failover コマンド ～ fast-flood コマンド

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。

フェールオーバー

no failover

構文の説明　このコマンドには引数またはキーワードはありません。

デフォルト　フェールオーバーはディセーブルです。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

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のフェールオーバーのイネーブルまたはディセーブルに限定されました（**failover active** コマンドを参照）。

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 ASA 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 リスクになるおそれがあります。ASA 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が、Easy VPN ハードウェア クライアントとして動作していないときにのみ許可されます。

例

次に、フェールオーバーをディセーブルにする例を示します。

```
ciscoasa(config)# no failover
ciscoasa(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	スタンバイ ユニットをアクティブに切り替えます。
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の **failover** コマンドを表示します。

failover active

スタンバイの ASA またはフェールオーバー グループをアクティブ ステートに切り替えるには、特権 EXEC モードで **failover active** コマンドを使用します。アクティブな ASA 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*]

構文の説明

group *group_id*	(任意)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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、フェールオーバー グループを含むように変更されました。

使用上のガイドライン

スタンバイ ユニットからのフェールオーバー切り替えを開始するには **failover active** コマンドを使用し、アクティブ ユニットからのフェールオーバー切り替えを開始するには **no failover active** コマンドを使用します。この機能を使用して、障害が発生したユニットを稼働させたり、メンテナンスのためにアクティブ ユニットをオフラインにしたりできます。ステートフル フェールオーバーを使用していない場合、すべてのアクティブ接続がドロップされるため、クライアントはフェールオーバーの発生後、接続を再確立する必要があります。

フェールオーバー グループの切り替えは、Active/Active フェールオーバーでのみ使用できます。Active/Active フェールオーバー ユニットでフェールオーバー グループを指定しないで **failover active** コマンドを入力すると、ユニットのすべてのグループがアクティブになります。

例

次に、スタンバイ グループ 1 をアクティブに切り替える例を示します。

```
ciscoasa# failover active group 1
```

関連コマンド

コマンド	説明
failover reset	ASA を、障害が発生した状態からスタンバイに変更します。

failover cloud authentication

ASAv でサービス プリンシパルを使用した Microsoft Azure への認証ができるようにするには、グローバル コンフィギュレーション モードで **failover cloud authentication** コマンドを使用します。Microsoft Azure 認証を無効にするには、このコマンドの **no** 形式を使用します。

failover cloud authentication {**application-id** *appl-id* | **directory-id** *dir-id* | **key** *secret-key*}

no failover cloud authentication {**application-id** *appl-id* | **directory-id** *dir-id* | **key** *secret-key* [**encrypt**]}

構文の説明

application-id *appl-id*	Azure インフラストラクチャからアクセス キーを要求するときに必要なアプリケーション ID を指定します。
directory-id *dir-id*	Azure インフラストラクチャからアクセス キーを要求するときに必要なディレクトリ ID を指定します。
key *secret-key*	Azure インフラストラクチャからアクセス キーを要求するときに必要な秘密キーを指定します。**encrypt** キーワードが存在する場合、この秘密キーは実行コンフィギュレーションで暗号化されます。

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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

自動的に API 呼び出しによって Azure ルート テーブルが変更されるようにするには、ASAv HA ユニットに Azure Active Directory のクレデンシャルが必要です。Azure は、簡単に言えばサービス アカウントであるサービス プリンシパルの概念を採用しています。サービス プリンシパルを使用すると、あらかじめ定義された Azure リソース セット内でタスクを実行するのに十分な権限と範囲のみを持つアカウントをプロビジョニングできます。

Azure リソース（ルート テーブルなど）へのアクセスまたはリソースの変更が必要となるアプリケーションがある場合は、Azure Active Directory（AD）アプリケーションを設定し、必要な権限を割り当てる必要があります。

Azure ポータルに Azure AD アプリケーションを登録すると、アプリケーション オブジェクトとサービス プリンシパル オブジェクトの 2 つのオブジェクトが Azure AD テナントに作成されます。サービス プリンシパル オブジェクトは、特定のテナントでのアプリケーションの使用に関するポリシーと権限を定義し、アプリケーション実行時のセキュリティ プリンシパルの基礎を提供します。

サービス プリンシパルを設定したら、**ディレクトリ ID**、**アプリケーション ID**、および**秘密キー**を取得します。これらは、Azure 認証クレデンシャルを設定するために必要です。

(注) Azure は、『*Azure Resource Manager Documentation*』で Azure AD アプリケーションとサービス プリンシパルを作成する方法について説明しています。

例

次に、パブリック クラウド フェールオーバー コンフィギュレーションに Azure 認証クレデンシャルを追加する例を示します。

```
(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-6931704e420
(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138b77ae9
(config)# failover cloud authentication key 5yOhH593dtD/O8gzAlWgulrkWz5dH02d2STk3LDbI4c=
(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	スタンバイ ユニットをアクティブに切り替えます。
failover cloud subscription-id	パブリック クラウド フェールオーバー コンフィギュレーションに Azure サブスクリプション ID を追加します。
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の **failover** コマンドを表示します。

failover cloud peer

パブリック クラウド フェールオーバー ピアを設定するには、グローバル コンフィギュレーション モードで **failover cloud peer** コマンドを使用します。フェールオーバー ピアを無効にするには、このコマンドの **no** 形式を使用します。

failover cloud peer {**ip** *ip-address* | **port** *port-number*}

no failover cloud peer

構文の説明

ip *ip-address*	パブリック クラウド HA ピアへの TCP フェールオーバー制御接続を確立するために使用する IP アドレスを指定します。
port *port-number*	Azure インフラストラクチャからアクセス キーを要求するときに必要なディレクトリ ID を指定します。

デフォルト

デフォルトは、**failover cloud port control** コマンドによって指定されたポート番号（指定されていない場合はデフォルトのポート番号）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

パブリック クラウド HA ピアへの TCP フェールオーバー制御接続を確立するには、IP アドレスが使用されます。すでにアクティブ ユニットである可能性がある HA ピアへのフェールオーバー接続を開こうとする場合は、ポートが使用されます。HA ピア間で NAT が 実行されている場合は、ここでのポートの設定が必要となる場合があります。この設定は、ほとんどの場合不要です。

このコマンドの **no** 形式を使用すると、ピアとなる IP アドレスが削除され、ポート番号がそのデフォルト値に設定されます。ポートが指定されていない場合、ポート番号は、以前にこのコマンドを使用して別の値が設定されていた場合であってもデフォルト値に設定されます。

例

次に、パブリック クラウド フェールオーバー ピアを設定する例を示します。

```
ciscoasa(config)# failover cloud peer ip 10.4.3.5 port 4444
ciscoasa(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	スタンバイ ユニットをアクティブに切り替えます。
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の **failover** コマンドを表示します。

failover cloud polltime

パブリック クラウドのフェールオーバー ユニットのポーリング タイムおよびホールド タイムを指定するには、グローバル コンフィギュレーション モードで **failover cloud 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ホールド タイムに戻すには、このコマンドの **no** 形式を使用します。

failover cloud polltime *poll_time* [**holdtime** *time*]

no failover cloud polltime

構文の説明

holdtime *time*	(任意)ユニットが制御ポートで hello メッセージを受信する間隔を設定します。この時間を経過すると、ピア ユニットで障害が発生したと見なされます。 有効な値は 3 ～ 60 秒です。装置のポーリング時間の 3 倍に満たない保持時間は入力できません。
polltime *poll_time*	hello メッセージ間の時間を設定します。 有効な値は 1 ～ 15 秒です。

デフォルト

ASAv のデフォルト値は次のとおりです。

- **polltime** *poll_time* は 5 秒です。
- **holdtime** *time* は 15 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

バックアップ ユニットがアクティブ ユニットの存在をモニタするために使用するポーリング間隔を設定するために使用されます。必要に応じ、アクティブ ユニットからの応答がない場合に、バックアップ ユニットがアクティブなロールを取る前に待機する時間（ホールド タイム）も設定できます。ホールド タイムは、強制的にポーリング タイムの 3 倍以上となります。ポーリング間隔を短くすると、ASA で障害を検出し、フェールオーバーをトリガーする速度が速くなります。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。

例

次に、パブリック クラウド フェールオーバー コンフィギュレーションでフェールオーバー ポーリングを設定する例を示します。

```
ciscoasa(config)# failover cloud polltime 10 holdtime 30
```

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	スタンバイ ユニットをアクティブに切り替えます。
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の **failover** コマンドを表示します。

failover cloud port

パブリック クラウド フェールオーバーのペアによって使用される 2 つの TCP ポート、2 つのピア間のフェールオーバー通信に使用するポート、および Azure ロード バランサのプローブに使用するポートを指定するには、グローバル コンフィギュレーション モードで **failover cloud port** コマンドを使用します。これらのポートをデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

failover cloud port {**control** *port-number* | **probe** *port-number* [**interface** if-name]}

no failover cloud port {**control** | **probe**}

構文の説明

control *port-number*	(任意)パブリック クラウド HA ピアとの通信に使用する TCP ポートを指定します。
probe *port-number*	(任意)Azure ロード バランサの健全性プローブへの応答に使用する TCP ポートを指定します。
interface if-name	(任意)Azure ロード バランサ プローブを受け入れるプローブ ポート用に設定するインターフェイスを指定します。省略すると、プローブは、プローブによって使用されるよく知られた送信元 IP アドレス(168.63.129.16)に到達するために最適であると、ASAv 内の IP ルーティング機能によって判断されるインターフェイスに受け入れられます。

デフォルト

パブリック クラウド フェールオーバーの TCP 制御ポート番号は 44442 です。

Azure ロード バランサの健全性プローブ ポート番号は 44441 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

デフォルトのポート値に戻すには、このコマンドの **no** 形式を使用します。

物理 ASA および非パブリック クラウドの仮想 ASA では、Gratuitous ARP 要求を使用してフェールオーバー条件を処理しますが、バックアップ ASA は、アクティブな IP アドレスと MAC アドレスに関連付けられていることを示す Gratuitous ARPP を送信します。ほとんどのパブリック クラウド環境では、このようなブロードキャスト トラフィックは許可されていません。このため、パブリック クラウドの HA 設定では、フェールオーバーが発生したときに通信中の接続を再起動する必要があります。

アクティブ装置の状態がバックアップ装置によってモニタされ、所定のフェールオーバー条件に一致しているかどうかが判別されます。所定の条件に一致すると、フェールオーバーが行われます。フェールオーバー時間は、パブリック クラウド インフラストラクチャの応答性に応じて、数秒～ 1 分を超える場合があります。

例

次に、パブリック クラウド フェールオーバー コンフィギュレーションに対し、フェールオーバー通信および Azure ロード バランサ プローブのための TCP ポートを設定する例を示します。

```
ciscoasa(config)# failover cloud port control 4444
ciscoasa(config)# failover cloud port probe 4443
```

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	スタンバイ ユニットをアクティブに切り替えます。
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の **failover** コマンドを表示します。

failover cloud route-table

内部ルートをアクティブ ユニットに向ける Azure ルート テーブルを設定するには、グローバル コンフィギュレーション モードで **failover cloud route-table** コマンドを使用します。ルート テーブル 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。

failover cloud route-table *table-name* [**subscription-id** *sub-id*]

no failover cloud route-table

構文の説明

table-name	ルート テーブルの名前を指定します。
subscription-id *sub-id*	(任意) Azure リソースを変更する際に必要な Azure サブスクリプション ID を指定します。ルート テーブル内にこのパラメータが存在する場合、それは、ルート テーブルを参照する際に使用される Azure サブスクリプションです。省略すると、グローバル コンフィギュレーション モードで設定されているサブスクリプション ID が使用されます。

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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。
9.9(2)	**subscription-id** パラメータが導入されました。

使用上のガイドライン

フェールオーバーでは、内部ルートをアクティブ装置に向ける必要があります。アクティブ装置は、設定されたルート テーブル情報を使用して自動的にルートを自身に向けます。

プライマリ装置とセカンダリ装置の両方でこれらの設定を構成します。プライマリ装置からセカンダリ装置への設定の同期はありません。

2 つ以上の Azure サブスクリプションでユーザ定義のルートを更新するには、オプションの **subscription-id** パラメータを使用します。**route-table** コマンド レベルの **subscription-id** は、グローバル レベルで指定された Azure サブスクリプション ID を上書きします。**subscription-id** を指定せずに **route-table** コマンドを入力すると、グローバル パラメータが使用されます。

ルート テーブル 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。

(注) このコマンドを入力すると、ASAv は **cfg-fover-cloud-rt** モードに切り替わります。

例

次の例では、パブリック クラウド フェールオーバーのルート テーブル コンフィギュレーションで cfg-fover-cloud-rt モードを有効にする方法を示します。

```
ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)#

ciscoasa(config)# failover cloud route-table inside-rt subscription-id cd5fe6b4-d2ed-45
ciscoasa(cfg-fover-cloud-rt)#
```

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。
rg	パブリック クラウド フェールオーバー コンフィギュレーションに Azure リソース グループを追加します。
route-table	パブリック クラウド フェールオーバー コンフィギュレーションに Azure ルート情報を追加します。
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の **failover** コマンドを表示します。
failover cloud subscription-id	パブリック クラウド フェールオーバー コンフィギュレーションに Azure サブスクリプション ID を追加します。

failover cloud route-table rg

ルート テーブル更新要求に必要な Azure リソース グループを設定するには、cfg-fover-cloud-rt コンフィギュレーション モードで **rg** コマンドを使用します。コンフィギュレーションからリソース グループ情報を削除するには、このコマンドの **no** 形式を使用します。

rg *resource-group*

no rg

構文の説明

resource-group	Azure リソース グループの名前を指定します。

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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

Azure リソース グループは、Azure ソリューション用の関連リソースを保持するコンテナです。リソース グループには、ソリューション用のすべてのリソースを含めるか、またはグループとして管理するリソースのみを含めることができます。リソース グループにリソースを割り当てる方法は、どうすれば組織にとって最も合理的になるかを考慮して決定します。

プライマリ装置とセカンダリ装置の両方でこれらの設定を構成します。プライマリ装置からセカンダリ装置への設定の同期はありません。

コンフィギュレーションからリソース グループ情報を削除するには、このコマンドの **no** 形式を使用します。

(注) Azure は、『*Azure Resource Manager Documentation*』でリソース グループについて説明しています。

例

次に、パブリック クラウド フェールオーバー コンフィギュレーションに Azure リソース グループを追加する例を示します。

```
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)#
```

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。
rg	パブリック クラウド フェールオーバー コンフィギュレーションに Azure リソース グループを追加します。
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の **failover** コマンドを表示します。

failover cloud route-table route

フェールオーバー中に更新を必要とするルートを設定するには、cfg-fover-cloud-rt コンフィギュレーション モードで **route** コマンドを使用します。コンフィギュレーションからルート情報を削除するには、このコマンドの **no** 形式を使用します。

route {**name** *route-name* **prefix** *address-prefix* **nexthop** *ip-address*}

no route name *route-name*

構文の説明

route-name	ルートの名前を指定します。
address-prefix	IP アドレス プレフィックス、スラッシュ（「/」）、および数字のネットマスクとして設定されるアドレス プレフィックスを指定します。例: 192.120.0.0/16。
ip-address	ネクスト ホップの 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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

フェールオーバーでは、内部ルートをアクティブ装置に向ける必要があります。アクティブ装置は、設定されたルート テーブル情報を使用して自動的にルートを自身に向けます。

プライマリ装置とセカンダリ装置の両方でこれらの設定を構成します。プライマリ装置からセカンダリ装置への設定の同期はありません。

コンフィギュレーションからルート情報を削除するには、このコマンドの **no** 形式を使用します。

(注) Azure は、『*Azure Resource Manager Documentation*』でルーティングの要件について説明しています。

例

次に、パブリック クラウド フェールオーバー コンフィギュレーションに更新が必要なルートを追加する例を示します。

```
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4
ciscoasa(cfg-fover-cloud-rt)#
```

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。
rg	パブリック クラウド フェールオーバー コンフィギュレーションに Azure リソース グループを追加します。
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の **failover** コマンドを表示します。

failover cloud subscription-id

Azure サービス プリンシパル用の Azure サブスクリプション ID 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 cloud subscription-id** コマンドを使用します。このコマンドの **no** 形式は、コンフィギュレーションからサブスクリプション情報を削除します。

failover cloud subscription-id *sub-id*

no failover cloud subscription-id

構文の説明

subscription-id *sub-id*	Azure リソースを変更する際に必要な Azure サブスクリプション ID 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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

Azure サブスクリプション ID は、内部ルートをアクティブ ユニットに向ける場合など、Azure ルート テーブルを変更するために必要です。

(注) サブスクリプション ID は、Azure ポータル（https://portal.azure.com）の「サブスクリプション（Subscriptions）」タブで参照できます。

例

次に、パブリック クラウド フェールオーバー コンフィギュレーションに Azure サブスクリプション ID を追加する例を示します。

```
(config)# failover cloud (config)# failover cloud subscription-id ab2fe6b2-c2bd-44
(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 cloud authentication	パブリック クラウド フェールオーバー コンフィギュレーションに Azure 認証クレデンシャルを追加します。
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の **failover** コマンドを表示します。

failover cloud unit

パブリック クラウド フェールオーバー コンフィギュレーションで ASAv をプライマリ ユニットまたはセカンダリ ユニット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。ユニットのロールの設定を削除するには、このコマンドの **no** 形式を使用します。

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

no failover cloud unit

構文の説明

プライマリ	ASAv をプライマリ ユニットとして指定します。
secondary	ASAv をセカンダリ ユニットとして指定します。

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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

冗長性を確保するために、ASAv をアクティブ/バックアップ高可用性（HA）設定でパブリック クラウド環境に展開します。パブリック クラウドでの HA は、アクティブな ASAv の障害がバックアップ ASAv へのシステムの自動フェールオーバーをトリガーするのを許可するステートレスなアクティブ/バックアップ ソリューションを実装します。

アクティブ/バックアップ フェールオーバーを設定する場合、1 つの装置をプライマリとして設定し、もう 1 つの装置をセカンダリとして設定します。この時点で、2 つのユニットは、デバイスとポリシーの設定、およびイベント、ダッシュボード、レポート、ヘルス モニタリングで、2 つの個別のデバイスとして機能します。

フェールオーバー ペアの 2 つの装置の主な相違点は、どちらの装置がアクティブでどちらの装置がバックアップであるか、つまりどちらの装置がアクティブにトラフィックを渡すかということに関連します。両方のユニットがトラフィックを渡すことができますが、プライマリ ユニットだけがロード バランサ プローブに応答し、構成済みのルートをプログラミングしてルートの接続先として使用します。バックアップ装置の主な機能は、プライマリ装置の正常性を監視することです。両方の装置が同時にスタート アップした場合（さらに動作ヘルスが等しい場合）、プライマリ装置が常にアクティブ装置になります。

例

次に、ASAv をパブリック クラウド フェールオーバー コンフィギュレーションにおけるプライマリ ユニットとして設定する例を示します。

```
ciscoasa(config)# failover cloud unit primary
```

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	スタンバイ ユニットをアクティブに切り替えます。
failover cloud peer	パブリック クラウド フェールオーバー ピアの情報を指定します。
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の **failover** コマンドを表示します。

failover exec

フェールオーバー ペアの特定のユニットに対してコマンドを実行するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **failover exec** コマンドを使用します。

failover exec {**active** | **standby** | **mate**} *cmd_string*

構文の説明

active	コマンドをフェールオーバー ペアのアクティブ ユニットまたはフェールオーバー グループに対して実行することを指定します。アクティブ ユニットまたはフェールオーバー グループに対して入力されたコンフィギュレーション コマンドは、スタンバイ ユニットまたはフェールオーバー グループに複製されます。
cmd_string	実行するコマンド。**show** コマンド、コンフィギュレーション コマンド、および EXEC コマンドがサポートされています。
mate	コマンドをフェールオーバー ピアに対して実行することを指定します。
standby	コマンドをフェールオーバー ペアのスタンバイ ユニットまたはフェールオーバー グループに対して実行することを指定します。スタンバイ ユニットまたはフェールオーバー グループに対して実行されたコンフィギュレーション コマンドは、アクティブ ユニットまたはフェールオーバー グループには複製されません。

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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

failover exec コマンドを使用して、フェールオーバー ペアの特定のユニットに対してコマンドを送信できます。

コンフィギュレーション コマンドはアクティブ装置またはコンテキストからスタンバイ装置またはコンテキストに複製されるため、いずれの装置にログインしているかにかかわらず、**failover exec** コマンドを使用して正しい装置にコンフィギュレーション コマンドを入力できます。たとえば、スタンバイ装置にログインしている場合、**failover exec active** コマンドを使用して、コンフィギュレーションの変更をアクティブ装置に送信できます。その後、これらの変更はスタンバイ装置に複製されます。スタンバイ装置またはコンテキストへのコンフィギュレーション コマンドの送信には、**failover exec** コマンドを使用しないでください。これらのコンフィギュレーションの変更はアクティブ装置に複製されないため、2 つのコンフィギュレーションが同期されなくなります。

コンフィギュレーション、exec、および **show** コマンドの出力は、現在のターミナル セッションで表示されます。したがって、**failover exec** コマンドを使用して、ピア装置で **show** コマンドを発行し、その結果を現在のターミナルに表示することができます。

ピア装置でコマンドを実行するには、ローカル装置でコマンドを実行できるだけの十分な権限を持っている必要があります。

コマンド モード

failover exec コマンドは、お使いのターミナル セッションのコマンド モードとは異なるコマンド モード状態を維持します。デフォルトで、**failover exec** のコマンド モードは、指定したデバイスに対するグローバル コンフィギュレーション モードです。このコマンド モードを変更するには、**failover exec** コマンドを使用して適切なコマンド（**interface** コマンドなど）を送信します。

指定されたデバイスの **failover exec** コマンド モードを変更しても、デバイスへのアクセスに使用しているセッションのコマンド モードは変更されません。たとえば、フェールオーバー ペアのアクティブ ユニットにログインしており、グローバル コンフィギュレーション モードで次のコマンドを発行した場合、セッションのコマンド モードはグローバル コンフィギュレーション モードのままですが、**failover exec** コマンドを使用して送信されるすべてのコマンドはインターフェイス コンフィギュレーション モードで実行されます。

```
ciscoasa(config)# failover exec interface GigabitEthernet0/1
ciscoasa(config)#
```

デバイスとの現在のセッションのコマンド モードを変更しても、**failover exec** コマンドで使用されるコマンド モードには影響しません。たとえば、アクティブ ユニットでインターフェイス コンフィギュレーション モードであるときに、**failover exec** のコマンド モードを変更していない場合、次のコマンドはグローバル コンフィギュレーション モードで実行されます。

```
ciscoasa(config-if)# failover exec active router ospf 100
ciscoasa(config-if)#
```

show failover exec コマンドを使用すると、指定したデバイスにコマンド モードが表示されます。**failover exec** コマンドを使用して送信されたコマンドは、このモードで実行されます。

セキュリティに関する注意事項

failover exec コマンドは、フェールオーバー リンクを使用してコマンドをピア装置に送信し、実行されたコマンドの出力をピア装置から受信します。盗聴や中間者攻撃を防止するには、**failover key** コマンドを使用してフェールオーバー リンクを暗号化する必要があります。

制限事項

- ゼロダウンタイム アップグレード手順を使用して 1 台の装置だけをアップグレードする場合は、機能するコマンドとして **failover exec** コマンドをサポートしているソフトウェアが両方の装置で動作している必要があります。
- コマンドの完成およびコンテキスト ヘルプは、*cmd_string* 引数のコマンドでは使用できません。

- マルチ コンテキスト モードでは、ピア装置のピア コンテキストだけにコマンドを送信できます。異なるコンテキストにコマンドを送信するには、まずログインしているユニットでそのコンテキストに変更する必要があります。
- 次のコマンドと **failover exec** コマンドを一緒に使用することはできません。
  - **changeto**
  - **debug**（**undebug**）
- スタンバイ装置が故障状態の場合、故障の原因がサービス カードの不具合であれば、**failover exec** コマンドからのコマンドは受信できます。それ以外の場合、リモート コマンドの実行は失敗します。
- **failover exec** コマンドを使用して、フェールオーバー ピアで特権 EXEC モードをグローバル コンフィギュレーション モードに切り替えることはできません。たとえば、現在のユニットが特権 EXEC モードのときに **failover exec mate configure terminal** コマンドを入力すると、**show failover exec mate** コマンドの出力に、failover exec セッションがグローバル コンフィギュレーション モードであることが示されます。ただし、ピア ユニットで **failover exec** コマンドを使用してコンフィギュレーション コマンドを入力した場合、現在のユニットでグローバル コンフィギュレーション モードを開始しない限り、その処理は失敗します。
- **failover exec mate failover exec mate** *コマンドのような、再帰的な* **failover exec** コマンドは入力できません。
- ユーザの入力または確認が必要なコマンドでは、**/nonconfirm** オプションを使用する必要があります。

例

次に、**failover exec** コマンドを使用して、アクティブ ユニットのフェールオーバー情報を表示する例を示します。コマンドはアクティブ ユニットで実行されるため、コマンドはローカルで実行されます。

```
ciscoasa(config)# failover exec active show failover

Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:31:50 jst May 2 2004
        This host: Primary - Active
                Active time: 2483 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         328        0          328        0
        sys cmd         329        0          329        0
```

```
        up time         0           0           0           0
        RPC services    0           0           0           0
        TCP conn        0           0           0           0
        UDP conn        0           0           0           0
        ARP tbl         0           0           0           0
        Xlate_Timeout   0           0           0           0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       329
        Xmit Q:         0       1       329
ciscoasa(config)#
```

次に、**failover exec** コマンドを使用して、ピア ユニットのフェールオーバー ステータスを表示する例を示します。コマンドはアクティブ ユニットであるプライマリ ユニットで実行されるため、セカンダリのスタンバイ ユニットの情報が表示されます。

```
ciscoasa(config)# failover exec mate show failover

Failover On
Failover unit Secondary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:19:59 jst May 2 2004
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Primary - Active
                Active time: 2604 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         344        0          344        0
        sys cmd         344        0          344        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       344
        Xmit Q:         0       1       344
```

次に、**failover exec** コマンドを使用して、フェールオーバー ピアのフェールオーバー コンフィギュレーションを表示する例を示します。コマンドはアクティブ ユニットであるプライマリ ユニットで実行されるため、セカンダリのスタンバイ ユニットの情報が表示されます。

```
ciscoasa(config)# failover exec mate show running-config failover

failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover polltime interface 3 holdtime 15
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
ciscoasa(config)#
```

次に、**failover exec** コマンドを使用して、スタンバイ ユニットからアクティブ ユニットにコンテキストを作成する例を示します。コマンドは、アクティブ ユニットからスタンバイ ユニットに複製されます。2 つの「Creating context…」メッセージに注目してください。1 回めは、コンテキスト作成時に **failover exec** コマンドによってピア ユニットから出力されたものであり、2 回めは複製されたコマンドによってローカルにコンテキストが作成されたときにローカル ユニットから出力されたものです。

```
ciscoasa(config)# show context

Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1

Total active Security Contexts: 1

! The following is executed in the system execution space on the standby unit.

ciscoasa(config)# failover exec active context text

Creating context 'text'... Done. (2)
Creating context 'text'... Done. (3)

ciscoasa(config)# show context
Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1
 text             default                         (not entered)

Total active Security Contexts: 2
```

次に、**failover exec** コマンドを使用してスタンバイ ステートのフェールオーバー ピアにコンフィギュレーション コマンドを送信したときに警告が返され、その警告が表示される例を示します。

```
ciscoasa# failover exec mate static (inside,outside) 192.168.5.241 192.168.0.241

        **** WARNING ****
        Configuration Replication is NOT performed from Standby unit to Active unit.
        Configurations are no longer synchronized.
ciscoasa(config)#
```

次に、**failover exec** コマンドを使用して、**show interface** コマンドをスタンバイ ユニットに送信する例を示します。

```
ciscoasa(config)# failover exec standby show interface

Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
      MAC address 000b.fcf8.c290, MTU 1500
      IP address 192.168.5.111, subnet mask 255.255.255.0
      216 packets input, 27030 bytes, 0 no buffer
      Received 2 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      284 packets output, 32124 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "outside":
      215 packets input, 23096 bytes
      284 packets output, 26976 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  23 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  24 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(10 Mbps)
      MAC address 000b.fcf8.c291, MTU 1500
      IP address 192.168.0.11, subnet mask 255.255.255.0
      214 packets input, 26902 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      215 packets output, 27028 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "inside":
      214 packets input, 23050 bytes
      215 packets output, 23140 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  21 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  21 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "failover", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
      Description: LAN/STATE Failover Interface
      MAC address 000b.fcf8.c293, MTU 1500
      IP address 10.0.5.2, subnet mask 255.255.255.0
      1991 packets input, 408734 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      1835 packets output, 254114 bytes, 0 underruns
```

```
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/2) software (0/0)
  Traffic Statistics for "failover":
      1913 packets input, 345310 bytes
      1755 packets output, 212452 bytes
      0 packets dropped
      1 minute input rate 1 pkts/sec,  319 bytes/sec
      1 minute output rate 1 pkts/sec,  194 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 1 pkts/sec,  318 bytes/sec
      5 minute output rate 1 pkts/sec,  192 bytes/sec
      5 minute drop rate, 0 pkts/sec
.
.
.
```

次に、ピア ユニットに対して不正なコマンドを発行したときにエラー メッセージが返され、そのエラー メッセージが表示される例を示します。

```
ciscoasa# failover exec mate bad command

bad command
  ^
ERROR: % Invalid input detected at '^' marker.
```

次に、フェールオーバーがディセーブルの場合に **failover exec** コマンドを使用してエラー メッセージが返され、そのエラー メッセージが表示される例を示します。

```
ciscoasa(config)# failover exec mate show failover

ERROR: Cannot execute command on mate because failover is disabled
```

関連コマンド

コマンド	説明
debug fover	フェールオーバー関連のデバッグ メッセージを表示します。
debug xml	**failover exec** コマンドによって使用される XML パーサーのデバッグ メッセージを表示します。
show failover exec	**failover exec** のコマンド モードを表示します。

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*

構文の説明

num	フェールオーバー グループの番号。有効な値は、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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

最大 2 つのフェールオーバー グループを定義できます。**failover group** コマンドは、マルチ コンテキスト モードが設定されたデバイスのシステム コンテキストにのみ追加できます。フェールオーバー グループは、フェールオーバーがディセーブルになっているときに限り作成および削除できます。

このコマンドを入力すると、フェールオーバー グループ コマンド モードが開始されます。フェールオーバー グループ コンフィギュレーション モードでは、**primary**、**secondary**、**preempt**、**replication http**、**interface-policy**、**mac address**、および **polltime interface** コマンドを使用できます。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**、**failover mac address** の各コマンドは、Active/Active フェールオーバー コンフィギュレーションでは何も行いません。これらは、**polltime interface**、**interface-policy**、**replication http**、および **mac address** の各フェールオーバー グループ コンフィギュレーション モード 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すべてのコンテキストは、デフォルトでフェールオーバー 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アクティブ/アクティブ 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。ネットワーク上に重複した MAC アドレスが存在しないようにするには、**mac address** コマンドを使用して、各物理インターフェイスに対して仮想アクティブ MAC アドレスおよび仮想スタンバイ MAC アドレスを割り当てる必要があります。

例

次に、2 つのフェールオーバー グループのコンフィギュレーションの例(抜粋)を示します。

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

関連コマンド

コマンド	説明
asr-group	非対称ルーティング インターフェイス グループ ID を指定します。
interface-policy	モニタリングによってインターフェイスの障害が検出された場合のフェールオーバー ポリシーを指定します。
join-failover-group	コンテキストをフェールオーバー グループに割り当てます。
mac address	フェールオーバー グループ内のコンテキストに対して仮想 MAC アドレスを定義します。
polltime interface	モニタ対象インターフェイスに送信される hello メッセージ間の時間を指定します。
preempt	高いプライオリティを持つユニットが、リブート後にアクティブ ユニットとなることを指定します。
プライマリ	フェールオーバー グループにおいて、プライマリ ユニットに対してより高いプライオリティを指定します。
replication http	選択したフェールオーバー グループに対して、HTTP セッションのレプリケーションを指定します。
secondary	フェールオーバー グループにおいて、セカンダリ ユニットに対してより高いプライオリティを指定します。

failover health-check bfd

ユニット ヘルス モニタリングに Bidirectional Forwarding Detection（BFD）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 health-check bfd** コマンドを使用します。BFD 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 health-check bfd *template_name*

no failover health-check bfd *template_name*

構文の説明

template_name	BFD テンプレートの名前。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

CPU の使用率が高い場合、通常のユニットのモニタリングにより誤ってアラームが発生する可能性があります。BFD メソッドは分散されていてるため、CPU の使用率が高い場合でも動作に影響はありません。

最初に、パケット レートを定義するための BFD シングルホップ テンプレートを設定する必要があります。

bfd-template single-hop *template_name*

bfd interval min-tx *milliseconds* **min-rx** *milliseconds* **multiplier** *multiplier_value*

次の制限事項を確認してください。

- FirePOWER 9300 および 4100 のみ
- アクティブ/スタンバイのみ
- ルーテッド モードのみ

例

次に、BFD ユニット ヘルス検出を有効にする例を示します。

```
ciscoasa(config)# bfd template single-hop failover-temp
ciscoasa(config-bfd)# bfd interval min-tx 50 min-rx 50 multiplier 3
ciscoasa(config)# failover health-check bfd failover-temp
```

関連コマンド

コマンド	説明
bfd template	BFD で使用するテンプレートを作成します。
bfd interval	テンプレートのパケット レートを定義します。

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、IPv4 アドレスとマスク、または IPv6 アドレスとプレフィックスを指定するには、グローバル コンフィギュレーション モードで **failover 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* | *ipv6_address*/*prefix* **standby***ipv6_address*]

no failover interface ip *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address*/*prefix* **standby***ipv6_address*]

構文の説明

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 デバイス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。
ipv6_address	プライマリ デバイス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、IPv6 アドレスを指定します。
prefix	アドレスの高次の連続ビットのうち、何個が IPv6 プレフィックス（IPv6 アドレスのネットワーク部分）を構成しているかを指定します。
standby *ip_address*	セカンダリ デバイスがプライマリ デバイスとの通信に使用する IP アドレスを指定します。
standby*ipv6_address*	セカンダリ デバイスがプライマリ デバイスとの通信に使用する IPv6 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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(2)	IPv6 アドレスのサポートが追加されました。

使用上のガイドライン

スタンバイ アドレスは、プライマリ アドレスと同じサブネットにある必要があります。

コンフィギュレーションに適用できる **failvover interface ip** コマンドは 1 つだけです。そのため、フェールオーバー インターフェイスには IPv6 アドレスまたは IPv4 アドレスのいずれか 1 つを割り当てることができます。IPv6 アドレスおよび IPv4 アドレスの両方をインターフェイスに割り当てることはできません。

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、ASA がトランスペアレント ファイアウォール モードで稼働し、システムに対してグローバルであっても、レイヤ 3 で動作します。

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

このコマンドは、ASA 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の一部である必要があります。

例

次に、フェールオーバー インターフェイスに IPv4 アドレスとマスクを指定する方法の例を示します。

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

次に、フェールオーバー インターフェイスに IPv6 アドレスとプレフィックスを指定する方法の例を示します。

```
ciscoasa(config)# failover interface ip lanlink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

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	指定したインターフェイスの状態をモニタします。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover interface-policy

モニタリングによってインターフェイスの障害が検出された場合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。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

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

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

構文の説明

num	パーセンテージとして使用される場合は 1 ～ 100 の数値を、数値として使用される場合は 1 ～インターフェイスの最大数を指定します。
%	(任意)*num* の数字が、モニタ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

デフォルトの設定は次のとおりです。

- *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、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

num 引数とオプションの **%** キーワードの間にはスペースを挿入しません。

障害が発生したインターフェイスの数が、設定されているポリシーの基準を満たし、他方の ASA が正しく機能している場合、ASA は自身を障害発生状態とマークして、フェールオーバーが行われる可能性があります(アクティブな ASA で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** コマンドでモニタ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 モードで **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

次に、2 通りの方法でフェールオーバー ポリシーを指定する例を示します。

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

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

関連コマンド

コマンド	説明
failover polltime	ユニットおよびインターフェイスのポーリング タイムを指定します。
failover reset	障害が発生したユニットを障害が発生していない状態に復元します。
monitor-interface	フェールオーバーのためにモニタ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ついての情報を表示します。

failover ipsec pre-shared-key

フェールオーバーの IPsec LAN-to-LAN トンネルと、ユニット間のステート リンクを確立してすべてのフェールオーバー通信を暗号化するには、グローバル コンフィギュレーション モードで **failover ipsec pre-shared-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 ipsec pre-shared-key *key*

no failover ipsec pre-shared-key

構文の説明

0	暗号化されていないパスワードを指定します。これはデフォルトです。
8	暗号化パスワードを指定します。マスター パスフレーズを使用する場合（**password encryption aes** および **key config-key password-encryption** コマンドを参照）、キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合（**more system:running-config** 出力からなど）、**8** キーワードを使用してキーの暗号化を指定します。 （注） **show running-config** の出力では、**failover ipsec pre-shared-key** は、***** と表示されます。このマスクされたキーはコピーできません。
key	IKEv2 によるトンネルの確立に使用される、両方のユニットに対するキーを指定します。最大長は 128 文字です。

コマンド デフォルト

0（暗号化なし）がデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

フェールオーバー通信をセキュリティ保護しない限り、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、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 ASA 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 リスクになるおそれがあります。ASA 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セキュリティ保護することをお勧めします。

暗号化方法として、レガシーの **failover key** 方式よりも、**failover ipsec pre-shared-key** 方式を使用することをお勧めします。

IPsec 暗号化とレガシーの **failover key** 暗号化の両方を使用することはできません。両方の方法を設定した場合は、IPsec が使用されます。ただし、マスター パスフレーズを使用する場合は（**password encryption aes** および **key config-key password-encryption** コマンドを参照）、IPsec 暗号化を設定する前に、**no failover key** コマンドを使用してフェールオーバー キーを削除する必要があります。

（注） フェールオーバー LAN-to-LAN トンネルは、IPsec（その他の VPN）ライセンスには適用されません。

例

次に、IPsec 事前共有キーを設定する例を示します。

```
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
```

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フェールオーバー コマンドを表示します。
show vpn-sessiondb	フェールオーバー IPsec トンネルを含む、VPN トンネルに関する情報を示します。

failover key

フェールオーバー ペアのユニット間での暗号化および認証された通信（フェールオーバー リンクとステート リンクによる）用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 [**0** | **8**] {**hex** *key* | *shared_secret*}

no failover key

構文の説明

0	暗号化されていないパスワードを指定します。これはデフォルトです。
8	暗号化パスワードを指定します。マスター パスフレーズを使用する場合（**password encryption aes** および **key config-key password-encryption** コマンドを参照）、共有秘密はコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合（**more system:running-config** 出力からなど）、**8** キーワードを使用して共有秘密が暗号化されていることを指定します。 （注） **failover key** の共有秘密は、**show running-config** の出力に ***** と表示されます。このマスクされたキーはコピーできません。
hex *key*	暗号キーの 16 進数値を指定します。キーは、32 文字の 16 進数文字（0 ～ 9、a ～ f）である必要があります。
shared_secret	英数字の共有秘密を指定します。秘密に使用できる文字数は、1 ～ 63 文字です。有効な文字は、数字、文字、または句読点の任意の組み合わせです。共有秘密は、暗号キーを生成するために使用されます。

デフォルト

0（暗号化なし）がデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**failover lan key** から **failover key** に変更されました。
7.0(4)	このコマンドが、**hex** *key* キーワードおよび引数を含むように変更されました。
8.3(1)	このコマンドは、**0** および **8** キーワードを使用してマスター パスフレーズをサポートするように変更されました。

使用上のガイドライン

フェールオーバー通信をセキュリティ保護しない限り、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、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 ASA 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 リスクになるおそれがあります。ASA 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セキュリティ保護することをお勧めします。

暗号化方法として、レガシーの **failover key** 方式よりも、**failover ipsec pre-shared-key** 方式を使用することをお勧めします。

IPsec 暗号化（**failover ipsec pre-shared-key** コマンド）とレガシーの **failover key** 暗号化の両方を使用することはできません。両方の方法を設定した場合は、IPsec が使用されます。ただし、マスター パスフレーズを使用する場合は（**password encryption aes** および **key config-key password-encryption** コマンドを参照）、IPsec 暗号化を設定する前に、**no failover key** コマンドを使用してフェールオーバー キーを削除する必要があります。

例

次に、フェールオーバー ペアのユニット間でフェールオーバー通信をセキュリティ保護するための共有秘密を指定する例を示します。

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

次に、フェールオーバー ペアの 2 つのユニット間でフェールオーバー通信をセキュリティ保護するための 16 進キーを指定する例を示します。

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

次に、**more system:running-config** 出力から、暗号化されたパスワードをコピーして貼り付けた例を示します。

```
ciscoasa(config)# failover key 8 TPZCVNgdegLhWMa
```

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フェールオーバー 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*}]

構文の説明

if_name	フェールオーバー専用の ASA 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	(任意)サブインターフェイス番号を指定します。
vlan_if	ASASM で、VLAN インターフェイスをフェールオーバー リンクとして指定するために使用されます。

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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	*phy_if* 引数が追加されました。
7.2(1)	*vlan_if* 引数が追加されました。
9.5(1)	このコマンドは、ASA 5506H-X の管理インターフェイスを受け入れるように変更されました。

使用上のガイドライン

フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。

フェールオーバー リンク データ

次の情報がフェールオーバー リンク経由で伝達されています。

- 装置の状態(アクティブまたはスタンバイ)
- hello メッセージ(キープアライブ)

- ネットワーク リンクの状態
- MAC アドレス交換
- コンフィギュレーションの複製および同期

フェールオーバー リンクのインターフェイス

使用されていないデータ インターフェイス（物理、冗長、または EtherChannel）はどれでも、フェールオーバー リンクとして使用できます。ただし、現在名前が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 リンク 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のためにだけ存在します。このインターフェイスは、フェールオーバー リンク用にのみ使用できます（ステート リンク用としても使用できます）。ASA は、ユーザ データ用とフェールオーバー用に異なるサブインターフェイスが設定されている場合でも、ユーザ データとフェールオーバー リンク間でのインターフェイスの共有はサポートしません。フェールオーバー リンクには、別の物理、EtherChannel、または冗長インターフェイスを使用する必要があります。

フェールオーバー リンクについては、次のガイドラインを参照してください。

- 5506-X ～ 5555-X：管理インターフェイスをフェールオーバー リンクとして使用できません。データ インターフェイスを使用する必要があります。5506H-X は唯一の例外で、フェールオーバー リンクとして管理インターフェイスを使用できます。
- 5506H-X：フェールオーバー リンクとして管理 1/1 インターフェイスを使用できます。フェールオーバー用に設定した場合は、デバイスをリロードして変更を反映させる必要があります。この場合、管理プロセスに管理インターフェイスが必要であるため、ASA Firepower モジュールも使用できません。
- 5585-X：データ インターフェイスとしては使用できますが、管理 0/0 インターフェイスは使用しないでください。この用途で必要とされるパフォーマンスをサポートしていません。
- Firepower 9300 ASA セキュリティ モジュール：管理タイプまたはデータ タイプのどちらかのインターフェイスをフェールオーバー リンクとして使用できます。インターフェイスを節約し、同じシャーシ内のモジュール間でフェールオーバー リンクを共有するには、管理タイプのインターフェイスを使用します。たとえば、それぞれ 3 つのセキュリティ モジュールを備えた 2 台のシャーシがあるとします。シャーシ間で 3 つのフェールオーバー ペアを作成できます。1 つの 10 GigabitEthernet 管理インターフェイスをシャーシ間で使用して、フェールオーバー リンクとして機能させることができます。各モジュール内で一意の VLAN サブインターフェイスを設定するだけです。
- すべてのモデル：1 GB インターフェイスは、フェールオーバーとステート リンクを組み合わせるには十分な大きさです。

フェールオーバー リンクとして使用される冗長インターフェイスについては、冗長性の増強による次の利点を参照してください：

- フェールオーバー ユニットが起動すると、メンバー インターフェイスを交互に実行し、アクティブ ユニットを検出します。
- メンバー インターフェイスの 1 つにあるピアからのキープアライブ メッセージの受信をフェールオーバー ユニットが停止した場合、別のメンバー インターフェイスに切り替えます。

フェールオーバー リンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバー リンクとして使用中の EtherChannel の設定は変更できません。

フェールオーバー リンクの接続

フェールオーバー リンクを次の 2 つの方法のいずれかで接続します。

- ASA のフェールオーバー インターフェイスと同じネットワーク セグメント(ブロードキャスト ドメインまたは VLAN)に他の装置のないスイッチを使用する。
- イーサネット ケーブルを使用して装置を直接接続します。外部スイッチは必要ありません。

装置間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらの装置のものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

ASA は、銅線イーサネット ポートで Auto-MDI/MDIX をサポートしているため、クロスオーバー ケーブルまたはストレート ケーブルのいずれかを使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

その他のガイドライン

- 接続中のスイッチで VLAN を使用する場合は、フェールオーバー リンク専用の VLAN を使用します。フェールオーバー リンクの VLAN を他の VLAN と共有すると、断続的にトラフィックの問題が発生したり、ping や ARP の障害が発生したりすることがあります。フェールオーバー リンクの接続にスイッチを使用する場合は、スイッチおよび ASA でフェールオーバー リンク専用のインターフェイスを使用します。インターフェイスを、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と共有しないでください。
- マルチ コンテキスト モードで動作するシステムでは、フェールオーバー リンクはシステム コンテキストにあります。システム コンテキストに設定できるインターフェイスは、このインターフェイス、および使用されている場合はステート リンクのみです。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。
- 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。

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 ASA 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 リスクになるおそれがあります。ASA 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

次に、共有フェールオーバーおよびステート リンクを含むプライマリ ユニットのフェールオーバー パラメータを設定する例を示します。

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
interface gigabitethernet 0/3
    no shutdown
failover link folink gigabitethernet0/3
failover ipsec pre-shared-key a3rynsun
failover
```

関連コマンド

コマンド	説明
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 ASA 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**}

構文の説明

プライマリ	ASA をプライマリ ユニットとして指定します。
secondary	ASA をセカンダリ ユニットとして指定します。

デフォルト

セカンダリ

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

Active/Standby フェールオーバーでは、フェールオーバー ユニットに対するプライマリとセカンダリの指定によって、起動時にどのユニットがアクティブになるかが決まります。次の場合に、起動時にプライマリ ユニットがアクティブ ユニットになります。

- 最初のフェールオーバー ポーリング チェックの間に、プライマリ ユニットとセカンダリ ユニットの両方がブート シーケンスを完了している。
- プライマリ ユニットがセカンダリ ユニットよりも前に起動している。

プライマリ ユニットの起動時にすでにセカンダリ ユニットがアクティブになっている場合、プライマリ ユニットはアクティブにはならずに、スタンバイ ユニットとなります。この場合、プライマリ ユニットを強制的にアクティブ ステータスに戻すには、セカンダリ(アクティブ)ユニットで **no failover active** コマンドを入力する必要があります。

Active/Active フェールオーバーでは、各フェールオーバー グループにプライマリまたはセカンダリのユニット 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によって、両方のユニットが（フェールオーバー ポーリング期間内に）同時に起動されたときに、起動時にフェールオーバー ペアのどのユニットでフェールオーバー グループのコンテキストがアクティブになるかが決まります。

このコマンドは、ASA 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の一部である必要があります。

例

次に、ASA を LAN ベースのフェールオーバーのプライマリ ユニットとして設定する例を示します。

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

関連コマンド

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

failover link

ステートフル フェールオーバー インターフェイスを指定し、ステートフル 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 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

構文の説明

if_name	ステートフル フェールオーバー専用の ASA インターフェイスの名前を指定します。
phy_if	(任意)物理インターフェイス ポートまたは論理インターフェイス 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ているインターフェイスを共有しているか、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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	*phy_if* 引数が追加されました。
7.0(4)	このコマンドが、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変更されました。
9.5(1)	このコマンドは、ASA 5506H-X の管理インターフェイスを受け入れるように変更されました。

使用上のガイドライン

ステートフル フェールオーバーを使用するには、接続ステート情報を渡すためのステートフル フェールオーバー リンク（ステート リンクとも呼ばれる）を設定する必要があります。

フェールオーバー リンクの共有

インターフェイスを節約するための最適な方法はフェールオーバー リンクの共有です。このインターフェイスでパフォーマンス上の問題が発生した場合は、別のインターフェイスをステート リンク専用にすることを検討してください。

専用インターフェイス

ステート リンク専用のデータ インターフェイス（物理、冗長、または EtherChannel）を使用できます。ステート リンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。

次の 2 つの方法のいずれかで、専用のステート リンクを接続します。

- ASA のフェールオーバー インターフェイスと同じネットワーク セグメント（ブロードキャスト ドメインまたは VLAN）に他の装置のないスイッチを使用する。
- イーサネット ケーブルを使用してアプライアンスを直接接続します。外部スイッチは必要ありません。

装置間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらの装置のものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

ASA は、銅線イーサネット ポートで Auto-MDI/MDIX をサポートしているため、クロスオーバー ケーブルまたはストレート ケーブルのいずれかを使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

長距離のフェールオーバーを使用する場合のステート リンクの遅延は、パフォーマンスを最善にするには 10 ミリ秒未満でなければならず、250 ミリ秒を超えないようにする必要があります。遅延が 10 ミリ秒を超えると、フェールオーバー メッセージの再送信により、どうしてもパフォーマンスが低下します。

その他のガイドライン

- 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 コンテキストに存在します。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。
- ステートフル フェールオーバー リンクが通常のデータ インターフェイスに設定されていない限り、ステートフル フェールオーバー リンクの IP アドレスと MAC アドレスは、フェールオーバー時に変更されません。

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 ASA 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 リスクになるおそれがあります。ASA 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

次に、共有フェールオーバーおよびステート リンクを含むプライマリ ユニットのフェールオーバー パラメータを設定する例を示します。

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
interface gigabitethernet 0/3
    no shutdown
failover link folink gigabitethernet0/3
failover ipsec pre-shared-key a3rynsun
failover
```

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。

failover mac address

物理インターフェイス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*

構文の説明

active_mac	アクティブな ASA の指定し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。ここで、h は 16 ビットの 16 進数です。
phy_if	MAC アドレスを設定するインターフェイスの物理名です。
standby_mac	スタンバイの ASA の指定し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。ここで、h は 16 ビットの 16 進数です。

デフォルト

設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

failover mac address コマンドを使用すると、Active/Standby フェールオーバー ペアの仮想 MAC アドレスを設定できます。仮想 MAC アドレスが定義されていない場合は、各フェールオーバー ユニットが起動したときに、それらのユニットではインターフェイスのバーンドイン MAC アドレスが使用され、それらのアドレスがフェールオーバー ピアと交換されます。プライマリ ユニットのインターフェイスの MAC アドレスが、アクティブ ユニットのインターフェイスに使用されます。

ただし、両方のユニットが同時にオンラインにならず、セカンダリ ユニットが最初に起動してアクティブになった場合、セカンダリ ユニットは、自身のインターフェイスにバーンドイン MAC アドレスを使用します。その後プライマリ ユニットがオンラインになると、セカンダリ ユニットはプライマリ ユニットから MAC アドレスを取得します。この変更によりネットワーク トラフィックが中断され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 ユニットがプライマリ ユニットよりも前にオンラインになり、アクティブ ユニットとなった場合でも、正しい MAC アドレスが使用されるようになります。

failover lan interface コマンドでは、フェールオーバーが発生した場合に IP アドレスおよび MAC アドレスが変更されないため、LAN ベースのフェールオーバーに設定されたインターフェイスでは、**failover mac address** コマンドは不要であり、使用できません。このコマンドは、ASA が Active/Active フェールオーバーに設定されている場合には何も行いません。

コンフィギュレーションに **failover mac address** コマンドを追加する場合は、仮想 MAC アドレスを設定し、コンフィギュレーションをフラッシュ メモリに保存して、フェールオーバー ペアをリロードすることを推奨します。アクティブな接続が存在するときに仮想 MAC アドレスを追加すると、これらの接続は停止します。また、仮想 MAC アドレス指定を有効にするには、**failover mac address** コマンドを含むコンフィギュレーション全体を、セカンダリ ASA のフラッシュ メモリに書き込む必要があります。

failover mac address がプライマリ ユニットのコンフィギュレーションに指定されている場合は、セカンダリ ユニットのブートストラップ コンフィギュレーションに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 モードで **mac address** コマンドを使用して、フェールオーバー グループの各インターフェイスの仮想 MAC アドレスを設定します。

他のコマンドまたは方法を使用して MAC アドレスを設定することもできますが、1 つの方法だけを使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。

例

次に、intf2 という名前のインターフェイスのアクティブ MAC アドレスおよびスタンバイ MAC アドレスを設定する例を示します。

```
ciscoasa(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	インターフェイスのステータス、コンフィギュレーション、および統計情報を表示します。

failover polltime

フェールオーバー ユニットのポーリング タイムおよびホールド タイムを指定するには、グローバル コンフィギュレーション モードで **failover polltime** コマンドを使用します。デフォルトのポーリング期間およびホールド タイムに戻すには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

holdtime *time*	(任意)ユニットが、フェールオーバー リンクで hello メッセージを受信する間隔を設定します。この時間を経過すると、ピア ユニットで障害が発生したと見なされます。 有効な値は 3 ～ 45 秒です。オプションの **msec** キーワードを使用した場合は、800 ～ 999 ミリ秒です。
msec	(任意)指定する時間がミリ秒単位であることを指定します。
poll_time	hello メッセージ間の時間を設定します。 有効な値は 1 ～ 15 秒です。オプションの **msec** キーワードを使用した場合は、200 ～ 999 ミリ秒です。
unit	(任意)コマンドがユニットのポーリング タイムおよびホールド タイムに使用されていることを示します。 このキーワードをコマンドに追加してもコマンドには影響がありませんが、コンフィギュレーションでこのコマンドを **failover polltime interface** コマンドと区別しやすくなります。

デフォルト

ASA のデフォルト値は次のとおりです。

- *poll_time* は 1 秒です。
- **holdtime** *time* は 15 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**failover poll** コマンドから **failover polltime** コマンドに変更され、**unit** キーワードおよび **holdtime** キーワードが含まれるようになりました。
7.2(1)	**holdtime** キーワードに **msec** キーワードが追加されました。**polltime** の最小値が 500 ミリ秒から 200 ミリ秒に引き下げられました。**holdtime** の最小値が 3 秒から 800 ミリ秒に引き下げられました。

使用上のガイドライン

ユニットのポーリング タイムの 3 倍未満の値を **holdtime** の値として入力することはできません。ポーリング時間が短いほど、ASA は短時間で故障を検出し、フェールオーバーをトリガーできます。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スイッチオーバーが発生する可能性があります。

1 回のポーリング期間中に装置がフェールオーバー リンクで hello パケットを受信しなかった場合、残りのインターフェイスで追加テストが実行されます。それでも保持時間内にピア装置から応答がない場合、その装置は故障していると見なされ、故障した装置がアクティブ装置の場合は、スタンバイ装置がアクティブ装置を引き継ぎます。

failover polltime [**unit**] コマンドおよび **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) フェールオーバー設定で、CTIQBE トラフィックが ASA を通過する場合には、ASA のフェールオーバー ホールド タイムを 30 秒未満に減らす必要があります。CTIQBE キープアライブ タイムアウトは 30 秒であるため、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 に再登録する必要があります。

例

次に、ユニットのポーリング タイムの頻度を 3 秒に変更する例を示します。

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

次に、200 ミリ秒ごとに hello パケットを送信し、800 ミリ秒以内にフェールオーバー インターフェイスで hello パケットを受信しないとフェールオーバーを実行するように ASA を設定する例を示します。オプションの **unit** キーワードがコマンドに含まれています。

```
ciscoasa(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ホールド タイムを指定します。
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 タイムおよびホールド タイムを指定します。
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のデータ インターフェイスの polltime および holdtime 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 polltime および holdtime を復元するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

holdtime *time*	(任意) ピア ユニットからの最後に受信した hello メッセージとインターフェイス テストの開始との間の時間 (計算として) を設定して、インターフェイスの健全性を判断します。また、各インターフェイス テストの期間を *holdtime*/16 として設定します。有効な値は 5 ～ 75 秒です。デフォルトは、*polltime* の 5 倍です。*polltime* の 5 倍よりも短い holdtime 値は入力できません。 インターフェイス テストを開始するまでの時間 (y) を計算するには、次のようにします。 1. x = (*holdtime*/*polltime*)/2、最も近い整数に丸められます。(.4 以下は切り下げ、.5 以上は切り上げ。) 2. y = x**polltime* たとえば、デフォルトの holdtime は 25 で、polltime が 5 の場合は y は 15 秒です。
polltime	hello パケットをピアに送信するまで待機する時間を指定します。有効な値の範囲は、1 ～ 15 秒です。デフォルトは 5 分です。オプションの **msec** キーワードを使用した場合、有効な値は 500 ～ 999 ミリ秒です。
msec	(任意) 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 倍です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**failover poll** コマンドから **failover polltime** コマンドに変更され、**unit** キーワード、**interface** キーワード、および **holdtime** キーワードが含まれるようになりました。
7.2(1)	オプションの **holdtime** *time* と、ミリ秒単位でポーリング タイム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

このコマンドは、Active/Standby フェールオーバーにのみ使用可能です。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 モードで **polltime interface** コマンドを使用します。

ポーリング時間が短いほど、ASA は短時間で故障を検出し、フェールオーバーをトリガーできます。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。

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) フェールオーバー設定で、CTIQBE トラフィックが ASA を通過する場合には、ASA のフェールオーバー ホールド タイムを 30 秒未満に減らす必要があります。CTIQBE キープアライブ タイムアウトは 30 秒であるため、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 に再登録する必要があります。

例

次に、インターフェイスの polltime の頻度を 15 秒に設定する例を示します。

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

次に、インターフェイスの polltime の頻度を 500 ミリ秒に、holdtime を 5 秒に設定する例を示します。

```
ciscoasa(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 ポーリング期間とホールド タイムを指定します。
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 タイムを指定します。
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 poll-time link-state

インターフェイス リンク ステートのポーリング時間を変更するには、グローバル コンフィギュレーション モードで **failover polltime link-state** コマンドを使用します。リンクステート ポールをディセーブルにするには、このコマンドの **no** 形式を使用します。

failover polltime link-state msec *poll_time*

no failover polltime link-state msec *poll_time*

構文の説明

msec *poll_time*	ポーリング時間を 300 ～ 799 ミリ秒で設定します。

コマンド デフォルト

デフォルトのポーリング時間は 500 ミリ秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、フェールオーバーのペアの ASA では、インターフェイスのリンク ステートが 500 ミリ秒ごとに確認されます。polltime はカスタマイズできます。たとえば、polltime を 300 ミリ秒に設定すると、ASA ではインターフェイスの障害やトリガーのフェールオーバーをより早く検出できるようになります。

アクティブ/アクティブ モードでは、システムに対してこのレートを設定します。フェールオーバー グループごとにこのレートを設定することはできません。

例

次に、リンクステートのポーリング時間を 300 ミリ秒に設定する例を示します。

```
ciscoasa(config)# failover polltime link-state msec 300
```

関連コマンド

コマンド	説明
failover polltime unit	ユニット ヘルス チェックのポーリング時間を設定します。
failover polltime interface	インターフェイス ヘルス チェックのポーリング時間を設定します。

failover reload-standby

スタンバイ ユニット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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

フェールオーバー ユニットが同期化されないときにこのコマンドを使用します。スタンバイ ユニットが再起動し、起動終了後にアクティブ ユニットと再同期化されます。

例

次に、アクティブ ユニットで **failover reload-standby** コマンドを使用して、スタンバイ ユニットを強制的にリブートする例を示します。

```
ciscoasa# 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 ユニットのメモリに書き込みます。

failover replication http

HTTP（ポート 80）接続のレプリケーション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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	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、ASA 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、また HTTP クライアントは接続試行が失敗すると通常は再試行するため、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** コマンドを使用すると、ステートフル フェールオーバー環境において HTTP セッションのステートフル レプリケーションが可能になりますが、システムのパフォーマンスに悪影響がある可能性があります。

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 モードで **replication http** コマンドを使用して、フェールオーバー グループごとに HTTP セッションのレプリケーションを制御します。

例

次に、HTTP 接続のレプリケーションをイネーブルにする例を示します。

```
ciscoasa(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 グループに対して、HTTP セッションのレプリケーションをイネーブルにします。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover replication rate

バルク同期接続レプリケーション レートを設定するには、グローバル コンフィギュレーション モードで **failover replication rate** 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 replication rate *rate*

no failover replication rate

構文の説明

rate	1 秒あたりの接続数を設定します。値とデフォルト設定はモデルの 1 秒あたりの最大接続数に応じて異なります。

コマンド デフォルト

モデルに応じて異なります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.4(4.1)/8.5(1.7)	このコマンドが追加されました。

使用上のガイドライン

ステートフル フェールオーバーを使用したときの、ASA がスタンバイ ユニットへ接続を複製するレートを設定できます。デフォルトでは、接続は 15 秒間隔でスタンバイ装置に複製されます。ただし、バルク同期が発生すると（たとえば、フェールオーバーを最初にイネーブルにしたときなど）、1 秒あたりの最大接続数の制限のために、大量の接続を同期するのに 15 秒では不十分な場合があります。たとえば、ASASM での最大接続数を 800 万とします。800 万の接続を 15 秒間で複製するということは、1 秒あたり約 53 万 3 千の接続を作成するということです。ただし、1 秒あたりに許可される最大接続数は 30 万です。複製レートが 1 秒あたりの最大接続数以下になるように指定できるようになり、同期期間はすべての接続が同期されるまで調整されます。

例

次に、フェールオーバー レプリケーション レートを 1 秒あたり 20000 接続に設定する例を示します。

```
ciscoasa(config)# failover replication rate 20000
```

関連コマンド

コマンド	説明
failover rate http	HTTP 接続レプリケーションをイネーブルにします。

failover reset

障害が発生した ASA を障害が発生していない状態に復元するには、特権 EXEC モードで **failover reset** コマンドを使用します。

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

構文の説明

group	（任意）フェールオーバー グループを指定します。**group** キーワードは、Active/Active フェールオーバーに対してのみ適用されます。
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

次の表に、コマンドを入力できるモードを示します。

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

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 を追加するように変更されました。

使用上のガイドライン

failover reset コマンドを使用すると、障害が発生したユニットまたはグループを、障害が発生していない状態に変更できます。**failover reset** コマンドはいずれのユニットでも入力できますが、常にアクティブ ユニットでコマンドを入力することを推奨します。アクティブ ユニットで **failover reset** コマンドを入力すると、スタンバイ ユニットが障害が発生していない状態に復元されます。

show failover コマンドまたは **show failover state** コマンドを使用して、ユニットのフェールオーバー ステータスを表示できます。

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は、**failover reset** を入力すると、ユニット全体がリセットされます。コマンドにフェールオーバー グループを指定すると、指定したグループのみがリセットされます。

例

次に、障害が発生したユニットを障害が発生していない状態に変更する例を示します。

```
ciscoasa# failover reset
```

関連コマンド

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

failover standby config-lock

フェールオーバー ペアのスタンバイ ユニットまたはスタンバイ コンテキストに対するコンフィギュレーションの変更をロックするには、グローバル コンフィギュレーション モードで **failover standby config-lock** コマンドを使用します。スタンバイ ユニットでのコンフィギュレーションを許可するには、このコマンドの **no** 形式を使用します。

failover standby config-lock

no failover standby config-lock

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、スタンバイ ユニットまたはスタンバイ コンテキストに対するコンフィギュレーションは、警告メッセージ付きで許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

通常のコンフィギュレーション同期以外の変更をスタンバイ ユニットに加えることができないように、スタンバイ ユニット（Active/Standby フェールオーバー）またはスタンバイ コンテキスト（Active/Active フェールオーバー）に対するコンフィギュレーション変更をロックできます。

例

次に、スタンバイ ユニットに対するコンフィギュレーションを許可しない例を示します。

```
ciscoasa(config)# failover standby config-lock
```

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	スタンバイ ユニットをアクティブに切り替えます。
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の **failover** コマンドを表示します。

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*]]

構文の説明

hh	タイムアウト値の時間を指定します。有効な値の範囲は、-1 ～ 1193 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なり、任意の時間が経過したあとでも接続を再開できます。 この値を 0 に設定し、他のタイムアウト値を指定しないと、コマンドがデフォルト値に設定されて再接続ができなくなります。**no failover timeout** コマンドを入力しても、この値がデフォルト(0)に設定されます。 **(注)** デフォルト値に設定すると、このコマンドは実行コンフィギュレーションに表示されません。
mm	(任意)タイムアウト値の分を指定します。有効な値の範囲は 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	(任意)タイムアウト値の秒を指定します。有効な値の範囲は 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、*hh*、*mm*、および *ss* は 0 であり、再接続はできないようになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、コマンド リストに表示されるように変更されました。

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** コマンドとともに使用されます。**nailed** オプションを指定すると、起動後、またはシステムがアクティブになった後、指定した時間内に接続を再確立できます。**failover timeout** コマンドでは、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** コマンドには影響しません。

(注) **nailed** オプションを **static** コマンドに追加すると、その接続で TCP ステート トラッキングとシーケンス チェックがスキップされます。

このコマンドの **no** 形式を使用すると、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すると、このコマンドは実行コンフィギュレーションに表示されません。

例

次に、スタンバイ グループ 1 をアクティブに切り替える例を示します。

```
ciscoasa(config)# failover timeout 12:30
ciscoasa(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 のアドレス変換ルールを設定します。

fallback（廃止）

接続の整合性が低下した場合に Cisco Intercompany Media Engine が VoIP から PSTN へフォールバックするために使用するフォールバック タイマーを設定するには、uc-ime コンフィギュレーション モードで **fallback** コマンドを使用します。フォールバックの設定を削除するには、このコマンドの **no** 形式を使用します。

fallback {**sensitivity-file** *filename* | **monitoring timer** *timer_millisec* **hold-down timer** *timer_sec*}

no fallback fallback {**sensitivity-file** *filename* | **monitoring timer** *timer_millisec* **hold-down timer** *timer_sec*}

構文の説明

filename	感度ファイルのファイル名を指定します。.fbs ファイル拡張子が含まれる、ディスクにあるファイルの名前を入力します。ファイル名を指定するときに、ローカル ディスク上のパスを含めることができます（例: `disk0:/file001.fbs`）。
hold-down timer	PSTN にフォールバックするかどうかを Cisco UCM に通知するまでに ASA が待機する時間を設定します。
monitoring timer	インターネットから受信した RTP パケットを ASA でサンプリングする時間間隔を設定します。ASA は、このデータ サンプルを使用して、通話に対して PSTN へのフォールバックが必要かどうか判断します。
sensitivity-file	通話中の PSTN フォールバックに使用するファイルを指定します。感度ファイルは ASA により解析され、RMA ライブラリに入力されます。
timer_millisec	ミリ秒単位でモニタリング タイマーの長さを指定します。10 ～ 600 の範囲で整数を入力します。デフォルトのモニタリング タイマーの長さは 100 ミリ秒です。
timer_sec	ホールドダウン タイマーの長さを秒単位で指定します。10 ～ 360 の範囲で整数を入力します。デフォルトのホールドダウン タイマーの長さは 20 秒です。

デフォルト

デフォルトのモニタリング タイマーの長さは 100 ミリ秒です。ホールドダウン タイマーの長さは 20 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.3(1)	コマンドが追加されました。
9.4(1)	このコマンドは、すべての **uc-ime** モード コマンドとともに廃止されました。

使用上のガイドライン

Cisco Intercompany Media Engine のフォールバック タイマーを指定します。

インターネット接続は、時間とともに品質が大幅に変化する可能性があります。そのため、接続の品質が良くてコールが VoIP 上で送信されたとしても、その接続品質は通話中に低下する可能性があります。エンド ユーザに対して全体にわたって良好な通話を保証するために、Cisco Intercompany Media Engine では通話中のフォールバックの実行が試みられます。

通話中のフォールバックを実行するには、インターネットから着信する RTP パケットを ASA でモニタし、情報を RTP Monitoring Algorithm（RMA）API に送信する必要があります。これにより、フォールバックが必要かどうかが ASA に示されます。フォールバックが必要になると、コールを PSTN へフォールバックする必要があることを通知するために、ASA から Cisco UCM に REFER メッセージが送信されます。

（注） SIP インスペクションに対して Cisco Intercompany Media Engine プロキシがイネーブルの場合、フォールバック タイマーは変更できません。フォールバック タイマーを変更する前に、Cisco Intercompany Media Engine プロキシを SIP インスペクションから削除します。

例

次に、フォールバック タイマーを指定するとともに、Cisco Intercompany Media Engine を設定する方法の例を示します。

```
ciscoasa(config)# uc-ime local_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback monitoring timer 120
ciscoasa(config-uc-ime)# fallback hold-down timer 30
```

次に、感度ファイルを指定するとともに、Cisco Intercompany Media Engine を設定する方法の例を示します。

```
ciscoasa(config)# uc-ime local_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback sensitivity-file local_uc-ime_fallback_policy
```

関連コマンド

コマンド	説明
show running-config uc-ime	Cisco Intercompany Media Engine プロキシの実行コンフィギュレーションを表示します。
show uc-ime	フォールバック通知、マッピング サービス セッション、およびシグナリング セッションに関する統計情報または詳細情報を表示します。
uc-ime	Cisco Intercompany Media Engine プロキシ インスタンスを ASA に作成します。

fast-flood

IS-IS リンクステート パケット（LSP）をフラッディングするには、ルータ ISIS コンフィギュレーション モードで **fast-flood** コマンドを使用します。高速フラッディングをディセーブルにするには、このコマンドの **no** 形式を使用します。

fast-flood [*lsp-number*]

no fast-flood [*lsp-number*]

構文の説明

lsp-number	（任意）SPF の開始前にフラッディングする LSP の数です。指定できる範囲は 1 ～ 15 です。デフォルトは 5 分です。

デフォルト

高速フラッディングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.6(1)	コマンドが追加されました。

使用上のガイドライン

fast-flood コマンドでは、指定した数の LSP が ASA から送信されます。LSP 数を指定しない場合、デフォルトとして 5 が使用されます。LSP は、SPF の実行前に SPF を呼び出します。LSP フラッディング プロセスを高速化すると、ネットワークの全体的なコンバージェンス時間が向上します。

ASA は SPF 計算を実行する前に、少なくとも SPF をトリガーした LSP を常にフラッディングする必要があります。

コンバージェンス時間を短縮するために、ASA が SPF 計算を実行する前に、LSP の高速フラッディングをイネーブルにしておくことをお勧めします。

例

次の例では、**fast-flood** コマンドを入力して、SPF 計算が開始される前に、SPF を呼び出す最初の 7 個の LSP をフラッディングするようにルータを設定しています。**show running-configuration** コマンドを入力すると、出力から、ASA で高速フラッディングがイネーブルにされていることがわかります。

```
ciscoasa# clear isis rib redistribution 10.1.0.0 255.255.0.0
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# router isis
ciscoasa(config-router)# fast-flood 7
ciscoasa(config-router)# end
ciscoasa# show running-config | inc fast-flood

fast-flood 7
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。

コマンド	説明
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。

コマンド	説明
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。