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

2007－ＤＳＭ－46／2007－ＱＡＩ－24（８）
2007／7／19

Throttlingによるspam対策のためのメールサーバの分別について

三原 槙仁† 吉田 和幸‡

†大分大学大学院工学研究科 〒870-1192 大分市旦野原700
‡大分大学総合情報処理センター 〒870-1192 大分市旦野原700
E-mail: ‡yoshida@csis.oita-u.ac.jp

あらまし 近年，spamメールに関する問題が大きな社会問題となってきている．メール受信時にゆっくり応答をするthrottling機能はspam対策として非常に有効である．しかしながら，throttling機能を使用すると，メールの受信が完了するまで，あるいはspam送信者があきらめるまでSMTPコネクションを維持する必要があるため，メールゲートウェイが過負荷になりやすい．メールゲートウェイに大量のspamメールが送りつけられた場合，それらを処理する間，正常なメールの受信ができないことがある．このような過負荷状態を防ぐにはメールゲートウェイの多重化により負荷を分散するといった方法が考えられるが，単純な負荷分散アルゴリズムではすべてのメールゲートウェイが過負荷に陥るといった危険性がある．本論文では，spamメールを送ってくるMTAの多くがDNSでIPアドレスの逆引きができないこと等に着目してメールを送るメールゲートウェイを決定し，主に通常のメールを処理するメールゲートウェイと主にspamを処理するメールゲートウェイとに多重化することによって負荷分散を行なう手法について論じる．本手法における負荷分散システムの設計及びシミュレーション結果について論じ，実際に開発した本手法を用いたシステムの運用結果を示す．その結果，送られて来るメールのspam含有率に応じた負荷分散を実現し，spamでないメールに与える影響を最小限にできることが確認できた．本システムを用いることにより，通信量の多い環境でもthrottlingといった計算機に対する負荷がかかるspam対策手法を用いることが可能になる．

キーワード 電子メール，spam対策，throttling

Classifying Mail Servers for Spam Control by Throttling

Makihito Mihara† and Kazuyuki Yoshida‡

† Dept. of Computer Science and Intelligent Systems, Oita University Dannoharu, Oita, 870-1192 Japan
‡ Information Processing Center, Oita University Dannoharu, Oita, 870-1192 Japan
E-mail: ‡yoshida@csis.oita-u.ac.jp

Abstract The throttling function, which replies slowly at the e-mail reception time, is very useful for controlling spasm at MTA (Mail Transfer Agent). By using this function, however, MTA is easy to become fault load, because MTA needs to maintain a SMTP connection until mail transfer completes or spam sender gives up transmission of e-mail. When huge amount of spams are sent to the MTA, MTA is not able to establish SMTP connection for normal e-mail transfer until mail processing for spams completes. With simple load balancer, there is a danger that all MTAs lapse into fault load. We describe, while the IP address of many of MTA which sends spams have no reverse record in DNS, the load sharing method with little influence on the normal mail is proposed. It was able to be confirmed to achieve the load-balancing corresponding to the number of spams, and to make the influence given to normal e-mail a minimum. Even if huge amount of spams are sent to MTA, it is able to use throttling function for spam control by this system..

Keyword E-mail, spam, spam control, throttling

1. はじめに

近年，インターネットの急速な発展と普及に伴い，電子メールを初めとするネットワークを介したコミュニケーションは不可欠な物となっている．これに伴いspamメールに関する問題が大きな社会問題となっている．spamメールとは受信者の意図を無視して無差別かつ大量に一括して送信される電子メールを指し，UCE (Unsolicited Commercial E-mail), UBE (Unsolicited Bulk E-mail)とも呼ばれる．

電子メールは通常の郵便と比べると，送信者側があまりに安易にメールを大量の相手に対して送信でき，送信者側の負担が金銭的にも時間的にも労力的にも極めて少ないといった特徴が挙げられる．そのためspamメールの数は非常に多く，世界のspamメール送信数

は一日に 550 億通 [1]，インターネットを流れる電子メールの 95%以上が spam メールであるという報告もある [2]．今後もインターネットの普及に伴い電子メールの流通量は増え続け，spam メールによる被害も増加の一途を辿るであろう．

spam メールの具体的な被害として，以下のことが挙げられる．

a. CPU ，ディスク，ネットワークリソースを浪費
  a1.メールの受信に時間（通信費用）がかかる
  a2. メールボックスが一杯になり，spam でないメールも受け取れなくなる
b. メールの分類・削除にかかる手間
  b1. メール受信後も閲覧，削除に時間がかかる
  b2. 重要なメールの見落としも問題
  b3. 精神的苦痛の発生
また，spam メールを原因とした間接的な被害として
c. 発信者詐称による間接的な被害
  c1. spam メール発信者との誤解
  c2. 苦情メールへの対処
  c3. 信頼性の低下
  c4. 通常メールを受信拒否される可能性
d. エラーメールの集中(バウンスメール)
  d1. 自組織アドレスに詐称された場合におこるものなので，発生頻度は小さいが被害は甚大
  d2. 事実上のサービス不能(denial of service attack) 攻撃
といったことが挙げられる．

現在，大分大学総合情報処理センターでは，ウィルスを検知・除去するためのメールゲートウェイを導入し，学内 LAN とインターネットとの間を行き来するメールについてウィルスの有無の検査と同時に spam 対策も行なっている [3) 4) 5)]．

いろいろな spam 対策を組み合わせて利用する際にそれらを適用する順序によって，spam 検出時に発生するエラーが異なるため，適用順を考慮する必要がある．その用件として以下の２つを設定した．(a)User unknown といった，メールアドレスの有無に関するエラーは，なるべく発生させないようにしたい．(b)コンテンツフィルタリングのように CPU パワーを必要とするものはなるべく後回しにする．また throttling，送信元 MTA の IP アドレスの検査，各ヘッダの検査等，実施するタイミングが固定されているものもある．そのため現在のところ，送られてきた電子メールに対して以下の順序で spam メール対策をしている．使用している MTA は sendmail[6]バージョン 8.13 である．

(1) throttling (greet_pause) [7]
(2)メールヘッダの形式検査 [5]
(3)外部の Blocking List を用いた送信メールサーバの IP アドレスの検査 [5]
(4)LDAP[8]を利用した学内各メールサーバのユーザアカウントの有無の検査 [4) 5)]
(5)greylisting[11]による送信メールサーバの検査 [12]
(6)spamassassin[9]によるメール内容の検査 [10]

greet_pause と greylist は，spam 送信サーバが，大量のメールを送ろうとするため，通常のメールサーバとは異なった動作をすることに注目して，spam 検出を行なおうとするものである．greylist は，一旦一時エラーを送って，再送を待つ方式である．このため，再送されるまで 30 分程度配送に余分な時間がかかる．さらに，再送されたメールであることを確認するために，送信元メールサーバの IP アドレス，送受信メールアドレス，時刻のデータベースを作成する必要があり，そのデータベースのためのメモリー領域を必要とする．このデータベースの保持期間等，設定すべきパラメータが多い．一方，greet_pause では，最初の応答まで待つ時間は，今のところ 60 秒までで十分効果があがっている．設定すべきパラメータは，待ち時間のみである．ただし，TCP コネクションを保ったまま待つので，sendmail のプロセス数，TCP セッション数が増えやすい．そのため，プロセス数があらかじめ決めた上限に達し，新たなプロセスを生成できず，通常のメールの配送に影響が出ることもある．

そこでわれわれは，MTA を多重化することによって負荷分散を行い，従来の spam 対策の効果を減らすことなく通常のメール配送への影響を軽減する手法を提案した [19]．本方式は throttling を用いる場合に効果的な負荷の分散手法である．

本論文の構成は以下の通り．まず 2 章で throttling と greylisting について論じ，3 章で関連研究について述べる．4 章で本システムの設計について述べ，5 章でその運用について述べるとともにその考察を行い，最後の 6 章で結論を述べる．

2. throttling と greylisting

spam メールが近い将来に無くなることは無いと考えられる．spam メールの被害を防ぐにはいかに受信側で対策するかが重要となる．

spam 対策で重要なのは spam メールを受け取らないことではなく，spam でないメールを確実に受け取ることである．さまざまな spam メール対策方法が考案されているが，spam の検出漏れ(false negative rate)よりも，通常のメールの誤検知(false positive rate)という観点で評価すべきである．見逃した spam メールは単に削除すればよいだけだが，重要なメールが spam と判

定されるとその影響は大きい．また，spam メールを大量に送られてきた場合，対策手法の計算機にかかる負荷が多いと，メール配送に遅延が発生するだけでなく MTA の運用自体が困難になってしまうことも起こりうる．

現在の主な spam 対策手法として，spamassasin[9]等のコンテンツフィルタリングがよく利用されている．コンテンツフィルタリングはメールの DATA 部をいったん受信し，メールのコンテンツを見てフィルタリングを行う．そのため CPU 負荷は他の手法と比べて小さくない．そして spam メールの手口が多様化していくにつれて，フィルタを行うためのルールも肥大化する傾向にあり，どうしても誤検知(false positive)の問題がつきまとう．そこで greylisting や throttling といった手法を用いることにより，メールの中身を見ずに，つまり spam メールかどうかではなく，spam 送信者かどうかという観点で判定することで，そもそも受け取る spam メールの数を減らすことが考えられた．これらは spam を見分ける効果も高く(false negative rate)，一般的な MTA からのメールを失う可能性も低い(false positive rate)として現在注目されている．

greylisting と throttling はどちらも spam 送信者が通常とは異なった動作をする MTA を使用するということを利用して，内容を見ないで spam を判断し，大小の差はあれ最終的にメールの配送に遅延を生じさせると言う点では同じである．多くの spam メールは短時間に大量のメールを送れるように最適化された専用ツールで送られる．メールを確実に送り届けることを旨とする一般の MTA とは異なり，少しぐらいのエラーは無視してでも高速かつ大量に送ることを目標に作成されており，タイムアウト時間が短い，一時エラーで再送しない，など一般の MTA と異なる挙動が見られることがある．この違いを利用することで spam メールを削減する．

greylisting は「Spam 発信 MTA は再送をしない」との仮説に基づく方法であり，一時的に受信を拒否し，再送されれば受信するといった動作をする．殆どの spam 発信 MTA は仮説どおりに動作し，高い効果を挙げている．ただしこの方法は配送遅延が大きく，場合によっては 1 時間以上かかるときもある．さらに，再送されたメールであることを確認するために，MTA の IP アドレス，送受信メールアドレス，時刻のデータベースを維持する必要があり，そのデータベースのためのメモリー領域を必要とする．また正当なメールの送信元の MTA に再送を強いることになる点や，spam 送信者でない一部の MTA に再送しないものも存在するため，ホワイトリストの管理が必要となる．

throttling は「spam 発信 MTA は timeout が短い」，「spam 発信 MTA は SMTP の確認応答手順を無視してメールを送る」との仮説に基づく方法であり，コネクション確立後の応答を遅延することで，spam 発信者の MTA がこちらの応答を無視してメールを配送してくるか，あるいはメールの配信をあきらめて接続を切断することを期待するものである．設定すべきパラメータは遅延時間のみであるので設定が簡単であり．再送かどうかの判定が不要であるので，greylisting より適用範囲が広い．また greylisting と比べると配送遅延が数十秒と非常に小さい．ただし throttling では拒否できないが，greylisting では拒否できるものがあり，対策としてどちらか一方に集約できるものではない．throttling では TCP コネクションを保ったまま待つので，プロセス数，TCP セッション数は増えやすいといった問題もある．そのためプロセス数があらかじめ決めた上限に達し，通常のメールの配送に影響が出ることもある．

2006 年 5 月 28 日から 6 月 3 日の 1 週間で大分大学の MTA は 14 万通以上のメールを受け取った(図 1)．その際，プロセス数の上限を超えメールを受付できない状態となってしまった．回数にして 1 週間で 626 回，1 回の停止時間はだいたい 15～19 秒で，累積停止時間は 1 週間で 10131 秒と，およそ 3 時間弱に上る．プロセス数の上限などを考慮の上，IP アドレスの逆引き，DNS Black List 等のブラックリストサービス[13)14)]等を利用して遅延時間を調整することで通常のメールになるべく影響が出ないようにする必要がある．

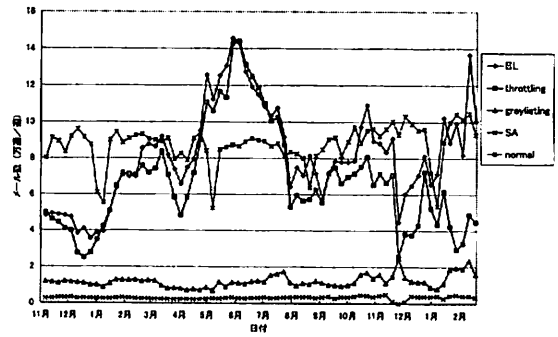

図 1 .MTA の負荷状態

3. 関連研究

計算機を多重化し，spam メールと spam でないメールを分離して処理を行う他の事例としては，普段は電子メールをやりとりしていない MTA に着目する方法[15)]，メールが配送される直前の DNS に対する問合せに着目する方法[16)]が考えられている．

普段は電子メールをやりとりしていない MTA に着目する方法[16)]は，送信者詐称に起因するバウンスメー

ルの集中に対しての対策であり，「普段は電子メールをやりとりしていない MTA が利用する DNS サーバにはこちらの MX レコードのキャッシュが無く，普段から電子メールをやりとりする MTA が利用する DNS サーバにはこちらの MX レコードのキャッシュが存在する」との仮説に基づく方法である．プライマリ MTA とセカンダリ MTA を用意し，複数のバウンスメール送信元 MTA を想定してプライマリ MTA においてバウンスメールを短時間に多数受け取った場合，もしくは DNS サーバに対して特定のドメインに対する MX レコードの問い合わせが短時間に多数あった場合に，DNS の MX レコードを書き換え，バウンスメールがセカンダリ MTA に行くように負荷分散を行う．バウンスメール送信元 MTA が一つの場合は，IP フィルタリングによってセカンダリ MTA にバウンスメールを送る．MX レコードの TTL，開始条件であるバウンスメールの件数や DNS の問い合わせ件数及びその単位時間の設定，DNS の MX レコードの書き換えの終了条件など，設定する項目が多く，利用者の環境やバウンスメールの送信状況に応じて最適なものに調整する必要がある．また，送信元の利用する MX レコードのキャッシュに依存しているため，正当なメールの送信元のキャッシュがない場合等例外が存在し，ホワイトリストの管理が必要となる．

メールが配送される直前の DNS に対する問合せに着目する方法 [17]では，まず DNS の問い合わせ元に応じて MX レコードの応答を変え，受信メールと対応付けすることで，「問い合わせ元 DNS サーバ，送信元 MTA，送信元ドメイン名」を持った DNS サーバエントリを作る．この中から DNS サーバのホワイトリストを作り，それに基づいて受信 MTA を決定し負荷分散を行う．通常のホワイトリストより情報量が多くなるため，単純な送信者アドレスの詐称を防げるなど，ホワイトリストの判定基準の自由度が高い．反面，送信元 DNS や MTA の組み合わせ数が多いので DNS サーバエントリの数が多くなり，従来のホワイトリストよりもメンテナンス等の管理が複雑となる．

4. 設計

本提案の概要は，spam メールを送ってくる MTA の多くが DNS で IP アドレスの逆引きができないこと等に着目して，主に通常のメールを処理する MTA と主に spam を処理する MTA とに多重化することによって負荷分散を行なうことである．

spam メールを処理するためにはどうしても計算機に負荷がかかる．さまざまなコンテンツフィルタリングは CPU にかかる負荷が多く，greylisting のような手法はメモリー領域を数多く必要とする．throttling はプロセス数やセッション数の増加が問題となる．インターネットに流れる spam メールの総数や容量が増え，複雑化していくにしたがい spam 対策手法も多肢にわたり，複雑化していく．spam メールを処理するための計算機負荷を下げることは難しい．計算機負荷が高くなれば大量の spam メールが，実質的なサービス不能攻撃となることも多くなり，spam でないメールの配送にも影響を与えることとなる．そこで負荷分散装置（ロードバランサ）を用いて複数の計算機の多重化により負荷を分散するといった方法が考えられる．しかしながら単純な負荷分散アルゴリズムではすべての MTA に等しく負荷を分散するため，十分な数の MTA を設置していない限り，すべての MTA が過負荷に陥る危険性がある．そこで，完全に過負荷にならないシステムを考えるのでは無く，過負荷状態に陥る量の spam メールが来ても spam でないメール配信にはなるべく影響を与えないシステムを考える．この方法を用いることにより，主に通常のメールを処理する MTA と主に spam メールを処理する MTA を分離することで，状況によっては spam メールを処理する MTA が過負荷状態に陥っても，通常のメールを処理する MTA は正常に稼動し続けることが可能になる．また，通常運用時にはいずれの MTA においても同様の spam 対策が行われるため，主に spam を処理する MTA に spam でないメール送られたとしても，遅延は生じるが，失われることはない．ここで提案する負荷分散装置は以下のようになる(図 2).

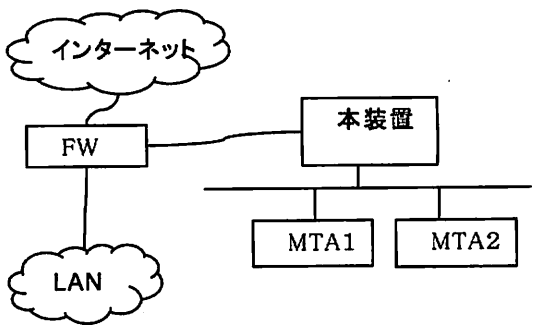

図 2．本装置の設置

通常の負荷分散装置と同様にファイアウォール(FW)と 2 つの MTA の間に配置し，NAT サーバとして動作する．spam でないと思われるメールは MTA 1 で処理し，spam である可能性の高いメールは MTA 2 へ振り向ける．その振り分け方法としてレイヤ 3 レベル(IP アドレス)を用いる．ある電子メールが本負荷分散装置により spam の可能性があるものと判断された場合は，そのディスティネーションアドレスをセカンダリ

MTA に変換する．この際問題となるのはその判断基準である．以前からの MTA の運用により，throttling で検出した spam は spam 全体の 4 割近くを占めており，さらにそのうち逆引き DNS に登録されていない IP アドレスの MTA から送られてくるものが半分以上を占めていたことがわかっている [7) 10)]．また，ブラックリストを用いたものも spam メールの検知の 4 割近くを占めていることがわかっている．

よって本研究では以下の判断基準を考慮する．

(a) パケットのソース IP アドレスが逆引き DNS に登録されていない場合

(b) ブラックリストに登録されているソース IP アドレス

これらを順に適用し，どちらかの条件に合致した場合，NAT[17)]の様にその宛先 IP アドレスをセカンダリ MTA に変換し，IP ヘッダ及び TCP ヘッダのチェックサムを書き変える．これにより spam メールの大半がセカンダリ MTA に送られると考えられる．

負荷分散装置のより具体的な動作について説明する．DNS の MX レコードには MTA1(図 1)の IP アドレスを設定している．

① インターネット側から MTA1 の TCP ポート 25 番宛ての SMTP パケットが届く．
② ソース IP アドレスを抽出する．
③ ソース IP が，
  A ソース IP アドレスが逆引き DNS に登録されていない場合，もしくはブラックリストに登録されている場合，ディスティネーション IP アドレスを MTA 2 に置き換える．
  B それ以外の場合は，何もしない
④ IP ヘッダ及び TCP ヘッダのチェックサムを書き変える

負荷分散装置は，以上のように動作を行う(図 3)．

なお，MTA 1 , MTA2 からの応答に対して負荷分散装置は以下のような動作をする．

① MTA1,2 から SMTP 通信の応答パケットが届く
② ソース IP アドレスを無条件に MTA 1 に変換する
③ IP ヘッダ及び TCP ヘッダのチェックサムを書き変える

MTA 1 , 2 がメールを送出する際の SMTP 通信等上記以外のパケットに関して，負荷分散装置は何もしない．

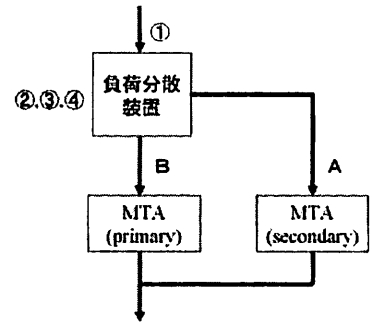

図 3 . 負荷分散装置の動作

また，実際の運用をより簡単にするため，プライマリ MTA とセカンダリ MTA のメールサーバの設定を同じにする．こうすることでセカンダリ MTA に送られたメールでも spam チェックの上，spam でないと判断された場合は通常とおり配送される．さらに各 MTA のメンテナンスの手間を軽減し，メンテナンス不足に起因する false positive や false negative の事故を回避できるといった効果も期待できる．

5. 運用

大分大学で運用しているメールゲートウェイに，今回開発した負荷分散装置を実装し，運用を行った．

2007 年 2 月 18 日から 1 週間で受け取った全メールは 288928 通．この状況で本システムを運用した結果，セカンダリ MTA に送られたメールの数は 55925 通．全体で spam でないと判定されたメールは 95373 通であり，その中で逆引き無しのメールは 3010 通であった (表 3)．また，spam メールの総数は 193555 通であり，逆引きにより検知された spam メールは 52915 通であった．これは設計時に想定した割合である 2 割強と近似しており，うまく負荷分散が行えていると言えるだろう．また，プライマリ MTA における今回実装しなかった DNS ブラックリストによる spam 検知は 71733 通であった．以上を負荷分散の割合で示すと，DNS の逆引きのみの判断の場合，spam 含有率 66%の環境で 24%の負荷分散ができたことを確認した．

表 1 07/2/18 から 1 週間で受け取ったメールの分類

	Primary MTA	Secondary MTA	total
ham	92363	3010	95373
spam	140640	52915	193555
total	233003	55925	288928
Spam ratio	60.4%	94.6%	67.0%

6. おわりに

本論文では，大量に発生する spam メールによるサービス不能攻撃に対して spam でないメールに影響を与えることなく MTA の負荷を分散する方法について，その設計及び実行結果について論じた．具体的には，spam メールを送ってくる IP アドレスは，DNS での逆引きができないといった点や，ブラックリストに載っていることがあるといった点を利用して電子メールを送る MTA を分類し，負荷を分散させた．

本手法を用いることで，送られて来るメールの spam 含有率に応じたプライマリ MTA の負荷が軽減でき，spam でないメールに与える影響を最小限にできることが確認できた．また，主に負荷がかかるメールを中心としてセカンダリ MTA に送っているので，実際のプライマリ MTA にかかる負荷の軽減率は，実際のメール数で見た軽減率以上のものが見込まれる．

これにより通信量の多い環境でも throttling といった計算機に対する負荷がかかる spam 対策手法を用いることができる．単純な負荷分散では過負荷状態に陥る量の spam メールが来ても，本システムではすべての MTA が過負荷に陥る危険性を低くし，spam メールを失うことはあっても，通常のメールを失う可能性は減少する．

今回は，メールサーバの IP アドレスの逆引き，ブラックリストの登録の有無という比較的コストのかかる DNS を用いる方法で，メールの振り分けをおこなった．今後の課題として，本装置内に，ホワイトリストあるいはブラックリストを持つことなどの分類基準のさらなる検討が必要である．

文　献

[1] MYCOM ジャーナル http://journal.mycom.co.jp/news/2006/06/29/002.html.

[2] BBC NEWS [More than 95% of e-mail is 'junk'], http://news.bbc.co.uk/1/hi/technology/5219554.htm

[3] 吉田，矢田，伊藤："spam メール対策と統合メール管理システムについて"，情報処理学会分散システム／インターネット運用技術シンポジウム 2004 論文集, pp.37-42,Jan.2004

[4] 吉田："LDAP を用いた統合メール管理システムについて"，学術情報処理研究 No.7, pp.55-59, Sept.2003

[5] 吉田：" 統合メール管理システムとその使用経験について"，大学情報システム環境研究, Vol.7,pp.47-52, Mar.2004

[6] Sendmail Home Page: http://www.sendmail.org/

[7] 吉田："throttling による spam メール抑制の効果について" 情報処理学会研究報告, Vol.2005 No.39 , pp.69-74 , May 2005

[8] RFC2251, "Lightweight Directory Access Protocol (v3)", http://rfc.net/rfc2251.html

[9] Apache Spamassassin Project: "Spamassassin," http://www.spamassassin.apache.org

[10] 吉田："メールゲートウェイにおける spam メールの検出について" 情報処理学会 DICOMO2004 シンポジウム論文集，pp.493-496，July 2004

[11] Greylisting.org: "a great weapon against spammers," http://www.greylisting.org/

[12] 吉田："greylisting による spam メールの抑制について"，情報処理学会分散システム／インターネット運用研究会，情報処理学会研究報告 2004-DSM-35, pp.19-24, Sept.2004

[13] The Spamhaus Project: http://www.spamhaus.org/

[14] Distributed Sender Blackhole List, http://dsbl.org/main

[15] 山井，岡山，宮下，繁田，丸山，中村："発信者詐称 spam メールに起因するバウンスメール集中への対策方法"，情報処理論文誌，Vol.47, No.4, pp.1010-1020, Apr.2006

[16] 丸山，中村，岡部，山井，岡山，宮下："動的に応答を変える DNS を利用した電子メール受信の優先制御"，情報処理論文誌，Vol.47, No.4, pp.1021-1030, Apr.2006

[17] RFC1631 "The IP Network Address Translator (NAT)", http://rfc.net/rfc1631.html

[18] 三原，吉田："メールゲートウェイの付加分散による spam 対策について"，情報処理学会分散システム／インターネット運用技術シンポジウム 2006，pp.67-72, Nov.2006