RaQをセキュアに使おう

株)アライブネット
RS事業部 企画開発G 小田 誠

このセッションで学ぶこと

- フィルタリングのコツ
- TCP/IPのしくみ
- フィルタするパケットの流れ
- ipchainsを使ったパケットのフィルタリング
- Tcpwrappersによるアクセス制限

なぜフィルタするのか

- インターネットは危険
  - 商用化される前は比較的安全だったが現在は危険
  - OCNの128kbpsぐらいの線でも頻繁にportscanされる
  - Cobaltは比較的安全ではある
- 社内の人間以外はアクセスを制限したい
  - POP3とかFTPによるアップロードなど
- ポリシーの違うネットワークを繋ぎたい
  - 社内LANとInternetを分ける
  - 社内でさらに別のネットワークを立ち上げる

何をフィルタするか

- TCP/IPまたはUDP/IPと呼ばれるパケット単位
  - インターネットの標準プロトコルとして通信に使われる
  →ipchains(linux 2.2),ipf(*BSD,Solaris)など
  Kernelに組み込めるため、処理コストが少ない
- コンテンツ単位
  - アダルトサイトとかアンダーグランドなサイト
  →フィルタソフト、アプリケーションゲートウェイ(squid,専用機)
  複雑なルールが組めるが、処理コストは高い
- 特定のユーザ単位
  - 荒らしなどの悪意のあるユーザを排除する
  →プロバイダや警察などの協力が必要かも
  上の2つでも解決できる場合があるかもしれない

どこでフィルタするか

- 専用ファイアーウォール
  - SonicWallなど
- ホストベースファイアーウォール
  - Linux,FreeBSD,Solaris,Windows2000
- アプリケーション
  - Sendmail,Apache,TcpWrappers,Squid

これら すべてをうまく組み合わせる方法がよい。

TCP/IPの簡略化モデル

サーバ 192.168.0.1

アプリ	プロトコル		port
Pro ftpd	FTP		21
OpenSSH	SSH	T	22
Sendmail	SMTP	C	25
Apache	HTTP	P	80
qpoper	POP3		110

クライアント:192.168.0.3

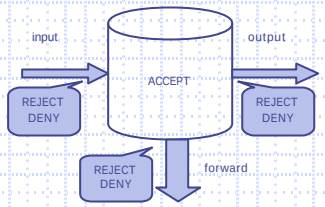
port		アプリ
1025		WS_FTP
2008	T	TeraTerm
3004	C	Eudora
1028	P	Netscape
3003		Eudora

クライアントPCがサーバにアクセスするには..

1. クライアントのNetscapeが空いているポートをさがす 1028番のポート。
2. 送信元のIPアドレス192.168.0.3ポート番号1028、送信先IPアドレス192.168.0.1ポート番号80番で接続をお願いする。
3. サーバ側は80番で接続を待っていたApacheが応答し接続する。
4. サーバとクライアントの間でデータの通信をする。
5. 通信を切断する。

netstat –na で接続の状態を見ることができる。

フィルタリングの方法



Ipchainsを使おう

- **パッケージのインストール**
  - http://www.cobaltreseq.com/rpms/ipchains-1.3.10-uC1.i386.rpm
  - http://www.cobaltreseq.com/pkg/RaQ3-Unofficial-20020901.pkg
  - Cobaltパッケージなら、管理画面からインストールします。
  - RPMならばsshログイン後にrpmコマンドを使います。

ipchainsのコマンドオプション

オプション	説明	振る舞い	説明
A	チェーンの追加	ACCEPT	パケットの通過を許可する
D	チェーンの削除	DENY	パケットを破棄する
P	ポリシーの変更(ACCEPT,DENY)	REJECT	パケットの通過を許可しない
L	ルールを一覧表示する	REDIRCT	パケットを別のサーバに飛ばす
F	ルールをすべて削除する		
N	新しいチェーンを作成する		
s	送信元IPアドレス		
d	送信先IPアドレス		
p	プロトコル名: tcp,udp,imcp		
j	振る舞い		
i	インターフェース名		
!	否定		

ipchainsの使用例

- **管理画面のアクセス制限**

```
ipchains –F
ipchains –A input –s 0/0 –d ! 127.0.0.1 81 –p tcp –j REJECT
ipchains –A input –s 10.0.3.0/24 –d 10.0.3.40 110 ¥
        –p tcp –j DENY
ipchains –L
ipchains-save –v > /etc/sysconfig/ipchains
```

保存するときに間違えると、誰もログインできなくなる場合があるので注意！

TCP-Wrappers

- **サービスに対してアクセス制限ができます**
  - inetdで呼び出されるもの
  - コンパイル時にlibwrapを使うように設定したもの

```
# vi /etc/hosts.allow
サービス名: IP アドレスまたはドメイン名 : 許可属性
ALL: 127.0.0.1/255.255.255.255 : allow
sshd: 210.196.148.245 : allow
sshd: 210.189.91.94/255.255.255.192 : allow
sshd: ALL : deny
pop-3 : ALL : allow
```