Cisco IOS セキュリティ コマンド リファレンス：コマンド D ～ L、Cisco IOS XE Release 3SE（Catalyst 3850 スイッチ）

初版：2013 年 01 月 11 日

最終更新：2013 年 01 月 11 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

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。

domain（AAA）～ dot1x timeout（EtherSwitch）

- dot1x timeout（EtherSwitch）， 102 ページ

domain（AAA）

RADIUS アプリケーションのユーザ名のドメイン オプションを設定するには、動的許可ローカル サーバ コンフィギュレーション モードで **domain** コマンドを使用します。 設定されたユーザ名のドメイン オプション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。

domain {**delimiter** *character*| **stripping [right-to-left]**}

no domain {**delimiter** *character*| **stripping [right-to-left]**}

構文の説明

delimiter *character*	ドメイン デリミタを指定します。 **@**、**/**、**$**、**%**、****、**#**、または **-** のいずれかのオプションを指定できます。
stripping	**@** ドメイン デリミタの左側にある名前と着信ユーザ名を比較します。
right-to-left	右から左方向に見て最初のデリミタで文字列を終了します。

コマンド デフォルト

ユーザ名のドメイン オプションは設定されていません。

コマンド モード

動的許可ローカル 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(31)SB14	このコマンドが導入されました。
12.2(33)SRC5	このコマンドが、Cisco IOS Release 12.2(33)SRC5 に統合されました。
Cisco IOS XE Release 2.3	このコマンドが変更されました。 このコマンドが ASR 1000 シリーズ ルータに実装されました。
15.1(2)T	このコマンドが Cisco IOS Release 15.1(2)T に統合されました。 このコマンドも変更されました。 **right-to-left** キーワードが追加されました。

使用上のガイドライン

ドメイン ストリッピングが設定されていない場合は、パケット オブ ディスコネクト（POD）のメッセージの認証、許可、およびアカウンティング（AAA）で提供される完全なユーザ名がオンライン加入者と比較されます。 ドメイン ストリッピングを設定すると、**@** ドメイン デリミタの前にあるユーザ名のみを使用した接続解除メッセージを送信できます。 ネットワーク アクセス サーバ（NAS）は、このユーザ名を潜在的なドメインを持つ任意のオンライン加入者と比較および照合します。

たとえば、ドメイン ストリッピングが設定されている場合に、ユーザ名「test」を使用した POD メッセージを送信すると、POD メッセージとオンライン加入者間の比較が実行され、ユーザ名「test@cisco.com」または「test」を使用した加入者が、指定されたユーザ名「test」と照合されます。

例

次の設定例を使用して、ユーザ名を右から左に向かって照合します。 ユーザ名が user1@cisco.com の場合、POD メッセージにより照合されるユーザ名は user1@cisco.com になります。

```
Router# configure terminal
Router(config)# aaa server radius dynamic-author
Router(config-locsvr-da-radius)# domain stripping right-to-left
Router(config-locsvr-da-radius)# domain delimiter @
Router(config-locsvr-da-radius)# end
```

次の設定例を使用して、ユーザ名を左から右に向かって照合します。 ユーザ名が user1@cisco.com の場合、POD メッセージにより照合されるユーザ名は user1 になります。

```
Router# configure terminal
Router(config)# aaa server radius dynamic-author
Router(config-locsvr-da-radius)# domain stripping
Router(config-locsvr-da-radius)# domain delimiter @
Router(config-locsvr-da-radius)# end
```

関連コマンド

コマンド	説明
aaa server radius dynamic-author	AAA サーバとしてデバイスを設定して、外部ポリシー サーバとの相互作用を実行します。

dot1x control-direction

（注） Cisco IOS Release 12.2(33) SXI では有効な **dot1x control-direction** コマンドは、**authentication control-direction** コマンドに置き換えられています。 詳細については、**authentication control-direction** コマンドを参照してください。

IEEE 802.1X が制御するポートを単方向または双方向に変更するには、インターフェイス コンフィギュレーション モードで **dot1x control-direction** コマンドを使用します。 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。

dot1x control-direction {**both**| **in**}

no dot1x control-direction

構文の説明

both	ポートで双方向制御をイネーブルにします。
in	ポートで単方向制御をイネーブルにします。

コマンド デフォルト

ポートは双方向モードに設定されています。

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（config-if）

コマンド履歴

リリース	変更内容
12.2(25)SEC	このコマンドが導入されました。
12.4(6)T	このコマンドが、Cisco IOS Release 12.4(6)T に統合されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型スイッチ（ISR）専用の Cisco IOS Release 12.4(4)XC 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。
12.2(33)SXI	このコマンドは、**authentication control-direction** コマンドに置き換えられました。

使用上のガイドライン

IEEE 802.1x 標準では、許可されていないデバイスが一般的にアクセス可能なポートを介して LAN に接続することを制限する、クライアント/サーバベースのアクセス コントロールと認証プロトコルが定義されています。 802.1x は、ポートごとに 2 つの個別の仮想アクセス ポイントを作成してネットワーク アクセスを制御します。 一方のアクセス ポイントが未制御ポート、もう一方は制御ポートです。単一のポートを通過するすべてのトラフィックは、両方のアクセス ポイントを利用できます。 802.1x は、スイッチまたは LAN が提供するサービスを利用できるようにする前に、スイッチのポートに接続されている各ユーザ デバイスを認証し、そのポートを VLAN（仮想 LAN）に割り当てます。 802.1x アクセス制御では、デバイスが認証されるまで、そのデバイスが接続されているポートを通過する Extensible Authentication Protocol over LAN（EAPOL）トラフィックのみが許可されます。 認証に成功すると、通常のトラフィックはポートを通過できるようになります。

単方向ステート

dot1x control-direction in インターフェイス コンフィギュレーション コマンドを使用してポートを単一方向に設定すると、そのポートはスパニングツリー フォワーディング ステートに移行します。

単方向制御ポートをイネーブルにすると、接続ホストはスリープ モードまたは電源切断状態になります。 ホストはそのネットワークの他の装置とトラフィックを交換しません。 単方向ポートに接続されているホストはトラフィックをネットワークに送信できず、ホストはネットワークの他の装置からのトラフィックだけを受信します。

双方向ステート

dot1x control-direction both インターフェイス コンフィギュレーション コマンドを使用してポートを双方向に設定すると、ポートは両方向のアクセスを制御します。 この状態では、スイッチ ポートは EAPOL パケットだけを受信または送信し、他のパケットはすべてドロップされます。

both キーワードを使用するか、またはこのコマンドの **no** 形式を使用すると、ポートはデフォルト設定の双方向モードに変更されます。

Catalyst 6500 シリーズ スイッチ

ポートを双方向に設定すると、Wake-on-LAN（WoL）による 802.1X 認証がイネーブルになります。

Cisco IOS Release 12.4(4)XC

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチ ポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。 ただし、コマンドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

例

次の例では、単方向制御をイネーブルにする方法を示します。

```
Switch(config-if)# dot1x control-direction in
```

次に、双方向制御をイネーブルにする方法を示します。

```
Switch(config-if)# dot1x control-direction both
```

または

```
Switch(config-if)# no dot1x control-direction
```

設定を確認するには、show dot1x all 特権 EXEC コマンドを入力します。 show dot1x all コマンド出力は、ポート名とポートのステートを除き、すべてのデバイスで同一です。 ホストがポートに接続されていてまだ認証されていない場合、次のように表示されます。

```
Supplicant MAC 0002.b39a.9275
AuthSM State = CONNECTING
BendSM State = IDLE
PortStatus = UNAUTHORIZED
```

dot1x control-direction in コマンドを入力して単方向制御をイネーブルにする場合、show dot1x all コマンド出力では次のように表示されます。

```
ControlDirection = In
```

dot1x control-direction in コマンドを入力しても、設定の競合によりポートでこのモードをサポートできない場合、show dot1x all コマンド出力では次のように表示されます。

```
ControlDirection = In (Disabled due to port settings):
```

次に、グローバル 802.1X パラメータをリセットする例を示します。

```
Switch(config)# dot1x default
```

例

次に、WoL を使った 802.1X 認証をイネーブルにし、ポートを双方向に設定する例を示します。

```
Switch(config)# interface gigabitethernet 5/1
Switch(config-if)# dot1x control-direction both
```

例

次に、スイッチ仮想インターフェイスのレイヤ 3 802.1X のサポートの例を示します（Cisco 870 ISR を使用）。

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
 dot1x control-direction in
```

関連コマンド

コマンド	説明
show dot1x	アイデンティティ プロファイルの詳細を表示します。

dot1x credentials

サプリカント設定時の 802.1X クレデンシャル プロファイルを指定する、またはクレデンシャル構造をインターフェイスに適用し、dot1x クレデンシャルのコンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードまたはインターフェイス コンフィギュレーション モードで **dot1x credentials** コマンドを使用します。 クレデンシャル プロファイルを削除するには、このコマンドの **no** 形式を使用します。

dot1x credentials *name*

no dot1x credentials

構文の説明

name	クレデンシャル プロファイルの名前。

コマンド デフォルト

クレデンシャル プロファイルは指定されません。

コマンド モード

グローバル コンフィギュレーションまたはインターフェイス 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
12.4(6)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

802.1Xクレデンシャル構造は、サプリカントを設定する場合に必要です。 このクレデンシャル構造は、ユーザ名、パスワード、および説明を含む場合があります。

例

次に、サプリカントの設定時に使用する必要があるクレデンシャル プロファイルの例を示します。

```
dot1x credentials basic-user
 username router
 password secret
 description This credentials profile should be used for most configured ports
```

dot1x pae supplicant キーワードおよびキーワードとともにクレデンシャル構造をインターフェイスに適用して、そのインターフェイス上でのサプリカント機能をイネーブルにできます。

```
interface fastethernet 0/1
```

```
dot1x credentials basic-user
dot1x pae supplicant
```

関連コマンド

コマンド	説明
anonymous-id (dot1x credential)	クレデンシャルプロファイルに関連付けられた匿名アイデンティティを指定します。
description (dot1x credential)	802.1X クレデンシャル プロファイルの説明を指定します。
password (dot1x credential)	802.1X クレデンシャルプロファイルのパスワードを指定します。
username (dot1x credential)	802.1X クレデンシャル プロファイルのユーザ名を指定します。

dot1x critical（グローバル コンフィギュレーション）

IEEE 802.1X クリティカル認証のパラメータを設定するには、グローバル コンフィギュレーション モードで **dot1x critical** コマンドを使用します。

dot1x critical {**eapol**| **recovery delay** *milliseconds*}

構文の説明

eapol	スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL-Success メッセージを送信するように指定します。
recovery delay *milliseconds*	使用不能になっていた RADIUS サーバが使用可能になったときに、クリティカル ポートを再初期化するためにスイッチが待機するリカバリ遅延時間を指定します。有効な値は 1 ～ 10000 ミリ秒です。

コマンド デフォルト

デフォルト設定は、次のとおりです。

- **eapol**：ディセーブル
- *milliseconds*：1000 ミリ秒

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.2(33)SXH	このコマンドが導入されました。
12.2(33)SXI	**recovery delay** キーワードは、**authentication critical recovery delay** コマンドに置き換えられました。

例

次に、スイッチが正常にクリティカル ポートを認証した場合にスイッチが EAPOL-Success メッセージを送信するよう指定する例を示します。

```
Switch(config)# dot1x critical eapol
```

次の例では、使用不能になっていた RADIUS サーバが使用可能になったときに、クリティカルなポートの再初期化をスイッチが待機するリカバリ遅延期間を設定する方法を示します。

```
Switch(config)# dot1x critical recovery delay 1500
```

関連コマンド

コマンド	説明
dot1x critical（インターフェイス コンフィギュレーション）	インターフェイスで 802.1X クリティカル認証をイネーブルにします。

dot1x critical（インターフェイス コンフィギュレーション）

802.1X クリティカル認証、および任意で 802.1X クリティカル認証リカバリと 802.1X クリティカル認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで **dot1x critical** コマンドを使用します。 802.1X クリティカル認証、および任意で 802.1X クリティカル認証リカバリと 802.1X クリティカル認証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。

dot1x critical [**recovery action reinitialize**]

no dot1x critical [**recovery action reinitialize**]

構文の説明

recovery action reinitialize	（任意）802.1X クリティカル認証リカバリをイネーブルにし、認証サーバが使用可能なときにポートが認証されるように指定します。

コマンド デフォルト

802.1X クリティカル認証はインターフェイス上でイネーブルです。

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（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXH	このコマンドが導入されました。

例

次に、IEEE 802.1X クリティカル認証をインターフェイス上でイネーブルにする例を示します。

```
Router(config-if)# dot1x critical
```

次に、認証サーバが使用可能な場合に 802.1X クリティカル認証リカバリをイネーブルにして、ポートを認証する例を示します。

```
Router(config-if)# dot1x critical recovery action reinitialize
```

次に、IEEE 802.1X クリティカル認証をインターフェイス上でディセーブルにする例を示します。

```
Router(config-if)# no
 dot1x critical
```

関連コマンド

コマンド	説明
dot1x critical（グローバル コンフィギュレーション）	802.1Xクリティカル認証パラメータを設定します。

dot1x default

最新の IEEE 802.1x 標準で指定されたデフォルト値にグローバル 802.1X 認証パラメータをリセットするには、グローバル コンフィギュレーション モードまたはインターフェイス コンフィギュレーション モードで **dot1x default** コマンドを使用します。

dot1x default

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルト値は次のとおりです。

- インターフェイス単位の 802.1X プロトコル イネーブル ステートは、ディセーブルです（強制的に許可）。
- 再認証試行間隔の秒数は、3600 秒です。
- 待機時間は 60 秒です。
- 再伝送時間は 30 秒です。
- 最高再伝送回数は 2 回です。
- 複数ホストのサポートは、ディセーブルです。
- クライアントのタイムアウト時間は 30 秒です。
- 認証サーバのタイムアウト時間は 30 秒です。

コマンド モード

グローバル コンフィギュレーション（config）インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.1(6)EA2	このコマンドが導入されました。
12.2(15)ZJ	このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに追加されました。
12.2(14)SX	このコマンドが Cisco IOS Release 12.2(14) SX の Supervisor Engine 720 に実装されました。

リリース	変更内容
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
12.2(17d)SXB	このコマンドが Cisco IOS Release 12.2(17d)SXB の Supervisor Engine 2 に実装されました。
12.4(6)T	インターフェイス コンフィギュレーションが、このコマンドのコンフィギュレーション モードとして追加されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型ルータ（ISR）専用の Cisco IOS Release 12.4(4)XC に統合されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

IEEE 802.1x 標準では、許可されていないデバイスが一般的にアクセス可能なポートを介して LAN に接続することを制限する、クライアント/サーバベースのアクセス コントロールと認証プロトコルが定義されています。 802.1x は、ポートごとに 2 つの個別の仮想アクセス ポイントを作成してネットワーク アクセスを制御します。 一方のアクセス ポイントが未制御ポート、もう一方は制御ポートです。単一のポートを通過するすべてのトラフィックは、両方のアクセスポイントを利用できます。 802.1x は、スイッチまたは LAN が提供するサービスを利用できるようにする前に、スイッチのポートに接続されている各ユーザデバイスを認証し、そのポートを VLAN（仮想 LAN）に割り当てます。 802.1x アクセス制御では、デバイスが認証されるまで、そのデバイスが接続されているポートを通過する Extensible Authentication Protocol（EAP）over LAN（EAPOL）トラフィックのみが許可されます。 認証に成功すると、通常のトラフィックはポートを通過できるようになります。

現在の 802.1X 設定を確認するには、**show dot1x** コマンドを使用します。

Cisco IOS Release 12.4(4)XC

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。 ただし、コマンドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

例

次に、グローバル 802.1X パラメータをリセットする例を示します。

```
Router(config)# dot1x default
```

次に、FastEthernet インターフェイス 0 のグローバル 802.1X パラメータをリセットする例を示します。

```
Router(config)# interface FastEthernet0
Router(config-if)# dot1x default
```

関連コマンド

コマンド	説明
dot1x critical（グローバル コンフィギュレーション）	802.1X クリティカル認証パラメータを設定します。
dot1x critical（インターフェイス コンフィギュレーション）	インターフェイスで 802.1X クリティカル認証をイネーブルにします。
dot1x max-req	認証プロセスを再開する前に、デバイスが EAP 要求/アイデンティティ フレームを送信する最大回数を設定します（応答を受信しないと仮定）。
dot1x re-authentication（EtherSwitch）	イーサネット スイッチ ネットワーク モジュールのクライアントの定期的な再認証をイネーブルにします。
dot1x timeout（EtherSwitch）	イーサネット スイッチ ネットワーク モジュールの再試行タイムアウトを設定します。
show dot1x	802.1X 情報を表示します。
show dot1x（EtherSwitch）	デバイスまたは指定されたインターフェイスの IEEE 802.1X 統計情報、管理ステータス、および動作ステータスを表示します。

dot1x guest-vlan

アクティブ VLAN を IEEE 802.1x のゲスト VLAN として指定するには、インターフェイス コンフィギュレーション モードで **dot1x guest-vlan** コマンドを使用します。 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。

dot1x guest-vlan vlan-id

no dot1x guest-vlan

構文の説明

vlan-id	アクティブ VLAN を IEEE 802.1x ゲスト VLAN として指定します。 指定できる範囲は1～4094です。

コマンド デフォルト

ゲスト VLAN は設定されません。

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
12.1(14)EA1	このコマンドが導入されました。
12.2(25)SE	このコマンドは、デフォルトのゲスト VLAN の動作を変えるように変更されました。
12.4(11)T	このコマンドが Cisco IOS Release 12.4(11)T 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。
15.3(1)S	このコマンドが、Cisco IOS Release 15.3(1)S に統合されました。

使用上のガイドライン

スタティック アクセス ポートにゲスト VLAN を設定できます。

IEEE 802.1x ポートごとにゲスト VLAN を設定して、現在 IEEE 802.1x 認証を実行していないクライアント（スイッチに接続されているデバイスまたはワークステーション）へのサービスを制限できます。 こうしたユーザは IEEE 802.1x 認証のためにシステムをアップグレードできますが、Windows 98 システムなどのホストでは IEEE 802.1x に対応できません。

IEEE 802.1x ポートでゲスト VLAN をイネーブルにした場合、認証サーバが Extensible Authentication Protocol over LAN（EAPOL）Request/Identity フレームに対する応答を受信しない、あるいは EAPOL パケットがクライアントから送信されないと、ソフトウェアではクライアントをゲスト VLAN に割り当てます。

Cisco IOS Release 12.4(11)T 以降では、スイッチは EAPOL パケット履歴を保持します。 リンクの存続時間内に別の EAPOL パケットがインターフェイス上で検出された場合、ゲスト VLAN 機能はディセーブルになります。 ポートがすでにゲスト VLAN ステートにある場合、ポートは無許可ステートに戻り、認証が再開されます。 EAPOL 履歴はリンクの損失でリセットされます。

スイッチ ポートがゲスト VLAN に移行すると、IEEE 802.1x 非対応クライアントはいくつでもアクセスが許可されます。 IEEE 802.1x 対応クライアントが、ゲスト VLAN を設定しているポートと同じポートに加入すると、ポートは RADIUS 設定 VLAN またはユーザ設定アクセス VLAN では無許可ステートに移行し、認証が再開されます。

ゲスト VLAN は、シングルホスト モードまたはマルチホスト モードの IEEE 802.1x スイッチ ポートでサポートされます。

リモート スイッチド ポート アナライザ（RSPAN）VLAN、音声 VLAN 以外のアクティブなすべての VLAN は、IEEE 802.1x のゲスト VLAN として設定できます。 ゲスト VLAN の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。

DHCP クライアントが接続されている IEEE 802.1x ポートのゲスト VLAN を設定した後、DHCP サーバからホスト IP アドレスを取得する必要があります。 クライアント上の DHCP プロセスが時間切れとなり、DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチ上の IEEE 802.1x 認証プロセスを再起動する設定を変更できます。 **dot1x max-reauth-req** インターフェイス コンフィギュレーション コマンドおよび **dot1x timeout tx-period** インターフェイス コンフィギュレーション コマンドを使用して、IEEE 802.1x 認証プロセスの設定を減らす必要があります。減らす量は、接続される IEEE 802.1x クライアントの種類によって変わります。

例

次の例では、VLAN 5 を IEEE 802.1x ゲスト VLAN として指定する方法を示します。

```
Switch(config-if)# dot1x guest-vlan 5
```

次の例では、スイッチの待機時間を 3 秒に設定し、スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を 15 に設定する方法、および IEEE 802.1x ポートが DHCP クライアントに接続されているときに VLAN 2 を IEEE 802.1x ゲスト VLAN としてイネーブルにする方法を示します。

```
Switch(config-if)# dot1x timeout max-reauth-req 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

show dot1x interface*interface-id* 特権 EXEC コマンドを入力して、デバイスまたは指定したインターフェイスに関する IEEE 802.1x の管理ステータスおよび動作ステータスを表示できます。

関連コマンド

コマンド	説明
dot1x max-reauth-req	スイッチが認証プロセスを再起動する前に、EAP-Request/Identity フレームを再送信する回数を指定します。
dot1x timeout	認証の再試行タイムアウトを設定します。
show dot1x	アイデンティティプロファイルの詳細を表示します。

dot1x guest-vlan supplicant

802.1x 対応サプリカントがゲスト VLAN に移行できるようにするには、グローバル コンフィギュレーション モードで **dot1x guest-vlan supplicant** コマンドを使用します。 802.1x 対応サプリカントがゲスト VLAN に移行できないようにするには、このコマンドの **no** 形式を使用します。

dot1x guest-vlan supplicant

no dot1x guest-vlan supplicant

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

802.1x 対応サプリカントはゲスト VLAN に移行できなくなります。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.2(33)SXH	このコマンドが導入されました。

例

次に、802.1x 対応サプリカントがゲスト VLAN に移行できるようにする例を示します。

```
Router(config)# dot1x guest-vlan supplicant
```

次に、802.1x 対応サプリカントがゲスト VLAN に移行できないようにする例を示します。

```
Router(config)# no dot1x guest-vlan supplicant
```

関連コマンド

コマンド	説明
dot1x critical（グローバル コンフィギュレーション）	802.1X クリティカル認証パラメータを設定します。
dot1x critical（インターフェイス コンフィギュレーション）	インターフェイスで 802.1X クリティカル認証をイネーブルにします。

dot1x initialize

（注） Cisco IOS Release 12.2(33) SXI では有効な **dot1x initialize** コマンドは、**clear authentication session** コマンドに置き換えられています。 詳細については、**clear authentication session** コマンドを参照してください。

すべての 802.1X 対応インターフェイスの 802.1X クライアントを初期化するには、特権 EXEC モードで **dot1x initialize** コマンドを使用します。 このコマンドには、**no** 形式はありません。

dot1x initialize [**interface** *interface-name*]

構文の説明

interface *interface-name*	（任意）初期化するインターフェイスを指定します。このキーワードを入力しない場合、すべてのインターフェイスが初期化されます。

コマンド デフォルト

ステート マシンはイネーブルになりません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(14)EA1	このコマンドが導入されました。
12.3(2)XA	このコマンドが、Cisco IOS Release 12.3(2)XA に統合されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。

使用上のガイドライン

このコマンドは、802.1X ステート マシンを初期化し、新たな認証環境を設定します。 このコマンドを入力した後、ポートの状態は無許可になります。

例

次に、手動でポートを初期化する例を示します。

```
Router# dot1x initialize interface gigabitethernet2/0/2
```

show dot1x [**interface** *interface-name*] コマンドを入力して、無許可ポートのステータスを確認できます。

関連コマンド

コマンド	説明
show dot1x	アイデンティティ プロファイルの詳細を表示します。

dot1x mac-auth-bypass

クライアント MAC アドレスに基づいてスイッチがクライアントを許可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 **dot1x mac-auth-bypass** コマンドを使用します。 MAC 認証バイパス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。

dot1x mac-auth-bypass [eap]

no dot1x mac-auth-bypass

構文の説明

eap	（任意）許可に拡張認証プロトコル（EAP）を使用するようにスイッチを設定します。

コマンド デフォルト

MAC 認証バイパスはディセーブルです。

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（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXH	このコマンドが導入されました。
15.1(4)M	このコマンドが、Cisco IOS Release 15.1(4)M に統合されました。

使用上のガイドライン

（注） MAC 認証バイパスをルーテッド ポートで使用するために、MAC アドレス ラーニングがポートでイネーブルになっていることを確認してください。

MAC 認証バイパス機能が 802.1X ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。 認証サーバには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。 許可が失敗した場合、VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

例

次に、MAC 認証バイパス機能をイネーブルにする例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x mac-auth-bypass
```

次に、認証に EAP を使用するようにスイッチを設定する例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x mac-auth-bypass eap
```

次に、MAC 認証バイパスをディセーブルにする例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)# no dot1x mac-auth-bypass
```

関連コマンド

コマンド	説明
dot1x critical（グローバル コンフィギュレーション）	802.1X クリティカル認証パラメータを設定します。
dot1x critical（インターフェイス コンフィギュレーション）	インターフェイスで 802.1X クリティカル認証をイネーブルにします。

dot1x max-reauth-req

オーセンティケータがクライアントに拡張認証プロトコル（EAP）要求/アイデンティティ フレーム送信する最大回数を設定するには（応答が受信されないと仮定）、インターフェイス コンフィギュレーション モードで **dot1x max-reauth-req** コマンドを使用します。 デフォルト設定の 2 に最大回数を設定するには、このコマンドの **no** 形式を使用します。

dot1x max-reauth-req *number*

no dot1x max-reauth-req

構文の説明

number	最大回数。 範囲は 1 ～ 10 です。 デフォルトは 2 です。

コマンド デフォルト

コマンドのデフォルトは 2 です。

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
12.2(18)SE	このコマンドが導入されました。
12.2(25)SEC	*number* 引数が追加されました。
12.4(6)T	このコマンドが、Cisco IOS Release 12.4(6)T に統合されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型ルータ（ISR）専用の Cisco IOS Release 12.4(4)XC に統合されました。

使用上のガイドライン

このコマンドのデフォルト値の変更は、信頼性のないリンクや特定のクライアントおよび認証サーバの特殊な動作問題など、異常な状況を調整する場合だけ行うようにしてください。

Cisco IOS Release 12.4(4)XC

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。 ただし、コマンドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

設定の確認

show dot1x [interface interface-id] コマンドを入力して、設定を確認できます。

例

次に、無許可ステートに変わる前に認証プロセスが再開される回数を4に設定する例を示します。

```
Router(config-if)# dot1x max-reauth-req 4
```

例

次に、スイッチ仮想インターフェイスのレイヤ 3 802.1X のサポートの例を示します（Cisco 870 ISR を使用）。

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
```

関連コマンド

コマンド	説明
dot1x max-req	認証プロセスを再開する前に、デバイスがEAP要求/アイデンティティ フレームを送信できる最大回数を設定します（応答を受信しないと仮定）。
dot1x timeout tx-period	スイッチが EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。
show dot1x	指定されたポートの IEEE 802.1X の状態を表示します。

dot1x max-req

認証プロセスを再開する前に、ネットワーキング デバイスまたはイーサネット スイッチ ネットワーク モジュールが拡張認証プロトコル（EAP）要求/アイデンティティ フレームを送信できる最大回数を設定するには（応答を受信しないと仮定）、インターフェイス コンフィギュレーション モードまたはグローバル コンフィギュレーション モードで **dot1x max-req** コマンドを使用します。 デフォルト設定の 2 に回数を設定するには、このコマンドの **no** 形式を使用します。

dot1x max-req *retry-number*

no dot1x max-req

構文の説明

retry-number	再試行の最大数。 値は 1 ～ 10 です。 デフォルト値は 2 です。 値は要求 ID を除くすべての EAP パケットに適用できます。

コマンド デフォルト

デフォルトの再試行回数は 2 回です。

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（config）グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.1(6)EA2	このコマンドが Cisco イーサネット スイッチ ネットワーク モジュールに導入されました。
12.2(14)SX	このコマンドが Cisco IOS Release 12.2(14) SX の Supervisor Engine 720 に実装されました。
12.2(15)ZJ	このコマンドが、シスコ イーサネット スイッチ ネットワーク モジュールの Cisco IOS Release 12.2(15) ZJ のプラットフォーム Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズに実装されました。
12.1(11)AX	このコマンドが、Cisco IOS Release 12.1(11)AX に統合されました。
12.1(14)EA1	このコマンドが Cisco IOS Release 12.1(14) EA1 に統合され、コンフィギュレーション モードは EtherSwitch ネットワーク モジュールを除き、インターフェイス コンフィギュレーション モードに変更されました。

リリース	変更内容
12.3(2)XA	このコマンドが Cisco IOS Release 12.3(2) XA に統合され、Cisco 806、Cisco 831、Cisco 836、Cisco 837、Cisco 1701、Cisco 1710、Cisco 1721、Cisco 1751-V、Cisco 1760 のルータ プラットフォームに実装されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合され、Cisco 1751、Cisco 2610XM、Cisco 2611XM、Cisco 2620XM、Cisco 2621XM、Cisco 2650XM、Cisco 2651XM、Cisco 2691、Cisco 3640、Cisco 3640A、Cisco 3660 のルータ プラットフォームに実装されました。
12.2(17d)SXB	このコマンドが Cisco IOS Release 12.2(17d)SXB の Supervisor Engine 2 に実装されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型ルータ（ISR）専用の Cisco IOS Release 12.4(4)XC に統合されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.(33)SXH に統合されました。

使用上のガイドライン

IEEE 802.1x 標準では、許可されていないデバイスが一般的にアクセス可能なポートを介して LAN に接続することを制限する、クライアント/サーバベースのアクセス コントロールと認証プロトコルが定義されています。 802.1x は、ポートごとに 2 つの個別の仮想アクセス ポイントを作成してネットワーク アクセスを制御します。 一方のアクセス ポイントが未制御ポート、もう一方は制御ポートです。 単一のポートを通過するすべてのトラフィックは、両方のアクセス ポイントを利用できます。 802.1x は、スイッチまたは LAN が提供するサービスを利用できるようにする前に、スイッチのポートに接続されている各ユーザ デバイスを認証し、そのポートを VLAN（仮想 LAN）に割り当てます。 802.1x アクセス制御では、デバイスが認証されるまで、そのデバイスが接続されているポートを通過する Extensible Authentication Protocol（EAP）over LAN（EAPOL）トラフィックのみが許可されます。 認証に成功すると、通常のトラフィックはポートを通過できるようになります。

（注） このコマンドのデフォルト値の変更は、信頼性のないリンクや特定のクライアントおよび認証サーバの特殊な動作問題など、異常な状況を調整する場合だけ行うようにしてください。

Cisco IOS Release 12.4(4)XC

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。 ただし、コマンドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

例

次に、ネットワーキング デバイスが EAP 要求/アイデンティティ メッセージをクライアント PC に送信する最大回数が 6 である例を示します。

```
Router(config) configure terminal
Router(config)# interface ethernet 0
Router(config-if)# dot1x max-req 6
```

次に、認証プロセスを再開するまでに、スイッチが EAP 要求/アイデンティティ フレームを送信する回数を 5 に設定する例を示します。

```
Router(config-if)# dot1x max-req 5
```

関連コマンド

コマンド	説明
dot1x port-control	制御ポートの許可ステートの手動制御をイネーブルにします。
dot1x re-authentication	802.1X インターフェイスのクライアント PC の定期的な再認証をグローバルでイネーブルにします。
dot1x reauthentication（EtherSwitch）	802.1Xインターフェイスのイーサネット スイッチ ネットワーク モジュール クライアントの定期的な再認証をイネーブルにします。
dot1x timeout	再試行タイムアウトを設定します。
dot1x timeout（EtherSwitch）	イーサネット スイッチ ネットワーク モジュールの再試行タイムアウトを設定します。
show dot1x	アイデンティティ プロファイルの詳細を表示します。
show dot1x（EtherSwitch）	デバイスまたは指定されたインターフェイスの IEEE 802.1X 統計情報、管理ステータス、および動作ステータスを表示します。

dot1x multiple-hosts

（注） このコマンドは、Cisco IOS Release 12.1(14)EA1 および Release 12.4(6)T で有効な **dot1x host-mode** コマンドに置き換えられました。

dot1x port-control インターフェイス コンフィギュレーション コマンドが **auto** に設定されている 802.1X 許可ポートに、複数のホスト（クライアント）が接続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 **dot1x multiple-hosts** コマンドを使用します。 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。

dot1x multiple-hosts

no dot1x multiple-hosts

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

複数ホストはディセーブルです。

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
12.1(6)EA2	このコマンドが導入されました。
12.2(15)ZJ	このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに追加されました。
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
12.1(14)EA1	このコマンドが Cisco IOS Release 12.1(14) EA1 で **dot1x host-mode** コマンドに置き換えられました。
12.4(6)T	このコマンドが T トレインで **dot1x host-mode** コマンドに置き換えられました。

使用上のガイドライン

このコマンドは、スイッチ ポートに限りサポートされます。

このコマンドにより、1 つの 802.1X 対応ポートに複数のクライアントを接続することができます。 このモードでは、接続されたホストのうち 1 つが認証に成功すれば、すべてのホストがネットワーク アクセスを許可されます。ポートが無許可ステートになった場合（再認証が失敗した場合、または Extensible Authentication Protocol over LAN（EAPOL）-Logoff メッセージを受信した場合）には、接続されたすべてのクライアントがネットワーク アクセスを拒否されます。

interface キーワードと **show dot1x**（EtherSwitch） 特権 EXEC コマンドを使用して、現在の 802.1X の複数ホスト設定を確認します。

例

次に、FastEthernet インターフェイス 0/1 上で 802.1X をイネーブルにし、マルチ ホストを許容する例を示します。

```
Router(config)# interface fastethernet0/1
Router(config-if)# dot1x port-control auto
Router(config-if)# dot1x multiple-hosts
```

関連コマンド

コマンド	説明
dot1x default	ポートの認証ステートの手動制御をイネーブルにします。
show dot1x（EtherSwitch）	デバイスまたは指定されたインターフェイスの IEEE 802.1X 統計情報、管理ステータス、および動作ステータスを表示します。

dot1x pae

ポート アクセス エンティティ（PAE）タイプを設定するには、インターフェイス コンフィギュレーション モードで **dot1x pae** コマンドを使用します。 設定された PAE タイプ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。

dot1x pae [**supplicant**| **authenticator**| **both**]

no dot1x pae [**supplicant**| **authenticator**| **both**]

構文の説明

supplicant	（任意）インターフェイスは、サプリカントとしてだけ機能し、オーセンティケータ向けのメッセージに応答しません。
authenticator	（任意）インターフェイスは、オーセンティケータとしてだけ機能し、サプリカント向けのメッセージに応答しません。
both	（任意）インターフェイスは、サプリカントおよびオーセンティケータとして動作するため、すべての dot1x メッセージに応答します。

コマンド デフォルト

PAE タイプは設定されません。

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
12.3(11)T	このコマンドが導入されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型ルータ（ISR）専用の Cisco IOS Release 12.4(4)XC に統合されました。
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

dot1x system-auth-control コマンドが設定されていない場合、**supplicant** キーワードがこのコマンドで使用できる唯一のキーワードとなります。（つまり、**dot1x system-auth-control** コマンドが設定されていない場合、インターフェイスをオーセンティケータとして設定できません）。

Cisco IOS Release 12.4(4)XC

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。ただし、コマンドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

例

次に、インターフェイスがサプリカントとして動作するように設定されている例を示します。

```
Router (config)# interface Ethernet1
Router (config-if)# dot1x pae supplicant
```

例

次に、スイッチ仮想インターフェイスのレイヤ 3 802.1X のサポートの例を示します（Cisco 870 ISR を使用）。

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
```

dot1x reauthentication

関連コマンド

コマンド	説明
dot1x system-auth-control	802.1X SystemAuthControl（ポートベース認証）をイネーブルにします。
interface	インターフェイス タイプを設定します。

dot1x port-control

（注） Cisco IOS Release 12.2(33) SXI では有効な **dot1x port-control** コマンドは、**authentication port-control** コマンドに置き換えられています。 詳細については、**authentication port-control** コマンドを参照してください。

制御ポートの許可ステートの手動制御をイネーブルにするには、インターフェイス コンフィギュレーション モードで **dot1x port-control** コマンドを使用します。 ポート制御値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。

dot1x port-control {**auto**| **force-authorized**| **force-unauthorized**}

no dot1x port-control

構文の説明

auto	802.1X ポートベースの認証をイネーブルにします。ポートは無許可ステートで開始し、ポート経由で送受信できるのは Extensible Authentication Protocol over LAN（EAPOL）フレームだけです。
force-authorized	インターフェイスの 802.1X をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可ステートに変更します。ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。 **force-authorized** キーワードはデフォルトです。
force-unauthorized	クライアントからの認証試行をすべて無視し、ポートを強制的に無許可ステートに変更して、このインターフェイス経由のすべてのアクセスを拒否します。

コマンド デフォルト

デフォルトの設定は force-authorized です。

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
12.1(6)EA2	このコマンドが Cisco イーサネット スイッチ ネットワーク モジュールに追加されました。
12.1(11)AX	このコマンドが、Cisco IOS Release 12.1(11)AX に統合されました。
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(15)ZJ	このコマンドが、Cisco イーサネット スイッチ ネットワーク モジュールのプラットフォーム Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズに実装されました。
12.3(2)XA	このコマンドが、Cisco 806、Cisco 831、Cisco 836、Cisco 837、Cisco 1701、Cisco 1710、Cisco 1721、Cisco 1751-V、および Cisco 1760 の Cisco スイッチに導入されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。 Cisco 1751、Cisco 2610XM、Cisco 2611XM、Cisco 2620XM、Cisco 2621XM、Cisco 2650XM、Cisco 2651XM、Cisco 2691、Cisco 3640、Cisco 3640A、および Cisco 3660 のプラットフォームにスイッチのサポートが追加されました。
12.2(17d)SXB	Supervisor Engine 2 上のこのコマンドのサポートが Cisco IOS Release 12.2（17d）SXB に追加されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型スイッチ（ISR）専用の Cisco IOS Release 12.4(4)XC 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)SXI	このコマンドが、**authentication port-control** コマンドに置き換えられました。

使用上のガイドライン

イーサネット スイッチ ネットワーク モジュールの場合

イーサネット スイッチ ネットワーク モジュールには、次の注意事項が適用されます。

- 802.1X プロトコルは、レイヤ 2 スタティック アクセス ポートでサポートされます。
- ポートが次のタイプのいずれかとして設定されていない場合に限り、**auto** キーワードを使用できます。

- トランク ポート：トランク ポートで 802.1X をイネーブルにしようとすると、エラー メッセージが表示され、802.1X はイネーブルになりません。 802.1x 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- EtherChannel ポート：ポート上で 802.1X をイネーブルにする前に、EtherChannel から 802.1X を削除する必要があります。 EtherChannel または EtherChannel 内のアクティブなポート上で 802.1x をイネーブルにしようとすると、エラーが表示され、802.1x はイネーブルになりません。 まだアクティブになっていない EtherChannel のポートで 802.1X をイネーブルにしても、そのポートが EtherChannel に加入することはありません。
- スイッチ ポート アナライザ（SPAN）宛先ポート：SPAN 宛先ポートで 802.1X をイネーブルにできますが、SPAN 宛先としてこのポートを削除するまで、802.1X はディセーブルに設定されます。 SPAN 送信元ポートでは 802.1x をイネーブルにすることができます。

デバイスで 802.1X をグローバルにディセーブルにするには、各ポートで 802.1X をディセーブルにする必要があります。 このタスクのグローバル コンフィギュレーション コマンドはありません。

Cisco IOS Release 12.4(4)XC の場合

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。 ただし、コマンドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

設定の確認

show dot1x コマンドを入力し、表示の 802.1x Port Summary セクションの Status カラムを確認することにより、設定を確認できます。 enabled ステータスとは、ポート制御値が auto または force-unauthorized に設定されていることです。

例

次の例では、クライアント PC の認証ステータスが認証プロセスによって決定されることを示します。

```
Switch(config)# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# dot1x port-control auto
```

例

次に、スイッチ仮想インターフェイスのレイヤ 3 802.1X のサポートの例を示します（Cisco 870 ISR を使用）。

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
```

```
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
```

dot1x reauthentication

関連コマンド

コマンド	説明
dot1x max-req	認証プロセスを再開する前に、スイッチまたはイーサネット スイッチ ネットワーク モジュールが EAP 要求/アイデンティティ フレームを送信できる最大回数を設定します（応答を受信しないと仮定）。
dot1x re-authentication	802.1Xインターフェイスのクライアントの定期的な再認証をグローバルでイネーブルにします。
dot1x reauthentication（**EtherSwitch**）	802.1Xインターフェイスのクライアントの定期的な再認証をイネーブルにします。
dot1x timeout	再試行タイムアウトを設定します。
dot1x timeout（**EtherSwitch**）	イーサネット スイッチ ネットワーク モジュールの再試行タイムアウトを設定します。
show dot1x	アイデンティティ プロファイルの詳細を表示します。
show dot1x（**EtherSwitch**）	スイッチまたは指定されたインターフェイスの IEEE 802.1X 統計情報、管理ステータス、および動作ステータスを表示します。

dot1x re-authenticate（特権 EXEC）

（注） Cisco IOS Release 12.2(33) SXI では有効な **dot1x re-authenticate** コマンドは、**clear authentication session** コマンドに置き換えられています。 詳細については、**clear authentication session** コマンドを参照してください。

指定した 802.1X 対応ポートの再認証を手動で開始するには、特権 EXEC モードで **dot1x re-authenticate** コマンドを使用します。

dot1x re-authenticate [**interface** *interface-name interface-number*]

構文の説明

interface *interface-name interface-number*	（任意）再認証を開始するインターフェイス。

コマンド デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。
12.3(2)XA	このコマンドが、Cisco IOS Release 12.3(2)XA に統合されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型ルータ（ISR）専用の Cisco IOS Release 12.4(4)XC に統合されました。

使用上のガイドライン

このコマンドを使用すると、再認証試行（re-authperiod）と自動再認証の間に設定された期間（秒）を待機する必要なく、クライアントを再認証できます。

Cisco IOS Release 12.4(4)XC

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。 ただし、コマン

ドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

例

次に、ポートに接続されているデバイスを手動で再認証する例を示します。

```
Router# dot1x re-authenticate interface gigabitethernet2/0/1
```

例

次に、スイッチ仮想インターフェイスのレイヤ 3 802.1X のサポートの例を示します（Cisco 870 ISR を使用）。

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
```

dot1x reauthentication

関連コマンド

コマンド	説明
dot1x reauthentication	802.1X インターフェイスのクライアント PC の定期的な再認証をグローバルでイネーブルにします。
dot1x timeout	再試行タイムアウトを設定します。

dot1x reauthentication

（注） Cisco IOS Release 12.2(33) SXI では有効な **dot1x reauthentication** コマンドは、**authentication periodic** コマンドに置き換えられています。 詳細については、**authentication periodic** コマンドを参照してください。

802.1X インターフェイス上でのクライアント PC の定期的な再認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで **dot1x reauthentication** コマンドを使用します。定期的な再認証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。

dot1x reauthentication

no dot1x reauthentication

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

定期的な再認証は設定されません。

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
12.2(14)SX	このコマンドが Supervisor Engine 720 に導入されました。
12.3(2)XA	このコマンドが、Cisco IOS Release 12.3(2)XA に統合されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。
12.2(17d)SXB	このコマンドが Cisco IOS Release 12.2(17d)SXB の Supervisor Engine 2 に実装されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型ルータ（ISR）専用の Cisco IOS Release 12.4(4)XC 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)SXI	このコマンドが、**authentication periodic** コマンドに置き換えられました。

使用上のガイドライン

再認証の間隔は、**dot1x timeout** コマンドを使用して設定できます。

Cisco IOS Release 12.4(4)XC

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。ただし、コマンドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

例

次に、再認証がイネーブルであり、再認証の間隔が1800秒として設定されている例を示します。

```
Router(config)# configure terminal
Router(config)# interface ethernet 0
Router(config-if)# dot1x reauthentication
Router(config-if)# dot1x timeout reauth-period 1800
```

例

次に、Cisco 870 ISR を使用したスイッチ仮想インターフェイスのレイヤ 3 802.1X のサポートの例を示します。

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
```

dot1x reauthentication

例

次に、クライアントの定期的な再認証をイネーブルにする例を示します。

```
Router(config-if)# dot1x reauthentication
Router(config-if)#
```

次に、クライアントの定期的な再認証をディセーブルにする例を示します。

```
Router(config-if)# no dot1x reauthentication
Router(config-if)#
```

関連コマンド

コマンド	説明
dot1x max-req	クライアントPCが802.1Xをサポートしないと結論する前に、ルータがEAP要求/アイデンティティ フレームをクライアントPCに送信できる最大回数を設定します（応答を受信しないと仮定）。
dot1x port-control	802.1X ポート制御値を設定します。
dot1x timeout	再試行タイムアウトを設定します。
show dot1x	802.1X 情報を表示します。

dot1x re-authentication（EtherSwitch）

イーサネット スイッチ ネットワーク モジュールのクライアントの定期的な再認証をイネーブルにするには、グローバル コンフィギュレーション モードで **dot1x re-authentication** コマンドを使用します。 定期的な再認証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。

dot1x re-authentication

no dot1x re-authentication

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

定期的な再認証はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(6)EA2	このコマンドが導入されました。
12.2(15)ZJ	このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに追加されました。
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。

使用上のガイドライン

定期的な再認証試行が行われる時間間隔を設定するには、**dot1x timeout re-authperiod** グローバル コンフィギュレーション コマンドを使用します。

例

次に、クライアントの定期的な再認証をディセーブルにする例を示します。

```
Router(config)# no dot1x re-authentication
```

次に、定期的な再認証をイネーブルにし、再認証を試行する間隔を4000秒に設定する例を示します。

```
Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000
```

関連コマンド

コマンド	説明
dot1x timeout（EtherSwitch）	イーサネット スイッチ ネットワーク モジュールの再試行タイムアウトを設定します。
show dot1x（EtherSwitch）	デバイスまたは指定されたインターフェイスの IEEE 802.1X 統計情報、管理ステータス、および動作ステータスを表示します。

dot1x system-auth-control

802.1X SystemAuthControl（ポートベース認証）をグローバルでイネーブルにするには、グローバル コンフィギュレーション モードで **dot1x system-auth-control** コマンドを使用します。SystemAuthControl 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。

dot1x system-auth-control

no dot1x system-auth-control

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

システム認証はデフォルトでディセーブルです。 このコマンドがディセーブルの場合、すべてのポートが強制的に許可されているように動作します。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.3(2)XA	このコマンドが導入されました。
12.2(14)SX	このコマンドがスーパーバイザ エンジン 720 に実装されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。
12.2(17d)SXB	Supervisor Engine 2 上のこのコマンドのサポートが Release 12.2(17d)SXB に拡張されました。
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。

使用上のガイドライン

IEEE 802.1x 標準では、許可されていないデバイスが一般的にアクセス可能なポートを介して LAN に接続することを制限する、クライアント/サーバベースのアクセス コントロールと認証プロトコルが定義されています。 802.1x は、ポートごとに 2 つの個別の仮想アクセス ポイントを作成してネットワーク アクセスを制御します。 一方のアクセス ポイントが未制御ポート、もう一方は制

御ポートです。単一のポートを通過するすべてのトラフィックは、両方のアクセスポイントを利用できます。802.1xは、スイッチまたはLANが提供するサービスを利用できるようにする前に、スイッチのポートに接続されている各ユーザデバイスを認証し、そのポートをVLAN（仮想LAN）に割り当てます。802.1xアクセス制御では、デバイスが認証されるまで、そのデバイスが接続されているポートを通過するExtensible Authentication Protocol（EAP）over LAN（EAPOL）トラフィックのみが許可されます。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

このコマンドの **no** 形式を使用すると、802.1X 関連の設定がすべて削除されます。

Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ

802.1Xをイネーブルにする前に、認証、許可、およびアカウンティング（AAA）をイネーブルにし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。

例

次に、SystemAuthControl をイネーブルにする例を示します。

```
Router(config)# dot1x system-auth-control
```

関連コマンド

コマンド	説明
aaa authentication dot1x	IEEE 802.1X を実行するインターフェイスで使用する 1 つまたは複数の AAA 方式を指定します。
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
debug dot1x	802.1X デバッグ情報を表示します。
description	802.1X プロファイルの説明を指定します。
device	静的に個々のデバイスを許可または拒否します。
dot1x initialize	すべての802.1X対応インターフェイスで802.1Xステート マシンを初期化します。
dot1x max-req	認証プロセスを再開する前に、ルータまたはイーサネット スイッチ ネットワーク モジュールが EAP 要求/アイデンティティ フレームを送信できる最大回数を設定します（応答を受信しないと仮定）。

コマンド	説明
dot1x port-control	制御ポートの許可ステートの手動制御をイネーブルにします。
dot1x re-authenticate	指定した 802.1X 対応ポートの再認証を手動で開始します。
dot1x reauthentication	802.1X インターフェイスのクライアント PC の定期的な再認証をグローバルでイネーブルにします。
dot1x timeout	再試行タイムアウトを設定します。
identity profile	アイデンティティプロファイルを作成し、アイデンティティ プロファイル コンフィギュレーション モードを開始します。
show dot1x	アイデンティティプロファイルの詳細および統計情報を表示します。
template	コマンドをクローニングできる仮想テンプレートを指定します。

dot1x timeout

再試行タイムアウトの値を設定するには、グローバルコンフィギュレーションモードまたはインターフェイス コンフィギュレーション モードで **dot1x timeout** コマンドを使用します。 再試行タイムアウトのデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

All Platforms Except the Cisco 7600 Series Switch

dot1x timeout {**auth-period** *seconds*| **held-period** *seconds*| **quiet-period** *seconds*| **ratelimit-period** *seconds*| **reauth-period** {*seconds*| **server**}| **server-timeout** *seconds*| **start-period** *seconds*| **supp-timeout** *seconds*| **tx-period** *seconds*}

no dot1x timeout {**auth-period** *seconds*| **held-period** *seconds*| **quiet-period** *seconds*| **ratelimit-period** *seconds*| **reauth-period** {*seconds*| **server**}| **server-timeout** *seconds*| **start-period** *seconds*| **supp-timeout** *seconds*| **tx-period** *seconds*}

Cisco 7600 Series Switch

dot1x timeout {**reauth-period** *seconds*| **quiet-period** *seconds*| **tx-period** *seconds*| **supp-timeout** *seconds*| **server-timeout** *seconds*}

no dot1x timeout {**reauth-period**| **quiet-period**| **tx-period**| **supp-timeout**| **server-timeout**}

構文の説明

auth-period *seconds*	サプリカント（クライアント）がオーセンティケータからの応答（Extensible Authentication Protocol over LAN（EAPOL）-Start 以外のパケット）を何秒待機するとタイムアウトとなるかを設定します。 • 指定できる範囲は 1 ～ 65535 です。デフォルトは 30 です。
held-period *seconds*	サプリカントで保留ステートが維持される秒数（つまり、サプリカントが試行に失敗した場合に再度クレデンシャルを送信するまでに待機する時間）を設定します。 • 指定できる範囲は 1 ～ 65535 です。デフォルトは 60 です。

quiet-period *seconds*	認証情報の交換に失敗した後、クライアントの再認証を試行する前に、オーセンティケータ（サーバ）が（保留ステートで）待機し続ける時間（秒単位）を設定します。 • Cisco 7600 シリーズ スイッチを除くすべてのプラットフォームの場合、範囲は 1 ～ 65535 です。 デフォルトは 120 です。 • Cisco 7600 シリーズ スイッチの場合、範囲は 0 ～ 65535 です。 デフォルトは 60 です。
ratelimit-period *seconds*	動作の不正なクライアント PC（たとえば、スイッチの処理能力を浪費する EAP-START パケットを送信する PC）から送信される EAP-START パケットを抑制します。 • オーセンティケータはレート制限時間中、認証に成功したクライアントからの EAPOL-Start パケットを無視します。 • 指定できる範囲は 1 ～ 65535 です。 デフォルトでは、レート制限はディセーブルになっています。

reauth-period {*seconds* | **server**}	自動再認証が開始されるまでの時間（秒単位）を設定します。 • **server** キーワードは、クライアントの再認証時間値を認証、許可、アカウンティング（AAA）サーバから Session-Timeout（RADIUS 属性 27）値として取得する必要があることを示します。**server** キーワードを使用すると、再認証時のアクションもサーバによって決定され、Termination-Action（RADIUS 属性 29）値として送信されます。終了処理は「終了」または「再認証」のいずれかになる場合があります。**server** キーワードを使用しない場合、終了処理は常に「再認証」になります。 • Cisco 7600 シリーズ スイッチを除くすべてのプラットフォームの場合、範囲は 1 ～ 65535 です。 デフォルト値は 3600 です。 • Cisco 7600 シリーズ スイッチの場合、範囲は 1 ～ 4294967295 です。 デフォルト値は 3600 です。 詳細については、「使用上のガイドライン」の項を参照してください。 （注） Cisco IOS Release 12.2(33) SXI では有効なこのフレーズは、**authentication timer reauthenticate** コマンドに置き換えられています。 詳細については、**authentication timer reauthenticate** コマンドを参照してください。
server-timeout *seconds*	連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。 • Cisco 7600 シリーズ スイッチを除くすべてのプラットフォームの場合、範囲は 1 ～ 65535 です。 デフォルトは 30 です。 • Cisco 7600 シリーズ スイッチの場合、範囲は 30 ～ 65535 です。 デフォルトは 30 です。 サーバが指定された時間内に 802.1X パケットへの応答を送信しない場合、パケットは再度送信されます。

start-period *seconds*	連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。 • 値は 1 ～ 65535 です。 デフォルトは 30 です。
supp-timeout *seconds*	EAP 要求 ID 以外のすべての EAP メッセージのオーセンティケータからホストへの再送信時間を設定します。 • Cisco 7600 シリーズ スイッチを除くすべてのプラットフォームの場合、範囲は 1 ～ 65535 です。 デフォルトは 30 です。 • Cisco 7600 シリーズ スイッチの場合、範囲は 30 ～ 65535 です。 デフォルトは 30 です。
tx-period *seconds*	クライアントへの EAP 要求 ID パケットの再送信間隔（応答が受信されると仮定）の秒数を設定します。 • Cisco 7600 シリーズ スイッチを除くすべてのプラットフォームの場合、範囲は 1 ～ 65535 です。 デフォルトは 30 です。 • Cisco 7600 シリーズ スイッチの場合、範囲は 30 ～ 65535 です。 デフォルトは 30 です。 • 802.1X パケットがサプリカントに送信され、サプリカントが再試行時間後に応答を送信しない場合、パケットは再度送信されます。

コマンド デフォルト

定期的な再認証および定期的なレート制限は行われません。

コマンド モード

グローバル コンフィギュレーションまたはインターフェイス コンフィギュレーション

Cisco 7600 スイッチ

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
12.2(14)SX	このコマンドが Supervisor Engine 720 に導入されました。
12.3(2)XA	このコマンドが、Cisco IOS Release 12.3(2)XA に統合されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。
12.2(18)SE	**server-timeout**、**supp-timeout**、および **tx-period** キーワードの範囲が変更されました。
12.2(17d)SXB	Supervisor Engine 2 上のこのコマンドのサポートが Cisco IOS Release 12.2（17d）SXB に追加されました。
12.3(11)T	**auth-period**、**held-period**、および **start-period** キーワードが追加されました。
12.2(25)SEC	**tx-period** キーワードの範囲が変更され、**reauth-period** および **server-timeout** キーワードが追加されました。
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	**supp-timeout** キーワードおよび **server-timeout** キーワードが追加されました。このコマンドのコンフィギュレーションモードが、インターフェイス コンフィギュレーション モードに変更されました。
12.4(6)T	**supp-timeout** キーワードが追加され、このコマンドは、Cisco IOS Release 12.4(6)T に統合されました。
12.4(4)XC	このコマンドが、Cisco 870 サービス統合型スイッチ（ISR）専用の Cisco IOS Release 12.4(4)XC 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)SXI	**reauth-period** キーワードは、**authentication timer reauthenticate** コマンドに置き換えられました。

使用上のガイドライン

Cisco IOS Release 12.4(4)XC では、Cisco ISR 870 上でのみ、このコマンドをレイヤ 2（スイッチポート）とレイヤ 3 に設定できます（スイッチ仮想インターフェイスの場合）。 ただし、コマンドは同時に 1 レイヤのみに対して機能できます。つまり、レイヤ 2 に設定されている場合に、レイヤ 3 にも設定することはできません（逆の場合も同様）。

Cisco 7600 スイッチ

dot1x timeout reauth-period コマンドを入力する前に、定期的な再認証をイネーブルにしておく必要があります。 定期的な再認証をイネーブルにするには、**dot1x reauthentication** コマンドを入力します。 定期的な再認証がイネーブルに設定されている場合にだけ、**dot1x timeout reauth-period** コマンドはシステムの動作を有効にします。

例

次に、さまざまな 802.1X 再送信時間およびタイムアウト時間が設定されている例を示します。

```
Switch(config)# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout auth-period 2000
Switch(config-if)# dot1x timeout held-period 2400
Switch(config-if)# dot1x timeout reauth-period 1800
Switch(config-if)# dot1x timeout quiet-period 600
Switch(config-if)# dot1x timeout start-period 90
Switch(config-if)# dot1x timeout supp-timeout 300
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x timeout server-timeout 60
```

次に、デフォルトの再認証時間に戻す例を示します。

```
Switch(config-if)# no dot1x timeout reauth-period
```

例

次に、Cisco 7600 スイッチの 802.1X 再送信時間およびタイムアウト時間を設定する例を示します。

```
Switch(config-if)# dot1x timeout reauth-period 4000
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x timeout supp-timeout 25
Switch(config-if)# dot1x timeout server-timeout 25
```

例

次に、スイッチ仮想インターフェイスのレイヤ 3 802.1X のサポートの例を示します（Cisco 870 ISR を使用）。

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
```

dot1x reauthentication

関連コマンド

コマンド	説明
dot1x max-req	認証プロセスを再開する前に、スイッチまたはイーサネット スイッチ モジュールが EAP 要求/アイデンティティ フレームを送信できる最大回数を設定します（応答を受信しないと仮定）。
dot1x port-control	802.1X ポート制御値を設定します。
dot1x re-authentication	802.1X インターフェイスのクライアント PC の定期的な再認証をグローバルでイネーブルにします。
show dot1x	802.1X 情報を表示します。

dot1x timeout（EtherSwitch）

イーサネット スイッチ ネットワーク モジュールがルータに搭載されている場合に、802.1X 認証情報交換の間の再試行秒数を設定するには、グローバル コンフィギュレーション モードで **dot1x timeout** コマンドを使用します。 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。

dot1x timeout {**quiet-period** *seconds*| **re-authperiod** *seconds*| **tx-period** *seconds*}

no dot1x timeout {**quiet-period** *seconds*| **re-authperiod** *seconds*| **tx-period** *seconds*}

構文の説明

quiet-period *seconds*	イーサネット スイッチ ネットワーク モジュールがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数を指定します。範囲は 0 ～ 65535 秒です。 デフォルトは 60 秒です。
re-authperiod *seconds*	再認証の間隔（秒）を指定します。指定できる範囲は 1 ～ 4294967295 です。 デフォルトは 3660 秒です。
tx-period *seconds*	要求を再送信するまでに、スイッチがクライアントからの EAP 要求/アイデンティティ フレームに対する応答を待機する時間（秒単位）。範囲は 1 ～ 65535 秒です。 デフォルトは 30 秒です。

コマンド デフォルト

quiet-period：60 秒 **re-authperiod**：3660 秒 **tx-period**：30 秒

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(6)EA2	このコマンドが導入されました。
12.2(15)ZJ	このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに追加されました。

リリース	変更内容
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。

使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

quiet-period キーワード

待機時間中は、イーサネット スイッチ ネットワーク モジュールは認証要求を受け入れまたは開始しなくなります。 デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

re-authperiod キーワード

re-authperiod キーワードは、**dot1x re-authentication** グローバル コンフィギュレーション コマンドを使用して定期的な再認証をイネーブルにしている場合にのみ、イーサネット スイッチ ネットワーク モジュールの動作に影響します。

例

次に、スイッチの待機時間を 30 秒に設定する例を示します。

```
Router(config)# dot1x timeout quiet-period 30
```

次に、定期的な再認証をイネーブルにし、再認証を試行する間隔を4000秒に設定する例を示します。

```
Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000
```

次に、要求を再送信する前に、スイッチが EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待機する時間を 60 秒に設定する方法を示します。

```
Router(config)# dot1x timeout tx-period 60
```

関連コマンド

コマンド	説明
dot1x max-req	デバイスが、認証プロセスを再始動する前に、EAP 要求/アイデンティティ フレームを送信する最大回数を設定します。
dot1x re-authentication（EtherSwitch）	イーサネット スイッチ ネットワーク モジュールのクライアントの定期的な再認証をイネーブルにします。

コマンド	説明
show dot1x（EtherSwitch）	デバイスまたは指定されたインターフェイスの IEEE 802.1X 統計情報、管理ステータス、および動作ステータスを表示します。

E

enable password

さまざまな権限レベルへのアクセスを制御するローカル パスワードを設定するには、グローバル コンフィギュレーション モードで **enable password** コマンドを使用します。 パスワードの要件を削除するには、このコマンドの **no** 形式を使用します。

enable password [**level** *level*] {*password*| [*encryption-type*] *encrypted-password*}

no enable password [**level** *level*]

構文の説明

level *level*	（任意）パスワードが適用されるレベル。 0 ～ 15 の数字を使用して最大 16 個の権限レベルを指定できます。 レベル 1 が通常の EXEC モード ユーザ権限です。 この引数が、コマンドまたはコマンドの **no** 形式で指定されていない場合、権限レベルはデフォルトの 15 になります（従来のイネーブル権限）。
password	イネーブル モードを開始するパスワードのユーザ タイプ。
encryption-type	（任意）パスワードの暗号化に使用されるシスコ独自のアルゴリズム。 現在使用可能な暗号化タイプは 5 だけです。 *encryption-type* を指定する場合は、入力する次の引数は暗号化されたパスワード（すでに Cisco ルータにより暗号化されたパスワード）である必要があります。
encrypted-password	ユーザが入力する暗号化パスワード。別のルータ設定からコピーされます。

コマンド デフォルト

パスワードは定義されていません。 デフォルトはレベル 15 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
10.0	このコマンドが導入されました。

リリース	変更内容
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

注意 enable password コマンドまたは enable secret コマンドのいずれも設定されていない場合に、コンソールに設定されている回線パスワードがある場合、コンソール回線パスワードはすべての VTY（Telnet および Secure Shell（SSH））セッションのイネーブル パスワードとして機能します。

このコマンドを **level** オプションとともに使用して、特定の権限レベルのパスワードを定義します。 レベルおよびパスワードを設定した後、このレベルにアクセスする必要のあるユーザにパスワードを提供してください。 各レベルでアクセスできるコマンドを指定するには、**privilege level** コンフィギュレーション コマンドを使用します。

通常、暗号化タイプを入力しません。 通常、このコマンドに Cisco ルータによりすでに暗号化されたパスワードをコピー アンド ペーストする場合に限り、暗号化タイプを入力します。

注意 暗号化タイプを指定し、クリア テキスト パスワードを入力した場合は、イネーブル モードを再開できません。 どのような方法で暗号化されたパスワードでも、失われた場合、回復することはできません。

service password-encryption コマンドが設定されている場合、**more nvram:startup-config** コマンドを入力すると、**enable password** コマンドで作成するパスワードの暗号化された形式が表示されます。

service password-encryption コマンドを使用して、パスワード暗号化をイネーブルまたはディセーブルにできます。

イネーブル パスワードの定義は、次のとおりです。

- 1 ～ 25 文字の大文字と小文字の英数字を含める必要があります。
- 先頭にスペースを指定できますが、無視されます。 ただし、中間および末尾のスペースは認識されます。
- パスワードを作成するときに、Ctrl+v キーの組み合わせを押してから疑問符（?）を入力すると、パスワードに疑問符を含めることができます。たとえば、*abc?123* というパスワードを作成するには、次の手順を実行します。
  - **abc** を入力します。

- **Ctrl+v** を押します。
- **?123** を入力します。

システムからイネーブル パスワードを入力するように求められた場合、疑問符の前に Ctrl+v を入力する必要はなく、パスワードのプロンプトにそのまま abc?123 と入力できます。

例

次に、権限レベル 2 のパスワード「pswd2」をイネーブルにする例を示します。

```
enable password level 2 pswd2
```

次に、暗号化タイプ 7 を使用して、ルータのコンフィギュレーション ファイルからコピーされた権限レベル 2 の暗号化パスワード「1i5Rkls3LoyxzS8t9」を設定する例を示します。

```
enable password level 2 5 $1$i5Rkls3LoyxzS8t9
```

関連コマンド

コマンド	説明
disable	特権 EXEC モードを終了し、ユーザ EXEC モードに戻ります。
enable	特権 EXEC モードを開始します。
enable secret	**enable password** コマンドよりも強化したセキュリティ レイヤを指定します。
privilege	ユーザの新しい権限レベルを設定し、コマンドをその権限レベルに関連付けます。
service password-encryption	パスワードを暗号化します。
show privilege	現在の権限レベルを表示します。

enable secret

enable password コマンドよりも強化したセキュリティ レイヤを指定するには、グローバル コンフィギュレーション モードで **enable secret** コマンドを使用します。 **enable secret** 機能をオフにするには、このコマンドの **no** 形式を使用します。

enable secret [**level** *level*] {**[0]** *unencrypted-password*| *encryption-type encrypted-password*}

no enable secret [**level** *level*] [*encryption-type encrypted-password*]

構文の説明

level *level*	（任意）パスワードが適用されるレベルを指定します。 1 ～ 15 の数字を使用して最大 15 個の権限レベルを指定できます。 レベル 1 が通常の EXEC モード ユーザ権限です。 *level* 引数が、コマンドまたはコマンドの **no** 形式で指定されていない場合、権限レベルはデフォルトの 15 になります（従来のイネーブル権限）。
0	（任意）暗号化されていないクリアテキスト パスワードを指定します。 パスワードは Secure Hash Algorithm（SHA）256 シークレットに変換されて、ルータに保存されます。
unencrypted-password	イネーブル モードを開始するユーザのパスワード。 このパスワードは、**enable password** コマンドで作成されたパスワードとは異なっている必要があります。
encryption-type	パスワードの暗号化に使用されるシスコ独自のアルゴリズム。 このコマンドで使用可能な暗号化タイプは 4 および 5. です。 • **4**：SHA-256 で暗号化されたシークレット ストリングを指定します。 SHA256 シークレット ストリングはルータ コンフィギュレーションからコピーされます。 • **5**：メッセージ ダイジェスト アルゴリズム 5（MD5）により暗号化されたシークレットを指定します。
encrypted-password	別のルータ コンフィギュレーションからコピーされる暗号化パスワード。

コマンド デフォルト

グローバルは定義されていません。コンフィグ（config）トのレベルは 15 です。

コマンド履歴

リリース	変更内容
11.0	このコマンドが導入されました。
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。
15.0(1)S	このコマンドが Cisco IOS Release 15.0(1)S に統合されました。 暗号化タイプ **4** のサポートが追加されました。
Cisco IOS XE Release 3.1S	このコマンドが Cisco IOS XE Release 3.1S に統合されました。 暗号化タイプ **4** のサポートが追加されました。
15.1(4)M	このコマンドが変更されました。 暗号化タイプ **4** のサポートが追加されました。
Cisco IOS Release 3.3.0SG	このコマンドが変更されました。 暗号化タイプ **5** はサポートされなくなりました。
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	このコマンドが変更されました。 暗号化タイプ **5** のサポート廃止の警告メッセージが変更されました。

使用上のガイドライン

注意 **enable password** コマンドまたは **enable secret** コマンドのいずれも設定されていない場合に、コンソールに回線パスワードが設定されている場合、コンソール回線パスワードはすべての vty（Telnet および Secure Shell（SSH））セッションのイネーブル パスワードとして機能します。

イネーブル パスワードよりも強化したセキュリティ レイヤを追加するには、**enable secret** コマンドを使用します。 **enable secret** コマンドでは、不可逆的な暗号化機能を使用してイネーブル シークレットパスワードが保存されるため、セキュリティが向上します。追加されたセキュリティ暗号化のレイヤは、パスワードがネットワークを通過する、または TFTP サーバに保存される環境において役立ちます。

通常、ルータのコンフィギュレーション ファイルからコピーした暗号化パスワードをこのコマンドにペーストする場合にのみ、暗号化タイプを入力します。

注意 暗号化タイプを指定し、クリアテキスト パスワードを入力した場合は、イネーブル モードを再開できません。 どのような方法で暗号化されたパスワードでも、失われた場合、回復することはできません。

enable password コマンドと **enable secret** コマンドに同じパスワードを使用した場合は、その方法が推奨されないことを示すエラー メッセージの警告が表示されますが、パスワードは受け入れられます。 ただし、同じパスワードを使用することにより、**enable secret** コマンドによって提供される追加のセキュリティが損なわれます。

（注） **enable secret** コマンドを使用してパスワードを設定した後には、**enable password** コマンドを使用して設定されたパスワードは、**enable secret** がディセーブルになっている場合、またはCisco IOS ソフトウェアの古いバージョンが使用されている場合（古い rxboot イメージを実行している場合など）にのみ動作します。 また、どのような方法で暗号化されたパスワードでも、失われた場合、回復することはできません。

service password-encryption コマンドが設定されている場合、**more nvram:startup-config** コマンドを入力すると、作成するパスワードの暗号化された形式が表示されます。

service password-encryption コマンドを使用して、パスワード暗号化をイネーブルまたはディセーブルにできます。

イネーブル パスワードの定義は、次のとおりです。

- 大文字と小文字両方の 1 ～ 25 文字の英数字を含める必要があります。
- 先頭にスペースを指定できますが、無視されます。 ただし、中間および末尾のスペースは認識されます。
- パスワードを作成するときに、Ctrl+v キーの組み合わせを押してから疑問符（?）を入力すると、パスワードに疑問符を含めることができます。たとえば、*abc?123* というパスワードを作成するには、次の手順を実行します。
  - **abc** を入力します。
  - **Ctrl+v** を押します。
  - **?123** を入力します。

システムからイネーブル パスワードを入力するように求められた場合、疑問符の前に Ctrl+v を入力する必要はなく、パスワードのプロンプトに **abc?123** と入力できます。

（注） 3.3.0SG から 3.2.0SG へのダウングレード中に、SHA256 により暗号化されたパスワードが設定されていて、SHA256 により暗号化されたパスワードが警告なしで失われた場合は、シークレット パスワードを再設定する必要があります。

例

次に、**enable secret** コマンドを使用してパスワードを指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable secret password
```

enable secret コマンドでパスワードを指定した後には、ユーザはアクセスするために、このパスワードを入力する必要があります。 **enable password** コマンドで設定されたパスワードは、動作しなくなります。

```
Password: password
```

次に、暗号化タイプ 4 を使用して、ルータのコンフィギュレーション ファイルからコピーされた権限レベル 2 の暗号化パスワード「1FaD0$Xyti5Rkls3LoyxzS8」をイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 4 $1$FaD0$Xyti5Rkls3LoyxzS8
```

次に、ユーザが **enable secret 5** *encrypted-password* コマンドを入力したときに表示される警告メッセージの例を示します。

```
Device(config)# enable secret 5 $1$FaD0$Xyti5Rkls3LoyxzS8

Warning: The CLI will be deprecated soon
'enable secret 5 <password>'
Please move to 'enable secret <password>' CLI
```

関連コマンド

コマンド	説明
enable	特権 EXEC モードを開始します。
enable password	さまざまな権限レベルへのアクセスを制御するローカル パスワードを設定します。
service password-encryption	パスワードを暗号化します。

enrollment http-proxy

プロキシ サーバを介して HTTP により認証局（CA）にアクセスするには、ca-trustpoint コンフィギュレーション モードで**enrollment http-proxy** コマンドを使用します。

enrollment http-proxy *host-name port-num*

構文の説明

host-name	CA を取得するために使用するプロキシ サーバを定義します。
port-num	CA へのアクセスに使用するポート番号を指定します。

コマンド デフォルト

このコマンドをイネーブルにしない場合、CA は HTTP 経由でアクセスされません。

コマンド モード

ca-trustpoint 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
12.2(8)T	このコマンドが導入されました。
12.2(18)SXD	このコマンドが、Cisco IOS Release 12.2(18)SXD に統合されました。

使用上のガイドライン

enrollment http-proxy コマンドは、**enrollment** コマンドとともに使用する必要があります。このコマンドにより、CA の登録パラメータを指定します。

例

次に、bomborra プロキシ サーバを介して HTTP により「ka」という名前の CA にアクセスする例を示します。

```
crypto ca trustpoint ka
 enrollment url http://kahului
 enrollment http-proxy bomborra 8080
 crl optional
```

関連コマンド

コマンド	説明
crypto ca trustpoint	ルータが使用する CA を宣言します。
enrollment	CA の登録パラメータを指定します。

enrollment url（ca-profile-enroll）

登録要求を送信する認証局（CA）サーバの URL を指定するには、ca-profile-enroll コンフィギュレーション モードで **enrollment url** コマンドを使用します。 登録プロファイルから登録 URL を削除するには、このコマンドの **no** 形式を使用します。

enrollment url *url*

no enrollment url *url*

構文の説明

url	ルータが証明書要求を送信する CA サーバの URL。 登録に Simple Certificate Enrollment Protocol（SCEP）を使用している場合、*url* 引数は、http://CA_name（CA_name は、CA のホスト ドメイン ネーム システム（DNS）名、または IP アドレス）の形式で指定する必要があります。 登録に TFTP を使用している場合は、*url* 引数を tftp://certserver/file_specification の形式で指定する必要があります。 （URL にファイル指定が含まれない場合、ルータの完全修飾ドメイン名（FQDN）が使用されます）。

コマンド デフォルト

このコマンドを使用して指定するまで、ルータは CA URL を認識しません。

コマンド モード

Ca-profile-enroll 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
12.2(13)ZH	このコマンドが導入されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。

使用上のガイドライン

このコマンドにより、証明書を認証し、証明書を登録するための異なる URL または異なる方法（たとえば、手動認証、TFTP 登録など）を指定することができます。

例

次に、プロファイル名「E」の HTTP 経由での証明書登録をイネーブルにする例を示します。

```
crypto pki trustpoint Entrust
  enrollment profile E
  serial
crypto pki profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

関連コマンド

コマンド	説明
crypto pki profile enrollment	登録プロファイルを定義します。

F ～ H

hostname（IKEv2 キーリング）

インターネット キー交換バージョン 2（IKEv2）キーリングのピアのホスト名を指定するには、IKEv2 キーリング ピア コンフィギュレーション モードで **hostname** コマンドを使用します。 ホスト名を削除するには、このコマンドの **no** 形式を使用します。

hostname *name*

no hostname

構文の説明

name	ピアの名前。

コマンド デフォルト

ホスト名は指定されません。

コマンド モード

IKEv2 キーリング ピア コンフィギュレーション（config-ikev2-keyring-peer）

コマンド履歴

リリース	変更内容
15.1(1)T	このコマンドが導入されました。
Cisco IOS XE リリース 3.3S	このコマンドが Cisco IOS XE Release 3.3S に統合されました。
15.2(4)S	このコマンドが Cisco IOS Release 15.2(4)S に統合されました。

使用上のガイドライン

IKEv2 キーリングを設定する場合は、このコマンドを使用して、次のようなホスト名によりピアを識別します。

- IKEv2 アイデンティティから独立している。
- IKEv2 イニシエータ上でのみ使用できる。
- ピアを識別するセキュリティ アソシエーションのセットアップ要求の一部として、IKEv2 により IPsec に対して提供されている。
- クリプト マップのみを使用し、トンネル保護を使用せずにピアを識別するために使用される。

例

次に、IKEv2 キーリングを設定する際にピアのホスト名を設定する例を示します。

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description peer1
Router(config-ikev2-keyring-peer)# hostname peer1.example.com
```

関連コマンド

コマンド	説明
address（ikev2 キーリング）	IKEv2 キーにおけるピアの IPv4 アドレスまたは範囲を指定します。
crypto ikev2 keyring	IKEv2 キーリングを定義します。
description（ikev2 キーリング）	IKEv2 キーリングの IKEv2 ピアまたはピア グループの説明を記述します。
identity（ikev2 キーリング）	アイデンティティの IKEv2 タイプによりピアを識別します。
peer	キーリングのピアまたはピア グループを定義します。
pre-shared-key（**ikev2 キーリング**）	IKEv2 ピアの事前共有キーを定義します。

identity profile ～ ip device tracking probe

identity profile

アイデンティティプロファイルを作成し、アイデンティティプロファイル コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **identity profile** コマンドを使用します。 アイデンティティ プロファイル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。

identity profile {**default| dot1x| eapoudp| auth-proxy**}

no identity profile {**default| dot1x| eapoudp| auth-proxy**}

構文の説明

default	サービス タイプはデフォルトです。
dot1x	802.1X のサービス タイプ。
eapoudp	Extensible Authentication Protocol over UDP（EAPoUDP）のサービス タイプ。
auth-proxy	認証プロキシのサービス タイプ。

コマンド デフォルト

アイデンティティ プロファイルは作成されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.3(2)XA	このコマンドが導入されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。
12.3(8)T	**eapoudp** キーワードが追加されました。
12.4(6)T	**dot1x** キーワードが削除されました。
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。

リリース	変更内容
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

identity profile コマンドおよび **default** キーワードにより、802.1X をサポートしないクライアントコンピュータのスタティック MAC アドレスを設定し、これらのクライアント コンピュータの許可または無許可を静的に切り替えることができます。 **identity profile** コマンドおよび **default** キーワードを発行し、ルータがアイデンティティ プロファイル コンフィギュレーション モードになると、非認証サプリカント（クライアントコンピュータ）がマッピングされる仮想アクセスインターフェイスの作成に使用可能なテンプレートの設定を指定できます。

identity profile コマンドおよび **dot1x** キーワードはサプリカントとオーセンティケータによって使用されます。 **dot1x** キーワードを使用して、802.1X 認証用のユーザ名、パスワード、またはその他のアイデンティティ関連の情報を設定できます。

identity profile コマンドおよび **eapoudp** キーワードを使用して、デバイスの IP アドレス、MAC アドレス、またはタイプに基づいてデバイスの認証または非認証を静的に切り替えることができ、**identity policy** コマンドを使用して、対応するネットワーク アクセス ポリシーを指定できます。

例

次に、アイデンティティ プロファイルおよびその説明を指定する例を示します。

```
Router (config)# identity profile default
Router (config-identity-prof)# description description_entered_here
```

次に、EAPoUDP アイデンティティ プロファイルを作成する例を示します。

```
Router (config)# identity policy eapoudp
```

関連コマンド

コマンド	説明
debug dot1x	802.1X デバッグ情報を表示します。
description	802.1X プロファイルの説明を指定します。
device	静的に個々のデバイスを許可または拒否します。
dot1x initialize	すべての 802.1X 対応インターフェイスで 802.1X ステート マシンを初期化します。

コマンド	説明
dot1x max-req	ルータがクライアント PC に EAP 要求/アイデンティティ フレームを送信できる最大回数を設定します。
dot1x max-start	オーセンティケータがクライアントに EAP 要求/アイデンティティ フレームを送信する最大回数を設定します（応答が受信されないと仮定）。
dot1x pae	802.1X 認証中の PAE タイプを設定します。
dot1x port-control	制御ポートの許可ステートの手動制御をイネーブルにします。
dot1x re-authenticate	指定した 802.1X 対応ポートの再認証を手動で開始します。
dot1x re-authentication	802.1X インターフェイスのクライアント PC の定期的な再認証をグローバルでイネーブルにします。
dot1x system-auth-control	802.1X SystemAuthControl（ポートベース認証）をイネーブルにします。
dot1x timeout	再試行タイムアウトを設定します。
identity policy	アイデンティティ ポリシーを作成します。
show dot1x	アイデンティティ プロファイルの詳細を表示します。
template（アイデンティティ プロファイル）	コマンドをクローニングできる仮想テンプレートを指定します。

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 IP アクセス リストまたはオブジェクト グループ アクセス コントロール リスト（OGACL）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 **ip access-group** コマンドを使用します。 IP アクセス リストまたは OGACL を削除するには、このコマンドの **no** 形式を使用します。

ip access-group {*access-list-name*| *access-list-number*} {**in**| **out**}

no ip access-group {*access-list-number*| *access-list-name*} {**in**| **out**}

構文の説明

access-list-name	**ip access-list** コマンドで指定された既存の IP アクセスリストまたは OGACL の名前。
access-list-number	既存のアクセス リストの番号。 • 標準または拡張の IP アクセス リストの 1 から 199 の整数。 • 標準または拡張の IP 拡張アクセス リストの 1300 から 2699 の整数。
in	インバウンドパケットに対してフィルタリングします。
out	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

アクセス リストは適用されません。

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（config-if）サービス ポリシーマップ コンフィギュレーション（config-service-policymap）

コマンド履歴

リリース	変更内容
10.0	このコマンドが導入されました。
11.2	引数 *access-list-name* が追加されました。

リリース	変更内容
12.2(28)SB	このコマンドが、サービス ポリシーマップ コンフィギュレーション モードで使用可能になりました。
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。
12.4(20)T	*access-list-name* キーワードが、OGACL の名前を受け入れるように変更されました。
Cisco IOS XE 3.3S	このコマンドが Cisco IOS XE Release 3.3S に統合されました。

使用上のガイドライン

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（警告メッセージは発行されません）。

インターフェイスへのアクセス リストの適用

アクセス リストまたは OGACL は、発信インターフェイスまたは着信インターフェイスに適用されます。 標準着信アクセス リストでは、インターフェイスがパケットを受信すると、Cisco IOS ソフトウェアがパケットの送信元アドレスをアクセス リストと比較して確認します。拡張アクセス リストまたは OGACL の場合は、ネットワーキング デバイスも宛先アクセス リストまたは OGACL を確認します。 アクセス リストまたは OGACL 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 OGACL がアドレスを拒否している場合は、パケットを廃棄し、インターネット制御管理プロトコル（ICMP）ホスト到達不能メッセージを返します。

通常の発信アクセス リストでは、デバイスがパケットを受信して、それを制御されたインターフェイスへ送信した後、ソフトウェアがパケットの送信元アドレスをアクセス リストと比較して確認します。 拡張アクセス リストまたは OGACL の場合は、ネットワーキング デバイスも宛先アクセス リストまたは OGACL を確認します。 アクセス リストまたは OGACL がアドレスを許可した場合、ソフトウェアはパケットを送信します。 アクセス リストまたは OGACL がアドレスを拒否している場合は、パケットを廃棄し、ICMP ホスト到達不能メッセージを返します。

発信アクセス リストまたは OGACL をイネーブルにすると、そのインターフェイスの自律スイッチングは自動的にディセーブルになります。 任意の CBus インターフェイスまたは CxBus インターフェイス上で着信アクセス リストまたは OGACL をイネーブルにすると、すべてのインターフェイスの自律スイッチングが自動的にディセーブルになります（例外：簡易アクセス リストにより設定された Storage Services Enabler（SSE）は、出力に対してのみ、パケットのスイッチングを継続して行えます）。

サービス ポリシー マップへのアクセス リストまたは OGACL の適用

ip access-group コマンドを使用して、Intelligent Services Gateway（ISG）の加入者単位のファイアウォールを設定できます。 加入者単位のファイアウォールは Cisco IOS ACL IP アクセス リストま

たはOGACLであり、加入者、サービス、およびパススルートラフィックが特定のIPアドレスおよびポートにアクセスしないようにするために使用します。

ACLおよびOGACLは、認証、許可、およびアカウンティング（AAA）サーバ上のユーザ プロファイルまたはサービス プロファイル、またはISG上のサービス ポリシー マップで設定できます。 OGACLまたは番号付きまたは名前付きIPアクセス リストはISG上で設定でき、ACLステートメントまたはOGACLステートメントをプロファイル設定に含めることができます。

ACLまたはOGACLをサービスに追加すると、そのサービスのすべての加入者は、そのサービスによる指定されたIPアドレス、サブネットマスク、およびポートの組み合わせにアクセスできなくなります。

例

次に、イーサネット インターフェイス0から発信されるパケットに対して、リスト101を適用する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 0
Router(config-if)# ip access-group 101 out
```

関連コマンド

コマンド	説明
deny	名前付きIPアクセス リストまたはOGACLにおいて、パケットを拒否する条件を設定します。
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。

ip access-list

IP アクセス リストまたはオブジェクト グループ アクセス コントロール リスト（ACL）を名前または番号で定義する、または IP ヘルパー アドレスの宛先を持つパケットのフィルタリングをイネーブルにするには、グローバル コンフィギュレーション モードで **ip access-list** コマンドを使用します。 IP アクセス リストまたはオブジェクト グループ ACL を削除する、または IP ヘルパー アドレスの宛先を持つパケットのフィルタリング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。

ip access-list {{**standard**| **extended**} {*access-list-name*| *access-list-number*}| **helper egress check**}

no ip access-list {{**standard**| **extended**} {*access-list-name*| *access-list-number*}| **helper egress check**}

構文の説明

standard	標準 IP アクセス リストを指定します。
extended	拡張 IP アクセス リストを指定します。 オブジェクト グループ ACL に必要です。
access-list-name	IP アクセス リストまたはオブジェクト グループ ACL の名前。 名前には、スペースまたは引用符を含めることができず、番号付けされたアクセスリストと混乱しないように、英文字で始める必要があります。
access-list-number	アクセス リスト番号。 • 標準 IP アクセス リストの範囲は、1 ～ 99 または 1300 ～ 1999 です。 • 拡張 IP アクセス リストの範囲は、100 ～ 199 または 2000 ～ 2699 です。
helper egress check	IP ヘルパー機能によって宛先サーバ アドレスにリレーされるトラフィックに対して、インターフェイスに適用される発信アクセス リストの照合機能の許可または拒否をイネーブルにします。

コマンド デフォルト

IP アクセス リストまたはオブジェクト グループ ACL は定義されないため、発信 ACL は IP ヘルパーによってリレーされるトラフィックを照合またはフィルタリングしません。

コマンド モード

グローバル コンフィギュレーション（config）

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。
12.2(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。
12.4(20)T	このコマンドが変更されました。 **deny** コマンドおよび **permit** コマンドが標準 IP アクセスリスト コンフィギュレーション モードまたは拡張 IP アクセスリスト コンフィギュレーション モードで使用されている場合に、オブジェクト グループ ACL が受け入れられるようになりました。
Cisco IOS XE Release 3.2S	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。
15.0(1)M5	このコマンドが変更されました。 **helper**、**egress**、および**check** キーワードが追加されました。
15.1(1)SY	このコマンドが変更されました。 **helper**、**egress**、および**check** キーワードが追加されました。
15.1(3)T3	このコマンドが変更されました。 **helper**、**egress**、および**check** キーワードが追加されました。
15.1(2)SNG	このコマンドが、Cisco ASR 901 シリーズの集約サービス ルータに実装されました。

使用上のガイドライン

名前付きまたは番号付き IP アクセス リストまたはオブジェクト グループ ACL を設定するには、このコマンドを使用します。 このコマンドにより、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。その場合は、**deny** コマンドおよび **permit** コマンドを使用して、拒否または許可されるアクセス条件を定義する必要があります。

ip access-list コマンドで **standard** キーワードまたは **extended** キーワードを指定すると、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たときに表示されるプロンプトが決定されます。オブジェクトグループACLを定義する場合は、**extended**キーワードを使用する必要があります。

オブジェクト グループおよびIPアクセス リストまたはオブジェクト グループACLは単独で作成できます。つまり、まだ存在していないオブジェクト グループ名を使用できます。

名前付きアクセス リストは、リリース 11.2 以前の Cisco IOS ソフトウェア リリースと互換性がありません。

ip access-group コマンドを使用して、アクセス リストをインターフェイスに適用します。

ip access-list helper egress check コマンドは、IP ヘルパー アドレス宛先を持つパケットの許可機能または拒否機能の発信 ACL 照合をイネーブルにします。 このコマンドとともに発信拡張 ACL を使用すると、送信元または宛先のユーザ データグラム プロトコル（UDP）ポートに基づいて IP ヘルパーによってリレーされたトラフィックを許可または拒否できます。 **ip access-list helper egress check** コマンドは、デフォルトでディセーブルです。出力 ACL は IP ヘルパーによってリレーされたトラフィックを照合およびフィルタリングしません。

例

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

```
Router> enable
Router# configure terminal
Router(config)# ip access-list standard Internetfilter
Router(config-std-nacl)# permit 192.168.255.0 0.0.0.255
Router(config-std-nacl)# permit 10.88.0.0 0.0.255.255
Router(config-std-nacl)# permit 10.0.0.0 0.255.255.255
```

次に、プロトコル ポートが my_service_object_group で指定されたポートと一致した場合に、my_network_object_group のユーザからのパケットを許可するオブジェクト グループ ACL 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)# permit tcp object-group my_network_object_group portgroup
 my_service_object_group any
Router(config-ext-nacl)# deny tcp any any
```

次に、ヘルパー アドレスの宛先を持つパケットの発信 ACL フィルタリングをイネーブルにする例を示します。

```
Router> enable
Router# configure terminal
Router(config)# ip access-list helper egress check
```

関連コマンド

コマンド	説明
deny	パケットを拒否する名前付き IP アクセス リストまたはオブジェクト グループ ACL の条件を設定します。
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 またはオブジェクト グループ ACL を適用します。
object-group network	オブジェクト グループ ACL 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	オブジェクト グループ ACL 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。

コマンド	説明
permit	パケットを許可する名前付き IP アクセス リストまたはオブジェクト グループ ACL の条件を設定します。
show ip access-list	IP アクセス リストまたはオブジェクト グループ ACL 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。

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するには、グローバル コンフィギュレーション モードで **ip access-list resequence** コマンドを使用します。

ip access-list resequence *access-list-name* **starting-sequence-number** *increment*

構文の説明

access-list-name	アクセス リストの名前。 名前にスペースや引用符を含めることはできません。
starting-sequence-number	アクセス リストのエントリは、この初期値を使用して、並べ直されます。 デフォルト値は 10 です。 可能なシーケンス番号の範囲は 1 ～ 2147483647 です。
increment	シーケンス番号が変更される幅の数値。 デフォルト値は 10 です。 たとえば、increment 値が 5 で開始シーケンス番号が 20 の場合、以降のシーケンス番号は 25、30、35、40 と続きます。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(14)S	このコマンドが導入されました。
12.2(15)T	このコマンドが、Cisco IOS Release 12.2(15)T 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

このコマンドにより、指定されたアクセス リストの **permit** エントリおよび **deny** エントリを、*starting-sequence-number* 引数により決定され初期シーケンス番号値で並べ直すことができ、これは、*increment* 引数に決定された増分により増え続けます。最も大きいシーケンス番号が使用可能な最大シーケンス番号を超える場合は、シーケンシングが発生しません。

以前のリリースとの下位互換性を保つため、シーケンス番号のないエントリが適用された場合には、最初のエントリにはシーケンス番号 10 が割り当てられます。連続してエントリを追加すると、シーケンス番号は 10 ずつ増分されます。 最大シーケンス番号は 2147483647 です。 生成したシーケンス番号がこの最大値を超えると、次のメッセージが表示されます。

```
Exceeded maximum sequence number.
```

シーケンス番号のないエントリを入力すると、アクセス リストの最後のシーケンス番号に 10 を加えたシーケンス番号が割り当てられ、リストの末尾に配置されます。

（シーケンス番号以外が）既存のエントリに一致するエントリを入力すると、何も変更されません。

既存のシーケンス番号を入力すると、次のエラー メッセージが表示されます。

```
Duplicate sequence number.
```

グローバル コンフィギュレーション モードで新しいアクセス リストを入力すると、そのアクセス リストのシーケンス番号が自動的に生成されます。

分散サポートが提供されます。ルート プロセッサ（RP）とラインカード（LC）にあるエントリのシーケンス番号は、常に同期されます。

シーケンス番号は NVRAM に保存されません。 つまり、シーケンス番号自体は保存されません。システムのリロード時には、設定されたシーケンス番号はデフォルトのシーケンス開始番号と増分に戻されます。

このコマンドは、名前付きの標準および拡張 IP アクセス リストと連動します。 アクセス リストの名前は番号として指定できるため、番号、名前付きアクセス リスト コンフィギュレーション モードで入力されている限り、番号を名前として使用できます。

例

次に、kmd1 という名前のアクセス リストを並べ直す例を示します。 開始シーケンス番号は 100、増分値は 5 です。

```
ip access-list resequence kmd1 100 5
```

関連コマンド

コマンド	説明
deny（IP）	パケットが名前付き IP アクセス リストを通過しない条件を設定します。

コマンド	説明
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。

ip admission

インターフェイスに適用されるレイヤ 3 ネットワーク アドミッション コントロール ルールを作成する、または認証、許可、アカウンティング（AAA）サーバが到達不能な場合にインターフェイスに適用できるポリシーを作成する場合は、インターフェイス コンフィギュレーション モードで **ip admission** コマンドを使用します。ネットワーク アクセス デバイスに適用できるグローバル ポリシーを作成するには、グローバル コンフィギュレーション モードで**任意のキーワード**および引数**を指定して ip admission コマンド**を使用します。アドミッション コントロール ルールを削除するには、このコマンドの **no** 形式を使用します。

ip admission *admission-name* [**event timeout aaa policy identity** *identity-policy-name*]

no ip admission *admission-name* [**event timeout aaa policy identity** *identity-policy-name*]

構文の説明

admission-name	認証ルールまたは許可ルールの名前。
event timeout aaa policy identity	AAA サーバが到達不能である場合に適用される認証ポリシーを指定します。
identity-policy-name	AAA サーバが到達不能の場合に適用される認証ルールまたは許可ルールの名前。

コマンド デフォルト

ネットワーク アドミッション コントロール ルールは、インターフェイスには適用されません。

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（config）グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.3(8)T	このコマンドが導入されました。
12.4(11)T	このコマンドが、**event timeout aaa policy identity** キーワードおよび *identity-policy-name* 引数を含むように変更されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。

使用上のガイドライン

許可ルールは、アドミッション コントロールを適用する方法を定義します。

任意のキーワードおよび引数は、AAA サーバが到達不能な場合にネットワーク アクセス デバイスまたはインターフェイスに適用されるネットワーク アドミッション ポリシーを定義します。このコマンドを使用して、デフォルトのアイデンティティ ポリシーを Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）セッションに関連付けることができます。

例

次に、「nacrule1」という名前のネットワーク アドミッション コントロール ルールをインターフェイスに適用する例を示します。

```
Router (config-if)# ip admission nacrule1
```

次に、AAA サーバが到達不能な場合に「example」という名前のアイデンティティ ポリシーをデバイスに適用する例を示します。

```
Router (config)# ip admission nacrule1 event timeout aaa policy identity example
```

関連コマンド

コマンド	説明
interface	インターフェイスを定義します。

ip admission proxy http

Web ベース認証中のカスタム認証プロキシ Web ページの表示を指定するには、グローバル コンフィギュレーション モードで **ip admission proxy http** コマンドを使用します。 デフォルトの Web ページの使用を指定するには、このコマンドの **no** 形式を使用します。

ip admission proxy http {{**login**| **success**| **failure**| **login expired**} **page file** *device:file-name*| **success redirect** *url*}

no ip admission proxy http {{**login**| **success**| **failure**| **login expired**} **page file** *device:file-name*| **success redirect** *url*}

構文の説明

login	ログイン時に表示される、ローカルに保存された Web ページを指定します。
success	ログインが成功した場合に表示される、ローカルに保存された Web ページを指定します。
failure	ログインが失敗した場合に表示される、ローカルに保存された Web ページを指定します。
login expired	ログインが期限切れになった場合に表示される、ローカルに保存された Web ページを指定します。
device	カスタム HTML ファイルが保存されているスイッチのメモリ ファイル システムのディスクまたはフラッシュ メモリを指定します。
file-name	指定した条件において、デフォルトの HTML ファイルの代わりに使用するカスタム HTML ファイルの名前を指定します。
success redirect *url*	ログインが成功した場合に表示される、外部 Web ページを指定します。

コマンド デフォルト

Web ベース認証時には、デフォルトの内部認証プロキシ Web ページが表示されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。

使用上のガイドライン

カスタマイズされた認証プロキシ Web ページの使用を設定する場合は、次の注意事項を考慮してください。

- カスタム Web ページ機能をイネーブルにするには、4 つのすべてのカスタム HTML ファイルを指定する必要があります。 4 つ未満のファイルが指定されている場合は、内部デフォルト HTML ページが使用されます。
- この 4 つのカスタム HTML ファイルはスイッチのディスクまたはフラッシュに存在している必要があります。 各 HTML ファイルの最大サイズは 8 KB です。
- カスタム ページ上のイメージは、アクセス可能な HTTP サーバ上になければなりません。 HTTP サーバにアクセスできるように、アドミッション ルール内に代行受信 ACL を設定する必要があります。
- カスタム ページからのすべての外部リンクでは、アドミッション ルール内で代行受信 ACL を設定する必要があります。
- 外部リンクまたは画像に必要なすべての名前解決では、有効な DNS サーバにアクセスするためにアドミッション ルール内で代行受信 ACL を設定する必要があります。
- カスタム Web ページ機能がイネーブルである場合、設定された auth-proxy-banner は使用されません。
- カスタム Web ページ機能がイネーブルである場合、成功ログイン機能のリダイレクション URL は利用不可能です。
- カスタム ログイン ページはパブリック Web 形式であるため、このページについて次の注意事項に留意してください。
  - ログイン形式では、ユーザ名およびパスワードのユーザ入力を受け入れて、そのデータを uname および pwd として POST する必要があります。
  - カスタム ログイン ページは、ページ タイムアウト、暗号化されたパスワード、冗長送信の防止など、Web フォームに対するベスト プラクティスに従う必要があります。
- ログイン成功時のリダイレクション URL を設定する場合、次の注意事項に従ってください。
  - カスタム認証プロキシ Web ページ機能がイネーブルである場合、リダイレクション URL 機能はディセーブルに設定され、CLI で利用できなくなります。 リダイレクションはカスタム ログイン成功ページ内で実行できます。
  - リダイレクション URL 機能がイネーブルである場合、設定された auth-proxy-banner は使用されません。

例

次に、カスタム認証プロキシ Web ページを設定する例を示します。

```
Router(config)# ip admission proxy http login page file disk1:login.htm
Router(config)# ip admission proxy http success page file disk1:success.htm
Router(config)# ip admission proxy http fail page file disk1:fail.htm
Router(config)# ip admission proxy http login expired page file disk1:expired.htm
```

次に、カスタム認証プロキシ Web ページの設定を確認する例を示します。

```
Router# show ip admission configuration
Authentication proxy webpage
 Login page          : disk1:login.htm
 Success page        : disk1:success.htm
 Fail Page           : disk1:fail.htm
 Login expired Page : disk1:expired.htm
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

次に、ログイン成功時のリダイレクション URL を設定する例を示します。

```
Router(config)# ip admission proxy http success redirect www.example.com
```

次に、ログイン成功時のリダイレクション URL を確認する例を示します。

```
Router# show ip admission configuration
Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.example.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

関連コマンド

コマンド	説明
ip http server ip https server	スイッチ内の HTTP サーバをイネーブルにします。
show ip admission configuration	Web ベース認証 IP アドミッションの設定を表示します。

ip device tracking probe

デバイス プローブのトラッキングをイネーブルにするには、コンフィギュレーション モードで **ip device tracking probe** コマンドを使用します。 デバイス プローブ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。

ip device tracking probe {**count** *count*| **delay** *delay*| **interval** *interval*}

構文の説明

count *count*	1 ～ 5 の IP トラッキング プローブの数を指定します。
delay *delay*	1 ～ 120 秒の IP トラッキング プローブの遅延時間を指定します。
interval *interval*	30 ～ 300 分の IP トラッキング プローブの間隔を指定します。

コマンド デフォルト

デバイス プローブ トラッキングはディセーブルです。

コマンド モード

コンフィギュレーション モード（config #）

コマンド履歴

リリース	変更内容
12.2(33)SXI7	このコマンドが導入されました。

例

次に、プローブの数を 5 に設定する例を示します。

```
Router(config)# ip device tracking probe count 5
```

次に、遅延時間を 60 に設定する例を示します。

```
Router(config)# ip device tracking probe delay 60
```

次に、間隔を 35 に設定する例を示します。

```
Router(config)# ip device tracking probe interval 35
```

関連コマンド

コマンド	説明
show ip device tracking	IP デバイス トラッキング テーブル内のエントリに関する情報を表示します。

ip scp server enable

ip scp server enable

ルータがリモート ワーク ステーションからファイルを安全にコピーできるようにするには、グローバル コンフィギュレーション モードで **ip scp server enable** を使用します。 セキュア コピー機能（デフォルト）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。

ip scp server enable

no ip scp server enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

セキュア コピー機能はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)S	このコマンドが Cisco IOS Release 12.0(21)S に統合され、Cisco 7500 シリーズ ルータおよび Cisco 12000 シリーズ ルータのサポートが追加されました。
12.2(18)SXD	このコマンドが、Cisco IOS Release 12.2(18)SXD に統合されました。
12.2(25)S	このコマンドが Cisco IOS Release 12.2(15)S に統合されました。
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。

使用上のガイドライン

Secure Shell（SSH）アプリケーションを使用したシステムからのファイルのセキュア コピーをイネーブルにするには、このコマンドを使用します。 このセキュア コピー機能は、Cisco IOS ソフトウェアの **copy** コマンドに追加することにより行われます。これにより、ルータ自体へのログイン中に、ルータとの間でのコピーするためのセキュア コピー プロトコル（scp）の使用が処理されます。 通常、ファイルのコピーは Cisco IOS ソフトウェアでは制限された操作であるため、こうしたファイルをコピーしようとしているユーザは正しいイネーブル レベルである必要があります。

また、Cisco IOS ソフトウェアにおいて、（Microsoft Windows および UNIX オペレーティング システムの両方でサポートされている）SSH アプリケーションを実行しているリモート ワークステーションと Cisco IOS ソフトウェア自体の間でのファイルのコピーを可能にする必要もあります。 この情報を取得するには、Cisco IOS ソフトウェアにおいて、認証、許可、アカウンティング（AAA）機能の認証および許可が設定されている必要があります。 SSH ではすでに AAA 認証に依存することにより、ユーザのユーザ名とパスワードが認証されます。 scp は、ユーザが正しい権限レベルにあるかをオペレーティング システムが判断できるように、AAA 認証をオンにする要件を追加します。

例

次に、ルータでリモートのワークステーションからファイルを安全にコピーできる一般的な設定の例を示します。 scp は適切に機能するために AAA 認証および許可に依存しているため、AAA を設定する必要があります。

```
aaa new-model
aaa authentication login default tac-group tacacs+
aaa authorization exec default local
username user1 privilege 15 password 0 lab
ip scp server enable
```

次に、scp を使用して SSH をサポートするフラッシュ メモリから SSH をサポートするサーバにシステム イメージをコピーする例を示します。

```
Router# copy flash:c4500-ik2s-mz.scp scp://user1@host1/
Address or name of remote host [host1]?
Destination username [user1]?
Destination filename [c4500-ik2s-mz.scp]?
Writing c4500-ik2s-mz.scp
Password:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

（注） scp を使用する場合、**copy** コマンドにパスワードを入力できません。プロンプトが表示された場合にパスワードを入力します。

関連コマンド

コマンド	説明
aaa authentication login	ログイン時の AAA 認証を設定します。
aaa authorization	ネットワークへのユーザ アクセスを制限するパラメータを設定します。
copy	コピー元からコピー先に任意のファイルをコピーします。
debug ip scp	scp 認証問題を解決します。
ip ssh port	tty 回線へのセキュア ネットワーク アクセスをイネーブルにします。

コマンド	説明
username	ユーザ名をベースとした認証システムを構築します。

ip ssh ～ ipv6 tacacs source-interface

ip ssh

ルータ上で Secure Shell（SSH）コントロール パラメータを設定するには、グローバル コンフィギュレーション モードで **ip ssh** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ip ssh [**timeout** *seconds*| **authentication-retries** *integer*]

no ip ssh [**timeout** *seconds*| **authentication-retries** *integer*]

構文の説明

timeout	（任意）SSH クライアントが応答するまでルータが待機する時間間隔。 この設定は、SSH ネゴシエーション フェーズに適用されます。 EXEC セッションが開始すると、vty に設定された標準のタイムアウトが適用されます。デフォルトでは、定義された 5 つの vty（0 ～ 4）があります。したがって、5 つのターミナル セッションが可能です。 SSH でシェルが実行されると、vty タイムアウトが始動します。 vty タイムアウトのデフォルトは 10 分です。
seconds	（任意）最大 120 秒のタイムアウト切断までの秒数。 デフォルトは 120 秒です。
authentication- retries	（任意）インターフェイスがリセットされるまでの試行回数。
integer	（任意）最大 5 回の認証再試行の再試行回数。デフォルトは 3 です。

コマンド デフォルト

SSH コントロール パラメータはルータのデフォルトの値に設定されます。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.0(5)S	このコマンドが導入されました。

リリース	変更内容
12.1(1)T	このコマンドが、Cisco IOS Release 12.1(1)T に統合されました。
12.2(17a)SX	このコマンドが、Cisco IOS Release 12.2(17a) SX に統合されました。
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。
Cisco IOS XE Release 2.4	このコマンドが、Cisco ASR 1000 シリーズ ルータに実装されました。

使用上のガイドライン

ルータ上でSSHを設定する前に、**crypto key generate rsa** コマンドを使用してSSHサーバをイネーブルにする必要があります。

例

次に、ルータ上で SSH コントロール パラメータを設定する例を示します。

```
ip ssh timeout 120
ip ssh authentication-retries 3
```

ip ssh dh min size

Secure Shell（SSH）サーバ上でモジュラス サイズを設定するには、特権 EXEC モードで **ip ssh dh min size** コマンドを使用します。 設定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。

ip ssh dh min size [*number*]

no ip ssh dh min size

構文の説明

number	（任意）キー サイズの最小ビット数。 デフォルトは 1024 です。

コマンド デフォルト

ビット キーのサポートはディセーブルです。

コマンド モード

特権 EXEC（#）

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。
15.1(2)S	このコマンドが Cisco IOS Release 15.1(2)S に統合されました。

使用上のガイドライン

CLI がクライアント側またはサーバ側から正常に解析されたことを確認するには、**ip ssh dh min size** コマンドを使用します。

例

次に、最小モジュラス サイズを 2048 ビットに設定する例を示します。

```
Router> enable
Router# ip ssh dh min size 2048
```

関連コマンド

コマンド	説明
show ip ssh	SSH サーバ接続のステータスを表示します。

ip ssh dscp

Secure Shell（SSH）設定に対して設定できる IP DiffServ コード ポイント（DSCP）値を指定するには、グローバル コンフィギュレーション モードで **ip ssh dscp** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ip ssh dscp *number*

no ip ssh dscp *number*

構文の説明

number	設定できる値。 デフォルト値は 0（ゼロ）です。 • *number*：0 ～ 63。

コマンド デフォルト

IP DSCP 値は指定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.4(20)S	このコマンドが導入されました。
12.2SR	このコマンドは、Cisco IOS Release 12.2SR トレインでサポートされます。特定の 12.2SR トレイン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。
12.2SX	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。特定の 12.2SX トレイン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	このコマンドが Cisco IOS Release 12.4(22)T に統合されました。

使用上のガイドライン

IP DSCP 値は、いずれかの端で生成された SSH トラフィックの SSH クライアントおよび SSH サーバの両方で設定できます。

例

次に、DSCP 値を 35 に設定する例を示します。

```
Router(config)# ip ssh dscp 35
```

関連コマンド

コマンド	説明
ip ssh precedence	設定できる IP precedence 値を指定します。

ip ssh pubkey-chain

SSH サーバ上でのユーザおよびサーバ認証の Secure Shell RSA（SSH-RSA）キーを設定するには、グローバル コンフィギュレーション モードで **ip ssh pubkey chain** コマンドを使用します。 SSH サーバ上でのユーザおよびサーバ認証の SSH-RSA キーを削除するには、このコマンドの **no** 形式を使用します。

ip ssh pubkey-chain

no ip ssh pubkey-chain

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

SSH-RSA キーは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
15.0(1)M	このコマンドが導入されました。
15.1(1)S	このコマンドが Cisco IOS Release 15.1(1)S に統合されました。

使用上のガイドライン

SSH サーバおよびユーザの公開キー認証を確保するには、**ip ssh pubkey chain** コマンドを使用します。

例

次に、公開キー生成をイネーブルにする例を示します。

```
Router(config)# ip ssh pubkey-chain
```

関連コマンド

コマンド	説明
ip ssh stricthostkeycheck	SSH サーバでの厳密なホスト キー チェックをイネーブルにします。

ip ssh stricthostkeycheck

Secure Shell（SSH）サーバ上での厳密なホスト キー チェックをイネーブルにするには、グローバル コンフィギュレーション モードで **ip ssh stricthostcheck** コマンドを使用します。 厳密なホスト キー チェック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。

ip ssh stricthostkeycheck

no ip ssh stricthostkeycheck

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

SSH サーバでの厳密なホスト キー チェックはイネーブルではありません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
15.0(1)M	このコマンドが導入されました。
15.1(1)S	このコマンドが Cisco IOS Release 15.1(1)S に統合されました。

使用上のガイドライン

SSH サーバ側の厳密なチェックを確保するには、**ip ssh stricthostkeycheck** コマンドを使用します。**ip ssh stricthostkeycheck** コマンドを設定すると、すべてのサーバが認証されます。

（注） このコマンドは、SSH バージョン 1 では使用できません。

- **ip ssh pubkey-chain** コマンドが設定されていない場合、**ip ssh stricthostkeycheck** コマンドを使用すると、SSH バージョン 2 の接続障害につながります。

例

次に、厳密なホスト キー チェックをイネーブルにする例を示します。

```
Router(config)# ip ssh stricthostkeycheck
```

関連コマンド

コマンド	説明
ip ssh pubkey-chain	SSH サーバ上でのユーザおよびサーバ認証の SSH-RSA キーを設定します。

ip ssh version

ルータで実行する Secure Shell（SSH）のバージョンを指定するには、グローバル コンフィギュレーション モードで **ip ssh version** コマンドを使用します。 設定された SSH バージョンをディセーブルにし、互換モードに戻るには、このコマンドの **no** 形式を使用します。

ip ssh version [**1**| **2**]

no ip ssh version [**1**| **2**]

構文の説明

1	（任意）ルータは SSH バージョン 1 のみを実行します。
2	（任意）ルータは SSH バージョン 2 のみを実行します。

コマンド デフォルト

このコマンドを設定しない場合、SSH は互換モードで動作します。つまり、バージョン 1 とバージョン 2 の両方がサポートされます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.3(4)T	このコマンドが導入されました。
12.3(2)XE	このコマンドが、Cisco IOS Release 12.3(2)XE に統合されました。
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。
12.3(7)JA	このコマンドが、Cisco IOS Release 12.3(7)JA に統合されました。
12.0(32)SY	このコマンドが、Cisco IOS Release 12.0(32)SY に統合されました。
12.4(20)T	このコマンドが、Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

ルータが誤ってセキュリティ レベルの低い SSH バージョン 1 接続を確立しないようにするには、**2** キーワードを指定してこのコマンドを使用できます。

例

次に、SSH バージョン 1 のサポートのみを設定する例を示します。

```
Router (config)# ip ssh version 1
```

次に、SSH バージョン 2 のみを設定する例を示します。

```
Router (config)# ip ssh version 2
```

次に、SSH バージョン 1 および SSH バージョン 2 を設定する例を示します。

```
Router (config)# no ip ssh version
```

関連コマンド

コマンド	説明
debug ip ssh	SSH のデバッグ メッセージを表示します。
disconnect ssh	ルータで SSH 接続を終了します。
ip ssh	ルータで SSH コントロール パラメータを設定します。
ip ssh rsa keypair-name	SSH 接続に使用する RSA キー ペアを指定します。
show ip ssh	ルータの SSH 接続を表示します。

ip verify unicast reverse-path

（注） このコマンドは、Cisco IOS Release 12.0(15)S で有効な **ip verify unicast source reachable-via** コマンドに置き換えられました。 **ip verify unicast source reachable-via** コマンドは、非対称ルーティングのサポートなどの高い柔軟性と機能を実現し、すべてのリバース パス転送の実装において使用する必要があります。 **ip verify unicast reverse-path** コマンドは引き続きサポートされます。

ユニキャスト リバース パス転送（ユニキャスト RPF）をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip verify unicast reverse-path** コマンドを使用します。 ユニキャスト RPF 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。

ip verify unicast reverse-path [*list*]

no ip verify unicast reverse-path [*list*]

構文の説明

list	（任意）次の範囲の番号付きアクセス コントロール リスト（ACL）を指定します。 • 1 ～ 99（IP 標準アクセス リスト） • 100 ～ 199（IP 拡張アクセス リスト） • 1300 ～ 1999（IP 標準アクセス リスト、拡張範囲） • 2000 ～ 2699（IP 拡張アクセス リスト、拡張範囲）

コマンド デフォルト

ユニキャスト RPF はディセーブルです。

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（config-if）

コマンド履歴

リリース	変更内容
11.1(CC) 12.0	このコマンドが導入されました。 このコマンドは Cisco IOS Release 11.2 または Cisco IOS Release 11.3 には含まれません。
12.1(2)T	*list* 引数を使用した ACL のサポートを追加しました。 ドロップまたは抑制されたパケットのインターフェイス単位の統計情報を追加しました。
12.0(15)S	**ip verify unicast source reachable-via** コマンドにより、このコマンドが置き換えられ、**allow-default**、**allow-self-ping**、**rx**、および **any** のキーワードが **ip verify unicast source reachable-via** コマンドに追加されました。
12.1(8a)E	**ip verify unicast reverse-path** コマンドが、Cisco IOS Release 12.1（8a）E に統合されました。
12.2(14)S	**ip verify unicast reverse-path** コマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(14)SX	**ip verify unicast reverse-path** コマンドが、Cisco IOS Release 12.2(14)SX に統合されました。
12.2(33)SRA	**ip verify unicast reverse-path** コマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

使用上のガイドライン

ルータが受信した変造または偽造（スプーフィング）された IP 送信元アドレスによって発生する問題を軽減するには、**ip verify unicast reverse-path interface** コマンドを使用します。 変造または偽造された送信元アドレスは、送信元 IP アドレスのスプーフィングに基づくサービス拒否（DoS）攻撃を示している可能性があります。

インターフェイスでユニキャスト RPF をイネーブルにすると、ルータはそのインターフェイスで受信されるすべてのパケットを検査します。 ルータの確認により、送信元アドレスが転送情報ベース（FIB）で表示されること、およびパケットを受信したインターフェイスと一致することが確保されます。 ルックアップは FIB の存在に依存するため、この「後方参照」機能はシスコ エクスプレス フォワーディングがルータでイネーブルになっている場合にだけ使用可能です。 シスコ エクスプレス フォワーディングでは、その動作の一部として FIB が生成されます。

ユニキャスト RPF を使用するには、ルータでシスコ エクスプレス フォワーディング スイッチングまたは分散型シスコ エクスプレス フォワーディング スイッチングをイネーブルにします。 シスコ エクスプレス フォワーディング スイッチングの入力インターフェイスを設定する必要はあ

りません。 シスコ エクスプレス フォワーディングがルータ上で実行されているかぎり、個々のインターフェイスは他のスイッチング モードで設定できます。

（注） ルータでシスコ エクスプレス フォワーディングをグローバルに設定することが非常に重要です。 ユニキャスト RPF は、シスコ エクスプレス フォワーディングがないと動作しません。

（注） ユニキャスト RPF は入力機能であり、入力方向においてのみルータのインターフェイスに適用されます。

ユニキャスト リバース パス転送機能は、ルータ インターフェイスで受信されたパケットが、パケットの送信元への最良リターン パスのいずれかに到達しているかどうかを確認します。 この機能は、シスコ エクスプレス フォワーディング テーブルで逆ルックアップを実行することで、この処理を行います。 ユニキャスト RPF がパケットのリターン パスを見つけることができない場合、ユニキャスト RPF は、ACL がユニキャスト リバース パス転送コマンドで指定されているかどうかに応じてパケットをドロップまたは転送できます。 コマンドで ACL を指定し、パケットがユニキャスト RPF の確認に失敗した場合にのみ、ACL を確認して（ACL で deny ステートメントを使用して）パケットをドロップするか、（ACL で permit ステートメントを使用して）転送するかを参照します。 パケットがドロップされるか転送されるかにかかわらず、パケットは、ユニキャスト RPF ドロップのグローバル IP トラフィック統計情報とユニキャスト RPF のインターフェイス統計情報でカウントされます。

ACL がユニキャスト リバース パス転送コマンドで指定されていない場合、ルータは偽造または変造されたパケットをただちにドロップし、ACL ロギングは行われません。 ルータおよびインターフェイス ユニキャスト RPF カウンタが更新されます。

ユニキャスト RPF イベントは、ユニキャスト リバース パス転送コマンドで使用する ACL エントリのロギング オプションを指定することでロギングできます。 ログ情報を使用して、送信元アドレスや時間など、攻撃に関する情報を収集できます。

ネットワークで RPF を使用する場所

ユニキャスト RPF は、有効な送信元ネットワーク（FIB に含まれているネットワーク）からのパケットを 1 つのパスにおいてのみ許可するインターフェイスで使用できます。 有効なネットワークが着信インターフェイスによってスイッチングされる限り、ユニキャスト RPF は、ルータに特定のネットワークへの複数のパスがある場合にも使用できます。 無効なネットワークのパケットはドロップされます。 たとえば、インターネット サービス プロバイダー（ISP）ネットワークのエッジにあるルータには、対称リバース パスが設定されている可能性があります。 さらに、重みやローカル プリファレンスなどの任意のボーダー ゲートウェイ プロトコル（BGP）属性を使用して、対称ルーティングが実現されていることを条件として、ユニキャスト RPF を特定のマルチホームの状況において適用できる場合もあります。

ユニキャスト RPF では、コストが等しいすべての「最良」リターン パスが有効と見なされます。つまり、複数のリターン パスが存在し、ルーティング コスト（ホップ カウント、重みなど）に関して他のパスと同等で、ルートが FIB に存在する場合、ユニキャスト RPF は機能します。 ユニキャスト RPF は、Enhanced Interior Gateway Routing Protocol（EIGRP）バリアントが使用されていて、送信元 IP アドレスに戻る同等でない候補パスが存在する場合にも機能します。

たとえば、ISP のネットワークのエッジにあるルータは、ISP ネットワークのコアにあるルータよりも対称リバースパスを持つ可能性が高くなります。ISP ネットワークのコアにあるルータでは、ルータからの最良の転送パスがルータへ返されるパケットに対して選択されるパスとなることが保証されません。このシナリオでは、非対称ルーティングの可能性がある場合、コマンドの新しい形式の **ip verify unicast source reachable-via** を使用する必要があります。

例

次に、ユニキャスト リバース パス転送機能がシリアル インターフェイスでイネーブルにされている例を示します。

```
ip cef
! or "ip cef distributed" for RSP+VIP based routers
!
interface serial 5/0/0
 ip verify unicast reverse-path
```

次の例では、ごくシンプルなシングルホームの ISP を使用して、ユニキャスト RPF と併用される入力および出力フィルタの概念について説明します。この例では、ISP が割り当てたクラスレスドメイン間ルーティング（CIDR）ブロック 192.168.202.128/28 を示します。アップストリーム インターフェイスでインバウンドおよびアウトバウンドフィルタの両方があります。ただし、通常の ISP はシングルホームではありません。そのため、（アウトバウンド トラフィックがあるリンクから送出され、別のリンク経由で返送される場合）非対称フローのプロビジョニングを ISP の境界ルータ上のフィルタに設計する必要があります。

```
ip cef distributed
!
interface Serial 5/0/0
 description Connection to Upstream ISP
 ip address 192.168.200.225 255.255.255.255
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip verify unicast reverse-path
 ip access-group 111 in
 ip access-group 110 out
!
access-list 110 permit ip 192.168.202.128 10.0.0.31 any
access-list 110 deny ip any any log
access-list 111 deny ip host 10.0.0.0 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 10.0.0.0 255.255.255.255 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 192.168.0.0 255.255.255.255 any log
access-list 111 deny ip 209.165.202.129 10.0.0.31 any log
access-list 111 permit ip any any
```

次に、ユニキャスト RPF に ACL とロギングを使用する例を示します。この例では、拡張 ACL 197 に、特定のアドレス範囲についてネットワーク トラフィックを拒否または拒否するエントリが設定されています。ユニキャスト RPF はイーサネット インターフェイス 0 に設定され、そのインターフェイスに到達するパケットを確認します。

たとえば、192.168.201.10 の送信元アドレスを持つパケットがイーサネット インターフェイス 0 に到達すると、ACL 197 の deny ステートメントのためにドロップされます。この場合、ACL 情報はロギングされます（この ACL エントリではロギング オプションが有効です）。また、ドロップされたパケットはインターフェイスごと、または全体としてカウントされます。192.168.201.100 の送信元アドレスを持つパケットがイーサネット インターフェイス 0 に到達すると、ACL 197 の permit ステートメントのために転送されます。ドロップまたは抑制されたパケットに関する ACL

情報は、ログ サーバにロギングされます（この ACL エントリではロギング オプションが有効です）。

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.255
 ip verify unicast reverse-path 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.255
!
access-list 197 deny   ip 192.168.201.0 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 10.0.0.63 any log-input
access-list 197 deny   ip 192.168.201.128 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 10.0.0.63 any log-input
access-list 197 deny ip host 10.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 255.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 192.168.0.0 255.255.255.255 any log-input
```

関連コマンド

コマンド	説明
ip cef	ルート プロセッサ カードでシスコ エクスプレス フォワーディングをイネーブルにします。

ipv6 tacacs source-interface

TACACS パケットの送信元アドレスに使用するインターフェイスを指定するには、グローバル コンフィギュレーション モードで **ipv6 tacacs source-interface** コマンドを使用します。 コンフィギュレーションから指定したインターフェイスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 tacacs source-interface *interface*

no ipv6 tacacs source-interface *interface*

構文の説明

interface	TACACS パケットの送信元アドレスに使用するインターフェイス。

コマンド デフォルト

インターフェイスは指定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

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

ipv6 tacacs source-interface コマンドは、TACACS パケットの送信元アドレスに使用するインターフェイスを指定します。

例

次に、TACACS パケットの送信元アドレスとして使用するギガビットイーサネットインターフェイスを設定する例を示します。

```
Router(config)# ipv6 tacacs source-interface GigabitEthernet 0/0/0
```

関連コマンド

コマンド	説明
tacacs server	IPv6 または IPv4 に対して TACACS+ サーバを設定して、TACACS+ サーバ コンフィギュレーション モードを開始します。

K ～ L

key（config-radius-server）

ルータと RADIUS サーバ間のすべての RADIUS 通信用の認証および暗号キーを指定するには、RADIUS サーバ コンフィギュレーション モードで **key** コマンドを使用します。 設定したキーを削除するには、このコマンドの **no** 形式を使用します。

key {**0** *string*| **7** *string*} *string*

no key

構文の説明

0 *string*	暗号化されていないキーが後ろに続くよう指定します。 暗号化されていない（クリアテキスト）共有キー。
7 *string*	非公開のキーが後ろに続くよう指定します。 非公開の共有キー。
string	暗号化されていない（クリアテキスト）共有キー。

コマンド デフォルト

認証および暗号キーはディセーブルになります。

コマンド モード

RADIUS サーバ コンフィギュレーション（config-radius-server）

コマンド履歴

リリース	変更内容
15.2(2)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

aaa new-model コマンドを使用して認証、許可、アカウンティング（AAA）認証をイネーブルにした後、**radius server key** コマンドを使用して認証および暗号キーを設定する必要があります。

（注） **aaa new-model** コマンドを実行後、RADIUS キーを指定します。

入力したキーは、RADIUS サーバで使用されるキーと一致する必要があります。 先頭のスペースはすべて無視されますが、キーの中間および末尾のスペースは使用できます。 キーにスペースを使用する場合、引用符をキーに含める場合を除き、引用符でキーを囲まないでください。

例

次に、IP アドレス 192.0.2.2 を持つホストを RADIUS サーバとして指定し、暗号キーとして rad123 を設定する例を示します。

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2
Device(config-radius-server)# key rad123
```

次に、認証および暗号キーを anykey に設定する例を示します。 7 は、非公開のキーが後ろに続くよう指定します。

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2
Device(config-radius-server)# key 7 anykey
```

設定を保存し、**show running-config** コマンドを使用すると、次のように暗号キーが表示されます。

```
Device# show running-config

radius server myserver
  address ipv4 192.0.2.2
  key 7 19283103834782sda
! The leading 7 indicates that the following text is encrypted.
```

関連コマンド

コマンド	説明
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
address ipv4	RADIUS サーバのアカウンティングおよび認証パラメータの IPv4 アドレスを設定します。
radius server	RADIUS サーバ設定の名前を指定し、RADIUS サーバ コンフィギュレーション モードを開始します。
show running-config	ルーティング デバイスの現在の設定を表示します。

key（TACACS+）

TACACS+ サーバでサーバ単位の暗号キーを設定するには、TACACS+ サーバ コンフィギュレーション モードで **key** コマンドを使用します。 サーバ単位の暗号キーを削除するには、このコマンドの **no** 形式を使用します。

key [**0**| **7**] *key-string*

no key [**0**| **7**] *key-string*

構文の説明

0	（任意）暗号化されていないキーが後ろに続くよう指定します。
7	（任意）非公開のキーが後ろに続くよう指定します。
key-string	非暗号化共有キー。

コマンド デフォルト

TACACS+ 暗号キーは設定されません。

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

key コマンドで、サーバ単位の暗号キーを設定することができます。

例

次に、key1 という名前の非暗号化共有キーを指定する例を示します。

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# key 0 key1
```

関連コマンド

コマンド	説明
tacacs server	IPv6 または IPv4 に対して TACACS+ サーバを設定して、TACACS+ サーバ コンフィギュレーション モードを開始します。

key-hash

セキュア シェル（SSH）Rivest、Shamir、およびAdleman（RSA）キータイプおよび名前を指定するには、SSH公開キー コンフィギュレーション モードで、**key-hash** コマンドを使用します。 SSH Rivest、Shamir、および Adleman（RSA）公開キーを削除するには、このコマンドの **no** 形式を使用します。

key-hash *key-type key-name*

no key-hash [*key-type key-name*]

構文の説明

key-type key-name	SSH RSA 公開キーのタイプと名前。

コマンド デフォルト

SSH キーのタイプと名前は指定されません。

コマンド モード

SSH 公開キー コンフィギュレーション（conf-ssh-pubkey-user）

コマンド履歴

リリース	変更内容
12.2(33)SRA	このコマンドは、Cisco IOS Release 12.(33)SRA よりも前のリリースに導入されました。

使用上のガイドライン

秘密キー-公開キー ペアの設定では、キー タイプを **ssh-rsa** にする必要があります。 公開キー ストリングのハッシュを計算するには、ハッシュ処理ソフトウェアを使用します。また、別のCisco IOS ルータからのハッシュ値をコピーすることもできます。 公開キー データを最初に入力するには、**key-string** コマンドを使用することが推奨されます。

例

次に、SSH キー タイプおよび名前を指定する例を示します。

```
Router(config)# ip ssh pubkey-chain
Router(conf-ssh-pubkey)# username test
Router(conf-ssh-pubkey-user)# key-hash ssh-rsa key1
Router(conf-ssh-pubkey-user))# exit
Router(config-pubkey)# exit
Router(config)# exit
```

関連コマンド

コマンド	説明
key-string	リモート ピアの SSH RSA 公開キーを指定します。

load-balance（server-group）

名前付き RADIUS サーバ グループに対して RADIUS サーバ ロード バランシングをイネーブルにするには、サーバ グループ コンフィギュレーション モードで load-balance コマンドを使用します。 名前付き RADIUS サーバ ロード バランシング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。

load-balance method least-outstanding [**batch-size** *number*] **[ignore-preferred-server]**

no load-balance

構文の説明

method least-outstanding	ロードバランシングの最少アウトスタンディング モードをイネーブルにします。
batch-size	（任意）バッチごとに割り当てられるトランザクションの数。
number	（任意）バッチのトランザクションの数。 • デフォルトは 25 です。 • 範囲は 1 ～ 2147483647 です。 （注） バッチ サイズがスループットと CPU の負荷に影響する場合があります。デフォルト バッチ サイズの 25 の使用を推奨します。これは、CPU の負荷に悪影響を及ぼさない、高スループットに最適化されているためです。
ignore-preferred-server	（任意）認証、許可、アカウンティング（AAA）の単一セッションに関連するトランザクションが、同一サーバを使用しようとしているかどうかを示します。 • 設定されている場合は、優先サーバ設定は使用されません。 • デフォルトは優先サーバを使用することです。

コマンド デフォルト

このコマンドを設定しない場合、名前付き RADIUS サーバ ロード バランシングは発生しません。

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。
12.4(11)T	このコマンドが Cisco IOS Release 12.4(11)T に統合されました。
12.2(33)SRC	このコマンドが、Cisco IOS Release 12.2(33)SRC に統合されました。

例

次の例は、名前付き RADIUS サーバ グループに対して有効にされたロード バランシングを示しています。 この例は、RADIUS コマンド出力の現在の設定、デバッグ出力、および AAA サーバ ステータス情報の 3 つの部分からなります。

例

次の例は、関連する RADIUS 設定を示しています。

```
Router# show running-config
.
.
.
aaa group server radius server-group1
 server 192.0.2.238 auth-port 2095 acct-port 2096
 server 192.0.2.238 auth-port 2015 acct-port 2016
 load-balance method least-outstanding batch-size 5
!
aaa authentication ppp default group server-group1
aaa accounting network default start-stop group server-group1
.
.
.
```

上記 RADIUS コマンド出力の現行設定内の行は、次のように定義されています。

- **aaa group server radius** コマンドは、2 つのメンバー サーバからなるサーバ グループの設定を表示します。
- **load-balance** コマンドは、バッチ サイズが指定されたグローバル RADIUS サーバ グループに対してロード バランシングをイネーブルにします。
- **aaa authentication ppp** コマンドは、RADIUS を使用してすべての PPP ユーザを認証します。
- **aaa accounting** コマンドは、クライアントが認証された後と start-stop キーワードを使用した切断後に、AAA サーバに対するすべてのアカウンティング要求の送信をイネーブルにします。

例

下のデバッグ出力は、上の設定に関する優先サーバの選択と要求の処理を示しています。

```
Router#
```

```
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):Server (192.0.2.238:2015,2016) now being
 used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000032):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
.
.
.
```

名前付き RADIUS サーバ グループのサーバ ステータス情報の例

下の出力は、名前付き RADIUS サーバ グループ設定例の AAA サーバ ステータスを示しています。

```
Router# show aaa servers
RADIUS:id 8, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
```

```
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
RADIUS:id 9, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
Router#
```

この出力は、2 つの RADIUS サーバのステータスを示しています。 両方のサーバが動作中ですが、カウンタが 0 分前にクリアされて以降は、どの要求も処理されていません。

関連コマンド

コマンド	説明
debug aaa sg-server selection	ルータ内の RADIUS および TACACS+ サーバグループ システムが特定のサーバを選択している理由を表示します。
debug aaa test	RADIUS ロードバランシングのため、アイドルタイマーまたはデッドタイマーが期限切れになる時間を示します。
radius-server host	ロード バランシング用の RADIUS 自動テストをイネーブルにします。
radius-server load-balance	グローバル RADIUS サーバ グループに対して RADIUS サーバ ロード バランシングをイネーブルにします。
test aaa group	RADIUS ロード バランシング サーバ応答を手動でテストします。