CHAPTER 10

アクティブ/アクティブ フェールオーバーの設定

この章では、アクティブ/アクティブ フェールオーバーを設定する方法について説明します。次の項目を取り上げます。

アクティブ/アクティブ フェールオーバーに関する情報

この項では、アクティブ/アクティブ フェールオーバーについて説明します。この項は、次の内容で構成されています。

アクティブ/アクティブ フェールオーバーの概要

アクティブ/アクティブ フェールオーバーは、マルチ コンテキスト モードの ASA でのみ使用できます。アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、両方の ASA がネットワーク トラフィックを渡すことができます。

アクティブ/アクティブ フェールオーバーでは、ASA のセキュリティ コンテキストは、*フェールオーバー グループ*に分割されます。フェールオーバー グループは、1 つまたは複数のセキュリティ コンテキストの論理グループにすぎません。最大 2 つのフェールオーバー グループを作成できます。管理コンテキストは、常にフェールオーバー グループ 1 のメンバです。未割り当てセキュリティ コンテキストもまた、デフォルトでフェールオーバー グループ 1 のメンバーです。

フェールオーバー グループは、アクティブ/アクティブ フェールオーバーにおいてフェールオーバーの基本単位を形成します。インターフェイス障害モニタリング、フェールオーバー、およびアクティブ/スタンバイ ステータスはすべて、フェールオーバー グループの属性であって、装置の属性ではありません。アクティブ フェールオーバー グループが故障すると、スタンバイ状態に変化し、スタンバイ フェールオーバー グループがアクティブになります。アクティブになったフェールオーバー グループのインターフェイスが、故障したフェールオーバー グループのインターフェイスの MAC アドレスと IP アドレスを引き継ぎます。スタンバイ状態になったフェールオーバー グループのインターフェイスが、スタンバイ MAC アドレスと IP アドレスを引き継ぎます。

（注） あるフェールオーバー グループが装置上で故障したというのは、装置が故障したという意味ではありません。その装置では、別のフェールオーバー グループが依然としてトラフィックを渡している場合があります。

フェールオーバー グループを作成する場合は、フェールオーバー グループ 1 がアクティブ状態にある装置に作成する必要があります。

（注） アクティブ/アクティブ フェールオーバーでは、各フェールオーバー グループのインターフェイスに対して仮想 MAC アドレスが生成されます。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。ネットワーク上で MAC アドレスが重複することを回避するには、必ず各物理インターフェイスに仮想のアクティブおよびスタンバイ MAC アドレスを割り当てます。

プライマリ/セカンダリ ステータスとアクティブ/スタンバイ ステータス

アクティブ/スタンバイ フェールオーバーの場合のように、アクティブ/アクティブ フェールオーバー ペアの一方の装置がプライマリ装置に指定され、もう一方の装置がセカンダリ装置に指定されます。アクティブ/スタンバイ フェールオーバーの場合とは異なり、両方の装置が同時に起動された場合、この指定ではどちらの装置がアクティブになるか指示しません。代わりに、プライマリまたはセカンダリの指定時に、次の 2 つの点を判定します。

- 同時にブートされたときに、実行コンフィギュレーションをペアに提供する装置がいずれかを判定します。
- 装置が同時にブートされたときに、各フェールオーバー グループがアクティブ状態で表示される装置がいずれかを判定します。コンフィギュレーションの各フェールオーバー グループは、プライマリまたはセカンダリ装置プリファレンスが設定されます。両方のフェールオーバー グループをペアのうち一方の装置でアクティブ状態に設定して、もう一方の装置にはスタンバイ状態の

フェールオーバー グループが含まれるように設定できます。ただし、さらに一般的なコンフィギュレーションでは、各フェールオーバー グループに異なる役割プリファレンスを割り当て、装置ごとにそれぞれ 1 つをアクティブにして、デバイス全体でトラフィックが分散するようにします。

（注）　ASA は、フェールオーバーとは別にロードバランシングも提供します。フェールオーバーとロード バランシングはどちらも同じコンフィギュレーションに存在できます。ロードバランシングについては 「ロード バランシングの設定」（P.70-13）を参照してください。

各フェールオーバー グループがアクティブになる装置は、次のように特定されます。

- ピア装置が使用できないときに装置がブートされると、両方のフェールオーバー グループがピア装置でアクティブになります。
- ピア装置がアクティブ（両方のフェールオーバー グループがアクティブ状態）の場合に装置がブートされると、フェールオーバー グループは、アクティブ装置でアクティブ状態のままになります。これは、次のいずれかの状態になるまで、フェールオーバー グループのプライマリ プリファレンスまたはセカンダリ プリファレンスには関係ありません。
  - フェールオーバーが発生した。
  - 手動でフェールオーバーを強制実行した。
  - フェールオーバー グループにプリエンプションを設定した。この設定により、優先する装置が使用可能になると、フェールオーバー グループはその装置上で自動的にアクティブになります。
- 同時に両方の装置がブートされると、コンフィギュレーションが同期化された後、各フェールオーバー グループは優先する装置上でアクティブになります。

デバイスの初期化とコンフィギュレーションの同期

コンフィギュレーションの同期がとられるのは、フェールオーバー ペアの一方または両方の装置がブートされたときです。コンフィギュレーションは、次のように同期化されます。

- ピア装置がアクティブ（ピア装置で両方のフェールオーバー グループがアクティブ）の間に装置がブートされると、ブートされた装置のプライマリまたはセカンダリ指定に関係なく、ブートされた装置はアクティブ装置にアクセスして実行コンフィギュレーションを取得します。
- 両方の装置が同時にブートされた場合、セカンダリ装置はプライマリ装置から実行コンフィギュレーションを取得します。

複製が開始されると、コンフィギュレーションを送信する装置の ASA コンソールに「Beginning configuration replication: Sending to mate」というメッセージが表示され、複製が完了すると、ASA に「End Configuration Replication to mate」というメッセージが表示されます。複製中、コンフィギュレーションを送信する装置に入力されたコマンドがピア装置に適切に複製されないことがあり、またコンフィギュレーションを受信する装置に入力されたコマンドが、受信中のコンフィギュレーションによって上書きされることがあります。コンフィギュレーションの複製処理中には、フェールオーバー ペアのどちらの装置にもコマンドを入力しないでください。コンフィギュレーションのサイズによって、複製は数秒で済むことも数分かかることもあります。

コンフィギュレーションを受信する装置の場合、コンフィギュレーションは実行メモリにだけ存在します。同期後にコンフィギュレーションをフラッシュ メモリに保存するには、フェールオーバー グループ 1 がアクティブ状態にあるシステム実行スペースに **write memory all** コマンドを入力します。コマンドはピア装置に複製され、コンフィギュレーションがフラッシュ メモリに書き込まれます。このコマンドで **all** キーワードを使用すると、システムとすべてのコンテキスト コンフィギュレーションが保存されます。

（注） 外部のサーバに保存されたスタートアップ コンフィギュレーションは、ネットワーク経由で両方の装置からアクセスできます。そのため、各装置で個別に保存する必要はありません。または、コンテキスト コンフィギュレーション ファイルをプライマリ装置のディスク上から外部サーバにコピーし、それからセカンダリ装置のディスクにコピーできます。セカンダリ装置がリロードされると、そのコンテキストが使用可能になります。

コマンドの複製

両方の装置が動作中になった後で、次のように、コマンドが一方の装置からもう一方の装置に複製されます。

- セキュリティ コンテキスト内で入力されたコマンドは、そのセキュリティ コンテキストがアクティブ状態で表示される装置から、ピア装置に複製されます。

（注） あるコンテキストがある装置でアクティブ状態と見なされるのは、そのコンテキストが属するフェールオーバー グループがその装置上でアクティブ状態である場合です。

- システム実行スペースで入力されたコマンドは、フェールオーバー グループ 1 がアクティブ状態の装置から、フェールオーバー グループ 1 がスタンバイ状態の装置に複製されます。
- 管理コンテキストで入力されたコマンドは、フェールオーバー グループ 1 がアクティブ状態の装置から、フェールオーバー グループ 1 がスタンバイ状態の装置に複製されます。

コマンドの複製を行うのに適切な装置上でコマンドを入力しなかった場合は、コンフィギュレーションは非同期になります。この変更内容は、次回に初期コンフィギュレーション同期が行われると失われることがあります。

表 10-1 に、スタンバイ装置に複製されるコマンドと複製されないコマンドを示します。

表 10-1　コマンドの複製

スタンバイ装置に複製されるコマンド	スタンバイ装置に複製されないコマンド
mode、**firewall**、および **failover lan unit** を除く、すべてのコンフィギュレーション コマンド	**copy running-config startup-config** を除く、すべての形式の **copy** コマンド
copy running-config startup-config	**write memory** を除く、すべての形式の **write** コマンド
delete	**debug**
mkdir	**failover lan unit**
rename	**firewall**
rmdir	**mode**
write memory	**show**

write standby コマンドを使用すると、非同期になったコンフィギュレーションを再同期化できます。アクティブ/アクティブ フェールオーバーの場合、**write standby** コマンドは次のように動作します。

- システム実行スペースで **write standby** コマンドを入力した場合は、ASA 上のシステム コンフィギュレーションおよびすべてのセキュリティ コンテキストのコンフィギュレーションがピア装置に書き込まれます。これには、スタンバイ状態のセキュリティ コンテキストのコンフィギュレーション情報が含まれています。このコマンドの入力は、フェールオーバー グループ 1 がアクティブ状態の装置上のシステム実行スペースで行う必要があります。

  （注）　セキュリティ コンテキストがピア装置でアクティブ状態にある場合、**write standby** コマンドによって、これらのコンテキストのアクティブな接続が切断されます。**write standby** コマンドを入力する前に、コンフィギュレーションを提供する装置で **failover active** コマンドを使用して、その装置ですべてのコンテキストがアクティブになるようにします。

- セキュリティ コンテキストで **write standby** コマンドを入力すると、セキュリティ コンテキストのコンフィギュレーションだけがピア装置に書き込まれます。このコマンドの入力は、セキュリティ コンテキストがアクティブ状態で表示される装置のセキュリティ コンテキストで行う必要があります。

複製されたコマンドは、ピア装置に複製された場合、フラッシュ メモリに保存されません。実行コンフィギュレーションに追加されます。複製されたコマンドを両方の装置のフラッシュ メモリに保存するには、変更を行った装置で **write memory** または **copy running-config startup-config** コマンドを使用します。コマンドはピア装置に複製されて、コンフィギュレーションがピア装置のフラッシュ メモリに保存されます。

フェールオーバーのトリガー

アクティブ/アクティブ フェールオーバーでは、次のいずれかのイベントが発生すると、フェールオーバーが装置レベルでトリガーされます。

- 装置でハードウェア障害が発生した。
- 装置で電源障害が発生した。
- 装置でソフトウェア障害が発生した。
- フェールオーバーを強制実行した。（「フェールオーバーの強制実行」（P.10-27）を参照）。

フェールオーバーは、次のいずれかのイベントが発生すると、フェールオーバー グループ レベルでトリガーされます。

- グループ内の多くのモニタ対象インターフェイスが故障した。
- フェールオーバーを強制実行した。（「フェールオーバーの強制実行」（P.10-27）を参照）。

フェールオーバー グループ内のインターフェイスの数または割合を指定することで各フェールオーバー グループにフェールオーバーしきい値を設定し、故障したインターフェイスがこのしきい値（インターフェイスの数または割合）を超えた場合にそのグループは故障したと判断されます。フェールオーバー グループには複数のコンテキストを含めることができ、また各コンテキストには複数のインターフェイスを含めることができるので、1 つのコンテキストのインターフェイスがすべて故障しても、そのコンテキストに関連するフェールオーバー グループが故障と判断されない可能性があります。

インターフェイスと装置のモニタリングの詳細については、「フェールオーバー ヘルスのモニタリング」（P.8-20）を参照してください。

フェールオーバーのアクション

アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、フェールオーバーは、システムごとに行うのではなく、フェールオーバー グループごとに行われます。たとえば、プライマリ装置で両方のフェールオーバー グループをアクティブと指定し、フェールオーバー グループ 1 が故障すると、フェールオーバー グループ 2 はプライマリ装置でアクティブのままですが、フェールオーバー グループ 1 はセカンダリ装置でアクティブになります。

（注） アクティブ/アクティブ フェールオーバーを構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにしてください。

表 10-2 に、各障害イベントに対するフェールオーバー アクションを示します。各障害イベントに対して、ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ フェールオーバー グループのアクション、およびスタンバイ フェールオーバー グループのアクションを示します。

表 10-2　アクティブ/アクティブ フェールオーバーのフェールオーバー動作

障害の状況	ポリシー	アクティブ グループのアクション	スタンバイ グループのアクション	注釈
装置で電源断またはソフトウェア障害が発生した	フェールオーバー	スタンバイになり、故障とマークする	アクティブになる アクティブに故障とマークする	フェールオーバー ペアの装置が故障すると、その装置のアクティブ フェールオーバー グループはすべて故障とマークされ、ピア装置のフェールオーバー グループがアクティブになります。
アクティブ フェールオーバー グループにおけるしきい値を超えたインターフェイス障害	フェールオーバー	アクティブ グループに故障とマークする	アクティブになる	なし。
スタンバイ フェールオーバー グループにおけるしきい値を超えたインターフェイス障害	フェールオーバーなし	動作なし	スタンバイ グループに故障とマークする	スタンバイ フェールオーバー グループが故障とマークされている場合、インターフェイス フェールオーバー障害しきい値を超えても、アクティブ フェールオーバー グループはフェールオーバーを行いません。
以前にアクティブであったフェールオーバー グループの復旧	フェールオーバーなし	動作なし	動作なし	フェールオーバー グループのプリエンプションが設定されている場合を除き、フェールオーバー グループは現在の装置でアクティブのままです。
スタートアップ時にフェールオーバー リンクに障害が発生した	フェールオーバーなし	アクティブになる	アクティブになる	スタートアップ時にフェールオーバー リンクがダウンしていると、両方の装置の両方のフェールオーバー グループがアクティブになります。

表 10-2　アクティブ/アクティブ フェールオーバーのフェールオーバー動作 （続き）

障害の状況	ポリシー	アクティブ グループのアクション	スタンバイ グループのアクション	注釈
ステートフル フェールオーバー リンクに障害が発生した	フェールオーバーなし	動作なし	動作なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。
動作中にフェールオーバー リンクに障害が発生した	フェールオーバーなし	n/a	n/a	各装置で、フェールオーバー インターフェイスが故障とマークされます。フェールオーバー リンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。

オプションのアクティブ/アクティブ フェールオーバー設定

次のアクティブ/スタンバイ フェールオーバー オプションは、最初にフェールオーバーを設定するときに、またはフェールオーバーを設定した後で設定できます。

- フェールオーバー グループ プリエンプション：プライマリまたはセカンダリのプライオリティをフェールオーバー グループに割り当てて、両方の装置が同時にブートされるときに、フェールオーバー グループがどの装置上でアクティブになるかを指定します。
- ステートフル フェールオーバーでの HTTP 複製：ステート情報の複製に接続を含めることができます。
- インターフェイス モニタリング：装置の最大 250 のインターフェイスをモニタし、フェールオーバーに影響を与えるインターフェイスを制御できます。
- インターフェイス ヘルス モニタリング：セキュリティ アプライアンスがより早くインターフェイスの障害を検出して対応できるようにします。
- フェールオーバー基準の設定：インターフェイス数またはモニタされているインターフェイスの割合を指定して、この数または割合を超えたインターフェイスに障害が発生した場合にフェールオーバーが発生するようにできます。
- 仮想 MAC アドレスの設定：セカンダリ装置がプライマリ装置よりも前にオンラインになっても、セカンダリ装置がアクティブ装置である場合、正しい MAC アドレスを使用するようにします。

アクティブ/アクティブ フェールオーバーのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
ASA 5505	サポートしない
ASA 5510、 ASA 5512-X	Security Plus ライセンス
他のすべてのモデル	基本ライセンス

フェールオーバー ユニットは、各ユニット上で同一のライセンスを必要としません。両方のユニット上にライセンスがある場合、これらのライセンスは単一の実行フェールオーバー クラスタ ライセンスに結合されます。このルールの例外は次のとおりです。

- ASA 5510 および 5512-X の Security Plus ライセンスの場合 : 基本ライセンスはフェールオーバーをサポートしないため、基本ライセンスのみを保持するスタンバイ ユニットではフェールオーバーをイネーブルにできません。
- ASA 5500-X の IPS モジュール ライセンスの場合：他のモデルで各装置のハードウェア モジュールを購入する必要があるのと同様、各装置用の IPS モジュール ライセンスを購入する必要があります。
- 暗号化ライセンス：両方のユニットに同じ暗号化ライセンスが必要です。

アクティブ/ アクティブ フェールオーバーの前提条件

アクティブ/アクティブ フェールオーバーでは、両方の装置に以下のものが必要です。

- 同じハードウェア モデル。
- 同じインターフェイス数。
- 同じタイプのインターフェイス。
- 同じソフトウェア バージョン（メジャー（最初の番号）およびマイナー（2 番目の番号）のバージョン番号が同じ）。ただし、アップグレード プロセス中は、異なるバージョンのソフトウェアを使用できます。たとえば、ある装置をバージョン 7.0(1) からバージョン 7.9(2) にアップグレードし、フェールオーバーをアクティブ状態のままにできます。長期的に互換性を維持するために、両方の装置を同じバージョンにアップグレードすることをお勧めします。
- 同じソフトウェア コンフィギュレーション。
- 同じモード（マルチコンテキスト モード）。
- 適切なライセンス。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

マルチ コンテキスト モードでだけサポートされます。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 フェールオーバーがサポートされています。

モデルのガイドライン

アクティブ/アクティブ フェールオーバーは、Cisco ASA 5505 では使用できません。

その他のガイドラインと制限事項

同じコンテキスト内の 2 個のインターフェイスを、同じ ASR グループ内で設定してはなりません。

ASA フェールオーバー ペアに接続されたスイッチ上でポート セキュリティを設定すると、フェールオーバー イベントが発生したときに通信の問題が起きることがあります。これは、1 つのセキュア ポートで設定または学習されたセキュア MAC アドレスが別のセキュア ポートに移動した場合に、スイッチのポート セキュリティ機能によって違反フラグが付けられるためです。

ASA フェールオーバー複製は、複数のコンテキストで設定を同時に変更しようとすると、失敗します。回避策は、各ユニットで設定変更を順番に加えることです。

アクティブ/アクティブ フェールオーバーでは次の機能はサポートされていません。

- フェールオーバー ペアの両方の装置からパケットを受信するには、すべてのインターフェイスにスタンバイ IP アドレスを設定する必要があります。
- スタンバイ IP アドレスは、現在スタンバイ装置であるセキュリティ アプライアンスで使用され、アクティブ IP アドレスと同じサブネットに存在する必要があります。
- 2 つのフェールオーバー グループの最大数を定義できます。
- フェールオーバー グループは、マルチ コンテキスト モード用に設定されているデバイスのシステム コンテキストに対してだけ追加できます。
- 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。
- **failover group** コマンドを入力すると、フェールオーバー グループ コマンド モードになります。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。
- **failover polltime interface**、**failover interface-policy**、**failover replication http**、**failover mac address** の各コマンドは、アクティブ/アクティブ フェールオーバー コンフィギュレーション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ます。フェールオーバー グループに割り当てられていないコンテキストはすべて、デフォルトでフェールオーバー グループ 1 になります。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。
- VPN フェールオーバーは使用できません （アクティブ/スタンバイ フェールオーバー設定だけは使用できます）。

アクティブ/アクティブ フェールオーバーの設定

この項では、イーサネット フェールオーバー リンクを使用してアクティブ/アクティブ フェールオーバーを設定する方法について説明します。LAN ベースのフェールオーバーを設定するときは、セカンダリ デバイスがプライマリ デバイスから実行コンフィギュレーションを取得する前に、セカンダリ デバイスをブートストラップしてフェールオーバー リンクを認識させる必要があります。

この項は、次の内容で構成されています。

- 「セカンダリ フェールオーバー装置の設定」（P.10-13）
- 「オプションのアクティブ/アクティブ フェールオーバー設定値の設定」（P.10-15）
- 「非対称にルーティングされたパケットのサポートの設定」（P.10-21）

アクティブ/アクティブ フェールオーバーの設定のタスク フロー

アクティブ/スタンバイ フェールオーバーを設定するには、次の手順を実行します。

ステップ 1　「プライマリ フェールオーバー装置の設定」（P.10-10）に従って、プライマリ装置を設定します。

ステップ 2　「セカンダリ フェールオーバー装置の設定」（P.10-13）に従って、セカンダリ装置を設定します。

ステップ 3　（任意）「オプションのアクティブ/アクティブ フェールオーバー設定」（P.10-7）に従って、オプションのアクティブ/アクティブ フェールオーバー設定を行います。

プライマリ フェールオーバー装置の設定

この項の手順に従って、アクティブ/アクティブ フェールオーバー コンフィギュレーションでプライマリ装置を設定します。この手順では、プライマリ装置でフェールオーバーをイネーブルにするために必要な最小のコンフィギュレーションが用意されています。

制限事項

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する場合は、ステートフル フェールオーバー リンクの IP アドレスは設定しないでください。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設定するには、後述の手順の **failover interface ip** コマンドを使用します。

前提条件

- すべての IP アドレスのスタンバイ アドレスを第 13 章「インターフェイス コンフィギュレーションの実行（ルーテッド モード）」または第 14 章「インターフェイス コンフィギュレーションの実行（トランスペアレント モード）」に従って設定します。
- この手順はシステム実行スペースで実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	**failover lan unit primary**	装置をプライマリ装置に指定します。
ステップ 2	**failover lan interface** *if_name phy_if* **例：** `hostname(config)# failover lan interface folink GigabitEthernet0/3`	フェールオーバー インターフェイスとして使用するインターフェイスを指定します。 *if_name* 引数は、*phy_if* 引数で指定されたインターフェイスに名前を割り当てます。 *phy_if* 引数は、物理ポート名（Ethernet1 など）にすることも、すでに作成されているサブインターフェイス（Ethernet0/2.3 など）にすることもできます。ASASM では、*phy_if* は VLAN を指定します。このインターフェイスは、他の目的に使用しないでください（オプションのステートフル フェールオーバー リンクは除く）。

ステップ 3	**failover interface ip** *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address*/*prefix* **standby***ipv6_address*]
	
	例：
	`hostname(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2`
	
	`hostname(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby 2001:a0a:b00::a0a:b71`
		アクティブおよびスタンバイ IP アドレスをフェールオーバー リンクに割り当てます。IPv4 アドレスまたは IPv6 アドレスのいずれかをインターフェイスに割り当てることができます。両方のアドレス タイプをフェールオーバー リンクに割り当てることはできません。
		
		スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。スタンバイ アドレスのサブネット マスクを指定する必要はありません。
		
		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。フェールオーバー リンクのアクティブ IP アドレスは、常にプライマリ装置にあります。スタンバイ IP アドレスは、セカンダリ装置にあります。

ステップ 4	**failover link** *if_name phy_if* **例：** `hostname(config)# failover link folink GigabitEthernet0/2`	（任意）ステートフル フェールオーバー リンクとして使用するインターフェイスを指定します。 **（注）** ステートフル フェールオーバー リンクがフェールオーバー リンクまたはデータ インターフェイスを使用する場合は、*if_name* 引数を指定することだけが必要です。 *if_name* 引数は、*phy_if* 引数で指定されたインターフェイスに論理名を割り当てます。*phy_if* 引数は、物理ポート名（Ethernet1 など）にすることも、すでに作成されているサブインターフェイス（Ethernet0/2.3 など）にすることもできます。ASASM では、*phy_if* は VLAN を指定します。このインターフェイスは、他の目的に使用しないでください（オプションのフェールオーバー リンクは除く）。

	コマンド	目的
ステップ 5	**failover interface ip** *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address*/*prefix* **standby***ipv6_address*] **例：** hostname(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2 hostname(config)# failover interface ip statelink 2001:a1a:b00::a0a:a70/64 standby 2001:a1a:b00::a0a:a71	(任意) アクティブおよびスタンバイ IP アドレスをステートフル フェールオーバー リンクに割り当てます。IPv4 アドレスまたは IPv6 アドレスのいずれかをインターフェイスに割り当てることができます。両方のアドレス タイプをステートフル フェールオーバー リンクに割り当てることはできません。 **(注)** ステートフル フェールオーバー リンクがフェールオーバー リンクまたはデータ インターフェイスを使用する場合は、この手順をスキップします。インターフェイスのアクティブおよびスタンバイ IP アドレスは、すでに定義しています。 スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。スタンバイ アドレスのサブネット マスクを指定する必要はありません。 ステートフル フェールオーバー リンク IP アドレスおよび MAC アドレスは、データ インターフェイスを使用しない限り、フェールオーバー時に変更されません。アクティブ IP アドレスは、常にプライマリ装置にあります。スタンバイ IP アドレスは、セカンダリ装置にあります。
ステップ 6	**interface** *phy_if* **no shutdown** **例：** hostname(config)# interface GigabitEthernet 0/3 hostname(config-if)# no shutdown	インターフェイスをイネーブルにします。 **(注)** ステートフル フェールオーバー リンクがフェールオーバー リンクまたは標準データ インターフェイスを使用する場合は、このステップをスキップします。インターフェイスは、すでにイネーブルです。
ステップ 7	**failover group** {**1** | **2**} **primary** | **secondary** **例：** hostname(config)# failover group 1 hostname(config-fover-group)# primary hostname(config-fover-group)# exit hostname(config)# failover group 2 hostname(config-fover-group)# secondary hostname(config-fover-group)# exit	フェールオーバー グループを設定します。 使用できるフェールオーバー グループは 2 つだけです。**failover group** コマンドは、指定されたフェールオーバー グループが存在しない場合はこれを作成し、フェールオーバー グループ コンフィギュレーション モードに移行します。 フェールオーバー グループごとに **primary** または **secondary** コマンドを使用して、フェールオーバー グループがプライマリ プリファレンスとセカンダリ プリファレンスのどちらを持つかを指定します。同じプリファレンスを両方のフェールオーバー グループに割り当てることができます。トラフィック共有コンフィギュレーションの場合は、各フェールオーバー グループに異なる装置プリファレンスを割り当てる必要があります。 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。 例では、フェールオーバー グループ 1 をプライマリ プリファレンスとして、フェールオーバー グループ 2 をセカンダリ プリファレンスとして割り当てています。

	コマンド	目的
ステップ 8	**context** *name* **join-failover-group {1 | 2}** **例：** hostname(config)# context Eng hostname(config-context)# join-failover-group 1 hostname(config-context) exit	各ユーザ 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（コンテキスト コンフィギュレーション モードで）。 未割り当てのコンテキストはすべて、自動的にフェールオーバー グループ 1 に割り当てられます。管理コンテキストは、常にフェールオーバー グループ 1 のメンバです。
ステップ 9	**failover** **例：** hostname(config)# failover	フェールオーバーをイネーブルにします。
ステップ 10	**copy running-config startup-config** **例：** hostname(config)# copy running-config startup-config	システム コンフィギュレーションをフラッシュ メモリに保存します。

セカンダリ フェールオーバー装置の設定

この項の手順に従って、アクティブ/アクティブ フェールオーバー コンフィギュレーションでセカンダリ装置を設定します。この手順では、セカンダリ装置でフェールオーバーをイネーブルにするために必要な最小のコンフィギュレーションが用意されています。

手順の詳細

セカンダリ フェールオーバー装置を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**failover lan interface** *if_name phy_if* **例：** `hostname(config)# failover lan interface folink GigabitEthernet0/3`	フェールオーバー インターフェイスとして使用するインターフェイスを指定します。 *if_name* 引数は、*phy_if* 引数で指定されたインターフェイスに名前を割り当てます。 *phy_if* 引数は、物理ポート名（Ethernet1 など）にすることも、すでに作成されているサブインターフェイス（Ethernet0/2.3 など）にすることもできます。ASASM では、*phy_if* は VLAN を指定します。このインターフェイスは、他の目的に使用しないでください（オプションのステートフル フェールオーバー リンクは除く）。

ステップ 2	**failover interface ip** *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address*/*prefix* **standby***ipv6_address*]
	
	例：
	`hostname(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2`
	
	`hostname(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby 2001:a0a:b00::a0a:b71`
		アクティブおよびスタンバイ IP アドレスをフェールオーバー リンクに割り当てます。IPv4 アドレスまたは IPv6 アドレスのいずれかをインターフェイスに割り当てることができます。両方のアドレス タイプをフェールオーバー リンクに割り当てることはできません。
		
		スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。スタンバイ アドレスのサブネット マスクを指定する必要はありません。
		
		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。フェールオーバー リンクのアクティブ IP アドレスは、常にプライマリ装置にあります。スタンバイ IP アドレスは、セカンダリ装置にあります。

ステップ 3	**interface** *phy_if* **no shutdown** **例：** `hostname(config-if)# interface GigabitEthernet0/3`	インターフェイスをイネーブルにします。
ステップ 4	**failover lan unit secondary** **例：** `hostname(config)# failover lan unit secondary`	（任意）この装置をセカンダリ装置に指定します。 **（注）** 以前に設定されていない場合、装置はデフォルトでセカンダリに指定されているので、この手順はオプションです。
ステップ 5	**failover** **例：** `hostname(config)# failover`	フェールオーバーをイネーブルにします。 フェールオーバーをイネーブルにすると、実行メモリのコンフィギュレーションがアクティブ装置からスタンバイ装置に送信されます。コンフィギュレーションが同期すると、メッセージ「Beginning configuration replication: Sending to mate」および「End Configuration Replication to mate」がアクティブ装置のコンソールに表示されます。

	コマンド	目的
ステップ 6	**copy running-config startup-config** **例：** hostname(config)# copy running-config startup-config	コンフィギュレーションをフラッシュ メモリに保存します。 実行コンフィギュレーションの複製が完了した後で、コマンドを入力します。
ステップ 7	**no failover active group** group_id **例：** hostname(config)# no failover active group 1	必要に応じて、プライマリ装置でアクティブなフェールオーバー グループすべてを強制的にセカンダリ装置でアクティブ状態にします。フェールオーバー グループを強制的にセカンダリ装置でアクティブにするには、プライマリ装置のシステム実行スペースでこのコマンドを入力します。 *group_id* 引数は、セカンダリ装置でアクティブにするグループを指定します。

オプションのアクティブ/アクティブ フェールオーバー設定値の設定

次のオプションのアクティブ/アクティブ フェールオーバー設定値は、最初にフェールオーバーを設定するときでも、フェールオーバーがすでに設定された後でも設定できます。特に指定のない限り、コマンドは、フェールオーバー グループ 1 がアクティブ状態の装置で入力する必要があります。

この項は、次の内容で構成されています。

フェールオーバー グループのプリエンプションの設定

プライマリまたはセカンダリのプライオリティをフェールオーバー グループに割り当てると、両方の装置が同時にブートされるときに、フェールオーバー グループがどの装置上でアクティブになるかが指定されます。しかし、ある装置がもう一方の装置よりも先にブートした場合、どちらのフェールオーバー グループもその装置上でアクティブになります。もう一方の装置がオンラインになると、その装置にプライオリティを認めているフェールオーバー グループはいずれも、その装置ではアクティブになりません。ただし、手動で強制された場合、フェールオーバーが行われた場合、またはそのフェール

オーバー グループが **preempt** コマンドで設定されている場合は除きます。**preempt** コマンドによって、フェールオーバー グループは、指定された装置が使用可能になると、その装置で自動的にアクティブになります。

特定のフェールオーバー グループにプリエンプションを設定するには、次のコマンドを入力します。

	コマンド	目的
ステップ 1	**failover group** {**1** | **2**} **例：** hostname(config)# failover group 1	フェールオーバー グループを指定します。
ステップ 2	**preempt** [delay] **例：** hostname(config-fover-group)# preempt 1200	指定した装置で、フェールオーバー グループがアクティブになります。 オプションの *delay* 値に秒数を入力して、その時間フェールオーバー グループが現在の装置でアクティブ状態に維持され、その後に指定された装置で自動的にアクティブになるようにできます。有効な値は 1 ～ 1200 です。 **（注）** ステートフル フェールオーバーがイネーブルの場合、プリエンプションは、フェールオーバー グループが現在アクティブになっている装置から接続が複製されるまで遅延されます。

例

次の例では、プライマリ装置のフェールオーバー グループ 1 をより高いプライオリティに設定し、セカンダリ装置のフェールオーバー グループ 2 をより高いプライオリティに設定します。どちらのフェールオーバー グループも preempt コマンドで待機時間が 100 秒に設定されているため、グループは、ユニットが使用可能になった 100 秒後に自動的にその優先ユニットでアクティブになります。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

ステートフル フェールオーバーでの HTTP 複製のイネーブル化

HTTP 接続をステート情報に含めることができるようにするには、HTTP 複製をイネーブルにする必要があります。HTTP 接続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再試行するため、HTTP 接続は複製されるステート情報に自動的には含まれません。

replication http コマンドを使用すると、ステートフル フェールオーバーがイネーブルになっている場合に、フェールオーバー グループに HTTP ステート情報を複製させることができます。

	コマンド	目的
ステップ 1	**failover group** {**1** | **2**} **例：** hostname(config)# failover group 1	フェールオーバー グループを指定します。
ステップ 2	**replication http** **例：** hostname(config-fover-group)# replication http	指定したフェールオーバー グループの HTTP ステートの複製をイネーブルにします。 このコマンドは、設定されているフェールオーバー グループだけに影響します。両方のフェールオーバー グループの HTTP ステート複製をイネーブルにするには、各グループで次のコマンドを入力する必要があります。次のコマンドは、システム実行スペースで入力する必要があります。

例

次の例では、フェールオーバー グループで可能な設定を示します。

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

インターフェイス モニタリングのディセーブル化とイネーブル化

特定のインターフェイスのモニタリングをディセーブルにし、別のモニタリングをイネーブルにすることで、フェールオーバー ポリシーに影響を与えるインターフェイスを制御できます。この機能を使用すると、重要度の低いネットワークに接続されているインターフェイスがフェールオーバー ポリシーに影響を与えないようにできます。

1 台の装置で最大 250 のインターフェイスをモニタできます。デフォルトでは、物理インターフェイスのモニタリングはイネーブルに、サブインターフェイスのモニタリングはディセーブルになっています。

インターフェイスのポーリング周期期間ごとに、セキュリティ アプライアンス フェールオーバー ペアの間で、hello メッセージが交換されます。フェールオーバー インターフェイスのポーリング時間は 3 ～ 15 秒です。たとえば、ポーリング時間を 5 秒に設定すると、あるインターフェイスで 5 回連続して hello が検出されないと（25 秒間）、そのインターフェイスでテストが開始します。

モニタ対象のフェールオーバー インターフェイスには、次のステータスが設定されます。

- Unknown：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- Normal：インターフェイスはトラフィックを受信しています。
- Testing：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。

- Link Down：インターフェイスまたは VLAN は管理のためにダウンしています。
- No Link：インターフェイスの物理リンクがダウンしています。
- Failed：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

アクティブ/アクティブ フェールオーバーでは、このコマンドはコンテキスト内でだけ有効です。

特定のインターフェイスについてインターフェイス モニタリングをイネーブルまたはディセーブルにするには、次のコマンドのいずれかを入力します。

次のいずれかを実行します。	
no monitor-interface *if_name* **例：** hostname/context (config)# no monitor-interface 1	インターフェイスのヘルス モニタリングをディセーブルにします。
monitor-interface *if_name* **例：** hostname/context (config)# monitor-interface 1	インターフェイスのヘルス モニタリングをイネーブルにします。

例

次の例では、「inside」という名前のインターフェイスでモニタリングをイネーブルにしています。

```
hostname(config)# monitor-interface inside
hostname(config)#
```

インターフェイス ヘルス モニタリングの設定

ASA は、各データ インターフェイスから hello パケットを送信して、インターフェイス ヘルスをモニタします。保持時間の半分以上が経過しても ASA がピア装置の対応するインターフェイスから hello パケットを受信しない場合、追加のインターフェイスのテストが開始されます。hello パケットまたはテストの正常終了の結果が指定した保持時間内に受信されない場合、インターフェイスは失敗としてマークされます。失敗したインターフェイスの数がフェールオーバー基準を満たしている場合、フェールオーバーが発生します。

ポーリング時間および保持時間を短縮すると、ASA はインターフェイスの障害に対してより迅速な検出と応答を実行できますが、多くのシステム リソースを消費することがあります。

インターフェイスのデフォルトのポーリング時間を変更するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**failover group** {**1** | **2**} **例：** hostname(config)# failover group 1	フェールオーバー グループを指定します。
ステップ 2	**polltime interface** *seconds* **例：** hostname(config-fover-group)# polltime interface seconds	アクティブ/アクティブ フェールオーバー コンフィギュレーションでのデータ インターフェイスのポーリング時間と保持時間を指定します。 ポーリング時間に有効な値は 1 ～ 15 秒で、オプションの **msec** キーワードを使用すると、500 ～ 999 ミリ秒です。hello パケットを受信できなかったときからインターフェイスが失敗としてマークされるまでの時間が、保持時間によって決まります。保持時間に有効な値は、5 ～ 75 秒です。ポーリング時間の 5 倍に満たない保持時間は入力できません。

例

次の部分的な例では、フェールオーバー グループで可能な設定を示します。フェールオーバー グループ 1 のデータ インターフェイスのインターフェイス ポーリング時間を 500 ミリ秒に設定し、保持時間を 5 秒に設定します。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# polltime interface msec 500 holdtime 5
hostname(config-fover-group)# exit
hostname(config)#
```

フェールオーバー基準の設定

デフォルトでは、1 つのインターフェイス障害でフェールオーバーが行われます。インターフェイス数またはモニタされているインターフェイスの割合を指定して、この数または割合を超えたインターフェイスに障害が発生した場合にフェールオーバーが発生するようにできます。フェールオーバー基準は、フェールオーバー グループごとに指定されます。

指定されたフェールオーバー グループのデフォルト フェールオーバー基準を変更するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**failover group** {**1** | **2**} **例：** hostname(config)# failover group 1	フェールオーバー グループを指定します。
ステップ 2	**interface-policy** *num*[%] **例：** hostname(config-fover-group)# interface-policy 225	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します。 インターフェイスの具体的な数を指定するときは、*num* 引数に 1 ～ 250 を設定できます。インターフェイスの割合を指定するときは、*num* 引数に 1 ～ 100 を設定できます。

次の部分的な例では、フェールオーバー グループで可能な設定を示します。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# interface-policy 25%
hostname(config-fover-group)# exit
hostname(config)#
```

仮想 MAC アドレスの設定

アクティブ/アクティブ フェールオーバーでは、すべてのインターフェイスで仮想 MAC アドレスを使用します。仮想 MAC アドレスを指定しない場合は、次のように計算されます。

- アクティブ装置のデフォルトの MAC アドレス：
  00a0.c9*physical_port_number.failover_group_id*01
- スタンバイ装置のデフォルトの MAC アドレス：
  00a0.c9*physical_port_number.failover_group_id*02

（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。ネットワーク上で MAC アドレスが重複することを回避するには、すべてのフェールオーバー グループに対して、必ず各物理インターフェイスに仮想のアクティブおよびスタンバイ MAC アドレスを割り当てます。

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。

show interface コマンドを使用して、インターフェイスが使用している MAC アドレスを表示します。

インターフェイスの特定のアクティブおよびスタンバイ MAC アドレスを設定するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**failover group** {**1** | **2**} **例：** `hostname(config)# failover group 1`	フェールオーバー グループを指定します。
ステップ 2	**mac address** *phy_if active_mac standby_mac* **例：** `hostname(config-fover-group)# mac address gigabitethernet1/0 0000.a000.a011 0000.a000.a012`	アクティブ装置およびスタンバイ装置の仮想 MAC アドレスを指定します。 *phy_if* 引数は、インターフェイスの物理名（GigabitEthernet1/0 など）です。ASASM では、*phy_if* は VLAN を指定します。*active_mac* および *standby_mac* 引数は、H.H.H 形式（H は 16 ビットの 16 進数）の MAC アドレスです。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。 *active_mac* アドレスはインターフェイスのアクティブ IP アドレスに関連付けられ、*standby_mac* はインターフェイスのスタンバイ IP アドレスに関連付けられます。

例

次の部分的な例では、フェールオーバー グループで可能な設定を示します。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac address gigabitethernet1/0 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

非対称にルーティングされたパケットのサポートの設定

アクティブ/アクティブ フェールオーバーで動作中の場合、装置は、ピア装置を経由して送信された接続用の返送パケットを受信することがあります。そのパケットを受信する ASA にはそのパケットの接続情報がないために、パケットはドロップされます。これが最もよく発生するのは、アクティブ/アクティブ フェールオーバー ペアの ASA 2 台が異なるサービス プロバイダーに接続されており、発信接続で NAT アドレスが使用されていない場合です。

返送パケットのドロップは、ドロップが発生する可能性のあるインターフェイスで **asr-group** コマンドを使用することで防止できます。**asr-group** コマンドで設定されたインターフェイスがセッション情報を持たないパケットを受信すると、同じグループ内の他のインターフェイスのセッション情報をチェックします。一致する情報が見つからない場合、パケットはドロップされます。一致する情報が見つかると、次の動作のうちいずれかが開始します。

- 着信トラフィックがピア装置に発信されると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットは他の装置にリダイレクトされます。このリダイレクトは、セッションがアクティブである限り続行されます。
- 着信トラフィックが同じ装置の別のインターフェイスに発信されると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットはストリームに再注入されます。

（注）　非対称ルーティングのサポートを設定するために **asr-group** コマンドを使用する方法は、**nailed** オプションを指定して static コマンドを使用する方法よりも安全です。**asr-group** コマンドは、非対称ルーティングを提供しません。非対称にルーティングされたパケットを正しいインターフェイスに戻します。

asr-group コマンドは、非対称ルーティングを提供しません。非対称にルーティングされたパケットを正しいインターフェイスに戻します。

前提条件

非対称ルーティングのサポートを正常に機能させるには、次の設定がされている必要があります。

- アクティブ/アクティブ フェールオーバー
- ステートフル フェールオーバー：アクティブ フェールオーバー グループにあるインターフェイスのセッションのステート情報を、スタンバイ フェールオーバー グループに渡します。
- replication http：HTTP セッションのステート情報は、スタンバイ フェールオーバー グループに渡されないため、スタンバイ インターフェイスに存在しません。ASA が非対称にルーティングされた HTTP パケットを再ルーティングできるように、HTTP ステート情報を複製する必要があります。

フェールオーバーを設定しなくても **asr-group** コマンドをインターフェイスに設定できますが、ステートフル フェールオーバーがイネーブルになるまで効果はありません。

手順の詳細

非対称にルーティングされたパケットのサポートを設定するには、次の手順を実行します。

ステップ 1　フェールオーバー ペアにアクティブ/アクティブ ステートフル フェールオーバーを設定します。「アクティブ/アクティブ フェールオーバーの設定」（P.10-9）を参照してください。

ステップ 2　非対称ルーティングのサポートに参加するインターフェイスそれぞれに、次のコマンドを入力します。コマンドがスタンバイ フェールオーバー グループに複製されるように、コンテキストがアクティブ状態の装置でコマンドを入力する必要があります。コマンドの複製については、「コマンドの複製」（P.10-4）を参照してください。

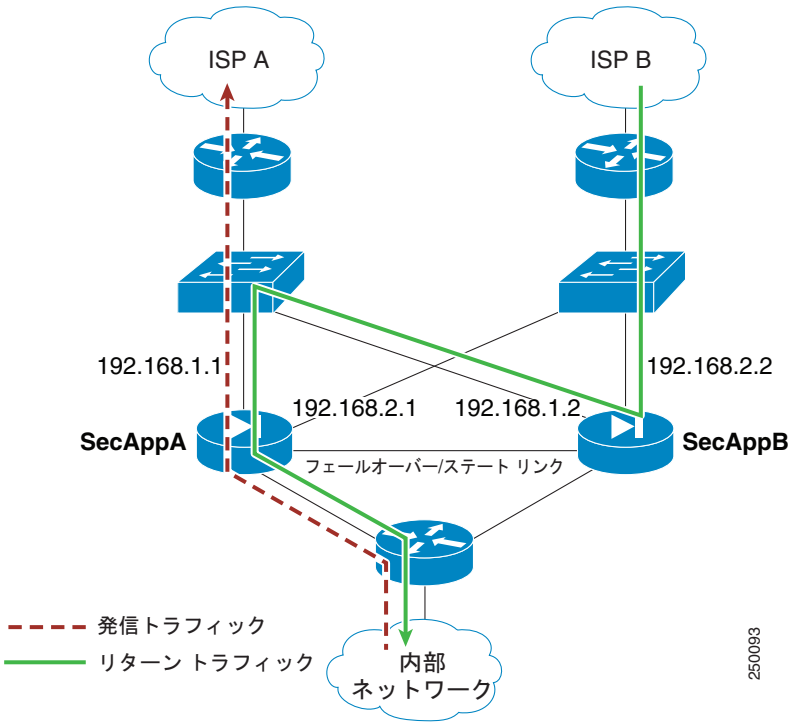
```
hostname/ctx(config)# interface phy_if
hostname/ctx(config-if)# asr-group num
```

num 範囲に有効な値は、1 ～ 32 です。非対称ルーティング グループに参加するインターフェイスそれぞれにコマンドを入力する必要があります。インターフェイスによって転送、受信、またはドロップされた ASR パケットの数を表示するには、**show interface detail** コマンドを使用します。ASA に複数の ASR グループを設定できますが、インターフェイスごとに 1 つだけです。同じ ASR グループのメンバーだけにセッション情報のチェックが行われます。

例

図 10-1 に、非対称ルーティングのサポートに対する **asr-group** コマンドの使用例を示します。

図 10-1　　ASR の例



2 つの装置に次のコンフィギュレーションがあります（コンフィギュレーションは関連するコマンドだけを示します）。図の「SecAppA」というラベルの付いたデバイスは、フェールオーバー ペアのプライマリ装置です。

例 10-1　　プライマリ装置のシステム コンフィギュレーション

```
hostname primary
interface GigabitEthernet0/1
description LAN/STATE Failover Interface
interface GigabitEthernet0/2
no shutdown
interface GigabitEthernet0/3
no shutdown
interface GigabitEthernet0/4
no shutdown
interface GigabitEthernet0/5
no shutdown
failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/1
failover link folink
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
primary
failover group 2
secondary
admin-context admin
```

```
context admin
description admin
allocate-interface GigabitEthernet0/2
allocate-interface GigabitEthernet0/3
config-url flash:/admin.cfg
join-failover-group 1
context ctx1
description context 1
allocate-interface GigabitEthernet0/4
allocate-interface GigabitEthernet0/5
config-url flash:/ctx1.cfg
join-failover-group 2
```

例 10-2　　管理コンテキストのコンフィギュレーション

```
hostname SecAppA
interface GigabitEthernet0/2
nameif outsideISP-A
security-level 0
ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
asr-group 1
interface GigabitEthernet0/3
nameif inside
security-level 100
ip address 10.1.0.1 255.255.255.0 standby 10.1.0.11
monitor-interface outside
```

例 10-3　　ctx1 コンテキストのコンフィギュレーション

```
hostname SecAppB
interface GigabitEthernet0/4
nameif outsideISP-B
security-level 0
ip address 192.168.2.2 255.255.255.0 standby 192.168.2.1
asr-group 1
interface GigabitEthernet0/5
nameif inside
security-level 100
ip address 10.2.20.1 255.255.255.0 standby 10.2.20.11
```

図 10-1 に、次のように動作する ASR のサポートを示します。

1. 発信セッションはASA SecAppA を通過します。このセッションによってインターフェイス outsideISP-A（192.168.1.1）を終了します。
2. 非対称ルーティングがある程度アップストリームに設定されているため、リターン トラフィックは、ASA SecAppB のインターフェイス outsideISP-B（192.168.2.2）を経由して戻ります。
3. 通常、リターン トラフィックは、そのインターフェイス 192.168.2.2 上にリターン トラフィックに関するセッション情報がないので、ドロップされます。ただし、インターフェイスは、コマンド **asr-group 1** で設定されます。装置は、同じ ASR グループ ID で設定された他のインターフェイス上のセッションを探します。
4. セッション情報は、装置 SecAppB 上でスタンバイ状態のインターフェイス outsideISP-A（192.168.1.2）にあります。ステートフル フェールオーバーは、SecAppA から SecAppB にセッション情報を複製します。

5. ドロップされる代わりに、レイヤ 2 ヘッダーはインターフェイス 192.168.1.1 の情報で書き直され、トラフィックはインターフェイス 192.168.1.2 からリダイレクトされます。そこから、発信元の装置のインターフェイスを経由して戻ります（SecAppA の 192.168.1.1）。この転送は、必要に応じて、セッションが終了するまで続行されます。

リモート コマンドの実行

リモート コマンドを実行すると、コマンド ラインに入力されたコマンドを特定のフェールオーバー ピアに送信できます。

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。

コマンドをフェールオーバー ピアに送信するには、次の手順を実行します。

ステップ 1　マルチ コンテキスト モードの場合は、**changeto** コマンドを使用して、設定したい内容にコンテキストを変更します。**failover exec** コマンドを使用して、フェールオーバー ピアでコンテキストを変更することはできません。

シングル コンテキスト モードの場合は、次の手順にスキップします。

ステップ 2　次のコマンドを使用して、所定のフェールオーバー装置にコマンドを送信します。

```
hostname(config)# failover exec {active | mate | standby}
```

active または **standby** キーワードを使用すると、その装置が現在の装置であっても、コマンドは指定された装置で実行されます。**mate** キーワードを使用すると、コマンドはフェールオーバー ピアで実行されます。

コマンド モードを変更するコマンドによって、現在のセッションのプロンプトが変更されることはありません。コマンドが実行されるコマンド モードを表示するには、**show failover exec** コマンドを使用する必要があります。詳細については、「コマンド モードの変更」（P.10-25）を参照してください。

コマンド モードの変更

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。デフォルトでは、**failover exec** コマンド モードは、指定されたデバイスのグローバル コンフィギュレーション モードで開始されます。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。**failover exec** を使用してモードを変更しても、セッション プロンプトは変更されません。

たとえば、フェールオーバー ピアのアクティブ装置のグローバル コンフィギュレーション モードにログインし、**failover exec active** コマンドを使用してインターフェイス コンフィギュレーション モードを変更した場合、ターミナル プロンプトはグローバル コンフィギュレーション モードのままですが、**failover exec** を使用して入力されるコマンドは、インターフェイス コンフィギュレーション モードで入力されます。

次の例は、ターミナル セッション モードと **failover exec** コマンド モードの違いを示しています。この例で、管理者はアクティブ装置の **failover exec** モードを、インターフェイス GigabitEthernet0/1 用のインターフェイス コンフィギュレーション モードに変更します。その後、**failover exec active** を使用して入力されたすべてのコマンドは、インターフェイス GigabitEthernet0/1 のインターフェイス コンフィギュレーション モードに送信されます。次に、管理者は failover exec active を使用して、そのインターフェイスに IP アドレスを割り当てます。プロンプトはグローバル コンフィギュレーション モードを示していますが、**failover exec active** モードはインターフェイス コンフィギュレーション モードです。

```
hostname(config)# failover exec active interface GigabitEthernet0/1
hostname(config)# failover exec active ip address 192.168.1.1 255.255.255.0 standby
192.168.1.2
hostname(config)# router rip
hostname(config-router)#
```

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、アクティブ装置のインターフェイス コンフィギュレーション モードで、**failover exec** 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。その結果、デバイスとのセッションはインターフェイス コンフィギュレーション モードのままで、**failover exec active** を使用して入力されたコマンドは、指定されたルーティング プロセスを実行するためルータ コンフィギュレーション モードに送信されます。

```
hostname(config-if)# failover exec active router ospf 100
hostname(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。**show failover exec** コマンドでは、**failover exec** コマンドと同じキーワード、つまり **active**、**mate**、または **standby** が使用されます。各デバイスの **failover exec** モードは個別に追跡されます。

次に、スタンバイ装置に入力された **show failover exec** コマンドの出力例を示します。

```
hostname(config)# failover exec active interface GigabitEthernet0/1
hostname(config)# sh failover exec active
Active unit Failover EXEC is at interface sub-command mode

hostname(config)# sh failover exec standby
Standby unit Failover EXEC is at config mode

hostname(config)# sh failover exec mate
Active unit Failover EXEC is at interface sub-command mode
```

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。

リモート コマンドの実行に関する制限事項

リモート コマンドの使用には、次の制限事項があります。

- 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装置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、現在の装置が特権 EXEC モードのときに **failover exec mate configure terminal** を入力すると、**show failover exec mate** 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、ピア装置で **failover exec** 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、現在の装置でグローバル 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。

フェールオーバーの制御

ここでは、フェールオーバーの制御およびモニタ方法について説明します。この項は、次の内容で構成されています。

フェールオーバーの強制実行

フェールオーバー グループがスタンバイ状態である装置のシステム実行スペースで、次のコマンドを入力します。

```
hostname# failover active group group_id
```

または、フェールオーバー グループがアクティブ状態である装置のシステム実行スペースで、次のコマンドを入力します。

```
hostname# no failover active group group_id
```

システム実行スペースに次のコマンドを入力すると、すべてのフェールオーバー グループがアクティブになります。

```
hostname# failover active
```

フェールオーバーのディセーブル化

アクティブ/アクティブ フェールオーバー ペアでフェールオーバーをディセーブル化すると、どの装置を優先するように設定されていようと、フェールオーバー グループはアクティブであるすべての装置でアクティブ状態のまま維持されます。システム実行スペースで **no failover** コマンドを実行します。

フェールオーバーをディセーブル化するには、次のコマンドを入力します。

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

障害が発生した装置またはフェールオーバー グループの復元

障害が発生した装置またはフェールオーバー グループを復元すると、その装置またはフェールオーバー グループは故障状態からスタンバイ状態になります。フェールオーバー グループまたは装置は、自動的にはアクティブ状態になりません。復元された装置またはグループは、フェールオーバー（強制または性質）によってアクティブになるまではスタンバイ状態のままです。ただし、フェールオーバー プリエンプションが設定されているフェールオーバー グループは例外です。以前アクティブであったフェールオーバー グループにプリエンプションが設定されており、障害が発生した装置が優先装置の場合、そのフェールオーバー グループはアクティブになります。

障害が発生した装置を障害のない状態に復元するには、次のコマンドを入力します。

```
hostname(config)# failover reset
```

障害が発生したアクティブ/アクティブ フェールオーバー グループを障害のない状態に復元するには、次のコマンドを入力します。

```
hostname(config)# failover reset group group_id
```

フェールオーバー機能のテスト

フェールオーバー機能をテストするには、次の手順を実行します。

ステップ 1　FTP などを使用して、異なるインターフェイス上のホスト間でファイルを送信し、アクティブ装置またはフェールオーバー グループが予期したとおりにトラフィックを渡しているかどうかをテストします。

ステップ 2　お使いのホストに接続しているインターフェイスが含まれたフェールオーバー グループがアクティブ状態の装置で、次のコマンドを入力し、スタンバイ装置にフェールオーバーを強制実行します。

```
hostname(config)# no failover active group group_id
```

ステップ 3　FTP を使用して、2 つの同じホスト間で別のファイルを送信します。

ステップ 4　テストが成功しなかった場合は、**show failover** コマンドを入力してフェールオーバー ステータスを確認します。

ステップ 5　テストが終了したら、ホストに接続しているインターフェイスが含まれたフェールオーバー グループがアクティブな装置で次のコマンドを入力すると、装置またはフェールオーバー グループをアクティブ ステータスに復元できます。

```
hostname(config)# failover active group group_id
```

アクティブ/アクティブ フェールオーバーのモニタリング

アクティブ/アクティブ フェールオーバーをモニタするには、次のいずれかのタスクを実行します。特に指定がない限り、コマンドはシステム実行スペースで入力します。

コマンド	目的
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。
show failover group	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。表示される情報は、**show failover** コマンドの場合と似ていますが、指定されたグループに対象が限定されます。
show monitor-interface	モニタ対象インターフェイスの情報を表示します。このコマンドは、セキュリティ コンテキスト内で入力します。
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。

モニタリング コマンドの出力の詳細については、『*Cisco ASA 5500 Series Command Reference*』を参照してください。

アクティブ/アクティブ フェールオーバーの機能履歴

表 10-3 に、この機能のリリース履歴を示します。

表 10-3　アクティブ/アクティブ フェールオーバーの機能履歴

機能名	リリース	機能情報
アクティブ/アクティブ フェールオーバー	7.0	アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、両方の ASA がネットワーク トラフィックを渡すことができます。 この機能および関連するコマンドが導入されました。
フェールオーバーでの IPv6 サポート	8.2(2)	**failover interface ip**、**show failover**、**ipv6 address**、**show monitor-interface** の各コマンドが変更されました。