# 第２２話（セキュリティⅠ）

タヌキ、しばらくセキュリティの話をするぞ。
個々のユーザにとってセキュリティとは、偽サイト（フィッシングサイト）や偽メール（フィッシングメール）、スパイクッキーから自分のPCを守りたい、自分の情報を守りたい、ということだ。
これらは、安易にメールの添付ファイルを開かない、個人情報を入力する時には、URLの左の鍵アイコンをクリックしCA（デジタル署名の認証局）を確認する、アンチウィルスソフトをインストールし、常にワクチンソフトを更新することで防ぐことができる。
第２２話で問題にするのは、サービスを提供する側のサーバをどのように守るか、という話だ。サーバには顧客の個人情報をはじめとして科学技術・政治・経済・軍事などの機密情報が多量に保存されている。それらは、相互に網の目状に繋がっており、日常的に使用されているので一部を遮断することができない。遮断できないものをどのように守るか、ということだ。

なるほど、ユーザの端末レベルのことは、オイラが注意すれば守れるけれども、サーバレベルでは、そうはいかないってことか。

タヌキ、サーバを守る技術を磨く為には、攻撃する対象のサーバが必要だということだ。例えば、何も無い野原らで泥棒が、鍵を開けたり、忍び込む技を磨いたりすることはできないだろう。セキュリティも同じことだ。ハッキング対象のサーバがあってこそ、ハッカーは、侵入したり、情報を盗み出すソフトの効果を試すことができるのさ。逆にサーバを管理する側は、ハッキングされないようにセキュリティを強化することができる。矛と盾の関係だ。しかし、ネット上の他社のサーバをテストに使うことはできない。それで、自分でテスト用のサーバを構築しなければならないのさ。

なるほどな、サーバが無いところで、ハッキングやセキュリティの実践力を身につけろ、というのは、野原で泥棒に入る練習をしろ、というのと同じか。それじゃダメじゃん！
でも、キツネ、オイラの学校の情報教育で、そういう実習をしたことがないぞ。

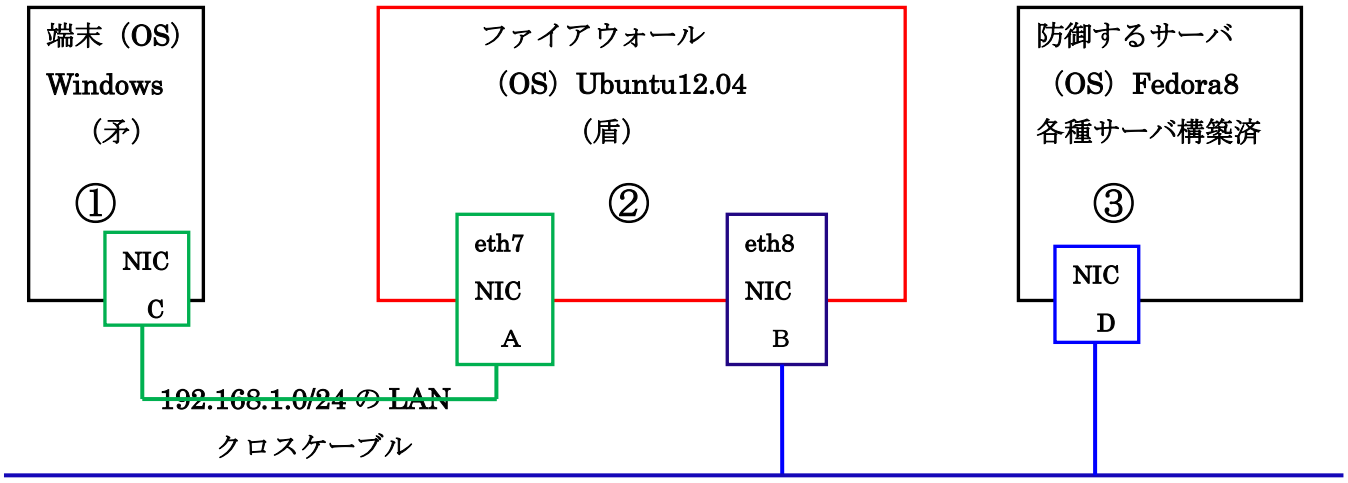
セキュリティの実習をする為には、教える側は矛と盾に該当する PC の準備をしなければならないし、生徒もネットワークの基礎程度の学習をしていなければならない。情報科学では、結構上級の部類に入るのだ。その人材を育成するとなるとしっかりとした計画に基づいて段階的に進めていかなければならないのだ。情報人材が１００万人必要だから、来年から情報教育をするぞ、という掛け声で育成できるレベルじゃないのだ。ナメンジャネエ、と言いたいね。

怒るのは勝手だが､それでオイラに教えてくれるのか？

タヌキ、簡単に言うと、結構大変だから、自分でも勉強してくださいね、ということだ。
最初は、盾（サーバ）を如何に守るか、ということだ。つまり、ファイアウォールの構築だ。日本語に直すとファイアウォールは、防火壁だ。壁を作り、外敵から内部を守るということだ。具体的に言うとファイアウォールは､ルーティング機能＋フィルタリング機能からできている｡ルータというハード(機器)も Linux の OS も、その両方の機能を持っている。その機能を学習し、正しく設定する、というのが学習目標だ。
考え方だが、一般に公開するサーバは、DMZ（非武装地帯）に置いて、重要なデータを保存しないで、ハッキングされてもしかたがない、内部のサーバはローカルに置いて公開しない、という方法もある。

実習を進める為には、以下のようなシステムを作らなければならない。これを見て意味わかんない、というレベルならセキュリティの勉強は止めた方が良いな。
ネットワークの基礎から勉強をし直してくれ。

## ［セキュリティ実習の為のテスト環境］




②の NIC の eth7 とか eth8 は何を意味しているのだ。

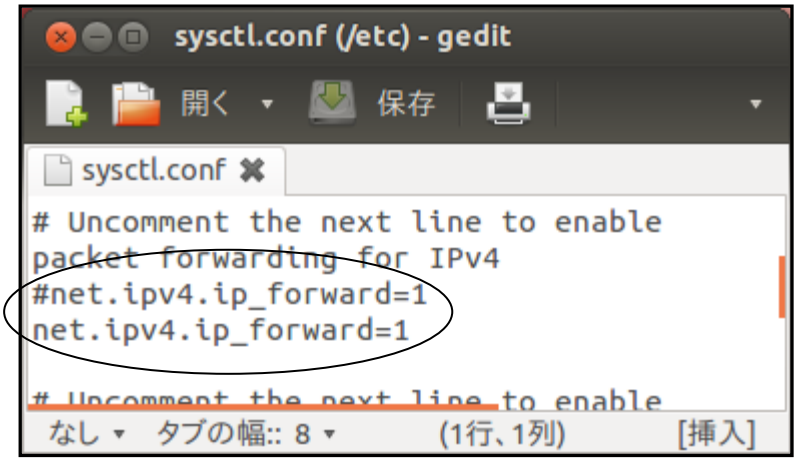
NIC（ネットワーク・インタフェース・カード）に一時的に付けられる名前だ。デバイス名とも言う。タヌキにわかるように、オイラは「NIC A」、「NIC B」という名前を付けたが、LinuxのOS（Ubuntu）では便宜上eth7、eth8という名前を付けるのさ。ただ、このデバイス名はログイン時に変ることがあるので、注意が必要だ。
まあ、上図を見て理解しろ、というのも無理な話なので、図の説明を次で簡単にするよ。

③の PC には、守るべきサーバ類と重要な情報（データ）が保存されている。そのサーバを①の端末 PC が狙っている。OS は一般に使われている Windows である。③の PC を守る為に立ちはだかるのが、②の PC（ファイアウォール）である。OS は、Ubuntu で標準でルーティング機能とフィルタリング機能を持っている。
さて、③の PC を守る為に、②のルーティング機能とフィルタリング機能の設定を行っていくのが、これからの学習である。

ルーティング機能とフィルタリング機能の設定か。
ハードのルータも同じ機能を持っているよな。

タヌキの言うように、②の PC をルータ（ハード）で置き換えても良いよ。ただ、ルータの場合、ラジオボタンをクリックすることで設定するので理解しにくい。詳細な設定も困難である。でもルータがファイアウォールとして機能することは知っておいた方が良いよ。

さて、始めるよ！
②にルータとしてのパケット中継機能を持たせる。
②の/etc/sysctl.conf（ファイル）を開いて
　net.ipv4.ip_forward の値が 0 になっていたら 1（有効）に設定する。



IPv4 の IP アドレスの中継を許可するのか。
今は、IPv6 もあるから注意しなければならないな。

最初に設定確認の勉強をしようか。②のフィルタリングがどのような設定状態か確認しよう。コマンドは必ず、root 権限で実行しないと受け付けてもらえないよ。
［# iptables　–t　filter　–L］これを省略した形で入力すると［# iptables　–L］となる。

```
root@ubun1204-[redacted] ~
    @ubun1204-[redacted] ~$ sudo -i
[sudo] password for [redacted]
root@ubun1204[redacted]:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ubun1204-[redacted] ~#
```

これは、デフォルト（規定値）の設定状態だな。INPUT、FORWARD、OUTPUT のいずれにもフィルターがかかっていない。パケットが通過できる状態になっている。これじゃ、いくらでもハッキングできるな。
次は、ルーティングの確認じゃ。ルーティングは、
［# iptables　－t　nat　–L　］と入力するんだ。

```
root@ubun1204-[redacted]: ~
[redacted]@ubun1204-[redacted]:~$ sudo -i
[sudo] password for [redacted]:
root@ubun1204-[redacted]:~# 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
root@ubun1204-[redacted]:~#
```

これもデフォルトの設定状態だな。この状態は、②の「NIC A」と「NIC B」間のルーティングの設定がされていない状態を示している。つまり、①の PC から②の PC にパケットは通らない、ということだ。通信はできない、ということだ。

なるほどな、フィルタとルーティングの設定はこのようにして見るのか。

まだまだ先が長いから、後は第２３話にするか。