pac key ～ port-misuse

permit

名前付き IP アクセス リストでパケットを許可する条件を設定するには、該当する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。IP 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。

permit *protocol* [*source-addr source-wildcard*] {**any**| **host** {*address*| *name*}} {*destination-addr destination-wildcard*| **any**| **host** {*address*| *name*}} **[dscp** *dscp-value*| **precedence** *precedence-value*| **fragments** *fragment-value*| **option** *option-value*| **reflect** *access-list-name*| **time-range** *time-range-value*| **ttl** *match-value ttl-value* **[ttl-value]**| **tos** *tos-value*| **timeout** *max-time*| **log** [*log-value*]| **log-input** [*log-input-value*]]

no permit *protocol* [*source-addr source-wildcard*] {**any**| **host** {*address*| *name*}} {*destination-addr destination-wildcard*| **any**| **host** {*address*| *name*}}

permit {**tcp**| **udp**} {*source-addr source-wildcard*| **any**| **host** *source-addr*} {*destination-addr destination-wildcard*| **any**| **host** *dest-addr*| *port-match-criteria* {*destination-addr destination-wildcard*| **any**| **host** *dest-addr*}} [*port-match-criteria port-number*| **fragments**| **ack**| **established**| **fin**| **psh**| **rst**| **syn**| **urg**| **match-all** *match-value*| **match-any** *match-value*| **dscp** *dscp-value*| **precedence** *precedence-value*| **option** *option-value*| **time-range** *time-range-value*| **ttl** *match-value ttl-value* [*ttl-value*]| **tos** *tos-value*| **log** [*log-value*]| **log-input** [*log-input-value*]]

no permit {**tcp**| **udp**} {*source-addr source-wildcard*| **any**| **host** *source-addr*} {*destination-addr destination-wild-card*| **any**| **host** *dest-addr*| *port-match-criteria* {*destination-addr destination-wild-card*| **any**| **host** *dest-addr*}}

構文の説明

protocol	プロトコルの名前または番号。有効な値は、**ahp**、**eigrp**、**esp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、、**tcp**、**pcp**、**pim**、**udp**、または IP プロトコル番号を表す 0 ～ 255 の範囲の整数です。任意のインターネットプロトコル（Internet Control Message Protocol（ICMP）、TCP、User Datagram Protocol（UDP）など）に一致するには、キーワード **ip** を使用します。その他の修飾子については、「使用上のガイドライン」を参照してください。
source-addr	（オプション）10 進表記の 4 つの部分をドットで区切った 32 ビット数として送信されるパケットの送信元ネットワークまたはホストの番号。
source-wildcard	（オプション）送信元に適用されるワイルドカード ビット。これは、10 進数の 4 つの部分をドットで区切ったものです。無視するビット位置に 1 を入れます。

any	送信元ホストまたは宛先ホストを、*source-addr* または *destination-addr value*、および *source-wildcard* または *destination-wildcard* の値（0.0.0.0 255.255.255.255）の短縮形として指定します。
host *address name*	1 つのホストの送信元アドレスまたは宛先アドレスおよび名前を指定します。
destination-addr	10 進表記の 4 つの部分をドットで区切った 32 ビット数として送信されるパケットの宛先ネットワークまたはホストの番号。
destination-wildcard	宛先に適用されるワイルドカードビット。これは、10 進数の 4 つの部分をドットで区切った 32 ビット数です。無視するビット位置に 1 を入れます。
dscp *dscp-value*	（オプション）特定の DiffServ コードポイント（DSCP）値が設定されているパケットと一致します。有効な値については、「使用上のガイドライン」を参照してください。
precedence *precedence-value*	（オプション）パケットの優先フィルタ レベルを指定します。有効な値は 0 ～ 7 の番号または名前です。有効な名前のリストについては、「使用上のガイドライン」を参照してください。
fragments *fragment-value*	（オプション）アクセス リスト エントリがパケットの先頭以外のフラグメントに適用され、フラグメントは許可または拒否されます。**fragments** キーワードの詳細については、「使用上のガイドライン」の「フラグメント」の「フラグメントのアクセス リストまたは OGACL 処理」と「フラグメントおよびポリシー ルーティング」を参照してください。
option *option-value*	（オプション）特定の IP オプション値番号を含むパケットに一致します。有効な値については、「使用上のガイドライン」を参照してください。
reflect *access-list-name*	（オプション）再帰的なアクセス リスト エントリを作成します。

time-range *time-range-value*	（オプション）時間範囲エントリ名を指定します。
ttl *match-value ttl-value*	（オプション）特定のTTL値を含むパケットに一致します。有効な値については、「使用上のガイドライン」を参照してください。
tos *tos-value*	（オプション）パケットのサービスフィルタリング レベルを指定します。有効な値は 0 ～ 15 の番号、または **access-list**（IP 拡張）コマンドの「使用上のガイドライン」にリストされている名前です。
timeout *max-time*	再帰 ACL の最大存続期間を指定します。有効な値は 1 ～ 2147483 秒です。

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。（コンソールに記録されるメッセージのレベルは **loggingconsole** コマンドで制御します）。 標準リストのメッセージには、アクセス リスト番号、パケットの許可/拒否、送信元アドレス、およびパケット数が含まれます。 拡張リストのメッセージには、アクセス リスト番号、パケットの許可/拒否、プロトコル（TCP、UDP、ICMP、または番号）が含まれます。また該当する場合には、送信元アドレスと宛先アドレス、ポート番号、およびユーザ定義 Cookie またはルータ生成ハッシュ値が含まれます。 標準リストと拡張リストの両方で、一致した最初のパケットに関するメッセージが生成され、その後 5 分間隔で、前の 5 分間で許可または拒否されたパケット数を含むメッセージが生成されます。 ロギング メッセージが多すぎて処理できない場合、または 1 秒以内に処理する必要があるロギング メッセージが複数ある場合、ロギング設備ではロギング メッセージ パケットの一部をドロップすることがあります。この動作により、ロギング パケットが多すぎるためにルータがリロードすることが防止されます。そのため、課金ツールや、アクセス リストと一致する数の正確な情報源としてロギング設備を使用しないでください。 **log** キーワード（および関連する *word* 引数）を指定した場合、このコマンドではその他のキーワードや設定は指定できません。

log-value	（オプション）ログ メッセージに付加されるユーザ定義 Cookie。Cookie の条件は次のとおりです。 • 文字以内である必要があります。 • 16 進表記（0x など）で始めることはできません。 • **reflect**、**fragment** といったキーワードと同じであることはできません。また、これらのキーワードの一部を使用することはできません。 **time-range** • 英数字のみを使用する必要があります。 ユーザ定義 Cookie はアクセス コントロール エントリ（ACE）syslog エントリに付加され、アクセス コントロール リストでその syslog エントリを生成した ACE を一意に識別します。
log-input *log-input-value*	（オプション）このエントリ（入力インターフェイスなど）とログを照合します。 **log-input** キーワード（および関連する *log-input-value* 引数）を指定した場合、このコマンドではその他のキーワードや設定は指定できません。
tcp	TCP プロトコルを指定します。
udp	UDP プロトコルを指定します。
port-match-criteria port-number	特定のポート番号を含むパケットのみに一致します。有効な値については、「使用上のガイドライン」を参照してください。

コマンド デフォルト　アクセス リストでパケットが許可される特定の条件はありません。

コマンド モード　標準アクセス リスト コンフィギュレーション（config-std-nacl） 拡張アクセス リスト コンフィギュレーション（config-ext-nacl）

コマンド履歴

リリース	変更内容
12.4(20)T	このコマンドが導入されました。
12.4(22)T	**log** キーワードと **log-input** キーワードに *word* 引数が追加されました。

使用上のガイドライン

パケットがアクセス リストで許可される条件を定義するには、**ipaccess-list** コマンドの後にこのコマンドを使用します。

Cisco IOS 15.0(1)M 以降のリリースでは、**permitipanyanylog** コマンドからログ エントリを削除するには **permitipanyany** コマンドを使用します。

Cisco IOS リリース 15.0(1)M より前のリリースでは、**log** オプションを **permitipanyanylog** コマンドから削除するには、**nopermitipanyanylog** コマンドと **permitipanyany** コマンドを使用します。

Cisco IOS リリース 15.0(1) M 以降のリリースでは、ログ エントリとユーザ定義 Cookie を削除するには **permitipanyany** [*log-value*] コマンドを使用します。

Cisco IOS リリース 15.0(1)M より前のリリースでは、ログ エントリとユーザ定義 Cookie を削除するには、**nopermitipanyanylog** [*log-value*] コマンドと **permitipanyany** コマンドを使用します。

フラグメントのアクセス リストまたは OGACL 処理

fragments キーワードを使用する場合と使用しない場合のアクセス リスト エントリの動作について、次の表で説明します。

表 *1*：フラグメントのアクセス リストまたは *OGACL* 処理

アクセス リスト エントリの状態...	結果

fragments キーワードが指定されておらず（デフォルトの動作）、すべてのアクセス リスト エントリ情報が一致している。	アクセス リスト エントリにレイヤ 3 情報のみが含まれている場合：
	• エントリは、非フラグメント パケット、先頭フラグメント、先頭以外のフラグメントに適用されます。
	
	アクセス リスト エントリにレイヤ 3 情報とレイヤ 4 情報が含まれている場合：
	• エントリは、非フラグメント パケットと先頭のフラグメントに適用されます。
	  • エントリが **permit** ステートメントであると、パケットまたはフラグメントは許可されます。
	  • エントリが **deny** ステートメントであると、パケットまたはフラグメントは拒否されます。
	
	• エントリは、次の方法で先頭以外のフラグメントにも適用されます。先頭以外のフラグメントにはレイヤ 3 情報のみが含まれているため、アクセス リスト エントリのレイヤ 3 の部分のみが適用されます。アクセス リスト エントリのレイヤ 3 の部分が一致し、
	  • エントリが **permit** ステートメントであると、先頭以外のフラグメントが許可されます。
	  • エントリが **deny** ステートメントであると、次のアクセス リスト エントリが処理されます。
	
	（注） 非初期フラグメントと、非フラグメントまたは初期フラグメントの場合では、**deny** ステートメントの処理方法は異なります。

アクセス リスト エントリの状態...	結果
fragments キーワードが指定され、すべてのアクセス リスト エントリ情報が一致している	（注） アクセス リスト エントリは、先頭以外のフラグメントにのみ適用されます。レイヤ 4 情報を含むアクセス リスト エントリには **fragments** キーワードは設定できません。

すべてのアクセス リスト エントリに **fragments** キーワードを追加しないでください。これは、IP パケットの最初のフラグメントは非フラグメントとして見なされ、以降のフラグメントとは独立して扱われるためです。先頭フラグメントは、アクセス リストの **fragments** キーワードが設定されている **permit** または **deny** エントリとは一致しません。パケットは、**fragments** キーワードが設定されていないアクセス リスト エントリで許可または拒否されるまで、次のアクセス リスト エントリとの比較が続行されます。したがって、**deny** エントリごとに、2 つのアクセス リスト エントリが必要になる場合があります。ペアの最初の **deny** エントリには **fragments** キーワードは含まれず、このエントリは先頭フラグメントに適用されます。ペアの 2 番目の **deny** エントリは、**fragments** キーワードを含んでおり、以降のフラグメントに適用されます。同じホストに対する複数の **deny** アクセス リスト エントリがあるが、レイヤ 4 ポートが異なる場合は、そのホストで **fragments** キーワードが設定された 1 つの **deny** アクセス リスト エントリを追加する必要があります。このように、パケットのすべてのフラグメントは、アクセス リストによって同様に扱われます。

IP データグラムのパケット フラグメントは個々のパケットと見なされ、それぞれ、アクセス リスト アカウンティングとアクセス リストの違反カウントの 1 つのパケットとして個別にカウントされます。

（注） アクセス リストおよび IP フラグメントに関するあらゆるケースを **fragments** キーワードで解決できるわけではありません。

フラグメントおよびポリシー ルーティング

ポリシー ルーティングが **matchipaddres** コマンドに基づくものであり、アクセス リストのエントリがレイヤ 4 ～ レイヤ 7 の情報に一致した場合、フラグメンテーションとフラグメント制御機能はポリシー ルーティングに影響を及ぼします。先頭フラグメントがポリシー ルーティングされなかった場合でも、先頭以外のフラグメントがアクセス リストを通過し、ポリシー ルーティングされることがあります。その逆もまた同じです。

前に説明したようにアクセス リスト エントリに **fragments** キーワードを使用すると、先頭フラグメントと先頭以外のフラグメントに対するアクションの照合を改善できるため、ポリシー ルーティングが想定どおりに機能する可能性が高くなります。

source-addr 引数と *destination-addr* 引数を使用すると、送信元グループと宛先グループを作成できます。次のキーワードおよび引数を使用できます。

- **dscp** *dscp-value*：（オプション）特定の DSCP 値を含むパケットと一致します。有効な値は次のとおりです。

- **0** ～ **63**：DiffServ コード ポイント値
- **af11**：AF11 dscp（001010）が設定されているパケットと一致します。
- **af12**：AF12 dscp（001100）が設定されているパケットと一致します。
- **af13**：AF13 dscp（001110）が設定されているパケットと一致します。
- **af21**：AF21 dscp（010010）が設定されているパケットと一致します。
- **af22**：AF22 dscp（010100）が設定されているパケットと一致します。
- **af23**：AF23 dscp（010110）が設定されているパケットと一致します。
- **af31**：AF31 dscp（011010）が設定されているパケットと一致します。
- **af32**：AF32 dscp（011100）が設定されているパケットと一致します。
- **af33**：AF33 dscp（011110）が設定されているパケットと一致します。
- **af41**：AF41 dscp（100010）が設定されているパケットと一致します。
- **af42**：AF42 dscp（100100）が設定されているパケットと一致します。
- **af43**：AF43 dscp（100110）が設定されているパケットと一致します。
- **cs1**：CS1（precedence 1）dscp（001000）が設定されているパケットと一致します。
- **cs2**：CS2（precedence 2）dscp（010000）が設定されているパケットと一致します。
- **cs3**：CS3（precedence 3）dscp（011000）が設定されているパケットと一致します。
- **cs4**：CS4（precedence 4）dscp（100000）が設定されているパケットと一致します。
- **cs5**：CS5（precedence 5）dscp（101000）が設定されているパケットと一致します。
- **cs6**：CS6（precedence 6）dscp（110000）が設定されているパケットと一致します。
- **cs7**：CS7（precedence 7）dscp（111000）が設定されているパケットと一致します。
- **default**：デフォルト dscp（000000）が設定されているパケットと一致します。
- **ef**：EF dscp（101110）が設定されているパケットと一致します。

- **fragments** ：（オプション）先頭以外のフラグメントをチェックします。前述の表を参照してください。
- **log** ：（オプション）このエントリとの一致をログに記録します。
- **log-input**（オプション）このエントリとの一致をログに記録します（入力インターフェイスなど）。
- **option** *option-value*：（オプション）特定の IP オプション値が設定されているパケットと一致します。有効な値は次のとおりです。
  - 0 ～ 255：IP オプションの値。
  - **add-ext**：Address Extension Option（147）が設定されているパケットと一致します。

- **any-options**：任意のオプションが設定されているパケットと一致します。
- **com-security**：Commercial Security Option（134）が設定されているパケットと一致します。
- **dps**：Dynamic Packet State Option（151）が設定されているパケットと一致します。
- **encode**：Encode Option（15）が設定されているパケットと一致します。
- **eool**：End of Options（0）が設定されているパケットと一致します。
- **ext-ip**：Extended IP Option（145）が設定されているパケットと一致します。
- **ext-security**：Extended Security Option（133）が設定されているパケットと一致します。
- **finn**：Experimental Flow Control Option（205）が設定されているパケットと一致します。
- **imitd**：IMI Traffic Descriptor Option（144）が設定されているパケットと一致します。
- **lsr**：Loose Source Route Option（131）が設定されているパケットと一致します。
- **match-all**：指定されたフラグがすべて存在する場合にパケットと一致します。
- **match-any**：指定されたいずれかのフラグが存在する場合にパケットと一致します。
- **mtup**：MTU Probe Option（11）が設定されているパケットと一致します。
- **mtur**：MTU Reply Option（12）が設定されているパケットと一致します。
- **no-op**：No Operation Option（1）が設定されているパケットと一致します。
- **psh**：PSH ビットが設定されているパケットと一致します。
- **nsapa**：NSAP Addresses Option（150）が設定されているパケットと一致します。
- **reflect**：再帰的なアクセス リスト エントリを作成します。
- **record-route**：Record Route Option（7）が設定されているパケットと一致します。
- **rst**：RST ビットが設定されているパケットと一致します。
- **router-alert**：Router Alert Option（148）が設定されているパケットと一致します。
- **sdb**：Selective Directed Broadcast Option（149）が設定されているパケットと一致します。
- **security**：Basic Security Option（130）が設定されているパケットと一致します。
- **ssr**：Strict Source Route Option（137）が設定されているパケットと一致します。
- **stream-id**：Stream ID Option（136）が設定されているパケットと一致します。
- **syn**：SYN ビットが設定されているパケットと一致します。
- **timestamp**：Time Stamp Option（68）が設定されているパケットと一致します。
- **traceroute**：Trace Route Option（82）が設定されているパケットと一致します。
- **ump**：Upstream Multicast Packet Option（152）が設定されているパケットと一致します。

- **visa**：Experimental Access Control Option（142）が設定されているパケットと一致します。
- **zsu**：Experimental Measurement Option（10）が設定されているパケットと一致します。

- **precedence** *precedence-value*：（オプション）特定の precedence 値を持つパケットと一致します。有効な値は次のとおりです。
  - 0 ～ 7：precedence 値。
  - **critical**：critical precedence（5）が設定されているパケットと一致します。
  - **flash**：flash precedence（3）が設定されているパケットと一致します。
  - **flash-override**：flash override precedence（4）が設定されているパケットと一致します。
  - **immediate**：immediate precedence（2）が設定されているパケットと一致します。
  - **internet**：internetwork control precedence（6）が設定されているパケットと一致します。
  - **network**：network control precedence（7）が設定されているパケットと一致します。
  - **priority**：priority precedence（1）が設定されているパケットと一致します。
  - **routine**：routine precedence（0）が設定されているパケットと一致します。
- **reflectacl-name** ：（オプション）再帰的なアクセス リスト エントリを作成します。
- **ttl** *match-value ttl-value*：（オプション）特定の TTL 値が設定されているパケットとの一致を指定します。有効な値は次のとおりです。
  - **eq**：指定された TTL 値が設定されているパケットと一致します。
  - **gt**：より大きい TTL 値が設定されているパケットと一致します。
  - **lt**：より小さい TTL 値が設定されているパケットと一致します。
  - **neq**：指定された TTL 値が設定されていないパケットと一致します。
  - **range**--TTL の範囲内のパケットと一致します。
- **time-range** *time-range-value*：（オプション）時間範囲エントリ名を指定します。
- **tos** ：指定された ToS 値を持つパケットと一致します。有効な値は次のとおりです。
  - 0 ～ 15：タイプ オブ サービス（ToS）値。
  - **max-reliability**：maximum reliable ToS（2）が設定されているパケットと一致します。
  - **max-throughput**：maximum throughput ToS（4）が設定されているパケットと一致します。
  - **min-delay**：minimum delay ToS（8）が設定されているパケットと一致します。
  - **min-monetary-cost**：minimum monetary cost ToS（1）が設定されているパケットと一致します。

- **normal**：normal ToS（0）が設定されているパケットと一致します。
- **timeout** *max-time*：（オプション）再帰 ACL の最大存続期間を指定します。有効な値は 1 ～ 2147483 秒です。

関連コマンド

Command	Description
deny	パケットを拒否する名前付き IP アクセス リストまたは OGACL の条件を設定します。
ipaccess-group	ACL または OGACL をインターフェイスまたはサービス ポリシー マップに適用します。
ipaccess-list	IP アクセス リストまたは OGACL を名前または番号で定義します。
ipaccess-listlogginghash-generation	ACE syslog エントリのハッシュ値の生成を有効にします。
showipaccess-list	IP アクセス リストまたは OGACL の内容を表示します。

permit (IP)

パケットが名前付き IP アクセス リストで許可される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。アクセス リストから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** *source* [*source-wildcard*]

[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] **[fragments]** [**log** [*user-defined-cookie*]]

no *sequence-number*

no permit *source* [*source-wildcard*]

no permit *protocol source source-wildcard destination destination-wildcard* [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] **[fragments]** [**log** [*user-defined-cookie*]]

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*]| *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] **[fragments]** [**log** [*user-defined-cookie*]]

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*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] **[fragments]** [**log** [*user-defined-cookie*]]

伝送制御プロトコル（**TCP**）

[sequence-number] permit tcp *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established** {**match-any**| **match-all**} {+-} *flag-name*| **precedence** *precedence*| **tos** *tos*| **ttl** *operator value*| **log**| **time-range** *time-range-name*| **fragments**| **log** | [*user-defined-cookie*]]

ユーザ データグラム プロトコル（**UDP**）

[*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] **[fragments]** [**log** [*user-defined-cookie*]]

構文の説明

sequence-number	（オプション）permit ステートメントに割り当てられているシーケンス番号。システムはこのシーケンス番号に基づいて、ステートメントをアクセス リストのその番号の位置に挿入します。

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* 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	（オプション）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は 1 を設定します。 • **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* 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	インターネットプロトコルの名前または番号。*protocol* 引数には、キーワード **eigrp**、**gre**、**icmp**、**igmp**、**ip**、**ipinip**、**nos**、**ospf**、**tcp**、または **udp** のいずれか、あるいはインターネットプロトコル番号を表す 0 ～ 255 の範囲内の整数を設定できます。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。 （注） **icmp**、**igmp**、**tcp,**および **udp** キーワードを入力するときには、**permit** コマンドの ICMP、IGMP、TCP、および UDP 形式で示されている特定のコマンド構文に従う必要があります。 （注） BGP トラフィックを許可するようにパケット フィルタを設定するには、プロトコル **tcp** を使用し、ポート番号 179 または bgp を指定します。 **bgp**
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* 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は 1 を設定します。 • **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* 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。
option *option-name*	（オプション）パケットは IP オプション（0 ～ 255 の番号で指定）または対応する IP オプション名（「使用上のガイドライン」の表に記載）に基づいてフィルタリングできます。
precedence *precedence*	（オプション）パケットは、優先レベル（0 ～ 7 の番号で指定）または名前でフィルタリングできます。
tos *tos*	（オプション）パケットは、タイプ オブ サービス（ToS）レベル（0 ～ 15 の番号で指定）または名前（**access-list**（IP extended）コマンドの「使用上のガイドライン」に記載）に基づいてフィルタリングできます。

ttl *operator-value*	（オプション）この **permit** ステートメントに指定されている TTL 値とパケットの TTL 値を比較します。 • *operator* は **lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、**neq**（等しくない）、または **range**（包含範囲）のいずれかです。 • *value* は 0 ～ 255 の範囲で指定します。 • 演算子が **range** の場合、2 つの値を 1 つのスペースで区切って指定します。 • リリース 12.0S では、演算子が **eq** または **neq** の場合、1 つの TTL 値だけを指定できます。 • その他のすべてのリリースでは、演算子が **eq** または **neq** の場合、最大 10 個の TTL 値をスペースで区切って指定できます。
time-range *time-range-name*	（オプション）この **permit** ステートメントに適用する時間範囲の名前。時間範囲の名前は **time-range** コマンドにより指定され、時間範囲の制約は **absolute** または **periodic** コマンドにより指定されます。
fragments	（オプション）アクセス リスト エントリがパケットの先頭以外のフラグメントに適用され、フラグメントが許可または拒否されます。**fragments** キーワードの詳細については、「使用上のガイドライン」の「フラグメント」および「フラグメントおよびポリシー ルーティング」の「フラグメントのアクセスリスト処理」を参照してください。
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 **loggingconsole** コマンドで制御します）。 **log** キーワード（および関連する *word* 引数）を指定した場合、このコマンドではその他のキーワードや設定は指定できません。

user-defined-cookie	（オプション）ログ メッセージに付加されるユーザ定義 Cookie。Cookie の条件は次のとおりです。 • 64 文字以内である必要があります。 • 16 進表記（0x など）で始めることはできません。 • **fragment,reflect** といったキーワードと同じであることはできません。また、これらのキーワードの一部を使用することはできません。 **time-range.** • 英数字のみを使用する必要があります。 ユーザ定義 Cookie は Allegro Crypto Engine（ACE）syslog エントリに付加され、アクセス コントロール リスト内でその syslog エントリを生成した ACE を一意に識別します。
icmp	ICMP パケットだけを許可します。**icmp** キーワードを入力するときには、**permit** コマンドの ICMP 形式で示されている特定のコマンド構文を使用する必要があります。
icmp-type	（オプション）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。メッセージ タイプの番号は 0 ～ 255 です。
icmp-code	（オプション）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。メッセージ コードの番号は 0 ～ 255 です。
icmp-message	（オプション）ICMP パケットは、ICMP メッセージ タイプ名、または ICMP メッセージ タイプとコード名によってフィルタリングできます。有効な名前は、**access-list**（IP extended）コマンドの「使用上のガイドライン」に記載されています。
igmp	IGMP パケットだけを許可します。**igmp** キーワードを入力するときには、**permit** コマンドの IGMP 形式で示されている特定のコマンド構文を使用する必要があります。

igmp-type	（オプション）IGMP パケットは、IGMP メッセージタイプまたはメッセージ名でフィルタリングできます。メッセージタイプの番号は 0 ～ 15 です。IGMP メッセージ名は、**access-list**（IP extended）コマンドの「使用上のガイドライン」に記載されています。
tcp	TCP パケットだけを許可します。**tcp** キーワードを入力するときには、**permit** コマンドの TCP 形式で示されている特定のコマンド構文を使用する必要があります。
operator	（オプション）発信元ポートまたは宛先ポートを比較します。演算子は **eq**（等しい）、**gt**（より大きい）、**lt**（より小さい）、**neq**（等しくない）、および **range**（包含範囲）です。 演算子が source および source-wildcard 引数の後にある場合、送信元ポートに一致する必要があります。演算子が destination および destination-wildcard 引数の後にある場合、宛先ポートに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。**eq**（等しい）および **neq**（等しくない）演算子に対し、最大 10 個のポート番号を入力できます。他のすべての演算子は 1 つのポート番号が必要です。
port	（オプション）TCP または UDP ポートの 10 進数の番号または名前。ポート番号の範囲は 0 ～ 65535 です。TCP ポート名と UDP ポート名は、**access-list(IPextended)** コマンドの「使用上のガイドライン」に記載されています。 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。TCP データグラムに ACK または RST ビットが設定されている場合に一致します。接続するための初期 TCP データグラムの場合は照合しません。

match-any | **match-all**	（オプション）TCP プロトコルのみ：TCP データグラムで特定の TCP フラグの設定の有無に関係なく、一致します。指定した TCP フラグのいずれかが存在している場合に一致するようにするには、**match-any** キーワードを使用します。あるいは、指定した TCP フラグがすべて存在している場合に一致するようにするには、**match-all** キーワードを使用します。1 つ以上の TCP フラグを一致基準として使用するには、**match-any** および **match-all** キーワードの後に、**+** または **-** キーワードと *flag-name* 引数を指定する必要があります。
+ | **-** *flag-name*	（オプション）TCP プロトコルのみ：**+** キーワードを使用する場合、*flag-name* 引数に指定した TCP フラグが TCP ヘッダーに含まれている IP パケットが一致します。**-** キーワードを使用する場合、*flag-name* 引数に指定した TCP フラグが含まれていない IP パケットが一致します。**+** キーワードと **-** キーワードの後には *flag-name* 引数を指定する必要があります。TCP フラグ名は、TCP をフィルタリングする場合に限り使用できます。TCP フラグのフラグ名は、**ack**、**fin**、**psh**、**rst**、**syn**、および **urg** です。
udp	UDP パケットだけを許可します。**udp** キーワードを入力するときには、**permit** コマンドの UDP 形式で示されている特定のコマンド構文を使用する必要があります。

コマンド デフォルト

名前付きアクセス リストでパケットが許可される特定の条件はありません。

コマンド モード

アクセス リスト コンフィギュレーション（config-ext-nacl）

コマンド履歴

リリース	変更内容
11.2	このコマンドが導入されました。
12.0(1)T	**time-range** *time-range-name* キーワードおよび引数が追加されました。

リリース	変更内容
12.0(11)	**fragments** キーワードが追加されました。
12.2(13)T	Cisco IOS ソフトウェアで IGRP プロトコルが使用できなくなったため、igrp キーワードは削除されました。
12.2(14)S	*sequence-number* 引数が追加されました。
12.2(15)T	*sequence-number* 引数が追加されました。
12.3(4)T	**option** *option-name* キーワードおよび引数が追加されました。**match-any**、**match-all,+,**、および **-** キーワードと *flag-name* 引数が追加されました。
12.3(7)T	コマンド機能が変更され、**eq** 演算子と **neq** 演算子の後に最大 10 個のポート番号を追加できるようになりました。これにより、連続しないポートを使用してアクセス リスト エントリを作成できます。
12.4	**drip** キーワードが追加されました。このキーワードでは、Optimized Edge Routing（OER）通信に使用する TCP ポート番号を指定できます。
12.4(2)T	**ttl** *operator value* キーワードおよび引数が追加されました。
12.2(27)SBC	このコマンドが、Cisco IOS Release 12.2(27)SBC に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
12.4(22)T	**log** キーワードに *word* 引数が追加されました。
Cisco IOS XE リリース 3.2	このコマンドが、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されました。

使用上のガイドライン

パケットが名前付きアクセス リストで許可される条件を定義するには、**ipaccess-list** コマンドの後に **permit** コマンドを使用します。

（注） Cisco IOS XE では、**permit** コマンドを使用して、ユーザがネットワークにアクセスするための包含ポート範囲を拡張 ACL で照合することはできません。

time-range キーワードでは、時間範囲を名前で指定できます。**time-range**、**absolute**、および **periodic** コマンドは、この **permit** ステートメントが有効になる時点を指定します。

log キーワード

ログ メッセージには、アクセス リスト番号またはアクセス リスト名、パケットの許可/拒否、プロトコル（TCP、UDP、ICMP、または番号）が含まれます。また該当する場合には、送信元アドレスと宛先アドレス、ポート番号、およびユーザ定義 Cookie またはルータ生成ハッシュ値も含まれます。一致した最初のパケットに関するメッセージが生成され、その後 5 分間隔で、前の 5 分間で許可または拒否されたパケット数を含むメッセージが生成されます。

5 分間の間隔が経過するまで待たずに、一致の数が設定可能なしきい値に到達した場合にロギング メッセージを生成するには、**ipaccess-listlog-update** コマンドを使用します。詳細については、**ipaccess-listlog-update** コマンドを参照してください。

ロギング メッセージが多すぎて処理できない場合、または 1 秒以内に処理する必要があるロギング メッセージが複数ある場合、ロギング設備ではロギング メッセージ パケットの一部をドロップすることがあります。この動作により、ロギング パケットが多すぎるためにルータがリロードすることが防止されます。そのため、課金ツールや、アクセス リストと一致する数の正確な情報源としてロギング設備を使用しないでください。

シスコ エクスプレス フォワーディングをイネーブルにしてから、**log** キーワードを使用するアクセス リストを作成した場合、アクセス リストと一致するパケットは、シスコ エクスプレス フォワーディングで交換されたものではありません。これらはファーストスイッチングで交換されたものです。ロギングにより、Cisco Express Forwarding が無効になります。

IP オプションのアクセス リスト フィルタリング

アクセス コントロール リストを使用して IP オプションを含むパケットをフィルタリングできます。これにより、IP オプションを含む偽のパケットでルータがいっぱいになることが防がれます。現在使用されていない IP オプションを含むすべての IP オプションが記載されている表を参照するには、Internet Assigned Numbers Authority（IANA）の最新情報（www.iana.org）を参照してください。

Cisco IOS ソフトウェアでは、パケットに 1 つ以上の正当な IP オプションが含まれているかどうかに基づいてパケットをフィルタリングできます。このためには、次の表に示すように、*option-name* 引数に IP オプション値または対応する名前を入力します。

表 *2*：*IP* オプションの値と名前

IP オプションの値と名前	説明
0 ～ 255	IP オプションの値。
add-ext	Address Extension Option（147）が設定されているパケットと一致します。
any-options	任意の IP オプションが設定されているパケットと一致します。

IP オプションの値と名前	説明
com-security	Commercial Security Option（134）が設定されているパケットと一致します。
dps	Dynamic Packet State Option（151）が設定されているパケットと一致します。
encode	Encode Option（15）が設定されているパケットと一致します。
eool	End of Options（0）が設定されているパケットと一致します。
ext-ip	Extended IP Options（145）が設定されているパケットと一致します。
ext-security	Extended Security Option（133）が設定されているパケットと一致します。
finn	Experimental Flow Control Option（205）が設定されているパケットと一致します。
imitd	IMI Traffic Descriptor Option（144）が設定されているパケットと一致します。
lsr	Loose Source Route Option（131）が設定されているパケットと一致します。
mtup	MTU Probe Option（11）が設定されているパケットと一致します。
mtur	MTU Reply Option（12）が設定されているパケットと一致します。
no-op	No Operation Option（1）が設定されているパケットと一致します。
nsapa	NSAP Addresses Option（150）が設定されているパケットと一致します。
psh	PSH ビットが設定されているパケットと一致します。
record-route	Router Record Route Option（7）が設定されているパケットと一致します。

IP オプションの値と名前	説明
reflect	再帰的なアクセス リスト エントリを作成します。
router-alert	Router Alert Option（148）が設定されているパケットと一致します。
rst	RST ビットが設定されているパケットと一致します。
sdb	Selective Directed Broadcast Option（149）が設定されているパケットと一致します。
security	Base Security Option（130）が設定されているパケットと一致します。
ssr	Strict Source Routing Option（137）が設定されているパケットと一致します。
stream-id	Stream ID Option（136）が設定されているパケットと一致します。
syn	SYN ビットが設定されているパケットと一致します。
timestamp	Time Stamp Option（68）が設定されているパケットと一致します。
traceroute	Trace Route Option（82）が設定されているパケットと一致します。
ump	Upstream Multicast Packet Option（152）が設定されているパケットと一致します。
visa	Experimental Access Control Option（142）が設定されているパケットと一致します。
zsu	Experimental Measurement Option（10）が設定されているパケットと一致します。

TCP フラグに基づく IP パケットのフィルタリング

特定の TCP フラグ グループが設定されているパケットのみ、または設定されていないパケットのみを許可することで、不正な TCP パケットを検出およびドロップするように、アクセスリストを構成するアクセス リスト エントリを設定できます。フィルタリングする TCP パケットについて、

TCP フラグの任意の組み合わせを選択できます。ユーザは、設定されているフラグと設定されていないフラグに基づいて照合できるようにアクセスリストエントリを設定できます。キーワード **+** および **-** とフラグ名を使用して、TCP ヘッダー フラグが設定されているかどうかに基づいて一致が決定することを指定します。キーワード **match-any** と **match-all** を使用し、キーワード **+** または **-** と *flag-name* 引数で指定されているフラグの一部またはすべてが設定されている場合または設定されていない場合に、パケットを許可することを指定します。

Optimized Edge Routing（OER）通信の許可

OER が設定されているネットワークでパケット フィルタリングをサポートするため、**drip** キーワードが **tcp** キーワードに導入されました。**drip** キーワードは、OER が内部通信に使用するポート 3949 を指定します。このオプションを使用して、OER マスタ コントローラと境界ルータ間での通信を許可するパケット フィルタを作成できます。**drip** キーワードは、TCP 送信元アドレス、宛先アドレス、および **eq** 演算子の後に入力されます。「例」に記載されている例を参照してください。

フラグメントのアクセス リスト処理

fragments キーワードを使用する場合と、使用しない場合に関するアクセス リスト エントリの動作は、次のようにまとめることができます。

アクセス リスト エントリの状態...	結果...

fragments キーワードが指定されておらず（デフォルトの動作）、すべてのアクセス リスト エントリ情報が一致している。	レイヤ 3 情報だけを含むアクセス リスト エントリの場合、このエントリは非フラグメント パケット、先頭フラグメント、先頭以外のフラグメントに適用されます。
	レイヤ 3 およびレイヤ 4 情報を含むアクセス リスト エントリの場合：
	• エントリは、非フラグメント パケットと先頭フラグメントに適用されます。
	  • エントリが **permit** ステートメントであると、パケットまたはフラグメントは許可されます。
	  • エントリが **deny** ステートメントであると、パケットまたはフラグメントは拒否されます。
	• エントリは、次の方法で先頭以外のフラグメントにも適用されます。非初期フラグメントにはレイヤ 3 情報のみが含まれているため、アクセス リスト エントリのレイヤ 3 の部分のみが適用されます。アクセス リスト エントリのレイヤ 3 の部分が一致し、
	  • エントリが **permit** ステートメントであると、先頭以外のフラグメントは許可されます。
	  • エントリが **deny** ステートメントであると、次のアクセス リスト エントリが処理されます。
	（注） 非初期フラグメントと、非フラグメントまたは初期フラグメントの場合では、**deny** ステートメントの処理方法は異なります。

fragments キーワードが指定され、すべてのアクセス リスト エントリ情報が一致している。	アクセス リスト エントリは、非初期フラグメントにのみ適用されます。レイヤ 4 情報を含むアクセスリスト エントリには、**fragments** キーワードは設定できません。

すべてのアクセス リスト エントリに **fragments** キーワードを追加することはできません。IP パケットの最初のフラグメントは非フラグメントとして見なされ、以降のフラグメントとは独立して扱われるためです。先頭フラグメントは、アクセス リストの **fragments** キーワードが設定された **permit** または **deny** エントリとは一致しません。パケットは、**fragments** キーワードが設定されていないアクセス リスト エントリによって許可または拒否されるまで、次のアクセス リスト エントリと比較されます。したがって、**deny** エントリごとに、2 つのアクセス リスト エントリが必要になる場合があります。ペアの最初の **deny** エントリには、**fragments** キーワードは含まれず、初期フラグメントに適用されます。ペアの 2 番目の **deny** エントリは、**fragments** キーワードを含んでおり、以降のフラグメントに適用されます。同じホストに対する複数の **deny** アクセス リスト エントリがあるが、レイヤ 4 ポートが異なる場合は、そのホストで **fragments** キーワードが設定された 1 つの **deny** アクセス リスト エントリを追加する必要があります。このように、パケットのすべてのフラグメントは、アクセス リストによって同様に扱われます。

IP データグラムのパケット フラグメントは個々のパケットと見なされ、それぞれ、アクセス リスト アカウンティングとアクセス リストの違反カウントの 1 つのパケットとして個別にカウントされます。

（注） アクセス リストおよび IP フラグメントに関するあらゆるケースを **fragments** キーワードで解決できるわけではありません。

フラグメントおよびポリシー ルーティング

ポリシー ルーティングが **matchipaddress** コマンドに基づくものであり、アクセス リストのエントリがレイヤ 4 ～ レイヤ 7 の情報に一致した場合、フラグメンテーションとフラグメント制御機能はポリシー ルーティングに影響を及ぼします。先頭フラグメントがポリシー ルーティングされなかった場合でも、先頭以外のフラグメントがアクセス リストで許可され、ポリシー ルーティングされることがあります。

アクセス リスト エントリに **fragments** キーワードを指定すると、先頭フラグメントと先頭以外のフラグメントに対するアクションの照合を改善できるため、ポリシー ルーティングが想定どおりに機能する可能性が高くなります。

非隣接ポートを使用するアクセス リスト エントリの作成

Cisco IOS リリース 12.3(7)T 以降では、1 つのアクセス コントロール エントリに複数の非隣接ポートを指定できます。これにより、同一の送信元アドレス、宛先アドレス、プロトコルの必要なアクセス リスト エントリの数が大幅に削減されます。多数のアクセス リスト エントリを管理している場合は、可能であれば非隣接ポートを使用してこれらのエントリを統合することを推奨します。**eq** 演算子と **neq** 演算子の後に最大 10 個のポート番号を指定できます。

例

次に、Internetfilter という名前の標準アクセス リストの条件を設定する例を示します。

```
ip access-list standard Internetfilter
 deny 192.168.34.0  0.0.0.255
 permit 172.16.0.0  0.0.255.255
 permit 10.0.0.0  0.255.255.255
! (Note: all other access implicitly denied).
```

次に、月曜日、火曜日、金曜日の 9:00 a.m. から 5:00 p.m までの間に Telnet トラフィックを許可する例を示します。

```
time-range testing
 periodic Monday Tuesday Friday 9:00 to 17:00
!
ip access-list extended legal
 permit tcp any any eq telnet time-range testing
!
interface ethernet0
 ip access-group legal in
```

次に、filter2 という名前の拡張アクセス リストの許可条件を設定する例を示します。アクセス リスト エントリは、NSAP Addresses IP オプション（IP オプション値は nsapa）を含むパケットが名前付きアクセス リストで許可されることを指定します。

```
ip access-list extended filter2
 permit ip any any option nsapa
```

次に、kmdfilter1 という名前の拡張アクセス リストの許可条件を設定する例を示します。アクセス リスト エントリは、RST IP フラグが設定されているパケットだけが名前付きアクセス リストで許可されることを指定します。

```
ip access-list extended kmdfilter1
 permit tcp any any match-any +rst
```

次に、kmdfilter1 という名前の拡張アクセス リストの許可条件を設定する例を示します。アクセス リスト エントリは、RST TCP フラグまたは FIN TCP フラグが設定されているパケットが名前付きアクセス リストで許可されることを指定します。

```
ip access-list extended kmdfilter1
 permit tcp any any match-any +rst +fin
```

次に、**show access-lists** コマンドを使用してアクセス リストを検証し、エントリを既存のアクセス リストに追加する例を示します。

```
Router# show access-lists
Standard IP access list 1
2 permit 10.0.0.0, wildcard bits 0.0.255.255
5 permit 10.0.0.0, wildcard bits 0.0.255.255
10 permit 10.0.0.0, wildcard bits 0.0.255.255
20 permit 10.0.0.0, wildcard bits 0.0.255.255
ip access-list standard 1
 15 permit 10.0.0.0 0.0.255.255
```

次に、シーケンス番号が 20 のエントリをアクセス リストから削除する例を示します。

```
ip access-list standard 1
 no 20
!Verify that the list has been removed.
Router# show access-lists
Standard IP access list 1
10 permit 0.0.0.0, wildcard bits 0.0.0.255
30 permit 0.0.0.0, wildcard bits 0.0.0.255
40 permit 0.4.0.0, wildcard bits 0.0.0.255
```

次に、リストにすでに存在するエントリの重複エントリをユーザが入力すると、何も変更されない例を示します。ユーザが追加しようとしているエントリは、アクセス リストのシーケンス番号 20 のエントリと重複しています。

```
Router# show access-lists 101
Extended IP access list 101
    10 permit ip host 10.0.0.0 host 10.5.5.34
    20 permit icmp any any
```

```
    30 permit ip host 10.0.0.0 host 10.2.54.2
    40 permit ip host 10.0.0.0 host 10.3.32.3 log
ip access-list extended 101
 100 permit icmp any any
Router# show access-lists 101
Extended IP access list 101
    10 permit ip host 10.3.3.3 host 10.5.5.34
    20 permit icmp any any
    30 permit ip host 10.34.2.2 host 10.2.54.2
    40 permit ip host 10.3.4.31 host 10.3.32.3 log
```

次に、シーケンス番号20のエントリがすでにリストに存在しているために、ユーザがシーケンス番号 20 の新しいエントリを入力しようとすると発生する動作の例を示します。エラー メッセージが表示され、アクセス リストは変更されません。

```
Router# show access-lists 101
Extended IP access lists 101
    10 permit ip host 10.3.3.3 host 10.5.5.34
    20 permit icmp any any
    30 permit ip host 10.34.2.2 host 10.2.54.2
    40 permit ip host 10.3.4.31 host 10.3.32.3 log
ip access-lists extended 101
 20 permit udp host 10.1.1.1 host 10.2.2.2
%Duplicate sequence number.
Router# show access-lists 101
Extended IP access lists 101
    10 permit ip host 10.3.3.3 host 10.5.5.34
    20 permit icmp any any
    30 permit ip host 10.34.2.2 host 10.2.54.2
    40 permit ip host 10.3.4.31 host 10.3.32.3 log
```

次に、非隣接ポートが設定されている 1 つのアクセス リスト エントリに統合可能ないくつかの **permit** ステートメントの例を示します。アクセス リスト aaa のアクセス リスト エントリのグループを表示するため、**showaccess-lists** コマンドが入力されます。

```
Router# show access-lists aaa
Extended IP access lists aaa
 10 permit tcp any eq telnet any eq 450
 20 permit tcp any eq telnet any eq 679
 30 permit tcp any eq ftp any eq 450
 40 permit tcp any eq ftp any eq 679
```

エントリはすべて同じ **permit** ステートメント用であり、ポートのみが異なるため、1 つの新しいアクセス リスト エントリに統合できます。次の例では、重複するアクセス リスト エントリを削除し、以前に表示されていたアクセス リスト エントリ グループを統合する新しいアクセス リスト エントリを作成します。

```
ip access-list extended aaa
 no 10
 no 20
 no 30
 no 40
 permit tcp any eq telnet ftp any eq 450 679
```

次に、統合アクセス リスト エントリの作成例を示します。

```
Router# show access-lists aaa
Extended IP access list aaa
 10 permit tcp any eq telnet ftp any eq 450 679
```

次のアクセス リストでは、TTL 値が 10 と 20 でタイプ オブ サービス（ToS）レベルが 3 の IP パケットをフィルタリングします。また、TTL が 154 を超える IP パケットをフィルタリングし、その規則を先頭以外のフラグメントにも適用します。フラッシュの優先レベルと 1 以外の TTL を持

つ IP パケットを許可し、そのようなパケットに関するログ メッセージをコンソールに送信します。他のすべてのパケットは拒否されます。

```
ip access-list extended canton
 deny ip any any tos 3 ttl eq 10 20
 deny ip any any ttl gt 154 fragments
 permit ip any any precedence flash ttl neq 1 log
```

次に、すべての TCP 送信元と宛先に適用され、OER マスタ コントローラと境界ルータ間の通信を許可するパケット フィルタを設定する例を示します。

```
ip access-list extended 100
 permit any any tcp eq drip
 exit
```

次に、filter_logging という名前の拡張アクセス リストの許可条件を設定する例を示します。このアクセス リスト エントリは、TCP プロトコル タイプで宛先ホストが 10.5.5.5 であるパケットだけが名前付きアクセス リストで許可され、その他のパケットはすべて拒否されることを指定します。また、ロギング メカニズムが有効になり、ユーザ定義 Cookie（Permit_tcp_to_10.5.5.5 または Deny_all）が適切な syslog エントリに付加されます。

```
ip access-list extended filter_logging
 permit tcp any host 10.5.5.5 log Permit_tcp_to_10.5.5.5
 deny ip any any log Deny_all
```

次に、すべての TCP 送信元と宛先に適用され、インバウンドおよびアウトバウンド BGP トラフィックを許可するパケット フィルタを設定する例を示します。

```
ip access-list extended 100
 permit tcp any eq bgp any eq bgp
```

関連コマンド

Command	Description
absolute	時間範囲が有効なときの絶対時間を指定します。
access-list(IPextended)	拡張 IP アクセス リストを定義します。
access-list(IPstandard)	標準 IP アクセス リストを定義します。
deny(IP)	パケットが名前付き IP アクセス リストで許可されない条件を設定します。
ipaccess-group	インターフェイスへのアクセスを制御します。
ipaccess-listlog-update	ロギング メッセージが生成される条件となるパケット数のしきい値を設定します。
ipaccess-listlogginghash-generation	ACE syslog エントリのハッシュ値の生成を有効にします。

Command	Description
ipaccess-listresequence	アクセス リストのアクセス リスト エントリにシーケンス番号を適用します。
ipoptions	ルータに送信された IP オプション パケットをドロップまたは無視します。
loggingconsole	システム ロギング（syslog）メッセージがすべての使用可能な TTY 回線に送信され、重大度に応じてメッセージが制限されます。
matchipaddress	標準アクセス リストまたは拡張アクセス リストで許可された宛先ネットワーク番号アドレスを含むすべてのルートを配するか、またはパケットに対してポリシー ルーティングを実行します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
showaccess-lists	アクセスリスト エントリ グループを表示します。
showipaccess-list	現在のすべての IP アクセス リストの内容を表示します。
time-range	アクセス リストまたはその他の機能が有効になる時点を指定します。

port

デバイスが設定されている RADIUS クライアントからの RADIUS 要求をリッスンするポートを指定するには、ダイナミック認証ローカル サーバ コンフィギュレーション モードで **port** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

port *port-number*

no port *port-number*

構文の説明

port-number	ポート番号。デフォルト値は、ポート 1700 です。

コマンド デフォルト

デバイスはデフォルト ポート（ポート 1700）で RADIUS 要求をリッスンします。

コマンド モード

ダイナミック認証サーバ コンフィギュレーション（config-locsvr-da-radius）

コマンド履歴

リリース	変更内容
12.2(28)SB	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

外部ポリシー サーバがルータにアップデートを動的に送信できるようにデバイス（ルータなど）を設定できるようになりました。この機能は CoA RADIUS 拡張により可能になりました。CoA によりピアツーピア機能が RADIUS に導入されました。この機能により、ルータと外部ポリシー サーバがそれぞれ RADIUS クライアントとサーバとして動作できます。ルータが RADIUS クライアントからの要求をリッスンするポートを指定するには、**port** コマンドを使用します。

例

次の例では、デバイスが RADIUS 要求をリッスンするポートとしてポート 1650 が指定されます。

```
aaa server radius dynamic-author
 client 10.0.0.1
 port 1650
```

関連コマンド

コマンド	説明
aaaserverradiusdynamic-author	デバイスを AAA サーバとして設定し、外部ポリシー サーバとの連携を容易にします。

port (TACACS+)

TACACS+ 接続に使用する TCP ポートを指定するには、TACACS+ サーバ コンフィギュレーション モードで **port** コマンドを使用します。TCP ポートを削除するには、このコマンドの **no** 形式を使用します。

port [*number*]

no port [*number*]

構文の説明

number	（オプション）TACACS+ サーバが Access-Request パケットの受信に使用するポートを指定します。有効な範囲は 1 ～ 65535 です。

コマンド デフォルト

ポートを設定しなかった場合は、ポート 49 が使用されます。

コマンド モード

TACACS+ サーバ コンフィギュレーション（config-server-tacacs）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2S	このコマンドが導入されました。

使用上のガイドライン

port コマンドを使用するときに *number* 引数を使用しないと、TCP ポート 49 が使用されます。

例

次に、TCP ポート 12 を指定する例を示します。

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# port 12
```

関連コマンド

Command	Description
tacacsserver	TACACS+ サーバを IPv6 または IPv4 に対して設定し、TACACS+ サーバ コンフィギュレーション モードを開始します。