〔研究紹介〕

認証機能を付加したsendmailの実現

情報科学センター 服部裕之*

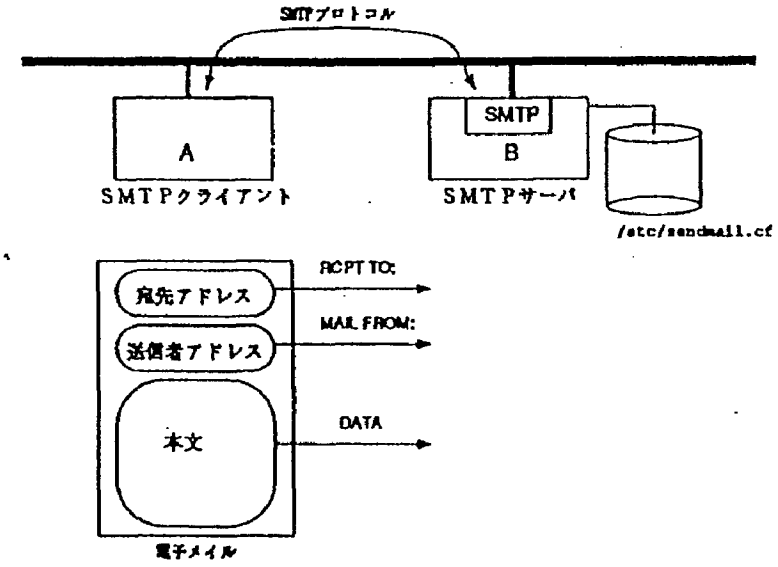
Abstract

セキュリティ上数々の問題を抱えるsendmailプログラムを改良し，SMTPアクセス要求ホストに対する確認機能を持たせた．これにより，あらかじめ許可されたマシン以外からのSMTPアクセス要求を拒否することが可能になった．

本稿では，認証機能を付加したsendmailプログラムの紹介をする．

1. sendmailの問題点

UNIX系ホストにおいて，電子メイルの配送に重要な役割を果たしているのが，UCB[1]で開発されたsendmailプログラムである．sendmailは世界的な広域ネットワークであるインターネットでは標準的に用いられている．しかし，sendmailにはさまざまなセキュリティ上あるいはメイルシステム管理上の問題点がみられる．例えばsendmailのSMTP[2]の実装上の問題である．SMTPというのは，ネットワークに接続されたマシンの間でメイルの転送を行なう時に用いられるプロトコルのことで，sendmailではTCP／IPのソケット機能を用いて実現している．



*明治大学情報科学センター（E-mail：hhat@isc.meiji.ac.jp）

1) University of California, Berkeley

2) Jonathan B. Postel, "Simple Mail Transfer Protocol", RFC821, 8 1982

例えばAというマシンからBというマシンへメイルを転送する時の仕組みを説明する．この時，マシンAはSMTPクライアントに，マシンBはSMTPサーバになる．Bでは，常にsendmailが起動しており，他のマシンからのSMTPアクセス要求を待っている．

まず，AはBに対して，SMTPのポート番号[3]を指定して，TCP／IP接続を行なう．そしてSMTPで定められている手順に従って，宛先メイルアドレス，送信者メイルアドレス，メイルの本文等をBに対して送信する．それを受けとったBではメイル構成ファイル[4]に従ってメイルアドレスを解析し，必要があればさらに他のマシンへ転送する．

ここで問題なのは，従来のSMTPサーバは，SMTPクライアントをえり好みできないという点である．つまり現在のsendmailは，ネットワークに接続されているどのホストからのSMTPアクセス要求でも，みな等しく受けつけてしまう．

これに関して，一昨年，本学内で次のような出来事があった．

ワークステーションを新規に購入したある研究室が，メイル関連の設定を行なっていた所，メイル構成ファイル[5]の設定の仕方が分からず，情報科学センターの適当なワークステーションからファイルをコピーしそのまま運用していた．センターのメイル構成ファイルでは，センター内から発信されるメイルは全て，その宛先アドレスに関わらず，一旦，miscfs[6]へ転送されるようになっている．そしてmiscfsで宛先アドレスを解析した後，mjugwy[7]（宛先が，学内他サブドメインもしくは学外ドメインの時）もしくは，ローカルスプール（isc. meiji. ac. jp宛のメイルの時）[8]にメイルを送る仕組みになっている．つまりセンターのメイル構成ファイルをそのままコピーすると，そのワークステーションから発信されたメイルは全てmiscfsに転送されてしまうばかりか，その時の差し出し人のメイルアドレスはまるでセンター内から発信されたかのようになってしまう．その為，容易にセンターのユーザに“なりすまして”メイルを出す事が可能である．

また，MacintoshでUNIXマシンとのメイルを実現するEudoraというフリーソフトウェアは，メイルを送信する際，ネットワークに接続されたUNIXマシンのsendmailを利用して行なっている．その為，誰でも簡単に“なりすまし”メイルを発信することが可能である．

これらの事は，SMTPサーバがアクセス要求を受け付ける際に，相手がホストの認証を一切行なわないというsendmailの仕組みにも大きな問題があるといわざるを得ない．

そこで，sendmailを改良し[9]，SMTPアクセス要求を受けつける際にそのホストの認証を行なうようにした．次節以降にその詳細を記す．

---

3) ポート番号は25番を用いる．
4) ／etc／sendmail. cf もしくは／usr／lib／sendmail. cf.
5) SunOS4. Xの場合，／etc／sendmail. cf.
6) miscfsは情報科学センター生田分室サブドメイン（isc. meiji. ac. jp）を代表するメイルサーバ．
7) mjugwyは明治大学ドメイン（meiji. ac. jp）を代表するメイルサーバ．
8) miscfsの／usr／spool／mail
9) WIDE Projectで4.3BSDのsendmailに改良を加えた，5.67+1.6Wをベースにした．

2. 認証機能を付加したsendmail

2・1 認証手順

今回作成した，認証機能を付加したsendmail（以下認証版sendmailと記す.）では次のような手段で相手ホストの認証を行なう.

1. daemonモードで起動した認証版sendmailは，SMTPポートをオープンしSMTPサーバとして他ホストからのアクセス要求を待つ.
2. SMTPサーバでは，SMTPクライアントからアクセス要求が発生したら，そのホストのIPアドレスを求め，あらかじめ登録されているSMTPアクセス可能ホストであるかどうかを判定する.
3. もしそのホストがSMTPアクセス可能ホストで無ければ，メイルの送信者に対して，不通通知を出す[10]．不通通知の具体的な内容については付録Aを参照.

2・2 SMTPアクセス可能ホストの定義

認証版sendmailはSMTPアクセス要求が来たら／etc／sendmail. authファイルを読み込み，そこに記載されている内容に従ってアクセス要求を受け入れるか否かを決定する.

／etc／sendmail. authのファイルフォーマットは次の通りである.

○／etc／sendmail. authのフォーマット

＜SMTP制限対象＞	＜制限内容＞	＜コメント＞
＜SMTP制限対象＞	＜制限内容＞	＜コメント＞
	⋮	
＜SMTP制限対象＞	＜制限内容＞	＜コメント＞

＜SMTP制限対象＞	[例]
ネットワークアドレス	133.26.*.*
ホスト名	mjugod01.isc.meiji.ac.jp
	mjugod01
ホストアドレス	133.26.136.15
デフォルト	default

＜制限内容＞	[例]
SMTPアクセス要求を受け付ける	Yes|yes|Ok|ok
SMTPアクセス要求を受け付けない	No|no

10) この時のメイルの差出人はMAILER-DAEMONである.

／etc／sendmail. auth ファイルは，次のルールに従って記述する．

- #で始まる行はコメントとみなす．
- 各行のフィールドはTABもしくは空白で区切る．
- ネットワークアドレスに＊を使う時は注意する．

  −133.26＊.36は133.26.＊.＊と見なされる．
- 制限対象は，

  default→ネットワークアドレス→ホスト名（ホストアドレス）

  の順序で記述する．

／etc／sendmail. auth ファイルの記述例については付録Bを参照のこと．

また，／etc／sendmail. auth をNISマップとして持つことも可能である．認証版 sendmail は，次のいずれかの条件が成り立った時にNISマップを参照する．

1. ／etc／sendmail. auth が存在しない．
2. ／etc／sendmail. auth の最後が＋で終っている．

この時，NISマップ名は必ずsendmail. authとする．

NISマップが参照されると，／etc／sendmail. auth で読み込んだ内容がオーバーライトされるので，注意を要する．

2･3 認証版sendmailの起動時オプション

認証版sendmailでは起動時オプションとして，従来の sendmail に加えて，さらに次のものが指定可能である．

-noauth	SMTPアクセス要求を出しているホストの認証を行なわない

認証版 sendmailは／etc／sendmail. auth もしくはNISより sendmail. auth の引用に成功すると，全てのホストからのSMTPアクセス要求の際に認証を行なう．しかし，この -noauth オプションを用いて sendmail を起動すると，たとえ sendmail. auth の引用に成功しても，従来のsendmailと同様にSMTPアクセス要求時にホストの認証を行なわない．

3. 認証版 sendmail の運用

現在，認証版sendmail[11]は情報科学センターの全てのワークステーション，及び，学外ネットワークとのgatewayホストにて1年以上も稼働しており，今のところ問題はみられない．

---

11) Version 2.1. 本プログラムは ftp. meiji. ac. jp :~ ftp／pub／meiji／src／5.67+1.6W+Mju2.1. tar. Z として anonymous FTP 公開している．

情報科学センター生田分室にあるワークステーションで稼働しているsendmailについては次のようなアクセス制限を設けている.

アクセス対象	制限	コメント
default	no	
133.26.*.*	no	133.26.*.* のIPアドレスは、SRI-NICより明治大学に割り振られたアドレス
133.26.138.*	yes	133.26.{138,142,146,160} * は情報科学センターの教育用ワークステーションに割り振られたアドレス
133.26.142.*	yes	
133.26.146.*	yes	
133.26.150.*	yes	
133.26.136.*	yes	133.26.136.* は情報科学センターの研究用ワークステーション、および、VP2200/10 UXP に割り振られたアドレス

これにより，情報科学センターに設置されている如何なるワークステーションに対しても，センターの管理するマシン以外からSMTP接続を行なうことは出来ない.

4. まとめ

認証版sendmailは，SMTPクライアントからのアクセス要求に対して，細かい管理が行なえるようになった. また，クライアントの認証は，SMTP要求が発生した時点で／etc／sendmail. authファイル等がチェックされるので，SMTPアクセス制限テーブルのアップデートに対して，sendmailを再起動せずともダイナミックに対応できるようになった. また，SMTPアクセス制限テーブルはNISを用いて共有出来る為，保守が極めて容易になっている. これは，情報科学センターのように多数のマシンを抱えている部局では極めて重要なことである.

IPアドレスは，ネットワークに接続するマシン毎に，ユーザが手動で設定する. その為，IPアドレスによる認証にはおのずと限界がある. より確実なメイル発信者の認証には，公開鍵暗号方式，秘密鍵暗号方式を駆使した，ディジタル署名などに頼る必要がある.

A SMTP 接続拒否時の不通通知の例

```
Received: from mjugod01.isc.meiji.ac.jp by mjuserv.isc.meiji.ac.jp (4.1/91.10.12)
        id AA05989; Wed, 11 Dec 91 16:01:19 JST
Received: from mjuserv by mjugod01.isc.meiji.ac.jp (5.65+M1.1/meiji-isc-c.1)
        id AA28505; Wed, 11 Dec 91 16:05:06 +0900
Date: Wed, 11 Dec 91 16:05:06 +0900
From: MAILER-DAEMON@isc.meiji.ac.jp (Mail Delivery Subsystem)
Subject: Returned mail: Service unavailable
Return-Path: <MAILER-DAEMON>
Message-Id: <9112110705.AA28505@mjugod01.isc.meiji.ac.jp>
To: <ob00020@isc.meiji.ac.jp>
Status: R

   ----- Transcript of session follows -----
554 <hhat@mjugod01>... Service unavailable: Connection refused by mjugod01.isc.meiji.ac.jp

   ----- Unsent message follows -----
Received: from mjuserv by mjugod01.isc.meiji.ac.jp (5.65+M1.1/meiji-isc-c.1)
        id AA28503; Wed, 11 Dec 91 16:05:06 +0900
Received: from mjugod02.isc.meiji.ac.jp by mjuserv.isc.meiji.ac.jp (4.1/91.10.12)
        id AA05986; Wed, 11 Dec 91 16:01:17 JST
Received: by mjugod02.isc.meiji.ac.jp (4.1/meiji-isc-c.1)
        id AA09198; Wed, 11 Dec 91 16:05:25 JST
Date: Wed, 11 Dec 91 16:05:25 JST
From: ob00020@isc.meiji.ac.jp (H.Hattori)
Return-Path: <ob00020@isc.meiji.ac.jp>
Message-Id: <9112110705.AA09198@mjugod02.isc.meiji.ac.jp>
To: hhat@mjugod01
Subject: test

this is test mail.
mjugod02 -> mjuserv -> mjugod01
                    --- Maybe IP connection refused.
```

B /etc/sendmail.auth の例

```
#### definition file for hosts permitted to access ######
#<seigen-taishou>   <seigen-naiyou>     <comment>
#      <seigen-taishou>:   network address 133.26.0.0, 133.26.*.*
#                          host name       mjugod01
#                          host address    133.26.136.15
#                          default
#       <seigen-naiyou>:   Yes, yes, OK, ok
#                      :   No, no,
default          No          # default
133.26.*.*       No          # all meiji.ac.jp
133.26.136.*     yes         # {samba*|musc}.isc.meiji.ac.jp
133.26.138.*     yes         # {polka*-1|tango*}.isc.meiji.ac.jp
133.26.142.*     yes         # {polka*-2}.isc.meiji.ac.jp
133.26.146.*     yes         # {waltz*-1}.isc.meiji.ac.jp
133.26.150.*     yes         # {waltz*-2}.isc.meiji.ac.jp
133.26.144.3     yes         # bolero01.isc.meiji.ac.jp
#### end definition ########################################
```