偽の送信者メールアドレスを持つメールの配送を防止するフィルタ

松 原 義 継†

現行のメール配送規約では，送信者を知るための情報である “From:” フィールドに記述されている送信者メールアドレスがその送信者本人に割り当てられている正規のメールアドレスであることが保障されない．本提案システム milter-bogus-from は，ユーザがメールを配送するときにこの送信者メールアドレスが正規であることを照合し，正規ではないメールは配送を拒否する．milter-bogus-from は，SMTP AUTH が実装されている Sendmail の下で，そのフィルタ API である milter を用いたフィルタであり，ネットワークの利用自体に認証を必要とする環境でなくても利用できる．正規メールアドレスは LDAP サーバから取得されるため，柔軟な管理が可能である．ユーザは SMTP AUTH に対応したメールクライアントソフトを導入することで利用可能であり，ユーザに対する負担は少ない．運用サイトにとっては自らのサイトから配送されたメールに対して，その送信者メールアドレスに一定の裏付けを与えることができる．

A Filter Blocking Mail Transfer with a Bogus Sender e-mail Address in “From:” Field

Yoshitsugu Matsubara†

The present e-mail transfer protocol can not assure that a sender e-mail address in the “From:” field is the correct e-mail address assigned by the site. This enables user to send mails with bogus sender e-mail addresses and causes troubles. The proposed system called “milter-bogus-from” checks the sender e-mail address through the “milter” API under Sendmail systems with the SMTP AUTH mechanism, and will work in general network systems without authentication mechanisms. The correct sender e-mail address is obtained through LDAP service, which enables us to manage users flexibly. Users can send e-mail massages through this mechanism by installing e-mail clients compatible with SMTP AUTH. Hosts transferring e-mail messages can authorize their e-mail messages with correct sender addresses.

1. 序 論

ネットワーク上におけるコミュニケーション手段として，メールは現在でも主要なツールの 1 つであり，ネットワーク基盤の整備とともに，その重要性は増している．しかし，不適切なメールの急増により，メールを介したコミュニケーションシステムの脆弱性も一般に指摘されており，たとえば山口[1] の記事がある．

RFC2821[2] 等のメール配送に関する規約では，送信者メールアドレスがその本人に対して運用サイトが割り当てた正規メールアドレスであることを裏付けるものが提供されない．これは，過失または故意を問わず，送信者メールアドレスに他人のメールアドレスもしくは存在しないメールアドレスを利用できることを意味する．このようなメールでは，メールヘッダもしくはメールサーバ内のログに記録されている配送記録を調べても送信者の特定は容易ではなく，これを悪用した spam メールが後を絶たない．送信者メールアドレスに対して一定の裏付けが与えられないことが，メールという重要なコミュニケーション手段の信頼性を損なっている．

これに対し著者は，メールクライアントソフト（MUA☆）から Sendmail[3]，postfix[4]，qmail[5] 等のメール配送ソフト（MTA:☆☆）にメールを配送するとき，正規メールアドレスを持つメールだけを配送させるシステムを提案する．この方法は，誤った送信者メールアドレスを持つメールの配送をその最初の MTA で防止できる．この方法ではメール本文の内容は問われないが，その送信者メールアドレスに一定の裏付けが与えられているので，異常な量のメール配送

† 佐賀大学
Saga University

☆ Message User Agent
☆☆ Message Transfer Agent

にともなう配送遅延発生およびメール本文の内容が原因の社会的問題発生等の際に送信者を調査することが容易になることが期待される．同時に，spam メールを配送する者たちに対してその配送自体を心理的に躊躇させることが期待できる．受信者に対する負担を軽減し，同時にネットワークにおける資源の浪費を抑止するためにも，送信者メールアドレスが誤っているメールを最初から配送しないことが望ましい．

上記の目的のため，著者は Sendmail のフィルタ API である milter [6] を用いてメール送信時に送信者メールアドレスを照合する Sendmail 用フィルタ milter-bogus-from を開発した．

本稿の構成は以下のとおりである．2 章では，milter-bogus-from の概要を述べる．3 章では，関連研究および本提案との相違を述べる．4 章では，その設計を述べる．5 章では，実装をふまえて，その使用例および運用モデルを述べる．最後にまとめと議論を 6 章で行う

2. 概　　要

本提案システム milter-bogus-from（以下,「本ソフトウェア」と呼ぶ）は，Sendmail が提供するフィルタ用 API である milter をその基礎にしている．milter は，Sendmail 内部で行われる各種処理に対するイベント関数等を提供している．

本ソフトウェアにおける，MUA および Sendmail 等との関係は**図 1** のようになる．SMTP AUTH [7] が機能している Sendmail があり，正規メールアドレスが登録されている LDAP [8] サーバがある．本ソフトウェアは，この Sendmail と LDAP サーバを結ぶことで，正規メールアドレスが送信者メールアドレスとして使われていることを確認する．

本ソフトウェアは，ユーザが MUA から Sendmail へ SMTP AUTH によりメールを配送する過程で，イベントの形でそのメールの送信者メールアドレスを LDAP サーバ上の正規メールアドレスと照合する．milter が組み込まれている Sendmail は，メール 1 通の処理に対して種類の異なる milter のイベントを複数回発生させる．これらイベントの中で，本ソフトウェアは SMTP AUTH で認証されたユーザ名および送信者メールアドレスを取得する．MUA から Sendmail へメール内容がすべて配送されると，そのことに対するイベントの中で，本ソフトエアは LDAP サーバに送信者メールアドレスの照合を行う．もしそれが正規メールアドレスである場合，メールヘッダおよび Sendmail のログにそのことが記録され，Sendmail は実際に配送を行う．そうでない場合は，Sendmail のログにそのことが記録され，Sendmail は MUA に対してコード 554 を返して，メール配送は行われない．

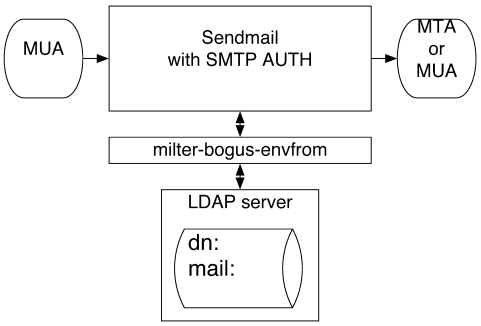

図 1 milter-bogus-from の概要
Fig. 1 Concept of milter-bogus-from.

送信者メールアドレスが正規のものではない場合の処理として，送信者メールアドレスを正規のものに置き換えて配送させることも考えられる．しかし，本ソフトウェアでは配送した本人に対して，正規メールアドレスの使用を促すことを重視した．

本ソフトウェアの機能を実現するためには，正規メールアドレスがあらかじめ登録されていることが必要である．本ソフトウェアはその登録先として LDAP 認証サービスを用いる．LDAP サーバ内に各利用者の正規メールアドレスを登録することで，通常の認証情報とともに一元管理が可能となる．さらに，LDAP の設定によって複数アドレスの登録等柔軟な運用体制が可能となる．

この仕組みでメールが配送された場合，SMTP AUTH で認証されたユーザがその正規メールアドレスを用いてメールを配送したことになるので，そのメールの受信者にとっては送信者メールアドレスに対する一定の裏付けが得られる．本ソフトウェアは，SMTP AUTH による認証が前提であるので，サイト外からこの Sendmail 経由でメール配送を行う場合でも，第三者による不正配送の心配はない．

本ソフトウェアの実現には SMTP AUTH および LDAP の導入が要求されるが，ユーザおよび管理者はそれに見合うだけの利点がもたらされる．

ユーザにとっては，SMTP AUTH に対応した MUA の導入が唯一の要求となるが，一度導入すれば，それ以後は従来どおりにメールの送受信が行える．何よりも，送信者メールアドレスを間違わずに配送できるので，メール配送に関するトラブルを防止できる．

管理者にとっては，LDAP による正規メールアドレスの管理が要求されるが，自らのサイトから配送され

るメールの送信者メールアドレスをその運用サイトとして保障できる．

3. 関連研究

本ソフトウェアに関連した他研究は，大きく 3 種類に分類される．

- 配送元サイトの確認
  送信者メールアドレスにおけるドメイン名の部分を調べたり，メールに署名を添付したりすることで，そのメールがそのドメイン名を持つサイトから配送されたことを保障する．Sender ID [9]，SPF [10]，DomainKeys [11] がこの方法に分類される．
  この方法では，そのメールを配送した者がその正規メールアドレスを使用していることまでは保障されず，同一サイト内でユーザ名を誤った場合に対応できない．
- ネットワーク利用時の認証
  ダイアルアップ PPP 接続もしくは利用時に認証が必要な演習室，もしくは Opengate [12] 等のように端末を利用する際に認証が必要なネットワーク下で，その認証したユーザが配送したメールの送信者メールアドレスを正規メールアドレスと照合する．石橋ら [13] が開発した送信者メールアドレスの詐称防止方法がこれに分類される．
  この方法では，MUA および MTA に対する変更が不要であるが，端末の利用に認証が不要なネットワーク下ではこの方法が利用できない．ネットワークに接続するすべての端末がその利用に認証が必要ではないので，この方式を利用できるネットワークは制限される．
- メール配送時の認証
  メール配送時に認証を行うことで，登録ユーザのみの配送を保障する．認証できないユーザはメールが配送できないので，登録外ユーザによる不正配送が防止できる．SMTP AUTH や POP before SMTP [14] がこの方式に分類される．
  メールヘッダおよびメールサーバのログにその記録が残されるので，配送したユーザの特定が容易になるが，登録ユーザがその正規メールアドレスを送信者メールアドレスとして正しく利用することが保障できない．登録ユーザ自身による送信者メールアドレスの誤りに対しては，これが防止できない．

本ソフトウェアでは，送信者メールアドレスは MUA から Sendmail にメールを配送する時点で照合されるので，この Sendmail より先の MTA もしくは MUA には制約がなく，配送元のサイト内だけで実現できる．SMTP AUTH はメール配送だけの認証であり，ネットワーク利用時の認証ではない．ネットワークを利用するすべての端末がその利用に認証を行うわけではないので，本ソフトウェアはその利用範囲が広い．

4. 設　　計

本章では，本ソフトウェアの設計の概要を述べる．

4.1 Sendmail から取得する情報

本システムにおいて，milter API を通じて Sendmail から取得する情報は以下のとおりである．

- 送信者メールアドレス
- SMTP AUTH で認証されたユーザ名
- 接続元端末の IP アドレス

送信者メールアドレスは “From:” の項目から取得できる．SMTP AUTH で認証されたユーザ名は，milter が提供する関数で取得できる．接続元の IP アドレスは，そのメールがローカルホストからのものであるか否かを判別するために用いる．これは，本ソフトウェアが動作しているホスト内部で管理者が cron 等で管理用情報をメールで自動配送する場合を考慮したものであり，これも milter が提供する関数で取得できる．

4.2 正規メールアドレスを管理するための LDAP ディレクトリの構造

本ソフトウェアの機能を実現するためには，ユーザ名を一意な識別名（dn）とするエントリがユーザごとに必要である．正規メールアドレスは，属性名 mail を持つ各エントリの属性として格納される．つまり，各ユーザごとにその属性としてその正規メールアドレスが管理される．

mail は，正規メールアドレス 1 つに対して最低 1 つが用意される．ユーザが複数個の正規メールアドレスを持つ場合は，その数分の mail が用意される．

dn および mail は，LDAP においてともに標準で用意されており，本ソフトウェア導入のために新規に属性を定義する負担は不要である．

4.3 記録のための情報

送信者メールアドレスの照合結果を記録することは，そのメールの受信者および配送元サイトにとって，その裏付けを示すために必要である．記録する情報は，その受信者が配送元サイトに問合せを行うことを前提に，その配送元の担当者が速やかに対応できることが望ましい．本ソフトウェアでは，**表 1** に示す内容が記録される．

照合結果のメッセージは，正規メールアドレスであっ

表 1 メールヘッダおよび MTA のログに記録される情報一覧
Table 1 Information recorded into the mail header and MTA log.

項目
照合結果のメッセージ
本ソフトウェアが動作しているホストの IP アドレス
照合された送信者メールアドレス
照合された時刻

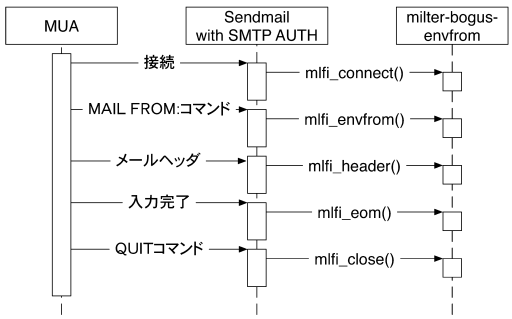

図 2 メール照合の流れ
Fig. 2 Flow of mail processing.

た場合の “Authenticated”，正規ではなかった場合の “Bogus”，そしてローカルホストから配送された場合の “Non-Authenticated due to localhost” の 3 つである．

4.4 処理の流れと機能

milter API では，Sendmail が発生させる各イベントに応じて開発者が必要な機能を実装しているイベント関数を登録することができる．milter の仕様上，本ソフトウェアの機能をすべて実現するためには複数のイベント関数が必要であるので，その必要な各イベント関数内でそれぞれが実現可能な処理を行い，それらイベント関数全体として本ソフトウェアのすべての機能が実現される．本ソフトウェアで定義したイベント関数名およびメールを処理する流れは**図 2** のようになる．

MUA が Sendmail にメールを配送し終わるまでに行われる手続きおよび Sendmail が呼び出すイベント関数の順序は次のようになる．

(1) 接続：MUA が Sendmail に接続することであり，この際にイベント関数 `mlfi_connect()` が呼び出される．
この関数内部での処理は次のとおりである．LDAP サーバへの接続を行い，その接続に失敗した場合は，正規メールアドレスとの照合が不可能になるので，配送拒否が Sendmail に返される．
イベント関数全体でメール 1 通を処理するために，イベント関数間で同一メールの情報を共有する必要がある．そのための共有変数を初期化する．
接続元端末の IP アドレスを共有変数に格納した後に，この関数は処理続行を Sendmail に返す．

(2) MAIL FROM: コマンド入力：RFC2821 で規定されている MAIL FROM: コマンドを入力し，Sendmail はイベント関数 `mlfi_from()` を呼び出す．SMTP AUTH で認証されたユーザ名は，この関数で取得される．そのユーザ名が共有変数に格納され，この関数は処理続行を Sendmail に返す．

(3) メールヘッダ入力：各メールヘッダが入力されるたびに Sendmail はイベント関数 `mlfi_header()` を呼び出す．
この関数内部では，メールヘッダのうち，From:の記述があるメールヘッダに対して，RFC2822[15] に基づき送信者メールアドレスが取得される．取得に成功した場合は共有変数にそれが格納される．最後に，この関数は処理続行を Sendmail に返す．

(4) 入力完了：入力完了を意味する “.”1 行が入力されると，Sendmail はイベント関数 `mlfi_eom()` を呼び出す．メール全体の入力は，ここで完了したことになる．
この関数内部では，これまでに得た情報を基に，最終的に配送を許可するか否かが判断される．その結果はメールのヘッダおよび Sendmail のログに記録される．
判断の手続きは以下の手順である．
(a) ローカルホストからの配送であれば，照合結果は “Non-Authenticated due to localhost” として配送許可．
(b) 認証されたユーザ名があり，その送信者メールアドレスが正規メールアドレスであれば，照合結果は “Authenticated” として配送許可．
(c) 上記のいずれにも該当しない場合は，照合結果は “Bogus” として配送拒否．
メッセージが “Authenticated” および “Non-Authenticated due to localhost” の場合はメールヘッダおよび Sendmail のログに結果が記録され，この関数は配送続行を Sendmail に返す．“Bogus” の場合は，Sendmail のログだけに結果が記録され，この関数は配送拒否を Sendmail

表 2 本ソフトウェアの開発環境
Table 2 The environment of the software.

種類	ソフトウェア名およびバージョン
OS	Solaris10
MTA	Sendmail 8.13.3
SMTP AUTH 用認証	Cyrus SASL 2.1.20
LDAP クライアント	OpenLDAP 2.2.15
LDAP サーバ	iPlanet Directory Server 5.2
開発言語	GCC 3.3.2

```
dn:     uid=matubara,ou=People,dc=saga-u,dc=ac,dc=jp
mail:   matubara@cc.saga-u.ac.jp
mail:   matubara@edu.cc.saga-u.ac.jp
```

図 3 LDAP サーバに登録された正規メールアドレス
Fig. 3 An e-mail address example registered in LDAP server.

```
X-Milter-bogus-from:  Authenticated; 133.49.50.4; matubara@cc.saga-u.ac.jp;
Fri Jun 10 14:39:33 2005
```

図 4 配送許可時のメールヘッダ内容の 1 例
Fig. 4 An example of attached header field in an accepted mail.

```
Jun 10 14:39:33 iyo sendmail[1157]:  [ID 801593 mail.info] j5A5dXdh001157:
Milter add:  header:  X-Milter-bogus-from:  Authenticated; 133.49.50.4;
matubara@cc.saga-u.ac.jp; Fri Jun 10 14:39:33 2005
```

図 5 配送許可時のログ内容の 1 例
Fig. 5 A log example for accepting mail transfer.

に返す.

(5) QUIT コマンド：MUA から Sendmail に QUIT コマンドが配送され，MUA と Sendmail との接続が閉じられる場合に，Sendmail はイベント関数 `mlfi_close()` を呼び出す.
この関数は，LDAP サーバとの接続を閉じて，処理に用いたメモリの開放を行い，処理続行を Sendmail に返す.
この関数が呼び出されるまでの間にイベント関数の 1 つが処理拒否を Sendmail に返している場合は，Sendmail は MUA に対してコード 554 を返して，メール配送を拒否する．そうでない場合は，Sendmail は MUA にコード 250 を返し，この Sendmail から先への配送が行われる.

5. 実例および運用モデル

本ソフトウェアの動作例として佐賀大学学術情報処理センターでの例で示す．本センターでは LDAP による認証が運用されているので，SMTP AUTH による認証および正規メールアドレスの管理はこの LDAP サーバを用いて行われる．本稿執筆時点で，この LDAP サーバに登録されているユーザ数は約 10,000 である．開発環境は**表 2** のとおりである.

5.1 実　　例

平成 17 年 3 月から著者自らのメールを実験対象として運用している結果の 1 例を示す．ここで記述されている送信者メールアドレスは著者自身に割り当てられているメールアドレスである．LDAP サーバには**図 3** のように正規メールアドレスが登録されている.

配送に用いた MUA は Microsoft 社の Outlook Express 6 である．本ソフトウェアは SMTP AUTH によるメール配送が前提であるので，著者に割り当てられているユーザ名およびパスワードは Outlook Express 6 における SMTP AUTH の設定項目で設定される.

5.1.1 正規メールアドレスによる配送時

送信者メールアドレスに正規メールアドレスが設定された場合，見かけ上は何の変化もなくメールが配送される．その受信者にとっても，従来どおりにメールが配送されるだけである.

そのメールヘッダには**図 4** のような 1 行が追加され，本ソフトウェアにより送信者メールアドレスが照合されたことが分かる．Sendmail のログには**図 5** のような記録が保存される．両者を比較することで，このメールにおける送信者メールアドレスの照合が本物

```
Jun 10 14:43:39 iyo sendmail[1176]: [ID 801593 mail.info] j5A5hccj001176:
Milter add: header: X-Milter-bogus-from: Bogus; 133.49.50.4;
xmatubara@cc.saga-u.ac.jp; Fri Jun 10 14:43:39 2005
```

図 7 配送拒否時のログ内容の 1 例
Fig. 7 A log example for rejecting mail transfer.

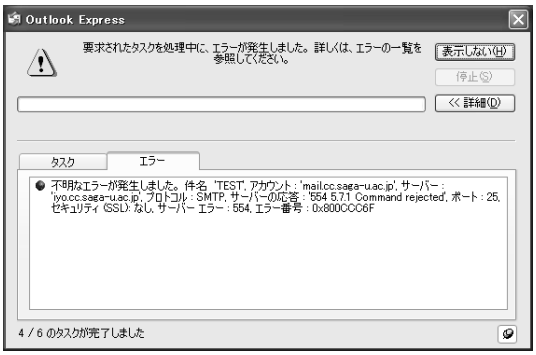

図 6 配送拒否時のメッセージの 1 例
Fig. 6 Error massage for rejected mail.

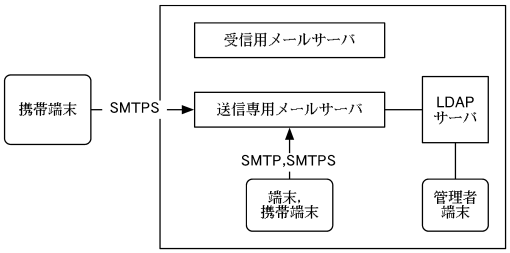

図 8 本ソフトウェアによるメール配送の運用モデル
Fig. 8 Service model of mail transfer.

であることが確認できる．

5.1.2 誤った送信者メールアドレスによる配送時

送信者メールアドレスを誤った場合，配送拒否メッセージが MUA に返され，**図 6** のようなダイアログが MUA 側の画面に表示される．コード 554 が返るため，利用者側でただちに送信拒否の理由を知ることはできないが，送信拒否の事実は知らされる．

Sendmail のログには**図 7** のような記録が保存される．利用者からの問合せがあれば，送信アドレスの不整合であることが利用者に知らされる．

5.2 運用モデル

本ソフトウェアを用いて MUA からメールを配送するシステムの運用モデルを**図 8** に示す．本モデルでは，本ソフトウェアが導入されているメールサーバをサイト内外から利用できることも考慮している．メールサーバは，SMTP AUTH を用いる関係上，MUA から Sendmail に配送する送信専用メールサーバと MTA

図 9 メールアドレス管理ソフト
Fig. 9 Tool for managing mail address registered in LDAP server.

から MUA に配送する受信専用メールサーバとに分けて運用される．サイト外からの配送は，出張等でサイト外にいる場合にノート PC 等の携帯端末上の MUA から利用することが想定されている．

サイト外からメール配送させる際には，セキュリティの観点から SMTPS [16] による暗号化配送のみを行わせる．サイト内からのメール配送は，外部に持ち出した携帯端末を内部でも利用することを考え，SMTP および SMTPS の両方の配送方法が用意される．

正規メールアドレスの登録作業は，管理者のみによりスクリプトもしくは Web ソフトウェアを用いて行われる．ユーザ自身に登録作業を行わせた場合，登録されたメールアドレスの管理者による確認が必要となり，管理コスト増大の恐れがある．そのため，管理者だけの作業とする．登録後の編集用として**図 9** のような Web ソフトウェア等を用意している．

6. まとめと議論

送信者メールアドレスの誤りに対して，MUA から MTA にメールが配送されるときにその送信者メールアドレスが正規メールアドレスであることを照合するフィルタ milter-bogus-from を開発した．本ソフト

ウェアは，MTA の 1 つである Sendmail のフィルタ API である milter を用いて Sendmail のフィルタとして動作し，SMTP AUTH で認証されたメールに対してその送信者メールアドレスを LDAP サーバに登録されている正規メールアドレスと照合する．それが正規メールアドレスの場合，その結果をメールヘッダおよび Sendmail のログに記録して，メールが実際に配送される．そうでない場合，Sendmail のログにそのことが記録され，配送は拒否される．

ユーザにとっては，正規メールアドレス以外の送信者メールアドレスは利用できなくなる．このことにより，その送信者メールアドレスに対して一定の裏付けを得ることができる．本ソフトウェア経由で spam メールが配送された場合でも，その配送者の特定が容易になることが期待できる．送信者メールアドレスに一定の裏付けが得られることは，メールによるコミュニケーションにおける信用という点で有益である．

正規メールアドレスを LDAP サーバで管理することで，SMTP AUTH に必要な認証情報も LDAP サーバに集めることができ，そのことでその管理コストの抑制が期待できる．本ソフトウェアで用いる LDAP の属性は，LDAP が標準で提供しているものだけであるので，その導入負担を抑えることができる．

本ソフトウェアを構成する基礎要素は，milter および SMTP AUTH，そして LDAP であり，これらは既存の技術である．これらの基礎要素の本来の目的は本ソフトウェアのそれとは異なる．本ソフトウェアは，それらを組み合わせることで送信者メールアドレスの誤りという問題を解決可能とした．

メール配送が拒否された場合，現状はエラーコードを MUA に返すだけであるが，ユーザに配送拒否のメールを配送することでユーザに状況を詳しく知らせる仕組みが考えられる．

実際に本ソフトウェアを用いてメールシステムを運用する場合，正規のメールサーバ以外のホストがメールを直接配送する場合がある．これは独自の MTA を有しているコンピュータウイルスが感染した場合やユーザが自分のホストをメールサーバにした場合等が考えられる．このような配送は本ソフトウェアで直接に防止することはできないが，ファイアウォールおよびレイヤスイッチに基づきメール配送をネットワークのレベルで制御することにより，これを防止することが考えられる．

本ソフトウェアは，その仕様上，Sendmail および LDAP サーバに対して正規メールアドレスの照合にともなう負荷を発生させる．そこで，著者および技術職員の 2 名が実際の業務の中で本ソフトウェア経由のメールを配送させることで，配送に関する実験を行っている．この実験に用いている本ソフトウェアを稼動させているメールサーバの機器は，Sun Microsystems 社製の Sun Fire V120 であり，その CPU は UltraSPARC-IIe 648 MHz，メモリ容量は 512 MB，OS は同社製の Solaris10 である．この配送実験においてメール 1 通の処理時間は 1 秒以内であるが，その負荷の評価および大規模な環境下での実証実験は今後の課題である．

謝辞 有益な議論をしていただいた大分大学吉田和幸氏，佐賀大学只木進一氏に感謝いたします．実験には，佐賀大学田中芳雄氏に協力いただきました．

参 考 文 献

1) 山口 英：SPAM だらけのメールボックス，*UNIX MAGAZINE*，Vol.20，No.3，pp.36–40 (2005).
2) Klensin, J.: Simple Mail Transfer Protocol, RFC2821 (2001).
3) Sendmail.org: Sendmail Home Page. http://www.sendmail.org
4) Postfix: Postfix Home Page. http://www.postfix.org
5) qmail: qmail Home Page. http://www.qmail.org
6) milter.org: milter Home Page. http://www.milter.org/
7) Myers, J.: SMTP Service Extension for Authentication, RFC2554 (1999).
8) Wahl, M., Howes, T. and Kille, S.: Lightweight Directory Access Protocol (v3), RFC2251 (1997).
9) Sender ID: Sender ID Home Page. http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx
10) Sender Policy Framework (SPF): SPF Home Page. http://spf.pobox.com/
11) DomainKeys: DomainKeys Home Page. http://antispam.yahoo.com/domainkeys
12) 只木進一，江藤博文，渡辺健次，渡辺義明：利用者移動端末に対応した大規模ネットワークの Opengate による構築と運用，情報処理学会論文誌，Vol.46, No.4, pp.922–929 (2005).
13) 石橋勇人，山井成良，安倍広多，大西克実，松浦敏雄：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，情報処理学会論文誌，Vol.41, No.11, pp.3133–3141 (2000).
14) Levine, J., Mueller, S.H. and Harkins, N.: POP before SMTP. http://www.iecc.com/pop-before-smtp.html
15) Resnick, P.: Internet Message Format, RFC2822 (2001).

16) Hoffman, P.: SMTP Service Extension for Secure SMTP over Transport Layer Security, RFC3207 (2002).

(平成 17 年 6 月 22 日受付)
(平成 18 年 2 月 1 日採録)

松原 義継（正会員）

昭和 44 年生．平成 3 年佐賀大学理工学部物理学科卒業．同年佐賀大学理工学部情報科学科（現，知能情報システム学科）技官．コンピュータネットワークシステムの管理に従事．平成 12 年より佐賀大学学術情報処理センターにて全学基幹コンピュータネットワークシステムの管理に従事．コンピュータネットワークシステムの運用に関する研究および開発に従事．IEEE Computer Society 会員．