retries コマンド～ rtp-min-port rtp-max-port コマンド

retries

ASA が応答を受信しないときに、DNS サーバのリストに再試行する回数を指定するには、グローバル コンフィギュレーション モードで **dns retries** 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。

retries *number*

no retries [*number*]

構文の説明

number	再試行回数を 0 ～ 10 の範囲で指定します。デフォルトは 2 です。

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

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

name-server コマンドを使用して DNS サーバを追加します。

dns name-server コマンドがこのコマンドに置き換えられました。

例

次に、再試行回数を 0 回に設定する例を示します。ASA は各サーバへの要求を 1 回のみ行います。

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# dns retries 0
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループ モードを開始します。
show running-config dns server-group	既存の DNS サーバ グループ コンフィギュレーションのうちの 1 つまたはすべてを表示します。

retry-count

クラウド Web セキュリティ プロキシ サーバに対するポーリングに連続して失敗した場合にサーバが到達不能であると見なす回数の値を設定するには、scansafe 汎用オプション コンフィギュレーション モードで **retry-count** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

retry-count *value*

no retry-count [*value*]

構文の説明

value	再試行回数の値（2 ～ 100）を入力します。デフォルトは 5 分です。

コマンド デフォルト

デフォルト値は 5 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
scansafe 汎用オプション コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

Cisco Cloud Web Security サービスに登録すると、プライマリ クラウド Web セキュリティ プロキシ サーバとバックアップ プロキシ サーバが割り当てられます。

クライアントがプライマリ サーバに到達できない場合、ASA は可用性を判定するためにタワーのポーリングを開始します（クライアントのアクティビティが存在しない場合、ASA は 15 分ごとにポーリングします）。設定された回数だけ再試行してもプロキシ サーバが使用できない場合（デフォルトは 5 回。この設定は設定可能）、サーバは到達不能として宣言され、バックアップ プロキシ サーバがアクティブになります。

クライアントまたは ASA が、再試行回数に到達する前に少なくとも 2 回連続してサーバに到達できる場合、ポーリングは停止し、タワーはアクセス可能であると判定されます。

再試行回数は、アプリケーション健全性チェックにも適用されます（イネーブルの場合）。

バックアップ サーバへのフェールオーバー後、ASA はプライマリ サーバをポーリングし続けます。プライマリ サーバが到達可能になると、ASA はプライマリ サーバの使用に戻ります。

例

次に、再試行回数の値を 7 に設定する例を示します。

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 health-check application
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。
health-check application	フェールオーバーのための、クラウド Web セキュリティのアプリケーション健全性チェックを有効にします。
http[s]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
match user group	ユーザまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバ オプションを設定します。
server {primary | backup}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。
show scansafe statistics	合計と現在の http 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。
ホワイトリスト	トラフィックのクラスでホワイトリスト アクションを実行します。

retry-interval

aaa-server host コマンドで事前に指定された特定の AAA サーバに対する再試行の時間間隔を設定するには、AAA サーバ ホスト モードで **retry-interval** コマンドを使用します。再試行間隔をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

retry-interval *seconds*

no retry-interval

構文の説明

seconds	要求の再試行間隔（1 ～ 10 秒）を指定します。これは、ASAが接続要求を再試行するまでに待機する時間です。

デフォルト

デフォルトの再試行間隔は 10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ ホスト	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは CLI ガイドラインに沿うように変更されました。

使用上のガイドライン

接続試行間に ASA が待機する秒数を指定またはリセットするには、**retry-interval** コマンドを使用します。ASA が AAA サーバへの接続を試行する時間の長さを指定するには、**timeout** コマンドを使用します。

（注） RADIUS プロトコルの場合、サーバが ICMP ポート到達不能メッセージで応答すると、再試行間隔の設定が無視され、AAA サーバはただちに障害状態になります。このサーバが AAA グループ内の唯一のサーバである場合は、サーバが再アクティブ化され、別の要求がサーバに送信されます。これは意図された動作です。

例

次に、コンテキストでの **retry-interval** コマンドの例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 7
ciscoasa(config-aaa-server-host)# retry-interval 9
ciscoasa(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始して、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。
timeout	ASA が AAA サーバへの接続を試行する時間の長さを指定します。

reval-period

NAC フレームワーク セッションにおける成功した各ポスチャ検証間の間隔を指定するには、nac ポリシー nac フレームワーク コンフィギュレーション モードで **reval-period** コマンドを使用します。このコマンドを NAC フレームワーク ポリシーから削除するには、このコマンドの **no** 形式を使用します。

reval-period *seconds*

no reval-period [*seconds*]

構文の説明

seconds	正常に完了した各ポスチャ確認の間隔の秒数。指定できる範囲は 300 ～ 86400 です。

デフォルト

デフォルト値は 36000 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
nac ポリシー nac フレームワーク コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
7.3(0)	コマンド名から「nac-」が削除されました。コマンドが、グループ ポリシー コンフィギュレーション モードから nac ポリシー nac フレームワーク コンフィギュレーション モードに移動されました。

使用上のガイドライン

ASA では、ポスチャ検証に成功するたびに、再検証タイマーが開始されます。このタイマーが期限切れになると、次の無条件のポスチャ検証がトリガーされます。ASA では、再検証中はポスチャ検証が維持されます。ポスチャ検証または再検証中にアクセス コントロール サーバが使用できない場合、デフォルトのグループ ポリシーが有効になります。

例

次に、再検証タイマーを 86400 秒に変更する例を示します。

```
ciscoasa(config-nac-policy-nac-framework)# reval-period 86400
ciscoasa(config-nac-policy-nac-framework)
```

次に、NAC ポリシーから再検証タイマーを削除する例を示します。

```
ciscoasa(config-nac-policy-nac-framework)# no reval-period
ciscoasa(config-nac-policy-nac-framework)
```

関連コマンド

コマンド	説明
eou timeout	NAC フレームワーク コンフィギュレーションで EAP over UDP メッセージをリモート ホストに送信した後に待機する秒数を変更します。
sq-period	NAC フレームワーク セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。
eou revalidate	1 つ以上の NAC フレームワーク セッションのポスチャ再確認をただちに強制します。

revert webvpn all

ASA のフラッシュ メモリから、すべての Web 関連データ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除するには、特権 EXEC モードで **revert webvpn all** コマンドを入力します。

revert webvpn all

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ASA のフラッシュ メモリから Web 関連のすべての情報（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）をディセーブルにし、削除するには、**revert webvpn all** コマンドを使用します。すべての Web 関連データを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。

例

次に、ASA からすべての Web 関連コンフィギュレーション データを削除するコマンドを示します。

```
ciscoasa# revert webvpn all
ciscoasa
```

関連コマンド

コマンド	説明
show import webvpn（オプション）	このコマンドは、ASA 上のフラッシュ メモリにそのとき存在する、さまざまなインポートされた WebVPN データおよびプラグインを表示します。

revert webvpn AnyConnect-customization

AnyConnect クライアント GUI のカスタマイズに使用されているファイルを ASA から削除するには、特権 EXEC モードで **revert webvpn AnyConnect-customization** コマンドを使用します。

revert webvpn AnyConnect-customization type *type* **platform** *platform* **name** *name*

構文の説明

type	カスタマイズ ファイルのタイプ。 • バイナリ:AnyConnect GUI を置き換える実行可能ファイル。 • resource:企業ロゴなどのリソース ファイル。 • トランスフォーム:MSI をカスタマイズするトランスフォーム。
platform	AnyConnect クライアントを実行しているエンドポイント デバイスの OS。**linux**、**mac-intel**、**mac-powerpc**、**win**、または **win-mobile** のいずれかを指定します。
name	削除するファイルを識別する名前(最大 64 文字)。

デフォルト

このコマンドにデフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

AnyConnect クライアント GUI をカスタマイズする手順の詳細については、『*AnyConnect VPN Client Administrator Guide*』を参照してください。

例

次に、AnyConnect GUI をカスタマイズするために以前にリソース ファイルとしてインポートした Cisco ロゴを削除する例を示します。

```
ciscoasa# revert webvpn AnyConnect-customization type resource platform win name
cisco_logo.gif
```

関連コマンド

コマンド	説明
カスタマイゼーション	トンネル グループ、グループ、またはユーザに対して使用するカスタマイゼーション オブジェクトを指定します。
export customization	カスタマイゼーション オブジェクトをエクスポートします。
import customization	カスタマイゼーション オブジェクトをインストールします。
revert webvpn all	すべての webvpn 関連データ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show webvpn customization	ASA のフラッシュ デバイスに存在する現在のカスタマイゼーション オブジェクトを表示します。

revert webvpn customization

ASA のキャッシュ メモリからカスタマイゼーション オブジェクトを削除するには、特権 EXEC モードで **revert webvpn customization** コマンドを入力します。

revert webvpn customization *name*

構文の説明

name	削除するカスタマイゼーション オブジェクトの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

指定したカスタマイゼーションのリモート クライアントレス SSL VPN サポートを削除し、ASA のキャッシュ メモリからそのカスタマイゼーション オブジェクトを削除するには、**revert webvpn customization** コマンドを使用します。カスタマイゼーション オブジェクトを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。カスタマイゼーション オブジェクトには、特定の指定されたポータル ページのコンフィギュレーション パラメータが含まれています。

バージョン 8.0 ソフトウェアでは、カスタマイゼーションの設定機能が拡張されており、新しいプロセスは以前のバージョンと互換性がありません。セキュリティ アプライアンスでは、8.0 ソフトウェアへのアップグレード時に、古い設定を使用して新しいカスタマイゼーション オブジェクトを生成することによって、現在の設定が保持されます。このプロセスは 1 回のみ実行されます。また、古い値は新しい値の一部を構成するサブセットに過ぎないため、このプロセスは古い形式から新しい形式への単なる変換ではありません。

(注) バージョン 7.2 のポータル カスタマイゼーションおよび URL リストは、バージョン 8.0 へのアップグレード前にバージョン 7.2(x) のコンフィギュレーション ファイルで適切なインターフェイスにおいてクライアントレス SSL VPN（WebVPN）がイネーブルになっている場合にのみ、ベータ 8.0 コンフィギュレーションで動作します。

例

次に、GroupB という名前のカスタマイゼーション オブジェクトを削除するコマンドを示します。

```
ciscoasa# revert webvpn customization groupb
ciscoasa
```

関連コマンド

コマンド	説明
カスタマイゼーション	トンネル グループ、グループ、またはユーザに対して使用するカスタマイゼーション オブジェクトを指定します。
export customization	カスタマイゼーション オブジェクトをエクスポートします。
import customization	カスタマイゼーション オブジェクトをインストールします。
revert webvpn all	すべての webvpn 関連データ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show webvpn customization	ASA のフラッシュ デバイスに存在する現在のカスタマイゼーション オブジェクトを表示します。

revert webvpn plug-in protocol

ASA のフラッシュ デバイスからプラグインを削除するには、特権 EXEC モードで **revert webvpn plug-in protocol** コマンドを入力します。

revert plug-in protocol *protocol*

構文の説明

protocol	次のいずれかのストリングを入力します。 • **rdp** Remote Desktop Protocol プラグインにより、リモート ユーザは Microsoft Terminal Services が実行するコンピュータに接続できます。 • **ssh** セキュア シェル プラグインにより、リモート ユーザがリモート コンピュータへのセキュア チャネルを確立したり、リモート ユーザが Telnet を使用してリモート コンピュータに接続したりできます。 • **vnc** Virtual Network Computing プラグインを使用すると、リモート ユーザはリモート デスクトップ共有をオンにしたコンピュータを、モニタ、キーボード、およびマウスを使用して表示および制御できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

指定した Java ベースのクライアント アプリケーションのクライアントレス SSL VPN サポートをディセーブルにし、削除して、ASA のフラッシュ ドライブからも削除するには、**revert webvpn plug-in protocol** コマンドを使用します。

例

次に、RDP のサポートを削除するコマンドを示します。

```
ciscoasa# revert webvpn plug-in protocol rdp
ciscoasa
```

関連コマンド

コマンド	説明
import webvpn plug-in protocol	指定したプラグインを URL から ASA のフラッシュ デバイスにコピーします。このコマンドを発行すると、クライアントレス SSL VPN での今後のセッションにおいて、Java ベースのクライアント アプリケーションの使用が自動的にサポートされます。
show import webvpn plug-in	ASA のフラッシュ デバイスに存在するプラグインのリストを示します。

revert webvpn translation-table

ASA のフラッシュ メモリから変換テーブルを削除するには、特権 EXEC モードで **revert webvpn translation-table** コマンドを入力します。

revert webvpn translation-table *translationdomain* **language** *language*

構文の説明

translationdomain	使用可能な変換ドメインは、次のとおりです。 • **AnyConnect** • **PortForwarder** • **バナー** • **csd** • **カスタマイゼーション** • **url-list** • **webvpn** • 使用可能な場合、Citrix、RPC、Telnet-SSH、および VNC のプラグインからのメッセージの変換。
language *language*	削除する言語を指定します。2 文字のコードを使用して言語を指定します。? と入力して、インストールされている言語を確認します。各ドメインにインストールされている言語を表示するには、**show import webvpn translation-table** コマンドを使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

インポートされた変換テーブルをディセーブルにし、削除して、フラッシュ メモリから削除するには、**revert webvpn translation-table** コマンドを使用します。変換テーブルを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。

例

次に、フランス語の AnyConnect 変換テーブルを削除するコマンドを示します。

```
ciscoasa# revert webvpn translation-table anyconnect language fr
ciscoasa#
```

関連コマンド

コマンド	説明
revert webvpn all	WebVPN 関連のすべてのデータ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show import webvpn translation-table	フラッシュ デバイスに存在する現在の変換テーブルを表示します。

revert webvpn url-list

ASA から URL リストを削除するには、特権 EXEC モードで **revert webvpn url-list** コマンドを入力します。

revert webvpn url-list template *name*

構文の説明

template *name*	URL リストの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ASA のフラッシュ ドライブから現在の URL リストをディセーブルにし、削除するには、**revert webvpn url-list** コマンドを使用します。URL リストを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。

revert webvpn url-list コマンドで使用される template 引数では、設定済みの URL リストの名前を指定します。このようなリストを設定するには、グローバル コンフィギュレーション モードで **url-list** コマンドを使用します。

例

次に、servers2 という URL リストを削除するコマンドを示します。

```
ciscoasa# revert webvpn url-list servers2
ciscoasa
```

関連コマンド

コマンド	説明
revert webvpn all	すべての webvpn 関連データ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show running-configuration url-list	現在の設定済み URL リスト コマンドのセットを表示します。
url-list（webvpn モード）	特定のユーザまたはグループ ポリシーに、WebVPN サーバおよび URL のリストを適用します。

revert webvpn webcontent

ASA のフラッシュ メモリ内の場所から指定した Web オブジェクトを削除するには、特権 EXEC モードで **revert webvpn webcontent** コマンドを入力します。

revert webvpn webcontent *filename*

構文の説明

filename	削除する Web コンテンツを含むフラッシュ メモリ ファイルの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

Web コンテンツを含むファイルをディセーブルにし、削除して、ASA のフラッシュ メモリからも削除するには、**revert webvpn content** コマンドを使用します。Web コンテンツを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。

例

次に、ASA のフラッシュ メモリから ABCLogo という Web コンテンツ ファイルを削除するコマンドを示します。

```
ciscoasa# revert webvpn webcontent abclogo
ciscoasa
```

関連コマンド

コマンド	説明
revert webvpn all	すべての webvpn 関連データ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show webvpn webcontent	現在 ASA のフラッシュ メモリに存在する Web コンテンツを表示します。

revocation-check

トラストプール ポリシーについて失効チェックが必要であるかどうかを定義するには、クリプト CA トラストプール コンフィギュレーション モードで **revocation-check** コマンドを使用します。デフォルトの失効チェック方法（*none*）に戻すには、このコマンドの **no** 形式を使用します。

revocation-check {[**crl**] [**ocsp**] [**none**] }

no revocation-check {[**crl**] [**ocsp**] [**none**]}

構文の説明

crl	ASA において、失効チェック方法として CRL を使用する必要があることを指定します。
none	ASA において、すべての方法でエラーが返された場合でも証明書ステータスを有効であると解釈する必要があることを指定します。
ocsp	ASA において、失効チェック方法として OCSP を使用する必要があることを指定します。

デフォルト

デフォルト値は *none* です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストプール コンフィギュレーション モード	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.13(1)	CRL または OCSP サーバとの接続問題に起因する失効チェックをバイパスするオプションが削除されました。

使用上のガイドライン

OCSP 応答の署名者は、通常、OCSP サーバ（レスポンダ）証明書です。デバイスは、応答を受信した後、レスポンダ証明書の検証を試みます。

通常、CA は、セキュリティが侵害される危険性を最小限に抑えるために、OCSP レスポンダ証明書のライフタイムを比較的短い期間に設定します。CA は、失効ステータス チェックが必要ないことを示す ocsp-no-check 拡張をレスポンダ証明書に組み込みます。ただし、この拡張が存在しない場合、デバイスは、この **revocation-check** コマンドでトラストポイントに設定された失効方法を使用して、証明書失効ステータスを確認しようとします。*none* オプションを設定してステータス チェックを無視していない限り、OCSP 失効チェックの失敗後、OCSP レスポンダ証明書に ocsp-no-check 拡張がない場合、OCSP レスポンダ証明書は検証可能である必要があります。

(注) オプションの引数を指定する場合、順序は問いませんが、*none* キーワードは必ず最後にする必要があります。

ASA では、それらの方法が設定した順序で試行されます。2 番目と 3 番目の方法は、前の方法でエラー(サーバのダウンなど)が返された場合にのみ、ステータスを失効と見なさずに試行されます。

クライアント証明書検証トラストポイントで、失効チェック方法を設定できます。また、レスポンダ証明書検証トラストポイントで、失効チェックなし(**revocation-check none**)を設定することもできます。設定例については、**match certificate** コマンドを参照してください。

ASA で **revocation-check crl none** コマンドを設定している場合、クライアントが ASA に接続すると、CRL がまだキャッシュされていないためダウンロードが自動的に開始され、証明書が検証されてから CRL のダウンロードが終了します。この場合、CRL がキャッシュされていないと、CRL のダウンロード前に ASA で証明書が検証されます。

ただし、ASA 9.13(1) 以降では、失効チェックをバイパスするための次のオプションはサポートされていません。

オプション	Action
revocation-check crl none	CRL にアクセスできない場合は、失効チェックをバイパスします
revocation-check ocsp none	OCSP チェックを実行できない場合は、失効チェックをバイパスします
revocation-check crl ocsp none	CRL にアクセスできない場合は、OCSP を試してください。OCSP を実行できない場合は、失効チェックをバイパスします
revocation-check ocsp crl none	OCSP を実行できない場合は、CRL を試し、それ以外の場合は失効チェックをバイパスします

そのため、アップグレード後に、サポートされなくなったすべての失効チェックコマンドは、末尾の **none** オプションを無視して新しい動作に移行します。

例

```
ciscoasa(config-ca-trustpoint)# revocation-check ?

crypto-ca-trustpoint mode commands/options:
  crl   Revocation check by CRL
  none  Ignore revocation check
  ocsp  Revocation check by OCSP
(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpool policy	トラストプール ポリシーを定義するコマンドを提供するサブモードを開始します。
match certificate allow expired-certificate	特定の証明書に対する有効期限チェックを管理者が免除できるようにします。
match certificate skip revocation-check	特定の証明書に対する失効チェックを管理者が免除できるようにします。

rewrite

WebVPN 接続上で、特定のアプリケーションまたはトラフィック タイプのコンテンツのリライトをディセーブルにするには、webvpn モードで **rewrite** コマンドを使用します。リライト ルールを削除するには、ルールを一意に識別するルール番号を指定して、このコマンドの **no** 形式を使用します。すべてのリライト ルールを削除するには、このコマンドの **no** 形式をルール番号を指定せずに使用します。

デフォルトで、ASA では、すべての WebVPN トラフィックがリライト（変換）されます。

rewrite order *integer* **{enable | disable} resource-mask** *string* **[name** *resource name***]**

no rewrite order *integer* **{enable | disable} resource-mask** *string* **[name** *resource name***]**

構文の説明

disable	このリライト ルールを、指定したトラフィックに対するコンテンツのリライトをディセーブルにするルールとして定義します。コンテンツのリライトをディセーブルにすると、トラフィックはセキュリティ アプライアンスを通過しません。
イネーブル化	このリライト ルールを、指定したトラフィックに対するコンテンツのリライトをイネーブルにするルールとして定義します。
整数	設定されているすべてのルール内でのルールの順序を設定します。指定できる範囲は 1 ～ 65534 です。
name	（任意）ルールを適用するアプリケーションまたはリソースの名前を指定します。
order	ASA がルールを適用する順序を定義します。
resource-mask	ルールのアプリケーションまたはリソースを指定します。
resource name	（任意）ルールを適用するアプリケーションまたはリソースを指定します。最大 128 バイトです。
string	照合するアプリケーションまたはリソースの名前を指定します。正規表現を使用できます。次のワイルドカードを使用できます。 照合対象として正規表現を含むことができるパターンを指定します。次のワイルドカードを使用できます。 *：すべてに一致します。このワイルドカードはこれだけでは使用できません。英数字の文字列とともに使用する必要があります。 ?：任意の 1 文字に一致します。 [!seq]：シーケンスにない任意の文字に一致します。 [seq]：シーケンス内の任意の文字に一致します。 最大 300 バイトです。

デフォルト

デフォルトでは、すべてをリライトします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

ASA では、WebVPN 接続経由で正しくレンダリングされるように、アプリケーションのコンテンツがリライトされます。外部パブリック Web サイトなどの一部のアプリケーションでは、この処理は必要ありません。これらのアプリケーションでは、コンテンツ リライトをオフにできます。

disable オプションを指定して rewrite コマンドを使用することによって、コンテンツ リライトを選択的にオフにし、ユーザが ASA を経由せずに直接特定のサイトをブラウズ可能にできます。これは、IPsec VPN 接続におけるスプリット トンネリングに似ています。

このコマンドは複数回使用できます。ASA では、順序番号に従ってリライト ルールが検索され、一致する最初のルールが適用されるため、エントリの設定順序は重要です。

例

次に、cisco.com ドメインの URL に対するコンテンツ リライトをオフにする順序番号 1 のリライト ルールを設定する例を示します。

```
ciscoasa(config-webpn)# rewrite order 2 disable resource-mask *cisco.com/*
```

関連コマンド

コマンド	説明
apcf	特定のアプリケーションに使用する非標準のルールを指定します。
proxy-bypass	特定のアプリケーションに対してコンテンツの最低限の書き換えを設定します。

re-xauth

IPsec ユーザに対して IKE キー再生成時に再認証を要求するには、グループ ポリシー コンフィギュレーション モードで **re-xauth enable** コマンドを発行します。IKE キー再生成時にユーザの再認証をディセーブルにするには、**re-xauth disable** コマンドを使用します。

実行コンフィギュレーションから re-xauth 属性を削除するには、このコマンドの **no** 形式を使用します。これにより、他のグループ ポリシーから IKE キー再生成時の再認証についての値が継承されます。

re-xauth {**enable** [**extended**] | **disable**}

no re-xauth

構文の説明

disable	IKE キー再生成時の再認証をディセーブルにします。
enable	IKE キー再生成時の再認証をイネーブルにします。
extended	認証クレデンシャルを再入力可能な時間を、設定されている SA の最大ライフタイムまで延長します。

デフォルト

IKE キー再生成時の再認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0.4	**extended** キーワードが追加されました。

使用上のガイドライン

IKE キー再生成時の再認証は、IPsec 接続に対してのみ適用されます。

IKE キー再生成時の再認証をイネーブルにすると、ASA では、最初のフェーズ 1 IKE ネゴシエーションにおいてユーザに対してユーザ名とパスワードの入力が求められ、その後 IKE キー再生成が行われるたびにユーザ認証が求められます。再認証によって、セキュリティが強化されます。

ユーザは、30 秒以内にクレデンシャルを入力する必要があります。また、約 2 分間で SA が期限切れになり、トンネルが終了するまでの間に、3 回まで入力を再試行できます。ユーザに対して、設定されている SA の最大ライフタイムまで認証クレデンシャルの再入力を許可するには、**extended** キーワードを使用します。

設定されているキー再生成間隔をチェックするには、モニタリング モードで **show crypto ipsec sa** コマンドを発行して、セキュリティ アソシエーションの秒単位のライフタイム、およびデータの KB 単位のライフタイムを表示します。

(注) 接続の他方の終端にユーザが存在しない場合、再認証は失敗します。

例

次に、FirstGroup という名前のグループ ポリシーに対して、キー再生成時の再認証をイネーブルにする例を示します。

```
ciscoasa(config) #group-policy FirstGroup attributes
ciscoasa(config-group-policy)# re-xauth enable
```

rip authentication mode

RIP バージョン 2 パケットで使用される認証のタイプを指定するには、インターフェイス コンフィギュレーション モードで **rip authentication mode** コマンドを使用します。デフォルトの認証方法に戻すには、このコマンドの **no** 形式を使用します。

rip authentication mode {**text** | **md5**}

no rip authentication mode

構文の説明

md5	RIP メッセージ認証に MD5 を使用します。
text	RIP メッセージ認証にクリア テキストを使用します(非推奨)。

デフォルト

デフォルトで、クリア テキスト認証が使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

インターフェイス上で **rip authentication** コマンドを表示するには、**show interface** コマンドを使用します。

例

次に、インターフェイス GigabitEthernet0/3 上で設定された RIP 認証の例を示します。

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# rip authentication mode md5
ciscoasa(config-if)# rip authentication key thisismykey key_id 5
```

関連コマンド

コマンド	説明
rip authentication key	RIP バージョン 2 認証をイネーブルにして、認証キーを指定します。
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
show running-config interface	指定したインターフェイスのコンフィギュレーション コマンドを表示します。
version	ASA でグローバルに使用される RIP のバージョンを指定します。

rip authentication key

RIP バージョン 2 パケットの認証をイネーブルにして、認証キーを指定するには、インターフェイス コンフィギュレーション モードで **rip authentication key** コマンドを使用します。RIP バージョン 2 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。

rip authentication key [0 | 8] *string* **key_id** *id*

no rip authentication key

構文の説明

0	暗号化されていないパスワードが続くことを指定します。
8	暗号化されたパスワードが後に続くことを指定します。
id	キー ID 値を指定します。有効な値の範囲は 1 ～ 255 です。
key	認証キー ストリングに使用される共有キーを指定します。このキーには、最大 16 文字を含めることができます。
string	暗号化されていない(クリアテキスト)ユーザ パスワードを指定します。

デフォルト

RIP 認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。ネイバー認証をイネーブルにする場合は、*key* 引数および *key_id* 引数が、RIP バージョン 2 更新を提供するネイバー デバイスによって使用されているものと同じである必要があります。*key* は、最大 16 文字のテキスト ストリングです。

インターフェイス上で **rip authentication** コマンドを表示するには、**show interface** コマンドを使用します。

例

次に、インターフェイス GigabitEthernet 0/3 上で設定された RIP 認証の例を示します。

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# rip authentication mode md5
ciscoasa(config-if)# rip authentication key 8 yWIvi0qJAnGK5MRWQzrhIohkGP1wKb 5
```

関連コマンド

コマンド	説明
rip authentication mode	RIP バージョン 2 パケットで使用される認証のタイプを指定します。
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
show running-config interface	指定したインターフェイスのコンフィギュレーション コマンドを表示します。
version	ASA でグローバルに使用される RIP のバージョンを指定します。

rip receive version

インターフェイスで受け入れる RIP のバージョンを指定するには、インターフェイス コンフィギュレーション モードで **rip receive version** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

version {[**1**] [**2**]}

no version

構文の説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

デフォルト

ASA は RIP バージョン 1 とバージョン 2 のパケットを受け入れます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

グローバル設定をインターフェイスごとに上書きするには、インターフェイスで **rip receive version** コマンドを入力します。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

例

次に、指定したインターフェイス上で RIP バージョン 1 と 2 のパケットを受信するように、ASA を設定する例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# rip send version 1 2
ciscoasa(config-if)# rip receive version 1 2
```

関連コマンド

コマンド	説明
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにして、そのプロセスのルータ コンフィギュレーション モードを開始します。
version	ASA でグローバルに使用される RIP のバージョンを指定します。

rip send version

インターフェイスで RIP アップデートを送信するために使用される RIP のバージョンを指定するには、インターフェイス コンフィギュレーション モードで **rip send version** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

rip send version {[**1**] [**2**]}

no rip send version

構文の説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

デフォルト

ASA は RIP バージョン 1 パケットを送信します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

グローバル RIP 送信バージョン設定をインターフェイスごとに上書きするには、インターフェイスで **rip send version** コマンドを入力します。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

例

次に、指定したインターフェイス上で RIP バージョン 1 と 2 のパケットを送受信するように、ASA を設定する例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# rip send version 1 2
ciscoasa(config-if)# rip receive version 1 2
```

関連コマンド

コマンド	説明
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。
version	ASA でグローバルに使用される RIP のバージョンを指定します。

rmdir

既存のディレクトリを削除するには、特権 EXEC モードで **rmdir** コマンドを使用します。

rmdir [**/noconfirm**] [**disk0: | disk1: | flash:**]*path*

構文の説明

/noconfirm	（任意）確認プロンプトを表示しないようにします。
disk0*:*	（任意）非着脱式内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	（任意）着脱式外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	（任意）非着脱式内部フラッシュを指定し、続けてコロンを入力します。ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、**flash** キーワードは **disk0** とエイリアス関係にあります。
path	（任意）削除するディレクトリの絶対または相対パス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ディレクトリが空でない場合、**rmdir** コマンドは失敗します。

例

次に、「test」という名前の既存のディレクトリを削除する例を示します。

```
ciscoasa# rmdir test
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
mkdir	新しいディレクトリを作成します。
pwd	現在の作業ディレクトリを表示します。
show file	ファイル システムに関する情報を表示します。

route

指定したインターフェイスにスタティック ルートまたはデフォルト ルートを入力するには、グローバル コンフィギュレーション モードで **route** コマンドを使用します。指定されたインターフェイスからルートを削除するには、このコマンドの **no** 形式を使用します。

route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] | **tunneled**]

no route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] | **tunneled**]

構文の説明

gateway_ip	ゲートウェイ ルータの IP アドレス（このルートのネクストホップ アドレス）を指定します。 （注） トランスペアレント モードでは、*gateway_ip* 引数は省略可能です。
interface_name	トラフィックがルーティングされるインターフェイスの名前を指定します。トランスペアレント モードの場合は、ブリッジ グループのメンバー インターフェイスの名前を指定します。ブリッジ グループでルーテッド モードを使用する場合は、BVI 名を指定します。ルーテッド モードで、不要なトラフィックを「ブラック ホール化」するには、**null0** インターフェイスを入力します。
ip_address	内部または外部ネットワーク IP アドレスを指定します。
metric	（オプション）このルートのアドミニストレーティブ ディスタンスを指定します。有効値の範囲は、1 ～ 255 です。デフォルト値は 1 です。
netmask	*ip_address* に適用するネットワーク マスクを指定します。
track *number*	（任意）このルートにトラッキング エントリを関連付けます。有効な値は、1 ～ 500 です。 （注） **track** オプションは、シングル、ルーテッド モードでのみ使用できます。
tunneled	ルートを VPN トラフィックのデフォルト トンネル ゲートウェイとして指定します。

デフォルト

metric のデフォルトは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	**track** *number* の値が追加されました。
9.2(1)	**null0** インターフェイス オプションが追加されました。
9.7(1)	統合ルーティングおよびブリッジングを使用している場合のルーテッド モードの BVI インターフェイスのサポートが追加されました。

使用上のガイドライン

インターフェイスに対してデフォルト ルートまたはスタティック ルートを入力するには、**route** コマンドを使用します。デフォルト ルートを入力するには、*ip_address* および *netmask* を **0.0.0.0** または短縮形の **0** に設定します。**route** コマンドを使用して入力されたすべてのルートは、コンフィギュレーションの保存時に保存されます。

トンネル トラフィックには、標準のデフォルト ルートの他に別のデフォルト ルートを 1 つ定義することができます。**tunneled** オプションを使用してデフォルト ルートを作成すると、ASA に着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティック ルートを使用してルーティングできない場合、このルートに送信されます。トンネルから出るトラフィックの場合、このルートは、その他の設定または学習されたデフォルト ルートをすべて上書きします。

tunneled オプションを使用したデフォルト ルートには、次の制約事項が適用されます。

- トンネル ルートの出力インターフェイスで、ユニキャスト RPF（**ip verify reverse-path**）をイネーブルにしないでください。トンネル ルートの出力インターフェイスで uRPF をイネーブルにすると、セッションに障害が発生します。
- セッションでエラーが発生する原因となるため、トンネル ルートの出力インターフェイスで TCP 代行受信をイネーブルにしないでください。
- VoIP インスペクション エンジン（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY）、DNS インスペクション エンジン、または DCE RPC インスペクション エンジンは、vlan-mapping オプションまたはトンネル ルートでは使用しないでください。vlan-mapping 設定によってパケットが間違ってルーティングされる可能性があるため、これらのインスペクション エンジンは、vlan-mapping 設定を無視します。

tunneled オプションを使用して複数のデフォルト ルートは定義できません。トンネル トラフィックの ECMP はサポートされていません。

スタティック ルートは、任意のインターフェイスで、ルータの外部に接続されているネットワークにアクセスする場合に作成します。たとえば、次のスタティック **route** コマンドでは、ASA によって、192.168.42.0 ネットワークへのすべてのパケットが 192.168.1.5 ルータ経由で送信されます。

```
ciscoasa(config)# route dmz 192.168.42.0 255.255.255.0 192.168.1.5 1
```

各インターフェイスの IP アドレスを入力すると、ASA によって、ルート テーブルに CONNECT ルートが作成されます。このエントリは、**clear route** コマンドや **clear configure route** コマンドを使用しても削除されません。

ACL の場合とは異なり、スタティック **null0** ルートはまったくパフォーマンスを低下させません。**null0** 設定は、ルーティング ループの防止に使用されます。BGP では、リモート トリガー型ブラック ホール ルーティングのために **null0** 設定を利用します。

例

次に、外部インターフェイスに対して、1 つのデフォルト **route** コマンドを指定する例を示します。

```
ciscoasa(config)# route outside 0 0 209.165.201.1 1
```

次に、ネットワークへのアクセスを提供するスタティック **route** コマンドを追加する例を示します。

```
ciscoasa(config)# route dmz1 10.1.2.0 255.0.0.0 10.1.1.4 1
ciscoasa(config)# route dmz1 10.1.3.0 255.0.0.0 10.1.1.4 1
```

次に、SLA 動作を使用して、外部インターフェイスに対して、10.1.1.1 ゲートウェイへのデフォルト ルートをインストールする例を示します。SLA 動作によって、このゲートウェイの可用性がモニタされます。この SLA 動作が失敗した場合は、DMZ インターフェイスのバックアップ ルートが使用されます。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.1.1.1 track 1
ciscoasa(config)# route dmz 0.0.0.0 0.0.0.0 10.2.1.1 254
```

次に、スタティック null0 ルートを設定する例を示します。

```
ciscoasa(config)# route null0 192.168.2.0 255.255.255.0
```

関連コマンド

コマンド	説明
clear configure route	スタティックに設定された **route** コマンドを削除します。
clear route	RIP などのダイナミック ルーティング プロトコルを通じて学習されたルートを削除します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

route-map

ルーティング プロトコル間でルートを再配布する条件を定義したり、ポリシー ルーティングをイネーブルにしたりするには、グローバル コンフィギュレーション モードで **route-map** コマンドを使用し、さらにルート マップ コンフィギュレーション モードで match コマンドと set コマンドを使用します。エントリを削除するには、このコマンドの **no** 形式を使用します。

route-map *name* [**permit | deny**] [*sequence number*]

no route-map *name* [**permit | deny**] [*sequence number*]

構文の説明

name	ルート マップに意味のある名前を指定します。redistribute ルータ コンフィギュレーション コマンドはこの名前を使用して、このルート マップを参照します。複数のルート マップで同じ名を共有できます。
permit	(オプション)このルート マップの一致基準が満たされた場合、**permit** キーワードが指定されていると、設定アクションに従ってルートが再配布されます。ポリシー ルーティングの場合、パケットはポリシーに従ってルーティングされます。 一致基準が満たされなかった場合、**permit** キーワードが指定されていると、同じマップ タグを持つ次のルート マップがテストされます。あるルートが、同じ名前を共有するルート マップ セットの一致基準のいずれをも満たさない場合、そのセットによる再配布は行われません。 **permit** キーワードがデフォルトです。
deny	(オプション)ルート マップの一致基準が満たされた場合でも、**deny** キーワードが指定されているとルートは再配布されません。ポリシー ルーティングの場合、パケットはポリシーに従ってルーティングされません。また、同じマップ タグ名を共有するルート マップは、これ以上検証されません。パケットがポリシー ルーティングの対象にならない場合、通常の転送アルゴリズムが使用されます。
sequence-number	(任意)すでに同じ名前で設定されているルート マップ リスト内の新しいルート マップの位置を指定する番号。このコマンドの no 形式を指定すると、このルート マップの位置が削除されます。

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

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ルートを再配布するには、ルート マップを使用します。

あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義するには、route-map グローバル コンフィギュレーション コマンドと、match および set ルート マップ コンフィギュレーション コマンドを使用します。**route-map** コマンドごとに、それに関連した match および set コマンドのリストがあります。match コマンドは、一致基準（現在の route-map コマンドで再配布が許可される条件）を指定します。set コマンドは、set 処理（match コマンドによって強制される基準が満たされた場合に実行される特定の再配布アクション）を指定します。**no route-map** コマンドはルート マップを削除します。

match ルート マップ コンフィギュレーション コマンドには、複数の形式があります。match コマンドの順序は任意に指定できます。すべての match コマンドが満たされないと、set コマンドで指定した set 処理に従ってルートの再配布が行われません。match コマンドの no 形式を使用すると、指定した一致基準が削除されます。

ルーティング プロセス間でルートを再配布する方法を詳細に制御する必要がある場合にルート マップを使用します。宛先ルーティング プロトコルは router 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指定します。ソース ルーティング プロトコルは redistribute ルータ コンフィギュレーション コマンドを使用して指定します。ルート マップの設定方法の例については、「例」のセクションを参照してください。

ルートがルート マップを通過するようにするときには、ルート マップに複数の要素を持たせることができます。route-map コマンドに関連付けられているどの match ステートメントとも一致しないルートは無視されます。したがって、そのルートは発信ルート マップ用にアドバタイズされることも、着信ルート マップ用に受け入れられることもありません。一部のデータのみ修正したい場合は、別にルート マップ セクションを設定して明示的に一致基準を指定する必要があります。

sequence-number 引数を使用した場合の動作は次のとおりです。

1. route-map name でエントリが定義されていない場合、sequence-number 引数を 10 にしたエントリが作成されます。
2. route-map name でエントリが 1 つしか定義されていない場合、そのエントリが後続の route-map コマンドのデフォルト エントリになります。このエントリの sequence-number 引数は変わりません。
3. route-map name で複数のエントリが定義されている場合、sequence-number 引数が必要であることを伝えるエラー メッセージが表示されます。
4. **no route-map name** コマンドが指定されると（sequence-number 引数なし）、ルート マップ全体が削除されます。

例

次の例は、ホップ カウント 1 でルートを OSPF に再配布する方法を示しています。ASA は、これらのルートをメトリック 5、メトリック タイプ 1 で外部 LSA として再配布します。

```
ciscoasa(config)# route-map 1-to-2 permit

ciscoasa(config-route-map)# match metric 11
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
```

次に、メトリック値が設定された EIGRP プロセス 1 に 10.1.1.0 のスタティック ルートを再配布する例を示します。

```
ciscoasa (config)# route outside 10.1.1.0 255.255.255.0 192.168.1.1
ciscoasa(config-route-map)# access-list mymap2 line 1 permit 10.1.1.0 255.255.255.0
ciscoasa(config-route-map)# route-map mymap2 permit 10
ciscoasa(config-route-map)# match ip address mymap2
ciscoasa(config-route-map)# router eigrp 1
ciscoasa(config)# redistribute static metric 250 250 1 1 1 route-map
```

関連コマンド

コマンド	説明
redistribute	ルートを 1 つのルーティング ドメインから他のルーティング ドメインに再配布します。
ルート	インターフェイスのスタティック ルートまたはデフォルト ルートを作成します。
ルータ	指定したプロトコルのルータ コンフィギュレーション モードを開始します。

route priority high

IS-IS プレフィックスに高いプライオリティを割り当てるには、ルータ ISIS コンフィギュレーション モードで **route priority high** コマンドを使用します。IP プレフィックス プライオリティを削除するには、このコマンドの **no** 形式を使用します。

route priority high *tag-value*

no route priority high *tag-value*

構文の説明

tag-value	特定のルート タグを持つ IS-IS IP プレフィックスにハイ プライオリティを割り当てます。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

IP プレフィックス プライオリティは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

グローバル ルーティング テーブルでより高速な処理とインストールを行うために、**route priority high** コマンドを使用して、より高いプライオリティの IS-IS IP プレフィックスにタグ付けすると、より速くコンバージェンスを達成できます。たとえば、Voice over IP（VoIP）トラフィックが、その他のタイプのパケットよりも速く更新されるようにするために、VoIP ゲートウェイ アドレスが最初に処理されるようにすることができます。

例

次に、**route priority high** コマンドを使用して、IS-IS IP プレフィックスにタグ値 100 を割り当てる例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# route priority high tag 100
```

関連コマンド

router-alert

IP オプション インスペクションにおいて、パケット ヘッダー内でルータ アラート IP オプションが存在する場合のアクションを定義するには、パラメータ コンフィギュレーション モードで **router-alert** 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。

router-alert action {allow | clear}

no router-alert action {allow | clear}

構文の説明

allow	ルータ アラート IP オプションを含むパケットを許可します。
clear	ルータ アラート オプションをパケット ヘッダーから削除してから、パケットを許可します。

デフォルト

デフォルトで、IP オプション インスペクションは、ルータ アラート IP オプションを含むパケットを許可します。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用するとデフォルト値を変更できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

ルータ アラート（RTRALT）または IP オプション 20 は、中継ルータに対して、そのルータ宛てのパケットではない場合でもパケットの内容を検査するように指示します。このインスペクションは、RSVP を実装している場合に役に立ちます。同様のプロトコルは、パケット配信パス上にあるルータでの比較的複雑な処理を必要とします。

例

次に、ポリシー マップにおけるプロトコル違反に対するアクションを設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

router bgp

ボーダー ゲートウェイ プロトコル(BGP)ルーティング プロセスを設定するには、グローバル コンフィギュレーション モードで **router bgp** コマンドを使用します。BGP ルーティング プロセスを削除するには、このコマンドの **no** 形式を使用します。

router bgp *autonomous-system-number*

no router bgp *autonomous-system-number*

構文の説明

autonomous-system-number	他の BGP ルータに対するルータを指定し、同時に渡されるルーティング情報のタギングをする、自律システムの番号。番号の範囲は 1 ～ 65535 です。

デフォルト

デフォルトでは BGP ルーティング プロセスはイネーブルではありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、自律システム間でのルーティング情報のループなしのやり取りが自動的に保証される、分散ルーティング コアを設定できます。

2009 年 1 月まで、企業に割り当てられていた BGP 自律システム番号は、RFC 4271『*A Border Gateway Protocol 4 (BGP-4)*』に記述された、1 ～ 65535 の範囲の 2 オクテットの数値でした。

現在は、自律システム番号の要求の増加に伴い、インターネット割り当て番号局(IANA)により割り当てられる自律システム番号は 65536 ～ 4294967295 の範囲の 4 オクテットの番号になります。

RFC 5396『*Textual Representation of Autonomous System (AS) Numbers*』には、自律システム番号を表す 3 つの方式が記述されています。シスコでは、次の 2 つの方式を実装しています。

- asplain：10 進表記方式。2 バイトおよび 4 バイト自律システム番号をその 10 進数値で表します。たとえば、65526 は 2 バイト自律システム番号、234567 は 4 バイト自律システム番号になります。
- asdot：自律システム ドット付き表記。2 バイト自律システム番号は 10 進数で、4 バイト自律システム番号はドット付き表記で表されます。たとえば、65526 は 2 バイト自律システム番号、1.169031（10 進表記の 234567 をドット付き表記にしたもの）は 4 バイト自律システム番号になります。

自律システム番号を表す 3 つ目の方法については、RFC 5396 を参照してください。

例

次の例は、自律システム番号 100 用に BGP プロセスを設定する方法を示しています。

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
show route bgp	ルーティング テーブルを表示します。
show bgp summary	すべてのボーダー ゲートウェイ プロトコル（BGP）接続のステータスを表示します。

router eigrp

EIGRP ルーティング プロセスを開始して、そのプロセス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 **router eigrp** コマンドを使用します。EIGRP ルーティ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。

router eigrp *as-number*

no router eigrp *as-number*

構文の説明

as-number	他の EIGRP ルータへのルートを識別する自律システム番号。ルーティング情報のタギングにも使用されます。有効値は 1 ～ 65535 です。

デフォルト

EIGRP ルーティングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードはサポートされます。

使用上のガイドライン

router eigrp コマンドは、EIGRP ルーティング プロセスを作成するか、または既存の EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。ASA では、単一の EIGRP ルーティング プロセスのみを作成できます。

次のルータ コンフィギュレーション モード コマンドを使用して、EIGRP ルーティング プロセスを設定します。

- **auto-summary**：自動ルート集約をイネーブルまたはディセーブルにします。
- **default-information**：デフォルト ルート情報の送受信をイネーブルまたはディセーブルにします。
- **default-metric**：EIGRP ルーティング プロセスに再配布されるルートのデフォルトのメトリックを定義します。
- **distance eigrp**：内部および外部 EIGRP ルートのアドミニストレーティブ ディスタンスを設定します。

- **distribute-list**：ルーティング更新で送受信されるネットワークをフィルタリングします。
- **eigrp log-neighbor-changes**：ネイバー ステートの変更のロギングをイネーブルまたはディセーブルにします。
- **eigrp log-neighbor-warnings**：ネイバー警告メッセージのロギングをイネーブルまたはディセーブルにします。
- **eigrp router-id**：固定ルータ ID を作成します。
- **eigrp stub**：ASA でスタブ EIGRP ルーティングを設定します。
- **neighbor**：EIGRP ネイバーをスタティックに定義します。
- **network**：EIGRP ルーティング プロセスに参加するネットワークを設定します。
- **passive-interface**：パッシブ インターフェイスとして動作するインターフェイスを設定します。
- **redistribute**：他のルーティング プロセスから EIGRP にルートを再配布します。

次のインターフェイス コンフィギュレーション モード コマンドを使用して、インターフェイス固有の EIGRP パラメータを設定します。

- **authentication key eigrp**：EIGRP メッセージ認証で使用される認証キーを定義します。
- **authentication mode eigrp**：EIGRP メッセージ認証で使用される認証アルゴリズムを定義します。
- **delay**：インターフェイスの遅延メトリックを設定します。
- **hello-interval eigrp**：EIGRP の hello パケットがインターフェイスから送信される間隔を変更します。
- **hold-time eigrp**：ASA によってアドバタイズされるホールド タイムを変更します。
- **split-horizon eigrp**：インターフェイスで EIGRP スプリット ホライズンをイネーブルまたはディセーブルにします。
- **summary-address eigrp**：サマリー アドレスを手動で定義します。

例

次に、自律システム番号 100 が付けられた EIGRP ルーティング プロセスのコンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-rtr)#
```

関連コマンド

コマンド	説明
clear configure eigrp	実行コンフィギュレーションから EIGRP ルータ コンフィギュレーション モード コマンドをクリアします。
show running-config router eigrp	実行コンフィギュレーションの EIGRP ルータ コンフィギュレーション モード コマンドを表示します。

router-id

固定ルータ ID を使用するには、ルータ コンフィギュレーション モード（OSPFv2 の場合）または IPv6 ルータ コンフィギュレーション モード（OSPFv3 の場合）で **router-id** コマンドを使用します。以前のルータ ID 動作を使用するように OSPF をリセットするには、このコマンドの **no** 形式を使用します。

router-id *id*

no router-id [*id*]

構文の説明

id	IP アドレス形式でルータ ID を指定します。

デフォルト

指定しない場合、ASA 上で最上位の IP アドレスがルータ ID として使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	このコマンドの処理順序が変更されました。このコマンドは、OSPFv2 コンフィギュレーションでは、**network** コマンドよりも先に処理されるようになりました。
9.0(1)	マルチ コンテキスト モードおよび OSPFv3 がサポートされています。

使用上のガイドライン

ASA では、OSPF コンフィギュレーションにおいて、デフォルトで、**network** コマンドによって指定されているインターフェイス上の最上位の IP アドレスが使用されます。最上位の IP アドレスがプライベート アドレスである場合、そのアドレスは hello パケットおよびデータベース定義で送信されます。特定のルータ ID を使用するには、**router-id** コマンドを使用して、ルータ ID としてグローバル アドレスを指定します。

ルータ ID は、OSPF ルーティング ドメイン内で一意である必要があります。同じ OSPF ドメイン内の 2 つのルータが同じルータ ID を使用している場合、ルーティングが正しく動作しない可能性があります。

OSPF コンフィギュレーションでは、**network** コマンドを入力する前に **router-id** コマンドを入力する必要があります。これにより、ASA によって生成されるデフォルトのルータ ID との競合を回避できます。競合がある場合は、次のメッセージが表示されます。

```
ERROR: router-id id in use by ospf process pid
```

競合する ID を入力するには、競合の原因となっている IP アドレスを含む **network** コマンドを削除し、**router-id** コマンドを入力して、**network** コマンドを再入力します。

クラスタ

レイヤ 2 クラスタリングでは、すべてのユニットで同じルータ ID を受け取る場合、**router-id** *id* コマンドを設定するか、ルータ ID を空白のままにする必要があります。

例

次に、ルータ ID を 192.168.1.1 に設定する例を示します。

```
ciscoasa(config-rtr)# router-id 192.168.1.1
ciscoasa(config-rtr)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show ospf	OSPFv2 ルーティング プロセスに関する一般情報を表示します。

router-id cluster-pool

レイヤ 3 クラスタリング用のルータ ID のクラスタ プールを指定するには、ルータ コンフィギュレーション モード（OSPFv2 の場合）または IPv6 ルータ コンフィギュレーション モード（OSPFv3 の場合）で **router-id cluster-pool** コマンドを使用します。

router-id cluster-pool hostname | A.B.C.D *ip_pool*

構文の説明

cluster-pool	レイヤ 3 クラスタリングが設定されている場合に IP アドレス プールを設定します。
hostname | A.B.C.D	この OSPF プロセスの OSPF ルータ ID を指定します。
ip_pool	IP アドレス プールの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	—	—
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

ルータ ID は、クラスタリングの OSPFv2 または OSPFv3 ルーティング ドメイン内で一意である必要があります。同じ OSPFv2 または OSPFv3 ドメイン内の 2 つのルータが同じルータ ID を使用している場合、クラスタリングでのルーティングが正しく動作しない可能性があります。

レイヤ 2 クラスタリングでは、すべてのユニットで同じルータ ID を受け取る場合、**router-id** *id* コマンドを設定するか、ルータ ID を空白のままにする必要があります。

レイヤ 3 クラスタのインターフェイスを設定するときは、インターフェイスの IP アドレスをユニットごとに一意にする必要があります。各ユニットのインターフェイスの IP アドレスが一意になるようにするには、**router-id cluster-pool** コマンドを使用して、OSPFv2 または OSPFv3 用に IP アドレスのローカル プールを設定します。

例

次に、OSPFv2 用にレイヤ 3 クラスタリングが設定されている場合の IP アドレス プールを設定する例を示します。

```
ciscoasa(config)# ip local pool rpool 1.1.1.1-1.1.1.4
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# router-id cluster-pool rpool
ciscoasa(config-rtr)# network 17.5.0.0 255.255.0.0 area 1
ciscoasa(config-rtr)# log-adj-changes
```

次に、OSPFv3 用にレイヤ 3 クラスタリングが設定されている場合の IP アドレス プールを設定する例を示します。

```
ciscoasa(config)# ipv6 router ospf 2
ciscoasa(config-rtr)# router-id cluster-pool rpool
ciscoasa(config-rtr)# interface gigabitEthernet0/0
ciscoasa(config-rtr)# nameif inside
ciscoasa(config-rtr)# security-level 0
ciscoasa(config-rtr)# ip address 17.5.33.1 255.255.0.0 cluster-pool inside_pool
ciscoasa(config-rtr)# ipv6 address 8888::1/64 cluster-pool p6
ciscoasa(config-rtr)# ipv6 nd suppress-ra
ciscoasa(config-rtr)# ipv6 ospf 2 area 0.0.0.0
```

関連コマンド

コマンド	説明
ipv6 router ospf	IPv6 のルータ コンフィギュレーション モードを開始します。
router ospf	ルータ コンフィギュレーション モードを開始します。
show ipv6 ospf	OSPFv3 ルーティング プロセスに関する一般情報を表示します。
show ospf	OSPFv2 ルーティング プロセスに関する一般情報を表示します。

router isis

IS-IS ルーティング プロトコルをイネーブルにし、IS-IS プロセスを指定するには、グローバル コンフィギュレーション モードで **router isis** コマンドを使用します。IS-IS ルーティ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。

router isis

no router isis

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。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、エリアの IS-IS ルーティングをイネーブルするために使用されます。エリアのエリア アドレスおよび ASA のシステム ID を指定するために、適切なネットワーク エンティティ タイトル（NET）が設定されている必要があります。隣接関係が確立されてダイナミック ルーティングが可能になる前に、1 つ以上のインターフェイスでルーティングをイネーブルにする必要があります。IS-IS の設定に使用するコマンドのリストについては、「関連コマンド」の表を参照してください。

例

次に、IS-IS ルーティングをイネーブルにする例を示します。

```
ciscoasa# configure terminal
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

関連コマンド

router ospf

OSPF ルーティング プロセスを開始して、そのプロセス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 **router ospf** コマンドを使用します。OSPF ルーティ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。

router ospf *pid*

no router ospf *pid*

構文の説明

pid	OSPF ルーティング プロセスの内部的に使用される ID パラメータ。有効な値は、1 ～ 65535 です。*pid* は、他のルータの OSPF プロセスの ID と一致する必要はありません。

デフォルト

OSPF ルーティングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードはサポートされます。

使用上のガイドライン

router ospf コマンドは、ASA 上で実行される OSPF ルーティング プロセスのグローバル コンフィギュレーション コマンドです。**router ospf** コマンドを入力すると、ルータ コンフィギュレーション モードであることを示す (config-router)# コマンド プロンプトが表示されます。

no router ospf コマンドを使用する場合は、必要な情報を指定する場合を除き、オプションの引数を指定する必要はありません。**no router ospf** コマンドは、*pid* によって指定された OSPF ルーティング プロセスを終了します。*pid* は、ASA においてローカルに割り当てます。OSPF ルーティング プロセスごとに固有の値を割り当てる必要があります。

router ospf コマンドは、次の OSPF 固有のコマンドとともに、OSPF ルーティング プロセスを設定するために使用されます。

- **area**：通常の OSPF エリアを設定します。
- **compatible rfc1583**：集約ルートのコスト計算に使用される方法を RFC 1583 に従った方法に戻します。
- **default-information originate**：OSPF ルーティング ドメインへのデフォルト外部ルートを生成します。
- **distance**：ルート タイプに基づいて、OSPF ルート アドミニストレーティブ ディスタンスを定義します。
- **ignore**：ルータがタイプ 6 Multicast OSPF（MOSPF）パケットのリンクステート アドバタイズメント（LSA）を受信した場合の syslog メッセージの送信を抑制します。
- **log-adj-changes**：OSPF ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。
- **neighbor**：ネイバー ルータを指定します。VPN トンネル経由での隣接関係の確立を許可するために使用します。
- **network**：OSPF が実行されるインターフェイス、およびそれらのインターフェイスのエリア ID を定義します。
- **redistribute**：指定されたパラメータに従って、ルーティング ドメイン間でのルートの再配布を設定します。
- **router-id**：固定ルータ ID を作成します。
- **summary-address**：OSPF の集約アドレスを作成します。
- **timer lsa arrival**：OSPF ネイバーから同一のリンクステート アドバタイズメント（LSA）を受け入れる最小間隔（ミリ秒）を定義します。
- **timer pacing flood**：フラッディング キュー内の LSA の更新の最小間隔（ミリ秒）を定義します。
- **timer pacing lsa-group**：LSA のグループのリフレッシュまたは管理の間隔（秒）を定義します。
- **timer pacing retransmission**：ネイバー再送信の最小間隔（ミリ秒）を定義します。
- **timer throttle lsa**：LSA の最初のオカレンスを生成する遅延（ミリ秒）を定義します。
- **timer throttle spf**：SPF 計算の変更を受信する遅延（ミリ秒）を定義します。
- **timer nsf wait**：NSF 再起動中のインターフェイス待機間隔を定義します。デフォルト値は 20 秒です。許容範囲は 1 ～ 65535 秒です。

例

次に、OSPF ルーティング プロセス番号 5 のコンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# router ospf 5
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションから OSPF ルータ コマンドをクリアします。
show running-config router ospf	実行コンフィギュレーション内の OSPF ルータ コマンドを表示します。

router rip

RIP ルーティング プロセスを開始して、そのプロセス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 **router rip** コマンドを使用します。RIP ルーティング プロセ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。

router rip

no router rip

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。

デフォルト

RIP ルーティングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

router rip コマンドは、ASA 上の RIP ルーティング プロセスを設定するためのグローバル コンフィギュレーション コマンドです。ASA では、1 つの RIP プロセスのみを設定できます。**no router rip** コマンドは、RIP ルーティング プロセスを終了し、そのプロセスのすべてのルータ コンフィギュレーションを削除します。

router rip コマンドを入力すると、コマンド プロンプトが、ルータ コンフィギュレーション モードであることを示す ciscoasa(config-router)# に変更されます。

router rip コマンドは、次のルータ コンフィギュレーション コマンドとともに、RIP ルーティング プロセスを設定するために使用されます。

- **auto-summary**：ルートの自動集約をイネーブルまたはディセーブルにします。
- **default-information originate**：デフォルト ルートを配布します。
- **distribute-list in**：着信ルーティング更新のネットワークをフィルタリングします。
- **distribute-list out**：発信ルーティング更新のネットワークをフィルタリングします。
- **network**：ルーティング プロセスでインターフェイスを追加または削除します。

- **passive-interface**：特定のインターフェイスをパッシブ モードに設定します。
- **redistribute**：他のルーティング プロセスから RIP ルーティング プロセスにルートを再配布します。
- **version**：ASA で使用される RIP プロトコル バージョンを設定します。

また、次のコマンドをインターフェイス コンフィギュレーション モードで使用して、インターフェイスごとの RIP プロパティを設定できます。

- **rip authentication key**：認証キーを設定します。
- **rip authentication mode**：RIP バージョン 2 によって使用される認証のタイプを設定します。
- **rip send version**：インターフェイスから更新を送信するために使用する RIP のバージョンを設定します。グローバル ルータ コンフィギュレーション モードでバージョンが設定されている場合は、このコマンドによって上書きされます。
- **rip receive version**：インターフェイスで受け入れる RIP のバージョンを設定します。グローバル ルータ コンフィギュレーション モードでバージョンが設定されている場合は、このコマンドによって上書きされます。

トランスペアレント モードでは RIP はサポートされていません。デフォルトで、ASA は、すべての RIP ブロードキャスト パケットおよびマルチキャスト パケットを拒否します。これらの RIP メッセージが、トランスペアレント モードで動作する ASA を通過できるようにするには、このトラフィックを許可するアクセス リスト エントリを定義する必要があります。たとえば、RIP バージョン 2 トラフィックが ASA を通過できるようにするには、次のようなアクセス リスト エントリを作成します。

```
ciscoasa(config)# access-list myriplist extended permit ip any host 224.0.0.9
```

RIP バージョン 1 のブロードキャストを許可するには、次のようなアクセス リスト エントリを作成します。

```
ciscoasa(config)# access-list myriplist extended permit udp any any eq rip
```

access-group コマンドを使用して、これらのアクセス リスト エントリを適切なインターフェイスに適用します。

ASA では、RIP ルーティングと OSPF ルーティングの両方を同時にイネーブルにできます。

例

次に、OSPF ルーティング プロセス番号 5 のコンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# router rip
ciscoasa(config-rtr)# network 10.0.0.0
ciscoasa(config-rtr)# version 2
```

関連コマンド

コマンド	説明
clear configure router rip	実行コンフィギュレーションから RIP ルータ コマンドをクリアします。
show running-config router rip	実行コンフィギュレーション内の RIP ルータ コマンドを表示します。

rtp-conformance

ピンホールを通過する RTP パケットが H.323 および SIP プロトコルに準拠しているかどうかをチェックするには、パラメータ コンフィギュレーション モードで **rtp-conformance** 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。

rtp-conformance [enforce-payloadtype]

no rtp-conformance [enforce-payloadtype]

構文の説明

enforce-payloadtype	シグナリング交換に基づいて、ペイロード タイプをオーディオまたはビデオであると指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、ピンホールを通過する RTP パケットが H.323 コールのプロトコルに準拠しているかどうかをチェックする例を示します。

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# rtp-conformance
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
debug rtp	H.323 および SIP インスペクションに関連する RTP パケットのデバッグ情報およびエラー メッセージを表示します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

rtp-min-port rtp-max-port（廃止予定）

電話プロキシ機能の rtp-min-port および rtp-max-port の制限を設定するには、電話プロキシ コンフィギュレーション モードで **rtp-min-port rtp-max-port** コマンドを使用します。電話プロキシ コンフィギュレーションから制限を削除するには、このコマンドの **no** 形式を使用します。

rtp-min-port *port1* **rtp-maxport** *port2*

no rtp-min-port *port1* **rtp-maxport** *port2*

構文の説明

port1	メディア ターミネーション ポイントの RTP ポート範囲の最小値を指定します。*port1* には、1024 ～ 16384 の値を指定できます。
port2	メディア ターミネーション ポイントの RTP ポート範囲の最大値を指定します。*port2* には、32767 ～ 65535 の値を指定できます。

デフォルト

デフォルトで、**rtp-min-port** キーワードの *port1* の値は 16384、**rtp-max-port** キーワードの *port2* の値は 32767 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Phone-Proxy コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	コマンドが追加されました。
9.4(1)	このコマンドは、すべての **phone-proxy** モード コマンドとともに廃止されました。

使用上のガイドライン

電話プロキシでサポートするコール数の規模を調整する必要がある場合は、メディア ターミネーション ポイントの RTP ポート範囲を設定します。

例

次に、**rtp-min-port** コマンドを使用して、メディア接続に使用するポートを指定する例を示します。

```
ciscoasa(config-phone-proxy)# rtp-min-port 2001 rtp-maxport 32770
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。