「マルチメディア，分散，協調とモバイル
(DICOMO2013)シンポジウム」 平成25年7月

milter manager を用いたメールサーバの運用における導入の効果

松井一乃[†1]　金髙一[†1]　池部実[†2]　吉田和幸[†3]

現在広く利用されている spam 対策技術のひとつに greylisting がある．greylisting は「spam 発信 MTA は再送をしない」との仮説に基づき送信者に対して一時エラーのレスポンスコードを返し，再送をうながす対策手法である．greylisting は spam 排除の効果は高いが，適用する全てのメールに再送要求をするため，通常メールにも大きな遅延が生じる．そこで大分大学では milter manager を導入し，S25R，SPF の判定結果によってメールを greylisting に適用するかを決定している．SPF，S25R を用いて通常メールと spam を判断することで， SPF，S25R による検査のみで受信できるメールが増え，greylisting による再送遅延を軽減できる．また，SPF，S25R によって誤検知された通常メールは greylisting によって救済することが可能となる．milter manager 導入後，通常メールのうち約 70%は SPF 及び S25R が処理しているため, greylisting を適用せずに受信できるようになった. また, 受信した通常メールに対する greylisting の再送要求割合を比較すると，milter manager 導入前と導入後では 43.1%から 12.4%まで減少していた．このことから，milter manager を導入することで配送遅延がかかる通常メールが減少したといえる．

The effect of the mail server operation using the milter manager in the Oita University

KAZUNO MATSUI[†1]　HAJIME KANETAKA[†1]
MUNORU IKEBE[†2]　KAZUYUKI YOSHIDA[†3]

1. はじめに

インターネットの急速な普及と発展に伴い，電子メールをはじめとしたネットワークを介したコミュニケーションは不可欠になっている．これに伴い，spam が大きな社会問題となってきている．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す．現在，ネットワークを流れる電子メールの約 64%が spam である 1)．spam による被害としては，フィッシング詐欺やメールに添付されたウイルスに受信者が感染するなどが挙げられる 2)．ユーザが spam の被害を受けないように，メールサーバの管理者は spam 対策をすることが重要である．大分大学のメールゲートウェイでは，iptables を用いて whitelist を参照し, 登録されている MTA（Mail Transfer Agent）からのメールかどうかで 2 つのプロセスへ振り分け，各プロセスで spam 対策を実施している．whitelist とは，信頼できる MTA の IP アドレスを列挙したリストである. whitelist に登録されていない MTA からのメールを処理するプロセス 1 では greylisting をはじめ様々な spam 対策を実施する．一方, whitelist に登録されている MTA からのメールを処理するプロセス 2 では信頼できる MTA からのメールであるため簡単な spam 対策を実施するにとどめている．プロセス 1 で実施している greylisting は「spam 発信 MTA は再送をしない」との仮説に基づき送信者に対して一時エラーのレスポンスコードを返し，再送をうながす対策手法である 3)．greylisting は spam 排除の効果は高いが，適用する全てのメールに再送要求をするため，プロセス 1 を通過する通常メールにも遅延が生じる 4)．そこで本研究では milter manager を用いて複数の spam 対策を組み合わせることで greylisting の再送要求に伴う通常メールの配送遅延を低減させることを目指す 5). milter manager を用いたメールシステムの運用における効果を示すために, milter manager 導入前と導入後の greylisting 適用数の比較，milter manager 導入後のメールに適用した spam 対策の変化について調査する．

本論文の構成は以下の通りである．まず，2 章で大分大学で利用している spam 対策手法について述べ, 3 章で大分大学のメールシステムの構成と問題点について述べる．そして，4 章で関連研究について述べ，5 章で milter manager を用いたメールシステム構成について述べる．6 章で運用結果について述べ，7 章でまとめと今後の課題について述べる．

2. spam 対策手法

大分大学では，複数の spam 対策を利用している．以下で大分大学が利用している spam 対策について詳しく述べる．

†1 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
†2 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
†3 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

2.1 greylisting

greylisting は「spam 発信 MTA は再送をしない」という仮説に基づいた対策手法である 3)4). 一時的に受信を拒否し，再送処理が行われたメールのみを受信する．再送処理が行われた MTA は一定期間 autowhitelist に登録される．autowhitelist 登録期間内であれば再送要求はせず, 直ちにメールを受信する．多くの spam 発信 MTA は仮説通りに動作するため，高い効果がある．しかし，MTA に再送を要求するため配送遅延が多く，1 時間以上の遅延が発生する場合も多い．

2.2 throttling

throttling とは「spam 発信 MTA は timeout が短い」,「spam 発信 MTA は SMTP(Simple Mail Transfer Protocol)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わざと遅延させ，メール送信者がこちらの応答を待たずにメールを送信してきた場合，spam と判断して受信を拒否する対策手法である 6)．throttling は設定すべきパラメータが遅延時間のみであり，設定は簡単であるが, TCP コネクションを保持したまま待機するため，送信側，受信側両方とも MTA のプロセス数，TCP セッションが増加しやすい問題がある．

2.3 blacklist

blacklist とは，spam 送信者の利用する MTA の IP アドレスをリスト化したものであり，TCP コネクション確立時に利用する対策である．blacklist に掲載されている IP アドレスからのアクセスを拒否することで，spam を拒否する．代表的な blacklist は SpamCop 7)や rbl.jp 8)，Spamhaus 9)がある．

2.4 whitelist

whitelist とは，信頼できる MTA の IP アドレスを記述したリストである．通常 MTA の中には，greylisting の再送要求に応答のない MTA や, blacklist に誤って登録された MTA が存在する．このような通常 MTA は greylisting や blacklist による対策でメールの受信を拒否してしまうため，通常メールにも関わらず受信できない．そのため，whitelist に他の spam 対策で誤検知される信頼できる MTA の IP アドレスを記載することで, 誤検知される通常メールを受信する．また，全てのメールに greylisting を適用すると，遅延や再送が必要になり，メール受信までに時間を要することになる．そこで，spam でないと確信が持てるメールをすぐに受信するために，信頼できる MTA の IP アドレスを whitelist に列挙し，その MTA から送信されるメールは greylisting の処理を省く．whitelist でメールを分別することで多くの通常メールを遅延なく受信できる．

2.5 SPF

SPF(Sender Policy Framework)10)とは SMTP によるメールの送受信において，送信者の正当性を検証し送信者のドメインの偽称を防ぐ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検証することでメール送信者の正当性を確認する．

送信側はあらかじめ自ドメインの権威 DNS サーバに, 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．同時にメール送信を許可しない MTA からのメールの送信があった場合の判定を記述する．SPF レコードの記述例を図 2.1 に示す．図 2.2 を例に認証の流れを示す．まずメールを受信すると(①)，受信者は送信者のメールアドレスのドメインの SPF レコードを送信元のドメインの権威 DNS サーバへ問い合わせ(②)，SMTP 接続元の IP アドレスと取得した SPF レコード(③)が一致するか確認することで，送信ドメインを認証する(④)．しかし，SPF はメールを転送すると誤検知することがある．これはメールを転送する際, 送信元の IP アドレスは自動的に書き換えられるが，送信者のメールアドレスは手動で書き換える必要がある. よって, メールアドレスの書き換えを忘れると，送信 MTA の IP アドレスと，送信者のメールアドレスから問い合わせた SPF レコードの IP アドレスが一致しないため，誤検知される．

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

図 2.1 SPF レコードの記述例

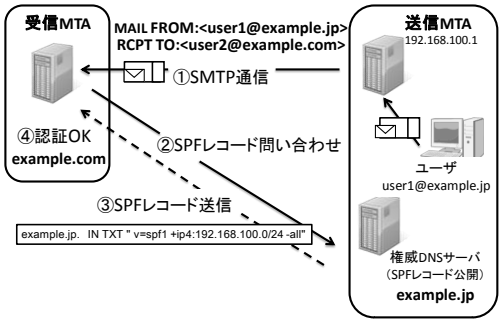

図 2.2　SPF による認証の流れ

2.6 S25R

シマンテックの調査報告 11)によると，spam の 81.2%は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ている．ボットに感染したエンドユーザコンピュータからの spam を排除する対策に S25R(Selective SMTP Rejection)がある 12)．S25R は SMTP アクセスを行ってきた MTA の FQDN（Fully Qualified Domain Name）を規則と照合し，エンドユーザコンピュータを推定し，SMTP アクセスを拒否する．企業や学術機関などに管理されている MTA のほとんどは FQDN を設定しているが, エンドユーザコンピュータの多くは FQDN を設定していない．もしくは，エンドユーザコンピュータに対して FQDN を設定していることがあるが，MTA と比較すると，IP アドレスの下位 16 ビットなど多くの数字を含むことが多い．図 2.3 に S25R で検知した FQDN の例を示す．S25R を用いることで，エンドユー

ザコンピュータからのメールはほとんど検出されるため，spam 排除に高い効果がある．しかし，通常メールを送信する MTA の中には，S25R の規則に該当するような FQDN を設定していることがある．そのため，このような MTA からの通常メールをエンドユーザコンピュータと誤検知する可能性がある．

m1-110-0-0-0.example.jp
adsl-0-0-0-0.adsDRU.net
1.1.1.1.f.sta.codetel.net.do

図 2.3 S25R で検知した FQDN の例

2.7 コンテンツフィルタリング

コンテンツフィルタリングとはメールヘッダや本文を spam の特徴を示した文字列と比較し，spam と判定したものを排除する spam 対策である．代表的なコンテンツフィルタリングは SpamAssassin 13)や bsfilter 14)がある．大分大学では Cloudmark 社の Cloudmark Authority 15)を使用している．

コンテンツフィルタリングはメールヘッダや本文を解析して spam を排除するため，メールを送信する際の挙動では通常メールと見分けのつかない spam を排除できる．しかし，メールヘッダや本文を解析するため，他の spam 対策よりサーバの資源を多く必要とする．また，spam の検出率を上げるためには大量の spam による学習が必要となり，学習データが増えるにつれ，サーバへかける負荷が大きくなる．

3. 関連研究

陳ら 17)は SMTP セッション中にやり取りされるホスト名や送信者のメールアドレスを用いて, spam を排除するメールシステムを提案した．このシステムでは HELO コマンドの内容が RFC の必須事項に従っていないメールや, 送信 MTA の FQDN の登録がないメールなど 4 つの条件によって spam を排除している．また，どの条件にも当てはまらなかったメールであっても greylisting を適用し，再送要求に応答のあったホストからのメールは 3 日間 greylisting を適用せずに直ちに受信する．greylisting は配送遅延が大きいため，信頼できるホストからのメールには greylisting を適用せず受信している．信頼できるホストの条件は，送信ホストの FQDN を持ち, なおかつ FQDN の正引き結果をさらに逆引きすると元の FQDN と一致し，HELO コマンドの内容が FQDN と一致するか，送信ホストの属性やサポートする機能を示していることである．しかし，通常メールのみを送信するホストであっても信頼できるホストの条件に当てはまらないホストも存在する．また，再送要求に応答があったホストからのメールであっても以前送信したメールから 3 日以上経過していれば再度再送要求する．頻繁にメールを送信するホストであれば 3 日以内にメールを送信すると考えられるが，メールの送信間隔が 3 日以上空くホストからのメールは毎回再送要求するため, 遅延が生じる．

また山井ら 18)は, SMTP セッションを強制切断することで spam を排除するシステムを構築した．このシステムではプライマリメールサーバとセカンダリメールサーバを利用し，プライマリメールサーバに SMTP コネクションを張ってきたユーザに対してリセットパケットを送ることで強制的にコネクションを切断し，セカンダリメールサーバへのメールの配送を促す．このようにすることで，greylisting と同等の効果を得られ, さらに配送遅延を大幅に削減した．

4. 大分大学のメールシステムの構成

4.1 システムの構成

大分大学のメールシステムの構成を図 4.1，各プロセスでの spam 対策の構成を図 4.2 に示す．

大分大学のメールシステムでは，最初に whitelist を用いてメールを 2 つのプロセスへと振り分ける. 実際は, iptables を用いて whitelist を参照し，登録されていない MTA からのメールはプロセス 1, 登録されている MTA からのメールならプロセス 2 へ振り分ける．図 4.2 に示すようにプロセス 1 では greylisting をはじめ様々な spam 対策を実施する．一方，プロセス 2 では信頼できる MTA からのメールであるため簡単な spam 対策を実施するにとどめている．各 spam 対策は, Sendmail のメールフィルタプラグインの仕組みである milter(mail filter)を利用している

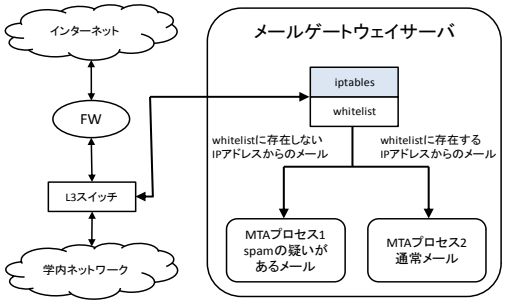

図 4.1 大分大学のメールシステムの構成

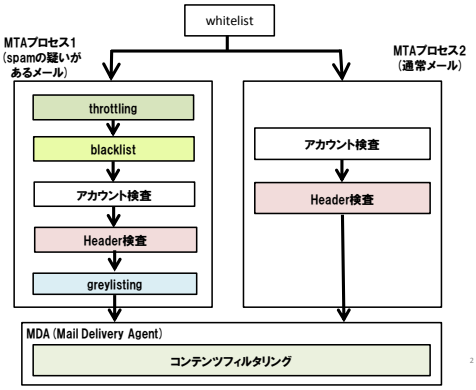

図 4.2 プロセスでの spam 対策

4.2 システムの問題点

大分大学では, whitelist に記述のない MTA からのメール

はプロセス 1 へ振り分け，多くの spam 対策を実施している．プロセス 1 の spam 対策の中には greylisting がある．greylisting は 2.1 節で述べたように，全てのメールに再送要求するため，通常メールであっても多くの配送遅延が発生する問題がある．できるだけ早く受信したいので，通常メールは greylisting を適用しないのが望ましい．

5. milter manager を用いたメールシステムの構成

5.1 spam 対策手法の利点と欠点

spam 対策には利点と欠点が存在する．greylisting は 2.1 節で述べたように，spam 排除の効果は高いが，配送遅延が発生する欠点がある．S25R は，エンドユーザコンピュータからのメールをほとんど検出するため，spam 排除に高い効果があるが，誤検知した通常メールの救済措置がない．また，SPF は，メール送信者の正当性を確認できるが，S25R と同様に誤検知した通常メールの救済措置がない．このように，spam 対策は一長一短である．

5.2 milter manager

milter manager 16)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 に転送する．通常，複数の milter を利用する場合には，図 5.1 に示すように登録した全ての milter をメールに対して適用する．しかし，milter manager を用いることで図 5.2 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できる．そのため，複数の spam 対策を milter manager を用いて組み合わせることで，各対策の利点を活かしつつ欠点を補い，誤検知が少なく，通常メールの配送遅延が小さいメールシステムを構築できる．

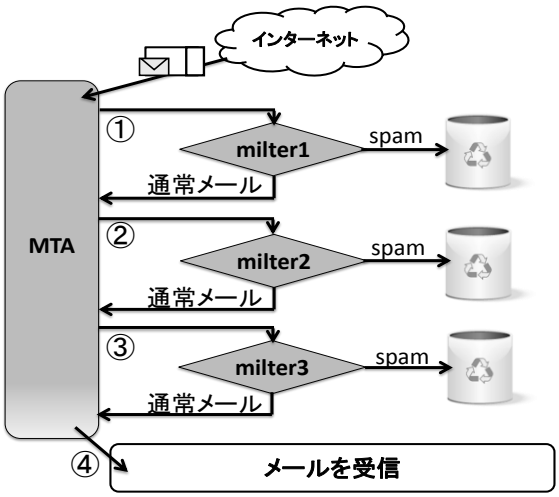

図 5.1 通常の milter の適用例

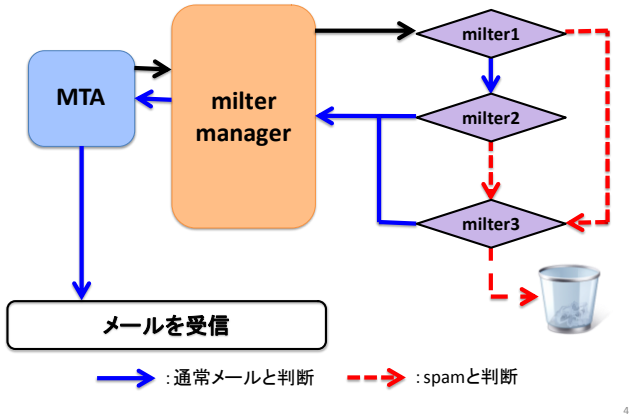

図 5.2 milter manager を用いた milter の適用例

5.3 システムの構成

milter manager を用いた spam 対策の適用順序を図 5.3，milter manager を用いたメールシステムの構成を図 5.4 に示す．milter manager を用いて，SPF，S25R の spam 対策の処理結果によって greylisting の適用の有無を決定している．適用の順序は以下の通りである．

(1) SPF を適用
(2) SPF の認証に成功した場合のみ S25R を適用
(3) SPF の認証に失敗した場合と S25R によって spam と判断された場合に greylisting を適用
(4) S25R によって通常メールと判断された場合と，greylisting において再送処理があった場合は MDA による処理を受ける．greylisting において初めて受信するメールの場合は一時エラーのレスポンスコードを返し，メールを削除

この順序で spam 対策を適用することで，通常メールは SPF，S25R を通過し，greylisting による再送遅延の影響を受けない．また，SPF，S25R で誤検知されたメールは greylisting によって救済できる．

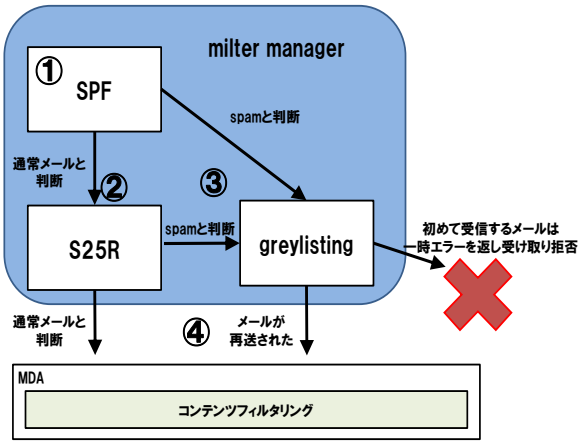

図 5.3 milter manager を用いた spam 対策の適用順序

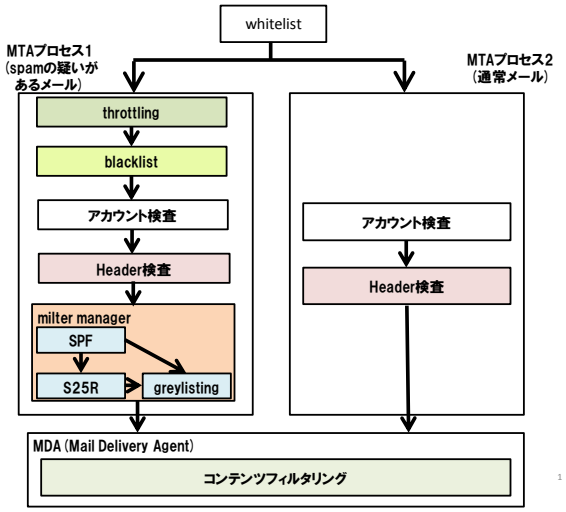

図 5.4 milter manager を用いたメールシステムの構成

表 1 システム全体でのメール受信数
(2012 年 12/30～2013 年 3/30)

プロセス	総受信数	通常メール数	spam 数
プロセス 1	1,955,370 通	596,724 通	1,358,646 通
プロセス 2	2,213,828 通	1,608,458 通	605,370 通
合計	4,169,198 通	2,205,182 通	1,964,016 通(A)

表 2 MTA プロセス 1 の各 spam 対策での spam 排除数
(2012 年 12/30～2013 年 3/30)

spam 対策	排除数(B)	spam 排除割合 B÷表 1(A)
thottling	1,095 通	0.1%
blacklist	656,085 通	33.3%
アカウント検査	28,129 通	1.3%
ヘッダー検査	161,478 通	8.2%
greylisting	511,859 通	26.4%
合計	1,358,646 通	69.3%

表 3 MTA プロセス 2 の各 spam 対策での spam 排除数
(2012 年 12/30～2013 年 3/30)

spam 対策	排除数(C)	spam 排除割合 (C÷表 1(A))
アカウント検査	425,565 通	21.6%
ヘッダー検査	179,805 通	9.1%
合計	605,370 通	30.7%

6. 運用結果

6.1 調査方法

調査期間は 2012 年 12 月 30 日から 2013 年 3 月 30 日までの約 3 ヵ月間である．本研究では MTA プロセス 1 で運用をしている milter manager の効果について調査するため，milter manager を用いていない MTA プロセス 2 は調査対象から除外した. MTA プロセス 2 を含むシステム全体のメール受信数を表 1，milter manager 導入後の MTA プロセス 1 の各 spam 対策での spam 排除数を表 2，MTA プロセス 2 の各 spam 対策での spam 排除数を表 3 に示す.

6.2 調査結果

milter manager を導入したメールサーバの運用の効果を調査するため，導入する前の 2011 年 6 月 26 日から 2011 年 9 月 25 日と比較した. 調査対象は大分大学宛に送信されたメールの内，MTA プロセス 1 で spam 対策を受けたメールである．MTA プロセス 1 の受信メール数を表 4，greylisting 再送要求数を表 5 に示す．また，milter manager 導入後の通常メールが処理を受けた spam 対策のルートと処理メール数を図 6.1，milter manager 導入後の greylisting において排除された spam が処理を受けた spam 対策のルートと処理メール数を図 6.2 に示す.

表 4 の milter manager 運用前と運用後を比較すると，メールの greylisting 適用割合が 64.3%から 35.4%に減少している．greylisting を適用したメールの詳細を調査すると，greylisting を適用したメールのうち，26%にあたる 181,084 通は通常メールであった．図 6.1 に示すように通常メール全体の 70%にあたる 415,640 通が greylisting の再送要求に伴う配送遅延を受けていない. milter manager 導入前は全てのメールに greylisting を適用していたため，受信した全ての通常メールが greylisting の再送要求に伴う配送遅延を受けていた．milter manager を導入することで，通常メールの greylisting 適用率を全てに適用していた 100%から 30%まで減少させることができた.

しかし，greylisting が所有する autowhitelist に記載のあるメールには再送要求をしないため greylisting 適用率だけでは, 通常メールにかかる配送遅延が減少したとはいえない. そこで greylisting の再送要求数について調査した．表 5 の milter manager 導入前と導入後の通常メールに対する再送要求の割合を比較すると，43.1%から 12.4%まで減少した. このことから，通常メールに対する再送要求が減少したと判断できる．また，図 6.2 に示す greylisting の再送要求に応答のなかったメールのうち全体の約 76%にあたる 389,013 通が SPF による認証に失敗していた．このことから，greylisting において排除された多くの spam はドメインを偽っている，もしくは SPF レコードを登録していないことが分かる.

表 4 受信メール数

期間	総受信数(D)	通常メール数(E)	spam 数(F)	spam 割合 (D÷F)	greylisting 適用数(G)	greylisting 適用割合(G÷D)
2011 年 6/26~ 2011 年 9/25（運用前）	1,801,035 通	496,045 通	1,304,990 通	72.4%	1,157,227 通	64.3%
2012 年 12/30～ 2013 年 3/30(運用後)	1,955,370 通	596,724 通	1,358,646 通	69.5%	692,943 通	35.4%

表 5 greylisting 再送要求

期間	再送要求数	autowhitelist 通過数	再送要求に応答があったメール数(H)	再送要求に応答がなかったメール数	通常メール再送要求割合 (H÷表 4(E))
2011 年 6/26~ 2011 年 9/25（運用前）	862,568 通	294,659 通	202,114 通	660,454 通	43.1%
2012 年 12/30～ 2013 年 3/30(運用後)	586,103 通	106,839 通	74,244 通	511,859 通	12.4%

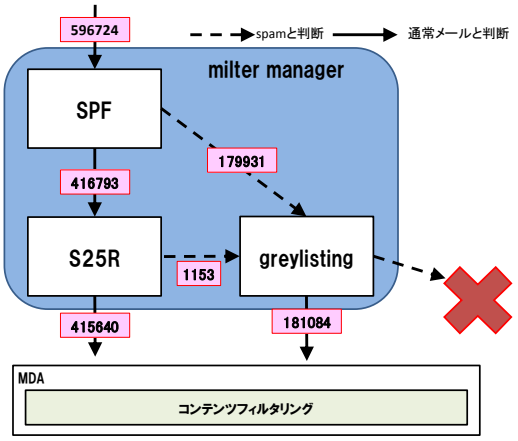

図 6.1 通常メールが通過したルート

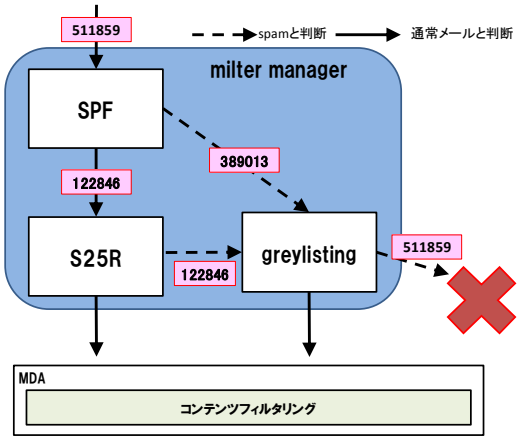

図 6.2 greylisting で検出した spam が通過したルート

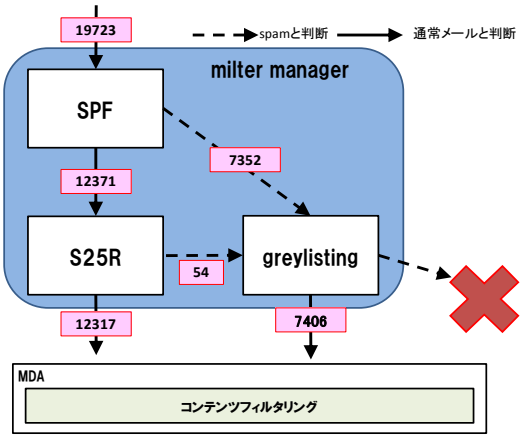

図 6.3 コンテンツフィルタリングで検出した spam が通過したルート

また，システムの検出漏れの調査のために milter manager 導入前と導入後のコンテンツフィルタリングで検出した spam 数を表 6 に示す．コンテンツフィルタリングは MTA で実施される spam 対策を全て通過したメールにのみ適用されるため，コンテンツフィルタリングで spam と判定されたメールは MTA の spam 対策で検出されなかった spam

表 6 コンテンツフィルタリングで検出した spam

期間	適用メール数 (F)	spam 数 (G)	検出漏れ率 (G÷F)
2011 年 6/26~ 2011 年 9/25（運用前）	496,045 通	30,755 通	6.2%
2012 年 12/30～ 2013 年 3/30(運用後)	596,724 通	19,723 通	3.3%

である．また，導入後の検出漏れした spam について spam 対策を受けたルートを調査した．調査結果を図 6.3 に示す．検出漏れの 62.7%にあたる 12,317 通は SPF,S25R が処理している．この 62.7%の spam 送信者は SPF レコードと FQDN を登録している．このような spam 送信者は通常メール送信サーバと同じ挙動で spam を送信しているため，もし greylisting を適用しても，再送要求にも応答するのではないかと考えられる．また greylisting の再送要求に応答のあった 37.3%にあたる 7,406 通も通常メール送信サーバと酷似した挙動で spam を送信しているため，メールを送信する際の挙動では spam と判断することは困難である．

7. おわりに

本論文では milter manager を用いたメールサーバの運用における効果について述べた．milter manager を導入することで, 通常メールに対する再送要求割合が 32.1%から 12.4%まで減少した．このことから，通常メールに対する再送要求が減少したといえる．また，検出漏れのあった spam は SPF レコードや FQDN の登録をしている MTA からのメールや，greylisting の再送要求に応答のあったメールであった．このような MTA から送信されるメールは通常メールと酷似した挙動でメールを送信するため，メールを送信する際の挙動で spam と判断することは困難であるため，メールヘッダや本文を用いて排除するのが望ましい．

今後の課題として，大分大学が受信した spam のメールヘッダや本文の特徴を調査していきたい．

参考文献

1) シマンテックインテリジェンス月次レポート 2013 年 1 月号，入手先
(http://www.symantec.com/content/ja/jp/enterprise/white_papers/sr_wp_spam_report_1301.pdf) (参照 2013-05-05)
2) 渡部稜太，愛甲健二: スパムメールの教科書，データハウス，(2006 年)
3) Greylisting.org - a great weapon against spammers, 入手先(http://www.greylisting.org/) (参照 2013-05-05)
4) 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 年 9 月)
5) 金高 一，松井 一乃，池部 実，吉田 和幸: 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，情報処理学会第 5 回インターネットと運用技術シンポジウム(IOTS2012）,pp.8-15,(2012 年 12 月)
6) 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)
7) SpamCop, 入手先(http://www.spamcop.net/)(参照 2013-05-05)
8) RBL.JP プロジェクト, 入手先(http://www.rbl.jp/)(参照 2013-05-05)
9) The Spamhaus Project 入手先(http://www. spamhaus.org/)(参照 2013-05-05)
10) W. Schlitt: Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1, RFC4408, ApLUR006 入手先(http://tools.ietf.org/rfc/rfc4408.txt)(参照 2013-05-05)
11) インターネットセキュリティ脅威レポート第 17 号, 入手先 (http://www.symantec.com/content/ja/jp/enterprise/white_papers/istr17_wp_201207.pdf)(参照 2013-05-05)
12) 阻止率 99%のスパム対策方式の研究報告, 入手先 (http://www.gabacho-net.jp/anti-spam/anti-spam-system.html)(参照 2013-05-05)
13) Apache Spamassassin Project:Spamassassin，入手先 (http://www.spamassassin.apache.org) (参照 2013-05-05)
14) bsfilter,入手先(http://bsfilter.org/)(参照 2013-05-05)
15) Cloudmark Authority 入手先 (http://www.cloudmark.com/ja/products/cloudmark-authority/index)(参照 2013-05-05)
16) milter を使った効果的な迷惑メール対策，入手先 (http://milter-manager.sourceforge.net/) (参照 2013-05-05)
17) 陳春祥,佐々木宣介,田中稔次郎: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, pp.1000-1009 (2006 年 4 月)
18) 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)