CHAPTER 23

# quit ～ router-id コマンド

## 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 |
| ユーザ EXEC | • | • | • | • | • |

**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**　***Ctrl Z*** のキー シーケンスを使用して、グローバル コンフィギュレーション（またはそれより上の）モードを終了することもできます。このキー シーケンスは、特権モードまたはユーザ EXEC モードでは無効です。

特権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、FWSM からログアウトすることになります。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

次に、**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例を示します。

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

Logoff
```

次に、**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、さらに **disable** コマンドを使用して特権 EXEC モードを終了する例を示します。

```
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 モードを終了する、または特権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

RADIUS 許可サーバによって VPN アクセスが許可された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** *password*

**no radius-common-pw**

## シンタックスの説明

| | |
|---|---|
| *password* | **aaa-server host** コマンドで指定された RADIUS サーバとのすべての許可トランザクションで共通パスワードとして使用する、最大 127 文字の英数字キーワード。大文字と小文字が区別されます。 |

## 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 |
| AAA サーバ ホスト | • | • | • | • | — |

## 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

このコマンドが有効なのは、RADIUS 許可サーバに限定されます。

RADIUS 許可サーバは、接続する各ユーザにパスワードとユーザ名を要求します。ユーザ名は FWSM が自動的に提供します。パスワードはここで入力します。RADIUS サーバの管理者は、この FWSM 経由でのサーバ アクセスを許可する各ユーザにこのパスワードが対応付けられるように、RADIUS サーバを設定する必要があります。必ず、RADIUS サーバの管理者にこの情報を提供してください。

共通のユーザ パスワードを指定しなかった場合、各ユーザのパスワードはそのユーザのユーザ名になります。たとえば、ユーザ名が [jsmith] というユーザの場合、デフォルトの RADIUS 許可は [jsmith] です。共通のユーザ パスワードとしてユーザ名を使用する場合は、セキュリティ対策として、自分のネットワーク以外では許可にこの RADIUS サーバを使用しないでください。

**（注）** パスワード フィールドは RADIUS プロトコルに必要であり、RADIUS サーバが要求しますが、ユーザがこのフィールドを認識する必要はありません。

## 例

次に、ホスト [1.2.3.4] 上の [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、再試行間隔を 7 秒、RADIUS 共通パスワードを [allauthpw] にする例を示します。

```
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
```

## 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 モードを開始し、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** | コンフィギュレーションからすべての AAA コマンド ステートメントを削除します。 |
| **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について、AAA サーバの統計情報を表示します。 |

# radius-with-expiry

FWSM が認証時に、MS-FHAPv2 を使用し、パスワードの更新についてユーザとネゴシエーションを行うようにするには、tunnel-group ipsec-attributes 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かった場合、FWSM はこのコマンドを無視します。

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。

**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

このコマンドのデフォルト設定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 |
| Tunnel-group ipsec-attributes 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

この属性を適用できるのは、IPSec リモートアクセス トンネルグループ タイプだけです。

## 例

次に、config-ipsec コンフィギュレーション モードを開始し、remotegrp というリモートアクセス トンネル グループの満了を指定して RADIUS を設定する例を示します。

```
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** | 設定されたトンネル グループをすべて消去します。 |
| **show running-config tunnel-group** | 指定された証明書マップ エントリを表示します。 |
| **tunnel-group-map default-group** | **crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリにトンネル グループを対応付けます。 |

# reactivation-mode

グループ内の障害サーバを再びアクティブにする方法（再アクティベーション 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* | （任意）グループの最終サーバが使用不能になってからすべてのサーバが再び使用可能になるまでの経過時間を指定します。 |
| ***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に限り、障害サーバを再びアクティブにします。 |
| ***timed*** | 30 秒間の停止時間を経て、障害サーバを再びアクティブにします。 |

## デフォルト

デフォルトの再アクティベーション モードは depletion です。デフォルトの deadtime 値は 10 です。deatime に指定できる値の範囲は 0 ～ 1440 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 |
| AAA サーバ グループ | • | • | • | • | — |

## 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

各サーバ グループには、そのサーバの再アクティベーション ポリシーを指定する属性があります。

***depletion*** モードでは、停止されたサーバは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、非アクティブのままです。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は、それらすべてのサーバが再びアクティブになります。この手法を使用すると、障害サーバが原因で接続遅延が生じる可能性を最小限に抑えられます。***depletion*** モードを使用する場合は、***deadtime*** パラメータも指定できます。***deadtime*** パラメータでは、グループの最終サーバが使用不能になってから、すべてのサーバが再び使用可能になるまでの経過時間（分）を指定します。このパラメータが意味を持つのは、サーバ グループをローカル フォールバック機能と組み合わせて使用する場合だけです。

***timed*** モードでは、30 秒間の停止時間を経て、障害サーバが再びアクティブになります。これは、ユーザがサーバ リストの先頭サーバをプライマリ サーバとして使用し、可能なかぎり常にオンラインにしておく場合に有用です。UDP サーバの場合、このポリシーは無効です。UDP はコネクションレス プロトコルであり、FWSM ではサーバの存在を判別できないので、UDP サーバが無条件にオンラインに戻されるからです。その結果、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、接続時間の増大または接続障害が発生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 グループは、***timed*** モードの使用が強制されます。したがって、リスト内のすべてのサーバが同等になります。

## 例

次に、[svrgrp1] という TACACS+ AAA サーバを設定し、deadtime を 15 分に設定して、depletion の再アクティベーション モードを使用する例を示します。

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

次に、[svrgrp2] という TACACS+ AAA サーバを設定し、timed の再アクティベーション モードを使用する例を示します。

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

## 関連コマンド

| | |
|---|---|
| **accounting-mode** | アカウンティング メッセージを 1 つのサーバだけに送信するか（シングル モード）、グループ内のすべてのサーバに送信するか（同時モード）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。 |
| **max-failed-attempts** | サーバ グループ内の個々のサーバが停止するまでに許容される障害回数を指定します。 |
| **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-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について、AAA サーバの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たネットワークを 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* | 指定された自律システムに対して外部になる OSPF メトリック ルートを指定します。有効値は **1** または **2** です。 |
| **internal** *type* | 指定された自律システムの内部にある OSPF メトリック ルートを指定します。 |
| match | （任意）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指定します。 |
| metric *metric_value* | （任意）0 ～ 16777214 の OSPF デフォルト メトリック値を指定します。 |
| metric-type *metric_type* | （任意）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 ルートと対応する外部リンク タイプ。次の 2 つのうちのどちらでも指定できます。1（タイプ 1 外部ルート）または 2（タイプ 2 外部ルート）です。 |
| **nssa-external** *type* | Not-So-Stubby Area（NSSA）に対して外部になるルートの OSPF メトリック タイプを指定します。有効値は **1** または **2** です。 |
| ospf *pid* | 現在の OSPF ルーティング プロセスに OSPF ルーティング プロセスを再配布する場合に使用します。*pid* では、OSPF ルーティング プロセス内部で使用される識別パラメータを指定します。有効値は 1 ～ 65535 です。 |
| route-map *map_name* | （任意）適用するルート マップの名前 |
| **static** | OSPF プロセスにスタティック ルートを再配布する場合に使用します。 |
| subnets | （任意）OSPF にルートを再配布する場合、指定されたプロトコルの再配布範囲を設定します。指定しなかった場合は、クラスフル ルートだけが再配布されます。 |
| tag *tag_value* | （任意）各外部ルートに結合する 32 ビット 10 進値。OSPF 自体はこの値を使用しません。この値は、ASBR 間で情報を伝達する場合に使用します。値を指定しない場合、BGP および EGP からのルートにはリモート Autonomous System（AS; 自律システム）の番号が使用され、他のプロトコルの場合にはゼロ（0）が使用されます。有効値は 0 ～ 4294967295 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 |
| 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 |
|---|---|
| 1.1(1) | このコマンドが追加されました。 |

## 例

次に、現在の OSPF プロセスにスタティック ルートを再配布する例を示します。

```
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 モードを開始します。 |
| **show running-config router** | グローバル ルータ コンフィギュレーションに指定されている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* | （任意）（24 時間制クロックを使用して）指定した時刻にソフトウェアがリロードされるように、スケジュールを設定します。月日を指定しなかった場合、現在日の指定時刻（指定時刻が現在の時刻以後の場合）または翌日の指定時刻（指定時刻が現在の時刻以前の場合）に、リロードが行われます。深夜 0 時にリロードを行うには、00:00 を指定します。リロードは 24 時間以内に行う必要があります。 |
| ***cancel*** | （任意）予定されているリロードを取り消します。 |
| *day* | （任意）1 ～ 31 で表した日付 |
| ***in*** [*hh*:]*mm*] | （任意）hh 時間後、または hh 時間 mm 分後にソフトウェアがリロードされるようにスケジュールを設定します。リロードは 24 時間以内に行う必要があります。 |
| ***max-hold-time*** [*hh*:]*mm* | （任意）シャットダウンまたはリブートを実行する前に、FWSM が他のサブシステムに通知するまで待機する、最大保留時間を指定します。この時間が経過すると、クイック（強制）シャットダウン / リブートが行われます。 |
| *month* | （任意）月名を指定します。月名を表す一意の文字列になるだけの文字数を入力します。たとえば、[Ju] の場合は June にも July にもなりえるので、一意ではありません。しかし、[Jul] は、この 3 文字から始まる月はほかにないので一意です。 |
| **noconfirm** | （任意）FWSM がユーザの確認を得なくてもリロードできるようにします。 |
| ***quick*** | （任意）クイック リロードを強制的に実行します。すべてのサブシステムへの通知またはすべてのサブシステムの適切なシャットダウンは行われません。 |
| ***reason*** *text* | （任意）1 ～ 255 文字で、リロードの理由を指定します。理由を記述したテキストは、オープンしているすべての IPSec VPN クライアント、端末、コンソール、Telnet、SSH、および ASDM 接続 / セッションに送信されます。<br><br>**（注）** isakmp など、アプリケーションによっては、IPSec VPN クライアントに理由を示したテキストを送信するための追加設定が必要になります。詳細については、ソフトウェア コンフィギュレーション マニュアルの該当するセクションを参照してください。 |
| ***save-config*** | （任意）シャットダウンの前に、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かった場合、保存されていない設定変更はリロード後にすべて失われます。 |

## 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) | このコマンドが変更され、次の新しい引数およびキーワードが追加されました。*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、FWSM がリブートし、フラッシュからコンフィギュレーションがリロードされます。

デフォルトでは、**reload** コマンドは対話型です。FWSM は最初に、コンフィギュレーションが変更されていて未保存かどうかを調べます。変更されていながら未保存の場合、FWSM はコンフィギュレーションの保存を要求します。マルチコンテキスト モードの場合、FWSM は未保存の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*** パラメータを指定した場合は、プロンプトを表示しないでコンフィギュレーションが保存されます。FWSM は次に、システムをリロードすることについて確認を求めます。***y*** で応答した場合または ***Enter*** キーを押した場合に限り、リロードが実行されます。確認後、FWSM は遅延パラメータ（キーワード ***in*** または ***at***）が指定されているかどうかに応じて、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。

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」ともいう）モードで動作します。リブートの実行直前に、登録されているすべてのサブシステムに通知が出されるので、各サブシステムはリブート前に正しくシャットダウンできます。このようなシャットダウンが行われるまで待たない場合は、***max-hold-time*** パラメータを使用して、最大待機時間を指定します。または、***quick*** パラメータを使用すると、関連サブシステムに通知したり、適切なシャットダウンが完了するまで待機したりすることなく、リロード プロセスが突然、強制的に開始されます。

***noconfirm*** パラメータを指定すると、**reload** コマンドを非対話式で動作させることができます。この場合、***save-config*** パラメータが指定されていないかぎり、FWSM は未保存コンフィギュレーションの有無を調べません。FWSM はまた、システムのリブート前に、ユーザに確認を求めません。遅延パラメータを指定しなかった場合、リロード プロセスがただちに開始またはスケジューリングされますが、***max-hold-time*** または ***quick*** パラメータで動作またはリロード プロセスを制御できます。

予定されたリロードを取り消すには、**reload cancel** を使用します。すでに開始されているリロードを取り消すことはできません。

**（注）** フラッシュ パーティションに書き込まれなかった設定変更は、リロード後に失われます。リブート前に、**write memory** コマンドを入力して、現在の設定をフラッシュ パーティションに保存してください。

**例**

次に、リブートしてコンフィギュレーションをリロードする例を示します。

```
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** | FWSM 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 session-threshold-exceeded** 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。このコマンドでは、FWSM がトラップを送信する場合に、アクティブでなければならないリモート アクセス セッション数を指定します。

**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* | FWSM がサポートするセッション限度以下の整数を指定します。 |

**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。 |

**例**

次に、しきい値を 1500 に設定する例を示します。

```
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** | しきい値トラップをイネーブルにします。 |

# rename

ファイルまたはディレクトリを元の名前から新しい名前に変更するには、特権 EXEC モードで **rename** コマンドを使用します。

**rename** ***[/noconfirm]*** **[flash:]** ***source-path*** **[flash:]** ***destination-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。 |
| *destination-path* | 変更後のファイルのパスを指定します。 |
| **flash:** | （任意）内蔵フラッシュ メモリを指定し、続けてコロンを指定します。 |
| *source-path* | 元のファイルのパスを指定します。 |

## 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 |
| 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

**rename flash: flash:** コマンドを使用すると、元のファイル名と変更後のファイル名を入力するように求められます。

複数のファイル システムにまたがって、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。

例を示します。

```
hostname# rename flash: disk1:
Source filename []? new-config
Destination filename []? old-config
%Cannot rename between filesystems
```

## 例

次に、[test] から [test1] にファイル名を変更する例を示します。

```
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 システムの情報を表示します。 |

# 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、引数またはキーワードはありません。

## デフォルト

ディセーブル

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## 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

デフォルトでは、FWSM はステートフル フェールオーバーがイネーブルの場合、HTTP セッション情報の複製を行いません。HTTP セッションは通常、有効期間が短いので、また、HTTP クライアントは通常、接続に失敗しても再試行するので、HTTP セッションの複製を行わない方がパフォーマンスが向上します。データまたは接続の重大な損失が生じることもありません。**replication http** コマンドを使用すると、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 レプリケーションが可能になりますが、システム パフォーマンスが低下する可能性があります。

このコマンドを使用できるのは、アクティブ / アクティブ フェールオーバーの場合だけです。アクティブ / スタンバイ フェールオーバーの場合は、アクティブ / アクティブ フェールオーバー構成のフェールオーバー グループを除いて、**failover replication http** コマンドと同じ機能が得られます。

## 例

次に、フェールオーバー グループの設定例を示します。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# replication http
hostname(config-fover-group)# exit
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **failover group** | アクティブ / アクティブ フェールオーバーを行うフェールオーバー グループを定義します。 |
| **failover replication http** | HTTP 接続の複製が行われるように、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。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。

**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** | ファイルに付加するコマンドを禁止します。 |
| **cdup** | 現在の作業ディレクトリの親ディレクトリを変更す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り出すクライアント 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** | 変更前のファイル名を指定するコマンドを禁止します。 |
| **rnto** | 変更後のファイル名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、リモート管理に使用します。 |
| **stou** | 一意のファイル名を使用してファイルを保存するコマンドを禁止します。 |

## 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 |
| 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

このコマンドは、厳密な FTP 検査の使用中に、FWSM を通過する FTP 要求内で許可されているコマンドを制御します。

## 例

次に、**stor**、**stou**、または **appe** コマンドが含まれている FTP 要求を FWSM にドロップさせる例を示します。

```
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# request-command deny put stou appe
```

**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。 |
| **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。 |
| **mask-syst-reply** | クライアントからの FTP サーバ応答を非表示にします。 |
| **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-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。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い場合に実行す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にもかかわらず、コンフィギュレーション リストに存在しない要求方式がトラフィックに含まれている場合に、FWSM 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* | FWSM を通過させる拡張メソッドの 1 つを指定します。 |
| **log** | （任意）Syslog を生成します。 |
| **reset** | クライアントおよびサーバに TCP リセット メッセージを送信します。 |
| **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* | FWSM を通過させる RFC メソッドの 1 つを指定します（表 23-1 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です。このコマンドをイネーブルしながら、サポート対象の要求メソッドを指定しなかった場合、ログを収集しないで接続を許可することがデフォルトのアクションになります。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、別のデフォルト アクションを指定します。

**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 |
| 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(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

**request-method** コマンドをイネーブルに設定した場合、FWSM はサポート対象で、なおかつ設定された要求メソッドのそれぞれに対応する HTTP 接続に、指定されたアクションを適用します。

FWSM は、設定済みリストの要求メソッドと一致*しない*すべてのトラフィックに、**default** アクションを適用します。**default** アクションは、ログを収集しないで接続を **allow**（許可）します。事前設定済みのデフォルト アクションを使用し、なおかつ 1 つ以上の要求メソッドを選択してアクション **drop** および **log** を指定した場合、FWSM は設定された要求メソッドが含まれている接続をドロップし、各接続を記録し、その他のサポート対象要求メソッドについては、あらゆる接続を許可します。

より限定的な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**（イベントを記録する場合）に変更します。その後、**allow** アクションを指定して、許可するメソッドを設定します。

**request-method** コマンドは、適用する設定ごとに 1 回ずつ入力します。**request-method** コマンドのインスタンスを 1 つ使用して、デフォルトのアクションを変更したり、設定済みメソッド リストに要求メソッドを 1 つ追加したりします。

このコマンドの **no** 形式を使用して、設定済みメソッドのリストから要求メソッドを削除すると、コマンドラインで要求メソッドのキーワードより後ろに指定した文字はすべて無視されます。

表 23-1 に、設定済みメソッド リストに追加できる、RFC 2616 で定義されているメソッドを示します。

**表 23-1　RFC 2616 のメソッド**

| Method | 説明 |
|---|---|
| connect | トンネル（SSL トンネリングなど）に動的に切り替え可能なプロキシと組み合わせて使用します。 |
| delete | 起点サーバが Request-URI で指定されたリソースを削除することを要求します。 |
| get | Request-URI で指定された情報またはオブジェクトを取得します。 |
| head | サーバが応答でメッセージ本文を返さないことを除き、get と同じです。 |
| options | Request-URI で指定されたサーバ上で使用可能な通信オプションに関する情報を求める要求を表します。 |
| post | Request-Line の Request-URI で指定されたリソースに新しく従属するものとして、要求に含まれているオブジェクトを起点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された Request-URI 下に格納することを要求します。 |
| trace | 要求メッセージのリモート アプリケーション レイヤ ループバックを起動します。 |

## 例

次に、事前設定されたデフォルトを使用して、許可ポリシーを指定する例を示します。この場合、明示的に禁止されていない、すべてのサポート対象要求メソッドが許可されます。

```
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
```

この例では、要求メソッド **options** および **post** だけがドロップされて、イベントが記録されます。

次に、制限型ポリシーを指定する例を示します。明示的に許可されていないすべての要求メソッドについて、接続がリセット（**reset**）され、イベントが記録（**log**）されるようにデフォルト アクションを変更します。

```
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
```

この場合、要求メソッド **get** および **put** は許可されます。それ以外のメソッドを使用するトラフィックが検出された場合、FWSM は接続をリセットして 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。 |

# request-queue

応答待ちでキューに格納する 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。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。この値をデフォルトの 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格納する GTP 要求の最大数。値の範囲は 1 ～ 4294967295 です。 |

## デフォルト

*max_requests* 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 |
| 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

**gtp request-queue** コマンドでは、応答待ちとしてキューに格納できる GTP 要求の最大数を指定します。限度に達しているときに新しい要求が着信すると、キュー格納期間が最も長い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はみなされず、応答待ちの要求キューには格納されません。

## 例

次に、要求キューの最大サイズとして 300 バイトを指定する例を示します。

```
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。 |

# resource acl-partition

マルチコンテキスト モードにおけるメモリ パーティションの数を最大値の 12 から引き下げるには、グローバル コンフィギュレーション モードで **resource acl-partition** コマンドを使用します。パーティション数を 12 に戻すには、このコマンドの **no** 形式を使用します。マルチコンテキスト モードでは、FWSM はルール コンフィギュレーションに割り当てるメモリを分割し、パーティションに各コンテキストを割り当てます。使用するコンテキスト数に合わせて、パーティション数を減らした方がよい場合があります。

**resource acl-partition** *number*

**no resource acl-partition** *number*

## シンタックスの説明

| | |
|---|---|
| *number* | 1 ～ 12 でパーティション数を指定します。 |

（注）　パーティションにコンテキストを割り当てる場合、パーティション番号は 0 から始まります。したがって、パーティション数が 12 の場合、パーティション番号は 0 ～ 11 になります。

## デフォルト

FWSM はデフォルトで 12 のメモリ パーティションを使用します。

## 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 | 該当なし | 該当なし | — | — | • |

## コマンド履歴

| リリース | 変更 |
|---|---|
| 2.3(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

マルチコンテキスト モードでは、FWSM はルール コンフィギュレーションに割り当てるメモリを分割し、パーティションに各コンテキストを割り当てます。デフォルトで、コンテキストは 12 のパーティションの 1 つに割り当てられます。1 つのパーティションで、ACE、AAA ルールなどを含めて、最大 12,130 のルールを提供します。FWSM は、起動時にロードされた順序で、パーティションにコンテキストを割り当てます。たとえば、12 のコンテキストがある場合、各コンテキストはそれぞれ専用のパーティションに割り当てられ、1 つのコンテキストで 12,130 のルールを使用できます。コンテキストをもう 1 つ追加すると、コンテキスト番号 1 と新しいコンテキスト番号 13 の両方がパーティション 1 に割り当てられ、12,130 のルールを分け合って使用できます。他の 11 のコンテキストは引き続き、それぞれ 12,130 のルールを使用できます。コンテキストを削除しても、パーティションのメンバーシップは変わらないので、リブートしないかぎり、分配が不平等になることがあります。リブートすると、コンテキストが均等に分配されます。

（注）　ルールは早いもの順に使用されるので、あるコンテキストが別のコンテキストより多くのルールを使用する場合があります。

**allocate-acl-partition** コマンドを使用すると、パーティションにコンテキストを手動で割り当てることができます。

パーティション数を変更するには、FWSM のリロードが必要です。フェールオーバーを使用している場合は、両方の装置でメモリ パーティションを一致させなければならないので、他方のフェールオーバー装置もリブートする必要があります。両方の装置が同時に停止すると、トラフィック損失が生じる可能性があります。

## 例

次に、メモリを 8 つの部分に分割する例を示します。

```
hostname(config)# resource acl-partition 8

This configuration command leads to repartitioning of ACL memory. It will not take
effect unless you save the configuration to startup configuration and reboot. Would
you like to save the configuration and reboot now? [n]
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **allocate-acl-partition** | 特定のメモリ パーティションにコンテキストを割り当てます。 |
| **context** | セキュリティ コンテキストを設定します。 |
| **show resource acl-partition** | 各メモリ パーティションに割り当てられているコンテキストおよび使用されているルール数を表示します。 |

# retry-interval

**aaa-server host** コマンドで事前に指定された特定の AAA サーバに対する再試行の時間間隔を設定するには、AAA サーバ ホスト モードで **retry-interval** コマンドを使用します。再試行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* | 要求の再試行間隔（1 ～ 10 秒）を指定します。これは、FWSM が接続要求を再試行するまでに待機する時間です。 |

## デフォルト

デフォルトの再試行間隔は 10 秒です。

## 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 ホスト | • | • | • | • | — |

## 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

**retry-interval** コマンドは、次の接続試行までに FWSM が待機する秒数を指定またはリセットする場合に使用します。FWSM が AAA サーバとの接続を試行する期間を指定するには、**timeout** コマンドを使用します。

## 例

次に、コンテキストの retry-interval コマンドを表示する例を示します。

```
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 7
hostname(config-aaa-server-host)# retry-interval 9
```

## 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 モードを開始し、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** | コンフィギュレーションから AAA コマンド ステートメント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について、AAA サーバの統計情報を表示します。 |
| **timeout** | FWSM が AAA サーバとの接続を試行する時間の長さを指定します。 |

# re-xauth

IKE 鍵の再生成時にユーザの再認証を要求するには、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** コマンドを実行します。IKE 鍵再生成時のユーザ再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。

実行コンフィギュレーションから re-xauth 属性を削除するには、このコマンドの **no** 形式を使用します。その結果、別のグループ ポリシーから IKE 鍵再生成時の再認証に関する値を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 鍵再生成時の再認証をディセーブルにします。 |
| **enable** | IKE 鍵再生成時の再認証をイネーブルにします。 |

## デフォルト

IKE 鍵再生成時の再認証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 |
| グループ ポリシー | • | — | • | — | — |

## 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

IKE 鍵再生成時の再認証をイネーブルにすると、FWSM は最初の フェーズ 1 IKE ネゴシエーション時に、ユーザ名とパスワードの入力をユーザに要求します。さらに、IKE 鍵再生成のつど、ユーザ認証を要求します。再認証によってセキュリティが強化されます。

設定した鍵再生成間隔が短すぎると、認証要求が繰り返されるので、ユーザにとって煩わしい場合があります。その場合は、再認証をディセーブルにします。設定されている鍵再生成間隔を調べるには、モニタリング モードで **show crypto ipsec sa** コマンドを実行します。秒数で示したセキュリティ アソシエーションの有効期間およびデータ容量（KB）で示した有効期間が表示されます。

**（注）** 接続の反対側にユーザがいなかった場合、再認証は失敗します。

## 例

次に、FirstGroup というグループ ポリシーに対して鍵再生成時の再認証をイネーブルにする例を示します。

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

# rip

RIP の設定をイネーブルにしたり値を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。FWSM 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** | （任意）RIP バージョン 2 の認証をイネーブルにします。 |
| **default** | インターフェイスのデフォルト 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* | 鍵の ID 値。有効値は 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待ち受け、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が、ルーティング アップデートはブロードキャストしません。 |
| ***text*** | RIP メッセージの認証にクリア テキストを使用します（非推奨）。 |
| **version** | （任意）RIP バージョンを指定します。有効値は **1** および **2** です。 |

## デフォルト

RIP はディセーブルです。

バージョンを指定しなかった場合、デフォルトで RIP バージョン 1 がイネーブルになります。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 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

**rip** コマンドを使用すると、インターフェイス上で RIP ルーティング アップデートを送受信できるようになります。RIP アップデートの送信と受信は別々に設定します。送信のみ、受信のみ、送信と受信の両方を各インターフェイス上で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 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に **rip** コマンドが 2 つ必要です。一方では ***default*** キーワードを指定して、RIP ルーティング アップデートの送信をイネーブルにします。もう一方では、***passive*** キーワードを指定して、RIP アップデートを受信し、これらのアップデート情報を使用してルーティング テーブルに入力できるようにします。

（注）　FWSM はインターフェイス間で RIP アップデートを受け渡しできません。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにして、MD5 ベースの暗号化を使用して RIP アップデートを認証できます。ネイバー 認証をイネーブルにする場合は、*key* および *key_id* 引数が RIP バージョン 2 アップデートを提供するネイバー装置で使用されているものと一致してい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 バージョン 2 を設定すると、所定のインターフェイス上でマルチキャスト アドレス 224.0.0.9 が登録され、マルチキャスト RIP バージョン 2 アップデートを受信できるようになります。パッシブ モードで RIP バージョン 2 を設定した場合、FWSM は宛先 IP が 224.0.0.9 の RIP バージョン 2 アップデートを受け付けます。デフォルト モードで RIP バージョン 2 を設定した場合、FWSM 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。インターフェイスに対応する RIP バージョン 2 コマンドを削除すると、インターフェイス カードからマルチキャスト アドレスの登録が解除されます。

（注）　マルチキャストをサポートするのは、Intel 10/100 およびギガビット インターフェイスだけです。

トランスペアレント モードの場合、RIP はサポートされません。FWSM はデフォルトで、すべての RIP ブロードキャストおよびマルチキャスト パケットを拒否します。トランスペアレント モードで動作している FWSM を RIP メッセージが通過できるようにするには、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、RIP バージョン 2 トラフィックがセキュリティ アプライアンスを通過できるようにするには、`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 バージョン 1 の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。アクセス リスト エントリを該当するインターフェイスに適用するには、**access-group** コマンドを使用します。

## 例

次に、バージョン 1 およびバージョン 2 のコマンドを組み合わせて、**rip** コマンドを入力したあとに **show running-config rip** コマンドで情報を表示する例を示します。**rip** コマンドを使用すると、次の操作を行うことができます。

- 外部インターフェイス上で MD5 認証を使用してバージョン 2 パッシブおよびデフォルト RIP をイネーブルにし、FWSM および他の RIP ピア（ルータなど）で使用する鍵を暗号化します。
- FWSM の内部インターフェイス上でバージョン 1 パッシブ RIP の待ち受けをイネーブルにします。
- FWSM の Demilitarized Zone（DMZ; 非武装地帯）インターフェイス上でバージョン 2 パッシブ RIP の待ち受けをイネーブルにします。

```
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
```

次に、バージョン 2 の機能を使用して、暗号鍵をテキスト形式で渡す例を示します。

```
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 RIP コマンドをすべて消去します。 |
| **debug rip** | RIP の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**] [**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）着脱不能な内蔵フラッシュを指定し、続けてコロンを指定します。 |
| *path* | （任意）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**

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**

ディレクトリが空でなかった場合、***rmdir*** コマンドは失敗します。

**例**

次に、[test] という既存のディレクトリを削除する例を示します。

```
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 システムの情報を表示します。 |

# route

指定され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。指定され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*]

**no route** *interface_name ip_address netmask gateway_ip* [*metric*]

## 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（このルートのネクストホップ アドレス）を指定します。<br><br>**（注）** トランスペアレント モードの場合、*gateway_ip* 引数は省略可能です。 |
| *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 |
| *ip_address* | 内部または外部ネットワークの IP アドレス |
| *metric* | （任意）このルートの管理距離。有効値は 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。 |

## デフォルト

*metric* はデフォルトで 1 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

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* および *netmask* を **0.0.0.0** に設定するか、または短縮形 **0** を使用します。**route** コマンドを使用して入力され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。

任意のインターフェイスでルータの外部に接続された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、FWSM は 192.168.42.0 ネットワーク宛のすべてのパケットを、このスタティック **route** コマンドを使用して 192.168.1.5 ルータ経由で送信します。

```
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、FWSM によってルート テーブルに CONNECT ルートが作成されます。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されません。

**route** コマンドで FWSM のいずれかのインターフェイスの IP アドレスをゲートウェイ IP アドレスとして使用した場合、FWSM はゲートウェイ IP アドレスに対して ARP を実行する代わりに、パケットの宛先 IP アドレスに対して ARP を実行します。

## 例

次に、外部インターフェイスに対してデフォルト **route** コマンドを 1 つ指定する例を示します。

```
hostname(config)# route outside 0 0 209.165.201.1 1
```

次に、以下のスタティック **route** コマンドを追加して、ネットワークへのアクセスを許可する例を示します。

```
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学習し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

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** | （任意）ルート マップの一致条件が満たされている場合に、ルートを再配布しないように指定します。 |
| *map_tag* | ルート マップ タグのテキスト。タグの最大長は 57 文字です。 |
| **permit** | （任意）このルート マップの一致条件が満たされている場合に、set アクションの制御に従ってルートを再配布するように指定します。 |
| *seq_num* | （任意）ルート マップのシーケンス番号。有効値は 0 ～ 65535 です。同じ名前ですでに設定されているルート マップ リストにおいて、新しいルート マップに与える位置を指定します。 |

## デフォルト

デフォルトの設定は次のとおりです。

- **permit**
- *seq_num* を指定しなかった場合、最初のルート マップには *seq_num* の値として 10 が割り当てられます。

## 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 |
| 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

**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 コマンドと、**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** コマンドで指定した条件が満たされている場合に実行される再配布アクション）を指定します。**no route-map** コマンドは、ルート マップを削除します。

**match 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番で入力できます。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、指定された一致条件が削除されます。

ルーティング プロセス間でのルートの再配布方法を細かく制御する場合は、ルート マップを使用します。宛先ルーティング プロトコルを指定するには、**router ospf** グローバル コンフィギュレーション コマンドを使用します。送信元ルーティング プロトコルを指定するには、**redistribute** ルータ コンフィギュレーション コマンドを使用します。

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** コマンドに関連する 1 つまたは複数の match 節と一致しないルートは、無視されます。無視されたルートは発信ルート マップにアドバタイズされず、着信ルート マップで受け付けられません。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。

*seq_number* 引数は次のとおりです。

1. 指定したタグを持つエントリを定義しなかった場合、*seq_number* 引数が 10 に設定されて、エントリが 1 つ作成されます。
2. 指定したタグを持つエントリを 1 つだけ定義した場合、このエントリは後続の **route-map** コマンドのデフォルト エントリになります。このエントリの *seq_number* 引数は変更されません。
3. 指定したタグを持つエントリを複数定義した場合、*seq_number* 引数が必要であることを示すエラー メッセージが表示されます。

（*seq-num* 引数を指定しないで）**no route-map** *map-tag* コマンドを指定すると、ルート マップ全体（*map-tag* テキストが同じすべての **route-map** エントリ）が削除されます。

**permit** キーワードが指定されていて、一致条件に適合しない場合、同じ *map_tag* タグを持つ次のルート マップがテストされます。ルートが、同じ名前のすべてのルート マップの一致条件に適合しない場合、そのルートは再配布されません。

## 例

次に、OSPF ルーティングで使用するルート マップを設定する例を示します。

```
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** | 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削除します。 |
| **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。 |
| **router ospf** | OSPF ルーティング プロセスを開始して設定します。 |
| **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。 |
| **show running-config route-map** | ルート マップの設定情報を表示します。 |

# 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* | 内部で使用される OSPF ルーティング プロセスの識別パラメータ。有効値は 1 ～ 65535 です。*pid* を他のルータ上の OSPF プロセス ID と一致させ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

**router ospf** コマンドは、FWSM で稼働する 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)# のようになり、ルータ コンフィギュレーション モードが開始されたことを示します。

**no router ospf** コマンドを使用する場合は、必要な情報以外、オプションの引数を指定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 プロセスを終了させます。*pid* は FWSM にローカルに割り当てます。OSPF ルーティング プロセスごとに一意の値を割り当てる必要があります。

OSPF ルーティング プロセスを設定する場合は、**router ospf** コマンドと次の OSPF 固有のコマンドを組み合わせて使用します。

- **area —** 正規の OSPF エリアを設定します。
- **compatible rfc1583 —** RFC 1583 に基づいてサマリー ルート コストを計算するための方法を復元します。
- **default-information originate —** OSPF ルーティング ドメインに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 ルートの管理距離を定義します。
- **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）をルータが受信するときに、Syslog メッセージの送信を抑制します。

- **log-adj-changes —** OSPF ネイバーが起動または停止するときに、ルータが Syslog メッセージを送信するように設定します。
- **neighbor —** ネイバー ルータを指定します。VPN トンネルを介して隣接関係を確立できるようにする場合に使用します。
- **network —** OSPF が稼働するインターフェイスおよびこ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、ルーティング ドメイン間でのルート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 グループ同期タイマー（LSA グループの更新間隔すなわち最大エージング）
- **timers spf —** SPF 計算の変更を受信するまでの遅延

FWSM 上で RIP が設定されている場合は、OSPF を設定できません。

## 例

次に、5 という番号が与えられた OSPF ルーティング プロセスに対してコンフィギュレーション モードを開始する例を示します。

```
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 コマンドを削除します。 |
| **show running-config router ospf** | 実行コンフィギュレーションの OSPF ルータ コマンドを表示します。 |

# 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。OSPF をリセットして直前のルータ ID の動作を使用するには、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

指定しなかった場合、FWSM 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 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 |
| ルータ 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

FWSM 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に格納されて送信されます。この状況を避けるには、**router-id** コマンドを使用して、ルータ ID に対応するグローバル アドレスを指定します。

## 例

次に、ルータ ID を 192.168.1.1 に設定する例を示します。

```
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 モードを開始します。 |
| **show ospf** | OSPF ルーティング プロセスに関する一般的な情報を表示します。 |