Ciscoネットワーク演習2　第12週　　 クラス　　　　番号　　　　氏名

• +2 –ACL

今回学ぶこと

**ACL：**アクセスリスト(ACL)の設定について学びます

ACLの設定

ACL(Access Control List)

ACL（アクセス制御リスト）は、トラフィックフィルタリングの最も一般的な手法の一つです。ACLの主な目的は、許可または拒否するパケットの種類を特定することにあります。ACLは、NATで使用される内部ホストの指定、QoS（Quality of Service）やキューイングなどの高度な機能のためのトラフィックの識別や分類、ルーティングの更新内容の制限、デバッグ出力の制限、仮想端末を介したルータへのアクセス制御など、多岐にわたる用途で使用されます。ACLはパケットの内容を分析し、そのパケットを許可するか、ブロックするかを決定します。主に標準ACLと拡張ACLの2種類があります。

標準ACLと拡張ACL

標準ACLは、送信元IPアドレスに基づいてトラフィックを制御します．これにはリスト番号1～99および1300～1999が使用されます．標準ACLは、通常、トラフィックの宛先に近いルータに設置されます．

一方、拡張ACLでは、送信元と宛先のIPアドレス、ポート番号などを基にしたより詳細な制御が可能です．拡張ACLのリスト番号は100～199および2000～2699の範囲にあります．拡張ACLは、トラフィックの送信元に近いルータに設置されることが一般的です．

標準ACLの設定(リストの作成手順)

　①リストの作成（グローバル設定モード）

**Router(config)#access-list** *番号***｛permit｜deny｝***送信元IPアドレス ワイルドカードマスク*

<例> **access-list 1 permit 192.168.1.0 0.0.0.255**　（192.168.1.0のネットワークだけ許可する）

　②インターフェイスにリストを適用（インターフェイスモード）

**Router(config-if)#ip access-group** *番号* **{in｜out}**

<例>ip access-group 1 in　(受信したパケットにリスト1を適用する)

　＊デフォルトはout（省略した場合は、out設定になる）

※内部論理  
ACLの内部論理では、リストは最初の行から順に比較されます。リスト内の項目がパケットに一致した時点で、それ以上の比較は行われず、リストの処理は終了します。該当する項目がリスト内に存在しない場合、リストの最後には「暗黙のdeny」が適用され、その結果パケットは拒否されます。

※ワイルドカードマスク  
複数アドレスやアドレス範囲をブロックするために、ワイルドカードマスクを使用します．ワイルドカードマスクを使用すると、より柔軟性が得られます．

・ワイルドカードマスクの例

　ワイルドカードマスク　0・・・一致、1・・・無視

　<例>192.168.10.0 0.0.0.255　⇒　192.168.10.0/24ネットワークのすべてのホスト

10.1.0.0 0.0.255.255　⇒　10.1.0.0/16ネットワークのすべてのホスト

200.1.10.5 0.0.0.0　⇒　200.1.10.5のホストのみ

・ワイルドカードマスクのキーワード(特殊なパラメータ)

**host**・・・ホスト示す、ワイルドカードの0.0.0.0と同じ意味を持つ．

**any**・・・すべてを示す、ワイルドカードの255.255.255.255と同じ意味を持つ．

<例>host 200.1.10.5　＝　200.1.10.5 0.0.0.0

標準ACLの確認

**show ip interface** ・・・リストを適用したインターフェイスの状態を表示

**show ip access-lists** ・・・IPアクセスリストを表示

**show access-lists *番号***・・・番号のアクセスリストを表示(番号を省略するとすべてのリスト)

拡張アクセスリスト

拡張アクセスリストは、標準ACLよりも詳細なトラフィック制御を可能にします。これには、送信元と宛先のIPアドレス、TCPやUDPなどのプロトコルタイプ、さらにはポート番号まで指定できます。拡張ACLは、リスト番号100～199および2000～2699で定義され、特にセキュリティが重視される環境で有効です。

・拡張ACLの設定(リストの作成手順)

①リストの作成（グローバル設定モード）

　　Router(config)#access-list 番号 {permit｜deny} プロトコル 送信元IPアドレス ワイルドカードマスク 宛先IPアドレス ワイルドカードマスク

　　<例> access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 80 （192.168.1.0/24からのHTTPトラフィックを許可）

②インターフェイスにリストを適用（インターフェイスモード）

　　Router(config-if)#ip access-group 番号 {in｜out}

　　<例> ip access-group 101 in （受信したパケットにリスト101を適用）

拡張ACLの利用シナリオは様々であり、特にDMZや企業の内部ネットワーク間のセキュリティを高めるために用いられます。また、拡張ACLはトラフィックの**送信元に近いルータに設置**されることが多く、不正アクセスの防止やネットワークリソースへのアクセス制御に効果的です。

拡張ACLの確認

・show ip interface ・・・リストを適用したインターフェイスの状態を表示

・show ip access-lists ・・・IPアクセスリストを表示

・show access-lists 番号 ・・・番号のアクセスリストを表示（番号を省略するとすべてのリストを表示）

拡張ACLは、その柔軟性と精度の高さから、ネットワークセキュリティの設計において重要な役割を果たします。適切に設定された拡張ACLは、ネットワークへの不正アクセスを効果的に防ぎながら、必要なトラフィックの流れを確保することができます。

名前付きアクセスリスト

名前付きアクセスリスト（ACL）は、標準ACLと拡張ACLの両方で使用できる、より柔軟なACL設定方法です。名前付きACLでは、リストに具体的な名称を付けることができ、管理や変更が容易になります。

標準ACLの名前付きリスト

名前付きの標準ACLでは、送信元IPアドレスに基づいてトラフィックを制御します。リストは明示的な名前を持ち、特定のIP範囲を許可または拒否するルールを含めることができます。  
名前付きの標準ACLも、標準ACLと同じくトラフィックの宛先に近いルータに設置されます．

設定手順

1. リストの作成（設定モード）:

ip access-list standard [リスト名]

2. ルールの追加:

permit または deny [送信元IPアドレス] [ワイルドカードマスク]

3. インターフェイスにリストを適用（インターフェイスモード）:

ip access-group [リスト名] {in｜out}

設定例：リスト名：ACL-Test、送信元10.16.10.0/24からのトラフィックを許可、  
**Router(config)#ip access-list standard ACL-Test  
Router(config-std-nacl)#permit 10.16.10.0 0.0.0.255  
Router(config-std-nacl)#exit  
Router(config)#int g0/0  
Router(config-if)#ip access-group ACL-Test in**

□名前付き標準ACLの設定練習（Packet Tracerでやってみよう）

ファイル「ITN+2-3SACLs.pkt」を開きましょう

1.「PC(192.168.1.10)」の「Command Prompt」からnara(172.22.30.2)へpingコマンドを実行する

　　[　接続できた　]

2.「192.168.1.0/24」ネットワークからnara(172.22.30.2)への接続を標準ACLで禁止する

　①アクセスリストを設定するルータは・・・[　　Nara　　]

②ルータにアクセスリストを設定する(ACL名：STOP-PC1)

Ip access-list standard STOP-PC1

Deny 192.168.1.0 0.0.0.255

Permit any

exit

③アクセスリストを適用したインターフェイス・・・[　　g0/1　　]

3.「PC1」からのアクセスができないかpingで確認する

　　[　接続できない　]

確認後「no ip access-list standard STOP- PC1」でアクセスリストを削除する

4.「192.168.1.10」と「192.168.1.11」からのpingのみ禁止するアクセスリストにSTOP-PC1-PC2　  
リスト名はSTOP-PC1-PC2

ip access-list standard STOP-PC1-PC2

Deny 192.168.1.10 0.0.0.0

Deny 192.168.1.11 0.0.0.0

Permit any

exit

設定後、PC1(192.168.1.10)からnara(172.22.30.2)にping　[できない]  
PC2(192.168.1.11)からnara(172.22.30.2)にping　[できない]

Switch(192.168.1.100)からnara(172.22.30.2)にping　　 [できた]

**【チェック1】上記の接続確認を教員にチェックしてもらうこと**

5.「ITN+2-3SACLsクラス名前.pkt」で保存し、提出しなさい．

拡張ACLの名前付きリスト

名前付きの拡張ACLでは、送信元と宛先のIPアドレス、プロトコルタイプ、ポート番号を使用して、より詳細なトラフィック制御が可能です。

設定手順

1. リストの作成（グローバル設定モード）:

ip access-list extended [リスト名]

2. ルールの追加:

permit または deny [プロトコル] [送信元IPアドレス] [ワイルドカードマスク] [宛先IPアドレス] [ワイルドカードマスク]

プロトコル： ip、tcp、udp、icmp(tcpとudpではポート番号の指定が可能)

3. インターフェイスにリストを適用（インターフェイスモード）:

ip access-group [リスト名] {in｜out}  
設定例：リスト名：EX-ACL  
送信元10.100.0.0/24から宛先192.168.10.0/24へのトラフィックをブロック  
送信元10.100.10.0/24から宛先192.168.10.1/32へのpingをブロック  
送信元192.168.1.0/24から宛先200.100.1.0/24へのWeb通信を許可  
送信元192.168.1.1/32からの全てのpingを許可

その他の通信は許可(リストにdeny設定がある場合、必ずその後にpermit設定が必要になります) インターフェイスｇ0/0の入力方向にＡＣＬの適用

**Router(config)#ip access-list extended EX-ACL  
Router(config-ext-nacl)#deny ip 10.100.0.0 0.0.0.255 192.168.10.0 0.0.0.255  
Router(config-ext-nacl)#deny icmp 10.100.10.0 0.0.0.255 host 192.168.10.1  
Router(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 200.100.1.0 0.0.0.255 eq 80**

**Router(config-ext-nacl)#permit icmp host 192.168.1.1 any   
Router(config-ext-nacl)#****permit ip any any  
Router(config-ext-nacl)#exit  
Router(config)#int g0/0  
Router(config-if)#ip access-group EX-ACL in**

名前付きACLの使用は、特に大規模なネットワークや複数のACLを管理する必要がある場合に便利です。リストに具体的な名前をつけることで、その目的や適用範囲が一目で理解しやすくなります。

□名前付き拡張ACLの設定練習（Packet Tracerでやってみよう）

ファイル「ITN+2-4EACLs.pkt」を開きましょう

1.「v01」の「Web Browser」からWeb Server(177.10.1.2)へ　アクセスする(URLにアドレスを入力)

　　　[　接続できた ]

2.「v01(192.168.1.10)」からWeb Server(177.10.1.2)へWebへの接続を禁止する

　①アクセスリストを設定するルータは・・・[　　　NARA　　　　]

　②ルータにアクセスリストを設定する(リスト名はSTOP-WEB)

Ip access-list **extended** STOP-WEB

Deny tcp host 192.168.1.10 host 177.10.1.2 eq 80

Permit ip any any

Exit

int g0/0

ip access-group STOP-WEB in

　③アクセスリストを適用したインターフェイス・・・[　　　G0/0　　　]

3.「ｖ01」からのアクセスができないか「Web Browser」で確認する

　　　[ 確認できない　]

4.「ｖ02」からのアクセスができるか「Web Browser」で 確認する

　　[　確認できた　]

5.現在設定されているアクセスリストを表示する。

　コマンド：[　show ip access-lists　]

　結果：

Standard IP access list STOP-WEB

10 deny host 192.168.1.10 (12 match(es))

20 permit any (26 match(es))

**【チェック2】上記の表示結果を教員にチェックしてもらうこと**

6.「ITN+2-4EACLsクラス名前.pkt」で保存し、提出する

**未チェックの場合はこのwordファイルも提出すること。**

参考：VTYへのアクセスリストの適用  
VTY（Virtual Terminal Lines）へのアクセスリストの適用は、リモートアクセス（特にSSH）を制御する上で重要なセキュリティ対策となります．VTYラインへのアクセスリストの適用により、特定のIPアドレスからの接続のみを許可し、不正アクセスを防ぐことが可能です．

VTYへのアクセスリストの適用

手順

① アクセスリストの作成

まず、特定のIPアドレスからのSSH接続を許可するアクセスリストを作成する．  
ここでは、宛先はVTYへの入力方向と確定しているため標準アクセスリストを使用．

例（名前付き標準ACL）: 192.168.10.0/24のネットワークからのSSH接続のみを許可

**Router(config)#ip access-list standard SSH-ACCESS**

**Router(config-std-acl)#permit 192.168.10.0 0.0.0.255**

②VTYラインへのアクセスリストの適用

次に作成したアクセスリストをVTYライン(SSH接続)に適用する．

**Router(config)#line vty 0 4** #VTYラインを指定

**Router(config-line)#access-class SSH-ACCESS in** #アクセスリストSSH-ACCESSを入力方向に適用

まとめ：

この設定により、指定されたIPアドレス範囲外からのSSH接続試行はすべて拒否されます。(192.168.10.0/24からのSSH接続のみ許可され、範囲外からのSSHアクセスは「暗黙のdeny」によりすべて拒否)．ネットワークのセキュリティが向上し、不正アクセスのリスクが減少します．

注意点：

ACL名への大文字の使用：ACLの名前に大文字を使用(全て大文字でなくても、Camel形式での使用も含む)することで、小文字の他の設定と視覚的に区別しやすくなります(ACL名に小文字が使用できないわけではなく、慣習的なものです)．

アクセスリストの設計: 許可するIPアドレス範囲を正確に定義することが重要です。  
間違った設定は、正当なユーザーのアクセスをブロック、正当ではないユーザーにアクセスする機会を与える可能性があります。

セキュリティ対策の一環として: VTYラインへのアクセスリストの適用は、ネットワークセキュリティの総合的な戦略の一部であるべきです。他のセキュリティ対策と組み合わせることが重要です。VTYラインへのアクセスリストの適用は、リモートアクセスのセキュリティを強化するための基本的かつ効果的な手段です。