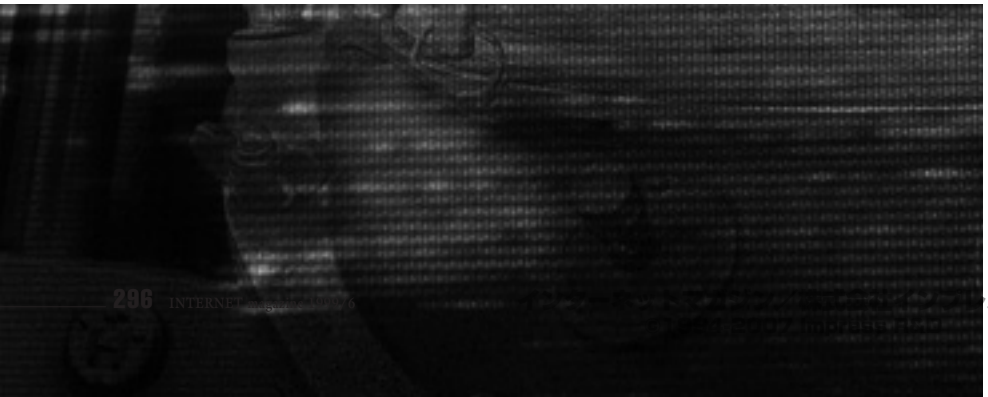
実践 Linux セキュリティー講座

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、今月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



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と、まったく同じ環境ではないかもしれません。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います。

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か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

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かが重要

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らなりません。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」はユーザー認証が甘いので、ユーザーがセキュリティー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。

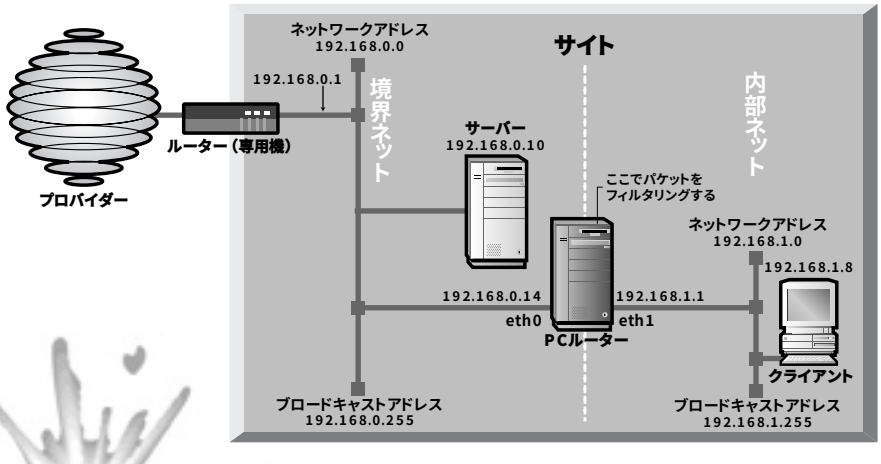
「何も通さない」から始める

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①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



のになります。

●DNS

まず最初に無条件で許可しても構わないプロトコルがあります。それがDNSのプロトコルです。DNSはホスト名をIPアドレスに変換するための機能です。ドメイン名で示されたホストにアクセスするには、DNSサーバーにアクセスする必要があります。

●HTTP

HTTPプトロコルを通すには、通信先ネットワークのポート80番を許可します。これには1つ問題があります。HTTPの使用するポート番号は必ずしも80番ではないからです。このような場合、ポート80番の通過を許可するだけでは、それ以外のポート番号を使うWWWサイトと通信できなくなります。

解決方法として通常はHTTPプロキシーを使います。HTTPプロキシーはWWWブラウザーのWWWサイトに対するリクエストを肩代わりして処理し、その結果をWWWブラウザーに返します。

HTTPプロキシーが使えるようにプロキシーサーバーのポート番号を許可しておけば、標準のポート番号を持たないWWWサイトでもプロキシーを経由して通信できるようになります。HTTPプロキシーはほとんどの場合プロバイダーが用意しているので、それを使うようにしましょう。

多くの場合、プロキシーのポート番号は8080ですが、これは絶対ではありません。必ずプロバイダーが提供している情報で確認してください。自分のサイト内でHTTPプロシキーを運用することについては機会を改めて説明します。

●電子メール

例となるサイトでは、外部からの電子メールはメールサーバーが一度受け取り、POPを使ってクライアント側に取り出すことにします。電子メールを送るときは、直接相手に接続することを想定しています。したがって、電子メールの受信についてはPOPによるサーバーとの通信を許可し、送信についてはSMTPによるすべてのネットワークとの通信を許可します。この構成はパソコンで電子メールソフトを使うような構成を意識しています。パソコンでプロバイダーにダイアルアップしている人にはお馴染みの環境でしょう。

●TELNET

TELNETは今回のネットワークでは使用しません。しかし、もし使うならば許可する接続は内部ネットから境界ネットのみに限定しましょう。さらに相手も限定します。

それぞれの手順は、PCルーターでリスト❷のように実行します。

フィルタリングの確認をする

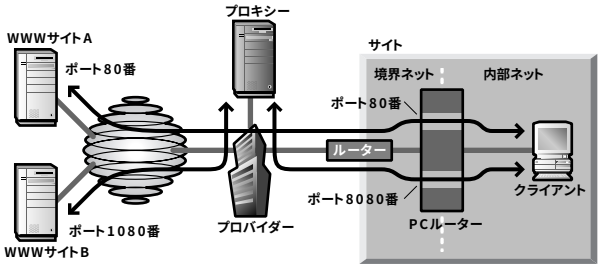
今回設定したフィルタリングの確認をします。リスト❸がその手順になります。ここでinside、dmzと表示されているのは、内部ネット、境界ネットの意味です。これは/etc/hostsにIPアドレスと名前の関連を定義することで表示させています。この定義がなければ、この名前はIPアドレスで表示されます。

フィルタリングが設定されると、フィルタリングを設定したコンピュータ（ここではPCルーター）に通過したパケットの情報（ログ）

リスト❶　すべてのパケットの通過を停止

```
# ipfwadm  -F -p deny ―――― すべてのパケットの通過を禁止
# ipfwadm  -F -f ―――――― フォワードのルールすべて無効
# ipfwadm  -I -f ―――――― 入力のルールすべて無効
# ipfwadm  -O -f ―――――― 出力のルールすべて無効
```

図2 プロキシーを使う例



HTTPはポート80番が一般的だが、ほかのポート番号を使っているサイトも多い。したがって、80番のポートだけ通過させても通信できないサイトがでてくる。そこで、プロバイダーなどに用意されているプロキシーを使って代理でアクセスしてもらう。一般的なプロキシーのポート番号は8080なので、このポートも通過させるようにしておく。

リスト❷　必要なパケットを通過させるフィルタリングの設定

●DNS（UDPポート番号53）の通過を内部ネットと外部との間で許可する

```
# ipfwadm -F -a accept -b -P udp -S 192.168.1.0/24 1024:65535  -D 0.0.0.0/0
53
```

●HTTPの通過を内部ネットと外部との間で許可する

HTTP（TCPポート番号80）を許可する

```
# ipfwadm -F -a accept -b -P tcp -S 192.168.1.0/24 1024:65535 -D 0.0.0.0/0
80
```

プロキシー（TCPポート番号8080）を許可する

```
# ipfwadm -F -a accept -b -P tcp -S 192.168.1.0/24 1024:65535 -D 0.0.0.0/0
8080
```

●電子メールのプロトコルの通過を許可する

POP3（TCPポート番号110）の通過を内部ネットと境界ネットとの間で許可する

```
# ipfwadm -F -a accept -b -P tcp -S 192.168.1.0/24 1024:65535 -D 192.168.0.0/24
110
```

SMTP（TCPポート番号25）の通過を内部ネットと外部との間で許可する

```
# ipfwadm -F -a accept -b -P tcp -S 192.168.1.0/24 1024:65535 -D 0.0.0.0/0
25
```

●TELNET（TCPポート番号23）の通過を内部ネットとサーバーとの間で許可する

```
# ipfwadm -F -a accept -b -P tcp -S 192.168.1.0/24 1024:65535 -D 192.168.0.1
23
```

オプションの意味

-F	フォワードを行う

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❹）。

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❺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❻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。

次回は、ipfwadmについてさらに詳しく解説します。

リスト❸　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❹　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❺　/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 -I -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
##プロキシー (8080)を許可
/sbin/ipfwadm -F -a accept -b -P tcp -S $INSIDE $USERPORT -D $ANY 8080
##POP3 (110)を許可（境界ネットから内部ネットのみ許可）
/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❻　/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的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