情報処理学会論文誌　Vol. 51　No. 3　989–997 (Mar. 2010)

適用時間限定型 greylisting を用いた迷惑メール対策における配送遅延の改善

石島　悌[†1]　平松初珠[†1]　林　治尚[†2]

迷惑メール対策において重要なことは，単に迷惑メールの排除を図ることだけではなく，見落としてはならないメールを遅滞なく確実に配送することである．迷惑メールを排除する手法の 1 つに greylisting があるが，配送遅延の発生が問題となる．また，さほど大きくない組織においては，その対策にかける初期投資や人材の不足が課題となっている．本論文では，利用者がメールを利用しない時間帯にのみ greylisting を適用し，24 時間適用する throttling を併用する手法を提案する．これにより，メールの配送遅延や作業負担など，従来の greylisting がかかえる問題を軽減することが可能となる．提案方式に基づいたシステムを実際に運用した結果，迷惑メールのおよそ 7 割を排除することができた．また，2 年間にわたって本システムを運用してきたが，業務上問題となる配送遅延は発生せず，提案方式の有効性を確認することができた．

Reducing Delay of E-mail Delivery in Controlling Spam Mails Using Greylisting with Running Time Restriction

Dai Ishijima,[†1] Hatsumi Hiramatsu[†1] and Haruhisa Hayashi[†2]

In controlling spam mails, it is important not only to reduce spam mails, but also to deliver non-spam mails without delay. Greylisting is known as one of spam control methods, but it has problem with delay in e-mail delivery. Small and medium enterprises have problems with an initial investment and shortage of staff for controlling spam mails. In this paper, we propose a method combining greylisting running only during user absence and throttling running for all day. The proposed method resolves the problems with delay in e-mail delivery and work load. The result of operation based on this method shows that it is possible to reduce about 70% of spam mails. According to the operation experience over two years, we confirm that the problem has not occured in business with this method.

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や事業所，そして教育研究機関などで広く利用されており，我々の生活や社会活動になくてはならない存在となった[1)]．その中でも，電子メールはウェブとともにインターネットで最も普及しているサービスの 1 つである．

しかし，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 1 つが，迷惑メールの存在である[2)]．迷惑メールは，ネットワークの帯域やメールサーバの資源などを浪費するだけでなく，それを受け取ってしまったメール利用者にとっても大きな負担となっている．

このような状況においては，必要なメッセージを確実に受信者に配送するとともに，不要なメールをできるだけ排除し，利用者の負担を軽減することが，ネットワークやメールを運用するシステム管理者に求められている．

一方，中小規模の事業所[⋆1]は，情報システムに関する初期投資が負担であると感じており[3)]，既存の迷惑メール対策アプライアンスの導入に消極的な組織も多い．また，大学などの大きな組織と比較すると，その運用や管理に携わる人材が不足していることが課題となっている．ネットワークやメールシステムの安定した運用は組織規模の大小にかかわらず求められる．情報システムの管理や運用を他の業務と兼任していることの多い中小規模の事業所に対して，できるだけ経済的負担や作業負担をかけない迷惑メール対策が求められている．

迷惑メール対策として，さまざまな手法がこれまでに提案されてきた．このことは，迷惑メール対策には，決定的なものは存在しないことを示している．多くの迷惑メールを排除できる手法として，公開ブラックリストやコンテンツフィルタリングがある．その一方で，これらの手法では，通常のメールを迷惑メールとして判断してしまう誤検出（false positive）も多い．

メールの役割を，見落としてはならないメッセージを確実に配送すること，ととらえるのであれば，誤検出を減らすことが重要となる．メール利用者が個々にメーラ（MUA: Mail

†1 大阪府立産業技術総合研究所情報電子部
Information and Electronics Department, Technology Research Institute of Osaka Prefecture
†2 兵庫県立大学学術総合情報センター
Library and Academic Information Center, University of Hyogo
⋆1 文献 3) によると，中小企業とは，おおむね従業員数 300 人以下の企業をさす．

User Agent）で行うフィルタリングであれば，誤検出があっても，迷惑メールフォルダに自動分類されるだけであり，ユーザ自身で対策の不備を回避することが可能である．しかし，組織の受信メールゲートウェイにおける対策では，誤検出があると，受信者には回避する手段はない．このため，受信メールゲートウェイでの対策は，迷惑メールを通過させてしまう見逃し（false negative）をある程度許容せざるをえない．

誤検出が少なく，有効に機能する迷惑メール対策として，greylisting[4)–6)] が知られている．この手法は，迷惑メールを送信する MTA（Mail Transfer Agent）は再送を行わないという仮説に基づくものである．その一方で，greylisting には，再送にともなう配送遅延が発生するという問題がある．

迷惑メール対策の有無にかかわらず，メールの配送には遅延が発生することや，確実に配送がなされるという保証がないことは，多くのシステム管理者にとっては常識かもしれない．しかし，メールを送信すれば短時間のうちに相手に届くものと信じている利用者も多い．このため，greylisting の導入にあたっては，配送遅延をうまく回避することが求められる．

配送遅延の問題を避けるためには，greylisting の適用対象外とするための静的ホワイトリスト（無条件で受信を行う送信 MTA を登録したリスト）が必要となるが，これをメンテナンスし続けることはシステム管理者にとって大きな負担となる[7)]．

そこで，本論文では，中小規模の事業所を主たる対象として，greylisting がかかえる上記の問題を回避するための迷惑メール対策方式を提案する．本方式では，配送遅延が問題となる時間帯には greylisting の適用を除外し，それ以外の時間帯にのみ greylisting を適用する．これによって，迷惑メールの抑止効果は限定的にはなるものの，配送遅延の問題を解消することが可能となる．一方，greylisting が無効となる時間帯があるため，送信 MTA に対する応答に遅延をかける throttling[6),8),9)] を併用する．

以下，2 章では，従来の greylisting の問題点について議論し，3 章では，提案方式の概要，有効に活用できる組織，設計，実装，設定などの詳細を説明する．4 章では提案方式に基づいたシステムを 2 年間にわたって運用した結果を報告し，提案方式の有効性について評価する．

2. 従来の greylisting とその問題点

greylisting では，送信 MTA の IP アドレス，エンベロープ From アドレス，エンベロープ To アドレスの 3 つの情報とその MTA が送信を試みた時刻をデータベースに記録し，再送判定に用いる．もし，これらの情報がデータベースに記録されていないか，記録されていたとしても，過去に送信を試みた時刻と現在時刻の差が小さい場合，受信 MTA は一時エラーを返し，送信 MTA に再送を促す．このため，初めてメールを送ってきた送信元については，必ず配送遅延が発生する．

通常，MTA は 30 分以上の間隔をあけてから再送を試みる[10)]．一方，迷惑メールを送信する MTA は，一定時間内にどれだけ多くのメールを送信できるかというスループットを重視するため，再送を行わない場合が多い．このため多くの場合，greylisting は有効な迷惑メール排除の手法となる．すなわち，greylisting は，多少の配送遅延を許容する代わりに迷惑メールを排除する手法であるといえる．

また，大手プロバイダなどのように，MTA を複数台運用しているため再送のたびに異なる MTA が送信を試みるような場合には，そのつど一時エラーが返されることになる．メールマガジンなどでは，再送のたびにエンベロープ From が変化することもあり，この場合も一時エラーが返され，状況によってはメールが配送されないままとなる可能性もある．さらには，一部には spam 業者ではないのに再送を試みない MTA を運用している組織が存在する．

このような問題を避けるためには，静的ホワイトリストを用いて，それらの MTA を greylisting の処理対象外とする方法がある．しかし，このホワイトリストを随時更新する作業は，1 章で述べたような中小規模の組織にとっては負担が大きい．

以上のような問題点を解決する方法として，SMTP セッションを強制切断する方法が提案されている[11)]．この手法では，送信元 IP アドレス，エンベロープ From アドレス，エンベロープ To アドレス以外にメールヘッダ情報などを活用する．これにより，再送判定処理を改善し，上で述べた問題点を解決している．多くの場合，この手法は有効ではあるが，プライマリ MTA が SMTP セッションを強制切断した直後に，送信側が DNS（Domain Name System）の MX レコードを正しく参照して，セカンダリ MTA に再送を試みるという動作をとらなければ，やはり配送遅延が発生する．

3. 適用時間を限定した greylisting による迷惑メール対策方式

前章で述べたとおり，従来の greylisting には，配送遅延およびそれを防ぐためにホワイトリストの更新が必要となるという問題がある．そこで，本章では，これらの弱点を克服するために，greylisting の適用時間を限定する方式を提案する．

また，提案方式では，中小企業のように規模があまり大きくない組織においても導入が容易となるよう，1 台の MTA で処理が完結するなど，その実装が複雑化しないようにする．

そして，そのような組織においても対応可能な程度に，迷惑メール対策における作業負担を抑えることを目指す．より具体的には，他の業務を兼任している管理者が月に数時間程度しか作業を行えない，あるいは，システム管理を外部委託している場合は，契約業者が週に 1 度作業を行うだけのような組織でも対応が可能となることを目標とする．

3.1　提案方式の概要

配送遅延などの問題を解決する最も単純な方法は，その原因である greylisting を使わない，というものである．そこで，受信者の状態を考えて greylisting を使うかどうかを決定する．

メールの配送遅延は，受信者の立場から考えると，つねに避けるべきものであるとはいえない．たとえば，受信者がメールを読めない環境にいれば，配送遅延は何時間起こっても受信者はまったく困らない．配送遅延が問題となるのは，受信者がメールを読みたいときだけである．

そこで，提案方式では，greylisting の適用をメールの受信者が不在となる時間帯に限定する．ただし，greylisting を適用しない時間帯においては，迷惑メールを排除することができないため，throttling を併用し，こちらは 24 時間適用する．throttling もまた，迷惑メールを送信する MTA の特徴を利用した迷惑メール対策手法の 1 つである．

メールを読みたいときに配送遅延が発生することは，受信者にとって問題となるが，同時にこれは送信者にとっても問題である．それは，送信したいメールがいつまでも送信キューに滞留することである．従来の greylisting では，負荷分散などを目的として複数の送信 MTA を用いると，かえって滞留時間が延びる恐れがある．提案方式においては，greylisting を適用しない時間を十分な長さだけ確保し，このような状況を避けることにする．

3.2　提案方式が有効な組織

提案方式が有効となる組織は，メールの利用時間や場所が限定されている組織である．これには多くの企業をはじめとする事業所が該当する．

これらの事業所では，大学などと異なり，就業規則などによって業務時間が明確に定められている．メールの利用者が事業所にいるのは，この業務時間と，やはり就業規則などで上限が定められている残業時間中に限られる．これらの事業所では，業務時間に残業時間を加えた就業時間を越えて業務を行うこと，すなわち，メールを利用することは不可能である．

また，事業所によっては，業務にかかわる情報の適正な管理という観点からも，業務によって得られた情報の持ち出しとなるメールの外部への転送や外部からのメールの閲覧を許可していないところがある．

以上のように，就業時間内にその事業所においてのみメールの利用を許可している組織において，提案方式は有効に利用することが可能である．

ウェブやメールがインターネットのサービスとして定着するにつれ，それらはいつでも利用可能な業務上のコミュニケーション手段として認識されつつある．メールについていえば，電話や FAX などと同じような感覚で使われることも増え，業務上の取り引きなどにも活発に使われている．そのような企業においては，メールの配送遅延は営業上の損失に直結している．その損失は，提案方式に要する負担より大きくなる．

メールの配送遅延が業務上の損失となるのであれば，greylisting を 24 時間適用することは不可能である．ホワイトリストを用いれば，greylisting の適用を避けることは可能であるが，ホワイトリストを事前に整備しておくことはできない．多くの組織ではメールの送信者をあらかじめ知っておくことができないからである．

1 章で述べたように，中小規模の事業所においては，情報システムに対する初期費用や運用時の管理作業が負担であると感じているところが多い．このような事業所は，たとえその効果が大きくても，高価なシステムや運用時に継続的に管理作業が発生するシステムを導入することに消極的である．提案方式は既存の MTA に後述の設定を加えるだけで導入でき，このような中小規模の事業所において特に有用である．さらに，提案方式は単純であるがゆえに，このような事業所においても，その管理作業は大きな負担とならない．

3.3　提案方式の設計

提案方式では，従来の greylisting の処理に**図 1** の破線内の条件分岐を 1 つ追加する．これにより，受信者がメールを読める状態では，メールを単純に通過させ，配送遅延の問題を回避することができる．従来方法からの変更点はこの 1 つだけであり，さまざまな greylisting の実装に容易に追加することができる．さらに，単純な機構であるがゆえに，この変更が不具合を引きおこす可能性を小さくすることができる．

throttling は，MTA に用意されている機能をそのまま用いる．こちらは greylisting とは異なり，24 時間適用する．

3.4　提案方式の実装

前節で述べた設計方針に基づき，実装を行った．本実装では，受信 MTA として Postfix [12] を用い，greylisting には，Postfix に付属している greylist.pl に図 1 の処理を追加したものを用いる．greylisting を適用する時間帯かどうかを判断する条件は，greylist.pl の内部に

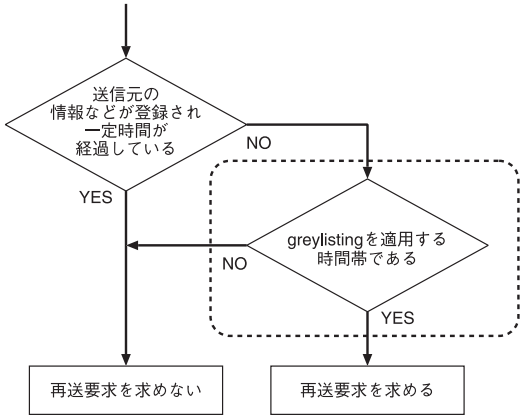


図 1　greylisting に追加した処理
Fig. 1　Processing flow of the proposed method.

直接記述せず，外部ファイルの存在によることにする[*1]．このファイルはプログラムのスケジュール実行を管理する cron を用いて生成・消去する．これによって，適用時間の変更を柔軟に行える．

greylist.pl は，greylisting の最も単純な実装の 1 つであり，送信 MTA の IP アドレスや送受信者エンベロープアドレスなどの履歴情報を蓄積するデータベースは，放置しておくとサイズが大きくなり続けるという問題がある．このため，適当なタイミングでデータベースから古い情報を削除するか，データベースを削除する必要がある．データベースから履歴情報が失われると配送遅延の発生が懸念される．

本実装では，greylisting の適用を除外する時間帯にデータベースを削除する．古い情報の削除ではなく，データベースの削除を選択したのは，処理の単純化のためである．このような単純な削除を選択しても，greylisting の適用を除外している時間帯であるため，配送遅延は発生しない．これにより，greylist.pl に必要不可欠なデータベースの管理作業は不要となる．

本実装で用いた Postfix においては，バージョン 2.3 以降において送信 MTA に対する応答に遅延をかけることができるようになった．SMTP セッションが確立し，グリーティングバナーと呼ばれる「`220 hostname…`」の応答メッセージを送信する直前や，「`RCPT To:`」コマンドに対する応答を送るときに，応答遅延をかけることができる．

throttling で設定する項目は，これらの 2 つ，あるいはいずれかの応答を送信する際の遅延時間だけである．この遅延時間に大きな値を指定すると，送信 MTA とのコネクションが確立されたままになり，MTA のリソースを消費してしまう．また，迷惑メール送信元でない MTA 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，迷惑メールを送ってくると思われる送信 MTA には長い遅延時間を，そうでないと思われる送信 MTA には短い遅延時間を設定する．

3.5　提案方式の設定

提案方式における各種設定は，これを利用する組織の状況に合わせて決定する必要がある．

著者らの属する大阪府立産業技術総合研究所では，多くのメール利用者の動静が 3.2 節の内容に該当する．また，同節で述べた中小規模の事業所を支援する立場でもあり，以下に提案方式の実践例として，その設定を紹介する．

当研究所では，業務時間は 9 時から 17 時 45 分までであり，通勤に利用する公共交通機関である路線バスは，朝 7 時 30 分から 21 時までの間しか運行していない．そこで，21 時から翌朝 6 時までの間にのみ greylisting を適用し，6 時から 21 時までは適用を除外することとした．7 時 30 分ではなく 6 時からとしたのは，配送遅延が生じても 90 分の余裕を見込んでおけば再送されると予想したからである．

また，通常，週末に出勤する職員はいないので，greylisting の適用を除外する時間帯は，土曜日，日曜日については 11 時から 14 時までの間だけとすることにした．

greylist.pl が用いるデータベースは，greylisting の適用時間外であればいつ削除してもよいが，毎週月曜の朝 8 時に行うこととした．greylist.pl が再送を求める判断基準となる最小再送間隔時間は 600 秒とした．

迷惑メールを送ってくる送信 MTA は，IP アドレスからドメイン名（FQDN: Fully Qualified Domain Name）を解決できないことが多いとの報告がなされている[13]．このことは，これまでの経験からも分かっていた．そこで，throttling については，たとえば**図 2** のように，送信 MTA に応じて待ち時間を変えるように設定した．

本実装で用いた Postfix では，待ち時間を「送信 MTA sleep 秒単位の遅延時間」という形式で指定する．送信 MTA の指定には正規表現を使うことができる（この機能は正規表現テーブルと呼ばれている）．図 2 の例は，ドメイン名を解決できない送信 MTA には 35

⋆1 ファイル`/var/mta/greylist.pass`が存在し，長さが 0 でなければ，greylisting の適用を除外する．

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

図 2　正規表現テーブルを用いた throttling 設定例
Fig. 2　Example of regular expression table for throttling.

秒，ADSL や FTTH などで接続し，プロバイダの正規の MTA を経由しない送信 MTA には 20 秒，それ以外のすべての送信 MTA については 1 秒遅延をかけるというものである．なお，実際に使用しているルールでは，送信 MTA をもう少し細かく分類している．

4. 提案方式の評価

前章で説明した提案方式に基づくシステムの運用を，2007 年 1 月より開始した．なお，導入から 3 カ月の間は，greylisting の適用時間や throttling の設定などの微調整を行った．前章で述べた設定で運用を始めたのは 2007 年 4 月に入ってからである．本章では，MTA のメール配送状況，受信者に対するアンケート，著者宛に到着した迷惑メールの件数で，提案方式の評価を行う．

4.1 メール配送状況による評価

提案方式の導入によって，メールの配送状況にどのような変化があったかを調べた．その期間は，導入の 1 年前である 2006 年 1 月から，導入して 2 年が経過した 2008 年 12 月までである．この期間のプライマリ MTA のログから，1 日あたりの SMTP 接続数，メール配送数，およびそれらの比であるメール配送率を 1 カ月単位で示したものが**図 3** である．

提案方式導入以前の 1 年間では，SMTP 接続回数は 746,478 回であり，570,445 通のメールが配送されている．導入後の 2 年間では，それぞれ，SMTP 接続回数は 3,304,862 回，メール配送数は 814,340 通である．なお，この SMTP 接続回数は，MTA のログをそのまま数えたものである．greylisting によって一時拒否され，再接続を行った回数も含まれる．

提案方式の導入以前は，メール配送数は SMTP 接続数に近い値を示しており，メール配送率（配送数/接続数）は 76.4%であった．メール配送数が SMTP 接続数より小さいのは，エンベロープ From のドメイン部が DNS で解決できない場合や受信者アドレスが存在しない場合，あるいは第三者中継を試みた場合に配送を拒否しているからである．

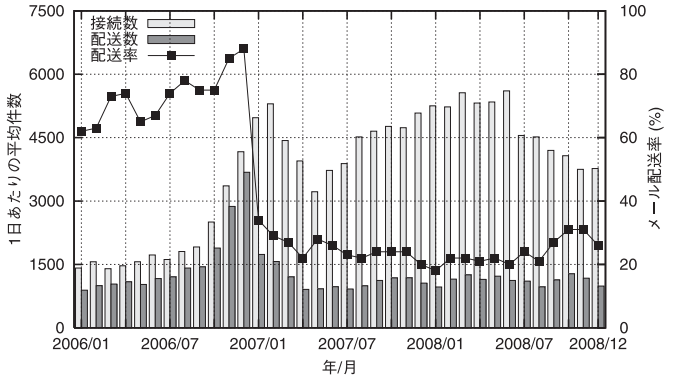


図 3　SMTP 接続数，配送数，配送率の経時変化
Fig. 3　The number of SMTP connections, delivered mails and delivery rate.

対策導入後は，SMTP 接続数とメール配送数に大きな差が見られ，配送率は 24.6%[⋆1]に低下した．総務省がまとめた資料[14] によると，全メールトラヒックに占める迷惑メールの割合は 75%となっており，配送率が約 25%となっていることはこれと矛盾しない．

提案システムが安定運用に移行した 2007 年 4 月以降の SMTP 接続数の 1 日あたりの平均値は 4,587 回であり，メール配送数の平均は 1 日あたり 1,093 通である．安定運用へ移行する際に，greylisting のログを詳細に記録するようにした．これにより，greylisting により一時拒否され，再接続を行った回数も得られるようになった．この平均値は 1 日あたり 227 回である．

以上のことから，SMTP 接続数から再接続回数を引いた値（4,360）とメール配送数の差である約 3,300 が排除できた迷惑メール件数の 1 つの目安となる．

ただし，提案方式導入以前においても，メールの配送率は 100%ではなかったため，提案方式によって排除できた迷惑メールは，$(4{,}587 - 227) \times 0.764 - 1{,}093 = 2{,}238$ 通と見積もるのが妥当である．この場合，迷惑メールを排除できた割合は，67.2%（$= 2{,}238/((4{,}587 - 227) \times 0.764)$）となる．

4.2 アンケートによる評価

提案方式によって，メールの配送遅延などの問題がないかどうかを調べるため，メール利

⋆1 後述する再接続回数が安定運用の前後で変化していないとすれば，25.9%になる．

表 1　迷惑メール対策の効果
Table 1　Result of questionnair survey.

対策前の迷惑	迷惑メールの減少					
メール受信数	1/10	1/3	少し	不変	増えた	計
1 日 10 通以上	3	7	5	2	0	17
1 日 1 通以上	2	3	3	2	0	10
週 1 通以上	0	0	1	1	0	2
月 1 通以上	0	0	1	2	0	3
なし	0	0	0	9	0	9
合計人数	5	10	10	16	0	41

用者を対象として，アンケート調査を 2007 年 6 月に行った．

アンケートの回答はメール利用者のおよそ 1/4 にあたる 41 人より得ることができた．なお，提案方式の導入にあたって，導入前に迷惑メールの件数をあらかじめ把握しておくためのアンケート調査を行わなかったこと，導入から半年の時間を経過していることなどから，必ずしも正確な情報が得られたわけではない．

アンケートでは以下の項目について質問した．

- 対策前の迷惑メール受信数
- 対策による迷惑メール減少の程度
- 不具合の有無

迷惑メールの受信数については，「毎日 100 通以上・毎日 10 通以上・毎日 1 通以上・毎週 1 通以上・毎月 1 通以上・受信なし」を選択肢とした．回収結果では，毎日 100 通以上迷惑メールを受信していたと回答した利用者はいなかった．

迷惑メール対策の効果については，「1/10 以下に減少した・1/3 以下に減少した・少し減少した・変化なし・増えた」を選択肢とした．これに関する調査結果を**表 1** に示す．増えたという回答を選んだ利用者はいなかった．

表 1 から，多くの迷惑メールを受信していた利用者ほど，その効果を感じていることが分かる．逆に，受信していた迷惑メールの数が元々少なければ，その効果を感じることも少ないだろう．

迷惑メールが減少していないと回答している利用者は 16 人いるが，そのうち 9 人は迷惑メールを受信しておらず，実質的に効果がないと答えているのは 7 人である．すなわち，本対策の効果を実感しているのは，迷惑メールを受信していた 32 人中 25 人のおよそ 8 割である．1/10 以下，1/3 以下に減少したと回答している利用者は 15 人であり，利用者の約半数は，本対策で効果が出ていると評価している．

不具合の有無については，

- メーリングリストなどの到着順が入れ替わる
- メールマガジンなどが届かなくなった
- 特定のアドレスからのメールが届かなくなった
- 業務時間内にメールがすぐに届かない
- 業務時間外にメールがすぐに届かない
- その他（自由記述）

についてたずねたが，アンケート調査時においては，不具合があると答えた利用者は皆無であった．greylisting によってメールの配送遅延が発生したり，再送を行わない MTA によりメールが配送されなくなったりすることが懸念されたが，アンケート調査時においては，そのような不具合がないことが分かった．

アンケート集計後，特定のプロバイダから夜間に送信されたメールが配送遅延するという報告が，提案システム導入から 10 カ月後の 2007 年 10 月 1 日に寄せられた．ただし，この配送遅延は業務上の問題となるものではなかった．

このプロバイダは再送間隔が 3 時間を超えていたため，3.5 節で述べた greylisting の適用時間設定では，配送遅延の問題を回避することができなかった．そこで，このプロバイダの送信 MTA を静的ホワイトリストに登録することにした．それ以降，配送遅延や配送もれなど不具合の報告はなく，本実装における設定の調整は，throttling の待ち時間を 2007 年に 3 回，2008 年に 2 回修正したのみである．

4.3　著者宛に届く迷惑メール件数の変化

MTA のログやアンケートから，迷惑メール受信数の変化の概略をつかむことができたが，迷惑メールの変化を正確には把握できないので，第 1 著者宛に届いた迷惑メールの数の経時変化を調査した．その結果を**図 4**，**図 5** に示す．

図 4 は，図 3 同様に，対策導入前の 1 年間と導入後の 2 年間における 1 日あたりの迷惑メール受信件数を月ごとに示したものである．この期間に受信した迷惑メールの総数は 52,984 通であり，対策導入前の 1 年間では 31,484 通，導入後の 2 年間では 21,500 通である．迷惑メールの 1 日あたりの平均受信数は，導入前は 86.3 通であったが，導入後は 29.7 通へと 65.6%減少した．

4.1 節で述べたプライマリ MTA でのメール総受信数と比較してみると，対策導入前は，総受信数（570,445）に占める著者宛の迷惑メールの割合は 5.47%であった．提案方式の導

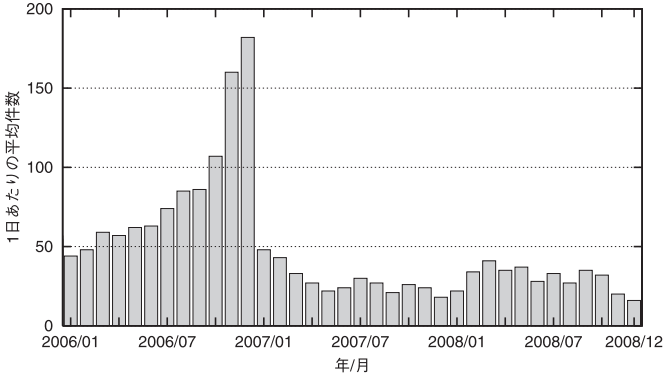


図 4　著者宛に届いた迷惑メール件数の変化
Fig. 4　The number of spam mails for author.

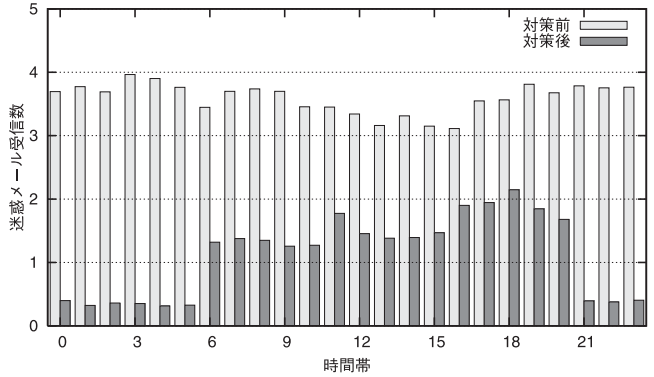


図 5　時間帯ごとの迷惑メール受信数の変化
Fig. 5　The number of spam mails in every hour.

入によって 2.64%（21,500/814,340）へと半分以下に減少している．

図 5 は，対策導入前 2006 年 1 月から 12 月までの 1 年間と，安定運用開始後の 2007 年 4 月から 2008 年 3 月までの 1 年間の時間帯ごとの迷惑メール受信件数を比較したものである．対策導入前は，1 時間あたり平均 3.59 通の迷惑メールを受信していたが，導入後は 1.12 通に減少している．

greylisting を適用していない 6 時から 21 時までの時間帯では，3.48 通から 1.57 通へと減少している．このことより，throttling によって，受信する迷惑メールは半分以下になったことが分かる．

greylisting を適用している 21 時から翌朝 6 時までに限ると，3.80 通から 0.36 通へとほぼ 1/10 へ大幅に減少していることが分かる．これは，greylisting と throttling の併用によって，受信する迷惑メールの件数は 1/10 となったことを意味している．

greylisting を適用している時間帯と throttling しか適用していない時間帯では，受信した迷惑メールの件数におよそ 5 倍の開きがある．このことは，迷惑メールの抑止効果については，greylisting がより有効であることを示している．夜間に適用している greylisting によって，職場から離れる時間帯（18 時から翌朝 9 時）に届く迷惑メールが，提案方式導入以前と比較して約 1/4 へと減少した．出勤時にチェックしなければならないメールの数が減り，負担が大きく軽減された．

4.4　配送遅延および配送もれに関する考察

提案方式によるシステムは，現在まで 2 年間運用した．メールの配送遅延は 4.2 節で述べた再送間隔が長いプロバイダの 1 件のみであった．配送もれの指摘はなかった．その他業務に支障をきたす問題は発生していない．

これは，業務時間とその前後には greylisting を適用せず，メールをそのまま通過させていることが有効に作用しているからであると考えられる．当研究所の利用者をはじめとするメール送信者は，深夜など，業務時間外にメールを送信することが少ないのであろう．メール送信者が 3.2 節で述べたような組織であり，メールを利用する時間帯が 6 時から 21 時までであれば，配送遅延および再送を行わない MTA による配送もれは，本実装では発生する恐れはない．

4.4.1　greylisting の適用時間

本実装では，greylisting の適用時間を平日は 21 時から翌朝 6 時までの 9 時間としている．これは，当研究所の勤務形態をもとに決定したものである．勤務時間が異なる環境では，適用時間を変更する必要がある．また，三交替制などで，つねに利用者が存在するためにメールの配送遅延が許されない環境では，当然のことながら，提案方式を利用することは不可能である．

図 5 から，greylisting を適用している時間帯では，到着する迷惑メールの件数をおよそ 1/10 に，適用していない時間帯ではおよそ 1/2 にすることができていることが分かる．も

し，適用時間を短くすれば，迷惑メールの阻止率は下がり，多くの迷惑メールが届くことが予想される．逆に，適用時間を長くすれば，より迷惑メールの数を減らすことが可能となる．たとえば，適用時間を 18 時から翌朝 9 時までの 15 時間とすれば，迷惑メールのおよそ 75%を排除できる計算になる．しかし，適用時間を長くすることは，配送遅延の増加を招く可能性がある．実際の導入現場にふさわしい適用時間の選定が必要となるだろう．

4.4.2　thottling による配送遅延

本実装では，朝 6 時から夜 21 時までの 15 時間を greylisting の適用対象外としている．この時間帯は greylisting による迷惑メールの排除を望めないため，throttling を併用することにしたが，throttling が配送遅延の原因となることも予測される．

本実装で利用している Postfix では，特に設定を行わなければ，SMTP セッションの最大数は 100 に制限されている．図 2 のような throttling を設定した場合，仮に IP アドレスからドメイン名を解決できない MTA からの接続が 0.3 秒に 1 回ずつあった場合，34 秒後には SMTP のセッション数が制限を超えてしまう．この状態で，迷惑メールの送信元でない MTA が接続を試みても，Postfix は接続数を超えているという応答を返し，配送遅延が発生してしまう．

幸いなことに，現状ではそのような状況にはなっていないが，受信するメールが多い組織では，負荷分散など[15] 何らかの対処が必要となってくる．

4.4.3　メーラによる並べ替え

アンケート調査では，メールの到着順序が入れ替わったという回答はなかったが，実際には配送遅延により到着順序が入れ替わった可能性がないとはいえない．これは，メーラがメールの一覧をリスト表示する際に，到着した順序ではなく，メールヘッダの Date フィールドで並べ替えを行う場合があるからである．

このような並べ替えがメーラ側で行われている場合，利用者が離席中に到着したメールについては，メールの配送遅延には気づかないことになる．しかし，これは 3.1 節で述べた配送遅延が問題とならないケースに該当するため，実運用上は問題にならない．

4.5　導入および運用時における作業負担に関する考察

これまでに述べたように，提案方式は，実装の簡単さと導入の容易さ，そして，安定運用へ移行した後のメンテナンスが大きな負担とならないこと目指して開発したものである．筆者らの組織での提案方式実施事例では，安定運用開始後に再送間隔が 3 時間を超えるプロバイダのホワイトリストへの登録や throttling の待ち時間調整を数度行った．メンテナンス作業は発生したが，1 章で述べた中小規模の事業所でも対応が可能な範囲にすることができた．

もし，本実装に基づくシステムを他の事業所などに導入する場合は，現状の設定をそのまま移すだけですむ．導入後には，当研究所で行った，greylisting の適用対象外とするためのホワイトリストの追加や，throttling の待ち時間調整が必要となるかもしれない．これらの作業がどの程度となるのかについては，当研究所が支援の対象としている中小規模の事業者への導入を通じて明らかにしたい．

受信者の立場からは，夜間に到着する迷惑メールが greylisting によって減少したため，始業時にメールをチェックする際の負担が軽減された．業務時間中は，greylisting が無効となっているものの，throttling により，迷惑メールは提案方式の導入により半分程度となった．

当研究所における提案方式の導入後，2008 年度に迷惑メールの自動分類機能を持つメーラを導入したため，受信者の負担はさらに減少した．メーラの迷惑メール分類機能では，見逃しや誤検知により，受信者の意図に沿うように分類できないこともある．しかし，仮に分類機能に不備があったとしても，提案方式により迷惑メールの総数が減少しているので，そのチェックの負担は，提案方式を導入しない場合より軽減される．実際に，分類機能に見逃しや誤検知あるとの報告があったが，それによる苦情は寄せられていない．

5. むすび

本論文では，従来の greylisting の問題点であった，配送遅延に対処するため，greylisting の適用時間を限定する方式を提案した．また，greylisting が適用されない時間帯に到着する迷惑メールを減少させるため，throttling を併用することとした．

提案方式に基づくシステムの実運用を 2 年間実施した．その結果，配送もれや，業務に支障をきたす配送遅延などの問題は発生しないことが分かった．また，提案方式の運用が安定してからは，設定変更を数回しか行っておらず，迷惑メール対策の省力化を実現することができた．この程度の作業であれば，1 章で述べたような中小規模の事業所でも十分対応可能である．

そして，提案方式で用いた greylisting と throttling は迷惑メール対策として有用であることを再確認した．メールログの解析から迷惑メールの 67.2%を排除できたことが分かり，著者宛に届く迷惑メールの件数は 65.6%減少した．

今後の課題として，提案方式を他の組織でも運用し，運用時の設定修正作業がどの程度になるのか，そして，迷惑メールの抑止効果がどの程度になるのかを調査することがあげられる．特に導入前後で迷惑メールの受信件数の変化を組織全体で集計し，効果の検証を

より精度良く行う必要があるだろう．また，Postfix 以外の MTA や greylisting の別の実装（Postgrey [16] など）でも同様の効果が得られるかどうかを調査する必要がある．

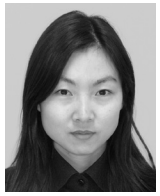
参 考 文 献

1) 総務省（編）：平成 20 年度版情報通信白書，ぎょうせい (2008).
2) ジェフ・モリガン：spam の撃退，ピアソン・エデュケーション (1999).
3) 中小企業庁（編）：2009 年度版中小企業白書，ぎょうせい (2009).
4) Harris, E.: The Next Step in the Spam Control War: Greylisting (online). http://projects.puremagic.com/greylisting/whitepaper.html (accessed 2009-09-23)
5) 吉田和幸：greylisting による spam メールの抑制について，情報処理学会分散システム/インターネット運用技術研究会研究報告，No.2004-DSM-35, pp.19–24 (2004).
6) 鈴木常彦：ブロッキング，スロットリング，情報処理，Vol.46, No.7, pp.754–757 (2005).
7) 松原義継，只木進一：milter-greylist のための静的 whitelist 自動生成，情報処理学会分散システム/インターネット運用技術研究会研究報告，No.2006-DSM-42, pp.43–46 (2006).
8) Woolridge, D., Law, J. and Kawasaki, M.: Spam throttling for qmail (online). http://spamthrottle.qmail.ca/ (accessed 2009-09-23)
9) 吉田和幸：throttling による spam メールの抑制の効果について，情報処理学会分散システム/インターネット運用技術研究会研究報告，No.2005-DSM-37, pp.69–74 (2005).
10) Klensin, J.: Simple Mail Transfer Protocol, RFC 5321, IETF (2008).
11) 山井成良，岡山聖彦，中村素典，清家　巧，漣　一平，河野圭太，宮下卓也：SMTP セッションの強制切断による spam メール対策，情報処理学会論文誌，Vol.50, No.3, pp.940–949 (2009).
12) Dent, K.D.: Postfix 実用ガイド，オライリー・ジャパン (2004).
13) 長谷川明生，山口榮作，鈴木常彦：迷惑メールの解析，情報科学技術フォーラム情報科学技術レターズ，Vol.6, pp.377–378 (2007).
14) 総務省迷惑メールへの対応の在り方に関する研究会：迷惑メールの現状と対策について（オンライン）(2007). http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/mail_ken/pdf/070822_2_2.pdf
15) 三原槙仁，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，情報処理学会分散システム/インターネット運用技術研究会研究報告，No.2007-DSM-72, pp.43–48 (2007).
16) Schweikert, D.: Postgrey – Postfix Greylisting Policy Server (online). http://postgrey.schweikert.ch/ (accessed 2009-02-22)

(平成 21 年 6 月 15 日受付)
(平成 21 年 12 月 17 日採録)

石島　悌（正会員）

1989 年京都工芸繊維大学工芸学部電気工学科卒業．1995 年同大学大学院工芸科学研究科博士後期課程修了．同年大阪府立産業技術総合研究所入所．電子工学ならびに情報通信分野での企業支援と研究業務に従事．現在，同研究所情報電子部主任研究員．プラズマ・核融合学会，日本物理学会，軽金属学会各会員．博士（学術）．



平松　初珠（正会員）

1999 年大阪府立大学工学部電気電子システム工学科卒業．2001 年東京工業大学大学院理工学研究科修士課程修了．2005 年大阪府立技術総合研究所入所．企業支援および研究業務，所内ネットワークの設計管理運用に従事．現在，同研究所情報電子部研究員．工学修士．

林　　治尚（正会員）

1989 年京都大学工学部工業化学科卒業．1995 年同大学大学院工学研究科分子工学専攻博士後期課程修了．同年姫路工業大学工学部応用化学科助手．大学統合にともない 2004 年より兵庫県立大学学術総合情報センター助教授（現・准教授）．計算物理化学，分子シミュレーション，情報セキュリティ，ネットワークシステムの研究に従事．日本化学会，日本コンピュータ化学会（理事），分子シミュレーション研究会各会員．博士（工学）．