東邦学誌
第34巻第2号
2005年12月
論　文

# 大学ネットワークにおけるspam対策とその効果

成　田　良　一

目　次

はじめに
1．インターネットにおけるspamの現状
2．spamの防止対策手法
3．spam防止対策の実際
4．spam防止対策の効果
5．spam防止対策の課題

## はじめに

本稿ではspamの現状とその対策について述べる。まず現在のインターネットにおけるspamの状況がどのようなものであるかを概観し、現状の防止対策手法の概要を述べる。筆者が所属する東邦学園大学・短期大学のネットワークでは、一年半ほど前からspamに対する防止対策を講じてきた。そこで採用した防止対策を時間順に報告し、管理運用上で生じてきた各種の問題点を論ずる。さらに、筆者個人が収集したspamの解析を行って防止対策の効果を計る。最後にspam防止対策の課題をまとめる。

## 1．インターネットにおけるspamの現状

### （1）spamと迷惑メール

電子メールはインターネットの初期の頃から使われ、インターネットでもっともよく使われているアプリケーションである。比較的簡単な仕組み（SMTP, cf.［1］,［2］）によって配送が行われ、電子メール自体のフォーマットも単純なものである。そのため、セキュリティ上の問題も残されており、それを悪用する者が非常に増えている。1990年代前半にもそのような悪用はあったが、1990年代後半から顕著に増大し、最近ではインターネット全体のトラフィックとしても無視できないものになっている。

電子メールの悪用にもさまざまな形態と名称がある。まず、spam, Junk Mail, UCE (Unsolicited Commercial Email), UBE (Unsolicited Bulk Email) など、これらは受信者が望まないメールを不特定多数に対して大量に送付する類いを指す。内容は広告・宣伝、詐欺、嘘の情報などが多い。本稿で扱うのはこの種類のメールである。代表してspamと呼ぶ[1]。

ウィルスメールも電子メールの悪用の一種である。ウィルスメールは大量に送付されることがあるが、これはメールの内容がコンピュータウィルスであり、ウィルス自体の伝搬を目的としたものであるため、spamとは性格が異なる。また総じて迷惑メールと呼ぶこともあるが、これはspamやウィルスメールを含んで、受信者が迷惑と感じるメールという一般的な用語である。また、最近フィッシング（Phishing）というメールとWWWを連動した詐欺の形態も増

加している。銀行やクレジットカード会社などの Web ページと同じデザインのページを作り、メールに記載されている URL を辿らせて誘い込む手口である。これはメールの様式に限って言えば、spam による詐欺の一種とみなすことができる。

spam を送る者（以下、spam 送信者と呼ぶ）は、単なる愉快犯もいるが、最近では営利を目的とする業者であることが多い。一般の受信者が望まないメールであっても、中には興味を抱く受信者もいて、その反応によって商品販売の利益を得たり、詐欺の犠牲者とするのである。一方、インターネットメールを大量に送付してもコストは安価であってほぼ一定である。そのため、大量に配布すればするだけ利益が上がるという構造になっている。

### （2）spam の手口

spam を防止する対策をとるためには、spam について詳しく知っておく必要がある。本項では spam のメールとしての特徴と spam 送信者の手口の概略を述べる。

spam の送付は、まず送り先のメールアドレスの収集から始まる。膨大なメールアドレスのリストが（公然または非公然に）販売されている。Web ページやネットニューズアーカイブなどに含まれるメールアドレスを自動収集する方法もある。また、よくある名前を列挙してドメイン名の前につけたメールアドレスを生成して用いることもある。最後の方法では膨大な宛先不明エラーが生じることになるが、後述するように差出人のメールアドレスを詐称してエラーメールや苦情の宛先を他に向けたり、他のサイトのメールホストを乗っ取ったりすることで spam 送信者自身への負荷を軽くしている。

spam 送信者はヘッダを改竄する。通常のメールでは受信者に届くまでの配送途中で経由したメールホストが Recieved ヘッダに記録されていく。spam 送信者の多くは、発信元と経路を特定しにくくするためにこの部分を偽造して送っている。そのため、自組織のメールホストに届く直前までの情報は信用できないことになる。また発信者自身の From アドレスを詐称しているのも当然であり、エラーによる Bounce メールが戻る Return-Path ヘッダも偽造している[2)]。これらの詐称メールアドレスも上記のリストなどからランダムに選ぶ手口が多い。

メールホストは古くは色々なメールを転送するような運用になっていた。これを悪用するとサイト外からそのメールホストを経由して外部に spam を送ることが可能になる。これを第三者不正メール中継あるいはオープンリレーと呼ぶ。spam 送信者自身の負荷を軽減するとともに、送信経路を混乱させるという効果がある。これに対しては、1990 年代初期から各組織で対策がとられて、メールホストが配送を受け付けるのは自ドメインのみとするように運用が改められた。しかし、まだ第三者不正メール中継を行うホストは存在するし、HTTP を経由した巧妙な乗っ取り手法なども使われている。

また、最近ではメールホストだけでなく、個人のパーソナルコンピュータも spam 送信に使われている。ウィルスなどによって個人のコンピュータを乗っ取り、所有者が知らないうちに spam を送信するという手口である。これをゾンビ（zombie）やボット（bot）と呼ぶ。OS のセキュリティアップデートなどを行わない初心者が狙われている。ゾンビの数は数千万台になっているという観測（cf. [3]）もある。

メール本文については内容による spam フィルタリング手法がある。spam 送信者はそれに対抗するために、ランダムなキーワードを挿入してベイジアン・フィルタリングをすり抜ける手法や、HTML メールにして一文字ごとに

HTML のコメントタグを挿入し単語の抽出を困難にするような手法を使っている（cf. [4]）。メール本文を見てそれが spam かどうかを判断するのは、最終的には人間である。内容によるフィルタリング手法の開発も進んでいるものの、自動的な排除は難しく、フィルタリング手法が高度になればそれに対抗する spam 送信の手口も高度になっていく。

## 2．spam の防止対策手法

spam を防止するのは MTA（Mail Transfer Agent）か MUA（Mail User Agent）かという議論がある。個人が容易にできる対策としては MUA による spam の分別である。最近の MUA では spam フィルタ機能を備えるものも増えてきた[3]。しかしメールホストが spam を受け取るということはインターネットのトラフィックを増加させることにつながる。インターネット全体の資源を spam から守るという視点から見ると、spam を受け取ること自体が問題であり、各サイトの最前段のメールホストにおいて防止対策をとることが必要不可欠である。MUA 側では MTA での防止策をくぐり抜けた少数の spam を排除するということになり、併用することで MUA 側の負荷も軽くなる。

以下には MTA における代表的な spam 対策手法をあげる。主に SMTP セッションでのフィルタリングの手法である。

### （1）ブラックリストとホワイトリスト

インターネットメールでは、メール配信の際に、外部の送信メールホストと自組織の受信メールホストの間で SMTP セッションが行われる。このとき、自組織の受信メールホストでは相手の IP アドレスやドメイン名が認識できる。相手のメールホストが spam 送信者のものだとわかっていれば、あらかじめブラックリストに登録しておき、受け取りを拒否することができる。また、相手のメールホストが信用できるものだと判断すれば、あらかじめホワイトリストに登録しておき、他のフィルタを経由せずに受け取ることができる。

この方法は、あらかじめユーザー側で spam だとわかっているものに対しては、完全な効力を発揮する。しかし、リストへの登録は人手で行う必要があり、spam 送信ホストは 1. に述べたようにゾンビも含めると膨大な数であるため、これだけで spam をブロックすることは困難であって、他の手法と併用する必要がある。

### （2）公開ブラックリスト

1.（2）で述べたように第三者不正メール中継を行うメールホストは少なくない。その対策として、このようなホストを収集して、リストを一般に公開することが古くから行われてきた。これを ORBL（Open Relay Black List）と呼ぶ。いくつかの組織が ORBL の運用を行っている。ORBL では申請や独自の調査（多くは自動化されている）により第三者不正メール中継ホストを収集してデータベースとしている。このリストは Web で公開され IP アドレスによる検索ができる。また MTA とのインタフェースがあり、MTA がフィルタリングする時の判断に利用できるようになっている。これは DNS を利用した仕組みであり、逆引きドメインに類似の形式で IP アドレスを埋込んだドメイン名を生成し、それを DNS クエリーによって検索できるようにしている。この仕組みから、DNSBL（DNS Black List）と呼ぶこともある。

第三者不正メール中継ホストはその管理者の未熟さや設定ミスによって起こることが多い。一度ブラックリストに載ると、そのサイトからのメールが拒否される事態が頻繁に起

こって管理者が気付くことになる。管理者が修正を施して第三者不正メール中継ホストで無くなった[4]場合には、ブラックリストからの抹消申請を行うことによって、公開ブラックリストからは削除される。インターネットにおいてメールが使えないという事態は致命的である。管理者は第三者不正メール中継ホストにならないように充分注意するとともに、もし公開ブラックリストに載った場合には速やかに対処する必要がある。

### （3）DNS チェック

これは、外部の送信メールホストとの間のSMTP セッションで得られる IP アドレスあるいはドメイン名を用い、DNS でわかる情報によって制限を行う方法である。PTR レコードを持つか、A レコードを持つか、PTR レコードと A レコードの一致を見る（パラノイド検査)、MX レコードを持つか、などの条件判断によって拒否するか否かを判断する。

### （4）グレイリスティング

グレイリスティング（greylisting）は2003年頃から使われ出した比較的新しい手法である。これは、「初めて届く」メールに対しては一度 4xx 系のエラーを返し、一定時間後に再送してきたら受け入れるという方式である。SMTP において 4xx 系のエラーはメールホストが一時的にメールを受け入れることができないことを表す。この場合には、SMTP では送信メールホストは一定の時間をおいて再送するという仕様（[1]）になっている。従って通常のメールであれば再送されて宛先に届くはずである。ところが spam 送信者は、再送するコストをかけず、すぐにあきらめて大量に配信することに専念することが多いようである。グレイリスティングは、このような spam 送信者の行動モデルに基づいて spam を阻止する仕組みである。

「初めて届く」メールの判断にはいくつかの考え方があるが、通常次の三つ組が一致するか否かで判断する。

(a) SMTP 送信元の IP アドレス
(b) The envelope sender address
(SMTP の MAIL FROM)
(c) The envelope reciept address
(SMTP の RECIEPT TO)

グレイリスティングの詳細については［5］を参照されたい。

### （5）メールヘッダパターンフィルタリング

これは上記の各種フィルタリングと異なり、メールのヘッダを見て判断する手法である。コンテンツフィルタリングの一種とも言えるが、メールボディの内容から判断するのではなく、ヘッダのパターンによって動作を指定するため、形式的な判断が容易である。たとえば X-Mailer を参照して、spam 送信者がよく使う種類の 大量配信用 MUA を判別し、そのメールを拒否することが可能である。

但し、このようなフィルタリングは SMTP セッション中に実行することはできない。一度メールを受け取り、キューに入れてから内容のパターンマッチングを行って指定された動作を行うことになる。

## 3．spam 防止対策の実際

本節では東邦学園大学・短期大学（以下、本学と記す）のネットワークで実施した spam 防止対策について述べる。

本学ではサーバー系のマシンの OS として Redhat Linux を用い、MTA は Postfix[5]を使用している。DMZ にメールゲートウェイを置き、外部からのメールはメールゲートウェイ

を通じて内部のメールホストに中継され、内部から外部に出されるメールは内部メールホストからメールゲートウェイを経由して外部に送られる。メールゲートウェイとして迷惑メールフィルタリング機能を持った専用製品を使用することも考えられるが、Postfix のフィルタリング機能によっても強力な制限が可能である。また Postfix は現代の代表的な MTA の一つとして使用者が多く開発も進んでおり、設定の柔軟性も高い（設定の詳細については［6］を参照せよ）。将来的に専用製品に置き換えるとしても、フィルタリングの機能や効果の評価が必要である。これらの理由から、メールゲートウェイにおける Postfix によるフィルタリングを行うこととした。

**（1）基本的フィルタリング（2004年4月21日～）**

次のフィルタリングを行った。

(a) ユーザー申請に基づくホワイトリスト
(b) ユーザー申請に基づくブラックリスト
(c) ORBL による拒否
(d) unknown client の拒否

ホワイトリストとブラックリストは最初は空であった。ユーザーからの情報に基づいて、拒否してはいけないものをホワイトリストに登録し、拒否すべきものをブラックリストに登録していった。

ORBL としては、ORDB（Open Relay Database, http://www.ordb.org/）および DSBL（Distributed Sender Blockhole List, http://www.dsbl.org/）を使用した。これらは広く使われているものである。

運用としては、学内ユーザーに届くはずのメールが ORBL によって拒否されることが問題となった。これは相手側のメールホストが第三者不正メール中継ホストとして登録されているということであるから、基本的にはそのホストからのメールは世界中で拒否されるいう重大な問題である。相手側の管理者が気づいていない可能性があり、電話などで直接連絡して、対策をとることと ORBL に抹消申請をしてもらうことを依頼することになる。連絡の結果、対策までに時間がかかるような場合には、一時的にホワイトリストに登録した。公開ブラックリストから削除されたことが確認された後で、ホワイトリストからも抹消した。相手先の連絡先の調査から始まり、実際の管理担当者に状況を伝えることが必要であり、人手のかかることである。ただ、インターネットコミュニティの一員としては避けては通れない。

ブラックリストについては、4．に述べるように筆者が収集した spam メールを解析して、5回以上送られた送信メールホストの IP アドレスを抽出し、それを使って6月10日に初期リストの作成を行った。ブラックリストの登録はユーザーからの申請によるが、筆者は初期リストと同様の作業を不定期に行って、ブラックリストに追加している。

unknown client は、DNS チェックによるフィルタリングの一つである。送信メールホストの IP アドレスが DNS に PTR レコードを持っていない（つまり逆引きできない）場合、または持っていても PTR レコードの指すドメイン名の IP アドレスと一致しない（逆引きして正引きした時に元と一致しない）場合に拒否する。DNS の運用上、各ドメインの正当なメールホストについては、このようになっているべきものである。そうでない場合は DHCP などによる動的な IP アドレスのついたマシンであったり、不正な手段によって乗っ取られたマシンである可能性が高い。実際、4．で述べるように、筆者の収集した spam メールの8割以上は、このようなマシンから送られている。

ところが、運用してみると、このように正

規の設定を行っていないドメインが数多くあることが判明した。熟練した管理者がいないドメインのみならず、大手の ISP や大規模な大学や企業の DNS 設定がこのようになっていない。上記の ORBL による拒否の対応と同様な対応を行ったが、一週間に一度くらいの頻度で発生したため、手間をかけることが不可能になり、5月17日にはこのフィルタリングの適用を終了した。DNS に関しては、現在ドメイン乗っ取り問題などが注目されているが、基本的な設定に関しても、まともな設定が広まることが望まれる。

**（2）グレイリスティング（2004年10月17日～）**

基本的なフィルタリングによっても、spam メールの数はさほど減少しなかった。防止対策直前に比較して、フィルタリング適用直後には 30% ほどになったが、その後 50-60% 程度に悪化し、2004年9月には防止対策直前とあまり変わらない状況になっていた。spam 発信者は IP アドレスを頻繁に変更して送信してくるため、固定的な IP アドレスのリストでは追いつかないというのがその主な原因である。そのような状況から、グレイリスティングを適用することとした。

Postfix は v.2.1 からグレイリスティングに対応しているため、バージョンアップが必要であった。OS 付属のものを使用せずにソースプログラムからインストールし、一ヶ月間の運用を行って安定性を確認した。その後、グレイリスティングを適用する設定を行った。

詳細は4．に述べるが、グレイリスティングの効果は劇的であった。グレイリスティング適用前と後を比較すると、ほぼ 1/10 に減少している。

最初のメールの拒否の時間は55分に設定した。これは60分の間隔を空けて再送するサイトが多いという仮定に基づくものであったが、ログの分析によると、最近の ISP などではもっと短い間隔で再送しているものも多いことがわかった。そのため2005年8月24日には拒否の時間を 25 分に縮めた。また一度通過した spam はその後はグレイリスティングを通過するため、この設定変更時にグレイリスティングをリセットした。

グレイリスティングの適用後、稀に再送しないサイトがあることもユーザーからの報告で判明している。イベント用の期間限定メールホストのようなもので設定が不十分なものではないかと考えられる。

グレイリスティングは spam を防止する代償として一度だけユーザーに不便をかけるものの、総合的にみてユーザーの利益となるものと評価できる。しかし、初回だけでなく二回目以後もメールが遅延するような場合がある。これは、再送に関しては最初のメールホストが行わず、別のメールホストに送られてそこから再送を行うという運用を行っているために生じる事態である。大規模な ISP などでメールホストの負荷を分散させるための仕組みと考えられるが、これはグレイリスティングには不都合な仕組みである。場合によっては三回目以後も別のメールホストが再送することがあり、何度送ってもメールは遅延して届くことになる。

**（3）その他**

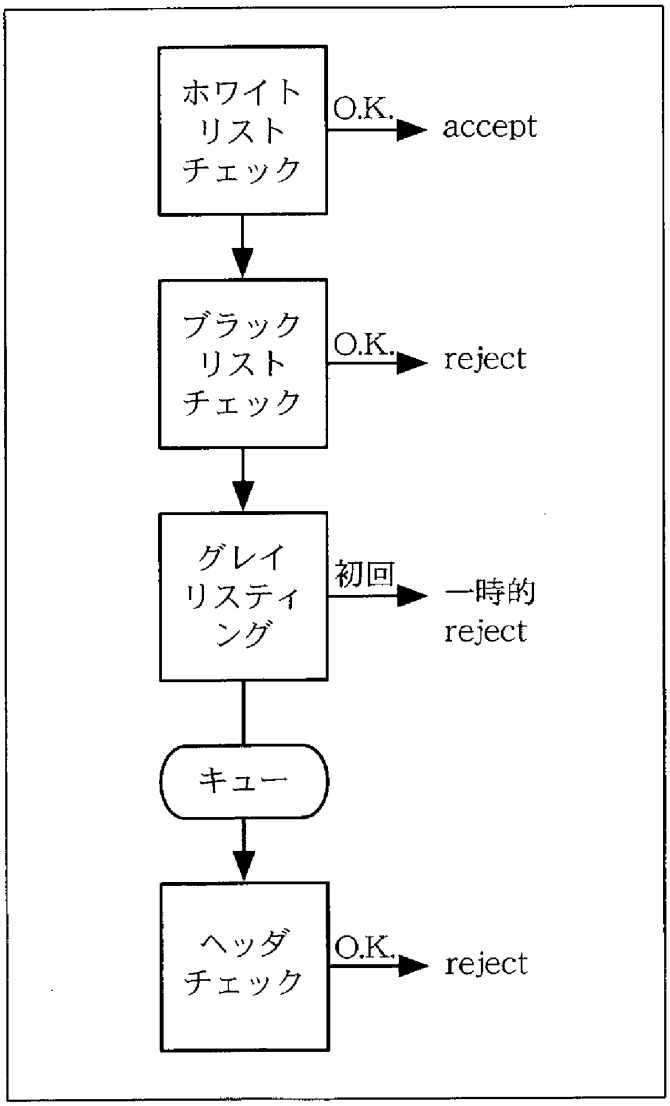
2005年3月9日に、ヘッダーチェックの適用を開始した。DM Mailer というパーソナルコンピュータで動く大量配信用の MUA[6] を使っている spam が発見され、X-Mailer ヘッダによるフィルタリングを追加した。

携帯電話発のメールは（2）の最後に述べたような仕組みで遅延することが多い。携帯電話発の spam メールは一時期非常に多かった。しかし、各キャリアの対策によって現在では減少

している。そのため、携帯電話発のメールについてはホワイトリストに入れて、一律に受理することとした（2005年９月29日）。

図１が現時点（2005年９月）のフィルタリング構成の概略である。２．に述べた各種のフィルタリング手法を併用している。

**図1　spam フィルタリングの構造**




## ４．spam 防止対策の効果

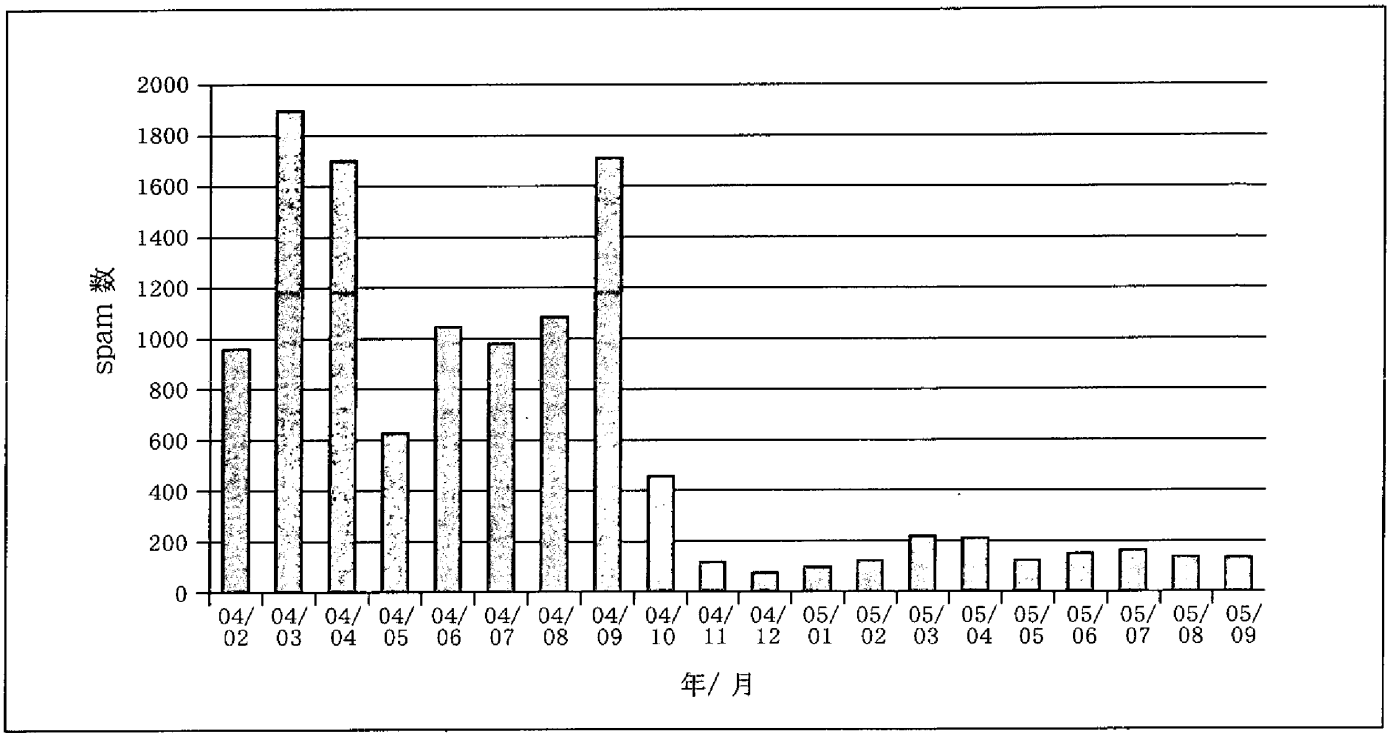
筆者は spam メールの分析のため、2003年11月頃から spam メールを削除せずに収集することとした。但し、網羅的に収集を行ったのは2004年２月７日からである。spam 防止策の具体化が決定したので定量的に効果を分析するために収集を行った。メールが spam であるかどうかをヘッダの情報だけで自動的に判断することは困難であり、人間がメール本文を見てはじめて spam であるかどうかを高い精度で判断できる。メールのログでは spam かどうかは判断することは不可能であり、どうしても人間の手による分別が必要となる。但し、長期にわたる人手による分別では間違いも生じるので、下記のデータについては厳密さは保証できない。

１．に述べたように spam の宛先は何らかの形でリストとして流通している。筆者のメールアドレスは長期にわたってネットニューズや Web ページに記載がある。そのために収集された可能性が高く、このようなリストに含まれているものと考えられる。このような状況からみて、筆者に届く spam は一般のユーザーと比較すると多い部類であろう。spam 対策を行う直前の時期には一日に数十通の spam が届き、ピーク時には 100 通を超えていた。

収集した spam メールを解析するプログラムを作成し、ヘッダ情報から、一通ごとに、発信日時、発信メールホストが名乗っているホスト名、発信メールホストのIP アドレス、逆引きしたホスト名、Message ID、To、From、Return-Path をリストにしている。これを基礎データとして、日ごとの spam 総数、spam 送信メールホストの IP アドレスの集計を行う。IP アドレスの集計から、一定の条件を満たす IP アドレスをブラックリストの候補とする。現在のブラックリスト候補の条件は、３回以上届いたか、または２回以上届いてホスト名が unknown（逆引きできない）のものとしている。

対策後の spam メールの数の推移を図2にあげる。これは日ごとの集計をまとめた月ごとの集計であるため、設定日前後の明確な効果は表現できていない。しかし、防止対策効果の概略の様子は充分判別できるだろう。

図2　spam の月次集計




まず、2004年４月下旬の基本的フィルタリングによって、50-60% に減少している。拒否した spam の多くは ORBL によるものと考えられる。大きい効果があった。その後６月頃から若干増加しているのは世の中の spam が増えたとも考えられるが、ブラックリストによる拒否により spam 送信者を刺激して標的となった可能性も考えられる。実証は難しい。この頃には一日あたり30通ほどの数であり、対策前より減少はしたものの個人レベル[7]で考えると、まだ多いといわざるを得ない。そして徐々に増加していき、2004年９月には一日あたり80通を超える日もあった。

2004年10月上旬のグレイリスティングによって、spam の数は約 1/10 に減少した。グレイリスティング適用後三日間ほどに届いた spam はゼロであった。実感上からもデータの上からも、グレイリスティングの spam に対する効果は非常に高いものであると言えよう。

なお、ブラックリストについては、不定期に更新しているため、その効果は測定しにくい。

上記の期間に、筆者自身が収集した spam メールの総数は12121通である。これらのメールのヘッダから分析できる spam の特徴として、次のことがわかった。

SMTP セッションで得られる外部送信メールホストが名乗るホスト名とセッション中に判別できる IP アドレスに対して、正当なものは名乗ったホスト名と IP アドレスから逆引きできるホスト名は一致するはずである。収集した spam メールの内、逆引きホスト名が unknown のもの（つまり逆引きできない IP アドレス）は8311通（68.6%）であり、名乗っているホスト名が IP アドレスから逆引きしたホスト名と異なるものは1573通（13.0%）、両方を合わせると9884通（81.5%）である。これらは意図的に動的な IP アドレスから発信されているものとゾンビによって発信されているものの両方が含まれると考えられる。いずれにせよ本学では中止した unknown client のフィルタリングを行えば排除されるものであり、DNS 設定が不備であるという現状が spam を増加させて

いる一因ともなっている。

また、ホスト名として本学のメールゲートウェイの IP アドレス（192.47.184.1）を名乗っているものが5591通（46.1%）に達した。これは上記の9884通に含まれる。手口としてあまり効果があるとは考えられないが、送信ホスト名を詐称して、送り先のメールホストの IP アドレスとすることもよくある手法と思われる。

逆引きできた場合の spam 送信者のドメインについては、多い方から net が1729通、 com が945通、jp が264通、br が107通であった。国別ドメインでは50ヶ国にわたり、世界中で spam が横行していることがわかる。

さらに、差出メールアドレスの詐称に関して、Return-Path と From に書かれたメールアドレスが異なるものは 1715通（14.1%）であった。From に書かれたメールアドレスが詐称されたもので Return-Path は詐称しなかった、あるいは詐称することに技術的に失敗したものと考えられる。この二つのメールアドレスが一致している場合であっても、本当のメールアドレスと信用するわけにはいかない。そういうものは Return-Path を詐称することに技術的に成功したものとも考えられる。経路のドメイン名などの情報と合わせて総合的に判断する必要がある。

## 5．spam 防止対策の課題

グレイリスティングは spam に対して、非常に高い効果を発揮することがわかった。しかし、3.（2）に述べたように、再送するメールホストが複数存在するサイトのメールを扱うことは難しい。何度送ってもメールが遅延するようではユーザーの迷惑となるため、ホワイトリストに入れざるを得ない。このようなサイトは、ドメイン内部からの spam 送信を排除する管理運用を行っているのであれば許容できる。ただ、そのような対策を行っているサイトであるかどうかを世界中のサイトについて調査するのは不可能である。現状ではユーザーからの申請によって調査し、必要に応じてホワイトリストに登録するのが現実的な解となっている。

なお、内部からの spam 送信排除については、運用面だけでなく技術的には Out Bound Port 25 Blocking や送信者ドメイン認証などの方式が広がり出している。これは本稿の主題からははずれるため詳述しないが、本学のネットワークでもその運用の第一歩を踏み出した。

グレイリスティングは、原理上、再送してくる spam に対しては無力である。あくまでも再送しない spam 送信者に対してのみ効果があるが、その数が多いのが現状であるために効果を発揮する。数多くのゾンビも現状では再送するような仕掛けにはなっていない。ISP や一刻を争う企業現場などではメール遅延に対してユーザーの理解を得るのが難しいために、そういう組織ではグレイリスティングを行うことは運用上難しい。このような現状からは、spam 送信者も再送する必要性は少ないのかも知れない。但し、今後、spam 送信者がグレイリスティングに適応してくる可能性はある。

spam メールの特徴の一つは、4．で述べたように送信メールホストの DNS における正当性がないということである。これによる排除を行うことができれば、グレイリスティングをすり抜ける spam の 80% が排除できるわけである。各サイトにおける DNS 設定の現状から、それができないという現実はいかんともしがたい。DNS の正しい設定の普及が強く望まれる。

現実的には、大学のネットワークではグレイリスティングの手法は充分に効果的である。一般的には spam 排除を過剰に行うと通常のメールが失われてしまうことがある。本学が行っているようなレベルでの複合的な防止対策によって通常のメールが失われる可能性は極めて小さ

い。ユーザーには若干の spam が届くものの、それは個人が MUA で選別できるくらいの量になっている。

個々のサイトではなくインターネット全体として spam 防止対策を行うために、日本の行政レベルでの対応も進み出したし、国際的な協力の上にたって多くの人が努力している。また、インターネットメールそのものの技術的な仕組みを見直す動きもある。抜本的に spam を排除することは近い将来に実現できるかも知れないがそれまでの間は spam 発信者と我々の戦いである。防御策を強めれば spamの手法も高度になっていく。あくまでもユーザーの利便性に立脚して、spam 撃退のためにたゆまない対応をしていかなければならないだろう。

## 謝辞

実際の spam 防止対策に関する管理運用に携わっている日本電子計算株式会社の戸田邦昭氏、河村宜明氏、江尻和隆氏、および本学情報システムセンターの村上道治氏、同僚の高木靖彦氏に感謝する。

〈注〉

1）"SPAM" は米 Hormel Foods 社が製造する缶詰食品であり、同社の登録商標である。1970年代の BBC 放送の番組 "Monty Python's Flying Circus" のコントの一つにおいて、"SPAM" という言葉をしつこく連呼して冗談とした（第2シリーズ・エピソード12)。大量メールの意味での spam はこれに由来する。登録商標と区別するために小文字で綴る。

2）spam 送信者に苦情を出そうとして、単純に差出人に返事を書くのは無駄であるし、詐称された人にとっても迷惑である。

3）実例としては Thunderbird やApple Mail などがある。

4）実際に第三者不正メール中継ホストになっていないかどうかを調べる手段はある。日本でよく使われているものでは、有限会社長崎ネットワークサービスが公開している第三者中継調査の Web ページ (http://www.nanet.co.jp/rlytest/relaytest.html) が有名である。

5）Postfix の公式 Web ページは http://www.postfix.org/ である。

6）このような MUA の一覧が http://apply.jca.apc.org/mail/rejectmailer.php にある。

7）筆者に届く通常の（spam でない）メールは、一日あたり数十通から百通程度である。

## 参考文献

[1] Postel, J. B., "Simple Mail Transfer Protocol", RFC 821, IETF (1982).

[2] Klensin, J. (ed.), "Simple Mail Transfer Protocol", RFC 2821, IETF (2001).

[3] Crocker, D.（安藤 訳），「世界の電子メールを spam 制御へ」，情報処理, 46巻7号 (2005), pp. 739-746.

[4] 安藤一憲,「フィルタリング」,情報処理, 46巻7号 (2005), pp.758-761.

[5] Harris, E., "The Next Step in the Spam Control War: Greylisting", http://projects.puremagic.com/greylisting/whitepaper.html (2003).

[6] Dent, K. D.,（菅野 訳），『Postfix実用ガイド』，オライリージャパン (2004).

（東邦学園短期大学 経営情報科）