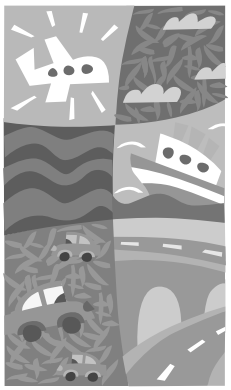


モバイルは今

認証付きメール送信

楯岡 孝道
電気通信大学 tate@cs.uec.ac.jp

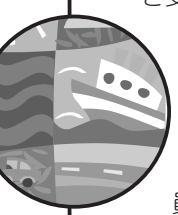
外出先などで，ダイアルアップ接続するISP（Internet Service Provider）ごとにメールアドレスが変わってしまい，困ることはないだろうか．携帯電話系のメールを常用する向きもあろうが，画面の狭さや添付ファイルの扱いの困難さから，業務用メールは当面パソコンのものがメインだろう．

未承諾広告メール（以下 SPAMメール）が社会問題化し，SPAMメールの送信者や中継者には厳しい目が向けられるようになっている．各ISPがダイアルアップユーザのために用意する送信用メールサーバでも，SPAMメールの中継に不正利用されないよう，一般に会員以外の使用を禁止している．そのため，IP接続に利用するISPがメールサーバのそれと異なると，しばしばメールアドレスも変えざるを得なくなる．これはIP接続に利用するISPと，メールアドレスが強く結びつけられているためである．

このような結びつきは，送信用メールサーバが会員を識別するための認証方法によって生じる．今回は送信用メールサーバがユーザ認証を行う方法について紹介する．

●

ISPの送信用メールサーバは，会員が送信するメールを受け付け，それを宛先の受信用メールサーバまで届ける機能を持つ．メールの受付には，多くの場合SMTP（Simple Mail Transfer Protocol）が利用される．従来のSMTPにはユーザ認証機能がないため，SPAMメールの中継に利用されないためには，会員からの送信要求であることを識別する何らかの機構が必要となる．



最も単純で広く用いられているのは，**図-1** のAの計算機のような，ISP内のIPアドレスのみに接続を限定する方法である．この方法は確実に会員のみに限定できるが，Bからのように，会員が他のISPから接続した場合には，それを拒否してしまう．このため，ISPごとに，そのISP用のメールアドレスから送信する必要がある．

場合によってはIP接続しているISPの送信用メールサーバを利用して，他のISPのメールアドレスを送信者名として送信することも可能だが，このような利用形態はSPAMメールの送信者と区別しにくいため，これを禁止しているISPも多い．このようなISPからIP接続する場合，メールアドレスに対応した送信用メールサーバを利用する必要がある．

これを解決するアドホックな解がPOP before SMTPと呼ばれる方法である．この方法では，会員によるメール受信に用いられるPOP（Post Office Protocol）がパスワードによる個人認証を含んでいることを利用し，POPによる認証が成功したIPアドレスからは，一時的にSMTP接続を許可する．つまり，利用者はメールを送信する直前にPOPを利用した受信処理を行えば，どのISPからIP接続していても送信用メールサーバを使用できる．この方法はメールリーダ側の変更なしで利用でき簡便である．しかし，POPによる認証成功後どれだけの時間SMTP接続を受け付けるかがアドホックにしか決定できないほか，NAT（Network Address Translation）等によって複数の利用者が同一のIPアドレスを共有している場合には，会員以外の利用者にも送信用メールサーバを利用されてしまう危険性がある．

この問題を解決するために，SMTPの拡張としてRFC2554 で定義されたSMTP認証 は，SMTPの中での個人認証を実現する．SMTP認証では複数の認証方式が許されているが，代表的なCRAM-MD5 方式では，メールリーダは，サーバから提示された時刻情報を含むチャレンジに，共有鍵を加え，そのハッシュ値をユーザ名とと

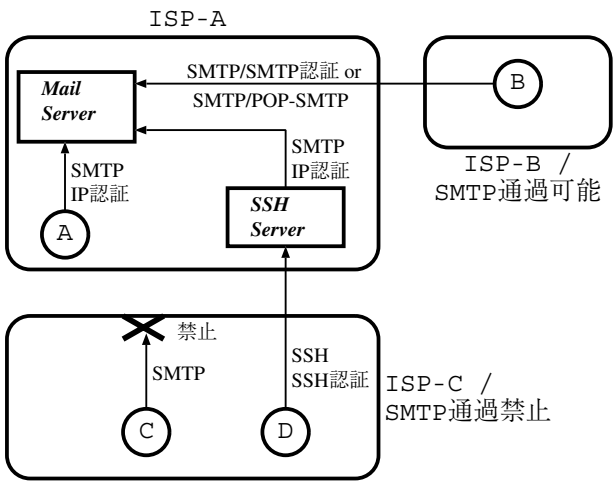


図-1　接続ISPとメールサーバとの通信方法

もにレスポンスとして送信する．サーバ側ではこのハッシュ値が正しいかどうかを検証する．この方式はSMTPのセッションごとに認証が可能になり，POP before SMTPのような問題はなくなる．また，送信用メールサーバを提供しているISPからIP接続する場合には認証なしで利用を許可し，他のISPから接続する場合には認証を求めるなど，段階的にも利用できる．POP before SMTPよりも確実な認証が可能なため，PDAに搭載されるものを含め，このSMTP認証に対応したメールリーダも増えてきた．

POP before SMTPやSMTP認証を使う場合，IP接続に利用しているISPのものとは異なる送信用メールサーバにメールリーダから直接SMTP接続を行うことになる．しかし，IP接続を提供しているISPの立場では，これはSPAMメールの送信者が，第三者のメールサーバを中継に用いてメールを送信する場合と区別がつきにくい．そのため，図-1のCのように，IP接続を提供するISP（図のISP-C）側から，他のISP（図のISP-A）宛のSMTP通信を禁止されてしまうことがある．

これを回避する少々変わった方法として，SSH（Secure SHell）のポート転送機能を用いる方法がある．ポート転送機能によって，SSHクライアント側のTCPポートを，あたかも送信用メールサーバのSMTP通信ポートであるかのように振る舞わせる．実際には図-1のDのように，SMTPのデータはSSH内の仮想回線を通してログイン先に送られ，ログイン先の計算機から送信用メールサーバに実際のSMTP接続が行われる．この方法ならば，ログイン先の計算機まではSSHの通信のみが許されればよい．また，ログイン先の計算機が送信用メールサーバを利用可能ならば，メールリーダやメールサーバの設定変更なしに利用できる．SSHログインが必要なためにISPが限定されるが，簡便に強力な認証とメールサーバまでの暗号化が可能なため，Mewなど一部のメールリーダへの組み込みが始まっている．

●

メールアドレスはネットワーク上での名前ともいえる．アドレスをTPOに合わせて使い分けるだけでなく，SPAMメールを避けるため，知らないメールアドレスからのメールを受信拒否するような利用者も増えてきている．また，今後の電子署名の普及に伴い，その識別子の1つとしての重要性も増すだろう．

従来の研究ネットワークとしてのインターネットは性善説によって発展してきたが，社会インフラとなり，その前提は完全に崩れてしまった．電子メールはインターネットで最も古い基本的なアプリケーションの1つだが，SPAMメールやウィルスメールなどに技術的に対処する必要が生まれ，認証などの改良が行われている．今回紹介した以外にも，TLS（Transport Layer Security）による通信内容の暗号化など，とりまく環境の変化に応じて，発展を続けている．

特にモバイル環境においては，いずれ，何らかの認証なしにはメールが送れなくなる日がくるだろう．あなたの電子メール環境は，生き残れるだろうか？

（平成15年9月1日受付）