大規模組織におけるPOP before SMTPに基づく管理の容易な電子メールシステム運用方法

山井成良[†] 岡山聖彦[††]
繁田展史[†††] 宮下卓也[†]

電子メールにおけるセキュリティ強化手法として，多数の下部組織を有する大規模組織では，組織宛のすべての電子メールをいったん受け取り，検査を行ったうえで組織内の他のメールサーバに中継するようなメールゲートウェイが導入されている場合が多い．ところが，この場合，正規の利用者が組織内メールサーバを用いて組織外から電子メールを発信する場合によく利用される POP before SMTP をそのまま用いることが困難であるという問題が生じる．そこで本論文では，メールゲートウェイに POP 通信を監視させることにより上記の問題を解決する運用方法を提案する．この方法では利用者端末や他のメールサーバの変更は必要なく，管理が容易であるという特徴を持つ．実験の結果，本方法のオーバヘッドは十分小さく，本方法の実用性が確認された．

An Operation Method of E-mail Systems for Large Scale Organizations Based on "POP before SMTP" with Minimal Administration

Nariyoshi Yamai,[†] Kiyohiko Okayama,[††] Nobufumi Shigeta[†††] and Takuya Miyashita[†]

In terms of security enhancement for e-mail, a large organization with many divisions often introduces a mail gateway, which receives all inbound e-mails, then examines and forwards them to other mail servers in the organization. However, in such an organization, "POP before SMTP" cannot be used for a legitimate user to send messages with an inner mail server from outside of the organization. To solve this problem, we propose an operation method that the mail gateway monitors all POP communication between a user's terminal and an inner mail server. Since this method does not require the configurations of either users' terminals or inner mail servers, it is easy for the administrators to introduce and maintain this method. Simulation experiments show that the overhead of the proposed method is small enough for practical use.

1. はじめに

電子メールはインターネットのサービスの中で最も普及しているサービスの１つであり，多くの下部組織を有する比較的規模の大きい組織では，たとえば下部組織ごとにメールサーバを設けるなど，多数のメールサーバを設置・運用しているところも多い．一方，電子メールはセキュリティの観点で最も問題の多いサービスの１つでもあり，コンピュータウィルスの感染，メールサーバのセキュリティホールを衝いた不正アクセス，第三者による不正中継などの脅威に対するセキュリティ対策が必須である．

これらの脅威への対策方法として，組織宛のすべての電子メールをいったん受け取り，組織内の他のメールサーバに中継するようなメールゲートウェイを導入する方法がよく用いられている．この方法では，メールゲートウェイにおいてコンピュータウィルスの検査・駆除，セキュリティパッチの確実な適用，第三者による不正中継の防止など，十分なセキュリティ対策を施しておくようにする．これに加えて，メールゲートウェイへの通信を除いて組織外アドレスから組織内アドレスに対する SMTP（Simple Mail Transfer Protocol）[1] による通信を遮断あるいはメールゲートウェイへ迂回させるように設定する．これにより，潜在的な脆弱性を持つ組織内のメールサーバに対する組織外からの攻撃を防止することが可能となる．

† 岡山大学総合情報基盤センター
Information Technology Center, Okayama University
†† 岡山大学工学部
Faculty of Engineering, Okayama University
††† 三菱電機コントロールソフトウェア株式会社
Mitsubishi Electric Control Software Corporation

ところで，第三者による不正中継に対する対策では，単に組織外の計算機から送られた組織外利用者宛の電子メールの中継を拒否するような単純な方法は，利用者の利便性を損なう危険性がある．たとえば，組織内メールサーバの利用者がノート型 PC などの利用者端末を用いて電子メールの読み書きを行う場合を考える．この場合，この利用者がこの端末を同一の設定で ISP（Internet Service Provider）などの組織外ネットワークに接続し，組織内メールサーバを経由して組織外利用者宛に電子メールを発信しようとすると，上記の単純な方法に基づくメールサーバはこれを不正中継と見なし，中継を拒否することになる．このため，利用者にとっては電子メール送信に関する端末設定を変更したり，組織内からの送信とは異なる手段で電子メールを送信したりする必要が生じることになり，利用者の利便性を損なうことになる．

このような問題に対する解決手法として，POP before SMTP と呼ばれる手法が知られている[2]．これは，電子メールを発信する場合には，利用者にまず POP（Post Office Protocol）[3),4)] を用いて電子メールの受信操作を行わせ，その操作にともなう利用者認証に成功した場合に限り，POP クライアントと同一の IP アドレスを持つ端末からの電子メールの中継を一時的に無条件で許可する手法で，ほとんどの利用者に対して設定変更を必要とせず簡単に利用できるなどの特徴を持つことから，ISP をはじめとする多くの組織で用いられている．

ところが，メールゲートウェイを導入している環境では，POP before SMTP の採用が困難である．すなわち，組織外から組織内への SMTP 通信が遮断される場合には組織内メールサーバを用いて電子メールの発信を行うことができない．また，組織外から組織内への SMTP 通信がメールゲートウェイに迂回される場合でも，SMTP サーバの役割を果たすのは POP サーバと異なるメールゲートウェイであるため，通常の方法では SMTP での中継可否の判断に POP サーバでの認証結果を用いることができない．代替手法として，たとえば組織内のすべてのメールサーバをメールゲートウェイに集約する手法など，いくつかの手法が考えられるが，これらの手法ではメールゲートウェイの管理者に多大な負荷がかかる点が新たな問題となる．

そこで本論文では，メールゲートウェイが導入されているような大規模組織において，POP before SMTP を実現する手法を提案する．この手法では，メールゲートウェイが POP 通信を監視することにより POP クライアントおよび POP サーバの IP アドレスならびに利用者認証の結果を取得し，これらの情報に基づきメールゲートウェイが SMTP での中継可否を判断する．これにより，利用者端末や各下部組織に設置されているメールサーバをまったく変更することなく，容易に POP before SMTP を実現することが可能となる．

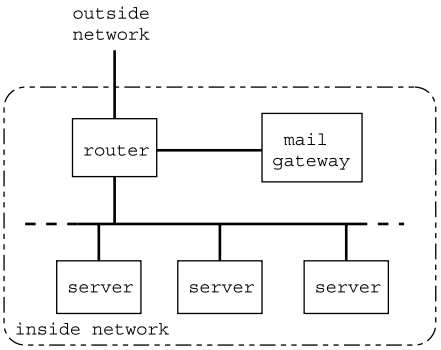


図 1 対象ネットワークの構成
Fig. 1 A target network configuration.

2. 大規模組織における電子メールの運用

2.1 対象となるネットワーク構成と運用形態

提案手法では，対象となる組織内ネットワークは，**図 1** に示すように，対外接続ルータ，メールゲートウェイ，各下部組織に設置されているメールサーバ（以下，末端メールサーバと表記する）から構成されているものとする．この図において，末端メールサーバはグローバル IP アドレスを持つものとする．また，対外接続ルータは特定の条件を満たす通信に対して通常と異なる経路制御の対象とする機能（ポリシルーティング機能）を備えており，組織外ネットワークから組織内ネットワークへのすべての SMTP 通信（宛先ポート番号が 25 番の TCP 通信）をメールゲートウェイに迂回するように設定されているものとする．したがって，組織外ネットワークからは末端メールサーバに対して直接 SMTP 通信を行うことはできないことになる．メールゲートウェイは，迂回させられた外部ネットワークからの SMTP 通信を受信すると，第三者による不正中継の有無やコンピュータウィルスの感染の有無などの検査を行った後に，あるいは検査を行いながら，末端メールサーバ上の MTA（Mail Transfer Agent）に電子メールを中継する．

提案手法を実際に適用するためには，上記のような構成が現実的なものかどうかが問題となるが，実際には上記のポリシルーティング機能は多くの市販ルータ

（レイヤ 3/4 スイッチを含む）で提供されているため，メールゲートウェイを導入している組織ではこのような構成をすでに採用している場合が多く，またそうでない組織でもこのような構成に変更することは容易であると思われる．なお，透過型ファイアウォールのなかには，図 1 における対外接続ルータの部分に設置され，メールゲートウェイと同様の役割を果たすものがあるが，提案手法ではそのようなファイアウォールを導入しているネットワークにも適用可能である．

2.2 電子メール運用における要求要件

前節で示したネットワーク構成において，メールゲートウェイや末端メールサーバの管理者ならびに利用者の負担を軽減するため，および多くのネットワーク環境で適用できるようにするためには，以下の各要件を満足することが望ましい．

(1) 末端メールサーバはメールゲートウェイとは独立して管理することができること．すなわち，メールゲートウェイの管理者は末端メールサーバに関する知識を必ずしも有する必要がなく，また末端メールサーバの管理者は必ずしもメールゲートウェイの存在に依存した特別の設定を行う必要がないこと．

(2) 末端メールサーバにアカウントを有する任意の電子メール利用者は，末端メールサーバを用いて組織内からも組織外からも同一の設定で電子メールの送受信を行うことができること．また，このとき，利用者端末上の MUA（Mail User Agent）には特別な機能を必要としないこと．

これらの要件のうち，前者は多くの電子メール運用環境で適用できるようにするため，およびメールゲートウェイや末端メールサーバの管理コストを軽減するための要件である．特に大学などの一部の組織では，末端メールサーバの管理者とメールゲートウェイの管理者が異なっていたり，たとえば文系の学部に設置されている末端メールサーバなどでは管理者は必ずしもメールサーバの運用に関する十分な知識を有しているとは限らなかったりするため，この要件を満たすことが望ましい．また，たとえば同一の管理者がメールゲートウェイと末端メールサーバの両方を管理・運用している場合でも，管理コストを軽減するためにはこの要件を満たすことが望ましい．一方，後者の要件は利用者の利便性を損なわないためのものである．すなわち，利用者がたとえばノート PC などの携帯型端末を用いて組織内，組織外のいずれから電子メールを送受信する場合でも，MUA の設定を変更したり特別な機能を持つ MUA を導入したりする必要がないことを意味する．

2.3 従来の運用方法とその問題点

前章で述べたように，図 1 の構成において正規の利用者が組織外ネットワークから組織外利用者宛に末端メールサーバを経由して電子メールを送信しようとした場合，単に SMTP を用いて送信するとメールゲートウェイがこれの通信を横取りし，第三者による不正中継と判断してこの電子メールの受信を拒否するという問題が生じる．

この問題を回避する方法として，まず組織内のすべての末端メールサーバをメールゲートウェイに集約する方法が考えられる．しかし，この方法は各末端メールサーバに登録されているアカウントをメールゲートウェイ上に移管する必要があるため，各末端メールサーバやメールゲートウェイの管理者に多大な負担を強いる点が問題となる．また，WWW に基づく電子メールシステム（たとえば文献 5)）を利用する方法，あるいは IMAP [6] など SMTP 以外のプロトコルを用いる方法も考えられるが，これらの方法はすべての末端メールサーバおよびすべての MUA がすでにこれらの方法を利用している場合のみ前節の要件を満たすことが可能であり，現実的には要件を満たすことは期待できない．

一方，SMTP を用いて電子メールの送信を行う場合，既存の末端メールサーバおよび MUA をそのまま利用する方法として，以下のような方法がある．

(1) SSH（secure shell）[7] や SSL（secure socket layer）[8] などを用いて送信用の SMTP コネクションをトンネリングする方法．

(2) delegate [9] などの POP プロクシをメールゲートウェイ上で動作させ，メールゲートウェイ自身が利用者認証を行う方法．

(3) 各末端メールサーバに発信用と受信用に個別の IP アドレスを割り当てる方法[10]．

(4) 末端メールサーバに SMTP-AUTH [11] 機能を導入する方法．

(5) 利用者端末上に MTA を導入する方法．

このうち，方法 (1) はすべての通信を暗号化できる面で組織外からのアクセス方法としては望ましいものである．しかし，この方法では末端メールサーバおよび利用者端末にトンネリング用プログラムを導入したうえでさらに利用者端末側で MUA の設定を変更する必要が生じるため，必ずしもトンネリングについて熟知しているとは限らない一般利用者に大きな負担を強いる点が問題となる．

また，方法 (2) では新たなソフトウェアを末端メー

ルサーバや利用者端末に導入する必要はないが，MUAにおいてPOPサーバをメールゲートウェイに設定し，さらにアクセスに用いる利用者名として「利用者名@末端メールサーバ名」のように末端メールサーバ名を含む形式に変更する必要がある点が問題となる．また，POPプロクシを用いると利用者端末・POPプロクシ間ではAPOP[3]を用いることができない．これは，APOPでは通信開始直後にサーバから送られる情報に基づいて認証が行われるにもかかわらず，通信開始直後はPOPプロクシは中継先が判断できず，この情報がクライアントに伝わらないためである．したがって，POPプロクシを用いると平文のパスワードを用いざるをえず，パスワードが漏洩する危険性も生じる．

方法(3)は各末端メールサーバに2つのIPアドレスを割り当て，そのうち1つはDNSのMXレコードとして登録して受信用に用い，もう1つはMXレコードとしては登録せずに送信用に用いる方法である．この際，対外接続ルータでは各送信用IPアドレス宛のSMTP通信は迂回させないように設定する．この状態で各末端メールサーバでPOP before SMTPを採用すれば，MUAの設定は同一のままで組織内からも組織外からも電子メールを発信することができる．しかし，この方法では，ポートスキャンなどにより送信用IPアドレスが発見され，このアドレス宛に直接SMTP通信を行われると，末端メールサーバが外部から攻撃されたり，メールゲートウェイで行われるべきコンピュータウィルスの検査などの処理が行われなくなったりする危険性が生じるため，各末端メールサーバで十分なセキュリティ対策を施す必要がある．また，対外接続ルータの設定のために，メールゲートウェイの管理者と各末端メールサーバの管理者が協調して作業する必要がある．したがって，この方法では特に末端メールサーバの管理者の負担が増大し，また前節の要件(1)を満たさない．

方法(4)は，末端メールサーバにおいてSMTP-AUTH機能を導入し，さらに受信用の25番とは異なるTCPポート（たとえば587番ポート[12]）を用いてMUAからの送信を待ち受け，受信した電子メールは宛先にかかわらず中継する方法である．この方法では，組織外のMTAは末端メールサーバと直接通信を行えるが，認証に成功しないと電子メールを送信できないため，第三者による不正中継を防止することができる．しかし，この方法が有効なのは末端メールサーバとMUAの双方がSMTP-AUTH機能に対応している場合に限られるため，特にすべてのMUAがSMTP-AUTH機能に対応しているとはいえない現状では前節の要件(2)を満たさない．

方法(5)は，利用者端末に発信専用のMTAを導入し，組織内の末端メールサーバを経由せずに電子メールを発信する方法である．この方法では組織内外にかかわらず同一の設定で電子メールを発信することが可能であるが，必ずしも組織内のすべての利用者がMTAを導入・設定するために必要な知識を有しているとは限らず，またMTAの導入・設定には一般にかなりの負担を利用者に強いるため，前節の要件(2)を満たさない．さらに，最近ではspamメール対策としてDNSによるホスト名の逆引きができないIPアドレスや，逆引きで得られたホスト名から動的に割り当てられたものと判断できるIPアドレスからは受信を拒否する手法[13),14)]を採用しているドメインも少なからず存在するため，利用者端末を接続するネットワーク環境と発信する電子メールの宛先によっては，配送に支障をきたす危険性もある．

以上のように，従来の電子メールの運用方法はいずれも前節の要件を満たさず，管理者や利用者に負担を強いる，あるいは適用可能な電子メール運用環境が限られるという点で問題があるといえる．

3. 大規模組織に適した電子メール運用方法

3.1 提案方法の概要

大規模組織における電子メールの運用において前章で述べたような問題が生じる最も大きな原因は，SMTPを用いて電子メールの送信を行う際にメールゲートウェイにおいてその通信が正規の利用者によるものであるかどうかの判断が行えない点である．ここで，MUAの設定を変更せずに利用できる要件を考慮すると，現状ではPOP before SMTPを基にした方法しか考えられない．そこで，以下ではメールゲートウェイにおけるPOP before SMTPの実現方法について議論する．

前章で述べたとおり，図1の構成ではメールゲートウェイでPOP before SMTPをそのまま用いることはできない．その原因は，メールゲートウェイが組織外にいる利用者と末端メールサーバとの間のPOP通信における認証結果を知ることができず，第三者による不正中継と区別できないためである．したがって，何らかの方法でメールゲートウェイがPOP通信における認証結果を取得できれば，それに応じて電子メールの中継の可否を制御し，POP before SMTPを実現することができる．

そこで本論文では，対外接続ルータによってSMTP通信だけでなくPOP通信もメールゲートウェイに迂回させ，メールゲートウェイ上でPOP通信内容を監

視することによって POP 通信における認証結果を取得する方法を提案する．これにより，メールゲートウェイは認証結果に基づいて電子メールの中継の可否を決定できる．また，本方法はメールゲートウェイにおいて POP 通信の内容を監視するだけで，IP アドレスやポート番号を含めて通信内容をいっさい変更しないため，2.3 節の方法 (2) とは異なり，末端メールサーバや利用者端末に変更をいっさい加えることなく APOP を含めたすべての機能を利用可能である．さらに，組織内の末端メールサーバが追加された場合や組織内のドメイン構造が変化した場合でも何ら変更を加える必要はない．以上のことから，提案方法は 2.2 節の要件をすべて満たし，大規模組織においても低コストで管理が容易な方法であるといえる．

3.2 メールゲートウェイでの処理

本節では，図 1 に示す構成において POP before SMTP 機能を実現するためにメールゲートウェイで行われる処理について述べる．

前節で述べたように，メールゲートウェイでは組織外の利用者端末と組織内の末端メールサーバとの間の POP 通信をすべて監視する必要がある．そのため，対外接続ルータでは組織外ネットワークから組織内ネットワークの POP 用ポート（TCP 110 番）宛への通信および組織内ネットワークの POP 用ポートから組織外ネットワークへの通信の両方をメールゲートウェイに迂回するように設定する．メールゲートウェイは迂回された通信を監視し，そのうち利用者認証に関するコマンドである PASS コマンドおよび APOP コマンドについて末端メールサーバから返される応答を確認する．すなわち，これらのコマンドに対する応答として末端メールサーバが「+OK」を返せば認証に成功したと見なして利用者端末と末端メールサーバの IP アドレスの組を一定時間記録し，「-ERR」を返せば認証に失敗したと見なして何も記録しない．これにより，メールゲートウェイではどの利用者端末とどの末端メールサーバとの間で認証が成功したかを確実に把握できるようになる．

なお，本方法では，メールゲートウェイで POP 通信を監視できるような構成であれば，対外接続ルータでの POP 通信の迂回は必ずしも必要ではない．したがって，たとえば対外接続ルータがミラーリングポートを持ち，このポートを用いてメールゲートウェイが POP 通信を監視するような構成でもよいし，また対外接続ルータの部分に透過型ファイアウォールが設置されている構成ではファイアウォール自身が POP 通信を監視してもよい．

一方，組織外ネットワークからの SMTP 通信については，従来の場合と同様にメールゲートウェイ自身が処理を行う．その際，POP before SMTP 機能を実現するために，メールゲートウェイは送信元の IP アドレスと本来の通信先である末端メールサーバの IP アドレスの両方を確認する．その結果，両者の組が POP 通信監視により記録されたものであれば，送信元 IP アドレスの使用者は直前に認証に成功したものと見なして宛先にかかわらず電子メール中継を認める．そうでなければ認証に成功していないものと見なして組織内利用者宛のメール中継のみを認め，組織外利用者宛のメール中継は第三者による不正中継として扱い許可しないようにする．

提案方法では，送信元 IP アドレスだけを確認する従来の POP before SMTP とは異なり，末端メールサーバの IP アドレスも確認する．これは，たとえば NAT 環境や DHCP 環境など認証に成功した端末と同一の IP アドレスが短時間のうちに他の利用者の端末からも利用される環境を考慮すると，送信元 IP アドレスだけの確認では，同一の IP アドレスを持つ他の端末から組織内の任意の IP アドレスを SMTP サーバとして指定して電子メールを送信するだけで不正中継が可能となり，不正中継される可能性が大幅に増加するためである．なお，このような環境では，提案方法においても，正しい末端メールサーバの IP アドレスが他の利用者に知られると不正中継を許す危険性がある．しかし，これは提案方法の欠点というよりむしろ POP before SMTP 自身の持つ欠点であり，また利用者認証後に無条件中継を許可する時間を短縮することによりこの危険性を十分小さくすることが可能であるため，本論文ではこれ以上議論しない．

3.3 全体の処理手順

全体の処理手順として，前節までに述べた内容をまとめたものを以下に示す．また，POP 通信時および SMTP 通信時の動作をそれぞれ **図 2**，**図 3** に示す．

(1) 準備として，対外接続ルータにおいて，POP 通信および SMTP 通信をメールゲートウェイに迂回するように設定しておく．

(2) 利用者は組織外の利用者端末から末端メールサーバとの間で POP 通信を開始する．この通信は対外接続ルータで迂回させられ，メールゲートウェイで監視されるが，通信内容はまったく変更されずに送信先に中継される．

(3) 認証を受けるため，利用者端末は USER コマンドに続けて PASS コマンドを，あるいは単独で APOP コマンドを末端メールサーバに送信

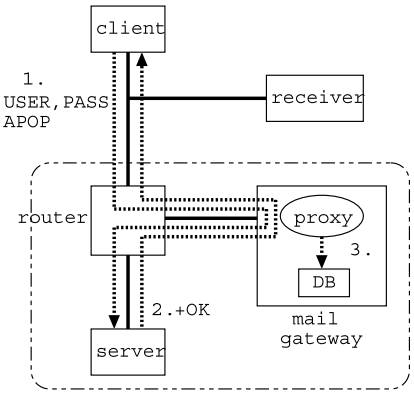


図 2 POP 通信時の処理手順
Fig. 2 Process of the proposed method on POP communication.

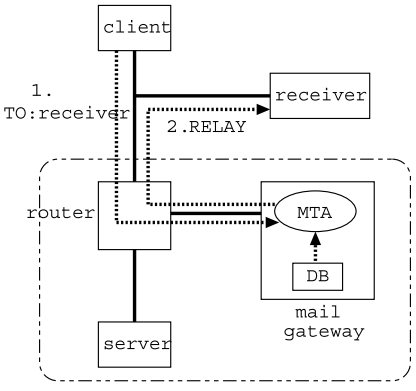


図 3 SMTP 通信時の処理手順
Fig. 3 Process of the proposed method on SMTP communication.

する（図 2 の 1.）.

(4) 末端メールサーバは PASS コマンドあるいは APOP コマンドの結果を利用者端末に返す（図 2 の 2.）.

(5) 上記 (3)，(4) の通信をメールゲートウェイは監視し，その結果が「+OK」あれば利用者認証に成功したと見なして利用者端末と末端メールサーバのそれぞれの IP アドレスの組を一定時間データベース（DB）に記録する（図 2 の 3.）.

(6) 引き続いて利用者は組織外の利用者端末から末端メールサーバとの間で SMTP 通信を開始する．この通信は対外接続ルータで迂回させられ，メールゲートウェイ上の MTA で受信される（図 3 の 1.）.

(7) メールゲートウェイ上の MTA は，利用者端末と本来の通信先である末端メールサーバの IP アドレスの組がデータベース（DB）に記録されているかどうかを確認する．もし記録されていれば，利用者端末からの電子メールを宛先にかかわらず受信し，コンピュータウィルスの検査など所定の処理を行った後に宛先に電子メールを配送する（図 3 の 2.）．そうでなければ，組織内宛の電子メールのみを受信し，所定の処理後に末端メールサーバに配送する．

(8) (5) で記録された情報は，通常の POP before SMTP と同様に一定時間経過後に削除する．

3.4 提案方法の適用に関する考察

提案方法は多くのネットワーク環境ではそのまま適用可能であるが，ネットワーク環境によっては多少の対策が必要な場合がある．本節では，そのままでは提案方法が適用できないネットワーク環境とその対策について考察する．

3.4.1 暗号化 POP 通信の導入

SSL や SSH などを用いて POP 通信を暗号化している末端メールサーバが存在する環境では，メールゲートウェイが POP 通信における認証結果を取得できないため，提案方法をそのまま利用することができない．しかし，このような環境では，POP 通信を暗号化している末端メールサーバにおいて，2.3 節の方法 (1) あるいは (4) を併用することにより，組織外からの電子メール発信を可能にすることができる．この場合，当該末端メールサーバとその利用者の MUA は設定変更が必要であるが，そのための負担は暗号化 POP 通信の導入と同程度であり，すでに暗号化 POP 通信を導入している環境では比較的容易に導入可能であると思われる．なお，我々が調査した範囲では，暗号化 POP 通信に対応している MUA はすべて方法 (1)，(4) の少なくとも一方に対応しており，MUA 自身の変更については特に考慮する必要はないと思われる．

3.4.2 プライベートアドレスの利用

2.1 節で述べたように，提案方法では末端メールサーバはグローバル IP アドレスを持つことを前提としており，プライベート IP アドレスを持っている場合には提案方法をそのまま適用することができない．しかし，このような場合でも 3.3 節の手順 (1)，(2) を以下のように置き換えれば，提案方法を適用することが可能である．

(1)’ 準備として，組織内の末端メールサーバと 1 対 1 に対応するグローバル IP アドレスをメールゲートウェイに重複して割り当て，組織外から末端メールサーバの A レコードに関する問合せがあれば DNS サーバがその末端メールサー

バに対応する IP アドレスを応答するように設定する．

(2)’ 利用者は組織外の利用者端末から上記 (1)’ で返された IP アドレスに対して POP 通信を開始する．メールゲートウェイはこの通信を監視しながら，本来の通信先である末端メールサーバに中継する．

なお，この対策方法は MUA で POP サーバ，SMTP サーバとして末端メールサーバの FQDN（Fully Qualified Domain Name）が DNS で参照されるように設定されている場合のみ有効で，たとえばプライベート IP アドレスが指定されている場合には，この方法でも対応できない．

3.4.3 組織外 MTA の IP アドレスの参照

提案方法では，組織外からのすべての SMTP 通信はいったんメールゲートウェイが受け取るため，末端メールサーバは組織外 MTA の代わりにメールゲートウェイとの間で SMTP 通信を行うことになる．このため，提案方法をそのまま適用しただけでは末端メールサーバが組織外 MTA の IP アドレスを参照して受信拒否や spam メール対策などを行うことができない．これは提案方法の問題というよりはむしろメールゲートウェイの導入に関する問題であり，またメールゲートウェイが末端メールサーバとの間で SMTP 通信を行う場合に，アドレス変換などにより自身のアドレスの代わりに発信元である組織外 MTA の IP アドレスを用いることにより解決することが可能である．

4. 提案方法の実装と性能評価

4.1 試作システムの実装

提案方法の有効性を検証するため，我々は前章で述べた POP before SMTP 機能をメールゲートウェイに実装し，**図 4** に示すような構成のシステムを試作した．図中で A〜H はそれぞれ IP アドレスを表し，このうち A〜C は組織外のアドレス，D，E はバリアセグメントのアドレス，F〜H は組織内のアドレスをそれぞれ表す．

この図において 2 台の利用者用端末，2 台の末端メールサーバ，およびメールゲートウェイはいずれも FreeBSD 4.5-RELEASE 搭載機であり，対外接続ルータに 100 Mbps で接続した．

対外接続ルータにはレイヤ 3 スイッチである Cisco Systems 社製 Catalyst 3550 を用い，ポリシールーティング機能を利用して組織外ネットワークと組織内ネットワークとの間で行われる POP 通信および SMTP 通信をメールゲートウェイに中継するように設定した．

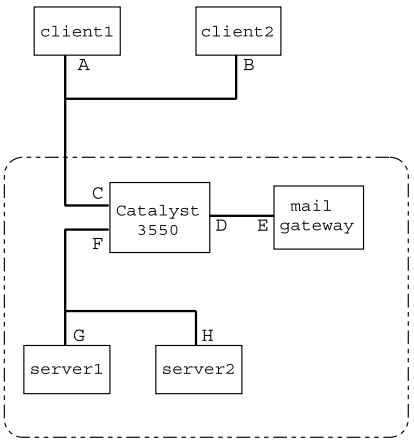


図 4 試作システムの構成
Fig. 4 The configuration of the prototype system.

具体的には，(発信元アドレス：ポート番号，宛先アドレス：ポート番号）の 4 つ組が，C 側のインタフェースで受信したパケットについては（組織外アドレス：任意，組織内アドレス：25）および（組織外アドレス：任意，組織内アドレス：110）である TCP パケットを，また F 側のインタフェースで受信したパケットについては（組織内アドレス：110，組織外アドレス：任意）である TCP パケットをそれぞれ強制的に D 側のインタフェースに出力するようにした．なお，コンピュータウィルスの検出，駆除などを行うために組織内アドレスから組織外アドレスへの SMTP 通信もメールゲートウェイで処理したい場合には，F 側のインタフェースで受信したパケットについて上記に加えて（組織内：25，組織外：任意）の TCP パケットも E 側インタフェースに強制的に出力するように設定すればよいが，試作システムではそのような設定は行わなかった．一方，D 側のインタフェースで受信したパケットはポリシールーティング機能を用いずに通常の経路制御に基づいて中継されるようにした．

メールゲートウェイでは，前章で述べた POP 通信監視機能と POP before SMTP 機能を実装した．このうち，前者については FreeBSD における標準コマンド ipfw（IP firewall）[15] の divert 機能[16] を用いてすべての POP 通信を監視プログラムがいったん受け取り，内容を確認したうえでそのまま再送出するようにした．これにより，利用者端末・末端メールサーバ間の POP 通信を見落とすことなく確実に監視することが可能となる．一方，後者については，任意の末端メールサーバ宛の通信をメールゲートウェイ上の MTA で受信して処理する必要があり，また利用者端末および末端メールサーバの両方の IP アドレスを確認して中継

の可否を決定する必要があることから，通常の MTA では対処することができない．そこで，試作システムでは 2 つの MTA と ipfw の fwd 機能を用いて POP before SMTP 機能を実装した．すなわち，**図 5** に示すように，メールゲートウェイにおいて無条件に中継を許すような MTA（MTA1）と第三者による不正中継を許さないような MTA（MTA2）を異なるポート番号（図では 10025 番と 25 番）で受信するように待機させておき，メールゲートウェイが SMTP 通信を受信すると，送信元アドレスと送信先アドレスとの間で POP 認証に成功している場合には MTA1 に，それ以外の場合には MTA2 に転送するように ipfw の fwd 機能を設定するようにした．なお，この場合，組織外ネットワークから MTA1 への直接アクセスを防止するためのフィルタリング設定が必要であることに注意する．

また，これにともない，認証に成功した利用者端末および末端メールサーバの IP アドレスの組は，実装の簡素化のため ipfw のルールとして管理することにした．すなわち，ipfw では番号をつけてルールを管理するため，無条件中継を許可する期間の長さに応じた番号の範囲を予約しておき，POP 通信監視機能で認証の成功を検出した場合には，認証時刻に対応する番号をつけたルールとしてこれらの IP アドレスの組を登録するようにし，また登録後に一定時間が経過すると，認証時刻に対応する番号がつけられたルールをすべて削除するようにした．具体的には，試作システムでは中継許可時間を最大 10 分間に設定したため，ルール番号 1000〜1009 を予約し，1 分ごとに（分の値の下 1 桁+1000）の番号を持つルールをすべて削除して，その後の 1 分間では認証に成功した IP アドレスの組を同じ番号で登録するようにした．したがって，同一の利用者端末・末端メールサーバ間で短時間に複数回の認証があった場合にはこれらの IP アドレスが複数のルールとして登録されるが，その場合でも登録されたルールのすべてが削除されるのは最後に認証に成功してから中継許可時間が経過した後であるため，正常に動作する．

なお，この方法では，同一の利用者端末・末端メールサーバ間で短時間に複数回の認証があった場合，これらの IP アドレスが複数のルールとして登録されるため ipfw のオーバヘッド増加が問題となりうるが，この問題についてはたとえば divert 機能を用いて SMTP 通信をすべて振り分け用プログラムが受け取り，このプログラムが送信元・送信先 IP アドレスに基づきいずれか適切な MTA に転送する方法により解決することが可能である．

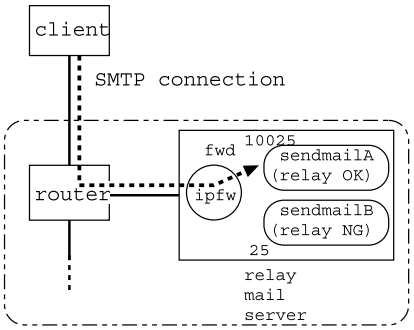


図 5 メールゲートウェイにおける SMTP 通信の処理
Fig. 5 Process of SMTP communication on the mail gateway.

4.2 動作確認と性能評価

試作システムの有効性を検証するため，最初に 図 4 の環境において動作確認を行った．まず，client1 と server1 との間で POP 認証を行い，client1 および client2 からそれぞれ server1，server2 の両方を SMTP サーバとして組織外のアドレス宛に電子メールの送信を試みたところ，client1 と server1 との組合せのみ正しく配送され，他の組合せでは不正中継として配送が拒否された．次に，認証に成功してから 15 分経過後に再び同様の実験を行ったところ，今度はすべての組合せで不正中継として配送が拒否された．以上の結果から，試作システムの POP before SMTP 機能は正しく動作していることが確認できた．

次に，試作システムの性能評価について述べる．提案方法では組織外の利用者端末と組織内の末端メールサーバとの間のすべての POP 通信がゲートウェイを経由するため，提案方法を用いない場合と比較すると応答速度や通信速度の低下が懸念される．そこで，提案方法を用いた場合と用いない場合について，POP 認証に要する時間および POP によるメッセージ取得時間をそれぞれ 100 回計測し，その平均値，最大値，最小値を求めた．ここで，POP 認証に要する時間は client1 が server1 にコネクションの確立を試みてから USER コマンド，PASS コマンド，QUIT コマンドを順に実行してコネクションが切断されるまでの時間を指し，またメッセージ取得時間は server1 に約 1 MB のメールが 1 通格納されている状態において，認証終了後に RETR コマンドを発行してから完了するまでの時間を指す．これらの時間はいずれも expect [17] を用いて計測したものである．

計測結果を **表 1** に示す．この結果から以下のことがいえる．まず，POP 認証に要する時間は 56 ms か

表 1 性能評価の結果
Table 1 Result of performance evaluation experiments.

proposed method	auth. time (ms)			retrieval time (ms)		
	ave	min	max	ave	min	max
active	61	59	69	621	619	629
inactive	56	54	92	618	617	628

ら 61 ms へと約 1 割増加しているが，その増加量 5 ms は POP 通信での一般的なセッション時間と比較すると十分小さく，実用上無視できると思われる．また，電子メール伝送時間も平均値が 618 ms から 621 ms と 3 ms の増加にとどまっており，提案方法のオーバヘッドは実用上無視できる程度に小さいといえる．

5. ま と め

本論文ではメールゲートウェイを導入しているような大規模組織において，メールゲートウェイで POP 通信を監視することにより POP before SMTP を実現する方法を提案した．これにより利用者端末や末端メールサーバの設定変更をまったく必要とせず低い管理コストで第三者による電子メールの不正中継を防止することが可能となった．また，提案方法を実装したシステムで性能評価を行った結果，オーバヘッドが実用上無視できる程度に小さいことが確認された．

今後の課題としては，実際の運用を通じて多数の利用者が同時に利用した場合の性能評価を行うことや，POP で認証した利用者名をもとに発信者アドレスの確認を行い，第三者による不正中継をより確実に防止することなどがあげられる．

謝辞 本研究の一部は平成 15〜16 年度科学研究費補助金（基盤研究（C）(2)，課題番号 15500039）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) Klensin, J.E.: Simple Mail Transfer Protocol, RFC2821, IETF (2001).
2) Harkins, N. and Levine, J.: POP before SMTP for Sendmail (2000). http://spam.abuse.net/adminhelp/smPbS.shtml
3) Myers, J. and Rose, M.: Post Office Protocol, Version 3, RFC1939, IETF (1996).
4) Gellens, R., Newman, C. and Lundblade, L.: POP3 Extension Mechanism, RFC2449, IETF (1998).
5) 渡辺健次，竹田暁彦，只木進一：IMAP に対応した Web ベースメールクライアント WebMailer の開発，学術情報処理研究，No.4, pp.35–43 (2000).
6) Crispin, M.: INTERNET MESSAGE ACCESS PROTOCOL, VERSION 4rev1, RFC2060, IETF (1996).
7) Barrett, D.J. and Silverman, R.: *SSH, The Secure Shell: The Definitive Guide*, O'Reilly (2001).
8) Viega, J., Messier, M. and Chandra, P.: *Network Security with OpenSSL*, O'Reilly (2002).
9) 佐藤 豊：*Delegate Home Page*. http://www.delegate.org/
10) 山井成良，宮下卓也，大隅淑弘，林 伸彦：岡山大学における電子メールシステムのセキュリティ対策，情報処理学会分散システム/インターネット運用技術研究会研究報告，No.2002-DSM-26, pp.61–66 (2002).
11) Myers, J.: SMTP Service Extension for Authentication, RFC2554, IETF (1999).
12) Gellens, R. and Klensin, J.: Message Submission, RFC2476, IETF (1997).
13) 前野年紀：非通知拒否方式 (2004). http://spam.qmail.jp/ptr.html
14) 広瀬雄二，大駒誠一：spam 対策に特化した SMTP wrapper の実装と検証，情報処理学会分散システム/インターネット運用技術研究会研究報告，No.2004-DSM-35, pp.25–30 (2004).
15) Antsilevich, U.J.S., Kamp, P.-H., Nash, A., Cobbs, A. and Rizzo, L.: ipfw — IP firewall and traffic shaper control program. http://www.freebsd.org/cgi/man.cgi?query=ipfw
16) Cobbs, A.: divert — kernel packet diversion mechanism. http://www.freebsd.org/cgi/man.cgi?query=divert
17) Libes, D.: *Exploring Expect*, O'Reilly (1994).

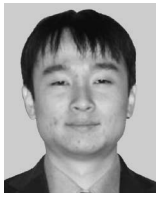
(平成 16 年 7 月 5 日受付)
(平成 17 年 2 月 1 日採録)

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助教授を経て，現在岡山大学総合情報基盤センター助教授．分散システム，マルチメディアシステム，マルチメディアネットワークの研究に従事．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．平成 6 年奈良先端科学技術大学院大学情報科学研究科助手．平成 10 年岡山大学工学部助手．インター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．



繁田　展史

平成 14 年岡山大学工学部情報工学科卒業．平成 16 年同大学大学院自然科学研究科博士前期課程修了．同年三菱電機コントロールソフトウェア株式会社入社．広域分散システム，高速ネットワーク等に興味を持つ．

宮下　卓也

平成 3 年岡山大学工学部電気電子工学科卒業．平成 5 年同大学大学院工学研究科（電気電子工学専攻）修了．平成 8 年同大学院自然科学研究科（知能開発科学専攻）修了．平成 9 年東京農工大学ベンチャービジネスラボラトリー博士研究員．平成 10 年岡山大学総合情報処理センター助手．平成 16 年岡山大学総合情報基盤センター助手．主にディジタル機器からの放射電磁雑音の計算機シミュレーションの研究に従事．情報処理教育，マルチメディア，高速ネットワーク等に興味を持つ．博士（工学）．IEEE，電子情報通信学会，エレクトロニクス実装学会各会員．