

PIX/ASA : アクティブ/アクティブ フェールオーバーの設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[表記法](#)

[アクティブ/アクティブ フェールオーバー](#)

[アクティブ/アクティブ フェールオーバーの概要](#)

[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](#)

[デバイスの初期化と設定の同期](#)

[コマンドの複製](#)

[フェールオーバー トリガ](#)

[フェールオーバー アクション](#)

[標準およびステートフル フェールオーバー](#)

[標準フェールオーバー](#)

[ステートフル フェールオーバー](#)

[フェールオーバー設定の制限項目](#)

[サポートされない機能](#)

[ケーブルベースでのアクティブ/アクティブ フェールオーバーの設定](#)

[前提条件](#)

[ネットワーク図](#)

[設定](#)

[LAN ベースでのアクティブ/アクティブ フェールオーバーの設定](#)

[ネットワーク図](#)

[プライマリ ユニットの設定](#)

[セカンダリ ユニットの設定](#)

[設定](#)

[確認](#)

[show failover コマンドの使用](#)

[監視対象インターフェイスの表示](#)

[実行コンフィギュレーションでのフェールオーバー コマンドの表示](#)

[フェールオーバー機能のテスト](#)

[強制フェールオーバー](#)

[フェールオーバーの無効化](#)

[障害ユニットの復元](#)

[障害が発生したユニットの新しいユニットとの交換](#)

[トラブルシューティング](#)

[フェールオーバーのシステム メッセージ](#)

[Primary Lost Failover communications with mate on interface interface_name \(プライマリで、インターフェイス interface_name のペアの相手とのフェールオーバー通信が失われた\)](#)

[デバッグ メッセージ](#)

[SNMP](#)

[フェールオーバー ポーリング時間](#)

[WARNING: フェールオーバー メッセージの複合化に失敗しました。](#)

[関連情報](#)

概要

フェールオーバーの設定には、専用のフェールオーバー リンクおよび必要に応じて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た2つのまったく同じセキュリティ アプライアンスが必要です。アクティブなインターフェイスとユニットのヘルスを監視することにより、特定のフェールオーバー条件を満たすかどうか判定されます。これらの条件が満たされると、フェールオーバーが発生します。

セキュリティ アプライアンスでは、**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**という2種類のフェールオーバー構成がサポートされています。各フェールオーバー設定には、フェールオーバーを決定して実行する固有の方法があります。アクティブ/アクティブ フェールオーバーの場合は、どちらのユニットもネットワークトラフィックを渡すことができます。これにより、ネットワークにロード バランシングを設定できます。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 モードで稼働するユニットでのみ使用できます。アクティブ/スタンバイ フェールオーバーの場合は、一方のユニットのみがトラフィックを渡すことができ、もう一方のユニットはスタンバイ状態で待機します。アクティブ/スタンバイ フェールオーバーは、シングル コンテキスト モードかマルチ コンテキスト モードのどちらで稼働するユニットでも使用できます。どちらのフェールオーバー設定でも、ステートフルフェールオーバーまたはステートレス (標準) フェールオーバーがサポートされます。

このドキュメントでは、Cisco PIX/ASA セキュリティ アプライアンスでの**アクティブ/アクティブ**フェールオーバーの設定方法に焦点を当てています。

アクティブ/スタンバイ フェールオーバー構成に関する詳細は、『[PIX/ASA 7.x アクティブ/スタンバイ フェールオーバーの設定例](#)』を参照してください。

注: マルチ コンテキスト では VPN はサポートされていないので、VPN フェールオーバーは、マルチ コンテキスト モードで稼働するユニットではサポートされていません。VPN フェールオーバーは、シングル コンテキスト 構成の**アクティブ/スタンバイ**設定でだけ利用できます。

このコンフィギュレーション ガイドでは、サンプル設定でPIX/ASA 7.x **アクティブ/アクティブ**テクノロジーを手短に紹介しています。このテクノロジーの基盤となる理論の詳細は、『[Cisco セキュリティ アプライアンス コマンド リファレンス、バージョン 7.2](#)』を参照してください。

前提条件

要件

ハードウェア要件

フェールオーバー設定に含める 2 台のユニットは、ハードウェア構成が同じである必要があります。同じモデル、同じ数と種類のインターフェイス、さらに同じ大きさの RAM が使用されている必要があります。

注: 2 台のユニットのフラッシュメモリのサイズは同一である必要はありません。フェールオーバー設定内でフラッシュメモリサイズが異なるユニットを使用する場合は、フラッシュメモリサイズが小さい方のユニットに、ソフトウェアイメージファイルおよび設定ファイルを格納するのに十分な領域があることを確認してください。十分な領域がない場合、フラッシュメモリサイズの大きい方のユニットから小さい方のユニットへの設定の同期が失敗します。

ソフトウェア要件

フェールオーバー設定に含める 2 台のユニットは、動作モード (ルーテッドまたはトランスペアレント、シングルまたはマルチ コンテキスト) が同じである必要があります。両方のユニットでは、メジャー (1 番目の番号) とマイナー (2 番目の番号) ソフトウェアバージョンが同じである必要がありますが、アップグレードプロセスの間は、異なるバージョンのソフトウェアを使用できます。たとえば、1 つのユニットをバージョン 7.0(1) からバージョン 7.0(2) にアップグレードしても、フェールオーバーをアクティブに保つことができます。ただし、長期的な互換性を保つため、両方のユニットを同じバージョンにアップグレードすることを推奨します。

フェールオーバー ペア上でのソフトウェアのアップグレードについての詳細は、『[ダウンタイムを発生させないフェールオーバー ペアのアップグレードの実行](#)』を参照してください。

ライセンス要件

PIX/ASA セキュリティ アプライアンス プラットフォームでは、最低限、一方のユニットに無制限 (UR) ライセンスが必要です。他方のユニットには、Failover Only Active-Active (FO_AA) ライセンス、あるいは別の UR ライセンスが必要です。制限付きライセンスのあるユニットはフェールオーバーには使用できず、FO_AA ライセンスのある 2 台のユニットをフェールオーバー ペアとして一緒に使用することはできません。

注: 追加の機能と利点を取得するには、フェールオーバー ペア上のライセンスのアップグレードが必要になる場合があります。アップグレードについての詳細は、『[フェールオーバーペア上のライセンス キー アップグレード](#)』を参照してください。

注: SSL VPN ピアやセキュリティ コンテキストなどのフェールオーバーに關与する両方のセキュリティ アプライアンス上のライセンス済み機能は、同一である必要があります。

注: FO ライセンスはアクティブ/アクティブ フェイルオーバーをサポートしません。

[使用するコンポーネント](#)

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- PIX セキュリティ アプライアンス バージョン 7.x 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

[関連製品](#)

この設定は、次のバージョンのハードウェアとソフトウェアにも使用できます。

- 7.x バージョン以降がインストールされた ASA

注: ASA 5505 シリーズ 適応型セキュリティ アプライアンスでは、アクティブ/アクティブ フェールオーバーは使用できません。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

アクティブ/アクティブ フェールオーバー

このセクションではアクティブ/スタンバイ フェールオーバーについて説明されており、次のトピックが含まれています。

- [アクティブ/アクティブ フェールオーバーの概要](#)
- [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](#)
- [デバイスの初期化と設定の同期](#)
- [コマンドの複製](#)
- [フェールオーバートリガ](#)
- [フェールオーバー アクション](#)

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 フェールオーバーを利用できるのは、マルチ コンテキスト モードのセキュリティ アプライアンスだけです。アクティブ/アクティブ フェールオーバーでは、どちらのセキュリティ アプライアンスでもネットワーク トラフィックを通過させられます。

アクティブ/アクティブ フェールオーバーでは、セキュリティ アプライアンス上のセキュリティ コンテキストをフェールオーバー グループに分割します。フェールオーバー グループとは、端的には 1 つ以上のセキュリティ コンテキストの論理グループです。セキュリティ アプライアンスにはフェールオーバー グループを 2 つまで作成できます。管理コンテキストは常にフェールオーバー グループ 1 のメンバになります。デフォルトでは、未割り当てのセキュリティ コンテキストもすべてフェールオーバー グループ 1 のメンバになります。

アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループがフェールオーバーの基本単位となります。インターフェイス障害モニタリング、フェールオーバー、およびアクティブ/スタンバイ ステータスは、すべてユニットではなくフェールオーバー グループの属性です。アクティブ側のフェールオーバー グループに障害が発生するとスタンバイ ステータスに変わり、一方で、スタンバイ側のフェールオーバー グループがアクティブになります。アクティブになるフェールオーバー グループのインターフェイスでは、障害が発生したフェールオーバー グループのインターフェイスの MAC アドレスと IP アドレスが引き継がれます。ここでスタンバイステートになったフェールオーバー グループのインターフェイスでは、スタンバイ側の MAC アドレスと IP アドレスが引き継がれます。

注: ユニットでのフェールオーバー グループの障害は、ユニットそのものに障害が発生しているわけではありません。ユニットには、トラフィックを通過させている別のフェールオーバー グループが備わっている場合があります。

[プライマリ/セカンダリ ステータスとアクティブ/スタンバイ ステータス](#)

アクティブ/スタンバイ フェールオーバーにおけるように、アクティブ/アクティブ フェールオーバー ペアの一方向のユニットがプライマリ ユニットになり、他方のユニットがセカンダリ ユニットになります。アクティブ/スタンバイ フェールオーバーとは異なり、この割り当ては、両方のユニットが同時に起動した場合にどちらのユニットがアクティブになるかということを示しているわけではありません。この場合、プライマリ/セカンダリの割り当てでは、次の2つの操作が行われます。

- 両方のユニットが同時に起動した際に、ペアに対してどちらのユニットが実行コンフィギュレーションを提供するかを判定する。
- 両方のユニットが同時に起動した際に、どのユニットで各フェールオーバー グループがアクティブ ステートとなるかを判定する。構成内の各フェールオーバー グループがプライマリかセカンダリのユニット プリファレンスに設定される。ペア内の一方向の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 ステートに設定できます。この場合、他方のユニットにはスタンバイ ステートのフェールオーバー グループが含まれます。ところが、さらに一般的な設定では、各フェールオーバー グループに異なるロール プリファレンスが割り当てられ、それぞれが他のユニットでアクティブにされます。これにより、各デバイスにトラフィックが分散されます。注: セキュリティ アプライアンスでは、ロード バランシング サービスは提供されません。ロード バランシングは、セキュリティ アプライアンスにトラフィックを受け渡すルータで処理される必要があります。

どのユニットで各フェールオーバー グループがアクティブになるかは、次のように判定されます。

- ユニットが起動した際にピア ユニットが利用できない場合、そのユニットでは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。
- ユニットが起動した際にピア ユニットがアクティブの場合 (両方のフェールオーバー グループがアクティブ ステート)、フェールオーバー グループのプリファレンスがプライマリかセカンダリかにかかわらず、次のいずれかの事象が発生するまでは、アクティブ ユニットではフェールオーバー グループがアクティブ ステートのままになります。フェールオーバーが発生する。no failover active コマンドにより、手動でフェールオーバー グループを他方のユニットに強制的に割り当てる。preempt コマンドでフェールオーバー グループを設定しており、優先ユニットでは、ユニットが利用可能になった時点で、そのフェールオーバー グループが自動的にアクティブになる。
- 両方のユニットが同時に起動する際に、設定の同期が行われた後で、優先ユニットで各フェールオーバー グループがアクティブになります。

デバイスの初期化と設定の同期

フェールオーバー ペアの一方向あるいは両方のユニットが起動した際に、設定の同期が行われます。設定の同期は次のように行われます。

- ユニットが起動した際にピア ユニットがアクティブの場合 (ユニットで両方のフェールオーバー グループがアクティブ)、プライマリかセカンダリかにかかわらず、起動ユニットからアクティブ ユニットにコンタクトして実行コンフィギュレーションが取得されます。
- 両方のユニットが同時に起動すると、セカンダリ ユニットでは、プライマリ ユニットから実行コンフィギュレーションが取得されます。

複製が始まると、コンフィギュレーションを送信しているユニットのセキュリティ アプライアンス 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「End Configuration Replication to mate」というメッセージが表示されます。複製中は、コンフィギュレーション送信側のユニットに入力されたコマンドはピアユニットに適

切に複製されない可能性があり、コンフィギュレーション受信側のユニットに入力されたコマンドは受信中のコンフィギュレーションで上書きされる可能性があります。コンフィギュレーションの複製プロセス中は、フェールオーバー ペアのいずれのユニットでもコマンドを入力しないようにしてください。コンフィギュレーションのサイズによって、複製に数秒から数分かかる場合があります。

コンフィギュレーション受信側のユニットで、そのコンフィギュレーションが存在するのは実行メモリ上だけです。同期完了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、アクティブ ステートのフェールオーバー グループ 1 のあるユニット上のシステム実行スペースで **write memory all** コマンドを入力します。このコマンドはピア ユニットに複製され、そこでコンフィギュレーションのフラッシュ メモリへの書き出しが実行されます。このコマンドに **all** キーワードを使用すると、システム コンフィギュレーション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全体のユニットからアクセスできるので、ユニットごとに個別に保存する必要はありません。代替策として、コンテキスト コンフィギュレーション ファイルをプライマリ ユニットのディスクから外部サーバにコピーしておいてから、セカンダリ ユニットのディスクにコピーすることができます。ユニットをリロードすると、コピーしたコンテキスト コンフィギュレーション ファイルを使用できるようになります。

コマンドの複製

両方のユニットが稼働すると、次のように、一方のユニットから他方のユニットにコマンドが複製されます。

- セキュリティ コンテキストに入力されたコマンドは、セキュリティ コンテキストがアクティブ ステートになっているユニットからピア ユニットに複製されます。注: ユニット上で所属するフェールオーバー グループがアクティブ ステートになっている場合、そのユニットのコンテキストがアクティブ ステートであると見なされます。
- システム実行スペースで入力されたコマンドは、フェールオーバー グループ 1 がアクティブ ステートになっているユニットから、フェールオーバー グループ 1 がスタンバイ ステートになっているユニットに複製されます。
- 管理コンテキストで入力されたコマンドは、フェールオーバー グループ 1 がアクティブ ステートになっているユニットから、フェールオーバー グループ 1 がスタンバイ ステートになっているユニットに複製されます。

設定コマンドとファイル コマンド (**copy**、**rename**、**delete**、**mkdir**、**rmdir** など) はすべて複製されますが、次の例外があります。 **show**、**debug**、**mode**、**firewall**、**failover lan unit** コマンドは複製されません。

コマンド複製のための適切なユニットでのコマンドの入力に失敗すると、設定の同期が崩れます。これらの変更は失われ、次回には初期設定の同期が実行されます。

同期が崩れた設定を再度同期させるには、**write standby** コマンドを使用できます。アクティブ /アクティブ フェールオーバーの場合、**write standby** コマンドは次のように機能します。

- システム実行スペースで **write standby** コマンドを入力すると、セキュリティ アプライアンス上のシステム設定とセキュリティ コンテキストのすべての設定がピア ユニットに書き出されます。これには、スタンバイ ステートになっているセキュリティ コンテキストの設定情報が含まれています。アクティブ ステートのフェールオーバー グループ 1 があるユニットのシステム実行スペースで、コマンドを入力する必要があります。注: ピア ユニットでアク

タイプ ステートになっているセキュリティ コンテキストがある場合は、これらのコンテキストによるアクティブな接続が **write standby** コマンドにより終了されます。 **write standby** コマンドを入力する前に、設定を提供するユニットで **failover active** コマンドを使用して、ユニットですべてのコンテキストがアクティブになっていることを確認してください。

- あるセキュリティ コンテキストで **write standby** コマンドを入力すると、そのセキュリティ コンテキストの設定だけがピア ユニットに書き出されます。セキュリティ コンテキストがアクティブ ステートになっているユニットのセキュリティ コンテキストで、コマンドを入力する必要があります。

ピア ユニットへの複製時には、複製されたコマンドはフラッシュ メモリには保存されません。複製されたコマンドは実行コンフィギュレーションに追加されます。両方のユニットで複製されたコマンドをフラッシュ メモリに保存するためには、変更したユニットで **write memory** コマンドか **copy running-config startup-config** コマンドを使用します。このコマンドはピア ユニットに複製され、ピア ユニット上のフラッシュ メモリへのコンフィギュレーションの書き出しが実行されます。

フェールオーバー トリガ

アクティブ/アクティブ フェールオーバーでは、次の条件のいずれかが発生すると、ユニットレベルでフェールオーバーがトリガーされる可能性があります。

- ユニットにハードウェア障害がある。
- ユニットに電源障害がある。
- ユニットにソフトウェア障害がある。
- **no failover active** コマンドか **failover active** コマンドがシステム実行スペースで入力された。

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

- グループ内で障害が発生したモニタリング対象のインターフェイスが多すぎる。
- **no failover active group group_id** コマンドか **failover active group group_id** コマンドが入力された。

フェールオーバー アクション

アクティブ/アクティブ フェールオーバー構成では、フェールオーバーはシステム ベースではなくフェールオーバー グループ ベースで発生します。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に割り当てている場合、フェールオーバー グループ 1 で障害が発生すると、プライマリ ユニットではフェールオーバー グループ 2 がアクティブのまま残り、セカンダリ ユニットではフェールオーバー グループ 1 がアクティブになります。

注: アクティブ/アクティブ フェールオーバーを設定する際には、両方のユニットに対するトラフィックを結合したものが各ユニットのキャパシティに収まることを確認してください。

次の表に、それぞれの障害イベントでのフェールオーバー アクションを示してあります。それぞれの障害イベントに対して、ポリシー (フェールオーバーを発生させるかどうか)、アクティブ フェールオーバー グループのアクション、スタンバイ フェールオーバー グループのアクションが示されています。

障害イベント	ポリシー	アクティブグループ	スタンバイグループ	注意事項
--------	------	-----------	-----------	------

	一	アクション	プ ア ク シ ヨ ン	
ユニットでの電源障害またはソフトウェア障害	フェールオーバー	スタンバイ移行。障害発生とマーキング。	スタンバイ移行。アクティブ障害してマークする	フェールオーバーペア内の一方のユニットに障害が発生すると、そのユニットではアクティブフェールオーバーグループがすべて障害発生とマーキングされ、ペアユニットでは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での基準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障害発生とマーキング。	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での基準を超えたインターフェイス障害	フェールオーバーなし	アクションなし	スタンバイグループに障害発生とマーキング。	スタンバイフェールオーバーグループが障害発生とマーキングされていると、インターフェイスの障害の基準を超えていても、アクティブフェールオーバーグループではフェールオーバーが試行されません。
以前のアクティブ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	アクションなし	アクションなし	preempt コマンドで設定されていない限り、現在のユニットでのフェールオーバーグループがアクティブのまま残ります。
起動時のフェールオーバーリンクの障害	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、両方のユニットのフェールオーバーグループがアクティブになります。

ステートフルフェールオーバーリンクの障害	フェールオーバーなし	アクションなし	アクションなし	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されます。
運用時のフェールオーバーリンクの障害	フェールオーバーなし	該当なし	該当なし	各ユニットでフェールオーバーインターフェイスが障害発生とマーキングされます。フェールオーバーリンクがダウンしている間は、ユニットではスタンバイユニットにフェールオーバーできないため、できるだけ早急にフェールオーバーリンクを復元する必要があります。

標準およびステートフルフェールオーバー

セキュリティ アプライアンスでは、標準とステートフルという 2 種類のフェールオーバーがサポートされています。ここでは次の項目について説明します。

- [標準フェールオーバー](#)
- [ステートフルフェールオーバー](#)

標準フェールオーバー

フェールオーバーが発生すると、すべてのアクティブな接続が終了されます。新しいアクティブユニットが引き継ぐ際に、クライアントで接続を再確立する必要があります。

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になっていると、アクティブユニットからスタンバイユニットに対して接続ごとのステート情報が継続的に引き渡されます。フェールオーバーが発生した後は、同じ接続情報を新しいアクティブユニットで使用できます。サポート対象のエンドユーザアプリケーションでは、同じ通信セッションを維持するために接続し直す必要はありません。

スタンバイユニットには次のようなステート情報が渡されます。

- NAT 変換テーブル
- TCP 接続状態
- UDP 接続状態
- ARP テーブル

- レイヤ 2 ブリッジ テーブル (透過ファイアウォール モードで稼働している場合)
- HTTP 接続状態 (HTTP 複製が有効になっている場合)
- ISAKMP および IPsec の SA テーブル
- GTP PDP 接続データベース

ステートフル フェールオーバーが有効になっていても、次の情報はスタンバイ ユニットには渡されません。

- HTTP 接続テーブル (HTTP 複製が有効になっていない場合)
- ユーザ認証 (uauth) テーブル
- ルーティング テーブル
- セキュリティ サービス モジュールのステート情報

注: アクティブな Cisco IP SoftPhone セッション中にフェールオーバーが発生すると、コール セッションのステート情報がスタンバイ ユニットに複製されるため、コールはアクティブのままになります。コールが終了すると、IP SoftPhone クライアントでは CallManager との接続が失われます。これが発生する理由は、スタンバイ ユニットには CTIQBE ハングアップ メッセージに関するセッション情報がないためです。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。

フェールオーバー設定の制限項目

次のタイプの IP アドレスではフェールオーバーを設定できません。

- DHCP で取得される IP アドレス
- PPPoE で取得される IP アドレス
- IPv6 形式のアドレス

さらに、次の制約があります。

- ASA 5505 適応型セキュリティ アプライアンスではステートフル フェールオーバーはサポートされていません。
- ASA 5505 適応型セキュリティ アプライアンスではアクティブ/アクティブ フェールオーバーはサポートされていません。
- ASA 5505 適応型セキュリティ アプライアンスで Easy VPN リモートが有効になっていると、フェールオーバーを設定できません。
- マルチ コンテキスト モードでは、VPN のフェールオーバーはサポートされていません。

サポートされない機能

マルチ コンテキスト モードでは、次の機能はサポートされていません。

- ダイナミック ルーティング プロトコルセキュリティ コンテキストでサポートされているのはスタティック ルートだけです。マルチ コンテキスト モードでは OSPF や RIP を有効にできません。
- VPN
- マルチキャスト

ケーブルベースでのアクティブ/アクティブ フェールオーバーの

設定

前提条件

はじめに、次を確認してください。

- 両方のユニットのハードウェア構成とソフトウェア構成が同じで、適切なライセンスがある。
- 両方のユニットのモード (シングルまたはマルチ、トランスペアレントまたはルーテッド) が同じ。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

フェールオーバー リンクとしてシリアル ケーブルを使用したアクティブ/アクティブ 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。このタスクでのコマンドは、フェールオーバーペアのプライマリ ユニットで入力します。プライマリ ユニットは、「Primary」というラベルが付いたケーブルの端が接続されているユニットです。マルチ コンテキスト モードのデバイスの場合、特に指示がない限り、コマンドはシステム実行スペースで入力します。

ケーブル ベースのフェールオーバーを使用する際には、フェールオーバー ペアのセカンダリ ユニットでブートストラップを実行する必要はありません。電源をオンにするようにとの指示が出るまでは、セカンダリ ユニットの電源はオフにしておきます。

注: ケーブルベースのフェールオーバーが利用可能なのは PIX 500 シリーズのセキュリティ アプライアンスだけです。

次の手順を実行して、ケーブルベースのアクティブ/アクティブ フェールオーバーを設定します。

1. フェールオーバー ケーブルを PIX 500 シリーズのセキュリティ アプライアンスに接続します。プライマリ ユニットとして使用するユニットに「Primary」とマーキングされたケーブル端が接続され、セカンダリ ユニットとして使用するユニットに「Secondary」とマーキングされたケーブル端が接続されていることを確認してください。
2. プライマリ ユニットの電源を入れます。
3. まだ設定していない場合は、アクティブ側とスタンバイ側の IP アドレスを、各データ インターフェイス (ルーテッド モード) 用、管理 IP アドレス (トランスペアレント モード) 用、あるいは管理専用インターフェイス用に設定します。スタンバイ IP アドレスは、現在スタンバイ ユニットであるセキュリティ アプライアンスで使用されます。これはアクティブ IP アドレスと同じサブネットにある必要があります。インターフェイス アドレスは、各コンテキスト内で設定する必要があります。コンテキストを切り替えるには、**changeto context** コマンドを使用します。コマンド プロンプトが `hostname/context(config-if)#` に変わります。ここでは、context が現在のコンテキストの名前になります。トランスペアレント ファイアウォール マルチ コンテキスト モードの各コンテキストの管理 IP アドレスを入力する必要があります。注: 専用ステートフル フェールオーバー インターフェイスを使用する場合は、ステートフル フェールオーバー リンクの IP アドレスは設定できません。専用ステートフル フェールオーバー インターフェイスを設定するには、後のステップで **failover interface ip** コマンドを使用します。`hostname/context(config-if)#ip address active_addr netmask standby standby_addr` この例では、プライマリ PIX の context1 に対する Outside イ

インターフェイスは次のように設定されています。PIX1/context1(config)#ip address

```
172.16.1.1 255.255.255.0 standby 172.16.1.2 context2
```

 については、次のようになります。

PIX1/context2(config)#ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2 ルーテッドファイアウォールモードでは、管理専用インターフェイスに関して、このコマンドは各インターフェイスに対してインターフェイス コンフィギュレーション モードで入力されます。トランスペアレント ファイアウォールモードでは、このコマンドはグローバル コンフィギュレーション モードで入力されます。

4. ステートフル フェールオーバーを有効にするには、ステートフル フェールオーバー リンクを設定します。ステートフル フェールオーバー リンクとして使用されるインターフェイスを指定します。hostname(config)#failover link if_name phy_if 次の例では、Ethernet2 インターフェイスを使用して、ステートフル フェールオーバー リンクのステート情報が交換されます。failover link stateful Ethernet2if_name 引数では、phy_if 引数で指定されているインターフェイスに論理名が割り当てられます。phy_if 引数には Ethernet1 のような物理ポート名を指定できますが、Ethernet0/2.3 のような事前に作成されたサブインターフェイスを指定することもできます。このインターフェイスは、(オプションでのフェールオーバーリンクを除いて) 他の目的に使用することはできません。次のように、ステートフル フェールオーバー リンクにアクティブとスタンバイの IP アドレスを割り当てます。

hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr 次の例では、ステートフル フェールオーバー リンクのアクティブ IP アドレスとして 10.0.0.1 が使用され、スタンバイ IP アドレスとして 10.0.0.2 が使用されています。PIX1(config)#failover

```
interface ip stateful 10.0.0.1 255.255.255.0 standby 10.0.0.2
```

 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内にある必要があります。スタンバイ IP アドレスのサブネット マスクの識別は不要です。ステートフル フェールオーバーで標準のデータインターフェイスが使用されている場合を除いて、フェールオーバーの際にステートフル フェールオーバー リンクの IP アドレスと MAC アドレスは変わりません。アクティブ IP アドレスは常にプライマリ ユニットに存在し、スタンバイ IP アドレスはセカンダリ ユニットに存在します。インターフェイスを有効にします。hostname(config)#interface phy_if
hostname(config-if)#no shutdown

5. フェールオーバー グループを設定します。フェールオーバー グループは 2 つまで持てます。フェールオーバー グループが存在しない場合、failover group コマンドにより指定のフェールオーバー グループが作成され、フェールオーバー グループ コンフィギュレーション モードに入ります。各フェールオーバー グループについて、primary コマンドか secondary コマンドを使用して、そのフェールオーバー グループの優先度がプライマリなのかセカンダリなのかを指定する必要があります。両方のフェールオーバー グループに同じ優先度を割り当てられます。ただし、ロード バランシングの設定のためには、各フェールオーバー グループに異なるユニット優先度を割り当てる必要があります。次の例では、failover group 1 にプライマリ優先度を割り当て、failover group 2 にセカンダリ優先度を割り当てています。

```
hostname(config)#failover group 1 hostname(config-fover-group)#primary hostname(config-fover-group)#exit hostname(config)#failover group 2 hostname(config-fover-group)#secondary hostname(config-fover-group)#exit
```

6. コンテキスト コンフィギュレーション モードで join-failover-group コマンドを使用して、フェールオーバー グループに各ユーザ コンテキストを割り当てます。未割り当てのコンテキストは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 のメンバになります。次のコマンドを入力して、フェールオーバー グループに各コンテキストを割り当てます。hostname(config)#context context_name
hostname(config-context)#join-failover-group {1 | 2} hostname(config-context)#exit

7. フェールオーバーを有効にします。hostname(config)#failover

8. セカンダリ ユニットの電源を入れ、まだ有効になっていない場合はセカンダリ ユニットでフェールオーバーを有効にします。hostname(config)#failover アクティブ ユニットから実行

メモリ内のコンフィギュレーションがスタンバイユニットに送信されます。コンフィギュレーションの同期が行われて、プライマリ コンソールに「Beginning configuration replication: Sending to mate」および「End Configuration Replication to mate」というメッセージが表示されます。注: まず、プライマリ デバイスで **failover** コマンドを発行し、次にセカンダリ デバイスで発行します。セカンダリ デバイス上で **failover** コマンドを発行した後、セカンダリ デバイスでは即座にプライマリ デバイスからコンフィギュレーションが取得され、スタンバイとしてセカンダリ デバイス自体が設定されます。プライマリ ASA はアップしたままであり、トラフィックの受け渡しが正常に行われます。そのため、プライマリ ASA 自体がアクティブデバイスとしてマークされます。この時点以降、アクティブ デバイス上で障害が発生する場合は、常にスタンバイ デバイスがアクティブになります。

9. プライマリ ユニットのフラッシュ メモリにコンフィギュレーションを保存します。プライマリ ユニットで入力されたコマンドはセカンダリ ユニットに複製されるので、セカンダリ ユニットでもコンフィギュレーションがフラッシュ メモリに保存されます。

```
hostname(config)#copy running-config startup-config
```

10. 必要な場合は、プライマリ側でアクティブなフェールオーバー グループをすべて、セカンダリ側で強制的にアクティブ ステートにします。セカンダリ ユニットでフェールオーバー グループを強制的にアクティブにするには、プライマリ ユニットのシステム実行スペースで次のコマンドを発行します。hostname#no failover active group group_id group_id 引数には、セカンダリ ユニットでアクティブにするグループを指定します。

設定

このドキュメントでは、次の設定を使用します。

- [PIX1 - システム設定](#)
- [PIX1 - Context1 の設定](#)
- [PIX1 - Context2 の設定](#)

PIX1 - システム設定

```
PIX1#show running-config : Saved PIX Version 7.2(2)
<system> ! hostname PIX1 enable password
8Ry2YjIyt7RRXU24 encrypted no mac-address auto !---
Enable the physical and logical interfaces in the system
execution !--- space by giving "no shutdown" before
configuring the same in the contexts ! interface
Ethernet0 ! interface Ethernet0.1 vlan 2 ! interface
Ethernet0.2 vlan 4 ! interface Ethernet1 ! interface
Ethernet1.1 vlan 3 ! interface Ethernet1.2 vlan 5 ! !---
Configure "no shutdown" in the stateful failover
interface !--- of both Primary and secondary PIX.
interface Ethernet2 description STATE Failover Interface
! interface Ethernet3 shutdown ! interface Ethernet4
shutdown ! interface Ethernet5 shutdown ! class default
limit-resource All 0 limit-resource ASDM 5 limit-
resource SSH 5 limit-resource Telnet 5 ! ftp mode
passive pager lines 24 !--- Command to enable the
failover feature failover !--- Command to assign the
interface for stateful failover failover link stateful
Ethernet2 !--- Command to configure the active and
standby IP's for the !--- stateful failover failover
interface ip stateful 10.0.0.1 255.255.255.0 standby
10.0.0.2 !--- Configure the group 1 as primary failover
group 1 !--- Configure the group 1 as secondary failover
group 2 secondary no asdm history enable arp timeout
```

```
14400 console timeout 0 admin-context admin context
admin config-url flash:/admin.cfg ! !--- Command to
create a context called "context1" context context1 !---
Command to allocate the logical interfaces to the
contexts allocate-interface Ethernet0.1 inside_context1
allocate-interface Ethernet1.1 outside_context1 config-
url flash:/context1.cfg !--- Assign this context to the
failover group 1 join-failover-group 1 ! context
context2 allocate-interface Ethernet0.2 inside_context2
allocate-interface Ethernet1.2 outside_context2 config-
url flash:/context2.cfg join-failover-group 2 ! prompt
hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

PIX1 - Context1 の設定

```
PIX1/context1(config)#show running-config : Saved : PIX
Version 7.2(2) <context> ! hostname context1 enable
password 8Ry2YjIyt7RRXU24 encrypted names ! interface
inside context1 nameif inside security-level 100 !---
Configure the active and standby IP's for the logical
inside !--- interface of the context1. ip address
192.168.1.1 255.255.255.0 standby 192.168.1.2 !
interface outside context1 nameif outside security-level
0 !--- Configure the active and standby IP's for the
logical outside !--- interface of the context1. ip
address 172.16.1.1 255.255.255.0 standby 172.16.1.2 !
passwd 2KFQnbNIdI.2KYOU encrypted access-list 100
extended permit tcp any host 172.16.1.1 eq www pager
lines 24 mtu inside 1500 mtu outside 1500 monitor-
interface inside monitor-interface outside icmp
unreachable rate-limit 1 burst-size 1 no asdm history
enable arp timeout 14400 static (inside,outside)
172.16.1.1 192.168.1.5 netmask 255.255.255.255 access-
group 100 in interface outside route outside 0.0.0.0
0.0.0.0 172.16.1.3 1 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute no snmp-server location
no snmp-server contact telnet timeout 5 ssh timeout 5 !
class-map inspection default match default-inspection-
traffic ! ! policy-map type inspect dns preset dns map
parameters message-length maximum 512 policy-map
global policy class inspection default inspect dns
preset dns map inspect ftp inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global policy global
Cryptochecksum:00000000000000000000000000000000 : end
```

PIX1 - Context2 の設定

```
PIX1/context2(config)#show running-config : Saved : PIX
Version 7.2(2) <context> ! hostname context2 enable
password 8Ry2YjIyt7RRXU24 encrypted names ! interface
inside context2 nameif inside security-level 100 !---
Configure the active and standby IP's for the logical
inside !--- interface of the context2. ip address
192.168.2.1 255.255.255.0 standby 192.168.2.2 !
interface outside context2 nameif outside security-level
0 !--- Configure the active and standby IP's for the
logical outside !--- interface of the context2. ip
address 172.16.2.1 255.255.255.0 standby 172.16.2.2 !
```



```
passwd 2KFQnbNIdI.2KYOU encrypted access-list 100
extended permit tcp any host 172.16.2.1 eq www pager
lines 24 mtu inside 1500 mtu outside 1500 monitor-
interface inside monitor-interface outside icmp
unreachable rate-limit 1 burst-size 1 no asdm history
enable arp timeout 14400 static (inside,outside)
172.16.2.1 192.168.2.5 netmask 255.255.255.255 access-
group 100 in interface outside route outside 0.0.0.0
0.0.0.0 172.16.2.3 1 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mqcq
0:05:00 mqcq-pat 0:05:00 timeout sip 0:30:00 sip media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute no snmp-server location
no snmp-server contact telnet timeout 5 ssh timeout 5 !
class-map inspection default match default-inspection-
traffic !! policy-map type inspect dns preset dns map
parameters message-length maximum 512 policy-map
global policy class inspection default inspect dns
preset dns map inspect ftp inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global policy global
Cryptochecksum:00000000000000000000000000000000 : end
```

LAN ベースでのアクティブ/アクティブ フェールオーバーの設定

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

このセクションでは、イーサネット フェールオーバー リンクを使用するアクティブ/アクティブ フェールオーバーの設定方法を説明しています。LAN ベースのフェールオーバーを設定している場合には、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できるようになるには、セカンダリ デバイスを起動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。

注: シスコは、ユニットを直接リンクするためにイーサネット クロスケーブルを使用する代わりに、プライマリ ユニットとセカンダリ ユニットの間に専用のスイッチを使用することを推奨しています。

このセクションでは、次の項目について説明しています。

- [プライマリ ユニットの設定](#)
- [セカンダリ ユニットの設定](#)

プライマリ ユニットの設定

次の手順を実行して、アクティブ/アクティブ フェールオーバー構成でのプライマリ ユニットを設定します。

1. まだ設定していない場合は、アクティブ側とスタンバイ側の IP アドレスを、各データ インターフェイス (ルーテッド モード) 用、管理 IP アドレス (トランスペアレント モード) 用、あるいは管理専用インターフェイス用に設定します。スタンバイ IP アドレスは、現在ス

スタンバイユニットであるセキュリティ アプライアンスで使用されます。これはアクティブ IP アドレスと同じサブネットにある必要があります。インターフェイスアドレスは、各コンテキスト内で設定する必要があります。コンテキストを切り替えるには、**changeto context** コマンドを使用します。コマンドプロンプトが `hostname/context(config-if)#` に変わります。ここでは、`context` が現在のコンテキストの名前になります。トランスペアレントファイアウォールモードで、各コンテキストの管理 IP アドレスを入力する必要があります。注: 専用ステートフルフェールオーバー インターフェイスを使用する場合は、ステートフルフェールオーバーリンクの IP アドレスは設定できません。専用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、後のステップで **failover interface ip** コマンドを使用します。

```
hostname/context(config-if)#ip address active_addr netmask standby
standby_addr
```

この例では、プライマリ PIX の context1 に対する Outside インターフェイスは次のように設定されています。

```
PIX1/context1(config)#ip address 172.16.1.1 255.255.255.0
standby 172.16.1.2 context2
```

については、次のようになります。

```
PIX1/context2(config)#ip
address 192.168.2.1 255.255.255.0 standby 192.168.2.2
```

ルーテッドファイアウォールモードでは、管理専用インターフェイスに関して、このコマンドは各インターフェイスに対してインターフェイス コンフィギュレーション モードで入力されます。トランスペアレントファイアウォールモードでは、このコマンドはグローバル コンフィギュレーション モードで入力されます。

- システム実行スペースで基本的なフェールオーバー パラメータを設定します。(PIX セキュリティ アプライアンスのみ) 次のように、LAN ベースのフェールオーバーを有効にします。

```
hostname(config)#failover lan enable
```

 次のように、ユニットをプライマリユニットに割り当てます。

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

 次のように、フェールオーバーリンクを指定します。

```
hostname(config)#failover lan interface if_name phy_if
```

 この例では、インターフェイス ethernet 3 を LAN ベースのフェールオーバー インターフェイスに使用しています。

```
PIX1(config)#failover lan interface LANFailover ethernet3
```

`if_name` 引数では、`phy_if` 引数で指定されているインターフェイスに論理名が割り当てられます。`phy_if` 引数には Ethernet1 のような物理ポート名を指定できますが、Ethernet0/2.3 のような事前に作成されたサブインターフェイスを指定することもできます。ASA 5505 適応型セキュリティ アプライアンスでは、`phy_if` で VLAN を指定します。このインターフェイスは、(オプションでのステートフルフェールオーバーリンクを除いて) 他の目的に使用することはできません。次のように、フェールオーバーリンクのアクティブ IP アドレスとスタンバイ IP アドレスを指定します。

```
hostname(config)#failover interface ip if_name ip_addr mask standby
ip_addr
```

 この例では、フェールオーバー インターフェイスのアクティブ IP アドレスに 10.1.0.1 を使用し、スタンバイ IP アドレスに 10.1.0.2 を使用しています。

```
PIX1(config)#failover interface ip LANFailover 10.1.0.1 255.255.255.0 standby 10.1.0.2
```

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内にある必要があります。スタンバイ IP アドレスのサブネット マスクの識別は不要です。フェールオーバーリンクの IP アドレスと MAC アドレスはフェールオーバー時には変化しません。アクティブ IP アドレスは常にプライマリユニットに存在し、スタンバイ IP アドレスはセカンダリユニットに存在します。

- ステートフルフェールオーバーを有効にするには、ステートフルフェールオーバーリンクを設定します。ステートフルフェールオーバーリンクとして使用されるインターフェイスを指定します。

```
hostname(config)#failover link if_name phy_if
```

```
PIX1(config)#failover link
stateful ethernet2
```

`if_name` 引数では、`phy_if` 引数で指定されているインターフェイスに論理名が割り当てられます。`phy_if` 引数には Ethernet1 のような物理ポート名を指定できますが、Ethernet0/2.3 のような事前に作成されたサブインターフェイスを指定することもできます。このインターフェイスは、(オプションでのフェールオーバーリンクを除いて) 他の目的に使用することはできません。注: ステートフルフェールオーバーリンクでフェールオ

ーバー リンクが標準のデータ インターフェイスが使用されている場合、必要なのは `if_name` 引数を追加するだけです。ステートフル フェールオーバー リンクにアクティブとスタンバイの IP アドレスを割り当てます。注: ステートフル フェールオーバー リンクでフェールオーバー リンクが標準のデータ インターフェイスが使用されている場合、このステップを省略します。 インターフェイスのアクティブとスタンバイの IP アドレスはすでに定義してあります。 `hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr` `PIX1(config)#failover interface ip stateful 10.0.0.1 255.255.255.0 standby 10.0.0.2` 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内にある必要があります。 スタンバイ アドレスのサブネット マスクを指定する必要はありません。 ステート リンクの IP アドレスと MAC アドレスは、フェールオーバーでは変わりません。 アクティブ IP アドレスは常にプライマリ ユニットに存在し、スタンバイ IP アドレスはセカンダリ ユニットに存在します。 インターフェイスを有効にします。注: ステートフル フェールオーバー リンクでフェールオーバー リンクが標準のデータ インターフェイスが使用されている場合、このステップを省略します。 インターフェイスはすでに有効になっています。

```
hostname(config)#interface phy_if hostname(config-if)#no shutdown
```

- フェールオーバー グループを設定します。 フェールオーバー グループは 2 つまで持てます。 フェールオーバー グループが存在しない場合、`failover group` コマンドにより指定のフェールオーバー グループが作成され、フェールオーバー グループ コンフィギュレーション モードに入ります。各フェールオーバー グループについて、`primary` コマンドか `secondary` コマンドを使用して、そのフェールオーバー グループの優先度がプライマリなのかセカンダリなのかを指定する必要があります。 両方のフェールオーバー グループに同じ優先度を割り当てられます。 ただし、ロード バランシングの設定のためには、各フェールオーバー グループに異なるユニット優先度を割り当てる必要があります。次の例では、`failover group 1` にプライマリ優先度を割り当て、`failover group 2` にセカンダリ優先度を割り当てています。

```
hostname(config)#failover group 1 hostname(config-fover-group)#primary hostname(config-fover-group)#exit hostname(config)#failover group 2 hostname(config-fover-group)#secondary hostname(config-fover-group)#exit
```

- コンテキスト コンフィギュレーション モードで `join-failover-group` コマンドを使用して、フェールオーバー グループに各ユーザ コンテキストを割り当てます。未割り当てのコンテキストは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 のメンバになります。次のコマンドを入力して、フェールオーバー グループに各コンテキストを割り当てます。 `hostname(config)#context context_name` `hostname(config-context)#join-failover-group {1 | 2}` `hostname(config-context)#exit`
- フェールオーバーを有効にします。 `hostname(config)#failover`

セカンダリ ユニットの設定

LAN ベースのアクティブ/アクティブ フェールオーバーを設定する際には、セカンダリ ユニットの起動して、フェールオーバー リンクを認識させる必要があります。 これにより、セカンダリ ユニットはプライマリ ユニットと通信して、プライマリ ユニットから実行コンフィギュレーションを受信できます。

次の手順を実行して、アクティブ/アクティブ フェールオーバー構成でのセカンダリ ユニットの起動します。

- (PIX セキュリティ アプライアンスのみ) 次のように、LAN ベースのフェールオーバーを有効にします。 `hostname(config)#failover lan enable`
- フェールオーバー インターフェイスを定義します。 次のように、プライマリ ユニットに使用したのと同じ設定を使用します。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。 `hostname(config)#failover lan interface if_name phy_if`

PIX1(config)#failover lan interface LANFailover ethernet3if_name 引数では、phy_if 引数で指定されているインターフェイスに論理名が割り当てられます。phy_if 引数には Ethernet1 のような物理ポート名を指定できますが、Ethernet0/2.3 のような事前に作成されたサブインターフェイスを指定することもできます。ASA 5505 適応型セキュリティ アプライアンスでは、phy_if で VLAN を指定します。次のように、フェールオーバー リンクにアクティブとスタンバイの IP アドレスを割り当てます。hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr PIX1(config)#failover interface ip LANFailover 10.1.0.1 255.255.255.0 standby 10.1.0.2 注: このコマンドは、フェールオーバー インターフェイスを設定した際にプライマリ ユニットに入力したとおりに入力します。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内に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。インターフェイスを有効にします。hostname(config)#interface phy_if hostname(config-if)#no shutdown

3. 次のように、このユニットをセカンダリ ユニットに割り当てます。

hostname(config)#failover lan unit secondary 注: あらかじめ他のように設定されていない限り、デフォルトではユニットがセカンダリに割り当てられているため、このステップは省略可能です。

4. フェールオーバーを有効にします。hostname(config)#failover フェールオーバーを有効にすると、アクティブ ユニットでは実行メモリ内の設定がスタンバイ ユニットに送信されます。設定が同期するように、**コンフィギュレーション複製を始めるメッセージ: 「Sending to mate」および「End Configuration Replication to mate」**というメッセージが表示されます。注: まず、プライマリ デバイスで failover コマンドを発行し、次にセカンダリ デバイスで発行します。セカンダリ デバイス上で failover コマンドを発行した後、セカンダリ デバイスでは即座にプライマリ デバイスからコンフィギュレーションが取得され、スタンバイとしてセカンダリ デバイス自体が設定されます。プライマリ ASA はアップしたままであり、トラフィックの受け渡しが正常に行われます。そのため、プライマリ ASA 自体がアクティブデバイスとしてマークされます。この時点以降、アクティブ デバイス上で障害が発生する場合は、常にスタンバイ デバイスがアクティブになります。

5. 実行コンフィギュレーションの複製が完了したら、次のコマンドを入力して、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。hostname(config)#copy running-config startup-config

6. 必要な場合は、プライマリ側でアクティブなフェールオーバー グループをすべて、セカンダリ ユニットで強制的にアクティブ ステートにします。セカンダリ ユニットでフェールオーバー グループを強制的にアクティブにするには、プライマリ ユニットのシステム実行スペースで次のコマンドを入力します。hostname#no failover active group group_id group_id 引数には、セカンダリ ユニットでアクティブにするグループを指定します。

設定

このドキュメントでは、次の設定を使用します。

プライマリ PIX

```
PIX1(config)#show running-config : Saved : PIX Version
7.2(2) <system> ! hostname PIX1 enable password
8Ry2YjIyt7RRXU24 encrypted no mac-address auto !
interface Ethernet0 ! interface Ethernet0.1 vlan 2 !
interface Ethernet0.2 vlan 4 ! interface Ethernet1 !
interface Ethernet1.1 vlan 3 ! interface Ethernet1.2
vlan 5 ! !--- Configure "no shutdown" in the stateful
failover interface as well as !--- LAN Failover
interface of both Primary and secondary PIX/ASA.
```

```

interface Ethernet2 description STATE Failover Interface
! interface Ethernet3 description LAN Failover Interface
! interface Ethernet4 shutdown ! interface Ethernet5
shutdown ! class default limit-resource All 0 limit-
resource ASDM 5 limit-resource SSH 5 limit-resource
Telnet 5 ! ftp mode passive pager lines 24 failover
failover lan unit primary !--- Command to assign the
interface for LAN based failover failover lan interface
LANFailover Ethernet3 !--- Command to enable the LAN
based failover failover lan enable !--- Configure the
Authentication/Encryption key failover key *****
failover link stateful Ethernet2 !--- Configure the
active and standby IP's for the LAN based failover
failover interface ip LANFailover 10.1.0.1 255.255.255.0
standby 10.1.0.2 failover interface ip stateful 10.0.0.1
255.255.255.0 standby 10.0.0.2 failover group 1 failover
group 2 secondary no asdm history enable arp timeout
14400 console timeout 0 admin-context admin context
admin config-url flash:/admin.cfg ! context context1
allocate-interface Ethernet0.1 inside_context1 allocate-
interface Ethernet1.1 outside_context1 config-url
flash:/context1.cfg join-failover-group 1 ! context
context2 allocate-interface Ethernet0.2 inside_context2
allocate-interface Ethernet1.2 outside_context2 config-
url flash:/context2.cfg join-failover-group 2 ! prompt
hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end

```

注: LAN ベースのフェールオーバーのシナリオでのコンテキストの設定は、ケーブル ベースのフェールオーバーの設定セクション「[PIX1 : context1 コンフィギュレーション](#)」と「[PIX1 : context2 コンフィギュレーション](#)」を参照してください。

セカンダリ PIX

```

PIX2#show running-config failover failover lan unit
secondary failover lan interface LANFailover Ethernet3
failover lan enable failover key ***** failover
interface ip LANFailover 10.1.0.1 255.255.255.0 standby
10.1.0.2

```

確認

[show failover コマンドの使用](#)

このセクションでは、**show failover** コマンドの出力について説明しています。各ユニットで、**show failover** コマンドを使用してフェールオーバー ステータスを確認できます。

プライマリ PIX

```

PIX1(config-subif)#show failover Failover On Cable status: N/A - LAN-based failover enabled
Failover unit Primary Failover LAN Interface: LANFailover Ethernet3 (up) Unit Poll frequency 15
seconds, holdtime 45 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface
Policy 1 Monitored Interfaces 4 of 250 maximum Version: Ours 7.2(2), Mate 7.2(2) Group 1 last
failover at: 06:12:45 UTC Apr 16 2007 Group 2 last failover at: 06:12:43 UTC Apr 16 2007 This
host: Primary Group 1 State: Active Active time: 359610 (sec) Group 2 State: Standby Ready
Active time: 3165 (sec) context1 Interface inside (192.168.1.1): Normal context1 Interface
outside (172.16.1.1): Normal context2 Interface inside (192.168.2.2): Normal context2 Interface
outside (172.16.2.2): Normal Other host: Secondary Group 1 State: Standby Ready Active time: 0
(sec) Group 2 State: Active Active time: 3900 (sec) context1 Interface inside (192.168.1.2):

```

```
Normal context1 Interface outside (172.16.1.2): Normal context2 Interface inside (192.168.2.1):
Normal context2 Interface outside (172.16.2.1): Normal Stateful Failover Logical Update
Statistics Link : stateful Ethernet2 (up) Stateful Obj xmit xerr rcv rerr General 48044 0 48040
1 sys cmd 48042 0 48040 1 up time 0 0 0 0 RPC services 0 0 0 0 TCP conn 0 0 0 0 UDP conn 0 0 0 0
ARP tbl 2 0 0 0 Xlate_Timeout 0 0 0 0 Logical Update Queue Information Cur Max Total Recv Q: 0 1
72081 Xmit Q: 0 1 48044
```

セカンダリ PIX

```
PIX1(config)#show failover Failover On Cable status: N/A - LAN-based failover enabled Failover
unit Secondary Failover LAN Interface: LANFailover Ethernet3 (up) Unit Poll frequency 15
seconds, holdtime 45 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface
Policy 1 Monitored Interfaces 4 of 250 maximum Version: Ours 7.2(2), Mate 7.2(2) Group 1 last
failover at: 06:12:46 UTC Apr 16 2007 Group 2 last failover at: 06:12:41 UTC Apr 16 2007 This
host: Secondary Group 1 State: Standby Ready Active time: 0 (sec) Group 2 State: Active Active
time: 3975 (sec) context1 Interface inside (192.168.1.2): Normal context1 Interface outside
(172.16.1.2): Normal context2 Interface inside (192.168.2.1): Normal context2 Interface outside
(172.16.2.1): Normal Other host: Primary Group 1 State: Active Active time: 359685 (sec) Group 2
State: Standby Ready Active time: 3165 (sec) context1 Interface inside (192.168.1.1): Normal
context1 Interface outside (172.16.1.1): Normal context2 Interface inside (192.168.2.2): Normal
context2 Interface outside (172.16.2.2): Normal Stateful Failover Logical Update Statistics Link
: stateful Ethernet2 (up) Stateful Obj xmit xerr rcv rerr General 940 0 942 2 sys cmd 940 0 940
2 up time 0 0 0 0 RPC services 0 0 0 0 TCP conn 0 0 0 0 UDP conn 0 0 0 0 ARP tbl 0 0 2 0
Xlate_Timeout 0 0 0 0 Logical Update Queue Information Cur Max Total Recv Q: 0 1 1419 Xmit Q: 0
1 940
```

状態を確認するには、**show failover state** コマンドを使用します。

プライマリ PIX

```
PIX1(config)#show failover state State Last Failure Reason Date/Time This host - Primary Group 1
Active None Group 2 Standby Ready None Other host - Secondary Group 1 Standby Ready None Group 2
Active None ====Configuration State=== Sync Done ====Communication State=== Mac set
```

セカンダリ ユニット

```
PIX1(config)#show failover state State Last Failure Reason Date/Time This host - Secondary Group
1 Standby Ready None Group 2 Active None Other host - Primary Group 1 Active None Group 2
Standby Ready None ====Configuration State=== Sync Done - STANDBY ====Communication State=== Mac
set
```

フェールオーバー ユニットの IP アドレスを確認するには、**show failover interface** コマンドを使用します。

プライマリ ユニット

```
PIX1(config)#show failover interface interface stateful Ethernet2 System IP Address: 10.0.0.1
255.255.255.0 My IP Address : 10.0.0.1 Other IP Address : 10.0.0.2 interface LANFailover
Ethernet3 System IP Address: 10.1.0.1 255.255.255.0 My IP Address : 10.1.0.1 Other IP Address :
10.1.0.2
```

セカンダリ ユニット

```
PIX1(config)#show failover interface interface LANFailover Ethernet3 System IP Address: 10.1.0.1
255.255.255.0 My IP Address : 10.1.0.2 Other IP Address : 10.1.0.1 interface stateful Ethernet2
System IP Address: 10.0.0.1 255.255.255.0 My IP Address : 10.0.0.2 Other IP Address : 10.0.0.1
```

[監視対象インターフェイスの表示](#)

監視対象インターフェイスのステータスを表示するには、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、グローバル設定モードで **show monitor-interface** コマンドを入力します。マルチ コンテキスト モードの場合は、コンテキスト内で **show monitor-interface** コマンドを入力します。

注: 特定のインターフェイスでヘルス モニタ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 [monitor-interface](#) コマンドを使用します。

```
monitor-interface <if_name>
```

プライマリ PIX

```
PIX1/context1(config)#show monitor-interface This host: Secondary - Active Interface inside (192.168.1.1): Normal Interface outside (172.16.1.1): Normal Other host: Secondary - Standby Ready Interface inside (192.168.1.2): Normal Interface outside (172.16.1.2): Normal
```

セカンダリ PIX

```
PIX1/context1(config)#show monitor-interface This host: Secondary - Standby Ready Interface inside (192.168.1.2): Normal Interface outside (172.16.1.2): Normal Other host: Secondary - Active Interface inside (192.168.1.1): Normal Interface outside (172.16.1.1): Normal
```

注: フェールオーバー IP アドレスを入力しない場合は、**show failover** コマンドによって IP アドレスが 0.0.0.0 と表示され、インターフェイスの監視は「waiting」（待機）状態になります。フェールオーバーが機能するには、フェールオーバー IP アドレスを設定する必要があります。フェールオーバーのさまざまなステータスの情報は、[show failover](#) を参照してください。

デフォルトでは、物理インターフェイスの監視が無効になっており、サブインターフェイスの監視は有効になっています。

[実行コンフィギュレーションでのフェールオーバー コマンドの表示](#)

実行設定内のフェールオーバー コマンドを表示するには、次のコマンドを入力します。

```
hostname(config)#show running-config failover
```

すべてのfailover コマンドが表示されます。マルチ コンテキスト モードで稼働するユニットでは、システム実行スペースで show running-config failover コマンドを入力します。デフォルト値を変更していないコマンドを含めて、実行コンフィギュレーションでのフェールオーバー コマンドを表示するには、**show running-config all failover** コマンドを入力します。

[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。

1. アクティブ ユニットやフェールオーバー グループが、別々のインターフェイス上でホスト間でファイルを送信するために FTP など期待どおりにトラフィックを通過させていることをテストします。
2. 次のコマンドを使用して、強制的にスタンバイ ユニットにフェールオーバーさせます。アクティブ/アクティブ フェールオーバーには、ホストに接続しているインターフェイスを含むフェールオーバー グループがアクティブになっているユニットで次のコマンドを入力します。hostname(config)#no failover active group *group_id*
3. FTP を使用して、同じ 2 つのホスト間で別のファイルを送信します。
4. テストが失敗した場合は、**show failover command**を入力してフェールオーバーのステータスを調べます。
5. 終了したら、次のコマンドを使用してユニットまたはフェールオーバー グループをアクティブ ステータスに戻すことができます。アクティブ/アクティブ フェールオーバーには、ホストに接続しているインターフェイスを含むフェールオーバー グループがアクティブになっているユニットで次のコマンドを入力します。hostname(config)#failover active group *group_id*

強制フェールオーバー

強制的にスタンバイ ユニットの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。

フェールオーバー グループがスタンバイ ステートになっているユニットのシステム実行スペースで、次のコマンドを入力します。

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

あるいは、フェールオーバー グループがアクティブ ステートになっているユニットのシステム実行スペースで、次のコマンドを入力します。

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

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

```
hostname#failover active
```

フェールオーバーの無効化

フェールオーバーをディセーブルにするには、次のコマンドを入力します。

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

アクティブ/スタンバイ ペアでフェールオーバーを無効にすると、再起動するまで各ユニットのアクティブとスタンバイのステートが保持されます。たとえば、スタンバイ ユニットのスタンバイモードのままなので、どちらのユニットでもトラフィックの受け渡しが始まりません。スタンバイ ユニットのアクティブにするには (フェールオーバーがディセーブルになっている場合でも)、[「強制フェールオーバー」](#) セクションを参照してください。

アクティブ/アクティブ ペアでフェールオーバーを無効にすると、どのユニットが優先に設定されているかに関係なく、フェールオーバー グループは現在アクティブになっているユニットでアクティブ状態のままになります。no failover コマンドは、システム実行スペースで入力できます。

障害ユニットの復元

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 グループを非障害ステートに復元するには、次のコマンドを入力します。

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

障害状態のユニットを障害解除状態に復元した場合、ユニットは自動的にアクティブになりません。(強制的または通常の)フェールオーバーによってアクティブにされるまで、復元されたユニットまたはグループはスタンバイ状態のままになります。ただし、preempt コマンドを使用して設定されているフェールオーバー グループは例外です。以前アクティブであり、フェールオーバー グループが preempt コマンドを使用して設定されていて、障害が発生したユニットが優先ユニットである場合、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。

障害が発生したユニットの新しいユニットとの交換

障害が発生したユニットを新しいユニットに交換するには、次の手順を実行します。

- プライマリ ユニットの no failover コマンドを実行します。セカンダリ ユニットのステータスが「standby unit as not detected」となります。
- プライマリ ユニットを取り外して、新しいユニットに交換します。

3. 交換したユニットでセカンダリ ユニットと同じバージョンのソフトウェアおよび ASDM が実行されていることを確認します。
4. 交換用のユニットで次のコマンドを実行します。

```
ASA(config)#failover lan unit primary ASA(config)#failover lan interface failover Ethernet3
ASA(config)#failover interface ip failover 10.1.0.1 255.255.255.0 standby 10.1.0.2
ASA(config)#interface Ethernet3 ASA(config-if)#no shut ASA(config-if)#exit
```
5. 交換用のプライマリ ユニートをネットワークに接続して、次のコマンドを実行します。

```
ASA(config)#failover
```

トラブルシューティング

フェールオーバーが発生すると、両方のセキュリティ アプライアンスからシステム メッセージが送信されます。ここでは次の項目について説明します。

1. [フェールオーバーのシステム メッセージ](#)
2. [デバッグ メッセージ](#)
3. [SNMP](#)

フェールオーバーのシステム メッセージ

セキュリティ アプライアンスでは、フェールオーバーに関連する多数のシステム メッセージが優先レベル 2 で発行され、これは重大な状態を示しています。これらのメッセージを表示するには『[Cisco セキュリティ アプライアンスのロギング設定とシステム ログ メッセージ](#)』を参照して、ロギングを有効にし、システム メッセージの説明を参照してください。

注: スイッチオーバーでは、フェールオーバーによりインターフェイスが論理的にシャットダウンされてから起動されるので、syslog の 411001 および 411002 メッセージが生成されます。これは正常な動作です。

Primary Lost Failover communications with mate on interface interface_name (プライマリで、インターフェイス interface_name のペアの相手とのフェールオーバー通信が失われた)

このフェールオーバー メッセージは、フェールオーバー ペアのうちの片方のユニットがペアのもう一方のユニットと通信できなくなっている場合に表示されます。セカンダリ ユニットが問題であれば、「Primary」の箇所は「Secondary」と表示されます。

(Primary) Lost Failover communications with mate on interface *interface_name*

所定のインターフェイスに接続されたネットワークが正しく動作していることを確認します。

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、『[Cisco セキュリティ アプライアンス コマンド リファレンス、バージョン 7.2](#)』を参照してください。

注: デバッグ出力は CPU プロセスで高い優先度を割り当てられているので、システムのパフォーマンスが大きな影響を受ける可能性があります。このため、`debug fover` コマンドの使用は、特定の問題のトラブルシューティングまたは Cisco テクニカルサポート要員とのトラブルシューテ

イング セッション中だけにしてください。

SNMP

フェールオーバーに対する SNMP syslog トラップを受け取るには、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 ホストを定義して、Cisco syslog MIB を SNMP 管理ステーションにコンパイルします。詳細については、『Cisco セキュリティ アプライアンス コマンド リファレンス、バージョン 7.2』で、snmp-server コマンドと [logging](#) コマンドを参照してください。

フェールオーバー ポーリング時間

フェールオーバー ユニットのポーリング時間とホールド時間を指定するには、グローバル コンフィギュレーション モードで、failover polltime コマンドを発行します。

failover polltime unit msec [time] は、hello メッセージをポーリングしてスタンバイ ユニットの存在を調べる時間間隔を表しています。

同様に、failover holdtime unit msec [time] は、フェールオーバー リンクでユニットが hello メッセージを受信するはずの時間枠を示しており、この時間が経過すると、ピア ユニットで障害が発生したものと宣言されます。

詳細については、『[failover polltime](#)』を参照してください。

WARNING: フェールオーバー メッセージの複合化に失敗しました。

エラー メッセージ :

```
Failover message decryption failure. Please make sure both units have the same failover shared key and crypto license or system is not out of memory
```

この問題はフェールオーバーのキー設定が原因で発生します。この問題を解決するには、フェールオーバー キーを削除し、新規の共有キーを設定します。

関連情報

- [Cisco 500 シリーズ PIX に関するサポート ページ](#)
- [Firewall Services Module \(FWSM; ファイアウォール サービス モジュール \) フェールオーバー設定](#)
- [FWSM フェールオーバー トラブルシューティング](#)
- [Cisco Secure PIX ファイアウォール でのフェールオーバーの仕組み](#)
- [Cisco 5500 シリーズ 適応型 セキュリティ アプライアンス に関するサポート ページ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)