Vol.2011-IOT-14 No.9
2011/7/15

メールの安定運用のための メールゲートウェイにおけるサーバ連携について

松竹俊和[†]　吉田和幸[‡]

LAN の入り口にメールゲートウェイを設置し，メールに添付されるウィルスの検査，spam 判定等をここで集中的に行うことも多い．我々は，このメールゲートウェイにおいて，宛先メールゲートウェイの検索や spam 判定のため，宛先，送信元の各メールアドレスのドメイン部については，DNS に登録の有無を確認し，自組織のメールアドレスのローカル部については，LDAP サーバに登録の有無を問い合わせている．DNS サーバ，LDAP サーバのような基幹サーバは複数台稼働させ，障害時にもサービスを停止しないようにしている．しかし，LAN スイッチの障害等により，メールゲートウェイと当該サーバとの通信断は起こりうる．このような場合に，本来正常に送られるべきメールは遅延が起こっても，紛失しないように運用しなければならない．本論文ではこのメールゲートウェイと他のサーバとの通信に障害が起きた時の運用方法とそれによる負荷の増加について述べる．

Cooperation with Mail Gateway and Other Servers for Stabilization of e-Mail Delivery

TOSHIKAZU MATSUTAKE[†]　KAZUYUKI YOSHIDA[‡]

The mail gateway which inspects e-mail whether it is spam, the mail with computer virus or normal e-mail, is set up between the LAN and the Internet. We operate the mail gateway that it checks DNS servers for domain part of e-mail address and LDAP servers for local part of e-mail address of our university. Core servers like DNS or LDAP servers set up redundantly and these services have not been stopped when the trouble occurs. But trouble may occur at the network between mail gateway and other servers. For this case, it is necessary to operate that the normal E-mail should not be to lose. In this paper, we describe operation method when trouble occurred the network between mail gateway and other servers and the load increased by this operation.

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，電子メールはネットワークを介したコミュニケーションの中でも可欠な物となっている．これに伴い spam が大きな社会問題となっている．spam 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，送信者側が容易にメールを多く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．我々は，spam 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各種の spam 対策をそのメールゲートウェイで行なっている [1) 2) 3)].

メールゲートウェイでは以下のような spam 対策を行っている．その適用順を決定するにあたり，以下の 2 つを考慮した．(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する．(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(Mail Transfer Agent)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．

(1) throttling (greet_pause) [5)]
(2) 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 [3)]
(3) 送信元・宛先メールアドレスのドメイン部の検査
(4) メールヘッダの形式検査 [3)]
(5) LDAP [6)]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 [2) 3)]
(6) greylisting [7)]による送信元メールサーバの検査 [8)]
(7) spf[19)]/sender-id[18)]による送信元メールサーバの検査

sendmail の throttling 機能と greylisting は，spam 送信サーバが，大量のメールを送ろうとするため，メール転送プロトコル(SMTP) [11)] の規定とは異なる動作をすることに注目して，spam 検出を行うものである．spf/sender-id は，送信元メールアドレスの正当な MTA を DNS により広報することにより，メール到着時に送信元メールサーバの IP アドレスと DNS で広報されている IP アドレスとを比較することにより，spam 判定を行うものである．

[†] 大分大学大学院工学研究科知能情報システム工学専攻
Department of Computer Science and Intelligent Systems, Oita University
[‡] 大分大学学術情報拠点情報基盤センター
Center for Academic Information and Library Services, Oita University

このように，spam 対策の中には，DNS や LDAP へ登録の有無や，登録情報の内容を問い合わせるものがある．しかしながら，DNS への問い合わせでは，キャッシュサーバを通してメール送信元の DNS へ問い合わせるので, 途中のネットワークの状況やメール送信元ドメインの DNS サーバの状況により, 問い合わせが timeout を起こして，回答を得られない可能性がある．同じ LAN 内にある LDAP への問い合わせに関しても，冗長構成等，サーバが停止しないよう対策を行ったとしても，途中の LAN スイッチの障害等で，回答が得られないことが考えられる．このような場合でも，メールを永久エラーとして廃棄するのではなく，DNS，LDAP の回復を待って，当該メールを配送すべきである．そこで我々は，メールゲートウェイの設定ファイルに置いて，サーバ間の通信障害時の対策を行っている．本論文ではこれらの対策とその運用結果について述べる．本論文の構成は以下の通りである．まず，2 章でメールゲートウェイと LDAP のサーバとの連携と障害時の対策について述べ, 3 章で DNS との連携と障害時の対策について述べる．4 章ではこの 2 つの障害時対策と利用者の利便性ついて考察する．5 章は結論である．サーバ連携障害時の対策をまとめ，課題について述べる．

2. LDAP サーバとの連携と障害時対策

図 1．にメールゲートウェイの構成と LDAP など他のサーバとの連携関係を示す．図 1 中の sendmail(前)は，受信したメールに対して各種の spam 対策を適用している．自組織宛に来たメールのローカル部について，LDAP にアカウントの有無を問い合わせている [1)2)3)]．LDAP に登録されていないものは，宛先不明エラーとして受信拒否する．このようにすることで，エラーメール(Bounce Mail)の発生を抑制できる．「宛先不明エラー」は恒久エラーであるため，そのメールは，送信元メールサーバで廃棄されるであろう．LDAP は，教育用 PC のログイン認証や e-Learning system の認証等にも

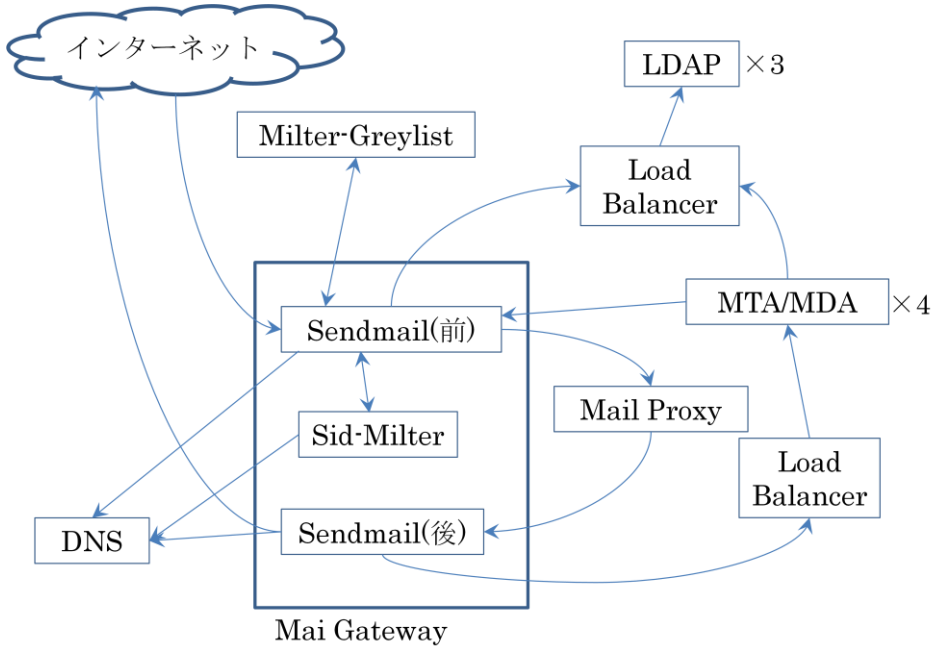

図 1．メールゲートウェイと他のサーバとの連携関係

```
DU oita-u.ac.jp
      ...
Scheck_rcpt
      ...
R$*<@$U>    $:$1<@$U> $| $(searchldap $1@$U $:<no> $) $| $(searchldap yoshida@$U $:<no> $)
R$*$|$*$|<no>     $#error $@ 4.7.1 $:451 busy now, try later
R$*$|<no>$|$*     $#error $@ 5.7.1 $:551 User Unknown
R$*<@$U>          $@ OK
```

図 2．Sendmail の設定(Ldap への問い合わせ)

使用している基幹サービスであるので，負荷分散装置を通して 3 台の LDAP サーバを運用しており，2 台までサーバが障害等でダウンしても残りのサーバで運用を継続でき，LDAP を利用する他のサーバは LDAP サーバの IP アドレスの変更等設定変更する必要がない．

このような障害対策を施しても，途中の LAN スイッチの不具合等で，メールゲートウェイと LDAP との通信ができないこともありうる．メールゲートウェイ内では，LDAP サーバとの通信ができないときの状態と，LDAP に登録がない状態との区別ができない．そのため，LDAP への問い合わせができなくなると，すべてのメールを宛先不明メールとして受信を拒否してしまう．これを防ぐために図 2 のように受信したメールの宛先メールアドレスとともに，必ず LDAP 中に存在するメールアドレスも同時に問い合わせる．後者の問い合わせに対して否定する回答が来た場合，LDAP サーバとの通信障害であるので，一時エラーとして，再送されるまでに LDAP サーバとの通信が回復することを期待する．前者の問い合わせが否定され，後者の問い合わせが肯定された場合，LDAP サーバとの通信は正常であるので，宛先不明エラーとする．

利用者のメールボックスが存在する図 2 中の MTA/MDA サーバ(以降 MDA と省略する)も当然 LDAP を利用している．LAN スイッチの障害箇所によっては，メールゲートウェイは LDAP と通信できるが，MDA が LDAP と通信できないこともありうる．この場合，メールゲートウェイを通過した後，MDA で宛先不明となって廃棄されてしまう．このような状況を避けるため，MDA においては，「宛先不明エラー」を恒久エラーではなく，一時エラーとしている．

メールゲートウェイは, MSA(Mail Submission Agent)の機能も持っており, MUA(Mail User Agent)から smtp auth を用いた認証要求が来た時，LDAP に ID/パスワードを問い合わせる．これに関しては，相手が MUA であり，LDAP との通信に障害が起き，送信ができなかった場合，メールは MUA 上に残り，利用者に認証失敗によりメール送信の失敗が伝わるので，これに関する障害対策は行っていない．

3. DNS サーバとの連携と障害時対策

メールの配送には, DNS の検索が欠かせない. spam 対策のいろいろな場面でも DNS との連携が必要になる．図 1 の sendmail(前)では，spam 送信者の blacklist の検索および，送信元メールアドレス，宛先メールアドレスそれぞれのドメイン部が DNS に登録されているかどうかの検査を行っている. spf[19]/sender-id[18]の検査を行う sid-milter では送信元メールサーバに関する情報を持っている spf レコード等を DNS へ問い合わせる．sendmail(後)では，配送先の決定のために DNS へ MX レコード等を問い合わせる．

DNS への問い合わせは，LAN 内の DNS キャッシュサーバに対して行い，キャッシュサーバ内にない場合, キャッシュサーバから問い合わせ先の DNS コンテンツサーバに問い合わせ内容を転送する．

```
Kcanon host -a<OK> -T<TEMP>
Kdnsmx dns -R MX -a<OK> -T<TEMP>
Kresolv sequence dnsmx canon
# Kdnsaaaa dns -R AAAA -a<OK> -T<TEMP>
# Kresolv sequence dnsmx canon dnsaaaa
...
SCheck_mail
...
R$*<@$*>$*              $: $1<@$2>$3 $| $(resolv $2. $: $2 <PERM> $)
R$+ $| $*<PERM>         $#error $@ 4.1.8 $: 418 Unreturnable address rejected
R$+ $| $*<TEMP>         $#error $@ 4.1.8 $: 418 Sender domain must be resolved
...
SCcheck_rcpt
...
R$*<@$*>$*              $: $1<@$2>$3 $| $(resolv $2. $: $2 <PERM> $)    host part
R$*<PERM>               $#error $@ 4.1.9 $: 419 Receiver domain unknown
R$*<TEMP>               $#error $@ 4.1.9 $: 419 Receiver domain must be resolved
...
```

図３．sendmail の設定(メールアドレスのドメイン部の検査)

blacklist 参照，spf/sender-id 検査について，DNS キャッシュサーバや，問い合わせ先の DNS コンテンツサーバの不調, あるいはインターネットの途中の経路の障害により，これらの問い合わせが完了しなかった場合，その登録がなかったことになり，その場合，メールゲートウェイは通常通り配送処理を行う．そのため，blacklist, spf/sender-id のために DNS の障害対策を施す必要はない．

一方，送信元および宛先メールアドレスのドメイン部の検査に関しては，DNS への問い合わせに対する応答が得られなかった場合，送信元／宛先メールアドレスのドメイン部が DNS に登録されていないことになってしまう. 送信元メールアドレスのドメイン部が DNS に登録されていないということは, 送信元メールアドレスが架空のものであり返信することができないため，spam であることが強く疑われる．宛先メールアドレスのドメイン部が DNS に登録されていないということは, 当該メールが配送不可能であることを示す．これらの場合には，メールゲートウェイが当該メールを受け取って配送処理を続けることは適切ではない．しかし，恒久エラーとしてしまうと DNS サーバへの通信障害の時に実際には通常のメールを spam あるいは配送不能メールとして廃棄してしまう可能性が残る．そのため，これらの場合，一時エラーとして再送を促し，再送時までに DNS が回復することを期待する(図３).

4. 障害対策の利用者への影響

2，3 章で述べたように，LDAP，DNS との間の通信障害に関しては一時エラーとすることでメールの紛失を起きないようにしている．まず，LDAP サーバとの連携について検討する．LAN 内にある LDAP サーバとの間の通信障害はまれであり，それが起きた場合にも，すぐに対処できるであろう．一方，DNS との連携に関しては，「登録なし」の応答があった場合，当該ドメインの DNS サーバとの間の通信障害のほか，メールアドレスの書き間違い, 送信元アドレスの偽装といったもともと DNS への登録がない場合も考えられる. この場合, DNS へ何回問い合わせても応答は当然「登録なし」なので，メールの再送回数が増える．

図 4 に LDAP サーバが正常に応答しなかったメール数を週ごとに集計したグラフ示す．LDAP サーバの運用が安定している時にはほとんど出現しないが，システム更新時期等のどうしても運用が不安定になる時期には起こりやすい．2011 年 3 月から 4 月にかけてメールゲートウェイ，LDAP サーバを含む情報基盤センターの大部分のシステムを更新した．図 4 ではこのシステム更新時期のみを表示している．この期間中でも大半は 0 であり，多い週でも 72 件である．LDAP との通信障害はまれであり，メールゲートウェイにはほとんど負荷をかけていない．

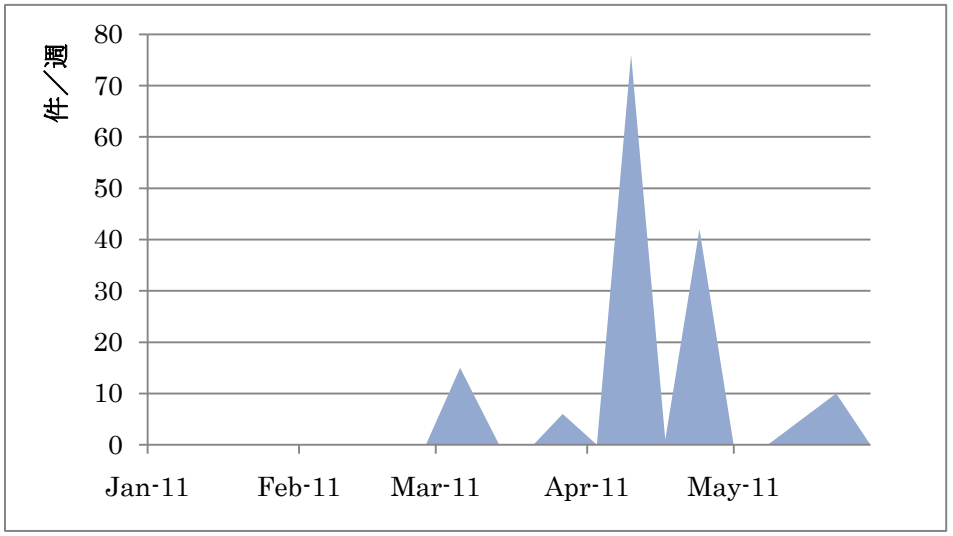

図４．LDAP が正常に応答しなかったメール数

図 5 にメールアドレスのドメイン部が DNS に登録されていないメールの週当たりの検出数を示す．sendmail,, postfix 等の MTA から送られてくる場合には，1 時間ごとに 5 日間つまり 120 回再送が繰り返される．spam であった場合には再送されないこともありうる [7]が，それを考慮しても，図 5 には相当数が重複して計数されている．図 6 には，週当たりのその他の spam 等の検出数を示す．図 5 の件数が重複しているとはいえ，図 5 と図 6 とを比べると図 5 の発生件数が極端に多いわけではなく greylisting での検出数の半分程度であり，メールゲートウェイの負荷としては負担になるほど大きくはない．

図 5 で 2011 年 3 月に急激に検出数が増えているのは，システム更新により MDA のユーザインターフェースが変更になったため，送信元，宛先メールアドレス双方の書き間違いが増えたものと考えられる．さらに宛先メールアドレスに関しては東日本大震災により DNS がダウンしてしまったドメインへのメールが滞留したものも含まれている．2011 年 4 月以降は，教務情報システムから学生の携帯メールアドレス宛のメールサービスが始まったことにより，携帯メールアドレスの登録ミスが多数発生しているものと思われる．

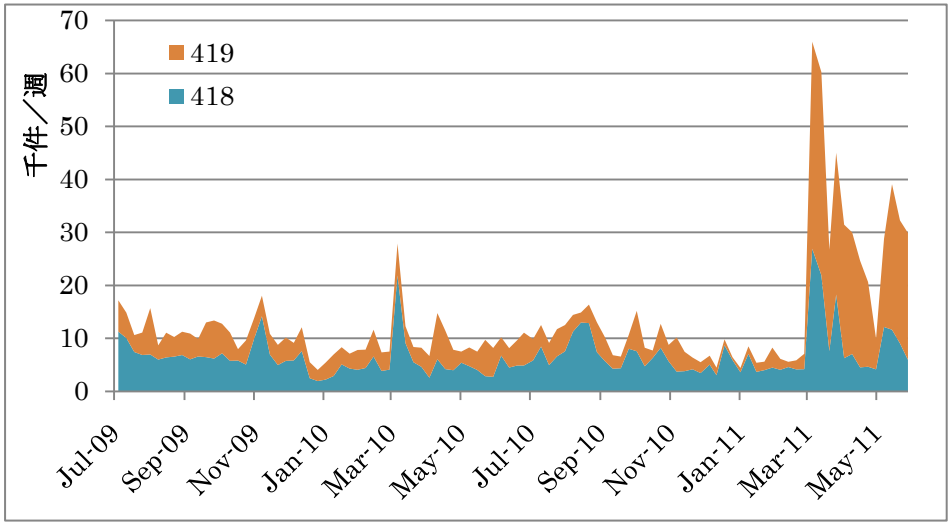

図５．メールアドレスのドメイン部が DNS に登録なしとされたメール数

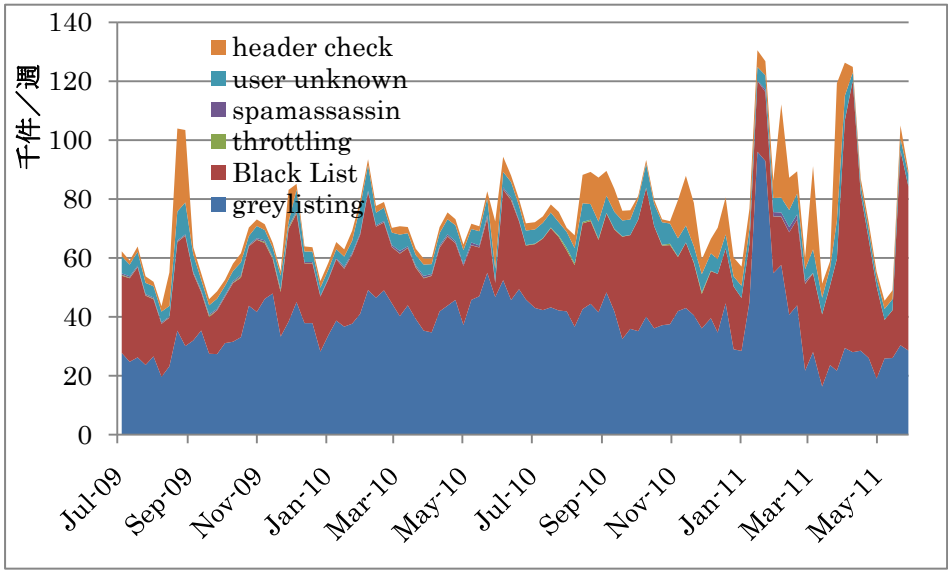

図６．spam 検出数

宛先メールアドレスを書き間違えた場合，途中で「まだ送信が完了していない」というメッセージが送信者へ送られるが，最終的に「送信できなかった」ことは通知されるには 5 日間かかる．利用者には「再送中」ではなく，早めに「宛先不明」を通知したい．さらに，メールの設定が不十分なサーバから送信元メールアドレスのドメイン部が初期値である localhost.localdomain のまま送られてくることがあり，これを受け入れていると，メールゲートウェイが過負荷になることも考えられる．そのため，今までに宛先 MTA が存在しなかったメールのドメイン部をいくつか集めて一覧表を作り，これと比較することで，同様に宛先を間違えたメール，送信元メールアドレスを設定していないあるいは設定ミスをしているメールを即座に恒久エラーとして検出している．現在，この一覧表には，101 件のドメイン名が登録されている．その一部を図 7 に示す．

oita-u.acjp
oita-u.a.cjp
oita-uac.jp
oita-uc.jp
oita-u.ad.jp
oita-u.au.jp
oita-a.ac.jp

図７．即座にエラーとするドメイン名の例

5. おわりに

本論文では，メールゲートウェイにおいて LDAP サーバ，DNS サーバへの検索要求に対して正常な応答が得られなかった場合の対策について述べた．LDAP サーバについては，サーバの正常動作を確かめるための余分な問い合わせを追加することにより一時エラー，恒久エラーに分けた．DNS サーバについては，問い合わせ先は任意のドメインの DNS になるため，「登録なし」となったドメイン名はすべて一時エラーとしている．ただし，明らかに書き間違いであると思われるドメイン名の一覧表を作り，再送数が極端に増えることを防いでいる．

DNS の検査に関しては，改良の余地があると思われる．運用を通じて改良していきたい．

参考文献

1) 吉田和幸，矢田哲二，原山博文，伊藤哲郎：“spam メール対策と統合メール管理システムについて”，情報処理学会論文誌，Vol.46，No.4，pp.1035-1040 (2005).
2) 吉田和幸：“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 (2003).
3) 吉田和幸:“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 (2004).
4) Sendmail Home Page: http://www.sendmail.org/
5) 吉田和幸：“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，TM2005-13，pp.69-74 (2005).
6) M.Wahl，T.Howes，S.Kille:“Lightweight Directory Access Protocol (v3)”, rfc2251, http://www.ietf.org (1997).
7) Greylisting.org - a great weapon against spammers: http://www.greylisting.org/
8) 吉田和幸：“greylisting による spam メールの抑制について”，情報処理学会研究報告，2004-DSM-35，pp.19-24 (2004).
9) Apache Spamassassin Project:“Spamassassin”, http://www.spamassassin.apache.org
10) 吉田和幸：“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 (2004).
11) J. Klensin;“Simple Mail Transfer Protocol (SMTP)”, rfc2821, http://www.ietf.org , Apr.2001
12) 三原槇仁，吉田和幸：“メールゲートウェイの負荷分散による 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 (2006)
13) 三原槇仁, 吉田和幸:“Throttling による spam 対策のためのメールサーバの分別について”，電子情報通信学会 信学技報，IA2007-17，pp.43-48 (2007).
14) 飯田隆義，吉田和幸：“spam メール対策のためのメールサーバの分別について”，情報処理学会 DICOMO2009 シンポジウム論文集，pp.1291-1296 (2009).
15) The Spamhaus Project: http://www.spamhaus.org/
16) K.Egevang, P.Francis:“The IP Network Address Translator (NAT)”, rfc1631, http://www.ietf.org , (1994).
17) 松竹 俊和，吉田 和幸:“iptables を利用した spam 対策用 whitelist を一元管理するためのメールシステム”，情報処理学会インターネットと運用技術シンポジウム 2010 論文集，Vol.2010, No.14, pp.75-80, (2010).
18) J. Lyon, M. Wong: Sender ID: Authenticating E-Mail，rfc4406, http://www.ietf.org , Apr.2006
19) M. Wong, W. Schlitt: Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1, rfc4408, http://www.ietf.org , Apr.2006