アクセス リスト コマンド

このモジュールでは、IP バージョン 4（IPv4）や IP バージョン 6（IPv6）のアクセス リストを設定する際に使用する Cisco IOS XR ソフトウェアのコマンドについて説明します。

ACL の概念、設定作業、および例の詳細については、『*IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*』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、XR 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 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ます。
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

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

clear access-list ipv4 コマンドを使用すると、特定の設定済みアクセス 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** コマンドにより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 引数でアスタリスク（*****）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。

egress での ACL はリリース 6.0 ではサポートされていません

タスク ID

タスク ID	動作
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/RP0/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/RP0/CPU0:router# clear access-list ipv4 marketing

RP/0/RP0/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
```

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、XR 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

なし

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

設定済みのアクセス リストをコピーするには、**copy access-list ipv4** コマンドを使用します。*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* 引数を使用して、ソース アクセス リストの内容のコピー先を指定できます。*destination-acl* 引数は一意の名前でなければなりません。アクセス リストまたはプレフィックス リストを示す *destination-acl* 引数名が存在する場合、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 リストが存在することをチェックしてから既存のリスト名をチェックし、既存のアクセス 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	動作
acl	読み取り、書き込み
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/RP0/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/RP0/CPU0:router# copy access-list ipv4 list-1 list-2
RP/0/RP0/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/RP0/CPU0:router# copy access-list ipv4 list-1 list-3

list-3 exists in access-list

RP/0/RP0/CPU0:router# show access-lists ipv4 list-3

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

deny（IPv4）

IPv4 アクセス リストの拒否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*] **counter** *counter-name*[**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*]] [**counter** *counter-name*]

no *sequence-number*

インターネット制御メッセージ プロトコル（ICMP）

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

インターネット グループ管理プロトコル（IGMP）

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

ユーザ データグラム プロトコル（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**] [**counter** *counter-name*]

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）。設定されているアクセスリストの最初のステートメントの番号を変更して、以降のステートメントを増分するには、**resequence access-list** コマンドを使用します。

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、*source* および *source-wildcard*（0.0.0.0 255.255.255.255）の短縮形として使用します。 • **host***source* の組み合わせを、*source* および *source* の *source-wildcard*（0.0.0.0）の短縮形として使用します。
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、*source* および *source-wildcard*（0.0.0.0 255.255.255.255）の短縮形として使用します。 • **host***source* の組み合わせを、*source* および *source* の *source-wildcard*（0.0.0.0）短縮形として使用します。
protocol	IP プロトコルの名前または番号。これには、**esp**、**eigrp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、**pim**、**pcp**、**tcp**、**udp** のいずれかのキーワードを指定するか、IP プロトコル番号を示す 0 ～ 255 の整数を指定できます。任意のインターネット プロトコル（ICMP、TCP、UDP など）と一致させるには、**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、*destination* および *destination-wildcard*（0.0.0.0 255.255.255.255）の短縮形として使用します。 • **host***destination* の組み合わせを、*destination* および *destination* の *destination-wildcard*（0.0.0.0）の短縮形として使用します。

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、*destination* および *destination-wildcard*（0.0.0.0 255.255.255.255）の短縮形として使用します。 • **host***destination* の組み合わせを、*destination* および *destination* の *destination-wildcard*（0.0.0.0）の短縮形として使用します。
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**：routine precedence（0）に一致するパケット • **priority**：priority precedence（1）に一致するパケット • **immediate**：immediate precedence（2）に一致するパケット • **flash**：flash precedence（3）に一致するパケット • **flash-override**：flash override precedence（4）に一致するパケット • **critical**：critical precedence（5）に一致するパケット • **internet**：internetwork control precedence（6）に一致するパケット • **network**：network control precedence（7）に一致するパケット

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。（コンソールに記録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果たします。
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* が指定されている場合にのみ、この値と照合されます。 *value1* と *value2* の両方が指定されている場合は、*value1* と *value2* の間の TTL 範囲とパケット TTL が照合されます。
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 • trace • 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。使用可能なオペランドは、**lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、**neq**（等しくない）、および **range**（包含範囲）です。 演算子を *source* と *source-wildcard* の値の後に置いた場合は、送信元ポートと照合されます。 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いた場合はと、TTL 値と照合されます。 **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：*flag-name* の前に **+** または **-** を付けます。TCP フラグを設定してパケットと照合するには、**+** *flag-name* 引数を使用します。TCP フラグを設定せずにパケットを照合するには、**-** *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。フラグ名は次のとおりです。**ack**、**fin**、**psh**、**rst**、**syn**。
counter	（任意）SNMP クエリーを使用して ACL カウンタへのアクセスをイネーブルにします。
counter-name	ACL カウンタ名を定義します。

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 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 6.0	このコマンドが導入されました。

使用上のガイドライン

アクセス リストでパケットを拒否する条件を指定するには、**ipv4 access-list** コマンドの後ろに **deny** コマンドを使用します。

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。

リスト全体を再入力せずに、既存のアクセス リストに **permit**、**deny**、または **remark** ステートメントを追加できます。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。

番号が連続している 2 つ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、まず **resequence access-list** コマンドを使用して最初のステートメントの番号を付け直し、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
- network
- 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。これらのプロトコルに対応するポート番号を検索するには、ポート番号の代わりに「?」を入力します。

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname
- 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。これらのプロトコルに対応するポート番号を検索するには、ポート番号の代わりに「?」を入力します。

- 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できます。

- ack
- fin
- psh
- rst
- syn

たとえば、**match-all** *+ack +syn* は、ack と syn の両方のフラグが設定されている TCP パケットを表示します。また、**match-any** *+ack -syn* は、ack が設定されている TCP パケットまたは syn が設定されていないが TCP パケットを表示します。

（注） ACL のいずれかの ACE に ABF 句が含まれている場合、その ACL はゼロ以外の圧縮レベルに適用できません。

タスク ID

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

例

次の例は、Internet filter という名前のアクセス リストに拒否条件を設定する方法を示しています。

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 deny 192.168.34.0 0.0.0.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 deny 172.16.0.0 0.0.255.255
RP/0/RP0/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/RP0/CPU0:router(config-ipv4-acl)# permit 10.0.0.0 0.255.255.255
```

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**}

no ipv4 access-group *access-list-name* {**ingress| egress**}

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	インバウンド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。

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	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

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。特定の IPv4 アクセス リストを指定するには、*access-list-name* 引数を使用します。着信パケットをフィルタリングするには **ingress** キーワードを使用し、発信パケットをフィルタリングするには **egress** キーワードを使用します。*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。

インターフェイス ACL による MPLS パケットのフィルタリングはサポートされていません。

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。

タスク ID

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

例

次の例は、tenGigE インターフェイス 0/0/0/2 の着信および発信パケットにフィルタリングを適用する方法を示しています。

```
RP/0/RP0/CPU0:router(config)# interface tenGigE 0/0/0/2
RP/0/RP0/CPU0:router(config-if)# ipv4 access-group p-ingress-filter ingress
```

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/RP0/CPU0:router(config)# interface tenGigE 0/0/0/2
RP/0/RP0/CPU0:router(config-if)# ipv4 access-group p-ingress-filter ingress
interface-statistics
```

ipv4 access-list

IPv4アクセス リストを名前で定義するには、XR 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

XR コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ipv4 access-list コマンドは、IPv4 アクセス リストを設定するために使用します。このコマンドを指定すると、ルータはアクセス リスト コンフィギュレーション モードになります。このモードでは、アクセスを拒否または許可する条件を **deny** または **permit** コマンドを使用して定義する必要があります。

既存の IPv4 アクセス リストの連続しているエントリの間に **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。先頭のエントリ番号（*base*）を指定し、ステートメントのエントリ番号を隔て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。

アクセス リストをインターフェイスに適用するには、**ipv4 access-group** コマンドを使用します。

タスク ID

タスク ID	動作
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/RP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 permit 192.168.34.0 0.0.0.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 permit 172.16.0.0 0.0.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 30 permit 10.0.0.0 0.255.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 39 remark Block BGP traffic from 172.16 net.
RP/0/RP0/CPU0:router(config-ipv4-acl)# 40 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203
 range 1300 1400
```

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、XR 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

デフォルト値は 1 です。

コマンド モード

XR コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

rate-number 引数は、インターフェイスに設定されているすべての 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	動作
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/RP0/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アップデートの数を指定するには、XR 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

XR コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

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	動作
basic-services	読み取り、書き込み
acl	読み取り、書き込み

例

次の例は、ルータに設定されている IPv4 アクセス リストごとに 10 のアップデートをロギングしきい値として設定する方法を示しています。

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list log-update threshold 10
```

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**（送信元）と **permit**（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*] **permit** *source* [*source-wildcard*] [**log**| **log-input**]

[*sequence-number*] **permit** *protocol net-group source-net-object-group-name destination source-port-object-group-name* **net-group** *destination-net-object-group-name***port-group** *destination-port-object-group-name*[**capture**][**precedence** *precedence*] [**default nexthop1** [**vrf** *vrf-name*] [**ipv4** *ipv4-address1* **nexthop2** [**vrf** *vrf-name*] [**ipv4** *ipv4-address2* **nexthop3** [**vrf** *vrf-name*] [**ipv4** *ipv4-address3*]] [**dscp** *dscp*] **[fragments]** [**log**| **log-input**] [**nexthop** [**track** *track-name*]] [**ttl** *ttl value* [*value1 ... value2*]][**counter** *counter-name*]

[*sequence-number*] **permit** *protocol* **net-group** *source-net-object-group-name* **port-group***source-port-object-group-name* **net-group** *destination-net-object-group-name***port-group***destination-port-object-group-name* **[capture]** [**precedence** *precedence*] [**default nexthop1** [**vrf** *vrf-name*][**ipv4** *ipv4-address1*] **nexthop2**[**vrf** *vrf-name*][**ipv4** *ipv4-address2*] **nexthhop3**[**vrf** *vrf-name*][**ipv4** *ipv4-address3*]] [**dscp range** *dscp dscp*] **[fragments]** [**log**| **log-input**] [**nexthop** [**track** *track-name*]] [**ttl** *ttl value* [*value1 ... value2*]][**counter** *counter-name*]

no *sequence-number*

インターネット制御メッセージ プロトコル（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]**[**counter** *counter-name*]

インターネット グループ管理プロトコル（IGMP）

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

ユーザ データグラム プロトコル（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**][**counter** *counter-name*]

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）。設定されているアクセスリストの最初のステートメントの番号を変更して、以降のステートメントを増分するには、**resequence access-list** コマンドを使用します。
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、*source* および *source-wildcard*（0.0.0.0 255.255.255.255）の短縮形として使用します。 • **host***source* の組み合わせを、*source* および *source* の *source-wildcard*（0.0.0.0）の短縮形として使用します。

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、*source* および *source-wildcard*（0.0.0.0 255.255.255.255）の短縮形として使用します。 • **host***source* の組み合わせを、*source* および *source* の *source-wildcard*（0.0.0.0）の短縮形として使用します。
protocol	IP プロトコルの名前または番号。これには、**esp**、**eigrp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、**pim**、**pcp**、**tcp**、**udp** のいずれかのキーワードを指定するか、IPプロトコル番号を示す0～255の整数を指定できます。任意のインターネット プロトコル（ICMP、TCP、UDPなど）と一致させるには、**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、*destination* および *destination-wildcard*（0.0.0.0 255.255.255.255）の短縮形として使用します。 • **host***destination* の組み合わせを、*destination* および *destination* の *destination-wildcard*（0.0.0.0）の短縮形として使用します。
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、*destination* および *destination-wildcard*（0.0.0.0 255.255.255.255）の短縮形として使用します。 • **host***destination* の組み合わせを、*destination* および *destination* の *destination-wildcard*（0.0.0.0）の短縮形として使用します。

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**：routine precedence（0）に一致するパケット • **priority**：priority precedence（1）に一致するパケット • **immediate**：immediate precedence（2）に一致するパケット • **flash**：flash precedence（3）に一致するパケット • **flash-override**：flash override precedence（4）に一致するパケット • **critical**：critical precedence（5）に一致するパケット • **internet**：internetwork control precedence（6）に一致するパケット • **network**：network control precedence（7）に一致するパケット
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って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が指定されていない場合のみとなります。

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に acl コマンドを設定する際に、ACL コンフィギュレーション コマンドで **capture** キーワードを指定しないと、トラフィックはミラーリングされません。ACL の設定で **capture** キーワードが使用され、送信元ポートに acl コマンドが設定されていない場合は、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-address1ipv4-address2ipv4-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。

dscp range*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。（コンソールに記録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果たします。
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* が指定されている場合にのみ、この値と照合されます。 *value1* と *value2* の両方が指定されている場合は、*value1* と *value2* の間の TTL 範囲とパケット TTL が照合されます。
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 • trace • 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。使用可能なオペランドは、**lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、**neq**（等しくない）、および **range**（包含範囲）です。 演算子を *source* と *source-wildcard* の値の後に置いた場合は、送信元ポートと照合されます。 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いた場合はと、TTL 値と照合されます。 **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：*flag-name*の前に**+**または**-**を付けます。TCPフラグを設定してパケットと照合するには、+ *flag-name*引数を使用します。TCPフラグを設定せずにパケットを照合するには、- *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。フラグ名は次のとおりです。**ack**、**fin**、**psh**、**rst**、**syn**。
counter	（任意）SNMPクエリーを使用してACLカウンタへのアクセスをイネーブルにします。**counter***counter-name*キーワードは、Cisco ASR 9000拡張イーサネットラインカードでのみ使用できます。
counter-name	ACLカウンタ名を定義します。

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 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 6.0	このコマンドが導入されました。

使用上のガイドライン

アクセス リストでパケットを許可する条件を指定するには、**ipv4 access-list** コマンドの後ろに **permit** コマンドを使用します。

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。

リスト全体を再入力せずに、既存のアクセス リストに **permit**、**deny**、または **remark** ステートメントを追加できます。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。

番号が連続している 2 つ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、まず **resequence access-list** コマンドを使用して最初のステートメントの番号を付け直し、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。

（注） ACL のいずれかの ACE に ABF 句が含まれている場合、その ACL はゼロ以外の圧縮レベルに適用できません。

次に、precedence の名前のリストを示します。

- critical
- flash
- flash-override
- immediate
- internet
- network
- 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。これらのプロトコルに対応するポート番号を検索するには、ポート番号の代わりに「?」を入力します。

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname
- 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。これらのプロトコルに対応するポート番号を検索するには、ポート番号の代わりに「?」を入力します。

- 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できます。

- ack
- fin
- psh
- rst
- syn

たとえば、**match-all** *+ack +syn* は、ack と syn の両方のフラグが設定されている TCP パケットを表示します。また、**match-any** *+ack -syn* は、ack が設定されている TCP パケットまたは syn が設定されていない TCP パケットを表示します。

タスク ID

タスク ID	動作
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/RP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 permit 192.168.34.0 0.0.0.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 permit 172.16.0.0 0.0.255.255
RP/0/RP0/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/RP0/CPU0:router(config-ipv4-acl)# deny 10.0.0.0 0.255.255.255
```

remark（IPv4）

IPv4 アクセス リストのエントリに有益なコメント（注釈）を記入するには、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 リスト内の **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 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 6.0	このコマンドが導入されました。

使用上のガイドライン

remark コマンドを使用すると、IPv4 アクセス リスト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。

削除するコメント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したいときに、連続エントリにシーケンス番号が付いているためステートメントを追加できない場合は、**resequence access-list ipv4** コマンドを使用します。

タスク ID

タスク ID	動作
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/RP0/CPU0:router(config)# ipv4 access-list telnetting
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 remark Do not allow user1 to telnet out
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 deny tcp host 172.16.2.88 255.255.0.0 any eq
telnet
RP/0/RP0/CPU0:router(config-ipv4-acl)# 30 permit icmp any any
RP/0/RP0/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
```

resequence access-list ipv4

既存のステートメントの番号を再設定して以降のステートメントを増分し、新しいIPv4アクセス リスト ステートメント（**permit**、**deny**、**remark**）を追加できるようにするには、XR EXEC モードで **resequence access-listipv4** 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。デフォルト値は 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。デフォルト値は 10 です。

コマンド デフォルト

base: 10

increment: 10

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

既存の IPv4 アクセス リストの連続しているエントリの間に **permit**、**deny**、または **remark** ステートメントを追加するには、**resequence access-list ipv4** コマンドを使用します。先頭のエントリ番号（*base*）を指定し、ステートメントのエントリ番号を隔て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	動作
acl	読み取り、書き込み

例

次の例では、既存のアクセス リストがあると想定しています。

```
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 リストにエントリを追加する場合は次のようにします。最初に、エントリの番号を付け直して（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追加ステートメントを挿入できるスペースを設けます。

```
RP/0/RP0/CPU0:router# resequence access-list ipv4 marketing 20 5
RP/0/RP0/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/RP0/CPU0:router(config)# ipv4 access-list marketing
RP/0/RP0/CPU0:router(config-ipv4-acl)# 3 remark Do not allow user1 to telnet out
RP/0/RP0/CPU0:router(config-ipv4-acl)# 4 deny tcp host 172.16.2.88 255.255.0.0 any eq telnet
RP/0/RP0/CPU0:router(config-ipv4-acl)# 29 remark Allow user2 to telnet out
RP/0/RP0/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
```

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、XR 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または引数はありません。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
acl	読み取り

例

次の例は、**show access-lists afi-all** コマンドの出力を示しています。

```
RP/0/RP0/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、XR EXEC モードで **show access-listsipv4** コマンドを使用します。

show access-lists ipv4 [*access-list-name* **hardware** {**ingress**| **egress**} [**interface** *type*] {**sequence** *number*| **location** *node-id*}| **summary** [*access-list-name*]| *access-list-name* [*sequence-number*]| **maximum [detail]** [**usage pfilter** {**resource-usage 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 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。
resource-usage	圧縮レベルの TCAM リソース使用量を表示します。
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

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

show access-listsipv4 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できます。

特定の方向（入力または出力）で特定のアクセス リスを使用するすべてのインターフェイスについて、アクセス リストのハードウェア コンテンツとカウンタを表示するには、**hardware**、**ingress** または **egress**、および **location** キーワードを使用します。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* キーワードと引数を使用します。インターフェイスのアクセス グループを設定するには、**ipv4 access-group** コマンドを使用してアクセス リストのハードウェア カウンタをイネーブルにする必要があります。

show access-lists ipv4 summary コマンドを使用すると、現在の全 IPv4 アクセス リストのサマリーを表示できます。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、特定のラインカードにプログラミングされているすべてのインターフェイスとアクセス リストのサマリーを表示できます。

egress での ACL はリリース 6.0 ではサポートされていません

タスク ID

タスク ID	動作
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/RP0/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
```

次の表で、この出力に表示される重要なフィールドを説明します。

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
ACL name	ハードウェアにプログラミングされた ACL の名前。
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。

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/RP0/CPU0:router# show access-lists ipv4 summary

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

次の表で、この出力に表示される重要なフィールドを説明します。

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/RP0/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
```

次の表で、この出力に表示される重要なフィールドを説明します。

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

次の例は、特定のラインカードに対するパケット フィルタリングの使用を表示します。

```
RP/0/RP0/CPU0:router# show access-lists ipv4 usage pfilter location 0/RP0/CPU0

Interface : tenGigE 0/0/0/1
Input Common-ACL : ipv4_c_acl  ACL : ipv4_i_acl_1
Output ACL : ipv4_i_acl_1
```

（注） バンドル インターフェイスに対するパケット フィルタリングの使用を表示するには、**show access-lists ipv4 usage pfilter location all** コマンドを使用します。

次の例は、 TCAM リソースの使用量を表示します。

```
RP/0/RP0/CPU0:router# sh access-lists ipv4 acl-v4 hardware ingress resource-usage location
 0/RP0/CPU0

Rules (ACE)              : 2
 TCAM Entries  used      : 2  ( 2048k total)
```

```
TCAM Key Width          : 160
```

show pfilter-ea

パケット フィルタ ea 情報を表示するには、ASR 9000 拡張イーサネット ラインカードで XR EXEC モード に入って show pfilter ea コ マンドを入力します。

show pfilter-ea fea {**ipv4 acl | ipv6 acl**} *acl-name***location***node-id*

構文の説明

ipv4 acl	IPv4 アクセス リストを示します。
ipv6 acl	IPv6 アクセス リストを示します。
acl-name	IPv4/IPv6 アクセス リストの名前。
location*node-id*	特定の IPv4/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。

コマンド デフォルト

なし

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ASR 9000 拡張イーサネット ラインカードでのみ使用できます。

タスク ID

タスク ID	動作
root-system	読み取り、書き込み

例

次の例は、パケット フィルタ ea 情報の表示方法を示しています。

```
RP/0/RP0/CPU0:router#  show feature-mgr client pfilter-ea feature-info summary location
0/RP0/CPU0

IFH         NPU DIR Lookup-type  VMR-ID      ACL-ID Refcnt Feature-Name
----------- --- --- -----------  ----------- ------ ------ ------------
0x8000048   0   IN  IPV4_ACL (L3) 0x2          3      1      skywarp_acl
0x8000038   0   IN  IPV4_ACL (L3) 0x1          2      1      v4-acl
0x8000040   0   IN  IPV4_ACL (L2) 0x200000001  2      1      v4-acl
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *4*：*show pfilter-ea* のフィールドの説明

フィールド	説明
IFH	ACL が適用されるインターフェイスのインターフェイス ハンドル
DIR	ACL が適用される方向を示します。IN は入力、OUT は出力。
Lookup-type	ACL のタイプ（IPv4 または IPv6）。L3/L2 はインターフェイスのタイプを示します。
Reference count	特定の ACL が適用されるインターフェイスの番号を示します。
Feature name	ハードウェアにプログラミングされた ACL の名前。