CHAPTER 20

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

mac address

アクティブ装置およびスタンバイ装置の仮想 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*]

シンタックスの説明

phy_if	MAC アドレスを設定するインターフェイスの物理名。
active_mac	アクティブ装置の仮想 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。h は、16 ビットの 16 進数値です。
standby_mac	スタンバイ装置の仮想 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。h は、16 ビットの 16 進数値です。

デフォルト

デフォルトは次のとおりです。

- アクティブ装置のデフォルト MAC アドレス：00a0.c9*physical_port_number*.*failover_group_id*01
- スタンバイ装置のデフォルト MAC アドレス：00a0.c9*physical_port_number*.*failover_group_id*02

コマンド モード

次の表は、このコマンドを入力でき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
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

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

同じネットワーク上に Active/Active 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。ネットワーク上の MAC アドレスを重複させないためには、各物理インターフェイスに必ずアクティブとスタンバイの仮想 MAC アドレスを割り当てるようにしてください。

例

次の例（抜粋）は、フェールオーバー グループに対して適用可能なコンフィギュレーションを示しています。

```
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作業で割り当てるには、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、このコマンドによって各コンテキストのインターフェイスに異なる MAC アドレスを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*]]

シンタックスの説明

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 進数値です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。フェールオーバーを使用する場合、この MAC アドレスはアクティブな MAC アドレスになります。
standby *mac_address*	（オプション）フェールオーバー用のスタンバイ 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、この新たにアクティブになった装置がアクティブな MAC アドレスの使用を開始してネットワーク障害を最小限にする一方で、アクティブでなくなった方の装置はスタンバイ 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。物理インターフェイスの MAC アドレスを設定するコマンドもある（シングル モードのこのコマンドを含む）ので、継承されるアドレスはそのコンフィギュレーションによって決定されます。

コマンド モード

次の表は、このコマンドを入力でき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
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

マルチ コンテキスト モードで、コンテキスト間のインターフェイスを共有する場合、一意の MAC アドレスを各コンテキストのインターフェイスに割り当てることができます。この機能により、セキュリティ アプライアンスではパケットを適切なコンテキストに分類しやすくなります。一意の MAC アドレスなしに共有インターフェイスを使用することは可能ですが、いくつかの制限があります。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

このコマンドを使用して各 MAC アドレスを手作業で割り当てるか、**mac-address auto** コンドを使用してコンテキストの共有インターフェイスの MAC アドレスを自動的に生成することができます。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します。

シングル コンテキスト モードの場合、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、一意の MAC アドレスをサブインターフェイスに割り当てることもできます。たとえば、サービス プロバイダーは MAC アドレスに基づいてアクセスを制御する場合もあります。

MAC アドレスは、他のコマンドや方法を使用して設定することもできます。MAC アドレスの設定方法には、次のような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およびサブインターフェイスに対して作用します。マルチ コンテキスト モードの場合は、各コンテキスト内で MAC アドレスを設定します。この機能を利用すると、同じインターフェイスに対して、複数のコンテキストでそれぞれ別の 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 モードの **failover mac address** コマンド（Active/Standby フェールオーバーの場合）。

   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** コマンドまたは **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 モードの **mac address** コマンド（Active/Active フェールオーバーの場合）。

   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** コマンドまたは **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、コンテキスト内の共有インターフェイスに適用されます。

5. Active/Active フェールオーバーにおける、物理インターフェイスのアクティブ MAC アドレスとスタンバイ 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** コマンドまたは **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** コマンドまたは **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

次の例では、GigabitEthernet 0/1.1 の MAC アドレスを設定します。

```
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 モードをシングルまたはマルチに設定します。
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 アドレスを各共有コンテキスト 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。MAC アドレスの自動割り当て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

no mac-address auto

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

自動生成はデフォルトではディセーブルです。

コマンド モード

次の表は、このコマンドを入力でき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
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。

使用上のガイドライン

コンテキストでインターフェイスを共有するには、一意の MAC アドレスを各コンテキストのインターフェイスに割り当てることをお勧めします。MAC アドレスを使用してコンテキスト内のパケットを分類します。インターフェイスを共有する場合に、各コンテキストのインターフェイス用の MAC アドレスがないときには、宛先 IP アドレスを使用してパケットを分類します。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。MAC アドレス方式と比較すると、この方式にはいくつかの制限があります。パケットの分類については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

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サブインターフェイスはすべて同一のバーンドイン MAC アドレスを使用します。

フェールオーバーで使用する場合、セキュリティ アプライアンスは各インターフェイスに対して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場合、この新たにアクティブになった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障害を最小限にします。**mac-address auto** コマンドは共有インターフェイスのみを設定するため、**mac-address** コマンドまたは **failover mac address** コマンドを使用して、Active/Standby コンフィギュレーションで非共有インターフェイスに仮想 MAC アドレスを依然として設定する必要があります（Active/Active フェールオーバーは仮想 MAC アドレスを物理インターフェイスに自動的に割り当てます）。

インターフェイスをコンテキストに割り当てると、新しい MAC アドレスがただちに生成されます。コンテキスト インターフェイスを生成した後にこのコマンドをイネーブルにした場合、このコマンドを入力するとただちに MAC アドレスがすべてのインターフェイスに生成されます。**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 アドレスを再度使用します。

MAC アドレスは次の形式を使用して生成します。

- アクティブ装置の MAC アドレス：12*_slot.port_subid.contextid*.
- スタンバイ装置の MAC アドレス：02*_slot.port_subid.contextid*.

インターフェイス スロットの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* はサブインターフェイスの内部 ID です。この ID は表示されません。*contextid* はコンテキストの内部 ID です。**show context detail** コマンドを使用して表示します。たとえば、ID 1 を持つコンテキストのインターフェイス GigabitEthernet 0/1.200 には次の生成された MAC アドレスが設定されています。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

まれなケースですが、生成された MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合した場合は、コンテキスト内でインターフェイスの MAC アドレスを手作業で設定します。MAC アドレスを手作業で設定するには、**mac-address** コマンドを参照してください。

MAC アドレスは、他のコマンドや方法を使用して設定することもできます。MAC アドレスの設定方法には、次のような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およびサブインターフェイスに対して作用します。マルチ コンテキスト モードの場合は、各コンテキスト内で MAC アドレスを設定します。この機能を利用すると、同じインターフェイスに対して、複数のコンテキストでそれぞれ別の 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 モードの **failover mac address** コマンド（Active/Standby フェールオーバーの場合）。

   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** コマンドまたは **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 モードの **mac address** コマンド（Active/Active フェールオーバーの場合）。

   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** コマンドまたは **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、コンテキスト内の共有インターフェイスに適用されます。

5. Active/Active フェールオーバーにおける、物理インターフェイスのアクティブ MAC アドレスとスタンバイ 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** コマンドまたは **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** コマンドまたは **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

次の例では、MAC アドレスの自動生成をイネーブルにします。

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

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（アクティブおよびスタンバイ）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 モードをシングルまたはマルチに設定します。
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 エントリの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。5 分の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。

mac-address-table *aging-time* *timeout_value*

no mac-address-table *aging-time*

シンタックスの説明

timeout_value	タイムアウトになるまで MAC アドレス テーブルで MAC アドレス エントリを維持する時間は、5 ～ 720 分（12 時間）です。デフォルトは 5 分です。

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

次の表は、このコマンドを入力でき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
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

使用上のガイドラインはありません。

例

次の例では、MAC アドレスのタイムアウトを 10 分に設定します。

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

関連コマンド

コマンド	説明
arp-inspection	ARP 検査をイネーブルにして、ARP パケットをスタティック ARP エントリと比較します。
firewall transparent	ファイアウォール モードを透過に設定します。
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。
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 エントリとスタティック エントリを含め、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。通常、MAC アドレスは、特定の MAC アドレスからトラフィックがインターフェイスに届いたときに、MAC アドレス テーブルに動的に追加されます。MAC アドレス テーブルには、必要に応じてスタティック MAC アドレスを追加できます。スタティック エントリを追加する 1 つの利点は、MAC スプーフィングから保護できることです。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、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すると、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*

シンタックスの説明

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

次の表は、このコマンドを入力でき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
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

次の例では、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。

```
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 モードを透過に設定します。
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。
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 ラーニングを再度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、受信するトラフィックの MAC アドレスを各インターフェイスが自動的にラーニングし、セキュリティ アプライアンスが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***

シンタックスの説明

interface_name	MAC ラーニングをディセーブルにするインターフェイス。
disable	MAC ラーニング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

次の表は、このコマンドを入力でき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
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

次の例では、外部インターフェイスの MAC ラーニングをディセーブルにします。

```
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 モードを透過に設定します。
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。
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、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

MAC アドレスの認証や認可を免除するために使用する 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 リスト 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*

シンタックスの説明

deny	この MAC アドレスに一致するトラフィックが MAC リストに一致しないこと、**aaa mac-exempt** コマンドに指定された際に認証と認可の両方の対象となることを示します。ffff.ffff.0000 といった MAC アドレス マスクを使用する MAC アドレスの範囲を許可し、その範囲の MAC アドレスを認証と認可の対象とする場合は、deny（拒否）エントリを MAC リストに追加しなければならないことがあります。
id	16 進数の MAC アクセス リストの番号を指定します。MAC アドレスのセットをグループ化するには、同じ ID の値を使用して必要な数だけ **mac-list** コマンドを入力します。パケットは最も一致するシナリオではなく、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です。permit（許可）エントリにおいては、permit エントリにより許可されたアドレスを拒否する場合、必ず permit エントリの前に deny エントリを入力します。
mac	12 桁の 16 進数形式（nnnn.nnnn.nnnn）で送信元 MAC アドレスを指定します。
macmask	マッチングに使用する MAC アドレスの一部を指定します。たとえば、ffff.ffff.ffff は MAC アドレスに完全に一致します。ffff.ffff.0000 は最初の 8 桁のみに一致します。
permit	この MAC アドレスに一致するトラフィックが MAC リストに一致することと、**aaa mac-exempt** コマンドに指定されたときに認証と認可の両方の対象から免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

次の表は、このコマンドを入力でき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
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のものです。

使用上のガイドライン

MAC アドレスを認証と認可の対象から免除するには、**aaa mac-exempt** コマンドを使用します。追加できる **aaa mac-exempt** コマンドのインスタンスは 1 つだけです。そのため、MAC リストに免除する MAC アドレスがすべて確実に含まれるようにしてください。複数の MAC リストを作成できますが、使用できるのは一度に 1 つだけです。

例

次の例では、1 つの MAC アドレスについて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、認証をバイパスしています。

```
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 を除く MAC アドレスのグループについて認証をバイパスします。permit 文の前に deny 文を入力してください。00a0.c95d.02b2 は permit 文にも一致するため、permit 文が最初に来ると、deny 文には一致しないためです。

```
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** コマンドで以前に指定されている MAC アドレスのリストを削除します。
show running-config mac-list	**mac-list** コマンドで指定されている 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**}

シンタックスの説明

domain_name	ドメイン名を指定します。
drop-connection	接続を終了します。
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

次の表は、このコマンドを入力でき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
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

次の例は、特定のドメインにメール リレーを設定する方法を示しています。

```
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 マップに含めるクラス 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検査クラス 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	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

management-access

IPSec VPN の使用時にセキュリティ アプライアンスを実行するために使用した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。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*

シンタックスの説明

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際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

次の表は、このコマンドを入力でき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
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のものです。

使用上のガイドライン

このコマンドを使用すると、IPSec VPN の使用時にセキュリティ アプライアンスに入った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った場合、このコマンドにより Telnet を使用して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ったときに、内部インターフェイスに対して ping を実行することができます。

定義できる管理アクセス用のインターフェイスは 1 つだけです。

例

次の例は、「inside」という名前のファイアウォール 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設定する方法を示しています。

```
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	管理アクセス用に設定されている内部インターフェイスの名前を表示します。

management-only

管理トラフィックだけを受け入れ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。トラフィックの通過を許可するには、このコマンドの **no** 形式を使用します。

management-only

no management-only

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

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

コマンド モード

次の表は、このコマンドを入力でき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
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 と呼ばれる管理専用インターフェイスが含まれており、このインターフェイスによってセキュリティ アプライアンスへのトラフィックをサポートします。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 の管理専用モードをディセーブルにして、他のインターフェイスと同様にトラフィックを通過させることもできます。

透過ファイアウォール 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 アプライアンスでは、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）を管理トラフィック用の第 3 のインターフェイスとして使用できます。モードはこの場合設定不能であり、常に管理専用にする必要があります。このインターフェイスを管理 IP アドレスから異なるサブネット上に移行させる場合、透過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。個々のインターフェイスではなく、セキュリティ アプライアンスまたはコンテキストに対して割り当てます。

例

次の例では、管理インターフェイスの管理専用モードをディセーブルにします。

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

次の例では、サブインターフェイスの管理専用モードをイネーブルにします。

```
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 モードに入ります。

map-name

ユーザ定義のアトリビュート名を Cisco アトリビュート名にマッピングするには、LDAP アトリビュート 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*

シンタックスの説明

user-attribute-name	Cisco アトリビュートにマッピングする、ユーザ定義のアトリビュート名を指定します。
Cisco-attribute-name	ユーザ定義の名前にマッピングする、Cisco アトリビュート名を指定します。

デフォルト

デフォルトでは、名前のマッピングは存在しません。

コマンド モード

次の表は、このコマンドを入力でき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
LDAP アトリビュート 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
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 コマンドを使用して、独自のアトリビュート名を作成し、それを Cisco アトリビュート名にマッピングできます。作成されたアトリビュート マップは、LDAP サーバにバインドすることができます。通常の手順は、次のとおりです。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用して、何も入力されていないアトリビュート マップを作成します。このコマンドにより、LDAP アトリビュート マップ コンフィギュレーション モードに入ります。
2. LDAP アトリビュート マップ コンフィギュレーション モードで **map-name** コマンドおよび **map-value** コマンドを使用して、アトリビュート 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** コマンドを使用して、LDAP サーバにアトリビュート マップをバインドします。このコマンドでは、「ldap」の後にハイフンを入力してください。

（注）　アトリビュート マッピング機能を正しく使用するには、Cisco LDAP アトリビュートの名前と値、およびユーザ定義アトリビュートの名前と値を理解しておく必要があります。

例

次のコマンド例では、LDAP アトリビュート マップ「myldapmap」内で、ユーザ定義のアトリビュート名「Hours」を、Cisco アトリビュート名「cVPN3000-Access-Hours」にマッピングします。

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

LDAP アトリビュート マップ コンフィギュレーション モードでは、次の例に示すように、「?」を入力して Cisco LDAP アトリビュート名の完全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）	ユーザ定義のアトリビュート名を Cisco LDAP アトリビュート名にマッピングするために、LDAP アトリビュート マップを作成し、名前を付けます。
ldap-attribute-map（AAA サーバ ホスト モード）	LDAP アトリビュート マップを LDAP サーバにバインドします。
map-value	ユーザ定義のアトリビュート値を、Cisco　アトリビュートにマッピングします。
show running-config ldap attribute-map	特定の実行 LDAP アトリビュート マップまたはすべての実行アトリビュート マップを表示します。
clear configure ldap attribute-map	すべての LDAP アトリビュート マップを削除します。

map-value

Cisco LDAP アトリビュートにユーザ定義の値をマッピングするには、LDAP アトリビュート 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*

シンタックスの説明

cisco-value-string	Cisco アトリビュートに対して Cisco 値の文字列を指定します。
user-attribute-name	Cisco アトリビュート名にマッピングする、ユーザ定義のアトリビュート名を指定します。
user-value-string	Cisco アトリビュート値にマッピングする、ユーザ定義の値文字列を指定します。

デフォルト

デフォルトでは、Cisco アトリビュートにマッピングされているユーザ定義の値はありません。

コマンド モード

次の表は、このコマンドを入力でき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
LDAP アトリビュート 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
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 コマンドを使用して、Cisco アトリビュート名と値に対して独自のアトリビュート値をマッピングできます。作成されたアトリビュート マップは、LDAP サーバにバインドすることができます。通常の手順は、次のとおりです。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用して、何も入力されていないアトリビュート マップを作成します。このコマンドにより、LDAP アトリビュート マップ コンフィギュレーション モードに入ります。
2. LDAP アトリビュート マップ コンフィギュレーション モードで **map-name** コマンドおよび **map-value** コマンドを使用して、アトリビュート 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** コマンドを使用して、LDAP サーバにアトリビュート マップをバインドします。このコマンドでは、「ldap」の後にハイフンを入力してください。

（注） アトリビュート マッピング機能を正しく使用するには、Cisco LDAP アトリビュートの名前と値、およびユーザ定義アトリビュートの名前と値を理解しておく必要があります。

例

次の例は、LDAP アトリビュート マップ コンフィギュレーション モードで入力され、ユーザ アトリビュート「Hours」のユーザ定義値を、workDay というユーザ定義の時間ポリシーと Daytime というシスコ定義の時間ポリシーに設定します。

```
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）	ユーザ定義のアトリビュート名を Cisco LDAP アトリビュート名にマッピングするために、LDAP アトリビュート マップを作成し、名前を付けます。
ldap-attribute-map（AAA サーバ ホスト モード）	LDAP アトリビュート 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 アトリビュート名を、Cisco LDAP アトリビュート名にマッピングします。
show running-config ldap attribute-map	特定の実行 LDAP アトリビュート マップまたはすべての実行アトリビュート 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** コマンドまたはクラス マップに一致するパケットの一部をマスクします。このマスク アクションはアプリケーション トラフィック用の検査ポリシー 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がこのアクションを許可しているわけでありません。たとえば、セキュリティ アプライアンス経由のトラフィックを許可するには、DNS アプリケーション検査で **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**]

シンタックスの説明

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

次の表は、このコマンドを入力でき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
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

検査ポリシー 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。検査ポリシー マップで使用できるコマンド自体は、アプリケーションによって異なります。アプリケーション トラフィックを識別する **match** コマンドまたは **class** コマンド（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect** コマンドを指す）を入力してから、**mask** コマンドを使用して **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します。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション検査をイネーブルにするときは、このアクションを含んでいる検査ポリシー マップをイネーブルにします。たとえば、**inspect dns dns_policy_map** コマンドを入力します。dns_policy_map は検査ポリシー マップの名前です。

例

次の例では、セキュリティ アプライアンス経由でトラフィックを許可する前に、DNS ヘッダーの RD フラグと RA フラグをマスクします。

```
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 マップに含めるクラス 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検査クラス 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	アプリケーション検査のための特別なアクションを定義します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

mask-banner

サーバのバナーを目立たないようにするには、パラメータ コンフィギュレーション モードで **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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力でき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
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

次の例は、サーバのバナーを隠す方法を示しています。

```
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 マップに含めるクラス 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検査クラス 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	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

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 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。このモードには、**ftp-map** コマンドを使用してアクセスできます。コンフィギュレー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。

mask-syst-reply

no mask-syst-reply

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力でき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
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

mask-syst-reply コマンドは、クライアントから FTP サーバ システムを保護するため、厳密な FTP 検査と併せて使用します。このコマンドをイネーブルにすると、**syst** コマンドへのサーバ応答は X の連続に置き換えられます。

例

次の例では、セキュリティ アプライアンスが syst コマンドへの FTP サーバ応答を X の連続に置き換えます。

```
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# mask-syst-reply
hostname(config-ftp-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先のトラフィック 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	アプリケーション検査用に特定の FTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
request-command deny	禁止する 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場合は、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、アクションを適用するトラフィックをアクセス リストで識別します。**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*

シンタックスの説明

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

次の表は、このコマンドを入力でき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
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 コマンドを入力してから、**match access-list** コマンドを入力してトラフィックを識別します。また、**match port** コマンドなどの別のタイプの **match** コマンドを入力することもできます。クラス マップには **match access-list** コマンドを 1 つだけ含めることができます。それを別の種類の **match** コマンドと組み合せることはできません。例外としては、セキュリティ アプライアンスで検査可能なすべてのアプリケーションが使用するデフォルトの TCP ポートと UDP ポートに一致する **match default-inspection-traffic** コマンドを定義する場合、**match access-list** コマンドを使用してトラフィックを絞り込んで一致させることができます。**match default-inspection-traffic** コマンドは一致するポートを指定するため、アクセス リストに含まれるポートは無視されます。

2. （アプリケーション検査のみ）**policy-map type inspect** コマンドを使用して、アプリケーション検査トラフィックのため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、インターフェイスに対するアクションを有効にします。

例

次の例では、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	すべてのトラフィックをクラス マップに含めます。
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場合、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に一致させます。**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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力でき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
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 コマンドの入力後には、**match any** コマンドを入力してすべてのトラフィックを識別します。また、**match port** コマンドなどの別のタイプの **match** コマンドを入力することもできます。**match any** コマンドを別のタイプの **match** コマンドと組み合せることはできません。
2. （アプリケーション検査のみ）**policy-map type inspect** コマンドを使用して、アプリケーション検査トラフィックのため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、インターフェイスに対するアクションを有効にします。

例

次の例は、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 クラスを定義する方法を示しています。

```
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 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 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*]

シンタックスの説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現クラス 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

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 マップ内で設定できます。GTP 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

次の例では、GTP 検査クラス マップのアクセス ポイント名に関する一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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 body

ESMTP メッセージ本文の長さ、または行の長さに関する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 body** コマンドを使用します。設定済みの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*

シンタックスの説明

length	ESMTP メッセージ本文の長さを指定します。
line length	ESMTP メッセージ本文の行の長さを指定します。
bytes	バイト単位で一致する数字を指定します。

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

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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

次の例では、ESMTP 検査ポリシー マップで、特定の本文の行の長さに関して一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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 着信側に関する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*]

シンタックスの説明

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

次の表は、このコマンドを入力でき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
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

次の例では、H.323 検査クラス マップで着信側に関する一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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 発信側に関する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*]

シンタックスの説明

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

次の表は、このコマンドを入力でき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
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

次の例では、H.323 検査クラス マップで発信側に関する一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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 証明書の検証プロセス時に、セキュリティ アプライアンスは証明書の失効ステータスをチェックし、セキュリティを維持します。このタスクを完了するために、CRL チェックまたは Online Certificate Status Protocol（OSCP; オンライン証明書ステータス プロトコル）が使用されます。CRL チェックの場合、セキュリティ アプライアンスは証明書の失効リストを取得し、解析してキャッシュします。このリストは失効した証明書の完全なリストを提供します。OCSP では、失効ステータスをよりスケーラブルな方法でチェックします。具体的には、証明書のステータスは、特定の証明書のステータスについて照会を行う検証機関によりローカライズされます。

証明書の一致規則を使用して、OCSP URL の上書きを設定できます。この上書きでは、リモートユーザ証明書の AIA フィールドの URL ではなく、失効ステータスをチェックする URL を指定します。一致規則により OCSP レスポンダ証明書の検証に使用するトラストポイントも設定されます。このトラストポイントにより、セキュリティ アプライアンスは自己署名証明書と、クライアント証明書の検証パスへの外部証明書を含む CA からのレスポンダ証明書を検証します。

証明書の一致規則を設定するには、暗号 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。この規則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。

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

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

シンタックスの説明

map-name	この規則に一致する証明書マップの名前を指定します。証明書マップを設定してから、一致規則を設定する必要があります。最大 65 文字です。
match certificate	この一致規則に証明書マップを指定します。
override ocsp	この規則は証明書の OCSP URL の上書きを目的とすることを指定します。
seq-num	この一致規則に優先順位を設定します。範囲は 1 ～ 10000 です。セキュリティ アプライアンスは、最初に一番小さいシーケンス番号を持つ一致規則を評価し、一致が見つかるまでより大きい番号を持つ一致規則を評価します。
trustpoint	（オプション）OCSP レスポンダ証明書の検証にトラストポイントを使用することを指定します。
trustpoint- name	（オプション）レスポンダ証明書を検証する上書きに使用するトラストポイントを指定します。
url	OCSP 失効ステータスの確認のために URL にアクセスすることを指定します。
URL	OCSP 失効ステータスを確認するためにアクセスする URL 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

次の表は、このコマンドを入力でき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
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 を設定する際には、次のヒントに留意してください。

- 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規則を設定できますが、暗号 CA 証明書マップごとに設定できる一致規則は 1 つだけです。ただし、複数の暗号 CA 証明書マップを設定し、それらを同一のトラストポイントに関連付けることができます。
- 証明書マップを設定してから一致規則を設定する必要があります。
- 自己署名の OCSP レスポンダ証明書を検証するトラストポイントを設定するには、自己署名のレスポンダ証明書をそれ自体のトラストポイントに、信頼できる CA 証明書としてインポートします。次に、レスポンダ証明書の検証に、自己署名の OCSP レスポンダ証明書を含むトラストポイントを使用できるよう、トラストポイントを検証するクライアント証明書に **match certificate** コマンドを設定します。クライアント証明書の検証パスに含まれないレスポンダ証明書を検証する場合にも、同じように設定します。
- 同一の CA がクライアント証明書とレスポンダ証明書を発行する場合、トラストポイントは両方の証明書を検証できます。ただし、異なる CA がクライアント証明書とレスポンダ証明書を発行する場合は、各証明書に 1 つずつ、計 2 つのトラストポイントを設定する必要があります。
- OCSP サーバ（レスポンダ）証明書は通常、OCSP 応答に署名します。応答の受信後、セキュリティ アプライアンスはレスポンダ証明書を検証しようとします。CA は通常、OCSP レスポンダ証明書の期限を比較的短期間に設定して、その信用が失われる危険を最小限にします。また、CA のレスポンダ証明書には、証明書の失効ステータス確認が不要であることを示す ocsp-no-check 拡張も一般に含まれます。ただし、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したのと同じ方法で失効ステータスを確認します。レスポンダ証明書が検証できない場合は、失効チェックに失敗します。失効チェックが失敗しないようにするには、トラストポイントを検証するレスポンダ証明書に **revocation-check none** を設定すると同時に、クライアント証明書に **revocation-check ocsp** を設定します。
- セキュリティ アプライアンスは、一致しない場合に、**ocsp url** コマンドの URL を使用します。**ocsp url** コマンドを設定していない場合は、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 拡張が含まれていない場合、失効ステータスのチェックは失敗します。

例

次の例では、newtrust というトラストポイントに証明書一致規則を作成する方法を示します。規則には mymap というマップ名、シーケンス番号 4、mytrust というトラストポイントが含まれ、URL 10.22.184.22 を指定します。

```
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)#
```

次の例では、暗号 CA 証明書マップを設定後、一致証明書規則を設定して、CA 証明書が含まれるトラストポイントを指定し、レスポンダ証明書を検証する方法を段階的に示します。newtrust トラストポイントに指定された CA が OCSP レスポンダ証明書を発行しない場合に、この方法が必要になります。

ステップ 1　マップ規則が適用される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。次の例では、証明書マップの名前は mymap、シーケンス番号は 1 です。mycert と一致する CN アトリビュートが含まれるサブジェクト名を持つクライアント証明書は mymap エントリと一致します。

```
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 レスポンダ証明書を検証するための CA 証明書が含まれ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、インポート後にローカルに信頼されます。この目的で、外部の CA 登録を介して証明書を入手することもできます。プロンプトが表示されたら、CA 証明書に貼り付けます。

```
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　失効チェック方法として OCSP を使用して元のトラストポイント newtrust を設定します。次に、証明書マップ mymap、およびステップ 2 で設定した自己署名トラストポイント mytrust を含む一致規則を設定します。

```
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の認証に newtrust トラストポイントを使用する接続では、クライアント証明書が mymap 証明書マップで指定したアトリビュート規則と一致するかどうかがチェックされます。その場合、セキュリティ アプライアンスは OCSP レスポンダ（10.22.184.22）にアクセスして、証明書の失効ステータスをチェックします。次に、mytrust トラストポイントを使用して、レスポンダ証明書が検証されます。

（注）　newtrust トラストポイントを設定して、OCSP を介してクライアント証明書の有効性をチェックします。ただし、mytrust トラストポイントは失効チェックなし（デフォルト）に設定されているので、OCSP レスポンダ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	暗号 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 モードに入ります。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の OCSP サーバを指定します。
revocation-check	失効のチェックに使用する方法（複数可）、およびその試行順序を指定します。

match cmd

ESMTP コマンド バーブに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*]

シンタックスの説明

verb *verb*	ESMTP コマンド バーブを指定します。
line length gt *bytes*	行の長さを指定します。
RCPT count gt *recipients_number*	受信者の数を指定します。

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

次の表は、このコマンドを入力でき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
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

次の例では、ESMTP 検査ポリシー マップに、ESMTP トランザクションで交換されるバーブ（メソッド）NOOP についての一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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 マップ内の inspect コマンドに対する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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

各検査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

次の表は、このコマンドを入力でき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
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

各種の **match** コマンドを使用して、クラス マップのトラフィック クラスに含まれるトラフィックを指定します。これらのコマンドは、クラス マップに含まれるトラフィックを定義するためのさまざまな基準を保持しています。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** 文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 クラスに包含され、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。どのトラフィック クラスのど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 トラフィックを一致させることができます。**match default-inspection-traffic** コマンドはその他の match コマンドの 1 つと併せて使用できます。このコマンドは、通常、***permit ip*** *src-ip dst-ip* 形式のアクセス リストです。

2 番目の **match** コマンドを **match default-inspection-traffic** コマンドと組み合せる際、**match default-inspection-traffic** コマンドを使用してプロトコルとポート情報を指定し、2 番目の **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）を指定するという規則があります。2 番目の **match** コマンドで指定したプロトコルまたはポート情報は、**inspect** コマンドでは無視されます。

たとえば、次の例で指定するポート 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
```

検査用のデフォルトのトラフィックは次のとおりです。

検査タイプ	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

次の例は、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 クラスを定義する方法を示しています。

```
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	すべてのトラフィックをクラス マップに含めます。
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（DNS リソース レコードまたはクエスチョン）セクションの Domain System Class（ドメイン システム クラス）に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 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*}

シンタックスの説明

eq	完全一致を指定します。
c_well_known	既知の名前である IN により DNS クラスを指定します。
c_val	DNS クラス フィールドに任意の値（0 ～ 65535）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、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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（クエスチョンと RR）を検査し、指定したクラスと照合します。DNS クエリーと DNS 応答の両方が確認されます。

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 マップでは、入力できるエントリは 1 つのみです。

例

次の例では、DNS 検査ポリシー マップで、DNS クラスについての一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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 タイプと RR タイプを含む、DNS タイプ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 dns-type** コマンドを使用します。設定した 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*}

シンタックスの説明

eq	完全一致を指定します。
t_well_known	A、NS、CNAME、SOA、TSIG、IXFR、または AXFR といった既知の名前を使用して DNS タイプを指定します。
t_val	DNS タイプ フィールドに任意の値（0 ～ 65535）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、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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（クエスチョンと RR）のすべてのセクションを検査し、指定したタイプと照合します。DNS クエリーと DNS 応答の両方が確認されます。

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 マップでは、入力できるエントリは 1 つのみです。

例

次の例では、DNS 検査ポリシー マップで、DNS タイプの一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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。設定済みの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*

シンタックスの説明

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を含むクラス 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、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 メッセージのドメイン名と定義済みリストを照合します。圧縮されているドメイン名は拡張後、照合されます。他の DNS **match** コンドと組み合せて一致条件を特定のフィールドに絞り込みます。

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 マップでは、入力できるエントリは 1 つのみです。

例

次の例では、DNS 検査ポリシー マップの DNS ドメイン名を照合する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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 マップ内の IETF 定義の DSCP 値（IP ヘッダー内）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 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***}

シンタックスの説明

values	IP ヘッダー内の最大 8 つの異なる IETF 定義の DSCP 値を指定します。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

次の表は、このコマンドを入力でき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
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

各種の **match** コマンドを使用して、クラス マップのトラフィック クラスに含まれるトラフィックを指定します。これらのコマンドは、クラス マップに含まれるトラフィックを定義するためのさまざまな基準を保持しています。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** 文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 クラスに包含され、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。どのトラフィック クラスのど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 ヘッダー内の IETF 定義の DSCP 値を一致させることができます。

例

次の例は、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 クラスを定義する方法を示しています。

```
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	該当するインターフェイスで受信されるパケットの比較基準として、TCP/UDP ポートを指定します。
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 ehlo-reply-parameter

ESMTP ehlo 応答パラメータに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*

シンタックスの説明

parameter	ehlo 応答パラメータを指定します。値には、8bitmime、auth、binarymime、checkpoint、dsn、etrn、others、pipelining、size、および vrfy が含まれます。

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

次の表は、このコマンドを入力でき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
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

次の例では、ESMTP 検査ポリシー マップで、ehlo 応答パラメータに関する一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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*]

シンタックスの説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現クラス 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

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 マップでは、入力できるエントリは 1 つのみです。

例

次の例では、FTP 検査クラス マップで、FTP 転送ファイル名に関する一致条件を設定する方法を示します。

```
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。
match any	すべてのトラフィックをクラス マップに含めます。
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*]

シンタックスの説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現クラス 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

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 マップでは、入力できるエントリは 1 つのみです。

例

次の例は FTP 検査ポリシー マップで FTP 転送ファイル タイプに関する一致条件を設定する方法を示します。

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

match flow ip destination-address

クラス マップ内のフロー IP の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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力でき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
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

各種の **match** コマンドを使用して、クラス マップのトラフィック クラスに含まれるトラフィックを指定します。これらのコマンドは、クラス マップに含まれるトラフィックを定義するためのさまざまな基準を保持しています。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** 文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 クラスに包含され、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。どのトラフィック クラスのどの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

トンネル グループでフローベースのポリシー アクションをイネーブルにするには、**match flow ip destination-address** と **match tunnel-group** コマンドを **class-map**、**policy-map**、および **service-policy** コマンドと併せて使用します。フローを定義する基準は、宛先 IP アドレスです。一意の 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 クラス全体ではなく各フローに適用されます。**match flow ip destination-address** コマンドを使用すると、QoS アクション ポリシングが適用されます。トンネル グループ内の各トンネルを、指定したレートにポリシングするには、**match tunnel-group** を使用します。

例

次の例は、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、各トンネルを指定したレートに制限する方法を示しています。

```
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のデータベースを作成および管理します。

match header

ESMTP ヘッダーに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 gt** *bytes* | **to-fields count gt** *to_fields_number*]

no match [**not**] **header [length gt** *bytes* | **to-fields count gt** *to_fields_number*]

シンタックスの説明

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。
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

次の表は、このコマンドを入力でき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
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

次の例では、ESMTP 検査ポリシー マップで、ヘッダーに関して一致条件を設定する方法を示します。

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

match header-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。設定したヘッダー 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*}

シンタックスの説明

eq	完全一致を指定します。設定されていない場合、**match-all** ビット マスク一致を指定します。
f_well_known	既知の名前を使用して DNS ヘッダー フラグ ビットを指定します。複数のフラグ ビットを入力でき、その場合は論理的に OR 関係になります。 QR（Query; クエリー）（注：QR=1 は、DNS 応答を示します） AA（Authoritative Answer; 権威ある回答） TC（TrunCation; 短縮） RD（Recursion Desired; 再帰要求） RA（Recursion Available; 再帰可能）
f_value	16 進数形式で任意の 16 ビット値を指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 マップまたはポリシー マップ内で設定できます。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

次の例では、DNS 検査ポリシー マップで、DNS ヘッダー フラグに関する一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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 サブスクライ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 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*]

シンタックスの説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現クラス 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

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 マップでは、入力できるエントリは 1 つのみです。

例

次の例では、SIP 検査クラス マップで、SIP IM サブスクライバに関して一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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 invalid-recipients

ESMTP の無効な受信者アドレスに関する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*

シンタックスの説明

count gt *number*	無効な受信者番号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

次の表は、このコマンドを入力でき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
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

次の例では、ESMTP 検査ポリシー マップで、無効な受信者数に関して一致条件を設定する方法を示します。

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

match ip address

指定したいずれかのアクセス リストによって渡されたルート アドレスまたは一致パケットを持つ、すべて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 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...*}

シンタックスの説明

acl	アクセス リストの名前。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

次の表は、このコマンドを入力でき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
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のものです。

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、つまり現在の **route-map** コマンドについて再配布を許可する条件を指定します。**set** コマンドには、設定アクション、つまり **match** コマンドで指定した基準を満たしている場合に実行する、個々の再配布アクションを指定します。**no route-map** コマンドを実行すると、ルートマップが削除されます。

例

次の例は、内部ルートを再配布する方法を示しています。

```
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。
match ip next-hop	指定したいずれかのアクセス リスト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ための条件を定義します。
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

指定したいずれかのアクセス リスト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***

シンタックスの説明

acl	ACL の名前。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。

デフォルト

ネクストホップ アドレスに一致する必要なく、ルートが自由に配布されます。

コマンド モード

次の表は、このコマンドを入力でき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
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のものです。

使用上のガイドライン

コマンド シンタックスの省略形（...）は、コマンド入力で *acl* 引数に複数の値を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、つまり現在の **route-map** コマンドについて再配布を許可する条件を指定します。**set** コマンドには、設定アクション、つまり **match** コマンドで指定した基準を満たしている場合に実行する、個々の再配布アクションを指定します。**no route-map** コマンドを実行すると、ルートマップが削除されます。

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の再配布を実行するには、すべての **match** コマンドに一致する必要があります。**match** コマンドを **no** 形式で実行すると、指定した一致基準が削除されます。

ルートマップを通じてルートを渡す場合、ルートマップはいくつかの部分に分かれることがあります。**route-map** コマンドに関連付けられているどの match 節にも一致しないルートは、すべて無視されます。一部のデータのみを修正するには、2 番目のルートマップ 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

次の例は、acl_dmz1 または acl_dmz2 のアクセス リストによって渡されたネクストホップ ルータ アドレスを持つルートを配布する方法を示しています。

```
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	指定したいずれかのアクセス リスト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ための条件を定義します。
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

ルータによってアドバタイジングされ、ACL で指定されたアドレスのサーバにアクセスす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 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...*}

シンタックスの説明

acl	ACL の名前。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。

デフォルト

ルートの送信元では、フィルタリングは実行されません。

コマンド モード

次の表は、このコマンドを入力でき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
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のものです。

使用上のガイドライン

コマンド シンタックスの省略形（...）は、コマンド入力で access-list-name 引数に複数の値を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、つまり現在の **route-map** コマンドについて再配布を許可する条件を指定します。**set** コマンドには、設定アクション、つまり **match** コマンドで指定した基準を満たしている場合に実行する、個々の再配布アクションを指定します。**no route-map** コマンドを実行すると、ルートマップが削除されます。

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の再配布を実行するには、すべての **match** コマンドに一致する必要があります。**match** コマンドを **no** 形式で実行すると、指定した一致基準が削除されます。

ルートマップは、いくつかの部分に分かれることがあります。**route-map** コマンドに関連付けられているどの match 節にも一致しないルートは、すべて無視されます。一部のデータのみを修正するには、2 番目のルートマップ 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および送信元ルータのアドレスは、状況によって異なります。

例

次の例は、ルータによってアドバタイジングされ、acl_dmz1 および acl_dmz2 の ACL で指定されたアドレスのサーバにアクセスするルートを配布する方法を示しています。

```
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ための条件を定義します。
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 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**]

シンタックスの説明

audio	オーディオ メディア タイプと照合することを指定します。
data	データ メディア タイプと照合することを指定します。
video	ビデオ メディア タイプと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

次の表は、このコマンドを入力でき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
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

次の例では、H.323 検査クラス マップで、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方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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*]

シンタックスの説明

message_id	1 ～ 255 の範囲の英数字 ID を指定します。
range *lower_range upper_range*	ID の下位と上位を指定します。

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

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 マップ内で設定できます。GTP 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

次の例では、GTP 検査クラス マップで、メッセージ ID に関して一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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 length

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 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*

シンタックスの説明

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 の最大長を指定します。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

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 マップ内で設定できます。GTP 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

次の例では、GTP 検査クラス マップで、メッセージの長さに関して一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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-path

Via ヘッダー フィールドでの指定のとおりに、SIP メッセージによって取得されるパ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 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*]

シンタックスの説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現クラス 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

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 マップでは、入力できるエントリは 1 つのみです。

例

次の例は、SIP 検査クラス マップの SIP メッセージによって取得されるパスに関して、一致条件を設定する方法を示しています。

```
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	すべてのトラフィックをクラス マップに含めます。
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 mime

ESMTP mime エンコード タイプ、mime ファイル名の長さ、または mime ファイル タイプについ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***]**

シンタックスの説明

encoding *type*	エンコード 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

次の表は、このコマンドを入力でき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
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

次の例では、ESMTP 検査ポリシー マップで、mime ファイル名の長さに関して一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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 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*}

シンタックスの説明

eq port	ポート名または番号を 1 つ指定します。
range beg_port end_port	ポート範囲の開始値と終了値（1 ～ 65535）を指定します。
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

次の表は、このコマンドを入力でき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
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 コマンドの入力後に、**matchport** コマンドを入力してトラフィックを指定します。あるいは、**match access-list** コマンドなど、異なるタイプの **match** コマンドを入力します（**class-map type management** コマンドのみが 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ます。それを別のタイプの **match** コマンドと組み合せることはできません。

2. （アプリケーション検査のみ）**policy-map type inspect** コマンドを使用して、アプリケーション検査トラフィックのため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、インターフェイスに対するアクションを有効にします。

例

次の例は、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 クラスを定義する方法を示しています。

```
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	すべてのトラフィックをクラス マップに含めます。
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 マップ内の優先順位値を指定するには、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*

シンタックスの説明

value	スペースで区切った最大 4 つの優先順位値を指定します。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

次の表は、このコマンドを入力でき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
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

各種の **match** コマンドを使用して、クラス マップのトラフィック クラスに含まれるトラフィックを指定します。これらのコマンドは、クラス マップに含まれるトラフィックを定義するためのさまざまな基準を保持しています。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** 文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 クラスに包含され、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。どのトラフィック クラスのど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 ヘッダー内の TOS バイトで表現された値を指定するには、**match precedence** コマンドを使用します。

例

次の例は、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 クラスを定義する方法を示しています。

```
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	すべてのトラフィックをクラス マップに含めます。
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 クエスチョンまたはリソース 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 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 question** コマンドを使用します。設定済みの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**}}

シンタックスの説明

question	DNS メッセージのクエスチョン部分を指定します。
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（回答）RR セクションを指定します。
authority	Authority（権威）RR セクションを指定します。
additional	Additional（追加）RR セクションを指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 ヘッダーを検査し、指定したフィールドと照合します。他の DNS **match** コマンドと組み合せて使用し、特定のクエスチョンまたは RR タイプの検査を定義します。

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 マップでは、入力できるエントリは 1 つのみです。

例

次の例では、DNS 検査ポリシー マップで、DNS クエスチョンに関して一致条件を設定する方法を示します。

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

match request-command

特定の FTP コマンドを制限するには、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 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...*]

シンタックスの説明

ftp_command	制限する 1 つまたは複数の FTP コマンドを指定します。

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

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 マップでは、入力できるエントリは 1 つのみです。

例

次の例では、FTP 検査ポリシー マップで、特定の FTP コマンドに関して一致条件を設定する方法を示します。

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

match request-method

SIP メソッド タイプに関して一致条件を設定するには、クラス マップ 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 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*

シンタックスの説明

method_type	RFC 3261 とサポートされる拡張機能に応じてメソッド タイプを指定します。サポートされるメソッド タイプは、ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update 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

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 マップでは、入力できるエントリは 1 つのみです。

例

次の例は、SIP 検査クラス マップの SIP メッセージによって取得されるパスに関して、一致条件を設定する方法を示しています。

```
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	すべてのトラフィックをクラス マップに含めます。
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 route-type

指定し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**]}}

シンタックスの説明

local	ローカルに生成された BGP ルート。
internal	OSPF のエリア内ルートおよびエリア間ルート、または EIGRP の内部ルート。
external	OSPF の外部ルートまたは EIGRP の外部ルート。
type-1	（オプション）ルート タイプ 1 を指定します。
type-2	（オプション）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、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力でき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
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のものです。

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、つまり現在の **route-map** コマンドについて再配布を許可する条件を指定します。**set** コマンドには、設定アクション、つまり **match** コマンドで指定した基準を満たしている場合に実行する、個々の再配布アクションを指定します。**no route-map** コマンドを実行すると、ルートマップが削除されます。

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の再配布を実行するには、すべての **match** コマンドに一致する必要があります。**match** コマンドを **no** 形式で実行すると、指定した一致基準が削除されます。

ルートマップは、いくつかの部分に分かれることがあります。**route-map** コマンドに関連付けられているどの match 節にも一致しないルートは、すべて無視されます。一部のデータのみを修正するには、2 番目のルートマップ 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 外部ルートにだけ一致し、**external type-2** キーワードはタイプ 2 外部ルートにだけ一致します。

例

次の例は、内部ルートを再配布する方法を示しています。

```
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	指定したいずれかのアクセス リスト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ための条件を定義します。
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 マップ内の偶数ポートの 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*

シンタックスの説明

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

次の表は、このコマンドを入力でき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
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

各種の **match** コマンドを使用して、クラス マップのトラフィック クラスに含まれるトラフィックを指定します。これらのコマンドは、クラス マップに含まれるトラフィックを定義するためのさまざまな基準を保持しています。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** 文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 クラスに包含され、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。どのトラフィック クラスのど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* ～ *starting_port* に *range* を加えた範囲の UDP の偶数ポート番号）に一致させるには、**match rtp** コマンドを使用します。

例

次の例は、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 クラスを定義する方法を示しています。

```
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	すべてのトラフィックをクラス マップに含めます。
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 アドレスについ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***]**

シンタックスの説明

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

次の表は、このコマンドを入力でき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
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

次の例では、ESMTP 検査ポリシー マップで、320 文字を超える長さの送信者電子メール アドレスに関して一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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*]

シンタックスの説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現クラス 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

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 マップでは、入力できるエントリは 1 つのみです。

例

次の例では、FTP 検査ポリシー マップで、FTP サーバに関して一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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 third-party-registration

サード パーティー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 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 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*]

シンタックスの説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現クラス 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

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 マップでは、入力できるエントリは 1 つのみです。

match third-party-registration コマンドは、SIP レジスタまたは SIP プロキシを使用して他のユーザを登録できるユーザを特定するために使用します。From 値と To 値が一致しない場合には、REGISTER メッセージの From ヘッダー フィールドにより特定されます。

例

次の例では、SIP 検査クラス マップで、サードパーティーの登録に関して一致条件を設定する方法を示します。

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

match tunnel-group

すでに定義されているトンネル グループに属するクラス マップ内のトラフィックに一致させるには、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*

シンタックスの説明

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

次の表は、このコマンドを入力でき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
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

各種の **match** コマンドを使用して、クラス マップのトラフィック クラスに含まれるトラフィックを指定します。これらのコマンドは、クラス マップに含まれるトラフィックを定義するためのさまざまな基準を保持しています。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** 文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 クラスに包含され、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。どのトラフィック クラスのど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** と **match tunnel-group** コマンドを **class-map**、**policy-map**、および **service-policy** コマンドと併せて使用します。フローを定義する基準は、宛先 IP アドレスです。一意の 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 クラス全体ではなく各フローに適用されます。**police** コマンドを使用すると、QoS アクション ポリシングが適用されます。トンネル グループ内の各トンネルを、指定したレートにポリシングするには、**match tunnel-group** を **match flow ip destination-address** と併せて使用します。

例

次の例は、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、各トンネルを指定したレートに制限する方法を示しています。

```
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 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 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*

シンタックスの説明

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

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 マップでは、入力できるエントリは 1 つのみです。

例

次の例では、SIP メッセージの URI に関して一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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 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*]

シンタックスの説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現クラス 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

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 マップでは、入力できるエントリは 1 つのみです。

例

次の例では、FTP 検査クラス マップで FTP ユーザ名に関して一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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 version

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 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*]

シンタックスの説明

vresion_id	0 ～ 255 の範囲のバージョンを指定します。
range *lower_range upper_range*	バージョンの上位と下位の範囲を指定します。

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

次の表は、このコマンドを入力でき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
クラス マップ コンフィギュレーションまたはポリシー 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 マップ内で設定できます。GTP 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

次の例では、GTP 検査クラス マップでメッセージ バージョンに関して一致条件を設定する方法を示します。

```
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	すべてのトラフィックをクラス マップに含めます。
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。

max-failed-attempts

サーバ グループ内のある特定のサーバに対して許容される失敗数（失敗数がこれを超えるとそのサーバが無効になる）を指定するには、AAA サーバ グループ 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

シンタックスの説明

number	1 ～ 5 の範囲の整数。前の **aaa-server** コマンドで指定したサーバ グループ内の所定のサーバで許可される失敗数を指定します。

デフォルト

number のデフォルト値は 3 です。

コマンド モード

次の表は、このコマンドを入力でき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
AAA サーバ グループ	•	•	•	•	—

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 モードに入って、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 パラメータを設定できるようにします。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa	すべての AAA サーバ、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 である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]

シンタックスの説明

drop	違反が発生した場合、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、独自または追加のログを記録することを指定します。このアクションは、任意のアクションに関連付けることができます。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力でき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
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までのホップ数をカウントします。宛先に到達する前に、ホップ数が 0 になることはありません。

例

次の例では、SIP 検査ポリシー マップで max-forwards-validation をイネーブルにする方法を示します。

```
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 マップに含めるクラス 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検査クラス 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	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

max-header-length

HTTP ヘッダー長に基づいて 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**]

シンタックスの説明

action	メッセージがこのコマンド検査に合格しなかったときに実行されるアクション。
allow	メッセージを許可します。
drop	接続を終了します。
bytes	バイト数（範囲は 1 ～ 65,535）。
log	（オプション）syslog を生成します。
request	要求メッセージ。
reset	TCP リセット メッセージをクライアントとサーバに送信します。
response	（オプション）応答メッセージ。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力でき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
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 ヘッダーを持つメッセージだけを許可します。それ以外の場合は、指定されたアクションを実施します。セキュリティ アプライアンスが TCP 接続をリセットして syslog エントリをオプションで作成するようにするには、**action** キーワードを使用します。

例

次の例では、HTTP 要求を 100 バイト以下の HTTP ヘッダーを持つものに限定します。ヘッダーが大きすぎる場合、セキュリティ アプライアンスが 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先のトラフィック クラスを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

max-object-size

セキュリティ アプライアンスが、WebVPN セッションに対して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*

シンタックスの説明

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でき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 サイズよりも大きくする必要があります。キャッシュ圧縮がイネーブルである場合、セキュリティ アプライアンスは、オブジェクト圧縮後のサイズを計算します。

例

次の例では、最大オブジェクト サイズである 4000 KB に設定する方法を示します。

```
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 モードに入ります。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシング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ング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-uri-length

HTTP 要求メッセージの URI 長に基づいて 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**]

シンタックスの説明

action	メッセージがこのコマンド検査に合格しなかったときに実行されるアクション。
allow	メッセージを許可します。
drop	接続を終了します。
bytes	バイト数（範囲は 1 ～ 65,535）。
log	（オプション）syslog を生成します。
reset	TCP リセット メッセージをクライアントとサーバに送信します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力でき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
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 を持つメッセージだけを許可します。それ以外の場合は、指定されたアクションを実施します。セキュリティ アプライアンスが TCP 接続をリセットして 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。

設定した値以下の長さを持つ URI が許可されます。それ以外の場合は、指定されたアクションが実施されます。

例

次の例では、HTTP 要求を 100 バイト以下の URI を持つものに限定します。URI が大きすぎる場合、セキュリティ アプライアンスが 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先のトラフィック クラスを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

mcc

IMSI プレフィックス フィルタリングのモバイル国番号とモバイル ネットワーク番号を指定するには、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。コンフィギュレー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。

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

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

シンタックスの説明

country_code	モバイル国番号を指定する 0（ゼロ）以外の 3 桁の値。1 桁または 2 桁のエントリは先頭に 0 が追加され、3 桁の値に生成されます。
network_code	ネットワーク番号を指定する 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 の組み合せをチェックしません。

コマンド モード

次の表は、このコマンドを入力でき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
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 フィルタリング用に使用します。受信されたパケットの IMSI 内の MCC と MNC が、このコマンドで設定した MCC/MNC と比較され、一致しない場合にドロップされます。

IMSI プレフィックス フィルタリングをイネーブルにするには、このコマンドを使用する必要があります。許可された MCC と MNC の組み合せを指定するのに、複数のインスタンスを設定できます。デフォルトでは、セキュリティ アプライアンスが MNC と MCC の組み合せの有効性をチェッ

クしないので、設定された組み合せの有効性を確認する必要があります。MCC と MNC 番号の詳細については、ITU E.212 の推奨事項である『*Identification Plan for Land Mobile Stations*』を参照してください。

例

次の例では、111 の MCC と 222 の MNC で IMSI プレフィックス フィルタリングのトラフィックを指定します。

```
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 GTP 統計情報を消去します。
debug gtp	GTP 検査に関する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	アプリケーション検査に使用する特定の 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-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。ファイバ SFP コネクタは、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 で使用できます。メディア タイプの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***]

シンタックスの説明

rj45	（デフォルト）メディア タイプを RJ-45 銅線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

次の表は、このコマンドを入力でき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
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)(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（1,000 Mbps）を使用するので、**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*** ではサポートされていません。

例

次の例では、メディア タイプを SFP に設定します。

```
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 モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
show running-config interface	インターフェイスの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*

シンタックスの説明

class_name	**class** コマンドを使用して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 クラスに割り当てられます。

コマンド モード

次の表は、このコマンドを入力でき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
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 つまたは複数のコンテキストがリソースを大量に消費しているために、他のコンテキストで接続が拒否されていることが分かった場合などは、リソース管理を設定することによって、リソースの使用をコンテキストごとに制限できます。セキュリティ アプライアンスでは、コンテキストをリソース クラスに割り当てることでリソースを管理します。各コンテキストは、クラスによって設定されるリソース制限値を使用します。

例

次の例では、test というコンテキストを gold というクラスに割り当てます。

```
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	リソースに対して制限を設定します。
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。

memory caller-address

メモリ問題を分離できるように、コール トレース用のプログラム メモリの特定の範囲を設定するには、特権 EXEC モードで ***memory caller-address*** コマンドを使用します。発信者 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。アドレスの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

シンタックスの説明

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

実際の発信者 PC が、メモリ トレース用に記録されます。

コマンド モード

次の表は、このコマンドを入力でき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
特権 EXEC	•	•	—	•	•

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

メモリ問題を特定のメモリ ブロックに分離するには、***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者 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機能になります。プログラムの個々の場所を分離するには、ライブラリ機能の開始および終了プログラム アドレスを設定して、ライブラリ機能のプログラムの発信者アドレスが記録されるようにします。

（注） 発信者アドレスのトレース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

次の例は、***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を示しています。

```
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に関する情報（プロファイリング）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の範囲を表示します。

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解放された後のメモリの変化を監視することができます。

memory delayed-free-poisoner enable

no memory delayed-free-poisoner enable

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力でき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
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 パフォーマンスに重大な影響を及ぼします。このコマンドは、Cisco TAC の指導の下で使用する必要があります。システムの使用頻度が高いときは、実稼働環境でこのコマンドを使用しないでください。

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中のアプリケーションからメモリを解放する要求が FIFO キューに書き込まれます。各要求が FIFO キューに書き込まれると、低レベルのメモリ管理に不要なメモリ中の関連付けられたバイトは、値 0xcc が書き込まれて「無効化」されます。

メモリ解放要求は、空きメモリ プールよりも多くのメモリがアプリケーションに必要になるまで、キューに保持されます。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引き出され、無効化されたメモリが検証されます。

メモリが変更されなかった場合、このメモリは低レベル メモリ プールに戻され、
delayed free-memory poisoner ツールは、最初の要求を行ったアプリケーションからメモリ要求を再発行します。このプロセスは、要求しているアプリケーションにとって十分なメモリが解放されるまで続行されます。

無効化されたメモリが変更済みの場合、クラッシュが発生し、クラッシュの原因を判断するための診断が出力されます。

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。**memory delayed-free-poisoner validate** コマンドを使用して、手動で検証を開始することもできます。

このコマンドの **no** 形式を実行すると、キュー内の要求が参照しているすべてのメモリは空きメモリ プールに戻され、それらのメモリの検証および統計カウンタの消去は行われません。

例

次の例では、delayed free-memory poisoner ツールをイネーブルにしています。

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

次に、delayed free-memory poisoner ツールが不正なメモリ再使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 20-1 で、上記の出力の重要な部分を説明します。

表 20-1　不正なメモリ使用の出力に関する説明

フィールド	説明
heap region	要求を行っているアプリケーションが使用できるアドレス領域とメモリ領域のサイズ。これは要求されたサイズと同じではありません。要求されたサイズは、メモリ要求が行われた時点でシステムがメモリを区分したサイズよりも小さくなる場合があります。
memory address	メモリ中の異常が検出された場所。
byte offset	byte offset はヒープ領域の先頭からの相対位置で、実行結果を使用してこのアドレスから始まるデータ構造を格納した場合、変更されたフィールドの検索に使用できます。値が 0 の場合、またはヒープ領域バイト カウントよりも値が大きい場合、問題は低レベル 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	特定のメモリ領域を対象にした最後の malloc/calloc/realloc および free コールが行われた命令アドレス。
Dumping...	検出された異常がヒープ メモリ領域の先頭から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 ヘッダーの次の 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およびキュー リンケージを格納するのに使用するメモリです。領域内のそれ以外のすべてのバイトには、システム ヒープ トレーラが発生するまで、0xcc が設定されている必要があります。

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消去します。
memory delayed-free-poisoner validate	delayed free-memory poisoner ツールのキュー内の要素を検証します。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況について要約を表示します。

memory delayed-free-poisoner validate

memory delayed-free-poisoner キュー内のすべての要素を検証するには、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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力でき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
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しておく必要があります。

memory delayed-free-poisoner validate コマンドを実行すると、**memory delayed-free-poisoner** キュー内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、クラッシュが発生し、クラッシュの原因を判断するための診断が出力されます。予期しない値が含まれていない場合は、要素はキューに保持され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 プールに戻されません。

（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

次の例では、**memory delayed-free-poisoner** キュー内のすべての要素を検証します。

```
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消去します。
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ついて要約を表示します。

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 プロファイ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*

シンタックスの説明

peak_value	メモリ使用状況のスナップショットがピーク使用状況のバッファに保存される、メモリ使用状況のしきい値を指定します。このバッファの内容は後で分析して、ピーク時のシステム メモリの必要量を判別できます。

デフォルト

メモリのプロファイリングは、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

次の表は、このコマンドを入力でき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
特権 EXEC	•	•	—	•	•

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

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メモリ テキストの範囲をプロファイルに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、メモリの一部はプロファイリング システムにより保持されます。***show memory status*** コマンドの出力を参照してください。

（注） メモリの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ことがあります。

次の例では、メモリ プロファイリングをイネーブルにします。

```
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に関する情報（プロファイリング）を表示します。

memory profile text

プロファイルに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*}

シンタックスの説明

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 ブロックのテキスト範囲終了点を指定します。
resolution	ソース テキスト領域に対するトレースの精度を指定します。
startPC	メモリ ブロックのテキスト範囲開始点を指定します。

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

次の表は、このコマンドを入力でき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
特権 EXEC	•	•	—	•	•

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

テキスト範囲が小さい場合、通常、「4」の精度で命令へのコールをトレースします。テキスト範囲が大きい場合、通常、最初のパスは粗精度で十分ですが、次のパスで範囲がより小さい領域セットに絞り込まれる可能性があります。

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

（注） メモリの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ことがあります。

例

次の例は、プロファイルにメモリのテキスト範囲を 4 の精度で設定する方法を示しています。

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

次の例では、テキスト範囲のコンフィギュレーションおよびメモリ プロファイリングのステータス（OFF）を表示します。

```
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。メモリのプロファイリングは、デフォルトで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消去します。
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に関する情報（プロファイリング）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の範囲を表示します。

memory-size

WebVPN のさまざまなコンポーネントがアクセスするセキュリティ アプライアンス上にメモリ量を設定するには、WebVPN モードで **memory-size** コマンドを使用します。メモリ量は、KB 単位の設定量または全メモリのパーセンテージのいずれでも設定できます。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 サイズの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***]**

シンタックスの説明

kb	メモリ量を KB 単位で指定します。
percent	メモリ量を、セキュリティ アプライアンス上の全メモリのパーセンテージとして指定します。
size	メモリ量を、KB 単位または全メモリのパーセンテージで指定します。

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

次の表は、このコマンドを入力でき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
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。

例

次の例は、WebVPN のメモリ サイズを 30 パーセントに設定する方法を示しています。

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

関連コマンド

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

message-length

設定した最大および最小の長さを満たしていない 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。この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*

シンタックスの説明

max	UDP ペイロードで許可される最大バイト数を指定します。
max_bytes	UDP ペイロードの最大バイト数。範囲は、1 ～ 65,536 です。
min	UDP ペイロードで許可される最小バイト数を指定します。
min_bytes	UDP ペイロードの最小バイト数。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

次の表は、このコマンドを入力でき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
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される長さは、GTP ヘッダーと残りのメッセージ部分（UDP パケットのペイロード）を合せたものです。

例

次の例では、20 ～ 300 バイトの長さのメッセージを許可します。

```
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 GTP 統計情報を消去します。
debug gtp	GTP 検査に関する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	アプリケーション検査に使用する特定の 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

インターフェイス上で MFIB 転送を再度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** コマンドを使用します。インターフェイス上で 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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力でき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
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、MFIB 転送はすべてのインターフェイスでイネーブルになります。特定のインターフェイス上で 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表示されるのは、このコマンドの **no** 形式のみです。

MFIB 転送をインターフェイス上でディセーブルにすると、他の方法で特別に設定しないかぎり、そのインターフェイスはマルチキャスト パケットを受け入れません。MFIB 転送がディセーブルになると、IGMP パケットも妨げられます。

例

次の例では、指定されたインターフェイスでの MFIB 転送をディセーブルにします。

```
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	インターフェイスで PIM をイネーブルにします。

min-object-size

セキュリティ アプライアンスが、WebVPN セッションに対して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場合は、値としてゼロ（0）を入力します。

min-object-size *integer range*

シンタックスの説明

integer range	0 ～ 10000 KB

デフォルト

デフォルト 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でき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 サイズよりも小さくする必要があります。キャッシュ圧縮がイネーブルである場合、セキュリティ アプライアンスは、オブジェクト圧縮後のサイズを計算します。

例

次の例では、最大オブジェクト サイズである 40 KB に設定する方法を示します。

```
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 モードに入ります。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシング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ング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

新しい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*

シンタックスの説明

noconfirm	（オプション）確認プロンプトを表示しないようにします。
disk0:	（オプション）内蔵フラッシュ メモリを指定し、続けてコロン（:）を入力します。
disk1:	（オプション）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:	（オプション）内蔵フラッシュ 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とパス。

デフォルト

パスを指定しない場合、ディレクトリは現在の作業ディレクトリに作成されます。

コマンド モード

次の表は、このコマンドを入力でき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
特権 EXEC	•	•	•	—	•

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

同じ名前のディレクトリがすでに存在する場合、新しい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移動します。
dir	ディレクトリの内容を表示します。
rmdir	指定し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 モードをシングルまたはマルチに設定するには、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、セキュリティ コンテキストと呼ばれる複数の仮想装置に分割できます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立した装置のように動作します。複数のコンテキストは、複数の独立型アプライアンスを持つことに相当します。シングル モードでは、セキュリティ アプライアンスは、1 つのコンフィギュレーションを保有し、1 つの装置のように動作します。マルチ モードでは、独自のコンフィギュレーションを持つ複数のコンテキストを作成できます。作成できるコンテキスト数は、ライセンスに応じて異なります。

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

シンタックスの説明

multiple	マルチ コンテキスト モードを設定します。
noconfirm	（オプション）確認用のプロンプトを表示することなく、モードを設定します。このオプションは、自動スクリプトに役立ちます。
single	コンテキスト モードをシングルに設定します。

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

次の表は、このコマンドを入力でき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
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、セキュリティ ポリシー、インターフェイス、および独立型装置で設定できるほとんどのオプションを指定するコンテキストごとのコンフィギュレーションが含まれます（コンテキスト コンフィギュレーションの場所の指定については、**config-url** コマンドを参照してください）。システム管理者は、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することによって、コンテキストを追加したり管理したりします。これは、シングル モードの場合のコンフィギュレーションと同様、スタートアップ コンフィギュレーションです。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的な設定を指定します。システム コンフィギュレーションには、システム自体のネットワーク インターフェイスまたはネットワークの設定は含まれません。ネットワーク リソースにアクセスする必要がある場合（サーバからコンテキストをダウンロードする場合など）、システム コンフィギュレーションは、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 1 つを使用します。

mode コマンドを使用してコンテキスト モードを変更する場合、リブートするためのプロンプトが表示されます。

コンテキスト モード（シングルまたはマルチ）は、リブート時も保持されますが、コンフィギュレーション ファイルには保存されません。別の装置にコンフィギュレーションをコピーする必要がある場合は、**mode** コマンドを使用して、新しい装置のモードが一致するように設定してください。

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 アプライアンスが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を構成する新しいスタートアップ コンフィギュレーションと、管理コンテキストを構成する admin.cfg（内蔵フラッシュ メモリのルート ディレクトリ内）です。元の実行コンフィギュレーションは、old_running.cfg（内蔵フラッシュ メモリのルート ディレクトリ内）として保存されます。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、システム コンフィギュレーションに「admin」という名前で管理コンテキストのエントリを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、必要に応じて、最初にスタートアップ コンフィギュレーション全体（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ができます。マルチ モードから継承されたシステム コンフィギュレーションは、シングル モードの装置では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 モードでは、すべての機能はサポートされていません。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

例

次の例では、モードをマルチに設定します。

```
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...
```

次の例では、モードをシングルに設定します。

```
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 モードに入ります。
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 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*

シンタックスの説明

if_name	監視対象に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、デフォルトではディセーブルです。

コマンド モード

次の表は、このコマンドを入力でき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
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 アプライアンスで監視できるインターフェイスの数は 250 です。hello メッセージは、各インターフェイスのポーリング間隔の間にセキュリティ アプライアンスのフェールオーバー ペア間で交換されます。フェールオーバー インターフェイスのポーリング間隔は、3 ～ 15 秒です。たとえば、ポーリング間隔が 5 秒に設定されている場合は、hello メッセージが 5 回続けて（25 秒）そのインターフェイスで聴取されないと、インターフェイスでテストが開始します。

監視対象のフェールオーバー インターフェイスのステータスは、次のいずれかになります。

- Unknown：初期ステータス。また、このステータスは、ステータスを判別できないことを意味します。
- Normal：インターフェイスがトラフィックを受信しています。
- Testing：5 ポーリング間隔の間、hello メッセージがインターフェイスで聴取されていません。
- Link Down：インターフェイスまたは VLAN が管理上ダウンしています。

- 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トラフィックが受信されておらず、ピア インターフェイスでもトラフィックが聴取されていません。

Active/Active 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のみ有効です。

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に対してデフォルトのインターフェイス ヘルス モニタリングを復元します。
failover interface-policy	フェールオーバーが発生する基準となる、監視対象のインターフェイスの障害数またはパーセンテージを指定します。
failover polltime	インターフェイスの 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*

シンタックスの説明

/ascii	（オプション）バイナリ モードでバイナリ ファイルと ASCII ファイルを表示します。
/binary	（オプション）バイナリ モードでファイルを表示します。
/ebcdic	（オプション）EBCDIC のバイナリ ファイルを表示します。
disk0	（オプション）内蔵フラッシュ メモリのファイルを表示します。
disk1:	（オプション）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:	（オプション）内蔵フラッシュ 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:	（オプション）FTP サーバのファイルを表示します。
http:	（オプション）Web サイトのファイルを表示します。
https:	（オプション）セキュア Web サイトのファイルを表示します。
system:	（オプション）ファイル システムを表示します。
tftp:	（オプション）TFTP サーバ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

ACSII モード

コマンド モード

次の表は、このコマンドを入力でき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
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ためのプロンプトを表示します。

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	指定し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。

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*]

シンタックスの説明

dense *output_if_name*	（オプション）稠密モード出力用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 フォワーディング）でのみサポートされています。
distance	（オプション）ルートの管理ディスタンス。より短い距離のルートが選択されます。デフォルトは 0 です。
in_if_name	mroute 用の着信インターフェイス名を指定します。
rpf_addr	mroute 用の着信インターフェイス名を指定します。RPF アドレスの PIM neighbor、PIM join、graft、prune の各メッセージがそのインターフェイスに送信されます。*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。それがルートである場合、ユニキャスト ルーティング テーブルから再帰ルックアップが行われ、直接接続されたシステムを検索します。
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

次の表は、このコマンドを入力でき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
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のものです。

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ときと同じインターフェイス上で、マルチキャスト パケットを受信すると予想します。マルチキャスト ルーティングをサポートしていないルートをバイパスする場合など、場合によっては、マルチキャスト パケットがユニキャスト パケットとは異なるパスを通ることがあります。

スタティック マルチキャスト ルートは、アドバタイジングまたは再配布されません。

マルチキャスト ルーティング 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の 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

次の例は、**mroute** コマンドを使用して、スタティック マルチキャスト ルートを設定する方法を示しています。

```
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	**mroute** コマンドをコンフィギュレーションから削除します。
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内の **mroute** コマンドを表示します。

msie-proxy except-list

クライアント PC 上でローカル バイパス用の Microsoft Internet Explorer ブラウザ プロキシ例外リスト設定値を設定するには、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。このアトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

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

no msie-proxy except-list

シンタックスの説明

none	IP アドレス / ホスト名およびポートが存在しないことを示し、例外リストを継承しないようにします。
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。ポート番号はオプションです。

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

次の表は、このコマンドを入力でき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
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

次の例は、FirstGroup というグループ ポリシーに対して Microsoft Internet Explorer プロキシ例外リスト（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）を設定する方法を示しています。

```
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 アトリビュートの値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー アトリビュートを削除します。

msie-proxy local-bypass

クライアント PC に対して Microsoft Internet Explorer ブラウザ プロキシ ローカル バイパス設定値を設定するには、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。このアトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

msie-proxy local-bypass {enable | disable}

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

シンタックスの説明

disable	クライアント PC に対して Microsoft Internet Explorer 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 に対して Microsoft Internet Explorer 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

次の表は、このコマンドを入力でき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
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

次の例は、FirstGroup というグループ ポリシーに対して Microsoft Internet Explorer プロキシ ローカル バイパスをイネーブルにする方法を示しています。

```
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 アトリビュートの値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー アトリビュートを削除します。

msie-proxy method

クライアント PC に対して Microsoft Internet Explorer ブラウザ プロキシ アクション（「方式」）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。このアトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

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

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

シンタックスの説明

auto-detect	クライアント PC に対して Internet Explorer の自動プロキシ 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 に対して Internet Explorer の HTTP ブラウザ プロキシ サーバ設定を変更しないようにします。
no-proxy	このクライアント PC に対して Interenet Explorer の HTTP プロキシ設定をディセーブルにします。
use-server	**msie-proxy server** コマンドで設定された値を使用するように Internet Explorer の HTTP プロキシ サーバ設定値を設定します。

デフォルト

デフォルトの方式は use-server です。

コマンド モード

次の表は、このコマンドを入力でき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
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

次の例は、FirstGroup というグループ ポリシーに対して Microsoft Internet Explorer プロキシ設定値として自動検出を設定する方法を示しています。

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

次の例では、クライアント PC のサーバとして QAserver サーバ、ポート 1001 を使用するように、FirstGroup というグループ ポリシーに対して Microsoft Internet Explorer プロキシ設定値を設定しています。

```
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 server	クライアント PC に対して Microsoft Internet Explorer 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 アトリビュートの値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー アトリビュートを削除します。

msie-proxy server

クライアント PC に対して Microsoft Internet Explorer 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。このアトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

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

no msie-proxy server

シンタックスの説明

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存在しないことを示し、サーバを継承しないようにします。
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。ポート番号はオプションです。

デフォルト

デフォルトでは、msie-proxy サーバは指定されていません。

コマンド モード

次の表は、このコマンドを入力でき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
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

次の例は、FirstGroup というグループ ポリシーに対して Microsoft Internet Explorer プロキシ サーバとして IP アドレス 192.168.10.1（ポート 880 を使用）を設定する方法を示しています。

```
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 アトリビュートの値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー アトリビュートを削除します。

mtu

インターフェイスの Maximum Transmission Unit（MTU; 最大伝送ユニット）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 **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 1,500 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*

シンタックスの説明

bytes	MTU のバイト数を指定します。有効値は 64 ～ 65,535 バイトです。
interface_name	内部または外部のネットワーク インターフェイスの名前。

デフォルト

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

コマンド モード

次の表は、このコマンドを入力でき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
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のものです。

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のサイズを設定できます。MTU 値より大きなデータは、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 RFC 1191 で定義されている IP Path MTU Discovery をサポートしています。IP Path MTU Discovery によって、ホストは、パスに沿ったさまざまなリンクの最大許容 MTU サイズでの相違を動的に検出して対応できます。パケットがインターフェイスに設定された MTU よりも大きいが、「don't fragment」（DF）ビットが設定されているため、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、発信元ホストに対してこの問題を警告しながらメッセージを送信します。ホスト側では、宛先用にパケットをフラグメント化して、パスに沿ったリンクすべての最小パケット サイズに合せる必要があります。

イーサネット インターフェイスの場合、デフォルトの MTU は 1 ブロック 1,500 バイトで、これは最大値でもあります。これはほとんどのアプリケーションで十分な値ですが、ネットワークの条件で必要とされる場合はこれより低い数値を選択できます。

Layer 2 Tunneling Protocol（L2TP）を使用している場合は、MTU サイズを 1,380 に設定することを推奨します。このサイズは、L2TP ヘッダー長と IPSec ヘッダー長に相当するためです。

例

次の例は、インターフェイスの MTU を指定する方法を示しています。

```
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ユニット値を消去します。
show running-config mtu	現在の最大伝送ユニットのブロック サイズを表示します。

multicast boundary

管理用マルチキャスト 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はマルチキャスト データ パケット フローを制限し、異なる管理ドメインでの同一マルチキャスト グループ アドレスの再使用をイネーブルにします。

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

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

シンタックスの説明

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 リストでは、境界によって影響を受けるアドレスの範囲が定義されます。このコマンドでは、標準 ACL だけを使用してください。拡張 ACL はサポートされていません。
filter-autorp	境界 ACL により拒否された Auto-RP メッセージをフィルタリングします。指定されない場合、Auto-RP メッセージはすべて渡されます。

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

次の表は、このコマンドを入力でき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
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

このコマンドを使用してインターフェイスに管理用の境界を設定し、*acl* 引数で定義された範囲内のマルチキャスト グループ アドレスをフィルタリングします。標準のアクセス リストは、対象となるアドレスの範囲を定義します。このコマンドを設定する場合、マルチキャスト データ パケットについては、いずれの方向においても境界をまたがってのフローは許可されません。マルチキャスト データ パケットを制限すると、異なる管理ドメインでの同一マルチキャスト グループ アドレスの再使用がイネーブルになります。

filter-autorp キーワードを設定すると、管理用の境界は Auto-RP の探索と通知のメッセージも検査し、境界 ACL により拒否された Auto-RP パケットから Auto-RP グループ範囲通知を削除します。Auto-RP グループ範囲内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、Auto-RP グループ範囲通知は境界によって許可され、渡されます。アドレスが許可されない場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージから削除された後で、Auto-RP メッセージが転送されます。

例

次の例では、すべての管理用アドレスに境界を設定し、Auto-RP メッセージをフィルタリングします。

```
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 アプライアンス上のマルチキャスト 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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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 PIM と IGMP をイネーブルにします。

コマンド モード

次の表は、このコマンドを入力でき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
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の PIM と 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 の場合は、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数は、システムの RAM 量によって制限されます。表 20-2 に、セキュリティ アプライアンスの RAM 量に基づいた特定のマルチキャスト テーブルの最大エントリ数を示します。これらの制限値に達すると、新しいエントリはすべて廃棄されます。

表 20-2　マルチキャスト テーブル エントリの制限値

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

例

次の例では、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	インターフェイスで IGMP をイネーブルにします。
pim	インターフェイスで PIM をイネーブルにします。