仮想プライベートネットワーク（VPN）の有効利用の検証

伊藤 康広、雨宮 尚範、原 祐一、野崎 公隆、鬼頭 良彦
工学系技術支援室　情報通信技術系

はじめに

依頼業務で増えてきていることに、LAN 内部で運用されている計算機の管理が挙げられる。通常 LAN 内部で運用される計算機は、セキュリティ対応のため、ファイアウォールなどの機器により外部からのアクセスが制限されている。従って、現場まで赴いて計算機を直接操作することになる。そこで遠隔操作により管理することを目的に、異なる LAN を同一ネットワーク上にあるように扱い、かつ LAN 間で安全に通信を行うことを可能にする技術である仮想プライベートネットワーク（VPN）について業務で利用できるか検証を行った。

1. 構築した VPN の概要

本研修ではインターネット VPN と呼ばれる VPN を構築した。大学内ネットワークをインターネットとみなし、学内の拠点間で通信を行うことを想定しているためである。VPN を構築するにあたっては、IPsec というプロトコルを使用して安全な通信を実現している。IPsec は IKE、ESP、AH などのプロトコルの組み合わせからなり、暗号化や認証、改ざん防止といった安全に通信するための機能を持っている。インターネット VPN とプロバイダが提供する IP 網を利用する VPN である IP-VPN と比較すると、一般に前者は通信品質や通信の安全性で劣るものの、安価に構築できるという利点がある。

2. ルータ単体の設定

VPN 構築のために、VPN サーバとしての機能を持ったヤマハ製のルータ RTX 810（図 1）を使用した。RTX 810 は IPsec が利用可能なルータとしては最も安価な製品の一つである。6 つまでの VPN 接続に対応しており、SOHO のような小規模なネットワークの構築に向いている。また、業務用の製品としては珍しく、Web ブラウザ上で基本的な設定ができるという特徴を持っている（図 2）。

図 1　RTX 810

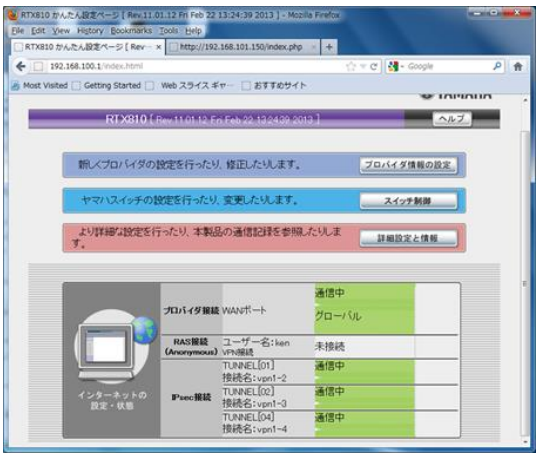

図 2　RTX 810 管理画面トップページ

管理画面からはルータの IP アドレスやルータ管理者に関する設定の他、VPN 接続のための設定などを行うことができる。

3. ルータと各種機器の 2 点間接続

Web ブラウザで閲覧できる管理画面から、個々のルータに対して設定を行った後、最も基本的な 2 点間 VPN 接続について検証した。暗号化する通信路の端点にある機器によって接続方法が異なるので、3 つに分けて検証結果を述べる。

1) ルータとルータの接続

構築したネットワークは図 3 のようなものである。

図 3 ルータとルータの接続

図 2 の画面から[詳細設定と情報]、[VPN 接続の設定]、[VPN 設定の追加]、[IPsec を利用したネットワーク型 LAN 間接続 VPN]とメニューを辿ることで、図 4 のような設定画面が表示される。ここで 2 つのルータに対して、四角い枠で囲った認証鍵と接続先の WAN（接続先の認証方法、ネットマスク）と LAN（経路情報の設定）について設定する。他は既定値でよいが、2 つの LAN で同じプライベートネットワークアドレスを用いてはならないことには注意が必要である。

図 4 ルータ間の VPN 接続における設定方法

正しく設定を完了すると管理画面のトップページに通信中と表示される。その状態になると ping コマンドによる PC 間の通信、リモートデスクトップ接続の他、接続先の LAN からのみ閲覧できるよう設定された管理画面が見られるということが確認できた。

2) ルータとモバイル機器の接続

iPad や Android を搭載したモバイル機器からルータへの VPN 接続について検証を行った。構築したネットワークは図 5 のようになる。接続するためのプロトコルに L2TP/IPsec を用いている。L2TP というのは 2 点間を結ぶ仮想的な直通回線を作るためのプロトコルである。L2TP 自体には安全な通信をするための仕組みはないので、IPsec と組み合わせて安全な通信を実現する。

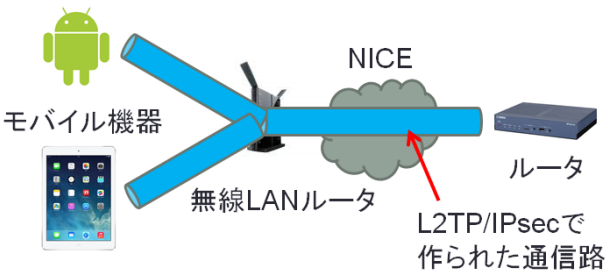

図 5 ルータとモバイル機器の接続

まずはルータの設定を行った。図 2 の画面から[詳細設定と情報]、[VPN 接続の設定]、[VPN 設定の追加]、[L2TP/IPsec を使用したリモートアクセス VPN サーバ (Anonymous)]とメニューを辿ることで、設定画面が表示される。その画面で接続ユーザ ID とそのパスワード、認証鍵を設定した。次にルータで設定した内容に合わせてモバイル機器を設定した。図 6 は iPad における設定画面のスクリーンショットである。この画面で、サーバ（接続先のルータの IP アドレス）、アカウント（ルータに設定済）、パスワード（ルータに設定済）、シークレット（ルータに設定した認証鍵）を設定した。

以上の設定を行った結果、モバイル機器でルータの LAN 側からしか閲覧できないよう設定したルータの管理画面を見ることができ、VPN 接続ができていることが確認できた。

図 6　iPad における VPN 接続設定

3)　ルータと PC の接続

図 7 のように PC からルータに接続するためには、PC に VPN 接続設定をするための VPN クライアントソフトが必要となる。今回はヤマハが公式に提供しているソフトウェア（YMS-VPN8）と、Microsoft の Windows が標準提供するソフトウェアの 2 つを用いて接続の検証を行った。ただし、後者のソフトウェアを利用した接続方法は、ヤマハがサポートしないため、非推奨の方法といえる。ここでは YMS-VPN8 を利用した方法について検証結果を述べる。

ルータはひとまず直前に紹介した 2)の場合と同様に設定する。YMS-VPN8 で設定するパラメータはルータに合わせて設定した（図 8）。

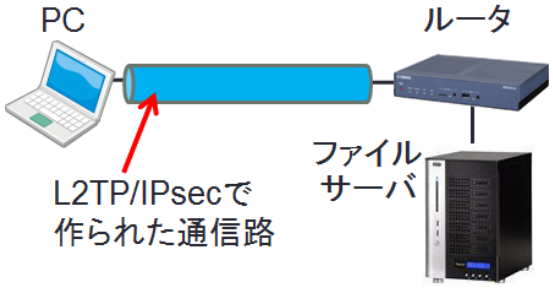

図 7　ルータと PC の接続

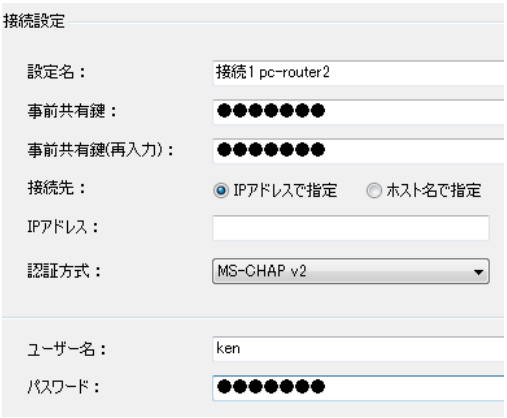

図 8　YMS-VPN8 の VPN 接続設定画面

このとき NAT トラバーサル機能を用いて VPN 接続をするため、ファームウェアを出荷直後のリビジョン Rev 11.01.04 から上げなければならなかった。NAT トラバーサルとは NAT や NAPT を使用している状況下において、IPsec を用いた通信を実現するための技術である。リビジョンは Web ブラウザの管理画面の操作で上げることができる。なお、NAT トラバーサル機能はリビジョンを上げるだけでは自動的に有効にならないので、コマンドを打って機能を有効にする必要がある。コマンドは、コンソ

ールあるいは Web ブラウザの管理画面から入力することができる。

その他にも、検証で使用した YMS-VPN8 のバージョン 1.0.0 では、L2TP における認証方式は MS-CHAP v2 にしか対応しておらず、ルータ側の認証方式は既定値からの変更が必要であった。また、IPsec の認証と暗号アルゴリズムを既定値から変更する必要もあった。表 1 はこれまでに挙げた変更すべき点を設定するために入力したコマンドである。

表 1　NAT トラバーサルを使った接続をするためにルータに入力したコマンド

```
ipsec ike nat-traversal 1 on ※NAT トラバーサルの有効化
nat descriptor masquerade static 200 4 192.168.100.1 udp 4500 ※4500 番ポートを開放
pp auth request mschap-v2 ※L2TP における認証方式の設定
※IPsec の認証、暗号アルゴリズムの変更。ブラウザ上の管理画面からでも設定可。
ipsec sa policy 101 1 esp aes-cbc sha-hmac
```

さらに、L2TP/IPsec を利用できるようにするために、PC 側ではレジストリを変更する必要があった。接続の検証に利用した Windows 7 のマシンでは、レジストリエディタを開き、HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥PolicyAgent 以下に DWORD（32 ビット）値の AssumeUDPEncapsulationContextOnSendRule を作成し、その値を 2 に設定することを行った。

この時点で Windows 7 の PC からファイルサーバに接続することはできたが、ファイルサーバへのファイルのアップロードが途中で止まる現象が一部の PC で見られた。その現象を解決するために PC の MTU（Maximum Transfer Unit）を調整した。MTU とは 1 回の転送で送るデータサイズの上限値である。ルータの MTU の既定値は一般的なネットワークを考慮して設定されているため変更したくなかったので、PC 側で管理者となり次のコマンドを入力して変更を行った（表 2）。

表 2　Windows マシンにおける MTU の設定

```
※VPN 接続の Idx を確認すると、53 と表示されている
C:¥Windows¥system32>netsh interface ipv4 show interfaces
Idx     Met         MTU          状態                名前
---  ----------  ----------  ------------  ---------------------------
  1          4275  4294967295  connected     Loopback Pseudo-Interface 1
 12          4265        1300  connected     ワイヤレス ネットワーク接続
 53            10        1400  connected     VPN 接続- ipsec
 11          4235        1300  connected     ローカル エリア接続
 13          4245        1300  disconnected  ローカル エリア接続 2
※確認した Idx の値に対して MTU の値を設定する
C:¥Windows¥system32>netsh interface ipv4 set interface 53 mtu=1210
```

以上の設定で PC からルータへの VPN 接続と、ルータ配下にあるファイルサーバへのファイルのアップロード、ダウンロードができること、ならびにファイルサーバの Web 管理画面を表示できることが確認できた。

4. VPN により安全な通信ができていることを確認する

VPN を利用する場合と利用しない場合とで、通信にどのような違いがあるかということを Wireshark というパケットキャプチャを用いて比較した。VPN を利用しない場合のネットワーク構成は図 9 のようになる。途中の経路でポートミラーリング（あるポートの送受信を他のポートにも流すこと）機能を有するハブを挟むことにより、左右の PC 間 の通信は Wireshark がインストールされた中央下部の PC 上で観察できる。今回は左右の PC 間で ping コマンドを流し、その通信の様子を観察した。

その結果、VPN 接続を用いない場合（図 9）では、図 10 の右下にあるように、ping request や ping reply と表示され、通信の内容が確認できた。一方、IPsec を用いてルータ間を暗号化した状態（図 11）では、ESP と表示され、ping コマンドを流していた通信の様子は見えないようになっていた（図 12）。ESP とはペイロード部に対しカプセル化を行い、通信を暗号化するプロトコルである。

これにより、容易に通信内容を解読されないようにするためには、暗号化を行う VPN を使うべきであるということが確認できた。

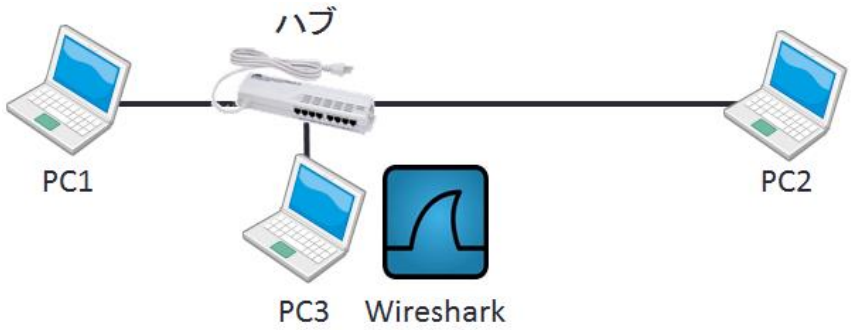

図 9　VPN を利用しないネットワーク

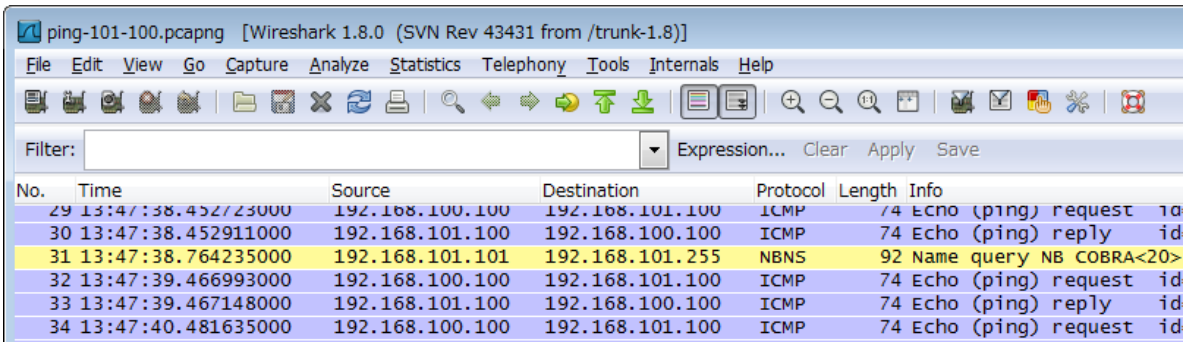

図 10　VPN を利用しない場合に Wireshark 上で ping コマンドを観察した結果

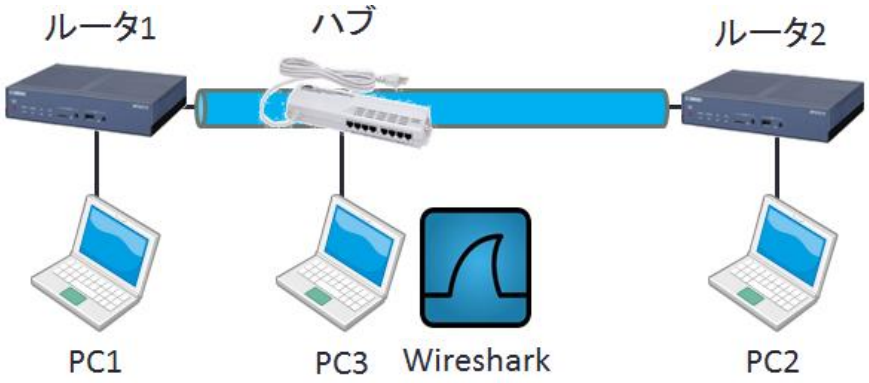

図 11　VPN を利用したネットワーク

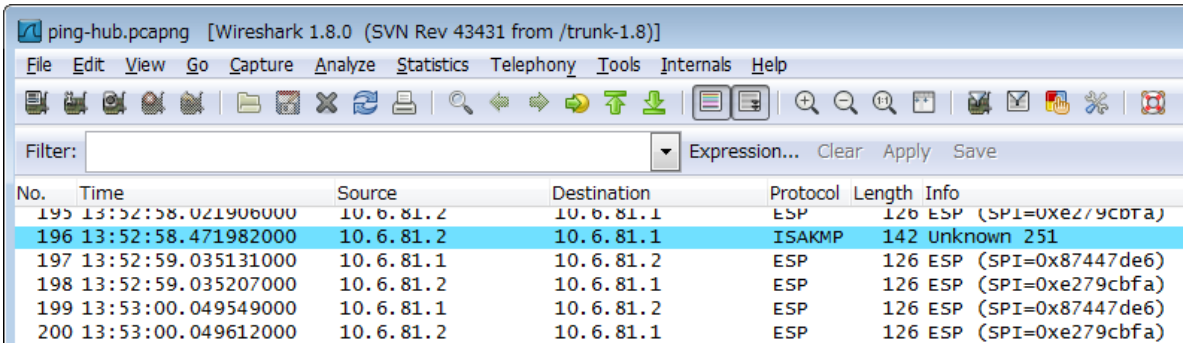

図 12　VPN 利用時に Wireshark 上で ping コマンドを確認した結果

5.　3 拠点間以上での接続

実際の現場では、複数の遠隔地にあるサーバを管理するということが考えられることから、3 拠点間以上でルータを用いて VPN 接続する方法について、2 種類のネットワーク構成で検証を行った。

1)　メッシュ型接続

メッシュ型接続では、各ルータがすべてのルータに対して VPN 接続の設定を行う。各ルータ間の設定は、3 の 1)で示した設定と同様に行えばよい。以下の図では 3 つのルータがあるので、各ルータで 2 つの VPN 接続の設定をすることになる。ルータが 3 つに増えても、すべてのルータ間で問題なく VPN 接続ができることを確認した。

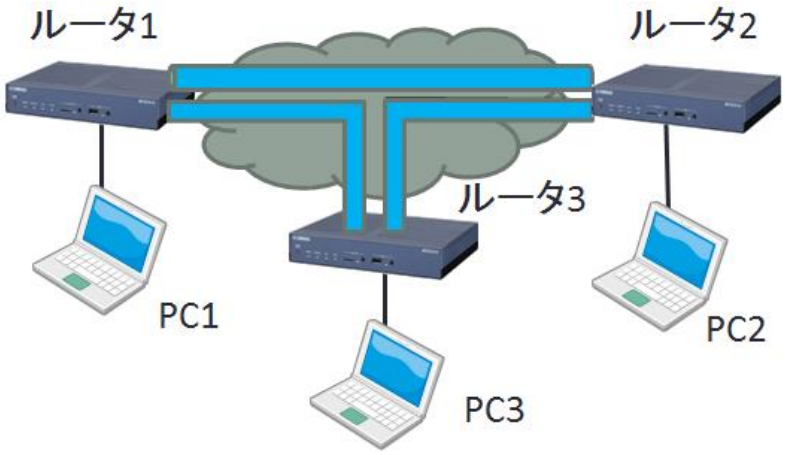

図 13　メッシュ型接続のネットワーク構成

2)　スター型接続

スター型接続は 1 つのルータが中央のルータとなり、他のルータ（以下子ルータと呼ぶ）は中央のルータにぶら下がるような接続形態である。検証の際には、より実際の現場に使われる形式に近づけるため、工学部の建物内にルータを配置し、学内のネットワークを経由するようにしてファイルサーバへ接続するようにした（図 14）。中央のルータでは各ルータへの設定を 3 の 1)と同様に設定すればよいが、子ルータでは中央ルータへの接続の設定の他、接続したい LAN を経路情報に指定する必要があった（図 15）。図中にあるすべての PC から、ファイルサーバのファイル操作（アップロード、ダウンロード）ができることを確認した。

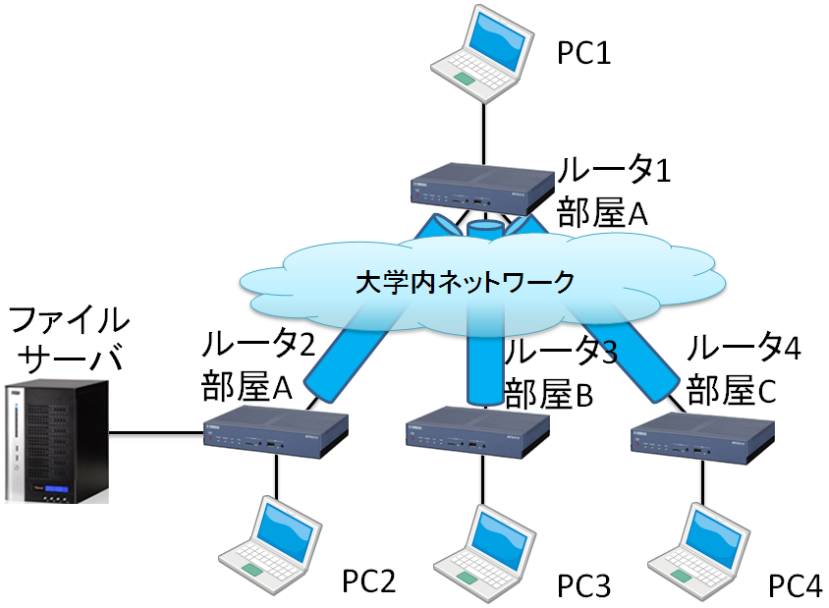

図 14　スター型接続のネットワーク構成

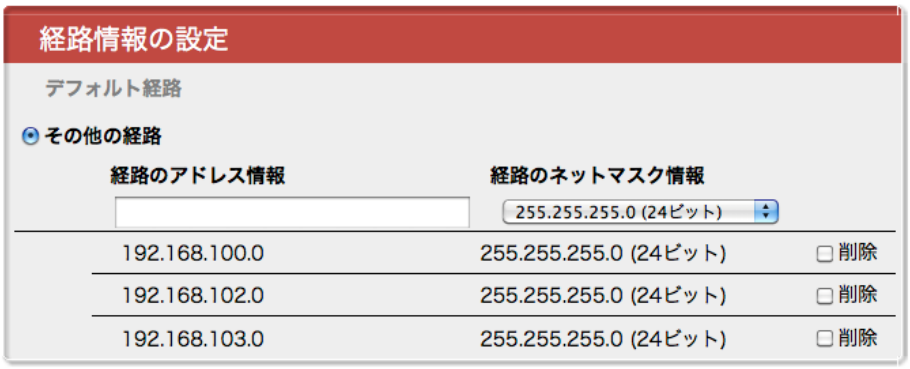

図 15　複数の LAN に VPN 接続するための経路情報の設定例

最後に、メッシュ型接続とスター型接続の特徴を表 3 にまとめておく。どちらを選択しても利点・欠点があるので、さまざまな観点を考慮して適切なネットワークの形態を選ぶべきである。

表 3　メッシュ型接続とスター型接続の特徴

特徴	メッシュ型	スター型
大規模化時の費用	高い（7 つ以上の VPN 接続が必要になったら、すべてのルータを上位機種に置換しなければならない）	安い（7 つ以上の VPN 接続が必要になったら、中央の機器のみを上位機種に置換すればよい）
ルータの負荷	ほぼ均一	中央の負荷が高くなる
設定の作業量	多い（すべてのルータで相互に接続するための設定が必要なため）	少ない（中央のルータと子ルータの間のみで設定が必要なため）
ルータ故障時の影響	どれが故障しても小さい	中央が故障したときはネットワーク全体が停止する

6. まとめ

本研修を通じて、VPN 対応ルータを用いてさまざまなネットワーク構成で VPN 接続ができることを検証できた。現地移動の負担を減らしつつ、安全な遠隔管理を行うことができるようになったと考えられる。また、VPN 利用時でもファイルサーバへの接続ができており、外出時にデータを PC に入れて持ち出さずに済むような設定方法があることを確認した。これにより、情報漏えい対策としても VPN が使えることが検証できた。

参考文献

1) ヤマハルータでつくるインターネット VPN ［第 3 版］、井上 孝司 著、毎日コミュニケーションズ
2) RTX 810 マニュアル（ http://www.rtpro.yamaha.co.jp/RT/manual/rtx810/Users.pdf ）