第10章

# iptablesによるパケットフィルタリング



2章のルータの項でも述べたように，Linuxではiptablesを使ってルータ機能の1つとされるパケットフィルタリングをします．

サーバを公開する場合，セキュリティ対策は欠かせません．そのために，不要なサービスを止めるなどの措置を施してきました．さらに，送られてくるパケットをカーネルレベルで選別するパケットフィルタリングを行います．

Vine Linuxではカーネル2.2系用のIPチェイン（用いるコマンドはipchains）と2.4系用のNetfilter（用いるコマンドはiptables）が用意されています．ここではNetfilterを利用します．また，これ以降，Netfilterという言葉でなく，コマンド名iptablesという言葉を用います．

設定するルールは，

1. ルータの役割を持たせる
2. Webサーバに誰でもアクセス可能にする
3. SMTPサーバに誰でもアクセス可能にする
4. 特定のサイトからSSHによるアクセスを可能にする
5. 内部LANからのアクセスはすべて許可する
6. 上記2～5以外はすべて拒否する

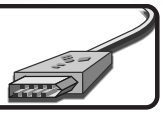
とします．

また，今回設定した環境は，インターネットに接続するインターフェースはeth1，LANのインターフェースはeth0としました．インターネットへの接続がPPPoEを利用するISPの場合は，上記「eth1」を「ppp0」などに読み替えてください．

実際のiptablesによるパケットフィルタリングルールは，つぎのサイト情報を大いに参考にさせていただきました．

**http://www.geocities.co.jp/SiliconValley-Bay/4893/adsl.html**

## 10.1 iptablesの概要



iptablesはパケットフィルタリングを行うツールです．パケットフィルタリングとは，パケットを通過させるか，破棄するかをパケットのヘッダーを見て判断するしくみです．

パケットフィルタリング/IPマスカレードはカーネルの仕事であり，iptablesは，カーネルにフィルタリング/IPマスカレードの細かい指示を行う道具です．

すなわち，iptablesを使えるようにするには，カーネルがパケットフィルタリングの機能を備える必要があります．そのために，iptablesを使えるように，カーネルを再構築する必要も出てきます．

iptablesの役割をまとめると，次の2つになります．

1. カーネルにパケットフィルタリングの指示を与える
2. カーネルにIPアドレス相互変換の指示を与える

ルータの役割を持たせるパケット処理とは，どのようなことをすればよいのでしょうか．ルータはネットワークを区切り，データのやり取りを行います．そこで必要なパケット処理をまとめると次のようになります．

1. グローバルIPアドレスとLANで用いるプライベートIPアドレスの相互変換
2. 外部からの必要なパケットを内部へ通過させ，不要なパケットは破棄
3. 内部からの必要なパケットを外部へ出し，不要なパケットは破棄

ネットワーク上を送受信されるデータには**図10.1**に示すような種々の情報が書き込まれています．iptablesはヘッダーを見て，許可・破棄・記録などの指示を与えます．

iptablesの特徴は，パケットフィルタリングのルールを実行するテーブルを持つことです．パケットフィルタリング専用のテーブル「filter」，NAT/IPマスカレード専用のテープル「nat」，ちょっと特殊なアドレス変換テーブル「mangle」です．それらのテーブルのイメージを**図10.2**に示します．

ICMP

| IPヘッダ | ICMPヘッダ | データ |
|---|---|---|

TCP

| IPヘッダ | TCPヘッダ | データ |
|---|---|---|

UDP

| IPヘッダ | UDPヘッダ | データ |
|---|---|---|

**図10.1◆送受信されるデータのパケット構造イメージ**