情報処理学会論文誌 Vol.55 No.3 1151–1159 (Mar. 2014)

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

ガーダ[1,a)] 山井 成良[2] 岡山 聖彦[2] 河野 圭太[2] 中村 素典[3]

受付日 2013年6月30日, 採録日 2013年12月4日

概要：重要な電子メールを遅滞なく受信者へ配送するために，信頼できる送信 MTA をあらかじめホワイトリストに登録し，優先的に配送する仕組みが考えられている．しかし，従来の方法では大規模なホワイトリストを扱えないか，扱える場合でも速度が遅くなるなどの問題があった．そこで，本論文ではレイヤ3スイッチのポリシルーティング機能を用いてホワイトリストを実現し，登録する送信 MTA を動的に変更することにより，大規模なホワイトリストでも速度を落とさずに優先配送できるシステムを提案する．また，提案システムを試作して性能評価を行った結果，大規模なホワイトリストをすべてレイヤ3スイッチに登録した場合と比較して高速に伝送できたことを示す．

キーワード：電子メール，迷惑メール，ホワイトリスト，優先配送，ポリシルーティング

E-mail Priority Delivery System with Dynamic Whitelist in the Layer 3 Switch

Gada[1,a)] Nariyoshi Yamai[2] Kiyohiko Okayama[2] Keita Kawano[2] Motonori Nakamura[3]

Received: June 30, 2013, Accepted: December 4, 2013

Abstract: In order to deliver important e-mails without unnecessary delay, some priority delivery methods with a whitelist, which includes trusted sending MTAs, are proposed so far. However, most of conventional methods have some problems with a large sized whitelist such as performance degradation, delivery failure, and so on. In this paper, we propose a priority delivery system with a layer 3 switch having policy based routing (PBR) function. By updating PBR entries dynamically, this system implements a large sized whitelist without performance degradation. We also address the implementation of the prototype system and its performance.

Keywords: e-mail, spam mail, whitelist, priority delivery, policy based routing

1. はじめに

電子メールはインターネットで最も普及しているコミュニケーション手段であり，多くの人により様々な目的に利用されている．一方，電子メールはセキュリティ的に問題の多いサービスでもある．特に，受信者の意図を無視して無差別かつ大量に送信される spam メールの蔓延により膨大な量のトラフィックがネットワークやメールサーバに大きな負荷をかけ，通常のメール配送に遅延が発生している [3]．多くの組織では spam メールに対処するため greylisting [4]，greet pause [5] などの様々な対策を適用しているが，その対策により，新たな負荷の高い処理を行う必要がある，大きな遅延が発生する，あるいは重要なメールが spam メールと誤判定されるなど，通常のメール配送

1 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama Uniersity, Okayama 700–8530, Japan
2 岡山大学情報統括センター
Center for Information Technology and Management, Okayama Univercity, Okayama 700–8530, Japan
3 国立情報学研究所
National Institute of Informatics, Chiyoda, Tokyo 101–8430, Japan
a) gada@dist.cne.okayama-u.ac.jp

本論文は文献 [1], [2] の内容を発展させたものである．

に支障が生じる状態が発生している [3].

これらの問題に対処するため，信頼できる送信 MTA（Mail Transfer Agent）をホワイトリストとして登録し，登録された MTA（優先送信 MTA）から送られたメールは無条件に受信する方法がよく用いられている．ホワイトリストを実現する代表的な方法としては，ルータで送信 MTA の IP アドレスに基づいて受信 MTA を振り分ける方法 [6] が知られている．しかし，この方法は信頼できる送信 MTA が増加したり，spam メールの通信量が増加したりした場合に十分な性能が得られないという問題が生じるため，大規模なホワイトリストを扱え，かつ大量の spam メールによる影響を受けにくい方法が望まれている．

そこで，本論文ではポリシルーティング（以下，PBR: Policy Based Routing）機能を持つレイヤ 3 スイッチ（以下，L3 スイッチ）を用いてホワイトリストを実現し，またホワイトリストに登録された送信 MTA を動的に変更するシステムを提案する [1], [2]．これにより，大規模なホワイトリストに対しても優先配送されるべき電子メールの伝送速度を落とさずに配送することが可能になる．

2. 従来の電子メール優先配送システムとその問題点

ホワイトリストを実現する代表的な方法として，(1) 受信 MTA 自身がホワイトリストを持つ方法，(2) 動的に応答を変える DNS サーバを用いて受信 MTA を変更する方法 [7]，(3) ルータで送信 MTA の IP アドレスに基づいて送信先 MTA を振り分ける方法 [6] がある．本章ではこれらの方法およびその問題点を述べる．

2.1 受信 MTA 自身がホワイトリストを持つ方法

一般に spam メール対策では，通常メールを誤って spam メールと判定する可能性が無視できないため，送信 MTA の FQDN（Fully Qualified Domain Name）や IP アドレス，あるいは電子メールの差出人アドレスに基づくホワイトリストを作成することが多い．特に greylisting [4] や greet pause [5] のような対策法では，誤判定が発生すると当該電子メールが失われるため，ホワイトリストの運用は必須である．

ところが，受信 MTA 自身がホワイトリストを持つ場合，その受信 MTA は優先配送の対象となる電子メール（以下，優先配送メール）だけでなくそれ以外の電子メール（以下，一般メール）も受信することになるため，多くの電子メールを受信して受信 MTA が過負荷になっている場合には優先配送メールの処理にも遅延が発生することになる．これに対して負荷分散のため複数の受信 MTA を運用する場合もあるが，優先配送メールと一般メールが混在する以上，本質的には同じ問題が発生しうる．

2.2 動的に応答を変える DNS サーバを用いて受信 MTA を変更する方法

文献 [7] では，送信 MTA に応じて受信 MTA を変更する方法として，問合せ元に応じて応答を変更できる機能を持つ DNS サーバを用いる方法が提案されている．この方法では優先配送される送信 MTA が使用する DNS サーバ（キャッシュサーバ）のリスト（ホワイト DNS サーバリスト）を作成し，このリストに含まれるキャッシュサーバからの問合せに対して優先配送メールを受信する MTA（優先受信 MTA）を応答する．これにより優先配送メールと一般メールを分離して処理を行うことが可能になり，一般メールを受信する MTA（一般受信 MTA）が過負荷になった場合でも優先配送メールを遅滞なく処理することが可能になる．

ところが，この方法ではホワイト DNS サーバリストの作成にかなりの手間が必要であるため，優先送信 MTA が増加するとホワイト DNS サーバリストの作成が事実上困難となるという問題がある．また同一のキャッシュサーバを使用する優先送信 MTA とそれ以外の MTA（一般送信 MTA）が存在する場合，これらの区別を行えずに両方とも優先受信 MTA で処理を行うことになる点も問題である．

2.3 ルータで IP アドレスに基づいて受信 MTA を振り分ける方法

文献 [3], [6] では Linux を搭載した PC ルータを用いて IP アドレスに基づいて受信 MTA を振り分ける装置（メール分別装置）を実現する方法が紹介されている．この方法では分別装置内で Linux におけるファイアウォール機能である iptables を用いてホワイトリストを実現し，通過する SMTP コネクションを送信元 IP アドレスに基づいて独立起動されている異なるプロセスあるいは異なる受信 MTA に振り分ける．このような方法は 2.2 節の方法と比較して実現が容易であり，また特に異なる受信 MTA に振り分ける場合には一般受信 MTA が過負荷になった場合でも優先配送メールを遅滞なく処理することが可能になる点で 2.1 節の方法より優れている．

ところが，この方法では Linux の iptables を用いてホワイトリストを実現しているため，ホワイトリストに登録される優先送信 MTA が増加すると性能が劣化するという問題がある．すなわち，iptables を用いてホワイトリストを実現する場合，すべてのパケットについて線形探索により送信元 IP がホワイトリストに含まれるかどうかの判定が行われるため，ホワイトリストのサイズに比例した探索時間が必要となる．PC ルータでの iptables の代わりにルータ（L3 スイッチ）の PBR 機能を用いれば，TCAM（Ternary Content Addressable Memory）による探索時間の短縮効果が期待できる [8] が，TCAM の容量には限りがあるため大規模なホワイトリストを扱うことができない点は解決さ

れない．

3. 大規模なホワイトリストに対応可能な電子メール優先配送システム

3.1 実現方針

前章で述べたように，ルータで IP アドレスに基づいて受信 MTA を振り分ける方法は他の方法より実現が容易でかつ効果的である点で優れているが，大規模なホワイトリストを扱う場合に性能が低下するという問題点がある．そこで本論文では L3 スイッチの PBR 機能を用いてホワイトリストを実現し，登録する送信 MTA を動的に変更することにより，大規模なホワイトリストの利用においても通常のメールの伝送速度を落とさずに優先配送できるシステムを提案する．

本システムではホワイトリストに登録する優先送信 MTA を最近配送が行われているものに限定することで通信速度の劣化を抑制する．具体的には L3 スイッチ上のホワイトリストに登録されていない送信 MTA からの SMTP コネクションは，確立時に大規模なホワイトリストを持つ装置（コントローラ）が送信 MTA を大規模なホワイトリストと照合し，ホワイトリストに含まれる場合はその送信 MTA を L3 スイッチのホワイトリストに登録してから通信を行わせるようにする．また，登録された送信 MTA は登録後から一定時間が経過すればホワイトリストから消去される．

3.2 提案システムの構成

提案システムは**図 1** に示すように L3 スイッチ，優先受信 MTA，一般受信 MTA，およびコントローラから構成される．このうち，優先受信 MTA，一般受信 MTA は個別の IP アドレスとは別に共通の仮想 IP アドレス（以下，共通 IP アドレス）を持ち，このアドレスが配送に用いられる．また，個別の IP アドレスは L3 スイッチで中継先を指定する際に用いられる．L3 スイッチは PBR 機能を持つ．すなわち，設定されたポリシに基づき，特定の条件を満たすパケットの中継先（next hop）を通常のものとは異なるように指定することができる．

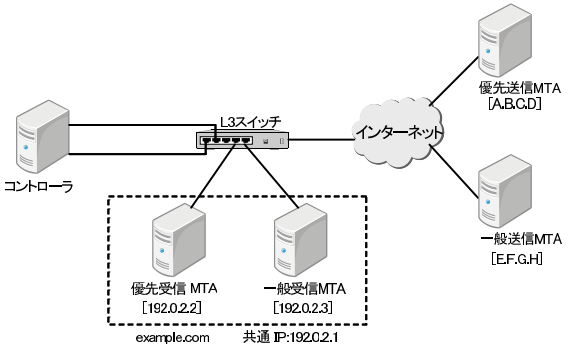


図 1 提案システムの構成
Fig. 1 System configuration.

コントローラは送信 MTA から送信されたパケットの一部を受信し，コントローラ自身が持つ大規模なホワイトリストに送信 MTA が含まれるかどうかによって L3 スイッチの設定を変更する役割を果たす．また後述するように，コントローラは優先受信 MTA あるいは一般受信 MTA から送信されたパケットの一部を受信し，その送信元が優先受信 MTA，一般受信 MTA のどちらであるかを区別して処理を行う必要がある．しかし，コントローラが受信するパケットは実際の送信元が優先受信 MTA，一般受信 MTA のいずれであってもその送信元 IP アドレスが共通 IP アドレスであるため，送信元 IP アドレスでは実際の送信元を区別することができない．そこで，提案システムでは L3 スイッチとコントローラとの間を 2 本のリンクで接続し，L3 スイッチでは優先受信 MTA あるいは一般受信 MTA から受け取ったパケットをコントローラに中継する際に送信元となる受信 MTA の種類に応じてこれらのリンクを使い分けるようにする．これによりコントローラはどちらのリンクからパケットを受信したかによってそのパケットの送信元がどちらの受信 MTA であるかを区別できるようになる．

なお，図 1 は論理的な構成を示したものであり，物理的な構成はこの図には限定されないことに注意する．たとえば，L3 スイッチとコントローラとの間のリンクが 1 本しかない構成においても，このリンク上で 2 本の VLAN を設定し，これらを使い分けることにより実質的に図 1 と同様の構成をとることが可能である．

以下では，この構成において送信 MTA が共通 IP アドレスに対して SMTP コネクションを確立して電子メールを送信する場合の本システムの動作を述べる．

3.3 コントローラが存在しない場合の動作

本システムの動作を理解しやすくするため，まずコントローラが存在しない場合の動作について説明する．この場合，L3 スイッチには優先送信 MTA が静的にホワイトリストに登録されている状態にあるものとする．この状態では，送信 MTA から共通 IP アドレス宛に送られたパケットは L3 スイッチにおいてポリシに基づき中継先が決定される．すなわち，送信 MTA の IP アドレスがホワイトリスト中に含まれれば優先受信 MTA の個別アドレスが中継先が，そうでなければ一般受信 MTA の個別アドレスが中継先として指定される．

受信 MTA は L3 スイッチが中継したパケットの宛先が自身の仮想 IP アドレスであるため，これを受信する．逆に受信したパケットに対する応答として受信 MTA から送信 MTA に送られるパケットの送信元 IP アドレスは共通 IP アドレスとなる．なお，この動作はサーバの負荷分散の際によく用いられる DSR（Direct Server Return）技術 [9] と同等である．

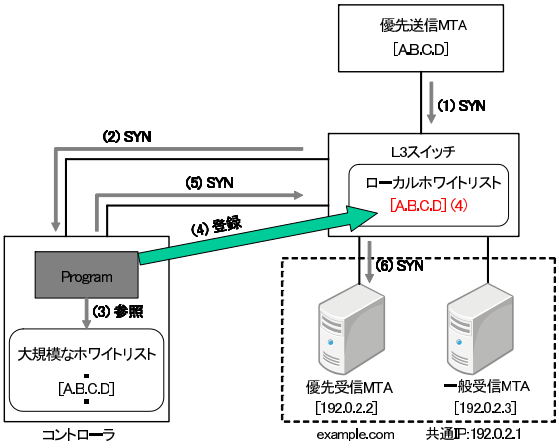


図 2 SYN パケットの処理
Fig. 2 SYN packet processing.

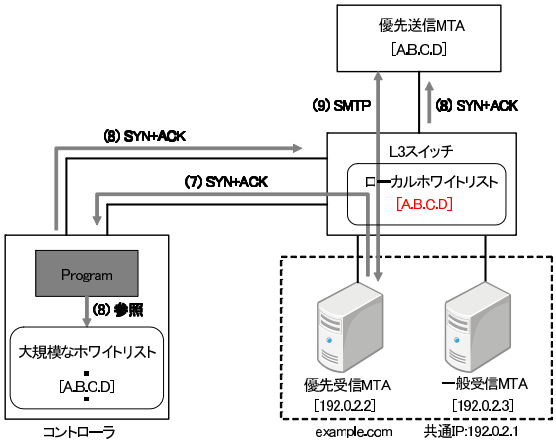


図 3 SYN+ACK パケットの処理
Fig. 3 SYN+ACK packet processing.

3.4 L3 スイッチへのホワイトリストへの登録

次にコントローラが存在する場合の動作を説明する．

L3 スイッチは，自身の持つホワイトリストに含まれない送信 MTA から共通 IP アドレス宛の SMTP コネクションの最初のパケット（以下，SYN パケット）を受け取ると，これをコントローラに中継する．コントローラは L3 スイッチ経由で SYN パケットを受け取った場合，送信 MTA が大規模なホワイトリストに含まれるかどうかを判断し，もし含まれれば送信 MTA を L3 スイッチ内のホワイトリストに登録して，その後パケットを L3 スイッチに送出する．そうでなければ，送信 MTA を L3 スイッチ内のホワイトリストに登録せずに単に SYN パケットを L3 スイッチに送出する．この動作により，大規模なホワイトリストに含まれる送信 MTA からのパケットは PBR により優先受信 MTA に中継され，それ以外の送信 MTA からのパケットは一般受信 MTA に中継される．SYN パケットの処理の流れを**図 2** に示す．

しかし，この動作に基づいて優先配送システムを試作した結果，L3 スイッチが持つホワイトリストは更新直後に過渡的な状態になり，SYN パケットが正しくない受信 MTA [*1] に中継される場合があることが確認された [2]．この場合，正しい受信 MTA は，SYN パケットを受信していないにもかかわらずホワイトリスト安定後には後続のパケットを受け取るため，RST パケットを送出して SMTP コネクションを強制切断する．そこで，このような動作を防止するため，SYN パケットに対する応答パケット（以下，SYN+ACK パケット）を優先受信 MTA あるいは一般受信 MTA から受信すると，L3 スイッチがこれをコントローラに中継するように設定する．その際，SYN+ACK パケットを受信した場合には，これを優先受信 MTA が接続されているポート，一般受信 MTA が接続されているポートのどちらから受信したかによって中継先のリンクが異なるように L3 スイッチを設定し，コントローラが SYN+ACK パケットの送信元を特定できるようにする．SYN+ACK パケットの処理の流れを**図 3** に示す．

送信 MTA と受信 MTA との間でやりとりされるこれ以外のパケットはコントローラには転送されず，送信 MTA と受信 MTA との間で直接やりとりされる．すなわち送信 MTA から受信 MTA への SYN パケット以外のパケットは，送信 MTA の IP アドレスが L3 スイッチが持つホワイトリストに含まれれば優先受信 MTA に，そうでなければ一般受信 MTA に中継される．優先受信 MTA あるいは一般受信 MTA から送信 MTA への SYN+ACK 以外のパケット[*2]は送信 MTA に中継される．

以下に，SMTP コネクションが確立されるまでの処理の流れを示す．なお，各ステップの番号は図 2，図 3 中に表示されている番号と対応する．

(1) L3 スイッチは自身の持つホワイトリストに含まれない送信 MTA から共通 IP アドレス宛の SMTP コネクションの最初の SYN パケットを受け取る．
(2) L3 スイッチは受け取った SYN パケットをコントローラに中継する．
(3) コントローラはパケットの送信元 IP アドレスを抽出し，大規模なホワイトリストに含まれるかどうかを判断する．
(4) もしパケットの送信元 IP アドレスが大規模なホワイトリストに含まれる場合，コントローラは送信元 IP アドレスを L3 スイッチ内のホワイトリストに登録する．そうでなければ，L3 スイッチの設定を変更しない．
(5) その後，コントローラは SYN パケットを L3 スイッチに中継する．
(6) L3 スイッチは自身の持つホワイトリストに基づき，優先受信 MTA，一般受信 MTA のどちらか中継先かを決定し，SYN パケットを中継する．

*1 SYN パケットの送信元が優先送信 MTA の場合は一般受信 MTA，そうでない場合には優先受信 MTA を指す．

*2 実際には後述するように RST パケットも除外される．

(7) L3 スイッチは受信 MTA から返される SYN+ACK パケットを受け取ると，受信 MTA に応じた特定のリンクを経由してこれをコントローラに中継する．

(8) コントローラは，SYN+ACK パケットを受け取るとその宛先 IP アドレスを抽出し，大規模なホワイトリストと照合して，このパケットが正しい受信 MTA から送られたものかどうかを判断する．もし優先受信 MTA から返される SYN+ACK パケットの宛先 IP アドレスがコントローラの大規模なホワイトリストに含まれる場合，あるいは一般受信 MTA から返される SYN+ACK パケットの宛先 IP アドレスがコントローラの大規模なホワイトリストに含まれない場合には，正しい受信 MTA から返されていると判断し，単に SYN+ACK パケットを L3 スイッチ経由で送信 MTA に中継する．逆に，一般受信 MTA から返される SYN+ACK パケットの宛先 IP アドレスが大規模なホワイトリストに含まれる場合，あるいは優先受信 MTA から返される SYN+ACK パケットの宛先 IP アドレスが大規模なホワイトリストに含まれない場合には，コントローラは L3 スイッチが持つホワイトリストが更新中のため正しくない受信 MTA から SYN+ACK パケットが返されていると判断し，単にパケットを廃棄する．これにより，後に送信 MTA から SYN パケットが再送されるが，その時点までに L3 スイッチが持つホワイトリストの更新が完了するのを期待する．

(9) 送信 MTA からの SYN 以後の通信は L3 スイッチ内のホワイトリストに基づき中継先が決定され，メールの伝送が行われる．

これらの動作により，最初の SYN パケットと応答 SYN + ACK パケットのみコントローラ経由で中継され，それ以外は L3 スイッチが直接中継するため，通信速度をほとんど低下させずにメール配送を行うことができる．

3.5 L3 スイッチ内のホワイトリストからの削除

L3 スイッチ内のホワイトリストはサイズが大きすぎるとパケットの中継速度が遅くなるため，何らかの基準でホワイトリストから登録している優先受信 MTA を削除する必要がある．ただし，コントローラは登録された各優先送信 MTA が通信中かどうかを分からない．この問題に対処するため，登録後一定時間経過した優先送信 MTA を削除する手法を採用する．

ところが，この手法では現在通信中の優先送信 MTA をホワイトリストから削除する可能性がある．**図 4** にそのとき行われる処理を示す．

(1) L3 スイッチは優先送信 MTA から送られた通信を受信する．

(2) コントローラの期限切れ処理により優先送信 MTA がホワイトリストから削除された場合，L3 スイッチは通信を一般受信 MTA へ中継する．

(3) 一般受信 MTA はこのとき発生する通信を取り扱えず，RST パケットを返す．

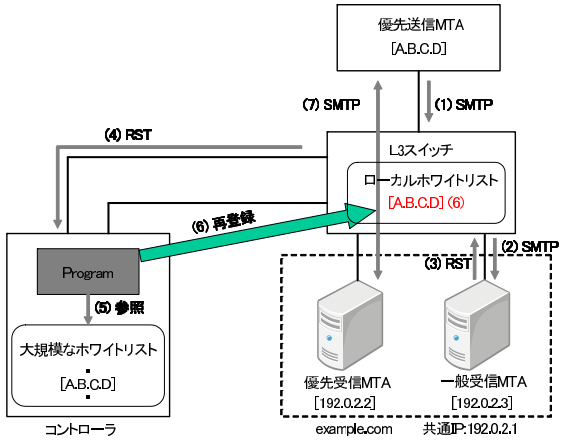


図 4 RST パケットの処理

Fig. 4 Process for deleting a priority sending MTA from the whitelist of L3SW.

ここで，もし L3 スイッチが RST パケットを優先送信 MTA に中継した場合，SMTP コネクションが強制切断される結果となる．このような結果を引き起こさないため，提案システムでは以下の動作をする．

(4) L3 スイッチは一般受信 MTA からの RST パケットをコントローラへ中継する．

(5) コントローラは RST パケットを受け取り，宛先 IP アドレスを抽出し，大規模なホワイトリストに含まれるかどうかを判定する．

(6) もし含まれる場合，コントローラは RST パケットの宛先 IP アドレスを L3 スイッチ内のホワイトリストに登録する．その後 RST パケットを廃棄する．

(7) これにより，通信中の優先送信 MTA は一般受信 MTA に中継されたパケットが途中で失われたものと判断し，当該パケットを再送し．通信を継続することができる．

4. 試作システムの実装と性能評価

本章では，試作システムの実装と動作確認および性能評価実験について述べ，また，考察に通じて本システムの有効性を確認する．

4.1 試作システムの実装

試作システムの構成は図 1 と同じである．L3 スイッチにはシスコシステムズ社製 Catalyst 3550-12T を使用した．

また，コントローラには FreeBSD 8.2-RELEASE を搭載した PC を使用した．コントローラとして使用した PC の諸元を**表 1** に示す．

以下では，L3 スイッチの設定およびコントローラの動作について，実装上注意が必要な点を述べる．

表 1 コントローラ用 PC の諸元
Table 1 Specification of PC for controller.

CPU	Intel Core i3 2100（3.1 GHz）
メモリ	4 GB
ネットワークインタフェース	100BaseTX

4.1.1 L3 スイッチの設定

本システムで使用したスイッチでは，以下のような設定により PBR が実行される．

(1) access-list コマンドを用いて PBR の対象となるパケットの条件を定義する．個々の access-list には番号が割り当てられており，1 つの access-list に複数の条件を定義することも可能である．
(2) route-map コマンドおよびそのサブコマンドにおいて PBR の対象となるパケットの条件を指定する．この指定は該当する access-list 番号の列挙により行う．また，指定した条件に対して，合致したパケットの中継先を指定する．

したがって，access-list を用いて送信元 IP アドレスが優先送信 MTA であるパケットを優先受信 MTA に中継するような条件を，個々の優先送信 MTA について定義すれば優先配送を実現できる．

ところが，使用した L3 スイッチ用ソフトウェアである IOS では，1 つの access-list に複数の条件が定義されている場合，各条件を個別に削除することができない．そこで，複数の access-list を用意し，新たに優先送信 MTA を登録する access-list を一定時間ごとに切り替えることにより対処することにした．また，これにより登録後一定時間が経過した場合の削除処理についても，該当する access-list を初期化・再利用するだけで実現できる．ただし，access-list を初期化する過程で一時的に PBR が無効化される状態になることが判明したため，削除対象となる access-list をいったん PBR の条件から外してから access-list の初期化を行い，その後 PBR の条件として再指定するようにした．

同時使用する access-list の本数は IOS の制約により 40 本とし，また新規登録用 access-list を 1 分ごとに切り替えるようにした．このため，優先送信 MTA は登録後 40 分で削除されることになる．

4.1.2 コントローラの実装

コントローラには，SYN パケット，SYN+ACK パケットおよび RST パケットの送受信を行う機能，および L3 スイッチの設定を変更する機能が必要である．本システムではこれらの機能を持つプログラムを perl により実装した．2 つの機能のうち，前者の機能については FreeBSD が持つ ipfw [10] および divert [11] 機能を用いて実現した．また，後者については telnet プロトコルにより L3 スイッチと変更可能な状態で常時接続するようにし，SYN パケット，SYN+ACK パケットや RST パケットを受信した場合にはただちに設定変更するようにした．

大規模なホワイトリストについては，本システムでは実装せず，すべての送信 MTA を優先送信 MTA として扱った．ただし，大規模なホワイトリストはハッシュ表などを用いることにより，短い時間で検索できるように容易に実装可能である．また，外部のホワイトリストサーバに問い合わせたり，文献 [3] に示されているように IP アドレスから得られた FQDN をもとに優先配送すべきかどうか判断したりする方法も容易に取り入れることができる．

4.2 動作確認実験

試作システムの動作を確認するため，図 1 と同様の実験環境を構築し，送信 MTA から電子メールを何通か配信して配送処理状況を観測する実験を行った．その際，送信 MTA が大規模なホワイトリストに含まれると見なした場合とそうでない場合の 2 つの場合について，同一の宛先メールアドレスを指定して送信 MTA から配送した．

実験の結果，前者の場合は 1 通目の配送のときに SYN パケットがコントローラに中継され，L3 スイッチの access-list が適切に更新されることを確認した．2 通目以降の配送では SYN パケットを含めたすべてのパケットが優先受信 MTA に直接中継されていることを確認した．ただし，1 通目の配送においてコントローラが access-list を更新した直後に稀に 1 パケットだけが一般受信 MTA に中継され，RST パケットが生成される状況が発生することが確認された．しかし，この場合でもこの RST パケットはコントローラに中継されて破棄されるだけでありメール配送自体は正常に行われることを確認した．

一方，後者の場合には，何通目の配送においても，まず SYN パケットがコントローラにいったん中継されるが何の処理も行われずただちに L3 スイッチを経由して一般受信 MTA に中継され，後続のパケットは一般受信 MTA に直接中継されることを確認した．

次に，優先送信 MTA から優先受信 MTA へ電子メールが配送されている途中で access-list の再利用が起きる状況を意図的に設定し，その場合の配送処理状況およびコントローラ，L3 スイッチの状態を観測する実験を行った．その結果，初期化・再利用処理を行った直後に一般受信 MTA で発生した RST パケットがコントローラに中継され，優先送信 MTA が access-list に再登録される様子が確認された．

以上の結果から，本システムは設計どおりに動作することが確認された．

4.3 性能評価実験

次に，本システムの性能評価実験を行った．

4.3.1 L3 スイッチの設定変更時間

最初に，access-list への登録処理および再利用処理にかかる時間を測定した．その結果を**表 2** に示す．これらの

表 2 access-list への登録処理および再利用処理時間
Table 2 Time required for registration and aging processes.

登録処理時間	再利用処理時間
7.8（ms）	54.7（ms）

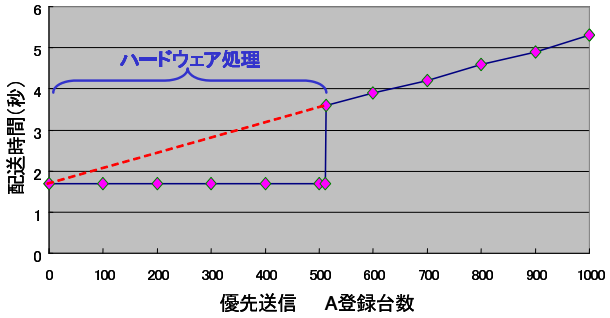


図 5 L3 スイッチ内のホワイトリストに登録される送信 MTA の数を変化させた場合のメール配送時間
Fig. 5 Delivery time per message for the number of registered MTAs in the L3SW.

結果より，登録処理は計算上 1 秒間で 128 台分の優先送信 MTA を登録することができ，実用上十分小さいといえる．また，再利用処理時間は比較的長くなっているが，1 分間に 1 度発生する処理であるため，こちらも実用上十分小さいといえる．

4.3.2 優先送信 MTA 登録台数に対するメール配送時間

本システムの有効性を確認するため，L3 スイッチ内のホワイトリストのサイズを変化させた場合のメール配送時間を測定した．この実験では，コントローラを追加せず，L3 スイッチ内のホワイトリストに登録される台数を 1,000 台まで増やした場合の優先受信 MTA でのそれぞれのメール処理時間を配送時間としてとった．なお，配送する電子メールの大きさは約 10 MB とし，送信 MTA，受信 MTA のネットワークインタフェースはともに 100BaseTX である．その結果を**図 5** に示す．

この実験から，登録台数が 512 台以下の場合には一定時間で送信できたが，これを超えると台数の増加に応じて配送時間も増加することが分かる．これは L3 スイッチ内の TCAM 容量が不足し，ソフトウェア処理により PBR を行っているため [8] である．この結果から，本システムを用いて L3 スイッチに登録する優先送信 MTA 台数がつねに 512 台以下になるように，コントローラが大規模なホワイトリストを基づき動的に変更すれば，メール配送をハードウェアで高速処理できるため，本システムは有効であるといえる．

4.3.3 多数の送信 MTA が同時にメール配送を行っている状況での性能評価

最後に，本システムの有効性を評価するため，優先送信 MTA とそうでない一般送信 MTA が多数存在し，同時にメール配送を行っている状況での性能評価実験を行った．

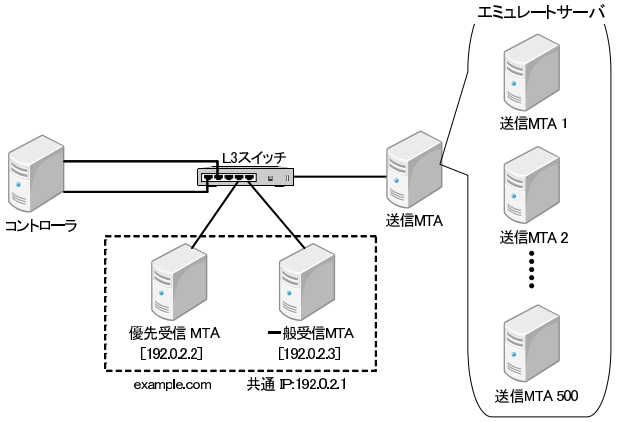


図 6 多数の送信 MTA がメール配送を行っている状況での性能評価実験環境
Fig. 6 Experiment environment in case of heavy traffic.

実験環境を**図 6** に示す．この実験では，準備できる機材の都合上，送信 MTA の台数を増やせなかったため，物理的な送信 MTA は 1 台であるものの，多数の送信 MTA が並列にメール配送を行っている状況をエミュレートして評価実験を行った．まず，送信 MTA では smtp-source [12] を用いて -s オプションを指定することにより並列的にメール配送を行うようにした．しかし，このままでは送信元 IP アドレスがすべて同じであるため，多数の送信 MTA がメール配送を行っている状態とは異なる．そこで，送信 MTA 上で送信元ポート番号に応じたランダムな送信元 IP アドレスを用いて SMTP 通信を行うような一種の NAT（Network Address Translation）機能を取り込んだ．これにより，送信 MTA で smtp-source のプロセス数（並列度）を増加させても各プロセスが用いる一時ポート番号がすべて異なるため，NAT 機能により各プロセスが使用する変換後の送信元 IP アドレスも異なることになり，結果として多数の送信 MTA が同時にメール送信を行っている状況をエミュレートできる．

この実験では，受信 MTA で用いた SMTP サーバプログラム postfix [13] の最大プロセス数の標準値（default_process_limit）が 100 であったことから，一般受信 MTA でただちには処理できないような十分大きな負荷を与えるために並列度を 500 とし，送信 MTA から同時に 500 通のメール送信を行う場合の性能評価実験を行った．そのとき，コントローラが送信元 IP アドレスに基づいて 1/10 の確率で優先送信 MTA と判定するようにシステムを構築して，優先受信 MTA，一般受信 MTA それぞれでのメール受信処理時間を測定した．その際，一般受信 MTA では spam メール対策を行うことを想定して SpamAssassin [14] を動作させた．

表 3 は優先受信 MTA，一般受信 MTA でのメール受信数とそれぞれの平均処理時間，処理時間の標準偏差，最大処理時間，最小処理時間を示す．その結果，500 通のメー

表 3 多数の送信 MTA が同時にメール配送を行って状況でのメール配送時間
Table 3 Delivery delay in case of heavy traffic.

	メール数	平均	標準偏差	最大	最小
優先	46 通	0.10 秒	0.02 秒	0.13 秒	0.07 秒
一般	454 通	5.0 秒	3.4 秒	16.9 秒	0.23 秒

ルのうち 46 通が優先受信 MTA で処理され，1 通あたりの平均処理時間が 0.10 秒であった，また，最小処理時間が 0.07 秒，最大処理時間が 0.13 秒，処理時間の標準偏差は 0.02 秒となった．残りの 454 通が一般受信 MTA で処理され，1 通あたりの平均処理時間が 5.0 秒であり，優先受信 MTA で処理されたメールと比べてかなり時間を要することが分かる．一般受信 MTA で処理されたメールでは，最小処理時間が 0.23 秒，最大処理時間が 16.9 秒である．その処理時間の標準偏差は 3.4 秒であることを確認した．

この結果から，試作システムは優先送信 MTA から送られるメールをそれ以外の一般送信 MTA から送られるメールと比べて配送遅延を大幅に減少させることができ，本システムは優先送信 MTA から送られるメールの優先配送処理に有効であるといえる．なお，一般受信 MTA での処理時間が長いのは SpamAssassin による処理時間の増加（最小処理時間で比較して約 3 倍）に加えて，負荷集中により見かけ上の処理速度が低下したためと思われる．

5. むすび

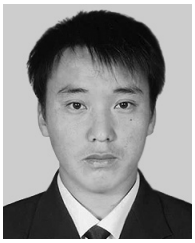
本論文では，spam メール対策により発生するメール配送遅延を減少させるため，L3 スイッチの PBR 機能を用いてホワイトリストを実現し，また，L3 スイッチ内のホワイトリストに登録された台数を一定数に抑え動的に変更するコントローラを追加することで，大規模なホワイトリストでも優先配送されるべきメールの配送速度を落とさずに優先配送できるシステムを提案した．またシステムを実装し，それぞれ正常に機能していることを確認した．

最後に，試作システムの有効性を確認するため，いくつかの性能評価実験環境を構築して評価実験を行い，試作システムは有効であることを確認した．今後の課題としては，本システムを実際の環境でも適用し，その有効性を検証することがあげられる．また，到着したパケットの内容に応じて動的に中継先を変更する手法は OpenFlow [15] などの SDN（software defined network）でも実現可能であることから，L3 スイッチの代わりに SDN 製品を用いて同様のシステムを実現することも今後の課題としてあげられる．

謝辞 本研究の一部は平成 23〜25 年度科学研究費補助金（基盤研究（C），課題番号 23500122）の補助を受けている．ここに記して感謝の意を表する．

参考文献

[1] ガーダ，諏訪秀治，山井成良，岡山聖彦，中村素典：レイヤ 3 スイッチを用いた大規模なホワイトリストに対応可能な電子メール優先配送システム，情報処理学会インターネットと運用技術研究会研究報告，Vol.2012-IOT-16, No.37, pp.1–6 (2012).
[2] 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の評価，情報処理学会第 75 回全国大会講演論文集，5X-8, Vol.2013, No.3, pp.377–378 (2013).
[3] 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 white list 自動作成システム，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, 情報処理学会 (2011).
[4] Harris, E.: The Next Step in the Spam Control War: Greylisting (online), available from ⟨http://projects.puremagic.com/greylisting/whitepaper.html⟩ (accessed 2013-06-28).
[5] Allman, E., Assmann, C. and Neil Shapiro, G.: Sendmail Installation and Operation Guide (online), available from ⟨http://www.sendmail.com/pdfs/open_source/installation_and_op_guide.pdf⟩ (accessed 2013-06-28).
[6] 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，情報処理学会インターネットと運用技術研究会研究報告，Vol.2010-IOT-8, No.14, pp.1–6 (2010).
[7] 丸山 伸，中村素典，岡部寿男，山井成良，岡山聖彦，宮下卓也：動的に応答を変える DNS を利用した電子メール受信の優先制御，情報処理学会論文誌，Vol.47, No.4, pp.1021–1030 (2006).
[8] Cisco, Inc.: Catalyst 3550 シリーズ スイッチの Switching Database Manager の説明と設定 (オンライン)，入手先 ⟨http://www.cisco.com/cisco/web/support/JP/100/1007/1007878_145-j.html⟩（参照 2013-06-28）.
[9] Bourke, T.: DSR (online), available from ⟨http://lbwiki.com/index.php/DSR⟩ (accessed 2013-06-28).
[10] Antsilevich, U.J.S., Kamp, P.-H., Nash, A., Cobbs, A. and Rizzo, L.: IPFW(8), FreeBSD System Manager's Manual (online), available from ⟨http://www.freebsd.org/cgi/man.cgi?query=ipfw⟩ (accessed 2013-06-28).
[11] Cobbs, A.: DIVERT(4), FreeBSD Kernel Interfaces Manual (online), available from ⟨http://www.freebsd.org/cgi/man.cgi?query=divert⟩ (accessed 2013-06-28).
[12] Venema, W.: Postfix manual – smtp-source(1) (online), available from ⟨http://www.postfix.org/smtp-source.1.html⟩ (accessed 2013-06-28).
[13] Venema, W.: The Postfix Home Page (online), available from ⟨http:///www.postfix.org/⟩ (accessed 2013-10-10).
[14] Apache Software Foundation: SpamAssassin: Welcome to SpamAssassin (online), available from ⟨http://spamassassin.apache.org/⟩ (accessed 2013-06-28).
[15] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S. and Turner, J.: OpenFlow: Enabling Innovation in Campus Networks (online), available from ⟨http://www.openflow.org/documents/openflow-wp-latest.pdf⟩ (accessed 2013-06-28).



ガーダ （学生会員）

平成 24 年岡山大学大学院自然科学研究科電子情報システム工学専攻博士前期課程修了．同年同大学院自然科学研究科産業創成工学専攻博士後期課程に進学し，現在在学中．主に重要な電子メールの優先配送に関する研究に従事．ネットワークセキュリティ，分散システム等の研究に興味を持つ．

山井 成良 （正会員）

昭和 59 年大阪大学工学部電子工学科卒業．昭和 61 年同大学大学院博士前期課程修了．昭和 63 年同大学院基礎工学研究科（物理系専攻情報工学分野）博士後期課程退学．同年奈良工業高等専門学校情報工学科助手．同講師，大阪大学情報処理教育センター助手，同大学大型計算機センター講師，岡山大学総合情報処理センター（現，情報統括センター）助教授を経て，平成 18 年より同教授．分散システム，ネットワーク運用管理，ネットワークセキュリティの研究に従事．IEEE，電子情報通信学会各会員．博士（工学）．

岡山 聖彦 （正会員）

平成 2 年大阪大学基礎工学部情報工学科卒業．平成 4 年同大学大学院基礎工学研究科博士前期課程修了．同年同大学院基礎工学研究科博士後期課程を退学し，同大学工学部助手．奈良先端科学技術大学院大学情報科学研究科助手，岡山大学工学部助手，同大学総合情報基盤センター助教を経て，平成 22 年同大学情報統括センター助教．平成 23 年同准教授．博士（工学）．インタネットアーキテクチャ，ネットワーク管理，ネットワークセキュリティの研究に従事．電子情報通信学会会員．

河野 圭太 （正会員）

平成 12 年大阪大学工学部電子情報エネルギー工学科卒業．平成 14 年同大学大学院工学研究科博士前期課程修了．平成 16 年同大学院情報科学研究科博士後期課程を修了し，同年岡山大学総合情報基盤センター助手．平成 19 年同センター助教，平成 22 年同大学情報統括センター助教を経て，平成 23 年同センター准教授．博士（情報科学）．モバイルネットワーク，分散システムの研究に従事．IEEE，電子情報通信学会各会員．

中村 素典 （正会員）

平成 6 年京都大学大学院工学研究科博士後期課程単位取得退学．立命館大学理工学部助手，京都大学経済学部助教授，京都大学学術情報メディアセンター助教授等を経て，平成 19 年より国立情報学研究所特任教授，現在に至る．博士（工学）．IEEE，日本ソフトウェア科学会，電子情報通信学会各会員．コンピュータネットワーク，ネットワークコミュニケーション，認証連携等の研究に従事．