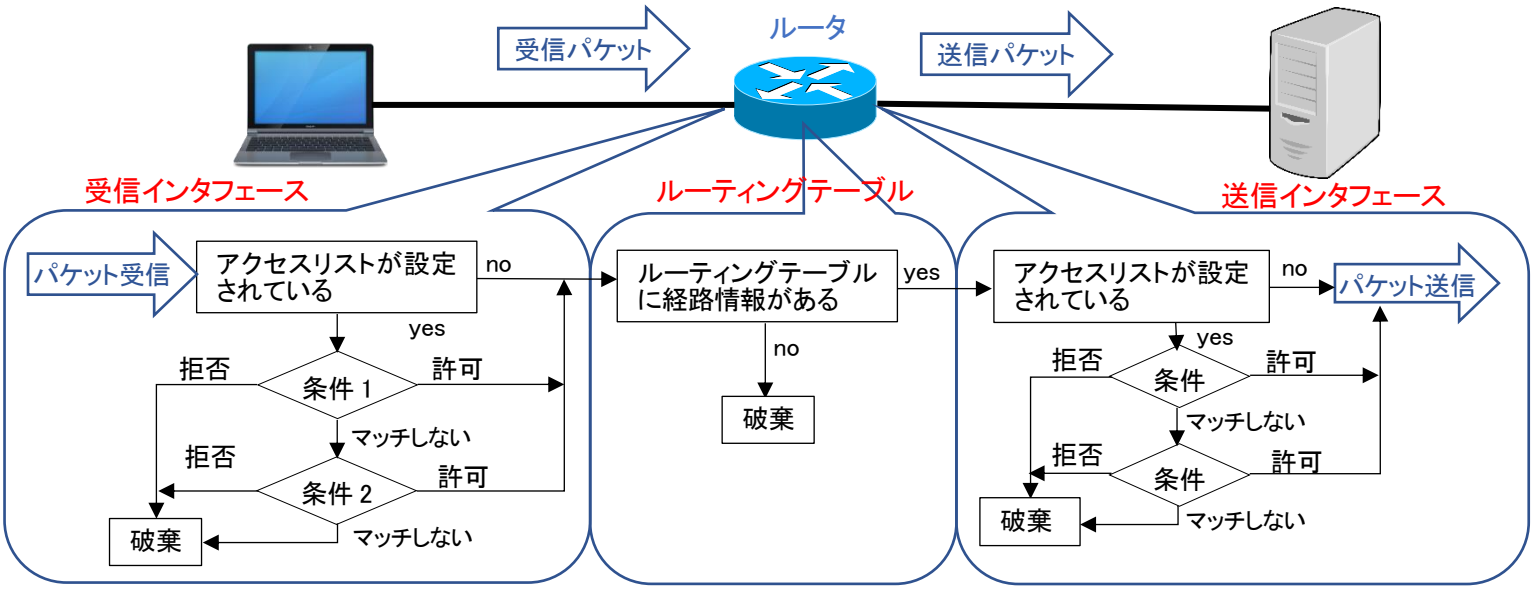
パケットフィルタ

一般的に企業では、システムに侵入するウィルスやクラッカーによる攻撃への対処だけでなく、他部門のサーバーや人事部の機密情報へのアクセスを、特定の社内ユーザに対して制限している。ネットワーク管理者は、広範囲に渡るトラフィックを管理して、セキュリティに対する企業ポリシーを柔軟に適用・管理する必要がある。こうした要求を満たすために、ルータではアクセスリスト(Access List)と呼ばれる機能を使って、事前に定義した条件に基づいてルータのインタフェースで送受信したパケットをチェックし、特定のサーバーやネットワークへのアクセスなどを制限(パケットフィルタリング:Packet Filtering)している。

本実験では、アクセスリストを作成してパケットフィルタリングの動作を確認する。

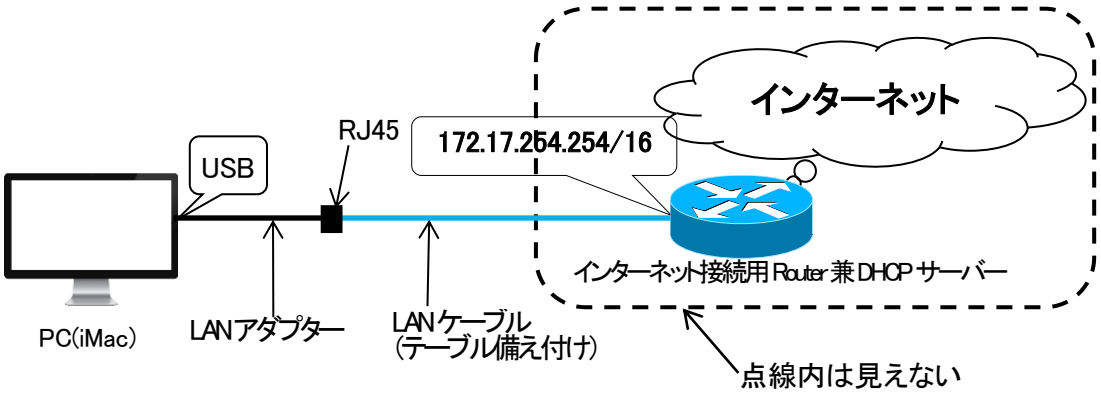


《図1　アクセスリストによるパケットフィルタリング》

1. 準備

(1) インターネット接続確認

図 2 のように PC(iMac)(以下、PC と記す)を接続し、PC の電源を入れて Windows を起動する。Windows 起動後、PC の IP アドレスを DHCP サーバー(172.17.254.254/16)から自動で割り当て、インターネット接続用 Router(172.17.254.254/16)を介して任意 Web サイト(http://www.google.com など)を閲覧する。

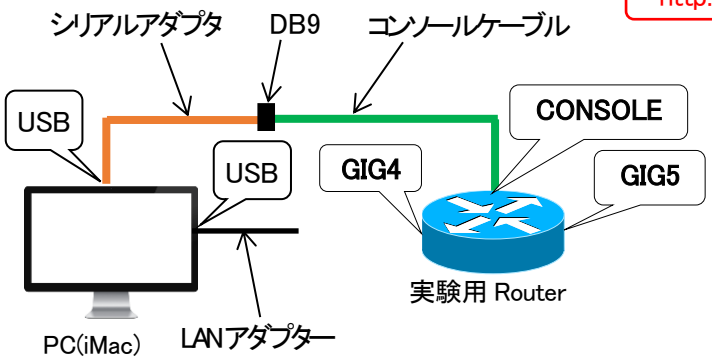


《図 2　機器構成 1》

(2) 実験用 Router(シスコ C841M)(以下、Router と記す)の DHCP 機能の無効化

図 3 のように Router と PC を接続する。このとき、Router の GIG4 と GIG5 には LAN ケーブルを接続しない。次に、第 5 回(5 月 20 日実施)の実験で行った“実験 1 3.Router の接続”の操作手順に従って、通信ソフト(Tera Term)を使用して PC と Router を接続する

http://cobayasi.com/com/5th.pdf



《図 3 機器構成 2》

通常、Router はデフォルトで DHCP(サーバー、クライアント)機能が有効になっている。本実験では、Router に IP アドレスを静的に(手動で)割り付けるために、以下のコマンドを使って DHCP 機能(IP アドレスを自動で割り付ける機能)を無効化する。

＊DHCP サーバー機能の無効化

```
Router(config)#no service dhcp
```

＊DHCP クライアント機能の無効化

Gigabitethernet 0/4 の省略形

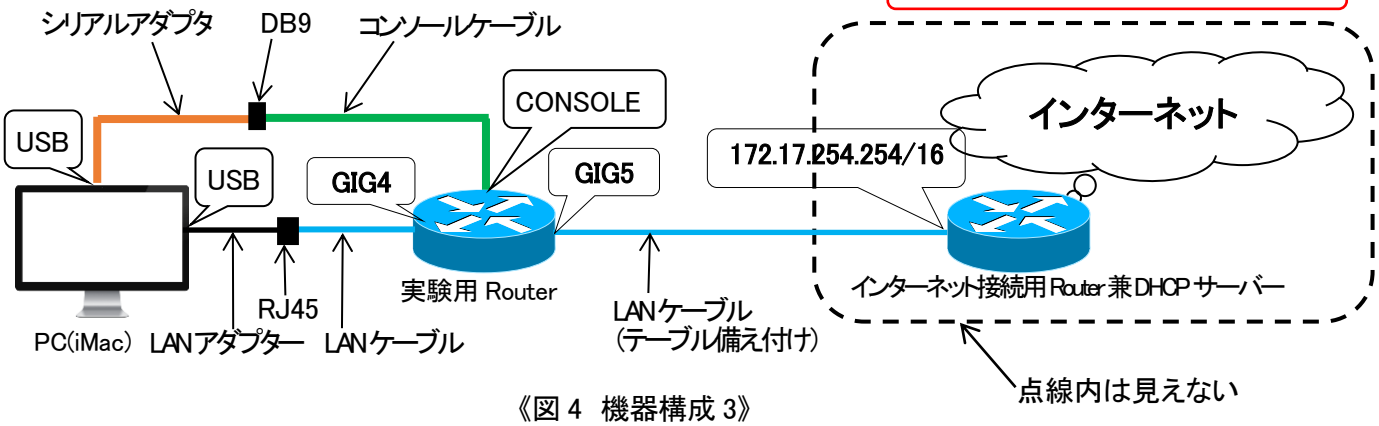
Gigabitethernet 0/5 の省略形

```
Router(config)#interface gig 0/4
Router(config-if)#no service dhcp
Router(config-if)#interface gig 0/5
Router(config-if)#no service dhcp
```

2. 【実験 1】 同じネットワーク内の全ホスト(PC)をインターネットに接続する

(1) 図 4 のように PC と Router 及びインターネット接続用 Router 兼 DHCP サーバーを接続する。次ページに示す<条件>に従って、PC と Router のインタフェース(GIG4,GIG5)に IP アドレスを付け、Router のインタフェースを起動する。操作手順は、第 5 回(5 月 20 日実施)の実験で行った“実験 6 2.IP アドレスの設定 及び 3.インタフェースの起動”。

http://cobayasi.com/com/5th.pdf



《図 4 機器構成 3》

〈条件〉

＊Router
GIG5 の IP アドレス：172.17.181.？
GIG4 の IP アドレス：172.18.0.1
サブネットマスク：255.255.0.0

＊PC
IP アドレス：172.18.0.2
サブネットマスクはすべて 255.255.0.0
デフォルトゲートウェイ：172.18.0.1
優先 DNS サーバー：172.17.254.254
代替 DNS サーバー：不要（空白）

※　？印は、各 PC の IP アドレス（机に貼られた白ラベルの記載番号）

★　この時、Router に設定した以下の①～③のコマンドを実験ノートに記録する。但し、動作モードの移行コマンドは除く。

① GIG4 に IP アドレスとサブネットマスクを設定するコマンドと IP アドレス及びサブネットマスク
② GIG5 に IP アドレスとサブネットマスクを設定するコマンドと IP アドレス及びサブネットマスク
③ インタフェース GIG4 と GIG5 を起動するコマンド

(2) 同じネットワーク内の全ホスト(PC)を指定するためのアクセスリストを作成する。このアクセスリストで指定したパケットだけが Router を通過する（パケットフィルタリング）

本実験の主目的

```
Router(config)#access-list 1 permit 172.18.0.0 0.0.255.255
```

リスト番号(1～99)　対象ホストアドレス　ワールドカードマスク

対象ホストアドレス	172.	18.	0.	0
ワイルドカードマスク（2 進数）	00000000.	00000000.	11111111.	11111111
ワイルドカードマスク（10 進数）	0.	0.	255.	255
条件に合ったホストアドレス	172.	18.	0～255.	1～254

★　この時、Router に設定した④アクセスリストを実験ノートに記録する。但し、動作モードの移行コマンドは除く。

(3) PC のネットワーク(172.18.0.0/16)から他のネットワーク（172.17.0.0/16）へパケットを送信するためのアドレス変換を設定する

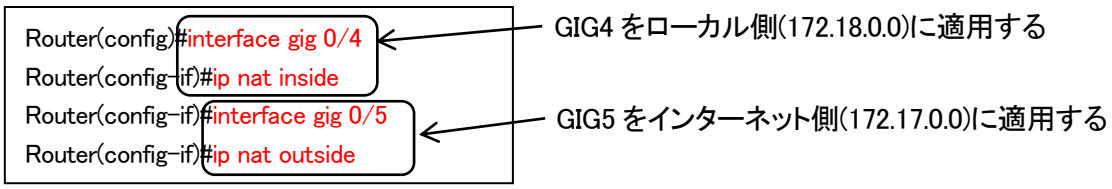
```
Router(config)#ip nat inside source list 1 interface gig 0/5 overload
```

リスト番号(1～99)
※(2)のアクセスリストの番号と同番

インターネット側のインタフェース名

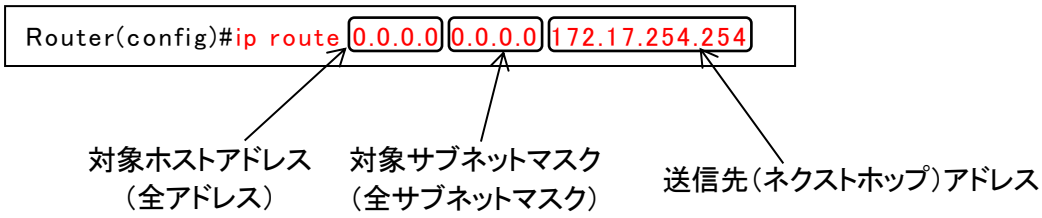
★　この時、Router に設定した⑤アドレス変換コマンドを実験ノートに記録する。但し、動作モードの移行コマンドは除く。

(4) (3)で設定したアドレス変換コマンドを、インタフェース GIG4,GIG5 に適用する(結びつける)。



★ この時、Router に設定した⑥インタフェース適用コマンドを実験ノートに記録する。但し、動作モードの移行コマンドは除く。

(5) PC から送信した全パケットをインターネット側のネットワーク(172.17.0.0/16)へ送るための経路情報を設定する。



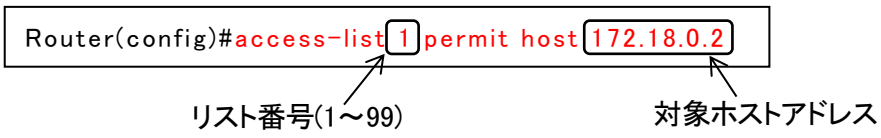
★ この時、Router に設定した⑦経路情報を実験ノートに記録する。但し、動作モードの移行コマンドは除く。

(6) PC からインターネット上の任意 Web サイトが閲覧可能／不可を確認する。
★この⑧結果を実験ノートに記録する。

(7) PC の IP アドレスを以下のように変更し、インターネット上の任意 Web サイトが閲覧可能／不可を確認する。実験終了後、PC の IP アドレスを元のアドレス(172.18.0.2)に戻す。
★この結果を実験ノートに記録する。

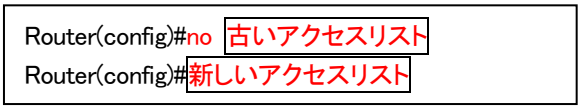
⑨ 172.18.0.3/16
⑩ 172.18.1.3/16
⑪ 172.19.0.2/16

3. 【実験 2】 特定のホスト(PC:172.18.0.2)だけをインターネットに接続する。
(1) 【実験 1】(2)で作成したアクセスリストを削除した後、以下の特定の PC(172.18.0.2)だけを指定するためのアクセスリストを作成して古いアクセスリストと入れ替える。※



★ この時、Router に設定した⑫アクセスリストを実験ノートに記録する。但し、動作モードの移行コマンドは除く。

※ アクセルリストの入れ替えは、以下のように古いアクセスリストを削除した後、新しいアクセスリストを作成する



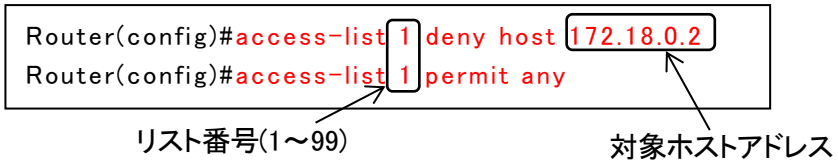
(2) PC からインターネット上の任意 Web サイトが閲覧可能／不可を確認する。また、PC の IP アドレスを以下のように変更し、インターネット上の任意 Web サイトが閲覧可能／不可を確認する。実験終了後、PC の IP アドレスを元のアドレス(172.18.0.2)に戻す。

★ この⑬結果を実験ノートに記録する。また、IP アドレスを変更したときの⑭⑮Web サイトの閲覧結果を実験ノートに記録する。

⑭172.18.0.3
⑮172.18.1.3

4. 【実験 3】 特定のホスト(PC:172.18.0.2)だけをインターネットに接続しない。

(1) 【実験 2】(1)で作成したアクセスリストを削除した後、以下の特定の PC(172.18.0.2)だけを指定除外するためのアクセスリストを作成する。



★ この時、Router に設定した⑯アクセスリストを実験ノートに記録する。但し、動作モードの移行コマンドは除く。

(2) PC からインターネット上の任意 Web サイトが閲覧可能／不可を確認する。また、PC の IP アドレスを以下のように変更し、インターネット上の任意 Web サイトが閲覧可能／不可を確認する。実験終了後、PC の IP アドレスを元のアドレス(172.18.0.2)に戻す。

★ この⑰結果を実験ノートに記録する。また、IP アドレスを変更したときの⑱⑲Web サイトの閲覧結果を実験ノートに記録する。

⑱172.18.0.2
⑲172.18.0.3

5. 【実験 4】 特定のホスト PC(172.18.＊.＊)だけをインターネットに接続するためのアクセスリストとアドレス変換コマンドを作成して Router に設定する。※＊印は偶数(2,4,・・・)を示す。

★ この時、Router に設定した⑳アクセスリストと㉑アドレス変換コマンドと、以下に示す IP アドレスを PC に割り付けた場合の㉒～㉕実験結果を、実験ノートに記録する。

㉒172.18.0.4
㉓172.18.2.2
㉔172.18.0.5
㉕172.18.1.1

＜アクセスリスト作成のヒント＞