全学メールサービスにおける迷惑メール・ウィルスメール対策

川田良文　山田一成
田島尚徳　柘植　朗

はじめに

2008 年１月から，統合サーバ上で新しい全学メールサービスが運用開始されました。昨今のメールサービス運用には迷惑メール対策・ウィルスメール対策が欠くことのできないものとなっており，全学メールサービスも例外ではありません。本稿では，全学メールサービスにおいて，迷惑メール対策をどのように実施しているかを主として解説し，ウィルスメール対策についても簡単に紹介します。

Ⅰ．概要

全学メールサービスのサーバは統合サーバ上に構築されていますが，迷惑メール・ウィルスメール対策は，別途用意した全学メール専用の配送サーバ上で行います（図１参照）。配送サーバは二重化されており，一台が停止した場合でも正常に配送が続けられるようになっています。

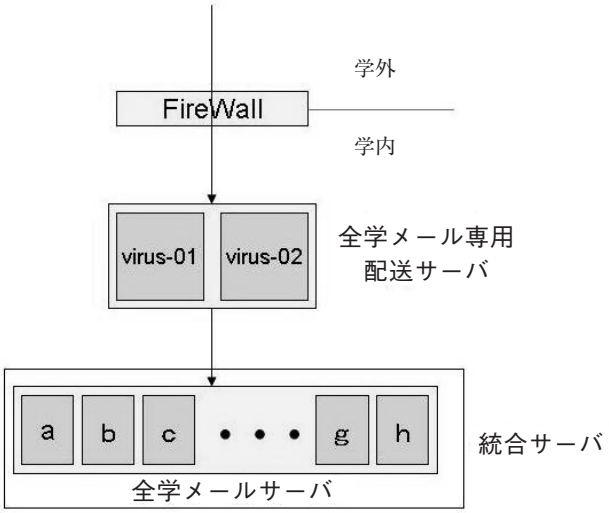

図１　システム概要

Ⅱ．迷惑メール対策

1．基本方針

全学メールサービスにおける迷惑メール対策では，「“検出”は行うが“遮断”はしない」方針をとることにしました。届くべきメールが届かないという事態を極力避けたいためです。どのような迷惑メール検出方法を選択したとしても，誤検出をなくすことは不可能だと考えられるため，「遮断はしない」ことを選択しました。検出した迷惑メールには，サブジェクトの先頭に“[**SPAM**]”という文字列を挿入します。図２はWebメールを利用したときの例です。「件名」に“[**SPAM**]”という文字列が現れています。

図２　検出された迷惑メール

検出された迷惑メールは，この文字列を利用してメールソフトで振り分けを行うことができます。そのためのメールソフトの設定方法は

http://www.icts.nagoya-u.ac.jp/service/mbox/antispam/

を参照ください。なお，必要なメールにも誤検出によって“[**SPAM**]”という文字列を付加してしまう可能性がありますので，振り分けたメールはすぐに削除するのではなく，しばらく保存しておくことを強くお勧めします。

2．検出方法

全学メールサービスでは「Selective SMTP Rejection（S25R）」と呼ばれる方法により，迷惑メールを検出します。この方法では，メール送信のために接続要求してきたホストが，“迷惑メールを送信していると考えられるホスト”である場合，そのホストからのメールをすべて迷惑メールと判断します。Fromアドレスやメールの内容などには関係なく，SMTP接続してきたホストの情報のみを判断材料としています。

S25R方式には“迷惑メールを送信していると考えられるホスト”であると判断するための基本的なルールがいくつか用意されていますが，今回は次の６つのルールを採用しました。

1）逆引きFQDNの最下位（左端）の名前が，数字以外の文字列で分断された２つ以上の数字列を含む。

例：123−45−67−89.aaa.bbb.com

（左端の 123−45−67−89 がハイフンで 4 つの数字列に区切った形式になっている）

2）逆引き FQDN の最下位の名前が，5 個以上連続する数字を含む。

例：a11335577.aaa.bbb.com

（左端の a11335577 が 8 個の連続した数字を含んでいる）

3）逆引き FQDN の上位 3 階層を除き，最下位または下位から 2 番目の名前が数字で始まる。

例：123a.456b.ccc.com

（左端かつ右から 4 番目の 123a が数字で始まっている。）

a12.34b.ccc.ddd.com

（左端から 2 番目かつ右から 4 番目の 34b が数字で始まっている）

4）逆引き FQDN の最下位の名前が数字で終わり，かつ下位から 2 番目の名前が，1 個のハイフンで分断された 2 つ以上の数字列を含む。

例：a123.4−56.bbb.com

（左端の a123 が数字で終わり，左から 2 番目の 4−56 がハイフンで 2 つの数字列に区切った形式になっている）

5）逆引き FQDN が 5 階層以上で，下位 2 階層の名前がともに数字で終わる。

例：a123.b456.ccc.ddd.com

（. で区切られた 5 つの名前でできていて，左端の a123 と左から 2 番目の b456 がどちらも数字で終わっている）

6）逆引き FQDN の最下位の名前が「dhcp」,「dialup」,「ppp」，または DSL 系の名前で始まり，かつ数字を含む。

例：ppp123.aaa.bbb.com

（左端の ppp123 が ppp で始まり，数字を含んでいる）

通常，これらに先行して「逆引きに失敗する」というルールを適用しますが，このルールに一致してしまうメールサーバが多数あるため，採用しませんでした。また，1）～ 6）のルールに該当してしまう正当なメールサーバをスパムホストと見なさないために，「メールエイリアス実験サービス（https://mynu.jp/itc/nu_alias.html）」で蓄積されたホワイトリストファイルを提供していただき，利用しています。

また，全学メール専用配送サーバでは postfix を使用していますが，postfix だけではサブジェクトに任意の文字列を挿入することができないため，外部フィルタを作成しました。前記のルールに該当したメールメッセージを外部フィルタに渡し，文字列を挿入した後，sendmail で postfix に戻しています。このため，配送サーバの負荷が若干増加することが予想されました。

３．実際の設定

1）postfix の main.cf ファイルに次の行を追加

```
smtpd_client_restrictions =
   check_client_access regexp:/etc/postfix/white_list,
   check_client_access regexp:/etc/postfix/generic_filter
```

2）ホワイトリストファイル（/etc/postfix/white_list）を作成

記述例：

```
/^133¥.6¥./                                  OK
/¥.nagoya-u¥.ac¥.jp$/                        OK
/¥.mixi¥.jp$/                                OK
/¥.ees¥.elsevier¥.com$/                      OK
/^mta-207-67-53-77¥.staging¥.extm¥.us$/      OK
```

3）基本ルール 1 ～ 6 を記述したファイル（/etc/postfix/generic_filter）を作成

```
/^[^.]*[0-9][^0-9.]+[0-9]/ FILTER filter:
/^[^.]*[0-9]{5}/ FILTER filter:
/^([^.]+¥.)?[0-9][^.]*¥.[^.]+¥..+¥.[a-z]/ FILTER filter:
/^[^.]*[0-9]¥.[^.]*[0-9]-[0-9]/ FILTER filter:
/^[^.]*[0-9]¥.[^.]*[0-9]¥.[^.] +¥..+¥./ FILTER filter:
/^(dhcp|dialup|ppp|[achrsvx]?dsl)[^.]*[0-9]/ FILTER filter:
```

4）postfix の master.cf ファイルに次の行を追加（実際は 1 行）

作成した外部フィルタは /home/filter/filter.sh とする

```
filter unix - n n - 50 pipe
flags=Rq user=filter argv=/home/filter/filter.sh -f ${sender} — ${recipient}
```

4．導入結果

迷惑メールの検出は 2008 年 5 月 26 日から開始しました。その後, 6 月に入ってからの迷惑メール検出件数とメール総数の推移は図 3 のようになっています。平均すると 1 日あたり約 6 万 3 千件のメールが配送され，そのうち迷惑メールの検出は約 2 万 6 千件でした。全配送メール中，約 41%になります。

「逆引き失敗」のルールをはずしていても 4 割以上が迷惑メールとして検出されていますので，実際には半分以上が迷惑メールと考えられます。約 2 年前に，ある SPAM メール対策アプライアンスをテストした際には，平均して約 30%が迷惑メールという結果になっていましたので，年々増加しつづけているようです。なお，S25R の原理上，メーリングリストから送られてくるものや，他のメールサーバのアドレスから転送されてくるものは検出不可能ですので，そこは転

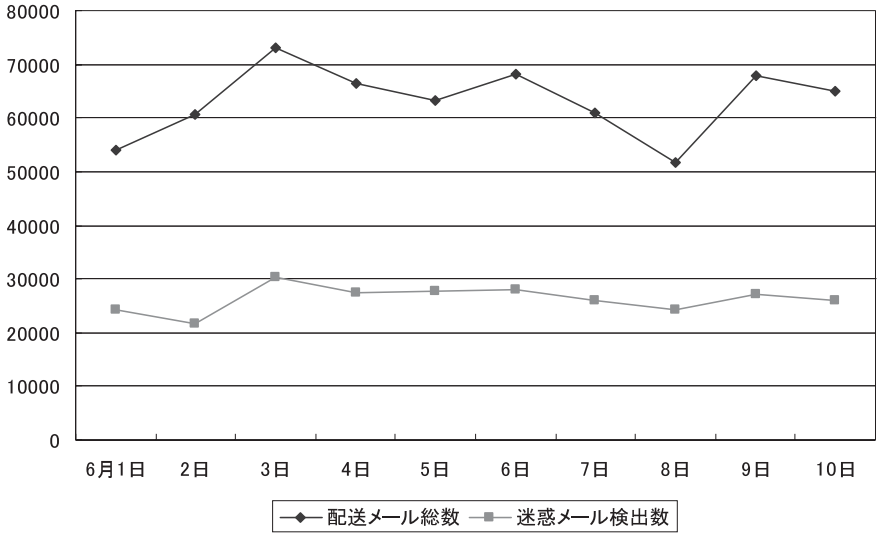

図３　迷惑メール検出数とメール総数

表１　load average

	1 分平均	5 分平均	15 分平均
5 月 22 ～ 23 日の平均	0.21	0.21	0.19
5 月 29 ～ 30 日の平均	0.22	0.21	0.18

送元のサーバで検出してもらう必要があります。また，そのような場合に対応するために迷惑メールフィルタを装備したメールソフトを使用するのも有効だと思われます。

「2. 検出方法」で，サーバの負荷が増加する懸念があると述べました。これを確認するために，簡易な方法として uptime コマンドを 10 分ごとに発行して調査を行いました。その結果が表 1 です。平均負荷値が変化するような影響はないようです。

Ⅲ. ウィルスメール対策

全学メールサービスのウィルスメール対策は，TrendMicro 社の InterScan Messaging Security Suite を利用しています。

図 4 にウィルスメール検出数を示します。数年前に比べてウィルスメール自体がかなりの減少傾向にあるようです。2008 年 5 月に配送サーバを通過したメール総数は約 210 万件でしたが，その内でウィルスメールは 152 件でした。2004 ～ 2005 年の状況については参考文献［3］を参照下さい。

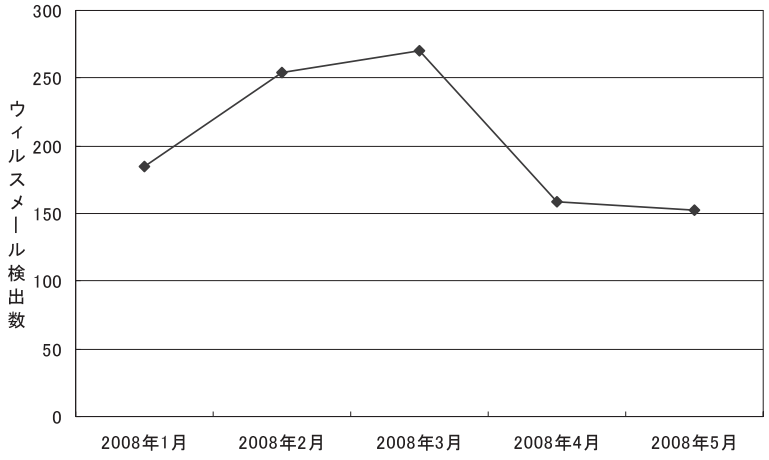

図４　ウィルスメール検出数

おわりに

以上，全学メールサービスでの迷惑メール・ウィルスメール対策について説明してきました。迷惑メールについての考え方は，目に触れるのも避けたいという方から，すべて自分で管理するので迷惑メール対策が迷惑という方まで千差万別なようです。「“検出”は行うが“遮断”はしない」という基本方針も，それらの意見の妥協点の一つとご理解ください。なお，迷惑メールではないにもかかわらず，サブジェクトに“[**SPAM**]”が挿入されたメールが届いた場合には，該当メールの送信者アドレス，受信者アドレス，送信日時，またはヘッダ部分のコピーを付けて，下記アドレスまでご連絡ください。ホワイトリストに追加いたします。

mbox-spam-chk@icts.nagoya-u.ac.jp

最後に，迷惑メール対策実施と本稿執筆にあたって，ご指導・データ提供をいただいた内藤久資准教授，山口由紀子助教，ならびにエイリアス実験サービスで蓄積されたホワイトリストをご提供いただいた梶田将司准教授に感謝いたします。

参考文献

[1]　浅見秀雄，阻止率 99％のスパム対策方式の研究報告― Selective SMTP Rejection（S25R）方式―，http://www.gabacho-net.jp/anti-spam/

[2]　内藤久資，山口由紀子，全学メールサービスの概要，名古屋大学情報連携基盤センターニュース，7，157−167，（2008）

[3]　山口由紀子，SPAM メールの傾向と対策，名古屋大学情報連携基盤センターニュース，Vol. 4，No. 3，169−174，2005

（かわた　よしふみ：名古屋大学情報連携統括本部情報推進部情報基盤課情報システムグループ）
（やまだ　かずなり：名古屋大学情報連携統括本部情報推進部情報基盤課情報システムグループ）
（たじま　ひさのり：名古屋大学情報連携統括本部情報推進部情報基盤課情報システムグループ）
（つげ　あきら：名古屋大学情報連携統括本部情報推進部情報基盤課情報基盤グループ）