CHAPTER 6

M ～ R のコマンド

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

コマンドのモード

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
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-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。

コマンドのモード

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
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。

コマンドのモード

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
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。

コマンドのモード

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
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 ベースの認証で使用する 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 アドレスのリストの使用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-list** コマンドは、先頭一致検索を使用して MAC アドレスのリストを追加します。

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	この基準と一致するトラフィックが MAC リストに含まれず、認証と認可の両方の対象となることを示します。
id	16 進数 の MAC アクセスリストの番号を指定します。
mac	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	ネットマスクを *mac* に指定および適用し、MAC アドレスのグループ化を許可します。
permit	この基準と一致するトラフィックが MAC リストに含まれ、認証と認可の両方の対象から除外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。

コマンドのモード

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
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。**mac-list** コマンドを使用して MAC アクセスリストの番号を設定してから、**aaa mac-exempt** コマンドを使用します。

AAA 免除だけが提供されます。認証が免除される MAC アドレスは、自動的に認可が免除されます。**mac-list** で他のタイプの AAA はサポートされていません。

例

次の例は、MAC アドレス リストを設定する方法を示しています。

```
hostname(config)# mac-list adc permit 00a0.cp5d.0282 ffff.ffff.ffff
hostname(config)# mac-list adc deny 00a1.cp5d.0282 ffff.ffff.ffff
hostname(config)# mac-list ac permit 0050.54ff.0000 ffff.ffff.0000
hostname(config)# mac-list ac deny 0061.54ff.b440 ffff.ffff.ffff
hostname(config)# mac-list ac deny 0072.54ff.b440 ffff.ffff.ffff
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定されたサーバ上での、LOCAL、TACACS+、または RADIUS のユーザ認証、または ASDM ユーザ認証をイネーブル化、ディセーブル化、または表示します。
aaa authorization	LOCAL または TACACS+ ユーザ認可サービスをイネーブルまたはディセーブルにします。
aaa mac-exempt	MAC アドレスのリストを認証と認可の対象から除外します。
clear configure mac-list	**mac-list** コマンドですでに指定した MAC アドレスのリストを、表示された MAC リストの番号とともに削除します。
show running-config mac-list	**mac-list** コマンドですでに指定した MAC アドレスのリストを、表示された MAC リストの番号とともに表示します。

management-access

セキュリティ アプライアンスの内部管理インターフェイスへのアクセス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 ***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	内部管理インターフェイスの名前。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

management-access コマンドを使用すると、*mgmt_if* で指定したファイアウォール インターフェイスの IP アドレスを使用して、内部管理インターフェイスを定義できます（インターフェイス名は **nameif** コマンドによって定義され、**show interface** コマンドの出力で引用符 " " に囲まれて表示されます）。

management-access コマンドは IPSec VPN トンネルを経由する場合だけ、次の内容をサポートします。また、1 つの管理インターフェイスだけをグローバルに定義できます。

- *mgmt_if* への SNMP ポーリング
- *mgmt_if* への HTTPS 要求
- *mgmt_if* への ASDM アクセス
- *mgmt_if* への Telnet アクセス
- *mgmt_if* への SSH アクセス
- *mgmt_if* への ping
- *mgmt_if* への syslog ポーリング
- *mgmt_if* への NTP 要求

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 5500 シリーズ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。

コマンドのモード　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
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 適応型セキュリティ アプライアンスには、Management 0/0 と呼ばれる専用の管理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。

（注）　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のみがトラフィックを通過させることができます。ただし、ASA 適応型セキュリティ アプライアンスでは、専用の管理インターフェイス（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。

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。

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。

コマンドのモード

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
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** コマンドに応答するサーバは一連の X 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 コマンドに応答する FTP サーバを X に置き換えます。

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

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。
functions	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

アクセスリストを使用してクラスマップ内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 access-list** コマンドを使用します。アクセスリストを削除するには、このコマンドの **no** 形式を使用します。

match access-list {*acl-id...}*

no match access-list {*acl-id...}*

シンタックスの説明

acl-id	一致基準として使用する ACL の名前を指定します。パケットが ACL のエントリに一致しない場合、照合の結果は no-match となります。パケットが ACL のエントリに一致し、許可エントリである場合、照合の結果は match となります。それ以外では、パケットが拒否 ACL エントリに一致する場合、照合の結果は no-match となります。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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 access-list コマンドでは、1 つまたは複数のアクセスリストを指定して特定のトラフィック タイプを指定できます。アクセス コントロール エントリの **permit** 文はトラフィックを包含し、**deny** 文はトラフィック クラスマップからトラフィックを除外します。

例

次の例は、クラスマップおよび **match access-list** 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)# access-list ftp_acl extended permit tcp any any eq 21
hostname(config)# class-map ftp_port
hostname(config-cmap)# match access-list ftp_acl
```

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	トラフィック マップの定義を削除します。
match any	クラスマップ内の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

クラスマップ内のすべてのトラフィックを含めるには、クラスマップ コンフィギュレーション モードで **match any** 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 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。

コマンドのモード

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
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。

デフォルトのクラスマップ（class-default）で **match any** コマンドを使用すると、すべてのパケットが一致します。

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	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 rtp	クラスマップ内の特定の RTP 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 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。

コマンドのモード

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
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
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
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
```

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	クラスマップ内の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 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。

コマンドのモード

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
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
```

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 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。

コマンドのモード　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
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
```

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 interface

指定したいずれかのインターフェイスの外部にネクストホップを持つ、すべてのルートを配布するには、ルートマップ コンフィギュレーション モードで **match interface** コマンドを使用します。一致インターフェイス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。

match interface *interface-name...*

no match interface *interface-name...*

シンタックスの説明

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

デフォルト

一致インターフェイスは定義されていません。

コマンドのモード

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
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 interface-type interface-number 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指定できます。**set** コマンドで指定した設定アクションに従ってルート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。**match** コマンドで指定したインターフェイスが複数ある場合、**no match interface** *interface-name* を使用して 1 つのインターフェイスを削除できます。

ルートマップは、いくつかの部分に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、外部にネクストホップ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 interface outside
```

関連コマンド

コマンド	説明
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 ip route-source	ルータによってアドバタイジングされ、アクセスリスト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 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。

コマンドのモード

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
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。

コマンドのモード

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
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。

コマンドのモード

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
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 metric

指定したメトリックを持つルートを再配布するには、ルートマップ コンフィギュレーション モードで **match metric** コマンドを使用します。エントリを削除するには、このコマンドの **no** 形式を使用します。

match metric *number*

no match metric *number*

シンタックスの説明

number	ルート メトリック（5 つの部分からなる IGRP のメトリックにすることができます）。有効値は 0 ～ 4294967295 です。

デフォルト

メトリック値では、フィルタリングは実行されません。

コマンドのモード

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
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指定できます。また、**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。

例

次の例は、メトリック 5 を持つ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 metric 5
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクストホップを持つ、すべてのルートを再配布します。
match ip next-hop	指定した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。
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 port

クラスマップ内の特定のポート番号を指定するには、クラスマップ コンフィギュレーション モードで **match port** 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 port {**tcp** | **udp**} {**eq** *eq_id* | **range** *beg_id end_id*}

no match port {**tcp** | **udp**} {**eq** *eq_id* | **range** *beg_id end_id*}

シンタックスの説明

eq *eq_id*	ポート名を指定します。
range *beg_id end_id*	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。

コマンドのモード

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
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。

ポートの範囲を指定するには、**match port** 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 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	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	クラスマップ内のすべてのトラフィックを含めます。
show running-config class-map	クラスマップ コンフィギュレーションに関する情報を表示します。

match precedence

クラスマップ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。

コマンドのモード

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
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
```

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	クラスマップ内の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 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。

コマンドのモード

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
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。

コマンドのモード

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
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
```

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	クラスマップ内の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 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。

コマンドのモード

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
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。

max-failed-attempts

サーバ グループ内の所定のサーバが無効になるまでに、許可される失敗数を指定するには、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。

コマンドのモード

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
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
```

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-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。

コマンドのモード

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
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)# exit
```

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-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。

コマンドのモード

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
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)# exit
```

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。

コマンドのモード

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
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
```

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用に特定の 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 タイプを銅製またはファイバ 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 タイプを銅製 RJ-45 コネクタに設定します。
sfp	メディア タイプをファイバ SFP コネクタに設定します。

デフォルト

デフォルトは **rj45** です。

コマンドのモード

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
7.0(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。

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（発信者 PC）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。

コマンドのモード

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
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

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*** コマンドの出力を示しています。

```
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 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。

コマンドのモード

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
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

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 ブロックの終了テキスト範囲を指定します。
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 ブロックの開始テキスト範囲を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

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クリアします。
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。

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。このモードは、**gtp-map** コマンドを使用してアクセスします。このコマンドを削除するには、**no** 形式を使用します。

message-length *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。

コマンドのモード

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
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）を合わせたものです。

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
```

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用に特定の 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。

mgcp-map

MGCP 検査のパラメータを定義するときに使用する、特定のマップを指定するには、グローバル コンフィギュレーション モードで **mgcp-map** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

mgcp-map *map_name*

no mgcp-map *map_name*

シンタックスの説明

map_name	MGCP マップの名前。最大文字数は 64 です。

デフォルト

MGCP コマンド キューのデフォルトは 200 です。

コマンドのモード

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
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

MGCP 検査のパラメータを定義するときに使用する、特定のマップを指定するには、**mgcp-map** コマンドを使用します。このコマンドを入力すると、システムがコンフィギュレーション モードに入って、個々のマップを定義するためのさまざまなコマンドを入力できるようになります。MGCP マップを定義したら、**inspect mgcp** コマンドを使用してマップをイネーブルにします。モジュラ ポリシー フレームワークを使用して、定義したトラフィック クラスに **inspect** コマンドを適用し、特定のインターフェイスにポリシーを適用します。MGCP マップ コンフィギュレーション モードで使用できるコマンドは、次のとおりです。

- **call-agent**：コール エージェントのグループを指定します。
- **command-queue**：キューに入れることができる MGCP コマンドの最大数を指定します。
- **gateway**：特定のゲートウェイを管理しているコール エージェントのグループを指定します。
- **no**：コマンドを否定するか、パラメータをデフォルト値に設定します。

例

次の例は、**mgcp-map** コマンドを使用して、MGCP 検査のパラメータを定義するときに使用する特定のマップ（mgcp-policy）を指定する方法を示しています。

```
hostname(config)# mgcp-map mgcp-policy
hostname(config-mgcp-policy)#
```

次の例は、MGCP トラフィックを識別し、MGCP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

次の例のように、MGCP 検査エンジンをイネーブルにします。ここでは、デフォルトのポート（2427）の MGCP トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map mgcp-port
hostname(config-cmap)# match port tcp eq 2427
hostname(config-cmap)# exit
hostname(config)# mgcp-map mgcp_inbound
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
hostname(config-mgcp-map)# command-queue 150
hostname(config)# policy-map mgcp_policy
hostname(config)# mgcp-map mgcp_
hostname(config-pmap)# class mgcp-port
hostname(config-pmap-c)# inspect mgcp mgcp_inbound
hostname(config-pmap-c)# exit
hostname(config)# service-policy mgcp_policy interface outside
```

ここでは、コール エージェント 10.10.11.5 と 10.10.11.6 がゲートウェイ 10.10.10.115 を制御できるようにし、コール エージェント 10.10.11.7 と 10.10.11.8 がゲートウェイ 10.10.10.116 と 10.10.10.117 の両方を制御できるようにしています。キューに入れることができる MGCP コマンドの最大数は、150 です。

すべてのインターフェイスの MGCP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
debug mgcp	MGCP に関するデバッグ情報の表示をイネーブルにします。
show mgcp	MGCP のコンフィギュレーションおよびセッション情報を表示します。
timeout mgcp	MGCP メディア接続のアイドル タイムアウトを設定します。このタイムアウト後、その MGCP メディア接続が終了します。
timeout mgcp-pat	MGCP PAT xlate のアイドル タイムアウトを設定します。このタイムアウト後、その MGCP PAT xlate が削除されます。

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）内部フラッシュ メモリを指定し、続けてコロン（:）を入力します。
disk1:	（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）内部フラッシュ メモリを指定し、続けてコロン（:）を入力します。ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。
path	作成するディレクトリの名前とパス。

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。

コマンドのモード

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
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

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。

コマンドのモード

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
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（内部フラッシュ 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（内部フラッシュ 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。

コマンドのモード

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
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
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）。

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）内部フラッシュ 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）内部フラッシュ メモリを指定し、続けてコロン（:）を入力します。ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。
ftp:	（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

コマンドのモード

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
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*] [*distance*]

no mroute *src smask in_if_name* [***dense*** *output_if_name*] [*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。
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。

コマンドのモード

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
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。

mtu

インターフェイスの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。

コマンドのモード

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
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。ただし、その場合は「don't fragment」（DF）ビットが設定されます。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（maximum transmission unit; MTU）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-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。

コマンドのモード

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
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 6-1 は、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ています。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 6-1　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。

name

名前を IP アドレスに関連付けするには、グローバル コンフィギュレーション モードで **name** コマンドを使用します。コンフィギュレーションから名前を削除することなく、テキスト名の使用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。

name *ip_address name*

no name *ip_address* **[***name***]**

シンタックスの説明

ip_address	名前を付けるホストの IP アドレスを指定します。
name	IP アドレスに割り当てられる名前を指定します。a ～ z、A ～ Z、0 ～ 9、ダッシュ、およびアンダースコアの文字を使用します。*name* は、63 文字以下にする必要があります。また、*name* の先頭は数字にすることはできません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

IP アドレスとの名前の関連付けをイネーブルにするには、***names*** コマンドを使用します。IP アドレスに関連付けることができるのは、1 つの名前だけです。

まず **names** コマンドを使用してから、**name** コマンドを使用する必要があります。**name** コマンドは、**names** コマンドの直後、かつ **write memory** コマンドの前に使用してください。

name コマンドを使用すると、ホストをテキスト名で識別し、テキスト文字列を IP アドレスにマッピングできます。**no name** コマンドを使用すると、テキスト名を使用できないようにできますが、コンフィギュレーションから名前は削除しません。名前のリストをコンフィギュレーションから消去するには、***clear configure name*** コマンドを使用します。

name 値の表示をディセーブルにするには、**no names** コマンドを使用します。

name コマンドと **names** コマンドは、両方ともコンフィギュレーションに保存されます。

name コマンドでは、ネットワーク マスクに名前を割り当てることはサポートされていません。たとえば、次のコマンドは拒否されます。

```
hostname(config)# name 255.255.255.0 class-C-mask
```

（注） マスクを必要とするどのコマンドも、受け入れたネットワーク　マスクとして名前を処理できません。

例

次の例は、**names** コマンドによって、**name** コマンドの使用をイネーブルにする方法を示しています。**name** コマンドは、192.168.42.3 への参照の代わりに **sa_inside** を使用し、209.165.201.3 の代わりに **sa_outside** を使用できるようにします。IP アドレスをネットワーク インターフェイスに割り当てる際に、**ip address** コマンドでこれらの名前を使用できます。**no names** コマンドは、**name** コマンド値の表示をディセーブルにします。その後で **names** コマンドを再度使用すると、**name** コマンド値の表示が元に戻ります。

```
hostname(config)# names
hostname(config)# name 192.168.42.3 sa_inside
hostname(config)# name 209.165.201.3 sa_outside

hostname(config-if)# ip address inside sa_inside 255.255.255.0
hostname(config-if)# ip address outside sa_outside 255.255.255.224

hostname(config)# show ip address
System IP Addresses:
    inside ip address sa_inside mask 255.255.255.0
    outside ip address sa_outside mask 255.255.255.224

hostname(config)# no names
hostname(config)# show ip address
System IP Addresses:
    inside ip address 192.168.42.3 mask 255.255.255.0
    outside ip address 209.165.201.3 mask 255.255.255.224

hostname(config)# names
hostname(config)# show ip address
System IP Addresses:
    inside ip address sa_inside mask 255.255.255.0
    outside ip address sa_outside mask 255.255.255.224
```

関連コマンド

コマンド	説明
clear configure name	名前のリストをコンフィギュレーションから消去します。
names	IP アドレスとの名前の関連付けをイネーブルにします。
show running-config name	IP アドレスに関連付けられた名前を表示します。

nameif

インターフェイスの名前を付けるには、インターフェイス コンフィギュレーション モードで **nameif** コマンドを使用します。名前を削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスのすべてのコンフィギュレーション コマンドで、インターフェイス タイプと ID（gigabitethernet0/1 など）ではなくインターフェイス名が使用されるので、トラフィックがインターフェイスを通過できるようにするにはインターフェイス名が必要です。

nameif *name*

no nameif

シンタックスの説明

name	最大 48 文字の名前を設定します。名前は大文字と小文字の区別がありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
7.0(1)	このコマンドが、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モードのコマンドに変更されました。

使用上のガイドライン

サブインターフェイスの場合、**vlan** コマンドを使用して VLAN を割り当ててから、**nameif** コマンドを入力する必要があります。

新しい値でこのコマンドを再入力することによって、名前を変更できます。**no** 形式のコマンドは入力しないでください。このコマンドを入力すると、該当する名前を指しているすべてのコマンドが削除されます。

例

次の例では、2 つのインターフェイスの名前を「inside」と「outside」に設定します。

```
hostname(config)# interface gigabitethernet0/1
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
hostname(config-if)# interface gigabitethernet0/0
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear xlate	既存の接続に関するすべての変換をリセットして、接続をリセットします。
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。
security-level	インターフェイスのセキュリティ レベルを設定します。
vlan	サブインターフェイスに VLAN ID を割り当てます。

names

name コマンドで設定可能な、IP アドレスから名前への変換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 **names** コマンドを使用します。アドレスから名前への変換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。

names

no names

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。

コマンドのモード　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
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　***name*** コマンドで設定した IP アドレスとの名前の関連付けをイネーブルにするには、**names** コマンドを使用します。**name** または **names** コマンドを入力する順番は、重要ではありません。

例　次の例は、名前と IP アドレスとの関連付けをイネーブルにする方法を示してします。

```
hostname(config)# names
```

関連コマンド

コマンド	説明
clear configure name	名前のリストをコンフィギュレーションから消去します。
name	名前を IP アドレスに関連付けます。
show running-config name	IP アドレスに関連付けられている名前のリストを表示します。
show running-config names	IP アドレスから名前への変換を表示します。

name-separator

電子メール、VPN ユーザ名、およびパスワード間のデリミタとして文字を指定するには、該当する電子メール プロキシ モードで **name-separator** コマンドを使用します。デフォルトの「:」に戻すには、このコマンドの **no** バージョンを使用します。

name-separator [*symbol*]

no name-separator

シンタックスの説明

symbol	（オプション）電子メール、VPN ユーザ名、およびパスワード間を区切る文字。使用できるのは、アットマーク（@）、パイプ（|）、コロン（:）、番号記号（#）、カンマ（,）、およびセミコロン（;）です。

デフォルト

デフォルトは、「:」（コロン）です。

コマンドのモード

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
Pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更
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

名前セパレータには、サーバ セパレータと異なるものを指定する必要があります。

例

次の例は、POP3S の名前セパレータとしてハッシュ（#）を設定する方法を示しています。

```
hostname(config)# pop3s
hostname(config-pop3s)# name-separator #
```

関連コマンド

コマンド	説明
server-separator	電子メールとサーバ名を区切ります。

nat

別のインターフェイスのマッピング アドレスに変換される、1 つのインターフェイスのアドレスを指定するには、グローバル コンフィギュレーション モードで **nat** コマンドを使用します。このコマンドは、ダイナミック NAT または PAT を設定します。ダイナミック NAT または PAT では、アドレスをマッピング アドレスのいずれかのプールに変換します。**nat** 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。

標準ダイナミック NAT の場合：

nat (*real_ifc) nat_id real_ip* [*mask* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*] [**norandomseq**]]] [**udp** *udp_max_conns*]

no nat (*real_ifc) nat_id real_ip* [*mask* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*] [**norandomseq**]]] [**udp** *udp_max_conns*]

ポリシー ダイナミック NAT と NAT 除外の場合：

nat (*real_ifc) nat_id* **access-list** *access_list_name* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*] [**norandomseq**]]] [**udp** *udp_max_conns*]

no nat (*real_ifc) nat_id* **access-list** *access_list_name* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*] [**norandomseq**]]] [**udp** *udp_max_conns*]

シンタックスの説明

access-list *access_list_name*	拡張アクセスリスト（別名、ポリシー NAT）を使用して、ローカル アドレスと宛先アドレスを指定します。**access-list** コマンドを使用してアクセスリストを作成します。このアクセスリストには、許可アクセス コントロール エントリだけが含まれている必要があります。***eq*** 演算子を使用して、アクセスリストにローカル ポートと宛先ポートをオプションで指定できます。NAT ID が **0** の場合、アクセスリストは NAT から除外されたアドレスを指定します。NAT 除外はポリシー NAT とは異なります。たとえば、ポート アドレスを指定できません。 **（注）** アクセスリストのヒット カウント（**show access-list** コマンドを参照）は、NAT 除外アクセスリストの場合は増分されません。
dns	（オプション）このコマンドに一致する DNS 応答で、A レコード（アドレス レコード）を書き直します。マッピングされているインターフェイスから実際のインターフェイスに移動する DNS 応答では、A レコードが、マッピングされた値から実際の値に書き直されます。逆に、実際のインターフェイスからマッピングされているインターフェイスに移動する DNS 応答では、A レコードが、実際の値からマッピングされた値に書き直されます。 DNS サーバにエントリがあるホストのアドレスが NAT 文に含まれ、クライアントとは異なるインターフェイスに DNS サーバがある場合、クライアントと DNS サーバに必要なホスト アドレスはそれぞれ異なります。一方にはグローバル アドレスが必要で、もう一方にはローカル アドレスが必要です。変換対象のホストは、クライアントまたは DNS サーバのどちらかと同じインターフェイス上になければなりません。通常、他のインターフェイスからのアクセスを許可する必要があるホストがスタティック トランスレーションを使用するので、このオプションは **static** コマンドと併せて使用するのが一般的です。

emb_limit	（オプション）ホストごとの初期接続の最大数を指定します。デフォルトは 0 で、初期接続に制限がないことを意味します。 初期接続の数を制限することで、DoS 攻撃から保護されます。セキュリティ アプライアンスでは、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。 このオプションは、外部 NAT には適用されません。TCP 代行受信機能が適用されるのは、よりセキュリティ レベルの高いホストまたはサーバのみです。外部 NAT に対して初期接続の制限を設定しても、その初期接続制限は無視されます。
real_ifc	実際の IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
real_ip	変換の対象となる実際のアドレスを指定します。**0.0.0.0**（または短縮形の **0**）を使用すると、すべてのアドレスを指定できます。
mask	（オプション）実際のアドレスのサブネット マスクを指定します。マスクを入力しない場合、IP アドレス クラスのデフォルト マスクが使用されます。
nat_id	NAT ID の整数を指定します。標準 NAT の場合、この整数は 1 ～ 2147483647 です。ポリシー NAT（nat id access-list）の場合、この整数は 1 ～ 65535 です。 アイデンティティ NAT（**nat 0**）と NAT 除外（**nat 0 access-list**）は、**0** の NAT ID を使用します。 **global** コマンドはこの ID を参照して、グローバル プールを *real_ip* に関連付けます。
norandomseq	（オプション）TCP ISN のランダム化保護をディセーブルにします。TCP シーケンスのランダム化をディセーブルにするのは、別のインライン ファイアウォールもシーケンス番号をランダム化していて、結果としてデータ順序が変わる場合だけにします。各 TCP 接続には、2 つの ISN があります。1 つはクライアントが生成し、1 つはサーバが生成します。セキュリティ アプライアンスは、ホストとサーバが生成する ISN をランダム化します。少なくとも 1 つの ISN をランダムに生成して、攻撃者が次の ISN を予想してセッションを乗っ取ることができないようにする必要があります。 **norandomseq** キーワードは外部 NAT に適用されません。ファイアウォールは、セキュリティの高いインターフェイスのホスト / サーバが生成する ISN だけをランダム化します。外部 NAT に対して **norandomseq** を設定しても、**norandomseq** キーワードは無視されます。
outside	（オプション）このインターフェイスのセキュリティ レベルが、**global** 文の一致で特定するインターフェイスより低い場合、outside を入力する必要があります。この機能は、外部 NAT または双方向 NAT と呼ばれます。

tcp *tcp_max_conns*	サブネット全体に関して、同時 TCP 接続と UDP 接続の最大数を指定します。デフォルトは 0 です。接続数の制限がないことを意味します（アイドル接続は、**timeout conn** コマンドで指定したアイドル タイムアウトの経過後に閉じられます）。 このオプションは、外部 NAT には適用されません。セキュリティ アプライアンスが追跡するのは、セキュリティの高いインターフェイスからセキュリティの低いインターフェイスに向かう接続のみです。
udp *udp_max_conns*	（オプション）**udp** キーワードとともに使用して、*real_ip* ホストがそれぞれ使用できる同時 UDP 接続の最大数を設定します。

デフォルト

tcp_max_conns、*emb_limit*、および *udp_max_conns* のデフォルト値は 0（無制限）です。この値は、最大使用可能値です。

コマンドのモード

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
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

ダイナミック NAT と PAT の場合、最初に **nat** コマンドを設定し、変換する所定のインターフェイスの実際のアドレスを指定します。次に、別の **global** コマンドを設定して、別のインターフェイスから出るときのマッピング アドレスを指定します（PAT の場合、このアドレスは 1 つです）。各 **nat** コマンドは、各コマンドに割り当てた番号である NAT ID を比較することによって、**global** コマンドとマッチングを行います。

セキュリティ アプライアンスは、NAT 規則がトラフィックに一致する場合に、アドレスを変換します。NAT 規則が一致しない場合、パケットの処理が続行します。例外は、**nat-control** コマンドを使用して NAT コントロールをイネーブルにする場合です。NAT コントロールでは、セキュリティの高いインターフェイス（内部）からセキュリティの低いインターフェイス（外部）に移動するパケットが NAT 規則に一致する必要があります。一致していないと、パケットの処理が停止します。NAT コントロールをイネーブルにした場合でも、NAT は同一セキュリティ レベルのインターフェイスでは必要ありません。必要に応じて、オプションで NAT を設定できます。

ダイナミック NAT は、宛先ネットワークでルーティング可能なマッピング アドレスのプールに実際のアドレスのグループを変換します。マッピング プールは、実際のグループより少ないアドレスで構成されます。変換するホストが宛先ネットワークにアクセスするときに、セキュリティ アプライアンスがマッピング プールの IP アドレスをホストに割り当てます。実際のホストが接続を開始する場合にのみ、変換が追加されます。変換が有効なのは接続されている間だけなので、所定のユーザが変換のタイムアウト後も同じ IP アドレスを維持することはありません（**timeout xlate** コマンドを参照）。そのため、アクセスリストによって接続が許可されている場合でも、ダイナミック NAT（または PAT）を使用するホストに、宛先ネットワーク上のユーザから確実に接続を開始できません。また、実際のホスト アドレスに直接接続しようとすると、セキュリティ アプライアンスが拒否します。ホストへの確実なアクセスについては、**static** コマンドを参照してください。

ダイナミック NAT には、次の短所があります。

- マッピング プール内のアドレスが実際のグループより少ない場合、トラフィック量が予想を超えるとアドレスが不足する可能性があります。

  PAT は単一アドレスのポートを使用して 64,000 を超える変換を実行できるので、この現象が頻繁に発生する場合は、PAT を使用してください。
- マッピング　プールで大量のルーティング可能なアドレスを使用しなければなりません。インターネットなどの登録アドレスが宛先ネットワークに必要な場合は、使用可能なアドレスが不足する可能性があります。

ダイナミック NAT の利点は、一部のプロトコルが PAT を使用できないということです。たとえば、GRE バージョン 0 のように、オーバーロードするポートを持たない IP プロトコルでは、PAT は動作しません。一部のマルチメディア アプリケーションのように、あるポートでデータ ストリームを流して別のポートで制御パスを提供するオープンスタンダードではない一部のアプリケーションでも、PAT は動作しません。

PAT では、複数の実際のアドレスを 1 つのマッピング IP アドレスに変換します。具体的には、セキュリティ アプライアンスが実際のアドレスと送信元ポート（実際のソケット）をマッピング アドレスと 1024 以上の一意なポート（マッピング ソケット）に変換します。送信元ポートはそれぞれの接続で異なるので、各接続には別個の変換が必要になります。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは異なる変換が必要です。

接続の期限が切れると、ポートの変換も 30 秒の非アクティビティの後、期限切れになります。タイムアウトは、設定できません。

PAT で使用できるマッピング アドレスは 1 つなので、ルーティング可能なアドレスの節約になります。セキュリティ アプライアンスのインターフェイス IP アドレスを PAT アドレスとして使用することもできます。PAT は、データ ストリームが制御パスと異なる一部のマルチメディア アプリケーションでは動作しません。

（注） 変換中であれば、リモート　ホストは、アクセスリストで許可されているかぎり変換対象のホストへの接続を開始できます。アドレスは（実際のアドレスとマッピング アドレスの両方とも）予測不能なので、ホストに接続できる可能性は非常に少なくなります。万一、接続が成功した場合は、アクセスリストのセキュリティに頼ることができます。

NAT コントロールをイネーブルにする場合、内部ホストは、外部ホストにアクセスするときに NAT 規則に一致する必要があります。一部のホストで NAT を実行しない場合は、それらのホストで NAT をバイパスできます（または、NAT コントロールをディセーブルにできます）。たとえば、NAT をサポートしていないアプリケーションを使用する場合に、NAT をバイパスすることになる可能性があります。**static** コマンドを使用して NAT をバイパスするか、次のいずれかのオプションを使用できます。

- アイデンティティ NAT（**nat 0** コマンド）：アイデンティティ NAT（ダイナミック NAT と類似）を設定する場合、特定のインターフェイスのホストの変換を制限しません。すべてのインターフェイスを通過する接続に、アイデンティティ NAT を使用する必要があります。そのため、インターフェイス A にアクセスするときに、実際のアドレスで標準変換を実行し、インターフェイス B にアクセスするときに、アイデンティティ NAT を使用するといった選択はできません。これに対して、標準ダイナミック NAT を使用した場合は、アドレスを変換する特定のインターフェイスを指定できます。アクセスリストに基づいて使用可能なすべてのネットワーク上で、アイデンティティ NAT を使用する実際のアドレスがルーティング可能でなければなりません。

  アイデンティティ NAT の場合、マッピング アドレスが実際のアドレスと同じでも、（アクセスリストで許可されている場合を含めて）外部から内部へ接続を開始することはできません。この機能では、スタティック アイデンティティ NAT または NAT 除外を使用してください。

- NAT 除外（**nat 0 access-list** コマンド）：NAT 除外を使用すると、変換対象のホストとリモートホストの両方で接続を開始できます。アイデンティティ NAT と同様、特定のインターフェイスのホストに対する変換を制限しないでください。すべてのインターフェイスを通過する接続に NAT 除外を使用する必要があります。ただし、NAT 除外では、変換する実際のアドレスを決定するときに（ポリシー NAT と同様）、実際のアドレスと宛先アドレスを指定できるので、NAT 除外を使用すると詳細な制御が可能になります。一方、ポリシー NAT と異なり、NAT 除外ではアクセスリストのポートは考慮されません。

ポリシー NAT では、拡張アクセスリストで送信元アドレスと宛先アドレスを指定することによって、アドレス変換対象の実際のアドレスを指定できます。オプションで、送信元ポートと宛先ポートも指定できます。標準 NAT で考慮されるのは、実際のアドレスだけです。たとえば、実際のアドレスがサーバ A にアクセスするときはマッピング アドレス A に変換できますが、サーバ B にアクセスするときにはマッピング アドレス B に変換できます。

セカンダリ チャネルのアプリケーション検査を必要とするアプリケーション（FTP、VoIP など）に対してポリシー NAT のポートを指定すると、セキュリティ アプライアンスは自動的にセカンダリ ポートを変換します。

（注） NAT 除外を除くすべてのタイプの NAT がポリシー NAT をサポートしています。NAT 除外では、アクセスリストを使用して実際のアドレスを指定しますが、ポートが考慮されない点がポリシー NAT と異なります。ポリシー NAT をサポートしない**スタティック** アイデンティティ NAT を使用すると、NAT 除外と同じ結果を得られます。

別の方法として、**set connection** コマンドを使用して、最大接続数、最大初期接続数、および TCP シーケンス ランダム化を設定できます。同じトラフィックに対して両方の方法でこれらの設定値を設定した場合、セキュリティ アプライアンスは小さい方の制限値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルにされている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

NAT コンフィギュレーションを変更し、新しい NAT 情報が使用される前の、既存の変換のタイムアウトを待機しない場合、**clear xlate** コマンドを使用して、変換テーブルを消去できます。ただし、変換テーブルを消去すると現在の接続がすべて切断されます。

例

たとえば、内部インターフェイス上の 10.1.1.0/24 ネットワークを変換するには、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.1-209.165.201.30
```

ダイナミック NAT 用のアドレス プールを、NAT プールを使い果たしたときのための PAT アドレスとともに指定するには、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.5
hostname(config)# global (outside) 1 209.165.201.10-209.165.201.20
```

ルーティングの簡略化などのために、セキュリティの低い DMZ（非武装地帯）のネットワーク アドレスを変換して内部ネットワーク（10.1.1.0）と同じネットワーク上に表示するには、次のコマンドを入力します。

```
hostname(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
hostname(config)# global (inside) 1 10.1.1.45
```

ポリシー NAT を使用して、1 つの実際のアドレスに 2 つの異なる宛先アドレスを指定するには、次のコマンドを入力します。

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 1 access-list NET1 tcp 0 2000 udp 10000
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list NET2 tcp 1000 500 udp 2000
hostname(config)# global (outside) 2 209.165.202.130
```

ポリシー NAT を使用して、それぞれが異なるポートを使用する、1 つの実際のアドレスと宛先アドレスのペアを指定するには、次のコマンドを入力します。

```
hostname(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 80
hostname(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 23
hostname(config)# nat (inside) 1 access-list WEB
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list TELNET
hostname(config)# global (outside) 2 209.165.202.130
```

関連コマンド

コマンド	説明
access-list deny-flow-max	作成できる同時拒否フローの最大数を指定します。
clear configure nat	NAT コンフィギュレーションを削除します。
global	グローバル アドレス プールに対してエントリを作成します。
interface	インターフェイスを作成および設定します。
show running-config nat	ネットワークに関連付けられているグローバル IP アドレスのプールを表示します。

nat (vpn load-balancing)

この装置の IP アドレスが NAT で変換される先の IP アドレスを設定するには、VPN ロードバランシング モードで **nat** コマンドを使用します。この NAT 変換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。

nat *ip-address*

no nat [***ip-adddress***]

シンタックスの説明

ip-address	この NAT で、この装置の IP アドレスを変換する先の IP 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。

コマンドのモード

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
VPN ロードバランシング	•	—	•	—	—

コマンド履歴

リリース	変更
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

まず、**vpn load-balancing** コマンドを使用して、VPN ロードバランシング モードに入る必要があります。

このコマンドの **no nat** 形式では、オプションの *ip-address* 値を指定する場合、IP アドレスが実行コンフィギュレーションの既存の NAT IP アドレスに一致する必要があります。

例

次は、VPN ロードバランシング コマンド シーケンスの例です。NAT 変換のアドレスを 192.168.10.10 に設定する **nat** コマンドが含まれます。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシング モードに入ります。

nat-control

NAT コントロールを強制するには、グローバル コンフィギュレーション モードで **nat-control** コマンドを使用します。NAT 規則を設定することなく、外部ネットワークとの通信を内部ホストに許可する NAT コントロールをディセーブルにするには、このコマンドの **no** 形式を使用します。

nat-control

no nat-control

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

NAT コントロールは、デフォルトではディセーブルです（**no nat-control** コマンド）。

コマンドのモード

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
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

nat-control がイネーブルの場合、内部ホストが外部ネットワークと通信する前に NAT 規則を設定する必要があります。**no nat-control** コマンドを使用すると、NAT 規則を設定することなく、内部ホストが外部ネットワークと通信できるようになります。NAT を実施するホストだけに、NAT 規則を設定する必要があります。

no nat-control コマンドと **nat 0**（アイデンティティ NAT）コマンドの相違点は、アイデンティティ NAT では、ローカル ホストからトラフィックを開始する必要があることです。**no nat-control** コマンドではこの必要がありません。また、static コマンドが内部ホストの通信を許可する必要がありません。

NAT コントロールをディセーブルにすることは、NAT 規則を設定することなく、同一セキュリティ レベルの 2 つのインターフェイス間の通信を許可する、同一セキュリティ レベルの通信機能と類似しています。唯一異なる点は、NAT コントロール機能はインターフェイスではなく、ホスト間であることです。

この機能には、新しい NAT 機能は追加されていません。既存のすべての NAT 機能が変更されていません。

次の表は、**nat-control** と **no nat-control** の結果を比較しています。

条件	nat-control	no nat-control
• 内部 NAT 規則なし • 外部 NAT 規則なし	拒否	継続
• 内部 NAT 規則あり • 外部 NAT 規則なし （ダイナミック外部 NAT なし）	継続	継続
• 内部 NAT 規則あり • 外部 NAT 規則なし （ダイナミック外部 NAT なし）[1]	拒否	継続

1. ***outside*** キーワードを使用した **nat** コマンドがインターフェイスに関連付けられている場合、インターフェイスでダイナミック外部 NAT がイネーブルにされます。

セキュリティ アプライアンスを通過する各パケットでアドレス変換を実行するのに、2 つの NAT ポリシー、つまり内部 NAT ポリシーと外部 NAT ポリシーが使用されます。**nat-control** コマンドがイネーブルの場合、セキュリティ アプライアンスで通信が許可されるまで、各内部アドレスに内部 NAT 規則が含まれている必要があります。さらに、インターフェイスで外部ダイナミック NAT がイネーブルの場合、セキュリティ アプライアンスで通信が許可されるまで、各外部アドレスに外部 NAT 規則が含まれている必要があります。

no nat-control コマンドが設定され、一致する NAT ポリシーがない場合、アドレスは書き直されないまま処理が続行されます。デフォルトでは、NAT コントロールはディセーブルで（**no nat-control** コマンド）。

注 : 下位互換性を維持するために、スタートアップ コンフィギュレーションが 6 以下である場合でも、**nat-control** コマンドが自動的にイネーブルにされます。

例

次の例では、**nat-control** をイネーブルにします。

```
hostname(config)# nat-control
```

関連コマンド

コマンド	説明
nat	他のインターフェイスのグローバル アドレスに変換される、1 つのインターフェイス上のアドレスを定義します。
show running-config nat-control	NAT コンフィギュレーションの要件を表示します。

nbns-server

NBNS サーバを設定するには、webvpn モードで **nbns-server** コマンドを使用します。NBNS サーバ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。

セキュリティ アプライアンスは NBNS サーバを照会し、NetBIOS 名を IP アドレスにマッピングします。リモート システム上のファイルにアクセスしたり、ファイルを共有したりするため、WebVPN には NetBIOS が必要です。

nbns-server {*ipaddr or hostname*} [master] [timeout *timeout*] [retry *retries*]

no nbns-server

シンタックスの説明

hostname	NBNS サーバのホスト名を指定します。
ipaddr	NBNS サーバの IP アドレスを指定します。
master	WINS サーバではなく、マスター ブラウザであることを示します。
retry	再試行値が後に続くことを示します。
retries	NBNS サーバの照会をリトライする回数を指定します。セキュリティ アプライアンスは、エラー メッセージを送信する前に、ユーザが指定した回数、サーバのリストを循環します。デフォルト値は 2 です。有効な範囲は、1 ～ 10 です。
timeout	タイムアウト値が後に続くことを示します。
timeout	クエリーを再送信する前に、セキュリティ アプライアンスが待機する時間を指定します。サーバ数が 1 つのみの場合は同じサーバ上に指定し、NBNS サーバが複数ある場合は別のサーバに指定します。デフォルトのタイムアウトは 2 秒です。有効な範囲は、1 ～ 30 秒です。

デフォルト

デフォルトでは、NBNS サーバは設定されていません。

コマンドのモード

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	•	—	•	—	—

コマンド履歴

リリース	変更
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

最大 3 つのサーバ エントリを設定できます。設定する最初のサーバはプライマリ サーバで、残りの 2 つのサーバは冗長構成用のバックアップになります。

一致するエントリをコンフィギュレーションから削除するには、**no** オプションを使用します。

例

次の例は、10.10.10.19 の IP アドレス、10 秒のタイムアウト値、および 8 回のリトライでマスター ブラウザである NBNS サーバを設定する方法を示しています。また、10.10.10.24 の IP アドレス、15 秒のタイムアウト値、および 8 回のリトライで NBNS WINS サーバを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
hostname(config-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
```

neighbor

ポイントツーポイントの非ブロードキャスト ネットワークにスタティック ネイバーを定義するには、ルータ コンフィギュレーション モードで **neighbor** コマンドを使用します。スタティックに定義されたネイバー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。**neighbor** コマンドは、VPN トンネルを介して OSPF ルートをアドバタイジングする場合に使用します。

neighbor *ip_address* [***interface*** *name*]

no neighbor *ip_address* [***interface*** *name*]

シンタックスの説明

interface *name*	（オプション）**nameif** コマンドで指定されるインターフェイス名。これを介して、ネイバーに到達できるようになります。
ip_address	隣接ルータの IP 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。

コマンドのモード

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
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
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

既知の各非ブロードキャスト ネットワーク ネイバーに、ネイバー エントリが 1 つ含まれている必要があります。インターフェイスのプライマリ アドレスに、ネイバー アドレスが存在する必要があります。

システムに直接接続されているインターフェイスと同じネットワーク上にネイバーがない場合、***interface*** オプションが指定されている必要があります。さらに、ネイバーに到達するには、スタティック ルートが作成されている必要があります。

例

次の例では、192.168.1.1 のアドレスの隣接ルータを定義します。

```
hostname(config-router)# neighbor 192.168.1.1
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

nem

ハードウェア クライアントのネットワーク拡張モードをイネーブルにするには、グループポリシー コンフィギュレーション モードで **nem enable** コマンドを使用します。NEM をディセーブルにするには、**nem disable** コマンドを使用します。NEM アトリビュートを実行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。このオプションを使用すると、値を別のグループポリシーから継承できます。

nem {**enable** | **disable**}

no nem

シンタックスの説明

disable	ネットワーク拡張モードをディセーブルにします。
enable	ネットワーク拡張モードをイネーブルにします。

デフォルト

ネットワーク拡張モードはディセーブルです。

コマンドのモード

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	•	—	•	—	—

使用上のガイドライン

ネットワーク拡張モードにより、ハードウェア クライアントは、VPN トンネルを介したリモート プライベート ネットワークに対して、ルーティング可能なネットワークを 1 つ提示できます。IPSec は、ハードウェア クライアントの背後にあるプライベート ネットワークからセキュリティ アプライアンスの背後にあるネットワークへのすべてのトラフィックをカプセル化します。PAT は適用されません。したがって、セキュリティ アプライアンスの背後にある装置は、ハードウェア クライアントの背後にある、トンネルを介したプライベート ネットワークに直接アクセスできます。これはトンネルを介した場合に限ります。逆の場合も同様です。ハードウェア クライアントがトンネルを開始する必要がありますが、トンネルがアップの状態になった後は、どちらの側からもデータ交換を開始できます。

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例は、FirstGroup という名前のグループポリシーの NEM を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
```

network area

OSPF が稼働するインターフェイスを定義し、これらのインターフェイスのエリア ID を定義するには、ルータ コンフィギュレーション モードで **network area** コマンドを使用します。アドレス / ネットマスクのペアで定義したインターフェイスの OSPF 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。

network *addr mask* ***area*** *area_id*

no network *addr mask* ***area*** *area_id*

シンタックスの説明

addr	IP アドレスを指定します。
area *area_id*	OSPF アドレス範囲に関連付けられるエリアを指定します。*area_id* は、IP アドレス形式または 10 進数形式のいずれかで指定できます。10 進数形式で指定した場合、有効値の範囲は 0 ～ 4294967295 です。
mask	ネットワーク マスク。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
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

インターフェイスで OSPF を稼働させるには、**network area** コマンドでインターフェイスのアドレスが指定されている必要があります。**network area** コマンドでインターフェイスの IP アドレスを指定していない場合、そのインターフェイス上で OSPF がイネーブルになりません。

セキュリティ アプライアンスで使用できる **network area** コマンドの数には制限がありません。

例

次の例では、192.168.1.1 のインターフェイスで OSPF をイネーブルにし、エリア 2 に割り当てます。

```
hostname(config-router)# network 192.168.1.1 255.255.255.0 area 2
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

network-object

ネットワーク オブジェクト グループにネットワーク オブジェクトを追加するには、ネットワーク コンフィギュレーション モードで **network-object** コマンドを使用します。ネットワーク オブジェクトを削除するには、このコマンドの **no** 形式を使用します。

network-object host *host_addr* | *host_name*

no network-object host *host_addr* | *host_name*

network-object *net_addr netmask*

no network-object *net_addr netmask*

シンタックスの説明

host_addr	ホスト IP アドレス（**name** コマンドを使用してホスト名がまだ定義されていない場合）。
host_name	ホスト名（**name** コマンドを使用してホスト名が定義されている場合）。
net_addr	ネットワーク アドレス。*netmask* とともに使用してサブネット オブジェクトを定義します。
netmask	ネットマスク。*net_addr* とともに使用してサブネット オブジェクトを定義します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
ネットワーク　コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
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

ネットワーク コンフィギュレーション モードでホストまたはサブネット オブジェクトを定義するには、**object-group** コマンドとともに **network-object** コマンドを使用します。

例

次の例は、ネットワーク コンフィギュレーション モードで **network-object** コマンドを使用して、新しいネットワーク オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group network sjj_eng_ftp_servers
hostname(config-network)# network-object host sjj.eng.ftp
hostname(config-network)# network-object host 172.16.56.195
hostname(config-network)# network-object 192.168.1.0 255.255.255.224
hostname(config-network)# group-object sjc_eng_ftp_servers
hostname(config-network)# quit
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

nt-auth-domain-controller

このサーバの NT プライマリ ドメイン コントローラ名を指定するには、AAA サーバ ホスト モードで **nt-auth-domain-controller** 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。

nt-auth-domain-controller *string*

no nt-auth-domain-controller

シンタックスの説明

string	このサーバの、最大 16 文字のプライマリ ドメイン コントローラ名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 ホスト	•	•	•	•	—

コマンド履歴

リリース	変更
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、NT 認証の AAA サーバでのみ有効です。最初に **aaa-server host** コマンドを使用して、ホスト コンフィギュレーション モードを開始する必要があります。*string* 変数の名前は、サーバ自体の NT エントリに一致する必要があります。

例

次の例では、このサーバの NT プライマリ ドメイン コントローラ名を「primary1」に設定します。

```
hostname(config)# aaa-server svrgrp1 protocol nt
hostname(configaaa-sesrver-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# nt-auth-domain-controller primary1
```

関連コマンド

コマンド	説明
aaa server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド文をコンフィギュレーションから削除します。
show running-config aaa-server	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。

ntp authenticate

NTP サーバとの認証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 **ntp authenticate** コマンドを使用します。NTP 認証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。

ntp authenticate

no ntp authenticate

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。

コマンドのモード

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
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

認証をイネーブルにすると、セキュリティ アプライアンスは NTP サーバが正しい信頼できるキーをパケットで使用している場合にのみサーバと通信します（**ntp trusted-key** コマンドを参照）。セキュリティ アプライアンスは、NTP サーバと同期をとるための認証キーも使用します（**ntp authentication-key** コマンドを参照）。

例

次の例では、NTP パケットで認証キー 42 を使用しているシステムのみと同期するようにセキュリティ アプライアンスを設定します。

```
hostname(config)# ntp authenticate
hostname(config)# ntp authentication-key 42 md5 aNiceKey
hostname(config)# ntp trusted-key 42
```

関連コマンド

コマンド	説明
ntp authentication-key	NTP サーバと同期するための暗号化認証キーを設定します。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバとの認証で、パケット内で使用するセキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp authentication-key

NTP サーバとの認証用のキーを設定するには、グローバル コンフィギュレーション モードで **ntp authentication-key** コマンドを使用します。キーを削除するには、このコマンドの **no** 形式を使用します。

ntp authentication-key *key_id* ***md5*** *key*

no ntp authentication-key *key_id* [***md5*** *key*]

シンタックスの説明

key_id	1 ～ 4294967295 のキー ID を指定します。**ntp trusted-key** コマンドを使用して、この ID を信頼できるキーとして指定する必要があります。
md5	MD5 として認証アルゴリズムを指定します。MD5 はサポートされている唯一のアルゴリズムです。
key	キーの値を、最大 32 文字の文字列として設定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

NTP 認証を使用するには、**ntp authenticate** コマンドも設定します。

例

次の例では、認証をイネーブルにし、信頼できるキー ID 1 と 2 を指定し、信頼できる各キー ID の認証キーを設定しています。

```
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(config)# ntp authentication-key 2 md5 aNiceKey2
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバとの認証で、パケット内で使用するセキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp server

セキュリティ アプライアンスの時刻を設定するために NTP サーバを指定するには、グローバル コンフィギュレーション モードで **ntp server** コマンドを使用します。サーバを削除するには、このコマンドの **no** 形式を使用します。複数のサーバを指定できます。セキュリティ アプライアンスは、最も正確なサーバを使用します。マルチ コンテキスト モードでは、システム コンフィギュレーションにのみ NTP サーバを設定します。

ntp server *ip_address* [***key*** *key_id*] [***source*** *interface_name*] [***prefer***]

no ntp server *ip_address* [***key*** *key_id*] [***source*** *interface_name*] [***prefer***]

シンタックスの説明

ip_address	NTP サーバの IP アドレスを設定します。
key *key_id*	**ntp authenticate** コマンドを使用して認証をイネーブルにする場合、このサーバの信頼できるキー ID を設定します。**ntp trusted-key** コマンドも参照してください。
source *interface_name*	ルーティング テーブルでデフォルトのインターフェイスを使用しない場合は、NTP パケットの発信インターフェイスを指定します。システムはマルチ コンテキスト モードのインターフェイスを包含しないので、管理コンテキストで定義されたインターフェイス名を指定します。
prefer	複数のサーバの正確性がほとんど変わらない場合、この NTP サーバを優先サーバとして設定します。NTP はアルゴリズムを使用して、最も正確なサーバを判別し、そのサーバと同期を取ります。複数のサーバの正確性がほとんど変わらない場合、***prefer*** キーワードが使用するサーバを指定します。ただし、特定のサーバの正確性が優先サーバより際立っている場合、セキュリティ アプライアンスがより正確なサーバを指定します。たとえば、セキュリティ アプライアンスは、優先された層 3 のサーバではなく、層 2 のサーバを使用します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
7.0(1)	このコマンドが、送信元インターフェイスをオプションで使用するように修正されました。

例

次の例では、2 つの NTP サーバを指定し、キー ID 1 と 2 の認証をイネーブルにします。

```
hostname(config)# ntp server 10.1.1.1 key 1 prefer
hostname(config)# ntp server 10.2.1.1 key 2
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(config)# ntp authentication-key 2 md5 aNiceKey2
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するための暗号化認証キーを設定します。
ntp trusted-key	NTP サーバとの認証で、パケット内で使用するセキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp trusted-key

信頼できるキー（NTP サーバとの認証に必要）として認証キー ID 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 **ntp trusted-key** コマンドを使用します。信頼できるキーを削除するには、このコマンドの **no** 形式を使用します。複数のサーバで使用する、複数の信頼できるキーを入力できます。

ntp trusted-key *key_id*

no ntp trusted-key *key_id*

シンタックスの説明

key_id	1 ～ 4294967295 のキー ID を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

NTP 認証を使用するには、**ntp authenticate** コマンドも設定します。サーバと同期を取るには、**ntp authentication-key** コマンドを使用して、キー ID の認証キーを設定します。

例

次の例では、認証をイネーブルにし、信頼できるキー ID 1 と 2 を指定し、信頼できる各キー ID の認証キーを設定しています。

```
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(config)# ntp authentication-key 2 md5 aNiceKey2
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するための暗号化認証キーを設定します。
ntp server	NTP サーバを指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

object-group

コンフィギュレーションの最適化に使用できるオブジェクト グループを定義するには、グローバル コンフィギュレーション モードで **object-group** コマンドを使用します。コンフィギュレーションからオブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

object-group {**protocol** | **network** | **icmp-type**} *obj_grp_id*

no object-group {**protocol** | **network** | **icmp-type**} *obj_grp_id*

object-group service *obj_grp_id* {**tcp** | **udp** | **tcp-udp**}

no object-group service *obj_grp_id* {**tcp** | **udp** | **tcp-udp**}

シンタックスの説明

icmp-type	echo や echo-reply など、ICMP タイプのグループを定義します。メインの **object-group icmp-type** コマンドを入力した後、**icmp-object** コマンドと **group-object** コマンドを使用して ICMP オブジェクトを ICMP タイプ グループに追加します。
network	ホストまたはサブネット IP アドレスのグループを定義します。メインの **object-group network** コマンドを入力した後、**network-object** コマンドと **group-object** コマンドを使用してネットワーク オブジェクトをネットワーク グループに追加します。
obj_grp_id	オブジェクト グループ（1 ～ 64 文字）を指定します。アルファベット、数字、アンダースコア（_）、ハイフン（-）、およびピリオド（.）を任意に組み合せることができます。
protocol	TCP や UDP などのプロトコル グループを定義します。メインの **object-group protocol** コマンドを入力した後、**protocol-object** コマンドと **group-object** コマンドを使用してプロトコル オブジェクトをプロトコル グループに追加します。
service	「eq smtp」や「range 2000 2010」などの TCP/UDP ポート仕様のグループを定義します。メインの **object-group service** コマンドを入力した後、**port-object** コマンドと **group-object** コマンドを使用してポート オブジェクトをサービス グループに追加します。
tcp	サービス グループが TCP に使用されることを指定します。
tcp-udp	サービス グループが TCP および UDP に使用できることを指定します。
udp	サービス グループが UDP に使用され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。

コマンドのモード

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
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

ホスト、プロトコル、サービスなどのオブジェクトはグループ化できます。グループ化をすると、グループ名を使用して 1 つのコマンドを発行してグループ内のすべての項目に適用できます。

object-group コマンドでグループを定義してから、任意のセキュリティ アプライアンス コマンドを使用すると、そのコマンドはグループ内のすべての項目に適用されます。この機能によってコンフィギュレーション サイズをかなり削減できます。

オブジェクト グループを定義したら、次のように該当するすべてのセキュリティ アプライアンス コマンドのグループ名より先に **object-group** キーワードを使用する必要があります。

```
hostname# show running-config object-group group_name
```

group_name はグループの名前です。

次の例は、オブジェクト グループを定義した後で使用する方法を示しています。

```
hostname(config)# access-list access_list_name permit tcp any object-group group_name
```

また、**access list** コマンドの引数をグループ化できます。

個々の引数	代替用のオブジェクト グループ
protocol	**object-group** *protocol*
host and subnet	**object-group** *network*
service	**object-group** *service*
icmp_type	**object-group** *icmp_type*

コマンドは階層構造にグループ化できます。したがって、あるオブジェクト グループを別のオブジェクト グループのメンバーにできます。

オブジェクト グループを使用するには、次のことを実行する必要があります。

- **object-group** キーワードは、すべてのコマンドでオブジェクト グループ名より先に使用する。

  ```
  hostname(config)# access-list acl permit tcp object-group remotes object-group
  locals object-group eng_svc
  ```

  remotes および *locals* はオブジェクト グループ名の例です。
- オブジェクト グループを空にしない。
- 別のコマンドで現在使用されている場合は、オブジェクト グループを削除したり、空にしたりすることはできない。

メインの **object-group** コマンドが入力されると、コマンド モードは対応するモードに変わります。オブジェクト グループは新規のモードで定義されます。アクティブ モードがコマンド プロンプト形式で示されます。たとえば、コンフィギュレーション端末モードのプロンプトは次のように表示されます。

```
hostname(config)#
```

hostname はセキュリティ アプライアンスの名前です。

ただし、**object-group** コマンドを入力すると、プロンプトは次のように表示されます。

```
hostname(config-type)#
```

hostname はセキュリティ アプライアンスの名前で、*type* は *object-group* のタイプです。

object-group モードを閉じて **object-group** メイン コマンドを終了するには、**exit** や **quit** コマンド、または **access-list** コマンドなどの有効な設定モード コマンドを使用します。

show running-config object-group コマンドは、定義されているすべてのオブジェクト グループを表示します。このとき、**show running-config object-group** *grp_id* コマンドを入力した場合は *grp_id* ごとに、**show running-config object-group** *grp_type* コマンドを入力した場合はグループ タイプごとに表示されます。引数を指定せずに **show running-config object-group** コマンドを入力すると、定義されているすべてのオブジェクト グループが表示されます。

それまでに定義した **object-group** コマンドのグループを削除するには、**clear configure object-group** コマンドを使用します。引数を指定せずに **clear configure object-group** コマンドを使用すると、別のコマンドで使用されていないが、すでに定義されいるすべてのオブジェクト グループを削除できます。*grp_type* 引数は、別のコマンドで使用されていないが、すでに定義されているすべてのオブジェクト グループのうち、そのグループ タイプだけを削除します。

object-group モードでは、**show running-config** および **clear configure** コマンドを含む他のすべてのセキュリティ アプライアンス コマンドを使用できます。

オブジェクトグループ モード内のコマンドは、**show running-config object-group** コマンド、**write** コマンド、または **config** コマンドで表示または保存した場合は、字下げして表示されます。

オブジェクトグループ モード内のコマンドには、メイン コマンドと同じコマンド特権レベルがあります。

access-list コマンドで複数のオブジェクト グループを使用している場合、このコマンドで使用されるすべてのオブジェクト グループの要素は相互に連結されます。最初に 1 番目のグループ要素が 2 番目のグループ要素に連結され、1 番目と 2 番目のグループ要素が 3 番目のグループ要素に連結されるというようになります。

説明テキストの開始位置は、**description** キーワードに続く空白（ブランクまたはタブ）直後の文字です。

例

次の例は、**object-group icmp-type** モードを使用して新しい icmp-type オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group icmp-type icmp-allowed
hostname(config-icmp-type)# icmp-object echo
hostname(config-icmp-type)# icmp-object time-exceeded
hostname(config-icmp-type)# exit
```

次の例は、**object-group network** コマンドを使用して新しいネットワーク オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group network sjc_eng_ftp_servers
hostname(config-network)# network-object host sjc.eng.ftp.servcers
hostname(config-network)# network-object host 172.23.56.194
hostname(config-network)# network-object 192.1.1.0 255.255.255.224
hostname(config-network)# exit
```

次の例は、**object-group network** コマンドを使用して新しいネットワーク オブジェクト グループを作成し、既存の object-group にマッピングする方法を示しています。

```
hostname(config)# object-group network sjc_ftp_servers
hostname(config-network)# network-object host sjc.ftp.servers
hostname(config-network)# network-object host 172.23.56.195
hostname(config-network)# network-object 193.1.1.0 255.255.255.224
hostname(config-network)# group-object sjc_eng_ftp_servers
hostname(config-network)# exit
```

次の例は、**object-group protocol** モードを使用して新しいプロトコル オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group protocol proto_grp_1
hostname(config-protocol)# protocol-object udp
hostname(config-protocol)# protocol-object ipsec
hostname(config-protocol)# exit

hostname(config)# object-group protocol proto_grp_2
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# group-object proto_grp_1
hostname(config-protocol)# exit
```

次の例は、**object-group service** モードを使用して新しいポート（サービス）オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group service eng_service tcp
hostname(config-service)# group-object eng_www_service
hostname(config-service)# port-object eq ftp
hostname(config-service)# port-object range 2000 2005
hostname(config-service)# exit
```

次の例は、テキスト説明をオブジェクト グループに追加およびオブジェクト グループから削除する方法を示しています。

```
hostname(config)# object-group protocol protos1
hostname(config-protocol)# description This group of protocols is for our internal
network

hostname(config-protocol)# show running-config object-group id protos1
object-group protocol protos1
description: This group of protocols is for our internal network

hostname(config-protocol)# no description
hostname(config-protocol)# show running-config object-group id protos1
object-group protocol protos1
```

次の例は、**group-object** モードを使用して、すでに定義されているオブジェクトで構成される新しいオブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group network host_grp_1
hostname(config-network)# network-object host 192.168.1.1
hostname(config-network)# network-object host 192.168.1.2
hostname(config-network)# exit

hostname(config)# object-group network host_grp_2
hostname(config-network)# network-object host 172.23.56.1
hostname(config-network)# network-object host 172.23.56.2
hostname(config-network)# exit

hostname(config)# object-group network all_hosts
hostname(config-network)# group-object host_grp_1
hostname(config-network)# group-object host_grp_2
hostname(config-network)# exit

hostname(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
hostname(config)#access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
hostname(config)#access-list all permit tcp object-group all_hosts any eq www
```

group-object コマンドを指定しない場合は、*host_grp_1* と *host_grp_2* ですでに定義されている IP アドレスをすべて含むように *all_hosts* グループを定義する必要があります。**group-object** コマンドを指定する場合は、重複してホストを定義する必要がなくなります。

次の例は、オブジェクト グループを使用してアクセスリストのコンフィギュレーションを簡略化する方法を示しています。

```
hostname(config)# object-group network remote
hostname(config-network)# network-object host kqk.suu.dri.ixx
hostname(config-network)# network-object host kqk.suu.pyl.gnl

hostname(config)# object-group network locals
hostname(config-network)# network-object host 172.23.56.10
hostname(config-network)# network-object host 172.23.56.20
hostname(config-network)# network-object host 172.23.56.194
hostname(config-network)# network-object host 172.23.56.195

hostname(config)# object-group service eng_svc ftp
hostname(config-service)# port-object eq www
hostname(config-service)# port-object eq smtp
hostname(config-service)# port-object range 25000 25100
```

このグループ化により、グループ化を使用しないと 24 行になるアクセスリストを 1 行で設定できます。その代わり、グループ化を使用するとアクセスリストのコンフィギュレーションは次のようになります。

```
hostname(config)# access-list acl permit tcp object-group remote object-group locals
object-group eng_svc
```

（注）　**show running-config object-group** コマンドおよび **write** コマンドを使用すると、オブジェクト グループ名で設定されているようにアクセスリストを表示できます。**show access-list** コマンドは、オブジェクトをグループ化せずに、アクセスリスト エントリを個々のエントリに展開して表示します。

関連コマンド

コマンド	説明
clear configure object-group	すべての **object group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

ospf authentication

OSPF 認証の使用を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 **ospf authentication** コマンドを使用します。デフォルトの認証スタンスに戻すには、このコマンドの **no** 形式を使用します。

ospf authentication [***message-digest*** | ***null***]

no ospf ***authentication***

シンタックスの説明

message-digest	（オプション）OSPF メッセージ ダイジェスト認証を使用するように指定します。
null	（オプション）OSPF 認証を使用しないように指定します。

デフォルト

デフォルトでは、OSPF 認証はイネーブルではありません。

コマンドのモード

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
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

ospf authentication コマンドを使用する前に、**ospf authentication-key** コマンドを使用してインターフェイスのパスワードを設定します。***message-digest*** キーワードを使用する場合、**ospf message-digest-key** コマンドを使用して、インターフェイスのメッセージ ダイジェスト キーを設定します。

下位互換性を維持するため、エリアの認証タイプが継続してサポートされます。認証タイプがインターフェイスに指定されていない場合、エリアの認証タイプが使用されます（エリアのデフォルトは null 認証です）。

オプションを指定せずにこのコマンドを使用する場合、簡易パスワード認証がイネーブルにされます。

例

次の例は、選択したインターフェイスで OSPF の簡易パスワード認証をイネーブルにする方法を示しています。

```
hostname(config-if)# ospf authentication
hostname(config-if)#
```

関連コマンド

コマンド	説明
ospf ***authentication-key***	隣接ルーティング デバイスで使用するためのパスワードを指定します。
ospf message-digest-key	MD5 認証をイネーブルにし、MD5 キーを指定します。

ospf authentication-key

隣接ルーティング デバイスで使用されるパスワードを指定するには、インターフェイス コンフィギュレーション モードで **ospf authentication-key** コマンドを使用します。パスワードを削除するには、このコマンドの **no** 形式を使用します。

ospf *authentication-key* *password*

no ospf authentication-key

シンタックスの説明

password	隣接ルーティング デバイスで使用するための OSPF 認証パスワードを割り当てます。パスワードは、9 文字未満にする必要があります。2 文字の間にブランク スペースを含めることができます。パスワードの最初または最後のスペースは無視されます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

このコマンドによって作成されたパスワードは、ルーティング プロトコル パケットが発信されるときに、OSPF ヘッダーに直接挿入されるキーとして使用されます。インターフェイス単位で、別個のパスワードを各ネットワークに割り当てることができます。同一ネットワーク上のすべての隣接ルータが、OSPF 情報を交換できる同じパスワードを持つ必要があります。

例

次の例は、OSPF 認証のパスワードを指定する方法を示しています。

```
hostname(config-if)# ospf authentication-key ThisMyPW
```

関連コマンド

コマンド	説明
area authentication	指定したエリアの OSPF 認証をイネーブルにします。
ospf authentication	OSPF 認証の使用をイネーブルにします。

ospf cost

インターフェイスを介した 1 パケットの送信コストを指定するには、インターフェイス コンフィギュレーション モードで **ospf cost** コマンドを使用します。インターフェイス コストをデフォルト値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。

ospf cost *interface_cost*

no ospf cost

シンタックスの説明

interface_cost	インターフェイスを介した 1 パケットの送信コスト（リンク状態メトリック）。これは 0 ～ 65535 の符号なし整数値です。0 は、インターフェイスに直接接続されているネットワークを表し、インターフェイスの帯域幅が高くなるほど、そのインターフェイスを通してパケットを送信する関連コストは低くなります。つまり、大きいコスト値は低い帯域幅のインターフェイスを表し、小さいコスト値は高い帯域幅のインターフェイスを表します。 セキュリティ アプライアンス上にある OSPF インターフェイスのデフォルト コストは 10 です。このデフォルトは Cisco IOS ソフトウェアとは異なり、デフォルト コストはファースト イーサネットおよびギガビット イーサネットの場合は 1、10BaseT の場合は 10 です。ECMP をネットワークで使用している場合は、このことを考慮に入れておくことが重要です。

デフォルト

デフォルトの *interface_cost* は 10 です。

コマンドのモード

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
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

ospf cost コマンドを使用すると、インターフェイスでの 1 パケットの送信コストを明示的に指定できます。*interface_cost* パラメータは、0 ～ 65535 の符号なし整数値です。

no ospf cost コマンドを使用すると、パス コストをデフォルト値にリセットできます。

例

次の例は、選択したインターフェイスで 1 パケットの送信コストを指定する方法を示しています。

```
hostname(config-if)# ospf cost 4
```

関連コマンド

コマンド	説明
show running-config interface	指定した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。

ospf database-filter

同期およびフラッディング中に OSPF インターフェイスへのすべての発信 LSA をフィルタリングするには、インターフェイス コンフィギュレーション モードで **ospf database-filter** コマンドを使用します。LSA を復元するには、このコマンドの **no** 形式を使用します。

ospf database-filter ***all out***

no ospf database-filter ***all out***

シンタックスの説明

all out	OSPF インターフェイスへのすべての発信 LSA をフィルタリングします。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

ospf database-filter コマンドは、OSPF インターフェイスへの発信 LSA をフィルタリングします。**no ospf database-filter all out** コマンドは、インターフェイスへの LSA のフォワーディングを復元します。

例

次の例は、**ospf database-filter** コマンドを使用して、発信 LSA をフィルタリングする方法を示しています。

```
hostname(config-if)# ospf database-filter all out
```

関連コマンド

コマンド	説明
show interface	インターフェイスのステータス情報を表示します。

ospf dead-interval

ネイバーがルータのダウンを宣言するまでの間隔を指定するには、インターフェイス コンフィギュレーション モードで **ospf dead-interval** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ospf dead-interval *seconds*

no ospf dead-interval

シンタックスの説明

seconds	hello パケットを 1 つも受信しない時間。*seconds* のデフォルトは、**ospf hello-interval** コマンドで設定した間隔の 4 倍です（範囲は 1 ～ 65,535）。

デフォルト

seconds のデフォルト値は、**ospf hello-interval** コマンドで設定した間隔の 4 倍です。

コマンドのモード

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
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

ospf dead-interval コマンドを使用すると、ネイバーがルータのダウンを宣言するまでのデッド間隔（hello パケットを 1 つも受信しない時間）を設定できます。*seconds* 引数はデッド間隔を指定します。この値はネットワーク上のすべてのノードで同じにする必要があります。*seconds* のデフォルトは、**ospf hello-interval** コマンドで設定した間隔の 4 倍です（1 ～ 65,535）。

no ospf dead-interval コマンドを使用すると、デフォルトの間隔値に戻ります。

例

次の例では、OSPF デッド間隔を 1 分に設定します。

```
hostname(config-if)# ospf dead-interval 60
```

関連コマンド

コマンド	説明
ospf hello-interval	インターフェイスで hello パケットを送信する間隔を指定します。
show ospf interface	OSPF 関連のインターフェイス情報を表示します。

ospf hello-interval

インターフェイスで hello パケットを送信する間隔を指定するには、インターフェイス コンフィギュレーション モードで **ospf hello-interval** コマンドを使用します。hello 間隔を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。

ospf hello-interval *seconds*

no ospf hello-interval

シンタックスの説明

seconds	インターフェイスで hello パケットを送信する間隔を指定します。有効値は、1 ～ 65,535 秒です。

デフォルト

hello-interval *seconds* のデフォルト値は 10 秒です。

コマンドのモード

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
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

この値は、hello パケットでアドバタイズされます。hello 間隔が短いほど、トポロジの変更が早急に検出されますが、より多くのルーティング トラフィックが結果として生じます。この値は、特定のネットワーク上のすべてのルータおよびアクセス サーバで同じにする必要があります。

例

次の例では、OSPF の hello 間隔を 5 秒に設定します。

```
hostname(config-if)# ospf hello-interval 5
```

関連コマンド

コマンド	説明
ospf dead-interval	ネイバーがルータのダウンを宣言するまでの間隔を指定します。
show ospf interface	OSPF 関連のインターフェイス情報を表示します。

ospf message-digest-key

OSPF の MD5 認証を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 **ospf message-digest-key** コマンドを使用します。MD5 キーを削除するには、このコマンドの **no** 形式を使用します。

ospf message-digest-key *key-id* ***md5*** *key*

no ospf message-digest-key

シンタックスの説明

key-id	MD5 認証をイネーブルにし、数値による認証キー ID 番号を指定します。有効値は、1 ～ 255 です。
md5 *key*	最大 16 バイトの英数字によるパスワード。キー文字の間にスペースを含めることができます。キーの最初または最後のスペースは無視されます。MD5 認証は、通信整合性の検証、送信元の認証、および適時性の確認を行います。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

ospf message-digest-key コマンドを使用すると、MD5 認証をイネーブルにできます。このコマンドの **no** 形式を使用すると、古い MD5 キーを削除できます。*key_id* は、1 ～ 255 の認証キー用数値 ID で、*key* は、最大 16 バイトの英数字によるパスワードです。MD5 は、通信整合性の検証、送信元の認証、および適時性の確認を行います。

例

次の例は、OSPF 認証の MD5 キーを指定する方法を示しています。

```
hostname(config-if)# ospf message-digest-key 3 md5 ThisIsMyMd5Key
```

関連コマンド

コマンド	説明
area authentication	OSPF エリア認証をイネーブルにします。
ospf authentication	OSPF 認証の使用をイネーブルにします。

ospf mtu-ignore

データベース パケット受信時の OSPF の最大伝送ユニット ミスマッチ検出をディセーブルにするには、インターフェイス コンフィギュレーション モードで **ospf mtu-ignore** コマンドを使用します。MTU ミスマッチ検出を復元するには、このコマンドの **no** 形式を使用します。

ospf mtu-ignore

no ospf mtu-ignore

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

デフォルトでは、**ospf mtu-ignore** はイネーブルになっています。

コマンドのモード

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
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

OSPF は、ネイバーが共通のインターフェイスで同じ MTU を使用しているかどうかをチェックします。このチェックは、ネイバーが Database Descriptor（DBD）パケットを交換するときに実行されます。DBD パケット受信時の MTU が着信インターフェイスに設定された IP MTU より高い場合、OSPF の隣接関係が確立されません。**ospf mtu-ignore** コマンドは、DBD パケット受信時の OSPF MTU ミスマッチ検出をディセーブルにします。これは、デフォルトでイネーブルになっています。

例

次の例は、**ospf mtu-ignore** コマンドをディセーブルにする方法を示しています。

```
hostname(config-if)# ospf mtu-ignore
```

関連コマンド

コマンド	説明
show interface	インターフェイスのステータス情報を表示します。

ospf network point-to-point non-broadcast

ポイントツーポイントの非ブロードキャスト ネットワークとして OSPF 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 **ospf network** ***point-to-point non-broadcast*** コマンドを使用します。このコマンド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。**ospf network** ***point-to-point non-broadcast*** コマンドを使用すると、VPN トンネルを介して OSPF ルートを送信できます。

ospf network ***point-to-point non-broadcast***

no ospf network ***point-to-point non-broadcast***

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。

コマンドのモード

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
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

インターフェイスをポイントツーポイントとして指定する場合、OSPF ネイバーを手動で設定する必要があります。ダイナミック検出はできません。OSPF ネイバーを手動で設定するには、ルータ コンフィギュレーション モードで **neighbor** コマンドを使用します。

インターフェイスをポイントツーポイントとして設定すると、次の制約事項が適用されます。

- 2 つ以上のネイバーをインターフェイスに定義できない。
- 暗号エンドポイントに向かうスタティック ルートを定義する必要がある。
- ネイバーを明示的に設定しないと、インターフェイスが隣接関係を形成できない。
- トンネルを介した OSPF がインターフェイスで実行されている場合、同じインターフェイス上で上流のルータによる標準 OSPF を実行できない。
- VPN トンネルを介して OSPF アップデートを受け渡すように OSPF ネイバーを指定する前に、インターフェイスに暗号マップをバインドする必要がある。OSPF ネイバーを指定した後、インターフェイスに暗号マップをバインドする場合、**clear local-host all** コマンドを使用して、OSPF 接続を消去し、OSPF の隣接関係が VPN トンネルを介して確立されるようにします。

例

次の例は、選択したインターフェイスをポイントツーポイントの非ブロードキャスト 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-if)# ospf network point-to-point non-broadcast
hostname(config-if)#
```

関連コマンド

コマンド	説明
neighbor	手動で設定された OSPF ネイバーを指定します。
show interface	インターフェイスのステータス情報を表示します。

ospf priority

OSPF ルータの優先順位を変更するには、インターフェイス コンフィギュレーション モードで **ospf priority** コマンドを使用します。デフォルトの優先順位に戻すには、このコマンドの **no** 形式を使用します。

ospf priority *number*

no ospf priority [*number*]

シンタックスの説明

number	ルータの優先順位を指定します。有効値は 0 ～ 255 です。

デフォルト

number のデフォルト値は 1 です。

コマンドのモード

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
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

ネットワークに接続されている 2 つのルータの両方が代表ルータになることを試行する場合、ルータの優先順位が高いルータが優先されます。両方のルータが同等である場合は、ルータ ID が高いルータが優先されます。ルータの優先順位が 0（ゼロ）に設定されているルータは、代表ルータまたはバックアップの代表ルータになる資格がありません。ルータの優先順位は、マルチアクセス ネットワーク（ポイントツーポイントではないネットワーク）へのインターフェイスにのみ設定されます。

例

次の例は、選択したインターフェイスで OSPF の優先順位を変更する方法を示しています。

```
hostname(config-if)# ospf priority 4
hostname(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF 関連のインターフェイス情報を表示します。

ospf retransmit-interval

インターフェイスに属する隣接ルータの LSA 再送間隔を指定するには、インターフェイス コンフィギュレーション モードで **ospf retransmit-interval** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ospf retransmit-interval *seconds*

no ospf retransmit-interval [*seconds*]

シンタックスの説明

seconds	インターフェイスに属する隣接ルータの LSA 再送間隔を指定します。有効値は、1 ～ 65,535 秒です。

デフォルト

retransmit-interval *seconds* のデフォルト値は 5 秒です。

コマンドのモード

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
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

ルータは、LSA をネイバーに送信する場合に、確認応答メッセージを受信するまで LSA を保持します。確認応答を受信しない場合、ルータは LSA を再送信します。

このパラメータの設定を慎重に行う必要があります。そうしない場合、不要な再送信が生じます。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

例

次の例は、LSA の再送間隔を変更する方法を示しています。

```
hostname(config-if)# ospf retransmit-interval 15
hostname(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF 関連のインターフェイス情報を表示します。

ospf transmit-delay

インターフェイス上のリンクステート アップデート パケットを送信するのに必要な予想時間を設定するには、インターフェイス コンフィギュレーション モードで **ospf transmit-delay** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ospf transmit-delay *seconds*

no ospf transmit-delay [*seconds*]

シンタックスの説明

seconds	インターフェイス上のリンクステート アップデート パケットを送信するのに必要な予想時間を設定します。デフォルト値は 1 秒で、範囲は 1 ～ 65,535 秒です。

デフォルト

seconds のデフォルト値は 1 秒です。

コマンドのモード

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
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

送信される前に、アップデート パケットの LSA には、*seconds* 引数で指定された値によって加算された経過時間が含まれている必要があります。値を割り当てるときは、インターフェイスの送信と伝搬遅延を考慮に入れる必要があります。

リンクを通じて送信される前に遅延が追加されていない場合、LSA がリンクを通じて伝播する時間が考慮されません。非常に低速のリンクでは、この設定は重要です。

例

次の例では、選択したインターフェイスの送信遅延を 3 秒に設定します。

```
hostname(config-if)# ospf restransmit-delay 3
hostname(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF 関連のインターフェイス情報を表示します。

outstanding

非認証の電子メール プロキシ セッションの数を制限するには、適切な電子メール プロキシ モードで **outstanding** コマンドを使用します。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。これにより、無制限の非認証セッション数が許可されます。電子メール ポートに対する DoS 攻撃（サービス拒絶攻撃）を制限するには、このコマンドを使用します。

電子メール プロキシ接続には、次の 3 つの状態があります。

1. 新しい電子メール接続は、「非認証」状態になります。
2. その接続でユーザ名が提示されると、「認証中」状態になります。
3. セキュリティ アプライアンスがその接続を認証すると、「認証済み」状態になります。

非認証状態の接続の数が、設定された限度を超えると、セキュリティ アプライアンスはオーバーロードを回避するため最も古い非認証接続を強制終了します。認証済みの接続は、強制終了されません。

outstanding {*number*}

no outstanding

シンタックスの説明

number	許可される非認証セッション数。範囲は、1 ～ 1,000 です。

デフォルト

デフォルトは 20 です。

コマンドのモード

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
Pop3s	•	•	—	—	•
Imap4s	•	•	—	—	•
Smtps	•	•	—	—	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例は、POP3S 電子メール プロキシの非認証セッション数の限度を 12 に設定する方法を示しています。

```
hostname(config)# pop3s
hostname(config-pop3s)# outstanding 12
```

participate

デバイスを仮想ロードバランシング クラスタに強制的に参加させるには、VPN ロードバランシング モードで **participate** コマンドを使用します。クラスタに参加した状態からデバイスを削除するには、このコマンドの **no** 形式を使用します。

participate

no participate

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

デフォルト動作では、デバイスは VPN ロードバランシング クラスタに参加しません。

コマンドのモード

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
VPN ロードバランシング	•	—	•	—	—

コマンド履歴

リリース	変更
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

VPN ロードバランシング モードに入るには、**interface** コマンドおよび **nameif** コマンドを使用してインターフェイスを設定してから、**vpn load-balancing** コマンドを使用する必要があります。また、事前に **cluster ip** コマンドを使用してクラスタの IP アドレスを設定し、仮想クラスタの IP アドレスが参照するインターフェイスを設定する必要があります。

このコマンドは、このデバイスを仮想ロードバランシング クラスタに強制的に参加させます。デバイスの参加をイネーブルにするには、このコマンドを明示的に発行する必要があります。

1 つのクラスタに参加しているすべてのデバイスの IP アドレス、暗号化設定、暗号鍵、およびポートの値は、クラスタ固有の同一の値である必要があります。

（注） 暗号化を使用する場合は、事前に **isakmp enable** *inside* コマンドを設定する必要があります。*inside* には、ロードバランシング内部インターフェイスを指定します。ロードバランシング内部インターフェイス上で isakmp がイネーブルになっていないと、クラスタ暗号化の設定を試みたときにエラー メッセージが表示されます。

isakmp が、**cluster encryption** コマンドを設定したときはイネーブルであったものの、**participate** コマンドを設定する前にディセーブルになった場合は、**participate** コマンドを入力したときにエラー メッセージが表示され、そのローカル デバイスはクラスタに参加しません。

例

次に、VPN ロードバランシング コマンド シーケンスの例を示します。これには、現在のデバイスが VPN ロードバランシング クラスタに参加できるようにする **participate** コマンドが含まれています。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
hostname(config-load-balancing)#
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシング モードに入ります。

passwd

ログイン パスワードを設定するには、グローバル コンフィギュレーション モードで **passwd** コマンドを使用します。パスワードをデフォルトの「cisco」に戻すには、このコマンドの **no** 形式を使用します。Telnet または SSH を使用して、CLI にデフォルト ユーザとしてアクセスするときは、ログイン パスワードを入力するためのプロンプトが表示されます。ログイン パスワードを入力すると、ユーザ EXEC モードに入ります。

{**passwd** | **password**} *password* [***encrypted***]

no {**passwd** | **password**} *password*

シンタックスの説明

encrypted	（オプション）パスワードが暗号化された形式であることを指定します。パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。何らかの理由でパスワードを別のセキュリティ アプライアンスにコピーする必要があるのに元のパスワードがわからない場合、暗号化されたパスワードとこのキーワードを使用して **passwd** コマンドを入力します。通常、このキーワードは、**show running-config passwd** コマンドを入力したときにだけ表示されます。
passwd* | *password	どちらのコマンドでも入力できます。これらは互いにエイリアス関係にあります。
password	パスワードに、大文字と小文字が区別される最大 80 文字の文字列を設定します。パスワードにスペースを含めることはできません。

デフォルト

デフォルト パスワードは「cisco」です。

コマンドのモード

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
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

このログイン パスワードはデフォルト ユーザ用です。**aaa authentication console** コマンドを使用して、Telnet または SSH のユーザごとに CLI 認証を設定した場合、このパスワードは使用されません。

例

次の例では、パスワードを Pa$$w0rd に設定します。

```
hostname(config)# passwd Pa$$w0rd
```

次の例では、別のセキュリティ アプライアンスからコピーした、暗号化されたパスワードをパスワードに設定します。

```
hostname(config)# passwd jMorNbK0514fadBh encrypted
```

関連コマンド

コマンド	説明
clear configure passwd	ログイン パスワードを消去します。
enable	特権 EXEC モードに入ります。
enable password	イネーブル パスワードを設定します。
show curpriv	現在ログインしているユーザの名前および特権レベルを表示します。
show running-config passwd	ログイン パスワードを暗号化された形式で表示します。

password (crypto ca trustpoint)

登録中に CA に登録するチャレンジ フレーズを指定するには、暗号 CA トラストポイント コンフィギュレーション モードで **password** コマンドを使用します。CA は、通常、このフレーズを使用して、その後の失効要求を認証します。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。

password *string*

no password

シンタックスの説明

string	パスワードの名前を文字列として指定します。最初の文字にを数字にすることはできません。文字列には、スペースを含む最大 80 文字の任意の英数字を使用できます。数字、スペース、任意の文字という形式のパスワードは指定できません。数字の後にスペースがあると、問題が発生します。たとえば、「hello 21」は適切なパスワードですが、「21 hello」は不適切です。パスワード チェックでは、大文字と小文字が区別されます。たとえば、「Secret」というパスワードと「secret」というパスワードは異なります。

デフォルト

デフォルトでは、パスワードを含めない設定になっています。

コマンドのモード

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 コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更
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

このコマンドを使用すると、実際の証明書登録を開始する前に、証明書の失効パスワードを指定できます。指定したパスワードは、アップデートされたコンフィギュレーションがセキュリティ アプライアンスによって NVRAM に書き込まれるときに暗号化されます。

このコマンドがイネーブルになっていない場合、証明書登録中にパスワードの入力は求められません。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、CA に登録するチャレンジ フレーズをトラストポイント central の登録要求に含めています。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# password zzxxyy
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。

password-prompt

WebVPN に対する初期ログイン用のパスワードを要求するプロンプトを設定するには、webvpn モードで **password-prompt** コマンドを使用します。デフォルトの「Password:」に戻すには、このコマンドの **no** 形式を使用します。

password-prompt [*prompt*]

no **password-prompt**

シンタックスの説明

prompt	（オプション）ユーザにパスワードの入力を求める文字列を指定します。最大 16 文字です。

デフォルト

デフォルト プロンプトは、「Password:」です。

コマンドのモード

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	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例は、「Enter Password:」というパスワード プロンプトを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# password-prompt Enter Password:
```

password-storage

クライアント システム上にログイン パスワードを保存することをユーザに許可するには、グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **password-storage enable** コマンドを使用します。パスワードの保存をディセーブルにするには、**password-storage disable** コマンドを使用します。

password-storage アトリビュートを実行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。これにより、password-storage の値を別のグループポリシーから継承できるようになります。

password-storage {enable | disable}

no password-storage

シンタックスの説明

disable	パスワードの保存をディセーブルにします。
enable	パスワードの保存をイネーブルにします。

デフォルト

パスワードの保存はディセーブルになっています。

コマンドのモード

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	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更
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

セキュアなサイトにあることが判明しているシステムに限り、パスワードの保存をイネーブルにしてください。

このコマンドは、対話型ハードウェア クライアント認証またはハードウェア クライアントの個別ユーザ認証とは関係ありません。

例

次の例は、FirstGroup というグループポリシーのパスワードの保存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)# password-storage enable
```

peer-id-validate

ピアの証明書を使用してピアのアイデンティティを確認するかどうかを指定するには、トンネルグループ ipsec アトリビュート モードで **peer-id-validate** コマンドを使用します。デフォルト値に戻すには、このコマンドの ***no*** 形式を使用します。

peer-id-validate *option*

no peer-id-validate

シンタックスの説明

option	次のオプションのいずれかを指定します。 • ***req***：必須 • ***cert***：証明書によってサポートされている場合 • ***nocheck***：確認しない

デフォルト

デフォルトでは、このコマンドの設定は ***req*** です。

コマンドのモード

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
トンネルグループ IPSec アトリビュート	•	—	•	—	—

コマンド履歴

リリース	変更
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

すべてのトンネルグループ タイプにこのアトリビュートを適用できます。

例

config-ipsec コンフィギュレーション モードで入力された次の例は、209.165.200.225 という名前の IPSec LAN-to-LAN トンネルグループのピアの証明書のアイデンティティを使用してのピアの確認を要求します。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-ipsec)# peer-id-validate req
hostname(config-ipsec)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネルグループを消去します。
show running-config tunnel-group	指定したトンネルグループまたはすべてのトンネルグループのコンフィギュレーションを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネルグループに関連付けます。

perfmon

パフォーマンス情報を表示するには、特権 EXEC モードで **perfmon** コマンドを使用します。

perfmon {**verbose** | **interval** *seconds* | **quiet** | **settings**}

シンタックスの説明

verbose	セキュリティ アプライアンス コンソールにパフォーマンス モニタ情報を表示します。
interval *seconds*	コンソールのパフォーマンス表示がリフレッシュされるまでの秒数を指定します。
quiet	パフォーマンス モニタの表示をディセーブルにします。
settings	interval を表示し、quiet と verbose のいずれであるかを表示します。

デフォルト

seconds は、120 秒です。

コマンドのモード

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
7.0(1)	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。

使用上のガイドライン

perfmon コマンドを使用すると、セキュリティ アプライアンスのパフォーマンスを監視できます。情報をすぐに表示するには、**show perfmon** コマンドを使用します。情報を 2 分間隔で表示し続けるには、**perfmon verbose** コマンドを使用します。指定した秒間隔で情報を表示し続けるには、**perfmon interval** *seconds* コマンドと **perfmon verbose** コマンドを併用します。

パフォーマンス情報は次のように表示されます。

PERFMON STATS:	Current	Average
Xlates	33/s	20/s
Connections	110/s	10/s
TCP Conns	50/s	42/s
WebSns Req	4/s	2/s
TCP Fixup	20/s	15/s
HTTP Fixup	5/s	5/s
FTP Fixup	7/s	4/s
AAA Authen	10/s	5/s
AAA Author	9/s	5/s
AAA Account	3/s	3/s

この情報では、変換、接続、Websense 要求、アドレス変換（「フィックスアップ」と呼ばれます）、および AAA トランザクションについて、毎秒発生する数が表示されます。

例

次の例は、パフォーマンス モニタ統計情報を 30 秒おきにセキュリティ アプライアンス コンソールに表示する方法を示しています。

```
hostname(config)# perfmon interval 120
hostname(config)# perfmon quiet
hostname(config)# perfmon settings
interval: 120 (seconds)
quiet
```

関連コマンド

コマンド	説明
show perfmon	パフォーマンス情報を表示します。

periodic

時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定するには、時間範囲コンフィギュレーション モードで ***periodic*** 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。

periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

no periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

シンタックスの説明

days-of-the-week	（オプション）最初の days-of-the-week 引数は、関連付けられている時間範囲が有効になる日または曜日です。2 番目の days-of-the-week 引数は、関連付けられている文の有効期間が終了する日または曜日です。 この引数は、任意の 1 つの曜日または曜日の組み合せです（monday（月曜日）、tuesday（火曜日）、wednesday（水曜日）、thursday（木曜日）、friday（金曜日）、saturday（土曜日）、および sunday（日曜日））。他に指定できる値は、次のとおりです。 • daily：月曜日～日曜日 • weekdays：月曜日～金曜日 • weekend：土曜日と日曜日 終了の曜日が開始の曜日と同じ場合は、終了の曜日を省略できます。
time	時刻を HH:MM 形式で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。
to	「開始時刻から終了時刻まで」の範囲を完成させるには、***to*** キーワードを入力する必要があります。

デフォルト

periodic コマンドに値が入力されていない場合、***time-range*** コマンドでの定義に従ったセキュリティ アプライアンスへのアクセスがすぐに有効になり、常時オンとなります。

コマンドのモード

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
時間範囲コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
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

時間ベース ACL を実装するには、***time-range*** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。次に、**access-list extended time-range** コマンドとともに使用して、時間範囲を ACL にバインドします。

periodic コマンドは、時間範囲をいつ有効にするかを指定する方法の 1 つです。別の方法は、***absolute*** コマンドを使用して絶対時間範囲を指定する方法です。これらのコマンドのいずれかを、***time-range*** グローバル コンフィギュレーション コマンドの後に使用します。このコマンドは、時間範囲の名前を指定します。***time-range*** コマンドごとに複数の ***periodic*** 値を入力できます。

終了の days-of-the-week 値が開始の days-of-the-week 値と同じである場合は、終了の days-of-the-week 値を省略できます。

time-range コマンドに ***absolute*** 値と ***periodic*** 値の両方が指定されている場合、***periodic*** コマンドは ***absolute start*** 時刻に達した後にだけ評価され、***absolute end*** 時刻に達した後はそれ以上評価されません。

time-range 機能はセキュリティ アプライアンスのシステム クロックに依存しています。ただし、この機能は、NTP 同期化により最適に動作します。

例

次にいくつかの例を示します。

必要な設定	入力内容
月曜日から金曜日の午前 8 時～午後 6 時のみ	***periodic weekdays 8:00:00 to 18:00***
毎日午前 8 時～午後 6 時のみ	***periodic daily 8:00 to 18:00***
月曜日午前 8 時～金曜日午後 8 時の 1 分おき	***periodic monday 8:00 to friday 20:00***
週末、つまり土曜日の朝から日曜日の終わりまで	***periodic weekend 00:00 to 23:59***
土曜日および日曜日の正午～深夜	***periodic weekend 12:00:00 to 23:59***

次の例は、月曜日から金曜日の午前 8 時～午後 6 時にセキュリティ アプライアンスにアクセスすることを許可する方法を示しています。

```
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
hostname(config-time-range)#
```

次の例は、特定の曜日（月曜日、火曜日、および金曜日）の午前 10 時 30 分～午後 12 時 30 分にセキュリティ アプライアンスにアクセスすることを許可する方法を示しています。

```
hostname(config-time-range)# periodic Monday Tuesday Friday 10:30 to 12:30
hostname(config-time-range)#
```

関連コマンド

コマンド	説明
absolute	時間範囲が有効である絶対時間を定義します。
access-list extended	セキュリティ アプライアンスへの IP トラフィックを許可または拒否するポリシーを設定します。
default	***time-range*** コマンドの ***absolute*** キーワードおよび ***periodic*** キーワードのデフォルト設定を復元します。
time-range	時間に基づいてセキュリティ アプライアンスのアクセス コントロールを定義します。

permit errors

無効な GTP パケットを許可する、または許可しないと解析が失敗してドロップされるパケットを許可するには、GTP マップ コンフィギュレーション モードで **permit errors** 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します。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。

permit errors

no permit errors

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

デフォルトでは、無効なパケットまたは解析中に失敗したパケットは、すべてドロップされます。

コマンドのモード

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
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

無効なパケット、またはセキュリティ アプライアンスを通じて送信されるメッセージの検査中にエラーが発生したパケットを許可し、それらがドロップされないようにするには、GTP マップ コンフィギュレーション モードで **permit errors** コマンドを使用します。

例

次の例では、無効なパケットまたは解析中に失敗したパケットが含まれたトラフィックを許可します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit errors
```

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。
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用に特定の GTP マップを適用します。
permit response	ロードバランシング GSN をサポートします。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

permit response

ロードバランシング GSN をサポートするには、GTP マップ コンフィギュレーション モードで **permit response** 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。permit response コマンドは、応答の送信先であった GSN とは異なる GSN からの GTP 応答を許可することにより、ロードバランシング GSN をサポートします。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。

permit response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

no permit response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

シンタックスの説明

from-object-group *from_obj_group_id*	**object-group** コマンドにより設定されたオブジェクトグループの名前を指定します。このコマンドでは、*to_obj_group_id* 引数で指定したオブジェクトグループ内の GSN の集合に対して応答を送信できます。セキュリティ アプライアンスがサポートするのは、IPv4 アドレスを持つネットワーク オブジェクトを含んだオブジェクトグループのみです。IPv6 アドレスは、現時点では GTP でサポートされていません。
to-object-group *to_obj_group_id*	**object-group** コマンドにより設定されたオブジェクトグループの名前を指定します。このコマンドでは、*rom_obj_group_id* 引数で指定したオブジェクトグループ内の GSN の集合から応答を受信できます。セキュリティ アプライアンスがサポートするのは、IPv4 アドレスを持つネットワーク オブジェクトを含んだオブジェクトグループのみです。IPv6 アドレスは、現時点では GTP でサポートされていません。

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、要求送信先のホスト以外の GSN からの GTP 応答をドロップします。

コマンドのモード

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
7.0(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

ロードバランシング GSN をサポートするには、GTP マップ コンフィギュレーション モードで **permit response** コマンドを使用します。**permit response** コマンドを使用して、応答の送信先であった GSN とは異なる GSN からの、GTP 応答を許可するように GTP マップを設定します。

ロードバランシング GSN のプールをネットワーク オブジェクトとして指定します。同様に、SGSN をネットワーク オブジェクトとして指定します。応答する GSN が、GTP 要求の送信先であった GSN と同じオブジェクト グループに属する場合、また応答する GSN が GTP 応答を送信できるオブジェクト グループに SGSN がある場合、セキュリティ アプライアンスはその応答を許可します。

例

次の例では、192.168.32.0 ネットワーク上の任意のホストから IP アドレス 192.168.112.57 を持つホストへの GTP 応答を許可します。

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.32.0 255.255.255.0
hostname(config)# object-group network sgsn1
hostname(config-network)# network-object host 192.168.112.57
hostname(config-network)# exit
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit response to-object-group sgsn1 from-object-group
gsnpool32
```

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。
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用に特定の GTP マップを適用します。
permit errors	無効な GTP パケットを許可します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

pfs

PFS をイネーブルにするには、グループポリシー コンフィギュレーション モードで **pfs enable** コマンドを使用します。PFS をディセーブルにするには、**pfs disable** コマンドを使用します。PFS アトリビュートを実行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。このオプションを使用すると、PFS の値を別のグループポリシーから継承できます。

IPSec ネゴシエーションで、PFS は新しい暗号鍵が以前のどの鍵とも無関係であることを保証します。

pfs {enable | disable}

no pfs

シンタックスの説明

disable	PFS をディセーブルにします。
enable	PFS をイネーブルにします。

デフォルト

PFS はディセーブルになっています。

コマンドのモード

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	•	—	•	—	—

コマンド履歴

リリース	変更
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

VPN クライアントとセキュリティ アプライアンスの PFS 設定は一致する必要があります。

例

次の例は、FirstGroup というグループポリシーの PFS を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# pfs enable
```

pim

インターフェイス上の PIM 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 **pim** コマンドを使用します。PIM 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。

pim

no pim

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 をイネーブルにします。

コマンドのモード

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
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、デフォルトではすべてのインターフェイスの PIM をイネーブルにします。**no** 形式の **pim** コマンドだけがコンフィギュレーションに保存されます。

（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。

例

次の例では、選択したインターフェイス上の PIM をディセーブルにします。

```
hostname(config-if)# no pim
```

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。

pim accept-register

PIM 登録メッセージがフィルタリングされるようにセキュリティ アプライアンスを設定するには、グローバル コンフィギュレーション モードで **pim accept-register** コマンドを使用します。フィルタリ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。

pim accept-register {***list*** *acl* | ***route-map*** *map-name*}

no pim accept-register

シンタックスの説明

list *acl*	アクセスリストの名前または番号を指定します。このコマンドでは、標準ホスト 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。
route-map *map-name*	ルートマップ名を指定します。参照先のルートマップでは、標準ホスト ACL を使用してください。拡張 ACL はサポートされていません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

非認証の送信元が RP に登録されないようにするには、このコマンドを使用します。非認証の送信元が RP に登録メッセージを送信すると、セキュリティ アプライアンスはただちに登録中止メッセージを送信します。

例

次の例では、PIM 登録メッセージを、「no-ssm-range」というアクセスリストに定義されている送信元からのものに制限します。

```
hostname(config)# pim accept-register list no-ssm-range
```

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。

pim dr-priority

指定ルータの選定に使用されるネイバーの優先順位をセキュリティ アプライアンス上に設定するには、インターフェイス コンフィギュレーション モードで **pim dr-priority** コマンドを使用します。デフォルトの優先順位に戻すには、このコマンドの **no** 形式を使用します。

pim dr-priority *number*

no pim dr-priority

シンタックスの説明

number	0 ～ 4294967294 の任意の数字。この数字は、指定ルータを判別するときに、デバイスの優先順位を判別するために使用されます。0 に指定すると、セキュリティ アプライアンスは指定ルータに選定されません。

デフォルト

デフォルト値は 1 です。

コマンドのモード

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
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

インターフェイス上の優先順位値が最も大きいデバイスが、PIM 指定ルータになります。複数のデバイスで同じ指定ルータ優先順位値が設定されている場合、IP アドレスが最大のデバイスが指定ルータになります。デバイスの hello メッセージに DR-Priority Option（指定ルータ優先順位オプション）が含まれていない場合は、そのデバイスが最も優先順位の高いデバイスであると見なされ、指定ルータになります。hello メッセージにこのオプションが含まれていないデバイスが複数ある場合は、最大の IP アドレスを持つデバイスが指定ルータになります。

例

次の例は、インターフェイスの指定ルータ優先順位を 5 に設定します。

```
hostname(config-if)# pim dr-priority 5
```

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。

pim hello-interval

PIM hello メッセージの頻度を設定するには、インターフェイス コンフィギュレーション モードで **pim hello-interval** コマンドを使用します。hello 間隔を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。

pim hello-interval *seconds*

no pim hello-interval [*seconds*]

シンタックスの説明

seconds	セキュリティ アプライアンスが hello メッセージを送信する前に待機する秒数。有効となる値の範囲は、1 ～ 3,600 秒です。デフォルト値は 30 秒です。

デフォルト

30 秒

コマンドのモード

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
7.0(1)	このコマンドが導入されました。

例

次の例では、PIM hello 間隔を 1 分に設定します。

```
hostname(config-if)# pim hello-interval 60
```

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。

pim join-prune-interval

PIM join/prune 間隔を設定するには、インターフェイス コンフィギュレーション モードで **pim join-prune-interval** コマンドを使用します。この間隔を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。

pim join-prune-interval *seconds*

no pim join-prune-interval [*seconds*]

シンタックスの説明

seconds	セキュリティ アプライアンスが join/prune メッセージを送信する前に待機する秒数。有効となる値の範囲は、10 ～ 600 秒です。デフォルトは、60 秒です。

デフォルト

60 秒

コマンドのモード

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
7.0(1)	このコマンドが導入されました。

例

次の例では、PIM join/prune 間隔を 2 分に設定します。

```
hostname(config-if)# pim join-prune-interval 120
```

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。

pim old-register-checksum

古い登録チェックサム方法論を使用する Rendezvous Point（RP; ランデブー ポイント）上の下位互換性を許可するには、グローバル コンフィギュレーション モードで **pim old-register-checksum** コマンドを使用します。PIM RFC 準拠の登録を生成するには、このコマンドの **no** 形式を使用します。

pim old-register-checksum

no pim old-register-checksum

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

セキュリティ アプライアンスは、PIM RFC 準拠の登録を生成します。

コマンドのモード

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
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 ソフトウェアは、PIM ヘッダーにチェックサムがある登録メッセージと、（Cisco IOS 方式を使用せずに）その次の 4 バイトだけを受け入れます。つまり、すべての PIM メッセージ タイプ用の完全な PIM メッセージがある登録メッセージを受け入れます。**pim old-register-checksum** コマンドは、Cisco IOS ソフトウェアと互換性のある登録を生成します。

例

次の例では、古いチェックサム計算を使用するようにセキュリティ アプライアンスを設定します。

```
hostname(config)# pim old-register-checksum
```

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。

pim rp-address

PIM Rendezvous Point（RP; ランデブー ポイント）のアドレスを設定するには、グローバル コンフィギュレーション モードで **pim rp-address** コマンドを使用します。RP アドレスを削除するには、このコマンドの **no** 形式を使用します。

pim rp-address *ip_address* [*acl*] [***bidir***]

no pim rp-address *ip_address*

シンタックスの説明

acl	（オプション）RP とともに使用するマルチキャスト グループを定義する、アクセスリストの名前または番号。これが標準の IP アクセスリストです。
bidir	（オプション）指定したマルチキャスト グループが、双方向モードで動作することを示します。このオプションを使用しないでコマンドを設定した場合、指定したグループは PIM 希薄モードで動作します。
ip_address	PIM RP として使用するルータの IP アドレス。これは、4 分割ドット 10 進表記のユニキャスト IP アドレスです。

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

PIM RP アドレスは設定されていません。

コマンドのモード

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
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

共通の PIM 希薄モード（PIM-SM）または双方向ドメイン内にあるすべてのルータは、周知の PIM RP アドレスの情報を必要とします。アドレスは、このコマンドを使用してスタティックに設定します。

（注）　セキュリティ アプライアンスは、Auto-RP をサポートしていません。したがって、**pim rp-address** コマンドを使用して、RP アドレスを指定する必要があります。

1 つの RP で複数のグループが処理されるように設定できます。アクセスリストで指定されているグループ範囲により、PIM RP グループ マッピングが決まります。アクセスリストが指定されていない場合、グループの RP は、IP マルチキャスト グループ範囲全体（224.0.0.0/4）に適用されます。

（注）　セキュリティ　アプライアンスは、実際の双方向コンフィギュレーションにかかわらず、常に、双方向機能を PIM hello メッセージ内でアドバタイズします。

例

次の例では、すべてのマルチキャスト グループの PIM RP アドレスに 10.0.0.1 を設定します。

```
hostname(config)# pim rp-address 10.0.0.1
```

関連コマンド

コマンド	説明
pim accept-register	PIM 登録メッセージをフィルタリングするように、候補 RP を設定します。

pim spt-threshold infinity

最後のホップ ルータの動作を、常に共有ツリーを使用し、Shortest-Path Tree（SPT; 最短パス ツリー）への切り替えを決して実行しないように変更するには、グローバル コンフィギュレーション モードで **pim spt-threshold infinity** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

pim spt-threshold infinity [***group-list*** *acl*]

no pim spt-threshold

シンタックスの説明

group-list *acl*	（オプション）アクセスリストで制限されている送信元グループを指定します。*acl* 引数には、標準 ACL を指定する必要があります。拡張 ACL はサポートされていません。

デフォルト

デフォルトでは、最後のホップ PIM ルータは最短パス送信元ツリーに切り替えます。

コマンドのモード

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
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

group-list キーワードを使用しない場合、このコマンドはすべてのマルチキャスト グループに適用されます。

例

次の例では、最短パス送信元ツリーに切り替えるのではなく、常に共有ツリーを使用するように最後のホップ PIM ルータを設定します。

```
hostname(config)# pim spt-threshold infinity
```

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。

ping

セキュリティ アプライアンスから他の IP アドレスが可視であるかどうかを判別するには、特権 EXEC モードで **ping** コマンドを使用します。

ping [*if_name*] *host* [**data** *pattern*] [**repeat** *count*] [**size** *bytes*] [**timeout** *seconds*] [**validate**]

シンタックスの説明

***data** pattern*	（オプション）16 ビット データ パターンを 16 進数で指定します。
host	ping 対象のホストの IPv4 または IPv6 アドレス、または名前を指定します。
if_name	（オプション）*host* へのアクセスに使用できる、***nameif*** コマンドで設定されたインターフェイス名を指定します。指定しない場合、*host* は解決されて IP アドレスに変換され、ルーティング テーブルを参照することで宛先インターフェイスが判別されます。
***repeat** count*	（オプション）ping 要求を繰り返す回数を指定します。
***size** bytes*	（オプション）データグラム サイズをバイト単位で指定します。
timeout *seconds*	（オプション）ping 要求がタイムアウトになるまでの秒数を指定します。
validate	（オプション）応答データを検証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。

コマンドのモード

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
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

ping コマンドでは、セキュリティ アプライアンスに接続があるかどうか、またはホストがネットワークで利用可能であるかどうかを判別できます。セキュリティ アプライアンスに接続がある場合は、**icmp permit any** *interface* コマンドが設定されていることを確認します。このコンフィギュレーションは、***ping*** コマンドで生成されたメッセージの応答および受け入れをセキュリティ アプライアンスに許可するために必要です。***ping*** コマンドの出力には、応答が受信されたかどうかが示されます。**ping** コマンドを入力したとき、ホストが応答していない場合は、次のようなメッセージが表示されます。

```
hostname(config)# ping 10.1.1.1
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

セキュリティ アプライアンスがネットワークに接続されていること、およびトラフィックの受け渡しを実行していることを確認するには、***show interface*** コマンドを使用します。指定した *if_name* のアドレスは ping の送信元アドレスとして使用されます。

内部ホストから外部ホストに ping を送信する場合は、次のいずれかを実行する必要があります。

- エコー応答用の ICMP ***access-list*** コマンドを作成します。たとえば、ping アクセスをすべてのホストに許可するには、***access-list acl_grp permit icmp any any*** コマンドを使用します。***access-group*** コマンドを使用して、テストの対象であるインターフェイスに ***access-list*** コマンドをバインドします。
- **inspect icmp** コマンドを使用して、ICMP 検査エンジンを設定します。たとえば、**inspect icmp** コマンドをグローバル サービス ポリシーの **class default_inspection** クラスに追加すると、内部ホストによって開始されたエコー要求に対する、セキュリティ アプライアンスを経由したエコー応答が許可されます。

拡張 ping を実行することもできます。拡張 ping では、キーワードを一度に 1 行ずつ入力できます。

ホスト間またはルータ間でセキュリティ アプライアンスを介して ping を実行しているときに ping が成功しない場合は、**capture** コマンドを使用して ping の成功を監視できます。

セキュリティ アプライアンス **ping** コマンドでは、インターフェイス名は必須ではありません。インターフェイス名が指定されていない場合、セキュリティ アプライアンスは、ルーティング テーブルをチェックして指定されたアドレスを検索します。インターフェイス名を指定して、ICMP エコー要求が送信されるときに経由するインターフェイスを指示できます。

例

次の例は、他の IP アドレスがセキュリティ アプライアンスから可視であるかどうかを判別する方法を示しています。

```
hostname# ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

次に、拡張 ping の例を示します。

```
hostname# ping
Interface: outside
Target IP address: 171.69.38.1
Repeat count: [5]
Datagram size: [100]
Timeout in seconds: [2]
Extended commands [n]:
Sweep range of sizes [n]:
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

関連コマンド

コマンド	説明
capture	インターフェイスでパケットをキャプチャします。
icmp	インターフェイスで終端する ICMP トラフィックに対して、アクセス規則を設定します。
show interface	VLAN コンフィギュレーションについての情報を表示します。

police

厳密なスケジューリング優先順位をこのクラスに適用するには、クラス モードで **police** コマンドを使用します。レート制限要件を削除するには、このコマンドの **no** 形式を使用します。

police [output] *conform-rate* {*conform-burst* | **conform-action {drop | transmit} | exceed-action {drop | transmit}}**

no police

シンタックスの説明

conform-action	レートが conform-burst の値より小さいときに実行されるアクション。
conform-burst	1,000 ～ 512,000,000 の範囲の値。適合レート値にスロットリングするまでに持続的なバーストで許容される最大瞬間バイト数を指定します。
conform-rate	このトラフィック フローのレート限度。8,000 ～ 2,000,000,000 の任意の値で、許容される最大速度（ビット / 秒）を指定します。
drop	パケットをドロップします。
exceed-action	このアクションは、レートが conform-rate 値と conform-burst 値の間であるときに実行されます。
output	出力方向に流れるトラフィックのポリシングをイネーブルにします。
transmit	パケットを伝送します。

デフォルト

デフォルトの動作や変数はありません。

コマンドのモード

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	—	—	•	—	—

コマンド履歴

リリース	変更
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

police コマンドを発行するには、**policy-map** コマンドと **class** コマンドをあらかじめ設定しておく必要があります。

（注） **police** コマンドは、最大速度および最大バースト レートを強制し、それらの値を適合レート値に強制的に合わせるだけです。***conform-action*** または ***exceed-action*** の指定内容は、存在する場合でも強制されません。

着信方向のトラフィックのポリシングは、サポートされていません。

優先順位とポリシングを、両方ともイネーブルにすることはできません。

既存の VPN クライアント トラフィック、LAN-to- LAN トラフィック、または非トンネル トラフィックが確立されているインターフェイスを対象として、サービス ポリシーを適用または削除した場合、QoS ポリシーは適用されず、トラフィック ストリームから削除されません。このような接続を対象として QoS ポリシーを適用または削除するには、接続を消去（ドロップ）して再確立する必要があります。

例

次に、**police** コマンドの例を示します。適合レート 100,000 ビット / 秒、バースト値 2,000,000 バイトを設定し、バースト レートを超過したトラフィックをドロップすることを指定しています。

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class firstclass class
hostname(config-pmap-c)# police 100000 20000 exceed-action drop
hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)# police 1000000 200000 exceed-action drop
hostname(config-pmap-c)# exit
```

関連コマンド

class	トラフィックの分類に使用するクラスマップを指定します。
clear configure policy-map	すべてのポリシーマップ コンフィギュレーションを削除します。ただし、ポリシーマップが service-policy コマンド内で使用されている場合、そのポリシーマップは削除されません。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
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。

policy

CRL を取得するための送信元を指定するには、ca-crl コンフィギュレーション モードで **policy** コマンドを使用します。

policy {***static*** | ***cdp*** | ***both***}

シンタックスの説明

both	CRL 配布ポイントを使用して CRL を取得することに失敗した場合は最大 5 つのスタティック CRL 配布ポイントを使用してリトライすることを、指定します。
cdp	チェック中の証明書に組み込まれた、CRL 配布ポイント拡張を使用します。この場合、セキュリティ アプライアンスは、チェック中の証明書の CRL 配布ポイント拡張から最大 5 つの CRL 配布ポイントを取得し、必要に応じて、設定されたデフォルト値で情報を増強します。セキュリティ アプライアンスは、プライマリ CRL 配布ポイントを使用して CRL を取得することに失敗した場合、リストにある次に利用可能な CRL 配布ポイントを使用してリトライします。これは、セキュリティ アプライアンスが CRL を取得するか、リストを使い果たすまで続行されます。
static	最大 5 つのスタティック CRL 配布ポイントを使用します。このオプションを指定する場合は、**protocol** コマンドで LDAP または HTTP URL も指定してください。

デフォルト

デフォルト設定は **cdp** です。

コマンドのモード

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
CRL コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、ca-crl コンフィギュレーション モードに入り、チェック中の証明書内の CRL 配布ポイントを使用して CRL 取得を実行すること、それに失敗した場合は、スタティック CRL 配布ポイントを使用することを設定します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# policy both
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
url	CRL を取得するためのスタティック URL のリストを作成および維持します。

policy-map

ポリシーを設定するには、グローバル コンフィギュレーション モードで **policy-map** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

policy-map *name*

no policy-map *name*

シンタックスの説明

name	このポリシーマップの名前。名前には、最大 40 文字を使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
7.0(1)	このコマンドはこのリリースで導入されました。

使用上のガイドライン

policy-map コマンドは、ポリシー（トラフィック クラスと 1 つまたは複数のセキュリティ関連のアクションのアソシエーション）を設定します。トラフィック クラスは、パケットの内容で識別可能な一連のトラフィックです。たとえば、ポート値 23 を持つ TCP トラフィックは、Telnet トラフィック クラスとして分類できます。ポリシーは、1 つの **class** コマンドと、関連付けられたアクションで構成されます。ポリシーマップでは、複数のポリシーを指定できます。**service-policy** コマンドでは、ポリシーマップをすべてのインターフェイス上でグローバルに有効にするか、目的のインターフェイス 1 つだけで有効にすることができます。

policy-map コマンドを使用すると、トラフィックを分類し、分類したトラフィックに機能固有のアクションを適用できます。

ポリシーマップの最大数は 64 です。

ポリシーマップ モードに入るには、**policy-map** コマンドを使用します。このモードで、**class** コマンドおよび **description** コマンドを入力できます。詳細については、個々のコマンドの説明を参照してください。

ポリシーマップ内の各種アクションが実行される順序は、これらのコマンド記述でアクションが出現する順序とは関係ありません。

例

次に、**policy-map** コマンドの例を示します。プロンプトの変化に注目してください。

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)#
```

次に、接続ポリシーに対する **policy-map** コマンドの例を示します。

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server

hostname(config-cmap)# match access-list http-server
hostname(config-cmap)# exit

hostname(config)# policy-map global-policy global
hostname(config-pmap)# description This policy map defines a policy concerning
connection to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

次に、「外部」インターフェイスに対する **policy-map** コマンドの例を示します。

```
hostname(config)# class-map outside-voip
hostname(config-cmap)# match ip rtp 2000 100
hostname(config-cmap)# exit

hostname(config)# policy-map outside-policy
hostname(config-pmap)# description This policy map defines policies for the outside
interface.
hostname(config-pmap)# class outside-voip
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# exit
hostname(config-pmap)#
```

関連コマンド

コマンド	説明
class	トラフィックの分類に使用するクラスマップを指定します。
clear configure policy-map	すべてのポリシーマップ コンフィギュレーションを削除します。ただし、ポリシーマップが service-policy コマンド内で使用されている場合、そのポリシーマップは削除されません。
description	ポリシーマップの説明を指定します。
help policy-map	policy-map コマンド シンタックスのヘルプを表示します。
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。

polltime interface

インターフェイス上の hello パケット間の間隔を指定するには、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 **polltime interface** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

polltime interface *time*

no polltime interface *time*

シンタックスの説明

time	hello メッセージの間隔。

デフォルト

デフォルトは、15 秒です。

コマンドのモード

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
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

現在のフェールオーバー グループと関連付けられたインターフェイスから hello パケットが送信される頻度を変更するには、**polltime interface** コマンドを使用します。ポーリング間隔が短いほど、セキュリティ アプライアンスは、それだけ速く障害を検出して、フェールオーバーを起動できます。ただし、検出が速すぎると、ネットワークが一時的に輻輳したときに不要な切り替えが発生する可能性があります。

インターフェイスの hello パケットが 5 回連続で検出されなかった場合は、インターフェイスのテストが発生します。

このコマンドを使用できるのは、Active/Active フェールオーバーに対してのみです。

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)# polltime interface 20
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 polltime	監視対象インターフェイスの hello パケット間の時間を設定します。

pop3s

POP3S コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **pop3s** コマンドを使用します。POP3S コマンド モードで入力したコマンドを削除するには、このコマンドの **no** バージョンを使用します。

POP3 は、インターネット サーバが電子メールを受信し、保持するために使用するクライアント / サーバ プロトコルです。受信者（または受信者のクライアント電子メール レシーバー）は、サーバ上のメールボックスを定期的に確認し、電子メールがあればダウンロードします。この標準プロトコルは、一般的な電子メール製品に組み込まれています。POP3S を使用すると、SSL 接続で電子メールを受信できます。

pop3s

no pop3

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。

コマンドのモード　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
7.0(1)	このコマンドが導入されました。

例　次の例は、POP3S コンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# pop3s
hostname(config-pop3s)#
```

関連コマンド

コマンド	説明
clear configure pop3s	POP3S コンフィギュレーションを削除します。
show running-config pop3s	POP3S の実行コンフィギュレーションを表示します。

port

電子メール プロキシがリスンするポートを指定するには、適切な電子メール プロキシ モードで **port** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

port {*portnum*}

no port

シンタックスの説明

portnum	電子メール プロキシが使用するポート。ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。

デフォルト

電子メール プロキシのデフォルト ポートは、次のとおりです。

電子メール プロキシ	デフォルト ポート
IMAP4S	993
POP3S	995
SMTPS	988

コマンドのモード

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
Pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更
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

ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。

例

次の例は、IMAP4S 電子メール プロキシのポートを 1066 に設定する方法を示しています。

```
hostname(config)# imap4s
hostname(config-imap4s)# port 1066
```

port-forward

転送 TCP ポートを介して WebVPN ユーザがアクセスできるアプリケーションのセットを設定するには、グローバル コンフィギュレーション モードで **port-forward** コマンドを使用します。複数のアプリケーションへのアクセスを設定するには、このコマンドを同じ listname で複数回（アプリケーションごとに 1 回）使用します。設定したリスト全体を削除するには、**no port-forward** *listname* コマンドを使用します。設定したアプリケーションを削除するには、**no port-forward** *listname localport* コマンドを使用します（*remoteserver* パラメータおよび *remoteport* パラメータを含める必要はありません）。

port-forward {*listname localport remoteserver remoteport description*}

no port-forward *listname*

no port-forward *listname localport*

シンタックスの説明

description	エンド ユーザのポート転送 Java アプレット画面に表示する、アプリケーション名または簡単な説明を入力します。最大 64 文字です。
listname	WebVPN ユーザがアクセスできるアプリケーション（転送 TCP ポート）のセットをグループ化します。最大 64 文字です。
localport	アプリケーションの TCP トラフィックをリスンするローカル ポートを指定します。ローカル ポート番号は、*listname* に対して一度だけ使用できます。
remoteport	このアプリケーションが接続するリモート サーバ上のポートを指定します。
remoteserver	リモート サーバの DNS 名または IP アドレスをアプリケーション用に入力します。DNS 名を使用することをお勧めします。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

デフォルト

デフォルトのポート転送リストはありません。

コマンドのモード

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 モード	•	—	•	—	—

コマンド履歴

リリース	変更
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

特定の TCP ポート転送アプリケーションへのアクセスを特定のユーザまたはグループポリシーに許可するには、webvpn モードの **port-forward** コマンドで、ここで作成した *listname* を使用します。

例

次の例は、IMAP4S 電子メール、SMTPS 電子メール、DDTS、および Telnet へのアクセスを提供する *SalesGroupPorts* というポート転送リストを作成する方法を示しています。次の表に、この例で使用されている、各アプリケーションの値を示します。

アプリケーション	ローカル ポート	サーバ DNS 名	リモート ポート	説明
IMAP4S 電子メール	143	IMAP4Sserver	20143	Get Mail
SMTPS 電子メール	25	SMTPSserver	20025	Send Mail
DDTS over SSH	22	DDTSserver	20022	DDTS over SSH
Telnet	23	Telnetserver	20023	Telnet

```
hostname(config)# port-forward SalesGroupPorts 143 IMAP4Sserver 20143 Get Mail
hostname(config)# port-forward SalesGroupPorts 25 SMTPSserver 20025 Send Mail
hostname(config)# port-forward SalesGroupPorts 22 DDTSserver 20022 DDTS over SSH
hostname(config)# port-forward SalesGroupPorts 23 Telnetserver 20023 Telnet
```

関連コマンド

コマンド	説明
clear configuration port-forward [*listname***]**	すべてのポート転送コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスはそのリストのコマンドのみ削除します。
port-forward	ユーザまたはグループポリシーの WebVPN アプリケーション アクセスをイネーブルにするには、webvpn モードでこのコマンドを使用します。
show running-config port-forward	現在設定されている **port-forward** コマンドのセットを表示します。
webvpn	グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	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。WebVPN のグローバル コンフィギュレーション値を設定できます。

port-forward (webvpn)

WebVPN アプリケーション アクセスをこのユーザまたはグループポリシーに対してイネーブルにするには、webvpn モードで **port-forward** コマンドを使用します。このモードには、グループポリシー モードまたはユーザ名モードから入ります。**port-forward none** コマンドを発行することで作成されたヌル値を含む、ポート転送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。**no** オプションを使用すると、リストを別のグループポリシーから継承できます。ポート転送リストを継承しないようにするには、**port-forward none** コマンドを使用します。

port-forward {**value** *listname* | **none**}

no port-forward

シンタックスの説明

none	フィルタリングを実行しないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリングの値を継承しないようにします。
value listname	WebVPN ユーザがアクセスできるアプリケーションのリストを指定します。リストを定義するには、コンフィギュレーション モードで port-forward コマンドを使用します。

デフォルト

デフォルトでは、ポート転送はディセーブルになっています。

コマンドのモード

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
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

コマンドを 2 回使用すると、先行する設定値が上書きされます。

webvpn モードで **port-forward** コマンドを使用してアプリケーション アクセスをイネーブルにする前に、WebVPN 接続で使用することをユーザに許可するアプリケーションのリストを定義する必要があります。このリストを定義するには、グローバル コンフィギュレーション モードで **port-forward** コマンドを使用します。

例

次の例は、*ports1* というポート転送リストを FirstGroup というグループポリシーに対して設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward value ports1
```

関連コマンド

コマンド	説明
clear configuration port-forward [*listname***]**	すべてのポート転送コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスはそのリストのコマンドのみ削除します。
port-forward	WebVPN ユーザがアクセスできるアプリケーション（転送ポート）を定義するには、コンフィギュレーション モードでこのコマンドを使用します。
show running-config port-forward	現在設定されている **port-forward** コマンドのセットを表示します。
webvpn	グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	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。WebVPN のグローバル コンフィギュレーション値を設定できます。

port-forward-name

エンド ユーザが TCP ポート転送を識別できる表示名を、特定のユーザまたはグループポリシーに対して設定するには、webvpn モードで **port-forward-name** コマンドを使用します。このモードには、グループポリシー モードまたはユーザ名モードから入ります。**port-forward-name none** コマンドを使用することで作成されたヌル値を含む、表示名を削除するには、このコマンドの no 形式を使用します。**no** オプションを指定すると、デフォルト名の「Application Access」が復元されます。表示名を復元しないようにするには、**port-forward none** コマンドを使用します。

port-forward-name {**value** *name* | **none**}

no port-forward-name

シンタックスの説明

none	表示名がないことを指定します。ヌル値を設定して、表示名を拒否します。値を継承しないようにします。
value *name*	エンド ユーザに対してポート転送を説明します。最大 255 文字です。

デフォルト

デフォルト名は「Application Access」です。

コマンドのモード

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	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例は、「Remote Access TCP Applications」という名前を FirstGroup というグループポリシーに対して設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
```

関連コマンド

コマンド	説明
webvpn	グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	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。WebVPN のグローバル コンフィギュレーション値を設定できます。

port-misuse

制限するアプリケーション カテゴリを指定することで 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 **port-misuse** 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。

port-misuse {**im** | **p2p** | **tunneling** | **default**} **action** {**allow** | **reset** | **drop**} [**log**]

no port-misuse {**im** | **p2p** | **tunneling** | **default**} **action** {**allow** | **reset** | **drop**} [**log**]

シンタックスの説明

action	設定されたカテゴリのアプリケーションが検出されたときに実行されるアクションを指定します。
allow	メッセージを許可します。
default	サポートされている要求メソッドがトラフィックに含まれていて、そのメソッドが設定済みリストに記載されていない場合に、セキュリティ アプライアンスが実行するデフォルト アクションを指定します。
im	インスタント メッセージ アプリケーション カテゴリのトラフィックを制限します。チェック対象のアプリケーションは、Yahoo Messenger、AIM、および MSN IM です。
log	（オプション）syslog を生成します。
p2p	ピアツーピア アプリケーション カテゴリのトラフィックを制限します。Kazaa アプリケーションがチェックされます。
reset	クライアントまたはサーバに TCP リセット メッセージを送信します。
tunneling	トンネリング アプリケーション カテゴリのトラフィックを制限します。チェック対象のアプリケーションは、HTTPort/HTTHost、GNU Httptunnel、GotoMyPC、Firethru、および Http-tunnel.com Client 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。このコマンドがイネーブルで、サポートされているアプリケーション カテゴリが指定されていないときのデフォルト アクションは、ロギングなしで接続を許可することです。デフォルト アクションを変更するには、**default** キーワードを使用して別のデフォルト アクションを指定します。

コマンドのモード

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
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

port-misuse 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、サポートおよび設定されている各アプリケーション カテゴリの HTTP 接続に対して、指定されているアクションを適用します。

セキュリティ アプライアンスは、設定済みリストにあるアプリケーション カテゴリに一致しないすべてのトラフィックに対して、**default** アクションを適用します。事前設定済みの **default** アクションでは、接続をロギングなしで **allow** します。

たとえば、事前設定済みのデフォルト アクションでは、**drop** および **log** というアクションを持つ 1 つまたは複数のアプリケーション カテゴリを指定すると、セキュリティ アプライアンスは、設定済みアプリケーション カテゴリが含まれている接続をドロップし、各接続をロギングし、サポートされているその他のアプリケーション タイプのすべての接続を許可します。

より厳しいポリシーを設定する場合は、デフォルト アクションを **drop**（または **reset**）および **log** に変更します（イベントをログに記録する場合）。その後、**allow** アクションで、許可する各アプリケーション タイプを設定します。

適用する設定ごとに 1 回、**port-misuse** コマンドを入力します。**port-misuse** コマンドのインスタンスを、デフォルト アクションを変更するために 1 つ、各アプリケーション カテゴリを設定済みアプリケーション タイプのリストに追加するために 1 つ使用します。

注意　これらの検査では、HTTP メッセージのエンティティ本体内の検索が必要なため、セキュリティ アプライアンスのパフォーマンスが影響を受ける場合があります。

このコマンドの **no** 形式を使用して、アプリケーション カテゴリを設定済みアプリケーション タイプのリストから削除する場合、コマンドラインでアプリケーション カテゴリ キーワードの後にある文字はすべて無視されます。

例

次の例では、事前設定済みのデフォルトを使用して、緩やかなポリシーを指定しています。サポートされているすべてのアプリケーション タイプを、個別に拒否されていない限り許可します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# port-misuse p2p drop log
hostname(config-http-map)# exit
```

この場合、ピアツーピア カテゴリの接続だけがドロップされ、イベントがロギングされます。

次の例では、厳しいポリシーを設定しています。デフォルト アクションは、個別に許可されていないすべてのアプリケーション タイプの接続をリセットし、イベントをロギングするように変更されています。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# port-misuse default action reset log
hostname(config-http-map)# port-misuse im allow
hostname(config-http-map)# exit
```

この場合、Instant Messenger アプリケーションだけが許可されます。サポートされているその他のアプリケーションの HTTP トラフィックが受信された場合、セキュリティ アプライアンスは接続をリセットし、syslog エントリを作成します。

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。

コマンド	説明
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。

port-object

ポート オブジェクトをサービス オブジェクト グループに追加するには、サービス コンフィギュレーション モードで **port-object** コマンドを使用します。ポート オブジェクトを削除するには、このコマンドの **no** 形式を使用します。

port-object eq *service*

no port-object eq *service*

port-object range *begin_service end_service*

no port-object range *begin_service end_service*

シンタックスの説明

begin_service	サービス範囲の開始値である、TCP ポートまたは UDP ポートの 10 進数または名前を指定します。この値は、0 ～ 65535 で指定する必要があります。
end_service	サービス範囲の終了値である、TCP ポートまたは UDP ポートの 10 進数または名前を指定します。この値は、0 ～ 65535 で指定する必要があります。
eq service	サービス オブジェクトに TCP ポートまたは UDP ポートの 10 進数または名前を指定します。
range	ポートの範囲（包含）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。

コマンドのモード

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
サービス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
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

特定のサービス（ポート）またはサービス範囲（複数のポート）のいずれかのオブジェクトを定義するには、**object-group** とともに、**port-object** コマンドをサービス コンフィギュレーション モードで使用します。

TCP サービスまたは UDP サービスの名前を指定する場合、その名前は、TCP、UDP、またはその両方でサポートされている名前のいずれかで、オブジェクト グループのプロトコル タイプと整合性を持つものである必要があります。たとえば、tcp、udp、tcp-udp の各プロトコル タイプの場合、名前はそれぞれ、有効な TCP サービス名、有効な UDP サービス名、TCP および UDP の有効なサービス名である必要があります。

番号を指定した場合、オブジェクトが表示されるときに、プロトコル タイプに基づいて、その番号が対応する名前（存在する場合）に変換されます。

次のサービス名がサポートされています。

表 6-2

TCP	UDP	TCP および UDP
bgp	biff	discard
chargen	bootpc	domain
cmd	bootps	echo
daytime	dnsix	pim-auto-rp
exec	nameserver	sunrpc
finger	mobile-ip	syslog
ftp	netbios-ns	tacacs
ftp-data	netbios-dgm	talk
gopher	ntp	
ident	rip	
irc	snmp	
h323	snmptrap	
hostname	tftp	
http	time	
klogin	who	
kshell	xdmcp	
login	isakmp	
lpd		
nntp		
pop2		
pop3		
smtp		
sqlnet		
telnet		
uucp		
whois		
www		

例

次の例は、サービス コンフィギュレーション モードで **port-object** コマンドを使用して、新しいポート（サービス）オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group service eng_service tcp
hostname(config-service)# port-object eq smtp
hostname(config-service)# port-object eq telnet
hostname(config)# object-group service eng_service udp
hostname(config-service)# port-object eq snmp
hostname(config)# object-group service eng_service tcp-udp
hostname(config-service)# port-object eq domain
hostname(config-service)# port-object range 2000 2005
hostname(config-service)# quit
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
show running-config object-group	現在のオブジェクト グループを表示します。

preempt

装置の優先順位が高い場合に、その装置をブート時にアクティブにするには、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 **preempt** コマンドを使用します。プリエンプ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。

preempt [*delay*]

no preempt [*delay*]

シンタックスの説明

seconds	ピアがプリエンプションされるまでの待ち時間（秒）。有効な値は 1 ～ 1,200 秒です。

デフォルト

デフォルトでは、待ち時間はありません。

コマンドのモード

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
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

プライマリまたはセカンダリの優先順位をフェールオーバー グループに割り当てると、両方の装置が（装置のポーリング時間内で）同時にブートしたときに、フェールオーバー グループがどの装置上でアクティブになるかが指定されます。ただし、ある装置がもう一方の装置よりも先にブートした場合、どちらのフェールオーバー グループもその装置上でアクティブになります。もう一方の装置がオンラインになると、優先順位として 2 番目の装置を持つフェールオーバー グループは、そのフェールオーバー グループが **preempt** コマンドを使用して設定されているか、手作業で **no failover**

active コマンドを使用してもう一方の装置に強制しない限り、2 番目の装置上ではアクティブになりません。フェールオーバー グループが **preempt** コマンドを使用して設定されている場合、そのフェールオーバー グループは、指定装置上で自動的にアクティブになります。

（注）　ステートフル フェールオーバーがイネーブルの場合、フェールオーバー グループが現在アクティブである装置から接続が複製されるまで、プリエンプションは実行されません。

例

次の例では、優先順位の高いプライマリ装置を持つフェールオーバー グループ 1 と、優先順位の高いセカンダリ装置を持つフェールオーバー グループ 2 を設定しています。どちらのフェールオーバー グループも、**preempt** コマンドを使用して待ち時間 100 秒で設定されています。したがって、これらのグループは、優先する装置が利用可能になってから 100 秒後に、その装置上で自動的にアクティブになります。

```
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。
primary	設定しているフェールオーバー グループのフェールオーバー ペア優先順位における、プライマリ装置を指定します。
secondary	設定しているフェールオーバー グループのフェールオーバー ペア優先順位における、セカンダリ装置を指定します。

prefix-list

ABR タイプ 3 LSA フィルタリングのプレフィックス リストのエントリを作成するには、グローバル コンフィギュレーション モードで **prefix-list** コマンドを使用します。プレフィックス 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。

prefix-list *prefix-list-name* [***seq*** *seq_num*] {***permit*** | ***deny***} *network/len* [***ge*** *min_value*] [***le*** *max_value*]

no prefix-list *prefix-list-name* [***seq*** *seq_num*] {***permit*** | ***deny***} *network/len* [***ge*** *min_value*] [***le*** *max_value*]

シンタックスの説明

/	*network* 値と *len* 値の間に必要な区切り記号。
deny	一致した条件へのアクセスを拒否します。
ge *min_value*	（オプション）一致する必要のある最小プレフィックス長を指定します。*min_value* 引数の値は、*len* 引数の値より大きくする必要があります。また、*max_value* 引数が存在する場合は、それ以下にする必要があります。
le *max_value*	（オプション）一致する必要のある最大プレフィックス長を指定します。*max_value* 引数の値は、*min_value* 引数が存在する場合は、その値以上にする必要があり、*min_value* 引数が存在しない場合は、*len* 引数の値より大きくする必要があります。
len	ネットワーク マスクの長さ。有効な値は 0 ～ 32 です。
network	ネットワーク アドレス。
permit	一致した条件へのアクセスを許可します。
prefix-list-name	プレフィックス リストの名前。プレフィックス リスト名にスペースを含めることはできません。
seq *seq_num*	（オプション）指定したシーケンス番号を、作成中のプレフィックス リストに適用します。

デフォルト

シーケンス番号を指定しない場合、プレフィックス リストの最初のエントリにシーケンス番号 5 が割り当てられ、以降の各エントリには、5 ずつ増加するシーケンス番号が割り当てられます。

コマンドのモード

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
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

prefix-list コマンドは、ABR タイプ 3 LSA フィルタリング コマンドです。ABR タイプ 3 LSA フィルタリングによって OSPF 実行中の ABR 機能を拡張し、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されると、指定したプレフィックスだけが一方から他方のエリアに送信されます。その他のプレフィックスは、すべてそれぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアが終点または起点となるトラフィック、あるいはそのエリアの着信および発信両方のトラフィックに適用できます。

プレフィックス リストの複数のエントリが所定のプレフィックスに一致する場合、最も小さいシーケンス番号を持つエントリが使用されます。セキュリティ アプライアンスは、プレフィックス リストの最上部から、つまり最も小さいシーケンス番号を持つエントリから検索を開始します。一致が見つかると、セキュリティ アプライアンスは、リストの残りの部分を調べません。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらをリストの上部に配置することもできます。

デフォルトでは、シーケンス番号は自動的に生成されます。それらは、**no prefix-list sequence-number** コマンドで抑制できます。シーケンス番号は、5 ずつ増分されます。プレフィックス リスト内に最初に生成されるシーケンス番号は 5 です。リスト内の次のエントリのシーケンス番号は 10 となり、以降も同様となります。あるエントリの値を指定し、後続のエントリの値を指定しない場合、生成されるシーケンス番号は、指定した値から 5 ずつ増分されます。たとえば、プレフィックス リストの最初のエントリのシーケンス番号を 3 と指定し、その後シーケンス番号を指定しないで 2 つのエントリを追加した場合、これら 2 つエントリに対して自動的に生成されるシーケンス番号は、8 および 13 となります。

ge キーワードおよび ***le*** キーワードを使用して、*network*/*len* 引数より具体的なプレフィックスと一致する必要のあるプレフィックスの長さの範囲を指定できます。***ge*** キーワードと ***le*** キーワードのいずれも指定しない場合は、完全一致が前提とされます。***ge*** キーワードだけを指定した場合の範囲は、*min_value* ～ 32 です。***le*** キーワードだけを指定した場合の範囲は、*len* ～ *max_value* です。

min_value 引数および *max_value* 引数の値は、次の条件を満たしている必要があります。

len < *min_value* <= *max_value* <= 32

特定のエントリをプレフィックス リストから削除するには、このコマンドの **no** 形式を使用します。プレフィックス リストを削除するには、**clear configure prefix-list** コマンドを使用します。**clear configure prefix-list** コマンドを使用すると、関連付けられた **prefix-list description** コマンドがある場合は、それもコンフィギュレーションから削除されます。

例

次の例では、デフォルト ルート 0.0.0.0/0 を拒否します。

```
hostname(config)# prefix-list abc deny 0.0.0.0/0
```

次の例では、プレフィックス 10.0.0.0/8 を許可します。

```
hostname(config)# prefix-list abc permit 10.0.0.0/8
```

次の例は、プレフィックス 192/8 を持つルートで最大 24 ビットのマスク長を受け入れる方法を示しています。

```
hostname(config)# prefix-list abc permit 192.168.0.0/8 le 24
```

次の例は、プレフィックス 192/8 を持つルートで 25 ビットより大きいマスク長を拒否する方法を示しています。

```
hostname(config)# prefix-list abc deny 192.168.0.0/8 ge 25
```

次の例は、すべてのアドレス空間で 8 ～ 24 ビットのマスク長を許可する方法を示しています。

```
hostname(config)# prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

次の例は、すべてのアドレス空間で 25 ビットより大きいマスク長を拒否する方法を示しています。

```
hostname(config)# prefix-list abc deny 0.0.0.0/0 ge 25
```

次の例は、プレフィックス 10/8 を持つすべてのルートを拒否する方法を示しています。

```
hostname(config)# prefix-list abc deny 10.0.0.0/8 le 32
```

次の例は、プレフィックス 192.168.1/24 を持つルートで長さが 25 ビットより大きいすべてのマスクを拒否する方法を示しています。

```
hostname(config)# prefix-list abc deny 192.168.1.0/24 ge 25
```

次の例は、プレフィックス 0/0 を持つすべてのルートを許可する方法を示しています。

```
hostname(config)# prefix-list abc permit 0.0.0.0/0 le 32
```

関連コマンド

コマンド	説明
clear configure prefix-list	**prefix-list** コマンドを実行コンフィギュレーションから削除します。
prefix-list description	プレフィックス リストの説明を入力できます。
prefix-list sequence-number	プレフィックス リストのシーケンス番号付けをイネーブルにします。
show running-config prefix-list	実行コンフィギュレーション内の **prefix-list** コマンドを表示します。

prefix-list description

プレフィックス リストに説明を追加するには、グローバル コンフィギュレーション モードで **prefix-list description** コマンドを使用します。プレフィックス リストの説明を削除するには、このコマンドの **no** 形式を使用します。

prefix-list *prefix-list-name* **description** *text*

no prefix-list *prefix-list-name* **description** [*text*]

シンタックスの説明

prefix-list-name	プレフィックス リストの名前。
text	プレフィックス リストの説明テキスト。最大で 80 文字入力できます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

prefix-list コマンドおよび **prefix-list description** コマンドは、特定のプレフィックス リスト名に対して任意の順序で入力できます。つまり、プレフィックス リストの説明を入力する前に、プレフィックス リストを作成する必要はありません。**prefix-list description** コマンドは、コンフィギュレーション内で常に、関連付けられたプレフィックス リストの前の行に記述されます。これは、コマンドを入力した順序とは関係ありません。

すでに説明があるプレフィックス リスト エントリに対して **prefix-list description** コマンドを入力した場合、元の説明は新しい説明に置き換えられます。

このコマンドの **no** 形式を使用している場合、テキスト説明を入力する必要はありません。

例

次の例では、MyPrefixList という名前のプレフィックス リストの説明を追加します。**show running-config prefix-list** コマンドは、プレフィックス リストの説明が実行コンフィギュレーションにすでに追加されているものの、プレフィックスリスト自体は設定されていないことを示します。

```
hostname(config)# prefix-list MyPrefixList description A sample prefix list
description
hostname(config)# show running-config prefix-list

!
prefix-list MyPrefixList description A sample prefix list description
!
```

関連コマンド

コマンド	説明
clear configure prefix-list	**prefix-list** コマンドを実行コンフィギュレーションから削除します。
prefix-list	ABR タイプ 3 LSA フィルタリングのプレフィックス リストを定義します。
show running-config prefix-list	実行コンフィギュレーション内の **prefix-list** コマンドを表示します。

prefix-list sequence-number

プレフィックス リストのシーケンス番号付け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 **prefix-list sequence-number** コマンドを使用します。プレフィックス リストのシーケンス番号付け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。

prefix-list sequence-number

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

プレフィックス リストのシーケンス番号付けは、デフォルトでイネーブルになっています。

コマンドのモード

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
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

コンフィギュレーションには、このコマンドの **no** 形式だけが記述されます。このコマンドの **no** 形式がコンフィギュレーションにある場合、シーケンス番号は、手動で設定したものも含めて、コンフィギュレーションの **prefix-list** コマンドから削除されます。また、新しいプレフィックス リスト エントリには、シーケンス番号が割り当てられません。

プレフィックス リストのシーケンス番号付けがイネーブルの場合、すべてのプレフィックス リスト エントリには、デフォルトの番号付け方式（開始値は 5 で、各番号は 5 ずつ増分される）で、シーケンス番号が割り当てられます。番号付けをディセーブルにする前に、シーケンス番号を手動でプレフィックス リスト エントリに割り当てた場合、手動で割り当てた番号が復元されます。自動番号付けがディセーブルになっているときに手動で割り当てたシーケンス番号も復元されます。ただし、番号付けがディセーブルの間、それらのシーケンス番号は表示されません。

例

次の例では、プレフィックス リストのシーケンス番号付けをディセーブルにします。

```
hostname(config)# no prefix-list sequence-number
```

関連コマンド

コマンド	説明
prefix-list	ABR タイプ 3 LSA フィルタリングのプレフィックス リストを定義します。
show running-config prefix-list	実行コンフィギュレーション内の **prefix-list** コマンドを表示します。

pre-shared-key

事前共有キーに基づく IKE 接続をサポートするために事前共有キーを指定するには、トンネルグループ ipsec アトリビュート コンフィギュレーション モードで **pre-shared-key** コマンドを使用します。デフォルト値に戻すには、このコマンドの ***no*** 形式を使用します。

pre-shared-key *key*

no pre-shared-key

シンタックスの説明

key	1 ～ 128 文字の英数字でキーを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
トンネルグループ ipsec アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
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

すべてのトンネルグループ タイプにこのアトリビュートを適用できます。

例

config-ipsec コンフィギュレーション モードで入力された次のコマンドは、209.165.200.225 という名前の IPSec LAN-to-LAN トンネルグループの IKE 接続をサポートするため、事前共有キー XYZX を指定します。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
hostname(config-ipsec)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネルグループを消去します。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネルグループに関連付けます。

primary

フェールオーバー グループに対するプライマリ装置の優先順位を高くするには、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 **primary** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

primary

no primary

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

フェールオーバー グループに対して **primary** または **secondary** が指定されていない場合、そのフェールオーバー グループはデフォルトの **primary** になります。

コマンドのモード

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
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

プライマリまたはセカンダリの優先順位をフェールオーバー グループに割り当てると、両方の装置が（装置のポーリング時間内で）同時にブートしたときに、フェールオーバー グループがどの装置上でアクティブになるかが指定されます。ある装置がもう一方の装置よりも先にブートした場合、どちらのフェールオーバー グループもその装置上でアクティブになります。もう一方の装置がオンラインになると、優先順位として 2 番目の装置を持つフェールオーバー グループは、そのフェールオーバー グループが **preempt** コマンドを使用して設定されているか、手作業で **no failover active** コマンドを使用してもう一方の装置に強制しない限り、2 番目の装置上ではアクティブになりません。

例

次の例では、優先順位の高いプライマリ装置を持つフェールオーバー グループ 1 と、優先順位の高いセカンダリ装置を持つフェールオーバー グループ 2 を設定しています。どちらのフェールオーバー グループも、**preempt** コマンドを使用して設定します。したがって、これらのグループは、優先する装置が利用可能になったとき、その装置上で自動的にアクティブになります。

```
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。
preempt	優先する装置が使用可能になったときに、フェールオーバー グループをその装置上で強制的にアクティブにします。
secondary	セカンダリ装置に、プライマリ装置より高い優先順位を設定します。

priority

厳密なスケジューリング優先順位をこのクラスに適用するには、クラス モードで **priority** コマンドを使用します。優先順位要件を削除するには、このコマンドの **no** 形式を使用します。

priority

no priority

シンタックスの説明

このコマンドには、パラメータも変数もありません。

デフォルト

デフォルトの動作や変数はありません。

コマンドのモード

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	—	—	•	—	—

コマンド履歴

リリース	変更
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

priority コマンドを発行するには、**policy-map** コマンドと **class** コマンドをあらかじめ設定しておく必要があります。

例

次に、ポリシーマップ モードの **priority** コマンドの例を示します。

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class firstclass
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)# exit
```

関連コマンド

class	トラフィックの分類に使用するクラスマップを指定します。
clear configure policy-map	すべてのポリシーマップ コンフィギュレーションを削除します。ただし、ポリシーマップが service-policy コマンド内で使用されている場合、そのポリシーマップは削除されません。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
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。

priority (vpn load balancing)

仮想ロードバランシング クラスタに参加するローカル デバイスの優先順位を設定するには、VPN ロードバランシング モードで **priority** コマンドを使用します。デフォルトの優先順位指定に戻すには、このコマンドの **no** 形式を使用します。

priority *priority*

no priority

シンタックスの説明

priority	このデバイスに割り当てる優先順位（範囲は 1 ～ 10）。

デフォルト

デフォルトの優先順位は、デバイスのモデル番号によって異なります。

モデル番号	デフォルトの優先順位
5520	5
5540	7

コマンドのモード

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
VPN ロードバランシング	—	—	•	—	—

コマンド履歴

リリース	変更
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

まず、**vpn load-balancing** コマンドを使用して、VPN ロードバランシング モードに入る必要があります。

このコマンドは、仮想ロードバランシング クラスタに参加しているローカル デバイスの優先順位を設定します。

優先順位は、1（最低）～ 10（最高）の整数である必要があります。

優先順位は、マスター選定プロセスで、VPN ロードバランシング クラスタ内のどのデバイスがそのクラスタのマスター デバイスまたはプライマリ デバイスになるかを決定する方法の 1 つとして使用されます。マスター選定プロセスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

このコマンドの ***no*** 形式を使用すると、優先順位指定がデフォルト値に戻ります。

例

次に、VPN ロードバランシング コマンド シーケンスの例を示します。これには、現在のデバイスの優先順位を 9 に設定する **priority** コマンドが含まれています。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシング モードに入ります。

priority-queue

インターフェイス上にプライオリティ キューイングを設定するには、グローバル コンフィギュレーション モードで priority-queue 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。

priority-queue *interface-name*

no priority queue *interface-name*

シンタックスの説明

interface-name	プライオリティ キューイングをイネーブル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

デフォルトでは、プライオリティ キューイングはディセーブルになっています。

コマンドのモード

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
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 アプライアンスでは、次の 2 つのトラフィック クラスを使用できます。1 つは優先順位が高く、遅延に影響されやすいトラフィック（音声およびビデオなど）用の Low-Latency Queuing（LLQ; 低遅延キューイング）で、もう 1 つは、それ以外のすべてのトラフィック用のベストエフォート（デフォルト）です。セキュリティ アプライアンスは、優先トラフィックを認識し、適切な Quality of Service（QoS; サービス品質）ポリシーを適用します。プライオリティキューのサイズと項目数を設定することで、トラフィック フローを微調整できます。

プライオリティ キューイングを有効にするには、**priority-queue** コマンドを使用して、インターフェイスのプライオリティキューをあらかじめ作成しておく必要があります。1 つの **priority-queue** コマンドを、**nameif** コマンドで定義できるすべてのインターフェイスに対して適用できます。

priority-queue コマンドを使用すると、プライオリティキュー モードに入ります。モードはプロンプトに表示されます。プライオリティキュー モードでは、いつでも送信キューに入れることができるパケットの最大数（**tx-ring-limit** コマンド）、およびバッファに入れることのできる両タイプ（優先またはベストエフォート）のパケット数を設定できます（**queue-limit** コマンド）。queue-limit の数を超えると、以後のパケットはドロップされます。

指定する tx-ring-limit 値および queue-limit 値は、優先順位の高い低遅延キューとベストエフォートキューの両方に適用されます。tx-ring-limit は、ドライバが許容できる両タイプのパケットの数です。このパケットの処理が終わると、ドライバは輻輳が解消するまで、インターフェイスの先頭にある、パケットをバッファしているキューの処理に戻ります。一般に、これらの 2 つのパラメータを調整することによって、低遅延トラフィックのフローを最適化できます。

キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これが「テール ドロップ」です。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファ サイズを大きくします。

（注） **queue-limit** コマンドと **tx-ring-limit** コマンドの値の範囲の上限は、実行時に動的に決まります。この上限値を表示するには、コマンドラインで **help** または **?** と入力します。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。キューは、使用可能なメモリの量を超えることはできません。理論上の最大パケット数は、2,147,483,647（つまり、全二重時の回線速度が上限）です。

既存の VPN クライアント トラフィック、LAN-to-LAN トラフィック、または非トンネル トラフィックが確立されているインターフェイスを対象として、サービス ポリシーを適用または削除した場合、QoS ポリシーは適用されず、トラフィック ストリームから削除されません。このような接続を対象として QoS ポリシーを適用または削除するには、接続を消去（ドロップ）して再確立する必要があります。

優先順位とポリシングを、両方ともイネーブルにすることはできません。

例

次の例では、test というインターフェイスのプライオリティキューを設定して、キューの上限を 30,000 パケット、送信キューの上限を 256 パケットと指定しています。

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 30000
hostname(priority-queue)# tx-ring-limit 256
```

関連コマンド

コマンド	説明
queue-limit	プライオリティキューに入れることができるパケットの最大数を指定します。この数を超えると、以後のデータはドロップされます。
tx-ring-limit	イーサネット送信ドライバのキューにいつでも入れることができるパケットの最大数を設定します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
clear configure priority-queue	現在のプライオリティキュー コンフィギュレーションを削除します。
show running-config [all] priority-queue	現在のプライオリティキュー コンフィギュレーションを表示します。**all** キーワードを指定すると、現在のすべてのプライオリティキュー、および queue-limit と tx-ring-limit のコンフィギュレーション値が表示されます。

privilege

コマンド特権レベルを設定するには、グローバル コンフィギュレーション モードで **privilege** コマンドを使用します。このコンフィギュレーションを禁止するには、このコマンドの **no** 形式を使用します。

privilege [**show** | **clear** | **configure**] **level** *level* [**mode** {**enable** | **configure**}] **command** *command*

no privilege [**show** | **clear** | **configure**] **level** *level* [**mode** {**enable** | **configure**}] **command** *command*

シンタックスの説明

clear	（オプション）指定されたコマンドに対応する **clear** コマンドの特権レベルを設定します。
command *command*	特権レベルを設定する対象のコマンドを指定します。
configure	（オプション）指定したコマンドの特権レベルを設定します。
level *level*	特権レベルを指定します。有効値は 0 ～ 15 です。
mode enable	（オプション）コマンドのイネーブル モード用のレベルであることを指定します。
mode configure	（オプション）コマンドの設定モード用のレベルであることを指定します。
show	指定されたコマンドに対応する **show** コマンドの特権レベルを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

privilege コマンドを使用すると、セキュリティ アプライアンスのコマンドにユーザ定義の特権レベルを設定できます。このコマンドは、**show** コマンド、および **clear** コマンドという関連するコンフィギュレーションに異なる特権レベルを設定する場合に特に役立ちます。新しい特権レベルを使用する前に、セキュリティ ポリシーでコマンドの特権レベル変更を必ず検証してください。

コマンドおよびユーザに特権レベルが設定されている場合、両者は比較されて指定ユーザが指定コマンドを実行できるかどうかが判別されます。ユーザの特権レベルがコマンドの特権レベルよりも低い場合、ユーザはそのコマンドを実行できません。

特権レベルを切り替えるには、**login** コマンドを使用して別の特権レベルにアクセスし、適切な **logout** コマンド、**exit** コマンド、または **quit** コマンドを使用してそのレベルを終了します。

mode enable キーワードおよび **mode configure** キーワードは、イネーブル モードと設定モードの両方を持つコマンドで使用します。

特権レベルの数字が小さいほど、レベルは低くなります。

（注）　**aaa authentication** コマンドと **aaa authorization** コマンドには、AAA サーバのコンフィギュレーションで使用する前に、定義する新しい特権レベルを入れる必要があります。

例

次の例は、個々のユーザに特権レベル「5」を設定する方法を示しています。

```
username intern1 password pass1 privilege 5
```

次の例は、特権レベル「5」の **show** コマンド セットを定義する方法を示しています。

```
hostname(config)# privilege show level 5 command alias
hostname(config)# privilege show level 5 command apply
hostname(config)# privilege show level 5 command arp
hostname(config)# privilege show level 5 command auth-prompt
hostname(config)# privilege show level 5 command blocks
```

次の例は、特権レベル 11 を AAA 許可コンフィギュレーション全体に適用する方法を示しています。

```
hostname(config)# privilege configure level 11 command aaa
hostname(config)# privilege configure level 11 command aaa-server
hostname(config)# privilege configure level 11 command access-group
hostname(config)# privilege configure level 11 command access-list
hostname(config)# privilege configure level 11 command activation-key
hostname(config)# privilege configure level 11 command age
hostname(config)# privilege configure level 11 command alias
hostname(config)# privilege configure level 11 command apply
```

関連コマンド

コマンド	説明
clear configure privilege	コンフィギュレーションから privilege コマンド文を削除します。
show curpriv	現在の特権レベルを表示します。
show running-config privilege	コマンドの特権レベルを表示します。

protocol http

CRL を取得するために許可する配布ポイント プロトコルとして HTTP を指定するには、ca-crl コンフィギュレーション モードで **protocol http** コマンドを使用します。アクセス権があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。

CRL 取得方法として許可した HTTP を削除するには、このコマンドの **no** 形式を使用します。

protocol http

no protocol http

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

デフォルトでは、HTTP を許可する設定になっています。

コマンドのモード

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
CRL コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更
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

このコマンドを使用する場合は、HTTP ルールを公開インターフェイス フィルタに必ず割り当ててください。

例

次の例では、ca-crl コンフィギュレーション モードに入り、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして HTTP を許可します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol http
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
protocol ldap	CRL の取得方法として LDAP を指定します。
protocol scep	CRL の取得方法として SCEP を指定します。

protocol ldap

CRL を取得するための配布ポイント プロトコルとして LDAP を指定するには、ca-crl コンフィギュレーション モードで **protocol ldap** コマンドを使用します。アクセス権があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。

CRL 取得方法として許可した LDAP プロトコルを削除するには、このコマンドの **no** 形式を使用します。

protocol ldap

no protocol ldap

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

デフォルトでは、LDAP を許可する設定になっています。

コマンドのモード

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
CRL コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

例

次の例では、ca-crl コンフィギュレーション モードに入り、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして LDAP を許可します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol ldap
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
protocol http	HTTP を CRL 取得方法として指定します。
protocol scep	SCEP を CRL 取得方法として指定します。

protocol scep

CRL を取得するための配布ポイント プロトコルとして SCEP を指定するには、crl 設定モードで **protocol scep** コマンドを使用します。アクセス権があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。

CRL 取得方法として許可した SCEP プロトコルを削除するには、このコマンドの **no** 形式を使用します。

protocol scep

no protocol scep

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

デフォルトでは、SCEP を許可する設定になっています。

コマンドのモード

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
CRL コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

例

次の例では、ca-crl コンフィギュレーション モードに入り、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして SCEP を許可します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol scep
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
protocol http	HTTP を CRL 取得方法として指定します。
protocol ldap	LDAP を CRL 取得方法として指定します。

protocol-object

プロトコル オブジェクトをプロトコル オブジェクト グループに追加するには、プロトコル コンフィギュレーション モードで **protocol-object** コマンドを使用します。ポート オブジェクトを削除するには、このコマンドの **no** 形式を使用します。

protocol-object *protocol*

no protocol-object *protocol*

シンタックスの説明

protocol	プロトコルの名前または番号。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
プロトコル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
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

プロトコル コンフィギュレーション モードでプロトコル オブジェクトを定義するには、**object-group** コマンドとともに **protocol-object** コマンドを使用します。

protocol 引数を使用して、IP プロトコルの名前または番号を指定できます。udp プロトコル番号は 17、tcp プロトコル番号は 6、egp プロトコル番号は 47 です。

例

次の例は、プロトコル オブジェクトを定義する方法を示しています。

```
hostname(config)# object-group protocol proto_grp_1
hostname(config-protocol)# protocol-object udp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# exit
hostname(config)# object-group protocol proto_grp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# group-object proto_grp_1
hostname(config-protocol)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
show running-config object-group	現在のオブジェクト グループを表示します。

pwd

現在の作業ディレクトリを表示するには、特権 EXEC モードで **pwd** コマンドを使用します。

pwd

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　デフォルトは、ルート ディレクトリ（/）です。

コマンドのモード　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
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、機能の点で ***dir*** コマンドと類似しています。

例　次の例は、現在の作業ディレクトリを表示する方法を示しています。

```
hostname# pwd
disk0:/
hostname# pwd
flash:
```

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。
more	ファイルの内容を表示します。

queue-limit (priority-queue)

プライオリティキューの深さを指定するには、プライオリティキュー モードで **queue-limit** 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。

queue-limit *number-of-packets*

no queue-limit *number-of-packets*

シンタックスの説明

number-of-packets	インターフェイスがパケットのドロップを開始するまで、キューに入れる（つまり、バッファ処理する）ことができる低遅延パケットまたは通常の優先順位のパケットの最大数を指定します。指定可能な値の範囲については、「使用上の注意」の項を参照してください。

デフォルト

デフォルトでは、キューの上限は 1,024 パケットです。

コマンドのモード

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
プライオリティキュー	•	•	•	•	—

コマンド履歴

リリース	変更
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 アプライアンスでは、次の 2 つのトラフィック クラスを使用できます。1 つは優先順位が高く、遅延に影響されやすいトラフィック（音声およびビデオなど）用の Low-Latency Queuing（LLQ; 低遅延キューイング）で、もう 1 つは、それ以外のすべてのトラフィック用のベストエフォート（デフォルト）です。セキュリティ アプライアンスは、優先トラフィックを認識し、適切な Quality of Service（QoS; サービス品質）ポリシーを適用します。プライオリティキューのサイズと項目数を設定することで、トラフィック フローを微調整できます。

プライオリティ キューイングを有効にするには、**priority-queue** コマンドを使用して、インターフェイスのプライオリティキューをあらかじめ作成しておく必要があります。1 つの **priority-queue** コマンドを、**nameif** コマンドで定義できるすべてのインターフェイスに対して適用できます。

priority-queue コマンドを使用すると、プライオリティキュー モードに入ります。モードはプロンプトに表示されます。プライオリティキュー モードでは、いつでも送信キューに入れることができるパケットの最大数（**tx-ring-limit** コマンド）、およびバッファに入れることのできる両タイプ（優先またはベストエフォート）のパケット数を設定できます（**queue-limit** コマンド）。queue-limit の数を超えると、以後のパケットはドロップされます。

（注） インターフェイスのプライオリティ キューイングをイネーブルにするには、**priority-queue** コマンドを設定する必要があります。

指定する tx-ring-limit および queue-limit は、優先順位の高い低遅延キューとベストエフォートキューの両方に適用されます。tx-ring-limit は、ドライバが許容できる両タイプのパケットの数です。このパケットの処理が終わると、ドライバは輻輳が解消するまで、インターフェイスの先頭にある、パケットをバッファしているキューの処理に戻ります。一般に、これらの 2 つのパラメータを調整することによって、低遅延トラフィックのフローを最適化できます。

キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これが「テール ドロップ」です。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファ サイズを大きくします。

（注）　**queue-limit** コマンドと **tx-ring-limit** コマンドの値の範囲の上限は、実行時に動的に決まります。この上限値を表示するには、コマンドラインで **help** または **?** と入力します。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。キューは、使用可能なメモリの量を超えることはできません。理論上の最大パケット数は 2,147,483,647 です。

例

次の例では、test というインターフェイスのプライオリティキューを設定して、キューの上限を 30,000 パケット、送信キューの上限を 256 パケットと指定しています。

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 30000
hostname(priority-queue)# tx-ring-limit 256
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定したインターフェイスの現在のプライオリティキュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show priority-queue statistics	指定したインターフェイスのプライオリティキュー統計情報を表示します。
show running-config [all] priority-queue	現在のプライオリティキュー コンフィギュレーションを表示します。**all** キーワードを指定すると、現在のすべてのプライオリティキュー、および queue-limit と tx-ring-limit のコンフィギュレーション値が表示されます。
tx-ring-limit	イーサネット送信ドライバのキューにいつでも入れることができるパケットの最大数を設定します。

queue-limit (tcp-map)

TCP ストリームのキューに入れることのできる順序付けされていないパケットの最大数を設定するには、tcp-map コンフィギュレーション モードで **queue-limit** 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。

queue-limit *pkt_num*

no queue-limit *pkt_num*

シンタックスの説明

pkt_num	順序付けされていないパケットがドロップされるまでに、TCP 接続のキューに入れることのできる、順序付けされていないパケットの最大数を指定します。範囲は 0 ～ 250 です。デフォルトは 0 です。

デフォルト

デフォルトの最大パケット数は 0 です。

コマンドのモード

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
tcp 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
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

tcp-map コマンドをモジュラ ポリシー フレームワーク インフラストラクチャとともに使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。tcp マップ コンフィギュレーション モードで **queue-limit** コマンドを使用すると、任意の TCP 接続の TCP パケットの順序付けをイネーブルにしたり、デフォルトで順序付けされている接続のキューの上限を変更したりできます。

検査、IDS 機能、または TCP check-retransmission のいずれかの機能がイネーブルになっている場合、パケットは TCP 接続上で順序付けされます。順序付けされている接続のパケット キューのデフォルトの上限は、1 フローにつき 2 つです。それ以外のすべての TCP 接続の場合、パケットは受信と同時に転送されます。これには、順序付けされていないパケットも含まれます。任意の TCP 接続の TCP パケットの順序付けをイネーブルにする、または順序付けされている接続のキューの上限を変更するには、**queue-limit** コマンドを使用します。この機能をイネーブルにすると、順序付けされていないパケットは、転送できるようになるまでキューに保持されるか、または一定の時間が経過するまでキューに保持されます。したがって、メモリ使用量は、パケットのバッファ処理により増加します。

例

次の例は、すべての Telnet 接続の TCP パケットの順序付けをイネーブルにする方法を示しています。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# queue-limit 8
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq telnet
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class-map	トラフィック分類に使用するクラスマップを指定します。
help	**policy-map** コマンド、**class** コマンド、および **description** コマンド シンタックスのヘルプを表示します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。

quit

現在のコンフィギュレーション モードを終了する、または特権 EXEC モードまたはユーザ EXEC モードからログアウトするには、**quit** コマンドを使用します。

quit

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。

コマンドのモード

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
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
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

キー シーケンス ***Ctrl+Z*** を使用しても、グローバル コンフィギュレーション（およびそれより上位の）モードを終了できます。このキー シーケンスは、特権 EXEC モードおよびユーザ EXEC モードでは機能しません。

特権 EXEC モードまたはユーザ EXEC モードで **quit** コマンドを入力すると、セキュリティ アプライアンスからログアウトします。特権 EXEC モードからユーザ EXEC モードに戻るには、**disable** コマンドを使用します。

例

次の例は、**quit** コマンドを使用してグローバル コンフィギュレーション モードを終了し、セッションからログアウトする方法を示しています。

```
hostname(config)# quit
hostname# quit

Logoff
```

次の例は、**quit** コマンドを使用してグローバル コンフィギュレーション モードを終了し、その後、**disable** コマンドを使用して特権 EXEC モードを終了する方法を示しています。

```
hostname(config)# quit
hostname# disable
hostname>
```

関連コマンド

コマンド	説明
exit	コンフィギュレーション モードを終了します。または、特権 EXEC モードまたはユーザ EXEC モードからログアウトします。

radius-common-pw

セキュリティ アプライアンスを経由してこの RADIUS 認可サーバにアクセスするすべてのユーザが使用する共通のパスワードを指定するには、AAA サーバ ホスト モードで **radius-common-pw** 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。

radius-common-pw *string*

no radius-common-pw

シンタックスの説明

string	この RADIUS サーバとのすべての認可トランザクションで共通のパスワードとして使用される最大 127 文字の英数字のキーワード。大文字と小文字は区別されます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 ホスト	•	•	•	•	—

コマンド履歴

リリース	変更
7.0(1)	このリリースで導入されました。

使用上のガイドライン

このコマンドは、RADIUS 認可サーバに対してのみ有効です。

RADIUS 認可サーバは、接続する各ユーザのパスワードとユーザ名を要求します。セキュリティ アプライアンスは、ユーザ名を自動的に入力します。ここでユーザは、パスワードを入力します。RADIUS サーバ管理者は、このパスワードを、このセキュリティ アプライアンスを経由してサーバに権限を与える各ユーザと関連付けるように、RADIUS サーバを設定する必要があります。この情報は、RADIUS サーバ管理者に必ず提供してください。

共通のユーザ パスワードを指定しない場合、各ユーザのパスワードは、ユーザ各自のユーザ名となります。たとえば、ユーザ名が「jsmith」のユーザは、「jsmith」と入力します。ユーザ名を共通のユーザ パスワードとして使用している場合は、セキュリティ対策として、この RADIUS サーバを使用ネットワーク外で認可用に使用しないでください。

（注） このフィールドは、基本的にスペースを埋めるためのものです。RADIUS サーバは、このフィールドを予期および要求しますが、使用することはありません。ユーザは、このフィールドを知っている必要はありません。

例

次の例では、ホスト「1.2.3.4」上に「svrgrp1」という RADIUS AAA サーバ グループを設定し、タイムアウト間隔を 9 秒に、リトライ間隔を 7 秒に設定します。さらに、RADIUS 共通パスワードを「allauthpw」に設定します。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# radius-common-pw allauthpw
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド文をコンフィギュレーションから削除します。
show running-config aaa-server	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。

radius-with-expiry

認証中に MS-CHAPv2 を使用してユーザとパスワード アップデートをネゴシエートするように、セキュリティ アプライアンスを設定するには、トンネルグループ ipsec アトリビュート コンフィギュレーション モードで **radius-with-expiry** コマンドを使用します。RADIUS 認証が設定されていない場合、このコマンドはセキュリティ アプライアンスで無視されます。

デフォルト値に戻すには、このコマンドの ***no*** 形式を使用します。

radius-with-expiry

no radius-with-expiry

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

デフォルトでは、このコマンドの設定はディセーブルになっています。

コマンドのモード

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
トンネルグループ ipsec アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
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

このアトリビュートは、IPSec リモートアクセス トンネルグループ タイプだけに適用できます。

例

次の例では、config-ipsec コンフィギュレーション モードで入り、remotegrp というリモートアクセス トンネルグループの radius-with-expiry を設定しています。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)# radius-with-expiry
hostname(config-ipsec)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネルグループを消去します。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネルグループに関連付けます。

reactivation-mode

グループ内の障害のあるサーバを再度有効にする方法（再有効化ポリシー）を指定するには、AAA サーバ グループ モードで **reactivation-mode** 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。

reactivation-mode depletion [**deadtime** *minutes*]

reactivation-mode timed

no reactivation-mode

シンタックスの説明

deadtime *minutes*	（オプション）グループ内の最後のサーバをディセーブルにしてから、すべてのサーバを再度イネーブルにするまでの時間の長さを指定します。
depletion	グループ内のすべてのサーバが非アクティブになった場合のみ、障害のあるサーバを再度有効にします。
timed	30 秒のダウン時間が経過した後に、障害のあるサーバを再度有効にします。

デフォルト

デフォルトの再有効化モードは depletion で、デフォルトの deadtime 値は 10 です。サポートされる deadtime 値の範囲は、0 ～ 1,440 分です。

コマンドのモード

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
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

各サーバ グループには、グループ内のサーバの再有効化ポリシーを指定するアトリビュートがあります。

depletion モードでは、あるサーバが無効になると、グループ内の他のすべてのサーバが非アクティブになるまで、そのサーバは非アクティブのままとなります。この事態が発生した場合、グループ内のすべてのサーバは再有効化されます。この方法で、障害のあるサーバが原因の接続遅延の発生が最小限に抑えられます。***depletion*** モードを使用している場合は、***deadtime*** パラメータも指定できます。***deadtime*** パラメータは、グループ内の最後のサーバをディセーブルにしてから、すべてのサーバを再度イネーブルにするまでの時間の長さ（分）を指定します。このパラメータは、サーバ グループがローカル フォールバック機能と連動して使用されている場合に限り、意味を持ちます。

timed モードでは、障害のあるサーバは、30 秒のダウン時間が経過した後に再有効化されます。これは、サーバ リスト内の最初のサーバをプライマリ サーバとして使用していて、可能な場合は常にそのサーバがオンラインであることが望ましい場合に役立ちます。このポリシーは、UDP サーバの場合は機能しません。UDP サーバへの接続は、たとえそのサーバが存在しない場合でも失敗しないため、UDP サーバは無条件にオンラインに戻ります。このモードでは、サーバ リストに到達不能なサーバが複数含まれている場合に、接続時間が長くなったり、接続が失敗したりする可能性があります。

同時アカウンティングがイネーブルになっているアカウンティング サーバ グループには、強制的に ***timed*** モードが適用されます。これは、所定のリスト内のすべてのサーバが同等であることを意味します。

例

次の例では、depletion 再有効化モードを使用するように、「srvgrp1」という aTACACS+ AAA サーバを設定します。deadtime は 15 分に設定します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-sersver-group)# reactivation-mode depletion deadtime 15
hostname(config-aaa-server)# exit
hostname(config)#
```

次の例では、timed 再有効化モードを使用するように、「srvgrp1」という aTACACS+ AAA サーバを設定します。

```
hostname(config)# aaa-server svrgrp2 protocol tacacs+
hostname(config-aaa-server)# reactivation-mode timed
hostname(config-aaa-server)# exit
hostname(config)#
```

関連コマンド

accounting-mode	アカウンティング メッセージを 1 つのサーバに送信するか、グループ内のすべてのサーバに送信するかを指定します。
aaa-server 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。
max-failed-attempts	サーバ グループ内の所定のサーバが無効になるまでに、そのサーバで許容される接続試行の失敗数を指定します。
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-server	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。

redistribute

あるルーティング ドメインから別のルーティング ドメインにルートを再配布するには、ルータ コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布を削除するには、このコマンドの **no** 形式を使用します。

redistribute {{***ospf*** *pid* [***match*** {***internal*** | ***external*** [***1*** | ***2***] | ***nssa-external*** [***1*** | ***2***]}]} | ***static*** | ***connected***} [***metric*** *metric_value*] [***metric-type*** *metric_type*] [***route-map*** *map_name*] [***tag*** *tag_value*] [***subnets***]

no redistribute {{***ospf*** *pid* [***match*** {***internal*** | ***external*** [***1*** | ***2***] | ***nssa-external*** [***1*** | ***2***]}]} | ***static*** | ***connected***} [***metric*** *metric_value*] [***metric-type*** *metric_type*] [***route-map*** *map_name*] [***tag*** *tag_value*] [***subnets***]

シンタックスの説明

connected	インターフェイスに接続されているネットワークを OSPF ルーティング プロセスに再配布することを指定します。
external *type*	指定した自律システムの外部の OSPF メトリック ルートを指定します。有効な値は、**1** または **2** です。
internal *type*	指定した自律システム内部の OSPF メトリック ルートを指定します。
match	（オプション）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指定します。
metric *metric_value*	（オプション）OSPF デフォルト メトリック値を指定します（0 ～ 16777214）。
metric-type *metric_type*	（オプション）OSPF ルーティング ドメインにアドバタイズされる、デフォルト ルートに関連付けられた外部リンク タイプ。2 つの値、つまり 1（タイプ 1 外部ルート）または 2（タイプ 2 外部ルート）のいずれかを使用できます。
nssa-external *type*	not-so-stubby area（NSSA; 準スタブ エリア）外部のルートの OSPF メトリック タイプを指定します。有効な値は、**1** または **2** です。
ospf *pid*	OSPF ルーティング プロセスを現在の OSPF ルーティング プロセスに再配布するために使用されます。*pid* には、OSPF ルーティング プロセス用に内部的に使用される識別パラメータを指定します。有効な値は、1 ～ 65535 です。
route-map *map_name*	（オプション）適用するルートマップの名前。
static	スタティック ルートを OSPF プロセスに再配布するために使用されます。
subnets	（オプション）ルートを OSPF に再配布する場合に、指定プロトコルの再配布を確認します。使用しない場合、クラスフル ルートだけが再配布されます。
tag *tag_value*	（オプション）各外部ルートに対応付けられた 32 ビットの 10 進値。この値は、OSPF 自体によって使用されることはありません。ASBR 間で情報を交換するために使用されます。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用され、その他のプロトコルには 0 が使用されます。有効な値は 0 ～ 4294967295 です。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード　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。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例　次の例は、スタティック ルートを現在の OSPF プロセスに再配布する方法を示しています。

```
hostname(config-router)# redistribute ospf static
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

reload

コンフィギュレーションをリブートおよびリロードするには、特権 EXEC モードで **reload** コマンドを使用します。

reload [**at** *hh*:*mm* [*month day* | *day month*]] [**cancel**] [**in** [*hh*:]*mm***]** [**max-hold-time** [*hh*:]*mm*] [**noconfirm**] [**quick**] [**reason** *text*] [**save-config**]

シンタックスの説明

at *hh*:*mm*	（オプション）指定された時刻（24 時間方式のクロックを使用）で実行するように、ソフトウェアのリロードをスケジューリングします。月日を指定しなかった場合、リロードは当日の指定された時刻（指定された時刻が現在の時刻よりあとの場合）または翌日（指定された時刻が現在の時刻より前の場合）に実行されます。00:00 を指定すると、リロードは午前 0 時にスケジューリングされます。リロードは 24 時間以内に実行する必要があります。
cancel	（オプション）スケジューリングされたリロードをキャンセルします。
day	（オプション）日付の番号を指定します。範囲は 1 ～ 31 です。
in [*hh*:]*mm*]	（オプション）指定された時刻（分または時と分）に有効になるように、ソフトウェアのリロードをスケジューリングします。リロードは 24 時間以内に実行する必要があります。
max-hold-time [*hh:*]*mm*	（オプション）シャットダウンまたはリブートの前に、セキュリティ アプライアンスが他のサブシステムに通知するまで待機する最小保持時間を指定します。この時間が経過すると、クイック（強制）シャットダウンまたはリブートが実行されます。
month	（オプション）月名を指定します。月名を表す一意の文字列を作成するため、十分な文字を入力します。たとえば、「Ju」は「June」または「July」を表す可能性があるため一意ではありませんが、「Jul」と入力すれば、正確にこれらの 3 文字で始まる月は他にないので一意になります。
noconfirm	（オプション）ユーザによる確認がないセキュリティ アプライアンスのリロードを許可します。
quick	（オプション）通知したり、すべてのサブシステムを正常にシャットダウンしたりすることなく、クイック リロードを強制します。
reason *text*	（オプション）リロードの理由を 1 ～ 255 文字で指定します。理由テキストは、すべての IPSec VPN クライアント、端末、Tenet、SSH、および ASDM の接続またはセッションに送信されます。 **（注）** isakmp などの一部のアプリケーションで、IPSec VPN クライアントに理由テキストを送信するには、追加コンフィギュレーションが必要です。詳細については、ソフトウェア コンフィギュレーション マニュアルの適切な項を参照してください。
save-config	（オプション）シャットダウンする前に、実行コンフィギュレーションをメモリに保存します。***save-config*** キーワードを入力しない場合、コンフィギュレーションに対する未保存の変更はすべて、リロード後に失われます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドは、次の新しい引数およびキーワードを追加するために修正されました。*day*、*hh*、*mm*、*month*、***quick***、***save-config***、および *text*。

使用上のガイドライン

このコマンドを使用すると、セキュリティ アプライアンスをリブートし、コンフィギュレーションをフラッシュからリロードできます。

デフォルトでは、**reload** コマンドは対話型です。セキュリティ アプライアンスは、コンフィギュレーションが修正されていないかどうかを最初にチェックしますが、保存はしません。その場合、セキュリティ アプライアンスは、コンフィギュレーションを保存するためのプロンプトを表示します。マルチ コンテキスト モードでは、セキュリティ アプライアンスは、保存されていないコンフィギュレーションがあるコンテキストごとにプロンプトを表示します。***save-config*** パラメータを指定すると、プロンプトが表示されることなくコンフィギュレーションが保存されます。その場合、セキュリティ アプライアンスは、システムをリロードしてよいか確認するプロンプトを表示します。***y*** と応答するか、***Enter*** キーを押す場合のみ、リロードが開始されます。確認後、セキュリティ アプライアンスは、リロード プロセスを開始するか、スケジューリングします。どちらが実行されるかは、遅延パラメータ（***in*** または ***at***）の指定によって異なります。

デフォルトでは、リロード プロセスは「グレースフル」（「ナイス」とも呼ばれる）モードで動作します。リブートが実行される直前に、登録されているすべてのサブシステムには通知が行われます。この通知により、サブシステムはリブート前に正常にシャットダウンできます。このようなシャットダウンが実行されるまで待つことを避けるには、***max-hold-time*** パラメータで最大待ち時間を指定します。別の方法として、***quick*** パラメータを使用することでも、影響を受けるサブシステムに通知したり、グレースフル シャットダウンを待機したりすることなく、リロード プロセスを強制的に開始できます。

noconfirm パラメータを指定すると、**reload** コマンドの動作を強制的に非対話型にすることができます。この場合、***save-config*** パラメータが指定されていない限り、セキュリティ アプライアンスは、保存されていないコンフィギュレーションをチェックしません。セキュリティ アプライアンスは、システムをリブートする前に確認のプロンプトをユーザに表示しません。遅延パラメータを設定していない場合は、リロード プロセスはすぐに開始またはスケジューリングされます。ただし、***max-hold-time*** パラメータまたは ***quick*** パラメータを指定して、動作またはリロード プロセスを制御することはできます。

スケジューリングされたリロードをキャンセルするには、**reload cancel** を使用します。すでに進行中のリロードは、キャンセルできません。

（注） フラッシュ　パーティションに書き込まれていないコンフィギュレーションの変更は、リロードすると失われます。リブートする前に、**write memory** コマンドを入力して、現在のコンフィギュレーションをフラッシュ パーティションに保存してください。

例

次の例は、コンフィギュレーションをリブートおよびリロードする方法を示しています。

```
hostname# reload
Proceed with ?  [confirm] y

Rebooting...

XXX Bios VX.X
...
```

関連コマンド

コマンド	説明
show reload	セキュリティ アプライアンスのリロード ステータスを表示します。

remote-access threshold session-threshold-exceeded

しきい値を設定するには、グローバル コンフィギュレーション モードで **remote-access threshold** コマンドを使用します。しきい値を削除するには、このコマンドの **no** 形式を使用します。このコマンドは、アクティブなリモートアクセス セッションの数を指定します。この数に達した時点で、セキュリティ アプライアンスはトラップを送信します。

remote-access threshold session-threshold-exceeded {*threshold-value*}

no **remote-access threshold session-threshold-exceeded**

シンタックスの説明

threshold-value	セキュリティ アプライアンスがサポートしているセッション上限以下の整数を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

例

次の例は、しきい値として 1500 を設定する方法を示しています。

```
hostname# remote-access threshold session-threshold-exceeded 1500
```

関連コマンド

コマンド	説明
snmp-server enable trap remote-access	しきい値のトラッピングをイネーブルにします。

rename

コピー元ファイル名からコピー先ファイル名に、ファイルまたはディレクトリの名前を変更するには、特権 EXEC モードで **rename** コマンドを使用します。

rename [*/noconfirm*] [disk0: | disk1: | flash:] *source-path* [disk0: | disk1: | flash:] *destination-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。
destination-path	コピー先ファイルのパスを指定します。
disk0:	（オプション）内部フラッシュ メモリを指定し、続けてコロン（:）を入力します。
disk1:	（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）内部フラッシュ メモリを指定し、続けてコロン（:）を入力します。
source-path	コピー元ファイルのパスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

rename flash: flash: コマンドは、コピー元とコピー先のファイル名を入力するためのプロンプトを表示します。

ファイル システム全体で、ファイルまたはディレクトリの名前を変更することはできません。

次の例を参考にしてください。

```
hostname# rename flash: disk1:
Source filename []? new-config
Destination filename []? old-config
%Cannot rename between filesystems
```

例

次の例は、「test」という名前のファイルを「test1」に変更する方法を示しています。

```
hostname# rename flash: flash:
Source filename [running-config]? test
Destination filename [n]? test1
```

関連コマンド

コマンド	説明
mkdir	新しいディレクトリを作成します。
rmdir	ディレクトリを削除します。
show file	ファイル システムに関する情報を表示します。

replication http

フェールオーバー グループの HTTP 接続の複製をイネーブルにするには、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 **replication http** コマンドを使用します。HTTP 接続の複製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。

replication http

no replication http

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　ディセーブルです。

コマンドのモード　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
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　デフォルトでは、ステートフル フェールオーバーがイネーブルの場合、セキュリティ アプライアンスは HTTP セッション情報を複製しません。HTTP セッションは通常は存続期間が短く、HTTP クライアントは接続試行が失敗すると通常はリトライするため、HTTP セッションの複製をしないことでシステムのパフォーマンスが向上します。複製をしなくても重要なデータや接続は失われません。**replication http** コマンドは、ステートフル フェールオーバー環境で HTTP セッションのステートフル複製をイネーブルにしますが、システム パフォーマンスには悪影響を与える可能性があります。

このコマンドを使用できるのは、Active/Active フェールオーバーに対してのみです。このコマンドは、Active/Active フェールオーバー コンフィギュレーションのフェールオーバー グループを除く、Active/Standby フェールオーバーに対して **failover replication http** コマンドと同じ機能を提供します。

例

次の例は、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)# replication http
hostname(config-fover-group)# exit
```

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 replication http	HTTP 接続を複製するように、ステートフル フェールオーバーを設定します。

request-command deny

FTP 要求内で特定のコマンドを禁止するには、FTP マップ コンフィギュレーション モードで **request-command deny** 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。

request-command deny { **appe** | **cdup** | **dele** | **get** | **help** | **mkd** | **put** | **rmd** | **rnfr** | **rnto** | **site** | **stou** }

no request-command deny { **appe** | **cdup** | **help** | **retr** | **rnfr** | **rnto** | **site** | **stor** | **stou** }

シンタックスの説明

appe	ファイルに対して付加を実行するコマンドを禁止します。
cdup	現在の作業ファイルの親ディレクトリに変更を加えるコマンドを禁止します。
dele	サーバ上のファイルを削除するコマンドを禁止します。
get	サーバからファイルを取得するクライアント コマンドを禁止します。
help	ヘルプ情報を提供するコマンドを禁止します。
mkd	サーバ上にディレクトリを作成するコマンドを禁止します。
put	サーバにファイルを送信するクライアント コマンドを禁止します。
rmd	サーバ上のディレクトリを削除するコマンドを禁止します。
rnfr	元のファイル名からの名前変更を指定するコマンドを禁止します。
rnto	新しいファイル名への名前変更を指定するコマンドを禁止します。
site	サーバ システム固有のコマンドを禁止します。通常は、リモート管理で使用されます。
stou	一意のファイル名を使用しているファイルを保存するコマンドを禁止します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード　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。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	シングル	マルチ コンテキスト	マルチ 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
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、厳密な FTP 検査を使用するときに、セキュリティ アプライアンスを通過する FTP 要求内で許可されるコマンドを制御するために使用します。

例　次の例では、**stor** コマンド、**stou** コマンド、または **appe** コマンドが含まれている FTP 要求をドロップするように、セキュリティ アプライアンスを設定します。

```
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# request-command deny put stou appe
hostname(config-ftp-map)# exit
```

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。
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-method

HTTP 要求メソッドに基づいて 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 **request-method** コマンドを使用します。このコマンドには、**http-map** コマンドを使用してアクセスできます。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。

request-method {{ **ext** *ext_methods* | **default**} | { **rfc** *rfc_methods* | **default**}} **action** {**allow** | **reset** | **drop**} [**log**]

no request-method { **ext** *ext_methods* | **rfc** *rfc_methods* } **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を指定します。
allow	メッセージを許可します。
default	サポートされている要求メソッドがトラフィックに含まれていて、そのメソッドが設定済みリストに記載されていない場合に、セキュリティ アプライアンスが実行するデフォルト アクションを指定します。
drop	接続を終了します。
ext	拡張メソッドを指定します。
ext-methods	セキュリティ アプライアンスを通過することを許可する拡張メソッドの 1 つを指定します。
log	（オプション）syslog を生成します。
reset	クライアントまたはサーバに TCP リセット メッセージを送信します。
rfc	RFC 2616 でサポートされているメソッドを指定します。
rfc-methods	セキュリティ アプライアンスを通過することを許可する RFC メソッドの 1 つを指定します（表 6-2 を参照）。

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。このコマンドがイネーブルで、サポートされている要求メソッドが指定されていない場合、デフォルト アクションでは、ロギングなしで接続が許可されます。デフォルト アクションを変更するには、**default** キーワードを使用して別のデフォルト アクションを指定します。

コマンドのモード

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
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

request-method 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、サポートおよび設定されている各要求メソッドの HTTP 接続に対して、指定されているアクションを適用します。

セキュリティ アプライアンスは、設定済みリストにある要求メソッドに一致しないすべてのトラフィックに対して、**default** アクションを適用します。**default** アクションでは、接続をロギングなしで **allow** します。事前設定済みのデフォルト アクションでは、**drop** および **log** というアクションを持つ 1 つまたは複数の要求メソッドを指定すると、セキュリティ アプライアンスは、設定済み要求メソッドが含まれている接続をドロップし、各接続をロギングし、サポートされているその他の要求メソッドが含まれているすべての接続を許可します。

より厳しいポリシーを設定する場合は、デフォルト アクションを **drop**（または **reset**）および **log** に変更します（イベントをログに記録する場合）。その後、**allow** アクションで、許可する各メソッドを設定します。

適用する設定ごとに 1 回、**request-method** コマンドを入力します。**request-method** コマンドのインスタンスを、デフォルト アクションを変更するために 1 つ、設定済みメソッドのリストに 1 つの要求メソッドを追加するために 1 つ使用します。

このコマンドの **no** 形式を使用して、要求メソッドを設定済みメソッドのリストから削除する場合、コマンドラインで要求メソッド キーワードの後にある文字はすべて無視されます。

RFC 2616 で定義されているメソッドで、設定済みメソッドのリストに追加できるものを表 6-2 に示します。

表 6-3　RFC 2616 メソッド

メソッド	説明
connect	トンネルに動的に切り替わることが可能なプロキシ（例、SSL トンネリング）とともに使用されます。
delete	Request-URI によって識別されたリソースをオリジン サーバが削除することを要求します。
get	Request-URI によって識別された情報またはオブジェクトをすべて取得します。
head	サーバが応答でメッセージ本文を返さないこと以外は、GET と同じです。
options	Request-URI によって識別されたサーバで使用できる、通信オプションについての情報の要求を表します。
post	要求に含まれているオブジェクトを、Request-Line 内の Request-URI によって識別されたリソースの新しい下位リソースとしてオリジン サーバが受け入れることを要求します。
put	含まれているオブジェクトを指定した Request-URI の下に保存することを要求します。
trace	リモートのアプリケーション層の要求メッセージのループバックを起動します。

例

次の例では、事前設定済みのデフォルトを使用して、緩やかなポリシーを指定しています。サポートされているすべての要求メソッドを、個別に拒否されていない限り許可します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# request-method rfc options drop log
hostname(config-http-map)# request-method rfc post drop log
hostname(config-http-map)# exit
```

この例では、**options** 要求メソッドおよび **post** 要求メソッドだけがドロップされ、イベントが記録されます。

次の例では、厳しいポリシーを設定します。デフォルト アクションは、個別に許可されていないすべての要求メソッドの接続を **reset** し、イベントを **log** するように変更されています。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# request-method rfc default action reset log
hostname(config-http-map)# request-method rfc get allow
hostname(config-http-map)# request-method rfc put allow
hostname(config-http-map)# exit
```

この場合、**get** 要求メソッドおよび **put** 要求メソッドが許可されます。その他のメソッドを使用するトラフィックが検出された場合、セキュリティ アプライアンスは接続をリセットし、syslog エントリを作成します。

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。

request-queue

応答待ちでキュー入れられる GTP 要求の最大数を指定するには、GTP マップ コンフィギュレーション モードで **request-queue** 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します。この数をデフォルトの 200 に戻すには、このコマンドの **no** 形式を使用します。

request-queue *max_requests*

no request-queue *max_requests*

シンタックスの説明

max_requests	応答待ちでキューに入れられる GTP 要求の最大数。範囲は、1 ～ 4,294,967,295 です。

デフォルト

max_requests のデフォルトは 200 です。

コマンドのモード

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
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

gtp request-queue コマンドは、応答待ちでキューに入れられる GTP 要求の最大数を指定します。限度に到達していて新しい要求が着信すると、最も長時間キューに入っている要求が削除されます。Error Indication、Version Not Supported、および SGSN Context Acknowledge の各メッセージは要求と見なされないため、応答を待つために要求キューに入れられることはありません。

例

次の例では、要求キューの最大サイズを 300 バイトに指定します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# request-queue-size 300
```

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用に特定の 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。

reserved-bits

TCP ヘッダーの予約済みビットを消去するには、または、予約済みビットが設定されたパケットをドロップするには、tcp マップ コンフィギュレーション モードで **reserved-bits** 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。

reserved-bits {**allow** | **clear** | **drop**}

no reserved-bits {**allow** | **clear** | **drop**}

シンタックスの説明

allow	TCP ヘッダー内に予約済みビットを持つパケットを許可します。
clear	TCP ヘッダー内の予約済みビットを消去してから、そのパケットを許可します。
drop	TCP ヘッダー内に予約済みビットを持つパケットをドロップします。

デフォルト

デフォルトでは、予約済みビットが許可されています。

コマンドのモード

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
tcp 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
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

tcp-map コマンドをモジュラ ポリシー フレームワーク インフラストラクチャとともに使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。予約済みビットのあるパケットがエンド ホストで処理される方法についてのあいまいさを排除するには、tcp マップ コンフィギュレーション モードで **reserved-bits** コマンドを使用します。あいまいさがあると、セキュリティ アプライアンスの非同期につながる場合があります。TCP ヘッダー内の予約済みビットを消去することを選択できます。さらには、予約済みビットが設定されたパケットをドロップすることも選択できます。

例

次の例は、予約済みビットが設定されたすべての TCP フローのパケットを消去する方法を示します。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# reserved-bits clear
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラスマップを指定します。
help	**policy-map** コマンド、**class** コマンド、および **description** コマンド シンタックスのヘルプを表示します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。

retry-interval

aaa-server host コマンドで以前に指定した特定の AAA サーバに対するリトライ間隔（時間の長さ）を設定するには、AAA サーバ ホスト モードで **retry-interval** コマンドを使用します。このリトライ間隔をデフォルト値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。

retry-interval *seconds*

no retry-interval

シンタックスの説明

seconds	要求をリトライする間隔を指定します（1 ～ 10 秒）。セキュリティ アプライアンスが接続要求をリトライするまでに待つ時間です。

デフォルト

デフォルトのリトライ間隔は 10 秒です。

コマンドのモード

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 ホスト	•	•	•	•	—

コマンド履歴

リリース	変更
7.0(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。

使用上のガイドライン

セキュリティ アプライアンスが接続試行を実行する間隔（秒数）を指定またはリセットするには、**retry-interval** コマンドを使用します。セキュリティ アプライアンスが AAA サーバへの接続確立の試行を継続する時間の長さを指定するには、**timeout** コマンドを使用します。

例

次の例は、コンテキスト内の **retry-interval** コマンドを示しています。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 7
hostname(config-aaa-server-host)# retry-interval 9
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド文をコンフィギュレーションから削除します。
show running-config aaa-server	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。
timeout	セキュリティ アプライアンスが AAA サーバへの接続確立の試行を継続する時間の長さを指定します。

re-xauth

ユーザが IKE キー再生成で再認証を受けることを必須とするには、グループポリシー コンフィギュレーション モードで **re-xauth enable** コマンドを使用します。IKE キー再生成でのユーザ認証をディセーブルにするには、**re-xauth disable** コマンドを使用します。

re-xauth アトリビュートを実行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。これにより、IKE キー再生成での再認証の値を別のグループポリシーから継承できるようになります。

re-xauth {**enable** | **disable**}

no re-xauth

シンタックスの説明

disable	IKE キー再生成での再認証をディセーブルにします。
enable	IKE キー再生成での再認証をイネーブルにします。

デフォルト

IKE キー再生成での再認証は、ディセーブルになっています。

コマンドのモード

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	•	—	•	—	—

コマンド履歴

リリース	変更
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

IKE キー再生成での再認証をイネーブルにすると、セキュリティ アプライアンスは、フェーズ 1 IKE ネゴシエーション中にユーザ名とパスワードの入力を求めるプロンプトを表示します。また、IKE キー再生成が実行されるたびに、ユーザ認証を求めるプロンプトを表示します。再認証により、セキュリティが向上します。

設定されているキー再生成間隔が極端に短い場合、ユーザは認証を繰り返し求められることに不便を感じることがあります。その場合は、再認証をディセーブルにしてください。設定されているキー再生成間隔を確認するには、モニタリング モードで **show crypto ipsec sa** コマンドを発行して、セキュリティ結合のライフタイムの秒単位データおよび KB 単位データを表示します。

（注） 接続相手側にユーザが存在しない場合、再認証は失敗します。

例

次の例は、FirstGroup というグループポリシーのキー再生成での再認証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)# re-xauth enable
```

rip

RIP 設定をイネーブルにしたり、変更したりするには、グローバル コンフィギュレーション モードで **rip** コマンドを使用します。セキュリティ アプライアンス RIP ルーティング テーブルのアップデート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。

rip *if_name* {**default** | **passive**} [**version** {**1** | **2** [**authentication** {***text*** | ***md5***} *key key_id*]}]

no rip *if_name* {**default** | **passive**} [**version** {**1** | **2** [**authentication** {***text*** | ***md5***} *key key_id*]}]

シンタックスの説明

authentication	（オプション）RIP Version 2 認証をイネーブルにします。
default	インターフェイス上のデフォルト ルートをブロードキャストします。
if_name	RIP をイネーブルにするインターフェイス。
key	RIP アップデートを認証する鍵。
key_id	キーを識別する値。有効な値は 1 ～ 255 です。
md5	RIP メッセージの認証に MD5 を使用します。
passive	インターフェイス上でパッシブ RIP をイネーブルにします。インターフェイスは RIP ルーティング ブロードキャストをリスンし、その情報を使用してルーティング テーブルに入力します。ただし、ルーティング アップデートのブロードキャストは行いません。
text	RIP メッセージの認証にクリア テキストを使用します（ただし、この方法は推奨しません）。
version	（オプション）RIP を指定します。有効値は **1** および **2** です。

デフォルト

RIP はディセーブルになっています。

バージョンを指定しない場合、デフォルトでは RIP Vrsion 1 がイネーブルになります。

コマンドのモード

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
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　**rip** コマンドを使用すると、インターフェイス上での RIP ルーティング アップデートの送受信をイネーブルにできます。RIP アップデートの送信と受信は、別々に設定できます。つまり、各インターフェイス上で、送信だけ、受信だけ、または送信と受信の両方をイネーブルにできます。RIP アップデートの受信をイネーブルにするには、**rip** コマンドで ***passive*** キーワードを使用します。デフォルト ルートのブロードキャストをイネーブルにするには、**rip** コマンドで ***default*** キーワードを使用します。インターフェイス上での RIP アップデートの送信と受信の両方をイネーブルにするには、そのインターフェイス用に 2 つの **rip** コマンドを使用する必要があります。1 つは ***default*** キーワードを使用して、RIP ルーティング アップデートの送信をイネーブルにするものです。もう 1 つは、***passive*** キーワードを使用して、RIP アップデートを受信し、それらのアップデートを使用してルーティング テーブルに入力するものです。

（注）　セキュリティ アプライアンスでは、インターフェイス間で RIP アップデートを通過させることはできません。

RIP Version 2 を指定する場合は、ネイバー認証をイネーブルにできます。また、MD5 ベースの暗号化を使用して RIP アップデートを認証することもできます。ネイバー認証をイネーブルにする場合は、*key* 引数および *key_id* 引数が、RIP Version 2 アップデートを提供する隣接デバイスで使用されているものと同じであることを確認する必要があります。*key* は、最大 16 文字のテキスト文字列です。

RIP Version 2 を設定すると、マルチキャスト アドレス 224.0.0.9 が各インターフェイスで登録され、マルチキャスト RIP Version 2 アップデートを受信できます。RIP Version 2 がパッシブ モードで設定されると、セキュリティ アプライアンスは IP 宛先が 224.0.0.9 の RIP Version 2 マルチキャスト アップデートを受け入れます。RIP Version 2 がデフォルト モードで設定されると、セキュリティ アプライアンスは IP マルチキャスト宛先 224.0.0.9 を使用してデフォルト ルート アップデートを送信します。インターフェイスの RIP Version 2 コマンドを削除すると、マルチキャスト アドレスがインターフェイス カードから登録解除されます。

（注）　Intel 10/100 およびギガビット インターフェイスだけがマルチキャストをサポートします。

RIP は、透過モードではサポートされません。デフォルトでは、セキュリティ アプライアンスは RIP ブロードキャストおよびマルチキャストのすべてのパケットを拒否します。透過モードで動作しているセキュリティ アプライアンスの通過を RIP メッセージに許可するには、このトラフィックを許可するアクセスリスト エントリを定義する必要があります。たとえば、セキュリティ アプライアンスの通過を RIP Version 2 トラフィックに許可するには、`access-list myriplist extended permit ip any host 224.0.0.9` のようなアクセスリスト エントリを作成します。RIP Version 1 ブロードキャストを許可するには、`access-list myriplist extended permit udp any any eq rip` のようなアクセスリスト エントリを作成します。**access-group** コマンドを使用して、これらのアクセスリスト エントリを適切なインターフェイスに適用します。

例

次の例は、Version 1 と Version 2 のコマンドを組み合せて、**rip** コマンドを入力した後に **show running-config rip** コマンドで情報のリストを表示する方法を示しています。**rip** コマンドでは、次のことを実行できます。

- 外部インターフェイスで MD5 認証を使用して Version 2 パッシブ RIP およびデフォルト RIP をイネーブルにし、セキュリティ アプライアンスおよびルータなどの他の RIP ピアで使用するキーを暗号化する。
- セキュリティ アプライアンスの内部インターフェイスで Version 1 パッシブ RIP のリスンをイネーブルにする。
- セキュリティ アプライアンスの dmz（非武装地帯）インターフェイスで Version 2 パッシブ RIP のリスンをイネーブルにする。

```
hostname(config)# rip outside passive version 2 authentication md5 thisisakey 2
hostname(config)# rip outside default version 2 authentication md5 thisisakey 2
hostname(config)# rip inside passive
hostname(config)# rip dmz passive version 2

hostname# show running-config rip
rip outside passive version 2 authentication md5 thisisakey 2
rip outside default version 2 authentication md5 thisisakey 2
rip inside passive version 1
rip dmz passive version 2
```

次の例は、暗号鍵をテキスト形式で渡す Version 2 機能の使用方法を示しています。

```
hostname(config)# rip out default version 2 authentication text thisisakey 3
hostname# show running-config rip
rip outside default version 2 authentication text thisisakey 3
```

関連コマンド

コマンド	説明
clear configure rip	実行コンフィギュレーションからすべての RIP コマンドを消去します。
debug rip	RIP に関するデバッグ情報を表示します。
show running-config rip	実行コンフィギュレーション内の RIP コマンドを表示します。

rmdir

既存のディレクトリを削除するには、特権 EXEC モードで **rmdir** コマンドを使用します。

rmdir [**/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）取り外しできない内部フラッシュ メモリを指定し、続けてコロン（:）を入力します。
disk1:	（オプション）取り外しできる外部フラッシュ 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）取り外しできない内部フラッシュを指定し、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	（オプション）削除するディレクトリの絶対パスまたは相対パス。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

ディレクトリが空でない場合、***rmdir*** コマンドは失敗します。

例

次の例は、「test」という名前の既存のディレクトリを削除する方法を示しています。

```
hostname# rmdir test
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
mkdir	新しいディレクトリを作成します。
pwd	現在の作業ディレクトリを表示します。
show file	ファイル システムに関する情報を表示します。

route

指定したインターフェイスのスタティック ルートまたはデフォルト ルートを入力するには、グローバル コンフィギュレーション モードで **route** コマンドを使用します。指定したインターフェイスから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。

route *interface_name ip_address netmask gateway_ip* [*metric* | ***tunneled***]

no route *interface_name ip_address netmask gateway_ip* [*metric* | ***tunneled***]

シンタックスの説明

gateway_ip	ゲートウェイ ルータの IP アドレスを指定します（このルートのネクストホップ アドレス）。 **（注）** *gateway_ip* 引数は、透過モードでのオプションです。
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。
ip_address	内部または外部のネットワーク IP アドレス。
metric	（オプション）このルートの管理ディスタンス。有効な値は、1 ～ 255 です。デフォルト値は 1 です。
netmask	*ip_address* に適用するネットワーク マスクを指定します。
tunneled	VPN トラフィックのデフォルト トンネル ゲートウェイとして、ルートを指定します。

デフォルト

metric のデフォルトは 1 です。

コマンドのモード

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
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

インターフェイスのデフォルト ルートまたはスタティック ルートを入力するには、**route** コマンドを使用します。デフォルト ルートを入力するには、*ip_address* と *netmask* を **0.0.0.0** に設定するか、短縮形の **0** を使用します。**route** コマンドを使用して入力したすべてのルートは、保存時にコンフィギュレーションに格納されます。

標準のデフォルト ルートに加えて、トンネル トラフィック用の別のデフォルト ルートを定義できます。***tunneled*** オプションを使用してデフォルト ルートを作成すると、セキュリティ アプライアンスに到達する暗号化されたトラフィックで、ラーニングされたルートまたはスタティック ルートのいずれでもルーティングできないトラフィックは、すべてこのルートに送信されます。トラフィックが暗号化されていない場合、標準のデフォルト ルート エントリが使用されます。***tunneled*** オプションで複数のデフォルト ルートを定義することはできません。トンネル トラフィックの ECMP はサポートされていません。

任意のインターフェイスでルータの外部に接続されているネットワークにアクセスするには、スタティック ルートを作成します。たとえば、セキュリティ アプライアンスはこのスタティック **route** コマンドを使用し、192.168.42.0 ネットワークに向けて 192.168.1.5 ルータ経由ですべてのパケットを送信します。

```
hostname(config)# route dmz 192.168.42.0 255.255.255.0 192.168.1.5 1
```

各インターフェイスの IP アドレスを入力すると、セキュリティ アプライアンスは、ルート テーブルに CONNECT ルートを作成します。このエントリは、**clear route** コマンドまたは **clear configure route** コマンドを使用しても削除できません。

route コマンドがセキュリティ アプライアンスのインターフェイスいずれか 1 つの IP アドレスをゲートウェイ IP アドレスとして使用する場合、セキュリティ アプライアンスはゲートウェイ IP アドレスに対して ARP を実行するのではなく、パケット内の宛先 IP アドレスに対して ARP を実行します。

例

次の例は、外部インターフェイスに対して 1 つのデフォルト **route** コマンドを指定する方法を示しています。

```
hostname(config)# route outside 0 0 209.165.201.1 1
```

次の例は、次のスタティック **route** コマンドを追加して、ネットワークへのアクセスを提供する方法を示しています。

```
hostname(config)# route dmz1 10.1.2.0 255.0.0.0 10.1.1.4 1
hostname(config)# route dmz1 10.1.3.0 255.0.0.0 10.1.1.4 1
```

関連コマンド

コマンド	説明
clear configure route	スタティックに設定された **route** コマンドを削除します。
clear route	RIP などのダイナミック ルーティング プロトコルを通じてラーニングされたルートを削除します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

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するには、グローバル コンフィギュレーション モードで **route-map** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

route-map *map_tag* [**permit** | **deny**] [*seq_num*]

no route-map *map_tag* [**permit** | **deny**] [*seq_num*]

シンタックスの説明

deny	（オプション）このルートマップが一致基準に適合した場合は、このルートを再配布しないことを指定します。
map_tag	ルートマップ タグのテキスト。テキストの長さは最大 57 文字です。
permit	（オプション）このルートマップが一致基準に適合した場合は、このルートを、設定アクションによる制御に従って再配布することを指定します。
seq_num	（オプション）ルートマップのシーケンス番号。有効な値は 0 ～ 65535 です。すでに同じ名前で設定されているルートマップのリストにおける新しいルートマップの位置を示します。

デフォルト

デフォルトは次のとおりです。

- **permit**
- *seq_num* を指定しない場合、*seq_num* の値 10 が最初のルートマップに割り当てられます。

コマンドのモード

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
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 コマンドを使用すると、ルートを再配布できます。

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 コマンドは、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。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 route-map 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。また、**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。

ルーティング プロセス間のルート再配布方法を細かく制御するには、ルートマップを使用します。宛先ルーティング プロトコルは、**router ospf** グローバル コンフィギュレーション コマンドで指定します。送信元ルーティング プロトコルは、**redistribute** ルータ コンフィギュレーション コマンドで指定します。

ルートマップを通じてルートを渡すとき、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** コマンドと関連する 1 つ以上の match 節と一致しないルートは、無視されます。そのルートが、発信ルートマップのためにアドバタイズされるか、着信ルートマップのために受け入れられることはありません。一部のデータのみを修正するには、正確に一致する基準を指定した 2 番目のルートマップ セクションを設定する必要があります。

seq_number 引数については、次のとおりです。

1. 提供されたタグでエントリを定義しない場合、*seq_number* 引数に 10 が設定されたエントリが作成されます。
2. 提供されたタグで 1 つだけエントリを定義した場合、そのエントリは、その後に続く **route-map** コマンドのデフォルト エントリとなります。このエントリの *seq_number* 引数は変更されません。
3. 提供されたタグで 2 つ以上のエントリを定義した場合、*seq_number* 引数が必要であることを示すエラー メッセージが出力されます。

no route-map *map-tag* コマンドを（*seq-num* 引数なしで）指定した場合、ルートマップ全体（同じ *map-tag* テキストを持つすべての **route-map** エントリ）が削除されます。

一致基準に適合しない場合に **permit** キーワードを指定してあれば、同じ *map_tag* を持つ次のルートマップがテストされます。ルートは、同じ名前を共有するルートマップ セットの一致基準に 1 つも一致しなかった場合、そのセットによって再配布されません。

例

次の例は、OSPF ルーティングで使用するルートマップを設定する方法を示しています。

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# show running-config route-map
route-map maptag1 permit 8
    set metric 5
    match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure 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削除します。
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。
router ospf	OSPF ルーティング プロセスを開始および設定します。
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。
show running-config route-map	ルートマップ コンフィギュレーションに関する情報を表示します。

router-id

固定ルータ ID を使用するには、ルータ コンフィギュレーション モードで **router-id** コマンドを使用します。先行の OSPF ルータ ID 動作を使用するように OSPF をリセットするには、このコマンドの **no** 形式を使用します。

router-id *addr*

no router-id [*addr*]

シンタックスの説明

addr	IP アドレス形式のルータ ID。

デフォルト

指定しない場合、セキュリティ アプライアンス上で最上位の IP アドレスがルータ ID として使用されます。

コマンドのモード

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
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
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

セキュリティ アプライアンス上で最上位の IP アドレスがプライベート アドレスの場合、このアドレスは hello パケットおよびデータベース定義で送信されます。この状況を回避するには、**router-id** コマンドを使用してルータ ID のグローバル アドレスを指定します。

例

次の例では、ルータ ID を 192.168.1.1 に設定します。

```
hostname(config-router)# router-id 192.168.1.1
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。

router ospf

OSPF ルーティング プロセスを開始し、そのプロセスのパラメータを設定するには、グローバル コンフィギュレーション モードで **router ospf** コマンドを使用します。OSPF 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。

router ospf *pid*

no router ospf *pid*

シンタックスの説明

pid	OSPF ルーティング プロセス用に内部的に使用される識別パラメータ。有効な値は、1 ～ 65535 です。*pid* は、他のルータ上の OSPF プロセスの ID と一致する必要はありません。

デフォルト

OSPF ルーティングはディセーブルになっています。

コマンドのモード

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
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

router ospf コマンドは、セキュリティ アプライアンス上で実行している OSPF ルーティング プロセスのグローバル コンフィギュレーション コマンドです。**router ospf** コマンドを入力すると、コマンド プロンプトは (config-router)# と表示されます。これは、ルータ コンフィギュレーション モードに入ったことを示しています。

no router ospf コマンドを使用する場合、必要な情報を提供するものでない限り、オプションの引数を使用する必要はありません。**no router ospf** コマンドは、*pid* で指定された OSPF ルーティング プロセスを終了します。*pid* をセキュリティ アプライアンス上でローカルに割り当てることができます。OSPF ルーティング プロセスごとに固有の値を割り当てる必要があります。

router ospf コマンドは、OSPF 固有の次のコマンドとともに使用され、OSPF ルーティング プロセスを設定します。

- **area**：通常の OSPF エリアを設定します。
- **compatible rfc1583**：RFC 1583 準拠のサマリー ルート コストの計算に使用される方式に戻します。
- **default-information originate**：OSPF ルーティング ドメイン内へのデフォルトの外部ルートを生成します。
- **distance**：ルート タイプに基づいて、OSPF ルートの管理ディスタンスを定義します。
- **ignore**：タイプ 6 Multicast OSPF（MOSPF）パケットの link-state advertisement（LSA; リンクステート アドバタイズメント）を受信した際に、syslog メッセージを送信しないようにします。

- **log-adj-changes**：OSPF 隣接ルータがアップ状態またはダウン状態になると syslog メッセージを送信するように、ルータを設定します。
- **neighbor**：隣接ルータを指定します。VPN トンネル経由での隣接関係の確立を可能にするために使用されます。
- **network**：OSPF を実行するインターフェイス、およびそれらのインターフェイスのエリア ID を定義します。
- **redistribute**：指定されたパラメータに基づく、あるルーティング ドメインから別のルーティング ドメインへのルートの再配布を設定します。
- **router-id**：固定ルータ ID を作成します。
- **summary-address**：OSPF の集約アドレスを作成します。
- **timers lsa-group-pacing**：OSPF LSA グループ間隔タイマー（リフレッシュまたは最大限にエージングされている LSA グループの間隔）。
- **timers spf**：SPF 計算に対する変更を受信する間隔。

セキュリティ アプライアンスで RIP が設定されている場合は、OSPF を設定できません。

例

次の例は、5 番の OSPF ルーティング プロセスのコンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# router ospf 5
hostname(config-router)#
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションから OSPF ルータ コマンドを消去します。
show running-config router ospf	実行コンフィギュレーション内の OSPF ルータ コマンドを表示します。