# 明示されていない受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

# A filter to block a mail with unseen receivers' e-mail addresses at the first transfer

松原義継*
Yoshitsugu MATSUBARA
佐賀大学学術情報処理センター
Computer and Network Center, Saga University
840-8502 佐賀市本庄町 1
1 Honjo, Saga 840-8502

メール配送において，メールの配送先を示す”To:”，”Cc:”，”Bcc:”フィールドに記述されている受信者メールアドレスと実際の受信者メールアドレスである”RCPT TO:”フィールドのメールアドレスは，メールの転送により必ずしも一致しない．しかしながら，これらが最初から一致しないのは，メールの好ましい使い方ではない．これに送信者メールアドレスの詐称も加われば，spam メール等が引き起こすメール配送に関する各種トラブルの素となる．著者は，メールクライアントソフトからメールサーバソフトウェアである Sendmail にメールを配送する時，Sendmail のフィルタ API である milter の形式で，両者が一致しないメールを配送拒否するフィルタ”milter-unseen-envrcpt”を開発した．

**キーワード**：受信者メールアドレス，spam メール，milter

In the protocols for e-mail transfer, receiver e-mail addresses appeared in the ”To:”, ”Cc:” and ”Bcc:” are not necessary to match those in the ”RCPT TO:” field, because addresses in ”RCPT TO:” field are generated in the case of a mail transfer or a mailing list transfer. Such mismatches at the first transfer, however, will arise several troubles about mail transfer, especially with a bogus sender e-mail address. The author developed a filer program 'milter-unseen-envrcpt' for Sendmail with milter API, which is rejected a mail with the mismatched receiver e-mail addresses at the first mail transfer.

**KEYWORDS** : Receiver e-mail address, spam mail, milter

*E-mail: matubara@cc.saga-u.ac.jp

# 1　序論

インターネット上におけるコミュニケーション手段として，電子メールは重要なツールの 1 つである．社会インフラとしてのインターネットが普及するに伴い，その重要性は増すばかりである．その一方で，ここ数年の spam メールの急増に伴い，電子メールというコミュニケーション手段の脆弱性が指摘されている．

RFC2821 [1] 等のメール配送の規約では，配送先の受信者メールアドレスは，受信者が目にする”To:”，”Cc:”，”Bcc:”フィールドの受信者メールアドレスではなく，ヘッダ部に書かれた”RCPT TO:”フィールドの受信者メールアドレスである．両受信者メールアドレスはその一致が保障されていないが，受信者が混乱しないためにも，基本的に両受信者メールアドレスは一致することが望ましい．これらが一致ない場合として，異なる受信者メールアドレスへの転送やメーリングリストへの投稿もしくは複数人同時配送がある．この 1 番目と 2 番目は，目的の相手にメールを配送した後に転送設定により異なる相手に配送される場合であり，3 番目はメールが各配送先に 1 通ずつ分けられる場合である．これらの場合はその理由が明白であるので問題となることは少ない．

その一方，配送の最初の時点で既に一致しないのは，故意及び過失を問わず，受信者が混乱するだけでありメールの好ましい使われ方ではない．

spam メールの中には，この不一致を悪用していると思われるものがあり，それらの中には”To:”，”Cc:”，”Bcc:”フィールドの受信者メールアドレスが空のものもある．送信者メールアドレスの詐称と組み合わせれば，存在しない相手から存在しない相手への spam メールが自分に配送されるということも可能である．このようなメールはその受信者にとってなんら有益ではなく，メールを用いたコミュニケーションにおける信頼性を損なうことになる．

そこで著者は，メール配送の最初の段階であるメールクライアントソフト (MUA: Mail User Agent) からメールサーバソフト (MTA: Message Transfer Agent) へメールを配送する時点で，両受信者メールアドレスの一致を確認することを提案する．配送の途中で両受信者メールアドレスが一致しなくなることはやむを得ないが，最初の時点では両受信者メールアドレスは一致していることが望ましい．そこで著者は，MTA の 1 つである Sendmail [2] のフィルタ API である milter [3] を用いて，これを実現する Sendmail 用のフィルタ milter-unseen-envrcpt を開発した．

本稿の構成は以下の通りである．2 節では，概要を述べる．3 節では，設計を述べる．4 節では，実例と運用モデルを述べる．最後にまとめと課題を第 5 節で行う．

# 2　概要

本提案の milter-unseen-envrcpt(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 及び Sendmail 等との関係は，図 2 のようになる．本ソフトウェアは，ユーザが MUA から Sendmail へメールを配送する過程で，イベントの形式で ”To:”，”Cc:”，”Bcc:”フィールドの受信者メールアドレスと，”RCPT TO:”フィールドの受信者メールアドレスメールを比較する．

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，本ソフトウェアは受信者メールアドレスを取得する．MUA から Sendmail へメールが全て配送されると，そのことに対するイベントの中で，本ソフトエアは両受信者メールアドレスを比較する．もしそれらが完全に一致するならば，メールヘッダ及び 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．

両受信者メールアドレスが一致しない場合，”To:”，”Cc:”，”Bcc:”フィールドにおける一致しない受信者メールアドレスを一致するように書き換えることも可能であるが，本ソフトウェアではそのメールを配送したユーザ本人に受信者メールアドレスを正しく入力させることを重視した．

例外処理として，本ソフトウェアが稼動しているホスト内部からのメールは，両受信者メールアドレスを比較せずに配送される．これは，cron 等による管理用

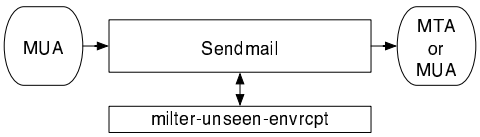


図 1: milter-unseen-envrcpt の概要

メールを管理者に配送する際に，そのローカルホスト内部で転送が行われることを考慮している．

この仕組みでメールが配送された場合，その配送先で転送が行われない限りは，両受信者メールアドレスは一致する．複数人同時に配送する場合は，各配送先で転送が行われない限りは”To:”，”Cc:”，”Bcc:”フィールドの中には”RCPT TO:”フィールドの受信者メールアドレスが必ず存在する．

本ソフトウェアは，あくまでフィルタであるのでユーザにはその存在が全く分からない．ユーザにとっては，本ソフトウェアを導入ための負担が全くなく，従来通りにメールを利用できる．運用サイトにとっても，一度導入するだけであり，それ以後の負担がない．何よりも，”To:”，”Cc:”，”Bcc:”フィールドの受信者メールアドレスに一定の保障が得られるので，メール配送に関するトラブル対応が容易になることが期待できる．

# 3　設計

## 3.1　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通りである．

- ”RCPT TO:”フィールドの受信者メールアドレス
- ”To:”, ”Cc:”, ”Bcc:”フィールドの受信者メールアドレス
- MUA が Sendmail と接続したネットワークインターフェースの IP アドレス

”RCPT TO:”フィールドの受信者メールアドレスは，イベント関数の引数として直接取得できる．”To:”, ”Cc:”, ”Bcc:”フィールドの受信者メールアドレスも，イベント関数の引数からそれを加工することで取得できる．MUA が Sendmail と接続したネットワークインターフェースの IP アドレスは，そのメールがローカルホストから配送されたものであるか否かを判別するために用いるのであり，これは milter が提供する関数で取得できる．

表 1: メールヘッダ及び MTA のログに記録される情報一覧

| 項目 |
|---|
| 比較結果のメッセージ |
| 本ソフトウェアが動作しているホストの IP アドレス |
| 比較された時刻 |

## 3.2　記録のための情報

受信者メールアドレスの比較結果を記録することは，そのメールの受信者及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い合わ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．

比較結果のメッセージは，一致した場合の”Matched”，一致しなかった場合の”Mismatched”，そしてローカルホストから配送された場合の”Localmail”の 3 つである．

## 3.3　処理の流れと機能

milter は，MUA から Sendmail にメールを配送する時，それを処理する各段階に応じたイベント関数等のインターフェースを提供している．開発者は，その目的に応じたイベント関数を定義し，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実現するためには複数のイベント関数が必要なので，各イベント関数毎にそこで実現可能な機能を実装し，イベント関数全体で本ソフトウェアの機能を実現する．

本ソフトウェアで定義したイベント関数は以下の通りであり，図 2 の通りに処理が流れる．

1. `smfi_connect()`: MUA が Sendmail に接続した際に呼び出される．メール 1 通を処理するために

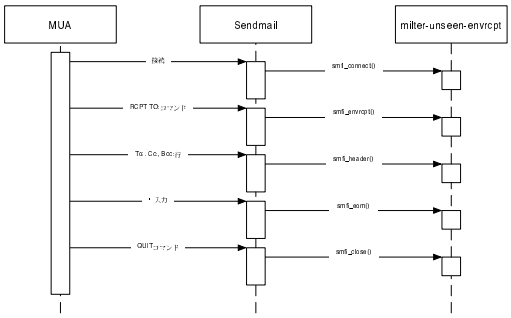


図 2: メール処理の流れ

複数のイベント関数を用いるので，イベント関数間での共有情報を格納する変数を初期化する．

ローカルホストからの接続である場合はその旨を共有変数に格納する．最後に，処理続行が Sendmail に返される．

2. `smfi_envrcpt()`: MUA が Sendmail に”RCPT TO:”コマンドを入力した際に呼び出される．この関数の引数として”RCPT TO:”フィールドの受信者メールアドレスが存在するので，それを”RCPT TO:”フィールドの受信者メールアドレスのリストに登録する．複数人同時にメールを配送する場合は，その人数分この関数が呼び出されるので，その度にこのリストに登録する．登録の際に，既に同じ受信者メールアドレスが登録されている場合は，それは登録されない．最後に，処理続行が Sendmail に返される．

3. `smfi_header()`: 各メールヘッダに対する処理であり，ヘッダ毎に呼び出される．

   各ヘッダの内，”To:”，”Cc:”，”Bcc:”に対してのみ，受信者メールアドレスの抽出を行う．この関数の引数としてこれらの内容が存在するので，RFC8222 [4] に基づき抽出を行い，もしできなければ，処理拒否が Sendmail に返される．抽出できれば，それらを”To:”，”Cc:”，”Bcc:”フィールドの受信者メールアドレスのリストに登録して，Sendmail に処理続行を返す．登録の際に，既に同じ受信者メールアドレスが登録されている場合は登録されない．最後に，処理続行が Sendmail に返される．

4. `smfi_eom()`: メール全体の処理が完了した時に，この関数が呼び出される．”RCPT TO:”フィールドの受信者メールアドレスのリストと”To:”，”Cc:”，Bcc:”フィールドの受信者メールアドレスのリストがここで比較される．

   もし，そのメールがローカルホストから配送された場合は，その比較結果は”Localmail”としてメールヘッダ及び Sendmail のログに記録され，処理続行が Sendmail に返される．

   リモートホストからのメールであれば，次の処理が行われる．始めに，両リストに登録されている受信者メールアドレス数が同じであることが調べられる．これが異なる場合は，異常な受信者メールアドレスがあるとみなして，比較結果は”Mismatched”として Sendmail のログに記録され，処理拒否が Sendmail に返される．それを踏まえて，”RCPT TO:”フィールドの受信者メールアドレスの全てが，”To:”，”Cc:”，”Bcc:”フィールドの受信者メールアドレスのリストに存在することが調べられる．全てが存在していれば，比較結果は”Matched”としてメールヘッダ及び Sendmail のログに記録され，処理続行が Sendmail に返される．そうでなければ，比較結果は”Mismatched”として Sendmail のログに記録され，処理拒否が Sendmail に返される．

5. `smfi_close()`: MUA から Sendmail に”QUIT”コマンドが入力され，MUA と Sendmail との接続が閉じられる場合に呼び出される．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 つで処理拒否が Sendmail に返されている場合は，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．

# 4　実例

本ソフトウェアは，Sun Microsystems 社製の OS である Solaris10 上で稼動している．Sendmail のバージョンは 8.13.3 であり，開発言語は C である．

平成 17 年 4 月から著者自らのメールを実験対象として実験運用している結果の 1 例を示す.

#### 4.0.1　正しい記述時

”To:”，”Cc:”，”Bcc:”フィールドの受信者メールアドレスと”RCPT TO:”フィールドの受信者メールアドレスが一致している場合，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，従来通りにメールが配送されるだけである．但し，そのメールヘッダには図 3 のような 1 行が追加されており，本ソフトウェアにより両受信者メールアドレスが比較されたことが分かる．同時に，Sendmail のログには図 4 のような記録が保存される．両者を比較することで，この照合が本物であることが確認できる.

#### 4.0.2　誤っている場合

両受信者メールアドレスの内容に不一致がある場合，配送拒否メッセージが MUA に返される．Sendmail のログには図 5 のような記録が保存される．これらにより，本ソフトウェアが有効に機能していることが分かる.

### 4.1　運用モデル

本ソフトウェアを用いてメール配送システムを構築する場合，ユーザがメール受信後に自身の携帯電話等へそれを転送することを想定して，配送専用メールサーバと受信専用のメールサーバが必要である．これは，転送されたメールは”RCPT TO:”フィールドの受信者メールアドレスが配送当初のものとは異なるので，本ソフトウェアでは配送拒否されてしまうからである．本ソフトウェアは配送専用メールサーバのみに導入し，ユーザが配送するメールをフィルタリングする.

## 5　まとめと議論

メール配送時，受信者が目にする”To:”，”Cc:”，そして”Bcc:”フィールドの受信者メールアドレスと実際の受信者メールアドレスである”RCPT TO:”フィールドの受信者メールアドレスは必ずしも一致しない．これは，メール転送，メーリングストへの投稿，そして複数人同時配送により発生する現象であるが，この不一致が最初から発生しているのは好ましくない．そこで，MUA から Sendmail へメールを配送する時に，それらが一致する場合のみ配送を許可するフィルタ milter-unseen-envrcpt を開発した．これは，MTA の 1 つである Sendmail 用のフィルタ API である milter を基にしている.

Sendmail がメールを処理する際に，その処理の内容に応じて発生する milter の各種イベント関数を通して両受信者メールアドレスを抽出する．抽出された受信者メールアドレスを基に両受信者メールアドレスを比較して，完全に一致する場合はメールヘッダ及び Sendmail のログにその旨が記録され，メールが実際に配送される．一致しない場合は，Sendmail のログにその旨が記録され，配送が拒否される.

本ソフトウェアは milter を用いているので，ユーザにはその存在が全く分からない．また自らのサイト単独で運用することができる．ユーザには本ソフトウェアのための特別な設定は全く要求されず，その導入負担は低い.

本ソフトウェアで配送拒否が発生した場合，Sendmail は MUA にエラーコードを返すだけであるが，ユーザに配送拒否メールを配送することでユーザに事態の詳細を知らせる仕組みが考えられる.

本ソフトウェアは，その仕様上，受信者メールアドレスの抽出及び比較のためにそのメールサーバに負荷を発生させる．実験運用上では，本ソフトウェアがメール 1 通を処理する時間は 1 秒以内であるが，負荷の評価及び大規模環境下での実証実験は今後の課題である.

## 参考文献

[1] C. Kalt. Internet relay chat: Channel management. RFC2821, April 2000.

[2] Sendmail.org. Sendmail home page. http://www.sendmail.org.

[3] milter.org. milter home page. http://www.milter.org/.

[4] C. Kalt. Internet relay chat: Client protocol. RFC2822, April 2000.

```
X-Milter-unseen-envrcpt:  Matched; 133.49.50.4; Thu May 19 09:57:41 2005
```

図 3: 配送許可時のメールヘッダ内容の 1 例

```
May 19 09:57:41 iyo sendmail[623]:  [ID 801593 mail.info] j4J0vfBW000623:
Milter add:  header:  X-Milter-unseen-envrcpt:  Matched; 133.49.50.4; Thu
May 19 09:57:41 2005
```

図 4: 配送許可時のログ内容の 1 例

```
May 19 10:08:04 iyo sendmail[655]:  [ID 801593 mail.info] j4J183x4000655:
Milter add:  header:  X-Milter-unseen-envrcpt:  Mismatched; 133.49.50.4;
Thu May 19 10:08:04 2005
```

図 5: 配送拒否時のログ内容の 1 例