適用時間を限定したgreylistingの透過型プロキシを用いた実装と評価

石島 悌[†1] 平松初珠[†1] 中井 亮[†2]

中小規模の事業者の多くは，情報通信ネットワークに関する初期投資が負担であることや，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であると認識している．しかし，電子メールをはじめとするネットワーク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．特に電子メールにおいては，迷惑メールを排除し，必要なメールを遅滞なく確実に配送することが求められている．そこで，本論文では適用時間を限定したgreylistingによる迷惑メール対策手法を廉価なPCに透過型プロキシとして実装することを提案する．これにより，導入にかかる負担が低下し，運用や管理も容易となる．およそ半年にわたる運用の結果，この方式は中小規模の事業者にとって負担が少なく，また迷惑メール対策手法として有効であることを確認することができた．

Implementation and Evaluation of Transparent Proxy for Greylisting Applied for a few Hours in a Day

Dai Ishijima,[†1] Hatsumi Hiramatsu[†1] and Ryo Nakai[†2]

Many small and medium-sized enterprises have problems with initial cost and shortage of staff for network system. However, stable operation of network system including e-mail is required, regardless of size of the enterprise. Especially in e-mail system, it is required to reduce spam mails and to deliver non-spam mails without delay. In this paper, we propose an implementation of tranparent proxy on low-cost PC for greylisting applied for a few hours in a day. It is expected that it reduces initial cost and easy to operate and manage. According to the operation result for half a year, we confirm that the proposed method is less stress for small and medium-sized enterprises and it is effective for controlling spam mails.

1. はじめに

電子メールはWebに次いでインターネットで広く利用されているサービスである[1]．企業や教育研究機関など，さまざまな組織になくてはならないコミュニケーション手段として定着しているが，迷惑メールに悩まされている利用者も多い．統計によれば，主要大手4社ISPが受信するメールのうち，およそ3/4は迷惑メールであるといわれている[2]．

中小規模の事業者においては，情報通信ネットワークに関する初期投資が負担であると感じている組織が多い．また，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[3]．

著者らはこれまでに，特に中小の事業者が運営するサイトにおいて，導入時および運用・管理において大きな負担をかけることなく受信メールゲートウェイの段階で迷惑メールを拒否する方式を提案してきた[4]．この方式の特徴は，メールの利用者が不在となる時間帯にのみ限定してgreylisting[5),6)]を適用することである．これによって，greylistingで問題となるメールの遅配が利用者には意識されず，また，greylistingで必要となるデータベースなどの管理作業を大きく軽減することが可能となる．

しかし，この提案方式においても，初期設定などの導入時における負担は発生する．そのため，専任のスタッフを確保することが困難な事業者においては，その負担が問題となっている．また，提案方式を用いたシステムにおいて何らかのトラブルが発生した場合，その切り分けが困難であることも，中小の事業者が提案方式による対策の導入をためらう一因となっている．

そこで，この提案方式を廉価なPCに透過型プロキシとして実装することによって，中小規模の事業者が抱える上述の課題を解決することを試みる．これにより，導入時および運用・管理にかかる負担を抑えるこ

†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 財団法人 大阪市都市型産業振興センター
Osaka Urban Industry Promotion Center

とができる．また，既存の受信 MTA（Mail Transfer Agent）をはじめとするネットワークシステム全体に大きな変更を加える必要もなく，障害発生時の原因の切り分けも非常に容易となる．

本論文では，2 章において上記提案手法について述べ，3 章では提案手法を透過型プロキシとして実装する方法を説明する．4 章では 3 章で説明したシステムの大阪産業創造館への導入について説明し，5 章ではその有効性を評価する．

2. 適用時間を限定した greylisting による迷惑メール対策

greylisting は，迷惑メールを送信してくる MTA は再送を行わないという仮説に基づく対策手法である．多くの場合，この仮説は正しく，それゆえ greylisting は迷惑メール対策手法として有用であるといわれている．

一方，greylisting は，メールを初めて受信したとき，送信元 MTA に対して再送を求めるため，その場合はメールの遅配が生じる．また，再送を求めるかどうかを判定するために，送信元 MTA の IP アドレス，送信者エンベロープ From アドレス，受信者アドレス，送信時刻といった情報をデータベースに記録する必要がある．遅配が好ましくない状況においては，greylisting の適用を回避するためのホワイトリストに送信元の情報を登録する作業が必要になる．

電子メールの送信者があらかじめ特定されている組織でなければ，greylisting の適用を回避させるべき MTA を知っておくことは困難である．それゆえ，一般的にはホワイトリストを事前に整備しておくことは困難である．このため，ホワイトリストへの登録作業は，受信者や送信者がメールの遅配に気づいてからとなる．つまり，ホワイトリストへの登録は，その組織の MTA 管理者の作業負担となるだけでなく，結果として，メールの利用者である組織内の受信者と組織外の送信者の利便性を損ねている．

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配の恐れがあることや，そもそも確実にメールの配送が行わ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，現在では，多くの組織でメールは電話や FAX などと同等に扱われ，送ったらすぐに相手先に届くものと信じている利用者も多い．そのような利用者や組織にとっては，メールの遅配は業務における時間の損失，あるいビジネスチャンスの取り逃しと認識されてしまう．

しかし，メールの遅配はいついかなるときでも避けるべき事象ではなく，メールの利用者が不在の場合には，遅配は問題とならない．

そこで，著者らは利用者が不在となる時間帯にのみ greylisting を用いる，適用時間を限定した greylisting

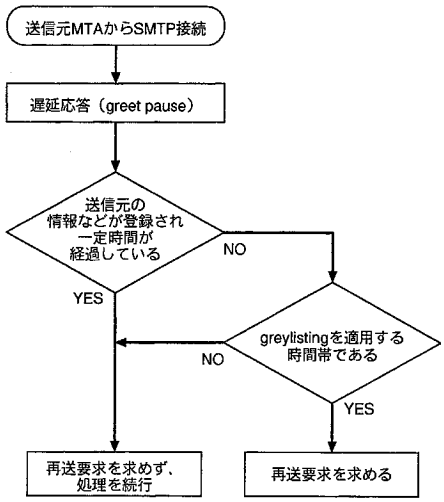

図 1　提案手法の概略

による迷惑メール対策手法を提案した．この手法では，利用者がメールを読み書きする時間帯では，greylisting を適用しない．その時間帯では，再送要求による遅配は発生せず，送信 MTA が再送を行わないことによる配送もれも発生しない．これにより，ホワイトリストの登録作業を基本的に放棄することが可能となる．

実際には，greylisting を適用している時間帯に送信されるメールもあり，再送間隔が数時間以上に設定されている MTA や再送を行わない MTA もごくまれに存在するため，そのような MTA のみをホワイトリストに登録する必要がある．

また，greylisting の適用を除外している時間帯にデータベースを空にすることができるため，放置しておくと容量が増大し続けるデータベースの管理も省略することが可能となる．

そして，greylisting の適用を除外している時間帯においては，できるだけ迷惑メールの受信を避けるため，送信元 MTA に対する応答に遅延をかける throttling（greet pause）[7),8)] を併用することにした．この提案手法の概略を図 1 に示す．

この提案手法は，業務時間が深夜に及ばない組織にとって非常に有用である．また，企業では大学などと異なり，就業規則などによって，時間外の業務を原則として禁止しているところが多い．また，業務にかかわる情報の適正な管理という観点からも，業務上知りえた情報の持ちだしとなる，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組織が多い．つまり，業務時間外には事実上メールへのアクセスはできない．

このような組織においては，業務時間外に到着する迷惑メールを減少させることは，業務効率の改善につながる．業務時間外に到着する迷惑メールが減少する

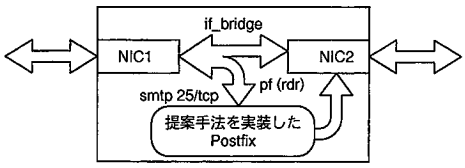

図 2　透過プロキシとしての実装

ことは，始業時に利用者がメールをチェックする際の負担を軽減できるからである．業務時間内には greylisting が無効であるため，迷惑メールが届く件数は，有効である時間帯とくらべ増加するが，それは逐次処理を行えばよい．

この提案手法により，大阪府立産業技術総合研究所では，受信する迷惑メールを受信 MTA においておよそ 1/4 に削減することが可能となった．

3. 提案手法の透過型プロキシを用いた実装

前述の提案手法は，既存の MTA 対して greylisting と throttling に関するいくつかの設定を加えるだけで実現できる．これまでに，Postfix や sendmail といった MTA の設定した経験があれば，提案手法を導入することはさほど困難なことではない．

一方，1 章で述べたとおり，中小規模の事業者においては，そのような経験を持った人材を確保することは難しい．また，MTA をはじめとして，ネットワークシステム全体の導入から運用・管理を外部に委託していることも多い．

このような場合には，提案手法の導入に関する設定は，委託に関する契約の範疇を越える場合があり，提案手法の導入が困難となる場合がある．特に，提案手法に起因する可能性のあるトラブルが仮に発生した場合の原因の切り分けや，責任の所在の明確化が問題となることが多い．

そこで，これらの問題を回避しつつ，専任の管理者がいない組織においても容易に導入できるように，提案手法を透過型プロキシとして実装した．本システムの概要を図 **2** に示す．

図 2 のように，本システムは 2 つのネットワークインターフェイスカード NIC1 と NIC2 を装備した PC を用い，これらのインターフェイスをブリッジとして動作させる．本システムの IP アドレスは NIC2 にのみ割り当てる．そして，パケットフィルタによって，NIC1 から NIC2 に（図 2 で左から右に）向かう SMTP トラフィックを，この PC で動作する MTA にリダイレクトする．本システムは，OS に FreeBSD 6.2R を，ブリッジとリダイレクト用のパケットフィルタには，それぞれ，OS に搭載されている if_bridge[9] と pf[10] を用いた．また，MTA には Postfix を用いた．

本システムでは，図 2 を左から右に通過しようとする SMTP トラフィックは，その宛先 IP アドレスがパケットフィルタによって，本システムの NIC2 の IP アドレスにリダイレクトされる．このとき，このトラフィックは NAT テーブルの対応表に記録される．NIC2 を発 IP アドレスとして持つトラフィックのうち，NAT テーブルの対応表に記録されているものは，発 IP アドレスが対応表のものに置き換えられる．以上の仕組みにより，NIC1 の左から NIC2 の右に通過する SMTP トラフィックは本システムが処理することとなる．本システムの左に位置する送信 MTA は，本システムの右に位置する元々の受信 MTA と本システムの区別がつかない．

以上のように，本システムはその右側に接続している MTA のプロキシとして動作する．本システムの MTA において greylisting と throttling を使うことにより，既存の MTA の設定を変更せずに，迷惑メールを拒否することが可能となる．

本システムを右から左に通過するトラフィックと SMTP 以外のトラフィックについては，パケットフィルタによるリダイレクトの対象とならず，単純にブリッジにより，片方の NIC からもう片方へそのまま通過する．

本システムはウェブキャッシュにおける squid のインラインプロキシとほぼ同等の構成である[11),12)]．squid によるウェブキャッシュと異なる点は，squid が組織の内部から外部へ向かう HTTP（80/tcp）トラフィックをウェブキャッシュの squid（3128/tcp）にリダイレクトするのに対して，本システムでは既存の MTA 向けの SMTP（25/tcp）トラフィックを本システムの MTA にリダイレクトすることである．

本システムの構成は，既存の市販されている迷惑メールアプライアンスと大きな違いはない．しかし，廉価な PC と無償のソフトウェアで構成されているため，導入についての負担はより小さい．本システムは，既存のアプライアンスを導入するほどのコストをかけたくない組織向けのものである．

4. 大阪産業創造館への提案システムの導入

大阪産業創造館は，中小・ベンチャー企業の支援拠点であり，大阪市経済局の外郭団体である財団法人大阪市都市型産業振興センターが運営している[13)]．経営相談をはじめ，セミナーやビジネススクールなどの中小・ベンチャー企業支援サービスを行っている．

大阪産業創造館の従業員数はおよそ 80 人であり，ここまでに述べた中小規模の事業者に該当する．また，その業務形態やメールの利用状況から，提案手法に基づく迷惑メール対策が有効であると考えられた．

本章では，まず，大阪産業創造館のネットワークについて説明し，次に，提案システムの導入について述べる．

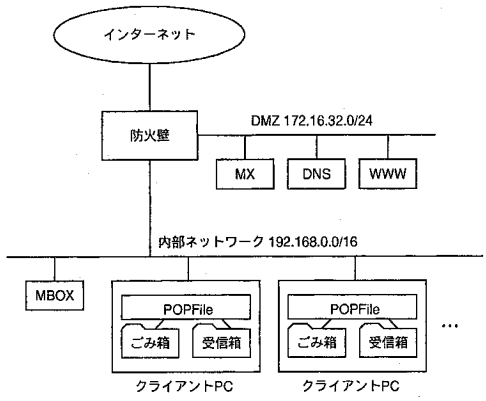

図 3　大阪産業創造館のネットワーク概略図

4.1　大阪産業創造館のネットワーク

大阪産業創造館のネットワーク概略図を図 3 に示す．なお，図 3 に示した IP アドレスは実際のものとは異なる．

大阪産業創造館では，外部に公開しているネットワークである DMZ にネームサーバ（DNS），ウェブサーバ（WWW），対外送受信メールサーバ（MX）を配置している．館内の内部ネットワークには，職員が直接利用するメールサーバ（MBOX）が配置されている．

外部からメールを受信する際には，MX がメールを受け取り，このときにウイルスチェックが行われる．添付ファイルなどがウイルスに感染している場合，そのメールは破棄される．そうでないメールは，内部ネットワークの MBOX に配送される．MBOX に配送されたメールには，館内のクライアント PC からアクセスする．

職員が用いるクライアント PC には，メールクライアント（MUA: Mail User Agent）として EdMax[14] が導入されており，迷惑メールの分別に POPFile[15] を用いている．受信したメールが POPFile により迷惑メールと判定された場合，そのメールはごみ箱フォルダに保存される．

メールを外部に送信する場合は，受信時の逆の経路が使われる．クライアント PC から MBOX にメールが送信され，MBOX から DMZ の MX に配送される．MX ではインターネットからの受信時と同様にウイルスチェックが行われ，ウイルスに感染していないメールだけが外部に送信される．

4.2　大阪産業創造館における迷惑メールの問題

大阪産業創造館においては，前節で述べたように，迷惑メールを各クライアントパソコンで動作する POPFile により分別している．このため，多くの場合，利用者は受信箱に到着するメールだけをチェックしていればよい．

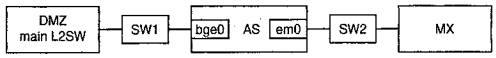

図 4　提案システムの接続図

しかし，他のフィルタリングソフトと同様に，POPFile においても見逃しにより迷惑メールが受信箱に分別されることがある．また，誤検知により，迷惑メールでないものがごみ箱フォルダに紛れ込んでしまうことがある．

受信する迷惑メールの件数が少なければ，フィルタリングソフトの見逃しや誤検知によって，間違った分別がなされる恐れは少ない．しかし，迷惑メールが増えてくると，見逃しや誤検知も増加し，メール利用者の利便性を大きく損ねてしまうことがある．

これらの問題を回避するため，対外 MTA である MX に 2 章で説明した提案手法を導入する，あるいは既存の迷惑メールアプライアンスを導入することが検討された．しかし，前者はネットワークの運用・管理に関する業務委託の都合上見送られることとなった．後者のアプライアンスの導入についても，予算など，諸事情により困難であることから見送られた．

4.3　提案システムの導入

迷惑メール対策アプライアンスに代わるものとして，提案手法に基づくシステムの導入が検討された．本システムについての運用・管理の責任は，業務委託には含まれず，大阪産業創造館が持つという条件で導入が決定した．

本システム（AS）は，図 4 のように，DMZ のメインスイッチと MX の間に，2 つのスイッチ（SW1, SW2）を介して割り込ませる形で接続した．メインスイッチと MX の間にそのまま本システムを配置せず，SW1, SW2 を配置したのは，LAN ケーブル配線の簡略化と次節で述べるトラブル発生時の切り離しを容易にするためである．

本システムに用いた PC の構成を表 1 に示す．文献 4) で示した大阪府立産業技術総合研究所における迷惑メール対策と，本システムの大きな違いは，透過プロキシとして実装したことを除けば，以下の 2 点である．

- Greylisting ポリシーサーバに Postgrey[16] を用いている
- 適用時間が 24 時から翌朝 6 時までである

なお，Postgrey には，時間帯によって greylisting の適用を除外するよう，そのプログラムに修正を加えた．

この 2 点以外の項目，たとえば throttling による遅延時間の設定などは，文献 4) で用いた値をそのまま流用した．これは，条件をできるだけ揃えておき，異なる組織で提案手法を運用した結果に差がでるかを調べるためである．

Postgrey には，メールの遅配をできるだけ避けるために，

- 複数回メールの配送に成功した送信 MTA をホワイトリストに自動登録する
- 送信 MTA の IP アドレスの下位 8 ビットを無視する

といった機能が用意されているが，これらは利用しなかった．また，Postgrey が利用するデータベースは週に一度リセットすることにしたため，Postgrey にあらかじめ用意されているデータベースから古いエントリを自動的に削除する機能も使っていない．

MX に向かう SMTP トラフィックをリダイレクト[17]するパケットフィルタの設定を図 5 に示す．パケットフィルタのルールは，上から順に評価して適用される．3 行目と 4 行目の「no rdr」の設定は，それぞれ，館内ネットワークおよび DMZ からの SMTP トラフィックを本システムで処理せず，そのまま MX に渡すための設定である．5 行目の「rdr」で始まる行は，それ以外，すなわちインターネットから MX に到達する SMTP トラフィックを本システムへリダイレクトする設定である．SMTP 以外のトラフィックと，MX からインターネットあるいは館内ネットワークへ（図 4 で右から左に）向かうトラフィックは，ブリッジ機能によってそのまま本システムを通過する．

本システムは，大阪産業創造館の全館停電および設備点検日である 2009 年 2 月 22 日に導入した．必要な設定は，事前に行ったヒアリングを元に大阪府立産業技術総合研究所であらかじめ済ませておき，導入日に図 4 の接続を行った．

大阪産業創造館において，本システム導入のために行った作業は以下のとおりである．

- 本システム用の IP アドレスを割り当てる
- MX において IP 転送を可能とする
- 本システムの情報を DNS に登録する（正引き，逆引きの両方）

4.4 障害発生時の切り離し

本システムは透過型プロキシとして動作しているため，障害発生時には，図 6 のようにネットワークケーブルの接続を変更することにって容易に切り離すことができる．この際，スイッチが学習している MAC アドレステーブルの情報を破棄することが望ましいため，切り離し手順は次のようになる．

(1) MX と SW2 を接続しているケーブルの SW2 側を抜く
(2) そのケーブルを SW1 の空きポートに接続する
(3) SW1 の電源を切る
(4) SW1 の電源を再投入する

もし，SW1 を使わずに，DMZ のメインスイッチと本システムや MX を直接接続している場合は，スイッチが学習した MAC アドレステーブル情報を消すために，DMZ のメインスイッチをリセットするといった動作が必要となる．DMZ のメインスイッチには，4.1 節で述べたように，MX 以外にネームサーバやウェブ

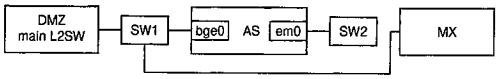

図 6 トラブル発生時の切り離し

サーバが接続されている．これらのサーバの接続性を確保するためには，DMZ のメインスイッチをリセットすることは好ましくない．メール以外のシステムに影響を与えないためはに，SW1 を独立させておくことが必要である．

障害復旧の際に，本システムを再び接続するときの手順は，次のようになる．

(1) MX と SW1 を接続しているケーブルの SW1 側を抜く
(2) そのケーブルを SW2 の空きポートに接続する
(3) SW1 の電源を切る
(4) SW1 の電源を再投入する

2009 年 2 月に本システムの運用を開始したのち，3 月に本システムが停止し，実際にシステムの切り離しを行った．システム停止の原因は，Postfix 付属の greylist.pl のデータベースが壊れてしまったことによる．このトラブルの後，Greylisting ポリシーサーバをより堅牢な Postgrey に置き換えた．その後，トラブルは発生せず，接続変更は行っていない．

4.5 後方散乱の防止

大阪産業創造館では，本システムの導入以前でも，実在するアカウントへのメール配送か，実在しないアカウントへの配送かの判断を MBOX で行っていた．つまり，本システムや MX は，存在しないアカウント宛のメールであってもそのまま処理を続行し，受信したメールは全て MBOX に配送される．

メールが MBOX に配送された時点において，その宛先が実在するかどうかが判定され，もし，存在しないアカウント宛のメールであれば，MBOX がバウンスメールをエンベロープ From で示されたアドレスに送信する．これは，後方散乱メールの配送に悪用される恐れがある．

これを防ぐためには，参考文献 18) で示されるような，受信メールゲートウェイにおける後方散乱メールの防止対策をとるか，存在しないアドレス宛のメールに対するバウンスメールを送信しないという措置をとる必要がある．

前者の対策は根本的な解決であるが，現状ではその対策を選択することはできなかった．また，後者の措置をとると，宛先をタイプミスするなどした悪意のない送信者に対してエラーを通知することができなくなる．

この問題に対する妥協案として，本システムにおいて，大阪産業創造館のアカウント発行ルールに適合しない宛先に対するメールを受信拒否する設定を追加した．具体的には図 7 のように，メールアカントのロー

表 1　透過プロキシシステムのハードウェア・ソフトウェア構成

項目	形式・仕様
PC 本体	DELL OptiPlex 330
CPU	Intel Core2Duo E4600 2.4GHz
RAM	1GB
NIC1	Broadcom BCM5754/5758 GbE Adaptor (on board, bge0)
NIC2	Intel Pro/1000 Network Connection (PCI Express, em0)
OS	FreeBSD 6.2R
透過プロキシ	pf（OS 付属），if_bridge（OS 付属）
MTA	Postfix-2.4.9
ポリシーサーバ	Postgrey-1.27（導入当初は Postfix 付属の greylist.pl）
適用時間	24:00—06:00

```
right_if="em0"
left_if="bge0"
no rdr on $left_if proto tcp from 172.16.32.0/16 to any port 25
no rdr on $left_if proto tcp from 192.168.1.0/24 to any port 25
rdr on $left_if proto tcp from any to any port 25 -> ($right_if) port 25
pass in all
pass out all
```

図 5　パケットフィルタの設定

カルパートが英数字で始まらないもの，そして，ローカルパートが英数字で終わらないものを受信拒否するようにした．この設定は，2009 年 7 月 21 日に追加した．

5. 迷惑メール対策の評価

本システムの有用性を評価するため，メール利用者に対してアンケート調査とログの解析を行った．本章ではこれらの調査結果をまとめる．

5.1 利用者アンケートによる評価

迷惑メール対策の効果に関する利用者アンケートを 2009 年 5 月に行った．アンケートの対象者は大阪産業創造館のメール利用者 77 名であり，そのうち 68 名から回答を得ることができた．回収率は 88.3%である．

アンケート項目は以下のとおりである．

- 対策前の迷惑メール受信件数
- 対策後の迷惑メール受信件数
- 対策の効果を感じたか
- 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．**表 2** に本システム導入前後における迷惑メール受信数の変化を示す．この表から，毎日 100 通以上迷惑メールを受信する利用者が 30 人から 6 人へと大きく減少していることがわかる．

毎日 10 通以上・毎日 1 通以上・毎週 1 通以上になったと回答した利用者は，対策導入後に増えているが，これはより多くの迷惑メールを受信していた利用者が減ったことに起因すると考えられる．

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 3** に示す．

表 3 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わかる．迷惑メールが減ったと感じている利用者は 44 人で，これは利用者の 64%である．迷惑メールが増えたと感じている利用者は 1 人であるが，この利用者は元々迷惑メールを受信していない．

本システム導入にともなう不具合については，その不具合の有無を選択してもらった．不具合があったを選択した場合は，さらにその具体例として，メーリングリストなどの到着順が入れ替わる・いままで購読していたメールマガジンなどが届かなくなった・業務時間内にメールがすぐに届かないことがある・業務時間外にメールがすぐに届かないことがある・その他，を選択してもらうことにした．

その結果，不具合がないと答えた利用者は 66 人であり，不具合があると答えた利用者は 2 人だった．不具合があると答えた利用者は，いずれもその不具合として，その他を選んでおり，業務に関するメールが迷惑メールとしてはじかれた，と回答していた．この回答者は，本システムと POPFile による分別を混同しているようである．アンケートを用意する際に，本システムによる対策と POPFile によるメールの分別が簡単に区別できるように，設問を工夫すべきだったか

```
/^[^A-Za-z0-9].*@sansokan.jp$/          550 User unknown
/[^A-Za-z0-9]@sansokan.jp$/             550 User unknown
```

図 7　受信拒否設定

表 2　迷惑メール受信数の変化

迷惑メール受信数	対策前	対策後
毎日 100 通以上	30	6
毎日 10 通以上	17	34
毎日 1 通以上	5	10
毎週 1 通以上	1	3
毎月 1 通以上	1	1
受信していない	14	14

表 3　迷惑メール対策の効果

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
毎日 100 通以上	16	13	1	0	0	30
毎日 10 通以上	3	6	1	7	0	17
毎日 1 通以上	0	2	0	3	0	5
毎週 1 通以上	0	1	0	0	0	1
毎月 1 通以上	0	0	0	1	0	1
受信していない	1	0	0	12	1	14
合計人数	20	22	2	23	1	68

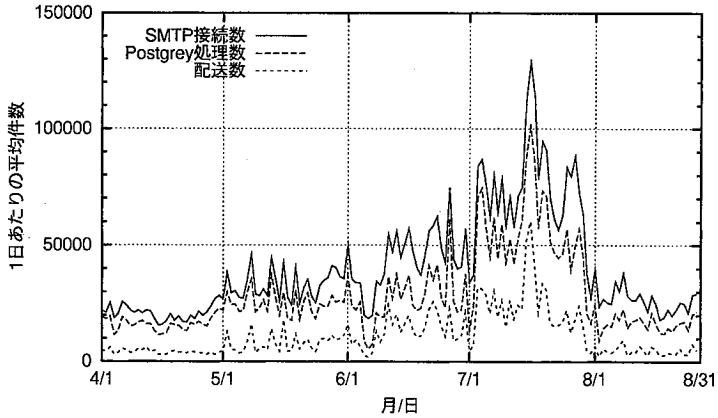

図 8　SMTP 接続数，Postgrey 処理数，配送数の経時変化

もしれない．

5.2　システムのログ解析による評価

本システムにおける greylisting と throttling の効果を検証するために，メールログから SMTP 接続回数，Postgrey 処理件数，配送メール数の変化を調べた．図 8 に 2009 年 4 月から 2009 年 8 月末までの結果を示す．

本システムにおいて，どれだけの迷惑メールを排除することができたかを示すためには，大阪産業創造館において受け取るはずであった迷惑メールの件数を正確に把握する必要がある．そして，実際に受け取ってしまった迷惑メールの件数と比較しなければならない．しかし，受け取るはずであった迷惑メールの件数を実際に得ることは困難である．そこで，その代用として，SMTP 接続回数を用い，これが受け取るはずであった迷惑メールの件数と，迷惑メール以外のメールの合計にほぼ一致するものとして議論を進める．

Postgrey の処理件数は，SMTP 接続後の throttling による遅延処理をかけたあとも，送信元 MTA が処理を続行した件数を表している．これは，図 8 の期間において，SMTP 接続数のおよそ 70%程度であり，throttling によって，約 30%の迷惑メールが排除できたと推測できる．

実際に配送されたメールの数は，SMTP 接続数のおよそ 27%であり，大阪府立産業技術総合研究所における提案手法とほぼ同等の効果が得られていることがわかる．

Postgrey の処理件数は配送されたメールの数の約 2.5 倍となっているが，このことは，throttling だけでは十分に迷惑メールを排除できていないことを示している．24 時間ずっと適用している throttling と比較すると，greylisting はその 1/4 にあたる夜間の 6 時間しか適用していないが，迷惑メールの排除には後者がより有効であることを示している．

6. おわりに

本論文では，著者らが運用してきた，適用時間を限定した greylisting による迷惑メール対策手法の透過型プロキシによる実装を紹介し，その運用結果を報告した．

およそ半年にわたる，大阪産業創造館における本システムの運用の結果，メール利用者が受信する迷惑メールの量を 1/4 程度に減らすことができた．この結果は，greylisting や throttling が迷惑メール対策として有効であることを示している．また，その効果は，大阪府立産業技術総合研究所で得られたものと大きな差はなかった．

本システムは，迷惑メール対策アプライアンスの導入が困難であったり，専任のネットワーク管理者を配置することが難しい中小規模の事業者における利用を想定したものである．本システムは MTA をはじめとする既存のネットワークの設定を大幅に変更することなく簡単に導入することができ，また，トラブル発生時の切り離しも容易である．

今後，府内の中小企業をはじめとする事業者への本システムの普及を図りたい．

参考文献

1) 総務省編：平成 21 年度版 情報通信白書, ぎょうせい, (2009).
2) 総務省編：迷惑メールへの対応の在り方に関する研究会 最終とりまとめ, p.12, (2008).
3) 中小企業庁編：中小企業白書 2008 年度版, ぎょうせい, (2008).
4) 石島 悌, 平松 初珠, 林 治尚, “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”, 情報処理学会研究報告, Vol.2007, No.38, pp.89—94, (2007).
5) Evan Harris: “The Next Step in the Spam Control War: Greylisting”, http://projects.puremagic.com/greylisting/whitepaper.html
6) 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, (2004).
7) Sendmail Consortium: Sendmail 8.13.0, http://www.sendmail.org/releases/8.13.0
8) 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, (2005).
9) http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/network-bridging.html
10) http://www.openbsd.org/faq/pf/index.html
11) http://www.squid-cache.org/
12) Transparent proxying with squid and pf, http://www.benzedrine.cx/transquid.html
13) 大阪産業創造館とは?, http://www.sansokan.jp/about/
14) EdMax インターネットメーラー, http://www.edcom.jp/edmaxtop.html
15) POPFile - Automatic Email Classification, http://getpopfile.org/docs/
16) Postgrey - Postfix Greylisting Policy Server, http://postgrey.schweikert.ch/
17) http://www.openbsd.org/faq/pf/rdr.html
18) 桝田 秀夫, 落合 優：“メールゲートウェイにおけるバウンスメール発生の抑制法とその評価”, 情報科学技術レターズ, Vol.6, pp.369—372.