メールクライアントに修正を要しない発信者詐称防止方式

石橋勇人[†] 山井成良[††] 安倍広多[†]
大西克実[†] 松浦敏雄[†]

現在では，インターネットは通信におけるインフラストラクチャとして広く社会に認知されており，多くの人々に利用されている．インターネット上のアプリケーションの中で，最も重要なものの１つが電子メールである．しかし，これまでの電子メール配送システムにはメールの発信者を確認する手段がなく，悪意のある発信者であれば簡単に身元を偽ることができるという技術的な問題があった．特に，ダイアルアップや情報コンセントなどを経由して利用者所有の計算機を接続するような場合には，電子メールに付加された発信者アドレスの正当性を確認する手段が存在しなかった．そこで，本論文では，認証サーバを導入することによって電子メールの発信者を確認する方式を提案する．本方式は，ダイアルアップ接続や認証付きの情報コンセント環境に対して適用でき，電子メールの発信者が発信者アドレスを詐称したことを検出できる．また，詐称を検出した場合にも，運用方針に応じて柔軟な対処が可能である．本方式では，電子メールの送信プロトコルには手を加えないため，既存の電子メールクライアントを修正することなく利用でき，既存環境への導入が容易である．我々は，本方式を実装して教育用電子メールサーバで運用しており，これまで１年以上にわたって動作を確認している．

A Method of Protection against Email Sender Address Spoofing without Modification of Internet Mail Clients

Hayato Ishibashi,[†] Nariyoshi Yamai,[††] Kota Abe,[†]
Katsumi Ohnishi[†] and Toshio Matsuura[†]

The Internet is well recognized as a communication infrastructure these days. Email is one of the most important applications running on the Internet. Despite of that, current Email systems don't have a method to identify a sender. It makes malicious users easily spoof their Email addresses. In this paper, we propose a method to identify each user who sends an Email message by introducing an authentication server. This method can be applied to dialup access and access via LAN sockets with authentication. It can detect a sender address spoofing, and when detected, flexible error processing can be applicable. Since the proposed method uses the SMTP protocol without any modification, existing mail clients are still available as they are. We have implemented the method and have been operating it for one year at our site.

1. はじめに

近年，インターネットの普及により，電子メールを用いた他者との通信が容易かつ迅速に行えるようになってきた．大学などの教育機関でも，すべての学生に電子メールの利用資格を与え，学内外の利用者とのコミュニケーションに自由に利用させているところが多い．一方，電子メールコミュニティの急速な拡大にともなって，SPAM メール（不特定多数の利用者に対する希望しない内容の電子メール）の送付や身元を偽っての電子メール発信など，電子メールの不正利用が問題視されるようになっている．

電子メールの不正利用に関して，SPAM メールの中継拒否など他組織からの不正利用の防止も重要であるが，特に大学などの教育機関では，それにも増して自組織の利用者（多くは学生）が不正利用を行わないようにすることが対外的な責務として重要である．そのためには，利用者に対して電子メールの正しい利用法（ネットワークエチケットなど）についての教育を徹底して行うことは必須であるが，それだけではなく，自組織の利用者による不正利用を抑制する技術的な仕組みを用意する必要がある．

このような仕組みの１つとして，メッセージの発信時に利用者認証を行い，発信者の詐称を防止すること

† 大阪市立大学学術情報総合センター
Media Center, Osaka City University
†† 岡山大学総合情報処理センター
Computer Center, Okayama University

が考えられる．これは SPAM メールの送付などの不正利用を直接防止するものではないが，不正利用が行われた場合でも発信者が特定できるため，不正利用を間接的に抑制する効果を持つ．この方式に基づく不正利用防止手法はいくつか提案されており，代表的なものとして，IDENT プロトコル[1] によって利用者認証を行う手法，SMTP（Simple Mail Transfer Protocol）[2] に認証機能を追加する手法などがある．しかし，これらの手法は利用者の計算機に特別なプログラムが必要であり，利用者が自己の所有する計算機をネットワークに接続して電子メールを利用するような環境に適用することは一般に困難である．また，従来の手法では発信者詐称が行われたメールに対する処理が限定され，たとえば，発信者アドレスを正しいものに書き換えることができない．

そこで，本研究では，認証サーバの導入によって発信者を特定する，電子メールの新しい発信者詐称防止方式を提案する．本方式では，信頼できる認証サーバ（たとえば，リモートアクセス環境における RADIUS[3] サーバ）を利用し，発信者を確認したうえで発信者アドレスとの照合を行う．本方式は，利用者の計算機には特別なプログラムを必要とせず，従来のクライアントプログラムをそのまま利用することが可能である．また，フロントエンドプログラムによって SMTP セッション中に利用者認証を行うため，処理が単純となり短時間で行うことができる．さらに，詐称された発信者アドレスを発見した場合に正しいものに書き換えるなど，運用方針に基づいた柔軟な対応が可能となる．

2. 現状と問題点

2.1 電子メールの利用環境

図 1 に示すように，本研究で想定している電子メールの利用環境では，いくつかのクライアント計算機とサーバ計算機がネットワークで接続されている．クライアント計算機には，メッセージの作成や閲覧を行うクライアントプログラム（MUA: Message User Agent）が導入されている．一方，サーバ計算機には，メッセージの配送，受信，保存を行うサーバプログラム（MTA: Message Transfer Agent）が導入されている．

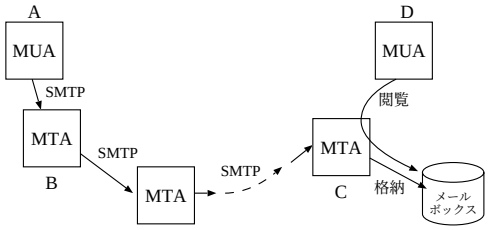

図 1 電子メールの利用環境
Fig. 1 Email environment.

クライアント計算機については，次に示すような利用環境が考えられる．

（環境 1）管理者だけが設定でき，利用開始にあたって利用者認証を要する計算機（たとえば，適切に管理された UNIX を搭載する計算機）がネットワークに接続されている環境

（環境 2）利用者が自由に設定できる計算機（たとえば，Windows 95/98 を搭載した計算機）がネットワークに常時接続されている環境

（環境 3）利用者が自由に設定できる計算機が公衆電話網などを介してネットワークに接続される環境

（環境 4）利用者が自由に設定できる計算機が情報コンセント（利用者に公開された Ethernet ポート）を介してネットワークに接続される環境

図 1 の環境において，メッセージは次のような手順で発信者から受信者に伝えられる．

(1) 電子メールを送信しようとする利用者は，クライアント計算機（A）上の MUA を用いてメッセージを作成し，送信する．

(2) 利用者から送信を指示されると，MUA はあらかじめ指定されたサーバ計算機上（B）で動作している MTA に SMTP を用いてメッセージを送る．

(3) MTA は，渡されたメッセージに書かれている宛先アドレスから次の配送先となるサーバ計算機を決定し，その計算機上で動作する MTA に SMTP を用いてメッセージを配送する．同様の操作が必要に応じて繰り返され，最終的にメッセージが宛先のサーバ計算機（C）に配送される．

(4) 宛先のサーバ計算機（C）上の MTA は，受け取ったメッセージを利用者ごとに用意されたメールボックスに保存する．

(5) 受信者は，クライアント計算機（D）上の MUA を用いてメッセージを閲覧する．

ここで，計算機 A，B，C，D の各々は必ずしも異なる計算機である必要はない．

2.2 現状における問題点

前節の手順のうち，従来から問題として指摘されているのは，(2) において計算機 A 上の MUA と計算機 B 上の MTA の間で利用者認証が行われないため，発信者の正しいアドレスを確認する手段がなく，いかなる発信者アドレスが付加された電子メールでも受け

入れざるをえないことである．このため，発信者アドレスの詐称を簡単に許してしまう．この問題に対処するため，これまでにいくつかの手法が試みられてきた．

ここで，正しいアドレスとは，利用者が電子メールを運用する機関〔大学や ISP（Internet Service Provider）など〕から与えられた正規のメールアドレスを意味している．また，発信者アドレスの詐称とは，利用者が与えられた正規のメールアドレス以外のアドレス，すなわち，他人のアドレスまたは架空のアドレスを発信者アドレスとして使用することを指すものとする．

次章では，従来の代表的な手法とその問題点を示す．

3. 従来の手法

3.1 IDENT プロトコルによる発信者情報の取得

インターネットにおける代表的な MTA の 1 つである sendmail[4] は，SMTP コネクションを張ってきたクライアントを使用している利用者の情報（利用者名）を IDENT プロトコルによって入手し，ヘッダにその情報を付加する機能を有している．したがって，クライアント計算機上で動作する IDENT サーバの情報が信頼できる環境（2.1 節の環境 1）では，この機能を利用して発信者情報を明らかとすることによって詐称の抑止効果とすることが可能である．

しかし，IDENT サーバは必ずしもクライアント計算機に導入されているわけではない．また，たとえ導入されていたとしても，2.1 節の環境 2〜4 では，その管理は利用者自身によって行われるため，IDENT プロトコルで得られる利用者情報は信頼できない．したがって，この情報を利用して発信者詐称を抑制することは困難である．

3.2 sendmail のアクセス制限機能の利用

sendmail には，SMTP セッション中にエンベロープ情報☆やクライアントの IP アドレスを用いて配送制限を行う機能が備えられている．この機能により，発信者アドレスのドメイン名部分を偽ったメッセージの配送を拒否することが可能である．

しかし，sendmail は発信者を特定できないため，正しいドメイン名を使用して発信名だけを偽ったアドレスを用いた場合には，電子メールの配送を拒否したり発信者アドレスを正しいものに書き換えたりすることはできない．

3.3 POP3 拡張機能による送信

2.1 節で述べたように，メッセージを読む場合にはクライアント計算機上で MUA を実行してメールボックスにアクセスする．この際に利用される代表的なプロトコルとして POP3 がある．POP3 は本来はメッセージ閲覧用のプロトコルであるが，メッセージの発信が可能な拡張コマンド[5] を持つ POP3 サーバ[6] も存在する．この拡張コマンドを用いる場合，POP3 セッションを開始するにあたって利用者認証が必要となるため，POP3 サーバに登録されていない利用者によるメッセージの発信を防止することが可能である．

しかし，現在の実装では，MTA に渡すメッセージ中の発信者アドレスと認証した利用者の照合は行われていない．したがって，正規利用者であればいかなるヘッダも付加することができる．また，たとえ照合を行うように改良したとしても，POP3 の拡張機能を用いてメッセージを発信できる MUA は少なく，ほとんどの MUA は SMTP による送信を行うので，2.1 節の環境 2〜4 のように利用者が使用する MUA を限定できない環境では，この手法は事実上利用できない．

3.4 SMTP の拡張機能による認証

最近，SMTP にクライアント計算機や発信者を認証する機能が追加された[7]．この機能を用いることによって，SMTP による電子メールの送信時に利用者認証を行うことができ，発信者アドレスの詐称を防止することが可能となる．

しかし，この機能に対応している MUA は少ないため，POP3 拡張機能による送信と同様に，前節の環境 2〜4 のように利用者が利用する MUA が限定できない環境では，事実上この手法は利用できない．

3.5 メール発信時における POP による認証の利用

クライアント計算機に特別なソフトウェアを必要としない手法として，POP プロトコルと sendmail を組み合わせる手法が提案されている[8]．この手法では，利用者がクライアント計算機から POP プロトコルによって認証を行った際に POP サーバがクライアント計算機の IP アドレスを記録しておき（この記録は一定期間後に消去される），sendmail は記録された IP アドレスを持つクライアント計算機からのメッセージのみを他者に配送する．これによって，正規利用者以外による電子メールの発信を防止することが可能である．

しかし，この手法では，発信者アドレスと POP サーバで認証した利用者とは特に照合されない．また，たとえこの照合を行うように改良したとしても，電子メールの発信を許可している期間中に同じ IP アドレスを割り当てられた別のクライアント計算機から同じ発信者アドレスを用いてメッセージが発信された場合，そのメッセージの配送を拒否できない．この問題は特

☆ メール転送のために用いられる発信者や受信者の情報．

に 2.1 節の環境 3，4 のように同一の IP アドレスが再利用される場合には無視できない．また，利用者にまず受信を行ってから送信を行う手順を強制する点で使い勝手が悪く，この手順を自動化するためには MUA の変更をともなうが，それは必ずしも可能ではないという問題がある．

4. 提案する発信者詐称防止方式

4.1 満たすべき条件

2 章で述べた内容を整理すると，従来の手法の問題点を解決しつつ発信者詐称を防止するためには，電子メールシステムが次の各条件を満足する必要がある．

（条件 1）利用者が管理するクライアント計算機に特別なソフトウェアを必要とせずに利用者を認証し，メッセージ発信者を特定できること．

（条件 2）メッセージの送信に SMTP をそのまま利用できること．すなわち，MUA に変更を加えず，既存のソフトウェアがそのまま利用できること．

（条件 3）特定した発信者と発信者アドレスを照合できること．

（条件 4）発信者詐称を検出した場合，対応を柔軟に選択できること．

4.2 認証サーバの導入

本論文で提案する方式では，条件 1（および条件 3 の一部）を満たすために認証サーバを導入する．ここでいう認証サーバは，

（機能 1）利用者を認証する機能

（機能 2）MTA からの問合せに応じて認証した利用者を答える機能

を実現する抽象的な概念であり，これらの機能が実現できるならば複数のソフトウェアの組合せであってもよい．

本方式では，利用者はクライアント計算機を利用し始める段階あるいはクライアント計算機をネットワークに接続する段階で認証サーバを用いて認証を行い，クライアント計算機がサーバ計算機にメッセージの配送要求を行う際には，サーバ計算機上の MTA が認証サーバに問合せを行うことによって利用者を特定する（**図 2**）．このように，本方式では認証サーバという信頼できる情報源を用いることによって，利用者側の計算機の OS や設定，MUA の種類などに依存することなく確実に利用者を特定することを可能としている．

4.2.1 認証サーバの実現法

ここで，2.1 節の環境 1〜4 のいずれにおいても上の（機能 1),（機能 2）を持つ認証サーバを導入して利用者の特定が可能であることを示す．

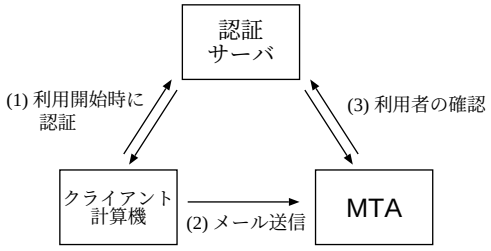

図 2 本論文の方式
Fig. 2 Overview of the proposed method.

環境 1 においては，元来システムが持つ認証機構（Unix における login など）が存在し，クライアント計算機の利用開始時点で認証が行われるため，利用者の認証が可能である（機能 1）．したがって，その認証機構と連携することによって，メッセージを発信しようとする利用者の情報（利用者名）を取得する機能があればよい．具体的には，たとえば，クライアント計算機に IDENT サーバを導入することによってメッセージの発信を要求した利用者を知ることが可能である（機能 2）．この場合には，システムが持つ認証機構と IDENT サーバの組合せが上でいう認証サーバの機能を果たすことになる．なお，IDENT サーバ導入のために発生する作業は管理者が最初に 1 度だけ行えばよいので，IDENT サーバの導入が利用者の負担となることはない．

環境 2 および 4 においては，文献 9)，10) の手法を用いることによって認証サーバに基づく利用者認証を行うことができる（機能 1）．この認証サーバはクライアント計算機と利用者の対応を保持しており，認証サーバへ問い合わせることによって利用者名を取得することが可能である（機能 2）．

環境 3 においては，通常ネットワーク接続時に認証サーバ（RADIUS サーバなど）を用いた利用者認証が行われているので，本手法においてもこれをそのまま利用することができる（機能 1）．したがって，その認証サーバからクライアント計算機と利用者の対応を取得することができればよい．RADIUS サーバにはそのような機能を持つ実装[11] が存在するので，利用者名の特定が可能である（機能 2）．

以上のように，いずれの環境においても条件 1（および 3 の一部）を満たすための認証サーバを導入し，利用者を特定することができる．

4.2.2 なりすましに対する安全性

本方式において問題となりうるのは，認証済のクライアント計算機の IP アドレスを詐称することによるなりすましである．すなわち，すでに認証されたクラ

イアント計算機の IP アドレスとその計算機に対応する利用者名を詐称することによって，他人の発信者アドレスを詐称できるかどうかという問題である．

環境 1 の場合は，利用者が環境を変更できないため，IP アドレスを詐称することは不可能である．物理的に別の計算機を接続して認証済のクライアント計算機の IP アドレスを付与できる可能性は存在するが，これについてはクライアント計算機を接続するハブ側で MAC アドレスフィルタリングを行うなどの対策により防止できる（これは本論文の場合に限らず一般的に必要となる対策である）．

環境 2 および 4 では，文献 9)，10) の手法を採用することを前提としている．この場合，IP アドレスの詐称はシステム的に防止されているので問題は起こらない．

環境 3 では，一般に IP アドレスはアクセスサーバ側から与えられ，それ以外のアドレスを利用することはできないため，やはり問題は起こりえない．

さらに，環境 3 や 4 のように動的に IP アドレスが割り当てられる環境で過去に認証されたことのある IP アドレスが再割当てされたとしても，利用者が利用を終了するとそれに同期して認証サーバからその利用者の情報（利用者名）を得ることができなくなるため，同じ IP アドレスを過去に使用していた利用者の電子メールアドレスを詐称することは不可能である．

このように，環境 1〜4 のいずれの場合においてもなりすましは防止できる．

4.3 フロントエンドプログラムの導入

本論文では，条件 2〜4 を満たすために，MTA にフロントエンドプログラムを導入する．このフロントエンドプログラムは SMTP によって MUA からのメッセージを受け取って本来の MTA に中継するようになっており，MUA としては従来のものをそのまま利用することができる．フロントエンドプログラムはメッセージを受け取ると，SMTP セッションを確立したまま MUA（が動作している計算機）の利用者を認証サーバに問い合わせ，メッセージ中に含まれる発信者アドレスと認証した利用者とを照合する．照合の結果，発信者詐称を検出した場合には，SMTP セッション中に配送を拒否できるだけでなく，エラーメールとして本来の差出人に送り返したり，発信者を強制的に書き換えたりするなど，柔軟な処理が可能である．

4.4 システム構成と動作

本節では，提案する方式におけるシステム全体の構成と動作を示す．

図 3 に示すように，本手法では図 1 の環境に加えて，ダイアルアップ認証サーバ（RADIUS サーバ）や IDENT サーバ，IP フィルタを導入する．また，サーバ計算機にはフロントエンドプログラム（auth-smtpd）を導入する．

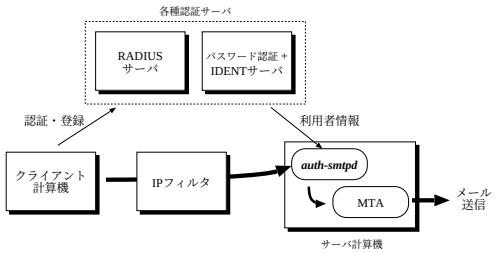

図 3 システム構成例
Fig. 3 A sample configuration of the system.

IP フィルタはクライアント計算機が他の（フロントエンドプログラムを持たない）MTA に接続することによって認証を逃れることを防止するためのものである．

次に，2.1 節の環境 3 を例にとり，利用者がメッセージを発信する場合のシステム全体の動作を述べる．なお，環境 1，2 ならびに 4 における動作も本質的には同様である．

(1) 利用者は，公衆電話回線などを介してクライアント計算機をリモートアクセスサーバに接続する．
(2) リモートアクセスサーバは認証サーバと通信して利用者認証を行い，正規の利用者であることを確認すると，クライアント計算機からのネットワークアクセスを許可する．このとき，認証サーバはクライアント計算機の IP アドレスと利用者名の対を保持しておく．
(3) 利用者は，クライアント計算機上の MUA を用いてメッセージを作成し，発信する．MUA はサーバ計算機に SMTP で接続する．
(4) サーバ計算機では，auth-smtpd が MUA からの SMTP 接続を受け付け，IP アドレスに基づいてクライアント計算機が監視対象であるかどうかを調べる．
(5) クライアント計算機が監視対象であれば，auth-smtpd はこれに対応する認証サーバ☆に問い合わせてクライアント計算機の利用者名を取得し，発信者詐称防止処理を行いながら MUA からの SMTP セッションを MTA に中継する．監視対

☆ クライアント計算機によって異なる場合があるため，1 台とは限らない．

象でなければ，MUA からの SMTP セッションを単に MTA に中継する．

(6) MTA は auth-smtpd が中継した SMTP セッションを処理し，通常どおりメッセージの配送を行う．

5. 実装と評価

5.1 発信者詐称時の対応方法

前章で述べたように，本システムでは発信者詐称に対して柔軟な処理を行うことができる．本章では，とりうる処理の選択肢を掲げ，実際の局面においてどのような処理を行うべきかについて考察する．

STMP における発信者アドレスには，2 つの種類がある．(1) SMTP セッション中の MAIL コマンドに含まれる発信者アドレス，(2) メッセージヘッダに含まれる From:ヘッダの発信者アドレス，の 2 種類である．これら 2 種類について，それぞれ詐称の可能性を考えなければならない．

このうち，(1) のアドレス（reverse-path，一般に Envelope From と呼ばれる）は，エラーメッセージを返す際に使用される情報であり，確実に発信者のところへ戻る経路を提供する必要がある[2] ため，正規アドレスに強制的に書き換えを行う．この書き換えによって，不正行為によって利用者名を偽った形でネットワーク接続を行わない限り，reverse-path の詐称は不可能となる．また，reverse-path は一般にシステムの動作記録の対象となるため，この書き換えによって動作記録の信頼性が増し，何らかの問題が生じた場合でも原因調査が容易になる効果も期待できる．

ここで，正規アドレスとして扱うのは，認証サーバから取得した利用者名とその認証サーバに対応するドメイン名（これはあらかじめ与えておく）から生成される電子メールアドレスである．認証に使用する利用者名（たとえば，PPP 接続におけるアカウント名）と電子メールアドレスにおける利用者名が異なる場合には，auth-smtpd 側にあらかじめ変換テーブルを用意することによって対応する．これは，(2) のアドレスについても同様である．

また，(2) のアドレスについては，利用者が電子メールアドレスを複数所有する場合があり，正規アドレスと一致しないことが必ずしも発信者アドレスの詐称を意味しない場合が考えられる．そのような利用は認めないという方針であれば問題はないが，そうでない場合には，やはり auth-smtpd 側にあらかじめ利用者ごとに利用可能な電子メールアドレスを複数登録しておき，発信者アドレスがこれらのアドレスのうちのいずれかに一致すれば詐称と判断しないような処理を行えばよい☆．

詐称を検出した場合の対応としては，次のような処理が考えられる．

（処理 1）SMTP セッション中にエラーとして配送を拒否する．
（処理 2）エラーメールとして発信者に送り返す．
（処理 3）強制的に正しいアドレスに書き換える☆☆．
（処理 4）From: には手を加えず，別途発信者を示すヘッダ（Sender:）を付加する☆☆☆．
（処理 5）単に破棄する．

我々の設計では，これらはいずれも実現可能であり，運用方針に基づいて選択することができる．いずれの場合においても利用者が指定した発信者アドレスは利用者のアカウント名とともに記録されるため，問題が生じた場合に追跡調査が可能である．

auth-smtpd プログラムは，現在のところ大阪市立大学学術情報総合センターと岡山大学総合情報処理センターにおいて運用しているが，大阪市立大学では，ダイアルアップサービスを対象として処理 4 を採用した．これは，電子メールの通常の使用範囲においても，次のような場合があることを配慮した結果である．

- 電子メールの再配布時のように，From: ヘッダが発信者とは異なる場合
- 電子メールアドレスを複数所有しており，ネットワーク利用時の認証に用いる利用者名から導かれる正規アドレスとは異なったアドレスを From: ヘッダに使用したい場合
- 上に関連して，PGP（Pretty Good Privacy）[12] による署名時のように，From: アドレスをキーとして使用する場合

なお，詐称の判断では正規アドレスのみを有効とした．これは，これ以外のアドレスを利用者自身を示す有効なアドレスであると管理者が確認することが困難なためである．

一方，岡山大学では，情報実習室の教育用計算機システム（Windows 95 搭載）を対象として処理 3 を採用した．このシステムは 2.1 節で述べた環境 2 に該当するが，認証サーバを用いた利用者認証を行っており，ある計算機を使用している利用者を認証サーバの

☆ ただし，登録するアドレスが利用者自身を示す有効なアドレスであることを登録時に確認できるしくみが必要である．
☆☆ さらに発信者に書き換えた旨の通知を行うなどの処理も可能である．
☆☆☆ Sender: がすでにあればその内容は X-Original-Sender: に，X-Original-Sender: があればさらにその前に X-Original-を付加することを繰り返し，元のヘッダをすべて保存する．

情報から特定することができる．

処理 3 を採用した理由は，次のとおりである．

- 利用者のほとんどは電子メールのヘッダ形式に対する知識が不足しており，発信者詐称を見破れない危険性が高い．
- 教育用計算機システムは各計算機を多くの利用者が共有して利用するため，新しい利用者がログインした場合に MUA の設定として直前の利用者のアドレスが残されていることがある．その場合，新しい利用者がメッセージを発信する際にそれをそのまま誤って用いる危険性が高い．
- 処理 1 や処理 2 では，エラーに直面した利用者が MUA を正しく設定し直してから同一内容を再送する必要があり，利用者のレベルを考慮すると負担が大きい．

5.2 実　　装

これまでに述べた設計方針に基づいて，auth-smtpd プログラムを実装した．実装には Perl5 を用いており，TCP のポート 25（SMTP サービス）にバインドされたデーモンプログラムとして動作する．このプログラムは，POSIX 準拠または BSD 準拠の Unix システムで動作するよう作成されている．

実際にメールの配送を行う MTA としては sendmail を使用しているが，特に sendmail に依存するものではないので，他の MTA でも使用可能である．

認証サーバとしては，現在のところ 2.1 節の環境 1 のための IDENT サーバと環境 2〜4 のための RADIUS サーバをサポートしている．RADIUS サーバには，DTC RADIUS [11] を使用した．この RADIUS サーバは，RADIUS の拡張機能として，認証した利用者名とクライアント計算機の IP アドレスの対応を答える機能を有しており，特に手を加えることはしていない．ダイアルアップ環境において使用されるアクセスサーバは利用者とクライアント計算機の IP アドレスとの対応関係の情報を保持しているので，このような機器に問い合わせることによって利用者名を取得するという方法も可能であろう．

IP フィルタとしては既存のルータのフィルタリング機能を使用している．

5.3 運用による評価

実装した auth-smtpd プログラムを大阪市立大学学術情報総合センターの教育用ダイアルアップサービスおよび岡山大学総合情報処理センターの教育用計算機システムに導入して実際に運用し，評価を行った．

大阪市立大学学術情報総合センターのダイアルアップサービスにおいて，auth-smtpd プログラムを稼動させることによって得られた結果ならびに Sender: が付加された理由をそれぞれ**表 1**，**表 2** に示す（1999 年度前半の結果である）．

表 1 大阪市立大学における実験結果
Table 1 Experimental results at Osaka City University.

稼働時間	6 カ月
全メール処理数	742,547 件
PPP 接続からのメール発信数	32,363 件
Sender: が付加された件数	1,976 件

表 2 大阪市立大学において Sender: が付加された理由
Table 2 Reasons of 'Sender:' header addition at Osaka City University.

他組織発行のメールアドレスを使用	1,171 件
利用者の設定が不適切（ドメイン名がない，タイプミスなど）	749 件
空アドレス（<>）	15 件
その他	41 件

大阪市立大学では，入学時に全学生に対して教育用計算機システムのアカウントを発行しており，学生はすべて教育用システムのドメインに属するアドレスを持っている．これに加えて，研究室配属の学生や大学院生は，その所属部局・研究室などの電子メールサーバを利用できるので，そちらのサーバのアドレスを持っていることがある．また，自分で ISP と契約して電子メールアドレスを持っている場合もある．このように 1 人で複数の電子メールアドレスを所有している学生が，教育用システムのサーバを使用しているにもかかわらず From: ヘッダに他のアドレスを指定している，という場合が表 2 の「他組織発行のメールアドレスを使用」に集計されている．また，空アドレスは，sendmail がエラーメッセージを返信する際に使用するアドレスである．その他と分類しているのは，

(1) 大阪市立大学では学部学生と大学院生に別のアカウントを発行しているが，大学院進学時にメールアドレスの設定のみ更新してダイアルアップ設定は学部時代のアカウントを使用している（またはその逆），
(2) 友人の計算機を借用し，メールの設定のみを変更して利用した，

という理由と推定される．

同様に，岡山大学総合情報処理センターの教育用計算機システムにおいて auth-smtpd プログラムを稼動させることによって得られた結果ならびに From: ヘッダの強制書き換えを行った理由をそれぞれ**表 3**，**表 4** に示す．

岡山大学では，Windows95 を OS とする PC を設

表 3 岡山大学における実験結果
Table 3 Experimental results at Okayama University.

稼働時間	10 日間
全メール処理数	77,896 件
教育用計算機システムからのメール発信数	816 件
From: ヘッダを書き換えた件数	90 件

表 4 岡山大学において From: ヘッダが書き換えられた理由
Table 4 Reasons of 'From:' header substitution at Okayama University.

利用者の設定が不適切	35 件
前の利用者がログアウトせず，別の利用者がそのまま使用した	29 件
不明（おそらく同上）	26 件

置した演習室において実験を行った．ここでは，利用者は使用前にログインし，使用後にログアウトするという利用形態を採用している．ここで From: ヘッダの書き換えが生じた理由に関して聞き取りによる追跡調査を行ったところ，前の利用者がログアウトせずに帰ってしまった PC を次の利用者がそのまま使用し，MUA の設定のみを自分用に書き換えて使用していたことが判明した．これが表 4 の 29 件である．調査ができなかったために不明に分類されている 26 件についても，おそらく同一の原因であると推測される．

5.4 処理速度の評価

本方式においてオーバヘッドとなるのは，次の各処理である．

(1) 接続してきたクライアントがチェック対象かどうかを調べる．
(2) 認証サーバ（RADIUS サーバ）へ利用者名を問い合わせる．
(3) From: ヘッダをチェックする．
(4) Sender: を付加する，あるいは From: ヘッダを書き換える．

このうち，(1) はすべての SMTP セッションで生じるが，(2) および (3) はチェック対象となるクライアント計算機からの接続時のみ，さらに (4) は (3) において書き換えの条件が成立したときのみに生ずるオーバヘッドである．

大阪市立大学において測定した電子メール 1 通あたりのオーバヘッドの実測値（ある 1 日分の平均値）を**表 5** に示す．この表より，本手法のオーバヘッドは十分小さいことが分かる．また，実際に稼動させてみた結果でも，実運用上問題となることはなかった．

表 5 本手法のオーバーヘッド
Table 5 Overheads of our method.

(1) クライアントのチェック	0.77 ms
(2) 認証サーバへの問合せ	901 ms
(3) From: ヘッダのチェック	1.45 ms
(4) Sender: ヘッダの付加	2.92 ms

6. ま と め

本論文では，信頼できる認証サーバを利用することによって，電子メールの配送プロトコルに手を加えることなく送信者認証を行い，発信者詐称を防止する方式について述べた．これにより受信者は確実に本来の送信者を知ることが可能となり，電子メールの不正利用を抑止する効果が得られる．本方式は利用者側の計算機に新たなソフトウェアを導入する必要がなく，利用者計算機の OS や MUA に依存しない．

本方式を実装したプログラムは，我々の教育用システムにおいて 1 年以上にわたって安定に稼働している．その結果，実際に発信者詐称が検出可能であり，またオーバヘッドが実用上問題ない範囲に収まることが確認された．

参 考 文 献

1) Johns, M.C.S.: Identification Protocol, RFC 1413 (1993).
2) Postel, J.B.: Simple Mail Transfer Protocol, RFC 821 (1982).
3) Rigney, C., Rubens, A.C., Simpson, W.A. and Willens, S.: Remote Authentication Dial In User Service (RADIUS), RFC 2138 (1997).
4) Sendmail: Sendmail Home Page `http://www.sendmail.org/`
5) Rose, M.: Post Office Protocol – Version 3 Extended Service Offerings, RFC 1082 (1988).
6) Qualcomm: Qpopper Home Page `http://www.eudora.com/freeware/qpop.html`
7) Myers, J.G.: SMTP Service Extension for Authentication, RFC 2554 (1999).
8) Harkins, N. and Levine, J.: How to restrict relaying through your mailserver to only local users, that have authenticated using Post Office Protocol `http://www.iecc.com/pop-before-smtp.html`
9) 石橋勇人，山井成良，安倍広多，大西克実，松浦敏雄：IP アドレス/MAC アドレス偽造に対応した情報コンセント不正アクセス防止方式，情報処理学会論文誌，Vol.40, No.12, pp.4353–4361 (1999).
10) 石橋勇人，阪本　晃，山井成良，安倍広多，大西克実，松浦敏雄：情報コンセントにおける認証とアドレス偽造防止を VLAN 機能により実現するシステム LANA2，情報処理学会研究報告，Vol.99, No.56, pp.137–142 (1999).

11) デジタルテクノロジー：DTC Radius 2.03
http://www.dtc.co.jp/Radius2.0/
12) Garfinkel, S.: *PGP: Pretty Good Privacy*, O'Reilly & Associates (1995).

(平成 12 年 1 月 21 日受付)
(平成 12 年 9 月 7 日採録)

石橋 勇人（正会員）

昭和 62 年京都大学大学院工学研究科修士課程情報工学専攻修了．平成元年同博士後期課程情報工学専攻退学．同年京都大学大型計算機センター助手．平成 10 年より大阪市立大学学術情報総合センター講師．高速ネットワーク，ネットワーク管理システム等に関する研究に従事．人工知能学会，電子情報通信学会，IEEE，ACM 各会員．

山井 成良（正会員）

昭和 61 年大阪大学大学院工学研究科（電子工学専攻）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）博士後期課程中退．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を経て，現在岡山大学総合情報処理センター助教授．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）．

安倍 広多（正会員）

平成 4 年大阪大学基礎工学部情報工学科卒業．平成 6 年同大学大学院博士前期課程修了．同年 NTT 入社．平成 8 年大阪市立大学助手．マルチスレッド機構の実装，マルチメディアアプリケーションの設計等に興味を持つ．電子情報通信学会会員．

大西 克実（正会員）

平成 4 年大阪大学工学部通信工学科卒業．平成 6 年同大学大学院修士（通信）課程修了．平成 8 年大阪市立大学助手となり現在に至る．組合せ最適化問題の解法，分散処理環境の利用に関する研究に従事．電子情報通信学会，日本 OR 学会各会員．

松浦 敏雄（正会員）

昭和 50 年大阪大学基礎工学部情報工学科卒業．昭和 54 年同大学大学院基礎工学研究科（情報工学専攻）後期博士課程退学後，同大学基礎工学部助手．平成 4 年同大学情報処理教育センター助教授，平成 7 年大阪市立大学教授．工学博士．ユーザインタフェース，マルチメディア，情報教育等に興味を持つ．ACM，IEEE，電子情報通信学会各会員．