社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2004－DSM－34 (7)
2004／7／30

Spamメールの解析

長谷川 明生
中京大学生命システム工学部 〒470-0393 豊田市貝津町床立101
hasegawa@akg.life.chukyo-u.ac.jp

あらまし 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も考察する。

キーワード Spam, UCE, Spamメール解析, Spam対策

Analysis of Spams

Abstract

Mails so called Spam or UCE have been increasing daily by anomalous rate. Since last August, the author archives UCE mails which sent to him. And the numbers of UCE mails archived exceeds 20000. These Spam mails are analyzed to find out the source addresses, origin and other characteristics. The author will make a brief discussion on the counterplan to Spam based on the analysis.

Keywords Spam,UCE, Analysis of Spam Mails, Counterplan to Spam

はじめに

2003年4月頃より，いわゆるSpamやUCEもしくはUCBと呼ばれる迷惑メールの数が急増してきている。このようなメールに対処するためのソフトウェアはオープンソースのSpamAssassin[1]やbsfilter[2]の他に商用のアプライアンスも含めて急速に増えてきている。しかし，これらの利用によっても，誤検知の危険はゼロではない。その一方で，このようなメールへの人力による対処は,その件数の増加のために不可能になりつつある。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。

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，コストのかからないSpam対策の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。中継サーバおよび配送サーバのMTAはpostfix[4]である。

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。

メールホストは，POP before SMTPサービスを提供しており，外部からのSMTP接続が可能となっているが，このホストに直接送りつけられたSpamメールの数は198通で，全体の1%未満であり，この198通はヘッダ解析の対象外とした。

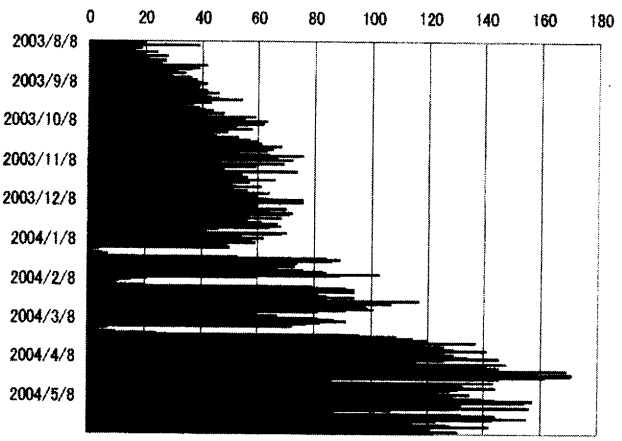

図1 実Spamメール解析によるSpam件数の推移

メールの件数および分類

図1に，Spamメールの件数を日毎に集計して示した。2003年8月の約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。

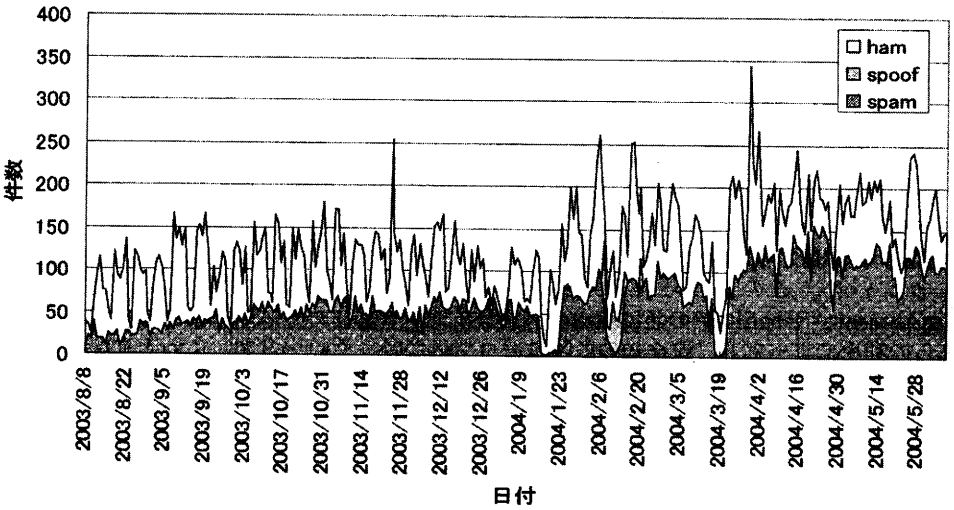

図2 メール分類

bsfilterのログからは，Spamメール，著者のアドレスを詐称したSpamのバックスキャッタ，通常のメールと，より細かい分類でメールの状況が理解できる。

図2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。

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アドレスの逆引きを試みた。図3に，Spam発信に利用されたドメインの割合を円グラフで示す。

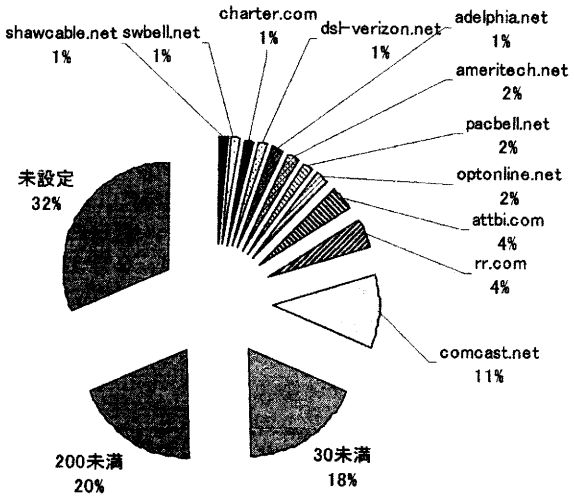

図3 Spam送信ドメイン別分類

DNS の逆引きが設定されていないものが 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。より詳細にみると，これら ISP の動的アドレスが利用されているケースが大半である。

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を調べると，結果は図 4 のようになる。

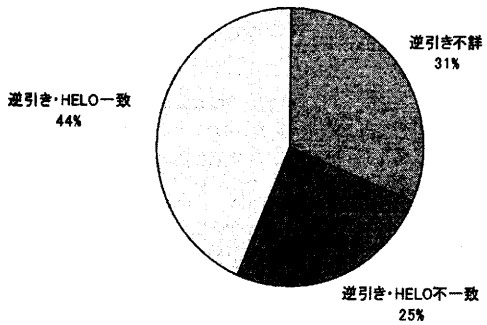

図4 逆引きとHELOパラメータの関係

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。なお，1 回だけ Spam 発信元に使われるというアドレスが 4000 近くあるので，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。

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 を排除した効果は図1および2に示されている。図2中の1月，2月の Spam 量の落ち込みは，それぞれ大口(comcast.net,client.attbi.com 等の図3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，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成果とともに，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可能な原因として，

（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，数日異常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，システムの再起動を繰り返しても解決しなかった。結果として（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。

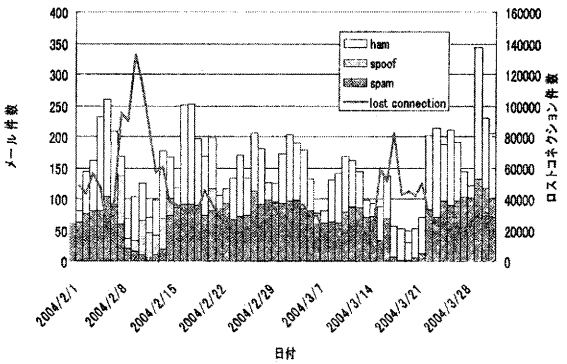

図5 Spamフィルタによるメール分類の時間変化とSMTP接続

問題の原因を明白にするために Spam 数の減少と中継サーバのログの得られた期間の外部からの SMTP 接続の状況の関係を調べた。

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たが読み取れる。コネクト数とロストコネクションの比の変化を図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。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。

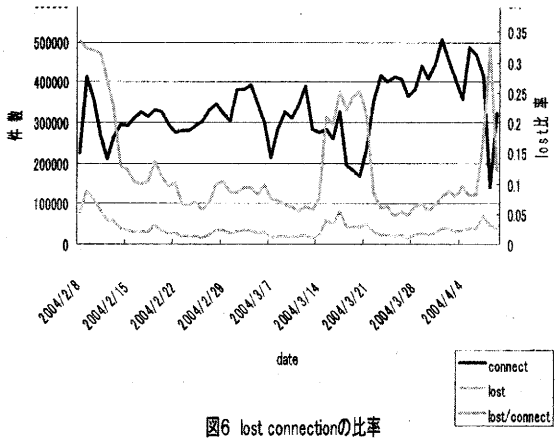

図6 lost connectionの比率

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，中継サーバでの受信時間，配送サーバでの受信時間およびメールホストでの受信時間の差を言う。

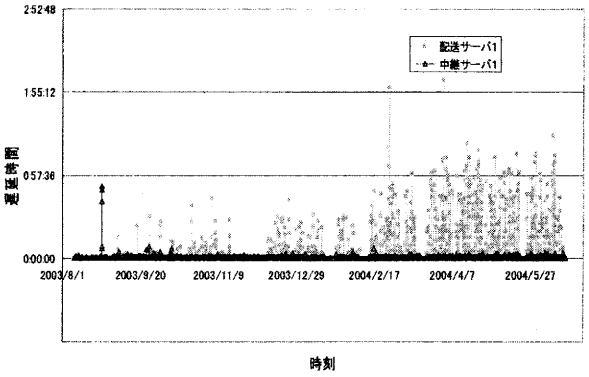

図7 遅延時間の推移(系統1)

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スルーする中継サーバおよびウィルスチェックに比して，配送サーバでは，配送できないメールキューの管理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発生件数を図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。

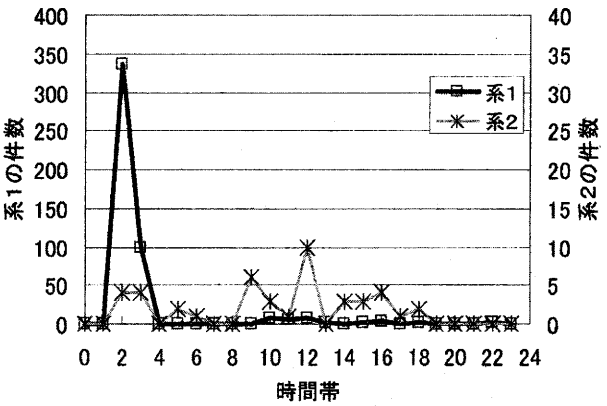

図8 メール配送遅延時間の系統別・時間帯別分布

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。このような統計の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分類による Spam 件数を比較して図９に示す。

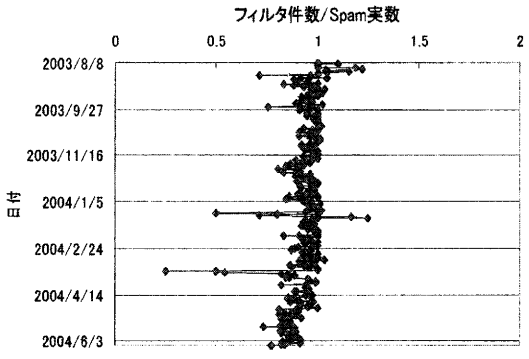

図9 Spamフィルタの検出率の推移

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。

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すして，実際のフィルタ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
[4]前野年紀，http://spam.qmail.jp/onazimi/index.html，2004