情報処理学会論文誌 Vol.55 No.12 2498–2510 (Dec. 2014)

推薦論文

milterの組合せ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導入の効果について

松井 一乃[1,a)] 金高 一[1,†1] 加来 麻友美[2,†2] 池部 実[2] 吉田 和幸[3]

受付日 2014年3月3日, 採録日 2014年9月12日

概要：spam 対策技術の 1 つである 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，適用するすべ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配送遅延が生じる．我々が運用しているメールサーバにおいても通常メールを受信するまでに平均 1 時間 15 分の遅延が生じていた．通常メール送信者を whitelist に登録すれば，そこからのメールの配送遅延は回避できる．しかしすべての通常メール送信者を whitelist に登録するのは不可能である．そこで 2012 年 2 月に milter manager を導入し，SPF，S25R の判定結果を用いて greylisting を適用するかを決定するメールシステムを構築した．SPF，S25R を用いて通常メールと spam を分類することで，SPF，S25R による検査のみで受信できるメールが増え，greylisting による再送を抑制できる．milter manager 導入前と導入後の通常メールに対する greylisting の再送要求割合を比較し，43.1%から 17.0%まで減少していたことを確認した．このことから，milter manager を用いて milter を組み合わせることで，通常メールに対する配送遅延を軽減することに成功した．

キーワード：spam，milter，greylisting，配送遅延，milter manager

Design for an Anti-spam Mail Server with Low Delivery Delay by the Incorporation of Milter and Its Operational Results

Kazuno Matsui[1,a)] Hajime Kanetaka[1,†1] Mayumi Kaku[2,†2] Minoru Ikebe[2] Kazuyuki Yoshida[3]

Received: March 3, 2014, Accepted: September 12, 2014

Abstract: Greylisting is a type of anti-spam measure. Greylisting works by assuming that contrary to legitimate MTA, a spam sender will not retry sending their junk mail after a temporary error. Greylisting is a low cost method with high detection rates, but it introduces a delay into legitimate mail delivery. In fact, the average delay of e-mail delivery was 1 hour and 15 minutes after sending in our mailing system. Although to put ham MTAs in whitelist reduces e-mail delivery delay, it seems impossible to register all ham MTAs. Therefore, we designed a new mail delivery system using milter manager in February 2012. The mail system uses the results of SPF and S25R in order to apply greylisting to mail classified as spam by either of those milters. As a result, legitimate mail is receivable without the delay from greylisting from before. We compared the retransmission request rates by greylisting before and after the introduction of the system. As a result, we have successfully reduced the retransmission request ratio of greylisting from 43.1% to 17.0% in our system. We succeeded in reducing the average delay of delivery of legitimate mail by the combination of the milters through milter manager.

Keywords: spam, milter, greylisting, delivery delay, milter manager

1. はじめに

インターネットの普及と発展にともない，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．これにともない，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に送信される電子メールを指す．現在，インターネットを流れる電子メールの約 64%が spam である [1]．spam による被害の例には，フィッシング詐欺やメールに添付されたファイルによるウイルス感染などがある [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 対策をすることが求められている．

spam 対策の 1 つに greylisting がある．greylisting は spam 排除の効果が高く，誤検知が少ない．しかし，適用するメールに再送を要求するため，greylisting を適用する通常メールに対して配送遅延を招く問題がある [3]．greylisting の適用にともなう通常メールに対する配送遅延の発生を回避するには，一般的に whitelist に通常メール送信者を登録する方法がある．whitelist に通常メール送信者を登録することで，greylisting を適用せずに受信することができる．しかし，whitelist はメールサーバの管理者が手動で管理し，メール送信者の追加や削除をするため，管理者にとって大きな負担となる [4]．大分大学においても，whitelist に通常メール送信者を登録することで，通常メールに対する greylisting の適用を回避させている．whitelist の作成には，我々が先行研究として開発，運用してきた whitelist 自動作成システムを用いている [5]．しかし，whitelist 自動作成システムの登録条件に一致する spam 送信 MTA（Mail Transfer Agent）があるため，spam 送信元となっている MTA を誤登録していないか管理者は確認する必要があり，whitelist のメンテナンスに手間がかかる．

そこで我々は milter manager [6] を用いて，SPF，S25R の結果をもとに greylisting の適用の有無を決定するメールシステムを構築した [7]．milter manager を用いて milter に対応した複数の spam 対策を組み合わせることで，各 spam 対策の利点を活かしつつ欠点を補うことができる．また，各 spam 対策の結果をもとに greylisting の適用を決定するため，whitelist に記載のない通常メール送信者からの通常メールであっても，配送遅延を低減させることができる．本論文では，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 適用数と再送要求数の比較，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．また，システムの誤検知や検知漏れの調査，システムの導入に関して，考察する．

本論文の構成は以下のとおりである．まず，2 章で従来の大分大学のメールシステム構成について述べ，3 章で関連研究について述べる．そして，4 章で低配送遅延を目指して構築したメールシステムについて説明する．5 章で運用結果について述べ本システムの有効性を示す．6 章で運用結果に対する考察を与える．7 章でまとめと今後の課題について述べる．

2. 従来の大分大学のメールシステム構成

2.1 システム構成

大分大学のメールシステムの構成を図 **1** に示す．大分大学のメールシステムでは，まずメールゲートウェイにおいて iptables [8] の NAPT（Network Address Port Translation）機能を用いて whitelist を参照し，登録されていない MTA からのメールは 25 番ポートのプロセス 1，登録されている MTA からのメールは 26 番ポートのプロセス 2 へ振り分ける [9]．iptables はパケットフィルタリング機能と NAPT 機能を提供する．whitelist は我々が開発した whitelist 自動作成システムを使用して作成する．図 1 に示すようにプロセス 1 では greylisting をはじめとして様々な spam 対策を実施する．一方，プロセス 2 ではメールサーバの管理者が信頼できる 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，

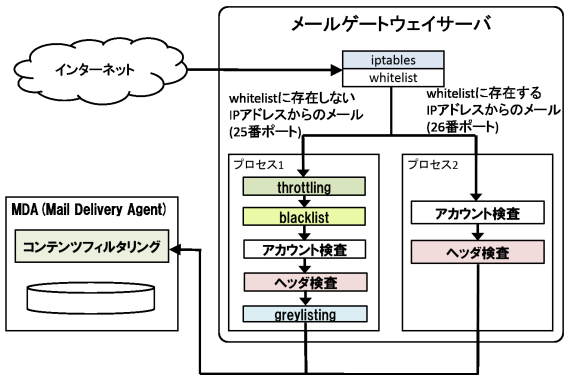


図 **1** メールシステムの構成

Fig. 1 Overview of mail system in Oita University.

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, Oita 870–1192, Japan
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, Oita 870–1192, Japan
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, Oita 870–1192, Japan
†1 現在，富士通株式会社
Presently with Fujitsu Limited
†2 現在，株式会社インフォセンス
Presently with infoSense corporation
a) v13e3022@oita-u.ac.jp

本論文の内容は 2013 年 7 月のマルチメディア，分散，協調とモバイル（DICOMO2013）シンポジウム 2013 にて報告され，インターネットと運用技術研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

Sendmail [10] 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．これらの対策後，メールは MDA（Mail Delivery Agent）へ送られ，コンテンツフィルタリングによるチェックの後，ユーザへ配送される．

2.2 spam 対策手法

本節では大分大学において利用している spam 対策を述べる．

2.2.1 greylisting

greylisting [11] は tempfailing 手法の 1 つで，「spam 発信 MTA は再送をしない」との仮説に基づいた対策手法である．一時的に受信を拒否し，一定時間は再送されたメールを受けずに，一定時間経過後に再送されたメールのみを受信する．再送した MTA は一定期間 greylisting の autowhitelist に登録される．再送されたメールの受け取り開始時間は受信者側が設定する．autowhitelist に登録されていれば，greylisting を適用しても再送要求はせず，すぐにメールを受信する．

多くの spam 発信 MTA は短時間に大量の spam を送信することを重視するので，再送要求には応じないことが一般的であるため，greylisting による spam 排除の効果が高い．しかし，送信元 MTA に対して再送を要求するため配送遅延が大きくなり，送信元 MTA の再送間隔の設定によっては，1 時間以上の遅延が発生する場合もある．

2.2.2 throttling

throttling とは「spam 発信 MTA はメール送信時の SMTP（Simple Mail Transfer Protocol）処理において応答が戻ってくるまでに許容される時間が短い」，「spam 発信 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わざと遅延させ，送信 MTA 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 と分類して受信を拒否する対策手法である [12]．throttling は遅延時間のみをパラメータとして設定する．しかし，throttling は TCP コネクションを保持したまま待機するため，受信 MTA のプロセス数，TCP セッション数が増加しやすく，サーバのリソースを消費してしまうという問題がある．

2.2.3 blacklist

blacklist とは，spam 送信 MTA の IP アドレスを登録したリストである．メールの送信者と受信者の間に TCP コネクションが確立したときに，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対策である．代表的な blacklist は SpamCop [13] や RBL.JP [14]，Spamhaus [15] がある．

2.2.4 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 からのメールであっても，spam 対策において spam と誤検知するケースが存在する．そのため，spam 対策で誤検知される通常 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．大分大学においては，すべてのメールに greylisting を適用すると，メール受信までに遅延が生じるため，信頼できる MTA の IP アドレスを whitelist に記載している．whitelist に記載された MTA から送信されるメールは spam 対策を省くことで，通常メールを遅延なく受信できる．

2.2.5 アカウント検査

アカウント検査とは，SMTP の「RCPT」コマンドによって送られてくる受信者のメールアドレスをチェックし，アカウント（メールアドレスにおける@の左側）が存在するならば受信し，存在しなければ宛先不明エラーとして受信拒否する対策である．大分大学においては LDAP（Lightweight Directory Access Protocol）を利用して，アカウントの有無を確認している．アカウント検査をすることで，宛先不明メールを早い段階で拒否できる．

2.2.6 ヘッダ検査

spam は，ヘッダと呼ばれるメールの付加情報が不完全であることが多く，ヘッダ形式を調べることで spam を判別できる．大分大学では Messege-ID，From の各ヘッダの形式が＜ローカル部@ドメイン部＞の形式でないメールは拒否する．To のヘッダ形式についてはアカウント検査でチェックしているため，ヘッダ検査では対象としていない．

2.2.7 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対策である．代表的なコンテンツフィルタリングは SpamAssassin [16] や bsfilter [17] がある．コンテンツフィルタリングではメールを送信する際の挙動だけでは通常メールと見分けのつかない spam でも，メールヘッダや本文に spam の特徴があれば排除できる．しかし，メールヘッダや本文を解析するため，他の spam 対策よりサーバのリソースを多く要し，サーバに大きな負荷がかかる．また，spam の検出率を向上させるためには大量の spam による学習が必要となり，学習データが増えるにつれ，サーバにかかる負荷が大きくなる．

2.2.8 whitelist 自動作成システム

whitelist 自動作成システムでは，2 つの登録条件のどちらかに該当した MTA を whitelist に登録する．(1) greylisting の再送要求に応答のあった MTA の IP アドレスに対して IP アドレスを逆引きし，得られた FQDN（Fully Qualified Domain Name）と送信元メールアドレスのドメインが後方一致した MTA を whitelist に登録する．(2) greylisting の再送要求に応答のあった MTA のうち，SPF（Sender Policy Framework）の認証に成功した MTA を whitelist に登録する．2011 年 2 月 2 日から前者を用いた whitelist の登録を開始し，2012 年 1 月 10 日から前者に加えて後者も用いた

whitelistの登録を開始した．whitelist自動作成システムの運用によって，2011年2月2日から2012年1月15日の運用期間中にwhitelistの登録件数は1,546件から15,426件に増加した．その結果，whitelist自動作成システム運用前後1カ月でgreylistingを適用する通常メールの割合を比較すると，56%から半分の27%まで減少した．

2.3 メールシステムの問題点

greylistingは2.2.1項で述べたように，autowhitelistに記載のないすべてのメールに再送要求するため，通常メールであっても配送遅延が発生するという問題がある．大分大学のメールシステムを2011年11月27日から2012年1月22日まで調査した結果，多くのspam対策を実施するプロセス1に振り分けられたメールでは平均1時間15分の配送遅延が生じていた．

通常メール送信者に対するgreylistingの適用を回避するために，whitelistへ登録する方法がある．しかし，whitelistへの登録は，greylistingに対して再送している通常メール送信者の調査などがあり，管理者が手動で登録する通常メール送信者の確認をするため，大きな負担となる．そのため，大分大学ではwhitelist自動作成システムによって，通常メール送信者をwhitelistに登録している．しかし，2.2.8項で述べたようにwhitelist自動作成システムの登録条件に一致するspam送信MTAがあるため，whitelist自動作成システムを用いた場合，メールサーバの管理者はspam送信者を誤登録していないかwhitelistを確認し，更新する必要がある．

3. 関連研究・関連システム

greylistingの再送要求にともなう配送遅延を低減させるには，通常メールに対するgreylistingの適用を回避させる方法や，SMTPセッションを強制的に切断する方法が提案されている．

3.1 通常メールに対するgreylistingの適用を回避させる手法

通常メールに対するgreylistingの適用を回避させる方法には，陳らの提案手法やS25RとgreylistingをRgrey，S25RとtarpittingをtaRgreyや石島らの提案手法がある．

陳ら[18]は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，DHCP（Dynamic Host Configuration Protocol）によって動的に割り当てられたIPアドレスからのメールなど4つの条件によってspamを排除している．また，どの条件にもあてはまらなかったメールでも信頼できるホスト以外からのメールはgreylistingを適用する．greylistingの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を適用せずにただちに受信する．しかし，固定IPアドレスを持たないMTAからのメールや，再送するたびに送信元サーバを変えて送信されるメールも存在するため，この手法では通常メールにもかかわらず受信できない可能性がある．

Rgrey[19]はS25Rによりspamと分類されたメールのみに対してgreylistingを適用する手法であり，taRgreyはtarpittingとS25Rの両方でspamと分類されたメールのみに対してgreylistingを適用する手法である．どちらの手法も再送要求をしない配送遅延の少ないspam対策を用いてメールを分類しているため，通常メールはgreylistingを適用せずに受信することが可能である．しかし，tarpittingは2013年3月時点で，大分大学における spam排除率が0.1%となっておりspamの排除数が少ないため，現在tarpittingは有効なspam対策とはいえない．また，S25Rについても2013年3月時点で大分大学においてgreylistingの再送要求に応答しなかったspamのうち，42.6%を検出できておらず，S25Rの適用結果のみでメールを受信することは，検知漏れを増加させる可能性がある．そのため，RgreyやtaRgreyではspamの検知漏れが生じる可能性がある．

石島ら[20]はユーザが活動する日中はメールにthrottlingを適用し，ユーザがメールを使用しない夜間のみ，greylistingとthrottlingを併用する手法を提案した．この手法を用いることで，日中に届くメールはgreylistingを適用しないため遅延なく受信できる．また，夜間はthrottlingと併用してgreylistingを使用するため，spam排除の効果も高い．しかし，この手法を用いた場合夜間に比べ，throttlingのみを適用する日中のspam受信数が多い．大分大学においてもthrottlingをspam対策に組み込んでいる．しかし，ほかのspam対策と比べると排除数が少ない．2006年時点では半数のspamを排除しているが，現在throttlingは有効なspam対策とはいえない．そのため，石島らの手法では日中にspamを受信する数が多くなるという問題がある．

上記の4つの手法では，通常メールに対するgreylistingの適用を回避させているが，通常メールを拒否したり，ユーザが受信するspam数が多くなったりしてしまう．

3.2 SMTPセッションの強制切断を用いた手法

SMTPセッションを強制的に切断する方法は，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．PMGに接続を試みた送信者のリストをSMGに渡すことで，再送されたメールのみを受け取ることが可能である．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できる．山井ら [21] は，ヘッダあるいはメッセージ全体を受信後に SMTP セッションを切断することで，異なる MTA からの再送への対処および誤検知されたメールの回復を可能とした．また，北川ら [22] は，PMG に対する 1 回目の SYN パケットに応答せず，再送された SYN パケットに対して RST パケットを返し，コネクションを強制切断する手法を提案した．2 回目の SYN パケットに応答することで PMG に接続を試みた送信者のリストを SMG に渡す時間を確保している．

どちらの手法も SMTP セッションを強制的に切断することで greylisting と同等の効果を得られ，さらに配送遅延を削減することに成功している．しかし，2 つの MTA を準備するため，既存のメールシステムに導入するには，システム構成を大きく変更する必要がある．

4. 低配送遅延を目指したメールシステム

本研究では，milter manager を用いて spam 対策を組み合わせることで通常メールにかかる配送遅延の削減を目指す．milter manager の導入にあたり，通常メールと spam を振り分けて，遅延の原因となる greylisting が不必要に適用されている通常メールを減らすために，SPF，S25R を新たに追加した．milter manager を用いて各 spam 対策の結果をもとに greylisting の適用を決定する．これにより，whitelist に登録されていない通常メール送信者からのメールであっても，配送遅延を低減させることが可能である．そのため，本システムでは whitelist に依存せずに配送遅延の発生するメールの数を抑制できる．

4.1 milter manager

milter manager [6] は複数の milter を管理する milter である．通常，複数の milter を利用する場合には，**図 2** に示すように各メールに対して登録したすべての milter を順に適用する．milter manager を用いることで**図 3** 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，メールによって適用する milter を変更できる．そのため，milter manager を用いて milter に対応した複数の spam 対策を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うことができる．

4.2 SPF

SPF（Sender Policy Framework）[23] 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詐称を防ぐ送信ドメイン認証方式である．SPF はメール受信時に，メールが送信者の持つメールアドレス（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

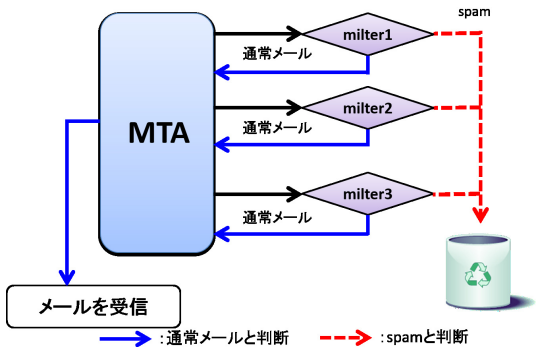


図 2 milter の適用例
Fig. 2 Example of the application of milter.

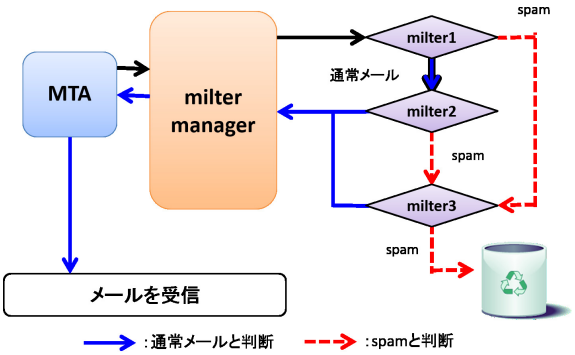


図 3 milter manager を用いた milter の適用例
Fig. 3 Example of the application of milter using milter manager.

example.jp. IN TXT " v=spf1 +ip4:192.168.100.0/24 -all"
ex.com. IN TXT " v=spf1 +ip4:192.168.150.0/24 +all"
spf.jp. IN TXT " v=spf1 +ip4:192.168.200.0/24 ~all"

図 4 SPF レコードの記述例
Fig. 4 Description examples of SPF records.

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．同時にその他の MTA からメールの送信があった場合の判定を SPF レコードの末尾に「記号 (+，-，~)all」の形式で記述する．「+all」は当該ドメインの送信 MTA として認証（pass），「-all」は拒否（fail），「~all」は当該ドメインの送信 MTA ではないが，通常 MTA の可能性があることを示す（softfail）．SPF レコードの記述例を**図 4** に示す．たとえば，図 4 の example.jp の SPF レコードの場合「-all」なので，192.168.100.0/24 のネットワークから送信されたメールは，自ドメインからのメールであるため認証成功とし，それ以外のネットワークからのメールは認証拒否とする．**図 5** に SPF による送信者認証の流れを示す．

（1）example.jp からのメールを example.com（受信 MTA）が受信
（2）example.jp の SPF レコードを ns.example.jp（権威 DNS サーバ）へ問い合わせる．

表 1 S25R のルール
Table 1 S25R rules.

pass	FQDN が以下の S25R のルールセットと一致しない
逆引きなし	FQDN が設定されていない
rule1	FQDN の最下位の名前が，数字以外の文字列で分断された 2 つ以上の数字列を含む
rule2	FQDN の最下位の名前が，5 個以上連続する数字を含む
rule3	FQDN の上位 3 階層を除き，最下位または下位から 2 番目の名前が数字で始まる
rule4	FQDN の最下位の名前が数字で終わり，かつ下位から 2 番目の名前が，1 個のハイフンで分断された 2 つ以上の数字列を含む
rule5	FQDN が 5 階層以上で，下位 2 階層の名前がともに数字で終わる
rule6	FQDN の最下位の名前が「dhcp」，「dialup」，「ppp」，または DSL 系の名前（「dsl」，「adsl」など）で始まり，かつ数字を含む

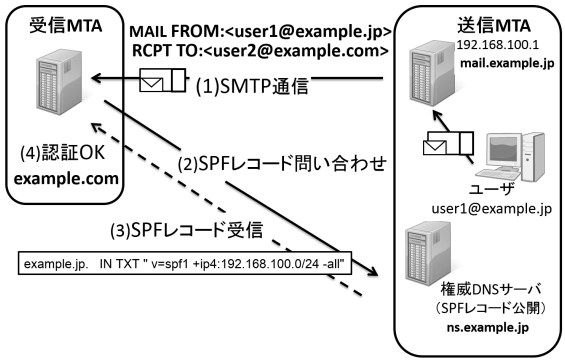


図 5 SPF による送信ドメイン認証
Fig. 5 Sender domain authentication using SPF.

(3) example.jp の SPF レコード受信.
(4) SMTP 接続元（送信 MTA）の IP アドレスと取得した SPF レコードに記載された IP アドレスが一致すれば送信ドメインを認証（pass），一致しない場合は認証失敗（fail）.

SPF を利用することで，ドメインを詐称して送信される spam を排除できる．しかし，SPF はメールを転送した場合や，メーリングリストから配送されるメールを spam として誤検知することがある．たとえばメールを転送する際，送信元の IP アドレスはメールサーバによって書き換えられるが，送信者のメールアドレスは書き換わらないためそのまま転送される．よって，転送前の送信者のメールアドレスから SPF レコードを取得するため，送信 MTA の IP アドレスが一致せず，誤検知する．

4.3 S25R

Symantec 社の調査報告 [24] によると，2011 年に送信された 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 を排除する対策の 1 つに S25R（Selective SMTP Rejection）[25] がある．S25R は接続してきた MTA の FQDN を S25R のルールと照合し，エンドユーザコンピュータであるかどうかを推定し，SMTP アクセスを拒否する．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．また，エンドユーザコンピュータに対して FQDN が設定されていることがあるが，IP アドレスの下位 16 ビットに相当する数字など管理上の便宜のための数字を含むことが多い．

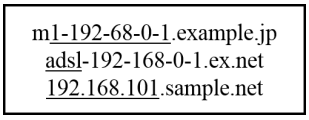


図 6 S25R で検知可能な FQDN の例
Fig. 6 Examples of detectable FQDN in S25R.

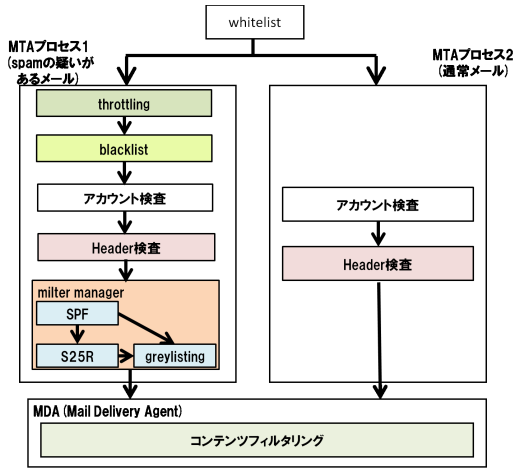


図 7 milter manager を用いたメールシステムの構成
Fig. 7 Mail system overview using the milter manager.

表 1 に S25R のルールセット，**図 6** に S25R で検知可能な FQDN の例を示す．S25R では，エンドユーザコンピュータからの spam をほとんど検出できる．しかし，通常の MTA の中にも，S25R の規則に該当する 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からの spam と誤検知する．

4.4 低配送遅延を目指したメールシステムの設計

低配送遅延を実現するために設計，構築した milter manager を用いたメールシステム全体の構成を**図 7**，milter manager を用いた spam 対策の適用順序を**図 8** に示す．図 7 のように，SMTP に準拠しない挙動をする MTA からのメールを拒否するための throttling と greylisting，spam

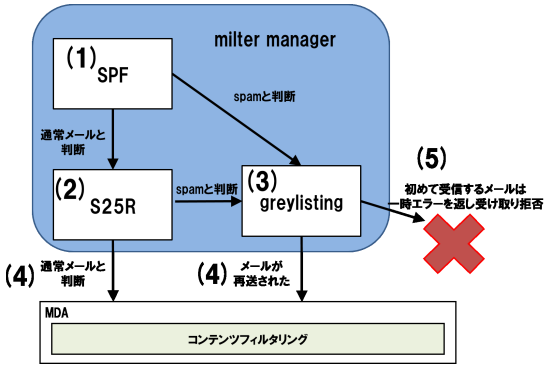


図 8 milter manager を用いた spam 対策の適用順序

Fig. 8 The application order of the anti-spam methods using milter manager.

送信者の IP アドレスを列挙した blacklist，ヘッダ情報に不備のあるメールを拒絶するアカウント検査とヘッダ検査を組み合わせることで，挙動の異なる spam の多くを排除できる．

また本システムでは，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とおりである．

（1）SPF を適用．
（2）SPF の認証に成功した場合，S25R を適用．
（3）SPF の認証に失敗した場合，あるいは S25R によって spam と分類された場合に greylisting を適用．
（4）S25R によって通常メールと分類した場合，あるいは greylisting において再送メールであった場合は MDA（Mail Delivery Agent）へ配送．
（5）greylisting において初めて受信するメールは一時エラーのレスポンスコードを返し，メールを拒否．

図 8 に示す順序で spam 対策を適用することで，通常メールは SPF，S25R を通過し，MDA に配送するため，greylisting による再送遅延の影響を受けない．また，SPF，S25R で誤検知した通常メールは greylisting によって救済できる．

5. 運用結果

5.1 調査方法

milter manager を導入したメールサーバによる配送遅延低減の調査期間は 2012 年 12 月 30 日から 2013 年 3 月 30 日までの 3 カ月間である．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，導入する前の期間から，比較的 spam 割合が近い 2011 年 6 月 26 日から 2011 年 9 月 25 日までの 3 カ月間と比較した．システムは 2012 年 1 月から運用を開始していたが，運用開始後しばらくは設定を調整していたため，安定運用を始めた 2012 年 12 月から調査した．メールに適用した spam 対策を調査するために，調査対象をメールログから抜粋し，SPF と S25R，greylisting の処理結果を集計した．本論文では通常メールに対する配送遅延とシステムの検知漏れ，SPF と S25R の誤検知の観点から調査した．通常メールに対する配送遅延を 5.3 節，システムの検知漏れを 5.4 節，SPF と S25R の誤検知を 5.5 節で述べる．調査対象は大分大学宛に送信されたメールである．また，2 つの調査期間では whitelist の登録件数が異なる．milter manager 導入後の運用期間における whitelist 登録件数は 15,426 件である．milter manager 導入前の運用期間では whitelist 自動作成システムの運用期間内であり，whitelist の最大登録数は 8,735 件，最小登録数は 5,660 件である．milter manager 導入前の whitelist 登録件数の遷移を**図 9** に示す．milter manager 導入後の運用期間は，whitelist 自動作成システムを用いて whitelist に MTA の登録をしていないため，whitelist の登録件数に変化はない．

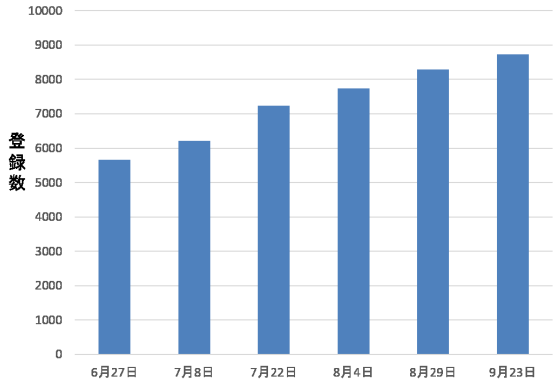


図 9 whitelist 登録件数の遷移
（2011 年 6 月 27 日～9 月 23 日）

Fig. 9 Transition of the number of IP addresses in whitelist (from June 27, 2011 to September 23, 2011).

表 2 メールシステム全体でのメール受信数
（2012 年 12 月 30 日～2013 年 3 月 30 日）

Table 2 The number of recieved mails in our email system (from December 30, 2012 to March 30, 2013).

プロセス	総受信数	通常メール数	spam 数
プロセス 1	2,022,057 通	663,411 通	1,358,646 通
プロセス 2	2,213,828 通	1,608,458 通	605,370 通
合計	4,235,885 通	2,271,869 通	1,964,016 通 (A)

5.2 メールシステム全体の調査結果

メールシステム全体のメール受信数を**表 2**，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 3**，MTA プロセス 2 の各 spam 対策での spam 排除数を**表 4** に示す．表 2 のシステム全体でのメール受信数をみると，通常メールの半数以上は whitelist に登録されているため MTA プロセス 2 が処理している．また，表 3，表 4 に示すように MTA プロセス 1 では blacklist や greylisting で排除される spam が多い．MTA プロセス 2 で検出した spam のうち 26.1%が，アカウント検査で排除

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

Table 3 The number of eliminated spam by each anti-spam method in MTA process 1
(from December 30, 2012 to March 30, 2013).

spam 対策	排除数 (B)	spam 排除割合 B ÷表 2 (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%
ヘッダ検査	161,478 通	8.2%
greylisting	511,859 通	26.4%
合計	1,358,646 通	69.3%

表 4 MTA プロセス 2 の各 spam 対策での spam 排除数
（2012 年 12 月 30 日～2013 年 3 月 30 日）

Table 4 The number of eliminated spam by each anti-spam method in MTA process 2
(from December 30, 2012 to March 30, 2013).

spam 対策	排除数 (B)	spam 排除割合 B ÷表 2 (A)
アカウント検査	425,565 通	21.6%
ヘッダ検査	179,805 通	9.1%
合計	605,530 通	30.7%

される spam であった．これは信頼できる MTA から送られたメールであっても，宛先を間違えていたり，大学を修了し，すでに登録が抹消されたユーザ宛のメールであった．

5.3 節以降では調査対象を，MTA プロセス 1 で spam 対策を受けたメールとする．本論文では図 7 の MTA プロセス 1 で運用をしている milter manager を用いた spam 対策の組合せの効果について調査する．そのため，通常メールを扱う MTA プロセス 2 は調査の対象から除外する．

5.3 調査 (1) 配送遅延の低減

milter manager を用いた spam 対策の効果を調べるために，通常メールに対する配送遅延を指標として調査した．通常メールに対する配送遅延の評価として，greylisting 適用数と再送要求数を調査した．greylisting 適用数と再送要求数が減少すれば，再送要求にともなう配送遅延がかかる通常メール数が減ることになる．配送遅延がかかる通常メール数が減少すれば，システム全体では通常メールに対する配送遅延が低減されたといえる．この調査において，通常メールは MDA が受信したメール，spam は greylisting の再送要求に応答しなかったメールとする．調査 (1) での調査対象は大分大学宛に送信されたメールのうち，MTA プロセス 1 で spam 対策の処理が適用されたメールである．MTA プロセス 1 の受信メール数を**表 5**，greylisting 再送要求数を**表 6**，メールの平均遅延を**表 7**，milter manager 導入後の通常メールが処理を受けた spam

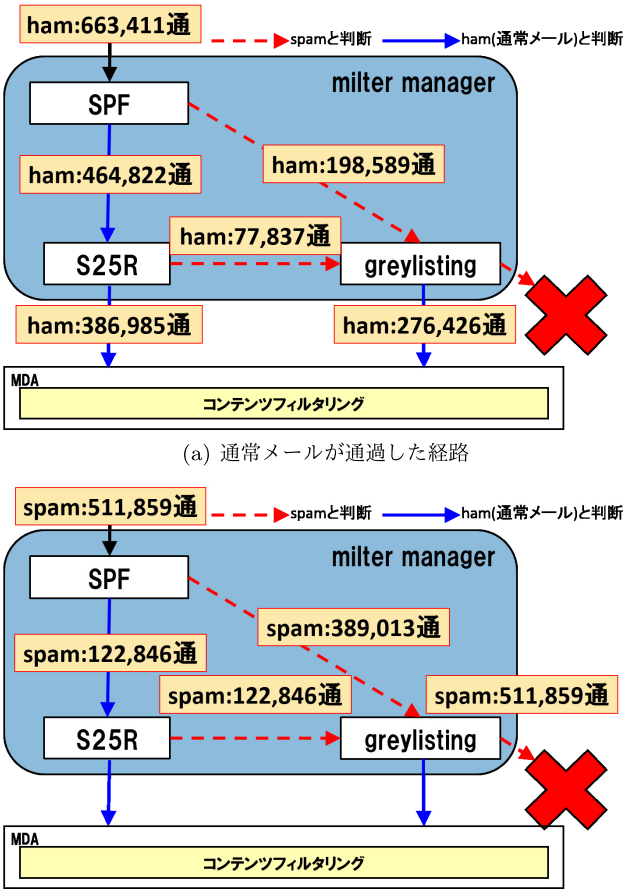


図 10 通常メールと spam が通過した経路

Fig. 10 The route of emails and spam in our mail system.

対策のルートと処理メール数を**図 10** (a)，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 10 (b) に示す．表 5 に示す milter manager を用いたシステムの運用前後において受信したメールを比較すると，greylisting の適用割合が 64.3%から 38.9%に減少していた．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，31%にあたる 276,426 通は通常メールであった．このことから，SPF，S25R で誤検知された通常メールを，greylisting を適用することで救済できた．また，図 10 (a) に示すように通常メール全体の 58%にあたる 386,985 通は SPF，S25R を pass しており，greylisting を適用していない．

しかし，greylisting の autowhitelist に記載された送信者は greylisting を適用しても再送要求しない．greylisting 適用率には，autowhitelist に記載され再送要求していない送信者も適用数に含まれている．よって，greylisting 適用率が高くても autowhitelist に記載されている送信者が多ければ実際に再送要求されたメール数は少なくなる．そのため，greylisting 適用率だけでは通常メールにかかる配送遅延の低減を確認できたことにはならない．そこで greylisting の

表 5 MTA プロセス 1 が受信したメール数
Table 5 The number of received mails in MTA process 1.

期間	総受信数 (C)	通常メール数 (D)	spam 数 (E)	spam 割合 (C/E)	greylisting 適用数 (F)	greylisting 適用割合 (F/C)
2011 年 6 月 26 日 ～2011 年 9 月 25 日（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 月 30 日 ～2013 年 3 月 30 日（運用後）	2,022,057 通	663,411 通	1,358,646 通	67.2%	788,285 通	38.9%

表 6 greylisting の再送要求数
Table 6 The number of retransmission request by greylisting.

期間	再送要求したメール数	autowhitelist 登録メール数	再送要求に応答したメール数 (G)	再送要求に応答しなかったメール数	通常メール再送要求割合 (G/表 5 (D))
2011 年 6 月 26 日 ～2011 年 9 月 25 日（運用前）	862,568 通	294,659 通	202,114 通	660,454 通	43.1%
2012 年 12 月 30 日 ～2013 年 3 月 30 日（運用後）	624,694 通	163,591 通	112,835 通	511,859 通	17.0%

表 7 メールの平均配送遅延
Table 7 Average delay of emails.

期間	通常メール数	合計配送遅延時間	平均配送遅延時間
2011 年 6 月 26 日～2011 年 9 月 25 日（運用前）	2,205,182 通	928,412,242 秒	421 秒
2012 年 12 月 30 日～2013 年 3 月 30 日（運用後）	2,271,869 通	140,141,246 秒	62 秒

再送要求数について調査した．表 6 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 17.0%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．通常メールの平均配送遅延時間を調査したところ，表 7 に示すように運用前と運用後では，421 秒から 62 秒まで減少した．よって，milter manager を用いて milter を組み合わせることにより通常メールにかかる配送遅延を低減できたことを確認した．

5.4 調査 (2) 検知漏れ

提案システムによる spam 検知漏れを調査するために，コンテンツフィルタリングで検出された spam 数を指標として調査した．ここでは，コンテンツフィルタリングで spam に分類されたメールを spam，通常メールに分類されたメールを通常メールとする．milter manager 運用前後のコンテンツフィルタリングで検出した spam 数の調査結果を**表 8** に示す．コンテンツフィルタリングは MDA で実施される spam 対策である．また，導入後の検知漏れした spam の SPF と S25R，greylisting の処理結果を集計することで spam が通過したルートを調査した．調査結果を**図 11** に示す．表 8 に示すように milter manager 運用前後では検知漏れ率が 6.2%から 13.5%に増加している．提案システム運用後の調査期間外にあたる 2012 年 7 月 29 日から 8 月 26 日までの約 1 カ月の spam 検知漏れを調査し

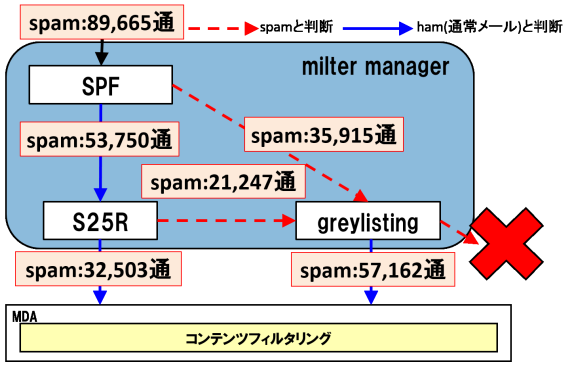


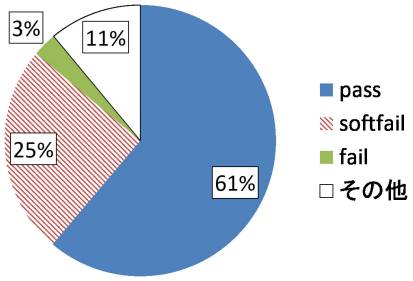
図 11 コンテンツフィルタリングで検出した spam が通過したルート
Fig. 11 The route of detected spam by the content filtering.

たところ，運用前に近い 5.8%の割合で検知漏れが発生していることが分かった．これらの検知漏れは受信する spam の種類に影響される可能性が高いと考えられる．通常メール送信者も利用するフリーメールや SMTP に準拠した挙動をする spam 送信 MTA から送られた spam に関しては，メールを送信する際の挙動が，通常メールと同じためメールを送信する際の挙動だけでは spam と分類することは困難である．

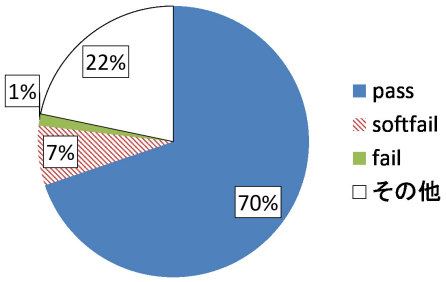
大分大学のメールシステムにおけるコンテンツフィルタリングでの分類結果はログに記載されるが，実際にメールの本文をみて検知漏れを調査できない．そのため，今回の調査では，コンテンツフィルタリングの検知漏れや誤検知

表 8 コンテンツフィルタリングで検出した spam 数
Table 8 The number of emails detected as spam by the content filtering.

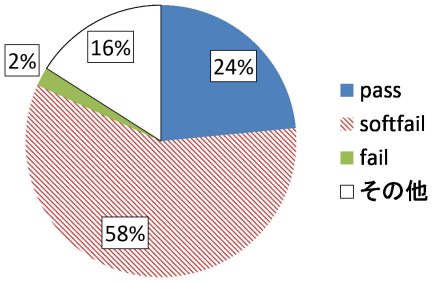
期間	適用メール数 (H)	spam 数 (I)	検知漏れ率 (I/H)
2011 年 6 月 26 日～2011 年 9 月 25 日（運用前）	496,043 通	30,755 通	6.2%
2012 年 12 月 30 日～2013 年 3 月 30 日（運用後）	663,411 通	89,665 通	13.5%
2012 年 7 月 29 日～2012 年 8 月 26 日（運用後（調査期間外））	449,454 通	26,280 通	5.8%



(a) MTA プロセス 1 の SPF 認証結果

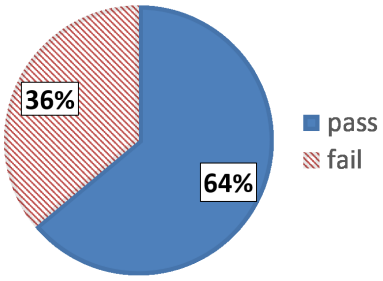


(b) 通常メールの SPF 認証結果

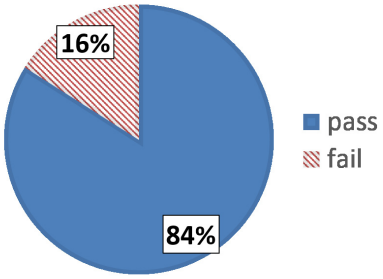


(c) spam の SPF 認証結果

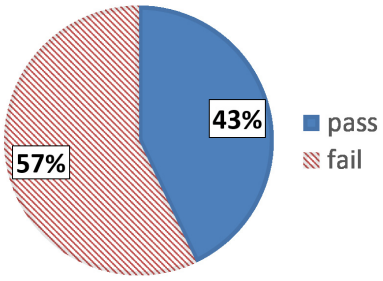
図 12 SPF の認証結果
Fig. 12 Authentication result by SPF.



(a) MTA プロセス 1 の S25R の適用結果



(b) 通常メールの S25R の適用結果



(c) spam の S25R の適用結果

図 13 S25R の適用結果
Fig. 13 Decision result by S25R.

は調査対象外とした．

5.5 調査 (3) SPF・S25R の誤検知

SPF，S25R の誤検知を調査するために，SPF と S25R において spam と分類されたメールのうち，greylisting の再送要求に応答したメールを指標として調査した．調査対象は，MTA プロセス 1 が処理をしたメールのうち，SPF を適用した 1,175,270 通のメールである．このときの通常メールは MDA が受信したメール，spam は greylisting の再送要求に応答しなかったメールと定義する．調査対象となる 1,175,270 通に SPF と S25R を適用した結果を**図 12** と**図 13** に示す．

図 12 (a) に MTA プロセス 1 の SPF の認証結果，図 12 (b) と図 12 (c) に通常メールと spam の SPF の認証結果を示す．ここでは認証結果が pass のメールを認証成功，pass 以外のメールを認証失敗としている．

図 12 (a) に示す MTA プロセス 1 の SPF の認証結果は認証成功を意味する pass が 61%を占めていた．図 12 (b) に示す通常メールの認証結果をみると，70%が認証成功，

残りの30%が認証失敗であった．図12(c)に示すspamの認証結果は，24%が認証成功，残りの76%が認証失敗であった．これらの結果から，SPFの認証結果で多くのメールに関しては通常メールとspamを判別できていた．しかし，通常メールでは30%のメールがspamと誤検知されていた．そのため，SPFの認証結果は通常メールを判別する1つの目安となるが，SPFの認証結果のみで，spamを排除すると通常メールを誤検知する可能性がある．

図13(a)にMTAプロセス1のS25Rの適用結果，図13(b)，図13(c)に通常メールとspamのS25Rの適用結果を示す．表1に示すS25Rのルールセットに一致しなかったメールをpass，一致したメールをfailとした．通常メールのうち，16%はS25Rのルールセットに該当したためspamと誤検知されていた．S25Rに関してもSPFと同様に，通常メールとspamを振り分ける1つの目安になるが，S25Rの結果だけでメールの受信や排除を決定することは誤検知の原因となる可能性がある．

以上の結果から，SPFとS25Rはspamを分類する目安となるが，誤検知が多いことがいえる．そのため，本システムではSPFとS25Rによってspamと分類されたメールをgreylistingに適用することで，SPFによって誤検知した30%，S25Rによって誤検知した16%の通常メールを救済できた．

6. 考察

本章では，実際にmilter managerを導入してから運用するまでに行う作業について考察する．本論文では，milter managerの導入および運用における作業負担，greylistingを利用することで誤検知される通常メール送信者をwhitelistに登録する作業，システム設計の3つについて考察する．

6.1 milter managerの導入および運用における作業負担に関する考察

milterの1つであるmilter managerは，PostfixやSendmailのようなmilterシステムをサポートしているMTAであれば，そのままインストールして使用することができる．そのため，従来のシステムの構成を大きく変更せずに導入することが可能である．各milterの設定はMTAに記述するのではなく，milter managerの設定ファイルにRubyで記述する．そのため，milterの設定をするにはRubyの知識が必要となる．しかしmilter managerの設定方法については，ドキュメントに設定例が示されているため自身でmilterを作るなど特別な場合を除き，ドキュメントを見れば設定できる．

また，本システムではmilter managerを用いてシステムを構築したが，milter-greylistを用いることでも本論文と同様のメールシステムを構築できる．しかしながら，milter-greylistでは組み合わせることができる対策がSPFとS25Rに限定され，他のspam対策を組み合わせることができない．milter managerを用いた場合，spam対策を自由に組み合わせることができる．そのため，システムを再構成するときの拡張性を考慮してmilter managerを用いる手法を採用した．

6.2 whitelistの作成による誤検知の対策

milter managerを運用するうえで，greylistingの再送要求に応答しない通常メール送信者に関しては，greylistingを適用しないようにwhitelistへの登録が必要である．先行研究として開発，運用してきたwhitelist自動作成システムではgreylistingの再送要求に応答し，autowhitelistに記載された通常メール送信者を対象としてwhitelistに登録している．そのため，固定IPアドレスを持たないMTAからのメールや，再送するたびに送信元サーバを変えて送信されるメールなど，greylistingによって誤検知された通常メール送信者をwhitelistに登録することができない．そのため，本論文で想定しているwhitelistの登録作業としては，届くべきメールが届かない場合に受信者や送信者から調査依頼を受けての追加や，管理者がログから誤検知されたメールを調査し作成する作業である．whitelistの作成に関する作業負担は，メールシステムの規模によって異なる．

しかし，今回の調査結果から，通常メール送信者の多くはSPFレコードとFQDNを登録していることが分かった．また，総務省の調査[26]においても，SPF未導入の割合が7.53%となっており，SPFが普及していることが分かる．このことから，greylistingの再送要求に応答しない通常メール送信者であっても，SPFレコードとFQDNを登録していればgreylistingを適用しないため，メールを受信できる．SPFレコードとFQDNを登録していない通常メール送信者に関しては，whitelistを作成する必要がある．

6.3 システムの設計に関する考察

milter managerを用いたメールシステムを設計する場合，milterの適用順序を考える必要がある．milterには，誤検知や検知漏れが多いもの，配送遅延が発生するものなど，それぞれ特徴があるため，その特徴を考慮した適用順序にしなければならない．SPF，S25RはDNSへレコード問合せのみなので，greylistingに比べると処理にほとんど時間がかからないが，5.5節で述べたようにSPFで30%，S25Rで16%の通常メールを誤検知している．そのため，SPFやS25Rでspamの排除を決定すると誤検知の原因となる可能性があるので，誤検知の少ないspam対策と組み合わせる必要がある．図12(a)と図13(a)から，SPFとS25Rでの分類割合はほぼ同一であり，どちらを先に適用してもよいことが確認できた．

また，greylistingのように配送遅延が生じるspam対策を最初に適用すると，通常メールに遅延が発生するため

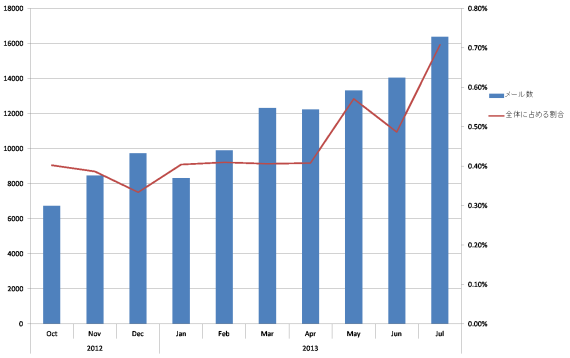


図 14 IPv6 を利用したメール数の遷移
（調査期間 2012 年 9 月 30 日～2013 年 8 月 31 日）

Fig. 14 Transition of the number of emails using IPv6 (from September 30, 2012 to August 31, 2013).

好ましくない．これらのことから，システムを設計するためには，誤検知や検知漏れ，遅延時間など様々な観点から milter を調査し，各 milter の長所を活かしながら，短所を補うことのできる適用順序にする必要がある．また，本研究では用いなかったが，SPF と同様に送信ドメイン認証の 1 つである DKIM（DomainKeys Identified Mail）[27] を用いて spam 対策をする方法もある．DKIM は電子署名を利用して送信者を認証する．SPF が送信元の偽装を検出可能であるのに対し，DKIM では送信元の偽装と，メール本文の改ざんを検出可能であり，さらにメールが転送された場合でも利用できる．しかし，SPF と比較すると 2013 年 9 月時点で DKIM 未導入率 [28] が 74%と高いため，今回は DKIM は利用しなかった．

7. おわりに

本論文では milter の組合せによる低配送遅延を目指した spam 対策メールサーバの運用における効果について述べた．milter manager を用いて milter を組み合わせることで，通常メールに対する再送要求割合が 43.1%から 17.0%まで減少し，平均配送遅延が 421 秒から 62 秒まで減少した．本システムの効果として，通常メールに対する greylisting の再送要求が減少した．また，検知漏れのあった spam は SPF レコードや FQDN を登録している MTA からの spam や，greylisting の再送要求に応答した spam であった．このような MTA から送信される spam は通常メールと同じ挙動でメールを送信するので，メールを送信する際の挙動で spam と分類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ことが望ましい．

また，大分大学のメールシステムを調査したところ，IPv6 を利用したメールの受信を開始した 2012 年 10 月から 12 月までの 3 カ月間で IPv6 を用いたメールが増加していた（**図 14**）．そのため，今後の課題として，IPv6 に対応した whitelist の作成があげられる．現在は iptables の NAPT 機能を用いて whitelist を参照し，各プロセスへメールを振り分けている．しかし，IPv6 用のパケットフィルタリングツールである ip6tables では NAPT 機能がないため，IPv6 を用いて送信されるメールはすべてプロセス 1 へ振り分ける．IPv6 で送信されるメールは，SPF レコードや FQDN が未登録であるケースがある．そのため，現在のシステム構成では IPv6 を用いて送信されたメールのほとんどに greylisting を適用するため，配送遅延が発生している．今後も IPv6 を用いたメールは増加する可能性が高いため，システムの IPv6 対応は課題である．

参考文献

[1] Symantec Intelligence Report，入手先 ⟨http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_02-2014.en-us.pdf⟩（参照 2014-05-19）．
[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)．
[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-DSM-35, pp.19–24 (2004)．
[4] 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-DSM-42, No.8, pp.43–45 (2006)．
[5] 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 2011 論文集，pp.39–44 (2011)．
[6] 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）．
[7] 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，情報処理学会インターネットと運用技術シンポジウム 2012 論文集，pp.8–15 (2013)．
[8] The netfilter.org “iptables” project，入手先 ⟨http://www.netfilter.org/projects/iptables/index.html⟩（参照 2014-05-19）．
[9] 飯田隆義，松竹俊和，吉田和幸：spam 対策用 whitelist を一元管理できるメールシステムとその運用について，情報処理学会研究報告，Vol.2010-IOT-8, No.14, pp.1–6 (2010)．
[10] Sendmail.com，入手先 ⟨https://www.sendmail.com/sm/open_source/⟩（参照 2014-06-17）．
[11] Greylisting.org - a great weapon against spammer，入手先 ⟨http://www.greylisting.org/⟩（参照 2013-05-05）．
[12] 吉田和幸：throttling による spam メール抑制の効果について，情報処理学会研究報告，Vol.2005-DSM-37 (2005)．
[13] SpamCop，入手先 ⟨http://www.spamcop.net/⟩（参照 2013-05-05）．
[14] RBL.JP プロジェクト，入手先 ⟨http://www.rbl.jp/⟩（参照 2013-05-05）．
[15] The Spamhaus Project，入手先 ⟨http://www.spamhaus.org/⟩（参照 2013-05-05）．
[16] Apache Spamassassin Project: Spamassassin，入手先 ⟨http://www.spamassassin.apache.org⟩（参照 2013-05-05）．
[17] Bsfilter.org，入手先 ⟨http://bsfilter.org/⟩（参照 2013-05-05）．
[18] 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)．
[19] K2-net，入手先 ⟨http://k2net.hakuba.jp/⟩（参照 2014-

05-19).
[20] 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, pp.989–997 (2006).
[21] 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).
[22] 北川直哉，高倉弘喜，鈴木常彦：再送動作のリアルタイム検出による spam 判別手法の実装と評価，電子情報通信学会論文誌，Vol.J96-D, No.3, pp.552–561 (2013).
[23] Schlitt, W.: Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, RFC4408 (2006).
[24] 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）.
[25] 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）.
[26] 総務省，送信ドメイン認証結果の集計（SPF），入手先 ⟨http://www.soumu.go.jp/main_content/000266776.pdf⟩（参照 2014-05-27）.
[27] Crocker, D., Hansen, T. and Kucherawy, M.: DomainKeys Identified Mail (DKIM) Signatures, RFC6376 (2011).
[28] 総務省，送信ドメイン認証結果の集計（DKIM），入手先 ⟨http://www.soumu.go.jp/main_content/000266777.pdf⟩（参照 2014-05-27）.

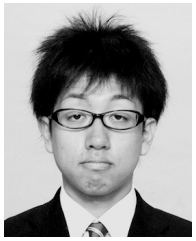
推薦文

本論文は代表的な spam メール対策技術の 1 つである greylisting を適用する際に問題になる再送遅延への対策として，milter manager と呼ばれる機構を利用して事前検査を行い，spam メールの疑いが強いメールだけを対象として greylisting を適用する方法の効果を評価している．spam メールに悩まされている多くの組織にとって参考になる内容であり，有用性が高いと判断できるため，推薦論文に推薦する．

（インターネットと運用技術研究会主査 山井成良）

松井 一乃 （学生会員）

平成 25 年大分大学工学部知能情報システム工学科卒業．同年同大学大学院工学研究科知能情報システム工学専攻博士前期課程に進学し，現在，在学中．ネットワークセキュリティに興味を持つ．



金高 一

平成 24 年大分大学工学部知能情報システム工学科卒業．平成 26 年同大学大学院工学研究科知能情報システム工学専攻博士前期課程修了．現在，富士通株式会社に勤務．

加来 麻友美

平成 26 年大分大学工学部知能情報システム工学科卒業．現在，株式会社インフォセンスに勤務．

池部 実 （正会員）

平成 16 年大分大学教育福祉科学部情報社会文化課程卒業．平成 18 年奈良先端科学技術大学院大学情報科学研究科博士前期課程修了．平成 23 年同大学情報科学研究科博士後期課程修了．同年筑波技術大学保健科学部特任助教を経て，平成 24 年大分大学工学部知能情報システム工学科助教，現在に至る．博士（工学）．インターネット，ネットワーク運用技術，ネットワークセキュリティ，広域分散処理システムの研究に従事．電子情報通信学会，ACM，IEEE 各会員．

吉田 和幸 （正会員）

昭和 54 年九州大学工学部情報工学科卒業．昭和 59 年同大学大学院工学研究科情報工学専攻博士後期課程修了．同年大分大学工学部講師，昭和 61 年同助教授，平成 14 年同総合情報処理センター助教授を経て，平成 20 年同学術情報拠点教授．工学博士．ネットワークの運用技術，セキュリティに関する研究に従事．電子情報通信学会，ソフトウェア科学会，ACM 各会員．