CHAPTER 22

pager ～ pwd コマンド

pager

Telnet セッションで [---more---] プロンプトが表示されるまでの、デフォルトのページ行数を設定するには、グローバル コンフィギュレーション モードで **pager** コマンドを使用します。

pager [lines] *lines*

シンタックスの説明

[**lines**] *lines*	[---more---] プロンプトが表示されるまでの 1 ページの行数を設定します。デフォルトは 24 行です。0 を指定するとページ制限はなくなります。指定できる範囲は 0 ～ 2147483647 行です。**lines** キーワードは省略できます。指定しても、しなくても、コマンドは同じです。

デフォルト

デフォルトは 24 行です。

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)	このコマンドが特権 EXEC モード コマンドからグローバル コンフィギュレーション モード コマンドに変更されました。**terminal pager** コマンドが特権 EXEC モード コマンドとして追加されました。

使用上のガイドライン

このコマンドを使用すると、Telnet セッションのデフォルトのページ行数設定が変更されます。現在のセッションに限定して、設定を一時的に変更する場合は、**terminal pager** コマンドを使用します。

管理コンテキスト、またはシステム実行スペースに対するセッションに Telnet 接続している場合に、別のコンテキストに切り替えると、所定のコンテキストにおける **pager** コマンドの設定に関係なく、ページャの行設定はユーザのセッションに従います。現在のページャ設定を変更するには、新しい設定値を指定して **terminal pager** コマンドを入力するか、現在のコンテキストで **pager** コマンドを入力します。**pager** コマンドを使用すると、コンテキストのコンフィギュレーションに新しいページャ設定が保存されるだけでなく、現在の Telnet セッションにも新しい設定が適用されます。

例

次に、表示行数を 20 に変更する例を示します。

```
hostname(config)# pager 20
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定を消去します。
show running-config terminal	現在の端末設定を表示します。
terminal	Telnet セッションでシステム ログ メッセージを表示できるようにします。
terminal pager	[---more---] プロンプトが表示されるまでに、Telnet セッションで表示される行数を設定します。このコマンドはコンフィギュレーションに保存されません。
terminal width	グローバル コンフィギュレーション モードで端末表示幅を設定します。

passwd

ログイン パスワードを設定するには、グローバル コンフィギュレーション モードで **passwd** コマンドを使用します。パスワードをデフォルトの [cisco] に戻すには、このコマンドの **no** 形式を使用します。Telnet または SSH を使用して、デフォルト ユーザとして CLI にアクセスする場合、ログイン パスワードが要求されます。ログイン パスワードを入力すると、ユーザ EXEC モードが開始されます。

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

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

シンタックスの説明

encrypted	（任意）パスワードが暗号形式になっていることを指定します。パスワードは暗号形式でコンフィギュレーションに保存されるので、入力後は元のパスワードを表示できません。別の FWSM にパスワードをコピーしなければならないが、元のパスワードがわからないという場合は、暗号化されたパスワードとこのキーワードを指定して **passwd** コマンドを入力します。通常、**show running-config passwd** コマンドを入力したときには、このキーワードだけが表示されます。
passwd* | *password	どちらのコマンドも入力できます。表記が異なるだけで内容は同じです。
password	最大 80 文字の大文字と小文字が区別される文字列として、パスワードを設定します。パスワードにスペースを含めることはできません。

デフォルト

デフォルトのパスワードは、[cisco] 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

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

例

次に、パスワードを Pa$$s0rd に設定する例を示します。

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

次に、別の FWSM からコピーした暗号パスワードにパスワードを設定する例を示します。

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

関連コマンド

コマンド	説明
clear configure passwd	ログイン パスワードを消去します。
enable	特権 EXEC モードを開始します。
enable password	イネーブル パスワードを設定します。
show curpriv	現在ログインしているユーザ名およびユーザ特権レベルを表示します。
show running-config passwd	暗号形式でログイン パスワードを表示します。

password (crypto ca trustpoint)

登録時に CA に登録する チャンレンジ フレーズを指定するには、crypto ca トラストポイント コンフィギュレーション モードで **password** コマンドを使用します。CA は通常、このフレーズを使用してその後の取り消し要求を認証します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

password *string*

no password

シンタックスの説明

string	文字列としてパスワード名を指定します。先頭文字を数字にすることはできません。文字列には、任意の英数字およびスペースを 80 文字まで使用できます。数字と何かの間にスペースを含めた形式でパスワードを指定することはできません。数字の後ろにスペースを指定すると、問題が発生します。たとえば、hello 21 は有効なパスワードですが、21 hello は無効です。パスワード検査では、大文字と小文字が区別されます。たとえば、パスワード Secret とパスワード secret は異なります。

デフォルト

パスワードを設定しないのがデフォルトの設定です。

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
crypto ca トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
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、認証の取り消しパスワードを指定してから、実際の認証登録を開始できます。指定したパスワードは、更新したコンフィギュレーションが FWSM によって NVRAM に書き込まれるときに暗号化されます。

このコマンドをイネーブルにした場合、認証登録時にパスワードが要求されなくなります。

例

次に、トラストポイント central の crypto ca トラストポイント コンフィギュレーション モードを開始し、トラストポイント central の登録要求に CA に登録したチャレンジ フレーズを含める例を示します。

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

関連コマンド

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

password-storage

ユーザがクライアント システム上でログイン パスワードを保存できるようにするには、グループ ポリシー コンフィギュレーション モードまたは username コンフィギュレーション モードで、**password-storage enable** コマンドを使用します。パスワードの保存を禁止するには、**password-storage 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 password-storage 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 password-storage の値を継承できるようになります。

password-storage {enable | disable}

no password-storage

シンタックスの説明

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

デフォルト

パスワードの保存はディセーブルです。

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	•	—	•	—	—
ユーザ名	•	—	•	—	—

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

パスワードの保存は、安全な場所に配置されていることが確実なシステムに限定してイネーブルにします。

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

例

次に、FirstGroup というグループ ポリシーに対してパスワードの保存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)# password-storage enable
```

peer-id-validate

ピアの証明書を使用してピアの ID を検証するかどうかを指定するには、tunnel-group ipsec-attributes モードで **peer-id-validate** コマンドを使用します。デフォルト値に戻すには、このコマンドの ***no*** 形式を使用します。

peer-id-validate *option*

no peer-id-validate

シンタックスの説明

option	次のいずれかのオプションを指定します。 • ***req***：必須 • ***cert***：証明書でサポートされる場合 • ***nocheck***：チェックしない

デフォルト

このコマンドのデフォルト設定は ***req*** 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

すべてのトンネルグループ タイプにこの属性を適用できます。

例

次に、config-ipsec コンフィギュレーション モードを開始し、209.165.200.255 という IPSec LAN-to-LAN トンネル グループに、ピアの証明書の ID を使用したピア検証を要求する例を示します。

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

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されたトンネル グループをすべて消去します。
show running-config tunnel-group	指定したトンネル グループまたはすべてのトンネル グループの設定を表示します。
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。

perfmon

FWSM が定期的にパフォーマンス情報を取得できるようにするには、特権 EXEC モードで **perfmon verbose** コマンドを使用します。パフォーマンス情報の出力を禁止するには、**perfmon quiet** コマンドを使用します。取得したパフォーマンス情報を表示するには、**show console-output** コマンドを使用します。

perfmon {**verbose** | **quiet**}

シンタックスの説明

verbose	パフォーマンス情報を取得します。
quiet	パフォーマンス モニタをディセーブルにします。

デフォルト

デフォルトのインターバルは 120 秒です。間隔の設定については、**perfmon interval** コマンドの項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
特権 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

パフォーマンス モニタをイネーブルにするには、**perfmon verbose** コマンドを入力します。ディセーブルにするには、**perfmon quiet** コマンドを入力します。**perfmon** コマンドの出力は Telnet セッションまたは SSH セッションのターミナル ウィンドウに表示され、当該セッションが終了した後にコンソールに転送されます。終了したセッションを再起動すると、コマンド出力は新しいセッション ウィンドウに表示されます。

例

次に、30 秒おきにパフォーマンス モニタ統計情報を取得する例を示します。

```
hostname# perfmon interval 30
hostname# perfmon verbose
hostname# show console-output
Context: my_context
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
TCP Intercept        0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
```

関連コマンド

コマンド	説明
perfmon settings	パフォーマンス モニタの設定値を表示します。
perfmon interval	パフォーマンス モニタの取得間隔を設定します。
show console-output	コンソール バッファを表示します。
show perfmon	パフォーマンス情報をただちに表示します。

perfmon interval

パフォーマンス情報を取得する間隔を秒数で設定するには、特権 EXEC モードで **perfmon interval** コマンドを使用します。

perfmon interval *seconds*

シンタックスの説明

seconds	パフォーマンス表示が更新されるまでの秒数を指定します。

デフォルト

seconds は 120 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
特権 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

パフォーマンス モニタをイネーブルにするには、**perfmon verbose** コマンドを入力します。ディセーブルにするには、**perfmon quiet** コマンドを入力します。出力は、Telnet または SSH ターミナル ウィンドウに表示されます。

例

次に、30 秒おきにパフォーマンス モニタ統計情報を取得する例を示します。

```
hostname# perfmon interval 30
hostname# perfmon verbose
```

関連コマンド

コマンド	説明
perfmon	FWSM がパフォーマンス モニタ情報を取得できるようにします。
perfmon settings	パフォーマンス モニタの設定値を表示します。
show console-output	コンソール バッファを表示します。
show perfmon	パフォーマンス情報を表示します。

perfmon settings

パフォーマンス モニタの設定値を表示するには、特権 EXEC モードで **perfmon settings** コマンドを使用します。

perfmon settings

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
1.1(1)	このコマンドが追加されました。

例　次に、**perfmon** の設定値を表示する例を示します。

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

関連コマンド

コマンド	説明
perfmon	FWSM がパフォーマンス モニタ情報を取得できるようにします。
perfmon interval	パフォーマンス モニタの取得間隔を設定します。
show console-output	コンソール バッファを表示します。
show perfmon	パフォーマンス情報をただちに表示します。

periodic

時間範囲をサポートする機能に、週単位の反復する時間範囲を指定するには、time range コンフィギュレーション モードで ***periodic*** コマンドを使用します。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。

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

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

シンタックスの説明

days-of-the-week	（任意）最初のこの引数は、対応する時間範囲が有効になる最初の日にちまたは曜日です。2 番めのこの引数は、対応するステートメントが有効な最後の日にちまたは曜日です。 この引数は、単一の曜日または曜日の組み合わせです。monday（月曜）、tuesday（火曜）、wednesday（水曜）、thursday（木曜）、friday（金曜）、saturday（土曜）、および sunday（日曜）を指定できます。その他の指定できる値は、次のとおりです。 • daily — 月曜～日曜 • weekdays — 月曜～金曜 • weekend — 土曜および日曜 終了する曜日が開始する曜日と同じ場合は、終了する曜日を省略できます。
time	HH:MM の形式で時刻を指定します。たとえば、8:00 は午前 8 時、20:00 は午後 8 時です。
to	「開始時刻から終了時刻」の範囲を完結させるために、***to*** キーワードを入力する必要があります。

デフォルト

periodic コマンドで値を入力しなかった場合、***time-range*** コマンドで定義された FWSM へのアクセスがただちに有効になり、なおかつ常時有効になります。

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
time-range 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

時間ベースの ACL を実行するには、***time-range*** コマンドを使用して、特定の時刻と曜日を定義します。次に、**access-list extended time-range** コマンドを使用して時間範囲を ACL にバインドします。

periodic コマンドは、時間範囲がいつ有効になるかを指定する 1 つの方法です。***absolute*** コマンドで、絶対時間間隔を指定する方法もあります。時間範囲の名前を指定する、***time-range*** グローバル コンフィギュレーション コマンドのあとで、どちらかのコマンドを使用します。1 つの ***time-range*** コマンドで複数の ***periodic*** を指定できます。

終了する曜日の値が開始の値と同じ場合は、終了の値を省略できます。

time-range コマンドに ***absolute*** と ***periodic*** の値が両方とも指定されていた場合、***periodic*** コマンドが評価されるのは、***absolute start*** の時刻に達してからであり、また、***absolute end*** の時刻を過ぎるてからは評価されません。

例

次に、**periodic** コマンドの設定例を示します。

設定内容	入力
月曜～金曜、午前 8 時～午後 6 時のみ	***periodic weekdays 8:00 to 18:00***
毎日、午前 8 時～午後 6 時のみ	***periodic daily 8:00 to 18:00***
月曜の午前 8 時～金曜の午後 8 時まで常時	***periodic monday 8:00 to friday 20:00***
毎週末、土曜午前～日曜夜	***periodic weekend 00:00 to 23:59***
土曜および日曜、正午～深夜 0 時	***periodic weekend 12:00 to 23:59***

次に、月曜～金曜、午前 8 時～午後 6 時に限定して、FWSM へのアクセスを許可する例を示します。

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

次に、特定の曜日（月曜、火曜、および金曜）、午前 10 時 30 分～午後 12 時 30 分に、FWSM へのアクセスを許可する例を示します。

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

関連コマンド

コマンド	説明
absolute	時間範囲が有効となる絶対時刻を定義します。
access-list extended	FWSM を介して IP トラフィックを許可または拒否するポリシーを設定します。
time-range	時間に基づく FWSM のアクセス制御を定義します。

permit errors

無効な GTP パケットまたは通常は解析エラーでドロップされるパケットを許可するには、GTP マップ コンフィギュレーション モードで **permit errors** コマンドを使用します。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。

permit errors

no permit errors

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

デフォルトでは、無効なパケットまたは解析中にエラーになったパケットはすべて、ドロップされます。

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
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 マップ コンフィギュレーション モードで **permit errors** コマンドを使用すると、無効な GTP パケットまたは通常は解析エラーになってドロップされるパケットが許可されます。

例

次に、無効なパケットまたは解析時にエラーになったパケットが含まれているトラフィックを許可する例を示します。

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

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
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。

pfs

PFS をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **pfs enable** コマンドを使用します。PFS をディセーブルにするには、**pfs disable** コマンドを使用します。実行コンフィギュレーションから PFS 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。このオプションにより、別のグループ ポリシーから PFS の値が継承されます。

PFS は IPSec ネゴシエーション時に、個々の新しい暗号鍵が前の鍵と無関係であることを保証します。

pfs {enable | disable}

no pfs

シンタックスの説明

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

デフォルト

PFS はディセーブルです。

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

VPN クライアントと FWSM で、PFS の設定を一致させる必要があります。

例

次に、FirstGroup というグループ ポリシーの PFS を設定する例を示します。

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

pim

インターフェイス上で PIM を再びイネーブルにするには、インターフェイス コンフィギュレーション モードで **pim** コマンドを使用します。PIM をディセーブルにするには、このコマンドの **no** 形式を使用します。

pim

no pim

シンタックスの説明

このコマンドには、引数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 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

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 をイネーブルにします。コンフィギュレーションには、**pim** コマンドの **no** 形式だけが保存されます。

（注） PIM は PAT ではサポートされません。PIM プロトコルはポートを使用しないのに対して、PAT が機能するのは、ポートを使用するプロトコルと組み合わせた場合に限られます。

例

次に、選択したインターフェイス上で PIM をディセーブルにする例を示します。

```
hostname(config)# interface Vlan101
hostname(config-subif)# no pim
```

関連コマンド

コマンド	説明
multicast-routing	FWSM のマルチキャスト ルーティングをイネーブルにします。

pim accept-register

PIM 登録メッセージをフィルタリングするように FWSM を設定するには、グローバル コンフィギュレーション モードで **pim accept-register** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式を使用します。

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

no pim accept-register

シンタックスの説明

list *acl*	アクセス リスト名または番号を指定します。このコマンドでは、標準ホスト Access Control List（ACL; アクセス制御リスト）を使用します。拡張 ACL はサポートされません。
route-map *map-name*	ルートマップ名を指定します。このコマンドで参照するルートマップでは、標準ホスト ACL を使用します。拡張 ACL はサポートされません。

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
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

このコマンドは、不正な送信元が RP に登録できないようにするために使用します。不正な送信元から RP に登録メッセージが送信されると、FWSM が登録停止メッセージを直ちに返します。

例

次に、[no-ssm-range] というアクセス リストで定義された送信元からのものに、PIM 登録メッセージを限定する例を示します。

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

関連コマンド

コマンド	説明
multicast-routing	FWSM のマルチキャスト ルーティングをイネーブルにします。

pim dr-priority

指定ルータの選定に使用するネイバー プライオリティを FWSM 上で設定するには、インターフェイス コンフィギュレーション モードで **pim dr-priority** コマンドを使用します。デフォルトのプライオリティに戻すには、このコマンドの **no** 形式を使用します。

pim dr-priority *number*

no pim dr-priority

シンタックスの説明

number	0 ～ 4294967294 の数値。この値を使用して、指定ルータを決定するときに、デバイスのプライオリティを判別します。0 を指定すると、FWSM は指定ルータになれません。

デフォルト

デフォルト値は 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
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

インターフェイス上でプライオリティ値が最大のデバイスが PIM 指定ルータになります。指定ルータ プライオリティが同じデバイスが複数ある場合、IP アドレスが最大のデバイスが DR になります。デバイスが hello メッセージに DR-Priority Option を組み込んでいない場合、そのデバイスはプライオリティが最も高いデバイスとみなされて、指定ルータになります。複数のデバイスがそれぞれの hello メッセージにこのオプションを組み込んでいない場合は、IP アドレスが最大のデバイスが指定ルータになります。

例

次に、インターフェイスの DR プライオリティを 5 に設定する例を示します。

```
hostname(config)# interface Vlan101
hostname(config-if)# pim dr-priority 5
```

関連コマンド

コマンド	説明
multicast-routing	FWSM のマルチキャスト ルーティングをイネーブルにします。

pim hello-interval

PIM hello メッセージの間隔を設定するには、インターフェイス コンフィギュレーション モードで **pim hello-interval** コマンドを使用します。hello 間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

pim hello-interval *seconds*

no pim hello-interval [*seconds*]

シンタックスの説明

seconds	hello メッセージを送信するまでに FWSM が待機する秒数。有効値は 1 ～ 3600 秒です。デフォルト値は 30 秒です。

デフォルト

デフォルトの値は、30 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
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。

例

次に、PIM hello 間隔を 1 分に設定する例を示します。

```
hostname(config)# interface Vlan101
hostname(config-if)# pim hello-interval 60
```

関連コマンド

コマンド	説明
multicast-routing	FWSM のマルチキャスト ルーティングをイネーブルにします。

pim join-prune-interval

PIM Join/Prune 間隔を設定するには、インターフェイス コンフィギュレーション モードで **pim join-prune-interval** コマンドを使用します。間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

pim join-prune-interval *seconds*

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

シンタックスの説明

seconds	Join/Prune メッセージを送信するまでに FWSM が待機する秒数。有効値は 10 ～ 600 秒です。デフォルトは 60 秒です。

デフォルト

60 秒

コマンド 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。

例

次に、PIM Join/Prune の間隔を 2 分に設定する例を示します。

```
hostname(config)# interface Vlan101
hostname(config-if)# pim join-prune-interval 120
```

関連コマンド

コマンド	説明
multicast-routing	FWSM のマルチキャスト ルーティングをイネーブルにします。

pim old-register-checksum

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

pim old-register-checksum

no pim old-register-checksum

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

FWSM は、PIM RFC 互換レジスタを生成します。

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

FWSM ソフトウェアは、Cisco IOS の方式ではなく、PIM ヘッダーのチェックサムと次の 4 バイトだけを使用して、登録メッセージを受け付けます。Cisco IOS の方式では、すべての PIM メッセージ タイプについて、PIM メッセージ全体を使用して登録メッセージを受け付けます。**pim old-register-checksum** コマンドは、Cisco IOS ソフトウェアと互換性のあるレジスタを生成します。

例

次に、旧式のチェックサム計算を使用するように FWSM を設定する例を示します。

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

関連コマンド

コマンド	説明
multicast-routing	FWSM のマルチキャスト ルーティングをイネーブルにします。

pim rp-address

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

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

no pim rp-address *ip_address*

シンタックスの説明

acl	（任意）RP で使用するマルチキャスト グループを定義する、アクセス リストの名前または番号。これは標準 IP アクセス リストです。
bidir	（任意）指定のマルチキャスト グループが双方向モードで動作することを指定します。このオプションを指定しないでコマンドを設定した場合、指定のグループは PIM sparse（疎）モードで動作します。
ip_address	PIM RP にするルータの IP アドレス。このアドレスは、4 つに区切られたドット付き 10 進表記のユニキャスト IP アドレスです。

デフォルト

PIM RP アドレスを設定しません。

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
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

共通 PIM sparse モード（PIM-SM）または bidir ドメイン内のすべてのルータに、well-known PIM RP アドレスを認識させる必要があります。このコマンドを使用すると、アドレスが静的に設定されます。

（注）　FWSM は Auto-RP をサポートしません。したがって、**pim rp-address** コマンドを使用して RP アドレスを指定する必要があります。

RP を 1 つ設定することによって、複数のグループを処理できます。アクセス リストで指定されたグループ範囲によって、PIM RP グループのマッピングが決まります。アクセス リストを指定しなかった場合、グループの RP が IP マルチキャスト グループ範囲（224.0.0.0/4）全体に適用されます。

（注）　FWSM は、実際の bidir 設定に関係なく、必ず PIM hello メッセージで bidir 機能をアドバタイズします。

例

次に、すべてのマルチキャスト グループに対して、PIM RP アドレスを 10.0.0.1 に設定する例を示します。

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

関連コマンド

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

pim spt-threshold infinity

必ず共有ツリーを使用し、Shortest-Path Tree（SPT）スイッチオーバーを実行しないように、ラスト ホップ ルータの動作を変更するには、グローバル コンフィギュレーション モードで **pim spt-threshold infinity** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

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

no pim spt-threshold

シンタックスの説明

group-list *acl*	（任意）アクセス リストで制限する送信元グループを指定します。*acl* 引数では、標準 Access Control List（ACL; アクセス制御リスト）を指定する必要があります。拡張 ACL はサポートされません。

デフォルト

ラスト ホップ PIM ルータは、デフォルトで送信元 SPT に切り替えます。

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

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

例

次に、ラスト ホップ PIM ルータが、送信元 SPT に切り替えるのではなく、必ず共有ツリーを使用するように設定する例を示します。

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

関連コマンド

コマンド	説明
multicast-routing	FWSM のマルチキャスト ルーティングをイネーブルにします。

ping

FWSM から他の IP アドレスを参照できるかどうかを決定するには、特権 EXEC モードで **ping** コマンドを使用します。

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

シンタックスの説明

***data** pattern*	（任意）16 進形式で 16 ビットのデータ パターンを指定します。
host	ping の対象となるホストの IPv4 または IPv6 アドレス、または名前を指定します。
if_name	（任意）*host* からアクセスできる、***nameif*** コマンドで設定されたインターフェイス名を指定します。指定しなかった場合、*host* は IP アドレスとして解決され、ルーティング テーブルに従って宛先インターフェイスが判別されます。
***repeat** count*	（任意）ping 要求を繰り返す回数を指定します。
***size** bytes*	（任意）データグラム サイズをバイト数で指定します。
timeout *seconds*	（任意）ping 要求をタイムアウトさせるまでに待機する秒数を指定します。
validate	（任意）応答データを検証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
特権 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

ping コマンドを使用すると、FWSM が接続されているかどうか、またはネットワーク上のホストを使用できるかどうかを判別できます。FWSM が接続されている場合は、**icmp permit any** *interface* コマンドが設定されているかどうかを確認します。FWSM が ***ping*** コマンドから生成されたメッセージに応答して受け付けることができるようにするには、この設定が必要です。***ping*** コマンドの出力は、応答が受信されたかどうかを示します。ホストが応答していない場合、**ping** コマンドを入力すると、次のようなメッセージが表示されます。

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

FWSM がネットワークに接続していて、トラフィックを送受信していることを確認するには、***show interface*** コマンドを使用します。指定された *if_name* のアドレスは、ping の送信元アドレスとして使用されます。

内部ホストから外部ホストに ping を実行させるには、次のいずれかの作業が必要です。

- エコー応答用の ICMP ***access-list*** コマンドを作成して、たとえば、すべてのホストに ping でアクセスできるようにしてから、***access-list acl_grp permit icmp any any*** コマンドを使用して、***access-group*** コマンドでテストするインターフェイスに ***access-list*** コマンドをバインドします。
- **inspect icmp** コマンドを使用して ICMP インスペクション エンジンを設定します。たとえば、グローバル サービス ポリシーに対応する **class default_inspection** クラスに **inspect icmp** コマンドを追加すると、内部ホストによって開始されたエコー要求に対する、FWSM を経由したエコー応答が許可されます。

拡張 ping も実行できます。この場合、一度に 1 行ずつキーワードを入力します。

ホスト間またはルータ間で、FWSM を介して ping を送信しても、ping を実行できない場合は、**capture** コマンドを使用して、ping の成否をモニタします。

FWSM **ping** コマンドには、インターフェイス名は不要です。インターフェイス名を指定しなかった場合、FWSM はルーティング テーブルを調べて、指定されたアドレスを検出します。インターフェイス名を指定すると、ICMP エコー要求の送信に使用されるインターフェイスを指定できます。

例

次に、FWSM から他の IP アドレスを参照できるかどうかを判別する例を示します。

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

次に、拡張 ping の例を示します。

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

関連コマンド

コマンド	説明
capture	インターフェイスでパケットをキャプチャします。
icmp	インターフェイスで終端する ICMP トラフィックのアクセス ルールを設定します。
show interface	VLAN の設定情報を表示します。

policy

CRL の取得元を指定するには、crl configure コンフィギュレーション モードで **policy** コマンドを使用します。crl configure コンフィギュレーション モードには、crypto ca トラストポイント コンフィギュレーション モードからアクセスします。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。

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

no policy [***static*** | ***cdp*** | ***both***]

シンタックスの説明

both	CRL 配布ポイントを使用して CRL を取得できなかった場合に、5 回を限度とし、スタティック CDP を使用して再試行することを指定します。
cdp	チェックする証明書に組み込まれた CDP 拡張子を使用します。この場合、FWSM は確認する証明書の CDP 拡張子から最大 5 つの CRL 配布ポイントを取得し、必要に応じて、設定されたデフォルト値で情報を補います。プライマリ CDP による CRL 取得に失敗した場合、FWSM はリストで次に使用可能な CDP を使用して再試行します。FWSM が CRL を取得するか、リストの終わりに達するまで、この作業が続けられます。
static	最大 5 つのスタティック CRL 配布ポイントを使用します。このオプションを指定する場合は、**protocol** コマンドで LDAP または HTTP URL も指定します。

デフォルト

デフォルトの設定は **cdp** 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
crl configure 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、ca-crl コンフィギュレーション モードを開始し、チェックする証明書に組み込まれた CRL 配布ポイント拡張子を使用して、またはそれが失敗した場合はスタティック CDP を使用して、CRL を取得することを設定する例を示します。

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

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
url	CRL を取得するためのスタティック URL リストを作成して維持します。

policy-map

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

policy-map *name*

no policy-map *name*

シンタックスの説明

name	このポリシーマップの名前。名前の最大長は 40 文字です。

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
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

policy-map コマンドでは、ポリシーを設定します。ポリシーは、トラフィック クラスとセキュリティに関連する 1 つ以上のアクションを関連付けたものです。トラフィック クラスは、パケットの内容で識別可能な 1 組のトラフィックです。たとえば、ポート値が 23 の TCP トラフィックは、Telnet トラフィック クラスとして分類できます。ポリシーは、**class** コマンドとそのコマンドに対応付られたアクションからなります。ポリシー マップでは複数のポリシーを指定できます。**service-policy** コマンドは、すべてのインターフェイス上でグローバルに、または 1 つのターゲット インターフェイス上でポリシー マップをアクティブにします。

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

ポリシー マップの最大数は 64 です。

policy-map コマンドを使用してポリシーマップ モードを開始します。ポリシーマップ モードでは、**class** コマンドおよび **description** コマンドを入力できます。詳細については、個々のコマンドの項を参照してください。

ポリシー マップの各種アクションが実行される順序は、これらのコマンド記述でアクションが出現する順序とは無関係です。

例

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

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

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

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

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

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

関連コマンド

コマンド	説明
class	トラフィックを分類するためのクラスマップを指定します。
clear configure policy-map	すべてのポリシー　マップ設定を削除します。ただし、service-policy コマンドでポリシー マップが使用されている場合は例外として、削除されません。
description	ポリシー マップの説明を指定します。
show running-config policy-map	現在のすべてのポリシー マップ設定を表示します。

polltime interface

インターフェイスにおける hello パケットの間隔を指定するには、フェールオーバー グループ コンフィギュレーション モードで **polltime interface** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

polltime interface *time*

no polltime interface *time*

シンタックスの説明

time	Hello メッセージの時間間隔

デフォルト

デフォルトは 15 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
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

polltime interface コマンドは、現在のフェールオーバー グループに関連付けられたインターフェイスから hello パケットを送信する間隔を変更する場合に使用します。ポーリング間隔を短くすると、FWSM による障害の検出とフェールオーバーの起動がより迅速に行われます。ただし、ネットワークが一時的に輻輳している場合には、不要なスイッチオーバーが行われる可能性があります。

連続して 5 回、インターフェイスの hello パケットが検出されなかった場合は、インターフェイスのテストが開始されます。

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。

例

フェールオーバー グループの設定例（部分）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)# polltime interface 20
hostname(config-fover-group)# exit
hostname(config)#
```

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 polltime	モニタ対象インターフェイスにおける hello パケットの時間間隔を設定します。

port-misuse

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

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

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

シンタックスの説明

action	設定したカテゴリのアプリケーションが検出されたときに実行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。
im	インスタント メッセージング アプリケーション カテゴリのトラフィックを制限します。チェックされるアプリケーションは Yahoo Messenger、AIM、および MSN IM です。
log	（任意）Syslog を生成します。
p2p	ピアツーピア アプリケーション カテゴリのトラフィックを制限します。Kazaa アプリケーションがチェックされます。
reset	クライアントおよびサーバに TCP リセット メッセージを送信します。
tunneling	トンネリング アプリケーション カテゴリのトラフィックを制限します。チェックされるアプリケーションは、HTTPort/HTTHost、GNU Httptunnel、GotoMyPC、Firethru、および Http-tunnel.com Client です。

デフォルト

このコマンドは、デフォルトではディセーブルです。このコマンドをイネーブルしながら、サポート対象のアプリケーション カテゴリ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

port-misuse 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アプリケーション カテゴリ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、設定されたリストのアプリケーション カテゴリ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。設定済みの **default** アクションでは、ロギングを行わずに接続を**許可**します。

たとえば、事前設定されたデフォルト アクションを使用し、なおかつ 1 つ以上のアプリケーション カテゴリを選択してアクション **drop** および **log** を指定した場合、FWSM は設定されたアプリケーション カテゴリが含まれている接続をドロップし、各接続を記録し、その他のサポート対象アプリケーション タイプについては、すべての接続を許可します。

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。そのあと、**allow** アクションを指定して、許可するアプリケーション タイプを設定します。

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

注意　これらの検査には、HTTP メッセージのエンティティ本体を検索する必要があるので、FWSM のパフォーマンスが低下する可能性があります。

このコマンドの **no** 形式を使用して、設定済みアプリケーション タイプのリストからアプリケーション カテゴリを削除すると、コマンドラインでアプリケーション カテゴリ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。

例

次に、設定済みのデフォルトを使用して、特に禁止されていないサポート対象アプリケーション タイプをすべて許可する、制限の緩いポリシーを設定する例を示します。

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

この場合、ピアツーピア カテゴリの接続だけがドロップされ、イベントが記録されます。

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アプリケーション タイプについて、接続がリセットされ、イベントが記録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)# port-misuse default action reset log
hostname(config-http-map)# port-misuse im allow
hostname(config-http-map)# exit
```

この場合、Instant Messenger アプリケーションだけが許可されます。それ以外のサポート対象アプリケーションの HTTP トラフィックを受信すると、FWSM によって接続がリセットされ、Syslog エントリが作成されます。

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。

port-object

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

port-object eq *service*

no port-object eq *service*

port-object range *begin_service end_service*

no port-object range *begin_service end_service*

シンタックスの説明

begin_service	サービス範囲の先頭値となる、TCP または UDP ポートを示す 10 進数または名前を指定します。この値は 0 ～ 65535 の範囲内にする必要があります。
end_service	サービス範囲の終了値となる、TCP または UDP ポートを示す 10 進数または名前を指定します。この値は 0 ～ 65535 の範囲内にする必要があります。
eq service	サービス オブジェクト用の TCP または UDP ポートを示す 10 進数または名前を指定します。
range	ポート範囲を指定します（包含型）

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
サービス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
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

port-object コマンドは **object-group** コマンドと組み合わせて使用し、サービス コンフィギュレーション モードで、特定のサービス（ポート）またはサービス範囲（複数のポート）のどちらかであるオブジェクトを定義します。

TCP または UDP サービスの名前を指定する場合は、サポート対象の TCP 名、UDP 名、またはその両方の名前のいずれかにする必要があります。また、オブジェクト グループのプロトコル タイプと矛盾しないようにする必要があります。たとえば、プロトコル タイプが tcp、udp、または tcp-udp の場合、名前はそれぞれ有効な TCP サービス名、有効な UDP サービス名、または有効な TCP/UDP サービス名にする必要があります。

番号を指定した場合は、オブジェクトの表示時に、プロトコル タイプに基づいて対応する名前（ある場合）に変換されます。

サポートされるサービス名は、次のとおりです。

表 22-1

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

例

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

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

関連コマンド

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

preempt

プライオリティの高い装置がブート時にアクティブになるようにするには、フェールオーバー グループ コンフィギュレーション モードで **preempt** コマンドを使用します。プリエンプションを削除するには、このコマンドの **no** 形式を使用します。

preempt [*delay*]

no preempt [*delay*]

シンタックスの説明

seconds	ピアに優先権が渡るまでの待機時間（秒数）。有効値は 1 ～ 1200 秒です。

デフォルト

デフォルトでは、待機時間はありません。

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
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

フェールオーバー グループにプライマリまたはセカンダリのプライオリティを割り当てると、両方の装置が（装置のポーリング時間内で）同時にブートした場合に、フェールオーバー グループのアクティブになる装置が指定されます。ただし、一方の装置が他方より先にブートした場合は、その装置上で両方のフェールオーバー グループがアクティブになります。他方の装置がオンラインになると、セカンダリ装置にプライオリティが与えられているフェールオーバー グループは、**preempt** コマンドでフェールオーバー グループが設定されているか、または **no failover active** コマンドで他方の装置に手動で強制的に移さないかぎり、セカンダリ装置上ではアクティブになりません。**preempt** コマンドでフェールオーバー グループが設定されている場合、フェールオーバー グループは指定された装置上で自動的にアクティブになります。

（注）　ステートフル フェールオーバーがイネーブルの場合、その時点でフェールオーバー グループがアクティブな装置から接続がコピーされるまで、プリエンプションは実行されません。

例

次に、プライマリ装置のプライオリティを高くしてフェールオーバー グループ 1 を設定し、セカンダリ装置のプライオリティを高くしてフェールオーバー グループ 2 を設定する例を示します。待機時間を 100 秒に指定した **preempti** コマンドで両方のフェールオーバー グループを設定するので、装置が使用可能になってから 100 秒後に、優先装置上でフェールオーバー グループが自動的にアクティブになります。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)#
```

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。
primary	設定するフェールオーバー グループのフェールオーバー ペアのプライマリ装置に、プライオリティを与えます。
secondary	設定するフェールオーバー グループのフェールオーバー ペアのセカンダリ装置に、プライオリティを与えます。

prefix-list

ABR タイプ 3 LSA フィルタリング用のプレフィクス リストにエントリを作成するには、グローバル コンフィギュレーション モードで **prefix-list** コマンドを使用します。プレフィクス リストのエントリを削除するには、このコマンドの **no** 形式を使用します。

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

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

シンタックスの説明

/	*network* 値と *len* 値の間に分離記号が必要です。
deny	条件が一致した場合にアクセスを拒否します。
ge *min_value*	（任意）最小限一致しなければならないプレフィクスの長さを指定します。*min_value* 引数の値は、*len* 引数の値より大きくなければなりません。また、*max_value* 引数を指定する場合は、その値以下でなければなりません。
le *max_value*	（任意）一致しなければならないプレフィクスの最大長を指定します。*max_value* 引数の値は、*min_value* 引数が指定されている場合、その値以上でなければなりません。または、*min_value* 引数が指定されていない場合は、*len* 引数の値より大きくなければなりません。
len	ネットワーク マスクの長さ。有効値は 0 ～ 32 です。
network	ネットワーク アドレス
permit	条件が一致した場合にアクセスを許可します。
prefix-list-name	プレフィクス リスト名。プレフィクス リスト名にスペースを含めることはできません。
seq *seq_num*	（任意）作成するプレフィクス リストに指定のシーケンス番号を適用します。

デフォルト

シーケンス番号を指定しなかった場合は、プレフィクス リストの最初のエントリにシーケンス番号として 5 が割り当てられ、以後、各エントリのシーケンス番号は 5 ずつ大きくなります。

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（**ip prefix-list** として）追加されました。
3.1(1)	このコマンドが **ip prefix-list** から **prefix-list** に変更されました。

使用上のガイドライン

prefix-list コマンドは、ABR タイプ 3 LSA フィルタリング コマンドです。ABR タイプ 3 LSA フィルタリングを使用すると、OSPF が動作している ABR の機能が拡張され、異なる OSPF エリア間でタイプ 3 LSA をフィルタリングできるようになります。プレフィクス リストの設定後は、指定したプレフィクスだけがあるエリアから別のエリアに送信されます。その他のプレフィクスはすべて、それぞれの OSPF エリアに限定されます。このタイプのエリア フィルタリングは、OSPF エリアに着信するトラフィック、OSPF エリアから発信するトラフィック、またはそのエリアの着信トラフィックと発信トラフィックの両方に適用できます。

プレフィクス リストの複数のエントリが所定のプレフィクスと一致した場合は、最小シーケンス番号のエントリが使用されます。FWSM は、プレフィクス リストの先頭、シーケンス番号が最小のエントリから検索を開始します。いったん一致すると、FWSM はそれ以上、リストを検索しません。効率をよくするには、小さいシーケンス番号を手動で割り当てることによって、最も一般的な一致または拒否のエントリがリストの先頭近くに来るようにします。

デフォルトでは、シーケンス番号は自動的に生成されます。**no prefix-list sequence-number** コマンドを使用すると、シーケンス番号の自動生成を抑制できます。シーケンス番号は、5 の倍数で生成されます。したがって、プレフィクス リストの先頭のシーケンス番号は 5 になります。リストの次のエントリには、10 のシーケンス番号が与えられます（以下、同様）。あるエントリに値を指定し、その後のエントリに値を指定しなかった場合、生成されるシーケンス番号は指定値から 5 ずつ増えていきます。たとえば、プレフィクス リストの先頭エントリに 3 というシーケンス番号を与えることを指定してから、2 つのエントリを追加し、なおかつ追加のエントリにシーケンス番号を指定しなかった場合、追加した 2 つのエントリには 8 および 13 というシーケンス番号が自動的に生成されます。

ge および ***le*** キーワードを使用すると、プレフィクスと一致すべきプレフィクス長の範囲を *network*/*len* 引数の場合より具体的に指定できます。***ge*** キーワードまたは ***le*** キーワードをどちらも指定しなかった場合は、完全一致が想定されます。***ge*** キーワードだけを指定した場合、範囲は *min_value* ～ 32 です。***le*** キーワードだけを指定した場合、範囲は *len* ～ *max_value* です。

min_value および *max_value* 引数の値は、次の条件を満たしていなければなりません。

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

プレフィクス リストから特定のエントリを削除するには、このコマンドの **no** 形式を使用します。プレフィクス リストを削除するには、**clear configure prefix-list** コマンドを使用します。**clear configure prefix_list** コマンドを使用すると、対応付られた **prefix-list description** コマンド（ある場合）もコンフィギュレーションから削除されます。

例

次に、デフォルト ルート 0.0.0.0/0 を拒否する例を示します。

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

次に、プレフィクス 10.0.0.0/8 を許可する例を示します。

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

次に、プレフィクス 192/8 のルートで最大 24 ビットのマスク長を受け付ける例を示します。

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

次に、プレフィクス 192/8 のルートで 25 ビットを超えるマスク長を拒否する例を示します。

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

次に、すべてのアドレス スペースで 8 ～ 24 ビットのマスク長を許可する例を示します。

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

次に、すべてのアドレス スペースで 25 ビットを超えるマスク長を拒否する例を示します。

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

次に、プレフィクスが 10/8 のすべてのルートを拒否する例を示します。

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

次に、プレフィクスが 192.168.1/24 のルートで、長さが 25 ビットを超えるすべてのマスクを拒否する例を示します。

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

次に、プレフィクスが 0/0 のすべてのルートを許可する例を示します。

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

関連コマンド

コマンド	説明
clear configure prefix-list	実行コンフィギュレーションから **prefix-list** コマンドを削除します。
prefix-list description	プレフィクス リストの説明を入力します。
prefix-list sequence-number	プレフィクス リストのシーケンス番号付けをイネーブルにします。
show running-config prefix-list	実行コンフィギュレーションに含まれている **prefix-list** コマンドを表示します。

prefix-list description

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

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

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

シンタックスの説明

prefix-list-name	プレフィクス リスト名
text	プレフィクス リストを説明するテキスト。80 文字まで入力できます。

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
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

prefix-list コマンドおよび **prefix-list description** コマンドは、特定のプレフィクス リスト名に対して任意の順序で入力できます。プレフィクス リストの説明を入力する前に、プレフィクス リストを作成する必要はありません。**prefix-list description** コマンドは必ず、コンフィギュレーションの対応するプレフィクス リストの前の行に配置されます。

すでに説明のあるプレフィクス リスト エントリに **prefix-list description** コマンドを入力した場合は、新しい説明によって元の説明が置き換えられます。

このコマンドの **no** 形式を使用する場合は、説明テキストの入力は不要です。

例

次に、MyPrefixList というプレフィクス リストの説明を追加する例を示します。**show running-config prefix-list** コマンドから、実行コンフィギュレーションにプレフィクス リストの説明が追加されているが、プレフィクス リストそのものは設定されていないことがわかります。

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

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

関連コマンド

コマンド	説明
clear configure prefix-list	実行コンフィギュレーションから **prefix-list** コマンドを削除します。
prefix-list	ABR タイプ 3 LSA フィルタリング用のプレフィクス リストを定義します。
show running-config prefix-list	実行コンフィギュレーションに含まれている **prefix-list** コマンドを表示します。

prefix-list sequence-number

プレフィクス リストのシーケンス番号付けをイネーブルにするには、グローバル コンフィギュレーション モードで **prefix-list sequence-number** コマンドを使用します。プレフィクス リストのシーケンス番号付けをディセーブルにするには、このコマンドの **no** 形式を使用します。

prefix-list sequence-number

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

プレフィクス リストのシーケンス番号付けは、デフォルトでイネーブルです。

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

コンフィギュレーションに含まれるのは、コマンドの **no** 形式だけです。コンフィギュレーションにこのコマンドの **no** 形式が指定されている場合、コンフィギュレーションの **prefix-list** コマンドから、手動設定されたものを含めてシーケンス番号が削除されます。また、新しいプレフィクス リスト エントリには、シーケンス番号が割り当てられません。

プレフィクス リストのシーケンス番号付けがイネーブルの場合、デフォルトの番号付け方式（5 から始まり 5 ずつ増加）を使用して、プレフィクス リストのすべてのエントリにシーケンス番号が割り当てられます。番号付けをディセーブルにする前に、プレフィクス リスト エントリにシーケンス番号が手動で設定されていた場合は、手動設定の番号が復元されます。自動番号付けがディセーブルのときに手動設定されたシーケンス番号も復元されます。ただし、番号付けがディセーブルの間はそれらのシーケンス番号は表示されません。

例

次に、プレフィクス リストのシーケンス番号付けをディセーブルにする例を示します。

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

関連コマンド

コマンド	説明
prefix-list	ABR タイプ 3 LSA フィルタリング用のプレフィクス リストを定義します。
show running-config prefix-list	実行コンフィギュレーションに含まれている **prefix-list** コマンドを表示します。

pre-shared-key

事前共有鍵に基づく IKE 接続をサポートするために、事前共有鍵を指定するには、tunnel-group ipsec-attributes コンフィギュレーション モードで **pre-shared-key** コマンドを使用します。デフォルト値に戻すには、このコマンドの ***no*** 形式を使用します。

pre-shared-key *key*

no pre-shared-key

シンタックスの説明

key	1 ～ 128 文字の英数字鍵を指定します。

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
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

すべてのトンネルグループ タイプにこの属性を適用できます。

例

config-ipsec コンフィギュレーション モードで次のコマンドを入力し、209.165.200.225 という IPSec LANto-LAN トンネル グループの IKE 接続をサポートするための事前共有鍵 XYZX を指定します。

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

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されたトンネル 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。

primary

フェールオーバー グループのプライオリティをプライマリ装置で高くするには、フェールオーバー グループ コンフィギュレーション モードで **primary** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

primary

no primary

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

フェールオーバー グループに関して、**primary** または **secondary** を指定しなかった場合、フェールオーバー グループのデフォルトは **primary** 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
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

フェールオーバー グループにプライマリまたはセカンダリのプライオリティを割り当てると、両方の装置が（装置のポーリング時間内で）同時にブートした場合に、フェールオーバー グループのアクティブになる装置が指定されます。一方の装置が他方より先にブートした場合は、その装置上で両方のフェールオーバー グループがアクティブになります。他方の装置がオンラインになると、セカンダリ装置にプライオリティが与えられているフェールオーバー グループは、**preempt** コマンドでフェールオーバー グループが設定されているか、または **no failover active** コマンドで他方の装置に手動で強制的に移さないかぎり、セカンダリ装置上ではアクティブになりません。

例

次に、プライマリ装置のプライオリティを高くしてフェールオーバー グループ 1 を設定し、セカンダリ装置のプライオリティを高くしてフェールオーバー グループ 2 を設定する例を示します。どちらのフェールオーバー グループも **preempt** コマンドを使用して設定するので、グループは優先装置が使用可能になった時点で、その装置上で自動的にアクティブになります。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)#
```

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。
preempt	優先装置が使用可能になった時点で、その装置上でフェールオーバー グループを強制的にアクティブにします。
secondary	セカンダリ装置にプライマリ装置より高いプライオリティを与えます。

privilege

コマンドの特権レベルを設定するには、グローバル コンフィギュレーション モードで **privilege** コマンドを使用します。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。

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

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

シンタックスの説明

clear	（任意）指定されたコマンドに対応する **clear** コマンドの特権レベルを設定します。
command *command*	特権レベルを設定するコマンドを指定します。
configure	（任意）指定したコマンドの特権レベルを設定します。
level *level*	特権レベルを指定します。有効値は 0 ～ 15 です。
mode enable	（任意）コマンドの特権モード用のレベルであることを指定します。
mode configure	（任意）コマンドのコンフィギュレーション モード用のレベルであることを指定します。
show	（任意）指定されたコマンドに対応する **show** コマンドの特権レベルを設定します。

デフォルト

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
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

privilege コマンドを使用すると、FWSM コマンドにユーザ定義の特権レベルを設定できます。このコマンドは、関連する configure、show、および clear コマンドに対応する、さまざまな特権レベルを設定する場合に便利です。新しい特権レベルを使用する前に、セキュリティ ポリシーを使用して、コマンドの特権レベルが変更されているかを確認してください。

コマンドおよびユーザに特権レベルが設定されている場合は、2 つの設定が比較されて、所定のユーザが指定されたコマンドを実行できるかどうかが判別されます。ユーザの特権レベルがコマンドの特権レベルよりも低い場合、ユーザはコマンドを実行できません。

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

mode enable および **mode configure** キーワードは、特権モードおよびコンフィギュレーション モードの両方を持つコマンドに使用します。

特権レベルは値が小さいほど、レベルが低くなります。

（注） 定義した新しい特権レベルを AAA（認証、認可、アカウンティング）サーバのコンフィギュレーションで使用するには、事前に **aaa authentication** および **aaa authorization** コマンドにその特権レベルを追加する必要があります。

例

次に、各ユーザの特権レベルを [5] に設定する例を示します。

```
hostname(config)# username intern1 password pass1 privilege 5
```

次に、特権レベルが [5] の一連の **show** コマンドを定義する例を示します。

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

次に、AAA 許可設定全体に特権レベル 11 を適用する例を示します。

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

関連コマンド

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

prompt

CLI プロンプトをカスタマイズするには、グローバル コンフィギュレーション モードで **prompt** コマンドを使用します。デフォルトのプロンプトに戻すには、このコマンドの **no** 形式を使用します。

prompt [<*keyword*> [*keyword*>] ...]

no prompt [<*keyword*> [*keyword*>] ...]

シンタックスの説明

キーワード	説明
context	現在のコンテキストを表示するようにプロンプトを設定します（マルチ モードのみ）。
domain	ドメインを表示するプロンプトを設定します。
hostname	ホスト名を表示するプロンプトを設定します。
priority	[failover lan unit] の設定を表示するようにプロンプトを設定します。
slot	必要に応じて、スロット位置を表示するようにプロンプトを設定します。
state	現在のトラフィック処理状態を表示するプロンプトを設定します。

デフォルト

デフォルトのプロンプトは、ホスト名またはコンテキスト プロンプトの後ろに、ユーザ EXEC モードを表すかぎカッコ（>）または特権 EXEC モードを表すポンド記号（#）を加えたものになります。

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
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

セッション プロンプトの表示を設定するには、コンフィギュレーション モード（P_CONF）、レプリケーション モード（P_REP）、シングル モード、およびマルチモードのシステム コンテキストで、**prompt** コマンドを使用します。設定されたプロンプトを表示できるのは、管理者のみです。ユーザ コンテキストの場合は、デフォルトのホスト名 / コンテキスト（config モード）プロンプトを表示できます。

プロンプトに情報を追加する機能により、複数のモジュールが存在する場合にログインしているモジュールを一目で把握することができます。フェールオーバー中、両方のモジュールのホスト名が同じ場合などに役立ちます。

例

次に、プロンプトを設定する例を示します。

```
fwsm(config)# prompt hostname context priority slot state
```

前提

```
hostname = myfwsm
context = admin
priority = failover lan unit primary
slot = 6 (assume FWSM)
state = Active (with failover enabled)
```

プロンプトの表示

```
myfwsm/admin/pri/6/act>
myfwsm/admin/pri/6/act#
myfwsm/admin/pri/6/act(config)#
myfwsm/admin/pri/6/act(config-interface)#
```

ヘルプおよび用途

```
FWSM(config)# help prompt

FWSM(config)# prompt ?

configure mode commands/options:
hostname    Configures the prompt to display the hostname
domain       Configures the prompt to display the domain
context       Configures the prompt to display the current context (multimode only)
priority       Configures the prompt to display the 'failover lan unit' setting
state           Configures the prompt to display the current traffic handling state
slot             Configures the prompt to display the slot location (when applicable)
```

関連コマンド

コマンド	説明
clear prompt	設定されたプロンプトを消去します。
show prompt	設定されているプロンプトを表示します。

protocol http

CRL を取得するために許可する配布ポイント プロトコルとして HTTP を指定するには、crl configure コンフィギュレーション モードで **protocol http** コマンドを使用します。crl configure コンフィギュレーション モードには、crypto ca トラストポイント コンフィギュレーション モードからアクセスします。許可された CRL 取得方式としての HTTP を削除するには、このコマンドの **no** 形式を使用します。許可されていれば、CRL 配布ポイントの内容によって、取得方式（HTTP、LDAP、SCEP、またはそれらすべて）が決まります。

protocol http

no protocol http

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

HTTP を許可するのがデフォルトの設定です。

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
crl configure 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場合は、パブリック インターフェイス フィルタに必ず HTTP ルールを割り当ててください。

例

次に、crl configure コンフィギュレーション モードを開始し、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして、HTTP を許可する例を示します。

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

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
protocol ldap	CRL の取得方式として LDAP を指定します。
protocol scep	CRL の取得方式として SCEP を指定します。

protocol ldap

CRL を取得するための配布ポイント プロトコルとして LDAP を指定するには、crl configure コンフィギュレーション モードで **protocol ldap** コマンドを使用します。crl configure コンフィギュレーション モードには、crypto ca トラストポイント コンフィギュレーション モードからアクセスします。許可された CRL 取得方式としての LDAP プロトコルを削除するには、このコマンドの **no** 形式を使用します。許可されていれば、CRL 配布ポイントの内容によって、取得方式（HTTP、LDAP、SCEP、またはそれらすべて）が決まります。

protocol ldap

no protocol ldap

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

LDAP を許可するのがデフォルトの設定です。

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
crl configure 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、crl configure コンフィギュレーション モードを開始し、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして、LDAP を許可する例を示します。

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

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
protocol http	CRL の取得方式として HTTP を指定します。
protocol scep	CRL の取得方式として SCEP を指定します。

protocol-object

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

protocol-object *protocol*

no protocol-object *protocol*

シンタックスの説明

protocol	プロトコルの名前または番号

デフォルト

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
プロトコル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
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

protocol-object コマンドは **object-group** コマンドと組み合わせて、プロトコル コンフィギュレーション モードで使用し、プロトコル オブジェクトを定義します。

protocol 引数で IP プロトコル名または番号を指定できます。UDP のプロトコル番号は 17、TCP のプロトコル番号は 6、EGP のプロトコル番号は 47 です。

例

次に、プロトコル オブジェクトを定義する例を示します。

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

関連コマンド

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

protocol scep

CRL を取得するための配布ポイント プロトコルとして SCEP を指定するには、crl configure コンフィギュレーション モードで **protocol scep** コマンドを使用します。crl configure コンフィギュレーション モードには、crypto ca トラストポイント コンフィギュレーション モードからアクセスします。許可された CRL 取得方式としての SCEP プロトコルを削除するには、このコマンドの **no** 形式を使用します。許可されていれば、CRL 配布ポイントの内容によって、取得方式（HTTP、LDAP、SCEP、またはそれらすべて）が決まります。

protocol scep

no protocol scep

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

SCEP を許可するのがデフォルトの設定です。

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
crl configure 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、crl configure コンフィギュレーション モードを開始し、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして、SCEP を許可する例を示します。

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

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
protocol http	CRL の取得方式として HTTP を指定します。
protocol ldap	CRL の取得方式として LDAP を指定します。

pwd

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

pwd

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトはルート ディレクトリ（/）です。

コマンド 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

このコマンドの機能は、***dir*** コマンドと類似しています。

例

次に、現在の作業ディレクトリを表示する例を示します。

```
hostname# pwd
flash:
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリ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。
more	ファイルの内容を表示します。