Vol.2012-IOT-16 No.37
2012/3/16

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

ガ ー ダ[†1] 諏訪秀治[†1] 山井成良[†2]
岡山聖彦[†2] 中村素典[†3]

重要な電子メールを遅延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，本稿ではレイヤ 3 スイッチのポリシールーティング機能を用いてホワイトリストを実現し，また登録する送信 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い，大規模なホワイトリストをすべてレイヤ 3 スイッチに登録する場合と比較して高速に伝送できることを示す．

E-mail Priority Delivery System with Large-sized Whitelist Using Layer 3 Switch

Gada,[†1] Shuji Suwa,[†1] Nariyoshi Yamai,[†2]
Kiyohiko Okayama[†2] and Motonori Nakamura[†3]

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.

1. まえがき

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．従来の電子メールサーバの運用では，送信者から受信者へ確実に配送することが最大の目標であったが，現在では電子メールを遅延無く受信者へ配送することも求められている．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．多くの組織では spam メールに対処するため greylisting[1)]，greet pause[2)] 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迷惑メールと誤判定されるなど，通常のメール配送に支障が生じる状態が発生している[3)]．

この問題に対処するため，上記のような spam メール対策を採用する際には信頼できる送信 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[3)] 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．

そこで本稿ではポリシールーティング（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．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．

†1 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University
†2 岡山大学情報統括センター
Center of Information Technology and Management, Okayama University
†3 国立情報学研究所
National Institute of Informatics

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)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[4]，(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[3] 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 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 メールと誤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できる．特に greylisting や greet pause 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，MTA 自身がホワイトリストを持つ場合，その 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 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 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 4) 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延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)，5) 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延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，全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）のポリシルーティング（以下，PBR: Policy Based Routing）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[6] 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処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（L3 スイッチ）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．そこで本稿では 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な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

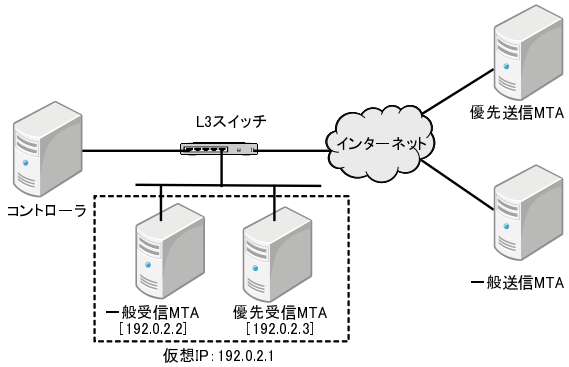

図 1 提案システムの構成

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 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．コントローラは大規模なホワイトリストを持ち，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する機能を持つ．また，L3 スイッチとの間で制御用コネクションを常時確立し，必要に応じて L3 スイッチの設定を変更する役割を果たす．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．

以下では，この構成における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 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[7] と同等である．

3.4 L3 スイッチへのホワイトリストへの登録

コントローラは L3 スイッチ内のホワイトリストに登録されていない送信 MTA が優先送信の対象かどうかを判断し，もし該当すれば L3 スイッチ内のホワイトリストに登録するように動作する．このような動作を可能にするため，**図 2** に示すように，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（同図 (1)），コントローラに中継するように動作する（同図 (2)）．コントローラは SYN パケットを受け取ると送信元 IP アドレスが優先送信 MTA のものであるかどうかを決定し（同図 (3)），もしそうであれば L3 スイッチのホワイトリストにこの送信元 IP アドレスを登録して（同図 (4)），その後に SYN パケットを L3 スイッチに中継する（同図 (5)）．これにより SYN パケットおよび以降のパケットは優先受信 MTA に中継される（同図 (6)）．また，送信 MTA が優先配送の対象でない場合には，コントローラは L3 スイッチの設定を変更せず，単に SYN パケットを L3 スイッチ経由で一般送信 MTA に中継する．これらの動作により，優先送信 MTA，一般送信 MTA のいずれも最初の SYN 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送信 MTA を削除する必要がある．ただし，登録数の上限は TCAM の使用量によって定まり，この量は登録する優先送信 MTA の IP アドレス[⋆1]や他の用途での使用[⋆2]に依存するため，明確な上限は不明である．そ

⋆1 複数の IP アドレスが併合されて 1 つのエントリとして登録される場合が存在する．
⋆2 たとえばフィルタリングのために ACL(Access Control List) を作成する場合など．

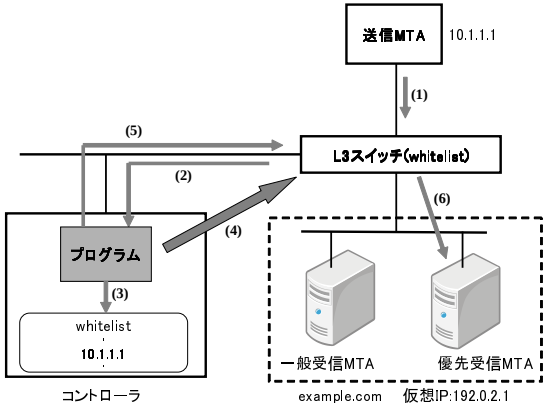

図 2 優先送信 MTA のホワイトリストへの登録時の動作

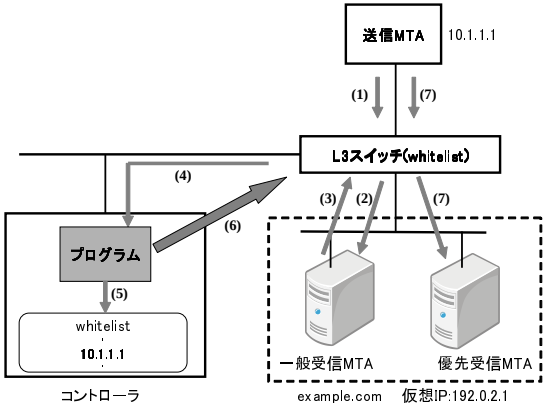

図 3 優先送信 MTA のホワイトリストからの削除時の動作

こで，本システムでは上限数を超えないようにする代わりに登録後一定時間が経過した優先送信 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．その場合，**図 3** に示すように削除後に優先送信 MTA から送られたパケット（同図 (1)）は一般受信 MTA に中継される（同図 (2)）ため，一般受信 MTA から RST フラグ付きパケット（RST パケット）が返送され（同図 (3)），SMTP コネクションが強制切断される結果となる．そこで，このような結果を引き起こさないようにするため，一般受信 MTA から送られた RST パケットをコントローラが受け取り（同図 (4)），この RST パケットの宛先がホワイトリストから直前に削除した優先送信 MTA のものであれば（同図 (5)）再度ホワイトリストに登録する（同図 (6)）ようにする．また，コントローラが受信した RST パケットはそのまま破棄する．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する（同図 (7)）ため，メール配送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，提案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．

表 1 コントローラ用 PC の諸元

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

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．

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，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 を一旦 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 分毎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 パケットの送受信および RST パケットの受信を行う機能，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[8] および divert[9] 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 パケットや RST パケットを受信した場合には直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，全ての送信 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 5) 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 パケットを含めた全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[⋆1]，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一旦中継されるが何の処理も行われず直ちに 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．

表 2 access-list への登録処理および再利用処理時間

登録処理時間	再利用処理時間
7.8 (ms)	54.7 (ms)

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，本システムは設計通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．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，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．

4.4 優先送信 MTA 登録台数に対するメール配送時間

最後に，本システムの有効性を確認するため，優先送信 MTA 登録台数を変化させた場合のメール配送時間を測定した．その結果を**図 4** に示す．なお，配送する電子メールの大きさは約 10MB とし，また登録する優先送信 MTA の IP アドレスはランダムに決定した．ま

⋆1 同一優先送信 MTA の重複登録をチェックしているため．

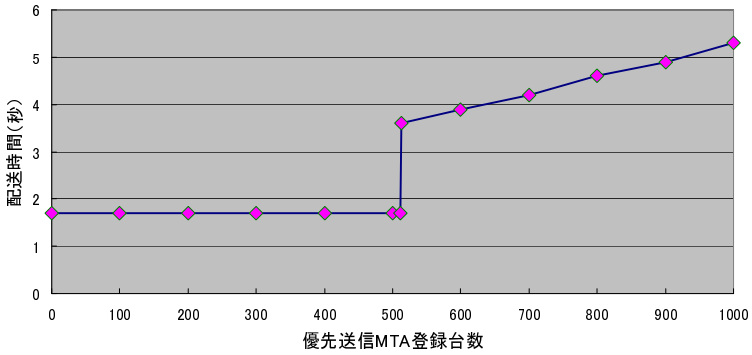

図 4 優先送信 MTA 登録台数に対するメール配送時間

た，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．

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わかる．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[6] 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 登録台数を抑えればメール配送時間を減少させることができるため，本システムは有効であるといえる．

5. むすび

本稿では，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した．また，試作システムを用いてその有効性を確認した．

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挙げられる．特に，多数の送信サーバがメール配送を行っている状況での性能評価実験は機材の都合で実施できなかったため，この実験を行って優先配送機能が正常に機能していることをまず確認したい．また，L3 スイッチの設定変更の際に，稀ではあるが予期しない中継処理が過渡的に見られたことから，L3 スイッチは動的な設定変更を想定していないと思われる．そこで，L3 スイッチの代わりに OpenFlow スイッチ[10] 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挙げられる．

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) Evan Harris: The Next Step in the Spam Control War: Greylisting (online), available from ⟨http://projects.puremagic.com/greylisting/whitepaper.html⟩ (accessed 2012-02-12).
2) 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 2012-02-12).
3) 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).
4) 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).
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 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，情報処理学会，pp.39–44 (2011).
6) Cisco, Inc.: Catalyst 3550 シリーズ スイッチの Switching Database Manager の説明と設定 (online)，⟨http://www.cisco.com/cisco/web/support/JP/100/1007/1007878_145-j.html⟩ (accessed 2012-02-12).
7) Tony Bourke: “DSR” (online)，⟨http://lbwiki.com/index.php/DSR⟩ (accessed 2012-02-12).
8) 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 2012-02-12).
9) Cobbs, A.: DIVERT(4), FreeBSD Kernel Interfaces Manual (online), avaiable from ⟨http://www.freebsd.org/cgi/man.cgi?query=divert⟩ (accessed 2012-02-12).
10) McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., Turner J.: “OpenFlow: Enabling Innovation in Campus Networks” (online), ⟨http://www.openflow.org/documents/openflow-wp-latest.pdf⟩ (accessed 2012-02-12) (2008).