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、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

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。アクティブユニットおよびインターフェイスのヘルスがモニターされて、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、一方のデバイスがアクティブユニットとしてトラフィックを通過させます。もう一方のデバイスはスタンバイユニットとなり、ア

クティブにトラフィックを通過させません。フェールオーバーが発生すると、アクティブユニットからスタンバイユニットにフェールオーバーし、そのスタンバイユニット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。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。

  Firepower 9300 の場合、高可用性は同じタイプのモジュール間でのみサポートされていますが、2 台のシャーシにモジュールを混在させることができます。たとえば、各シャーシには SM-56、SM-48、および SM-40 があります。SM-56 モジュール間、SM-48 モジュール間、および SM-40 モジュール間にハイアベイラビリティペアを作成できます。

- インターフェイスの数とタイプが同じであること。

  プラットフォーム モードと Firepower 4100/9300 シャーシFirepower 2100 では、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が FXOS で同一に事前構成されている必要があります。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 でそのインターフェイスを変更してから、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。

- 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）。
- 単一モードの場合：同じファイアウォール モードにあること（ルーテッドまたはトランスペアレント）。

  マルチコンテキスト モードでは、ファイアウォール モードはコンテキスト レベルで設定され、混合モードを使用できます。
- 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 セキュア クライアント イメージがあること。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。
- （Firepower 4100/9300）同じフロー オフロード モードを使用し、両方とも有効または無効になっている。

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。シスコでは、フェールオーバーリンクまたはステートフルフェールオーバーリンク内の2つのデバイス間で同じインターフェイスを使用することを推奨しています。たとえば、フェールオーバー リンクで、デバイス 1 で eth0 を使用していた場合は、デバイス 2 でも同じインターフェイス（eth0）を使用します。

⚠

注意 フェールオーバー リンクおよびステート 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ー名、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、サブインターフェイス、またはEtherChannel）はいずれ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）。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。

ASA は、ユーザー 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をサポートしていません。同じ親の別のサブインターフェイスをフェールオーバーリンクやデータのために使用することもできません。

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。
- Firepower 4100/9300：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。
- リンクのサイジングについては、次のガイドラインを参照してください。

表 *1:* フェールオーバー リンクのサイズ

モデル	結合フェールオーバー リンクとステート リンクのインターフェイス サイズ
Firepower 1010	1 Gbps
Firepower 1100	1 Gbps
Cisco Secure Firewall 1200	1 Gbps
Cisco Secure Firewall 3100	Cisco Secure Firewall 3105：1 Gbps Cisco Secure Firewall 3110：1 Gbps Cisco Secure Firewall 3120：1 Gbps Cisco Secure Firewall 3130：10 Gbps Cisco Secure Firewall 3140：10 Gbps
Firepower 4100	10 Gbps
Cisco Secure Firewall 4200	10 Gbps
Firepower 9300	10 Gbps

交替頻度は、ユニットのホールド時間と同じです（**failover polltime unit** コマンド）。

（注） 設定が大きく、ユニットのホールド時間が短い場合、メンバーインターフェイスを交互に切り替えると、セカンダリユニットの参加/再参加を防止できます。この場合、セカンダリユニットが参加するまで、メンバーインターフェイスの 1 つを無効にします。

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）に他のデバイス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ユニットを直接接続する。外部スイッチは必要ありません。

ユニット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ユニット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。

フェールオーバー リンクの共有

インターフェイスを節約するための最適な方法はフェールオーバー リンクを共有することです。ただし、大規模な構成とトラフィックの多いネットワークを使用する場合は、ステート リンクとフェールオーバー リンクに専用のインターフェイスを使用すること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、または EtherChannel）を使用できます。専用のステートリンクの要件についてはフェールオーバー リンクのインターフェイス （4 ページ）、ステートリンクの接続についてはフェールオーバー リンクの接続 （6 ページ）を参照してください。

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

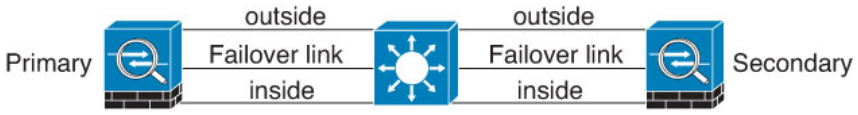
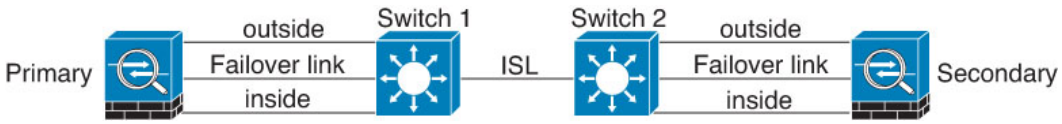


図 *2:* 2 つのスイッチを使用した接続：非推奨



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

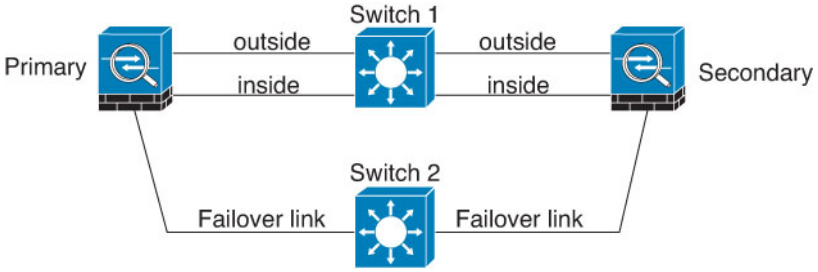
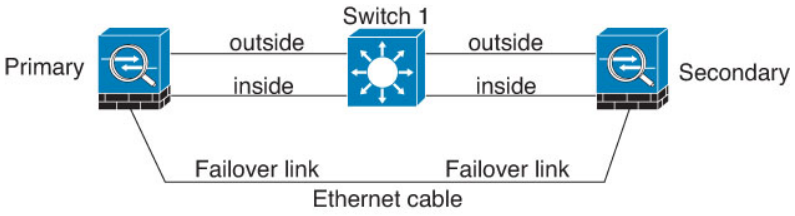


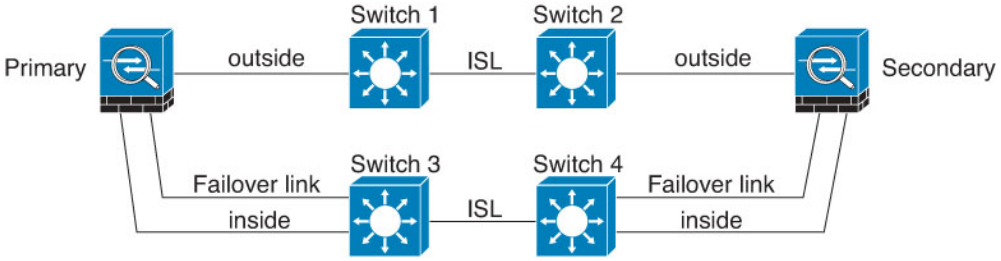
図 *4:* ケーブルを使用した接続



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 スイッチを使用した接続



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にアクティブ IP アドレスとスタンバイ IP アドレスを指定できます。通常、フェールオーバーが発生すると、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 アドレスのペアリングの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） 推奨されてはいますが、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 アドレスがなければ、アクティブ装置はネットワーク テストを実行してスタンバイ インターフェイスの状態を確認することはできません。できることはリンク ステートの追跡のみです。また、管理目的でそのインターフェイス上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。

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 アドレスの使用方法については、次を参照してください。

1. アクティブ装置は常に、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. アクティブ装置がフェールオーバーすると、スタンバイ装置は障害が発生した装置の 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. 障害が発生した装置がオンライン状態に戻ると、スタンバイ状態になり、スタンバイの 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起動した場合、プライマリ装置の MAC アドレスを認識していないため、セカンダリ装置がアクティブ装置になり、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。このため、ネットワーク トラフィックが中断することがあります。同様に、新しいハードウェアでプライマリ装置をスワップ アウトすると新しい MAC アドレスが使用されます。

フェールオーバーを無効にし、フェールオーバー設定を無効状態に設定した場合は、フェールオーバーを手動で再開するか、デバイスを再起動する必要があります。デバイスを再起動するのではなく、コマンド **failover reset** を使用してフェールオーバーを再開することをお勧めします。フェールオーバー設定が無効なスタンバイ装置をリロードすると、スタンバイ装置はアクティブ装置として起動し、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。これにより、IP アドレスが重複し、ネットワークトラフィックが中断されます。**failover reset** コマンドを使用してフェールオーバーを有効にし、トラフィックフローを復元します。

（注） スタンドアロンデバイスでフェールオーバーを有効にすると、データインターフェイスがフェールオーバーのネゴシエーション状態でダウンし、トラフィックが中断されます。

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。セカンダリ装置がプライマリ装置より先にオンラインになった場合でも、セカンダリ装置がアクティブ装置であるときに正しい MAC アドレスを使用するように、プライマリ装置とセカンダリ装置の両方で仮想MACアドレスを設定することをお勧めします。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。MACアドレスが変わった場合、ASAはスタティック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 アドレスの使用方法については、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 のコンテキストにある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。また、MACアドレスが競合している場合などには、必要に応じて手動でMACアドレスを設定できます。
2. 各装置は、アクティブ 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、およびスタンバイ フェールオーバー グループのスタンバイアドレスを使用します。たとえば、プライマリ装置はフェールオーバーグループ 1 に対してアクティブであるため、フェールオーバーグループ 1 のコンテキストに対してアクティブなアドレスを使用します。また、スタンバイアドレスを使用するフェールオーバーグループ 2 のコンテキストに対してはスタンバイです。
3. ある装置がフェールオーバーすると、別の装置が障害が発生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. 障害が発生した装置がオンライン状態に戻り、プリエンプトオプションを有効にすると、フェールオーバーグループが再開されます。

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 つの方法だけ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、使用される MAC アドレスは多くの変数によって決まるため、予測できないことがあります。手動の方法には、次で説明されている自動生成方法に加えて、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の場合は、フェールオーバー グループ モード **mac address** コマンドが含まれます。

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対して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 を設定できます。また、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）。非共有インターフェイスの場合、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できます（アクティブ/アクティブモードでは、すべてのインターフェイスのMACアドレスが自動生成されます）。

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。

フェールオーバーでの MAC アドレス テーブルの更新

フェールオーバー時、新しいアクティブ デバイスとして指定されたデバイスは、MAC テーブル内の各 MAC アドレス エントリに対してマルチキャスト パケットを生成し、それをすべてのブリッジ グループ インターフェイスに送信します。このアクションにより、ブリッジグループ内の上流スイッチは、新しいアクティブデバイスのインターフェイスでルーティングテーブルを更新し、正確なトラフィック転送を保証します。

マルチキャストパケットの生成および上流スイッチのルーティングテーブルを更新するのにかかる時間は、MACアドレステーブルのエントリ数とブリッジ グループ インターフェイスの数によって異なります。フェールオーバーイベント中に発生した遅延に関連する統計を表示するには、コマンド **show failover statistics state-switch-delay** を使用します。

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。

ステートフル フェールオーバー

ステートフルフェールオーバーが有効な場合、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。

サポートされる機能

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

- NAT 変換テーブル
- TCP 接続状態と UDP 接続状態（）。その他の IP プロトコル タイプと ICMP は、新しいパケットが到着すると新しいアクティブデバイスで確立されるため、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 複製が有効でない場合）。
- HTTP 接続状態（HTTP 複製が有効の場合）：デフォルトでは、ステートフル フェールオーバーが有効のときには、ASA は HTTP セッション情報を複製しません。HTTP レプリケーションを有効にすることをお勧めします。
- 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順序が不正なパケットを破棄します。
- ARP テーブル
- レイヤ 2 ブリッジ テーブル（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 セッションおよびピン 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有効になります。
- スタティック/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 OSPF や EIGRP などのダイナミック ルーティング プロトコルに参加します。そのため、アクティブ装置上のダイナミック ルーティング プロトコルを介して学習されたルートは、スタンバイ装置のルーティング情報ベース（RIB）テーブルに保持されます。フェールオーバーイベントが発生した場合、最初はアクティブなセカンダリ装置にプライマリ装置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切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、インターフェイス上に構成された DHCP サーバは DHCP クライアントにアドレスを付与する前に ping を送信してアドレスが使用されていないことを確認するため、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 には関係ありません。
- 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 クライアントでは Cisco Call Manager との接続が解除されます。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 のエンド 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。
- すべての接続から、確立された接続だけがスタンバイ デバイスに複製されます。

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。
- 一部のクライアントレス SSL VPN 機能。
  - スマート トンネル
  - ポートフォワーディング
  - プラグイン
  - Java アプレット
  - IPv6 クライアントレスまたは セキュアクライアント 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場合は、フェールオーバーに関して特別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STPに参加し続けます。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。

フェールオーバーのヘルス モニタリング

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 ヘルスをモニターします。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。

装置のヘルス モニターリング

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）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 リンクは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。

ハートビートモジュールの冗長性

HAの各ユニットは、クラスタ制御リンクを介してブロードキャスト キープアライブ ハートビートパケットを定期的に送信します。コントロールプレーンがトラフィックの処理でビジー状態になっていると、ハートビートパケットがピアに届かなかったり、CPUの過負荷が原因でピアがハートビートパケットを処理しないことがあります。設定可能なタイムアウト期間内にピアがキープアライブステータスを伝えられない場合、誤ったフェールオーバーまたはスプリットブレインシナリオが発生します。

データプレーンのハートビートモジュールは、コントロールプレーンでのトラフィックの輻輳による誤ったフェールオーバーまたはスプリットブレインの発生を回避するために役立ちます。

- 追加のハートビートモジュールは、コントロール プレーン モジュールと同様に機能しますが、データ プレーン トランスポート インフラストラクチャを使用してハートビートメッセージを送受信します。
- ピアがデータプレーンでハートビートパケットを受信すると、カウンタが増加します。
- コントロールプレーンでのハートビート転送が失敗した場合、ノードはデータプレーンのハートビートカウンタをチェックします。カウンタが増加している場合、ピアは稼働しており、この状況ではクラスタはフェールオーバーを実行しません。

（注）
- HA が有効な場合、追加のハートビートモジュールは常にデフォルトで有効になっています。データプレーンの追加のハートビートモジュールのポーリング間隔を設定する必要はありません。このモジュールは、コントロールプレーンに設定したものと同じハートビート間隔を使用します。
- この機能は、バージョン 7.3 では使用できません。

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監視できます（マルチコンテキスト 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ーする必要があります。たとえば、マルチコンテキストモードでは、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による利点を得ることができます）。

ユニットは、モニター対象のインターフェイス上で 15 秒間 hello メッセージを受信しなかった場合に（デフォルト）、インターフェイステストを実行します。（この時間を変更するには、**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Criteria]** > **[Failover Poll Times]** を参照してください。）1 つのインターフェイスに対するインターフェイステストのいずれかが失敗したものの、他のユニット上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は、そのインターフェイスに障害があるものと見なされ、ASAはテストの実行を停止します。

障害が発生したインターフェイスの数に対して定義したしきい値が満たされ（**[設定（Configuration）]**> **[デバイス管理（Device Management）]** > **[ハイアベイラビリティとスケーラビリティ（High Availability and Scalability）]** > **[フェールオーバー（Failover）]** > **[基準（Criteria）]** > **[インターフェイスポリシー（Interface Policy）]** を参照）、さらに、アクティブユニットでスタンバイ装置よりも多くの障害が発生した場合は、フェールオーバーが発生します。両方のユニット上のインターフェイスに障害が発生した場合は、両方のインターフェイスが「未知」状態になり、フェールオーバー インターフェイス ポリシーで定義されているフェールオーバー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。

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。各テストの時間は約1.5秒（デフォルト）、またはフェールオーバー インターフェイスの保留時間の 1/16 （**[設定（Configuration）] > [デバイス管理（Device Management）] > [ハイアベイラビリティとスケーラビリティ（High Availability and Scalability）] > [フェールオーバー（Failover）] > [基準（Criteria）] > [フェールオーバーポーリング時間（Failover Poll Times）]**を参照）。

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、テストが停止したと見なします。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 アクティビティ テスト：ネットワークの受信アクティビティのテストです。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。テスト中にユニットが適切なパケットを受信すると、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。両方の装置がトラフィックを受信した場合、テストは停止します。どちらか一方のユニット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ていないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、ASA は ARP テストを開始します。

3. ARP テスト：ARP が正しく応答するかどうかをテストします。各ユニットは、ARP テーブル内の最新のエントリの IP アドレスに対して単一の ARP 要求を送信します。ユニットがテスト中に ARP 応答またはその他のネットワーク トラフィックを受信する場合、インターフェイスは動作していると見なされます。ユニットが ARP 応答を受信しない場合、ASAは、ARP テーブル内の「次の」エントリの IP アドレスに対して単一の ARP 要求を送信します。ユニットがテスト中に ARP 応答またはその他のネットワーク トラフィックを受信する場合、インターフェイスは動作していると見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニット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ていないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、ASA はブートストラップ ping テストを開始します。

4. ブロードキャスト Ping テスト：ping 応答が正しいかどうかをテストします。各ユニットがブロードキャスト ping を送信し、受信したすべてのパケットをカウントします。パケットはテスト中にパケットを受信すると、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。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニット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ていないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信しない場合、ARP テストを使用してテストが再開さ

れます。両方の装置が ARP およびブロードキャスト ping テストからトラフィックを受信し続けない場合、これらのテストは永久に実行し続けます。

インターフェイス ステータス

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

Firepower ハイアベイラビリティペアでは、次のイベントでフェールオーバーがトリガーされます。

- アクティブユニットの 50% を超える Snort インスタンスがダウンした場合
- アクティブユニットのディスク容量使用率が 90% を超えた場合
- アクティブユニットで **no failover active** コマンドが実行された場合、またはスタンバイユニットで **failover active** コマンドが実行された場合
- アクティブユニットで障害が発生したインターフェイスの数がスタンバイユニットよりも多くなった場合
- アクティブデバイスのインターフェイス障害が設定されたしきい値を超えた場合

  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。デフォルト値を変更するには、フェールオーバーが発生するしきい値として、障害が発生したインターフェイスの数またはモニター対象インターフェイスの割合を設定します。アクティブデバイスでしきい値を超えると、フェールオーバーが発生します。スタンバイデバイスでしきい値を超えると、ユニットが **Fail** 状態に移行します。

  デフォルトのフェールオーバー条件を変更するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

表 *2:*

コマンド	目的
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	デフォルトのフェールオーバー基準を変更します。 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。

（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 *3: ASA*

フェールオーバー条件	最小	デフォルト	最大数
アクティブユニットの電源の喪失、ハードウェアのダウン、ソフトウェアのリロードまたはクラッシュにより、モニター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メッセージを受信しなくなる。	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 ユニットの 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デリ指定に関係なく、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。

ファイルの複製

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。

- セキュア クライアント イメージ
- CSD イメージ
- セキュア クライアント 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 セキュア クライアント プロファイルのキャッシュ済みファイルが使用されます。セキュア 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

コマンドの複製

起動した後、アクティブユニットで入力したコマンドはただちにスタンバイユニットに複製されます。コマンドを複製する場合、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変更は、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変更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。

- 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** を除く）
- **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。

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

設定同期の最適化

デバイスが一時停止後に再起動するか、フェールーバーを再開する場合、参加するデバイスは実行中の設定をクリアします。次に、アクティブデバイスが、設定全体を参加デバイスに送信して完全に同期します。アクティブデバイスの設定が大規模な場合、このプロセスには数分かかることがあります。

設定同期最適化機能により、設定ハッシュ値を交換して、参加ユニットとアクティブユニットの設定を比較できます。アクティブデバイスと参加デバイスの両方で計算されたハッシュが一致する場合、参加デバイスは完全な設定同期をスキップし、フェールオーバー設定に再参加します。 この機能により、さらに迅速なピアリングが可能になり、メンテナンスウィンドウとアップグレード時間が短縮されます。

設定同期の最適化のガイドラインと制限事項

- 設定同期最適化機能は、デフォルトで有効になっています。
- ASA のマルチコンテキストモードは、完全な設定同期中にコンテキストの順序を共有することによって設定同期最適化をサポートし、後続のノード再参加中にコンテキストの順序を比較できるようにします。
- パスフレーズとフェールオーバー IPsec キーを設定すると、アクティブユニットとスタンバイユニットで計算されたハッシュ値が異なるため、設定同期の最適化で効果を得られません。
- ダイナミック ACL または SNMPv3 を使用してデバイスを設定すると、設定同期最適化は効果を発揮しません。
- アクティブデバイスは、デフォルトの動作として、LAN リンクのフラッピングによって完全な設定を同期します。アクティブデバイスとスタンバイデバイス間のフェールオーバーフラッピングの間、設定同期最適化はトリガーされず、デバイスによって完全な設定同期が実行されます。
- フェールオーバー設定が中断やアクティブデバイスとスタンバイデバイス間のネットワーク通信の切断から復旧する際に、設定同期最適化がトリガーされます。

設定同期の監視

設定同期最適化機能が有効になっている場合、syslog メッセージが生成され、アクティブユニットと参加ユニットで計算されたハッシュ値が一致するか、一致しないか、または操作がタイムアウトになったかどうかが表示されます。また、ハッシュ要求を送信してからハッシュ応答を取得して比較するまでの経過時間も表示されます。

設定同期の最適化をモニタリングするには、次のコマンドを使用します。これらのコマンドは、[ツール（Tools）] > [コマンドラインインターフェイス（Command Line Interface）] で実行できます。

- **show failover config-sync checksum**

  デバイスのステータスとチェックサムに関する情報を表示します。

- **show failover config-sync configuration**

  デバイスの設定とチェックサムに関する情報を表示します。

- **show failover config-sync status**

  設定同期最適化機能のステータスを表示します。

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。ただし、セカンダリ装置の設定を保持するために、障害が発生した装置を交換する前に、スタンバイ装置をプライマリに設定する必要があります。

（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つの装置の主な相違点は、どちらの装置がアクティブでどちらの装置がスタンバイであるか、つまりどちらの IP アドレスを使用し、どちらの装置で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。
- プライマリ装置のMACアドレスは常にアクティブIPアドレスと組み合わされます。このルールの例外は、セカンダリ装置がアクティブになり、フェールオーバー リンク経由でプライマリ装置の 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 *4:* フェールオーバー イベント

障害イベント	ポリシー	アクティブユニットのアクション	スタンバイユニットのアクション	注記
アクティブユニットが故障(電源またはハードウェア)	フェールオーバー	該当なし	アクティブになる アクティブを障害としてマークする	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メッセージが受信されることはありません。
以前にアクティブだったユニットが復旧	フェールオーバーなし	スタンバイになる	なし	なし。
スタンバイユニットが故障(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	該当なし	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。
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	アクティブになる 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 フェールオーバーリンクに故障とマークする	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	なし	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。

障害イベント	ポリシー	アクティブユニットのアクション	スタンバイユニットのアクション	注記
しきい値を超えたアクティブユニットでインターフェイスに障害が発生	フェールオーバー	アクティブを障害としてマークする	アクティブになる	なし。
しきい値を超えたスタンバイユニットでインターフェイスに障害が発生	フェールオーバーなし	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の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、プライマリユニット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 はプライマリユニット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 はセカンダリユニット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 *5:* フェールオーバー イベント

障害イベント	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	注記
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	スタンバイになる 故障とマークする	アクティブになる アクティブを障害としてマークする	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	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	なし	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。

障害イベント	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	注記
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。
ステート リンクの障害	フェールオーバーなし	なし	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	適用対象外	適用対象外	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

ほとんどのモデルでは、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 仮想	ASAv のフェールオーバー ライセンスを参照してください。
Firepower 1010	両方のユニットの Security Plus ライセンス。Firepower 1010 のフェールオーバー ライセンスを参照してください。
Firepower 1100	Firepower 1100 のフェールオーバー ライセンスを参照してください。
Cisco Secure Firewall 1210/1220	「Secure Firewall 1210/1220 のフェールオーバー ライセンス」を参照してください。
Secure Firewall 1230/1240/1250	Secure Firewall 1230/1240/1250 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
Cisco Secure Firewall 3100/4200	Secure Firewall 3100 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	「Firepower 4100/9300のフェールオーバーライセンス」を参照してください。
ISA 3000	両方のユニットの Security Plus 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。

（注） 有効な永続キーが必要です。まれに、ISA 3000 で、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。

モデルのサポート

- Firepower 1010 および Cisco Secure Firewall 1210/1220：
  - フェールオーバーを使用する場合は、スイッチポート機能を使用しないでください。スイッチポートはハードウェアで動作するため、アクティブユニットとスタンバイユニットの両方でトラフィックを通過させ続けます。フェールオーバーは、トラフィックがスタンバイユニットを通過するのを防ぐように設計されていますが、この機能はスイッチポートには拡張されていません。通常の フェールオーバー のネットワーク設定では、両方のユニットのアクティブなスイッチ ポートがネットワーク ループにつながります。スイッチング機能には外部スイッチを使用することをお勧めします。VLAN インターフェイスはフェールオーバーによってモニタできますが、スイッチ ポートはモニタできません。理論的には、1 つのスイッチ ポートを VLAN に配置して、フェールオーバー を正常に使用することができますが、代わりに物理ファイアウォール インターフェイスを使用する設定の方が簡単です。
  - ファイアウォール インターフェイスはフェールオーバー リンクとしてのみ使用できます。

- FirePOWER 9300：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 ASA 仮想 では、レイヤ 2 接続が必要なため、通常の フェールオーバーはサポートされません。代わりに、パブリック クラウドでのハイ アベイラビリティのためのフェールオーバーを参照してください。

ハイアベイラビリティを実現するための ASA 仮想 のフェールオーバー

ASA 仮想 を使用してフェールオーバーペアを作成する場合は、データインターフェイスを各 ASA 仮想 に同じ順序で追加する必要があります。完全に同じインターフェイスが異なる順序で各 ASA 仮想 に追加されると、ASA 仮想 コンソールにエラーが表示されることがあります。また、フェールオーバー機能にも影響が出ることがあります。

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 ポートが、トポロジの変化を検出すると 30 ～ 50 秒間ブロッキング状態になる可能性があります。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、スイッチで STP PortFast 機能を有効にすることができます。

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

  この回避策は、ルーテッド モード インターフェイスとブリッジ グループ インターフェイスの両方に接続された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 STP に参加し続けます。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。

- 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ー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 を使用すれば、IPsec トンネルが不要になります。
- 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直後に、syslog メッセージの送信元アドレスが数秒間フェールオーバー インターフェイス アドレスになります。
- （フェールオーバー中に）コンバージェンスを向上させるには、どの設定やインスタンスにも関連付けられていない HA ペアのインターフェイスをシャットダウンする必要があります。
- 評価モードでフェールオーバー暗号化を設定すると、システムは暗号化に DES を使用します。エクスポート準拠アカウントを使用してデバイスを登録すると、デバイスはリブート後に AES を使用します。したがって、アップグレードのインストール後など、何らかの理由でシステムがリブートすると、ピアは通信できなくなり、両方のユニットがアクティブユニットになります。デバイスを登録するまで、暗号化を設定しないことを推奨します。評価モードで暗号化を設定する場合は、デバイスを登録する前に暗号化を削除することを推奨します。
- フェールオーバーで SNMPv3 を使用する場合、フェールオーバーユニットを交換すると、SNMPv3 ユーザは新しいユニットにレプリケートされません。ユーザを新しいユニットに強制的にレプリケートするには、SNMPv3 ユーザをアクティブユニットに再度追加する必要があります。または、新しいユニットにユーザを直接追加できます。アクティブユニットで **snmp-server user** *username group-name* **v3** コマンドを入力するか、暗号化されていない形式の *priv-password* オプションと *auth-password* オプションを使用してスタンバイユニットに直接入力することにより、各ユーザを再設定します。
- デバイスは、SNMP クライアントのエンジンデータをピアと共有しません。
- 非常に多数のアクセスコントロールルールと NAT ルールがある場合、設定のサイズによって効率的な設定のレプリケーションが妨げられる可能性があり、その結果、スタンバイユニットがスタンバイ準備完了状態に達するまでの時間が長くなります。これは、コンソールまたは SSH セッションを介したレプリケーション中にスタンバイユニットに接続する機能にも影響を与える可能性があります。設定のレプリケーションのパフォーマンスを向上させるには、**asp rule-engine transactional-commit access-group** および **asp rule-engine transactional-commit nat** コマンドを使用して、アクセスルールと NAT の両方でトランザクションコミットを有効にします。
- スタンバイロールに移行する フェールオーバー ペアのユニットは、アクティブユニットとクロックを同期します。

  例：

```
firepower#show clock
01:00:52 UTC Mar 1 2022

...
01:01:18 UTC Mar 1 2022 <======= Incorrect (previous) clock
Cold Standby               Sync Config               Detected an Active mate

19:38:21 UTC Apr 9 2022 <======= Updated clock
Sync Config                Sync File System          Detected an Active mate
...
firepower/sec/stby#show clock
19:38:40 UTC Apr 9 2022
```

- フェールオーバーのユニットは、クロックを動的に同期しません。同期が行われるときのイベントの例を次に示します。
  - 新しい フェールオーバー ペアが作成される。
  - フェールオーバー が中断されて再作成される。
  - フェールオーバーリンクを介した通信が中断され、再確立される。
  - 、フェールオーバーステータスが CLI で手動で変更された。
- フェールオーバー を有効にすると、すべてのルートが強制的に削除され、フェールオーバーの進行がアクティブ状態に変わった後に再度追加されます。このフェーズ中に接続が失われる可能性があります。
- スタンドアロンデバイスでフェールオーバーを有効にすると、データインターフェイスがフェールオーバーのネゴシエーション状態でダウンし、トラフィックが中断されます。
- フェールオーバー設定では、一般にポート53を使用する短時間の接続はすぐに閉じられ、それらの接続がアクティブからスタンバイに転送または同期されることはありません。そのため、両方の フェールオーバー デバイスの接続数に違いが生じる可能性があります。これは、短時間の接続の予期される動作です。長時間（たとえば、30 ～ 60 秒を超える）の接続の比較を試みることができます。
- フェールオーバー 設定では、初期接続（3 ウェイ ハンドシェイク プロセスがまだ完了していない接続要求）はすぐに閉じられ、アクティブデバイスとスタンバイデバイス間で同期されません。この設計により、HA システムの効率とセキュリティが確保されます。このため、両方のフェールオーバーデバイスで接続数に違いが生じる可能性がありますが、これは予想されることです。
- フェールオーバー LAN リンクがバックツーバックで接続されておらず、代わりに 1 つ以上のスイッチを介して接続されている場合、中間経路内の障害によってアクティブユニットとスタンバイユニットの接続が失われ、アクティブ/スタンバイ状態の一貫性が失われる可能性があります。これは フェールオーバー 機能には影響しませんが、アクティブユニットとスタンバイユニット間のフェールオーバーリンク経路を確認して回復することをお勧めします。

  フェールオーバー LAN リンクがダウンしている場合、設定はピアユニットに複製されない可能性があるため、設定を展開することは推奨されません。

- Cisco ASA の OSPF では、近くのスイッチがダウンし、Cisco ASA インターフェイスが同じスイッチに接続されている場合、ファイアウォール内のインターフェイスもダウンしてスイッチの障害が発生します。これは予期された動作です。これにより、設計どおりに高可用性フェールオーバーがトリガーされます。
- スタンバイの Cisco ASA が別のスイッチに接続されている場合は、インターフェイスが起動すると、ルーティングテーブルは、アクティブの Cisco ASA のルーティングテーブルとは異なります。これにより、ルートと隣接関係（アジャセンシー）が更新されるまでの短期間（約 15 ー 17 秒）の障害が発生します。
- トランスペアレントモードでは、アクティブユニットでホットスタンバイルータ（HSRP）の MAC アドレスが失われるという問題が発生した場合は、MAC アドレスのスタティック マッピングを作成します。

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が。
- すべての物理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。

High Availability and Scalability Wizard を使用して、手順を踏んでアクティブ/スタンバイ フェールオーバー コンフィギュレーションを作成することができます。

手順

ステップ 1 **[Wizards]** > **[High Availability and Scalability]** を選択します。次の手順でこのウィザードのガイドラインを確認してください。

ステップ 2 [Failover Peer Connectivity and Compatibility] 画面で、ピア装置の IP アドレスを入力します。このアドレスは、ASDMアクセスがイネーブルになっているインターフェイスである必要があります。

デフォルトでは、ピア アドレスは ASDM 管理インターフェイスのスタンバイ アドレスに割り当てられます。

ステップ 3 [LAN Link Configuration] 画面で次のように設定します。

- [インターフェイス（Interface）]：物理インターフェイス ID、サブインターフェイス ID、または EtherChannel インターフェイス ID を指定できます。Firepower 1010 では、インターフェイスはファイアウォール インターフェイス ID です。スイッチ ポート ID または VLAN ID を指定することはできません。Firepower 4100/9300 では、任意のデータタイプ インターフェイスを使用できます。
- [Active IP Address]：この IP アドレスは、未使用のサブネット上にある必要があります。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。169.254.1.0/24 and fd00:0:0:*::/64 は内部的に使用されるサブネットであり、フェールオーバー リンクやステート リンクに使用することはできません。
- [Standby IP Address]：この IP アドレスは、アクティブ IP アドレスと同じネットワーク上にある必要があります。
- （オプション）[Communications Encryption]：フェールオーバー リンクの通信を暗号化します。**注**：秘密キーの代わりに、IPsec 事前共有キーを使用することをお勧めします。これはウィザードを終了した後に設定できます（フェールオーバーの設定変更 （45ページ）を参照）。

ステップ 4 ステートフル フェールオーバー用に別のインターフェイスを選択する場合は、[State Link Configuration] 画面で次の設定を行います。

- [Active IP Address]：この IP 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ある必要があります。 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。169.254.1.0/24 and fd00:0:0:*::/64 は内部的に使用されるサブネットであり、フェールオーバー リンクやステート リンクに使用することはできません。
- [Standby IP Address]：この IP アドレスは、アクティブ IP アドレスと同じネットワーク上にある必要があります。

ステップ 5 [Finish] をクリックすると、ウィザードは [Waiting for Config Sync] 画面を表示します。

指定された時間が経過した後に、ウィザードはセカンデリ装置にフェールオーバー設定を送信し、フェールオーバー設定が完了したことを示す情報画面が表示されます。

- フェールオーバーがセカンデリ装置でイネーブルになっているかどうかわからない場合は、指定した時間だけ待ちます。
- フェールオーバーがすでにイネーブルなことがわかっている場合は、[Skip configuring peer] をクリックします。
- セカンダリ装置でフェールオーバーがイネーブルでないことがわかっている場合は、[Stop waiting *xx* more seconds] をクリックすると、フェールオーバーのブートストラップ設定はすぐにセカンダリ装置に送信されます。

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。

High Availability and Scalability Wizard を使用して、手順を踏んでアクティブ/アクティブ フェールオーバー コンフィギュレーションを作成することができます。

手順

ステップ 1 **[Wizards]** > **[High Availability and Scalability]** を選択します。次の手順でこのウィザードのガイドラインを確認してください。

ステップ 2 [Failover Peer Connectivity and Compatibility Check] 画面では、ピアの IP アドレスは、ASDM アクセスが有効になっているインターフェイスである必要があります。

デフォルトでは、ピア アドレスは、ASDM の接続先インターフェイスのスタンバイ アドレスに割り当てられます。

ステップ 3 [Security Context Configuration] 画面では、ウィザード内でマルチ コンテキスト モードに変換した場合、管理コンテキストのみが表示されます。ウィザードを終了した後に他のコンテキストを追加できます。

ステップ 4 [LAN Link Configuration] 画面で次のように設定します。

- [Interface]：物理インターフェイス ID、サブインターフェイス ID、冗長インターフェイス ID、または EtherChannel インターフェイス ID を指定できます。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。その場合は、設定を保存してから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 4100/9300 では、任意のデータタイプ インターフェイスを使用できます。
- [Active IP Address]：この IP アドレスは、未使用のサブネット上にある必要があります。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。169.254.1.0/24 and fd00:0:0:*::/64 は内部的に使用されるサブネットであり、フェールオーバー リンクやステート リンクに使用することはできません。

- [Standby IP Address]：この IP アドレスは、アクティブ IP アドレスと同じネットワーク上にある必要があります。
- （オプション）[Communications Encryption]：フェールオーバー リンクの通信を暗号化します。**注**：秘密キーの代わりに、IPsec 事前共有キーを使用することをお勧めします。これはウィザードを終了した後に設定できます（フェールオーバーの設定変更 （45 ページ）を参照）。

ステップ 5 ステートフル フェールオーバー用に別のインターフェイスを選択する場合は、[State Link Configuration] 画面で次の設定を行います。

- [Active IP Address]：この IP 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ある必要があります。 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。169.254.1.0/24 and fd00:0:0:*::/64 は内部的に使用されるサブネットであり、フェールオーバー リンクやステート リンクに使用することはできません。
- [Standby IP Address]：この IP アドレスは、アクティブ IP アドレスと同じネットワーク上にある必要があります。

ステップ 6 [Finish] をクリックすると、ウィザードは [Waiting for Config Sync] 画面を表示します。

指定された時間が経過した後に、ウィザードはセカンデリ装置にフェールオーバー設定を送信し、フェールオーバー設定が完了したことを示す情報画面が表示されます。

- フェールオーバーがセカンデリ装置でイネーブルになっているかどうかわからない場合は、指定した時間だけ待ちます。
- フェールオーバーがすでにイネーブルなことがわかっている場合は、[Skip configuring peer] をクリックします。
- セカンダリ装置でフェールオーバーがイネーブルでないことがわかっている場合は、[Stop waiting *xx* more seconds] をクリックすると、フェールオーバーのブートストラップ設定はすぐにセカンダリ装置に送信されます。

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 （33 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。ここでは、アクティブ/アクティブ モードでのフェールオーバー グループごとのHTTP複製のイネーブル化について説明します。アクティブ/スタンバイ モードで HTTP 複製を設定する場合は、フェールオーバーの設定変更 （45 ページ）を参照してください。

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 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** の順に選択します。

ステップ 2 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するには、[Setup] タブをクリックし、[Disable configuration changes on the standby unit] チェック ボックスをオンにします。

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 3 [BFD Health Check] で、[Manage] をクリックして、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。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。

[Configuration] > **[Device Setup]** > **[Routing]** > **[BFD]** > **[Template]** ページが開きます。[Add] をクリックして、シングルホップテンプレートを作成します。マルチホップはサポートされていません。間隔の設定には、ミリ秒を指定できます。マイクロ秒はサポートされていません。テンプレートの詳細については、BFD テンプレートの作成 を参照してください。

ステップ 4 [Criteria] タブをクリックします。

ステップ 5 装置のポーリング時間を設定します。

[Failover Poll Times] 領域で、次を設定します。

- [Unit Failover]：装置間の Hello メッセージの間の時間。範囲は 1 ～ 15 秒または 200 ～ 999 ミリ秒です。
- [Unit Hold Time]：装置がフェールオーバー リンク上で Hello メッセージを受信する必要がある時間（この時間に受信しなかった場合は、装置がピアの障害のテスト プロセスを開始する）を設定します。範囲は 1 ～ 45 秒または 800 ～ 999 ミリ秒です。ポーリング時間の 3 倍より少ない値は入力できません。

（注）
このペインの他の設定はアクティブ/スタンバイ モードにのみ適用されます。アクティブ/アクティブ モードでは、フェールオーバー グループごとに残りのパラメータを設定する必要があります。

ステップ 6 （アクティブ/アクティブ モードのみ）[Active/Active] タブをクリックし、フェールオーバー グループを選択して [Edit] をクリックします。

ステップ 7 （アクティブ/アクティブ モードのみ）プリエンプションでの使用時にフェールオーバー グループの優先するロールを変更するには、[Primary] または [Secondary] をクリックします。

ウィザードを使用した場合、フェールオーバー グループ 1 はプライマリ装置に割り当てられ、フェールオーバー グループ 2 はセカンダリ装置に割り当てられます。標準以外の設定が必要な場合は、別の装置を優先するように指定できます。これらの設定は、プリエンプション処理の設定と併用してのみ使用されます。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）。

ステップ 8 （アクティブ/アクティブ モードのみ）フェールオーバー グループ プリエンプションを設定するには、[Preempt after booting with optional delay of] チェック ボックスをオンにします。

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）。

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。

手動でフェールオーバーすると、プリエンプション処理のオプションが無視されます。

（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。

ステップ 9 [Interface Policy] を設定します。

- [Number of failed interfaces that triggers failover]：フェールオーバーをトリガーするために必要な障害が発生したインターフェイスの具体的な数を 1 ～ 250 で定義します。障害が発生したモニター対象インターフェイスの数が指定した値を超えると、ASA はフェールオーバーします。

- [Percentage of failed interfaces that triggers failover]：フェールオーバーをトリガーするために必要な障害が発生した設定済みインターフェイスの割合を定義します。障害が発生したモニター対象インターフェイスの数が設定した割合を超えると、ASA はフェールオーバーします。

（注）
[Use system failover interface policy] オプションは使用しないでください。現時点ではグループごとのポリシーのみが設定できます。

ステップ 10 （アクティブ/スタンバイ モード）インターフェイスのポーリング時間を設定します。

[Failover Poll Time] 領域で、次を設定します。

- **Monitored Interfaces**：インターフェイスのポーリング時間を指定します。ピアに hello パケットを送信するまで待機する時間。範囲は 1 ～ 15 秒または 500 ～ 999 ミリ秒です。デフォルトは 5 秒です。
- [Link State]：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。範囲は 300 ～ 799 ミリ秒です。
- **Interface Hold Time**：ピア ユニットからの最後に受信した hello メッセージとインターフェイステストの開始との間の時間（計算として）を設定して、インターフェイスの健全性を判断します。また、各インターフェイス テストの期間を *holdtime*/16 として設定します。有効な値は 5 ～ 75 秒です。デフォルトは、polltime の5倍です。polltime の 5 倍よりも短い holdtime 値は入力できません。

  インターフェイステストを開始するまでの時間（y）を計算するには、次のようにします。

  1. x = (*holdtime*/*polltime*)/2、最も近い整数に丸められます。（.4 以下は切り下げ、.5 以上は切り上げ。）
  2. y = x**polltime*

  たとえば、デフォルトの holdtime は 25 で、polltime が 5 の場合は y は 15 秒です。

アクティブ/アクティブ モードの場合、[Add/Edit Failover Group] ダイアログボックスでインターフェイス ポーリング時間を設定します。

ステップ 11 （アクティブ/アクティブ モードのみ）HTTP 複製をイネーブルにするには、[Enable HTTP Replication] チェック ボックスをオンにします。

セッションの複製レートについては、「フェールオーバーの設定変更 （45 ページ）」の項を参照してください。

（注）
フェールオーバーを使用しているときに、スタンバイ装置から HTTP フローを削除すると遅延が生じます。このため **show conn count** 出力には、アクティブ装置とスタンバイ装置で異なる

数が表示されることがあります。数秒待ってコマンドを再発行すると、両方の装置で同じカウントが表示されます。

ステップ 12 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：[MAC Addresses] タブをクリックし、[Add] をクリックします。

  [Add/Edit Interface MAC Address] ダイアログボックスが表示されます。

- アクティブ/アクティブ モード：[Active/Active] [タブの下部に移動します。

他の方法を使用して 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。

a) [Physical Interface] ドロップダウンリストからインターフェイスを選択します。
b) [Active MAC Address] フィールドに、アクティブ インターフェイスの新しい MAC アドレスを入力します。
c) [Standby MAC Address] フィールドに、スタンバイ インターフェイスの新しい MAC アドレスを入力します。
d) [OK] をクリックします。（アクティブ/アクティブ モードのみ）再度 [OK] をクリックします。

ステップ 13 [適用（Apply）] をクリックします。

インターフェイス モニタリングの設定およびスタンバイ アドレスの設定

デフォルトでは、すべての物理インターフェイス、またはFirepower 1010 の場合、およびSecure Firewall 1210/1220 すべての VLAN インターフェイス インターフェイス モニタリングの場合、Firepower 1010 および Secure Firewall 1210/1220 スイッチポートが対象です。

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。

装置ごとに最大 1025 のインターフェイスをモニターできます（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）。

ウィザードでスタンバイ IP アドレスを設定しなかった場合は、手動で設定できます。

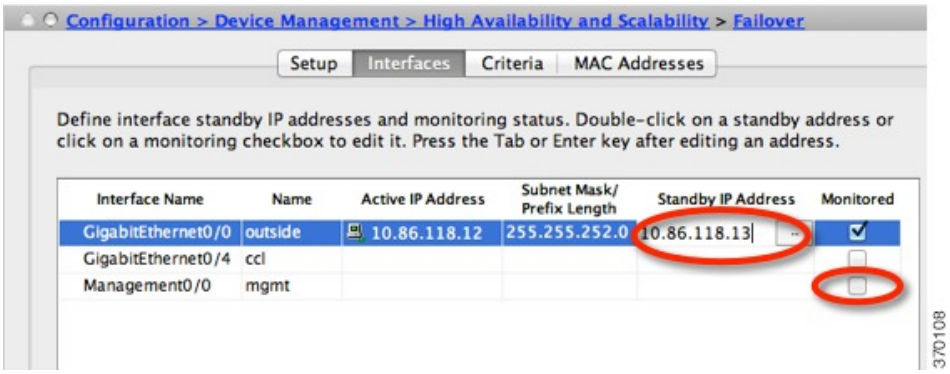
始める前に

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

ステップ 1 シングル モードでは、**[Configuration]** > **[Device Management]** > **[High Availability]** > **[Failover]** > **[Interfaces]** の順に選択します。

マルチ コンテキスト モードでは、コンテキスト内で [Configuration] > [Device Management] > [Failover] > [Interfaces] を選択します。



設定されているインターフェイスのリストが、表示されます。[Monitored] カラムに、フェールオーバー基準の一部としてインターフェイスがモニターされているかどうかが表示されます。モニターされている場合は、[Monitored] チェック ボックスがオンになっています。

各インターフェイスの IP アドレスが [Active IP Address] カラムに表示されます。インターフェイスのスタンバイ IP アドレスが設定されている場合は、[Standby IP address] カラムに表示されます。フェールオーバー リンクおよびステート リンクについては IP アドレスは表示されません。これらのアドレスはこのタブから変更できません。

ステップ 2 表示されているインターフェイスのモニタリングをディセーブルにするには、インターフェイスの [Monitored] チェックボックスをオフにします。

ステップ 3 表示されているインターフェイスのモニタリングをイネーブルにするには、インターフェイスの [Monitored] チェックボックスをオンにします。

ステップ 4 スタンバイ IP アドレスを持っていない各インターフェイスに対して、[Standby IP Address] フィールドをダブルクリックしてフィールドに IP アドレスを入力します。

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。

ステップ 5 [適用（Apply）] をクリックします。

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。

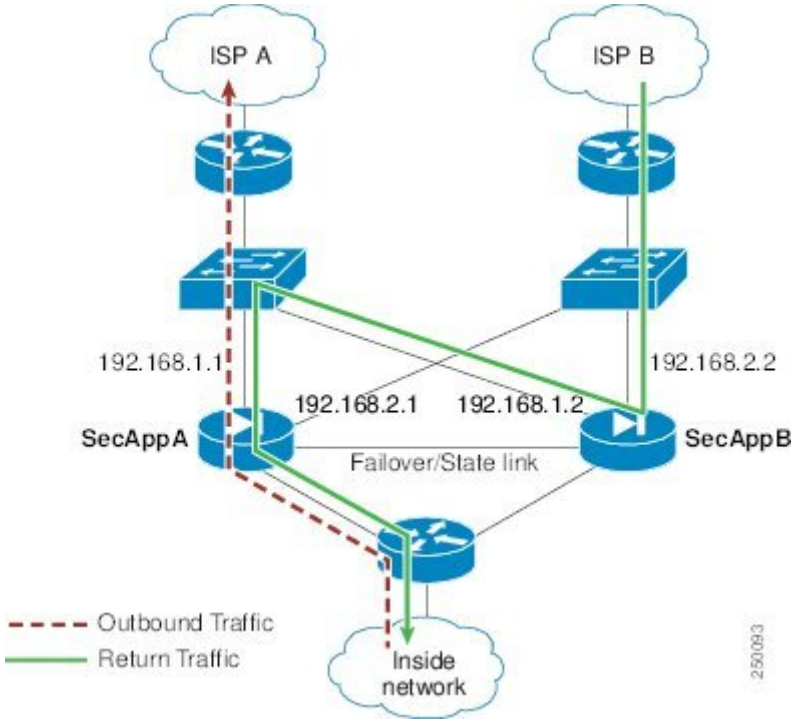
返送パケットのドロップは、非対称にルーティングされたパケットを許可することによって防ぐことができます。そのためには、それぞれの ASA の同様のインターフェイスを同じ ASR グループに割り当てます。たとえば、両方の ASA が、内部インターフェイスでは同じ内部ネットワークに接続している一方、外部インターフェイスでは別の ISP に接続しているとします。プライマリ装置で、アクティブ コンテキストの外部インターフェイスを ASR グループ 1 に割り当て、セカンダリ装置でも、アクティブ コンテキストの外部インターフェイスを同じ ASR グループ 1 に割り当てます。プライマリ装置の外部インターフ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 *6 : 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 プライマリ装置のアクティブ コンテキストで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[ASR Groups]** の順に選択します。

ステップ 2 非対称にルーティングされたパケットを受信するインターフェイスについて、ドロップダウンリストから **ASR グループ ID** を選択します。

ステップ 3 [Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

ステップ 4 ASDM をセカンダリ装置に接続し、プライマリ装置のコンテキストと同様のアクティブ コンテキストを選択します。

ステップ 5 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[ASR Groups]** の順に選択します。

ステップ 6 この装置の同様のインターフェイスについて、同じ **ASR グループ ID** を選択します。

ステップ 7 [Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

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 を有効化した後に 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設定変更

ウィザードを使用しない場合や、設定を変更する場合に、手動でフェールオーバーを設定できます。ここでは、ウィザードに含まれていないため手動で設定する必要がある次のオプションについても説明します。

- フェールオーバー トラフィックを暗号化するための IPsec 事前共有キー
- HTTP 複製レート
- HTTP 複製（アクティブ/スタンバイ モード）

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 シングルモードでは、**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Setup]** の順に選択します。

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 [Configuration] > [Device Management] > [Failover] > [Setup] を選択します。

ステップ 2 [Enable Failover] チェックボックスをオンにします。

（注）
デバイスに変更を適用するまで、フェールオーバーは実際にはイネーブルになりません。

ステップ 3 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、次のオプションのいずれかを使用します。

- [IPsec Preshared Key]（優先）：フェールオーバー装置間のフェールオーバー リンクで IPsec LAN-to-LAN トンネルを確立するために、IKEv2 によって使用される事前共有キーです。注：フェールオーバー LAN-to-LAN トンネルは、IPsec（他の VPN）ライセンスには適用されません。
- [Secret Key]：フェールオーバー通信の暗号化に使用される秘密キーを入力します。このフィールドを空白のままにした場合は、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パスワードまたはキーを含め、フェールオーバー通信がクリア テキストになります。

  [Use 32 hexadecimal character key]：秘密キーに 32 文字の 16 進キーを使用するには、このチェック ボックスをオンにします。

ステップ 4 [LAN Failover] 領域で、フェールオーバー リンクの次のパラメータを設定します。

- [Interface]：フェールオーバー リンクに使用するインターフェイスを選択します。フェールオーバーには専用インターフェイスが必要ですが、ステートフル フェールオーバーとインターフェイスを共有できます。

  このリストには、未設定のインターフェイスまたはサブインターフェイスのみが表示され、フェールオーバー リンクとして選択できます。インターフェイスをフェールオーバー リンクに指定すると、そのインターフェイスは [Configuration] > [Interfaces] ペインでは編集できません。

- [Logical Name]：「failover」などのフェールオーバー通信に使用するインターフェイスの論理名を指定します。この名前は情報を提供するためのものです。

- [Active IP]：インターフェイスのアクティブ IP アドレスを指定します。IP アドレスは、IPv4 または IPv6 アドレスのどちらにすることもできます。この IP 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。

- [Standby IP]：インターフェイスのスタンバイ IP アドレスを指定します。アクティブ IP アドレスと同じサブネット上のアドレスを指定します。

- [Subnet Mask]：サブネット マスクを指定します。

- [Preferred Role]：この ASA の優先されるロールがプライマリ装置であるかセカンダリ装置であるかを指定するために、[Primary] または [Secondary] を選択します。

ステップ 5 （オプション）次の手順でステート リンクを設定します。

- [Interface]：ステート リンクに使用するインターフェイスを選択します。選択できるのは、未設定のインターフェイスまたはサブインターフェイス、フェールオーバー リンク、または [--Use Named--] オプションです。

  （注）
  フェールオーバー リンク専用インターフェイスとステート リンク専用インターフェイスの 2 つのインターフェイスを別々に使用することを推奨します。

  未設定のインターフェイスまたはサブインターフェイスを選択した場合、そのインターフェイスの**アクティブ IP**、**サブネット マスク**、**論理名**、および**スタンバイ IP** を入力する必要があります。

  フェールオーバー リンクを選択した場合は、**アクティブ IP**、**サブネット マスク**、**論理名**、および**スタンバイ IP** の値を指定する必要はありません。フェールオーバー リンクに指定されている値が使用されます。

  [--Use Named--] オプションを選択した場合、[Logical Name] フィールドは、名前のついたインターフェイスのドロップダウン リストになります。このリストからインターフェイスを選択します。**アクティブ IP**、**サブネット マスク/プレフィックスの長さ**、**スタンバイ IP** の値を指定する必要はありません。そのインターフェイスに指定された値が使用されます。

- [Logical Name]：「state」などのステート通信に使用するインターフェイスの論理名を指定します。この名前は情報を提供するためのものです。

- [Active IP]：インターフェイスのアクティブ IP アドレスを指定します。IP アドレスは、IPv4 または IPv6 アドレスのどちらにすることもできます。この IP 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。
- [Standby IP]：インターフェイスのスタンバイ IP アドレスを指定します。アクティブ IP アドレスと同じサブネット上のアドレスを指定します。
- [Subnet Mask]：サブネット マスクを指定します。
- （オプション、アクティブ/スタンバイのみ）[Enable HTTP Replication]：このオプションにより、アクティブ HTTP セッションをスタンバイ ファイアウォールにコピーするステートフル フェールオーバーがイネーブルになります。HTTP 複製を許可しない場合、HTTP 接続はフェールオーバーの発生時に切断されます。アクティブ/アクティブ モードでは、フェールオーバー グループごとに HTTP 複製を設定します。

  （注）
  フェールオーバーを使用しているときに、スタンバイ装置から HTTP フローを削除すると遅延が生じます。このため **show conn count** 出力には、アクティブ装置とスタンバイ装置で異なる数が表示されることがあります。 数秒待ってコマンドを再発行すると、両方の装置で同じカウントが表示されます。

ステップ 6 [Replication] 領域で、セッション複製レートを 1 秒あたり接続数で設定します。最小および最大レートはモデルによって決まります。デフォルトは最大レートです。デフォルトを使用するには、[Use Default] チェックボックスをオンにします。

ステップ 7 [Apply] をクリックします。

コンフィギュレーションがデバイスに保存されます。

ステップ 8 フェールオーバーをイネーブルにすると、フェールオーバー ピアを設定するためのダイアログボックスが表示されます。

- 後でフェールオーバー ピアに接続して手動で同様の設定を行う場合は、[No] をクリックします。
- ASDM によって自動的にフェールオーバー ピア上の関連するフェールオーバー設定が行われるようにするには、[Yes] をクリックします。[Peer IP Address] フィールドにピアの IP アドレスを指定します。

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 フェールオーバーを装置レベルで強制するには次を行います。

a) コンテキスト モードに応じて画面を選択します。

- シングル コンテキスト モードでは、[Monitoring] > [Properties] > [Failover] > [Status] を選択します。
- マルチ コンテキスト モードでは、システムで [Monitoring] > [Failover] > [System] を選択します。

b) 次のいずれかのボタンをクリックします。

- [Make Active] をクリックすると、この装置がアクティブ装置になります。
- [Make Standby] をクリックすると、相手装置がアクティブ装置になります。

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 レベルで強制するには次を行います。

a) システムで、[Monitoring] > [Failover] > [Failover Group #] を開きます。# は、制御するフェールオーバー グループの番号です。

b) 次のいずれかのボタンをクリックします。

- [Make Active] をクリックすると、この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。
- [Make Standby] をクリックすると、相手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。

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 （47 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 シングルモードでは、**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Setup]** の順に選択します。

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 [Configuration] > [Device Management] > [Failover] > [Setup] を選択します。

ステップ 2 [Enable Failover] チェックボックスをオフにします。

ステップ 3 [Apply] をクリックします。

ステップ 4 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。

a) [Save] ボタンをクリックします。

b) [Tools] > [System Reload] を選択して、ASA をリロードします。

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 フェールオーバーを装置レベルで復元するには次を行います。

a) コンテキスト モードに応じて画面を選択します。

- シングル コンテキスト モードでは、[Monitoring] > [Properties] > [Failover] > [Status] を選択します。
- マルチ コンテキスト モードでは、システムで [Monitoring] > [Failover] > [System] を選択します。

b) [Reset Failover] をクリックします。

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) システムで、[Monitoring] > [Failover] > [Failover Group #] を開きます。# 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

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。複製されたコマンドをスタンバイ装置のフラッシュ メモリに保存するには、[File] > [Save Running Configuration to Flash] の順に選択します。

フェールオーバーのモニタリング

このセクションの手順に従うことで、フェールオーバーのステータスをモニターできます。

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、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug fover** コマンドを使用してください。

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

（注） フェールオーバー イベントが発生した後、デバイスのモニタリングを継続するには、ASDM を再起動するか、または [Devices] ペインに表示される別のデバイスに切り替えて、元の ASA に戻る手順を実行する必要があります。この操作が必要なのは、ASDM がデバイスから切断されて再接続された場合、接続のモニタリングが再確立されないためです。

[Monitoring] > [Properties] > [Failover] を選択して、アクティブ/スタンバイ フェールオーバーをモニターします。

[Monitoring] > [Properties] > [Failover] 領域で次の画面を使用して、アクティブ/アクティブ フェールオーバーをモニターします。

システム

[System] ペインには、システムのフェールオーバー状態が表示されます。また、システムのフェールオーバー状態を次の方法で制御できます。

- デバイスのアクティブ/スタンバイ状態を切り替える。
- 障害が発生したデバイスをリセットする。

- スタンバイ装置をリロードする。

フィールド

[Failover state of the system]：表示専用。ASA のフェールオーバー状態を表示します。表示される情報は、**show failover** コマンドで受け取る出力と同じです。表示出力に関する詳細については、コマンド リファレンスを参照してください。

[System] ペインでは、次のアクションを使用できます。

- [Make Active]：アクティブ/スタンバイ コンフィギュレーションで、このボタンをクリックすると、ASA がアクティブ装置になります。アクティブ/アクティブ コンフィギュレーションで、このボタンをクリックすると、ASA で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。
- [Make Standby]：アクティブ/スタンバイ ペアで、このボタンをクリックすると、ASA がスタンバイ装置になります。アクティブ/アクティブ コンフィギュレーションで、このボタンをクリックすると、ASA で両方のフェールオーバー グループがスタンバイ状態になります。
- [Reset Failover]：このボタンをクリックして、システムを障害状態からスタンバイ状態にリセットします。システムをアクティブ状態にはリセットできません。アクティブ装置でこのボタンをクリックすると、スタンバイ装置がリセットされます。
- [Reload Standby]：このボタンをクリックして、スタンバイ装置を強制的にリロードします。
- [Refresh]：このボタンをクリックして、[system] フィールドのフェールオーバー状態にあるステータス情報をリフレッシュします。

フェールオーバー グループ 1 およびフェールオーバー グループ 2

[Failover Group 1] ペインおよび [Failover Group 2] ペインには、選択したグループのフェールオーバー状態が表示されます。また、グループのアクティブ/スタンバイ状態を切り替えるか、または障害が発生したグループをリセットして、グループのフェールオーバー状態を制御することもできます。

フィールド

[Failover state of Group[*x*]]：表示専用。選択したフェールオーバー グループのフェールオーバー状態を表示します。表示される情報は、**show failover group** コマンドで受け取る出力と同じです。

このペインで次のアクションを実行できます。

- [Make Active]：このボタンをクリックして、フェールオーバー グループを ASA のアクティブ ユニットにします。
- [Make Standby]：このボタンをクリックして、フェールオーバー グループを ASA で強制的にスタンドバイ状態にします。

- [Reset Failover]：このボタンをクリックして、システムを障害状態からスタンバイ状態にリセットします。システムをアクティブ状態にはリセットできません。アクティブ装置でこのボタンをクリックすると、スタンバイ装置がリセットされます。
- [Refresh]：このボタンをクリックして、[system] フィールドのフェールオーバー状態にあるステータス情報をリフレッシュします。

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。 次の画面が変更になりました。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup]。
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。 ASDM の変更はありませんでした。
フェールオーバーに IPv6 のサポートが追加	8.2(2)	次の画面が変更されました。 [Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup]。 [Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces]。

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、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。 次の画面が変更されました。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup]。
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。 次の画面が変更されました。[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Interfaces]
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。 次の画面が変更されました。[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Setup]

機能名	リリース	機能情報
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可能	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。 次の画面が変更されました。[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Setup]
キャリア グレードNATの強化がフェールオーバーおよび ASA クラスタリングでサポート	9.5(2)	キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、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。 変更された画面はありません。
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の セキュアクライアント からのダイナミック ACL における同期時間の改善	9.6(2)	フェールオーバーペアで セキュアクライアント を使用するとき、関連付けられているダイナミック ACL（dACL）における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。 変更された画面はありません。
マルチコンテキストモードのセキュアクライアント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 セキュアクライアント 接続のステートフル フェールオーバーがサポートされるようになりました。 変更された画面はありません。

機能名	リリース	機能情報
より迅速に検出を行うための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可能	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。 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Criteria]**
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。 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Setup]**
フェールオーバー遅延の無効化	9.15(1)	ブリッジグループまたは IPv6 DAD を使用する場合、フェールオーバーが発生すると、新しいアクティブユニットは、スタンバイユニットがネットワーキングタスクを完了してスタンバイ状態に移行するまで、最大3000ミリ秒待機します。その後、アクティブユニットはトラフィックの受け渡しを開始できます。この遅延を回避するために、待機時間を無効にすると、スタンバイユニットが移行する前にアクティブユニットがトラフィックの受け渡しを開始します。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Enable switchover waiting for peer state]**
HA ピアリングを高速化する設定同期最適化機能	9.18(1)	設定同期最適化機能により、config-hash 値を交換して参加ユニットとアクティブユニットの設定を比較できます。アクティブユニットと参加ユニットの両方で計算されたハッシュが一致する場合、参加ユニットは完全な設定同期をスキップして HA に再参加します。この機能により、さらに迅速な HA ピアリングが可能になり、メンテナンスウィンドウとアップグレード時間が短縮されます。

機能名	リリース	機能情報
ハートビートモジュールの冗長性	9.20(1)	ASA高可用性のデータプレーンに追加のハートビートモジュールが導入されました。このハートビートモジュールは、コントロールプレーンのトラフィックの輻輳やCPUの過負荷が原因で発生する可能性のある、偽フェールオーバーやスプリットブレインシナリオを回避するのに役立ちます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。