deny ～ dialer aaa

deny

名前付き IP アクセス リストまたは Object Group Access Control List (OGACL) に条件を適用するには、適切なコンフィギュレーション モードで **deny** コンフィギュレーション コマンドを使用します。 IP アクセス リストまたは OGACL 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。

deny *protocol* {*src-addr src-wildcard*| **object-group** *object-group-name*| **any**| **host** {*addr*| *name*}} {*dest-addr dest-wildcard*| **any**| **eq** *port*| **gt** *port*| **host** {*addr*| *name*}| **lt** *port*| **neq** *port*| **portgroup** *srcport-groupname*| **object-group** *dest-addr-groupname*| **range** *port*| [**dscp** *type*| **fragments**| **option** *option*| **precedence** *precedence*| **log**| **log-input**| **time-range** *time-range-name*| **tos** *tos*| **ttl** *ttl-value*]}

no deny *protocol* {*src-addr src-wildcard*| **object-group** *object-group-name*| **any**| **host** {*addr*| *name*}} {*dest-addr dest-wildcard*| **any**| **eq** *port*| **gt** *port*| **host** {*addr*| *name*}| **lt** *port*| **neq** *port*| **portgroup** *srcport-groupname*| **object-group** *dest-addr-groupname*| **range** *port*| [**dscp** *type*| **fragments**| **option** *option*| **precedence** *precedence*| **log**| **log-input**| **time-range** *time-range-name*| **tos** *tos*| **ttl** *ttl-value*]}

構文の説明

protocol	プロトコル名または番号。有効な値は、**eigrp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、**tcp**、または **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。 一致条件としてインターネット プロトコル（Internet Control Message Protocol（ICMP）、TCP、User Datagram Protocol（UDP）など）を指定するには、キーワード **ip** を使用します。 その他の修飾詞については、「使用上のガイドライン」の項を参照してください。
src-addr	10 進表記の 4 つの部分をドットで区切った 32 ビット量のパケットの送信元ネットワークまたはホストの番号。
src-wildcard	10 進表記の 4 つの部分をドットで区切った、送信元ネットワークに適用するワイルドカード ビット。 無視するビット位置に 1 を入れます。
object-group *object-group-name*	オブジェクト グループの送信元名または宛先名を指定します。
any	任意の送信元ホストまたは宛先ホストを *source-addr* または *destination-addr* の値 および *source-wildcard*、または *destination-wildcard* の値 0.0.0.0 255.255.255.255 の省略形として指定します。

host *addr*	シングルホストの送信元アドレスまたは宛先アドレスを指定します。
host *name*	シングルホストの送信元名または宛先名を指定します。
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。
object-group *source-addr-group-name*	送信元アドレス グループ名を指定します。
destination-addr	10 進表記の 4 つの部分をドットで区切った 32 ビット量のパケットの送信先ネットワークまたはホストの番号。
destination-wildcard	10 進表記の 4 つの部分をドットで区切った 32 ビット量の宛先元に適用するワイルドカードビット。 無視するビット位置に 1 を入れます。
eq *port*	指定のポート番号のパケットだけを照合します。有効値については「使用上のガイドライン」の項を参照してください。
gt *port*	より大きいポート番号のパケットだけを照合します。有効値については「使用上のガイドライン」の項を参照してください。
lt *port*	より小さいポート番号のパケットだけを照合します。有効値については「使用上のガイドライン」の項を参照してください。
neq *port*	指定のポート番号以外のパケットだけを照合します。有効値については「使用上のガイドライン」の項を参照してください。
portgroup *srcport-group-name*	送信元ポート オブジェクト グループ名を指定します。
object-group *dest-addr-group-name*	宛先アドレス グループ名を指定します。
portgroup *destport-group-name*	宛先ポート オブジェクト グループ名を指定します。

dscp *type*	（任意）指定の DiffServ コード ポイント（DSCP）値とパケットを照合します。有効値については「使用上のガイドライン」の項を参照してください。
fragments	（任意）アクセス リスト エントリをパケットの先頭以外のフラグメントに適用します。フラグメントはそれに従って許可または拒否されます。 **fragment** キーワードの詳細については、「使用上のガイドライン」の「フラグメントのアクセス リスト処理」の項および「deny, （2 ページ）」の項を参照してください。
option *option*	（任意）指定の IP オプション値数とパケットを照合します。有効値については「使用上のガイドライン」の項を参照してください。
precedence *precedence*	（任意）パケットの優先順位のフィルタリング レベルを指定します。有効な値は 0 ～ 7 の数値、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。

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。（コンソールにロギングするメッセージのレベルは、**logging console** コマンドで制御します）。 標準リスト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または拒否されたか、送信元アドレス、およびパケット数があります。 拡張リスト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。 標準リストおよび拡張リストの両方の場合で、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、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。 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。 この動作によって、ロギング パケットが多すぎてルータがリロードすることを回避します。 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-input	（任意）入力インターフェイスを含むこのエントリにログを照合します。
time-range *time-range-name*	（任意）時間範囲のエントリ名を指定します。
tos *tos*	（任意）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 の数値、または **access-list**（IP 拡張）コマンドの「使用上のガイドライン」の項に記載されている名前です。

option option	（任意）IP オプション値とパケットを照合します。有効値については「使用上のガイドライン」の項を参照してください。
fragments	（任意）アクセス リスト エントリをパケットの先頭以外のフラグメントに適用します。フラグメントはそれに従って許可または拒否されます。 **fragment** キーワードの詳細については、「使用上のガイドライン」の「deny, （2 ページ）」の項および「deny, （2 ページ）」の項を参照してください。
ttl *ttl-value*	（任意）指定の存続可能時間（ttl）値とパケットを照合します。

コマンド デフォルト

パケットがアクセス リストの通過を拒否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。

使用上のガイドライン

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には、**ip access-list** コマンドに続いてこのコマンドを使用します。

portgroup キーワードは、拡張 ACL を設定する場合にだけ表示されます。

address 値、または *object-group-name* 値は、**object-group** コマンドを使用して作成されます。

object-group *object-group-name* キーワードおよび引数を使用すると、ACL を使用するアクセス ポリシーの定義に使用できるユーザ（またはサーバ）の論理グループを作成できます。 たとえば、1 つの ACL エントリを使用して、engineering という名前のオブジェクト グループに、すべてのエンジニアリング サーバへのアクセスを許可できます。 論理グループを使用しない場合は、エンジニアリング グループの各ユーザに ACL エントリが 1 つずつ必要です。

演算子を *source-addr*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-addr* 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。

TCP または UDP ポート番号を入力する場合、TCP または UDP ポートの 10 進数または名前を入力できます。 ポート番号の範囲は 0 ～ 65535 です。 TCP および UDP ポート名は、**access-list**（IP 拡張）コマンドの「使用上のガイドライン」の項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。

dscp *type* キーワードおよび引数の有効値は、次のとおりです。

- 0 ～ 63：DiffServ コード ポイント（DSCP）値。
- **af11**：AF11 dscp（001010）とパケットを照合します。
- **af12**：AF12 dscp（001100）とパケットを照合します。
- **af13**：AF13 dscp（001110）とパケットを照合します。
- **af21**：AF21 dscp（010010）とパケットを照合します。
- **af22**：AF22 dscp（010100）とパケットを照合します。
- **af23**：AF23 dscp（010110）とパケットを照合します。
- **af31**：AF31 dscp（011010）とパケットを照合します。
- **af32**：AF32 dscp（011100）とパケットを照合します。
- **af33**：AF33 dscp（011110）とパケットを照合します。
- **af41**：AF41 dscp（100010）とパケットを照合します。
- **af42**：AF42 dscp（100100）とパケットを照合します。
- **af43**：AF43 dscp（100110）とパケットを照合します。
- **cs1**：CS1（優先順位 1）dscp（001000）とパケットを照合します。
- **cs2**：CS2（優先順位 2）dscp（010000）とパケットを照合します。
- **cs3**：CS3（優先順位 3）dscp（011000）とパケットを照合します。
- **cs4**：CS4（優先順位 4）dscp（100000）とパケットを照合します。
- **cs5**：CS5（優先順位 5）dscp（101000）とパケットを照合します。
- **cs6**：CS6（優先順位 6）dscp（110000）とパケットを照合します。
- **cs7**：CS7（優先順位 7）dscp（111000）とパケットを照合します。
- **default**：デフォルトの dscp（000000）とパケットを照合します。
- **ef**：EF dscp（101110）とパケットを照合します。

eq *port* キーワードおよび引数の有効な値は次のとおりです。

- 0 ～ 65535：ポート番号。

- **bgp**：ボーダー ゲートウェイ プロトコル（179）。
- **chargen**：Character ジェネレータ（19）。
- **cmd**：リモート コマンド（rcmd、514）。
- **daytime**：Daytime（13）。
- **discard**：Discard（9）。
- **domain**：ドメイン ネーム サービス（53）。
- **echo**：Echo（7）。
- **exec**：Exec（rsh、512）。
- **finger**：Finger（79）。
- **ftp**：ファイル転送プロトコル（21）。
- **ftp-data**：FTP データ接続（20）。
- **gopher**：Gopher（70）。
- **hostname**：NIC ホストネーム サーバ（101）。
- **ident**：Ident Protocol（113）。
- **irc**：インターネット リレー チャット（194）。
- **klogin**：Kerberos ログイン（543）。
- **kshell**：Kerberos シェル（544）。
- **login**：ログイン（rlogin、513）。
- **lpd**：プリンタ サービス（515）。
- **nntp**：Network News Transport Protocol（119）。
- **pim-auto-rp**：PIM Auto-RP（496）。
- **pop2**：Post Office Protocol v2（109）。
- **pop3**：Post Office Protocol v3（110）。
- **smtp**：Simple Mail Transfer Protocol（25）。
- **sunrpc**：Sun Remote Procedure Call（111）。
- **syslog**：Syslog（514）。
- **tacacs**：TAC Access Control System（49）。
- **talk**：Talk（517）。
- **telnet**：Telnet（23）。
- **time**：Time（37）。
- **uucp**：UNIX 間コピー プログラム（540）。

- **whois**：Nicname（43）。
- **www**：World Wide Web（HTTP、80）。

gt *port* キーワードおよび引数の有効な値は次のとおりです。

- 0 ～ 65535：ポート番号。
- **biff**：Biff（メール通知、comsat、512）。
- **bootpc**：ブートストラップ プロトコル（BOOTP）クライアント（68）。
- **bootps**：ブートストラップ プロトコル（BOOTP）サーバ（67）。
- **discard**：Discard（9）。
- **dnsix**：DNSIX セキュリティ プロトコル監査（195）。
- **domain**：ドメイン ネーム サービス（DNS、53）。
- **echo**：Echo（7）。
- **isakmp**：Internet Security Association および Key Management Protocol（500）。
- **mobile-ip**：モバイル IP 登録（434）。
- **nameserver**：IEN116 ネーム サービス（廃止、42）。
- **netbios-dgm**：NetBIOS データグラム サービス（138）。
- **netbios-ns**：NetBIOS ネーム サービス（137）。
- **netbios-ss**：NetBIOS セッション サービス（139）。
- **non500-isakmp**：Internet Security Association および Key Management Protocol（4500）。
- **ntp**：ネットワーク タイム プロトコル（123）。
- **pim-auto-rp**：PIM Auto-RP（496）。
- **rip**：ルーティング情報プロトコル（ルータ、in.routed、520）。
- **snmp**：簡易ネットワーク管理プロトコル（161）。
- **snmptrap**：SNMP トラップ（162）。
- sunrpc：Sun Remote Procedure Call（111）。
- **syslog**：System Logger（514）。
- **tacacs**：TAC Access Control System（49）。
- **talk**：Talk（517）。
- **tftp**：Trivial File Transfer Protocol（69）。
- **time**：Time（37）。
- **who**：Who サービス（rwho、513）。

- **xdmcp**：X Display Manager Control Protocol（177）。

lt *port* キーワードおよび引数の有効な値は次のとおりです。

- 0 ～ 65535：ポート番号。
- **biff**：Biff（メール通知、comsat、512）。
- **bootpc**：ブートストラップ プロトコル（BOOTP）クライアント（68）。
- **bootps**：ブートストラップ プロトコル（BOOTP）サーバ（67）。
- **discard**：Discard（9）。
- **dnsix**：DNSIX セキュリティ プロトコル監査（195）。
- **domain**：ドメイン ネーム サービス（DNS、53）。
- **echo**：Echo（7）。
- **isakmp**：Internet Security Association および Key Management Protocol（500）。
- **mobile-ip**：モバイル IP 登録（434）。
- **nameserver**：IEN116 ネーム サービス（廃止、42）。
- **netbios-dgm**：NetBIOS データグラム サービス（138）。
- **netbios-ns**：NetBIOS ネーム サービス（137）。
- **netbios-ss**：NetBIOS セッション サービス（139）。
- **non500-isakmp**：Internet Security Association および Key Management Protocol（4500）。
- **ntp**：ネットワーク タイム プロトコル（123）。
- **pim-auto-rp**：PIM Auto-RP（496）。
- **rip**：ルーティング情報プロトコル（ルータ、in.routed、520）。
- **snmp**：簡易ネットワーク管理プロトコル（161）。
- **snmptrap**：SNMP トラップ（162）。
- **sunrpc**：Sun Remote Procedure Call（111）。
- **syslog**：System Logger（514）。
- **tacacs**：TAC Access Control System（49）。
- **talk**：Talk（517）。
- **tftp**：Trivial File Transfer Protocol（69）。
- **time**：Time（37）。
- **who**：Who サービス（rwho、513）。
- **xdmcp**：X Display Manager Control Protocol（177）。

neg *port* キーワードおよび引数の有効な値は次のとおりです。

- 0 ～ 65535：ポート番号。
- **biff**：Biff（メール通知、comsat、512）。
- **bootpc**：ブートストラップ プロトコル（BOOTP）クライアント（68）。
- **bootps**：ブートストラップ プロトコル（BOOTP）サーバ（67）。
- **discard**：Discard（9）。
- **dnsix**：DNSIX セキュリティ プロトコル監査（195）。
- **domain**：ドメイン ネーム サービス（DNS、53）。
- **echo**：Echo（7）。
- **isakmp**：Internet Security Association および Key Management Protocol（500）。
- **mobile-ip**：モバイル IP 登録（434）。
- **nameserver**：IEN116 ネーム サービス（廃止、42）。
- **netbios-dgm**：NetBIOS データグラム サービス（138）。
- **netbios-ns**：NetBIOS ネーム サービス（137）。
- **netbios-ss**：NetBIOS セッション サービス（139）。
- **non500-isakmp**：Internet Security Association および Key Management Protocol（4500）。
- **ntp**：ネットワーク タイム プロトコル（123）。
- **pim-auto-rp**：PIM Auto-RP（496）。
- **rip**：ルーティング情報プロトコル（ルータ、in.routed、520）。
- **snmp**：簡易ネットワーク管理プロトコル（161）。
- **snmptrap**：SNMP トラップ（162）。
- **sunrpc**：Sun Remote Procedure Call（111）。
- **syslog**：System Logger（514）。
- **tacacs**：TAC Access Control System（49）。
- **talk**：Talk（517）。
- **tftp**：Trivial File Transfer Protocol（69）。
- **time**：Time（37）。
- **who**：Who サービス（rwho、513）。
- **xdmcp**：X Display Manager Control Protocol（177）。

option *option* キーワードおよび引数の有効値は、次のとおりです。

- 0 ～ 255：IP オプション値。
- **add-ext**：Address Extension Option（147）とパケットを照合します。
- **any-options**：ANY Option とパケットを照合します。
- **com-security**：Commercial Security Option（134）とパケットを照合します。
- **dps**：Dynamic Packet State Option（151）とパケットを照合します。
- **encode**：Encode Option（15）とパケットを照合します。
- **eool**：End of Options（0）とパケットを照合します。
- **ext-ip**：Extended IP Option（145）とパケットを照合します。
- **ext-security**：Extended Security Option（133）とパケットを照合します。
- **finn**：Experimental Flow Control Option（205）とパケットを照合します。
  - **imitd**：IMI Traffic Desriptor Option（144）とパケットを照合します。
  - **lsr**：Loose Source Route Option（131）とパケットを照合します。
  - **match-all**：指定されたすべてのフラグを持つかどうかパケットを照合します。
  - **match-any**：指定されたいずれかのフラグを持つかどうかパケットを照合します。
  - **mtup**：MTU Probe Option（11）とパケットを照合します。
  - **mtur**：MTU Reply Option（12）とパケットを照合します。
  - **no-op**：No Operation Option（1）とパケットを照合します。
  - **psh**：PSH ビットについてパケットを照合します。
  - **nsapa**：NSAP Addresses Option（150）とパケットを照合します。
  - **reflect**：再帰アクセス リスト エントリを作成します。
  - **record-route**：Record Route Option（7）パケットを照合します。
  - **rst**：RST ビットについてパケットを照合します。
  - **router-alert**：Router Alert Option（148）とパケットを照合します。
  - **sdb**：Selective Directed Broadcast Option（149）とパケットを照合します。
  - **security**：Basic Security Option（130）とパケットを照合します。
  - **ssr**：Strict Source Routing Option（137）とパケットを照合します。
  - **stream-id**：Stream ID Option（136）とパケットを照合します。
  - **syn**：SYN ビットについてパケットを照合します。
- **timestamp**：Time Stamp Option（68）とパケットを照合します。
- **traceroute**：Trace Route Option（82）とパケットを照合します。

- **ump**：Upstream Multicast Packet Option（152）とパケットを照合します。
- **visa**：Experimental Access Control Option（142）とパケットを照合します。
- **zsu**：Experimental Measurement Option（10）とパケットを照合します。

tos *value* キーワードおよび引数の有効値は、次のとおりです。

- 0 ～ 15：タイプ オブ サービス値。
- **max-reliability**：最大信頼性 ToS（2）とパケットを照合します。
- **max-throughputy**：最大スループット ToS（4）とパケットを照合します。
- **min-delay**：最小遅延 ToS（8）とパケットを照合します。
- **min-monetary-cost**：最小金銭コスト ToS（1）とパケットを照合します。
- **normal**：通常 ToS（0）とパケットを照合します。

フラグメントのアクセス リストまたは OGACL 処理

fragments キーワードを指定するかどうかによるアクセス リスト エントリの動作は、次の表のようにまとめることができます。

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ず（デフォルト動作）、すべてのアクセス リスト エントリ情報が一致する	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は許可されます。
	  • エントリが **deny** ステートメントの場合は、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する	（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 **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** キーワードを単純に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 **fragments** キーワードが含まれているアクセス リスト **permit** エントリまたは **deny** エントリとは一致せず、パケットは次のアクセス リスト エントリと比較されます。この比較は、**fragments** キーワードが含まれていないアクセス リスト エントリによってパケットが許可または拒否されるまで続きます。 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** エントリには **fragments** キーワードは含まれ、以降のフラグメントに適用されます。 同じホストに複数の **deny** アクセス リスト エントリがあり、それぞれのレイヤ 4 ポートが異なる場合、そのホストに追加する必要があるのは、**fragments** キーワードを指定した **deny** アクセス リスト エントリ 1 つだけです。 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。

フラグメントとポリシー ルーティング

ポリシー ルーティングが **match ip address** 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。

portgroup *srcport-groupname* または **portgroup** *destport-groupname*のキーワードおよび引数を使用して、送信元または宛先グループに基づくオブジェクト グループを作成できます。

例

次に、すべての TCP パケットを拒否するアクセス リストを作成する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended my_ogacl_policy
Router(config-ext-nacl)# deny tcp any any
Router(config-ext-nacl)# exit
Router(config)# exit
```

関連コマンド

コマンド	説明
ip access-group	インターフェイスまたはサービス ポリシーマップに ACL または OGACL を適用します。
ip access-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。
object-group network	OGACL で使用するネットワーク オブジェクト グループを定義します。
object-group service	OGACL で使用するサービス オブジェクト グループを定義します。
permit	名前付き IP アクセス リストまたは OGACL において、パケットを許可する条件を設定します。
show ip access-list	IP アクセス リストまたは OGACL の内容を表示します。
show object-group	設定されているオブジェクト グループに関する情報を表示します。

deny（IP）

名前付き IP アクセス リストに条件を適用するには、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。 アクセス リストから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** *source* [*source-wildcard*]

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

no *sequence-number*

no deny *source* [*source-wildcard*]

no deny *protocol source source-wildcard destination destination-wildcard*

Internet Control Message Protocol (ICMP)

[*sequence-number*] **deny icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*]| *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] **[log]** [**time-range** *time-range-name*] **[fragments]**

Internet Group Management Protocol (IGMP)

[*sequence-number*] **deny igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] **[log]** [**time-range** *time-range-name*] **[fragments]**

Transmission Control Protocol (TCP)

[sequence-number] deny tcp *source source-wildcard* [*operator port* [*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**]

User Datagram Protocol (UDP)

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

構文の説明

sequence-number	（任意）deny ステートメントに割り当てられたシーケンス番号。 シーケンス番号に基づいて、システムがアクセス リストの番号付きの位置にステートメントを挿入します。

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、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* を *source* および *source-wildcard* の値 *source* 0.0.0.0 の省略形として使用する。
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は1を設定します。 • **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* を *source* および *source-wildcard* の値 *source* 0.0.0.0 の省略形として使用する。
protocol	インターネットプロトコルの名前または番号。*protocol*引数は、**eigrp**、**gre**、**icmp**、**igmp**、**ip**、**ipinip**、**nos**、**ospf**、**tcp**、または**udp**、キーワードのいずれか、または、インターネット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（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。 （注） **icmp**、**igmp**、**tcp**、および **udp** キーワードを入力する場合は、**deny** コマンドの ICMP、IGMP、TCP、および UDP 形式に示される固有のコマンド構文に従う必要があります。

icmp	ICMP パケットのみを拒否します。 **icmp** キーワードを入力する場合、**deny** コマンドの ICMP 形式に示される固有のコマンド構文を使用する必要があります。
igmp	IGMP パケットのみを拒否します。 **igmp** キーワードを入力する場合、**deny** コマンドの IGMP 形式に示される固有のコマンド構文を使用する必要があります。
tcp	TCP パケットのみを拒否します。 **tcp** キーワードを入力する場合、**deny** コマンドの TCP 形式に示される固有のコマンド構文を使用する必要があります。
udp	UDP パケットのみを拒否します。 **udp** キーワードを入力する場合、**deny** コマンドの UDP 形式に示される固有のコマンド構文を使用する必要があります。
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* を *destination* 0.0.0.0 の *destination* および *destination-wildcard* の省略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、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* を *destination* 0.0.0.0 の *destination* および *destination-wildcard* の省略形として使用します。
option *option-name*	（任意）パケットは、0 ～ 255 の番号、または「使用上のガイドライン」の項の表に記載された、対応する IP オプション名によって指定される IP オプションによってフィルタ処理されます。
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。
tos *tos*	（任意）パケットは、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」の項の表に記載された、名前によって指定されるタイプ オブ サービス（ToS）レベルによってフィルタ処理されます。

ttl *operator value*	（任意）この **deny** ステートメントで指定されている TTL 値とパケットの TTL 値を比較します。 • *operator* は、**lt**（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）、または **range**（inclusive range：包含範囲）です。 • *value* の範囲は 0 ～ 255 です。 • 演算子（operator）が**range**の場合は、スペースで区切った 2 つの値を指定します。 • Release 12.0S の場合、演算子が **eq** または **neq** の場合、TTL 値を 1 つしか指定できません。 • その他のリリースの場合、演算子が **eq** または **neq** の場合、スペースで区切って、10 個の TTL 値が指定できます。 パケットの TTL が 10 個の値の 1 個と一致する場合、このエントリは、一致すると見なされます。
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。（コンソールにロギングするメッセージのレベルは、**logging console** コマンドで制御します）。
time-range *time-range-name*	（任意）**deny** ステートメントに適用する時間範囲の名前。 時間範囲の名前と制限事項は、**time-range** コマンドと、**absolute** または **periodic** コマンドによってそれぞれ指定します。
fragments	（任意）アクセス リスト エントリをパケットの先頭以外のフラグメントに適用します。フラグメントはそれに従って許可または拒否されます。 **fragment** キーワードの詳細については、「使用上のガイドライン」の「deny（IP），（17 ページ）」の項および「deny（IP），（17 ページ）」の項を参照してください。

icmp-type	（任意）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	（任意）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	（任意）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 タイプおよびコード名によってフィルタリングできます。 使用可能な名前は**access-list**（IP 拡張）コマンドの「使用上のガイドライン」の項に記載されています。
igmp-type	（任意）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 タイプは、0 ～ 15 の数値です。 IGMP メッセージ名は、**access-list**（IP 拡張）コマンドの「使用上のガイドライン」の項に記載されています。
operator	（任意）送信元ポートまたは宛先ポートを比較します。 演算子（operator）には、**lt**（less than; 未満）、**gt**（greater than; よりも多い）、**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）、**neq**（等しくない）演算子に対して最大 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	（任意）TCP ポートまたは UDP ポートの 10 進数または名前。 ポート番号の範囲は 0 ～ 65535 です。 TCP および UDP ポート名は、**access-list**（IP 拡張）コマンドの「使用上のガイドライン」の項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。 （注） **established** キーワードは、古いコマンドラインインターフェイス（CLI）形式でのみ使用可能です。 新しい CLI 形式を使用するには、**match-any** または **match-all** キーワードの後に、**+** または **-** キーワードと *flag-name* 引数を続けて使用する必要があります。
match-any | **match-all**	（任意）TCP プロトコルの場合にだけ、TCP データグラムに特定のフラグセットがある、またはない場合に一致します。 **match-any** キーワードを使用すると、指定した TCP フラグのいずれかが存在する場合に一致し、**match-all** キーワードを使用すると、指定した TCP フラグのすべてが存在する場合に一致します。 1 つ以上の TCP フラグの照合を行うには、**match-any** および **match-all** キーワードに、**+** または **-** キーワード、および *flag-name* 引数を続ける必要があります。

+|- *flag-name*	（任意）TCP プロトコルの場合にだけ、+ キーワードは、TCP ヘッダーに *flag-name* 引数で指定された TCP フラグが含まれる場合に、IP パケットを受け入れます。 -キーワードは*flag-name* 引数で指定された TCP フラグを含まない IP パケットをフィルタリングします。 + および - キーワードの後に *flag-name* 引数を続ける必要があります。 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次のとおりです。**urg**、**ack**、**psh**、**rst**、**syn**、**fin**。

コマンド デフォルト　パケットが名前付きアクセス リストの通過を拒否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

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。
12.0(11)	**fragments** キーワードが追加されました。
12.2(13)T	igrp キーワードは、IGRP プロトコルが Cisco IOS ソフトウェアで利用できなくなったため、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、および *flag-name* 引数が追加されました。
12.3(7)T	非隣接ポートを使用してアクセス リスト エントリが作成できるように、コマンド機能が変更され、最大 10 個のポート番号が **eq** および **neq** 演算子の後に追加できるようになりました。
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。

リリース	変更内容
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。

使用上のガイドライン

パケットが名前付きアクセス リストを通過できない条件を指定するには、**ip access-list** コマンドに続いてこのコマンドを使用します。

time-range キーワードでは、時間範囲を名前で指定することができます。**time-range**、**absolute**、および **periodic** コマンドは、この **deny** ステートメントが有効になるときを指定します。

log キーワード

ログ 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、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。

（5 分間隔待機する代わりに）一致の数が設定可能なしきい値に達したときにロギング メッセージを生成するには、**ip access-list log-update** コマンドを使用します。詳細については **ip access-list log-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。この動作によって、ロギングパケットが多すぎてルータがクラッシュすることを回避します。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（CEF）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、CEF で交換されたものではありません。これらはファースト交換されたものです。ロギングは、CEF をディセーブルにします。

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 リストは、IP オプションを使用してパケットをフィルタ処理し、IP オプションを含むスプリアスパケットでルータが飽和状態になるのを防ぐために使用できます。現在使用中でないものを含む。すべてのIPオプションの完全な表を参照するには、URL：www.iana.org から、最新のインターネット割り当て番号局（IANA）情報を参照してください。

Cisco IOS ソフトウェアでは、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することで、パケットが正規の IP オプションを 1 つ以上を含んでいるかどうかに応じてパケットをフィルタ処理できます。

表 *2*：*IP* オプションの値と名前

IP オプションの値または名前	説明
0 ～ 255	IP オプション値。
add-ext	Address Extension Option（147）とパケットを照合します。
any-options	任意の IP オプションとパケットを照合します。
com-security	Commercial Security Option（134）とパケットを照合します。
dps	Dynamic Packet State Option（151）とパケットを照合します。
encode	Encode Option（15）とパケットを照合します。
eool	End of Options（0）とパケットを照合します。
ext-ip	Extended IP Options（145）とパケットを照合します。
ext-security	Extended Security Option（133）とパケットを照合します。
finn	Experimental Flow Control Option（205）とパケットを照合します。
imitd	IMI Traffic Descriptor Option（144）とパケットを照合します。
lsr	Loose Source Route Option（131）とパケットを照合します。
mtup	MTU Probe Option（11）とパケットを照合します。
mtur	MTU Reply Option（12）とパケットを照合します。

IP オプションの値または名前	説明
no-op	No Operation Option（1）とパケットを照合します。
nsapa	NSAP Addresses Option（150）とパケットを照合します。
psh	PSH ビットについてパケットを照合します。
record-route	Router Record Route Option（7）とパケットを照合します。
reflect	再帰アクセス リスト エントリを作成します。
rst	RST ビットについてパケットを照合します。
router-alert	Router Alert Option（148）とパケットを照合します。
sdb	Selective Directed Broadcast Option（149）とパケットを照合します。
security	Base Security Option（130）とパケットを照合します。
ssr	Strict Source Routing Option（137）とパケットを照合します。
stream-id	Stream ID Option（136）とパケットを照合します。
syn	SYN ビットについてパケットを照合します。
timestamp	Time Stamp Option（68）とパケットを照合します。

TCP フラグに基づく IP パケットのフィルタリング

アクセス リストを構成するアクセス リスト エントリは、TCP フラグの特定のグループが設定されている、あるいは設定されていないパケットのみを受け入れることで、無許可の TCP パケット検出してドロップするように設定できます。 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。 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マッチングできるように、アクセス リスト エントリを設定できます。 TCP ヘッダー フラグがセットされているかどうかに基づいて一致が決定されることを指定するには、+および-キーワードとフラグ名を使用します。 + または - キーワードと *flag-name* 引数によって指定されたフラ

グのうちのいずれかまたはすべてが、それぞれ、設定されているかまたは設定されていないパケットを許可するには、**match-any** キーワードおよび **match-all** キーワードを使用します。

フラグメントのアクセス リスト処理

fragments キーワードを指定するかどうかによるアクセス 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ず（デフォルト動作）、すべてのアクセス リスト エントリ情報が一致する	レイヤ 3 情報のみを含むアクセス 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、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、非初期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する	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 **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。 初期フラグメントは、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** エントリには **fragments** キーワードは含まれ、以降のフラグメントに適用されます。 同じホストに複数の **deny** アクセス リスト エントリがあり、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。

フラグメントとポリシー ルーティング

ポリシー ルーティングが **match ip address** 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。

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。

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 Release 12.3(7)T 以降のリリースでは、同じアクセス コントロール エントリで非隣接ポートを指定できます。これによって、同じ送信元アドレス、宛先アドレス、およびプロトコルに必要なアクセス リスト エントリを大幅に減らすことができます。 多数のアクセス リスト エントリを維持する場合は、非隣接ポートを使用して、可能な限りそれらを統合することを推奨します。**eq** および **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 リストに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、月曜日から金曜日までの午前 8:00 から午後 6:00 の HTTP トラフィックが拒否される例を示します。

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
ip access-list extended strict
 deny tcp any any eq http time-range no-http
!
interface ethernet 0
 ip access-group strict in
```

次に、シーケンス番号 25 を持つエントリを拡張 IP アクセス リスト 150 に追加する例を示します。

```
ip access-list extended 150
 25 deny ip host 172.16.3.3 host 192.168.5.34
```

次に、上で示した拡張アクセス リストの例から、シーケンス番号 25 でエントリを削除する例を示します。

```
 no 25
```

次に、filter2 という拡張アクセス リストに拒否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、パケットに IP オプションの ssr 値で表される Strict Source Routing IP Option が含まれる場合、パケットが名前付きアクセス リストを通過できないように指定します。

```
ip access-list extended filter2
 deny ip any any option ssr
```

次に、kmdfilter1 という拡張アクセス リストに拒否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 および FIN TCP フラグがそのパケットに設定されている場合、パケットが名前付きアクセス リストを通過できないように指定します。

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

次に、非隣接ポートを使用して 1 つのアクセス リスト エントリに統合できる複数の **deny** ステートメントの例を示します。 **show access-lists** コマンドは、abc というアクセス リストについて、アクセス リスト エントリ グループを表示するために入力されます。

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

エントリはすべて同じ **deny** 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 abc
 no 10
 no 20
 no 30
 no 40
 deny tcp any eq telnet ftp any eq 450 679
```

次の例では、統合されたアクセス リスト エントリを作成します。

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

次のアクセス リストでは、TTL 値が 10 および 20 であるタイプ オブ サービス（ToS）レベル 3 を含む IP パケットをフィルタ処理します。 また、TTL が 154 より大きい IP パケットをフィルタ処理し、非初期フラグメントにそのルールを適用します。 フラッシュの優先レベルを持ち、TTL が 1 ではない IP パケットを許可し、その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。 その他のパケットはすべて拒否されます。

```
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
```

関連コマンド

コマンド	説明
absolute	時間範囲が有効なときの絶対時間を指定します。
access-list（IP 拡張）	拡張 IP アクセス リストを定義します。
access-list（IP 標準）	標準 IP アクセス リストを定義します。
ip access-group	インターフェイスへのアクセスを制御します。
ip access-list	IP アクセス リストを名前で定義します。
ip access-list log-update	ロギング メッセージを生成するパケット数のしきい値を設定します。
ip access-list resequence	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。
ip options	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。
logging console	システム ロギング（syslog）メッセージをすべての使用可能な TTY 回線に送信し、重大度に基づいてメッセージを制限する。
match ip address	標準または拡張アクセス リストに許可された宛先ネットワーク番号アドレスを持つルートを配信し、パケットのポリシー ルーティングを実行します。

コマンド	説明
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。
permit（IP）	パケットが名前付き IP アクセス リストを通過する条件を設定します。
remark	名前付き IP アクセス リスト中のエントリに有益なコメント（注釈）を作成します。
show access-lists	アクセスリストエントリのグループを表示します。
show ip access-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、または他の機能が有効となる時間を指定します。

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。

deny *protocol* {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] **[undetermined-transport]**

no deny *protocol* {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] **[undetermined-transport]**

Internet Control Message Protocol

deny icmp {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*]| *icmp-message*] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol

deny tcp {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] **[ack]** [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] **[established] [fin]** [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] [**neq** {*port*| *protocol*}] **[psh]** [**range** {*port*| *protocol*}] **[routing]** [**routing-type** *routing-number*] **[rst]** [**sequence** *value*] **[syn]** [**time-range** *name*] **[urg]**

User Datagram Protocol

deny udp {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] [**neq** {*port*| *protocol*}] [**range** {*port*| *protocol*}] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

構文の説明

protocol	インターネットプロトコルの名前または番号。これは、キーワード **ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**sctp**、**tcp**、**udp**、または **hbh** にするか、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*	拒否条件を設定する送信元 IPv6 ホスト アドレス。 この *source-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。

operator [*port-number*]	（任意）指定のプロトコルの送信元または宛先ポートを比較するオペランドを指定します。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-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。 任意の *port-number* 引数は 10 進数、または TCP あるいは UDP ポートの名前です。 ポート番号の範囲は 0 ～ 65535 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*	拒否条件を設定する宛先 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。
host *destination-ipv6-address*	拒否条件を設定する宛先 IPv6 ホストアドレス。 この *destination-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
auth	トラフィックを、任意のプロトコルと組み合わせた認証ヘッダーの存在に対して照合させることができます。
dest-option-type	（任意）IPv6 パケットを、各 IPv6 パケットヘッダー内のホップバイホップオプション拡張ヘッダーに照合します。

doh-number	（任意）IPv6宛先オプション拡張ヘッダーを表す、0 から 255 の範囲の任意の整数。
doh-type	（任意）宛先オプション ヘッダー タイプ。 可能な宛先オプション ヘッダー タイプ。それに対応する*doh-number*値は、home-address：201 です。
dscp *value*	（任意）各IPv6パケットヘッダーのトラフィック クラス フィールドのトラフィック クラス値と DiffServ コード ポイント値を照合します。指定できる範囲は 0 ～ 63 です。
flow-label *value*	（任意）各 IPv6 パケット ヘッダーのフロー ラベル フィールドのフロー ラベル値とフロー ラベル値を照合します。 指定できる範囲は 0 ～ 1048575 です。
fragments	（任意）フラグメント拡張ヘッダーに 0 以外のフラグメント オフセットが含まれる場合、非初期フラグメント パケットを照合します。**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。
hbh	（任意）ホップバイホップ オプション ヘッダーを指定します。
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。（コンソールにロギングす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。

mobility	（任意）拡張ヘッダーのタイプ。ヘッダー内の mobility-header-type フィールドの値に関係なく、モビリティ ヘッダーを含むすべての IPv6 パケットの照合を可能にします。
mobility-type	（任意）モビリティ ヘッダーのタイプ。 このキーワードとともに、*mh-number* 引数、または *mh-type* 引数のいずれかを使用する必要があります。
mh-number	（任意）IPv6 モビリティ ヘッダー タイプを表す、0 から 255 の範囲の任意の整数。
mh-type	（任意）モビリティ ヘッダー タイプの名前。可能なモビリティ ヘッダー タイプとそれに対応する *mh-number* 値は、次のとおりです。 • 0：bind-refresh • 1：hoti • 2：coti • 3：hot • 4：cot • 5：bind-update • 6：bind-acknowledgment • 7：bind-error
routing	（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。
routing-type	（任意）タイプ フィールドの値を持つルーティング ヘッダーを個別に照合させることができます。 このキーワードとともに、*routing-number* 引数を使用する必要があります。
routing-number	IPv6 ルーティング ヘッダー タイプを表す、0 から 255 の範囲の任意の整数。 可能なルーティング ヘッダー タイプとそれに対応する *routing-number* 値は、次のとおりです。 • 0：標準 IPv6 ルーティング ヘッダー • 2：モバイル IPv6 ルーティング ヘッダー

sequence *value*	（任意）アクセスリストステートメントのシーケンス番号を指定します。 指定できる範囲は1～4294967295です。
time-range *name*	（任意）拒否ステートメントに適用する時間範囲を指定します。 時間範囲の名前と制限事項は、**time-range** コマンドと、**absolute** または **periodic** コマンドによってそれぞれ指定します。
undetermined-transport	（任意）レイヤ4プロトコルが定義されていない送信元からのパケットを照合します。 **undetermined-transport** 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。
icmp-type	（任意）ICMP パケットのフィルタリングに ICMP メッセージ タイプを指定します。 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。 ICMP メッセージ タイプは、次に示す事前定義された文字列とそれに対応する数値を含む、0 ～ 255 までの数値です。 • 144：dhaad-request • 145：dhaad-reply • 146：mpd-solicitation • 147：mpd-advertisement
icmp-code	（任意）ICMP パケットのフィルタリングに ICMP メッセージ コードを指定します。 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	（任意）ICMP パケットのフィルタリングに ICMP メッセージ名を指定します。 ICMP パケットは、ICMP メッセージ名、または ICMP メッセージタイプおよびコードによってフィルタリングできます。 使用可能な名前については、「使用上のガイドライン」を参照してください。
ack	（任意）TCP プロトコルの場合に限り ACK ビットを設定します。

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、照合が行われます。 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。
fin	（任意）TCP プロトコルの場合に限り、FIN ビットを設定します。送信元からのデータはこれ以上ありません。
neq {*port* | *protocol*}	（任意）指定のポート番号上にないパケットだけを照合します。
psh	（任意）TCP プロトコルの場合に限り、PSH ビットを設定します。
range {*port* | *protocol*}	（任意）ポート番号範囲のパケットだけを照合します。
rst	（任意）TCPプロトコルの場合に限りRST ビットを設定します。
syn	（任意）TCPプロトコルの場合に限りSYN ビットを設定します。
urg	（任意）TCPプロトコルの場合に限りURG ビットを設定します。

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。

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 (config-ipv6-acl)#

コマンド履歴

リリース	変更内容
12.0(23)S	このコマンドが導入されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。

リリース	変更内容
12.4(2)T	*icmp-type* 引数が拡張されました。 **dest-option-type**、**mobility**、**mobility-type**、および **routing-type** キーワードが追加されました。*doh-number*、*doh-type*、*mh-number*、*mh-type*、および *routing-numberr* 引数が追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG 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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 集約シリーズ ルータで追加されました。
12.4(20)T	**auth** キーワードが追加されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
15.2(3)T	このコマンドが変更されました。 **hbh** キーワードのサポートが追加されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

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

パケットがアクセスリストを通過する条件を定義する、または、アクセスリストを再帰アクセスリストとして定義するには、**ipv6 access-list** コマンドの後ろに **deny**（IPv6）コマンドを使用します。

protocol 引数に IPv6 を指定すると、パケットの IPv6 ヘッダーに対して照合を行います。

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**、**remark**、または **evaluate** 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。

Cisco IOS Release 12.2(2)T 以降のリリース、12.0(21)ST、および 12.0(22)S では、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドと **deny** および **permit** キーワードを使用することで、IPv6アクセスコントロールリスト（ACL）が定義され、その拒否条件と許可条件が設

定されます。 Cisco IOS Release 12.0(23)S 以降のリリースでは、IPv6 ACL は、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用することにより定義され、許可条件と拒否条件は、IPv6 アクセス リスト コンフィギュレーション モードで **deny** コマンドおよび **permit** コマンドを使用して設定されます。 IPv6 ACL の定義の詳細については、**ipv6 access-list** コマンドを参照してください。

（注） Cisco IOS Release 12.0(23)S 以降のリリースでは、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）。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。 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。

source-ipv6-prefix/*prefix-length* と *destination-ipv6-prefix*/*prefix-length* の両方の引数をトラフィックのフィルタリングに使用します（送信元プレフィックスはトラフィックの送信元に基づいて、宛先プレフィックスはトラフィックの宛先に基づいてトラフィックをフィルタリングします）。

（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-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。

undetermined-transport 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。

次に、ICMP メッセージの名前のリストを示します。

- beyond-scope
- destination-unreachable
- echo-reply
- echo-request
- header
- hop-limit
- mld-query
- mld-reduction
- mld-report
- nd-na

- nd-ns
- next-header
- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- port-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded
- unreachable

例

次の例では、toCISCO という名の IPv6 アクセス リストを設定し、そのアクセス リストをイーサネット インターフェイス 0 上の発信トラフィックに適用する方法を示します。 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イーサネット インターフェイス 0 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イーサネット インターフェイス 0 から出て行かないようになります。 また、この 2 番めの拒否エントリは、すべての一致をコンソールに表示します。 リスト中の最初の許可エントリは、すべての ICMP パケットがイーサネット インターフェイス 0 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、その他のすべてのトラフィックがイーサネット インターフェイス 0 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。

```
ipv6 access-list toCISCO
 deny tcp any any gt 5000
 deny ::/0 lt 5000 ::/0 log
 permit icmp any any
 permit any any
interface ethernet 0
 ipv6 traffic-filter toCISCO out
```

次の例では、IPsec AH がある場合にも TCP または UDP 解析を許可する方法を示します。

```
IPv6 access list example1
    deny tcp host 2001::1 any log sequence 5
```

```
permit tcp any any auth sequence 10
permit udp any any auth sequence 20
```

関連コマンド

コマンド	説明
ipv6 access-list	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。
ipv6 traffic-filter	インターフェイス上の着信または発信 IPv6 トラフィックをフィルタリングします。
permit（IPv6）	IPv6アクセス リストに許可条件を設定します。
show ipv6 access-list	現在のすべての IPv6 アクセス リストの内容を表示します。

dialer aaa

ダイヤラがダイヤル情報のために認証、許可、アカウンティング（AAA）サーバにアクセスできるようにするには、インターフェイス コンフィギュレーション モードで dialer aaa コマンドを使用します。 この機能をディセーブルにするには、このコマンドの no 形式を使用します。

dialer aaa [**password** *string*| **suffix** *string*]

no dialer aaa [**password** *string*| **suffix** *string*]

構文の説明

password *string*	（任意）認証用のデフォルト以外のパスワードを定義します。 パスワード文字列は最大128文字を使用できます。
suffix *string*	（任意）認証用のサフィックスを定義します。 サフィックス文字列は最大 64 文字を使用できます。

コマンド デフォルト

この機能は、デフォルトでイネーブルではありません。

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
12.0(3)T	このコマンドが導入されました。
12.1(5)T	password、および **suffix** キーワードが追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.(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。

使用上のガイドライン

このコマンドは、大規模のダイヤル アウトおよびレイヤ 2 トンネリング プロトコル（L2TP）ダイヤルアウト機能に必要です。 このコマンドを使用すると、サフィックス、パスワード、またはその両方を指定できます。 パスワードを指定しない場合、デフォルトのパスワードは「cisco」になります。

（注） IP アドレスのみが **dialer aaa suffix**コマンドのユーザ名として指定できます。

例

次の例では、宛先 IP アドレス 10.1.1.1 で、インターフェイス Dialer1 からパケットを送信しているユーザを表示します。 アクセス要求メッセージのユーザ名は、「10.1.1.1@ciscoDoD」で、パスワードは「cisco」です。

```
interface dialer1
 dialer aaa
 dialer aaa suffix @ciscoDoD password cisco
```

関連コマンド

コマンド	説明
accept dialout	L2TP ダイヤル アウト コールをトンネリングする要求を受け入れ、受け入れダイヤル アウト VPDN サブグループを作成します。
dialer congestion-threshold	接続されたリンクの輻輳のしきい値を指定します。
dialer vpdn	ダイヤラ プロファイルまたは DDR ダイヤラが L2TP ダイヤル アウトを使用できるようにします。