tcp wrapper

天野研 修士2年 松本秀夫

4月26日木曜日

1 inetd

UNIXシステムへのネットワーク経由のアクセスは、sendmailのような常駐型のdaemonへのものと、常駐はせずにアクセス要求があった時に起動されるものに分けられます。inetdは、後者の場合にアクセス要求を受け取り、要求に応じたdaemonなどを起動します。

inetdの設定は/etc/inetd.confに記述します。このファイルにはネットワーク越しのログインやネットワーク越しのファイル転送などを司るプログラムを起動するために必要なデータが書いてあります。まずは/etc/inetd.confを見てみましょう。ずらずらといろんな事が書いてありますが、ほとんどは次のようなスタイルになっていると思います。

```
ftp stream  tcp nowait  root /usr/libexec/ftpd ftpd -l
```

それぞれの項目の意味は、順にサービス名／ソケットタイプ／プロトコル／{wait—nowait}／ユーザ名／サーバプログラム名／サーバプログラム引数となっています[1]。行の先頭に#がついている行はコメント行で、先ほどのような行についていた場合はそのサービスが無効になっているという事になります。サービスが有効になっているものは、外部からのアクセスがあれば対応するプログラムを起動させます。

2 tcp wrapperとは?

inetd経由のネットワークアクセスを監視し、アクセス制限を行うのがtcp wrapperです。例えばtelnetの場合は、通常外部からtelnetのアクセスがあった場合は叩かれたポート(普通23番)に応じてtelnetdが起動し、応答します。tcp wrapperを入れていたときは、外部からのアクセスをまずtcp wrapperが受取り、そのアクセスが安全であると確認できてから(細かく設定が可能)改めてtelnetdを起動します。

3 tcp wrapperの利用

FreeBSDの場合、以前はtcpdという別のプログラムを用意してtcp wrapperを用いていましたが、現在はinetdにtcp wrapperの機能が組み込まれていますのでtcpdを介さずにアクセスの制御が行えます。

inetdに組み込まれているtcp wrapperを有効にするには、起動時に`inetd -wW`とすれば良く[2]、また大抵デフォルトでこのモードで起動されます。

4 アクセス制御

tcp wrapperは相手のIPアドレスによってアクセスの拒否/許可の設定ができます。これらの設定を行うファイルは、以前は/etc/hosts.allowと/etc/hosts.denyというファイルにそれぞれ許可ホスト/拒否ホストを記述していましたが、現在は全て/etc/hosts.allowに記述するようになっています。

まずは最初から用意されている/etc/hosts.allowを見てみましょう。#から始まるコメント行がずらずらと並んでいる筈です。しばらく眺めていくと次のような行があります。

```
# The rules here work on a "First match wins" basis.
ALL : ALL : allow
```

[1] 詳しくはman inetdを読んで下さい。
[2] wは外部サービスに対して、Wは組み込みの内部サービスに対してそれぞれtcp wrapperをオンにします。

ここに書いてあるように、このファイルでは最初にマッチしたルールが適用されます[3]。2つ目の行は、「全てのサービスに対して全てのホストからのアクセスを許可する」という意味です。つまり、このデフォルトの状態ではtcp wrapperの効果が事実上無効になっている訳です。そこで、このファイルを書き換えてやる必要があります。

/etc/hosts.allowの記述の仕方は次のようになります。

`daemon名 : クライアントリスト : オプション`

- daemon名
  起動されるdaemonの名前(ftpdやtelnetdなど)です。サービス名ではないことに注意してください。ALLと記述することで全てのネットワークデーモンを指定することもできます。
- クライアントリスト
  コンマで区切られたホスト名・ドメイン名・ネットワーク名です。ホスト名はドメイン名の付いたものでも、IPアドレスでも指定できます。ドメイン名は最初にピリオドをつけます。クライアントリストでもALLと記述することで全てのアクセスを指定することができます。
- オプション
  基本的にここでは{allow,deny}を設定します。また、ログを取ったりほかのコマンドを指定したりすることもできます。

例:

```
telnetd : 192.168.33. : allow
ftpd : 133.5.18.0/255.255.255.0 : allow
ALL : .db.is.kyushu-u.ac.jp : allow
ALL : ALL : deny
```

1行目はIPアドレスが192.168.33.*であるホストからのtelnetに対するアクセスを許可します。2行目も同様にIPアドレス133.5.18.*からのftpに対するアクセスを許可します。3行目はすべてのサービスに対する*.db.is.kyushu-u.ac.jpからのアクセスの許可を示します。4行目はすべてのサービスに対するすべてのアクセスを拒否します。

研究室におけるセキュリティポリシー

研究室においては、基本的にごく一部のサービスを除いてはすべてのアクセスを拒否します。

まず、/etc/inetd.confでftp以外のサービスはすべて無効にし、アクセス自体を受け取らないようにします。次に、/etc/hosts.allowを書き換えます。ここでは、先ほど有効にしたftpについて研究室のマシンからのアクセス(133.5.18ラインと192.168.33ライン)からのみアクセスを許可します。また、sshについては(おそらく)すべてのホストからのアクセスを許可しても良いでしょう。あとはすべて拒否します。

5 アクセス制御の確認

アクセスの制御がきちんとできているかどうかを確認するのには、tcpdchkやtcpdmatchを使います。

tcpdchkを実行すると、/etc/hosts.allowの書式などがチェックされます。書式に問題がある場合には警告が出ます。

tcpdmatchは次のように用いてアクセス制限が行われているのかを確認します。

`tcpdmatch サービス名 アクセス元`

例えばftpアクセスが許可されている場合には次のような結果が表示されます。

```
% tcpdmatch ftpd ホスト名
client:   hostname ホスト名
client:   address  ホストのアドレス
server:   process  ftpd
matched:  /etc/hosts.allow line 1
access:   granted
```

[3]マッチする内容がなかった場合は許可ホストと見なされます。

また、アクセスが拒否されている場合には次のようになります。

```
% tcpdmatch ftpd ホスト名
client:   hostname ホスト名
client:   address  ホストのアドレス
server:   process  ftpd
matched:  /etc/hosts.deny line 1
access:   denied
```

6　マニュアル

もっと詳しい説明が、hosts_options(5) や hosts_access(3) に書いてあります。

```
% man hosts_options
% man hosts_access
```

と入力して読んでみましょう。