実践的セキュリティ対策法

Windows 2000をルータにしてファイアウォールを構築してみる

Special Feature

吉田かおる　*text by Yoshida, Kaoru*
日本電気株式会社
Eラーニング事業部

「ファイアウォールさえ導入すればセキュリティは万全」という誤解は、ここ数年で解消されはじめたはずだ。もちろんこの“誤解”の一番大きな点は「さえ導入すれば」の部分である。あくまでもファイアウォールは導入されていて当然と思う方がいい。では、ファイアウォールをどのようにして構築すればよいのか。手慣れたOSで構築できる方法はないのだろうか？　本稿では、Windows 2000を使用して、セキュアなファイアウォールの構築方を詳解してゆく。

はじめに

ファイアウォールとは特定の製品を表わす言葉ではなく、あくまで概念です。よって、ファイアウォールを構築するということは、さまざまなセキュリティ対策のためのハードウェアやソフトウェアを組み合わせていくことを指します。本稿ではWindows 2000のパケットフィルタリング機能といくつかのセキュリティツールを組み合わせて、ファイアウォールを構築していく方法を紹介します。

今回、想定するケースは、スモールオフィスや個人事務所などの小規模ネットワークにおけるファイアウォールの構築です。社内ネットワークは、ADSLや光ファイバなどによる常時接続でISPに接続されていることを前提しています（図1）。なお、ファイアウォールの構築では、専用のファイアウォール製品を利用することもできますが、その基本を理解していただくために、あえて、Windows 2000が標準で実装するRRAS（Routing and Remote Access Service）を使用しています。

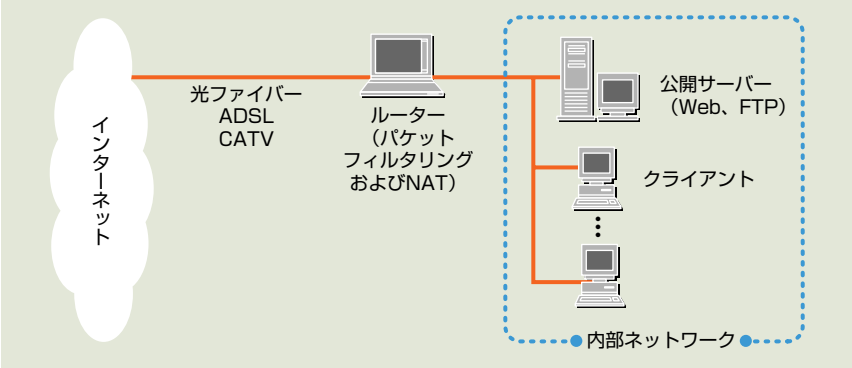
基礎知識編

まず、はじめにWindows 2000を今回のファイアウォール構築の中心であるパケットフィルタリングルーター（以後、ルーター）として利用するメリットを紹介します。また、Windows 2000のソフトウェアルーターであるRRASの概要も合わせて紹介します。Windows 2000をルーターとして利用するケースはまだあまり多くありませんが、このメリットに魅力を感じる方もいらっしゃると思います。

ルーターとしてWindows 2000を利用するメリット

現在、ADSLや光ファイバなどの常時接続のためのルーター（ブロードバンドルーター）が低価格で販売されています。また、Linuxと各種ソフトウェアを組み合わせることで、コストをかけず

図1：今回、想定するネットワーク構成



にルーターを構築することも可能です。つまり、ルーターの選択肢は数多くあるわけです。その中でWindows 2000をルーターとして採用するメリットとは何でしょうか？　それについてまとめてみました。

①使い慣れたOSだから

設定ミスや知識不足により、適切なセキュリティ対策が施されていないルーターはとても危険です。よって、使い慣れたOSを利用する意義は大きいと言えます。使い慣れたOSであれば、セキュリティホールの対処から運用時の注意事項まで把握しやすいでしょう。

②将来的な拡張が可能だから

RRASによるファイアウォール構築に対して限界を感じた場合は、すぐにその機能を拡張できます。たとえば、RRASにフリーウェアやシェアウェアのロギングツールを追加したり、よりレベルの高いセキュリティを求めるなら、Check Pointの「FireWall-1」やマイクロソフトの「Internet Security and Acceleration Server（ISA）」などの専用ファイアウォール製品を導入することもできます。この時、RRASで構築したネットワークインフラを変更する必要はほとんどありません。

③UPnPをサポートしているから

プライベートだけでなくビジネスの分野でもWindows Messengerがよく利用されています。しかし、Windows Messengerによる音声チャットやビデオチャットは、その通信手順が複雑なため、通常のルーターではサポートされておらず、サポートを表明したメーカーでもまだ、実際に製品を出荷しているケースは少数です。しかし、Windows 2000のRRASは、UPnP（Universal Plug and Play）をすでにサポートしているため、これらのサービスを容易に利用することができます。

RRASとは何か？

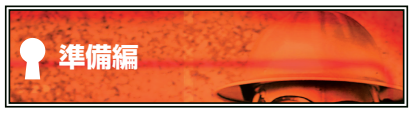
RRAS（Routing and Remote Access Service）は、その名前の通り、Windows 2000 Serverをルーターとして、またはリモートアクセスサーバーとして運用するためのサービスです。Windows 2000 Professionalにもそのサブセットが用意されていますが、Microsoft管理コンソール（MMC）が用意されていないなど一部の機能が削られています。Windows 2000 ServerのRRASでは次のサービスを提供しています。

①ルーターとしての機能

複数のネットワークアダプタを実装したマルチホームのWindows 2000をルーターとして構成することができます。この時、ルーティングプロトコルとして、RIPv2およびOSPFをサポートします。また、モデムやISDNのTA（ターミナルアダプタ）を使ったダイヤルアップ接続もサポートし、ダイヤルアップルーターとして使用することもできます。

②リモートアクセスサーバーとしての機能

リモートアクセスサーバーとして、モデムやTAを使ったリモートアクセスを受け付けることができます。また、VPNサーバーとしての機能も充実しており、IPSec、PPTP、L2TPによるインターネットを介したリモートアクセスも受け付けることができます。さらにRADIUSクライアントとして動作し、リモートアクセスの認証を、RADIUSサーバーで集中管理させることもできます。なお、Windows 2000には、別途、RADIUSサーバーとして、IAS（Internet Authentication Service）が用意されています。



それでは、ルーターとして使用するコンピュータにWindows 2000をセットアップしていきましょう。ルーター専用機であれば、それほど高いパフォーマンスは必要ありません。Windows 2000が稼動すれば多少古いコンピュータでも大

丈夫でしょう。また、常時接続ための多くのルーターにはネットワークアダプタが最低2枚必要ですが、トラブルを減らすために、最初は1枚のネットワークアダプタを挿した状態でインストールを行ないます。インストールの終了後、もう1枚のネットワークアダプタを追加します。

①Windows 2000をインストールし、基本的なセキュリティ対策を行なう

まず、Windows 2000をインストールします。今回のケースでは、ルーターがインターネットに露出するため、特に厳重なセキュリティ対策が必要となります。パーティションはNTFSでフォーマットし、アクセサリやユーティリティ、ネットワークサービスなどのWindowsコンポーネントはすべて削除します。インストール後には、最新のサービスパックを適用します。また、サービスパックの提供後に公開された修正モジュールも必要なものはすべて適用してください。この時、修正モジュールをまとめたセキュリティロールアップパッケージを利用すると修正モジュールの適用がかなり楽になります。最後に、administratorのパスワードを複雑なものに変更し、監査の設定を行ないます。これで、基本的なセキュリティ対策は終了です。

②ネットワークアダプタを追加する

続いて、2枚目のネットワークアダプタを追加します。Windows 2000ではプラグアンドプレイによりネットワークアダプタは自動的に識別され、必要なドライバがインストールされます。もし、標準でサポートされていないネットワークアダプタであればダイアログボックスの指示に従い、添付のFDやCD-ROMからドライバをインストールしてください。なお、Windows 2000がサポートするネットワークアダプタの枚数には制限がありませんので、スクリーンドサブネットを構築する場合はさらに3枚目のネットワークアダプタをインストールしてもよいでしょう。

また、ADSLによる常時接続の多くは、ユーザーの認証やIPアドレスの配布にPPPoE（Point-to-Point Protocol Over Ethernet）が使用されているため、PPPoEソフトウェアが必要となります。たとえば、NTTのフレッツADSLでは、「フレッツ接続ツール」という名前でPPPoEソフトウェアを配布しています。必要な場合はPPPoEソフトウェアもインストールしてください。これでネットワークのインフラが整いました。

③ネットワークアダプタに名前を付ける

次に、「コントロールパネル」から「ネットワークとダイヤルアップ接続」をダブルクリックし、ルーターとして運用するために必要なネットワークアダプタの設定を行ないます。「ネットワークとダイヤルアップ接続」には、接続アイコンがいくつか作成されています。このアイコンには、ネットワークアダプタを追加した順に「ローカルエリア接続」、「ローカルエリア接続2」といった名前が付けられています。また、ADSLでは、PPPoEソフトウェアも接続アイコンとして登録されています。

これらの名前はRRASの設定画面に表示されるため、操作ミスに防ぐ目的から分かりやすい名前に変更しておきます。ここではインターネット側のネットワークアダプタ（ADSLでは、PPPoEソフトウェア）を「external」、内部ネットワーク側のネットワークアダプタを「internal」としています（図2）。

④ネットワークアダプタにIPアドレスを割り当てる

各アダプタにIPアドレスを割り当てていきます。ISPより与えられたグローバルIPアドレスは、「external」に割り当てます。合わせて「external」には、ISPのDNSサーバーのIPアドレスも割り当てます。これはDNSプロキシの機

図2：RRASでの操作ミスを防ぐためにネットワークアダプタを分かりやすい名前に変更

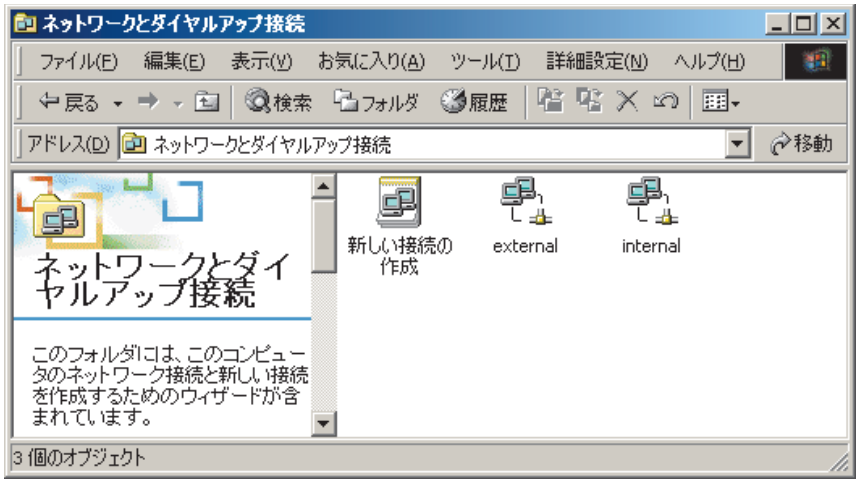


図３：インターネット側のネットワークアダプタから不要なサービスをアンバインドする

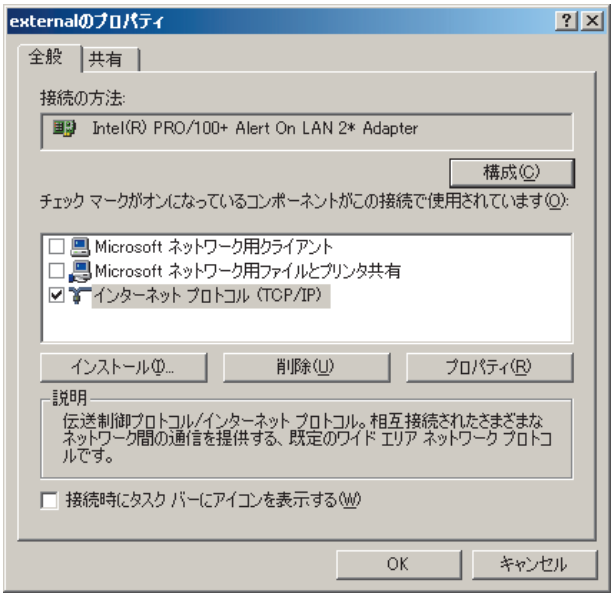
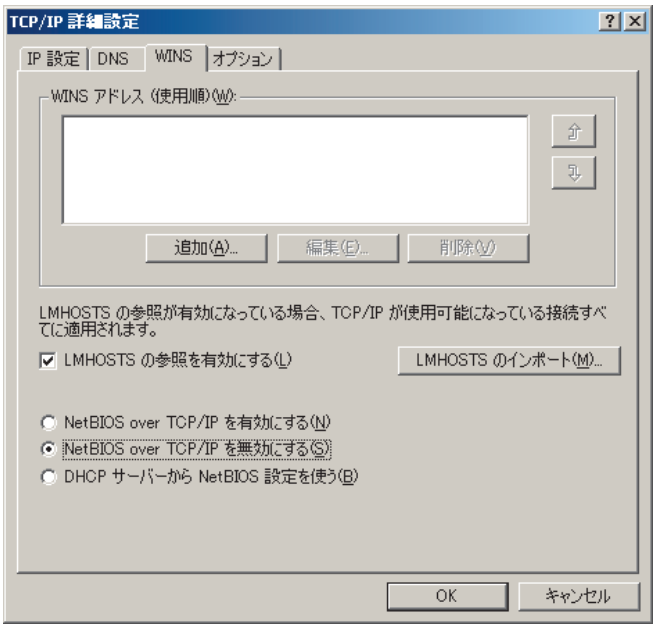


図４：インターネット側のネットワークアダプタでNBTを無効化する



能を利用する場合に重要です。また、「internal」には、プライベートアドレスを割り当てます。

⑤インターネット側のネットワークアダプタでNetBIOSを無効化する

Windows 2000のNetBIOSは攻撃に悪用されるケースが多いため、インターネット側のネットワークアダプタのプロパティでNetBIOSを無効化します。デフォルトでは「Microsoftネットワーク用クライアント」と「Microsoftネットワーク用ファイルとプリンタ共有」がバインドされたままになっていますので、チェックマークをはずします（図3）。

ただし、この状態では、NetBIOSのポートである139/TCP、137/UDP、138/UDPがオープンされたままなので、NULL接続などの問題が発生します。そこで「インターネットプロトコル(TCP)」-［プロパティ］ボタン-［詳細設定］ボタン-［WINS］タブから「NetBIOS over TCP/IPを無効にする」を選択して、NetBIOSを完全に無効化します（図4）。

RRASセットアップ編

これまでの作業で、RRASをセットアップするための準備が整いました。では、早速RRASをセットアップしてみましょう。なお、RRASはWindows 2000の標準コンポーネントとしてあらかじめインストールされているため、コンポーネントそのものの追加は不要です。RRASのセットアップウィザードを使って、RRASの構成と有効化を行ないます。RRASのセットアップウィザードは複雑で分かりづらいため、順を追って紹介します。

手順

①管理者アカウントでログオンし、「スタート」メニューから「プログラム」-「管理ツール」-「ルーティングとリモートアクセス」をクリックします。

②RRASの管理コンソールが表示されます（図5）。ただし、この時点ではRRASは有効化されていないため、管理コンソールは空っぽです。RRASを有効化するには、左ペインのホスト名（今回はRRASSV）で右ボタンクリックし、「ルーティングとリモートアクセスの構成と有効化」をクリックします。

③「ルーティングとリモートアクセスサーバーのセットアップウィザードの開始」ダイアログボックスが表示されます（図6）。［次へ］ボタンをクリックします。

④「標準的な構成」ダイアログボックスが表示されます。ここでRRASの用途を選択します。用途に応じて必要なプロトコルとサービスがセットアップされます（図7）。なお、選択され