CHAPTER 20

mac address コマンド～ multicast-routing コマンド

mac address

アクティブ ユニットおよびスタンバイ ユニットの仮想 MAC アドレスを指定するには、フェールオーバー グループ コンフィギュレーション モードで **mac address** コマンドを使用します。デフォルトの仮想 MAC アドレスに戻すには、このコマンドの **no** 形式を使用します。

mac address *phy_if* [*active_mac*] [*standby_mac*]

no mac address *phy_if* [*active_mac*] [*standby_mac*]

構文の説明

phy_if	MAC アドレスを設定するインターフェイスの物理名です。
active_mac	アクティブ ユニットの仮想 MAC アドレス。MAC アドレスは h.h.h 形式で入力する必要があります。ここで、h は 16 ビットの 16 進数です。
standby_mac	スタンバイ ユニットの仮想 MAC アドレス。MAC アドレスは h.h.h 形式で入力する必要があります。ここで、h は 16 ビットの 16 進数です。

デフォルト

デフォルトの設定は次のとおりです。

- アクティブ ユニットのデフォルトの MAC アドレス：00a0.c9*physical_port_number.failover_group_id*01
- スタンバイ ユニットのデフォルトの MAC アドレス：00a0.c9*physical_port_number.failover_group_id*02

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

仮想 MAC アドレスがフェールオーバー グループに対して定義されていない場合は、デフォルト値が使用されます。

同じネットワーク上にアクティブ/アクティブ フェールオーバー ペアが複数ある場合は、あるペアのインターフェイスに割り当てられているものと同じデフォルト仮想 MAC アドレスが、他のペアのインターフェイスに割り当てられることがあります。これは、デフォルト仮想 MAC アドレスの決定方法に基づいた動作です。ネットワーク上で MAC アドレスが重複することを回避するには、必ず各物理インターフェイスに仮想のアクティブおよびスタンバイ MAC アドレスを割り当てます。

例

次の部分的な例では、フェールオーバー グループで可能な設定を示します。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
failover mac address	物理インターフェイスの仮想 MAC アドレスを指定します。

mac-address

プライベート MAC アドレスをインターフェイスまたはサブインターフェイスに手動で割り当てるには、インターフェイス コンフィギュレーション モードで **mac-address** コマンドを使用します。マルチコンテキスト モードでは、このコマンドは各コンテキストでそれぞれ別の MAC アドレスをインターフェイスに割り当てることができます。MAC アドレス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。

mac-address *mac_address* [**standby** *mac_address*]

no mac-address [*mac_address* [**standby** *mac_address*]]

構文の説明

mac_address	このインターフェイスの MAC アドレスを H.H.H 形式で設定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。フェールオーバーを使用する場合は、この MAC アドレスがアクティブな MAC アドレスとなります。 **（注）** 自動生成されたアドレス（**mac-address auto** コマンド）は A2 で始まるため、A2 を含む手動 MAC アドレスは自動生成を使用しようとしても開始できません。
standby *mac_address*	（任意）フェールオーバーのスタンバイ MAC アドレスを設定します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

デフォルト

デフォルトの MAC アドレスは、物理インターフェイスのバーンドイン MAC アドレスです。サブインターフェイスは、物理インターフェイスの MAC アドレスを継承します。一部のコマンド（シングル モードでのこのコマンドを含む）は物理インターフェイスの MAC アドレスを設定するため、継承されるアドレスはその設定によって異なります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(5)	**mac-address auto** コマンドと併用するときには、MAC アドレスを開始する A2 の使用が制限されました。

使用上のガイドライン

マルチ コンテキスト モードでは、コンテキスト間でインターフェイスを共有した場合、各コンテキストでそれぞれ固有の MAC アドレスをインターフェイスに割り当てることができます。この機能を使用すると、セキュリティ アプライアンスはパケットを適切なコンテキストに容易に分類できます。固有の MAC アドレスがなくても共有インターフェイスを使用できますが、制限があります。詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

このコマンドで各 MAC アドレスを手動で割り当てることができます。あるいは **mac-address auto** コマンドを使用して、コンテキストで共有インターフェイスの MAC アドレスを自動的に生成できます。MAC アドレスを自動的に生成する場合、**mac-address** コマンドを使用して、生成されたアドレスを上書きできます。

シングル コンテキスト モード、またはマルチ コンテキスト モードで共有されないインターフェイスの場合は、固有の MAC アドレスをサブインターフェイスに割り当てることを推奨します。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。

他のコマンドまたは方式で MAC アドレスを設定することもできます。MAC アドレスの設定方法には次の優先順位があります。

1. インターフェイス コンフィギュレーション モードの **mac-address** コマンド。

   このコマンドは、物理インターフェイスとサブインターフェイスに対して使用します。マルチ コンテキスト モードでは、MAC アドレスを各コンテキスト内で設定します。この機能を使用すると、複数のコンテキストの同じインターフェイスに異なる MAC アドレスを設定できます。

2. グローバル コンフィギュレーション モードでの Active/Standby フェールオーバーのための **failover mac address** コマンド。

   このコマンドは、物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** または **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

3. フェールオーバー グループ コンフィギュレーション モードでの Active/Active フェールオーバーのための **mac address** コマンド。

   このコマンドは、物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** または **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

4. グローバル コンフィギュレーション モードでの **mac-address auto** コマンド（マルチ コンテキスト モードのみ）。

   このコマンドは、コンテキストの共有インターフェイスに適用されます。

5. Active/Active フェールオーバーの場合の物理インターフェイスのためのアクティブ MAC アドレスおよびスタンバイ MAC アドレスの自動生成。

   この方法は、物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** または **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

6. バーンドイン MAC アドレス。この方法は、物理インターフェイスに適用されます。

   サブインターフェイスは、**mac-address** または **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

例

次に、GigabitEthernet 0/1.1 の MAC アドレスを設定する例を示します。

```
hostname/contextA(config)# interface gigabitethernet0/1.1
hostname/contextA(config-if)# nameif inside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

```
hostname/contextA(config-if)# mac-address 030C.F142.4CDE standby 040C.F142.4CDE
hostname/contextA(config-if)# no shutdown
```

関連コマンド

コマンド	説明
failover mac address	Active/Standby フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac address	Active/Active フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac-address auto	マルチ コンテキスト モードでの共有インターフェイスの MAC アドレス（アクティブおよびスタンバイ）を自動生成します。
mode	セキュリティ コンテキスト モードをマルチまたはシングルに設定します。
show interface	MAC アドレスを含む、インターフェイスの特性を表示します。

mac-address auto

プライベート MAC アドレスを各コンテキスト インターフェイスに自動的に割り当てるには、グローバル コンフィギュレーション モードで **mac-address auto** コマンドを使用します。自動 MAC アドレスをディセーブルにするには、このコマンドの **no** 形式を使用します。

mac-address auto prefix *prefix*

no mac-address auto

構文の説明

prefix *prefix*	MAC アドレスの一部として使用されるプレフィックスを設定します。*prefix* は、0 ～ 65535 の 10 進数です。このプレフィックスは、4 桁の 16 進数値に変換されます。プレフィックスにより、各セキュリティ アプライアンスはそれぞれ固有の MAC アドレスを使用するようになるため、次のように 1 つのネットワーク セグメントに複数のセキュリティ アプライアンスを配置できます。プレフィックスの使用方法の詳細については、「MAC Address Format」を参照してください。

デフォルト

自動生成はデフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(5)	**prefix** キーワードが追加されました。プレフィックスを使用し、固定の開始値（A2）を使用し、フェールオーバー ペアのプライマリ ユニットおよびセカンダリ ユニットの MAC アドレスで別の方式を使用するように、MAC アドレス形式が変更されました。MAC アドレスは現在、リロード間で持続されるようになっています。コマンド パーサーは現在、自動生成がイネーブルになっているかどうかをチェックします。MAC アドレスを手動でも割り当てることができるようにする場合は、A2 を含む手動 MAC アドレスは開始できません。

使用上のガイドライン

インターフェイスを共有するコンテキストを許可するには、固有の MAC アドレスを各共有コンテキスト インターフェイスに割り当てることを推奨します。MAC アドレスは、コンテキスト内でパケットを分類するために使用されます。インターフェイスを共有するものの、各コンテキストにインターフェイスの固有の MAC アドレスがない場合は、宛先 IP アドレスがパケットの分類に使用されます。宛先ア

ドレスは、コンテキスト NAT コンフィギュレーションと照合されます。この方法には、MAC アドレスの方法に比べるといくつか制限があります。パケットの分類の詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、コンテキスト内のインターフェイスの MAC アドレスを手動で設定できます。MAC アドレスを手動で設定するには、**mac-address** コマンドを参照してください。

デフォルトの MAC アドレス

デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。

自動生成された MAC アドレスはすべて、A2 で始まります。自動生成された MAC アドレスは、リロード間で持続されます。

手動 MAC アドレスとの通信

MAC アドレスを手動で割り当てた場合、自動生成がイネーブルになっていても、手動で割り当てた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます。

自動生成されたアドレスは A2 で始まるため、手動 MAC アドレスを A2 で始めることはできません。たとえ自動生成も使用する予定であってもそれは同じです。

フェールオーバー用の MAC アドレス

フェールオーバーで使用できるように、セキュリティ アプライアンスはインターフェイスごとにアクティブとスタンバイの両方の MAC アドレスを生成します。アクティブ ユニットがフェールオーバーしてスタンバイ ユニットがアクティブになると、その新規アクティブ ユニットがアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。詳細については、「MAC Address Format」を参照してください。

prefix キーワードが導入される前に従来のバージョンの **mac-address auto** コマンドを使用してフェールオーバー ユニットをアップグレードする場合は、「prefix キーワードを使用しない従来の MAC アドレス形式」の項を参照してください。

MAC Address Format

セキュリティ アプライアンスは、次の形式を使用して MAC アドレスを生成します。

A2xx.yyzz.zzzz

xx.yy はユーザ定義のプレフィックスで、zz.zzzz はセキュリティ アプライアンスが生成した内部カウンタです。スタンバイ MAC アドレスの場合、内部カウンタが 1 増えることを除けばアドレスは同じです。

プレフィックスの使用方法を示す例の場合、プレフィックス 77 を設定すると、セキュリティ アプライアンスは 77 を 16 進数値 004D（yyxx）に変換します。MAC アドレスで使用すると、プレフィックスはセキュリティ アプライアンスネイティブ形式に一致するように逆にされます（xxyy）。

A2**4D.00**zz.zzzz

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1.03**zz.zzzz

MAC アドレスが生成される場合

コンテキストでインターフェイスの **nameif** コマンドを設定すると、ただちに新規 MAC アドレスが生成されます。コンテキスト インターフェイスを設定した後でこのコマンドをイネーブルにした場合、コマンドを入力するとただちにすべてのインターフェイスの MAC アドレスが生成されます。**no**

mac-address auto コマンドを使用すると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。

他の方法を使用した MAC アドレスの設定

他のコマンドまたは方式で MAC アドレスを設定することもできます。MAC アドレスの設定方法には次の優先順位があります。

1. インターフェイス コンフィギュレーション モードの **mac-address** コマンド。

   このコマンドは、物理インターフェイスとサブインターフェイスに対して使用します。マルチ コンテキスト モードでは、MAC アドレスを各コンテキスト内で設定します。この機能を使用すると、複数のコンテキストの同じインターフェイスに異なる MAC アドレスを設定できます。

2. グローバル コンフィギュレーション モードでの Active/Standby フェールオーバーのための **failover mac address** コマンド。

   このコマンドは、物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** または **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

3. フェールオーバー グループ コンフィギュレーション モードでの Active/Active フェールオーバーのための **mac address** コマンド。

   このコマンドは、物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** または **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

4. グローバル コンフィギュレーション モードでの **mac-address auto** コマンド（マルチ コンテキスト モードのみ）。

   このコマンドは、コンテキストの共有インターフェイスに適用されます。

5. Active/Active フェールオーバーの場合の物理インターフェイスのためのアクティブ MAC アドレスおよびスタンバイ MAC アドレスの自動生成。

   この方法は、物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** または **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

6. バーンドイン MAC アドレス。この方法は、物理インターフェイスに適用されます。

   サブインターフェイスは、**mac-address** または **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

システム コンフィギュレーションでの MAC アドレスの表示

システム実行スペースから割り当てられた MAC アドレスを表示するには、**show running-config all context** コマンドを入力します。

割り当てられた MAC アドレスを表示するには、**all** オプションが必要です。このコマンドはグローバル コンフィギュレーション モードでのみユーザによる設定が可能ですが、**mac-address auto** コマンドは割り当てられた MAC アドレスとともに各コンテキストのコンフィギュレーションに読み取り専用エントリとして表示されます。コンテキスト内で **nameif** コマンドで設定される割り当て済みのインターフェイスだけに MAC アドレスが割り当てられます。

（注） MAC アドレスをインターフェイスに手動で割り当てるものの、その際に自動生成がイネーブルになっていると、手動 MAC アドレスが使用中のアドレスとなりますが、コンフィギュレーションには自動生成されたアドレスが引き続き表示されます。後で手動 MAC アドレスを削除すると、表示されている自動生成アドレスが使用されます。

コンテキスト内の MAC アドレスの表示

コンテキスト内の各インターフェイスで使用されている MAC アドレスを表示するには、**show interface | include (Interface)|(MAC)** コマンドを入力します。

（注）　**show interface** コマンドは、使用中の MAC アドレスを表示します。MAC アドレスを手動で割り当てた場合に、自動生成がイネーブルになっていたときは、システム コンフィギュレーション内の未使用の自動生成アドレスのみを表示できます。

prefix キーワードを使用しない従来の MAC アドレス形式

バージョン 8.0(5) 以前、**mac-address auto** コマンドには **prefix** キーワードが含まれていませんでした。この旧バージョンのコマンドは引き続き使用できるため、フェールオーバー ペア間でアップグレードを実行できます。アップグレードしても自動的に変換されないため、このコマンドはアップグレードしたフェールオーバー ユニットとアップグレードしなかったフェールオーバー ユニット間でこれまでどおり一致したものとなります。両ユニットを新しいソフトウェア バージョンにアップグレードした後には、**prefix** キーワードを使用するようにこのコマンドを変更する必要があります。

prefix キーワードがないと、MAC アドレスは次の形式で生成されます。

- アクティブ ユニットの MAC アドレス：12*_slot.port_subid.contextid*.
- スタンバイ ユニットの MAC アドレス：02*_slot.port_subid.contextid*.

インターフェイス スロットがないプラットフォームの場合、スロットは常に 0 です。*port* はインターフェイス ポートです。*subid* は、表示不可能なサブインターフェイスの内部 ID です。*contextid* は、**show context detail** コマンドで表示可能なコンテキストの内部 ID です。たとえば、ID 1 のコンテキスト内のインターフェイス GigabitEthernet 0/1.200 には、次の生成済み MAC アドレスがあります。サブインターフェイス 200 の内部 ID は 31 です。

- アクティブ：1200.0131.0001
- スタンバイ：0200.0131.0001

この従来の MAC アドレス生成方法では、リロード間で MAC アドレスが持続されず、同じネットワーク セグメントに複数のセキュリティ アプライアンスを配置できず（固有の MAC アドレスが保証されないため）、手動で割り当てた MAC アドレスとの MAC アドレスの重複が回避されません。

例

次に、プレフィックス 78 で自動 MAC アドレス生成をイネーブルにする例を示します。

```
hostname(config)# mac-address auto prefix 78
```

show running-config all context admin コマンドからの次の出力には、Management0/0 インターフェイスに割り当てられたプライマリおよびスタンバイ MAC アドレスが表示されます。

```
hostname# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

show running-config all context コマンドからの次の出力には、すべてのコンテキスト インターフェイスのすべての MAC アドレス（プライマリおよびスタンバイ）が表示されます。GigabitEthernet0/0 と GigabitEthernet0/1 の各メイン インターフェイスはコンテキスト内部に **nameif** コマンドで設定されないため、それらのインターフェイスの MAC アドレスは生成されていないことに注意してください。

```
hostname# show running-config all context
```

```
admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

関連コマンド

コマンド	説明
failover mac address	Active/Standby フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac address	Active/Active フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac-address	物理インターフェイスまたはサブインターフェイスの MAC アドレス（アクティブとスタンバイ）を手動で設定します。マルチ コンテキスト モードでは、同じインターフェイスに対して、コンテキストごとにそれぞれ別の MAC アドレスを設定することができます。
mode	セキュリティ コンテキスト モードをマルチまたはシングルに設定します。
show interface	MAC アドレスを含む、インターフェイスの特性を表示します。

mac-address-table aging-time

MAC アドレス テーブルのエントリにタイムアウトを設定するには、グローバル コンフィギュレーション モードで **mac-address-table aging-time** コマンドを使用します。デフォルト値の 5 分に戻すには、このコマンドの **no** 形式を使用します。

mac-address-table aging-time *timeout_value*

no mac-address-table aging-time

構文の説明

timeout_value	タイムアウトするまで MAC アドレス エントリが MAC アドレス テーブルにとどまることができる時間。有効な値は、5 ～ 720 分（12 時間）です。5 分がデフォルトです。

デフォルト

デフォルトのタイムアウトは 5 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

使用方法のガイドラインはありません。

例

次に、MAC アドレスのタイムアウトを 10 分に設定する例を示します。

```
hostname(config)# mac-address-timeout aging time 10
```

関連コマンド

コマンド	説明
arp-inspection	ARP パケットとスタティック ARP エントリを比較する ARP インスペクションをイネーブルにします。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。

コマンド	説明
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	ダイナミック エントリおよびスタティック エントリを含む MAC アドレス テーブルを表示します。

mac-address-table static

MAC アドレス テーブルにスタティック エントリを追加するには、グローバル コンフィギュレーション モードで **mac-address-table static** コマンドを使用します。スタティック 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。MAC アドレスは通常、特定の MAC アドレスからのトラフィックがインターフェイスに入るときに MAC アドレス テーブルにダイナミックに追加されます。スタティック MAC アドレスは、必要に応じて MAC アドレス テーブルに追加できます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。スタティック エントリと同じ MAC アドレスを持つクライアントが、そのスタティック エントリに一致しないインターフェイスにトラフィックを送信しようとした場合、セキュリティ アプライアンスはトラフィックをドロップし、システム メッセージを生成します。

mac-address-table static *interface_name mac_address*

no mac-address-table static *interface_name mac_address*

構文の説明

interface_name	送信元インターフェイス。
mac_address	テーブルに追加する MAC アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、スタティック MAC アドレスのエントリを MAC アドレス テーブルに追加する例を示します。

```
hostname(config)# mac-address-table static inside 0010.7cbe.6101
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。

コマンド	説明
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	MAC アドレス テーブルのエントリを表示します。

mac-learn

インターフェイスの MAC アドレス ラーニングをディセーブルにするには、グローバル コンフィギュレーション モードで **mac-learn** コマンドを使用します。MAC アドレス ラーニングを再びイネーブルにするには、このコマンドの **no** 形式を使用します。デフォルトでは、各インターフェイスはトラフィックに入る MAC アドレスを自動的に学習し、セキュリティ アプライアンスは対応するエントリを MAC アドレス テーブルに追加します。必要に応じて MAC アドレス ラーニングをディセーブルにできます。

mac-learn *interface_name* **disable**

no mac-learn *interface_name* **disable**

構文の説明

interface_name	MAC アドレス学習をディセーブルにするインターフェイス。
disable	MAC 学習をディセーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、外部インターフェイスでの MAC アドレス学習をディセーブルにする例を示します。

```
hostname(config)# mac-learn outside disable
```

関連コマンド

コマンド	説明
clear configure mac-learn	**mac-learn** コンフィギュレーションをデフォルトに設定します。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。

コマンド	説明
show mac-address-table	ダイナミック エントリおよびスタティック エントリを含む MAC アドレス テーブルを表示します。
show running-config mac-learn	**mac-learn** コンフィギュレーションを表示します。

mac-list

認証や許可から MAC アドレスを削除するのに使用される MAC アドレスのリストを指定するには、グローバル コンフィギュレーション モードで **mac-list** コマンドを使用します。MAC アドレス リストの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。

mac-list *id* {**deny | permit**} *mac macmask*

no mac-list *id* {**deny | permit**} *mac macmask*

構文の説明

deny	この MAC アドレスに一致するトラフィックは MAC アドレス リストと照合せず、**aaa mac-exempt** コマンドに指定されているときには認証と許可の両方の対象となることを示します。ffff.ffff.0000 などの MAC アドレス マスクを使用して、ある範囲の MAC アドレスを許可し、その範囲の MAC アドレスを強制的に認証および許可する場合には、MAC アドレス リストに拒否エントリを追加することが必要になる場合があります。
id	MAC アクセス リストの 16 進数値を指定します。一連の MAC アドレスをグループ化するには、同じ ID 値で必要な回数の **mac-list** コマンドを入力します。パケットが最適に一致するエントリではなく最初に一致するエントリを使用するため、エントリの順序が重要になります。permit エントリがあり、その permit エントリで許可されているアドレスを拒否する場合は、permit エントリよりも前に deny エントリを入力してください。
mac	送信元 MAC アドレスを 12 桁の 16 進数形式、つまり、nnnn.nnnn.nnnn で指定します。
macmask	MAC アドレスのどの部分を照合に使用するかを指定します。たとえば、ffff.ffff.ffff は完全に MAC アドレスと一致します。ffff.ffff.0000 は最初の 8 桁だけ一致します。
permit	この MAC アドレスに一致するトラフィックは MAC アドレス リストと照合せず、**aaa mac-exempt** コマンドに指定されているときには認証と許可の両方から削除されることを示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

認証および許可からの MAC アドレスの削除をイネーブルにするには、**aaa mac-exempt** コマンドを使用します。1 つの **aaa mac-exempt** コマンドのみを追加できるため、削除するすべての MAC アドレスが MAC アドレス リストに含まれていることを確認してください。複数の MAC リストを作成できますが、一度に使用できるのは 1 つだけです。

例

次の例では、1 個の MAC アドレスに対する認証をバイパスします。

```
hostname(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# aaa mac-exempt match abc
```

次のエントリでは、ハードウェア ID が 0003.E3 であるすべての Cisco IP Phone について、認証をバイパスします。

```
hostname(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
hostname(config)# aaa mac-exempt match acd
```

次の例では、00a0.c95d.02b2 以外の MAC アドレス グループの認証をバイパスします。00a0.c95d.02b2 は permit ステートメントとも一致するため、permit ステートメントよりも前に deny ステートメントを入力します。permit ステートメントが前にある場合、deny ステートメントとは一致しません。

```
hostname(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
hostname(config)# aaa mac-exempt match 1
```

関連コマンド

コマンド	説明
aaa authentication	ユーザ認証をイネーブルにします。
aaa authorization	ユーザ認可サービスをイネーブルにします。
aaa mac-exempt	MAC アドレスのリストを認証と認可の対象から免除します。
clear configure mac-list	**mac-list** コマンドで指定されている MAC アドレスのリストを削除します。
show running-config mac-list	**mac-list** コマンドで以前指定された MAC アドレスのリストを表示します。

mail-relay

ローカル ドメイン名を設定するには、パラメータ コンフィギュレーション モードで **mail-relay** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

mail-relay *domain_name* **action** {**drop-connection** | **log**}

no mail-relay *domain_name* **action** {**drop-connection** | **log**}

構文の説明

domain_name	ドメイン名を指定します。
drop-connection	接続を閉じます。
log	システム ログ メッセージを生成します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、特定のドメインへのメール中継を設定する例を示します。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mail-relay mail action drop-connection
```

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。

management-access

VPN の使用時にセキュリティ アプライアンスへの通過ルートとなるインターフェイス以外のインターフェイスへの管理アクセスを許可するには、グローバル コンフィギュレーション モードで **management-access** コマンドを使用します。管理アクセスをディセーブルにするには、このコマンドの **no** 形式を使用します。

management-access *mgmt_if*

no management-access *mgmt_if*

構文の説明

mgmt_if	別のインターフェイスからセキュリティ アプライアンスに入るときにアクセスする管理インターフェイスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドを使用すると、フル トンネル IPSec VPN または SSL VPN クライアント（AnyConnect 2.x クライアント、SVC 1.x）を使用するときや、サイトツーサイト IPSec トンネルを横断するときには、セキュリティ アプライアンスへの通過ルートとなるインターフェイス以外のインターフェイスに接続できます。たとえば、外部インターフェイスからセキュリティ アプライアンスに入る場合、このコマンドを使用すると、Telnet で内部インターフェイスに接続できます。あるいは、外部インターフェイスから入るときには、内部インターフェイスに ping を実行できます。

次のアプリケーションを使用できます。

- SNMP ポーリング
- HTTPS 要求
- ASDM アクセス
- Telnet アクセス
- SSH アクセス
- ping
- Syslog ポーリング

- NTP 要求

管理アクセス インターフェイスは 1 つだけ定義できます。

（注） 管理アクセス インターフェイスにスタティック NAT ステートメントは適用されません。適用した場合、リモート VPN ユーザが管理インターフェイスにアクセスできなくなります。

例

次に、ファイアウォール インターフェイスを管理アクセス インターフェイスとして「inside」という名前で設定する例を示します。

```
hostname(config)# management-access inside
hostname(config)# show management-access
management-access inside
```

関連コマンド

コマンド	説明
clear configure management-access	セキュリティ アプライアンスの管理アクセスのための、内部インターフェイスのコンフィギュレーションを削除します。
show management-access	管理アクセスのために設定された内部インターフェイスの名前を表示します。

management-only

管理トラフィックのみを受け付けるようにインターフェイスを設定するには、インターフェイス コンフィギュレーション モードで **management-only** コマンドを使用します。通過トラフィックを許可するには、このコマンドの **no** 形式を使用します。

management-only

no management-only

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ASA 5510 以降の適応型セキュリティ アプライアンス上の Management 0/0 インターフェイスは、デフォルトでは管理専用モードに設定されます。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ASA 5510 以降の適応型セキュリティ アプライアンスには、Management 0/0 という専用の管理インターフェイスが含まれ、セキュリティ アプライアンスへのトラフィックをサポートするようになっています。ただし、**management-only** コマンドを使用することで、任意のインターフェイスを管理専用インターフェイスとして設定できます。また、Management 0/0 の場合、管理専用モードをディセーブルにできるため、このインターフェイスは他のインターフェイスと同じくトラフィックを通過させることができます。

トランスペアレント ファイアウォール モードでは、2 つのインターフェイスだけがトラフィックを通過させることができます。ただし、ASA 5510 以降の適応型セキュリティ アプライアンスの場合、Management 0/0 インターフェイス（物理インターフェイスまたはサブインターフェイスのいずれか）を管理トラフィック用に 3 つめのインターフェイスとして使用できます。この場合モードは設定不可となり、常に管理専用にする必要があります。セキュリティ アプライアンスまたはコンテキストには割り当てられ、個々のインターフェイスには割り当てられない管理 IP アドレスとは別のサブネットにこのインターフェイスを配置する場合、トランスペアレント モードでこのインターフェイスの IP アドレスを設定することもできます。

例

次に、管理インターフェイスで管理専用モードをディセーブルにする例を示します。

```
hostname(config)# interface management0/0
hostname(config-if)# no management-only
```

次に、サブインターフェイスで管理専用モードをイネーブルにする例を示します。

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# management-only
```

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。

map-name

ユーザ定義の属性名をシスコ属性名にマッピングするには、LDAP 属性マップ コンフィギュレーション モードで **map-name** コマンドを使用します。

このマッピングを削除するには、このコマンドの **no** 形式を使用します。

map-name *user-attribute-name Cisco-attribute-name*

no map-name *user-attribute-name Cisco-attribute-name*

構文の説明

user-attribute-name	シスコ属性にマッピングするユーザ定義の属性名を指定します。
Cisco-attribute-name	ユーザ定義の属性名にマッピングするシスコ属性名を指定します。

デフォルト

デフォルトでは、名前のマッピングはありません。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
LDAP 属性マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

map-name コマンドでは、ユーザ定義の属性名をシスコ属性名にマッピングできます。その後、作成された属性マップを LDAP サーバにバインドできます。一般的な手順には次のものが含まれます。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用し、何も入力されていない属性マップを作成します。このコマンドは LDAP 属性マップ モードを開始します。
2. LDAP 属性マップ モードで **map-name** コマンドと **map-value** コマンドを使用し、属性マップに情報を入力します。
3. AAA サーバ ホスト モードで **ldap-attribute-map** コマンドを使用し、属性マップを LDAP サーバにバインドします。このコマンドでは「ldap」の後にハイフンを付けます。

（注） 属性マッピング機能を正しく使用するには、Cisco LDAP 属性名と値の両方を理解し、さらにユーザ定義属性名と値を理解しておく必要があります。

例

次に、LDAP 属性マップ myldapmap でユーザ定義の属性名 Hours をシスコ属性名 cVPN3000-Access-Hours にマッピングする例を示します。

```
hostname(config)# ldap attribute-map myldapmap
```

```
hostname(config-ldap-attribute-map)# map-name Hours cVPN3000-Access-Hours
hostname(config-ldap-attribute-map)#
```

LDAP 属性マップ モードでは、次の例に示すように、「?」を入力してシスコ LDAP 属性名の詳細なリストを表示できます。

```
hostname(config-ldap-attribute-map)# map-name ?
ldap mode commands/options:
cisco-attribute-names:
  cVPN3000-Access-Hours
  cVPN3000-Allow-Network-Extension-Mode
  cVPN3000-Auth-Service-Type
  cVPN3000-Authenticated-User-Idle-Timeout
  cVPN3000-Authorization-Required
  cVPN3000-Authorization-Type
    :
    :
  cVPN3000-X509-Cert-Data
hostname(config-ldap-attribute-map)#
```

関連コマンド

コマンド	説明
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。
ldap-attribute-map（AAA サーバ ホスト モード）	LDAP 属性マップを LDAP サーバにバインドします。
map-value	ユーザ定義の属性値をシスコ属性にマッピングします。
show running-config ldap attribute-map	実行中の特定の LDAP 属性マップまたは実行中のすべての属性マップを表示します。
clear configure ldap attribute-map	すべての LDAP 属性マップを削除します。

map-value

ユーザ定義の値をシスコ LDAP 属性にマッピングするには、LDAP 属性マップ コンフィギュレーション モードで **map-value** コマンドを使用します。マップ内の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。

map-value *user-attribute-name user-value-string Cisco-value-string*

no map-value *user-attribute-name user-value-string Cisco-value-string*

構文の説明

cisco-value-string	シスコ属性のシスコ値ストリングを指定します。
user-attribute-name	シスコ属性名にマッピングするユーザ定義の属性名を指定します。
user-value-string	シスコ属性値にマッピングするユーザ定義の値のストリングを指定します。

デフォルト

デフォルトでは、シスコ属性にマッピングされるユーザ定義の値がありません。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
LDAP 属性マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

map-value コマンドでは、ユーザ定義の属性値をシスコ属性名および属性値にマッピングできます。作成された属性マップは、LDAP サーバにバインドできます。一般的な手順には次のものが含まれます。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用し、何も入力されていない属性マップを作成します。このコマンドは LDAP 属性マップ モードを開始します。
2. LDAP 属性マップ モードで **map-name** コマンドと **map-value** コマンドを使用し、属性マップに情報を入力します。
3. AAA サーバ ホスト モードで **ldap-attribute-map** コマンドを使用し、属性マップを LDAP サーバにバインドします。このコマンドでは「ldap」の後にハイフンを付けます。

（注） 属性マッピング機能を正しく使用するには、Cisco LDAP 属性名と値の両方を理解し、さらにユーザ定義属性名と値を理解しておく必要があります。

例

次に、LDAP 属性マップ モードを開始し、ユーザ定義の属性 Hours のユーザ定義の値をユーザ定義の時間ポリシー workDay とシスコ定義の時間ポリシー Daytime に設定する例を示します。

```
hostname(config)# ldap attribute-map myldapmap
hostname(config-ldap-attribute-map)# map-value Hours workDay Daytime
hostname(config-ldap-attribute-map)#
```

関連コマンド

コマンド	説明
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。
ldap-attribute-map（AAA サーバ ホスト モード）	LDAP 属性マップを LDAP サーバにバインドします。
map-name	ユーザ定義の LDAP 属性名を、Cisco LDAP 属性名にマッピングします。
show running-config ldap attribute-map	実行中の特定の LDAP 属性マップまたは実行中のすべての属性マップを表示します。
clear configure ldap attribute-map	すべての LDAP マップを削除します。

mask

モジュラ ポリシー フレームワークを使用する場合、一致コンフィギュレーション モードまたはクラス コンフィギュレーション モードで **mask** コマンドを使用して、**match** コマンドと一致するパケットの一部またはクラス マップをマスクして除外します。この mask アクションは、アプリケーション トラフィックのインスペクション ポリシー マップ（**policy-map type inspect** コマンド）で有効です。ただし、すべてのアプリケーションでこのアクションが許可されているわけではありません。たとえば、セキュリティ アプライアンスでのトラフィックの通過を許可する前に、DNS アプリケーション インスペクションに **mask** コマンドを使用してヘッダー フラグをマスクします。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

mask [**log**]

no mask [**log**]

構文の説明

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

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力して、アプリケーション トラフィック（**class** コマンドは、**match** コマンドが含まれている既存の **class-map type inspect** コマンドを参照します）を識別した後、**mask** コマンドを入力して、**match** コマンドまたは **class** コマンドに一致するパケットの一部をマスクできます。

レイヤ 3/4 のポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにすると、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect dns dns_policy_map** コマンドを入力します。ここで dns_policy_map はインスペクション ポリシー マップの名前です。

例

次に、セキュリティ アプライアンスでのトラフィックの通過を許可する前に、DNS ヘッダーで RD フラグおよび RA フラグをマスクする例を示します。

```
hostname(config-cmap)# policy-map type inspect dns dns-map1
hostname(config-pmap-c)# match header-flag RD
hostname(config-pmap-c)# mask log
hostname(config-pmap-c)# match header-flag RA
hostname(config-pmap-c)# mask log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

mask-banner

サーバ バナーを難読化するには、パラメータ コンフィギュレーション モードで **mask-banner** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

mask-banner

no mask-banner

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、サーバ バナーをマスクする例を示します。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner
```

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。

mask-syst-reply

FTP サーバ応答をクライアントから見えないようにするには、**ftp-map** コマンドを使用してアクセスできる FTP マップ コンフィギュレーション モードで **mask-syst-reply** 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。

mask-syst-reply

no mask-syst-reply

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。

デフォルト

このコマンドは、デフォルトでイネ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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
FTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

クライアントから FTP サーバ システムを保護するには、厳格な FTP インスペクションで mask-syst-reply コマンドを使用します。このコマンドをイネーブルにすると、**syst** コマンドに対するサーバからの応答は一連の X に置き換えられます。

例

次に、セキュリティ アプライアンスで syst コマンドに対する FTP サーバの応答を一連の X に置き換える例を示します。

```
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# mask-syst-reply
hostname(config-ftp-map)#
```

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
ftp-map	FTP マップを定義し、FTP マップ コンフィギュレーション モードをイネーブルにします。
inspect ftp	アプリケーション インスペクションに使用する特定の FTP マップを適用します。

コマンド	説明
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
request-command deny	不許可にする FTP コマンドを指定します。

match access-list

モジュラ ポリシー フレームワーク を使用するときは、クラス マップ コンフィギュレーション モードで **match access-list** コマンドを使用して、アクセス リストに基づいてアクションを適用するトラフィックを特定します。**match access-list** 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 access-list *access_list_name*

no match access-list *access_list_name*

構文の説明

access_list_name	一致条件として使用するアクセス リストの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

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** コマンドを使用して、アクションを適用するレイヤ 3 と 4 のトラフィックを指定します。

   class-map コマンドを入力した後、**match access-list** コマンドを入力してトラフィックを識別できます。または、別のタイプの **match** コマンド（**match port** コマンドなど）を入力できます。クラス マップには 1 つの **match access-list** コマンドのみを含めることができ、他のタイプの **match** コマンドとは組み合わせることができません。セキュリティ アプライアンスでインスペクトできるすべてのアプリケーションが使用するデフォルトの TCP ポートおよび UDP ポートを照合する **match default-inspection-traffic** コマンドを定義する場合は、例外として **match access-list** コマンドを使用して照合するトラフィックの範囲を絞り込めます。**match default-inspection-traffic** コマンドによって照合するポートが指定されるため、アクセス リストのポートはすべて無視されます。

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

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

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

例

次に、3 つのアクセス リストに一致する 3 つのレイヤ 3/4 クラス マップを作成する例を示します。

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp

hostname(config-cmap)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp

hostname(config-cmap)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
hostname(config-cmap)# match access-list host_foo
```

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 any

モジュラ ポリシー フレームワーク を使用するときは、クラス マップ コンフィギュレーション モードで **match any** コマンドを使用して、アクションを適用するすべてのトラフィックを一致させます。**match any** 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 any

no match any

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

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** コマンドを使用して、アクションを適用するレイヤ 3 と 4 のトラフィックを指定します。

   class-map コマンドを入力した後、**match any** コマンドを入力してすべてのトラフィックを識別できます。または、別のタイプの **match** コマンド（**match port** コマンドなど）を入力できます。**match any** コマンドは、他のタイプの **match** コマンドとは組み合わせることができません。

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

例

次に、クラス マップおよび **match any** 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。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match any
```

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 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 apn

GTP メッセージのアクセス ポイント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 apn** 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**] **apn regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **apn 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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、GTP クラス マップまたは GTP ポリシー マップで設定できます。GTP 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、GTP インスペクション クラス マップのアクセス ポイント名に関して一致条件を設定する例を示します。

```
hostname(config-cmap)# match apn class gtp_regex_apn
```

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。

コマンド	説明
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 body

ESMTP 本文メッセージの長さまたは 1 行の長さに対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 body** 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 [**not**] **body [length | line length] gt** *bytes*

no match [**not**] **body [length | line length] gt** *bytes*

構文の説明

length	ESMTP 本文メッセージの長さを指定します。
line length	ESMTP 本文メッセージの 1 行の長さを指定します。
bytes	一致する数値をバイト単位で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ESMTP インスペクション ポリシー マップで本文 1 行の長さに関して一致条件を設定する例を示します。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match body line length 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。
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 called-party

H.323 着信側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 called-party** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **called-party [regex** *regex***]**

no match [**not**] **match** [**not**] **called-party [regex** *regex***]**

構文の説明

regex *regex*	正規表現を照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、H.323 インスペクション クラス マップで着信側に関して一致条件を設定する例を示します。

```
hostname(config-cmap)# match called-party regex caller1
```

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 calling-party

H.323 発信側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 calling-party** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **calling-party** [**regex** *regex*]

no match [**not**] **match** [**not**] **calling-party** [**regex** *regex*]

構文の説明

regex *regex*	正規表現を照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、H.323 インスペクション クラス マップで発信側に関して一致条件を設定する例を示します。

```
hostname(config-cmap)# match calling-party regex caller1
```

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 certificate

PKI 証明書検証プロセス中、セキュリティ アプライアンスは証明書失効ステータスを確認してセキュリティを確保します。また、CRL チェックまたは Online Certificate Status Protocol（OCSP）を使用してこのタスクを完了できます。CRL チェックでは、セキュリティ アプライアンスは失効した証明書の詳細なリストである証明書失効リストを取得、解析、およびキャッシュします。OCSP は失効ステータスを確認する拡張性の高い方法であり、検証局で証明書ステータスをローカライズします。この検証局が特定の証明書のステータスを問い合わせます。

証明書一致ルールには、OCSP URL オーバーライドを設定できます。このオーバーライドには、リモート ユーザ証明書の AIA フィールドの URL ではなく、失効ステータスを確認するための URL を指定します。一致ルールには、OCSP 応答側証明書の検証に使用するトラストポイントも設定できます。これにより、セキュリティ アプライアンスは自己署名証明書やクライアント証明書の検証パスの外部にある証明書など任意の CA からの応答側証明書を検証できます。

証明書一致ルールを設定するには、クリプト CA トラストポイント モードで **match certificate** コマンドを使用します。コンフィギュレーションからルールを削除するには、このコマンドの **no** 形式を使用します。

match certificate *map-name* **override ocsp [trustpoint** *trustpoint-name***]** *seq-num* **url** *URL*

no match certificate *map-name* **override ocsp**

構文の説明

map-name	このルールに一致する証明書マップの名前を指定します。一致ルールを設定する前に、証明書マップを設定する必要があります。最大 65 文字です。
match certificate	この一致ルールの証明書マップを指定します。
override ocsp	ルールの目的が証明書の OCSP URL を上書きすることであることを指定します。
seq-num	この一致ルールのプライオリティを設定します。指定できる範囲は、1 ～ 10000 です。セキュリティ アプライアンスは、まずシーケンス番号が最も小さな一致ルールを評価し、それから順に一致が見つかるまで高い番号の一致ルールを評価していきます。
trustpoint	（任意）トラストポイントを使用して OCSP 応答側証明書を確認することを指定します。
trustpoint-name	（任意）応答側証明書を検証するために オーバーライドとともに使用するトラストポイントを特定します。
url	OCSP 失効ステータスの URL にアクセスすることを指定します。
URL	OCSP 失効ステータスのためにアクセスする URL を識別します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表に、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	透過	シングル	マルチ コンテキスト	システム
暗号 CA トラストポイント モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン　OCSP を設定するときは、次のヒントに留意してください。

- 1 つのトラストポイント コンフィギュレーション内に複数の一致ルールを設定できますが、各クリプト CA 証明書マップに指定できる一致ルールは 1 つだけです。ただし、複数のクリプト CA 証明書マップを設定し、それらを同じトラストポイントに関連付けることができます。
- 一致ルールを設定する前に、証明書マップを設定する必要があります。
- 自己署名 OCSP 応答側証明書を検証するようにトラストポイントを設定するには、自己署名応答側証明書を信頼できる CA 証明書として独自のトラストポイントにインポートします。次に、自己署名 OCSP 応答側証明書が含まれているトラストポイントを使用して応答側証明書を検証するように、トラストポイントを検証するクライアント証明書の **match certificate** コマンドを設定します。同じことが、クライアント証明書の検証パスの外部にある応答側証明書の検証にも当てはまります。
- クライアント証明書と応答側証明書の両方を同じ CA が発行している場合には、1 つのトラストポイントでどちらも検証できます。しかし、クライアント証明書と応答側証明書を発行している CA が異なる場合は、トラストポイントを証明書ごとに 1 つずつ計 2 つ設定する必要があります。
- OCSP サーバ（応答側）証明書は一般に、OCSP 応答に署名します。セキュリティ アプライアンスが応答を受け取ると、応答側の証明書を検証しようとします。CA は通常、自身の OCSP 応答側証明書のライフタイムを比較的短い期間に設定して、証明書が侵害される可能性を最小限に抑えます。CA は一般に、応答側証明書に ocsp-no-check 拡張を含めて、この証明書では失効ステータス チェックが必要ないことを示します。しかし、この拡張が含まれていない場合、セキュリティ アプライアンスはトラストポイントに指定されているものと同じ方法で自身の失効ステータスをチェックしようとします。応答側証明書が検証可能でない場合、失効チェックは失敗します。このような失敗を回避するには、トラストポイントを検証する応答側証明書には **revocation-check none** を設定し、クライアント証明書には **revocation-check ocsp** を設定します。
- セキュリティ アプライアンスは、一致が見つからない場合、**ocsp url** コマンドの URL を使用します。**ocsp url** コマンドを設定しなかった場合は、リモート ユーザ証明書の AIA フィールドが使用されます。証明書に AIA 拡張がない場合、失効ステータスのチェックは失敗します。

例　次に、newtrust という名前のトラストポイントの証明書一致ルールを作成する例を示します。ルールには、マップ名 mymap、シーケンス番号 4、トラストポイント mytrust があり、URL として 10.22.184.22 が指定されています。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust 4
url 10.22.184.22
```

```
hostname(config-ca-trustpoint)#
```

その次に、クリプト CA 証明書マップを段階的に設定し、CA 証明書が含まれているトラストポイントを識別して応答側証明書を検証するための一致証明書ルールを設定する例を示します。これが必要になるのは、newtrust トラストポイントで識別した CA が OCSP 応答側証明書を発行していない場合です。

ステップ 1　マップ ルールの適用先のクライアント証明書を識別する証明書マップを設定します。この例では、証明書マップの名前は mymap で、シーケンス番号は 1 です。サブジェクト名に mycert という CN 属性が含まれているクライアント証明書はどれも、mymap エントリに一致します。

```
hostname(config)# crypto ca certificate map mymap 1 subject-name attr cn eq mycert
hostname(config-ca-cert-map)# subject-name attr cn eq mycert
hostname(config-ca-cert-map)#
```

ステップ 2　OCSP 応答側証明書の検証に使用する CA 証明書が含まれているトラストポイントを設定します。自己署名証明書の場合、これは自己署名証明書自体であり、インポートされてローカルに信頼できるようになっています。この目的で外部の CA 登録を介して証明書を取得することもできます。CA 証明書に貼り付けるように求められたら貼り付けます。

```
hostname(config-ca-cert-map)# exit
hostname(config)# crypto ca trustpoint mytrust
hostname(config-ca-trustpoint)# enroll terminal
hostname(config-ca-trustpoint)# crypto ca authenticate mytrust
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

MIIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
v8RqzqpmZYguveV9cLQK5tsxqW3DysMU/4/qUGPfkVZ0iKPCgpIAWmq2ojhCFPyx
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit
INFO: Certificate has the following attributes:
Fingerprint:     7100d897 05914652 25b2f0fc e773df42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

ステップ 3　OCSP を失効チェック方法にして、元のトラストポイント newtrust を設定します。次に、ステップ 2 で設定した証明書マップ mymap および自己署名トラストポイント mytrust を含めた一致ルールを設定します。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# enroll terminal
hostname(config-ca-trustpoint)# crypto ca authenticate newtrust

Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
OPIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit
```

```
INFO: Certificate has the following attributes:
Fingerprint:     9508g897 82914638 435f9f0fc x9y2p42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# revocation-check ocsp
hostname(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust 4
url 10.22.184.22
```

クライアント証明書認証に newtrust トラストポイントを使用する接続はどれも、mymap 証明書マップに指定されている属性ルールにクライアント証明書が一致するかどうかを確認します。一致する場合、セキュリティ アプライアンスは 10.22.184.22 にある OCSP 応答側にアクセスして証明書失効ステータスを確認します。次に、mytrust トラストポイントを使用して、応答側証明書を検証します。

（注） newtrust トラストポイントは、OCSP 経由でクライアント証明書の失効チェックを実行するように設定されます。ただし、mytrust トラストポイントにはデフォルトの失効チェック方法が設定されています。デフォルトは none であるため、OCSP 応答側証明書に対して失効チェックは実行されません。

関連コマンド

コマンド	説明
crypto ca certificate map	クリプト CA 証明書マップを作成します。このコマンドは、グローバル コンフィギュレーション モードで使用します。
crypto ca trustpoint	暗号 CA トラストポイント モードを開始します。このコマンドは、グローバル コンフィギュレーション モードで使用します。
ocsp disable-nonce	OCSP 要求のナンス拡張をディセーブルにします。
ocsp url	トラストポイントに関連付けられているすべての証明書をチェックするために使用する OCSP サーバを指定します。
revocation-check	失効確認に使用する方法、および確認を行う順序を指定します。

match cmd

ESMTP コマンド verb 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 cmd** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **cmd** [**verb** *verb* | **line length gt** *bytes* | **RCPT count gt** *recipients_number*]

no match [**not**] **cmd** [**verb** *verb* | **line length gt** *bytes* | **RCPT count gt** *recipients_number*]

構文の説明

verb *verb*	ESMTP コマンド verb を指定します。
line length gt *bytes*	1 行の長さを指定します。
RCPT count gt *recipients_number*	受信者の電子メール アドレスの数を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ESMTP トランザクションで交換される verb（メソッド）NOOP に関して一致条件を ESMTP インスペクション ポリシー マップに設定する例を示します。

```
hostname(config-pmap)# match cmd verb NOOP
```

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 default-inspection-traffic

クラス マップに inspect コマンドのデフォルトのトラフィックを指定するには、クラス マップ コンフィギュレーション モードで **match default-inspection-traffic** 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 default-inspection-traffic

no match default-inspection-traffic

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。

デフォルト

各インスペクションのデフォルトのトラフィックについては、「使用上のガイドライン」を参照してください。

コマンド 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

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。トラフィック クラスは、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ときに、その一環として **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。

match default-inspection-traffic コマンドを使用すると、個々の **inspect** コマンドのデフォルトのトラフィックを照合できます。**match default-inspection-traffic** コマンドは、一般に **permit ip** *src-ip dst-ip* という形式のアクセス リストであるもう 1 つの match コマンドと併用できます。

match default-inspection-traffic コマンドともう 1 つの match コマンドを組み合わせるためのルールは、**match default-inspection-traffic** コマンドを使用してプロトコルおよびポート情報を指定し、別の **match** コマンドを使用して他のすべての情報（IP アドレスなど）を指定するというものです。もう 1 つの **match** コマンドに指定されているプロトコルやポート情報は、**inspect** コマンドでは無視されます。

たとえば、次の例に指定されているポート 65535 は無視されます。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# match port 65535
```

インスペクション用のデフォルトのトラフィックは、次のようになります。

インスペクション タイプ	プロトコル タイプ	送信元ポート	宛先ポート
ctiqbe	tcp	該当なし	1748
dcerpc	tcp	該当なし	135
dns	udp	53	53
ftp	tcp	該当なし	21
gtp	udp	2123、3386	2123、3386
h323 h225	tcp	該当なし	1720
h323 ras	udp	該当なし	1718 ～ 1719
http	tcp	該当なし	80
icmp	icmp	該当なし	該当なし
ils	tcp	該当なし	389
im	tcp	該当なし	1 ～ 65539
ipsec-pass-thru	udp	該当なし	500
mgcp	udp	2427、2727	2427、2727
netbios	udp	137 ～ 138	該当なし
rpc	udp	111	111
rsh	tcp	該当なし	514
rtsp	tcp	該当なし	554
sip	tcp,udp	該当なし	5060
skinny	tcp	該当なし	2000
smtp	tcp	該当なし	25
sqlnet	tcp	該当なし	1521
tftp	udp	該当なし	69
xdmcp	udp	177	177

例

次に、クラス マップおよび **match default-inspection-traffic** 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。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match default-inspection-traffic
hostname(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 dns-class

DNS Resource Record or Question セクションの Domain System Class 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 dns-class** コマンドを使用します。設定済みのクラスを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **dns-class** {**eq** *c_well_known* | *c_val*} {**range** *c_val1 c_val2*}

no match [**not**] **dns-class** {**eq** *c_well_known* | *c_val*} {**range** *c_val1 c_val2*}

構文の説明

eq	完全一致を指定します。
c_well_known	既知の名前 IN で DNS クラスを指定します。
c_val	DNS クラス フィールド（0 ～ 65535）に任意の値を指定します。
range	範囲を指定します。
c_val1 c_val2	一致範囲を示す値を指定します。それぞれの値の範囲は、0 ～ 65535 です。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、このコマンドは DNS メッセージのすべてのフィールド（質問および RR）を調べ、指定されたクラスを照合します。DNS クエリーと応答の両方が検査されます。

一致対象は、**match not header-flag QR** と **match question** の 2 つのコマンドによって DNS クエリーのクエスチョン部分にまで絞ることができます。

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は 1 つのみです。

例

次に、DNS インスペクション ポリシー マップに DNS クラスに関して一致条件を設定する例を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match dns-class eq IN
```

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 dns-type

クエリー タイプや RR タイプなど DNS 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 dns-type** コマンドを使用します。設定された DNS タイプを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **dns-type** {**eq** *t_well_known* | *t_val*} {**range** *t_val1 t_val2*}

no match [**not**] **dns-type** {**eq** *t_well_known* | *t_val*} {**range** *t_val1 t_val2*}

構文の説明

eq	完全一致を指定します。
t_well_known	A、NS、CNAME、SOA、TSIG、IXFR、AXFR のいずれかの既知の名前で DNS タイプを指定します。
t_val	DNS タイプ フィールド（0 ～ 65535）に任意の値を指定します。
range	範囲を指定します。
t_val1 t_val2	一致範囲を示す値を指定します。それぞれの値の範囲は、0 ～ 65535 です。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、このコマンドは DNS メッセージのすべてのセクション（質問および RR）を調べ、指定されたタイプを照合します。DNS クエリーと応答の両方が検査されます。

一致対象は、**match not header-flag QR** と **match question** の 2 つのコマンドによって DNS クエリーのクエスチョン部分にまで絞ることができます。

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は 1 つのみです。

例

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

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

```
hostname(config-pmap)# match dns-type eq a
```

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 domain-name

DNS メッセージ ドメイン名リスト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 domain-name** 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 [**not**] **domain-name regex** *regex_id*

match [**not**] **domain-name regex class** *class_id*

no match [**not**] **domain-name regex** *regex_id*

no match [**not**] **domain-name regex class** *class_id*

構文の説明

regex	正規表現を指定します。
regex_id	正規表現 ID を指定します。
class	複数の正規表現エントリが含まれているクラス マップを指定します。
class_id	正規表現クラス マップ ID を指定します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、定義済みのリストと DNS メッセージのドメイン名を照合します。圧縮されたドメイン名は、照合の前に展開されます。一致条件は、他の DNS **match** コマンドと併用して、特定のフィールドにまで絞り込むことができます。

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は 1 つのみです。

例

次に、DNS インスペクション ポリシー マップで DNS ドメイン名を照合する例を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match domain-name regex
```

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 dscp

クラス マップの（IP ヘッダーの）IETF-defined DSCP 値を識別するには、クラス マップ コンフィギュレーション モードで **match dscp** 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 dscp {*values*}

no match dscp {*values*}

構文の説明

values	IP ヘッダーに最大 8 種類の IETF-defined DSCP 値を指定します。指定できる範囲は、0 ～ 63 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

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。トラフィック クラスは、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ときに、その一環として **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。

match dscp コマンドを使用すると、IP ヘッダーの IETF-defined DSCP 値を照合できます。

例

次に、クラス マップおよび **match dscp** 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。

```
hostname(config)# class-map cmap
```

```
hostname(config-cmap)# match dscp af43 cs1 ef
hostname(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 port	TCP/UDP ポートをそのインターフェイスで受信したパケットに対する比較基準として指定します。
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 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。

match [**not**] **ehlo-reply-parameter** *parameter*

no match [**not**] **ehlo-reply-parameter** *parameter*

構文の説明

parameter	ehlo reply パラメータを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ESMTP インスペクション ポリシー マップに 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。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(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。
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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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 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。

```
hostname(config)# class-map type inspect ftp match-all ftp_class1
hostname(config-cmap)# description Restrict FTP users ftp1, ftp2, and ftp3 from accessing
/root
hostname(config-cmap)# match username regex class ftp_regex_user
hostname(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。

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 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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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 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。

```
hostname(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。

コマンド	説明
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。

match flow ip destination-address

no match flow ip destination-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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

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。トラフィック クラスは、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ときに、その一環として **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 グループに対するフローベースのポリシー アクションをイネーブルにするには、**match flow ip destination-address** および **match tunnel-group** コマンドを **class-map**、**policy-map**、および **service-policy** コマンドと併用します。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。

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

関連コマンド

コマンド	説明
class-map	トラフィック 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

ESMTP ヘッダー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 header** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ESMTP インスペクション ポリシー マップにヘッダーに関して一致条件を設定する例を示します。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(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。

コマンド	説明
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-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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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は 1 つのみです。

例

次に、DNS インスペクション 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。

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

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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 インスペクション 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。

```
hostname(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。

コマンド	説明
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 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。

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

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。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(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。
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

指定され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...*}

no match ip address {*acl...*}

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

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** コンフィギュレーション コマンド、および **set** コンフィギュレーション コマンドを使用すると、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 **match** コマンドと **set** コマンドが関連付けられます。**match** コマンドは、一致基準（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。

```
hostname(config)# route-map name
hostname(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、すべてのルートを再配布します。

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 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

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

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

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 グローバル コンフィギュレーション コマンド、**match** コンフィギュレーション コマンド、および **set** コンフィギュレーション コマンドを使用すると、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 **match** コマンドと **set** コマンドが関連付けられます。**match** コマンドは、一致基準（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。ルートが **route-map** コマンドに関係のあるどの match 句とも一致しない場合、この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。

```
hostname(config)# route-map name
hostname(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*

no 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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

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 グローバル コンフィギュレーション コマンド、**match** コンフィギュレーション コマンド、および **set** コンフィギュレーション コマンドを使用すると、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 **match** コマンドと **set** コマンドが関連付けられます。**match** コマンドは、一致基準（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。ルートが **route-map** コマンドに関係のあるどの match 句とも一致しない場合、この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。

```
hostname(config)# route-map name
hostname(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 login-name

インスタント メッセージング用のクライアント 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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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。

```
hostname(config)# class-map type inspect im im_class
hostname(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。

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。
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。

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、H.323 インスペクション 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。

```
hostname(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。
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 id

GTP メッセージ ID 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 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 id** [*message_id* | **range** *lower_range upper_range*]

no match [**not**] **message id** [*message_id* | **range** *lower_range upper_range*]

構文の説明

message_id	識別子を英数字 1 ～ 255 で指定します。
range *lower_range upper_range*	ID の下限と上限を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、GTP クラス マップまたは GTP ポリシー マップで設定できます。GTP 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、GTP インスペクション クラス 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。

```
hostname(config-cmap)# match message id 33
```

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。

コマンド	説明
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 length

GTP メッセージ ID の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 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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、GTP クラス マップまたは GTP ポリシー マップで設定できます。GTP 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、GTP インスペクション クラス 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。

```
hostname(config-cmap)# match message length min 8 max 200
```

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。

コマンド	説明
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-path

Via ヘッダー フィールドの指定に従って SIP メッセージがたどるパ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 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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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。

```
hostname(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。

コマンド	説明
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 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。

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ESMTP インスペクション ポリシー マップに 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。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(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。

コマンド	説明
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 peer-ip-address

インスタント メッセージングのピア 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 IP アドレスのネットマスクを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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。

```
hostname(config)# class-map type inspect im im_class
hostname(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。

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。
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 メッセージングのピア 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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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。

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match peer-login-name regex peerlogin
```

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。
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 TCP ポートまたは UDP 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**} {**eq** *port* | **range** *beg_port end_port*}

no match port {**tcp** | **udp**} {**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。
udp	UDP ポートを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

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、アクションの適用対象となるレイヤ 3 と 4 のトラフィックを指定します。

   class-map コマンドを入力した後、**matchport** コマンドを入力してトラフィックを識別できます。また、**match access-list** コマンドなど **match** コマンドの別のタイプを入力できます（**class-map type management** コマンドだけが match port コマンドを許可します）。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** コマンドとは組み合わせることができません。

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

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。

```
hostname(config)# class-map cmap
hostname(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 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。

match precedence *value*

no match precedence *value*

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

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。トラフィック クラスは、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ときに、その一環として **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。

```
hostname(config)# class-map cmap
```

```
hostname(config-cmap)# match precedence 1
hostname(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 メッセージング 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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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 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。

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match protocol yahoo-im
```

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。
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

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

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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は 1 つのみです。

例

次に、DNS インスペクション 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。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match question
```

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 req-resp

HTTP 要求と HTTP 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。

match [**not**] **req-resp content-type mismatch**

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

構文の説明

content-type	要求の受け入れタイプに対する応答でコンテンツ タイプを照合することを指定します。
mismatch	応答の content type フィールドが、要求の accept フィールドのいずれかの MIME タイプに一致する必要があることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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。

上記のチェックに失敗した場合、セキュリティ アプライアンス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。

```
hostname(config)# policy-map type inspect http http_map
hostname(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。
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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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。

```
hostname(config)# policy-map type inspect ftp ftp_map1
hostname(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。
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。

コマンド	説明
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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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。

```
hostname(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。

コマンド	説明
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。

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

表 20-1　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\.xyz.com/.*\.asp」または「www\.xyz[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。

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

local	ローカルに生成された BGP 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
external	OSPF 外部ルートまたは EIGRP 外部ルート。
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。
nssa-external	外部 NSSA を指定します。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

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** コンフィギュレーション コマンド、および **set** コンフィギュレーション コマンドを使用すると、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 **match** コマンドと **set** コマンドが関連付けられます。**match** コマンドは、一致基準（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。ルートが **route-map** コマンドに関係のあるどの match 句とも一致しない場合、この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 type 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。

```
hostname(config)# route-map name
hostname(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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

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。トラフィック クラスは、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ときに、その一環として **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）とマッチングするには、**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。

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

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

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。

```
hostname(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。
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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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。

セキュリティ アプライアンスは、FTP サーバ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 メッセージに基づいて、サーバ名とマッチングします。220 サーバ メッセージには、行が複数含まれることがあります。サーバとのマッチングは、DNS を介して解決されるサーバ名の 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 サーバに関して一致条件を設定する例を示します。

```
hostname(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 メッセージング 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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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。

```
hostname(config)# class-map type inspect im im_class
hostname(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 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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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を登録できるユーザ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。

```
hostname(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。

コマンド	説明
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マッチングするには、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。

match tunnel-group *name*

no match tunnel-group *name*

構文の説明

name	トンネル グループ名のテキスト。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

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。トラフィック クラスは、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ときに、その一環として **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 アクションをイネーブルにするには、**match flow ip destination-address** コマンドおよび **match tunnel-group** コマンドを **class-map**、**policy-map**、**service-policy** の各コマンドと併用します。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** を **match flow ip destination-address** と併用します。

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。

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

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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。

```
hostname(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。

コマンド	説明
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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	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、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。

```
hostname(config)# regex badurl www.url1.com/rtsp.avi
hostname(config)# policy-map type inspect rtsp rtsp-map
hostname(config-pmap)# match url-filter regex badurl
hostname(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。

コマンド	説明
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 username

FTP ユーザ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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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 ユーザ名に関して一致条件を設定する例を示します。

```
hostname(config)# class-map type inspect ftp match-all ftp_class1
hostname(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。

コマンド	説明
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 version

GTP メッセージ ID の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 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**] **version** [*version_id* | **range** *lower_range upper_range*]

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

構文の説明

vresion_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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、GTP クラス マップまたは GTP ポリシー マップで設定できます。GTP 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、GTP インスペクション クラス 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。

```
hostname(config-cmap)# match version 1
```

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。

コマンド	説明
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。

max-failed-attempts

サーバ グループの特定のサーバが非アクティブ化されるまでに、そのサーバに対して許可されている試行の失敗数を指定するには、AAA サーバ 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、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*

no max-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 グループの特定のサーバに対して許可されている接続試行の失敗数を指定する 1 ～ 5 の範囲の整数。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA-server グループ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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

例

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# max-failed-attempts 4
hostname(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 グループ コンフィギュレーション モードを開始して、グループ内のすべてのホストに共通する、グループ固有の AAA サーバ パラメータを設定できるようにします。

clear configure aaa-server	AAA サーバ 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、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

max-forwards-validation

Max-forwards ヘッダー フィールドが 0 かどうかのチェックをイネーブルにするには、パラメータ コンフィギュレーション モードで **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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

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。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(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 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。このモードには、**http-map** コマンドを使用してアクセスできます。この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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

max-header-length コマンドをイネーブルにすると、セキュリティ アプライアンスは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、そのようなヘッダーがない場合には指定されたアクションを実行します。セキュリティ アプライアンスが TCP 接続をリセットし、任意で syslog エントリを作成するようにするには、**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、セキュリティ アプライアンスは TCP 接続をリセットし、syslog エントリを作成します。

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

WebVPN セッションに対してセキュリティ アプライアンスが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 *integer range*

構文の説明

integer range	0 ～ 10000 KB

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
キャッシュ モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

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。キャッシュ圧縮がイネーブルになっている場合、セキュリティ アプライアンスは、オブジェクトを圧縮してからサイズを計算します。

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。

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

要求がタイムアウトされるまでにセキュリティ アプライアンスが失敗した SSO 認証を再試行できる回数を設定するには、特定の SSO サーバ 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*

no max-retry-attempts

構文の説明

retries	失敗した SSO 認証に対して、セキュリティ アプライアンスが認証を再試行する回数 指定できる範囲は 1 ～ 5 回です。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
config-webvpn-sso-saml	•	—	•	—	—
config-webvpn-sso-siteminder	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。セキュリティ アプライアンスは、現在、SiteMinder-type の SSO サーバと SAML POST-type の SSO サーバをサポートしています。

このコマンドは SSO サーバの両タイプに適用されます。

いったん SSO 認証をサポートするようにセキュリティ アプライアンスを設定すると、任意で 2 つのタイムアウト パラメータを調整できます。

- **max-retry-attempts** コマンドを使用してセキュリティ アプライアンスが失敗した SSO 認証を再試行できる回数。
- 失敗した SSO 認証がタイムアウトするまでの秒数（**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。

```
hostname(config-webvpn)# sso-server my-sso-server type siteminder
```

```
hostname(config-webvpn-sso-siteminder)# max-retry-attempts 4
hostname(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
policy-server-secret	SiteMinder SSO サーバ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 サーバを作成します。
web-agent-url	セキュリティ アプライアンスが SiteMinder SSO 認証を要求する SSO サーバの 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 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。このモードには、**http-map** コマンドを使用してアクセスできます。この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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

max-uri-length コマンドをイネーブルにすると、セキュリティ アプライアンスは設定された制限内の URI があるメッセージのみを許可し、そのような URI がない場合には指定されたアクションを実行します。セキュリティ アプライアンスに 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、セキュリティ アプライアンスは TCP 接続をリセットし、syslog エントリを作成します。

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

mcc

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、GTP マップ 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。

mcc *country_code* **mnc** *network_code*

no mcc *country_code* **mnc** *network_code*

構文の説明

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。

デフォルト

デフォルトでは、セキュリティ アプライアンスは有効な 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、IMSI プレフィックス フィルタリングに使用されます。受信パケットの IMSI の MCC および MNC は、このコマンドで設定された MCC および MNC と比較され、一致しない場合はドロップされます。

このコマンドは、IMSI プレフィックス フィルタリングをイネーブルにするために使用する必要があります。複数のインスタンスを設定して許可する MCC と MNC の組み合わせを指定できます。デフォルトでは、セキュリティ アプライアンスは 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。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# mcc 111 mnc 222
hostname(config-gtpmap)#
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
debug gtp	GTP インスペクションの詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション 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 address

IP アドレスを電話プロキシ機能へのメディア接続に使用するように指定するには、電話プロキシ コンフィギュレーション モードで **media-termination address** 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-termination address *ip_address* [**rtp-min-port** *port1* **rtp-maxport** *port2*]

no media-termination address *ip_address* [**rtp-min-port** *port1* **rtp-maxport** *port2*]

構文の説明

ip_address	電話プロキシでメディア終端時に使用できるように作成する仮想 IP アドレスを指定します。電話プロキシのインスタンスごとに設定できる仮想インターフェイスは 1 つのみです。ASA 電話プロキシは、シグナリング メッセージのメディア アドレス部分にメディア終端 IP アドレスを挿入します。
rtp-max-port *port2*	メディア ターミネーション ポイントの RTP ポート範囲の最大値を指定します。*port2* には、32767 ～ 65535 の値を指定できます。
rtp-min-port *port1*	メディア ターミネーション ポイントの RTP ポート範囲の最小値を指定します。*port1* には、1024 ～ 16384 の値を指定できます。

デフォルト

デフォルトで、**rtp-min-port** キーワードの *port1* の値は 16384、**rtp-max-port** キーワードの *port2* の値は 32767 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
電話プロキシ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(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

セキュリティ アプライアンスには、次の基準を満たすメディア終端の IP アドレスが必要です。

- IP アドレスは、ネットワーク上の別のデバイスによって使用されることがなく、セキュリティ アプライアンスインターフェイスに接続されたネットワーク上にある未使用の IP アドレスである、パブリックにルーティング可能な IP アドレスです。
- セキュリティ アプライアンスインターフェイス IP アドレスと同じ IP アドレスを指定することはできません。特に、セキュリティ アプライアンスでセキュリティ レベルが最も低いインターフェイスと同じにすることはできません。
- IP アドレスは、既存のスタティック NAT 規則と重複できません。

- IP アドレスは、CUCM または TFTP サーバの IP アドレスと同じにはできません。
- 他のインターフェイスの IP 電話がメディア終端アドレスに到達できるように、他のインターフェイスにルートを追加します。

電話プロキシでサポートするコール数の規模を調整する必要がある場合は、メディア ターミネーション ポイントの RTP ポート範囲を設定します。

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。

```
hostname(config-phone-proxy)# media-termination address 192.168.1.4
```

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0（4）	このコマンドが導入されました。

使用上のガイドライン

sfp 設定は、固定速度（1000 Mbps）を使用するため、**speed** コマンドを使用すると、インターフェイスがリンク パラメータをネゴシエートす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。

```
hostname(config)# interface gigabitethernet1/1
hostname(config-if)# media-type sfp
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(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*

no member *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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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 コンテキストがセキュリティ アプライアンス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。セキュリティ アプライアンスでは、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。

```
hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(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 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*

no member-interface *physical_interface*

構文の説明

physical_interface	**gigabitethernet0/1** などのインターフェイス ID を識別します。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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

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。この場合、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コンフィギュレーションのみが物理パラメータ（**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を入力することもできます。

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は、最初に追加された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 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、メンバー インターフェイスの MAC アドレスとは関係なく使用される MAC アドレ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（**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は、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。

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

このユーザがメンバであるグループ名のリストを指定するには、ユーザ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。この属性をコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

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	このユーザが所属するグループを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ名属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このユーザ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。

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

関連コマンド

コマンド	説明
clear configure username	ユーザ名データベース全体または指定されたユーザ名のみをクリアします。

コマンド	説明
show running-config username	特定のユーザまたはすべてのユーザに対して現在実行されているユーザ コンフィギュレーションを表示します。
username	ユーザ名のデータベースを作成および管理します。

memory delayed-free-poisoner enable

delayed free-memory poisoner ツールをイネーブルにするには、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。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できます。

memory delayed-free-poisoner enable

no memory delayed-free-poisoner enable

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。

デフォルト

memory delayed-free-poisoner enable コマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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。

このツールをイネーブルにすると、セキュリティ アプライアンスで実行されているアプリケーションによるメモリ解放要求が 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、検証を手動で開始できます。

このコマンドの **no** 形式は、要求で参照されるキュー内のすべてのメモリを検証なしで空きメモリ プールに返し、統計カウンタをクリアします。

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。

```
hostname# 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
```

表 20-2 に、出力の重要な部分を示します。

表 20-2　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。
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。

memory delayed-free-poisoner validate

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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 ツールをイネーブル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。

```
hostname# 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、メモリの問題を容易に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。

memory caller-address *startPC endPC*

no memory caller-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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

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イネーブルにすると、セキュリティ アプライアンス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範囲、および **show memory-caller address** コマンドによる表示結果の例を示します。

```
hostname# memory caller-address 0x00109d5c 0x00109e08
hostname# memory caller-address 0x009b0ef0 0x009b0f14
hostname# memory caller-address 0x00cf211c 0x00cf4464
```

```
hostname# 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	セキュリティ アプライアンスのメモリ使用状況（プロファイリング）に関する情報を表示します。
show memory-caller address	セキュリティ アプライアンス上に設定されているアドレス範囲を表示します。

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）をイネーブルにするには、特権 EXEC モードで **memory profile enable** コマンドを使用します。メモリのプロファイルリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

memory profile enable peak *peak_value*

no memory profile enable peak *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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

メモリ プロファイリングをイネーブルにする前に、**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 テキスト範囲を設定する必要があります。

clear memory profile コマンドを入力するまで、一部のメモリはプロファイリング 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、セキュリティ アプライアンス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。

```
hostname# 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	セキュリティ アプライアンスのメモリ使用状況（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。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。

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

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、続けて **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、セキュリティ アプライアンス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。

```
hostname# 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。

```
hostname# 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	セキュリティ アプライアンスのメモリ使用状況（プロファイリング）に関する情報を表示します。
show memory-caller address	セキュリティ アプライアンス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セキュリティ アプライアンス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	セキュリティ アプライアンス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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

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。

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

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イネーブルにするには、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。

memory tracking enable

no memory tracking enable

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。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0（8）	このコマンドが導入されました。

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。

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。

```
hostname# 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。
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。

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 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。

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

no merge dacl

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 ユーザの場合は、ACL は Cisco AV ペア ACL、ダウンロード可能 ACL、および セキュリティ アプライアンス 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 が結合されているどうかを判断します。セキュリティ アプライアンス で設定される 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。

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 と結合されません。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA-server グループ コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

AV ペアおよびダウンロード可能な 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。

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

関連コマンド

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

message-length

設定された最大および最小の長さを満たさない GTP パケットをフィルタリングするには、GTP マップ 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。このモードには、**gtp-map** コマンドを使用してアクセスできます。コマンドを削除するには、**no** 形式を使用します。

message-length min *min_bytes* **max** *max_bytes*

no message-length min *min_bytes* **max** *max_bytes*

構文の説明

max	UDP ペイロードに許可されている最大バイト数を指定します。
max_bytes	UDP ペイロード内の最大バイト数。範囲は、1 ～ 65,536 です。
min	UDP ペイロードに許可されている最少バイト数を指定します。
min_bytes	UDP ペイロード内の最小バイト数。範囲は、1 ～ 65,536 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	No

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドで指定する長さは、GTP ヘッダーとメッセージの残りの部分（UDP パケットのペイロード）の合計です。

例

次に、長さが 20 ～ 300 バイトのメッセージを許可する例を示します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit message-length min 20 max 300
hostname(config-gtpmap)#
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
debug gtp	GTP インスペクションの詳細情報を表示します。

コマンド	説明
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション 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。

mfib forwarding

インターフェイスで MFIB 転送を再びイネーブルにするには、インターフェイス コンフィギュレーション モードで **mfib forwarding** を使用します。インターフェイスで MFIB 転送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。

mfib forwarding

no mfib forwarding

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。

デフォルト

multicast-routing コマンドは、デフォルトではすべてのインターフェイスの MFIB 転送をイネーブルにします

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

マルチキャスト ルーティングをイネーブルにすると、デフォルトではすべてのインターフェイスで MFIB 転送がイネーブルになります。特定のインターフェイスで MFIB 転送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。実行コンフィギュレーションには、このコマンドの **no** 形式だけが表示されます。

インターフェイスで MFIB 転送がディセーブルになっている場合、特に他の方法を設定しない限り、そのインターフェイスはマルチキャスト パケットを受け付けません。MFIB 転送がディセーブルになっていると、IGMP パケットも阻止されます。

例

次に、指定されたインターフェイスで MFIB 転送をディセーブルにする例を示します。

```
hostname(config)# interface GigabitEthernet 0/0
hostname(config-if)# no mfib forwarding
```

関連コマンド

コマンド	説明
multicast-routing	マルチキャスト ルーティングをイネーブルにします。
pim	インターフェイス上の PIM をイネーブルにします。

min-object-size

WebVPN セッションに対してセキュリティ アプライアンスがキャッシュできるオブジェクトの最小サイズを設定するには、キャッシュ モードで min-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。最小オブジェクト サイズを設定しないようにするには、値にゼロ（0）を入力します。

min-object-size *integer range*

構文の説明

integer range	0 ～ 10000 KB。

デフォルト

デフォルトのサイズは 0 KB です。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
キャッシュ モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

最小オブジェクト サイズは、最大オブジェクト サイズよりも小さい値である必要があります。キャッシュ圧縮がイネーブルになっている場合、セキュリティ アプライアンスは、オブジェクトを圧縮してからサイズを計算します。

例

次に、最大オブジェクト サイズを 40 KB に設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# min-object-size 40
hostname(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。

コマンド	説明
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。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。

mkdir

新規ディレクトリを作成するには、特権 EXEC モードで **mkdir** コマンドを使用します。

mkdir [**/noconfirm**] [**disk0: | disk1: | flash:**]*path*

構文の説明

noconfirm	（任意）確認プロンプトを表示しないようにします。
disk0:	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	（任意）外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。
path	作成するディレクトリの名前およびパス。

デフォルト

パスを指定しないと、現在の作業ディレクトリにディレクトリが作成されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

同じ名前のディレクトリがすでに存在する場合、新規のディレクトリは作成されません。

例

次の例は、「backup」という新しいディレクトリを作成する方法を示しています。

```
hostname# mkdir backup
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。
dir	ディレクトリの内容を表示します。
rmdir	指定されたディレクトリを削除します。
pwd	現在の作業ディレクトリを表示します。

mode

セキュリティ コンテキスト モードを single または multiple に設定するには、グローバル コンフィギュレーション モードで **mode** コマンドを使用します。1 つの セキュリティ アプライアンス をいくつかのパーティションに分けて複数の仮想デバイス（セキュリティ コンテキストと呼びます）に配置できます。各コンテキストは独立したデバイスとして動作し、独自のセキュリティ ポリシー、インターフェイス、および管理者で構成されています。複数のコンテキストが存在することは、複数のスタンドアロン アプライアンスが設置されていることと同じです。シングル モードでは、セキュリティ アプライアンスはシングル コンフィギュレーションを備え、単一デバイスとして動作します。マルチ モードでは、複数のコンテキストを作成し、それぞれに独自のコンフィギュレーションを設定できます。許可されるコンテキストの数は、保有するライセンスによって異なります。

mode {**single** | **multiple**} [**noconfirm**]

構文の説明

multiple	マルチ コンテキスト モードを設定します。
noconfirm	（任意）ユーザに確認を求めることなく、モードを設定します。このオプションは自動スクリプトで役立ちます。
single	コンテキスト モードを single に設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

マルチ コンテキスト モードでは、セキュリティ アプライアンスに各コンテキストのコンフィギュレーションが含まれ、それぞれのコンフィギュレーションでは、スタンドアロン デバイスに設定できるセキュリティ ポリシー、インターフェイス、およびほぼすべてのオプションが識別されます（コンテキスト コンフィギュレーションの場所を識別するには、**config-url** コマンドを参照してください）。システム管理者がコンテキストを追加および管理するには、コンテキストをシステム コンフィギュレーションに設定します。これが、シングル モード設定と同じく、スタートアップ コンフィギュレーションとなります。システム コンフィギュレーションは、セキュリティ アプライアンス の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

mode コマンドを使用してコンテキスト モードを変更すると、再起動するように求められます。

コンテキスト モード（シングルまたはマルチ）は、リブートされても持続されますが、コンフィギュレーション ファイルには保存されません。コンフィギュレーションを別のデバイスにコピーする必要がある場合は、**mode** コマンドを使用して、新規デバイスのモードを match に設定します。

シングル モードからマルチ モードに変換すると、セキュリティ アプライアンスは実行コンフィギュレーションを 2 つのファイルに変換します。システム コンフィギュレーションで構成される新規スタートアップ コンフィギュレーションと、（内部フラッシュ メモリのルート ディレクトリの）管理コンテキストで構成される admin.cfg です。元の実行コンフィギュレーションは、old_running.cfg として（内部フラッシュ メモリのルート ディレクトリに）保存されます。元のスタートアップ コンフィギュレーションは保存されません。セキュリティ アプライアンス は、管理コンテキストのエントリをシステム コンフィギュレーションに「admin」という名前で自動的に追加します。

マルチ モードからシングル モードに変換する場合は、先にスタートアップ コンフィギュレーション全体（使用可能な場合）をセキュリティ アプライアンスにコピーすることを推奨します。マルチ モードから継承されるシステム コンフィギュレーションは、シングル モード デバイスで完全に機能するコンフィギュレーションではありません。

マルチ コンテキスト モードのすべての機能がサポートされるわけではありません。詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

例

次に、モードを multiple に設定する例を示します。

```
hostname(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Convert the system configuration? [confirm] y
Flash Firewall mode: multiple

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode

Rebooting....

Booting system, please wait...
```

次に、モードを single に設定する例を示します。

```
hostname(config)# mode single
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Flash Firewall mode: single

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode



Rebooting....
```

```
Booting system, please wait...
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにコンテキストを設定し、コンテキスト コンフィギュレーション モードを開始します。
show mode	現在のコンテキスト モード（シングルまたはマルチ）を表示します。

monitor-interface

特定のインターフェイスでヘルス モニタリングをイネーブルにするには、グローバル コンフィギュレーション モードで **monitor-interface** コマンドを使用します。インターフェイスのモニタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

monitor-interface *if_name*

no monitor-interface *if_name*

構文の説明

if_name	モニタするインターフェイスの名前を指定します。

デフォルト

物理インターフェイスのモニタリングは、デフォルトでイネーブルになっています。論理インターフェイスのモニタリングは、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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンス用にモニタできるインターフェイスの数は 250 です。インターフェイス ポーリング頻度ごとに、セキュリティ アプライアンス フェールオーバー ペア間で hello メッセージが交換されます。フェールオーバー インターフェイスのポーリング時間は 3 ～ 15 秒です。たとえば、ポーリング時間を 5 秒に設定すると、あるインターフェイスで 5 回連続して hello が検出されないと（25 秒間）、そのインターフェイスでテストが開始します。

モニタ対象のフェールオーバー インターフェイスには、次のステータスが設定されます。

- Unknown：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- Normal：インターフェイスはトラフィックを受信しています。
- Testing：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- Link Down：インターフェイスまたは VLAN は管理のためにダウンしています。
- No Link：インターフェイスの物理リンクがダウンしています。
- Failed：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

アクティブ/アクティブ フェールオーバーでは、このコマンドはコンテキスト内でだけ有効です。

例

次の例では、「inside」という名前のインターフェイスでモニタリングをイネーブルにしています。

```
hostname(config)# monitor-interface inside
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure monitor-interface	すべてのインターフェイスでデフォルトのインターフェイス ヘルス モニタリングに戻します。
failover interface-policy	モニタするインターフェイスの数または割合を指定します。モニタの対象となるのは、障害が発生すると、フェールオーバーが発生するインターフェイスです。
failover polltime	インターフェイスでの hello メッセージ間の間隔を指定します（Active/Standby フェールオーバー）。
polltime interface	インターフェイスでの hello メッセージ間の間隔を指定します（Active/Active フェールオーバー）。
show running-config monitor-interface	実行コンフィギュレーション内の **monitor-interface** コマンドを表示します。

more

ファイルの内容を表示するには、**more** コマンドを使用します。

more {**/ascii** | **/binary**| **/ebcdic** | **disk0:** | **disk1:** | **flash:** | **ftp:** | **http:** | **https:** | **system:** | **tftp:**}*filename*

構文の説明

/ascii	（任意）バイナリ ファイルをバイナリ モード、ASCII ファイルをバイナリ モードで表示します。
/binary	（任意）任意のファイルをバイナリ モードで表示します。
/ebcdic	（任意）バイナリ ファイルを EBCDIC で表示します。
disk0:	（任意）内部フラッシュ メモリのファイルを表示します。
disk1:	（任意）外部フラッシュ メモリ カードのファイルを表示します。
flash:	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。
ftp:	（任意）FTP サーバ上のファイルを表示します。
http:	（任意）Web サイトのファイルを表示します。
https:	（任意）セキュア Web サイトのファイルを表示します。
system:	（任意）ファイル システムを表示します。
tftp:	（任意）TFTP サーバ上のファイルを表示します。
filename	表示するファイルの名前を指定します。

デフォルト

ASCII モード

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

more filesystem: コマンドは、ローカル ディレクトリまたはファイル システムのエイリアスを入力するように求めます。

例

次の例は、「test.cfg」という名前のローカル ファイルの内容を表示する方法を示しています。

```
hostname# more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005
```

```
XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@my_context.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

関連コマンド

コマンド	説明
cd	指定されたディレクトリに変更します。
pwd	現在の作業ディレクトリを表示します。

mount（CIFS）

セキュリティ アプライアンスから Common Internet File System（CIFS; 共通インターネット ファイル システム）にアクセスできるようにするには、グローバル コンフィギュレーション モードで **mount** コマンドを使用します。このコマンドを使用すると、設定マウント cifs コンフィギュレーション モードを開始できます。CIFS ネットワーク ファイル システムをマウント解除するには、このコマンドの **no** 形式を使用します。

mount *name* **type cifs server** *server-name* **share** *share* **status enable | status disable [domain** *domain-name* **] username** *username* **password** *password*

[**no**] **mount** *name* **type cifs server** *server-name* **share** *share* **status enable | status disable [domain** *domain-name* **] username** *username* **password** *password*

構文の説明

domain *domain-name*	（任意）CIFS ファイル システムでのみ、この引数には Windows NT ドメイン名を指定します。最大 63 文字が許可されます。
name	ローカル CA に割り当てられる既存のファイル システムの名前を指定します。
no	すでにマウント済みの CIFS ファイル システムを削除し、アクセスできないようにします。
password *password*	ファイル システムのマウントのための認可されたパスワードを指定します。
server *server-name*	CIFS ファイル システム サーバの定義済みの名前（またはドット付き 10 進表記の IP アドレス）を指定します。
share *sharename*	サーバ内のファイル データにアクセスするために、特定のサーバ共有（フォルダ）を名前で明示的に識別します。
status enable/disable	ファイル システムの状態をマウント済みまたはマウント解除済み（使用可能または使用不能）として識別します。
type	マウントするファイル システムの CIFS タイプを指定します。代替の **type** キーワードについては、**mount（FTP）**コマンドを参照してください。
type cifs	マウントされるファイル システムが CIFS であることを指定します。CIFS は、CIFS 共有ディレクトリにボリューム マウント機能を提供するファイル システムです。
user *username*	ファイル システムのマウントが認可されているユーザ名。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
設定マウント cifs コンフィギュレーション	•	•	•	—	•
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

mount コマンドは、Installable File System（IFS）を使用して、CIFS ファイル システムをマウントします。IFS（ファイル システム API）を使用すると、セキュリティ アプライアンスはファイル システム用のドライバを認識し、ロードすることができます。

mount コマンドは、セキュリティ アプライアンス上の CIFS ファイル システムを UNIX ファイル ツリーにアタッチします。逆に、**no mount** コマンドはそのアタッチを解除します。

mount コマンドに指定されている *mount-name* は、セキュリティ アプライアンスにすでにマウントされているファイル システムを参照するために、他の CLI コマンドで使用されます。たとえば、ローカル認証局用にファイル ストレージを設定する **database** コマンドでは、データベース ファイルをフラッシュ ストレージでないストレージに保存するために、すでにマウントされているファイル システムのマウント名が必要です。

CIFS リモート ファイル アクセス プロトコルは、アプリケーションがローカル ディスクおよびネットワーク ファイル サーバ上のデータを共有する方法と互換性があります。TCP/IP を運用し、インターネットのグローバル DNS を使用する CIFS は、Windows オペレーティング システムにネイティブのファイル共有プロトコルである Microsoft のオープンでクロス プラットフォームの Server Message Block（SMB; サーバ メッセージ ブロック）プロトコルを拡張したものです。

mount コマンドを使用した後は、必ずルート シェルを終了してください。mount-cifs-config モードの **exit** キーワードは、ユーザをグローバル コンフィギュレーション モードに戻します。

再接続するには、接続をストレージに再マッピングします。

（注） CIFS ファイル システムと FTP ファイル システムのマウントがサポートされています（**mount** *name* **type ftp** コマンドを参照）。Network File System（NFS; ネットワーク ファイル システム）ボリュームのマウントは、このリリースではサポートされていません。

例

次に、*cifs://amer;chief:big-boy@myfiler02/my_share* を *cifs_share* というラベルとしてマウントする例を示します。

```
hostname(config)# mount cifs_share type CIFS
hostname (config-mount-cifs)# server myfiler02a
```

関連コマンド

コマンド	説明
debug cifs	CIFS デバッグ メッセージをロギングします。
debug ntdomain	Web VPN NT ドメイン デバッグ メッセージをロギングします。
debug webvpn cifs	WebVPN CIFS デバッグ メッセージをロギングします。
dir all-filesystems	セキュリティ アプライアンスにマウントされているすべてのファイル システムのファイルを表示します。

mount（FTP）

セキュリティ アプライアンスからファイル転送プロトコル（FTP）ファイル システムにアクセスできるようにするには、グローバル コンフィギュレーション モードで **mount** *name* **type ftp** コマンドを使用して、マウント FTP コンフィギュレーション モードを開始します。**no mount** *name* **type ftp** コマンドは、FTP ネットワーク ファイル システムをマウント解除するために使用されます。

[**no**] **mount** *name* **type FTP server** *server-name* **path** *pathname* **status enable | status disable mode active | mode passive username** *username* **password** *password*

構文の説明

exit	Mount-FTP コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻ります。
ftp	マウントされるファイル システムが FTP であることを指定します。FTP は Linux カーネル モジュールであり、FTP 共有ディレクトリをマウントできるようにする FTP ボリューム マウント機能で Virtual File System（VFS; 仮想ファイル システム）を拡張したものです。
mode	FTP 転送モードをアクティブまたはパッシブとして識別します。
no	すでにマウントされている FTP ファイル システムを削除し、アクセスできないようにします。
password *password*	ファイル システムのマウントのための認可されたパスワードを指定します。
path *pathname*	指定された FTP ファイル システム サーバへのディレクトリ パス名を指定します。パス名にスペースを含めることはできません。
server *server-name*	FTPFS ファイル システム サーバの定義済みの名前（またはドット付き 10 進表記の IP アドレス）を指定します。
status enable/disable	ファイル システムの状態をマウント済みまたはマウント解除済み（使用可能または使用不能）として識別します。
username *username*	ファイル システムのマウントが認可されているユーザ名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
設定マウント ftp	•	•	•	—	•
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

mount *name* **type ftp** コマンドは、Installable File System（IFS）を使用して、指定されたネットワーク ファイル システムをマウントします。IFS（ファイル システム API）を使用すると、セキュリティ アプライアンスはファイル システム用のドライバを認識し、ロードすることができます。

FTP ファイル システムが実際にマウントされていることを確認するには、**dir all-filesystems** 命令を使用します。

mount コマンドに指定されているマウント名は、他の CLI コマンドがセキュリティ アプライアンスですでにマウントされているファイル システムを参照するときに使用されます。ローカル認証局用にファイル ストレージを設定する **database** コマンドでは、データベース ファイルをフラッシュ ストレージでないストレージに保存するために、すでにマウントされているファイル システムのマウント名が必要です。

（注）　FTP-type マウントの作成時に **mount** コマンドを使用するには、FTP サーバに UNIX ディレクトリ リスト スタイルが必要です。Microsoft FTP サーバには、デフォルトで MS-DOS ディレクトリ リスト スタイルがあります。

（注）　CIFS ファイル システムと FTP ファイル システムのマウントがサポートされています （**mount** *name* **type ftp** コマンドを参照）。Network File System（NFS; ネットワーク ファイル システム）ボリュームのマウントは、このリリースではサポートされていません。

例

次に、*ftp://amor;chief:big-kid@myfiler02* を *my ftp:* というラベルとしてマウントする例を示します。

```
hostname(config)# mount myftp type ftp server myfiler02a path status enable username
chief password big-kid
```

関連コマンド

コマンド	説明
debug webvpn	WebVPN デバッグ メッセージをロギングします。
ftp mode passive	セキュリティ アプライアンス上の FTP クライアントと FTP サーバとの通信を制御します。

mroute

スタティック マルチキャスト ルートを設定するには、グローバル コンフィギュレーション モードで **mroute** コマンドを使用します。スタティック マルチキャスト ルートを削除するには、このコマンドの **no** 形式を使用します。

mroute *src smask* {*in_if_name* [**dense** *output_if_name*] | *rpf_addr*} [*distance*]

no mroute *src smask* {*in_if_name* [**dense** *output_if_name*] | *rpf_addr*} [*distance*]

構文の説明

dense *output_if_name*	（任意）デンス モード出力のインターフェイス名。 **dense** *output_if_name* キーワードと引数のペアは、SMR スタブ マルチキャスト ルーティング（igmp 転送）に対してだけサポートされます。
distance	（任意）ルートのアドミニストレーティブ ディスタンス。ディスタンスが小さいルートが優先されます。デフォルトは 0 です。
in_if_name	mroute の着信インターフェイス名を指定します。
rpf_addr	mroute の着信インターフェイスを指定します。RPF アドレスが PIM ネイバーである場合、PIM Join メッセージ、接合メッセージ、および Prune メッセージがそのアドレスに送信されます。*rpf-addr* 引数には、直接接続されたシステムのホスト IP アドレスまたはネットワーク / サブネット番号を指定します。ルートである場合、直接接続されたシステムを検索するために、ユニキャスト ルーティング テーブルから再帰検索が実施されます。
smask	マルチキャスト送信元ネットワーク アドレス マスクを指定します。
src	マルチキャスト送信元の IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドを使用すると、マルチキャスト送信元の検索場所をスタティックに設定できます。セキュリティ アプライアンスは、特定の送信元にユニキャスト パケットを送信する際に使用したものと同じインターフェイスでマルチキャスト パケットを受信するものと想定します。場合によっては、マルチキャスト ルーティングをサポートしないルートをバイパスするなど、マルチキャスト パケットがユニキャスト パケットとは別のパスをたどることがあります。

スタティック マルチキャスト ルートはアドバタイズも再配布もされません。

マルチキャスト ルート テーブルの内容を表示するには、**show mroute** コマンドを使用します。実行コンフィギュレーションで mroute コマンドを表示するには、**show running-config mroute** コマンドを使用します。

例

次に、**mroute** コマンドを使用して、スタティック マルチキャスト ルートを設定する例を示します。

```
hostname(config)# mroute 172.16.0.0 255.255.0.0 inside
```

関連コマンド

コマンド	説明
clear configure mroute	コンフィギュレーションから **mroute** コマンドを削除します。
show mroute	IPv4 マルチキャスト ルーティング テーブルを表示します。
show running-config mroute	コンフィギュレーションの **mroute** コマンドを表示します。

msie-proxy except-list

クライアント PC でローカル バイパスを対象に Microsoft Internet Explorer のブラウザ プロキシ例外リスト設定を設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy except-list** コマンドを入力します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

msie-proxy except-list {value *server*[*:port*] **| none}**

no msie-proxy except-list

構文の説明

none	IP アドレス / ホスト名またはポートがなく、例外リストを継承しないことを示します。
value *server:port*	IP アドレスまたは MSIE サーバの名前、およびこのクライアント PC に適用されるポートを指定します。ポート番号は任意です。

デフォルト

デフォルトでは、msie-proxy except-list 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

例

次に、Microsoft Internet Explorer のプロキシ例外リストを設定する例を示します。IP アドレス 192.168.20.1 のサーバで構成され、ポート 880 を使用し、FirstGroup というグループ ポリシーを対象とします。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

msie-proxy local-bypass

クライアント PC の Microsoft Internet Explorer のブラウザ プロキシ ローカル バイパス設定を設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy local-bypass** コマンドを入力します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

msie-proxy local-bypass {enable | disable}

no msie-proxy local-bypass {enable | disable}

構文の説明

disable	クライアント PC の Microsoft Internet Explorer のブラウザ プロキシ ローカル バイパス設定をディセーブルにします。
enable	クライアント PC の Microsoft Internet Explorer のブラウザ プロキシ ローカル バイパス設定をイネーブルにします。

デフォルト

デフォルトでは、msie-proxy local-bypass 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、FirstGroup というグループ ポリシーの Microsoft Internet Explorer のプロキシ ローカル バイパスをイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy local-bypass enable
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

msie-proxy method

クライアント PC のブラウザ プロキシ アクション（「メソッド」）を設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy method** コマンドを入力します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]

no msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]

（注）　この構文に適用される条件については、「使用上のガイドライン」を参照してください。

構文の説明

auto-detect	クライアント PC の Internet Explorer または Firefox で自動プロキシ サーバ検出の使用をイネーブルにします。
no-modify	このクライアント PC では、ブラウザの HTTP ブラウザ プロキシ サーバ設定をそのままにしておきます。
no-proxy	このクライアント PC では、ブラウザの HTTP プロキシ設定をディセーブルにします。
use-pac-url	**msie-proxy pac-url** コマンドに指定されているプロキシ自動コンフィギュレーション ファイル URL から HTTP プロキシ サーバ設定を取得するように Internet Explorer に指示します。このオプションは、Internet Explorer にだけ有効です。
use-server	**msie-proxy server** コマンドに設定された値を使用するように、ブラウザの HTTP プロキシ サーバ設定を設定します。

デフォルト

デフォルトのメソッドは use-server 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(2)	use-pac-url オプションが追加されました。

使用上のガイドライン

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行には、最大 100 文字含めることができます。

Safari ブラウザは、auto-detect をサポートしません。Firefox ブラウザおよび Safari ブラウザでは、これらのコマンド オプションを一度に 1 つだけ使用できます。Microsoft Internet Explorer は、このコマンド オプションの次の組み合わせをサポートします。

[no] msie-proxy method no-proxy

[no] msie-proxy method no-modify

[no] msie-proxy method [auto-detect] [use-server] [use-pac-url]

テキスト エディタを使用して、自分のブラウザにプロキシ自動コンフィギュレーション（.pac）ファイルを作成できます。.pac ファイルとは、URL のコンテンツに応じて、使用する 1 つ以上のプロキシ サーバを指定するロジックを含む JavaScript ファイルです。.pac ファイルは、Web サーバにあります。**use-pac-url** を指定すると、Internet Explorer は .pac ファイルを使用してプロキシ設定を判別します。.pac ファイルの取得元の URL を指定するには、**msie-proxy pac-url** コマンドを使用します。

例

次に、FirstGroup というグループ ポリシーの Microsoft Internet Explorer プロキシ設定として自動検出を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy method auto-detect
hostname(config-group-policy)#
```

次に、クライアント PC のサーバとしてサーバ QASERVER、ポート 1001 を使用するように、FirstGroup というグループ ポリシーの Microsoft Internet Explorer プロキシ設定を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server QAserver:port 1001
hostname(config-group-policy)# msie-proxy method use-server
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
msie-proxy pac-url	プロキシ自動コンフィギュレーション ファイルの取得先となる URL を指定します。
msie-proxy server	クライアント PC に対して、Microsoft Internet Explorer のブラウザ プロキシ サーバおよびポートを設定します。
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

msie-proxy pac-url

プロキシ情報の検索場所をブラウザに指示するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy pac-url** コマンドを入力します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

msie-proxy pac-url {**none** | **value** *url*}

no msie-proxy pac-url

構文の説明

none	URL 値がないことを指定します。
value *url*	使用するプロキシ サーバが 1 つ以上定義されているプロキシ自動コンフィギュレーション ファイルをブラウザが取得できる Web サイトの URL を指定します。

デフォルト

デフォルト値は none です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

要件

プロキシ自動コンフィギュレーション機能を使用するには、リモート ユーザは Cisco AnyConnect VPN クライアントを使用する必要があります。プロキシ自動コンフィギュレーション URL の使用をイネーブルにするには、**msie-proxy method** コマンドを **use-pac-url** オプションとともに設定する必要があります。

このコマンドを使用する理由

多くのネットワーク環境が、Web ブラウザを特定のネットワーク リソースに接続する HTTP プロキシを定義しています。HTTP トラフィックがネットワーク リソースに到達できるのは、プロキシがブラウザに指定され、クライアントが HTTP トラフィックをプロキシにルーティングする場合だけです。SSLVPN トンネルにより、HTTP プロキシの定義が複雑になります。企業ネットワークにトンネリングするときに必要なプロキシが、ブロードバンド接続経由でインターネットに接続されるときや、サード パーティ ネットワーク上にあるときに必要なものとは異なることがあるためです。

また、大規模ネットワークを構築している企業では、複数のプロキシ サーバを設定し、一時的な状態に基づいてユーザがその中からプロキシ サーバを選択できるようにすることが必要になる場合があります。.pac ファイルを使用すると、管理者は数多くのプロキシからどのプロキシを社内のすべてのクライアント コンピュータに使用するかを決定する単一のスクリプト ファイルを作成できます。

次に、PAC ファイルを使用する例をいくつか示します。

- ロード バランシングのためリストからプロキシをランダムに選択します。
- サーバのメンテナンス スケジュールに対応するために、時刻または曜日別にプロキシを交代で使用します。
- プライマリ プロキシで障害が発生した場合に備えて、使用するバックアップ プロキシ サーバを指定します。
- ローカル サブネットを元に、ローミング ユーザ用に最も近いプロキシを指定します。

プロキシ自動コンフィギュレーション機能の使用方法

テキスト エディタを使用して、自分のブラウザにプロキシ自動コンフィギュレーション（.pac）ファイルを作成できます。.pac ファイルとは、URL のコンテンツに応じて、使用する 1 つ以上のプロキシ サーバを指定するロジックを含む JavaScript ファイルです。.pac ファイルの取得元の URL を指定するには、**msie-proxy pac-url** コマンドを使用します。次に、**msie-proxy method** コマンドに **use-pac-url** を指定すると、ブラウザは .pac ファイルを使用してプロキシ設定を判別します。

例

次に、FirstGroup というグループ ポリシーのプロキシ設定を www.mycompanyserver.com という URL から取得するように、ブラウザを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy pac-url value http://www.mycompanyserver.com
hostname(config-group-policy)#
```

次に、FirstGroup というグループ ポリシーのプロキシ自動コンフィギュレーション機能をディセーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy pac-url none
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
msie-proxy method	クライアント PC のブラウザ プロキシ アクション（「メソッド」）を設定します。
msie-proxy server	クライアント PC に対して、Microsoft Internet Explorer のブラウザ プロキシ サーバおよびポートを設定します。
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

msie-proxy server

クライアント PC 用に Microsoft Internet Explorer のブラウザ プロキシ サーバおよびポートを設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy server** コマンドを入力します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

msie-proxy server {value *server*[*:port*] **| none}**

no msie-proxy server

構文の説明

none	プロキシ サーバに指定されている IP アドレス/ホスト名またはポートがなく、サーバが継承されないことを示します。
value *server:port*	IP アドレスまたは MSIE サーバの名前、およびこのクライアント PC に適用されるポートを指定します。ポート番号は任意です。

デフォルト

デフォルトでは、no msie-proxy server が指定されます。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

例

次に、Microsoft Internet Explorer プロキシ サーバとして IP アドレス 192.168.10.1 を設定し、ポート 880 を使用し、FirstGroup というグループ ポリシーを対象にする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server value 192.168.21.1:880
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

mtu

インターフェイスの最大伝送単位を指定するには、グローバル コンフィギュレーション モードで **mtu** コマンドを使用します。イーサネット インターフェイスの MTU ブロック サイズを 1500 にリセットするには、このコマンドの **no** 形式を使用します。このコマンドは、IPv4 トラフィックと IPv6 トラフィックをサポートしています。

mtu *interface_name bytes*

no mtu *interface_name bytes*

構文の説明

bytes	MTU のバイト数。有効な値は、64 ～ 65,535 バイトです。
interface_name	内部または外部ネットワーク インターフェイス名。

デフォルト

イーサネット インターフェイスのデフォルトの *bytes* は 1500 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

mtu コマンドを使用すると、接続で送信されるデータ サイズを設定できます。MTU 値よりも大きいデータは、送信前にフラグメント化されます。

セキュリティ アプライアンスは、IP パス MTU ディスカバリを（RFC 1191 での規定に従って）サポートします。これにより、ホストはパスに沿ったさまざまなリンクで許容される最大 MTU サイズをダイナミックに検出し、各サイズの差に対処できます。パケットがインターフェイスに対して設定されている MTU よりも大きくなっているものの、「Don't Fragment」（DF）ビットが設定されているために、セキュリティ アプライアンスがデータグラムを転送できないことがあります。ネットワーク ソフトウェアは、メッセージを送信ホストに送信して、問題を警告します。送信ホストは、パスに沿ったすべてのリンクのうち最小のパケット サイズに適合するように、宛先へのパケットをフラグメント化する必要があります。

イーサネット インターフェイスのブロックのデフォルトの MTU は 1500 バイトです（最大値でもあります）。ほとんどのアプリケーションではこの値で十分ですが、ネットワーク状況によってはこれよりも小さい値にすることもできます。

Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）を使用するときは、L2TP ヘッダーと IPSec ヘッダーの長さを踏まえて MTU サイズを 1380 に設定することを推奨します。

例

次に、インターフェイスの MTU を指定する例を示します。

```
hostname(config)# show running-config mtu
mtu outside 1500
mtu inside 1500
hostname(config)# mtu inside 8192
hostname(config)# show running-config mtu
mtu outside 1500
mtu inside 8192
```

関連コマンド

コマンド	説明
clear configure mtu	すべてのインターフェイスの設定済み最大伝送単位値をクリアします。
show running-config mtu	現在の最大伝送単位のブロック サイズを表示します。

multicast boundary

管理用スコープのマルチキャスト アドレスのマルチキャスト境界を設定するには、インターフェイス コンフィギュレーション モードで **multicast boundary** コマンドを使用します。境界を削除するには、このコマンドの **no** 形式を使用します。マルチキャスト境界により、マルチキャスト データ パケット フローが制限され、同じマルチキャスト グループ アドレスを複数の管理ドメインで再利用できるようになります。

multicast boundary *acl* [**filter-autorp**]

no multicast boundary *acl* [**filter-autorp**]

構文の説明

acl	アクセス リストの名前または番号を指定します。アクセス リストには、境界の影響を受けるアドレスの範囲を定義します。このコマンドでは、標準 ACL だけを使用します。拡張 ACL はサポートされていません。
filter-autorp	境界 ACL によって拒否された Auto-RP メッセージをフィルタリングします。指定されていない場合、すべての Auto-RP メッセージが通過します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、*acl* 引数によって定義されている範囲でマルチキャスト グループ アドレスをフィルタリングするようにインターフェイスに管理用スコープの境界を設定するために使用されます。影響を受けるアドレス範囲は、標準アクセス リストによって定義されます。このコマンドが設定されている場合、マルチキャスト データ パケットはいずれの方向であっても境界を通過できません。マルチキャスト データ パケット フローを制限すると、同じマルチキャスト グループ アドレスを複数の管理ドメインで再利用できます。

filter-autorp キーワードを設定した場合、管理用スコープの境界は Auto-RP 検出メッセージおよびアナウンス メッセージを調べ、境界 ACL によって拒否される Auto-RP パケットから Auto-RP グループ範囲アナウンスメントを削除します。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界を通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

例

次に、すべての管理用スコープのアドレスの境界を設定し、Auto-RP メッセージをフィルタリングする例を示します。

```
hostname(config)# access-list boundary_test deny 239.0.0.0 0.255.255.255
hostname(config)# access-list boundary_test permit 224.0.0.0 15.255.255.255
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# multicast boundary boundary_test filter-autorp
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。

multicast-routing

セキュリティ アプライアンスの IP マルチキャスト ルーティングをイネーブルにするには、グローバル コンフィギュレーション モードで **multicast routing** コマンドを使用します。IP マルチキャスト ルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

multicast-routing

no multicast-routing

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。

デフォルト

multicast-routing コマンドは、デフォルトですべてのインターフェイスで PIM および IGMP をイネーブルにします。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

multicast-routing コマンドは、すべてのインターフェイスで PIM および IGMP をイネーブルにします。

（注） PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

セキュリティ アプライアンスが PIM RP である場合は、セキュリティ アプライアンスの未変換の外部アドレスを RP アドレスとして使用します。

マルチキャスト ルーティング テーブルのエントリの数は、システムに搭載されているメモリの量によって制限されます。表 20-3 に、セキュリティ アプライアンス上のメモリの量に基づく特定のマルチキャスト テーブルのエントリの最大数を示します。この上限に達すると、新しいエントリは廃棄されます。

表 20-3　マルチキャスト テーブルのエントリの制限

テーブル	16 MB	128 MB	128 + MB
MFIB	1000	3000	5000
IGMP グループ	1000	3000	5000
PIM ルート	3000	7000	12000

例

次に、セキュリティ アプライアンスで IP マルチキャスト ルーティングをイネーブルにする例を示します。

```
hostname(config)# multicast-routing
```

関連コマンド

コマンド	説明
igmp	インターフェイスに対して IGMP をイネーブルにします。
pim	インターフェイス上の PIM をイネーブルにします。