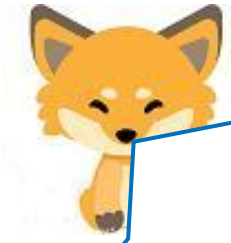
第２３話（セキュリティⅡ）

タヌキ、第２２話からの続きだ。
では、eth7（NIC A）から入ったパケットを eth8（NIC B）に通すルーティングの実習をしてみようか。
目的は、①（端末）から③の Web サーバにアクセスし、html ファイルを表示する、というものだ。つまり、ファイアウォール（②）のデフォルトでは、全てのサーバにアクセスできない設定になっているが、自分の会社のホームページへのアクセスだけを許可する時の設定だ。
②の PC の端末で以下のように入力し、実行する。

```
# iptables –t nat –A POSTROUTING –o eth8 –s 192.168.1.0/24 –j MASQUERADE
```

なんだか難しそうな命令が沢山並んでいるな。
#は、root 権限で実行しなさいということか。iptables は、一時的にファイアウォール（ルーティング、フィルター）設定をしなさい、というコマンドか。nat は、ルーティング設定だな。キツネ、後の解説をしてくれ。



OK！タヌキ、前回の説明を良く記憶しているな、エライ、エライ。
-A はルールを追加するぞ、というオプションだ。追加するルールは、POSTROUTING（ポストルーティング）だ。このルールは、「NIC A」から入ってきた 192.168.1.0/24 のネットワークに属するプライベート IP アドレスを「NIC B」から出る時に 172.17.50.11 という 1 個の IP アドレスに変換するということだ。-s (送信元)オプションは、eth7 から入ってきたネットワークアドレスである 192.168.1.0/24 のパケットを　eth8 から出て行く時に 172.17.50.11 に変換する。-o (out の意味)のオプションはパケットが eth8 から出て行くこと。-j オプションは、ターゲットである MASQUERADE（NAT 変換）を許可する、ということだ。192.168.1.0/24 の 24 はプレフィックスといい、サブネットマスクのことだ。ただし、eth8 には 172.17.50.11 の IP アドレスを割り振っているから、注意してね。

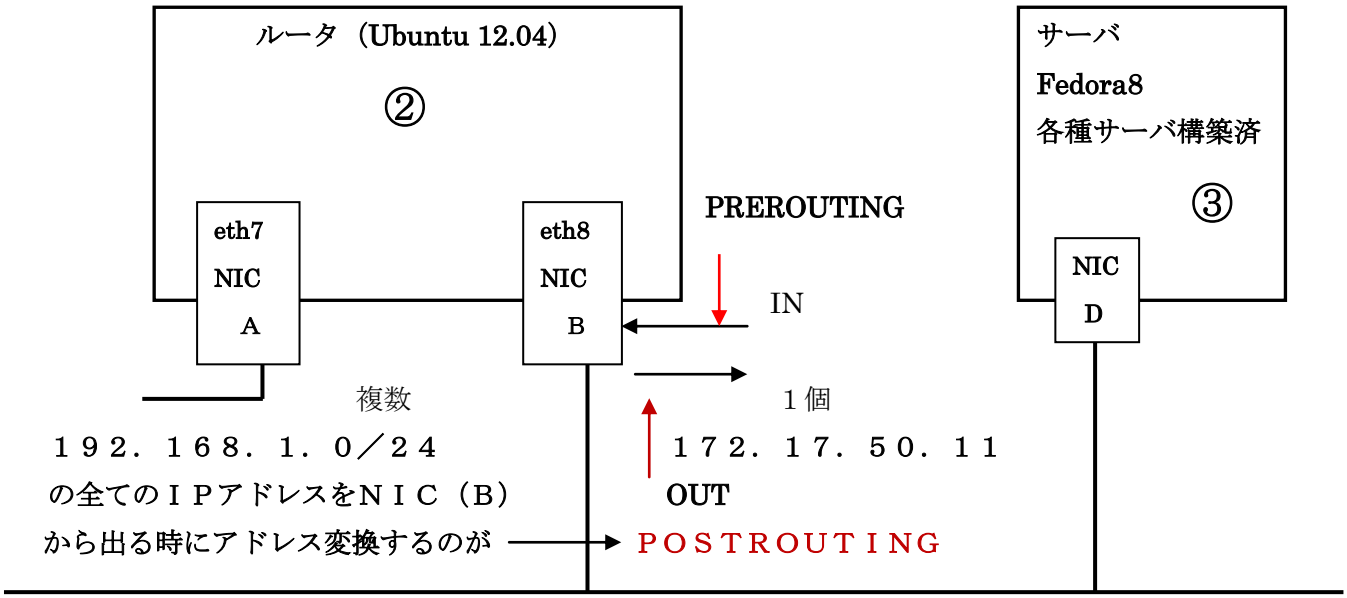
なるほどな、ところで実行すると IP テーブルは一時的にどのような状態になるのだ。

前回、IP テーブルのルーティングの状態を表示するコマンドの使い方を解説したよな。覚えているか。確か
iptables –n nat –L
これを実行してみて。以下のように表示されるはずだ。

```
root@ubuntu12-04: ~
oruser@ubuntu12-04:~$ sudo -i
[sudo] password for oruser:
root@ubuntu12-04:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  192.168.1.0/24       anywhere
root@ubuntu12-04:~#
```

上図の「target」は MASQUERADE（NAT 変換）を指している。prot（プロトコル）は all で全てのプロトコルが対象ということだ。opt（オプション）は、-- つまり、オプションの設定無し。source（送信元）は、192.168.1.0/24 のネットワークアドレスに属する全ての PC が該当する。destination（目的地）は、anywhere つまり全ての PC に eth8 に設定（172.17.50.11）した IP アドレスで送信する、という意味になる。
以上を、さらに詳しく図示すると以下の図になる。

［図解］



キツネ、これは一時的な設定だと言っていたが、恒久的な設定にする為にはどうするのだ？

タヌキ、「# iptables save 」というコマンドを実行すると恒久的な設定になる。それは、一時的に設定した内容が、/etc/sysconfig/iptables（ファイル）に書き込まれ、サーバの起動の度に実行されます。ですから、間違った設定をした場合、iptables ファイルから設定内容を削除するまで間違った状態で実行されます。ファイルへの書き込みは、内容を理解した上で行いましょうね。

じゃあキツネ、一時的な設定を一時的に削除する場合にはどうするのだ？

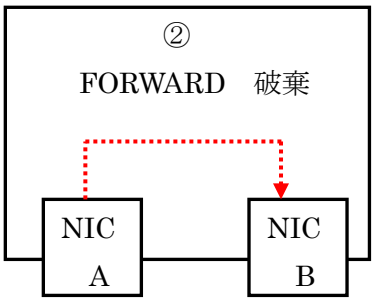
タヌキ、以下のコマンドを入力すると良いよ。
-D というオプションは Delete(削除)の意味だ。

```
# iptables -t nat -D POSTROUTING -o eth8 -s 192.168.1.0/24 -j MASQUERADE
```

ルーティングの話を中断して、フィルタリングの話をしようか。第２２話で②の PC は、デフォルトの状態で、フィルターはかけられていなくて、全てのパケットが通過可能の状態になっている、という説明をしたよな。タヌキ、覚えているか。eth7 から eth8 にパケットを渡すことを許可するフィルタリングのルール（チェインとも言う）は FORWARD だ。このルールにパケットを破棄（渡さない）するようにフィルタリングをかける設定が以下のようになる。説明を図解しておくよ。

```
#  iptables  –t  filter  -P  FORWARD  DROP
```

［図解］



フィルターの設定確認は以下の命令だったよな。

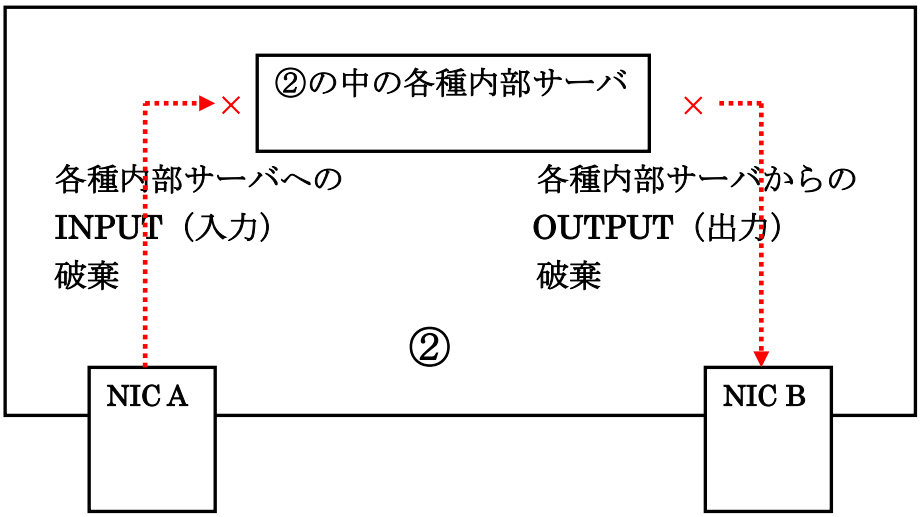
```
#  iptables  –t  filter  -L
```

```
root@ubuntu12-04: ~
oruser@ubuntu12-04:~$ sudo -i
[sudo] password for oruser:
root@ubuntu12-04:~# iptables -P FORWARD DROP
root@ubuntu12-04:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ubuntu12-04:~#
```

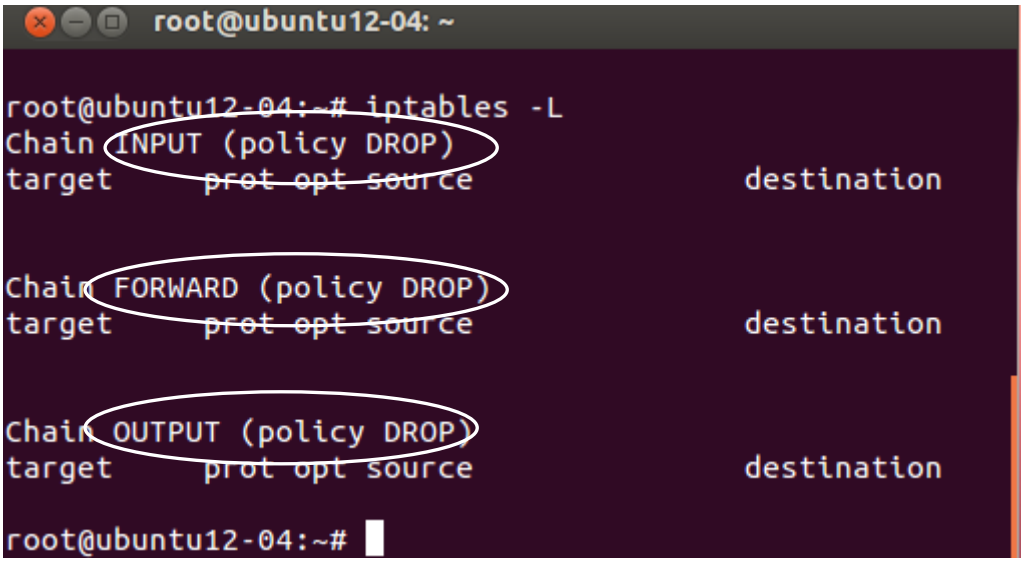
上図で、FORWARD のポリシーが DROP（破棄）になっていればフィルターがかかっている、ということだな。

次は、フィルタリングのルールである INPUT と OUTPUT の話だ。この理解は大変に重要だ。つまり、INPUT とは、パケットがどこに入ろうとするのか、OUTPUT とは、パケットがどこから出ようとするのか、ということだ。すべて、ファイアウォールを設定する②の PC 内部の話だ。図解した方がわかりやすいので、以下に示す。

［図解］フィルタリングの INPUT と OUTPUT の意味



iptables –t filter -P INPUT DROP
iptables –t filter -P OUTPUT DROP
とすれば、②の PC の内部のサーバ（もし有るとすれば）には外部からアクセスできなくなるし、内部サーバからデータが流出することも防げるのだ。納得！
iptables –t fileter -L で設定確認をしておくぞ。

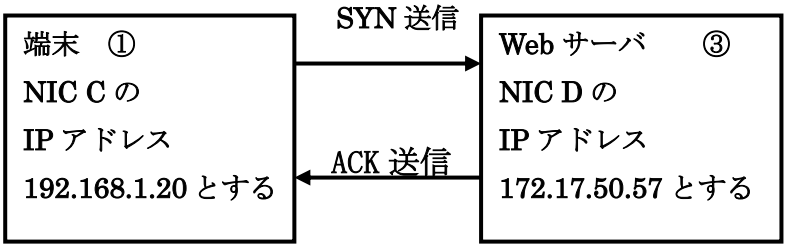


タヌキ、ここからが問題だ。
上図のように②の PC で完全にフィルタリングがかかり、③のサーバへのアクセスができなくなっています。
これが最初の正しいフィルタリング設定です。ただ、このままでは、③のサーバに対して外部からのアクセスが一切できない状態です。この状態から、外部ユーザにアクセスを許可するサーバだけ設定を解除していくのです。では、③の Web サーバへのアクセスだけを有効にするようなフィルタリングの設定を②にしてみよう。以下のように、外部ユーザから Web サーバに送られる、接続要求（SYN 送信）パケットを通過させるルールと Web サーバから外部ユーザにアクセスを許可（ACK 送信）するよ、というパケットを通過させる２つのルールを実行することになる。

［Web サーバのフィルター解除］

```
# iptables -t filter –A FORWARD –p tcp --dport 80 –d 172.17.50.57 –j ACCEPT

# iptables -t filter –A FORWARD –p tcp ! --syn –m state --state
                    ESTABLISHED --sport 80 –s 172.17.50.57 –j ACCEPT
```

この状態を図示すると右のようになる。



キツネ、オプションなどの説明を詳しくしてくれないか。

そうか、やはりこれだけじゃ少々らんぼうか。
次ページに補足解説をまとめておくよ。

［補足解説］

SYN 送信　：クライアントからサーバへ最初に送られる接続要求。

-t　filter　を省略している。

-p　：プロトコルの指定

tcp　：TCP プロトコル

--dport　：送信先ポート

80　：ポート番号８０は、http（web サーバ）

-- d　：送信先 IP アドレス

172.17.50.57　：③の NIC の IP アドレス

-j　：ターゲット

ACCEPT　：パケットの通過を許可

［補足解説］

ACK 送信　：サーバからのクライアントへの応答パケットの許可。

! –syn　：SYN フラグ以外を許可。

-m state　--state　：ステータスの指定。

ESTABLISHED　：ステータスの１つ。サーバとクライアント双方のコネクション許可。

sport　：送信元ポート

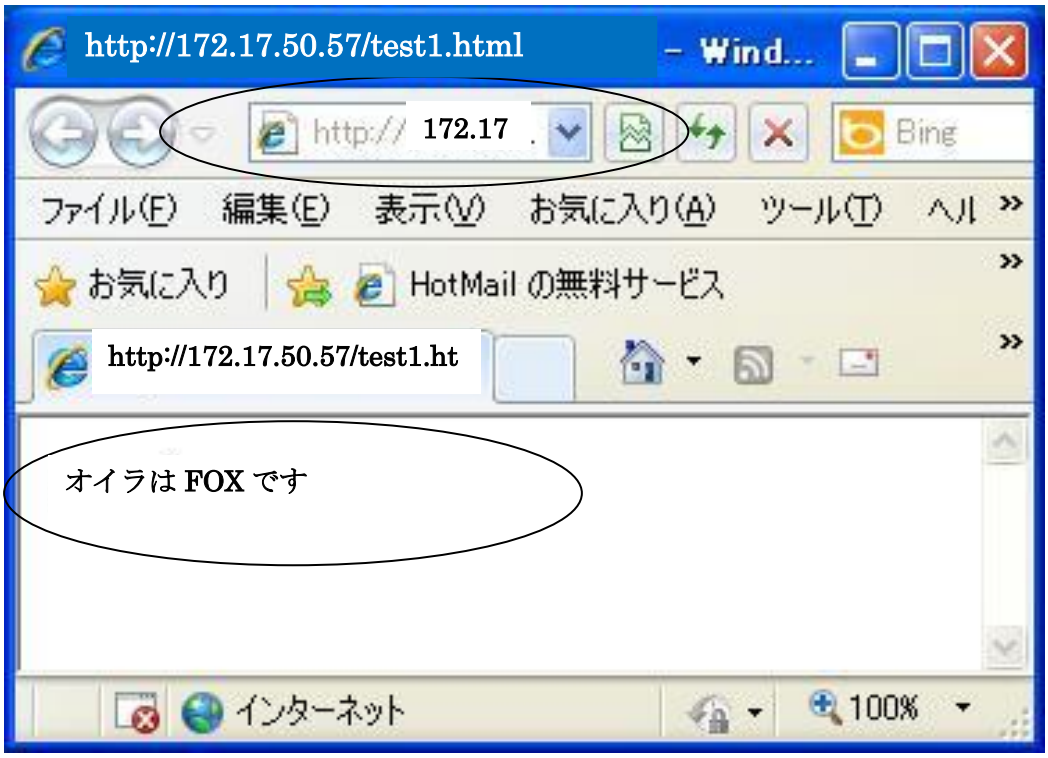
80　：送信元（Web サーバ）のポート番号

-s　：送信元の IP アドレス指定

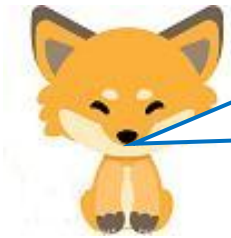
172.17.50.57　：③の NIC の IP アドレス

これで良く理解できる。キツネ、ありがとう。
それで、外部ユーザが、Web サーバにアクセスできるようになったかどうか、どうやってテストするのだ？

そうなんだ。フィルタリングがかかっている事を確認する場合も解除されたことを確認する場合もテスト用のサーバが必要になるのだ。これが、家の無い野原で泥棒に入る練習はできないよ、ということなんだ。だからサーバ構築力が必要なんだよ。
といっても確認しなければならないよな。③のPCのWebサーバには、/var/www/html/というディレクトリがある、そのディレクトリにtest1.htmlというファイルを作って保存するのだ。内容は、「オイラはFOXです」程度で良いよ。端末①のPCのブラウザを起動し、［http://172.17.50.57/test1.html］というURLを入力し、以下の表示がされたら解除されている、ということだ。



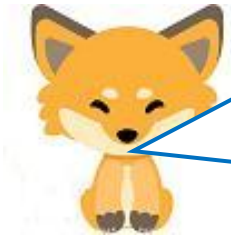
キツネ、表示されたぞ！



そうか、DNSサーバが構築されていればもっと本格的なアクセスができるのだがな。この状態では、DNSサーバにもフィルターがかかっているので、解除しなければならない。以下のようにすると、ドメイン名でアクセスできるようになるぞ。

[DNS サーバのフィルター解除]

```
# iptables -t filter –A FORWARD –p udp --dport 53 –j ACCEPT

# iptables -t filter –A FORWARD –p udp --sport 53 –j ACCEPT
```



上の５３は、DNSサーバのポート番号だ、ポートを開ける。つまり、DNSサーバへのアクセスを可能にする、ということだ。プロトコルはTCPで無く、UDPであることに注意してくれ。UDPプロトコルは、コネクションレス型（パケットの着信を確認しない）のプロトコルだからな。これでドメイン名でアクセスできると同時に「nslookup」コマンドも使えるぞ。

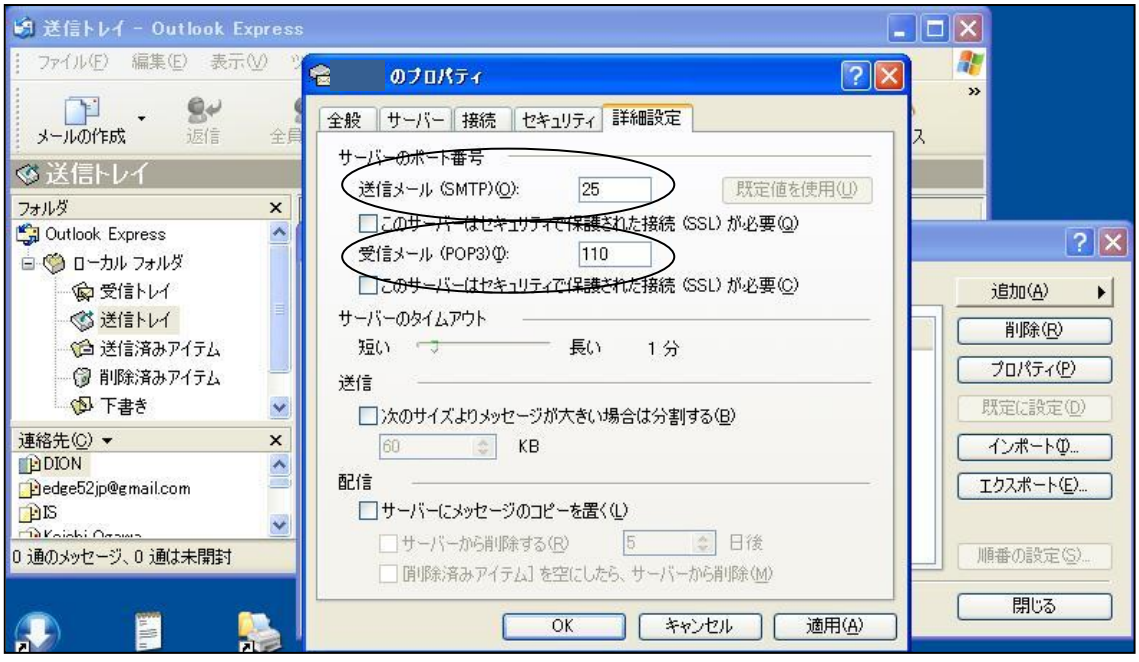
タヌキ、メールサーバも使えるようにフィルターを解除した方が良いよな。メールサーバにはSMTPサーバとPOPサーバがあったよな、それでこれも両方とも解除しなければメールの送受信ができないよ。以下のようにすれば、解除できるのだ。

［SMTP サーバと POP サーバのフィルター解除］

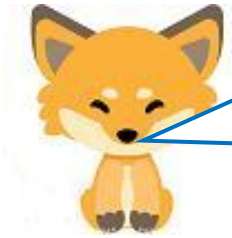
```
# iptables -t filter –A FORWARD –p tcp --dport 25 –j ACCEPT
# iptables -t filter –A FORWARD –p tcp --sport 25 –j ACCEPT

# iptables -t filter –A FORWARD –p tcp --dport 110 –j ACCEPT
# iptables -t filter –A FORWARD –p tcp --sport 110 –j ACCEPT
```

上のように実行すれば全ての外部ユーザがメールサーバを使えるようになるよ。タヌキ、フィルタリングが解除されているか忘れずに確認

25 は SMTP サーバのポート番号、110 は POP サーバのポート番号だったよな。確認は、適当なメーラでやるんだったよな。オイラは、outlook Express を使うぞ。



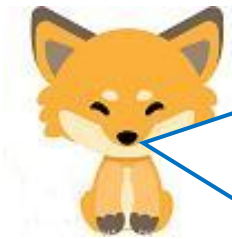
キツネ、ついでに全てのユーザではなく、セキュリティを高める為に特定の外部ユーザだけがメールサーバにアクセスできるようにする設定を教えてくれないか。



了解。以下のようにすれば、①のPC（IPアドレス：192.168.1.20とする）だけが③のPC（IPアドレス：172.17.50.57とする）のメールサーバにアクセスできるようになるよ。

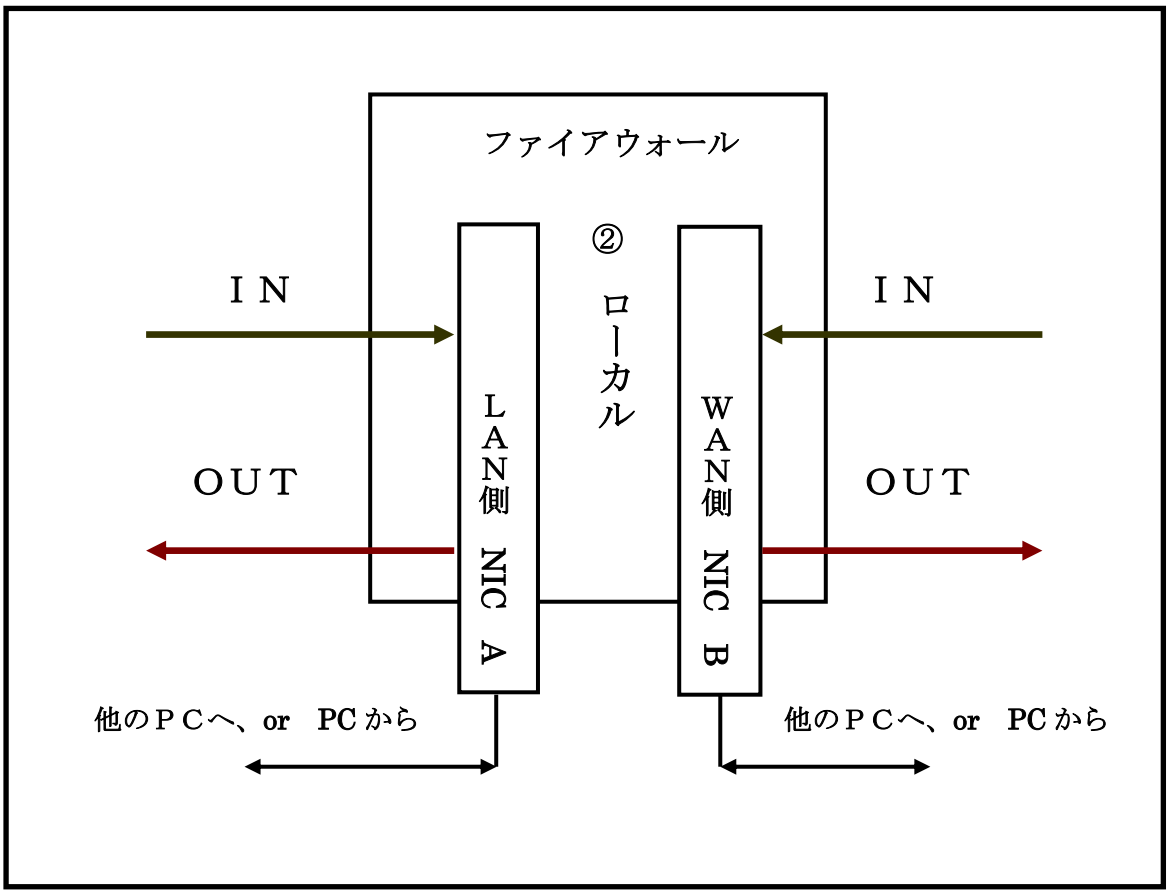
［特定ユーザのみフィルター解除］

```
# iptables -t filter –A FORWARD –p tcp -s 192.168.1.20 --dport 25
                                                -d 172.17.50.57 –j ACCEPT
# iptables -t filter –A FORWARD –p tcp -s 172.17.50.57 --sport 25
                                                -d 192.168.1.20 –j ACCEPT

# iptables -t filter –A FORWARD –p tcp -s 192.168.1.20 --dport 110
                                                -d 172.17.50.57 –j ACCEPT
# iptables -t filter –A FORWARD –p tcp -s 172.17.50.57 --sport 110
                                                -d 192.168.1.20 –j ACCEPT
```



タヌキの言うように特定ユーザに限定した方が良いかもね。悪意あるハッカーは、サーバのポートスキャンをしてセキュリティが甘く、開いているポートを狙ってくるから、最初は完全にフィルターをかけ、必要なポートだけのフィルター解除をして行くこと心がけてほしいな。
一つ注意して置きたい大切なことがあるのだ。
それは、次ページで説明するよ。

間違えて理解している場合が多いので、コメントしておくよ！
じつは、これまで述べてきたルール設定の中にある「-i eth7」や 「–o eth8」の「–i」や「 –o」のオプションは NIC への IN や OUT を指しているのだ。
注意してほしいのは、この IN や OUT は、インターネットからＬＡＮ側に入ってくるときＩＮ、ＬＡＮ側からインターネットに出て行くときＯＵＴと間違って解釈している学生を多くいるのだ。
ＷＡＮ側であろうが、ＬＡＮ側であろうが、パケットがＮＩＣに入ってくるときは、ＩＮであり、逆にＮＩＣから出て行くときは、ＯＵＴなのだ。iptables を実行する時には、ここが大きなポイントとなる。ＩＮ、ＯＵＴの区別（ルータ専用機もＬｉｎｕｘのルーティングも基本は同じ）をしっかり理解してほしいのだ。
図示すると以下のようになる。



長くなったから、この辺で終わりにし、次は

第２４話　にまわそうか。