参考

http://saoshi.gooside.com/

http://ult.riise.hiroshima-u.ac.jp/~nagato/?iptables%A4%CB%A4%E8%A4%EBNAT

http://www.linux.or.jp/JM/html/iptables/man8/iptables.8.html

http://www.atmarkit.co.jp/flinux/rensai/security04/security04a.html

http://ft-lab.ne.jp/cgi-bin/wiki.cgi?page=iptables

パケットの流れとチェイン

INPUT

受信したパケットがサーバ自身のプロセスを処理する前に通ります。

OUTPUT

サーバ自身にて何らかの処理を行った後に、外部に出るときに通ります。

FORWARD

対象サーバを経由するときにの通り道です。主にルータ機能をもったサーバでのフィルタリング設定を行います。

PREROUTING

パケットがサーバに入ってきたとき、パケットのアドレス変換を行う必要がある場合はここで変換処理を行います。

POSTROUTING

サーバからパケットが出るときに、パケットのアドレス変換を行う必要がある場合はここで変換処理を行います。

サンプル

```
#!/bin/sh

IPTABLES="/sbin/iptables"
/etc/init.d/iptables stop

$IPTABLES -t filter -F # フィルター　クリア
$IPTABLES -t nat -F #NAT クリア

$IPTABLES -P FORWARD DROP # 全てのフォワードをドロップ
$IPTABLES -P INPUT DROP       # 全てのインバウンドをドロップ
$IPTABLES -P OUTPUT ACCEPT # 全てのアウトバウンドを許可

# 指定ポートのインバウンドを許可
$IPTABLES -A INPUT -i ppp0 -p tcp --dport 80 -j ACCEPT
IPTABLES -A INPUT -i ppp0 -p tcp --dport 22 -j ACCEPT

# ループバック（127.0.0.1）を許可
$IPTABLES -A INPUT -i lo -j ACCEPT
# 指定アドレスからのインバウンドを許可
$IPTABLES -A INPUT -i eth0 -s 192.168.0.0/24 -j ACCEPT
```

```
# $IPTABLES -A INPUT -p icmp -j ACCEPT
# ICMP echo
$IPTABLES -A INPUT -p icmp --icmp-type 8 -j ACCEPT
# ICMP echo reply
$IPTABLES -A INPUT -p icmp --icmp-type 0 -j ACCEPT

# 確立しているコネクションとそれに関連したインバウンドを許可
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# フォワード、マスカレイド設定
$IPTABLES -A FORWARD -d 192.168.0.0/24 -j ACCEPT
$IPTABLES -A FORWARD -s 192.168.0.0/24 -j ACCEPT
$IPTABLES -t nat -A POSTROUTING -o ppp0 -s 192.168.0.0/24 -j MASQUERADE
$IPTABLES -t nat -A POSTROUTING -o ppp1 -s 192.168.0.0/24 -j MASQUERADE

# 指定ポートへのアクセスをローカル PC のポートへ転送
$IPTABLES -t nat -A PREROUTING -i ppp0 -p tcp --dport 3000: -j DNAT --to 192.168.0.2
$IPTABLES -t nat -A PREROUTING -i ppp0 -p tcp --dport 3000 -j DNAT --to 192.168.0.2

echo 1 > /proc/sys/net/ipv4/ip_forward
```