CHAPTER 12

email ～ ftp-map コマンド

email

エンロールメント実行中に証明書の Subject Alternative Name 拡張に特定の電子メール アドレスを付加するには、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、**email** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

email *address*

no email [*address***]**

シンタックスの説明

address	電子メール アドレスを指定します。*address* の最大長は、64 文字です。

デフォルト

デフォルトは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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 のエンロールメント要求に電子メール アドレス jjh@nhf.net を含める例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# email jjh@nhf.net
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。

enable

特権 EXEC モードを開始するには、ユーザ EXEC モードで、**enable** コマンドを使用します。

enable [*level*]

シンタックスの説明

level	（任意）0 ～ 15 の特権レベルを入力します。

デフォルト

コマンド許可を使用しない場合には、特権レベル 15 を入力します。この場合、デフォルトのレベルは、ユーザ名に設定されているレベルに応じて異なります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ 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

デフォルトのイネーブル パスワードは設定されていません。パスワードの設定については、**enable password** コマンドを参照してください。

デフォルトの 15 以外の特権レベルを使用するには、ローカル コマンド許可を設定し（**aaa authorization command** コマンドを使用し、***LOCAL*** キーワードを指定）、**privilege** コマンドを使用して、コマンドを異なる特権レベルに設定します。ローカル コマンド許可を設定しない場合、特権レベルは無視され、設定したレベルに関係なく、レベル 15 にアクセスします。現在の特権レベルを表示するには、**show curpriv** コマンドを参照してください。

レベル 2 以上は、特権 EXEC モードを開始します。レベル 0 および 1 は、ユーザ EXEC モードを開始します。

特権 EXEC モードを終了するには、**disable** コマンドを使用します。

例

次に、特権 EXEC モードを開始する例を示します。

```
hostname> enable
Password: Pa$$w0rd
hostname#
```

次に、レベル 10 の特権 EXEC モードを開始する例を示します。

```
hostname> enable 10
Password: Pa$$w0rd10
hostname#
```

関連コマンド

コマンド	説明
enable password	イネーブル パスワードを設定します。
disable	特権 EXEC モードを終了します。
aaa authorization command	コマンド許可を設定します。
privilege	ローカル コマンド許可のコマンド特権レベルを設定します。
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。

enable password

特権 EXEC モードのイネーブル 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、**enable password** コマンドを使用します。15 以外のレベルのパスワードを削除するには、このコマンドの **no** 形式を使用します。レベル 15 のパスワードを削除することはできません。

enable password *password* **[level** *level*] [***encrypted***]

no enable password level *level*

シンタックスの説明

encrypted	（任意）パスワードが暗号形式であ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。何らかの理由でパスワードを別の FWSM にコピーする必要があり、元のパスワードが不明な場合には、暗号化されたパスワードとこのキーワードを使用して、**enable password** コマンドを入力します。通常、このキーワードが表示されるのは、**show running-config enable** コマンドを入力した場合だけです。
level *level*	（任意）0 ～ 15 の特権レベルのパスワードを設定します。
password	英数字と特殊文字を使用し、大文字と小文字を区別した 16 文字までの文字列でパスワードを設定します。パスワードには、疑問符およびスペースを除くすべての文字が使用できます。

デフォルト

デフォルトのパスワードは設定されていません。デフォルトのレベルは、15 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

特権レベル 15（デフォルト レベル）のデフォルトのパスワードはブランクです。パスワードをブランクに戻すには、*password* に何もテキストを入力しないでください。

マルチ コンテキスト モードでは、システム コンフィギュレーションおよび各コンテキストのイネーブル パスワードを作成できます。

デフォルトの 15 以外の特権レベルを使用するには、ローカル コマンド許可を設定し（**aaa authorization command** コマンドを使用し、***LOCAL*** キーワードを指定）、**privilege** コマンドを使用して、コマンドを異なる特権レベルに設定します。ローカル コマンド許可を設定しない場合、特権レベルは無視され、設定したレベルに関係なく、レベル 15 にアクセスします。現在の特権レベルを表示するには、**show curpriv** コマンドを参照してください。

レベル 2 以上は、特権 EXEC モードを開始します。レベル 0 および 1 は、ユーザ EXEC モードを開始します。

例

次に、イネーブル パスワードを Pa$$w0rd に設定する例を示します。

```
hostname(config)# enable password Pa$$w0rd
```

次に、レベル 10 のイネーブル パスワードを Pa$$w0rd に設定する例を示します。

```
hostname(config)# enable password Pa$$w0rd10 level 10
```

次に、イネーブル パスワードを、別の FWSM からコピーした暗号化パスワードに設定する例を示します。

```
hostname(config)# enable password jMorNbK0514fadBh encrypted
```

関連コマンド

コマンド	説明
aaa authorization command	コマンド許可を設定します。
enable	特権 EXEC モードを開始します。
privilege	ローカル コマンド許可のコマンド特権レベルを設定します。
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 enable	イネーブル パスワードを暗号化形式で表示します。

endpoint

エンドポイントに HSI グループを関連付けるには、HSI グループ コンフィギュレーション モードで **endpoint** コマンドを使用します。エンドポイントを削除するには、このコマンドの **no** 形式を使用します。

endpoint *ip address interface*

no endpoint *ip address interface*

シンタックスの説明

ip address	エンドポイントの IP アドレスを指定します。
interface	エンドポイントに接続している FWSM 上のインターフェイスを指定します。

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
HSI 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
FWSM 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

endpoint コマンドを使用して、HSI グループに関連付けるエンドポイントを指定します。HSI グループにより、H.225 コール シグナリングに HSI が含まれている場合、FWSM で H.245 接続用のダイナミックなポート固有のピンホールをオープンできます。

各 HSI グループに、最大 10 のエンドポイントを設定できます。エンドポイントを設定する前に、グループ内に HSI を設定しておく必要があります。HSI グループを削除する場合には、事前にすべてのエンドポイントと HSI を削除する必要があります。

例

次に、H.225 マップを定義する例を示します。

```
hostname(config)# h225-map hmap
hostname(config-h225-map)# hsi-group 1
hostname(config-h225-map-hsi-grp)# hsi 10.10.15.11
hostname(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
hostname(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
hostname(config-h225-map-hsi-grp)# exit
hostname(config-h225-map-hsi-grp)# exit
```

関連コマンド

コマンド	説明
hsi	HSI グループに関連付ける HSI を定義します。
hsi-group	HSI グループを定義し、HSI グループ コンフィギュレーション モードをイネーブルにします。
h225-map	H.225 マップを定義し、H.225 マップ コンフィギュレーション モードを開始します。
inspect h323 h225	H.323 アプリケーション検査に H.225 マップを適用します。

enforcenextupdate

NextUpdate CRL フィールドの処理方法を指定するには、crl configure コンフィギュレーション モードで、**enforcenextupdate** コマンドを使用します。このコマンドを設定すると、CRL に有効な NextUpdate フィールドが必要になります。このコマンドを使用しない場合、FWSM は、NextUpdate フィールドが欠落または期限切れになっている CRL を許可します。

NextUpdate フィールドの期限切れまたは欠落を許可するには、このコマンドの **no** 形式を使用します。

enforcenextupdate

no enforcenextupdate

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

デフォルトの設定は、許可しない（オン）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 に対し、CRL が有効な NextUpdate フィールドを持つように設定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# enforcenextupdate
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
cache-time	キャッシュのリフレッシュ タイムを分単位で指定します。
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。

enrollment retry count

再試行カウントを指定するには、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、**enrollment retry count** コマンドを使用します。再試行カウントをデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。証明書を要求すると、FWSM は CA から証明書を受信するまで待機します。設定された再試行期限内に FWSM が証明書を受信しなかった場合、証明書の要求が再度送信されます。FWSM は、応答を受信するか、設定された再試行期限が終了するまで要求を再度繰り返します。

enrollment retry count *number*

no enrollment retry count

シンタックスの説明

number	エンロールメント要求を送信する最大試行回数を設定します。有効範囲は、0、1 ～ 100 回です。

デフォルト

デフォルトの *number* は、0（無制限）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

このコマンドは任意で、自動エンロールメントが設定されている場合にのみ適用されます。

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 内のエンロールメントの再試行回数を 20 回に設定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment retry count 20
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。
enrollment retry period	エンロールメント要求を再送信するまでの待機時間を分単位で指定します。

enrollment retry period

再試行期限を指定するには、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、**enrollment retry period** コマンドを使用します。再試行期限をデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。証明書を要求すると、FWSM は CA から証明書を受信するまで待機します。指定した再試行期限内に FWSM が証明書を受信しなかった場合、証明書の要求が再度送信されます。

enrollment retry period *minutes*

no enrollment retry period

シンタックスの説明

minutes	エンロールメント要求の送信を試みる間隔を分単位で設定します。有効範囲は、1 ～ 60 分です。

デフォルト

デフォルトの設定は、1 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
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

このコマンドは任意で、自動エンロールメントが設定されている場合にのみ適用されます。

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 内のエンロールメントの再試行期限を 10 分に設定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment retry period 10
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	すべてのエンロールメント パラメータを、システムのデフォルト値に戻します。
enrollment retry count	エンロールメント要求の再試行回数を定義します。

enrollment terminal

トラストポイントのエンロールメントのカットアンドペースト（手動エンロールメント）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、**enrollment terminal** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment terminal

no enrollment terminal

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

デフォルトの設定は、オフです。

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。

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 にカットアンドペースト方式の CA エンロールメントを指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment terminal
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。
enrollment retry count	エンロールメント要求を送信する再試行回数を設定します。
enrollment retry period	エンロールメント要求を再送信するまでの待機時間を分単位で指定します。
enrollment url	トラストポイントに自動エンロールメント（SCEP）を指定し、URL を設定します。

enrollment url

トラストポイントを登録するために自動エンロールメント（SCEP）を指定し、エンロールメント URL を設定するには、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 **enrollment url** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment url *url*

no enrollment url

シンタックスの説明

url	自動エンロールメント用の URL 名を指定します。最大文字長は 1 K です（事実上無制限です）。

デフォルト

デフォルトの設定は、オフです。

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。

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 に URL https://enrollsite での SCEP エンロールメントを指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url https://enrollsite
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。
enrollment retry count	エンロールメント要求を送信する再試行回数を設定します。
enrollment retry period	エンロールメント要求を再送信するまでの待機時間を分単位で指定します。
enrollment terminal	トラストポイントのカットアンドペースト方式のエンロールメントを指定します。

erase

ファイル システムを消去して、再フォーマットするには、特権 EXEC モードで、***erase*** コマンドを使用します。このコマンドは、非表示システム ファイルを含むすべてのファイルを上書きして、ファイル システムを消去し、ファイル システムを再インストールします。

erase [**flash:**]

シンタックスの説明

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。

注意　フラッシュ メモリを消去すると、フラッシュ メモリ内に保管されているライセンス情報も削除されます。フラッシュ メモリを消去する前に、ライセンス情報を保管してください。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

erase コマンドは、OxFF パターンを使用してフラッシュ メモリ上の全データを消去し、デバイスの空のファイル システム割り当てテーブルを再書き込みします。

（非表示システム ファイルを除く）すべての表示ファイルを削除するには、***erase*** コマンドの代わりに、***delete /recursive*** コマンドを使用します。

例

次に、ファイル システムを消去して、再フォーマットする例を示します。

```
hostname# erase flash:
```

関連コマンド

コマンド	説明
delete	非表示システム ファイルを除き、すべての表示ファイルを削除します。
format	（非表示システム ファイルを含む）すべてのファイルを消去し、ファイル システムをフォーマットします。

established

確立された接続に基づくポート上のリターン接続を許可するには、グローバル コンフィギュレーション モードで、**established** コマンドを使用します。**established** 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。

established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

no established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

シンタックスの説明

est_protocol	確立されている接続の検索に使用する IP プロトコル（UDP または TCP）を指定します。
dest_port	確立されている接続の検索に使用する宛先ポートを指定します。
permitfrom	（任意）指定ポートからのリターン プロトコル接続を許可します。
permitto	（任意）指定ポート宛のリターン プロトコル接続を許可します。
port [*-port*]	（任意）リターン接続の宛先ポート（UDP または TCP）を指定します。
protocol	（任意）リターン接続が使用する IP プロトコル（UDP または TCP）。
source_port	（任意）確立されている接続の検索に使用する送信元ポートを指定します。

デフォルト

デフォルトの設定は次のとおりです。

- *dest_port* — 0（ワイルドカード）
- *source_port* — 0（ワイルドカード）

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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。
3.1(1)	CLI（コマンドライン インターフェイス）から、***to*** および ***from*** のキーワードが削除されました。代わりに、***permitto*** および ***permitfrom*** のキーワードを使用します。

使用上のガイドライン

established コマンドは、FWSM を経由した発信接続のリターン アクセスを許可します。このコマンドは、ネットワークから発信され、FWSM によって保護される元の接続、および外部ホスト上の同じ 2 つのデバイス間の着信リターン接続上で動作します。**established** コマンドを使用すると、接続の検索に使用する宛先ポートを指定できます。これにより、コマンドを細かく制御できるため、宛先ポートが判明していて送信元ポートが不明なプロトコルをサポートできます。**permitto** および **permitfrom** キーワードは、リターン着信接続を定義します。

注意　**established** コマンドには、必ず **permitto** キーワードおよび **permitfrom** キーワードを指定することを推奨します。これらのキーワードを使用せずに **established** コマンドを使用すると、セキュリティ上のリスクが生じます。これは、外部システムに接続を行った場合、外部システムから関連する内部ホストに無制限にアクセスできるためです。この場合、内部システムが攻撃を受ける危険があります。

例

established コマンドを正しく使用しないとセキュリティ違反が発生する可能性があることを示す例を以下に示します。

次の例では、内部システムがポート 4000 上で外部ホストに TCP 接続した場合、外部ホストは、任意のプロトコルを使用し、任意のポート上にリターン アクセスする可能性があります。

```
hostname(config)# established tcp 4000 0
```

プロトコルに使用ポートが指定されていない場合、送信元ポートおよび宛先ポートに **0** を指定できます。ワイルドカード ポート（0）は、必要な場合のみ使用してください。

```
hostname(config)# established tcp 0 0
```

（注）　**established** コマンドを正しく動作させるには、**permitto** キーワードで指定したポート上で、クライアントが待機している必要があります。

established コマンドは、**nat 0** コマンドと併用できます（**global** コマンドがない場合）。

（注）　**established** コマンドは、PAT とは併用できません。

FWSM は、**established** コマンドの使用により、XDMCP をサポートします。

注意　FWSM を通じて XWindows システムを使用すると、セキュリティ上のリスクが生じる場合があります。

XDMCP はデフォルトではオンですが、次のように **established** コマンドが入力されるまで、セッションは完了しません。

```
hostname(config)# established tcp 6000 0 permitto tcp 6000 permitfrom tcp 1024-65535
```

established コマンドを使用すると、内部の XDMCP（UNIX または ReflectionX）搭載ホストから、外部の XDMCP 搭載 XWindows サーバにアクセスできます。UDP/177 ベースの XDMCP が TCP ベースの XWindows セッションをネゴシエートし、以降の TCP リターン接続が許可されます。リターン トラフィックの送信元ポートは不明なので、*source_port* フィールドには 0（ワイルドカード）を指定します。*dest_port* は、6000 ＋ *n* である必要があります。*n* はローカル ディスプレイ番号です。この値を変更するには、次の UNIX コマンドを使用します。

```
hostname(config)# setenv DISPLAY hostname:displaynumber.screennumber
```

established コマンドが必要な理由は、（ユーザとの対話に基づいて）多数の TCP 接続が生成されますが、これらの接続に使用される送信元ポートが不明であるためです。宛先ポートだけがスタティックになります。FWSM は、XDMCP フィックスアップを透過的に行います。設定は不要ですが、TCP セッションに対応するには **established** コマンドが必要です。

次に、プロトコル A を使用して 2 つのホスト間、SRC ポート C からポート B までを接続する例を示します。FWSM およびプロトコル D を経由したリターン接続を許可するには、送信元ポートがポート F に対応し、宛先ポートがポート E に対応している必要があります（プロトコル D は、プロトコル A と異なっていてもかまいません）。

```
hostname(config)# established A B C permitto D E permitfrom D F
```

次に、TCP 宛先ポート 6060 および任意の送信元ポートを使用し、内部ホストから外部ホストに接続を開始する例を示します。FWSM は、TCP 宛先ポート 6061 および任意の TCP 送信元ポートを経由するホスト間のリターン トラフィックを許可します。

```
hostname(config)# established tcp 6060 0 permitto tcp 6061 permitfrom tcp 0
```

次に、UDP 宛先ポート 6060 および任意の送信元ポートを使用し、内部ホストから外部ホストに接続を開始する例を示します。FWSM は、TCP 宛先ポート 6061 と TCP 送信元ポート 1024 ～ 65535 を経由するホスト間のリターン トラフィックを許可します。

```
hostname(config)# established udp 6060 0 permitto tcp 6061 permitfrom tcp 1024-65535
```

次に、ローカル ホストから外部ホストに対して、ポート 9999 で TCP 接続を開始する例を示します。この例では、外部ホストのポート 4242 から、ローカル ホストのポート 5454 に戻るパケットが許可されます。

```
hostname(config)# established tcp 9999 permitto tcp 5454 permitfrom tcp 4242
```

関連コマンド

コマンド	説明
clear configure established	確立されたコマンドをすべて削除します。
show running-config established	確立された接続に基づいて許可された着信接続を表示します。

exit

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

exit

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 / ユーザ EXEC モードで **exit** コマンドを入力すると、FWSM からログアウトします。特権 EXEC モードからユーザ EXEC モードに戻るには、**disable** コマンドを使用します。

例

次に、**exit** 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)# exit
hostname# exit

Logoff
```

次に、**exit** 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、次に、**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)# exit
hostname# disable
hostname>
```

関連コマンド

コマンド	説明
quit	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。

failover

フェールオーバー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、**failover** コマンドを使用します。フェールオーバー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。

failover

no failover

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。
3.1(1)	このコマンドは、コンフィギュレーションのフェールオーバーをイネーブルまたはディセーブルにするように制限されました（**failover active** コマンドを参照してください）。

使用上のガイドライン

フェールオーバー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。

注意　フェールオーバーの間すべての情報が送信されます。フェールオーバー鍵を使用して通信のセキュリティを確保していない場合、ステートフル フェールオーバー リンクがクリア テキストで送信されます。FWSM に設定されているユーザ名、パスワード、および事前共有鍵がクリア テキストで送信されるので、セキュリティ上に大きなリスクが生じます。フェールオーバー鍵を使用して、フェールオーバー通信のセキュリティを確保することを推奨します。

例

次に、フェールオーバーをディセーブルにする例を示します。

```
hostname(config)# no failover
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure failover	実行コンフィギュレーションから **failover** コマンドを消去し、フェールオーバーをデフォルトの設定に戻します。
failover active	スタンバイ装置をアクティブに切り換えます。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover active

スタンバイ FWSM またはフェールオーバー グループをアクティブ ステートに切り換えるには、特権 EXEC モードで、**failover active** コマンドを使用します。アクティブ FWSM またはフェールオーバー グループをスタンバイに切り換えるには、このコマンドの **no** 形式を使用します。

failover active [***group*** *group_id*]

no failover active [***group*** *group_id*]

シンタックスの説明

group *group_id*	(任意)アクティブに切り換えるフェールオーバー グループを指定します。

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)	このコマンドが追加されました。

使用上のガイドライン

スタンバイ装置からフェールオーバーの切り換えを開始するには、**failover active** コマンドを使用します。アクティブ装置からフェールオーバーの切り換えを開始するには、**no failover active** コマンドを使用します。この機能を使用して、障害が発生した装置をサービス状態に復帰させたり、アクティブ装置をメンテナンスのために強制的にオフラインにすることができます。ステートフル フェールオーバーを使用していない場合、すべてのアクティブ接続がドロップされるので、クライアントはフェールオーバーの発生後、接続を再確立する必要があります。

フェールオーバー グループの切り換えができるのは、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。フェールオーバー グループを指定せずに、アクティブ / アクティブ フェールオーバー装置上で **failover active** コマンドを入力すると、装置のすべてのグループがアクティブになります。

例

次に、スタンバイ グループ 1 をアクティブに切り換える例を示します。

```
hostname# failover active group 1
```

関連コマンド

コマンド	説明
failover reset	FWSM を、障害ステートからスタンバイに移行します。

failover group

アクティブ / アクティブ フェールオーバー グループを設定するには、グローバル コンフィギュレーション モードで、**failover group** コマンドを使用します。フェールオーバー グループを削除するには、このコマンドの **no** 形式を使用します。

failover group *num*

no failover group *num*

シンタックスの説明

num	フェールオーバー グループ番号です。有効値は、1 または 2 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

最大 2 つのフェールオーバー グループを定義できます。**failover group** コマンドを追加できるのは、マルチ コンテキスト モード用に設定されたデバイスのシステム コンテキストに対してだけです。フェールオーバー グループを作成または削除するには、フェールオーバーをディセーブルにする必要があります。

このコマンドを入力すると、フェールオーバー グループ コマンド モードになります。**primary**、**secondary**、**preempt**、**replication http**、**interface-policy**、および **polltime interface** の各コマンドが、フェールオーバー グループ コンフィギュレーション モードで使用できます。グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。

（注）　**failover polltime interface**、**failover interface-policy**、および **failover replication http** コマンドは、アクティブ / アクティブ フェールオーバー 設定には影響しません。これらは、フェールオーバー グループ コンフィギュレーション モードの **polltime interface**、**interface-policy**、および **replication http** の各コマンドにより上書きされます。

フェールオーバー グループを削除する場合には、フェールオーバー グループ 1 を最後に削除する必要があります。フェールオーバー グループ 1 には、常に、管理コンテキストが含まれています。フェールオーバー グループに割り当てられていないコンテキストはすべて、デフォルトでフェールオーバー グループ 1 に含まれます。コンテキストが明示的に割り当てられているフェールオーバー グループは、削除できません。

例

次に、2 つのフェールオーバー グループに使用可能なコンフィギュレーション例の一部を示します。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# 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
asr-group	非対称ルーティング インターフェイス グループ ID を指定します。
interface-policy	モニタリングによりインターフェイス障害が検出された場合のフェールオーバー ポリシーを指定します。
join-failover-group	コンテキストをフェールオーバー グループに割り当てます。
polltime interface	モニタ対象インターフェイスに送信する hello メッセージの間隔を指定します。
preempt	リブート後、プライオリティの高い装置がアクティブ装置になるように指定します。
primary	プライマリ装置に、フェールオーバー グループでの高いプライオリティを指定します。
replication http	選択したフェールオーバー グループの HTTP セッション複製を指定します。
secondary	セカンダリ装置に、フェールオーバー グループでの高いプライオリティを指定します。

failover interface ip

フェールオーバー インターフェイスおよびステートフル フェールオーバー インターフェイスに IP アドレスおよびマスクを指定するには、グローバル コンフィギュレーション モードで、**failover interface ip** コマンドを使用します。IP 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。

failover interface ip *if_name ip_address mask* ***standby*** *ip_address*

no failover interface ip *if_name ip_address mask* ***standby*** *ip_address*

シンタックスの説明

if_name	フェールオーバーまたはステートフル フェールオーバー インターフェイスのインターフェイス名を指定します。
ip_address mask	プライマリ モジュールのフェールオーバーまたはステートフル フェールオーバー インターフェイスの IP アドレスおよびマスクを指定します。
standby *ip_address*	プライマリ モジュールと通信するためにスタンバイ モジュールが使用する IP アドレスを指定します。

デフォルト

デフォルトの設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

フェールオーバーおよびステートフル フェールオーバー インターフェイスは、FWSM がトランスペアレント ファイアウォール モードで稼働し、システムに対してグローバルであっても、レイヤ 3 で動作します。

マルチ コンテキスト モードでは、（**monitor-interface** コマンドを除き）システム コンテキストにフェールオーバーを設定します。

FWSM を LAN フェールオーバー用にブートストラップする場合には、このコマンドがコンフィギュレーションに含まれている必要があります。

例

次に、フェールオーバー インターフェイスに IP アドレスおよびマスクを指定する例を示します。

```
hostname(config)# failover interface ip lanlink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

関連コマンド

コマンド	説明
clear configure failover	実行コンフィギュレーションから **failover** コマンドを消去し、フェールオーバーをデフォルトの設定に戻します。
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。
failover link	ステートフル フェールオーバーに使用するインターフェイスを指定します。
monitor-interface	指定したインターフェイスの状態をモニタします。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover interface-policy

モニタによりインターフェイス障害が検出された場合のフェールオーバー ポリシーを指定するには、グローバル コンフィギュレーション モードで、**failover interface-policy** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

failover interface-policy *num*[*%*]

no failover interface-policy *num*[*%*]

シンタックスの説明

num	パーセンテージで指定する場合、1 ～ 100 を指定します。数値で指定する場合は、1 からインターフェイスの最大数を指定します。
%	（任意）数値 *num* が監視対象インターフェイスの割合であることを指定します。

デフォルト

デフォルトのインターフェイス ポリシーは 50% です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

引数 *num* とオプション キーワード **%** の間にスペースはありません。

障害が発生したインターフェイス数が設定したポリシーに適合した場合、その他の FWSM が正常に動作していても、FWSM は障害状態であるとみなし、フェールオーバーが実行される場合があります（アクティブ FWSM に障害が発生した場合）。**monitor-interface** コマンドでモニタ対象として指定されたインターフェイスだけがポリシーのカウントに含まれます。

（注）　このコマンドは、アクティブ / スタンバイ フェールオーバーだけに適用されます。アクティブ / アクティブ フェールオーバーの場合には、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、**interface-policy** コマンドを使用し、各フェールオーバー グループにインターフェイス ポリシーを設定します。

例

次に、フェールオーバー ポリシーを指定する 2 種類の例を示します。

```
hostname(config)# failover interface-policy 20%

hostname(config)# failover interface-policy 5
```

関連コマンド

コマンド	説明
failover polltime	装置およびインターフェイスのポーリング間隔を指定します。
failover reset	障害が発生した装置を、障害のないステートに戻します。
monitor-interface	フェールオーバーのためにモニタするインターフェイスを指定します。
show failover	装置のフェールオーバー ステートに関する情報を表示します。

failover key

フェールオーバー ペアの装置間で暗号化および認証された通信を行うための鍵を指定するには、グローバル コンフィギュレーション モードで、**failover key** コマンドを使用します。共有秘密鍵を削除するには、このコマンドの **no** 形式を使用します。

failover key {*secret* | ***hex*** *key*}

no failover key

シンタックスの説明

hex *key*	16 進数値の暗号鍵を指定します。鍵には、32 文字の 16 進数値（0 ～ 9、a ～ f）を指定する必要があります。
secret	英数字の共有シークレットを指定します。シークレットは、1 ～ 63 文字で指定できます。有効値は、数字、文字、または句読点の任意の組み合わせです。共有シークレットは、暗号鍵を生成するために使用されます。

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
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

装置間のフェールオーバー通信を暗号化および認証するには、両装置に共有シークレットまたは 16 進数値の鍵を設定する必要があります。フェールオーバー鍵を指定しない場合、フェールオーバー通信はクリア テキストで送信されます。

注意　フェールオーバーの間すべての情報が送信されます。フェールオーバー鍵を使用して通信のセキュリティを確保していない場合、ステートフル フェールオーバー リンクがクリア テキストで送信されます。FWSM に設定されているユーザ名、パスワード、および事前共有鍵がクリア テキストで送信されるので、セキュリティ上に大きなリスクが生じます。フェールオーバー鍵を使用して、フェールオーバー通信のセキュリティを確保することを推奨します。

例

次に、フェールオーバー ペアの装置間で安全なフェールオーバー通信を行うために、共有シークレットを指定する例を示します。

```
hostname(config)# failover key abcdefg
```

次に、フェールオーバー ペアの 2 つの装置間で安全なフェールオーバー通信を行うために、16 進数値の鍵を指定する例を示します。

```
hostname(config)# failover key hex 6a1ed228381cf5c68557cb0c32e614dc
```

関連コマンド

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

failover lan interface

フェールオーバーの通信に使用するインターフェイス名および VLAN（仮想 LAN）を指定するには、グローバル コンフィギュレーション モードで、**failover lan interface** コマンドを使用します。フェールオーバー インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

failover lan interface *if_name* ***vlan*** *vlan*

no failover lan interface *if_name* ***vlan*** *vlan*

シンタックスの説明

if_name	フェールオーバー専用の FWSM インターフェイスの名前を指定します。
vlan *vlan*	VLAN 番号を指定します。

デフォルト

デフォルトの設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

アクティブおよびスタンバイのモジュールは、各モジュールの運用ステータスを判別するために、このリンク上で継続的に通信します。フェールオーバー リンク上の通信には、モジュールのステート（アクティブまたはスタンバイ）、hello メッセージ（その他のすべてのインターフェイスにも送信されます）、および 2 つのモジュール間のコンフィギュレーションの同期化が含まれます。

フェールオーバーには、フェールオーバー トラフィックを転送するための専用インターフェイスが必要ですが、ステートフル フェールオーバー リンクには LAN フェールオーバー インターフェイスを使用することもできます。LAN フェールオーバーとステートフル フェールオーバーの両方に同じインターフェイスを使用する場合には、インターフェイスに、フェールオーバーおよびステートフル フェールオーバーの両方のトラフィックを処理できるだけの十分な容量が必要です。

フェールオーバー リンクには、専用 VLAN を使用します。フェールオーバー リンクの VLAN を他の VLAN と共有すると、トラフィックが中断されたり、ping 障害および ARP 障害の原因になります。

モジュール上の任意の未使用インターフェイスを、フェールオーバー インターフェイスとして使用できます。現在、名前が設定されているインターフェイスを指定することはできません。フェールオーバー インターフェイスは、通常のネットワーキング インターフェイスとしては設定されず、フェールオーバー通信専用として存在します。このインターフェイスは、フェールオーバー リンク用（および任意にステート リンク用）としてのみ使用してください。

マルチ コンテキスト モードを実行しているシステムでは、フェールオーバー リンクはシステム コンテキストに常駐します。システム コンテキストに設定できるインターフェイスは、このインターフェイスとステート リンク（使用する場合）だけです。その他のインターフェイスはすべて、セキュリティ コンテキストから設定し、セキュリティ コンテキストに割り当てられます。

（注）　フェールオーバー リンクの IP アドレスおよび MAC（メディア アクセス制御）アドレスは、フェールオーバーが発生しても変わりません。

このコマンドの **no** 形式を使用すると、フェールオーバー インターフェイスの IP アドレスもクリアされます。

フェールオーバー用に FWSM をブートストラップする場合には、このコマンドがコンフィギュレーションに含まれている必要があります。

例

次に、フェールオーバー LAN インターフェイスを設定する例を示します。

```
hostname(config)# failover lan interface folink vlan 101
```

関連コマンド

コマンド	説明
failover lan unit	LAN ベース フェールオーバーのプライマリ装置またはセカンダリ装置を指定します。
failover link	ステートフル フェールオーバー インターフェイスを指定します。

failover lan unit

FWSM を、フェールオーバー コンフィギュレーションのプライマリ装置またはセカンダリ装置として設定するには、グローバル コンフィギュレーション モードで、**failover lan unit** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

failover lan unit {***primary*** | ***secondary***}

no failover lan unit {***primary*** | ***secondary***}

シンタックスの説明

primary	FWSM を、プライマリ装置として指定します。
secondary	セキュリティ アプライアンスを、セカンダリ装置として指定します。

デフォルト

デフォルトは、セカンダリです。

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
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

アクティブ / スタンバイ フェールオーバーの場合、フェールオーバー装置をプライマリおよびセカンダリに指定すると、ブート時にアクティブになる装置が決まります。次の状況では、ブート時にプライマリ装置がアクティブ装置になります。

- 初回のフェールオーバー ポーリング チェックの実行中に、プライマリおよびセカンダリの両装置がブート シーケンスを完了した場合
- プライマリ装置が、セカンダリ装置よりも先に起動した場合

プライマリ装置の起動時に、セカンダリ装置がすでにアクティブ装置になっていた場合には、プライマリ装置はアクティブにならず、スタンバイ装置になります。この場合、プライマリ装置を強制的にアクティブ ステータスに戻すには、スタンバイ（アクティブ）装置上で **no failover active** コマンドを入力する必要があります。

アクティブ / アクティブ フェールオーバーの場合には、各フェールオーバー グループにプライマリ装置またはセカンダリ装置の優先順位を指定します。この優先順位により、起動時に両方の装置が（フェールオーバー ポーリング実行中に）同時に起動した場合、フェールオーバー グループ内のフェールオーバー ペアのどの装置がアクティブになるかが判別されます。

フェールオーバー用に FWSM をブートストラップする場合には、このコマンドがコンフィギュレーションに含まれている必要があります。

例

次に、FWSM をプライマリ装置として設定する例を示します。

```
hostname(config)# failover lan unit primary
```

関連コマンド

コマンド	説明
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。

failover link

ステートフル フェールオーバー インターフェイスおよび VLAN（仮想 LAN）を指定するには、グローバル コンフィギュレーション モードで、**failover link** コマンドを使用します。ステートフル フェールオーバー インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

failover link *if_name* [***vlan*** *vlan*]

no failover link

シンタックスの説明

if_name	ステートフル フェールオーバー専用の FWSM インターフェイスの名前を指定します。
vlan *vlan*	（任意）ステートフル アップデート情報に使用する VLAN を設定します。ステートフル フェールオーバー インターフェイスが、フェールオーバー通信に割り当てられたインターフェイスを共有する場合には、この引数は不要です。

デフォルト

デフォルトの設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

フェールオーバー通信インターフェイスを共有しない場合には、物理インターフェイスまたは論理インターフェイスの引数が必要です。

failover link コマンドは、ステートフル フェールオーバーをイネーブルにします。ステートフル フェールオーバーをディセーブルにして、ステートフル フェールオーバー インターフェイスの IP アドレス設定をクリアするには、**no failover link** コマンドを使用します。

ステートフル フェールオーバーを使用するには、すべてのステート情報を転送するステート リンクを設定する必要があります。ステート リンクは、2 つの方法で設定できます。ステート リンク用の専用インターフェイスを使用するか、またはフェールオーバー リンクを使用します。

注意　ステートフル フェールオーバー リンクと、通常のファイアウォール インターフェイスを共有することはできません。旧バージョンのソフトウェアには、この制約は適用されていませんでした。旧バージョンの FWSM ソフトウェアからアップグレードする場合、ステート リンクと通常のファイアウォール インターフェイスとの共有が設定されていると、アップグレードの実行時にファイアウォール インターフェイスに関する設定が失われます。設定が失われないようにするには、アップグレードを実行する前に、ステート リンクを別の物理インターフェイスに移動するか、またはステートフル フェールオーバーをディセーブルにしてください。

ステート トラフィックは、大容量になることがあります。フェールオーバー リンクをステート リンクとして使用したときにパフォーマンスが低下するようであれば、ステート トラフィック用に個別の専用リンクを設定してください。

マルチ コンテキスト モードでは、ステート リンクはシステム コンテキストに常駐します。システム コンテキストに常駐するインターフェイスは、このインターフェイスとフェールオーバー インターフェイスだけです。その他のインターフェイスはすべて、セキュリティ コンテキストから設定し、セキュリティ コンテキストに割り当てられます。

（注）　ステート リンクの IP アドレスおよび MAC（メディア アクセス制御）アドレスは、フェールオーバーが発生しても変わりません。

注意　フェールオーバーの間すべての情報が送信されます。フェールオーバー鍵を使用して通信のセキュリティを確保していない場合、ステートフル フェールオーバー リンクがクリア テキストで送信されます。FWSM に設定されているユーザ名、パスワード、および事前共有鍵がクリア テキストで送信されるので、セキュリティ上に大きなリスクが生じます。フェールオーバー鍵を使用して、フェールオーバー通信のセキュリティを確保することを推奨します。

例

次に、ステートフル フェールオーバー インターフェイスを指定する例を示します。

```
hostname(config)# failover link stateful_if vlan 101
```

関連コマンド

コマンド	説明
failover interface ip	**failover** コマンドおよびステートフル フェールオーバー インターフェイスの IP アドレスを設定します。
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。
mtu	インターフェイスに MTU を指定します。

failover polltime

フェールオーバー装置、インターフェイスのポーリング間隔、および装置のホールド タイムを指定するには、グローバル コンフィギュレーション モードで、**failover polltime** コマンドを使用します。デフォルトのポーリング間隔に戻すには、このコマンドの **no** 形式を使用します。

failover polltime [***unit***] [***msec***] *time* [***holdtime*** *time*]

failover polltime ***interface*** *time*

no failover polltime [***unit***] [***msec***] *time* [***holdtime*** *time*]

no failover polltime interface *time*

シンタックスの説明

holdtime *time*	（任意）ピア装置に障害が宣言されたあと、装置がフェールオーバー リンク上で hello メッセージを受信する時間を設定します。有効値は 3 ～ 45 秒です。
interface *time*	インターフェイス モニタリングのポーリング間隔を指定します。有効値は 3 ～ 15 秒です。
msec	（任意）メッセージの送信間隔をミリ秒単位で指定します。有効値の範囲は、500 ～ 999 ミリ秒です。
time	Hello メッセージの時間間隔有効値は 1 ～ 15 秒、または ***msec*** キーワードを指定した場合、500 ～ 999 ミリ秒です。
unit	（任意）フェールオーバー リンク上で送信する hello メッセージの頻度を設定します。

デフォルト

デフォルトの設定は次のとおりです。

- **unit** のポーリング *time* は、1 秒です。
- ポーリング時間を指定しており、なおかつ ***holdtime*** キーワードで保留時間を指定していない場合、***holdtime*** *time* はポーリング時間（最小値は 3 秒）の 3 倍になります。***holdtime*** キーワードで保留時間を指定する場合は、ポーリング *time* の 3 倍以上にする必要があります。***clear configure failover*** コマンドを入力した場合、保留時間は 15 秒です。
- **interface** のポーリング *time* 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
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。
2.2(1)	このコマンドが、**failover poll** コマンドから、**failover polltime** コマンドに変更され、***unit***、***interface***、および ***holdtime*** キーワードが追加されました。

使用上のガイドライン

holdtime には、装置のポーリング間隔の 3 倍未満の値を指定することはできません。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。

unit または ***interface*** キーワードを指定しない場合、装置のポーリング間隔が設定されます。

コンフィギュレーションには、**failover polltime unit** コマンドおよび **failover polltime interface** コマンドの両方を含めることができます。

（注） **failover polltime interface** コマンドは、アクティブ / スタンバイ フェールオーバーだけに適用されます。アクティブ / アクティブ フェールオーバーの場合には、**failover polltime interface** コマンドの代わりに、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。

ホールド タイム中にフェールオーバー通信インターフェイス上で hello パケットが受信されなかった場合、ピア装置は障害状態であるとみなされ、スタンバイ装置がアクティブに切り替わります。*interface* の hello パケットが 5 回連続して受信されなかった場合、インターフェイスのテストが実行されます。

（注） フェールオーバー設定で、CTIQBE トラフィックが FWSM を通過する場合には、セキュリティ アプライアンスのフェールオーバー ホールド タイムを 30 秒未満に設定すべきです。CTIQBE のキープアライブのタイムアウトは 30 秒なので、フェールオーバー状況でフェールオーバーが実行される前に、タイムアウトになることがあります。CTIQBE がタイムアウトになると、Cisco CallManager への Cisco IP SoftPhone 接続がドロップされるので、IP SoftPhone クライアントは CallManager に再登録する必要があります。

例

次に、装置のポーリング間隔を 3 秒に設定する例を示します。

```
hostname(config)# failover polltime 3
```

関連コマンド

コマンド	説明
polltime interface	アクティブ / アクティブ フェールオーバー コンフィギュレーション用のインターフェイスのポーリング間隔を指定します。
show failover	フェールオーバーのコンフィギュレーション情報を表示します。

failover reload-standby

スタンバイ装置を強制的にリブートするには、特権 EXEC モードで、**failover reload-standby** コマンドを使用します。

failover reload-standby

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、フェールオーバー装置の同期化が実行されない場合に使用します。スタンバイ装置が再起動し、ブート完了後、アクティブ装置と再び同期化を実行します。

例

次に、アクティブ装置上で **failover reload-standby** コマンドを使用し、スタンバイ装置を強制的にリブートする例を示します。

```
hostname# failover reload-standby
```

関連コマンド

コマンド	説明
write standby	スタンバイ装置のメモリに実行コンフィギュレーションを書き込みます。

failover replication http

HTTP（ポート 80）接続の複製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、**failover 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。

failover replication http

no failover 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
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

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。**failover replication http** コマンドは、ステートフル フェールオーバー環境で HTTP セッションをステートフルに複製できますが、システムのパフォーマンスに影響することがあります。

アクティブ / アクティブ フェールオーバー設定では、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、フェールオーバー グループ単位で HTTP セッションの複製を制御します。

例

次に、HTTP 接続の複製をイネーブルにする例を示します。

```
hostname(config)# failover replication http
```

関連コマンド

コマンド	説明
replication http	特定のフェールオーバー グループの HTTP セッションの複製をイネーブルにします。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover reset

障害が発生した FWSM を、障害のないステートに戻すには、特権 EXEC モードで、**failover reset** コマンドを使用します。

failover reset [***group*** *group_id*]

シンタックスの説明

group	（任意）フェールオーバー グループを指定します。
group_id	フェールオーバー グループ番号です。

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
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。
3.1(1)	このコマンドが、任意でフェールオーバー グループ ID を指定できるように変更されました。

使用上のガイドライン

failover reset コマンドにより、障害が発生した装置またはグループを、障害のないステートに戻すことができます。**failover reset** コマンドは、どちらの装置からでも入力できますが、常にアクティブ装置上で入力することを推奨します。アクティブ装置で **failover reset** コマンドを入力すると、スタンバイ装置に障害が発生しません。

装置のフェールオーバー ステータスは、**show failover** コマンドまたは **show failover state** コマンドで表示できます。

このコマンドの **no** 形式はありません。

アクティブ / アクティブ フェールオーバーでは、**failover reset** コマンドを入力すると、装置全体がリセットされます。このコマンドにフェールオーバー グループを指定すると、指定したグループだけがリセットされます。

例

次に、障害が発生した装置を、障害のないステートに戻す例を示します。

```
hostname# failover reset
```

関連コマンド

コマンド	説明
failover interface-policy	モニタリングによりインターフェイス障害が検出された場合のフェールオーバー ポリシーを指定します。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。

failover suspend-config-sync

フェールオーバー コンフィギュレーションの同期化を一時停止するには、グローバル コンフィギュレーション モードで、**failover suspend-config-sync** コマンドを使用します。フェールオーバー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。

failover suspend-config-sync

no failover suspend-config-sync

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
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更
2.3(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

このコマンドを実行できるのは、アクティブ装置上だけです。このコマンドを実行すると、インターフェイスのモニタリングおよび論理アップデートがディセーブルになります。

例

次に、フェールオーバー コンフィギュレーションの同期化を一時停止する例を示します。

```
hostname(config)# failover suspend-config-sync
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure failover	実行コンフィギュレーションから **failover** コマンドを削除します。
failover	フェールオーバーをイネーブルにします。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

filter activex

FWSM を通過する HTTP トラフィックの ActiveX オブジェクトを削除するには、グローバル コンフィギュレーション モードで、**filter activex** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter activex {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

no filter activex {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

シンタックスの説明

except	指定した **filter** 条件に対して、例外を作成します。
foreign_ip	アクセス対象のうち、セキュリティ レベルが最も低いインターフェイスの IP アドレスを指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスクを指定します。必ず、特定のマスク値を指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
local_ip	アクセス対象のうち、セキュリティ レベルが最も高いインターフェイスの IP アドレスを指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
local_mask	*local_ip* のネットワーク マスクを指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
port	フィルタリングを適用する TCP ポートを指定します。通常、ポート 21 ですが、他の値も使用できます。ポート 21 には、**http** または **url** を使用できます。許可される値の範囲は、0 ～ 65535 です。予約済みポートおよびその値のリストは、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください。
port **-***port*	（任意）ポート範囲を指定します。

デフォルト

このコマンドは、デフォルトではディセーブルです。

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

ActiveX オブジェクトには、保護されたネットワーク上のホストおよびサーバの攻撃を目的としたコードが含まれていることがあるので、セキュリティ上のリスクになります。**filter activex** コマンドを使用すると、ActiveX オブジェクトをディセーブルにできます。

ActiveX コントロール（旧 OLE コントロールまたは OCX コントロール）は、Web ページまたは他のアプリケーションに挿入できるコンポーネントです。これらのコントロールには、カスタム フォーム、カレンダー、または情報を収集または表示するためのサードパーティの拡張形式が含まれています。ActiveX には、ワークステーション障害およびネットワーク セキュリティ上の問題の原因になる、またはサーバ攻撃に使用されるなど、技術的に多数の潜在的な問題があります。

filter activex コマンドは、HTML Web ページ内の HTML の <object> コマンドをコメント化して除外することにより、これらをブロックします。HTML ファイルの ActiveX フィルタリングは、<APPLET>、</APPLET>、<OBJECT CLASSID> 、および </OBJECT> タグを選択してコメントに置換することにより実行されます。トップレベルのタグをコメントに変換することで、ネストされたタグのフィルタリングもサポートされます。

注意　<object> タグは、Java アプレット、イメージ ファイル、およびマルチメディア オブジェクトにも使用されますが、これらもこのコマンドによりブロックされます。

<OBJECT> または </OBJECT> HTML タグが複数のネットワーク パケット上に分割されている場合、またはタグ内のコードが MTU（最大伝送ユニット）のバイト数を超えている場合には、FWSM でタグをブロックできません。

ActiveX のブロックは、ユーザが ***alias*** コマンドを使用して参照する IP アドレスにアクセスする場合には、実行されません。

例

次に、すべての発信接続上で、ActiveX オブジェクトをブロックする例を示します。

```
hostname(config)# filter activex 80 0 0 0 0
```

このコマンドにより、ポート 80 上のすべてのローカル ホストからの Web トラフィック、およびすべての外部ホストへの接続に対して、ActiveX オブジェクトがブロックされます。

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに転送します。
filter java	FWSM を通過する HTTP トラフィックから Java アプレットを削除します。
show running-config filter	フィルタリング設定を表示します。
url-server	**filter** コマンドで使用する N2H2 または Websense サーバを指定します。

filter ftp

Websense サーバでフィルタリングする FTP（ファイル転送プロトコル）トラフィックを指定するには、グローバル コンフィギュレーション モードで、**filter ftp** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

（注）　**filter ftp** コマンドをイネーブルにすると、FTP インスペクションもイネーブルになります（FTP インスペクションがどのポリシー マップに設定されていない場合も同様）。これにより、FTP のアクティブ接続が許可されます。アクティブ接続を許可しない場合は、FTP サーバがパッシブ FTP 接続のみを受け入れるように設定してください。

filter ftp {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*] [**allow**] [**interact-block**]

no filter ftp {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*] [**allow**] [**interact-block**]

シンタックスの説明

port	フィルタリングを適用する TCP ポートを指定します。通常、ポート 21 ですが、他の値も使用できます。ポート 80 の場合、**ftp** を使用できます。
port **-***port*	（任意）ポート範囲を指定します。
except	指定した **filter** 条件に対して、例外を作成します。
local_ip	アクセス対象のうち、セキュリティ レベルが最も高いインターフェイスの IP アドレスを指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
local_mask	*local_ip* のネットワーク マスクを指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
foreign_ip	アクセス対象のうち、セキュリティ レベルが最も低いインターフェイスの IP アドレスを指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスクを指定します。必ず、特定のマスク値を指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
allow	（任意）サーバが使用不可の場合、フィルタリングを適用せずに、FWSM からの発信接続を許可します。このオプションを指定しない場合、N2H2 または Websense サーバがオフラインになると、FWSM は N2H2 または Websense サーバがオンラインに戻るまで、ポート 80（Web）の発信トラフィックを停止します。
interact-block	（任意）ユーザが、対話型 FTP プログラムを使用して FTP サーバに接続するのを防止します。

デフォルト

このコマンドは、デフォルトではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

filter ftp コマンドでは、Websense サーバによってフィルタリングされる FTP トラフィックを指定します。FTP フィルタリングは、N2H2 サーバ上ではサポートされません。

この機能をイネーブルにすると、ユーザがサーバに FTP GET 要求を発行した場合、FWSM はその要求を FTP サーバおよび Websense サーバの両方に同時に送信します。Websense サーバにより接続が許可されると、FWSM は、正常な FTP リターン コードを変更せずにユーザに戻します。正常なリターン コードとは、[250: CWD command successful] などです。

Websense サーバが接続を拒否した場合、FWSM は、接続が拒否されたことを示すために FTP リターン コードを変更します。たとえば、FWSM は、コード 250 を、[550 Requested file is prohibited by URL filtering policy] に変更します。Websense がフィルタリングするのは、FTP GET コマンドだけです。PUT コマンドはフィルタリングしません。

完全なディレクトリ パスが提供されない対話型の FTP セッションを防止するには、**interactive-block** オプションを使用します。対話型 FTP クライアントでは、完全パスを指定せずにディレクトリを変更できます。たとえば、**cd /public/files** の代わりに **cd ./files** を入力できます。これらのコマンドが使用される前に、URL フィルタリング サーバを指定し、イネーブルにする必要があります。

例

次に、FTP フィルタリングをイネーブルに設定する例を示します。

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter ftp 21 0 0 0 0
hostname(config)# filter ftp except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
filter https	Websense サーバでフィルタリングされる HTTPS トラフィックを識別します。
filter java	FWSM を通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバに転送します。
show running-config filter	フィルタリング設定を表示します。
url-server	**filter** コマンドで使用する N2H2 または Websense サーバを識別します。

filter https

Websense サーバでフィルタリングする HTTPS トラフィックを指定するには、グローバル コンフィギュレーション モードで、**filter https** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter https {[*port*[**-***port*] | **except**} *local_ip local_mask foreign_ip foreign_mask*] [**allow**]

no filter https {[*port*[**-***port*] | **except**} *local_ip local_mask foreign_ip foreign_mask*] [**allow**]

シンタックスの説明

port	フィルタリングを適用する TCP ポートを指定します。通常、ポート 443 ですが、他の値も使用できます。ポート 443 の場合、**https** を使用できます。
port **-***port*	（任意）ポート範囲を指定します。
except	（任意）指定した **filter** 条件に対して、例外を作成します。
dest-port	宛先ポート番号を指定します。
local_ip	アクセス対象のうち、セキュリティ レベルが最も高いインターフェイスの IP アドレスを指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
local_mask	*local_ip* のネットワーク マスクを指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
foreign_ip	アクセス対象のうち、セキュリティ レベルが最も低いインターフェイスの IP アドレスを指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスクを指定します。必ず、特定のマスク値を指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
allow	（任意）サーバが使用不可の場合、フィルタリングを適用せずに、FWSM からの発信接続を許可します。このオプションを指定しない場合、N2H2 または Websense サーバがオフラインになると、FWSM は N2H2 または Websense サーバがオンラインに戻るまで、ポート 443 の発信トラフィックを停止します。

デフォルト

このコマンドは、デフォルトではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン　FWSM は、外部の Websense フィルタリング サーバを使用した HTTPS および FTP（ファイル転送プロトコル）サイトのフィルタリングをサポートします。

（注）　N2H2 フィルタリング サーバでは、HTTPS はサポートされません。

HTTPS フィルタリングは、サイトが許可されていない場合、SSL 接続のネゴシエーションを完了しないことによって実行されます。ブラウザには、[The Page or the content cannot be displayed]（ページまたはコンテンツを表示できません）などのエラー メッセージが表示されます。

HTTPS コンテンツは暗号化されているので、FWSM は、ディレクトリおよびファイル名の情報なしで URL 検索を送信します。

例　次に、10.0.2.54 ホストからの接続を除く、すべての発信 HTTPS 接続をフィルタリングする例を示します。

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter https 443 0 0 0 0
hostname(config)# filter https except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
filter activex	FWSM を通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter java	FWSM を通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバに転送します。
show running-config filter	フィルタリング設定を表示します。
url-server	**filter** コマンドで使用する N2H2 または Websense サーバを識別します。

filter java

FWSM を通過する HTTP トラフィックから Java アプレットを削除するには、グローバル コンフィギュレーション モードで、**filter java** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter java {[*port*[**-***port*] | **except**} *local_ip local_mask foreign_ip foreign_mask*]

no filter java {[*port*[**-***port*] | **except**} *local_ip local_mask foreign_ip foreign_mask*]

シンタックスの説明

port	フィルタリングを適用する TCP ポートを指定します。通常、ポート 80 ですが、他の値も使用できます。ポート 80 の場合、**http** または **url** を使用できます。
port **-***port*	（任意）ポート範囲を指定します。
except	（任意）指定した **filter** 条件に対して、例外を作成します。
local_ip	アクセス対象のうち、セキュリティ レベルが最も高いインターフェイスの IP アドレスを指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
local_mask	*local_ip* のネットワーク マスクを指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
foreign_ip	アクセス対象のうち、セキュリティ レベルが最も低いインターフェイスの IP アドレスを指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスクを指定します。必ず、特定のマスク値を指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。

デフォルト

このコマンドは、デフォルトではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

Java アプレットには、保護されたネットワーク上のホストおよびサーバの攻撃を目的としたコードが含まれていることがあるので、セキュリティ上のリスクになります。**filter java** コマンドを使用すると、Java アプレットを削除できます。

filter java コマンドは、発信接続から FWSM に戻る Java アプレットをフィルタリングして、排除します。ユーザは HTML ページを受信しますが、web ページのアプレットのソース コードはコメントとして除外されているので、アプレットを実行することはできません。

applet または /applet HTML タグが複数のネットワーク パケット上に分割されている場合、またはタグ内のコードが MTU のバイト数を超えている場合には、FWSM でタグをブロックできません。Java アプレットが <object> タグ内に存在することが判明している場合には、**filter activex** コマンドを使用して削除します。

例

次に、すべての発信接続上で、Java アプレットをブロックする例を示します。

```
hostname(config)# filter java 80 0 0 0 0
```

このコマンドにより、ポート 80 上のすべてのローカル ホストからの Web トラフィック、およびすべての外部ホストへの接続に対して、Java アプレットがブロックされます。

次に、保護されたネットワーク上のホストへの Java アプレットのダウンロードをブロックする例を示します。

```
hostname(config)# filter java http 192.168.3.3 255.255.255.255 0 0
```

このコマンドにより、ホスト 192.168.3.3 が Java アプレットをダウンロードできなくなります。

関連コマンド

コマンド	説明
filter activex	FWSM を通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter url	トラフィックを URL フィルタリング サーバに転送します。
show running-config filter	フィルタリング設定を表示します。
url-server	**filter** コマンドで使用する N2H2 または Websense サーバを識別します。

filter url

トラフィックを URL フィルタリング サーバに転送するには、グローバル コンフィギュレーション モードで、**filter url** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter url {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*] [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

no filter url {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*] [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

シンタックスの説明

allow	サーバが使用不可の場合、フィルタリングを適用せずに、FWSM からの発信接続を許可します。このオプションを指定しない場合、N2H2 または Websense サーバがオフラインになると、FWSM は N2H2 または Websense サーバがオンラインに戻るまで、ポート 80（Web）の発信トラフィックを停止します。
cgi_truncate	URL に、CGI スクリプトなどの疑問符（?）で始まるパラメータ リストが含まれている場合、疑問符以降のすべての文字を削除して、フィルタリング サーバに送信する URL を切り捨てます。
except	指定した **filter** 条件に対して、例外を作成します。
foreign_ip	アクセス対象のうち、セキュリティ レベルが最も低いインターフェイスの IP アドレスを指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスクを指定します。必ず、特定のマスク値を指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
http	ポート 80 を指定します。80 の代わりに **http** または **www** を使用してポート 80 を指定することもできます。
local_ip	アクセス対象のうち、セキュリティ レベルが最も高いインターフェイスの IP アドレスを指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
local_mask	*local_ip* のネットワーク マスクを指定します。**0.0.0.0**（または短縮形、**0**）を使用すると、全ホストを指定できます。
longurl-deny	URL が URL バッファ サイズの制限を超えている場合、または URL バッファを使用できない場合、URL 要求を拒否します。
longurl-truncate	URL が URL バッファ制限を越えている場合、Websense サーバに送信元ホスト名または IP アドレスだけを送信します。
mask	任意のマスクを指定します。
[*port*[**-***port*]	（任意）フィルタリングを適用する TCP ポートを指定します。通常、ポート 80 ですが、他の値も使用できます。ポート 80 の場合、**http** または **url** を使用できます。任意にポート範囲を指定するには、ハイフンを付けて 2 つめのポートを追加します。
proxy-block	ユーザによる HTTP プロキシ サーバへの接続を防止します。
url	FWSM を通過するデータから、URL をフィルタリングします。

デフォルト

このコマンドは、デフォルトではディセーブルです。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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　**filter url** コマンドを使用すると、発信ユーザに対して、N2H2 または Websense フィルタリング アプリケーションを使用してユーザが指定した WWW URL へのアクセスを防止することができます。

（注）　**filter url** コマンドを発行する前に、**url-server** コマンドを設定しておく必要があります。

filter url コマンドの **allow** オプションは、N2H2 または Websense サーバがオフラインになった場合の FWSM の動作を決定します。**filter url** コマンドに **allow** オプションを指定すると、N2H2 または Websense サーバがオフラインになった場合、ポート 80 のトラフィックは、フィルタリングされずに FWSM を通過します。**allow** オプションを使用しない場合、サーバがオフラインになると、FWSM は、サーバがオンラインに戻るまでポート 80（Web）の発信トラフィックを停止するか、他の URL サーバを使用できる場合には、次の URL サーバに制御を渡します。

（注）　**allow** オプションを使用した場合、N2H2 または Websense サーバがオフラインになると、FWSM は代替サーバに制御を渡します。

FWSM と N2H2 または Websense サーバを併用することにより、企業のセキュリティ ポリシーに基づいて、ユーザの Web サイトへのアクセスを拒否できます。

Websense フィルタリング サーバの使用方法

Websense プロトコル Version 4 により、ホストと FWSM 間でグループおよびユーザ名が認証できます。FWSM がユーザ名の検索を実行すると、Websense サーバは URL フィルタリングおよびユーザ名のロギングを実行します。

N2H2 サーバは、512 MB の最低推奨 RAM が搭載された IFP サーバが稼働する Windows ワークステーション（2000、NT、または XP）でなければなりません。また、N2H2 サービスでは、長い URL のサポートは Websense の上限より少ない 3 KB に制限されます。

Websense プロトコル Version 4 には、次の拡張機能が含まれています。

- URL フィルタリングにより、FWSM で、Websense サーバで定義されたポリシーに基づいて、発信 URL 要求をチェックできます。
- ユーザ名のロギングにより、Websense サーバ上でユーザ名、グループ、およびドメイン名を追跡できます。

- ユーザ名検索により、FWSM でユーザ認証テーブルを使用し、ホスト IP アドレスをユーザ名にマップできます。

Websense の情報は、次の Web サイトから入手できます。

http://www.websense.com/

設定手順

URL をフィルタリングする手順は、次のとおりです。

ステップ 1　ベンダー特定の適切な **url-server** コマンド形式を使用して、N2H2 または Websense サーバを指定します。

ステップ 2　**filter** コマンドを使用して、フィルタリングをイネーブルにします。

ステップ 3　必要に応じて、**url-cache** コマンドを使用してスループットを改善します。

（注）　**url-cache** コマンドは、Websense ログを更新しませんが、Websense のアカウンティング レポートに影響することがあります。**url-cache** コマンドを使用する前に、Websense の実行ログを累積してください。

ステップ 4　実行情報を表示するには、**show url-cache statistics** コマンドおよび **show perfmon** コマンドを使用します。

長い URL の処理

Websense フィルタリング サーバの場合最大 4 KB、N2H2 フィルタリング サーバの場合最大 1159 バイトまでの URL のフィルタリングがサポートされます。

最大許容サイズを超える URL 要求を処理するには、***longurl-truncate*** および ***cgi-truncate*** オプションを使用します。

URL が最大長を超えている場合、**longurl-truncate** または **longurl-deny** オプションがイネーブルに設定されていないと、FWSM はそのパケットをドロップします。

longurl-truncate オプションを使用すると、URL が最大許容長を超えている場合、FWSM はフィルタリング サーバで評価できるように URL のホスト名または IP アドレスの部分だけを送信します。URL が最大許容長を超えている場合に、発信 URL トラフィックを拒否するには、**longurl-deny** オプションを使用します。

CGI URL を、パラメータをつけずに CGI スクリプトの場所とスクリプト名だけに短縮するには、**cgi-truncate** オプションを使用します。長い HTTP 要求のほとんどは、CGI 要求です。パラメータ リストが非常に長い場合、パラメータ リストを含む完全な CGI 要求を待機および送信すると、メモリ リソースが消費され、FWSM のパフォーマンスに影響します。

HTTP 応答のバッファリング

デフォルトでは、ユーザが特定の Web サイトへの接続要求を発行すると、FWSM は要求を Web サーバおよびフィルタリング サーバに同時に送信します。Web コンテンツ サーバの応答よりも前にフィルタリング サーバからの応答がない場合、Web サーバからの応答はドロップされます。これにより、Web クライアント側では、Web サーバからの応答が遅れることになります。

HTTP 応答バッファをイネーブルにすると、Web コンテンツ サーバからの応答がバッファに保管され、フィルタリング サーバが接続を許可した時点で、応答が要求側ユーザに転送されます。これにより、遅延を緩和することができます。

HTTP 応答バッファをイネーブルにするには、次のコマンドを入力します。

```
url-block block block-buffer-limit
```

block-buffer-limit に、バッファするブロックの最大数を指定します。許容値は 0 ～ 128 で、一度にバッファできる 1550 バイト ブロック数を指定します。

例

次に、10.0.2.54 ホストからの接続を除く、すべての発信 HTTP 接続をフィルタリングする例を示します。

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter url 80 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

次に、ポート 8080 で待ち受けるプロキシ サーバを宛先とする、すべての発信 HTTP 接続をブロックする例を示します。

```
hostname(config)# filter url 8080 0 0 0 0 proxy-block
```

関連コマンド

コマンド	説明
filter activex	FWSM を通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter java	FWSM を通過する HTTP トラフィックから Java アプレットを削除します。
url-block	フィルタリング サーバのフィルタリング判断を待機する間 Web サーバ応答で使用する URL バッファを管理します。
url-cache	N2H2 または Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュ サイズを設定します。
url-server	**filter** コマンドで使用する N2H2 または Websense サーバを識別します。

firewall transparent

ファイアウォール モードをトランスペアレント モードに設定するには、グローバル コンフィギュレーション モードで、**firewall transparent** コマンドを使用します。ルーテッド モードに戻すには、このコマンドの **no** 形式を使用します。トランスペアレント ファイアウォールは、「通信上の困難」または「ステルス ファイアウォール」のように動作するレイヤ 2 ファイアウォールで、接続先デバイスへのルータ ホップとして認識されません。このモードを、マルチ コンテキスト モードの各セキュリティ コンテキストに個別に設定できるようになりました。

firewall *transparent*

no firewall *transparent*

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
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。
3.1(1)	このモードを、マルチ コンテキスト モードの各セキュリティ コンテキストに個別に設定できるようになりました。以前は、このコマンドをシステム実行スペースに入力し、全コンテキストにモードを設定していました。

使用上のガイドライン

両方のモードでサポートされるコマンドはほとんどないので、モードを変更すると、FWSM はコンフィギュレーションをクリアします。コンフィギュレーションをすでに実装している場合には、モードを変更する前に、コンフィギュレーションを必ずバックアップしてください。このバックアップは、新しいコンフィギュレーションを作成するときの参照として使用できます。

firewall transparent コマンドでモードを変更するテキスト コンフィギュレーションを FWSM にダウンロードする場合には、必ず、コンフィギュレーションの最初にこのコマンドを設定してください。FWSM は、このコマンドを読み込むとすぐにモードを変更し、ダウンロードしたコンフィギュレーションの読み取りを継続します。このコマンドが、コンフィギュレーションの途中に設定されていると、FWSM はそこまでのコンフィギュレーションをすべてクリアします。

例

次に、ファイアウォール モードをトランスペアレントに変更する例を示します。

```
hostname(config)# firewall transparent
```

関連コマンド

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

format

すべてのファイルを消去して、ファイル システムをフォーマットするには、特権 EXEC モードで、**format** コマンドを使用します。このコマンドは、非表示システム ファイルを含め、ファイル システム上の全ファイルを消去し、ファイル システムを再インストールします。

format {**flash:**}

シンタックスの説明

flash:	内蔵フラッシュ メモリを、コロンを付けて指定します。

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

format コマンドは、指定したファイル システム上の全データを消去し、デバイスに FAT 情報を再書き込みします。

注意　***format*** コマンドは、破壊されたフラッシュ メモリをクリーンアップする必要がある場合に限り、十分に注意して使用してください。

（非表示システム ファイルを除く）すべての表示ファイルを削除するには、***format*** コマンドの代わりに、***delete /recursive*** コマンドを使用します。

例

次に、フラッシュ メモリをフォーマットする例を示します。

```
hostname# format flash:
```

関連コマンド

コマンド	説明
delete	ユーザに表示されるすべてのファイルを削除します。
erase	すべてのファイルを削除し、フラッシュ メモリをフォーマットします。
fsck	破壊されたファイル システムを修復します。

fqdn

エンロールメント実行中に証明書の Subject Alternative Name 拡張に特定の FQDN（完全修飾ドメイン名）を付加するには、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、**fqdn** コマンドを使用します。fqdn の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。

fqdn *fqdn*

no fqdn

シンタックスの説明

fqdn	完全なドメイン名を指定します。*fqdn* の最大長は、64 文字です。

デフォルト

デフォルトでは、FQDN は含まれません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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 のエンロールメント要求に FQDN engineering を含める例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# fqdn engineering
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。
enrollment retry count	エンロールメント要求を送信する再試行回数を設定します。
enrollment retry period	エンロールメント要求の送信を試みるまでの待機時間を分単位で指定します。
enrollment terminal	トラストポイントのカットアンドペースト方式のエンロールメントを指定します。

fragment

パケット分割の管理を追加し、NFS との互換性を改善するには、グローバル コンフィギュレーション モードで、**fragment** 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。

fragment {**size** | **chain** | **timeout** *limit*} [*interface*]

no fragment {**size** | **chain** | **timeout** *limit*} [*interface*]

シンタックスの説明

chain *limit*	完全な IP パケットの分割可能な最大数（1 ～ 8200）を指定します。デフォルトの値は、24 です。
interface	（任意）FWSM インターフェイスを指定します。インターフェイスを指定しない場合、このコマンドはすべてのインターフェイスに適用されます
size *limit*	再構成を待機する IP 再構成データベースに保管できる最大パケット数（1 ～ 30000）を設定します。デフォルトの値は、200 です。
timeout *limit*	すべての分割パケットの到達を待機する最大秒数（1 ～ 30）を指定します。デフォルトの値は、5 です。パケットの最初のフラグメントが着信すると、タイマーが起動します。指定秒数が経過してもパケットのフラグメントがすべて着信しない場合は、すでに着信したパケットのフラグメントがすべて廃棄されます。

デフォルト

デフォルトの設定は次のとおりです。

- ***chain*** は、24 パケットです。
- *interface* は、すべてのインターフェイスです。
- ***size*** は、200 です。
- ***timeout*** は、5 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
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(3)	このコマンドが追加されました。
3.1(1)	このコマンドが変更され、***chain***、***size***、または ***timeout*** のいずれかの引数の選択が必要になりました。旧リリースのソフトウェアと異なり、***fragment*** コマンドを入力する場合には、必ず 1 つの引数を指定する必要があります。

使用上のガイドライン

デフォルトでは、FWSM は、完全な IP パケットを再構成するために、最大 24 の分割パケットを受け入れます。ネットワークのセキュリティ ポリシーに基づいて、各インターフェイスに **fragment chain 1** *interface* コマンドを入力し、分割されたパケットが FWSM を通過しないように、FWSM を設定する必要があります。limit を 1 に設定した場合、すべてのパケットが、分割されていない完全な状態でなければなりません。

FWSM を通過するネットワーク トラフィックのほとんどが NFS である場合、データベースのオーバーフローを防ぐために、さらに調整が必要になることがあります。

WAN インターフェイスのように、NFS サーバとクライアント間の MTU（最大伝送ユニット）サイズが小さい環境では、**chain** キーワードの追加調整が必要になることがあります。この場合、効率を改善するために NFS over TCP を使用することを推奨します。

例

次に、外部インターフェイスおよび内部インターフェイス上で、分割されたパケットを防ぐ例を示します。

```
hostname(config)# fragment chain 1 outside
hostname(config)# fragment chain 1 inside
```

分割されたパケットを防ぐ必要のある他の各追加インターフェイスに対して、続けて **fragment chain 1** *interface* コマンドを入力します。

次に、外部インターフェイス上に分割データベースを設定し、最大サイズを 2000、チェーンの最大長を 45、待機時間を 10 秒に設定する例を示します。

```
hostname(config)# fragment size 2000 outside
hostname(config)# fragment chain 45 outside
hostname(config)# fragment timeout 10 outside
```

関連コマンド

コマンド	説明
clear configure fragment	すべての IP フラグメント再構成設定をデフォルト値にリセットします。
clear fragment	IP フラグメント再構成モジュールの処理データを消去します。
show fragment	IP フラグメント再構成モジュールの処理データを表示します。
show running-config fragment	IP フラグメント再構成設定を表示します。

fsck

ファイル システムのチェックと不良セクタの修復を行うには、特権 EXEC モードで、**fsck** コマンドを使用します。

fsck [/no confirm]{**disk0: | disk1: | flash:**}

シンタックスの説明

/noconfirm	（任意）修復の確認プロンプトを表示しません。
disk0:	内蔵フラッシュ メモリを、コロンを付けて指定します。
disk1:	外部フラッシュ メモリ カードを、コロンを付けて指定します。
flash:	内蔵フラッシュ メモリを、コロンを付けて指定します。ASA 5500 シリーズでは、***flash*** キーワードのエイリアスとして ***disk0*** が定義されています。

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
7.0	このコマンドが追加されました。

使用上のガイドライン

fsck コマンドは、ファイル システムをチェックし、破損箇所を修復します。物理的な修復手順を実行する前に、このコマンドを試してみてください。

/noconfirm キーワードを指定すると、確認プロンプトなしで破損箇所が自動的に修復されます。

例

次に、フラッシュ メモリのファイル システムをチェックする例を示します。

```
hostname# fsck flash:
```

関連コマンド

コマンド	説明
delete	ユーザに表示されるすべてのファイルを削除します。
erase	すべてのファイルを削除し、フラッシュ メモリをフォーマットします。
format	非表示システム ファイルを含め、ファイル システム上の全ファイルを消去し、ファイル システムを再インストールします。

ftp mode passive

FTP（ファイル転送プロトコル）モードをパッシブに設定するには、グローバル コンフィギュレーション モードで、**ftp mode passive** コマンドを使用します。FTP クライアントをアクティブ モード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。

ftp mode passive

no ftp mode passive

デフォルト

このコマンドは、デフォルトではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

使用上のガイドライン

ftp mode passive コマンドは、FTP モードをパッシブに設定します。FWSM は、FTP を使用して、FTP サーバとの間でイメージ ファイルまたはコンフィギュレーション ファイルのアップロードまたはダウンロードを実行できます。**ftp mode passive** コマンドは、FWSM 上の FTP クライアントと FTP サーバとの通信方法を制御します。

パッシブ FTP では、クライアントが制御接続およびデータ接続の両方を開始します。パッシブ モードは、サーバのステートを決定します。つまり、サーバは、クライアントによって開始された制御接続およびデータ接続の両方を受動的に受け入れます。

パッシブ モードでは、宛先ポートと送信元ポートは、いずれも一時ポート（1024 以上）になります。このモードは、クライアントが **passive** コマンドを発行し、パッシブ データ接続の設定を開始するときにクライアントによって設定されます。パッシブ モードでのデータ接続の受信側であるサーバは、特定の接続を待ち受けるポート番号で応答します。

例

次に、FTP モードをパッシブに設定する例を示します。

```
hostname(config)# ftp mode passive
```

関連コマンド

copy	FTP（ファイル転送プロトコル）サーバとの間でイメージ ファイルまたはコンフィギュレーション ファイルをアップロードまたはダウンロードします。
debug ftp client	FTP クライアントのアクティビティに関する詳細情報を表示します。
show running-config ftp mode	FTP クライアントの設定を表示します。

ftp-map

厳密な FTP（ファイル転送プロトコル）検査のためのパラメータを定義する特定のマップを指定するには、グローバル コンフィギュレーション モードで、**ftp-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。

ftp-map *map_name*

no ftp-map *map_name*

シンタックスの説明

map_name	FTP マップの名前を指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

ftp-map コマンドを使用して、厳密な FTP 検査用のパラメータの定義に使用する特定のマップを指定します。このコマンドを入力すると、特定のマップを定義するための各種コマンドを入力できる、FTP マップ コンフィギュレーション モードが開始されます。FTP クライアントが FTP サーバに特定のコマンドを送信しないようにするには、**request-command deny** コマンドを使用します。

FTP マップを定義したあと、**inspect ftp strict** コマンドを使用して、マップをイネーブルにします。さらに、**class-map**、**policy-map**、および **service-policy** コマンドを使用して、トラフィックのクラスを定義し、クラスに **inspect** コマンドを適用し、1 つまたは複数のインターフェイスにポリシーを適用します。

例

次に、FTP トラフィックを指定し、FTP マップを定義し、ポリシーを定義し、外部インターフェイスにポリシーを適用する例を示します。

```
hostname(config)# class-map ftp-port
hostname(config-cmap)# match port tcp eq 21
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# request-command deny put stou appe
hostname(config-ftp-map)# policy-map inbound_policy
hostname(config-pmap)# class ftp-port
hostname(config-pmap-c)# inspect ftp strict inbound_ftp
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

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。
inspect ftp	アプリケーション検査に特定の FTP マップを適用します。
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-command deny	禁止する FTP コマンドを指定します。