po - pq

police

QoS ポリシングをクラスマップに適用するには、クラス コンフィギュレーション モードで **police** コマンドを使用します。レート制限を削除するには、このコマンドの **no** 形式を使用します。

police { **output** | **input** } *conform-rate* [*conform-burst*] [**conform-action** [**drop** | **transmit**] [**exceed-action** [**drop** | **transmit**]]]
no police

構文の説明

conform-rate	このトラフィッククラスのレート制限を 8000 ～ 2000000000 ビット/秒の範囲で設定します。ASA 仮想 および Firepower 4100/9300 の場合、範囲は 8000 ～ 100000000000 です。たとえば、トラフィックを 5 Mbps に制限するには、5000000 と入力します。
conform-burst	適合レート値にスロットリングするまでに、持続したバーストで許可された最大瞬間バイト数を 1000 ～ 512000000 バイトの範囲で指定します。ASA 仮想 および Firepower 4100/9300 の場合、範囲は 1000 ～ 25600000000 です。 このパラメータを省略した場合、デフォルト値は conform-rate のバイト数の 1/32 です（つまり、conform-rate が 100,000 の場合、conform-burst のデフォルト値は 100,000/32 = 3,125 です）。conform-rate の単位はビット/秒で、conform-burst の単位はバイト数です。
conform-action [**drop** | **transmit**]	トラフィックがポリシングレートとバーストサイズを下回った場合に実行するアクションを設定します。トラフィックを **drop** または **transmit** できます。デフォルトでは、トラフィックは送信されます。
exceed-action [**drop** | **transmit**]	トラフィックがポリシングレートとバーストサイズを上回った場合に実行するアクションを設定します。ポリシングレートとバーストサイズを上回ったパケットを **drop** または **transmit** できます。デフォルトでは、超過パケットはドロップされます。
input	入力方向のトラフィック フローのポリシングをイネーブルにします。
output	出力方向のトラフィック フローのポリシングをイネーブルにします。

コマンド デフォルト

デフォルトの動作や変数はありません。

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 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。
7.2(1)	**input** オプションが追加されました。着信方向のトラフィックのポリシングがサポートされます。

使用上のガイドライン

ポリシングは、設定した最大レート（ビット/秒単位）を超えるトラフィックが発生しないようにして、1つのトラフィック フローが全体のリソースを占有しないようにする方法です。トラフィックが最大レートを超えると、ASAは超過した分のトラフィックをドロップします。また、ポリシングでは、許可されるトラフィックの最大単一バーストも設定されます。

ポリシングをイネーブルにするには、Modular Policy Framework を使用して次のように設定します。

1.class-map：ポリシングを実行するトラフィックを指定します。

2.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.police**：クラスマップのポリシングを有効にします。

3.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。

ASA で必要な場合は、個々の QoS 機能を単独で設定できます。ただし、普通は、たとえば一部のトラフィックを優先させて、他のトラフィックによって帯域幅の問題が発生しないようにするために、複数の QoS 機能を ASA に設定します。

次に、インターフェイスごとにサポートされる機能の組み合わせを示します。

- 標準プライオリティキューイング（特定のトラフィックの場合）+ ポリシング（その他のトラフィックの場合）

同じトラフィックのセットに対して、プライオリティキューイングとポリシングを両方設定することはできません。

- トラフィックシェーピング（1 つのインターフェイス上のすべてのトラフィックの場合）+ 階層型プライオリティキューイング（トラフィックのサブセットの場合）。

通常、トラフィックシェーピングをイネーブルにした場合、同じトラフィックに対してはポリシングをイネーブルにしません。ただし、このような設定は ASA では制限されていません。

次のガイドラインを参照してください。

- QoS は単方向に適用されます。ポリシーマップを適用するインターフェイスに出入りする（**input** または **output** を指定したかによって異なる）トラフィックだけが影響を受けます。
- 確立済みのトラフィックが存在するインターフェイスに対して、サービス ポリシーが適用または削除されると、トラフィック ストリームに対して QoS ポリシーは適用または削除されません。そのような接続の QoS ポリシーを適用または削除するには、接続をクリアして再確立する必要があります。**clear conn** コマンドを参照してください。
- to-the-box トラフィックはサポートされません。
- VPN トンネル バイパス インターフェイスとの間のトラフィックはサポートされません。
- トンネル グループ クラス マップを照合する場合、出力ポリシングのみがサポートされます。

例

次に、出力方向の **police** コマンドの例を示します。このコマンドは、適合レートを 100,000 ビット/秒、バースト値を 20,000 バイトに設定します。

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class-map firstclass
ciscoasa(config-cmap)# class localclass

ciscoasa(config-pmap-c)# police output 100000 20000
ciscoasa(config-cmap-c)# class class-default
ciscoasa(config-pmap-c)#
```

次に、内部 Web サーバーを宛先とするトラフィックにレート制限を実行する例を示します。

```
ciscoasa# access-list http_traffic permit tcp any 10.1.1.0 255.255.255.0 eq 80
ciscoasa# class-map http_traffic
ciscoasa(config-cmap)# match access-list http_traffic
ciscoasa(config-cmap)# policy-map outside_policy
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# police input 56000
ciscoasa(config-pmap-c)# service-policy outside_policy interface outside
ciscoasa(config)#
```

関連コマンド

class	トラフィックの分類に使用するクラス マップを指定します。
clear configure policy-map	すべてのポリシーマップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。
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。

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。

policy

CRL の取得元を指定するには、ca-crl コンフィギュレーション モードで **policy** コマンドを使用します。

policy { **static** | **cdp** | **both** }

構文の説明

both	CRL 配布ポイントを使用した CRL の取得に失敗した場合は、スタティック CDP を最大 5 つ使用して再試行します。
cdp	チェック対象の証明書内に埋め込まれている CDP 拡張を使用します。この場合、ASA は検証対象の証明書の CDP 拡張から最大 5 つの CRL 配布ポイントを取得します。さらに必要に応じて、設定されたデフォルト値を使用して情報を増強します。ASA がプライマリ CDP を使用して CRL を取得するのに失敗した場合は、リストで次に使用可能な CDP を使用して再試行します。再試行は、ASA が CRL を取得するかリストの最後に到達するまで、繰り返されます。
static	最大で 5 つのスタティック CRL 配布ポイントを使用します。このオプションを指定する場合は、**protocol** コマンドを使用して LDAP または HTTP URL も指定します。

コマンド デフォルト

デフォルト設定は**cdp**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
CRL 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。

例

次に、ca-crl コンフィギュレーション モードを開始し、チェック対象の証明書内にある CRL 配布ポイント拡張を使用して CRL 取得を行うように設定し、失敗した場合はスタティック CDP を使用する例を示します。

```
ciscoasa(configure)# crypto ca trustpoint central
```

```
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# policy both
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
url	CRL 取得用のスタティック URL のリストを作成および維持します。

policy-list

ボーダー ゲートウェイ プロトコル（BGP）のポリシーリストを作成するには、ポリシー マップ コンフィギュレーション モードで **policy-list** コマンドを使用します。ポリシーリストを削除するには、このコマンドの **no** 形式を使用します。

policy-list *policy-list-name* { **permit** | **deny** }
no policy-list *policy-list-name*

構文の説明

policy-list-name	設定するポリシー リストの名前。
permit	条件に一致した場合にアクセスを許可します。
deny	条件に一致した場合にアクセスを拒否します。

コマンド 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。

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
グローバル設定	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

ルート マップ内でポリシー リストが参照されると、ポリシー リスト内の match 文すべてが評価され、処理される。1 つのルート マップに 2 つ以上のポリシー リストを設定できる。1 つのルート マップ内で設定された複数のポリシー リストは、AND セマンティクスまたは OR セマンティクスを使用して評価されます。ポリシー リストは、同じルート マップ内にあるがポリシー リストの外で設定されている他の既存の match および set 文とも共存できます。1 つのルート マップ エントリ内で複数のポリシー リストが照合を行う場合、ポリシー リストすべては受信属性だけで照合を行います。

policy-list のサブコマンドを次に示します。

サブコマンド	Details
match as-path [path-list-number]	AS パスを照合します。AS パスのパス リスト番号を複数指定できます。
Match community[community-name][exact-match]	コミュニティ名は必須で、完全一致は任意です。複数の名前を指定できます。
Match interface [interface-name]	複数のインターフェイス名を指定できます。
match metric <0-4294967295>	複数の番号を指定できます。
Match ip address [acl name prefix-list [prefix-listname]]	ACL またはプレフィックス リストの名前を複数指定できます。ただし、1 つのポリシー リストにプレフィックスリストと ACL の両方を含めることはできず、どちらか一方しか指定できません。
Match ip next-hop [acl name | prefix-list [prefix-listname]]	ACL またはプレフィックス リストの名前を複数指定できます。ただし、1 つのポリシー リストにプレフィックスリストと ACL の両方を含めることはできず、どちらか一方しか指定できません。
Match ip route-source [acl name | prefix-list [prefix-listname]]	ACL またはプレフィックス リストの名前を複数指定できます。ただし、1 つのポリシー リストにプレフィックスリストと ACL の両方を含めることはできず、どちらか一方しか指定できません。
Default match	上記のすべての「照合」オプションをデフォルトに設定します。
Help	後続のコマンドのヘルプを表示します。
なし	コマンドの否定です。
終了	ポリシー マップ モードを終了します。

例

次に、AS が 1 でメトリックが 10 のネットワーク プレフィックスをすべて許可するポリシーリストの設定例を示します。

```
ciscoasa(config)#  policy-list POLICY-LIST-NAME-1 permit
ciscoasa(config-policy-list)# match as-path 1
ciscoasa(config-policy-list)# match metric 10
ciscoasa(config-policy-list)# end
```

次に、コミュニティが 20 でメトリックが 10 のトラフィックを許可するポリシー リストの設定例を示します。

```
ciscoasa(config)#  policy-list POLICY-LIST-NAME-2 permit
ciscoasa(config-policy-list)# match community 20
```

```
ciscoasa(config-policy-list)# match metric 10
ciscoasa(config-policy-list)# end
```

次に、コミュニティが 20 でメトリックが 10 のトラフィックを拒否するポリシー リストの設定例を示します。

```
ciscoasa(config)#  policy-list POLICY-LIST-NAME-3 deny
ciscoasa(config-policy-list)# match community 20
ciscoasa(config-policy-list)# match metric 10
```

policy-map

モジュラ ポリシー フレームワークを使用する場合、グローバル コンフィギュレーション モードで**policy-map** コマンド（**type**キーワードなし）を使用し、レイヤ3/4クラスマップ（**class-map** または **class-map type management** コマンド）で特定したトラフィックにアクションを割り当てます。レイヤ 3/4 ポリシー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。

policy-map*name*
no policy-map *name*

構文の説明

name	このポリシー マップの名前を最大 40 文字で指定します。すべてのタイプのポリシー マップで同じ名前スペースが使用されるため、別のタイプのポリシーマップですでに使用されている名前は再度使用できません。

コマンド デフォルト

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するポリシーがコンフィギュレーションに含まれ、特定のインスペクションがすべてのインターフェイスのトラフィックに適用されます（グローバル ポリシー）。すべてのインスペクションがデフォルトでイネーブルになっているわけではありません。適用できるグローバル ポリシーは1つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。（特定の機能では、グローバル ポリシーはインターフェイス ポリシーより優先されます）。

デフォルト ポリシーには、次のアプリケーション インスペクションが含まれます。

- DNS
- FTP
- H323（H225）
- H323（RAS）
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny（SCCP）
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP

• IP オプション

デフォルト ポリシー コンフィギュレーションには、次のコマンドが含まれます。

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
message-length maximum client auto
message-length maximum 512
dns-guard
protocol-enforcement
nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225 _default_h323_map
  inspect h323 ras _default_h323_map
  inspect ip-options _default_ip_options_map
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp _default_esmtp_map
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
```

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
グローバル設定	• 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

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. class-map コマンドまたは **class-map type management** コマンドを使用して、アクションを適用するレイヤ 3 およびレイヤ 4 のトラフィックを指定します。

2. （アプリケーション インスペクションのみ）**policy-map type 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 トラフィックの特別なアクションを定義します。

3.policy-map コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。

4.service-policy コマンドを使用して、インターフェイスでのアクションをアクティブにします。

ポリシー マップの最大数は 64 ですが、各インターフェイスには、ポリシー マップを 1 つだけ適用できます。同一のポリシー マップを複数のインターフェイスに適用できます。レイヤ 3/4 ポリシーマップ内にある複数のレイヤ 3/4 クラスマップを特定でき（**class** コマンドを参照）、1 つ以上の機能タイプの複数のアクションを各クラスマップに割り当てることができます。

例

次に、接続ポリシーの **policy-map** コマンドの例を示します。このコマンドは、Web サーバー 10.1.1.1 への接続許可数を制限します。

```
ciscoasa(config)# access-list http-server permit tcp any host 10.1.1.1
ciscoasa(config)# class-map http-server
ciscoasa(config-cmap)# match access-list http-server
ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# description This policy map defines a policy concerning connection
 to http server.
ciscoasa(config-pmap)# class http-server
ciscoasa(config-pmap-c)# set connection conn-max 256
```

次の例は、ポリシー マップでの複数の照合の動作を示しています。

```
ciscoasa(config)# class-map inspection_default
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80
ciscoasa(config)# policy-map outside_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect http http_map
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:10:0
```

次の例は、トラフィックが最初の利用可能なクラスマップと一致した場合に、同じ機能ドメインのアクションが指定されている後続のクラスマップと照合されないことを示しています。

```
ciscoasa(config)# class-map telnet_traffic
ciscoasa(config-cmap)# match port tcp eq 23
ciscoasa(config)# class-map ftp_traffic
ciscoasa(config-cmap)# match port tcp eq 21
ciscoasa(config)# class-map tcp_traffic
ciscoasa(config-cmap)# match port tcp range 1 65535
ciscoasa(config)# class-map udp_traffic
ciscoasa(config-cmap)# match port udp range 0 65535
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class telnet_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:0:0
ciscoasa(config-pmap-c)# set connection conn-max 100
ciscoasa(config-pmap)# class ftp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:5:0
ciscoasa(config-pmap-c)# set connection conn-max 50
ciscoasa(config-pmap)# class tcp_traffic
```

```
ciscoasa(config-pmap-c)# set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)# set connection conn-max 2000
```

Telnet 接続は、開始時に **class telnet_traffic** と一致します。同様に FTP 接続は、開始時に **class ftp_traffic** と一致します。Telnet および FTP 以外の TCP 接続の場合は、**class tcp_traffic** と一致します。Telnet 接続または FTP 接続は **class tcp_traffic** と一致しますが、すでに他のクラスと一致しているため、ASA はこの照合を行いません。

NetFlow イベントは、Modular Policy Framework を使用して設定されます。Modular Policy Framework が NetFlow 用に設定されていない場合、イベントはログに記録されません。トラフィックはクラスが設定される順序に基づいて照合されます。一致が検出されると、その他のクラスはチェックされません。NetFlow イベントの場合、コンフィギュレーションの要件は次のとおりです。

- flow-export destination（NetFlow コレクタ）は、その IP アドレスによって一意に識別されます。
- サポートされるイベント タイプは、flow-create、flow-teardown、flow-denied、および all です（前述の 4 つのイベント タイプを含みます）。
- 各コレクタに送信する NetFlow レコードを決定するために NetFlow コレクタおよびフィルタのアドレスを設定するには、**flow-export event-type** {**all** | **flow-create** | **flow-denied** | **flow-update** | **flow-teardown**} **destination** コマンドを使用します。
- flow-export アクションは、インターフェイス ポリシーでサポートされません。
- flow-export アクションがサポートされるのは、**class-default** コマンド、および **match any** コマンドまたは **match access-list** コマンドで使用されるクラスに限られます。
- NetFlow コレクタが定義されていない場合は、コンフィギュレーション アクションは発生しません。
- NetFlow セキュア イベント ロギングのフィルタリングは、順序に関係なく実行されます。

次に、ホスト 10.1.1.1 と 20.1.1.1 の間のすべての NetFlow イベントを送信先 15.1.1.1 にエクスポートする例を示します。

```
ciscoasa(config)# access-list
 flow_export_acl
 permit ip host 10.1.1.1 host 20.1.1.1
ciscoasa(config)# class-map flow_export_classciscoasa(config-cmap)# match access-list
flow_export_aclciscoasa(config)# policy-map global_policyciscoasa(config-pmap)# class
flow_export_classciscoasa(config-pmap-c)# flow-export event-type all destination
15.1.1.1
```

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
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ポリシーマップが **service-policy** コマンドで使用されている場合、そのポリシーマップは削除されません。
class-map	トラフィック クラス マップを定義します。
service-policy	ポリシー マップをインターフェイスに割り当てるか、またはすべてのインターフェイスにグローバルに割り当てます。
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。

policy-map type inspect

モジュラ ポリシー フレームワークを使用する場合、グローバル コンフィギュレーション モードで **policy-map type inspect** コマンドを使用して、アプリケーション トラフィック検査のための特別なアクションを定義します。インスペクション ポリシー 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。

policy-map type inspect *application policy_map_name*
no policy-map［ **type inspect** *application* ］*policy_map_name*

構文の説明

application	対象とするアプリケーション トラフィックのタイプを指定します。利用可能なタイプは次のとおりです。 • **dcerpc** • **diameter** • **dns** • **esmtp** • **ftp** • **gtp** • **h323** • **http** • **im** • **ip-options** • **ipsec-pass-thru** • **ipv6** • **lisp** • **m3ua** • **mgcp** • **netbios** • **radius-accounting** • **rtsp** • **scansafe** • **sctp** • **sip** • **skinny** • **snmp**
policy_map_name	このポリシー マップの名前を最大 40 文字で指定します。「_internal」または「_default」で始まる名前は予約されており、使用できません。すべてのタイプのポリシー マップで同じ名前スペースが使用されるため、別のタイプのポリシー マップですでに使用されている名前は再度使用できません。

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
グローバル設定	• 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。
8.2(1)	IPv6 インスペクションをサポートするために **ipv6** キーワードが追加されました。
9.0(1)	クラウド Web セキュリティをサポートするために **scansafe** キーワードが追加されました。
9.5(2)	LISP インスペクションをサポートするために **lisp** キーワードが追加されました。
9.5(2)	**diameter** および **sctp** キーワードが追加されました。
9.6(2)	**m3ua** キーワードが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークでは、多くのアプリケーション インスペクションで実行される特別なアクションを設定できます。レイヤ 3/4 のポリシーマップ（**policy-map** コマンド）で、**inspect** コマンドを使用して検査エンジンを有効にする場合は、**policy-map type inspect** コマンドで作成されたインスペクション ポリシーマップで定義されているアクションもオプションで有効にできます。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。

インスペクション ポリシーマップは、ポリシーマップ コンフィギュレーション モードで入力するコマンドのうち、次の 1 つ以上の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：**match** コマンドをインスペクション ポリシー マップで直接定義して、アプリケーション固有の基準（URL ストリングなど）とアプリケーション トラフィックを照合できます。次に、一致コンフィギュレーション モードで **drop**、**reset**、**log** などのアクションを有効にします。**match** コマンドを使用できるかどうかは、アプリケーションによって異なります。
- **class** コマンド：このコマンドは、ポリシーマップ内のインスペクション クラス マップを特定します（インスペクション クラス マップの作成については、**class-map type inspect** コマンドを参照してください）。インスペクション クラス マップには、**match** コマンドが含まれます。このコマンドは、ポリシーマップ内のアクションを有効にするアプリケーション固有の基準（URL ストリングなど）とアプリケーション トラフィックを照合します。クラスマップを作成することと、インスペクション ポリシー マップ内で **match** コマ

ンドを直接使用することの違いは、複数の照合結果をグループ化できることと、クラスマップを再使用できることです。

- **parameters** コマンド：パラメータは検査エンジンの動作に影響します。パラメータ コンフィギュレーションモードで使用できるコマンドは、アプリケーションによって異なります。

ポリシーマップでは、複数の **class** または **match** コマンドを指定できます。

一部の **match** コマンドでは、パケット内のテキストと照合する正規表現を指定できます。**regex** コマンドおよび **class-map type regex** コマンド（複数の正規表現をグループ化）を参照してください。

デフォルトのインスペクション ポリシー マップ コンフィギュレーションには、次のコマンドが含まれます。

```
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 message-length maximum 512
 dns-guard
 protocol-enforcement
 nat-rewrite
```

1 つのパケットが複数の異なる **match** コマンドまたは **class** コマンドと一致する場合、ASA のアクション適用順序は、ポリシーマップにアクションが追加された順序ではなく、ASA の内部ルールによって決まります。内部ルールは、アプリケーションのタイプとパケット解析の論理的進捗によって決まり、ユーザーが設定することはできません。HTTP トラフィックの場合、Request Method フィールドの解析が Header Host Length フィールドの解析よりも先に行われ、Request Method フィールドに対するアクションは Header Host Length フィールドに対するアクションより先に行われます。たとえば、次の match コマンドは任意の順序で入力できますが、**match request method get** コマンドが最初に照合されます。

```
ciscoasa(config-pmap)# match request header host length gt 100
ciscoasa(config-pmap-c)# reset
ciscoasa(config-pmap-c)# match request method get
ciscoasa(config-pmap-c)# log
```

アクションがパケットをドロップすると、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** コマンドに対して **reset**（**drop-connection** など）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）。

パケットは、同じ複数の **match** または **class** コマンドと照合される場合、ポリシーマップ内の各コマンドの順序に従って照合されます。たとえば、ヘッダーの長さが 1001 のパケットの場合は、次に示す最初のコマンドと照合されてログに記録され、それから 2 番目のコマンドと照合されてリセットされます。2 つの **match** コマンドの順序を逆にすると、2 番目の **match** コマンドとの照合前にパケットのドロップと接続のリセットが実行され、ログには記録されません。

```
ciscoasa(config-pmap)# match request header length gt 100
ciscoasa(config-pmap-c)# log
ciscoasa(config-pmap-c)# match request header length gt 1000
ciscoasa(config-pmap-c)# reset
```

クラスマップは、そのクラスマップ内で優先順位が最低の**match**コマンドに基づいて、別のクラスマップまたは**match**コマンドと同じタイプであると判断されます（優先順位は内部ルールに基づいています）。クラスマップに、別のクラスマップと同じタイプの優先順位が最低の**match**コマンドがある場合、そのクラスマップはポリシーマップに追加された順序で照合されます。クラスマップごとに優先順位が最低のコマンドが異なる場合は、優先順位が最高の**match**コマンドを持つクラスマップが最初に照合されます。

使用中のインスペクション ポリシー マップを別のマップ名と交換する場合は、**inspect** *protocol map* コマンドを削除し、新しいマップを使用して再度入力する必要があります。次に例を示します。

```
ciscoasa(config)# policy-map test
ciscoasa(config-pmap)# class sip
ciscoasa(config-pmap-c)# no
 inspect sip sip-map1
ciscoasa(config-pmap-c)# inspect sip sip-map2
```

例

次の例では、HTTP インスペクション ポリシー マップとその関連クラス マップを示します。このポリシー マップは、サービス ポリシーがイネーブルにするレイヤ 3/4 ポリシー マップによってアクティブになります。

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
ciscoasa(config)# class-map type regex match-any URLs
ciscoasa(config-cmap)# match
 regex
 example
ciscoasa(config-cmap)# match
 regex
 example2
ciscoasa(config-cmap)# class-map type inspect http match-all http-traffic
ciscoasa(config-cmap)# match req-resp content-type mismatch
ciscoasa(config-cmap)# match request body length gt 1000
ciscoasa(config-cmap)# match not request uri regex class URLs
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop-connection log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# protocol-violation action log
ciscoasa(config-pmap-p)# policy-map test
ciscoasa(config-pmap)# class test
(a Layer 3/4 class map not shown)
ciscoasa(config-pmap-c)# inspect http http-map1
ciscoasa(config-pmap-c)# service-policy inbound_policy interface outside
```

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。
parameters	インスペクション ポリシー マップのパラメータ コンフィギュレーション モードを開始します。
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。

policy-route

インターフェイスでポリシーベースルーティングを設定するには、インターフェイス コンフィギュレーション モードで **policy-route** コマンドを使用します。

policy-route { **route-map** *route_map_name* | **cost** *value* | **path-monitoring** { **IPv4** | **IPv6** | **auto** | **auto4** | **auto6** }
no policy-route { **route-map** *route_map_name* | **cost** *value* | **path-monitoring** { **IPv4** | **IPv6** | **auto** | **auto4** | **auto6** }

構文の説明

cost *value*	ポリシーベースルーティング評価のインターフェイスの相対コストを設定します。値は 1 ー 65535 です。デフォルトは 0 です。この値は、コマンドの **no** バージョンを使用してリセットできます。値が小さいほど、プライオリティが高くなります。たとえば、1 は 2 よりも優先されます。
route-map*route_map_name*	ポリシーベースルーティングに使用するルートマップの名前を指定します。
path-monitoring	インターフェイスのピアのモニタリングタイプを設定して、フレキシブルメトリックを収集します。

コマンド デフォルト

デフォルトのルートマップはありません。デフォルトのコストは 0 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
インターフェイス 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
9.4(1)	このコマンドが追加されました。
9.17(1)	**cost** キーワードが追加されました。
9.18(1)	このコマンドは、トラフィックをルーティングするための最適なパスを決定する PBR のパスモニタリング機能を含めるように拡張されました。

使用上のガイドライン

一致基準とすべての match 句を満たす場合のアクションを指定するルートマップを設定したら、**policy-route route-map** コマンドを使用して、特定のインターフェイスに適用します。

ルートマップの基準として **set adaptive-interface cost** を使用する場合は、**policy-route cost** コマンドを使用して、インターフェイスのコストを設定します。

policy-route コストを設定し、ルートマップで **set adaptive-interface cost** コマンドを使用すると、出力トラフィックは、同じインターフェイスコストを持つ任意の選択されたインターフェイス間（アップしていると仮定）でラウンドロビン ロード バランシングされます。コストが異なる場合、コストの高いインターフェイスが、最もコストの低いインターフェイスへのバックアップとして使用されます。

たとえば、2 つの WAN リンクに同じコストを設定すると、これらのリンク間でトラフィックをロードバランシングして、パフォーマンスを向上させることができます。ただし、一方の WAN リンクの帯域幅が他方よりも高い場合は、高帯域幅リンクのコストを 1 に設定し、低帯域幅リンクを2に設定して、高帯域幅リンクがダウンしている場合にのみ低帯域幅リンクを使用します。

例

次に、ポリシーベースルーティングのインターフェイスにルートマップを適用する例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map testmapv4
ciscoasa(config)# show run interface GigabitEthernet0/0
!
interface GigabitEthernet0/0
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  policy-route route-map testmapv4
!
ciscoasa(config)# show route-map testmapv4
route-map testmapv4, permit, sequence 10
   Match clauses:
       ip address (access-lists): testaclv4
   Set clauses:
               ip next-hop 1.1.1.1
```

次に、不等コストを設定する例、つまり、output1 が優先リンクで、output2 は output1 がダウンしている場合にのみ使用される例を示します。インターフェイス間でロードバランシングを設定するには、等コスト値を設定します。

```
interface G0/0
  nameif outside1
  policy-route cost 1

interface G0/1
  nameif outside2
  policy-route cost 2
```

パスモニタリング機能は、トラフィックを転送しなくなったルートリンクまたはパスの障害を検出します。脅威防御が RTT、ジッター、パケット損失、平均オピニオン評点（MOS）などの評価指標を収集して、トラフィックを転送するためのベストパスを決定できるようにします。

パスモニタリングを設定するには、**policy-route** コマンドを使用します。ピアゲートウェイから評価指標を収集するためにデバイスが使用する必要があるモニタリングタイプを指定する必要があります。自動オプションの場合、モニタリングのために、デフォルトルートのネクストホップがピアとして使用されます。IPv4が最初に試行され、次に IPv6 が試行されます。VTI インターフェイスの場合、auto オプションはサポートされていません。ピアの IPv4 または IPv6 アドレスを指定する必要があります。

```
ciscoasa(config-if)# policy-route ?

interface mode commands/options:
  cost             set interface cost
  path-monitoring  Keyword for path monitoring
  route-map        Keyword for route-map
ciscoasa(config-if)# policy-route path-monitoring ?
interface mode commands/options:
  A.B.C.D     peer-ipv4
  X:X:X:X::X  peer-ipv6
  auto        Use remote peer IPv4/6 based on config
  auto4       Use only IPv4 address based on config
  auto6       Use only IPv6 address based on config

ciscoasa(config-if)# policy-route path-monitoring auto
```

policy-server-secret（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。

SiteMinder SSO サーバーへの認証要求を暗号化するために使用する秘密鍵を設定するには、webvpn sso siteminder コンフィギュレーション モードで **policy-server-secret** コマンドを使用します。秘密鍵を削除するには、このコマンドの **no** 形式を使用します。

policy-server-secret *secret-key*
no policy-server-secret

（注） このコマンドは、SiteMinder SSO 認証で必要です。

構文の説明

secret-key 認証通信を暗号化するために秘密キーとして使用されるストリング。文字の最小数や最大数の制限はありません。

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
config-webvpn-sso-siteminder 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。まず **sso-server** コマンドを使用して SSO サーバーを作成します。SiteMinder

SSO サーバーの場合、**policy-server-secret** コマンドを使用して ASA と SSO サーバー間の認証通信を保護します。

コマンド引数 *secret-key* は、パスワードと同様に作成、保存、および設定が可能です。このコマンド引数は、**policy-server-secret** コマンドを使用して ASA で設定され、Cisco Java プラグイン認証スキームを使用して SiteMinder Policy Server で設定されます。

このコマンドは、SiteMinder-type の SSO サーバーにのみ適用されます。

例

次に、config-webvpn-sso-siteminder モードで、引数としてランダムなストリングを使用して、SiteMinder SSO サーバー認証通信の秘密キーを作成する例を示します。

```
ciscoasa(config-webvpn)# sso-server my-sso-server type siteminder
ciscoasa(config-webvpn-sso-siteminder)# policy-server-secret @#ET&
ciscoasa(config-webvpn-sso-siteminder)#
```

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。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
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。

policy static sgt

手動で設定した Cisco TrustSec リンクにポリシーを適用するには、CTS 手動インターフェイス コンフィギュレーション モードで **policy static sgt** コマンドを使用します。手動で設定した CTS リンクに対するポリシーを削除するには、このコマンドの **no** 形式を使用します。

policy static sgt *sgt_number*［ **trusted** ］
no policy static sgt *sgt_number*［ **trusted** ］

構文の説明

sgt *sgt_number*	ピアからの着信トラフィックに適用する SGT 番号を指定します。有効な値の範囲は 2 ～ 65519 です。
static	リンクの着信トラフィックに SGT ポリシーを指定します。
trusted	コマンドで SGT が指定されたインターフェイスの入力トラフィックでは、SGT を上書きしてはいけないことを示します。デフォルトは untrusted 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
CTS 手動インターフェイス 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
9.3(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

このコマンドでは、手動で設定した CTS リンクにポリシーを適用します。

制約事項

- 物理インターフェイス、VLAN インターフェイス、ポート チャネル インターフェイスおよび冗長インターフェイスでのみサポートされます。
- BVI、TVI、VNI などの論理インターフェイスや仮想インターフェイスではサポートされません。

例

次に、レイヤ2SGTインポジション用のインターフェイスをイネーブルにし、インターフェイスが信頼できるかどうかを定義する例を示します。

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual

ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

関連コマンド

コマンド	説明
cts manual	レイヤ 2 SGT インポジションをイネーブルにし、CTS 手動インターフェイス コンフィギュレーション モードを開始します。
propagate sgt	インターフェイスでセキュリティグループタグ（**sgt** と呼ばれる）を伝播します。伝搬はデフォルトでイネーブルになっています。

polltime interface

Active/Active フェールオーバー コンフィギュレーションのデータインターフェイス polltime および holdtime を指定するには、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 **polltime interface** 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。

polltime interface ［ **msec** ］ *polltime* ［ **holdtime** *time* ］
no polltime interface ［ **msec** ］ *polltime* ［ **holdtime** *time* ］

構文の説明

holdtime 時刻	（任意）ピア ユニットからの最後に受信した hello メッセージとインターフェイス テストの開始との間の時間（計算として）を設定して、インターフェイスの健全性を判断します。また、各インターフェイステストの期間を *holdtime*/16 として設定します。有効な値は 5 ～ 75 秒です。デフォルトは、*polltime* の 5 倍です。*polltime* の 5 倍よりも短い holdtime 値は入力できません。 インターフェイス テストを開始するまでの時間（y）を計算するには、次のようにします。 **1.** x = (*holdtime* /*polltime)/2*、最も近い整数に丸められます。（.4 以下は切り下げ、.5 以上は切り上げ。） **2.** y = x**polltime* たとえば、デフォルトの holdtime は 25 で、polltime が 5 の場合は y は 15 秒です。
interface *time*	hello パケットをピアに送信するまで待機する時間を指定します。有効な値の範囲は、1 ～ 15 秒です。デフォルトは 5 分です。オプションの **msec** キーワードを使用した場合、有効な値は 500 ～ 999 ミリ秒です。
msec	（任意）指定する時間がミリ秒単位であることを指定します。

コマンド デフォルト

ポーリングの *time* は 5 秒です。

holdtime *time* は、ポーリングの *time* の 5 倍です。

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
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。
7.2(1)	このコマンドは、任意の **holdtime** *time* 値とポーリング時間をミリ秒で指定する機能を含めるように変更されました。

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。Active/Standby フェールオーバー コンフィギュレーションで **failover polltime interface** コマンドを使用します。

ポーリング時間を短縮すると、ASA で障害を検出し、フェールオーバーをトリガーする速度が速くなります。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。

構成に **polltime unit** コマンドおよび **polltime interface** コマンドの両方を含めることができます。

（注） フェールオーバー設定で、CTIQBE トラフィックが ASA を通過する場合は、ASA のフェールオーバーホールド時間を 30 秒未満にする必要があります。CTIQBE キープアライブ タイムアウトは 30 秒であるため、フェールオーバーの状況ではフェールオーバーが発生する前にタイムアウトする可能性があります。CTIQBE がタイムアウトした場合、Cisco CallManager への Cisco IP SoftPhone の接続はドロップされ、IP SoftPhone クライアントは CallManager に再登録する必要があります。

例

次の部分的な例では、フェールオーバー グループで可能な設定を示します。フェールオーバー グループ 1 のデータ インターフェイスのインターフェイス ポーリング時間を 500 ミリ秒に設定し、保持時間を 5 秒に設定します。

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

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 polltime	装置のフェールオーバー ポーリング期間とホールドタイムを指定します。

コマンド	説明
failover polltime interface	Active/Standby フェールオーバー コンフィギュレーションのインターフェイス ポーリング期間およびホールド タイムを指定します。

poll-timer

ネットワーク オブジェクト グループで定義された完全修飾ドメイン名（FQDN）を解決するために、ASA が DNS サーバーにクエリする期間のタイマーを指定するには、DNS サーバー グループ グローバル コンフィギュレーション モードで **poll-timer** コマンドを使用します（DefaultDNS サーバーグループの場合のみ）。タイマーを削除するには、このコマンドの **no** 形式を使用します。

poll-timer minutes *minutes*
no poll-timer minutes *minutes*

構文の説明

minutes *minutes*	タイマーを分単位で指定します。有効な値は、1 ～ 65535 分です。

コマンド デフォルト

デフォルトでは、DNS タイマーは 240 分または 4 時間です。

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
DNS サーバーグループ 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
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、DefaultDNS サーバーグループでのみサポートされます。

このコマンドは、ネットワーク オブジェクト グループで定義された FQDN を解決するために、ASA が DNS サーバーに照会する期間のタイマーを指定します。FQDN は、DNS ポーリング タイマーの期限切れ、または、解決された IP エントリの TTL の期限切れのいずれかが発生した時点で解決されます。

このコマンドは、少なくとも 1 つのネットワーク オブジェクト グループがアクティブ化されている場合にのみ有効です。

例

次に、DNS ポーリング タイマーを 240 分に設定する例を示します。

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# poll-timer minutes 240
```

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 サーバー グループを設定できる DNS サーバー グループ モードを開始します。
show running-config dns-server group	既存の DNS サーバー 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。

pop3s（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。

POP3S コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **pop3s** コマンドを使用します。POP3S コマンドモードで入力したすべてのコマンドを削除するには、このコマンドの **no** 形式を使用します。

POP3 は、インターネット サーバーが電子メールを受信して保持するために使用するクライアント/サーバー プロトコルです。ユーザー（またはクライアント電子メール レシーバ）は、定期的にメールボックスをチェックして、メールがある場合はそれをダウンロードします。この標準プロトコルは、ほとんどの著名な電子メール製品に組み込まれています。POP3S を使用すると、SSL 接続で電子メールを受信できます。

pop3s
no pop3

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
グローバル設定	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止されました。

例

次に、POP3S コンフィギュレーション モードを開始する例を示します。

```
ciscoasa
(config)#
```

```
 pop3s
ciscoasa(config-pop3s)#
```

関連コマンド

コマンド	説明
clear configure pop3s	POP3S コンフィギュレーションを削除します。
show running-config pop3s	POP3S の実行コンフィギュレーションを表示します。

port（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。

電子メールプロキシでリッスンするポートを指定するには、適切な電子メール プロキシ コマンドモードで **port** 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。

port *portnum*
no port

構文の説明

portnum	電子メール プロキシで使用するポート。ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。

コマンド デフォルト

電子メール プロキシのデフォルト ポートは次のとおりです。

電子メールプロキシ	デフォルトポート
IMAP4S	993
POP3S	995
SMTPS	988

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
pop3s	• 対応	—	• 対応	—	—
Imap4s	• 対応	—	• 対応	—	—
Smtps	• 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。

リリース	変更内容
9.5(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

ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。

例

次に、IMAP4S 電子メール プロキシ用にポート 1066 を設定する例を示します。

```
ciscoasa
(config)#
 imap4s
ciscoasa(config-imap4s)# port 1066
```

portal-access-rule（廃止）

HTTPヘッダー内に存在するデータに基づいて、クライアントレスSSL VPNセッションを許可または拒否するグローバルなクライアントレス SSL VPN アクセス ポリシーを設定できます。拒否された場合は、エラー コードがクライアントに返されます。この拒否は、ユーザー認証の前に行われるため、処理リソースの使用が最小限に抑えられます。

portal-access-rule none
no portal-access-rule *priority* [{ **permit** | **deny** [**code** *code*]} { **any** | **user-agent match** *string* }
no portal-access-rule *priority* [{ **permit** | **deny** [**code** *code*]} { **any** | **user-agent match** *string* }]
clear configure webvpn portal-access-rule

構文の説明

none	すべてのポータルアクセスルールを削除します。クライアントレスSSL VPN セッションが HTTP ヘッダーに基づいて制限されません。
priority	ルールのプライオリティ。範囲：1 ～ 65535。
permit	HTTP ヘッダーに基づいてアクセスを許可します。
deny	HTTP ヘッダーに基づいてアクセスを拒否します。
code	返された HTTP ステータス コードに基づいてアクセスを許可または拒否します。デフォルト：403。
code	アクセスを許可するか拒否するかの基準として使用するHTTPステータス コードの番号。範囲：200 ～ 599。
any	HTTP ヘッダーのすべての文字列を照合します。
user-agent match	HTTP ヘッダーの文字列の比較をイネーブルにします。
string	照合するHTTPヘッダーの文字列を指定します。検索する文字列をワイルドカード（*）で囲むと、その文字列を含む文字列が照合されます。ワイルドカードを使用しない場合は、完全に一致する文字列だけが照合されます。 （注） 検索文字列でワイルドカードを使用することを推奨します。ワイルドカードを使用しないと、ルールでいずれの文字列も照合されなかったり、想定よりもはるかに少ない文字列しか照合されないことがあります。 スペースを含む文字列を検索する場合は、“*a string*” のように引用符で囲む必要があります。引用符とワイルドカードの両方を使用する場合、検索文字列は、“**a string**” のようになります。
no portal-access-rule	単一のポータル アクセス ルールを削除する場合に使用します。

clear configure webvpn portal-access-rule	portal-access-rule none コマンドと同じです。

コマンド デフォルト

portal-access-rule none

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 モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(5)	このコマンドが ASA 8.2.5 と 8.4(2) で同時に追加されました。
8.4(2)	このコマンドが ASA 8.2.5 と 8.4(2) で同時に追加されました。
9.17(1)	Web VPN のサポートが終了したため、このコマンドは廃止されました。

使用上のガイドライン

このチェックは、ユーザー認証の前に実行されます。

例

次に、3 つのポータル アクセス ルールを作成する例を示します。

- ポータル アクセス ルール 1 では、ASA からコード 403 が返され、HTTP ヘッダーに Thunderbird が含まれている場合に、試行されたクライアントレス SSL VPN 接続を拒否します。
- ポータル アクセス ルール 10 では、HTTP ヘッダーに MSIE 8.0（Microsoft Internet Explorer 8.0）が含まれている場合に、試行されたクライアントレス SSL VPN 接続を許可します。
- ポータル アクセス ルール 65535 では、それ以外に試行されたクライアントレス SSL VPN 接続をすべて許可します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match *Thunderbird*
ciscoasa(config-webvpn)# portal-access-rule 10 permit user-agent match "*MSIE 8.0*"
ciscoasa(config-webvpn)# portal-access-rule 65535 permit any
```

（注） HostScan がインストールされている場合、port-access-rule 機能は、ASA が Cisco Secure Desktop ポータルなどのページを開くことを停止しません。Cisco Secure Desktop ポートを回避するには、HostScan をアンインストールする必要があります。

関連コマンド

コマンド	説明
show run webvpn	WebVPN コンフィギュレーションをポータル アクセス ルールもすべて含めて表示します。
show vpn-sessiondb detail webvpn	VPNセッションに関する情報を表示します。このコマンドには、情報を完全または詳細に表示するためのオプションが含まれています。表示するセッションのタイプを指定できる他、情報をフィルタリングおよびソートするためのオプションが用意されています。
debug webvpn request *n*	特定のレベルのデバッグ メッセージのロギングをイネーブルにします。デフォルト：1。範囲：1 ～ 255。

port-channel load-balance

EtherChannelについて、ロードバランシングアルゴリズムを指定するには、インターフェイスコンフィギュレーション モードで **port-channel load-balance** コマンドを使用します。この値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

（注） ASA ハードウェアモデルおよび ISA 3000 でのみサポートされます。

port-channel load-balance { **dst-ip** | **dst-ip-port** | **dst-mac** | **dst-port** | **src-dst-ip** | **src-dst-ip-port** | **src-dst-mac** | **src-dst-port** | **src-ip** | **src-ip-port** | **src-mac** | **src-port** | **vlan-dst-ip** | **vlan-dst-ip-port** | **vlan-only** | **vlan-src-dst-ip** | **vlan-src-dst-ip-port** | **vlan-src-ip** | **vlan-src-ip-port** }
no port-channel load-balance

構文の説明

dst-ip	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 宛先 IP アドレス
dst-ip-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 宛先 IP アドレス • 接続先ポート
dst-mac	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 宛先 MAC アドレス
dst-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 宛先ポート
src-dst-ip	（デフォルト）パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 送信元 IP アドレス • 宛先 IP アドレス

src-dst-ip-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 送信元 IP アドレス • 宛先 IP アドレス • 送信元ポート（Source Port） • 接続先ポート
src-dst-mac	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 送信元 MAC アドレス • 宛先 MAC アドレス
src-dst-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 送信元ポート • 宛先ポート
src-ip	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 送信元 IP アドレス
src-ip-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 送信元 IP アドレス • ソース ポート
src-mac	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 送信元 MAC アドレス
src-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 送信元ポート

vlan-dst-ip	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • VLAN • 宛先 IP アドレス
vlan-dst-ip-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • VLAN • 宛先 IP アドレス（Destination IP address） • 宛先ポート
vlan-only	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • VLAN
vlan-src-dst-ip	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • VLAN • 送信元 IP アドレス • 宛先 IP アドレス
vlan-src-dst-ip-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • VLAN • 送信元 IP アドレス • 宛先 IP アドレス • 送信元ポート • 宛先ポート
vlan-src-ip	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • VLAN • 送信元 IP アドレス

vlan-src-ip-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • VLAN • 送信元 IP アドレス • ソース ポート

コマンド デフォルト

デフォルトは **src-dst-ip** 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
インターフェイス 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
8.4(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、パケットの送信元および宛先の IP アドレス（**src-dst-ip**）をハッシュすることによって、パケットを EtherChannel 内のインターフェイスに分散します。生成されたハッシュ値をアクティブなリンクの数で割り、そのモジュロ演算で求められた余りの値によってフローの割り当て先のインターフェイスが決まります。*hash_value* **mod** *active_links* の結果が 0 となるパケットはすべて、EtherChannel 内の最初のインターフェイスに送信されます。以降、結果が 1 となるパケットは 2 番目のインターフェイスに、結果が 2 となるパケットは 3 番目のインターフェイスに、というように送信されます。たとえば、15 個のアクティブ リンクがある場合、モジュロ演算では 0 ～ 14 の値が得られます。6 個のアクティブ リンクの場合、値は 0 ～ 5 となり、以降も同様になります。

クラスタリングのスパンド EtherChannel の場合、ロード バランシングは ASA 単位で行われます。たとえば、8 台の ASA にわたるスパンド EtherChannel 内に 32 個のアクティブ インターフェイスがあり、EtherChannel 内の 1 台の ASA あたり 4 個のインターフェイスがある場合、ロード バランシングは 1 台の ASA の 4 個のインターフェイス間でのみ行われます。

アクティブ インターフェイスがダウンし、スタンバイ インターフェイスに置き換えられない場合、トラフィックは残りのリンク間で再バランスされます。失敗はレイヤ 2 のスパニングツリーとレイヤ 3 のルーティング テーブルの両方からマスクされるため、他のネットワーク デバイスへのスイッチオーバーはトランスペアレントです。

例

次に、送信元および宛先のIPアドレスとポートを使用するようにロードバランシング アルゴリズムを設定する例を示します。

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# port-channel load-balance src-dst-ip-port
```

関連コマンド

コマンド	説明
channel-group	EtherChannel にインターフェイスを追加します。
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブインターフェイスの最小数を指定します。
show lacp	LACP情報（トラフィック統計情報、システムID、ネイバーの詳細など）が表示されます。
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

port-channel min-bundle

EtherChannelについて、ポートチャネルインターフェイスがアクティブになるために必要なアクティブインターフェイスの最小数を指定するには、インターフェイスコンフィギュレーション モードで **port-channel min-bundle** コマンドを使用します。この値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

（注） ASA ハードウェアモデルおよび ISA 3000 でのみサポートされます。

port-channel min-bundle *number*
no port-channel min-bundle

構文の説明

number	ポートチャネル インターフェイスがアクティブになるために必要なアクティブ インターフェイスの最小数を 1 ～ 8 の範囲で指定します。9.2(1) 以降では、1 ～ 16 の範囲で指定できます。

コマンド デフォルト

デフォルトは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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
インターフェイス 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
8.4(1)	このコマンドが追加されました。
9.2(1)	アクティブ インターフェイスの数が 8 から 16 に増加しました。

使用上のガイドライン

このコマンドは、ポートチャネル インターフェイスに対して入力します。チャネル グループ内のアクティブインターフェイス数がこの値よりも小さい場合、ポートチャネルインターフェイスがダウンし、デバイスレベル フェールオーバーが開始されます。

例

次に、ポートチャネルがアクティブになるために必要なアクティブ インターフェイスの最小数を 2 に設定する例を示します。

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# port-channel min-bundle 2
```

関連コマンド

コマンド	説明
channel-group	EtherChannel にインターフェイスを追加します。
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブインターフェイスの最小数を指定します。
show lacp	LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

port-channel span-cluster

EtherChannel を ASA クラスタのスパンド EtherChannel として設定するには、インターフェイス コンフィギュレーション モードで **port-channel span-cluster** コマンドを使用します。スパニングを無効にするには、このコマンドの **no** 形式を使用します。

（注） ASA ハードウェアモデルでのみサポートされます。他のモデルは、暗黙的にデータ EtherChannel をスパンドモードに設定します。

port-channel span-cluster [**vss-load-balance**]
no port-channel span-cluster [**vss-load-balance**]

構文の説明

vss-load-balance （オプション）VSS ロードバランシングをイネーブルにします。ASA を VSS または vPC の 2 台のスイッチに接続する場合は、VSS ロードバランシングを有効にする必要があります。この機能を使用すると、ASA と VSS（または vPC）ペアとの間の物理リンク接続の負荷が確実に分散されます。ロードバランシングをイネーブルにする前に、各メンバーインターフェイスに対して **channel-group** コマンドの **vss-id** キーワードを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
インターフェイス 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
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

この機能を使用するには、スパンド EtherChannel モード（**cluster interface-mode spanned**）に移行する必要があります。

この機能を使用すると、ユニットあたり1つ以上のインターフェイスをグループ化して、クラスタのすべてのユニットに広がるEtherChannelとすることができます。EtherChannelによって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。スパンドEtherChannelは、ルーテッドとトランスペアレントのどちらのファイアウォールモードでも設定できます。ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレントモードでは、IP アドレスはインターフェイスではなくブリッジグループに割り当てられます。EtherChannelは初めから、ロード バランシング機能を基本的動作の一部として備えています。

例

次に、tengigabitethernet 0/8インターフェイスを唯一のメンバとするEtherChannel（ポートチャネル2）を作成し、クラスタ全体のスパンドEtherChannelにする例を示します。ポート チャネル 2 に 2 つのサブインターフェイスを追加しています。

```
interface tengigabitethernet 0/8
channel-group 2 mode active
no shutdown
interface port-channel 2
port-channel span-cluster
interface port-channel 2.10
vlan 10
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE
interface port-channel 2.20
vlan 20
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開始します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。スパンドEtherChannelまたは個別インターフェイスのどちらかを設定できます。

port-forward（廃止）

クライアントレス SSL VPN セッションのユーザーが転送先 TCP ポートからアクセスできるアプリケーションセットを設定するには、webvpn コンフィギュレーション モードで **port-forward** コマンドを使用します。

port-forward { *list_name local_port remote_server remote_port description* }

複数アプリケーションへのアクセスを設定するには、アプリケーションごとに同じ *list_name* を 1 回ずつ、複数回指定してこのコマンドを使用します。

リストから設定済みアプリケーションを削除するには、**no port-forward** *list_name local_port* コマンドを使用します（*remote_server* and *remote_port* パラメータを指定する必要はありません）。

no port-forward *listname localport*

設定済みのリスト全体を削除するには、**no port-forward** *list_name* コマンドを使用します。

no port-forward *list_name*

構文の説明

description	エンドユーザーのポート フォワーディング Java アプレット画面に表示されるアプリケーション名または短い説明を指定します。最大 64 文字です。
list_name	クライアントレス SSL VPN セッションのユーザーがアクセスできる一連のアプリケーション（転送先 TCP ポート）をグループ化します。最大 64 文字です。
local_port	アプリケーションの TCP トラフィックを受信するローカル ポートを指定します。ローカル ポート番号は *list_name* あたり 1 回のみ使用できます。1 ～ 65535 の範囲のポート番号を入力します。既存サービスとの競合を避けるために、1024 よりも大きいポート番号を使用します。
remote_port	リモート サーバーでこのアプリケーション用に接続するポートを指定します。これは、アプリケーションで使用する実際のポートです。1 ～ 65535 の範囲のポート番号、またはポート名を入力します。
remote_server	アプリケーションのリモート サーバーの DNS 名または IP アドレスを指定します。IP アドレスを入力する場合は、IPv4 形式か IPv6 形式で入力できます。特定の IP アドレス用にクライアント アプリケーションを設定する必要がないように、ホスト名を使用することを推奨します。dns server-group コマンドの **name-server** では、ホスト名を IP アドレスに解決する必要があります。

コマンド デフォルト

デフォルトのポート フォワーディング リストはありません。

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
webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	コマンド モードが webvpn に変更されました。
9.17(1)	Web VPN のサポートが終了したため、このコマンドは廃止されました。

使用上のガイドライン

ポート転送は Microsoft Outlook Exchange（MAPI）プロキシをサポートしていません。ただし、Microsoft Outlook Exchange 2010 に対してはスマート トンネルのサポートを設定できます。

例

次の表に、サンプル アプリケーションで使用する値を示します。

アプリケーション	ローカルポート	サーバー DNS 名	リモートポート	説明
IMAP4S 電子メール	20143	IMAP4Sserver	143	メール取得
SMTPS 電子メール	20025	SMTPSserver	25	メール送信
DDTS over SSH	20022	DDTSserver	22	DDTS over SSH
Telnet	20023	Telnetserver	23	Telnet

次に、これらのアプリケーションへのアクセスを提供する *SalesGroupPorts* という名前のポート フォワーディング リストを作成する例を示します。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20025 SMTPSserver 25 Send Mail
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20022 DDTSserver 22 DDTS over SSH
```

```
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20023 Telnetserver 23 Telnet
```

関連コマンド

コマンド	説明
port-forward auto-start	このコマンドはグループ ポリシー webvpn またはユーザー名 webvpn モードで入力します。ユーザーがクライアントレス SSL VPN セッションにログインするときに、ポート フォワーディングを自動的に開始して、指定したポート フォワーディング リストを割り当てます。
port-forward enable	このコマンドはグループポリシー webvpn またはユーザー名 Wwebvpn モードで入力します。ユーザーがログインするときに、指定したポートフォワーディング リストを割り当てますが、ポートフォワーディングはユーザーが手動で開始する必要があります。開始するには、クライアントレス SSL VPN ポータルページで [**Application Access**] > [**Start Applications**] ボタンを使用します。
port-forward disable	このコマンドはグループ ポリシー webvpn またはユーザー名 webvpn モードで入力します。ポート フォワーディングをオフにします。

port-forward-name（廃止）

特定のユーザーポリシーやグループポリシーのエンドユーザーに対して TCP ポートフォワーディングを特定する表示名を設定するには、グループポリシーモードまたはユーザー名モードから開始する webvpn モードで **port-forward-name** コマンドを使用します。**port-forward-name none** コマンドを使用して作成したヌル値を含めて、表示名を削除するにはこのコマンドの no 形式を入力します。**,no** オプションを指定すると、デフォルト名「Application Access」が復元されます。表示名を使用しないようにするには、**port-forward none** コマンドを入力します。

port-forward-name { **value** *name* | **none** }
no port-forward-name

構文の説明

none	表示名がないことを指定します。ヌル値を設定して、表示名を拒否します。値は継承しません。
value *name*	エンドユーザーにポート フォワーディングを説明します。最大 255 文字です。

コマンド デフォルト

デフォルトの名前は「Application Access」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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.17(1)	Web VPN のサポートが終了したため、このコマンドは廃止されました。

例

次の例は、FirstGroup という名前のグループ ポリシーに「Remote Access TCP Applications」という名前を設定する方法を示しています。

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
```

```
 webvpn
ciscoasa(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
```

関連コマンド

コマンド	説明
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザー名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザー名に適用するパラメータを設定できるようにします。
webvpn	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。WebVPN のグローバル設定を設定できます。

port-object

タイプが TCP、UDP、または TCP-UDP のサービスオブジェクトグループにポートオブジェクトを追加するには、オブジェクトグループサービスコンフィギュレーションモードで**port-object**コマンドを使用します。ポート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。

port-object { **eq** *port* | **range** *begin_port end_port* }
no port-object { **eq** *port* | **range** *begin_port end_port* }

構文の説明

range *begin_port end_port*	ポート範囲の開始値と終了値を 0 ～ 65535 の範囲で指定します。
eq *port*	サービス オブジェクトの TCP または UDP ポートの 10 進数（0 ～ 65535）または名前を指定します。

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 サービス 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
7.0(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

port-object コマンドは、特定のポートまたはポート範囲のオブジェクトを定義するために、**object-group service** *protocol* コマンドと組み合わせて使用します。

TCP または UDP サービスの名前を指定する場合は、サポートされる TCP や UDP のいずれかの名前で、オブジェクト グループのプロトコル タイプと整合性を持つものである必要があります。たとえば、プロトコル タイプが tcp、udp、および tcp-udp の場合、名前はそれぞれ有効な TCP サービス名、有効な UDP サービス名、または有効な TCP および UDP サービス名である必要があります。

番号を指定した場合、オブジェクトが表示されるときに、プロトコルタイプに基づいて、その番号が対応する名前（存在する場合）に変換されます。

次のサービス名がサポートされています。

[TCP]	UDP	TCP および UDP
bgp	biff	discard
chargen	bootpc	domain
cmd	bootps	echo
daytime	dnsix	pim-auto-rp
exec	nameserver	sunrpc
finger	mobile-ip	syslog
ftp	netbios-ns	tacacs
ftp-data	netbios-dgm	talk
gopher	ntp	
ident	rip	
irc	snmp	
h323	snmptrap	
hostname	tftp	
http	time	
klogin	who	
kshell	xdmcp	
login	isakmp	
lpd		
nntp		
pop2		
pop3		
smtp		
sqlnet		
Telnet		
uucp		

[TCP]	UDP	TCP および UDP
whois		
www		

例

次に、新規ポート（サービス）オブジェクトグループを作成するために、サービス コンフィギュレーション モードで **port-object** コマンドを使用する例を示します。

```
ciscoasa(config)# object-group service eng_service tcp
ciscoasa(config-service)# port-object eq smtp
ciscoasa(config-service)# port-object eq telnet
ciscoasa(config)# object-group service eng_service udp
ciscoasa(config-service)# port-object eq snmp
ciscoasa(config)# object-group service eng_service tcp-udp
ciscoasa(config-service)# port-object eq domain
ciscoasa(config-service)# port-object range 2000 2005
ciscoasa(config-service)# quit
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
show running-config object-group	現在のオブジェクト グループを表示します。

post-max-size

アップロードするオブジェクトの最大許容サイズを指定するには、グループポリシー webvpn コンフィギュレーション モードで **post-max-size** コマンドを使用します。このオブジェクトを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** バージョンを使用します。

post-max-size *size*
no post-max-size

構文の説明

size	ポストするオブジェクトに許可される最大サイズを指定します。指定できる範囲は 0 ～ 2147483647 です。サイズを 0 に設定すると、オブジェクトのポストが実質的に禁止されます。

コマンド デフォルト

デフォルトのサイズは 2147483647 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
グループ ポリシー webvpn コンフィギュレーション 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。

例

次に、ポストするオブジェクトの最大サイズを 1500 バイトに設定する例を示します。

```
ciscoasa
(config)#

group-policy test attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa
(config-group-webvpn)#
post-max-size 1500
```

関連コマンド

コマンド	説明
download-max-size	ダウンロードするオブジェクトの最大サイズを指定します。
upload-max-size	アップロードするオブジェクトの最大サイズを指定します。
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザー名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザー名に適用するパラメータを設定できるようにします。
webvpn	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。WebVPN のグローバル設定を設定できます。

power inline

Firepower 1010 イーサネット 1/7 または 1/8 インターフェイスで Power on Ethernet+（PoE+）を有効または無効にするには、インターフェイス コンフィギュレーション モードで **power inline** コマンドを使用します。デフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

power inline { **auto** | **never** | **consumption wattage** *milliwatts* }

（注） Firepower 1010 でのみサポートされています。Firepower 1010E ではサポートされていません。

構文の説明

consumption wattage *milliwatts*	ワット数をミリワット単位で手動で指定します（4000～30000）。ワット数を手動で設定し、LLDP ネゴシエーションを無効にする場合は、このコマンドを使用します。
auto	給電先デバイスのクラスに適したワット数を使用して、給電先デバイスに自動的に電力を供給します。Firepower 1010 は LLDP を使用して、適切なワット数をさらにネゴシエートします。
never	PoE を無効にします。

コマンド デフォルト

デフォルトは **auto** 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
インターフェイス 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
9.13(1)	コマンドが追加されました。

使用上のガイドライン

Firepower 1010 は、IEEE 802.3af（PoE）と 802.3at（PoE+）の両方をサポートしています。PoE+ は、Link Layer Discovery Protocol（LLDP）を使用して電力レベルをネゴシエートします。PoE+

は、受電デバイスに最大 30 ワットの電力を提供できます。電力は必要なときのみ供給されます。

インターフェイスをシャットダウンすると、デバイスへの給電が無効になります。Firepower 1010 の場合、イーサネット 1/7 および 1/8 は PoE+ をサポートします。

例

次に、イーサネット 1/7 のワット数を手動で設定し、イーサネット 1/8 の電力を auto に設定する例を示します。

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)# power inline consumption wattage 10000
ciscoasa(config-if)# interface ethernet1/8
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)#
```

関連コマンド

コマンド	説明
show power inline	PoE ステータスを表示します。

power-supply

ISA 3000 のデュアル電源の場合、デュアル電源を ASA OS で想定される構成として確立するには、グローバル コンフィギュレーション モードで **power-supply** コマンドを使用します。デュアル電源を無効にするには、このコマンドの **no** 形式を使用します。

power-supply dual
no power-supply dual

構文の説明

dual	デュアル電源を指定します。

コマンド デフォルト

デフォルトでは、デュアル電源が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
グローバル設定	• 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

1 つの電源に障害が発生すると、ASA はアラームを発します。デフォルトでは、ASA で単一電源が想定されており、装備している電源のいずれかが機能しているかぎりアラームを発しません。

例

次に、デュアル電源を確立する例を示します。

```
ciscoasa(config)# power-supply dual
```

pppoe client route distance

PPPoE を通じて学習したルートにアドミニストレーティブ ディスタンスを設定するには、インターフェイス コンフィギュレーション モードで **pppoe client route distance** 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。

pppoe client route distance *distance*
no pppoe client route distance *distance*

構文の説明

distance PPPoE を介して学習したルートに適用するアドミニストレーティブ ディスタンス。有効な値は、1 ～ 255 です。

コマンド デフォルト

PPPoE を介して学習したルートには、デフォルトで 1 のアドミニストレーティブ ディスタンスが割り当てられます。

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
インターフェイス コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

pppoe client route distance コマンドは、ルートが PPPoE を通じて学習された場合にのみチェックされます。ルートが PPPoE を通じて学習された後に **pppoe client route distance** コマンドを入力しても、指定したアドミニストレーティブディスタンスは、学習された既存のルートに影響を与えません。指定したアドミニストレーティブディスタンスが設定されるのは、このコマンドの入力後に学習されたルートだけです。

PPPoE でルートを取得するには、**ip address pppoe** コマンドで **setroute** オプションを指定する必要があります。

PPPoE を複数のインターフェイスで設定している場合、インストールされたルートの優先順位を指定するには、各インターフェイスで **pppoe client route distance** コマンドを使用する必要があります。複数のインターフェイスでの PPPoE クライアントのイネーブル化は、オブジェクト トラッキングでのみサポートされています。

PPPoE を使用して IP アドレスを取得する場合は、フェールオーバーを設定できません。

例

次に、GigabitEthernet0/2 上で PPPoE によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニターされます。この SLA 動作が失敗した場合は、GigabitEthernet0/3 上で PPPoE により取得したセカンダリ ルートが使用されます。

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

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
ip address pppoe	PPPoE により取得した IP アドレスを使用して、指定したインターフェイスを設定します。
ppoe client secondary	セカンダリ PPPoE クライアント インターフェイスのトラッキングを設定します。
pppoe client route track	PPPoE により学習したルートを、トラッキング エントリ オブジェクトに関連付けます。
sla monitor	SLA モニタリング動作を定義します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

pppoe client route track

追加ルートをトラッキング済みの指定オブジェクト番号に関連付けるように PPPoE クライアントを設定するには、インターフェイス コンフィギュレーション モードで **pppoe client route track** コマンドを使用します。PPPoE ルートトラッキングを削除するには、このコマンドの **no** 形式を使用します。

pppoe client route track *number*
no pppoe client route track

構文の説明

number トラッキング エントリのオブジェクト ID。有効な値は、1 ～ 500 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
インターフェイス コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

pppoe client route track コマンドは、ルートが PPPoE を通じて学習された場合にのみチェックされます。ルートが PPPoE から学習された後で **pppoe client route track** コマンドを入力すると、学習された既存のルートはトラッキングオブジェクトに関連付けられません。指定したトラッキング オブジェクトに関連付けられるのは、このコマンドの入力後に学習されたルートだけです。

PPPoE でルートを取得するには、**ip address pppoe** コマンドで **setroute** オプションを指定する必要があります。

PPPoE を複数のインターフェイスで設定している場合、インストールされたルートの優先順位を指定するには、各インターフェイスで **pppoe client route distance** コマンドを使用する必要があります。PPPoE クライアントを複数のインターフェイス上でイネーブルにすることは、オブジェクト トラッキングのみでサポートされます。

PPPoE を使用して IP アドレスを取得する場合は、フェールオーバーを設定できません。

例

次に、GigabitEthernet0/2 上で PPPoE によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニターされます。この SLA 動作が失敗した場合は、GigabitEthernet0/3 上で PPPoE により取得したセカンダリ ルートが使用されます。

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

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
ip address pppoe	PPPoE により取得した IP アドレスを使用して、指定したインターフェイスを設定します。
ppoe client secondary	セカンダリ PPPoE クライアント インターフェイスのトラッキングを設定します。
pppoe client route distance	PPPoE によって学習されたルート アドミニストレーティブ ディスタンスを割り当てます。
sla monitor	SLA モニタリング動作を定義します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

pppoe client secondary

PPPoEクライアントをトラッキング済みオブジェクトのクライアントとして登録し、トラッキング状態に基づいて起動または終了するように設定するには、インターフェイス コンフィギュレーション モードで **pppoe client secondary** コマンドを使用します。クライアントの登録を削除するには、このコマンドの **no** 形式を使用します。

pppoe client secondary track *number*
no pppoe client secondary track

構文の説明

number トラッキング エントリのオブジェクト ID。有効な値は、1 ～ 500 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
インターフェイス コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

pppoe client secondary コマンドは、PPPoE セッションが開始されたときにのみチェックされます。ルートが PPPoE から学習された後で **pppoe client route track** コマンドを入力すると、学習された既存のルートはトラッキングオブジェクトに関連付けられません。指定したトラッキング オブジェクトに関連付けられるのは、このコマンドの入力後に学習されたルートだけです。

PPPoE でルートを取得するには、**ip address pppoe** コマンドで **setroute** オプションを指定する必要があります。

PPPoE を複数のインターフェイスで設定している場合、インストールされたルートの優先順位を指定するには、各インターフェイスで **pppoe client route distance** コマンドを使用する必要があります。PPPoEクライアントを複数のインターフェイス上でイネーブルにすることは、オブジェクト トラッキングのみでサポートされます。

PPPoE を使用して IP アドレスを取得する場合は、フェールオーバーを設定できません。

例

次に、GigabitEthernet0/2 上で PPPoE によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニターされます。この SLA 動作が失敗した場合は、GigabitEthernet0/3 上で PPPoE により取得したセカンダリ ルートが使用されます。

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

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
ip address pppoe	PPPoE により取得した IP アドレスを使用して、指定したインターフェイスを設定します。
ppoe client secondary	セカンダリ PPPoE クライアント インターフェイスのトラッキングを設定します。
pppoe client route distance	PPPoE によって学習されたルート アドミニストレーティブ ディスタンスを割り当てます。
pppoe client route track	PPPoE により学習したルートを、トラッキング エントリ オブジェクトに関連付けます。
sla monitor	SLA モニタリング動作を定義します。

prc-interval

部分的なルート計算（PRC）の IS-IS スロットリングをカスタマイズするには、ルータ ISIS コンフィギュレーション モードで **prc-interval** 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。

prc-interval *prc-max-wait* ［ *prc-initial-wait prc-second-wait* ］
no prc-interval

構文の説明

prc-max-wait	2 つの連続 PRC 計算の最大間隔を示します。範囲は、1 ～ 120 秒です。
prc-initial-wait	（任意）トポロジ変更後の初期 PRC 計算遅延を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 2000 ミリ秒です。
prc-second-wait	（任意）最初と 2 番めの PRC 計算間のホールド タイム（ミリ秒単位）を示します。値の範囲は 1 ～ 120,000 ミリ秒です。

コマンド デフォルト

デフォルトは、次のとおりです。

prc-max-wait：5 秒

prc-initial-wait：2000 ミリ秒

prc-second-wait：5000 ミリ秒

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

PRC は Shortest Path First（SPF）計算を実行せずにルートを計算するソフトウェア プロセスです。これは、ルーティング システム自体のトポロジが変更されていないものの特定の IS でアナウンスされた情報で変更が検出されたり、そのようなルートをルーティング情報ベース（RIB）に再インストールしようとしたりすることが必要な場合に可能です。

次の説明を参照して、このコマンドのデフォルト値を変更するかどうか決定する際の参考にしてください。

- *prc-initial-wait* 引数は、最初の LSP を生成する前の初期待機時間（ミリ秒）を表します。
- *prc-second-wait* 引数は、最初と 2 番めの LSP 生成間の待機時間（ミリ秒単位）を示します。
- 各後続待機間隔は、*prc-max-wait* 間隔で指定された待機間隔に到達するまで、前の間隔の 2 倍であるため、この値により最初と 2 番めの間隔の後、PRC 計算のスロットリングまたは低下が発生します。最大時間に到達すると、ネットワークが安定するまで、待機時間は最大値のままとなります。
- ネットワークが安定し、*prc-max-wait* 間隔の 2 倍の時間内にトリガーがなければ、高速動作（最初の待機時間）に戻ります。

例

次に、PRC の間隔の例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# prc-interval 2 50 100
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。

コマンド	説明
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。

コマンド	説明
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。

コマンド	説明
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

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。