アクセス リスト コマンド

この章では、Cisco ASR 9000 シリーズ アグリゲーション サービス ルータの IP Version 4（IPv4）および IP Version 6（IPv6）のアクセス リストを設定するために使用する Cisco IOS XR ソフトウェアコマンドについて説明します。

アクセス コントロール リスト（ACL）は、ネットワーク トラフィック プロファイルをまとめて定義する 1 つ以上の Access Control Entry（ACE; アクセス コントロール エントリ）です。 このプロファイルは、トラフィック フィルタリング、プライオリティ キューイングまたはカスタム キューイング、およびダイナミック アクセス コントロールなどの Cisco IOS XR ソフトウェアソフトウェア機能によって参照されるようになります。 各 ACL には、送信元アドレス、宛先アドレス、プロトコル、およびプロトコルに固有のパラメータなどの基準に基づく、アクション要素（許可または拒否）やフィルタ要素が含まれています。

ACL の概念、設定タスク、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide*』を参照してください。

clear access-list ipv4

IPv4 アクセス リスト カウンタをクリアするには、EXEC モードで **clear access-list ipv4** コマンドを使用します。

clear access-list ipv4 *access-list name* [*sequence-number* | hardware { ingress | egress}] [interface *type interface-path-id*][location *node-id* | sequence *number*]

構文の説明

access-list-name	特定の IPv4 アクセス リストの名前。 この名前にスペースや引用符を含めることはできませんが、数値を含めることはできます。
sequence-number	（任意）アクセス リストのカウンタをクリアする特定のシーケンス番号。 範囲は 1 ～ 2147483644 です。
hardware	アクセス リストを、インターフェイスのアクセス グループとして識別します。
ingress	着信方向を指定します。
egress	発信方向を指定します。
interface	（任意）インターフェイスの統計情報をクリアします。
type	インターフェイスのタイプ。 詳細については、疑問符（?）オンライン ヘルプ機能を使用してください。
interface-path-id	物理インターフェイスまたは仮想インターフェイス。 （注） ルータに現在設定されているすべてのインターフェイスのリストを表示するには、**show interfaces** コマンドを使用します。 ルータの構文の詳細については、疑問符（?）を使用してオンライン ヘルプを参照してください。
location *node-id*	（任意）指定したノードからのハードウェア リソース カウンタをクリアします。 *node-id* 引数は、*rack/slot/module* の形式で入力します。
sequence *number*	（任意）特定のシーケンス番号を持つアクセス リストのカウンタをクリアします。 範囲は 1 ～ 2147483644 です。

コマンド デフォルト

デフォルトでは、指定された IPv4 アクセス リストがクリアされます。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

clear access-list ipv4 コマンドを使用すると、指定された設定済みのアクセス リストのカウンタをクリアすることができます。 シーケンス番号を使用すると、特定のシーケンス番号を持つアクセス リストのカウンタをクリアすることができます。

hardware キーワードを使用すると、**ipv4 access-group** コマンドを使用してイネーブルにしたアクセス リストのカウンタをクリアすることができます。

access-list-name 引数内にあるアスタリスク（*****）を使用すると、すべてのアクセス リストをクリアすることができます。

（注） アクセス リストは、複数のインターフェイスで共有できます。 ハードウェア カウンタをクリアすると、指定されたアクセス リストを指定された方向（入力または出力）で使用しているすべてのインターフェイスの全カウンタがクリアされます。

タスク ID

タスク ID	操作
basic-services	読み取り、書き込み
acl	読み取り、書き込み
bgp	読み取り、書き込み、実行

例

次の例では、*marketing* という名前のアクセス リストのカウンタがクリアされます。

```
RP/0/RSP0/CPU0:router# show access-lists ipv4 marketing

ipv4 access-list marketing
  10 permit ip 192.168.34.0 0.0.0.255 any (51 matches)
  20 permit ip 172.16.0.0 0.0.255.255 any (26 matches)
  30 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203 30 (5 matches)
```

```
RP/0/RSP0/CPU0:router# clear access-list ipv4 marketing

RP/0/RSP0/CPU0:router# show access-lists ipv4 marketing

ipv4 access-list marketing
  10 permit ip 192.168.34.0 0.0.0.255 any
  20 permit ip 172.16.0.0 0.0.255.255 any
  30 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203 30
```

次の例では、発信方向の acl_hw_1 という名前のアクセス リストのカウンタがクリアされます。

```
RP/0/RSP0/CPU0:router# show access-lists ipv4 acl_hw_1 hardware egress location 0/2/cp0

ipv4 access-list acl_hw_1
  10 permit icmp 192.168.36.0 0.0.0.255 any (251 hw matches)
  20 permit ip 172.16.3.0 0.0.255.255 any (29 hw matches)
  30 deny tcp any any (58 hw matches)

RP/0/RSP0/CPU0:router# clear access-list ipv4 acl_hw_1 hardware egress location 0/2/cp0

RP/0/RSP0/CPU0:router# show access-lists ipv4 acl_hw_1 hardware egress location 0/2/cp0

ipv4 access-list acl_hw_1
  10 permit icmp 192.168.36.0 0.0.0.255 any
  20 permit ip 172.16.3.0 0.0.255.255 any
  30 deny tcp any any
```

関連コマンド

コマンド	説明
ipv4 access-group, （31 ページ）	インターフェイス上の着信または発信の IPv4 トラフィックをフィルタリングします。
ipv4 access-list , （34 ページ）	IPv4 アクセス リストを定義し、また、IPv4 アクセス リスト コンフィギュレーション モードを開始します。
resequence access-list ipv4 , （85 ページ）	既存のステートメントの番号を付け直して後続のステートメントの番号を増加して、新しい IPv4 アクセス リスト ステートメントを許可します。

clear access-list ipv6

IPv6 アクセス リストのカウンタをクリアするには、EXEC モードで **clear access-list ipv6** コマンドを使用します。

clear access-list ipv6 *access-list-name* [*sequence-number*| **hardware** {**ingress**| **egress**}] [**interface** *type interface-path-id*] [**location** *node-id*| **sequence** *number*]

構文の説明

access-list-name	特定の IPv6 アクセス リストの名前。 この名前にスペースや引用符を含めることはできませんが、数値を含めることはできます。
sequence-number	（任意）アクセス リストのカウンタをクリアする、特定のアクセス コントロール エントリ（ACE）の特定のシーケンス番号。 範囲は 1 ～ 2147483644 です。
hardware	（任意）アクセス リストを、インターフェイスのアクセス グループとして識別します。
ingress	（任意）着信方向を指定します。
egress	（任意）発信方向を指定します。
interface	（任意）インターフェイスの統計情報をクリアします。
type	（任意）インターフェイスのタイプ。 詳細については、疑問符（?）オンライン ヘルプ機能を使用してください。
instance *interface-path-id*	物理インターフェイスまたは仮想インターフェイス。 （注） ルータに現在設定されているすべてのインターフェイスのリストを表示するには、**show interfaces** コマンドを使用します。ルータの構文の詳細については、疑問符（?）を使用してオンライン ヘルプを参照してください。
location *node-id*	（任意）カード インターフェイス上でイネーブルのアクセス リストのカウンタをクリアします。 *node-id* 引数は、rack/slot/module の形式で入力します。
sequence *number*	（任意）アクセス リストのカウンタをクリアする特定のシーケンス番号を指定します。 範囲は 1 ～ 2147483644 です。

コマンド デフォルト

EXEC デフォルトでは、指定された IPv6 アクセス リストがクリアされます。

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

clear access-list ipv6 コマンドは、IPv6 に固有のものを除き、**clear access-list ipv4** コマンドと類似しています。

clear access-list ipv6 コマンドを使用すると、指定された設定済みのアクセス リストのカウンタをクリアすることができます。 シーケンス番号を使用すると、特定のシーケンス番号を持つアクセス リストのカウンタをクリアすることができます。

hardware キーワードを使用すると、**ipv6 access-group** コマンドを使用してイネーブルにしたアクセス リストのカウンタをクリアすることができます。

access-list-name 引数内にあるアスタリスク（*****）を使用すると、すべてのアクセス リストをクリアすることができます。

（注） アクセス リストは、複数のインターフェイスで共有できます。 ハードウェア カウンタをクリアすると、指定されたアクセス リストを指定された方向（入力または出力）で使用しているすべてのインターフェイスの全カウンタがクリアされます。

タスク ID

タスク ID	操作
basic-services	読み取り、書き込み
acl	読み取り、書き込み
network	読み取り、書き込み

例

次の例では、*marketing* という名前のアクセス リストのカウンタがクリアされます。

```
RP/0/RSP0/CPU0:router# show access-lists ipv6 marketing
ipv6 access-list marketing
  10 permit ipv6 3333:1:2:3::/64 any (51 matches)
  20 permit ipv6 4444:1:2:3::/64 any (26 matches)
```

```
  30 permit ipv6 5555:1:2:3::/64 any (5 matches)
RP/0/RSP0/CPU0:router# clear access-list ipv6 marketing
RP/0/RSP0/CPU0:router# show access-lists ipv6 marketing
ipv6 access-list marketing
  10 permit ipv6 3333:1:2:3::/64 any
  20 permit ipv6 4444:1:2:3::/64 any
  30 permit ipv6 5555:1:2:3::/64 any
```

次の例では、発信方向の acl_hw_1 という名前のアクセス リストのカウンタがクリアされます。

```
RP/0/RSP0/CPU0:router# show access-lists ipv6 acl_hw_1 hardware egress location 0/2/cp0
ipv6 access-list acl_hw_1
  10 permit ipv6 3333:1:2:3::/64 any (251 hw matches)
  20 permit ipv6 4444:1:2:3::/64 any (29 hw matches)
  30 deny tcp any any (58 hw matches)
RP/0/RSP0/CPU0:router# clear access-list ipv6 acl_hw_1 hardware egress location 0/2/cp0
RP/0/RSP0/CPU0:router# show access-lists ipv6 acl_hw_1 hardware egress location 0/2/cp0
ipv6 access-list acl_hw_1
  10 permit ipv6 3333:1:2:3::/64 any
  20 permit ipv6 4444:1:2:3::/64 any
  30 deny tcp any any
```

関連コマンド

コマンド	説明
ipv6 access-list , （43 ページ）	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。

copy access-list ipv4

既存の IPv4 アクセス リストのコピーを作成するには、EXEC モードで **copy access-list ipv4** コマンドを使用します。

copy access-list ipv4 *source-acl destination-acl*

構文の説明

source-acl	コピー元のアクセス リストの名前
destination-acl	*source-acl* 引数の内容がコピーされる宛先のアクセス リストの名前

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

copy access-list ipv4 コマンドを使用すると、設定済みのアクセス リストをコピーすることができます。 *source-acl* 引数を使用してコピー元のアクセス リストを指定し、*destination-acl* 引数を使用すると、送信元アクセス リストの内容のコピー先を指定することができます。 *destination-acl* 引数は一意な名前である必要があり、アクセス リストまたはプレフィックス リストに *destination-acl* 引数名が存在する場合は、そのアクセス リストはコピーされません。 **copy access-list ipv4** コマンドは、送信元アクセス リストが存在していたら既存のリスト名を確認して、既存のアクセス リストまたはプレフィックス リストが上書きされないようにします。

タスク ID

タスク ID	操作
acl	読み取り、書き込み

タスク ID	操作
filesystem	実行

例

次の例では、アクセス リスト list-1 のコピーが作成されます。

```
RP/0/RSP0/CPU0:router# show access-lists ipv4 list-1

ipv4 access-list list-1
  10 permit tcp any any log
  20 permit ip any any
RP/0/RSP0/CPU0:router# copy access-list ipv4 list-1 list-2
RP/0/RSP0/CPU0:router# show access-lists ipv4 list-2
ipv4 access-list list-2
  10 permit tcp any any log
  20 permit ip any any
```

次の例では、アクセス リストの list-1 から list-3 へのコピーが、list-3 のアクセス リストがすでに存在しているために拒否されています。

```
RP/0/RSP0/CPU0:router# copy access-list ipv4 list-1 list-3

list-3 exists in access-list

RP/0/RSP0/CPU0:router# show access-lists ipv4 list-3

ipv4 access-list list-3
  10 permit ip any any
  20 deny tcp any any log
```

関連コマンド

コマンド	説明
ipv4 access-list , （34 ページ）	IPv4 アクセス リストを定義し、また、IPv4 アクセス リスト コンフィギュレーション モードを開始します。
show access-lists ipv4 , （92 ページ）	現在の IPv4 アクセス リストすべての内容を表示します。

copy access-list ipv6

既存の IPv6 アクセス リストのコピーを作成するには、EXEC モードで **copy access-list ipv6** コマンドを使用します。

copy access-list ipv6 *source-acl destination-acl*

構文の説明

source-acl	コピー元のアクセス リストの名前
destination-acl	*source-acl* 引数の内容のコピー先のアクセス リスト

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

copy access-list ipv6 コマンドを使用すると、設定済みのアクセス リストをコピーすることができます。 *source-acl* 引数を使用してコピー元のアクセス リストを指定し、*destination-acl* 引数を使用すると、送信元アクセス リストの内容のコピー先を指定することができます。 *destination-acl* 引数は一意な名前である必要があり、アクセス リストまたはプレフィックス リストに *destination-acl* 引数名が存在する場合は、そのアクセス リストはコピーされません。 **copy access-list ipv6** コマンドは、送信元アクセスリストが存在していたら既存のリスト名を確認して、既存のアクセスリストまたはプレフィックス リストが上書きされないようにします。

タスク ID

タスク ID	操作
acl	読み取り、書き込み

タスク ID	操作
filesystem	実行

例

次の例では、アクセス リスト list-1 のコピーが作成されます。

```
RP/0/RSP0/CPU0:router# show access-lists ipv6 list-1

ipv6 access-list list-1
  10 permit tcp any any log
  20 permit ipv6 any any

RP/0/RSP0/CPU0:router# copy access-list ipv6 list-1 list-2

RP/0/RSP0/CPU0:router# show access-lists ipv6 list-2

ipv6 access-list list-2
  10 permit tcp any any log
  20 permit ipv6 any any
```

次の例では、アクセス リストの list-1 から list-3 へのコピーが、list-3 のアクセス リストがすでに存在しているために拒否されています。

```
RP/0/RSP0/CPU0:router# copy access-list ipv6 list-1 list-3

list-3 exists in access-list

RP/0/RSP0/CPU0:router# show access-lists ipv6 list-3
ipv6 access-list list-3
  10 permit ipv6 any any
  20 deny tcp any any log
```

関連コマンド

コマンド	説明
ipv6 access-list , （43 ページ）	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
show access-lists ipv6, （98 ページ）	現在のすべての IPv6 アクセス リストの内容を表示します。

deny（IPv4）

IPv4 アクセス リストの条件を設定するには、アクセス リスト コンフィギュレーション モードで **deny** コマンドを使用します。 **deny** コマンドには、**deny**（送信元）および **deny**（プロトコル）の 2 つのバージョンがあります。 アクセス リストから条件を削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **deny** *source* [*source-wildcard*] [**log**| **log-input**]

*[sequence-number]***deny***protocol source source-wildcard destination destination-wildcard*[**precedence***precedence*] [**dscp***dscp*] [**fragments**] [*packet-length operator packet-length value*] [**log** | **log-input**] [**ttl** *ttl value [value1....value2]*]

no *sequence-number*

Internet Control Message Protocol (ICMP)

[*sequence-number*] **deny icmp** *source source-wildcard destination destination-wildcard* [*icmp-type*] [*icmp-code*] [**precedence** *precedence*] [**dscp** *dscp*] **[fragments]** [**log**| **log-input**] **[icmp-off]**

Internet Group Management Protocol (IGMP)

[*sequence-number*] **deny igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**dscp** *value*] **[fragments]** [**log**| **log-input**]

User Datagram Protocol (UDP)

[*sequence-number*] **deny udp** *source source-wildcard* [*operator* {*port*| *protocol-port*}] *destination destination-wildcard* [*operator* {*port*| *protocol-port*}] [**precedence** *precedence*] [**dscp** *dscp*] **[fragments]** [**log**| **log-input**]

構文の説明

sequence-number	（任意）アクセス リスト中の **deny** ステートメントの番号。 この番号により、アクセス リスト中のステートメントの順番を識別します。 番号は 1 ～ 2147483644 です （デフォルトで、最初のステートメントの番号は 10 で、後続のステートメントは 10 ずつ増加していきます）。**resequence access-list** コマンドを使用すると、設定済みアクセス リスト中の最初のステートメントの番号を変更し、後続のステートメントの番号を増加することができます。
source	パケットの送信元のネットワークまたはホストの番号。 送信元を指定する場合、代わりに次の 3 つの方法を使用できます。 • 32 ビットの 4 分割ドット付き 10 進表記を使用する。 • **any** キーワードを、0.0.0.0 255.255.255.255 の *source* および *source-wildcard* の短縮形として使用する。 • **host** *source* の組み合わせを、*source* 0.0.0.0 の *source* および *source-wildcard* の短縮形として使用する。

source-wildcard	送信元に適用されるワイルドカード ビット。 送信元のワイルドカードを指定するには、次の 3 つの方法から選択します。 • 32 ビットの 4 分割ドット付き 10 進表記を使用する。 無視するビット位置に 1 を入れます。 • **any** キーワードを、0.0.0.0 255.255.255.255 の *source* および *source-wildcard* の短縮形として使用する。 • **host** *source* の組み合わせを、*source* 0.0.0.0 の *source* および *source-wildcard* の短縮形として使用する。
protocol	IP プロトコルの名前または番号。 キーワード **ahp** 、 **esp** 、 **eigrp** 、 **gre** 、 **icmp** 、 **igmp** 、 **igrp** 、 **ip** 、 **ipinip** 、 **nos** 、 **ospf** 、 **pim** 、 **pcp** 、 **tcp** 、または **udp** のいずれか 1 つ、あるいは IP プロトコル番号を表す 0 ～ 255 の整数にすることができます。 任意のインターネット プロトコル（ICMP、TCP、および UDP を含む）に一致させるには、**ip** キーワードを使用します。 ICMP および TCP では、さらに、このテーブルの後半に記載されている修飾子を許可します。
destination	パケットの宛先のネットワークまたはホストの番号。 宛先を指定するには、次の 3 つの方法から選択します。 • 32 ビットの 4 分割ドット付き 10 進表記を使用する。 • **any** キーワードを、0.0.0.0 255.255.255.255 の *destination* および *destination-wildcard* の短縮形として使用する。 • **host** *destination* の組み合わせを、*destination* 0.0.0.0 の *destination* および *destination-wildcard* の短縮形として使用する。
destination-wildcard	宛先に適用されるワイルドカード ビット。 宛先のワイルドカードを指定するには、次の 3 つの方法から選択します。 • 32 ビットの 4 分割ドット付き 10 進表記を使用する。 無視するビット位置に 1 を入れます。 • **any** キーワードを、0.0.0.0 255.255.255.255 の *destination* および *destination-wildcard* の短縮形として使用する。 • **host** *destination* の組み合わせを、*destination* 0.0.0.0 の *destination* および *destination-wildcard* の短縮形として使用する。

precedence *precedence*	（任意）パケットは、precedence レベル（0 ～ 7 の番号で指定）または次の名前でフィルタリングできます。 • **routine**：パケットを routine precedence（0）と一致させます。 • **priority**：パケットを priority precedence（1）と一致させます。 • **immediate**：パケットを immediate precedence（2）と一致させます。 • **flash**：パケットを flash precedence（3）と一致させます。 • **flash-override**：パケットを flash override precedence（4）と一致させます。 • **critical**：パケットを critical precedence（5）と一致させます。 • **internet**：パケットを internetwork control precedence（6）と一致させます。 • **network**：パケットを network control precedence（7）と一致させます。

dscp *dscp*	（任意）DiffServ コード ポイント（DSCP）により、Quality of Service のコントロールが提供されます。 *dscp* の値は次のとおりです。 • **0–63**：DiffServ コード ポイント値 • **af11**：パケットを AF11 dscp（001010）と一致させます。 • **af12**：パケットを AF12 dscp（001100）と一致させます。 • **af13**：パケットを AF13 dscp（001110）と一致させます。 • **af21**：パケットを AF21 dscp（010010）と一致させます。 • **af22**：パケットを AF22 dscp（010100）と一致させます。 • **af23**：パケットを AF23 dscp（010110）と一致させます。 • **af31**：パケットを AF31 dscp（011010）と一致させます。 • **af32**：パケットを AF32 dscp（011100）と一致させます。 • **af33**：パケットを AF33 dscp（011110）と一致させます。 • **af41**：パケットを AF41 dscp（100010）と一致させます。 • **af42**：パケットを AF42 dscp（100100）と一致させます。 • **af43**：パケットを AF43 dscp（100110）と一致させます。 • **cs1**：パケットを CS1（precedence 1）dscp（001000）と一致させます。 • **cs2**：パケットを CS2（precedence 2）dscp（010000）と一致させます。 • **cs3**：パケットを CS3（precedence 3）dscp（011000）と一致させます。 • **cs4**：パケットを CS4（precedence 4）dscp（100000）と一致させます。 • **cs5**：パケットを CS5（precedence 5）dscp（101000）と一致させます。 • **cs6**：パケットを CS6（precedence 6）dscp（110000）と一致させます。 • **cs7**：パケットを CS7（precedence 7）dscp（111000）と一致させます。 • **default**：デフォルト DSCP（000000） • **ef**：パケットを EF dscp（101110）と一致させます。
fragments	（任意）このアクセス リスト エントリーを適用すると、ソフトウェアが IPv4 パケットのフラグメントを検査するようになります。 このキーワードを指定すると、フラグメントがアクセス キー リスト エントリーによる制約を受けます。

log	（任意）コンソールに送信されるエントリに一致するパケットに関するロギング メッセージ情報が出力されます。（コンソールに記憶されるメッセージのレベルは **logging console** コマンドで制御します） このメッセージに含まれるものには、アクセス リスト番号、パケットが許可されたか拒否されたか、プロトコルがTCP、UDP、ICMP、または番号であったか、さらに、該当する場合は、送信元と宛先アドレス、および送信元と宛先ポート番号があります。このメッセージは、フローに一致した最初のパケットに対して生成され、5分間隔で、前の5分間に許可または拒否されたパケット数を含みます。
log-input	（任意）ロギング メッセージに入力インターフェイスも含まれることを除き、**log** キーワードと同じ機能を提供します。
ttl	（任意）Time-To-Life（TTL）値との一致をオンにします。
ttl value [*value1. value2*[	（任意）フィルタリングに使用される TTL 値 値の範囲は 1 ～ 255 です。 *value* が指定される場合にだけ、この値に対する一致になります。 *value1* および *value2* の両方が指定された場合、*value1* と *value2* の間の TTL の範囲に対してパケット TTL が一致されます。
icmp-off	（任意）拒否されたパケットに対して ICMP 生成をオフにします。
icmp-type	（任意）ICMPパケットのフィルタリングのためのICMPメッセージタイプ。範囲は 0 ～ 255 です。
icmp-code	（任意）ICMPパケットのフィルタリングのためのICMPメッセージコード。範囲は 0 ～ 255 です。
igmp-type	（任意）IGMPパケットをフィルタリングするための、IGMPメッセージタイプ（0 ～ 15）または次のようなメッセージ名。 • dvmrp • host-query • host-report • mtrace • mtrace-response • pim • precedence • トレース • v2-leave • v2-report • v3-report

operator	（任意）演算子は、送信元ポートまたは宛先ポートを比較するために使用されます。 オペランドとして使用可能なものには、**lt**（less than：より小さい）、**gt**（greater than：より大きい）、**eq**（equal：等しい）、**neq**（not equal：等しくない）、および **range**（inclusive range：包含範囲）があります。 演算子を *source* および *source-wildcard* の値の後に置く場合、送信元ポートと一致する必要があります。 演算子を *destination* および *destination-wildcard* の値の後に置く場合、宛先ポートと一致する必要があります。 演算子を **ttl** キーワードの後に置く場合、TTL 値と一致します。 **range** 演算子には 2 つのポート番号が必要です。 他のすべての演算子は 1 つのポート番号が必要です。
port	TCP または UDP ポートの 10 進数。 ポート番号の範囲は 0 ～ 65535 です。 TCP ポートは、TCP をフィルタリングする場合にだけ使用できます。 UDP ポートは、UDP をフィルタリングする場合にだけ使用できます。
protocol-port	TCP または UDP ポートの名前。 TCP および UDP ポートの名前は、「使用上のガイドライン」に示されています。 TCP ポート名は TCP をフィルタリングする場合に限り使用できます。 UDP ポート名は UDP をフィルタリングする場合に限り使用できます。
established	（任意）TCP プロトコルの場合にだけ、確立された接続を表示します。
match-any	（任意）TCP プロトコルの場合にだけ、TCP フラグの任意の組み合わせをフィルタリングします。
match-all	（任意）TCP プロトコルの場合にだけ、すべての TCP フラグをフィルタリングします。
+ | -	（必須）TCP プロトコル **match-any**、**match-all** の場合、プレフィックス *flag-name* の前に **+** または **-** を付けます。 TCP フラグを設定したパケットを一致させるには、*+flag-name* 引数を使用します。 TCP フラグを設定してないパケットを一致させるには、*-flag-name* 引数を使用します。
flag-name	（任意）TCP プロトコルが **match-any**、**match-all** の場合。 フラグの名前は、**ack** 、 **fin** 、 **psh** 、 **rst** 、 **syn** になります。

コマンド デフォルト

IPv4 アクセス リストの送受信時にパケットが拒否される特定の条件はありません。

ICMP メッセージの生成はデフォルトでイネーブルです。

コマンド モード

IPv4 アクセス リストの設定

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ipv4 access-list コマンドに続いて **deny** コマンドを使用すると、パケットがアクセス リストを通過できない条件を指定することができます。

デフォルトでは、アクセス リストの最初のステートメントは 10 で、その次のステートメントからは 10 ずつ増加します。

permit、**deny**、または **remark** ステートメントを、リスト全体を再入力せずに既存のアクセス リストに追加できます。 新しいステートメントをリストの最後尾以外に追加するには、所属先を示すために 2 つの既存のエントリ番号の間にある適切なエントリ番号を持つ新しいステートメントを作成します。

2 つの連続した番号のステートメントの間（たとえば、10 行と 11 行の間）にステートメントを追加する場合は、最初に **resequence access-list** コマンドを使用して、最初のステートメントに番号を付け直して、後続の各ステートメントの番号を増加させます。 *increment* 引数を使用すると、ステートメント間に新しい未使用の行番号が生成されます。次に、アクセス リスト中の所属先を指定する *entry-number* 引数を持つ新しいステートメントを追加します。

次に、precedence の名前のリストを示します。

- critical
- flash
- flash-override
- immediate
- internet
- ネットワーク
- priority
- routine

次に、ICMP メッセージ タイプの名前のリストを示します。

- administratively-prohibited
- alternate-address
- conversion-error

- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- reassembly-timeout
- redirect
- router-advertisement
- router-solicitation

- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- traceroute
- ttl-exceeded
- unreachable

次に、ポート番号の代わりに使用できるTCPポート名のリストを示します。 これらのプロトコルの参考情報については、現在の *Assigned Numbers* RFC を参照してください。 ポート番号の位置に ? を入力すると、これらのプロトコルに対応するポート番号を見つけることができます。

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- ホスト名
- ident
- irc
- klogin
- kshell
- login
- lpd
- nntp
- pim-auto-rp
- pop2

- pop3
- smtp
- sunrpc
- tacacs
- talk
- telnet
- time
- uucp
- whois
- www

次の UDP ポート名は、ポート番号の代わり使用できます。 これらのプロトコルの参考情報については、現在の *Assigned Numbers* RFC を参照してください。 ポート番号の位置に ? を入力すると、これらのプロトコルに対応するポート番号を見つけることができます。

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs

- talk
- tftp
- time
- who
- xdmcp

次のフラグを、**match-any** と **match-all** キーワード、および + と - 記号とともに使用すると、表示するフラグを選択することができます。

- ack
- fin
- psh
- rst
- syn

たとえば、**match-all** + *ack* + *syn* は TCP パケットを ack および syn フラグをセットして表示し、**match-any** + *ack* - *syn* は TCP パケットを ack をセットするか syn をセットしないで表示します。

タスク ID

タスク ID	操作
ipv4	読み取り、書き込み
acl	読み取り、書き込み

例

次に、Internetfilter という名前のアクセス リストの拒否条件を設定する方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 deny 192.168.34.0 0.0.0.255
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 20 deny 172.16.0.0 0.0.255.255
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 25 deny tcp host 172.16.0.0 eq bgp host
192.168.202.203 range 1300 1400
RP/0/RSP0/CPU0:router(config-ipv4-acl)# permit 10.0.0.0 0.255.255.255
```

関連コマンド

コマンド	説明
ipv4 access-group, （31 ページ）	インターフェイス上の着信または発信の IPv4 トラフィックをフィルタリングします。

コマンド	説明
ipv4 access-list , （34 ページ）	IPv4 アクセス リストを定義し、また、IPv4 アクセス リスト コンフィギュレーション モードを開始します。
permit（IPv4） , （55 ページ）	IPv4アクセス リストの許可条件を設定します。
remark（IPv4） , （81 ページ）	IPv4 アクセス リスト エントリに関する有益な設定を挿入します。
resequence access-list ipv4 , （85 ページ）	既存の IPv4 アクセス リスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。
show access-lists ipv4 , （92 ページ）	現在の IPv4 アクセス リストすべての内容を表示します。

deny（IPv6）

IPv6 アクセス リストの拒否条件を設定するには、IPv6 アクセス リスト コンフィギュレーション モードで **deny** コマンドを使用します。 拒否条件を削除するには、このコマンドの **no** 形式を使用します。

[sequence-number] **deny***protocol*{*source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address*}[*operator* {*port* | *protocol-port*}] [**dscp***value*] [**routing**] [**authen**] [**destopts**] [**fragments**] [*packet-length operator packet-length value*] [**log** | **log-input**] [**ttl** *operator ttl value*]

no *sequence-number*

Internet Control Message Protocol (ICMP)

*[sequence-number]***deny icmp** {*source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address*}{*destination-ipv6-prefix/ prefix-length* | *any* | *host destination-ipv6-address*}[*icmp-type*] [*icmp-code*][**dscp** *value*] [routing] [**authen**] [**destopts**] [**fragments**] [**log**] [**log-input**] [**icmp-off**]

Transmission Control Protocol (TCP)

*[sequence-number]***deny tcp**{*source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address*}[*operator*{*port* | *protocol-port*}]{*destination-ipv6-prefix/ prefix-length* | *any* | *host destination-ipv6-address*}[*operator*{*port* | *protocol* | *port*}] [**dscp***value*] [**routing**] [**authen**] [**destopts**] [**fragments**] [**established**]{**match-any** | **match-all** | + | **-**}[*flag-name*] [**log**] [**log-input**]

User Datagram Protocol (UDP)

*[sequence-number]***deny tcp**{*source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address*}[*operator*{*port* | *protocol-port*}]{*destination-ipv6-prefix/ prefix-length* | *any* | *host destination-ipv6-address*}[*operator*{*port* | *protocol* | *port*}] [**dscp***value*] [**routing**] [**authen**] [**destopts**] [**fragments**] [**established**][*flag-name*] [**log**] [**log-input**]

構文の説明

sequence-number	（任意）アクセス リスト中の **deny** ステートメントの番号。 この番号により、アクセス リスト中のステートメントの順番を識別します。 範囲は 1 ～ 2147483644 です。 （デフォルトで、最初のステートメントの番号は 10 で、後続のステートメントは 10 ずつ増加していきます）。**resequence access-list** コマンドを使用すると、設定済みアクセス リスト中の最初のステートメントの番号を変更し、後続のステートメントの番号を増加することができます。
protocol	インターネット プロトコルの名前または番号。 キーワード **ahp** 、**eigrp**、**esp** 、**gre**、 **icmp** 、**igmp**、**igrp**、**ipinip**、 **ipv6** 、**nos**、**ospf**、 **pcp** 、 **tcp** 、または **udp** のいずれか 1 つ、あるいは IPv6 プロトコル番号を表す 0 ～ 255 の整数にすることができます。

source-ipv6-prefix / *prefix-length*	拒否条件を設定する送信元 IPv6 ネットワークまたはネットワークのクラス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
any	IPv6 プレフィックス ::/0 の省略形。
host *source-ipv6-address*	拒否条件の設定先に関する送信元の IPv6 ホスト アドレス。 *source-ipv6-address* 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。
operator {*port* | *protocol-port*}	（任意）指定されたプロトコルの送信元ポートまたは宛先ポートを比較するオペランド。 オペランドには、**lt**（less than：より小さい）、**gt**（greater than：より大きい）、**eq**（equal：等しい）、**neq**（not equal：等しくない）、および **range**（inclusive range：包含範囲）があります。 *source-ipv6-prefix / prefix-length* 引数の後ろに演算子が置かれた場合、送信元ポートと一致する必要があります。 *destination-ipv6-prefix / prefix-length* 引数の後ろに演算子が置かれた場合、宛先ポートと一致する必要があります。 **range** 演算子には 2 つのポート番号が必要です。 他のすべての演算子は 1 つのポート番号が必要です。 *port* 引数は、TCP または UDP ポートの 16 進数です。 範囲は 0 ～ 65535 です。 *protocol-port* 引数は、TCP または UDP ポートの名前です。 TCP ポート名は TCP をフィルタリングする場合に限り使用できます。 UDP ポート名は UDP をフィルタリングする場合に限り使用できます。
destination-ipv6-prefix / *prefix-length*	拒否条件の設定先に関する宛先の IPv6 ネットワークまたはネットワーク クラス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
host *destination-ipv6-address*	拒否条件の設定先に関する宛先の IPv6 ホスト アドレス。 *destination-ipv6-address* 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。
dscp *value*	（任意）DiffServ コード ポイント（DSCP）値を、各 IPv6 パケット ヘッダーのトラフィック クラス フィールド内のトラフィック クラス値に、一致させます。 指定できる範囲は、0 ～ 63 です。
ルーティング	（任意）ソースルート パケットを、各 IPv6 パケット ヘッダー内の拡張ヘッダーに一致させます。

authen	（任意）IPv6 認証ヘッダーが存在する場合に一致します。
destopts	（任意）IPv6 宛先オプション ヘッダーが存在する場合に一致します。
fragments	（任意）フラグメント拡張ヘッダーにゼロ以外のフラグメント オフセットが含まれているフラグメント化された非初期パケットと一致させます。**fragments** キーワードは、*operator* [*port-number*] 引数が指定されていない場合に限り指定できるオプションです。
log	（任意）コンソールに送信されるエントリに一致するパケットに関するロギング メッセージ情報が出力されます。（コンソールに記憶されるメッセージのレベルは **logging console** コマンドで制御します） メッセージには、アクセス リスト名、シーケンス番号、パケットが拒否されたかどうか、プロトコル（TCP、UDP、ICMP または番号のいずれか）、適正な場合には送信元/宛先アドレス、送信元/宛先ポート番号が含まれます。 メッセージは、一致した最初のパケットに対して生成され、その後、5 分間隔で拒否されたパケット数を含めて生成されます。
log-input	（任意）ロギング メッセージに入力インターフェイスも含まれることを除き、**log** キーワードと同じ機能を提供します。
ttl	（任意）Time-To-Life（TTL）値との一致をオンにします。
operator	（任意）指定されたプロトコルの送信元ポートまたは宛先ポートを比較するオペランド。 オペランドには、**lt**（less than：より小さい）、**gt**（greater than：より大きい）、**eq**（equal：等しい）、**neq**（not equal：等しくない）、および **range**（inclusive range：包含範囲）があります。
ttl value [*value1 ... value2*]	（任意）フィルタリングに使用される TTL 値 値の範囲は 1 ～ 255 です。 *value* が指定される場合にだけ、この値に対する一致になります。 *value1* および *value2* の両方が指定された場合、*value1* と *value2* の間の TTL の範囲に対してパケット TTL が一致されます。
icmp-off	（任意）拒否されたパケットに対して ICMP の生成をオフにします。
icmp-type	（任意）ICMP パケットのフィルタリングのための ICMP メッセージ タイプ。 ICMP パケットは、ICMP メッセージ タイプでフィルタリングできます。 範囲は 0 ～ 255 です。
icmp-code	（任意）ICMP パケットのフィルタリングのための ICMP メッセージ コード。 ICMP メッセージ タイプによってフィルタリングされる ICMP パケットは、ICMP メッセージ コードによってもフィルタリングできます。 範囲は 0 ～ 255 です。
established	（任意）TCP プロトコルの場合にだけ、確立された接続を表示します。

match-any	（任意）TCP プロトコルの場合にだけ、TCP フラグの任意の組み合わせをフィルタリングします。
match-all	（任意）TCP プロトコルの場合にだけ、すべての TCP フラグをフィルタリングします。
+|-	（必須）TCP プロトコル **match-any**、**match-all** の場合、プレフィックス *flag-name* の前に **+** または **-** を付けます。 TCP フラグを設定したパケットを一致させるには、**+***flag-name* 引数を使用します。 TCP フラグを設定してないパケットを一致させるには、**-***flag-name* 引数を使用します。
flag-name	（任意）TCP プロトコルが **match-any**、**match-all** の場合。 フラグの名前は、**ack**、**fin**、**psh**、**rst**、**syn** になります。

コマンド デフォルト

IPv6 アクセス リストは定義されていません。

ICMP メッセージの生成はデフォルトでイネーブルです。

コマンド モード

IPv6 アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

deny（IPv6）コマンドは、IPv6 に固有のものを除き、deny（IPv4）コマンドと類似しています。

ipv6 access-list コマンドに続いて、**deny**（IPv6）コマンドを使用すると、パケットがアクセス リストを通過する条件を定義することができます。

protocol 引数に **ipv6** を指定すると、パケットの IPv6 ヘッダーを一致対象とします。

デフォルトでは、アクセス リストの最初のステートメントの番号は 10 で、その次のステートメントからは 10 ずつ増加します。

permit、deny、または remark ステートメントを、リスト全体を再入力せずに既存のアクセス リストに追加できます。 新しいステートメントをリストの最後尾以外に追加するには、所属先を示すために 2 つの既存のエントリ番号の間にある適切なエントリ番号を持つ新しいステートメントを作成します。

source-ipv6-prefix/prefix-length および *destination-ipv6-prefix/prefix-length* の引数は両方とも、トラフィック フィルタリング（送信元プレフィックスがトラフィック送信元に基づいてトラフィックをフィルタリングし、宛先プレフィックスがトラフィック宛先に基づいてトラフィックをフィルタリングする）に使用されます。

（注） アクセス リストでなく、IPv6 プレフィックス リストは、ルーティング プロトコル プレフィックスのフィルタリングに使用する必要があります。

fragments キーワードは、*operator* [*port* | *protocol-port*] 引数が指定されない場合だけのオプションです。

タスク ID

タスク ID	操作
acl	読み取り、書き込み

例

次に、toCISCO という名前の IPv6 アクセス リストを設定し、そのアクセス リストを GigabitEthernet インターフェイス 0/2/0/2 上の発信トラフィックに適用する方法の例を示します。 具体的には、リスト中の最初の拒否エントリにより、5000 を超える宛先 TCP ポート番号を持つすべてのパケットは GigabitEthernet インターフェイス 0/2/0/2 から出て行かないようになります。 リスト中の 2 番目の拒否エントリにより、5000 より小さい送信元 UDP ポート番号を持つすべてのパケットは GigabitEthernet インターフェイス 0/2/0/2 から出て行かないようになります。 2 番目の拒否エントリは、コンソールにもすべての一致を記録します。 リスト中の最初の許可エントリは、すべての ICMP パケットが GigabitEthernet インターフェイス 0/2/0/2 から出て行くことを許可します。 リスト中の 2 番目の許可エントリは、他のすべてのトラフィックが GigabitEthernet インターフェイス 0/2/0/2 から出て行くことを許可します。 2 番目の許可エントリは、すべての条件の暗黙的な拒否は各 IPv6 アクセス リストの最後にあるという理由で必要です。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list toCISCO
RP/0/RSP0/CPU0:router(config-ipv6-acl)# deny tcp any any gt 5000
RP/0/RSP0/CPU0:router(config-ipv6-acl)# deny ipv6 any lt 5000 any log
RP/0/RSP0/CPU0:router(config-ipv6-acl)# permit icmp any any
RP/0/RSP0/CPU0:router(config-ipv6-acl)# permit any any
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group tOCISCO out
```

関連コマンド

コマンド	説明
ipv6 access-list , （43 ページ）	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。

コマンド	説明
permit（IPv6） , （75 ページ）	IPv6アクセス リストに許可条件を設定します。
remark（IPv6） , （83 ページ）	IPv6 アクセス リスト エントリに関する有益な設定を挿入します。
resequence access-list ipv6 , （88 ページ）	既存の IPv6 アクセス リスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。

ipv4 access-group

インターフェイスへのアクセスを制御するには、インターフェイス コンフィギュレーション モードで **ipv4 access-group** コマンドを使用します。 指定されたアクセス グループを削除するには、このコマンドの **no** 形式を使用します。

ipv4 access-group *access-list-name* {**ingress| egress**} **[hardware-count] [interface-statistics]**

no ipv4 access-group *access-list-name* {**ingress| egress**} **[hardware-count] [interface-statistics]**

構文の説明

access-list-name	**ipv4 access-list** コマンドで指定された IPv4 アクセス リストの名前。
ingress	着信パケットに対してフィルタリングします。
egress	発信パケットをフィルタリングします。
hardware-count	（任意）アクセス グループのハードウェア カウンタにアクセスするように指定します。
interface-statistics	（任意）ハードウェア内のインターフェイス単位の統計情報を指定します。

コマンド デフォルト

インターフェイスには、適用される IPv4 アクセス リストがありません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ipv4 access-group コマンドを使用すると、インターフェイスへのアクセスを制御することができます。 指定されたアクセス グループを削除するには、このコマンドの **no** 形式を使用します。 *access-list-name* 引数を使用すると、特定の IPv4 アクセス リストを指定することができます。

ingress キーワードを使用すると着信パケットをフィルタリングでき、または **egress** キーワードを使用すると発信パケットをフィルタリングできます。 *hardware-count* 引数を使用すると、アクセス グループのハードウェア カウンタをイネーブルにすることができます。

許可されたパケットは、*hardware-count* 引数を使用してハードウェア カウンタがイネーブルにされた場合にだけカウントされます。拒否されたパケットは、ハードウェアカウンタがイネーブルかどうかにかかわらずカウントされます。

（注） **ipv4 access-group** コマンドを使用したパケット フィルタリング アプリケーションの場合、パケット カウンタは各方向のハードウェア内に維持されます。 同じ方向の複数のインターフェイス上で1つのアクセス グループを使用すると、イネーブルにされた *hardware-count* 引数を持つ各インターフェイスに対してパケットがカウントされます。

アクセスリストがアドレスを許可する場合は、ソフトウェアはパケットの処理を継続します。アクセス リストでアドレスが拒否されている場合、ソフトウェアはパケットを廃棄し、インターネット制御メッセージ プロトコル（ICMP）ホスト到達不能メッセージを返します。

指定したアクセス リストが存在しない場合は、すべてのパケットが通過します。

デフォルトでは、一意のまたはインターフェイス単位のACL統計情報はディセーブルになっています。

タスク ID

タスク ID	操作
acl	読み取り、書き込み
network	読み取り、書き込み

例

次に、GigabitEthernet Packet-over-SONET（POS）インターフェイス 0/2/0/2 との間の着信または発信パケットへのフィルタリングの適用方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv4 access-group p-ingress-filter ingress
RP/0/RSP0/CPU0:router(config-if)# ipv4 access-group p-egress-filter egress
```

次に、ハードウェア内のインターフェイス統計情報の適用方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv4 access-group p-ingress-filter ingress
interface-statistics
```

関連コマンド

コマンド	説明
clear access-list ipv4, （3 ページ）	IPv4 アクセス リスト一致カウンタをリセットします。
deny（IPv4） , （13 ページ）	IPv4 アクセス リストの拒否条件を設定します。
ipv4 access-list , （34 ページ）	IPv4 アクセス リストを定義し、また、IPv4 アクセス リスト コンフィギュレーション モードを開始します。
permit（IPv4） , （55 ページ）	IPv4 アクセス リストの許可条件を設定します。
show access-lists ipv4 , （92 ページ）	現在の IPv4 アクセス リストすべての内容を表示します。
show ipv4 interface	IPv4 用に設定されたインターフェイスの使用可能性ステータスを表示します。

ipv4 access-list

IPv4 アクセス リストを名前で定義するには、グローバル コンフィギュレーション モードで **ipv4 access-list** コマンドを使用します。 IPv4 アクセス リスト中のすべてのエントリを削除するには、このコマンドの **no** 形式を使用します。

ipv4 access-list *name*

no ipv4 access-list *name*

構文の説明

name	アクセス リストの名前。 名前にはスペースや疑問符を使用できません。

コマンド デフォルト

定義されている IPv4 アクセス リストはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 4.3.0	このコマンドは、BNG でサポートされていました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ipv4 access-list コマンドを使用すると、IPv4 アクセス リストを設定することができます。 このコマンドはルータをアクセス リスト コンフィギュレーション モードに設定します。このモードでは、拒否または許可されたアクセス条件は **deny** or **permit** コマンドを使用して定義される必要があります。

既存の IPv4 アクセス リスト中の連続したエントリ間に **permit**、deny、または remark ステートメントを追加する場合は、**resequence access-list ipv4** コマンドを使用します。 最初のエントリ番号（*base*）とステートメントのエントリ番号を分けるための増分を指定します。 既存のステートメントの番号が再設定され、未使用のエントリ番号で新しいステートメントが追加できるようになります。

ipv4 access-group コマンドを使用すると、アクセス リストをインターフェイスに適用することができます。

タスク ID

タスク ID	操作
acl	読み取り、書き込み

例

次に、Internetfilter という名前の標準アクセス リストを定義する方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RSP0/CPU0:router(config-if)# 10 permit 192.168.34.0 0.0.0.255
RP/0/RSP0/CPU0:router(config-if)# 20 permit 172.16.0.0 0.0.255.255
RP/0/RSP0/CPU0:router(config-if)# 30 permit 10.0.0.0 0.255.255.255
RP/0/RSP0/CPU0:router(config-if)# 39 remark Block BGP traffic from 172.16 net.
RP/0/RSP0/CPU0:router(config-if)# 40 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203
range 1300 1400
```

関連コマンド

コマンド	説明
clear access-list ipv4, （3 ページ）	IPv4 アクセス リスト一致カウンタをリセットします。
deny（IPv4）, （13 ページ）	名前付き IPv4 アクセス リストの拒否条件を設定します。
ipv4 access-group, （31 ページ）	インターフェイス上の着信または発信の IPv4 トラフィックをフィルタリングします。
permit（IPv4）, （55 ページ）	名前付き IPv4 アクセス リストの許可条件を設定します。
remark（IPv4）, （81 ページ）	IPv4 アクセス リスト エントリに関する有益な設定を挿入します。
resequence access-list ipv4 , （85 ページ）	既存の IPv4 アクセス リスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。
show access-lists ipv4 , （92 ページ）	現在の IPv4 アクセス リストすべての内容を表示します。

ipv4 access-list log-update rate

IPv4 アクセス リストが記録されるレートを指定するには、グローバル コンフィギュレーション モードで **ipv4 access-list log-update rate** コマンドを使用します。 更新レートをデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ipv4 access-list log-update rate *rate-number*

no ipv4 access-list log-update rate *rate-number*

構文の説明

rate-number	ルータ上で IPv4 アクセス ヒット ログが生成される毎秒のレート。 範囲は 1 ～ 1000 です。

コマンド デフォルト

デフォルトは 1 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

rate-number 引数は、インターフェイスに設定されたすべての IPv4 アクセス リストに適用されます。 つまり、システムに常に 1 ～ 1000 のログ エントリがあるということです。

タスク ID

タスク ID	操作
ipv4	読み取り、書き込み
acl	読み取り、書き込み

例

次に、システムの IPv4 アクセス ヒット ロギング レートを設定する方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list log-update rate 10
```

ipv4 access-list log-update threshold

IPv4アクセスリストにロギングされる更新数を指定するには、グローバルコンフィギュレーション モードで **ipv4 access-list log-update threshold** コマンドを使用します。 ロギングの更新数をデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ipv4 access-list log-update threshold *update-number*

no ipv4 access-list log-update threshold *update-number*

構文の説明

update-number	ルータに設定された IPv4 アクセス リストごとに記録される更新数。範囲は 0 ～ 2147483647 です。

コマンド デフォルト

IPv4 アクセス リストの場合、2147483647 の更新が記録されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

IPv4 アクセス リスト更新は、1 番目のロギング更新に続いて 5 分間隔で記録されます。 ロギングをより頻繁に更新する場合は、更新数を小さく（デフォルトよりも小さい数）するほうが有益です。

タスク ID

タスク ID	操作
basic-services	読み取り、書き込み
acl	読み取り、書き込み

例

次に、ルータに設定された IPv4 アクセス リストごとに 10 の更新のロギングしきい値を設定する方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list log-update threshold 10
```

関連コマンド

コマンド	説明
deny（IPv4） ,（13 ページ）	IPv4 アクセス リストの拒否条件を設定します。
ipv4 access-list ,（34 ページ）	IPv4 アクセス リストを定義し、また、IPv4 アクセス リスト コンフィギュレーション モードを開始します。
permit（IPv4） ,（55 ページ）	IPv4 アクセス リストの許可条件を設定します。
show access-lists ipv4 ,（92 ページ）	現在の IPv4 アクセス リストすべての内容を表示します。

ipv6 access-group

インターフェイスへのアクセスを制御するには、インターフェイス コンフィギュレーション モードで **ipv6** access-group コマンドを使用します。 指定されたアクセス グループを削除するには、このコマンドの **no** 形式を使用します。

ipv6 access-group *access-list-name* {**ingress| egress**} **[interface-statistics]**

no ipv6 access-group *access-list-name* {**ingress| egress**} **[interface-statistics]**

構文の説明

access-list-name	**ipv6 access-list** コマンドで指定されたとおりの IPv6 アクセス リストの名前。
ingress	着信パケットに対してフィルタリングします。
egress	発信パケットをフィルタリングします。
interface-statistics	（任意）ハードウェア内のインターフェイス単位の統計情報を指定します。

コマンド デフォルト

インターフェイスには、適用される IPv6 アクセス リストがありません。

コマンド モード

インターフェイス コンフィギュレーション

L2 トランスポート

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ipv6 access-group コマンドは、IPv6 に固有のものを除き、**ipv4 access-group** コマンドと類似しています。

ipv6 access-group コマンドを使用すると、インターフェイスへのアクセスを制御することができます。 指定されたアクセス グループを削除するには、このコマンドの **no** 形式を使用します。 *access-list-name* を使用すると、特定の IPv6 アクセス リストを指定することができます。 **ingress** キーワードを使用すると着信パケットをフィルタリングすることができ、また、**egress** キーワードを使用すると発信パケットをフィルタリングすることができます。

L2 インターフェイスの IPv6 ACL に l2 トランスポート モードで **ipv6 access-group** コマンドを使用します。

（注） **ipv6 access-group** コマンドを使用したパケット フィルタリング アプリケーションの場合、パケット カウンタは各方向のハードウェア内に維持されます。 同じ方向の複数のインターフェイス上で 1 つのアクセス グループが使用される場合、各インターフェイスでパケットがカウントされます。

アクセスリストがアドレスを許可する場合は、ソフトウェアはパケットの処理を継続します。アクセス リストがアドレスを拒否する場合は、ソフトウェアはパケットをドロップして、レートが制限されたインターネット制御メッセージプロトコル（ICMP）ホスト到達不能メッセージを戻します。

指定したアクセス リストが存在しない場合は、すべてのパケットが通過します。

デフォルトでは、一意のまたはインターフェイス単位の ACL 統計情報はディセーブルになっています。

タスク ID

タスク ID	操作
acl	読み取り、書き込み
ipv6	読み取り、書き込み

例

次に、GigabitEthernet interface 0/2/0/2 との間の着信または発信パケットへのフィルタリングの適用方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group p-in-filter ingress
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group p-out-filter egress
```

次に、ハードウェア内のインターフェイス統計情報の適用方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group p-in-filter ingress interface-statistics
```

次に、L2 インターフェイス用に設定された IPv6 ACL の例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# interface gigabitEthernet 0/1/0/4
RP/0/RSP0/CPU0:router(config-if)# l2transport
```

```
RP/0/RSP0/CPU0:router(config-if-l2)# ipv6 access-group access-grp1 ingress
RP/0/RSP0/CPU0:router(config-if-l2)# ipv6 access-group access-grp2 ingress
```

関連コマンド

コマンド	説明
copy access-list ipv6, （11 ページ）	既存の IPv6 アクセス リストをコピーします。
deny（IPv6） , （25 ページ）	IPv6アクセス リストの拒否条件を設定します。
ipv6 access-list , （43 ページ）	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
permit（IPv6） , （75 ページ）	パケットが名前付き IPv6 アクセス リストを渡す条件を設定します。
show ipv6 interface	IPv6向けに設定されたインターフェイスの使用状況を表示します。

ipv6 access-list

IPv6 アクセス リストを定義してルータを IPv6 アクセス リスト コンフィギュレーション モードに設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用します。 アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

ipv6 access-list *name*

no ipv6 access-list *name*

構文の説明

name	IPv6 アクセス リスト名。 名前は、スペース、疑問符を含むことができず、また、数字で始めることはできません。

コマンド デフォルト

定義されている IPv6 アクセス リストはありません。

コマンド モード

グローバル コンフィギュレーション

L2 トランスポート

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ipv6 access-list コマンドは、IPv6 に固有のものを除き、**ipv4 access-list** コマンドと類似しています。

IPv6 アクセス リストは、送信元と宛先アドレス、IPv6 オプション ヘッダー、およびより細かな精度の制御のための上位層プロトコル タイプの情報に基づくトラフィック フィルタリングに使用されます。 IPv6 アクセス リストは **ipv6 access-list** コマンドをグローバル コンフィギュレーション モードで使用することにより定義され、その許可と拒否の条件は **deny** および **permit** コマンドを IPv6 アクセス リスト コンフィギュレーション モードで使用することにより設定されます。 **ipv6 access-list** コマンドを設定すると、ルータを IPv6 アクセス リスト コンフィギュレーション モードに設定し、プロンプト router は router (config-ipv6-acl)# に変わります。 IPv6 アクセス リスト コン

フィギュレーション モードから、定義済みの IPv6 アクセス リストに許可および拒否の条件を設定できます。

L2 インターフェイスの IPv6 ACL に l2 トランスポート モードで **ipv6 access-list** コマンドを使用します。

IPv6 オプション ヘッダーおよび省略可能な上位層プロトコル タイプ情報に基づく IPv6 トラフィックのフィルタリングの詳細については、deny（IPv6）， （25 ページ）および permit（IPv6）， （75 ページ）コマンドを参照してください。 変換済み IPv6 アクセス コントロール リスト（ACL）コンフィギュレーションの例については、「例」を参照してください。

（注） 方向単位に 1 つのインターフェイスに適用できる IPv6 アクセス リストは 1 つだけです。

（注） どの IPv6 アクセス リストにも最後の一致条件として暗黙の **deny ipv6 any any** ステートメントがあります。 1 つの IPv6 アクセス リストには、暗黙の **deny ipv6 any any** ステートメントを有効にするために少なくとも 1 つのエントリが含まれる必要があります。

（注） アクセス リストでなく、IPv6 プレフィックス リストは、ルーティング プロトコル プレフィックスのフィルタリングに使用する必要があります。

access-list-name 引数を持つ **ipv6 access-group** インターフェイス コンフィギュレーション コマンドを使用すると、IPv6 アクセス リストを IPv6 インターフェイスに適用することができます。

（注） **ipv6 access-group** コマンドを持つインターフェイスに適用される IPv6 アクセス リストは、ルータが発信でなく転送するトラフィックをフィルタリングします。

（注） すべての IPv6 ACL には最後の一致条件として、暗黙の **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および **deny ipv6 any any** ステートメントがあります （元の 2 つの一致条件により ICMPv6 ネイバー探索が可能になります）。1 つの IPv6 ACL には、暗黙の **deny ipv6 any any** ステートメントを有効にするために少なくとも 1 つのエントリが含まれる必要があります。**permit icmp any any nd-na permit icmp any any nd-ns deny ipv6 any any deny ipv6 any any**

IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを利用するため、デフォルトで、インターフェイス上での IPv6 ネイバー探索パケットの送受信が IPv6 ACL によって暗黙的に許可されます。 IPv4 の場合、IPv6 ネイバー探索プロセスに相当するアドレス解決プロトコル（ARP）では、個別のデータ リンク層プロトコルを利用するため、デフォルトで、インターフェイス上での ARP パケットの送受信が IPv4 ACL によって暗黙的に許可されます。

タスク ID

タスク ID	操作
acl	読み取り、書き込み
ipv6	読み取り、書き込み

例

次に、list2 という名前の IPv6 アクセス リストの設定してその ACL をインターフェイス GigabitEthernet 0/2/0/2 上の発信トラフィックに適用する方法の例を示します。 具体的には、1 番目の ACL エントリにより、ネットワーク fec0:0:0:2::/64（発信元 IPv6 アドレスの 1 番目の 64 ビットのようなサイトローカルプレフィックス fec0:0:0:2）からのすべてのパケットがインターフェイス GigabitEthernet 0/2/0/2 から出て行くのが防止されます。 ACL の 2 番目のエントリは、その他のすべてのトラフィックがインターフェイス GigabitEthernet 0/2/0/2 から出て行くことを許可します。 2 番目のエントリは、各 IPv6 ACL の末尾に暗黙的な deny all 条件があるため、必要となります。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list list2
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 10 deny fec0:0:0:2::/64 any
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 20 permit any any

RP/0/RSP0/CPU0:router# show ipv6 access-lists list2

ipv6 access-list list2
  10 deny ipv6 fec0:0:0:2::/64 any
  20 permit ipv6 any any

RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group list2 out
```

（注） IPv6 は、グローバル コンフィギュレーション モードから IPv6 アクセス リスト コンフィギュレーション モードに変換される **permit any any** ステートメントおよび **deny any any** ステートメントでプロトコル タイプとして自動的に設定されます。

（注） IPv6 ルータは、送信元または宛先アドレスのいずれかとしてリンクローカル アドレスを持つ別のネットワークの IPv6 パケットに転送されません（パケットの送信元インターフェイスは、パケットの宛先インターフェイスとは異なります）。

次に、L2 インターフェイス用に設定された IPv6 ACL の例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# interface gigabitEthernet 0/1/0/4
RP/0/RSP0/CPU0:router(config-if)# l2transport
RP/0/RSP0/CPU0:router(config-if-l2)# ipv6 access-list LIST1 ingress
RP/0/RSP0/CPU0:router(config-if-l2)# ipv6 access-list LIST2 ingress
```

関連コマンド

コマンド	説明
deny（IPv6） , （25 ページ）	IPv6アクセス リストの拒否条件を設定します。
permit（IPv6） , （75 ページ）	IPv6アクセス リストの許可条件を設定します。
remark（IPv6） , （83 ページ）	IPv6 アクセス リスト エントリに関する有益な設定を挿入します。

ipv6 access-list log-update rate

IPv6 アクセス リストが記録されるレートを指定するには、グローバル コンフィギュレーション モードで **ipv6 access-list log-update rate** コマンドを使用します。 更新レートをデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ipv6 access-list log-update rate *rate-number*

no ipv6 access-list log-update rate *rate-number*

構文の説明

rate-number	ルータ上で IPv6 アクセス ヒット ログが生成される毎秒のレート。 範囲は 1 ～ 1000 です。

コマンド デフォルト

デフォルトは 1 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

rate-number 引数は、インターフェイスに設定されたすべての IPv6 アクセス リストに適用されます。 つまり、システムに常に 1 ～ 1000 のログ エントリがあるということです。

タスク ID

タスク ID	操作
ipv6	読み取り、書き込み
acl	読み取り、書き込み

例

次に、システムの IPv6 アクセス ヒット ロギング レートを設定する方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list log-update rate 10
```

ipv6 access-list log-update threshold

IPv6アクセスリスト（ACL）に記録される更新数を指定するには、グローバルコンフィギュレーション モードで **ipv6 access-list log-update threshold** コマンドを使用します。 ロギングの更新数をデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ipv6 access-list log-update threshold *update-number*

no ipv6 access-list log-update threshold *update-number*

構文の説明

update-number	ルータに設定された IPv6 アクセス リストごとに記録される更新数。範囲は 0 ～ 2147483647 です。

コマンド デフォルト

IPv6 アクセス リストの場合、350000 の更新が記録されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ipv6 access-list log-update threshold コマンドは、IPv6 固有のものを除き、**ipv4 access-list log-update threshold** コマンドと類似しています。

IPv6 アクセス リスト更新は、1 番目のロギング更新に続いて 5 分間隔で記録されます。 ロギングをより頻繁に更新する場合は、更新数を小さく（デフォルトよりも小さい数）するほうが有益です。

タスク ID

タスク ID	操作
acl	読み取り、書き込み

タスク ID	操作
ipv6	読み取り、書き込み

例

次に、ルータに設定された IPv6 アクセス リストごとに 10 の更新のロギングしきい値を設定する方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list log-update threshold 10
```

ipv6 access-list maximum ace threshold

IPv6アクセス リストのアクセス コントロール エントリ（ACE）の最大数を設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list maximum ace threshold** コマンドを使用します。 IPv6アクセス リストのACE制限をリセットするには、このコマンドの **no** 形式を使用します。

ipv6 access-list maximum ace threshold *ace-number*

no ipv6 access-list maximum ace threshold *ace-number*

構文の説明

ace-number	ACE の設定可能最大数。 範囲は 50000 ～ 350000 です。

コマンド デフォルト

IPv6 アクセス リストでは、50,000 の ACE が設定可能です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク IDを含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ipv6 access-list maximum ace threshold コマンドを使用すると、IPv6 アクセス リストの ACE の設定可能最大数を設定することができます。 Out Of Resource（OOR）は、システムに設定可能な ACE 数を制限します。 ACE の設定可能最大数に達した場合、新しい ACE の設定は拒否されます。

タスク ID

タスク ID	操作
acl	読み取り、書き込み
ipv6	読み取り、書き込み

例

次に、IPv6 アクセス リストの ACE の最大数を 75000 に設定する方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list maximum ace threshold 75000
```

関連コマンド

コマンド	説明
show access-lists ipv6, （98 ページ）	現在のすべての IPv6 アクセス リストの内容を表示します。

ipv6 access-list maximum acl threshold

IPv6 アクセス コントロール リスト（ACL）の設定可能最大数を設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list maximum acl threshold** コマンドを使用します。 IPv6 ACL 制限をリセットするには、このコマンドの **no** 形式を使用します。

ipv6 access-list maximum acl threshold *acl-number*

no ipv6 access-list maximum ace threshold *acl-number*

構文の説明

acl-number	ACL の設定可能最大数。 範囲は 1000 ～ 16000 です。

コマンド デフォルト

1000 の IPv6 ACL を設定できます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ipv6 access-list maximum acl threshold コマンドを使用すると、IPv6 ACL の設定可能最大数を設定することができます。 Out Of Resource（OOR）は、システムに設定可能な ACL 数を制限します。この制限に達すると、新しい ACL が拒否されます。

タスク ID

タスク ID	操作
acl	読み取り、書き込み
ipv6	読み取り、書き込み

例

次に、IPv6 ACL の設定可能最大数を 1500 に設定する方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list maximum acl threshold 1500
```

関連コマンド

コマンド	説明
show access-lists ipv6, （98 ページ）	現在のすべての IPv6 アクセス リストの内容を表示します。

permit（IPv4）

IPv4 アクセス リストの条件を設定するには、アクセス リスト コンフィギュレーション モードで **permit** コマンドを使用します。 **permit** コマンドには、**permit** (source)、および **permit** (protocol) の 2 つのバージョンがあります。 アクセス リストから条件を削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **permit** *source* [*source-wildcard*] [**log**| **log-input**]

[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* **[capture]** [**precedence** *precedence*] [**default nexthop** [*ipv4-address1*] [*ipv4-address2*] [*ipv4-address3*]] [**dscp** *dscp*] **[fragments]** [**log**| **log-input**] [**nexthop** [**track** *track-name*] [*ipv4-address1*] [*ipv4-address2*] [*ipv4-address3*]] [**ttl** *ttl value* [*value1 ... value2*]]

no *sequence-number*

Internet Control Message Protocol (ICMP)

[*sequence-number*] **permit icmp** *source source-wildcard destination destination-wildcard* [*icmp-type*] [*icmp-code*] [**precedence** *precedence*] [**dscp** *dscp*] **[fragments]** [**log**| **log-input**] **[icmp-off]**

Internet Group Management Protocol (IGMP)

[*sequence-number*] **permit igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**dscp** *value*] **[fragments]** [**log**| **log-input**]

User Datagram Protocol (UDP)

[*sequence-number*] **permit udp** *source source-wildcard* [*operator* {*port*| *protocol-port*}] *destination destination-wildcard* [*operator* {*port*| *protocol-port*}] [**precedence** *precedence*] [**dscp** *dscp*] **[fragments]** [**log**| **log-input**]

構文の説明

sequence-number	（任意）アクセス リスト中の **permit** ステートメントの番号。この番号により、アクセスリスト中のステートメントの順番を識別します。 範囲は 1 ～ 2147483644 です。 （デフォルトで、最初のステートメントの番号は 10 で、後続のステートメントは 10 ずつ増加していきます）。**resequence access-list** コマンドを使用すると、設定済みアクセス リスト中の最初のステートメントの番号を変更し、後続のステートメントの番号を増加することができます。

source	パケットの送信元のネットワークまたはホストの番号。送信元を指定する場合、代わりに次の 3 つの方法を使用できます。 • 32 ビットの 4 分割ドット付き 10 進表記を使用する。 • **any** キーワードを、0.0.0.0 255.255.255.255 の *source* および *source-wildcard* の短縮形として使用する。 • **host** *source* の組み合わせを、*source* 0.0.0.0 の *source* および *source-wildcard* の短縮形として使用する。
source-wildcard	送信元に適用されるワイルドカード ビット。 送信元のワイルドカードを指定するには、次の 3 つの方法から選択します。 • 32 ビットの 4 分割ドット付き 10 進表記を使用する。 無視するビット位置に 1 を入れます。 • **any** キーワードを、0.0.0.0 255.255.255.255 の *source* および *source-wildcard* の短縮形として使用する。 • **host** *source* の組み合わせを、*source* 0.0.0.0 の *source* および *source-wildcard* の短縮形として使用する。

protocol	IP プロトコルの名前または番号。 キーワード **ahp** 、 **esp** 、 **eigrp** 、 **gre** 、 **icmp** 、 **igmp** 、 **igrp** 、 **ip** 、 **ipinip** 、 **nos** 、 **ospf** 、 **pim** 、 **pcp** 、 **tcp** 、または **udp** のいずれか 1 つ、あるいは IP プロトコル番号を表す 0 ～ 255 の整数にすることができます。 任意のインターネット プロトコル（ICMP、TCP、および UDP を含む）に一致させるには、**ip** キーワードを使用します。 ICMP および TCP では、さらに、このテーブルの後半に記載されている修飾子を許可します。
destination	パケットの宛先のネットワークまたはホストの番号。宛先を指定するには、次の 3 つの方法から選択します。 • 32 ビットの 4 分割ドット付き 10 進表記を使用する。 • **any** キーワードを、0.0.0.0 255.255.255.255 の *destination* および *destination-wildcard* の短縮形として使用する。 • **host** *destination* の組み合わせを、*destination* 0.0.0.0 の *destination* および *destination-wildcard* の短縮形として使用する。

destination-wildcard	宛先に適用されるワイルドカード ビット。 宛先のワイルドカードを指定するには、次の 3 つの方法から選択します。 • 32 ビットの 4 分割ドット付き 10 進表記を使用する。 無視するビット位置に 1 を入れます。 • **any** キーワードを、0.0.0.0 255.255.255.255 の *destination* および *destination-wildcard* の短縮形として使用する。 • **host** *destination* の組み合わせを、*destination* 0.0.0.0 の *destination* および *destination-wildcard* の短縮形として使用する。

precedence *precedence*	（任意）パケットは、precedence レベル（0 ～ 7 の番号で指定）または次の名前でフィルタリングできます。 • **Routine**：パケットを routine precedence（0）と一致させます。 • **priority**：パケットを priority precedence（1）と一致させます。 • **immediate**：パケットを immediate precedence（2）と一致させます。 • **flash**：パケットを flash precedence（3）と一致させます。 • **flash-override**：パケットを flash override precedence（4）と一致させます。 • **critical**：パケットを critical precedence（5）と一致させます。 • **internet**：パケットを internetwork control precedence（6）と一致させます。 • **network**：パケットを network control precedence（7）と一致させます。

default	（任意）このエントリのデフォルトのネクストホップを指定します。 **default** キーワードを設定すると、ACLベースの転送アクションが実行されるのは、パケットの宛先の PLU ルックアップの結果によりデフォルトルートを決定する場合、つまり、パケット宛先のルートを指定しない場合だけとなります。
capture	一致するトラフィックをキャプチャします。 ミラーリング送信元ポートで acl コマンドを設定するときに、ACL コンフィギュレーションコマンドが **capture** キーワードを使用しない場合、トラフィックはミラーリングされません。ACL 設定が **capture** キーワードを使用し、acl コマンドが送信元ポートで設定されていない場合、ポートトラフィック全体がミラーリングされ、**capture** アクションは影響を受けません。

ipv4-address1 ipv4-address2 ipv4-address3	（任意）1 ～ 3 のネクストホップ アドレスを使用します。 IP アドレスのタイプの定義は、次のとおりです。 • デフォルトの IP アドレス：ルーティング テーブル内にパケットの宛先アドレスの暗黙ルートがない場合、パケットを転送する必要のある宛先へのパスにあるネクスト ホップ ルータを指定します。 現在稼働中の接続されたインターフェイスに関連付けられた最初の IP アドレスは、パケットのルーティングに使用されます。 • 指定された IP アドレス：パケットを転送する必要のある宛先へのパスにあるネクスト ホップ ルータを指定します。 現在稼働中の接続されたインターフェイスに関連付けられた最初の IP アドレスは、パケットのルーティングに使用されます。

dscp *dscp*

（任意）DiffServ コードポイント（DSCP）により、Quality of Service のコントロールが提供されます。 *dscp* の値は次のとおりです。

- 0–63：ディファレンシエーテッド サービス コードポイント値。
- af11：パケットを AF11 dscp（001010）と一致させます。
- af12：パケットを AF12 dscp（001100）と一致させます。
- af13：パケットを AF13 dscp（001110）と一致させます。
- af21：パケットを AF21 dscp（010010）と一致させます。
- af22：パケットを AF22 dscp（010100）と一致させます。
- af23：パケットを AF23 dscp（010110）と一致させます。
- af31：パケットを AF31 dscp（011010）と一致させます。
- af32：パケットを AF32 dscp（011100）と一致させます。
- af33：パケットを AF33 dscp（011110）と一致させます。
- af41：パケットを AF41 dscp（100010）と一致させます。
- af42：パケットを AF42

dscp（100100）と一致させます。

- af43：パケットを AF43 dscp（100110）と一致させます。
- cs1：パケットを CS1（precedence 1）dscp（001000）と一致させます。
- cs2：パケットを CS2（precedence 2）dscp（010000）と一致させます。
- cs3：パケットを CS3（precedence 3）dscp（011000）と一致させます。
- cs4：パケットを CS4（precedence 4）dscp（100000）と一致させます。
- cs5：パケットを CS5（precedence 5）dscp（101000）と一致させます。
- cs6：パケットを CS6（precedence 6）dscp（110000）と一致させます。
- cs7：パケットを CS7（precedence 7）dscp（111000）と一致させます。
- default：デフォルト DSCP（000000）
- ef：パケットを EF dscp（101110）と一致させます。

fragments	（任意）このアクセス リスト エントリーを適用すると、ソフトウェアが IPv4 パケットの非初期フラグメントを検査するようになります。このキーワードを指定すると、フラグメントがアクセス キー リスト エントリーによる制約を受けます。
log	（任意）コンソールに送信されるエントリに一致するパケットに関するロギング メッセージ情報が出力されます。（コンソールに記憶されるメッセージのレベルは **logging console** コマンドで制御します） このメッセージに含まれるものには、アクセスリスト番号、パケットが許可されたか拒否されたか、プロトコルが TCP、UDP、ICMP、または番号であったか、さらに、該当する場合は、送信元と宛先アドレス、および送信元と宛先ポート番号があります。このメッセージは、フローに一致した最初のパケットに対して生成され、5 分間隔で、前の 5 分間に許可または拒否されたパケット数を含みます。
log-input	（任意）ロギング メッセージに入力インターフェイスも含まれることを除き、**log** キーワードと同じ機能を提供します。
nexthop1、nexthop2、nexthop3	（任意）このエントリの指定されたネクストホップを転送します。
track *track-name*	このネクストホップの TRACK 名を指定します。
ttl	（任意）Time-To-Life（TTL）値との一致をオンにします。

ttl value [*value1 ... value2*]	（任意）フィルタリングに使用される TTL 値 値の範囲は 1 ～ 255 です。 *value* が指定される場合にだけ、この値に対する一致になります。 *value1* および *value2* の両方が指定された場合、*value1* と *value2* の間の TTL の範囲に対してパケット TTL が一致されます。
icmp-off	（任意）拒否されたパケットに対して ICMP の生成をオフにします。
icmp-type	（任意）ICMP パケットのフィルタリングのための ICMP メッセージ タイプ。 範囲は 0 ～ 255 です。
icmp-code	（任意）ICMP パケットのフィルタリングのための ICMP メッセージ コード。 範囲は 0 ～ 255 です。
igmp-type	（任意）IGMP パケットをフィルタリングするための、IGMP メッセージ タイプ（0 ～ 15）または次のようなメッセージ名。 • dvmrp • host-query • host-report • mtrace • mtrace-response • pim • precedence • トレース • v2-leave • v2-report • v3-report

operator	（任意）演算子は、送信元ポートまたは宛先ポートを比較するために使用されます。 オペランドとして使用可能なものには、**lt**（less than：より小さい）、**gt**（greater than：より大きい）、**eq**（equal：等しい）、**neq**（not equal：等しくない）、および **range**（inclusive range：包含範囲）があります。 演算子を *source* および *source-wildcard* の値の後に置く場合、送信元ポートと一致する必要があります。 演算子を *destination* および *destination-wildcard* の値の後に置く場合、宛先ポートと一致する必要があります。 演算子を **ttl** キーワードの後に置く場合、TTL 値と一致します。 **range** 演算子には 2 つのポート番号が必要です。他のすべての演算子は 1 つのポート番号が必要です。
port	TCP または UDP ポートの 10 進数。 範囲は 0 ～ 65535 です。 TCP ポートは、TCP をフィルタリングする場合にだけ使用できます。 UDP ポートは、UDP をフィルタリングする場合にだけ使用できます。
protocol-port	TCP または UDP ポートの名前。 TCP および UDP ポートの名前は、「使用上のガイドライン」に示されています。 TCP ポート名は TCP をフィルタリングする場合に限り使用できます。 UDP ポート名は UDP をフィルタリングする場合に限り使用できます。

established	（任意）TCPプロトコルの場合にだけ、確立された接続を表示します。
match-any	（任意）TCPプロトコルの場合にだけ、TCPフラグの任意の組み合わせをフィルタリングします。
match-all	（任意）TCPプロトコルの場合にだけ、すべての TCP フラグをフィルタリングします。
+ | -	（必須）TCP プロトコル **match-any**、**match-all** の場合、プレフィックス *flag-name* の前に + または - を付けます。 TCP フラグを設定したパケットを一致させるには、+*flag-name* 引数を使用します。 TCP フラグを設定してないパケットを一致させるには、-*flag-name* 引数を使用します。
flag-name	（任意）TCP プロトコルが **match-any**、**match-all** の場合。フラグの名前は、 **ack** 、 **fin** 、 **psh** 、 **rst** 、 **syn** になります。

コマンド デフォルト

IPv4 アクセス リストの送受信時にパケットが拒否される特定の条件はありません。

ICMP メッセージの生成はデフォルトでイネーブルです。

コマンド モード

IPv4 アクセス リストの設定

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 4.0.1	**capture** キーワードが追加されました。

使用上のガイドライン このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ipv4 access-list コマンドに続いて **permit** コマンドを使用すると、パケットがアクセス リストを通過できる条件を指定することができます。

デフォルトでは、アクセス リストの最初のステートメントは 10 で、その次のステートメントからは 10 ずつ増加します。

permit、**deny**、または **remark** ステートメントを、リスト全体を再入力せずに既存のアクセス リストに追加できます。 新しいステートメントをリストの最後尾以外に追加するには、所属先を示すために 2 つの既存のエントリ番号の間にある適切なエントリ番号を持つ新しいステートメントを作成します。

2 つの連続した番号のステートメントの間（たとえば、10 行と 11 行の間）にステートメントを追加する場合は、最初に **resequence access-list** コマンドを使用して、最初のステートメントに番号を付け直して、後続の各ステートメントの番号を増加させます。 *increment* 引数を使用すると、ステートメント間に新しい未使用の行番号が生成されます。次に、アクセス リスト中の所属先を指定する *entry-number* を持つ新しいステートメントを追加します。

次に、precedence の名前のリストを示します。

- critical
- flash
- flash-override
- immediate
- internet
- ネットワーク
- priority
- routine

次に、ICMP メッセージ タイプの名前のリストを示します。

- administratively-prohibited
- alternate-address
- conversion-error
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- general-parameter-problem

- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- reassembly-timeout
- redirect
- router-advertisement
- router-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request

- traceroute
- ttl-exceeded
- unreachable

次に、ポート番号の代わりに使用できるTCPポート名のリストを示します。 これらのプロトコルの参考情報については、現在の *Assigned Numbers* RFC を参照してください。 ポート番号の位置に ? を入力すると、これらのプロトコルに対応するポート番号を見つけることができます。

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- ホスト名
- ident
- irc
- klogin
- kshell
- login
- lpd
- nntp
- pim-auto-rp
- pop2
- pop3
- smtp
- sunrpc
- tacacs
- talk

- telnet
- time
- uucp
- whois
- www

次の UDP ポート名は、ポート番号の代わり使用できます。 これらのプロトコルの参考情報については、現在の *Assigned Numbers* RFC を参照してください。 ? を入力すると、これらのプロトコルに対応するポート番号を見つけることができます。

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs
- talk
- tftp
- time
- who
- xdmcp

次のフラグを、**match-any** と **match-all** キーワード、および + と - 記号とともに使用すると、表示するフラグを選択することができます。

- ack
- fin
- psh
- rst
- syn

たとえば、**match-all** + *ack* + *syn* は TCP パケットを ack および syn フラグを設定して表示し、**match-any** + *ack* - *syn* は TCP パケットを ack を設定するか syn を設定しないで表示します。

タスク ID

タスク ID	操作
ipv4	読み取り、書き込み
acl	読み取り、書き込み

例

次に、Internetfilter という名前のアクセス リストの許可条件を設定する方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 permit 192.168.34.0 0.0.0.255
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 20 permit 172.16.0.0 0.0.255.255
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 25 permit tcp host 172.16.0.0 eq bgp host
192.168.202.203 range 1300 1400
RP/0/RSP0/CPU0:router(config-ipv4-acl)# deny 10.0.0.0 0.255.255.255
```

関連コマンド

コマンド	説明
deny（IPv4），（13 ページ）	**IPv4 アクセス リストの条件を設定します。**
ipv4 access-group,（31 ページ）	インターフェイス上の着信または発信の IPv4 トラフィックをフィルタリングします。
ipv4 access-list ,（34 ページ）	IPv4 アクセス リストを定義し、また、IPv4 アクセス リスト コンフィギュレーション モードを開始します。
remark（IPv4），（81 ページ）	IPv4 アクセス リスト エントリに関する有益な設定を挿入します。

コマンド	説明
deny（IPv4），（13 ページ）	**IPv4 アクセス リストの条件を設定します。**
resequence access-list ipv4 ，（85 ページ）	既存の IPv4 アクセス リスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。
show access-lists ipv4 ，（92 ページ）	現在の IPv4 アクセス リストすべての内容を表示します。

permit（IPv6）

IPv6 アクセス リストの許可条件を設定するには、IPv6 アクセス リスト コンフィギュレーション モードで **permit** コマンドを使用します。 許可条件を削除するには、このコマンドの **no** 形式を使用します。

[sequence-number] **permit** *protocol* {*source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address*}[*operator* {*port* | *protocol-port*} capture] [**dscp** *value*] [**routing**] [**authen**] [**destopts**] [**fragments**] [*packet-length operator packet-length value*] [**log** | **log-input**] [**ttl** *operator ttl value*]**[default] nexthop1** [**vrf** *vrf-name-1*] [**ipv6** *ipv6-address-1*] [**nexthop2** [**vrf** *vrf-name-2*] [**ipv6** *ipv6-address-2*] [**nexthop3** [**vrf** *vrf-name-3*] [**ipv6** *ipv6-address-3*]]]

no *sequence-number*

Internet Control Message Protocol (ICMP)

[sequence-number] **permit icmp** {*source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address*} {*destination-ipv6-prefix/ prefix-length* | *any* | *host destination-ipv6-address*}[*icmp-type*] [*icmp-code*][**dscp** *value*] [routing] [**authen**] [**destopts**] [**fragments**] [**log**] [**log-input**] [**icmp-off**]

Transmission Control Protocol (TCP)

[sequence-number] **permit tcp**{*source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address*}[*operator*{*port* | *protocol-port*}]{*destination-ipv6-prefix/ prefix-length* | *any* | *host destination-ipv6-address*}[*operator*{*port* | *protocol* | *port*}] [**dscp** *value*] [**routing**] [**authen**] [**destopts**] [**fragments**] [**established**]{**match-any | match-all | + | -**}[*flag-name*] [**log**] [**log-input**]

User Datagram Protocol (UDP)

[sequence-number] **permit tcp**{*source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address*}[*operator*{*port* | *protocol-port*}]{*destination-ipv6-prefix/ prefix-length* | *any* | *host destination-ipv6-address*}[*operator*{*port* | *protocol* | *port*}] [**dscp** *value*] [**routing**] [**authen**] [**destopts**] [**fragments**] [**established**][*flag-name*] [**log**] [**log-input**]

構文の説明

sequence-number	（任意）アクセス リスト中の **permit** ステートメントの番号。 この番号により、アクセス リスト中のステートメントの順番を識別します。 範囲は 1 ～ 2147483644 です （デフォルトで、最初のステートメントの番号は 10 で、後続のステートメントは 10 ずつ増加していきます）。**resequence access-list** コマンドを使用すると、設定済みアクセス リスト中の最初のステートメントの番号を変更し、後続のステートメントの番号を増加することができます。
protocol	インターネット プロトコルの名前または番号。 次のキーワードのいずれかになります。**ahp**、 **eigrp**、 **esp**、 **gre**、 **icmp**、 **igmp**、 **igrp**、 **isinip**、 **ipv6**、 **nos**、 **ospf**、 **pcp**、 **sctp**、 **tcp**、or **udp**、または IPv6 プロトコル番号を表す 0 ～ 255 の範囲の整数。

source-ipv6-prefix / *prefix-length*	許可条件が設定される送信元の IPv6 ネットワークまたはネットワークのクラス。 この引数は、RFC 2373 に記載されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
any	IPv6 プレフィックス ::/0 の省略形。
capture	一致するトラフィックをキャプチャします。 ミラーリング送信元ポートで acl コマンドを設定するときに、ACL コンフィギュレーション コマンドが **capture** キーワードを使用しない場合、トラフィックはミラーリングされません。 ACL 設定が **capture** キーワードを使用し、acl コマンドが送信元ポートで設定されていない場合、ポートトラフィック全体がミラーリングされ、**capture** アクションは影響を受けません。
host *source-ipv6-address*	許可条件の設定先に関する、送信元の IPv6 ホスト アドレス。 *source-ipv6-address* 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。
vrf *vrf-name*	VPN ルーティング/転送（VRF）インスタンスを指定します。
nexthop1、**nexthop2**、**nexthop3**	（任意）このエントリのネクスト ホップを指定します。
operator {*port* | *protocol-port*}	（任意）指定されたプロトコルの送信元ポートまたは宛先ポートを比較するオペランド。 オペランドには、**lt**（less than：より小さい）、**gt**（greater than：より大きい）、**eq**（equal：等しい）、**neq**（not equal：等しくない）、および **range**（inclusive range：包含範囲）があります。 *source-ipv6-prefix* / *prefix-length* 引数の後ろに演算子が置かれた場合、送信元ポートと一致する必要があります。 *destination-ipv6-prefix* / *prefix-length* 引数の後ろに演算子が置かれた場合、宛先ポートと一致する必要があります。 **range** 演算子には 2 つのポート番号が必要です。 他のすべての演算子は 1 つのポート番号が必要です。 *port* 引数は、TCP または UDP ポートの 16 進数です。 ポート番号の範囲は 0 ～ 65535 です。 *protocol-port* 引数は、TCP または UDP ポートの名前です。 TCP ポート名は TCP をフィルタリングする場合に限り使用できます。 UDP ポート名は UDP をフィルタリングする場合に限り使用できます。

destination-ipv6-prefix / prefix-length	許可条件が設定される宛先の IPv6 ネットワークまたはネットワークのクラス。 この引数は、RFC 2373 に記載されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
host *destination-ipv6-address*	許可条件が設定される宛先の IPv6 ホスト アドレスを指定します。 *destination-ipv6-address* 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。
dscp *value*	（任意）DiffServ コード ポイント（DSCP）値を、各 IPv6 パケット ヘッダーの Traffic Class フィールドのトラフィック クラス値に一致させます。範囲は 0 ～ 63 です。
ルーティング	（任意）ソースルート パケットを、各 IPv6 パケット ヘッダー内の拡張ヘッダーに一致させます。
authen	（任意）IPv6 認証ヘッダーが存在する場合に一致します。
destopts	（任意）IPv6 宛先オプション ヘッダーが存在する場合に一致します。
fragments	（任意）フラグメント拡張ヘッダーにゼロ以外のフラグメント オフセットが含まれているフラグメント化された非初期パケットと一致させます。**fragments** キーワードは、*operator* [*port-number*] 引数が指定されていない場合に限り指定できるオプションです。
log	（任意）コンソールに送信されるエントリに一致するパケットに関するロギング メッセージ情報が出力されます。（コンソールに記憶されるメッセージのレベルは **logging console** コマンドで制御します） このメッセージに含まれるものには、アクセス リスト名とシーケンス番号、パケットが許可されているか、プロトコルが TCP、UDP、ICMP、または番号であるか、さらに、該当する場合は、送信元と宛先アドレス、および送信元と宛先ポート番号があります。 メッセージは、一致した最初のパケットに対して生成され、その後、5 分間隔で、その 5 分間隔の前に許可されたパケット数を含めて生成されます。
log-input	（任意）**log** キーワードと同じ機能を提供しますが、ロギング メッセージに入力インターフェイスも含まれます。
ttl	（任意）存続可能時間（TTL）値との一致をオンにします。
operator	（任意）指定されたプロトコルの送信元ポートまたは宛先ポートを比較するオペランド。 オペランドには、**lt**（less than：より小さい）、**gt**（greater than：より大きい）、**eq**（equal：等しい）、**neq**（not equal：等しくない）、および **range**（inclusive range：包含範囲）があります。

ttl value [*value1 value2*]	（任意）フィルタリングに使用される TTL 値 範囲は 1 ～ 255 です。 *value* が指定される場合にだけ、この値に対する一致になります。 *value1* および *value2* の両方が指定された場合、*value1* と *value2* の間の TTL の範囲に対してパケット TTL が一致されます。
icmp-off	（任意）拒否されたパケットに対して ICMP 生成をオフにします。
icmp-type	（任意）ICMP パケットのフィルタリングのための ICMP メッセージ タイプ。 範囲は 0 ～ 255 です。
icmp-code	（任意）ICMP パケットのフィルタリングのための ICMP メッセージ コード。 範囲は 0 ～ 255 です。
established	（任意）TCP プロトコルの場合にだけ、確立された接続を表示します。
match-any	（任意）TCP プロトコルの場合にだけ、TCP フラグの任意の組み合わせをフィルタリングします。
match-all	（任意）TCP プロトコルの場合にだけ、すべての TCP フラグをフィルタリングします。
+ | -	（必須）TCP プロトコル **match-any**、**match-all** の場合、プレフィックス *flag-name* の前に + または - を付けます。 TCP フラグを設定したパケットを一致させるには、+*flag-name* 引数を使用します。 TCP フラグを設定してないパケットを一致させるには、-*flag-name* 引数を使用します。
flag-name	（必須）TCP プロトコルが **match-any**、**match-all** の場合。 フラグの名前は、**ack**、**fin**、**psh**、**rst**、**syn** になります。

コマンド デフォルト

IPv6 アクセス リストは定義されていません。

ICMP メッセージの生成はデフォルトでイネーブルです。

コマンド モード

IPv6 アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 4.0.1	capture キーワードが追加されました。

リリース	変更内容
リリース 4.2.0	VRF-Aware ABF に対して IPv6 サポートがイネーブルにされています。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

permit（IPv6）コマンドは、IPv6 に固有のものを除き、**permit**（IPv4）コマンドと類似しています。

ipv6 access-list コマンドに続いて、**permit**（IPv6）コマンドを使用すると、パケットがアクセス リストを通過する条件を定義することができます。

protocol 引数に **ipv6** を指定すると、パケットの IPv6 ヘッダーを一致対象とします。

デフォルトでは、アクセス リストの最初のステートメントの番号は 10 で、その次のステートメントからは 10 ずつ増加します。

permit、**deny**、または **remark** ステートメントを、リスト全体を再入力せずに既存のアクセス リストに追加できます。 新しいステートメントをリストの最後尾以外に追加するには、所属先を示すために 2 つの既存のエントリ番号の間にある適切なエントリ番号を持つ新しいステートメントを作成します。

source-ipv6-prefix/prefix-length および *destination-ipv6-prefix/prefix-length* の引数は両方とも、トラフィック フィルタリング（送信元プレフィックスがトラフィック送信元に基づいてトラフィックをフィルタリングし、送信先プレフィックスがトラフィック宛先に基づいてトラフィックをフィルタリングする）に使用されます。

（注） アクセス リストでなく、IPv6 プレフィックス リストは、ルーティング プロトコル プレフィックスのフィルタリングに使用する必要があります。

fragments キーワードは、*operator* [*port* | *protocol-port*] 引数が指定されない場合だけに使用可能なオプションです。

タスク ID

タスク ID	操作
acl	読み取り、書き込み

例

次に、toCISCO という名前の IPv6 アクセス リストを設定し、そのアクセス リストを GigabitEthernet interface 0/2/0/2 上の発信トラフィックに適用する方法の例を示します。 具体的には、リスト中の

最初の拒否エントリにより、5000 を超える宛先 TCP ポート番号を持つすべてのパケットは GigabitEthernet interface 0/2/0/2 から出て行かないようになります。 リスト中の 2 番目の拒否エントリによって、5000 より小さい、送信元 UDP ポート番号を持つすべてのパケットは GigabitEthernet interface 0/2/0/2 から出て行かないようになります。 2 番目の拒否エントリは、コンソールにもすべての一致を記録します。 リスト中の最初の許可エントリは、すべての ICMP パケットが GigabitEthernet interface 0/2/0/2 から出て行くことを許可します。 リスト中の 2 番目の許可エントリは、他のすべてのトラフィックが GigabitEthernet interface 0/2/0/2 から出て行くことを許可します。 2 番目の許可エントリは、すべての条件の暗黙的な拒否は各 IPv6 アクセス リストの最後にあるという理由で必要です。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list toCISCO
RP/0/RSP0/CPU0:router(config-ipv6-acl)# deny tcp any any gt 5000
RP/0/RSP0/CPU0:router(config-ipv6-acl)# deny ipv6 any lt 5000 any log
RP/0/RSP0/CPU0:router(config-ipv6-acl)# permit icmp any any
RP/0/RSP0/CPU0:router(config-ipv6-acl)# permit any any
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group tOCISCO out
```

次に、v6-abf-acl という名前の IPv6 アクセス リストを設定し、そのアクセス リストを GigabitEthernet interface 0/0/2/0 上の着信トラフィックに適用する方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list  v6-abf-acl
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 10 permit ipv6 any any default nexthop1 vrf vrf_A
ipv6 11::1 nexthop2 vrf vrf_B ipv6 22::2 nexthop3 vrf vrf_C ipv6 33::3
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 20 permit ipv4 any any
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/0/2/0
RP/0/RSP0/CPU0:router(config-if)#  ipv6 access-group v6-abf-acl ingress
```

関連コマンド

コマンド	説明
deny（IPv6） , （25 ページ）	IPv6 アクセス リストに拒否条件を設定します。
ipv6 access-list , （43 ページ）	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
remark（IPv6） , （83 ページ）	IPv6 アクセス リスト エントリに関する有益な設定を挿入します。
resequence access-list ipv6 , （88 ページ）	既存の IPv6 アクセス リスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。

remark（IPv4）

IPv4 アクセス リスト中のエントリに有益なコメント（注釈）を書くには、IPv4 アクセス リスト コンフィギュレーション モードで **remark** コマンドを使用します。 コメントを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **remark** *remark*

no *sequence-number*

構文の説明

sequence-number	（任意）アクセス リスト中の **remark** ステートメントの番号。 この番号により、アクセス リスト中のステートメントの順番を識別します。 範囲は 1 ～ 2147483646 です。 （デフォルトでは、1 番目のステートメントの番号は 10 で、後続のステートメントの番号は 10 ずつ増加していきます）。
remark	アクセス リスト中のエントリを記述するコメント（最大 255 文字まで）です。

コマンド デフォルト

IPv4 アクセス リストのエントリには注釈がありません。

コマンド モード

IPv4 アクセス リストの設定

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

remark コマンドを使用すると、IPv4 アクセス リスト中のエントリに有益なコメントを書き込むことができます。 コメントを削除するには、このコマンドの **no** 形式を使用します。

注釈は最大 255 文字まで可能で、これより長い文字は切り捨てられます。

削除する注釈のシーケンス番号がわかっている場合は、**no** *sequence-number* コマンドで削除できます。

既存のアクセス リストにステートメントを追加する場合に **resequence access-list ipv4** コマンドを使用すると、連続したエントリのシーケンス番号は追加ステートメントを許可しなくなります。

タスク ID

タスク ID	操作
ipv4	読み取り、書き込み
acl	読み取り、書き込み

例

次の例では、発信 Telnet を使用するための user1 サブネットは許可されません。

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list telnetting
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 remark Do not allow user1 to telnet out
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 20 deny tcp host 172.16.2.88 255.255.0.0 any eq
telnet
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 30 permit icmp any any
RP/0/RSP0/CPU0:router# show ipv4 access-list telnetting

ipv4 access-list telnetting
  0 remark Do not allow user1 to telnet out
  20 deny tcp 172.16.2.88 255.255.0.0 any eq telnet out
  30 permit icmp any any
```

関連コマンド

コマンド	説明
deny（IPv4） , （13 ページ）	IPv4 アクセス リストの拒否条件を設定します。
ipv4 access-list , （34 ページ）	IPv4 アクセス リストを定義し、また、IPv4 アクセス リスト コンフィギュレーション モードを開始します。
permit（IPv4） , （55 ページ）	IPv4 アクセス リストの許可条件を設定します。
resequence access-list ipv4 , （85 ページ）	既存の IPv4 アクセス リスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。
show access-lists ipv4 , （92 ページ）	現在の IPv4 アクセス リストすべての内容を表示します。

remark（IPv6）

IPv6 アクセス リスト中のエントリに有益なコメント（注釈）を書くには、IPv6 アクセス リスト コンフィギュレーション モードで **remark** コマンドを使用します。 コメントを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **remark** *remark*

no *sequence-number*

構文の説明

sequence-number	（任意）アクセス リスト中の **remark** ステートメントの番号。 この番号により、アクセス リスト中のステートメントの順番を識別します。 範囲は 1 ～ 2147483646 です。 （デフォルトでは、1 番目のステートメントの番号は 10 で、後続のステートメントの番号は 10 ずつ増加していきます）。
remark	アクセス リスト中のエントリを記述するコメント（最大 255 文字まで）です。

コマンド デフォルト

IPv6 アクセス リストのエントリには注釈がありません。

コマンド モード

IPv6 アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

remark（IPv6）コマンドは、IPv6 に固有のものを除き、**remark**（IPv4）コマンドと類似しています。

remark コマンドを使用すると、IPv6 アクセス リスト中のエントリに有益なコメントを書き込むことができます。 コメントを削除するには、このコマンドの **no** 形式を使用します。

注釈は最大 255 文字まで可能で、これより長い文字は切り捨てられます。

削除する注釈のシーケンス番号がわかっている場合は、**no** *sequence-number* コマンドで削除できます。

既存のアクセス リストにステートメントを追加する場合に **resequence access-list ipv6** コマンドを使用すると、連続したエントリのシーケンス番号は追加ステートメントを許可しなくなります。

タスク ID

タスク ID	操作
acl	読み取り、書き込み

例

次の例では、1 つの注釈が追加されています。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list Internetfilter
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 10 permit ipv6 3333:1:2:3::/64 any
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 20 permit ipv6 4444:1:2:3::/64 any
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 30 permit ipv6 5555:1:2:3::/64 any
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 39 remark Block BGP traffic from a given host
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 40 deny tcp host 6666:1:2:3::10 eq bgp host
7777:1:2:3::20 range 1300 1400
RP/0/RSP0/CPU0:router# show ipv6 access-list Internetfilter

ipv6 access-list Internetfilter
  10 permit ipv6 3333:1:2:3::/64 any
  20 permit ipv6 4444:1:2:3::/64 any
  30 permit ipv6 5555:1:2:3::/64 any
  39 remark Block BGP traffic from a given host
  40 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range host 6666:1:2:3::10 eq
bgp host 7777:1:2:3::20 range 1300 1400
```

関連コマンド

コマンド	説明
deny（IPv6）, （25 ページ）	IPv6アクセス リストの拒否条件を設定します。
ipv6 access-list, （43 ページ）	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
permit（IPv6）, （75 ページ）	IPv6アクセス リストの許可条件を設定します。
resequence access-list ipv6, （88 ページ）	既存の IPv6 アクセス リスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。

resequence access-list ipv4

既存のステートメントに番号を付け直し、後続のステートメントの番号を増加させて、新しいIPv4アクセス リスト ステートメント（**permit**、**deny**、または **remark**）を追加できるようにするには、EXEC モードで **resequence access-list ipv4** コマンドを使用します。

resequence access-list ipv4 *name* [*base* [*increment*]]

構文の説明

name	IPv4 アクセス リストの名前。
base	（任意）指定されたアクセス リスト中の 1 番目のステートメントであり、アクセス リスト中の順番を決定します。 最大値は 2147483644 です。 デフォルトは 10 です。
increment	（任意）以降のステートメントでの、ベース シーケンス番号に対する増分。最大値は 2147483644 です。 デフォルトは 10 です。

コマンド デフォルト

base: 10

increment: 10

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

resequence access-list ipv4 コマンドを使用すると、**permit**、**deny**、または **remark** ステートメントを既存の IPv4 アクセス リスト中の連続したエントリ間に追加することができます。 最初のエントリ番号（*base*）とステートメントのエントリ番号を分けるための増分を指定します。 既存のステートメントの番号が再設定され、未使用のエントリ番号で新しいステートメントが追加できるようになります。

タスク ID

タスク ID	操作
acl	読み取り、書き込み

例

次の例では、既存のアクセス リストがあるとしています。

```
ipv4 access-list marketing
  1 permit 10.1.1.1
  2 permit 10.2.0.0 0.0.255.255
  3 permit tcp host 10.2.2.2 255.255.0.0 any eq telnet
```

アクセスリスト中に追加エントリを追加する場合は次のようにします。最初に、エントリに順番を付け直して（ステートメントを番号20から始めて5ずつ増加させる）、既存の各ステートメント間に4つの追加ステートメントを挿入できるスペースを取ります。

```
RP/0/RSP0/CPU0:router# resequence access-list ipv4 marketing 20 5
RP/0/RSP0/CPU0:router# show access-lists ipv4 marketing

ipv4 access-list marketing
  20 permit 10.1.1.1
  25 permit 10.2.0.0
  30 permit tcp host 10.2.2.2 255.255.0.0 any eq telnet
```

これで、新しいエントリを追加できます。

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list marketing
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 3 remark Do not allow user1 to telnet out
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 4 deny tcp host 172.16.2.88 255.255.0.0 any eq
telnet
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 29 remark Allow user2 to telnet out
RP/0/RSP0/CPU0:router# show access-lists ipv4 marketing

ipv4 access-list marketing
  3 remark Do not allow user1 to telnet out
  4 deny tcp host 171.69.2.88 255.255.0.0 any eq telnet
  20 permit 10.1.1.1
  25 permit 10.2.0.0
  29 remark Allow user2 to telnet out
  30 permit tcp host 10.2.2.2 255.255.0.0 any eq telnet
```

関連コマンド

コマンド	説明
deny（IPv4） , （13 ページ）	IPv4アクセス リストの拒否条件を設定します。
ipv4 access-list , （34 ページ）	IPv4 アクセス リストを定義し、また、IPv4 アクセス リスト コンフィギュレーション モードを開始します。
permit（IPv4） , （55 ページ）	IPv4アクセス リストの許可条件を設定します。

コマンド	説明
remark（IPv4） , （81 ページ）	IPv4 アクセス リストに関する有益な注釈を挿入します。
show access-lists ipv4 , （92 ページ）	現在の IPv4 アクセス リストすべての内容を表示します。

resequence access-list ipv6

既存のステートメントに番号を付け直して後続のステートメントの番号を増加させて、新しいIPv6アクセスリストステートメント（**permit**、**deny**、または**remark**）を追加できるようにするには、EXEC モードで **resequence access-list ipv6** コマンドを使用します。

resequence access-list ipv6 *name* [*base* [*increment*]]

構文の説明

name	IPv6 アクセス リストの名前。
base	（任意）指定されたアクセス リスト中の 1 番目のステートメントであり、アクセス リスト中の順番を決定します。 最大値は 2147483646 です。 デフォルトは 10 です。
increment	（任意）以降のステートメントでの、ベース シーケンス番号に対する増分。最大値は 2147483644 です。 デフォルトは 10 です。

コマンド デフォルト

base: 10

increment: 10

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

resequence access-list ipv6 コマンドは、IPv6 に固有のものを除き、**resequence access-list ipv4** コマンドと類似しています。

resequence access-list ipv6 コマンドを使用すると、**permit**、**deny**、または **remark** ステートメントを既存の IPv6 アクセス リスト中の連続したエントリ間に追加することができます。 最初のエントリ番号（*base*）とステートメントのエントリ番号を分けるための増分を指定します。 既存のス

テートメントの番号が再設定され、未使用のエントリ番号で新しいステートメントが追加できるようになります。

タスク ID

タスク ID	操作
acl	読み取り、書き込み

例

次の例では、既存のアクセス リストがあるとしています。

```
ipv6 access-list Internetfilter
  10 permit ipv6 3333:1:2:3::/64 any
  20 permit ipv6 4444:1:2:3::/64 any
  30 permit ipv6 5555:1:2:3::/64 any
```

アクセス リスト中に追加エントリを追加する場合は次のようにします。最初に、エントリに番号を付け直して（ステートメントの番号を 20 から始めて 5 ずつ増加させる）、既存の各ステートメント間に 4 つの追加ステートメントを挿入できるスペースを取ります。

```
RP/0/RSP0/CPU0:router# resequence access-list ipv6 Internetfilter 20 5
RP/0/RSP0/CPU0:router# show access-lists ipv6 Internetfilter

ipv6 access-list Internetfilter
  20 permit ipv6 3333:1:2:3::/64 any
  25 permit ipv6 4444:1:2:3::/64 any
  30 permit ipv6 5555:1:2:3::/64 any
```

これで、新しいエントリを追加できます。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list Internetfilter
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 3 remark Block BGP traffic from a given host
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 4 deny tcp host 6666:1:2:3::10 eq bgp host
7777:1:2:3::20 range 1300 1400
RP/0/RSP0/CPU0:router# show access-lists ipv6 Internetfilter

ipv6 access-list Internetfilter
  3 remark Block BGP traffic from a given host
  4 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range 1300 1404 deny tcp host
171.69.2.88 255.255.0.0 any eq telnet
  20 permit ipv6 3333:1:2:3::/64 any
  25 permit ipv6 4444:1:2:3::/64 any
  30 permit ipv6 5555:1:2:3::/64 any
```

関連コマンド

コマンド	説明
deny（IPv6） , （25 ページ）	IPv6 アクセス リストの拒否条件を設定します。
ipv6 access-list , （43 ページ）	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
permit（IPv6） , （75 ページ）	IPv6 アクセス リストの許可条件を設定します。

コマンド	説明
remark（IPv6） , （83 ページ）	IPv6 アクセス リスト エントリに関する有益な設定を挿入します。

show access-lists afi-all

現在の IPv4 および IPv6 アクセス リストの内容を表示するには、EXEC モードで **show access-lists afi-all** コマンドを使用します。

show access-lists afi-all

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
acl	読み取り

例

次に、**show access-lists afi-all** コマンドからの出力例を示します。

```
RP/0/RSP0/CPU0:router# show access-lists afi-all

ipv4 access-list crypto-1
 10 permit ipv4 65.21.21.0 0.0.0.255 65.6.6.0 0.0.0.255
 20 permit ipv4 192.168.241.0 0.0.0.255 192.168.65.0 0.0.0.255
```

show access-lists ipv4

現在の IPv4 アクセス リストの内容を表示するには、EXEC モードで **show access-lists ipv4** コマンドを使用します。

show access-lists ipv4 [*access-list-name* **hardware** {**ingress**| **egress**} [**interface** *type interface-path-id*] {**sequence** *number*| **location** *node-id*}| **summary** [*access-list-name*]| *access-list-name* [*sequence-number*]| **maximum [detail]** [**usage pfilter** {**location** *node-id*| **all**}]]

構文の説明

access-list-name	（任意）特定の IPv4 アクセス リストの名前。 この名前にスペースや引用符を含めることはできませんが、数値を含めることはできます。
hardware	（任意）アクセス リストを、インターフェイスのアクセス リストとして識別します。
ingress	（任意）着信インターフェイスを指定します。
egress	（任意）発信インターフェイスを指定します。
interface	（任意）インターフェイス統計情報を表示します。
type	（任意）インターフェイスのタイプ。詳細については、疑問符（?）オンライン ヘルプ機能を使用してください。
interface-path-id	物理インターフェイスまたは仮想インターフェイス。 （注） ルータに現在設定されているすべてのインターフェイスのリストを表示するには、**show interfaces** コマンドを使用します。 ルータの構文の詳細については、疑問符（?）を使用してオンライン ヘルプを参照してください。
sequence *number*	（任意）特定の IPv4 アクセス リストのシーケンス番号。 範囲は 1 ～ 2147483644 です。
location *node-id*	（任意）特定の IPv4 アクセス リストの場所。 *node-id* 引数は、*rack/slot/module* の形式で入力します。
summary	（任意）現在のすべての IPv4 アクセス リストのサマリーを表示します。
sequence-number	（任意）特定の IPv4 アクセス リストのシーケンス番号。 範囲は 1 ～ 2147483644 です。
maximum	（任意）IPv4 アクセス コントロール リスト（ACL）およびアクセス コントロール エントリ（ACE）の現在の設定可能最大数を表示します。

detail	（任意）完全な out-of-resource（OOR）の詳細を表示します。
usage	（任意）指定されたラインカード上のアクセス リストの使用方法を表示します。
pfilter	（任意）指定されたラインカードのパケット フィルタリングの使用方法を表示します。
all	（任意）すべてのラインカードの場所を表示します。

コマンド デフォルト

デフォルトでは、すべての IPv4 アクセス リストを表示します。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

show access-lists ipv4 コマンドを使用すると、すべての IPv4 アクセス リストの内容を表示することができます。 特定の IPv4 アクセス リストの内容を表示するには、*name* 引数を使用します。 *sequence-number* 引数を使用すると、アクセス リストのシーケンス番号を指定することができます。

hardware、**ingress** または **egress**、および **location** キーワードを使用すると、ハードウェア内容、および指定された方向（入力または出力）の指定されたアクセス リストを使用するすべてのインターフェイスのアクセス リストを表示することができます。 特定のアクセス リスト エントリの内容を表示するには、**sequence** *number* キーワードおよび引数を使用します。インターフェイスのアクセス グループは、イネーブルにするアクセス リスト ハードウェア カウンタ用の **ipv4 access-group** コマンドを使用して設定する必要があります。

show access-lists ipv4 summary コマンドを使用すると、現在のすべての IPv4 アクセス リストのサマリーを表示することができます。 特定の IPv4 アクセス リストのサマリーを表示するには、*name* 引数を使用します。

show access-lists ipv4 maximum detail コマンドを使用すると、IPv4 アクセス リストの OOR の詳細を表示することができます。 OOR は、システムに設定可能な ACL および ACE の数を制限します。 この制限に達すると、新しい ACL または ACE が拒否されます。

show access-list ipv4 usage コマンドを使用すると、指定されたラインカードにプログラミングされたすべてのインターフェイスおよびアクセス リストのサマリーを表示することができます。

タスク ID

タスク ID	操作
acl	読み取り

例

次の例では、すべての IPv4 アクセス リストの内容が表示されています。

```
RP/0/RSP0/CPU0:router# show access-lists ipv4

ipv4 access-list 101
  10 deny udp any any eq ntp
  20 permit tcp any any
  30 permit udp any any eq tftp
  40 permit icmp any any
  50 permit udp any any eq domain
ipv4 access-list Internetfilter
  10 permit tcp any 172.16.0.0 0.0.255.255 eq telnet
  20 deny tcp any any
  30 deny udp any 172.18.0.0 0.0.255.255 lt 1024
  40 deny ipv4 any any log
```

次の例では、acl_hw_1 という名前のアクセス リストの内容が表示されています。

```
RP/0/RSP0/CPU0:router# show access-lists ipv4 acl_hw_1 hardware egress location 0/2/cp0

ipv4 access-list acl_hw_1
  10 permit icmp 192.168.36.0 0.0.0.255 any (251 hw matches)
  20 permit ip 172.16.3.0 0.0.255.255 any (29 hw matches)
  30 deny tcp any any (58 hw matches)
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 *1*：*show access-lists ipv4* の *hardware* フィールドの説明

フィールド	説明
hw matches	ハードウェア一致の数
next-hop	ネクスト ホップがプログラミングされ、FIB から到達可能。
ACL name	ハードウェアにプログラミングされた ACL の名前。

フィールド	説明
Sequence Number	各 ACE シーケンス番号は、ACE に設定された値に対応するすべてのフィールドとともにハードウェア内にプログラミングされます。
Grant	ACE ルールによって、grant は拒否、許可、またはその両方に設定されます。
Logging	Logging は、ACE がログ オプションを使用してログをイネーブルにする場合にオンに設定されます。
Per ace icmp	Per ace icmp がハードウェア内でオンに設定されると、ICMP は到達不能で、レートが制限され、生成されます。デフォルトでは、オンに設定されます。
Hits	ACE のハードウェア カウンタ。
Statistics pointer	Statistics pointer は、ハードウェア カウンタに割り当てられたポインタです。
Number of TCAM entries	ACE をハードウェアにプログラミングするために使用される TCAM エントリの数。

次の例では、すべての IPv4 アクセス リストのサマリーが表示されています。

```
RP/0/RSP0/CPU0:router# show access-lists ipv4 summary

ACL Summary:
  Total ACLs configured: 3
  Total ACEs configured: 11
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 *2*：*show access-lists ipv4 summary* のフィールドの説明

フィールド	説明
Total ACLs configured	設定された IPv4 ACL の数
Total ACEs configured	設定された IPV4 ACE の数

次の例では、すべての IPv4 アクセス リストの OOR の詳細が表示されています。

```
RP/0/RSP0/CPU0:router# show access-lists ipv4 maximum detail
```

```
Default max configurable acls :5000
Default max configurable aces :200000
Current configured acls       :1
Current configured aces       :2
Current max configurable acls :5000
Current max configurable aces :200000
Max configurable acls         :9000
Max configurable aces         :350000
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 *3*：*show access-lists ipv4 maximum detail* コマンドのフィールドの説明

フィールド	説明
Default max configurable acls	IPv4 ACL のデフォルトの設定可能最大数
Default max configurable aces	IPv4 ACE のデフォルトの設定可能最大数
Current configured acls	設定された IPv4 ACL の数
Current configured aces	設定された IPv4 ACE の数
Current max configurable acls	IPv4 ACL の設定可能最大数
Current max configurable aces	IPv4 ACE の設定可能最大数
Max configurable acls	IPv4 ACL の設定可能最大数
Max configurable aces	IPv4 ACE の設定可能最大数

関連コマンド

コマンド	説明
clear access-list ipv4, （3 ページ）	IPv4 アクセス リスト一致カウンタをリセットします。
copy access-list ipv4 , （9 ページ）	既存の IPv4 アクセス リストをコピーします。
deny（IPv4） , （13 ページ）	IPv4アクセスリストの拒否条件を設定します。
ipv4 access-group, （31 ページ）	インターフェイス上の着信または発信の IPv4 トラフィックをフィルタリングします。
ipv4 access-list , （34 ページ）	IPv4 アクセス リストを定義し、また、IPv4 アクセス リスト コンフィギュレーション モードを開始します。
permit（IPv4） , （55 ページ）	IPv4アクセスリストの許可条件を設定します。

コマンド	説明
remark（IPv4） , （81 ページ）	IPv4 アクセス リスト エントリに関する有益な設定を挿入します。
resequence access-list ipv4 , （85 ページ）	既存の IPv4 アクセス リスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。

show access-lists ipv6

現在の IPv6 アクセス リストの内容を表示するには、EXEC モードで **show access-lists ipv6** コマンドを使用します。

show access-lists ipv6 [*access-list-name* **hardware** {**ingress**| **egress**} [**interface** *type interface-path-id*] {**sequence** *number*| **location** *node-id*}| **summary** [*access-list-name*]| *access-list-name* [*sequence-number*]| **maximum [detail]** [**usage pfilter** {**location** *node-id*| **all**}]]

構文の説明

access-list-name	（任意）特定の IPv6 アクセス リストの名前。 この名前にスペースや引用符を含めることはできませんが、数値を含めることはできます。
hardware	（任意）アクセス リストを、インターフェイスのアクセス リストとして識別します。
ingress	（任意）着信インターフェイスを指定します。
egress	発信インターフェイスを指定します。
interface	（任意）インターフェイス統計情報を表示します。
type	（任意）インターフェイスのタイプ。 詳細については、疑問符（?）オンライン ヘルプ機能を使用してください。

interface-path-id	（任意）次のような物理インターフェイスのインスタンスまたは仮想インターフェイスのインスタンスです。 • 物理インターフェイス インスタンス。 名前表記は *rack/slot/module/port* です。値の間に表記の一部としてスラッシュが必要です。 ◦ *rack*：ラックのシャーシ番号。 ◦ *slot*：モジュラ サービス カードまたはラインカードの物理スロット番号。 ◦ *module*：モジュール番号。 物理層インターフェイス モジュール（PLIM）は、常に 0 です。 ◦ *port*：インターフェイスの物理ポート番号。 （注） ルートプロセッサ カード上の管理イーサネットインターフェイスに関しては、物理スロット番号は英数字（RSP0）であり、モジュールは CPU0 です。 例：インターフェイス MgmtEth0/RSP0/CPU0/0 • 仮想インターフェイス インスタンス。 数字の範囲は、インターフェイス タイプによって異なります。 ルータの構文の詳細については、疑問符（?）を使用してオンライン ヘルプを参照してください。
sequence *number*	（任意）特定の IPv6 アクセス リストのシーケンス番号。 範囲は 1 ～ 2147483644 です。
location *node-id*	（任意）特定の IPv6 アクセス リストの場所。 *node-id* 引数は、*rack/slot/module* の形式で入力します。
summary	（任意）現在のすべての IPv6 アクセス リストのサマリーを表示します。
sequence-number	（任意）特定の IPv6 アクセス リストのシーケンス番号。 範囲は 1 ～ 2147483644 です。
maximum	（任意）IPv6 アクセス コントロール リスト（ACL）およびアクセス コントロール エントリ（ACE）の現在の設定可能最大数を表示します。
detail	（任意）完全な out-of-resource（OOR）の詳細を表示します。
usage	（任意）指定されたラインカード上のアクセス リストの使用方法を表示します。
pfilter	（任意）指定されたラインカードのパケット フィルタリングの使用方法を表示します。
all	（任意）すべてのラインカードの場所を表示します。

コマンド デフォルト すべての IPv6 アクセス リストを表示します。

コマンド モード EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

使用上のガイドライン このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

show access-list ipv6 コマンドは、IPv6 に固有のものを除き、**show access-list ipv4** コマンドと類似しています。

show access-lists ipv6 コマンドを使用すると、すべての IPv6 アクセス リストの内容を表示することができます。 特定の IPv6 アクセス リストの内容を表示するには、*name* 引数を使用します。 *sequence-number* 引数を使用すると、アクセス リストのシーケンス番号を指定することができます。

hardware、**ingress** または **egress**、および **location** キーワードを使用すると、ハードウェア内容、および指定された方向（入力または出力）の指定されたアクセス リストを使用するすべてのインターフェイスのアクセス リストを表示することができます。 特定のアクセス リスト エントリの内容を表示するには、**sequence** *number* キーワードおよび引数を使用します。インターフェイスのアクセス グループは、イネーブルにするアクセス リスト ハードウェア カウンタ用の **ipv6 access-group** コマンドを使用して設定する必要があります。

show access-lists ipv6 summary コマンドを使用すると、現在のすべての IPv6 アクセス リストのサマリーを表示することができます。 特定の IPv6 アクセス リストのサマリーを表示するには、*name* 引数を使用します。

show access-lists ipv6 maximum detail コマンドを使用すると、IPv6 アクセス リストの OOR の詳細を表示することができます。 OOR は、システムに設定可能な ACL および ACE の数を制限します。 この制限に達すると、新しい ACL または ACE が拒否されます。

show access-list ipv6 ipv4 usage コマンドを使用すると、指定されたラインカードにプログラミングされたすべてのインターフェイスおよびアクセス リストのサマリーを表示することができます。

タスク ID

タスク ID	操作
acl	読み取り

例

次の例では、すべての IPv6 アクセス リストの内容が表示されています。

```
RP/0/RSP0/CPU0:router# show access-lists ipv6

ipv6 access-list Internetfilter
  3 remark Block BGP traffic from a given host
  4 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range 1300 1404 deny tcp host
171.69.2.88 255.255.0.0 any eq telnet
  20 permit ipv6 3333:1:2:3::/64 any
  25 permit ipv6 4444:1:2:3::/64 any
  30 permit ipv6 5555:1:2:3::/64 any
ipv6 access-list marketing
  10 permit ipv6 7777:1:2:3::/64 any (51 matches)
  20 permit ipv6 8888:1:2:3::/64 any (26 matches)
  30 permit ipv6 9999:1:2:3::/64 any (5 matches)
```

次の例では、Internetfilter という名前のアクセス リストの内容が表示されています。

```
RP/0/RSP0/CPU0:router# show access-lists ipv6 Internetfilter

ipv6 access-list Internetfilter
  3 remark Block BGP traffic from a given host
  4 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range 1300 1404 deny tcp host
171.69.2.88 255.255.0.0 any eq telnet
  20 permit ipv6 3333:1:2:3::/64 any
  25 permit ipv6 4444:1:2:3::/64 any
  30 permit ipv6 5555:1:2:3::/64 any
```

次の例では、acl_hw_1 という名前のアクセス リストの内容が表示されています。

```
RP/0/RSP0/CPU0:router# show access-lists ipv6 acl_hw_1 hardware egress location 0/2/cp0

ipv6 access-list acl_hw_1
  10 permit icmp any any (251 hw matches)
  20 permit ipv6 3333:1:2:3::/64 any (29 hw matches)
  30 deny tcp any any (58 hw matches)
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 *4*：*show access-lists ipv6 hardware* コマンドのフィールドの説明

フィールド	説明
hw matches	ハードウェア一致の数

次の例では、すべての IPv6 アクセス リストのサマリーが表示されています。

```
RP/0/RSP0/CPU0:router# show access-lists ipv6 summary

ACL Summary:
```

```
  Total ACLs configured: 3
  Total ACEs configured: 11
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 5 : *show access-lists ipv6 summary* コマンドのフィールドの説明

フィールド	説明
Total ACLs configured	設定された IPv6 ACL の数
Total ACEs configured	設定された IPV6 ACE の数

次の例では、すべての IPv6 アクセス リストの OOR の詳細が表示されています。

```
RP/0/RSP0/CPU0:router# show access-lists ipv6 maximum detail

Default max configurable acls :1000
Default max configurable aces :50000
Current configured acls       :1
Current configured aces       :2
Current max configurable acls :1000
Current max configurable aces :50000
Max configurable acls         :2000
Max configurable aces         :100000
```

関連コマンド

コマンド	説明
copy access-list ipv6, （11 ページ）	既存の IPv6 アクセス リストをコピーします。
deny（IPv6）, （25 ページ）	IPv6 アクセス リストの拒否条件を設定します。
ipv6 access-list , （43 ページ）	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
permit（IPv6）, （75 ページ）	IPv6 アクセス リストの許可条件を設定します。
remark（IPv6）, （83 ページ）	IPv6 アクセス リスト エントリに関する有益な設定を挿入します。
resequence access-list ipv6 , （88 ページ）	既存の IPv4 アクセス リスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。