぐ機能がありません。この場合はsendmailを思い切って最新のバージョンにアップしましょう。バージョン8.8以降のものでしたら設定により防ぐことができます。また、最新のバージョン8.9ではディフォルト(暗黙のうちに)でSPAMの中継をしないようになってます。

なお、SPAMの不正中継に関する詳細やsendmailのバージョンアップの手順の詳細はJPCERT/CC(コンピュータ緊急対応センター)の以下のURLを参照してください。

電子メールの不正中継
http://www.jpcert.or.jp/tech/97-0001/

sendmailのバージョンアップ
http://www.jpcert.or.jp/tech/98-0001/

実際の設定、特に本学に固有な設定などは本広報の記事を参考にしてください。

3. メールの不正中継とは？

本来、sendmail 等のメールサーバの機能を実現するソフトウェアはMTA(Messsge Transfer Agent)と呼ばれ、メールを中継するように作られている。ここに目を付け、商業メール等を他人のサーバを利用して送り付けるものが不正中継と言われるものです。ダイレクトメールなどは多数の人に送れば効果的で、これらの業者が大量のメールを処理できるだけの能力をもったサーバを持ち運用すれば何ら問題ないのですが費用がかかります。又、その形態の運用をすると受け取る側で送り元のサーバを特定でき、簡単に受け取り拒否を設定できます。これらの理由からSPAMは他人のサーバを中継に使います。また、そのサーバでメーリングリストを運用している場合は特に要注意です。一挙に大量のメールを送りつけることができます。本学のサーバが利用された場合に考えられる被害をまとめると

1. 本学の資産の不正利用

本学の器材（メールサーバ等）は研究，教育等の目的に導入されており、商用に利用されるべきでありません。その上に SPAM の不正中継に利用された場合は、そのワークステーションのメモリー，ハードディスク（メールスプール）などのハードウェア資源が大量に使われますので、本来のユーザが使えない事態も生じます。また、ネットワークのトラフィックもあがりますので、これらのものが極端な場合は本来の目的に使えないと言う事態になります。その挙げ句に管理者のメールアドレスにSPAMを送り付けられた方から沢山の抗議のメールが届き、対処を余儀なくされます。

2. 本学からのメールの受け取りが拒否される事態の発生

これもまた深刻な問題です。最近SPAMの被害が広がると共にSPAMを出すドメインのブラックリストデータベースの各種サービスが開始されております。sendmail にこのデータベースを参照するように設定するとここに登録されているドメインを持つアドレスからのメールを拒否します。つまり、本学のメールサーバが登録されると本学からのメールがそのように設定されたサーバを持つ組織には着かないようになります。これまでに kenroku に関係したSPAM騒動で登場したデータベースで現在も活動しているデータベースとそのURLを以下に示す。

・orbs.org の Open Relay Behaviour-modification System (ORBS)
URL:http://www.orbs.org/

・Mail Abuse Prevention System Realtime Blackhole List (MAPS-RBL)
URL:http://maps.vix.com/

これらのデータベースの仕組みはそれぞれ違うが、SPAMの被害にあった人からのメールを受け取り、幾つかのチェック用のプログラムを自動的に起動させSPAMの被害を発生するサーバかどうかチェックします。問題のあるサーバである場合は直ちにあるいは管理者に対策するようにメールをし、猶予期間の後にデータベースに登録をします。これらのサーバにおいて対策を完了し、管理者がデータベースの削除の処置をしな

い限りデータベースから削除されません。始末の悪いことに、一般的に sendmail は同一組織内の中継(本学内同士の中継)は許すように設定され、また、スパムの発信元では不正中継が発覚しにくいように複数のサーバにまたがって中継を企てます。ですから学内のどこかに不正中継の禁止の設定のないサーバがあるとそこを経由して、設定のあるサーバが中継に利用され、ちゃんと管理されているにも関わらずそのサーバまでブラックリストに載ってしまう事態が生じます。本センターで運用している kenroku はたびたびこの被害にあっており、そのたびにサーバの管理者に連絡を取り、対策をお願いし、データベースの削除の手続きする羽目に陥ります(対策が完了するまでデータベースの削除はできないので、すぐに対処できない(管理体制が確立されていない)サーバの場合は停止をお願いしたこともあります)。

この特集号をきっかけに本学においてもメールサーバが無秩序に構築されるのではなく、しっかりとした管理体制のもとで外部の組織に迷惑をかけること無しに大いに利用されることを望んでおります。

なお、SPAM対策の事例は次頁以降に紹介されていますので、研究室の器材に応じて利用下さい。

事例1	UNIXワークステーション編	18頁
事例2, 3	Macintosh編	29, 35頁
事例4	PC UNIX(Linux)編	40頁
事例5	Windows NT編	48頁