ウィルスとＳＰＡＭ

長谷川　明　生

Ⅰ．ウィルス問題

年明けから，BagleやMyDoomの亜種が猛威を振るったと思ったら，２月後半になって，これらのさらなる亜種やNetSky.Dがはびこっています。これらのウィルスが昨年世を騒がせたものと異なる点は，増殖の仕方です。昨年話題になったものは，Windowsのセキュリティ上の弱点を攻撃する特性を持っていたので，パッチが当てられていないソフトウェアなら無条件に感染しました。今年に入ってから，流行しているものは，電子メールの添付ファイルとして送られており，その添付ファイルを利用者の意思で開かないかぎり感染しません。しかしながら，学内でも結構な数の感染パソコンを出してしまいました。これは，ウィルス対策ソフトウェアが入っていないシステムが相変わらず存在することや，添付ファイルをうっかり開いてしまう利用者がいるということを意味します。しかも，MyDoomとNetSkay.Dの両方に感染した人の数は決して０ではありません。また，さらに悪質なNetSky.Qも出現しました。

ウィルス感染を軽く考えないでください。世界的に流行したウィルスについては，ウィルス対策ソフトウェアを販売している会社等から除染ソフトウェアが提供されることがあります。しかし，このようなソフトウェアの利用で，問題がすべて解決するというわけではありません。汚染から復旧できない場合の方が多いのです。この場合，オペレーティングシステムの導入からやり直すことが必要になって，貴重なデータやプログラムが反故になります。それだけなら個人の被害ですみますが，ウィルス付きメールを大量にばら撒いたことによる他人への迷惑には計り知れないものがあります。

システムを最新の状態に常に保つようにするとか，ウィルス対策ソフトウェアやパーソナルファイアウォールの利用は常識です。ウィルス対策ソフトウェアを入れた上で，常にデータベースを最新にしておく必要があります。最近の新種や亜種の出現の多さから，自動更新だけでは不十分で，何日かに一回は手動更新をした方がいいようです。

Ⅱ．SPAMの動向

SPAMも相変わらず増加の一途をたどっています。図１は，私宛に送られてきたSPAMについて，日付けを横軸にとってグラフ表示したものです。面倒なので，以前紹介したbsfilterのログをもとに作成しています。件数は一日のメールの累計でしめしてあります。これを見ると，私の場合は，全メールの半数がSPAMであることがわかります。また，ある時期，SPAMやウィルスのFromに，私のメールアドレスが使われたために大量のエラーメールが送りつけられてきました。

図中では，薄い色で表示されている部分です。日々の変動が大きいのですが，全体の傾向としてSPAMが増加傾向にあることも注意すると読み取れます。１月の中旬及び２月初旬のメール数とSPAM数両方が極端に減少している時期があります。１月は，SPAMの大半の送信元であるアメリカやヨーロッパのインターネット接続業者の動的アドレスからのメール受信を拒否する設定を，２月の分は逆引きできないクライアントからの接続を拒否した場合です。これは，大学入り口の中継サーバに設定しました。いずれもかなり効果があることがわかりますし，その効果は図にも見えています。が，同時に，メール中継サーバに対して，サービス不能攻撃，コネクトして，放置するもしくは，コネクトしてタイムアウト前にディスコネクトするという攻撃が行われ，それぞれ設定を解除するまで1週間以上にわたって続きました。SPAMを仕掛けるグループが，SPAM配送効果についてモニターしているように思えます。といって，すべてをゴミ箱へ落とすことも過激すぎるように思えます。で，現状では，差出人のアドレスに返信可能かどうか（ドメインに対するMXレコードもしくはAレコードの有無）だけをチェックしています。

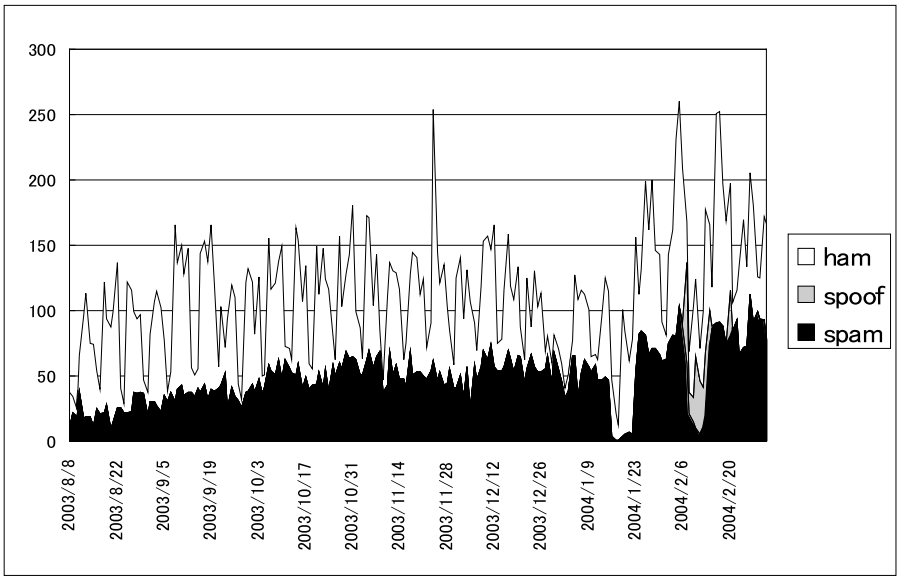

図１　SPAM数の変化

もう少し技術が進歩すれば，アプライアンスサーバでSPAMには目印をつけて，利用者がメールリーダで仕分けをするということも可能になると思われますが，現状では，UNIXベースで，アプライアンスを構築する必要があり，SPAM判別用のソフト自身が処理が重く，組織全体で対処するには無理があるように思えます。

Ⅲ．SPAM対策再考

現状では，SPAMを利用者個人で対処するのが一番合理的で，問題が少ないと思います。前回紹介したbsfilterは，ベイズ統計を利用したSPAMフィルタで，かなりの効果が期待できます。パ

ソコンでのメールの読み書きでは，Mozilla Thunderbirdといったベイズフィルタ機能を持ったものが使えます。Mozilla以外にもベイズ統計を利用したフィルタが出てきています。ただし，これも万能ではありません。このようなフィルタでは，使っているうちに判別能力が向上しますが，同時にSPAM判別用のデータベースが肥大化するという問題があります。私の場合，データベースの容量が16MBを越えてしまい，ベイズ確率データベースの更新に非常な時間がかかることになってしまいました。このためにデータベースを初期化することになりました。bsfilterでは，データベースが10MBを越えると-uオプションおよび-aオプションでの確率データベース更新は実用的ではありません。-uオプションを付ける場合には，.forwardでのprocmail処理を停止しておく必要があります。

ベイズ統計フィルタの普及に対して，SPAM側からの反撃もあります。数文字からなる無意味単語を大量に含んだメールや256文字を越えるような無意味文字列を数個だけ含んだメールがそれです。SPAM送出側は，このようなメールを送ることにより，ベイズフィルタのデータベースの破壊や混乱を狙っています。データベースが肥大化した場合には，思い切って，データベースをリセットすることも考慮に入れてください。ただし，このような作業中は，procmailでの処理を止めるといった配慮が必要です。

パソコンで，ベイズフィルタを利用している場合も，似たような配慮が必要です。私は，最近Mozilla Thunderbirdを愛用していますが，少しの学習で，きれいにSPAMをカットしてくれます。しかし，データベースが肥大化するとどうなるか今から心配しています。

（はせがわ　あきうみ：中京大学生命システム工学部
前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）