



CHAPTER 8

アクティブ/スタンバイ フェールオーバーの設定

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

- 「アクティブ/スタンバイ フェールオーバーに関する情報」 (P.8-1)
- 「アクティブ/スタンバイ フェールオーバーのライセンス要件」 (P.8-6)
- 「アクティブ/スタンバイ フェールオーバーの前提条件」 (P.8-7)
- 「ガイドラインと制限事項」 (P.8-7)
- 「アクティブ/スタンバイ フェールオーバーの設定」 (P.8-8)
- 「フェールオーバーの制御」 (P.8-18)
- 「アクティブ/スタンバイ フェールオーバーのモニタリング」 (P.8-20)
- 「アクティブ/スタンバイ フェールオーバーの機能履歴」 (P.8-20)

アクティブ/スタンバイ フェールオーバーに関する情報

ここでは、アクティブ/スタンバイ フェールオーバーを設定する手順について説明します。次の項目を取り上げます。

- 「アクティブ/スタンバイ フェールオーバーの概要」 (P.8-1)
- 「プライマリ/セカンダリ ステータスとアクティブ/スタンバイ ステータス」 (P.8-2)
- 「デバイスの初期化とコンフィギュレーションの同期」 (P.8-2)
- 「コマンドの複製」 (P.8-3)
- 「フェールオーバーのトリガー」 (P.8-4)
- 「フェールオーバーのアクション」 (P.8-5)

アクティブ/スタンバイ フェールオーバーの概要

アクティブ/スタンバイ フェールオーバーでは、スタンバイ ASA を使用して、障害の発生した装置の機能を引き継ぐことができます。アクティブ装置が故障すると、スタンバイ状態に変わり、そしてスタンバイ装置がアクティブ状態に変わります。アクティブになる装置が、障害の発生した装置の IP アドレス（または、トランスペアレント ファイアウォールの場合は管理 IP アドレス）および MAC アドレスを引き継いで、トラフィックの転送を開始します。現在スタンバイになっている装置が、スタンバイ

の 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)

マルチ コンテキスト モードの場合、ASA は装置全体 (すべてのコンテキストを含む) をフェールオーバーできますが、個々のコンテキストを別々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 ステータスとアクティブ/スタンバイ ステータス

フェールオーバー ペアの 2 台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 アドレスを使用するかおよびどちらの装置がアクティブにトラフィックを渡すかということに関連します。

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 アドレスと結び付けられています。このルールの例外は、セカンダリ装置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。

デバイスの初期化とコンフィギュレーションの同期

コンフィギュレーションの同期は、フェールオーバー ペア的一方または両方のデバイスがブートされると行われます。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。スタンバイ装置は、その初期スタートアップを完了すると、自分の実行コンフィギュレーションを削除し (アクティブ装置との通信に必要なフェールオーバー コマンドを除く)、アクティブ装置は自分のコンフィギュレーション全体をスタンバイ装置に送信します。

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。



(注)

セカンダリ装置がブートされてプライマリ装置を検出できないと、その装置はアクティブ装置になります。アクティブ IP アドレスには、セカンダリ装置自体の MAC アドレスを使用します。しかし、プライマリ装置が使用可能になると、セカンダリ装置は 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。これを回避するには、フェールオーバー ペアを仮想 MAC アドレスで設定します。詳細については、「[仮想 MAC アドレスの設定](#)」(P.8-17) を参照してください。

複製が開始されると、アクティブ装置の ASA コンソールに「Beginning configuration replication: Sending to mate」というメッセージが表示され、複製が完了すると、ASA に「End Configuration Replication to mate」というメッセージが表示されます。複製中、アクティブ装置に入力されたコマン

ドがスタンバイ装置に適切に複製されないことがあり、またスタンバイ装置に入力されたコマンドが、アクティブ装置から複製されているコンフィギュレーションによって上書きされることがあります。コンフィギュレーションの複製処理中には、フェールオーバー ペアのどちらの装置にもコマンドを入力しないでください。コンフィギュレーションのサイズによって、複製は数秒で済むことも数分かかることもあります。



(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 ピアに同期化されません。

スタンバイ装置の場合、コンフィギュレーションは実行メモリにだけ存在します。同期化後にコンフィギュレーションをフラッシュ メモリに保存するには、次のようにします。

- シングル コンテキスト モードの場合は、アクティブ装置で **write memory** コマンドを入力します。コマンドはスタンバイ装置に複製され、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。
- マルチ コンテキスト モードの場合は、システム実行スペースからアクティブ装置で **write memory all** コマンドを入力します。コマンドはスタンバイ装置に複製され、コンフィギュレーションがフラッシュ メモリに書き込まれます。このコマンドで **all** キーワードを使用すると、システムとすべてのコンテキスト コンフィギュレーションが保存されます。



(注)

外部のサーバに保存されたスタートアップ コンフィギュレーションは、ネットワーク経由で両方の装置からアクセスできます。そのため、各装置で個別に保存する必要はありません。または、ディスク上のコンテキストを、アクティブ装置から外部サーバにコピーし、それからスタンバイ装置のディスクにコピーできます。スタンバイ装置で、装置がリロードされると、そのコンテキストが使用可能になります。

コマンドの複製

コマンドの複製は常に、アクティブ装置からスタンバイ装置の方向に行われます。アクティブ装置にコマンドを入力すると、そのコマンドがフェールオーバー リンクを通してスタンバイ装置に送信されます。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。

スタンバイ ASA に複製されるコマンドは、次のとおりです。

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

- **copy running-config startup-config** を除く、すべての形式の **copy** コマンド
- **write memory** を除く、すべての形式の **write** コマンド
- **debug**

- **failover lan unit**
- **firewall**
- **show**
- **terminal pager** および **pager**



(注)

スタンバイ装置上で行った変更は、アクティブ装置に複製されません。スタンバイ装置にコマンドを入力すると、ASAに「**** WARNING **** Configuration Replication is NOT performed from Standby unit to Active unit.Configurations are no longer synchronized.」というメッセージが表示されます。このメッセージは、コンフィギュレーションに影響しない数多くのコマンドを入力したときにも表示されます。

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。



(注)

スタンバイ フェールオーバーは、次のファイルと設定コンポーネントを複製しません。

- AnyConnect イメージ
- CSD イメージ
- ASA イメージ
- AnyConnect プロファイル
- ローカル認証局 (CA)
- ASDM イメージ

複製されたコマンドをスタンバイ装置、スタンバイ装置のフラッシュ メモリに保存するには、次の手順を実行します。

- シングル コンテキスト モードの場合は、アクティブ装置で **copy running-config startup-config** コマンドを使用します。コマンドはスタンバイ装置に複製され、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。
- マルチ コンテキスト モードの場合は、システム実行スペースおよびディスク上の各コンテキスト内からアクティブ装置に **copy running-config startup-config** コマンドを入力します。コマンドはスタンバイ装置に複製され、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。外部のサーバにスタートアップ コンフィギュレーションがあるコンテキストは、ネットワーク経由で両方の装置からアクセスできます。そのため、各装置で個別に保存する必要はありません。または、ディスク上のコンテキストを、アクティブ装置から外部サーバにコピーし、それからスタンバイ装置のディスクにコピーできます。

フェールオーバーのトリガー

次のいずれかのイベントが発生した場合、装置が故障する可能性があります。

- 装置でハードウェア障害または電源断が発生した。
- 装置でソフトウェア障害が発生した。
- 多くのモニタ対象インターフェイスが故障した。
- フェールオーバーを強制実行した。 ([「フェールオーバーの強制実行」 \(P.8-18\)](#) を参照してください)。

フェールオーバーのアクション

アクティブ/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。

表 8-1 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 8-1 フェールオーバー動作

障害の状況	ポリシー	アクティブアクション	スタンバイアクション	注釈
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。
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 インターフェイスに故障とマークする	フェールオーバー インターフェイス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 インターフェイス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。
ステートフル フェールオーバー リンクに障害が発生した	フェールオーバーなし	動作なし	動作なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。

表 8-1 フェールオーバー動作（続き）

障害の状況	ポリシー	アクティブ アクション	スタンバイ アクション	注釈
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。

オプションのアクティブ/スタンバイ フェールオーバー設定

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

- ステートフル フェールオーバーでの HTTP 複製：ステート情報の複製に接続を含めることができます。
- インターフェイス モニタリング：装置の最大 250 のインターフェイスをモニタし、フェールオーバーに影響を与えるインターフェイスを制御できます。
- インターフェイス ヘルス モニタリング：ASA がより早くインターフェイスの障害を検出して対応できるようにします。
- フェールオーバー基準の設定：インターフェイス数またはモニタされているインターフェイスの割合を指定して、この数または割合を超えたインターフェイスに障害が発生した場合にフェールオーバーが発生するようにできます。
- 仮想 MAC アドレスの設定：セカンダリ装置がプライマリ装置よりも前にオンラインになっても、セカンダリ装置がアクティブ装置である場合、正しい MAC アドレスを使用するようにします。

アクティブ/スタンバイ フェールオーバーのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
ASA 5505	Security Plus ライセンス（ステートフル フェールオーバーはサポートされません）。
ASA 5510、 ASA 5512-X	Security Plus ライセンス
他のすべてのモデル	基本ライセンス

フェールオーバー ユニットの、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 クラスター ライセンスに結合されます。このルールの特例は次のとおりです。

- ASA 5505、5510、および 5512-X の Security Plus ライセンスの場合：基本ライセンスはフェールオーバーをサポートしないため、基本ライセンスのみを保持するスタンバイ ユニットのフェールオーバーをイネーブルにできません。

- ASA 5500-X の IPS モジュール ライセンスの場合：他のモデルで各装置のハードウェア モジュールを購入する必要があるのと同様、各装置用の IPS モジュール ライセンスを購入する必要があります。
- 暗号化ライセンス：両方のユニットに同じ暗号化ライセンスが必要です。

アクティブ/スタンバイ フェールオーバーの前提条件

アクティブ/スタンバイ フェールオーバーには、次の前提条件があります。

- 両方の装置が同じ ASA であり、専用のフェールオーバー リンク（オプションで、ステートフル フェールオーバー リンク）で相互に接続されている必要があります。
- 両方の装置が、同じソフトウェア コンフィギュレーションと適切なライセンスを備えている必要があります。
- 両方の装置のモード（シングルまたはマルチ、透過またはルーテッド）が同じである必要があります。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

- シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。
- マルチ コンテキスト モードでは、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。

ファイアウォール モードのガイドライン

- トランスペアレント ファイアウォール モードおよびルーテッド ファイアウォール モードでサポートされます。

IPv6 のガイドライン

- IPv6 フェールオーバーがサポートされています。

モデルのガイドライン

- ステートフル フェールオーバーは、ASA 5505 ではサポートされていません。

その他のガイドラインと制限事項

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

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

アクティブ/スタンバイ フェールオーバーには、次のガイドラインと制限事項が適用されます。

- フェールオーバー ペアの両方の装置からパケットを受信するには、すべてのインターフェイスにスタンバイ IP アドレスを設定する必要があります。
- スタンバイ IP アドレスは、現在スタンバイ装置である ASA で使用されます。スタンバイ IP アドレスは、アクティブ装置で対応しているインターフェイス上のアクティブ IP アドレスと同じサブネット内にある必要があります。
- フェールオーバー ペアのアクティブ装置でコンソール端末のページ設定を変更した場合、アクティブなコンソール端末のページ設定は変更されますが、スタンバイ装置の設定は変更されません。アクティブ装置で発行されたデフォルト コンフィギュレーションは、スタンバイ装置の動作にも影響を与えます。
- インターフェイス モニタリングをイネーブルにすると、1 台の装置で最大 250 のインターフェイスをモニタできます。
- デフォルトでは、ステートフル フェールオーバーがイネーブルの場合、ASA は HTTP セッション情報を複製しません。HTTP セッションは一般的に存続期間が短いことと、HTTP クライアントは接続試行が失敗すると再試行するのが一般的であることから、HTTP セッションの複製をしないほうがシステムのパフォーマンスが向上します。複製をしなくても重要なデータや接続は失われません。**failover replication http** コマンドを使用するとステートフル フェールオーバー環境で HTTP セッションのステートフルな複製がイネーブルになりますが、システムのパフォーマンスが低下する可能性があります。
- AnyConnect イメージはフェールオーバー ペアの両方の ASA で同一である必要があります。ヒットレス 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レポート手順で WebVPN 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。

アクティブ/スタンバイ フェールオーバーの設定

この項では、アクティブ/スタンバイ フェールオーバーを設定する方法について説明します。この項は、次の内容で構成されています。

- 「[アクティブ/スタンバイ フェールオーバーの設定のタスク フロー](#)」 (P.8-8)
- 「[プライマリ装置の設定](#)」 (P.8-9)
- 「[セカンダリ装置の設定](#)」 (P.8-12)
- 「[オプションのアクティブ/スタンバイ フェールオーバー設定値の設定](#)」 (P.8-14)

アクティブ/スタンバイ フェールオーバーの設定のタスク フロー

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

-
- ステップ 1** 「プライマリ装置の設定」(P.8-9) に従って、プライマリ装置を設定します。
- ステップ 2** 「セカンダリ装置の設定」(P.8-12) に従って、セカンダリ装置を設定します。
- ステップ 3** (任意) 「オプションのアクティブ/スタンバイ フェールオーバー設定値の設定」(P.8-14) に従って、オプションのアクティブ/スタンバイ フェールオーバー設定を行います。
-

プライマリ装置の設定

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

制限事項

専用のステートフル フェールオーバー インターフェイスを使用する場合は、ステートフル フェールオーバー リンクにインターフェイス コンフィギュレーション モードの IP アドレスを設定しないでください。専用のステートフル フェールオーバー インターフェイスを設定するには、後述の手順の **failover interface ip** コマンドを使用します。

前提条件

- すべての IP アドレスのスタンバイ アドレスを第 12 章「インターフェイス コンフィギュレーションの実行 (ルーテッド モード)」または第 13 章「インターフェイス コンフィギュレーションの実行 (トランスペアレント モード)」に従って設定します。
- 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。

手順の詳細

	コマンド	目的
ステップ 1	<code>failover lan unit primary</code>	装置をプライマリ装置に指定します。
ステップ 2	<code>failover lan interface if_name interface_id</code> 例 : <code>hostname(config)# failover lan interface folink GigabitEthernet0/3</code>	フェールオーバー インターフェイスとして使用するインターフェイスを指定します。このインターフェイスは、他の目的に使用しないでください（オプションのステートフル フェールオーバー リンクは除く）。 <i>if_name</i> 引数は、 <i>interface_id</i> 引数で指定されたインターフェイスに名前を割り当てます。 インターフェイス ID は、物理インターフェイスまたは冗長インターフェイスにすることができます。ASA 5505 または ASASM では、 <i>interface_id</i> には VLAN を指定します。 (注) 順序が不正なパケットを防ぐために、フェールオーバーまたはステート リンクとして EtherChannel を使用できますが、EtherChannel のインターフェイスは 1 個のみが使用されます。そのインターフェイスに障害が発生した場合、その EtherChannel の次のインターフェイスが使用されます。フェールオーバー リンクとして使用中は、EtherChannel 設定を変更できません。設定を変更するには、変更を行う間に EtherChannel をシャットダウンする、または一時的にフェールオーバーをディセーブルにする必要があります。いずれのアクションも、フェールオーバーがその期間発生するのを防止します。
ステップ 3	<code>failover interface ip if_name [ip_address mask standby ip_address ipv6_address/prefix standby ipv6_address]</code> 例 : <code>hostname(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2</code> <code>hostname(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby 2001:a0a:b00::a0a:b71</code>	アクティブおよびスタンバイ IP アドレスをフェールオーバー リンクに割り当てます。IPv4 アドレスまたは IPv6 アドレスのいずれかをインターフェイスに割り当てることができます。両方のアドレス タイプをフェールオーバー リンクに割り当てることはできません。 スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。スタンバイアドレスのサブネット マスクを指定する必要はありません。 フェールオーバー リンクの IP アドレスおよび MAC アドレスは、フェールオーバー時に変更されません。フェールオーバーリンクのアクティブ IP アドレスは、常にプライマリ装置にあります。スタンバイ IP アドレスは、セカンダリ装置にあります。
ステップ 4	<code>interface interface_id</code> <code>no shutdown</code> 例 : <code>hostname(config)# interface vlan100 hostname(config-if)# no shutdown</code>	インターフェイスをイネーブルにします。

コマンド	目的
<p>ステップ 5 <code>failover link if_name interface_id</code></p> <p>例 :</p> <pre>hostname(config)# failover link statelink GigabitEthernet0/2</pre>	<p>(任意) ステートフル フェールオーバー リンクとして使用するインターフェイスを指定します。このインターフェイスは、他の目的に使用しないでください (オプションのフェールオーバー リンクは除く)。</p> <p>(注) ステートフル フェールオーバー リンクがフェールオーバー リンクまたはデータ インターフェイスを使用する場合は、<code>if_name</code> 引数を指定することだけが必要です。</p> <p><code>if_name</code> 引数は、<code>interface_id</code> 引数で指定されたインターフェイスに論理名を割り当てます。<code>interface_id</code> 引数は、物理ポート名 (Ethernet1 など) にすることも、すでに作成されているサブインターフェイス (Ethernet0/2.3 など) にすることもできます。インターフェイスは、物理インターフェイスにすることも冗長インターフェイスにすることもできます。</p> <p>(注) 順序が不正なパケットを防ぐために、フェールオーバーまたはステート リンクとして EtherChannel を使用できませんが、EtherChannel のインターフェイスは 1 個のみが使用されます。そのインターフェイスに障害が発生した場合、その EtherChannel の次のインターフェイスが使用されます。フェールオーバー リンクとして使用中は、EtherChannel 設定を変更できません。設定を変更するには、変更を行う間に EtherChannel をシャットダウンする、または一時的にフェールオーバーをディセーブルにする必要があります。いずれのアクションも、フェールオーバーがその期間発生するのを防止します。</p>
<p>ステップ 6 <code>failover interface ip if_name [ip_address mask standby ip_address ipv6_address/prefix standby ipv6_address]</code></p> <p>例 :</p> <pre>hostname(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2</pre> <pre>hostname(config)# failover interface ip statelink 2001:ala:b00::a0a:a70/64 standby 2001:ala:b00::a0a:a71</pre>	<p>(任意) アクティブおよびスタンバイ IP アドレスをステートフル フェールオーバー リンクに割り当てます。IPv4 アドレスまたは IPv6 アドレスのいずれかをインターフェイスに割り当てることができます。両方のアドレス タイプをステートフル フェールオーバー リンクに割り当ててはできません。</p> <p>(注) ステートフル フェールオーバー リンクがフェールオーバー リンクまたはデータ インターフェイスを使用する場合は、この手順をスキップします。インターフェイスのアクティブおよびスタンバイ IP アドレスは、すでに定義しています。</p> <p>スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。スタンバイ アドレスのサブネット マスクを指定する必要はありません。</p> <p>ステートフル フェールオーバー リンク IP アドレスおよび MAC アドレスは、データ インターフェイスを使用しない限り、フェールオーバー時に変更されません。アクティブ IP アドレスは、常にプライマリ装置にあります。スタンバイ IP アドレスは、セカンダリ装置にあります。</p>

	コマンド	目的
ステップ7	<pre>interface interface_id no shutdown</pre> <p>例:</p> <pre>hostname(config)# interface vlan100 hostname(config-if)# no shutdown</pre>	<p>(任意) インターフェイスをイネーブルにします。</p> <p>ステートフル フェールオーバー リンクがフェールオーバー リンクまたはデータ インターフェイスを使用する場合は、この手順をスキップします。インターフェイスは、すでにイネーブルです。</p>
ステップ8	<pre>failover</pre> <p>例:</p> <pre>hostname(config)# failover</pre>	<p>フェールオーバーをイネーブルにします。</p>
ステップ9	<pre>copy running-config startup-config</pre> <p>例:</p> <pre>hostname(config)# copy running-config startup-config</pre>	<p>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。</p>

セカンダリ装置の設定



セカンダ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 インターフェイス用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。

前提条件

LAN ベースのフェールオーバーを設定するときは、セカンダリ デバイスがプライマリ デバイスから実行コンフィギュレーションを取得する前に、セカンダリ デバイスをブートストラップしてフェールオーバー リンクを認識させる必要があります。

手順の詳細

セカンダリ装置を設定するには、次の手順を実行します。

コマンド	目的
<p>ステップ1 <code>failover lan interface if_name interface_id</code></p> <p>例: hostname(config)# failover lan interface folink vlan100</p>	<p>フェールオーバー インターフェイスとして使用するインターフェイスを指定します。プライマリ装置に使用したものと同一設定を使用します。</p> <p><code>if_name</code> 引数は、<code>interface_id</code> 引数で指定されたインターフェイスに名前を割り当てます。</p> <p>インターフェイス ID は、物理インターフェイスまたは冗長インターフェイスにすることができます。EtherChannel インターフェイスはサポートされていません。</p>
<p>ステップ2 <code>failover interface ip if_name [ip_address mask standby ip_address ipv6_address/prefix standby ipv6_address]</code></p> <p>例: hostname(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2 hostname(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby 2001:a0a:b00::a0a:b71</p>	<p>アクティブおよびスタンバイ IP アドレスをフェールオーバー リンクに割り当てます。IPv4 アドレスまたは IPv6 アドレスのいずれかをインターフェイスに割り当てることができます。両方のアドレス タイプをフェールオーバー リンクに割り当ててはできません。</p> <p>フェールオーバー ペアの両方の装置からパケットを受信するには、すべてのインターフェイスにスタンバイ IP アドレスを設定する必要があります。</p> <p> (注) プライマリ装置にフェールオーバー インターフェイスを設定する場合 (同じ IP アドレスを含む)、プライマリ装置でこのコマンドを入力するときは、正確に入力してください。</p>
<p>ステップ3 <code>interface interface_id</code></p> <p><code>no shutdown</code></p> <p>例: hostname(config)# interface vlan100 hostname(config-if)# no shutdown</p>	<p>インターフェイスをイネーブルにします。</p>
<p>ステップ4 <code>failover lan unit secondary</code></p> <p>例: hostname(config)# failover lan unit secondary</p>	<p>(任意) この装置をセカンダリ装置に指定します。</p> <p> (注) 以前に設定されていない場合、装置はデフォルトでセカンダリに指定されているので、この手順はオプションです。</p>

	コマンド	目的
ステップ 5	<code>failover</code> 例： <code>hostname(config)# failover</code>	フェールオーバーをイネーブルにします。 フェールオーバーをイネーブルにすると、実行メモリのコンフィギュレーションがアクティブ装置からスタンバイ装置に送信されます。コンフィギュレーションが同期すると、メッセージ「Beginning configuration replication: Sending to mate」および「End Configuration Replication to mate」がアクティブ装置のコンソールに表示されます。
ステップ 6	<code>copy running-config startup-config</code> 例： <code>hostname(config)# copy running-config startup-config</code>	コンフィギュレーションをフラッシュ メモリに保存します。 実行コンフィギュレーションの複製が完了した後で、コマンドを入力します。

オプションのアクティブ/スタンバイ フェールオーバー設定値の設定

この項は、次の内容で構成されています。

- 「ステートフル フェールオーバーでの HTTP 複製のイネーブル化」 (P.8-14)
- 「インターフェイス モニタリングのディセーブル化とイネーブル化」 (P.8-15)
- 「フェールオーバー基準の設定」 (P.8-16)
- 「装置およびインターフェイスのヘルス ポーリング時間の設定」 (P.8-16)
- 「仮想 MAC アドレスの設定」 (P.8-17)

フェールオーバー ペアのプライマリ装置を最初に設定する（「[プライマリ装置の設定](#)」 (P.8-9) を参照）場合、または、初期コンフィギュレーションの後でフェールオーバー ペアのアクティブ装置を設定する場合は、オプションのアクティブ/スタンバイ フェールオーバーを設定できます。

ステートフル フェールオーバーでの HTTP 複製のイネーブル化

HTTP 接続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含まれません。

ステートフル フェールオーバーがイネーブルの場合に、HTTP ステート複製をイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

コマンド	目的
<code>failover replication http</code> 例： <code>hostname (config)# failover replication http</code>	HTTP ステート複製をイネーブルにします。

インターフェイス モニタリングのディセーブル化とイネーブル化

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

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

インターフェイス ポーリング頻度ごとに、ASA フェールオーバー ペア間で hello メッセージが交換されます。フェールオーバー インターフェイスのポーリング時間は 3 ~ 15 秒です。たとえば、ポーリング時間を 5 秒に設定すると、あるインターフェイスで 5 回連続して hello が検出されないと (25 秒間)、そのインターフェイスでテストが開始します。

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

- **Unknown** : 初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- **Normal** : インターフェイスはトラフィックを受信しています。
- **Testing** : ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- **Link Down** : インターフェイスまたは VLAN は管理のためにダウンしています。
- **No Link** : インターフェイスの物理リンクがダウンしています。
- **Failed** : インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

シングル コンフィギュレーション モードの装置の特定の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セーブルにするには、次のいずれかのコマンドを入力します。また、マルチ コンフィギュレーション モードの装置の場合は、各セキュリティ コンテキスト内で次のコマンドを入力する必要があります。

次のいずれかを実行します。

no monitor-interface *if_name*

インターフェイスのヘルス モニタリングをディセーブルにします。

例 :

```
hostname(config)# no monitor-interface
lanlink
```

monitor-interface *if_name*

インターフェイスのヘルス モニタリングをイネーブルにします。

例 :

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

フェールオーバー基準の設定

インターフェイス数またはモニタされているインターフェイスの割合を指定して、この数または割合を超えたインターフェイスに障害が発生した場合にフェールオーバーが発生するようにできます。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。

デフォルトのフェールオーバー基準を変更するには、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。

コマンド	目的
<code>failover interface-policy num[%]</code>	デフォルトのフェールオーバー基準を変更します。
例 : <code>hostname (config)# failover interface-policy 20%</code>	インターフェイスの具体的な数を指定するときは、 <i>num</i> 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、 <i>num</i> 引数に 1 ~ 100 を設定できます。

装置およびインターフェイスのヘルス ポーリング時間の設定

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

ポーリング時間および保持時間を短縮すると、ASA はインターフェイスの障害に対してより迅速な検出と応答を実行できますが、多くのシステム リソースを消費することがあります。ポーリング時間と保持時間を延長すると、ASA がネットワーク上でフェールオーバーし、長時間の遅延が発生するのを防止できます。

コマンド	目的
<pre>failover polltime interface [msec] time [holdtime time]</pre> <p>例:</p> <pre>hostname (config): failover polltime interface msec 500 holdtime 5</pre>	<p>インターフェイスのポーリング時間と保持時間を変更します。</p> <p>ポーリング時間の有効な値は 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。</p> <p>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。</p>
<pre>failover polltime [unit] [msec] poll_time [holdtime [msec] time]</pre> <p>例:</p> <pre>hostname(config)# failover polltime unit msec 200 holdtime msec 800</pre>	<p>装置のポーリング時間と保持時間を変更します。</p> <p>ユニットのポーリング タイムの 3 倍未満の値を holdtime の値として入力することはできません。ポーリング時間が短いほど、ASA は短時間で故障を検出し、フェールオーバーをトリガーできます。ただし短時間での検出は、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。</p> <p>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。</p> <p>コンフィギュレーションには、failover polltime [unit] コマンドと failover polltime interface コマンドの両方を含めることができます。</p>

仮想 MAC アドレスの設定

アクティブ/スタンバイ フェールオーバーでは、プライマリ装置の MAC アドレスは常にアクティブ IP アドレスに関連付けられています。セカンダリ装置は、最初にブートされてアクティブになると、そのインターフェイスの焼き付け済み MAC アドレスを使用します。プライマリ装置がオンラインになると、セカンダリ装置はプライマリ装置から MAC アドレスを取得します。この変更によって、ネットワーク トラフィックが中断することがあります。

各インターフェイスに仮想 MAC アドレスを設定して、セカンダリ装置がプライマリ装置よりも前にオンラインになっても、セカンダリ装置がアクティブ装置である場合、正しい MAC アドレスを使用するようにします。仮想 MAC アドレスを使用しない場合、フェールオーバー ペアは焼き付け済み NIC アドレスを MAC アドレスとして使用します。



(注)

フェールオーバーまたはステートフル フェールオーバー リンクには、仮想 MAC アドレスは設定できません。これらのリンクの MAC アドレスおよび IP アドレスは、フェールオーバー中に変更されません。

インターフェイスの仮想 MAC アドレスを設定するには、アクティブ装置で次のコマンドを入力します。

■ フェールオーバーの制御

コマンド	目的
<pre>failover mac address phy_if active_mac standby_mac</pre> <p>例:</p> <pre>hostname (config): failover mac address Ethernet0/2 00a0.c969.87c8 00a0.c918.95d8</pre>	<p>インターフェイスの仮想 MAC アドレスを設定します。</p> <p><i>phy_if</i> 引数は、インターフェイスの物理名 (Ethernet1 など) です。 <i>active_mac</i> および <i>standby_mac</i> 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。</p> <p><i>active_mac</i> 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、<i>standby_mac</i> 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。</p> <p>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。</p> <p>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。</p>

フェールオーバーの制御

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

- 「フェールオーバーの強制実行」(P.8-18)
- 「フェールオーバーのディセーブル化」(P.8-18)
- 「障害が発生した装置の復元」(P.8-19)

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、次のいずれかのコマンドを入力します。

コマンド	目的
<pre>failover active</pre> <p>例:</p> <pre>hostname# failover active</pre>	<p>フェールオーバー ペアのスタンバイ装置で入力された場合に、フェールオーバーを強制実行します。スタンバイ装置はアクティブ装置になります。</p>
<pre>no failover active</pre> <p>例:</p> <pre>hostname# no failover active</pre>	<p>フェールオーバー ペアのアクティブ装置で入力された場合に、フェールオーバーを強制実行します。アクティブ装置はスタンバイ装置になります。</p>

フェールオーバーのディセーブル化

フェールオーバーをディセーブル化するには、次のコマンドを入力します。

コマンド	目的
no failover 例: hostname (config) # no failover	フェールオーバーをディセーブルにします。アクティブ/スタンバイ ペアでフェールオーバーをディセーブルにすると、再起動され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。たとえば、スタンバイ装置はスタンバイ 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。(フェールオーバーがディセーブル化されていても) スタンバイ装置をアクティブにするには、「 フェールオーバーの強制実行 」(P.8-18) を参照してください。

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、次のコマンドを入力します。

コマンド	目的
failover reset 例: hostname (config) # failover reset	障害が発生したユニットを障害が発生していない状態に復元します。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、フェールオーバー(強制または性質)によってアクティブになるまではスタンバイ状態のままです。

フェールオーバー機能のテスト

フェールオーバー機能をテストするには、次の手順を実行します。

- ステップ 1** FTP などを使用して、異なるインターフェイス上のホスト間でファイルを送信し、アクティブ装置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。
hostname (config) # **no failover active**
- 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。
hostname (config) # **no failover active**



(注)

ASA のインターフェイスの 1 つがダウンしたときも、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。

アクティブ/スタンバイ フェールオーバーのモニタリング



(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。ASDM がデバイスから切断されて再接続されるとモニタリング接続が再確立されないため、このアクションが必要になります。

アクティブ/スタンバイ フェールオーバーをモニタするには、次のいずれかのコマンドを入力します。

コマンド	目的
<code>show failover</code>	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。
<code>show monitor-interface</code>	モニタ対象インターフェイスの情報を表示します。
<code>show running-config failover</code>	実行コンフィギュレーション内のフェールオーバー コマンドを表示します。

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

アクティブ/スタンバイ フェールオーバーの機能履歴

表 8-2 に、この機能のリリース履歴を示します。

表 8-2 オプションのアクティブ/スタンバイ フェールオーバー設定の機能履歴

機能名	リリース	機能情報
この機能が導入されました。	7.0	この機能が導入されました。
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)	<code>failover interface ip</code> 、 <code>show failover</code> 、 <code>ipv6 address</code> 、 <code>show monitor-interface</code> の各コマンドが変更されました。