VPN を用いたネットワークの設定とセキュリティの検証

藤原冨未治*
*工学研究科・工学部技術部 電子・情報技術系

はじめに

サーバの管理・運用を行う場合、管理者が通常管理するサーバが集中化されておらず分散化して設置されている場合は、作業効率を考慮し Unix、Linux 系サーバの多くはネットワーク経由のキャラクタ環境でログインして作業を行っている。しかし Windows サーバでは GUI ベースでの管理が前提条件にあるためキャラクタベースのログイン環境では管理面での不都合が生じてくる。GUI 環境をネットワーク経由でリモート制御することも可能であるが、ファイアウォール下にある場合はファイアウォールを通過する作業が必要であることとセキュリティホールになりやすいためこの制御は困難な状況になる。このため現在の Windows サーバの管理は主に管理者がサーバが設置されている場所で作業しており、他のサーバに比べて運用面での不都合や作業効率の問題が指摘されていた。

そこで今回の研鑽では、VPN（Virtual Private Network）による仮想専用線によるアクセス方式を用いることによりファイアウォールの問題やセキュリティの問題を解決し、Windows サーバ管理を他のサーバと同じようにネットワーク経由で制御する方法の検証を行った。

１． VPN とは

VPN はインターネット等のネットワーク上に専用線を使用した場合と同じようなプライベートなネットワークを仮想的に構築することを言い、パケットの内容を VPN 用のプロトコルでカプセル化し仮想トンネルを通して別の拠点まで届け、そこで元のデータを取り出してネットワーク上に再送信している。VPN は、IP と TCP/UDP 層レベルで実現する技術であり、 VPN による仮想トンネルによって通信が行われている。これ以外の部分は、通常の TCP/IP ネットワークと全く同じように機能する。既存の TCP/IP ネットワーク において、ルータを介して複数のネットワークを接続するのと同じように、ネットワークを VPN 対応装置に接続するだけである。VPN 対応装置は、仮想的な通信トンネルをインターネット上に構築し、LAN 側から送信されたパケットを、トンネルを通じて目的のネットワークへ届け、逆方向もまた同じようにトンネルを通ってパケットの受信が行われる。

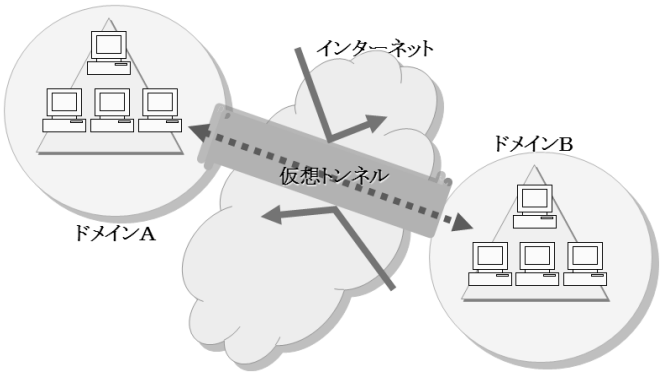

図 1．VPN の概念

仮想トンネルを構成するのには VPN 用にハード構成された専用ルータを使用する場合や、WindowsServer のソフトとして組み込まれている RRAS（Routing Remote Access Service）を利用する場合等がある。

２．VPN の種類

インターネットで使用する VPN の種類として以下の 2 種類の接続方法がある。

(1). リモート・アクセス VPN

ドメイン外部から接続するコンピュータとドメイン内の VPN 装置の間に暗号化などを施した安全な通信路として仮想トンネルを作成し、データの送受信を行う方式。VPN 装置は、外部からの接続要求に対してダイヤルアップ接続と同様なユーザー認証を行う(図 2)。

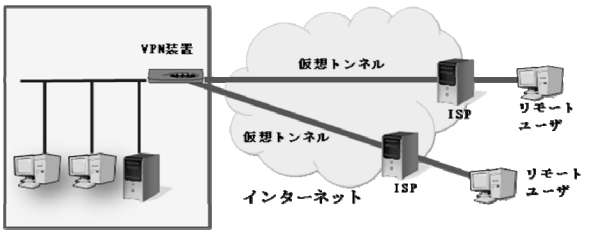

図 2. リモート・アクセス VPN

(2). LAN 間接続 VPN

2 つのドメイン間に設置された VPN 装置の間に仮想トンネルを作り、あたかも専用線でつないだかのように両ドメインの LAN 同士を接続する方式(図 3)。

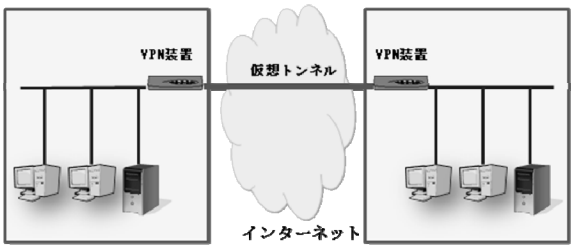

図 3. LAN 間接続 VPN

３．VPN の接続方法

VPN 接続に用いられる通信方法には主に次のようなものがある。

- PPTP

  Point to Point Tunneling Protocol の略、ダイヤルアップ接続で使われる PPP プロトコルを拡張して圧縮や暗号化を組み込んだもので、Windows 系 OS のシステムでよく使われている。

- IPsecVPN

  IP SecurityVPN の略､IP にセキュリティ機能を持たせたものでありトンネリングに L2TP（Layer 2 Tunneling Protocol）プロトコルを用い、暗号化に IPsec を用いる方法。

- SSL-VPN（OpenVPN、SoftEher）

  暗号化技術に HTTP 通信の暗号化技術である SSL（Secure Sockets Layer）を使用して接続する方法。

４．PPTP を用いた VPN 構成

今回は、VPN の接続に PPTP 機能を有したルータ（YAMAHA RT56v）を用い、リモート・アクセス通信と LAN 間接続のテストを行った。ルータの主な仕様を次に示す。

YAMAHA ブロードバンド VoIP ルータ　RT56v

- WAN インターフェイス：イーサネット 10/100BASE-TXx1 ポート(RJ-45)
- LAN インターフェイス:イーサネット 10/100BASE-TXx4 ポート､スイッチング HUB(RJ-45)
- LINE インターフェイス：2 線式(RJ-11)x1、PB,DP(10PPS,20PPS)
- アナログインターフェイス：2 線式(RJ-11)x3、PB,DP(10PPS,20PPS)自動認識
- 機能：ブロードバンド対応、ファイアウォール機能、インターネット電話機能、PPPTP による仮想プライベートネットワーク構築

この VPN ルータを用いたそれぞれの接続環境を以下に示す。

(1). PPTP によるリモート・アクセス

VPN ルータで WAN と LAN を区切り LAN 内部に Windows Server で構成されるドメインを配置し、WAN 側から WindowsXP クライアントでリモート・アクセスの検証をおこなった。クライアントでは、Windows 標準の PPTP 機能を用いた(図 4)。

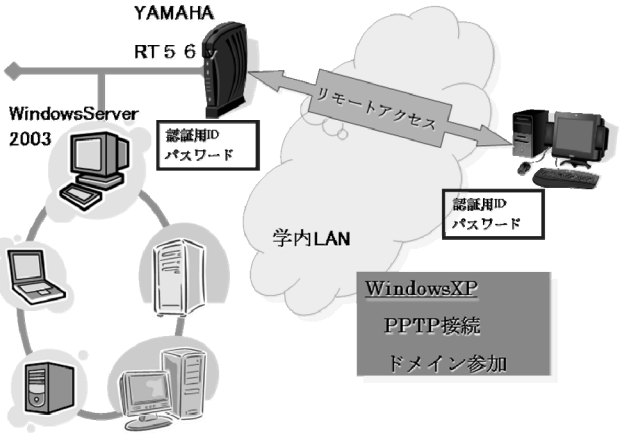

図 4. PPTP-VPN 接続 1

VPN ルータ側で VPN ネットワーク名、認証用 ID とパスワードを設定した後、クライアント側で VPN ルータの設定環境に合わせたものを設定（ネットワーク名、ID、パスワード等）し VPN 接続出来るかどうかの検証を行った結果、

- WAN 上のクライアントから LAN 内のローカルドメインマシンに対し LAN 内で設定されているローカル IP を指定して Ping を打った結果正常に応答が返ってきた。
- LAN 内の WindowsServer2003 が管理している Windows ドメインに WAN 上のクライアントが参加することが出来た。

(2). PPTP による LAN 間接続

次に LAN 間接続では、インターネット上に VPN ルータを 2 台設置し片方の LAN 側（Domain A）に Windows ドメインを置き、もう片方(Domain B)にはクライアントとして WindowsXP、Windows2000、Windows98 の各マシンを配置した(図 5)。まず VPN ルータで PPTP のサーバとクライアントの設定を施す必要があるため Domain A の VPN ルータをサーバ、もう一方の Domain B の VPN ルータをクライアントとして設定し、リモート・アクセスの時と同様にネットワーク名、認証 ID、パスワード等の設定を施した後接続できるかどうかの検証を行った。その結果、

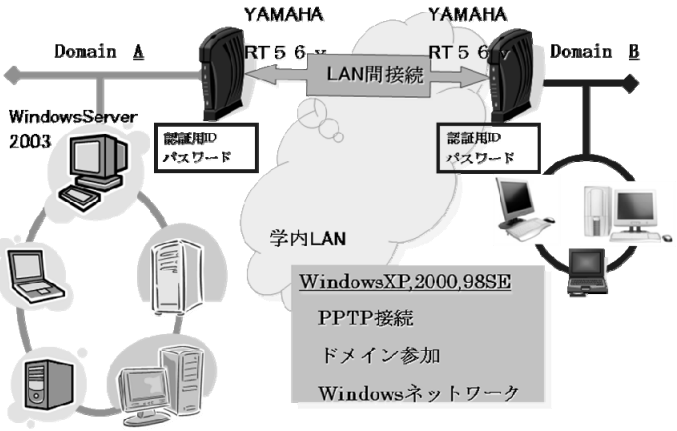

図 5. PPTP-VPN 接続 2

- Domain B の WindowsXP、Windows2000、Windows98 の各クライアントから Domain A 内のマシンのローカル IP に対して Ping を打った結果正常に応答が返ってきた。
- Domain B の WindowsXP、Windows2000 の各クライアントから Domain A の Windows ドメインに参加することができた。
- Domain B の WindowsXP、Windows2000、Windows98 の各クライアントから Domain A の Windows ネットワークでネットワーク名、コンピュータ名が表示されファイルアク

セスできることを確認した。

この結果からリモート・アクセス、LAN 間接続とも正常に接続が行われているということが確認できた。

５．セキュリティの検証

PPTP での LAN 間接続時における Windows マシン間のデータのやり取りを検証した。

まずアクセス側の WindowsXP マシンにキャプチャソフト導入し、接続状態を解析したのが図 6 である。ここでは、LAN 間に接続されている VPN ルータの MAC アドレスが表示され両ルータ間で接続が行われており、通信規格として IPv4、パケットの送り先 IP が VPN ルータクライアントから VPN ルータサーバへ指定されている。またプロトコル 47 で通信を行っているので PPTP での通信規格の GRE ヘッダでパケットがカプセル化されていることがわかる。

この結果から、VPN ルータで LAN 間接続されているデータはインターネット上を流れる際、通常のパケットではなく PPTP パケットして通信されていることがわかった。

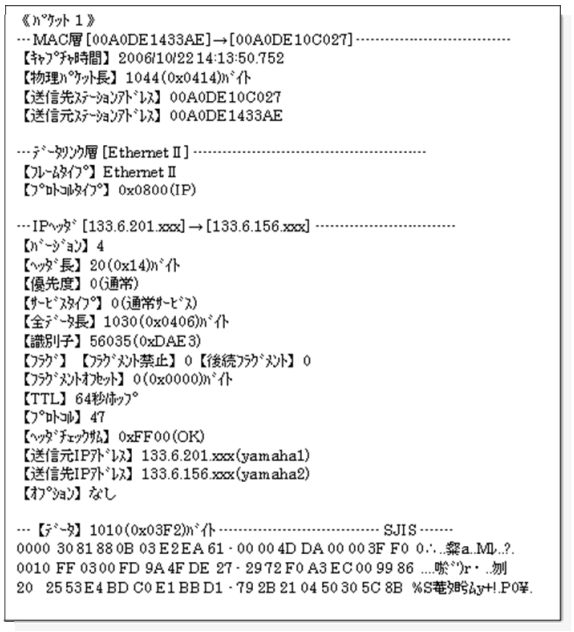

図 6. ネットワークキャプチャーデータ（例）

６．まとめ

本研鑽により VPN の基礎および構成等を理解することができた。また簡易機能ではあるが VPN ルータを用い実際に PPTP による VPN 接続を行うことにより、LAN 上のローカルドメインと WAN 上のクライアントとのリモート・アクセス通信が出来ることを確認しローカルドメイン内の Windows ドメインに参加出来ることも確認した。さらにドメイン間における LAN 間接続が出来ることを確認し、VPN ルータ間にレイヤースイッチが配置されている場合においてもレイヤーを超えて通信が出来ることが確認できた。これにより当初の目的であった Windows サーバのネットワーク経由での管理が他のサーバと同様に可能となり得ることが確認でき、運用面での問題の一解決手法となることがわかった。

尚、本研鑽は科学研究費（奨励研究）の補助を受けて実施した。

参考文献

[1] YAMAHA RT56v ブロードバンド VoIP ルータ 活用マニュアル

[2] 村島修一，“Windows Server 2003 実戦ガイド”，技術評論社

[3] 井上孝司，“Windows Server 2000 2003 ネットワーク管理ガイド”，秀和システム