FreeBSD ネットワーク構築（ファイアウォール編）

早川　正人*
名古屋大学工学部・工学研究科技術部

はじめに

雇用・能力開発機構中部職業能力開発促進センター（ポリテクセンター中部）で能力開発セミナーが、２００２年2月１４日、１５日の２日間開講された。今回は情報・通信系の「FreeBSD ネットワーク構築（ファイアウォール編)」コースに参加したので報告する。

１．FreeBSD４．４のインストール

FreeBSD は UNIX 互換 OS でフリーソフトウェアとしてソースコードを含めて無償で公開されており、FreeBSD プロジェクトによって管理されている。

インストールの前準備として、次の情報を整理しておく。

１）使用する PC のハードウェア構成の情報収集。

２）ハードディスクの容量、および使い方。(各ディレクトリの割り当て)

３）使用する IP アドレス、サブネットマスク等のネットワーク情報。

インストールは CD-ROM から起動し、インストールモードに通常は Standard を選択する。各項目の質問に答え、必要なところを入力して進めて行く。

また、インストール等でわからない所があれば以下の URL を参考にすると良い。

http://www.jp.freebsd.org/　　(FreeBSD Project Japan)

２．サーバーマシンのセキュリティレベルを上げる

以下にあげる項目に沿って、サーバーマシン自体のセキュリティレベルを向上させる。

１）コンソールからの root のログインを禁止する。また、仮想コンソールを使用不可にする。

２）マシンの Ctrl＋Alt＋Delete によるリブートを禁止する。

３）不要なデーモンを停止させる。(起動させない)

４）inetd と Tcpwrapper（tcpd）による限定されたクライアント接続の設定をする。

３．ファイアウォール構築に際しての前提構築

１）2 枚のネットワークインターフェースを適切に稼動させる。

/etc/rc.config ファイルに以下を記述する

ifconfig_xl0=”inet 192.168.6.1 netmask 255.255.255.0”

ifconfig_xl1=”inet 192.168.7.1 netmask 255.255.255.0”

２）起動時に IP 転送を開始する設定。

/etc/rc.config ファイルに gateway_enable=”YES” を追加する

３）デフォルトゲートウェイを追加する。

route add default 192.168.7.254

---

*電子・情報技術系

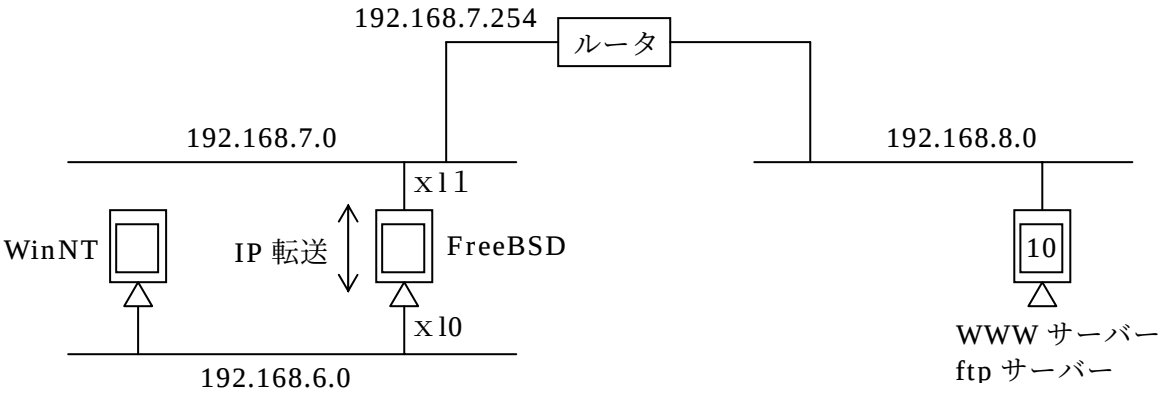

図１　ネットワーク構成

４．Delegate（PROXY プログラム）

「電総研」の佐藤豊氏が作成した一種の proxy プログラムで、非常に高機能で現在も細部の見直しやバージョンアップが続けられている。また、Windows 版も存在する。

インストールおよび起動

１）Delegate を http://www.delegate.org/ から ftp で取得しファイルを展開、解凍する。

２）作成されたディレクトリに移動し make コマンドを実行する。

３）実行ファイル delegated を /usr/local/sbin にコピーする。

４）Delegated の起動：/usr/local/sbin/delegated -8080 SERVER=http

５）自動起動：/usr/local/etc/rc.d/dlegated.sh （起動ファイルを作成する）

５．IPFW（フィルター型のファイアウォール ）

FreeBSD とともに配布されている IPFW は、カーネル内において IP アカウンティングとシステムを通過するパケットのフィルタリングを行うシステムであり、必要とする機能によってオプションをカーネルコンフィグレーションファイルに追加するためカーネルの再構築が必要となる。

IPFW の使用方法

・カーネルの再構築。

Kernel ファイルに ”Options　IPFIREWALL ”を記述する

・/etc/rc.local に firewall_enable=”YES ”を追加する。

・設定されているルールのリストを表示する。（/etc/rc.firewall などで設定）

ipfw list

・設定されているルールをクリアする。（全て通さない設定）

ipfw -f flush

・ルールを設定する。（全てを通す設定）

ipfw add allow ip from any to any

６．おわりに

今回のセミナーは２日間という短い時間で、予定していた研修内容の全てが実習出来なかったのが残念であったが、セキュリティ対策の重要さを改めて考えるうえで良い講習であった。