CHAPTER 20

mac-address-table aging-time ～ multicast-routing コマンド

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。デフォルト値の 5 分に戻すには、このコマンドの **no** 形式を使用します。

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

no mac-address-table *aging-time*

シンタックスの説明

timeout_value	MAC アドレス エントリがタイムアウトするまでに、MAC アドレス テーブルにとどまっている時間。5 ～ 720 分（12 時間）。5 分がデフォルトです。

デフォルト

デフォルトのタイムアウトは 5 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

例

次に、MAC アドレスのタイムアウトを 10 分に設定する例を示します。

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

関連コマンド

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

mac-address-table static

MAC アドレス テーブルにスタティック エントリを追加するには、グローバル コンフィギュレーション モードで **mac-address-table static** コマンドを使用します。スタティック エントリを削除するには、このコマンドの **no** 形式を使用します。

mac-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を設定します。
mac_address	テーブルに追加する MAC アドレスを設定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

MAC アドレスは通常、特定の MAC アドレスからのトラフィックがインターフェイスに着信したときに、MAC アドレス テーブルに動的に追加されます。必要に応じて、MAC アドレス テーブルにスタティック 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利点の 1 つは、MAC スプーフィング対策になることです。クライアントがスタティック エントリと同じ MAC アドレスを使用して、スタティック エントリと一致しないインターフェイスにトラフィックを送信しようとした場合、FWSM はトラフィックをドロップして、システム メッセージを生成します。

例

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

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

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table aging-time	ダイナミック MAC（メディア アクセス制御）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 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 コマンドで **mac-learn** コマンドを使用します。MAC アドレス ラーニングを再びイネーブルにするには、このコマンドの **no** 形式を使用します。

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を設定します。
disable	MAC ラーニングをディセーブルにします。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトで、各インターフェイスは着信トラフィックの MAC アドレスを自動的に学習し、FWSM が MAC アドレス テーブルに対応するエントリを追加します。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。

例

次に、外部インターフェイス上で MAC ラーニングをディセーブルにする例を示します。

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

関連コマンド

コマンド	説明
clear configure mac-learn	**mac-learn** の設定をデフォルトにします。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table static	MAC（メディア アクセス制御）アドレス テーブルにスタティック MAC アドレス エントリを追加します。
show mac-address-table	ダイナミック エントリおよびスタティック エントリを含めて、MAC アドレス テーブルを表示します。
show running-config mac-learn	**mac-learn** の設定を表示します。

mac-list

MAC ベースの認証に使用する MAC アドレスのリストを指定するには、グローバル コンフィギュレーション モードで **mac-list** コマンドを使用します。MAC アドレス リストの使用を禁止するには、このコマンドの **no** 形式を使用します。**mac-list** コマンドを使用すると、先頭一致検索を使用する MAC アドレスのリストが追加されます。

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	条件と一致するトラフィックは、MAC リストに*含めない*で、認証と許可の両方を要求することを指定します。
id	MAC アクセス リストに英数字の名前を指定します。
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	*mac* にネットマスクを指定して適用し、MAC アドレスのグループ分けができるようにします。
permit	条件と一致するトラフィックを MAC リストに*含め*、認証と許可の両方を免除することを指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

1 組の MAC アドレスをグループとしてまとめるには、同じ id 値を使用して、必要な回数だけ **mac-list** コマンドを入力します。**aaa mac-exempt** コマンドを使用する前に、**mac-list** コマンドを使用して MAC アクセス リスト番号を設定します。

実行されるのは AAA 免除だけです。認証が免除される MAC アドレスは、許可が自動的に免除されます。それ以外のタイプの AAA は **mac-list** ではサポートされません。

例

次に、MAC アドレス リストの設定例を示します。

```
hostname(config)# mac-list adc permit 00a0.ca5d.0282 ffff.ffff.ffff
hostname(config)# mac-list adc deny 00a1.ca5d.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、LOCAL、TACACS+、または RADIUS ユーザ認証をイネーブルまたはディセーブルに設定したり、表示したりします。または ASDM ユーザ認証をイネーブルまたはディセーブルにしたり、表示したりします。
aaa authorization	LOCAL または TACACS+ ユーザ認証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 リストの認証および許可を免除します。
clear configure mac-list	指定の MAC リスト番号を使用して、**mac-list** コマンドで指定した MAC アドレス リストを削除します。
show running-config mac-list	指定の MAC リスト番号を使用して、**mac-list** コマンドで指定した MAC アドレス リストを表示します。

management-access

FWSM へのログイン時に使用したインターフェイス以外のインターフェイスに対する管理アクセスを許可するには、グローバル コンフィギュレーション モード ***management-access*** コマンドを使用します。このアクセスを禁止するには、このコマンドの **no** 形式を使用します。

management-access *mgmt_if*

no management-access *mgmt_if*

シンタックスの説明

mgmt_if	別のインターフェイスから FWSM に接続するときにアクセスする管理インターフェイスの名前を指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、FWSM へのログイン時に使用した以外のインターフェイスに接続できます。たとえば、外部インターフェイスから FWSM にログインした場合、このコマンドを使用することによって、Telnet で内部インターフェイスに接続できます。または、外部インターフェイスからログインした場合は、内部インターフェイスに ping を実行できます。

定義できる管理インターフェイスは 1 つだけです。

management-access コマンドは、IPSec VPN トンネルを介して、次の場合に限りサポートされます。

- 管理インターフェイスへの SNMP ポーリング
- 管理インターフェイスへの HTTPS 要求
- 管理インターフェイスへの ASDM アクセス
- 管理インターフェイスへの Telnet アクセス
- 管理インターフェイスへの SSH アクセス
- 管理インターフェイスへの ping
- 管理インターフェイスへの Syslog ポーリング
- 管理インターフェイスへの NTP 要求

例

次に、管理アクセス用インターフェイスとして、[inside] というファイアウォール インターフェイスを設定する例を示します。

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

関連コマンド

コマンド	説明
clear configure management-access	FWSM の管理アクセス用インターフェイスの設定を削除します。
show management-access	管理アクセス用に設定されているインターフェイスの名前を表示します。

mask-syst-reply

クライアントから FTP サーバ応答が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。FTP マップ コンフィギュレーション モードには、**ftp-map** コマンドを使用してアクセスします。この設定を削除するには、このコマンドの **no** 形式を使用します。

mask-syst-reply

no mask-syst-reply

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

クライアントから FTP サーバ システムを保護するには、完全 FTP 検査を指定して、mask-syst-reply コマンドを使用します。このコマンドをイネーブルにすると、**syst** コマンドに対するサーバの応答が X の連続に置き換えられます。

例

次に、syst コマンドに対する FTP サーバの応答を FWSM が X に置き換えるようにする例を示します。

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

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
ftp-map	FTP マップを定義し、FTP マップ コンフィギュレーション モードをイネーブルにします。
inspect ftp	特定の FTP マップがアプリケーション検査で使用されるようにします。
policy-map	特定のセキュリティ アクションにクラス マップを対応付けます。
request-command deny	禁止する FTP コマンドを指定します。

match access-list

クラス マップでアクセス リストを使用してトラフィックを特定するには、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	一致条件として使用する ACL の名前を指定します。パケットが ACL のエントリと一致しなかった場合、照合結果は no-match になります。パケットが ACL のエントリと一致し、なおかつ許可エントリだった場合、照合結果は match になります。拒否の ACL エントリと一致した場合の照合結果は、no-match になります。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

match コマンドは、トラフィック クラスのクラス マップに含まれるトラフィックを特定する場合に使用します。このコマンドでさまざまな条件を指定して、クラス マップに含まれるトラフィックを定義します。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てセキュリティ機能を設定するときに、**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** コマンドを使用することによって、クラスに含めるトラフィックを定義できます。

インターフェイスにトラフィック クラスが適用されると、そのインターフェイスで受信したパケットがクラス マップの **match** ステートメントで定義された条件と比較されます。指定された条件と一致したパケットは、トラフィック クラスに含まれ、そのトラフィック クラスに対応付けられたアクションの対象となります。トラフィック クラスで指定された条件のいずれとも一致しなかったパケットは、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 コマンドを使用し、1 つ以上のアクセス リストを指定することによって、具体的なトラフィック タイプを特定できます。トラフィックは、アクセス制御エントリの **permit** ステートメントによってトラフィック クラス マップに組み込まれ、**deny** ステートメントによってトラフィック クラス マップから除外されます。

例

次に、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 クラスを定義する例を示します。

```
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	インターフェイスにトラフィック クラスを適用します。
clear configure class-map	トラフィック マップ定義を削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップで具体的なポート番号を指定します。
show running-config class-map	クラス マップの設定情報を表示します。

match any

クラス マップにすべてのトラフィックを含めるには、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、引数またはキーワードはありません。

デフォルト　このコマンドには、デフォルトの動作または値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン　**match** コマンドは、トラフィック クラスのクラス マップに含まれるトラフィックを特定する場合に使用します。このコマンドでさまざまな条件を指定して、クラス マップに含まれるトラフィックを定義します。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てセキュリティ機能を設定するときに、**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** コマンドを使用することによって、クラスに含めるトラフィックを定義できます。

インターフェイスにトラフィック クラスが適用されると、そのインターフェイスで受信したパケットがクラス マップの **match** ステートメントで定義された条件と比較されます。指定された条件と一致したパケットは、トラフィック クラスに含まれ、そのトラフィック クラスに対応付けられたアクションの対象となります。トラフィック クラスで指定された条件のいずれとも一致しなかったパケットは、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 any コマンドを使用すると（デフォルト クラス マップの class-default と同様）、すべてのパケットが一致します。

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

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

関連コマンド

コマンド	説明
class-map	インターフェイスにトラフィック クラスを適用します。
clear configure class-map	トラフィック マップの定義をすべて削除します。
match access-list	クラス マップでアクセス リスト トラフィックを特定します。
match rtp	クラス マップで特定の RTP ポートを指定します。
show running-config class-map	クラス マップの設定情報を表示します。

match default-inspection-traffic

クラス マップで inspect コマンドに対応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、引数またはキーワードはありません。

デフォルト

各検査のデフォルト トラフィックについては、「使用上のガイドライン」を参照してください。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

match コマンドは、トラフィック クラスのクラス マップに含まれるトラフィックを特定する場合に使用します。このコマンドでさまざまな条件を指定して、クラス マップに含まれるトラフィックを定義します。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てセキュリティ機能を設定するときに、**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** コマンドを使用することによって、クラスに含めるトラフィックを定義できます。

インターフェイスにトラフィック クラスが適用されると、そのインターフェイスで受信したパケットがクラス マップの **match** ステートメントで定義された条件と比較されます。指定された条件と一致したパケットは、トラフィック クラスに含まれ、そのトラフィック クラスに対応付けられたアクションの対象となります。トラフィック クラスで指定された条件のいずれとも一致しなかったパケットは、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** コマンドに対応するデフォルト トラフィックを照合できます。**match default-inspection-traffic** コマンドは、他の 1 つの match コマンドと組み合わせて使用できます。通常は、***permit ip*** *src-ip dst-ip* の形式で、access-list と組み合わせます。

match default-inspection-traffic コマンドと 2 番めの **match** コマンドを組み合わせる場合は、**match default-inspection-traffic** コマンドでプロトコルおよびポート情報を指定し、2 番めの **match** コマンドでその他のあらゆる情報（IP アドレスなど）を指定するのがルールです。2 番めの **match** コマンドで指定したプロトコルおよびポート情報は、**inspect** コマンドに関しては無視されます。

たとえば、次の例で指定した 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 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

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

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

関連コマンド

コマンド	説明
class-map	インターフェイスにトラフィック クラスを適用します。
clear configure class-map	トラフィック マップの定義をすべて削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを特定します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップの設定情報を表示します。

match dscp

クラス マップで IETF 定義の（IP ヘッダーの）DSCP 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 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 IETF で定義された DSCP 値を 8 種類まで指定します。範囲は 0 ～ 63 です。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

match コマンドは、トラフィック クラスのクラス マップに含まれるトラフィックを特定する場合に使用します。このコマンドでさまざまな条件を指定して、クラス マップに含まれるトラフィックを定義します。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てセキュリティ機能を設定するときに、**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** コマンドを使用することによって、クラスに含めるトラフィックを定義できます。

インターフェイスにトラフィック クラスが適用されると、そのインターフェイスで受信したパケットがクラス マップの **match** ステートメントで定義された条件と比較されます。指定された条件と一致したパケットは、トラフィック クラスに含まれ、そのトラフィック クラスに対応付けられたアクションの対象となります。トラフィック クラスで指定された条件のいずれとも一致しなかったパケットは、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 で定義された DSCP 値を照合できます。

例

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

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

関連コマンド

コマンド	説明
class-map	インターフェイスにトラフィック クラスを適用します。
clear configure class-map	トラフィック マップの定義をすべて削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを特定します。
match port	そのインターフェイスで受信したパケットの比較条件として、TCP/UDP ポートを指定します。
show running-config class-map	クラス マップの設定情報を表示します。

match interface

指定されたインターフェイスのいずれかを起点とするネクスト ホップが存在するルートを配布するには、ルート マップ コンフィギュレーション モードで **match interface** コマンドを使用します。match interface エントリを削除するには、このコマンドの **no** 形式を使用します。

match interface *interface-name...*

no match interface *interface-name...*

シンタックスの説明

interface-name	**nameif** コマンドで指定されたインターフェイスの名前。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ません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

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

route-map グローバル コンフィギュレーション コマンドや、**match** および **set** コンフィギュレーション コマンドを使用すると、ルーティング プロトコル間でのルートの再配布条件を定義できます。各 **route-map** コマンドには、**match** および **set** コマンドが関連付けられています。**match** コマンドでは一致条件（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドでは set アクション（**match** コマンドの実行条件が満たされている場合に実行される特定の再配布アクション）を指定します。**no route-map** コマンドを使用すると、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番で指定できます。**set** コマンドで指定された set アクションに従ってルートを再配布するには、すべての **match** コマンドと「一致する」必要があります。**match** コマンドの **no** 形式を使用すると、指定の一致条件が削除されます。**match** コマンドで複数のインターフェイスが指定されている場合、**no match interface** *interface-name* で削除できるインターフェイスは 1 つだけです。

ルート マップは複数の部分で構成できます。**route-map** コマンドに関連付けられているどの match 節と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変更する場合は、別のルート マップ セクションを設定し、明示的な一致を指定します。

例

次に、ネクスト ホップが外部のルートを配布する例を示します。

```
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	指定のアクセス リストのいずれかと一致する、ネクストホップ ルータ アドレスが含まれるすべてのルートを配布します。
match ip route-source	アクセス リストで指定されたアドレスにあるルータおよびアクセス サーバによってアドバタイズされたルートを再配布します。
match metric	指定されたメトリックのルートを再配布します。
route-map	ルーティング プロトコル間でルートを再配布する条件を定義します。
set metric	ルート マップに対応する宛先ルーティング プロトコルのメトリック値を指定します。

match ip address

指定されたアクセス リストのいずれかと一致するルート アドレスまたは一致パケット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 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	ACL を名前で指定します。複数の ACL を指定できます。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

route-map グローバル コンフィギュレーション コマンドや、**match** および **set** コンフィギュレーション コマンドを使用すると、ルーティング プロトコル間でのルートの再配布条件を定義できます。各 **route-map** コマンドには、**match** および **set** コマンドが関連付けられています。**match** コマンドでは一致条件（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドでは set アクション（**match** コマンドの実行条件が満たされている場合に実行される特定の再配布アクション）を指定します。**no route-map** コマンドを使用すると、ルート マップが削除されます。

例

次に、内部ルートを再配布する例を示します。

```
hostname(config)# route-map name
hostname(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

関連コマンド

コマンド	説明
match interface	指定のインターフェイスを起点とするネクスト ホップのあるルートを配布します。
match ip next-hop	指定のアクセス リストのいずれかと一致する、ネクストホップ ルータ アドレスが含まれるすべてのルートを配布します。
match metric	指定されたメトリックのルートを再配布します。
route-map	ルーティング プロトコル間でルートを再配布する条件を定義します。
set metric	ルート マップに対応する宛先ルーティング プロトコルのメトリック値を指定します。

match ip next-hop

指定されたアクセス リストのいずれかと一致するネクスト ホップ ルータ アドレス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 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

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

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

route-map グローバル コンフィギュレーション コマンドや、**match** および **set** コンフィギュレーション コマンドを使用すると、ルーティング プロトコル間でのルートの再配布条件を定義できます。各 **route-map** コマンドには、**match** および **set** コマンドが関連付けられています。**match** コマンドでは一致条件（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドでは set アクション（**match** コマンドの実行条件が満たされている場合に実行される特定の再配布アクション）を指定します。**no route-map** コマンドを使用すると、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番で入力できます。**set** コマンドで指定された set アクションに従ってルートを再配布するには、すべての **match** コマンドと「一致する」必要があります。**match** コマンドの **no** 形式を使用すると、指定の一致条件が削除されます。

ルート マップを使用してルートを渡す場合、ルート マップは複数の部分で構成できます。**route-map** コマンドに関連付けられているどの match 節と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変更する場合は、別のルート マップ セクションを設定し、明示的な一致を指定します。

例

次に、アクセス リスト acl_dmz1 または acl_dmz2 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例を示します。

```
hostname# 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	指定のインターフェイスを起点とするネクスト ホップのあるルートを配布します。
match ip next-hop	指定のアクセス リストのいずれかと一致する、ネクストホップ ルータ アドレスが含まれるすべてのルートを配布します。
match metric	指定されたメトリックのルートを再配布します。
route-map	ルーティング プロトコル間でルートを再配布する条件を定義します。
set metric	ルート マップに対応する宛先ルーティング プロトコルのメトリック値を指定します。

match ip route-source

アクセス リストで指定されたアドレス上のルータおよびアクセス サーバによってアドバタイズされたルートを再配布するには、ルート マップ コンフィギュレーション モードで **match ip route-source** コマンドを使用します。ネクストホップ エントリを削除するには、このコマンドの **no** 形式を使用します。

match ip route-source {*acl...*| ***prefix-list*** *prefix_list*}

no match ip route-source {*acl...*| ***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	プレフィックス リストの名前

デフォルト

ルート送信元に関するフィルタリングを行いません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

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

route-map グローバル コンフィギュレーション コマンドや、**match** および **set** コンフィギュレーション コマンドを使用すると、ルーティング プロトコル間でのルートの再配布条件を定義できます。各 **route-map** コマンドには、**match** および **set** コマンドが関連付けられています。**match** コマンドでは一致条件（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドでは set アクション（**match** コマンドの実行条件が満たされている場合に実行される特定の再配布アクション）を指定します。**no route-map** コマンドを使用すると、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番で入力できます。**set** コマンドで指定された set アクションに従ってルートを再配布するには、すべての **match** コマンドと「一致する」必要があります。**match** コマンドの **no** 形式を使用すると、指定の一致条件が削除されます。

ルート マップは複数の部分で構成できます。**route-map** コマンドに関連付けられているどの match 節と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変更する場合は、別のルート マップ セクションを設定し、明示的な一致を指定します。ルートのネクストホップおよび送信元ルータ アドレスは、異なる場合があります。

例

次に、アクセス リスト acl_dmz1 および acl_dmz2 で指定されたアドレス上のルータおよびアクセス サーバによってアドバタイズされたルートを配布する例を示します。

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

関連コマンド

コマンド	説明
match interface	指定のインターフェイスを起点とするネクスト ホップのあるルートを配布します。
match ip next-hop	指定のアクセス リストのいずれかと一致する、ネクストホップ ルータ アドレスが含まれるすべてのルートを配布します。
match metric	指定されたメトリックのルートを再配布します。
route-map	ルーティング プロトコル間でルートを再配布する条件を定義します。
set metric	ルート マップに対応する宛先ルーティング プロトコルのメトリック値を指定します。

match metric

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

match metric *number*

no match metric *number*

シンタックスの説明

number	ルータ メトリック値。有効値は 0 ～ 4294967295 です。

デフォルト

メトリック値に関するフィルタリングを行いません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

route-map グローバル コンフィギュレーション コマンドや、**match** および **set** コンフィギュレーション コマンドを使用すると、ルーティング プロトコル間でのルートの再配布条件を定義できます。各 **route-map** コマンドには、**match** および **set** コマンドが関連付けられています。**match** コマンドでは一致条件（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドでは set アクション（**match** コマンドの実行条件が満たされている場合に実行される特定の再配布アクション）を指定します。**no route-map** コマンドを使用すると、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番で指定できます。また、**set** コマンドで指定された set アクションに従ってルートを再配布するには、すべての **match** コマンドと「一致する」必要があります。**match** コマンドの **no** 形式を使用すると、指定の一致条件が削除されます。

ルート マップは複数の部分で構成できます。**route-map** コマンドに関連付けられているどの match 節と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変更する場合は、別のルート マップ セクションを設定し、明示的な一致を指定します。

例

次に、メトリックが 5 のルートを再配布する例を示します。

```
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	指定のインターフェイスを起点とするネクスト ホップのあるルートを配布します。
match ip next-hop	指定のアクセス リストのいずれかと一致する、ネクストホップ ルータ アドレスが含まれるすべてのルートを配布します。
route-map	ルーティング プロトコル間でルートを再配布する条件を定義します。
set metric	ルート マップに対応する宛先ルーティング プロトコルのメトリック値を指定します。

match port

クラス マップで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（1 ～ 65535）の開始値と終了値を指定します。
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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

match コマンドは、トラフィック クラスのクラス マップに含まれるトラフィックを特定する場合に使用します。このコマンドでさまざまな条件を指定して、クラス マップに含まれるトラフィックを定義します。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てセキュリティ機能を設定するときに、**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** コマンドを使用することによって、クラスに含めるトラフィックを定義できます。

インターフェイスにトラフィック クラスが適用されると、そのインターフェイスで受信したパケットがクラス マップの **match** ステートメントで定義された条件と比較されます。指定された条件と一致したパケットは、トラフィック クラスに含まれ、そのトラフィック クラスに対応付けられたアクションの対象となります。トラフィック クラスで指定された条件のいずれとも一致しなかったパケットは、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 port コマンドは、ポート範囲を指定する場合に使用します。

例

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

```
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq 8080
```

関連コマンド

コマンド	説明
class-map	インターフェイスにトラフィック クラスを適用します。
clear configure class-map	トラフィック マップの定義をすべて削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを特定します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップの設定情報を表示します。

match precedence

クラス マップで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	最大 4 つの優先順位値をスペースで区切って指定します。範囲は 0 ～ 7 です。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

match コマンドは、トラフィック クラスのクラス マップに含まれるトラフィックを特定する場合に使用します。このコマンドでさまざまな条件を指定して、クラス マップに含まれるトラフィックを定義します。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てセキュリティ機能を設定するときに、**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** コマンドを使用することによって、クラスに含めるトラフィックを定義できます。

インターフェイスにトラフィック クラスが適用されると、そのインターフェイスで受信したパケットがクラス マップの **match** ステートメントで定義された条件と比較されます。指定された条件と一致したパケットは、トラフィック クラスに含まれ、そのトラフィック クラスに対応付けられたアクションの対象となります。トラフィック クラスで指定された条件のいずれとも一致しなかったパケットは、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 precedence コマンドは、IP ヘッダーの TOS バイトで表された値を指定する場合に使用します。

例

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

```
hostname(config)# class-map cmap
hostname(config-cmap)# match precedence 1
```

関連コマンド

コマンド	説明
class-map	インターフェイスにトラフィック クラスを適用します。
clear configure class-map	トラフィック マップの定義をすべて削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを特定します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップの設定情報を表示します。

match route-type

指定されたタイプのルートを再配布するには、ルート マップ コンフィギュレーションモードで **match route-type** コマンドを使用します。ルート タイプ エントリを削除するには、このコマンドの **no** 形式を使用します。

match route-type {**local** | **internal** | {**external** [**type-1** | **type-2**]} | {**nssa-external** [**type-1** | **type-2**]}}

no match route-type {**local** | **internal** | {**external** [**type-1** | **type-2**]} | {**nssa-external** [**type-1** | **type-2**]}}

シンタックスの説明

external	OSPF 外部ルート（タイプ 1 またはタイプ 2）を照合します。
internal	OSPF エリア内ルートおよびエリア間ルートを照合します。
local	ローカルで生成されたルートを照合します。
nssa-external	OSPF NSSA 外部ルート（タイプ 1 またはタイプ 2）を照合します。
type-1	（任意）タイプ 1 のルートだけを照合します。
type-2	（任意）タイプ 2 のルートだけを照合します。

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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

route-map グローバル コンフィギュレーション コマンドや、**match** および **set** コンフィギュレーション コマンドを使用すると、ルーティング プロトコル間でのルートの再配布条件を定義できます。各 **route-map** コマンドには、**match** および **set** コマンドが関連付けられています。**match** コマンドでは一致条件（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドでは set アクション（**match** コマンドの実行条件が満たされている場合に実行される特定の再配布アクション）を指定します。**no route-map** コマンドを使用すると、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番で入力できます。**set** コマンドで指定された set アクションに従ってルートを再配布するには、すべての **match** コマンドと「一致する」必要があります。**match** コマンドの **no** 形式を使用すると、指定の一致条件が削除されます。

ルート マップは複数の部分で構成できます。**route-map** コマンドに関連付けられているどの match 節と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変更する場合は、別のルート マップ セクションを設定し、明示的な一致を指定します。

例

次に、内部ルートを再配布する例を示します。

```
hostname(config)# route-map name
hostname(config-route-map)# match route-type internal
```

関連コマンド

コマンド	説明
match interface	指定のインターフェイスを起点とするネクスト ホップのあるルートを配布します。
match ip next-hop	指定のアクセス リストのいずれかと一致する、ネクストホップ ルータ アドレスが含まれるすべてのルートを配布します。
match metric	指定されたメトリックのルートを再配布します。
route-map	ルーティング プロトコル間でルートを再配布する条件を定義します。
set metric	ルート マップに対応する宛先ルーティング プロトコルのメトリック値を指定します。

match rtp

クラス マップで偶数番号のポートの 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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

match コマンドは、トラフィック クラスのクラス マップに含まれるトラフィックを特定する場合に使用します。このコマンドでさまざまな条件を指定して、クラス マップに含まれるトラフィックを定義します。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てセキュリティ機能を設定するときに、**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** コマンドを使用することによって、クラスに含めるトラフィックを定義できます。

インターフェイスにトラフィック クラスが適用されると、そのインターフェイスで受信したパケットがクラス マップの **match** ステートメントで定義された条件と比較されます。指定された条件と一致したパケットは、トラフィック クラスに含まれ、そのトラフィック クラスに対応付けられたアクションの対象となります。トラフィック クラスで指定された条件のいずれとも一致しなかったパケットは、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 rtp コマンドは、RTP ポート（*starting_port* から *starting_port* に *range* を加えたものまでの間の偶数の UDP ポート）を照合する場合に使用します。

例

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

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

関連コマンド

コマンド	説明
class-map	インターフェイスにトラフィック クラスを適用します。
clear configure class-map	トラフィック マップの定義をすべて削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを特定します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップの設定情報を表示します。

max-failed-attempts

サーバ グループ内の所定のサーバが停止するまでに、サーバで許容される試行失敗の回数を指定するには、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。この指定を削除して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 の整数。先行する **aaa-server** コマンドで指定されたサーバ グループの個々のサーバで許容される、接続試行の失敗回数を指定します。

デフォルト

number のデフォルト値は 3 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ グループ	•	•	•	•	—

コマンド履歴

リリース	変更
7.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを発行する前に、AAA サーバまたは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 モードを開始して、グループ固有の AAA サーバ パラメータおよびグループ内の全ホストに共通の AAA サーバ パラメータを設定します。
clear configure aaa-server	すべての AAA サーバ コンフィギュレーションを削除します。
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について、AAA サーバの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。HTTP マップ コンフィギュレーション モードには、**http-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、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失敗した場合に実行するアクション
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（1 ～ 65535）
log	（任意）Syslog を生成します。
request	メッセージを要求します。
reset	クライアントおよびサーバに TCP リセット メッセージを送信します。
response	（任意）応答メッセージ

デフォルト

このコマンドは、デフォルトではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
3.1	このコマンドが追加されました。

使用上のガイドライン

max-header-length コマンドをイネーブルにすると、FWSM は HTTP ヘッダーが設定限度内のメッセージだけを許可し、それ以外のメッセージには指定されたアクションを実行します。FWSM に TCP 接続をリセットさせ、任意で Syslog エントリを作成する場合は、**action** キーワードを使用します。

例

次に、HTTP ヘッダーが 100 バイト以下の HTTP 要求に制限する例を示します。ヘッダーが大きすぎる場合、FWSM は TCP 接続をリセットし、Syslog エントリを作成します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# max-header-length request bytes 100 action log reset
hostname(config-http-map)# 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トラフィック クラスを定義します。
debug appfw	拡張 HTTP 検査に関連付られたトラフィックの詳細情報を表示します。
http-map	拡張 HTTP 検査を設定するために HTTP マップを定義します。
inspect http	特定の HTTP マップがアプリケーション検査で使用されるようにします。
policy-map	特定のセキュリティ アクションにクラス マップを対応付けます。

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。HTTP マップ コンフィギュレーション モードには、**http-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、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失敗した場合に実行するアクション
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（1 ～ 65535）
log	（任意）Syslog を生成します。
reset	クライアントおよびサーバに TCP リセット メッセージを送信します。

デフォルト

このコマンドは、デフォルトではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
3.1	このコマンドが追加されました。

使用上のガイドライン

max-uri-length コマンドをイネーブルにすると、FWSM は URI が設定限度内のメッセージだけを許可し、それ以外のメッセージには指定されたアクションを実行します。FWSM に TCP 接続をリセットさせ、Syslog エントリを作成する場合は、**action** キーワードを使用します。

長さが設定値以下の URI は許可されます。それ以外は、指定されたアクションが実行されます。

例

次に、URI が 100 バイト以下のものに HTTP 要求を制限する例を示します。URI が大きすぎる場合、FWSM は TCP 接続をリセットし、Syslog エントリを作成します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# max-uri-length 100 action reset log
hostname(config-http-map)# 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トラフィック クラスを定義します。
debug appfw	拡張 HTTP 検査に関連付られたトラフィックの詳細情報を表示します。
http-map	拡張 HTTP 検査を設定するために HTTP マップを定義します。
inspect http	特定の HTTP マップがアプリケーション検査で使用されるようにします。
policy-map	特定のセキュリティ アクションにクラス マップを対応付けます。

mcc

IMSI プレフィクス フィルタリングのために、モバイル国別コードおよびモバイル ネットワーク コードを指定するには、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。この設定を削除するには、このコマンドの **no** 形式を使用します。

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

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

シンタックスの説明

country_code	モバイル国別コードを指定する、ゼロ以外の 3 桁の値。1 桁または 2 桁の値を入力した場合は、前に 0 が付加されて 3 桁の値が作成されます。
network_code	ネットワーク コードを指定する 2 桁 または 3 桁の値

デフォルト

デフォルトでは、FWSM は MCC/MNC の組み合わせが有効かどうかを確認しません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IMSI プレフィクスのフィルタリングに使用します。受信したパケットの IMSI に含まれている MCC および MNC とこのコマンドで設定された MCC/MNC が比較され、一致していない場合はパケットがドロップされます。

IMSI プレフィクス 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。複数のインスタンスを設定し、許可する MCC と MNC の組み合わせを指定できます。デフォルトでは、FWSM は MNC と MCC の組み合わせが有効かどうかを調べないので、ユーザ側で設定された組み合わせの有効性を確認する必要があります。MCC コードおよび MNC コードの詳細については、ITU E.212 の勧告『*Identification Plan for Land Mobile Stations*』を参照してください。

例

次に、MCC として 111、MNC として 222 を指定して、IMSI プレフィクス フィルタリングを行うトラフィックを特定する例を示します。

```
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 検査の詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	特定の GTP マップがアプリケーション検査で使用されるようにします。
show service-policy inspect gtp	GTP 設定を表示します。

member

リソース クラスにコンテキストを割り当てるには、コンテキスト コンフィギュレーション モードで **member** コマンドを使用します。クラスからコンテキ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。

member *class_name*

no member *class_name*

シンタックスの説明

class_name	**class** コマンドで作成したクラス名を指定します。

デフォルト

デフォルトでは、コンテキストはデフォルト クラスに割り当てられます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、コンテキスト別の最大限度が適用される場合を除き、あらゆるセキュリティ コンテキストが FWSM のリソースに無制限にアクセスできます。ただし、1 つまたは複数のコンテキストがリソースを多く使用しすぎていて、他のコンテキストの接続が拒否される場合など、リソース管理を設定してコンテキストごとのリソースの使用を制限できます。FWSM は、リソース クラスにコンテキストを割り当てることによってリソースを管理します。各コンテキストは、クラスによって設定されたリソース限度を使用します。

例

次に、gold クラスにコンテキスト test を割り当てる例を示します。

```
hostname(config)# context test
hostname(config-ctx)# allocate-interface vlan100 int1
hostname(config-ctx)# allocate-interface vlan102 int2
hostname(config-ctx)# allocate-interface vlan110-vlan115 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold
hostname(config-ctx)# allocate-acl-partition 0
```

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
context	セキュリティ コンテキストを設定します。
limit-resource	リソース限度を設定します。
show resource allocation	各クラスのリソース割り当てを表示します。
show resource types	制限を設定できるリソース タイプを表示します。

memory caller-address

メモリの問題を特定するために、コール トレースすなわち発信者 PC 用にプログラム メモリの特定の範囲を設定するには、特権 EXEC モードで ***memory caller-address*** コマンドを使用します。発信者 PC は、メモリ割り当てプリミティブを呼び出したプログラムのアドレスです。アドレス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

メモリ追跡では、実際の発信者 PC が記録されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドのサポートが追加されました。

使用上のガイドライン

memory caller-address コマンドは、メモリの問題を特定のメモリ ブロックに分離するために使用します。

場合によって、メモリ割り当てプリミティブの実際の発信者 PC は、プログラムのさまざまな場所で使用される既知のライブラリ関数です。プログラム内の個々の位置を特定するには、ライブラリ関数の開始プログラム アドレスと終了プログラム アドレスを設定し、ライブラリ関数の発信者プログラム アドレスを記録します。

（注） 発信者のアドレス トレースをイネーブルにすると、FWSM のパフォーマンスが一時的に低下する可能性があります。

例

次に、***memory caller-address*** コマンドを使用して設定されたアドレス範囲を表示する例、および ***show memory-caller address*** コマンドの出力例を示します。

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

hostname# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用率（メモリ プロファイリング）のモニタリングをイネーブルにします。
memory profile text	プロファイリングするメモリのテキスト範囲を設定します。
show memory	OS で使用可能な最大物理メモリおよび現在の空きメモリに関するサマリーを表示します。
show memory binsize	特定の bin サイズに対して割り当てられたチャンクに関するサマリー情報を表示します。
show memory profile	FWSM のメモリ使用率（プロファイル）に関する情報を表示します。
show memory-caller address	FWSM に設定されたアドレス範囲を表示します。

memory delayed-free-poisoner enable

delayed free-memory poisoner ツールをイネーブルにするには、特権 EXEC モードで **memory delayed-free-poisoner enable** コマンドを使用します。delayed free-memory poisoner ツールをディセーブルにするには、このコマンドの **no** 形式を使用します。delayed free-memory poisoner ツールを使用すると、アプリケーションによって解放されたメモリが、解放後に変更されていないか監視できます。

memory delayed free poisoner enable

no memory delayed free poisoner enable

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

memory delayed-free-poisoner enable コマンドは、デフォルトではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

delayed free-memory poisoner ツールをイネーブルにすると、メモリ使用状況およびシステム パフォーマンスに重大な影響があります。このコマンドは、シスコ TAC の監視のもとでのみ使用してください。システムの負荷が大きい時間帯に実稼働環境でこのコマンドを使用しないでください。

このツールをイネーブルにすると、FWSM で実行中のアプリケーションによって発行されたメモリ解放要求が FIFO キューに書き込まれます。各要求が FIFO キューに書き込まれる際、その対象となるメモリ バイトのうち低レベルのメモリ管理には使用されない部分に、値 0xcc が書き込まれて「無効化」されます。

メモリ解放要求は、アプリケーションで、空きメモリ プールよりも多くのメモリが必要になるまで、キューに保持されます。メモリが必要になると、最初のメモリ解放要求がキューから取り出され、無効化されたメモリが検証されます。

無効化されたメモリ領域が変更されていない場合は、低レベルのメモリ プールに戻され、delayed free-memory poisoner ツールが、最初の要求を行ったアプリケーションからのメモリ要求を再発行します。このプロセスは、要求元のアプリケーションにとって十分なメモリが解放されるまで繰り返されます。

無効化されたメモリ領域が変更されている場合は、クラッシュが発生し、クラッシュの原因を判断するための診断が出力されます。

delayed free-memory poisoner ツールは、定期的に、キューに登録されているすべての要素を自動的に検証します。**memory delayed-free-poisoner validate** コマンドを使用して、検証を手動で起動することもできます。

このコマンドの **no** 形式を使用すると、要求によって参照されているキュー内のすべてのメモリ領域が空きメモリ プールに戻されます。その際、それらのメモリに対する検証は行われず、すべての統計情報カウンタは消去されます。

例

次の例では、delayed free-memory poisoner ツールをイネーブルにする例を示します。

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

次に、delayed free-memory poisoner ツールがメモリの不正な再利用を検出したときの出力例を示します。

```
delayed-free-poisoner validate failed because a
        data signature is invalid at delayfree.c:328.

    heap region:    0x025b1cac-0x025b1d63 (184 bytes)
    memory address: 0x025b1cb4
    byte offset:    8
    allocated by:   0x0060b812
    freed by:       0x0060ae15

Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80:                         ef cd 1c a1 e1 00 00 00  |          ........
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02  |  #.........`.h.^.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02  |  ..[...`.....l&[.
025b1cb0: 8e a5 ea 10 ff ff ff ff cc cc cc cc cc cc cc cc  |  ................
025b1cc0: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  |  ................
025b1cd0: cc cc cc cc cc cc cc cc                         |  ........

An internal error occurred.  Specifically, a programming assertion was
violated.  Copy the error message exactly as it appears, and get the
output of the show version command and the contents of the configuration
file.  Then call your technical support representative.

assertion "0" failed: file "delayfree.c", line 191
```

表 20-1 に、上記の出力の重要な部分について説明します。

表 20-1　不正メモリ使用の出力の説明

フィールド	説明
heap region	要求を行っているアプリケーションが使用できるアドレス領域とメモリ領域のサイズ。これは要求されたサイズと同じではありません。システムは、メモリ要求が行われた時点でメモリを分配する方法をとるため、アプリケーションが使用できるサイズは要求されたサイズよりも小さくなる場合があります。
memory address	メモリ内の異常が検出されたアドレス
byte offset	byte offset はヒープ領域の先頭からの相対位置で、実行結果を使用してこのアドレスから始まるデータ構造を格納した場合、変更されたフィールドを検索できます。値が 0 またはヒープ領域バイト カウントよりも値が大きい場合、問題は低レベル ヒープ パッケージの予期しない値であることを示している可能性があります。

表 20-1　不正メモリ使用の出力の説明（続き）

フィールド	説明
allocated by/freed by	特定のメモリ領域を対象にした最後の malloc/calloc/realloc および free コールが行われた命令アドレス
Dumping...	メモリ領域のダンプ。検出された異常がヒープ メモリ領域の先頭からどれだけ近いかに応じて、1 つまたは 2 つのダンプが出力されます。システム ヒープ ヘッダーの次の 8 バイトは、このツールがさまざまなシステム ヘッダー値のハッシュおよびキュー リンケージを格納するのに使用するメモリです。領域内のそれ以外のすべてのバイトには、システム ヒープ トレーラが検出される位置まで、0xcc に設定されている必要があります。

関連コマンド

コマンド	説明
clear memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューおよび統計情報を消去します。
memory delayed-free-poisoner validate	delayed free-memory poisoner ツールのキュー内の要素を検証します。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況について要約を表示します。

memory delayed-free-poisoner validate

memory delayed-free-poisoner キュー内のすべての要素を検証するには、特権 EXEC モードで ***memory delayed-free-poisoner validate*** コマンドを使用します。

memory delayed free poisoner enable

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

memory delayed-free-poisoner validate コマンドを使用するには、まず **memory delayed-free-poisoner enable** コマンドを使用して delayed free-memory poisoner ツールをイネーブルする必要があります。

memory delayed-free-poisoner validate コマンドを実行すると、**memory delayed-free-poisoner** キューの各要素が検証されます。予期せぬ値が格納された要素が見つかると、クラッシュが発生し、クラッシュの原因を判断するための診断が出力されます。予期せぬ値が見つからなければ、キュー内の各要素はそのままで、ツールによって通常どおり処理されます。**memory delayed-free-poisoner validate** コマンドによって、キューに登録されているメモリがシステムのメモリ プールに戻されることはありません。

（注） delayed free-memory poisoner ツールは、定期的に、キューに登録されているすべての要素を自動的に確認します。

例

次の例では、**memory delayed-free-poisoner** キュー内に登録されているすべての要素を検証しています。

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

関連コマンド

コマンド	説明
clear memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューおよび統計情報を消去します。
memory delayed-free-poisoner enable	delayed free-memory poisoner ツールをイネーブルにします。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況について要約を表示します。

memory profile enable

メモリ使用状況のモニタ（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をピーク使用状況バッファに保管する、メモリ使用状況しきい値を指定します。このバッファの内容をあとで分析し、システムに必要なピーク メモリを決定します。

デフォルト

メモリ プロファイリングは、デフォルトでディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドのサポートが追加されました。

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*** コマンドでプロファイリングするメモリ テキスト範囲を設定しておく必要があります。

一部のメモリは、***clear memory profile*** コマンドが入力されるまで、プロファイリング システムが保持します。***show memory status*** コマンドの出力を参照してください。

（注） メモリ プロファイリングをイネーブルにすると、FWSM のパフォーマンスが一時的に低下する可能性があります。

次に、メモリ プロファイリングをイネーブルにする例を示します。

```
hostname# memory profile enable
```

関連コマンド

コマンド	説明
memory profile text	プロファイリングするメモリのテキスト範囲を設定します。
show memory profile	FWSM のメモリ使用率（プロファイル）に関する情報を表示します。

memory profile text

プロファイリングするメモリのプログラム テキスト範囲を設定するには、特権 EXEC モードで ***memory profile text*** コマンドを使用します。この設定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 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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドのサポートが追加されました。

使用上のガイドライン

テキスト範囲が小さい場合、通常は [4] の精度で命令呼び出しをトレースします。テキスト範囲が大きい場合、通常 1 回めは粗い精度で十分です。次の回で、セットの領域数を減らして範囲を絞り込みます。

memory profile text コマンドを使用してテキスト範囲を入力したあとで、***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 プロファイリングは、デフォルトでディセーブルです。

（注） メモリ プロファイリングをイネーブルにすると、FWSM のパフォーマンスが一時的に低下する可能性があります。

例

次に、精度を 4 にして、プロファイリングするメモリのテキスト範囲を設定する例を示します。

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

次に、テキスト範囲の設定およびメモリ プロファイリングのステータス（OFF）を表示する例を示します。

```
hostname# show memory profile
InUse profiling: OFF
Peak profiling: OFF
Profile:
0x004018b4-0x004169d0(00000004)
```

（注）　メモリ プロファイリングを開始するには、***memory profile enable*** コマンドを入力する必要があります。メモリ プロファイリングは、デフォルトでディセーブルです。

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が保持しているバッファを消去します。
memory profile enable	メモリ使用率（メモリ プロファイリング）のモニタリングをイネーブルにします。
show memory profile	FWSM のメモリ使用率（プロファイル）に関する情報を表示します。
show memory-caller address	FWSM に設定されたアドレス範囲を表示します。

message-length

設定された最大長および最小長を満たしていない 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。GTP マップ コンフィギュレーション 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、**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 ペイロードで使用でき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 ～ 65536 です。
min	UDP ペイロードで使用でき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 ～ 65536 です。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドで指定する長さは、GTP ヘッダーとメッセージのその他の部分の合計です。それが UDP パケットのペイロードです。

例

次に、長さが 20 ～ 300 バイトのメッセージを許可する例を示します。

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

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 検査の詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	特定の GTP マップがアプリケーション検査で使用されるようにします。
show service-policy inspect gtp	GTP 設定を表示します。

mfib forwarding

インターフェイス上で MFIB 転送を再度イネーブルにするには、インターフェイス コンフィギュレーション モードで **mfib forwarding** コマンドを使用します。インターフェイス上の MFIB 処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

mfib forwarding

no mfib forwarding

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

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

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

例

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

```
hostname(config)# interface Vlan55
hostname(config-if)# no mfib forwarding
```

関連コマンド

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

mgcp-map

MGCP 検査のパラメータを定義する、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 モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

mgcp-map コマンドは、MGCP 検査のパラメータを定義するための具体的なマップを指定する場合に使用します。このコマンドを入力すると、コンフィギュレーション モードが開始され、具体的なマップを定義するための各種コマンドを入力できます。MGCP マップの定義後、**inspect mgcp** コマンドを使用してマップをイネーブルにします。Modular Policy Framework 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 グループを指定します。
- **command-queue —** キューに格納できる 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するコール エージェント グループを指定します。
- **no —** コマンドを取り消して、パラメータをデフォルト値に設定します。

例

次に、**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ためのマップ（mgcp-policy）を指定する例を示します。

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

次に、MGCP トラフィックを指定し、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例を示します。次の例のように MGCP 検査 エンジンをイネーブルにすると、デフォルト ポート（2427）上で MGCP トラフィックと照合するクラス マップが作成されます。さらに、外部ポリシーにサービス ポリシーが適用されます。

```
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-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
```

この場合、コール エージェント 10.10.11.5 および 10.10.11.6 でゲートウェイ 10.10.10.115 を制御し、コール エージェント 10.10.11.7 および 10.10.11.8 でゲートウェイ 10.10.10.116 および 10.10.10.117 の両方を制御できるようになります。キューに格納できる 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で 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 のデバッグ情報を表示できるようにします。
show mgcp	MGCP の設定およびセッション情報を表示します。
timeout	MGCP に関連するアイドル タイムアウトを設定します。

mkdir

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

mkdir [**/noconfirm**] [**flash:**]*path*

シンタックスの説明

noconfirm	（任意）確認のプロンプトを抑制します。
flash:	（任意）内蔵フラシュ メモリを指定し、続けてコロンを指定します。
path	作成するディレクトリの名前およびパス

デフォルト

パスを指定しなかった場合、現在の作業ディレクトリでディレクトリが作成されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドのサポートが追加されました。

使用上のガイドライン

名前が同じ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

次に、[backup] という新しいディレクトリを 1 つ作成する例を示します。

```
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を指定のディレクトリに変更します。
dir	ディレクトリの内容を表示します。
rmdir	指定の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 FWSM をセキュリティ コンテキストと呼ばれる複数の仮想デバイスに分割できます。各コンテキストは、独立したデバイスと同様に動作し、それぞれに独自のセキュリティ ポリシー、インターフェイス、および管理者が与えられます。マルチコンテキストは、複数のスタンドアロン アプライアンスを使用する場合と類似しています。シングル モードの場合、FWSM はコンフィギュレーションを 1 つだけ使用し、単一デバイスとして動作します。マルチモードの場合は、複数のコンテキストを作成し、そのそれぞれに独自のコンフィギュレーションを与えることができます。使用できるコンテキストの数は、ライセンスによって決まります。

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	（任意）ユーザに確認を求めずに、モードを設定します。このオプションは、自動化されたスクリプトで便利です。
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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

マルチコンテキスト モードの場合、FWSM はセキュリティ ポリシー、インターフェイス、およびスタンドアロン デバイスで設定できるほぼすべてのオプションを指定したコンフィギュレーションを各コンテキストに組み込みます（コンテキスト コンフィギュレーションの保管場所を指定する **config-url** コマンドの項を参照）。システム管理者は、シングル モードの設定と同様、スタートアップ コンフィギュレーションとしてのシステム コンフィギュレーションで設定することによって、コンテキストを追加して管理します。システム コンフィギュレーションでは、FWSM の基本的な設定値を指定します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワークそのものの設定値は含まれません。システムがネットワーク 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）、admin コンテキストとして指定されたコンテキストの 1 つを使用します。

mode コマンドを使用してコンテキスト モードを変更すると、リブートが要求されます。

コンテキスト モード（シングルまたはマルチ）は、リブート後も有効ですが、コンフィギュレーション ファイルには保管されません。コンフィギュレーションを別のデバイスにコピーする場合は、**mode** コマンドを使用して、新しいデバイスのモードが一致するように設定します。

シングル モードからマルチモードに変更すると、FWSM によって実行コンフィギュレーションが 2 つのファイルに変換されます。システム コンフィギュレーションを形成する新しい スタートアップ コンフィギュレーションおよび admin コンテキストを形成する admin.cfg（内蔵フラシュ 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 という名前で（内蔵フラシュ メモリのルート ディレクトリ内に）保存されます。元のスタートアップ コンフィギュレーションは保存されません。FWSM は、[admin] の名前でシステム コンフィギュレーションに admin コンテキストのエントリを追加します。

マルチモードからシングル モードに変換する場合は、最初に完全なスタートアップ コンフィギュレーション（利用できる場合）を FWSM にコピーしなければならない可能性があります。マルチモードから継承したシステム コンフィギュレーションがシングル モード デバイスで全面的に機能するコンフィギュレーションとは限らないからです。

マルチコンテキスト モードですべての機能がサポートされるわけではありません。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください。

例

次に、マルチモードを設定する例を示します。

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

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

Rebooting....

Booting system, please wait...
```

次に、シングル モードを設定する例を示します。

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

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



Rebooting....

Booting system, please wait...
```

関連コマンド

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

monitor-interface

特定のインターフェイス上でヘルス 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	モニタするインターフェイスの名前を指定します。

デフォルト

論理インターフェイスのモニタリングは、デフォルトでディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

FWSM でモニタできるインターフェイスの数は 250 です。インターフェイス ポーリング間隔のつど、FWSM フェールオーバー ペア間で hello メッセージが交換されます。フェールオーバー インターフェイスのポーリング時間は、3 ～ 15 秒です。たとえば、ポーリング時間が 5 秒に設定されている場合、インターフェイスに hello メッセージが連続して 5 つ（25 秒間）着信しないと、インターフェイスでテストが開始されます。

モニタ対象フェールオーバー インターフェイスのステータスは、次のとおりです。

- Unknown — 初期ステータス。ステータスを判別できない場合も、このステータスになります。
- Normal — インターフェイスはトラフィックを受信中です。
- Testing — hello メッセージが 5 回にわたるポーリング時間中、インターフェイスに着信しませんでした。
- Link Down — インターフェイスまたは VLAN が管理上のダウン状態です。
- No Link — インターフェイスの物理リンクがダウン状態です。
- Failed — インターフェイスにトラフィックが着信していませんが、ピア インターフェイスには着信しています。

アクティブ / アクティブ フェールオーバーの場合、このコマンドが有効なのはコンテキスト内に限られます。

例

次に、[inside] というインターフェイス上でモニタリングをイネーブルにする例を示します。

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

関連コマンド

コマンド	説明
clear configure monitor-interface	実行コンフィギュレーションから **monitor-interface** コマンドを削除します。
failover interface-policy	フェールオーバーが発生する基準となる、モニタ対象インターフェイスの障害数または割合を指定します。
failover polltime	インターフェイス上の hello メッセージの間隔を指定します（アクティブ / スタンバイ フェールオーバー）。
polltime interface	インターフェイス上の hello メッセージの間隔を指定します（アクティブ / アクティブ フェールオーバー）。
show running-config monitor-interface	実行コンフィギュレーションに含まれている **monitor-interface** コマンドを表示します。

more

ファイルの内容を表示するには、特権 EXEC モードで **more** コマンドを使用します。

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

シンタックスの説明

/ascii	（任意）バイナリ モードでバイナリ ファイルおよび ASCII ファイルを表示します。
/binary	（任意）すべてのファイルをバイナリ モードで表示します。
/ebcdic	（任意）バイナリ ファイルを EBCDIC で表示します。
flash:	（任意）内蔵フラシュ メモリを指定し、続けてコロンを指定します。
ftp:	（任意）FTP サーバ上のファイルを表示します。
http:	（任意）Web サイトのファイルを表示します。
https:	（任意）セキュア Web サイトのファイルを表示します。
system:	（任意）ファイル システムを表示します。
tftp:	（任意）TFTP サーバ上のファイルを表示します。
filename	表示するファイルの名前を指定します。

デフォルト

ASCII モード

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

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の入力を要求します。

例

次に、ローカル ファイル [test.cfg] の内容を表示する例を示します。

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

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

関連コマンド

コマンド	説明
cd	指定されたディレクトリに切り替えます。
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* | *rpf_neighbor*} [***dense*** *output_if_name*] [*distance*]

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

シンタックスの説明

dense *output_if_name*	（任意）dense モード出力に対応するインターフェイス名 ***dense*** *output_if_name* キーワードと引数のペアがサポートされるのは、SMR スタブ マルチキャスト ルーティング（igmp 転送）の場合だけです。
distance	（任意）ルートの管理距離。距離の小さいルートほど、優先されます。デフォルトの値は、0 です。
in_if_name	mroute の着信インターフェイス名を指定します。
rpf_neighbor	セキュリティ アプライアンスの RPF ネイバーを指定します。
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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、マルチキャスト送信元の位置を静的に設定できます。FWSM では、特定の送信元にユニキャスト パケットを送信するときに使用するの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ことが想定されます。マルチキャスト ルーティングをサポートしないルートをバイパスする場合など、状況によって、マルチキャスト パケットにユニキャスト パケットと異なるパスを使用することがあります。

スタティック マルチキャスト ルートは、アドバタイズも再配布も行われません。

（注） このコマンドを使用すると、インターフェイス名または RPF ネイバーを指定できますが、両方を同時に指定することはできません。

show mroute コマンドを使用すると、マルチキャスト ルート テーブルの内容が表示されます。**show running-config mroute** コマンドを使用すると、実行コンフィギュレーションに指定されている mroute コマンドが表示されます。

例

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

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

関連コマンド

コマンド	説明
show running-config mroute	コンフィギュレーションの **mroute** コマンドを表示します。

mtu

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

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。有効値は 64 ～ 65,535 バイトです。
interface_name	内部または外部ネットワークのインターフェイス名

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

mtu コマンドを使用すると、接続上で送信するデータ サイズを設定できます。MTU 値よりも大きなデータは、送信前に分割されます。

FWSM は IP パス MTU 検出（RFC 1191 で定義）をサポートします。ホストはこの機能を使用することにより、パス上の各リンクの最大許容 MTU サイズの差異を動的に検出したり、調整したりできます。場合によっては、パケットがインターフェイスに設定された MTU よりも大きいにもかかわらず、[don't fragment]（DF）ビットが設定されているため、FWSM がデータグラムを転送できないことがあります。ネットワーク ソフトウェアは送信側ホストにメッセージを送信して、この問題を警告します。ホストはこの宛先へのパケットを分割して、パス上のすべてのリンクの最小パケット サイズに合わせる必要があります。

デフォルトの MTU は、イーサネット インターフェイスのブロック内で 1500 バイトです（この値は最大値でもあります）。ほとんどのアプリケーションではこの値で十分に機能しますが、ネットワーク条件に応じて、より小さな値を選択することができます。

Layer 2 Tunneling Protocol（L2TP）を使用する場合は、L2TP ヘッダー長および IPSec ヘッダー長に対応させるために、MTU サイズを 1380 に設定することを推奨します。

例

次に、インターフェイスの MTU を指定する例を示します。

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

関連コマンド

コマンド	説明
clear configure mtu	すべてのインターフェイスに設定された MTU 値を消去します。
show running-config mtu	現在の MTU ブロック サイズを表示します。

multicast-routing

FWSM 上で 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、引数またはキーワードはありません。

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

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

（注） PIM は PAT ではサポートされません。PIM プロトコルはポートを使用しないのに対して、PAT はポートを使用するプロトコルに限って機能します。

セキュリティ アプライアンスが PIM RP の場合は、RP アドレスとしてセキュリティ アプライアンスの未変換外部アドレスを使用します。

マルチキャスト ルーティング テーブルのエントリ数は、システム上の RAM 容量によって制限されます。表 20-2 に、セキュリティ アプライアンスの RAM 容量に基づいた最大エントリ数をマルチキャスト テーブル別に示します。これらの限度に達すると、新しいエントリは廃棄されます。

表 20-2　マルチキャスト テーブルのエントリ限度

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

例

次に、FWSM 上で IP マルチキャスト ルーティングをイネーブルにする例を示します。

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

関連コマンド

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