経済学部と自宅を結ぶ暗号化経路の試み

PPP over TCP over SSH

安田伸一
yasudas@cc.saga-u.ac.jp

1. はじめに

自宅のインターネット接続を ISDN ダイヤルアップ接続からADSL 常時接続に替えました。“すぐに使えるインターネット”のまま、電話代を節約しようという目論見です。しかし、電子メールで手間を増やしてしまいました。

学外からインターネット経由で学内の電子メールを読む方法として、SSL で暗号化された webmailer を使うか、SSH などで POP や IMAP の通信を暗号化する、などの方法がありますが、使い慣れたメール・リーダを利用するには SSH を使うことになります。この方法では、POP や IMAP のポート・フォワーディングを行うために TeraTerm でログインするなどといった、事前の準備が必要となります。このため、大学の電子メールが“すぐに使えるインターネット”でなくなっていました。

また、ときどき、研究室の PC と ftp でファイル転送していますが、大学にダイヤルアップするときと違い、商用のプロバイダ経由では暗号化経路を用意しないと ftp を使いたくありませんよね。

そこで、佐賀大学LANと自宅LANを接続する暗号化経路を用意します。自宅と学内との間のすべての通信を自動的に暗号化経路を経由させることで、“すぐに使える安全なインターネット”を実現します。POP/IMAPも ftp もパスワード盗聴の心配なく、すぐに利用できます。また、暗号化経路さえ用意できれば、学部 LAN の NetBIOS over TCP/IP だって自宅から利用できます。

ただし、筆者が経済学部のネットワーク管理者である関係上、佐賀大学と自宅を結ぶ暗号化経路ではなくて、筆者が実験した経済学部と自宅を結ぶ暗号化経路を紹介します。

2. 全体像

ここで紹介する方法は、工藤智行「SSH の話（その4）」（FreeBSD サイト管理風雲録 第 19 回、Software Design 誌 2001 年 3 月号、技術評論社）で紹介されていたPPP over SSHの方法を、経済学部と自宅を結ぶ例に応用したものです。

まず、経済学部と自宅の二つのネットワークは、PPP over TCP で相互に通信します。PPP over TCP は FreeBSD などにインストールされている ppp（ユーザ ppp、iij-ppp）に組み込まれている機能で、シリアル・ポートの代わりに TCP/IP を経由して point to point のネットワークを作ります。そして、この PPP over TCP の通信を SSH のポート・フォワーディングで暗号化します。

経済学部 LAN は 133.49.52.0/22 のサブネットで、自宅 LAN は NAT の中にある 192.168.1.0/24 のサブネットです。今回、紹介する暗号化経路は、この二つのサブネットを接続します。ただし、単純な二つのサブネットの接続ではなく、二つの点で変則的です。まず、自宅 LAN がプライベート・アドレスで構成されているので、暗号化経路の出口も NAT を経由してアドレス変換を行います。したがって、経済学部と自宅の二つのサブネットは、二つのネットワークが対等に接続されているというよりも、NAT 内に構成している自宅 LAN から経済学部 LAN にダイヤルアップ接続している構成になります。

もうひとつの注意点は、自宅 LAN と経済学部 LAN との間の通信のうち、SSH の通信だけは、現実のインターネットを経由した通信でなくてはならず、暗号化経路にルーティングできないことです。今回は、経済学部 LAN の中に SSH サーバを設置したので、このサーバを含まないIPアドレスの範囲だけが暗号化経路を経由するよう

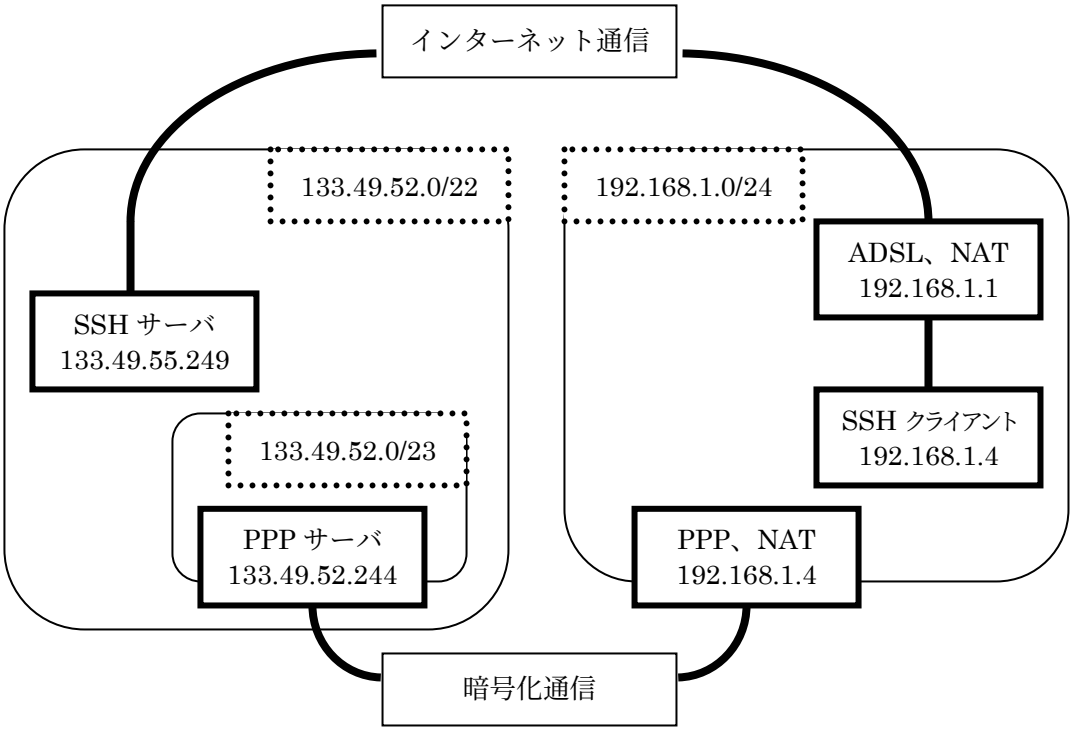

図 1　暗号化通信の構成

にルーティングしました。経済学部全体が暗号化経路を経由するように設定していない点で変則的です。

具体的には、次のように設定しています(図 1)。

- 経済学部側の SSH サーバは、133.49.55.249 のアドレスを持つ FreeBSD マシンです。
- 自宅側の SSH クライアントは、192.168.1.4 のアドレスを持つ FreeBSD マシンです。
- 自宅 LAN では、経済学部内の 133.49.52.0/23 のアドレスに対する通信が PPP にルーティングされて、PPP の NAT でアドレス変換された後、暗号化経路を経由します。ここには、SSH サーバの 133.49.55.249 が含まれません。それ以外の通信は、ADSL モデムにルーティングされ、ADSL モデムの NAT でアドレス変換されてプロバイダへ出て行きます。

3. 経済学部側の設定

経済学部側には、SSH で暗号化通信を受け付ける機能と、PPP over TCP で通信を受け付ける機能が必要となります。今回は、同一のパソコンで両方の機能を担当させました。

3.1 SSH の設定

SSH の設定は、特に必要ありません。通常の SSH 通信を受け付ける設定ができていれば、そのまま利用できます。

3.2 PPP over TCP の準備

PPP over TCP は、9010 ポートへの接続をきっかけにして PPP が起動するように inetd に設定します。9010 ポートを使うのは、お手本の丸写しです。

/etc/services にポート 9010/tcp の名前を登録し、/etc/inetd.conf に 9010/tcp ポートへの接続で PPP が起動するように指定します。その後、inetd に HUP シグナルを送信して、設定を更新します。

/etc/inetd.conf

```
ssh-vpn  stream  tcp  nowait  root  /usr
/sbin/ppp  ppp -direct ssh-vpn
```

/etc/services

```
ssh-vpn  9010/tcp  # PPP over TCP
```

カーネルに PPP が利用する tun デバイスが組み込まれていて、/dev/tun* が作成済みであることを確認しま

す。そして、/etc/rc.conf に gateway_enable="YES"を追加します。

/etc/rc.conf

```
gateway_enable="YES"
```

/etc/ppp ディレクトリの ppp.conf と ppp.secret に接続を受け付ける項目を作成します。ここでは、ssh-vpn ラベルで始まる設定でサーバ側の PPP の動作を指定しています。

ユーザ認証には、PAP を利用します。PAP はパスワードを平文で通信しますが、PPP の通信は暗号化経路を経由するので、PAP でも十分です。

point to point で利用する IP アドレスは、クライアント側で指定することにしました。

enable proxy でクライアントの通信の ARP 返答を代行させます。なお、よく似た設定の proxyall はクライアント側サブネットの ARP 返答の代行です。今回はクライアント側が NAT を使うので、proxyall は設定しません。

/etc/ppp/ppp.conf

```
ssh-vpn:
# PPP over SSH for VPN
 set ifaddr 0.0.0.0 0.0.0.0
 set timeout 0
 enable pap
 enable proxy
```

/etc/ppp/ppp.secret

```
YourPAPName  YourPAPPassword
```

4. 自宅側の設定

自宅側には、PPP over TCP で経済学部側と通信する機能と、この PPP over TCP を SSH で暗号化する機能が必要となります。こちらも、同一のパソコンで両方の機能を担当させました。

また、自宅側は、ユーザ shinichi で設定ができるようにしています。

4.1 SSH の設定

SSH によるポート・フォワーディングは、次のコマンドで実行します。

クライアント側マシンの 9010 ポートでの通信を経済学部側サーバ 133.49.55.249 の SSH サーバに転送し、SSH サーバではこの通信を localhost の 9010 ポートに転送します。つまり、自宅側マシンと経済学部側マシンとの間で 9010 ポートを相互に SSH で暗号化通信します。

ポート 9010 は、サーバ側で決めた ssh-vpn のポート番号です。ここで指定したポート番号が特権ポートではないので、このコマンドはユーザ権限で実行できます。また、ログアウトしても動作しつづけます。

```
> ssh -f -t -x -C -P -L 9010:localhost:9010
 133.49.55.249 /bin/cat
shinichi@133.49.55.249's password:
> netstat
 (中略)
tcp4  0  0  localhost.9010  *.*  LISTEN
```

4.2 PPP over TCP の設定

こちらも、カーネルに PPP が利用する tun デバイスが組み込まれていて、/dev/tun* が作成済みであることを確認します。同じく、/etc/rc.conf に gateway_enable="YES"を追加します。

/etc/rc.conf

```
gateway_enable="YES"
```

発呼側の PPP は、/etc/ppp/ppp.conf で設定します。

ユーザ shinichi で ppp の実行ができるようにするには、network グループへの登録と ppp.conf でのユーザ名の指定が必要となります。allow users は、ppp を実行できる network グループのユーザを指定します。default に指定しないと何もできません。各セクションでの指定も必要です。

ラベル warmhole は、お手本の丸写しです。

デバイス名に、ローカルの TCP ポート 9010 を指定します。

authname と authkey で、サーバで指定した PAP のユーザ名とパスワードを指定します。

set ifaddr では、point to point 接続に使う IP アドレスを指定しています。今回は、クライアント側で一元管理することにしましたので、ここで両方を指定します。

add! で、念のために ssh の接続経路を変更しないように、経済学部側 SSH サーバ 133.49.55.249 への接続は ADSL モデム 192.168.1.1 を経由するように指定します。正しく動作するようになったら、必要ありません。

add で PPP で通信する経済学部側のネットワーク 133.49.52.0/23 への経路を指定します。SSH サーバ 133.49.55.249 を含まないようにするため、本来の経済

学部のサブネット 133.49.52.0/22 は指定できません。

クライアント側のネットワークがプライベート・アドレスなので、PPP の NAT でアドレス変換します。これにより、サーバ側から見えるクライアント側のアドレスが一つだけになり、サーバ側で ifaddr 以外の経路指定が必要なくなりました。

/etc/ppp/ppp.conf

```
default:
 allow users shinichi

warmhole:
# PPP over SSH
 allow users shinichi
 set escape 0xff
 set device localhost:9010/tcp
 set dial
 set timeout 0
 set authname YourPAPName
 set authkey YourPAPPassword
 set ifaddr 133.49.52.245 133.49.52.244
 add! 133.49.55.249 192.168.1.1   # SSH
connection to eco
 add 133.49.52.0/23 HISADDR
 nat enable yes
 nat log yes
```

VPN を開始するには、PPP で dial warmhole を実行します。シェルから切り離してバックグラウンドで実行するには、-background オプションをつけます。

```
> ppp
Working in interactive mode
Using interface: tun0
ppp ON mimizuku> dial warmhole
ppp ON mimizuku>
Ppp ON mimizuku>
PPp ON mimizuku>
PPP ON mimizuku>
```

または、

```
> ppp -background warmhole
```

これで、自宅と経済学部の間の暗号化通信が開始されました。

4.3 自宅側サブネット内の経路指定

自宅側サブネット内の他のマシンでは、暗号化通信を行っている経済学部の一部 133.49.52.0/23 へ向けた通信を PPP マシンに振り向けてやることで、PPP マシンと同様に暗号化通信ができます。

例えば、Windows 2000 マシンでは次のようにして、再起動後も有効な経路を登録できます。

```
C:\WINDOWS>route -p add 133.49.53.0 mask 255.255.
254.0 192.168.1.4
C:\WINDOWS>tracert -d 133.49.53.1
  1     6 ms     3 ms     3 ms  192.168.1.4
  2   176 ms   125 ms   133 ms  133.49.52.244
  3   133 ms  1124 ms   131 ms  133.49.53.1
Trace complete.
```

5. NetBIOS over TCP/IP の設定

Windows が使っているファイル共有でネットワークを越えるホストと通信するには、WINS サーバを使うか、lmhosts ファイルに登録する方法があります。今回の暗号化通信では、自宅側に WINS サーバを用意できませんでしたので、Windows のファイル共有を行うマシンには、lmhosts ファイルを作成しました。

Windows 95/98 では、C:¥Windows に LMHOSTS ファイルを作成します。Windows 2000 では、C:¥WINNT¥system32¥drivers¥etc に LMHOSTS ファイルを作成します。いずれのフォルダにも、サンプルが LMHOSTS.SAM という名前で用意されているので、参考になります。

例えば、経済学部内の ntp サーバの NetBIOS 名が clock で IP アドレスが 133.49.52.5 のマシンは、次のように指定します。

C:\WINNT\system32\drivers\etc\LMHOSTS

```
133.49.52.5  clock  #PRE
```

6. むすび

上のような実験によって、経済学部内の電子メールを読むたびごとに TeraTerm でログインすることなく、すぐに利用できることができます。また、自宅内のどのマシンからも安全に経済学部の Windows マシンの共有ファイルにアクセスできるようになりました。

これを応用すれば、自宅から安全に学術情報処理センターのメール・サーバも安全に自宅から利用できるはずです。また、技術的には、利用が学内 IP アドレスに限られている附属図書館の百科事典「ネットで百科」などのサービスも自宅から利用できるように設定できるでしょう。しかし、これらの応用は、学術情報処理センターのセ

キュリティ運用方針や附属図書館の契約形態など、技術以外の問題を解決する必要がありますので、実験は慎重にする必要があると思います。

残されている課題として、通信速度とプロトコルのオーバヘッドがあります。

現在の設定では通信速度が遅く、Windows のファイル共有は ftp 代わり程度にしか利用できません。ping の平均応答時間は 130 ミリ秒台です。それでも、十分に便利さを感じていますが、うっかりファイル数の多いフォルダを表示しようとすると困ることになります。遅さの原因が仕組み自体なのか、マシンの性能不足なのか、また他に原因があるのかは、これから調べなくてはなりません。

今回は、PPP のパケットが TCP パケットで運ばれ、この TCP パケットが SSH の TCP パケットで運ばれています。TCP プロトコルのオーバヘッドを押さえるためには、PPP の通信を UDP に変更すれば、通信速度も向上できるかもしれません。今後、必要があれば調査しようと思います。