情報処理学会論文誌 Vol.56 No.3 777–787 (Mar. 2015)

電子メール優先配送システムにおける信頼できるMTAから送られた迷惑メールへの対策

ガーダ[1,a)] 松岡 政之[2] 山井 成良[3] 岡山 聖彦[4] 河野 圭太[4] 中村 素典[5]

受付日 2014年6月25日, 採録日 2014年12月3日

概要：迷惑メールの蔓延により発生する膨大な量のトラフィックがネットワークや電子メールサーバに大きな負荷をかけ，通常の電子メール配送に遅延が発生している．これに対して，重要な電子メールを遅延なく配送できるようにするため，我々の研究グループは信頼できるMTA（Mail Transfer Agent）から送られる電子メールを専用のMTAで受信する，電子メール優先配送システムを提案した．このシステムでは信頼できる送信MTAから送られる電子メールを簡単な検査だけで受信するため，迷惑メール対策により発生する配送遅延を軽減することが可能になる．しかし，本システムでは信頼できるMTAから迷惑メールが送られてきた場合も簡単な検査しか行えないという問題があった．そこで本論文では信頼できるMTAから送られてきた電子メールであっても迷惑メールと疑われる場合には，一時エラーや強制切断により一般用のMTAへ再送させ，十分な検査を行う方法を提案する．

キーワード：電子メール，迷惑メール対策，優先配送，SMTP

Countermeasure of Spam Mails Sent by Trusted MTAs on E-mail Priority Delivery System

Gada[1,a)] Masayuki Matsuoka[2] Nariyoshi Yamai[3] Kiyohiko Okayama[4] Keita Kawano[4] Motonori Nakamura[5]

Received: June 25, 2014, Accepted: December 3, 2014

Abstract: Enormous traffic generated by spam mails brings heavy load to networks and mail servers, which causes a large delay on legitimate mail delivery. In order to deliver important e-mails without unnecessary delay, we proposed an e-mail priority delivery system, where a dedicated receiving Mail Transfer Agent (MTA) receives all messages sent from trusted MTAs and performs only simple anti-spam measures. However, this system has some problems such that the dedicated receiving MTA easily receives even spam mails sent from trusted MTAs through only simple anti-spam measures. In this paper, we propose a method to perform full anti-spam measures on suspicious messages sent from trusted sending MTAs, by introducing tempfailing and SMTP session abort on the dedicated receiving MTA.

Keywords: E-mail, anti-spam, priority delivery, SMTP

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．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的であった

[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] 株式会社インフォメーション・ディベロプメント
Information Development Co., Ltd., Chiyoda, Tokyo 102–0084, Japan
[3] 東京農工大学大学院工学研究院
Institute of Engineering, Tokyo University of Agriculture and Technology, Koganei, Tokyo 184–8588, Japan
[4] 岡山大学情報統括センター
Center for Information Technology and Management, Okayama University, Okayama 700–8530, Japan
[5] 国立情報学研究所
National Institute of Informatics, Chiyoda, Tokyo 101–8430, Japan
[a)] gada.net@s.okayama-u.ac.jp

© 2015 Information Processing Society of Japan

が，現在では電子メールを遅滞な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迷惑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電子メールサーバに大きな負荷をかけ，通常の電子メール配送に遅延が発生している．多くの組織では迷惑メールに対処するため greylisting [1]，greet pause [2]，フィルタリングなどの様々な対策を適用している．しかし，これらの対策により，たとえば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，あるいは重要な電子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]．

重要な電子メールを遅滞なく受信者へ配送する手段として，信頼できる MTA（Mail Transfer Agent）から送られる電子メールを専用の MTA で受信し，優先的に配送する仕組み（優先配送システム）がしばしば採用されている．その実装例として，我々の研究グループではレイヤ 3 スイッチのポリシルーティング機能を用いて小規模なホワイトリストに登録する送信 MTA の数が増加した場合でも伝送速度の劣化を抑制できる優先配送システムを提案し，その有効性を確認した [4], [5]．

従来の優先配送システムでは，信頼できる送信 MTA から送られてきた電子メールはすべて正当な電子メールであると見なし，専用の MTA で無条件であるいは比較的簡単な検査を経て受信するように構成されているものが多い．このような構成により，専用の MTA における検査によるオーバヘッドを軽減したり，検査用の機器やライセンスの削減により運用コストを低く保ったりする効果が期待できる．ところが実際には，信頼できる送信 MTA から送られてきた電子メールであっても，ウィルス感染端末からの発信，パスワード漏洩による第三者からの発信，あるいは転送設定などにより，迷惑メールが混在する可能性があり，簡単な検査だけで受信すると危険が生じる場合もありうる．

そこで，本論文では優先配送システムにおいて，信頼できる MTA から送られてきた電子メールにまず簡単な検査を行い，迷惑メールと疑われる場合には，一時エラーや強制切断により一般用の MTA へ再送させ，十分な検査を行う方法を提案する．また，専用の MTA でのオーバヘッドを軽減するため，迷惑メールの疑いがあるかどうかを早い段階で判定する方法についても示す．

以下，2 章では電子メール優先配送システムおよび本研究で対象とするシステムとその問題点を述べ，3 章でその問題点を解決する提案システムの実現方針について述べ，4 章では提案システムの実装と動作確認について述べる．最後に，5 章で本論文をまとめ，今後の課題について述べる．

2. 電子メール優先配送システムとその問題点

本章では，既存の電子メール優先配送システムとして，特に我々の研究グループが開発したシステムについて，その構成や仕組みを説明する．また，電子メール優先配送システムが持つ問題点についても述べる．

2.1 電子メール優先配送システム

一般に受信 MTA で処理する電子メールのトラフィック量や迷惑メール対策による負荷が高くなると，電子メールの配送遅延時間は長くなる．電子メール優先配送システムは，一般の電子メールと比較して小さい遅延時間で重要な電子メールを配送するシステムである．多くのシステムでは信頼できる送信 MTA のリストをホワイトリストとして持ち，ホワイトリストに含まれる送信 MTA から送られてきた電子メールは無条件あるいは比較的簡単な検査を経て受信するよう構成されている．

電子メール優先配送システムを実現する代表的な方法として，まず受信 MTA 自身がホワイトリストを持ち，送信 MTA がホワイトリストに含まれるかどうかによって受信 MTA 内での処理内容を切り替える方法があげられる．しかし，この方法では，受信 MTA が 1 台しかなく，優先配送すべき電子メール（優先配送メール）だけではなくそれ以外の電子メール（一般メール）も混在して受信することになるため，受信 MTA が過負荷になり，優先配送メールの処理に遅延が発生するという問題が生じる．

電子メール優先配送システムを実現する別の方法として，一般メールを受信する MTA（一般受信 MTA）と優先配送メールを受信する MTA（優先受信 MTA）の 2 種類の MTA を用意し，送信 MTA が信頼できるかどうかによって配送先を切り替える方法がある．この方法では配送先を切り替える方法として，動的に応答を変える DNS サーバを用いる方法 [6]，PC ルータでポリシルーティング（PBR: Policy Based Routing）機能を用いる方法 [3]，レイヤ 3（L3）スイッチで PBR 機能を動的に設定する方法 [4], [5] などがある．本論文では 2 種類の MTA を用いる電子メール優先配送システムを対象とする．

2.2 2 種類の MTA を用いる電子メール優先配送システム

本論文で対象とする，2 種類の MTA を用いる電子メール優先配送システムの例として，文献 [4], [5] のシステムの構成および動作を説明する．本システムは**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 アドレスを持つ．共通の IP アドレスは電子メール配送に用いられ，個別の IP アドレスは L3 スイッチでパケットの中継先を指定する際に用いられる．L3 スイッチは PBR

© 2015 Information Processing Society of Japan

機能を持ち，自身の持つホワイトリストに基づいてパケットの中継先を決定する．また，ホワイトリストに含まれない送信 MTA からの SYN パケットなど，ホワイトリストの更新判断に必要なパケットはコントローラに中継する．コントローラは大規模なホワイトリストを持ち，送信 MTA が優先配送の対象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，L3 スイッチ内のホワイトリストに登録される送信 MTA を動的に変更する．本システムは PC ルータで PBR 機能を用いる方法とは異なり，コントローラ内の大規模ホワイトリストに登録する送信 MTA の数が増加しても優先配送メールの配送速度を落とさず優先配送できるという特徴を有する．

なお，本システムでは宛先ドメインに対する MX レコードとして，共通の仮想 IP アドレスに対応するホスト名に加えて，それより低い優先度で一般受信 MTA 固有の IP アドレスに対応するホスト名を登録するものとする．これにより，優先受信 MTA に障害が発生している場合でも一般受信 MTA で優先配送対象の電子メールを受信することができ，配送への影響を軽減することが可能となる．

2.3 従来の電子メール優先配送システムの問題点

従来の電子メール優先配送システムでは，基本的に電子メールの内容ではなく，送信 MTA に応じて配送先の MTA が決定される．したがって信頼できる MTA から迷惑メールが送られた場合，この迷惑メールは優先受信 MTA で処理されるため，比較的簡単な対策しか行われず，結果として迷惑メールがそのまま受信者に届くという問題がある．このような問題は，たとえば信頼できる MTA 上で優先配送システムに向かって転送設定が行われている場合，信頼できる MTA の利用者がウイルスに感染した場合，信頼できる MTA の利用者名とパスワードが不正利用された場合などに起こりうる．

この問題への対策として，優先受信 MTA でも一般受信 MTA と同等の迷惑メール対策を行う方法が考えられる．しかし，この方法では迷惑メール対策処理の増加により優先受信 MTA の負荷が増大し，特に大量の電子メールが信頼できる MTA から配送された場合には配送遅延が無視できなくなることが予想される．また，優先受信 MTA にも同じ程度の迷惑メール対策を導入すると金銭的な運用コストが増加するという別の問題も生じる．

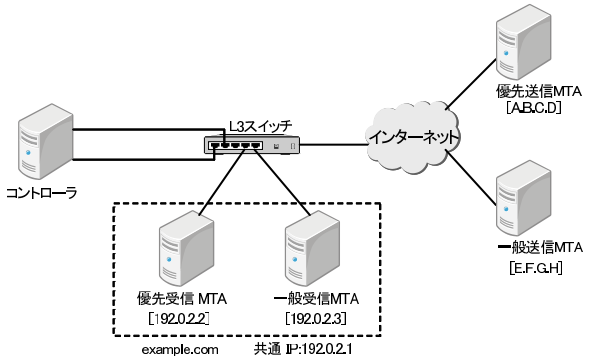

図 1 既存システムの構成
Fig. 1 Existing system configuration.

3. 優先受信 MTA における迷惑メール処理

前章で述べたように，信頼できる MTA から優先受信 MTA 宛に大量の迷惑メールが送られる状況では，優先受信 MTA 上で十分な対策が行われなかったり，配送遅延が増加したり，あるいは金銭的な運用コストの増加を招いたりするなどの問題が生じる．そこで，本章ではこれらの問題を軽減するため，優先受信 MTA における迷惑メール処理方法について述べる．

3.1 提案手法の概要

従来の電子メール優先配送システムでは SMTP（Simple Mail Transfer Protocol）プロトコル [7] による接続（SMTP コネクション）確立時に配送先となる受信 MTA を決定していた．この時点での受信 MTA 決定で利用可能な情報は実質的には送信 MTA の IP アドレスしかないため，同一の信頼できる MTA から通常の電子メールと混在して迷惑メールが送られると配送先を切り替えることができない．

一方，図 2 に示すように，いったん SMTP コネクションを確立した後には，エンベロープやヘッダなどから多くの情報が得られる．特に，ヘッダ中に含まれる情報は一般的に迷惑メールの判断に使われており，非常に有用である．

これらの情報のうち，エンベロープの情報は SMTP の MAIL コマンドや RCPT コマンドの引数として与えられるため，それぞれのコマンドが入力されたときに検査を行い，迷惑メールの疑いがある場合にはコマンドの応答として一時エラーを返すことにより，ただちに次の優先度を持つ一般受信 MTA に配送先を切り替えることができる．一方，ヘッダ中に含まれる情報は DATA コマンド後に入手可能であるが，SMTP ではヘッダ終了時に一時エラーを返す

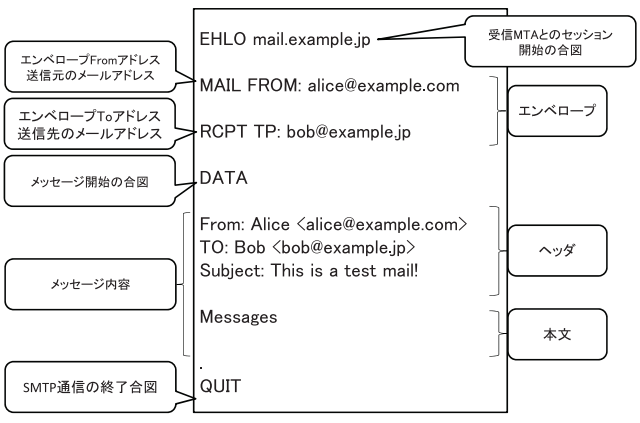

図 2 受信 MTA が利用可能な情報
Fig. 2 Information available on receiving MTA.

© 2015 Information Processing Society of Japan

ことができない．

代わりの方法として，優先受信 MTA で信頼できる送信 MTA から送られた電子メールを受信した後，比較的簡単な検査を行い，迷惑メールの疑いがある場合にはこれを一般受信 MTA に転送する方法が考えられる．この方法であれば優先受信 MTA では迷惑メール対策を新たに行う必要がなくなり，金銭的な運用コストの増加も招かない．しかし，この方法でも，特に信頼できる MTA からウイルスを含んだ電子メールのようなサイズの大きい電子メールが多数送られてきた場合，優先受信 MTA の負荷が増大するという問題は解消できない．

そこで，本論文では受信中にエンベロープ，ヘッダ，本文などを検査し，迷惑メールの疑いがあると判断した早期の段階で，MAIL コマンドや RCPT コマンドに対して一時エラーを返したり，ヘッダや本文の受信中に SMTP コネクションを強制切断 [8] したりする方法を提案する．SMTP コネクションの強制切断は一時エラーの一種として扱われる [7] ため，このように動作することで，迷惑メールの疑いがある電子メールを早い段階で次の優先度を持つ MX である一般受信 MTA で処理することができ，優先受信 MTA の負荷をあまり増加させることなく十分な迷惑メール対策を行うことが可能になる．

なお，SMTP コネクションの強制切断は我々の以前の研究 [8] でも用いているが，本論文とは目的や切断条件が異なる．文献 [8] では，greylisting のような再送を求める迷惑メール対策（tempfailing）を用いる場合に再送かどうかを確実に判定することを目的として，初回受信時に Message-ID などのヘッダ情報を取得した後に強制切断を行う．一方，本論文では迷惑メールの疑いがある場合に早期に一般受信 MTA で処理させることを目的として，ヘッダや本文の内容に基づき強制切断を行うかどうか，行う場合にはいつ行うかを決定する．

3.2 優先受信 MTA での迷惑メール判定

提案方法を実現するうえで，迷惑メールの疑いがあるかどうかをどのような基準で判定するかが重要となる．たとえば，添付ファイルが含まれる電子メールはそうでない電子メールと比較して十分な検査を行う必要がある．ただし，送信 MTA で一般受信 MTA と同じ検査を行っているのであれば，一般受信 MTA での再検査は不要で，優先受信 MTA でそのまま受信してもかまわない．そこで，提案方法では送信 MTA に応じて迷惑メール検査の評価基準を個別に設定できることを前提としている．

本方法における迷惑メールの判定は，(1) エンベロープ情報受信時，(2) ヘッダ受信時，(3) 本文受信時の各時点で行うことが可能である．以下では，各時点でどのような基準に基づいて迷惑メールの検査が行えるかについて述べる．

なお，本論文では一時エラーや強制切断により早期に判定可能な検査内容について述べるが，その有効性については本論文で議論する範囲を越える点に注意する．

3.2.1 エンベロープ情報受信時の判定基準

SMTP コネクション確立後，DATA コマンドが送られる前に優先受信 MTA が得られる情報には，送信元 IP アドレス，エンベロープ From アドレス，エンベロープ To アドレスなどがある．これらの情報を用いることで，たとえば，エンベロープ From アドレスと送信元 IP アドレスを SPF（Sender Policy Framework）[9] を用いて照合することにより，転送された電子メールかどうかを判別し，転送された電子メールであれば MAIL コマンドに対して一時エラーを返して一般受信 MTA への再送を送信 MTA に促すことができる．

3.2.2 ヘッダ受信時の判定基準

DATA コマンドの後，優先受信 MTA が最初に受信するヘッダからは多くの情報が得られる．これらを組み合わせれば様々な判定基準を設定可能である．たとえば，ヘッダ From アドレスと送信元 IP アドレスとの照合，Content-Type ヘッダによる添付ファイルの有無や記述言語の検査，あるいは送信側での迷惑メール検査の有無などが考えられる．

3.2.3 本文受信時の判定基準

上記のように，もしメッセージ全体を受信した後に迷惑メール検査を行うのであれば優先受信 MTA の負荷を軽減することにはならない．しかし，提案手法では SMTP コネクションを途中で強制切断機能の利用を前提としているため，本文受信中の早い段階で判定を行うことができれば優先受信 MTA の負荷を軽減することにつながる．本文受信時の判定の例として，添付ファイルが S/MIME [10] の署名やテキストファイルのような安全なものだけであればそのまま優先受信 MTA で受信し，それ以外の種類のファイルに関する Content-Type が見つかればその時点で強制切断する方法が考えられる．

3.3 一般受信 MTA での処理

提案方法では，信頼できる送信 MTA から見ると一般受信 MTA はセカンダリ MX であるが，一般受信 MTA 自身は信頼できる送信 MTA 以外の送信 MTA から見た場合に当該ドメインのプライマリ MX であるため，信頼できる送信 MTA から送られた電子メールに対してもこれを受信した後，優先受信 MTA には中継せず，迷惑メール検査を行った後で宛先メールボックスにメッセージを書き込む．したがって，基本的には一般受信 MTA の設定は変更する必要がない．しかし，一般受信 MTA で tempfailing を採用している場合には以下に示す動作により，一般受信 MTA での処理が大幅に遅れることとなる．

(1) まず，信頼できる MTA から優先受信 MTA への配送が一時エラーや強制切断により失敗した場合，信頼でき

© 2015 Information Processing Society of Japan

る送信 MTA はセカンダリ MX である一般受信 MTA にただちに再送する．

(2) 一般受信 MTA が一時エラーを返した場合，信頼できる送信 MTA は一定時間待ったあと，再び優先受信 MTA へ配送を試みる．

(3) この配送が再び失敗し，一般受信 MTA へ再送を行った段階で，初めてこの配送は成功する．

したがって，この配送は少なくとも信頼できる送信 MTA での再送間隔だけ遅延することとなり，また優先受信 MTA は同じ電子メールに対して 2 度の検査を行うため，その負荷も増大する．

そこで，このような動作を防止するため，一般受信 MTA では信頼できる送信 MTA をホワイトリストに登録するか，あるいは優先受信 MTA から再送かどうかを判断するのに必要な情報を取得する必要が生じる．ただし，これらの対策は複数の受信 MTA を用いた tempfailing では一般的であり [3], [8], [11], [12]，実装は比較的容易である．そのため，本論文では一般受信 MTA における対策は割愛し，優先受信 MTA における対策に焦点を当てる．

4. 試作システムの実装と動作確認実験

提案方法により迷惑メールの疑いがある電子メールを早期に一般受信 MTA に処理させることが可能であることを検証するため，我々は試作システムを実装し，動作確認実験を行った．本章では試作システムの実装方法と動作確認実験の内容を述べる．

4.1 試作システムの概要

我々は優先受信 MTA において電子メールの受信中に迷惑メールの可能性があると判断したメールについて，その通信を強制切断することによる迷惑メール対策システムを実装した．本実装では，受信 MTA として Postfix [13]，電子メールフィルタとして Postfix キュー投入前コンテンツフィルタ（以下，キュー投入前フィルタ）[14] を使用し，フィルタプログラムは Perl [15] を用いて作成した．

キュー投入前フィルタは**図 3** に示すように，メッセージが Postfix キューに投入される過程において，前段に位置する SMTP サーバ（フィルタ前 SMTP サーバ）からメッセージを受け取り，メッセージの内容を監視してフィルタ前 SMTP サーバに終了コードを返したり，メッセージの内容を変更して後段に位置する SMTP サーバ（フィルタ後 SMTP サーバ）に渡したりすることができる，一種のプロクシである．そのため，受信 MTA がメッセージを受信する前にメッセージの内容に基づいて迷惑メールの可能性があるかどうかの判断を行うことができる．

フィルタ前 SMTP サーバおよびキュー投入前フィルタの動作は次に示すとおりである．

(1) EHLO コマンドおよび MAIL FROM コマンドに対する応答はフィルタ前 SMTP サーバが送信 MTA に応答する．この時点ではキュー投入前フィルタにはいっさいデータは送信されない．

(2) RCPT TO コマンドを受け取った時点でフィルタ前 SMTP サーバは送信 MTA に応答を返すとともに，それまでに受信したエンベロープ情報をキュー投入前フィルタに送信する．キュー投入前フィルタは受け取ったデータをフィルタ後 SMTP サーバへ送信する．以降，キュー投入前フィルタは受け取ったデータを順次フィルタ後 SMTP サーバへ送信する．

(3) DATA コマンドを受け取った時点でフィルタ前 SMTP サーバは送信 MTA に応答を返すとともに，DATA コマンドをキュー投入前フィルタに送信する．

(4) フィルタ前 SMTP サーバは送信 MTA から送られてきたデータをバッファリングする．しかし，受信バッファの容量を超えるデータを受信した場合その時点でバッファリングしているデータをキュー投入前フィルタに送信し，受信データを新たにバッファリングする．

(5) メッセージ終了の合図である「.」を受け取った時点でフィルタ前 SMTP サーバはバッファリングしている受信データをキュー投入前フィルタに送信する．一方，キュー投入前フィルタはフィルタ前 SMTP サーバに応答を返す．「.」を受け取ったフィルタ後 SMTP サーバはキューに一時保存しておいた電子メールを宛先メールボックスへ配送する．

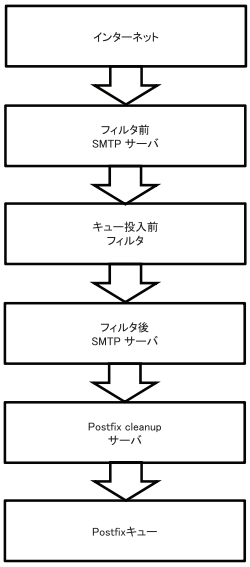

図 3 Postfix におけるキュー投入前フィルタを用いた場合の処理の流れ

Fig. 3 Process flow with before-queue filter on Postfix.

4.2 キュー投入前フィルタを用いた強制切断プログラム

本節ではキュー投入前フィルタを用いた強制切断プログラムについて説明する．本フィルタでは，SPF を用いた判

© 2015 Information Processing Society of Japan

定，エンベロープ From アドレスとヘッダ From アドレスを用いた判定，添付ファイルの種類による判定についての実装を行った．また，これらのルールについて送信 MTA に応じて容易に設定できるように実装を行った．実装したフィルタプログラムは TCP 10025 番ポートでフィルタ前 SMTP サーバからのコネクションを待ち受け，またフィルタ後 SMTP サーバが待ち受ける TCP 10026 番ポートへのコネクションを持つ．

4.2.1 SPF を用いた判定

SPF は受信した電子メールに対してエンベロープ From に示されている送信元ドメインと送信 MTA の IP アドレスを DNS により照合し，この電子メールの送信元が偽装されたものでないかを検出することを目的としている．一般に転送された電子メールでは SPF による検査が失敗する場合が多いため，信頼できる MTA から SPF による検査に失敗した電子メールが届いた場合，その電子メールは転送されたものであるか，あるいはウイルス感染などの理由により送信された迷惑メールの可能性が非常に高い．そのため，SPF による検査に失敗した電子メールは一般受信 MTA で十分な検査を行うべきであるといえる．

通常 SPF はエンベロープ情報を受信した時点で判断することができるが，試作システムの設計段階ではキュー投入前フィルタで集中的に判定を行うようにしたため，送信 MTA の IP アドレスを事前に取得することが困難であった．そこで，試作システムの実装では電子メールヘッダ中の Received ヘッダに含まれる IP アドレスを用いて SPF の判定を行うようにした．この実装方法では判定時期がエンベロープ情報受信時よりは遅くなるが，それでもキュー投入前フィルタがヘッダを受信した時点で判定を行うことができるため，SPF の検査に失敗した電子メールに対してはサイズの大きいものでもメッセージ全体を受信前に切断することが可能である．

4.2.2 エンベロープ From アドレスとヘッダ From アドレスを用いた判定

この判定条件では，通常の場合は受信電子メールのエンベロープ From アドレスとヘッダ From アドレスは一致しているはずであるという事実を前提にしている．受信電子メールのエンベロープ From アドレスとヘッダ From アドレスが一致するかどうかを検査し，一致しなければ迷惑メールの可能性があると判断する．両者が一致しない場合，信頼できる MTA を送信元あるいは中継地点として利用した迷惑メールの可能性がある．特に信頼できる送信 MTA である利用者が受信 MTA 宛に転送するように設定している場合，エンベロープ From アドレスとヘッダ From アドレスが一致しないことが多いが，このような場合では送信 MTA 側で転送に特段の制限を行っていない限り通常の電子メールに加えて迷惑メールも転送されるため，一般受信 MTA で十分な検査を行うべきである．この判定条件は優先受信 MTA で受信した電子メールが送信 MTA から転送されたものであるかどうかを判別する際に有効である[*1]．

また，信頼できる送信 MTA でメーリングリストを運用している場合，設定によっては必ずしも両者が一致するとは限らない．もしそのような設定のメーリングリストが投稿者の認証を行わずに配送しているのであれば，迷惑メールも優先受信 MTA に配送される可能性がある．このようなメーリングリストから配送された電子メールを優先受信 MTA で受信した場合，上記の判定条件により，このような電子メールを優先受信 MTA ではなく一般受信 MTA で受信し，精密な検査を行うことが可能になる．ただし，メーリングリストの投稿において管理者の承認が必要であったり投稿者の認証を行ったりするように設定されている場合など，エンベロープ From アドレスとヘッダ From アドレスが一致しなくても，必ずしも一般受信 MTA で受信する必要があるとは限らない点に注意する．このような場合に対処するには，4.2.5 項で述べるように送信 MTA に応じて判定内容を設定する必要がある．

この判定方法ではヘッダ From アドレスを用いるため，ヘッダ情報を受信したタイミングで判断を行い，迷惑メールの可能性があると判断すれば本文を受信する前に切断することが可能である．

4.2.3 添付ファイルの種類による判定

電子メールはコンピュータウイルスなどのマルウエアの配布経路の 1 つであり，特にマルウエアは添付ファイルとして配布されることが多い [16]．そのため，添付ファイルを含む電子メールは特に十分な検査を行う必要がある．しかし，たとえばテキストファイルだけが添付されている電子メールなど，添付ファイルを含む電子メールがすべて危険であるとは限らない．そこで，本項では添付ファイルを含む電子メールにおける判定方法について述べる．

図 4 は添付ファイルを含む電子メールの添付ファイルに関連する部分の例である．この図の 2 行目に示すとおり，添付ファイルを含む電子メールは「Content-type: multipart/mixed;」をヘッダに含んでおり，その次の行に「boundary=”ランダムな文字列”」を含んでいる [17]．この二重引用符で囲まれた文字列は電子メール 1 通ごとに異なり，またその電子メール内で固有の文字列で構成されている．また，それ以降本文中でこの文字列の先頭に”- -”を付け加えた文字列は添付ファイルごとの境界を表している．図 4 の場合では 6 行目が本文の開始位置を表し，12 行目が本文の終わりかつ 1 つ目の添付ファイルの開始位置を表している．また，7 行目は本文がテキストであることを示し，13 行目は添付ファイルがテキストファイルであることを示している．これを用いれば，添付ファイルとは無関係に本文中に Content-Type などの記述があっても，そ

[*1] 4.2.1 項で述べた SPF による判定でも SPF レコードの設定によっては判別可能な場合がある．

© 2015 Information Processing Society of Japan

```
MIME-Version: 1.0
Content-Type: multipart/mixed;
 boundary="------------101080403040808080405050"

This is a multi-part message in MIME format.
--------------010108040304080808040505
Content-Type: text/plain; charset=ISO-2022-JP
Content-Transfer-Encoding: 7bit

test message

--------------010108040304080808040505
Content-Type: text/plain; charset=Shift_JIS;
 name="testfile.txt"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename="testfile.txt"

dGVzdA==
--------------010108040304080808040505--
```

図 4 添付ファイルを含む電子メールの例
Fig. 4 A sample message containing an attached file.

れが単なる電子メール本文であるのか添付ファイルに関する記述であるのかを判別することができる．

そこで，本実装では次の手順で添付ファイルの種類（Content-Type）を判定し，迷惑メールの可能性があるかを判断している．

(1) ヘッダを検査し，Content-Type: multipart/mixed を含むか検査をする．含む場合は (2) の処理をし，含まない場合は添付ファイルを含まないと判断しこの処理を終了する．
(2) Content-Type: multipart/mixed の行またはその次行にある boundary の文字列を抽出する．
(3) 抽出した boundary の文字列を本文から検索し，発見した場合はその次行にある Content-Type を抽出する．
(4) (3) で抽出した Content-Type で添付ファイルの種類を判定し，安全であると判断するとさらにファイルが添付されてないかを確認するため，(3) の手順に戻る．一方，迷惑メールの可能性があると判断するとその時点で強制切断のルーチンを呼び出し，以降の行の読み込まない．

試作システムでは，Content-Type がテキストファイルを表す text/plain の場合および S/MIME の署名を表す application/x-pkcs7-signature [10] の 2 種類の場合のみ安全だと判断するようにしたが，安全だと判断するものを追加したり，指定のものだけ迷惑メールの可能性があると判断したりするよう変更することも可能である．

4.2.4 強制切断手法

本項では，本研究で実装したフィルタプログラムにおける電子メール受信の強制切断方法について述べる．

キュー投入前フィルタが電子メールの受信を拒否する場合，フィルタ前 SMTP サーバに対してネガティブな SMTP の応答を返せばよく，またフィルタ後 SMTP サーバとは SMTP のコネクションを切断すればよい．このため，前項までで述べた判定方法を用いて迷惑メールの可能性があると判断すると，ただちにこれらの処理を行えばよいことになる．

ところが，フィルタ前 SMTP サーバは本文終了の合図である「.」を受け取りフィルタプログラムに渡すまでフィルタプログラムからの応答を送信 MTA に転送することはないため，電子メール受信の早い段階で受信電子メールが迷惑メールの可能性があると判断した場合でも，強制切断を行うことができない．我々が以前に試作したシステム [8] では，強制切断を行うために FreeBSD の divert 機能 [18] を用いて送信 MTA，受信 MTA 間のパケットを監視し，DATA コマンド後に送信 MTA から送られた空白行を受信した時点で送信 MTA，受信 MTA の両方に RST パケットを送出することで強制切断を行っていた．ところが，本論文で試作したシステムでは送信 MTA とは直接通信を行っていないキュー投入前フィルタが強制切断の有無や時期を判断するため，同じ方法は採用できない．そこで，本実装では受信 MTA のフィルタ前 SMTP サーバのプロセスを強制終了する方法で送信 MTA とフィルタ前 SMTP サーバとのコネクションを切断し，強制的に電子メールの受信を中止することとした．

キュー投入前フィルタがフィルタ前 SMTP サーバを強制終了するには，フィルタ前 SMTP サーバのプロセス IP を特定する必要がある．しかし，フィルタ前 SMTP サーバとキュー投入前フィルタは双方のプロセス間に親子関係はないため，キュー投入前フィルタがフィルタ前 SMTP サーバのプロセス IP を直接取得することは困難である．そこでキュー投入前フィルタがその通信相手であるフィルタ前 SMTP サーバのプロセス ID を特定するため lsof コマンド [19] を用いた．lsof コマンドとは Unix プロセスがオープンしているファイルの情報を表示できる Unix のコマンドである．lsof コマンドを用いれば，オープンしているファイルにアクセスしているプロセスのコマンド名やプロセス ID，使用中の利用者名などを表示でき，TCP 通信のコネクションが確立していればその両端の IP アドレスやポート番号も表示することが可能である．

lsof コマンドを用いた電子メール受信の強制切断手順を以下に述べる．

(1) Perl の getpeername() および sockaddr_in() を用いてフィルタ前 SMTP サーバのポート番号を抽出する．
(2) 抽出したポート番号を引数として lsof コマンドを実行し，フィルタ前 SMTP サーバのプロセス ID を取得する．
(3) (2) で取得したプロセス ID に対してシグナル SIGTERM を送出し，フィルタ前 SMTP サーバのプロセスを強制終了する．これにより，送信 MTA とのコネクションが切断される．

© 2015 Information Processing Society of Japan

```
#IPaddress          rules
aaa.bbb.ccc.ddd     afs
eee.fff.ggg.hhh     a
```

図 5 迷惑メール判定用設定ファイルの記述例
Fig. 5 A sample configuration file for spam discrimination.

表 1 設定ファイルの判定の記述の意味
Table 1 Description for spam discrimination configuration setting.

記述	適用する判定
a	添付ファイルの種類による判定
f	エンベロープ From アドレスとヘッダ From アドレスを用いた判定
s	SPF を用いた判定

上記の手順を受信メールが迷惑メールの可能性があると判断後ただちに行うことで，受信中に強制切断を行うことが可能である．直接 25 番ポートでコネクションを確立しているプロセスを参照せず (1) の手順を行う理由として，フィルタ前 SMTP サーバが複数の電子メールを受信している場合，SMTP サーバは複数の受信プロセスを起動しているので，フィルタプログラムが検査している電子メールを受信している SMTP サーバのプロセスを特定するためである．

4.2.5 判定適用対象の設定

試作システムでは，3 つの判定を用いて優先受信 MTA で受信した電子メールが迷惑メールの可能性があるかどうかを判断するよう実装したが，信頼できる MTA の中でも送信 MTA に応じて適用したい判定が異なることが想定される．そこで，設定ファイルとして送信 MTA の IP アドレスとどの判定を適用するかを記述する設定ファイルを用意し，設定ファイルの記述どおりの判定しか適用されないよう実装した．

設定ファイルでは，**図 5** のように，送信 MTA の IP アドレスとその送信 MTA に適用する判定方法を記述する．適用する判定方法は，試作システムでは 3 つであったため **表 1** に示すとおりである．これを用いると，たとえば，図 5 の場合，aaa.bbb.ccc.ddd という IP アドレスを持つ MTA から送信されてきた電子メールに関しては，添付ファイルの種類による判定，エンベロープ From アドレスとヘッダ From アドレスを用いた判定，SPF を用いた判定の 3 つを適用することを意味するのに対し，eee.fff.ggg.hhh という IP アドレスを持つ MTA から送信されてきた電子メールに関しては添付ファイルの種類による判定しか適用しないことを意味する．

この設定ファイルにおいて判定を適用する MTA を IP アドレスによって指定した理由は，試作システムが対象とする電子メール優先配送システムでは優先配送すべき MTA の IP アドレスのリストをホワイトリストとして保持しているためである．

4.3 その他の実装の提案

提案方法の実装では，試作システムでの実装方法以外にも様々な実装方法が想定される．本節ではいくつかの実装方法について説明する．

4.3.1 postfwd を用いた実装

postfwd [20] は Postfix において様々なルールによって電子メールの受信に対して拒否したり一時エラーを返したりできるソフトウェアである．

postfwd は，SMTP アクセスポリシの外部サーバへの委譲機能を用いて postfwd のサーバに受信電子メールを渡すことで実行される．postfwd を用いることによって，たとえば短時間に大量の電子メールが同一 MTA から送られるなど，通常の電子メール配送ではない可能性が高い場合や，送信 MTA から送られてきた EHLO コマンドのアドレスや宛先アドレスなどが不正な場合など，様々な場合に応じて細かい制御をすることが可能となる．

本実装ではキュー投入前フィルタでも同様の処理を行えるため，postfwd は用いなかった．

4.3.2 header_checks などを用いた実装

header_checks [21] とは Postfix に搭載されている機能で，受信電子メールに対して 1 行ごとに正規表現を用いて検査を行うものである．header_checks は MIME 関連を除く最初のメッセージヘッダを検査するもので，他に MIME 関連のメッセージヘッダのみを検査する mime_header_checks，添付されたメッセージヘッダを検査する nested_header_checks，その他すべてのコンテンツを検査する body_check がある．

これらは，Postfix が本来備えている機能であり，容易に設定することが可能であるが，正規表現での入力検査のみしか行えず，また REJECT などに指定したルールが実行されるとその時点でその電子メールの検査を中止するが，受け取った電子メールを一度 Postfix キューへ受信してから検査を行うため，本研究で実装したフィルタに比べると切断タイミングは遅れてしまうという問題がある．このため，本実装では header_checks を用いなかった．

4.3.3 Milter を用いた実装

そのほか，通常の迷惑メール対策でよく利用される Milter を用いて拒否することも可能である．たとえば，電子署名を用いて送信ドメイン認証を行う DKIM フィルタ [22], [23], [24] を利用することにより，送信 MTA が DKIM に対応していれば送信元アドレスが詐称されている場合に優先受信 MTA での受信をやめ，一般受信 MTA で検査を行うことができる．また，Milter を用いれば sendmail [25] など，Postfix 以外の MTA にも適用することが可能である．

本実装では汎用性よりも提案方法の有効性の検証を重視

© 2015 Information Processing Society of Japan

表 2 実験環境
Table 2 Experimental environment.

ホスト計算機

OS	VMware ESXi5
CPU	Intel(R) Xeon(R) E5620
メモリ	18 GB
HDD	1 TB

仮想計算機

OS	FreeBSD/amd64 8.2-RELEASE
割当 CPU	2.40 GHz 8 コア
割当メモリ	2 GB
割当 HDD	256 GB
MTA	Postfix 2.8

したため，Milter を用いなかった．

4.4 動作確認実験

試作システムで作成したフィルタプログラムをキュー投入前フィルタとして実装し，telnet を用いて電子メールを送信し動作確認実験を行った．実験環境を**表 2** に示す．

4.4.1 SPF を用いた判定

まず，送信 MTA について SPF を用いた判定を使うよう設定ファイルに記述した．その後，DNS サーバに送信 MTA に関する SPF レコードを記述し電子メールを送信した結果，電子メール送信が正常に完了し，有線受信 MTA のメールボックスに正しく配送されていることを確認した．

次に，DNS サーバから送信 MTA に関する SPF レコードを削除し，同様に電子メールを送信した．その結果，SPF の判定に基づいて切断できることを確認した．

4.4.2 エンベロープ From アドレスとヘッダ From アドレスを用いた判定

まず，エンベロープ From アドレスとヘッダ From アドレスを用いた判定を使うため設定ファイルの記述を変更した．その後，エンベロープ From アドレスとヘッダ From アドレスが一致する電子メールを送信した．その結果，正常に電子メール送信が完了し，有線受信 MTA のメールボックスに正しく配送されていることを確認した．

次に，エンベロープ From アドレスとヘッダ From アドレスが異なる電子メールを送信した．その結果，エンベロープ From アドレスとヘッダ From アドレスの判定に基づいて切断できることを確認した．

4.4.3 添付ファイルの種類による判定

まず，添付ファイルの種類による判定を使うため設定ファイルの記述を変更した．その後，テキストファイルのみを添付したものと同等の電子メールを送信した．その結果，Content-Type として text/plain しか含まないので，正常に電子メール送信が完了し，有線受信 MTA のメールボックスに正しく配送されていることを確認した．

次に，PDF ファイルのみを添付したものと同等の電子メールを送信した．その結果，Content-Type として application/pdf を含むため，添付ファイルの種類による判定に基づいて切断できることを確認した．

4.4.4 電子メール受信中における強制切断

最後に，容量の大きい電子メールの受信中に迷惑メールの可能性があると判断する場合の実験を行った．試作システムではどのくらいのデータが送信された時点でフィルタ前 SMTP サーバの受信バッファからフィルタプログラムに送られるのかも同時に確認するため，1,024 byte ずつデータを送信した．

その結果，28 回送信した時点で本文終了の合図である「.」を送信する前に切断されることが確認できた．これは Postfix のフィルタ前 SMTP サーバの受信バッファの容量が 27〜28 KB であるためであると思われる．この結果より，添付ファイルを含むような大きなサイズの電子メールに対しては十分早い段階で強制切断を行えているといえる．

上記の切断までに要する送信量は，たとえば Postfix の改変によりフィルタ前 SMTP サーバの受信バッファサイズを縮小すると削減できると思われる．これによりさらに早い段階での強制切断が可能となり，優先受信 MTA の負荷を減少させる効果が期待できる．一方，受信バッファサイズを縮小すると，特に送信 MTA，優先受信 MTA 間の帯域幅遅延積が大きい場合に通信速度が遅くなることが懸念される．適切な受信バッファサイズは送信 MTA，優先受信 MTA 間のネットワーク特性，送信 MTA が配送を試みる電子メールの到着頻度や大きさの分布，優先受信 MTA で行う検査内容など，多くの要因により影響を受けるため，その調整方法は今後の課題である．

5. むすび

本研究では，電子メール優先配送システムにおいて信頼できる MTA から送信されてきた迷惑メールに対して，電子メールの受信中に簡易な検査を行い，その結果に応じて一時エラーもしくは SMTP コネクションを強制切断することで，送信 MTA に対して再送を促し，一般受信 MTA で十分な検査を行って受信する方法を提案した．また，提案手法に基づき，できる限り早期のタイミングで強制切断するためキュー投入前フィルタを用いてフィルタプログラムを作成し，SMTP の受信プロセスを強制終了することによる強制切断方法を用いて実装した．その結果，設定どおりに正しく切断でき，電子メール優先配送システムの負荷を減少させながら，信頼できる MTA から送られた迷惑メールの疑いのない電子メールを短い遅延時間で受信できることを確認した．

今後の課題として，フィルタプログラムの様々な判定基準への拡張があげられる．また，試作システムではどの MTA から送られてきた電子メールに対しどんなルールを

© 2015 Information Processing Society of Japan

適用するかだけの簡易な設定ファイルしか作成しなかったため，より細かい設定を容易にできるよう入力インタフェースを改良していきたい．さらに，実際の電子メール優先配送システムに本システムを実装して，受信環境に合わせた設定を行ったり，受信バッファサイズなどの調整を行ったりし，実環境での提案方法の有効性を検証したい．

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] Harris, E.: The Next Step in the Spam Control War: Greylisting (online), available from ⟨http://projects.puremagic.com/greylisting/whitepaper.html⟩ (accessed 2014-09-30).
[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 2014-09-30).
[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] 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，Vol2012-IOT-16, No.37, pp.1–6 (2012).
[5] 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).
[6] 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).
[7] Klensin, J.: Simple Mail Transfer Protocol, RFC5321, IETF (2008).
[8] 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迷惑メール対策，情報処理学会論文誌，Vol.50, No.3, pp.940–949 (2009).
[9] Wong, M. and Schlitt, W.: Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1, RFC4408, IETF (2006).
[10] Dusse, S., Hoffman, P., Ramsdell, B., Lundblade, L. and Repka, L.: S/MIME Version 2 Message Specification, RFC2311, IETF (1998).
[11] 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).
[12] 北川直哉，高倉弘喜，鈴木常彦：通信挙動の特異性を利用した spam 送信ホスト検出システムの開発，電子情報通信学会論文誌，Vol.J97-D, No.5, pp.987–1000 (2014).
[13] Venema, W.: The Postfix Home Page (online), available from ⟨http://www.postfix.org/⟩ (accessed 2014-09-30).
[14] Postfix Before-Queue Content Filter (online), available from ⟨http://www.postfix.org/SMTPD_PROXY_README.html⟩ (accessed 2014-09-30).
[15] Perl.org: The Perl Programming Language (online), available from ⟨http://www.perl.org/⟩ (accessed 2014-09-30).
[16] 独立行政法人情報処理推進機構セキュリティセンター：ウイルス対策のしおり（第 10 版）（オンライン），入手先 ⟨http://www.ipa.go.jp/security/antivirus/documents/01_virus.pdf⟩ （参照 2014-09-30）．
[17] Freed, N. and Borenttein, N.: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types, RFC2046, IETF (1996).
[18] Cobbs, A.: DIVERT(4), FreeBSD Kernel Interfaces Manual (online), available from ⟨http://www.freebsd.org/cgi/man.cgi?query=divert⟩ (accessed 2014-09-30).
[19] Abell, V.: Vic Abell's Home Page (online), available from ⟨http://people.freebsd.org/~abe/⟩ (accessed 2014-09-30).
[20] Kessler, J.: postfwd - postfix firewall daemon (online), available from ⟨http://postfwd.org/⟩ (accessed 2014-09-30).
[21] Postfix manual - header_checks(5) (online), available from ⟨http://www.postfix.org/header_checks.5.html⟩ (accessed 2014-09-30).
[22] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J. and Thomas, M.: DomainKeys Identified Mail (DKIM) Signatures, RFC4871, IETF (2007).
[23] Crocker, D.: RFC 4871 DomainKeys Identified Mail (DKIM) Signatures – Update, RCF5672, IETF (2009).
[24] Crocker, D., Hansen, T. and Kucherawy, M.: DomainKeys Identified Mail (DKIM) Signatures, RFC6376, IETF (2011).
[25] Sendmail, Inc.: Open Source - Sendmail.com (online), available from ⟨http://www.sendmail.com/sm/open_source/⟩ (accessed 2014-09-30).

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．

松岡 政之 （正会員）

平成 24 年岡山大学工学部通信ネットワーク工学科卒業．平成 26 年同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．同年株式会社インフォメーション・ディベロプメントに就職．主にネットワークセキュリティ製品の販売・導入に従事．電子メールシステム，ネットワークセキュリティ等の研究に興味を持つ．

© 2015 Information Processing Society of Japan

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 年同教授．平成 26 年より東京農工大学大学院工学研究院教授．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）

1994 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，2007 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．

© 2015 Information Processing Society of Japan