



ネットワークの構成を決める

これから構築するサイトのネットワーク構成を図1のように想定します。

想定するネットワーク構成内では、前回PCにNICを2枚インストールしてテストしたときのIPアドレスは使用しません。PCルーター用に再度新たなIPアドレスを振りなおします。

これ以降は境界ネットワークを境界ネットとし、内部ネットワークを内部ネットとします。

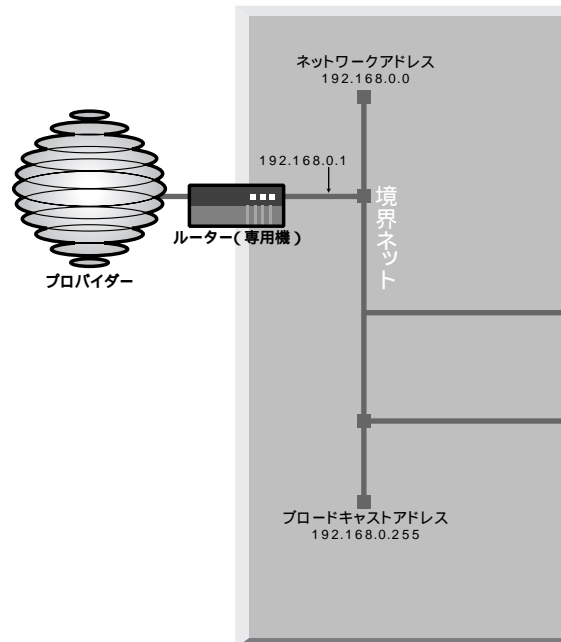
ネットワークの方針を決める

まず全体を簡略化するために、次のように方針を決めます。

サイト内にあるすべてのネットワーク機材のIPアドレスはスタティックアドレスとします。

スタティックアドレスとは、コンピュータに割り当てたIPアドレスを固定的に使用方法です。一方、コンピュータのIPアドレスを事前に決めずに、コンピュータをネットワークに

図1 サイトのネットワーク構成



実践 Linux セキュリティー講座

前回はLinuxをインストールした古いIPCをルーターとして使うために、NIC (Network Interface Card)を2枚インストールして動くところまで確認しました。また、2枚のNIC間でIPパケットが流れるように、IPフォワードの設定も行いました。今回はこのPCを境界ネットワークと内部ネットワークを区切るためのルーターとして動作させるまでの作業を行います。

第4回 Linuxマシンをルーターにする その2

ソフトウェアコンサルタント すずきひろのぶ



接続したときに自動でIPアドレスを割り当てる方法もあります。これには一般にDHCP (Dynamic Host Configuration Protocol) という技術を使います。DHCPサーバーを用意しておけば、クライアントをネットワークに接続したときに、DHCPサーバーが自動的に適切なIPアドレスを割り当てます。市販されているダイアルアップルーターの多くはDHCPのサーバー機能を持っていますので、たくさんのユーザーがすでにこの機能を利用していると思います。

今回の説明では、ネットワークの構造やマシン関係を明確にしてわかりやすくするために、スタティックアドレスを使うことにします。

プロバイダー側(インターネット側)とサイト側のアドレスは独立に考えます。

専用線接続のときは、プロバイダーからサイト内のコンピュータに対してグローバルアドレスというインターネット上で唯一のIPアドレスがいくつか与えられます。これも話をわかりやすくするために、説明中では境界ネットと内部ネットに対してプライベートアドレ

スを割り当てます。プライベートアドレスとは、私的なサイト内で自由に使っているIPアドレスです。グローバルアドレスはインターネット上で唯一のもですが、プライベートアドレスは同じものが世界中にいくつあってもかまいません(ただし、プライベートアドレスの情報はインターネット上に流すことはできません)。

グローバルアドレスをどう扱うかの方策は、今後の連載中で説明します。

サーバー、クライアント、PCルーターはLinux RedHat 5.2を使います。

これはいろいろなOSや複数のLinuxパッケージを混在させると話が混乱してしまうからです。本誌1999年1月号付録CD-ROMに入っているRedhat 5.2を想定しています。なお、3月19日にレーザー5より日本語版Redhat Linux 5.2が発売されました。日本語環境が使いたい場合にはこの製品を購入するか、無償で提供しているものをレーザー5のWWWサイトからダウンロードしてください。

レーザー5

j <http://www.cdrom.co.jp/>

/etc/hostsを作る

/etc/hostsはIPアドレスとコンピュータ名の組み合わせを記述したファイルです。Linuxはネットワーク上にどのようなマシンがあるかを探すときに、このファイルの内容を参照します。

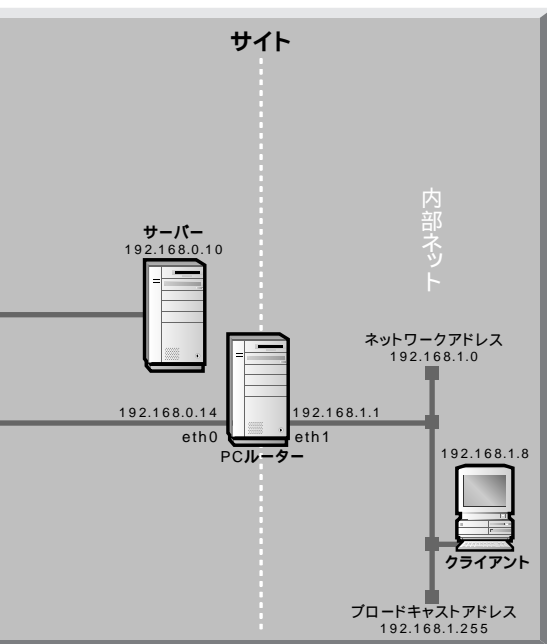
まず、今回のネットワークを想定したリスト1のような/etc/hosts用のファイルを作り、サーバー、PCルーター、クライアントの各々のマシンにコピーします。

ネットワークに詳しい方ですとDNS (Domain Name System) を使う方法が思い浮かぶでしょうが、これは今後の連載中に取り上げることにします。今回は、単純で確実な/etc/hostsを使ってネットワークのIPアドレスとコンピュータ名の対応付けをします。

コンピュータ名には別名を複数付けることもできます(リスト2)。

ネットワークの設定をしよう

次に各コンピュータ(PCルーター、クライ



リスト1 /etc/hosts

#アドレス	マシン名	
192.168.0.1	rt1	← インターネット接続ルーター
192.168.1.8	client1	← クライアント
192.168.0.10	server1	← サーバー
192.168.0.14	opcrt	← 内部PCルーター (境界ネット側のNIC)
192.168.1.1	ipcrt	← 内部PCルーター (内部ネット側のNIC)

リスト2 /etc/hosts (複数の名前を付けた場合の例)

(省略)	
192.168.0.10	server1 mail www ftp linux01
192.168.0.14	opcrt pcrt01 linux02
192.168.1.1	ipcrt pcrt02 linux03



アント、サーバー)のネットワークの設定をしていきます。

まず、PCルーターのネットワークの設定をします。ディレクトリー/etc/sysconfig/network-scriptsにあるifcfg-eth0とifcfg-eth1をリスト3、リスト4のように変更します。また、/etc/sysconfig/networkの内容はリスト5のようになります。

クライアントは図2のネットワーク構成に従ってネットワークの設定をします。方法はPCルーターの場合と同様に、3つのファイルを書き換えます。

サーバーはまず図3のネットワーク構成でネットワークの設定を行ってください。方法は、これもPCルーターと同様に3つのファイルを書き換えます。

ルーティングの設定をしよう

以上の設定が終わった段階では、サーバー

は境界ネット以外のネットワークに属するIPアドレス宛てにIPパケットを送ろうとすると、相手がネットワーク上にないのでルーター(ゲートウェイ)にIPパケットを送ります(図4)。ルーターは受け取ったIPパケットを目的のIPアドレス宛てに送ります(このとき相手がネットワーク上になければ、さらに別のルーターにIPパケットを送ります)。このようにIPパケットをほかのコンピュータに中継させて目的のIPアドレスへ送ることをルーティングといいます。

サーバーがクライアントへIPパケットを送るためには、PCルーターを経由させる必要があります。そこでサーバーに内部ネット向けのIPパケットはPCルーターを経由するように設定します(図5)。このルーティングの設定はスタティックルーティングにします。スタティックルーティングとは、最初に手動で決められたルーティング情報に沿ってルーティングさせることです(これに対し、ルーティング

情報が状況に応じて変化するダイナミックルーティングもあります)。

ファイル/etc/sysconfig/static-routesを作成してリスト6の記述を行います。ファイルstatic-routesはLinuxマシンの起動時に、ディレクトリー/etc/sysconfig/network-scriptsにあるスクリプトの1つであるifup-routesに自動的に読み込まれて処理されます。正しくルーティングが行われたかどうかを確認するには/sbin/route -nを実行します。サーバーのルーティングはリスト7のようになっているはずですが。

PCルーターの動作を確認する

すでにPCルーターのIPフォワーディングをYESにしていますので、現在は、内部ネットにあるクライアントと境界ネットにあるサーバーとでやり取りできているはずですが。確認のためクライアントからサーバーへ、サーバーか

リスト3 PCルーターのifcfg-eth0

```
DEVI CE=eth0
IPADDR=192.168.0.14 ← IPアドレス
NETMASK=255.255.255.0 ← ネットマスク
NETWORK=192.168.0.0 ← ネットワーク
BROADCAST=192.168.0.255 ← ブロードキャスト
ONBOOT=yes
```

リスト4 PCルーターのifcfg-eth1

```
DEVI CE=eth1
IPADDR=192.168.1.1
NETMASK=255.255.255.0
NETWORK=192.168.1.0
BROADCAST=192.168.1.255
ONBOOT=yes
```

リスト5 /etc/sysconfig/network

```
NETWORKING=yes
FORWARD_IPV4=yes ← 前回同様にyesにしておきます
HOSTNAME= ホスト名
DOMAINNAME= ドメイン名
GATEWAY=192.168.0.1
GATEWAYDEV=eth0
```

図2 クライアントのネットワーク構成

IPアドレス	192.168.1.8
ネットマスク	255.255.255.0
ネットワーク	192.168.1.0
ブロードキャスト	192.168.1.255
ゲートウェイ	192.168.1.1

図3 サーバーのネットワーク構成

IPアドレス	192.168.0.10
ネットマスク	255.255.255.0
ネットワーク	192.168.0.0
ブロードキャスト	192.168.0.255
ゲートウェイ	192.168.0.1





[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