

ハイ アベイラビリティのためのフェールオーバー

この章では、Cisco ASA のハイ アベイラビリティを達成するために、アクティブ/スタンドバイまたはアクティブ/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。

- フェールオーバーについて （1 ページ）
- フェールオーバーのライセンス （31 ページ）
- フェールオーバーのガイドライン （33 ページ）
- フェールオーバーのデフォルト （35 ページ）
- アクティブ/スタンバイ フェールオーバーの設定 （35 ページ）
- アクティブ/アクティブ フェールオーバーの設定 （41 ページ）
- オプションのフェールオーバー パラメータの設定 （47 ページ）
- フェールオーバー の管理 （57 ページ）
- モニタリング フェールオーバー （64 ページ）
- フェールオーバーの履歴 （66 ページ）

フェールオーバーについて

フェールオーバーの設定では、専用フェールオーバー リンク（および任意でステート リンク）を介して相互に接続された 2 つの同じ ASA が必要です。アクティブ装置およびインターフェイスのヘルスがモニタされて、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断されます。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 モード

ASA は、アクティブ/アクティブ フェールオーバーとアクティブ/スタンバイ フェールオーバーの 2 つのフェールオーバー モードをサポートします。各フェールオーバー モードには、フェールオーバーを判定および実行する独自の方式があります。

- アクティブ/スタンバイ フェールオーバーでは、1 台の装置がアクティブ装置です。この装置がトラフィックを渡します。スタンバイ装置は、アクティブにトラフィックを渡しま

せん。フェールオーバーが発生すると、アクティブ装置がスタンバイ装置にフェールオーバーし、そのスタンバイ装置がアクティブになります。シングルまたはマルチ コンテキスト モードでは、ASA のアクティブ/スタンバイ フェールオーバーを使用できます。

- 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 フェールオーバーでは、ASA のセキュリティ コンテキストを 2 つのフェイルオーバー グループ に分割します。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。一方のグループは、プライマリ ASA でアクティブになるよう割り当てられます。他方のグループは、セカンダリ ASA でアクティブになるよう割り当てられます。フェールオーバーが行われる場合は、フェールオーバー グループ レベルで行われます。

両方のフェールオーバー モードとも、ステートフルまたはステートレス フェールオーバーをサポートします。

フェールオーバー のシステム要件

この項では、 フェールオーバー コンフィギュレーションにあるASAのハードウェア要件、ソフトウェア要件、およびライセンス要件について説明します。

ハードウェア要件

フェールオーバー コンフィギュレーションの 2 台の装置は、次の条件を満たしている必要があります。

- 同じモデルであること。
- インターフェイスの数とタイプが同じであること。

  Firepower 2100 および Firepower 4100/9300 シャーシ の場合は、 フェールオーバー を有効にする前に、すべてのインターフェイスをFXOSで同じように事前設定する必要があります。フェールオーバーを有効にした後でインターフェイスを変更する場合は、スタンバイ ユニットの FXOS でインターフェイスを変更し、アクティブ ユニットで同じ変更を行います。FXOSでインターフェイスを削除した場合（たとえば、ネットワーク モジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。
- 同じモジュール（存在する場合）がインストールされていること。
- 同じ RAM がインストールされていること。

フェールオーバー コンフィギュレーションで装置に異なるサイズのフラッシュ メモリを使用している場合、小さい方のフラッシュ メモリを取り付けた装置に、ソフトウェア イメージ ファイルおよびコンフィギュレーション ファイルを格納できる十分な容量があることを確認してく

ださい。十分な容量がない場合、フラッシュ メモリの大きい装置からフラッシュ メモリの小さい装置にコンフィギュレーションの同期が行われると、失敗します。

ソフトウェア要件

フェールオーバー コンフィギュレーションの2台の装置は、次の条件を満たしている必要があります。

- ファイアウォール モードが同じであること（ルーテッドまたは透過）。
- コンテキスト モードが同じであること（シングルまたはマルチ）。
- ソフトウェア バージョンが、メジャー（最初の番号）およびマイナー（2番目の番号）ともに同じであること。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一時的に使用できます。たとえば、ある装置をバージョン 8.3(1) からバージョン 8.3(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 AnyConnect イメージを持っていること。中断のないアップグレードを実行するときにフェールオーバー ペアのイメージが一致しないと、アップグレード プロセスの最後のリブート手順でクライアントレス SSL VPN 接続が切断され、データベースには孤立したセッションが残り、IP プールではクライアントに割り当てられた IP アドレスが「使用中」として示されます。
- 同じ FIPS モードであること。

ライセンス要件

フェールオーバー コンフィギュレーションの2台の装置は、ライセンスが同じである必要はありません。これらのライセンスは結合され、1つのフェールオーバー クラスタ ライセンスが構成されます。

フェールオーバー リンクとステートフル フェールオーバー リンク

フェールオーバー リンクとオプションのステートフル フェールオーバー リンクは、2 つの装置間の専用接続です。

注意 フェールオーバー リンクおよびステート リンク経由で送信される情報は、IPsec トンネルまたはフェールオーバー キーを使用して通信を保護しない限り、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 IPsec トンネルまたはフェールオーバー キーによってセキュリティ保護することをお勧めします。

フェールオーバー リンク

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。ほとんどのモデルでは、以下で明示的に説明されていない限り、フェールオーバー用の管理インターフェイスを使用できません。

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 および Firepower 4100 上の ASA：統合されたフェールオーバー リンクとステート リンクには、10 GB のデータ インターフェイスを使用することを推奨します。フェールオーバー リンクに管理タイプのインターフェイスを使用することはできません。

- 他のすべてのモデル：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。

ステートフル フェールオーバー リンク

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。

（注） ステートフル フェールオーバー リンクの帯域幅は、少なくともデータ インターフェイスの帯域幅と同等にすることを推奨します。

フェールオーバー リンクと共有

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。ただし、設定が大規模でトラフィックが膨大なネットワークを使用している場合は、ステート リンクとフェールオーバー リンク専用のインターフェイスを検討する必要があります。

専用のインターフェイス

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 デバイス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ミリ秒を上回る場合、フェールオーバー メッセージの再送信によって、パフォーマンスが低下する可能性があります。

フェールオーバーの中断の回避とデータ リンク

すべてのインターフェイスで同時に障害が発生する可能性を減らすために、フェールオーバー リンクとデータ インターフェイスは異なるパスを通すことを推奨します。フェールオーバー リンクがダウンした場合、フェールオーバーが必要かどうかの決定に、ASAはデータ インターフェイスを使用できます。その後、フェールオーバー動作は、フェールオーバー リンクのヘルスが復元されるまで停止されます。

耐障害性のあるフェールオーバー ネットワークの設計については、次の接続シナリオを参照してください。

シナリオ 1：非推奨

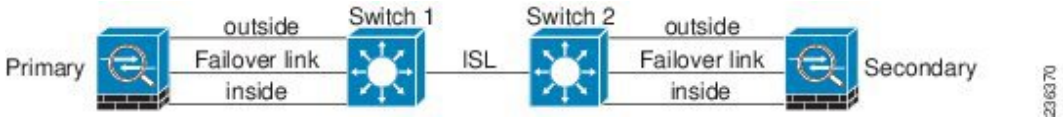
単一のスイッチまたはスイッチ セットが 2 つの ASA 間のフェールオーバー インターフェイスとデータ インターフェイスの両方の接続に使用される場合、スイッチまたはスイッチ間リンク

がダウンすると、両方の ASA がアクティブになります。したがって、次の図で示されている次の 2 つの接続方式は推奨しません。

図 *1:* 単一のスイッチを使用した接続：非推奨



図 *2:* 2 つのスイッチを使用した接続：非推奨



シナリオ 2：推奨

フェールオーバー リンクには、データ インターフェイスと同じスイッチを使用しないことを推奨します。代わりに、次の図に示すように、別のスイッチを使用するか直接ケーブルを使用して、フェールオーバー リンクを接続します。

図 *3:* 異なるスイッチを使用した接続

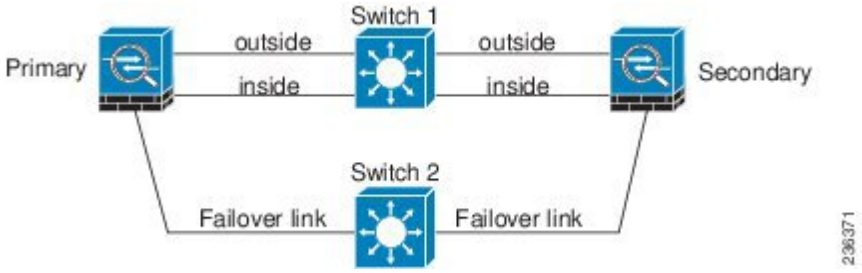
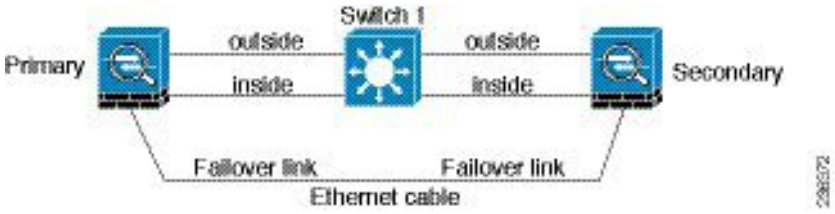


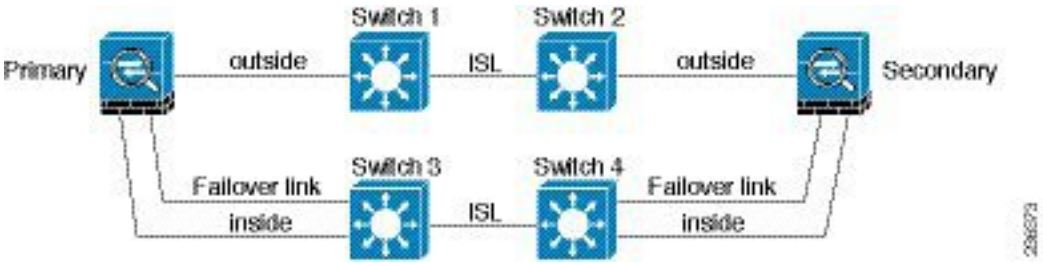
図 *4:* ケーブルを使用した接続



シナリオ 3：推奨

ASA データ インターフェイスが複数セットのスイッチに接続されている場合、フェールオーバー リンクはいずれかのスイッチに接続できます。できれば、次の図に示すように、ネットワークのセキュアな側（内側）のスイッチに接続します。

図 *5:* セキュアなスイッチを使用した接続



シナリオ 4：推奨

最も信頼性の高いフェールオーバー構成では、次の図に示すように、フェールオーバー リンクに冗長インターフェイスを使用します。

図 *6:* 冗長インターフェイスを使用した接続

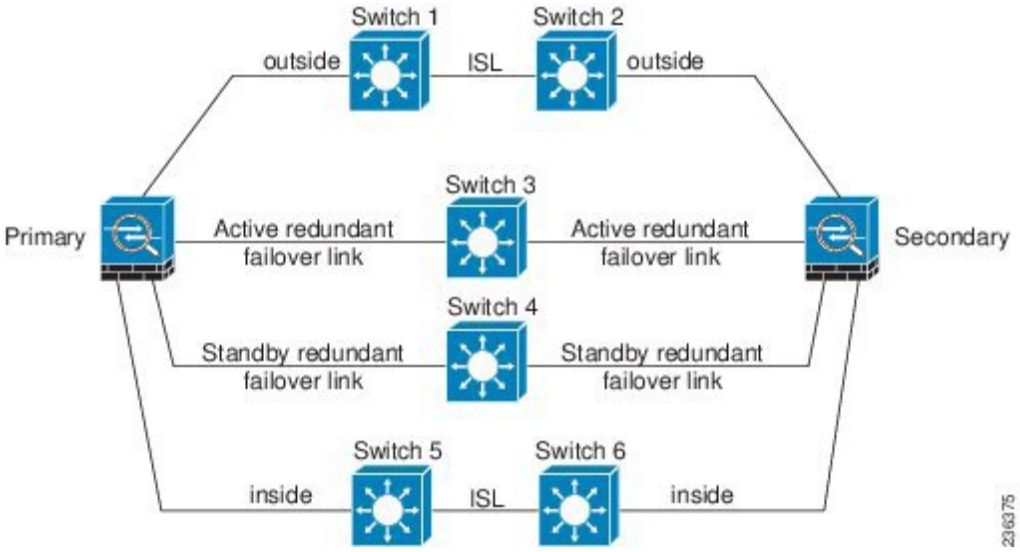
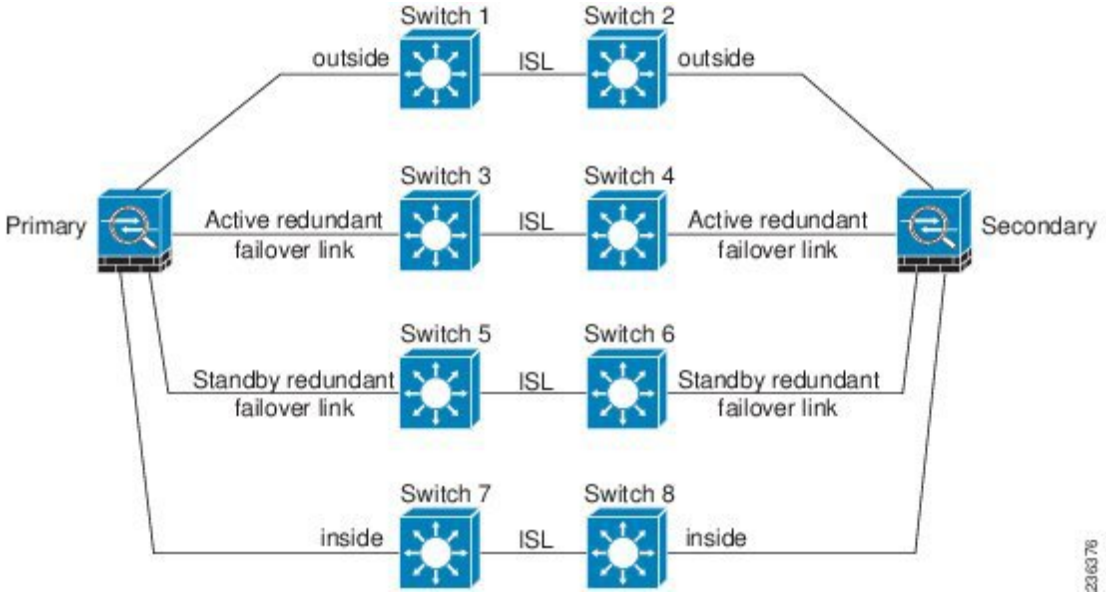


図 *7 : Inter-Switch Link*（*ISL*）を使用した接続



フェールオーバー の MAC アドレスと IP アドレス

インターフェイスを設定する場合、同じネットワーク上のアクティブ IP アドレスとスタンバイ IP アドレスを指定できます。一般的に、フェールオーバーが発生した場合、新しいアクティブ装置がアクティブな IP アドレスと MAC アドレスを引き継ぎます。ネットワーク デバイスは、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

（注） 推奨されていますが、スタンバイ アドレスは必須ではありません。スタンバイ IP アドレスがないと、アクティブ装置はスタンバイ インターフェイスの状態を確認するためのネットワーク テストを実行できません。リンク ステートのみ追跡できます。また、管理目的でそのインターフェイスのスタンバイ装置に接続することもできません。

ステート リンク用の IP アドレスおよび MAC アドレスは、フェールオーバー実行後も変更されません。

アクティブ/スタンバイ IP アドレスと MAC アドレス

アクティブ/スタンバイ フェールオーバー の場合、フェールオーバー イベント中の IP アドレスと MAC アドレスの使用については、次を参照してください。

1. アクティブな装置は常にプライマリ装置の IP アドレスと MAC アドレスを使用します。
2. アクティブ装置が故障すると、スタンバイ装置は故障した装置の IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。

3. 故障した装置がオンラインに復帰すると、スタンバイ状態となり、スタンバイ IP アドレスと MAC アドレスを引き継ぎます。

ただし、セカンダリ装置がプライマリ装置を検出せずにブートした場合、セカンダリ装置がアクティブ装置になります。プライマリ装置の MAC アドレスを認識していないため、自分の MAC アドレスを使用します。プライマリ装置が使用可能になると、セカンダリ（アクティブ）装置は MAC アドレスをプライマリ装置の MAC アドレスに変更します。これによって、ネットワーク トラフィックが中断されることがあります。同様に、プライマリ装置を新しいハードウェアと交換すると、新しい MAC アドレスが使用されます。

仮想 MAC アドレスがこの中断を防ぎます。なぜなら、アクティブ MAC アドレスは起動時にセカンダリ装置によって認識され、プライマリ装置のハードウェアが新しくなっても変わらないからです。仮想 MAC アドレスを設定しなかった場合、トラフィック フローを復元するために、接続されたルータの ARP テーブルをクリアする必要がある場合があります。ASA は MAC アドレスを変更するときに、スタティック NAT アドレスに対して Gratuitous ARP を送信しません。そのため、接続されたルータはこれらのアドレスの MAC アドレスの変更を認識できません。

アクティブ/アクティブ IP アドレスと MAC アドレス

アクティブ/アクティブ フェールオーバーの場合、フェールオーバー イベント中の IP アドレスと MAC アドレスの使用については、次を参照してください。

1. プライマリ装置は、フェールオーバー グループ 1 および 2 のコンテキストのすべてのインターフェイスに対して、アクティブおよびスタンバイ MAC アドレスを自動生成します。必要に応じて、たとえば、MAC アドレスの競合がある場合は、MAC アドレスを手動で設定できます。
2. 各装置は、そのアクティブ フェールオーバー グループにアクティブな IP アドレスと MAC アドレスを使用し、そのスタンバイ フェールオーバー グループにスタンバイ アドレスを使用します。たとえば、フェールオーバー グループ 1 でプライマリ装置がアクティブである場合、フェールオーバー グループ 1 のコンテキストでアクティブなアドレスを使用します。フェールオーバー グループ 2 のコンテキストではスタンバイであるため、スタンバイ アドレスを使用します。
3. 装置が故障すると、他の装置は故障したフェールオーバー グループの アクティブな IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。
4. 故障した装置がオンラインに戻り、preempt オプションが有効になっている場合、フェールオーバー グループを再開します。

仮想 MAC アドレス

ASA には、仮想 MAC アドレスを設定する複数の方法があります。1 つの方法のみ使用することをお勧めします。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。手動方法にはインターフェイス モード **mac-address** コマンド、**failover mac address** コマンドが含

まれ、アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ モード **mac address** コマンドが、以下で説明する自動生成方法に加えて含まれます。

マルチ コンテキスト モードでは、共有インターフェイスに仮想アクティブおよびスタンバイ MAC アドレスを自動的に生成するように ASA を設定することができ、これらの割り当てはセカンダリ装置に同期されます（**mac-address auto** コマンドを参照してください）。共有以外のインターフェイスでは、アクティブ/スタンバイ モードの MAC アドレスを手動で設定することができます（アクティブ/アクティブ モードはすべてのインターフェイスに MAC アドレスを自動生成します）。

アクティブ/アクティブ フェールオーバーでは、仮想 MAC アドレスはデフォルト値またはインターフェイスごとに設定できる値のいずれかとともに常に使用されます。

ASAサービスモジュールのシャーシ内およびシャーシ間モジュール配置

プライマリとセカンダリの ASASM は、同じスイッチ内または 2 台の異なるスイッチに搭載できます。

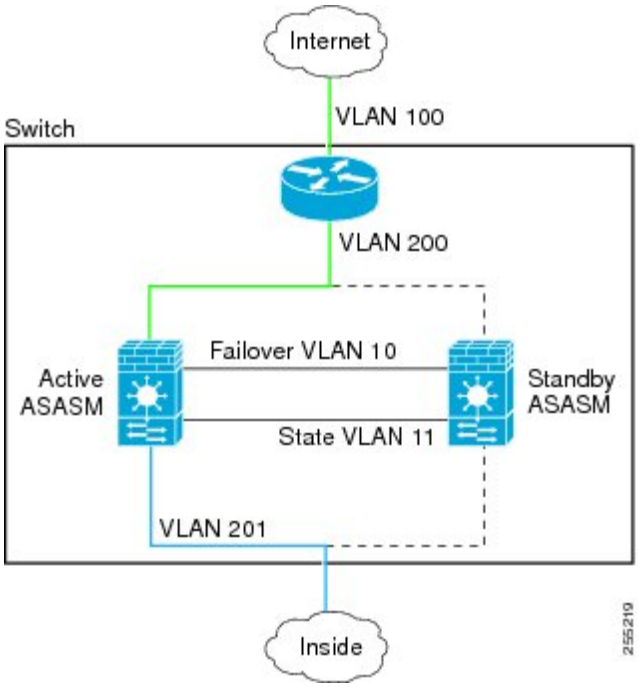
シャーシ内フェールオーバー

セカンダリ ASASM をプライマリ ASASM と同じスイッチに搭載した場合は、モジュール レベルの障害から保護する必要があります。

両方の ASASM に同じ VLAN が割り当てられますが、ネットワーキングに参加するのはアクティブ モジュールだけです。スタンバイ モジュールは、トラフィックを転送しません。

次の図は、一般的なスイッチ内の構成を示します。

図 *8:* スイッチ内フェールオーバー



シャーシ間フェールオーバー

スイッチレベルの障害から保護するため、セカンダリ ASASM を別のスイッチに搭載できます。ASASM は直接スイッチとフェールオーバーを調整するのではなく、スイッチと協調してフェールオーバー操作を行います。スイッチのフェールオーバー設定については、スイッチのマニュアルを参照してください。

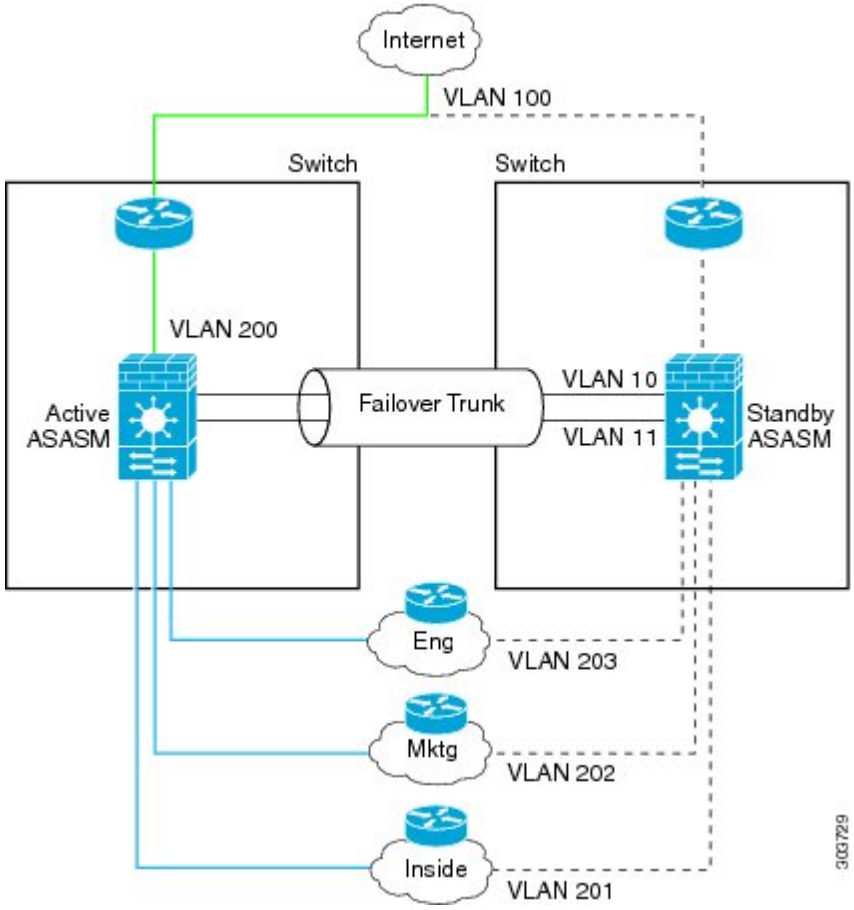
ASASM 間のフェールオーバー通信の信頼性を高めるために、2 台のスイッチ間に EtherChannel トランク ポートを設定して、フェールオーバーおよびステート VLAN を伝送することをお勧めします。

他の VLAN については、両方のスイッチがすべてのファイアウォール VLAN にアクセスでき、モニタ対象 VLAN が両方のスイッチ間で正常に hello パケットを渡すことができるようにします。

次の図は、スイッチと ASASM の一般的な冗長構成を示します。2 台のスイッチ間のトランクは、フェールオーバー ASASM VLAN（VLAN 10 と 11）を転送します。

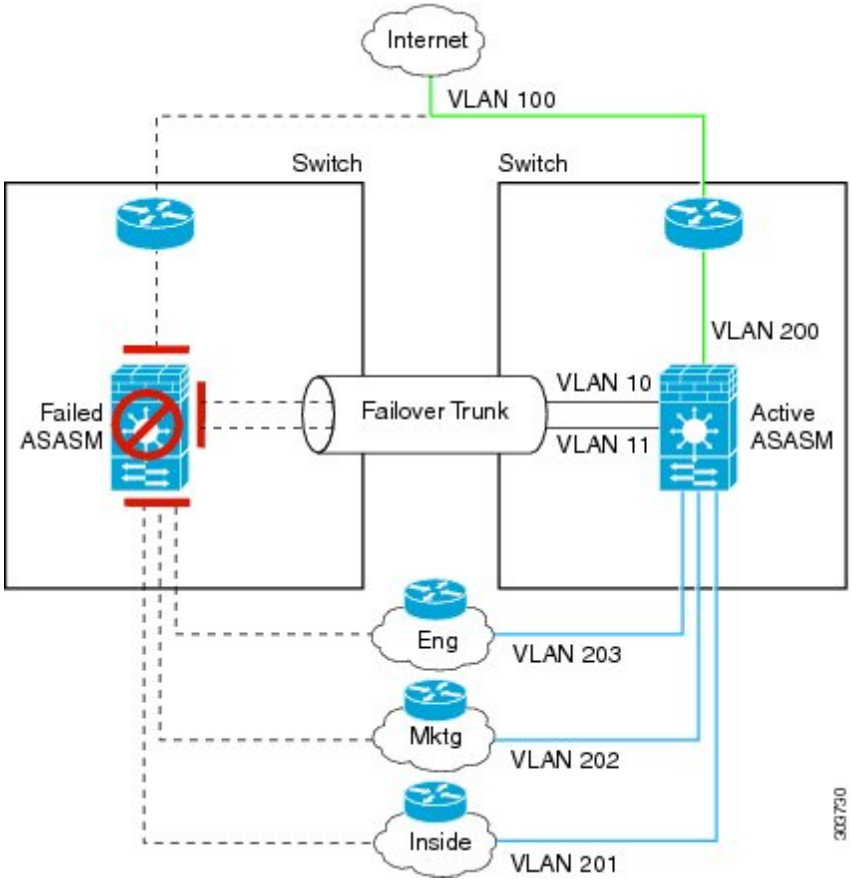
（注） ASASM のフェールオーバーはスイッチのフェールオーバーに依存しない独立した機能ですが、スイッチのフェールオーバーが発生した場合には、ASASM もそれに対応します。

図 *9* : 通常の動作



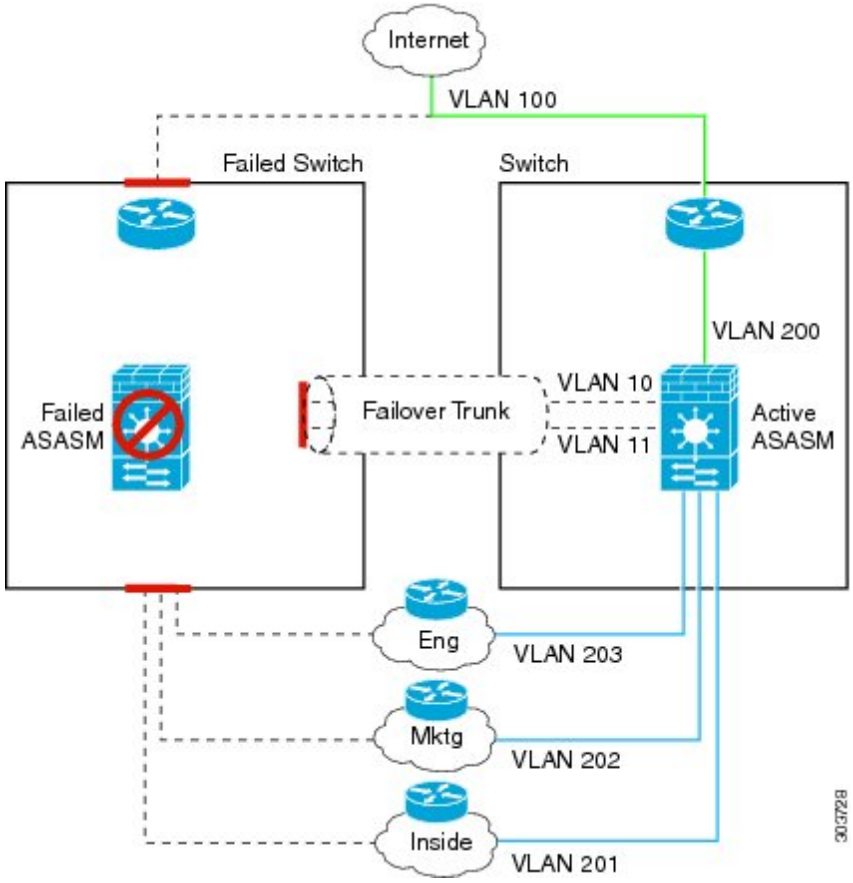
プライマリ ASASM に障害が発生すると、セカンダリ ASASM がアクティブになってファイアウォール VLAN を通過します。

図 *10 : ASASM* の障害



スイッチ全体に障害が発生し、ASASMにも障害が発生した場合（電源切断など）には、スイッチと ASASM の両方でセカンダリ ユニットへのフェールオーバーが実行されます。

図 *11* : スイッチの障害



ステートレス フェールオーバーとステートフル フェールオーバー

ASA は、アクティブ/スタンバイ モードとアクティブ/アクティブ モードの両方に対して、ステートレスとステートフルの 2 種類のフェールオーバーをサポートします。

（注） クライアントレス SSL VPN の一部のコンフィギュレーション要素（ブックマークやカスタマイゼーションなど）はVPNフェールオーバーサブシステムを使用していますが、これはステートフル フェールオーバーの一部です。フェールオーバー ペアのメンバ間でこれらの要素を同期するには、ステートフルフェールオーバーを使用する必要があります。ステートレスフェールオーバーは、クライアントレス SSL VPN には推奨されません。

ステートレス フェールオーバー

フェールオーバーが行われると、アクティブ接続はすべてドロップされます。新しいアクティブ装置が引き継ぐ場合、クライアントは接続を再確立する必要があります。

（注） クライアントレス SSL VPN の一部のコンフィギュレーション要素（ブックマークやカスタマイゼーションなど）はVPNフェールオーバーサブシステムを使用していますが、これはステートフル フェールオーバーの一部です。フェールオーバー ペアのメンバ間でこれらの要素を同期するには、ステートフル フェールオーバーを使用する必要があります。ステートレス（標準）フェールオーバーは、クライアントレス SSL VPN には推奨できません。

Stateful Failover

ステートフル フェールオーバーが有効の場合、アクティブ装置は接続ごとのステート情報をスタンバイ装置に継続的に渡します。アクティブ/アクティブ フェールオーバーの場合は、アクティブとスタンバイのフェールオーバー グループ間でこれが行われます。フェールオーバーの発生後も、新しいアクティブ装置で同じ接続情報が利用できます。サポートされているエンドユーザのアプリケーションでは、同じ通信セッションを保持するために再接続する必要はありません。

Supported Features

ステートフル フェールオーバーでは、次のステート情報がスタンバイ ASAに渡されます。

- NAT 変換テーブル
- TCP 接続と UDP 接続、および状態。他のタイプの IP プロトコルおよび ICMP は、新しいパケットが到着したときに新しいアクティブ ユニットで確立されるため、アクティブ装置によって解析されません。
- HTTP 接続テーブル（HTTP 複製を有効にしない場合）。
- HTTP 接続状態（HTTP 複製が有効化されている場合）：デフォルトでは、ステートフル フェールオーバーが有効化されているときには、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。
- SCTP 接続状態。ただし、SCTP インスペクションのステートフル フェールオーバーはベスト エフォートです。フェールオーバー中、SACK パケットが失われると、失われたパケットが受信されるまで、新しいアクティブ ユニットはキューにある他のすべての out of order パケットを破棄します。
- ARP テーブル
- レイヤ 2 ブリッジ表（ブリッジ グループ用）
- ISAKMP および IPSec SA テーブル
- GTP PDP 接続データベース
- SIP シグナリング セッションとピンホール。

- ICMP 接続状態：ICMP 接続の複製は、個々のインターフェイスが非対称ルーティング グループに割り当てられている場合にだけイネーブルになります。
- スタティックおよびダイナミック ルーティング テーブル：ステートフル フェールオーバーはダイナミック ルーティング プロトコル（OSPF や EIGRP など）に参加するため、アクティブ装置上のダイナミック ルーティング プロトコルによる学習ルートが、スタンバイ装置のルーティング情報ベース（RIB）テーブルに維持されます。フェールオーバー イベントで、アクティブなセカンダリ ユニットには最初にプライマリ ユニットをミラーリングするルールがあるため、パケットは通常は最小限の中断でトラフィックに移動します。フェールオーバーの直後に、新しくアクティブになった装置で再コンバージェンス タイマーが開始されます。次に、RIB テーブルのエポック番号が増加します。再コンバージェンス中に、OSPF および EIGRP ルートは新しいエポック番号で更新されます。タイマーが期限切れになると、失効したルート エントリ（エポック番号によって決定される）はテーブルから削除されます。これで、RIB には新しくアクティブになった装置での最新のルーティング プロトコル転送情報が含まれています。

  （注） ルートは、アクティブ装置上のリンクアップまたはリンクダウン イベントの場合のみ同期されます。スタンバイ装置上でリンクがアップまたはダウンすると、アクティブ装置から送信されたダイナミック ルートが失われることがあります。これは正常な予期された動作です。

- DHCP サーバ：DHCP アドレス リースは複製されません。ただし、インターフェイスで設定された DHCP サーバは、DHCP クライアントにアドレスを付与する前にアドレスが使用されていないことを確認するために ping を送信するため、サービスに影響はありません。ステート情報は、DHCP リレーまたは DDNS とは関連性がありません。
- Cisco IP SoftPhone セッション：コール セッション ステート情報がスタンバイ装置に複製されるため、Cisco IP SoftPhone セッションの実行中にフェールオーバーが起こっても、コールは実行されたままです。コールが終了すると、IP SoftPhone クライアントは Cisco Call Manager との接続を失います。これは、CTIQBE ハングアップ メッセージのセッション情報がスタンバイ装置に存在しないために発生します。IP SoftPhone クライアントでは、一定の時間内に CallManager からの応答が受信されない場合、CallManager に到達できないものと判断されて登録が解除されます。
- RA VPN：リモート アクセス VPN エンド ユーザは、フェールオーバー後に VPN セッションを再認証または再接続する必要はありません。ただし、VPN 接続上で動作するアプリケーションは、フェールオーバー プロセス中にパケットを失って、パケット損失から回復できない可能性があります。

サポートされない機能

ステートフル フェールオーバーでは、次のステート情報はスタンバイ ASAに渡されません。

- ユーザ認証（uauth）テーブル

- TCP ステート バイパス接続
- マルチキャスト ルーティング。
- ASA FirePOWER モジュールなどのモジュールのステート情報。
- 一部のクライアントレス SSL VPN 機能
  - スマート トンネル
  - ポート転送
  - プラグイン
  - Java アプレット
  - IPv6 クライアントレスまたは Anyconnect セッション
  - Citrix 認証（Citrix ユーザはフェールオーバー後に再認証が必要です）

フェールオーバーのブリッジ グループ要件

ブリッジグループを使用する際に、フェールオーバーの特殊な考慮事項があります。

アプライアンス、ASAv のブリッジグループ必須要件

アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニングツリープロトコル（STP）を実行している接続済みスイッチ ポートは、トポロジ変更を検出すると 30 ～ 50 秒間ブロッキング ステートに移行できます。ポートがブロッキング ステートである間のトラフィックの損失を回避するために、スイッチ ポート モードに応じて次の回避策のいずれかを設定できます。

- アクセス モード：スイッチで STP PortFast 機能をイネーブルにします。

```
interface interface_id
  spanning-tree portfast
```

PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは引き続き STP に参加しています。したがって、ポートがループの一部になる場合、最終的には STP ブロッキング モードに遷移します。

- トランク モード：EtherType アクセス ルールを使用して、ブリッジグループのメンバー インターフェイス上の ASA の BPDU をブロックします。

```
access-list id ethertype deny bpdu
access-group id in interface name1
access-group id in interface name2
```

BPDU をブロックすると、スイッチの STP はディセーブルになります。ネットワーク レイアウトで ASA を含むループを設定しないでください。

上記のオプションのどちらも使用できない場合は、フェールオーバー機能またはSTPの安定性に影響する、推奨度の低い次の回避策のいずれかを使用できます。

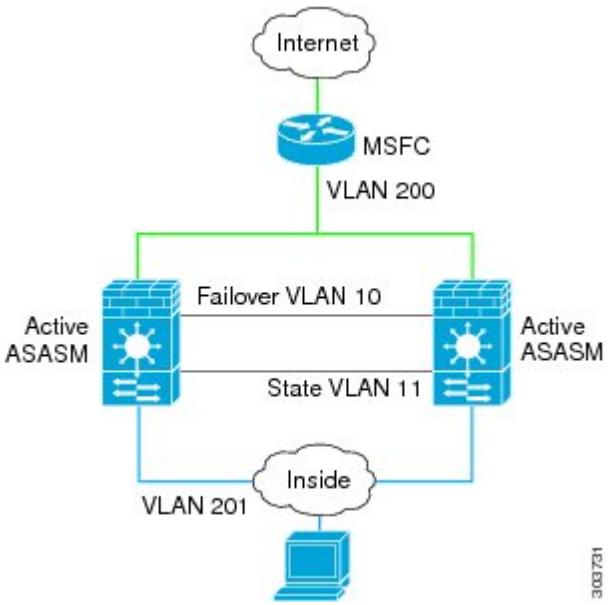
- インターフェイス モニタリングをディセーブルにします。
- ASA がフェールオーバーする前に、インターフェイスのホールド時間を STP が収束可能になる大きい値に増やします。
- STP がインターフェイスのホールド時間よりも速く収束するように、STP タイマーを減らします。

ASA サービス モジュールのブリッジグループ必須要件

ブリッジグループでのフェールオーバーの使用時にループを回避するには、BPDUの通過を許可し（デフォルト）、BPDU転送をサポートするスイッチ ソフトウェアを使用する必要があります。

両方のモジュールが互いの存在を検出する場合や、不正なフェールオーバー リンクなどによって、両方のモジュールが同時にアクティブになるときに、ループが発生することがあります。両方のASASMが2つの同じVLAN間でパケットをブリッジングするので、ブリッジグループメンバー間のパケットが両方のASASMによって無限に複製され、ループが発生します。BPDUがタイミングよく交換された場合は、スパニングツリープロトコルによって、これらのループが遮断されます。ループを遮断するには、VLAN 200 と VLAN 201 間で送信される BPDU をブリッジングする必要があります。

図 *12*：ブリッジグループ ループ



フェールオーバーのヘルス モニタ

ASAは、各装置について全体的なヘルスおよびインターフェイス ヘルスをモニタします。この項では、各装置の状態を判断するために、ASAがテストを実行する方法について説明します。

ユニットのヘルス モニタリング

ASAは、hello メッセージでフェールオーバー リンクをモニタして相手装置のヘルスを判断します。フェールオーバー リンクで 3 回連続して hello メッセージを受信しなかったときは、フェールオーバー リンクを含む各データ インターフェイスでLANTEST メッセージを送信し、ピアが応答するかどうかを確認します。 FirePOWER 9300 および 4100 シリーズでは、hello メッセージよりも信頼性の高い Bidirectional Forwarding Detection（BFD）モニタリングを有効にできます。ASAが行うアクションは、相手装置からの応答によって決まります。次の可能なアクションを参照してください。

- ASAがフェールオーバー リンクで応答を受信した場合、フェールオーバーは行われません。
- ASAがフェールオーバー リンクで応答を受信せず、データ インターフェイスで応答を受信した場合、装置のフェールオーバーは行われません。フェールオーバー リンク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。
- ASAがどのインターフェイスでも応答を受信しなかった場合、スタンバイ装置がアクティブ モードに切り替わり、相手装置を故障に分類します。

インターフェイス モニタリング

最大 1025 のインターフェイスをモニタできます（マルチ モードでは、すべてのコンテキスト間で分割）。重要なインターフェイスをモニタする必要があります。たとえば、マルチモードでは、共有インターフェイスを監視するように1つのコンテキストを設定する場合があります（インターフェイスが共有されているため、すべてのコンテキストがそのモニタリングで監視されます）。

装置が、2回のポーリング期間中にモニタ対象のインターフェイス上でhello メッセージを受信しない場合、インターフェイステストを実行します。1つのインターフェイスに対するすべてのインターフェイステストがすべて失敗したが、相手装置のこの同じインターフェイスが正常にトラフィックを渡し続けている場合、そのインターフェイスは故障していると見なされます。故障したインターフェイスがしきい値を超えている場合は、フェールオーバーが行われます。相手装置のインターフェイスでもすべてのネットワーク テストに失敗した場合、両方のインターフェイスは “Unknown” 状態になり、フェールオーバーの限界値に向けてのカウントは行われません。

インターフェイスは、何らかのトラフィックを受信すると、再度動作状態になります。故障したASAは、インターフェイス障害しきい値が満たされなくなった場合、スタンバイ モードに戻ります。

ASA Firepower SSP などのサービス モジュールがある場合、ASA はバックプレーン インターフェイスを介してモジュールもモニタします。モジュールの障害は装置の障害と見なされ、フェールオーバーがトリガーされます。この設定は設定可能です。

インターフェイスに IPv4 および IPv6 アドレスが設定されている場合、ASA は IPv4 を使用してヘルス モニタリングを実行します。

インターフェイスに IPv6 アドレスだけが設定されている場合、ASA は ARP ではなく IPv6 ネイバー探索を使用してヘルス モニタリング テストを実行します。ブロードキャスト ping テストの場合、ASA は IPv6 全ノード アドレス（FE02::1）を使用します。

（注） 障害が発生した装置が回復せず、実際には障害は発生していないと考えられる場合は、**failover reset** コマンドを使用して状態をリセットできます。ただし、フェールオーバー条件が継続している場合、装置は再び障害状態になります。

インターフェイス テスト

ASAでは、次のインターフェイス テストが使用されます。

1. リンク アップ/ダウンテスト：インターフェイス ステータスのテストです。リンク アップ/ダウンテストでインターフェイスがダウンしていることが示された場合、ASAは障害が発生したと見なします。ステータスがアップの場合、ASAはネットワーク アクティビティを実行します。
2. ネットワーク動作のテスト：ネットワークの受信動作のテストです。このテストの目的は、障害が発生している（いずれかにある場合）装置を判別するためにLANTESTメッセージを使用したネットワーク トラフィックを生成することです。テストの開始時に、各装置はインターフェイスの受信パケット カウントをリセットします。テスト中に装置がパケットを受信すると（最大 5 秒間）、すぐにインターフェイスは正常に動作していると見なされます。いずれか一方の装置だけがトラフィックを受信している場合は、トラフィックを受信しなかった装置が故障していると見なされます。どちらの装置もトラフィックを受信しなかった場合、ASAは ARP テストを開始します。
3. ARPテスト：取得したエントリの最後の2つの装置ARPキャッシュの読み取り。装置は、ネットワーク トラフィックを発生させるために、1 回に 1 つずつ、これらのマシンに ARP 要求を送信します。各要求後、装置は最大 5 秒間受信したトラフィックをすべてカウントします。トラフィックが受信されれば、インターフェイスは正常に動作していると見なされます。トラフィックが受信されなければ、ARP 要求が次のマシンに送信されます。リストの最後まで、まったくトラフィックが受信されなかった場合、ASAはpingテストを開始します。
4. ブロードキャスト ping テスト：このテストでは、ブロードキャスト ping 要求が送信されます。装置は、最大 5 秒間、すべての受信パケット数をカウントします。この時間間隔の間にパケットが受信されると、インターフェイスが正常に動作しているものと見なされ、テストは停止します。トラフィックが受信されなければ、ARPテストからやり直します。

Interface Status

モニタ対象のインターフェイスには、次のステータスがあります。

- 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。

フェールオーバー 時間

次の表は、最少、デフォルトおよび最大フェールオーバー時間を示します。

（注） CLI または ASDM を使用して手動でフェールオーバーした場合、もしくは ASA をリロードした場合、フェールオーバーはすぐに開始され、次に示すタイマーの影響は受けません。

表 *1 : ASA*

フェールオーバー条件	最小ハードウェア	デフォルト	最大
アクティブ装置で電源断が生じる、または通常の動作が停止する。	800 ミリ秒	15 秒	45 秒
アクティブ ユニット メイン ボード インターフェイス リンクがダウンする。	500 ミリ秒	5 秒	15 秒
アクティブ装置の 4GE モジュール インターフェイス リンクがダウンする。	2 秒	5 秒	15 秒
アクティブ ユニット Firepower モジュールは失敗する。	2 秒	2 秒	2 秒

フェールオーバー条件	最小ハードウェア	デフォルト	最大
アクティブ装置のインターフェイスは実行されているが、接続の問題によりインターフェイス テストを行っている。	5 秒	25 秒	75 秒

設定の同期

フェールオーバーには、さまざまなタイプのコンフィギュレーション同期があります。

コンフィギュレーションの複製の実行

コンフィギュレーションの複製は、フェールオーバーペアの一方または両方のデバイスのブート時に実行されます。

アクティブ/スタンバイ フェールオーバーでは、コンフィギュレーションは常に、アクティブ装置からスタンバイ装置に同期化されます。

アクティブ/アクティブ フェールオーバーでは、起動ユニットのプライマリまたはセカンダリ指定に関係なく、2番目に起動したユニットは、最初に起動したユニットから実行コンフィギュレーションを取得します。両方のユニットの起動後、システム実行スペースに入力されたコマンドは、フェールオーバー グループ 1 がアクティブ状態であるユニットから複製されます。

スタンバイ/セカンドユニットが初期スタートアップを完了すると、実行コンフィギュレーションを削除し（アクティブ ユニットとの通信に必要な**failover** コマンドを除く）、アクティブ ユニットはコンフィギュレーション全体をスタンバイ/セカンド ユニットに送信します。複製が開始されると、アクティブ ユニットの 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、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。コンフィギュレーションのサイズによって、複製には数秒から数分かかります。

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。コンフィギュレーションの変更の保存に従ってコンフィギュレーションをフラッシュ メモリに保存する必要があります。たとえば、アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブ状態であるユニット上の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。



（注） 複製中、コンフィギュレーションを送信しているユニット上に入力されたコマンドは、ピアユニットに正常に複製されず、コンフィギュレーションを受信するユニット上に入力されたコマンドは、受信したコンフィギュレーションによって上書きできます。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。

（注） **crypto ca server** コマンドおよび関連するサブコマンドはフェールオーバーをサポートしません。**no crypto ca server** コマンドを使用して、削除する必要があります。

File Replication

コンフィギュレーションの同期は次のファイルと構成コンポーネントを複製しません。したがって、これらのファイルが一致するように手動でコピーする必要があります。

- AnyConnect イメージ
- CSD イメージ
- AnyConnect プロファイル

  ASA では、フラッシュ ファイル システムに保存されたファイルではなく、cache:/stc/profiles に保存された AnyConnect クライアント ファイルのキャッシュ済みファイルが使用されます。AnyConnect クライアント プロファイルをスタンバイ装置に複製するには、次のいずれかを実行します。

  - アクティブ装置で **write standby** コマンドを入力します。
  - アクティブ装置でプロファイルを再適用します。
  - スタンバイ装置をリロードします。

- ローカル認証局（CA）
- ASA イメージ
- ASDM イメージ

Command Replication

スタートアップ後、アクティブ装置に入力したコマンドはただちにスタンバイ装置に複製されます。コマンドを複製するために、アクティブ コンフィギュレーションをフラッシュ メモリに保存する必要はありません。

アクティブ/アクティブ フェールオーバーでは、システム実行スペースに入力したコマンドは、フェールオーバー グループ 1 がアクティブ状態である装置から複製されます。

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同期されません。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。

スタンバイ ASA に複製されるコマンドは、次のとおりです。

- 次を除くすべてのコンフィギュレーション コマンド。**mode**、**firewall**、および **failover lan unit**
- **copy running-config startup-config**

- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

スタンバイ ASA に複製されないコマンドは、次のとおりです。

- 次を除く、すべての形式の **copy** コマンド。 **copy running-config startup-config**
- 次を除く、すべての形式の **write** コマンド。 **write memory**
- **debug**
- **failover lan unit**
- **firewall**
- **show**
- **terminal pager** および **pager**

アクティブ/スタンバイ フェールオーバーについて

アクティブ/スタンバイ フェールオーバーでは、障害が発生した装置の機能を、スタンバイ ASAに引き継ぐことができます。アクティブ装置に障害が発生した場合、スタンバイ装置がアクティブ装置になります。

（注） マルチコンテキスト モードでは、ASA は装置全体（すべてのコンテキストを含む）のフェールオーバーを行いますが、各コンテキストを個別にフェールオーバーすることはできません。

プライマリ/セカンダリ ロールとアクティブ/スタンバイ ステータス

フェールオーバーペアの2つのユニットの主な相違点は、どちらのユニットがアクティブでどちらのユニットがスタンバイであるか、つまりどちらの IP アドレスを使用するか、およびどちらのユニット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。

しかし、プライマリである装置（コンフィギュレーションで指定）とセカンダリである装置との間で、いくつかの相違点があります。

- 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。
- プライマリ ユニットの MAC アドレスは常に、アクティブ IP アドレスと結び付けられています。このルールの例外は、セカンダリ ユニットがアクティブであり、フェールオー

バー リンク経由でプライマリ ユニットの MAC アドレスを取得できない場合に発生します。この場合、セカンダリ装置の MAC アドレスが使用されます。

起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はスタンバイ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時にブートされた場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がスタンバイ装置になります。

フェールオーバー イベント

アクティブ/スタンバイ フェールオーバーでは、フェールオーバーは装置ごとに行われます。マルチ コンテキスト モードで動作中のシステムでも、個々のコンテキストまたはコンテキストのグループをフェールオーバーすることはできません。

次の表に、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。この表には、各フェールオーバー イベントに対して、フェールオーバー 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）、アクティブ装置が行うアクション、スタンバイ装置が行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 *2:* フェールオーバー イベント

障害の状況	ポリシー（Policy）	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	注意
アクティブ装置が故障（電源またはハードウェア）	フェールオーバー	n/a	アクティブになる アクティブに故障とマークする	モニタ対象インターフェイスまたはフェールオーバー リンクで hello メッセージは受信されません。
以前にアクティブであった装置の復旧	フェールオーバーなし	スタンバイになる	動作なし	なし。
スタンバイ装置が故障（電源またはハードウェア）	フェールオーバーなし	スタンバイに故障とマークする	n/a	スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。

障害の状況	ポリシー（**Policy**）	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	注意
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	フェールオーバーリンクに故障とマークする	フェールオーバーリンクに故障とマークする	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。
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	フェールオーバーリンクに故障とマークする	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、両方の装置がアクティブになります。
ステートリンクの障害	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。
アクティブ装置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	アクティブに故障とマークする	アクティブになる	なし。
スタンバイ装置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	スタンバイに故障とマークする	スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。

アクティブ/アクティブ フェールオーバーの概要

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。

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 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

バーでは、ASA のセキュリティ コンテキストを 2 つまでのフェールオーバー グループに分割します。

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。フェールオーバー グループをプライマリ ASA でアクティブに割り当て、フェールオーバー グループ 2 をセカンデリ ASA でアクティブに割り当てることができます。フェールオーバーが行われる場合は、フェールオーバー グループ レベルで行われます。たとえば、インターフェイス障害パターンに応じて、フェールオーバー グループ 1 をセカンデリ ASA にフェールオーバーし、続いてフェールオーバー グループ 2 をプライマリ ASA にフェールオーバーすることができます。このイベントは、プライマリ ASA でフェールオーバー グループ 1 のインターフェイスがダウンしたがセカンデリではアップしており、セカンデリ ASA でフェールオーバー グループ 2 のインターフェイスがダウンしたがプライマリ ASA ではアップしている場合に発生する可能性があります。

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 のメンバです。アクティブ/アクティブ フェールオーバーが必要であるが複数コンテキストは必要ない場合、最もシンプルな設定は他のコンテキストを 1 つ追加し、それをフェールオーバー グループ 2 に割り当てることです。

（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。

（注） 必要に応じて両方のフェールオーバー グループを 1 つの ASA に割り当てることもできますが、この場合、アクティブな ASA を 2 つ持つというメリットはありません。

フェールオーバー グループのプライマリ/セカンデリ ロールとアクティブ/スタンバイ ステータス

アクティブ/スタンバイ フェールオーバーと同様、アクティブ/アクティブ フェールオーバー ペアの 1 つの装置がプライマリ ユニットに指定され、もう 1 つの装置がセカンダリ ユニットに指定されます。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。

- ペアが同時に起動したときに、プライマリ装置が実行コンフィギュレーションを提供します。
- 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。プリエンプションで使用すると、このプレファレンスはフェールオーバー グループが起動後に正しいユニットで実行されるようにします。プリエンプションがない場合、両方のグループは最初に起動したユニットで動作します。

起動時のフェールオーバー グループのアクティブ装置の決定

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

- 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。

フェールオーバー イベント

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。

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。

次の表に、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 *3:* フェールオーバー イベント

障害の状況	ポリシー（**Policy**）	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	注意
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。

障害の状況	ポリシー（**Policy**）	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	注意
ステートリンクの障害	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、フェールオーバーリンク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。

フェールオーバーのライセンス

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。このルールには、いくつかの例外があります。フェールオーバーの正確なライセンス要件については、次の表を参照してください。

モデル	ライセンス要件
ASA 5506-X および ASA 5506W-X	• アクティブ/スタンバイ：Security Plus ライセンス。 • アクティブ/アクティブ：サポートなし。 （注） 各ユニットに同じ暗号化ライセンスが必要です。

モデル	ライセンス要件
ASA 5512-X ～ ASA 5555-X	• ASA 5512-X：Security Plus ライセンス。 • 他のモデル：基本ライセンス。 （注） • 各ユニットに同じ暗号化ライセンスが必要です。 • マルチ コンテキスト モードでは、各ユニットに同じ AnyConnect Apex ライセンスが必要です。 • 各ユニットに同じ IPS モジュール ライセンスが必要です。両方の装置の IPS 側で IPS シグニチャ サブスクリプションも必要です。次のガイドラインを参照してください。 • IPS シグニチャ サブスクリプションを購入するには、IPS がプリインストールされた ASA が必要です（製品番号に、たとえば ASA5515-IPS-K9 のように「IPS」が含まれている必要があります）。IPS ではない製品番号の ASA に IPS シグニチャ サブスクリプションを購入することはできません。 • 両方の装置に IPS シグニチャ サブスクリプションが必要です。このサブスクリプションは ASA ライセンスではないため、フェールオーバー間で共有されません。 • IPS シグニチャ サブスクリプションには、装置ごとに個別の IPS モジュール ライセンスが必要です。他の ASA のライセンスと同様に、IPS モジュール ライセンスも技術的にはフェールオーバー クラスタ ライセンスで共有されます。しかし、IPS シグニチャ サブスクリプションの要件によって、装置ごとに個別の IPS モジュール ライセンスを購入する必要があります。
ASAv	ASAv のフェールオーバー ライセンスを参照してください。

モデル	ライセンス要件
Firepower 2100 の ASA	Firepower 2100 のフェールオーバー ライセンスを参照してください。
Firepower 4100/9300 シャーシ 上の ASA	Firepower 4100/9300 シャーシ の ASA のフェールオーバー ライセンスを参照してください。
他のすべてのモデル	基本ライセンスまたは標準ライセンス。 （注） • 各ユニットに同じ暗号化ライセンスが必要です。 • マルチ コンテキスト モードでは、各ユニットに同じ AnyConnect Apex ライセンスが必要です。

（注） 有効な永続キーが必要です。まれに、PAK 認証キーを削除できることもあります。キーがすべて 0 の場合は、フェールオーバーを有効化するには有効な認証キーを再インストールする必要があります。

フェールオーバーのガイドライン

コンテキスト モード

- アクティブ/アクティブ モードは、マルチ コンテキスト モードでのみサポートされます。
- マルチ コンテキスト モードでは、特に注記がない限り、手順はすべてシステム実行スペースで実行します。

サポート モデル

- ASA 5506W-X：内部 GigabitEthernet 1/9 インターフェイスのインターフェイス モニタリングを無効にする必要があります。これらのインターフェイスは、デフォルトのインターフェイス モニタリング チェックを実行するために通信することができないため、予期されたインターフェイス通信の障害により、スイッチがアクティブからスタンバイに切り替えられ、元に戻ります。
- FirePOWER 9300 の ASA：シャーシ間フェールオーバーを使用して最良の冗長性を確保することを推奨します。

- Microsoft Azure や Amazon Web Services などのパブリック クラウド ネットワーク上の ASAv では、レイヤ 2 接続が必要なため、フェールオーバーはサポートされません。パブリック クラウドの高可用性のフェールオーバーを参照してください。
- ASA FirePOWER モジュールはフェールオーバーを直接サポートしていません。ASA がフェールオーバーすると、既存の ASA FirePOWER フローは新しい ASA に転送されます。新しい ASA の ASA FirePOWER モジュールが、その転送の時点からトラフィックの検査を開始します。古いインスペクションのステートは転送されません。

  フェールオーバーの動作の整合性を保つために、ハイアベイラビリティな ASA ペアの ASA FirePOWER モジュールで一貫したポリシーを保持する必要があります。

（注） ASA FirePOWER モジュールを設定する前に、フェールオーバー ペアを作成します。モジュールが両方のデバイスにすでに設定されている場合は、フェールオーバー ペアを作成する前にスタンバイ デバイスのインターフェイスの設定をクリアします。スタンバイ デバイスの CLI から、 **clear configure interface** コマンドを入力します。

その他のガイドライン

- アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニングツリープロトコル（STP）を実行している接続済みスイッチ ポートは、トポロジ変更を検出すると 30 ～ 50 秒間ブロッキング ステートに移行できます。ポートがブロッキング ステートである間のトラフィック損失を防ぐには、スイッチで STP PortFast 機能を有効にします。

  interface *interface_id***spanning-tree portfast**

  この回避策は、ルーテッド モードおよびブリッジ グループ インターフェイスの両方に接続されているスイッチに適用されます。PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは引き続き STP に参加しています。したがって、ポートがループの一部になる場合、最終的には STP ブロッキング モードに遷移します。
- ローカル CA サーバが設定されている場合、フェールオーバーを有効にできません。CA コンフィギュレーションを削除するには、**no crypto ca server** コマンドを使用します。
- 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。この問題は、あるセキュア 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、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た場合に発生します。
- すべてのコンテキストにわたり、1 台の装置の最大 1025 のインターフェイスをモニタできます。

- アクティブ/スタンバイ フェールオーバーと VPN IPsec トンネルの場合、SNMP を使用して VPN トンネル上でアクティブ ユニットとスタンバイ ユニットの両方をモニタすることはできません。スタンバイ ユニットにはアクティブ VPN トンネルがないため、NMS に向けられたトラフィックはドロップされます。代わりに、暗号化付き SNMPv3 を使用すると、IPsec トンネルが必要ありません。
- アクティブ/アクティブ フェールオーバーでは、同じコンテキスト内の2つのインターフェイスを同じ ASR グループ内で設定することはできません。
- アクティブ/アクティブ フェールオーバーでは、最大 2 つのフェールオーバー グループを定義できます。
- アクティブ/アクティブ フェールオーバーでフェールオーバー グループを削除する場合は、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。

フェールオーバーのデフォルト

デフォルトでは、フェールオーバー ポリシーは次の事項が含まれます。

- ステートフル フェールオーバーでの HTTP 複製は行われません。
- 単一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。
- インターフェイスのポーリング時間は 5 秒です。
- インターフェイスのホールド時間は 25 秒です。
- 装置のポーリング時間は 1 秒です。
- 装置のホールド時間は 15 秒です。
- 仮想 MAC アドレスはマルチ コンテキスト モードで無効化されています。ASASM では、デフォルトで有効になっています。
- すべての物理インタフェイス、または ASASM の場合、すべての VLAN インターフェイスをモニタリングします。

アクティブ/スタンバイ フェールオーバーの設定

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、プライマリ装置とセカンデリ装置の両方で基本的なフェールオーバー設定を構成します。その他すべての設定をプライマリ装置でのみ行った後、セカンデリ装置に設定を同期させます。

アクティブ/スタンバイ フェールオーバーのプライマリ装置の設定

この項の手順に従って、アクティブ/スタンバイ フェールオーバー構成のプライマリを設定します。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。

始める前に

- フェールオーバー リンクとステート リンクを除くすべてのインターフェイスのスタンバイ IP アドレスを設定することを推奨します。ポイントツーポイント接続に 31 ビット サブネット マスクを使用する場合、スタンバイ IP アドレスを設定しないでください。
- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。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

ステップ 1 この装置をプライマリ装置に指定します。

failover lanunit primary

ステップ 2 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。

failover laninterface *if_name interface_id*

例：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

このインターフェイスは、他の目的には使用できません（オプションのステート リンクは除く）。

if_name 引数は、インターフェイスに名前を割り当てます。

interface_id 引数には、データ物理インターフェイス、サブインターフェイス、冗長インターフェイス、または EtherChannel インターフェイス ID を指定できます。ASASM では、*interface_id* に VLAN ID を指定します。ASA 5506H-X の場合に限り、管理 1/1 インターフェイスをフェールオーバー リンクとして指定できます。その場合、**write memory** を使用してコンフィギュレーションを保存してから、**reload** を使用してデバイスをリロードする必要があります。デバイスをリロードした後は、このインターフェイスと ASA FirePOWER モジュールの両方をフェールオーバーに使用できなくなります。ASA FirePOWER モジュールには管理用インターフェイスが必要であり、そのインターフェイスは 1 つの機能にのみ使用できます。FirePOWER 9300 ASA セキュリティ モジュールでは、データ タイプまたは管理タイプの任意のインターフェイスを使用できます。

ステップ 3 アクティブ IP アドレスとスタンバイ IP アドレスをフェールオーバー リンクに割り当てます。

failover interface ip *failover_if_name* {*ip_address mask* | *ipv6_address* / *prefix*} **standby** *ip_address*

例：

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

または：

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

このアドレスは、未使用のサブネット上になければなりません。このサブネットは IP アドレスが 2 つだけの 31 ビット（255.255.255.254）にすることができます。

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。

ステップ 4 フェールオーバー リンクをイネーブルにします。

interface *failover_interface_id*

no shutdown

例：

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

ステップ 5 （オプション）ステート リンクとして使用するインターフェイスを指定します。

failover link *if_name interface_id*

例：

```
ciscoasa(config)# failover link folink gigabitethernet0/3
```

フェールオーバー リンクをステート リンクと共有することができます。

if_name 引数は、インターフェイスに名前を割り当てます。

interface_id 引数には、物理インターフェイス、サブインターフェイス、冗長インターフェイス、または EtherChannel インターフェイス ID を指定できます。ASASM では、*interface_id* に VLAN ID を指定します。

ステップ 6 別のステート リンクを指定した場合、ステート リンクにアクティブ IP アドレスとスタンバイ IP アドレスを割り当てます。

failover interface ip *state_if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

例：

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

または：

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

このアドレスは、フェールオーバー リンクとは異なる未使用のサブネット上になければなりません。 このサブネットは IP アドレスが 2 つだけの 31 ビット（255.255.255.254）にすることができます。

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。

ステート リンクを共有する場合は、この手順をとばしてください。

ステップ 7 別のステート リンクを指定した場合、ステート リンクをイネーブルにします。

interface *state_interface_id*

no shutdown

例：

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

ステート リンクを共有する場合は、この手順をとばしてください。

ステップ 8 （オプション）フェールオーバー リンクおよびステート リンクの通信を暗号化するには、次のいずれかを実行します。

- （優先）すべてのフェールオーバー通信を暗号化するには、装置間のフェールオーバー リンクおよびステート リンクの IPsec LAN-to-LAN トンネルを確立します。

  failover ipsecpre-shared-key [**0** | **8**] *key*

  例：

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

  key は最大 128 文字です。両方の装置に同じキーを指定します。キーは IKEv2 によってトンネルを確立するために使用されます。

  マスターパスフレーズ（マスターパスフレーズの設定を参照）を使用している場合、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は（たとえば **more system:running-config** の出力からのコピー）、キーワード **8** を使用してキーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

  show running-config の出力では、**failover ipsec pre-shared-key** は ***** のように表示されます。このマスクされたキーはコピーできません。

  フェールオーバー リンクおよびステート リンクの暗号化を設定しない場合、フェールオーバー通信はクリア テキストになります。この通信にはコマンド複製中に送信されるコンフィギュレーション内のすべてのパスワードやキーも含まれます。

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、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。

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。

- （オプション）フェールオーバー リンクおよびステート リンクのフェールオーバー通信を暗号化します。

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  例：

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  1 ～ 63 文字の *shared_secret* または 32 文字の **16 進数**キーを使用します。*shared_secret* には、数字、文字、または句読点の任意の組み合わせを使用できます。共有秘密または 16 進数キーは暗号キーを生成するために使用されます。両方の装置に同じキーを指定します。

  マスター パスフレーズ（マスター パスフレーズの設定を参照）を使用している場合、共有秘密または 16 進数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は（たとえば **more system:running-config** の出力からのコピー）、キーワード **8** を使用して共有秘密または 16 進数キーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

  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。

  フェールオーバー リンクおよびステート リンクの暗号化を設定しない場合、フェールオーバー通信はクリア テキストになります。この通信にはコマンド複製中に送信されるコンフィギュレーション内のすべてのパスワードやキーも含まれます。

ステップ 9 フェールオーバーをイネーブルにします。

failover

ステップ 10 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。

write memory

例

次に、プライマリ装置用のフェールオーバー パラメータの設定例を示します。

```
failover lan unit primary
```

```
failover lan interface folink gigabitethernet0/3

failover interface ip folink 172.27.48.0 255.255.255.254 standby 172.27.48.1
interface gigabitethernet 0/3
  no shutdown
failover link folink gigabitethernet0/3
failover ipsec pre-shared-key a3rynsun
failover
```

アクティブ/スタンバイ フェールオーバーのセカンダリ装置の設定

セカンデリ装置に必要なコンフィギュレーションは、フェールオーバー リンクのコンフィギュレーションだけです。セカンダリ装置には、プライマリ装置と初期に通信するために、これらのコマンドが必要です。プライマリ装置がセカンダリ装置にコンフィギュレーションを送信した後、2 つのコンフィギュレーション間で唯一、不変の相違点は **failover lan unit** コマンドです。このコマンドで各装置がプライマリかセカンダリかを識別します。

始める前に

- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。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

ステップ 1 **failover lan unit primary** コマンドを除いて、プライマリ装置とまったく同じコマンドを再入力します。任意で **failover lan unit secondary** コマンドに置き換えることもできますが、**secondary** はデフォルト設定のため、必須ではありません。アクティブ/スタンバイ フェールオーバーのプライマリ装置の設定 （36 ページ）を参照してください。

次に例を示します。

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-ifc)# no shutdown
ciscoasa(config-ifc)# failover link folink gigabitethernet0/3
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

ステップ 2 フェールオーバー コンフィギュレーションが同期された後で、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。

```
ciscoasa(config)# write memory
```

アクティブ/アクティブ フェールオーバーの設定

ここでは、アクティブ/アクティブ フェールオーバーの設定方法について説明します。

アクティブ/アクティブ フェールオーバーのプライマリ装置の設定

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。

始める前に

- マルチ コンテキスト モードの有効化またはディセーブル化に従って、マルチ コンテキスト モードをイネーブルにします。
- ルーテッド モード インターフェイスとトランスペアレント モード インターフェイスに従って、フェールオーバー リンクとステート リンクを除くすべてのインターフェイスのスタンバイ IP アドレスを設定することを推奨します。 ポイントツーポイント接続に 31 ビット サブネット マスクを使用する場合、スタンバイ IP アドレスを設定しないでください。
- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- 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

ステップ 1 この装置をプライマリ装置に指定します。

failover lanunitprimary

ステップ 2 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。

failover laninterface *if_name interface_id*

例：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

このインターフェイスは、他の目的には使用できません（オプションのステート リンクは除く）。

if_name 引数は、インターフェイスに名前を割り当てます。

interface_id 引数には、物理インターフェイス、サブインターフェイス、冗長インターフェイス、または EtherChannel インターフェイス ID を指定できます。ASASM では、*interface_id* に VLAN ID を指定します。

ステップ 3 アクティブ IP アドレスとスタンバイ IP アドレスをフェールオーバー リンクに割り当てます。

standby failover interface ip *if_name* {*ip_address mask* | *ipv6_address*/*prefix* } **standby** *ip_address*

例：

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

または：

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

このアドレスは未使用のサブネット上になければなりません。 このサブネットは IP アドレスが 2 つだけの 31 ビット（255.255.255.254）にすることができます。

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。

ステップ 4 フェールオーバー リンクをイネーブルにします。

interface *failover_interface_id*

no shutdown

例：

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

ステップ 5 （オプション）ステート リンクとして使用するインターフェイスを指定します。

failover link *if_name interface_id*

例：

```
ciscoasa(config)# failover link statelink gigabitethernet0/4
```

フェールオーバー リンクまたはデータ インターフェイスとは異なるインターフェイスを指定することをお勧めします。

if_name 引数は、インターフェイスに名前を割り当てます。

interface_id 引数には、物理インターフェイス、サブインターフェイス、冗長インターフェイス、または EtherChannel インターフェイス ID を指定できます。ASASM では、*interface_id* に VLAN ID を指定します。

ステップ 6 別のステート リンクを指定した場合、ステート リンクにアクティブ IP アドレスとスタンバイ IP アドレスを割り当てます。

このアドレスは、フェールオーバー リンクとは異なる未使用のサブネット上になければなりません。 このサブネットは IP アドレスが 2 つだけの 31 ビット（255.255.255.254）にすることができます。

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。

ステート リンクを共有する場合は、この手順をとばしてください。

failover interface ipstate *if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

例：

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

または：

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

ステップ 7 別のステート リンクを指定した場合、ステート リンクをイネーブルにします。

interface *state_interface_id*

no shutdown

例：

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

ステート リンクを共有する場合は、この手順をとばしてください。

ステップ 8 （オプション）フェールオーバー リンクおよびステート リンクの通信を暗号化するには、次のいずれかを実行します。

- （優先）すべてのフェールオーバー通信を暗号化するには、装置間のフェールオーバー リンクおよびステート リンクの IPsec LAN-to-LAN トンネルを確立します。

  failover ipsecpre-shared-key [**0** | **8**] *key*

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

  key は最大 128 文字です。両方の装置に同じキーを指定します。キーは IKEv2 によってトンネルを確立するために使用されます。

  マスターパスフレーズ（マスターパスフレーズの設定を参照）を使用している場合、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は（たとえば **more system:running-config** の出力からのコピー）、キーワード **8**

を使用してキーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

show running-config の出力では、**failover ipsec pre-shared-key** は ***** のように表示されます。このマスクされたキーはコピーできません。

フェールオーバー リンクおよびステート リンクの暗号化を設定しない場合、フェールオーバー通信はクリア テキストになります。この通信にはコマンド複製中に送信されるコンフィギュレーション内のすべてのパスワードやキーも含まれます。

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、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。

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。

- （オプション）フェールオーバー リンクおよびステート リンクのフェールオーバー通信を暗号化します。

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  1 ～ 63 文字の *shared_secret* または 32 文字の **16 進数**キーを使用します。

  shared_secret には、数字、文字、または句読点の任意の組み合わせを使用できます。共有秘密または16進数キーは暗号キーを生成するために使用されます。両方の装置に同じキーを指定します。

  マスター パスフレーズ（マスター パスフレーズの設定を参照）を使用している場合、共有秘密または 16 進数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は（たとえば **more system:running-config** の出力からのコピー）、キーワード **8** を使用して共有秘密または 16 進数キーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

  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。

  フェールオーバー リンクおよびステート リンクの暗号化を設定しない場合、フェールオーバー通信はクリア テキストになります。この通信にはコマンド複製中に送信されるコンフィギュレーション内のすべてのパスワードやキーも含まれます。

ステップ 9　フェールオーバー グループ 1 を作成します。

failover group1

primary

preempt [*delay*]

例：

```
ciscoasa(config-fover-group)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 1200
```

通常、プライマリ装置にグループ 1 を割り当て、セカンデリ装置にグループ 2 を割り当てます。グループの primary または secondary の設定にかかわらず、両方のフェールオーバー グループが最初にブートしたユニットでアクティブになります（それらが同時に起動したように見える場合でも、一方のユニットが最初にアクティブになります）。**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。

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。

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。

手動でフェールオーバーすると、**preempt** コマンドは無視されます。

ステップ 10 フェールオーバー グループ 2 を作成して、セカンデリ装置に割り当てます。

failover group 2

secondary

preempt [*delay*]

例：

```
ciscoasa(config-fover-group)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 1200
```

ステップ 11 特定のコンテキストのコンテキスト コンフィギュレーション モードに入り、その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。

context *name*

join-failover-group {**1** | **2**}

例：

```
ciscoasa(config)# context Eng
ciscoasa(config-ctx)# join-failover-group 2
```

コンテキストごとにこのコマンドを繰り返します。

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 のメンバーです。グループ 2 に割り当てることはできません。

ステップ 12 フェールオーバーをイネーブルにします。

failover

ステップ 13 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。

write memory

例

次に、プライマリ装置用のフェールオーバー パラメータの設定例を示します。

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3

failover interface ip folink 172.27.48.0 255.255.255.254 standby 172.27.48.1
interface gigabitethernet 0/3
  no shutdown
failover link statelink gigabitethernet0/4

failover interface ip statelink 172.27.48.2 255.255.255.254 standby 172.27.48.3
interface gigabitethernet 0/4
  no shutdown
failover group 1
  primary
  preempt
failover group 2
  secondary
  preempt
context admin
  join-failover-group 1
failover ipsec pre-shared-key a3rynsun
failover
```

アクティブ/アクティブ フェールオーバーのセカンデリ装置の設定

セカンデリ装置に必要なコンフィギュレーションは、フェールオーバー リンクのコンフィギュレーションだけです。セカンダリ装置には、プライマリ装置と初期に通信するために、これらのコマンドが必要です。プライマリ装置がセカンダリ装置にコンフィギュレーションを送信した後、2 つのコンフィギュレーション間で唯一、不変の相違点は **failover lan unit** コマンドです。このコマンドで各装置がプライマリかセカンダリかを識別します。

始める前に

- マルチ コンテキスト モードの有効化またはディセーブル化に従って、マルチ コンテキスト モードをイネーブルにします。
- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- 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

ステップ 1 **failover lan unit primary** コマンドを除いて、プライマリ装置とまったく同じコマンドを再入力します。任意で **failover lan unit secondary** コマンドに置き換えることもできますが、**secondary** はデフォルト設定のため、必須ではありません。また、プライマリ装置から複製されるので、**failover group** コマンドおよび **join-failover-group** コマンドを入力する必要もありません。アクティブ/アクティブ フェールオーバーのプライマリ装置の設定 （41 ページ）を参照してください。

次に例を示します。

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
no shutdown
ciscoasa(config)# failover link statelink gigabitethernet0/4
INFO: Non-failover interface config is cleared on GigabitEthernet0/4 and its sub-interfaces
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
ciscoasa(config)# interface gigabitethernet 0/4
no shutdown
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

ステップ 2 フェールオーバー コンフィギュレーションがプライマリ装置と同期された後で、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。

ciscoasa(config)# **write memory**

ステップ 3 必要に応じて、フェールオーバー グループ 2 がセカンデリ装置でアクティブになるように設定します。

failover activegroup2

オプションのフェールオーバー パラメータの設定

必要に応じてフェールオーバー設定をカスタマイズできます。

フェールオーバー基準とその他の設定の構成

この項で変更可能な多くのパラメータのデフォルト設定については、フェールオーバーのデフォルト （35 ページ）を参照してください。アクティブ/アクティブ モードでは、ほとんどの条件をフェールオーバー グループごとに設定します。

始める前に

- マルチ コンテキスト モードのシステム実行スペースで次の設定を行います。
- ユニットのヘルス モニタリングの Bidirectional Forwarding Detection（BFD）については次の制限を参照してください。
  - 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

手順

ステップ 1 装置のポーリング時間およびホールド時間を変更します。

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

例：

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

polltime の範囲は 1 ～ 15 秒または 200 ～ 999 ミリ秒です。**holdtime** の範囲は 1 ～ 45 秒または 800 ～ 999 ミリ秒です。ユニットのポーリング時間の 3 倍未満の holdtime の値を入力することはできません。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。

1 回のポーリング期間中に、装置がフェールオーバー通信インターフェイスで hello パケットを検出しなかった場合、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。

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。

ステップ 2 ユニットのヘルス モニタリングの BFD を設定します。

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。

a) フェールオーバーのヘルス検出に使用する BFD テンプレートを定義します。

bfd-template single-hop *template_name*

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

例：

```
ciscoasa(config)# bfd template single-hop failover-temp
```

```
ciscoasa(config-bfd)# bfd interval min-tx 50 min-rx 50 multiplier 3
```

min-tx で、BFD制御パケットがフェールオーバー ピアに送信されるレートを指定します。有効値は 50 ～ 999 ミリ秒です。**min-rx** で、BFD 制御パケットをフェールオーバー ピアから受信するレートの期待値を指定します。有効値は 50 ～ 999 ミリ秒です。フェールオーバー ピアから紛失した連続した BFD 制御パケットの数が、**multiplier** で指定した数に達すると、BFD はそのピアが利用不可になっていることを宣言します。指定できる範囲は 3 ～ 50 です。

このテンプレートのエコーおよび認証も設定できます。BFDテンプレートの作成 を参照してください。

b) ヘルス モニタリングの BFD を有効化します。

failover health-check bfd *template_name*

例：

```
ciscoasa(config)# failover health-check bfd failover-temp
```

ステップ 3 インターフェイス リンク ステート ポーリング時間を変更します。

failover polltime link-state msec *poll_time*

例：

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

範囲は 300 ～ 799 ミリ秒です。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。

ステップ 4 セッションの複製レートを、1 秒間の接続数で設定します。

failover replication rate *conns*

例：

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

最小および最大レートはモデルによって異なります。デフォルトは最大レートです。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。

ステップ 5 スタンバイ装置またはコンテキストのコンフィギュレーションを直接変更できないようにします。

failover standby config-lock

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。

ステップ 6 （アクティブ/アクティブ モードのみ）カスタマイズするフェールオーバー グループを指定します。

failovergroup {**1** | **2**}

例：

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)#
```

ステップ 7 HTTP ステート複製をイネーブルにします。

- アクティブ/スタンバイ モードの場合

  failover replication http

- アクティブ/アクティブ モードの場合

  replication http

HTTP 接続がステート情報複製に含まれるようにするには、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。

（注） フェールオーバーの使用時にスタンバイユニットからHTTPフローを削除すると、遅延のために、**show conn count** の出力はアクティブなユニットとスタンバイ ユニットで異なる数を表示する可能性があります。数秒待ってからコマンドを再発行すると、両方のユニットで同じ番号が表示されるようになります。

ステップ 8 インターフェイスに障害が発生したときのフェールオーバーのしきい値を設定します。

- アクティブ/スタンバイ モードの場合

  failoverinterface-policy *num* [%]

  例：

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

- アクティブ/アクティブ モードの場合

  interface-policy *num* [%]

  例：

  ```
  ciscoasa(config-fover-group)# interface-policy 20%
  ```

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。

インターフェイスの具体的な数を指定するときは、*num* 引数に 1 ～ 1025 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。

ステップ 9 インターフェイスのポーリング時間とホールド時間を変更します。

- アクティブ/スタンバイ モードの場合

  failoverpolltimeinterface [**msec**] *time* [**holdtime** *time*]

  例：

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

- アクティブ/アクティブ モードの場合

  polltimeinterface [**msec**] *time* [**holdtime***time*]

  例：

```
ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
```

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。

インターフェイス リンクがダウンしていると、インターフェイスのテストは実行されず、設定されたフェールオーバー基準に障害のあるインターフェイスの数が合致するか、または基準を超過している場合、スタンバイ装置は、1 つのインターフェイス ポーリング期間内でアクティブになります。

ステップ 10 インターフェイスの仮想 MAC アドレスを設定します。

- アクティブ/スタンバイ モードの場合

  failover mac address *phy_if active_mac standby_mac*

  例：

```
ciscoasa(config)# failover mac address gigabitethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

- アクティブ/アクティブ モードの場合

  mac address *phy_if active_mac standby_mac*

  例：

```
ciscoasa(config-fover-group)# mac address gigabitethernet0/2 00a0.c969.87c8
00a0.c918.95d8
```

phy_if 引数は、インターフェイスの物理名（gigabitethernet0/1 など）です。

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。

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。

ステップ 11 （アクティブ/アクティブ モードのみ）他のフェールオーバー グループについてこの手順を繰り返します。

インターフェイス モニタリングの設定

デフォルトでは、すべての物理インターフェイス、（ASASM の場合は）すべての VLAN インターフェイス、および ASA にインストールされるすべてのハードウェア/ソフトウェア モジュール（ASA FirePOWER モジュールなど）でモニタリングが有効化されています。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除外できます。

始める前に

- 装置ごとに最大 1025 のインターフェイスをモニタできます（マルチ コンテキスト モードのすべてのコンテキストにわたって）。
- マルチ コンテキスト モードで、各コンテキスト内のインターフェイスを設定します。

手順

インターフェイスのヘルス モニタリングをイネーブルまたはディゼーブルにします。

[**no**] **monitor-interface** {*if_name* | **service-module**}

例：

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)# no monitor-interface eng1
```

ASA FirePOWER モジュールなどの特定のハードウェア/ソフトウェア モジュールの障害によってフェールオーバーをトリガーすることが望ましくない場合は、**no monitor-interface service-module** コマンドを使用してモジュールのモニタリングを無効化できます。なお、ASA

5585-X では、サービス モジュールのモニタリングを無効にする場合、個別にモニタされるモジュール上の各インターフェイスのモニタリングを無効にすることもできます。

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 モード）

アクティブ/アクティブ フェールオーバーでの実行中に、ピア装置を経由して開始された接続に対する返送パケットを、装置が受信する場合があります。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。このドロップが多く発生するのは、アクティブ/アクティブ フェールオーバー ペアの 2 台の ASA が異なるサービス プロバイダーに接続されており、アウトバウンド接続に NAT アドレスが使用されていない場合です。

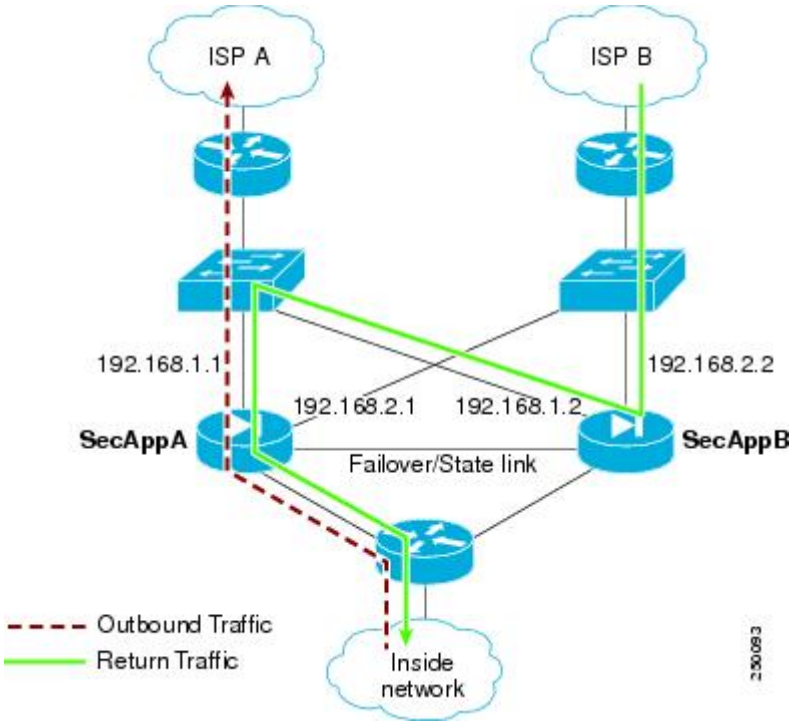
返送パケットのドロップは、非対称にルーティングされたパケットを許可することによって防ぐことができます。そのためには、それぞれの ASA の同様のインターフェイスを同じ ASR グループに割り当てます。たとえば、両方の ASA が、内部インターフェイスでは同じ内部ネットワークに接続している一方、外部インターフェイスでは別の ISP に接続しているとします。プライマリ装置で、アクティブ コンテキストの外部インターフェイスを ASR グループ 1 に割り当て、セカンダリ装置でも、アクティブ コンテキストの外部インターフェイスを同じ ASR グループ 1 に割り当てます。プライマリ装置の外部インターフ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（この場合 ASR グループ 1）内のスタンバイ コンテキスト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） この機能は、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。

次の図に、非対称にルーティングされたパケットの例を示します。

図 *13 : ASR* の例



1. アウトバウンド セッションが、アクティブな SecAppA コンテキストを持つ ASA を通過します。このパケットは、インターフェイス外の ISP-A（192.168.1.1）から送信されます。
2. 非対称ルーティングがアップストリームのどこかで設定されているため、リターン トラフィックは、アクティブな SecAppB コンテキストを持つ ASA のインターフェイス外部の ISP-B（192.168.2.2）経由で戻ります。
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。しかし、このインターフェイスは、ASR グループ 1 の一部として設定されています。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. このセッション情報は、SecAppB を持つ装置上の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。

始める前に

- 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。
- プライマリ装置およびセカンダリ装置の各アクティブ コンテキスト内でこの手順を実行します。
- コンテキスト内に ASR グループとトラフィック ゾーンの両方を設定することはできません。コンテキスト内にゾーンを設定した場合、どのコンテキストインターフェイスも ASR グループに含めることはできません。

手順

ステップ 1 プライマリ装置で、非対称にルーティングされたパケットを許可するインターフェイスを指定します。

interface *phy_if*

例：

```
primary/admin(config)# interface gigabitethernet 0/0
```

ステップ 2 インターフェイスの ASR グループ番号を設定します。

asr-group *num*

例：

```
primary/admin(config-ifc)# asr-group 1
```

num 範囲に有効な値は、1 ～ 32 です。

ステップ 3 セカンダリ装置で、非対称にルーティングされたパケットを許可するインターフェイスを指定します。

interface *phy_if*

例：

```
secondary/ctx1(config)# interface gigabitethernet 0/1
```

ステップ 4 インターフェイスの ASR グループ番号をプライマリ装置のインターフェイスに一致するように設定します。

asr-group *num*

例：

```
secondary/ctx1(config-ifc)# asr-group 1
```

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。

プライマリ装置のシステム コンフィギュレーション

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

SecAppA コンテキスト コンフィギュレーション

```
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
```

SecAppB コンテキスト コンフィギュレーション

```
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
```

フェールオーバー の管理

この項では、フェールオーバーの設定を変更する方法、ある装置から別の装置にフェールオーバーを強制実行する方法など、 フェールオーバーをイネーブルにした後に フェールオーバー装置を管理する方法について説明します。

フェールオーバーの強制実行

スタンバイ装置を強制的にアクティブにするには、次の手順を実行します。

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 スタンバイ装置で入力した場合、フェールオーバーが強制実行されます。スタンバイ装置はアクティブ装置になります。

group *group_id* を指定する場合は、指定するアクティブ/アクティブ フェールオーバー グループのスタンバイ装置でこのコマンドを入力すると、フェールオーバーが強制実行されます。スタンバイ装置はそのフェールオーバー グループのアクティブ装置になります。

- アクティブ/スタンバイ モードのスタンバイ装置の場合

  failover active

- アクティブ/アクティブ モードのスタンバイ装置の場合

  failoveractive [**group** *group_id*]

  例：

```
standby# failover active group 1
```

ステップ 2 アクティブ装置で入力した場合、フェールオーバーが強制実行されます。アクティブ装置はスタンバイ装置になります。

group *group_id* を指定する場合は、指定するフェールオーバー グループのアクティブ装置でこのコマンドを入力すると、フェールオーバーが強制実行されます。アクティブ装置はそのフェールオーバー グループのスタンバイ装置になります。

- アクティブ/スタンバイ モードのアクティブ装置の場合

  no failover active

- アクティブ/アクティブ モードのアクティブ装置の場合

  nofailoveractive [**group** *group_id*]

  例：

```
active# no failover active group 1
```

フェールオーバーのディセーブル化

1 つまたは両方の装置でフェールオーバーをディセーブルにすると、リロードするまで各装置のアクティブおよびスタンバイ状態が維持されます。アクティブ/アクティブ フェールオーバー ペアの場合、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。

フェールオーバーをディセーブルにする際、次の特性を参照してください。

- スタンバイ装置/コンテキストはスタンバイ モードのまま維持されるので、両方の装置はトラフィックの転送を開始しません（これは疑似スタンバイ状態と呼ばれます）。
- スタンバイ装置/コンテキストは、アクティブ装置/コンテキストに接続されていない場合でもそのスタンバイ IP アドレスを引き続き使用します。
- スタンバイ装置/コンテキストによる、フェールオーバー上における接続に対するリッスンは継続されます。フェールオーバーをアクティブ装置/コンテキストで再度イネーブルにすると、そのコンフィギュレーションの残りが再同期化された後に、スタンバイ装置/コンテキストが通常のスタンバイ状態に戻ります。
- スタンバイ装置で手動でフェールオーバーをイネーブルにしてアクティブ化しないでください。代わりに、フェールオーバーの強制実行 （57 ページ）を参照してください。スタンバイ装置でフェールオーバーをイネーブルにすると、MAC アドレスの競合が発生し、IPv6 トラフィックが中断される可能性があります。

- 完全にフェールオーバーをディセーブルにするには、no failover コンフィギュレーションをスタートアップ コンフィギュレーションに保存してからリロードします。

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 フェールオーバーをディセーブルにします。

no failover

ステップ 2 完全にフェールオーバーをディセーブルにするには、コンフィギュレーションを保存してをリロードします。

write memory

reload

障害が発生した装置の復元

障害が発生した装置を障害のない状態に復元するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 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。

- アクティブ/スタンバイ モードの場合

  failoverreset

- アクティブ/アクティブ モードの場合

  failoverreset [**group** *group_id*]

  例：

```
ciscoasa(config)# failover reset group 1
```

障害が発生した装置を障害のない状態に復元しても、その装置が自動的にアクティブになるわけではありません。復元された装置は、（強制または自然な形での）フェールオーバー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。例外は、フェールオーバー グループ

（アクティブ/アクティブ モードのみ）にフェールオーバー プリエンプションが設定されている場合です。 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である場合、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。

group *group_id* を指定した場合、このコマンドは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します。

ステップ 2 （アクティブ/アクティブ モードのみ）フェールオーバーをフェールオーバー グループ レベルで復元するには次を行います。

a) [System] で、[Monitoring] > [Failover] > [Failover Group #] を選択します。# は、制御するフェールオーバー グループの番号です。

b) [Reset Failover] をクリックします。

コンフィギュレーションの再同期

アクティブ装置に write standby コマンドを入力すると、スタンバイ装置で実行コンフィギュレーションが削除され（アクティブ装置との通信に使用するフェールオーバー コマンドを除く）、アクティブ装置のコンフィギュレーション全体がスタンバイ装置に送信されます。

マルチ コンテキスト モードの場合、システム実行スペースに **write standby** コマンドを入力すると、すべてのコンテキストが複製されます。あるコンテキスト内で **write standby** コマンドを入力すると、コマンドはそのコンテキスト コンフィギュレーションだけを複製します。

複製されたコマンドは、実行コンフィギュレーションに保存されます。

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。

手順

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 アクティブ装置で次のコマンドを入力し、フェールオーバーを強制実行します。

アクティブ/スタンバイ モード

ciscoasa(config)# **nofailoveractive**

アクティブ/アクティブ モード

ciscoasa(config)# **nofailoveractivegroup** *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、新しくアクティブになった装置で次のコマンドを入力すると、装置をアクティブ ステータスに復元できます。

アクティブ/スタンバイ モード

ciscoasa(config)# **nofailoveractive**

アクティブ/アクティブ モード

ciscoasa(config)# **failoveractivegroup** *group_id*

（注） ASA インターフェイスの 1 つがダウンしたとき、フェールオーバーの観点からは、これも装置の問題と見なされます。インターフェイスの 1 つがダウンしていることを ASA が検出した場合は、インターフェイスのホールド時間を待たずに、フェールオーバーがただちに行われます。インターフェイスのホールド時間が有効であるのは、ASA が自身のステータスを OK と見なしているときだけです（ピアから hello パケットを受信していなくても）。インターフェイスのホールド時間をシミュレートするには、ピアが他のピアから hello パケットを受信するのを停止させるために、スイッチ上で VLAN をシャットダウンします。

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。

コマンドの送信

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。

手順

ステップ 1 マルチ コンテキスト モードの場合は、**changeto context***name* 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。

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。

ciscoasa(config)# **failoverexec** {**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。

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

```
ciscoasa(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。

```
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。**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。

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

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

ciscoasa(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ぐためには、フェールオーバー リンクの暗号化をイネーブルに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、**noconfirm** オプションを使用する必要があります。たとえば、mate をリロードするには、次を入力します。

  failover exec mate reload noconfirm

モニタリング フェールオーバー

このセクションでは、 フェールオーバー ステータスをモニタできます。

フェールオーバー メッセージ

フェールオーバーが発生すると、両方の ASA がシステム メッセージを送信します。

フェールオーバーの syslog メッセージ

ASA は、深刻な状況を表すプライオリティ レベル 2 のフェールオーバーについて、複数の syslog メッセージを発行します。これらのメッセージを表示するには、『syslog メッセージ ガイド』を参照してください。フェールオーバーに関連付けられているメッセージ ID の範囲は次のとおりです：101xxx、102xxx、103xxx、104xxx、105xxx、210xxx、311xxx、709xxx、727xxx。たとえば、105032 および 105043 はフェールオーバー リンクとの問題を示しています。

（注） フェールオーバーの最中に、ASAは論理的にシャットダウンした後、インターフェイスを起動し、syslog メッセージ 411001 および 411002 を生成します。これは通常のアクティビティです。

フェールオーバー デバッグ メッセージ

デバッグ メッセージを表示するには、**debug fover** コマンドを入力します。詳細については、コマンド リファレンスを参照してください。

（注） CPUプロセスではデバッグ出力に高プライオリティが割り当てられているため、デバッグ出力を行うとシステム パフォーマンスに大きく影響することがあります。このため、**debug fover** コマンドは、特定の問題に対するトラブルシューティングや、Cisco TAC とのトラブルシューティング セッションに限定して使用してください。

SNMP のフェールオーバー トラップ

フェールオーバーに対する SNMP syslog トラップを受信するには、SNMP トラップを SNMP 管理ステーションに送信するように SNMP エージェントを設定し、syslog ホストを定義し、お使いの SNMP 管理ステーションに Cisco syslog MIB をコンパイルします。

フェールオーバー ステータスのモニタリング

フェールオーバー ステータスをモニタするには、次のいずれかのコマンドを入力します。

- **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。

- **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。

- **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。

フェールオーバーの履歴

機能名	リリース	機能情報
アクティブ/スタンバイ フェールオーバー	7.0(1)	この機能が導入されました。
アクティブ/アクティブ フェールオーバー	7.0(1)	この機能が導入されました。
フェールオーバー キーの 16 進数値サポート	7.0(4)	フェールオーバー リンクの暗号化用に16進数値が指定できるようになりました。 **failover key hex** コマンドが変更されました。
フェールオーバー キーのマスター パスフレーズのサポート	8.3(1)	フェールオーバー キーが、実行コンフィギュレーションとスタートアップ コンフィギュレーションの共有キーを暗号化するマスターパスフレーズをサポートするようになりました。一方のASAから他方に共有秘密をコピーする場合、たとえば、**more system:running-config** コマンドを使用して、正常に暗号化共有キーをコピーして貼り付けることができます。 （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。 次のコマンドが変更されました。**failover key** [**0** | **8**]
フェールオーバーにIPv6のサポートが追加されました。	8.2(2)	次のコマンドが変更されました。**failover interface ip**、**show failover**、**ipv6 address**、**show monitor-interface**

機能名	リリース	機能情報
「同時」ブートアップ中のフェールオーバー グループのユニットの設定の変更。	9.0(1)	以前のバージョンのソフトウェアでは「同時」ブートアップが許可されていたため、フェールオーバー グループを優先ユニットでアクティブにする **preempt** コマンドは必要ありませんでした。しかし、この機能は、両方のフェールオーバー グループが最初に起動するユニットでアクティブになるように変更されました。
フェールオーバー リンクおよびステート リンクの通信を暗号化する IPsec LAN-to-LAN トンネルのサポート	9.1(2)	フェールオーバー キーに独自の暗号化を使用する代わりに（**failover key** コマンド）、フェールオーバー リンクおよびステート リンクの暗号化に IPsec LAN-to-LAN トンネルが使用できるようになりました。 （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。 **failover ipsec pre-shared-key**、**show vpn-sessiondb** の各コマンドが導入または変更されました。
ハードウェア モジュールのヘルス モニタリングの無効化	9.3(1)	ASA はデフォルトで、インストール済みハードウェア モジュール（ASA FirePOWER モジュールなど）のヘルス モニタリングを行います。特定のハードウェア モジュールの障害によってフェールオーバーをトリガーすることが望ましくない場合は、モジュールのモニタリングをディセーブルにできます。 **monitor-interface service-module** コマンドが変更されました。

機能名	リリース	機能情報
フェールオーバーペアのスタンバイ装置またはスタンバイ コンテキストのコンフィギュレーション変更のロック	9.3(2)	通常のコンフィギュレーションの同期を除いてスタンバイ装置上で変更ができないように、スタンバイ装置（アクティブ/スタンバイ フェールオーバー）またはスタンバイ コンテキスト（アクティブ/アクティブ フェールオーバー）のコンフィギュレーション変更をロックできるようになりました。 **failover standby config-lock** コマンドが導入されました。
ASA 5506H のフェールオーバー リンクとして、管理 1/1 インターフェイスを使用できるようになりました。	9.5(1)	管理 1/1 インターフェイスは、ASA 5506H に限りフェールオーバー リンクとして設定できるようになりました。この機能により、デバイスの他のインターフェイスをデータインターフェイスとして使用できます。この機能を使用した場合、ASA FirePOWER モジュールは使用できません。このモジュールでは管理 1/1 インターフェイスを通常の管理インターフェイスとして維持することが必須です。 次のコマンドが変更されました。**failover lan interface**、**failover link**
キャリア グレード NAT の強化は、フェールオーバーおよび ASA クラスタリングでサポートされます。	9.5(2)	キャリア グレードまたは大規模 PAT では、NAT で 1 度に 1 つのポート変換を割り当てるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。この機能は、フェールオーバーおよび ASA クラスタの導入でサポートされます。 次のコマンドが変更されました。**show local-host**

機能名	リリース	機能情報
アクティブ/スタンバイ フェールオーバーを使用するとき、AnyConnectからのダイナミック ACL の同期時間が改善されました。	9.6(2)	フェールオーバー ペアで AnyConnect を使用するとき、関連付けられているダイナミック ACL（dACL）のスタンバイ ユニットへの同期時間が改善されました。以前は、大規模な dACL の場合、スタンバイユニットが可用性の高いバックアップを提供するのではなく同期作業で忙しい間は、同期時間が長時間に及ぶことがありました。 変更されたコマンドはありません。
マルチ コンテキスト モードのAnyConnect接続のステートフル フェールオーバー	9.6(2)	マルチ コンテキスト モードでAnyConnect接続のステートフル フェールオーバーがサポートされました。 変更されたコマンドはありません。
より迅速に検出を行うために、インターフェイスのリンク ステート モニタリングを設定できるようになりました。	9.7(1)	デフォルトでは、フェールオーバーペアの ASA は、500 ミリ秒ごとにインターフェイスのリンク ステートをチェックします。ポーリングの間隔を 300 ミリ秒から 799 ミリ秒の間で設定できるようになりました。たとえば、ポーリング時間を 300 ミリ秒に設定すると、ASAはインターフェイス障害やトリガーのフェールオーバーをより迅速に検出できます。 次のコマンドが導入されました。 **failover polltime link-state**
FirePOWER 9300 および 4100 でのアクティブ/スタンバイ フェールオーバー ヘルス モニタリングで、双方向フォワーディング検出（BFD）がサポートされました。	9.7(1)	FirePOWER 9300 および 4100 上のアクティブ/スタンバイ ペアの 2 つのユニット間のフェールオーバー ヘルス チェックに対して、双方向フォワーディング検出（BFD）を有効にできるようになりました。ヘルス チェックに BFD を使用すると、デフォルトのヘルス チェックより信頼性が高まり、CPUの使用を抑えることができます。 次のコマンドが導入されました。 **failover health-check bfd**