



## LinuxでPCをルーターに

さて、実際に手を動かしながらLinuxを使ってルーターをセットアップしてみます。作業のステップは以下のとおりです。

- ① ルーターにするPCの機材を揃える
- ② 2枚目のネットワークカード (NIC) をPCにインストールして使えるようにする
- ③ 実際にネットワークが使えるかテストする
- ④ ルーターとしてPCを設定する
- ⑤ PCがルーターとして機能するかテストする

このルーターは前回説明したスクリーンサブネット構造での境界ネットワークのセグメントと内部ネットワークのセグメントを区切るためのルーターとして使います (右下図)。

今回は上記ステップのうちの①から③までを解説します。実際のネットワークで使うルーターにするには④と⑤の作業が必要になりますが、具体的なネットワークの設計が必要となるので次回以降に説明します。

今回取り上げる複数のNICをインストールするノウハウはLinuxをルーターにするだけに留まらず、Linuxのネットワークのパフォーマンス向上など多目的に利用できます。

たくさんのクライアントが一斉にサーバーにアクセスした場合、たとえサーバー自体の能力に問題なくても、ネットワークの出入り口が混雑しすぎてパンクしてしまうことがあります。このような場合に複数のNICをインストールして負荷を分散させておく方法が非常に有効になります。あるいは大量にデータが流れることによってネットワークが飽和している場合、サーバーを2つの異なるネットワークセグメントにつないでネットワークのトラフィックを軽減させることもできます。

## ハードウェアを揃えよう

今回の実験で使用しているのはゲートウェイ2000 P5-75という手元にあった古いIPCです。

購入時スペック

CPU ペンティアム75MHz

# 実践 Linux セキュリティー講座

前回まではLinuxについてというよりも、セキュリティーやファイアウォールについての概念的な説明をしてきました。今回は実際にPCにLinuxをインストールして各種設定を行って、Linuxマシンをルーターとして機能させる方法を説明します。Linuxのインストールについては詳しく説明しないので、1999年1月号の集中企画を参考にしてください。

## 第3回 Linuxマシンをルーターにする

ソフトウェアコンサルタント すずきひろのぶ





メモリー 16Mバイト  
HDD 660Mバイト  
PCIバス (プラグアンドプレイ対応)

購入時は16Mバイトのメモリーだったのを後に32Mバイト増やして、現在は合計48Mバイトとなっています。また、NICもなかったのでスリーコム社の「3C590 10bT」を購入してインストールしていました。ここ1年ほどは電気を入れたこともなく、ホコリを被っていたPCです。

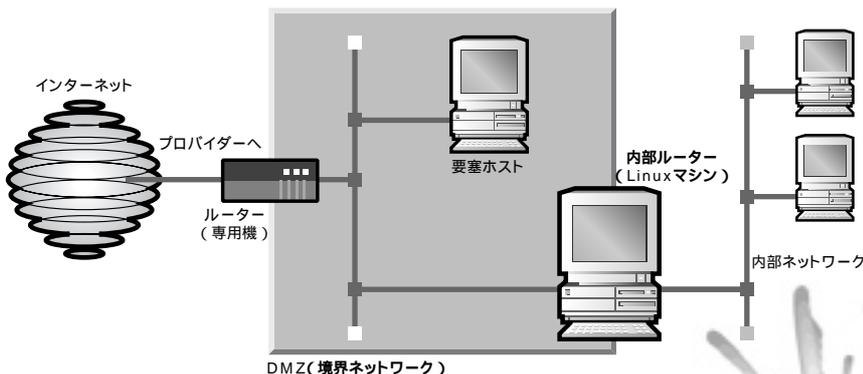
PCIバスでなくとも各種の設定はできますが、PCIバスのプラグアンドプレイの機能があれば設定は格段に簡単になるので、ここでの説明はこの機能が正常に動作することを前提とします。

このPCに新しいNICをインストールします。今回筆者が新たに購入したのはナカガワメタル社から発売されているPCIバスイーサネットアダプターカード「TR-PCI-10」です。これを選んだ理由は技術的な面からはノベルNE2000互換というポピュラーな仕様のNICであることです。経済的な面からは秋葉原で物色した中で一番安かったからです。店頭販売価格は1,680円でした。この価格で決めたといってもいいでしょう。

## PCにLinuxをインストールする

まず購入したNICをインストールする前の状態のPCにLinuxをインストールするところ

図 セットアップするLinuxマシン (ルーター)



から話を始めましょう。インストールの方法は1999年1月号の集中企画「RedHatで今すぐできるLinuxインターネットサーバー完全マスター」に書かれている「Linuxのインストールにチャレンジ」(233ページ)を参考に行えばいいでしょう。Linuxも1999年1月号に付属していたRedHat 5.2のCD-ROMを使います。

このインストール手順の中で、マシンの用途の選択があります(1999年1月号234ページの の部分)。慣れている人は「Custom」を、慣れていない人は「Workstation」を選択してください。「Custom」を選択したときは、パーティションは“/”用に1つ、あとはスワップ用に1つ設定するだけで十分です。インストールするパッケージを選択する部分では「Networked Workstation」のみを選択します。「X window」やそのほかのツールは基本的に必要ありません。

また、稼働させるサービスを選択する部分では、初期状態でいろいろなサービスが選択されていますが、「lpd」と「sendmail」は選択を取り消します。それ以外は通常のインストールのとおりです。

インストールが終わった時点で約110Mバイトのディスク領域が使われています。ですから、もし古いIPCでディスク容量も200Mバイトとか300Mバイトと小さいものであってもわざわざディスクを買い足す必要はありません。またCD-ROMが付いていないようなPCでも大丈夫です。ネットワーク経由でイン

ストールできるからです。

## 2枚目のNICをインストールする

次にPCの電源を切って、2枚目のNICをPCIバスに差し込みます。PCをブートさせるとLinuxはPCIバスにインストールされたNICを自動的に確認します。なお、両方のNICともネットワークに接続(ハブに接続)しておいてください。

NICをLinuxが認識したかどうかはリスト1のようにして確認できます。

もし、「Ethernet controller」(2枚目のNIC)を認識していなかったら、接続不良かPCIバスのプラグアンドプレイ機能に対応していないか、それともNIC自体の不良などのハードウェア的な問題の可能性も考えられます。もう一度NICを確認してみてください。

## eth1を作成する

eth0やeth1はOS側が認識しているイーサネットのデバイスのことです。OSは直接ハードウェアを操作するのではなく、eth0やeth1といったソフトウェアとしてのデバイス进行操作します。

Linuxのインストール時に装着されていたNICはインストーラーがeth0として自動的に認識しています。まず、最初のNICが確実に動作しているかをリスト2のようにして確認してください。

次にeth1を認識させる設定を行います。RedHatの場合、NICの追加は次のような手順で行います。

- ① /etc/lilo.conf にeth1を設定
- ② /etc/conf.modules にeth1のデバイスドライバを設定
- ③ /etc/sysconfig/network-scripts/ ifcfg-eth1を作成
- ④ マシンを再起動

まずカーネルに新規にeth1が必要なことを



通知します。そのためには/etc/lilo.confに次の行を加えます。

```
append="ether=0,0,eth1"
```

このetherに関する記述フォーマットは、

```
ether=IRQ,I/Oアドレス,名前
```

となっています。IRQを0、I/Oアドレスを0と指定すると、lilo（起動時に初期設定を行うプログラム）が自動的に適切なパラメータを選択してくれます。

次に、/etc/conf.modulesに次の行を加え

ます。これはeth1がne（NE2000用）のデバイスドライバを使うということをカーネルへ通知します。

```
alias eth1 ne
```

NE2000ではなくほかの種類のNICの場合は、/lib/modules/preferred/netに各種のデバイスドライバが用意されているので、そのデバイスドライバを指定してください。

/etc/sysconfig/network-scripts/ifcfg-eth0はeth0のネットワークの設定ファイルです。インストール時に設定したネットワークの情報が書かれています（リスト3）。

/etc/sysconfig/network-scripts/ifcfg-eth0をコピーして/etc/sysconfig/network-scripts/ifcfg-eth1を作成し、DEVICE（デバイス名）とIPADDR（IPアドレス）の情報を書き換えます。まだテスト段階なので、IPアドレスは内部ネットワークと同じセグメントにしておきます。ここでは192.168.1.33としておきます（リスト4）。

これが終了したらLinuxをリブートします。次にOSがブートする時には、/etc/sysconfig/network-scripts/ifcfg-eth1を読み込んで自動的にeth1を設定してくれます。正しく設定されたかどうかはリスト5のように確認できます。

### リスト1 NICの認識の確認

```
% cat /proc/pci ← catコマンドの実行

PCI devices found:
Bus 0, device 14, function 0:
 Ethernet controller: 3Com 3C590 10bT (rev 0).
 Medium devsel. IRQ 15. Master Capable. Latency=248. Min Gnt=3. Max
 Lat=8.
 I/O at 0xfcc0.

Bus 0, device 12, function 0:
 Ethernet controller: VIA Technologies VT 82C926 Amazon (rev 0).
 Medium devsel. IRQ 11.
 I/O at 0xfce0.

表示結果
```

### リスト3 eth0のネットワーク情報

```
DEVICE=eth0
IPADDR=192.168.1.32
NETMASK=255.255.255.0
NETWORK=192.168.1.0
BROADCAST=192.168.1.255
ONBOOT=yes
```

### リスト4 eth1のネットワーク情報

```
DEVICE=eth1 ← デバイス名を変える
IPADDR=192.168.1.33 ← IPアドレスを変える
NETMASK=255.255.255.0
NETWORK=192.168.1.0
BROADCAST=192.168.1.255
ONBOOT=yes
```

### リスト2 最初のNICの動作確認

```
% /sbin/ifconfig ← ifconfigコマンドの実行

lo Link encap:Local Loopback
inet addr:127.0.0.1 Bcast:127.255.255.255 Mask:255.0.0.0
UP BROADCAST LOOPBACK RUNNING MTU:3584 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0

eth0 Link encap:Ethernet HWaddr 00:A0:24:7B:72:74
inet addr:192.168.1.32 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:203 errors:0 dropped:0 overruns:0 frame:0
TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
collisions:0
Interrupt:15 Base address:0xfcc0

表示結果
```





## IPパケットが届くかチェック

外部のマシンから該当するIPアドレスへリスト6のようにpingを実行してみます。

もし、pingの packets が正常に届かない場合は、ケーブルなどが外れていないか、接続を中心にチェックしてください。また、設定ミスがないかを確認してください。

## IPフォワードを可能にする

現在の状態(初期設定のままのインストール状態)では2つのNICの間でIPパケットをやり取りする機能(IPフォワード)はOFFの状態

になっているはずですが、本当にOFFの状態かを/var/log/messagesに残っているブート時の記録をリスト7のように確認してみてください。

IPフォワードをONにするには、リスト8のように/etc/sysconfig/networkにあるFORWARD\_IPV4の値をyesにします(yesではなくても“no”あるいは“false”以外の記述であればなんでも構いません)。

この設定を行った後に、PCをリブートさせると、ブート時に出力されるメッセージには‘ip forwarding off’のメッセージが現れなくなり、IPフォワーディングができるようになります。

## 参考資料を手に入れよう

参考資料としては1999年1月号付録のCD-ROM内の/doc/HOWTOに収められている付属ドキュメント(英語)が役に立ちます。またこれらの英語ドキュメントはボランティアの手により日本語化されています。しかも、インターネットを通じて入手することができます。Linuxはソフトウェアだけでなく、こういった文書も無料で手に入られるのです。これらの文書は日本Linux協会のウェブサイトから入手できます。

日本Linux協会

URL //www.linux.or.jp

### 参考資料

- Ethernet-HOWTO
- Multiple-Ethernet
- Firewall-HOWTO

### リスト5 追加したNICの動作確認

```
% /sbin/ifconfig <----- ifconfigコマンドの実行

lo          Link encap:Local Loopback
... (省略)
eth0       Link encap:Ethernet HWaddr 00:A0:24:7B:72:74
... (省略)

eth1       Link encap:Ethernet HWaddr 00:00:02:00:26:06
            inet addr:192.168.1.33 Bcast:192.168.1.255 Mask:255.255.255.0
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:17 errors:0 dropped:0 overruns:0 frame:0
            TX packets:132 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0
            Interrupt:11 Base address:0xfce0
```

表示結果

## いよいよルーターが本格始動

次号では今回セットアップしたLinuxマシンをルーターとして稼働させます。実際のネットワークの構成を考えながら、それに合ったセットアップの方法を解説します。この部分がファイアーウォール構築の大きな第一歩といえるでしょう。

### リスト6 IPパケットが届くかどうか確認

```
% ping 192.168.1.32 <----- pingコマンドの実行(最初のNIC)

PING 192.168.1.32 (192.168.1.32): 56 data bytes
64 bytes from 192.168.1.32: icmp_seq=0 ttl=64 time=0.6 ms
64 bytes from 192.168.1.32: icmp_seq=1 ttl=64 time=0.6 ms
^C <----- Ctrl+Cで終了させる
% ping 192.168.1.33 <----- pingコマンドの実行(追加したNIC)
```

表示結果

### リスト8 IPフォワードをonにする (/etc/sysconfig/network)

```
変更前
NETWORKING=yes
FORWARD_IPV4=false
HOSTNAME=ホスト名
DOMAINNAME=ドメイン名
GATEWAY=192.168.1.254
GATEWAYDEV=eth0

変更後
NETWORKING=yes
FORWARD_IPV4=yes <----- falseをyesに変更
HOSTNAME=ホスト名
DOMAINNAME=ドメイン名
GATEWAY=192.168.1.254
GATEWAYDEV=eth0
```

### リスト7 /var/log/messagesでIPフォワードの状態をチェック

```
% grep forwarding /var/log/messages | tail -<----- grepコマンドを使う

Feb 3 17:47:06 red kernel: sysctl: ip forwarding off
            <----- IPフォワードがoffになっている
```





## [インターネットマガジン バックナンバーアーカイブ] ご利用上の注意

このPDFファイルは、株式会社インプレスR&D(株式会社インプレスから分割)が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

<http://i.impressRD.jp/bn>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真の撮影者、イラストの作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元(株式会社インプレス R&D)、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D(当時は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接のおよび間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先

**株式会社インプレスR&D**

All-in-One INTERNET magazine 編集部

[im-info@impress.co.jp](mailto:im-info@impress.co.jp)