

ASA/PIX : トランスペアレント モードでのアクティブ/スタンバイ フェールオーバーの設定

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/スタンバイ フェールオーバー](#)

[アクティブ/スタンバイ 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](#)

[LAN ベースのアクティブ/スタンバイ 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](#)

[トラブルシューティング](#)

[フェールオーバー監視](#)

[ユニット障害](#)

[LU 割り当て接続の失敗](#)

[フェールオーバーのシステム メッセージ](#)

[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](#)

[フェールオーバー設定での証明書/秘密鍵のエクスポート](#)

[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。](#)

[問題： フェールオーバーは透過的でアクティブ/スタンバイ な 多重 モード フェールオーバーを設定した後常にフラップしています](#)

[ASA モジュール フェールオーバー](#)

[フェールオーバー メッセージのブロック割り当ての失敗](#)

[AIP モジュール フェールオーバーの問題](#)

[既知の問題](#)

[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、次の 2 つのフェールオーバー コンフィギュレーションをサポートしています。

- [アクティブ/アクティブ フェールオーバー](#)
- [アクティブ/スタンバイ フェールオーバー](#)

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。

トランスペアレント ファイアウォールは、*bump-in-the-wire* またはステルス ファイアウォールのように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。セキュリティ アプライアンスによって、その内部ポートおよび外部ポート上に同じネットワークが接続されます。ファイアウォールはルーティング ホップではないため、トランスペアレント ファイアウォールを既存のネットワークに簡単に導入できます。IP アドレスの再設定は必要ありません。デフォルトのルーテッド ファイアウォール モードまたは透過型ファイアウォール モードで稼働するように、適応型セキュリティ アプライアンスを設定できます。多くのコマンドが両方のモードではサポートされないため、モードを変更すると適応型セキュリティ アプライアンスによって設定がクリアされます。すでにデータを入力したコンフィギュレーションが用意されている場合、モードを変更する前に必ずそのコンフィギュレーションをバックアップしてください。新しいコンフィギュレーションを作成する際に、このバックアップ コンフィギュレーションを参照用に使用できます。トランスペアレント モードでファイアウォール アプライアンスを設定するときの詳細は、「[PIX/ASA：透過型ファイアウォールの設定例](#)」を参照してください。

このドキュメントでは、ASA セキュリティ アプライアンスにトランスペアレント モードでアク

ティブ/スタンバイ フェールオーバーを設定する方法を中心に取り上げています。

注: 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 のフェールオーバーは、**アクティブ/スタンバイ フェールオーバー** 構成でのみ使用できます。

フェールオーバーには管理インターフェイスを使用しないことを推奨いたします。特に、ステートフル フェールオーバーの場合、一方のセキュリティ アプライアンスから他方のセキュリティ アプライアンスに常に接続情報が送信されるので、管理インターフェイスの使用は推奨されません。フェールオーバー用のインターフェイスは、通常のトラフィックを渡すインターフェイスと少なくとも同じ容量である必要があります。さらに、ASA 5540 のインターフェイスはギガビットですが、管理インターフェイスは FastEthernet のみです。管理インターフェイスは管理トラフィック専用の設計になっており、management0/0 と指定されます。ただし、**management-only** コマンドを使用すると、任意のインターフェイスを管理専用インターフェイスとして設定できます。また、Management 0/0 については、管理専用モードを無効にして、他のインターフェイスと同じようにトラフィックを受け渡すようにすることができます。 [management-only](#) コマンドの詳細は、『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 8.0』を参照してください。

この設定ガイドでは、PIX/ASA 7.x のアクティブ/スタンバイ テクノロジーの概要と併せて、設定例を紹介しています。このテクノロジーの基礎になっている理論背景についての詳細は、『[ASA/PIX コマンド リファレンス ガイド](#)』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方法の詳細は、『[Cisco セキュリティ アプライアンス コマンドライン コンフィギュレーション ガイド、バージョン 8.0](#)』の「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」セクションを参照して

ください。

ライセンス要件

ASA セキュリティ アプライアンス プラットフォームでは、少なくとも 1 つのユニットに無制限 (UR) ライセンスが備わっている必要があります。

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。詳細は、『[PIX/ASA: フェールオーバー ペアのライセンスキーのアップグレード](#)』を参照してください。

注: フェールオーバーに関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 (SSL VPN ピアやセキュリティ コンテキスト) は、同一である必要があります。

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。

- ASA 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。

- PIX セキュリティ アプライアンス バージョン 7.x 以降

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/スタンバイ 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/スタンバイ 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/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 フェールオーバーを利用すると、スタンバイ セキュリティ アプライアンス

スを使用して故障したユニットの機能を引き継ぐことができます。アクティブなユニットが故障すると、そのユニットはスタンバイ状態に変わり、スタンバイユニットがアクティブ状態に変わります。アクティブになったユニットは、故障したユニットの IP アドレスか、トランスペアレントファイアウォールの場合の管理 IP アドレスと、MAC アドレスを引き継ぎ、トラフィックの受け渡しを開始します。スタンバイ状態になったユニットは、スタンバイ IP アドレスと MAC アドレスを受け継ぎます。ネットワークデバイスで認識される MAC と IP のアドレス対応は変わらないので、ネットワークのどこにも ARP エントリの変更やタイムアウトは発生しません。

注: マルチ コンテキスト モードの場合、セキュリティ アプライアンスでは、ユニット全体、つまりすべてのコンテキストをフェールオーバーできる一方で、個別コンテキストの個別フェールオーバーはできません。

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 つのユニットの間の主な違いは、どちらのユニットがアクティブでどちらのユニットがスタンバイかということ、つまり、どの IP アドレスを使用し、どちらのユニットがプライマリでアクティブにトラフィックを受け渡すかということに関係します。

コンフィギュレーションでどちらのユニットがプライマリに指定されており、どちらのユニットがセカンダリに指定されているのに基づき、ユニットの間にはいくつかの違いが存在します。

- 両方のユニットが同時に起動された場合（そして動作ヘルスが同等である場合）、常にプライマリユニットがアクティブユニットになります。
- プライマリユニットの MAC アドレスが常に、アクティブな IP アドレスに結び付けられます。セカンダリユニットがアクティブであり、フェールオーバーリンクを通してプライマリ MAC アドレスを取得できない場合は、このルールに対する例外が発生します。この場合は、セカンダリ MAC アドレスが使用されます。

デバイスの初期化と設定の同期

フェールオーバー ペア的一方または両方のデバイスがブートすると、設定の同期が発生します。設定は、常にアクティブユニットからスタンバイユニットに同期化されます。スタンバイユニットでは初期起動が完了すると、アクティブユニットとの通信に必要なフェールオーバーコマンドを除いて実行コンフィギュレーションがクリアされ、アクティブユニットからユニットのコンフィギュレーション全体がスタンバイユニットに送信されます。

アクティブユニットは次のようにして決定されます。

- ユニットがブートして、ピアがすでにアクティブとして動作していることが検出されると、そのユニットはスタンバイユニットになります。
- ユニットがブートして、ピアが検出されない場合、そのユニットはアクティブユニットになります。
- 両方のユニットが同時にブートした場合は、プライマリユニットがアクティブユニットになり、セカンダリユニットがスタンバイユニットになります。

注: セカンダリユニットがブートして、プライマリユニットが検出されない場合は、セカンダリユニットがアクティブユニットになります。自身の MAC アドレスをアクティブ IP アドレスとして使用します。プライマリユニットが使用可能になると、セカンダリユニットでは MAC アドレスがプライマリユニットの MAC アドレスに変更されるので、ネットワークトラフィックが中断する可能性があります。この問題を回避するには、フェールオーバーペアに仮想 MAC アドレスを設定します。詳細は、このドキュメントの「[ケーブルベースのアクティブ/スタンバイフ](#)

[フェールオーバーの設定](#)」セクションを参照してください。

複製が始まると、アクティブ 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。複製の間は、アクティブ ユニットで入力したコマンドはスタンバイ ユニットに正しく複製できず、スタンバイ ユニットで入力されたコマンドは、アクティブ ユニットから複製される設定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に含まれるフェールオーバー ペアのいずれのユニットでも、コマンドを入力しないでください。コンフィギュレーションのサイズにより、複製には数秒から数分かかる可能性があります。

セカンダリ ユニットでは、同期動作に応じてプライマリ ユニットからの複製メッセージを監視できます。

```
ASA> .  
  
      Detected an Active mate  
Beginning configuration replication from mate.  
End configuration replication from mate.
```

ASA>
スタンバイ ユニットでは、コンフィギュレーションは実行メモリ上だけに存在しています。同期の後でコンフィギュレーションをフラッシュ メモリに保存するには、次のコマンドを入力します。

- シングル コンテキスト モードの場合は、アクティブ ユニットで **copy running-config startup-config** コマンドを入力します。このコマンドがスタンバイ ユニットに複製され、スタンバイ ユニットで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、アクティブ ユニットで、システム実行スペースおよびディスクの各コンテキスト内から、**copy running-config startup-config** コマンドを入力します。このコマンドがスタンバイ ユニットに複製され、スタンバイ ユニットで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。外部サーバ上のスタートアップ コンフィギュレーションのコンテキストは、どちらのユニットからもネットワーク経由で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。または、アクティブ ユニットからディスク上のコンテキストを外部サーバにコピーした後、そのコンテキストをスタンバイ ユニットのディスクにコピーして、ユニットをリロードするときに利用できるようにすることもできます。

[コマンドの複製](#)

コマンドの複製は、常に、アクティブ ユニットからスタンバイ ユニットに向かって行われます。コマンドがアクティブ ユニットで入力されると、フェールオーバー リンクを經由してスタンバイ ユニットに送られます。コマンドを複製するために、アクティブな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。

注: スタンバイ ユニットで行われた変更は、アクティブ ユニットへは複製されません。スタンバイ ユニットでコマンドを入力すると、セキュリティ アプライアンスに「**** WARNING **** Configuration Replication is NOT performed from Standby unit to Active unit.」というメッセージが表示されます。これでコンフィギュレーションは同期しません。このメッセージは、コンフィギュレーションに影響を与えないコマンドを入力した場合でも表示されます。

アクティブ ユニットで **write standby** コマンドを入力すると、スタンバイ ユニットでは、アクテ

イブ ユニットとの通信に使用するフェールオーバー コマンドを除く実行コンフィギュレーションがクリアされ、アクティブ ユニットからコンフィギュレーション全体がスタンバイ ユニットに送信されます。

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で **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。コンテキスト内で **write standby** コマンドを入力した場合は、コンテキストのコンフィギュレーションのみが複製されます。

複製されたコマンドは、実行コンフィギュレーションに格納されます。複製されたコマンドをスタンバイ ユニットのフラッシュ メモリに保存するには、次のコマンドを入力します。

- シングル コンテキスト モードの場合は、アクティブ ユニットで **copy running-config startup-config** コマンドを入力します。このコマンドがスタンバイ ユニットに複製され、スタンバイ ユニットで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、アクティブ ユニットで、システム実行スペースおよびディスクの各コンテキスト内から、**copy running-config startup-config** コマンドを入力します。このコマンドがスタンバイ ユニットに複製され、スタンバイ ユニットで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。外部サーバ上のスタートアップ コンフィギュレーションのコンテキストは、どちらのユニットからもネットワーク経由で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。または、アクティブ ユニットからディスク上のコンテキストを外部サーバにコピーした後、このコンテキストをスタンバイ ユニットのディスクにコピーすることもできます。

フェールオーバー トリガ

ユニットが障害状態になる可能性があるのは、次のいずれかのイベントが発生した場合です。

- ユニットにハードウェア障害または電源障害がある。
- ユニットにソフトウェア障害がある。
- 多くの監視対象インターフェイスで障害が発生する。
- アクティブ ユニットで **no failover active** コマンドが入力される。または、スタンバイ ユニットで **failover active** コマンドが入力される。

フェールオーバー 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ユニット単位で発生します。マルチ コンテキスト モードが稼働しているシステムであっても、個別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、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。表では、障害イベントごとに、フェールオーバー ポリシー（フェールオーバーするかしないか）、アクティブ ユニットで実行されるアクション、スタンバイ ユニットで実行されるアクション、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が示されています。表には、フェールオーバーの動作が示されています。

障害イベント	ポリシー	アクティブ アクション	スタンバイ アクション	注意事項
アクティ	フ	該当な	アクテ	監視対象インターフ

ブユニットの障害 (電源またはハードウェア)	フェールオーバーなし	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	エイスマたはフェールオーバーリンクでhelloメッセージを受信することはありません。
以前アクティブであったユニットの復旧	フェールオーバーなし	スタンバイになる	アクションなし	なし
スタンバイユニットの障害 (電源またはハードウェア)	フェールオーバーなし	スタンバイを障害としてマークする	該当なし	スタンバイユニットが障害としてマークされると、アクティブユニットでは、インターフェイス障害のしきい値を超えてもフェールオーバーが試行されません。
動作中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	フェールオーバーインターフェイスを障害としてマークする	フェールオーバーインターフェイスを障害としてマークする	フェールオーバーリンクがダウンしている間は、ユニット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、できる限り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。
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	フェールオーバーインターフェイスを障害としてマークする	アクティブになる	起動時にフェールオーバーリンクがダウンすると、両方のユニットがアクティブになります。
ステータス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	ステータス情報が古くなり、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。

	一 バ ー な し			
アクティ ブ ユニッ トでのイ ンターフ ェイス障 害がしき い値を超 過	フ ェ ー ル オ ー バ ー	アクテ ィブを と 障 害 し て マ ー ク す る	アクテ ィブに なる	なし
スタンバ イ ユニッ トでのイ ンターフ ェイス障 害がしき い値を超 過	フ ェ ー ル オ ー バ ー な し	アクシ ョンな し	スタン バイを と 障 害 し て マ ー ク す る	スタンバイ ユニッ トが障害としてマ ークされると、アクテ ィブ ユニットでは 、インターフェイス 障害のしきい値を超 えてもフェールオー バーが試行されませ ん。

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いだ後で、クライアントでは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 (ファイアウォールがトランスペアレント ファイアウォール モードで稼動している場合に限る)
- 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。

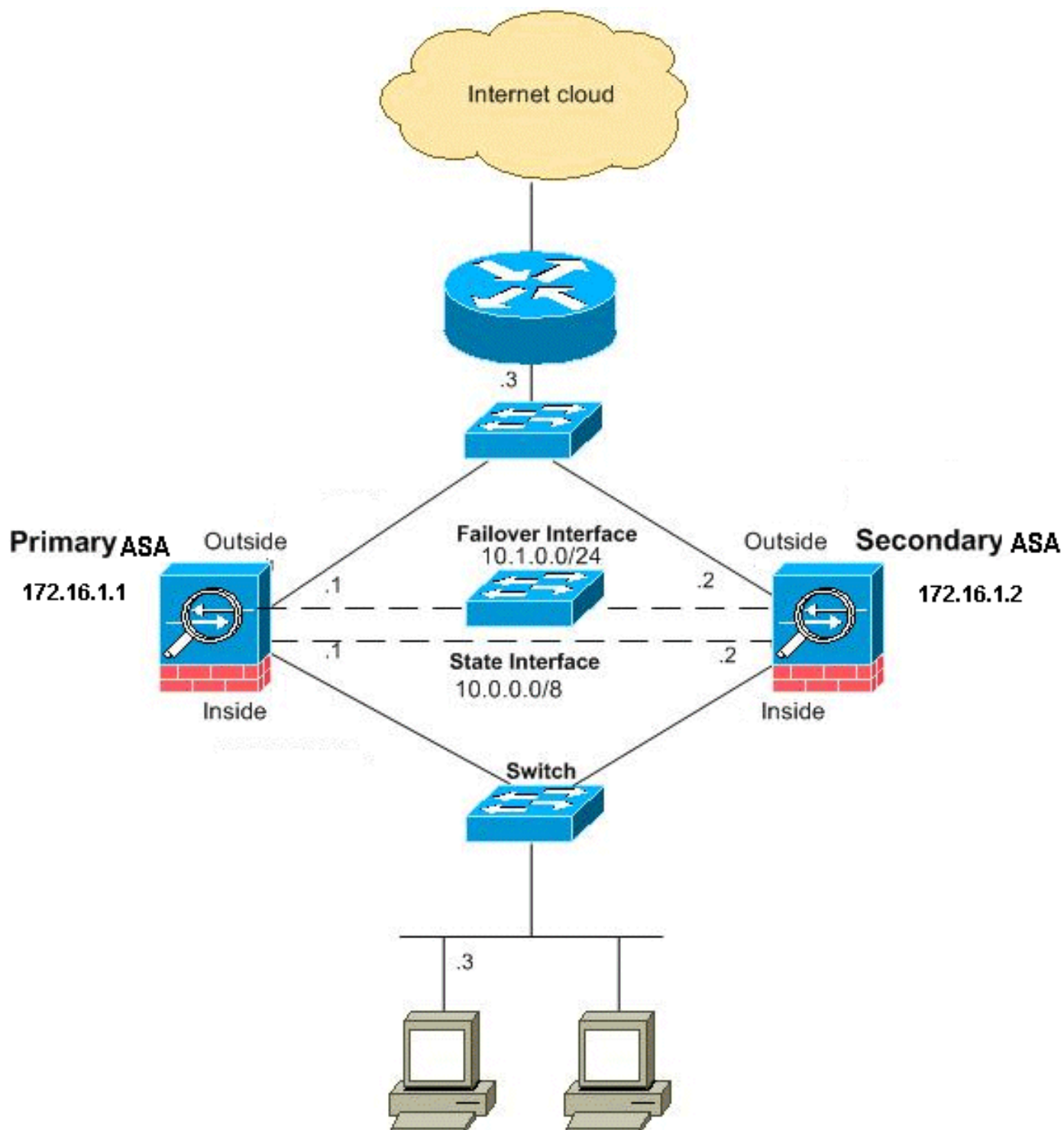
- HTTP 接続テーブル (HTTP 複製が有効になっていない場合)
- ユーザ認証 (uauth) テーブル
- ルーティング テーブル
- セキュリティ サービス モジュールのステート情報

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 クライアントは Cisco CallManager との接続がなくなります。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。一定時間内に Cisco CallManager から応答を受信しない場合、IP SoftPhone クライアントでは、Cisco CallManager に到達できないと見なして登録解除します。

LAN ベースのアクティブ/スタンバイ 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 リンクを使用してトランスペアレント モードでアクティブ/スタンバイ フェールオーバーを設定する方法を説明しています。LAN ベースのフェールオーバーを設定する場合は、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、先にセカンダリ デバイスでブートストラップを実行して、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: ケーブル ベースのフェールオーバーから LAN ベースのフェールオーバーに変更する場合は、各インターフェイスへのアクティブおよびスタンバイ IP アドレスの割り当てなど、ケーブル ベースのフェールオーバー設定で済んでいる多くの手順は省略できます。

プライマリ ユニットの設定

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 ユ

ユニットを設定するには、次の手順を実行します。この手順では、プライマリ ユニットでフェールオーバーを有効にするために必要な最低限の設定を行います。マルチ コンテキスト モードの場合、特に指示がない限り、すべての手順をシステム実行スペースで実行します。

アクティブ/スタンバイ フェールオーバー ペアのプライマリ ユニットを設定するには、次の手順を実行します。

1. まだ行っていない場合は、管理インターフェイス (トランスペアレント モード) に、アクティブとスタンバイの IP アドレスを設定します。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。注: 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 IP アドレスを設定しないでください。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(config-if)#ip address active_addr netmask standby standby_addr` 各インターフェイスに IP アドレスが必要なルーテッド モードとは異なり、透過型ファイアウォールにはデバイス全体に割り当てられた IP アドレスがあります。セキュリティ アプライアンスでは、この IP アドレスをシステム メッセージまたは AAA 通信などのセキュリティ アプライアンスから発信されるパケットの送信元アドレスとして使用します。この例では、プライマリ ASA の IP アドレスは以下のように設定されています。`hostname(config)#ip address 172.16.1.1 255.255.0.0 standby 172.16.1.2` ここでは、172.16.1.1 がプライマリ ユニットに使用され、172.16.1.2 がセカンダリ (スタンバイ) ユニットに割り当てられます。注: マルチ コンテキスト モードでは、各コンテキスト内からインターフェイス アドレスを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。
2. (PIX セキュリティ アプライアンス プラットフォームのみ) 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`
3. ユニットのプライマリ ユニットとして指定します。`hostname(config)#failover lan unit primary`
4. フェールオーバー インターフェイスを定義します。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` このドキュメントでは、「failover」(Ethernet0 のインターフェイス名) がフェールオーバー インターフェイスに使用されています。`hostname(config)#failover lan interface failover Ethernet3 if_name` 引数により、`phy_if` 引数で指定されているインターフェイスに名前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。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` このドキュメントでは、フェールオーバー リンクを設定するために、10.1.0.1 がアクティブ ユニットに使用され、10.1.0.2 がスタンバイ ユニットに使用され、「failover」が Ethernet0 のインターフェイス名になっています。`hostname(config)#failover interface ip failover 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 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 アドレスと MAC アドレスはフェールオーバー時には変化しません。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 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` 次の例では、Ethernet3 がフェールオーバーに使用されます。

```
hostname(config)#interface ethernet3 hostname(config-if)#no shutdown
```

5. (オプション) 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 リンクとして使用す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、フェールオーバー リンクのステート情報を交換するための Ethernet2 のインターフェイス名として「state」を使用しています。hostname(config)#failover link state Ethernet2 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、指定する必要がある引数は if_name だけです。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。オプションでフェールオーバー リンクとして使用する場合を除き、このインターフェイスを他の目的に使用しないでください。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 リンクまたはデータ インターフェイスが使用されている場合は、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 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。hostname(config)#failover interface ip state 10.0.0.1 255.0.0.0 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。データ インターフェイスを使用していない場合、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。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 リンクまたはデータ インターフェイスが使用されている場合は、この手順をスキップします。インターフェイスはすでに有効になっています。hostname(config)#interface phy_if hostname(config-if)#no shutdown 注: たとえば、このシナリオでは、Ethernet2 がステートフル フェールオーバー リンクに使用されています。hostname(config)#interface ethernet2 hostname(config-if)#no shutdown

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

セカンダリ ユニットの設定

セカンダリ ユニットで必要な設定は、フェールオーバー インターフェイスについてだけです。セカンダリ ユニットでは、最初にプライマリ ユニットと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 ユニットからコンフィギュレーションがセカンダリ ユニットに送信された後、2つのコンフィギュレーションで永続的に異なっているのは、failover lan unit コマンドだけです。このコマンドにより、それぞれのユニットがプライマリまたはセカンダリとして指定されて

います。

マルチ コンテキスト モードの場合、特に指示がない限り、すべての手順をシステム実行スペースで実行します。

セカンダリ ユニットを設定するには、次の手順を実行します。

1. (PIX セキュリティ アプライアンス プラットフォームのみ) 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`
2. フェールオーバー インターフェイスを定義します。プライマリ ユニットに使用したものと同一設定を使用します。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` このドキュメントでは、Ethernet0 が LAN フェールオーバー インターフェイスに使用されています。

`hostname(config)#failover lan interface failover Ethernet3 if_name` 引数により、`phy_if` 引数で指定されているインターフェイスに名前が割り当てられます。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` このドキュメントでは、フェールオーバー リンクを設定するために、10.1.0.1 がアクティブ ユニットに使用され、10.1.0.2 がスタンバイ ユニットに使用され、「failover」が Ethernet0 のインターフェイス名になっています。

`hostname(config)#failover interface ip failover 10.1.0.1 255.255.255.0 standby 10.1.0.2`
注: このコマンドは、プライマリ ユニットでフェールオーバー インターフェイスを設定した際に入力したものと厳密に一致するように入力します。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` たとえば、このシナリオでは、Ethernet0 がフェールオーバーに使用されます。 `hostname(config)#interface ethernet3 hostname(config-if)#no shutdown`

3. (オプション) このユニットをセカンダリ ユニットとして指定します。
`hostname(config)#failover lan unit secondary` **注:** ユニットは、前もって設定されていない限り、デフォルトでセカンダリとして指定されるため、この手順はオプションです。
4. フェールオーバーを有効にします。 `hostname(config)#failover` **注:** 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。
5. 実行コンフィギュレーションの複製が完了した後で、コンフィギュレーションをフラッシュメモリに保存します。 `hostname(config)#copy running-config startup-config`

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 ASA
<pre>ASA#show running-config ASA Version 7.2(3) ! --- To set the firewall mode to transparent mode, !--- use the firewall transparent command !--- in global configuration mode. firewall transparent hostname ASA domain-name default.domain.invalid enable password 2KFQnbNIdI.2KYOU encrypted names ! interface Ethernet0 nameif failover description LAN Failover Interface ! interface Ethernet1 nameif inside security-level 100 ! interface Ethernet2 nameif outside security-level 0 !--- Configure no shutdown in the stateful failover interface</pre>


```

!--- of both Primary and secondary ASA. interface
Ethernet3 nameif state description STATE Failover
Interface ! interface Ethernet4 shutdown no nameif no
security-level no ip address ! interface Ethernet5
shutdown no nameif no security-level no ip address !
passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns
server-group DefaultDNS domain-name
default.domain.invalid access-list 100 extended permit
ip any any pager lines 24 mtu outside 1500 mtu inside
1500 !--- Assign the IP address to the Primary and !---
Secondary ASA Security Appliance. ip address 172.16.1.1
255.255.255.0 standby 172.16.1.2 failover failover lan
unit primary failover lan interface failover Ethernet0
failover lan enable failover key ***** failover link
state Ethernet3 failover interface ip failover 10.1.0.1
255.255.255.0 standby 10.1.0.2 failover interface ip
state 10.0.0.1 255.0.0.0 standby 10.0.0.2 asdm image
flash:/asdm-522.bin no asdm history enable arp timeout
14400 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 snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! 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 prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end

```

セカンダリ ASA

```

ASA#show running-config ASA Version 7.2(3) ! hostname
ASA domain-name default.domain.invalid enable password
2KFQnbNIdI.2KYOU encrypted names ! failover failover lan
unit secondary failover lan interface failover Ethernet0
failover lan enable failover key ***** failover
interface ip failover 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 ASA

```

ASA#show failover Failover On Cable status: N/A - LAN-based failover enabled Failover unit
Primary Failover LAN Interface: failover Ethernet0 (up) Unit Poll frequency 200 milliseconds,
holdtime 800 milliseconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface

```

```
Policy 1 Monitored Interfaces 2 of 250 maximum Version: Ours 7.2(3), Mate 7.2(3) Last Failover
at: 00:08:03 UTC Jan 1 1993 This host: Primary - Active Active time: 1820 (sec) Interface inside
(172.16.1.1): Normal Interface outside (172.16.1.1): Normal Other host: Secondary - Standby
Ready Active time: 0 (sec) Interface inside (172.16.1.2): Normal Interface outside (172.16.1.2):
Normal Stateful Failover Logical Update Statistics Link : state Ethernet3 (up) Stateful Obj xmit
xerr rcv rerr General 185 0 183 0 sys cmd 183 0 183 0 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 0 0 L2BRIDGE Tbl 2 0 0 0 Xlate_Timeout 0 0 0 0 Logical
Update Queue Information Cur Max Total Recv Q: 0 1 7012 Xmit Q: 0 1 185
```

セカンダリ ASA

```
ASA(config)#show failover Failover On Cable status: N/A - LAN-based failover enabled Failover
unit Secondary Failover LAN Interface: failover Ethernet0 (up) Unit Poll frequency 200
milliseconds, holdtime 800 milliseconds Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1 Monitored Interfaces 2 of 250 maximum Version: Ours 7.2(3), Mate 7.2(3) Last
Failover at: 16:39:12 UTC Aug 9 2009 This host: Secondary - Standby Ready Active time: 0 (sec)
Interface inside (172.16.1.2): Normal Interface outside (172.16.1.2): Normal Other host: Primary
- Active Active time: 1871 (sec) Interface inside (172.16.1.1): Normal Interface outside
(172.16.1.1): Normal Stateful Failover Logical Update Statistics Link : state Ethernet3 (up)
Stateful Obj xmit xerr rcv rerr General 183 0 183 0 sys cmd 183 0 183 0 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 0 0 L2BRIDGE Tbl 0 0 0 0
Xlate_Timeout 0 0 0 0 Logical Update Queue Information Cur Max Total Recv Q: 0 1 7043 Xmit Q: 0
1 183
```

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 ASA

```
ASA#show failover state State Last Failure Reason Date/Time This host - Primary Active None
Other host - Secondary Standby Ready Comm Failure 00:02:36 UTC Jan 1 1993 ====Configuration
State=== Sync Done ====Communication State=== Mac set
```

セカンダリ ユニット

```
ASA#show failover state State Last Failure Reason Date/Time This host - Secondary Standby Ready
None Other host - Primary Active 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

```
ASA#show failover interface interface failover Ethernet0 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 interface state Ethernet3
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
```

セカンダリ ユニット

```
ASA#show failover interface interface failover Ethernet0 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 state Ethernet3
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。

プライマリ ASA

```
ASA(config)#show monitor-interface This host: Primary - Active Interface inside (172.16.1.1):
```

Normal Interface outside (172.16.1.1): Normal Other host: Secondary - Standby Ready Interface
inside (172.16.1.2): Normal Interface outside (172.16.1.2): Normal

セカンダリ ASA

```
ASA(config)#show monitor-interface This host: Secondary - Standby Ready Interface inside  
(172.16.1.2): Normal Interface outside (172.16.1.2): Normal Other host: Primary - Active  
Interface inside (172.16.1.1): 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。さまざまなフェールオーバー状態についての詳細は、『[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](#)』の「*show failover*」セクションを参照してください。

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
```

すべてのフェールオーバー 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/スタンバイ フェールオーバーの場合は、アクティブ ユニットで次のコマンドを入力します。hostname(config)#no failover active
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/スタンバイ フェールオーバーの場合は、アクティブ ユニットで次のコマンドを入力します。hostname(config)#failover active

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。

スタンバイ ユニットで次のコマンドを入力します。

```
hostname#failover active
```

アクティブ ユニットで次のコマンドを入力します。

```
hostname#no 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を開始されません。スタンバイ ユニットのアクティブにする (フェールオーバーが無効にされている場合でも) には、「[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](#)

故障したユニットの障害状態を解除するには、次のコマンドを入力します。

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

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。

[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。このセクションでは、次の項目について説明しています。

- [フェールオーバー監視](#)
- [ユニット障害](#)
- [%ASA-3-210005: LU 割り当て接続の失敗](#)
- [フェールオーバーのシステム メッセージ](#)
- [デバッグ メッセージ](#)
- [SNMP](#)
- [既知の問題](#)

[フェールオーバー監視](#)

次の例では、フェールオーバーによりネットワーク インターフェイスの監視が開始されなかった場合の動作を説明しています。フェールオーバーが発生しても、ネットワーク インターフェイスで他方のユニットからの 2 番目の hello パケットが受信されるまでは、そのインターフェイスの監視が開始されません。これには約 30 秒かかります。スパニング ツリー プロトコル (STP) が稼動するネットワーク スイッチにユニットが接続されている場合は、スイッチで設定されている forward delay 時間 (通常は 15 秒に設定) の 2 倍に、この 30 秒の遅延を加えた時間がかかります。これは、ASA のブートアップ時およびフェールオーバー イベントの直後に、ネットワーク スイッチで一時的なブリッジ ループが検出されるためです。このループが検出されると、forward delay 時間だけ、これらのインターフェイスでのパケットの転送が停止されます。その後、スイッチはさらに forward delay 時間だけ listen モードに入り、この間はブリッジ ルー

プのリッスンが行われ、トラフィックの転送は行われません（つまり、フェールオーバーの hello パケットは転送されません）。転送遅延時間 2 回分（30 秒）の後、トラフィック フローが再開されます。各 ASA は、他方のユニットから 30 秒に相当する hello パケットを受信するまで、waiting モードに留まります。ASA では、トラフィックを渡している間は、hello パケットを受信しないことを理由に他のユニットを障害扱いにすることはありません。他のすべてのフェールオーバー、つまり、電源、インターフェイスのリンク喪失、およびフェールオーバー ケーブルの hello の監視は引き続き行われます。

フェールオーバーに関しては、ASA インターフェイスに接続するすべてのスイッチ ポートで PortFast をイネーブルにすることを強く推奨いたします。さらに、これらのポートではチャネリングとトランキングを無効にする必要があります。ASA のインターフェイスがフェールオーバーの間にダウンした場合、スイッチでは、ポートの状態が listening から learning を経て forwarding に移行するまでの間、30 秒間待つ必要はありません。

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Active
Active time: 6930 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
Other host: Secondary - Standby
Active time: 15 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Normal (Waiting)
```

まとめると、フェールオーバーの問題を絞り込むには次の手順を確認します。

- 「待機」 / 「障害」 状況のインターフェイスに接続されているネットワーク ケーブルを調べて、可能であれば交換します。
- 2 つのユニットの間に接続されているスイッチがある場合は、「待機」 / 「障害」 状態のインターフェイスに接続されているネットワークが正常に機能していることを確認します。
- 「待機」 / 「障害」 状況のインターフェイスに接続されているスイッチ ポートを調べて、可能であれば、そのスイッチの別の FE ポートを使用します。
- インターフェイスに接続されているスイッチ ポートで、PortFast を有効にしてあり、トランキングとチャネリングを無効にしてあることを確認します。

ユニット障害

この例では、フェールオーバーによって障害が検出されています。プライマリ ユニットの インターフェイス 1 が障害の原因であることに注意してください。ユニットは、障害のために waiting モードに戻っています。故障したユニットでは、ネットワークから自分自身が削除され（インターフェイスがダウン）、ネットワークには hello パケットが送信されなくなります。アクティブ ユニットは、故障したユニットの交換後にフェールオーバー通信が再開されるまで、waiting 状態に留まります。

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Standby (Failed)
Active time: 7140 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Failed (Waiting)
Other host: Secondary - Active
Active time: 30 (sec)
```

Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)

LU 割り当て接続の失敗

次のエラーメッセージが表示される場合、メモリの問題が存在する可能性があります。

LU

この問題はシスコ バグ ID [CSCte80027](#) ([登録ユーザのみ](#)) に記述されています。この問題を解決するには、この不具合が修正されているソフトウェアバージョンにファイアウォールをアップグレードします。この不具合が修正されている ASA ソフトウェアバージョンは、8.2(4)、8.3(2)、8.4(2) などです。

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。

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](#)』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ィング 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](#)』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` コマンドを使用します。

`failover polltime unit msec [time]` は、スタンバイ ユニットの存在を調べる時間間隔を表すために hello メッセージをポーリングします。

同様に、`failover holdtime unit msec [time]` は、ユニットがフェールオーバー リンクで hello メッ

セージを受信する必要がある時間間隔の設定を表します。この時間が経過すると、ピアユニットは障害として宣言されます。

アクティブ/スタンバイ フェールオーバー設定でデータ インターフェイス ポーリング時間とデータ インターフェイス 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 interface** コマンドを使用します。デフォルトのポーリング時間とホールド時間を復元するには、このコマンドの **no** 形式を使用します。

```
failover polltime interface [msec] time [holdtime time]
```

データ インターフェイス上で hello パケットが送信される頻度を変更するには、**failover polltime interface** コマンドを使用します。このコマンドは、アクティブ/スタンバイ フェールオーバーでのみ使用できます。アクティブ/アクティブ フェールオーバーの場合は、**failover polltime interface** コマンドではなく、フェールオーバー グループ コンフィギュレーション モードで **polltime interface** コマンドを使用します。

インターフェイス ポーリング時間の 5 倍未満の **holdtime** 値は入力できません。より高速なポーリング時間の場合は、セキュリティ アプライアンスではより高速に障害を検出し、フェールオーバーをトリガーすることが可能です。ただし、ネットワークが一時的に輻輳している場合、より高速な検出によって不要な切り替えが発生する可能性があります。ホールド時間の半分を超えてもインターフェイスで hello パケットが受信されない場合、インターフェイス テストが開始されます。

コンフィギュレーションには、**failover polltime unit** コマンドと **failover polltime interface** コマンドのどちらも含めることができます。

次の例では、インターフェイス ポーリング時間の頻度は 500 ミリ秒、ホールド時間は 5 秒に設定されています。

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

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』の「[failover polltime](#)」のセクションを参照してください。

[フェールオーバー設定での証明書/秘密鍵のエクスポート](#)

プライマリ デバイスによって秘密キー/証明書がセカンダリ ユニットへ自動的に複製されます。証明書および秘密鍵を含むコンフィギュレーションをスタンバイ ユニットに複製するには、アクティブ ユニットでコマンド **write memory** を発行します。スタンバイ ユニット上のすべての鍵および証明書は消去され、アクティブ ユニットのコンフィギュレーションによって再入力されます。

注: アクティブ デバイスから証明書、鍵、およびトラストポイントを手動でインポートした後に、スタンバイ デバイスへのエクスポートはしないでください。

[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。

問題：フェールオーバーは透過的でアクティブ/スタンバイな多重モードフェールオーバーを設定した後常にフラップしています

フェールオーバーは両方の ASA の内部インターフェイスが直接接続され、両方の outside インターフェイスが ASA 直接接続される時安定しています。しかしフェールオーバーはスイッチが中間使用される時フラップしています。

解決策： この問題を解決するために ASA インターフェイスの BPDU をディセーブルにしてください。

ASA モジュール フェールオーバー

Advanced Inspection and Prevention Security Services Module (AIP-SSM) または Content Security and Control Security Services Module (CSC-SSM) がアクティブ ユニットとスタンバイユニットで使用されている場合、フェールオーバーに関しては ASA と無関係に動作します。モジュールはアクティブ ユニットとスタンバイユニットに手動で設定される必要があり、フェールオーバーによってモジュールのコンフィギュレーションが複製されることはありません。

フェールオーバーについては、AIP-SSM モジュールまたは CSC-SSM モジュールを備えたどちらの ASA ユニットも、同じハードウェア タイプである必要があります。たとえば、プライマリユニットに ASA-SSM-10 モジュールが含まれている場合、セカンダリユニットにも ASA-SSM-10 モジュール含まれている必要があります。

フェールオーバー メッセージのブロック割り当ての失敗

エラー メッセージ： %PIX|ASA-3-105010: (Primary) Failover message block alloc failed

説明： ブロック メモリが削除されました。これは一時的なメッセージであり、セキュリティ アプライアンスは復旧します。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。

推奨処置： 現在のブロック メモリを監視するために、show blocks コマンドを使用します。

AIP モジュール フェールオーバーの問題

フェールオーバー コンフィギュレーションに 2 つの ASA があり、それぞれに AIP-SSM が含まれている場合、AIP-SSM のコンフィギュレーションを手動で複製する必要があります。フェールオーバー メカニズムによって複製されるのは、ASA の設定だけです。AIP-SSM はフェールオーバーに含まれていません。

まず、フェールオーバーについては、AIP-SSM は ASA とは無関係に動作します。フェールオーバーに関して、ASA の観点から必要なことは、AIP モジュールが同じハードウェア タイプであることです。その他には、フェールオーバーの他の部分と同様に、アクティブとスタンバイの間での ASA のコンフィギュレーションが同期している必要があります。

AIP のセットアップについて言えば、AIP は事実上独立したセンサーです。これら 2 つの間ではフェールオーバーは存在せず、相互に認識していません。コードのバージョンとは無関係に実行することが可能です。つまり、バージョンは一致している必要がなく、ASA では、フェールオーバーに関して、AIP 上でのコードのバージョンを問いません。

AIP 上で設定した管理インターフェイス IP を介して、ASDM により AIP への接続が開始されま

す。つまり、通常は HTTPS を介してセンサーに接続します。接続は、センサーのセットアップ方法に依存します。

IPS (AIP) モジュールとは無関係に ASA のフェールオーバーが発生する可能性があります。接続先は管理 IP であるため、引き続き同じ AIP に接続されています。他方の AIP に接続するには、その管理 IP に再接続して設定およびアクセスを行う必要があります。

[ASA を参照して下さい: ASA から AIP SSM へのネットワークトラフィックの送信の設定例](#)』を参照してください。Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス (ASA) を介して Advanced Inspection and Prevention Security Services Module (AIP-SSM) (IPS) にネットワークトラフィックを送信する方法の詳細および設定例が示されています。

[既知の問題](#)

バージョン 8.x のソフトウェアとバージョン 6.x の ASDM をフェールオーバー コンフィギュレーションに使用しているときに、セカンダリ ASA で ASDM にアクセスしようとした場合、次のエラーが表示されます。

```
Error: The name on the security certificate is invalid or does not match the name of the site
```

証明書では、発行者とサブジェクト名は、アクティブユニットの IP アドレスになります。スタンバイユニットの IP アドレスではありません。

ASA バージョン 8.x では、内部 (ASDM) 証明書はアクティブ ユニットからスタンバイ ユニットに複製されます。その結果、このようなエラー メッセージが表示されます。ただし、バージョン 7.x のコードを実行する 5.x の ASDM 上で同じファイアウォールが動作している場合、ASDM にアクセスしようとする次の通常のセキュリティ警告が表示されます。

```
The security certificate has a valid name matching the name of the page you are trying to view
```

証明書を確認すると、発行者とサブジェクト名がスタンバイ ユニットの IP アドレスになっています。

[関連情報](#)

- [Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス](#)
- [Cisco PIX Firewall ソフトウェア](#)
- [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](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)