CHAPTER 23

queue-limit コマンド～ rtp-conformance コマンド

queue-limit（プライオリティ キュー）

プライオリティ キューの深さを指定するには、プライオリティ キュー モードで **queue-limit** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

queue-limit *number-of-packets*

no queue-limit *number-of-packets*

シンタックスの説明

number-of-packets	インターフェイスがパケットのドロップを開始するまで、キューに入れる（つまり、バッファ処理する）ことができる低遅延パケットまたは通常の優先順位のパケットの最大数を指定します。指定可能な値の範囲については、「使用上の注意」の項を参照してください。

デフォルト

デフォルトでは、キューの上限は 1,024 パケットです。

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	透過	シングル	コンテキスト	システム
プライオリティ キュー	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、次の 2 つのトラフィック クラスを使用できます。1 つは優先順位が高く、遅延に影響されやすいトラフィック（音声およびビデオなど）用の Low-Latency Queuing（LLQ; 低遅延キューイング）で、もう 1 つは、それ以外のすべてのトラフィック用のベストエフォート（デフォルト）です。セキュリティ アプライアンスは、優先トラフィックを認識し、適切な Quality of Service（QoS; サービス品質）ポリシーを適用します。プライオリティ キューのサイズと項目数を設定することで、トラフィック フローを微調整できます。

プライオリティ キューイングを有効にするには、**priority-queue** コマンドを使用して、インターフェイスのプライオリティ キューをあらかじめ作成しておく必要があります。1 つの **priority-queue** コマンドを、**nameif** コマンドで定義できるすべてのインターフェイスに対して適用できます。

priority-queue コマンドを使用すると、プライオリティ キュー モードに入ります。モードはプロンプトに表示されます。プライオリティ キュー モードでは、いつでも送信キューに入れることができるパケットの最大数（**tx-ring-limit** コマンド）、およびバッファに入れることのできる両タイプ（優先またはベストエフォート）のパケット数を設定できます（**queue-limit** コマンド）。queue-limit の数を超えると、以後のパケットはドロップされます。

（注） インターフェイスのプライオリティ キューイングをイネーブルにするには、**priority-queue** コマンドを設定する必要があります。

指定する tx-ring-limit および queue-limit は、優先順位の高い低遅延キューとベストエフォート キューの両方に適用されます。tx-ring-limit は、ドライバが許容できる両タイプのパケットの数です。このパケットの処理が終わると、ドライバは輻輳が解消するまで、インターフェイスの先頭にある、パケットをバッファしているキューの処理に戻ります。一般に、これらの 2 つのパラメータを調整することによって、低遅延トラフィックのフローを最適化できます。

キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これが「テール ドロップ」です。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファ サイズを大きくします。

（注） **queue-limit** コマンドと **tx-ring-limit** コマンドの値の範囲の上限は、実行時に動的に決まります。この上限値を表示するには、コマンドラインで **help** または **?** と入力します。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。キューは、使用可能なメモリの量を超えることはできません。理論上の最大パケット数は 2,147,483,647 です。

例

次の例では、test というインターフェイスのプライオリティ キューを設定して、キューの上限を 30,000 パケット、送信キューの上限を 256 パケットと指定しています。

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 30000
hostname(priority-queue)# tx-ring-limit 256
hostname(priority-queue)#
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show priority-queue statistics	指定したインターフェイスのプライオリティ キュー統計情報を表示します。
show running-config [all] priority-queue	現在のプライオリティ キュー コンフィギュレーションを表示します。**all** キーワードを指定すると、現在のすべてのプライオリティ キュー、および queue-limit と tx-ring-limit のコンフィギュレーション値が表示されます。
tx-ring-limit	イーサネット送信ドライバのキューにいつでも入れることができるパケットの最大数を設定します。

queue-limit（tcp マップ）

TCP ストリームのキューに入れることのできる順序付けされていないパケットの最大数を設定するには、tcp マップ コンフィギュレーション モードで **queue-limit** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

queue-limit *pkt_num*

no queue-limit *pkt_num*

シンタックスの説明

pkt_num	順序付けされていないパケットがドロップされるまでに、TCP 接続のキューに入れることのできる、順序付けされていないパケットの最大数を指定します。範囲は 0 ～ 250 です。デフォルトは 0 です。

デフォルト

デフォルトの最大パケット数は 0 です。

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	透過	シングル	コンテキスト	システム
tcp マップ 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
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。tcp マップ コンフィギュレーション モードで **queue-limit** コマンドを使用すると、任意の TCP 接続の TCP パケットの順序付けをイネーブルにしたり、デフォルトで順序付けされている接続のキューの上限を変更したりできます。

検査、IDS 機能、または TCP check-retransmission のいずれかの機能がイネーブルになっている場合、パケットは TCP 接続上で順序付けされます。順序付けされている接続のパケット キューのデフォルトの上限は、1 フローにつき 2 つです。それ以外のすべての TCP 接続の場合、パケットは受信と同時に転送されます。これには、順序付けされていないパケットも含まれます。任意の TCP 接続の TCP パケットの順序付けをイネーブルにする、または順序付けされている接続のキューの上限を変更するには、**queue-limit** コマンドを使用します。この機能をイネーブルにすると、順序付けされていないパケットは、転送できるようになるまでキューに保持されるか、または一定の時間が経過するまでキューに保持されます。したがって、メモリ使用量は、パケットのバッファ処理により増加します。

例

次の例は、すべての Telnet 接続の TCP パケットの順序付けをイネーブルにする方法を示しています。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# queue-limit 8
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq telnet
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

コマンド	説明
class-map	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。

quit

現在のコンフィギュレーション モードを終了する、または特権 EXEC モードまたはユーザ EXEC モードからログアウトするには、**quit** コマンドを使用します。

quit

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

キー シーケンス ***Ctrl+Z*** を使用しても、グローバル コンフィギュレーション（およびそれより上位の）モードを終了できます。このキー シーケンスは、特権 EXEC モードおよびユーザ EXEC モードでは機能しません。

特権 EXEC モードまたはユーザ EXEC モードで **quit** コマンドを入力すると、セキュリティ アプライアンスからログアウトします。特権 EXEC モードからユーザ EXEC モードに戻るには、**disable** コマンドを使用します。

例

次の例は、**quit** コマンドを使用してグローバル コンフィギュレーション モードを終了し、セッションからログアウトする方法を示しています。

```
hostname(config)# quit
hostname# quit

Logoff
```

次の例は、**quit** コマンドを使用してグローバル コンフィギュレーション モードを終了し、その後、**disable** コマンドを使用して特権 EXEC モードを終了する方法を示しています。

```
hostname(config)# quit
hostname# disable
hostname>
```

関連コマンド

コマンド	説明
exit	コンフィギュレーション モードを終了します。または、特権 EXEC モードまたはユーザ EXEC モードからログアウトします。

radius-common-pw

セキュリティ アプライアンスを経由してこの RADIUS 認可サーバにアクセスするすべてのユーザが使用する共通のパスワードを指定するには、AAA サーバ ホスト モードで **radius-common-pw** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

radius-common-pw *string*

no radius-common-pw

シンタックスの説明

string	この RADIUS サーバとのすべての認可トランザクションで共通のパスワードとして使用される最大 127 文字の英数字のキーワード。大文字と小文字は区別されます。

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	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このリリースで導入されました。

使用上のガイドライン

このコマンドは、RADIUS 認可サーバに対してのみ有効です。

RADIUS 認可サーバは、接続する各ユーザのパスワードとユーザ名を要求します。セキュリティ アプライアンスは、ユーザ名を自動的に入力します。ここでユーザは、パスワードを入力します。RADIUS サーバ管理者は、このパスワードを、このセキュリティ アプライアンスを経由してサーバに権限を与える各ユーザと関連付けるように、RADIUS サーバを設定する必要があります。この情報は、RADIUS サーバ管理者に必ず提供してください。

共通のユーザ パスワードを指定しない場合、各ユーザのパスワードは、ユーザ各自のユーザ名となります。たとえば、ユーザ名が「jsmith」のユーザは、「jsmith」と入力します。ユーザ名を共通のユーザ パスワードとして使用している場合は、セキュリティ対策として、この RADIUS サーバを使用ネットワーク外で認可用に使用しないでください。

（注） このフィールドは、基本的にスペースを埋めるためのものです。RADIUS サーバは、このフィールドを予期および要求しますが、使用することはありません。ユーザは、このフィールドを知っている必要はありません。

例

次の例では、ホスト「1.2.3.4」上に「svrgrp1」という RADIUS AAA サーバ グループを設定し、タイムアウト間隔を 9 秒に、リトライ間隔を 7 秒に設定します。さらに、RADIUS 共通パスワードを「allauthpw」に設定します。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# radius-common-pw allauthpw
hostname(config-aaa-server-host)# exit
hostname(config)#
```

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 モードに入って、ホスト固有の AAA 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 コマンド文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。

radius-with-expiry

認証中に MS-CHAPv2 を使用してユーザとパスワード アップデートをネゴシエートするようにセキュリティ アプライアンスを設定するには、トンネル グループ ipsec アトリビュート コンフィギュレーション モードで **radius-with-expiry** コマンドを使用します。RADIUS 認証が設定されていない場合、このコマンドはセキュリティ アプライアンスで無視されます。

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。

radius-with-expiry

no radius-with-expiry

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、このコマンドの設定はディセーブルになっています。

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	透過	シングル	コンテキスト	システム
トンネル グループ ipsec アトリビュート 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
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは廃止されました。**password-management** コマンドに置き換えられました。**radius-with-expiry** コマンドの **no** 形式はサポートされなくなりました。

使用上のガイドライン

このアトリビュートは、IPSec リモートアクセス トンネル グループ タイプだけに適用できます。

例

次の例では、config-ipsec コンフィギュレーション モードで入り、remotegrp というリモートアクセス トンネル グループの radius-with-expiry を設定しています。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# radius-with-expiry
hostname(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループを消去します。
password-management	パスワードの管理をイネーブルにします。トンネル グループ一般アトリビュート コンフィギュレーション モードでは、**radius-with-expiry** コマンドはこのコマンドに置き換えられます。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec アトリビュートを設定します。

rate-limit

モジュラ ポリシー フレームワークを使用するとき、一致またはクラス コンフィギュレーション モードで **rate-limit** コマンドを使用して、**match** コマンドまたはクラス マップと一致するパケットのメッセージ レートを制限します。このレート制限アクションは、アプリケーション トラフィックの検査ポリシー マップ（**policy-map type inspect** コマンド）で有効です。ただし、すべてのアプリーションでこのアクションが許可されるわけではありません。このアク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。

rate-limit *messages_per_second*

no rate-limit *messages_per_second*

シンタックスの説明

messages_per_second	秒ごとにメッセージを制限します。

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	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス 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
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

検査ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。検査ポリシー マップで使用できるコマンド自体は、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを特定した後（**class** コマンドは、**match** コマンドを含む、既存の **class-map type inspect** コマンドを参照します）、メッセージのレートを制限する **rate-limit** コマンドを入力できます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション検査をイネーブルにするときは、このアクションを含んでいる検査ポリシー マップをイネーブルにします。たとえば、**inspect dns dns_policy_map** コマンドを入力します。dns_policy_map は検査ポリシー マップの名前です。

例

次の例では、招待要求メッセージを毎秒 100 件までに制限します。

```
hostname(config-cmap)# policy-map type inspect sip sip-map1
hostname(config-pmap-c)# match request-method invite
hostname(config-pmap-c)# rate-limit 100
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス 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検査クラス 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。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

reactivation-mode

グループ内の障害のあるサーバを再度有効にする方法を指定するには、AAA サーバ グループ モードで **reactivation-mode** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

no reactivation-mode [**depletion** [**deadtime** *minutes*] | **timed**]

シンタックスの説明

deadtime *minutes*	（オプション）グループ内の最後のサーバをディセーブルにしてから、すべてのサーバを再度イネーブルにするまでの時間の長さを、0 から 1440 分までの間で指定します。デフォルトは 10 分です。
depletion	グループ内のすべてのサーバが非アクティブになった場合のみ、障害のあるサーバを再度有効にします。
timed	30 秒のダウン時間が経過した後に、障害のあるサーバを再度有効にします。

デフォルト

デフォルトの再有効化モードは depletion で、デフォルトの deadtime 値は 10 です。

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	透過	シングル	コンテキスト	システム
AAA サーバ ホスト 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
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

各サーバ グループには、グループ内のサーバの再有効化ポリシーを指定するアトリビュートがあります。

depletion モードでは、あるサーバが無効になると、グループ内の他のすべてのサーバが非アクティブになるまで、そのサーバは非アクティブのままとなります。この事態が発生した場合、グループ内のすべてのサーバは再有効化されます。この方法で、障害のあるサーバが原因の接続遅延の発生が最小限に抑えられます。***depletion*** モードを使用している場合は、***deadtime*** パラメータも指定できます。***deadtime*** パラメータは、グループ内の最後のサーバをディセーブルにしてから、すべてのサーバを再度イネーブルにするまでの時間の長さ（分）を指定します。このパラメータは、サーバ グループがローカル フォールバック機能と連動して使用されている場合に限り、意味を持ちます。

timed モードでは、障害のあるサーバは、30 秒のダウン時間が経過した後に再有効化されます。これは、サーバ リスト内の最初のサーバをプライマリ サーバとして使用していて、可能な場合は常にそのサーバがオンラインであることが望ましい場合に役立ちます。このポリシーは、UDP サーバの場合は機能しません。UDP サーバへの接続は、たとえそのサーバが存在しない場合でも失敗しないため、UDP サーバは無条件にオンラインに戻ります。このモードでは、サーバ リストに到達不能なサーバが複数含まれている場合に、接続時間が長くなったり、接続が失敗したりする可能性があります。

同時アカウンティングがイネーブルになっているアカウンティング サーバ グループには、強制的に ***timed*** モードが適用されます。これは、所定のリスト内のすべてのサーバが同等であることを意味します。

例

次の例では、depletion 再有効化モードを使用するように、「srvgrp1」という aTACACS+ AAA サーバを設定します。deadtime は 15 分に設定します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-sersver-group)# reactivation-mode depletion deadtime 15
hostname(config-aaa-server)# exit
hostname(config)#
```

次の例では、timed 再有効化モードを使用するように、「srvgrp1」という aTACACS+ AAA サーバを設定します。

```
hostname(config)# aaa-server svrgrp2 protocol tacacs+
hostname(config-aaa-server)# reactivation-mode timed
hostname(config-aaa-server)#
```

関連コマンド

accounting-mode	アカウンティング メッセージを 1 つのサーバに送信するか、グループ内のすべてのサーバに送信するかを指定します。
aaa-server protocol	AAA サーバ グループ コンフィギュレーション モードに入って、グループ内のすべてのホストに共通する、グループ固有の AAA パラメータを設定できるようにします。
max-failed-attempts	サーバ グループ内の所定のサーバが無効になるまでに、そのサーバで許容される接続試行の失敗数を指定します。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
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。

redistribute（OSPF）

あるルーティング ドメインから OSPF ルーティング ドメインにルートを再配布するには、ルータ コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布を削除するには、このコマンドの **no** 形式を使用します。

redistribute {{***ospf*** *pid* [***match*** {***internal*** | ***external*** [***1*** | ***2***] | ***nssa-external*** [***1*** | ***2***]}]} | **rip** | ***static*** | ***connected***} [***metric*** *metric_value*] [***metric-type*** *metric_type*] [***route-map*** *map_name*] [***tag*** *tag_value*] [***subnets***]

no redistribute {{***ospf*** *pid* [***match*** {***internal*** | ***external*** [***1*** | ***2***] | ***nssa-external*** [***1*** | ***2***]}]} | ***rip*** | ***static*** | ***connected***} [***metric*** *metric_value*] [***metric-type*** *metric_type*] [***route-map*** *map_name*] [***tag*** *tag_value*] [***subnets***]

シンタックスの説明

connected	インターフェイスに接続されているネットワークを OSPF ルーティング プロセスに再配布することを指定します。
external *type*	指定した自律システムの外部の OSPF メトリック ルートを指定します。有効な値は、**1** または **2** です。
internal *type*	指定した自律システム内部の OSPF メトリック ルートを指定します。
match	（オプション）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ための条件を指定します。
metric *metric_value*	（オプション）OSPF デフォルト メトリック値を指定します（0 ～ 16777214）。
metric-type *metric_type*	（オプション）OSPF ルーティング ドメインにアドバタイズされる、デフォルト ルートに関連付けられた外部リンク タイプ。2 つの値、つまり ***1***（タイプ 1 外部ルート）または ***2***（タイプ 2 外部ルート）のいずれかを使用できます。
nssa-external *type*	NSSA への外部のルートの OSPF メトリック タイプを指定します。有効な値は、**1** または **2** です。
ospf *pid*	OSPF ルーティング プロセスを現在の OSPF ルーティング プロセスに再配布するために使用されます。*pid* には、OSPF ルーティング プロセス用に内部的に使用される識別パラメータを指定します。有効な値は、1 ～ 65535 です。
rip	ネットワークを RIP ルーティング プロセスから現在の OSPF ルーティング プロセスに再配布するように指定します。
route-map *map_name*	（オプション）ソース ルーティング プロトコルから現在の OSPF ルーティング プロトコルへインポートされたルートをフィルタリングするために使用されるルート マップの名前です。指定しない場合、すべてのルートが再配布されます。
static	スタティック ルートを OSPF プロセスに再配布するために使用されます。
subnets	（オプション）ルートを OSPF に再配布する場合に、指定プロトコルの再配布を確認します。使用しない場合、クラスフル ルートだけが再配布されます。
tag *tag_value*	（オプション）各外部ルートに対応付けられた 32 ビットの 10 進値。この値は、OSPF 自体によって使用されることはありません。ASBR 間で情報を交換するために使用されます。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用され、その他のプロトコルには 0 が使用されます。有効な値は 0 ～ 4294967295 です。

デフォルト

コマンドのデフォルト値は、次のとおりです。

- ***metric*** *metric-value*：0
- ***metric-type*** *type-value*：***2***
- ***match***：***Internal***、***external 1***、***external 2***
- ***tag*** *tag-value*：0

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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.2(1)	このコマンドが、***rip*** キーワードを含めるように修正されました。

例

次の例は、スタティック ルートを現在の OSPF プロセスに再配布する方法を示しています。

```
hostname(config)# router ospf 1
hostname(config-router)# redistribute static
```

関連コマンド

コマンド	説明
redistribute（RIP）	ルートを RIP ルーティング プロセスへ再配布します。
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

redistribute（RIP）

別のルーティング ドメインから RIP ルーティング プロセスにルートを再配布するには、ルータ コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布を削除するには、このコマンドの **no** 形式を使用します。

redistribute {{***ospf*** *pid* [***match*** {***internal*** | ***external*** [***1*** | ***2***] | ***nssa-external*** [***1*** | ***2***]}]} | ***static*** | ***connected***} [***metric*** {*metric_value* | ***transparent***}] [***route-map*** *map_name*]

no redistribute {{***ospf*** *pid* [***match*** {***internal*** | ***external*** [***1*** | ***2***] | ***nssa-external*** [***1*** | ***2***]}]} | ***static*** | ***connected***} [***metric*** {*metric_value* | ***transparent***}] [***route-map*** *map_name*]

シンタックスの説明

connected	インターフェイスに接続されているネットワークを RIP ルーティング プロセスに再配布することを指定します。
external *type*	指定した自律システムの外部の OSPF メトリック ルートを指定します。有効な値は、**1** または **2** です。
internal *type*	指定した自律システム内部の OSPF メトリック ルートを指定します。
match	（オプション）OSPF から RIP へルートを再配布するための条件を指定します。
metric {*metric_value* | ***transparent***}	（オプション）再配布されるルートの RIP メトリック値を指定します。*metric_value* として有効な値は 0 から 16 です。メトリックを ***transparent*** に設定すると、現在のルート メトリックが使用されます。
nssa-external *type*	not-so-stubby area（NSSA; 準スタブ エリア）外部のルートの OSPF メトリック タイプを指定します。有効な値は、**1** または **2** です。
ospf *pid*	OSPF ルーティング プロセスを RIP ルーティング プロセスに再配布するために使用されます。*pid* には、OSPF ルーティング プロセス用に内部的に使用される識別パラメータを指定します。有効な値は、1 ～ 65535 です。
route-map *map_name*	（オプション）ソース ルーティング プロセスから RIP ルーティング プロセスへインポートされたルートをフィルタリングするために使用されるルート マップの名前です。指定しない場合、すべてのルートが再配布されます。
static	スタティック ルートを OSPF プロセスに再配布するために使用されます。

デフォルト

コマンドのデフォルト値は、次のとおりです。

- ***metric*** *metric-value*：0
- ***match***：***Internal***、***external 1***、***external 2***

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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例は、スタティック ルートを現在の RIP プロセスに再配布する方法を示しています。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# redistribute static metric 2
```

関連コマンド

コマンド	説明
redistribute（OSPF）	他のルーティング ドメインから OSPF へルートを再配布します。
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 モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

regex

テキストを照合するための正規表現を作成するには、グローバル コンフィギュレーション モードで **regex** コマンドを使用します。正規表現を削除するには、このコマンドの **no** 形式を使用します。

regex *name regular_expression*

no regex *name* [*regular_expression*]

シンタックスの説明

name	最大 40 文字の正規表現名を指定します。
regular_expression	最大 100 文字の正規表現を指定します。正規表現に使用できるメタ文字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。

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	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

regex コマンドは、テキストの照合が必要なさまざまな機能に使用できます。たとえば、モジュラ ポリシー フレームワークで*検査ポリシー マップ*を使用してアプリケーション検査に対する特殊なアクションを設定できます（**policy map type inspect** コマンドを参照）。検査ポリシー マップでは、1 つ以上の **match** コマンドを含んだ検査クラス マップを作成することで、アクションの実行対象となるトラフィックを指定できます。または、**match** コマンドを検査ポリシー マップ内で直接使用することもできます。一部の **match** コマンドでは、パケットに含まれているテキストを正規表現を使用して識別できます。たとえば、HTTP パケットに含まれている URL 文字列と一致するかどうかを確認できます。正規表現クラス マップ内で正規表現をグループ化できます（**class-map type regex** コマンドを参照）。

正規表現では、完全に文字列と一致するようにテキスト文字列を照合するか、*メタ文字*を使用してテキスト文字列のさまざまな形を照合できます。特定のアプリケーション トラフィックの内容を照合するために正規表現を使用できます。たとえば、HTTP パケット内の本文を照合できます。

表 23-1 は、特殊な意味を持つメタ文字のリストです。

表 23-1　regex のメタ文字

文字	説明	注意事項
.	ドット	任意の 1 文字と一致します。たとえば、**d.g** は dog、dag、dtg、および doggonnit などの文字を含むすべての文字と一致します。
(*exp*)	部分正規表現	部分正規表現によって文字を前後の文字と区別します。部分正規表現には他のメタ文字を使用できます。たとえば、**d(o|a)g** は dog と dag に一致しますが、**do|ag** は do と ag に一致します。また、部分正規表現は繰り返しを意味する文字を区別するために、繰り返し限定作用素と共に使用できます。たとえば、**ab(xy){3}z** は abxyxyxyz に一致します。
|	代用	この記号によって区切られた表現の一方と一致します。たとえば、**dog|cat** は dog または cat と一致します。
?	疑問符	直前の文字が含まれない場合と 1 つ含まれる場合があることを示す限定作用素です。たとえば、**lo?se** は、lse または lose と一致します。 **（注）** **Ctrl+V** キーを入力して疑問符を入力する必要があります。そうしないと、ヘルプ機能が起動されます。
*	アスタリスク	直前の文字が含まれない、1 つ含まれる、繰り返し含まれる場合があることを示す限定作用素です。たとえば、**lo*se** は lse、lose、loose などと一致します。
+	プラス記号	直前の文字が 1 つ以上含まれることを示す限定作用素です。たとえば、**lo+se** は lose と loose に一致しますが、lse とは一致しません。
{*x*}	繰り返し限定作用素	表現が *x* 回、完全に繰り返された文字と一致します。たとえば、**ab(xy){3}z** は abxyxyxyz に一致します。
{*x*,}	最小繰り返し限定作用素	表現が最低限 *x* 回繰り返された文字と一致します。たとえば、**ab(xy){2,}z** は abxyxyz、abxyxyxyz に一致します。
[*abc*]	文字クラス	括弧内の任意の文字と一致します。たとえば、**[abc]** は a、b、または c と一致します。
[^*abc*]	否定文字クラス	括弧内に含まれていない 1 つの文字と一致します。たとえば、**[^abc]** は a、b、または c 以外の 1 文字と一致します。**[^A-Z]** は大文字でない 1 文字と一致します。
[*a-c*]	文字の範囲クラス	指定の範囲内の任意の文字と一致します。**[a-z]** は任意の小文字と一致します。文字と範囲を組み合せることができます。**[abcq-z]** は a、b、c、q、r、s、t、u、v、w、x、y、z と一致し、[**a-cq-z**] も同様です。 ダッシュ（-）記号は、括弧内の最後または最初の文字である場合にのみダッシュとして判断されます。たとえば、**[abc-]** または **[-abc]** などです。
""	引用符	文字列内の末尾と先頭に空いたスペースを保持します。たとえば、**" test"** と指定すると、照合時に先頭のスペースが保持されます。
^	キャレット	行頭を指定します。

表 23-1　regex のメタ文字（続き）

文字	説明	注意事項
\	エスケープ文字	メタ文字と共に使用した場合、表記どおりの文字と一致します。たとえば、**\[** は左角括弧（[）と一致します。
char	文字	文字がメタ文字でない場合、表記どおりの文字と一致します。
\r	キャリッジ リターン	キャリッジ リターン n 0x0d と一致します。
\n	改行	新行 0x0a と一致します。
\t	タブ	タブ 0x09 と一致します。
\f	改ページ	改ページ 0x0c と一致します。
\x*NN*	エスケープされた 16 進数	16 進数（2 桁）を使用する ASCII 文字と一致します。
\NNN	エスケープされた 8 進数	ASCII 文字を 8 進数（3 桁）として照合します。たとえば、040 はスペースを表します。

一致させる対象の文字と完全に一致するかどうか正規表現をテストするには、**test regex** コマンドを入力します。

正規表現のパフォーマンスへの影響は、2 つの主要な要因によって決定されます。

- 正規表現を使用して検索するために必要なテキストの長さ。

  正規表現エンジンは、検索テキストが短い場合、セキュリティ アプライアンスのパフォーマンスにあまり影響を与えません。
- 正規表現を使用して検索するために必要な正規表現関連テーブルの数。

検索テキストの長さがパフォーマンスに与える影響

正規表現を使用した検索を設定する場合、検索するテキストのすべてのバイトは通常、正規表現データベースと照合され、一致する表現が検出されます。検索するテキストの長さに比例して検索時間も長くなります。この検索時間の変化を説明したパフォーマンス テスト ケースを次に示します。

- ある HTTP トランザクションには、300 バイト長の GET 要求と 3250 バイト長の応答が含まれる。
- URI の検索の正規表現が 445 件、要求本文検索の正規表現が 34 件。
- 応答本文検索の正規表現が 55 件。

HTTP GET 要求のみの URI と本文を検索するようポリシーが設定されると、スループットは次のようになります。

- 該当する正規表現データベースが検索されない場合は 420 mbps。
- 該当する正規表現データベースが検索された場合は 413 mbps（これは正規表現利用時のオーバーヘッドが比較的小さいことを示しています）。

しかし、HTTP 応答本文全体も検索するようにポリシーが設定されている場合は、長い応答本文（3250 バイト）を検索することになるので、スループットは 145 mbps に落ちます。

正規表現を使用した検索のテキストの長さが長くなる要因について次に示します。

- 正規表現を使用した検索は複数のさまざまなプロトコル フィールドで設定されます。たとえば、HTTP 検査では、URI だけが正規表現検索用に設定され、URI フィールドだけが正規表現検索の対象となる場合、検索テキストの長さは URI の長さに制限されます。ただし、ヘッダー、本文などの他のプロトコル フィールドも正規表現検索用に設定されている場合、ヘッダーと本文の長さを含めるために検索テキストの長さは長くなります。

- 検索対象のフィールドは長くなります。たとえば、URI が正規表現検索用に設定されると、GET 要求での長い URI の検索は長くなります。また、現在、HTTP 本文の長さは、デフォルトで 200 バイトまでに制限されています。ただし、本文を検索するようポリシーが設定され、本文検索テキストの長さが 5000 バイトに変更された場合、本文検索が長くなるためパフォーマンスに重大な影響が生じます。

関連する正規表現テーブルの数がパフォーマンスに与える影響

現在、URI のすべての正規表現など、同じプロトコル フィールドに設定されているすべての正規表現は、1 つまたは複数の正規表現関連テーブルから構成されるデータベースに保存されます。テーブルの数は、テーブルの構築時に必要なメモリの総容量とメモリの可用性により決定します。正規表現データベースは、次の条件に基づいて、複数のテーブルに分割されます。

- テーブルの最大サイズが 32 MB に制限されているために、必須メモリ総容量が 32 MB 以上であること。
- 隣接する最大メモリが完全な正規表現データベースの構築に不足している場合、サイズの小さい複数のテーブルが構築され、すべての正規表現を収容します。メモリのフラグメンテーションの程度は、相互に影響し合う多くの要因に応じて異なり、フラグメンテーションのレベルを予想することはできません。

複数の関連テーブルでは、各テーブルは正規表現を使用した検索で必ず対象となるので、検索時間は対象テーブルの数に比例して長くなります。

特定のタイプの正規表現は、テーブルのサイズを非常に大きくする傾向があります。ワイルドカードや繰り返しの使用を可能なかぎり避ける方法で正規表現を設計することを検討してください。次のメタ文字の説明については、表 23-1 を参照してください。

- ワイルドカードを使用した正規表現：
  - ドット（.）
- あるクラスの任意の文字と一致するさまざまな文字クラス：
  - [^a-z]
  - [a-z]
  - [abc]]
- 繰り返しを使用した正規表現：
  - *
  - +
  - {n,}
- ワイルドカードと繰り返しを組み合せた正規表現は、テーブルのサイズを劇的に増加させる可能性があります。例：
  - 123.*xyz
  - 123.+xyz
  - [^a-z]+
  - [^a-z]*
  - .*123.*（これは "123" の照合と同じなので実行されません）

次の例では、ワイルドカードと繰り返しの有無に応じて正規表現のメモリ消費量がどのように変化するかを示します。

- 次の 4 つの正規表現のデータベース サイズは、958,464 バイトです。

```
regex r1 "q3rfict9(af.*12)*ercvdf"
regex r2 "qtaefce.*qeraf.*adasdfev"
regex r3 "asdfdfdfds.*wererewr0e.*aaaxxxx.*xxx"
regex r4 "asdfdfdfds.*wererewr0e.*afdsvcvr.*aefdd"
```

- 次の 4 つの正規表現のデータベース サイズは、10240 バイトだけです。

```
regex s1 "abcde"
regex s2 "12345"
regex s3 "123xyz"
regex s4 "xyz123"
```

正規表現の数が多いと正規表現データベースに必要とされるメモリ総容量が増えるので、メモリが断片化されるとテーブルの数が増える可能性が高くなります。正規表現の数の変化に応じたメモリ消費量の例を次に示します。

- 100 個の URI をサンプリング：3,079,168 バイト
- 200 個の URI をサンプリング：7,156,224 バイト
- 500 個の URI をサンプリング：11,198,971 バイト

（注） コンテキストごとの正規表現の最大数は 2048 です。

debug menu regex 40 10 コマンドを使用して、各 regex データベースに関連テーブルがいくつあるかを表示できます。

例

次の例では、検査ポリシー マップで使用する 2 つの正規表現を作成します。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
```

関連コマンド

コマンド	説明
class-map type inspect	アプリケーション固有のトラフィックに一致するかどうかを調べるための検査クラス マップを作成します。
policy-map	トラフィック クラスを 1 つまたは複数のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
class-map type regex	正規表現クラス マップを作成します。
test regex	正規表現をテストします。

reload

コンフィギュレーションをリブートおよびリロードするには、特権 EXEC モードで **reload** コマンドを使用します。

reload [**at** *hh*:*mm* [*month day* | *day month*]] [**cancel**] [**in** [*hh*:]*mm***]** [**max-hold-time** [*hh*:]*mm***]** [**noconfirm**] [**quick**] [**reason** *text*] [**save-config**]

シンタックスの説明

at *hh*:*mm*	（オプション）指定された時刻（24 時間方式のクロックを使用）で実行するように、ソフトウェアのリロードをスケジューリングします。月日を指定しなかった場合、リロードは当日の指定された時刻（指定された時刻が現在の時刻よりあとの場合）または翌日（指定された時刻が現在の時刻より前の場合）に実行されます。00:00 を指定すると、リロードは午前 0 時にスケジューリングされます。リロードは 24 時間以内に実行する必要があります。
cancel	（オプション）スケジューリングされたリロードをキャンセルします。
day	（オプション）日付の番号を指定します。範囲は 1 ～ 31 です。
in [*hh*:]*mm*]	（オプション）指定された時刻（分または時と分）に有効になるように、ソフトウェアのリロードをスケジューリングします。リロードは 24 時間以内に実行する必要があります。
max-hold-time [*hh:*]*mm*	（オプション）シャットダウンまたはリブートの前に、セキュリティ アプライアンスが他のサブシステムに通知するまで待機する最小待機期間を指定します。この時間が経過すると、クイック（強制）シャットダウンまたはリブートが実行されます。
month	（オプション）月名を指定します。月名を表す一意の文字列を作成するため、十分な文字を入力します。たとえば、「Ju」は「June」または「July」を表す可能性があるため一意ではありませんが、「Jul」と入力すれば、正確にこれらの 3 文字で始まる月は他にないので一意になります。
noconfirm	（オプション）ユーザによる確認がないセキュリティ アプライアンスのリロードを許可します。
quick	（オプション）通知したり、すべてのサブシステムを正常にシャットダウンしたりすることなく、クイック リロードを強制します。
reason *text*	（オプション）リロードの理由を 1 ～ 255 文字で指定します。理由テキストは、すべての IPSec VPN クライアント、端末、Tenet、SSH、および ASDM の接続またはセッションに送信されます。 **（注）** isakmp などの一部のアプリケーションで、IPSec VPN クライアントに理由テキストを送信するには、追加コンフィギュレーションが必要です。詳細については、ソフトウェア コンフィギュレーション マニュアルの適切な項を参照してください。
save-config	（オプション）シャットダウンする前に、実行コンフィギュレーションをメモリに保存します。***save-config*** キーワードを入力しない場合、コンフィギュレーションに対する未保存の変更はすべて、リロード後に失われます。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、次の新しい引数およびキーワードを追加するために修正されました。*day*、*hh*、*mm*、*month*、***quick***、***save-config***、および *text*。

使用上のガイドライン　このコマンドを使用すると、セキュリティ アプライアンスをリブートし、コンフィギュレーションをフラッシュからリロードできます。

デフォルトでは、**reload** コマンドは対話型です。セキュリティ アプライアンスは、コンフィギュレーションが修正されていないかどうかを最初にチェックしますが、保存はしません。その場合、セキュリティ アプライアンスは、コンフィギュレーションを保存するためのプロンプトを表示します。マルチ コンテキスト モードでは、セキュリティ アプライアンスは、保存されていないコンフィギュレーションがあるコンテキストごとにプロンプトを表示します。***save-config*** パラメータを指定すると、プロンプトが表示されることなくコンフィギュレーションが保存されます。その場合、セキュリティ アプライアンスは、システムをリロードしてよいか確認するプロンプトを表示します。***y*** と応答するか、***Enter*** キーを押した場合のみ、リロードが開始されます。確認後、セキュリティ アプライアンスは、リロード プロセスを開始するか、スケジューリングします。どちらが実行されるかは、遅延パラメータ（***in*** または ***at***）の指定によって異なります。

デフォルトでは、リロード プロセスは「グレースフル」（「ナイス」とも呼ばれる）モードで動作します。リブートが実行される直前に、登録されているすべてのサブシステムには通知が行われます。この通知により、サブシステムはリブート前に正常にシャットダウンできます。このようなシャットダウンが実行されるまで待つことを避けるには、***max-hold-time*** パラメータで最大待ち時間を指定します。別の方法として、***quick*** パラメータを使用することでも、影響を受けるサブシステムに通知したり、グレースフル シャットダウンを待機したりすることなく、リロード プロセスを強制的に開始できます。

noconfirm パラメータを指定すると、**reload** コマンドの動作を強制的に非対話型にすることができます。この場合、***save-config*** パラメータが指定されていない限り、セキュリティ アプライアンスは、保存されていないコンフィギュレーションをチェックしません。セキュリティ アプライアンスは、システムをリブートする前に確認のプロンプトをユーザに表示しません。遅延パラメータを設定していない場合は、リロード プロセスはすぐに開始またはスケジューリングされます。ただし、***max-hold-time*** パラメータまたは ***quick*** パラメータを指定して、動作またはリロード プロセスを制御することはできます。

スケジューリングされたリロードをキャンセルするには、**reload cancel** を使用します。すでに進行中のリロードは、キャンセルできません。

（注）　フラッシュ　パーティションに書き込まれていないコンフィギュレーションの変更は、リロードすると失われます。リブートする前に、**write memory** コマンドを入力して、現在のコンフィギュレーションをフラッシュ パーティションに保存してください。

例

次の例は、コンフィギュレーションをリブートおよびリロードする方法を示しています。

```
hostname# reload
Proceed with ?  [confirm] y

Rebooting...

XXX Bios VX.X
...
```

関連コマンド

コマンド	説明
show reload	セキュリティ アプライアンスのリロード ステータスを表示します。

remote-access threshold session-threshold-exceeded

しきい値を設定するには、グローバル コンフィギュレーション モードで **remote-access threshold** コマンドを使用します。しきい値を削除するには、このコマンドの **no** 形式を使用します。このコマンドは、アクティブなリモートアクセス セッションの数を指定します。この数に達した時点で、セキュリティ アプライアンスはトラップを送信します。

remote-access threshold session-threshold-exceeded {*threshold-value*}

no **remote-access threshold session-threshold-exceeded**

シンタックスの説明

threshold-value	セキュリティ アプライアンスがサポートしているセッション上限以下の整数を指定します。

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	透過	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	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1) (1)	このコマンドが導入されました。

使用上のガイドライン

例

次の例は、しきい値として 1500 を設定する方法を示しています。

```
hostname# remote-access threshold session-threshold-exceeded 1500
```

関連コマンド

コマンド	説明
snmp-server enable trap remote-access	しきい値のトラッピングをイネーブルにします。

rename

コピー元ファイル名からコピー先ファイル名に、ファイルまたはディレクトリの名前を変更するには、特権 EXEC モードで **rename** コマンドを使用します。

rename ***[/noconfirm]*** ***[*****flash:*****]*** *source-path* **[flash:]** *destination-path*

シンタックスの説明

/noconfirm	（オプション）確認プロンプトを表示しないようにします。
destination-path	コピー先ファイルのパスを指定します。
flash:	（オプション）内蔵フラッシュ メモリを指定し、続けてコロン（:）を入力します。
source-path	コピー元ファイルのパスを指定します。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

rename flash: flash: コマンドは、コピー元とコピー先のファイル名を入力するためのプロンプトを表示します。

ファイル システム全体で、ファイルまたはディレクトリの名前を変更することはできません。

次の例を参考にしてください。

```
hostname# rename flash: disk1:
Source filename []? new-config
Destination filename []? old-config
%Cannot rename between filesystems
```

例

次の例は、「test」という名前のファイルを「test1」に変更する方法を示しています。

```
hostname# rename flash: flash:
Source filename [running-config]? test
Destination filename [n]? test1
```

関連コマンド

コマンド	説明
mkdir	新しいディレクトリを作成します。
rmdir	ディレクトリを削除します。
show file	ファイル システムに関する情報を表示します。

rename（クラス マップ）

クラス マップの名前を変更するには、クラス マップ コンフィギュレーション モードで **rename** コマンドを入力します。

rename *new_name*

シンタックスの説明

new_name	クラス マップの新しい名前の最大長は 40 文字です。class-default という名前は予約されています。

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	透過	シングル	コンテキスト	システム
クラス マップ 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
7.0(1)(1)	このコマンドが導入されました。

例

次の例では、test から test2 にクラス マップ名を変更する方法を示します。

```
hostname(config)# class-map test
hostname(config-cmap)# rename test2
```

関連コマンド

コマンド	説明
class-map	クラス マップを作成します。

replication http

フェールオーバー グループの HTTP 接続の複製をイネーブルにするには、フェールオーバー グループ コンフィギュレーション モードで **replication http** コマンドを使用します。HTTP 接続の複製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。

replication http

no replication http

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

ディセーブルです。

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	透過	シングル	コンテキスト	システム
フェールオーバー グループ 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
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、ステートフル フェールオーバーがイネーブルの場合、セキュリティ アプライアンスは HTTP セッション情報を複製しません。HTTP セッションは通常は存続期間が短く、HTTP クライアントは接続試行が失敗すると通常はリトライするため、HTTP セッションの複製をしないことでシステムのパフォーマンスが向上します。複製をしなくても重要なデータや接続は失われません。**replication http** コマンドは、ステートフル フェールオーバー環境で HTTP セッションのステートフル複製をイネーブルにしますが、システム パフォーマンスには悪影響を与える可能性があります。

このコマンドを使用できるのは、Active/Active フェールオーバーに対してのみです。このコマンドは、Active/Active フェールオーバー コンフィギュレーションのフェールオーバー グループを除く、Active/Standby フェールオーバーに対して **failover replication http** コマンドと同じ機能を提供します。

例

次の例は、フェールオーバー グループに対して適用可能なコンフィギュレーションを示しています。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# replication http
hostname(config-fover-group)# exit
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
failover replication http	HTTP 接続を複製するように、ステートフル フェールオーバーを設定します。

request-command deny

FTP 要求内で特定のコマンドを禁止するには、FTP マップ コンフィギュレーション モードで **request-command deny** コマンドを使用します。このモードには、**ftp-map** コマンドを使用してアクセスできます。コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

request-command deny { **appe** | **cdup** | **dele** | **get** | **help** | **mkd** | **put** | **rmd** | **rnfr** | **rnto** | **site** | **stou** }

no request-command deny { **appe** | **cdup** | **help** | **retr** | **rnfr** | **rnto** | **site** | **stor** | **stou** }

シンタックスの説明

appe	ファイルに対して付加を実行するコマンドを禁止します。
cdup	現在の作業ファイルの親ディレクトリに変更を加えるコマンドを禁止します。
dele	サーバ上のファイルを削除するコマンドを禁止します。
get	サーバからファイルを取得するクライアント コマンドを禁止します。
help	ヘルプ情報を提供するコマンドを禁止します。
mkd	サーバ上にディレクトリを作成するコマンドを禁止します。
put	サーバにファイルを送信するクライアント コマンドを禁止します。
rmd	サーバ上のディレクトリを削除するコマンドを禁止します。
rnfr	元のファイル名からの名前変更を指定するコマンドを禁止します。
rnto	新しいファイル名への名前変更を指定するコマンドを禁止します。
site	サーバ システム固有のコマンドを禁止します。通常は、リモート管理で使用されます。
stou	一意のファイル名を使用しているファイルを保存するコマンドを禁止します。

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	透過	シングル	コンテキスト	システム
FTP マップ 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
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　このコマンドは、厳密な FTP 検査を使用するときに、セキュリティ アプライアンスを通過する FTP 要求内で許可されるコマンドを制御するために使用します。

例　次の例では、**stor** コマンド、**stou** コマンド、または **appe** コマンドが含まれている FTP 要求をドロップするように、セキュリティ アプライアンスを設定します。

```
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# request-command deny put stou appe
hostname(config-ftp-map)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
ftp-map	FTP マップを定義し、FTP マップ コンフィギュレーション モードをイネーブルにします。
inspect ftp	アプリケーション検査用に特定の FTP マップを適用します。
mask-syst-reply	FTP サーバ応答をクライアントから見えないようにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

request-data-size

SLA オペレーション要求パケットのペイロードのサイズを設定するには、SLA モニタ プロトコル コンフィギュレーション モードで **request-data-size** 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。

request-data-size *bytes*

no request-data-size

シンタックスの説明

bytes	要求パケット ペイロードのサイズ（バイト単位）。有効な値は 0 ～ 16384 です。最小値は、使用するプロトコルにより異なります。エコー タイプの場合、最小値は 28 バイトです。この値は、プロトコルまたは PMTU で許可されている最大値より大きい値に設定しないでください。

（注） セキュリティ アプライアンスは、8 バイトのタイムスタンプをペイロードに追加します。このため、実際のペイロードは *bytes* + 8 になります。

デフォルト

デフォルトのバイトは 28 です。

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	透過	シングル	コンテキスト	システム
SLA モニタ プロトコル 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
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

到達可能性については、ソースとターゲット間での PMTU の変化を検出するため、デフォルトのデータ サイズを増やさなければならない場合があります。PMTU が低いとセッションのパフォーマンスに影響を与える傾向があります。低い PMTU が検出された場合、2 番目のパスが使用されることを示している可能性があります。

例

次の例では、ICMP エコー要求 / 応答時間プローブ オペレーションを使用する、ID が 123 の SLA オペレーションを設定しています。エコー要求パケットのペイロード サイズを 48 バイト、SLA オペレーション中に送信されるエコー要求の数を 5 に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# num-packets 5
hostname(config-sla-monitor-echo)# request-data-size 48
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
num-packets	SLA オペレーション中に送信する要求パケットの数を指定します。
sla monitor	SLA 監視オペレーションを定義します。
type echo	SLA オペレーションをエコー応答時間プローブ オペレーションとして設定します。

request-method

HTTP 要求メソッドに基づいて HTTP トラフィックを制限するには、HTTP マップ コンフィギュレーション モードで **request-method** コマンドを使用します。このモードには、**http-map** コマンドを使用してアクセスできます。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。

request-method {{ **ext** *ext_methods* | **default**} | { **rfc** *rfc_methods* | **default**}} **action** {**allow** | **reset** | **drop**} [**log**]

no request-method { **ext** *ext_methods* | **rfc** *rfc_methods* } **action** {**allow** | **reset** | **drop**} [**log**]

シンタックスの説明

action	メッセージがこのコマンド検査に合格しなかったときに実行されるアクションを指定します。
allow	メッセージを許可します。
default	サポートされている要求メソッドがトラフィックに含まれていて、そのメソッドが設定済みリストに記載されていない場合に、セキュリティ アプライアンスが実行するデフォルト アクションを指定します。
drop	接続を終了します。
ext	拡張メソッドを指定します。
ext-methods	セキュリティ アプライアンスを通過することを許可する拡張メソッドの 1 つを指定します。
log	（オプション）syslog を生成します。
reset	TCP リセット メッセージをクライアントまたはサーバに送信します。
rfc	RFC 2616 でサポートされているメソッドを指定します。
rfc-methods	セキュリティ アプライアンスを通過することを許可する RFC メソッドの 1 つを指定します（表 23-2 を参照）。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。このコマンドがイネーブルで、サポートされている要求メソッドが指定されていない場合、デフォルト アクションでは、ロギングなしで接続が許可されます。デフォルト アクションを変更するには、**default** キーワードを使用して別のデフォルト アクションを指定します。

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	透過	シングル	コンテキスト	システム
HTTP マップ 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
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

request-method コマンドをイネーブルにすると、セキュリティ アプライアンスは、サポートおよび設定されている各要求メソッドの HTTP 接続に対して、指定されているアクションを適用します。

セキュリティ アプライアンスは、設定済みリストにある要求メソッドに一致*しない*すべてのトラフィックに対して、**default** アクションを適用します。**default** アクションでは、接続をロギングなしで **allow** します。事前設定済みのデフォルト アクションでは、**drop** および **log** というアクションを持つ 1 つまたは複数の要求メソッドを指定すると、セキュリティ アプライアンスは、設定済み要求メソッドが含まれている接続をドロップし、各接続をロギングし、サポートされているその他の要求メソッドが含まれているすべての接続を許可します。

より厳しいポリシーを設定する場合は、デフォルト アクションを **drop**（または **reset**）および **log** に変更します（イベントをログに記録する場合）。その後、**allow** アクションで、許可する各メソッドを設定します。

適用する設定ごとに 1 回、**request-method** コマンドを入力します。**request-method** コマンドのインスタンスを、デフォルト アクションを変更するために 1 つ、設定済みメソッドのリストに 1 つの要求メソッドを追加するために 1 つ使用します。

このコマンドの **no** 形式を使用して、要求メソッドを設定済みメソッドのリストから削除する場合、コマンドラインで要求メソッド キーワードの後にある文字はすべて無視されます。

RFC 2616 で定義されているメソッドで、設定済みメソッドのリストに追加できるものを表 23-2 に示します。

表 23-2　RFC 2616 メソッド

メソッド	説明
connect	トンネルに動的に切り替わることが可能なプロキシ（例、SSL トンネリング）と共に使用されます。
delete	Request-URI によって識別されたリソースをオリジン サーバが削除することを要求します。
get	Request-URI によって識別された情報またはオブジェクトをすべて取得します。
head	サーバが応答でメッセージ本文を返さないこと以外は、GET と同じです。
options	Request-URI によって識別されたサーバで使用できる、通信オプションについての情報の要求を表します。
post	要求に含まれているオブジェクトを、Request-Line 内の Request-URI によって識別されたリソースの新しい下位リソースとしてオリジン サーバが受け入れることを要求します。
put	含まれているオブジェクトを指定した Request-URI の下に保存することを要求します。
trace	リモートのアプリケーション層の要求メッセージのループバックを起動します。

例

次の例では、事前設定済みのデフォルトを使用して、緩やかなポリシーを指定しています。サポートされているすべての要求メソッドを、個別に拒否されていない限り許可します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# request-method rfc options drop log
hostname(config-http-map)# request-method rfc post drop log
hostname(config-http-map)
```

この例では、**options** 要求メソッドおよび **post** 要求メソッドだけがドロップされ、イベントが記録されます。

次の例では、厳しいポリシーを設定します。デフォルト アクションは、個別に許可されていないすべての要求メソッドの接続を **reset** し、イベントを **log** するように変更されています。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# request-method rfc default action reset log
hostname(config-http-map)# request-method rfc get allow
hostname(config-http-map)# request-method rfc put allow
hostname(config-http-map)#
```

この場合、**get** 要求メソッドおよび **put** 要求メソッドが許可されます。その他のメソッドを使用するトラフィックが検出された場合、セキュリティ アプライアンスは接続をリセットし、syslog エントリを作成します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

request-queue

応答待ちでキュー入れられる GTP 要求の最大数を指定するには、GTP マップ コンフィギュレーション モードで **request-queue** コマンドを使用します。このモードには、**gtp-map** コマンドを使用してアクセスできます。この数をデフォルトの 200 に戻すには、このコマンドの **no** 形式を使用します。

request-queue *max_requests*

no request-queue *max_requests*

シンタックスの説明

max_requests	応答待ちでキューに入れられる GTP 要求の最大数。範囲は、1 ～ 4,294,967,295 です。

デフォルト

max_requests のデフォルトは 200 です。

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	透過	シングル	コンテキスト	システム
GTP マップ 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
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

gtp request-queue コマンドは、応答待ちでキューに入れられる GTP 要求の最大数を指定します。限度に到達していて新しい要求が着信すると、最も長時間キューに入っている要求が削除されます。Error Indication、Version Not Supported、および SGSN Context Acknowledge の各メッセージは要求と見なされないため、応答を待つために要求キューに入れられることはありません。

例

次の例では、要求キューの最大サイズを 300 バイトに指定します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# request-queue-size 300
hostname(config-gtpmap)#
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
debug gtp	GTP 検査に関する詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査に使用する特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

request-timeout

失敗した SSO 認証の試行がタイムアウトになるまでの秒数を設定するには、webvpn-sso-siteminder コンフィギュレーション モードで **request-timeout** コマンドを使用します。これは CA SiteMinder コマンドによる SSO です。

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。

request-timeout *seconds*

no request-timeout

シンタックスの説明

seconds	失敗した SSO 認証試行がタイムアウトになるまでの秒数です。範囲は 1 ～ 30 秒です。端数はサポートされていません。

デフォルト

デフォルトでは、このコマンドの値は 5 秒です。

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	透過	シングル	コンテキスト	システム
webvpn-sso-siteminder 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
7.1.1	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを 1 度入力すると、再入力しなくてもさまざまなサーバで各種のセキュアなサービスにアクセスできます。現在、セキュリティ アプライアンスは、Computer Associates の eTrust SiteMinder SSO サーバ（以前の Netegrity SiteMinder）をサポートしています。

セキュリティ アプライアンスが SSO 認証をサポートするように設定したら、次の 2 つのタイムアウト パラメータをオプションで調整できます。

- 失敗した SSO 認証試行がタイムアウトになるまでの秒数。これには **request-timeout** コマンドを使用します。
- セキュリティ アプライアンスが失敗した SSO 認証を再試行する回数（**max-retry-attempts** コマンドを参照）。

例

webvpn-sso-siteminder コンフィギュレーション モードで入力された次の例では、SiteMinder SSO サーバ「example」の認証タイムアウトを 10 秒に設定しています。

```
hostname(config-webvpn)# sso-server example type siteminder
hostname(config-webvpn-sso-siteminder)# request-timeout 10
hostname(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
max-retry-attempts	失敗した SSO 認証に対して、セキュリティ アプライアンスが認証を再試行する回数を設定します。
policy-server-secret	SSO サーバへの認証要求の暗号化に使用する秘密鍵を作成します。
show webvpn sso-server	SSO サーバの動作統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
test sso-server	テスト認証要求で SSO サーバをテストします。
web-agent-url	セキュリティ アプライアンスが SSO 認証を要求する SSO サーバの URL を指定します。

reserved-bits

TCP ヘッダーの予約済みビットを消去するには、または、予約済みビットが設定されたパケットをドロップするには、tcp マップ コンフィギュレーション モードで **reserved-bits** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

reserved-bits {**allow** | **clear** | **drop**}

no reserved-bits {**allow** | **clear** | **drop**}

シンタックスの説明

allow	TCP ヘッダー内に予約済みビットを持つパケットを許可します。
clear	TCP ヘッダー内の予約済みビットを消去してから、そのパケットを許可します。
drop	TCP ヘッダー内に予約済みビットを持つパケットをドロップします。

デフォルト

デフォルトでは、予約済みビットが許可されています。

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	透過	シングル	コンテキスト	システム
tcp マップ 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
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。予約済みビットのあるパケットがエンド ホストで処理される方法についてのあいまいさを排除するには、tcp マップ コンフィギュレーション モードで **reserved-bits** コマンドを使用します。あいまいさがあると、セキュリティ アプライアンスの非同期につながる場合があります。TCP ヘッダー内の予約済みビットを消去することを選択できます。さらには、予約済みビットが設定されたパケットをドロップすることも選択できます。

例

次の例は、予約済みビットが設定されたすべての TCP フローのパケットを消去する方法を示します。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# reserved-bits clear
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。

reset

モジュラ ポリシー フレームワークを使用する場合、パケットをドロップして接続を終了し、一致またはクラス コンフィギュレーション モードで **reset** コマンドを使用して、**match** コマンドまたはクラス マップと一致するトラフィックに対して TCP のリセットを送信します。このリセット アクションは、アプリケーション トラフィックの検査ポリシー マップ（**policy-map type inspect** コマンド）で有効です。このアク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。

reset [**log**]

no reset [**log**]

シンタックスの説明

log	一致をログに記録します。システム ログ メッセージの番号は、アプリケーションによって異なります。

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	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス 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
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

検査ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。検査ポリシー マップで使用できるコマンド自体は、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを特定した後（**class** コマンドは、**match** コマンドを含む、既存の **class-map type inspect** コマンドを参照します）、**reset** コマンドを入力してパケットをドロップし、**match** コマンドまたは **class** コマンドと一致するトラフィックの接続を終了します。

接続をリセットすると、検査ポリシー マップのそれ以降のアクションは実行されません。たとえば、最初のアクションが接続のリセットである場合、それ以降の **match** コマンドまたは **class** コマンドとは一致しません。最初のアクションがパケットのロギングである場合は、接続のリセットなどの 2 番目のアクションが発生する可能性があります。同じ **match** または **class** コマンドに対して、**reset** と **log** アクションを両方を設定できます。その場合、パケットは、指定の一致によってリセットされるまでロギングされます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション検査をイネーブルにするときは、このアクションを含んでいる検査ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は検査ポリシー マップの名前です。

例

次の例では、接続をリセットして、http-traffic クラス マップと一致するとログを送信します。同じパケットが 2 番目の **match** コマンドにも一致する場合、そのパケットはすでにドロップされているため、処理されません。

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# reset log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス 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検査クラス 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。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

retries

セキュリティ アプライアンスが応答を受信しないときに、一連の DNS サーバへのアクセスを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*]

シンタックスの説明

number	再試行の回数を 0 ～ 10 の間で指定します。デフォルトは 2 です。

デフォルト

デフォルトでは、再試行の回数は 2 です。

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	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

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 コマンドは、このコマンドに置き換えられます。

例

次の例では、再試行の回数を 0 に設定します。セキュリティ アプライアンスは各サーバを 1 回だけ試します。

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

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 モードに入ります。
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を 1 つまたはすべて表示します。

retry-interval

aaa-server host コマンドで以前に指定した特定の AAA サーバに対するリトライ間隔（時間の長さ）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。このリトライ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

シンタックスの説明

seconds	要求をリトライする間隔を指定します（1 ～ 10 秒）。セキュリティ アプライアンスが接続要求をリトライするまでに待つ時間です。

デフォルト

デフォルトのリトライ間隔は 10 秒です。

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	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

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

使用上のガイドライン

セキュリティ アプライアンスが接続試行を実行する間隔（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。**timeout** コマンドを使用して、セキュリティ アプライアンスが AAA サーバへの接続を試みる時間の長さを指定します。

例

次の例は、コンテキスト内の **retry-interval** コマンドを示しています。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 7
hostname(config-aaa-server-host)# retry-interval 9
hostname(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 モードに入って、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 コマンド文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	セキュリティ アプライアンスが AAA サーバへの接続確立の試行を継続する時間の長さを指定します。

revocation-check

失効チェックの方法を 1 つまたは複数設定するには、暗号 CA トラストポイント モードで **revocation-check** コマンドを使用します。セキュリティ アプライアンスは設定された順番でその方法を試行します。2 番目、3 番目の方法は、ステータスが失効として検出された場合とは反対に、直前の方法がエラー（サーバ ダウンなど）になった場合にのみ実行されます。

失効チェックの方法は、トラストポイントを検証するクライアント証明書に設定できます。また、トラストポイントを検証する応答側証明書に失効チェックなし（**revocation-check none**）を設定することもできます。**match certificate** コマンドのマニュアルには、手順に沿って示したコンフィギュレーション例が含まれています。

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**] [**none**] [**ocsp**]}

no revocation-check

シンタックスの説明

crl	セキュリティ アプライアンスで失効チェック方法として CRL を使用することを指定します。
none	セキュリティ アプライアンスはすべての方法でエラーが返されても、証明書の状況を有効であると解釈することを指定します。
ocsp	セキュリティ アプライアンスで OCSP を失効チェック方法として使用す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	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。次のように各コマンドが置き換えられました。 • **crl optional** は、**revocation-check crl none** に置き換えられました。 • **crl required** は、**revocation-check crl** に置き換えられました。 • **crl nocheck** は、**revocation-check none** に置き換えられました。

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。この応答の受信後、デバイスはレスポンダ証明書を確認します。

通常、CA は OCSP レスポンダ証明書の寿命を比較的短期間に設定して、セキュリティが脅かされる機会を最小限に抑えます。CA では、レスポンダ証明書内に失効状況を確認する必要がないことを示す ocsp-no-check 拡張機能を含みます。ただし、この拡張機能が含まれていない場合、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する失効方法を使用して証明書の失効状況を確認しようとします。状況チェックを無視する *none* オプションも設定しないと OCSP 失効チェックは失敗するので、OCSP レスポンダ証明書は、ocsp-no-check 拡張機能が含まれていない場合に検証可能である必要があります。

例

次に例では、newtrust というトラストポイントに対して、OCSP と CRL の失効方法をこの順番で設定する方法を示します。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# revocation-check ocsp crl
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	暗号 CA トラストポイント モードに入ります。このコマンドは、グローバル コンフィギュレーション モードで使用します。
match certificate	OCSP 上書き規則を設定します。
ocsp disable-nonce	OCSP 要求のナンス拡張をディセーブルにします。
ocsp url	トラストポイントに関連付けられているすべての証明書をチェックするための OCSP サーバを指定します。

rewrite

特定のアプリケーションまたは WebVPN 接続のトラフィックのタイプのコンテンツ 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。リライト規則を削除するには、このコマンドの **no** 形式を、規則を一意に識別する規則番号を付けて使用します。リライト規則をすべて削除するには、コマンドの **no** 形式を、規則番号を付けずに使用します。

デフォルトでは、セキュリティ アプライアンスはすべての WebVPN トラフィックのリライトまたは変換を行います。

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

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

シンタックスの説明

disable	リライト規則を、指定されたトラフィックに対するコンテンツ リライトをディセーブルにする規則として定義します。コンテンツ 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。
enable	リライト規則を、指定されたトラフィックに対するコンテンツ リライトをイネーブルにする規則として定義します。
integer	設定済みのすべての規則の順序を設定します。範囲は 1 ～ 65534 です。
name	（オプション）規則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	セキュリティ アプライアンスが規則を適用する順序を定義します。
resource-mask	規則のアプリケーションまたはリソースを指定します。
resource name	（オプション）規則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	正規表現を含むことができるアプリケーションまたはリソースと一致するよう、アプリケーションまたはリソースの名前を指定します。次のワイルドカードを使用できます。 正規表現を含むことができるパターンと一致するよう、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。 * ：すべてと一致します。このワイルドカードはこれだけでは使用できません。英数字の文字列と共に使用する必要があります。 ? ：任意の 1 文字と一致します。 [!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、すべてリライトします。

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	透過	シングル	コンテキスト	システム
WebVPN モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン　セキュリティ アプライアンスは、WebVPN 接続上でアプリケーションが正しく動作するよう、アプリケーションのコンテンツ リライトを行います。外部の公的 Web サイトなど、コンテンツ リライトが不要なアプリケーションもあります。このようなアプリケーションには、コンテンツ リライトをオフにすることもできます。

コンテンツ リライトを選択的にオフにするには、disable オプションで rewrite コマンドを使用し、ユーザがセキュリティ アプライアンスを介さずに直接特定のサイトを閲覧できるようにします。これは、IPSec VPN 接続のスプリット トンネリングと類似しています。

このコマンドは複数回使用できます。セキュリティ アプライアンスはリライト規則を順番に検索し、一致した最初の規則を適用するため、エントリを設定する順序は重要です。

例　次の例は、cisco.com ドメインの URL のコンテンツ リライトをオフにする、1 番目のリライト規則を設定する方法を示しています。

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

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規則を指定します。
proxy-bypass	特定のアプリケーションの最小限のコンテンツ リライトを設定します。

re-xauth

ユーザが IKE キー再生成で再認証を受けることを必須とするには、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** コマンドを使用します。IKE キー再生成でのユーザ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。

re-xauth アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。これにより、IKE キー再生成での再認証の値を別のグループ ポリシーから継承できるようになります。

re-xauth {**enable** | **disable**}

no re-xauth

シンタックスの説明

disable	IKE キー再生成での再認証をディセーブルにします。
enable	IKE キー再生成での再認証をイネーブルにします。

デフォルト

IKE キー再生成での再認証は、ディセーブルになっています。

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	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IKE キー再生成での再認証をイネーブルにすると、セキュリティ アプライアンスは、フェーズ 1 IKE ネゴシエーション中にユーザ名とパスワードの入力を求めるプロンプトを表示します。また、IKE キー再生成が実行されるたびに、ユーザ認証を求めるプロンプトを表示します。再認証により、セキュリティが向上します。

設定されているキー再生成間隔が極端に短い場合、ユーザは認証を繰り返し求められることに不便を感じることがあります。その場合は、再認証をディセーブルにしてください。設定されているキー再生成間隔を確認するには、モニタリング モードで **show crypto ipsec sa** コマンドを発行して、セキュリティ結合のライフタイムの秒単位データおよび KB 単位データを表示します。

（注） 接続相手側にユーザが存在しない場合、再認証は失敗します。

例

次の例は、FirstGroup というグループ ポリシーのキー再生成での再認証をイネーブルにする方法を示しています。

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

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、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 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 *key* ***key_id*** *key_id*

no rip authentication key

シンタックスの説明

key	RIP アップデートを認証するキー。このキーの最大長は 16 文字です。
key_id	キー ID 値：有効な値は 1 ～ 255 です。

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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

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することで、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、*key* 引数と *key_id* 引数は、RIP バージョン 2 アップデートを提供するネイバー デバイスによって使用される引数と同じでなければなりません。*key* は、最大 16 文字のテキスト文字列です。

特定のインターフェイスについて **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

次の例では、インターフェイス GigabitEthernet0/3 に対して設定されている RIP 認証を表示しています。

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# rip authentication mode md5
hostname(config-if)# rip authentication key thisismykey key_id 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タイプを指定します。
rip receive version	指定した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	セキュリティ アプライアンス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 mode

RIP バージョン 2 パケットで使用される認証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

シンタックスの説明

md5	RIP メッセージ認証には MD5 を使用します。
text	RIP メッセージ認証にはクリア テキストを使用します（推奨しません）。

デフォルト

クリア テキスト認証はデフォルトでは使用されません。

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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

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することで、RIP アップデートを認証できます。

特定のインターフェイスについて **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

次の例では、インターフェイス GigabitEthernet0/3 に対して設定されている RIP 認証を表示しています。

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# rip authentication mode md5
hostname(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	指定した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	セキュリティ アプライアンス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。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

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

no version

シンタックスの説明

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

セキュリティ アプライアンスは、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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

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、インターフェイスに対して **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することで、RIP アップデートを認証できます。

例

次の例では、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セキュリティ アプライアンスを設定しています。

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(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、そのプロセスのルータ コンフィギュレーション モードに入ります。
version	セキュリティ アプライアンス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。デフォルトに戻すには、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

シンタックスの説明

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

セキュリティ アプライアンスは 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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

RIP 送信バージョンの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、インターフェイスに対して **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することで、RIP アップデートを認証できます。

例

次の例では、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セキュリティ アプライアンスを設定しています。

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

関連コマンド

コマンド	説明
rip receive version	指定した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 モードに入ります。
version	セキュリティ アプライアンス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**] [**flash:**]*path*

シンタックスの説明

noconfirm	（オプション）確認プロンプトを表示しないようにします。
flash:	（オプション）取り外しできない内蔵フラッシュを指定し、続けてコロン（:）を入力します。
path	（オプション）削除するディレクトリの絶対パスまたは相対パス。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

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

次の例は、「test」という名前の既存のディレクトリを削除する方法を示しています。

```
hostname# 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のスタティック 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。指定し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***]

シンタックスの説明

gateway_ip	ゲートウェイ ルータの IP アドレスを指定します（このルートのネクストホップ アドレス）。 （注）　*gateway_ip* 引数は、透過モードでのオプションです。
interface_name	内部または外部のネットワーク インターフェイスの名前。
ip_address	内部または外部のネットワーク IP アドレス。
metric	（オプション）このルートの管理ディスタンス。有効な値は、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*	（オプション）トラッキング エントリとこのルートを関連付けます。有効な値は 1 ～ 500 です。 （注）　***track*** オプションは、単独のルーテッド モードでのみ有効です。
tunneled	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、ルートを指定します。

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	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.2(1)	***track*** *number* 値が追加されました。

使用上のガイドライン

インターフェイスのデフォルト 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* と *netmask* を **0.0.0.0** に設定するか、短縮形の **0** を使用します。**route** コマンドを使用して入力したすべてのルートは、保存時にコンフィギュレーションに格納されます。

標準のデフォルト ルートに加えて、トンネル トラフィック用の別のデフォルト ルートを定義できます。***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、セキュリティ アプライアンスに到達する暗号化されたトラフィックで、ラーニングされたルートまたはスタティック ルートのいずれでもルーティングできないトラフィックは、すべてこのルートに送信されます。トラフィックが暗号化されていない場合、標準のデフォルト ルート エントリが使用されます。***tunneled*** オプションで複数のデフォルト ルートを定義することはできません。トンネル トラフィックの ECMP はサポートされていません。

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には、スタティック ルートを作成します。たとえば、セキュリティ アプライアンスはこのスタティック **route** コマンドを使用し、192.168.42.0 ネットワークに向けて 192.168.1.5 ルータ経由ですべてのパケットを送信します。

```
hostname(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、セキュリティ アプライアンスは、ルート テーブルに CONNECT ルートを作成します。このエントリは、**clear route** コマンドまたは **clear configure route** コマンドを使用しても削除できません。

route コマンドがセキュリティ アプライアンスのインターフェイスいずれか 1 つの IP アドレスをゲートウェイ IP アドレスとして使用する場合、セキュリティ アプライアンスはゲートウェイ IP アドレスに対して ARP を実行するのではなく、パケット内の宛先 IP アドレスに対して ARP を実行します。

例

次の例は、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方法を示しています。

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

次の例は、次のスタティック **route** コマンドを追加して、ネットワークへのアクセスを提供する方法を示しています。

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

次の例は、デフォルト ルートを外部インターフェイスの 10.1.1.1 ゲートウェイにインストールするために SLA オペレーションを使用します。SLA オペレーションはゲートウェイの可用性を監視します。SLA 操作が失敗すると、dmz インターフェイスでバックアップ ルートが使用されます。

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

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ラーニング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

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ための条件を定義するには、グローバル コンフィギュレーション モードで **route-map** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

route-map *map_tag* [**permit** | **deny**] [*seq_num*]

no route-map *map_tag* [**permit** | **deny**] [*seq_num*]

シンタックスの説明

deny	（オプション）このルートマップが一致基準に適合した場合は、このルートを再配布しないことを指定します。
map_tag	ルートマップ タグのテキスト。テキストの長さは最大 57 文字です。
permit	（オプション）このルートマップが一致基準に適合した場合は、このルートを、設定アクションによる制御に従って再配布することを指定します。
seq_num	（オプション）ルートマップのシーケンス番号。有効な値は 0 ～ 65535 です。すでに同じ名前で設定されているルートマップのリストにおける新しいルートマップの位置を示します。

デフォルト

デフォルトは次のとおりです。

- **permit**
- *seq_num* を指定しない場合、*seq_num* の値 10 が最初のルートマップに割り当てられます。

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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

route-map コマンドを使用すると、ルートを再配布できます。

route-map グローバル コンフィギュレーション コマンド、**match** コンフィギュレーション コマンド、および **set** コンフィギュレーション コマンドは、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ための条件を定義します。各 **route-map** コマンドには、**match** コマンドと **set** コマンドが関連付けられます。**match** コマンドは、一致基準、つまり現在の **route-map** コマンドについて再配布を許可する条件を指定します。**set** コマンドには、設定アクション、つまり **match** コマンドで指定した基準を満たしている場合に実行する再配布アクションを指定します。**no route-map** コマンドを実行すると、ルートマップが削除されます。

match route-map 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** コマンドは任意の順序で入力できます。また、**set** コマンドで指定した設定アクションに従ってルートの再配布を実行するには、すべての **match** コマンドに一致する必要があります。**match** コマンドを **no** 形式で実行すると、指定した一致基準が削除されます。

ルーティング プロセス間のルート再配布方法を細かく制御するには、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 ospf** グローバル コンフィギュレーション コマンドで指定します。送信元ルーティング プロトコルは、**redistribute** ルータ コンフィギュレーション コマンドで指定します。

ルートマップを通じてルートを渡すとき、ルートマップはいくつかの部分に分かれることがあります。**route-map** コマンドと関連する 1 つ以上の match 節と一致しないルートは、無視されます。そのルートが、発信ルートマップのためにアドバタイズされるか、着信ルートマップのために受け入れられることはありません。一部のデータのみを修正するには、正確に一致する基準を指定した 2 番目のルートマップ セクションを設定する必要があります。

seq_number 引数については、次のとおりです。

1. 提供されたタグでエントリを定義しない場合、*seq_number* 引数に 10 が設定されたエントリが作成されます。
2. 提供されたタグで 1 つだけエントリを定義した場合、そのエントリは、その後に続く **route-map** コマンドのデフォルト エントリとなります。このエントリの *seq_number* 引数は変更されません。
3. 提供されたタグで 2 つ以上のエントリを定義した場合、*seq_number* 引数が必要であることを示すエラー メッセージが出力されます。

no route-map *map-tag* コマンドを（*seq-num* 引数なしで）指定した場合、ルートマップ全体（同じ *map-tag* テキストを持つすべての **route-map** エントリ）が削除されます。

一致基準に適合しない場合に **permit** キーワードを指定してあれば、同じ *map_tag* を持つ次のルートマップがテストされます。ルートは、同じ名前を共有するルートマップ セットの一致基準に 1 つも一致しなかった場合、そのセットによって再配布されません。

例

次の例は、OSPF ルーティングで使用するルートマップを設定する方法を示しています。

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# show running-config route-map
route-map maptag1 permit 8
    set metric 5
    match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure route-map	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ための条件を削除します。
match interface	指定したいずれかのインターフェイスの外部にネクストホップを持つ、すべてのルートを再配布します。
router ospf	OSPF ルーティング プロセスを開始および設定します。
set metric	ルートマップの宛先ルーティング プロトコルのメトリック値を指定します。
show running-config route-map	ルートマップ コンフィギュレーションに関する情報を表示します。

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 モードで **router-id** コマンドを使用します。先行の OSPF 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 *addr*

no router-id [*addr*]

シンタックスの説明

addr	IP アドレス形式のルータ ID。

デフォルト

指定しない場合、セキュリティ アプライアンス上で最上位の 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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

セキュリティ アプライアンス上で最上位の IP アドレスがプライベート アドレスの場合、このアドレスは hello パケットおよびデータベース定義で送信されます。この状況を回避するには、**router-id** コマンドを使用してルータ ID のグローバル アドレスを指定します。

例

次の例では、ルータ ID を 192.168.1.1 に設定します。

```
hostname(config-router)# router-id 192.168.1.1
hostname(config-router)#
```

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 モードに入ります。
show ospf	OSPF 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 ospf

OSPF ルーティング プロセスを開始し、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*

シンタックスの説明

pid	OSPF ルーティング プロセス用に内部的に使用される識別パラメータ。有効な値は、1 ～ 65535 です。*pid* は、他のルータ上の 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になっています。

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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

router ospf コマンドは、セキュリティ アプライアンス上で実行している 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、コマンド プロンプトは (config-router)# と表示されます。これは、ルータ コンフィギュレーション モードに入ったことを示しています。

no router ospf コマンドを使用する場合、必要な情報を提供するものでない限り、オプションの引数を使用する必要はありません。**no router ospf** コマンドは、*pid* で指定された OSPF ルーティング プロセスを終了します。*pid* をセキュリティ アプライアンス上でローカルに割り当てることができます。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、OSPF 固有の次のコマンドと共に使用され、OSPF ルーティング プロセスを設定します。

- **area**：通常の OSPF エリアを設定します。
- **compatible rfc1583**：RFC 1583 準拠のサマリー ルート コストの計算に使用される方式に戻します。
- **default-information originate**：OSPF ルーティング ドメイン内へのデフォルトの外部ルートを生成します。
- **distance**：ルート タイプに基づいて、OSPF ルートの管理ディスタンスを定義します。
- **ignore**：タイプ 6 Multicast OSPF（MOSPF）パケットの link-state advertisement（LSA; リンクステート アドバタイズメント）を受信した際に、syslog メッセージを送信しないようにします。

- **log-adj-changes**：OSPF 隣接ルータがアップ状態またはダウン状態になると syslog メッセージを送信するように、ルータを設定します。
- **neighbor**：隣接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可能にするために使用されます。
- **network**：OSPF を実行す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基づく、あるルーティング ドメインから別のルーティング ドメインへ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。
- **timers lsa-group-pacing**：OSPF LSA グループ間隔タイマー（リフレッシュまたは最大限にエージングされている LSA グループの間隔）。
- **timers spf**：SPF 計算に対する変更を受信する間隔。

セキュリティ アプライアンスで RIP が設定されている場合は、OSPF を設定できません。

例

次の例は、5 番の OSPF ルーティング プロセスのコンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# router ospf 5
hostname(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 コマンドを消去します。
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、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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

RIP ルーティングはディセーブルになっています。

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	透過	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

router rip コマンドは、セキュリティ アプライアンス上で実行している RIP 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。セキュリティ アプライアンスで RIP プロセスを 1 つだけ設定できます。**no router rip** コマンドは RIP ルーティング プロセスを停止し、その処理のためのすべてのルータ 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 プロンプトは `hostname(config-router)#` に変更されます。これは、ルータ コンフィギュレーション モードに入ったことを示しています。

router rip コマンドは、次のルータ コンフィギュレーション コマンドと共に使用され、RIP ルーティング プロセスを設定します。

- **auto-summary**：ルートの自動集約をイネーブル / 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**：着信するルーティング アップデートのネットワークをフィルタリングします。
- **distribute-list out**：送信するルーティング アップデート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 プロセスからインターフェイスを追加 / 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 プロセスからのルートを RIP ルーティング プロセスに再配布します。
- **version**：セキュリティ アプライアンスで使用される RIP プロトコル バージョンを設定します。

さらに、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、RIP プロパティをインターフェイスごとに設定できます。

- **rip authentication key**：認証キーを設定します。
- **rip authentication mode**：RIP バージョン 2 で使用される認証タイプを設定します。
- **rip send version**：インターフェイス外に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**：インターフェイスによって受け入れられる 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。

RIP は、透過モードではサポートされません。デフォルトで、セキュリティ アプライアンスはすべての RIP ブロードキャス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 メッセージが透過モードで動作するセキュリティ アプライアンスを通過することを許可するには、このトラフィックを許可するようアクセス リストの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 トラフィックのセキュリティ アプライアンス通過を許可するには、`access-list myriplist extended permit ip any host 224.0.0.9` などのアクセス リスト エントリを作成します。RIP バージョン 1 ブロードキャストを許可するには、`access-list myriplist extended permit udp any any eq rip` などのアクセス リスト エントリを作成します。アクセス リスト エントリをインターフェイスに適用するには、**access-group** コマンドを使用します。

RIP と OSPF ルーティングをセキュリティ アプライアンスで同時にイネーブルにできます。

例

次の例は、5 番の OSPF ルーティング プロセスのコンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# 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 コマンドを消去します。
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

ピンホールを流れる RIP パケットの H.323 および SIP におけるプロトコル適合性を確認するには、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]

シンタックスの説明

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 / ビデオに分類します。

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	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例は、ピンホールを流れる RIP パケットの H.323 コールにおけるプロトコル適合性を確認する方法を示しています。

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

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス 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検査クラス マップを作成します。
debug rtp	H.323 および SIP 検査に関連付けられた 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。
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	現在のすべてのポリシー マップ コンフィギュレーションを表示します。