Vol.2009-CSEC-46 No.14
2009/7/2

メールゲートウェイにおける応答遅延を用いたスパム対策について

浜 元 信 州[†1]　青 山 茂 義[†1]　三 河 賢 治[†1]

本報告では，公開リスト，HELO コマンドの引数を利用し，効率よく応答遅延を行う方式を提案し，この方式をもちいて，新潟大学メールゲートウェイサーバでスパムメール対策を行った結果について報告する．通常，スパムメール対策では，ホワイトリストなどのメンテナンスが欠かせないが，この方式では，公開リストを利用するため，リストのメンテナンスをサーバ管理者側では行わない．導入から現在まで，偽陽性判定の報告はなく，メンテナンスフリーでの運用が出来ている．対策前からユーザに届くメールは 3 割減となり，特定のメールアドレス宛てに対する調査では，本方式導入前に届いていたスパムメールの 9 割を削除することが出来ていることが分かった．

On the SPAM blocking for the mail gateway server using the SMTP throttling

Nobukuni Hamamoto,[†1] Shigeyoshi Aoyama[†1]
and Kenji Mikawa[†1]

We proposed a new method to block SPAM mail using some blacklist and the argument of HELO command sent by a remote server. We implemented our method to the mail gateway server of Niigata university. In this technical report, we describe how our method blocks SPAM mail and the blocking, false-positive/negative rate observed at our server. In our method, server adminstrator does not need to manage the whitelist of mail servers. Instead of the whitelist, we use some of the well-maintaind public lists. After implementing our method to the out mail gateway server, we do not recieved any false-positive report from our user. The arrived mails to our server and arrived SPAM mails to the paticular mail address are reduced by approximately 30% and 90 %, respectively.

1. はじめに

近年，インターネットを流れるメールの 80%ものメールがスパムメールとも言われている．[1)] この状況は，ネットワークトラフィックの無駄であると同時に，スパムメールの処理がメールサーバに負荷をかけるなど，管理者にとっても問題である．また，個々のユーザにおいてもスパムメールに紛れて大事なメールを見逃すなどの問題がある．特に，近年ではフィッシングの手段として使われるなど，ただの迷惑だけではなく，実害もあり，社会問題になりつつある．

新潟大学では，メールゲートウェイサーバを運用し，大学内に宛てたメールは全てこのサーバを経由するように構成している。メールのウイルス対策，スパム対策などは，このサーバ上で行われている．近年，スパムメールへの対策の要望が高まっていることから，2006 年より，過去にスパム送信したホストの IP を登録している公開ブラックリスト（公開リスト A）に登録されている IP を拒否するスパムメール対策を行ってきた．しかしながら，検出率が十分とは言えなかったため，応答遅延を組み合わせた新方式によるスパム対策を行った．本報告ではその方式と実運用での評価結果について述べる．

2. 既存のスパム対策技術

古典的には，スパム配送手法として，第三者中継を許可しているホストの利用があったが現在はほとんどのホストで第三者中継を拒否しているため、スパム配送手段としては用いられていない．現在，迷惑メール送信の方法として主流と考えられるのはボットに感染したコンピュータなどから送信する方法であると考えられている．[2)] また，スパム送信を専門とした業者もおり，独自にメールサーバを運用して送信しているようなケースもあると考えられている．

このような状況に対して，様々な対策が考えられてきた．IP ブラックリストの利用，接続ホスト名の利用など接続ホストレベルでの判定の他，応答遅延による対策，ベイジアンフィルタリング，送信者認証，ISP レベルでの送信サーバの管理など送信側での対策，法的対策などが挙げられる．大学のメールゲートウェイに導入するという観点から，以下に主な手法についての概略と利点，問題点を述べる．

†1 新潟大学 情報基盤センター
Center for academic information service, Niigata University

大学のメールゲートウェイの特徴としては，大規模 ISP ほどではないがユーザ数が多いことがある．新潟大学の場合は，約 20,000 人の構成員が利用している．このため，扱うメール数が多く，サーバ負荷が高い方法を採用した場合，メールの遅延などを容易に引き起こしてしまう．可能であれば，メールゲートウェイ上でスパム判定したメールにヘッダをつけて転送するようなサーバに負荷をかける方法は採用しない方が望ましい．この方法では、ユーザにヘッダ付きのスパムメールが届いてしまうため，体感的には大きくは変わらないことも問題である。また、近年は，メーラでもスパムフィルタリング機能の強化が強化されているため，メールゲートウェイでヘッダをつけなくとも，同様の判定がメーラでも出来るようになりつつある．このため，メールゲートウェイでの対策としては有用ではないと思われる．

また，メールゲートウェイという性質上，他サーバ上のユーザのメールを取り扱うこととなるので，メールの本文をみて判定するような方法を取ることが出来ない．さらに，大学構成員には，留学生や，国際共同研究を行っている研究者も多く，国外とのメール送受信が少なくない．このため、送信元の国により判別するような方法を使うことが出来ない．最後に，多くの大規模なメールゲートウェイの場合，その煩雑さから，常時監視して手動でメンテナンスを行うような方法を取ることが難しい．

2.1 公開リストの利用

インターネット上では，過去に迷惑メールを送信したなど問題のあるサーバを登録したリストが公開されている．通常，サーバの IP アドレスを登録することが多いが，FQDN などを登録する場合もある．公開リストを利用したスパムメール判定方式として一般的なものは，受信サーバ側でメール受信時に接続元の IP を調べ，公開リストに登録されているか否かによってメールの受信許可/拒否を判定する方式である．公開リストは，ボランティアや企業などが，ユーザからの報告や独自調査の結果を利用することにより，登録，削除を行っている．様々なリストが公開されているが，代表的なものとしては，下記が挙げられる．

- Spamhaus (http://www.spamhaus.org/zen)
- Spamcop SCBL (http://www.spamcop.net/bl.shtml)
- SORBS (http://www.us.sorbs.net/)
- no-more-funn (http://www.moensted.dk/spam/no-more-funn/)
- Barracuda BRBL (http://www/barracudacentral.org/rbl)

公開リストは，その管理方針により登録方法が異なる．また、ほとんどの場合、登録理由によりカテゴリ分けされている．例えば、Spamhaus の場合，スパム送信が過去に観測されたサーバは SBL に登録，管理上の問題で他者にのっとられたサーバは XBL に登録，プロバイダ管理の IP でメールサーバとして運用される可能性の低いエンドユーザに割り当てている IP は PBL に登録されている．SBL, XBL では基本的に過去に問題があったと思われる IP アドレスのみを登録していることになるが，PBL については，過去の実績とは関わらず条件に該当する IP を登録しているようである．その他の公開リストでもほぼ同様のカテゴリ分けがなされている．

ブラックリストの利用は，リスト管理をユーザ側で行う必要がないという利点があるが，非迷惑メールを迷惑メールとみなす「偽陽性判定」があるとの指摘もある．新潟大学では，2006 年 6 月より公開リスト A に登録されている IP からの接続を全て拒否するというスパム対策を行ってきたが，これによる「偽陽性判定」は今まで学内から一度も報告されたことがない．しかしながら，メールゲートウェイを通過するスパムメールが多いとの意見が多くあったため，この対策で十分とは言えなかった．実際，公開リスト A を含む多くの公開リストで，検出から登録までに時間がかかるため，その間のスパムを防げないという問題が指摘されている．[3)]

2.2 ホスト名情報の利用

メール受信側において，ホスト名の情報を利用し，メール受信の許可/拒否の判定を行う方式である．もっとも単純なものは，IP アドレスから DNS の逆引きを行い，登録のないものはメールサーバではないとみなし，受信を拒否する方式である．サーバの場合，多くの場合は逆引き登録しているが，登録は必須ではない．このため，誤検知率も高いといわれている．

この方式を推し進めたものの一つに S25R(Selective SMTP Rejection) と呼ばれる方式がある．[4)] この方式では，逆引きの失敗の他に，ホスト名に対して下記の 6 つのルールを設けて該当したものをエラーコード 450 で拒否し再送要求をする．

(1) 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二つ以上の数字列を含む
(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
(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
(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二つ以上の数字列を含む
(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
(6) 逆引き FQDN の最下位の名前が「dhcp」,「dialup」,「ppp」，または DSL 系の名前

（「dsl」,「adsl」,「xdsl」など）で始まり，かつ数字を含む

この方式は，プロバイダなどでエンドユーザに与えられる IP アドレスのホスト名をかなりよく拾うことが出来る．このため，Bot などによって送られるエンドユーザ回線からのスパムを効率よく拒否できる．設定が容易なことや，その効果の高さから，大学で採用例もある．[5] しかしながら，逆引き失敗の条件だけをみても偽陽性判定があることが判っているため，再送要求のログを確認し，ホワイトリストを手動で整備する必要がある．論文[4] 中でもホワイトリストなしの運用では 17%の偽陽性判定があるとの記述がある．また，手動でホワイトリストを管理した場合には、メールの遅延が起こるという問題もある．

2.3 HELO コマンドの引数を利用

RFC2821 では HELO メッセージの引数は，FQDN か IP リテラルと規定されている．ここで，IP リテラルとは IP アドレスを [] でくくった形式である．例えば IP アドレス 192.168.1.1 の場合には，IP リテラルは [192.168.1.1] となる．この方式は、上記 2 つの以外の引数を指定する場合には，正当なメールサーバではないと考え拒否する方式である．RFC を根拠とした方法であるため，比較的問題は少ないと考えられる．特に sendmai, postfix, qmail などの一般的なソフトウエアを用いた送信では問題は起こらない．しかし，メール配信ソフトウエアを独自に作成，利用している場合などは，HELO コマンドの引数が RFC に準拠していない場合もある．このため，この方式を取ることによりメールが届かなくなる可能性も否定できない．

2.4 応 答 遅 延

ブラックリスト，S25R などの方法で接続元サーバに問題があると判定された場合，通常，接続拒否，または，許可を行う．しかし，明確に許可/拒否の判断が難しい場合も多い．このため，許可，拒否を行わず，応答を遅延する方法を取る場合がある（Tarpitting, Greetpause, Throttling などと呼ばれている）．RFC2821 では，各コマンドのタイムアウト値が SHOULD で規定されている．スパムメール送信などの大量のメール送信を行う場合には，効率よくメールを配送するため，タイムアウトの前に接続を切るケースが多い．このため，わざと応答を遅らせることにで，スパムメールを受け取らないようにすることが出来る．この方法の問題点としては，若干であるが配送が遅延すること，大量接続があった際，サーバの接続数を使い切る可能性があること，RFC どおりのタイムアウト値を守って送信してくるスパムメールもあるため，完全にスパムメールを防げるわけではないことが挙げられる．

2.5 グレイリスティング

通常のメールサーバであれば，エラーコード 450 で拒否されたメールに対しては再送信を行わなくてはいけない．しかしながら，大量メール送信を効率よく行う場合には，再送信を行わない場合があるので，結果としてスパムメールのみを拒否することが出きるという方法である．再送を行ってきたホストについては，2 度目以降は拒否は行わない．この方法ではホワイトリスト管理が自動化されるなどの利点がある一方で，少なくとも最初はメールが遅延するという問題がある．

2.6 フィルタリング

メールの内容をみて，スパムメールか否かを判定する方式を総称してフィルタリングと呼ぶ．例としては，スパムメールに含まれると思われる単語を登録しておき，この単語を含むメールは拒否というする方式がある．代表的なフィルタリングの手法の中でも強力なものがベイジアンフィルタリングである．この方式では，スパムメール，非スパムメールを単語レベルなどで区切ってスパムメールが現れる確率 $P(A)$，メールに各々の単語が現れる確率 $P(B)$，スパムメールに単語が現れる確率 $P(B|A)$ を学習させる．この学習結果を利用して，ベイズ則により，届いたメールを単語などに分解しこの単語をもつメールがスパムメールである確率 $P(A|B) = P(A)P(B|A)/P(B)$ が計算出来る．この値を用いて新着メールについての，スパムらしさを推測し，許可/拒否の判定を行う．メールの中身を見れる場合には有用な方法で，Thunderbird, Mac OS X Mail, SpamAssasin など多数のメーラやプラグインにて実装されている．しかしながら，大学のメールゲートウェイでは，メールの中身を見ることが難しいので，この方式を採用することが難しい．また，メール全体を読み込むこととなるので負荷がかかることも懸念される．この方式のもう一つの問題点は，スパムメールを学習させる必要があることである．大学の全ユーザに対して継続的にスパム申告を行なっていただくことは運用上難しい．

2.7 送信ドメイン認証の利用

メールの差出人のドメイン詐称を判断するための手段として送信ドメイン認証という方法がある．差出人ドメインに対応する IP アドレスを DNS の追加情報として公開する Sender-ID 方式と DNS 上にサーバの公開鍵を登録し，メールサーバ上でメールに署名する DKIM 方式がある．Sender-ID 方式では，届いたメールに対して，差出人のドメインと接続サーバの IP を照合して差出人ドメインの詐称を確認する．DKIM 方式では，サーバ上で署名した送信メールの署名情報により差出人のドメインなどを明らかにする．これにより，差出人ドメインの詐称が出来なくなる．将来的には，スパムメール判定に利用出来るが，2008 年 4 月

時点では国内の普及度が両者合わせても 2 割程度であるため，今のところ，実運用にのせることは難しい.[6)]

2.8 送信制限による対策 (OP25B)

ボットなどに感染したパソコンからスパムメールが送信されると考えると，ISP などでエンドユーザ向けに提供される IP からのメール送信は，あらかじめブロックすることが有効な対策と考えられる．Outbound Port 25 Blocking (OP25B) と呼ばれるこの対策は，日本では現在ほぼ全ての ISP で行われている．新潟大学でもメールサーバ以外から学外へはメール送信出来ないよう対策を行っている．

3. 提案方式と実装

今回，新潟大学のメールゲートウェイで行った対策では，2.4 で述べた応答遅延を利用した．ただし，全ての接続に対して応答遅延を行うとメールの遅延や大量接続に対応出来ない可能性があるため，学外からの接続に限定している．公開リスト A は既に利用済みなので，今回の対策では，これを補うものを考案した．このリストの問題点であるスパムメールが発信されてから登録されるまでのタイムラグを解消するためには，予防措置的に怪しい IP を登録しておく必要がある．現在，Bot を利用した，エンドユーザ回線からのスパムメール送信が主流であると推測されることから，今回の対策では，エンドユーザ回線の IP アドレスを登録している公開リスト (公開リスト B) を利用する．同様のエンドユーザ回線の判定法には，S25R 方式という簡便な方法がある．そこで，初めに，S25R でのエンドユーザ回線の判別と，公開リスト B での判別についてどの程度違いがあるかについて調べた結果を報告する．

図 1 には，接続があったサーバのうち，公開リスト A に該当しないサーバのホスト名について，公開リスト B に登録されているサーバからの宛先数，S25R に該当するサーバから宛先数について集計を行った．× 印で示したものは，公開リスト B 及び S25R の両方に該当する宛先の割合である．白四角は両方に該当しない場合，＋ は，公開リスト B についてのみ該当するもの，*は S25R のルールのみに該当するものである．

両者ともに該当する × 印のものと，両者ともに該当しない白四角のものを合わせると全体の 8 割近くとなる．両者のデータベースは多くが共通と考えてよい．しかしながら，S25R にのみ該当する宛先が 2 割程度ある一方，公開リスト B にのみ登録されている宛先は 5%程度であるので，S25R 方式の方がブロックするメールは多いと考えられる．

しかしながら，論文[4)] にもあるように，S25R 方式の場合には，S25R に合致する宛先の

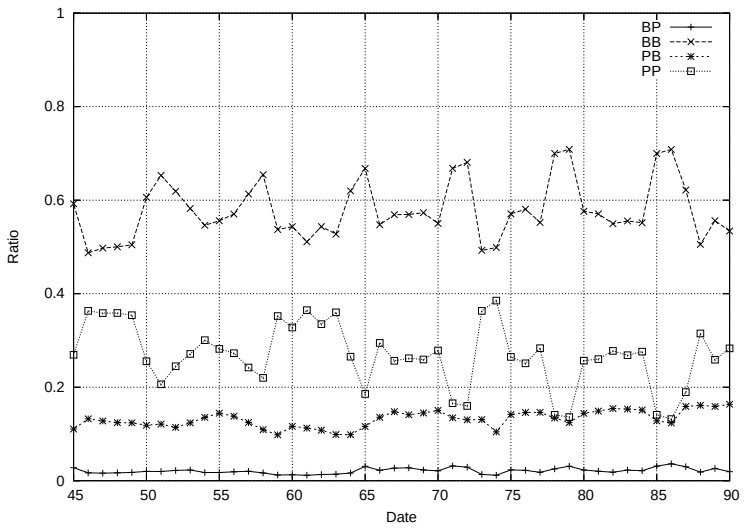

図 1 接続があったサーバのうち，公開リスト A に該当しないサーバのホスト名について，宛先数の割合をしめす．横軸は経過日数であり，1 日ごとの集計結果となっている．× 印で示したものは，公開リスト B 及び S25R の両方に該当する宛先の割合である．白四角は両方に該当しない場合，＋ は，公開リスト B についてのみ該当するもの，*は S25R のルールのみに該当するものである．

17%程度が正常なメールを出すサーバと報告されているため，ホワイトリストの整備が必須である．今回の我々の方式では，公開リスト B を利用することにより，サーバ管理者側でホワイトリストのメンテナンスをしなくとも偽陽性判定のない運用が出来る可能性があるため，検出率は落ちると思われるが，こちらを採用することにした．

一方で，公開リスト B に登録されているが S25R 方式には該当しない宛先も 5%ほどであるが存在する．我々の方法では，このような宛先でも検知するので，ここからのスパムメールは応答遅延により拒否できる可能性がある．これに該当する宛先は 5000 程度あった．主なものを参考までに表 1 に示す．

今回の対策では，さらに，2.3 節で述べた HELO コマンドの引数の条件も組み合わせて，下記の条件を設定した．条件 (1) は新潟大学で従来から行われていたものと変わらない，条件 (2),(3) が新たに追加された部分である．

(1) 公開リスト A に登録されている IP からの接続は「拒否」
(2) 下記の両方を満たす場合は「拒否」どちらか一方の場合は「応答遅延」

Vol.2009-CSEC-46 No.14
2009/7/2

BAC24ca.bac.pppool.de
Broadband-Dynamic-Central1436.connect.com.fj
D128.D-IP01.lipetsk.ru
La45c.l.pppool.de
VPN-148.PPTP-197-SA.GlobalNET.ba
aaeo30.neoplus.adsl.tpnet.pl
public8651.xdsl.centertel.pl
user-0ccemdu.cable.mindspring.com

表 1 公開リスト B に登録されているが，S25R には該当しないサーバのホスト名の例

(a) 公開リスト B に登録されている IP からの接続
(b) HELO コマンドの引数が FQDN か IP リテラル以外

(3) HELO コマンドに引数が学内のホスト名の場合は「拒否」

(a),(b) の条件を組み合わせて拒否判定をすることにより，応答遅延を起こす接続を減らし，メールサーバへの負荷を減らしている．また，拒否はエラーコード 550 で行ない，再送を要求しない．

上記の実装を行うため，MTA は postfix2.4 系を利用した．上記のうち，(2) の部分に関しては標準の設定では実現出来ないため，上記の条件を満たすよう postfix ポリシーサーバを作成し，実装を行った．[7)]

今回の実装での接続判定は下記の順番で行われる．なお，postfix では RCPT コマンド受け取った段階で，下記の確認が実行される．一つの接続で複数 RCPT を実行する場合には，応答遅延が複数回行われる．

(1) 接続 IP アドレスが学内なら許可，学外なら下記を実行
(2) 公開リスト A へ登録されていれば拒否
(3) HELO コマンドの引数が niigata-u.ac.jp で終われば拒否
(4) 学内サーバにユーザがいなければ拒否
(5) ポリシーサーバへ転送

4. 結　　果

図 2 に新潟大学メールゲートウェイにて上記提案方式の実装を行った結果を示す．横軸が経過日数であるが，45 日目 (2008 年 8 月 5 日) に上記条件のうち (2),(3) について導入を行った．横軸は，学外から受信したメールの宛先数に対する割合を示す．なお，応答遅延により接続が切れる場合には，1 接続あたり 1 宛先としてカウントしている．

条件 (2),(3) の導入の前後に依らず全体的な傾向として，*で示した公開リスト A で拒否

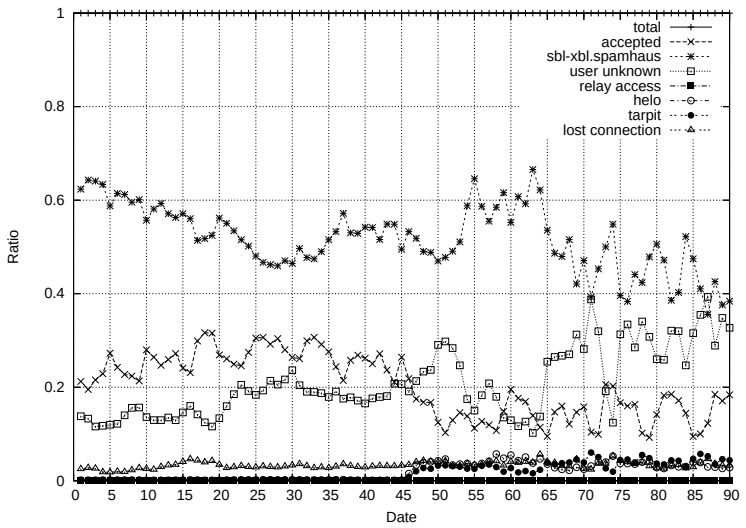

図 2 メールゲートウェイサーバにて処理したメールの割合．届いた宛先数を 1 とした．*は公開リスト A で拒否したもの，□は宛先不明のもの，■はリレー配送，○は HELO コマンドが不正のもの，●は応答遅延の結果届かなかったもの，△は原因不明で接続が切れたものを示す．

しているメール数は全体のうち 50%程度であることが分かる．次に□で示したユーザがいないため拒否されるメールがやはり全体の 2 割程度であることが分かる．また，原因不明で送信サーバに接続を切られるケースがあり常に 5%程度を占めている．■で示している第三者中継により拒否されるメールも若干あるが，全体の 0.1%未満であり，現在では第三者中継を利用したスパムメール配信はないと考えてよい．

新対策導入後には，× で示した受信しているメールが従来の 25%程度の値から 15%程度に落ち込んでいる．これは，新たな対策の導入の効果である．拒否理由としては，○で示した条件 (3)，または，条件 (2) の (a),(b) 両方を満たしたため拒否となった宛先が 5%程度，(2) のうち (a),(b) のどちらか 1 つを満たしたため，応答遅延となり，接続が失われたものが 5%程度となる．

2008 年 8 月 5 日の導入から現在まで，学内から届くはずのメールが届かなかったという偽陽性判定の報告は一件もない．少なくとも新潟大学の環境では，現在まで公開リスト B の他にホワイトリストのメンテナンスをすることなく運用が出来ている．

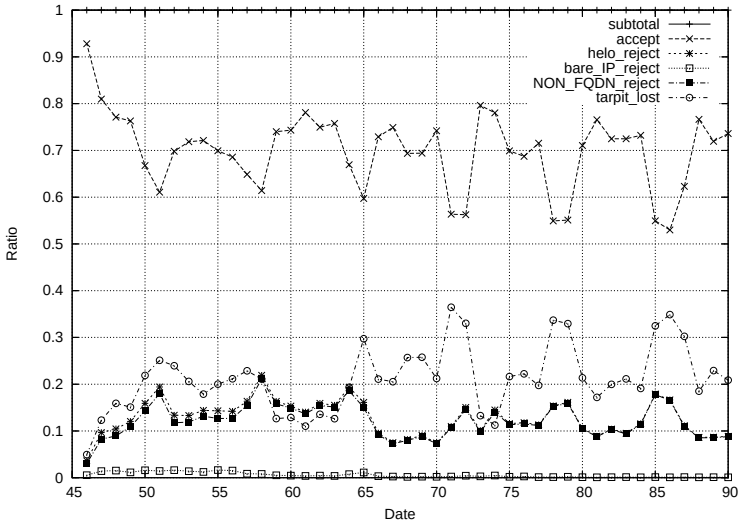

図 3 × は許可した宛先，○は応答遅延により届かなかった宛先，*は HELO コマンドの引数が FQDN でない文字列のもの，□は HELO コマンドの引数が IP アドレスの宛先である．それぞれ，対策前に届いていた宛先数に対する割合で示す．

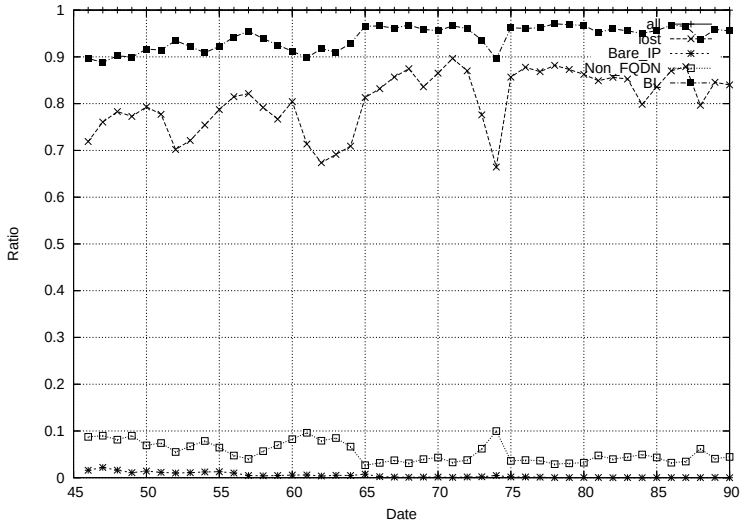

図 4 ■は公開リスト B に登録があるサーバからの宛先，*は HELO コマンドの引数が IP アドレスのもの，□は HELO コマンドの引数が FQDN でないものを表す．それぞれ，応答遅延を行ったメールの宛先の総数に対する割合で示す．

今回，新たに対策を入れた (2),(3) の部分についての効果をみるため，図 3 では，対策を入れる前に届いていた宛先数に対する割合を示す．横軸は経過日数である．今回の対策前に届いていた宛先数は全体の宛先数から，今までも対策のあった公開リスト A によるもの，及び，ユーザには届かなかったユーザ不明のもの，原因不明で接続が途切れるもの，第三者中継によるものを差し引いた宛先になる．

このように基準を変えると，ユーザから見て，× で示したユーザに届いたメールは，この方式による対策前と比べて 7 割程度になる．残りの 3 割は拒否されたメールとなるが，原因を見ると最も多いのが白丸で示した応答遅延によって届かなかったメールであり，おおよそ 2 割となる．

残りの 1 割は条件 (a) と (b) の両方を満たすため拒否したものである．原因は，HELO コマンドの引数が FQDN ではない文字列になっているものがほとんどである．引数が IP アドレスのものはほとんどない．この (a),(b) 両方を満たすとき拒否するという条件は，応答遅延による接続数増大を防ぎ，サーバの接続リソース軽減に役立っている．届かなかった全メール 3 割に対して，条件に該当し，拒否しているメールは 1 割であるから，この条件によるサーバ負荷軽減効果は少なくない．

図 4 には，応答遅延を行ったメールの宛先を，原因別に応答遅延を行った宛先数に対する割合で示している．横軸には日数を表す．応答遅延を行った理由は，条件 (2) の (a),(b) のいずれか一つを満たす場合である．ただし，条件 (a) については，HELO 引数が IP アドレスの場合と文字列だが FQDN でない場合の 2 つに分類した．

■は公開リスト B に登録があるサーバからの宛先数を示しており，95%近くが該当している．HELO コマンドの引数が不正なものは，5%程度であり，*で示した引数が IP アドレスのものはほとんどなく，5%のほぼ全てが□で示している FQDN でない引数のサーバからの宛先であることが分かる．

応答遅延を行ったメールのうち，遅延中に接続が切れてしまい，結果としてメールを拒否したものを × で示しているが，全体の 80%程度との結果になった．

このように，応答遅延が起こるのはほとんどが (a) の条件である公開リスト B への登録が

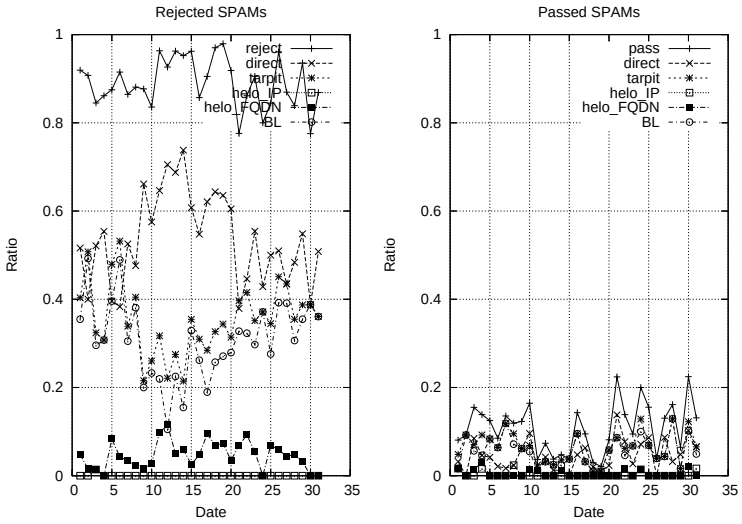

図 5 左図は，人間がスパムと判定したメールのうち，拒否したスパムメール，右図は，拒否出来なかったスパムメールの割合を示す．なお，今回の対策を入れる前から拒否していた公開リスト A により拒否されたメールなどはカウントしていない．
＋ は届かなかった/届いたものの総計，×は直接拒否/許可したもの，*は応答遅延の結果届かなかった/届いたもの，■は Helo コマンドの引数が FQDN でないため応答遅延し届かなかった/届いたもの，□は同じく IP アドレスだったので応答遅延し届かなかった/届いたもの，○は公開リスト B に登録があったため応答遅延し届かなかった/届いたものである．

理由であり，エンドユーザ回線からの接続と考えられる．(b) の HELO コマンドの不正による遅延はほとんどないため，(a),(b) の両方を満たすことを確認することなく (b) の HELO コマンドの不正のみで削除する方が簡便とも考えられる．しかしながら，(b) の条件にのみ合致する正常なメールを送るサーバが報告されたため，(b) のみの条件で拒否は出来ない。

届いたメールにスパムメールが含まれているかどうかは，実際に人間がメールの内容を見てみないとわからない．このため，情報基盤センターの特定のアドレスに届いたメールに関してのみ人間がスパム判定を行なった結果を図 5 に示す．なお，届かなかったメールについては，内容が分からないため，判定が出来ないが，差出人から推測して迷惑メールと判断出来たため，一律迷惑メールとしてカウントした．なお、今回この集計に利用したアドレスは，迷惑メール数が一日あたり 50 から 100 通程度届くアドレスである．

図 5 の左図は，人間がスパムと判定したメールのうち，拒否したスパムメール，右図は，拒否出来なかったスパムメールの割合を示す．なお，今回の対策を入れる前から拒否していた公開リスト A により拒否したメールなどはカウントしていない．

図 5 の左図を見ると，スパムメールのうち今回の対策で拒否出来ているメールは ＋ に示すように 90%程度となる．拒否した原因としては，× に示す直接拒否したものが全体の 5 割程度，これは (2),(3) の条件の両方を満たしたものとなる．次に，応答遅延の結果，受信しなかったものが*に示した 4 割程度となる．この原因はほとんどが○に示す公開リスト B に登録のあったものである．次に多いのが■で示す HELO コマンドの引数が FQDN でないものであり 1 割程度となる．

一方右の図を見ると，今回の対策で阻止出来なかったスパムメールは ＋ で示すもので，迷惑メール全体の 1 割程度であることがわかる．その原因は様々だが，∗ で示した応答遅延にもかからず直接届いたスパムメールは，今回届いたスパムメールの半分程度であることが分かる．遅延にかかるメールも今までの傾向と同様にほとんどが○で示した公開リスト B によるものである．

なお，今回のデータには示さなかったが，正常メールのうち，応答遅延にかかって到着したメールはなかった．しかしながら，この統計に利用したアドレスとは別のアドレスで，(2) の (b) の条件に該当するが遅延して届いたものがあった．送信元から推測して，メーリングリスト配送業者のサーバのようである．

以上のように，今回の対策では，特定のメールアドレスに対しては，今まで届いていたスパムメールの 9 割近くを排除する結果となった．しかしながら，これは特定のメールアドレスでの場合であることに注意してほしい．

5. 結論と今後の課題

今回の提案方式を新潟大学メールゲートウェイに実装することで，スパム対策を行った．今回の対策後，受信メールを 3 割ほど削減することに成功した．一方で，導入から現在まで，偽陽性判定が疑われるケースについては報告がない．ただし，正常メールの中でも，応答遅延の条件に該当し，メールは遅延したもの，接続が切れず受信していたケースが 1 件のみ報告された．

特定のメールアドレスについて，拒否できたスパムメールを調査したところ，対策前に比べて，9 割程度の迷惑メールを拒否しているという結果となった．また，HELO コマンドの引数による判定のみでは，偽陽性判定があることが報告されたが，公開リスト B と HELO コマンド引数を組み合わせて拒否と応答遅延に分けて判定することで，偽陽性判定は無く

Vol.2009-CSEC-46 No.14
2009/7/2

なった．拒否条件の導入により応答遅延を起こす接続を 2/3 に減らすことに成功し，サーバの負荷軽減が出来た．以上のように，今回の方式では，サーバ管理者側でホワイトリストなどの常時メンテナンスをしなくとも，新潟大学のメールゲートウェイとして運用可能であり，かつ，スパムメール対策として有効な設定となることが分かった．

しかしながら，スパムメールが届かなくなったわけではないことや，Bot プログラムが配送効率を多少犠牲にしても応答遅延の方式に対応した場合には，効果が弱くなるなどの問題もある．今後は，普及が期待されている送信ドメイン認証の結果なども組み合わせるなどして，さらに有効なスパム対策を考える必要がある．

謝辞　今回の迷惑メール対策の試験運用，及び，メール集計に協力くださった新潟大学情報基盤センター技術補佐員の沢田浩様に感謝致します．

参 考 文 献

1) C. Rossow: Anti-spam mearure of European ISPs/ESPs (online), available from ⟨http://www.internet-sicherheit.de/fileadmin/docs/publikationen/anti-spam-measures-of-europian-isps-esps.pdf⟩
2) M. Swimmer, I. Whalley, B. Leiba and N. Borenstein: Breaking Anti-Spam Systems with Parastic Spam (online), available from ⟨http://www.ceas.cc/2006/9.pdf⟩
3) R. Ramachandran, D. Dagon and N. Feamster: Can DNS-Based Blacklists Keep Up with Bots ? (online), available from ⟨http://www.ceas.cc/2006/14.pdf⟩
4) H. Asami: Study Report of an Anti-spam System with a 88% Block Rate – The Selective SMTP Rejection (S25R) System – (online), available from ⟨http://www.gabacho-net.jp/en//anti-spam/paper.html⟩
5) 川田良文，山田一成，田島尚徳，拓殖明: 全学メールサービスにおける迷惑メール・ウイルスメール対策, 名古屋大学情報連携基盤センターニュース Vol7, No 3 pp290-294 (2008)
6) 本間輝彰: JEAG テクニカルアップデート　～迷惑メールの現状と技術的課題等について～, 第 5 回迷惑メール対策カンファレンス
7) Postfix SMTP Access Policy Delegation (online), available from ⟨http://www.postfix.org/SMTPD_POLICY_README.html⟩