mac address コマンド～ match dscp コマンド

mac address

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

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

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

構文の説明

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

デフォルト

デフォルトの設定は次のとおりです。

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

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

他のコマンドまたは方法を使用して MAC アドレスを設定することもできますが、1 つの方法だけを使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。

例

次の部分的な例では、フェールオーバー グループで可能な設定を示します。

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

関連コマンド

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

mac-address

プライベート MAC アドレスをインターフェイスまたはサブインターフェイスに手動で割り当てるには、インターフェイス コンフィギュレーション モードで **mac-address** コマンドを使用します。マルチ コンテキスト モードでは、このコマンドは各コンテキストでそれぞれ別の MAC アドレスをインターフェイスに割り当てることができます。クラスタの個々のインターフェイスに、MAC アドレスのクラスタ プール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* | **site-id** *number* [**site-ip** *ip_address*]] | **cluster-pool** *pool_name*}

no mac-address [*mac_address* [**standby** *mac_address* | **site-id** *number* [**site-ip** *ip_address*]] | **cluster-pool** *pool_name*]

構文の説明

cluster-pool *pool_name*	個別インターフェイス モードのクラスタ（**cluster interface-mode** コマンドを参照）、または任意のクラスタ インターフェイス モードの管理インターフェイスについて、各クラスタ メンバの特定のインターフェイスに使用する MAC アドレスのプールを設定します。プールは **mac-address pool** コマンドを使用して定義します。
mac_address	このインターフェイスの MAC アドレスを H.H.H 形式で設定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。フェールオーバーを使用する場合は、この MAC アドレスがアクティブな MAC アドレスとなります。 （注） 自動生成されたアドレス（**mac-address auto** コマンド）は A2 で始まるため、A2 を含む手動 MAC アドレスは自動生成を使用しようとしても開始できません。
site-id *number*	（任意、ルーテッド モードのみ）サイト間クラスタリングの場合、各サイトのサイト固有 MAC アドレスを設定します。
site-ip *ip_address*	（任意、ルーテッド モードのみ）サイト間クラスタリングの場合、各サイトのサイト固有 IP アドレスを設定します。この IP アドレスはグローバル IP アドレスと同じサブネット内になければなりません。
standby *mac_address*	（任意）フェールオーバーのスタンバイ MAC アドレスを設定します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(5)/8.2(2)	**mac-address auto** コマンドと併用するときには、MAC アドレスを開始する A2 の使用が制限されました。
9.0(1)	クラスタリングをサポートするために、**cluster-pool** キーワードが追加されました。
9.5(1)	**site-id** キーワードが追加されました。
9.6(1)	**site-ip** キーワードが追加されました。

使用上のガイドライン

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

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

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

他のコマンドまたは方法を使用して MAC アドレスを設定することもできますが、1 つの方法だけを使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。

クラスタリングの場合は、スパンド EtherChannel のグローバル MAC アドレスを設定する必要があります。MAC アドレスが手動設定されている場合、その MAC アドレスは現在のマスター ユニットに留まります。マルチ コンテキスト モードでは、コンテキスト間でインターフェイスを共有した場合、MAC アドレスの自動生成をイネーブルにする必要があります。非共有インターフェイスについては MAC アドレスを手動で設定する必要があることに注意してください。

ルーテッド モードのサイト間クラスタリングの場合は、各サイトのマスター ユニットでサイト固有の MAC アドレスと IP アドレスを設定してから、各ユニットで **site-id** コマンドを使用してそれをサイトに割り当てます。

例

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

```
ciscoasa/contextA(config)# interface gigabitethernet0/1.1
ciscoasa/contextA(config-if)# nameif inside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa/contextA(config-if)# mac-address 030C.F142.4CDE standby 040C.F142.4CDE
ciscoasa/contextA(config-if)# no shutdown
```

次に、スパンド EtherChannel ポートチャネル 1のサイト固有 MAC アドレスを設定する例を示します。

```
ciscoasa(config-if)# interface port-channel 1
ciscoasa(config-if)# port-channel span-cluster
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1 site-ip 10.7.7.1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2 site-ip 10.7.7.2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3 site-ip 10.7.7.3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4 site-ip 10.7.7.4
```

関連コマンド

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

mac-address auto

プライベート MAC アドレスを各共有コンテキスト 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。自動 MAC アドレスをディセーブルにするには、このコマンドの **no** 形式を使用します。

mac-address auto [**prefix** *prefix*]

no mac-address auto

構文の説明

prefix *prefix*	（オプション）MAC アドレスの一部として使用するユーザ定義のプレフィックスを設定します。*prefix* は、0 ～ 65535 の 10 進数です。プレフィックスを入力しない場合、ASA でデフォルトのプレフィックスが生成されます。 このプレフィックスは、4 桁の 16 進数値に変換されます。プレフィックスにより、各 ASA はそれぞれ固有の MAC アドレスを使用（異なるプレフィックスの値を使用）するようになるため、1 つのネットワーク セグメントに複数の ASA を配置したりできます。

デフォルト

自動 MAC アドレス 生成はデフォルトでディスエーブルになっています（デフォルトでイネーブルになっている ASASM の場合を除く）。イネーブルにすると、ASA は、インターフェイス（ASA 5500-X）またはバックプレーン（ASASM）MAC アドレスの最後の 2 バイトに基づいてプレフィックスを自動生成します。必要に応じて、プレフィックスをカスタマイズできます。

MAC アドレスの生成をディセーブルにした場合は、デフォルトの MAC アドレスは次のようになります。

- ASA 5500-X シリーズ アプライアンスの場合：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、1 つの物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。
- ASASM の場合：すべての VLAN インターフェイスが同じ MAC アドレスを使用します。これは、バックプレーンの MAC アドレスから導出されたものです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(5)/8.2(2)	**prefix** キーワードが追加されました。プレフィックスを使用し、固定の開始値（A2）を使用し、フェールオーバー ペアのプライマリ ユニットおよびセカンダリ ユニットの MAC アドレスで別の方式を使用するように、MAC アドレス形式が変更されました。MAC アドレスはリロード後も維持されるようになりました。コマンド パーサーは現在、自動生成がイネーブルになっているかどうかをチェックします。MAC アドレスを手動でも割り当てることができるようにする場合は、A2 を含む手動 MAC アドレスは開始できません。
8.5(1)	ASASM の場合にのみ自動生成がデフォルトでイネーブルになる（**mac-address auto**）ようになりました。
8.6(1)	現在、ASA は、MAC アドレスの自動生成設定をデフォルトのプレフィックスを使用するように変換します。ASA は、インターフェイス（ASA 5500）またはバックプレーン（ASASM）MAC アドレスの最後の 2 バイトに基づいてプレフィックスを自動生成します。この変換は、リロード時または MAC アドレス生成を再度イネーブルにすると、自動的に行われます。MAC アドレス生成の従来の方法は使用できなくなります。 **（注）** フェールオーバー ペアのヒットレス アップグレードを維持するため、ASA は、フェールオーバーがイネーブルである場合、リロード時に既存のコンフィギュレーションの MAC アドレス方式を変換 *しません*。

使用上のガイドライン

インターフェイスを共有するコンテキストを許可するには、固有の MAC アドレスを各共有コンテキスト インターフェイスに割り当てることを推奨します。MAC アドレスは、コンテキスト内でパケットを分類するために使用されます。インターフェイスを共有するものの、各コンテキストにインターフェイスの固有の MAC アドレスがない場合は、宛先 IP アドレスがパケットの分類に使用されます。宛先アドレスは、コンテキスト NAT コンフィギュレーションと照合されます。この方法には、MAC アドレスの方法に比べるといくつか制限があります。パケットの分類の詳細については、CLI 設定ガイドを参照してください。

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

手動 MAC アドレスとの通信

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

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

フェールオーバー用の MAC アドレス

フェールオーバーで使用できるように、ASA はインターフェイスごとにアクティブとスタンバイの両方の MAC アドレスを生成します。アクティブ ユニットがフェールオーバーしてスタンバイ ユニットがアクティブになると、その新規アクティブ ユニットがアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。詳細については、「プレフィックスを使用する場合の MAC アドレス形式」を参照してください。

prefix キーワードが追加される前に従来のバージョンの **mac-address auto** コマンドを使用してフェールオーバーユニットをアップグレードする場合は、「プレフィックスを使用しない場合の MAC アドレス形式（従来の方法）」の項を参照してください。

プレフィックスを使用する場合の MAC アドレス形式

ASA は、次の形式を使用して MAC アドレスを生成します。

A2*xx.yyzz.zzzz*

xx.yy はユーザ定義プレフィックスまたはインターフェイス（ASA 5500）またはバックプレーン（ASASM）MAC アドレスの最後の 2 バイトに基づいて自動生成されたプレフィックス、*zz.zzzz* は ASA によって生成される内部カウンタです。スタンバイ MAC アドレスの場合、内部カウンタが 1 増えることを除けばアドレスは同じです。

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

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

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

A2**F1.03***zz.zzzz*

プレフィックスを使用しない場合の MAC アドレス形式（従来の方法）

この方法は、フェールオーバーを使用しており、バージョン 8.6 以降にアップグレードした場合に使用できます。この場合、プレフィックス方式を手動でイネーブルにする必要があります。

プレフィックスを指定しないと、MAC アドレスは次の形式で生成されます。

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

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

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

この MAC アドレス生成方法では、リロード間で MAC アドレスが持続されず、同じネットワークセグメントに複数の ASA を配置できず（固有の MAC アドレスが保証されないため）、手動で割り当てた MAC アドレスとの MAC アドレスの重複が回避されません。これらの問題を回避するため、プレフィックスを使用して MAC アドレスを生成することをお勧めします。

MAC アドレスが生成される場合

コンテキストでインターフェイスの **nameif** コマンドを設定すると、ただちに新規 MAC アドレスが生成されます。コンテキスト インターフェイスを設定した後でこのコマンドをイネーブルにした場合、コマンドを入力するとただちにすべてのインターフェイスの MAC アドレスが生成されます。**no mac-address auto** コマンドを使用すると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。

他の方法を使用した MAC アドレスの設定

他のコマンドまたは方法を使用して MAC アドレスを設定することもできますが、1 つの方法だけを使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。

システム コンフィギュレーションでの MAC アドレスの表示

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

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

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

コンテキスト内の MAC アドレスの表示

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

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

例

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

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

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

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

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

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

```
ciscoasa# show running-config all context

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

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

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

関連コマンド

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

mac-address pool

ASA クラスタの個々のインターフェイスで使用する MAC アドレス プールを追加するには、グローバル コンフィギュレーション モードで **mac-address pool** コマンドを使用します。未使用のプールを削除するには、このコマンドの **no** 形式を使用します。

mac-address pool *name start_mac_address* **-** *end_mac_address*

no mac-address pool *name* [*start_mac_address* **-** *end_mac_address*]

構文の説明

name	プールの名前を 63 文字以内で指定します。
start_mac_address **-** *end_mac_address*	最初の MAC アドレスと最後の MAC アドレスを指定します。ダッシュ (-) の前後にスペースが必要です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このプールは、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 cluster-pool** コマンドで使用できます。インターフェイスに MAC アドレスを手動で設定することはあまりありませんが、そのような場合には、このプールを使用して各インターフェイスに一義的な MAC アドレスを割り当てます。

例

次に、8 個の MAC アドレスを含む MAC アドレス プールを追加し、GigabitEthernet 0/0 インターフェイスに割り当てる例を示します。

```
ciscoasa(config)# mac-address pool pool1 000C.F142.4CD1 - 000C.F142.4CD7
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-ifc)# mac-address cluster-pool pool1
```

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ます。
mac-address	インターフェイスの MAC アドレスを設定します。

mac-address-table aging-time

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

mac-address-table aging-time *timeout_value*

no mac-address-table aging-time

構文の説明

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

デフォルト

デフォルトのタイムアウトは 5 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	Integrated Routing and Bridging（IRB; 統合ルーティングおよびブリッジング）を使用するときに、ルーテッド モードでこのコマンドを設定できるようになりました。

使用上のガイドライン

使用方法のガイドラインはありません。

例

次に、MAC アドレスのタイムアウトを 10 分に設定する例を示します。

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

関連コマンド

コマンド	説明
arp-inspection	ARP パケットとスタティック ARP エントリを比較する ARP インスペクションをイネーブルにします。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	ダイナミック エントリおよびスタティック エントリを含む MAC アドレス テーブルを表示します。

mac-address-table static

MAC アドレス テーブルにスタティック エントリを追加するには、グローバル コンフィギュレーション モードで **mac-address-table static** コマンドを使用します。スタティック エントリを削除するには、このコマンドの **no** 形式を使用します。MAC アドレスは通常、特定の MAC アドレスからのトラフィックがインターフェイスに入るときに MAC アドレス テーブルにダイナミックに追加されます。スタティック MAC アドレスは、必要に応じて MAC アドレス テーブルに追加できます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。スタティック エントリと同じ MAC アドレスを持つクライアントが、そのスタティック エントリに一致しないインターフェイスにトラフィックを送信しようとした場合、ASA はトラフィックをドロップし、システム メッセージを生成します。

mac-address-table static *interface_name mac_address*

no mac-address-table static *interface_name mac_address*

構文の説明

interface_name	送信元のブリッジ グループ メンバー インターフェイス。
mac_address	テーブルに追加する MAC アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	Integrated Routing and Bridging（IRB; 統合ルーティングおよびブリッジング）を使用するときに、ルーテッド モードでこのコマンドを設定できるようになりました。

例

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

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

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	MAC アドレス テーブルのエントリを表示します。

mac-learn

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

mac-learn *interface_name* **disable**

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

構文の説明

interface_name	MAC 学習をディセーブルにするブリッジ グループ メンバー インターフェイス。
disable	MAC 学習をディセーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	Integrated Routing and Bridging（IRB; 統合ルーティングおよびブリッジング）を使用するときに、ルーテッド モードでこのコマンドを設定できるようになりました。

例

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

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

関連コマンド

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

mac-list

認証や許可から MAC アドレスを削除するのに使用される MAC アドレスのリストを指定するには、グローバル コンフィギュレーション モードで **mac-list** コマンドを使用します。MAC アドレス リストのエントリを削除するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

例

次の例では、1 個の MAC アドレスに対する認証をバイパスします。

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

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

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

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

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

関連コマンド

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

mail-relay

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

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

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

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、特定のドメインへのメール中継を設定する例を示します。

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

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

management-access

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

management-access *mgmt_if*

no management-access *mgmt_if*

構文の説明

mgmt_if	別のインターフェイスから ASA に入るときにアクセスする管理インターフェイスの名前を指定します。物理または仮想インターフェイスを指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.9.(2)	仮想インターフェイスが指定可能になりました。

使用上のガイドライン

このコマンドを使用すると、フル トンネル IPsec VPN または SSL VPN クライアント（AnyConnect 2.x クライアント、SVC 1.x）を使用するときや、サイトツーサイト IPsec トンネルを横断するときには、ASA への通過ルートとなるインターフェイス以外のインターフェイスに接続できます。ASA 管理インターフェイスへの接続には Telnet、SSH、Ping、または ASDM を使用できます。

管理アクセス インターフェイスは 1 つだけ定義できます。

9.5(1) 以降、別個の管理/データ ルーティング テーブルでのルーティングを考慮すると、VPN の端末インターフェイスと管理アクセス インターフェイスは同じ種類である（つまり両方とも管理専用インターフェイスであるか、通常のデータ インターフェイスである）必要があります。したがって、稀に VPN 端末インターフェイスが管理専用である場合を除き、管理専用インターフェイス上には管理アクセスを設定しないでください。

管理アクセス インターフェイスと VPN ネットワークの間でアイデンティティ NAT を使用する場合（VPN トラフィックに共通の NAT コンフィギュレーションを使用する場合）、**nat** コマンドの **route-lookup** キーワードを指定する必要があります。ルート ルックアップがない場合、ASA は、ルーティング テーブルの内容に関係なく、**nat** コマンドで指定されたインターフェイスからトラフィックを送信します。たとえば、**management-access inside** を設定すると、VPN ユーザが外部から内部インターフェイスを管理できます。アイデンティティ **nat** コマンドで **(inside,outside)** を指定した場合、ASA で、内部ネットワークに管理トラフィックを送信しません。これは、内部インターフェイスの IP アドレスには戻りません。ルート ルックアップ オプションを使用すると、ASA は、内部ネットワークの代わりに内部インターフェイスの IP アドレスに直接トラフィックを送信できます。VPN クライアントから内部ネットワーク上のホストへのトラフィックの場合、ルート ルックアップ オプションがあっても正しい出力インターフェイス（内部）になるため、通常のトラフィック フローは影響を受けません。

例

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

```
ciscoasa(config)# management-access inside
```

関連コマンド

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

management-only

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

management-only [**individual**]

no management-only [**individual**]

構文の説明

individual	Firepower 9300 ASA セキュリティ モジュール クラスタの場合は、スパンド インターフェイス モードのときに管理インターフェイスに **individual** キーワードを指定する必要があります。

デフォルト

Management *n*/*n* インターフェイス（該当するモデルを使用している場合）は、デフォルトで管理専用モードに設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	ASA クラスタリングをサポートするために、管理インターフェイスの例外として、このコマンドが実行コンフィギュレーションからインターフェイス セクションの先頭に移動されました。
9.4(1.152)	**individual** キーワードが追加されました。

使用上のガイドライン

ほとんどのモデルには、Management *n*/*n* という専用の管理インターフェイスが含まれ、ASA へのトラフィックをサポートするようになっています。ただし、**management-only** コマンドを使用することで、任意のインターフェイスを管理専用インターフェイスとして設定できます。

（注） ASA 5585-X を除くすべてのモデルでは、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することはできません。このコマンドはデフォルトで常にイネーブルになります。

トランスペアレント ファイアウォール モードでは、許可される最大通過トラフィック インターフェイスに加えて、管理インターフェイス（物理インターフェイス、サブインターフェイス（使用しているモデルでサポートされている場合）、管理インターフェイスからなる EtherChannel インターフェイス（複数の管理インターフェイスがある場合）のいずれか）を個別の管理インターフェイスとして使用できます。他のインターフェイス タイプは管理インターフェイスとして使用できません。

使用しているモデルに管理インターフェイスが含まれていない場合は、データ インターフェイスからトランスペアレント ファイアウォールを管理する必要があります。

マルチ コンテキスト モードでは、どのインターフェイスも（これには管理インターフェイスも含まれます）、コンテキスト間で共有させることはできません。コンテキスト単位で管理を行うには、管理インターフェイスのサブインターフェイスを作成し、管理サブインターフェイスを各コンテキストに割り当てます。ASA 5585-X 以外では、管理インターフェイスがサブインターフェイスを許可しないため、コンテキスト単位で管理を行うにはデータ インターフェイスに接続する必要があることに注意してください。

管理インターフェイスは、通常のブリッジ グループの一部ではありません。動作上の目的から、設定できないブリッジ グループの一部です。

例

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

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

次に、サブインターフェイスで管理専用モードをイネーブルにする例を示します。

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

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

map-domain

マッピングアドレスとポート(MAP)ドメインを設定するには、グローバル コンフィギュレーション モードで **map-domai** コマンドを使用します。MAP ドメインを削除するには、このコマンドの **no** 形式を使用します。

map-domain *name*

no map-domain *name*

構文の説明

name	MAP ドメインの名前は、英数字で最大 48 文字です。また、名前には、ピリオド(.)、スラッシュ(/)、およびコロン(:)の特殊文字を含めることもできます。

デフォルト

デフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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 モード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(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

アドレスとポートのマッピング(MAP)は、主にサービスプロバイダー(SP)ネットワークで使用する機能です。サービスプロバイダーは、IPv6 専用ネットワーク、MAP ドメインを稼働でき、同時に、IPv4 専用のサブスクライバをサポートし、パブリックインターネット上の IPv4 専用サイトとの通信ニーズに対応します。MAP は、RFC7597、RFC7598、および RFC7599 で定義されています。

MAP ドメイン内のサービスプロバイダーの場合、NAT46 を介した MAP の利点は、サブスクライバの IPv4 アドレスに対する IPv6 アドレスの代替(および SP ネットワークエッジでの IPv4 への変換)がステートレスであることです。これにより、NAT46 と比較して SP ネットワーク内の効率が向上します。

MAP 変換(MAP-T)と MAP カプセル化(MAP-E)という 2 つのマップ技術があります。ASA は MAP-T をサポートしています。MAP-E はサポートされていません。

MAP-T を設定するには、1 つまたは複数のドメインを作成します。カスタマーエッジ(CE)およびボーダーリレー(BR)デバイスで MAP-T を設定する場合は、各ドメインに参加するデバイスごとに同じパラメータを使用するようにしてください。

最大 25 個の MAP-T ドメインを設定できます。マルチコンテキストモードでは、コンテキストごとに最大 25 のドメインを設定できます。

例

次の例では、1 という名前の MAP-T ドメインを作成して、ドメインの変換ルールを設定しています。

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

関連コマンド

コマンド	説明
basic-mapping-rule	MAP ドメインの基本マッピング ルールを設定します。
default-mapping-rule	MAP ドメインのデフォルト マッピング ルールを設定します。
ipv4-prefix	MAP ドメインの基本マッピング ルールの IPv4 プレフィックスを設定します。
ipv6-prefix	MAP ドメインの基本マッピング ルールの IPv6 プレフィックスを設定します。
map-domain	マッピング アドレスおよびポート(MAP)ドメインを設定します。
share-ratio	MAP ドメインの基本マッピング ルールのポート数を設定します。
show map-domain	マッピング アドレスおよびポート(MAP)ドメインに関する情報を表示します。
start-port	MAP ドメインの基本マッピング ルールの開始ポートを設定します。

map-name

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

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

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

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

構文の説明

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

デフォルト

デフォルトでは、名前のマッピングはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

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

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

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

例

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

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

LDAP 属性マップ コンフィギュレーション モードで「?」を入力すると、シスコのすべての LDAP 属性名を表示できます。

```
ciscoasa(config-ldap-attribute-map)# map-name <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
ciscoasa(config-ldap-attribute-map)#
```

関連コマンド

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

mapping-service（廃止予定）

Cisco Intercompany Media Engine プロキシに対してマッピング サービスを設定するには、UC-IME コンフィギュレーション モードで **mapping-service** コマンドを使用します。プロキシからマッピング サービスを削除するには、このコマンドの **no** 形式を使用します。

mapping-service listening-interface *interface* [**listening-port** *port*] **uc-ime-interface** *interface*

no mapping-service listening-interface *interface* [**listening-port** *port*] **uc-ime-interface** *interface*

構文の説明

interface	リッスンするインターフェイスまたは uc-ime インターフェイスに使用されるインターフェイスの名前を指定します。
listening-interface	マッピング要求を ASA がリッスンするインターフェイスを設定します。
listening-port	（任意）マッピング サービスのリスニング ポートを設定します。
port	（任意）マッピング要求を ASA がリッスンする TCP ポート番号を指定します。このポート番号は、デバイス上の他のサービス（Telnet や SSH など）との競合を避けるために、1024 以上にする必要があります。デフォルトでは、このポート番号は TCP 8060 です。
uc-ime-interface	リモート Cisco UCM に接続するインターフェイスを設定します。

デフォルト

デフォルトでは、Cisco Intercompany Media Engine プロキシのオフパス配置のためのマッピング サービスは、TCP ポート 8060 でリッスンします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
UC-IME コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
9.4(1)	このコマンドは、すべての **uc-ime** モード コマンドとともに廃止されました。

使用上のガイドライン

ASA の Cisco Intercompany Media Engine プロキシのオフパス配置の場合、マッピング サービスをプロキシ コンフィギュレーションに追加します。マッピング サービスを設定するには、マッピング要求をリッスンする外部インターフェイス（リモート エンタープライズ側）およびリモートの Cisco UCM に接続するインターフェイスを指定する必要があります。

（注） Cisco Intercompany Media Engine プロキシに対して設定できるマッピング サーバは 1 つだけです。

Cisco Intercompany Media Engine プロキシがオフパス配置に対して設定されたときにマッピング サービスを設定します。

オフ パス配置では、Cisco Intercompany Media Engine のインバウンド コールおよびアウトバウンド コールは、Cisco Intercompany Media Engine プロキシを使用してイネーブルにされた適応型セキュリティ アプライアンスを通過します。適応型セキュリティ アプライアンスは DMZ にあり、主に Cisco Intercompany Media Engine をサポートするように設定されています。通常のインターネットに接続するトラフィックは、この ASA を通過しません。

すべてのインバウンド コールのシグナリングは、宛先の Cisco UCM のグローバル IP アドレスが ASA 上に設定されているため、ASA に誘導されます。アウトバウンド コールの場合、着信側はインターネット上の任意の IP アドレスになる可能性があります。そのため、ASA には、インターネット上の着信側のグローバル IP アドレスごとに ASA 上で内部 IP アドレスを動的に提供するマッピング サービスが設定されます。

Cisco UCM は、すべてのアウトバウンド コールを、インターネット上の着信側のグローバル IP アドレスではなく、適応型セキュリティ アプライアンス上のマッピング内部 IP アドレスに直接送信します。その後、ASA によって、それらのコールは着信側のグローバル IP アドレスに転送されます。

例

次に ... をする例を示します。

```
ciscoasa(config)# uc-ime offpath_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback monitoring timer 120
ciscoasa(config-uc-ime)# fallback hold-down timer 30
ciscoasa(config-uc-ime)# mapping-service listening-interface inside listening-port 8060
uc-ime-interface outside
```

関連コマンド

コマンド	説明
show running-config uc-ime	Cisco Intercompany Media Engine プロキシの実行コンフィギュレーションを表示します。
show uc-ime	フォールバック通知、マッピング サービス セッション、およびシグナリング セッションに関する統計情報または詳細情報を表示します。
uc-ime	Cisco Intercompany Media Engine プロキシ インスタンスを ASA に作成します。

map-value

ユーザ定義の値をシスコの LDAP の値にマッピングするには、LDAP 属性マップ コンフィギュレーション モードで **map-value** コマンドを使用します。マップ内のエントリを削除するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

デフォルト

デフォルトでは、シスコ属性にマッピングされるユーザ定義の値がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

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

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

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

例

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

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

関連コマンド

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

マスク

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

mask [log]

no mask [log]

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

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

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

例

次に、ASA でのトラフィックの通過を許可する前に、DNS ヘッダーで RD フラグおよび RA フラグをマスクする例を示します。

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

関連コマンド

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

mask-banner

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

mask-banner

no mask-banner

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、サーバ バナーをマスクする例を示します。

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

関連コマンド

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

mask-syst-reply

FTP サーバ応答をクライアントから見えないようにするには、**ftp-map** コマンドを使用してアクセスできる FTP マップ コンフィギュレーション モードで **mask-syst-reply** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

mask-syst-reply

no mask-syst-reply

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

例

次に、ASA で syst コマンドに対する FTP サーバの応答を一連の X に置き換える例を示します。

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

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
ftp-map	FTP マップを定義し、FTP マップ コンフィギュレーション モードをイネーブルにします。

コマンド	説明
inspect ftp	アプリケーション インスペクションに使用する特定の FTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
request-command deny	不許可にする FTP コマンドを指定します。

match access-list

モジュラ ポリシー フレームワーク を使用するときは、クラス マップ コンフィギュレーション モードで **match access-list** コマンドを使用して、アクセス リストに基づいてアクションを適用するトラフィックを特定します。**match access-list** コマンドを削除するには、このコマンドの **no** 形式を使用します。

match access-list *access_list_name*

no match access-list *access_list_name*

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

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

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

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

3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

例

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

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

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

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

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

関連コマンド

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

match any

モジュラ ポリシー フレームワーク を使用するときは、クラス マップ コンフィギュレーション モードで **match any** コマンドを使用して、アクションを適用するすべてのトラフィックを一致させます。**match any** コマンドを削除するには、このコマンドの **no** 形式を使用します。

match any

no match any

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

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

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

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

例

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

```
ciscoasa(config)# class-map cmap
ciscoasa(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、ポリシー マップ コンフィギュレーション モードで **match apn** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **apn regex** {*regex_name* | **class** *regex_class_name*}

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

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、GTP ポリシー マップで設定できます。

例

次に、GTP インスペクション ポリシー マップのアクセス ポイント名に関して一致条件を設定する例を示します。

```
ciscoasa(config-pmap)# match apn class gtp_regex_apn
```

関連コマンド

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

match application-id

Diameter メッセージの Diameter アプリケーション ID に関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match application-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**] **application-id** *app_id* [*app_id_2*]

no match [**not**] **application-id** *app_id* [*app_id_2*]

構文の説明

app_id	Diameter アプリケーションの名前または番号（0 ～ 4294967295）。照合する連続番号が付されたアプリケーションの範囲がある場合は、2 番目の ID を含めることができます。アプリケーションの名前または番号別に範囲を定義でき、第 1 ID および第 2 ID の間のすべての番号に適用されます。

デフォルト

Diameter インスペクションでは、すべてのアプリケーションが許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Diameter インスペクション クラス マップまたは Diameter インスペクション ポリシー マップで設定できます。このコマンドを使用すると、Diameter アプリケーション ID に基づいてトラフィックをフィルタ処理できます。その後、パケットをドロップしたり、接続をドロップしたり、一致するトラフィックをログに記録したりすることができます。

これらのアプリケーションは IANA に登録されます。次のコア アプリケーションがサポートされますが、他のアプリケーションもフィルタ処理できます。アプリケーション名のリストについては、CLI ヘルプを参照してください。

- **3gpp-rx-ts29214**（16777236）
- **3gpp-s6a**（16777251）

- **3gpp-s9**（16777267）
- **common-message**（0）（基本 Diameter プロトコル）

http://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml [英語] に IETF の登録済みアプリケーション、コマンド コード、および属性値ペアのリストがありますが、このリストにあるすべての項目が Diameter インスペクションでサポートされているわけではありません。技術仕様については、3GPP Web サイトを参照してください。

例

次に、アプリケーション ID 3gpp-s6a と 3gpp-s13 に関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect diameter match-any log_app
ciscoasa(config-cmap)# match application-id 3gpp-s6a
ciscoasa(config-cmap)# match application-id 3gpp-s13
```

関連コマンド

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

match as-path

BGP 自律システム パス アクセス リストを照合するには、ルートマップ コンフィギュレーション モードで **match as-path** コマンドを使用します。パス 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。

match as-path *path-list-number*

no match as-path *path-list-number*

構文の説明

path-list-number	自律システム パス アクセス リストの番号。

デフォルト

パス リストは定義されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

match as-path コマンドおよび **set weight** コマンドで設定した値はグローバル値よりも優先されます。たとえば、ルート マップ コンフィギュレーションの **match as-path** コマンドおよび **set weight** コマンドで割り当てた重みは、**neighbor weight** コマンドで割り当てた重みよりも優先されます。

ルート マップは、いくつかの部分にわかれている可能性があります。**route-map** コマンドに関連付けられているどの **match** ステートメントとも一致しないルートは無視されます。したがって、そのルートは発信ルート マップ用にアドバタイズされることも、着信ルート マップ用に受け入れられることもありません。一部のデータのみを変更したい場合は、別のルートマップ セクションに明示的に match を指定する必要があります。この方法でパス リスト名を複数指定することができます。

例

次に、自律システム（AS）パスと BGP AS パス アクセス リスト as-path-acl を照合する設定の例を示します。

```
ciscoasa(config)# route-map IGP2BGP
ciscoasa(config-route-map)# match as-path 23
```

関連コマンド

コマンド	説明
set-weight	ルーティング プロトコルの BGP 重みを指定します。
neighbor-weight	ネイバー接続に重みを割り当てます。

match avp

Diameter メッセージの Diameter 属性値ペア（AVP）に関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match avp** 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。

属性のみによって AVP を照合する場合：

match [**not**] **avp** *code* [*code-2*] [**vendor-id** *id_number*]

no match [**not**] **avp** *code* [*code-2*] [**vendor-id** *id_number*]

属性の値に基づいて AVP を照合する場合：

match [**not**] **avp** *code* [**vendor-id** *id_number*] *value*

no match [**not**] **avp** *code* [**vendor-id** *id_number*] *value*

構文の説明

code	属性値ペアの名前または番号（1 ～ 4294967295）。最初のコードについては、カスタム AVP、RFC または 3GPP 技術仕様に登録されている AVP、およびソフトウェアで直接サポートされている AVP の名前を指定できます。特定の範囲の AVP を照合する場合は、2 つ目のコードを番号のみで指定します。値によって AVP を照合する場合は、2 つ目のコードを指定できません。AVP 名のリストについては、CLI ヘルプを参照してください。
value	AVP の値の部分。これは、AVP の データ タイプがサポートされている場合にのみ設定できます。たとえば、アドレス データ タイプがある AVP の IP アドレスを指定できます。このパラメータを設定する方法の詳細については、この後の「使用上のガイドライン」を参照してください。
vendor-id *id_number*	（任意）ベンダーの ID 番号（0 ～ 4294967295）も照合します。たとえば、3GPP ベンダー ID は 10415、IETF は 0。

デフォルト

Diameter インスペクションでは、すべての AVP が許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Diameter インスペクション クラス マップまたは Diameter インスペクション ポリシー マップで設定できます。このコマンドを使用すると、Diameter AVP に基づいてトラフィックをフィルタ処理できます。その後、パケットをドロップしたり、接続をドロップしたり、一致するトラフィックをログに記録したりすることができます。

AVP 名のリストについては、CLI ヘルプを参照してください。
http://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml [英語] に IETF の登録済みアプリケーション、コマンド コード、および属性値ペアのリストがありますが、このリストにあるすべての項目が Diameter インスペクションでサポートされているわけではありません。技術仕様については、3GPP Web サイトを参照してください。

値の照合を設定する場合は、サポートされているデータ タイプに固有の値オプションの構文は次のとおりです。

- Diameter アイデンティティ、Diameter URI、オクテット文字列：これらのデータ タイプの照合には正規表現または正規表現クラス オブジェクトを使用します。

  {**regex** *regex_name* | **class** *regex_class*}

- [Address]：照合する IPv4 または IPv6 アドレスを指定します。たとえば、10.100.10.10 または 2001:DB8::0DB8:800:200C:417A。
- [Time]：開始日時と終了日時を指定します。両方を指定する必要があります。時間は 24 時間形式で指定します。

  date *year month day* **time** *hh*:*mm*:*ss* **date** *year month day* **time** *hh*:*mm*:*ss*

  次に例を示します。

  date 2015 feb 5 time 12:00:00 date 2015 mar 9 time 12:00:00

- 数値：番号の範囲を指定します。

  range *number_1 number_2*

  有効な番号の範囲は、データ タイプによって異なります。

  - Integer32：-2147483647 ～ 2147483647
  - Integer64：-9223372036854775807 ～ 9223372036854775807
  - Unsigned32：0 ～ 4294967295
  - Unsigned64：0 ～ 18446744073709551615
  - Float32：8 桁の小数点表現
  - Float64：16 桁精度の小数点表記

例

次に、機能交換要求/応答コマンド メッセージで host-ip-address AVP に含まれる特定の IP アドレスに関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect diameter match-all block-ip
ciscoasa(config-cmap)# match command-code cer-cea
ciscoasa(config-cmap)# match avp host-ip-address 1.1.1.1
```

関連コマンド

コマンド	説明
class-map type inspect	インスペクション クラス マップを作成します。
diameter	カスタム属性値ペアを作成します。
inspect diameter	Diameter インスペクションを有効にします。
policy-map type inspect	インスペクション ポリシー マップを作成します。

match body

ESMTP 本文メッセージの長さまたは 1 行の長さに対して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match body** コマンドを使用します。設定されたセクションを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **body [length | line length] gt** *bytes*

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

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

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

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

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

match called-party

H.323 着信側に関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match called-party** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

regex *regex*	正規表現を照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

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

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

関連コマンド

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

match calling-party

H.323 発信側に関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match calling-party** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

regex *regex*	正規表現を照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

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

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

関連コマンド

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

match certificate

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

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

no match certificate *map-name* **[override ocsp | override cdp]**

構文の説明

map-name	このルールに一致する証明書マップの名前を指定します。一致ルールを設定する前に、証明書マップを設定する必要があります。65 文字以内で指定します。
override ocsp	ルールの目的が証明書の OCSP URL を上書きすることであることを指定します。
seq-num	この一致ルールのプライオリティを設定します。有効な範囲は 1 ～ 10000 です。ASA は、まずシーケンス番号が最も小さな一致ルールを評価し、それから順に一致が見つかるまで高い番号の一致ルールを評価していきます。
トラストポイント	(任意) トラストポイントを使用して OCSP 応答側証明書を確認することを指定します。
trustpoint-name	(オプション) レスポンダ証明書を検証するために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 URL にアクセスすることを指定します。
URL	OCSP 失効ステータスのためにアクセスする URL を識別します。
override cdp	ルールの目的が証明書の CRL URL を上書きすることであることを指定します。
index	リスト内の各 URL のランクを設定します。1 ～ 5 の値を指定します。ASA は、最初に最低ランク (1) の URL を試します。
url	CRL 失効ステータスの URL にアクセスすることを指定します。
URL	CRL 失効ステータスにアクセスする URL。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.13(1)	cdp オーバーライドを設定するためのプロビジョニングが追加されました。

使用上のガイドライン

PKI 証明書検証プロセスでは、セキュリティを維持するために、ASA によって証明書の失効ステータスがチェックされます。これには、CRL チェックまたはオンライン認証ステータス プロトコル（OCSP）のどちらかが使用されます。CRL チェックを使用すると、ASA によって、無効になった証明書がすべてリストされている CRL が取得、解析、およびキャッシュされます。OCSP は失効ステータスを確認する拡張性の高い方法であり、検証局で証明書ステータスをローカライズします。この検証局が特定の証明書のステータスを問い合わせます。

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

OCSP と同様に、**match certificate** コマンドを使用して CDP URL のオーバーライドを設定できます。このコマンドは、証明書マップを介したスタティック CDP URL の識別をサポートします。CRL 検証が必要な証明書ごとに、証明書の CDP 拡張とこの設定にマッピングされている URL に基づいて CRL が取得されます。**config-ca-crl** サブモードで **policy** コマンドを使用すると、証明書またはスタティック CDP から CDP を除外できます。

OCSP を設定するときは、次の要件に注意してください。

- 1 つのトラストポイント コンフィギュレーション内に複数の一致ルールを設定できますが、各クリプト CA 証明書マップに指定できる一致ルールは 1 つだけです。ただし、複数のクリプト CA 証明書マップを設定し、それらを同じトラストポイントに関連付けることができます。
- 一致ルールを設定する前に、証明書マップを設定する必要があります。
- 自己署名 OCSP 応答側証明書を検証するようにトラストポイントを設定するには、自己署名応答側証明書を信頼できる CA 証明書として独自のトラストポイントにインポートします。次に、自己署名 OCSP 応答側証明書が含まれているトラストポイントを使用して応答側証明書を検証するように、トラストポイントを検証するクライアント証明書の **match certificate** コマンドを設定します。同じことが、クライアント証明書の検証パスの外部にある応答側証明書の検証にも当てはまります。

- クライアント証明書と応答側証明書の両方を同じ CA が発行している場合には、1 つのトラストポイントでどちらも検証できます。しかし、クライアント証明書と応答側証明書を発行している CA が異なる場合は、トラストポイントを証明書ごとに 1 つずつ計 2 つ設定する必要があります。
- OCSP サーバ（応答側）証明書は一般に、OCSP 応答に署名します。ASA が応答を受け取ると、応答側の証明書を検証しようとします。CA は通常、自身の OCSP 応答側証明書のライフタイムを比較的短い期間に設定して、証明書が侵害される可能性を最小限に抑えます。CA は一般に、応答側証明書に ocsp-no-check 拡張を含めて、この証明書では失効ステータス チェックが必要ないことを示します。しかし、この拡張が含まれていない場合、ASA はトラストポイントに指定されているものと同じ方法で自身の失効ステータスをチェックしようとします。応答側証明書が検証可能でない場合、失効チェックは失敗します。この可能性を防ぐには、**revocation-check none** コマンドを使用して応答側の証明書を検証するトラストポイントを設定し、**revocation-check ocsp** コマンドを使用してクライアント証明書を設定します。
- ASA は、一致が見つからない場合、**ocsp url** コマンドで指定された URL を使用します。**ocsp url** コマンドが設定されていない場合、ASA はリモート ユーザ証明書の AIA フィールドを使用します。証明書に AIA 拡張がない場合、失効ステータスのチェックは失敗します。

例

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

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

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

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

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

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

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

MIIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
```

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

% Certificate successfully imported
```

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

```
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# enroll terminal
ciscoasa(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
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# revocation-check ocsp
ciscoasa(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust 4
url 10.22.184.22
```

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

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

関連コマンド

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

match certificate allow expired-certificate（廃止）

特定の証明書に対する有効期限チェックを管理者が免除できるようにするには、CA トラストプール コンフィギュレーション モードで **match certificate allow expired-certificate** コマンドを使用します。特定の証明書の免除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 certificate <map> allow expired-certificate

no match certificate <map> allow expired-certificate

構文の説明

allow	失効した証明書を受け入れます。

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

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Ca trustpool コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.13(1)	このコマンドは削除されました。

使用上のガイドライン

トラストプールの match コマンドでは、証明書マップ オブジェクトを利用して、証明書固有の例外やグローバル トラストプール ポリシーに対するオーバーライドを設定します。一致ルールは検証する証明書ごとに記述されます。

関連コマンド

コマンド	説明
match certificate skip revocation check	特定の証明書に対する失効チェックを免除します。

match certificate skip revocation-check

特定の証明書に対する失効チェックを管理者が免除できるようにするには、CA トラストプール コンフィギュレーション モードで **match certificate skip revocation-check** コマンドを使用します。失効チェックの免除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 certificate map skip revocation-check

no match certificate map skip revocation-check

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Ca trustpool コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

トラストプールの match コマンドでは、証明書マップ オブジェクトを利用して、証明書固有の例外やグローバル トラストプール ポリシーに対するオーバーライドを設定します。一致ルールは検証する証明書ごとに記述されます。

例

次に、サブジェクト DN の共通名が「mycompany123」である証明書に対する有効性チェックをスキップする例を示します。

```
crypto ca certificate map mycompany 1
subject-name attr cn eq mycompany123
crypto ca trustpool policy
match certificate mycompany skip revocation-check
```

関連コマンド

コマンド	説明
match certificate allow expired-certificate	特定の証明書に対する有効期限チェックを免除します。

match cmd

ESMTP コマンド verb に関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match cmd** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

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

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

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match command-code

Diameter メッセージの Diameter コマンド コードに関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match command-code** 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**] **command-code** *code* [*code_2*]

no match [**not**] **command-code** *code* [*code_2*]

構文の説明

code	Diameter コマンド コードの名前または番号（0 ～ 4294967295）。照合する連続番号が付されたコマンド コードの範囲がある場合は、2 番目のコードを含めることができます。コマンド コードの名前または番号別に範囲を定義でき、第 1 コードおよび第 2 コードの間のすべての番号に適用されます。コマンド コード名のリストについては、CLI ヘルプを参照してください。

デフォルト

Diameter インスペクションでは、すべてのコマンド コードが許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Diameter インスペクション クラス マップまたは Diameter インスペクション ポリシー マップで設定できます。このコマンドを使用すると、Diameter コマンド コードに基づいてトラフィックをフィルタ処理できます。その後、パケットをドロップしたり、接続をドロップしたり、一致するトラフィックをログに記録したりすることができます。

http://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml [英語] に IETF の登録済みアプリケーション、コマンド コード、および属性値ペアのリストがありますが、このリストにあるすべての項目が Diameter インスペクションでサポートされているわけではありません。技術仕様については、3GPP Web サイトを参照してください。

例

次に、機能交換要求/応答コマンド メッセージで host-ip-address AVP に含まれる特定の IP アドレスに関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect diameter match-all block-ip
ciscoasa(config-cmap)# match command-code cer-cea
ciscoasa(config-cmap)# match avp host-ip-address 1.1.1.1
```

関連コマンド

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

match community

ボーダー ゲートウェイ プロトコル(BGP)コミュニティを照合するには、ルートマップ コンフィギュレーション モードで **match community** コマンドを使用します。コンフィギュレーション ファイルから **match community** コマンドを削除し、システムをデフォルトの条件(BGP コミュニティ リスト エントリを削除)に戻すには、このコマンドの **no** 形式を使用します。

match community {*standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**]}

no match community {*standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**]}

構文の説明

standard-list-number	コミュニティの 1 つ以上の許可グループまたは拒否グループを識別する標準コミュニティ リスト番号(1 ～ 99)を指定します。
expanded-list-number	コミュニティの 1 つ以上の許可グループまたは拒否グループを識別する拡張コミュニティ リスト番号(100 ～ 500)を指定します。
community-list-name	コミュニティ リストの名前。
exact	(任意)完全一致が必要であることを示します。指定されたすべてのコミュニティのみが存在する必要があります。

デフォルト

ルート マップではコミュニティ リストの照合は行われません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

ルート マップは、いくつかの部分にわかれている可能性があります。**route-map** コマンドに関連付けられているどの **match** コマンドとも一致しないルートは無視されます。したがって、そのルートは発信ルート マップ用にアドバタイズされることも、着信ルート マップ用に受け入れられることもありません。一部のデータのみを変更したい場合は、別のルートマップ セクションに明示的に match を指定する必要があります。

コミュニティ リスト番号に基づく照合は、BGP に適用できる **match** コマンドのタイプの 1 つです。

例

次に、コミュニティ リスト 1 と一致するルートの重みが 100 に設定される例を示します。コミュニティ 109 を含むすべてのルートの重みが 100 に設定されます。

```
ciscoasa(config)#  community-list 1 permit 109
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)#  match community 1
ciscoasa(config-route-map)# set weight 100
```

次に、コミュニティ リスト 1 と一致するルートの重みを 200 に設定する例を示します。コミュニティ 109 を含むすべてのルートの重みが 200 に設定されます。

```
ciscoasa(config)#  community-list 1 permit 109
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)# match community 1 exact
ciscoasa(config-route-map)# set weight 200
```

次の例では、コミュニティ リスト LIST_NAME と一致するルートの重みが 100 に設定されます。コミュニティ 101 を含むすべてのルートの重みが 100 に設定されます。

```
ciscoasa(config)#  community-list LIST_NAME permit 101
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)# match community LIST_NAME
ciscoasa(config-route-map)# set weight 100
```

次の例は、拡張コミュニティ リスト 500 と一致するルートを示しています。拡張コミュニティ 1 のあるルートに、150 に設定されたウェイトがあります。

```
ciscoasa(config)#  community-list 500 permit [0-9]*
ciscoasa(config)# route-map MAP_NAME permit 10
ciscoasa(config-route-map)# match extcommunity 500
ciscoasa(config-route-map)# set weight 150
```

関連コマンド

コマンド	説明
set-weight	ルーティング プロトコルの BGP 重みを指定します。
community-list	BGP コミュニティ リストを作成または設定します。

match default-inspection-traffic

クラス マップに inspect コマンドのデフォルトのトラフィックを指定するには、クラス マップ コンフィギュレーション モードで **match default-inspection-traffic** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

match default-inspection-traffic

no match default-inspection-traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.6(2)	DNS over TCP インスペクション用に TCP/53 が追加されました（デフォルトではディスエーブル）。M3UA および STUN のデフォルト ポートも追加されました。

使用上のガイドライン

match コマンドは、クラス マップのトラフィック クラスに含まれているトラフィックを指定するために使用されます。これらのコマンドには、クラス マップに含まれるトラフィックを定義するさまざまな基準が含まれています。トラフィック クラスは、モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定するときに、その一環として **class-map** グローバル コンフィギュレーション コマンドを使用して定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

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

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

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

たとえば、次の例に指定されているポート 65535 は無視されます。

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

インスペクション用のデフォルトのトラフィックは、次のようになります。

インスペクション タイプ	プロトコル タイプ	送信元ポート	宛先ポート
ctiqbe	tcp	該当なし	2748
dcerpc	tcp	該当なし	135
diameter	tcp、sctp	該当なし	3868
dns	udp、tcp	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
ip-options	rsvp	該当なし	該当なし
ipsec-pass-thru	udp	該当なし	500
m3ua	sctp	該当なし	2905
mgcp	udp	2427、2727	2427、2727
netbios	udp	137 ～ 138	該当なし
radius-accounting	udp	該当なし	1646
rpc	udp	111	111
rsh	tcp	該当なし	514
rtsp	tcp	該当なし	554
sctp	sctp	any	any
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
stun	tcp、udp	該当なし	3478

tftp	udp	該当なし	69
waas	tcp	該当なし	1 ～ 65535
xdmcp	udp	177	177

例

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

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

関連コマンド

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

match dns-class

DNS Resource Record or Question セクションの Domain System Class に関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match dns-class** コマンドを使用します。設定済みのクラスを削除するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

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

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

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

例

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

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

関連コマンド

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

match dns-type

クエリー タイプや RR タイプなど DNS タイプに関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match dns-type** コマンドを使用します。設定された DNS タイプを削除するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

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

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

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

例

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

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match dns-type eq a
```

関連コマンド

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

match domain-name

DNS メッセージ ドメイン名リストに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match domain-name** コマンドを使用します。設定されたセクションを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **domain-name regex** *regex_id*

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

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

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

構文の説明

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

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

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

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

例

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

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

関連コマンド

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

match dpc

M3UA データ メッセージの宛先ポイント コード(DPC)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 dpc** 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**] **dpc** *code*

no match [**not**] **dpc** *code*

構文の説明

code	*zone-region-sp* 形式の宛先ポイント コード。

デフォルト

M3UA インスペクションでは、すべての宛先ポイント コードが許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
ポリシー マップ設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは M3UA インスペクション ポリシー マップで設定できます。宛先ポイント コードに基づいてパケットをドロップできます。ポイント コードは *zone-region-sp* 形式で、各要素に使用できる値は SS7 バリアントによって異なります。バリアントは ポリシー マップの **ss7 variant** コマンドで定義できます。

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

例

次に、ITU の特定の宛先ポイント コードに関して一致条件を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match dpc 1-5-1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インスペクションをイネーブルにします。
match opc	M3UA 発信ポイント コードと一致させます。
policy-map type inspect	インスペクション ポリシー マップを作成します。
ss7 variant	ポリシー マップで使用する SS7 バリアントを指定します。

match dscp

クラス マップの（IP ヘッダーの）IETF-defined DSCP 値を識別するには、クラス マップ コンフィギュレーション モードで **match dscp** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

match dscp {*values*}

no match dscp {*values*}

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

match コマンドは、クラス マップのトラフィック クラスに含まれているトラフィックを指定するために使用されます。これらのコマンドには、クラス マップに含まれるトラフィックを定義するさまざまな基準が含まれています。トラフィック クラスは、モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定するときに、その一環として **class-map** グローバル コンフィギュレーション コマンドを使用して定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

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

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

例

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

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match dscp af43 cs1 ef
ciscoasa(config-cmap)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを指定します。
match port	TCP/UDP ポートをそのインターフェイスで受信したパケットに対する比較基準として指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。