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

2007－ＤＳＭ－45（16）
2007／5／11

メンテナンスフリーを目指した 適用時間限定型greylistingによる迷惑メール対策とその効果

石島 悌† 平松 初珠† 林 治尚††

† 大阪府立産業技術総合研究所 情報電子部
〒 594-1157 大阪府和泉市あゆみ野 2-7-1
†† 兵庫県立大学 学術総合情報センター
〒 671-2201 兵庫県姫路市書写 2167
E-mail: †{ishijima,hiramatsu}@tri.pref.osaka.jp, ††hayashi@laic.u-hyogo.ac.jp

あらまし 迷惑メール対策において，効果の高い手法の一つとしてgreylistingが知られている．しかし，この手法では，リストのメンテナンスが必要なことと，配送遅延の発生が問題となっている．そこで，受信者がいつでもメールを読める状態にある業務時間内は，再送要求を出さずにそのままメールを配送することとし，greylistingが適用される時間を限定した．これによって，リストのメンテナンスと配送遅延の問題を解決することを試みた．一方，このままでは，業務時間内に配送される迷惑メールの減少が期待できないので，throttlingを併用することとした．本稿では，以上の適用時間を限定したgreylistingとthrottlingを併用した迷惑メール対策と，その効果について報告する．
キーワード 迷惑メール，greylisting，配送遅延，メンテナンスフリー，throttling

An Anti-Spam Method with Greylisitng at Night and its Effectiveness

Dai ISHIJIMA†, Hatsumi HIRAMATSU†, and Haruhisa HAYASHI††

† Information and Electronics Department, Technology Research Institute of Osaka Prefecture
Ayumino 2-7-1, Izumi City, Osaka, 594-1157 Japan
†† Library and Academic Information Center, University of Hyogo
2167, Shosha, Himeji City, Hyogo, 671-2201 Japan
E-mail: †{ishijima,hiramatsu}@tri.pref.osaka.jp, ††hayashi@laic.u-hyogo.ac.jp

Abstract Greylisting is known as one of the highest effective method within anti-spam method. However, it has issues that requires the maintenance of the list, and forces delivery delay of e-mails. So, we tried to resolve those issues by transfering e-mails without retransmission request during working hours. And also we used throttling to try to reduce spam mails during working hours. In this paper, we report on the controlling spam mails with greylisting and throttling, and it's effectiveness.
Key words Anti-Spam method, Greylisting, Delivery Delay, Maintainance-Free, Throttling

1. はじめに

インターネットは，業種や規模を問わず，多くの企業・事業所や教育機関で使われるようになった．また，世帯普及率も年々向上し，今や，我々の生活や社会活動になくてはならないメディアに成長した[1]．

その中でも，電子メールはインターネットでのコミュニケーションツールとして定着している．単なるメッセージの送受信だけでなく，添付ファイルを使って，さほど大きくないデータをやりとりするといった用途でも使われている．インターネット利用者にとって，メールは最も身近で手軽なコミュニケーションツールの一つであるといっていいだろう．

その一方で，メールをとりまく環境にはさまざまな問題もある．その中で最も大きな問題となっているものの一つが，迷惑メールである．迷惑メールには，受信者の意図にかかわらず，勧誘や宣伝を目的として大量に送られてくるメールや，不正プログラムに感染したパソコンから，感染の拡大を目的として送られてくるメールなどがある[2]．

迷惑メール対策には，メールの中身をチェックするコンテンツフィルタリングや，迷惑メールを送信してくるSMTPク

ライアントの特徴的な挙動を逆手にとった greylisting [3] や throttling [4] といった手法がある．これらの手法は，実際に多くのサイトで利用されている．

greylisting は，迷惑メールを送信する SMTP クライアントは再送をほとんど行わない，という仮説に基づく手法である．

この手法では，送信元の SMTP クライアントに関する情報とアクセス時刻をデータベースに記録する．そして，そのデータベースを参照して，過去にメールの送信を試みた SMTP クライアントであればそのまま配送し，そうでなければ再送要求を出す．

この仮説は多くの場合有効であり，greylisting は効果の高い迷惑メール対策手法であるという評価を得ている．一方，データベースに記録されていない送信元からのメールについては，再送のために配送遅延が生じる．これを防ぐためには，greylisting の適用を避けるためのホワイトリスト [5] やデータベースの適切なメンテナンスが必要である．

なお，遅延を防ぐ手法として，複数の MTA を運用し，連携をとる方法がある [6]．この方法は，大学や大企業のように，複数の MTA を運用する余裕のある，比較的規模の大きな組織にとっては非常に有用な手段である．しかし，中小事業者のように，割り当てられているグローバル IP アドレスの少ない組織では，この手法を採用するのは難しい．

ところで，受信者の立場からすると，配送の遅延が問題となるのは，受信者自身がメールを読むことができる状態にいるときのみである．最終的にメールが配送されるのであれば，受信者がメールを読めない状態においては，何時間メールが遅延したとしても全く問題とならないといえる．

そこで，大阪府立産業技術総合研究所（以下，大阪府産技研）では，職員が不在となる夜間にのみ greylisting を適用し，業務時間内はデータベースへの登録を行い，メールを遅延なく通過させる，適用時間を限定した greylisitng を導入した．この手法では，業務時間内は配送遅延が発生しない．

また，通常の greylisting では，時間の経過につれて，送信元情報を蓄積するためのデータベースが大きくなっていく．データベースを無制限に成長させることは好ましくないので，適当なタイミングで古いデータを消すといったメンテナンス作業が必要となる．

一方，今回の提案手法では，業務時間内にデータベースを空にするという非常に荒っぽいデータベースの管理が可能となる．これは，業務時間内であればそのまま配送するという本方式の利点をいかした方法である．つまり，greylisting で必須となるデータベースのメンテナンス作業を事実上放棄することが可能となる．

しかしながら，この適用時間限定型の greylisting では，業務時間内に配送される迷惑メールには対処できない．このため，SMTP クライアントに対してゆっくりと応答する throttling を併用することにした．

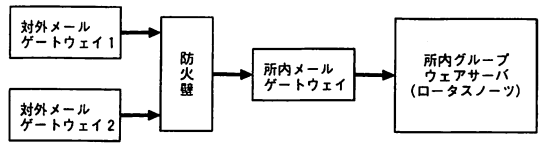

図 1　大阪府産技研の電子メールシステム概略図

2. 大阪府産技研の電子メールシステムとこれまでの対策

2.1 大阪府産技研の電子メールシステム

大阪府産技研では，1996 年の移転統合時に所内ネットワークシステムを構築し，それと同時に電子メールの利用を開始した．各メールゲートウェイや防火壁，グループウェアサーバは随時更新しているが，システムの全体構成は，導入時から大きくは変わってない．現在のメールシステムの概略を図 1 に示す．

対外メールゲートウェイは 2 台あり，所外からのメールはこのいずれかが受信する．これらのメールゲートウェイでは MTA として Postfix [7], [8] を利用している．

これらの対外メールゲートウェイで受信したメールは，防火壁と所内メールゲートウェイを経由して，所内グループウェアサーバであるロータスノーツに配送される．

2.2 これまでの迷惑メール対策

大阪府産技研においても，近年，多くの迷惑メールが届くようになった．そこで，積極的とはいえないが，各部署や職員が開設しているウェブページにメールアドレスを書かない，インターネットでの技術相談は，メールではなく PHP を使ったウェブアプリケーションで受け付ける [9] といった方法をとってきた．なお，ウェブアプリケーションで技術相談を受け付けているのは，相談内容を受付窓口で一括管理するという目的もある．

メールアドレスをウェブページに掲載しない方針を決定した後に採用された職員には，迷惑メールはほとんど届いていない．しかし，それ以前にウェブページを開設し，自身の連絡先としてメールアドレスを掲載していた職員には，多くの迷惑メールが届くことが問題となっている．

そこで，所内メールゲートウェイにおいて，Procmail [10] を使ったコンテンツフィルタリングを，希望者を対象として実施している．なお，グループウェアサーバには，迷惑メールを分別するフィルタリングの機能はない．

フィルタリングによって，本来読まなければならないメールまで排除してしまっては，迷惑メール対策として本末転倒である．そこで，このフィルタリングでは，Procmail で迷惑メールと判定したメールの Subject に「MAY-BE-JUNK」という文字列を付け加え，グループウェアサーバの機能によって受信フォルダを振り分けることにした．つまり，この方式では，迷惑メールも含め，すべてのメールはグループウェアサーバに配送される．

このフィルタリングによる分別で，職員が直接目にする迷惑メールは劇的に減少し，おおむね週に数通以下になった．しかし，グループウェアサーバが処理するメールの件数自体は減少

しない．このため，なるべく入口である対外メールゲートウェイで迷惑メールを排除することが求められるようになってきた．

また，メールを媒介とするコンピュータウイルスについては，グループウェアサーバにおいて，ウイルスチェックを行っている．このため，メールを介してウイルスに感染するといった被害はほとんど発生していない．しかし，問題となるメールは年々増加する傾向にあり，グループウェアサーバにあまり負荷がかからないようにすることも求められてきた．

3. greylisting と throttling による対策

次に，以上の現状を踏まえ，今回導入した適用時間を限定した greylisting と throttling による対策について説明する．

3.1 適用時間限定型 greylisting

greylisting は，ホワイトリストに登録されていない発信元や，これまでにメールを送信してきたことのない発信者からのメールに対して，再送信を要求することによって，迷惑メールの受信を避ける手法である．

その性質上，これまでにメールを送ってきた発信元の IP アドレス，送信元メールアドレス，宛先メールアドレス，アクセス時刻などをデータベースに蓄積しておく必要がある．このため，データベースのメンテナンスを行わないと，データベースに記録されていく情報は，時間の経過とともに増えていく．そして，何らかのタイミングでデータベースをメンテナンスする必要が生じる．

また，ホワイトリストやデータベースに登録されていない発信者からのメールは，必ず再送要求が返されるため，メールの配送に遅延が発生するというデメリットが存在している．

しかし，この手法は迷惑メール対策としては非常に有効な手段なので広く用いられている．

ここで，メール配送の遅配について考えてみる．確かに，メール配送において遅配が発生するというのは，送信側からすればメールスプールに割くリソースなどが要求されることや，受信側からすればすぐに届かないという大きなデメリットがある．しかし，メール配送の遅配というのは，いかなる場合でも避けなければならない事象であるとはいえない．

たとえば，職員が全員帰宅してメールを読むことができない状況であれば，ある人に送信されたメールは，その人が出勤する直前まで配送が遅れても，受信側としては全く問題とならない．

もちろん，送信側の立場からすれば，いつまでもメールがスプールに居座り続けるという状況は好ましいとはいえない．とはいえ，負荷分散などを目的として，複数の MTA を配送に使っているようなケースでなければ，メールの遅配は通常 30 分から数時間程度で解消する．

次に，職員が仕事場にいて，いつでもメールを読むことができる時間帯を考える．このときはできるだけ遅配を減らした方がよい．すべてのメールについて遅配をなくすには，greylisting による再送要求を出さない，というのが最も単純な解決方法である．

大阪府産技研では，職員の勤務時間は基本的に 9:00 から 17:45 までであり，最寄駅からの公共交通機関であるバスは，朝は 7 時半から，夜は 21 時前までしか運行されていない．そこで，職員が不在となる 21 時から翌朝 6 時までは greylisting を適用し，6 時から 21 時までは greylisting のデータベースへの登録のみを行い，メールをそのまま配送するという対策を行うこととした．

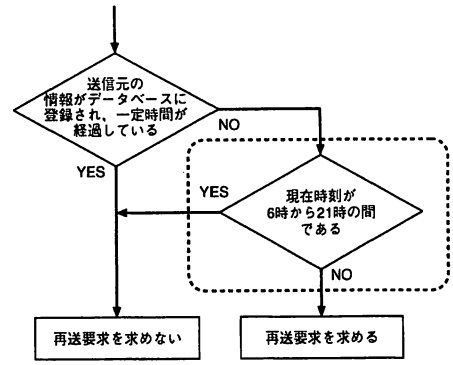

図 2 greylist.pl に追加した処理

また，このように業務時間中はメールを素通しすることによって，負荷分散などを目的として複数の MTA を運用している，大手プロバイダなどから発信されたメールをいつまでも受け付けない，という好ましくない状況を避けることができる．

なお，greylisting に用いたソフトウェアは，MTA である Postfix に付属する `examples/smtpd-policy/greylist.pl` をベースとしている．この元の perl スクリプトに，図 2 の点線内の条件分岐を追加し，6 時から 21 時までの間なら，再送要求を出さないこととした．

ここで，再送要求を返さない時間を朝 6 時からに設定したのは，再送による遅延が発生しても，出勤時間までには確実に配送されるように余裕を見込んだためである．

また，greylisting に用いるデータベースは，毎週月曜日の朝 7 時頃に空にしている．この時間は，greylisting の登録のみを行っているので，データベースをいきなり空にしても遅配が生じる恐れはない．データベースを空にする時は，MTA である Postfix は一旦停止させている．このため，2 台ある対外メールゲートウェイにおいて，データベースを空にする時間をずらしている．

3.2 throttling の併用

前述のように，夜間にのみ適用時間を限定した greylisting は，業務時間内とその前後，すなわち今回の場合，朝 6 時から夜 21 時までに到着する迷惑メールには全く効果がない．そのため，その時間帯については，送信側の SMTP クライアントに対してゆっくり応答する throttling を併用することにした．

Postfix においては，バージョン 2.3 以降からアクセスマップにおいて sleep 指示子を使うことによって，SMTP クライアントに対する反応を遅らせることができるようになった．また，そのアクセスマップを適用するタイミングは，TCP セッションが確立し「`220 hostname …`」のグリーティングバナーを送

```
/^unknown$/                                  sleep 35
/^ppp[0-9]+\.some-provider\.ne\.jp$/         sleep 20
/./                                          sleep  1
```

図 3　正規表現マップを用いた throttling 設定例

る直前と,「RCPT To:」に対する返事を送信するときの 2 つを選ぶことができる.

throttling で設定する項目は，これらの 2 つ，あるいはいずれかのタイミングで待つ秒数だけである．この設定秒数に大きな値を指定すると，SMTP クライアントとのコネクションが張られたままになり，MTA のリソースを消費してしまう．また，迷惑メールの送信元でない SMTP クライアントを無駄に待たせてしまうことにもなる．

そこで，throttling におけるこれらの好ましくない状況を避けるため，正規表現マップを用いることにより，迷惑メールを送ってくると思われる SMTP クライアントには長い待ち時間を，そうでないと思われる SMTP クライアントには短い待ち時間を設定した．

これまでの経験から，迷惑メールを送ってくる SMTP クライアントは，ドメイン名を IP アドレスから逆引きできないところが多いことが判っていた．そこで，たとえば図 3 のように，接続元に応じて待ち時間を変えるように設定した．

この例は，ドメイン名を逆引きできない SMTP クライアントには 35 秒，ADSL や FTTH などで接続し，プロバイダの正規の MTA を経由しない SMTP クライアントには 20 秒，それ以外のすべての SMTP クライアントについては 1 秒待つというものである．なお，実際に使用しているルールでは，SMTP クライアントをもう少し細かく分類している．

また，throttling は，greylisting とは異なり，24 時間ずっと適用することにした．

4. 本迷惑メール対策の効果と考察

ここまで説明した，適用時間限定型 greylisting と throttling の併用による迷惑メール対策を，2007 年 1 月 4 日から，図 1 の 2 台の対外メールゲートウェイに適用した．次に，その効果について説明する．

まず，著者（石島，以下同じ）宛に届き，所内メールゲートウェイでの Procmail によるフィルタリングで，迷惑メールと判定したメールの件数の変化を図 4 に示す．その期間は，対策実施日である 2007 年 1 月 4 日をはさんだ，2006 年 11 月 1 日から翌 2007 年 3 月 31 日までである．

なお，この図に示しているものは，フィルタリングで迷惑メールと判定されたメールの件数である．今回の対策とは関係なく，実際に目にする迷惑メールは，週に数通程度である．

この図 4 から，対策実施前の 2006 年 11 月と 12 月では，1 日平均で約 170 通の迷惑メールが届いていたが，1 月以降は 40 通程度にまで大幅に減少していることがわかる．

一方，迷惑メールの数はおよそ 1/4 へと大幅に減少したものの，その数はゼロにはなっていない．これは，昼間は greylisting

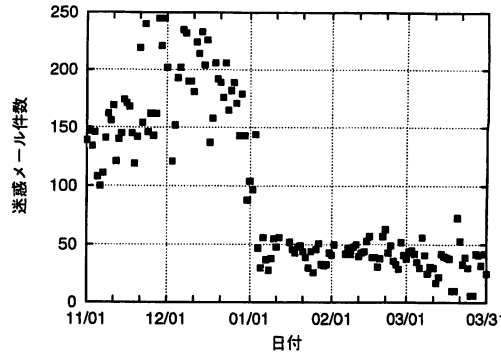

図 4　迷惑メール数の変化

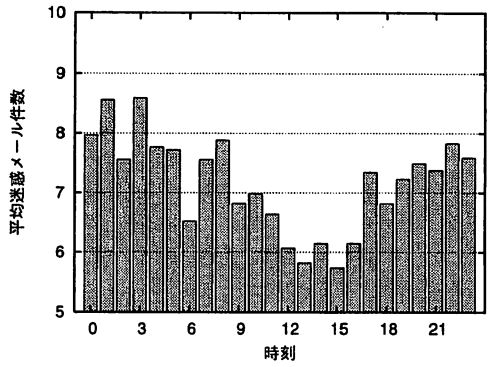

図 5　対策前の時間帯別迷惑メール数

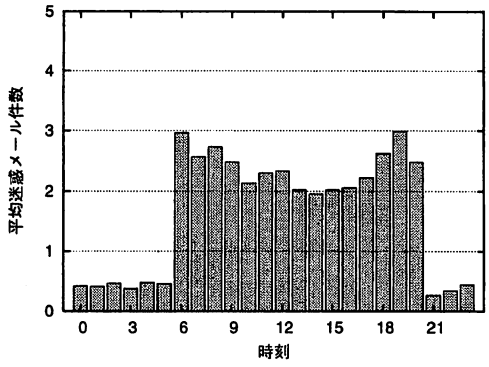

図 6　対策後の時間帯別迷惑メール数

に用いるデータベースの登録のみを行い，メールが素通しになっていることに起因するものであると考えられる．

このことについて，対策実施前および実施後の時間帯別の迷惑メール件数を調べた．その結果を，それぞれ図 5 および図 6 に示す．

図 5 から，対策実施前は，1 時間あたり平均して約 7.2 通の迷惑メールが到着していることがわかる．昼間は迷惑メールが若干少ないが，時間帯による変化はさほど大きくはない．最も迷惑メールが多いのは 3 時の約 8.6 通で，逆に最も少ないのは

15 時の約 5.7 通である．

次に，対策実施後の時間帯別の迷惑メール件数であるが，こちらは，図 6 から，夜間に到着する迷惑メールが激減していることがわかる．greylisting が機能している夜間に届く迷惑メールは約 0.4 通であり，対策前の同時間帯の約 7.9 通と比較しておよそ 1/20 にまで減少している．

一方，昼間に到着した迷惑メールは，対策実施前の約 6.7 通から約 2.4 通へ，およそ 1/3 に減少した．昼間の迷惑メールが夜間ほど減少していないのは，throttling しか機能させていないことが原因であろう．

また，図 6 の結果より，夜間に受信した迷惑メールの数は，昼間のおよそ 1/6 であることがわかる．このことから，greylisting が迷惑メール対策として非常に有効であることが，あらためて確認できた．

なお，夜間においても受信している迷惑メールがゼロでないことは，greylisting と throttling の双方をすり抜けてくるものがあることを示している．この根本原因として支配的なものが，両対策が有効でない迷惑メールであるのか，それとも昼間に greylisting のデータベースにその発信元が登録された迷惑メールであるのかを判断するには，対外メールゲートウェイのログなどを精査する必要がある．

もちろん，今回提案した手法も，従来からの greylisting や throttling が効かない迷惑メールには無力である．そのような迷惑メールには，第三者中継機能を悪用された MTA を経由するものや，プロバイダなどから転送されてくるものがある．

以上の結果は，著者宛のメールについての結果である．次に，大阪府産技研全体での結果について考えてみる．メール利用者全員に対するヒアリングを行うなど，大規模な調査はまだ行っていないが，まずは MTA のログから調べることにした．

調査の対象には，大阪府産技研全体で受信しているメール数にほぼ等しいと考えることのできる，防火壁から所内メールゲートウェイに配送されたメール件数を選び，その変化を追いかけることにした．

図 7 に，対策実施前後である，2006 年 11 月 21 日から 2007 年 2 月 11 日までに，防火壁から所内メールゲートウェイに配送されたメールの件数の変化を示す．

なお，配送メール数がゼロとなっている日があるが，これは，電気設備の法定点検などのために停電となり，ネットワークをすべて止めたことが原因である．停電からの復帰後には，多くのメールが配送されている．これは送信元のメールスプールに保存されていたメールが配送されたためであると考えられる．

この図から，対策実施前は，1 日あたり約 3400 通のメールが，防火壁から所内メールゲートウェイに配送されていたことがわかる．そして，対策実施後は，その数がおよそ半分の約 1600 通に減少していることがわかる．

この減少分である約 1800 通が，適用時間を限定した greylisting と throttling によって配送が阻止できた迷惑メールの件数である予想できる．しかしながら，これについては，職員にヒアリングを行ったり，2 台の対外メールゲートウェイのログなどを精査する必要があるだろう．

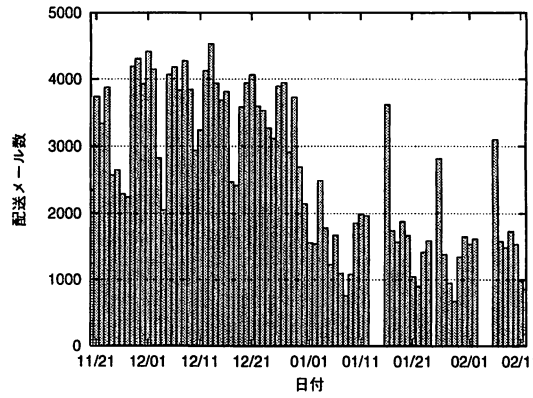

図 7　メール配送数の変化

受信したメールがこのように減少したため，所内メールゲートウェイで実施しているフィルタリングや，グループウェアサーバで実施しているウイルスチェックなどに要していたリソースも減少していると予想できる．これらについても，グループウェアサーバのログなどで検証する必要がある．

なお，以上の迷惑メール対策を導入してから，購読していたメールマガジンが配送されなくなったといった不具合については，現在のところ報告を受けていない．

5. まとめと今後の課題

本稿では，従来の greylisting が持つ問題点を解決する手法として，適用時間限定型の greylisting を提案した．

この手法では，メールの再送によって発生する遅配が好ましくない時間帯には，データベースへの登録のみを行う．その一方で，メールの遅配が問題とならない夜間には greylisting を適用して，迷惑メールを排除する．greylisting の適用時間を限定することによって，日中のメールの遅配についての問題を解決し，さらにデータベースのメンテナンスフリー化を実現した．

この適用時間限定型の greylisting では，昼間に送信されてくる迷惑メールには対処できないので，それについては throttling を併用することによって，効果は十分ではないかもしれないが，できるだけ迷惑メールを排除することを試みた．

そして，以上の 2 つの対策を 2007 年 1 月 4 日より実施し，対外メールゲートウェイで受信してしまう迷惑メールの数を，およそ 1/4 へと大幅に減少させることに成功した．また，その結果から，greylisting および throttling が，迷惑メール対策として非常に有効であることを再確認することができた．

今回提案した手法は，三交替制などで 24 時間仕事を続けている事業所や，夜遅くまで多くの学生や教員が活動している大学などにとっては，さほど有用でないかもしれない．しかし，そうではない事業所，特に中小事業者にとっては，対策がメールゲートウェイ 1 台だけで完結するため導入が容易であり，本手法を効果的に活用できるのではないかと期待している．

また，今回の適用時間限定型の greylisting では，曜日に関わりなく，朝 6 時から夜 21 時までであれば，そのままメール

を通過させることにしている．多くの事業所の勤務形態を考えると，週末のように出勤する職員が少ない曜日においては，greylisting を通過させる時間帯をしぼることが合理的であろう．大阪府産技研では，土日については，メールをそのまま通過させる時間帯を 11 時から 14 時までにしぼるという変更を加えた．今後，この変更の効果がどのよう効いてくるのか，さらに調査を続ける予定である．

そして，迷惑メール対策は，greylisting や throttling に限るものでない．今後，研究所全体でコンテンツフィルタリングを併用するなどして，迷惑メールに対するユーザの負担をさらに減らすことを検討している．

文　献

[1] 総務省, 平成 17 年度版 情報通信白書, ぎょうせい, Jun. 2006.

[2] 独立行政法人 情報処理推進機構, 情報セキュリティ読本 改訂版, 実教出版, Nov. 2006.

[3] 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, Vol. 2004, No. 96, pp. 19—24, Sep. 2004.

[4] 吉田 和幸, "throttling による spam メールの抑制について", 情報処理学会研究報告, Vol. 2005, No. 39, pp. 69—74, May 2005.

[5] 松原 義継, 只木 進一, "milter-greylist のための静的 whitelist 自動生成", 情報処理学会研究報告, Vol. 2006, No. 80, pp. 43—46, Jul. 2006.

[6] 山井 成良, 遠一平, 岡山 聖彦, 河野 圭太, 中村 素典, 丸山 伸, 宮下 卓也, "SMTP セッションの強制切断による spam メール対策手法", 情報科学技術レターズ, vol. 5, pp. 367—370, Aug. 2006.

[7] Kyle D. Dent, Postfix 実用ガイド, オライリー・ジャパン, Aug. 2004.

[8] 相馬 崇宏, 永井 謙芝, 大島 雅明, 小宮 由里子, 南 弘征, 高井 昌彰, 水田 正弘, "キャンパスネットワークにおける低コスト迷惑メール対策とその効果について", 情報処理学会研究報告, Vol. 2006, No. 42, pp. 1—6, May 2006.

[9] 平松 初珠, "PHP を用いたインターネット相談システムの構築", 大阪府立産業技術総合研究所テクニカルシート, No. 06006, Sep. 2006.

[10] ジェフ・モリガン, "Procmail", spam の撃退, pp. 95—133, ピアソン・エデュケーション, Dec. 1999.