



## 境界と内部の間を制御する

前回も説明しましたが、この記事で扱っているサイトのネットワーク構成は図1のようになっています。実際にみなさんがネットワークを使うとき、まったく同じ環境ではないかもしれませんが、しかし、小さなネットワークでよく使われる典型的な環境だと思えます。

今回説明するフィルタリングの設定は、「境界ネット」と「内部ネット」の間でやり取りされるIPパケットを制御するものです。具体的には2つのネットワークを中継するPCルーターを使ってフィルタリングします。今回解説するパケットフィルタリングの知識は、インターネットとローカルネットワークを接続するルーターにも活用できます。

## 制御に使う情報は4つ

インターネットではIPパケットというデータのまとまりをやり取りしています。そのIPパケットのヘッダーには「送り元アドレス」、「送り先アドレス」、「プロトコル種別」(TCP、UDP、ICMPの区別)、そして「ポート番号」といった情報が入っています。IPパケットに対し、この情報を使ってアクセスの制限を加えようというのがパケットフィルタリングです(以下、文中では単にフィルタリングと呼びます)。

それでは、FTPやHTTPといったアプリケーションレベルの「プロトコル」を判断するにはどうすればいいのでしょうか? これは、TCPがUDPかというIPレベルのプロトコルの違いと、ポート番号で区別しています。

インターネットの通信プログラムはどのIPレベルのプロトコル(TCPやUDP)も、どのポート番号(0から65535番まで)も使うことができます。しかし、プログラムが勝手にプロトコルやポート番号を使ってしまうと、そのルールを知らないマシン同士はお互いに通信できません。

そこでプロトコルとポート番号の組み合わせは、インターネット全体の共通規約として決めておく必要があります。代表的なアプリ

# 実践 Linux セキュリティー講座

前回はパケットをフィルタリングするためのソフトウェア、「ipfwadm」のインストールまでで終わってしまいました。そこで、今回はパケットフィルタリングのためのルールを決めて設定するところまで解説します。ここまで終了すると、Linuxを活用したルーターによる保護の話は一段落です。

## 第5回 パケットフィルタリングを設定する

ソフトウェアコンサルタント すずきひろのぶ



ケーションレベルのプロトコルに関しては、IANA (ICANN) という組織が調整しています。その一覧は次のURLから入手できます。

**URL** <http://www.isi.edu/in-notes/iana/assignments/port-numbers>

Linux では代表的なプロトコルとポート番号の組み合わせが/etc/servicesに登録されています。

## 制御できることできないこと

パケットをフィルタリングするために使われる情報は、送信元および送信先アドレス、プロトコル種別、ポート番号です。この4つがわかれば、インターネット上のプロトコルとして定義されていない任意のプログラムのパケットもフィルタリングできます。

TELNETを例に取ると、フィルタリングによって次のようなパケットの制御ができます。

- ・TELNETのすべてのパケットを許可 / 拒絶する
- ・特定のアドレスから発信されたTELNETのパケットを許可 / 拒絶する
- ・特定のアドレス宛てのTELNETのパケットを許可 / 拒絶する

フィルタリングはIPパケットのヘッダーが持っている情報を使います。このため、パケットの中のデータ部分に基づいて、判断や制御を行うわけではありません。

たとえば、電子メールの中にウイルスが添付されているからといって、そのパケットだけをフィルタリングして排除することはできません。パスワードファイルを転送しているパケットだけをフィルタリングすることもできません。パケットの中にはユーザー情報がないので、ユーザー別によるフィルタリングもできません。

## サイトで何をするのが重要

どのプロトコルを通すかは個々のサイトで考える必要があります。このネットワークで

は、クライアントは次のサービスを使用するということにして話を進めます。

- ・インターネット上 (サーバーも含む) のウェブサイトにアクセスする
- ・サーバーからPOPで電子メールを取り出す
- ・電子メールを送る

ユーザーの電子メールは図1の「サーバー」が受け取ることにします。本来ならば、電子メールを送るときはサーバー経由で送るか直接送るかや、DNSはどこにあるのかなどを決めなければなりません。しかし、この記事ではフィルタリングだけに話を集中させたいので、あえて決めないこととします。

## 通すべきではないものもある

よく知られているプロトコルの中には、フィルタリングによってある程度制御したとしても安全性が低いものがあります。

まず、NFSやNIS (YP) といったプロトコルは通過させるべきではありません。これはRPCという仕組みをベースにしているプロトコルで、いろいろな問題が発生する可能性があります。

rloginやrshといった「rコマンド」と呼ばれるものが使っているプロトコルも通過させるべきではありません。「rコマンド」はユーザー

一認証が甘いので、ユーザーがセキュリティホールを作りやすくなっています。

Xウィンドウのプロトコルも通過させるべきではありません。接続認証が甘いのと同時に、トロイの木馬に使われる可能性があります。

どうしてもrloginやrsh、rcpといった機能が必要であれば、暗号システムを使ったSSH (Secured Shell) を代替として使います。SSHに関しては機会を改めて説明します。

通すべきではないプロトコルはほかにもたくさんあるでしょう。調べたところ、インターネット上で使うプロトコルとして正当に登録されているものは、約4600種類ありました。どんなプロトコルを通すべきかは多少なりとも考慮が必要です。

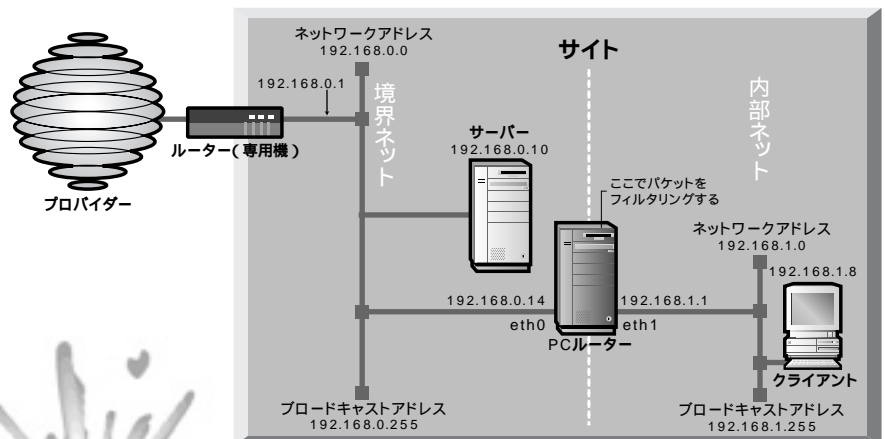
## 「何も通さない」から始める

フィルタリングを設定するのに、まずはすべてのパケットの通過を確実に停止させます。手順はPCルーターでリストのように実行します。すべてのパケットの通過を停止させるのは、フェイルセーフの考え方を取り入れているからです。この方法によって、明示的に示したプロトコルのみを通すことができます。

次に、必要に応じてプロトコルを通しますが、なるべく最小限にとどめておく必要があります。

今回の例で通すべきプロトコルは、次のも

図1 サイトのネットワーク構成







がすべて記録されます。ログは以下のようになります。

- 外から内に入ってきたIPパケットのログ  
/proc/net/ip\_input
- 内から外に出ていったIPパケットのログ  
/proc/net/ip\_output
- IPフォワーディングのログ  
/proc/net/ip\_forward
- IPアカウントに関するログ  
/proc/net/ip\_acct

このログはデータ列の記録なので、そのままではわかりづらくなっています。わかりやすく表示するには、ipfwadmの機能を使うといいでしょう。先にどのパケットを監視するかについてフィルターを指定します。ここで指定したフィルターが表示の対象になります(リスト④)。

## 起動時の設定をしておく

ここまではフィルタリングを手動で行ってきました。この方法では、PCルーターを再起動すると無効になってしまいます。そこでフィルタリングの設定をまとめたシェルスクリプトを作成し、起動時に実行させるようにします。まずリスト⑤のようなシェルスクリプトを作成します。このファイルを/etc/sysconfig/network-scripts/ifup-ipfilterというファイルとして保存します。

次に、/etc/sysconfig/network-scripts/ifup-postというファイルがありますので、このスクリプトの中にリスト⑥のような行を追加します(必ずexitより前に追加してください)。

## 完全な設定はこれから

これでフィルタリングの設定は一通り終わりました。あとは、使っている環境に合わせて設定して下さい。

今回は、ipfwadmについてさらに詳しく解説します。

### リスト③ フィルタリングの設定を確認する

```
$ /sbin/ipfwadm -F -l
IP firewall forward rules, default policy: deny
type  prot  source                destination          ports
acc   tcp   inside/24             dmz/24               1024: 65535 -> telnet
acc   tcp   inside/24             anywhere             1024: 65535 -> http
acc   tcp   server                inside/24            1024: 65535 -> smtp
acc   tcp   inside/24             dmz/24               1024: 65535 -> pop-3
acc   tcp   inside/24             dmz/24               1024: 65535 -> telnet
```

### リスト④ ログの表示の仕方

```
通過するすべてのTCPのパケットを記録
# /sbin/ipfwadm -A -i -P tcp -S 0.0.0.0/0 -D 0.0.0.0/0

内部ネットワークからのTELNETのパケットを記録
# /sbin/ipfwadm -A -i -P tcp -S 192.168.1.0/24 -D 0.0.0.0/0 23

ipfwadmでログを表示させる
# /sbin/ipfwadm -A -l
IP accounting rules
pkts bytes dir prot source                destination          ports
121  5054 i/o tcp  inside/24             anywhere             any -> telnet
```

### リスト⑤ /etc/sysconfig/network-scripts/ifup-ipfilter

```
#!/bin/sh
INSIDE=192.168.1.0/24 #変数設定
DMZ=192.168.0.0/24 #変数設定
ANY=0.0.0.0/0 #変数設定
USERPORT="1024: 65535" #変数設定

if [ ! -f $C ]; then
    ## ipfwadmがインストールされているかどうかのチェック
    echo "IP filter: ipfwadm not found" >&2
    exit 0
fi

##初期状態はすべての通信を拒否してフィルタリングを無効にする
/sbin/ipfwadm -F -p deny
/sbin/ipfwadm -F -f
/sbin/ipfwadm -l -f
/sbin/ipfwadm -O -f
## DNS (53)を許可
/sbin/ipfwadm -F -a accept -b -P udp -S $INSIDE $USERPORT -D $ANY 53
##HTTP (80)を許可
/sbin/ipfwadm -F -a accept -b -P tcp -S $INSIDE $USERPORT -D $ANY 80
##プロキシ (8080)を許可
/sbin/ipfwadm -F -a accept -b -P tcp -S $INSIDE $USERPORT -D $ANY 8080
##POP3 (110)を許可 (境界ネットワークから内部ネットワークのみ許可)
/sbin/ipfwadm -F -a accept -b -P tcp -S $INSIDE $USERPORT -D $DMZ 110
##SMTP (25)を許可
/sbin/ipfwadm -F -a accept -b -P tcp -S $INSIDE $USERPORT -D $ANY 25
exit 0
```

### リスト⑥ /etc/sysconfig/network-scripts/ifup-postの追加

```
FILTER=/etc/sysconfig/network-scripts/ifup-ipfilter
if [ -f $FILTER ]; then
    sh $FILTER
fi
```





## [インターネットマガジン バックナンバーアーカイブ] ご利用上の注意

このPDFファイルは、株式会社インプレスR&D(株式会社インプレスから分割)が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

<http://i.impressRD.jp/bn>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真の撮影者、イラストの作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元(株式会社インプレス R&D)、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D(当時は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接のおよび間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先

**株式会社インプレスR&D**

All-in-One INTERNET magazine 編集部

[im-info@impress.co.jp](mailto:im-info@impress.co.jp)