# 3.1 ルーティングとリモートアクセスサービス

## 3.1.1 ルーティングとリモートアクセスサービスの概要

Windowsでは，異なるネットワーク間のルーティング（IP通信の転送）や，電話回線やインターネット経由でのネットワーク環境へのログオンを行うサーバー機能があります．この機能は「ルーティングとリモートアクセスサービス」と呼ばれ（本書では以下「RRAS」と呼びます），Windows 2000以降のすべてのオペレーティングシステム（OS）に標準的に実装されています．ただし，サーバーOSとクライアントOSでは内容が多少異なります．

Windows 2000 Server，Windows Server 2003，Windows Server 2008といったサーバーOSでは，RRASを構築・設定するための管理コンソールが標準的に用意されています．また，リモートアクセスに関する制限（接続数の制限）はWindows Server 2003では1,000クライアントとなっています．

一方，Windows 2000 Professional，Windows XP Professional，Windows Vistaといったクライアント OSでは，RRASを動作させるためのサービスはインストールされていますが，構築・設定するための管理コンソールがありません．ですから，クライアントOSで利用する場合，決められたGUIウィザードによる設定（着信接続についての設定など）か，コマンドによる操作で設定を行うことになります．

また，クライアントOSでのダイヤルアップやVPNの着信接続は1クライアントに制限されています．

本書では，Windows Server 2008のRRAS機能について述べていきますので，既存OSのRRAS実装についてはこれ以上述べませんが，Windows Server 2008ではRRASの細かい実装が変わったところがあるため，非常に便利になった反面，古いシステムのリプレースを考えている場合，注意が必要なケースもあります．

## 3.1.2 ルーティングとリモートアクセスサービスが提供する機能

RRASが提供するサーバー機能には，次のものがあります．

### ルーティング機能

コンピュータに接続された，二つ以上のネットワークカードに設定された，異なるネットワーク間にIP通信で発生するパケットを転送します（**図3.1**）．いわゆる，ネットワークルーター機能を提供します．二つのネットワーク間をダイヤルアップ接続でつなぐことも可能です．

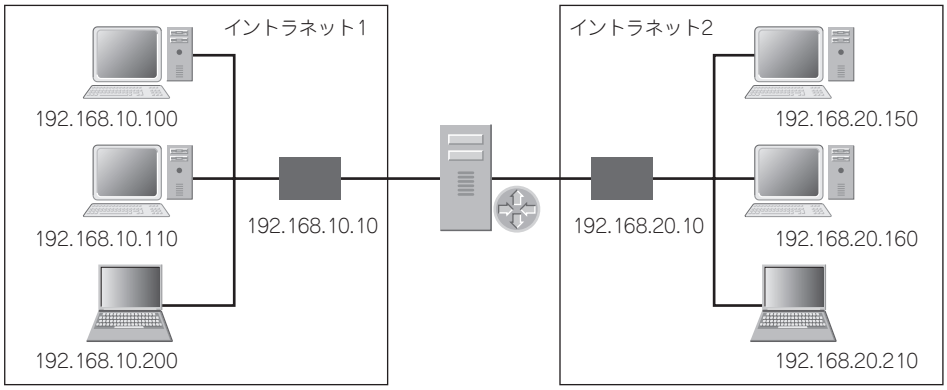


**図3.1　RRASの機能 ― ルーティング**

### ネットワークアドレス変換(NAT)機能

ネットワークを内部と外部に分け，内部ネットワークからのIP通信をほかのネットワークにルーティングし，ルーティングの際に内部ネットワークのIPアドレスを外部ネットワークのIPアドレスに変換して付け替えます(**図3.2**)．少ない外部ネットワークのIPアドレスを内部ネットワークのコンピュータが共用することができます．いわゆる，NATルーター機能を提供します．3.2節で後述する「仮想プライベートネットワーク」と組み合わせることも可能です．

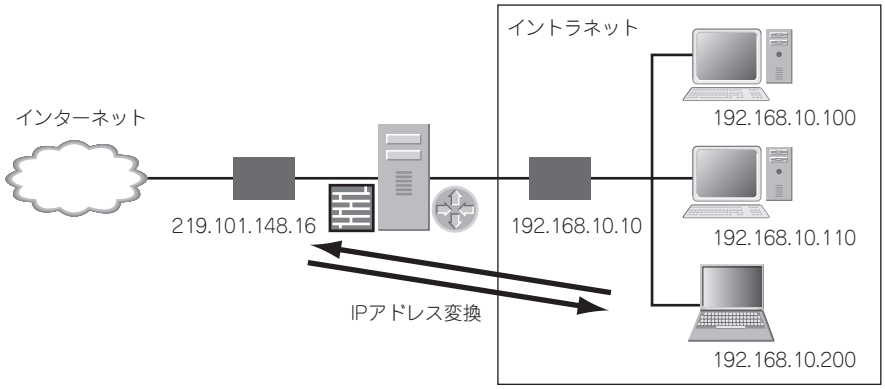


**図3.2　RRASの機能 ― NAT**

### リモートアクセス機能(ダイヤルアップネットワーク)

ダイヤルアップなどの電話回線経由で，物理的なネットワークカード(イーサネット)を使わずにサーバーにログオンして，自分自身をネットワークの一部として利用することができます(**図3.3**)．こういった機能一般をリモートアクセスといいます．電話回線を使うリモートアクセス接続はダイヤルアップネットワークと呼ばれ，電話回線用に設

計された通信プロトコルであるPoint to Point Protocol（PPP）を使って通信が行われます．PPPはイーサネットで使う通信プロトコル（IPプロトコル）を包み込んで送受信を行うことができるので，電話回線でつながれたクライアントとサーバーでは，LAN上で通信をしているようにふるまうことができます．

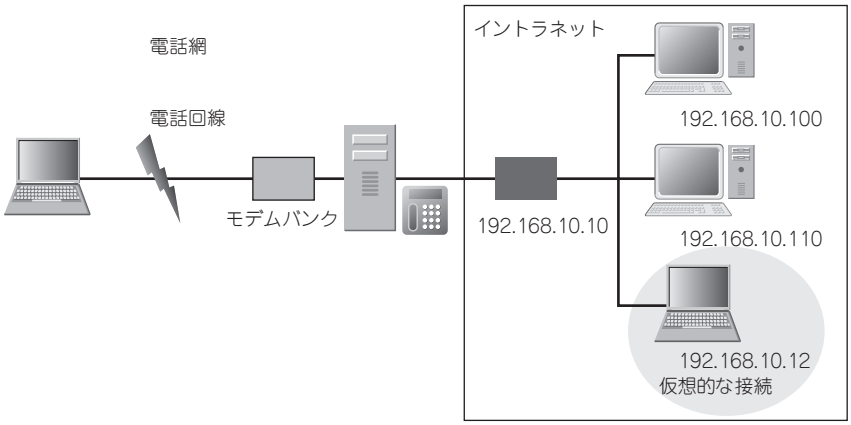


**図3.3　RRASの機能 ― ダイヤルアップネットワーク**

ダイヤルアップネットワークでは，モデムやISDN設備といったハードウェアを介して，電話回線またはISDN回線で通信のやり取りが行われます．電話回線のみを利用するため盗聴の危険がインターネットほどはないので，データの暗号化を行わないで通信を行うことができます．ダイヤルアップネットワークの認証には，PAP（Password Authentication Protocol）といった平文パスワードを送るものや，MS-CHAP（Microsoft Challenge Handshake Protocol）というチャレンジ（パスワードに不可逆な変換を加えた文字列）などを利用することができます．

### リモートアクセス機能（仮想プライベートネットワーク（VPN））

ダイヤルアップネットワークはサーバーやクライアントにモデムバンクやISDN設備といった追加ハードウェアが必要ですが，たくさんのダイヤルアップ接続を行いたい場合，専用のハードウェアの費用がかさんでしまうなどの問題があります．こういった問題に応えるため，リモートアクセスで使うPPPプロトコルをもう一度IPプロトコルに包んでしまうことで，インターネット経由でリモートアクセス接続を行うことができます．これを仮想プライベートネットワーク（VPN；Virtual Private Network）といいます（**図3.4**）．

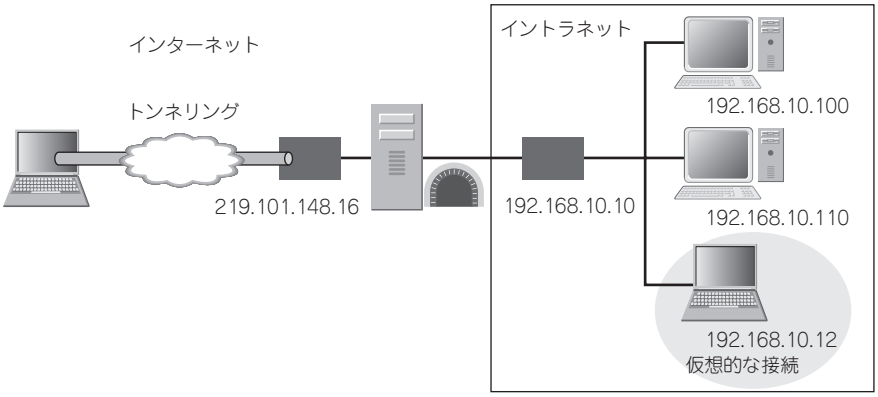


**図3.4　RRASの機能 ― VPN**

この機能を実現するのがトンネリングプロトコルで，PPTP（Point to Point Tunneling Protocol）やL2TP（Layer 2 Tunneling Protocol）が利用されます．Windows Server 2008では，これらのプロトコルに加えて，新しくSSTP（Secure Socket Tunneling Protocol；セキュアソケット トンネリングプロトコル）というプロトコルが利用できます．

VPNでは，通信内容のすべてがIPパケットとしてインターネットを通過するため，かんたんに盗聴傍受されてしまいます．そのため，必要なデータは必ず暗号化させて送受信させます．PPTPやL2TP，SSTPそれぞれが異なる方法で暗号化と復号（暗号を元に戻す）を実装しています．

またVPNでは，外部のクライアントが1台1台ネットワークに接続にいくリモートアクセスVPNが多く使われますが，異なるネットワーク間をインターネット経由でLANのように接続するといった使い方（例えば専用線に似た使い方）もとることができます．これをルーター間VPNと呼びます（**図3.5**）．

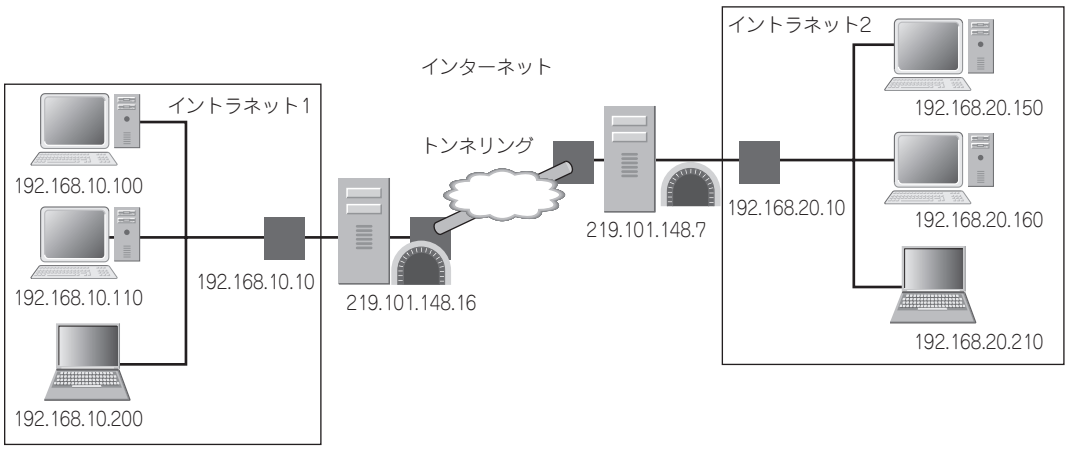


**図3.5　RRASの機能 ― ルーター間VPN**