CHAPTER 12

email コマンド～ functions コマンド

email

登録中に、指定された電子メール アドレスを証明書のサブジェクト代替名の拡張に含めるには、暗号 CA トラストポイント コンフィギュレーション モードで **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

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

デフォルト値は設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central の登録要求に電子メールアドレスの jjh@nhf.net を含めます。

```
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 モードに入ります。

enable

特権 EXEC モードに入るには、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	（オプション）特権レベルは 0 ～ 15 の間です。

デフォルト

特権レベル 15 を入力します。ただし、コマンドの認可を使用している場合は、デフォルトのレベルはユーザ名に設定されたレベルによって異なります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

デフォルトのイネーブル パスワードはブランクです。パスワードを設定するには、**enable password** コマンドを参照してください。

デフォルトである 15 以外の特権レベルを使用するには、ローカル コマンド認可を設定し（**aaa authorization command** コマンドを参照。***LOCAL*** キーワードを指定する）、**privilege** コマンドを使用して、コマンドを別の特権レベルに設定します。ローカル コマンド認可を設定しない場合は、イネーブル レベルが無視され、設定したレベルにかかわらずレベル 15 にアクセスできます。現在の特権レベルを表示するには、**show curpriv** コマンドを使用します。

レベル 2 以上は特権 EXEC モードに入ります。レベル 0 およびレベル 1 は、ユーザ EXEC モードに入ります。

disable コマンドを入力して、特権 EXEC モードを終了します。

例

次の例では、特権 EXEC モードに入ります。

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

次の例では、レベル 10 の特権 EXEC モードに入ります。

```
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	コマンド認可を設定します。
privilege	ローカル コマンド認可のため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の名前および特権レベルを表示します。

enable gprs

RADIUS アカウンティングにより GPRS をイネーブルにするには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **enable gprs** コマンドを使用します。このモードには、**inspect radius-accounting** コマンドを使用してアクセスできます。セキュリティ アプライアンスは、セカンダリ PDP コンテキストを適切に処理するために、アカウンティング要求停止メッセージの 3GPP VSA 26-10415 をチェックします。

このオプションは、デフォルトではディセーブルになっています。この機能をイネーブルにするには、GTP ライセンスが必要です。

enable gprs

no enable gprs

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、RADIUS アカウンティングにより GPRS をイネーブルにする方法を示しています。

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enable gprs
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングの検査を設定します。
parameters	検査ポリシー マップのパラメータを設定します。

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 のパスワードは削除できません。

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

no enable password level *level*

シンタックスの説明

encrypted	（オプション）パスワードが暗号化された形式であることを指定します。パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。何らかの理由でパスワードを別のセキュリティ アプライアンスにコピーする必要があるが、元のパスワードを知らない場合、暗号化されたパスワードとこのキーワードを指定して、**enable password** コマンドを入力します。通常、このキーワードは、**show running-config enable** コマンドを入力したときにだけ表示されます。
level *level*	（オプション）特権レベル 0 ～ 15 のパスワードを設定します。
password	パスワードに、大文字と小文字が区別される最大 16 文字の英数字および特殊文字の文字列を設定します。パスワードには疑問符（?）とスペースを除く任意の文字を使用できます。

デフォルト

デフォルトのパスワードはブランクです。デフォルトのレベルは 15 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

イネーブル レベル 15（デフォルトのレベル）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リセットする場合は、*password* に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、各コンテキストだけでなく、システム コンフィギュレーションにもイネーブル パスワードを作成できます。

デフォルトである 15 以外の特権レベルを使用するには、ローカル コマンド認可を設定し（**aaa authorization command** コマンドを参照。***LOCAL*** キーワードを指定する）、**privilege** コマンドを使用して、コマンドを別の特権レベルに設定します。ローカル コマンド認可を設定しない場合は、イネーブル レベルが無視され、設定したレベルにかかわらずレベル 15 にアクセスできます。現在の特権レベルを表示するには、**show curpriv** コマンドを使用します。

レベル 2 以上は特権 EXEC モードに入ります。レベル 0 およびレベル 1 は、ユーザ EXEC モードに入ります。

例

次の例では、イネーブル パスワードを Pa$$w0rd に設定します。

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

次の例では、レベル 10 のイネーブル パスワードを Pa$$w0rd10 に設定します。

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

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

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

関連コマンド

コマンド	説明
aaa authorization command	コマンド認可を設定します。
enable	特権 EXEC モードに入ります。
privilege	ローカル コマンド認可のため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の名前および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された形式で表示します。

encryption

IKE ポリシー内の暗号化アルゴリズムを指定するには、暗号 isakmp ポリシー コンフィギュレーション モードで **encryption** コマンドを使用します。暗号化アルゴリズムをデフォルト値の **des** 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。

encryption {**aes | aes-192| aes-256 | des | 3des**}

no encryption {**aes | aes-192| aes-256 | des | 3des**}

シンタックスの説明

3des	IKE ポリシーで、Triple DES 暗号化アルゴリズムを使用することを指定します。
aes	IKE ポリシーで使用する暗号化アルゴリズムが、128 ビット キーを使用する AES であることを指定します。
aes-192	IKE ポリシーで使用する暗号化アルゴリズムが、192 ビット キーを使用する AES であることを指定します。
aes-256	IKE ポリシーで使用する暗号化アルゴリズムが、256 ビット キーを使用する AES であることを指定します。
des	IKE ポリシーで使用する暗号化アルゴリズムが、56 ビット DES-CBC であることを指定します。
priority	Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。

デフォルト

デフォルトの ISAKMP ポリシー暗号化は **3des** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	**isakmp policy encryption** コマンドは既存のものです。
7.2.(1)	**isakmp policy encryption** コマンドが、**encryption** コマンドに置き換えられました。

例

次の例は、グローバル コンフィギュレーション モードで、**encryption** コマンドを使用する方法を示しています。この例では、優先順位番号 25 の IKE ポリシーに 128 ビット キーの AES 暗号化アルゴリズムを使用するように設定します。

```
hostname(config)# crypto isakmp policy 25
hostname(config-isakmp-policy)# encryption aes
```

次の例では、グローバル コンフィギュレーション モードで、優先順位番号 40 の IKE ポリシーに 3DES アルゴリズムを使用するように設定します。

```
hostname(config)# crypto isakmp policy 40
hostname(config-isakmp-policy)# encryption 3des
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

endpoint

H.323 プロトコル検査のために HSI グループにエンドポイントを追加するには、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。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。

endpoint *ip_address if_name*

no endpoint *ip_address if_name*

シンタックスの説明

ip_address	追加するエンドポイントの IP アドレス。HSI グループあたり最大で 10 のエンドポイントが許可されます。
if_name	エンドポイントがセキュリティ アプライアンスに接続されるインターフェイス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、H.323 検査ポリシー マップでエンドポイントを HSI グループに追加する方法を示しています。

```
hostname(config-pmap-p)# hsi-group 10
hostname(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
hostname(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
hsi-group	HSI グループを作成します。
hsi	HSI を HSI グループに追加します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

endpoint-mapper

DCERPC 検査のためにエンドポイント マッパー オプションを設定するには、パラメータ コンフィギュレーション モードで **endpoint-mapper** コマンドを使用します。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。

endpoint-mapper [**epm-service only**] [**lookup-operation** [**timeout** *value*]]

no endpoint-mapper [**epm-service only**] [**lookup-operation** [**timeout** *value*]]

シンタックスの説明

epm-service only	バインディング時にエンドポイント マッパー サービスを適用します。
lookup-operation	エンドポイント マッパー サービスのルックアップ オペレーションをイネーブルにします。
timeout *value*	ルックアップ オペレーションからのピンホールのタイムアウトを指定します。範囲は 0:0:1 ～ 1193:0:0 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、DCERPC ポリシー マップにエンドポイント マッパーを設定する方法を示しています。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# endpoint-mapper epm-service-only
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

enforcenextupdate

NextUpdate CRL フィールドの処理方法を指定するには、ca-crl 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。これが設定された場合、このコマンドは CRL の NextUpdate フィールドを無効にしないことを要求します。使用されない場合、セキュリティ アプライアンスは、不明または無効な CRL の NextUpdate フィールドを許可します。

無効または不明な NextUpdate フィールドを許可するには、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、引数もキーワードもありません。

デフォルト

デフォルト設定は実行（オン）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、ca-crl コンフィギュレーション モードに入り、CRL の NextUpdate フィールドをトラストポイント central に対して期限切れにしないことを要求します

```
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時間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 モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。

enrollment retry count

リトライ回数を指定するには、暗号 CA トラストポイント コンフィギュレーション モードで **enrollment retry count** コマンドを使用します。セキュリティ アプライアンスは、証明書を要求した後、CA から証明書を受信するまで待機します。設定されたリトライ期間内にセキュリティ アプライアンスが証明書を受信しない場合、別の証明書要求が送信されます。セキュリティ アプライアンスが応答を受信するか、リトライ回数が設定回数に達するまで、要求は繰り返されます。

リトライ回数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。

enrollment retry count *number*

no enrollment retry count

シンタックスの説明

number	登録要求の送信を再試行する最大回数です。有効な範囲は 0、1 ～ 100 リトライです。

デフォルト

number のデフォルト設定は、0（無制限）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドはオプションであり、自動登録を設定している場合のみ適用されます。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central 内で登録のリトライ回数を 20 リトライに設定します。

```
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 モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。
enrollment retry period	登録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

リトライ期間を指定するには、暗号 CA トラストポイント コンフィギュレーション モードで **enrollment retry period** コマンドを使用します。セキュリティ アプライアンスは、証明書を要求した後、CA から証明書を受信するまで待機します。指定されたリトライ期間内にセキュリティ アプライアンスが証明書を受信しない場合、別の証明書要求が送信されます。

リトライ期間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。

enrollment retry period *minutes*

no enrollment retry period

シンタックスの説明

minutes	登録要求の送信を試行する分単位の間隔です。有効な範囲は 1 ～ 60 分です。

デフォルト

デフォルト設定は 1 分です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドはオプションであり、自動登録を設定している場合のみ適用されます。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central 内で登録のリトライ期間を 10 分に設定します。

```
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 モードに入ります。
default enrollment	すべての登録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	登録を要求するリトライの回数を定義します。

enrollment terminal

このトラストポイントでのカット アンド ペースト登録を指定するには（手動登録とも呼ばれる）、暗号 CA トラストポイント コンフィギュレーション モードで **enrollment terminal** コマンドを使用します。このコマンド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。

enrollment terminal

no enrollment terminal

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルト設定はオフです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central の CA 登録のカット アンド ペースト方式を指定します。

```
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 モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。
enrollment retry period	登録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	このトラストポイントでの自動登録（SCEP）を指定し、URL を設定します。

enrollment url

このトラストポイントで登録し、登録 URL を設定するために自動登録（SCEP）を指定するには、暗号 CA トラストポイント コンフィギュレーション モードで **enrollment url** コマンドを使用します。このコマンド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。

enrollment url *url*

no enrollment url

シンタックスの説明

url	自動登録で使用する URL の名前を指定します。最大長は 1,000 文字（実質上の無制限）です。

デフォルト

デフォルト設定はオフです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central の SCEP 登録を URL https://enrollsite で指定します。

```
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 モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。
enrollment retry period	登録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	このトラストポイントを使用したカット アンド ペースト登録を指定します。

eou allow

クライアントレス認証をイネーブルにするには、グローバル コンフィギュレーション モードで **eou allow** コマンドを使用します。クライアントレス認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

eou allow clientless

no eou allow clientless

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

クライアントレス認証はデフォルトでイネーブルになります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは EAPoUDP 要求に応答しないホストにのみ適用されます。このコマンドが有効になるのは、次の条件をすべて満たしている場合だけです。

- クライアントレス認証をサポートするために、ネットワーク上にアクセス コントロール サーバが設定されている。
- セキュリティ アプライアンス上にネットワーク アドミッション コントロールが設定されている。

例

次の例はクライアントレス認証をイネーブルにします。

```
hostname(config)# eou allow clientless
hostname(config)#
```

次の例はクライアントレス認証をディセーブルにします。

```
hostname(config)# no eou allow clientless
hostname(config)#
```

関連コマンド

コマンド	説明
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
eou clientless	クライアントレス認証に使用するユーザ名とパスワードを変更します。

eou clientless

クライアントレス認証用にアクセス コントロール サーバに送信するユーザ名とパスワードを変更するには、グローバル コンフィギュレーション モードで **eou clientless** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou clientless username *username*

eou clientless password *password*

デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

no eou clientless username

no eou clientless password

シンタックスの説明

username	EAPoUDP 要求に応答しないリモートホストのクライアントレス認証を得るためにアクセス コントロール サーバに送信したユーザ名を変更します。
username	クライアントレス ホストをサポートするために、アクセス コントロール サーバに設定したユーザ名を入力します。1 ～ 64 文字の ASCII 文字を入力します。前後のスペース、ポンド記号（#）、疑問符（?）、引用符（"）、アステリスク（*）、角括弧（< と >）は除きます。
password	EAPoUDP 要求に応答しないリモート ホストのクライアントレス認証を得るためにアクセス コントロール サーバに送信したパスワードを変更します。
password	クライアントレス ホストをサポートするために、アクセス コントロール サーバに設定したパスワードを入力します。4 ～ 32 文字の ASCII 文字を入力します。

デフォルト

ユーザ名およびパスワード アトリビュートのデフォルト値は clientless です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドが有効になるのは、次の条件をすべて満たしている場合のみです。

- クライアントレス認証をサポートするために、ネットワーク上にアクセス コントロール サーバが設定されている。
- セキュリティ アプライアンス上でクライアントレス認証がイネーブルになっている。
- セキュリティ アプライアンス上にネットワーク アドミッション コントロールが設定されている。

例

次の例はクライアントレス認証のユーザ名を sherlock に変更します。

```
hostname(config)# eou clientless username sherlock
hostname(config)#
```

次の例はクライアントレス認証のユーザ名をデフォルト値である clientless に変更します。

```
hostname(config)# no eou clientless username
hostname(config)#
```

次の例はクライアントレス認証のパスワードを secret に変更します。

```
hostname(config)# eou clientless password secret
hostname(config)#
```

次の例はクライアントレス認証のパスワードをデフォルト値である clientless に変更します。

```
hostname(config)# no eou clientless password
hostname(config)#
```

関連コマンド

コマンド	説明
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
eou allow	クライアントレス認証をイネーブルにします。

eou initialize

1 つ以上のネットワーク アドミッション コントロール セッションに割り当てられたリソースを消去し、セッションごとに新しい無条件のポスチャ確認を開始するには、EXEC モードで **eou initialize** コマンドを使用します。

eou initialize {**all** | **group** *tunnel-group* | **ip** *ip-address*}

シンタックスの説明

all	このセキュリティ アプライアンス上のすべての NAC セッションを再確認します。
group	トンネル グループに割り当てられているすべての NAC セッションを再確認します。
ip	単一の NAC セッションを再確認します。
ip-address	トンネルのリモート ピア側の IP アドレス。
tunnel-group	トンネルをセットアップするパラメータのネゴシエーションに使用されるトンネル グループの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

リモート ピアのポスチャが変更されたり、割り当てられたアクセス ポリシー（ダウンロードされた ACL）が変更された場合に、セッションに割り当てられたリソースを消去するには、このコマンドを使用します。このコマンドを入力すると、EAPoUDP アソシエーションとポスチャ確認に使用するアクセス ポリシー（ダウンロードされた ACL）が消去されます。NAC デフォルト ACL は再確認時には有効です。そのためセッションを初期化すると、ユーザのトラフィックが妨げられる可能性があります。このコマンドは、ポスチャ確認から免除されているピアには作用しません。

例

次の例では、すべての NAC セッションを初期化します。

```
hostname# eou initialize all
hostname
```

次の例では、tg1 というトンネル グループに割り当てられたすべての NAC セッションを初期化します。

```
hostname# eou initialize group tg1
hostname
```

次の例では、IP アドレス 209.165.200.225 が設定されているエンドポイントの NAC セッションを初期化します。

```
hostname# eou initialize 209.165.200.225
hostname
```

関連コマンド

コマンド	説明
eou revalidate	1 つまたはそれ以上の NAC セッションのポスチャ再確認をただちに強制します。
nac-reval-period	ネットワーク アドミッション コントロール セッションで正常に完了した各ポスチャ確認の間隔を指定します。
nac-sq-period	ネットワーク アドミッション コントロール セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。

eou max-retry

セキュリティ アプライアンスが EAP over UDP メッセージをリモート コンピュータに再送信する回数を変更するには、グローバル コンフィギュレーション モードで **eou max-retry** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou max-retry *retries*

no eou max-retry

シンタックスの説明

retries	再送信期限切れの応答で送信された再試行の回数を制限します。1 ～ 3 の値を入力します。

デフォルト

デフォルト値は 3 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドが有効になるのは、次の条件をすべて満たしている場合のみです。

- クライアントレス認証をサポートするために、ネットワーク上にアクセス コントロール サーバが設定されている。
- セキュリティ アプライアンス上でクライアントレス認証がイネーブルになっている。
- セキュリティ アプライアンス上にネットワーク アドミッション コントロールが設定されている。

例

次の例では、EAP over UDP 再送信の回数を 1 回に制限します。

```
hostname(config)# eou max-retry 1
hostname(config)#
```

次の例では、EAP over UDP 再送信の回数をデフォルト値の 3 回に変更します。

```
hostname(config)# no eou max-retry
hostname(config)#
```

関連コマンド

debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。

eou port

Cisco Trust Agent と通信する EAP over UDP のポート番号を変更するには、グローバル コンフィギュレーション モードで **eou port** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou port *port_number*

no eou port

シンタックスの説明

port_number	EAP over UDP 通信用に指定される、クライアント エンドポイント上のポート番号。この番号は Cisco Trust Agent 上で設定されるポート番号です。1024 ～ 65535 の値を入力します。

デフォルト

デフォルト値は 21862 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、EAP over UDP 通信用ポート番号を 62445 に変更します。

```
hostname(config)# eou port 62445
hostname(config)#
```

次の例では、EAP over UDP 通信用ポート番号をデフォルト値に変更します。

```
hostname(config)# no eou port
hostname(config)#
```

関連コマンド

debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
eou initialize	1 つまたはそれ以上の NAC セッションに割り当てられているリソースを消去し、新しい無条件のポスチャ確認をセッションごとに開始します。
eou revalidate	1 つまたはそれ以上の NAC セッションのポスチャ再確認をただちに強制します。

eou revalidate

1 つまたは複数のネットワーク アドミッション コントロール セッションについてポスチャの即時再確認を強制するには、EXEC モードで **eou revalidate** コマンドを使用します。

eou revalidate {**all** | **group** *tunnel-group* | **ip** *ip-address*}

シンタックスの説明

all	このセキュリティ アプライアンス上のすべての NAC セッションを再確認します。
group	トンネル グループに割り当てられているすべての NAC セッションを再確認します。
ip	単一の NAC セッションを再確認します。
ip-address	トンネルのリモート ピア側の IP アドレス。
tunnel-group	トンネルをセットアップするパラメータのネゴシエーションに使用されるトンネル グループの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ピアのポスチャまたは割り当てられたアクセス ポリシー（ダウンロードされた ACL）が変更された場合、このコマンドを使用します。このコマンドは新しい、無条件のポスチャ確認を開始します。コマンドを入力する前に有効であったポスチャ確認と割り当てられたアクセス ポリシーは、新しいポスチャ確認が成功するか失敗するまで有効のままです。このコマンドは、ポスチャ確認から免除されているピアには作用しません。

例

次の例では、すべての NAC セッションを再確認します。

```
hostname# eou revalidate all
hostname
```

次の例では、tg-1 というトンネル グループに割り当てられたすべての NAC セッションを再確認します。

```
hostname# eou revalidate group tg-1
hostname
```

次の例では、IP アドレス 209.165.200.225 が設定されているエンドポイントの NAC セッションを再確認します。

```
hostname# eou revalidate ip 209.165.200.225
hostname
```

関連コマンド

コマンド	説明
eou initialize	1 つまたはそれ以上の NAC セッションに割り当てられているリソースを消去し、新しい無条件のポスチャ確認をセッションごとに開始します。
nac-reval-period	ネットワーク アドミッション コントロール セッションで正常に完了した各ポスチャ確認の間隔を指定します。
nac-sq-period	ネットワーク アドミッション コントロール セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。

eou timeout

EAPoUDP メッセージをリモート ホストに送信した後の待機秒数を変更するには、グローバル コンフィギュレーション モードで **eou timeout** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou timeout {**hold-period | retransmit**} *seconds*

no eou timeout {**hold-period | retransmit**}

シンタックスの説明

hold-period	EAPoUDP メッセージ送信後の最長待機時間は EAPoUDP 再試行数と同じです。**eou initialize** コマンドまたは **eou revalidate** コマンドを実行すると、この設定時間も消去されます。この設定時間が経過すると、セキュリティ アプライアンスは EAP over UDP とリモート ホストとの関連付けを新たに開始します。
retransmit	EAPoUDP メッセージ送信後の最長待機時間。リモート ホストからの応答により、この設定時間は消去されます。**eou initialize** コマンドまたは **eou revalidate** コマンドを実行すると、この設定時間も消去されます。設定時間が経過すると、セキュリティ アプライアンスは EAPoUDP メッセージをリモート ホストに再送します。
seconds	セキュリティ アプライアンスが待機する秒数。hold-period アトリビュートには、範囲 60 ～ 86400 の値、retransmit アトリビュートには、範囲 1 ～ 60 の値をそれぞれ入力します。

デフォルト

hold-period アトリビュートのデフォルト値は 180 です。

retransmit アトリビュートのデフォルト値は 3 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、新しい EAP over UDP アソシエーションを開始するまでの待機時間を 120 秒に変更します。

```
hostname(config)# eou timeout hold-period 120
hostname(config)#
```

次の例では、新しい EAP over UDP アソシエーションを開始するまでの待機時間をデフォルト値に変更します。

```
hostname(config)# no eou timeout hold-period
hostname(config)#
```

次の例では、再送待機時間を 6 秒に変更します。

```
hostname(config)# eou timeout retransmit 6
hostname(config)#
```

次の例では、再送待機時間をデフォルト値に変更します。

```
hostname(config)# no eou timeout retransmit
hostname(config)#
```

関連コマンド

コマンド	説明
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
eou max-retry	セキュリティ アプライアンスが EAP over UDP メッセージをリモート コンピュータに再送する回数を変更します。

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、非表示のシステム ファイルを含むすべてのファイルを上書きし、ファイル システムを消去してからファイル システムを再インストールします。

erase [**disk0: | disk1: | flash:**]

シンタックスの説明

disk0:	（オプション）内蔵フラッシュ メモリを指定し、続けてコロン（:）を入力します。
disk1:	（オプション）外部のコンパクト フラッシュ メモリ カードを指定し、続けてコロン（:）を入力します。
flash:	（オプション）内蔵フラッシュ メモリを指定し、続けてコロン（:）を入力します。

注意　フラッシュ メモリを消去すると、フラッシュ メモリに保存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存してください。

ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

erase コマンドは、OxFF パターンを使用してフラッシュ メモリ上のすべてのデータを消去し、空のファイル システム割り当てテーブルをデバイスに書き直します。

すべての可視ファイル（非表示のシステム ファイルを除く）を削除するには、***erase*** コマンドではなく、***delete /recursive*** コマンドを使用します。

（注）　Cisco PIX セキュリティ アプライアンスでは、***erase*** コマンドと ***format*** コマンドは同じ処理を実行します。ユーザ データを 0xFF パターンを使用して破棄します。

（注）　Cisco ASA 5500 シリーズのセキュリティ アプライアンスでは、***erase*** コマンドを実行すると、ディスク上のすべてのユーザ データが 0xFF パターンを使用して破棄されます。一方、***format*** コマンドはファイル システムの制御構造をリセットするだけです。生ディスク読み取りツールを使用すると、この情報はまだ参照できる可能性があります。

例

次の例では、ファイル システムを消去して再フォーマットします。

```
hostname# erase flash:
```

関連コマンド

コマンド	説明
delete	非表示のシステム ファイルを除く、すべての可視ファイルを削除します。
format	すべてのファイル（非表示のシステム ファイルを含む）を消去して、ファイル システムをフォーマットします。

esp

IPSec Pass Thru 検査用に esp トンネルと AH トンネルのパラメータを指定するには、パラメータ コンフィギュレーション モードで **esp** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

{**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

no {**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

シンタックスの説明

esp	esp トンネルのパラメータを指定します。
ah	AH トンネルのパラメータを指定します。
per-client-max *n*	1 つのクライアントから最大トンネルを指定します。
timeout *time*	esp トンネルにアイドルタイムを指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、UDP 500 トラフィックを許可する方法を示しています。

```
hostname(config)# access-list test-udp-acl extended permit udp any any eq 500
hostname(config)# class-map test-udp-class
hostname(config-pmap-c)# match access-list test-udp-acl

hostname(config)# policy-map type inspect ipsec-pass-thru ipsec-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 32 timeout 00:06:00
hostname(config-pmap-p)# ah per-client-max 16 timeout 00:05:00

hostname(config)# policy-map test-udp-policy
hostname(config-pmap)# class test-udp-class
hostname(config-pmap-c)# inspect ipsec-pass-thru ipsec-map
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

established

確立されている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 dport* [*sport*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

no established *est_protocol dport* [*sport*] [**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ルックアップに使用する IP プロトコル（UDP または TCP）を指定します。
dport	確立されている接続のルックアップに使用する宛先ポートを指定します。
permitfrom	（オプション）指定されたポートから発信されるリターン プロトコル接続を許可します。
permitto	（オプション）指定されたポート宛のリターン プロトコル接続を許可します。
port [*-port*]	（オプション）リターン接続の（UDP または TCP）宛先ポートを指定します。
protocol	（オプション）リターン接続により使用される IP プロトコル（UDP または TCP）です。
sport	（オプション）確立されている接続のルックアップに使用する送信元ポートを指定します。

デフォルト

デフォルトは次のとおりです。

- *dport*：0（ワイルドカード）
- *sport*：0（ワイルドカード）

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	***to*** および ***from*** キーワードが、CLI から削除されました。代わりに ***permitto*** および ***permitfrom*** キーワードを使用してください。

使用上のガイドライン

established コマンドは、発信接続に対するリターン アクセスがセキュリティ アプライアンスを通るのを許可します。このコマンドは、ネットワークからの発信で、セキュリティ アプライアンスによって保護されている元の接続、および外部ホスト上の同じ 2 つのデバイス間の着信であるリターン接続を扱います。**established** コマンドを使用すると、接続のルックアップに使用する宛先ポートを指定できます。この追加によって、コマンドをさらに制御できるようになり、宛先ポートは既知であるが、送信元ポートは未知のプロトコルをサポートできます。**permitto** キーワードと **permitfrom** キーワードは、リターン着信接続を定義します。

注意　**established** コマンドには常に **permitto** キーワードと **permitfrom** キーワードを指定することを推奨します。この 2 つのキーワードを指定せずに **established** コマンドを使用すると、外部システムに接続したときに、その外部システムが接続に関係する内部ホストに無制限に接続できるため、セキュリティ リスクになるおそれがあります。この状況は、内部システムへの攻撃に利用される可能性があります。

次の例は、**established** コマンドを正しく使用しなかった場合に発生する可能性のあるセキュリティ違反を示しています。

この例は、内部システムがポート 4000 上の外部ホストに TCP 接続を作成した場合、外部ホストは、任意のプロトコルを使用して任意のポート上に戻れることを示しています。

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

使用するポートをプロトコルが指定しない場合、送信元ポートおよび宛先ポートを **0** に指定できます。必要な場合に限り、ワイルドカード ポート（0）を使用します。

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

（注）　**established** コマンドが正しく動作するには、クライアントが **permitto** キーワードで指定したポート上でリッスンしている必要があります。

established コマンドは、**nat 0** コマンド（**global** コマンドがない）を付けて使用できます。

（注）　**established** コマンドを、PAT と共に使用することはできません。

セキュリティ アプライアンスは、**established** コマンドと連携して XDMCP をサポートしています。

注意　セキュリティ アプライアンスを介して XWindows システム アプリケーションを使用すると、セキュリティ リスクになる恐れがあります。

XDMCP は、デフォルトでオンになっていますが、**established** コマンドを次のように入力するまでセッションは確立されません。

```
hostname(config)# established tcp 0 6000 to tcp 6000 from tcp 1024-65535
```

established コマンドを入力すると、内部の XDMCP（UNIX または ReflectionX）搭載ホストが、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、それに続く 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が不明であるため、*sport* フィールドは 0（ワイルドカード）と指定する必要があります。*dport* は、6000 + *n* である必要があります。ここで、*n* は、ローカル ディスプレイ番号です。UNIX コマンドを使用して、この値を変更します。

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

established コマンドが必要な理由は、多くの TCP 接続が生成され（ユーザとの対話に基づき）、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です。セキュリティ アプライアンスは、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** コマンドの入力が必要です。

例

次の例では、2 つのホスト間の、プロトコル A を使用した SRC ポート B からポート C を宛先とする接続を示しています。セキュリティ アプライアンスを通過するリターン接続でプロトコル D（プロトコル A はプロトコル D と異なる可能性がある）を許可するには、送信元ポートはポート F に対応し、宛先ポートはポート E に対応している必要があります。

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

この例は、内部ホストから外部ホストに対し、TCP 送信元ポート 6060 と任意の宛先ポートを使用して接続を開始する方法を示しています。セキュリティ アプライアンスは、このホスト間に TCP 宛先ポート 6061 と TCP 送信元ポート 6059 を経由するリターン トラフィックを許可します。

```
hostname(config)# established tcp 6060 0 permitto tcp 6061 permitfrom tcp 6059
```

この例は、内部ホストから外部ホストに対し、UPD 宛先ポート 6060 と任意の送信元ポートを使用して接続を開始する方法を示しています。セキュリティ アプライアンスは、このホスト間に TCP 宛先ポート 6061 と TCP 送信元ポート 1024-65535 を経由するリターン トラフィックを許可します。

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

次の例は、ローカル ホスト 10.1.1.1 が外部のホスト 209.165.201.1 に対してポート 9999 上で TCP 接続を開始する方法を示しています。この例では、外部ホスト 209.165.201.1 のポート 4242 からのパケットがローカル ホスト 10.1.1.1 のポート 5454 に戻ることが許可されます。

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

次の例は、外部ホスト 209.165.201.1 の任意のポートからローカル ホスト 10.1.1.1 のポート 5454 に戻るパケットを許可する方法を示しています。

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

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	確立されている接続に基づく、許可済みの着信接続を表示します。

exceed-mss

スリーウェイ ハンドシェイクの間にピアによって設定された TCP の最大セグメント サイズを超えるデータ長のパケットを許可またはドロップするには、tcp マップ コンフィギュレーション モードで **exceed-mss** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

exceed-mss {**allow** | **drop**}

no exceed-mss {**allow** | **drop**}

シンタックスの説明

allow	MSS を超えるパケットを許可します。
drop	MSS を超えるパケットをドロップします。

デフォルト

デフォルトでは、パケットはドロップされます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。スリーウェイ ハンドシェイクの間にピアによって設定された TCP の最大セグメント サイズを超えるデータ長の TCP パケットをドロップするには、tcp マップ コンフィギュレーション モードの **exceed-mss** コマンドを使用します。

例

次の例では、ポート 21 で MSS を超過するパケットを送信するフローを許可します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# exceed-mss allow
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq ftp
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

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

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、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

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

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

例

次の例は、**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 モードを終了してセッションからログアウトする方法を示しています。

```
hostname(config)# exit
hostname# exit

Logoff
```

次の例は、**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 モードを終了する方法と、**disable** コマンドを使用して特権 EXEC モードを終了する方法を示しています。

```
hostname(config)# 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 モードを終了します。または、特権 EXEC モードまたはユーザ EXEC モードからログアウトします。

expiry-time

オブジェクトのキャッシングが、オブジェクトの再確認なしで期限切れになる時刻を設定するには、キャッシュ モードで **expiry-time** コマンドを使用します。有効期限を新しい値で再設定するには、もう一度このコマンドを使用します。有効期限をコンフィギュレーションから削除してデフォルト値の 1 分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。

expiry-time *time*

no expiry-time

シンタックスの説明

time	セキュリティ アプライアンスがオブジェクトを再確認せずにキャッシュする場合に必要な時間を分単位で表します。

デフォルト

1 分。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
キャッシュ モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

有効期限は、セキュリティ アプライアンスがオブジェクトを再確認せずにキャッシュする場合に必要な時間を分単位で表したものです。再確認は、コンテンツを再び確認することによって行われます。

例

次の例では、有効期限を 13 分に設定する方法を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)#expiry-time 13
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードに入ります。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシングをディセーブルにします。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシングに関する再確認ポリシーを設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

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、引数もキーワードもありません。

デフォルト

フェールオーバーはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、コンフィギュレーションで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ことに制限されています（**failover active** コマンドを参照してください）。
7.2(1)	ASA 5505 デバイスに固有のフェールオーバー機能のサポートが追加されました。

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 リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになる恐れがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

ASA 5505 デバイスではステートレス フェールオーバーのみ許可されます。さらに、Easy VPN ハードウェア クライアントとして機能していない場合に限ります。

例

次の例では、フェールオーバーをディセーブルにします。

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

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover active	アクティブにするスタンバイ装置を切り替えます。
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内の **failover** コマンドを表示します。

failover active

スタンバイ セキュリティ アプライアンスまたはフェールオーバー グループをアクティブ状態にするには、特権 EXEC モードで **failover active** コマンドを使用します。アクティブなセキュリティ アプライアンスまたはフェールオーバー グループをスタンバイに切り替えるには、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*	(オプション)アクティブにするフェールオーバー グループを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、新しいフェールオーバー グループを含めるように修正されました。

使用上のガイドライン

failover active コマンドを使用して、スタンバイ装置からフェールオーバー スイッチを起動します。または、アクティブ装置から **no failover active** コマンドを使用して、フェールオーバー スイッチを起動します。この機能を使用して、障害が発生した装置をサービスに戻し、メンテナンスのため、アクティブ装置を強制的にオフラインにします。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な接続はドロップされます。フェールオーバーが発生した後、クライアントはそれらの接続を再度確立する必要があります。

フェールオーバー グループの切り替えは、Active/Active フェールオーバーでのみ利用可能です。フェールオーバー グループを指定せずに Active/Active フェールオーバー装置に **failover active** コマンドを入力した場合、装置上のすべてのグループがアクティブになります。

例

次の例では、スタンバイ グループ 1 をアクティブにしています。

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

関連コマンド

コマンド	説明
failover reset	セキュリティ アプライアンスを、障害が発生した状態からスタンバイに変更します。

failover group

Active/Active 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 グループの番号。有効値は、1 または 2 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

最大 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 コンテキストにだけ追加できます。フェールオーバー グループの作成と登録は、フェールオーバーがディセーブルにされている場合のみ可能です。

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 モードに入ります。**primary**、**secondary**、**preempt**、**replication http**、**interface-policy**、**mac address**、および **polltime interface** コマンドは、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**、**failover replication http**、および **failover mac address** コマンドは、Active/Active フェールオーバー コンフィギュレーションに影響を与えません。それらのコマンドは、フェールオーバー コンフィギュレーション モードの **polltime interface**、**interface-policy**、**replication http**、および **mac address** コマンドによって上書きされます。

フェールオーバー グループを削除するときは、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、デフォルトによりフェールオーバー グループ 1 に割り当てられます。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。

（注）　同じネットワーク上に Active/Active フェールオーバー ペアが複数ある場合は、あるペアのインターフェイスに割り当てられているものと同じデフォルト仮想 MAC アドレスが、他のペアのインターフェイスに割り当てられることがあります。これは、デフォルト仮想 MAC アドレスの決定方法に基づいた動作です。ネットワーク上の MAC アドレスを重複させないためには、**mac address** コマンドを使用して、各物理インターフェイスに必ずアクティブとスタンバイの仮想 MAC アドレスを割り当てるようにしてください。

例

次の例（抜粋）は、2 つのフェールオーバー グループに対して適用可能なコンフィギュレーションを示しています。

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

関連コマンド

コマンド	説明
asr-group	非対称のルーティング インターフェイス グループ ID を指定します。
interface-policy	モニタリングがインターフェイス障害を検出したときのフェールオーバー ポリシーを指定します。
join-failover-group	フェールオーバー グループにコンテキストを割り当てます。
mac address	フェールオーバー グループ内のコンテキストの仮想 MAC アドレスを定義します。
polltime interface	監視されているインターフェイスに送信される hello メッセージの間隔を指定します。
preempt	リブート後、優先順位がより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 グループに対するより高い優先順位を指定します。
replication http	選択されたフェールオーバー グループに対して HTTP セッションの複製を指定します。
secondary	セカンダリ装置に、フェールオーバー グループに対するより高い優先順位を指定します。

failover interface ip

フェールオーバー インターフェイスとステートフル フェールオーバー インターフェイスに対して IP アドレスと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です。
ip_address mask	プライマリ モジュール上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 インターフェイスに対して、IP アドレスとマスクを指定します。
standby *ip_address*	セカンダリ モジュールがプライマリ モジュールとの通信に使用する IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

フェールオーバー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、レイヤ 3 の機能です。そのことは、セキュリティ アプライアンスが透過的なファイアウォール モードで動作していても、インターフェイスがシステムにグローバルであっても変わりません。

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

このコマンドは、セキュリティ アプライアンスを LAN フェールオーバー用にブートストラップするときにコンフィギュレーションに含める必要があります。

例

次の例は、フェールオーバー インターフェイスに対して IP アドレスとマスクを指定する方法を示しています。

```
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	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
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	指定されたインターフェイスのヘルスを監視します。
show running-config failover	実行コンフィギュレーション内の **failover** コマンドを表示します。

failover interface-policy

モニタリングがインターフェイス障害を検出したときのフェールオーバーの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	パーセンテージとして使用されるときは 1 ～ 100 の数字を指定し、番号として使用されるときは 1 からインターフェイスの最大数の数字を指定します。
%	（オプション）*num* の数が監視対象インターフェイスのパーセンテージであることを指定します。

デフォルト

デフォルトは次のとおりです。

- *num* は 1 です。
- 物理インターフェイスのモニタリングは、デフォルトでイネーブルになっています。論理インターフェイスのモニタリングは、デフォルトではディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

num 引数とオプションの **%** キーワードの間にスペースを含めないでください。

障害が発生したインターフェイスの数が設定済みポリシーの基準を満たした場合、他のセキュリティ アプライアンスが正常に機能しているときは、セキュリティ アプライアンスは自身を障害としてマークし、場合によってはフェールオーバーが発生します（アクティブなセキュリティ アプライアンスに障害が発生した場合）。ポリシーでカウントされるのは、**monitor-interface** コマンドで監視対象として指定したインターフェイスのみです。

（注）　このコマンドが適用されるのは、Active/Standby フェールオーバーのみです。Active/Active フェールオーバーでは、フェールオーバー グループ コンフィギュレーション モードの **interface-policy** コマンドを使用して、各フェールオーバー グループのインターフェイス ポリシーを設定します。

例

次の例では、フェールオーバー ポリシーを指定する 2 つの方法を示しています。

```
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	装置とインターフェイスのポーリング回数を指定します。
failover reset	障害が発生した装置を、障害が発生する前の状態に戻します。
monitor-interface	フェールオーバーのために監視対象に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状態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のキーを指定するには、グローバル コンフィギュレーション モードで **failover key** コマンドを使用します。キーを削除するには、このコマンドの **no** 形式を使用します。

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

no failover key

シンタックスの説明

hex *key*	暗号キー用の 16 進値を指定します。キーは、32 個の 16 進文字（0-9、a-f）にする必要があります。
secret	英数字の共有秘密を指定します。秘密には 1 ～ 63 文字を設定できます。有効な文字は、番号、文字、または句読点の任意の組み合せです。共有秘密は、暗号キーを生成するために使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドは、**failover lan key** から **failover key** に修正されました。
7.0(4)	このコマンドは、***hex*** *key* キーワードおよび引数を含めるように変更されました。

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して認証するには、共有秘密または 16 進キーを使用して両方の装置を設定する必要があります。フェールオーバー キーを指定しない場合、フェールオーバー通信はクリアで送信されます。

（注） PIX セキュリティ アプライアンス プラットフォームでは、装置を接続するために専用のシリアル フェールオーバー ケーブルを使用している場合、フェールオーバー キーが設定されていても、このフェールオーバー リンク経由の通信は暗号化されません。フェールオーバー キーは LAN ベースのフェールオーバー通信だけを暗号化します。

注意　フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになる恐れがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次の例は、フェールオーバー ペアの装置間のフェールオーバー通信を保護するために共有秘密を指定する方法を示しています。

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

次の例は、フェールオーバー ペアの装置間のフェールオーバー通信を保護するために 16 進キーを指定する方法を示しています。

```
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内の failover コマンドを表示します。

failover lan enable

LAN ベースのフェールオーバーを PIX セキュリティ アプライアンス上で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 lan enable** コマンドを使用します。LAN ベースの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 lan enable

no failover lan enable

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

イネーブルになっていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドの **no** 形式を使用して LAN ベースのフェールオーバーをディセーブルにした場合、フェールオーバー ケーブルがインストールされている場合はケーブル ベースのフェールオーバーが使用されます。このコマンドは、PIX セキュリティ アプライアンスでのみ使用できます。

注意　フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになる恐れがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次の例では、LAN ベースのフェールオーバーをイネーブルにします。

```
hostname(config)# failover lan enable
```

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 lan unit	LAN ベースのフェールオーバーでの、プライマリ装置またはセカンダリ装置を指定します。
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。
show running-config failover	実行コンフィギュレーション内の **failover** コマンドを表示します。

failover lan interface

フェールオーバー通信に使用されるインターフェイスを指定するには、グローバル コンフィギュレーション モードで **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* {*phy_if*[*.sub_if*] | *vlan_if*}

no failover lan interface [*if_name* {*phy_if*[*.sub_if*] | *vlan_if*}]

シンタックスの説明

if_name	フェールオーバー専用のセキュリティ アプライアンス インターフェイスの名前を指定します。
phy_if	物理インターフェイスを指定します。
sub_if	（オプション）サブインターフェイス番号を指定します。
vlan_if	ASA 5505 適応型セキュリティ アプライアンス上で使用され、フェールオーバー リンクとして VLAN インターフェイスを指定します。

デフォルト

設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドが、*phy_if* 引数を含めるように修正されました。
7.2(1)	このコマンドが、*vlan_if* 引数を含めるように修正されました。

使用上のガイドライン

LAN フェールオーバーでは、フェールオーバー トラフィックを送信するための専用のインターフェイスが必要です。ただし、ステートフル フェールオーバー リンクに対しては、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。

（注）　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対して同じインターフェイスを使用する場合、インターフェイスには LAN ベースの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のトラフィックを処理するための十分な容量が必要です。

デバイス上の使用されていない任意のイーサネット 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。現在名前で設定されているインターフェイスは指定できません。フェールオーバー インターフェイスは、通常のネットワーク インターフェイスとしては設定されません。フェールオーバー通信専用です。このインターフェイスは、フェールオーバー リンクのために（およびオプションで状態リンクのために）だけ使用する必要があります。LAN ベースのフェールオーバー リンクは、リンクにホストまたはルータのない専用スイッチを使用するか、装置を直接リンクするためのクロスオーバー イーサネット ケーブルを使用して接続できます。

（注）　VLAN を使用する場合は、フェールオーバー リンクのための専用 VLAN を使用します。フェールオーバー リンク VLAN を他の VLAN と共有すると、断続的なトラフィック障害や PING および ARP 障害が発生する場合があります。スイッチを使用してフェールオーバー リンクに接続する場合、スイッチ上の専用インターフェイスと、セキュリティ アプライアンス上の専用インターフェイスをフェールオーバー リンク用に使用してください。通常のネットワーク トラフィックを伝送するサブインターフェイスを持つインターフェイスを共有しないでください。

マルチ コンテキスト モードを実行しているシステム上では、フェールオーバー リンクはシステム コンテキスト内にあります。このインターフェイスと状態リンク（使用されている場合）が、システム コンテキスト内にある設定可能な唯一のインターフェイスです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。

（注）　フェールオーバー リンクの IP アドレスおよび MAC アドレスは、フェールオーバー時に変更されません。

このコマンドの **no** 形式では、フェールオーバー インターフェイスの IP アドレス設定も消去されます。

このコマンドは、セキュリティ アプライアンスを LAN フェールオーバー用にブートストラップするときにコンフィギュレーションに含める必要があります。

例

次の例では、PIX 500 シリーズセキュリティ アプライアンス上にフェールオーバー LAN インターフェイスを設定します。

```
hostname(config)# failover lan interface folink Ethernet4
```

次の例では、ASA 5500 シリーズ適応型セキュリティ アプライアンス（ASA 5505 適応型セキュリティ アプライアンスを除く）上にサブインターフェイスを使用してフェールオーバー LAN インターフェイスを設定します。

```
hostname(config)# failover lan interface folink GigabitEthernet0/3.1
```

次の例では、ASA 5505 適応型セキュリティ アプライアンス上にフェールオーバー LAN インターフェイスを設定します。

```
hostname(config)# failover lan interface folink Vlan6
```

関連コマンド

コマンド	説明
failover lan enable	PIX セキュリティ アプライアンス上で、LAN ベースのフェールオーバーをイネーブルにします。
failover lan unit	LAN ベースのフェールオーバーでの、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

LAN フェールオーバー設定でセキュリティ アプライアンスをプライマリ装置またはセカンダリ装置のいずれかに設定するには、グローバル コンフィギュレーション モードで **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	セキュリティ アプライアンス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

セカンダリです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

Active/Standby フェールオーバーの場合、フェールオーバー装置のプライマリ宛先およびセカンダリ宛先は、ブート時にどちらの装置がアクティブになるかを指定します。次の状態が発生すると、プライマリ装置がブート時にアクティブ装置になります。

- プライマリ装置およびセカンダリ装置の両方が、最初のフェールオーバー ポーリング チェック内にブート シーケンスを完了した。
- プライマリ装置がセカンダリ装置の前にブートした。

プライマリ装置がブートするときにセカンダリ装置がすでにアクティブであった場合、プライマリ装置はアクティブではなくスタンバイ装置になります。この場合、強制的にプライマリ装置をアクティブ ステータスに戻すために、**no failover active** コマンドをセカンダリ（アクティブ）装置に発行する必要があります。

Active/Active フェールオーバーに対して、各フェールオーバー グループにはプライマリ装置またはセカンダリ装置のプリファレンスが割り当てられます。このプリファレンスは、両方の装置が同時に起動する場合（フェールオーバー ポーリング期間内で）、フェールオーバー グループのコンテキストのフェールオーバー ペアのどの装置をアクティブにするかを決定します。

このコマンドは、セキュリティ アプライアンスを LAN フェールオーバー用にブートストラップするときにコンフィギュレーションに含める必要があります。

例

次の例では、LAN ベースのフェールオーバーでセキュリティ アプライアンスをプライマリ装置として設定します。

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

関連コマンド

コマンド	説明
failover lan enable	PIX セキュリティ アプライアンス上で、LAN ベースのフェールオーバーをイネーブルにします。
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 インターフェイスを指定するには、グローバル コンフィギュレーション モードで **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* [*phy_if*]

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セキュリティ アプライアンス インターフェイスの名前を指定します。
phy_if	（オプション）物理インターフェイスまたは論理インターフェイスのポートを指定します。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または標準ファイアウォール インターフェイスを共有している場合、この引数は必要ありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドが、*phy_if* 引数を含めるように修正されました。
7.0(4)	このコマンドは、標準ファイアウォール インターフェイスを受け入れるように修正されました。

使用上のガイドライン

このコマンドはステートフル フェールオーバーをサポートしない ASA 5505 シリーズ適応型セキュリティ アプライアンスでは利用できません。

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は、フェールオーバー通信または標準ファイアウォール インターフェイスを共有していない場合に必要です。

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するには、**no failover link** コマンドを入力します。専用のステートフル フェールオーバー インターフェイスを使用している場合、**no failover link** コマンドを実行すると、ステートフル フェールオーバー インターフェイスの IP アドレス設定も消去されます。

ステートフル フェールオーバーを使用するには、すべての状態情報を渡すようにステートフル フェールオーバー リンクを設定する必要があります。ステートフル フェールオーバー リンクの設定には、次の 3 つのオプションがあります。

- ステートフル フェールオーバー リンク専用のイーサネット インターフェイスを使用できます。

- LAN ベースのフェールオーバーを使用している場合、フェールオーバー リンクを共有できます。
- 内部インターフェイスなどの通常のデータ インターフェイスを共有できます。ただし、このオプションは推奨されていません。

ステートフル フェールオーバー リンク専用のイーサネット インターフェイスを使用している場合、スイッチまたは装置を直接接続するクロスケーブルを使用できます。スイッチを使用する場合、このリンク上に他のホストまたはルータは設定できません。

（注）　セキュリティ アプライアンスに直接接続するシスコ スイッチ ポート上で PortFast オプションをイネーブルにします。

フェールオーバー リンクをステートフル フェールオーバー リンクとして使用している場合、利用可能な最速のイーサネット インターフェイスを使用する必要があります。インターフェイス上でパフォーマンスの低下が見られる場合は、別のインターフェイスをステートフル フェールオーバー インターフェイス専用にすることを検討してください。

ステートフル フェールオーバー リンクとしてデータ インターフェイスを使用する場合は、そのインターフェイスをステートフル フェールオーバー リンクとして指定しようとすると次の警告が表示されます。

```
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
  Sharing Stateful failover interface with regular data interface is not
  a recommended configuration due to performance and security concerns.
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
```

データ インターフェイスをステートフル フェールオーバー インターフェイスと共有すると、リプレイ アタックを受けやすくなります。さらに、大容量のステートフル フェールオーバー トラフィックがインターフェイスに送信される可能性があり、そのネットワーク セグメントでパフォーマンスが低下する恐れがあります。

（注）　ステートフル フェールオーバー インターフェイスとしてデータ インターフェイスを使用することは、シングル コンテキスのルーテッド モードのみでサポートされています。

マルチ コンテキスト モードでは、ステートフル フェールオーバー リンクはシステム コンテキスト内にあります。このインターフェイスとフェールオーバー インターフェイスが、システム コンテキスト内にある唯一のインターフェイスです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。

マルチ コンテキスト モードでは、ステートフル フェールオーバー インターフェイスはシステム コンテキスト内にあります。このインターフェイスとフェールオーバー インターフェイスが、システム コンテキスト内にある唯一のインターフェイスです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。

（注）　ステートフル フェールオーバー リンクが通常のデータ インターフェイスで設定されている場合を除き、ステートフル フェールオーバー リンクの IP アドレスおよび MAC アドレスは、フェールオーバーで変更されません。

注意　フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになる恐れがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次の例は、ステートフル フェールオーバー インターフェイスとして専用インターフェイスを指定する方法を示しています。次の例のインターフェイスには、既存のコンフィギュレーションはありません。

```
hostname(config)# failover link stateful_if e4
INFO: Non-failover interface config is cleared on Ethernet4 and its sub-interfaces
```

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	インターフェイスの最大伝送ユニットを指定します。

failover mac address

物理インターフェイスのためのフェールオーバー仮想 MAC アドレスを指定するには、グローバル コンフィギュレーション モードで **failover mac address** コマンドを使用します。仮想 MAC 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 mac address *phy_if active_mac standby_mac*

no failover mac address *phy_if active_mac standby_mac*

シンタックスの説明

phy_if	MAC アドレスを設定するインターフェイスの物理名。
active_mac	アクティブなセキュリティ アプライアンスの、指定されたインターフェイスに割り当てられた MAC アドレス。MAC アドレスは、h.h.h 形式で入力する必要があります。h は、16 ビットの 16 進数値です。
standby_mac	スタンバイ セキュリティ アプライアンスの指定されたインターフェイスに割り当てられた MAC アドレス。MAC アドレスは、h.h.h 形式で入力する必要があります。h は、16 ビットの 16 進数値です。

デフォルト

設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

failover mac address コマンドは、Active/Standby フェールオーバー ペア用の仮想 MAC アドレスを設定します。仮想 MAC アドレスが定義されていない場合、各フェールオーバー装置はブート時にインターフェイスとしてバーンドイン MAC アドレスを使用し、それらのアドレスをフェールオーバー ピアと交換します。プライマリ装置上のインターフェイスの MAC アドレスは、アクティブ装置のインターフェイスに使用されます。

ただし、両方の装置が同時にオンラインにならず、セカンダリ装置が最初にブートしてアクティブになった場合は、独自のインターフェイスとしてバーンドイン MAC アドレスを使用します。プライマリ装置がオンラインになると、セカンダリ装置はプライマリ装置から MAC アドレスを取得します。この変更はネットワーク トラフィックを妨げる可能性があります。インターフェイスに仮想 MAC アドレスを設定すると、セカンダリ装置がプライマリ装置の前にオンラインになる場合でも、セカンダリ装置がアクティブ装置であるときに正しい MAC アドレスが使用されます。

LAN ベースのフェールオーバー用に設定されているインターフェイスには、**failover mac address** コマンドは、必要ありません（したがって、このコマンドは使用できません）。**failover lan interface** コマンドは、フェールオーバーが発生したときに IP アドレスおよび MAC アドレスのどちらも変更しないためです。セキュリティ アプライアンスが Active/Active フェールオーバーに対して設定され

ている場合、このコマンドは無効です。

failover mac address コマンドをコンフィギュレーションに追加する場合は、仮想 MAC アドレスを設定し、そのコンフィギュレーションをフラッシュ メモリに保存し、次にフェールオーバー ペアをリロードすることが最も良い方法です。アクティブ接続があるときに仮想 MAC アドレスが追加されると、そのアクティブ接続は停止します。また、**failover mac address** コマンドを含む完全なコンフィギュレーションをセカンダリ セキュリティ アプライアンスのフラッシュ メモリに書き込んで、仮想 MAC アドレッシングを有効にする必要があります。

failover mac address がプライマリ装置のコンフィギュレーションで指定された場合、それをセカンダリ装置のブートストラップ コンフィギュレーションでも指定する必要があります。

（注） このコマンドが適用されるのは、Active/Standby フェールオーバーのみです。Active/Active フェールオーバーでは、フェールオーバー グループ コンフィギュレーション モードの **mac address** コマンドを使用して、フェールオーバー グループのインターフェイスごとに仮想 MAC アドレスを設定します。

例

次の例では、intf2 という名前のインターフェイスに対してアクティブおよびスタンバイ MAC アドレスを設定します。

```
hostname(config)# failover mac address Ethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

関連コマンド

コマンド	説明
show interface	インターフェイス ステータス、設定、および統計情報を表示します。

failover polltime

フェールオーバー装置のポーリング期間および待機期間を指定するには、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期間および待機期間に戻すには、このコマンドの **no** 形式を使用します。

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

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

シンタックスの説明

holdtime *time*	（オプション）、装置がフェールオーバー リンクで hello メッセージを受信する期間を設定します。この期間が経過すると、ピア装置は障害状態であると宣言されます。 有効な値の範囲は 3 ～ 45 秒ですが、オプションの ***msec*** キーワードが指定されている場合は 800 ～ 999 ミリ秒となります。
msec	（オプション）指定する時間がミリ秒単位であることを指定します。
time	hello メッセージの間隔。 有効な値の範囲は 1 ～ 15 秒ですが、オプションの ***msec*** キーワードが指定されている場合は 200 ～ 999 ミリ秒となります。
unit	（オプション）装置のポーリング期間および待機期間にコマンドを使用することを指定します。 コマンドにこのキーワードを追加してもコマンドに影響しませんが、コンフィギュレーションでこのコマンドと **failover polltime interface** コマンドとの識別が容易になります。

デフォルト

PIX セキュリティ アプライアンス上のデフォルト値は次のとおりです。

- ポーリングの *time* は 15 秒です。
- **holdtime** *time* は 45 秒です。

ASA セキュリティ アプライアンス上のデフォルト値は次のとおりです。

- ポーリングの *time* は 1 秒です。
- **holdtime** *time* は 15 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**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*** というキーワードを含むようになりました。
7.2(1)	***msec*** キーワードが ***holdtime*** キーワードに追加されました。***polltime*** 最短値が 500 ミリ秒から 200 ミリ秒に短縮されました。***holdtime*** 最短値が 3 秒から 800 ミリ秒に短縮されました。

使用上のガイドライン

装置のポーリング時間の 3 倍未満の ***holdtime*** 値は入力できません。ポーリング時間が短いほど、セキュリティ アプライアンスは、それだけ速く障害を検出して、フェールオーバーを起動できます。ただし、検出が速すぎると、ネットワークが一時的に輻輳したときに不要な切り替えが発生する可能性があります。

hello パケットが、あるポーリング期間にフェールオーバー通信インターフェイスまたはケーブルで受信されない場合、追加テストが残りのインターフェイス全体で実施されます。待機期間内にピア装置から応答がない場合、この装置に障害が発生したと見なされ、障害が発生した装置がアクティブ装置であると、スタンドバイ装置が代わってアクティブ装置になります。

failover polltime [**unit**] コマンドと **failover polltime interface** コマンドの両方をコンフィギュレーションに含めることができます。

（注） CTIQBE トラフィックがフェールオーバー コンフィギュレーションのセキュリティ アプライアンスを通過するときは、セキュリティ アプライアンスのフェールオーバー待機時間を 30 秒より低く設定する必要があります。CTIQBE キープアライブ タイムアウトは 30 秒で、フェールオーバーの状況ではフェールオーバーが発生する前にタイムアウトする可能性があります。CTIQBE がタイムアウトした場合、Cisco CallManager への Cisco IP SoftPhone の接続はドロップされ、IP SoftPhone クライアントは CallManager を使用して再登録する必要があります。

例

次の例では、装置のポーリング間隔を 3 秒に設定します。

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

次の例では、hello パケットがその時間内にフェールオーバー インターフェイスで受信されない場合、セキュリティ アプライアンスが 200 ミリ秒ごとに hello パケットを送信し、800 ミリ秒でフェールオーバーするよう設定します。次のコマンドには、オプションの ***unit*** キーワードが含まれます。

```
hostname(config)# failover polltime unit msec 200 holdtime msec 800
```

関連コマンド

コマンド	説明
failover polltime interface	Active/Standby フェールオーバー コンフィギュレーションのインターフェイス ポーリング期間および待機期間を指定します。
polltime interface	Active/Active フェールオーバー コンフィギュレーションのインターフェイス ポーリング期間および待機期間を指定します。
show failover	フェールオーバー コンフィギュレーションの情報を表示します。

failover polltime interface

Active/Standby フェールオーバー コンフィギュレーションでデータ インターフェイスのポーリング期間と待機期間を指定するには、グローバル コンフィギュレーション モードで **failover polltime interface** コマンドを使用します。デフォルトのポーリング期間および待機期間に戻すには、このコマンドの **no** 形式を使用します。

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

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

シンタックスの説明

holdtime *time*	(オプション)データ インターフェイスがデータ インターフェイスで hello メッセージを受信する期間を設定します。この期間が経過すると、ピアは障害状態であると宣言されます。有効な値は 5 ～ 75 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時間を指定します。有効となる値の範囲は、3 ～ 15 秒です。オプションの ***msec*** キーワードを使用した場合、有効となる値は 500 ～ 999 ミリ秒です。
msec	（オプション）指定する時間がミリ秒単位であることを指定します。

デフォルト

デフォルト値は次のとおりです。

- ポーリングの *time* は 5 秒です。
- **holdtime** *time* は、ポーリングの *time* の 5 倍の値です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**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*** というキーワードを含むようになりました。
7.2(1)	オプションの ***holdtime*** *time* とミリ秒でポーリング期間を指定する機能が追加されました。

使用上のガイドライン

failover polltime interface コマンドを使用して、hello パケットをデータ インターフェイスで送信する頻度を変更します。このコマンドは、Active/Active フェールオーバーに対してのみ使用できます。Active/Active フェールオーバーの場合、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** コマンドを、**failover polltime interface** コマンドの代わりに使用します。

インターフェイスのポーリング時間の 5 倍未満の ***holdtime*** 値は入力できません。ポーリング時間が短いほど、セキュリティ アプライアンスは、それだけ速く障害を検出して、フェールオーバーを起動できます。ただし、検出が速すぎると、ネットワークが一時的に輻輳したときに不要な切り替えが発生する可能性があります。インターフェイスのテストが開始されるのは、待機期間の半分が経過したときに、インターフェイス上で hello パケットが受信されていない場合です。

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

（注） CTIQBE トラフィックがフェールオーバー コンフィギュレーションのセキュリティ アプライアンスを通過するときは、セキュリティ アプライアンスのフェールオーバー待機時間を 30 秒より低く設定する必要があります。CTIQBE キープアライブ タイムアウトは 30 秒で、フェールオーバーの状況ではフェールオーバーが発生する前にタイムアウトする可能性があります。CTIQBE がタイムアウトした場合、Cisco CallManager への Cisco IP SoftPhone の接続はドロップされ、IP SoftPhone クライアントは CallManager を使用して再登録する必要があります。

例

次の例では、インターフェイスのポーリング間隔を 15 秒に設定します。

```
hostname(config)# failover polltime interface 15
```

次の例では、インターフェイスのポーリング間隔を 500 ミリ秒、待機期間を 5 秒にそれぞれ設定します。

```
hostname(config)# failover polltime interface msec 500 holdtime 5
```

関連コマンド

コマンド	説明
failover polltime	装置のフェールオーバー ポーリング期間と待機期間を指定します。
polltime interface	Active/Active フェールオーバー コンフィギュレーションのインターフェイス ポーリング期間を指定します。
show failover	フェールオーバー コンフィギュレーションの情報を表示します。

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、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、フェールオーバー装置が同期しない場合に使用します。スタンバイ装置は、ブーティングが終了した後で、再起動してアクティブ装置に再度同期します。

例

次の例は、スタンバイ装置を強制的にリブートするために、アクティブ装置で **failover reload-standby** コマンドを使用する方法を示しています。

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

関連コマンド

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

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、引数もキーワードもありません。

デフォルト

ディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドが、**failover replicate http** から **failover replication http** に変更されました。

使用上のガイドライン

デフォルトでは、ステートフル フェールオーバーがイネーブルの場合、セキュリティ アプライアンスは HTTP セッション情報を複製しません。HTTP セッションは通常は存続期間が短く、HTTP クライアントは接続試行が失敗すると通常はリトライするため、HTTP セッションの複製をしないことでシステムのパフォーマンスが向上します。複製をしなくても重要なデータや接続は失われません。**failover replication http** コマンドは、ステートフル フェールオーバーの環境で HTTP セッションのステートフル複製をイネーブルにしますが、システムのパフォーマンスに悪影響を及ぼす可能性があります。

Active/Active フェールオーバー コンフィギュレーションでは、フェールオーバー グループ コンフィギュレーション モードの **replication http** コマンドを使用して、各フェールオーバー グループの HTTP セッションの複製を設定します。

例

次の例は、HTTP 接続の複製をイネーブルにする方法を示しています。

```
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 グループでの 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内の **failover** コマンドを表示します。

failover reset

障害が発生したセキュリティ アプライアンスを障害が発生する前の状態に戻すには、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	（オプション）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 グループの番号。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、オプションのフェールオーバー グループ ID を許可するように修正されました。

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が発生する前の状態に変更できます。**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でコマンドを入力することをお勧めします。アクティブ装置で **failover reset** コマンドを入力すると、スタンバイ装置を「unfail」にします。

装置のフェールオーバー ステータスは、**show failover** 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。

Active/Active フェールオーバーで **failover reset** を入力すると、装置全体がリセットされます。コマンドでフェールオーバー グループを指定すると、指定されたグループだけがリセットされます。

例

次の例は、障害が発生した装置を、障害が発生する前の状態に変更する方法を示しています。

```
hostname# failover reset
```

関連コマンド

コマンド	説明
failover interface-policy	モニタリングがインターフェイス障害を検出するとき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 timeout

非対称ルーテッド セッションのフェールオーバーの再接続タイムアウト値を指定するには、グローバル コンフィギュレーション モードで **failover timeout** コマンドを使用します。デフォルトのタイムアウト値に戻すには、このコマンドの **no** 形式を使用します。

failover timeout *hh*[**:***mm*:[**:***ss*]]

no failover timeout [*hh*[**:***mm*:[**:***ss*]]

シンタックスの説明

hh	タイムアウト値を時間単位で指定します。有効となる値の範囲は、-1 ～ 1,193 です。デフォルトでは、この値は 0 に設定されています。 この値を -1 に設定すると、タイムアウトがディセーブルにされ、任意の時間が経過した後でも接続を再開できます。 他のタイムアウト値を指定しないでこの値を 0 に設定すると、コマンドはデフォルト値に戻り、接続の再開はできません。**no failover timeout** コマンドも、この値をデフォルト（0）に設定します。 **（注）** デフォルト値に設定されている場合、このコマンドは実行コンフィギュレーション内に表示されません。
mm	（オプション）タイムアウト値を分単位で指定します。有効となる値の範囲は、0 ～ 59 です。デフォルトでは、この値は 0 に設定されています。
ss	（オプション）タイムアウト値を秒単位で指定します。有効となる値の範囲は、0 ～ 59 です。デフォルトでは、この値は 0 に設定されています。

デフォルト

デフォルトでは、*hh*、*mm*、および *ss* は 0 です。この設定では、再接続は行われません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドがコマンド リストに表示されるように修正されました。

使用上のガイドライン

このコマンドは、***nailed*** オプションを指定した **static** コマンドと共に使用します。***nailed*** オプションを使用すると、ブートアップ後またはシステムがアクティブになった後に、指定された時間内で接続を再確立できます。**failover timeout** コマンドは、その時間を指定します。設定しない場合は、接続を再確立できません。**failover timeout** コマンドは、**asr-group** コマンドに影響しません。

（注）　***nailed*** オプションを **static** コマンドに追加すると、その接続について、TCP のステート トラッキングおよびシーケンス チェッキングがスキップされます。

このコマンドの ***no*** 形式を入力すると、デフォルト値に戻ります。**failover timeout 0** を入力しても、デフォルト値に戻ります。デフォルト値に設定されている場合、このコマンドは実行コンフィギュレーション内に表示されません。

例

次の例では、スタンバイ グループ 1 をアクティブにしています。

```
hostname(config)# failover timeout 12:30
hostname(config)# show running-config failover
no failover
failover timeout 12:30:00
```

関連コマンド

コマンド	説明
static	ローカル IP アドレスをグローバル IP アドレスにマッピングすることによって、固定の 1 対 1 のアドレス変換規則を設定します。

file-bookmarks

認証された WebVPN ユーザに対して表示される WebVPN ホームページの File Bookmarks タイトルまたは File Bookmarks リンクをカスタマイズするには、webvpn カスタマイゼーション モードで **file-bookmarks** コマンドを使用します。

file-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

[**no**] **file-bookmarks** {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

link	リンクを変更することを指定します。
title	タイトルを変更することを指定します。
style	HTML スタイルを変更することを指定します。
text	テキストを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのリンクのスタイルは color:#669999;border-bottom: 1px solid #669999;text-decoration:none です。

デフォルトのタイトルのスタイルは color:#669999;background-color:#99CCCC;font-weight:bold です。

デフォルトのタイトルのテキストは「File Folder Bookmarks」です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。

- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、File Bookmarks のタイトルを「Corporate File Bookmarks」にカスタマイズします。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# file-bookmarks title text Corporate File Bookmarks
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの Application Access ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの Browse Networks ボックスをカスタマイズします。
web-applications	WebVPN ホームページの Web Application ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの Web Bookmarks タイトルまたはリンクをカスタマイズします。

file-encoding

Common Internet File System サーバからのページに対する文字エンコーディングを指定するには、webvpn コンフィギュレーション モードで **file-encoding** コマンドを使用します。**no** 形式は、file-encoding アトリビュートの値を削除します。

file-encoding {server-name | server-ip-addr} *charset*

no file-encoding {server-name | server-ip-addr}

シンタックスの説明

charset	最大 40 文字から成る文字列で、http://www.iana.org/assignments/character-sets で特定されている有効な文字セットのいずれかに相当するもの。上記のページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。たとえば、iso-8859-1、shift_jis、ibm850 などです。 この文字列は、大文字と小文字が区別されません。コマンド インタプリタは、セキュリティ アプライアンス コンフィギュレーションで、大文字を小文字に変換します。
server-ip-addr	文字エンコーディングを指定する CIFS サーバの IP アドレス（ドット 10 進表記）。
server-name	文字エンコーディングを指定する CIFS サーバの名前。 セキュリティ アプライアンスは指定した大文字や小文字を保持しますが、名前をサーバと照合する場合は大文字と小文字の区別を無視します。

デフォルト

WebVPN コンフィギュレーションに file-encoding エントリを明示的に持たないすべての CIFS サーバからのページは、character-encoding アトリビュートから文字エンコーディング値を継承します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

webvpn character-encoding アトリビュートの値とは異なる文字エンコーディングが必要なすべての CIFS サーバに対する file-encoding エントリを入力します。

CIFS サーバから WebVPN ユーザにダウンロードされた WebVPN ポータル ページは、サーバを識別する WebVPN file-encoding アトリビュートの値を符号化します。符号化が行われなかった場合は、character-encoding アトリビュートの値を継承します。リモート ユーザのブラウザは、この値を文字エンコーディング セットのエントリにマッピングして、使用する適切な文字セットを決定します。WebVPN コンフィギュレーションで CIFS サーバ用の file-encoding エントリが指定されてなく、character-encoding アトリビュートも設定されていない場合、WebVPN ポータル ページは値を指定し

ません。WebVPN ポータル ページが文字エンコーディングを指定しない場合、またはブラウザがサポートしていない文字エンコーディング値を指定した場合、リモート ブラウザはブラウザ自身のデフォルト エンコーディングを使用します。

CIFS サーバに適切な文字エンコーディングを、広域的には webvpn character-encoding アトリビュートによって、個別的には file-encoding の上書きによってマッピングすることで、ページと同様にファイル名やディレクトリ パスを適切にレンダリングすることが必要な場合には、CIFS ページの正確な処理と表示が可能になります。

（注）　character-encoding の値および file-encoding の値は、ブラウザによって使用されるフォント ファミリを排除するものではありません。日本語 Shift_JIS 文字エンコーディングを使用している場合、フォント ファミリを入れ替えるには、次の例で示すように webvpn カスタマイゼーション コマンド モードで **page style** コマンドを使用してこれらの値の設定を含めるか、webvpn カスタマイゼーション コマンド モードで **no page style** コマンドを入力して、フォント ファミリを削除する必要があります。

例

次の例では、「CISCO-server-jp」という名前の CIFS サーバの file-encoding アトリビュートが日本語 Shift_JIS 文字をサポートするように設定し、フォント ファミリを削除し、デフォルトの背景色を保持しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# file-encoding CISCO-server-jp shift_jis
F1-asa1(config-webvpn)# customization DfltCustomization
F1-asa1(config-webvpn-custom)# page style background-color:white
F1-asa1(config-webvpn-custom)#
```

次の例では、CIFS サーバ 10.86.5.174 の file-encoding アトリビュートが IBM860（エイリアス「CP860」）キャラクタをサポートするように設定します。

```
hostname(config)# webvpn
hostname(config-webvpn)# file-encoding 10.86.5.174 cp860
hostname(config-webvpn)
```

関連コマンド

コマンド	説明
character-encoding	すべての WebVPN ポータル ページ（WebVPN コンフィギュレーションの file-encoding エントリで指定されたサーバからのページを除く）で使用されるグローバルな文字エンコーディングを指定します。
show running-config [all] webvpn	WebVPN の実行コンフィギュレーションを表示します。デフォルトのコンフィギュレーションを含めるには、**all** キーワードを使用します。
debug webvpn cifs	Common Internet File System に関するデバッグ メッセージを表示します。

filter

このグループ ポリシーまたはユーザ名の WebVPN 接続に使用するアクセス リストの名前を指定するには、webvpn モードで **filter** コマンドを使用します。**filter none** コマンドを発行して作成されたヌル値を含むアクセス リストを削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できます。フィルタ値を継承しないようにするには、**filter value none** コマンドを使用します。

ACL を設定して、このユーザまたはグループ ポリシーについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**filter** コマンドを使用して、これらの ACL を WebVPN トラフィックに適用します。

filter {**value** *ACLname* | **none**}

no filter

シンタックスの説明

none	**webvpntype** アクセス リストがないことを示します。ヌル値を設定して、アクセス リストを拒否します。アクセス リストを他のグループ ポリシーから継承しないようにします。
value *ACLname*	設定済みアクセス リストの名前を指定します。

デフォルト

WebVPN アクセス リストは、**filter** コマンドを使用して指定するまで適用されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN モード	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

WebVPN は、**vpn-filter** コマンドで定義された ACL を使用しません。

例

次の例は、FirstGroup という名前のグループ ポリシーの *acl_in* という名前のアクセス リストを呼び出すフィルタを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# filter acl_in
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成します。または、ダウンロード可能なアクセス リストを使用します。
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル コンフィギュレーション値を設定できます。

filter activex

セキュリティ アプライアンスを通過する 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。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

filter activex | java <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*>

no filter activex | java <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*>

シンタックスの説明

port	フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 21 ですが、他の値でも受け入れられます。**http** または **url** リテラルをポート 21 に使用できます。許可される値の範囲は 0 ～ 65535 です。
-port	（オプション）ポートの範囲を指定します。
except	先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。
mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用して、すべての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になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ActiveX オブジェクトは、保護されたネットワーク上のホストやサーバを攻撃することを目的としたコードを含んでいる場合があるため、セキュリティ リスクになる恐れがあります。**filter activex** コマンドを使用して、ActiveX オブジェクトをディセーブルにできます。

ActiveX コントロールは、以前は OLE コントロールまたは OCX コントロールと呼ばれており、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、情報の収集や表示に使用するためのカスタム フォームや、カレンダ、多数のサードパーティ

フォームがあります。技術としては、ActiveX には、ネットワーク クライアントに対して起こる可能性のある問題、たとえば、ワークステーション障害の発生、ネットワーク セキュリティ問題の導入、またはサーバへの攻撃というような問題が数多く生じています。

filter activex コマンドは、HTML Web ページ内でコメント アウトすることにより HTML <object> コマンドをブロックします。HTML ファイルの ActiveX フィルタリングは、<APPLET> と </APPLET> および <OBJECT CLASSID> と </OBJECT> タグをコメントで選択的に置き換えることにより実行されます。入れ子タグのフィルタリングは、トップ レベルのタグをコメントに変換することでサポートされています。

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 オブジェクトでも使用されますが、これらも、このコマンドによってブロックされます。

<object> タグまたは </object> HTML タグがネットワーク パケット間で分割されている場合、またはタグ内のコードが MTU 内のバイト数よりも長い場合、セキュリティ アプライアンスはタグをブロックできません。

ActiveX ブロッキングは、***alias*** コマンドで参照されている IP アドレスにユーザがアクセスした場合、または WebVPN トラフィックの場合は実行されません。

（注）　ポート 80 に対して **filter activex** コマンドを **inspect im** コマンドと共に設定すると、**inspect im** コマンドはディセーブルになります。

例

次の例では、すべての発信接続で Activex オブジェクトがブロックされるように指定します。

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

このコマンドは、ポート 80 上において、あらゆるローカル ホストから来て、あらゆる外部ホスト接続へ向かう Web トラフィックに ActiveX オブジェクトのブロッキングが適用されることを指定します。

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 サーバに向けて送ります。
filter java	セキュリティ アプライアンスを通過する 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 コンフィギュレーションを表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter ftp

Websense サーバまたは N2H2 サーバによりフィルタリングされる FTP 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。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

filter ftp <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**interact-block**]

no filter ftp <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**interact-block**]

シンタックスの説明

port	フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 21 ですが、他の値でも受け入れられます。ポート 80 の代わりに、**ftp** リテラルを使用できます。
-port	（オプション）ポートの範囲を指定します。
except	先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。
mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
allow	（オプション）サーバが利用できなければ、発信接続はフィルタリングなしでセキュリティ アプライアンスを通過します。このオプションを省略した場合、および N2H2 サーバまたは Websense サーバがオフラインの場合、セキュリティ アプライアンスは発信ポート 80（Web）トラフィックを、N2H2 サーバまたは Websense サーバがオンラインに戻るまで、停止します。
interact-block	（オプション）ユーザが対話型の FTP プログラムを使用して FTP サーバに接続しないようにします。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

filter ftp コマンドは、Websense サーバまたは N2H2 サーバによってフィルタリングされる FTP トラフィックを特定します。

この機能をイネーブルにした後で、ユーザが FTP GET 要求をサーバに発行すると、セキュリティ アプライアンスは FTP サーバと Websense サーバまたは N2H2 サーバに同時に要求を送信します。Websense サーバまたは N2H2 サーバが接続を許可する場合、セキュリティ アプライアンスは正常な FTP の戻りコードが変更されずにユーザに到達することを許します。たとえば、正常な戻りコードは「250: CWD command successful」です。

Websense サーバまたは N2H2 サーバが接続を拒否する場合、セキュリティ アプライアンスは、FTP の戻りコードを接続が拒否されたことを表示するように変更します。たとえば、セキュリティ アプライアンスはコード 250 を「550 Requested file is prohibited by URL filtering policy」に変更します（Websense は FTP GET コマンドだけをフィルタリングし、PUT コマンドはフィルタリングしません）。

interactive-block オプションを使用して、ディレクトリ パス全体を提供しない対話型 FTP セッションを防ぎます。対話型 FTP クライアントでは、ユーザはパス全体を入力せずにディレクトリを変更できます。たとえば、ユーザは **cd /public/files** の代わりに **cd ./files** を入力する可能性があります。これらのコマンドを使用する前に、URL フィルタリング サーバを指定してイネーブルにする必要があります。

例

次の例は、FTP フィルタリングをイネーブルにする方法を示しています。

```
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 サーバまたは N2H2 サーバによってフィルタリングされる HTTPS トラフィックを指定します。
filter java	セキュリティ アプライアンスを通過する 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 サーバに向けて送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter https

N2H2 サーバまたは Websense サーバによりフィルタリングされる 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。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

filter https <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**]

no filter https <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**]

シンタックスの説明

port	フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 443 ですが、他の値でも受け入れられます。ポート 443 の代わりに、**https** リテラルを使用できます。
-port	（オプション）ポートの範囲を指定します。
except	（オプション）先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。
mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
allow	（オプション）サーバが利用できなければ、発信接続はフィルタリングなしでセキュリティ アプライアンスを通過します。このオプションを省略した場合、および N2H2 サーバまたは Websense サーバがオフラインの場合、セキュリティ アプライアンスは発信ポート 443 トラフィックを、N2H2 サーバまたは Websense サーバがオンラインに戻るまで、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になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

セキュリティ アプライアンスは、外部 Websense または N2H2 フィルタリング サーバを使用して、HTTPS サイトおよび FTP サイトのフィルタリングをサポートします。

HTTPS フィルタリングは、サイトが許可されない場合に SSL 接続ネゴシエーションの完了を防ぐことにより動作します。ブラウザには、「The Page or the content cannot be displayed」などのエラーメッセージが表示されます。

HTTPS のコンテンツは暗号化されているため、セキュリティ アプライアンスはディレクトリおよびファイル名の情報なしで URL ルックアップを送信します。

例

次の例では、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	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter java	セキュリティ アプライアンスを通過する 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 サーバに向けて送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter java

セキュリティ アプライアンスを通過する 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。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

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	フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 80 ですが、他の値でも受け入れられます。ポート 80 の代わりに、**http** または **url** リテラルを使用できます。
*port***-***port*	（オプション）ポートの範囲を指定します。
except	（オプション）先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。
local_mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用して、すべての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になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

Java アプレットは、保護されたネットワーク上のホストやサーバを攻撃することを目的としたコードを含んでいる場合があるため、セキュリティ リスクになる恐れがあります。**filter java** コマンドを使用して、Java アプレットを削除できます。

filter java コマンドは、発信接続からセキュリティ アプライアンスに返る Java アプレットをフィルタリングします。ユーザは、引き続き HTML ページを受信できますが、アプレットに対する Web ページのソースがコメント アウトされるため、アプレットは実行できません。**filter java** コマンドは WebVPN トラフィックをフィルタリングしません。

applet または /applet HTML タグがネットワーク パケット間で分割されている場合、またはタグ内のコードが MTU 内のバイト数よりも長い場合、セキュリティ アプライアンスはタグをブロックできません。Java アプレットは、<object> タグに含まれていることが分かっていれば、**filter activex** コマンドを使用して削除します。

（注）　ポート 80 に対して **filter java** コマンドを **inspect im** コマンドと共に設定すると、**inspect im** コマンドはディセーブルになります。

例

次の例では、すべての発信接続で Java アプレットがブロックされるように指定します。

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

このコマンドは、ポート 80 上において、あらゆるローカル ホストから来て、あらゆる外部ホスト接続へ向かう Web トラフィックに Java ブロッキングが適用されることを指定します。

次の例では、保護されたネットワーク上のホストに Java アプレットをダウンロードすることをブロックします。

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

このコマンドは、ホスト 192.168.3.3 が Java アプレットをダウンロードしないようにします。

関連コマンド

コマンド	説明
filter activex	セキュリティ アプライアンスを通過する 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 サーバに向けて送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter url

トラフィックを URL フィルタリング サーバに向けて送るには、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。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

filter url <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

no filter url <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

シンタックスの説明

allow	サーバが利用できなければ、発信接続はフィルタリングなしでセキュリティ アプライアンスを通過します。このオプションを省略した場合、および N2H2 サーバまたは Websense サーバがオフラインの場合、セキュリティ アプライアンスは発信ポート 80（Web）トラフィックを、N2H2 サーバまたは Websense サーバがオンラインに戻るまで、停止します。
cgi_truncate	URL のパラメータ リストに CGI スクリプトなどの疑問符（?）から始まるリストがある場合は、疑問符を含む疑問符以降のすべての文字を削除することにより、フィルタリング サーバに送信された URL を切り捨てます。
except	先行の **filter** 条件に対する例外を作成します。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
http	ポート 80 を指定します（ポート 80 を示す 80 の代わりに **http** または **www** を入力できます）。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。
local_mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用して、すべての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 バッファが利用できない場合に、URL 要求を拒否します。
longurl-truncate	URL が URL バッファの制限を超えている場合、発信ホスト名または発信 IP アドレスだけを N2H2 または Websense サーバに送信します。
mask	任意のマスク。
-*port*	（オプション）フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 80 ですが、他の値でも受け入れられます。ポート 80 の代わりに、**http** または **url** リテラルを使用できます。ハイフンの後に 2 番目のポートを追加すると、オプションでポートの範囲を指定します。
proxy-block	ユーザが HTTP プロキシ サーバに接続できないようにします。
url	セキュリティ アプライアンス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になっています。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　**filter url** コマンドを使用することで、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指示した World Wide Web URL に、発信ユーザがアクセスしないようにします。

（注）　**filter url** コマンドを実行するには、事前に **url-server** コマンドを設定する必要があります。

filter url コマンドの **allow** オプションは、N2H2 サーバまたは Websense サーバがオフラインになった場合のセキュリティ アプライアンスの動作を決定します。**filter url** コマンドで **allow** オプションを使用している場合、N2H2 サーバまたは Websense サーバがオフラインになると、ポート 80 トラフィックはフィルタリングなしでセキュリティ アプライアンスを通過します。**allow** オプションなしの場合、サーバがオフラインになると、セキュリティ アプライアンスはサーバがオンラインに戻るまで発信ポート 80（Web）のトラフィックを停止するか、または他の URL サーバが利用できる場合は、次の URL サーバに制御を渡します。

（注）　**allow** オプションが設定されている場合、N2H2 サーバまたは Websense サーバがオフラインになると、セキュリティ アプライアンスは制御を代替サーバに渡します。

N2H2 サーバまたは Websense サーバは、セキュリティ アプライアンスと共に動作して、企業のセキュリティ ポリシーに基づいて、ユーザが Web サイトにアクセスすることを拒否します。

フィルタリング サーバの使用

Websense プロトコル Version 4 は、グループとユーザ名の認証を、ホストとセキュリティ アプライアンスの間でイネーブルにします。セキュリティ アプライアンスがユーザ名のルックアップを実行し、次に、Websense サーバが URL フィルタリングとユーザ名ロギングを処理します。

N2H2 サーバは、IFP Server を実行している Windows ワークステーション（2000、NT、または XP）であり、推奨する最小メモリとして 512 MB RAM を搭載している必要があります。また、N2H2 サービス用の長い URL のサポートは、Websense の上限よりも少ない 3 KB に制限されます。

Websense プロトコルの Version 4 には、次の機能拡張があります。

- URL フィルタリングを使用すると、セキュリティ アプライアンスは、発信 URL 要求を Websense サーバ上に定義されているポリシーと照合してチェックします。
- ユーザ名ロギングは、Websense サーバ上のユーザ名、グループ、およびドメイン名を追跡します。

- ユーザ名ルックアップを使用すると、セキュリティ アプライアンスがユーザ認証テーブルを使用して、ホストの IP アドレスをユーザ名にマッピングできます。

Websense に関する情報は、次の Web サイトで利用できます。

http://www.websense.com/

設定手順

次の手順を実行して、URL フィルタリングを行います。

ステップ 1　N2H2 サーバまたは Websense サーバに **url-server** コマンドの該当するベンダー固有の形式を指示します。

ステップ 2　**filter** コマンドで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。ただし、このコマンドは Websense ログをアップデートしないため、Websense アカウンティング レポートに影響を与える可能性があります。**url-cache** コマンドを使用する前に Websense 実行ログを集めます。

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

長い URL の扱い

Websense フィルタリング サーバでは最大 4 KB の URL、N2H2 フィルタリング サーバでは最大 3 KB の URL がサポートされています。

最大の許可サイズよりも長い URL 要求を処理できるようにするには、***longurl-truncate*** および ***cgi-truncate*** オプションを使用します。

最大サイズよりも URL が長い場合、**longurl-truncate** オプションまたは **longurl-deny** オプションがイネーブルになっていないと、パケットはセキュリティ アプライアンスによりドロップされます。

longurl-truncate オプションを使用すると、許可された最大長よりも URL が長い場合、セキュリティ アプライアンスは URL のホスト名または IP アドレスの部分だけを評価のためにフィルタリング サーバに送信します。許可された最大長よりも URL が長い場合に発信 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。

パラメータなしで CGI スクリプトの場所とスクリプト名だけが含まれるように CGI URL を切り捨てるには、**cgi-truncate** オプションを使用します。長い HTTP 要求の多くは 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 リソースがすべて使われてセキュリティ アプライアンス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 サイトに接続する要求を発行すると、セキュリティ アプライアンスは Web サーバとフィルタリング サーバに同時に要求を送信します。フィルタリング サーバが Web コンテンツ サーバの前に応答しない場合、Web サーバからの応答はドロップされます。これが原因で、Web クライアントからは Web サーバの応答が遅れているように見えます。

HTTP 応答バッファをイネーブルにすることにより、Web コンテンツ サーバからの応答はバッファされ、フィルタリング サーバが接続を許可すると、応答は要求したユーザに転送されます。これにより、発生する可能性のある遅延を防ぎます。

HTTP の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 をバッファされるブロックの最大数で置き換えます。許可される値は、1 ～ 128 で、一度にバッファされることが可能な 1,550 バイトのブロック数を指定します。

（注）　ポート 80 に対して **filter url** コマンドを **inspect im** コマンドと共に設定すると、**inspect im** コマンドはディセーブルになります。

例

次の例では、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
```

次の例では、ポート 8080 上でリッスンするプロキシ サーバに向かう発信 HTTP 接続をすべてブロックします。

```
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	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter java	セキュリティ アプライアンスを通過する 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 サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは 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、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

fips enable

システムまたはモジュールで FIPS に準拠するためのポリシー チェックをイネーブルまたはディセーブルにするには、**fips enable** コマンドまたは [**no**] **fips enable** コマンドを使用します。

fips enable

[no] fips enable

シンタックスの説明

enable	FIPS に準拠するためのポリシー チェックをイネーブルまたはディセーブルします。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

FIPS 準拠の動作モードで実行するには、**fips enable** コマンドと、セキュリティ ポリシーに指定された正しい設定との両方を適用する必要があります。内部 API は、実行時に正しい設定を強制するためにデバイスが移行することを許可します。

「fips enable」がスタートアップ コンフィギュレーションにある場合、FIPS POST が実行されて、次のコンソール メッセージが表示されます。

```
Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set
forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights
clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical
Data and Computer Software clause at DFARS sec. 252.227-7013.

               Cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706

....
Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9

INFO: FIPS Power-On Self-Test in process.  Estimated completion in 90 seconds.
.................................................
INFO: FIPS Power-On Self-Test complete.
Type help or '?' for a list of available commands.
sw8-5520>
```

例

```
sw8-ASA(config)# fips enable
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に格納されているシステムまたはモジュールの FIPS コンフィギュレーション情報を消去します。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、および設定をディセーブルにします。
fips self-test poweron	パワーオン セルフテストを実行します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンス上で実行されている FIPS コンフィギュレーションを表示します。

fips self-test poweron

パワーオン セルフテストを実行するには、**fips self-test powereon** コマンドを使用します。

fips self-test poweron

シンタックスの説明

poweron	パワーオン セルフテストを実行します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを実行すると、デバイスは FIPS 140-2 準拠に要求されるすべてのセルフテストを実行します。テストは、暗号アルゴリズム テスト、ソフトウェア整合性テスト、およびクリティカル機能テストで構成されています。

例

```
sw8-5520(config)# fips self-test poweron
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に格納されているシステムまたはモジュールの FIPS コンフィギュレーション情報を消去します。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、および設定をディセーブルにします。
fips enable	システムまたはモジュールで FIPS に準拠するためのポリシーチェックをイネーブルまたはディセーブルにします。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンス上で実行されている FIPS コンフィギュレーションを表示します。

firewall transparent

ファイアウォール モードを透過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。透過的なファイアウォールは、「bump in the wire」または「stealth firewall」の機能を果たすレイヤ 2 のファイアウォールで、接続装置に対するルータ ホップとしては見られません。

firewall ***transparent***

no firewall ***transparent***

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

マルチ コンテキスト モードでは、すべてのコンテキストに対して 1 つのファイアウォール モードだけを使用できます。システム コンフィギュレーションでモードを設定する必要があります。このコマンドは、情報提供だけを目的として各コンテキスト コンフィギュレーションでも表示されますが、コンテキストにこのコマンドを入力することはできません。

コマンドの多くは両方のモードではサポートされていないため、モードを変更すると、セキュリティ アプライアンスによってコンフィギュレーションが消去されます。データが入力されたコンフィギュレーションがある場合、モードを変更する前にコンフィギュレーションをバックアップしてください。新しいコンフィギュレーションを作成するときに、このバックアップを参照として使用できます。

firewall transparent コマンドを使用してモードを変更するように設定されているセキュリティ アプライアンスに、テキスト コンフィギュレーションをダウンロードする場合は、そのコマンドをコンフィギュレーションの先頭に置くようにしてください。セキュリティ アプライアンスはコマンドを読み込むとすぐにモードを変更してから、ダウンロードしたコンフィギュレーションの読み込みを継続します。このコマンドがコンフィギュレーションの後ろの方に置かれていると、コンフィギュレーションでコマンドより前に置かれているラインはセキュリティ アプライアンスによりすべて消去されます。

例

次の例では、ファイアウォール モードを透過的なモードに変更します。

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

関連コマンド

コマンド	説明
arp-inspection	ARP 検査をイネーブルにして、ARP パケットをスタティック ARP エントリと比較します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show firewall	ファイアウォール モードを示します。
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、MAC アドレス テーブルを表示します。

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、非表示のシステム ファイルを含むファイル システム上のすべてのファイルを消去し、ファイル システムを再インストールします。

format {**disk0: | disk1: | flash:**}

シンタックスの説明

disk0:	後ろにコロンを付けて内蔵フラッシュ メモリを指定します。
disk1:	外部フラッシュ メモリ カードを指定し、続けてコロン (:) を入力します。
flash:	後ろにコロンを付けて内蔵フラッシュ メモリを指定します。ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

format コマンドは、指定されたファイル システム上のすべてのデータを消去し、デバイスに FAT 情報を再度書き込みます。

注意　***format*** コマンドは、破損したフラッシュ メモリをクリーン アップするのに必要な場合のみ、細心の注意を払って使用してください。

すべての可視ファイル（非表示のシステム ファイルを除く）を削除するには、***format*** コマンドではなく、***delete /recursive*** コマンドを使用します。

（注）　Cisco PIX セキュリティ アプライアンスでは、***erase*** コマンドと ***format*** コマンドは同じ処理を実行します。ユーザ データを 0xFF パターンを使用して破棄します。

破損したファイル システムを修復する場合は、**format** コマンドを入力する前に **fsck** コマンドを入力してみてください。

（注）　Cisco ASA 5500 シリーズのセキュリティ アプライアンスでは、***erase*** コマンドを実行すると、ディスク上のすべてのユーザ データが 0xFF パターンを使用して破棄されます。一方、***format*** コマンドはファイル システムの制御構造をリセットするだけです。生ディスク読み取りツールを使用すると、この情報はまだ参照できる可能性があります。

破損したファイル システムを修復する場合は、**format** コマンドを入力する前に **fsck** コマンドを入力してみてください。

例

この例は、フラッシュ メモリをフォーマットする方法を示しています。

```
hostname# format flash:
```

関連コマンド

コマンド	説明
delete	ユーザから見え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	破損したファイル システムを修復します。

forward interface

スイッチが組み込まれたモデル（ASA 5505 適応型セキュリティ アプライアンスなど）では、インターフェイス コンフィギュレーション モードで **no forward interface** コマンドを使用して、ある VLAN が別の VLAN にアクセスすることを制限します。このコマンドを入力できるのは、VLAN インターフェイスのインターフェイス コンフィギュレーション モードだけです。接続できるように戻すには、**forward interface** コマンドを使用します。ライセンスによってサポートされる VLAN の数によっては、1 つの VLAN だけに制限しなければならないことがあります。

forward interface vlan *number*

no forward interface vlan *number*

シンタックスの説明

vlan *number*	この VLAN インターフェイスがトラフィックを開始できない VLAN ID を指定します。

デフォルト

デフォルトでは、すべてのインターフェイスは他のいずれのインターフェイスに対してもトラフィックを開始できます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ルーテッド モードでは、ASA 5505 適応型セキュリティ アプライアンスの Base ライセンスの場合、アクティブな VLAN を 3 つまで、Security Plus ライセンスの場合は 5 つまで設定できます。アクティブな VLAN とは、**nameif** コマンドが設定されている VLAN です。どちらのライセンスでも、非アクティブな VLAN を ASA 5505 適応型セキュリティ アプライアンス上に 5 つまで設定できますが、それらの VLAN をアクティブにする場合は、ライセンスに関する次のガイドラインを遵守してください。

Base ライセンスの場合、3 つ目の VLAN を **no forward interface** コマンドで設定し、この VLAN による別の VLAN へのアクセスを制限する必要があります。

たとえば、インターネット アクセス用に外部に割り当てた VLAN が 1 つ、内部ワーク ネットワーク用に割り当てた VLAN が 1 つ、さらにホームネットワーク用に割り当てた 3 つ目の VLAN があるとします。ホーム ネットワークはワーク ネットワークにアクセスする必要はありません。そのためホーム VLAN には **no forward interface** コマンドを使用します。ワーク ネットワークはホームネットワークにアクセスできますが、ホームネットワークはワーク ネットワークにアクセスできません。

nameif コマンドで設定した VLAN インターフェイスがすでに 2 つある場合、**no forward interface** コマンドを入力してから、3 つ目のインターフェイスで **nameif** コマンドを入力します。セキュリティ アプライアンスでは、ASA 5505 適応型セキュリティ アプライアンスで Base ライセンスの場合、3 つの VLAN インターフェイスが完全に機能することを許可しません。

例

次の例では、3 つの LAN インターフェイスを設定しています。3 つ目のホーム インターフェイスはトラフィックをワーク インターフェイスに転送できません。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address dhcp
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif work
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# no forward interface vlan 200
hostname(config-if)# nameif home
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
backup interface	たとえば、インターフェイスをバックアップ リンクとして ISP に割り当てます。
clear interface	**show interface** コマンドのカウンタを消去します。
interface vlan	VLAN インターフェイスを作成し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。

fqdn

登録中に、指定された FQDN を証明書のサブジェクト代替名の拡張に含めるには、暗号 CA トラストポイント コンフィギュレーション モードで **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* | **none**]

no fqdn

シンタックスの説明

fqdn	完全修飾ドメイン名を指定します。*fqdn* の最大長は 64 文字です。
none	非完全修飾ドメイン名を指定します。

デフォルト

デフォルト設定では、FQDN は含まれません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

証明書を使用する Nokia VPN クライアントの認証をサポートするセキュリティ アプライアンスを設定する場合、**none** キーワードを使用します。Nokia VPN クライアントの証明書認証に関する詳細は、**crypto isakmp identity** コマンドまたは **isakmp identity** コマンドを参照してください。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central の登録要求に FQDN エンジニアリングを含めます。

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# fqdn engineering
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。
enrollment retry period	登録要求の送信を試行するまでの待機時間を、分単位で指定します。
enrollment terminal	このトラストポイントを使用したカット アンド ペースト登録を指定します。

fragment

特別なパケット フラグメント化の管理を提供して NFS との互換性を向上させるには、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。

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 パケットがフラグメント化されるパケット数の最大値を示す。
interface	（オプション）セキュリティ アプライアンスのインターフェイスを指定します。インターフェイスが指定されていなければ、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*	再構成のために待機している IP 再構成データベースに含めることができる、パケットの最大数を設定します。
timeout *limit*	フラグメント化されたパケット全体の到着を待つ最大秒数を指定します。タイマーは、パケットの最初のフラグメントが到着すると始動します。指定した秒数以内にパケットのすべてのフラグメントが到着しない場合、それまでに受信したパケット フラグメントはすべて廃棄されます。

デフォルト

デフォルトは次のとおりです。

- ***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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、***chain***、***size***、または ***timeout*** のいずれかの引数を必ず選択するように変更されました。ソフトウェアの以前のリリースでサポートされていた、これらの引数を入力しない ***fragment*** コマンドは、入力できなくなりました。

使用上のガイドライン

デフォルトでは、セキュリティ アプライアンスは、完全な IP パケットの再構築をするために、最大 24 個のフラグメントを受け入れます。ネットワーク 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ついて **fragment chain 1** *interface* コマンドを入力することで、フラグメント化されたパケットがセキュリティ アプライアンスを通過できなくするようにセキュリティ アプライアンスの設定を検討する必要があります。制限に 1 を設定すると、すべてのパケットが元のまま、つまり、フラグメント化されていない状態である必要があります。

セキュリティ アプライアンス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、さらに調整が必要になる可能性があります。

WAN インターフェイスなどのように NFS サーバとクライアントの間の MTU サイズが小さな環境では、**chain** キーワードをさらに調整する必要があります。この場合、効率を改善するには NFS over TCP の使用を推奨します。

size *limit* に大きな値を設定すると、セキュリティ アプライアンスは、さらにフラグメント フラッディングによる DoS 攻撃を受けやすくなります。***size limit*** に 1550 プールまたは 16384 プール内のブロックの総数以上の値を設定しないでください。

デフォルト値では、フラグメント フラッディングによって発生する DoS 攻撃が制限されます。

例

次の例は、フラグメント化したパケットを外部および内部のインターフェイスで防ぐ方法を示しています。

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

パケットのフラグメント化をさせない追加インターフェイスそれぞれに対して、続けて **fragment chain 1** *interface* コマンドを入力します。

次の例では、外部インターフェイスのフラグメント データベースを、最大サイズ 2000、最大チェイン長 45、待ち時間 10 秒に設定する方法を示しています。

```
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コンフィギュレーションを、デフォルトにリセットします。
clear fragment	IP フラグメント再構成モジュールの運用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運用データを表示します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

frequency

選択した SLA オペレーションが繰り返される頻度を設定するには、SLA モニタ プロトコル コンフィギュレーション モードで **frequency** 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。

frequency *seconds*

no frequency

シンタックスの説明

seconds	SLA プローブ間の秒数。有効な値は 1 ～ 604,800 秒です。この値は **timeout** 値未満にはできません。

デフォルト

デフォルトの間隔は 60 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SLA モニタ 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	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

SLA オペレーションは動作中、指定の頻度で繰り返し実行されます。たとえば、60 秒の頻度に設定した ***ipIcmpEcho*** オペレーションは動作中、エコー要求パケットの送信を 60 秒ごとに 1 度繰り返し実行します。たとえば、エコー オペレーションのデフォルトのパケット数は 1 です。このパケットは、オペレーションの開始時に送信され、60 秒後に再度送信されます。

個々の SLA オペレーションで、指定した頻度値より実行に時間がかかる場合、busy という統計カウンタの値が増え、オペレーションはすぐに繰り返されません。

frequency コマンドに指定する値は、**timeout** コマンドに指定した値未満にはできません。

例

次の例では、ID が 123 の SLA オペレーションを設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。SLA オペレーションの頻度は 3 秒、タイムアウト値は 1000 ミリ秒に設定されます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
sla monitor	SLA 監視オペレーションを定義します。
timeout	SLA オペレーションが応答を待機する期間を定義します。

fsck

ファイル システムのチェックを実行し、破損を修復するには、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	オプション。修復確認のためのプロンプトを表示しません。
disk0:	後ろにコロンを付けて内蔵フラッシュ メモリを指定します。
disk1:	外部フラッシュ メモリ カードを指定し、続けてコロン (:) を入力します。
flash:	後ろにコロンを付けて内蔵フラッシュ メモリを指定します。ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

fsck コマンドは破損したファイル システムをチェックし、修復を試みます。他の方法を用いる前に、まずこのコマンドを使用してください。

/noconfirm キーワードは、最初に確認を求めずに破損を自動的に修復します。

例

次の例では、フラッシュ メモリのファイル システムのチェック方法を示しています。

```
hostname# fsck flash:
```

関連コマンド

コマンド	説明
delete	ユーザから見え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	ファイル システム上にある非表示のシステム ファイルを含むすべてのファイルを削除し、ファイル システムを再インストールします。

ftp mode passive

FTP 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になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ftp mode passive コマンドは、FTP モードをパッシブに設定します。セキュリティ アプライアンスは、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 FTP サーバへのアップロードや FTP サーバからのダウンロードに FTP を使用できます。**ftp mode passive** コマンドは、セキュリティ アプライアンス上の FTP クライアントが FTP サーバと対話する方法を設定します。

パッシブ FTP では、クライアントが制御接続とデータ接続の両方を開始します。パッシブ モードはサーバ状態を参照します。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と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の両方が一時ポートです（1023 より大きい）。クライアントが **passive** コマンドを発行してパッシブなデータ接続の設定を開始するため、このモードはクライアントにより設定されます。パッシブ モードでのデータ接続の受信者であるサーバは、特定の接続をリッスンしているポート番号で応答します。

例

次の例では、FTP モードをパッシブに設定します。

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

関連コマンド

copy	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 FTP サーバとの間で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な情報を表示します。
show running-config ftp mode	FTP クライアントのコンフィギュレーションを表示します。

functions

このユーザまたはグループ ポリシーに対して、WebVPN 経由でポート フォワーディング java アプレット、Citrix サポート、ファイル アクセス、ファイル ブラウジング、ファイル サーバ エントリ、webtype ACL のアプリケーション、HTTP プロキシ、MAPI プロキシ、ポート フォワーディング、または URL エントリに関する自動ダウンロードを設定するには、グループ ポリシーまたはユーザ名モードから入力する webvpn モードで **functions** コマンドを使用します。設定済み機能を削除するには、このコマンドの **no** 形式を使用します。

functions none コマンドを発行して作成されたヌル値を含むすべての設定済み機能を削除するには、このコマンドの **no** 形式を引数なしで使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できます。機能の値を継承しないようにするには、**functions none** コマンドを使用します。

functions {**auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **http-proxy** | **url-entry** | **mapi** | **port-forward** | **none**}

no functions [**auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **url-entry** | **mapi** | **port-forward**]

シンタックスの説明

auto-download	WebVPN ログインの際に、ポート フォワーディング java アプレットの自動ダウンロードをイネーブルまたはディセーブルにします。最初にポート フォワーディング、Outlook/Exchange プロキシ、または HTTP プロキシをイネーブルにする必要があります。
citrix	MetaFrame アプリケーション サーバからリモート ユーザへの端末サービスのサポートを、イネーブルまたはディセーブルにします。このキーワードを使用すると、セキュリティ アプライアンスがセキュリティの高い Citrix コンフィギュレーション内でセキュアなゲートウェイとして動作できます。これらのサービスにより、ユーザは標準の Web ブラウザから MetaFrame アプリケーションにアクセスできます。
file-access	ファイル アクセスをイネーブルまたはディセーブルにします。イネーブルの場合、WebVPN のホームページにはサーバ リスト内のファイル サーバが一覧表示されます。ファイル ブラウジングまたはファイル エントリをイネーブルにするには、ファイル アクセスをイネーブルにする必要があります。
file-browsing	ファイル サーバおよび共有のブラウジングをイネーブルまたはディセーブルにします。ファイル サーバのユーザ エントリを許可するには、ファイル ブラウジングをイネーブルにする必要があります。
file-entry	ファイル サーバの名前を入力するユーザ機能をイネーブルまたはディセーブルにします。
filter	webtype ACL を適用します。イネーブルにすると、セキュリティ アプライアンスは webvpn の **filter** コマンドで定義された webtype ACL を適用します。
http-proxy	リモート ユーザへの HTTP アプレット プロキシの転送をイネーブルまたはディセーブルにします。プロキシは、Java、ActiveX、および Flash などの独特のマングリングに干渉するテクノロジーに効果的です。プロキシを使用するとマングリングはバイパスされますが、セキュリティ アプライアンスの使用は確実に継続されます。転送されたプロキシはブラウザの古いプロキシ設定を自動的に変更し、すべての HTTP および HTTPS 要求を新しいプロキシ設定にリダイレクトします。HTML、CSS、JavaScript、VBScript、ActiveX、および Java を含む、すべてのクライアント側のテクノロジーを実質的にサポートします。サポートしているブラウザは、Microsoft Internet Explorer だけです。

mapi	Microsoft Outlook/Exchange のポート転送をイネーブルまたはディセーブルにします。
none	すべての WebVPN **functions** にヌル値を設定します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから機能を継承しないようにします。
port-forward	ポート転送をイネーブルにします。イネーブルにすると、セキュリティ アプライアンスは webvpn の **port-forward** コマンドで定義されたポート フォワーディング リストを使用します。
url-entry	URL のユーザ エントリをイネーブルまたはディセーブルにします。イネーブルになっても、セキュリティ アプライアンスは依然として URL を任意の設定された URL またはネットワーク ACL に制限します。URL エントリをディセーブルにすると、セキュリティ アプライアンスは WebVPN ユーザをホームページ上の URL に制限します。

デフォルト

デフォルトでは、この機能はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	auto-download キーワードと citrix キーワードが追加されました。
7.0(1)	このコマンドが導入されました。

例

次の例は、FirstGroup という名前のグループ ポリシーに対してファイル アクセス、ファイル ブラウジング、および MAPI プロキシを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# functions file-access file-browsing MAPI
```

関連コマンド

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