

一般的に使用される IP ACL の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[特定のホストによるネットワークアクセスの許可](#)

[特定のホストによるネットワークアクセスの拒否](#)

[連続した IP アドレスの範囲へのアクセスの許可](#)

[Telnetトラフィック\(TCP、ポート23\)を拒否する方法](#)

[内部ネットワークだけにTCPセッションを始めさせる方法](#)

[FTPトラフィック\(TCP、ポート21\)を拒否する方法](#)

[FTPトラフィックの許可\(アクティブ FTP\)](#)

[FTPトラフィックの許可\(パッシブ FTP\)](#)

[pingの許可\(ICMP\)](#)

[HTTP、Telnet、Mail、POP3、FTPの許可](#)

[DNSの許可](#)

[ルーティングの更新を許可する](#)

[ACLに基づくトラフィックのデバッグ](#)

[MACアドレスフィルタリング](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、IPパケットをフィルタリングする、一般的に使用されるIPアクセスコントロールリスト(ACL)の設定例について説明します。

前提条件

要件

この設定を開始する前に、次の要件が満たされていることを確認してください。

- IP アドレッシングに関する基本的な知識。

詳細は、『[IP のアドレッシングとサブネット化について \(新規ユーザ向け\)](#)』を参照してください。

い。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

IPアクセスコントロールリスト(ACL)は、次の項目に基づいてパケットをフィルタリングします。

- 送信元アドレス
- 宛先アドレス
- パケットの種類
- 上記の項目の組み合わせ

ACLでは、ネットワークトラフィックをフィルタリングするために、ルーティング対象のパケットをルータ インターフェイスで転送するかブロックするかが制御されます。ルータでは各パケットが検査され、ACLで指定された条件に基づいて、パケットを転送するかドロップするかが判断されます。ACLの条件には、次のものがあります。

- トラフィックの送信元アドレス
- トラフィックの宛先アドレス
- 上位層プロトコル

このドキュメントの例に示すように ACL を構成するには、次の手順を実行します。

1. ACL を作成する。
2. ACL をインターフェイスに適用する。

IP ACL は、IP パケットに適用される許可/拒否条件の連続的な集まりです。ルータは、一度に 1 つずつ ACL 内の条件とパケットを照らし合わせてテストします。

Cisco IOS® ソフトウェアがパケットを受け入れるか拒否するかは、最初に一致した条件に基づいて決定されます。Cisco IOSソフトウェアでは、最初の一一致後に条件のテストを停止するため、条件の順序は重要です。一致する条件が 1 つもないと、ルータでは暗黙的な deny all 句によりパケットが拒否されます。

次に、Cisco IOS ソフトウェアで設定できる IP ACL の例を示します。

- 標準 ACL
- 拡張 ACL
- ダイナミック (ロック アンド キー) ACL

- IP 名前付き ACL
- 再帰 ACL
- 時間範囲を使用する時間ベース ACL
- コメント付き IP ACL エントリ
- コンテキストベース ACL
- 認証プロキシ
- ターボ ACL
- 分散型時間ベース ACL

この文書では、一般的に使用される標準 ACL と拡張 ACL について説明します。Cisco IOS ソフトウェアでサポートされている各種の ACL の詳細と、ACL の設定方法および編集方法については、『[IP アクセスリストの設定](#)』を参照してください。

標準 ACL のコマンド構文の形式は、`access-list access-list-number {permit|deny} {host|source source-wildcard|any}` です。

標準 ACL では、トラフィックを制御するために、IP パケットの送信元アドレスと ACL に設定されたアドレスが比較されます。

拡張 ACL では、トラフィックを制御するために、IP パケットの送信元アドレスおよび宛先アドレスと ACL に設定されたアドレスが比較されます。また、拡張 ACL をさらに詳細に設定すると、次のような条件に基づいてトラフィックをフィルタリングできます。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことを、ご了承ください。

- プロトコル
- ポート番号
- Differentiated Services Code Point (DSCP; DiffServ コード ポイント) 値
- 優先順位値
- 同期シーケンス番号 (SYN) ビットの状態

拡張 ACL のコマンド構文の形式は次のとおりです。

IP

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} protocol source source-wildcard destination destination-wildcard
[precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

インターネット制御メッセージ プロトコル (ICMP)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} icmp source source-wildcard destination destination-wildcard
[[icmp-type] [icmp-code] | [icmp-message]] [precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

Transport Control Protocol (TCP; トランスポート制御プロトコル)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} tcp source source-wildcard [operator [port]] destination destination-wildcard [operator
[established] [precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

ユーザ データグラム プロトコル (UDP)

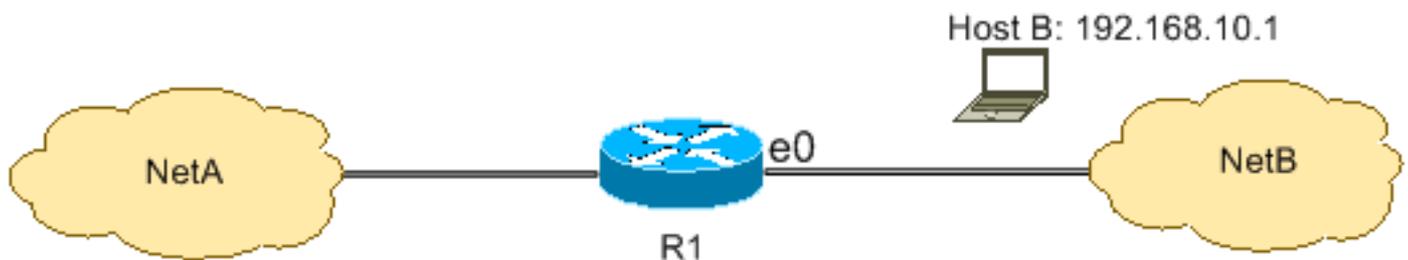
```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} udp source source-wildcard [operator [port]] destination destination-wildcard [operator
[precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

設定

このセクションの設定例では、最も一般的な IP ACL を使用しています。

特定のホストによるネットワーク アクセスの許可

次の図は、選択したホストにネットワークへのアクセス許可が付与されていることを示しています。Host B から発信された NetA 宛てのトラフィックはすべて許可されますが、NetB から発信された NetA 宛ての他のトラフィックはすべて拒否されます。



R1 の表に掲載されている出力は、このホストがネットワークへのアクセスをどのように許可されるかを示しています。この出力は、次のことを示しています。

- この設定では、IP アドレス 192.168.10.1 を持つホストだけが、R1 の Ethernet 0 インターフェイスを通過することを許可されています。
- このホストは、NetA の IP サービスにアクセスできます。
- NetB 内のその他のホストは NetA にアクセスできません。
- この ACL には deny 文が設定されていません。

デフォルトでは、すべての ACL の最後に暗黙的な deny all 句が存在します。明示的に許可されて

いないトラフィックはすべて拒否されます。

R1

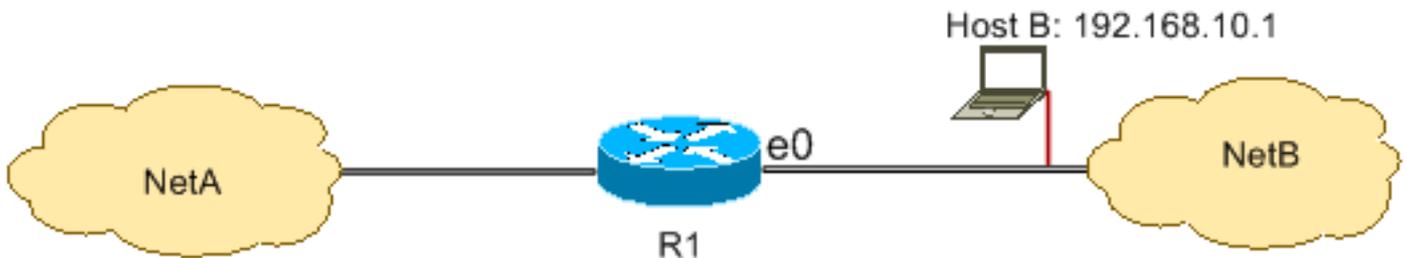
```
hostname R1
!  
interface ethernet0  
 ip access-group 1 in  
!  
access-list 1 permit host 192.168.10.1
```

 注:ACLでは、ホストBから発信されたパケットを除き、NetBからNetAへのIPパケットがフィルタリングされます。ホストBからNetAへのパケットは、引き続き許可されます。

 注:ACL access-list 1 permit 192.168.10.1 0.0.0.0も、同じルールを設定する別の方法です。

特定のホストによるネットワーク アクセスの拒否

次の図は、ホストBから発信されたNetA宛でのトラフィックが拒否され、NetBから発信されたNetAへの他のすべてのトラフィックが許可されていることを示しています。



次の設定では、ホスト 192.168.10.1/32 からのパケットが R1 の Ethernet 0 を通過することは拒否されていますが、その他のパケットはすべては許可されています。すべての ACL には暗黙的な deny all 句が存在するので、その他すべてのパケットを明示的に許可するには、access list 1 permit any コマンドを使用する必要があります。

R1

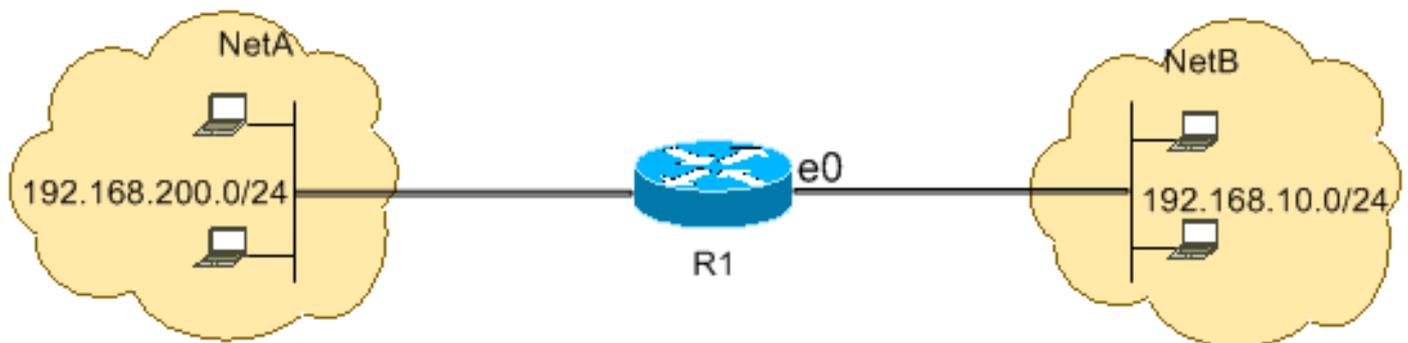
```
hostname R1
!  
interface ethernet0  
 ip access-group 1 in  
!  
access-list 1 deny host 192.168.10.1  
access-list 1 permit any
```

 注：文の順序は、ACLの動作にとって重要です。次のコマンドに示すように、エントリの順序を逆にすると、最初の行がすべてのパケットの送信元アドレスに一致してしまいます。そのため、この ACL では、ホスト 192.168.10.1/32 による NetA へのアクセスをブロックできません。

```
access-list 1 permit any
access-list 1 deny host 192.168.10.1
```

連続した IP アドレスの範囲へのアクセスの許可

次の図は、ネットワークアドレス192.168.10.0/24を持つNetB内のすべてのホストが、NetA内のネットワーク192.168.200.0/24にアクセスできることを示しています。



次の設定では、ネットワーク 192.168.10.0/24 内の送信元アドレスとネットワーク 192.168.200.0/24 内の宛先アドレスが指定された IP ヘッダーを持つ IP パケットは、NetA にアクセスすることを許可されています。ACL の最後には暗黙的な deny all 句が存在するので、その他のトラフィックはすべて R1 の Ethernet 0 の内側に通過することを拒否されます。

R1

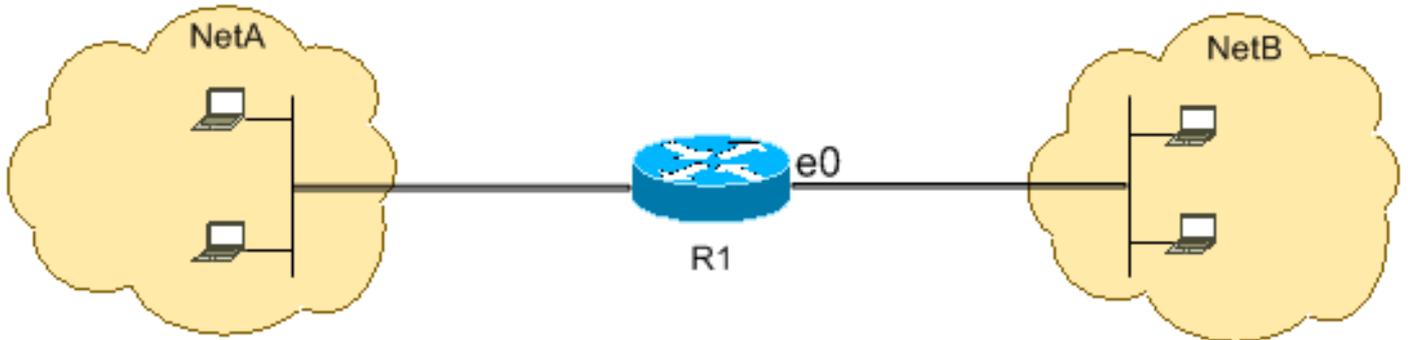
```
hostname R1
!
interface ethernet0
 ip access-group 101 in
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255
```

 注：コマンド access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255 では、0.0.0.255 がマスク 255.255.255.0 を持つネットワーク 192.168.10.0 の逆マスクです。ACL では、ネットワークアドレスの何ビットを照合する必要があるかを指定するために、逆マスクが使用されます。上の表に示す ACL では、192.168.10.0/24 ネットワーク内の送信元アドレスと 192.168.200.0/24 ネットワーク内の宛先アドレスが指定されたすべてのホストが許可されています。

ネットワークアドレスのマスクの詳細と、ACLに必要な逆マスクの算出方法については、『[IP アクセスリストの設定](#)』の「[マスク](#)」セクションを参照してください。

Telnetトラフィック(TCP、ポート23)を拒否する方法

より高度なセキュリティの問題に対処するために、パブリックネットワークからプライベートネットワークへのTelnetアクセスを無効にすることができます。次の図は、NetB (パブリック) からNetA (プライベート) に向かうTelnetトラフィックを拒否する方法を示しています。これにより、NetAはNetBとのTelnetセッションを開始および確立でき、その他すべてのIPトラフィックは許可されます。



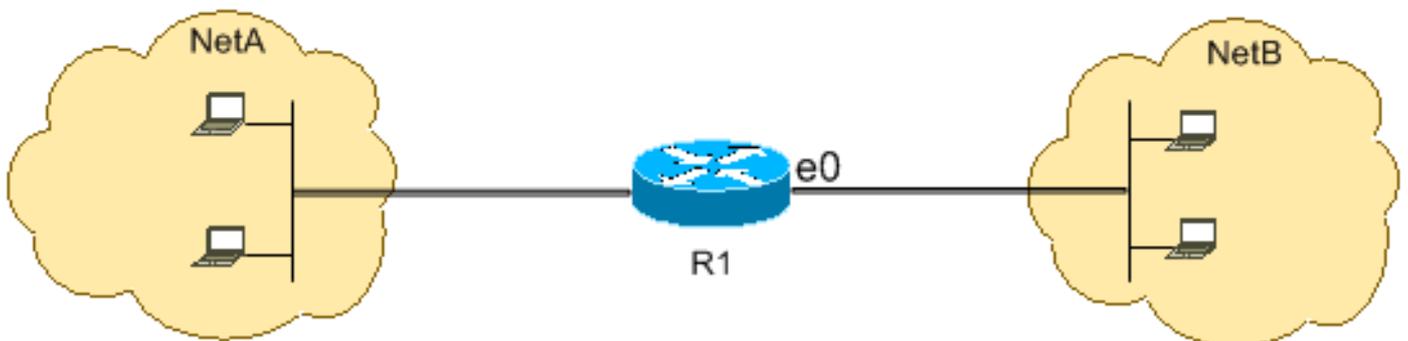
TelnetではTCPポート23が使用されます。次の設定では、NetAのポート23宛てのTCPトラフィックがすべてブロックされ、その他のIPトラフィックはすべて許可されています。

R1

```
hostname R1
!  
interface ethernet0  
  ip access-group 102 in  
!  
access-list 102 deny tcp any any eq 23  
access-list 102 permit ip any any
```

内部ネットワークだけにTCPセッションを始めさせる方法

次の図は、NetAから発信されたNetB宛てのTCPトラフィックが許可されているのに対し、NetBから発信されたNetA宛てのTCPトラフィックが拒否されていることを示しています。



この例の ACL は、次のことを目的としています。

- NetA 内のホストが NetB 内のホストへの TCP セッションを開始し確立することを許可する。
- NetB 内のホストが NetA 内のホストへの TCP セッションを開始し確立することを拒否する。

この設定では、次の条件を満たすデータグラムが、R1 のインターフェイス Ethernet 0 の内側に通過することを許可されています。

- 確認応答(ACK)ビットまたはリセット(RST)ビットが設定されている (TCPセッションが確立されていることを示す)
- 宛先ポート値が 1023 よりも大きい

R1

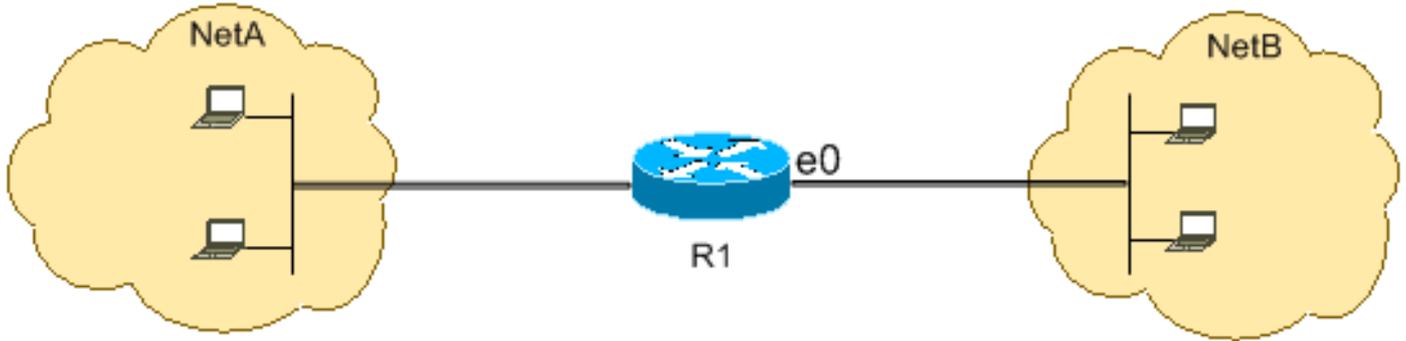
```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any any gt 1023 established
```

IP サービス用の代表的なポートの大部分では 1023 未満の値が使用されているため、宛先ポートが 1023 未満であるデータグラム、または ACK/RST ビットがセットされていないデータグラムは、ACL 102 により拒否されます。したがって、NetBのホストがTCP接続を開始し、1023未満のポート番号の最初のTCPパケット(同期/開始パケット(SYN/RST)ビットセットなし)を送信すると、そのパケットは拒否され、TCPセッションは失敗します。NetA から NetB に対して開始された TCP セッションが許可される理由は、これらの TCP セッションでは戻りパケットに ACK/RST ビットがセットされていて、1023 よりも大きいポート値が使用されているためです。

ポートの完全なリストについては、『[RFC 1700](#)』を参照してください。

FTP トラフィック(TCP 、ポート21) を拒否する方法

次の図は、NetBから発信されたNetA宛でのFTP (TCP、ポート21) およびFTPデータ (ポート20) トラフィックが拒否され、その他すべてのIPトラフィックが許可されていることを示しています。



FTP では、ポート 21 およびポート 20 が使用されます。ポート 21 およびポート 20 宛ての TCP トラフィックは拒否され、その他すべてのトラフィックは明示的に許可されています。

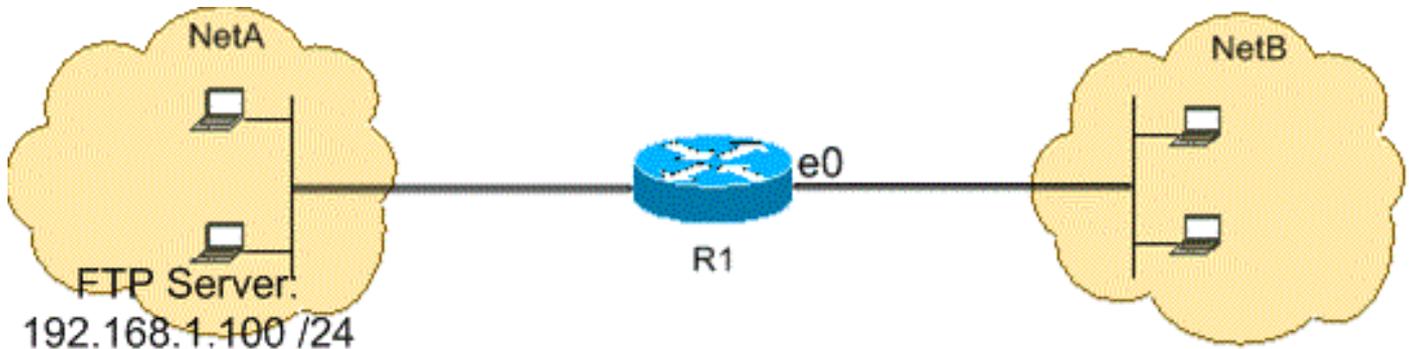
R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 deny tcp any any eq ftp
access-list 102 deny tcp any any eq ftp-data
access-list 102 permit ip any any
```

FTP トラフィックの許可 (アクティブ FTP)

FTP の動作モードには、アクティブ モードとパッシブ モードの 2 種類があります。

FTP がアクティブ モードで動作している場合、FTP サーバでは制御用にポート 21 が使用され、データ用にポート 20 が使用されます。FTP サーバ (192.168.1.100) は NetA 内にあります。次の図は、NetB から発信され FTP サーバ (192.168.1.100) を宛先とする FTP (TCP、ポート 21) および FTP データ (ポート 20) トラフィックが許可され、その他すべての IP トラフィックが拒否されていることを示しています。



R1

```
hostname R1
```

```

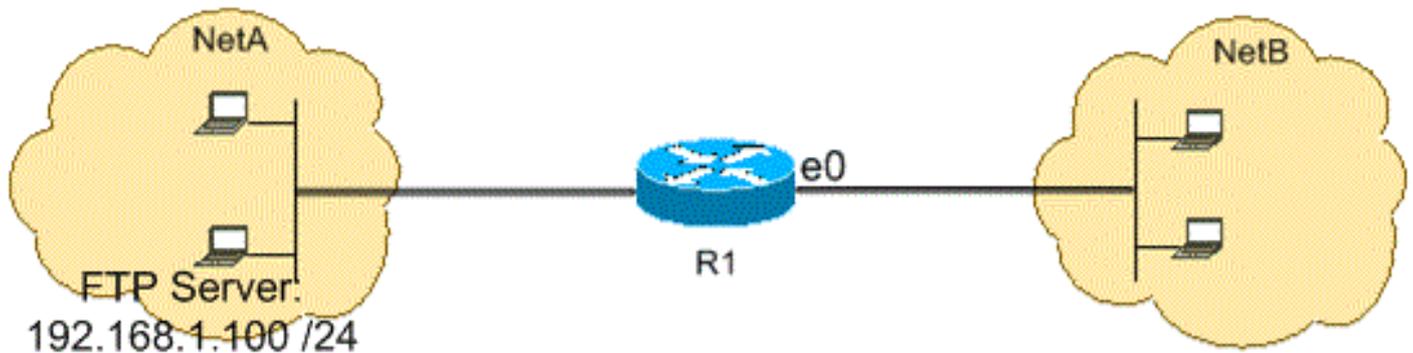
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 eq ftp-data established
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 eq ftp-data any

```

FTP トラフィックの許可 (パッシブ FTP)

FTP の動作モードには、アクティブ モードとパッシブ モードの 2 種類があります。

FTP がパッシブ モードで動作している場合、FTP サーバでは制御用にポート 21 が使用され、データ用に 1024 番以降のダイナミック ポートが使用されます。FTP サーバ (192.168.1.100) は NetA 内にあります。次の図は、NetBから発信されFTPサーバ(192.168.1.100)に向かう FTP (TCP、ポート21) およびFTPデータ (ポート1024以上) トラフィックが許可され、その他すべてのIPトラフィックが拒否されていることを示しています。



R1

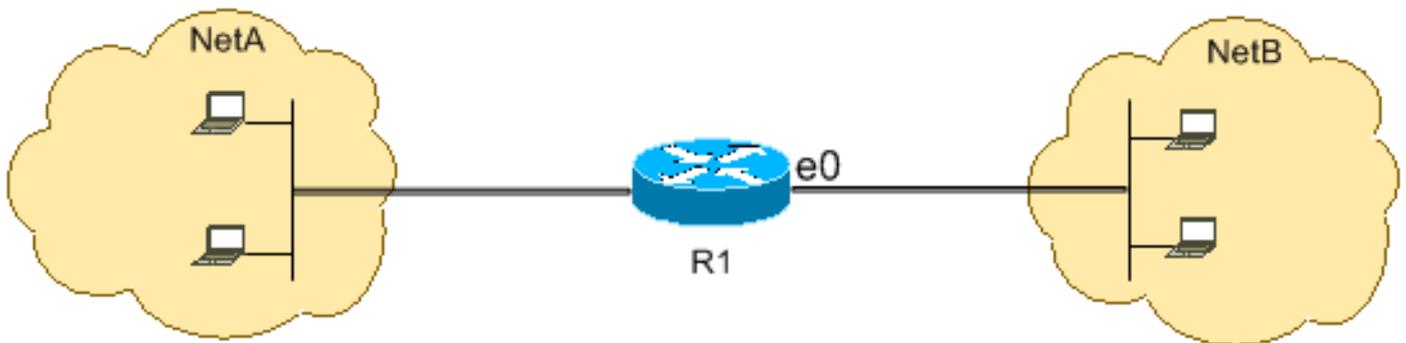
```

hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 gt 1023
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 gt 1023 any established

```

ping の許可 (ICMP)

次の図は、NetAから発信されたNetB宛でのICMPが許可され、NetBから発信されたNetA宛でのpingが拒否されていることを示しています。



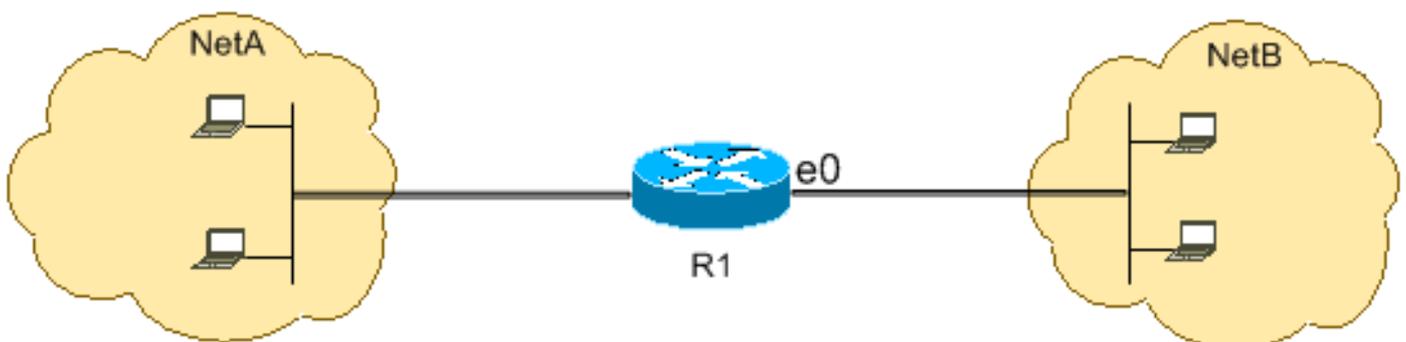
次の設定では、NetB から NetA に向かうパケットのうち、エコー応答 (ping 応答) パケットだけがインターフェイス Ethernet 0 を通過することを許可されています。ただし、この設定では、NetB から NetA に ping が発行された場合、すべてのエコー要求 ICMP パケットがブロックされます。そのため、NetA 内のホストは NetB 内のホストに ping を発行できますが、NetB 内のホストは NetA 内のホストに ping を発行できません。

R1

```
hostname R1
!  
interface ethernet0  
 ip access-group 102 in  
!  
access-list 102 permit icmp any any echo-reply
```

HTTP、Telnet、Mail、POP3、FTP の許可

次の図では、HTTP、Telnet、Simple Mail Transfer Protocol (SMTP ; シンプルメール転送プロトコル)、POP3、およびFTPのトラフィックだけが許可され、NetBから発信されたNetA宛での残りのトラフィックが拒否されていることが示されています。



次の設定では、WWW (ポート 80)、Telnet (ポート 23)、SMTP (ポート 25)、POP3 (ポー

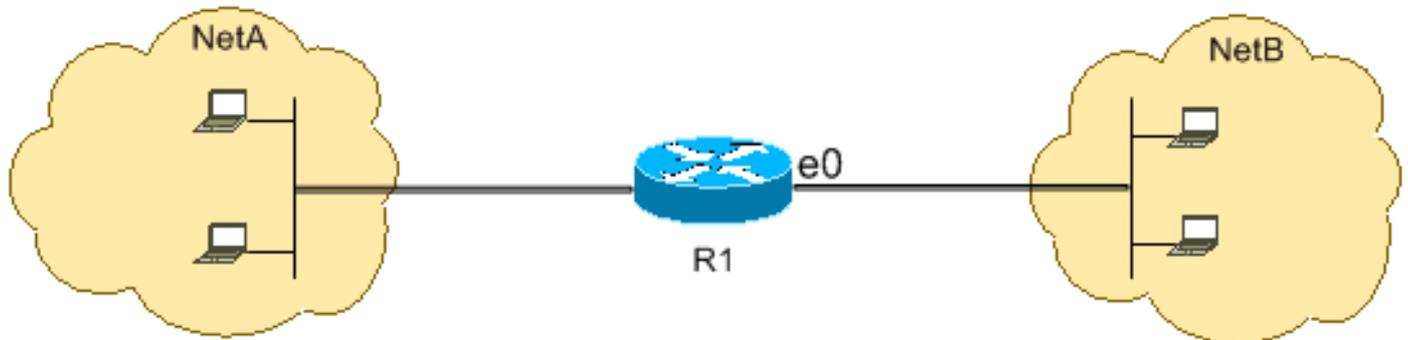
ト 110)、FTP (ポート 21)、または FTP データ (ポート 20) に一致する宛先ポート値が指定された TCP トラフィックが許可されます。ACL の最後にある暗黙的な deny all 句により、permit 句に一致しないその他すべてのトラフィックが拒否されることに注意してください。

R1

```
hostname R1
!  
interface ethernet0  
  ip access-group 102 in  
!  
access-list 102 permit tcp any any eq www  
access-list 102 permit tcp any any eq telnet  
access-list 102 permit tcp any any eq smtp  
access-list 102 permit tcp any any eq pop3  
access-list 102 permit tcp any any eq 21  
access-list 102 permit tcp any any eq 20
```

DNS の許可

次の図は、ドメインネームシステム(DNS)トラフィックだけが許可され、NetBから発信されたNetA宛ての残りのトラフィックが拒否されていることを示しています。



次の設定では、宛先ポート値 53 が指定された TCP トラフィックが許可されています。ACL の最後にある暗黙的な deny all 句により、permit 句に一致しないその他のトラフィックはすべて拒否されます。

R1

```
hostname R1
!  
interface ethernet0  
  ip access-group 102 in  
!  
access-list 102 permit udp any any eq domain  
access-list 102 permit udp any eq domain any  
access-list 102 permit tcp any any eq domain  
access-list 102 permit tcp any eq domain any
```

ルーティングの更新を許可する

インターフェイスにインバウンド ACL を適用するときは、ルーティング アップデートがフィルタリングで拒否されないようにする必要があります。ルーティング プロトコル パケットを許可するには、次の一覧の中で該当する ACL を使用します。

Routing Information Protocol (RIP) を許可するには、次のコマンドを入力します。

```
access-list 102 permit udp any any eq rip
```

Interior Gateway Routing Protocol (IGRP) を許可するには、次のコマンドを入力します。

```
access-list 102 permit igrp any any
```

Enhanced IGRP (EIGRP) を許可するには、次のコマンドを入力します。

```
access-list 102 permit eigrp any any
```

Open Shortest Path First (OSPF) を許可するには、次のコマンドを入力します。

```
access-list 102 permit ospf any any
```

Border Gateway Protocol (BGP) を許可するには、次のコマンドを入力します。

```
<#root>
```

```
access-list 102 permit tcp any any eq
```

```
179
```

```
access-list 102 permit tcp any eq
```

```
179
```

```
any
```

ACL に基づくトラフィックのデバッグ

debug コマンドを使用すると、メモリや処理能力などのシステムリソースが消費され、極端な状況ではシステムの負荷が高くなり、動作速度が低下することがあります。debug コマンドを使用するときは、十分に注意してください。debug コマンドの影響を少なくするには、ACL を使用して、検査する必要があるトラフィックを選択的に定義します。このような設定では、パケットのフィルタリングは行われません。

次の設定では、10.1.1.1 ~ 172.16.1.1 の間にあるホストのパケットに対してのみ、debug ip packet コマンドが有効になります。

```
<#root>
R1(config)#
access-list 199 permit tcp host 10.1.1.1 host 172.16.1.1
R1(config)#
access-list 199 permit tcp host 172.16.1.1 host 10.1.1.1
R1(config)#
end

R1#debug ip packet 199 detail
IP packet debugging is on (detailed) for access list 199
```

debug コマンドの影響についての詳細は、『[debug コマンドの重要な情報](#)』を参照してください。

[debug](#) コマンドを含む ACL の使用方法については、『[ping および traceroute コマンドについて](#)』の「[debug コマンドの使用](#)」セクションを参照してください。

MAC アドレス フィルタリング

特定の MAC レイヤステーションの送信元アドレスまたは宛先アドレスを含むフレームをフィルタリングできます。システムにこれらのアドレスをいくつ設定してもパフォーマンスには影響しません。MAC レイヤアドレスを基準にしてフィルタリングを行うには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

```
<#root>
Router#
config terminal
Router(config)#
bridge irb
Router(config)#
bridge 1 protocol ieee
```

```
Router(config)#
```

```
bridge 1 route ip
```

ブリッジプロトコルを、トラフィックのフィルタリングを必要とするインターフェイスに適用します。このアクセスリストは、bridge-group <group number> {input-address-list <ACL number>} コマンドで作成します。 | output-address-list <ACL番号>):

```
<#root>
```

```
Router#
```

```
config terminal
```

```
Router(config-if)#
```

```
interface fastEthernet0/0
```

```
Router(config-if)#
```

```
no ip address
```

```
Router(config-if)#
```

```
bridge-group 1 input-address-list 700
```

```
Router(config-if)#
```

```
exit
```

Bridged Virtual Interface(BVI)を作成し、物理イーサネットインターフェイスに割り当てられたIPアドレスを適用します。

```
<#root>
```

```
Router#
```

```
config terminal
```

```
Router(config-if)#
```

```
int bvi1
```

```
Router(config-if)#
```

```
ip address 192.168.1.1 255.255.255.0
```

```
Router(config-if)#
```

```
exit
```

```
Router(config)#
```

```
access-list 700 deny aaaa.bbbb.cccc 0000.0000.0000
```

```
Router(config)#
```

```
access-list 700 permit 0000.0000.0000 ffff.ffff.ffff
```

この設定を使用すると、access-list 700 で設定された MAC アドレスだけがルータで許可されます。アクセスリストコマンドaccess-list <ACL number> deny <mac address> 0000.0000.0000を使用して、アクセスできないMACアドレス (MACアドレス) を拒否し、残りのアドレス (この例ではaaaa.bbbb.cccc) を許可します。



注:MACアドレスごとに、アクセスリストのすべての行を作成します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [IP アクセスリストの設定](#)
- [アクセスリストに関するサポートページ](#)
- [IP ルーティングに関するサポート ページ](#)
- [IP ルーティング プロトコルに関するサポート ページ](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。