サイエンティフィック･システム研究会　　2004 年 8 月 5 日
システム技術研究会　2004 年度　第 1 回会合資料

Spam メールの解析と Spam 対策

中京大学生命システム工学部
長谷川　明生
hasegawa@akg.life.chukyo-u.ac.jp

梗　概

Spam や UCE と呼ばれる迷惑メールの数は，増加の一途をたどっている．筆者は，このようなメールへの対策を考えるために，昨年 8 月以来 Spam メールを蓄積しており，その件数は 20000 件を超えた．そこで、Spam メールの傾向や特徴を分析した．その結果に基づいて，Spam メールの防止対策について考察する．

キーワード　Spam，UCE，Spam メール解析，Spam 対策

はじめに

いわゆる Spam や UCE もしくは UBE と呼ばれる迷惑メールの数が急増してきている. さらに, ワームやコンピュータウィルスの中には，増殖のために大量のメールを無作為に発信するものもある．迷惑メール発信の手口も，コンピュータウィルスによる SMTP プロクシのインストールやトロイの木馬の利用といったように, 悪質化の一途をたどっている. このようなメールに対して, 人力による対処は,その件数の増加のために不可能になりつつある.

Spam メールを自動的に処理するシステムは，オープンソースの SpamAssassin[1] や bsfilter[2] の他に，ウィルス対策機能と Spam 対策を組み合わせたような商用ソフトウェアも広く市販されるようになっている．このようなソフトウェアの利用はかなりの効果を持つが，誤検知の問題は無視できない．誤検知の中でも，正常なメールを Spam として排除してしまうことが最大の問題である．また，メールサーバの管理者にとっては，Spam フィルタが Spam 発信に対する苦情メールを排除してしまうことが悩みとなっている．

著者は，2003 年 8 月に Spam メールの自動処理のために bsfilter と procmail[3] の組み合わせによる Spam メールの自動フィルタリングを開始した．それとともに，フィルタのログと Spam メールを解析のために保存している．また，フィルタによる誤検知を避け，正確な Spam メールのサンプルを残すために Spam と判定されたメールの目視による再分類も実行している．現在，アーカイブしている Spam メールの数は，20000 通を超え，今も日々増え続けている．Spam メールのアーカイブとその解析は，Spam 対策を検討するためには実態の把握が必要と考えたからである．著者宛に送られてくる Spam が Spam の代表的サンプルという保証はないが，20000 通を超える Spam の解析は，Spam の特徴を把握する一助になると考えられる．

今回，保存しているフィルタのログおよび全 Spam メールのヘッダ情報を解析し，その結果に基づいて，Spam 対策の基本的なありかたについて検討する．

データの解析

解析に用いた Spam メールは, 名古屋大学情報連携基盤センターの共同利用のメールサーバ(以下メールホストと呼ぶ.)の著者の ID 宛に届いたものである. 解析は, 2003 年 8 月 8 日から 2004 年 6 月 8 日までの Spam メールのアーカイブおよび bsfilter のログについて行った．この間の Spam メール数は 22969 通である.

名古屋大学では，Spam 中継被害対策およびウィルス対策のために，外部からの SMTP 接続を２系統にファイアウォールを用いて制限している．各系統は，外部からのメールを受信する中継サーバ，ウィルスチェックサーバおよびウィルスチェックのすんだメールを内部に配送する配送サーバより構成されている．このシステムの概念図を図 1 に示す．中継サーバおよび配送サーバの MTA は postfix[4] である．系 2 は，系 1 のバックアップ経路として用意しており，DNS の MX 値を系１に対して大きく設定している．系 1 と系２の差は，配送サーバの仕様だけである．系 1

の配送サーバには下流の停電等に備えて十分な容量のスプールを確保している. 中継サーバおよび配送サーバは，Sparc Ⅲ 400MHz, メモリー 256MB という少し古いものであり，能力的には少し問題がある.

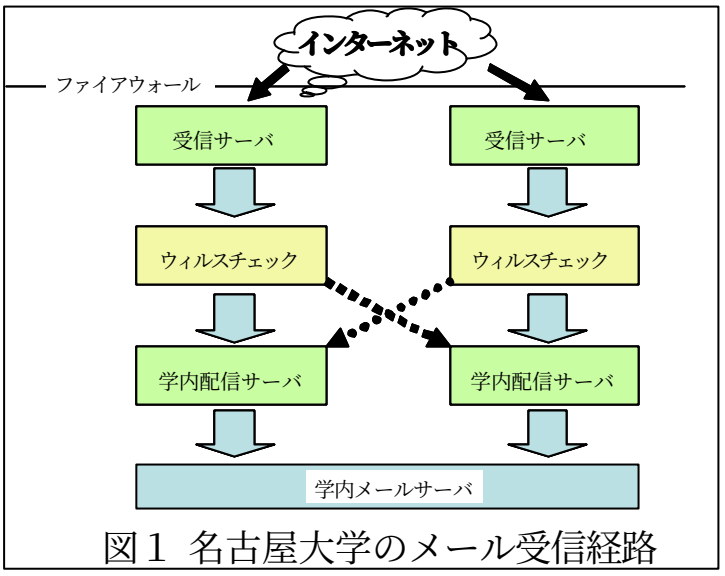

図１ 名古屋大学のメール受信経路

メールホストに到着した Spam メールのヘッダの情報から, メールが中継サーバに到着した時刻, 配送サーバに届いた時刻, メールホストに届いた時刻およびメールを中継サーバ発信したホストに関する情報を Perl スクリプトにより抜き出した.

Spam メールを収集しているメールホストは，DNS 的には名古屋大学外からは MX が見えないように設定されているが，POP before SMTP サービスを提供しているので，直接ホスト名や IP アドレスを指定すれば外部からの SMTP 接続が可能となっている．今回の調査期間中に，このホストに外部から直接送られた Spam メールの数は 198 通であった．これは，全 Spam 数の 1%未満であり，この 198 通はヘッダ解析の対象外とした.

メールの件数および分類

図 2 に，2003 年 8 月 8 日からの Spam メール件数の変化を日付を縦軸にとって示す．期間の当初の約 20 件/日に比較すると，2004 年の 6 月には，8 倍以上の 160 件/日と日々Spam が増加していることがわかる．2004 年 1 月, 2 月, 3 月に顕著な Spam メール数の減少が見られる点に着目されたい．この原因については，後ほど考察する.

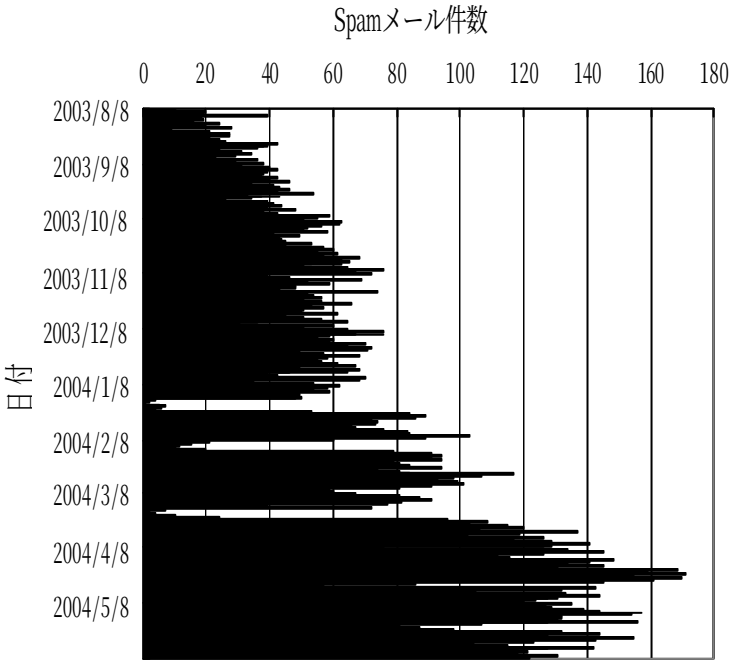

図2　実Spamメール解析によるSpam件数の推移

この期間の bsfilter および procmail による処理では，分類として，Spam，spoof（著者のアドレスを詐称したことによるエラーメール），ham（正常なメール）に分類している．この分類による各メール数の変化を積み重ねグラフにして図３に示した.

図３からは，定常的に受信するメールの半数が Spam であることがわかる．また，先述した 1 月, 2 月, 3 月の Spam の減少についても特異な状況が読み取れる．2 月には Spam 数減少の時期に，偶然か著者のアドレスを詐称したメールが無視できない数あったことも見て取れる.

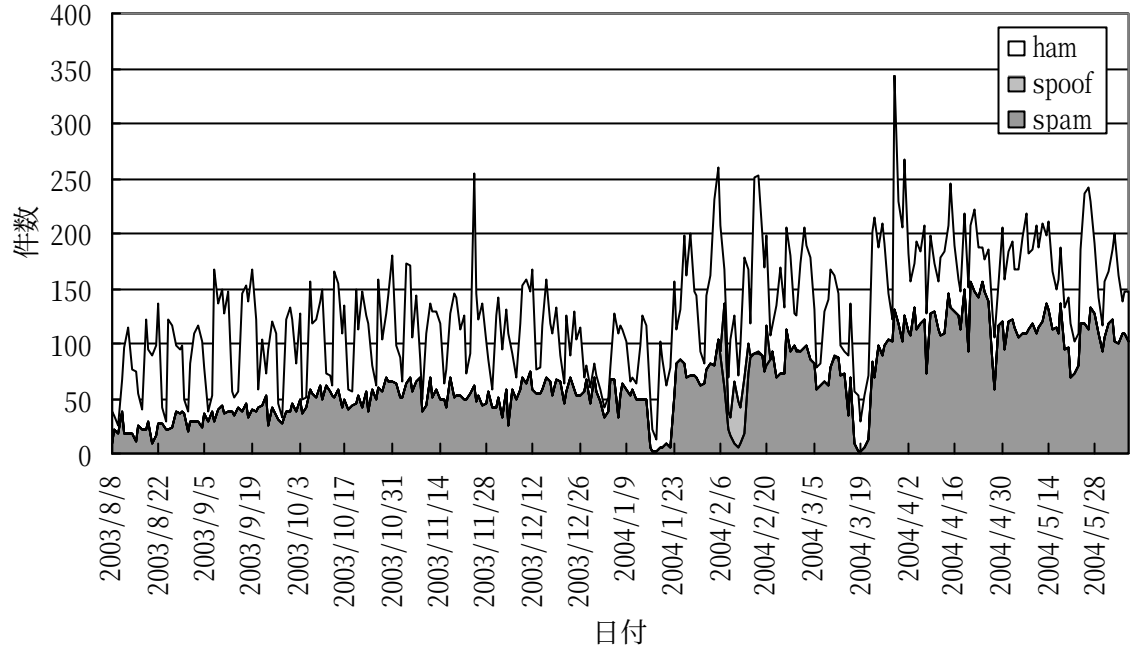

図 3　メールの bsfilter と procmail による分類

Spam はどこから来るか？

ヘッダから抜き出した Spam 発信元の IP アドレスを元に逆引きを試みた．表 1 に，Spam 発信に利用されたドメインの名前と当該ドメインからの Spam メール送付件数を示す．ただし，Spam メール発信数の少ないドメインについては，まとめて示している．

Spam 送付に使われたホストのうちで，DNS の逆引きが設定されていないものが約 32%存在する．これに対して，200 通以上（割合にして 1%以上）Spam メールを発信したドメインは非常に限定されていることが見て取れる．表では，ISP 単位にまとめているために読み取れないが，DNS の逆引き結果をみると，大量の Spam メールは ISP が DHCP により動的に割り当てていると推定される名前のホストから発信されるケースが大半をしめている．

表 1 IP アドレスから見た Spam 送信ドメイン

ドメイン	送付件数	比率（%）
shawcable.net	221	1.13
swbell.net	262	1.34
charter.com	282	1.44
dsl-verizon.net	284	1.45
adelphia.net	293	1.50
ameritech.net	320	1.63
pacbell.net	362	1.85
optonline.net	390	1.99
attbi.com	711	3.63
発信 1 回	731	3.73
rr.com	822	4.20
発信 10 回以下	1360	6.95
発信 200 回以下	1432	7.31
発信 100 回以下	3806	19.44
comcast.net	2181	11.14
未設定	6125	31.28
合計	19582	100.00

HELO コマンドで与えられる情報と実際に接続してきたホストのドメイン名との一致度を調べると，結果は図 4 のようになる．図 3 および図 4 から，逆引きが設定されていないものおよび逆引きと HELO パラメータ値の不一致の排除に，大量の Spam を送付してくる ISP のアドレスの排除を組み合わせると約 6 割の Spam メールが排除できそうである．ただし，DNS で引けるかどうかだけの検査だけでは，大規模 ISP のブロードバンド端末からの Spam 発信は，排除できないこともわかる．

以上は，IP アドレスから見たケースであるが，メールヘッダの From から見た場合の差出人の所属ドメインの分類は表 2 のようになる．もちろん，Spam メールの From の値は詐称されてい

表２ よく使われる From 値

From のドメイン	Spam 件数	割合 (%)
yahoo.com.hk	101	0.50
yahoo.ca	109	0.53
juno.com	122	0.60
earthlink.net	136	0.67
email.com	148	0.73
LYCOS.COM	156	0.77
excite.com	184	0.90
mail.com	190	0.93
attbi.com	239	1.17
aol.com	501	2.46
MSN.COM	751	3.68
HOTMAIL.COM	994	4.88
yahoo.com	1665	8.17
100 回未満	4547	22.30
1 回きり	4727	23.18
10回未満	5819	28.54
合計	20389	100.00

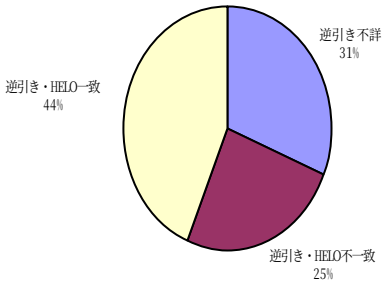

図4　逆引きとHELOパラメータの関係

るのが普通なので，これは詐称に利用されやすいドメインのリストでもある．なお，１回だけ Spam 発信元に使われるアドレスが 5000 近くあるので，データベースを利用して，初見の From からの接続を一旦サーバエラーとして拒否する方式も考えられる．いわゆる「一見さんお断り」方式[5]も，30 分程度の配送遅延を許容するならば一定の効果が見込まれる．

しかしながら，値やパターンでフィルタするという観点からは，IP アドレスもしくは ISP のドメイン名でフィルタするのに対して，ヘッダの From の値によるパターンマッチフィルタは，効率が悪いといえる．

Spam 対策と問題点

もっとも古典的な Spam 対策である DNS のチェックおよび前節で指摘した大口の Spam 送信 ISP を排除した効果は，前述したように，図２および図３に示されている．図３中の 1 月，2 月の Spam 量の落ち込みは，それぞれ 1 月は，大口(comcast.net,client.attbi.com 等の表 1 中の ISP および明白に動的アドレスとわかるドメイン)からの接続の拒否，2 月は DNS 検索による受信拒否を行った結果である．3 月の配送量の落ち込みは，特定の Spam 発信に利用されたドメイン名（gfk.se ドメイン）からのメール受領拒否設定に対応している．しかしながら，対策開始と同時に，Spam メールの顕著な減少という明白なフィルタの効果とともに，正常なメールの受信数の落ち込みとメール配送の許容できない遅延がみられるようになった．問題のメール配送遅延は，設定（1 月 16 日，2 月 14 日，3 月 17 日の午前 9 時）から 2〜3 時間で始まり，MTA の再起動やシステムのリブートでは回復しなかった．1 月および 2 月に発生した配送遅延は，Spam 拒否設定を解除後 1 週間で正常に戻った．

このメール配送異常の考えられる原因として，

（１） Spam 拒否設定のためのシステム資源不足
（２） Spam の短期的集中によるシステムの資源不足
（３） Spam 発信者からのメール中継システムへの DDoS 攻撃が考えられる．

しかし，Spam 拒否設定解除の効果が，数日以上経過しないと見えてこない事実から，（1）の資源不足は直接の原因とは考えられない．（2）ならば，Spam 拒否設定の有無にかかわらず発生するはずである．また，メモリーリークのような資源不足が原因であれば，システムの再起動によって回復することが予想される．しかしながら，1 月から 3 月にかけて発生した異常は，MTA の再起動やシステムの再起動を繰り返しても解決しなかった．したがって，（3）の DDoS の可能性がもっとも高いと考えられる．

3 月の異常については，関係する拒否ドメインが 1 個のみなので，原因を DDoS と仮定して，問題が長く継続しないと予想して解除しなかった．実際に，予想どおりに異常な状態は約一週間で収束した．

問題の原因を明白にするために Spam 数の変動と中継サーバへの外部からの SMTP 接続の状況の関係を調べた．期間はログが得られた 2 月 1 日から 3 月 31 日の範囲である．その結果を図５に示す．図５から，拒否設定を行った直後から，完結しない SMTP 接続（lost connection）が増加し 1 週間近く継続していることが読み取れる．

システムが接続数の増加による負荷に対応できず，その結果ロストコネクションが発生している可能性も捨てきれないので，さらにコネクト数とロストコネクション数の比について調査した．ログのローテーションの関係で，図 5 と 1 週間期間がずれているが，比の変化を図６に示す．

問題の期間中，中継サーバの MTA（postfix）で設定した受信プロセス数の上限までの接続が常

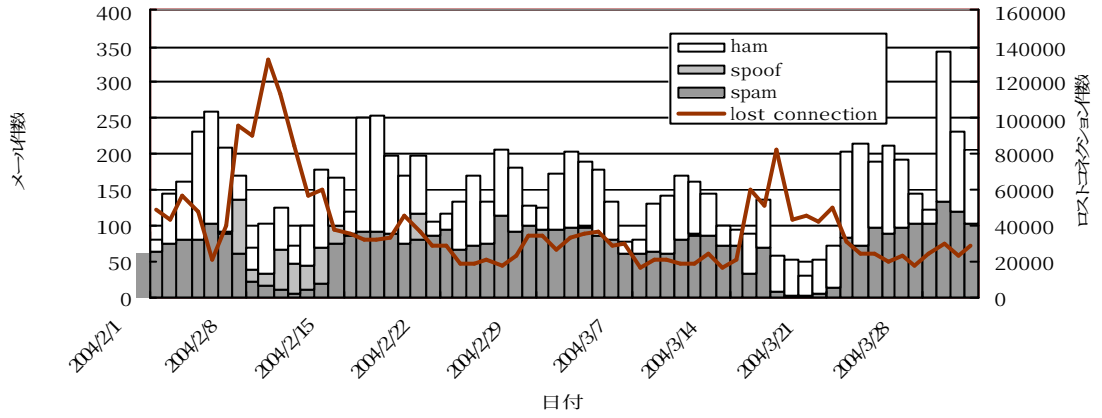

図５　Spamフィルタによるメール分類の時間変化とSMTP接続

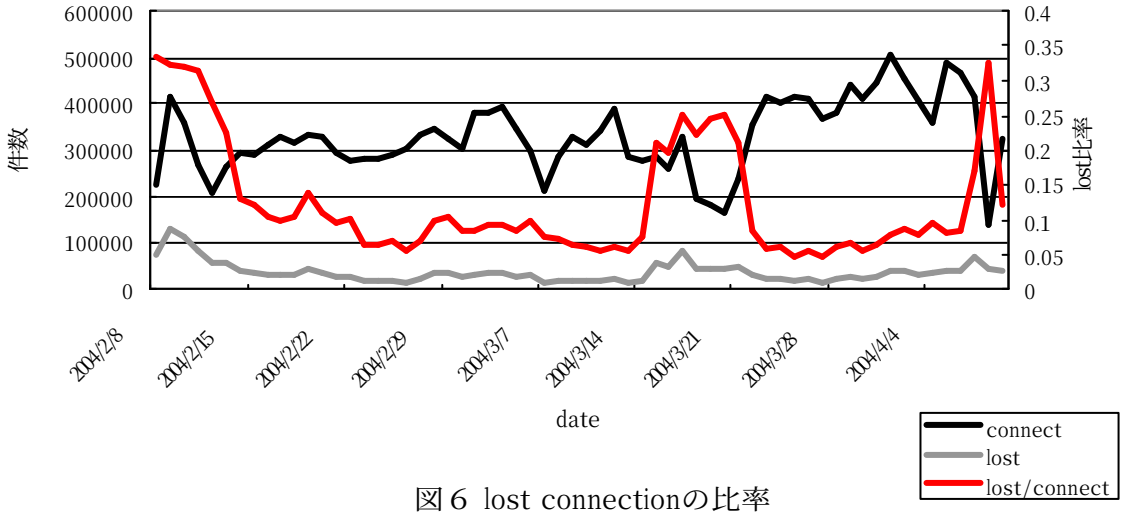

図６ lost connectionの比率

時存在した．ログからは，コネクトしたままタイムアウトまで放置する，もしくは，コネクトして切断するという状況が継続して発生していたように見えたが，図６からも異常な接続の存在が見て取れる．なお，図６の 4 月に発生している異常は，システム再起動によって解決したので，３月までの Spam 拒否設定による問題とは原因が異なると考えられる．

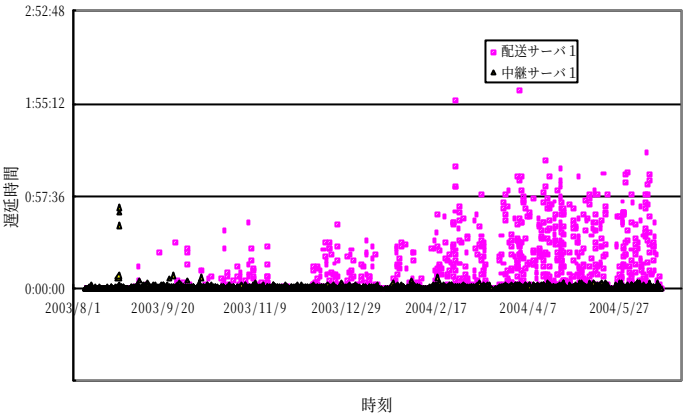

図7　遅延時間の推移（系統1）

メール遅延の解析

メールのヘッダの解析から，メール系統１（主系統）でのメール配送遅延の時間変化を中継サーバと配送サーバについて図 7 に示す．ここで，メール配送遅延とは，1 個のメールについて，中継サーバでの外部からのメール受信時刻と配送サーバでの受信時刻の差および配送サーバでの受信時刻とメールホストでの受信時刻の差を言う．前者を中継サーバの遅延，後者を配送サーバでの遅延と考えることにする．

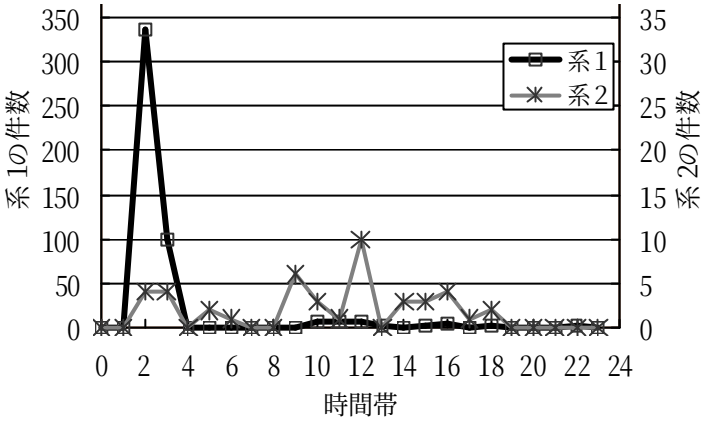

図８　メール配送遅延時間の系統別・時間帯別分布

図７からは，遅延が配送サーバに起因することが明白である．これは，受け取ったメールを原則として次のサーバに発送する作業だけを実行する中継サーバおよびウィルスチェックサーバに比して，配送サーバでは，すぐには配送できないメールをキューに書き出したり，定期的にキューされたメールの再送をするといった処理が必要な分だけ負荷が高いためと思われる．

配送遅延が 10 分以上のメールについて，中継サーバでの受信時間帯ごとの件数を図８に示した．図８からは，メール遅延の発生が午前 2 時台および３時台に集中して発生していることが明らかである．また，MX 的に系統１のバックアップとなっている系統２には，系統１に見られるような明白なピークは存在しない．これらのことから，Spam の発信が MX を参照せずに行われていることが推測される．また，Spam 発信そのものが少数のグループによってコントロールされているようである．

Spam とポートスキャン

Spam メールの発信元とポートスキャンの発信件数の関係を調査してみた．前節で，Spam 対策と DDoS との関係について述べた．DDoS を疑った根拠のひとつは，フィルタの設定直後に，Spam フィルタに設定したドメインからの Telnet

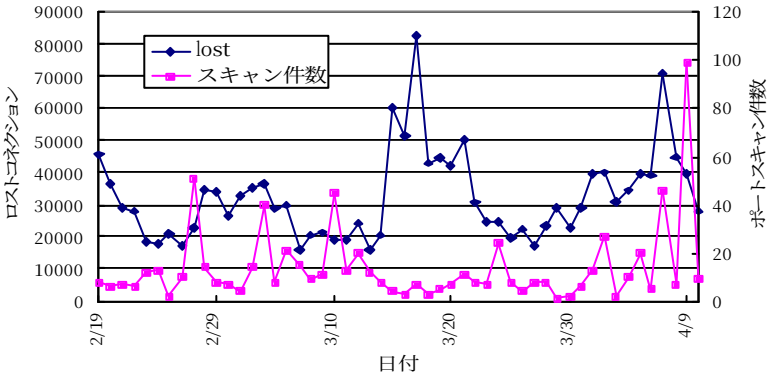

図9　ロストコネクションとポートスキャン

ポートや FTP ポートへのスキャンが増加したように体感したからでもある．MTA によるフィルタかファイアウォールによるドメイン単位のフィルタなのかをプロファイリングされているように感じた．この実感が，単なる錯覚なのかを確認するために，ロストコネクション数とポートスキャン数の対応のグラフ化を試みた．日単位で見た場合，DDoS に先立つスキャンといった現象はなかった．念のために，中継サーバの tcpd のログで不正アクセス件数を調査してみたが，DDoS と連動した傾向はなかった．

Spam フィルタの効果

Spam メール対策の中で，ベイズ統計を応用したフィルタの利用が一般的になりつつある．このような統計に基づくフィルタでは，誤検知が問題になる．ここでは，ベイズ統計を利用したフィルタの一つである bsfilter のログと実際に人間の手で分類した Spam 件数を比較して図 10 に示す．

実際の Spam 件数を分母にとっているので，比が 1 を越えるというのは，Spam でないものを Spam と判定したということであり，比が 1 未満というのは Spam を見落としたことになる．Spam 発信側でも，ベイズ統計フィルタのデータベースを乱すための 5 文字程度の大量の無意味ワードよりなるメールの送信や 255 文字以上の無意味単語よりなるメールが増大しており，導入当初の 100%近い bsfilter の Spam 検出率が時とともに徐々に低下していることが見て取れる．

センターとしての Spam 対策

センターとしてオープンリレー対策やウィルスメール対策とともに Spam 対策を行う場合，DDoS の可能性を考慮したハードウェア能力の高いシステムが必要である．内部ネットワークに Spam メールの到達性をモニタする端末が存在することも考慮に入れた定期的なネットワークやホスト機器の監査も必要と考えられる．

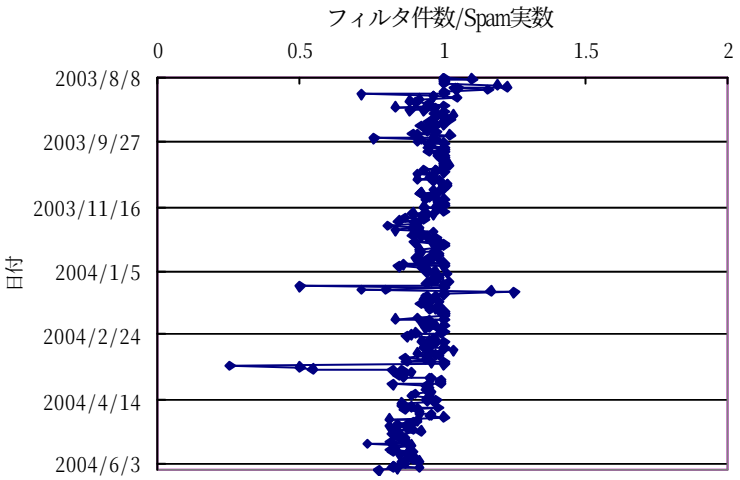

図10　Spamフィルタの検出率の推移

利用者によって，Spam の定義が異なるので，一律に Spam メールを排除することには困難があり，誤ったフィルタを避けるためには，Spam 判定の閾値を意図的に低くしなければならない．したがって，Spam 対策を組織として導入するなら，Spam メールにマークを追加して，実際のフィルタ操作は利用者に任せるという運用が理想的である．しかしながら，あくまで Spam フィルタ等の対策は，小手先の対策であって，Spam メールを根本的になくすには，大規模 ISP の管理体制の問題，大規模 ISP や IDC の不適切な DNS 管理といった問題を解決することが必要である．大規模 ISP の対応が当てにできないなら，プロトコルや MTA といったレベルでの認証といった課題に取り組む必要がある．

おわりに

本論文では，アーカイブしている Spam メールのヘッダの解析結果を中心に述べた．究極の Spam 対策は発信元対策であるが，現状では，より効果的で誤りの少ないフィルタ方式が望まれている．どのような方式であれ，統計的手法による判別では，誤検出は避けられない．より効果的なフィルタを実現するには，メールの内容まで理解したフィルタが必要であり，そのためにも，今後はアーカイブした Spam メールの本文解析を行いたい．

なお，本研究は，著者が名古屋大学在籍中に着手したものである．

参考文献

[1] http://www.spamassassin.org
[2] http://www.bsfilter.org
[3] http://www.procmail.org
[4] Venema, W., http://www.postfix.org
[5]前野年紀，http://spam.qmail.jp/onazimi/index.html，2004