第8回　IPアクセスリスト

標準IPアクセスリスト
拡張IPアクセスリスト
アクセスリストの作成と実装

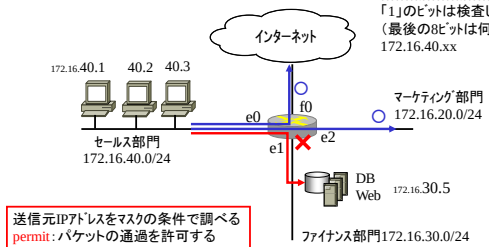
標準IPアクセスリストの例

ファイナンス部門のサーバをセールス部門に見せない

Router (config) #access-list 10 deny 172.16.40.0 0.0.0.255

リスト番号（1~99）　禁止　送信元IPアドレス　ワイルドカードマスク

00000000.00000000.00000000.11111111
「1」のビットは検査しない
（最後の8ビットは何でもよい）
172.16.40.xx



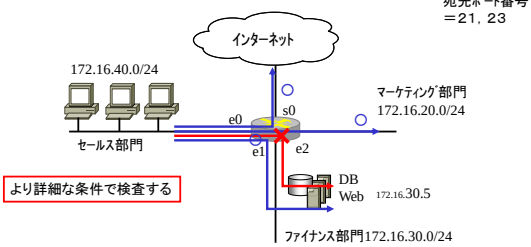
送信元IPアドレスをマスクの条件で調べる
permit：パケットの通過を許可する
deny：パケットの通過を禁止する

拡張IPアクセスリストの例

セールス部門にはファイナンス部門サーバのDB（telnetとFTP）を見せない
ただし，サーバのホームページ閲覧（Webアクセス）は許可したい

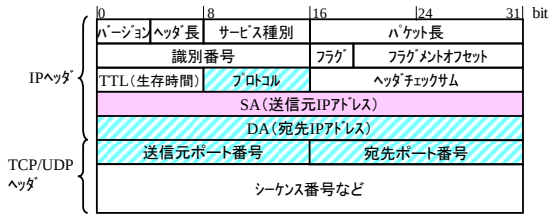
Router(config) #access-list 110 deny tcp 172.16.40.0 0.0.0.255 172.16.30.5 0.0.0.0 eq 21
Router(config) #access-list 110 deny tcp 172.16.40.0 0.0.0.255 172.16.30.5 0.0.0.0 eq 23

リスト番号（100~199）　拒否　プロトコル　送信元IPアドレスとワイルドカードマスク　宛先IPアドレスとワイルドカードマスク　宛先ポート番号＝21，23



より詳細な条件で検査する

アクセスリストの種類とフィルタリングの条件



標準IPアクセスリスト：送信元IPアドレスのみが指定可能
拡張IPアクセスリスト：送信元IPアドレスの他に，宛先IPアドレス，プロトコル，送信元ポート番号，宛先ポート番号の指定が可能

IPアクセスリストの構文

- ネットワークへのアクセスを制御する条件文のリスト
  - 主な目的：パケットのフィルタリング（組織内のネットワークを外部から保護）
- 標準IPアクセスリスト：送信元IPアドレスのみをチェックする
  - access-list number {permit | deny} source [mask]
    - number(注)：1～99の範囲　　注：アクセスリスト番号
  - 例：172.16.40.0/24のホストからのアクセスを拒否
  - Router (config) #access-list 10 deny 172.16.40.0 0.0.0.255
- 拡張IPアクセスリスト：プロトコル，送信元・宛先のIPアドレス・ポート番号をチェックする
  - access-list number {permit | deny} protocol source [mask] [operator port] destination [mask] [operator port] [established] [log]
    - number：100～199の範囲
  - 例：全ての送信元から，ホスト172.16.30.5へのtelnetアクセスを拒否
  - Router(config) #access-list 110 deny tcp any host 172.16.30.5 eq 23
- any＝0.0.0.0 255.255.255.255（何でも良い）
- host 172.16.30.5＝172.16.30.5 0.0.0.0（そのアドレスだけ）

- [　　]を付けたパラメータは，省略しても良い

コマンドのパラメータ

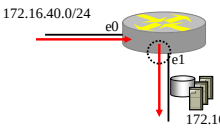
引数	説明
number	アクセスリスト番号． 標準IPアクセスリスト：1～99，拡張IPアクセスリスト：100～199
permit | deny	permit：アクセス許可，　deny：アクセス拒否　どちらか一方を指定
source	送信元IPアドレス
destination	宛先IPアドレス
mask（オプション）	IPアドレスをグループ化するためのマスク．省略時は0.0.0.0
protocol	IP，TCP，UDP，ICMPなどネットワーク層，トランスポート層プロトコルを指定． IPを指定時は，IPを使用する全てのパケットが対象となる
operator port（オプション）	特定のアプリケーション層プロトコルを指定するのに使用する． operator：eq（＝），neq（≠），lt（＜），gt（＞）の何れか一つ port：アプリケーション層プロトコルのポート番号か名前を指定
Established（オプション）	Ackビットがオンの TCPセグメントを全て許可する．TCPのインバウンドにのみ有効．Ackを拒否することによる通信不可の防止．
log（オプション）	条件に該当するパケットをlogに記録する

IPアクセスリストの実装（1）

```
Router #config t
Router(config) #access-list 10 deny 172.16.40.0  0.0.0.255
Router(config) #access-list 10 permit any
Router(config) #int e1
Router(config-if) #ip-access-group  10 out
```

この条件文が無いと，暗黙のdenyにより，全ﾊﾟｹｯﾄが廃棄される
（条件文にpermitがある場合は，不要）

e1から出る（ｱｳﾄﾊﾞｳﾝﾄﾞ）ﾊﾟｹｯﾄに対し，
ﾘｽﾄ番号10の条件を実装



仮に，上記のﾘｽﾄをe0の入り口に適用すると
172.16.40.0/24からの全ﾊﾟｹｯﾄが拒否される
（このｻﾌﾞﾈｯﾄは外との通信ができない）

access-listｺﾏﾝﾄﾞにより，指定番号ﾘｽﾄの条件文が1行ずつ追加される．
ﾊﾟｹｯﾄが通過する度に，1行目から順に，条件と合致するかを調べ，通過をpermit（許可）またはdeny（拒否）．

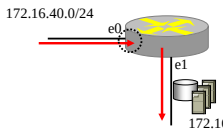
暗黙のdeny
全ての条件に合致しないﾊﾟｹｯﾄは通過をdeny（拒否）される．

IPアクセスリストの実装（2）

```
Router #config t
Router(config) #access-list 110 deny tcp any host 172.16.30.5  eq 21
Router(config) #access-list 110 deny tcp any host 172.16.30.5  eq 23
Router(config) #access-list 110 permit ip any any
Router(config) #int e0
Router(config-if) #ip-access-group  110 in
```

暗黙のdenyを打ち消す場合，
拡張IPｱｸｾｽﾘｽﾄでは，
permit ip any anyとする．

e0に入る（ｲﾝﾊﾞｳﾝﾄﾞ）ﾊﾟｹｯﾄに対し，
ﾘｽﾄ番号110の条件を適用



ｻﾌﾞﾈｯﾄの全ﾎｽﾄに対し，ｲﾝﾊﾞｳﾝﾄﾞに適用する場合，送信元IPｱﾄﾞﾚｽは，
any（何でも良い）の場合が多い．
（ﾁｪｯｸ条件が緩い方が，ﾙｰﾀの負荷が小さい）

ポート番号とプロトコル

RouterA (config)#access-list 110 deny tcp any host 172.16.30.2 eq ？
<0-65535>　　Port number

bgp	Border Gateway Protocol (179)	login	Login (rlogin, 513)
chargen	Character generator (19)	lpd	Printer service (515)
cmd	Remote conunands (rcmd, 514)	nntp	Network News Transport Protocol (119)
daytime	Daytime (13)	pim-auto-rp	PIM Auto-RP (496)
discard	Discard (9)	pop2	Post Office Protocol v2 (l09)
domain	Domain Name Service (53)	pop3	post Office Protocol v3 (110)
echo	Echo (7)	**smtp**	**Simple Mail Transport Protocol (25)**
exec	Exec (rsh, 512)	sunrpc	Sun Remote Procedure Call (111)
finger	Finger (79)	syslog	Syslog (514)
ftp	**File Transfer Protocol (21)**	tacacs	TAC Access Control System (49)
ftp-data	FTP data connections (20,21)	talk	Talk (517)
gopher	Gopher (70)	**telnet**	**Telnet (23)**
hostname	NIC hostname server (101)	time	Time (37)
ident	Ident Protocol (113)	uucp	Unix-to-Unix Copy Program (540)
irc	Internet Relay Chat (194)	whois	Nicname (43)
klogin	Kerberos login (543)	**www**	**World Wide Web (HTTP, 80)**
kshell	Kerberos shell (544)		

赤字のプロトコルとポート番号は覚えよう

標準IPアクセスリストの例（1）

ﾘｽﾄ番号
↓　拒否　発ｱﾄﾞﾚｽ　ﾜｲﾙﾄﾞｶｰﾄﾞﾏｽｸ

```
access-list 10 deny 192.168.20.0 0.0.0.255        1行目
access-list 10 deny 192.168.30.0 0.0.0.255        2行目
access-list 10 deny 192.168.40.0 0.0.0.255        3行目
access-list 10 permit any                         4行目
            許可　全てのﾊﾟｹｯﾄ
```

外向き
```
int e0
ip access-group 10 out
```

内向き
```
int e0
ip access-group 10 in
```

比較ﾙｰﾙ
・ﾘｽﾄ上の条件文順に比較（1行目，2行目，3行目・・・）
・ある行と一致⇒その行のアクションを実行，比較終了
・ﾘｽﾄの最後には，暗黙のdeny（どの行にも不一致⇒廃棄）

標準IPアクセスリストの例（2）

```
access-list 10 deny 172.16.0.0 0.0.255.255
access-list 10 permit any
```

ﾜｲﾙﾄﾞｶｰﾄﾞﾏｽｸ値　:255　その8ﾋﾞｯﾄを検査しない（何でも良い）
　　:0　その8ﾋﾞｯﾄが一致するかを検査
　　詳しい説明は，次のｽﾗｲﾄﾞを参照

上のﾘｽﾄは，ﾈｯﾄﾜｰｸ172.16.0.0上の全ﾎｽﾄからのﾊﾟｹｯﾄを廃棄

```
access-list 10 deny host 172.16.30.2
access-list 10 permit any
```
または
```
access-list 10 deny 172.16.30.2 0.0.0.0
access-list 10 permit any
```
同じ意味

ﾎｽﾄ172.16.30.2からのﾊﾟｹｯﾄを廃棄

ワイルドカードマスク

2進数のマスク値：「0」のビットは値の一致を検査，「1」のビットは検査しない

（1）アドレスの全ビット（32ビット）の値が一致
```
RouterA(config)#access-list 10 deny 172.16.30.5 0.0.0.0
```
同じ意味
```
RouterA(config)#access-list 10 permit host 172.16.30.5
RouterA(config)#access-list 10 permit 172.16.30.5
```

（2）アドレスの最後の8ビットはどんな値でもマッチする（条件に合う）
```
RouterA(config)#access-list 10 deny 172.16.30.0 0.0.0.255
```

（3）どんな値でもマッチする
```
RouterA(config)#access-list 10 permit 0.0.0.0 255.255.255.255
```
同じ意味
```
RouterA(config)#access-list 10 permit any
```

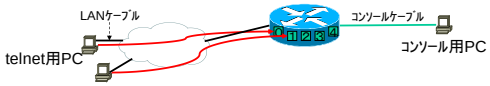
（4）アドレスの第4オクテットの値が0～63だったらマッチする
```
RouterA(config)#access-list 10 permit 172.16.30.0 0.0.0.63
```
63=00111111　上位2ビット一致　00000000～00111111
00xxxxxx　下位6ビット何でも良い　0　～　63

（5）アドレスの第4オクテットが，128～135だったらマッチする
```
RouterA(config)#access-list 10 permit 172.16.30.128 0.0.0.7
```
7=00000000　上位5ビット一致　10000000～10000111
10000xxx　下位3ビット何でも良い　128　～　135

VTYの設定とtelnetログイン

4.8節(p.211)

- VTY：Virtual TeletYpe（仮想遠隔端末）
  （Virtual Terminal Lineの略という説もある。Yが何の略かは不明）
  - Ciscoルータには，5個（0，1，2，3，4）のVTY回線がある
  - 同時に5つのホストが接続できる（空いているVTY回線を割り当て）



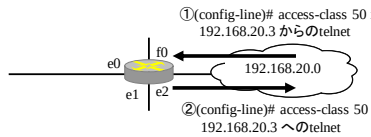
- telnetを可能とするための設定（コンソール用PCから）
  - (config)# line vty 0 4　ラインコンフィグモードにする（0～4のポートに設定）
  - (config-line)# login　ログイン時のパスワードチェック有効化
  - (config-line)# password xxxxxx　←認証用パスワード文字列
- コマンドプロンプトからのtelnetログイン（telnet用PCから）
  - C:¥>telnet 192.168.11.1
  - password: xxxxxxxx
  - Router>

ルータの場合：インタフェースのIPアドレス
スイッチの場合：管理用IPアドレス

アクセスクラスの設定（VTYアクセス制御）

192.168.20.3のホストだけが，telnet許可
Router (config) # access-list 50 permit 192.168.20.3
Router (config) # line vty 0 4
Router (config-line) # access-class 50 in
　他のホストは全部拒否なので，暗黙のdenyのままで良い（permit anyは不要）
　内向きに50番リストを適用（192.168.20.0→VTYポートの方向）

内向き（インバウンド）と外向き（アウトバウンド）



注：access-groupは，ルータから発生するトラフィックは規制できない
　access-classは，ルータのVTYポートから発生するTelnetトラフィックが規制できる

アクセスリスト実装時の注意点

・インタフェース毎，プロトコル毎，方向毎にそれぞれ1つ設定できる
（例：IPアクセスリストは，各インタフェース毎に内向き，外向き各1つ）
・より具体的な条件はリストの一番上に
・新しいエントリは，常にリストの一番下に追加される．
・1行の削除は不可（リスト全体を削除）．編集前に，エディタにコピー
（唯一の例外は，名前付きアクセスリスト）
・条件文中にpermitが無い場合，最後にpermit anyのエントリが必要
（これが無いと，暗黙のdenyにより，全パケットが破棄される）
・リストを作ってからインタフェースに適用
・access-group：外から受信したパケットのみ比較（ルータ発のパケットはスルー）

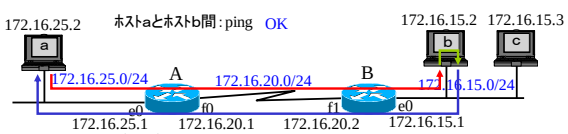
一般原則として（例外あり），
・標準IPアクセスリストはできるだけ宛先に近いところに
・拡張IPアクセスリストはできるだけ送信元に近いところに

IPアクセスリストの確認

コマンド	ルストの内容	適用インタフェース	備考
show access-list(注)	○	×	アクセスリストの内容を表示
show ip access-list (注)	○	×	同上（但しipアクセスリストのみ）
show ip interface	×	○	インタフェースに適用されたリスト番号を確認
show running-config	○	○	configの全情報

注：リスト番号を指定するとその番号のリストのみを表示（省略時は，全リストを表示）

ルーティングの確認



ルータAのルーティングテーブル

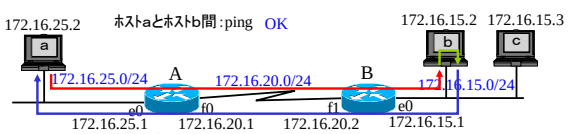
```
C   172.16.20.0/24 is directly connected, FirstEthernet0
C   172.16.25.0/24 is directly connected, Ethernet0
S   172.16.15.0/24 [1/0] via 172.16.20.2
```

ゲートウェイのIPアドレス（中継ルータのIPアドレス）
メトリック（RIPの場合はホップ数）
アドミニストレーティブディスタンス
宛先サブネット
スタティックルートの表示（スタティックルーティングで設定したルート）

ルータBのルーティングテーブル

```
C   172.16.15.0/24 is directly connected, Ethernet0
C   172.16.20.0/24 is directly connected, FirstEthernet1
S   172.16.25.0/24 [1/0] via 172.16.20.1
```

ルーティングの確認



ルータAのルーティングテーブル

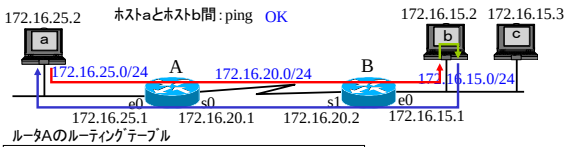
```
C   172.16.20.0/24 is directly connected, FirstEthernet0
C   172.16.25.0/24 is directly connected, Ethernet0
S   172.16.15.0/24 [1/0] via 172.16.20.2
```

④メトリック（RIPの場合はホップ数）
⑤ゲートウェイのIPアドレス（中継ルータのIPアドレス）
③アドミニストレーティブディスタンス
②宛先サブネット
①スタティックルートの表示（スタティックルーティングで設定したルート）

ルータBのルーティングテーブル

```
C   172.16.15.0/24 is directly connected, Ethernet0
C   172.16.20.0/24 is directly connected, FirstEthernet1
S   172.16.25.0/24 [1/0] via 172.16.20.1
```

ルーティングの確認

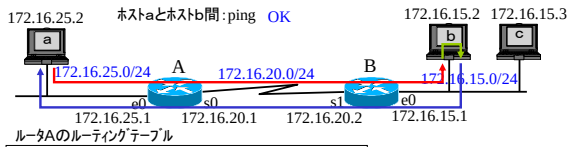


ルータAのルーティングテーブル

```
C   172.16.20.0/24 is directly connected, FirstEthernet0
C   172.16.25.0/24 is directly connected, Ethernet0
S   172.16.15.0/24 [1/0] via 172.16.20.2
```

期末試験予想問題
ルータBのルーティングテーブルを書け

ルーティングの確認



ルータAのルーティングテーブル

```
C   172.16.20.0/24 is directly connected, FirstEthernet0
C   172.16.25.0/24 is directly connected, Ethernet0
S   172.16.15.0/24 [1/0] via 172.16.20.2
```

期末試験予想問題
ルータBのルーティングテーブルを書け

```
C   172.16.15.0/24 is directly connected, Ethernet0
C   172.16.20.0/24 is directly connected, FirstEthernet1
S   172.16.25.0/24 [1/0] via 172.16.20.1
```