match r – me

match regex

正規表現クラスマップで正規表現を識別するには、クラスマップタイプ正規表現コンフィギュレーション モードで **match regex** コマンドを使用します。クラスマップから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。

match regex *name*
no match regex *name*

構文の説明

name	**regex** コマンドを使用して追加した正規表現の名前。

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 タイプ正規表現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(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

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。正規表現は、**class-map type regex** コマンドの後に複数の **match regex** コマンドを使用して、正規表現クラスマップにグループ化できます。

たとえば、インスペクション ポリシー マップを使用して、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。

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 url_example
ciscoasa(config-cmap)# match regex url_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 test interface outside
```

関連コマンド

コマンド	説明
class-map type regex	正規表現クラスマップを作成します。
regex	正規表現を追加します。
test regex	正規表現をテストします。

match req-resp

HTTP 要求と応答の両方に関して一致条件を設定するには、ポリシーマップ コンフィギュレーション モードで **match req-resp** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

match ［ **not** ］ **req-resp content-type mismatch**
no match ［ **not** ］ **req-resp content-type mismatch**

構文の説明

content-type mismatch	HTTP 応答の content-type フィールドが対応する HTTP 要求メッセージの accept フィールドと一致しないトラフィックを照合します。

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
ポリシー 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
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドでは、次のチェックを行うことができます。

- content-type ヘッダーの値がサポート対象コンテンツ タイプの内部リストにあることを確認します。
- ヘッダー content-type が、メッセージのデータまたはエンティティ本文の実際のコンテンツに一致することを確認します。
- HTTP 応答の content type フィールドが、対応する HTTP 要求メッセージの **accept** フィールドと一致することを確認します。

メッセージが前述のいずれかのチェックに失敗した場合、ASA は設定されたアクションを実行します。

次に、サポート対象コンテンツ タイプのリストを示します。

audio/* |	audio/basic |	video/x-msvideo
audio/mpeg |	audio/x-adpcm |	audio/midi
audio/x-ogg |	audio/x-wav |	audio/x-aiff |
application/octet-stream	application/pdf	application/msword
application/vnd.ms-excel	application/vnd.ms-powerpoint	application/postscript
application/x-java-arching	application/x-msn-messenger	application/x-gzip
image |	application/x-java-xm	application/zip
image/jpeg |	image/cgf |	image/gif |
image/x-3ds |	image/png |	image/tiff |
image/x-portable-bitmap |	image/x-bitmap |	image/x-niff |
text/* |	image/x-portable-greymap |	image/x-xpm |
text/plain |	text/css	text/html |
text/xmcd	text/richtext |	text/sgml
video/-flc	text/xml	video/*
video/sgi	video/mpeg	video/quicktime
video/x-mng	video/x-avi	video/x-fli

このリストのコンテンツ タイプの中には、メッセージの本文部分で確認できないように、対応する正規表現（magic number）がないものがあります。この場合、HTTP メッセージは許可されます。

例

次に、HTTP ポリシーマップで HTTP メッセージのコンテンツ タイプに基づいて HTTP トラフィックを制限する例を示します。

```
ciscoasa
(config)#
 policy-map type inspect http http_map
ciscoasa
(config-pmap)#
 match req-resp content-type mismatch
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。

コマンド	説明
clear configure class-map	すべてのクラス マップを削除します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match request-command

特定の FTP コマンドを制限するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match request-command** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **request-command** *ftp_command* [*ftp_command* . . .]
no match [**not**] **request-command** *ftp_command* [*ftp_command* . . .]

構文の説明

ftp_command	制限する FTP コマンドを 1 つ以上指定します。

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
クラス マップまたはポリシー 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
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップに入力できるエントリは 1 つのみです。

例

次に、FTP インスペクション ポリシー マップに特定の FTP コマンドに関して一致条件を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ftp ftp_map1
ciscoasa(config-pmap)# match request-command stou
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。

コマンド	説明
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match request-method

SIPメソッドタイプに関して一致条件を設定するには、クラスマップまたはポリシーマップコンフィギュレーション モードで **match request-method** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **request-method** *method_type*
no match [**not**] **request-method** *method_type*

構文の説明

method_type	RFC 3261 およびサポートされている拡張に従って、メソッド タイプを指定します。サポートされているメソッド タイプには、ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update 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
クラス マップまたはポリシー 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
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップに入力できるエントリは 1 つのみです。

例

次の例では、SIP インスペクション クラス マップで SIP メッセージによって取得されるパスの一致条件を設定する方法を示します。

```
ciscoasa(config-cmap)# match request-method ack
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match request method

HTTP 要求に関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match request method** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

match [**not**] **request** { *built-in-regex* | **regex** { **regex_name** | **class** *class_map_name* } }
no match [**not**] **request** { *built-in-regex* | **regex** { **regex_name** | **class** *class_map_name* } }

構文の説明

built-in-regex	コンテンツ タイプ、方法、または転送エンコーディングの組み込みの正規表現を指定します。
class *class_map name*	正規表現タイプのクラス マップの名前を指定します。
regex *regex_name*	**regex** コマンドを使用して設定されている正規表現の名前を指定します。

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
ポリシー 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
7.2(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

表 *1:* 組み込みの正規表現値

bcopy	bdelete	bmove	bpropfind
bproppatch	connect	copy	delete
edit	get	getattribute	getattributenames
getproperties	head	index	lock
mkcol	mkdir	move	notify

options	poll	post	propfind
proppatch	put	revadd	revlabel
revlog	revnum	save	search
setattribute	startrev	stoprev	subscribe
trace	unedit	unlock	unsubscribe

例

次に、「GET」メソッドまたは「PUT」メソッドで「www\.example.com/.*\.asp」または「www\example[0-9][0-9]\.com」にアクセスしようとしている HTTP 接続を許可し、ロギングする HTTP インスペクション ポリシー マップを定義する例を示します。それ以外の URL/メソッドの組み合わせは、サイレントに許可されます。

```
ciscoasa(config)# regex url1 "www\.example.com/.*\.asp
ciscoasa(config)# regex url2 "www\.example[0-9][0-9]\.com"
ciscoasa(config)# regex get "GET"
ciscoasa(config)# regex put "PUT"
ciscoasa(config)# class-map type regex match-any url_to_log
ciscoasa(config-cmap)# match regex url1
ciscoasa(config-cmap)# match regex url2
ciscoasa(config-cmap)# exit
ciscoasa(config)# class-map type regex match-any methods_to_log
ciscoasa(config-cmap)# match regex get
ciscoasa(config-cmap)# match regex put
ciscoasa(config-cmap)# exit
ciscoasa(config)# class-map type inspect http http_url_policy
ciscoasa(config-cmap)# match request uri regex class url_to_log
ciscoasa(config-cmap)# match request method regex class methods_to_log
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map type inspect http http_policy
ciscoasa(config-pmap)# class http_url_policy
ciscoasa(config-pmap-c)# log
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match route-type

指定されたタイプのルートを再配布するには、ルートマップ コンフィギュレーション モードで **match route-type** コマンドを使用します。ルートタイプ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。

match route-type { **local** | **internal** | { **external** [**type-1** | **type-2**] } | { **nssa-external** [**type-1** | **type-2**] } }
no match route-type { **local** | **internal** | { **external** [**type-1** | **type-2**] } | { **nssa-external** [**type-1** | **type-2**] } }

構文の説明

external	OSPF 外部ルートまたは EIGRP 外部ルート。
internal	OSPFエリア内およびエリア間ルート、またはEIGRP内部ルート
local	ローカルに生成された BGP ルート。
nssa-external	外部 NSSA を指定します。
type-1	（任意）ルート タイプ 1 を指定します。
type-2	（任意）ルート タイプ 2 を指定します。

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
ルート マップ 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。
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

route-map グローバル コンフィギュレーション コマンド、**match** および **set** コンフィギュレーション コマンドを使用すると、あるルーティングプロトコルから別のルーティングプロトコル

にルートを再配布するための条件を定義できます。各 **route-map** コマンドには、そのコマンドに関連付けられた **match** および **set** コマンドがあります。**match** コマンドは、一致基準（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドは、設定アクション（**match** コマンドが指定している基準を満たした場合に実行する特定の再配布アクション）を指定します。**no route-map** コマンドは、ルートマップを削除します。

match ルート マップ コンフィギュレーション コマンドには、複数の形式があります。**match** コマンドは任意の順序で入力できます。**set** コマンドで指定した設定アクションに従ってルートを再配布するには、すべての **match** コマンドで「一致」する必要があります。**match** コマンドの **no** 形式を使用すると、指定した一致基準が削除されます。

ルートマップは、いくつかの部分にわかれている可能性があります。**route-map** コマンドに関係のあるいずれの match 句とも一致しないルートは無視されます。一部のデータのみを修正するには、別のルート マップ セクションを設定して、正確に一致する基準を指定する必要があります。

OSPF の場合、**external type-1** キーワードはタイプ 1 外部ルートにのみ一致し、**external type-2** キーワードはタイプ 2 外部ルートにのみ一致します。

例

次の例では、内部ルートを再配布する方法を示します。

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match route-type internal
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを再配布します。
match ip next-hop	指定したアクセス リストのいずれかによって渡されるネクストホップ ルータ アドレスを持つルートを配布します。
match metric	指定したメトリックを持つルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。

match rtp

クラスマップに偶数ポートの UDP ポート範囲を指定するには、クラス マップ コンフィギュレーション モードで **match rtp** 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。

match rtp *starting_port range*
no match rtp *starting_port range*

構文の説明

starting_port	偶数 UDP 宛先ポートの下限を指定します。指定できる範囲は、2000 ～ 65535 です。
range	RTP ポートの範囲を指定します。指定できる範囲は、0 ～ 16383 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
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。

使用上のガイドライン

match コマンドは、クラスマップのトラフィッククラスに含まれているトラフィックを指定するために使用されます。これらのコマンドには、クラスマップに含まれるトラフィックを定義するさまざまな基準が含まれています。モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定する一環として、**class-map** グローバル コンフィギュレーション コマンドを使用してトラフィッククラスを定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィッククラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラスマップの **match** ステートメントで定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに含まれ、そのトラフィック クラスに関連付けられているアクションの対象になります。あらゆるトラフィック クラスのいずれの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

RTP ポート（*starting_port* から *starting_port* に *range* を加えた値の範囲の偶数 UDP ポート番号）と照合するには、**match rtp** コマンドを使用します。

例

次に、クラスマップおよび **match rtp** コマンドを使用して、トラフィッククラスを定義する例を示します。

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
 rtp 20000 100
ciscoasa(config-cmap)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラスマップ内のアクセスリストトラフィックを指定します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match selection-mode

Create PDP Context 要求の選択モード情報要素の一致を設定するには、ポリシー マップ コンフィギュレーション モードで **match selection-mode** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **selection-mode** *mode_value*
no match [**not**] **selection-mode** *mode_value*

構文の説明

mode_value Create PDP Context 要求の選択モード情報要素。選択モードでは、メッセージにアクセス ポイント名（APN）の発信元を指定しますが、次のいずれかになります。

- 0：確認済み。APN はモバイル ステーションまたはネットワークによって指定されており、サブスクリプションが確認されています。
- 1：モバイル ステーション。APN はモバイル ステーションによって指定されており、サブスクリプションは確認されていません。
- 2：ネットワーク。APN はネットワークによって指定されており、サブスクリプションは確認されていません。
- 3：予約済み（未使用）

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
ポリシー 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
9.10(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、GTP ポリシー マップで設定できます。

Create PDP Context 要求の選択モード情報要素をフィルタリングすることができます。選択モードでは、メッセージにアクセスポイント名（APN）の発信元を指定します。これらのモードに基づいて、メッセージをドロップしたり、必要に応じてログに記録したりできます。選択モードフィルタリングは、GTPv1 および GTPv2 のみでサポートされています。

例

次の例では、選択モード 1 および 2 を照合し、それらのモードを持つ Create PDP Context メッセージをドロップしたり、ログに記録したりする方法を示しています。

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# match selection-mode 1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap)# match selection-mode 2
ciscoasa(config-pmap-c)# drop log
```

関連コマンド

コマンド	説明
drop	基準に一致するパケットをドロップします。
log	基準に一致するパケットをログに記録します。
inspect gtp	GTP アプリケーションインスペクションをイネーブルにします。
policy-map type inspect gtp	GTP インスペクションポリシーマップを作成または編集します。

match sender-address

ESMTP 送信者電子メールアドレスに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match sender-address** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

match [**not**] **sender-address** [**length gt** *bytes* | **regex** *regex*]
no match [**not**] **sender-address** [**length gt** *bytes* | **regex** *regex*]

構文の説明

length gt *bytes*	送信者電子メールアドレスの長さを照合することを指定します。
regex *regex*	正規表現を照合することを指定します。

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
ポリシー 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
7.2(1)	このコマンドが追加されました。

例

次に、ESMTP インスペクション ポリシー マップに長さが 320 文字を超える送信者電子メール アドレスに関して一致条件を設定する例を示します。

```
ciscoasa(config-pmap)# match sender-address length gt 320
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。

コマンド	説明
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match server

FTP サーバーに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match server** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **server regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **server regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラスマップを指定します。

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
クラス マップまたはポリシー 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
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップに入力できるエントリは 1 つのみです。

ASA は、FTP サーバーに接続するときにログインプロンプトの上方に表示される初期 220 サーバーメッセージに基づいて、サーバー名と照合します。220 サーバー メッセージには、行が複数含まれることがあります。サーバーとのマッチングは、DNS を介して解決されるサーバー名の FQDN に基づきません。

例

次に、FTP インスペクション ポリシー マップに FTP サーバーに関して一致条件を設定する例を示します。

```
ciscoasa(config-pmap)# match server class regex ftp-server
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match service

特定のインスタント メッセージ サービスに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match service** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] { **service** { **chat** | **file-transfer** | **games** | **voice-chat** | **webcam** | **conference** }
no match [**not**] { **service** { **chat** | **file-transfer** | **games** | **voice-chat** | **webcam** | **conference** }

構文の説明

chat	インスタント メッセージング チャット サービスを照合することを指定します。
file-transfer	インスタント メッセージング ファイル転送サービスを照合することを指定します。
games	インスタント メッセージング ゲーム サービスを照合することを指定します。
voice-chat	インスタント メッセージング音声チャット サービスを照合することを指定します。
webcam	インスタントメッセージングWebカメラ サービスを照合することを指定します。
conference	インスタント メッセージング会議サービスを照合することを指定します。

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
クラス マップまたはポリシー 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
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IM クラス マップまたは IM ポリシー マップ内で設定できます。IM クラス マップに入力できるエントリは 1 つのみです。

例

次に、インスタント メッセージング クラス マップにチャット サービスに関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match service chat
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match service-indicator

M3UA メッセージのサービスインジケータに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match service-indicator** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **service-indicator** *number*
no match [**not**] **service-indicator** *number*

構文の説明

number	サービス インジケータ番号（0 ～ 15）。サポートされているインジケータ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

M3UA インスペクションでは、すべてのサービス インジケータが許可されます。

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
ポリシー マップ設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(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 M3UA インスペクション ポリシー マップで設定できます。サービス インジケータに基づいてパケットをドロップできます。使用可能なサービスインジケータは次のとおりです。これらのサービス インジケータの詳細については、M3UA RFC およびドキュメントを参照してください。

- 0：シグナリング ネットワーク管理メッセージ
- 1：シグナリング ネットワーク テストおよびメンテナンス メッセージ
- 2：シグナリング ネットワーク テストおよびメンテナンス特別メッセージ
- 3：SCCP
- 4：電話ユーザー部
- 5：ISDN ユーザー部
- 6：データ ユーザー部（コールおよび回線関連のメッセージ）

- 7：データ ユーザー部（設備の登録およびキャンセル メッセージ）
- 8：MTP テスト ユーザー部に予約済み
- 9：ブロードバンド ISDN ユーザー部
- 10：サテライト ISDN ユーザー部
- 11：予約済み
- 12：AAL タイプ 2 シグナリング
- 13：ベアラー非依存コール制御
- 14：ゲートウェイ制御プロトコル
- 15：予約済み

例

次に、M3UA サービス インジケータに関して一致条件を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match service-indicator 15
ciscoasa(config-pmap-c)# drop
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インスペクションをイネーブルにします。
policy-map type inspect	インスペクション ポリシー マップを作成します。

match third-party-registration

第三者登録の要求者に関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match third-party-registration** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **third-party-registration regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **third-party-registration regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラスマップを指定します。

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
クラス マップまたはポリシー 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
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップに入力できるエントリは 1 つのみです。

third-party registration match コマンドは、SIP 登録または SIP プロキシで他のユーザーを登録できるユーザーを特定するために使用されます。From と To の値が一致しない場合には、REGISTER メッセージの From ヘッダー フィールドで識別されます。

例

次に、SIP インスペクション クラス マップに第三者登録に関して一致条件を設定する例を示します。

```
ciscoasa(config-cmap)# match third-party-registration regex class sip_regist
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match tunnel-group

以前に定義したトンネルグループに属するクラスマップのトラフィックと照合するには、クラス マップ コンフィギュレーション モードで **match tunnel-group** 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。

matchtunnel-group*name*
nomatchtunnel-group*name*

構文の説明

name トンネル グループ名のテキスト。

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。

使用上のガイドライン

match コマンドは、クラスマップのトラフィッククラスに含まれているトラフィックを指定するために使用されます。これらのコマンドには、クラスマップに含まれるトラフィックを定義するさまざまな基準が含まれています。モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定する一環として、**class-map** グローバル コンフィギュレーション コマンドを使用してトラフィッククラスを定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィッククラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラスマップの **match** ステートメントで定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに含まれ、そのトラフィック クラスに関連付けられているアクションの対象になります。あらゆるトラフィック クラスのいずれの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

フローベースのポリシーアクションを有効にするには、**match flow ip destination-address** と **match tunnel-group** コマンドを、**class-map**、**policy-map**、および **service-policy** コマンドとも

に使用します。フローを定義する基準は、宛先 IP アドレスです。固有の IP 宛先アドレスに向かうトラフィックは、すべてフローと見なされます。ポリシーのアクションは、トラフィックのクラス全体ではなく各フローに適用されます。QoS アクションポリシーを適用するには、**police** コマンドを使用します。トンネルグループ内の各トンネルを指定されたレートに規制するには、 **match tunnel-group** とともに **match flow ip destination-address** を使用します。

例

次の例では、トンネル グループ内でフローベースのポリシングをイネーブルにして、指定のレートに各トンネルを制限する方法を示します。

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
 tunnel-group
ciscoasa(config-cmap)# match flow ip destination-address
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# police 56000
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラスマップ内のアクセス リスト トラフィックを指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。
tunnel-group	IPsec および L2TP の接続固有レコードのデータベースを作成および管理します。

match uri

SIP ヘッダーの URI に関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match uri** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **uri** { **sip** | **tel** } **length gt** *gt_bytes*
no match [**not**] **uri** { **sip** | **tel** } **length gt** *gt_bytes*

構文の説明

sip	SIP URI を指定します。
tel	TEL URI を指定します。
length gt *gt_bytes*	URI の最大長を指定します。値の範囲は、0 ～ 65536 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
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	— • 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップに入力できるエントリは 1 つのみです。

例

次に、SIP メッセージの URI に関して一致条件を設定する例を示します。

```
ciscoasa(config-cmap)# match uri sip length gt
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match url-filter

RTSP メッセージの URL フィルタリングに関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match url-filter** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **url-filter regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **url-filter regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラスマップを指定します。

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
クラス マップまたはポリシー 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
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

このコマンドは、RTSP クラス マップまたはポリシー マップで設定できます。

例

次に、RTSP インスペクション ポリシー マップに URL フィルタリングに関して一致条件を設定する例を示します。

```
ciscoasa(config)# regex badurl www.example.com/rtsp.avi
ciscoasa(config)# policy-map type inspect rtsp rtsp-map
ciscoasa(config-pmap)# match url-filter regex badurl
ciscoasa(config-pmap-p)# drop-connection
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match user group

クラウドWebセキュリティのホワイトリストに追加するユーザーやグループを指定するには、クラス マップ コンフィギュレーション モードで **match user group** コマンドを使用します。一致を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] { [**user** *username*] [**group** *groupname*] }
no match [**not**] { [**user** *username*] [**group** *groupname*] }

構文の説明

not	（オプション）ユーザーやグループをクラウド Web セキュリティを使用してフィルタリングするように指定します。たとえば、グループ「cisco」をホワイトリストに登録し、ユーザー「johncrichton」および「aerynsun」からのトラフィックをスキャンする場合、これらのユーザーに **match not** を指定できます。
user *username*	ホワイトリストに追加するユーザーを指定します。
group *groupname*	ホワイトリストに追加するグループを指定します。

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
クラス マップ コンフィギュレーション モード	• 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

AAA ルールまたは IDFW を使用する場合、その他の場合にはサービスポリシールールに一致する特定のユーザーやグループからの Web トラフィックが、スキャンのためにクラウド Web セキュリティ プロキシ サーバーにリダイレクトされないように ASA を設定できます。クラウド Web セキュリティスキャンをバイパスすると、ASA はプロキシサーバーに接続せず、最初に要求された Web サーバーからコンテンツを直接取得します。Web サーバーから応答を受け

取ると、データをクライアントに送信します。このプロセスはトラフィックの「ホワイトリスト」といいます。

ACL を使用してクラウド Web セキュリティに送信するトラフィックのクラスを設定すると、ユーザーまたはグループに基づいてトラフィックを免除する同じ結果を得ることができますが、ホワイトリストを使用した方がより簡単です。ホワイトリスト機能は、ユーザーおよびグループだけに基づき、IP アドレスには基づかないことに注意してください。

ホワイトリストをインスペクション ポリシー マップ（**policy-map type inspect scansafe**）の一部として作成しておくことで、**inspect scansafe** コマンドを使用してクラウドWebセキュリティのアクションを指定する際にそのマップを使用できます。

例

次に、HTTP および HTTPS インスペクション ポリシー マップの同じユーザーおよびグループをホワイトリストに記載する例を示します。

```
ciscoasa(config)# class-map type inspect scansafe match-any whitelist1
ciscoasa(config-cmap)# match user user1 group cisco
ciscoasa(config-cmap)# match user user2
ciscoasa(config-cmap)# match group group1
ciscoasa(config-cmap)# match user user3 group group3
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# https
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザーとグループのインスペクション クラス マップを作成します。
inspect scansafe	このクラスのトラフィックに対するクラウドWebセキュリティインスペクションをイネーブルにします。
match user group	ユーザーまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
whitelist	トラフィックのクラスでホワイトリストアクションを実行します。

match username

FTPユーザー名に関して一致条件を設定するには、クラスマップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match username** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **username regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **username regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラスマップを指定します。

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
クラス マップまたはポリシー 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
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップに入力できるエントリは 1 つのみです。

例

次に、FTP インスペクション クラス マップに FTP ユーザー名に関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect ftp match-all ftp_class1
ciscoasa(config-cmap)# match username regex class ftp_regex_user
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match uuid

DCERPC メッセージの汎用一意識別子（UUID）に関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match uuid** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match［ **not** ］**uuid** *type*
no match［ **not** ］**uuid** *type*

構文の説明

type 照合する UUID タイプ。次のいずれかが必要です。

- **ms-rpc-epm**：Microsoft RPC EPM メッセージを照合します。
- **ms-rpc-isystemactivator**：ISystemMapper メッセージを照合します。
- **ms-rpc-oxidresolver**：OxidResolver メッセージを照合します。

コマンド デフォルト

DCERPC インスペクションでは、すべてのメッセージ タイプが許可されます。

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
クラス マップまたはポリシー 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
9.5(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、DCERPC インスペクション クラス マップまたは DCERPC インスペクション ポリシーマップで設定できます。このコマンドを使用すると、DCERPC UUID に基づいてトラフィックをフィルタ処理できます。その後、リセットしたり、一致するトラフィックをログに記録したりすることができます。

例

次に、DCERPC メッセージに含まれる ms-rpc-isyustemactivator UUID に関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect dcerpc dcerpc-cmap

ciscoasa(config-cmap)# match uuid ms-rpc-isystemactivator
```

関連コマンド

コマンド	説明
class-map type inspect	インスペクション クラス マップを作成します。
policy-map type inspect	インスペクション ポリシー マップを作成します。

match version

GTP インスペクションで GTP バージョンに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match version** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **version** [*version_id* | **range** *lower_range upper_range*]
no match [**not**] **version** [*version_id* | **range** *lower_range upper_range*]

構文の説明

version_id	バージョンを 0 ～ 255 の範囲で指定します。
range *lower_range upper_range*	バージョンの下限および上限を指定します。

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
ポリシー 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
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、GTP ポリシー マップで設定できます。

例

次に、GTP インスペクション ポリシー マップにメッセージ バージョンに関して一致条件を設定する例を示します。

```
ciscoasa(config-pmap)# match version 1
```

関連コマンド

コマンド	説明
inspect gtp	GTP トラフィックのインスペクションを設定します。

max-area-addresses

IS-IS エリアの追加の手動アドレスを設定するには、ルータ ISIS コンフィギュレーション モードで **max-area-addresses** コマンドを使用します。手動のアドレスを無効にするには、このコマンドの **no** 形式を使用します。

max-area-addresses *number*
no max-area-addresses *number*

構文の説明

number	追加するマニュアル アドレスの数。範囲は3 ～ 234 です。

コマンド デフォルト

IS-IS エリア用のマニュアル アドレスは設定されません。

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 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

このコマンドにより、追加マニュアル アドレスを設定することでIS-IS エリアのサイズを最大化できるようになります。各マニュアルアドレスを作成するには、追加するアドレスの数を指定し、NET アドレスを割り当てます。

例

次に、3 つのアドレスを設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# max-are-addreses 3
```

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。

コマンド	説明
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。
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。

コマンド	説明
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。
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 ASA のデータベースに更新されずに存在する最長時間を設定します。
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。

コマンド	説明
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。
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。

max-failed-attempts

サーバーグループ内の所定のサーバーが停止するまでに、サーバーで許可される AAA トランザクションの失敗数を指定するには、AAA サーバー グループ コンフィギュレーション モードで **max-failed-attempts** コマンドを使用します。この指定を削除して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。

max-failed-attempts*number*
nomax-failed-attempts

構文の説明

number	前述の **aaa-server** コマンドに指定されているサーバーグループの特定のサーバーに対して許可されている AAA トランザクションの失敗数を指定する 1 ～ 5 の範囲の整数。

コマンド デフォルト

number のデフォルト値は 3 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
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

このコマンドを発行する前に、AAA サーバまたは AAA サーバ グループを設定しておく必要があります。

例

```
ciscoasa
(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa
(config-aaa-server-group)# max-failed-attempts 4
ciscoasa
(config-aaa-server-group)#
```

関連コマンド

コマンド	説明
aaa-server *server-tag***protocol** *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、グループ固有の AAA サーバー パラメータおよびグループ内のすべてのホストに共通の AAA サーバー パラメータを設定します。
clear configure aaa-server	AAA サーバーのコンフィギュレーションをすべて削除します。
show running-config aaa	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。

max-forwards-validation

Max-forwardsヘッダーフィールドが0かチェックするには、パラメータ コンフィギュレーション モードで **max-forwards-validation** 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。

max-forwards-validation action { **drop** | **drop-connection** | **reset** | **log** } [**log**]
no max-forwards-validation action { **drop** | **drop-connection** | **reset** | **log** } [**log**]

構文の説明

drop	検証発生時にパケットをドロップします。
drop-connection	違反が発生した場合、接続をドロップします。
reset	違反が発生した場合、接続をリセットします。
log	違反が発生した場合、スタンドアロンまたは追加のログを記録することを指定します。任意のアクションと関連付けることができます。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、宛先へのホップの数をカウントします。宛先に達する前に0になることができません。

例

次に、SIP インスペクション ポリシー マップに最大転送数の検証をイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect sip sip_map
```

```
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# max-forwards-validation action 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。
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。

max-header-length

HTTP ヘッダーの長さに基づいて HTTP トラフィックを制限するには、**http-map** コマンドを使用してアクセスできる HTTP マップ コンフィギュレーション モードで **max-header-length** コマンドを使用します。こ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。

max-header-length { **request** *bytes* [**response** *bytes*] | **response** *bytes* } **action** { **allow** | **reset** | **drop** } [**log**]
no max-header-length { **request** *bytes* [**response** *bytes*] | **response** *bytes* } **action** { **allow** | **reset** | **drop** } [**log**]

構文の説明

action	メッセージがこのコマンド インスペクションに合格しなかったときに実行されるアクションです。
allow	メッセージを許可します。
drop	接続を閉じます。
bytes	バイト数です。範囲は 1 ～ 65535 です。
log	（任意）syslog を生成します。
request	要求メッセージ。
reset	クライアントおよびサーバーに TCP リセット メッセージを送信します。
response	（任意）応答メッセージ。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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
HTTP 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

max-header-length コマンドを有効にすると、ASA は設定された制限内の HTTP ヘッダーがあるメッセージのみを許可し、その他のメッセージの場合には指定されたアクションを実行します。ASA に TCP 接続をリセットさせて、必要に応じて、syslog エントリを作成させるには、**action** キーワードを使用します。

例

次に、HTTP 要求を HTTP ヘッダーが 100 バイトを超えない要求に制限する例を示します。ヘッダーが大きすぎる場合、ASA は TCP 接続をリセットして、syslog エントリを作成します。

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# max-header-length request bytes 100 action log reset
ciscoasa(config-http-map)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug appfw	拡張HTTPインスペクションに関連するトラフィックの詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
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。

max-lsp-lifetime

ASA のデータベースで更新されることなく、LSP を保持できる最大時間を設定するには、ルータ コンフィギュレーション モードで **max-lsp-lifetime** コマンドを使用します。デフォルトの有効期間に戻すには、このコマンドの **no** 形式を使用します。

max-lsp-lifetime *seconds*
nomax-lsp-lifetime

構文の説明

seconds	LSP のライフタイム（秒数）。指定できる範囲は 1 ～ 65535 です。

コマンド デフォルト

デフォルト値は 1200 秒（20 分）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
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

更新 LSP の着信前にライフタイムを超えると、LSP がデータベースからドロップされます。

lsp-refresh-interval コマンドを使用して LSP の更新間隔を変更する場合、LSP の最大有効期間を調整する必要がある場合があります。LSP は、ライフタイムが経過するまで定期的にリフレッシュされる必要があります。**lsp-refresh-interval** コマンドに対して設定される値は、**max-lsp-lifetime** コマンドに対して設定される値よりも小さな値である必要があり、そうでない場合、リフレッシュされる前に LSP がタイムアウトします。LSP 間隔と比べて LSP ライフタイムを大幅に少なくするという設定ミスをした場合、ソフトウェアが LSP リフレッシュ間隔を減らして、LSP がタイムアウトしないようにします。

各コマンドでより大きな値を使用して、制御トラフィックを削減することができます。この場合、クラッシュしたルータや到達不能のルータからの古い LSP がより長くデータベースで保持されるようになり（そのために無駄なコストが発生する）、未検出の不適切な LSP がアクティブなままとなる（非常にまれ）リスクも増大します。

例

次に、40 分間の LSP ライフタイムを設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# max-lsp-lifetime 2400
```

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。
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。

コマンド	説明
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。
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。

コマンド	説明
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 ASA のデータベースに更新されずに存在する最長時間を設定します。
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。
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。

コマンド	説明
summary-address	IS-IS の集約アドレスを作成します。

maximum-paths（BGP）

ルーティング テーブルにインストールできる並列 BGP ルートの最大数を制御するには、アドレス ファミリ コンフィギュレーション モードで maximum-paths 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。

maximum-paths [**ibgp**] *number-of-paths*
no maximum-paths [**ibgp**] *number-of-paths*

構文の説明

ibgp	（オプション）ルーティング テーブルにインストールできる内部 BGP ルートの最大数を制御できます。
number-of-paths	ルーティング テーブルにインストールするルートの数。

コマンド デフォルト

デフォルトでは、BGP はルーティング テーブルにベストパスを 1 つだけインストールします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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
アドレスファミリ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

maximum-paths コマンドは、BGP ピアリング セッションに等コストまたは非等コスト マルチパス ロード シェアリングを設定するために使用されます。ルートを BGP ルーティング テーブル内のマルチパスとして導入する場合、ルートはすでにある他のルートと同じネクスト ホップを持つことはできません。BGP ルーティング プロセスは、BGP マルチパス ロード シェアリングが設定されている場合、BGP ピアに最適パスをアドバタイズします。等コスト ルートの場合、最下位のルータ ID を持つネイバーからのパスは、ベストパスとしてアドバタイズされます。

BGP 等コスト マルチパス ロード シェアリングを設定するには、すべてのパス属性を同じにする必要があります。パスの属性には、重み値、ローカル プリファレンス、自律システム パス

（長さだけでなく、属性全体）、オリジン コード、MED、および Interior Gateway Protocol（IGP）のディスタンスが含まれます。

例

次に、2 つの並列 iBGP パスをインストールする例を示します。

```
ciscoasa(config)# router bgp 3
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

関連コマンド

コマンド	説明
show bgp	BGP ルーティング テーブル内のエントリを表示します。

maximum-paths（IS-IS）

IS-IS プロトコルのマルチパス ロード シェアリングを設定するには、ルータ ISIS コンフィギュレーション モードで **maximum-paths** コマンドを使用します。ISIS ルートのマルチパス ロード シェアリ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。

maximum-paths *number-of-paths*
no maximum-paths *number-of-paths*

構文の説明

number-of-paths	ルーティング テーブルにインストールするルートの数。指定できる範囲は 1 ～ 8 です。

コマンド デフォルト

デフォルトでは、IS-IS はルーティング テーブルにベストパスを 1 つだけインストールします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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 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

maximum-paths コマンドは、ASA で ECMP が設定されている場合に IS-IS マルチパス ロード シェアリングを設定するために使用されます。

例

次に、ルーティング テーブルの最大パス数を 8 に設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# maximum-paths 8
```

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。

コマンド	説明
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。
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。

コマンド	説明
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。
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 ASA のデータベースに更新されずに存在する最長時間を設定します。
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。

コマンド	説明
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-ISIPプレフィックスにハイプライオリティを割り当てます。
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。

max-object-size

WebVPN セッションに対してが ASA キャッシュできるオブジェクトの最大サイズを設定するには、キャッシュモードで max-object-size コマンドを使用します。サイズを変更するには、このコマンドを再度使用します。

max-object-size*integerrange*

構文の説明

integer range	0 ～ 10000 KB

コマンド デフォルト

1000 KB

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

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
キャッシュモード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

最大オブジェクトサイズは、最小オブジェクトサイズよりも大きい値である必要があります。キャッシュ圧縮が有効になっている場合、ASA では、オブジェクトを圧縮してからサイズが計算されます。

例

次に、最大オブジェクト サイズを 4000 KB に設定する例を示します。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa(config-webvpn-cache)# max-object-size
 4000
ciscoasa(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードを開始します。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシュをディセーブルにします。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシュに関する再確認ポリシーを設定します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

max-retry-attempts（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。

要求がタイムアウトされるまでに ASA が失敗した SSO 認証を再試行できる回数を設定するには、特定の SSO サーバータイプの webvpn コンフィギュレーション モードで **max-retry-attempts** 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。

max-retry-attempts *retries*
nomax-retry-attempts

構文の説明

retries	ASA が失敗した SSO 認証を再試行する回数。指定できる範囲は 1 ～ 5 回です。

コマンド デフォルト

このコマンドのデフォルト値は 3 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
クラス マップ タイプ正規表現コンフィギュレーション	• 対応	—	• 対応	—	—
config-webvpn-sso-saml-idp	• 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。ASA は、現在、SiteMinder-type の SSO サーバーと SAML POST-type の SSO サーバーをサポートしています。

このコマンドは SSO サーバーの両タイプに適用されます。

一度 SSO 認証をサポートするように ASA を設定すると、必要に応じて、2 つのタイムアウトパラメータを調整できます。

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

例

次に、webvpn-sso-siteminder コンフィギュレーション モードを開始し、my-sso-server という名前の SiteMinder SSO サーバ名に対する認証再試行を 4 つ設定する例を示します。

```
ciscoasa(config-webvpn)# sso-server my-sso-server type siteminder
ciscoasa(config-webvpn-sso-siteminder)#
max-retry-attempts 4
ciscoasa(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
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。
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。
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。

max-uri-length

HTTP 要求メッセージの URI の長さに基づいて HTTP トラフィックを制限するには、**http-map** コマンドを使用してアクセスできる HTTP マップ コンフィギュレーション モードで **max-uri-length** コマンドを使用します。こ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。

max-uri-length *bytes* **action** { **allow** | **reset** | **drop** } [**log**]
no max-uri-length *bytes* **action** { **allow** | **reset** | **drop** } [**log**]

構文の説明

action	メッセージがこのコマンド インスペクションに合格しなかったときに実行されるアクションです。
allow	メッセージを許可します。
drop	接続を閉じます。
bytes	バイト数です。範囲は 1 ～ 65535 です。
log	（任意）syslog を生成します。
reset	クライアントおよびサーバに TCP リセット メッセージを送信します。

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
HTTP 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

max-uri-length コマンドを有効にすると、ASA は設定された制限内の URI があるメッセージのみを許可し、それ以外のメッセージには指定されたアクションを実行します。ASA に TCP 接続をリセットさせて、Syslog エントリを作成させるには、**action** キーワードを使用します。

長さが設定された値以下のURIが許可されます。それ以外の場合には、指定されたアクションが実行されます。

例

次に、HTTP 要求を URI が 100 バイトを超えない要求に制限する例を示します。URI が大きすぎる場合、ASA は TCP 接続をリセットし、syslog エントリを作成します。

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# max-uri-length 100 action reset log
ciscoasa(config-http-map)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug appfw	拡張HTTPインスペクションに関連するトラフィックの詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
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。

mcast-group

VXLAN VNI インターフェイスのマルチキャストグループを指定するには、インターフェイス コンフィギュレーションモードで**mcast-group** コマンドを使用します。このグループを削除するには、このコマンドの **no** 形式を使用します。

mcast-group *mcast_ip*
nomcast-group

構文の説明

mcast_ip	マルチキャストグループの IP アドレス（IPv4 または IPv6）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
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。
9.20(1)	このコマンドで IPv6 をサポートするようになりました。

使用上のガイドライン

ASA がピア VTEP の背後にあるデバイスにパケットを送信する場合、ASA には次の 2 つの重要な情報が必要です。

- リモート デバイスの宛先 MAC アドレス
- ピア VTEP の宛先 IP アドレス

ASA がこの情報を検出するには 2 つの方法あります。

- 単一のピア VTEP IP アドレスを ASA に静的に設定できます。

手動で複数のピアを定義することはできません。

ASA が VXLAN カプセル化 ARP ブロードキャストを VTEP に送信し、エンド ノードの MAC アドレスを取得します。

- マルチキャストグループは、**mcast-group** コマンドを使用して VNI インターフェイスごとに（または VTEP 全体に）設定できます。

ASA は、IP マルチキャスト パケット内の VXLAN カプセル化 ARP ブロードキャスト パケットを VTEP 送信元インターフェイスを経由して送信します。この ARP 要求への応答により、ASA はリモート VTEP の IP アドレスと、リモート エンド ノードの宛先 MAC アドレスの両方を取得することができます。

ASA は VNI インターフェイスのリモート VTEP IP アドレスに対する宛先 MAC アドレスのマッピングを維持します。

VNI インターフェイスに対してマルチキャストグループを設定しない場合、使用可能な場合は、VTEP 送信元インターフェイス設定のデフォルトグループが使用されます（**default-mcast-group** コマンド）。**peer ip** コマンドを使用して VTEP 送信元インターフェイスに対して手動で VTEP ピア IP を設定した場合、VNI インターフェイスに対してマルチキャストグループは指定できません。マルチキャストは、マルチ コンテキスト モードではサポートされていません。

例

次に、VNI 1 インターフェイスを設定し、マルチキャスト グループ 236.0.0.100 を指定する例を示します。

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。

コマンド	説明
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN送信元インターフェイスがNVE専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNIインターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ2転送テーブル（MACアドレステーブル）を表示します。
show nve	NVEインターフェイスのパラメータ、ステータス、および統計情報とキャリアインターフェイス（送信元インターフェイス）のステータス、このNVEをVXLAN VTEPとして使用するVNI、ならびにこのNVEインターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレントモードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

mcc

GTP インスペクションで IMSI プレフィックス フィルタリングのモバイル国コードおよびモバイルネットワークコードを識別するには、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 **mcc** 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。

［ **drop** ］ **mcc** *country_code* **mnc** *network_code*
no ［ **drop** ］ **mcc** *country_code* **mnc** *network_code*

構文の説明

drop	プレフィックスの組み合わせに一致する接続をドロップすることを指定します。結果として、指定された組み合わせが不要なプレフィックスを示していることになります。 このキーワードを指定しない場合、接続は許可されるプレフィックスの組み合わせと一致する必要があります。 特定のマップ内のすべてのプレフィックス フィルタリングは、「すべてドロップ」または「すべて許可」で統一されている必要があります。
country_code	モバイル国コードを識別するゼロ以外の 3 桁の値。エントリが 1 桁または 2 桁の場合には、その先頭に 0 が付加されて 3 桁の値が作成されます。
network_code	ネットワーク コードを識別する 2 桁または 3 桁の値。

コマンド デフォルト

デフォルトでは、GTP インスペクションは有効な MCC/MNC の組み合わせをチェックしません。

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
7.0(1)	このコマンドが追加されました。
9.16(1)	**drop** キーワードが追加されました。

使用上のガイドライン

コマンドは必要な回数入力して、ターゲットとなるすべての MCC/MNC ペアを指定できますが、ポリシーマップ内のすべてのコマンドは **mcc** または **drop mcc** である必要があります。これらのコマンドを組み合わせることはできません。

デフォルトでは、GTP インスペクションは、有効なモバイル カントリ コード（MCC）とモバイル ネットワーク コード（MNC）の組み合わせをチェックしません。IMSI プレフィックス フィルタリングを設定すると、受信パケットの IMSI の MCC と MNC が、設定された MCC と MNC の組み合わせと比較されます。次に、コマンドに基づいて次のいずれかのアクションが実行されます。

- **mcc** コマンド：一致しない場合、パケットはドロップされます。
- **drop mcc** コマンド：一致する場合、パケットはドロップされます。

モバイル カントリ コードは 0 以外の 3 桁の数字で、1 桁または 2 桁の値のプレフィックスとして 0 が追加されます。モバイル ネットワーク コードは 2 桁または 3 桁の数字です。

許可またはドロップするすべての MCC と MNC の組み合わせを追加します。デフォルトでは、ASA は MNC と MCC の組み合わせが有効であるかどうかをチェックしないため、設定した組み合わせが有効であるかどうかを確認する必要があります。MCC および MNC コードの詳細については、ITU E.212 勧告『*Identification Plan for Land Mobile Stations*』を参照してください。

例

次に、MCC を 111、MNC を 222 として、IMSI プレフィックス フィルタリングのトラフィックを識別する例を示します。

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mcc 111 mnc 222
```

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。

media-termination（廃止予定）

電話プロキシ機能へのメディア接続に使用するメディア ターミネーション インスタンスを指定するには、電話プロキシ コンフィギュレーション モードで **media-termination** コマンドを使用します。

電話プロキシ コンフィギュレーションからメディア ターミネーション アドレスを削除するには、このコマンドの **no** 形式を使用します。

media-terminationinstance_name
nomedia-termination*instance_name*

構文の説明

instance_name	メディア ターミネーション アドレスを使用するインターフェイスの名前を指定します。1 つのインターフェイスに設定できるメディア ターミネーション アドレスは 1 つだけです。

コマンド デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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
Phone-Proxy コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	コマンドが追加されました。
8.2(1)	このコマンドは、メディア ターミネーション アドレスで NAT を使用できるように更新されました。 **rtp-min-port** キーワードおよび **rtp-max-ports** キーワードがコマンドシンタックスから削除され、独立したコマンドとなりました。
9.4(1)	このコマンドは、すべての **phone-proxy** モードコマンドとともに廃止されました。

使用上のガイドライン

ASA では、次の基準を満たすメディアターミネーションの IP アドレスが設定されている必要があります。

メディア ターミネーション インスタンスでは、すべてのインターフェイスに対してグローバルなメディア ターミネーション アドレスを設定することも、インターフェイスごとにメディ

アターミネーションアドレスを設定することもできます。しかし、グローバルなメディア ターミネーション アドレスと、インターフェイスごとに設定するメディア ターミネーション アドレスは同時に使用できません。

複数のインターフェイスに対してメディア ターミネーション アドレスを設定する場合、IP 電話との通信時に ASA で使用するアドレスを、インターフェイスごとに設定する必要があります。

IP アドレスは、そのインターフェイスのアドレス範囲内で使用されていない、パブリックにルーティング可能な IP アドレスです。

メディア ターミネーション インスタンスの作成時およびメディア ターミネーション アドレスの設定時に満たす必要がある前提条件の完全なリストについては、CLI 設定ガイドを参照してください。

例

次に、media-termination address コマンドを使用して、メディア接続に使用する IP アドレスを指定する例を示します。

```
ciscoasa(config-phone-proxy)# media-termination mta_instance1
```

関連コマンド

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

media-type

メディアタイプを銅線またはファイバギガビットイーサネットに設定するには、インターフェイス コンフィギュレーション モードで **media-type** コマンドを使用します。ASA 5500 シリーズ適応型セキュリティアプライアンスの 4GE SSM でファイバ SFP コネクタが使用可能になります。メディアタイプ設定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。

media-type { **rj45** | **sfp** }
no media-type [**rj45** | **sfp**]

構文の説明

rj45	（デフォルト）メディア タイプを銅線 RJ-45 コネクタに設定します。
sfp	メディア タイプをファイバ SFP コネクタに設定します。

コマンド デフォルト

デフォルトは **rj45** 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
7.0(4)	このコマンドが追加されました。

使用上のガイドライン

sfp 設定では、固定速度（1000 Mbps）が使用されるため、**speed** コマンドを使用すると、インターフェイスにリンクパラメータをネゴシエートさせるかどうかを設定できます。**duplex** コマンドは、**sfp** ではサポートされません。

例

次に、メディア タイプを SFP に設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet1/1
ciscoasa(config-if)# media-type sfp
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、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。
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。
show running-config interface	インターフェイス コンフィギュレーションを表示します。
speed	インターフェイスの速度を設定します。

member

コンテキストをリソースクラスに割り当てるには、コンテキストコンフィギュレーションモードで**member**コマンドを使用します。コンテキストをリソースクラスから削除するには、このコマンドの **no** 形式を使用します。

member*class_name*
nomember*class_name*

構文の説明

class_name	**class** コマンドで作成したクラス名を指定します。

コマンド デフォルト

デフォルトでは、コンテキストはデフォルトのクラスに割り当てられます。

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
コンテキスト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。

使用上のガイドライン

デフォルトでは、コンテキストごとの上限値が適用されていない限り、すべてのセキュリティコンテキストがASAのリソースに無制限にアクセスできます。ただし、1つ以上のコンテキストがリソースを大量に使用しており、他のコンテキストが接続を拒否されている場合は、リソース管理を設定してコンテキストごとのリソースの使用を制限できます。ASAは、リソースクラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。

例

次に、コンテキスト テストをゴールド クラスに割り当てる例を示します。

```
ciscoasa(config-ctx)# context
 test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url
```

```
 ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold
```

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
context	セキュリティ コンテキストを設定します。
limit-resource	リソースの制限を設定します。
show resource allocation	リソースを各クラスにどのように割り当てたかを表示します。
show resource types	制限を設定できるリソース タイプを表示します。

member-interface

物理インターフェイスを冗長インターフェイスに割り当てるには、インターフェイス コンフィギュレーション モードで **member-interface** コマンドを使用します。このコマンドは、冗長インターフェイス タイプでのみ使用できます。2 つのメンバ インターフェイスを冗長インターフェイスに割り当てることができます。メンバーインターフェイスを削除するには、このコマンドの **no** 形式を使用します。冗長インターフェイスから両方のメンバ インターフェイスは削除できません。冗長インターフェイスには、少なくとも 1 つのメンバインターフェイスが必要です。

member-interface*physical_interface*
nomember-interface*physical_interface*

構文の説明

physical_interface	インターフェイス ID（**gigabitethernet 0/1** など）を指定します。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。

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
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

両方のメンバ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。たとえば、両方ともイーサネットにする必要があります。

名前が設定されている場合は、物理インターフェイスを冗長インターフェイスに追加できません。まず **no nameif** コマンドを使用して名前を削除する必要があります。

⚠

注意 コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

冗長インターフェイスペアの一部である物理インターフェイスに使用できる唯一の構成は物理パラメータ（**speed** コマンド、**duplex** コマンド、**description** コマンド、**shutdown** コマンドなど）です。また、**default** や **help** などの実行時コマンドも入力できます。

アクティブ インターフェイスをシャットダウンすると、スタンバイ インターフェイスがアクティブになります。

アクティブインターフェイスを変更するには、 **redundant-interface** コマンドを入力します。

冗長インターフェイスでは、追加した最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバー インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、冗長インターフェイスに MAC アドレスを割り当てることができます。これはメンバーインターフェイスの MAC アドレスに関係なく使用されます（**mac-address** コマンドまたは **mac-address auto** コマンドを参照）。アクティブインターフェイスがスタンバイインターフェイスにフェールオーバーした場合、同じMACアドレスが維持されるため、トラフィックが妨げられることはありません。

例

次の例では、2 つの冗長インターフェイスを作成します。

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

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。
redundant-interface	アクティブなメンバ インターフェイスを変更します。
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。

memberof

このユーザーがメンバーであるグループ名のリストを指定するには、ユーザー名属性コンフィギュレーション モードで **memberof** コマンドを使用します。この属性を構成から削除するには、このコマンドの **no** 形式を使用します。

memberof *group_1*［，*group_2*，．．．*group_n*］
no memberof *group_1*［，*group_2*，．．．*group_n*］

構文の説明

group_1 through group_n	このユーザーが所属するグループを指定します。

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
ユーザー名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
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

このユーザーが所属するグループ名のカンマ区切りリストを入力します。

例

次に、グローバル コンフィギュレーション モードを開始し、ユーザー名を newuser という名前で作成し、newuser が DevTest グループおよび管理グループのメンバであることを指定する例を示します。

```
ciscoasa(config)# username newuser nopassword
ciscoasa(config)# username newuser attributes
ciscoasa(config-username)# memberof DevTest,management
ciscoasa(config-username)#
```

関連コマンド

コマンド	説明
clear configure username	ユーザー名データベース全体または指定されたユーザー名のみをクリアします。
show running-config username	特定のユーザーまたはすべてのユーザーに対して現在実行されているユーザー コンフィギュレーションを表示します。
username	ユーザー名のデータベースを作成および管理します。

memory appcache-threshold enable

メモリ アプリケーション キャッシュのしきい値を有効にするには、コンフィギュレーション モードで **memory appcache-threshold enable** コマンドを使用します。**memory appcache-threshold,** を無効にするには、このコマンドの **no** 形式を使用します。

memoryappcache-thresholdenable
nomemoryappcache-thresholdenable

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 **memory appcache-threshold enable** コマンドは、Cisco ASA 5585-X FirePOWER SSP-60（5585-60）ではデフォルトで有効になっています。

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
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
9.10(1)	このコマンドが導入されました。

使用上のガイドライン

memory appcache-threshold を有効にすると、特定のメモリしきい値に達した後、アプリケーション キャッシュの割り当てが制限されるため、デバイスの管理性と安定性を維持するためのメモリが予約ができます。

ASA 9.10.1 リリースでは、memory appcache-threshold 機能が 5585-60 に実装され、through-the-box 接続のみに対して、アプリケーション キャッシュの割り当てが制限されていました。

このコマンドは、システム メモリの 85 % にアプリケーション キャッシュの割り当てしきい値を設定します。メモリ使用率がしきい値レベルに達すると、デバイスへの新しい through-the-box 接続がドロップされます。

コマンドの **no** 形式を使用すると、すべてのメモリ割り当て制限が検証なしに使用されます。現在の統計カウンタは、**clear memory appcache-threshold** コマンドが実行されるまで、トラブルシューティング履歴を維持するために保持されます。

9.10.1 リリースでは、SNP Conn Core 00 アプリケーション キャッシュ タイプのみが管理されます。この名前は、「show mem app-cache」の出力と一致しています。

例

次に、appcache-memory しきい値を有効にする例を示します。

```
ciscoasa(config)# memory appcache-threshold enable
```

関連コマンド

コマンド	説明
show memory appcache-threshold	メモリ appcache しきい値のステータスとヒット数を表示します。
clear memory appcache-threshold	memory appcache-threshold のヒット カウントをクリアします。

memory delayed-free-poisoner enable

delayed free-memory poisoner ツールを有効にするには、特権 EXEC モードで **memory delayed-free-poisoner enable** コマンドを使用します。delayed free-memory poisoner ツールを無効にするには、このコマンドの **no** 形式を使用します。delayed free-memory poisoner ツールを使用すると、アプリケーションによってメモリが解放された後、解放メモリの変化をモニターできます。

memorydelayed-free-poisonerenable
nomemorydelayed-free-poisonerenable

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

memory delayed-free-poisoner enable コマンドは、デフォルトで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
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

delayed free-memory poisoner ツールをイネーブルにすると、メモリ使用状況およびシステム パフォーマンスに大きな影響を及ぼします。このコマンドは、Cisco TAC の指導の下でのみ使用する必要があります。システムの使用率が高い間は、実働環境では実行しないでください。

このツールを有効にすると、ASA で実行されているアプリケーションによって、メモリ解放要求が FIFO キューに書き込まれます。要求がキューに書き込まれるたびに、それに伴うメモリ バイトのうち、下位メモリ管理には必要ないバイトが、値 0xcc で書き込まれて「改ざん」されます。

メモリ解放要求は、空きメモリ プールにある量よりも多くのメモリがアプリケーションで必要になるまで、キューに残ります。メモリが必要になると、最初のメモリ解放要求がキューから取り出され、改ざんされたメモリが検証されます。

メモリに変更がない場合、メモリは下位メモリ プールに返され、ツールは最初に要求を行ったアプリケーションからのメモリ要求を再発行します。この処理は、要求元のアプリケーションに十分なメモリが解放されるまで続きます。

改ざんされたメモリに変更があった場合、システムは強制的にクラッシュし、クラッシュの原因を突き止めるための診断出力を作成します。

delayed free-memory poisoner ツールは、定期的にキューのすべての要素を自動的に検証します。また、**memory delayed-free-poisoner validate** コマンドを使用して手動で検証を開始できます。

このコマンドの **no** 形式を実行すると、キュー内の要求で参照されるすべてのメモリが検証されずに空きメモリプールに返され、すべての統計カウンタがクリアされます。

例

次に、delayed free-memory poisoner ツールをイネーブルにする例を示します。

```
ciscoasa# memory delayed-free-poisoner enable
```

次に、delayed free-memory poisoner ツールが不正なメモリ再利用を検出した場合の出力例を示します。

```
delayed-free-poisoner validate failed because a
        data signature is invalid at delayfree.c:328.
    heap region:    0x025b1cac-0x025b1d63 (184 bytes)
    memory address: 0x025b1cb4
    byte offset:    8
    allocated by:   0x0060b812
    freed by:       0x0060ae15
Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80:                         ef cd 1c a1 e1 00 00 00  |          ........
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02  |  #.........`.h.^.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02  |  ..[...`.....l&[.
025b1cb0: 8e a5 ea 10 ff ff ff ff cc cc cc cc cc cc cc cc  |  ................
025b1cc0: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  |  ................
025b1cd0: cc cc cc cc cc cc cc cc                         |  ........
An internal error occurred.  Specifically, a programming assertion was
violated.  Copy the error message exactly as it appears, and get the
output of the show version command and the contents of the configuration
file.  Then call your technical support representative.
assertion "0" failed: file "delayfree.c", line 191
```

<xref> に、出力の重要な部分を示します。

表 *2:* 不正なメモリ使用に関する出力の説明

フィールド	説明
heap region	要求元のアプリケーションが使用できるメモリ領域のアドレス領域およびサイズ。これは、要求されたサイズと同じ値ではなく、メモリ要求が行われたときにシステムがメモリを配分できるように小さくなることがあります。
memory address	障害が検出されたメモリの位置。

フィールド	説明
byte offset	バイト オフセットはヒープ領域の先頭を基準にしており、このアドレスから始まるデータ構造を保持するためにフィールドが変更された場合には、バイト オフセットを使用してそのフィールドを見つけることができます。値が 0 か、またはヒープ領域バイト カウントよりも大きい値である場合は、問題が下位ヒープ パッケージの予期しない値であることを示している可能性があります。
allocated by/freed by	この特定のメモリ領域に関して実施された最後の malloc/calloc/realloc および解放要求の命令アドレス。
Dumping...	検出された障害がヒープ メモリ領域の先頭にどれだけ近いかに応じて、1 つまたは 2 つのメモリ領域のダンプ。システム ヒープ ヘッダーに続く 8 バイトは、このツールがさまざまなシステム ヘッダー値のハッシュとキュー リンクを保持するために使用するメモリです。システム ヒープ トレーラが検出されるまでの領域内のそれ以外のバイトは、0xcc に設定する必要があります。

関連コマンド

コマンド	説明
clear memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューおよび統計情報をクリアします。
memory delayed-free-poisoner validate	delayed free-memory poisoner ツールのキュー内要素の検証を強制実行します。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況に関する要約を表示します。

memory delayed-free-poisoner validate

memory delayed-free-poisoner キューのすべての要素を強制的に検証するには、特権 EXEC モードで **memory delayed-free-poisoner validate** コマンドを使用します。

memorydelayed-free-poisonervalidate

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
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

memory delayed-free-poisoner validate コマンドを発行する場合は、事前に **memory delayed-free-poisoner enable** コマンドを使用して delayed free-memory poisoner ツールを有効にする必要があります。

memory delayed-free-poisoner validate コマンドにより、**memory delayed-free-poisoner** キューの各要素が検証されます。要素に予期しない値が含まれている場合、システムは強制的にクラッシュし、クラッシュの原因を突き止めるための診断出力を作成します。予期しない値が存在しない場合、要素はキューに残り、ツールによって正常に処理されます。**memory delayed-free-poisoner validate** コマンドを実行しても、キュー内のメモリはシステムメモリプールに返されません。

（注） delayed free-memory poisoner ツールは、定期的にキューのすべての要素を自動的に検証します。

例

次に、**memory delayed-free-poisoner** キューのすべての要素を検証する例を示します。

```
ciscoasa# memory delayed-free-poisoner validate
```

関連コマンド

コマンド	説明
clear memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューおよび統計情報をクリアします。
memory delayed-free-poisoner enable	delayed free-memory poisoner ツールをイネーブルにします。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況に関する要約を表示します。

memory caller-address

コールトレースまたは発信元 PC 用にプログラムメモリの特定の範囲を設定して、メモリの問題を特定できるようにするには、特権 EXEC モードで **memory caller-address** コマンドを使用します。発信元PCは、メモリ割り当てプリミティブを呼び出したプログラムのアドレスです。アドレス範囲を削除するには、このコマンドの **no** 形式を使用します。

memorycaller-address*startPCendPC*
nomemorycaller-address

構文の説明

endPC	メモリブロックの終了アドレス範囲を指定します。
startPC	メモリブロックの開始アドレス範囲を指定します。

コマンド デフォルト

メモリを追跡できるように、実際の発信元 PC が記録されます。

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
7.0	このコマンドが追加されました。

使用上のガイドライン

メモリの問題を特定のメモリブロックに限定するには、**memory caller-address** コマンドを使用します。

場合によっては、メモリ割り当てプリミティブの実際の発信元 PC が、プログラムの多くの場所で使用されている既知のライブラリ関数であることがあります。プログラムの個々の場所を特定するには、そのライブラリ関数の開始プログラム アドレスおよび終了プログラム アドレスを設定し、それによってライブラリ関数の呼び出し元のプログラムアドレスを記録します。

（注） 発信元アドレスの追跡を有効にすると、ASA のパフォーマンスが一時的に低下することがあります。

例

次に、**memory caller-address** コマンドで設定したアドレスの範囲、および **show memory-caller address** コマンドの表示結果の例を示します。

```
ciscoasa# memory caller-address 0x00109d5c 0x00109e08

ciscoasa# memory caller-address 0x009b0ef0 0x009b0f14

ciscoasa# memory caller-address 0x00cf211c 0x00cf4464

ciscoasa# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
show memory	物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について要約を表示します。
show memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。
show memory profile	ASA のメモリ使用状況（プロファイリング）に関する情報を表示します。
show memory-caller address	ASA 上に設定されているアドレス範囲を表示します。

memory logging

メモリロギングを有効にするには、グローバル コンフィギュレーション モードで **memory logging** コマンドを使用します。メモリロギ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。

memory logging [**1024-4194304**] [**wrap**] [**size** [**1-2147483647**]] [**process** *process-name*] [**context** *context-name*]
nomemorylogging

構文の説明

1024-4194304	メモリ ロギング バッファのロギング エントリの数を指定します。指定する必要がある引数はこれだけです。
context *context-name*	モニターする仮想コンテキストおよびコンテキスト名を指定します。
process *process-name*	モニターするプロセスおよびプロセス名を指定します。 （注） Checkheaps プロセスは、非標準の方法でメモリ アロケータを使用するため、プロセスとして完全に無視されます。
size 1-2147483647	モニターするサイズおよびエントリ数を指定します。
wrap	バッファのラップ時にバッファを保存します。保存できるのは一度だけです。複数回ラップされると上書きされる可能性があります。バッファがラップすると、そのデータの保存をイネーブルにするトリガーがイベント マネージャに送信されます。

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
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
9.4(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

メモリ ロギング パラメータを変更するには、それをディセーブルにしてから、再度イネーブルにします。

例

次に、メモリ ロギングをイネーブルにする例を示します。

```
ciscoasa
(config)#
memory logging 202980
```

関連コマンド

コマンド	説明
event memory-logging-wrap	メモリ ロギング ラップ イベントへの応答をイネーブルにします。
show memory logging	メモリ ロギングの結果を表示します。

memory profile enable

メモリ使用状況のモニタリング（メモリプロファイリング）を有効にするには、特権 EXEC モードで **memory profile enable** コマンドを使用します。メモリプロファイルリ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。

memoryprofileenablepeak*peak_value*
nomemoryprofileenablepeak*peak_value*

構文の説明

peak_value	メモリ使用状況のスナップショットを使用率ピーク バッファに保存するメモリ使用状況しきい値を指定します。このバッファの内容を後で分析して、システムのピーク時のメモリ ニーズを判断できます。

コマンド デフォルト

デフォルトでは、メモリ プロファイリングはディセーブルになっています。

コマンド モード

次の表に、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	このコマンドが追加されました。

使用上のガイドライン

メモリプロファイリングを有効にする前に、**memory profile text** コマンドを使用して、プロファイリングするメモリのテキスト範囲を設定する必要があります。

一部のメモリは、**clear memory profile** コマンドを入力するまでプロファイリングシステムによって保持されます。**show memory status** コマンドの出力を参照してください。

（注） メモリプロファイリングをイネーブルにすると、ASA のパフォーマンスが一時的に低下する場合があります。

次に、メモリ プロファイリングをイネーブルにする例を示します。

```
ciscoasa# memory profile enable
```

関連コマンド

コマンド	説明
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
show memory profile	ASA のメモリ使用状況（プロファイリング）に関する情報を表示します。

memory profile text

プロファイリングするメモリのプログラムテキスト範囲を設定するには、特権EXECモードで **memory profile text** コマンドを使用します。無効にするには、このコマンドの **no** 形式を使用します。

memory profile text { *startPC endPC* | **all** *resolution* }
no memory profile text { *startPC endPC* | **all** *resolution* }

構文の説明

all	メモリブロックのテキスト範囲全体を指定します。
endPC	メモリブロックの終了テキスト範囲を指定します。
resolution	ソース テキスト領域の追跡精度を指定します。
startPC	メモリブロックの開始テキスト範囲を指定します。

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	このコマンドが追加されました。

使用上のガイドライン

テキスト範囲が小さい場合、精度を「4」にすると、命令への呼び出しが正常に追跡されます。テキスト範囲が大きい場合、精度を粗くしても初回通過には十分であり、範囲は次回の通過でさらに小さな領域にまで絞り込むことができます。

メモリプロファイリングを開始するには、**memory profile text** コマンドでテキスト範囲を入力した後、**memory profile enable** コマンドを入力する必要があります。デフォルトでは、メモリプロファイリングはディセーブルになっています。

（注） メモリプロファイリングをイネーブルにすると、ASAのパフォーマンスが一時的に低下する場合があります。

例

次に、精度を 4 にして、プロファイリングするメモリのテキスト範囲を設定する例を示します。

```
ciscoasa# memory profile text 0x004018b4 0x004169d0 4
```

次に、メモリ プロファイリングのテキスト範囲のコンフィギュレーションおよびステータス（OFF）を表示する例を示します。

```
ciscoasa# show memory profile
InUse profiling: OFF Peak profiling: OFF Profile: 0x004018b4-0x004169d0(00000004)
```

（注） メモリプロファイリングを開始するには、**memory profile enable** コマンドを入力する必要があります。デフォルトでは、メモリ プロファイリングはディセーブルになっています。

関連コマンド

コマンド	説明
clear memory profile	メモリ プロファイリング機能によって保持されているバッファをクリアします。
memory profile enable	メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。
show memory profile	ASA のメモリ使用状況（プロファイリング）に関する情報を表示します。
show memory-caller address	ASA 上に設定されているアドレス範囲を表示します。

memory-size

WebVPN のさまざまなコンポーネントがアクセスできる ASA 上のメモリ容量を設定するには、webvpn モードで **memory-size** コマンドを使用します。設定されたメモリ容量（KB 単位）または合計メモリの割合として、メモリ容量を設定できます。設定されたメモリサイズを削除するには、このコマンドの **no** 形式を使用します。

（注） 新しいメモリ サイズ設定を有効にするには、リブートが必要です。

memory-size { **percent** | **kb** } *size*
no memory-size [{ **percent** | **kb** } *size*]

構文の説明

kb	メモリ容量をキロバイト単位で指定します。
percent	ASA 上のメモリ容量を合計メモリの割合として指定します。
size	メモリ容量を KB 単位または合計メモリの割合として指定します。

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
webvpn モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

設定したメモリ容量は、ただちに割り当てられます。このコマンドを設定する前に、show memory を使用して、使用可能なメモリ容量を確認してください。設定に合計メモリの割合を使用する場合は、設定した値が使用可能な割合を下回っていることを確認してください。設定にキロバイトの値を使用する場合は、設定した値がキロバイト単位の使用可能なメモリ容量を下回っていることを確認してください。

例

次に、WebVPN メモリ サイズを 30 % に設定する例を示します。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 memory-size percent 30
ciscoasa(config-webvpn)#
ciscoasa(config-webvpn)# reload
```

関連コマンド

コマンド	説明
show memory webvpn	WebVPN メモリ使用状況の統計情報を表示します。

memory tracking enable

ヒープメモリ要求の追跡を有効にするには、特権 EXEC モードで **memory tracking enable** コマンドを使用します。メモリ追跡を無効にするには、このコマンドの **no** 形式を使用します。

memorytrackingenable
nomemorytrackingenable

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
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(8)	このコマンドが追加されました。

使用上のガイドライン

ヒープメモリ要求を追跡するには、**memory tracking enable** コマンドを使用します。メモリ追跡を無効にするには、このコマンドの **no** 形式を使用します。

メモリ追跡をイネーブルにする前に、app-agent heartbeat コマンドのデフォルトの間隔とカウント値を次のように変更してください。

app-agent heartbeat interval 6000 retry-count 6

例

次に、ヒープ メモリ要求の追跡をイネーブルにする例を示します。

```
ciscoasa# memory tracking enable
```

関連コマンド

コマンド	説明
clear memory tracking	現在収集されているすべての情報をクリアします。
show memory tracking	現在割り当てられているメモリを表示します。

コマンド	説明
show memory tracking address	ツールの追跡対象である現在割り当てられている各メモリのサイズ、位置、および最上位呼び出し元関数を一覧表示します。
show memory tracking dump	このコマンドは、指定されたメモリアドレスのサイズ、位置、呼び出しスタックの一部、およびメモリダンプを表示します。
show memory tracking detail	ツール内部の動作の洞察に使用されるさまざまな内部詳細情報を表示します。

memory-utilization

システムメモリが事前に定義されたレベルまで使用されたときに、自動的にリブートするか、またはクラッシュするようにASAを設定するには、memory utilizationコマンドを使用します。メモリ使用状況が設定されたしきい値の上限に到達すると、システムは自動的にリロードします。しきい値は90 ～ 99 %の範囲です。

memory-utilization reload-threshold < **%** >
memory-utilization reload-threshold < **%** > [**crashinfo**]

構文の説明

reload-threshold	システム メモリのしきい値の上限を指定します。
crashinfo	（オプション）使用する場合、システム リロードの前にクラッシュ情報を保存することを指定します。

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	• 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

一般にメモリ使用状況が極めて高くなる環境に遭遇することがわかっているシステム上にこの機能を設定しないことを推奨します。システムリロードの前にクラッシュ情報ファイルを生成するには、オプションのcrashinfo引数を使用します。

例

次に、ASA 上にメモリ使用状況機能を設定する例を示します。

```
ciscoasa# memory-utilization reload-threshold 95
```

関連コマンド

コマンド	説明
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
memory profile enable	メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。
clear memory profile	メモリ プロファイリング機能によって保持されているバッファをクリアします。
show memory profile	ASA のメモリ使用状況（プロファイリング）に関する情報を表示します。

merge-dacl

ダウンロード可能 ACL と、RADIUS パケットから Cisco AV ペアで受信した ACL をマージするには、AAA サーバー グループ コンフィギュレーション モードで **merge-dacl** コマンドを使用します。ダウンロード可能 ACL と、RADIUS パケットから Cisco AV ペアで受信した ACL のマージを無効にするには、このコマンドの **no** 形式を使用します。

merge dacl { **before_avpair** | **after_avpair** }
nomergedacl

構文の説明

after_avpair	ダウンロード可能 ACL のエントリを Cisco AV ペアのエントリの後に配置する必要があることを指定します。このオプションは、VPN 接続にのみ適用されます。VPN ユーザーの場合は、ACL は Cisco AV ペア ACL、ダウンロード可能 ACL、および ASA で設定される ACL の形式になります。このオプションでは、ダウンロード可能 ACL と AV ペア ACL を結合するかどうかを決定します。ASA で設定されている ACL には適用されません。
before_avpair	ダウンロード可能 ACL のエントリを Cisco AV ペア のエントリの前に配置する必要があることを指定します。

コマンド デフォルト

デフォルト設定は **no merge dacl** で、ダウンロード可能な ACL は Cisco AV ペア ACL とマージされません。

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 グループ コンフィギュレーション	• 対応	• 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

AV ペアおよびダウンロード可能 ACL の両方を受信した場合は、AV ペアが優先し、使用されます。

例

次の例では、ダウンロード可能 ACL のエントリが Cisco AV ペアのエントリの前に配置されるように指定しています。

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

関連コマンド

コマンド	説明
aaa-server host	サーバーと、そのサーバーが属する AAA サーバー グループを識別します。
aaa-server protocol	サーバー グループ名とプロトコルを識別します。
max-failed-attempts	次のサーバーを試す前にグループ内の AAA サーバーに送信する要求の最大数を指定します。

message-length

設定された最大の長さを満たさない DNS パケットをフィルタリングするには、パラメータ コンフィギュレーション モードで message-length コマンドを使用します。このコマンドを削除するには、**no** 形式を使用します。

message-length maximum { *length* | **client** { *length* | **auto** } | **server** { *length* | **auto** } }
no message-length maximum { *length* | **client** { *length* | **auto** } | **server** { *length* | **auto** } }

構文の説明

length	DNS メッセージの最大許容バイト数（512 ～ 65535）を指定します。
client {*length* | **auto**}	クライアント DNS メッセージの最大許容バイト数（512 ～ 65535）を指定します。最大長をリソースレコードと同じ値に設定する場合は、**auto** を指定します。
server {*length* | **auto**}	サーバー DNS メッセージの最大許容バイト数（512 ～ 65535）を指定します。最大長をリソースレコードと同じ値に設定する場合は、**auto** を指定します。

コマンド デフォルト

デフォルトの検査では、DNS メッセージの最大長は 512、クライアントの長さは **auto** に設定されます。

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
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

DNS インスペクション マップのパラメータとして DNS メッセージの最大長を設定できます。

例

次に、DNS インスペクション ポリシー マップで DNS メッセージの最大長を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
```

```
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length 512
ciscoasa(config-pmap-p)# message-length client auto
```

関連コマンド

コマンド	説明
parameter	ポリシー マップ コンフィギュレーション モードからパラメータ コンフィギュレーション モードを開始します。
policy-map type inspect dns	DNS インスペクション ポリシー マップを作成します。

message-tag-validation

M3UA メッセージに含まれる特定のフィールドの内容を検証するには、パラメータ コンフィギュレーション モードで **message-tag-validation** 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 モードにアクセスするには、まず **policy-map type inspect m3ua** コマンドを入力します。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。

message-tag-validation { **dupu** | **error** | **notify** }
no message-tag-validation { **dupu** | **error** | **notify** }

構文の説明

dupu	宛先ユーザー部使用不可（DUPU）メッセージの検証をイネーブルにします。ユーザー/理由フィールドが存在し、有効な理由およびユーザー コードのみが含まれている必要があります。
error	エラー メッセージの検証をイネーブルにします。すべての必須フィールドが存在し、許可された値のみが含まれている必要があります。各エラー メッセージには、そのエラー コードの必須フィールドが含まれている必要があります。
notify	通知メッセージの検証をイネーブルにします。ステータス タイプおよびステータス情報フィールドには、許可された値のみが含まれている必要があります。

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
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
9.7(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

特定のフィールドの内容がチェックされ、指定された M3UA メッセージ タイプに関して検証されるようにするには、このコマンドを使用します。検証で合格しなかったメッセージはドロップされます。

例

次に、M3UA インスペクションでの DUPU、エラー、および通知メッセージの検証をイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-tag-validation dupu
ciscoasa(config-pmap-p)# message-tag-validation error
ciscoasa(config-pmap-p)# message-tag-validation notify
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インスペクションをイネーブルにします。
policy-map type inspect	インスペクション ポリシー マップを作成します。
show service-policy inspect m3ua	M3UA 統計情報を表示します。

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するには、ルータ ISIS コンフィギュレーション モードで **metric** コマンドを使用します。メトリック値を無効にして、デフォルトメトリック値の 10 に戻すには、このコマンドの **no** 形式を使用します。

metric *default-value* [**level-1** | **level-2**]
no metric *default-value* [**level-1** | **level-2**]

構文の説明

default-value	リンクに割り当てられ、宛先へのリンクを介したパス コストを計算するために使用されるメトリック値。指定できる範囲は 1 ～ 63 です。
level-1	（任意）IS-IS レベル 1 IPv4 または IPv6 メトリックを設定します。
level-2	（任意）IS-IS レベル 2 IPv4 または IPv6 メトリックを設定します。

コマンド デフォルト

デフォルトは 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
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

すべての IS-IS インターフェイスのデフォルトメトリック値を変更する必要がある場合、**metric** コマンドを使用して、すべてのインターフェイスをグローバルに設定することを推奨します。メトリック値がグローバルに設定されている場合、新規値を設定せずに誤って設定済みのメトリックをインターフェイスから削除したり、デフォルト メトリック 10 に戻るよう誤ってインターフェイスに許可したりするなどの、ユーザーのエラーを防ぐことができるため、ネットワーク内で優先度の高いインターフェイスとなります。

metric コマンドを入力して、デフォルトの IS-IS インターフェイスメトリック値を変更すると、有効になっているインターフェイスでは、デフォルト値 の10 ではなく新しい値が使用されます。パッシブ インターフェイスでは、メトリック値 0 が引き続き使用されます。

例

次に、グローバル メトリック 111 で IS-IS インターフェイスを設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# metric 111
```

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。
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。

コマンド	説明
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。
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。

コマンド	説明
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 ASA のデータベースに更新されずに存在する最長時間を設定します。
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。
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。

コマンド	説明
summary-address	IS-IS の集約アドレスを作成します。

metric-style

新スタイルのタイプ、長さ、および値（TLV）オブジェクトだけを生成して受け入れるように IS-IS が動作するルータを設定するには、ルータ ISIS コンフィギュレーション モードで **metric-style** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

metric-style [**narrow** | **transition** | **wide**] [**level-1** | **level-2** | **level-1-2**]
no metric [**level-1** | **level-2** | **level-1-2**]

構文の説明

narrow	旧スタイルの TLV とナロー メトリックを使用するように ASA に指示します。
transition	（任意）移行時に旧スタイルおよび新スタイルの TLV の両方を受け入れるように ASA に指示します。
wide	新スタイルの TLV を使用してワイド メトリックを伝送するように ASA に指示します。
level-1	（任意）ルーティング レベル 1 でこのコマンドをイネーブルにします。
level-2	（任意）ルーティング レベル 2 でこのコマンドをイネーブルにします。
level-1-2	（任意）旧スタイルおよび新スタイルの TLV の両方を受け入れようにルータに指示します。

コマンド デフォルト

デフォルトは 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
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

metric-style wide コマンドを入力する場合、ASA は新スタイル TLV だけを生成し、受け入れます。したがって、ASA で使用されるメモリやリソースは、旧スタイルと新スタイルの両方の TLV を生成した場合よりも少なくなります。

このスタイルは、ネットワーク全体で MPLS トラフィック エンジニアリングをイネーブルにする場合に最適です。

例

次に、レベル 1 で新スタイルの TLV を生成し、受け入れるように ASA を設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# metric-style wide level-1
```

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。
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。

コマンド	説明
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。
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。

コマンド	説明
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 ASA のデータベースに更新されずに存在する最長時間を設定します。
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。
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。

コマンド	説明
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。