milter manager による低配送遅延を目指した spam 対策メールサーバの設計とその運用結果

金髙一[†]　松井一乃[††]　池部実[††]　吉田和幸[†††]

現在，spam 対策手法として，メール送信サーバの挙動を検査する対策手法である greylisting や throttling が広く用いられている．しかし，これらの対策手法は通常メールの受信にも遅延を強いる．本研究では，milter manager を用いて SPF，S25R に spam と判断された場合にのみ，検出率は高いが遅延が大きい greylisting を適用することにした．これにより，現在の spam 対策システムより少ない spam 対策でメールを処理することができ，メール受信までの遅延低減へとつながる．本システムを 1 カ月運用した結果，従来のシステムと比べ greylisting の適用割合を 54.0%から 39.7%へ削減．また，受信した通常メールに対する配送遅延を従来のシステムから改善することができた．

Design of Low Delivery Delay for Antispam System Using Milter Manager and Its Operational Results

HAJIME KANETAKA[†]　KAZUNO MATSUI[††]
MINORU IKEBE[††]　KAZUYUKI YOSHIDA[†††]

There are many anti-spam techniques. However, there is not the perfect technique. For example, the greylisting is high detection rate. But, it is time consuming for mail retransmission. Therefore, we use some anti-spam techniques with using its advantages and covering its weaknesses. We design an anti-spam system using the milter manager. We are aim to reduce mail delivery delays. Our system applies to the greylisting spam mails that are determined only by S25R and SPF. In our system's operational results, we confirmed the reduction in rate of applicable of the greylisting from 54.0% to 39.7%. Moreover,previous our system has been reduced from the system to the mail delivery delays.

1. はじめに

インターネットの急速な発展と普及に伴い，電子メールを始めとするネットワークを介したコミュニケーションは必要不可欠となっている．電子メールは通常の郵便と比べると，送信者側が容易に大量のメッセージを送信でき，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小さい．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．

システム管理者が大量の spam から被害を防ぐ方法として，複数の spam 対策手法を同時に利用することが一般的である．

大分大学学術情報拠点情報基盤センターでは，spam 対策のためのメールゲートウェイを導入し，送受信するメールについてさまざまな spam 対策を行い，運用してきた[1][2][3]．メールゲートウェイでは，受信を許可する MTA(Mail Transfer Agent)の IP アドレスを記述した whitelist を参照し，whitelist に記述がある MTA からのメールには少数の spam 対策のみを行い，whitelist に記述がない MTA からのメールであれば多重の spam 対策を行ってきた．これにより，whitelist に記述がある MTA からのメールは，spam 対策手法による配送遅延を受けずに受信することができるが，通常メールであるが whitelist に記述がない MTA からのメールは，すべての spam 対策手法が適用されるため，各 spam 対策手法による配送遅延により，メールの受信までに時間がかかる問題があった．そこで本研究では，milter manager[4]を用いて複数の spam 対策手法を組み合わせてシステムを改良する．我々のシステムでは，配送遅延が少ないが誤検出が多い対策手法で spam と判定した場合のみ，配送遅延が大きいが誤検出，検出漏れが少ない spam 対策手法を行うことでメールに対する配送遅延を削減し，効果的に spam の排除を目指す．

本論文の構成は以下の通りである．まず，2 章で既存の spam 対策手法について述べ，3 章で大分大学で運用してきた従来のシステムの問題点を述べる．4 章では milter manager を用いて低配送遅延を目指した spam

† 大分大学大学院工学研究科知能情報システム工学専攻
Course of Computer Science and Intelligent Systems, Graduate School of Engineering, Oita University
†† 大分大学工学部知能情報システム工学科
Department of Computer Science and Intelligent Systems, Faculty of Engineering, 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

対策メールサーバシステムの設計について述べる．5章で本システムの運用結果及び考察を述べ，最後に6章でまとめと今後の課題を述べる．

2. 既存の spam 対策手法

様々な spam 対策手法がこれまで提案されてきた．spam 対策手法にはそれぞれ長所・短所がある．そのため，spam 対策手法を組み合わせることにより様々な種類の spam を検出できる．2.1~2.8 節では大分大学で利用している spam 対策手法を中心に，2.9 節ではその他の spam 対策手法，2.10 節では spam 対策における関連研究について説明する．

2.1 コンテンツフィルタリング

SpamAssassin[5]に代表されるコンテンツフィルタリングは広く利用されている[6]．コンテンツフィルタリングはメールの内容から spam 判定する．そのため，spam に特徴的なメールの内容かどうかをチェックするため，メールサーバに与える負荷は後述する他の spam 対策手法と比べて大きい．そして，spam が多様化していくにつれて，フィルタリングルールが肥大化する傾向にある．また，検出率を上げるためには大量の spam による学習が必要である．

2.2 greylisting

greylisting[7]は「spam 送信 MTA は再送をしない」との仮説に基づき，一時的に受信を拒否し，送信元 MTA から再送された場合，メールを受信する spam 対策手法である．図 1 に大分大学における spam 対策別の検出数を示す．greylisting による検出数が全体の 70%以上を占めており，高い効果を挙げている(調査期間 2011 年 7 月 31 日~8 月 20 日)．ただし，greylisting は配送遅延が大きく，通常メールの送信元 MTA にも再送を強いる．さらに，greylisting による再送では，再送されたメールであることを確認するために，送信元 MTA の IP アドレス，送受信メールアドレス，最初のメール受付時刻を保持する必要がある．

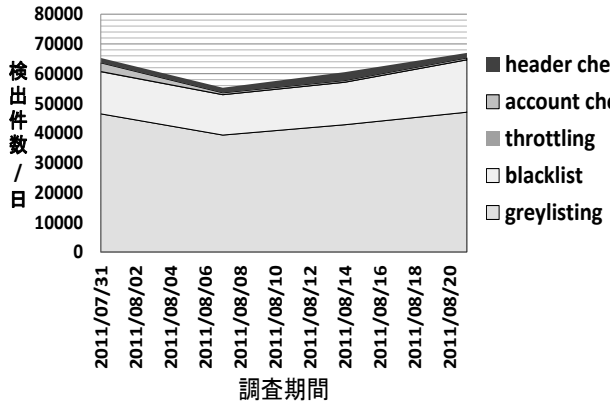

図 1　大分大学における spam 検出数の内訳

2.3 throttling

throttling[8]は「spam 送信 MTA は timeout が短い」，「spam 送信 MTA は SMTP の確認応答手順を無視してメールを送る」との仮説に基づき，コネクション確立後の応答を遅延することで，spam 送信 MTA がこちらの応答を無視してメールを配送するか，メールの配送をあきらめて接続を切断することを期待する spam 対策手法である．throttling では必要なパラメータは遅延時間のみであり，容易に設定できる．また，再送かどうかの判定が不要なので greylisting より適用範囲が広く，配送遅延も greylisting と比べると数十秒と非常に小さい．しかし，throttling は TCP コネクションを保持した状態で待つため，プロセス数，TCP セッション数が増えやすい問題がある．

2.4 S25R

ボットに感染したエンドユーザコンピュータから送信される spam が増加傾向にある[10]．通常メールは，ISP(Internet Service Provider)や組織の中継 MTA を経由して送信されるのに対し，ボットから送信される spam は，ボットに感染したエンドユーザコンピュータ自身が中継 MTA となり直接送信する．S25R(Selective SMTP Rejection)[11]は IP アドレスの逆引きで得られる FQDN(Fully Qualified Domain Name)の特徴に注目し，SMTP[12]アクセスしてきたクライアントが中継 MTA かボットに感染したエンドユーザコンピュータかを識別する．その結果，ボットに感染したエンドユーザコンピュータからのメールであれば，spam と判断し受信を拒否する．

2.5 SPF

SPF(Sender Policy Framework)[13]は，SMTP によるメールの送受信において送信者のドメインの偽称を防ぎ，正当性を検証する送信ドメイン認証方式である．SPF はメールを受信時に，送信者であるメールアドレス(エンベロープ送信者）のドメインから送信されたものかどうかを確認することで spam 判定する．

送信側はあらかじめ自ドメインの権威 DNS サーバ上に，自ドメインでメール送信を許可する MTA を特定する SPF レコードを登録する．

図 2 に示した SPF レコードの例は，example.jp ドメインにおける MTA の IP アドレスが 192.168.100.0/24 に存在することを意味している．~all は，192.168.100.0/24 以外の IP アドレスを持つ MTA から送信された場合においても，メールを拒否すべきではないことを意味する(softfail)．また，-all と記述されていた場合，192.168.100.0/24 以外の IP アドレスを持つ MTA から送信された example.jp ドメインのメールは，ドメインを詐称して送信されている可能性が高いため，メールを拒否すべきであることを意味する(fail)．

受信者はメール受信時，送信者として指定されたメールアドレスのドメイン部分に示されるドメインの SPF レコードを送信者のドメインの権威 DNS サーバへ問い合わせて，SMTP 接続先の IP アドレスが取得した SPF レコードと一致するか確認することで，送信ドメインの認証を実施する(図 3)．

```
example.jp.  IN TXT " v=spf1 +ip4:192.168.100.0/24 ~all"
```

図 2　SPF レコードの例

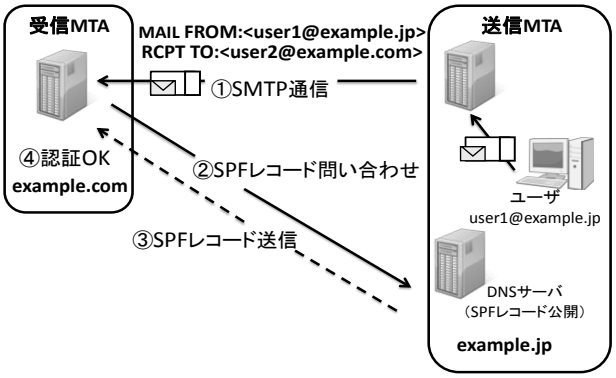

図 3　SPF を用いた送信ドメイン認証の流れ

2.6　whitelist

MTA の中には，これまで述べた spam 対策を適用した場合，spam 送信 MTA として誤検出される MTA も存在する．誤検出される MTA から送信されるメールを受信するために whitelist を利用する．信頼できる MTA の IP アドレスを whitelist に記述することで，その信頼できる MTA から送信されるメールには spam 対策を省略し，通常メールのほとんどを即座に受信できる．

それに加えて，通常 MTA が greylisting や throttling などの，配送処理に時間がかかる spam 対策手法によって spam 送信 MTA と判断されたとき，次回送信時に再びこれらの spam 対策手法が適用されることを防ぐために whitelist を利用する．

これまでには，greylisting によって動的に作成される auto-whitelist[14]から件数の多い送信元を管理者が選び, MTA のドメイン名と送信元メールアドレスのドメイン部分が一致することを確認した後，whitelist に自動で追加登録するシステムを開発し，大分大学のメールシステムに適用してきた[15].

2.7　blacklist

blacklist とは，spam に関連する MTA の IP アドレスをリスト化したものであり，SMTP アクセスにおける TCP コネクション開始時に利用する対策である．blacklist に登録されている IP アドレスからのアクセスを拒否することで，spam の受信を拒否する．現在，広く利用されている blacklist として Spamhaus の DNSBL がある．

2.8　header check，account check

spam はメールヘッダが不完全であることが多く，header check では，このヘッダ形式を調べることで spam 判定する．大分大学では Message-ID：，From：各ヘッダの形式が<ローカル部@ドメイン部>の形式になっていないメールを拒否する．

account check では，大分大学に送られてき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る[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．これにより，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 MTA で廃棄される．

2.9　その他の spam 対策手法

この他のよく利用される対策手法として，ここでは DKIM(DomainKeys Identified Mail)[16]と OP25B(Outbound Port 25 Blocking)[17]について述べる．

DKIM は電子署名を用いた送信ドメイン認証技術である．対して，2.5 節で述べた SPF は IP アドレスを用いた送信ドメイン認証技術である．

DKIM では，送信側はあらかじめ自ドメインを管理する DNS サーバを使用して, 署名に利用する公開鍵を公開する．公開鍵は，図 4 に示すように FQDN に対する TXT レコードとして登録する．図 4 は，example.jp が登録した公開鍵であることを意味している．次に送信側では，メールのヘッダ及びボディを基に図 5 に示すように電子署名を作成し, それを DKIM-Signature ヘッダとして電子メールに付加する．

受信側はメール受信時，送信者のドメインの DNS サーバに公開鍵を問い合わせ，取得した公開鍵から電子署名を照合する方法で送信者のドメインを認証する．メッセージのヘッダや本文を元に電子署名を作成するため，中継 MTA などで電子署名または電子署名の元になった電子メールのデータが変更されなければ，メールが転送された場合においても転送先で認証が可能になる(図 6).

```
sls.dkim._domainkey.example.jp.  IN TXT  "v=DKIM1; k=rsa;
t=y; p=MIGfMA0GCSqGSIb3...<省略>"
```

図 4　公開鍵のレコードの例

```
DKIM-Signature: a=rsa-sha1; c=nowsp/nowsp; d=sm-test.com; s=tls.dkim;
    t=1138613234; h=X-DomainKeys:DomainKey-Signature:Mime-Version:
    Content-Type:Message-Id:Content-Transfer-Encoding:Cc:From:Subject:
    Date:To:X-Mailer:X-ok-sendmail.com;
    b=B+TTx8CgkswOZf6vVbkxPuY034xRqYPXLjhClUhwX（以下省略）=
```

図 5　DKIM-Signature ヘッダの例

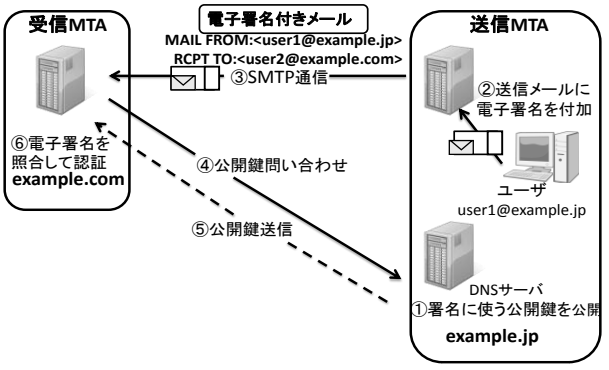

図 6　DKIM を用いた送信ドメイン認証の流れ

これまで述べてきた手法は受信側での対策である．これに対して OP25B は，送信側の spam 対策である．

通常，ユーザがメールを送信する場合には，ISP の SMTP サーバを利用するが，spam 配信プログラムは独自の SMTP サーバを用意して直接メールを配信する場合や，ウイルスに感染したエンドユーザコンピューを用いて spam を送信することが多い．OP25B は，ISP のネットワークを経由して ISP 外へ接続する SMTP 通信をすべてブロックする．これにより ISP 外の SMTP サーバに対して直接 SMTP でメールを送信することができなくなり，spam の送信を未然に防ぐ．OP25B の影響を受けるのは，ISP の SMTP サーバと異なる SMTP サーバでメールを送信している場合のみであり，自身が加入している ISP の回線と SMTP サーバを使用しているユーザには OP25B の影響はない．

2.10 関連研究

石島ら[18]は，組織においてユーザがメールを利用しない時間帯にのみ greylisting を適用し，常時 throttling を適用し，2 つの spam 対策を併用する手法を提案している．これにより，greylisting が抱えるメールの配送遅延の問題点を軽減した．

陳ら[19]は，SMTP セッションフィルタ及び greylisting を併用することで greylisting によって生じるメール受信の遅延を改善する手法を提案している．具体的には，オープンブラックリスト(OBL:Open Black List)に登録されている送信者からの接続を拒否し，初めて送信してくる送信者には greylisting を適用して再送を促すという方式である．

山井[20]らは，greylisting によって生じる配送遅延や管理の問題点を解決するために，SMTP セッション強制切断による手法を提案した．この手法はプライマリメールゲートウェイ(PMG:Primary Mail Gateway)，セカンダリメールゲートウェイ(SMG:Secondary Mail Gateway)の 2 台のメールゲートウェイを用意し，PMG への配送を拒否することにより，SMG への配送を促す．多くの正常な MTA に対して短時間での再送を促し，greylisting で問題となっていた通常メールの配送遅延を大幅に軽減した．

石島らは，greylisting を利用者の少ない時間帯のみ使用する手法を提案した．しかし，大分大学などの学術機関は，学生だけでなく研究者が昼夜問わずメールを利用する可能性があるため，適用時間を限定することはできない．陳らの greylisting と OBL を併用する手法において OBL は管理者の方針などによって登録内容が異なり，誤って登録されると通常メールを受信できなくなるため，導入には注意が必要である．山井らの提案手法を大分大学に導入するには，環境作成やシステムの設定に時間がかかるため，本研究ではこれまでに運用経験のある greylisting を用いた spam 対策手法を検討する．

3. 従来のシステム構成と問題点

3.1 大分大学のメールシステム

大分大学の従来のメールシステムの構成を図 7 に示す．spam 対策を実施するメールゲートウェイの前に iptables を設置している．iptables は Linux に実装されたパケットフィルタリング及び NAT，NAPT 機能を持つ[21]．メールゲートウェイは，spam を処理する MTA プロセス 1，通常メールを処理する MTA プロセス 2 が独立して動作している．iptables は whitelist を参照し，whitelist に登録された MTA からのメールの場合 MTA プロセス 2，登録されていない MTA からのメールの場合 MTA プロセス 1 へ振り分ける[22]．図 8 に MTA プロセス 1, 2 でそれぞれ実施する spam 対策を示す．MTA プロセス 1 では，throttling や greylisting など様々な対策を行う．一方，MTA プロセス 2 では whitelist によって信頼されている MTA からのメールのみ処理するため，2 つの spam 対策，account check，header check のみを実施する．

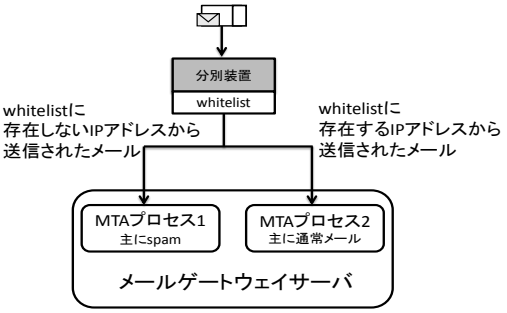

図 7　従来のメールシステムの構成

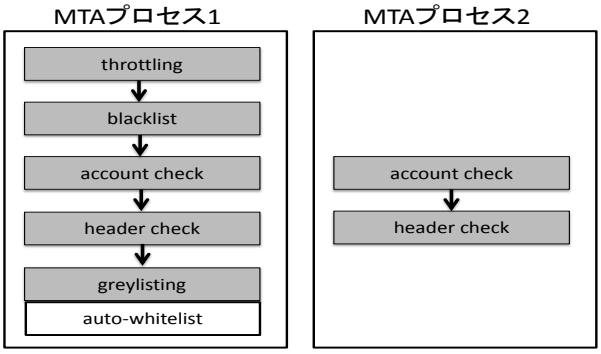

図 8　各 MTA プロセスにおける spam 対策

3.2 従来のシステムの問題点

従来のメールシステムでは，通常メールであるにも関わらず whitelist に送信元 IP アドレスが存在しないため spam と判断され MTA プロセス 1 に送られたメールは，greylisting を含む全ての spam 対策を経て配送されるため，メールを受信するまでに多くの時間を費やす問題が存在した．この問題を解決するためには，spam 対策手法は whitelist により spam と判断されたメールに対し全て適用するのではなく，各 spam 対策処理へ配送された後でも，通常メールと判断された時点で残りの spam 対策手法を省略し，すぐに受信できることが望ましい．

4. milter manager を用いた spam 対策システム

4.1 spam 対策手法の長所・短所

spam を検出・排除するために，spam 対策手法は数多く考案されている．また，各 spam 対策手法は 2 章で述べたようにそれぞれ長所・短所がある．そのため複数の手法を組み合わせて対応する必要がある．

大分大学のメールシステムで主として利用している greylisting は，メールの遅延が起こりうる．S25R は，負荷も軽く処理時間も短い方法だが，SMTP 接続を拒否するためのルールであり，S25R に spam 送信 MTA と誤検出された通常 MTA を救済する手段がない．SPF はドメインの詐称を防ぎ，送信者を認証することができる．2012 年現在 IIJ の調査によると，SPF の普及率は 69.6%であり，「jp」ドメインに限っての SPF 導入率は 2012 年 5 月時点で 43.9%[23]であるため，SPF のみによる spam 対策では不十分である．よって，各 spam 対策手法を組み合わせ，それらの適用を各プロセス配送後でも決めることができる milter manager を導入することで各 spam 対策手法の短所を補うシステムを構築する．

4.2 milter

milter とは mail filter の略で，Sendmail[24]のメールフィルタプラグインの仕組みである．メールフィルタは，メールを監視し，特定の種類のメールを自動的に選別し，通過・遮断する機能を持つ．milter を用いることにより，Sendmail 本体を変更せずに，迷惑メールフィルタやウイルスチェックなどの機能を Sendmail に組み込むことができる．milter は Sendmail とは別プロセスで動作し，milter と Sendmail とは独自のプロトコルである milter protocol で通信する．milter protocol は，Postfix 等の Sendmail 以外の MTA の機能拡張にも利用されている．

4.3 milter manager

milter manager[4]は複数の milter を管理する milter である．milter manager には複数の milter を登録でき，milter manager に対する milter セッションは登録した複数の milter に転送される．milter manager に登録した milter を「子 milter」と呼ぶ．つまり，milter manager はプロキシとして動作し，MTA 側からは，milter manager は 1 つの milter である．一方，子 milter 側からは，milter manager は MTA となる(図 9).

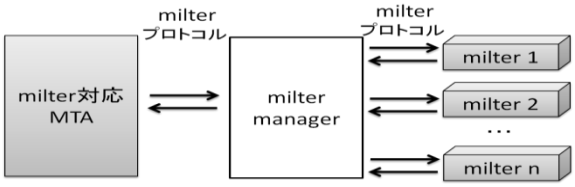

図 9　MTA と milter manager 及び，子 milter の関係

通常，複数の milter を利用する場合には，図 10 に示すように登録した全ての milter がメールに対して適用される．しかし，milter manager は図 11 に示すように各 milter の処理結果を他の milter の適用条件として利用が可能なため，複数の milter を管理者が指定した条件によって適用できる．

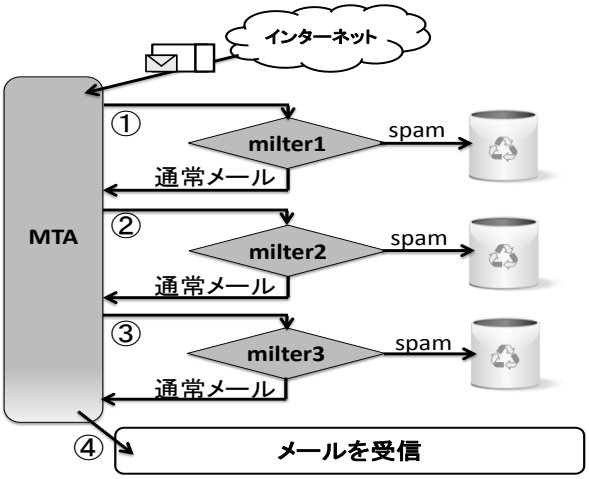

図 10　通常の milter 適用の例

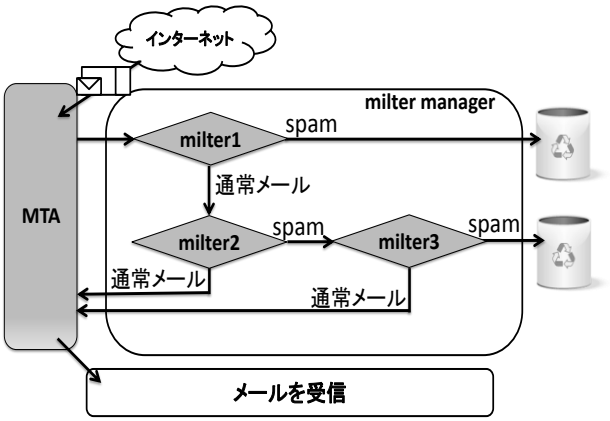

図 11　milter manager 導入後の milter 適用の例

4.4 milter manager を用いたメールシステムの構成

本研究では，4.1 節で述べた各 spam 対策手法の長所を活かし，短所を補うために，3.1 節で示した従来のシステムに milter manager を導入し，低配送遅延，spam の高検出を目指したメールサーバシステムを構築する．図 12 に spam 判定の流れを示す．

①iptables によるメール分別
iptables は whitelist を参照し，whitelist に登録された MTA からのメールであれば，主に通常メールを処理する MTA プロセス 2，登録されていない MTA からのメールであれば，主に spam を処理する MTA プロセス 1 へ振り分ける．

②MTA プロセス 2 での spam 検査
account check，header check で検査し，通常メールであれば学内へ配送，spam であれば破棄する．

③SPF による spam 判定
SPF による送信者認証が成功したら通常メールと判断して S25R を適用，送信者認証が失敗したら spam の可能性があるため greylisting を適用する．

④S25R による spam 判定
送信元 MTA の FQDN が S25R のルール[25]に一致しない場合，通常メールと判断して学内各メールサーバへ配送，S25R のルールに一致した場合，spam の可能性があるため greylisting を適用する．
⑤greylisting による spam 判定
メールが再送された場合，通常メールと判断して学内各メールサーバへ配送，メールが再送されない場合，再送要求をした MTA を spam 送信 MTA と判断する．

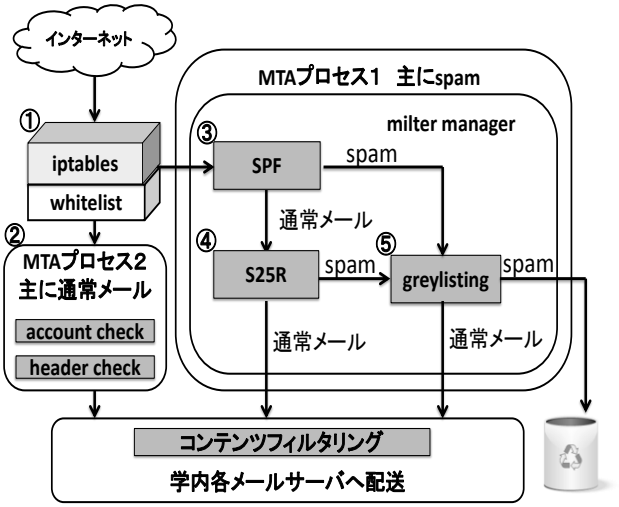

図 12　milter manager を利用したメールシステム

4.5 システムの利点

この手法では，S25R あるいは SPF で疑わしいと判断したメールに対して greylisting を適用する．そのため，spam 送信者以外からのメールに対してのみ再送要求をして配送遅延が生じる割合を減らしている．本システムは milter manager を利用することにより，「各 milter の処理結果を他の milter の適用条件として利用し，通常メールに対してすべての milter が適用される」という問題点を解決する．つまり，フィルタリングによる誤検出を抑えることが可能となる．

5 運用結果

5.1 greylisting 適用件数の低減効果

以前のシステムでは，MTA プロセス 1 に送られたメールに対して無条件で全ての spam 対策を適用していた．MTA プロセス 1 へ送られた通常メールは greylisting によって大きな配送遅延が発生していた．

表 1 は，milter manager 運用前後の greylisting 適用メール数と spam メール数の割合を比較している．運用前後では，greylisting の適用割合が 54.0%から 39.7%まで減少している．このことから，配送遅延のかかるメールが減少していることがわかる．
また，図 13 に示す greylisting の適用件数の推移からも，システム導入前と比べて導入後が greylisting の適用割合が減少している．

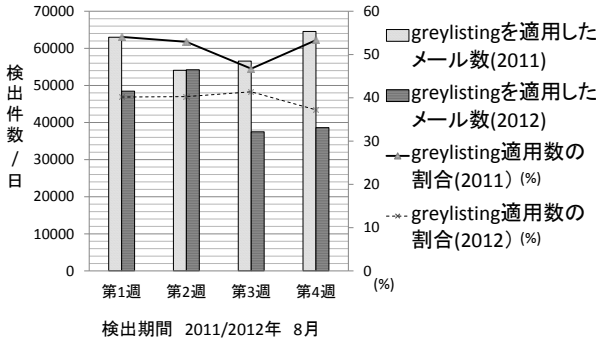

図 13　greylisting の適用件数の推移

表 2 にコンテンツフィルタリングでの spam 判定を示す．コンテンツフィルタリングで spam と判断されたメールの割合が増加していることから，spam を処理する MTA プロセス 1 で検出漏れが発生していることがわかる．

表 3 に MTA プロセス 1 で適用される各 spam 対策手法の spam 検出数の内訳を示す．図 12 のフロー図のとおり SPF，S25R で spam として検出されるメールは，次に greylisting によって spam 判定が行われる．そのため，表 3 の SPF，S25R の spam 数(☆)は「spam の可能性のあるメール数」を表す．

表 1．greylisting 適用件数と spam の割合

期間	メール総数(A)	適用メール数(B)	適用割合(B/A)	spam 数(C)	spam 割合(C/B)
2011 7/31~8/27 (運用前)	441,073 通	238,205 通	54.0%	175,019 通	73.4%
2012 7/29~8/26 (運用後)	449,454 通	178,792 通	39.7%	112,268 通	62.7%

表 2．コンテンツフィルタリング適用件数と spam の割合

期間	適用メール数(A)	spam 数(B)	spam 割合(B/A)
2011 7/31~8/27 (運用前)	441,073 通	5,769 通	1.3%
2012 7/29~8/26 (運用後)	449,454 通	26,280 通	5.84%

表 3. システム導入後の spam 検出数の内訳(2012 7/31~8/27)

	適用メール数(A)	適用割合(A/メール総数)	spam 数(B)	spam 割合(B/メール総数)
blacklist	449,454 通	100%	219,690 通	48.8%
header check	229,764 通	51.1%	483 通	0.1%
throttling など	229,281 通	51.0%	39101 通	8.7%
SPF	180,106 通	40.0%	☆ 78,381 通	☆ 17.4%
S25R	101,725 通	22.6%	☆ 100,411 通	☆ 22.3%
greylisting	178,792 通	39.7%	112,268 通	24.9%

5.2 配送遅延の低減効果

次に, spam 対策による配送遅延の低減について述べる．表 4 にシステム導入前(2011/7/31~8/27)の平均配送遅延と導入後(2012/7/29~8/26)の平均配送遅延を示す．遅延値の計算方法は,

$$\frac{\text{greylisting によって発生した配送遅延時間}}{\text{MTA プロセス 1 で受信した通常メール数}}$$

とした．つまり主に spam を処理する MTA プロセス 1 における通常メール 1 通あたりに発生する平均配送遅延時間を求めている．SPF，S25R は greylisting に比べると spam 対策に要する時間が 1 秒未満と短いため計算からは除外する．

表 4 の greylisting による遅延時間の合計が 2011 年と比べて 2012 年が少ないことから，greylisting に対して短い間隔で再送を行う MTA が増えたことがわかる．

表 4. プロセス 1 における通常メールの平均配送遅延

	greylisting による遅延時間の合計	通常メール数	平均遅延時間
2011 7/31~8/27	295,936,549 秒	142,308 通	2,079 秒
2012 7/29~8/26	4,044,231 秒	67,838 通	59.6 秒

6 おわりに

本論文では，milter manager を用いた spam 対策メールサーバを構築し, それらの運用結果について述べた．これにより，少ない spam 対策の組み合わせで通常メールを受信することができた．また，運用の結果，多くの通常メールが greylisting による遅延の影響を受けなくなり平均配送遅延時間が低減した．

本論文で述べた milter manager による spam 対策システムは，現在複数の spam 対策手法を併用している，もしくは，これから新たな spam 対策手法を加えようとしているシステムに対して有用であると考えられる．この理由として milter manager には，milter 自動検出機能がついており，新たに設定ファイルを変更する必要がなく，容易に新規導入可能なためである．

本論文で報告した運用結果からコンテンツフィルタリングでの spam 検出件数の増加から，MTA プロセス 1 における spam 検出率が低下している可能性がある．これは SPF レコードを登録しており，かつ S25R のルールセットにも該当しないドメインを持つ spam 送信者から送信される spam が原因であると考えられる．

今後の課題として spam 候補を振り分ける対策の追加により，検出漏れを減らせるようにしたい．

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 年 4 月
[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 年 9 月
[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 年 3 月
[4]milter を使った効果的な迷惑メール対策 http://milter-manager.sourceforge.net/
[5] Apache Spamassassin Project:“Spamassassin”, http://www.spamassassin.apache.org
[6] 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，情報処理学会マルチメディア，分散，協調とモバイル(DICOMO2004)シンポジウム論文集，pp.493-496，2004 年 7 月
[7]Greylisting.org - a great weapon against spammers: http://www.greylisting.org/
[8]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ついて，情報処理学会研究報告，分散システム/インターネット技術, 2007-DSM-46，pp.43-48, 2007 年 7 月
[9]The Spamhaus Project: http://www.spamhaus.org/
[10]McAfee Labs Threats Report for Q1 2012: Threats Gone Wild http://blogs.mcafee.com/mcafee-labs/mcafee-labs-threat-report-for-q1-2012-threats-gone-wild
[11]スパム対策技術 http://www.gabacho-net.jp/anti-spam/
[12]J. Klensin;“Simple Mail Transfer Protocol (SMTP)”, RFC5321, http://www.ietf.org , Oct. 2008 http://tools.ietf.org/rfc/rfc5321.txt

[13] W. Schlitt：“Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1”，RFC4408, Apr.2006
http://tools.ietf.org/rfc/rfc4408.txt
[14]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，分散システム/インターネット技術，2004-DSM-35,pp.19-24,2004 年 9 月
[15]松竹俊和，金高一，吉田和幸：spam メール対策による遅延を低減するための whitelist 自動作成システム，情報処理学会，インターネットと運用技術シンポジウム論文集(IOTS2011)，pp.39-44，2011 年 11 月
[16]Yahoo! Inc：“Domain-Based Email Authentication Using Public Keys Advertised in the DNS (DomainKeys)”RFC4871,May. 2007
http://www.ietf.org/rfc/rfc4871.txt
[17]J.Klesin：“Message Submission”RFC2476,Dec. 1998
http://www.puni.net/~mimori/rfc/rfc2476.txt
[18]石島悌，平松初珠，林治尚：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, 情報処理学会論文誌 Vol.51 No.3 989-997, 2010 年 3 月
[19]陳春祥，佐々木宣介，田中稔次朗：SMTP セッションフィルタとグレイリストを併用した迷惑メール対策，情報処理学会論文誌 Vol.47 No.4 1000-1009，2006 年 4 月
[20]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.3 940-949，2009 年 3 月
[21] netfilter/iptables project homepage
http://www.netfilter.org/projects/iptables/
[22]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 第 3 回 インターネットと運用技術シンポジウム論文集 (IOTS2010)，pp.75-80，2010 年 12 月
[23]桜庭秀次：メッセージテクノロジー「送信ドメイン認証技術の普及と認証する識別子」Internet Infrastructure Review(IIR) Vol.16 (2012 年 8 月 21 日発行)
http://www.iij.ad.jp/company/development/report/iir/016.html
[24]Sendmail Home Page: http://www.sendmail.org/
[25] 阻止率 99%のスパム対策方式の研究報告
http://www.gabacho-net.jp/anti-spam/anti-spam-system.html