IPv4・IPv6に対応したwhitelistの作成とメールシステムの構築・運用

松井 一乃[1]　山口 舞子[2]　池部 実[2]　吉田 和幸[3]

概要：大分大学では whitelist を利用して通常メールに対する配送遅延を軽減させている．しかし，現在利用している whitelist は IPv6 に対応していないため，IPv6 にて送信されたメールは，多くの spam 対策が適用され，配送遅延が生じていた．また，spam 対策において誤検知され，通常メールにもかかわらず受信できないメールが存在した．そこで本研究では，IPv4・IPv6 に対応した whitelist を DNS にて用いて実装した．DNS を用いたリストの参照方法は，spam 対策のひとつである blacklist で使われている．本研究では blacklist の仕組みを応用して whitelist を実装した．本論文では IPv4・IPv6 に対応した whitelist を用いたメールシステムの構築・運用結果を報告する．

Implementation for an anti-spam mail system with whitelist supported IPv4/IPv6 and its operational results

Kazuno Matsui[1]　Maiko Yamaguchi[2]　Minoru Ikebe[2]　Kazuyuki Yoshida[3]

Abstract: The mail system in Oita University has introduce whitelist for reduction of delivery delay. However, the whitelist is not support IPv6. Therefore, our mail system impose many delay time on legitimate mail system using IPv6. And, our mail system is judged false positive in mail from legitimate mail systems using IPv6 in anti spam measure. In this research, we designed new whitelist system supported IPv4/IPv6 using DNS. Blacklist is one of spam measures. The blacklist references a IP address using DNS. Therefore, we apply the reference method of blacklist to implementation of new whitelist. In this paper, we report new mail system using whitelist supported IPv4/IPv6.

1. はじめに

インターネットの普及と発展に伴い，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 55%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 対策のひとつである 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 の適用に伴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．大分大学では iptables を用いて whtielist を実装している．whitelist に記載のある送信 MTA(Mail Transfer Agent) からのメールは NAPT(Network Address Port Translation) 機能を用いて 26 番ポートへ振り分け，処

[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

© 2015 Information Processing Society of Japan

理している．iptables の IPv6 対応版である ip6tables には NAPT 機能がないため，IPv6 を利用して送信されたメールは，whitelist に登録できず，greylisting によって配送遅延が生じていた．

そこで本研究では DNS(Domain Name System) を用いて IPv4・IPv6 に対応した whitelist を作成し，メールシステムに導入する．DNS を用いたリストの参照方法は，広く普及しており，その仕組みを応用して whitelist を実装した．本論文では，DNS を用いた whitelist の構成，whitelist を導入したメールシステムの運用結果について述べる．本論文の構成は，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 IPv4・IPv6 に対応した whitelist の構成，5 章で whitelist の導入効果について述べ，6 章でまとめる．

2. 従来の大分大学のメールシステム構成

2.1 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．各 spam 対策は，Sendmail[17] 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．

2.1.1 greylisting

greylisting [4] は tempfailing 手法のひとつで，「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．また，再送するたびに異なる MTA からメールを送信するメールシステムも存在する．再送ごとに MTA が変わると，送信 MTA の IP アドレスが前回送信したメールと異なるため，greylisting では再送と判断せず，誤検知する．

2.1.2 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 [5]．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 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，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問題がある．

2.1.3 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コネクションが確立した時に，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[6] や RBL.JP[7]，Spamhaus[8] がある．

2.1.4 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，全てのメールに 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．

2.1.5 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．

2.1.6 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．

2.1.7 milter manager

milter manager[9] 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 1 に示すように各メールに対して登録した全ての milter を順に適用する．milter manager を用いることで図 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，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

© 2015 Information Processing Society of Japan

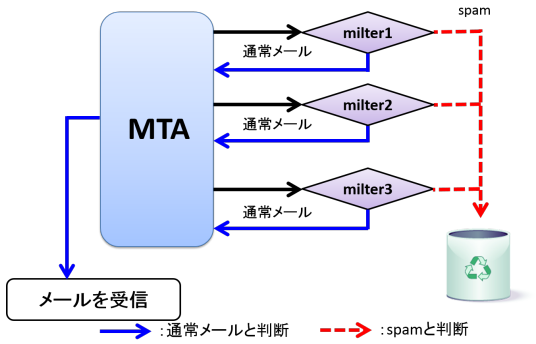

図 1　milter の適用例

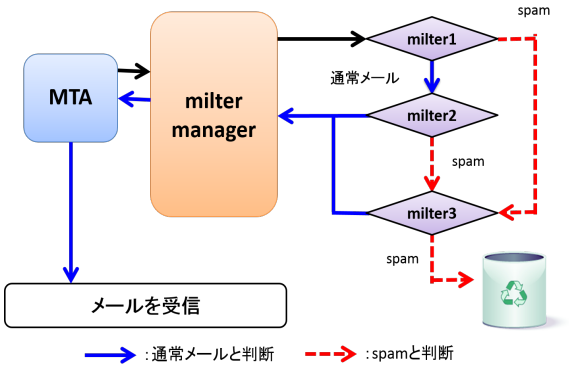

図 2　milter manager を用いた milter の適用例

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 3　SPF レコードの記述例

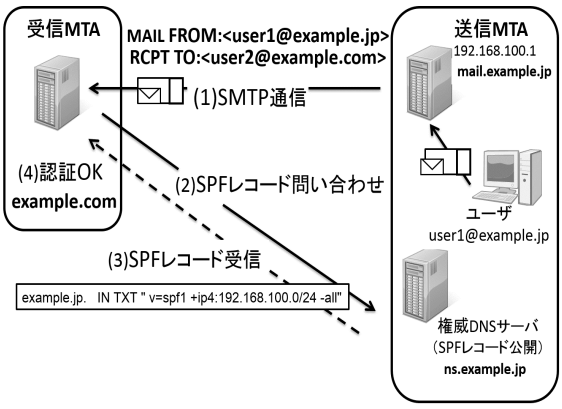

図 4　SPF による送信ドメイン認証

つつ欠点を補うことができる．

2.1.8　SPF

SPF(Sender Policy Framework)[11] 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，メールが送信者のもつメールアドレス（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 3 に示す．例えば，図 3 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 4 に SPF による送信者認証の流れを示す．

m1-192-68-0-1.example.jp
adsl-192-168-0-1.ex.net
192.168.101.sample.net

図 5　S25R で検知可能な FQDN の例

（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．

（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．例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．

2.1.9　S25R

Symantec 社の調査報告 [10] 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 を排除する対策のひとつに S25R(Selective SMTP Rejection)[12] がある．S25R は接続してきた MTA の FQDN を S25R のルールと照合

© 2015 Information Processing Society of Japan

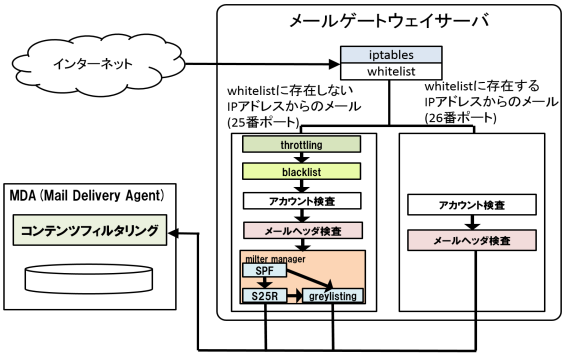

図 6　メールシステムの構成

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 5 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．

2.1.10　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[13] や bsfilter[14] 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必要し，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　システム構成

大分大学のメールシステムの構成を図 6 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[15] の NAPT 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 [16]．iptables はパケットフィルタリング機能と NAPT 機能を提供する．図 6 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．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．また本システムではプロセス 1 にて，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．

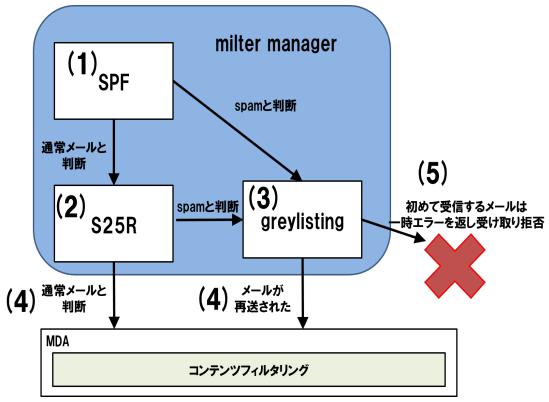

図 7　milter manager を用いた spam 対策の適用順序

（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 7 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．

2.3　メールシステムの問題点

従来のメールシステムでは iptables を使用していたため，IPv6 を利用して送信されたメールはすべて 25 番ポートのプロセス 1 が処理をしていた．従来のメールシステムを変更せずに IPv6 を利用したメールを振り分けるためには iptables の IPv6 向けの実装である ip6tables を導入する必要がある．しかし，ip6tables には NAPT 機能が実装されていない．そのため，IPv6 を利用して送信されたメールはすべて 25 番ポートのプロセス 1 に振り分けられる．プロセス 1 では milter manager を用いて通常メールに対する配送遅延を軽減している．しかし，IPv6 を利用してメールを送信する MTA には，FQDN が S25R によって誤検知

© 2015 Information Processing Society of Japan

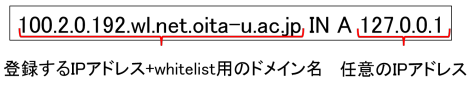

図 8　whitelist に登録する A レコードの例 (IPv4 アドレス)

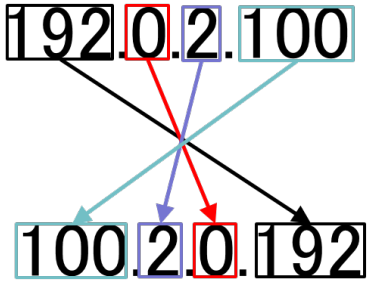

図 9　IPv4 アドレスの並び替え

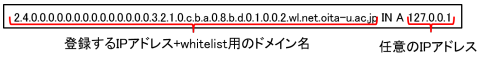

図 10　whitelist に登録する A レコードの例 (IPv6 アドレス)

される MTA が多く，greylisting が適用され，大きな配送遅延が生じている．

3. 関連研究・関連システム

通常メールに対する配送遅延を軽減させる方法には，通常メール送信者を whitelist に登録する方法がある．

ガーダら [18] はレイヤ 3 スイッチのポリシルーティング機能を用いて whitelist を実装することで通常メールに対する配送遅延を軽減させた．レイヤ 3 スイッチに通常メール送信 MTA を登録し，登録の有無によって受信する MTA を動的に変更している．受信する MTA を動的に変更することで，大規模な whitelist の利用においても通常メールの伝送速度を落とさずに優先配送できる．

4. IPv4・IPv6 に対応した whitelist の構成

IPv6 を利用するメール送信者の多くは S25R で spam と誤検知され，greylisting による配送遅延が生じる．そのため，IPv6 を利用するメール送信者を whitelist に登録することで，メールを配送遅延なく受信できるシステムを構築する．新たに，IPv6 に対応した whitelist を作成するため，DNS を用いた whitelist を実装する．

4.1 DNS を用いた whitelist の構成

本研究では blacklist の仕組みを応用して DNS を用いた whitelist を作成する．DNS は，インターネットにおけるドメイン名と IP アドレスの対応関係を相互変換するための分散データベースシステムである [19]．ドメイン名はアルファベット，数字，ハイフン (-) から構成される．DNS

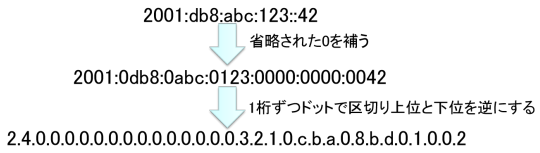

図 11　IPv6 アドレスの並び替え

のサーバには，DNS 権威サーバと DNS キャッシュサーバの 2 つの機能がある．

DNS 権威サーバは，ドメイン名空間に関する情報を管理し，外部からの要求に対し，自らが管理している情報を応答する．DNS 権威サーバは資源レコード形式で情報を管理している．

DNS キャッシュサーバは，クライアントからの問い合わせ (クエリ) に対して，再帰的に名前解決をし，その結果をキャッシュする．また，キャッシュサーバへ名前解決要求をするクライアントをリゾルバと呼ぶ．通常，リゾルバは OS の機能の 1 つとして提供されている．DNS を用いた whitelist は，DNS を用いた blacklist と同様の方法で実装する．DNS 権威サーバに対して，whitelist に登録する MTA の IP アドレスを A レコードとして登録する．A レコードはホストの IP アドレス (IPv4) を定義するレコードである．例として 192.0.2.100 を登録する場合の A レコードを図 8 に示す．登録する IP アドレスを図 9 のように並び替え，whitelist 用のドメイン名と統合して，FQDN を構成する．さらに，DNS 権威サーバがクエリに対して応答する任意の IP アドレスとホスト名を組にして A レコードとして登録する． 図 10 は，2001:db8:abc:123::42 を whitelist に登録する際の A レコードを示す．IPv6 アドレスを A レコードとして whitelist に登録する際も，IPv4 と同様に，whitelist 用のドメイン名と図 11 のように並び替えた IP アドレスを統合した FQDN と，任意の IP アドレスとホスト名を対にして A レコードとして登録する．IPv6 アドレスは，アドレス長が 128 ビットであり，16 ビットごとにコロン (:) で区切って表記する．コロンで区切られた 16 ビットすべてが 0 のフィールドが連続する場合，0 を省略して「::」と表記できる．whitelist に登録する際は 0 を補完して並べ替える．

DNS を用いて whitelist を作成する利点は， メールサーバにかかる負荷の軽減が可能なことである．従来のメールシステムで用いていた iptables では，IP レイヤの 1 パケットごとに whitelist を参照し，振り分けていた．一方，DNS を用いた whitelist ではメール 1 通につき 1 度 DNS に問い合わせるのみで，メールの振り分けが可能である．しかし，外部の権威 DNS サーバに対して whitelist の有無を問い合わせるため，名前解決応答待ち時間が増加する可能性がある．

© 2015 Information Processing Society of Japan

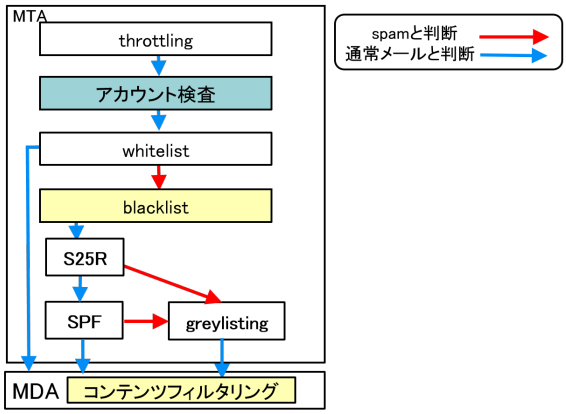

図 12　IPv4・IPv6 に対応した whitelist を用いたメールシステムの構成

4.2　IPv4・IPv6 に対応した whitelist を用いたメールシステムの構成

IPv4・IPv6 に対応した whitelist を用いたメールシステムの構成を図 12 に示す．IPv6・IPv4 に対応した whitelist を導入するにあたってシステム全体を再構築した．whitelist は greylisting のプログラムに DNS へ問い合わせる機能を記述することで実装した．図 12 に示すメールシステムに組み込まれている spam 対策のうち，whitelist，blacklist，SPF，S25R は greylisting の拡張機能を用いて実装したため，milter manager を除外した．図 12 に示すように，whitelist をアカウント検査の後に適用するように変更し，メールヘッダ検査を削除した．アカウント検査と throttling は Sendmail で実装している機能であり，適用順序を変更できないため whitelist より前で適用している．また，メールヘッダ検査は誤検知が多かったため，再構築する際に除外した．

5.　IPv4・IPv6 に対応した whitelist を用いたメールシステムの導入効果

5.1　調査方法

IPv4・IPv6 に対応した whitelist を用いたメールシステムの導入効果の調査期間は 2014 年 11 月 23 日から 12 月 20 日である．システム導入前の 2013 年 11 月 24 日から 12 月 21 日までの期間と比較する．調査対象は，大分大学のメールシステムが受信したメールのうち，IPv6 を利用して送信されたメールである．調査対象をメールログから抜粋し，配送遅延時間を調査した．本調査では，図 12 に示す MTA で適用する spam 対策において spam と分類されたメールを spam，MDA が受信したメールを通常メールと定義する．IPv4・IPv6 に対応した whitelist 導入前後では，IPv6 アドレスの whitelist 登録件数を 0 件から 28 件まで増やした．whitelist にはネットワークアドレス単位で登録している．調査時に，whitelist には/48 単位で 2 件，/56 単位で 1 件，/64 単位で 25 件を登録していた．実際の登録 IPv6 アドレス数は 2423×10^{21} となる．whitelist には，大学や研究機関などの信頼できる送信者や，Google のメールサーバの IPv6 アドレスを手動で登録した．

表 2　IPv6 を利用して送信されたメール数

期間	MTA 数	通常メール数 (C)	spam 数 (D)	spam 割合 (D/B)
導入前	1,058	11,895 通	1,722 通	12.6%
導入後	933	11,000 通	911 通	7.6%

5.2　調査結果と考察

IPv4・IPv6 を利用したメールの割合を表 1，IPv6 を利用して送信された spam 数と通常メール数を表 2，配送遅延時間を表 3 に示す．表 1 に示す IPv4・IPv6 を利用したメールの割合を導入前後で比較すると 1.0%から 0.7%まで減少していた．しかし，表 2 の IPv6 を利用して送信された通常メール数はほぼ同じである．割合が変化したのは IPv4 アドレスを利用して送信されたメール数が影響していたためである．

表 2 に示す spam 割合が導入前後では 12.6%から 7.6%に減少している．導入前の spam の挙動を調査したところ，2.1.1 節で述べた greylisting において誤検知される挙動を発見した．誤検知される挙動を示した通常メール送信者を IPv4・IPv6 に対応した whitelist 導入時に whitelist に登録した．IPv4・IPv6 に対応した whitelist 導入後，whitelist に登録されている IPv6 アドレスの MTA から送信された 9577 通のメールは greylisting において誤検知されることなく受信しており，spam と誤検知されるメールが減少したためと考えられる．

表 3 に示す再送要求数を IPv4・IPv6 に対応した whitelist 導入前後で比較すると，2,403 通から 430 通まで減少していた．それに伴い，平均配送遅延時間が whitelist 導入前後で 432 秒から 239 秒まで減少していた．また，whitelist に登録されている IPv6 アドレスの MTA から送信された 9577 通は再送要求をしないため，配送遅延なく受信している．これらのことから IPv4・IPv6 に対応した whitelist を導入することで，IPv6 を利用して送信された通常メールに対する配送遅延を軽減することを確認できた．

6.　おわりに

本論文では，IPv4・IPv6 に対応した whitelist を導入したメールシステムの運用結果について述べた．DNS を用いて IPv4・IPv6 に対応した whitelist をメールシステムに導入することで，IPv6 を利用して送信された通常メールに対する平均配送遅延時間が 432 秒から 239 秒まで減少した．本システムを導入することで IPv6 を利用して送信された通常メールに対する配送遅延を軽減できる．

今後の課題として IPv6 アドレスを持つ MTA を whitelist

© 2015 Information Processing Society of Japan

表 1　IPv4・IPv6 メールの割合

期間	全メール数 (A)	IPv6 メール数 (B)	IPv4 メール数	IPv6 メール割合 (B/A)
導入前	1,284,041 通	13,617 通	1,270,424 通	1.0%
導入後	1,733,598 通	11,911 通	1,721,687 通	0.7%

表 3　配送遅延時間

期間	whitelist 登録者からのメール数	再送要求応答数	配送遅延時間合計 (E)	平均配送遅延時間 (E/C)
導入前	0 通	2,403 通	5,146,681 秒	432 秒
導入後	9,577 通	430 通	2,633,315 秒	239 秒

へ登録する際の基準を検討する必要がある．現在 IPv6 アドレスを whitelist に登録する際には，メールサーバの管理者が手動で登録している．今後，IPv6 を利用したメールが増加すると考えられるため，手動で通常メール送信者を whitelist に登録するのはメールサーバの管理者に負担がかかる．そのため，通常メール送信者を自動で whitelist へ登録するシステムを作る必要がある．先行研究として本研究室では whitelist 自動作成システムを開発，運用してきた [20]．whitelist 自動作成システムでは greylisting の再送要求に応答した MTA の中から SPF の認証に成功した MTA と，MTA の IP アドレスに対して逆引きし，得られた FQDN 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．しかし，IPv6 アドレスを利用する MTA には FQDN が設定されていない MTA や，greylisting において誤検知される MTA がある．そのため，whitelist 自動作成システムにおける IPv6 アドレスの登録基準を検討する必要がある．

参考文献

[1] Symantec Intelligence Report，入手先 ⟨http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_11-2014.en-us.pdf⟩（参照 2015-01-20）.
[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] Greylisting.org - a great weapon against spammer，入手先 ⟨http://www.greylisting.org/⟩（参照 2013-05-05）.
[5] 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).
[6] SpamCop，入手先 ⟨http://www.spamcop.net/⟩（参照 2013-05-05）.
[7] RBL.JP プロジェクト，入手先 ⟨http://www.rbl.jp/⟩（参照 2013-05-05）.
[8] The Spamhaus Project，入手先 ⟨http://www.spamhaus.org/⟩（参照 2013-05-05）.
[9] 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）.
[10] 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）.
[11] Schlitt, W.: Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, *RFC4408* (2006).
[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.org，入手先 ⟨http://bsfilter.org/⟩（参照 2013-05-05）.
[15] The netfilter.org ”iptables” project，入手先 ⟨http://www.netfilter.org/projects/iptables/index.html⟩（参照 2014-05-19）.
[16] 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).
[17] Sendmail.com，入手先 ⟨https://www.sendmail.com/sm/open_source/⟩（参照 2014-06-17）.
[18] ガーダ, 山井成良，岡山聖彦，河野圭太，中村素典：レイヤ 3 スイッチによる動的ホワイトリストを用いた電子メール優先配送システム，情報処理学会論文誌，Vol. 55, No. 3, pp. 1151–1159 (2014).
[19] 民田雅人，森下泰宏，坂口智哉：実践 DNS DNSSEC 時代の DNS の設定と運用，アスキーメディアワークス (2011).
[20] 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 ()IOTS2011 論文集，pp. 39–44 (2011).

© 2015 Information Processing Society of Japan