迷惑メール対策

宮崎大学工学部教育研究支援技術センター
森　圭史朗

はじめに

学内において，電子メールは業務を行う上でなくてはならないものになっている．事務連絡等は，メーリングリストサーバを利用し，全教職員へ一斉にメールで送信するようになっている．メールを活用することで，文書のペーパーレス化による経費削減や学内便を利用するより迅速な情報伝達ができる．しかし，年々増加傾向にある迷惑メールには注意する必要がある．メールサーバには，毎日大量の迷惑メールが送信されて来ている．迷惑メール対策を行っていないと迷惑メール内の不正プログラムにより PC 内の情報が外部に漏洩していたり，遠隔操作で外部から利用されてしまったりする場合がある．メールサーバ運用には，メールリレーやメール爆弾対策等のセキュリティ対策を行っていれば問題はないが，メールを利用する側のセキュリティのためにもサーバ側での迷惑メール対策が必要になる．

本報では，メールサーバにおける迷惑メール対策について報告する．

キーワード：スパムメール，メールサーバ，グレイリスト，S25R，ブラックリスト

1. 迷惑メールとは

全世界のメールのうち約 65%が迷惑メールである．迷惑メールとは，匿名（送信アドレスを偽装）で大量送信される迷惑なメールのことであり，表 1 にような一方的に送られてくる広告メールや架空請求メール等（ウイルスメールやワームも含む）受信者にとって不要なメールのことである．この迷惑メールの中でも悪質なものは，メール本文中にあるリンク先に不正プログラムをダウンロードするものやフィッシングサイトに誘導し，クレジットカードや銀行口座等の ID，パスワードなどの個人情報を取得しようとするものもある．

表 1　迷惑メールの種類

種　類	内　容
ウイルスメール	ウイルスやワームが添付されている
フィッシングメール	リンク先の Web ページで個人情報を入力させる
広告メール	製品の宣伝，出会い系サイトの案内
デマメール	株価操作等の偽のニュース速報

2.メールの配送のしくみ

メール配送は，信頼性のある TCP プロトコルの 25 ポートを使用し，メールサーバとユーザー間，あるいはメールサーバ間において図 1 のようなテキストベースのメール通信を行う．理想的なメールサーバとして，メール受信側は，DNS の MX に従いメールを受信する．一方，メール送信側は，メールアドレスのドメイン部が DNS の正引きと逆引きに登録されていることが望まれる．

メール送信時の流れは以下の通りである．

① 送信側から受信側に接続開始を促す．
② 受信側からサーバのホスト名が送信側に送られる．
③ 送信側は，「HELO」コマンドにより送信側ドメイン名を送信する．（HELO コマンドで存在しないドメイン名を使用するとエラーメールとなる．）
④ 受信側は，送信側のホスト名と IP アドレスを検索し，送信側に送る．
⑤ 送信側は，「MAIL From:」コマンドにより送信者のメールアドレスを受信側に送信する．
⑥ 受信側は，送信側に ok を送る．
⑦ 送信側は，「RCPT To:」コマンドにより送信先のメールアドレスを受信側に送信する．
⑧ 受信側は，送信側に ok を送る．
⑨ 送信側は，「DATA」コマンドを送ることによりよりメール本文を送信することを受信側に伝える．
⑩ 受信側は，送信側に go ahead を送る．
⑪ 「Subject:」コマンドにより件名，メール本文を入力し，最後に「.」（ピリオド）で終了す

るとメール本文が受信側に送信される．

⑫ 受信側は，送信側に ok とメッセージ ID を送る．

⑬ 送信側が「quit」コマンドを受信側に送信し接続を終了する．

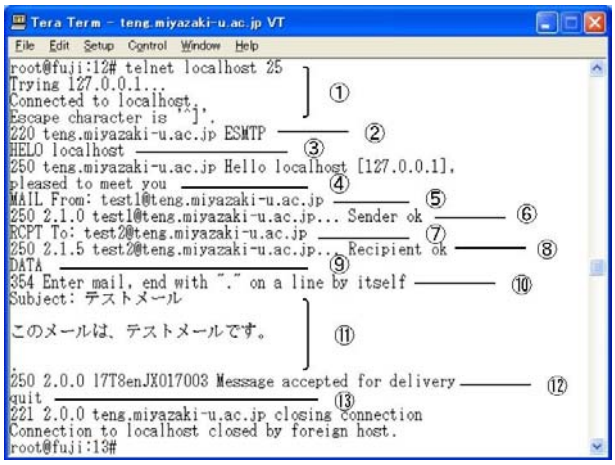

図 1　Telnet でメールを送信する様子

3. 迷惑メール対策の概要

迷惑メール対策用のメールサーバを新たに構築し，図 2 のように設置する．そして，迷惑メール対策用メールサーバに対し，3 つの迷惑メール対策（S25R，Greylist，ブラックリスト）を導入する．また，ユーザーがメールチェックを行う受信側メールサーバでは，IP アドレス制限によりメールを直接インターネット上から受信できなくし，インターネット上からの届くメールは，すべて迷惑メール対策用メールサーバを経由させて受信するようにする．

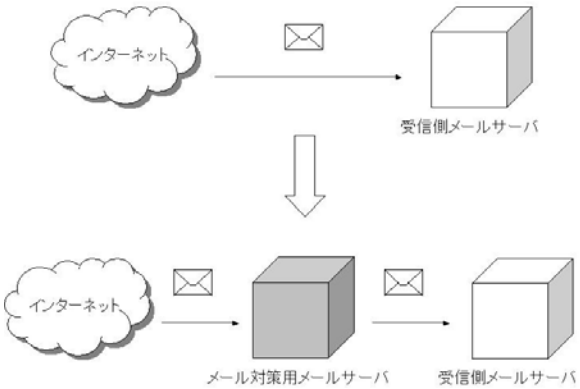

図 2　迷惑メール対策メールサーバ導入位置

4.導入した迷惑メール対策について

メールサーバでは，S25R，Greylist，ブラックリスト，IP アドレス制限の 4 つの手法を用いて迷惑メール対策を行う．これらの手法について以下に説明する．

S25R（Selective SMTP Rejection）

S25R は，インターネット上からメールを受け取る際，送信元のメールサーバの IP アドレスからホスト名を逆引きし，DNS の正引きと逆引きが一致したもの及びホワイトリストに登録したものを受信する．

Greylist

Greylist は，メールを受け取る際，初めてアクセスしてきた送信元のメールサーバに一時的エラーコードを返し，メールの再度送信を促す．一定時間後，送信元メールサーバからメールが再送信された場合及びホワイトリストに登録されている場合は受信する．

迷惑メール送信業者のメールサーバからのメールは，大量のメールを短い時間で送信しようとするため再度送信を行わない．このような再送信されないメールを受信しないようにする．

ブラックリスト

ブラックリストは，迷惑メール送信業者が利用するメールサーバ，迷惑メールの中継を許す管理の甘いサーバ，トロイの木馬やウイルス等に感染したゾンビ PC 等の迷惑メール送信元の IP アドレスを列記したものである．

メールサーバ運用管理者の中には，このブラックリストの提供者（例・DSBL，spamcop，CBL）と契約を結んで最新版のリストの供給を受け，迷惑メール遮断に役立てているところもある．これらのブラックリストは，リアルタイムに更新される事から RBL（Realtime Blackhole List）と呼ばれている．

IP アドレス制限

通常，メールは，DNS の MX 情報を元にメールサーバに届けられるが，迷惑メール送信業者の中には，あらかじめメール送信ポート TCP25 を探し出し，DNS の MX を無視して送りつけてくるものがある．このようなメールは，新たに迷惑メール対策用のメールサーバを経由してこないため，迷惑メールを受信してしまう．このような迷惑メールに対処するため既存のメールサーバには，迷惑メール対策用のメールサーバからのみ許可するようにする．

5. 迷惑メール対策用サーバについて

5-1.構成

迷惑メール対策用のサーバ OS には，現役引退した古いPCを再利用したためFreeBSD-4.10を採用し，迷惑メール対策ソフトウェアとして，S25R+Greylist（Greylist に S25R を組み込んだもの）と表 2 にある 4 つのブラックリストを利用することにした．メールサーバには，表 3 に示した qmail を用いたメールサーバ構成にした．

表２　ブラックリストの種類

ブラックリスト名	主な対象
all.rbl.jp	ウィルスメール，迷惑メール
dnsbl.sorbs.net	メール中継，迷惑メール，ゾンビ PC，ダイヤルアップ
bl.spamcop.net	迷惑メール
sbl-xbl.spamhaus.org	メール中継

表３　メールサーバ構成

	ソフトウェア名
tcpserver	cdb-0.75
	ucspi-tcp-0.88
メールサーバ	qmail-1.0.3
	dot-forward-0.71
	fastforward-0.51
メール転送	checkpassword-0.90
	qmail-vida-0.53
S25R+Greylist	qgrey-0.1-0.3
	qGreylist-0.3

S25R と Greylist の欠点とその対応

S25R と Greylist にはそれぞれ問題点がある．S25R は，メールサーバをホスティングサービス（レンタルサーバ）で利用している場合，送信元の IP アドレスとドメインを管理しているサーバは必ずしも一致しない. この様なメールサーバは，一つ一つホワイトリストにメールサーバを登録しないとメールが受信されない．また，Greylist は，すべてのメールサーバに対して，一時的エラーコードを返すため, 理想的なメールサーバからのメールもすぐには届かなくなる．

これら 2 つの問題点を解消するために S25R と Greylist を併用することにした．S25R+Greylist を用いることで, 理想的なメールサーバからのメールは，S25R により遅延なく受信し，送信元メールサーバの逆引きホスト名がドメイン名と一致しないもの（迷惑メールと疑われるもの）は，Greylist で対応する．ホスティングサービス（送信サーバ名とメールアドレスが異なる）を利用しているメールサーバからのメールは, 再度メールが送信されてくるので問題なく受信する．

メールサーバ内でのメール処理

迷惑メール対策メールサーバ内でのメール処理を図 3 に示す.

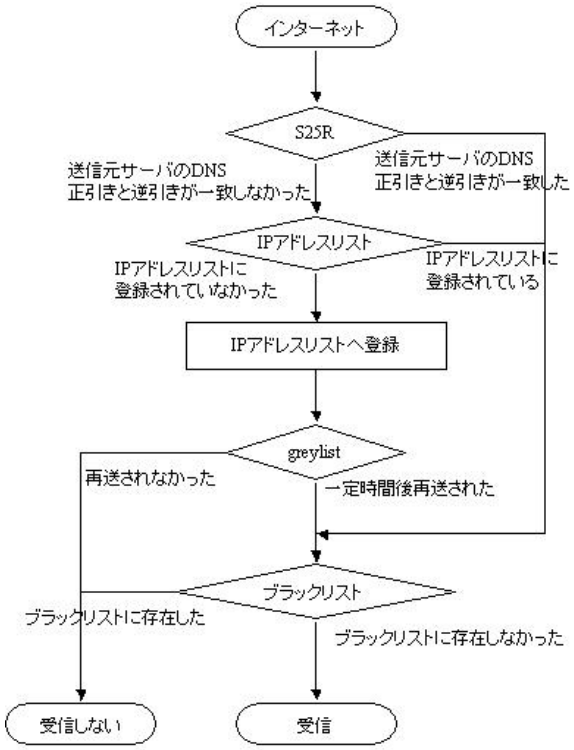

図３　サーバ内でのメール処理の流れ

インターネット上から来たメールが受信されるには，S25R+Greylist とブラックリストの 2 つの迷惑メール対策フィルタを通過しなければならないように構成されている．

インターネット上からのメールは，S25R で送信元 IP アドレスとメールアドレスのドメイン名が一致しているか確認される．一致すれば，ブラックリストに登録されてないか確認し, 登録されていなければ, 受信を許可する. S25R において，送信元とメールアドレスのドメインが一致しないものは，Greylist により対応する．Greylist の IP アドレスリストに登録されていた場合, ブラックリストに登録されていなければ受信許可されるが，Greylist に初めてアクセスしてきた IP アドレ

スは，IP アドレスリストに追加され，送信元メールサーバに再度メール送信を促す. 一定時間後，メールが再送されればブラックリストに登録されてないかを確認し, ブラックリストになければ，受信を許可される．Greylist において再送されなかった場合は，IP アドレスリストから送信元 IP アドレスを削除する. ブラックリストに登録されていた場合は，メールを受信しない.

5-2. 設定

迷惑メール対策メールサーバを構築する際の主な設定例の一部を以下に示す.

S25R+Greylist 設定例

/var/qmail/bin/greylist ファイル内で主に設定する部分を以下に示す.

```
メール再送を促す時間（秒）
  my $greytime = 25 * 60;
メール再送受付時間（秒）
  my $maxageonce = 45 * 60;
受信許可後の IP アドレス保存時間（秒）
  my $maxagegood = 20 * 24 * 60 * 60;
期限切れ IP アドレスの削除間隔（秒）
  my $cleanupinterval = 15 * 60;
ネットマスクの設定（クラス）
  my $Greylistclassc = 0;
```

受信許可したメールの転送設定例

/var/qmail/control ディレクトリ内にある rcpthosts ファイルに転送したいドメイン名を追加し, 同ディレクトリ内にある smtproutes ファイルに以下の内容で作成する.

[転送するドメイン名]:[転送先ホスト名または，IP アドレス]

メールサーバ起動スクリプト設定例

S25R+Greylist とブラックリストを利用するように組み込んだ qmail の起動スクリプトの一部を以下に示す.

```
$tcpserver -c 10 -vhR -l mail -x /var/qmail/tcp.smtp.
cdb -u $qmailuid -g $nofilesgid 0 smtp /var/qmail/
bin/greylist rblsmtpd -r all.rbl.jp -r dnsbl.sorbs.net -r
bl.spamcop.net –r sbl-xbl.spamhaus.org -b -c /var/
qmail/bin/qmail-smtpd 2>&1 | /var/qmail/bin/
splogger rblsmtpd 2 &
```

6.迷惑メール対策の実績

表 4 は, 学内のあるサブドメインのメールサーバに迷惑メール対策メールサーバを設置した結果である.

メールサーバに届くメール総数のうち迷惑メールが 70%にも達することがわかる. 拒否されたメールのうち 73%のメールが S25R+Greylist により拒否され, 25%のメールがブラックリストにより拒否していることがわかる．また，DNS サーバの MX を無視したメールも 2.3%の若干ではあるが拒否されている.

表４　メールサーバログの解析

メール総数		139036
受信許可メール		42335
拒否メールの総数		96651
内訳	S25R+Greylist	70929
	ブラックリスト	23440
	IP アドレス制限	2245

※ログ解析期間 2006 年 12 月～2007 年 8 月

7.まとめ

迷惑メール対策メールサーバを導入した結果, 迷惑メールについての問い合わせがなくなったため，ユーザーには，ほとんど迷惑メールが届いていないと思われる.

S25R+Greylist 導入前は，メールの件名や本文, 添付ファイルの拡張子から迷惑メールやウイルスメールを拒否するテキストフィルタを利用していたので, 定期的にフィルタの更新をする必要があったが，S25R+Greylist 導入後は，メールデータを受信する前に送信元 IP アドレスでメールを受信するか破棄するかを判断するため, ネットワークトラフィックにも負担をかけずに済み, テキストフィルタより確実に迷惑メールを排除できるようになった.

迷惑メール対策メールサーバ導入したことにより，メールを利用するユーザー側は，以前のように毎回のメールチェック時に迷惑メールを削除する必要がなくなった. また，メールから不正プログラムを取り込み PC がトラブルを生じることがなくなったことは, メールを利用するユーザー側に対しても十分なセキュリティ対策を講じることができたと思う.