q - res

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 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。

（注） このコマンドは、ASA 5580 の 10 ギガビット イーサネットインターフェイスではサポートされていません（10 ギガビット イーサネットインターフェイスは、ASA 5585-X でプライオリティ キュー用にサポートされています）。また、このコマンドは、ASA 5512-X ～ ASA 5555-X の管理インターフェイスではサポートされていません。このコマンドは、ASA サービスモジュールではサポートされていません。

queue-limit *number-of-packets*
no queue-limit *number-of-packets*

構文の説明

number-of-packets キューイング（バッファリング）可能な低遅延または通常のプライオリティのパケットの最大数を指定します。この最大数を超えると、インターフェイスでパケットのドロップが開始されます。値の範囲の上限は、実行時にダイナミックに決定されます。この制限を表示するには、コマンドラインで **help** または **?** を入力します。主な決定要素は、キューをサポートするために必要なメモリと、デバイス上で使用可能なメモリです。キューは、使用可能なメモリを超えることはできません。理論的な最大パケット数は、2147483647 です。

コマンド デフォルト

デフォルトのキューの制限は 1024 パケットです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
プライオリティ キュー 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

ASAでは、遅延の影響を受けやすい、プライオリティの高いトラフィック（音声およびビデオなど）用の低遅延キューイング（LLQ）と、それ以外のトラフィック用のベストエフォート（デフォルト）という2つのトラフィッククラスを使用できます。ASAは、プライオリティトラフィックを認識して、適切なQuality of Service（QoS）ポリシーを適用します。プライオリティ キューのサイズと深さを設定して、トラフィック フローを微調整できます。

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

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 コマンドで、プライオリティ キュー コンフィギュレーション モードを開始します。これ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）、およびパケットをドロップする前にバッファに入れることができるタイプ（プライオリティまたはベストエフォート）のパケット数（**queue-limit** コマンド）を設定できます。

指定する tx-ring-limit および queue-limit は、プライオリティ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方のタイプのパケットの数です。このパケット数を超えると、ドライバはインターフェイスの先頭にある複数のキューにパケットを戻し、輻輳が解消するまでそのキューでパケットをバッファしておきます。通常、これらの2つのパラメータを調整することで、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。

例

次に、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、キュー制限を 234 パケット、送信キュー制限を 3 パケットに指定する例を示します。

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 234
ciscoasa(priority-queue)# tx-ring-limit 3
```

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。

コマンド	説明
show priority-queue statistics	指定され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、このコマンドは現在のすべてのプライオリティキュー、queue-limit、および tx-ring-limit コンフィギュレーションの値を表示します。
tx-ring-limit	イーサネット送信ドライバのキューに任意のタイミングで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接続において、順序が不正なパケットのバッファリング可能最大数を設定し、正しい順序に整列するには、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。値を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。このコマンドは、**set connection advanced-options** コマンドを使用してイネーブルにされる TCP 正規化ポリシーの一部です。

queue-limit *pkt_num* **timeout** *seconds*
no queue-limit

構文の説明

pkt_num	TCP接続において、正しい順序に整列し直すことができる、順序が不正なパケットのバッファリング可能最大数を 1 ～ 250 の範囲で指定します。デフォルトは 0 です。この値は、この設定がディセーブルであり、トラフィックのタイプに応じてデフォルトのシステム キュー制限が使用されることを意味しています。詳細については、「使用上のガイドライン」を参照してください。
timeout *seconds*	（任意）順序が不正なパケットをバッファ内に保持可能な最大時間を 1 ～ 20 秒の範囲で設定します。デフォルトは 4 秒です。パケットの順序が不正であり、このタイムアウト期間内に渡されなかった場合、それらのパケットはドロップされます。 *pkt_num* 引数を 0 に設定した場合は、どのトラフィックのタイムアウトも変更できません。**timeout** キーワードを有効にするには、 limit を 1 以上に設定する必要があります。

コマンド デフォルト

デフォルト設定は0です。この値は、このコマンドがディセーブルであることを意味しています。

デフォルトのタイムアウトは 4 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 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(4)/8.0(4)	**timeout** キーワードが追加されました。

使用上のガイドライン

TCP 正規化をイネーブルにするには、モジュラ ポリシー フレームワークを次のように使用します。

1.tcp-map：TCP 正規化アクションを指定します。

- **a.queue-limit**：tcp マップ コンフィギュレーション モードでは、 **queue-limit** コマンドおよびその他数多くのコマンドを入力できます。

2.class-map：TCP 正規化を実行するトラフィックを指定します。

3.policy-map：各クラスマップに関連付けるアクションを指定します。

- **a.class**：アクションを実行するクラスマップを指定します。
- **b.set connection advanced-options**：作成した TCP マップを指定します。

4.service-policy：ポリシーマップをインターフェイスごとに、またはグローバルに割り当てます。

TCP 正規化を有効にしない場合、または **queue-limit** コマンドがデフォルトの 0 に設定されている場合（つまりコマンドが無効の場合）、トラフィックのタイプに応じてデフォルトのシステムキュー制限が使用されます。

- アプリケーション インスペクション（**inspect** コマンド）、IPS（**ips** コマンド）、および TCP チェック再送信（TCP map **check-retransmission** コマンド）のための接続のキュー制限は 3 パケットです。ASA が異なるウィンドウ サイズの TCP パケットを受信した場合は、アドバタイズされた設定と一致するようにキュー制限がダイナミックに変更されます。
- 他の TCP 接続の場合は、異常なパケットはそのまま通過します。

queue-limit コマンドを 1 以上に設定した場合、すべての TCP トラフィックに対して許可される異常なパケットの数は、この設定と一致します。たとえば、アプリケーション インスペクション、IPS、および TCP チェック再送信トラフィックの場合、**queue-limit** 設定が優先され、TCP パケットからアドバタイズされたすべての設定が無視されます。その他の TCP トラフィックについては、異常なパケットはバッファに格納されて、そのまま通過するのではなく、正しい順序に設定されます。

例

次に、すべての Telnet 接続のキュー制限を 8 パケットに、バッファ タイムアウトを 6 秒に設定する例を示します。

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# queue-limit 8 timeout 6
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq telnet
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

関連コマンド

コマンド	説明
class-map	サービス ポリシーに対してトラフィックを指定します。
policy-map	サービス ポリシーのトラフィックに適用するアクションを指定します。
set connection advanced-options	TCP 正規化をイネーブルにします。
service-policy	サービス ポリシーをインターフェイスに適用します。
show running-config tcp-map	TCP マップ コンフィギュレーションを表示します。
tcp-map	TCP マップを作成して、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。

quick-start

IP オプションインスペクションが設定されたパケットヘッダーでクイックスタート（QS）オプションが発生したときに実行する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 **quick-start** 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。

quick-start action { **allow** | **clear** }
no quick-start action { **allow** | **clear** }

構文の説明

allow	クイックスタート IP オプションを含むパケットを許可します。
clear	クイックスタート 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。

コマンド デフォルト

デフォルトでは、IP オプション インスペクションは、クイックスタート IP オプションを含むパケットをドロップします。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
9.5(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、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、特定の IP オプションを持つどの IP パケットが 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。

例

次に、IP オプション インスペクションのアクションをポリシーマップで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)# quick-start 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。

quit

現在のコンフィギュレーションモードを終了するか、特権EXECモードまたはユーザー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

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルト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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ユーザーEXEC	• 対応	• 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

また、キーシーケンス **Ctrl Z** を使用して、グローバル コンフィギュレーション（および上位の）モードを終了できます。このキー シーケンスは、特権EXECモードまたはユーザーEXECモードでは動作しません。

特権 EXEC モードまたはユーザー EXEC モードで **quit** コマンドを入力すると、ASA からログアウトします。特権 EXEC モードからユーザー EXEC モードに戻るには、**disable** コマンドを使用します。

例

次に、**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例を示します。

```
ciscoasa(config)# quit
ciscoasa# quit
Logoff
```

次に、**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 モードを終了する例を示します。

```
ciscoasa(config)# quit
```

```
ciscoasa# disable
ciscoasa>
```

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するか、または特権EXECモードやユーザーEXEC モードからログアウトします。

quota management-session

ASA で許可する集約管理セッション、ユーザーごとの管理セッション、およびプロトコルごとの管理セッションの最大数を設定するには、グローバル コンフィギュレーション モードで **quota management-session** コマンドを使用します。クォータをデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

quota management-session [**ssh** | **telnet** | **http** | **user**] *number*
no quota management-session [**ssh** | **telnet** | **http** | **user**] *number*

構文の説明

number	実行を許可する ASDM、SSH、および Telnet の最大同時セッション数を指定します。（9.12 以降）その他のキーワードを指定せずに入力すると、この引数では 1 ～ 15 のセッションの集約数が設定されます。デフォルトは 15 です。（9.10 以前）有効な値は 0（無制限）～ 10,000 です。
ssh	1 ～ 5 の SSH セッションの最大数を設定します。デフォルトは 5 分です。
telnet	1 ～ 5 の Telnet セッションの最大数を設定します。デフォルトは 5 分です。
http	1 ～ 5 の HTTPS（ASDM）セッションの最大数を設定します。デフォルトは 5 分です。
user	1 ～ 5 のユーザーごとのセッションの最大数を設定します。デフォルトは 5 分です。

コマンド デフォルト

（9.12 以降）集約のデフォルト値は 15 です。

SSH、Telnet、HTTP、およびユーザーのデフォルト値は 5 です。

（9.10 以前）デフォルト値は 0 で、セッション数の制限はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
9.1(2)	このコマンドが追加されました。

リリース	変更内容
9.12(1)	システムではなく、コンテキスト内でこのコマンドを入力できるようになりました。また、集約制限に加えて、ユーザーとプロトコルごとの制限を設定できるようになりました。集約セッションの最大数が15になりました。0（無制限）または16以上に設定してアップグレードすると、値は15に変更されます。

使用上のガイドライン

割り当て量に達すると、それ以降の管理セッション要求は拒否され、syslogメッセージが生成されます。デバイスのロックアウトを回避するため、管理セッション割り当て量のメカニズムではコンソール セッションはブロックされません。

（注） マルチコンテキストモードではASDMセッションの数を設定することはできず、最大セッション数は5で固定されています。

（注） また、**limit-resource** コマンドを使用して最大管理セッション（SSHなど）のコンテキストあたりのリソース制限を設定した場合は、小さい方の値が使用されます。

例

次の例では、集約管理セッション クォータを8に設定し、個々のセッション制限をさまざまな数量に設定しています。

```
ciscoasa
(config)#
quota management-session 8
ciscoasa(config)# quota management-session ssh 3
ciscoasa(config)# quota management-session telnet 1
ciscoasa(config)# quota management-session http 4
ciscoasa(config)# quota management-session user 2
```

関連コマンド

コマンド	説明
show run quota management-session	管理セッション割り当て量の現在の値を表示します。
show quota management-session	管理セッションの統計情報を表示します。

radius-common-pw

ASA経由でRADIUS認可サーバーにアクセスするすべてのユーザーが使用する共通のパスワードを指定するには、AAAサーバーホストモードで**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

構文の説明

string RADIUSサーバーにおけるすべての認可トランザクションで共通パスワードとして使用される最大 127 文字の英数字キーワード。大文字と小文字は区別されます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
aaa-server host	• 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

このコマンドは、RADIUS 認可サーバーに対してのみ有効です。

RADIUS 認可サーバーでは、各接続ユーザーに対してパスワードおよびユーザー名が必要です。ASA では、ユーザー名が自動的に指定されます。ここでは、パスワードを入力します。RADIUSサーバー管理者は、このASA経由でRADIUSサーバーに対して認可を行う各ユーザーにこのパスワードが関連付けられるようにRADIUSサーバーを設定する必要があります。この情報は、RADIUS サーバー管理者に伝えてください。

共通のユーザーパスワードを指定しなかった場合、各ユーザーのパスワードはユーザー名になります。共通ユーザーパスワードにユーザー名を使用する場合は、セキュリティ上の予防措置として、ネットワーク上の他のいずれの場所でもRADIUSサーバーを認可に使用しないでください。

13-125

（注） *string* 引数は、実質的には意味がありません。RADIUS サーバーはこのフィールドを要求しますが、実際には使用されません。ユーザはこのことを知っている必要はありません。

例

次に、ホスト「1.2.3.4」に「svrgrp1」という名前の RADIUS AAA サーバー グループを設定し、タイムアウト時間を 9 秒に、再試行間隔を 7 秒に、RADIUS 共通パスワードを「allauthpw」に設定する例を示します。

```
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 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa
(config-aaa-server-host)#
radius-common-pw allauthpw
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(config)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバー 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 サーバー 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 サーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルの AAA サーバー統計情報を表示します。

radius-reject-message

認証が拒否された場合のログイン画面でのRADIUS拒否メッセージの表示を有効にするには、トンネルグループ webvpn 属性コンフィギュレーション モードで **radius-eject-message** コマンドを使用します。コンフィギュレーションからコマンドを削除するには、**no** 形式を使用します。

radius-reject-message
no radius-reject-message

コマンド デフォルト

デフォルトでは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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ 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
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

リモート ユーザーに対して、認証の失敗についての RADIUS メッセージを表示する場合は、このコマンドをイネーブルにします。

例

次に、engineering という名前の接続プロファイルに対して RADIUS 拒否メッセージの表示をイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group engineering webvpn-attributes
ciscoasa(config-tunnel-webvpn)# radius-reject-message
```

radius-with-expiry (Deprecated)

（注） このコマンドをサポートする最後のリリースは、Version 8.0(1) でした。

認証中にMS-CHAPv2を使用してユーザーとパスワードアップデートをネゴシエートするように ASA を設定するには、トンネルグループ ipsec 属性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。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

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドのデフォルト設定は、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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ ipsec 属性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。
7.1(1)	このコマンドは廃止されました。**password-management** コマンドに置き換わっています。**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。
8.0(2)	このコマンドは廃止されました。

使用上のガイドライン

この属性は、IPSec リモート アクセス トンネル グループ タイプに対してのみ適用できます。RADIUS 認証が設定されていない場合、ASA ではこのコマンドは無視されます。

例

次に、設定 ipsec コンフィギュレーション モードで、remotegrp という名前のリモート アクセス トンネル グループに対して radius-with-expiry を設定する例を示します。

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

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 グループをクリアします。
password-management	パスワード管理をイネーブルにします。このコマンドは、トンネルグループ一般属性モードでは、**radius-with-expiry** 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 属性を設定します。

RAID

RAID 内の SSD を管理するには、特権 EXEC モードで **raid** コマンドを使用します。

（注） このコマンドは、Cisco Secure Firewall 3100 でのみサポートされています。

raid { **add** | **remove** | **remove-secure** } **local-disk** { **1** | **2** } [*psid*]

構文の説明

add	SSD を RAID に追加します。新しい SSD と RAID の同期が完了するまでに数時間かかることがありますが、その間、ファイアウォールは完全に動作します。再起動もでき、電源投入後に同期は続行されます。
psid	以前に別のシステムで使用されていて、まだロックされている SSD を追加する場合は、*psid* と入力します。*psid* は SSD の背面に貼られたラベルに印刷されています。または、システムを再起動し、SSD を再フォーマットして RAID に追加できます。
remove	SSD を RAID から取り外し、データをそのまま保持します。
remove-secure	SSD を RAID から取り外し、自己暗号化ディスク機能を無効にして、SSD を安全に消去します。
local-disk {**1** | **2**}	SSD（disk1 または disk2）を指定します。

コマンド デフォルト

SSD が 2 つある場合、起動時に RAID が形成されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
9.17(1)	このコマンドは、Cisco Secure Firewall 3100 に導入されました。

使用上のガイドライン

ファイアウォールの電源が入っているときに、次のタスクを実行できます。

- SSD の 1 つをホットスワップする：SSD に障害がある場合は、交換できます。SSD が 1 つしかない場合、ファイアウォールの電源がオンになっている間 SSD は取り外せません。
- SSD の 1 つを取り外す：SSD が 2 つある場合は、1 つを取り外すことができます。
- 2 つ目の SSD を追加する：SSD が 1 つの場合は、2 つ目の SSD を追加して RAID を形成できます。

注意 この手順を使用して、SSD を RAID から削除する前に SSD を取り外さないでください。データが失われる可能性があります。

例

次に、RAID から disk2 が削除され、安全に消去される例を示します。

```
ciscoasa# raid remove-secure local-disk 2
```

関連コマンド

コマンド	説明
show raid	RAID ステータスを表示します。
show ssd	SSD ステータスを表示します。

range

ネットワークオブジェクトのアドレスの範囲を設定するには、オブジェクトコンフィギュレーション モードで **range** コマンドを使用します。コンフィギュレーションからオブジェクトを削除するには、このコマンドの **no** 形式を使用します。

range *ip_addr_1 ip_addr2*
no range *ip_addr_1 ip_addr2*

構文の説明

ip_addr_1	範囲の最初の IP アドレス（IPv4 または IPv6）を指定します。
ip_addr_2	範囲の最後の IP アドレスを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
オブジェクトネットワーク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
8.3(1)	このコマンドが追加されました。
9.0(1)	IPv6 アドレスのサポートが追加されました。

使用上のガイドライン

既存のネットワーク オブジェクトを異なる IP アドレスを使用して設定すると、新しいコンフィギュレーションが既存のコンフィギュレーションに置き換わります。

例

次に、範囲ネットワーク オブジェクトを作成する例を示します。

```
ciscoasa (config)# object network OBJECT_RANGE
ciscoasa (config-network-object)# range 10.1.1.1 10.1.1.8
```

関連コマンド

コマンド	説明
clear configure object	作成されたすべてのオブジェクトをクリアします。
description	ネットワーク オブジェクトに説明を追加します。
fqdn	完全修飾ドメイン名のネットワーク オブジェクトを指定します。
host	ホスト ネットワーク オブジェクトを指定します。
nat	ネットワーク オブジェクトの NAT をイネーブルにします。
object network	ネットワーク オブジェクトを作成します。
object-group network	ネットワーク オブジェクト グループを作成します。
show running-config object network	ネットワーク オブジェクト コンフィギュレーションを表示します。
subnet	サブネット ネットワーク オブジェクトを指定します。

ras-rcf-pinholes

ゲートキーパーがネットワーク内にある場合に、H.323 エンドポイント間でのコール設定を有効にするには、パラメータ コンフィギュレーション モードで **ras-rcf-pinholes** 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。

ras-rcf-pinholes enable
no ras-rcf-pinholes enable

構文の説明

enable	H.323 エンドポイント間でのコール設定をイネーブルにします。

コマンド デフォルト

デフォルトでは、このオプションは無効になっています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
8.0(5)	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 には、RegistrationRequest/RegistrationConfirm（RRQ/RCF）メッセージに基づいてコールのピンホールを開くオプションが含まれています。これらの RRQ/RCF メッセージはゲートキーパーとの間で送信されるため、コール側エンドポイントの IP アドレスは不明であり、ASA は送信元 IP アドレス/ポート 0/0 を通じてピンホールを開けます。

例

次に、これらのコールのピンホールを開くアクションをポリシーマップに設定する例を示します。

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# ras-rcf-pinholes enable
```

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。

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。

rate-limit

モジュラポリシーフレームワークを使用する場合は、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インスペクション ポリシー マップに使用できますが（**policy-map type inspect** コマンド）、すべてのアプリケーションでこのアクションが許可されてい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 *rate*
no rate-limit *rate*

構文の説明

rate トラフィックにレート制限を適用します（1～4294967295）。ESMTP、GTP、RTSP、および SIP の場合、レートはパケット/秒単位です。SCTP の場合、レートはキロビット/秒（Kbps）単位です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 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。
9.5(2)	このコマンドはSCTPインスペクションに拡張されました（レートはパケット/秒単位ではなく Kbps 単位）。

使用上のガイドライン

インスペクション 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。インスペクション ポリシー マップで使用できる実際のコマンドは、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 トラフィックを指定した後（**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）、**rate-limit** コマンドを入力して、メッセージのレートを制限できます。

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インスペクションを有効にする場合、このアクションを含むインスペクションポリシーマップを有効にできます。たとえば、**inspect sip sip_policy_map** コマンドを入力します。sip_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、invite 要求を 1 秒あたり 100 メッセージに制限する例を示します。

```
ciscoasa(config-cmap)# policy-map type inspect sip sip-map1
ciscoasa(config-pmap-c)# match request-method invite
ciscoasa(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。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
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。

reactivation-mode

グループ内の障害が発生したサーバーを再アクティブ化する方法を指定するには、AAA サーバー プロトコル 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** }

構文の説明

deadtime *minutes*	（任意）グループ内の最後のサーバーがディセーブルになってから、その後すべてのサーバーを再度イネーブルにするまでの時間を 0 ～ 1440 分の範囲で指定します。デフォルトは 10 分です。
depletion	グループ内のすべてのサーバーが非アクティブになった後でのみ、障害が発生したサーバーを再アクティブ化します。
timed	30 秒のダウン時間の後、障害が発生したサーバを再アクティブ化します。

コマンド デフォルト

デフォルトの再アクティブ化モードは depletion で、デフォルトの deadtime の値は 10 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバープロトコル 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

各サーバ グループには、所属するサーバの再アクティブ化ポリシーを指定する属性があります。

depletion モードでは、非アクティブになったサーバーは、グループにある他のすべてのサーバーが非アクティブになるまで非アクティブのままとなります。すべてのサーバーが非アクティブになると、グループ内のすべてのサーバーが再アクティブ化されます。このアプローチでは、障害が発生したサーバーに起因する接続遅延の発生を最小限に抑えられます。**depletion** モードが使用されている場合は、**deadtime** パラメーターも指定できます。**deadtime** パラメー

タでは、グループ内の最後のサーバーが無効になってから、その後すべてのサーバーを再度有効にするまでの時間を分単位で指定します。このパラメータは、サーバー グループがローカル フォールバック機能とともに使用されている場合にのみ意味があります。さらに、ローカル フォールバックが使用されないアカウンティングにもグループを使用すると、デッドタイムがキャンセルされます。この問題は、アカウンティング用に（同じサーバーで）別のグループを作成することで回避できます。

timedモードでは、障害が発生したサーバーは30秒のダウンタイム後に再アクティブ化されます。このモードは、サーバー リスト内の最初のサーバーをプライマリ サーバーとして使用しており、このサーバーを可能な限りオンラインに維持する必要がある場合に役立ちます。このポリシーは、UDP サーバーの場合は機能しません。サーバーが存在しない場合でも UDP サーバーへの接続に障害が発生することはないため、UDPサーバーはすぐに再度オンラインになります。サーバー リストに到達不能な複数のサーバーが含まれている場合には、接続時間が遅延したり、接続に失敗する場合があります。

同時アカウンティングが無効になっているアカウンティング サーバー グループでは、**timed** モードが強制的に使用されます。このことは、特定のリスト内のすべてのサーバーが同等に扱われることを意味しています。

（注） SDI サーバー グループには、1 つのサーバーしか含まれていないため、このコマンドは SDI サーバー グループに対して無視されます。

例

次に、「svrgrp1」という TACACS+ AAA サーバーを設定し、deadtime を 15 分に設定して、depletion の再アクティベーション モードを使用する例を示します。

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

次に、「svrgrp1」という TACACS+ AAA サーバーを設定し、timed の再アクティベーション モードを使用する例を示します。

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

関連コマンド

accounting-mode	アカウンティング メッセージが単一のサーバーに送信されるか、またはグループ内のすべてのサーバーに送信されるかを示します。

aaa-server protocol	AAA サーバー グループ コンフィギュレーション モードを開始して、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 サーバー パラメータを設定できるようにします。
max-failed-attempts	サーバー グループ内の所定のサーバーが非アクティブ化されるまでに、そのサーバー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 サーバー 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サーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルのAAAサーバー統計情報を表示します。

record-entry

CTL ファイルの作成に使用されるトラストポイントを指定するには、CTL ファイル コンフィギュレーション モードで record-entry コマンドを使用します。CTL からレコード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。

record-entry [**capf cucm cucm-tftp tftp**] **trustpoint** *trustpoint* **address** *ip_address* [**domain-name** *domain_name*]
no record-entry [**capf cucm cucm-tftp tftp**] **trustpoint** *trustpoint* **address** *ip_address* [**domain-name** *domain_name*]

構文の説明

capf	このトラストポイントのロールを CAPF に指定します。1 つの CAPF トラストポイントのみを設定できます。
cucm	このトラストポイントのロールを CCM に指定します。複数の CCM トラストポイントを設定できます。
cucm-tftp	このトラストポイントのロールを CCM+TFTP に指定します。複数の CCM+TFTP トラストポイントを設定できます。
domain-name *domain_name*	（任意）トラストポイントの DNS フィールドの作成に使用されるトラストポイントのドメイン名を指定します。この名前は、サブジェクト DN の一般名フィールドに追加されて、DNS 名が作成されます。トラストポイントに FQDN が設定されていない場合は、ドメイン名を設定する必要があります。
address *ip_address*	トラストポイントの IP アドレスを指定します。
tftp	このトラストポイントのロールを TFTP に指定します。複数の TFTP トラストポイントを設定できます。
trustpoint *trust_point*	インストールされているトラストポイントの名前を設定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CTL ファイル 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
8.0(4)	コマンドが追加されました。

使用上のガイドライン

domain-name は、1 つのみ指定できます。CTL ファイルが存在しない場合は、手動でこの証明書を CUCM から ASA にエクスポートします。

このコマンドは、電話プロキシの CTL ファイルを設定していない場合にのみ使用します。すでに CTL ファイルを設定している場合は、このコマンドを使用しないでください。

ip_address 引数に指定する IP アドレスは、トラストポイントの CTL レコードで使用される IP アドレスとなるため、グローバル アドレス、または IP Phone によって認識されるアドレスである必要があります。

CTL ファイルで必要な各エントリに対して、さらに record-entry コンフィギュレーションを追加します。

例

次に、**record-entry** コマンドを使用して、CTL ファイルの作成に使用されるトラストポイントを指定する例を示します。

```
ciscoasa(config-ctl-file)# record-entry
 cucm-tftp
 trustpoint cucm1 address 192.168.1.2
```

関連コマンド

コマンド	説明
ctl-file (global)	Phone Proxy コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。
ctl-file (phone-proxy)	Phone Proxy コンフィギュレーションで使用する CTL ファイルを指定します。
phone-proxy	Phone Proxy インスタンスを設定します。

record-route

IP オプションインスペクションが設定されたパケットヘッダーで Record Route（RR）オプションが発生したときに実行する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 **record-route** 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。

record-route action { **allow** | **clear** }
no record-route action { **allow** | **clear** }

構文の説明

allow	レコード ルート IP オプションを含むパケットを許可します。
clear	レコードルート 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。

コマンド デフォルト

デフォルトでは、IP オプション インスペクションは、レコード ルート IP オプションを含むパケットをドロップします。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
9.5(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、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、特定の IP オプションを持つどの IP パケットが 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。

例

次に、IP オプション インスペクションのアクションをポリシーマップで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)# record-route 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。

redirect-fqdn

VPN ロードバランシングモードで完全修飾ドメイン名を使用したリダイレクトを有効または無効にするには、グローバル コンフィギュレーション モードで **redirect-fqdn enable** コマンドを使用します。

redirect-fqdn { **enable** | **disable** }
no redirect-fqdn { **enable** | **disable** }

（注） VPN ロード バランシングを使用するには、Plus ライセンスを備えた ASA モデル 5510、または ASA モデル 5520 以降が必要です。また、VPN ロード バランシングには、アクティブな 3DES/AES ライセンスも必要です。セキュリティ アプライアンスは、ロード バランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。アクティブな 3DES または AES のライセンスが検出されない場合、セキュリティ アプライアンスはロード バランシングをイネーブルにせず、ライセンスでこの使用方法が許可されていない場合には、ロードバランシング システムによる 3DES の内部コンフィギュレーションも抑止します。

構文の説明

disable	完全修飾ドメイン名を使用したリダイレクトをディセーブルにします。
enable	完全修飾ドメイン名を使用したリダイレクトをイネーブルにします。

コマンド デフォルト

この動作は、デフォルトでは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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
VPN ロード バランシング 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

デフォルトで、ASA はロードバランシング リダイレクションの IP アドレスだけをクライアントに送信します。DNS 名に基づく証明書が使用されている場合、セカンダリ デバイスにリダイレクトされるとその証明書は無効になります。

VPN クライアント接続を別のクラスタ デバイス（クラスタ内の別の ASA）にリダイレクトするときに、この ASA は VPN クラスタ マスターとして、DNS 逆ルックアップを使用し、そのクラスタ デバイスの（外部 IP アドレスではなく）完全修飾ドメイン名（FQDN）を送信できます。

クラスタ内のロードバランシング デバイスのすべての外部および内部ネットワーク インターフェイスは、同じ IP ネットワーク上に存在する必要があります。

IP アドレスではなく FQDN を使用して WebVPN ロード バランシングを実行するには、次の設定手順を実行する必要があります。

1. **redirect-fqdn enable** コマンドを使用して、ロードバランシングのための FQDN の使用を有効にします。
2. DNS サーバーに、各 ASA 外部インターフェイスのエントリを追加します（エントリが存在しない場合）。それぞれの ASA 外部 IP アドレスに、ルックアップ用にそのアドレスに関連付けられた DNS エントリが設定されている必要があります。これらの DNS エントリに対しては、逆ルックアップもイネーブルにする必要があります。
3. dns domain-lookup inside コマンドを使用して、ASA で DNS ルックアップをイネーブルにします。inside の部分には、DNS サーバーへのルートを持つ任意のインターフェイスを指定します。
4. dns name-server 10.2.3.4 のように、ASA に DNS サーバーの IP アドレスを定義します（10.2.3.4 は、DNS サーバーの IP アドレス）。

例

次に、リダイレクトを無効にする **redirect-fqdn** コマンドの例を示します。

```
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# redirect-fqdn disable
ciscoasa(config-load-balancing)#
```

次に、完全修飾ドメイン名のリダイレクトをイネーブルにし、クラスタのパブリック インターフェイスを「test」と指定し、クラスタのプライベート インターフェイスを「foo」と指定するインターフェイス コマンドを含む、VPN ロード バランシング コマンド シーケンスの例を示します。

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# nat 192.168.10.10
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster key 123456789
ciscoasa(config-load-balancing)# cluster encryption
ciscoasa(config-load-balancing)# cluster port 9023
```

```
ciscoasa(config-load-balancing)# redirect-fqdn enable
ciscoasa(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
clear configure vpn load-balancing	ロード バランシングの実行時コンフィギュレーションを削除し、ロード バランシングをディセーブルにします。
show running-config vpn load-balancing	現在の VPN ロードバランシング仮想クラスタのコンフィギュレーションを表示します。
show vpn load-balancing	VPN ロード バランシング実行時の統計情報を表示します。
vpn load-balancing	VPN ロード バランシング モードを開始します。

redistribute（IPv6 ルータ OSPF）

OSPFv3 ルーティングドメインから別の OSPFv3 ルーティングドメインに IPv6 ルートを再配布するには、IPv6 ルータ OSPF 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。再配布を無効にするには、このコマンドの **no** 形式を使用します。

redistribute *source-protocol* [*process-id*] [**include-connected** { **level-1** | **level-1-2** | **level-2** }] [*as-number*] [**metric** { *metric-value* **transparent** }] [**metric-type** *type-value* **] [match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] }] [**tag** *tag-value*] [**route-map** *map-tag*]

no redistribute *source-protocol* [*process-id*] [**include-connected** { **level-1** | **level-1-2** | **level-2** }] [*as-number*] [**metric** { *metric-value* **transparent** }] [**metric-type** *type-value* **] [match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] }] [**tag** *tag-value*] [**route-map** *map-tag*]

構文の説明

as-number	ルーティング プロセスの自律システム番号を指定します。有効値の範囲は 1 ～ 65535 です。
external	指定した自律システムの外部にあり、タイプ 1 またはタイプ 2 の外部ルートとして OSPFv3 にインポートされる OSPFv3 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。
include-connected	（オプション）ソース プロトコルから学習したルートと、ソース プロトコルが動作しているインターフェイス上の接続先プレフィックスを、ターゲット プロトコルで再配布できるようにします。
internal	指定した自律システムの内部にある OSPFv3 メトリック ルートを指定します。
level-1	Intermediate System-to-Intermediate System（IS-IS）用に、レベル 1 ルートが他の IP ルーティング プロトコルに個別に再配布されることを指定します。
level-1-2	IS-IS 用に、レベル 1 とレベル 2 の両方のルートが他の IP ルーティング プロトコルに個別に再配布されることを指定します。
level-2	IS-IS 用に、レベル 2 ルートが他の IP ルーティング プロトコルに個別に再配布されることを指定します。
map-tag	設定したルート マップの識別情報を指定します。
match	（オプション）他のルーティング ドメインにルートを再配布します。
metric *metric_value*	（オプション）OSPFv3 のデフォルト メトリック値を指定します。有効な値の範囲は、0 ～ 16777214 です。

metric-type *metric_type*	（オプション）OSPFv3 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のルートに関連付けられる外部リンク タイプを指定します。1（タイプ 1 外部ルート）または 2（タイプ 2 外部ルート）を指定できます。
nssa-external	自律システムの外部にあり、タイプ 1 またはタイプ 2 の外部ルートとして IPv6 用の Not-So-Stubby Area（NSSA）の OSPFv3 にインポートされるルートを指定します。
process-id	（オプション）OSPFv3 ルーティング プロセスをイネーブルにする場合に管理目的で割り当てる番号を指定します。
route-map *map_name*	（オプション）送信元ルーティング プロトコルから現在の OSPFv3 ルーティング プロトコルにインポートするルートをフィルタリングするために使用するルート マップの名前を指定します。このキーワードを指定し、ルート マップ タグを 1 つも指定しないと、いずれのルートもインポートされません。指定しない場合は、すべてのルートが再配布されます。
source-protocol	ルートの再配布元のプロトコルを指定します。有効な値は、connected、ospf、または static です。
tag *tag_value*	（オプション）各外部ルートに付加する 32 ビットの 10 進値を指定します。この値は OSPFv3 自身には使用されませんが、ASBR 間の情報伝達に使用できます。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。有効値の範囲は、0 ～ 4294967295 です。
transparent	（オプション）再配布ルートのルーティング テーブル メトリックを RIP メトリックとして使用します。

コマンド デフォルト

コマンドのデフォルトは次のとおりです。

- **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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPv6 ルータ OSPF 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
9.0(1)	このコマンドが追加されました。

例

次に、スタティック ルートを現在の OSPFv3 プロセスに再配布する例を示します。

```
ciscoasa(config-if)# ipv6
 router ospf 1
ciscoasa(config-rtr)# redistribute static
```

関連コマンド

コマンド	説明
ipv6 router ospf	OSPFv3 のルータ コンフィギュレーション モードを開始します。
show running-config ipv6 router	OSPFv3 のルータ コンフィギュレーションのコマンドを表示します。

redistribute（ルータ EIGRP）

1 つのルーティングドメインから EIGRP 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 EIGRP 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 { { **eigrp** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** } [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*
no redistribute { { **eigrp** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** } [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*

構文の説明

bandwidth	EIGRP 帯域幅メトリック（キロビット/秒）。有効な値は、1 ～ 4294967295 です。
connected	インターフェイスに接続されているネットワークを EIGRP ルーティング プロセスに再配布することを指定します。
delay	EIGRP 遅延メトリック（10 マイクロ秒単位）有効な値は、0 ～ 4294967295 です。
external *type*	指定した自律システムの外部にある EIGRP 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の内部にある EIGRP メトリック ルートを指定します。
load	EIGRP 有効帯域幅（負荷）メトリック。有効な値は、1 ～ 255 です（255 は 100% の負荷を示します）。
match	（任意）OSPF から EIGRP にルートを再配布する条件を指定します。
metric	（任意）EIGRP ルーティング プロセスに再配布されるルートの EIGRP メトリックの値を指定します。
mtu	パスの MTU。有効値は 1 ～ 65535 です。
nssa-external *type*	NSSA の外部にあるルートの EIGRP 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。
eigrp *pid*	EIGRP ルーティング プロセスに EIGRP ルーティング プロセスを再配布するために使用します。*pid* では、EIGRP ルーティング プロセス内部で使用される識別パラメータを指定します。有効値は 1 ～ 65535 です。
信頼性	EIGRP 信頼性メトリック。有効な値は、0 ～ 255 です（255 は 100% の信頼性を示します）。
rip	RIP ルーティング プロセスから EIGRP ルーティング プロセスへのネットワークの再配布を指定します。

route-map *map_name*	（任意）送信元ルーティング プロトコルから EIGRP ルーティング プロセスにインポートされる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。指定しない場合は、すべてのルートが再配布されます。
static	EIGRP ルーティング プロセスにスタティック ルートを再配布するために使用します。

コマンド デフォルト

コマンドのデフォルトは次のとおりです。

- **match**：**Internal**、**external 1**、**external 2**

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ EIGRP 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 モードのサポートが追加されました。

使用上のガイドライン

EIGRP 構成に **default-metric** コマンドを設定していない場合は、redistribute コマンドで **metric** を指定する必要があります。

例

次に、スタティック ルートおよび接続ルートを EIGRP ルーティング プロセスに再配布する例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# redistribute static
ciscoasa(config-router)# redistribute connected
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成し、このプロセスのコンフィギュレーション モードを開始します。

コマンド	説明
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

redistribute（ルータ OSPF）

1つのルーティングドメインからOSPF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 OSPF 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** 形式をオプションを指定せずに使用します。このコマンドの **no** 形式でオプションを指定した場合、そのオプションの構成だけが削除されます。

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

構文の説明

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。
eigrp *as-number*	OSPF ルーティング プロセスに EIGRP ルートを再配布するために使用します。*as-number* は、EIGRP ルーティング プロセスの自律システム番号を指定します。有効値は 1 ～ 65535 です。
external *type*	指定した自律システムの外部にある 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の内部にある OSPF メトリック ルートを指定します。
match	（任意）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*	（任意）OSPF のデフォルト メトリック値を、0 ～ 16777214 の範囲で指定します。
metric-type *metric_type*	（任意）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ている外部リンク タイプ。**1**（タイプ 1 外部ルート）または **2**（タイプ 2 外部ルート）のいずれかの値を指定できます。
nssa-external *type*	NSSA の外部にあるルートの 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*	現在の OSPF ルーティング プロセスに OSPF ルーティング プロセスを再配布するために使用します。*pid* は OSPF ルーティング プロセス用に内部で使用される ID パラメータを指定します。有効な値は 1 ～ 65535 です。
rip	RIP ルーティング プロセスから現在の OSPF ルーティング プロセスへのネットワークの再配布を指定します。

route-map *map_name*	（任意）送信元ルーティング プロトコルから現在の OSPF ルーティング プロセスにインポートされる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。指定しない場合は、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	（任意）OSPF へのルートの再配布において、指定したプロトコルの再配布の範囲を指定します。使用しない場合は、クラスフル ルートのみが再配布されます。
tag *tag_value*	（任意）各外部ルートに付けられた 32 ビットの 10 進値。この値は OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。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。有効値の範囲は、0 ～ 4294967295 です。

コマンド デフォルト

コマンドのデフォルトは次のとおりです。

- **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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ OSPF 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。
7.2(1)	このコマンドは、**rip** キーワードを含むように変更されました。
8.0(2)	このコマンドは、**eigrp** キーワードを含むように変更されました。

リリース	変更内容
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、スタティック ルートを現在の OSPF プロセスに再配布する例を示します。

```
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# redistribute static
```

関連コマンド

コマンド	説明
redistribute (RIP)	RIP ルーティング プロセスにルートを再配布します。
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

redistribute（ルータ 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 RIP 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** | **eigrp** *as-number* } [**metric** *metric_value*] [**transparent**] [**route-map** *map_name*]
no redistribute { { **ospf** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** | **eigrp** *as-number* } [**metric** *metric_value*] [**transparent**] [**route-map** *map_name*]

構文の説明

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。
eigrp *as-number*	RIP ルーティング プロセスに EIGRP ルートを再配布するために使用します。*as-number* は、EIGRP ルーティング プロセスの自律システム番号を指定します。有効値は 1 ～ 65535 です。
external *type*	指定した自律システムの外部にある 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の内部にある OSPF メトリック ルートを指定します。
match	（任意）OSPF から RIP にルートを再配布する条件を指定します。
metric {*metric_value* | **transparent**}	（任意）再配布するルートの RIP メトリック値を指定します。*metric_value* の有効な値は、0 ～ 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）の外部にあるルートの 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*	RIP ルーティング プロセスに OSPF ルーティング プロセスを再配布するために使用します。*pid* は OSPF ルーティング プロセス用に内部で使用される ID パラメータを指定します。有効な値は 1 ～ 65535 です。
route-map *map_name*	（任意）送信元ルーティングプロトコルからRIPルーティングプロセスにインポートされる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。指定しない場合は、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。

コマンド デフォルト

コマンドのデフォルトは次のとおりです。

- **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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ RIP 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
7.2(1)	このコマンドが追加されました。
8.0(2)	このコマンドは、**eigrp** キーワードを含むように変更されました。
9.0(1)	マルチ コンテキスト モードはサポートされます。

例

次に、スタティック ルートを現在の RIP プロセスに再配布する例を示します。

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

関連コマンド

コマンド	説明
redistribute (router eigrp)	他のルーティング ドメインから EIGRP にルートを再配布します。
redistribute (router ospf)	他のルーティング ドメインから OSPF に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。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

redistribute isis

特にレベル 1 からレベル 2 またはレベル 2 からレベル 1 へ IS-IS ルートを再配布するには、ルータ ISIS コンフィギュレーション モードで **redistribute isis** コマンドを使用します。再配布を無効にするには、このコマンドの **no** 形式を使用します。

redistribute isis ip { **level-1** | **level-2** } **into** { **level-2** | **level-1** } [[**distribute-list** *list-number*] | [**route-map** *map-tag*]]
no redistribute isis ip { **level-1** | **level-2** } **into** { **level-2** | **level-1** } [[**distribute-list** *list-number*] | [**route-map** *map-tag*]]

構文の説明

level-1 | level-2	IS-IS ルートを再配布するレベル元とレベル先。
into	ルートが再配布されるレベル元と、ルートを再配布するレベル先を区別するキーワード。
distribute-list *list-number*	（任意）IS-IS 再配布を制御する配布リスト番号。配布リストまたはルートマップのいずれかを指定できますが、両方を指定できません。
route-map *map-tag*	（任意）IS-IS 再配布を制御するルートマップ名。配布リストまたはルートマップのいずれかを指定できますが、両方を指定できません。

コマンド デフォルト

このコマンドにデフォルトの動作または値はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ isis 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

IS-IS では、すべてのエリアがスタブ エリアで、バックボーン（レベル 2）からエリア（レベル 1）へルーティング情報がリークしません。レベル 1 だけのルートは、そのエリア内にある最も近いレベル 1 - レベル 2 ルータへのデフォルト ルートを使用します。このコマンドにより、レベル 2 IP ルートをレベル 1 エリアに再配布することができます。この再配布により、レベル 1 だけのルータが IP プレフィックスのエリア外への最良パスを選択することができるよ

うになります。これは IP のみの機能であり、CLNS ルーティングはまだスタブ ルーティングです。

制御と安定性を増すために、配布リストまたはルートマップを設定して、どのレベル2 IP ルートをレベル 1 に再配布できるのかを制御できます。これを使用すると、大規模な IS-IS-IP ネットワークは、スケーラビリティを向上させるためにエリアを使用できます。

（注） **redistribute isis** コマンドを機能させるためには、**metric-style wide** コマンドを指定する必要があります。

例

次の例では、アクセス リスト 100 がレベル 1 からレベル 2 への IS-IS の再配布を制御しています。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0000.0001.00
ciscoasa(config-router)# metric-style wide
ciscoasa(config-router)# redistribute isis ip level-1 into level-2 distribute-list 100
ciscoasa(config-router)# access-list 100 permit ip 10.10.10.0 0.0.0.255 any
```

次の例では、110 のタグの付いたルートだけが再配布されるように、match-tag という名前のルート マップがレベル 1 からレベル 2 への IS-IS の再配布を制御します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0000.0001.00
ciscoasa(config-router)# metric-style wide
ciscoasa(config-router)# redistribute isis ip level-1 into level-2 route-map match-tag
ciscoasa(config-router)# route-map match-tag permit 10
ciscoasa(config-router)# match tag 11
```

関連コマンド

redundant-interface

アクティブにする冗長インターフェイスのメンバーインターフェイスを設定するには、特権 EXEC モードで **redundant-interface** コマンドを使用します。

redundant-interface redundant *number* **active-member** *physical_interface*

構文の説明

active-member *physical_interface*	アクティブ メンバーを設定します。有効値については、**interface** コマンドを参照してください。両方のメンバー インターフェイスが同じ物理タイプである必要があります。
redundant *number*	冗長インターフェイス ID（**redundant1** など）を指定します。

コマンド デフォルト

デフォルトで、コンフィギュレーション内の最初のメンバーインターフェイスが使用可能な場合、そのインターフェイスがアクティブ インターフェイスとなります。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
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

どのインターフェイスがアクティブであるかを表示するには、次のコマンドを入力します。

```
ciscoasa# show interface redundant
number
 detail
 | grep Member
```

次に例を示します。

```
ciscoasa# show interface redundant1
 detail
 | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

例

次に、冗長インターフェイスを作成する例を示します。デフォルトでは、gigabitethernet 0/0がコンフィギュレーション内の最初のインターフェイスであるため、このインターフェイスがアクティブです。redundant-interface コマンドでは、gigabitethernet 0/1 をアクティブ インターフェイスに設定しています。

```
ciscoasa(config-if)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# redundant-interface redundant1 active-member gigabitethernet0/1
```

関連コマンド

コマンド	説明
clear interface	**show interface** コマンドのカウンタをクリアします。
debug redundant-interface	冗長インターフェイスのイベントまたはエラーに関するデバッグ メッセージを表示します。
interface redundant	冗長インターフェイスを作成します。
member-interface	冗長インターフェイス ペアにメンバー インターフェイスを割り当てます。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

regex

テキストを照合する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*
regex *name* [*regular_expression*]

構文の説明

name	正規表現名を最大 40 文字で指定します。
regular_expression	最大 100 文字の正規表現を指定します。正規表現で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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
7.2(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

regex コマンドは、テキスト照合が必要なさまざまな機能で使用できます。たとえば、インスペクション ポリシー マップを使用して、モジュラ ポリシー フレームワークを使用したアプリケーション インスペクションの特別なアクションを設定できます（**policy map type inspect** コマンドを参照）。インスペクション ポリシー マップでは、1 つ以上の **match** コマンドを含んだインスペクション 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識別できます。または、**match** コマンドをインスペクション 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、パケット内の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 パケット内の URL 文字列を照合できます。正規表現クラスマップ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）。

正規表現は、ストリングそのものとしてテキスト ストリングと文字どおりに照合することも、*metacharacters* を使用してテキスト ストリングの複数のバリアントと照合することもできます。

正規表現を使用して、特定のアプリケーショントラフィックの内容（HTTPパケット内の本文テキストなど）を照合できます。

（注） 最適化のために、ASA では、難読化解除された URL が検索されます。難読化解除では、複数のスラッシュ（/）が単一のスラッシュに圧縮されます。通常、「http://」のようなダブル スラッシュが使用される文字列では、代わりに「http:/」を検索してください。

表 1 : regex メタ文字 に、特別な意味を持つメタ文字の一覧を示します。

表 *1 : regex* メタ文字

文字	説明	注記
.	ドット	任意の単一文字と一致します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。
(*exp***)**	サブ表現	サブ表現は、文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。たとえば、**d(o|a)g** は dog および dag に一致しますが、**do|ag** は do および ag に一致します。また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
|	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。たとえば、**dog|cat** は、dog または cat に一致します。
?	疑問符	直前の表現が 0 または 1 個存在することを示す修飾子。たとえば、**lo?se** は、lse または lose に一致します。 （注） **Ctrl+V** を入力してから疑問符を入力しないと、ヘルプ機能が呼び出されます。
*	アスタリスク	直前の表現が 0、1、または任意の個数存在することを示す修飾子。たとえば、**lo*se** は、lse、lose、loose などに一致します。
+	プラス	直前の表現が少なくとも 1 個存在することを示す修飾子。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
{*x***}** または **{***x***,}**	最小繰り返し限定作用素	少なくとも *x* 回繰り返します。たとえば、 **ab(xy){2,}z** は、abxyxyz や abxyxyxyz などに一致します。
[*abc***]**	文字クラス	カッコ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 に一致します。

文字	説明	注記
[^*abc*]	否定文字クラス	角カッコに含まれていない単一文字と一致します。たとえば、**[^abc]** は a、b、c 以外の任意の文字に一致し、**[^A-Z]** は大文字以外の任意の 1 文字に一致します。
[*a-c*]	文字範囲クラス	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。文字と範囲の組み合わせも可能です。**[abcq-z]** は、a、b、c、q、r、s、t、u、v、w、x、y、z、および**[a-cq-z]** に一致します。 ダッシュ（-）文字は、角カッコ内の最初の文字または最後の文字である場合にのみリテラルとなります（**[abc-]** や **[-abc]**）。
""	引用符	文字列の末尾または先頭のスペースを保持します。たとえば、**"test"** は、一致を検索する場合に先頭のスペースを保持します。
^	キャレット	行の先頭を指定します。
\	エスケープ文字	メタ文字とともに使用すると、リテラル文字と一致します。たとえば、**\[** は左角カッコに一致します。
char	文字	文字がメタ文字でない場合は、リテラル文字と一致します。
\r	復帰	復帰 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	タブ	タブ 0x09 と一致します。
\f	改ページ	フォーム フィード 0x0c と一致します。
\x*NN*	エスケープされた 16 進数	16 進数（厳密に 2 桁）を使用した ASCII 文字と一致します。
\NNN	エスケープされた 8 進数	8 進数（厳密に 3 桁）としての ASCII 文字と一致します。たとえば、文字 040 はスペースを表します。

使用上のガイドライン

正規表現が想定どおりに一致するかどうかをテストするには、**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、主に次の 2 つの要因によって決定されます。

- 正規表現照合で検索される必要があるテキストの長さ。

検索長が短い場合は、正規表現エンジンの ASA に対するパフォーマンス上の影響は小さくなります。

- 正規表現照合で検索される必要がある正規表現チェーン テーブルの数。

検索長のパフォーマンスへの影響

正規表現検索を設定すると、通常は、検索対象テキストのすべてのバイトが正規表現データベースに対して検査されて、一致が検索されます。検索対象テキストが長くなるほど、検索時間も長くなります。次に、この現象を表すパフォーマンス テスト ケースを示します。

- ある HTTP トランザクションでは、1 回の 300 バイトの GET 要求と 1 回の 3250 バイトの応答が行われます。
- URI 検索には 445 の正規表現が、要求本文検索には 34 の正規表現が使用されます。
- 応答本文検索には 55 の正規表現が使用されます。

URI および HTTP GET 要求の本文のみを検索するようにポリシーを設定すると、スループットは次のようになります。

- 対応する正規表現データベースが検索されない場合は 420 Mbps。
- 対応する正規表現データベースが検索される場合は 413 Mbps（正規表現を使用するオーバーヘッドが比較的小さいことがわかります）。

ただし、HTTP 応答本文全体も検索するようにポリシーを設定すると、応答本文の検索対象が長いため（3250 バイト）、スループットは 145 Mbps まで低下します。

正規表現検索のテキスト長が長くなる要因は次のとおりです。

- 複数の異なるプロトコル フィールドに対して正規表現検索が設定されている場合。たとえば、HTTP インスペクションでは、URI にのみ正規表現照合が設定されていると、URI フィールドのみが正規表現照合のために検索され、検索長は URI 長に制限されます。ただし、ヘッダーや本文などの他のプロトコル フィールドにも正規表現照合が設定されていると、ヘッダー長や本文長の分だけ検索長が長くなります。
- 検索対象のフィールドが長い場合。たとえば、URI に正規表現検索が設定されている場合、GET 要求内の長い URI の検索長は長くなります。また、現在、HTTP 本文の検索長はデフォルトで 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にポリシーを設定し、本文検索長が 5000 バイトに変更されると、本文検索が長くなるため、パフォーマンスに対して大きな影響があります。

正規表現チェーンテーブル数のパフォーマンスへの影響

現在、同じプロトコル フィールドに設定されたすべての正規表現（URI に対するすべての正規表現など）は、1 つ以上の正規表現チェーン テーブルで構成されるデータベースに構築されます。テーブルの数は、必要な合計メモリ量、およびテーブル構築時に使用可能なメモリ量によって決定されます。次のいずれかの条件が満たされる場合、正規表現データベースは複数のテーブルに分割されます。

- 必要な合計メモリが 32 MB を超える場合。これは、最大テーブル サイズが 32 MB に制限されているためです。

- 最大連続メモリ サイズが正規表現データベース全体を構築するのに十分ではない場合、複数の小さなテーブルが構築されて、それらのテーブルにすべての正規表現が格納されます。メモリ フラグメンテーションの程度は、相互に関連する数多くの要因によって左右されるため、フラグメンテーションのレベルを予測することは事実上不可能です。

複数のチェーン テーブルがある場合、正規表現照合において各テーブルが検索される必要があるため、検索時間は検索対象のテーブル数に比例して長くなります。

特定のタイプの正規表現では、テーブル サイズが大幅に増加する傾向があります。可能な限りワイルドカードおよび繰り返し要素を避けるように正規表現を設計することを推奨します。次のメタ文字については、表 1 : regex メタ文字 を参照してください。

- ワイルドカード タイプの指定を伴う正規表現
- ドット（.）
- クラス内の任意の文字に一致するさまざまな文字クラス
- [^a-z]
- [a-z]
- [abc]]
- 繰り返しタイプの指定を伴う正規表現
- *
- +
- {n,}
- 次のようにワイルドカードタイプの正規表現と繰り返しタイプの正規表現を組み合わせると、テーブル サイズが大幅に増加する可能性があります。
- 123.*xyz
- 123.+xyz
- [^a-z]+
- [^a-z]*
- .*123.*（これは、「123」と照合することと同じであるため、このような指定は行わないでください）。

次に、ワイルドカードや繰り返しの有無によって正規表現のメモリ使用量がどのように異なるかについての例を示します。

- 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 サイズはわずか 10240 バイトです。

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

正規表現の数が増えると、正規表現データベースで必要になる合計メモリ量も増え、そのためメモリがフラグメント化されている場合にはより多くのテーブル数が必要になる可能性があります。次に、異なる正規表現数でのメモリ使用量の例を示します。

- 100 サンプル URI：3,079,168 バイト
- 200 サンプル URI：7,156,224 バイト
- 500 サンプル URI：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 データベースにあるチェーンテーブルの数を表示できます。

例

次に、インスペクション ポリシー マップで使用する 2 つの正規表現を作成する例を示します。

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(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と照合するインスペクション 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 つ以上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 インスペクション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

リブートして構成をリロードするには、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**]

構文の説明

at *hh*:*mm*	（任意）ソフトウェアのリロードが（24 時間制で）指定された時刻に行われるようにスケジューリングします。月日を指定しない場合、リロードは、指定時刻が現在時刻よりも後の場合は当日の指定時刻に、指定時刻が現在時刻よりも前の場合は翌日の指定時刻に行われます。00:00 を指定すると、深夜 0 時のリロードが設定されます。リロードは、24 時間以内に実行される必要があります。
cancel	（任意）スケジューリングされているリロードをキャンセルします。
day	（任意）1 ～ 31 の範囲で日付を指定します。
in [*hh*:]*mm*]	（任意）指定した分数、または時間および分数が経過したときにソフトウェアがリロードされるようにスケジューリングします。リロードは、24 時間以内に実行される必要があります。
max-hold-time [*hh*:*mm*	（任意）シャットダウンまたはリブートの前に他のサブシステムに対して通知するために ASA が待機する最大ホールド時間を指定します。この時間が経過すると、（強制）クイック シャットダウンまたはリブートが実行されます。
month	（任意）月の名前を指定します。月の名前を表す一意のストリングを作成するために十分な文字を入力します。たとえば、「Ju」は、June または July を表すことができるため一意ではありませんが、「Jul」は一意です。これは、「Jul」で始まる月は「July」しかないためです。
noconfirm	（任意）ユーザーの確認なしでリロードすることを ASA に許可します。
quick	（任意）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*	（任意）リロードの理由を 1 ～ 255 文字で指定します。理由のテキストは、すべての開いている IPsec VPN クライアント、端末、コンソール、Telnet、SSH、および ASDM 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は、IPsec VPN クライアントに理由のテキストを送信するために追加のコンフィギュレーションが必要となります。詳細については、VPN CLI 設定ガイドを参照してください。

save-config	（任意）シャットダウンの前に、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、未保存の構成の変更はリロード後にすべて失われます。
save-show-tech	（任意）リロードの実行前に **show tech** コマンドの出力をファイルに保存します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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)	このコマンドが変更されて、*day*、*hh*、*mm*、*month*、**quick**、**save-config**、および *text* という新しい引数とキーワードが追加されました。
9.1(3)	**save-show-tech** キーワー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、ASA をリブートして、構成をフラッシュメモリからリロードできます。

reload コマンドは、デフォルトではインタラクティブです。ASA は、まず構成が変更されていて、未保存であるかどうかをチェックします。未保存の場合、構成を保存するように求められます。マルチコンテキストモードでは、ASA によって、未保存の構成がある各コンテキストに対してプロンプトが表示されます。**save-config** キーワードを指定すると、構成はプロンプトなしで保存されます。次に、システムのリロードを確認するプロンプトが表示されます。**y** と入力するか、または **Enter** キーを押した場合にのみリロードが行われます。確認後、ASA は遅延キーワード（**in** または **at**）の指定状況に応じて、リロードプロセスを開始またはスケジューリングします。

デフォルトでは、リロードプロセスは「グレースフル」モードで実行されます。すべての登録されているサブシステムは、リブート実行の前に通知されるため、リブート前に適切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発生するまで待機しない場合は、**max-hold-time** キーワードを指定して、待機する最大時間を指定します。または、**quick** キーワードを使用して、影響のあ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せずに、すぐに強制的にリロードプロセスを開始できます。

noconfirm キーワードを指定すると、**reload** コマンドを非対話形式で強制的に実行できます。この場合、ASA では、**save-config** キーワードを指定していない限り、未保存の構成の有無はチェックされません。また、システムをリブートする前に、確認のプロンプトは表示されません。遅延キーワードを指定していない限り、リロードプロセスが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** キーワードまたは **quick** キーワードを指定して、動作またはリロードプロセスを制御できます。

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** コマンドを使用します。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、リロード後に失われます。リブートの前に、**write memory** コマンドを入力して、フラッシュパーティションに現在の構成を保存してください。

例

次に、リブートしてコンフィギュレーションをリロードする例を示します。

```
ciscoasa#
reload
Proceed with ?  [confirm]
 y
Rebooting...
XXX
Bios VX.X
...
```

関連コマンド

コマンド	説明
show reload	ASA 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。この数を超えると、ASA によってトラップが送信されます。

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

構文の説明

threshold-value	ASA でサポートされるセッションの制限数以下の整数を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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。

例

次に、しきい値を 1500 に設定する例を示します。

```
ciscoasa# 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	しきい値によるトラッピングをイネーブルにします。

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*

構文の説明

new_name	クラス マップの新しい名前を最大 40 文字で指定します。「class-default」という名前は予約されています。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 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。

例

次に、test というクラス マップの名前を test2 に変更する例を示します。

```
ciscoasa(config)# class-map test
ciscoasa(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。

rename（特権 EXEC）

ファイルまたはディレクトリの名前を送信元のファイル名から宛先のファイル名に変更するには、特権 EXEC モードで **rename** コマンドを使用します。

rename [**/noconfirm**] [**disk0 :** | **disk1 :** | **flash:**] *source-path* [**disk0 :** | **disk1 :** | **flash:**] *destination-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。
destination-path	新しいファイル名のパスを指定します。
disk0 :	（任意）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）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）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。
source-path	元のファイル名のパスを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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

rename flash: flash: コマンドを入力すると、送信元と宛先のファイル名を入力するように求められます。

ファイル システムにまたがってファイルやディレクトリの名前を変更することはできません。

次に例を示します。

```
ciscoasa# rename flash: disk1:
Source filename []? new-config
```

```
Destination filename []? old-config
%Cannot rename between filesystems
```

例

次に、「test」というファイルの名前を「test1」に変更する例を示します。

```
ciscoasa# 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。

renewal-reminder

ユーザー証明書が期限切れになる何日前に、証明書所有者に再登録の初回リマインダを送信するかを指定するには、CA サーバー コンフィギュレーション モードで **renewal-reminder** コマンドを使用します。期間をデフォルトの 14 日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。

renewal-reminder *days*
no renewal-reminder

構文の説明

days	発行されている証明書が期限切れになる何日前に証明書所有者に対して再登録の初回リマインダを送信するかを指定します。有効な値の範囲は、1 ～ 90 日です。

コマンド デフォルト

デフォルト値は 14 日間です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CA サーバー 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
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

通知は全部で 3 種類あります。ユーザー データベースに電子メール アドレスが指定されていれば、3 種類の通知がそれぞれ電子メールで自動的に証明書所有者に送信されます。電子メールアドレスが存在しない場合は、更新を管理者に通知する syslog メッセージが生成されます。

デフォルトでは、証明書が期限切れになる前に、CA サーバーから次の 3 種類の電子メール メッセージが指定した順序で送信されます。

1. 証明書の登録案内

2. 確認：証明書の登録案内

3. 最終確認：証明書の登録案内

最初の電子メールは案内で、2 番目の電子メールは確認、3 番目の電子メールは最終確認です。この通知のデフォルトの設定は 14 日です。証明書の有効期限の 14 日前に最初の案内が送信さ

れ、有効期限の 7 日前に確認の電子メールが送信され、有効期限の 3 日前に最終確認の電子メールが送信されます。

renewal-reminder の間隔は、**renewal-reminder** *days* コマンドを使用してカスタマイズできます。

例

次に、証明書有効期限の 7 日前に ASA からユーザーに対して有効期限通知を送信するように指定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# renewal-reminder 7
ciscoasa
(config-ca-server)
#
```

次に、有効期限通知のタイミングをデフォルトである証明書有効期限の 14 日前にリセットする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no renewal-reminder
ciscoasa
(config-ca-server)
#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバー コンフィギュレーション モードのコマンド セットにアクセスできるようにします。これらのコマンドセットを使用することで、ローカル CA を設定および管理できます。
lifetime	CA 証明書、すべての発行されている証明書、および CRL のライフタイムを指定します。
show crypto ca server	ローカル CA サーバーのコンフィギュレーション詳細を表示します。

replication http

フェールオーバーグループに対してHTTP接続のレプリケーションを有効にするには、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

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ディセーブル

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 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、ASA 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、また HTTP クライアントは接続試行が失敗すると通常は再試行するため、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** コマンドを使用すると、ステートフル フェールオーバー環境において HTTP セッションのステートフル レプリケーションが可能になりますが、システムのパフォーマンスに悪影響が出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 フェールオーバー構成のフェールオーバーグループ用であることを除いて、Active/Standby フェールオーバー用の **failover replication http** コマンドと機能的に同じです。

例

次の例では、フェールオーバー グループで可能な設定を示します。

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# replication http
ciscoasa(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 接続を複製するためのステートフル フェールオーバーを設定します。

request-command deny

FTP 要求内の特定のコマンドを禁止するには、**ftp-map** コマンドを使用してアクセスできる 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。設定を削除するには、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** }

構文の説明

appe	ファイルへの追加を行うコマンドを拒否します。
cdup	現在の作業ディレクトリの親ディレクトリに移動するコマンドを拒否します。
dele	サーバーのファイルを削除するコマンドを拒否します。
get	サーバーからファイルを取得するクライアント コマンドを拒否します。
help	ヘルプ情報を提供するコマンドを拒否します。
mkd	サーバー上にディレクトリを作成するコマンドを拒否します。
put	サーバーにファイルを送信するクライアント コマンドを拒否します。
rmd	サーバー上のディレクトリを削除するコマンドを拒否します。
rnfr	変更元ファイル名を指定するコマンドを拒否します。
rnto	変更先ファイル名を指定するコマンドを拒否します。
site	サーバー システムに固有のコマンドを禁止します。通常、リモート管理に使用します。
stou	固有のファイル名を使用してファイルを保存するコマンドを拒否します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 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

このコマンドは、ストリクト FTP インスペクションを使用する場合に、ASA 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

次に、**stor**、**stou**、または **appe** コマンドを含む FTP 要求を ASA でドロップする例を示します。

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

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 インスペクションに使用する特定の FTP マップを適用します。
mask-syst-reply	FTP サーバー応答をクライアントに対して非表示にします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

request-data-size

SLA 動作要求パケットのペイロードのサイズを設定するには、SLA モニター 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

構文の説明

bytes 要求パケットの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応じて異なります。エコー タイプでは、最小値は 28 バイトです。プロトコルまたは PMTU で許可されている最大値よりも大きい値を設定しないでください。

（注） ASA によって 8 バイトのタイムスタンプがペイロードに追加されるため、実際のペイロードは *bytes* + 8 バイトになります。

コマンド デフォルト

デフォルトの *bytes* は 28 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
SLA モニター プロトコル 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

到達可能性を確保するために、デフォルトのデータ サイズを大きくして、送信元と宛先との間の PMTU の変化を検出する必要がある場合があります。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可能性が高くなります。また、低い PMTU が検出された場合は、セカンダリ 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/応答時間プローブ動作を使用する、ID が 123 の SLA 動作を設定しています。この例では、エコー要求パケットのペイロード サイズを 48 バイト、SLA 動作中に送信されるエコー要求の数を 5 に設定しています。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

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

関連コマンド

コマンド	説明
num-packets	SLA 動作中に送信する要求パケットの数を指定します。
sla monitor	SLA モニタリング動作を定義します。
type echo	SLA動作をエコー応答時間プローブ動作として設定します。

request-queue

キューで応答待ちができる GTP 要求数の最大値を指定するには、ポリシー マップ パラメータ 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。この数字をデフォルトの 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*

構文の説明

max_requests 応答を待機する GTP 要求のキューイング可能最大数（1 ～ 4294967295）。

コマンド デフォルト

デフォルトは 200 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
7.0(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

request-queue コマンドは、応答を待機する GTP 要求のキューイング可能最大数を指定します。この上限に達した後に新しい要求が到着すると、最も長い時間キューに入っていた要求が削除されます。「Error Indication」、「Version Not Supported」および「SGSN Context Acknowledge」というメッセージは、要求と見なされないため、応答待ち要求のキューに入れられません。

例

次に、最大要求キュー サイズを 300 に指定する例を示します。

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# request-queue 300
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
inspect gtp	アプリケーションインスペクションに使用する特定の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（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

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 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。

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

構文の説明

seconds 失敗した SSO 認証の試行がタイムアウトするまでの秒数。指定できる範囲は 1 ～ 30 秒です。小数の値はサポートされていません。

コマンド デフォルト

このコマンドのデフォルト値は 5 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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。
9.5(2)	SAML 2.0 がサポートされたため、このコマンドは廃止されました。

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、ユーザーはユーザー名とパスワードを一度だけ入力すれば、別のサーバーでさまざまなセキュアなサービスにアクセスできます。現在、ASA では、SiteMinder-type および SAML POST-type の SSO サーバーがサポートされています。

このコマンドは SSO サーバーの両タイプに適用されます。

SSO 認証をサポートするように ASA を設定後、2 つのタイムアウトパラメータを調整できます。

- 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（**request-timeout** コマンドを使用）。
- ASA が失敗した SSO 認証を再試行する回数。（**max-retry-attempts command.)** を参照）。

例

次に、webvpn 設定 sso siteminder モードで、SiteMinder-type SSO サーバー「example」の認証タイムアウトを 10 秒に設定する例を示します。

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

関連コマンド

コマンド	説明
max-retry-attempts	SSO 認証に失敗した場合に ASA が再試行する回数を設定します。
policy-server-secret	SiteMinder SSO サーバーへの認証要求の暗号化に使用する秘密キーを作成します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバーの運用統計情報を表示します。
sso-server	シングル サインオン サーバーを作成します。
test sso-server	テスト認証要求で SSO サーバーをテストします。
web-agent-url	ASA が SiteMinder SSO 認証を要求する SSO サーバーの URL を指定します。

reserved-bits

TCPヘッダーの予約ビットをクリアしたり、予約ビットが設定されているパケットをドロップしたりするには、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** }

構文の説明

allow	TCP ヘッダーの予約ビットが設定されているパケットを許可します。
clear	TCP ヘッダーの予約ビットをクリアして、パケットを許可します。
drop	TCPヘッダーの予約ビットが設定されているパケットをドロップします。

コマンド デフォルト

デフォルトで、予約ビットは許可されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 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

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

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 モードを開始します。予約ビットが設定されているパケットの末端のホストにおける処理方法を明確に指定するには、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。処理方法が明確でないと、ASA が非同期の状態になる可能性があります。TCP ヘッダーの予約ビットをクリアしたり、予約ビットが設定されているパケットをドロップしたりできます。

例

次に、すべてのTCPフローにおいて、予約ビットが設定されているパケットをクリアする例を示します。

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

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	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、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。

reserve-port-protect

メディアネゴシエーション中の予約ポートの使用を制限するには、パラメータ コンフィギュレーション モードで **reserve-port-protect** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。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。

reserve-port-protect
no reserve-port-protect

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルト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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
8.0(2)	このコマンドが追加されました。

例

次に、RTSPインスペクション ポリシーマップで予約ポートを保護する例を示します。

```
ciscoasa(config)# policy-map type inspect rtsp rtsp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# reserve-port-protect
```

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。

コマンド	説明
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。

reset

モジュラ ポリシー フレームワークを使用する場合は、パケットをドロップし、接続を閉じ、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 TCP リセットを送信します。このリセットアクションは、インスペクション ポリシー マップ（**policy-map type inspect** コマンド）でアプリケーション トラフィックに対して使用できますが、すべてのアプリケーションでリセットアクションを使用でき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。

reset [**log**]
no reset [**log**]

構文の説明

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 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。

使用上のガイドライン

インスペクション 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。インスペクション ポリシー マップで使用できる実際のコマンドは、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 トラフィックを指定した後（**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、**match** コマンドまたは **class** コマンドに一致するトラフィックに対してパケットをドロップし、接続を閉じることができます。

接続をリセットした後は、インスペクション ポリシーマップ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** または **class** コマンドが一致することはありません。最初のアクションがパケットのログへの記録である場合、接続のリセットなどの2番目のアクションは実行されます同じ**match**コマンドまたは**class**コマンドに対して**reset** アクションと**log**アクションの両方を設定できます。その場合、パケットは特定の一致でリセットされる前にログに記録されます。

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 インスペクションをイネーブルにする場合、このアクションを含むインスペクション 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、インスペクション ポリシー マップの名前です。

例

次に、http-traffic クラス マップに一致した場合に、接続をリセットして、ログを送信する例を示します。同じパケットが 2 番めの **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。

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(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。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
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。

resolver

DNS 要求を解決する Cisco Umbrella DNS サーバーのアドレスを設定するには、Cisco Umbrella コンフィギュレーション モードで **resolver** 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。

resolver { **ipv4** | **ipv6** } *ip_address*
no resolver { **ipv4** | **ipv6** } *ip_address*

構文の説明

ipv4 *ip_address*	使用する Umbrella DNS サーバーの IPv4 アドレス。
ipv6 *ip_address*	使用する Umbrella DNS サーバーの IPv6 アドレス。

コマンド デフォルト

デフォルトの DNS リゾルバは 208.67.220.220 および 2620:119:53::53 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
Umbrella の設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.12(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

コマンドを2回入力して、IPv4アドレスとIPv6アドレスの両方を設定できます。有効なUmbrella DNS サーバーのみを指定できます。

例

次の例は、Cisco Umbrella のデフォルト以外の DNS リゾルバを定義しています。サーバーは 208.67.222.222 および 2620:119:35::35 です。

```
ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# resolver ipv4 208.67.222.222

ciscoasa(config-umbrella)# resolver ipv6 2620:119:35::35
```

関連コマンド

コマンド	説明
umbrella-global	Cisco Umbrella グローバルパラメータを設定します。

responder-only

VTI トンネルの一端をレスポンダとしてのみ動作するように設定するには、IPsec プロファイル コンフィギュレーション モードで responder-only コマンドを使用します。レスポンダ専用モードを削除するには、このコマンドの no 形式を使用します。

responder-only
no responder-only

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルト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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPsec プロファイル設定	• 対応	• ×	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(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して、VTI トンネルの一端がレスポンダとしてのみ動作するように設定できます。

レスポンダ専用の一端は、トンネルまたはキー再生成を開始しません。

このオプションは、コリジョン処理が使用できない場合、または IKEv1 を使用しているときにトンネルの両端が同時にトンネリングを開始する場合に便利です。レスポンダ専用の終端上の IKE トンネルまたは IPsec トンネルのキー再生成設定は、設定済みの場合もすべて無視されます。

例

次に、IPsec プロファイルにレスポンダ専用モードを追加する例を示します。

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# responder-only
```

関連コマンド

コマンド	説明
crypto ipsec profile	新しい IPsec プロファイルを作成します。
set ikev1 transform-set	IKEv1 変換セットを IPsec プロファイル設定に使用するように指定します。
set pfs	PFS グループを IPsec プロファイル設定に使用するように指定します。
set security-association lifetime	IPsec プロファイル設定でのセキュリティ アソシエーションの期間を指定します。これは、キロバイト単位か秒単位、またはその両方で指定します。
set trustpoint	VTI トンネル接続の開始時に使用する証明書を定義するトラストポイントを指定します。

rest-api

インストール済みのREST APIエージェントをフラッシュから有効にするには、**agent**キーワードを使用します。エージェントをディセーブルにするには、このコマンドのno形式を使用します。

このASAにREST APIパッケージをダウンロード（**copy** コマンドを使用）した後、パッケージを確認してインストールするには、imageキーワードを使用します。REST APIエージェントのバージョンとASAのバージョンが一致している必要があります。このパッケージをアンインストールするには、このコマンドのno形式を使用します。

rest-api［ **agent** | **image disk0 :** / *package* ］
no rest-api［ **agent** | **image disk0 :** / *package* ］

構文の説明

agent	インストール済みのREST APIエージェントをイネーブルにします。
image disk0:/*package*	*package* で指定したダウンロード済みのREST APIイメージをインストールします。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
REST APIエージェントのイネーブル化/ディセーブル化	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(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REST APIパッケージについて互換性と有効性のチェックを実行するには、**image**キーワードを指定してこのコマンドを発行します。パッケージがすべてのチェックにパスすると、内部フラッシュにインストールされます。

REST APIのコンフィギュレーションはスタートアップ コンフィギュレーション ファイルに保存されます。この構成をクリアするには、**clear configure** コマンドを使用します。

REST API パッケージをインストールまたは更新した後、ASA はリブートされません。

インストール済みの REST API エージェントを有効にするには、このコマンドを **agent** キーワードを指定して使用します。

例

次に、REST API パッケージを cisco.com からダウンロードしてインストールする例を示します。

```
ciscoasa(config)# copy tftp://10.7.0.80/asa-restapi-9.3.2-32.pkg  disk0:
ciscoasa(config)# rest-api image disk0:/asa-restapi-121-lfbff-k8.SPA
```

次に、実行中の REST API エージェントをディセーブルにして既存の REST API エージェントをアップグレードしてから、新しい REST API エージェントをダウンロードし、インストールして起動する例を示します。

```
ciscoasa(config)# no rest-api agent
ciscoasa(config)# copy tftp://10.7.0.80/asa-restapi-121-lfbff-k8.SPA disk0:
ciscoasa(config)# rest-api image disk0:/asa-restapi-121-lfbff-k8.SPA
ciscoasa(config)# rest-api agent
```

関連コマンド

コマンド	説明
copy	指定した REST API パッケージを TFTP サーバーから内部フラッシュ メモリにコピーします。
show rest-api agent	REST API エージェントが実行中かどうかを確認します。
clear configure	REST API のコンフィギュレーションを含む実行コンフィギュレーションをクリアします。

restore

ASAの構成、証明書、キー、およびイメージをバックアップファイルから復元するには、特権EXECモードで **restore** コマンドを使用します。

restore [**/noconfirm**] [**context** *ctx-name*] [**interface** *name*] [**cert-passphrase** *value*] [**location** *path*]

構文の説明

cert-passphrase *value*	VPNの証明書や事前共有キーを復元する際は、証明書を復号するために、**cert-passphrase** キーワードで秘密鍵を指定する必要があります。証明書の復号化に使用するパスフレーズをPKCS12形式で入力します。
context *ctx-name*	システム実行スペースからマルチコンテキストモードに入り、指定したコンテキストを復元する場合は、**context** キーワードを入力します。バックアップされた各コンテキストファイルは、個別に復元する必要があります。つまり、**restore** コマンドをファイルごとに再入力する必要があります。
interface *name*	（任意）バックアップをコピーするインターフェイスの名前を指定します。インターフェイスを指定しなかった場合、ASAは管理専用ルーティング テーブルを確認し、一致するものが見つからなければ、データのルーティング テーブルを確認します。
location *path*	復元先**location**として、ローカルディスクまたはリモートのURLを指定できます。locationを指定しない場合は、次のデフォルト名が使用されます。 • シングルモード：disk0:*hostname*.backup.*timestamp*.tar.gz • マルチモード：disk0:*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz
/noconfirm	**location** パラメータと **cert-passphrase** パラメータの入力を要求しないように指定します。警告およびエラーメッセージをバイパスしてバックアップを続行できるようにします。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
9.3(2)	このコマンドが追加されました。
9.5(1)	**interface** *name* 引数が追加されました。

使用上のガイドライン

次のガイドラインを参照してください。

- 復元を開始するには、復元先に少なくとも 300 MB の使用可能なディスク領域が必要です。
- バックアップ中またはバックアップ後にコンフィギュレーションを変更した場合、その変更内容はバックアップに含められません。バックアップの実行後にコンフィギュレーションを変更してから復元を実行した場合、このコンフィギュレーションの変更は上書きされます。結果として、ASA は異なる挙動をすることもあります。
- 復元は一度に 1 つしか開始できません。
- コンフィギュレーションは、元のバックアップを実行したときと同じ ASA バージョンにのみ復元できます。復元ツールを使用して、ASA の異なるバージョン間でコンフィギュレーションを移行することはできません。コンフィギュレーションの移行が必要な場合、ASA は、新しい ASA OS をロードした時に常駐するスタートアップ コンフィギュレーションを自動的にアップグレードします。
- クラスタリングを使用している場合、スタートアップ コンフィギュレーション、実行コンフィギュレーション、およびアイデンティティ証明書のみを復元できます。ユニットごとに別々にバックアップを作成および復元する必要があります。
- フェールオーバーを使用する場合、バックアップの作成および復元は、アクティブ ユニットとスタンバイ ユニットに対して別々に行う必要があります。
- ASA にマスター パスフレーズを設定している場合は、この手順で作成したバックアップ コンフィギュレーションの復元時にそのマスター パスフレーズが必要となります。ASA のマスターパスフレーズが不明な場合は、CLI コンフィギュレーション ガイドを参照して、バックアップを続行する前に、マスターパスフレーズをリセットする方法を確認してください。
- PKCS12 データをインポート（**crypto ca trustpoint** コマンドを使用）する際にトラストポイントが RSA キーを使用している場合、インポートされたキーペアにはトラストポイントと同じ名前が割り当てられます。この制約のため、ASDM コンフィギュレーションを復元した後でトラストポイントおよびそのキー ペアに別の名前を指定した場合、スタートアップ コンフィギュレーションは元のコンフィギュレーションと同じになるのに、実行コンフィギュレーションには異なるキー ペア名が含まれることになります。つまり、キーペアとトラストポイントに別の名前を使用した場合は、元のコンフィギュレーションを復元できないということです。この問題を回避するため、トラストポイントとそのキーペアには必ず同じ名前を使用してください。

- インターフェイスを指定しなかった場合、ASA は管理専用ルーティング テーブルを確認し、一致するものが見つからなければ、データのルーティングテーブルを確認します。管理専用インターフェイスを経由するデフォルトルートがある場合は、すべての**restore**トラフィックがそのルートに一致するため、データルーティングテーブルが確認されることはありません。このシナリオでは、データインターフェイスから復元する必要がある場合にそのインターフェイスを指定します。
- CLIを使用してバックアップしてからASDMを使用して復元したり、その逆を行うことはできません。
- 各バックアップ ファイルに含まれる内容は次のとおりです。
- 実行コンフィギュレーション
- スタートアップ コンフィギュレーション
- すべてのセキュリティ イメージ

Cisco Secure Desktop およびホスト スキャンのイメージ

Cisco Secure Desktop およびホスト スキャンの設定

AnyConnect（SVC）クライアントのイメージおよびプロファイル

AnyConnect（SVC）のカスタマイズおよびトランスフォーム

- アイデンティティ証明書（アイデンティティ証明書に関連付けられた RSA キー ペアは含まれるが、スタンドアロン キーは除外される）
- VPN 事前共有キー
- SSL VPN コンフィギュレーション
- アプリケーション プロファイルのカスタム フレームワーク（APCF）
- ブックマーク
- カスタマイゼーション
- ダイナミック アクセス ポリシー（DAP）
- プラグイン
- 接続プロファイル用の事前入力スクリプト
- プロキシ自動設定
- 変換テーブル
- Web コンテンツ
- バージョン情報

例

次に、バックアップを復元する例を示します。

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?
Copying Backup file to local disk... Done!
Extracting the backup file ... Done!
Warning: The ASA version of the device is not the same as the backup version, some
configurations might not work after restore!
 Do you want to continue? [confirm] y
Begin restore ...
IMPORTANT: This backup configuration uses master passphrase encryption. Master passphrase
 is required to restore running configuration, startup configuration and VPN pre-shared
 keys.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Restoring [Running Configuration]
Following messages are as a result of applying the backup running-configuration to this
 device, please note them for future reference.
ERROR: Interface description was set by failover and cannot be changed
ERROR: Unable to set this url, it has already been set
Remove the first instance before adding this one
INFO: No change to the stateful interface
Failed to update LU link information
.Range already exists.
WARNING: Advanced settings and commands should only be altered or used
under Cisco supervision.
ERROR: Failed to apply media termination address 198.0.1.228 to interface outside, the
IP is already used as media-termination address on interface outside.
ERROR: Failed to apply media termination address 198.0.0.223 to interface inside, the
IP is already used as media-termination address on interface inside.
WARNING: PAC settings will override http- and https-proxy configurations. Do not overwrite
 configuration file if you want to preserve the old http- and https-proxy configurations.
Cryptochecksum (changed): 98d23c2c ccb31dc3 e51acf88 19f04e28
 Done!
Restoring UC-IME ticket ... Done!
Enter the passphrase used while backup to encrypt identity certificates. The default is
 cisco. If the passphrase is not correct, certificates will not be restored.
No passphrase was provided for identity certificates. Using the default value: cisco.
If the passphrase is not correct, certificates will not be restored.
Restoring Certificates ...
Enter the PKCS12 data in base64 representation....
ERROR: A keypair named Main already exists.
INFO: Import PKCS12 operation completed successfully
. Done!
Cleaning up ... Done!
Restore finished!
```

関連コマンド

コマンド	説明
backup	ASA の構成、キー、証明書、およびイメージをバックアップファイルからバックアップします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。