



match e – match q

- [match ehlo-reply-parameter](#) (3 ページ)
- [match filename](#) (5 ページ)
- [match filetype](#) (7 ページ)
- [match flow ip destination-address](#) (9 ページ)
- [match header \(ポリシー マップ タイプ インスペクション ESMTP\)](#) (11 ページ)
- [match header \(ポリシー マップ タイプ インスペクション IPv6\)](#) (13 ページ)
- [match header-flag](#) (16 ページ)
- [match im-subscriber](#) (18 ページ)
- [match interface](#) (20 ページ)
- [match invalid-recipients](#) (22 ページ)
- [match ip address](#) (24 ページ)
- [match ip next-hop](#) (26 ページ)
- [match ip route-source](#) (28 ページ)
- [match ipv6 address](#) (30 ページ)
- [match login-name](#) (32 ページ)
- [match media-type](#) (34 ページ)
- [match message class](#) (36 ページ)
- [match message id](#) (38 ページ)
- [match message length](#) (40 ページ)
- [match message-path](#) (42 ページ)
- [match metric](#) (44 ページ)
- [match mime](#) (46 ページ)
- [match msisdn](#) (48 ページ)
- [match opc](#) (50 ページ)
- [match peer-ip-address](#) (52 ページ)
- [match peer-login-name](#) (54 ページ)
- [match port](#) (56 ページ)
- [match ppid](#) (58 ページ)
- [match precedence](#) (60 ページ)
- [match protocol](#) (62 ページ)

- [match question \(64 ページ\)](#)

match ehlo-reply-parameter

ESMTP ehlo reply パラメ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 ehlo-reply-parameter** 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**] **ehlo-reply-parameter** *parameter*
no match [**not**] **ehlo-reply-parameter** *parameter*

構文の説明

パラメータ ehlo reply パラメータを指定します。

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спекションポリシーマップに ehlo reply パラメ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 esmtp esmtp_map
ciscoasa (config-pmap)# match ehlo-reply-parameter auth
```

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 filename

FTP転送のファイル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 filename** 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**] **filename regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **filename 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ーは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転送ファイル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)# description Restrict FTP users ftp1, ftp2, and ftp3 from accessing /root
ciscoasa(config-cmap)# match username regex class ftp_regex_user
ciscoasa(config-cmap)# match filename regex ftp-file
```

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 filetype

FTP 転送のファイルタイプ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 filetype** 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 ] filetype regex [ regex_name | class regex_class_name ]
no match [ not ] filetype 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ーは 1 つのみです。

例

次に、FTP インспекションポリシーマップに FTP 転送ファイルタイプに関して一致条件を設定する例を示します。

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

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 flow ip destination-address

クラスマップにフロー IP 宛先アドレスを指定するには、クラス マップ コンフィギュレーション モードで **match flow ip destination-address** 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。

matchflowipdestination-address
nomatchflowipdestination-address

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
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
 ス

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。

トンネルグループで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、**match flow ip destination-address** 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** 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
ciscoasa(config)#
```

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	VPNの接続固有レコードを格納するデータベースを作成し、管理します。

match header (ポリシー マップ タイプ インспекション ESMTP)

ESMTP ヘッダーの一致条件を設定するには、ポリシーマップタイプインспекション ESMTP コンフィギュレーション モードで **match header** 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**] **header** [[**length** | **line length**] **gt bytes** | **to-fields count gt to_fields_number**]
no match [**not**] **header** [[**length** | **line length**] **gt bytes** | **to-fields count gt to_fields_number**]

構文の説明

length gt bytes	ESMTP ヘッダー メッセージの長さを照合することを指定します。
line length gt bytes	ESMTP ヘッダー メッセージの 1 行の長さを照合することを指定します。
to-fields count gt to_fields_number	To: フィールドの数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 タイプ インспекション ESMTP 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спекション ポリシー マップにヘッダー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 esmtp esmtp_map
ciscoasa (config-pmap)# match header length gt 512

```

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 header (ポリシー マップ タイプ インスペクション IPv6)

IPv6 ヘッダーの一致条件を設定するには、ポリシー マップ タイプ インスペクション IPv6 コンフィギュレーション モードで **match header** 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 ] header { ah | count gt number | destination-option | esp | fragment | hop-by-hop
| routing-address count gt number | routing-type { eq | range } number }
no match [ not ] header { ah | count gt number | destination-option | esp | fragment | hop-by-hop
| routing-address count gt number | routing-type { eq | range } number }
```

構文の説明

ah	IPv6 認証拡張ヘッダーを照合します。
count gt number	IPv6 拡張ヘッダーの最大数 (0 ~ 255) を指定します。
destination-option	IPv6 宛先オプション拡張ヘッダーを照合します。
esp	IPv6 カプセル化セキュリティ ペイロード (ESP) 拡張ヘッダーを照合します。
fragment	IPv6 フラグメント拡張ヘッダーを照合します。
hop-by-hop	IPv6 ホップバイホップ拡張ヘッダーを照合します。
not	(オプション) 指定したパラメータを照合しません。
routing-address count gt number	IPv6 ルーティング ヘッダー タイプ 0 のアドレスの最大数として、0 ~ 255 の数値よりも大きい値を設定します。
routing-type {eq range} number	IPv6 ルーティング ヘッダー タイプ (0 ~ 255) を照合します。範囲を指定するには、値をスペースで区切ります (例: 30 40)

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 マップタイプインスペクション IPv6 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
ス

8.2(1) このコマンドが追加されました。

使用上のガイドライン

照合するヘッダーを指定します。デフォルトでは、パケットはログに記録されます (**log**)。パケットを破棄する場合は、一致コンフィギュレーションモードで **drop** コマンドを入力します (必要に応じて、**log** コマンドを入力してログに記録することもできます)。

照合する拡張ごとに、**match** コマンドと **drop** アクション (オプション) を再入力します。

例

次に、ヘッダーが hop-by-hop、destination-option、routing-address、および routing type 0 であるすべての IPv6 パケットを破棄してログに記録するインスペクション ポリシー マップを作成する例を示します。

```
policy-map type inspect ipv6 ipv6-pm
  parameters
    match header hop-by-hop
      drop log
    match header destination-option
      drop log
    match header routing-address count gt 0
      drop log
    match header routing-type eq 0
      drop 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。
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。

コマンド	説明
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 header-flag

DNS ヘッダーフラグ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 header-flag** コマンドを使用します。設定されたヘッダーフラグを削除するには、このコマンドの **no** 形式を使用します。

```
match [ not ] header-flag [ eq ] { f_well_known | f_value }
no match [ not ] header-flag [ eq ] { f_well_known | f_value }
```

構文の説明

eq 完全一致を指定します。設定されていない場合は、**match-all** ビットマスク照合を指定します。

f_well_known 既知の名前で DNS ヘッダーフラグビットを指定します。複数のフラグビットを入力し、論理 OR を適用することもできます。

QR (Query、(注) QR=1、DNS 応答を示します)

AA (Authoritative Answer)

TC (TrunCation)

RD (Recursion Desired)

RA (Recursion Available)

f_value 任意の 16 ビット値を 16 進数形式で指定します。

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
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
ス

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、DNS クラス マップまたは DNS ポリシー マップで設定できます。DNS クラス マップでは、入力できるエントリーは1つのみです。

例

次に、DNS インспекションポリシーマップにDNS ヘッダー フラグ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 dns preset_dns_map
ciscoasa(config-pmap)# match header-flag AA
```

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 im-subscriber

SIP IM 加入者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 im-subscriber** 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 ] im-subscriber regex [ regex_name | class regex_class_name ]
no match [ not ] im-subscriber 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 変更内容
ス

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ーは 1 つのみです。

例

次に、SIP インспекションクラスマップに SIP IM 加入者に関して一致条件を設定する例を示します。

```
ciscoasa(config-cmap)# match im-subscriber regex class im_sender
```

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 interface

指定されたインターフェイスのいずれかを起点とするネクストホップが存在するルートを配布するには、ルートマップコンフィギュレーションモードで **match interface** コマンドを使用します。match interface 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 interface *interface-name*
no match interface *interface-name*

構文の説明

interface-name インターフェイスの名前（物理インターフェイスではありません）。複数のインターフェイス名を指定できます。

コマンド デフォルト

一致インターフェイスは定義されません。

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 変更内容
 ス

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

コマンド構文内の省略記号 (...) は、コマンドを入力するときに、interface-type interface-number 引数に対応する値を複数指定できることを意味します。

route-map global 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指定できます。**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。 **match** コマンドで複数のインターフェイスが指定されている場合は、 **no match interface interface-name** を使用して1つのインターフェイスを削除できます。

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** コマンドに関するあるいずれの **match** 句とも一致しないルートは無視されます。一部のデータだけを変更する場合は、別のルートマップセクションを設定し、明示的な一致を指定します。

例

次に、ネクスト ホップが外部のルートを配布する例を示します。

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match interface outside
```

関連コマンド

コマンド	説明
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 ip route-source	アクセスリストで指定されたアドレスにあるルータおよびアクセスサーバーによってアドバタイズされたルートを再配布します。
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 invalid-recipients

ESMTP 無効受信者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 invalid-recipients** 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] invalid-recipients count gt number
no match [not] invalid-recipients count gt number

構文の説明

count gt number 無効な受信者数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 変更内容
ス

7.2(1) このコマンドが追加されました。

例

次に、ESMTP インспекションポリシーマップに無効な受信者数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 esmtp esmtp_map
ciscoasa (config-pmap)# match invalid-recipients count gt 1000
```

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 ip address

指定したいいずれかのアクセスリストによって渡されるルートアドレスまたはマッチパケットがある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 ip address** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

match ip address { *acl* . . . } **prefix-list**
no match ip address { *acl* . . . } **prefix-list**

構文の説明

acl アクセスリストの名前を指定します。複数のアクセスリストを指定できます。

prefix-list 照合するプレフィックス リスト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
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 変更内容
ス

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 global 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。

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 ip address acl_dmz1 acl_dmz2
```

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 ipv6 address	指定したいずれかのアクセスリストによって渡される IPv6 ルート アドレスまたはマッチ パケットがあるルートを再配布します。
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 ip next-hop

指定されたいずれかのアクセスリストによって渡されるネクストホップ ルータ アドレスがある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 ip next-hop** コマンドを使用します。ネクストホッ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 ip next-hop { acl . . . } | prefix-list prefix_list
no match ip next-hop { acl . . . } | prefix-list prefix_list
```

構文の説明

<i>acl</i>	ACL の名前です。複数の ACL を指定できます。
prefix-list <i>prefix_list</i>	プレフィックス リストの名前です。

コマンド デフォルト

ルートは自由に配布されます。ネクストホップ アドレスを照合する必要はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルート 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 変更内容
ス

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

コマンド構文に含まれる省略符号 (...) は、コマンド入力に *acl* 引数の値を複数含めることができることを示します。

route-map global 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。

ルートがルートマップを通過するようにするときには、ルートマップに複数の要素を持たせることができます。**route-map** コマンドに関係のあるいずれの**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。

例

次に、アクセスリスト `acl_dmz1` または `acl_dmz2` によって渡されるネクストホップルータアドレスがあるルートを配布する例を示します。

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ip next-hop acl_dmz1 acl_dmz2
```

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 ip route-source

ACLに指定されているアドレスにあるルータおよびアクセスサーバーによってアドバタイズされた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 ip route-source** コマンドを使用します。ネクストホッ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 ip route-source { acl . . . } prefix-list prefix_list
match ip route-source { acl . . . }
```

構文の説明

acl ACL の名前です。複数の ACL を指定できます。

prefix_list プレフィックス リストの名前です。

コマンド デフォルト

ルート送信元でのフィルタリングはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルート 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 変更内容
ス

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

コマンド構文に含まれる省略符号 (...) は、コマンド入力に **access-list-name** 引数の値を複数含めることができることを示します。

route-map global 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** コマンドに関するあるいずれの**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。ルートのネクストホップアドレスと送信元ルータアドレスが同じではない場合があります。

例

次に、**acl_dmz1** および **acl_dmz2** という ACL で指定されたアドレスにあるルータおよびアクセス サーバーによってアドバタイズされたルートを配布する例を示します。

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ip route-source acl_dmz1 acl_dmz2
```

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	指定したいずれかの ACL によって渡されたネクストホップルータアドレスを持つ、すべての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 ipv6 address

指定したいいずれかのアクセスリストによって渡されるIPv6ルートアドレスまたはマッチパケットがある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 ipv6 address** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

match ipv6 address { *acl* . . . } **prefix-list**
no match ipv6 address { *acl* . . . } **prefix-list**

構文の説明

acl アクセスリストの名前を指定します。複数のアクセスリストを指定できます。

prefix-list 照合するプレフィックス リスト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
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 変更内容
ス

9.1(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

route-map global 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。

例

次に、内部ルートを再配布する例を示します。access-list acl_dmz1 extended permit ipv6 any <net> <mask>

```
ciscoasa(config)# access-list acl_dmz1 extended permit ipv6 any <net> <mask>
```

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ipv6 address acl_dmz1 acl_dmz2
```

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、すべてのルートを配布します。
match ip address	指定したいずれかのアクセスリストによって渡されるルートアドレスまたはマッチ パケットがある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 login-name

インスタントメッセージ用のクライアントログイン名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 login-name** 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 ] login-name regex [ regex_name | class regex_class_name ]
no match [ not ] login-name 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 変更内容
ス

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タリは 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 マップにクライアント ログイン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 im im_class
ciscoasa(config-cmap)# match login-name regex login
```


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 media-type

H.323 メディアタイプ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 media-type** 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] media-type [audio | data | video]
no match [not] media-type [audio | data | video]

構文の説明

audio オーディオメディアタイプを照合することを指定します。

data データ メディア タイプを照合することを指定します。

video ビデオ メディア タイプ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 変更内容
ス

7.2(1) このコマンドが追加されました。

例

次に、H.323 インспекション クラス マップにオーディオメディアタイプに関して一致条件を設定する例を示します。

```
ciscoasa(config-cmap)# match media-type audio
```

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 message class

M3UA メッセージのメッセージクラスおよびタイプに対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 message class** 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 ] message class class_id [ id message_id ]
no match [ not ] message class class_id [ id message_id ]
```

構文の説明

class_id メッセージクラス。サポートされているクラスとタイプ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。

id 指定されているクラス内のメッセージタイプ。
message_id

コマンド デフォルト

M3UA インспекションでは、レート制限なしにすべてのメッセージクラスおよび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
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 変更内容
ス

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спекションポリシーマップで設定できます。メッセージクラスおよびタイプに基づいてパケットをドロップまたはレート制限できます。次の表に、使用可能な値を示します。これらのメッセージの詳細については、M3UA のRFCおよびドキュメンテーションを参照してください。

M3UA メッセージクラス	メッセージIDタイプ
0 (管理メッセージ)	0 ~ 1
1 (転送メッセージ)	1

M3UA メッセージクラス	メッセージIDタイプ
2 (SS7シグナリングネットワーク管理メッセージ)	1 ~ 6
3 (ASP 状態メンテナンス メッセージ)	1 ~ 6
4 (ASP トラフィック メンテナンス メッセージ)	1 ~ 4
9 (ルーティング キー管理メッセージ)	1 ~ 4

例

次に、M3UA メッセージ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 message class 2 id 6
ciscoasa(config-pmap-c)# drop
ciscoasa(config-pmap-c)# match message class 9
ciscoasa(config-pmap-c)# drop
```

関連コマンド

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

match message id

GTP メッセージ ID の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 message id** 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 ] message { v1 | v2 } id [ message_id | range lower_range upper_range }
no match [ not ] message { v1 | v2 } id [ message_id | range lower_range upper_range }
```

構文の説明

{v1 v2}	(9.5(1)以降) GTP のバージョンを示します。GTPv0 ~ 1 の場合は v1 、GTPv2 の場合は v2 を使用します。
<i>message_id</i>	メッセージ ID。1 ~ 255 を指定できます。
range lower_range upper_range	メッセージ ID の範囲。範囲の下限と上限を指定します。

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 変更内容
ス

7.2(1) このコマンドが追加されました。

9.5(1) **{v1 | v2}** キーワードが追加されました。

使用上のガイドライン

このコマンドは、GTP ポリシー マップで設定できます。

例

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

```
ciscoasa(config-pmap)# match message id 33
```

リリース 9.5(1) 以降では、**{v1 | v2}** キーワードを追加する必要があります。

```
ciscoasa(config-pmap)# match message v2 id 33
```

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。

match message length

GTP メッセージ ID の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 message length** 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**] **message length** **min** *min_length* **max** *max_length*
no match [**not**] **message length** **min** *min_length* **max** *max_length*

構文の説明

min *min_length* メッセージ ID の最小の長さを指定します。値の範囲は 1 ～ 65536 です。

max *max_length* メッセージ ID の最大の長さを指定します。値の範囲は 1 ～ 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
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 変更内容
ス

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спекションポリシーマップにメッセージの長さに関して一致条件を設定する例を示します。

```
ciscoasa(config-pmap)# match message length min 8 max 200
```

関連コマンド

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

コマンド	説明
match message id	メッセージIDに基づいてトラフィックを照合します。

match message-path

Via ヘッダーフィールドの指定に従って SIP メッセージが通過するパスに関する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 message-path** 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**] **message-path regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **message-path 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 変更内容
ス

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タリは 1 つのみです。

例

次の例では、SIP インспек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 message-path regex class sip_message
```

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 metric

指定されたメトリックを持つ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 metric** コマンドを使用します。エントリを削除するには、このコマンドの **no** 形式を使用します。

match metric number
no match metric number

構文の説明

number ルート メトリック (5 つの部分からなる IGRP のメトリック)。有効な値は 0 ~ 4294967295 です。

コマンド デフォルト

メトリック値に関するフィルタリングを行いません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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 global 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** コマンドの順序は任意に指定できます。すべての **match** コマンドが満たされないと、**set** コマンドで指定した設定アクションに従ってルートの再配布が行われません。**match** コマンドの **no** 形式を使用すると、指定した一致基準が削除されます。

ルートマップは、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。

例

次に、メトリックが 5 のルートを再配布する例を示します。

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match metric 5
```

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。
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 mime

ESMTP MIME エンコーディングタイプ、MIME ファイル名の長さ、または MIME ファイルタイプ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 mime** 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**] **mime** [**encoding type** | **filename length gt bytes** | **filetype regex**]
no match [**not**] **mime** [**encoding type** | **filename length gt bytes** | **filetype regex**]

構文の説明

encoding type エンコーディングタイプを照合することを指定します。

filename length gt bytes ファイル名の長さを照合することを指定します。

filetype regex ファイルタイプ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 変更内容
ス

7.2(1) このコマンドが追加されました。

例

次に、ESMTP インспекション ポリシー マップに MIME ファイル名の長さ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 esmtp esmtp_map
ciscoasa (config-pmap)# match mime filename length gt 255
```

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 msisdn

Create PDP Context 要求、Create Session 要求、および Modify Bearer Response メッセージの GTP モバイルステーション国際サブスクライバディレクトリ番号 (MSISDN) 情報要素の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 msisdn** 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 ] msisdn regex { regex_name | class class_name }
no match [ not ] msisdn regex { regex_name | class class_name }
```

構文の説明

regex_name 正規表現オブジェクトの名前。

class 正規表現クラスの名前。
class_name

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
ス

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 要求のモバイルステーション国際サブスクライバディレクトリ番号 (MSISDN) 情報要素をフィルタリングできます。特定の MSISDN に基づいて、または最初の x 桁数に応じた MSISDN の範囲に基づいて、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。MSISDN を指定するには、正規表現を使用します。MSISDN 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

次に、正規表現オブジェクトを使用して MSISDN 一致条件を設定する例を示します。


```
ciscoasa(config)# policy-map type inspect gtp gtp-map
```

```
ciscoasa(config-pmap)# match msisdn regex msisdn1
```

```
ciscoasa(config-pmap-c)# drop log
```

次に、正規表現クラスを使用して MSISDN 一致条件を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
```

```
ciscoasa(config-pmap)# match msisdn regex class msisdn2
```

```
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 opc

M3UA データメッセージの発信ポイントコード（OPC）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 opc** 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**] **opc code**
no match [**not**] **opc code**

構文の説明

code zone -region -sp 形式の発信ポイントコード。

コマンド デフォルト

M3UA インспекションでは、すべての発信ポイント コードが許可されます。

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 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 変更内容
ス

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спекションポリシー マップで設定できます。発信ポイントコードに基づいてパケットをドロップできます。ポイントコードは *zone -region -sp* 形式で、各要素に使用可能な値は SS7 バリエーションによって異なります。バリエーションはポリシーマップの **ss7 variant** コマンドで定義できます。

- ITU : ポイント コードは 14 ビットで 3-8-3 形式です。値の範囲は、[0-7]-[0-255]-[0-7] です。これは、デフォルトの SS7 バリエーションです。
- ANSI : ポイント コードは 24 ビットで 8-8-8 形式です。値の範囲は、[0-255]-[0-255]-[0-255] です。
- Japan : ポイント コードは 16 ビットで 5-4-7 形式です。値の範囲は、[0-31]-[0-15]-[0-127] です。

- China : ポイントコードは 24 ビットで 8-8-8 形式です。値の範囲は、[0-255]-[0-255]-[0-255] です。

例

次に、ITU の特定の発信ポイントコー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 m3ua m3ua-map
ciscoasa(config-pmap)# match opc 1-5-1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インспекションをイネーブルにします。
match dpc	M3UA 宛先ポイントコードと一致させます。
policy-map type inspect	インспекションポリシーマップを作成します。
ss7 variant	ポリシーマップで使用する SS7 バリエントを指定します。

match peer-ip-address

インスタントメッセージのピア IP アドレス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 peer-ip-address** 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 ] peer-ip-address ip_address ip_address_mask
no match [ not ] peer-ip-address ip_address ip_address_mask
```

構文の説明

ip_address クライアントまたはサーバーのホスト名または IP アドレスを指定します。

ip_address_mask クライアントまたはサーバー IP アドレスのネットマスクを指定します。

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 変更内容
ス

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タリは 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 マップにピア IP 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)# class-map type inspect im im_class
ciscoasa(config-cmap)# match peer-ip-address 10.1.1.0 255.255.255.0
```

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 peer-login-name

インスタントメッセージのピアログイン名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 peer-login-name** 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 ] peer-login-name regex [ regex_name | class regex_class_name ]
no match [ not ] peer-login-name 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 変更内容
ス

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タリは 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ピアログイン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 im im_class
ciscoasa(config-cmap)# match peer-login-name regex peerlogin
```

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。
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 port

モジュラ ポリシー フレームワークを使用する場合、クラスマップ コンフィギュレーション モードで **match port** コマンドを使用して、アクションを適用するポートを照合します。 **match port** 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。

```
match port { tcp | udp | sctp } { eq port | range beg_port end_port }
no match port { tcp | udp | sctp } { eq port | range beg_port end_port }
```

構文の説明

eq port	単一のポート名またはポート番号を指定します。
range beg_port end_port	ポート範囲の開始値および終了値を 1 ~ 65535 の範囲で指定します。
tcp	TCP ポートを指定します。
sctp	SCTP ポートを指定します。
udp	UDP ポートを指定します。

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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース 変更内容
ス

7.0(1) このコマンドが追加されました。

9.7(1) **sctp** キーワードが追加されました。

使用上のガイドライン

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

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

class-map コマンドの入力後に、**match port** コマンドを入力してトラフィックを指定します。あるいは、**match access-list** コマンドなど、別のタイプの **match** コマンドを入力できます（**class-map type management** コマンドでのみ **match port** コマンドが許可されます）。クラスマップには **match port** コマンドを1つだけ含めることができ、他のタイプの **match** コマンドと組み合わせることはできません。

1. （アプリケーションインスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーションインスペクショントラフィックの特別なアクションを定義します。
2. **policy-map** コマンドを使用して、レイヤ3と4のトラフィックにアクションを適用します。
3. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

例

次に、クラスマップおよび **match port** 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 port tcp eq 8080
```

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 access-list	アクセスリストに従ってトラフィックを照合します。
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 ppid

SCTP インспекションのためにペイロードプロトコルID (PPID) に関して一致条件を設定するには、インспекション ポリシー マップ コンフィギュレーションモードで **match ppid** 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 ] ppid ppid_1 [ ppid_2 ]
no match [ not ] ppid ppid_1 [ ppid_2 ]
```

構文の説明

ppid_1 [*ppid_2*] PPID 番号 (0 ~ 4294967295) または名前で SCTP PPID を指定します (使用可能な名前については、CLI ヘルプを参照)。範囲を指定するための2つ目の (より大きな) PPID を含めることができます。

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спекション 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
ス

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、SCTP インспек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、PPID に対してフィルタ処理を行い、それらの ID に特別なアクション (ドロップ、ログ、レート制限など) を適用できます。

PPID に対してフィルタ処理を行う場合は、次の点に注意してください。

- PPID はデータ チャンクに含まれており、1 つのパケットが複数のデータ チャンクを持つ場合があります。パケットに異なる PPID を持つデータ チャンクが含まれている場合、パケットはフィルタ処理されず、割り当てられたアクションがパケットに適用されません。
- PPID フィルタリングを使用してパケットをドロップまたはレート制限する場合は、トランスミッタによりドロップされたパケットが再送されることに注意してください。レート

制限が適用された PPID のパケットは再試行で通過する可能性があります。ドロップされた PPID のパケットは再びドロップされます。ネットワーク上のこのような反復的ドロップの最終成果を評価することができます。

例

次に、未割り当ての PPID（この例の作成時点で未割り当て）をドロップし、PPID 32～40 にレート制限を適用し、Diameter PPID をログに記録する SCTP インスペクションポリシーマップを作成する例を示します。

```
policy-map type inspect sctp sctp-pmap
  match ppid 58 4294967295
    drop
  match ppid 26
    drop
  match ppid 49
    drop
  match ppid 32 40
    rate-limit 1000
  match ppid diameter
    log
```

関連コマンド

コマンド	説明
drop	一致するトラフィックをドロップします。
inspect sctp	SCTP インスペクションをイネーブルにします。
log	一致するトラフィックをログに記録します。
policy-map type inspect sctp	SCTP インスペクションポリシーマップを作成します。
rate-limit	一致するトラフィックにレート制限を適用します。

match precedence

クラスマップに `precedence` 値を指定するには、クラス マップ コンフィギュレーション モードで `match precedence` 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。

`matchprecedencevalue`

`nomatchprecedence` 値

構文の説明

`value` 最大 4 つの `precedence` 値をスペースで区切って指定します。指定できる範囲は、0 ~ 7 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 変更内容
ス

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。

IP ヘッダーに TOS バイトで表される値を指定するには、**match precedence** コマンドを使用します。

例

次に、クラスマップおよび **match precedence** 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
precedence 1
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 protocol

MSN や Yahoo などの特定のインスタントメッセージプロトコル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 protocol** 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 ] protocol { msn-im | yahoo-im }
no match [ not ] protocol { msn-im | yahoo-im }
```

構文の説明

msn-im MSN インスタント メッセージング プロトコルを照合することを指定します。

yahoo-im Yahoo インスタント メッセージング プロトコル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 変更内容
ス

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タリは 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 Yahoo インスタント メッセージング プロトコル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 protocol yahoo-im
```

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。
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 question

DNSの質問またはリソースレコード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 question** コマンドを使用します。設定されたセクションを削除するには、このコマンドの **no** 形式を使用します。

```
match { question | { resource-record answer | authority | additional } }
no match { question | { resource-record answer | authority | additional } }
```

構文の説明

<i>question</i>	DNS メッセージの質問部分を指定します。
<i>resource-record</i>	DNS メッセージのリソースレコード部分を指定します。
<i>answer</i>	Answer RR セクションを指定します。
<i>authority</i>	Authority RR セクションを指定します。
<i>additional</i>	Additional RR セクションを指定します。

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
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 変更内容
ス

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、このコマンドは DNS ヘッダーを調べ、指定されたフィールドとマッチングします。また、他の DNS **match** コマンドと併用して、特定の質問または RR タイプのインスペクションを定義できます。

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

例

次に、DNS インспекション ポリシー マップに DNS 質問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 dns preset_dns_map
ciscoasa(config-pmap)# match question
```

関連コマンド

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

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。