SPAMとワーム

長谷川　明生

Ⅰ．SPAM対策

今年度に入ってから，UCE（Unsolicited Commercial E-mail）とかUBE（Unsolicited Bulk E-mail）と呼ばれる迷惑メールが急増しています。このようなメールを単にSPAM（スパム）と呼ぶこともあります。SPAMを送りつけるアドレスは，専用のソフトウェアでWebサーバを巡回しコンテンツに埋め込まれたメールアドレス（掲示板やチャットは宝庫です。）らしいものを収集するとか，ネットワーク管理者データベースや各種の検索サービスを使って集めているようです。

典型的なSPAMの例を以下に示します。

```
Subject: Sh0cking site - extrem (towers rainy)
From: “Dominick McMullen” <dominickmcMullen_bp@CREATIONmail.com>
To: x99999x@nucc.cc.nagoya-u.ac.jp
Date: Fri, 08 Aug 2003 12:21:08 +0000
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)
X-Mew: Charset for body is not specified.
X-Mew: Text/Plain in Multipart/Alternative as a singlepart

                As Seen On TV: CNN, ABC News And More ...
```

SPAMの発信者や発信元のホスト名やドメイン名は偽造されていることが普通です。また，何段にも中継を重ねて複雑な経路をとおしてメールを送ることで，発信元の特定を困難にしています。メールの件名もOutlookのようなソフトウェアの簡単なSPAMフィルタではフィルタできないように工夫がされています。スペルがそれらしく，しかし一部紛らわしく変えてあります。

このメールのヘッダは，実際には次ページの枠中のリストのようになっていて，通常のメールソフトウェアの設定では，本当の経路は見えません。

このメールは，CLICKITmail.com (unknown [211.175.124.41])から発信されたようですが，CLICKITmail.comのアドレスは211.175.124.41ではありませんし，返信アドレス（Return-Path:）のCREATIONmail.comとも関係なさそうです。実際にどこから，だれがこのようなメールを発信したかを突き止めることは，この例でもわかるとおり不可能です。

現在，NICEでは，このようなSPAMを排除するために，メールゲートウェイで簡単なメールの

```
Return-Path: <dominickmcMullen_bp@CREATIONmail.com>
Received: from postman1.nagoya-u.ac.jp (postman1.nagoya-u.ac.jp [133.6.1.24])
        by nucc.cc.nagoya-u.ac.jp (8.11.6p2/3.7W) with ESMTP id h78AsY413849
        for <x99999x@nucc.cc.nagoya-u.ac.jp>; Fri, 8 Aug 2003 19:54:35 +0900 (JST)
Received: from mailgate1.nagoya-u.ac.jp (chk1.nagoya-u.ac.jp [133.6.1.22])
        by postman1.nagoya-u.ac.jp (Postfix) with ESMTP id F08DB36BC3
        for <x99999x@nucc.cc.nagoya-u.ac.jp>; Fri, 8 Aug 2003 19:54:33 +0900 (JST)
Received: from CLICKITmail.com (unknown [211.175.124.41])
        by mailgate1.nagoya-u.ac.jp (Postfix) with SMTP id 1CB105665D
        for <x99999x@nucc.cc.nagoya-u.ac.jp>; Fri, 8 Aug 2003 19:54:32 +0900 (JST)
Message-ID: <99fc01c35da7$138f8e85$f6032fc0@2517cv2>
```

チェックを行っています。これは，メールサーバのキューを調べるとか，受け取ったSPAMメールの件名の共通パターンを調べて簡単なフィルタを設定することで実現しています。この機能は，Sobigウィルス対策では一定の効果がありました。これは，件名の出現パターンが非常に限定されていたから可能だったことで，SPAMメール全般となると先の例に示したように，パターンマッチだけのフィルタでは不十分です。また，受け取ったメールがSPAMであるかどうかやメールの迷惑度は受け取る個人によっても異なるので一律の対策は困難です。

そこで，最近話題のベイズ統計を利用したメールフィルタを共同利用のメールサーバ（ホスト名nucc）にインストールして試してみました。ここで利用したソフトウェアは，bsfilter（http://www.h2.dion.ne.jp/~nabeken/bsfilter/）とprocmail（http://www.procmail.org/）の組み合わせです。試してみての効果はというと，筆者の場合は，すばらしいものでした。毎日20通以上目にしていたSPAMをほとんど目にしなくなりました。統計的な処理による関係上，誤判定が０ではないので，SPAMも保存しておいて，時々目をとおす必要があります。

センターのメールサーバ利用者は，以下のようにすると，フィルタの効果を試すことができます。

１．ホームディレクトリに「Mail」というディレクトリが存在しなければ作成します。

２．~/Mailの下に，ファイル「spam.log」を作成する。このファイルには，メールの処理状況が記録されます。

```
touch ~/Mail/spam.log
```

３．~/Mailの下にディレクトリ「spam」を作成します。SPAMと判定されたメールは，このディレクトリに移動されます。

```
mkdir ~/Mail/spam/
```

４．フィルタが利用するデータベースをホームディレクトリに展開します。この操作で，ホームディレクトリに「.bsfilter」というディレクトリが作成されます。

```
zcat  /usr/local/model/spamfilter/bsdb.tar.gz  |  tar  xvf  -
```

５．procmail用の設定ファイルのモデルをコピーします。そして，コピー先の「.procmailrc」のx99999xの部分を自分の課題番号に変更してください。

cp /usr/local/model/spamfilter/procmailrc ~/.procmailrc

６．ファイル「.forward」を設定します。

① モデルからコピーします。

cp /usr/local/model/spamfilter/forward forward

② 課題番号x99999xの部分を自分のものに変更します。

③ 編集のすんだforwardファイルを「.forward」にコピーします。

④ 念のためにファイルのモードを変更しておきます。

chmod 640 .forward

これで，SPAMとみなされたものだけがメールボックスから抜かれて，~/Mail/spamディレクトリの下に移動されます。

その結果として，普通にメールを読んでいる分には，ほとんどSPAMメールを見ることはありません。ただし，英文のメールで，タイトルがシンプルなものはSPAMと誤判定される可能性があります。判定精度をあげるために，適宜以下の手順でデータベースを更新していきます。

１．SPAMでないものが誤ってSPAMと判定された場合（spamディレクトリの123が誤判定の場合）

bsfilter -S -c -u ~/Mail/spam/123

２．SPAMが正常なメールに紛れ込んだ場合（SPAMメールを１個のファイルとして~/Mail/spam/124に保存してから）

bsfilter -C -s -u ~/Mail/spam/124

SPAMメールのファイルも課金対象となりますので，時々読んで，不要なものは削除しておくとよいでしょう。これは，誤判定防止にもなります。SPAMを保存するディレクトリのメールを読むにはmnewsの利用が最適です。これには，以下のようにします。

nucc% mnews -m -nMH

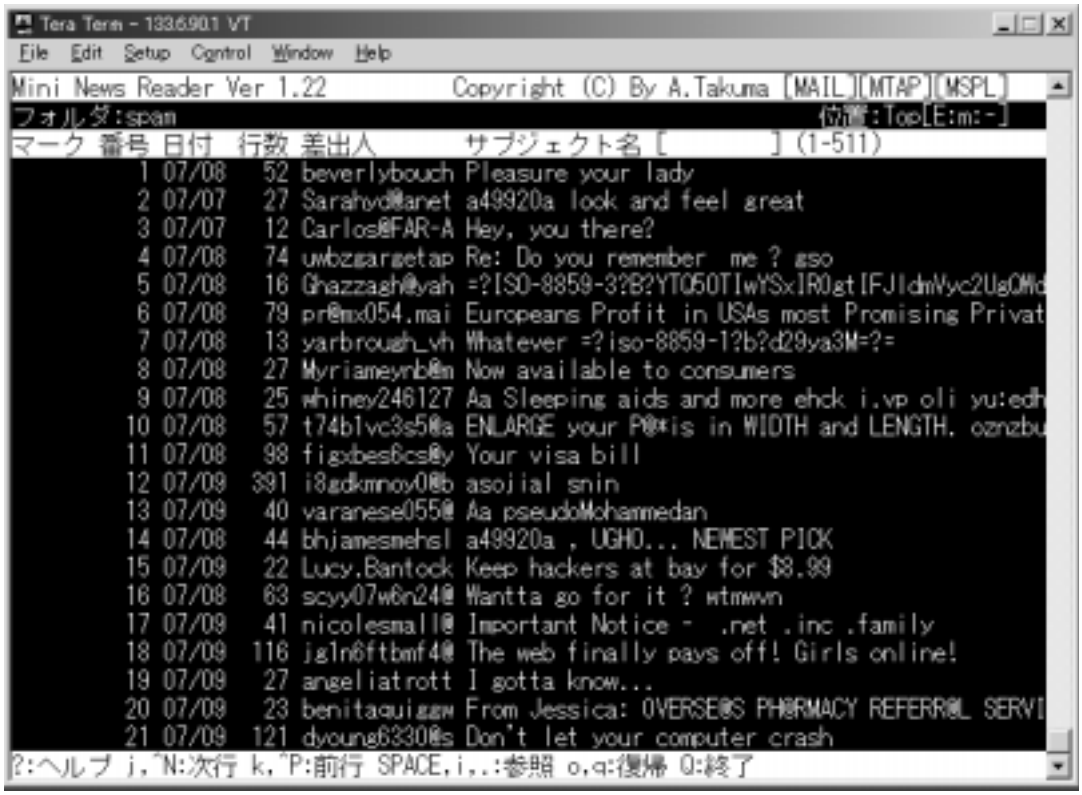
上のコマンドでmnewsを実行すると次頁のようになります。

タイトルから，SPAMが，専用のディレクトリに移動されていることがわかります。ぜひ一度，nuccに課題番号をお持ちの方はbsfilterを試してみてください。

また，このようなメールとは別に，チェーンメールやインターネットを利用した無限連鎖講まがいのものの勧誘も相変わらず存在します。最近では，海外からの送金の手伝いの依頼といった詐欺的なメールも増加しています。債務があるので振り込めといった詐欺メールもなくなってはいません。これらのメールに対しては，無視することが最善の策です。

Ⅱ．ワーム騒動

８月12日に始まったW32/MSBlaster騒動は９月に入ってようやく終息に向かい始めました。このワームは，WindowsのRPCのバグを狙ったもので，tcpポートの135番に接続して，セキュリテ



ィ対策のされていないホストに侵入し，侵入に成功すると135/TCPをスキャンして感染先を探します。これらのポートは，以前からファイアウォールによりフィルタしており，外部からの攻撃による感染はないはずだったのですが，感染したノート型コンピュータの学内への持込により内部に感染が拡大してしまいました。同じセキュリティホールを狙ったW32/Welchiaの発生が対策を複雑なものにしました。

W32/Welchiaは，感染するとW32/MSBlasterを削除してから活動を始めます。このため，W32/MSBlasterの感染を警告した時点では，利用者のコンピュータ上のW32/MSBlasterワームは後から感染したW32/Welchiaによって削除され検出されないという例が多発しました。また，駆除しただけで，適切にセキュリティパッチが行われなかったために，感染を繰り返すケースもありました。

今回のワームの感染の原因となったバグは既知のもので，適切にWindows updateがなされていれば問題がなかったはずのものでした。普段の適切な保守をお願いします。また，家庭でネットワークに接続して利用したコンピュータをNICEに接続する前には，最新のデータベースを使ってウィルスチェックをしてから接続してください。

（はせがわ　あきうみ：名古屋大学情報連携基盤センター大規模計算支援環境研究部門）